Consignes :

- Les projets seront réalisés en groupes de 4 à 5 étudiants.
- Chaque groupe doit soumettre un rapport et une présentation du projet.
- Les livrables doivent être soumis **en ligne sur Moodle** avant le **05/12/2022 à 23:59**. Les livrables soumis par e-mail seront automatiquement rejetés.
- Chaque groupe doit présenter son projet devant un jury. **Les présentations sont programmées le 07/12/2022**. Chaque groupe aura 20 min de présentation et 5 min de Q/R.
- La note finale tiendra compte de la qualité de tous les livrables et de la présentation.
- Vous êtes tenu de réaliser le projet vous-même. Deux projets similaires détectés, les deux groupes auront systématiquement 0.
- De même, tout signe de plagiat, la note sera 0.
- L'évaluation sera basée sur les détails de la solution (adressage, durcissement, implémentation, etc.)

Projets

Projet 1 : SecureNet

Présentation de l'entreprise : Votre société est engagée pour concevoir l'infrastructure réseau de la société "SecureNet", spécialisée dans les services informatiques. SecureNet a 5 départements : IT, RH, vendeurs, marketing et l'administration et possède un parc de 6 serveurs, à savoir, AD, Web, DHCP, Email, RH, Fichier.

SecureNet dispose également d'une connexion Internet qui est partagée par les différents départements.

Disposition des bâtiments :

Récemment, SecureNet a acquis trois bâtiments :

- Le premier bâtiment abrite la ferme de serveurs au premier étage, la moitié du département IT au deuxième étage et Marketing au troisième étage.
- Le deuxième bâtiment abrite le reste du service IT au premier étage et la moitié des vendeurs au deuxième étage.
- Le troisième bâtiment comprend le reste des vendeurs au premier étage et RH et l'administration au deuxième étage.

Exigence :
L'entreprise a des exigences spécifiques pour l'infrastructure réseau :

- **Département IT :** Le service IT communique avec l'administration et vendeurs et peut accéder au parc des serveurs et à Internet.
- **Département vendeurs :** communique avec IT et marketing et peut accéder à Internet. Ils ont accès aux serveurs fichier, web, email.
- **Département administration** : L'administration communique avec Marketing et IT et peut accéder à Internet. Ils ont accès aux serveurs fichier, web, email.
- **Département marketing** : ils peuvent communiquer avec vendeurs et administrations et ne peuvent pas accéder à Internet. Ils ont accès aux serveurs fichier, email.
- **Département RH** : ils ne peuvent communiquer avec personne mais peuvent accéder à Internet. Ils ont accès aussi au serveur qui héberge l'application RH, et au serveur email.
- Les serveurs doivent être dans une DMZ
- **Tous les serveurs** doivent être accessibles au service IT
- Les serveurs Web et email doivent être accessibles depuis internet
- **Seuls IT et vendeurs auront des PCs portables.**
- Chaque bâtiment dispose de 13 téléphones IP.
- L'adresse IP doit être de l'ordre de 192.168.112.0/20, où le personnel est réparti comme suit comme suit : IT : 153, RH : 59, Vendeurs : 452 Marketing : 124 et Administration : 99.

Travail demandé :

1. Architecture du Réseau LAN :

- **Architecture Globale :** Proposez une vue d'ensemble de la structure du réseau LAN en identifiant les principaux composants et leur emplacement dans le bâtiment.
- **Architecture Détaillée :** Fournissez une vue plus détaillée de chaque étage, y compris les connexions entre les départements et les équipements nécessaires.

2. Équipement Réseau Requis :

- Spécifiez le type d'équipement réseau (routeurs, commutateurs, pare-feux, etc.) nécessaires pour répondre aux exigences de l'entreprise.

3. Coût de la Conception :

- Estimez les coûts de mise en œuvre de la conception, y compris les serveurs, ordinateurs portables, composants réseau, téléphones IP, etc., en expliquant vos choix d'équipement (vous pouvez ignorer le cout du câblage).

4. Schéma d'Adressage IP :

- Proposez un schéma d'adressage IP pour l'entreprise, en précisant la méthode choisie (par classes, par bloc, VLSM, etc.) et en justifiant votre choix. Fournissez des détails sur les adresses réseau, les masques de sous-réseau, les plages d'adresses d'hôtes et les adresses de diffusion.

5. Politique de sécurité :

- La société vous demande de créer **Politique de Sécurité des Systèmes d'Information (PSSI)** et une politique de sécurité réseau (Network Equipment Security Guidelines) qui définit les principes, les procédures et les lignes directrices à suivre pour appliquer, gérer, surveiller et maintenir la sécurité d'un réseau informatique de l'entreprise.

6. Segmentation du Réseau et Routage :

- Mettez en place une segmentation de réseau et implémenter un routage (statique ou dynamique) pour interconnecter le réseau de l'entreprise.

7. Sécurisation du Réseau : Mettez en place un plan détaillé pour sécuriser le réseau.

- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut pour des mots de passe forts et uniques, et appliquez des politiques de mots de passe robustes. Mettez en place des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau et restreindre l'accès non autorisé. Désactivez les services inutiles et utilisez le protocole Secure Shell (SSH) pour la gestion à distance. Configurez la journalisation et l'audit pour surveiller les événements de sécurité. Sécurisez l'accès physique au routeur et activez le démarrage sécurisé pour protéger le micrologiciel et les configurations. Utilisez le protocole Network Time Protocol (NTP) pour une horloge précise et configurez le système de journalisation syslog pour stocker les journaux sur des serveurs distants. Désactivez les interfaces et protocoles inutilisés, comme le protocole de découverte Cisco (CDP). (**Liste non exhaustive**)
- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut, sécurisez les interfaces de gestion, configurez les accès SSH, configurez Port Security, désactivez les ports et les services non utilisés, restreignez l'accès SNMP avec une authentification solide, mettez en place des VLAN pour la segmentation du réseau, utilisez l'authentification basée sur le port comme le 802.1X, activez le suivi DHCP, utilisez DAI et IP Source Guard pour prévenir les attaques de spoofing d'adresse, contrôlez l'accès à la gestion, sécurisez l'accès physique, etc (**Liste non exhaustive**)

8. Sécurisation avec Firewalls : Configuration des paramètres de base du pare-feu

- Configurez vos firewalls ASA pour séparer les segments de réseau interne et DMZ et externe. Créez des listes de contrôle d'accès (ACL) pour contrôler le flux de trafic. Testez le pare-feu en simulant divers scénarios d'attaque et en vous assurant que seul le trafic autorisé est autorisé selon les exigences de l'entreprise.

