Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Vous pouvez nous joindre ici

.

Email: training.ecs.fr@arrow.com
Phone: 01 49 97 50 00

Sophos Certified Architect - XG

CODE:	DURÉE:	PRIX H.T.:
SOP_SCA-XG	24 Hours (3 Jours)	€1,800.00

Description

Ce cours comporte des parties théoriques et des travaux pratiques permettant de comprendre le fonctionnent du XG firewall de Sophos.

Objectifs

· - Comprendre les différents modes de déploiement du XG
· - Les protocoles de routages utilisés, l'agrégation de liens et l'usage de VLANs
· - Aperçu de l'inspection stateful et des politiques strictes· - FastPath/IPS/anti-DOS/Flooding/ATP
· - Reverse proxy et authentification : publication de serveurs et utilisation de templates
· - La gestion d'authentifications SSO, LDAP, NTLM et les nouveaux agents
o Sophos Transparent Authentication Suite - STASo Sophos Authentication for Thin Clients - SATC
· - Gestion de sites distants avec RED (Remote ethernet device)
· - Gestion sans fil d'Access Points Sophos et des hotspots· - Les différents modes d'utilisation VPNo Distant
o Site-à-siteo Hôte-à-hôte· - Utilisation de la haute disponibilité
· - Modules dédiés au dépannage, SF Loader et au dimensionnement

L'obtention de la certification se fait par un passage d'examen en ligne au travers du portail partenaire Sophos

b. L'évaluation se fait sur différents types de questions

1. Sur des scénarii évoqués en cours
2. Sur le contenu du cours
3. Sur le contenu des travaux pratiques

c. 3 passages de certification sont possibles

Audience

Partenaires Sophos

Prérequis

1. Avoir passé la certification Certitied Engineer Sophos XG Firewall
2. Avoir des connaissances en réseau et sécurité informatique
3. Avoir une expérience de configuration d'équipements réseau
4. Être capable de dépanner des environnements Windows en réseau
5. Avoir une expérience d'administration et de configuration de systèmes Linux/UNIX

Programme

Module 1: Enterprise Deployment Scenarios
Module 2: Advanced Firewall
Module 3: Authentication
Labs 1 - 3
Module 4: Webserver Protection
Module 5: RED Management
6Module 6: Wireless Protection
Labs 4 - 6
Module 7: Enterprise VPN
Module 8: High Availability
Module 9: Troubleshooting
Labs 7 - 9

Déroulé du cours sur les 3 jours Module 10: Sizing **Détails des TP :** • Lab 1: Déploiement
? Enregistrements pour évaluation des numéros de série et activation des passerelles
? Configuration de la passerelle en bridge de niveau 2 et 3? Configuration des réseaux, interfaces et zones
? Configuration du routage à plusieurs chemin et de l'uplink balancing• Lab 2: Network Protection
? Visualisation de la table de connexions? Utilisation de l'outil de capture de paquet en ligne de commande
• Lab 3: Webserver Protection? Configuration d'un reverse proxy
? Configuration de load balancing et du routage de site path? Configuration de la reverse authentification pour un site web
• Lab 4: Authentification? Intégration Active Directory? Configuration du single sign-on• Lab 5: RED
? Activation RED? Configuration d'un tunnel RED tunnel? Connexion d'un boitier RED• Lab 6: Wireless
? Configuration de réseaux sans fil? Connexion d'un access point? Configuration d'un réseau maillé
? Configuration d'une authentification RADIUS? Création d'un hotspot• Lab 7: VPNs
? Configuration de VPNs site-à-site avec des clés RSA? Configuration du failover VPN
? Configuration du NAT dans le VPN? Revue des journaux d'événements VPN• Lab 8: HA
? Activation de la haute dispo en actif-actif entre deux passerelles Sophos• Lab 9: SF Loader
? Remise à zéro du mot de passe administrateur depuis le SF Loader
? Procéder à des tests de performances disque et mémoires depuis le SF Loader

Dates de session

Sur demande. Merci de nous contacter

Informations Complémentaires

Cette formation est également disponible sous forme de formation sur site. Veuillez nous contacter pour en savoir plus.