03 20 61 95 06
formation@access-it.fr

Formation CISCO SWSA Sécuriser les accès Web avec Cisco Web Security Appliance

Durée de la formation : 2 jour(s) / 14 heure(s)

OBJECTIFS

A l'issue de la formation, l'apprenant sera capable de :
Apprendre à installer et à vérifier Cisco WSA
Savoir déployer des services de proxy
Comprendre comment utiliser l'authentification
Être en mesure de configurer des stratégies
Pouvoir mettre en place une défense contre les logiciels malveillants
Savoir configurer des stratégies de sécurité des données
Comprendre comment mettre en oeuvre l'administration et le dépannage
Se préparer à l'examen Securing the Web with Cisco Web Security Appliance (300-725 SWSA)

PREREQUIS

Avoir des connaissances sur TCP/IP, les services DNS, SSH, FTP, SNMP, HTTP et HTTPS
Avoir de l'expérience sur le routage IP
Être certifié CCNA
Connaissances de Windows
Cette formation ne peut être financée que dans le cadre d'un projet d'entreprise (prise en charge entreprise ou OPCO). Les dossiers à financement personnel et CPF ne sont pas pris en compte.

PUBLIC

Architectes de sécurité
Concepteurs de systèmes
Administrateurs réseau
Ingénieurs d'exploitation
Les gestionnaires de réseau, les techniciens de réseau ou de sécurité, et les ingénieurs et gestionnaires de sécurité responsables de la sécurité Web
Intégrateurs et partenaires Cisco

03 20 61 95 06
formation@access-it.fr

Formation CISCO SWSA Sécuriser les accès Web avec Cisco Web Security Appliance

Durée de la formation : 2 jour(s) / 14 heure(s)

PROGRAMME

Décrire Cisco WSA

Cas d'utilisation de la technologie
Solution Cisco WSA
Caractéristiques de Cisco WSA
Architecture de Cisco WSA
Service proxy
Moniteur de trafic de couche 4 intégré
Prévention contre la perte de données
Cisco Cognitive Intelligence
Outils de gestion
Cisco Advanced Web Security Reporting (AWSR) etintégration tierce
Appliance de gestion de la sécurité du contenu Cisco (SMA)

Déploiement de services proxy

Mode direct explicite vs mode transparent
Redirection du trafic en mode transparent
Protocole de contrôle du cache Web
Flux amont et aval du protocole de communication WebCache (WCCP)
Contournement de proxy
Mise en cache du proxy
Fichiers de configuration automatique du proxy (PAC)
Proxy FTP
Proxy Socket Secure (SOCKS)
Journal d'accès proxy et en-têtes HTTP
Personnalisation des noti7cations d'erreur avec les pages de noti7cation de l'utilisateurfinal (EUN)

Utilisation de l'authentification

Protocoles d'authentification
Domaines d'authentification
Suivi des informations d'identification de l'utilisateur
Mode proxy explicite (avant) ettransparent
Contournement de l'authentification avec des agents problématiques
Rapports et authentification
Nouvelle authentification
Authentification proxy FTP
Dépannage de la jonction de domaines ettest de l'authentification
Intégration avec Cisco Identity Services Engine (ISE)

Création de stratégies de déchiffrement pour contrôlerle trafic HTTPS

Présentation de l'inspection TLS (Transport Layer Security) / SSL (Secure Sockets Layer)
Présentation du certificat
Présentation des politiques de décryptage HTTPS
Activation de la fonction proxy HTTPS

03 20 61 95 06
formation@access-it.fr

Formation CISCO SWSA Sécuriser les accès Web avec Cisco Web Security Appliance

Durée de la formation : 2 jour(s) / 14 heure(s)

Balises de liste de contrôle d’accès (ACL) pour l’inspection HTTPS
Exemples de journaux d’accès

Comprendre les politiques d'accès au trafic différenciées etles profils d'identification

Présentation des politiques d’accès
Groupes de stratégies d’accès
Aperçu des profils d’identification
Profils d’identification et authentification
Ordonnance de traitement des politiques d’accès et des profils d’identification
Autres types de politiques
Exemples de journaux d’accès
Balises de décision ACL et groupes de stratégies
Application des stratégies d’utilisation acceptable en fonction du temps et du volume de trafic et des notifications aux utilisateurs finaux

Défense contre les logiciels malveillants

Filtres de réputation de sites Web
Analyse anti-malware
Analyse du trafic sortant
Anti-Malware etréputation dans les politiques
Filtrage de la réputation des fichiers et analyse des fichiers
Cisco Advanced Malware Protection
Fonctions de réputation et d’analyse de 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 catégorie d’URL
Moteur d’analyse de contenu dynamique
Visibilité et contrôle des applications Web
Application des limites de bande passante multimédia
Contrôle d’accès logiciel en tant que service (SaaS)
Filtrage du contenu pour adultes

Sécurité des données et prévention des pertes de données

Sécurité des données
Solution de sécurité des données Cisco
Définitions des politiques de sécurité des données
Journaux de sécurité des données

Administration et dépannage

Surveillez l’appliance de sécurité WebCisco
Rapports Cisco WSA
Surveillance de l’activité du système via des journaux
Tâches d’administration système

03 20 61 95 06
formation@access-it.fr

Formation CISCO SWSA Sécuriser les accès Web avec Cisco Web Security Appliance

Durée de la formation : 2 jour(s) / 14 heure(s)

Dépannage
Interface de ligne de commande

Références

Comparaison des modèles Cisco WSA
Comparaison des modèles Cisco SMA
Présentation de la connexion, de l'installation et de la configuration
Déploiement du modèle OVF (Open Virtualization Format) de Cisco Web Security Appliance
Mappage des ports de machine virtuelle (VM) de l'appliance de sécurité Web Cisco aux réseaux corrects
Connexion à l'appliance virtuelle Cisco Web Security
Activation du moniteur de trafic de couche 4 (L4TM)
Accès et exécution de l'assistant de configuration du système
Reconnexion à l'appliance de sécurité WebCisco
Présentation de la haute disponibilité
Redondance matérielle
Présentation du protocole CARP (Common Address Redundancy Protocol)
Configuration des groupes de basculement pour la haute disponibilité
Comparaison des fonctionnalités entre les options de redirection du trafic
Scénarios d'architecture lors du déploiement de Cisco AnyConnect® Secure Mobility

03 20 61 95 06
formation@access-it.fr

Formation CISCO SWSA Sécuriser les accès Web avec Cisco Web Security Appliance

Durée de la formation : 2 jour(s) / 14 heure(s)

Prise en compte du handicap
Pour les personnes en situation de handicap, afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous via notre formulaire de contact ou par mail (formation@access-it.fr) ou par téléphone (0320619506). Un entretien avec notre référente handicap pourra être programmé afin d'identifier les besoins et aménagements nécessaires.

Modalités et moyens Pédagogiques, techniques et d'encadrement mis en œuvre
Répartition théorie/pratique : 45%/55%. Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques s'articulant autour d'une application fil rouge, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
Formation accessible à distance de n'importe où et n'importe quand, via un ordinateur type PC disposant d'une connexion à Internet à haut débit (ADSL ou plus).
Pour assurer un démarrage dans les meilleures conditions au premier jour de la formation, notre service logistique se met systématiquement en relation, en amont, avec vous afin de réaliser un test de validation technique et de vous présenter l'environnement de formation.
Pendant toute la durée de la formation, le stagiaire dispose d'une assistance technique et pédagogique illimitée, par e-mail, avec un délai de prise en compte et de traitement qui n'excède pas 24h. En complément, le stagiaire peut planifier un rendez-vous pédagogique avec un formateur expert afin d'échanger sur des éléments de la formation.
La durée de la formation affichée sur cette page est une durée estimée qui peut varier en fonction du profil du stagiaire et de ses objectifs (notamment s'il souhaite valider sa formation par le passage d'un examen de certification).
Durant la formation, le formateur prévoit :
Des démonstrations organisées en modules et en séquences découpées le plus finement possible, en suivant le programme pédagogique détaillé sur cette page ;
Des énoncés et corrigés de travaux pratiques à réaliser tout au long de la formation ;
Des travaux pratiques sont proposés ; la plateforme prévoit l'environnement technique nécessaire à la réalisation de l'ensemble des travaux pratiques ;
Le formateur valide les connaissances acquises après chaque TP ;
Il est proposé un ou plusieurs livres numériques faisant office d'ouvrage(s) de référence sur le thème de la formation.

Validation et sanction de la formation
Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation par courrier électronique.
A la demande, il sera délivré un certificat de réalisation.

