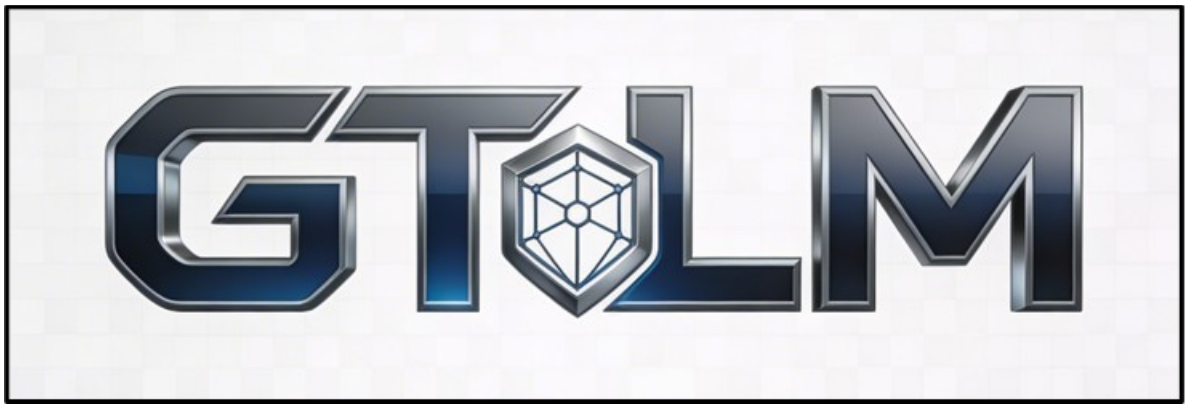
# DOE
# Infrastructure GTLM



# Table des matières

# Présentation générale

Ce document a pour objectif de présenter de manière synthétique et technique l'environnement d'infrastructure mis en place dans le cadre de l'épreuve E6 du BTS SIO option SISR. L'environnement présenté correspond à une maquette de système d'information d'entreprise nommée GTLM, construite afin de reproduire un contexte professionnel réaliste autour de la virtualisation, de l'administration système, de la segmentation réseau, de la sécurisation des flux et du déploiement de services d'infrastructure.

L'infrastructure repose sur une architecture virtualisée sous Proxmox VE, associée à un découpage logique par VLAN et à l'utilisation d'équipements réseau Cisco et Fortinet. Plusieurs services y sont intégrés afin de répondre à des besoins de centralisation, de supervision, de collaboration, de gestion des utilisateurs, de sauvegarde et d'interconnexion sécurisée entre sites.

# Objectif du DOE

Le DOE a pour finalité de permettre au jury de comprendre rapidement l'environnement technique global, les choix d'architecture effectués, le rôle des différents composants et la cohérence de l'ensemble des réalisations professionnelles intégrées à la maquette GTLM.

# Contexte

La maquette GTLM a été conçue pour simuler le fonctionnement d'une PME disposant d'un système d'information structuré. Le besoin identifié était de disposer d'un environnement complet permettant d'héberger plusieurs services d'infrastructure, tout en garantissant leur séparation logique, leur accessibilité et un premier niveau de sécurité.

Dans ce cadre, plusieurs problématiques ont été traitées : l'hébergement centralisé des services, la mise en place d'un cloud collaboratif, l'administration centralisée des utilisateurs et des postes, la supervision de l'infrastructure, la sauvegarde des données ainsi que l'interconnexion sécurisée entre deux sites distincts.

