Deploying Cisco ASA VPN Solutions

Duration: 5 Days Course Code: VPN Version: 2.0

Overview:

This five-day instructor-led course is aimed at providing network security engineers with the knowledge and skills that they need to implement and maintain Cisco ASA adaptive security appliance-based perimeter solutions.Delegates should be able to use Cisco ASA features to reduce the risk to the IT infrastructure and applications and to provide detailed operations support for the Cisco ASA security appliance.

Target Audience:

This course is designed for anyone who implements and maintains VPN features on the Cisco ASA as well as those individuals seeking VPN specialisation or CCNP Security certification.

Objectives:

- **After you complete this course you will be able to:**
- Describe the general properties of the Cisco ASA security appliance VPN subsystem
- Implement and maintain Cisco clientless remote access Secure Sockets Layer (SSL) VPNs on the Cisco ASA security appliance VPN gateway
- Implement and maintain Cisco AnyConnect client-based remote access SSL VPNs on the Cisco ASA security appliance VPN gateway, according to policies and environmental requirements
- Implement and maintain Cisco remote access IP Security (IPsec) VPNs on the Cisco ASA VPN gateway, according to policies and environmental requirements
- Implement and maintain site-to-site VPN solutions on the Cisco ASA security appliance VPN gateway, according to policies and environmental requirements
- Deploy endpoint security with Cisco Secure Desktop and dynamic access policy (DAP), and deploy and manage high-availability and high-performance features of the Cisco ASA security appliance

Prerequisites:

Attendees should meet the following prerequisites:

- CCNA Security Certification **ICND1** and **IINS** Required.
- **FIREWALL** attendance recommended

Testing and Certification

Recommended preparation for exam(s):

- **642-648** - Deploying Cisco ASA VPN Solutions

VPN is one of the four courses required for the Cisco Certified Network Professional for Security Career Certification, and is required along with SECURE for those delegates looking to achieve the VPN Specialist Certification.

Follow-on-Courses:

The following courses are recommended for further study :

- SECURE - Securing Cisco Routers and Switches
- IPS - Implementing Cisco Intrusion Prevention System

Content:

Cisco ASA Adaptive Security Appliance VPN Architecture and Common Components

- Evaluating the Cisco ASA Adaptive Security Appliance VPN Subsystem Architecture
- Evaluating the Cisco ASA Adaptive Security Appliance Software Architecture
- Implementing Profiles, Group Policies, and User Policies
- Implementing PKI Services

Cisco ASA Adaptive Security Appliance Clientless Remote Access SSL VPN Solutions

- Deploying Basic Clientless VPN Solutions
- Deploying Advanced Application Access for Clientless SSL VPNs
- Deploying Advanced Authentication and SSO for Clientless SSL VPNs
- Customizing the Clientless SSL VPN User Interface and Portal

Cisco AnyConnect Remote Access SSL Solutions

- Deploying a Basic Cisco AnyConnect Full-Tunnel SSL VPN Solution
- Deploying an Advanced Cisco AnyConnect Full-Tunnel SSL VPN Solution
- Deploying Advanced Authentication, Authorization, and Accounting in Cisco Full-Tunnel VPNs

Cisco ASA Adaptive Security Appliance Remote Access IPsec VPNs

- Deploying Cisco Remote Access VPN Clients
- Deploying Basic Cisco Remote Access IPsec VPN Solutions

Cisco ASA Adaptive Security Appliance Site-to-Site IPsec VPN Solutions

- Deploying Basic Site-to-Site IPsec VPNs
- Deploying Advanced Site-to-Site IPsec VPNs

Endpoint Security and High Availability for Cisco ASA VPNs

- Implementing Cisco Secure Desktop and DAP for SSL VPNs
- Deploying High-Availability Features in Cisco ASA Adaptive Security Appliance VPNs

Labs

- Lab 2-1: Configuring Basic Clientless VPN Access on the Cisco ASA Security Appliance
- Lab 2-2: Configuring Advanced Application Access for Clientless SSL VPNs
- Lab 2-3: Customizing the SSL VPN Portal on the Cisco ASA Security Appliance
- Lab 3-1: Configuring Basic Cisco AnyConnect Client Full-Tunnel SSL VPNs Using Local Password Authentication
- Lab 3-2: Deploying the Cisco AnyConnect Client with Centralized Management
- Lab 3-3: Configuring Basic Cisco AnyConnect Full-Tunnel SSL VPNs Using Local CA and SCEP Proxy
- Lab 4-1: Deploying Basic Remote Access IPsec VPN with IKEv2
- Lab 5-1: Deploying a Basic Cisco ASA Security Appliance IPsec IKEv1 Site-to-Site VPN
- Lab 6-1: Deploying Cisco Secure Desktop in Cisco SSL VPNs
- Lab 6-2: Configuring a Load-Balancing SSL VPN Cluster

Additional Information:

Recertification:
Cisco professional level certifications (CCNP, CCNP SP Operations, CCNP Wireless, CCDP, CCNP Security, CCNP Voice, and CCIP) are valid for three years. To recertify, pass any 642 exam that is part of the professional level curriculum or pass any CCIE/CCDE written exam before the certification expiration date.

Achieving or recertifying any of the certifications above automatically extends your active Associate and Professional level certification(s) up to the point of expiration of the last certification achieved. For more information, access the Cisco About Recertification page

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