

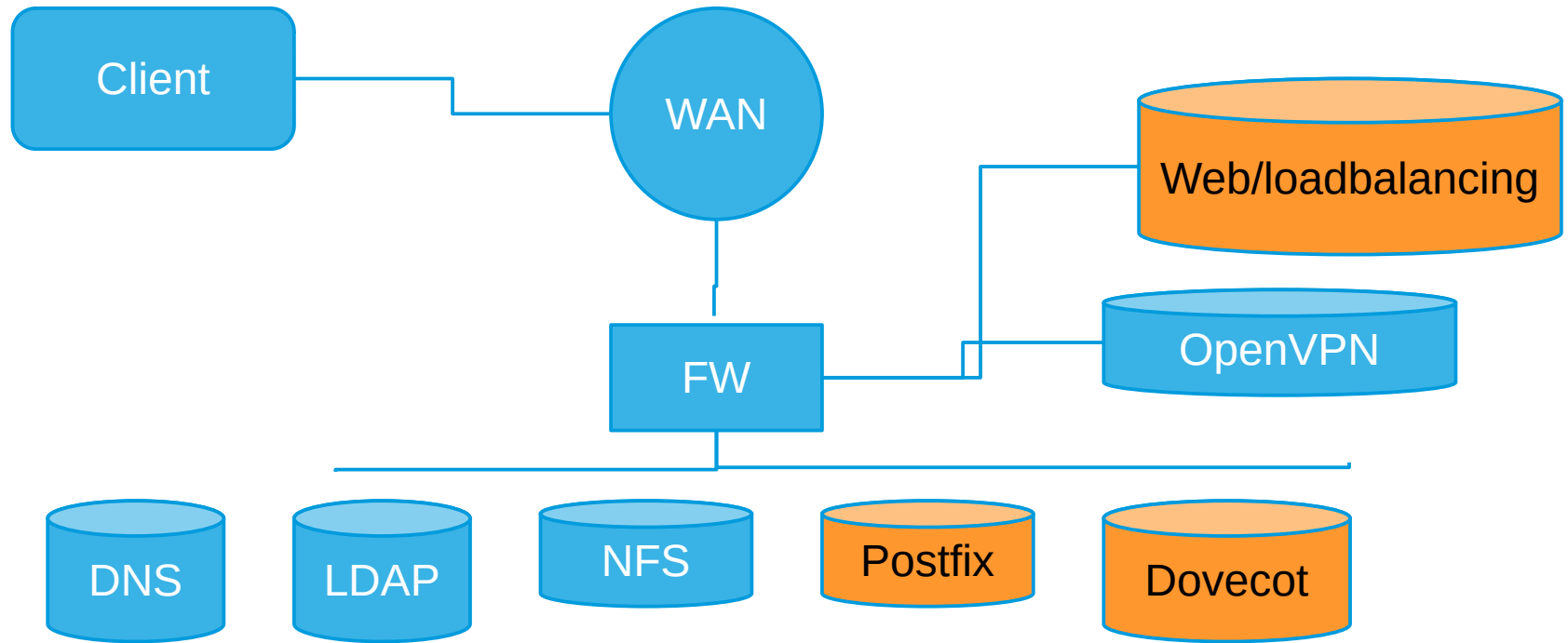
SAE4.Cyber.01

Sécuriser un système d'information

Objectif

- Créer un réseau d'entreprise
 - Un pare-feu
 - Avec un annuaire LDAP pour l'authentification
 - Un service de partage de fichiers NFS
 - Un service de messagerie
 - Un accès VPN pour postes nomades
 - un bastion apache guacamole
- Créer une infrastructure de clés pour
 - sécuriser les protocoles par TLS
 - authentifier les postes nomades

Schéma de principe



Organisation de la SAE

- Groupe de 3 étudiants
- Liberté dans le choix technique pour répondre au cahier des charges
- Évaluation par compétences lors des TD et TP de SAE
- Présentation de 20min
 - Présentation de la solution technique
 - Motivations de vos choix
 - Un zoom sur l'aspect sécurisation
 - Une évaluation des risques

Tâche à réaliser

- Définir un plan d'adressage IP
- Mise en place d'un LAB sur proxmox
- Mise en place du pare-feu et d'un bastion
- Mise en place d'un service DNS
- Mise en place d'une IGC
- Création d'un annuaire LDAP
- Création d'un serveur OpenVPN et d'un serveur NFS
- Création du poste Client

Tâche à réaliser pour les FI

- Création d'un serveur PostFix SMTP
- Création d'un serveur Dovecot IMAP
- Mise en place d'un client de messagerie
- Mise en place d'un service Web avec de la haute-disponibilité

