

Aruba Network Security – Mise en oeuvre

5 jours (35 heures)

Perfectionnement

Classe à distance

à partir de

3 600 € HT par personne (TVA en vigueur)

Contenu mis à jour le 30/09/2026. Document téléchargé le 06/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Décrire les concepts de sécurité intermédiaires
- Utiliser le portefeuille Aruba pour mettre en oeuvre la ZTS (Zero Trust Security) et protéger leurs réseaux contre les menaces
- Configurer l'infrastructure réseau Aruba et les solutions ClearPass pour authentifier et contrôler les utilisateurs filaires et sans fil, ainsi que les utilisateurs distants sur un VPN client-site
- Collecter une variété d'informations contextuelles sur CPPM (ClearPass Policy Manager)
- Mettre en oeuvre des politiques avancées de mappage des rôles et d'application
- Utiliser ClearPass Device Insight pour améliorer la visibilité
- Configurer des fonctions telles que le NAE (Network Analytics Engine) ArubaOS-CX, le WIDS/WIPS (Wireless Intrusion Detection System/Intrusion Prevention System) Aruba et le système IDS/IPS de la passerelle Aruba, ainsi que les enquêtes sur les alertes.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Ingénieurs réseau responsables de la mise en oeuvre des contrôles de sécurité sur les réseaux d'entreprise.

Prérequis

Avoir suivi la formation ANSF "Aruba Network Security – Les fondamentaux" ou avoir les connaissances équivalentes en matière d'éléments essentiels en sécurité réseau d'Aruba.

Programme

1 Pendant votre formation

Aruba Network Security – Mise en oeuvre

Stratégie de sécurité Aruba et principes fondamentaux de ClearPass

- Expliquer la ZTS (Zero Trust Security) d'Aruba
- Expliquer comment les solutions Aruba s'appliquent aux différents vecteurs de sécurité

Déployer des certificats "trusted" dans les solutions Aruba

- Décrire les dépendances PKI (Public Key Infrastructure)
- Configurer les certificats appropriés et les autorités de certification "trusted root" sur le CPPM (ClearPass Policy Manager)

Mettre en oeuvre la norme 802.1x basée sur des certificats

- Déployer AAA pour les WLAN avec CPPM
- Déployer l'authentification basée sur les certificats pour les utilisateurs et les appareils

Mettre en oeuvre des politiques avancées sur le pare-feu Aruba OS basé sur les rôles

- Déployer AAA pour les WLAN avec CPPM
- Définir et appliquer des politiques avancées de pare-feu

Evaluer les différentes postures des endpoints

Mettre en oeuvre une infrastructure de réseau "trusted"

- Mettre en place une authentification et une autorisation sécurisées des gestionnaires de l'infrastructure réseau, y compris :
 - Autorisation TACACS+ avancée
 - Authentification multi-facteurs
- Protocoles L2 et L3 sécurisés, ainsi que d'autres protocoles tels que SFTP

Implémenter 802.1X et le contrôle d'accès basé sur les rôles d'AOS-CX

- Déployer l'AAA pour les périphériques câblés à l'aide de CPPM, y compris les rôles locaux et téléchargeables

- Expliquer la segmentation dynamique, y compris ses avantages et ses cas d'usage
- Déployer la segmentation dynamique à l'aide du pilotage de VLAN
- Configurer l'authentification 802.1X pour les AP (points d'accès)

Mettre en oeuvre la segmentation dynamique sur des switches AOS-CX

- Expliquer la segmentation dynamique, y compris ses avantages et ses cas d'usage
- Déployer la segmentation dynamique, y compris :
 - UBT (User-Based Tunneling)
 - VNBT (Virtual Network-Based Tunneling)

Surveiller avec NAE (Network Analytics Engine)

- Déployer et utiliser Network Analytics
- Les agents Engine (NAE) pour la surveillance

Mettre en oeuvre le WIDS/WIPS

- Expliquer la technologie WIPS et WIDS d'Aruba
- Configurer la détection et l'atténuation des AP "rogue"

Utiliser le CPPM et l'intégration de tiers pour atténuer les menaces

- Décrire les types et les niveaux de log et utiliser le Ingress Event Engine CPPM pour intégrer des solutions de logging tierces
- Configurer l'intégration entre l'infrastructure Aruba et le CPPM

Mettre en oeuvre le profilage des dispositifs avec CPPM

- Expliquer les avantages et les méthodes de classification des endpoints sur CPPM, y compris les méthodes actives et passives
- Déployer et appliquer la classification des endpoints aux appareils
- Analyser les données de classification des endpoints sur CPPM pour identifier les risques

Introduction à CPDI (ClearPass Device Insight)

- Définir CPDI
- Analyser les données de classification des endpoints sur CPDI

Déployer CPDI

- Définir et déployer CPDI
- Analyser les données de classification des endpoints sur CPDI

Intégrer CPDI à CPPM

- Intégrer CPPM et CPDI
- Atténuer les menaces en utilisant CPDI pour identifier les flux de trafic et appliquer des tags et CPPM pour prendre des mesures basées sur les tags

Utiliser les captures de paquets pour étudier les problèmes de sécurité

- Effectuer des captures de paquets sur l'infrastructure Aruba localement et à l'aide de Central
- Interpréter les captures de paquets

Etablir un accès à distance sécurisé

- Expliquer les concepts VPN
- Comprendre que les solutions SD-WAN d'Aruba automatisent le déploiement de VPN pour le WAN
- Décrire les passerelles Aruba de la série 9x00
- Concevoir et déployer des VPN à distance à l'aide d'Aruba VIA

Configurer l'IDS/IPS de la passerelle Aruba

- Décrire les passerelles de la série Aruba 9x00
- Définir et appliquer des politiques UTM

Utiliser les alertes de Central pour étudier les problèmes de sécurité

- Examiner les alertes de Central
- Recommander des actions basées sur l'analyse des alertes de Central

Certification (en option)

- Prévoir l'achat de la certification en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectue en ligne, et durera en moyenne 1h30

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 23 novembre 2026 au 27 novembre 2026 (5 jours / 35 heures)

À distance

Du 23 novembre 2026 au 27 novembre 2026 À distance

- 23 novembre 2026 9h00 – 15h00
- 24 novembre 2026 9h00 – 15h00
- 25 novembre 2026 9h00 – 15h00
- 26 novembre 2026 9h00 – 15h00
- 27 novembre 2026 9h00 – 15h00