ATELIER PROFESSIONNELLE 2024/2025
PETRISSANS BASTIEN

TECH UNIVERS

WEB, REDONDANCE, HAPROX, HEARTBEAT, VPN SSL

Par les Astartes: Ellande; Haïzé; Léo

INTRODUCTION

Insérez votre texte ici Insérez votre texte ici Insérez votre texte ici Insérez votre texte ici Insérez votre texte ici Insérez votre texte ici.

L’organisation cliente

TechUniverse est une entreprise dynamique spécialisée dans la vente de gadgets électroniques, de téléphones portables, d'ordinateurs portables, d'accessoires et de gadgets connectés. Avec des offres attrayantes et une réputation de fiabilité, TechUniverse est devenue une destination incontournable pour les passionnés de technologie.

Le site web de TechUniverse a été initialement conçu pour répondre à une demande modérée, mais la popularité de l'entreprise a entraîné une augmentation exponentielle du trafic en ligne. Malheureusement, le site n'a pas été suffisamment optimisé pour gérer cette charge de trafic élevée, ce qui a conduit à des retards dans le chargement des pages, des erreurs de connexion et des temps d'attente frustrants pour les clients.

Cette surcharge du site web a eu un impact négatif sur l'expérience client, entraînant des abandons de panier, des pertes de ventes potentielles et une réduction de la satisfaction client.

Pour résoudre ce problème urgent, l'équipe de direction de TechUniverse a lancé un projet d’amélioration de son infrastructure de DMZ en prenant en compte la surcharge des serveurs ainsi que le manque de haute disponibilité.

De plus, TechUniverse souhaite mettre en place une solution de connexion à distance sur son LAN pour les télétravailleurs.

Objectifs

➢ Votre mission

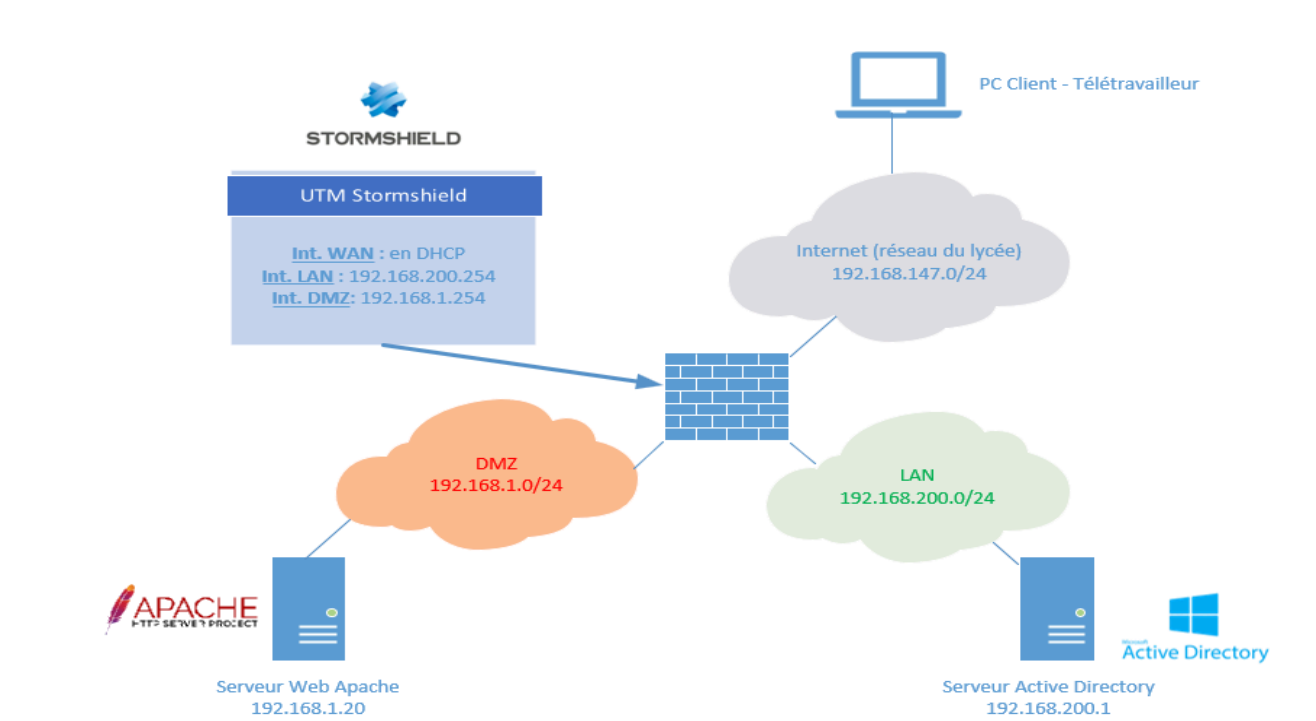
Vous êtes une personne salariée de l'entreprise TechUniverse affectée à l'équipe informatique. Vous participez à l'étude d'amélioration de la haute disponibilité de l'infrastructure DMZ de la société et votre mission consiste à préparer l'intégration de la solution pour le client. Cette préparation se fera sur une maquette de test constituée de machines virtuelles afin de préparer le projet.

