Training: Broadcom

Web Protection - Edge SWG Planning, Implementation, and Administration

TRAINING GOALS:

The Symantec Web Protection—Edge SWG Planning, Implementation, and Administration course provides a detailed introduction to the features that comprise Edge SWG, which is the on-premise component of Symantec Web Protection. These applications include ProxySG, Management Center, Reporter, Content Analysis, and High Risk Isolation.

Course 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

This course includes practical hands-on exercises that enable students to test their understanding of the concepts presented in the lessons.

CONSPECT:

- 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
- Module 3: Applying security and web usage policy to encrypted traffic
  - Introduction to TLS
  - Managing HTTPS traffic on the ProxySG
- Module 4: Providing security and web usage policies based on role or group
  - Authentication basics on the ProxySG

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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 5: 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
  - Inform users when web access is denied or restricted due to policy
- Module 6: Protecting the endpoint from malicious activity
  - WebPulse technical details
  - Introduction to Intelligence Services
  - Using Intelligence Services data feeds in policy
  - Ensuring safe downloads
- Module 7: 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 8: Reporting for Edge SWG features
  - How Reporter delivers centralized web reporting
  - Configuring access logging on the ProxySG
  - Using the Reporter Admin Console to configure log processing on Reporter
- 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: Providing security for risky and unknown websites with High Risk Isolation

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

    - Introduction to High Risk Isolation
    - Configuring HRI
    - Overview of Symantec Web Isolation
- Module 12: Monitoring Edge SWG features
    - Monitoring devices from within Management Center
    - Monitor and maintain the Content Analysis
    - Troubleshooting tips
- 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 Web Protection
- Module 16: Course review
    - Symantec Web Protection--Edge SWG Planning, Implementation, and Administration course review
- Appendix A: Using Content Policy Language (CPL)
    - Basic CPL concepts
    - Intermediate CPL concepts
    - Using CPL best practices
- Appendix B: Introduction to Hypertext Transport Protocol (HTTP)
    - Basic HTTP concepts

REQUIREMENTS:

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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Broadcom. (course completion)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007