Sécuriser le Web avec Cisco Web Security Appliance

Durée: 2 Jours **Réf de cours: SWSA** **Version: 3.0**

Résumé:

Apprenez à mettre en œuvre, 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 œuvre des stratégies pour contrôler le trafic et l'accès HTTPS, à mettre en œuvre des paramètres et des stratégies de contrôle d'utilisation, à utiliser les fonctionnalités anti-malware de la solution, à mettre en œuvre la sécurité des données et la prévention contre les pertes de données, à réaliser l'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.
Mis à jour 15/01/2024

Public visé:

Ce cours s'adresse aux personnes travaillant sur le déploiement, l'installation et l'administration de l'Appliance Cisco Web Security.

Objectifs pédagogiques:

- **A l'issue de ce cours, les stagiaires seront en mesure de :**
- Décrire Cisco WSA
- Déployer les services proxy
- Utiliser l'authentification
- Décrire les stratégies de décryptage pour contrôler le trafic HTTPS
- Comprendre les stratégies d'accès au trafic différencié et les profils d'identification
- Appliquer des paramètres de contrôle d'utilisation acceptable
- Se défendre contre les malwares
- Décrire la sécurité des données et la prévention contre la perte des données
- Réaliser l'administration et le dépannage

Pré-requis:

Les connaissances et les compétences nécessaires avant de suivre cette formation sont :

- Les services TCP/IP, y compris le DNS (Domain Name System), FTP, SNMP (Simple Network Management Protocol), HTTP et HTTPS
- Le routage IP
- Le CCNA est recommandé
- Une certification industrielle adéquate ISC)2, (CompTIA) Security+, EC-Council, GIAC, ISACA
- Une expertise Windows : Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)
- G013 - Formation CompTIA Security+
- ICND1 - Interconnexion de réseaux Cisco - ICND1
- IINS - Mettre en oeuvre la sécurité des réseaux Cisco
- SCOR - Mettre en oeuvre et gérer les solutions de sécurité Cisco
- SFNDU - Understanding Cisco Security Foundations

Test et certification

Cette formation prépare au passage de l'examen suivant :

300-725 - Securing the Web with Cisco Web Security Appliance

La réussite de l'examen comptera comme électif pour atteindre la certification de sécurité CCNP et fournira le titre de spécialiste certifié Cisco - Certification de sécurité du contenu Web.

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

Les stagiaires qui suivent la formation SWSA peuvent être intéressés par le cours :

- SESA - Securing your Email with Cisco Email Security Appliance

Contenu:

Description de Cisco WSA

- Cas d'usage de la technologie
- La solution Cisco WSA
- Les fonctionnalités de Cisco WSA
- L'architecture de Cisco WSA
- Le service de Proxy
- Le contrôle intégré du trafic de la couche 4
- La prévention contre les pertes de données
- Cisco Cognitive Intelligence
- Les outils de gestion
- Le reporting AWSR (Advanced Web Security Reporting) et l'intégration tierce partie
- L'appliance Cisco Content Security Management (SMA)

Déploiement des services Proxy

- Expliquer le mode Forward versus le mode Transparent
- Redirection du trafic en mode transparent
- Le protocole de contrôle du cache Web
- Flux ascendant et descendant du protocole WCCP (Web Cache Communication Protocol)
- Le proxy Bypass
- La mise en cache du proxy
- Les fichiers PAC (Proxy Auto-Config)
- Le proxy FTP
- Le proxy SOCKS (Socket Secure)
- Les logs d'accès du proxy et les entêtes http
- La personnalisation des notifications d'erreurs avec les pages EUN (End User Notification)

Utilisation de l'authentification

- Les protocoles d'authentification
- Les domaines d'authentification
- Les credentials de tracking des utilisateurs
- Les modes proxy explicite (Forward) et transparent
- Le contournement de l'authentification avec les agents à problème
- Reporting et authentification
- Re-authentification
- L'authentification Proxy FTP
- Résolution des problèmes liés à la jonction de domaines et au test d'authentification
- Intégration avec ISE (Cisco Identity Services Engine)

Création de stratégies de décryptage pour contrôler le trafic HTPPS

- Vue d'ensemble des protocoles TLS (Transport Layer Security) / SSL (Secure Sockets Layer)
- Vue d'ensemble des certificats
- Vue d'ensemble des stratégies de décryptage HTTPS
- Activation de la fonction Proxy HTTPS

Comprendre les stratégies d'accès au trafic différencié et aux profils d'identification

- Vue d'ensemble des stratégies d'accès
- Les stratégies de groupe d'accès
- Vue d'ensemble des profils d'identification
- Profils d'identification et authentification
- Stratégie d'accès et ordre de traitement des profils d'identification
- Autres types de stratégies
- Les tags de décision ACL et les stratégies de groupe
- L'application de stratégies d'utilisation basée sur le temps et le trafic de volume acceptable et les notifications End-User

Se défendre contre les malwares

- Les filtres basés sur la réputation des sites Web
- Le scanning Anti-Malware
- Scan du trafic sortant
- Anti-malware et réputation dans les stratégies
- Filtrage de fichiers et analyse de fichiers
- Protection avancée contre les malwares
- Fonctionnalités d'analyse et de réputation des fichiers
- Intégration avec Cisco Cognitive Intelligence

Application des paramètres acceptables de contrôle d'utilisation

- Contrôle de l'utilisation du web
- Filtrage d'URL
- Solutions par catégorie d'URL
- Moteur d'analyse de contenu intelligent
- Visibilité et contrôle des applications Web
- Application de limites de bandes passantes pour les media
- Contrôle de l'accès SaaS (Software as a Service)
- Filtrage du contenu pour adulte

Sécurité des données et prévention contre la perte de données

- Sécurité des données
- Solutions Cisco de sécurité des données
- Définition des stratégies de sécurité des données
- Journaux de sécurité des données

Administration et dépannage

- Surveillance de l'appliance Cisco Web Security
- Rapports Cisco WSA
- Surveillances de l'activité système aux travers des journaux
- Dépannage
- Interface ligne de commande

Travaux Pratiques

- Lab 1: Configurer l'appliance Cisco Web Security
- Lab 2: Déployer les services Proxy
- Lab 3: Configurer l'authentification Proxy
- Lab 4: Configurer l'inspection HTTPS
- Lab 5: Créer et appliquer une stratégie d'utilisation basée sur le temps/la date
- Lab 6: Configurer la protection avancée contre les Malwares
- Lab 7: Configurer les exceptions basées sur l'entête
- Lab 8: Utiliser les flux de sécurité tierce partie et les flux externes MS Office 365
- Lab 9: Valider un certificat intermédiaire
- Lab 10: Visualiser les services de reporting et la traçabilité Web
- Lab 11: Réaliser la mise à jour centralisée du logiciel Cisco AsyncOS en utilisant Cisco SMA

- Les tags ACL (Access Control List) pour inspecter HTPPS
- Exemples de journaux d'accès

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Un support de cours officiel sera remis aux stagiaires.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement