Projet

SAE4.Cyber.01
Sécuriser un système d’information

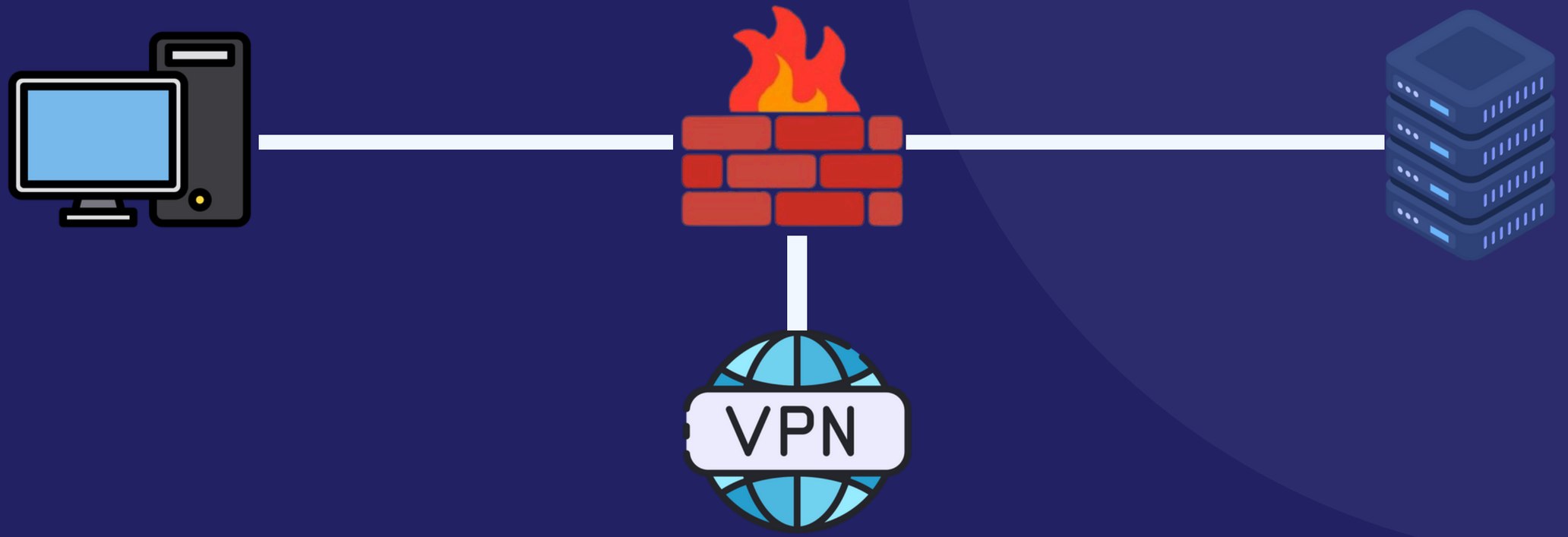
Rayane SADEK - Alexis STOCK

Mise en place d’un réseau d’entreprise sécurisé

Objectifs :

- Créer un réseau avec services essentiels
- Sécuriser les communications internes et externes
- Authentifier les utilisateurs via LDAP
- Protéger les accès avec un pare-feu et un VPN

Architecture du réseau



Plan d’adressage

Client (Linux)	(WAN)10.0.2.5 (TUN) 10.10.10.6
FireWall +VPN (PfSense + OpenVPN)	(LAN) 192.168.0.1 (WAN) 10.0.2.4
Serveur (LDAP NFS DNS)	192.168.0.2

IP

Projet

Sécurité et services

Pare-feu

PfSense : configuration des règles de filtrage pour contrôler le trafic entrant et sortant.

LDAPs (TLS

Serveur LDAP sécurisé par un certificat TLS émis par pfSense.
Authentification centralisée des utilisateurs.

NFS + PAM LDAP

pfSense agit comme autorité de certification (CA).
Génération des certificats client et serveur via pfSense.
Certificat exporté depuis pfSense, puis importé sur le client.

OpenVPN

pfSense agit comme autorité de certification (CA).
Génération des certificats client et serveur via pfSense.
Certificat exporté depuis pfSense, puis importé sur le client.

DNS (BIND9)

Serveur configuré avec zones directes et inverses.

PKI (Infrastructure à Clés Publiques)

pfSense = racine de confiance (CA).
Utilisation de certificats serveur/client pour sécuriser LDAP, VPN.

Déroulement du projet

Étapes majeures

- Création du Lab sur VirtualBox
- Installation et configuration de Debian
- Configuration des services (DNS, LDAP, NFS, VPN)
- Mise en place de TLS

Choix techniques

- LDAP pour centraliser l’authentification
- VPN pour la sécurité externe
- pfSense pour la gestion du trafic
- Host-Only pour toute les VM du LAN
- Tous les services centraliser sur une machine (DNS, LDAP, NFS)

