Gestion de la Sécurité du Réseau

1. Architecture de Sécurité :

A) Pare-feu et IPS

- Pare-feu Cisco ASA en entrée du réseau pour filtrer le trafic entrant et sortant.
- IPS Cisco juste après le pare-feu pour détecter et bloquer les menaces en temps réel.

B) Segmentation du Réseau

- VLANs distincts pour chaque département : Marketing (VLAN 10), Production (VLAN 20), Développement (VLAN 30).
- Deux DMZ : une pour les serveurs de diffusion de films, une autre pour les serveurs de messagerie, web intranet et DNS.

2. ACLs pour les VLANs :

VLAN 10 - Marketing :

- Accès autorisés : Serveur web intranet, serveur de messagerie, serveur de fichiers
- Accès refusés : Serveurs de diffusion de films

VLAN 20 - Production :

- Accès autorisés : Serveurs de diffusion de films, serveur web intranet, serveur de messagerie, serveur de fichiers

VLAN 30 - Développement :

- Accès autorisés : Serveur web intranet, serveur de messagerie, serveur de fichiers, serveur applicatif
- Accès refusés : Serveurs de diffusion de films

3. Politique de Sécurité des Employés :

A) Authentification et Gestion des Accès

- Mots de passe complexes : Minimum 12 caractères, combinaison de lettres, chiffres et caractères spéciaux.
- Authentification à deux facteurs (2FA) pour les systèmes critiques et données sensibles.

- Changement de mot de passe obligatoire tous les 90 jours.
- Principe du moindre privilège (PoLP).

B) Formation et Sensibilisation

- Sessions trimestrielles de formation à la cybersécurité.
- Simulations régulières de phishing.

C) Utilisation Acceptable des Ressources

- Interdiction d'installer des logiciels non autorisés.
- Restriction de l'utilisation des supports de stockage externes.
- Politique de bureau propre : sécurisation des documents sensibles et écrans.

D) Télétravail et Accès à Distance

- Utilisation obligatoire d'un VPN pour l'accès à distance.
- Contrôles d'accès basés sur la localisation et le contexte.

E) Conformité

- Audits réguliers des politiques de sécurité.
- Vérifications des logs.

4. Sécurité des Terminaux :

- Antivirus et anti-malware sur tous les postes de travail.
- Mises à jour régulières des systèmes.

5. Sécurité Wi-Fi :

- Chiffrement WPA3 sur tous les réseaux sans fil.
- Réseaux invités séparés et isolés du réseau interne.

6. Surveillance et Réponse aux Incidents :

- Dispositifs de logs auprès du pare-feu et de l'IPS.
- Monitoring des postes de travail.

7. Gestion des Accès Distants :

- VPN sécurisé pour les accès à distance.
- Authentification multifactorielle obligatoire pour les connexions VPN.

8. Sécurité Physique :

- Contrôle d'accès aux locaux techniques.
- Séparation des zones de travail et des zones de serveurs, notamment pour les DMZ.

9. Audits et Conformité :

- Audits de sécurité réguliers.
- Veille réglementaire pour assurer la conformité aux normes en vigueur.