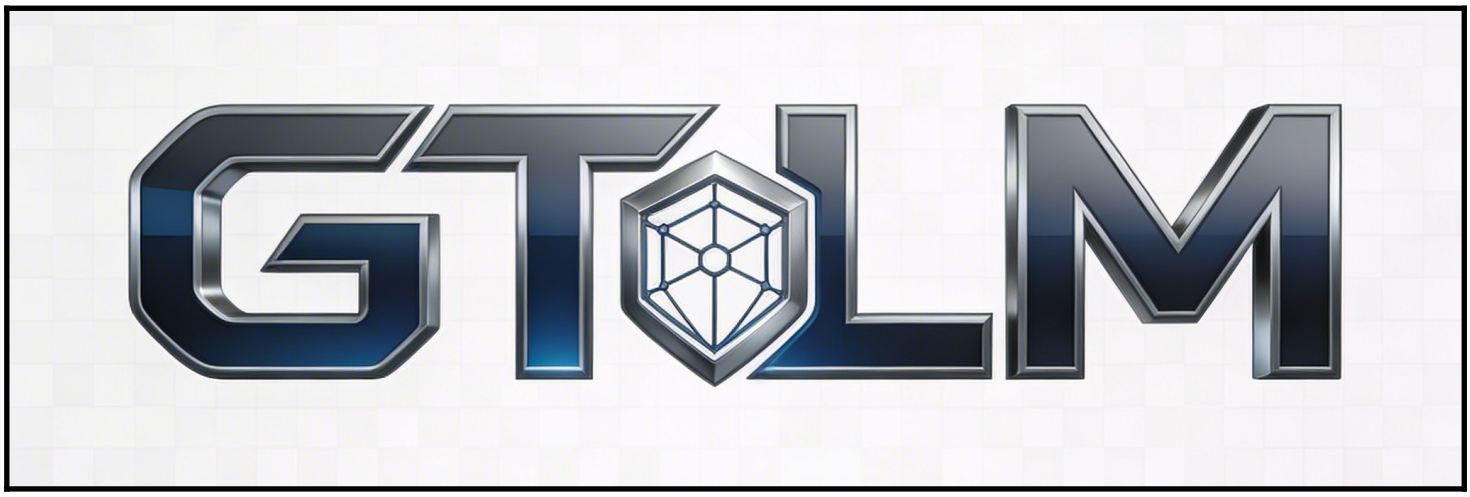
Procédure Technique - Réseau GTLM

Mise en place et paramétrage du Réseau



Gildas CHERAUD BOISTEAU, Lucas MOCQUILLON, Tom GENEST

BTS Service Informatique aux Organisations option SISR

Sommaire

1. Introduction

a. Contexte

Dans le cadre de la mise en place du système d'information de GTLM, une infrastructure réseau segmentée a été mise en place afin d'assurer la communication entre les différents services tout en garantissant la sécurité des échanges.

Cette infrastructure repose sur plusieurs équipements réseau, notamment un pare-feu Fortinet FortiWiFi 60D, deux routeurs Cisco ISR 900 Serie et un switch Catalyst 2960, permettant de structurer le réseau en plusieurs VLAN distincts.

L'objectif est de séparer les usages du système d'information afin d'améliorer la sécurité, la gestion des flux et l'administration globale de l'infrastructure. Les principaux segments réseau sont les suivants :

- un réseau utilisateurs (VLAN 10)
- un réseau serveurs (VLAN 20)
- une zone démilitarisée (VLAN 30)
- un réseau WiFi invités (VLAN 50)
- un réseau de management (VLAN 90)

Cette architecture s'inscrit dans une logique de maquette fonctionnelle visant à reproduire une infrastructure d'entreprise complète, intégrant à la fois des services internes et des services exposés.

b. Objectif de la procédure

Cette procédure technique a pour objectif de décrire l'ensemble des étapes nécessaires à la mise en place et à la configuration de l'infrastructure réseau GTLM.

Elle constitue un document de référence permettant :

- de reproduire l'architecture réseau
- de comprendre le rôle de chaque équipement
- de faciliter les opérations de maintenance et de dépannage
- d'assurer la cohérence des configurations au sein du système d'information

Ce document détaille les configurations techniques des équipements réseau, notamment les règles de filtrage, le routage, la segmentation VLAN et l'interconnexion des différents éléments de l'infrastructure.