Évaluation compétences

- Savoir faire un plan d'adressage IP
 - Savoir décrire le routage
 - Savoir décrire les règles de filtrage
- Mise en place du Lab sur Proxmox
 - Connaître les différents types de réseau
 - Création des VM (clonage, snapshot, ...)
 - Faire un rapport sur l'usage

Évaluation Compétences

- Service DNS
 - Savoir décrire le fonctionnement du DNS
 - Savoir configurer un serveur BIND9
 - Savoir configurer une zone DNS
 - Savoir configurer une zone DNS inverse
- IGC
 - Savoir créer un certificat racine
 - Savoir créer un certificat serveur
 - Savoir créer un certificat client

Évaluation des compétences

- Service LDAP
 - Comprendre le fonctionnement d'un annuaire LDAP
 - Savoir configurer un annuaire LDAPs (TLS)
 - Savoir initialiser une base LDAP
 - Savoir écrire un fichier LDIF
 - Savoir utiliser les commandes ldapadd, ldapmodify
 - Savoir définir un compte dans LDAP
 - Savoir modifier un mot de passe utilisateur

Évaluation par Compétences

- Serveur OpenVPN
 - Comprendre le principe d'un VPN
 - Savoir configurer un serveur OpenVPN
 - Savoir configurer un client OpenVPN
 - Savoir configurer le filtrage pour OpenVPN
 - Savoir configurer le routage pour OpenVPN

Évaluation par compétences

- Service NFS
 - Comprendre les configurations d'authentification PAM
 - Configurer une authentification par LDAP d'un serveur Debian
 - Comprendre le fichier de configuration NFS export
 - Savoir configurer un client NFS

Évaluation par compétences

- Service WEB
 - Savoir configurer un serveur web (apache2 ou nginx)
 - Savoir configurer un service https avec une IGC
 - Savoir mettre en place un service haute-disponibilité (loadbalancing)
 - Savoir mettre en place un proxy authentifiant (squid)

Évaluation par compétences

- Service SMTP
 - savoir configurer postfix utilisant un annuaire LDAP
 - savoir mettre en place une sécurisation TLS (smtps)
 - savoir mettre en place une authentification
 - savoir lire les logs

Évaluation par compétences

- Bastion Apache Guacamole
 - Installation
 - Identification LDAP
 - Utilisation
 - Gestion des logs

Évaluation par compétences

- Service dovecot IMAP/POP
 - savoir configurer un serveur IMAP dovecot utilisant LDAP
 - savoir sécurisé le protocole IMAPs par un certificat TLS
 - savoir configurer un client de messagerie utilisant une IGC
 - savoir analyser les logs du serveur dovecote

Présentation

- 5min par étudiant + 5min Questions
- Faire une démo en vidéo
- Savoir faire une présentation technique
- Savoir argumenter ses choix
- Savoir faire des schémas détaillés
- Savoir être concis et claire
- Savoir prendre du recul par rapport à son travail
- Savoir faire une évaluation de risques

Proxmox

- Le but de la SAE est de tester la plateforme de virtualisation
- faire un rapport sur l'utilisation de la plateforme :
 - utilisation/ergonomie
 - Bug/Difficulté
 - suggestions
- Comptes : SAE4C1_Gr1 à SAE4C1_GR13
- mot de passe : unique communiquer au groupe
- Réseaux : GrXNet1 et GrXnet2 : sans dhcp GrXNat : réseau NAT

proxmox : CPU/mise en veille

- Hardware de la VM :
 - CPU : EPYC-Milan-v3 (identique au hardware)
 - flags : nested-virt : permet de faire un hyperviseur dans proxmox ?
- Pour éviter que la machine se bloque (sous debian):
 - Système/matériel/gestion de l'énergie
 - Affichage : mise en veille : jamais

proxmox : Ceph

- Ceph : cloud de stockage sur 3 Pcs avec 2 disques de 10To et 2 carte réseaux 10G
- stockage au format RBD : Rados Block Device
- Stockage identifié par **SAE4Cyber01_Gr2_300Go**
- Quota de 300Go, attention en cas de dépassement crash du stockage. Il faut voir avec Moi ou Joshua pour vous débloquer
- Permet les snapshot et clone liée

proxmox : clone liée

- **Les clone liées sont sur le même disque que le template de base**
- Créer une VM sur votre disque ceph_ (nouvelle VM, clone intégrale, ...)
- Transformer la VM en template
- Créer des clones liées à partir du template