

Firewall – Architecture et déploiement

3 jours (21 heures)

Initiation

Présentiel ou classe à distance

à partir de

2 085 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 03/10/2026.

Objectifs

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

- Décrire les concepts de base et les fonctionnalités des firewalls
- Reconnaître l'architecture de réseau et de sécurité, et le rôle des firewalls dans la protection des réseaux
- Configurer et gérer les firewalls de manière efficace
- Déployer et utiliser pfSense pour la sécurité des réseaux.

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

À qui s'adresse cette formation ?

Professionnels de l'informatique et de la sécurité des réseaux souhaitant acquérir ou approfondir leurs connaissances sur les firewalls.

Prérequis

Avoir des connaissances de base en réseaux et en sécurité informatique, ainsi que de l'expérience de base avec les systèmes d'exploitation Windows et Linux.

Programme

1 Pendant votre formation

Firewall – Architecture et déploiement

Jour 1 – Introduction et concepts fondamentaux

Matin – Introduction aux firewalls et sécurité réseau

- Comprendre le rôle et l'importance des firewalls dans la protection des réseaux
- Vue d'ensemble des différents types de firewalls
 - Stateful
 - Stateless
 - Application-layer...
- Concepts de NAT (Network Address Translation) : types
 - Statique
 - Dynamique
 - PAT
- Introduction à la DMZ (Demilitarized Zone) et utilisation dans une architecture sécurisée
- Comprendre le modèle OSI et les protocoles critiques pour la sécurité réseau

Après-midi – Sécurisation et principes clés

- Les bases des règles de sécurité des firewalls : structure et meilleures pratiques
- Sécurité des couches physiques et liaisons réseau
- Présentation de l'architecture de sécurité de l'ANSSI
- Introduction à l'analyse de protocoles réseau avec Wireshark

Exemples de travaux pratiques (à titre indicatif)

- *Installation de Wireshark et première analyse du trafic réseau pour identifier les protocoles utilisés*

Jour 2 – Configuration et gestion des firewalls

Matin – Firewalls sous Linux et Windows

- Introduction et prise en main d'IPtables / NFtables sous Linux
 - Règles de filtrage
 - Chaînes
 - Tables
- Gestion et configuration des firewalls Windows
 - Définition des règles
 - Stratégies

- Sécurisation avancée des connexions entrantes et sortantes

Exemples de travaux pratiques (à titre indicatif)

- Configuration d'IPtables et implémentation des règles de pare-feu sous Windows

Après-midi – Firewall Cisco ASA

- Présentation du firewall Cisco ASA
 - Fonctionnalités
 - Architecture
 - Scénarios d'utilisation
- Configuration de base du Cisco ASA pour la gestion des trafics (DMZ, LAN, WAN)
- Introduction à l'utilisation des ACL (Access Control Lists) pour le contrôle des accès

Exemples de travaux pratiques (à titre indicatif)

- Installation, configuration et gestion de trafic avec Cisco ASA

Jour 3 – Gestion Unifiée des Menaces (UTM) et sécurité avancée

Matin – Concepts de Gestion Unifiée des Menaces (UTM)

- Qu'est-ce qu'un UTM ? Fonctionnalités essentielles : IPS, IDS, proxy, anti-malware, VPN
- Définition et explication des technologies associées : SIEM, SOC, EDR, XDR, MDR, SOAR
- Concepts de "firewalking" : techniques et applications pour tester la sécurité des firewalls

Après-midi – Mise en pratique avec pfSense

- Installation et configuration avancée de pfSense : gestion des interfaces et des services
- Utilisation de pfSense comme UTM : configuration de l'IPS/IDS, proxy et reverse proxy
- Mise en place d'un VPN sécurisé pour protéger les communications réseau

Exemples de travaux pratiques (à titre indicatif)

- Installation et configuration complète de pfSense
- Implémentation de VPN
- Tests de sécurité avec firewalking

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 7 octobre 2026 au 9 octobre 2026 (3 jours / 21 heures)

Paris La Défense

Du 7 octobre 2026 au 9 octobre 2026

Paris La Défense

- 7 octobre 2026 9h00 – 16h00
- 8 octobre 2026 9h00 – 16h00
- 9 octobre 2026 9h00 – 16h00