Securing the Web with Cisco Web Security Appliance (SWSA)

ID SWSA **Prix** CHF 2 070,– (Hors Taxe) **Durée** 2 jours

A qui s'adresse cette formation

- Architectes de sécurité
- Concepteurs de systèmes
- Administrateurs réseau
- Ingénieurs des opérations
- Responsables de la sécurité web, techniciens réseau ou de sécurité, et ingénieurs et managers en sécurité
- Intégrateurs et partenaires Cisco

Cette formation prépare à la/aux certifications

Cisco Certified Network Professional Security (CCNP SECURITY)

Pré-requis

Pour tirer pleinement parti de ce cours, vous devez avoir des connaissances sur les sujets suivants :

- Services TCP/IP, y compris le système de noms de domaine (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP et HTTPS
- Routage IP

Vous devez avoir une ou plusieurs des compétences techniques de base suivantes ou des connaissances équivalentes :

- Certification Cisco (CCENT ou supérieure)
- Certification dans l'industrie pertinente [International Information System Security Certification Consortium ((ISC)2), Computing Technology Industry Association (CompTIA) Security+, International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA]
- Lettre de réussite de Cisco Networking Academy (CCNA® 1 et CCNA 2)
- Expertise Windows : Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)

Vous devez avoir les compétences et connaissances suivantes avant de suivre ce cours :

- Ressources de formation en sécurité web sur https://www.cisco.com/c/m/en_us/products/security/web-security-training.html

Objectifs

Après avoir suivi ce cours, vous devriez être en mesure de :

- Décrire Cisco WSA
- Déployer des services proxy
- Utiliser l'authentification
- Décrire les politiques de déchiffrement pour contrôler le trafic HTTPS
- Comprendre les politiques d'accès différenciées au trafic et les profils d'identification
- Appliquer les paramètres de contrôle d'utilisation acceptable
- Défendre contre les logiciels malveillants
- Décrire la sécurité des données et la prévention des pertes de données
- Effectuer l'administration et le dépannage

Contenu

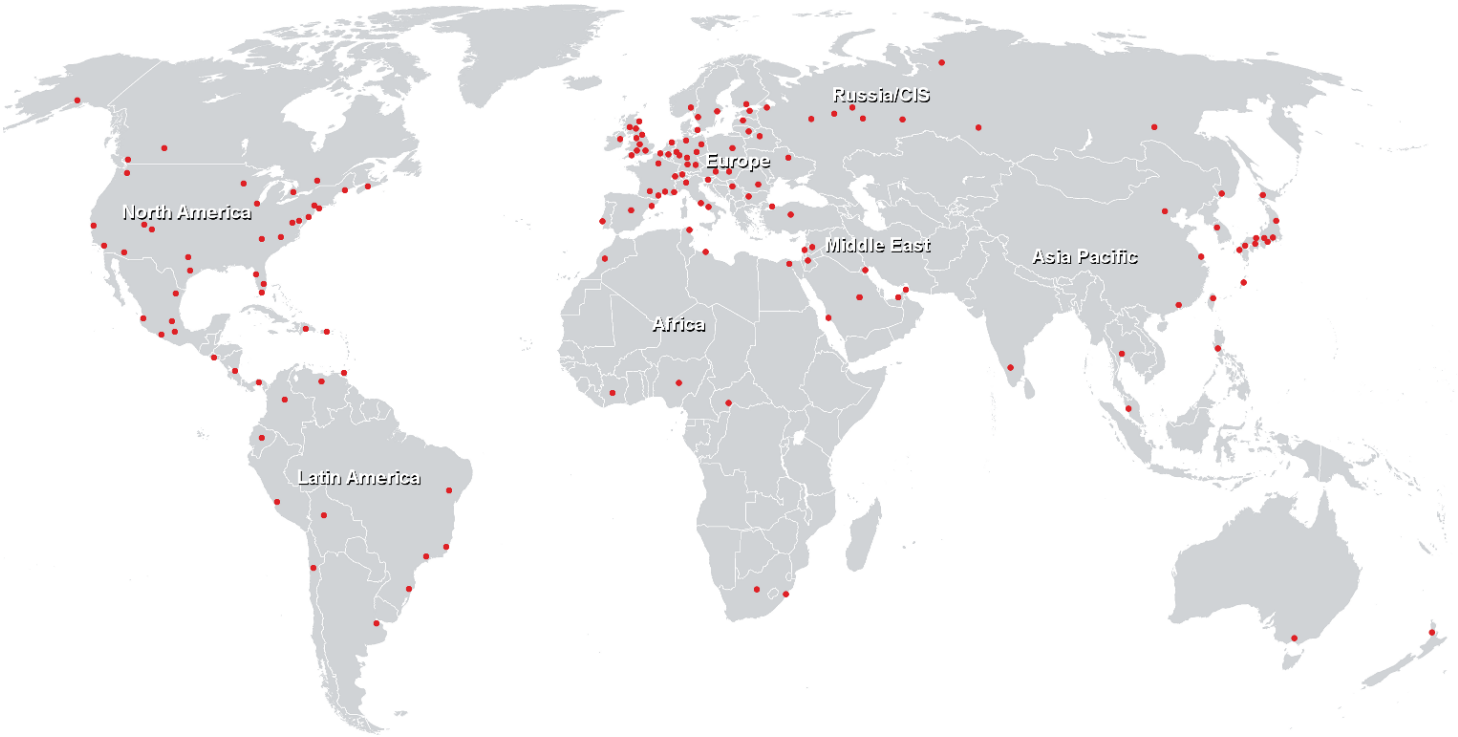
- Description du Cisco WSA
- Déploiement des services proxy
- Utilisation de l'authentification
- Création de politiques de déchiffrement pour contrôler le trafic HTTPS
- Compréhension des politiques d'accès au trafic différencié et des profils d'identification
- Défense contre les malwares
- Application des paramètres de contrôle d'utilisation acceptable
- Sécurité des données et prévention des pertes de données
- Administration et dépannage
- Références

Labs

- Configurer le Cisco Web Security Appliance
- Déployer des services proxy
- Configurer l'authentification proxy
- Configurer l'inspection HTTPS
- Créer et appliquer une politique d'utilisation acceptable

basée sur le temps/date
- Configurer la protection avancée contre les malwares
- Configurer des exceptions d'en-tête de référent
- Utiliser des flux de sécurité tiers et le flux externe de MS Office 365
- Valider un certificat intermédiaire
- Afficher les services de rapport et le suivi web
- Effectuer une mise à jour centralisée du logiciel Cisco AsyncOS à l'aide de Cisco SMA

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch