Deploying Cisco ASA VPN Solutions

Längd: 5 Days **Kurskod: VPN**

Sammanfattning:

This five-day course aims to provide delegates with the knowledge and skills required to configure, maintain and operate VPN solutions based on the Cisco ASA 5500 Series Adaptive Security Appliance (ASA) including: Site to Site IPsec VPN, Remote access SSL VPN.

Målgrupp:

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

Målsättning:

- **After you complete this course you will be able to:**
- Evaluate the Cisco ASA adaptive security appliance VPN subsystem
- Deploy Cisco ASA adaptive security appliance IPsec VPN solutions
- Deploy Cisco ASA adaptive security appliance Cisco AnyConnect remote access VPN solutions
- Deploy Cisco ASA adaptive security appliance clientless remote access VPN solutions
- Deploy advanced Cisco ASA adaptive security appliance VPN solutions

Förkunskaper:

Attendees should meet the following prerequisites:

- CCNA Certification, ICND1 and ICND2 or CCNABC Required
- CCNA Security Certification IINS Required.
- FIREWALL attendance recommended

Test och certifiering

Recommended preparation for exam(s):

- 642-647 - Deploying Cisco ASA VPN Solutions

VPN is one of four courses required for the Cisco Certified Network Professional for Security Career Certification

Fortsättningskurs:

The following courses are recommended for further study :

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

Innehåll:

Evaluating the Cisco ASA Adaptive Security Appliance VPN Subsystem

- Evaluating the Cisco ASA Adaptive Security Appliance Software Architecture
- Evaluating the Cisco ASA Adaptive Security Appliance VPN Subsystem Architecture
- Applying Common Cisco ASA Adaptive Security Appliance Remote Access VPN Configuration Concepts

Deploying Cisco ASA Adaptive Security Appliance IPsec VPN Solutions

- Deploying Basic Site-to-Site IPsec VPNs
- Deploying Certificate Authentication in Site-to-Site IPsec VPNs
- Deploying the Cisco IPsec VPN Client
- Deploying Basic Easy VPN Solutions
- Deploying Advanced Authentication in Cisco Easy VPN Solutions
- Deploying the Cisco ASA 5505 Adaptive Security Appliance as an Easy VPN Hardware Client

Deploying Cisco ASA Adaptive Security Appliance AnyConnect Remote

- Access VPN Solutions
- Deploying a Basic Cisco AnyConnect Full Tunnel SSL VPN Solution
- Advanced Deployment of the Cisco AnyConnect VPN Client
- Deploying Advanced Authentication in AnyConnect Full Tunnel SSL VPNs

Deploying Cisco ASA Adaptive Security Appliance Clientless Remote

- Access VPN Solutions
- Deploying a Basic Clientless VPN Solution
- Deploying Advanced Application Access for Clientless SSL VPN
- Deploying Advanced Authentication and Single Sign-On in a Clientless SSL VPN
- Customizing the Clientless SSL VPN User Interface and Portal

Deploying Advanced Cisco ASA Adaptive Security Appliance VPN Solutions

- Deploying VPN Authorization, Access Control, and Accounting
- Deploying Cisco Secure Desktop in SSL VPNs
- Deploying Dynamic Access Policies
- Deploying High Availability and High Performance in SSL and IPsec VPNs

Labs

- Lab 2-1: Deploying a Basic Cisco ASA IPsec Site-to-Site VPN
- Lab 2-2: Deploying a Certificate-Based Cisco ASA IPsec Site-to-Site VPN
- Lab 2-3: Deploying Basic Easy VPN
- Lab 2-4: Deploying Advanced Easy VPN Server with Certificate-based Authentication
- Lab 2-5: Deploying the Cisco ASA 5505 as a Hardware Easy VPN Client
- Lab 3-1: Configuring a Basic Cisco AnyConnect Full Tunnel SSL VPN using Local Password Authentication
- Lab 3-2: Configuring a Basic AnyConnect Full Tunnel SSL VPN Using the Local CA
- Lab 3-3: Deploying the Cisco AnyConnect Client with Centralized Management
- Lab 4-1: Configuring Basic Clientless VPN Access
- Lab 4-2: Configuring Advanced Application Access in Clientless SSL VPNs
- Lab 4-3: Customizing the SSL VPN Portal
- Lab 5-1: Deploying SSL VPN Access Policies and Authorization Parameters
- Lab 5-2: Deploying Cisco Secure Desktop and DAP in SSL VPNs
- Lab 5-3: 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

Övrig information:

För mer information eller kursbokning, vänligen kontakta oss på telefon. 020-73 73 73

info@globalknowledge.se

www.globalknowledge.se

Vretenvägen 13, plan 3, 171 54 Solna