Question 1 : Que veut dire l’acronyme DDOS ?

Question 2 : Quelle caractéristique DNS peut-on utiliser pour réduire l’efficacité d’une attaque DDOS

Question 3 : Comment peut-on mitiger une attaque DDOS ?

Question 4 : Pourquoi anycast est-il lié à BGP ?

Réponse 1 : Distributed denial of service (Attaque par déni de service distribué)

Réponse 2 : SPF (mail), Anycast, BGP

1. SPF : Le SPF (Sender Policy Framework) est un système de validation par courrier électronique pour empêcher les spammeurs d’envoyer des messages au nom de votre domaine. Avec le SPF, une organisation peut publier des serveurs de messagerie autorisés. Avec les informations liées au DMARC, il donne au récepteur (ou aux systèmes récepteurs) des informations sur la fiabilité de l’origine d’un email.  
   Le SPF est, tout comme le DMARC, une technique d’authentification par courrier électronique qui utilise le DNS (Domain Name Service). Cela vous permet, en tant qu’expéditeur d’un e-mail, de spécifier quels serveurs de messagerie sont autorisés à envoyer des e-mails au nom de votre domaine.
2. Anycast : **Anycast** est une technique d'adressage et de routage permettant de rediriger les données vers le serveur informatique le "plus proche" ou le "plus efficace" selon la politique de routage. Avec anycast, une adresse IP peut être affiliée à plusieurs machine. Exemple : je me connecte sur le site de l’etml depuis Lausanne alors je vais utiliser le serveur de Lausanne. Si je me trouve à Berne, la requête va être redirigée sur le serveur de Berne. (un client émet une requête spécifique, celle-ci n’est généralement communiquée qu’à un serveur anycast du groupe. Ce serveur procède ensuite à la requête DNS du client. Le schème de routage ne fonctionne que sous sa forme prévue si l’adresse IP utilisée a également été **explicitement déclarée adresse anycast sur les routeurs correspondant**d’un réseau anycast.)
3. BGP : Le protocole BGP (Border Gateway Protocol) est l'un des protocoles clés à utiliser pour réaliser la redondance de connexion Internet. Quand vous connectez votre réseau à deux fournisseurs de services Internet différents (ISPs), cela s'appelle l'*hébergement multiple*. L'hébergement multiple fournit la redondance et l'optimisation du réseau. Il sélectionne l'ISP qui offre le meilleur chemin à une ressource. Quand vous exécutez BGP avec plusieurs fournisseurs de services, vous prenez le risque que votre système autonome (AS) devienne un AS de transit. Le trafic Internet passe ainsi par votre AS et utilise potentiellement toute la bande passante et toutes les ressources sur le CPU de votre routeur. Ce document traite de ce problème, avec des exemples de configuration appropriés.

Réponse 3 : Les entreprises comme cloudflare(qui sont spécialisé dans la sécurité internet) nous protègent au mieux des DDOS. Ils ont plusieurs manières de nous protéger.

1. Couche 7 (application) : quand le centre de données reçoit une requête, ils peuvent voir si le visiteur est un threat, un agent et la vitesse des requêtes envoyer. Tout ressources déjà mises en cache sont servies directement depuis les centres de données, les autres requêtes des clients sont envoyées sur notre site.
2. Couche 4 (transport) : ils envoient du trafic TCP plus rapidement que le service d’internet grâce à un system de routage intelligent et d’apprentissage automotique (Machine-Learning) autour des points de congestion du réseau. Il atténue le réseau de plus de 172 Tbps la détection instantanée des menaces et un délai d'atténuation (Time-to-Mitigate, TTM) inférieur à 3 s contre la plupart de ces dernières.
3. Couche 3 (réseau) : Ils protège les sous-résous IP contre les DDOS et accélère le trafic réseau, en utilisant des protocoles réseau comme BGP (anycast), GRE, IPsec pour le routage et l’encapsulation.

Réponse 4 : Parce que les paquets sont dirigé vers un routeur central qui lui-même va rediriger vers la bonne route. Le BGP permet a anycast de transporté les données au-delà des réseaux individuels d’un fournisseur d’accès à internet. (**Divers itinéraires alternatifs peuvent être rendus disponibles au niveau national, et même mondial.)**