Les besoins exprimés par le gérant de TechUniverse

Le responsable des services techniques vous a missionné pour 4 tâches différentes

1. Maquette de l'infrastructure actuelle :

Il vous faut dans un premier temps maquetter l'infrastructure en vous appuyant sur le schéma ci-dessous (voir également les prérequis machines virtuelles) :



- Pour le serveur Apache, vous réaliserez la maquette avec la page par défaut d'Apache.
- Pour valider le bon fonctionnement de votre infrastructure, la page Web doit être accessible depuis le WAN (un PC de la salle). Grâce à l'IP publique de l'entreprise (l'adresse WAN de votre UTM).

2. Répartition de la charge des serveurs Web :

La solution proposée pour éviter la surcharge des serveurs Web est d'utiliser un répartiteur de charge (load-balancer). Pour cela, vous allez créer un deuxième serveur Web qui héberge le même serveur Web que le premier et vous allez ensuite tester la solution HAProxy pour réaliser la répartition de charge.

Voir le rendu de la mission 3 qui concerne également cette mission.

3. Mise en place de la haute disponibilité au niveau du HAProxy :

Suite à la mise en place du HAProxy, un problème de haute disponibilité se pose. En effet, votre répartisseur de charge constitue maintenant un SPOF (single point of failure ou point de défaillance unique) dans votre infrastructure.

Vous allez donc « doubler » votre HAProxy en mettant en place un cluster HeartBeat.

- A rendre : Une procédure d'installation de votre cluster Heartbeat + HAProxy

4. Mettre en place une solution de télétravail pour les agents de l'entreprise :

Il vous est demandé de mettre en place une solution de VPN SSL qui va permettre aux télétravailleurs de la société de se connecter à distance sur le LAN de l'entreprise. L'authentification devra se faire sur l'Active Directory et l'accès au VPN doit être limité à un groupe de l'AD.

- A rendre : Topologie réseaux et système de votre solution.

- **Conseil** : utilisez LibreOffice Draw sur votre machine. Vous pouvez télécharger l'extension qui permet de réaliser des schémas réseaux : https://extensions.libreoffice.org/en/extensions/show/vrt-network-equipment

Prérequis

Prérequis matériels :

- 1 switch Netgear 8 ports pour commuter la DMZ
- Câbles RJ45

Prérequis machines virtuelles :

Pour réaliser cette maquette, vous aurez besoin de 5 machines virtuelles.

Renomme la machine : hostnamectl set-hostname <nom d'hôte>

Nom de la VM	Rôle	OS	Type d'adressage	nom
UTM-STORMSHIELD	UTM	OVA fourni par Stormshield	Statique	Ellande
SRV-WEB1	Serveur WEB	Debian 12	Statique	Haïzé
SRV-WEB2	Serveur WEB	Debian 12	Statique	Léo
SRV-HAPROXY1	Reverse proxy, load balancing	Debian 12	Statique	Haïzé
SRV-HAPROXY2	Reverse proxy, load balancing	Debian 12	Statique	Léo
SRV-ADTECH	Serveur Active Directory DNS	Windows Server 2022	Statique	Ellande

Pour un gain de temps, vous trouverez sur le partage smb:\\sio.lan :

- L'OVA de la VM Stormshield déjà mis à disposition

Attention : lors de l'import sur VirtualBox n'oubliez pas de regénérer l'adresse MAC de la carte réseau de l'interface WAN du Stormshield.

Organisation

- Chaque groupe de travail sera composé de 3 étudiants.
  Attention, cela reste un travail d'équipe et vous devez être en mesure de comprendre ce qui a été fait par votre partenaire de groupe. Utilisez des outils de gestion de projet, cela sera un plus pour votre organisation interne ainsi que pour votre portfolio.

- Conseil pour la mise en œuvre la maquette :

- 1 PC : - Avec la VM Stormshield:
  - Interface WAN en accès par pont sur le réseau du lycée
  - Interface DMZ sur une carte réseau libre vers le switch
  - Interface LAN sur un réseau interne virtual Box
  - Avec le serveur AD DNS interconnecté avec un réseau VirtualBox interne
- 1 PC avec les 2 HAProxys connectés sur le switch
- 1 PC Avec les 2 serveurs webs connectés sur le switch

- Respecter les bonnes pratiques dans votre maquette :
  - Configurer l'ensemble des noms de machines de vos serveurs, PCs et équipements réseaux.
  - Utilisez les protocoles d'administrations SSH et RDP (vous avez des clients sur les machines hôtes)
  - Utilisez des comptes nominatifs pour administrer les serveurs

    - Respectez une nomenclature de nommage pour vos machines

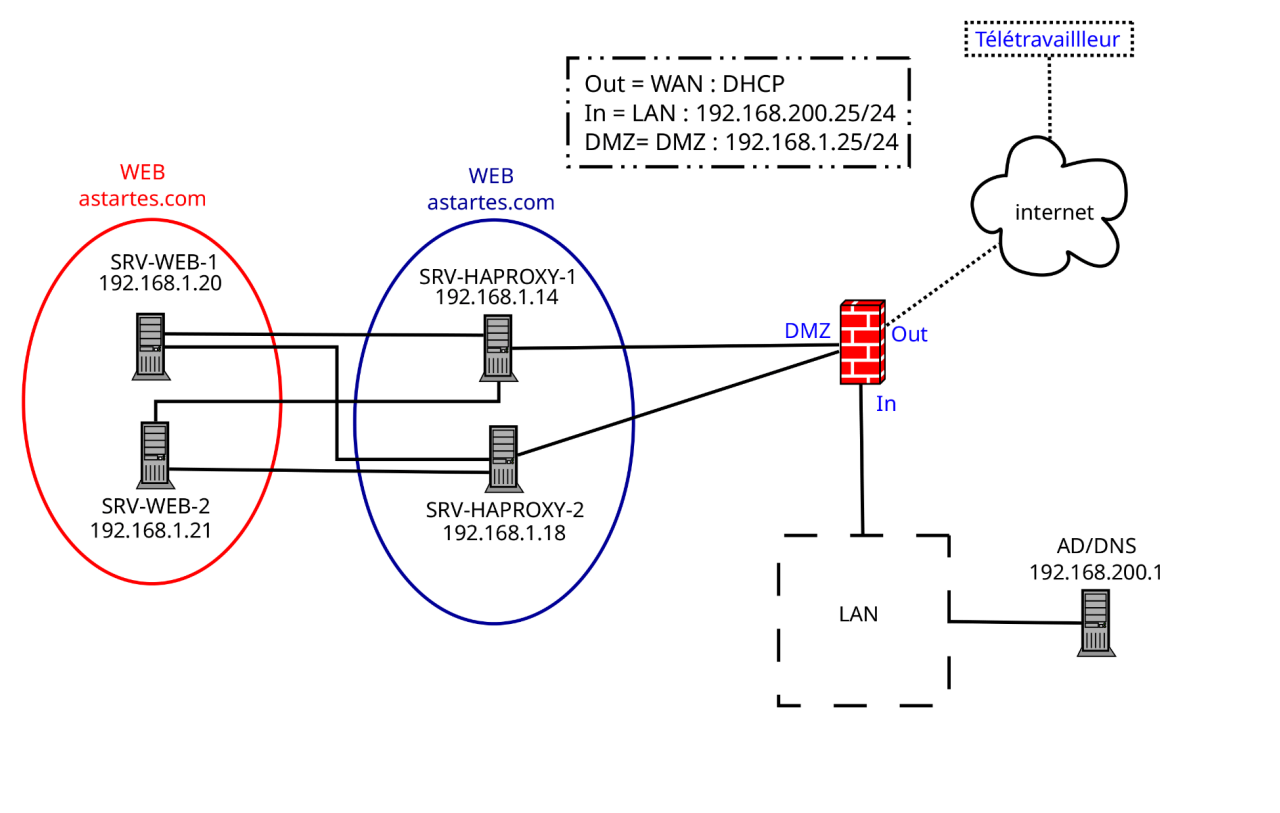
- Des dépôts pour l'ensemble des rendus sont disponibles sur Moodle. Les rendus doivent être professionnels, avec une page de garde, un sommaire, des en têtes et pied de pages. Vous pouvez réutiliser la fiche méthode « Rédigez une procédure » de première année.

