FROGGY Network

SPÉCIALISTE DE CONCEPTION DE SOLUTIONS OPÉRATIONNELLES

Des solutions designées et intégrées par ses experts, rendant accessibles à des partenaires non spécialistes les meilleures technologies IAAS / PAAS / CYBER

DESIGNER

CLOUD SERVICES for MSP

DISTRIBUTEUR

FORMATIONS EN **SYSTEME, RESEAU & CYBERSECURITE**

FROGGY FORMATION
Edition **2025**

Centre de formation agréé n° 11 98 00000 00 | Certifié QUALIOPI

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

froggy-network.com

CLAVISTER NETWALL FUNDAMENTALS

Clavister NetWall

SECURITE DES RESEAUX AVEC UNE COMPLEXITE REDUITE ET UNE PROTECTION AVANCEE CONTRE LES MENACES

Les pares-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 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 PEDAGOGIQUES

- 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 VISE

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

📌 PREREQUIS

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

⏱️ DUREE

2 jours (14 heures)

👨‍🏫🏢 MODALITES PEDAGOGIQUES

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

MODALITES D'EVALUATION

- Auto-évaluation des acquis
- Travaux pratiques supervisés
- Questionnaire de satisfaction

SUPPORTS FOURNIS

- PDF officiel Clavister
- Accès aux scripts et ressources
- Fiche d'auto-évaluation

♿ ACCESSIBILITE

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

💶 TARIF

Sur devis – prise en charge possible via OPCO

🔗 LIEN VERS LES RESSOURCES

- Réserver une session :
  Téléphone 01 88 83 38 00
  Courriel formation@froggy-network.com
  Formulaire web Contactez-nous | Froggy Network

📚 PROGRAMME DETAILLE

JOUR	CHAPITRES	CONTENU PRINCIPAL
1	1.Getting started with CLI	Découverte du CLI, configuration des interfaces LAN, commandes de base, scripts CLI
	2.Web UI	Navigation dans l'interface Web, gestion des logs, certificats, mises à jour, objets de configuration
	3.DHCP Server	Création d'un serveur DHCP, ajout d'hôtes statiques, configuration client Windows
	4.IP Policies	Routage, NAT, règles d'accès, translation d'adresses, inspection avec état
	5.Centralized Management & Logging	Installation et configuration d'InControl et InCenter, gestion centralisée, agents de logs
	6.User Authentication	Authentification locale et RADIUS, portail captif, MFA, gestion des groupes et des droits
2	7.Secure Web Access	Filtrage de contenu Web (WCF), antivirus, inspection HTTPS avec NetEye, redirection vers portail
	8.Application Control & Traffic Management	Contrôle applicatif (BitTorrent, etc.), QoS, pipes, shaping, règles par groupe utilisateur
	9.Threat Prevention	IP reputation, IDP, protection DoS, scanner, botnet, seuils et règles de sécurité
	10.Logging & Analytics	Analyse des logs via Web UI, InControl, InCenter, Cloud Services, création de rapports
	11.Site-to-Site VPN	Configuration d'un tunnel IPsec entre deux sites, authentification par clé pré-partagée
	12.Roaming VPN	VPN nomade avec IKEv2 ou OneConnect, configuration client Windows, authentification forte