TRAINING OFFERING

Vous pouvez nous joindre ici

.

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

SOPHOS   SG UTM : Administrator

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

Description

This course is designed for technical professionals who will be administering Sophos SG UTM and provides the skills necessary to manage common day-to-day tasks.
It consists of presentations and practical lab exercises to reinforce the taught content, and electronic copies of the supporting documents for the course will be provided to each trainee through the online portal.
The course is expected to take 2 days to complete, of which approximately half will be spent on the practical exercises.

Objectifs

On completion of this course, trainees will be able to:
? Recognize the main technical capabilities and how they protect against threats? Complete common configuration tasks
? Backup and restore the system? Complete common day-to-day tasks? View and manage logs and reports

Training Development

Lab Environment
Each student will be provided with a pre-configured environment which simulates a company network with two sites, a head office and a branch office and contains Windows Servers and two SG UTMs.

Prérequis

There are no prerequisites for this course; however it is recommended that trainees should:
? Have networking knowledge equivalent to CompTIA N+ or better? Be familiar with security best practices
? Be able to setup a Windows server? Have experience of configuring and managing network gateway devices
? Have knowledge of general Windows networking and Microsoft Active Directory
If you are uncertain whether you meet the necessary prerequisites to take this course, please email us at training.ecs.fr@arrow.com and we will be happy to help.

Programme

Module 1: Security Threats and how the UTM Protects Against Them ? Identify common threats
? Recognize the protection provided by Sophos UTM**Module 2: Getting Started with XG Firewall**
? Perform basic system configuration? Create network, service and time definitions? Configure interfaces on the UTM
? Configure how multiple Internet links are used by the UTM? Labs? Configure a UTM using the Setup Wizard
? Navigate the WebAdmin? Configure system settings? Create definitions? Configure interfaces and routing
Module 3: Network Protection ? Create firewall and NAT rules
? Configure intrusion prevention and Advanced Threat Protection (ATP)? Labs? Create firewall rules? Configure NATing
? Demonstrate Advanced Threat Protection? Configure Intrusion Prevention (IPS)**Module 4: Site-to-Site Connections**
? Explain the VPN options available for site-to-site connections? Configure an SSL and IPsec site-to-site VPN
? Understand RED deployment and configuration? Labs? Configure an SSL site-to-site VPN? Configure an IPsec site-to-site VPN
Module 5: Authentication ? Describe the authentication methods available on the UTM? Configure local users and groups
? Enable directory services authentication? Configure single sign-on for web filtering? Enable one-time passwords? Labs (40 mins)
? Configure local authentication and the User Portal? Configure external authentication using Active Directory
? Enable one-time passwords? Configure Active Directory SSO for web filtering
Module 6: Web Protection and Application Control ? Describe the main features in the Web Protection module
? Configure web filtering with multiple policies? Enable Application Control and create rules to block applications? Labs
? Deploy the HTTPS CA certificate? Configure Filter Actions? Manage Websites? Configure Web Policies? Configure Web Profiles
? Configure Application Control**Module 7: Email Protection** ? Enable the Quarantine Report? Configure simple Email Protection

? Configure Data Protection? Configure SPX encryption? Configure SMTP Profiles? Labs (65 mins)
? Enable and configure quarantine digests? Configure an Email Protection Policy for MTA mode
? Encrypt emails that match a Data Control List using SPX? Manage quarantined items as a user
Module 8: Wireless and Remote Access ? Describe the main capabilities of Wireless Protection
? Configure wireless access points? Create hotspots? Configure SSL remote access? Enable the HTML5 VPN portal
? Describe support for native Cisco VPN clients? Labs (25 mins)? Configure an SSL remote access VPN
? Configure the HTML5 VPN Portal**Module 9: Endpoint Protection and Mobile Control** ? Install and launch the endpoint client
? Manage protected endpoints? Describe the integration between Sophos Mobile Control and the UTM
? List the types of configuration that can be pushed to Sophos Mobile Control
Module 10: Logging, Reporting and Troubleshooting? Understand remote monitoring and managing in the UTM
? Examine options for logging? Understand on-box reporting and iView? Examine available troubleshooting tools? Labs (30 mins)
? Run, customize and schedule reports? View and manage log files? Use built-in support tools

Options

Certification
To become a Sophos Certified Administrator, trainees must take and pass an online assessment. The assessment tests their knowledge of both the presented and practical content. The pass mark for the assessment is 80%, and is limited to 4 attempts.

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.