Projet SAE4.Cyber.01 : Sécuriser un système d'information

Présenté par Eric Petersen & Marius Keltz, étudiants en Réseaux & Télécommunications à l'IUT de Colmar. Ce projet explore la sécurisation d'infrastructures informatiques complexes.

Objectifs du Projet

Création d'une infrastructure réseau sécurisée

Nous avons conçu et mis en œuvre une architecture réseau robuste et sécurisée.

Intégration de services clés

- Pare-feu, LDAP, NFS, VPN, DNS
- Messagerie (Postfix/Dovecot)
- Web HTTPS
- Infrastructure de Gestion de Clés (IGC)

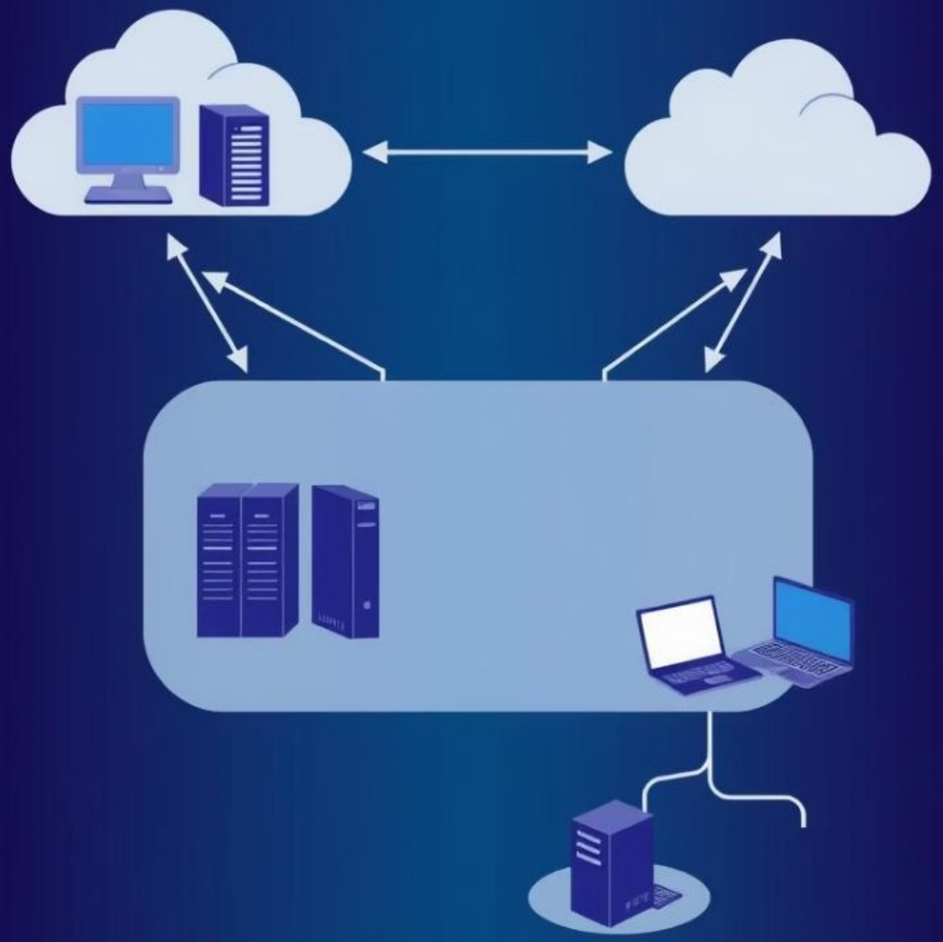


Schéma et Plan d’adressage

Architecture Réseau

Le schéma détaille les segments LAN, WAN, et VPN pour une isolation efficace des services.

Plan d'Adressage IP

Une séparation claire des adresses IP garantit la sécurité et la gestion des services.

Laboratoire Virtualisé

Utilisation de VirtualBox pour un environnement de laboratoire portable et isolé.

Architecture Réseau

Plan IP

Zone	Réseau	Masque	Usage
WAN	192.168.56.0/24	255.255.255.0	NAT VirtualBox / Internet
LAN	192.168.129.0/24	255.255.255.0	Services internes, DHCP, postes de test
VPN	10.0.8.0/24	255.255.255.0	Pool d’adresses pour clients OpenVPN

Équipement	Interface	IP	Interface
Firewall	WAN	dhcp	via NAT VirtualBox
	VPN	10.0.8.1	gateway VPN
	LAN	192.168.129.1	gateway LAN
Load-balancer (HAProxy)	–	192.168.129.10	LAN
Web #1	–	192.168.129.10	LAN
Web #2	–	192.168.129.11	LAN
Mail (Postfix/Dovecot)	–	192.168.129.14	LAN
LDAPS	–	192.168.129.12	LAN
NFS	–	192.168.129.13	LAN
DHCP (isc-dhcp-server)	–	192.168.129.2	LAN
DNS (BIND9)	–	192.168.129.2	LAN
Client Linux	–	DHCP	WAN

Pare-feu & DNS

Règles de Pare-feu

Implémentation de règles DROP/ACCEPT pour chaque service afin de contrôler le trafic.