Périmètre : cette procédure concerne les équipements actifs suivants :

- FortiWiFi 60D (FWF60D-GTLM)

- Routeurs Cisco ISR 900 Series (R1-ISR900-GTLM et R2-ISR900-GTLM)
- Switch Cisco Catalyst 2960

Elle ne couvre pas la configuration des machines virtuelles Proxmox ni les services applicatifs (GLPI, Zabbix, Nextcloud,AD), qui font l'objet d'une procédure dédiée.

c. Plan d'adressage du SI

L'infrastructure réseau repose sur un plan d'adressage structuré permettant de segmenter les différents usages du système d'information.

VLANs

VLAN	Nom	Réseau	Passerelle virtuelle	Plage DHCP
Transit	Lien Firewall - Routeurs	172.16.0.0/29	172.16.0.1 (Forti)	—
10	Utilisateurs	192.168.10.0/24	192.168.10.254 (HSRP)	100 – 200
20	Serveurs	192.168.20.0/24	192.168.20.254 (HSRP)	198 – 200 (tests)
30	DMZ	192.168.30.0/24	192.168.30.1 (Forti)	—
50	WiFi GTLM	192.168.50.0/24	192.168.50.1 (Forti)	2 – 254
90	Management	192.168.90.0/24	192.168.90.254 (HSRP)	—

Lien inter-équipements (réseau transit 172.16.0.0/29)

Équipement	Interface	Adresse IP	Rôle
FortiWiFi FWF60D	LAN	172.16.0.1 /29	Passerelle par défaut des ISR
R1-ISR900-GTLM	GigabitEthernet4	172.16.0.2 /29	Routeur principal (HSRP Active)
R2-ISR900-GTLM	GigabitEthernet4	172.16.0.3 /29	Routeur secondaire (HSRP Standby)

Services VLAN 20 – Réseau serveurs

Service / VM	Adresse IP	Rôle
SRV-AD01	192.168.20.50/24	Active Directory / DNS / DHCP
Proxmox PROD	192.168.20.2/24	Hyperviseur production
Proxmox Backup	192.168.20.3/24	Hyperviseur backup
GLPI	192.168.20.11/24	Gestion des actifs IT
Zabbix	192.168.20.13/24	Supervision réseau
Nginx Proxy Manager	192.168.20.15/24	Reverse proxy
Vaultwarden	192.168.20.25/24	Coffre mots de passe
Ubackup	192.168.20.123/24	Sauvegardes (PBS)

Services VLAN 30 – DMZ

Service / VM	Adresse IP	Rôle
Nextcloud	192.168.30.12/24	Collaboration / stockage fichiers

d. Intégration de l'infrastructure réseau

L'infrastructure réseau s'intègre dans un environnement global comprenant des services virtualisés hébergés sur des serveurs Proxmox.

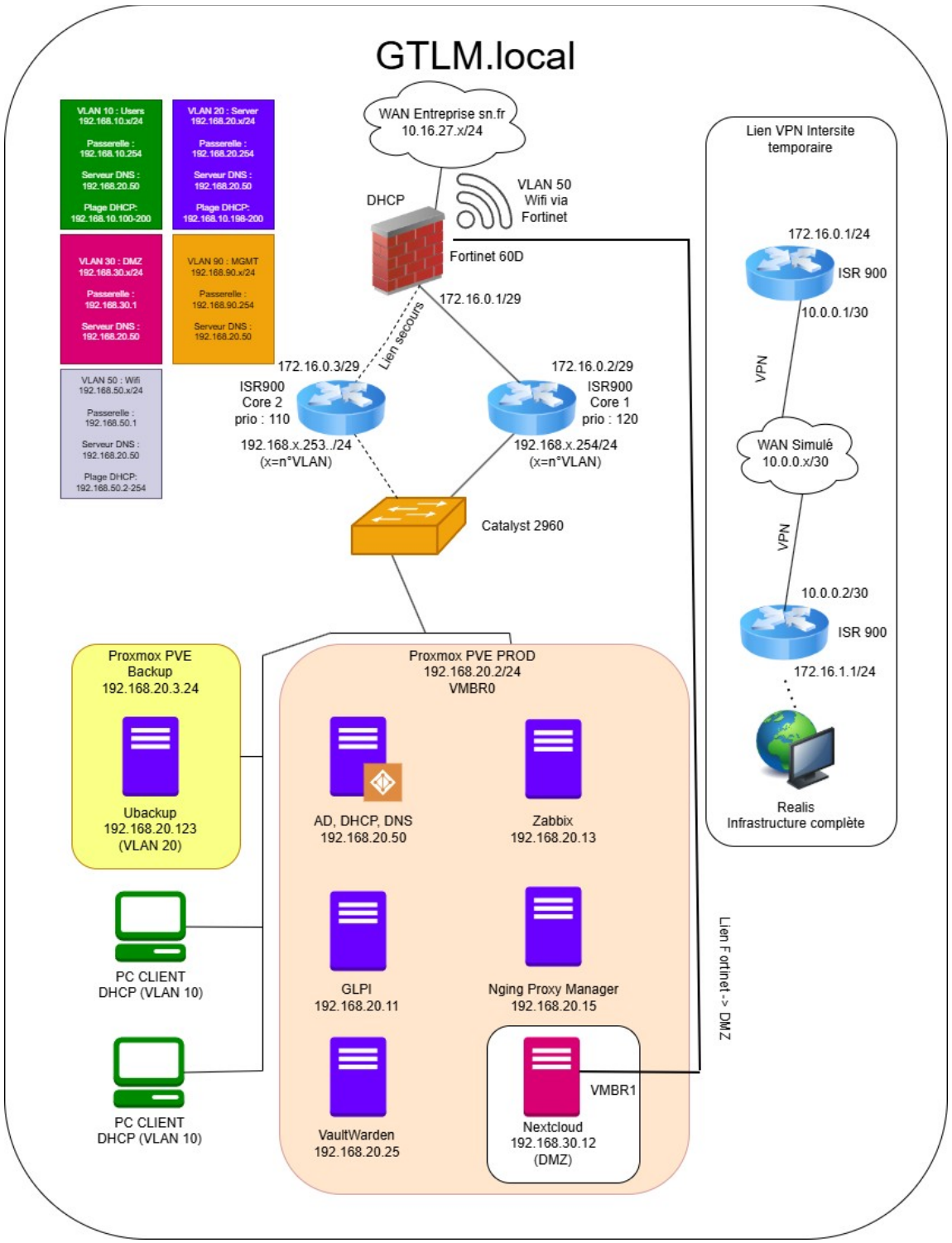
Le **switch Catalyst 2960** assure la segmentation du réseau via la configuration des VLAN et des ports en mode access ou trunk. Il est segmenter par slots de port, pour un segmentation visuel

Les **routeurs Cisco ISR 900 (R1 et R2)** assurent le routage inter-VLAN via des sous-interfaces (router-on-a-stick) et la redondance de passerelle via HSRPv2. Ils effectuent également le NAT PAT vers internet via le FortiWifi.

Le **FortiWiFi 60D** joue un rôle central dans la sécurisation de l'infrastructure :

- filtrage des flux entre LAN, DMZ et WAN
- gestion des accès externes (Internet via SN.fr)
- isolation du réseau WiFi GTLM (VLAN 50)
- gestion directe de la DMZ

Topologie réseau :



Interconnexion inter-site (VPN IPsec – POC)

Dans le cadre de l'évolution du système d'information, une interconnexion entre le site principal de GTLM et un site distant a été mise en place sous forme de maquette (Proof of Concept).

Cette interconnexion repose sur un tunnel VPN site-à-site IPsec établi entre deux routeurs Cisco ISR 900. Dans ce contexte :

- le lien WAN est simulé via un réseau dédié (10.0.0.0/30)
- les réseaux distants utilisent des plages d'adressage distinctes (172.16.0.0/24 et 172.16.1.0/24)
- le tunnel VPN est établi entre les deux routeurs ISR 900

Il s'agit d'une maquette de validation et non d'un déploiement en production. La configuration détaillée du VPN fait l'objet d'une documentation dédiée.

2. Configuration du Switch Catalyst 2960

Prérequis

- Accès console au switch
- IOS version 12.2 ou supérieure
- Câbles trunk connectés vers R1, R2 et le FortiWifi

Sauvegarde préalable

Avant toute modification, sauvegarder la configuration actuelle :

```
Switch# copy running-config startup-config
Switch# copy running-config tftp
```

2.1 Création des VLANs

```
Switch# conf t
Switch(config)# vlan 10
Switch(config-vlan)# name Utilisateurs
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name Serveurs
Switch(config-vlan)# exit
Switch(config)# vlan 30
Switch(config-vlan)# name DMZ
```

```
Switch(config-vlan)# exit
Switch(config)# vlan 90
Switch(config-vlan)# name Management
Switch(config-vlan)# exit
```

2.2 Configuration des ports Access

Ports	Mode	VLAN	Description
Fa0/1 – Fa0/12	access	10	Postes utilisateurs
Fa0/13 – Fa0/24	access	20	Serveurs VLAN 20
Fa0/25 – Fa0/36	access	30	DMZ
Gi0/2	access	30	Accès DMZ supplémentaire

Exemple de configuration des slots de ports access :

```
Switch(config)# interface range FastEthernet0/1 - 12
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
```

2.3 Configuration des ports Trunk

Port	VLANs autorisés	VLAN natif	Options
Fa0/37	10, 20, 30, 90	—	—
Fa0/38	10, 20, 30, 90	—	—
Fa0/39	10, 20, 90	90	Pas de VLAN 30
Fa0/40	10, 20, 30, 90	—	—
Fa0/47	10, 20, 30, 90	90	portfast trunk
Gi0/1	10, 20, 30, 90	90	portfast trunk

Exemple de configuration d'un port trunk :

```
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport trunk native vlan 90
Switch(config-if)# switchport trunk allowed vlan 10,20,30,90
```

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree portfast trunk
Switch(config-if)# exit
```

2.4 Interface de management (VLAN 90)

```
Switch(config)# interface vlan 90
Switch(config-if)# ip address 192.168.90.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

2.5 Vérifications switch

```
Switch# show vlan brief
Switch# show interfaces trunk
Switch# show run
```

3. Configuration des routeurs Cisco ISR 900 (HSRP)

Prérequis

- Accès console sur chaque routeur
- IOS 15.8 avec licence Security (`securityk9`) – modèle C921-4P
- Trunk actif depuis le switch sur le port GigabitEthernet5

Sauvegarde préalable

```
Router# copy running-config startup-config
Router# copy running-config tftp
```

3.1 Tracking de l'interface WAN

Le tracking permet à HSRP de détecter une panne de l'interface WAN et de déclencher la bascule :

```
R1(config)# track 1 interface GigabitEthernet4 line-protocol
```

Appliquer la même commande sur R2.

3.2 Interface WAN vers FortiGate

```
R1(config)# interface GigabitEthernet4
R1(config-if)# ip address 172.16.0.2 255.255.255.248
R1(config-if)# ip nat outside
R1(config-if)# no shutdown
R1(config-if)# exit
```

Sur **R2** : remplacer 172.16.0.2 par 172.16.0.3.

3.3 Sous-interfaces VLAN (Router-on-a-stick)

La configuration HSRP est identique sur R1 et R2, seules les adresses IP physiques et les priorités diffèrent. Comme montrer si dessous

Tableau des paramètres HSRP par VLAN

VLAN	IP R1 (Active)	IP R2 (Standby)	IP virtuelle HSRP	Prio R1	Prio R2
10	192.168.10.252	192.168.10.253	192.168.10.254	120	110
20	192.168.20.252	192.168.20.253	192.168.20.254	120	110
90	192.168.90.252	192.168.90.253	192.168.90.254	120	110

Configuration complète sur R1

```
R1(config)# interface GigabitEthernet5.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.252 255.255.255.0
R1(config-subif)# ip helper-address 192.168.20.50
R1(config-subif)# ip nat inside
R1(config-subif)# ip access-group VLAN10-IN in
R1(config-subif)# standby version 2
R1(config-subif)# standby 10 ip 192.168.10.254
R1(config-subif)# standby 10 priority 120
R1(config-subif)# standby 10 preempt delay minimum 30
R1(config-subif)# standby 10 track 1 decrement 20
R1(config-subif)# exit

R1(config)# interface GigabitEthernet5.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.252 255.255.255.0
R1(config-subif)# ip nat inside
R1(config-subif)# standby version 2
```

```
R1(config-subif)# standby 20 ip 192.168.20.254
R1(config-subif)# standby 20 priority 120
R1(config-subif)# standby 20 preempt delay minimum 30
R1(config-subif)# standby 20 track 1 decrement 20
R1(config-subif)# exit

R1(config)# interface GigabitEthernet5.90
R1(config-subif)# encapsulation dot1Q 90 native
R1(config-subif)# ip address 192.168.90.252 255.255.255.0
R1(config-subif)# ip nat inside
R1(config-subif)# standby version 2
R1(config-subif)# standby 90 ip 192.168.90.254
R1(config-subif)# standby 90 priority 120
R1(config-subif)# standby 90 preempt delay minimum 30
R1(config-subif)# standby 90 track 1 decrement 20
R1(config-subif)# exit
```

Sur **R2** : remplacer .252 par .253 et la priorité 120 par 110 pour chaque VLAN.