9. Configuration Site-to-Site IPsec VPN

- L'entreprise a une annexe distante qui a accès aux ressources de l'entreprise internet via VPN. Configurez un VPN d'accès distant pour offrir un accès sécurisé aux employés au réseau d'entreprise. Mettez en place un VPN site à site en utilisant IPsec pour sécuriser les connexions entre deux succursales.

10. Points d'Accès Wi-Fi :

- Discutez de la possibilité pour l'entreprise d'installer des points d'accès Wi-Fi dans les bâtiments. Si oui, mettez en place un réseau sans fil sécurisé avec le chiffrement WPA2. Configurez le filtrage MAC, les VLAN et d'autres mesures de sécurité.

11. Evolutivité de l'architecture :

- Comment allez-vous planifier la croissance future de l'entreprise, en termes d'ajout de nouveaux départements, de serveurs, etc. ? Comment cela affectera-t-il la conception du réseau et les performances ?

12. Simulation avec Packet Tracer :

- Créez des simulations réseau en utilisant Packet Tracer pour représenter votre conception. Fournissez des adresses IP pour deux équipements par sous-réseau pour simplifier les schémas. Assurez-vous que l'ensemble des réponses précédentes est cohérent dans les simulations.

13. Documentation du Rapport :

- Assurez-vous que toutes les étapes, configurations, explications et captures d'écran sont documentées dans le rapport final. **Le document à rendre ne doit pas dépasser 10 pages**. Une synthèse et analyse du travail sont les critères de notation du rapport.

Projet 2 : ITXcelerate

Présentation de l'entreprise : Votre société est engagée pour concevoir l'infrastructure réseau de la société "ITXcelerate" spécialisée dans le conseil et les services informatiques. ITXcelerate compte 6

départements : IT, Ingénieurs, RH, Finance, Marketing et Management et dispose d'une ferme de 6 serveurs, à savoir, AD, Web, DHCP, Email, RH, Fichier.

ITXcelerate dispose également d'une connexion Internet qui est partagée par les différents départements.

Disposition des bâtiments :

Récemment, ITXcelerate a acquis trois bâtiments :

- Le premier bâtiment abrite la ferme de serveurs au premier étage, la moitié du département IT au deuxième étage et moitié des ingénieurs en troisième étage
- Le deuxième bâtiment abrite le reste du département des ingénieurs au premier étage et marketing au deuxième.
- Le troisième bâtiment comprend le reste de IT au premier étage et les ressources humaines, les finances au deuxième étage et management au troisième étage.

Exigence :
L'entreprise a des exigences spécifiques pour l'infrastructure réseau :

- **Département IT :** Le service IT communique avec management et ingénieur et peut accéder au parc des serveurs et à Internet.
- **Département ingénieurs :** communique avec marketing et IT et peut accéder à Internet. Il a accès aux serveurs Web, fichier et email
- **Département management** : communique avec finance et IT et peut accéder à Internet. Il a accès aux serveurs Web, fichier et email
- **Département marketing** : ils peuvent communiquer avec ingénieurs et ne peuvent pas accéder à Internet. Il a accès aux serveurs fichier et email
- **Département finance** : ne peut communiquer qu'avec management et peut accéder à Internet. Il a accès aux serveurs fichier et email
- **Département RH** : ne peut communiquer avec personne et peut accéder à Internet. Il a accès aux serveurs RH et email.
- Les serveurs doivent être dans une DMZ
- Tous les serveurs doivent être accessibles au service IT
- Les serveurs Web et email doivent être accessibles depuis internet
- **Seuls IT et management auront des PCs portables.**
- Chaque bâtiment dispose de 19 téléphones IP.
- Le personnel se répartit comme suit : IT : 163, Ingénieurs : 301, RH : 43, Finance : 28, Marketing : 19 et Management : 14. L'adresse IP dont dispose l'entreprise est 172.24.208.0/21

Travail demandé :

1. Architecture du Réseau LAN :

- **Architecture Globale :** Proposez une vue d'ensemble de la structure du réseau LAN en identifiant les principaux composants et leur emplacement dans le bâtiment.
- **Architecture Détaillée :** Fournissez une vue plus détaillée de chaque étage, y compris les connexions entre les départements et les équipements nécessaires.

2. Équipement Réseau Requis :

- Spécifiez le type d'équipement réseau (routeurs, commutateurs, pare-feux, etc.) nécessaires pour répondre aux exigences de l'entreprise.

3. Coût de la Conception :

- Estimez les coûts de mise en œuvre de la conception, y compris les serveurs, ordinateurs portables, composants réseau, téléphones IP, etc., en expliquant vos choix d'équipement (vous pouvez ignorer le cout du câblage).

4. Schéma d'Adressage IP :

- Proposez un schéma d'adressage IP pour l'entreprise, en précisant la méthode choisie (par classes, par bloc, VLSM, etc.) et en justifiant votre choix. Fournissez des détails sur les adresses réseau, les masques de sous-réseau, les plages d'adresses d'hôtes et les adresses de diffusion.

5. Politique de sécurité :

- La société vous demande de créer **Politique de Sécurité des Systèmes d'Information (PSSI)** et une politique de sécurité réseau (Network Equipment Security Guidelines) qui définit les principes, les procédures et les lignes directrices à suivre pour appliquer, gérer, surveiller et maintenir la sécurité d'un réseau informatique de l'entreprise.

6. Segmentation du Réseau et Routage :

- Mettez en place une segmentation de réseau et implémenter un routage (statique ou dynamique) pour interconnecter le réseau de l'entreprise.