Projet

Problèmes rencontrés

DNS

Inverement de zone mauvaise configuration fichié de conf

LDAPS

Mauvaise exportation du certificat donc pas authentification impossible

FireWall

Règle de FW donc redirection incorrect

Sécurité et évaluation des risques

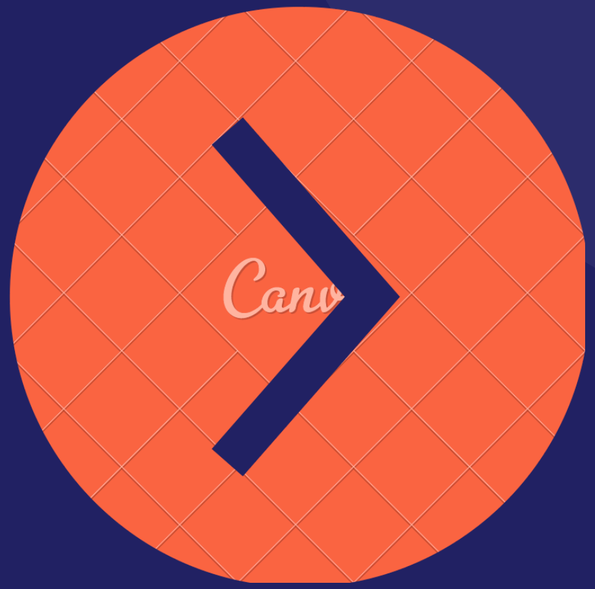
Mesures mises en place

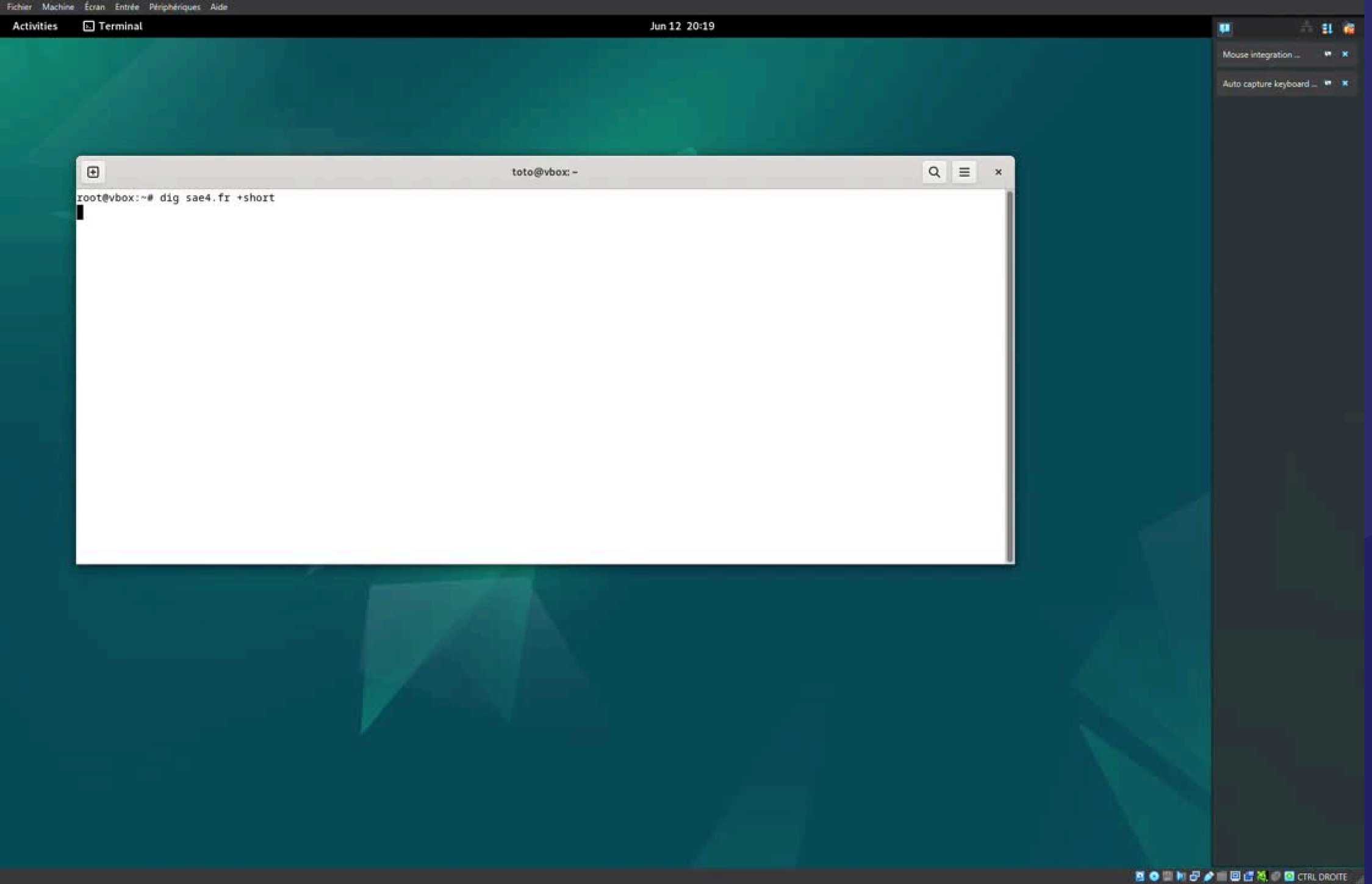
- TLS sur LDAP et VPN
- Règles pfSense restrictives
- Authentification LDAP pour NFS

Risques

- Failles potentielles si certificats mal protégés
- Utilisation de mots de passe faibles → à surveiller

Démonstration vidéo




Fichier Machine Écran Entrée Périphériques Aide
Activities
Terminal
Jun 12 20:19
Mouse integration ...
Auto capture keyboard ...
toto@vbox: ~
root@vbox:~# dig sae4.fr +short
CTRL DROITE

VIDÉO

Conclusion

Ce qu’on a appris :

- Création du Lab sur VirtualBox
- Installation et configuration de Debian
- Configuration des services (DNS, LDAP, NFS, VPN)
- Mise en place de TLS avec une IGC

Merci pour votre attention