



FORMATIONS EN SYSTÈME, RÉSEAU & CYBERSÉCURITÉ

CLAVISTER NETWALL BASICS



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

Les pare-feux de nouvelle génération (NGFW) sont essentiels pour sécuriser les environnements hybrides (sur site/centre de données, nuage, SaaS) et fournir une protection avancée contre les logiciels malveillants et les intrusions. Les NGFW sont explicitement conçus pour inclure le contrôle des applications, les systèmes de prévention des intrusions, l'anti-malware, l'inspection approfondie des paquets et de nombreuses autres fonctions de sécurité réseau nécessaires pour lutter contre les cybermenaces actuelles.

Clavister est un pionnier de la sécurité des réseaux, depuis le lancement de l'un des premiers pare-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 NetWall depuis zéro
- Mettre en œuvre un accès Internet sécurisé
- Créer des tunnels VPN (site-à-site et nomades)
- Appliquer des règles de sécurité et de QoS
- Gérer les logs avec InControl et Cloud Services

MODALITÉS PÉDAGOGIQUES

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

MODALITÉS D'ÉVALUATION

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

ACCESSIBILITÉ

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

LIVRABLES

- Attestation de formation
- Support de cours PDF
- Accès aux ressources Clavister (documentation, guides)

PUBLIC VISÉ

- Professionnels IT
- Administrateurs réseau
- Techniciens sécurité

PRÉREQUIS

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

DURÉE

1 JOUR
(7 heures)

SUPPORTS FOURNIS

- PDF officiel Clavister
- Accès aux scripts et ressources

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 0 Getting Started	●	Accès à l'interface Web/CLI, configuration initiale (LAN, WAN, DHCP, DNS), gestion des certificats, import de scripts
Chapitre 1 IP Policies	●	Routage, NAT, règles d'accès, inspection avec état, translation d'adresses (SAT, NAT), ordonnancement des règles
Chapitre 2 Centralized Management & Logging	●	Installation et configuration d'InControl, gestion centralisée des firewalls, configuration des agents de logs
Chapitre 3 Secure Web Access	●	Filtrage de contenu Web (WCF), inspection HTTPS avec NetEye, profils de sécurité applicative
Chapitre 4 IP Policies	●	Détection et blocage d'applications (BitTorrent, etc.), gestion de la bande passante (QoS, pipes, priorités)
Chapitre 5 Threat Prevention	●	IP Reputation, IDP, protection DoS, botnet, phishing, règles de seuils
Chapitre 6 Logging & Analytics	●	Analyse des logs via InControl/InCenter, tableaux de bord, filtres, rapports
Chapitre 7 Site-to-Site VPN	●	Configuration d'un tunnel IPsec entre deux sites, authentification par clé pré-partagée
Chapitre 8 Roaming VPN	●	VPN nomade avec IKEv2 ou OneConnect, configuration client Windows, authentification forte (MFA, RADIUS)