3.4 NAT PAT (accès Internet)

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R1(config)# access-list 1 permit 192.168.90.0 0.0.0.255
R1(config)# ip nat inside source list 1 interface GigabitEthernet4 overload
```

3.5 Routes statiques

```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.1
```

Appliquer la même commande sur R2.

3.6 ACL VLAN 10 – Filtrage des flux utilisateurs

L'ACL `VLAN10-IN` est appliquée en entrée sur la sous-interface `GigabitEthernet5.10` des deux routeurs. Elle contrôle les flux émis depuis les postes utilisateurs (VLAN 10) :

```
ip access-list extended VLAN10-IN
 ! Autoriser DHCP (relay)
 permit udp any any eq bootps bootpc
 ! Autoriser HTTP/HTTPS vers serveurs internes
 permit tcp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 eq www 443
 ! Autoriser DNS vers n'importe quel serveur
 permit udp 192.168.10.0 0.0.0.255 any eq domain
```

```
! Autoriser LDAP vers AD
permit tcp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 eq 389
! Autoriser accès complet vers 192.168.20.10
permit ip 192.168.10.0 0.0.0.255 host 192.168.20.10
! Autoriser HTTP/HTTPS vers Nextcloud (DMZ)
permit tcp 192.168.10.0 0.0.0.255 host 192.168.30.12 eq www 443
! Autoriser ping vers Nextcloud uniquement
permit icmp 192.168.10.0 0.0.0.255 host 192.168.30.12
! Bloquer tout accès direct au reste de la DMZ (log activé)
deny   ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 log
! Autoriser le reste (accès Internet)
permit ip 192.168.10.0 0.0.0.255 any
```

3.7 Vérifications routeurs

```
Router# show standby brief
Router# show ip route
Router# show ip nat translations
Router# show ip access-lists VLAN10-IN
Router# show track 1
Router# show run
```

4. Configuration du FortiWiFi 60D

Prérequis

- Accès à l'interface web 172,16,0,1 ou accès console
- Interface lan connectée au réseau transit (172.16.0.0/29)
- Interface dmz connectée au switch (VLAN 30)
- Interface wan1 connectée au WAN (SN.fr) en DHCP

4.1 Interfaces réseau

Interface	Adresse IP	Masque	Rôle
wan1	DHCP (SN.fr)	/24	Accès Internet
lan	172.16.0.1	/29	Lien vers routeurs ISR900
dmz	192.168.30.1	/24	Zone démilitarisée
wifi-GTLM	192.168.50.1	/24	Réseau WiFi

```
config system interface
    edit "lan"
        set ip 172.16.0.1 255.255.255.248
        set allowaccess ping https ssh http
        set role lan
    next
    edit "dmz"
        set ip 192.168.30.1 255.255.255.0
        set allowaccess ping https http
        set role dmz
    next
    edit "wifi-GTLM"
        set ip 192.168.50.1 255.255.255.0
        set role lan
    next
end
```

4.2 DNS système

```
config system dns
    set primary 192.168.20.50
    set secondary 8.8.8.8
    set domain "GTLM.local"
end
```

4.3 Routes statiques

```
config router static
    edit 1
        set dst 192.168.10.0 255.255.255.0
        set gateway 172.16.0.2
        set device "lan"
    next
    edit 2
        set dst 192.168.20.0 255.255.255.0
        set gateway 172.16.0.2
        set device "lan"
    next
    edit 3
        set dst 192.168.90.0 255.255.255.0
        set gateway 172.16.0.2
        set device "lan"
    next
```

```
  edit 4
    set dst 192.168.30.0 255.255.255.0
    set gateway 192.168.30.1
    set device "dmz"
  next
end
```

Le FortiWifi utilise 172.16.0.2 (R1 active) comme passerelle vers les VLAN internes. En cas de bascule HSRP, R2 prend l'IP virtuelle et le trafic continue sans modification.

4.4 Politiques firewall

ID	Nom	Src Intf	Dst Intf	Services	Action	NAT
1	Cisco-Internet	lan	wan1	ALL	ACCEPT	Oui
2	DMZ	dmz	wan1	ALL	ACCEPT	Oui
3	lan to dmz	lan	dmz	HTTP, HTTPS, PING, RDP	ACCEPT	Non
4	wifi_GTLM	wifi-GTLM	wan1	ALL	ACCEPT	Oui
5	Wifi to DMZ	wifi-GTLM	dmz	HTTP , HTTPS	ACCEPT	NON

