DAWAN

Plan de la formation

www.dawan.fr

Formation Certified Stormshield Network Administrator (NT-CSNA)

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	3 250,00 CHF HT (standard) 2 600,00 CHF HT (remisé)
Public :	Responsables informatique, administrateurs réseaux, techniciens informatiqu
Pré-requis :	Avoir de bonnes connaissances TCP/IP Il est demandé aux stagiaires souhaita s'inscrire en formation CSNA de valider au préalable qu'ils disposent des connaissances nécessaires pour participer à la formation grâce au test d'auto évaluation au lien suivant: https://institute.stormshield.eu/courses/CSNAPREREQUISITEFR/?language=fre
Objectifs :	Prendre en main un firewall SNS et connaître son fonctionnement - Configure firewall dans un réseau - Définir et mettre en œuvre des politiques de filtrage de routage - Configurer un contrôle d'accès aux sites web en http et https (proxy) - Configurer des politiques d'authentification - Mettre en place différe types de réseaux privés virtuels (VPN IPSec et VPN SSL)
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants l dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	RéS102509-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73

Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standa
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Prendre en main le firewall

Enregistrer un compte sur l’espace client et accéder aux ressources techniques
Initialiser le boîtier et présenter l’interface d’administration
Configurer le système et les droits d'administration
Installer la licence et mettre à jour la version du système
Sauvegarder et restaurer une configuration
Atelier : Configurer un firewall Stormshield et tester les sauvegardes et restaurations

Analyser les traces et supervisions

Présenter les catégories de traces
Superviser et créer des graphiques d’historiques
Atelier : Créer des graphiques de supervision basés sur les traces système

Gérer les objets

Expliquer la notion d’objet et les types d’objets utilisables
Présenter les objets réseau et les objets routeur
Atelier : Créer et manipuler des objets réseau et routeur dans le firewall

Configurer le réseau

Apprendre les modes de configuration d’un boîtier dans un réseau
Identifier les types d'interfaces (Ethernet, modem, bridge, VLAN, GRETAP)
Maîtriser les types de routage et leurs priorités
Atelier : Configurer un réseau en utilisant différentes interfaces et types de routage

Configurer la translation d’adresses (NAT)

Effectuer la translation sur flux sortant (déguisement)
Effectuer la translation sur flux entrant (redirection)

Mettre en place une translation bidirectionnelle (un pour un)
Atelier : Configurer les règles NAT et tester le déguisement et la redirection

Maîtriser le filtrage

Comprendre les généralités sur le filtrage et la notion de suivi de connexion (stateful)
Présenter les paramètres d'une règle de filtrage
Ordonnancer les règles de filtrage et de translation
Atelier : Configurer des règles de filtrage et tester le suivi de connexion

Assurer la protection applicative

Mettre en place le filtrage URL en HTTP et HTTPS
Configurer l'analyse antivirale et l'analyse par détonation Breach Fighter
Configurer le module de prévention d'intrusion et les profils d'inspection de sécurité
Atelier : Configurer le filtrage URL et tester l'analyse par détonation

Gérer les utilisateurs et l'authentification

Configurer les annuaires d'utilisateurs
Présenter les différentes méthodes d'authentification (LDAP, Kerberos, Radius, Certificat SSL, SPNEGO, SSO)
Enrôler des utilisateurs
Mettre en place une authentification explicite via portail captif
Atelier : Configurer une méthode d'authentification et enrôler des utilisateurs

Configurer les réseaux privés virtuels

Comprendre les concepts et généralités VPN IPSec (IKEv1 et IKEv2)
Configurer un VPN site-à-site avec clé pré-partagée
Créer une Virtual Tunneling Interface
Atelier : Configurer un VPN IPSec site-à-site et tester la connexion sécurisée

Mettre en place un VPN SSL

Comprendre le principe de fonctionnement du VPN SSL
Configurer un VPN SSL
Atelier : Déployer et tester une connexion VPN SSL sur un appareil client