

Mis à jour le 08/10/2026

S'inscrire

Formation Essentiels en matière de sécurité réseau d'Aruba (ANSF)

4 jours (28 heures)

Présentation

HPE Aruba Networking propose des technologies pour protéger les réseaux filaires et sans fil. Avec le renforcement des équipements, les protocoles LAN sécurisés, les mécanismes d'authentification et de chiffrement et la sécurité de l'edge, vous disposez des bases nécessaires pour construire une infrastructure réseau mieux protégée contre les menaces.

Notre formation Essentiels en matière de sécurité réseau d'Aruba (ANSF) vous permettra de consolider vos connaissances pour sécuriser les infrastructures de vos clients ou partenaires. Elle s'adresse aux ingénieurs réseau et techniciens de support disposant de six mois à un an d'expérience en environnements filaires et sans fil.

Vous apprendrez à définir la terminologie de sécurité, à renforcer les commutateurs AOS-CX et les dispositifs AOS, puis à appliquer les mécanismes de protection adaptés aux réseaux LAN, WLAN et WAN.

À l'issue de la formation, vous serez en mesure de relier les menaces aux mesures de protection, de choisir les technologies d'authentification et de chiffrement et de classer les points de terminaison pour adapter les contrôles d'accès.

Cette formation aborde également la détection des menaces et les premières démarches d'analyse forensique. Des ateliers pratiques vous permettront de vérifier les protections et d'exploiter les journaux dans une situation d'investigation.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Définir la terminologie de sécurité
- Renforcer les dispositifs AOS-CX et AOS
- Sécuriser un WLAN et un LAN câblé
- Sécuriser le WAN
- Classer les points de terminaison
- Détecter les menaces et enquêter par analyse forensique

Public visé

- Ingénieur réseau en environnement client
- Ingénieur réseau en environnement partenaire
- Technicien de support réseau

Pré-requis

- Compréhension de base des concepts de réseaux filaires, fortement recommandée
- Compréhension de base des concepts de réseaux sans fil, fortement recommandée
- Compréhension de base des concepts de sécurité, fortement recommandée

Pré-requis techniques

- Ordinateur équipé d'un navigateur web et d'un client SSH pour les accès aux équipements de laboratoire
- Connexion Internet stable autorisant les accès nécessaires à l'environnement pédagogique
- Accès aux équipements AOS-CX et AOS du laboratoire selon les modalités communiquées avant la formation

Programme de notre formation Essentiels en matière de sécurité réseau d'Aruba (ANSF)

[Jour 1 - Matin]

Menaces de sécurité et stratégie de protection

- Terminologie de sécurité : menace, vulnérabilité, risque et attaque
- Principes de confidentialité, intégrité et disponibilité
- Menaces courantes dans les environnements filaires et sans fil
- Construction d'une stratégie de protection fondée sur la défense en profondeur et le moindre privilège
- Atelier pratique : Analyser un scénario d'entreprise, identifier les menaces et associer les mesures de protection adaptées.

[Jour 1 - Après-midi]

Technologies de sécurité réseau

- Fonctions des pare-feu et des listes de contrôle d'accès
- Principes de segmentation réseau et séparation des flux
- Rôles des mécanismes authentification, autorisation et traçabilité
- Protection du WAN par filtrage et tunnels chiffrés
- Place de la détection des menaces et de la journalisation dans une stratégie de sécurité
- Atelier pratique : Définir une politique de filtrage pour des flux LAN et WAN, puis vérifier les communications autorisées et interdites.

[Jour 2 - Matin]

Renforcement des commutateurs AOS-CX

- Surfaces d'exposition des commutateurs AOS-CX et priorités de renforcement
- Gestion des comptes administrateurs, des privilèges et des mots de passe
- Protection des accès de gestion avec SSH, HTTPS et restrictions d'accès
- Sécurisation de la supervision avec SNMPv3 et collecte des journaux
- Réduction des services exposés et protection des plans de gestion et de contrôle
- Atelier pratique : Renforcer un commutateur AOS-CX et vérifier les accès administratifs, les services exposés et les événements journalisés.

[Jour 2 - Après-midi]

Renforcement des dispositifs AOS

- Identification des fonctions sensibles et des accès de gestion des dispositifs AOS
- Protection des comptes administrateurs et limitation des privilèges
- Restriction des accès de gestion et réduction de la surface d'attaque
- Protection des communications de contrôle et des services d'administration
- Configuration de la journalisation pour conserver les événements utiles à une investigation
- Atelier pratique : Appliquer une procédure de renforcement à un dispositif AOS et contrôler les accès ainsi que la remontée des journaux.

[Jour 3 - Matin]

Protocoles LAN sécurisés

- Risques associés aux protocoles de niveau 2 dans un LAN câblé
- Protection contre les serveurs DHCP non autorisés avec DHCP snooping
- Protection contre l'usurpation ARP avec Dynamic ARP Inspection
- Protection de la topologie avec les mécanismes de sécurisation Spanning Tree
- Contrôle des ports et articulation des protections avec la segmentation LAN
- Atelier pratique : Configurer les protections disponibles sur le commutateur de laboratoire et vérifier leur comportement face à des événements DHCP, ARP et Spanning Tree contrôlés.

[Jour 3 - Après-midi]

Authentification et chiffrement réseau

- Fonctionnement de 802.1X et échanges entre client, équipement réseau et serveur RADIUS
- Rôle des méthodes EAP et des certificats dans l'authentification réseau
- Choix des mécanismes de protection WPA2 et WPA3 pour un WLAN
- Application de l'authentification aux accès LAN câblés et sans fil
- Principes des tunnels VPN IPsec pour protéger les communications WAN
- Atelier pratique : Configurer un accès WLAN authentifié, vérifier le chiffrement et analyser les échanges d'authentification réussis ou refusés.

[Jour 4 - Matin]

Sécurité de l'edge et classification des terminaux

- Positionnement des contrôles de sécurité à l'edge avec HPE Aruba Networking
- Association entre identité, rôle et droits d'accès réseau
- Application des politiques de filtrage aux utilisateurs et aux équipements
- Principes de classification des points de terminaison à partir des attributs observés
- Adaptation des contrôles d'accès selon le profil du terminal et son contexte
- Atelier pratique : Classer plusieurs points de terminaison à partir des informations disponibles et vérifier les droits d'accès associés à leurs profils.

[Jour 4 - Après-midi]

Détection des menaces et analyse forensique à l'edge

- Identification des signaux de menace dans les événements réseau et sans fil
- Lecture des alertes et distinction entre événement attendu et activité suspecte
- Collecte et mise en relation des journaux, des identités et des profils de terminaux
- Démarche initiale d'analyse forensique et reconstitution chronologique des événements
- Conservation des éléments observés et formulation des conclusions d'investigation
- Atelier pratique : Enquêter sur un incident simulé à partir de journaux et d'alertes, identifier le terminal concerné et restituer une chronologie argumentée.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son

inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.