```
config firewall policy
 edit 1
 set name "Cisco-Internet"
 set srcintf "lan"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
 edit 2
 set name "DMZ"
 set srcintf "dmz"
 set dstintf "wan1"
 set srcaddr "all"
```

```
set dstaddr "all"
set action accept
set schedule "always"
    set service "ALL"
    set nat enable
  next
  edit 3
    set name "lan to dmz"
    set srcintf "lan"
    set dstintf "dmz"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "HTTP" "HTTPS" "PING" "RDP"
    set nat enable
  next
  edit 4
    set name "wifi_GTLM"
    set srcintf "wifi-GTLM"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable
  next
  edit 5
    set name "WIFI_TO_DMZ_NEXTCLOUD"
    set srcintf "wifi-guest"
    set dstintf "dmz"
    set srcaddr "all"
    set dstaddr "NEXTCLOUD_DMZ"
    set action accept
    set schedule "always"
    set service "HTTP" "HTTPS"
    set nat disable
  next
end
```

4.5 DHCP WiFi GTLM (VLAN 50)

Le FortiWifidistribue directement les adresses IP pour le réseau WiFi :

```
config system dhcp server
 edit 1
 set default-gateway 192.168.50.1
 set netmask 255.255.255.0
 set interface "wifi-GTLM"
 config ip-range
 edit 1
 set start-ip 192.168.50.2
 set end-ip 192.168.50.254
 next
 end
 set dns-server1 192.168.50.1
 next
end
```

4.6 WiFi – SSID GTLM

```
config wireless-controller vap
   edit "wifi-GTLM"
      set ssid "WIFI-GTLM"
      set schedule "always"
   next
end
```

4.7 Vérifications FortiGate

```
FWF60D-GTLM # show system interface
FWF60D-GTLM # show system dns
FWF60D-GTLM # show router static
FWF60D-GTLM # show firewall policy
FWF60D-GTLM # show firewall address
FWF60D-GTLM # show firewall addrgrp
FWF60D-GTLM # show firewall service group
FWF60D-GTLM # show firewall service custom
FWF60D-GTLM #  show system admin
FWF60D-GTLM # show user local
FWF60D-GTLM # show vpn ssl settings
FWF60D-GTLM # show wireless-controller vap
FWF60D-GTLM # show system dhcp server
```

4 .8 DNS local du WIFI-GTLM

```
config system dns-database
   edit "gtlm.local"
      set domain "gtlm.local"
      set view shadow
      set authoritative enable
      config dns-entry
         edit 1
            set hostname "nextcloud"
            set ip 192.168.30.12
            set type A
         next
      end
   next
end

config system dns-server
   edit "wifi-guest"
      set mode recursive
   next
end
```

5. Tests et vérifications

Matrice des flux attendus

Source	Destination	Service	Résultat attendu	Équipement de contrôle
VLAN 10	192.168.20.50 (AD)	HTTP/HTTPS	Autorisé	ACL VLAN10-IN
VLAN 10	192.168.20.50 (AD)	DNS (UDP 53)	Autorisé	ACL VLAN10-IN
VLAN 10	192.168.30.12 (Nextcloud)	HTTP/HTTPS	Autorisé	ACL VLAN10-IN
VLAN 10	192.168.30.12 (Nextcloud)	ICMP	Autorisé	ACL VLAN10-IN
VLAN 10	192.168.30.1 (DMZ gateway)	Tout	Bloqué (log)	ACL VLAN10-IN
VLAN 50 (WiFi)	192.168.20.50	Tout	Bloqué	FortiWifi

VLAN 50 (WiFi)	8.8.8.8 (Internet)	Tout	Autorisé	FortiWifi
VLAN 50 (Wifi)	192.168.30.12	HTTP/HTTPS	Autorisé	FortiWifi
DMZ	192.168.20.0/24	Tout	Bloqué	FortiWifi(pas de politique)

Test 1 – Connectivité inter-VLAN

Objectif : Vérifier que le routage inter-VLAN fonctionne correctement via les routeurs ISR en HSRP.

Procédure (depuis un poste VLAN 10) :

