Managing Advanced Cisco SSL VPN (CAVPN) v1.0

SASSL

Delivery Type: Classroom
Duration: 3 days

Overview

This three-day course focuses on providing advanced knowledge and features of Secure Sockets Layer (SSL) VPNs on the Cisco Adaptive Security Appliance (ASA). Learners will be able to evaluate various deployment options for SSL VPNs and configure advanced features using the Cisco Advanced Security Device Manager (ASDM) GUI.

Target Audience

Any engineer involved in the deployment and management of a SSL solution

Pre-Requisites

Attendees should meet the following prerequisites:

- ✓ Skills and knowledge equivalent to those learned in VPN
- ✓ Working knowledge of the Microsoft Windows operating system, including Microsoft Internet Explorer

Certification

Recommended preparation for exam(s):

- ✓ Thers are no exams currently associated with this course

Objectives

After completing this program, you will be able to:

- ✓ Describe client-based and clientless VPN solutions
- ✓ Explain the relationship between tunnel groups, group and user policies, connection profiles, and dynamic access policies
- ✓ Describe basic and advanced features of the clientless WebVPN solution, including smart tunnels, web ACLs, plug-ins, auto-signon, bookmarks, and portal customization
- ✓ Describe basic and advanced features within Cisco AnyConnect client version 3.0, including firewall policy push, Trusted Network Detection (TND), login scripts and profile editor
- ✓ Describe the features and benefits of Cisco Secure Desktop and understand the differences between the prelogin policies and Host Scan; use Cisco Secure Desktop to integrate Endpoint Assessment and Advanced Endpoint Assessment (AEA)
- ✓ Configure dynamic access policies (DAPs)
- ✓ Explain how the username credential can be automatically populated and how the connection profile can be chosen automatically using the prefill

93 Tsar Boris III Blvd., 1612 Sofia, Bulgaria
+359 2 903 59 33 @ sales@dada.bg

and certificate mapping features in the Cisco ASA appliance

- ✓ Describe the process required to enroll the Cisco ASA appliance with a third-party certificate authority (CA) and how to enroll and retrieve user-based certificates to provide mutual authentication

93 Tsar Boris III Blvd., 1612 Sofia, Bulgaria
+359 2 903 59 33 @ sales@dada.bg