# Architecture de l'infrastructure

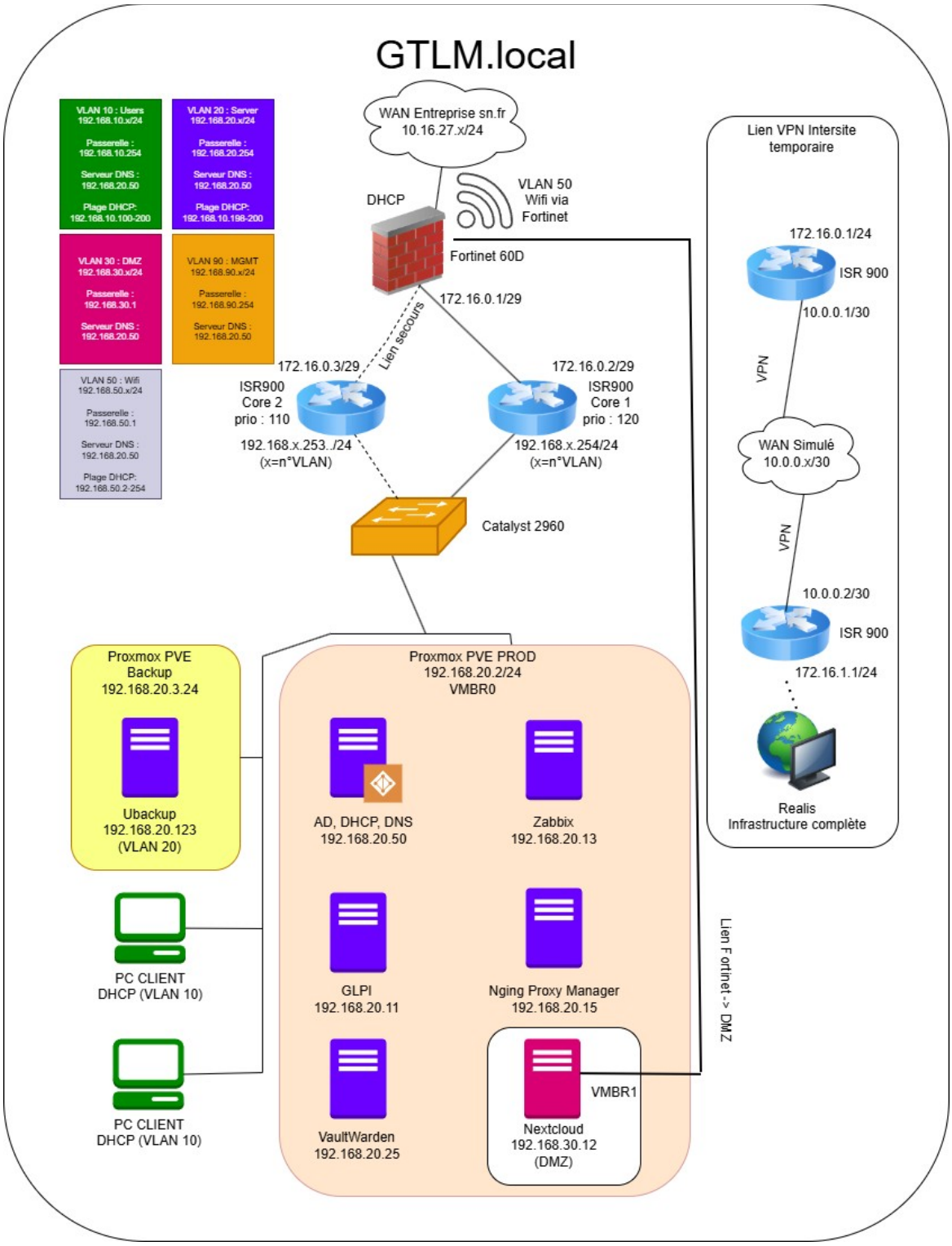
L'environnement s'appuie sur deux serveurs Proxmox VE, un pare-feu FortiWifi 60D, deux routeurs Cisco ISR 900 en HSRP et un switch Cisco Catalyst 2960. Cette architecture permet d'héberger les machines virtuelles et conteneurs nécessaires au fonctionnement des différents services, tout en assurant une segmentation réseau cohérente.

Le réseau est segmenté en plusieurs VLAN afin d'isoler les usages et de limiter la surface d'exposition. Les principaux segments documentés sont le VLAN 10 pour les utilisateurs, le VLAN 20 pour les serveurs, le VLAN 30 pour la DMZ et le VLAN 90 pour l'administration.

# Plan d'adressage principal

| Élément | Adresse / Réseau | Rôle |
|---|---|---|
| VLAN 10 | 192.168.10.0/24 | Réseau utilisateurs |
| VLAN 20 | 192.168.20.0/24 | Réseau serveurs |
| VLAN 30 | 192.168.30.0/24 | DMZ |
| VLAN 90 | 192.168.90.0/24 | Management |
| GW Vlan 10/20/90 | 192.168.20.254 HSRP | Passerelle des ISR |
| GW Vlan 30 | 192.168.30.1 DMZ | Passerelle du Fortiwifi DMZ |
| Proxmox PROD | 192.168.20.2:8006 // pve.gtlm.local:8006 | Hyperviseur principal |
| Proxmox Backup | 192.168.20.3:8006 // pvebackup.gtlm.local:8006 | Hébergement de la sauvegarde |
| AD / DNS / DHCP | 192.168.20.50 | Contrôleur de domaine |
| GLPI | 192.168.20.11 // glpi.gtlm.local | ITSM / gestion de parc |
| Zabbix | 192.168.20.13/zabbix/ // zabbix.gtlm.local/zabbix | Supervision |
| Nginx Proxy Manager | 192.168.20.15 | Publication / reverse proxy |
| Vaultwarden | 192.168.20.25 // vault.gtlm.local | Gestionnaire de mots de passe |
| UrBackup | 192.168.20.123 | Sauvegarde |
| Nextcloud | 192.168.30.12 // nextcloud.gtlm.local/nextcloud | Cloud collaboratif en DMZ |

# Schéma réseau :


GTLM.local
VLAN 10 : Users
192.168.10.x/24
Passerelle :
192.168.10.254
Serveur DNS :
192.168.20.50
Plage DHCP:
192.168.10.100-200
VLAN 20 : Server
192.168.20.x/24
Passerelle :
192.168.20.254
Serveur DNS :
192.168.20.50
Plage DHCP:
192.168.10.198-200
VLAN 30 : DMZ
192.168.30.x/24
Passerelle :
192.168.30.1
Serveur DNS :
192.168.20.50
VLAN 90 : MGMT
192.168.90.x/24
Passerelle :
192.168.90.254
Serveur DNS :
192.168.20.50
VLAN 50 : Wifi
192.168.50.x/24
Passerelle :
192.168.50.1
Serveur DNS :
192.168.20.50
Plage DHCP:
192.168.50.2-254
WAN Entreprise sn.fr
10.16.27.x/24
DHCP
VLAN 50
Wifi via
Fortinet
Fortinet 60D
172.16.0.1/29
Lien secours
172.16.0.3/29
ISR900
Core 2
prio : 110
192.168.x.253../24
(x=n°VLAN)
172.16.0.2/29
ISR900
Core 1
prio : 120
192.168.x.254/24
(x=n°VLAN)
Catalyst 2960
Proxmox PVE
Backup
192.168.20.3.24
Ubackup
192.168.20.123
(VLAN 20)
PC CLIENT
DHCP (VLAN 10)
PC CLIENT
DHCP (VLAN 10)
Proxmox PVE PROD
192.168.20.2/24
VMBR0
AD, DHCP, DNS
192.168.20.50
Zabbix
192.168.20.13
GLPI
192.168.20.11
Nging Proxy Manager
192.168.20.15
VaultWarden
192.168.20.25
VMBR1
Nextcloud
192.168.30.12
(DMZ)
Lien Fortinet -> DMZ
Lien VPN Intersite
temporaire
172.16.0.1/24
ISR 900
10.0.0.1/30
VPN
WAN Simulé
10.0.0.x/30
VPN
10.0.0.2/30
ISR 900
172.16.1.1/24
Realis
Infrastructure complète

# Virtualisation et hébergement

L'ensemble de l'infrastructure repose sur Proxmox VE, utilisé comme solution principale de virtualisation. Ce choix permet de centraliser l'hébergement des services, de mutualiser les ressources matérielles et de faciliter l'administration des machines virtuelles et conteneurs .

Les services internes sont majoritairement hébergés sur le serveur Proxmox PROD, tandis que la partie sauvegarde est isolée sur un second serveur dédié (Proxmox Backup). Cette organisation permet de distinguer les fonctions de production et de sauvegarde au sein de la maquette.

