BROADCOM SOFTWARE

Course Description

Symantec Web Protection - Cloud SWG Planning, Implementation, and Administration R1

Course Code: 000208

Course Description

The Symantec Web Protection - Cloud SWG Planning, Implementation, and Administration course is intended for IT professionals who will be planning, installing, configuring or administering the Symantec Cloud Secure Web Gateway.

Delivery Method

Instructor-Led

Duration

Two Days

Course Objectives

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

- Describe the architecture, components and process flow of Cloud SWG
- Identify installation, configuration and administration of the core features and products of Cloud SWG.
- Identify the key elements for planning a Cloud SWG deployment

Labs

- Lab Login and Cloud SWG Portal Introduction
- Install and Explore the WSS Agent
- Create a Bypass List
- Create a Custom PAC File for Remote Locations
- Implement Web and Cloud Access Protection Integration
- Install Auth Connector
- Create and Deploy Policies to Limit Social Media Use
- Create a Source Geography based Policy to Ensure Save Internet Usage
- Create a Customized Response Page
- Block Sites Based on Risk Level
- Improved Administration with Cloud SWG Reporting Tools

Hands-On

This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

Prerequisites

- Working knowledge of cloud based solutions
- Knowledge of internet traffic protocols
- Basic understanding of principles of authentication

Additional Courses Available

- Web Protection Cloud SWG – Diagnostics and Troubleshooting
- Web Protection Edge SWG – Planning, Implementation, and Administration

Certification

Exam 250-554: Administration of Symantec Web Security Service – R1.2

Course Outline

Module 1: Cloud Delivered Security

- What is Cloud Delivered Security
- What are the Key Considerations for Having Cloud Delivered Security
- What are the Key Features Needed for Cloud Delivered Security

Module 2: Cloud SWG Connection Architecture and Functionality

- Cloud SWG Infrastructure
- Cloud SWG Connection Architecture
- Cloud SWG Features
- Cloud SWG Additional Products

Module 3: Getting Started with Cloud SWG

- Initial Registration
- User Administration
- Licensing
- Data Privacy Settings

Module 4: Enable Remote Users to Securely Access the Internet

- Remote Users and Solutions
- WSS Agent Access Method
- Web and Cloud Access Protection Access Method
- Cloud Connect Defense (CCD) Access

Module 5: Provide Safe and Proper Web Usage Based on User Identity

- Authentication and Cloud SWG
- Auth Connector
- SAML
- Remote Authentication Methods with Auth Connector
- Authentication with WSS Agent and Web and Cloud Access Protection Access Methods

Module 6: Create a more Effective Work Environment for Employee Web Usage

- Configure Content Filtering Rules to Determine Internet Usage
- Setting Global Content Filtering Policy Rules
- Creating Custom Response Pages
- Universal Policy Enforcement

Module 7: Providing Web Protection Against Malware

- Cloud SWG Threat Protection
- Malware Analysis and Cloud SWG
- Threat Protection Policies
- Creating Threat Protection Policy Rules

Module 8: Enable Encrypted Traffic Inspection

- Encrypted Traffic
- SSL Configuration
- Configuring SSL Exceptions
- Topic Title

Module 9: Enable Corporate Users to Securely Access the Internet

- Firewall/VPN (IPsec) Access Method
- FQDN-IKEv2 Firewall Access Method
- TransProxy (Explicit Proxy Over IPsec) Access Method
- Proxy Forwarding Access Method

Module 10: Identify Web Usage and Security Statistics with Reports

- Reports Overview
- Pre-defined Reports
- Simple Reporting
- Custom Reporting
- Forensic Reporting

- Managing and Using Reports

Module 11: Enable Mobile Users to Securely Access the Internet

- About Mobile Device Security
- Authentication for Mobile Users
- SEP-Mobile Solution
- Android Mobile Access Enrollment Process

Module 12: Planning Cloud SWG Deployments

- Assessment of Needs
- Design – Access Methods and Authentication
- Design – Policy, Reporting and Threat Protection
- Design Evaluation