- Durée du projet : 7 semaines

Rapport de TP – Optimisation de l’infrastructure DMZ chez TechUniverse

1. Architecture technique

Nom VM	Rôle	OS	IP	Type IP
UTM-STORMSHIELD	UTM/Firewall	OVA Stormshield	Wan : DHCP Lan : 192.168.200.254 DMZ : 192.168.1.254	auto Statique Statique
SRV-WEB1	Serveur Web Apache	Debian 12	192.168.1.20	Statique
SRV-WEB2	Serveur Web Apache	Debian 12	192.168.1.21	Statique
SRV-HAPROXY1	Load Balancer	Debian 12	192.168.1.14	Statique
SRV-HAPROXY2	Load Balancer secondaire	Debian 12	192.168.1.18	Statique
SRV-ADTECH	Active Directory, DNS	Windows Server 2022	192.168.200.1	Statique



---

2. Mission 1 – Maquette de l'infrastructure actuelle

Objectif

Reproduire une infrastructure DMZ avec un pare-feu UTM (Stormshield), deux serveurs web, et valider l'accessibilité depuis le WAN via Apache.

Étapes techniques

1. **UTM Stormshield** : 3 interfaces configurées
    - WAN (accès pont lycée)
    - LAN (réseau interne avec AD)
    - DMZ (vers switch connecté aux serveurs Web/HAProxy)

2. **SRV-WEB1 & SRV-WEB2**

Installation Apache :

```
sudo apt update
```

```
sudo apt install apache2 -y
```

Validation via page par défaut sur :

http://192.168.1.20

http://192.168.1.21

3. **Règle NAT/Port forwarding sur Stormshield**

    - Redirection du port 80 vers SRV-WEB1
    - Test depuis un PC externe via IP publique (WAN UTM)

---

3. Mission 2 – Mise en place de HAProxy

Objectif

Installer un **répartiteur de charge** pour répartir les requêtes web entre SRV-WEB1 et SRV-WEB2.

Étapes techniques

a. Installer HAProxy (SRV-HAPROXY1)

```
sudo apt update
```

```
sudo apt install haproxy -y
```

b. Configuration `/etc/haproxy/haproxy.cfg` :

```
frontend http_front
   bind *:80
   default_backend http_back

backend http_back
   balance roundrobin
   server web1 192.168.1.20:80 check
   server web2 192.168.1.21:80 check
```

c. Redirection du port 80 vers HAProxy via Stormshield

d. Tests

- Actualisation rapide depuis un navigateur montre l'alternance de pages de SRV-WEB1 et SRV-WEB2

---

4. Mission 3 – Cluster HeartBeat pour HAProxy

Objectif

Éviter que le HAProxy devienne un **SPOF** en mettant en place un **cluster haute disponibilité** avec HeartBeat entre SRV-HAPROXY1 et SRV-HAPROXY2.

Étapes techniques

a. Installer HeartBeat sur les 2 serveurs

sudo apt install heartbeat -y

b. Configuration commune :

Fichier `/etc/ha.d/ha.cf` :

logfacility local0

keepalive 2

deadtime 10

warntime 5

initdead 20

bcast eth0

node haproxy1

node haproxy2

Fichier `/etc/ha.d/haresources` (sur HAPROXY1) :

haproxy1 IPaddr::192.168.1.30/24/eth0 haproxy

`192.168.1.30` devient l'**IP virtuelle** du cluster.

c. Démarrage du service HeartBeat

sudo systemctl start heartbeat

d. Test de basculement

- Éteindre `SRV-HAPROXY1` → IP 192.168.1.30 bascule sur `SRV-HAPROXY2`
- Vérification avec `ip a` et en accédant au site web

---

5. Mission 4 – Mise en place VPN SSL

Objectif

Permettre aux télétravailleurs de se connecter **sécurisé** au réseau interne via **VPN SSL**, avec **authentification AD**.

Étapes techniques

a. Choix de la solution : OpenVPN Access Server ou pfSense + OpenVPN

- Ici, exemple avec **OpenVPN installé sur Debian** connecté à SRV-ADTECH

b. Installation OpenVPN :

sudo apt install openvpn easy-rsa -y

c. Configuration serveur VPN

- Génération des certificats
- Configuration `/etc/openvpn/server.conf` :

port 1194

proto udp

dev tun

ca ca.crt

cert server.crt

key server.key

dh dh.pem

server 10.8.0.0 255.255.255.0

push "route 192.168.1.0 255.255.255.0"

d. Intégration Active Directory via LDAP

Installation de `openvpn-auth-ldap` ou plugin équivalent, puis config :

plugin /usr/lib/openvpn/openvpn-auth-ldap.so /etc/openvpn/auth-ldap.conf

e. Authentification par groupe AD

Configurer la restriction à un groupe `g_vpn` avec le filtre LDAP :

(&(memberOf=CN=g_vpn,OU=Groupes,DC=techuniverse,DC=lan))

f. Client OpenVPN

- Génération des fichiers `.ovpn`
- Test depuis un PC distant → Ping vers le LAN via VPN

---

6. Mission 5 - UTM; Configuration complète du Stormshield pour la DMZ

Objectif

Configurer l'UTM Stormshield afin de protéger l'infrastructure de TechUniverse en :

- Filtrant les flux réseau entre WAN, LAN et DMZ
- Permettant l'accès aux serveurs Web depuis l'extérieur
- Autorisant la communication entre les serveurs DMZ et l'AD pour l'authentification

---

1. Architecture réseau UTM

Interface	Rôle	IP affectée	Réseau associé
WAN	Internet	Dynamique (via pont)	Réseau du lycée
DMZ	Zone publique	192.168.1.25	192.168.100.0/24
LAN	Privé	192.168.200.25	192.168.200.0/24

---

2. Configuration des interfaces réseau

Ouvrir l'interface d'administration Stormshield via navigateur :

https://<adresse_wan_du_utm>

1. Connexion avec les identifiants fournis.
2. Aller dans **Configuration > Réseau > Interfaces**
3. Configurer les interfaces :

a. Interface WAN :

- Type : DHCP client
- Interface physique liée à la carte réseau en mode pont VirtualBox

b. Interface DMZ :

- IP statique : `192.168.1.25`
- Masque : `255.255.255.0`

c. Interface LAN :

- IP statique : `192.168.200.25`
- Masque : `255.255.255.0`

---

3. Routage et NAT

1. Aller dans **Configuration > Routage / NAT > Règles NAT**
2. Ajouter une **règle NAT** pour accéder à HAProxy :

Source	Destination IP	Port	Traduction
WAN_ANY	UTM WAN IP	80	192.168.1.30 (IP virtuelle HAProxy)

3. Cocher **Activer le NAT** et **Activer la translation d'adresse source**

---

4. Règles de filtrage (firewall)

Aller dans **Configuration > Politique de sécurité > Filtrage**

Créer les règles suivantes :

a. Accès HTTP depuis l'extérieur vers HAProxy :

Source	Destination	Service	Action
ANY (WAN)	192.168.1.30:80	HTTP	Accepter

b. Accès DMZ → LAN pour authentification AD (LDAP) :

Source	Destination	Service	Action
192.168.1.0	192.168.200.10	LDAP/LDAPS	Accepter

c. VPN (optionnel si VPN passe par Stormshield) :

