Ambient IT
128 Boulevard Macdonald
75019 Paris

Mail : formation@ambient-it.net
Tél : +33 (0)1 40 34 11 53

AMBIENT-IT

Formation Fortinet : Fortigate Infrastructure Security

(EDU-**NSE4**)

5 jours (35 heures)

PRÉSENTATION

Fortinet est à devenu depuis quelques années leader au sein de sécurité réseau, Avec son outil Fortigate qui permet la gestion unifiée des menaces consolide plusieurs fonctions de sécurité telles que pare-feu, la prévention d'intrusion, le filtrage web, ainsi que la protection anti-malware et anti-spam.

Dans cette formation de 5 jours Fortigate Security sera mis en avant les 3 premiers jours afin que saisissiez les les fondamentaux de cette technologie vous aurez la main sur des équipements qui se trouvent sur notre environnement de formation. Au travers des exercices vous configurerez des règles pare-feu, des tunnels VPN IPSEC, des accès VPN SSL, la protection contre les malwares, des profils de filtrage d'URL, l'authentification des utilisateurs au travers d'un portail captif.

À l'issue de ses 3 jours nous passerons a Fortigate l'infrastructure vous prendrez en main les fonctions d'architectures avancées du FortiGate. vous configurerez de la SD-Wan, du routage avancé, la mise en haute disponibilité des FortiGate, le mode transparent, des tunnels IPsec redondés, les VDOMS, le Single Sign On

À l'issue de ces 5 jours de formation vous sera capable de maîtriser Forgate Security ainsi que son infrastructure et de passeé la certification NSE4.

Comme dans toute nos formations nous utiliserons la dernière version stable du logiciel Fortigate 6.4.

Objectifs Fortigate Security

- Décrire les fonctionnalités des UTM du FortiGate
- Neutraliser les menaces véhiculées au travers des malwares, les applications nocives et limiter les accès aux sites inappropriés
- Contrôler les accès au réseau selon les types de périphériques utilisés
- Authentifier les utilisateurs au travers du portail captif personnalisable
- Mettre en œuvre un VPN SSL pour l'accès des utilisateurs nomades au réseau de l'entreprise
- Mettre en œuvre un VPN IPsec pour l'accès des utilisateurs nomades au réseau de l'entreprise
- Appliqué de la PAT, de la source NAT et de la destination NAT
- Interpréter les logs et générer des rapports
- Utiliser la GUI et la CLI
- Mettre en œuvre la protection anti-intrusion

- Maîtriser l’utilisation des applications au sein de votre réseau

Objectifs Fortigate Infrastructure

- Configuré de la SD-Wan,
- Monitorer le statut de chaque lien de la SDWan
- Configurer de la répartition de charge au sein de la SD-Wan
- Déployer un cluster de FortiGate,
- Inspecter et sécuriser le trafic réseau sans impacter le routage,
- Analyser la table de routage d’un FortiGate
- Diviser un FortiGate physique en plusieurs FortiGates virtuels indépendants, via la mise en œuvre des Virtual Domains
- Étudier et choisir une architecture de VPN IPsec
- Comparer les VPN IPsec en mode Interface (route-base) ou Tunnel (Policy-based)
- Implémenter une architecture de VPN IPSec refondée,
- Troubleshooter et diagnostiquer des problématiques simples sur le FortiGate,
- Mettre en œuvre l’identification utilisateur ou l’authentification transparente dans les environnements active Directory.

PUBLIC VISÉ

- Architecte réseau et sécurités FortiGate
- Administrateur firewall FortiGate

PRÉ-REQUIS

- Connaissance des couches du modèle OSI
- Connaissance des concepts de firewall

Programme FortiGate Security - 3 jours

Introduction sur FortiGate et les UTM

- Caractéristiques de haut niveau
- Décisions de mise en place
- Administration de base
- Serveurs intégrés
- Maintenance Fondamentale
- FortiGate dans le Sécurity Fabric

Firewall

- Les règles de Firewall
  - Politiques de pare-feu
  - Configuration des stratégies de pare-feu
  - Gestion des politiques de pare-feu
- Les règles de Firewall avec authentification des utilisateurs
  - Méthodes d'authentification pare-feu d'authentification
  - Serveurs d'authentification à distance
  - Groupes d'utilisateurs
  - Utilisation des stratégies de pare-feu pour l'authentification
  - Authentification par le biais d'un portail captif
  - Surveillance et dépannage

Le NAT

- Introduction au NAT
- Politique de pare-feu NAT
- NAT central
- Sessions

Gestion des logs et supervision

- Log Basics
- Local Logging
- Remote Logging
- Log Settings
- View, Search, and Monitor Logs
- Protecting Log Data

Certificats Contrôle applicatif & Filtrage URL

- Certificats
  - Authentification et sécurisation des données à l'aide de certificats
  - Inspecter les données chiffrées
  - Gérer les certificats numériques dans FortiGate
- Contrôle applicatif
  - Modes d'inspection
  - Notions de base sur le filtrage Web
  - Fonctions supplémentaires de filtrage Web par proxy
  - Filtrage DNS
- Filtrage URL
  - Modes d'inspection
  - Notions de base sur le filtrage Web
  - Fonctions supplémentaires de filtrage Web par proxy

LES VPN

- VPN SSL
  - Décrire SSL-VPN
  - Modes de déploiement SSL-VPN
  - Configuration des SSL-VPNs
  - Royaumes et signets personnels
  - L'accès SSL-VPN
- Le VPN IPSEC en mode dial-up
- IPsec Introduction
- IKE Phase 1 and IKE Phase 2
- Dialup IPsec VPN

Programme FortiGate Infrastructure - 2 jours

Routage

- Routage FortiGate
- Moniteur de routage et attributs d'itinéraire
- Routage à multiples trajets

SD-Wan

- Introduction au WAN défini par logiciel
- SLA de performance SD-WAN
- Règles SD-WAN

La virtualisation & Analyse L2

- Virtualisation
  - Concepts VDOM
  - Administrateurs VDOM
  - Configuration des VDOMs
  - Liens inter-VDOM
- Analyse L2
  - Le VPN IPSec en mode site à site
  - Le FSSO
  - La haute disponibilité
  - Le Proxy explicite
  - Les diagnostics

Le VPN IPSec en mode site à site & FSSO

- VPN
  - Topologies VPN
  - Configuration VPN site à site
- FSSO
  - Fonction et déploiement de l'FSSO
  - FSSO Avec Active Directory
  - Authentification NTLM
  - Paramètres de l'FSSO

Proxy Explicite

- Concepts de proxy Web
- Configuration du serveur proxy Web
- Authentification et autorisation des serveurs proxy Web

Haute disponibilité & Diagnostics

- HA Modes de fonctionnement
- Synchronisation des clusters HA
- Charge de travail et basculement de l'AP
- Diagnostics
  - Diagnostic général
  - Flux de débogage
  - CPU et mémoire
  - Firmware et Hardware

Certification

Ce cours ainsi que FortiGate Infrastructure préparent au passage de la certification NSE4.

Sociétés concernées

Cette formation s’adresse aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée.

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 multiple permet de vérifier l'acquisition correcte des compétences.

Sanction

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