# Services déployés

Plusieurs services ont été intégrés dans l'environnement afin de couvrir les besoins essentiels d'un système d'information d'entreprise. Leur déploiement s'inscrit dans une logique de complémentarité entre administration, sécurité, exploitation et continuité de service.

| Service | Technologie | Fonction principale |
|---|---|---|
| Virtualisation | Proxmox VE | Hébergement des services |
| Cloud collaboratif | Nextcloud | Partage et synchronisation de fichiers |
| Supervision | Zabbix | Surveillance des équipements et services |
| Annuaire | Active Directory | Authentification centralisée |
| Résolution de noms | DNS | Résolution interne du domaine |
| Attribution IP | DHCP | Distribution automatique des adresses |
| Gestion de parc / support | GLPI | Inventaire et helpdesk |
| Sauvegarde | UrBackup | Protection et restauration des données |
| Interconnexion | VPN IPsec | Liaison sécurisée entre deux sites |

# Sécurité logique

La sécurité de l'environnement repose d'abord sur la segmentation réseau par VLAN et sur l'utilisation d'une DMZ pour les services exposés. Nextcloud est placé dans le VLAN 30 afin d'être isolé du réseau interne et de limiter l'impact d'une compromission éventuelle sur les services hébergés dans le VLAN 20.

Les flux entre les zones sont contrôlés par le pare-feu Fortiwifi 60D, tandis que l'interconnexion entre sites s'appuie sur un tunnel VPN IPsec mis en place entre deux routeurs Cisco ISR 900. Des ACL étendues ont été appliquées sur le WAN afin de n'autoriser que les protocoles nécessaires au fonctionnement du VPN, notamment ESP et ISAKMP .

# Administration centralisée

L'administration des utilisateurs et des postes repose sur un serveur Windows Server 2022 promu en contrôleur de domaine Active Directory. Ce serveur assure également les rôles DNS et DHCP pour le domaine GTLM.local, ce qui permet de centraliser l'authentification, la résolution de noms et l'attribution des paramètres réseau.

L'annuaire est structuré en unités d'organisation, groupes et utilisateurs, et des stratégies de groupe sont appliquées aux postes du domaine. Cette organisation facilite l'administration du parc et l'application homogène des paramètres système.

# Supervision et exploitation

La supervision de l'environnement est assurée par Zabbix, déployé comme service de monitoring des équipements et des serveurs. Cette solution permet de vérifier la disponibilité des ressources et d'anticiper les incidents d'exploitation au sein de la maquette.

GLPI complète cette logique d'exploitation en apportant une solution de gestion de parc et de support utilisateur. Le service est hébergé dans le VLAN serveurs et peut évoluer vers une intégration avec l'Active Directory et Zabbix afin de centraliser davantage l'exploitation du système d'information.

# Sauvegarde et continuité

La maquette intègre une solution de sauvegarde avec un second environnement Proxmox et une machine dédiée à UrBackup. Les sauvegardes sont transférées depuis l'hyperviseur principal vers le serveur de sauvegarde afin de préserver une copie distincte des services critiques.

Cette organisation répond à un besoin de continuité minimale de service dans le cadre d'une maquette pédagogique. Les documents mentionnent également comme axes d'amélioration la mise en place d'un cluster Proxmox, de mécanismes de haute disponibilité et d'une redondance accrue sur les services sensibles, notamment Active Directory.

# Interconnexion site à site

Une interconnexion sécurisée entre un site principal GTLM et un site distant a été mise en place dans un environnement de maquette distinct. Cette liaison repose sur un tunnel VPN IPsec entre deux routeurs Cisco ISR 900, avec un WAN simulé en 10.0.0.0/30 et deux réseaux locaux en 172.16.0.0/24 et 172.16.1.0/24.

Cette réalisation permet de démontrer la capacité de l'infrastructure à relier deux réseaux distants de manière sécurisée tout en conservant des plans d'adressage séparés. Les tests de validation confirment l'établissement du tunnel et le bon fonctionnement du chiffrement des flux .

# Conclusion

L'infrastructure GTLM constitue un environnement technique global reposant sur la virtualisation, la segmentation réseau et l'intégration de services complémentaires. L'ensemble permet de répondre aux besoins de centralisation, de supervision, de collaboration, de gestion du parc, de sauvegarde et d'interconnexion sécurisée dans un cadre cohérent avec les attendus de l'épreuve E6 du BTS SIO option SISR.

Ce DOE a pour rôle de fournir au jury une vision synthétique et structurée de l'environnement étudié, afin de faciliter la compréhension des réalisations présentées lors de l'épreuve. Il peut également servir d'introduction générale avant la présentation détaillée de chaque fiche de réalisation professionnelle.

i