- Ouvrir les ports `1194` (UDP) ou `443` selon configuration VPN SSL

---

5. Bonnes pratiques appliquées

- Interfaces bien nommées (`INT-DMZ`, `INT-LAN`, etc.)
- Pas d'accès LAN complet depuis la DMZ
- Règles firewall les plus restrictives possibles
- Journalisation activée pour chaque règle sensible
- Interfaces surveillées avec alertes actives

---

7. Mission 6 – Active Directory; Mise en place de SRV-ADTECH

Objectif

Mettre en place un **contrôleur de domaine** sous **Windows Server 2022**, centralisant l'authentification des utilisateurs et services (dont VPN). Ce serveur sera intégré au réseau LAN, accessible depuis la DMZ de manière contrôlée.

---

1. Configuration du contrôleur de domaine

a. Renommer la machine

Rename-Computer -NewName "SRV-ADTECH" -Restart

b. Attribuer une IP statique via GUI ou PowerShell :

New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.200.10 -PrefixLength 24 -DefaultGateway 192.168.200.1

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 127.0.0.1

c. Installation des rôles AD DS et DNS

Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Install-WindowsFeature -Name DNS -IncludeManagementTools

d. Promotion en tant que contrôleur de domaine

Import-Module ADDSDeployment

Install-ADDSForest -DomainName "techuniverse.lan" -DomainNetbiosName "TECHUNIVERSE" -SafeModeAdministratorPassword (ConvertTo-SecureString "Password123!" -AsPlainText -Force) -InstallDNS

Un redémarrage est automatique à la fin.

---

2. Création des unités organisationnelles et comptes

a. OU (Organisation Units)

Ouvrir "**Utilisateurs et Ordinateurs Active Directory**", créer :

- `OU=Utilisateurs`
- `OU=Groupes`
- `OU=VPN`

b. Comptes utilisateurs de test

New-ADUser -Name "Alice Durand" -SamAccountName "adurand" -AccountPassword (ConvertTo-SecureString "Password123!" -AsPlainText -Force) -Enabled $true -Path "OU=Utilisateurs,DC=techuniverse,DC=lan"

c. Groupe VPN

New-ADGroup -Name "g_vpn" -GroupScope Global -Path "OU=Groupes,DC=techuniverse,DC=lan"

Add-ADGroupMember -Identity "g_vpn" -Members "adurand"

---

3. Intégration au projet VPN

Le contrôleur AD est utilisé pour :

- Authentifier les connexions VPN via LDAP
- Restreindre les connexions au groupe `g_vpn`

Les ports suivants doivent être ouverts depuis la DMZ :

Service	Port	Utilité
LDAP	389	Authentification simple
LDAPS	636	LDAP sécurisé
DNS	53	Résolution domaine local

---

4. Bonnes pratiques appliquées

- Comptes d’administration nominatifs
- Mots de passe complexes activés
- OU séparées pour gestion facilitée
- Rôles DNS/AD distincts de la DMZ
- Journalisation des accès activée

---

8. Tests réalisés

Fonctionnalité	Résultat attendu	Vérifié
Accès web via IP publique	Page Apache s'affiche	✅
Répartition de charge HAProxy	Alternance entre les deux serveurs Web	✅
Bascule du cluster HeartBeat	IP virtuelle bascule sur nœud secondaire	✅
Ping UTM depuis serveur DMZ	Réponse de 192.168.1.1	✅
Accès au site depuis WAN (port 80)	Redirection vers HAProxy OK	✅
Résolution LDAP depuis DMZ vers AD	Connexion au domaine possible	✅
Ajout d'un utilisateur dans l'AD	Compte visible depuis console	✅
Ping depuis serveur DMZ	Réponse de `192.168.200.10`	✅
Authentification VPN via LDAP	Réussie pour un membre `g_vpn`	✅

9. Conclusion

Ce projet a permis de renforcer l'infrastructure DMZ de TechUniverse de manière **fiable et évolutive :**

- **Amélioration des performances Web** grâce à la répartition de charge
- **Haute disponibilité assurée** avec HeartBeat
- **Connexion sécurisée** des employés en télétravail avec le VPN AD

L'ensemble est facilement transposable à la production, et répond aux besoins de croissance de l'entreprise.
