MOC 50357 B Implementing Forefront Threat Management Gateway 2010

Course Summary

Description

This course provides students with the knowledge and skills to envision, design, and deploy web access, remote access and mail protection solutions using Microsoft Forefront Threat Management Gateway 2010 (TMG), enabling them to identify the requirements and make the appropriate design decisions that will come up during the deployment process, and providing hands-on experience with the products.

Objectives

At the end of this course, students will be able to:

- Understand the new features and the value proposition for Forefront TMG.
- Explain how Forefront TMG protects clients and servers from Web-based threats.
- Describe how Forefront TMG enable outside systems to secure connect to internal services and applications.
- Describe how Forefront TMG integrates with Forefront Protection 2010 for Exchange and Microsoft Exchange Server 2010 to protect an organization from mail-based threats.
- Design an enterprise solution using Forefront TMG considering availability, scalability, operations, and migration from an existing Microsoft Internet Security and Acceleration (ISA) solution.

Topics

- Forefront Threat Management Gateway (TMG) 2010 Overview
- Secure Web Gateway
- Remote Access Gateway
- Secure Mail Relay
- Forefront TMG 2010 Design and Deployment Considerations

Audience

This course is intended for Architects, Consultants, and Technical Sales Professionals involved in designing, deploying, or operating security solutions.

Prerequisites

Before attending this course, students must have:

- A good understanding of Active Directory and Group Policies.
- A good understanding of Windows TCP/IP networking.

Duration

Two days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

MOC 50357 B Implementing Forefront Threat Management Gateway 2010

Course Outline

I. Forefront Threat Management Gateway (TMG) 2010 Overview

This module explains the new features introduced in Forefront TMG 2010, the different deployment scenarios for the product, and introduces the basic concepts used in its configuration.

A. Introduction to Forefront TMG
B. Installation and Initial Setup
C. Basic Configuration Concepts

Lab: Installing Forefront Threat Management Gateway 2010

- Install Forefront TMG on a Windows Server 2008 R2 server
- Perform an initial configuration of Forefront TMG using the Getting Started wizards

After completing this module, students will be able to:

- Describe a brief history of the Microsoft edge security products.
- Explain the current threat landscape and how this drove changes in the edge security strategy.
- List the new features in Forefront TMG and their value propositions.
- Describe the key scenarios for Forefront TMG and how it differentiates from Microsoft IAG/UAG.
- Describe the SKU differentiation and subscription model.
- Explain the installation requirements and install process for Forefront TMG.

II. Secure Web Gateway

This module explains the new features introduced in Forefront TMG 2010, and how they can be used to enable users to securely and safely browse the Web.

A. Secure Web Gateway Overview
B. HTTPS Inspection
C. URL Filtering
D. Malware Protection
E. Intrusion Prevention

Lab: Secure Web Gateway

- Create web access policies for Contoso users, including inspection of HTTPS sessions
- Modify web access policy to include protection from malware
- Investigate the Network Inspection System (NIS)

After completing this module, students will be able to:

- Describe the threats affecting enterprise users browsing the Web.
- Identify the key Forefront TMG features that address those threats (application proxy, granular access control, malware inspection, URL filtering, HTTPS inspection, NIS), and describe each of these features in detail.

III. Remote Access Gateway

This module explains the new features introduced in Forefront TMG 2010 can be used to enable users to securely access corporate network resources from anywhere.

A. Remote Access Gateway Overview
B. Non-HTTP Server Publishing
C. Web Publishing
D. Virtual Private Networking (VPN) Connectivity

Lab: Remote Access Gateway

- Use Web Publishing to publish Exchange Web Services

After completing this module, students will be able to:

- Understand how Forefront TMG can publish Web and non-Web services to external users.
- Explain the security features and benefits added by Forefront TMG in each of these publishing scenarios.
- Discuss the new Forefront TMG features for virtual private networking, such as Secure Socket Tunneling Protocol (SSTP) and Network Access Protection (NAP).

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

MOC 50357 B Implementing Forefront Threat Management Gateway 2010

Course Outline (cont'd)

IV. Secure Mail Relay
This module explains how Forefront TMG 2010 and Forefront Protection 2010 for Exchange Server can work together with Microsoft Exchange Server to provide premium protection from spam and malware.

A. Secure Mail Relay Overview
B. Solution Components
C. Configuring SMTP Protection

Lab: Secure Mail Relay

- Install Active Directory LDS and Exchange Edge Server
- Install Forefront Protection 2010 for Exchange Server
- Install Forefront Threat Management Gateway
- Configure Exchange EdgeSync
- Define an E-mail Policy

After completing this module, students will be able to:

- Describe the mail threats facing organization, and explain what the key Forefront TMG features are that address these threats.
- Explain how Forefront TMG and Forefront Protection 2010 for Exchange Server are deployed together for premium antispam and antimalware protection.
- Describe in detail how Forefront TMG performs spam filtering, malware filtering, and content filtering.
- Describe the implementation process for this scenario and how the solution is configured.

V. Forefront TMG 2010 Design and Deployment Considerations
This module explains the common deployment scenarios for Forefront TMG 2010, and what to consider when designing Forefront TMG 2010 solutions.

A. Logical Design Considerations
B. Scalability and Availability
C. Client Configuration
D. Migration Options

After completing this module, students will be able to:

- Review the network, scalability, availability and operational considerations and best practices when designing and deploying a solution based on Forefront TMG.
- Identify the best practices when configuring clients to use Forefront TMG.
- Describe migration procedures from ISA Server to Forefront TMG, and between the different versions of Forefront TMG.

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically