Configuring BIG-IP APM: Access Policy Manager v.17.5 Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

This course covers three typical deployment scenarios for BIG-IP Access Policy Manager (APM) and is broken into three individual lessons. In lesson one, you learn how to configure BIG-IP APM to provide Active Directory-based authentication for a load-balanced pool of web servers.

Building on that, in lesson two, you learn how to create a policy that provides an SSL VPN (Network Access) resource to users, but only when they log into BIG-IP APM using a corporate-issued PC.

Finally, lesson three builds on the first two lessons to create a policy that provides a dynamic landing page with both SSL VPN as well as an OWA (Portal Access) resource, but only to users with special authorization.

This course is intended for network administrators, operators, and engineers responsible for managing the normal day-to-day operation and administration of BIG-IP Access Policy Manager.

Prerequisites

The following course-specific knowledge and experience is suggested before attending this course:

- Hands-on experience with BIG-IP
- Basic web application delivery (BIG-IP LTM)
- HTML, HTTP, HTTPS as well as some CSS and JavaScript
- Telnet, SSH and TLS/SSL
- VPN or tunnel encapsulation, Layer 4 NAT and Access Control Lists

What You Will Learn

- Getting started with the BIG-IP system
- APM Traffic Processing and APM Configuration Wizards
- APM Access Policies, Access Profiles
- Visual Policy Editor, Branches and Endings
- APM Portal Access and Rewrite Profiles
- Single Sign-On and Credential Caching
- APM Network Access and BIG-IP Edge Client
- Layer 4 and Layer 7 Access Control Lists
- APM Application Access and Webtop Types
- Remote Desktop, Optimized Tunnels and Webtop Links
- LTM Concepts including Virtual Servers, Pools, Monitors and SNAT'ing
- APM + LTM Use Case for Web Applications
- Visual Policy Editor Macros
- AAA Servers and Authentication and Authorization with Active Directory and RADIUS
- Endpoint Security with Windows Process Checking, Protected Workspace and Firewalls
- iRules, Customization and SAML