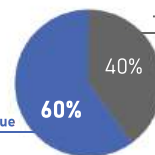




Cybersécurité : Pare-feu UTM & VPN pour PME

5
Jours10
MAX
Places

Public Visé

Techniciens/Ingénieurs IT débutants
Techniciens/Ingénieurs support / helpdesk
Techniciens/Ingénieurs CFA



Pré-requis

Connaissances de base en réseaux : IP / masque, passerelle, VLAN / ping, traceroute
Avoir déjà manipulé un routeur ou un switch



Objectifs Opérationnels

- Comprendre le rôle d'un pare-feu UTM dans une architecture réseau PME (zones, WAN, LAN, DMZ, Wi-Fi invités).
- Choisir et dimensionner un pare-feu UTM adapté à un besoin (débit, nombre d'utilisateurs, services UTM activés).
- Mettre en service un pare-feu UTM.
- Créer et maintenir des politiques de sécurité (NAT, filtrage par adresse, port, service, horaire, utilisateur).
- Segmenter un réseau PME : VLAN, DMZ, zone invités, accès inter-sites.
- Mettre en place des VPN site à site entre deux sites.
- Mettre en place un VPN nomade (accès distant) pour les utilisateurs mobiles.
- Exploiter les fonctions de base d'un UTM : journalisation, filtrage web simple, supervision, sauvegarde de configuration.
- Appliquer des bonnes pratiques de documentation exploitation et dépannage en environnement PME.



Travaux Pratiques

- cartographie d'un réseau PME et identification du positionnement du pare-feu.
- mise en service d'un pare-feu UTM (WAN, LAN, règles de base, NAT) et validation des accès Internet.
- création de VLAN/zones supplémentaires (DMZ, invités) filtrage inter-zones et tests.
- mise en place d'un VPN site à site entre deux sites simulés.
- mise en place d'un VPN nomade, sauvegarde de configuration et gestion de pannes courantes.



Matériels Pédagogiques

- Routeur
- Firewall
- Switch Niveau 3
- Serveur Pfsense
- Support de formation



Attestation

Attestation de formation professionnelle agréé par l'état

