Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Symantec Web Protection – Edge SWG Administration R2

CODE:	LENGTH:	PRICE:
SYM_000269	32 Hours (4 days)	€3,000.00

Description

The Symantec Web Protection—Edge SWG Administration R2 course provides a detailed introduction to the features that comprise Edge SWG, which is the on-premise component of Symantec Network Protection.
These applications include Edge SWG (Edge SWG), Management Center, Reporter, Content Analysis, and High Risk Isolation.
This course includes practical hands-on exercises that enable students to test their understanding of the concepts presented in the lessons.

Objectives

By the completion of this course, you will be able to:

- Describe the major Edge SWG functions and capabilities
- Write policies to defend enterprise networks against malware attacks and to enforce acceptable Internet browsing behavior
- Understand how the various applications work together to secure enterprise networks
- View reports and monitor solution performance

Prerequisites

- Basic understanding of networking concepts
- Basic understanding of network security concepts
- Basic understanding of the use of proxy servers

Programme

Module 1: Introduction to Symantec Edge SWG

- Overview of Web Protection Suite
- Overview of Edge SWG components

Module 2:
Intercepting web traffic and applying policy

- How the ProxySG intercepts traffic
- Writing policy on the ProxySG
- Layer and rule evaluation order in the VPM
- Inform users when web access is denied or restricted due to policy

Module 3:
Applying security and web usage policy to encrypted traffic

- Introduction to TLS
- Managing HTTPS traffic on the ProxySG

Module 4:
Centrally managing devices with Management Center

- How Management Center centralizes and simplifies device management

- Configuring the ProxySG with the ProxySG Admin Console
- Creating and distributing VPM policies
- Creating and managing jobs
- Use reports to analyze web browsing activity

Module 5:
Providing security and web usage policies based on role or group

- Authentication basics on the ProxySG
- Using IWA authentication on the ProxySG
- Authentication modes in explicit and transparent modes
- Connecting to the Windows domain directly using IWA direct
- Connecting to the Windows domain using IWA BCAAA
- Using roles and groups in policy

Module 6:
Enforcing corporate guidelines for acceptable Internet browsing behavior

- Create strong corporate guidelines for acceptable Internet use
- Use website categorization to enforce acceptable use guidelines
- Provide the ProxySG with categorization databases to be referenced in policy
- Set the Request URL Category object in policy to enforce acceptable use guidelines

Module 7:
Protecting the endpoint from malicious activity

- WebPulse technical details
- Introduction to Intelligence Services
- Using Intelligence Services data feeds in policy
- Ensuring safe downloads

Module 8:
Providing security for risky and unknown websites with High Risk Isolation

- Introduction to High Risk Isolation
- Configuring HRI
- Overview of Symantec Web Isolation

Module 9:
Enhancing security with virus scanning

- Introduction to Content Analysis
- Exploring the Content Analysis management console
- Configuring communication with the ProxySG over ICAP
- Configuring malware scanning options

Module 10:
Using malware analysis to analyze potentially malicious files

- Introduction to malware analysis
- Preparing the use malware analysis
- Performing malware analysis

Module 11:
Monitoring Edge SWG features

- Monitoring devices from within Management Center
- Monitor and maintain the Content Analysis
- Troubleshooting tips

Module 12:
Reporting for Edge SWG features

- How Reporter delivers centralized web reporting
- Configuring access logging on Edge SWG
- Using the Reporter Admin Console to configure log processing on Reporter

Module 13:
Understanding SGOS architecture and caching on the Edge SWG

- SGOS architecture

- Caching on the Edge SWG
- Using HTTP compression

Module 14:
Using built-in diagnostic tools on the Edge SWG

- Exploring sysinfo files
- Using policy tracing and policy coverage
- Using packet captures
- Sending service information to Symantec

Module 15:
Expanding security with cloud integrations

- Introduction to Cloud SWG
- Using Universal Policy Enforcement
- Integrating CloudSOC with Symantec Network Protection

Module 16:
Course review

- Symantec Web Protection--Edge SWG Administration R2 course review

Appendix A:
Using Content Policy Language (CPL)

- SSP hardware platform overview
- Introduction to ISG

Appendix B:
Using Content Policy Language (CPL)

- Basic CPL concepts
- Intermediate CPL concepts
- Using CPL best practices

Appendix C:
Introduction to Hypertext Transport Protocol (HTTP)

- Basic HTTP concepts

Follow on courses

Additional Courses Available

- Web Protection Cloud SWG – Administration R2
- Web Protection Cloud SWG – Diagnostics and Troubleshooting R2
- Web Protection Edge SWG – Diagnostics and Troubleshooting R2

Test and Certification

The 250-589: Symantec Web Protection – Edge SWG R2 Technical Specialist certification exam includes content from this course and its companion course, Symantec Web Protection – Edge SWG Diagnostics & Troubleshooting R2
Available at an additional cost.

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.