# Consignes

* **Les réponses doivent être d’une couleur différente aux questions *(surtout pas de rouge)***
* **Les réponses doivent être à la suite des questions.**
* **Si vous n’avez pas répondu à une question, la surligner en jaune**
* **Vous pouvez compléter vos réponses par des schémas**
* **Pensez à une mise en forme propre pour le correcteur**
* **Toute triche sera sanctionnée.**

***Le non-respect des consignes suivantes sera pénalisant pour la note finale !!!***

**Une fois terminé, vous devrez créer une archive contenant :**

* **L’étude cas.**
* **Le tableau ACL+NAT x DMZ (fourni)**
* **Le Packet Tracer configuré**

**Vous devrez compresser cette archive (7zip,zip,rar) et la renommer (compte pour la note) de la manière suivante :**

**Nom-prénom-ReaRes2-TSSR-XXXX ( XXXX = Numéro de votre session ex : TSSR-1904)**

# Sujet :

(Suite REA3)

Engineer Aero a subi plusieurs attaques informatiques durant ces derniers mois. Même si votre équipe a su intervenir aux bons moments et empêcher des problèmes graves pour l’entreprise, vous avez la responsabilité de renforcer la sécurité de votre infrastructure réseau afin de réduire au maximum les risques que peut encourir votre entreprise.

Vous allez donc devoir mettre en place un filtrage restreint dans votre infrastructure.

**ÉTUDE DE CAS**

Étude de solution : La Sécurisation

## 1- Filtrage réseau

L’utilisation de filtrage pour sécuriser le Traffic interne sur le réseau est une bonne solution, disposant de routeur Cisco, vous décidez d’utiliser les ACLs. Pour cela vous avez besoin d’informations sur son fonctionnement.

1. Quelle est la différence entre ACL et ACE ?

Une ACL (Access Control List) est une liste composée d’ACE (Access Control Entry). Les ACE sont des filtres qui permettent ou pas la circulation de données.

1. Quelle est la différence entre ACL étendue et standard ?

L’ACL standard ne prend en paramètre que l’adresse de destination, or l’ACL extended elle permet de renseigner les ports, le protocole de transport, ainsi que l’adresse source.

1. Peut-on créer autant d’ACL que l’on veut pour filtrer un réseau ou sous-réseau ?

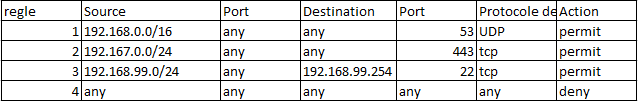
Théoriquement oui, mais il y a quand même des limites en fonction du matériel utilisé, et de l’espace disponible.

1. Dans une ACL toutes les règles sont-elles lues ? Justifier.

Non. Elles sont lues en commençant par la première, et une fois qu’une ACL correspond alors la lecture s’arrête.

1. Dans le cadre de la mise en place de règles, sur un routeur modèle Cisco comment se programme la règle 4 ?

Il n’est pas nécessaire d’implémenter cette règle dans la liste, car une fois qu’il y a une règle permit, alors tout le reste est refuse (deny) automatiquement.



## 2 - DMZ

Engineer Aero souhaite rendre accessible un site web aux client extérieurs, pour mieux le sécuriser vous souhaitez le mettre dans une DMZ, pour cela vous avez besoin de certaines informations qui sont les suivantes :

1. Qu’est-ce qu’une DMZ ?

C’est une zone démilitarisée. Une zone qui sera accessible depuis les réseaux interne et les réseaux public (externe) afin de procurer des services. Elle est écartée des autres réseaux pour ne pas créer de faille de sécurité.

1. Quelles sont les 2 implantations de la DMZ les plus répandues ?

Entre deux routeurs/pare-feu, donc complètement isolée. Ou bien après le même routeur/pare-feu que les autres réseaux.

1. Quelles sont les restrictions de base à suivre pour créer d’une DMZ ?

Les éléments (généralement des serveurs) dans la DMZ ne doivent pas envoyer de requêtes, ils doivent seulement y répondre (ex : Ne peut pas accéder à internet mais peut quand même répondre aux requêtes venant des réseaux externe). Elle doit être séparée au maximum des autres réseaux.

1. Pour la mise en place de notre DMZ pour notre serveur web, on nous recommande d’utiliser un MSR en /30 pour quelle(s) raison(s) ?

Cela nous permet d’avoir uniquement 2 adresses disponible pour du matériel dans ce sous réseaux, ce qui permet d’éviter que des personnes malveillantes puisse s’introduire dans le réseau et utiliser la technique du middle man.

## 3 – Mise en place de règle de filtrage

***Lisez attentivement les consignes, pour tout doute ou questions demandez à votre formateur.***

Votre schéma de base se trouve sur le document excel « **rea\_rés\_2\_acl-X-dmz**».  
Vous disposez de la plage d’adresses **172.16.0.0 /16** que vous allez segmenter d’une façon sécurisée, optimisée et facile d’utilisation au quotidien, vous appliquerez la plage **10.0.0.0 /30 pour votre DMZ**.

Dans le but de sécuriser votre infrastructure, vous allez mettre en place un filtrage sur le réseau grâce aux ACLs, suivis d’une mise en place de la DMZ avec l’aide des tableaux fournie.

**Travaux à faire :**

**Complétez** les tableaux contenus dans le fichier Excel « **rea\_rés\_2\_acl-X-dmz** » :

* Dans l’onglet DMZ, vous devrez **compléter des tableaux ACL pour chaque interface de votre DMZ.**
* **Complétez les tableaux NAT.**
* **Le schéma** réseaux sur **Packet tracer vous est remis,** vous devrez mettre en place les **services** (DHCP, DNS), le SSH pour les périphériques intermédiaires.
* Votre **DMZ** (avec un serveur web [www.aero.net](http://www.aero.net) accessible aux utilisateurs externe) et **les règles ACL** demandées.

**Des Commentaires explicatifs pour chacune des règles écrites sont attendus**

**Vous mettrez une capture d’écran de votre schéma avec toute les informations concernant votre plan d’adressage dans le doc Excel sur l’onglet DMZ à l’emplacement prévus**.