7. Sécurisation du Réseau : Mettez en place un plan détaillé pour sécuriser le réseau.

- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut pour des mots de passe forts et uniques, et appliquez des politiques de mots de passe robustes. Mettez en place des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau et restreindre l'accès non autorisé. Désactivez les services inutiles et utilisez le protocole Secure Shell (SSH) pour la gestion à distance. Configurez la journalisation et l'audit pour surveiller les événements de sécurité. Sécurisez l'accès physique au routeur et activez le démarrage sécurisé pour protéger le micrologiciel et les configurations. Utilisez le protocole Network Time Protocol (NTP) pour une horloge précise et configurez le système de journalisation syslog pour stocker les journaux sur des serveurs distants. Désactivez les interfaces et protocoles inutilisés, comme le protocole de découverte Cisco (CDP). (**Liste non exhaustive**)
- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut, sécurisez les interfaces de gestion, configurez les accès SSH, configurez Port Security, désactivez les ports et les services non utilisés, restreignez l'accès SNMP avec une authentification solide, mettez en place des VLAN pour la segmentation du réseau, utilisez l'authentification basée sur le port comme le 802.1X, activez le suivi DHCP, utilisez DAI et IP Source Guard pour prévenir les attaques de spoofing d'adresse, contrôlez l'accès à la gestion, sécurisez l'accès physique, etc (**Liste non exhaustive**)

8. Sécurisation avec Firewalls : Configuration des paramètres de base du pare-feu

- Configurez vos firewalls ASA pour séparer les segments de réseau interne et DMZ et externe. Créez des listes de contrôle d'accès (ACL) pour contrôler le flux de trafic. Testez le pare-feu en simulant divers scénarios d'attaque et en vous assurant que seul le trafic autorisé est autorisé selon les exigences de l'entreprise.

9. Configuration Site-to-Site IPsec VPN

- L'entreprise a une annexe distante qui a accès aux ressources de l'entreprise internet via VPN. Configurez un VPN d'accès distant pour offrir un accès sécurisé aux employés au réseau d'entreprise. Mettez en place un VPN site à site en utilisant IPsec pour sécuriser les connexions entre deux succursales.

10. Points d'Accès Wi-Fi :

- Discutez de la possibilité pour l'entreprise d'installer des points d'accès Wi-Fi dans les bâtiments. Si oui, mettez en place un réseau sans fil sécurisé avec le chiffrement WPA2. Configurez le filtrage MAC, les VLAN et d'autres mesures de sécurité.

11. Evolutivité de l'architecture :

- Comment allez-vous planifier la croissance future de l'entreprise, en termes d'ajout de nouveaux départements, de serveurs, etc. ? Comment cela affectera-t-il la conception du réseau et les performances ?

12. Simulation avec Packet Tracer :

- Créez des simulations réseau en utilisant Packet Tracer pour représenter votre conception. Fournissez des adresses IP pour deux équipements par sous-réseau pour simplifier les schémas. Assurez-vous que l'ensemble des réponses précédentes est cohérent dans les simulations.

13. Documentation du Rapport :

- Assurez-vous que toutes les étapes, configurations, explications et captures d'écran sont documentées dans le rapport final. **Le document à rendre ne doit pas dépasser 10 pages**. Une synthèse et analyse du travail sont les critères de notation du rapport.

Projet 3 : WebWeave

Présentation de l'entreprise : Votre boite est engagée pour concevoir l'infrastructure réseau d'une entreprise « WebWeave » spécialisée dans le développement web.

WebWeave a 5 départements à savoir IT, développeurs, finance, RH et administration et dispose d'un parc de 8 serveurs, à savoir Web, email, RH, fichier, AD, DHCP, DNS, Base de données.

WebWeave dispose d'une connexion Internet commune aux différents services.

Disposition des bâtiments :
Récemment, WebWeave a acquis deux immeubles :

- Le premier bâtiment a le parc de serveurs au premier étage, la moitié du IT au deuxième étage et la moitié des développeurs.
- Dans le second bâtiment :
    - Au premier étage vous trouvez le reste des développeurs et l'IT
    - Au deuxième étage, vous trouvez le département RH et ½ Finance
    - Au troisième étage, vous trouvez 1/2 Finance et administration

Exigence :
L'entreprise a des exigences spécifiques pour l'infrastructure réseau :

- **Département IT :** Le service IT communique avec les développeurs et peut accéder au parc des serveurs et à Internet.
- **Département développeurs :** Le service communique avec IT et peut accéder aux serveurs Web, email, fichier, Base de données.
- **Département administration** : L'administration communique avec RH et peut accéder à Interne. Il peut accéder aux serveurs Web, email, fichier.
- **Département finance :** ne peut communiquer avec personne mais peut accéder à Internet. Il peut accéder aux serveurs email et fichier
- **Département RH** : les RH ne peuvent communiquer qu'avec l'administration mais ne peuvent pas accéder à Internet. Ils peuvent accéder aux serveur email, fichier et RH
- Les serveurs doivent être dans une DMZ
- Tous les serveurs doivent être accessibles au service IT
- Les serveurs Web et email doivent être accessibles depuis internet
- **Seuls IT et départements des développeurs auront des PCs portables.**
- L'entreprise dispose de 19 téléphones IP.
- L'adresse IP doit être de la plage 10.0.0.0/20 où le personnel de WebWeave est divisé comme suit : IT : 39, développeurs : 546, Finance : 112, HR : 116 et Administration : 15.

Travail demandé :

1. Architecture du Réseau LAN :

- **Architecture Globale :** Proposez une vue d'ensemble de la structure du réseau LAN en identifiant les principaux composants et leur emplacement dans le bâtiment.
- **Architecture Détaillée :** Fournissez une vue plus détaillée de chaque étage, y compris les connexions entre les départements et les équipements nécessaires.

2. Équipement Réseau Requis :

- Spécifiez le type d'équipement réseau (routeurs, commutateurs, pare-feux, etc.) nécessaires pour répondre aux exigences de l'entreprise.

3. Coût de la Conception :

- Estimez les coûts de mise en œuvre de la conception, y compris les serveurs, ordinateurs portables, composants réseau, téléphones IP, etc., en expliquant vos choix d'équipement (vous pouvez ignorer le cout du câblage).

4. Schéma d'Adressage IP :

- Proposez un schéma d'adressage IP pour l'entreprise, en précisant la méthode choisie (par classes, par bloc, VLSM, etc.) et en justifiant votre choix. Fournissez des détails sur les adresses réseau, les masques de sous-réseau, les plages d'adresses d'hôtes et les adresses de diffusion.

5. Politique de sécurité :

- La société vous demande de créer **Politique de Sécurité des Systèmes d'Information (PSSI)** et une politique de sécurité réseau (Network Equipment Security Guidelines) qui définit les principes, les procédures et les lignes directrices à suivre pour appliquer, gérer, surveiller et maintenir la sécurité d'un réseau informatique de l'entreprise.

6. Segmentation du Réseau et Routage :

- Mettez en place une segmentation de réseau et implémenter un routage (statique ou dynamique) pour interconnecter le réseau de l'entreprise.

7. Sécurisation du Réseau : Mettez en place un plan détaillé pour sécuriser le réseau.

- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut pour des mots de passe forts et uniques, et appliquez des politiques de mots de passe robustes. Mettez en place des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau et restreindre l'accès non autorisé. Désactivez les services inutiles et utilisez le protocole Secure Shell (SSH) pour la gestion à distance. Configurez la journalisation et l'audit pour surveiller les événements de sécurité. Sécurisez l'accès physique au routeur et activez le démarrage sécurisé pour protéger le micrologiciel et les configurations. Utilisez le protocole Network Time Protocol (NTP) pour une horloge précise et configurez le système de journalisation syslog pour stocker les journaux sur des serveurs distants. Désactivez les interfaces et protocoles inutilisés, comme le protocole de découverte Cisco (CDP). (**Liste non exhaustive**)
- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut, sécurisez les interfaces de gestion, configurez les accès SSH, configurez Port Security, désactivez les ports et les services non utilisés, restreignez l'accès SNMP avec une authentification solide, mettez en place des VLAN pour la segmentation du réseau, utilisez l'authentification basée sur le port comme le 802.1X, activez le suivi DHCP, utilisez DAI et IP Source Guard pour prévenir les attaques de spoofing d'adresse, contrôlez l'accès à la gestion, sécurisez l'accès physique, etc (**Liste non exhaustive**)

8. Sécurisation avec Firewalls : Configuration des paramètres de base du pare-feu

- Configurez vos firewalls ASA pour séparer les segments de réseau interne et DMZ et externe. Créez des listes de contrôle d'accès (ACL) pour contrôler le flux de trafic. Testez le pare-feu en simulant divers scénarios d'attaque et en vous assurant que seul le trafic autorisé est autorisé selon les exigences de l'entreprise.

9. Configuration Site-to-Site IPsec VPN

- L'entreprise a une annexe distante qui accès aux ressources de l'entreprise internet via VPN. Configurez un VPN d'accès distant pour offrir un accès sécurisé aux employés au réseau d'entreprise. Mettez en place un VPN site à site en utilisant IPsec pour sécuriser les connexions entre deux succursales.

10. Points d'Accès Wi-Fi :

- Discutez de la possibilité pour l'entreprise d'installer des points d'accès Wi-Fi dans les bâtiments. Si oui, mettez en place un réseau sans fil sécurisé avec le chiffrement WPA2. Configurez le filtrage MAC, les VLAN et d'autres mesures de sécurité.

11. Evolutivité de l'architecture :

- Comment allez-vous planifier la croissance future de l'entreprise, en termes d'ajout de nouveaux départements, de serveurs, etc. ? Comment cela affectera-t-il la conception du réseau et les performances ?

12. Simulation avec Packet Tracer :

- Créez des simulations réseau en utilisant Packet Tracer pour représenter votre conception. Fournissez des adresses IP pour deux équipements par sous-réseau pour simplifier les schémas. Assurez-vous que l'ensemble des réponses précédentes est cohérent dans les simulations.

13. Documentation du Rapport :

- Assurez-vous que toutes les étapes, configurations, explications et captures d'écran sont documentées dans le rapport final. **Le document à rendre ne doit pas dépasser 10 pages**. Une synthèse et analyse du travail sont les critères de notation du rapport.

Projet 4 : WebSolutions

Présentation de l'entreprise : Votre société est engagée pour concevoir l'infrastructure réseau d'une petite entreprise, "WebSolutions", spécialisée dans le développement web. WebSolutions compte 5 départements, à savoir IT, développeurs, marketing, RH et administration, et dispose d'une ferme de 6 serveurs, à savoir, AD, Web, DHCP, Email, RH, base de données.

WebSolutions dispose également d'une connexion Internet qui est partagée par les différents départements.

Disposition des bâtiments :
WebSolutions a acquis deux bâtiments :

- Le premier bâtiment abrite la ferme de serveurs au premier étage et la moitié du département IT au deuxième étage et la moitié des développeurs aux troisième étage
- Dans le second bâtiment :
  - Au premier étage se trouvent les RH et le reste de IT
  - Au deuxième étage, vous trouverez le reste des développeurs et le marketing.
  - Au troisième étage, vous trouverez le marketing et l'administration.

Exigence :
L'entreprise a des exigences spécifiques pour l'infrastructure réseau :

- **Département IT :** Le service IT communique avec les développeurs et peut accéder au parc des serveurs et à Internet.
- **Département développeurs :** communique avec IT et marketing et peut accéder à Internet. Il peut accéder aux serveurs, web, email, base de données
- **Département administration** : L'administration communique avec marketing et peut accéder à Internet. Il peut accéder au serveur email
- **Département marketing** : ils peuvent communiquer avec développeurs et administration et ne peuvent pas accéder à Internet. Il peut accéder au serveur email
- **Département RH** : ne peut communiquer qu'avec l'administration et peut accéder à Internet. Il peut accéder au serveur RH
- Les serveurs doivent être dans une DMZ
- Tous les serveurs doivent être accessibles au service IT
- Les serveurs Web et email doivent être accessibles depuis internet
- **Seuls IT et développeurs auront des PCs portables.**
- Chaque bâtiment dispose de 9 téléphones IP.
- Le personnel se répartit comme suit : IT: 110, Développeurs : 923 Marketing: 62, RH: 45, and administration: 11. L'adresse IP dont dispose WebSolutions est 192.168.208.0/20

Travail demandé :

1. Architecture du Réseau LAN :

- **Architecture Globale :** Proposez une vue d'ensemble de la structure du réseau LAN en identifiant les principaux composants et leur emplacement dans le bâtiment.
- **Architecture Détaillée :** Fournissez une vue plus détaillée de chaque étage, y compris les connexions entre les départements et les équipements nécessaires.

2. Équipement Réseau Requis :

- Spécifiez le type d'équipement réseau (routeurs, commutateurs, pare-feux, etc.) nécessaires pour répondre aux exigences de l'entreprise.

3. Coût de la Conception :

- Estimez les coûts de mise en œuvre de la conception, y compris les serveurs, ordinateurs portables, composants réseau, téléphones IP, etc., en expliquant vos choix d'équipement (vous pouvez ignorer le cout du câblage).

4. Schéma d'Adressage IP :

- Proposez un schéma d'adressage IP pour l'entreprise, en précisant la méthode choisie (par classes, par bloc, VLSM, etc.) et en justifiant votre choix. Fournissez des détails sur les adresses réseau, les masques de sous-réseau, les plages d'adresses d'hôtes et les adresses de diffusion.

5. Politique de sécurité :

- La société vous demande de créer **Politique de Sécurité des Systèmes d'Information (PSSI)** et une politique de sécurité réseau (Network Equipment Security Guidelines) qui définit les principes, les procédures et les lignes directrices à suivre pour appliquer, gérer, surveiller et maintenir la sécurité d'un réseau informatique de l'entreprise.

6. Segmentation du Réseau et Routage :

- Mettez en place une segmentation de réseau et implémenter un routage (statique ou dynamique) pour interconnecter le réseau de l'entreprise.

7. Sécurisation du Réseau : Mettez en place un plan détaillé pour sécuriser le réseau.

- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut pour des mots de passe forts et uniques, et appliquez des politiques de mots de passe robustes. Mettez en place des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau et restreindre l'accès non autorisé. Désactivez les services inutiles et utilisez le protocole Secure Shell (SSH) pour la gestion à distance. Configurez la journalisation et l'audit pour surveiller les événements de sécurité. Sécurisez l'accès physique au routeur et activez le démarrage sécurisé pour protéger le micrologiciel et les configurations. Utilisez le protocole Network Time Protocol (NTP) pour une horloge précise et configurez le système de journalisation syslog pour stocker les journaux sur des serveurs distants. Désactivez les interfaces et protocoles inutilisés, comme le protocole de découverte Cisco (CDP). (**Liste non exhaustive**)
- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut, sécurisez les interfaces de gestion, configurez les accès SSH, configurez Port Security, désactivez les ports et les services non utilisés, restreignez l'accès SNMP avec une authentification solide, mettez en place des VLAN pour la segmentation du réseau, utilisez l'authentification basée sur le port comme le 802.1X, activez le suivi DHCP, utilisez DAI et IP Source Guard pour prévenir les attaques de spoofing d'adresse, contrôlez l'accès à la gestion, sécurisez l'accès physique, etc (**Liste non exhaustive**)

8. Sécurisation avec Firewalls : Configuration des paramètres de base du pare-feu

- Configurez vos firewalls ASA pour séparer les segments de réseau interne et DMZ et externe. Créez des listes de contrôle d'accès (ACL) pour contrôler le flux de trafic. Testez le pare-feu en simulant divers scénarios d'attaque et en vous assurant que seul le trafic autorisé est autorisé selon les exigences de l'entreprise.

9. Configuration Site-to-Site IPsec VPN

- L'entreprise a une annexe distante qui a accès aux ressources de l'entreprise internet via VPN. Configurez un VPN d'accès distant pour offrir un accès sécurisé aux employés au réseau d'entreprise. Mettez en place un VPN site à site en utilisant IPsec pour sécuriser les connexions entre deux succursales.

10. Points d'Accès Wi-Fi :

- Discutez de la possibilité pour l'entreprise d'installer des points d'accès Wi-Fi dans les bâtiments. Si oui, mettez en place un réseau sans fil sécurisé avec le chiffrement WPA2. Configurez le filtrage MAC, les VLAN et d'autres mesures de sécurité.

11. Evolutivité de l'architecture :

- Comment allez-vous planifier la croissance future de l'entreprise, en termes d'ajout de nouveaux départements, de serveurs, etc. ? Comment cela affectera-t-il la conception du réseau et les performances ?

12. Simulation avec Packet Tracer :

- Créez des simulations réseau en utilisant Packet Tracer pour représenter votre conception. Fournissez des adresses IP pour deux équipements par sous-réseau pour simplifier les schémas. Assurez-vous que l'ensemble des réponses précédentes est cohérent dans les simulations.

13. Documentation du Rapport :

- Assurez-vous que toutes les étapes, configurations, explications et captures d'écran sont documentées dans le rapport final. **Le document à rendre ne doit pas dépasser 10 pages**. Une synthèse et analyse du travail sont les critères de notation du rapport.

Projet 5 : WCare

Présentation de l'entreprise : Votre entreprise est engagée pour concevoir l'infrastructure réseau de l'entreprise "WCare" spécialisée dans le conseil et les services informatiques.

WCare compte 6 départements à savoir, IT, Ingénieurs, RH, comptabilité, vendeurs et administration et il dispose d'une batterie de serveurs de 8 serveurs, à savoir, web, email, RH, fichier, DHCP, DNS, Base de données et AD. L'entreprise dispose d'une connexion Internet commune aux différents services.

Disposition des bâtiments :
Récemment, WCare a acquis trois immeubles :

- Le premier bâtiment a le parc de serveurs au premier étage, la moitié du service IT au deuxième étage et la moitié du service ingénieurs.
- Le deuxième bâtiment abrite le reste du service IT au premier étage et moitié des ingénieurs au deuxième étage.
- Le troisième bâtiment a le département des vendeurs au premier étage et RH. Au deuxième étage on trouve les comptables et l'administration.

Exigence :
L'entreprise a des exigences spécifiques pour l'infrastructure réseau :

- **Département IT :** Le service IT communique avec les ingénieurs et peut accéder au parc des serveurs et à Internet.
- **Département ingénieurs :** Le service communique avec IT et vendeurs et peut accéder à Internet. Il a accès aux web, email, base de données
- **Département administration** : L'administration communique avec RH et vendeurs et peut accéder à Internet. Il a accès au fichier et email
- **Département vendeurs** : ils peuvent communiquer avec les ingénieurs et administration et peuvent accéder à Internet. Il a accès à web, email, fichier
- **Département comptabilité :** ne peut communiquer avec personne mais peut accéder à Internet. Il a accès au serveur fichier
- **Département RH** : les RH ne peuvent communiquer qu'avec l'administration et ne peuvent pas accéder à Internet. Il a accès à RH
- Les serveurs doivent être dans une DMZ
- Tous les serveurs doivent être accessibles au service IT
- Les serveurs Web et email doivent être accessibles depuis internet
- **Seuls IT et départements des ingénieurs auront des PCs portables.**
- L'entreprise dispose de 17 téléphones IP.
- L'adresse IP de l'entreprise est 10.72.72.0/21 où le personnel est divisé comme suit : IT : 198, Ingénieurs : 254, RH : 23, Comptables : 18, Vendeurs : 72, et Administration : 12.

Travail demandé :

1. Architecture du Réseau LAN :

- **Architecture Globale :** Proposez une vue d'ensemble de la structure du réseau LAN en identifiant les principaux composants et leur emplacement dans le bâtiment.