```
ping 192.168.20.50   → AD/DHCP (doit répondre)
ping 192.168.30.12   → Nextcloud (doit répondre)
ping 192.168.90.1    → Switch management (doit répondre)
ping 8.8.8.8         → Internet (doit répondre)
```

Résultat attendu : réponses ICMP sans perte de paquets.

Test 2 – Relay DHCP VLAN 10

Objectif : Vérifier qu'un poste du VLAN 10 obtient une adresse IP depuis le serveur AD (192.168.20.50).

Procédure :

1. Connecter un poste sur un port Fa0/1 à Fa0/12 du switch
2. Forcer un renouvellement DHCP : `ipconfig /release -- ipconfig /renew` (Windows)
3. Vérifier l'adresse obtenue : doit être dans 192.168.10.100 – 192.168.10.200
4. Vérifier la passerelle reçue : 192.168.10.254
5. Vérifier le DNS reçu : 192.168.20.50

Test 3 – Bascule HSRP

Objectif : Vérifier la bascule automatique en cas de panne de R1.

Procédure :

1. Vérifier l'état initial : `R1# show standby brief` → R1 doit être **Active**, R2 **Standby**
2. Simuler une panne en déconnectant l'interface WAN de R1 : `R1(config)# interface GigabitEthernet4` → `shutdown`
3. Attendre ~30 secondes (délai preempt configuré)
4. Vérifier la bascule : `R2# show standby brief` → R2 doit passer **Active**
5. Tester la connectivité depuis un poste VLAN 10 vers Internet
6. Remettre en service R1 : `R1(config)# interface GigabitEthernet4` → `no shutdown`
7. Vérifier que R1 reprend le rôle Active (preempt configuré)

Résultat attendu : interruption de moins de 30 secondes, R1 reprend le rôle Active après rétablissement.

Test 4 – Filtrage ACL VLAN 10

Objectif : Vérifier que les restrictions ACL sont bien appliquées.

```
# Depuis un poste VLAN 10
ping 192.168.30.12          → doit répondre (ICMP autorisé)
curl http://192.168.30.12   → doit fonctionner (HTTP autorisé)
ping 192.168.30.1           → doit échouer (passerelle DMZ bloquée)
telnet 192.168.30.5 22      → doit échouer (accès SSH DMZ bloqué)
```

Vérification des logs sur le routeur :

```
Router# show ip access-lists VLAN10-IN
```

Test 5 – Isolation WiFi GTLM

Objectif : Vérifier que le WiFi GTLM n'accède pas au réseau interne mais a la DMZ.

```
# Depuis un équipement connecté au SSID WIFI-GTLM
ping 192.168.20.50   → doit échouer (réseau serveurs)
ping 192.168.10.1    → doit échouer (réseau utilisateurs)
ping 192.168.30.12   → doit répondre (réseau DMZ - Nextcloud)
ping 8.8.8.8         → doit répondre (Internet autorisé)
```

Test 6 – Résolution DNS interne

Objectif : Vérifier que les noms internes sont résolus depuis les postes VLAN 10.

