

FICHE PROJET : Montage d'une salle Informatique.

Sommaire

1. Contexte et Objectifs du Projet
 2. Architecture et Configuration Générale
 3. Configuration Point par Point (Services & Équipements)
 4. Sécurité, Flux et Isolation
 5. Maintenance et Stratégie de Reset
-

1. Contexte et Objectifs

- Le Projet : Création d'une infrastructure complète et sécurisée dédiée à l'apprentissage du pentest et de la cyberdéfense.
- Objectif Pédagogique : Fournir un environnement réel où les étudiants peuvent planifier, déployer et tester des attaques dans un cadre contrôlé.
- Réalisme Technique : Simulation d'un réseau d'entreprise hybride.

2. Configuration Générale

Topologie :

Table de routage :

Services

Tr	IP	Tr	Mac Address	Service	Tr	Hostname	Role	Pool DHCP	Tr	Comment	URL
	192.168.10.1		70:10:5c:7b:7a:80	Switch CISCO		SioPba	Service réseau	Static		VLAN	
	192.168.10.2		e8:9c:25:7f:fc:81	DHCP		siodhcp	Service réseau	Static			
	192.168.10.3		0b:8f:c3:9e:6e:f6	Proxmox secondaire		siovirt	Proxmox	Static		GLPI, WinAD,	https://192.168.10.3:8006/
	192.168.10.4		b8:85:84:ad:b6:68	Zentyal		sioad	Service réseau	Static		Zentyal AD and DNS	https://192.168.10.4:8443
	192.168.10.5		90:09:d0:79:71:15	NAS		sionas	Service réseau	Static			http://192.168.10.5:5000
	192.168.10.6		a4:bb:6d:da:a3:c4	Proxmox principale		siovirt2	Proxmox	Static			https://192.168.10.6:8006/
	192.168.10.7		bc:24:11:2e:7d:cc	VM GLPI, WIKIJS		sioinx	Gestion du parc	Static		GLPI, Wikijs	http://192.168.10.7:8080/front/central.php
	192.168.10.8		bc:24:11:f7:c4:32	VM OPSI		siopsi	Gestion du parc	Static		Déploiement/Gestion d'image	
	192.168.10.9		bc:24:11:9a:ea:14	VM VPN		siovpn	Service réseau	Static		Open VPN	
	192.168.10.254		78:9A:18:16:70:BA	Switch Mikrotik		MikroTik	Gateway Net	Static		Passerelle	http://192.168.10.254

Postes

Tr	IP	Tr	Mac Address	Tr	Hostname	OS	Pool DHCP
	192.168.10.110		b8:85:84:aec2:d9		sio10	Poste Win.	Static
	192.168.10.111		b8:85:84:aec6:54		sio11	Poste Win.	Static
	192.168.10.112		b8:85:84:aec6:1c		sio12	Poste Win.	Static
	192.168.10.113		b8:85:84:aec5:83		sio13	Poste Kali	Static
	192.168.10.114		b8:85:84:aec5:f0		sio14	Poste Ubun.	Static
	192.168.10.115		b8:85:84:aec8:d4		sio15	Poste Ubun.	Static

Services/Matériel Utilisés :

Postes:

- 3 Postes Windows
- 1 poste Kali Linux
- 2 Postes Ubuntu

Services:

- Switch CISCO ; Réseau (VLAN)
- DHCP ; Réseau
- 2 Proxmox (Principal , Secondaire ;GLPI,WinAD) ;
- Zentyal ; Réseau (AD , DNS)
- NAS ;Réseau
- 4 VM (GLPI , WIKIJS,OPSI,VPN) ; Gestion de parc , Réseau
- Switch Mikrotik ; Gateway NET (PASSERELLE)

Inventaire de la salle :