- **Architecture Détaillée :** Fournissez une vue plus détaillée de chaque étage, y compris les connexions entre les départements et les équipements nécessaires.

2. Équipement Réseau Requis :

- Spécifiez le type d'équipement réseau (routeurs, commutateurs, pare-feux, etc.) nécessaires pour répondre aux exigences de l'entreprise.

3. Coût de la Conception :

- Estimez les coûts de mise en œuvre de la conception, y compris les serveurs, ordinateurs portables, composants réseau, téléphones IP, etc., en expliquant vos choix d'équipement (vous pouvez ignorer le cout du câblage).

4. Schéma d'Adressage IP :

- Proposez un schéma d'adressage IP pour l'entreprise, en précisant la méthode choisie (par classes, par bloc, VLSM, etc.) et en justifiant votre choix. Fournissez des détails sur les adresses réseau, les masques de sous-réseau, les plages d'adresses d'hôtes et les adresses de diffusion.

5. Politique de sécurité :

- La société vous demande de créer **Politique de Sécurité des Systèmes d'Information (PSSI)** et une politique de sécurité réseau (Network Equipment Security Guidelines) qui définit les principes, les procédures et les lignes directrices à suivre pour appliquer, gérer, surveiller et maintenir la sécurité d'un réseau informatique de l'entreprise.

6. Segmentation du Réseau et Routage :

- Mettez en place une segmentation de réseau et implémenter un routage (statique ou dynamique) pour interconnecter le réseau de l'entreprise.

7. Sécurisation du Réseau : Mettez en place un plan détaillé pour sécuriser le réseau.

- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut pour des mots de passe forts et uniques, et appliquez des politiques de mots de passe robustes. Mettez en place des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau et restreindre l'accès non autorisé. Désactivez les services inutiles et utilisez le protocole Secure Shell (SSH) pour la gestion à distance. Configurez la journalisation et l'audit pour surveiller les événements de sécurité. Sécurisez l'accès physique au routeur et activez le démarrage sécurisé pour protéger le micrologiciel et les configurations. Utilisez le protocole Network Time Protocol (NTP) pour une horloge précise et configurez le système de journalisation syslog pour stocker les journaux sur des serveurs distants. Désactivez les interfaces et protocoles inutilisés, comme le protocole de découverte Cisco (CDP). (**Liste non exhaustive**)
- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut, sécurisez les interfaces de gestion, configurez les accès SSH, configurez Port Security, désactivez les ports et les services non utilisés, restreignez l'accès SNMP avec une authentification solide, mettez en place des VLAN pour la segmentation du réseau, utilisez l'authentification basée sur le port comme le 802.1X, activez

le suivi DHCP, utilisez DAI et IP Source Guard pour prévenir les attaques de spoofing d'adresse, contrôlez l'accès à la gestion, sécurisez l'accès physique, etc (**Liste non exhaustive**)

8. Sécurisation avec Firewalls : Configuration des paramètres de base du pare-feu

- Configurez vos firewalls ASA pour séparer les segments de réseau interne et DMZ et externe. Créez des listes de contrôle d'accès (ACL) pour contrôler le flux de trafic. Testez le pare-feu en simulant divers scénarios d'attaque et en vous assurant que seul le trafic autorisé est autorisé selon les exigences de l'entreprise.

9. Configuration Site-to-Site IPsec VPN

- L'entreprise a une annexe distante qui a accès aux ressources de l'entreprise internet via VPN. Configurez un VPN d'accès distant pour offrir un accès sécurisé aux employés au réseau d'entreprise. Mettez en place un VPN site à site en utilisant IPsec pour sécuriser les connexions entre deux succursales.

10. Points d'Accès Wi-Fi :

- Discutez de la possibilité pour l'entreprise d'installer des points d'accès Wi-Fi dans les bâtiments. Si oui, mettez en place un réseau sans fil sécurisé avec le chiffrement WPA2. Configurez le filtrage MAC, les VLAN et d'autres mesures de sécurité.

11. Evolutivité de l'architecture :

- Comment allez-vous planifier la croissance future de l'entreprise, en termes d'ajout de nouveaux départements, de serveurs, etc. ? Comment cela affectera-t-il la conception du réseau et les performances ?

12. Simulation avec Packet Tracer :

- Créez des simulations réseau en utilisant Packet Tracer pour représenter votre conception. Fournissez des adresses IP pour deux équipements par sous-réseau pour simplifier les schémas. Assurez-vous que l'ensemble des réponses précédentes est cohérent dans les simulations.

13. Documentation du Rapport :

- Assurez-vous que toutes les étapes, configurations, explications et captures d'écran sont documentées dans le rapport final. **Le document à rendre ne doit pas dépasser 10 pages**. Une synthèse et analyse du travail sont les critères de notation du rapport.

Projet 6 : Univel

Présentation de l'entreprise : Votre société est chargée de concevoir l'infrastructure réseau de l'université "Univel". Univel compte 5 départements, à savoir les RH, l'informatique, la recherche, les professeurs et les étudiants, et dispose d'une ferme de 6 serveurs, à savoir, AD, Web, DHCP, Email, RH, Fichier.

Univel dispose également d'une connexion Internet partagée par les différents départements.

Disposition des bâtiments :
Univel possède deux campus :

- Le premier bâtiment abrite la ferme de serveurs au premier étage et la moitié du département informatique. Au deuxième étage, il y a les salles de classe des étudiants et au troisième étage les RH.
- Dans le deuxième bâtiment :
  - Au premier étage, on trouve le reste de l'informatique et la recherche
  - Au deuxième étage, vous trouverez les bureaux des professeurs et les salles de classe des étudiants.
  - Au troisième étage, vous trouverez les bureaux des professeurs et les salles de classe des étudiants.