```
# Depuis un poste VLAN 10 avec le DNS en 192.168.20.50
nslookup glpi.gtlm.local    → doit retourner 192.168.20.11
```

nslookup nextcloud.gtlm.local → doit retourner 192.168.30.12
nslookup vault.gtlm.local → doit retourner 192.168.20.25

Objectif : Vérifier que les noms internes sont résolus depuis les postes sur le wifi.

#Depuis un poste connecter en Wifi avec le DNS en 192.168.50.1

nslookup nextcloud.gtlm.local → doit retourner 192.168.30.12

Tableau récapitulatif des tests

Test	Objectif	Résultat attendu
1 – Inter-VLAN	Ping depuis VLAN 10 vers VLAN 20, 30, 90	Réponses ICMP sans perte
2 – DHCP Relay	Obtention d'adresse IP VLAN 10	IP dans .100-.200, passerelle .254, DNS .50
3 – HSRP	Bascule automatique si R1 tombe	Interruption < 30s, R2 Active, R1 reprend
4 – ACL VLAN10	Vérification filtrage	Trafic non autorisé bloqué, log généré
5 – WiFi GTLM	Isolation réseau invités	Pas d'accès LAN interne, Internet & DMZ - OK
6 – DNS interne	Résolution noms GTLM.local	Réponses correctes depuis SRV-AD01

7. Erreurs courantes rencontrées

Symptôme	Cause probable	Commande de diagnostic	Solution
Aucune passerelle HSRP active	Priorités identiques sur R1 et R2	show standby brief	Corriger la priorité : standby 10 priority 120
Poste VLAN 10 sans adresse IP	ip helper-address absent ou incorrect	show run int Gi5.10	Ajouter ip helper-address 192.168.20.50 sur Gi5.10

VLAN non visible sur trunk	VLAN non autorisé sur le port trunk	show interfaces trunk	switchport trunk allowed vlan add X
Nextcloud inaccessible depuis VLAN 10	ACL trop restrictive	show ip access-lists VLAN10-IN	Vérifier les règles permit vers host 192.168.30.12
WiFi GTLM accède au réseau interne	Politique Fortinet wifi-GTLM → lan existante	get firewall policy	Supprimer la politique non souhaitée
Pas d'accès Internet depuis VLAN 10	Route par défaut manquante ou NAT incorrect	show ip route + show ip nat trans	Vérifier ip route 0.0.0.0 0.0.0.0 172.16.0.1 et NAT PAT
R2 ne reprend pas le rôle Active	Preempt non configuré sur R2	show standby	Ajouter standby 10 preempt sur R2
DNS interne non résolu	Mauvais serveur DNS distribué par DHCP	ipconfig /all (Windows)	Vérifier le DHCP scope sur SRV-AD01

8. Conclusion

La mise en place de cette infrastructure réseau a permis de structurer le système d'information de GTLM autour d'une architecture segmentée, redondante et sécurisée.

L'utilisation de VLANs permet de séparer les différents usages du réseau : postes utilisateurs, serveurs, DMZ, WiFi invités et administration. Le routage inter-VLAN, assuré par les routeurs Cisco ISR 900 en HSRPv2, garantit la haute disponibilité des passerelles avec une bascule automatique en moins de 30 secondes en cas de panne.

Le pare-feu FortiWiFi 60D assure le filtrage des flux, la gestion des accès au réseau externe ainsi que la sécurisation des services exposés en DMZ. Le switch Catalyst 2960 assure la gestion des VLANs, l'interconnexion des équipements via des ports trunk & access .

9. Nomenclature

- **ACL (Access Control List)** : liste de règles permettant d'autoriser ou de bloquer des flux réseau selon l'adresse source, destination, le protocole et les ports
- **ACL étendue** : type d'ACL filtrant selon l'adresse source, destination, le protocole et les ports (utilisée ici : VLAN10-IN)
- **DHCP Relay (ip helper-address)** : fonctionnalité permettant de relayer les requêtes DHCP broadcast vers un serveur DHCP distant, sur un autre sous-réseau
- **DMZ (Demilitarized Zone)** : zone réseau isolée hébergeant les services accessibles depuis l'extérieur, tout en protégeant le réseau interne
- **DNS (Domain Name System)** : service permettant la résolution de noms de domaine en adresses IP, ici assuré par le serveur Active Directory (192.168.20.50)
- **dot1Q (802.1Q)** : protocole d'encapsulation VLAN utilisé sur les liens trunk
- **FortiWiFi 60D** : pare-feu matériel Fortinet assurant le filtrage, le NAT, la gestion du WiFi et la sécurisation des zones réseau
- **HSRP (Hot Standby Router Protocol)** : protocole Cisco de redondance de passerelle permettant à deux routeurs de partager une adresse IP virtuelle
- **ip helper-address** : voir DHCP Relay
- **NAT PAT (Network Address Translation / Port Address Translation)** : traduction d'adresses permettant à plusieurs hôtes de partager une seule adresse publique internet
- **Portfast** : option STP permettant à un port de passer immédiatement en état forwarding, sans attendre la convergence STP (utilisé sur les ports trunk vers routeurs)
- **Preempt (HSRP)** : option permettant au routeur avec la plus haute priorité de reprendre automatiquement le rôle Active lors de son retour en ligne
- **Router-on-a-stick** : technique de routage inter-VLAN via des sous-interfaces sur un seul port physique (ici GigabitEthernet5 des ISR921)
- **STP (Spanning Tree Protocol)** : protocole évitant les boucles réseau en désactivant les liens redondants – le switch est configuré en root bridge (priorité 4096)
- **Trunk** : lien réseau transportant plusieurs VLANs simultanément via l'encapsulation 802.1Q
- **VLAN (Virtual Local Area Network)** : segmentation logique d'un réseau physique permettant d'isoler différents types de trafic sur une même infrastructure
- **WAN (Wide Area Network)** : réseau étendu permettant l'accès à Internet (ici via FAI SN.fr)
- **WLAN (Wireless Local Area Network)** : réseau local sans fil (ici SSID WIFI-GTLM sur VLAN 50)
- **DNS Database (FortiWiFi)** : zone DNS locale créée sur le FortiWiFi permettant de résoudre les noms internes (ex : nextcloud.gtlm.local → 192.168.30.12) pour les clients du réseau WiFi.

Document rédigé dans le cadre du BTS SIO SISR – GTLM – Promo 24-26