FROGGY Network

FORMATIONS EN SYSTÈME, RÉSEAU & CYBERSÉCURITÉ

FORMATION RÉSEAU

CLAVISTER NETWALL FUNDAMENTALS

Clavister NetWall

SÉCURITÉ DES RÉSEAUX AVEC UNE COMPLEXITE RÉDUITE ET UNE PROTECTION AVANCÉE CONTRE LES MENACES.

Clavister NetWall Fundamentals est la première formation à suivre pour toute personne ne connaissant pas la gamme de produits NetWall. Elle constitue le prérequis pour toutes les autres formations du parcours NetWall et, en tant que telle, la toute première étape pour devenir à la fois un expert NetWall et une personne plus complète et plus performante. Tant les débutants que les techniciens ayant de l'expérience avec d'autres fournisseurs de pare-feu sont les bienvenus.
À l'issue de cette formation, vous aurez une bonne compréhension de la sécurité de base des réseaux, de la manière d'installer et de configurer correctement un pare-feu de nouvelle génération et de la façon dont il s'intègre dans un réseau. Vous aurez également une bonne connaissance de ses différents sous-systèmes et de leur utilité.

Ce cours couvre un large éventail de sujets et vous permet d'acquérir les connaissances nécessaires pour :

- utiliser l'ensemble des outils d'administration et de gestion des journaux : CLI, interface web et InControl
- comprendre les concepts de routage, d'objets et de politiques de sécurité
- configurer et utiliser les fonctions de gestion des menaces telles que la détection et la prévention des intrusions, le contrôle des applications, la réputation des adresses IP, etc.
- utiliser pleinement l'authentification
- configurer facilement des tunnels VPN LAN-to-LAN et itinérants

Clavister est un pionnier de la sécurité des réseaux, depuis le lancement de l'un des premiers pares-feux il y a 25 ans jusqu'au développement des pare-feu virtualisés les plus rapides, en passant par l'intégration de la sécurité des réseaux avec le SD-WAN sécurisé et le SASE. Des petites et moyennes entreprises (PME) aux grandes entreprises, en passant par les centres de données et les opérateurs de téléphonie mobile, nous proposons des NGFW adaptés aux besoins de chaque organisation.

OBJECTIFS PÉDAGOGIQUES

- Installer et configurer un pare-feu Clavister NetWall (CLI + Web UI)
- Mettre en œuvre un serveur DHCP
- Créer et gérer des politiques IP (NAT, SAT, FwdFast)
- Mettre en œuvre l'authentification des utilisateurs (local, RADIUS, MFA)
- Sécuriser l'accès web (NetEye, ALG, filtrage HTTPS)
- Appliquer le contrôle applicatif et la gestion de la bande passante
- Déployer des tunnels VPN (site-à-site et nomades)
- Exploiter les logs avec InControl, InCenter et Cloud Services
- Mettre en œuvre les fonctions de prévention des menaces (IDP, IP reputation)

PUBLIC VISÉ

- Administrateurs systèmes et réseaux
- Techniciens cybersécurité
- Intégrateurs et consultants IT

PRÉREQUIS

- Connaissances de base en réseau IP
- Expérience avec Windows Server recommandée

DURÉE

2 JOURS
(14 heures)

MODALITÉS PÉDAGOGIQUES

- Présentiel ou distanciel
- Alternance de théorie et de travaux pratiques
- Accès à un environnement de lab virtuel (VNC)
- 2 tentatives de certification incluses

MODALITÉS D'ÉVALUATION

- Test de positionnement préparatoire
- Travaux pratiques supervisés
- Certification éditeur

SUPPORTS FOURNIS

- PDF officiel Clavister
- Accès aux scripts et ressources

ACCESSIBILITÉ

Formation accessible aux personnes en situation de handicap
(nous contacter pour adaptation)

TARIF

SUR DEVIS

PRISE EN CHARGE POSSIBLE VIA OPCO

RÉSERVER UNE SESSION

01 88 83 38 00
formation@froggy-network.com
Contactez-nous | Froggy Network

PROGRAMME DÉTAILLÉ

JOUR 1

Chapitre 1 **Getting started with CLI**	Découverte du CLI, configuration des interfaces LAN, commandes de base, scripts CLI
Chapitre 2 **Web UI**	Navigation dans l'interface Web, gestion des logs, certificats, mises à jour, objets de configuration
Chapitre 3 **DHCP Server**	Création d'un serveur DHCP, ajout d'hôtes statiques, configuration client Windows
Chapitre 4 **IP Policies**	Routage, NAT, règles d'accès, translation d'adresses, inspection avec état
Chapitre 5 **Centralized Management & Logging**	Installation et configuration d'InControl et InCenter, gestion centralisée, agents de logs
Chapitre 6 **User Authentication**	Authentification locale et RADIUS, portail captif, MFA, gestion des groupes et des droits

JOUR 2

Chapitre 7 **Secure Web Access**	Filtrage de contenu Web (WCF), antivirus, inspection HTTPS avec NetEye, redirection vers portail
Chapitre 8 **Application Control & Traffic Management**	Contrôle applicatif (BitTorrent, etc.), QoS, pipes, shaping, règles par groupe utilisateur
Chapitre 9 **Threat Prevention**	IP reputation, IDP, protection DoS, scanner, botnet, seuils et règles de sécurité
Chapitre 10 **Logging & Analytics**	Analyse des logs via Web UI, InControl, InCenter, Cloud Services, création de rapports
Chapitre 11 **Site-to-Site VPN**	Configuration d'un tunnel IPsec entre deux sites, authentification par clé pré-partagée
Chapitre 12 **Roaming VPN**	VPN nomade avec IKEv2 ou OneConnect, configuration client Windows, authentification forte