Managing Advanced Cisco SSL VPN (CAVPN)

Duration: 3 Days **Course Code: SASSL** **Version: 1.0**

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

Objectives:

- **After you complete this course you should 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 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

Prerequisites:

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

Testing and Certification

Recommended preparation for exam(s) :

- Thers are no exams currently associated with this course

Content:

Feature Mapping and Scenario Discussion

- SSL Technology Overview
- Clientless SSL Feature Overview
- AnyConnect Feature Overview
- Group Deployment Type (Clientless versus AnyConnect)
- License Requirements for Suggested Solution

Initializing ASA and Preparing for PKI and AAA Support

- Basic ASA Configuration
- Validating Licenses
- Generating Self-Signed Certificate to Be Used with ASDM
- Enrolling Digital Certificate from CA Server to Be Used for SSL VPN Access
- Configuring Integration with AAA Servers (RADIUS, LDAP)
- Review of Logging

Connection Profile and Group Policy Configuration

- Creating Connection Profiles and Group Policies
- Configuring Group Policy
- Creating Bookmarks

Enhanced Clientless WebVPN Features

- Plug-ins
- Uploading the RDP Plug-in
- Configuring Smart Tunnels
- Auto-signon for HTTP/S resources
- Auto-signon for forms-based authentication
- Kerberos Constrained Delegation
- Microsoft extensions to KCD for VPN authentication
- Portal customization

Enhanced Cisco AnyConnect Client Features

- AnyConnect 3.0 Features
- AnyConnect Secure Mobility
- Trusted Network Detection
- Always-on VPN
- Login Script
- AnyConnect Client Profile configuration
- AnyConnect diagnostics

Cisco Secure Desktop Deployment and Prelogin Assessment

- Install,configure and manage Cisco Secure Desktop
- Test and troubleshoot Cisco Secure Desktop issues

Dynamic Access Policies

- Describing DAP Attributes
- Configuring DAP
- Using Endpoint Assessment Policies with DAP
- Working with Policy Objects

Securing Resources with Webtype and Network ACLs

- Feature Overview
- Configuring and Applying Webtype ACLs
- Configuring and Applying Network-Based ACLs

Cisco Secure Desktop Endpoint Assessment

- Configuring Cisco Secure Desktop for Advanced Host Scan
- Configuring DAP Policy to Utilize Advanced Host Scan
- Testing and Troubleshooting the Configuration

Certificate-Based Authentication

- Obtain a User Certificate
- Configure VPN authentication with client certificates
- Configure Connection Profile selection
- Configure Group Policy selection
- Configure LDAP Attribute maps for Authorization settings
- Two-Factor Authentication
- Test and Verify the Configuration

Advanced Troubleshooting

- SSL VPN Troubleshooting
- AnyConnect Troubleshooting
- Clientless SSL VPN Troubleshooting

Scaling SSL VPN

- Introduction
- Configuring Load Balancing
- Monitoring
- Verifying and Troubleshooting
- Configuring a Shared License

Labs

- Lab 1: Accessing the Lab Machines

Lab 2: Initializing the Cisco ASA Appliance and Preparing for PKI and AAA Support

- Lab 3: Configuring Basic Clientless and Client-Based SSL VPNs
- Lab 4: Enhanced Clientless WebVPN Features
- Lab 5: Enhanced Cisco AnyConnect Client Features
- Lab 6: Cisco Secure Desktop Deployment and Prelogin Assessment
- Lab 7: Host Scan and DAPs
- Lab 8: Securing Resources with Webtype ACLs
- Lab 9: Cisco Secure Desktop Endpoint Assessment
- Lab 10: Certificate-Based Authentication
- Lab 11: Advanced Troubleshooting

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK