# CAS DMAT

**Barème**

| | | |
|---|---|---|
| Dossier A | **Intégration et sécurisation du site de Trèves** | 50 points |
| Dossier B | **Ouverture à l'Allemagne** | 15 points |
| Dossier C | **Evolution du stockage et de la sécurisation des données** | 35 points |
| | Total | 100 points |

## Dossier A – Analyse de la demande et choix d'une solution

### Mission A.1 – Sécurisation des sites

**Question A.1.1**
Expliquer le rôle des règles N°1 et N°2 et les réseaux locaux virtuels (VLAN) concernés.

**Commutateur S3X-M1 - zone IN**

| *N° de règle* | *Adresse source* | *Port source* | *Adresse dest* | *Port dest* | Action |
|---|---|---|---|---|---|
| 1 | 172.18.224.0/24 | * | 172.18.145.0/24 | 22(SSH) | Autoriser |
| 2 | * | * | 172.18.31.1/32 | 53(DNS) | Autoriser |
| … | | | | | |
| Défaut | Toutes | Tous | Toutes | Tous | Refuser |

Règle N°1 - L'adresse source 172.18.224.0/24 correspond au Vlan 224 de la DSI, il est autorisé à accéder en SSH aux adresses 172.18.145.0 à 172.18.145.255 qui correspondent au VLAN 145 ou VLAN serveur
Règle N°2 – toutes les adresses source/ports source sont autorisés à accéder au serveur DNS 172.18.31.1 du VLAN DMZ via le port DNS (53), cette règle permet d'effectuer les résolutions DNS depuis n'importe quelle adresse vers le serveur DNS de la DMZ

**Question A.1.2**
Écrire la (ou les) règle(s) permettant d'autoriser les communications SSH vers les serveurs de Trèves depuis les réseaux locaux virtuels (VLAN) DSI de Trèves et de Metz.

**Question A.1.3**
Écrire la (ou les) règle(s) permettant d'autoriser les communications DNS des réseaux de Trèves vers le serveur DNS de Metz.

**Règles de filtrage RtTr de Trèves**

| *N° de règle* | *Adresse source* | *Port source* | *Adresse dest* | *Port dest* | Action |
|---|---|---|---|---|---|
| 1 | 172.19.224.0/24 | * | 172.19.145.0/24 | 22(SSH) | Autoriser |
| 2 | 172.18.224.0/24 | * | 172.19.145.0/24 | 22(SSH) | Autoriser |
| 3 | 172.19.0.0/16 | * | 172.18.31.1/32 | 53(DNS) | Autoriser |
| … | | | | | |
| *Défaut* | *Toutes* | *Tous* | *Toutes* | *Tous* | *Refuser* |

**Mission A.2 – Proposition d'une solution d'infrastructure**

**Question A.2.1**

Ajouter les enregistrements DNS nécessaires afin de prendre en compte le nouveau site de Trèves.

| | | | | |
|---|---|---|---|---|
| 1 | $TTL 172800 | | | |
| 2 | @ IN SOA dmat.net. hostmaster.dmat.net. (2018102200; serial 21600; refresh 3600; retry 3600000; expire 86400 ) | | | |
| | | | | |
| 3 | @ | IN | NS | SrvDnsM.dmat.net. |
| 4 | @ | IN | NS | SrvDnsEs.dmat.net. |
| 5 | @ | IN | NS | SrvDnsTh.dmat.net. |
| 5b | @ | IN | NS | SrvDnsTr.dmat.net. |
| 6 | | IN | MX 10 | SrvMailM.dmat.net. |
| 7 | | IN | MX 20 | SrvMailEs.dmat.net. |
| 8 | SrvDnsM | IN | A | 172.18.31.1 |
| 9 | SrvDnsEs | IN | A | 172.17.31.1 |
| 10 | SrvDnsTh | IN | A | 172.16.31.1 |
| 10b | SrvDnsTr | IN | A | 172.19.31.1 |
| | ; serveur web public Srv-Pub | | | |
| 11 | SrvPubM | IN | A | 172.18.65.1 |
| | ; serveur web Srv-GC | | | |
| 12 | SrvGcM | IN | A | 172.18.67.1 |
| | ; Alias pour le serveur public | | | |
| 13 | www | IN | CNAME | SrvPubM.dmat.net. |

**Question A.2.2**

a) Proposer un paramétrage DNS des postes clients qui permette d'assurer la résolution DNS même en cas de panne du serveur DNS local.

Il faut configurer les postes clients pour que le DNS du site de Trèves réponde de manière préférée aux requêtes DNS des postes en local et en cas d'échec le DNS du site de Metz
Adresse DNS 1 (préféré) : adresse IP DNS de Trèves soit 172.19.31.1
Adresse DNS 2 (auxiliaire) : adresse IP DNS de Metz soit 172.18.31.1

**Question A.2.2**

b) Proposer une procédure détaillée qui permette de tester ce paramétrage en vous appuyant sur les serveurs connus de l'entreprise qui sont présents sur le site de Metz.

La commande NSLOOKUP ou DIG sera utilisée pour vérifier quel serveur effectue la résolution DNS

1 NSLOOKUP S*rvPubM.dmat.net* doit renvoyer le serveur de Trèves et non celui de Metz
Serveur : SrvDnsTr.dmat.net
Adresse : 172.19.31.1
Réponse faisant autorité :
Nom : *SrvPubM.dmat.net*
Adresse : 172.18.65.1

2 Afin de vérifier que la résolution depuis Metz fonctionne, on arrête le service DNS local (ou on désactive la carte réseau du serveur…)

3 On effectue à nouveau le test précédent qui doit retourner l'adresse du serveur de Metz

**Mission A.3 – Gestion des serveurs avec Ansible**

**Question A.3.1**
Citer quatre arguments en faveur de l'utilisation d'un logiciel de gestion de configuration comme Ansible pour configurer les serveurs.

Arguments possibles :

- Constituer une base de référence (centralisée) sur les configurations modèles des machines.
- Éviter les tâches répétitives : on ne réalise le travail de configuration qu'une seule fois.
- Déployer automatiquement et rapidement des machines.
- Permettre une configuration homogène de parc ce qui réduit les risques d'erreurs et simplifie la maintenance.
- S'assurer que les machines conservent leur configuration.
- Effectuer des actions simultanément sur tout ou partie de son infrastructure (mise à jour globale de sécurité, audit de tous les serveurs, etc..).
- Gérer son infrastructure avec du code plutôt que des actions manuelles : toute action sur le système est alors versionnée, testée, automatisée, reproductible.

**Question A.3.2**
Détailler les étapes nécessaires au déploiement de la configuration des serveurs du site de Trèves via le logiciel Ansible.

Étape 1 : ajouter au fichier /etc/ansible/hosts :

- un groupe [site_treves] qui comprend tous les serveurs de Trèves ;
- les noms des serveurs à chaque groupe spécifique.

Étape 2 : copier la clé publique du serveur Ansible de Metz sur chaque machine.

Étape 3 : exécuter :

- le playbook de base : ansible-playbook baseServers.yml -e "nomsHotes=site_treves" ;
- les playbook spécifiques.

**Question A.3.3**
a) Écrire le fichier d'instructions (*playbook*) « securSSH.yml » permettant de répondre aux contraintes de sécurité quant au service SSH.
b) Écrire la commande qui exécute le fichier d'instructions (*playbook)*.

a)

```
- name: Suppression de l'authentification par mot de passe
  hosts: Dmat-Out
  tasks:
 - name: modification du fichier de configuration
  lineinfile:
       dest:/etc/ssh/sshd_config
       regexp: '^PasswordAuthentication'
       line: 'PasswordAuthentication no'

 - name: redémarrage du service ssh
      service:
        name: ssh
        state: restarted
```

b)

```
ansible-playbook securSSH.yml
```

*Si on a utilisé une variable (par exemple « nomsHotes » alors la commande sera ansible-playbook securSSH.yml -e "nomsHotes= Dmat-Out"*

## Dossier B – Ouverture à l'Allemagne

### Mission B.1 – Choix d'une solution technique

**Question B.1.1**
Parmi les matériels présents, lister ceux qui doivent être remplacés en expliquant les raisons de ce changement.

Les points d'accès sont à changer car ils ne seront plus administrables à distance avec IPv6.

Les commutateurs de niveau 2 ne seront plus administrables à distance avec IPv6, il faut donc les changer.

**Question B.1.2**
Présenter trois avantages de la solution Dual-Stack Lite12 par rapport à l'IPv6 natif.

Les avantages de cette solution par rapport à l'IPv6 natif.

- Transparent pour l'entreprise car IPv6 est géré au niveau du FAI.
- Ne nécessite pas de changement de matériel.
- Ne nécessite pas de modification sur le réseau interne de l'entreprise : permet de conserver l'adressage IPv4 du réseau interne de l'entreprise.
- Ne nécessite pas de compétences particulières ou de formation du personnel
- Pas d'incidence sur la connexion Internet

*Dual-Stack Lite12 permet d'interconnecter des réseaux IPv4 à travers un réseau de FAI en IPv6 natif (full IPv6). Le routeur chez le client est connecté au FAI en IPv6 et tout le trafic IPv4 de l'entreprise est encapsulé dans un tunnel IPv6 vers IPv4 (6to4). Ceci permet donc de conserver l'adressage IPv4 au niveau du réseau interne de l'entreprise*

*Cependant, Dual-Stack Lite 12 utilise un système d'encapsulation d'IPv4 dans IPv6, cette solution est donc plus lente.*

### Mission B.2 – Proposition d'une solution d'infrastructure

**Question B.2.1**
Écrire les enregistrements à ajouter au fichier DNS afin de prendre en compte l'adressage IPv6.

*Le serveur Web public de DMat a l'adresse : 2002:7a7b:0:1241::1*

*Le serveur Web Grand Compte de DMat a l'adresse : 2002:7a7b:0:1243::1*

Ajouter l'enregistrement de type AAAA pour les adresses IPv6 des 2 serveurs

```
SrvPubM    IN   AAAA      2002:7a7b:0:1241::1
SrvGcM     IN   AAAA      2002:7a7b:0:1243::1
```

# Dossier C – Évolution du stockage et de la sécurité des données

## Mission C.1 – Choix et gestion d'une solution de stockage

**Question C.1.1**
Présenter deux avantages d'utiliser une solution XSan Raid pour stocker les fichiers de développement 3D plutôt que le stockage sur les stations de travail.

