Formation Sécuriser le Web avec Cisco Web Security Appliance

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Apprenez à mettre en oeuvre, utiliser et maintenir l'appliance de sécurité Web Cisco® (WSA), pour fournir une protection avancée pour les e-mails professionnels et un contrôle contre les menaces de sécurité Web. En suivant cette formation, vous apprendrez à déployer des services proxy, à utiliser l'authentification, à mettre en oeuvre des politiques pour contrôler le trafic et l'accès HTTPS, à mettre en oeuvre des paramètres et des politiques de contrôle d'utilisation, à utiliser les fonctionnalités anti-malware de la solution, à mettre en oeuvre sécurité des données et prévention des pertes de données, administration de la solution Cisco WSA, etc. Le suivi de cette formation permet de valider un total de 16 crédits dans le cadre du programme d'Education Continue Cisco (CCE) pour les professionnels qui souhaitent renouveler leur titre de certification.

Référence	SWSA
Durée	2 jours (14h)
Tarif	2 070 €HT
Repas	40 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 22 au 23 septembre 2025

du 2 au 3 mars 2026

VOIR TOUTES LES DATES

Objectifs

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

Public

| Les personnes impliquées dans le déploiement, l'installation et l'administration d'un dispositif de sécurité Web Cisco.

Prérequis

| Services TCP/IP, y compris Domain Name System (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 :
| CCNA Recommandé
| Certification industrielle pertinente (ISC)2, (CompTIA) Security+, EC-Council, GIAC, ISACA
| Expertise Windows : Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)
| Lab 11:

Programme de la formation

Description de Cisco WSA

| Cas d'utilisation de la technologie
| Solution Cisco WSA
| Fonctionnalités Cisco WSA
| Architecture Cisco WSA
| Service proxy

| Moniteur de trafic de couche 4 intégré
| Prévention de la perte de données
| Intelligence cognitive Cisco
| Outils de gestion
| Cisco Advanced Web Security Reporting (AWSR) et intégration tierce
| Appliance de gestion de la sécurité du contenu Cisco (SMA)

Déploiement des services proxy
| Mode de transfert explicite vs mode transparent
| Redirection du trafic en mode transparent
| Protocole de contrôle du cache Web
| Flux montant et descendant du protocole de communication de cache Web (WCCP)
| Contournement du proxy
| Mise en cache proxy
| Fichiers de configuration automatique du proxy (PAC)
| Proxy FTP
| Proxy Socket Secure (SOCKS)
| Journal d'accès proxy et en-têtes HTTP
| Personnalisation des notifications d'erreur avec les pages de notification de l'utilisateur final (EUN)

Utilisation de l'authentification
| Protocoles d'authentification
| Domaines d'authentification
| Suivi des informations d'identification de l'utilisateur
| Mode proxy explicite (transfert) et transparent
| Contournement de l'authentification avec des agents problématiques
| Rapports et authentification
| Ré-authentification
| Authentification proxy FTP
| Dépannage de la jonction de domaines et test d'authentification
| Intégration avec Cisco Identity Services Engine (ISE)

Création de politiques de déchiffrement pour contrôler le trafic HTTPS
| Présentation de l'inspection TLS (Transport Layer Security)/Secure Sockets Layer (SSL)
| Présentation du certificat
| Présentation des politiques de déchiffrement HTTPS
| Activation de la fonction proxy HTTPS
| Balises de liste de contrôle d'accès (ACL) pour l'inspection HTTPS
| Exemples de journaux d'accès

Comprendre les politiques d'accès au trafic différencié et les profils d'identification
| Présentation des stratégies d'accès
| Accéder aux groupes de stratégies
| Présentation des profils d'identification
| Profils d'identification et authentification
| Ordre de traitement de la politique d'accès et des profils d'identification
| Autres types de polices
| Exemples de journaux d'accès
| Balises de décision ACL et groupes de stratégies
| Application des politiques d'utilisation acceptable basées sur le temps et sur le volume de trafic, et des notifications aux utilisateurs finaux

Défense contre les logiciels malveillants
| Filtres de réputation Web
| Analyse anti-malware
| Analyse du trafic sortant
| Anti-malware et réputation dans les politiques
| Filtrage de la réputation des fichiers et analyse des fichiers
| Protection avancée contre les logiciels malveillants de Cisco
| Fonctionnalités d'analyse et de réputation des fichiers
| Intégration avec Cisco Cognitive Intelligence

Application des paramètres de contrôle d'utilisation acceptable
| Contrôle de l'utilisation du Web
| Filtrage d'URL
| Solutions de catégories d'URL

| Moteur d'analyse de contenu dynamique
| Visibilité et contrôle des applications Web
| Application des limites de bande passante multimédia
| Logiciel en tant que service (SaaS) Contrôle d'accès
| Filtrage du contenu réservé aux adultes

Sécurité des données et prévention des pertes de données
| Sécurité des données
| Solution de sécurité des données Cisco
| Définitions de la politique de sécurité des données
| Journaux de sécurité des données

Exécution de l'administration et du dépannage
| Surveiller l'appliance de sécurité Web Cisco
| Rapports Cisco WSA
| Surveillance de l'activité du système via les journaux
| Tâches d'administration système
| Dépannage
| Interface de ligne de commande
| Lab 1 : Configurer l'appliance de sécurité Web Cisco
| Lab 2 : Déployer des services proxy
| Lab 3 : Configurer l'authentification proxy
| Lab 4 : Configurer l'inspection HTTPS
| Lab 5 : Créer et appliquer une politique d'utilisation acceptable basée sur l'heure/la date
| Lab 6 : Configurer la protection avancée contre les logiciels malveillants
| Lab 7 : Configurer les exceptions d'en-tête de référent
| Lab 8 : Utiliser des flux de sécurité tiers et un flux externe MS Office 365
| Lab9 : Valider un certificat intermédiaire
| Lab 10 : Afficher les services de création de rapports et le suivi Web
| Lab 11 : effectuer une mise à niveau centralisée du logiciel Cisco AsyncOS à l'aide de Cisco SM

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

HUB Formation - 14 avenue de l'Opéra - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.