

<b>Public</b>	Responsables sécurité. Ingénieurs systèmes et réseaux. Architectes sécurité. Techniciens réseaux ou sécurité.
<b>Durée</b>	4 jours - 28 heures
<b>Pré-requis</b>	Bonnes connaissances en administration réseaux avec équipements Cisco et en sécurité informatique.
<b>Objectifs</b>	<p>Connaître les fonctionnalités du firewall Cisco ASA</p> <p>Configurer un firewall ASA</p> <p>Configurer les fonctions essentielles à l'aide de l'ASDM et du CLI</p> <p>Configurer la stratégie d'accès basée sur les ACLs (Listes de contrôle d'accès)</p> <p>Analyser et restreindre le flux (entrant et sortant)</p> <p>Configurer un VPN pour les accès distants</p> <p>Optimiser les règles de sécurité</p>
<b>Méthodes pédagogiques</b>	<p>Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire.</p> <p>La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.</p> <p>Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.</p>
<b>Moyens techniques</b>	<p>1 poste de travail complet par personne</p> <p>De nombreux exercices d'application</p> <p>Mise en place d'ateliers pratiques</p> <p>Remise d'un support de cours</p> <p>Passage de certification(s) dans le cadre du CPF</p> <p>Remise d'une attestation de stage</p>
<b>Modalité d'évaluation des acquis</b>	<p>Evaluation des besoins et objectifs en pré et post formation</p> <p>Evaluation technique des connaissances en pré et post formation</p> <p>Evaluation générale du stage</p>
<b>Délai d'accès</b>	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
<b>Accessibilité handicapés</b>	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

## 1. INTRODUCTION

- Les technologies et caractéristiques des firewalls.
- Présentation des firewalls. Terminologie et fonctionnalités.
- Exemples d'architecture. La gamme ASA.
- Le démarrage avec un ASA. L'interface utilisateur. Configuration du firewall.
- Paramétrage de NTP. Les niveaux de sécurité ASA.
- Configuration de Syslog.

## 2. TRADUCTION D'ADRESSES ET CONNEXIONS

- NAT dynamique, PAT et NAT statique.
- La fonction TCP Intercept.
- Connexions, redirection de ports.
- Configuration DMZ.

## 3. ACL ET CONTENT FILTERING

- Présentation des ACL.
- Configuration des ACL.
- Filtrage de code actif malicieux.
- Filtrage d'URL.
- Les groupes d'objets.
- Présentation des groupes d'objets. Les usages.
- La configuration des groupes d'objets.

## 4. CONFIGURATION AAA

- Présentation de Cisco Secure ACS.
- Installation de Cisco Secure ACS.
- Configurer l'authentification et l'autorisation.
- Téléchargement des ACL.
- Dépannage AAA.

## 5. ROUTAGE ET COMMUTATION

- Rappels sur les VLAN.
- Fonctionnalités supportées.
- Routage statique et dynamique.
- Le Multicast.

## 6. VPN

- Mise en place des VPN.
- Configuration d'IPSec.
- Le client VPN Cisco.
- Configuration de l'accès distant avec Easy VPN.
- Configuration du serveur Easy VPN.
- Caractéristiques d'Easy VPN distant.
- Présentation et configuration du client.
- Présentation et configuration du WebVPN.

## 7. TRANSPARENT FIREWALL

- Transparent versus Routed firewall.
- Fonctionnalités non supportées.
- Configuration des adresses IP, des ACL et d'ARP.
- Maintenance et dépannage.

## 8. FAILOVER

- Présentation des modes de Failover. Configuration de Failover et de Lan Failover. Mise en place du Failover.
- Configuration de Failover.
- Configuration de Lan Failover.
- Mise en place du Failover en mode Active/Active.

## 9. CISCO SECURITY APPLIANCE DEVICE MANAGER

- Utilisation de ASDM pour la configuration de ASA.
- Création de VPN site à site et d'accès distant VPN.

## 10. MAINTENANCE

- Configuration de l'accès.
- Niveaux de privilèges.
- Password Recovery.
- Gestion de l'IOS.
- Gestion de la configuration.
- Gestion des licences.

## NOUS CONTACTER

### Siège social

16, ALLÉE FRANÇOIS VILLON  
38130 ÉCHIROLLES

### Téléphone

04 76 23 20 50 - 06 81 73 19 35

### Suivez-nous sur les réseaux sociaux, rejoignez la communauté !



ACF Audit Conseil Formation



@ACF\_Formation



ACFauditconseilformation

### Centre de formation

87, RUE GÉNÉRAL MANGIN  
38000 GRENOBLE

### E-mail

contact@audit-conseil-formation.com