Serveur DNS BIND9

Configuration de zones directes et inverses pour une résolution de noms fiable.

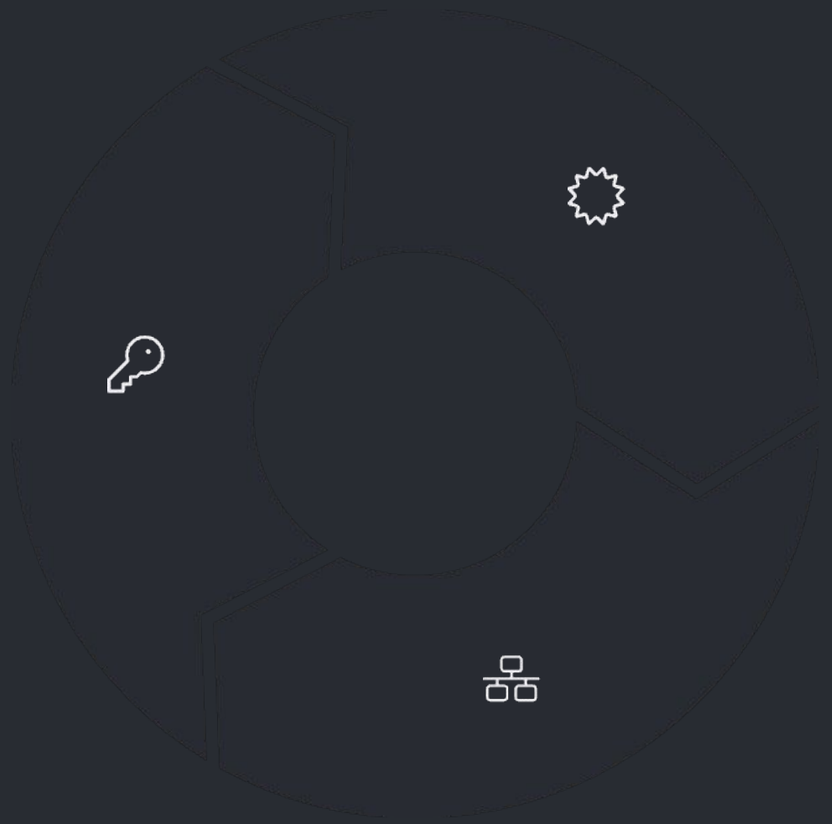
Sécurisation DNS

Mise en place d'ACL et désactivation de la récursion pour prévenir les attaques.

IGC et Certificats TLS

Création de CA Racine

Nous avons généré une Autorité de Certification (CA) racine via OpenSSL.



Émission de Certificats

Des certificats spécifiques pour le Web, le Mail, le VPN, et IMAP ont été créés.

Application des Certificats

Ces certificats sont utilisés pour sécuriser les communications HTTPS, IMAPS, SMTPS et VPN.

