

Anti-virus Administration for WebShield

The prevalence of viruses today – and living with the resulting constant threat – has created the need for new security products and strategies. This course is specifically designed for individuals who implement gateway-scanning solutions, such as the WebShield 3.0 and SpamKiller products. Learn how to protect your network from email viruses, Web Site risks, and unwanted Spam. Learn how to use these perimeter-designed products in a live network setting.



Skill Building

Before taking this class we recommend that participants have a general understanding of LAN technologies, TCP/IP and Windows operating systems, and the ability to demonstrate basic networking skills.

Exercises

All topics are supported by hands-on exercises specifically designed to increase knowledge retention. Classroom exercises provide the basic hands-on experience needed to install, configure, and manage McAfee anti-virus products.

Course Materials

- Student Manual

Duration

- Two Days

Students Learn To

- Identify how viruses can affect a network when found at the mail server and gateway
- Describe the importance of multi-layer defense systems
- Install and configure WebShield 3.0 Appliance
- Install and configure SpamKiller for the WebShield 3.0 Appliance
- Describe the difference between Explicit Proxy, Transparent Bridging, and Transparent Routing
- Install an WS3100, WS3200 or WS3300 to a network and see how it scans for viruses and other malicious code
- Configure the WebShield Appliance for Explicit Proxy
- Configure WebShield Appliance for Transparent Bridging

Suggested Next Course

To gain a core set of skills and knowledge on anti-virus management, participants may also choose to attend:

- McAfee Intranet Defense: VirusScan and ePolicy Orchestrator (TRN-AVD-101-TCL)
- Anti-virus Administration for GroupShield (TRN-AVD-201-TCL)

Contact Information

Phone: 866-210-2715

E-mail: education@mcafee.com

Website: www.mcafee.com

Daily Outline

Day 1

WebShield Appliance WS3100, WS3200, and WS3300

- Quarantined email features
- Networking Essentials
- Overview - Firewalls, DMZ zones, Firewall rules, Routers
- Overview – DNS, Internet communication, Proxies
- The Appliance Concept
- Common features
- Hardware and software
- Basic Configuration of the Appliance
- Logging onto the Appliance
- Configuring the Inside Network, Outside Network
- Changing the password and time configuration
- System status and System Profiles
- Lab: Setup the basic configuration of the Appliance
- Appliance Implementation
- Explicit Proxy, Transparent Bridging, Transparent Routing
- When to use Explicit Proxy and how to configure Explicit Proxy
- When to use Transparent Bridging and how to configure Transparent Bridging
- SMTP configuration
- Configure Exchange to route to the Appliance
- Configure DNS to send SMTP to the Appliance
- Configure the Appliance for SMTP Explicit Proxy
- Configure SMTP disclaimers
- Configure Performance SMTP tuning
- Configure the SMTP Anti-Relay
- Deferred email features
- Routing Characters
- Updating Anti-Virus and Anti-Spam
- Gathering Throughput Statistics
- Lab: Basic SMTP configuration for Explicit Proxy
- Lab: Testing configuration
- Advanced SMTP Configuration
- Content Filtering for SMTP, Creating Rules
- Attachment filtering configuration
- Anti-Spam Configuration
- Using a Real-time Black-Hole list
- Using SpamKiller add-on
- Understanding SpamKiller features
- Lab: Testing the SMTP for Anti-Virus
- Lab: Create a Content Blocking rule
- Lab: Testing the Content Blocking rule Lab: Create an Attachment Blocking Rule
- Lab: Testing the Attachment Blocking Rule

Day 2

- Understanding Sub-Policies
- Policy-Groups
- Individual Groups and LDAP
- Lab: URL-Blocking
- Comfort-Pages and Data-Trickling
- Lab: Message Splitting
- Lab: Configure SpamKiller on the Appliance and configure the Outlook client for Junk email
- Lab: Test the SpamKiller configuration
- Lab: Configure SpamKiller to block all spam
- Lab: Test SpamKiller configuration
- Lab: LDAP-Configuration and Integration
- Load-Sharing
- Lab: Configure Load-Sharing
- Logs and Alert-Viewer
- Importing and Exporting Data
- Backup and Restoring Configuration
- ePolicy Orchestrator and the Appliance
- Lab: Installing the ePO agent onto the Appliance
- Lab: Configure the Appliance in ePO
- Lab: Reporting on the Appliance in ePO
- Advanced Scenarios