Type de formation
Professionnalisante ayant pour objectif le perfectionnement, l'élargissement des compétences

Moyens permettant de suivre l'exécution de l'action
Le contrôle de la présence des stagiaires sera assuré par la vérification de l'assiduité des participants. Le stagiaire signera une feuille de présence par demi-journée de formation. Celle-ci sera également signée par le formateur.

Modalité d'évaluation des acquis
Durant la formation, le participant est amené à mettre en pratique les éléments du cours par la réalisation de travaux pratiques réalisés sur PC.
La validation des acquis du stagiaire est faite par le formateur à la fin de chaque atelier. Cette validation individuelle est possible du fait du faible nombre de participants par session de formation (6 personnes maximum).
A la fin de la formation, le stagiaire a donc atteint les objectifs fixés par la formation.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par l'éditeur en passant un examen de certification.
Access it étant centre d'examen ENI, les examens peuvent être réalisés sur demande à distance ou dans nos locaux de Villeneuve d'Ascq.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification

Assistance Post-Formation
Toute personne ayant suivi une formation avec Access it bénéficie d'une assistance post-formation d'une durée de 1 mois. Ce nouveau service d'accompagnement permet aux stagiaires rencontrant des difficultés dans la mise en oeuvre des connaissances acquises de solliciter l'aide de nos formateurs sur des aspects relatifs aux programmes de formation suivis. Pour en bénéficier, il suffit de se rendre sur la page contact de notre site web et de remplir le formulaire. Une réponse est apportée par mail ou par téléphone dans un délai de 48 heures.

Centre d'Examen
Notre centre de formation agréé Qualiopi bénéficie de l'agrément d'ENI et ICDL pour les certifications informatiques. C'est pour nos clients la garantie de pouvoir suivre des formations préparant à des certifications professionnelles.

Aide à l'orientation
Pour chacune des grandes thématiques couvertes par notre offre de formation, nous proposons via nos spécialistes un rendez-vous physique ou téléphonique qui via un diagnostic permettra aux personnes souhaitant être accompagnées dans le choix d'un programme ou dans la définition d'un parcours de formation une orientation vers les programmes les plus adaptés à leurs besoins et à leur niveau.

Aspects Pratiques
Dès leur inscription, les participants sont contactés par nos services qui s'assurent que les débits internet constatés sur le lieu depuis lequel ils souhaitent se former sont suffisants pour suivre la formation dans des conditions optimales.
À l'occasion de cet appel, nos experts s'assurent également qu'ils disposent du matériel nécessaire pour suivre la formation (PC Portable, webcam, Micro-casque..).
Avant le début de la formation, les participants reçoivent un lien leur permettant d'accéder à la classe virtuelle et leurs identifiants personnels de connexion. Un aide à l'utilisation de la solution de visioconférence utilisée leur est également proposée.
Le jour de la formation, ils se connectent à la classe virtuelle depuis leur navigateur internet. Ils voient et entendent le formateur ainsi que les autres participants et peuvent à tout moment communiquer avec eux.
Ils participent aux échanges et réalisent les ateliers dans les mêmes conditions que s'ils étaient en salle. Grâce à nos outils de prise en main à distance, les formateurs peuvent à tout moment prendre la main sur leurs postes pour les aider ou vérifier leurs TP.
Tout au long de la formation, les participants peuvent bénéficier de l'assistance immédiate de nos experts en composant le numéro qui leur a été communiqué avant la formation.
Des bilans intermédiaires ont lieu en présence des participants du formateur et du référent pédagogique d'Access it afin de vérifier l'état d'avancement de la session, les difficultés rencontrées et permettre d'éventuels actions correctives.

Bénéfices pour les participants
Se former depuis leur lieu de travail ou leur domicile,
Accéder sans se déplacer à la qualité d'une formation délivrée par un formateur consultant ayant une expérience probante sur le sujet animé.
Bénéficier à distance de la richesse d'une formation interentreprises : échanges avec le formateur et les autres participants, partages d'expériences, ateliers pratiques…
Pouvoir se former en toutes circonstances et notamment en cas d'imprévus.

Bénéfices pour l'entreprise
Optimiser ses budgets en limitant les frais de déplacement et d'hébergement.
Proposer à tous ses collaborateurs, quelle que soit leur situation géographique, des formations de qualité (en Inter comme en Intra).
Limiter les temps de déplacement.
Proposer davantage de choix dans les formations à des collaborateurs peu mobiles.
Assurer la montée en compétences de ses collaborateurs quelles que soient les circonstances