Exigence :
L'entreprise a des exigences spécifiques pour l'infrastructure réseau :

- **Département informatique :** communique avec les étudiants et professeurs et peut accéder au parc des serveurs et à Internet.
- **Département professeurs :** communique avec informatique et étudiants et recherche et peut accéder à Internet. Ils ont accès aux serveur email et fichier
- **Les étudiants** : ils peuvent communiquer avec l'informatique et les professeurs et peuvent accéder à Internet. Ils ont accès aux emails
- **Département RH :** ne peut communiquer avec personne mais peut accéder à Internet. Ils ont accès aux serveurs RH et fichier
- **Département Recherche** : ne peut communiquer qu'avec les professeurs et ne peut pas accéder à Internet. Ils ont accès aux serveurs email, fichier
- Les serveurs doivent être dans une DMZ
- Tous les serveurs doivent être accessibles au service informatique
- Les serveurs Web et email doivent être accessibles depuis internet
- **Seuls recherche et professeurs auront des PCs portables.**
- L'université dispose de 20 téléphones IP.
- L'adresse IP doit être comprise entre 172.17.64.0/20 avec un nombre de postes réparti comme suit : informatique : 33, professeurs : 172, RH : 65, Recherche : 32 et étudiants : 874

Travail demandé :

1. Architecture du Réseau LAN :

- **Architecture Globale :** Proposez une vue d'ensemble de la structure du réseau LAN en identifiant les principaux composants et leur emplacement dans le bâtiment.
- **Architecture Détaillée :** Fournissez une vue plus détaillée de chaque étage, y compris les connexions entre les départements et les équipements nécessaires.

2. Équipement Réseau Requis :

- Spécifiez le type d'équipement réseau (routeurs, commutateurs, pare-feux, etc.) nécessaires pour répondre aux exigences de l'université.

3. Coût de la Conception :

- Estimez les coûts de mise en œuvre de la conception, y compris les serveurs, ordinateurs portables, composants réseau, téléphones IP, etc., en expliquant vos choix d'équipement (vous pouvez ignorer le cout du câblage).

4. Schéma d'Adressage IP :

- Proposez un schéma d'adressage IP pour l'université, en précisant la méthode choisie (par classes, par bloc, VLSM, etc.) et en justifiant votre choix. Fournissez des détails sur les adresses réseau, les masques de sous-réseau, les plages d'adresses d'hôtes et les adresses de diffusion.

5. Politique de sécurité :

- L'université vous demande de créer **Politique de Sécurité des Systèmes d'Information (PSSI)** et une politique de sécurité réseau (Network Equipment Security Guidelines) qui définit les principes, les procédures et les lignes directrices à suivre pour appliquer, gérer, surveiller et maintenir la sécurité d'un réseau informatique de l'université.

6. Segmentation du Réseau et Routage :

- Mettez en place une segmentation de réseau et implémenter un routage (statique ou dynamique) pour interconnecter le réseau de l'université.

7. Sécurisation du Réseau : Mettez en place un plan détaillé pour sécuriser le réseau.

- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut pour des mots de passe forts et uniques, et appliquez des politiques de mots de passe robustes. Mettez en place des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau et restreindre l'accès non autorisé. Désactivez les services inutiles et utilisez le protocole Secure Shell (SSH) pour la gestion à distance. Configurez la journalisation et l'audit pour surveiller les événements de sécurité. Sécurisez l'accès physique au routeur et activez le démarrage sécurisé pour protéger le micrologiciel et les configurations. Utilisez le protocole Network Time Protocol (NTP) pour une horloge précise et configurez le système de journalisation syslog pour stocker les journaux sur des serveurs distants. Désactivez les interfaces et protocoles inutilisés, comme le protocole de découverte Cisco (CDP). (**Liste non exhaustive**)
- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut, sécurisez les interfaces de gestion, configurez les accès SSH, configurez Port Security, désactivez les ports et les services non utilisés, restreignez l'accès SNMP avec une authentification solide, mettez en place des VLAN pour la segmentation du réseau, utilisez l'authentification basée sur le port comme le 802.1X, activez le suivi DHCP, utilisez DAI et IP Source Guard pour prévenir les attaques de spoofing d'adresse, contrôlez l'accès à la gestion, sécurisez l'accès physique, etc (**Liste non exhaustive**)

8. Sécurisation avec Firewalls : Configuration des paramètres de base du pare-feu

- Configurez vos firewalls ASA pour séparer les segments de réseau interne et DMZ et externe. Créez des listes de contrôle d'accès (ACL) pour contrôler le flux de trafic. Testez le pare-feu en simulant divers scénarios d'attaque et en vous assurant que seul le trafic autorisé est autorisé selon les exigences de l'entreprise.

9. Configuration Site-to-Site IPsec VPN

- L'université a une annexe distante qui a accès aux ressources de l'entreprise internet via VPN. Configurez un VPN d'accès distant pour offrir un accès sécurisé aux employés au réseau d'entreprise. Mettez en place un VPN site à site en utilisant IPsec pour sécuriser les connexions entre deux succursales.

10. Points d'Accès Wi-Fi :

- Discutez de la possibilité pour l'université d'installer des points d'accès Wi-Fi dans les bâtiments. Si oui, mettez en place un réseau sans fil sécurisé avec le chiffrement WPA2. Configurez le filtrage MAC, les VLAN et d'autres mesures de sécurité.

11. Evolutivité de l'architecture :

- Comment allez-vous planifier la croissance future de l'université, en termes d'ajout de nouveaux départements, de serveurs, etc. ? Comment cela affectera-t-il la conception du réseau et les performances ?

12. Simulation avec Packet Tracer :

- Créez des simulations réseau en utilisant Packet Tracer pour représenter votre conception. Fournissez des adresses IP pour deux équipements par sous-réseau pour simplifier les schémas. Assurez-vous que l'ensemble des réponses précédentes est cohérent dans les simulations.

13. Documentation du Rapport :

- Assurez-vous que toutes les étapes, configurations, explications et captures d'écran sont documentées dans le rapport final. **Le document à rendre ne doit pas dépasser 10 pages**. Une synthèse et analyse du travail sont les critères de notation du rapport.

Project 7 : Summit Institute

Présentation de l'entreprise : Votre entreprise est engagée pour concevoir l'infrastructure réseau de l'université "Summit Institute" qui compte 6 départements, à savoir l'administration, IT, R&D, Professeurs et étudiants, et RH.

L'université dispose d'un parc de 6 serveurs, à savoir, AD, Web, DHCP, Email, RH, Fichier.

Summit Institute dispose également d'une connexion Internet commune aux différents services.

Disposition des bâtiments :
Summit Institute a un campus de deux bâtiments :

- Le premier campus abrite au premier étage le parc de serveurs et la moitié du service IT. Au deuxième étage, il y a la moitié des bureaux des professeurs et les salles de classe des étudiants, et le troisième étage il y a l'administration.
- Dans le deuxième bâtiment :
  - Au premier étage, vous trouverez le reste de IT, R&D, le reste des bureaux des professeurs
  - Au deuxième étage, vous trouvez les salles de classe des étudiants.
  - Au troisième étage, vous trouvez RH et les salles de classe des étudiants.

Exigence :
L'entreprise a des exigences spécifiques pour l'infrastructure réseau :

- **Département IT :** Le service IT communique avec l'administration et peut accéder au parc des serveurs et à Internet.
- **Département Professeur :** Le service communique avec les étudiants et peut accéder à Internet. Ils ont accès aux serveurs fichier et email
- **Département administration** : L'administration communique avec IT et RH et peut accéder à Internet. Ils ont accès aux serveur web et email,
- **Les étudiants** : ils peuvent communiquer avec les professeurs et peuvent accéder à Internet. Ils ont accès aux emails
- **Département R&D :** ne peut communiquer avec personne mais peut accéder à Internet. Ils ont accès aux serveurs email et fichier
- **Département RH** : les RH ne peuvent communiquer qu'avec l'administration et ne peuvent pas accéder à Internet. Ils ont accès aux serveurs RH
- Les serveurs doivent être dans une DMZ
- Tous les serveurs doivent être accessibles au service IT
- Les serveurs Web et email doivent être accessibles depuis internet
- **Seuls IT et les professeurs auront des PCs portables.**
- Summit Institute dispose de 11 téléphones IP.
- Le personnel de l'université est réparti comme suit : IT : 66, Professeurs : 33, administration : 150, R&D : 13, RH : 5 et étudiants : 1350. L'adresse IP doit être comprise entre 10.1.32.0/20

Travail demandé :

1. Architecture du Réseau LAN :

- **Architecture Globale :** Proposez une vue d'ensemble de la structure du réseau LAN en identifiant les principaux composants et leur emplacement dans le bâtiment.

- **Architecture Détaillée :** Fournissez une vue plus détaillée de chaque étage, y compris les connexions entre les départements et les équipements nécessaires.

2. Équipement Réseau Requis :

- Spécifiez le type d'équipement réseau (routeurs, commutateurs, pare-feux, etc.) nécessaires pour répondre aux exigences de Summit Institute.

3. Coût de la Conception :

- Estimez les coûts de mise en œuvre de la conception, y compris les serveurs, ordinateurs portables, composants réseau, téléphones IP, etc., en expliquant vos choix d'équipement (vous pouvez ignorer le cout du câblage).

4. Schéma d'Adressage IP :

- Proposez un schéma d'adressage IP pour Summit Institute, en précisant la méthode choisie (par classes, par bloc, VLSM, etc.) et en justifiant votre choix. Fournissez des détails sur les adresses réseau, les masques de sous-réseau, les plages d'adresses d'hôtes et les adresses de diffusion.

5. Politique de sécurité :

- Summit Institute vous demande de créer **Politique de Sécurité des Systèmes d'Information (PSSI)** et une politique de sécurité réseau (Network Equipment Security Guidelines) qui définit les principes, les procédures et les lignes directrices à suivre pour appliquer, gérer, surveiller et maintenir la sécurité d'un réseau informatique de Summit Institute.

6. Segmentation du Réseau et Routage :

- Mettez en place une segmentation de réseau et implémenter un routage (statique ou dynamique) pour interconnecter le réseau de Summit Institute.

7. Sécurisation du Réseau : Mettez en place un plan détaillé pour sécuriser le réseau.

- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut pour des mots de passe forts et uniques, et appliquez des politiques de mots de passe robustes. Mettez en place des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau et restreindre l'accès non autorisé. Désactivez les services inutiles et utilisez le protocole Secure Shell (SSH) pour la gestion à distance. Configurez la journalisation et l'audit pour surveiller les événements de sécurité. Sécurisez l'accès physique au routeur et activez le démarrage sécurisé pour protéger le micrologiciel et les configurations. Utilisez le protocole Network Time Protocol (NTP) pour une horloge précise et configurez le système de journalisation syslog pour stocker les journaux sur des serveurs distants. Désactivez les interfaces et protocoles inutilisés, comme le protocole de découverte Cisco (CDP). (**Liste non exhaustive**)
- Mettre en œuvre les meilleures pratiques de sécurité pour le durcissement des routeurs : changez les mots de passe par défaut, sécurisez les interfaces de gestion, configurez les accès SSH, configurez Port Security, désactivez les ports et les services non utilisés, restreignez l'accès SNMP avec une authentification solide, mettez en place des VLAN pour la segmentation du réseau, utilisez l'authentification basée sur le port comme le 802.1X, activez

le suivi DHCP, utilisez DAI et IP Source Guard pour prévenir les attaques de spoofing d'adresse, contrôlez l'accès à la gestion, sécurisez l'accès physique, etc (**Liste non exhaustive**)

8. Sécurisation avec Firewalls : Configuration des paramètres de base du pare-feu

- Configurez vos firewalls ASA pour séparer les segments de réseau interne et DMZ et externe. Créez des listes de contrôle d'accès (ACL) pour contrôler le flux de trafic. Testez le pare-feu en simulant divers scénarios d'attaque et en vous assurant que seul le trafic autorisé est autorisé selon les exigences de l'entreprise.

9. Configuration Site-to-Site IPsec VPN

- Summit Institute a une annexe distante qui a accès aux ressources de l'entreprise internet via VPN. Configurez un VPN d'accès distant pour offrir un accès sécurisé aux employés au réseau d'entreprise. Mettez en place un VPN site à site en utilisant IPsec pour sécuriser les connexions entre deux succursales.

10. Points d'Accès Wi-Fi :

- Discutez de la possibilité pour l'entreprise d'installer des points d'accès Wi-Fi dans les bâtiments. Si oui, mettez en place un réseau sans fil sécurisé avec le chiffrement WPA2. Configurez le filtrage MAC, les VLAN et d'autres mesures de sécurité.

11. Evolutivité de l'architecture :

- Comment allez-vous planifier la croissance future de l'entreprise, en termes d'ajout de nouveaux départements, de serveurs, etc. ? Comment cela affectera-t-il la conception du réseau et les performances ?

12. Simulation avec Packet Tracer :

- Créez des simulations réseau en utilisant Packet Tracer pour représenter votre conception. Fournissez des adresses IP pour deux équipements par sous-réseau pour simplifier les schémas. Assurez-vous que l'ensemble des réponses précédentes est cohérent dans les simulations.

13. Documentation du Rapport :

- Assurez-vous que toutes les étapes, configurations, explications et captures d'écran sont documentées dans le rapport final. **Le document à rendre ne doit pas dépasser 10 pages**. Une synthèse et analyse du travail sont les critères de notation du rapport.