Centralisation des données

-> fichiers accessibles depuis l'ensemble des postes sans recopie de poste en poste.

-> Sauvegarde plus simple.

Fiabilité des données (RAID).

**Question C.1.2**
a) Présenter, sous forme d'un tableau comparatif, les caractéristiques des deux configurations envisagées en termes de stockage utile, de tolérance de pannes et de performance.
b) Proposer la solution à mettre en œuvre pour le nouveau pôle Design d'Esch-sur-Alzette en expliquant votre choix.

a)

| | 3 grappes de 4 disques | 4 grappes de 3 disques |
|---|---|---|
| Stockage utile | On perd l'équivalent d'un disque de parité par grappe. Stockage utile = 3 (grappes) x 3 (disques) x 500 (capacité d'un DD) = 4,5 To | On perd l'équivalent d'un disque de parité par grappe. Stockage utile = 4 (grappes) x 2 (disques) x 500 (capacité d'un DD) = 4 To |
| Tolérance de panne | Risque de perte de données à partir du 2ème DD défaillant (si les 2 DD en panne appartiennent à la même grappe) | Idem |
| Performance | Parallélisation des écritures sur 3 grappes | Parallélisation des écritures sur 4 grappes -> *plus rapide* |

b)
La solution que je préconise pour le nouveau pôle Design d'Esch-sur-Alzette est de faire 4 grappes de 3 disques. En effet, même si le stockage utile est un peu plus faible (*-12,5%*), la rapidité est meilleure, ce qui est un critère primordial (*document C1)*

**Mission C.2 – Protection des données pour une mise en conformité avec le RGPD**[1]

**Question C.2.1**

Indiquer, en argumentant, si la solution actuelle d'accès aux locaux sensibles vous semble être en totale conformité avec la politique de protection des accès aux locaux sensibles de DMat et les exigences du RGPD.

La solution actuelle (accès par jeu de clés) d'accès aux locaux sensibles n'est pas en totale conformité avec la politique de protection des accès aux locaux sensibles de DMat et les exigences du RGPD.

En effet, l'accès par jeu de clés, a quelques inconvénients du fait que les clés sont obligatoirement affectées par local :

- du fait du nombre de clés important à gérer par employé, le vol de clé (et l'accès non autorisé à un local) peut passer inaperçu ;
- il faut changer tout le système en cas de perte de clé et le local en question est vulnérable jusqu'au changement effectif ;
- une copie de clés est possible (même si c'est compliqué).

Il est ainsi difficile de s'assurer qu'un utilisateur donné n'a pas accès à un local, ce qui ne répond pas aux exigences du RGPD.

Par ailleurs, il n'est pas possible, rien qu'avec ce système, de restreindre de manière fiable l'accès selon une plage horaire ni d'enregistrer les dates et heures d'accès par employé (anonymat).

Enfin, le nombre de clés nécessairement important et les habilitations gérées via un simple fichier texte ne rendent pas le système souple, notamment lors de mouvement du personnel.

**Question C.2.2**

Présenter trois avantages d'une solution basée sur la technologie NFC par rapport à la solution actuelle.

La solution NFC apporte une flexibilité et une plus-value indéniable par rapport au système actuel et répondent aux exigences du RGPD et des souhaits du DSI :

- l'identifiant est affecté à l'employé, le contrôle d'accès est basé sur une vérification des utilisateurs ;
- le système est centralisé et accorde ou refuse de manière automatique la demande (plus de fichier « traitement de texte » dans lequel il peut y avoir des incohérences et difficile à mettre à jour) ;
- toute entrée et sortie (et éventuellement tentative de fraude) peut être archivée et horodatée avec la possibilité d'alerte immédiate.
- il n'y a plus de trousseaux de clés (éventuellement perdus à gérer) : un seul badge en lieu et place de plusieurs clés ;
- en cas de perte ou de vol ou de soupçon de compromission d'un badge, il suffit d'en donner un autre (et de désactiver le badge actuel).

1 RGPD :Règlement général européen relatif à la protection des données personnelles

**Question C.2.3**
Pour chaque élément du système de contrôle des habilitations, préciser le local technique dans lequel vous l'installerez. *Justifier votre réponse*

Trois éléments :

- le contrôleur ;
- le serveur accueillant le logiciel de contrôle d'accès ;
- la base de données.

Pour chaque site :

- chaque contrôleur sera positionné dans le local qu'il protège ;
- deux serveurs doivent être installés (le serveur d'application et le serveur de base de données) : le serveur d'application accueillant le logiciel de contrôle d'accès doit être dans le local 4 (serveurs applicatifs ne contenant pas de données sensibles) et la base de données doit être dans un serveur du local 2 (stockage des données sensibles).