LDAP et Authentification

1 **LDAPs Chiffré**

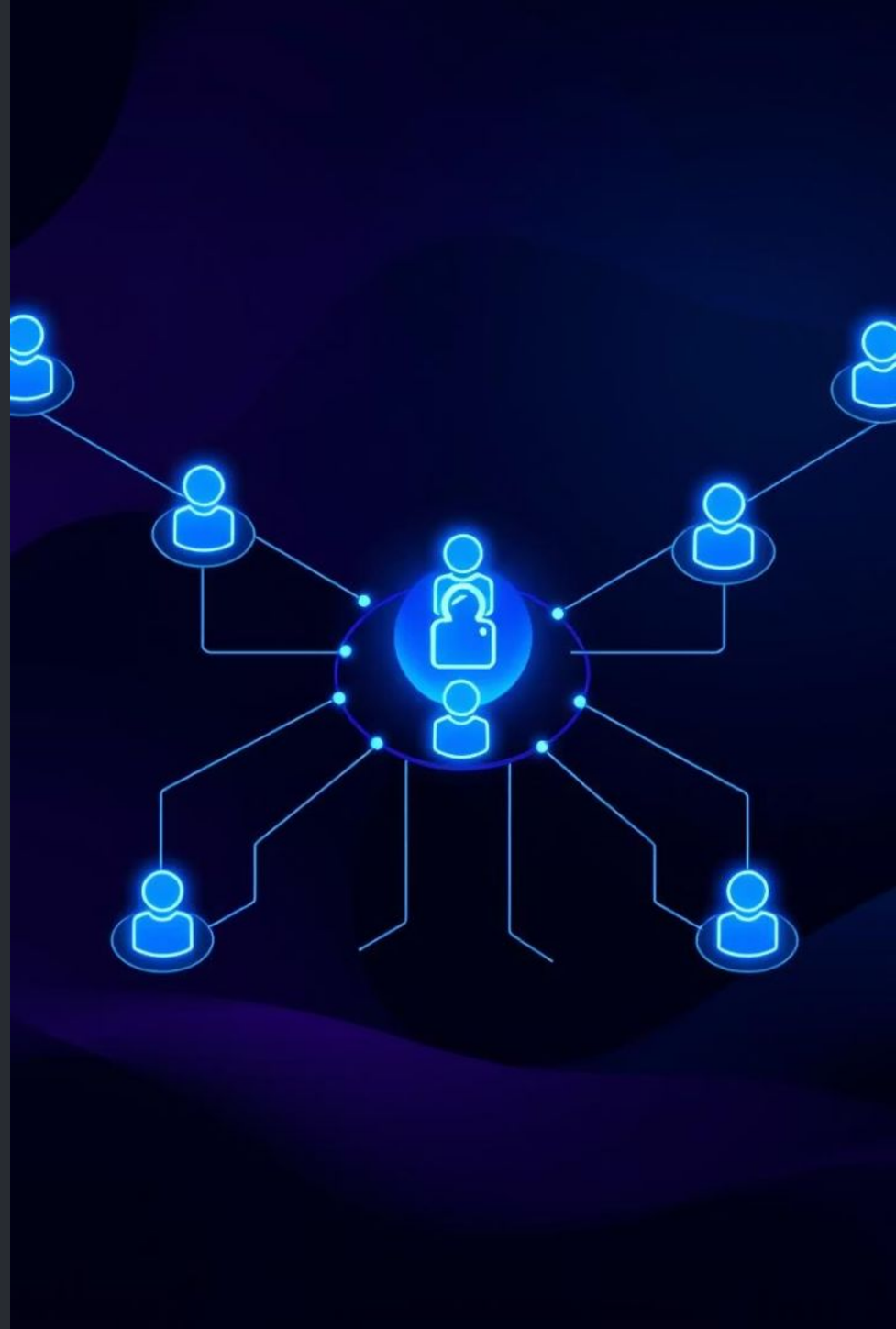
Le service LDAP est configuré avec le chiffrement TLS pour une sécurité accrue.

2 **Gestion des Utilisateurs**

Les utilisateurs sont gérés via des fichiers LDIF pour une administration efficace.

3 **Authentification Centralisée**

LDAP est intégré pour l'authentification des services de mail, NFS et PAM.



Mail : Postfix & Dovecot

Configuration SMTP/IMAP

Postfix gère l'envoi (SMTP) et Dovecot la réception (IMAP) des e-mails.

Authentification Sécurisée

L'authentification se fait via LDAP et les communications sont sécurisées par TLS.

Tests et Validation

Des tests exhaustifs ont été menés avec Thunderbird, accompagnés d'analyses de logs.

NFS & OpenVPN

Partage NFS Sécurisé

Des partages de fichiers réseau sont configurés avec authentification LDAP.

2

VPN OpenVPN

Mise en place d'OpenVPN avec des certificats client et serveur.

Routage et Tests

Le routage vers le LAN est assuré, avec des tests de connectivité rigoureux.

Service Web & Sécurité Globale

Service Web HTTPS

Apache2 ou Nginx sont configurés avec HTTPS pour une communication sécurisée.

Sécurité Globale

La combinaison de TLS, VPN et pare-feu assure une protection multicouche.

Risques Identifiés

Les attaques par bruteforce et la compromission de la CA sont des risques potentiels.

Conclusion & Questions

1

Compétences Acquises

Ce projet a permis de renforcer nos compétences en sécurité des systèmes d'information.

2

Défis Relevés

Nous avons surmonté des difficultés techniques pour réaliser une infrastructure robuste.

3

Remerciements

Merci de votre attention et de votre intérêt pour notre travail.

4

Questions

Nous sommes à votre disposition pour toute question concernant ce projet.