SIO10	BB-85-84-AE-E2-D9	DHCP	PC	Windows	SIO1-Ubuntu	Firefox	Oracle Virtualbox	Avast antivirus	Open VPN	Libre Office	Windows update	Winget upgrade	Pilotes Dell	Avast	En cours	PC admin et VM (SIO10)
SIO11	BB-85-84-AE-E5-54	DHCP	PC	Windows	SIO1-Ubuntu	Firefox	Oracle Virtualbox	Avast antivirus	Open VPN	Libre Office	Windows update	Winget upgrade	Pilotes Dell	Avast	En cours	PC admin et VM (SIO11)
SIO12	BB-85-84-AE-E5-1C	DHCP	PC	Windows	SIO1-Ubuntu	Firefox	Oracle Virtualbox	Avast antivirus	Open VPN	Libre Office	Windows update	Winget upgrade	Pilotes Dell	Avast	En cours	PC admin et VM (SIO12)
SIO13	BB-85-84-AE-E5-83	DHCP	PC	Windows	SIO1-Ubuntu	Firefox	Oracle Virtualbox	Avast antivirus	Open VPN	Libre Office	Windows update	Winget upgrade	Pilotes Dell	Avast	En cours	PC admin et VM (SIO13)
SIO14	BB-85-84-AE-E5-F0	DHCP	PC	Windows	SIO1-Ubuntu	Firefox	Oracle Virtualbox	Avast antivirus	Open VPN	Libre Office	Windows update	Winget upgrade	Pilotes Dell	Avast	En cours	PC admin et VM (SIO14)
SIO15	BB-85-84-AE-E5-D4	DHCP	PC	Windows	SIO1-Ubuntu	Firefox	Oracle Virtualbox	Avast antivirus	Open VPN	Libre Office	Windows update	Winget upgrade	Pilotes Dell	Avast	En cours	PC admin et VM (SIO15)
SIO16	BB-85-84-AE-E9-3F	DHCP	PC	Windows		Firefox	Oracle Virtualbox	Avast antivirus	Open VPN	Libre Office	Windows update	Winget upgrade	Pilotes Dell	Avast	En cours	Invité (SIO16)
SIOADMIN	BB-85-84-AD-B5-68	192.168.10.12	PC	Zentyal											En cours	Administration réseau
SIONAS	90-09-00-79-71-15		NAS													Notes

3. Configuration Point par Point (**PLUS A JOUR A PARTIR D'ICI**)

A. Cœur de Réseau (MikroTik & Cisco)

- Routeur (MikroTik CHR) : Gère le routage inter-VLAN et l'accès WAN via **bridge-vlans** avec **vlan-filtering=yes**.
- Switch (Cisco/MikroTik) : Distribution des VLANs en mode Trunk vers le routeur et en mode Access vers les équipements finaux.

B. Services Réseau (Ubuntu 24.04 LTS)

- DHCP (ISC-DHCP-Server) : Attribution dynamique d'IP sur les 6 VLANs avec baux statiques pour les équipements critiques.
- DNS (Bind9) : Résolution interne pour le domaine **sio.lan**.
- DDNS (Mises à jour dynamiques) : Intégration sécurisée par clé TSIG permettant au serveur DHCP de mettre à jour automatiquement les enregistrements DNS.

C. Gestion et Déploiement

- Active Directory (Zentyal) : Gestion centralisée des identités et des politiques de groupe.
- OPSI : Serveur de déploiement pour la gestion automatisée des images systèmes.
- GLPI & WikiJS : Gestion de parc, ticketing et base de connaissances documentaire.

4. Sécurité, Flux et Isolation

C'est ce qui fait que ton lab est "Cyber".

- Isolation Inter-VLAN : Par défaut, le trafic est bloqué. Seul le DNS (port 53) est autorisé pour permettre la communication vers le serveur central (192.168.10.2).
- Contrôle de l'accès Internet : Utilisation du NAT Masquerade, activé uniquement pour le VLAN 30 (Admin). Les autres VLANs sont isolés du monde extérieur.

5. Maintenance et Stratégie de Reset

- Snapshots : Utilisation des fonctionnalités de Proxmox pour restaurer une machine cible à son état "propre" après une attaque.
- Automatisation : Scripts Bash pour réinstaller les services DNS/DHCP en cas de corruption majeure.