Implementing Cisco Secure Access Solutions

Duration: 5 Days Course Code: SISAS

Overview:

This course has been designed to provide engineers with the foundational knowledge and skills required to implement and manage network access security through the deployment of the Cisco Identity Services Engine and 802.1x Solution.
Students will gain hands-on experience with configuring advanced Cisco security solutions to enable secure device connection to the network and for mitigating outside threats. At the end of the course, students will be able to reduce the risk to their IT infrastructures and applications using Cisco's ISE appliance features and provide operational support to identity and network access control.

Target Audience:

This course is aimed at engineers looking to deploy or support a Cisco's Identity Services Engine solution and individuals looking to achieve the Cisco Certified Network Professional Certification for Security.

Objectives:

- **After completing this course you should be able to:**
- Understand Cisco Identity Services Engine architecture and access control capabilities
- Understand 802.1X architecture, implementation and operation
- Understand commonly implemented Extensible Authentication Protocols (EAP)
- Implement Public-Key Infrastructure with ISE
- Understand the implement Internal and External authentication databases
- Implement MAC Authentication Bypass
- Implement identity based authorization policies
- Understand Cisco TrustSec features
- Implement Web Authentication and Guest Access
- Implement ISE Posture service
- Implement ISE Profiling
- Understand Bring Your Own Device (BYOD) with ISE
- Troubleshoot ISE

Prerequisites:

Attendees should meet the following prerequisites:

- Cisco Certified Network Associate Certification **ICND1** and **ICND2** or **CCNABC**
- Cisco Certified Network AssociateSecurity Certification **ICND1** and **IINS**
- Knowledge of Microsoft Windows Operating System

Testing and Certification

Recommended Preparation for Exam(s):

- **300-208** - Implementing Cisco Secure AccessSolutions Exam

Follow-on-Courses:

Delegates looking to achieve the Cisco Certified Network Professional Certification for Security should also attend the following courses.

- **SENSS** - Implementing Cisco Edge Network Security Solutions
- **SITCS** - Implementing Cisco Threat Control Solutions
- **SIMOS** - Implementing Cisco Secure Mobility Solutions

Content:

Threat Mitigation Through Identity Services

- Identity Services
- 802.1X and EAP
- Identity System Quick Start

Cisco Identity Services Engine (ISE) Fundamentals

- Cisco ISE Overview
- Cisco ISE with PKI
- Cisco ISE Authentication
- Configuring Cisco ISE for External Authentication

Advanced Access Control

- Certificate-based User Authentication
- Authorization
- Security Group Access (SGA) and MACsec Implementation

Web Authentication and Guest Access

- Describe the Cisco Email Security Solutions
- Guest Access Services

Endpoint Access Control Enhancements

- Posture
- Profiler
- BYOD

Troubleshooting Network Access Control

- Troubleshooting Network Access Control

Labs

- Lab 1-1: Bootstrap Identity System
- Lab 2-1: Enroll Cisco ISE in PKI
- Lab 2-2: Implement MAB and Internal Authentication
- Lab 2-3: Implement External Authentication
- Lab 3-1: Implement EAP-TLS
- Lab 3-2: Implement Authorization
- Lab 4-1: Implement Central WebAuth and Guest Services
- Lab 5-1: Implement Posture Service
- Lab 5-2: Implement the Profile Service
- Lab 6-1: Troubleshooting Network Access Control

Further Information:

For More information, or to book your course, please call us on +254 713 027 191

training@clclearningafrica.com

www.clclearningafrica.com

Computer Learning Centre 2nd Floor Museum Hill Centre, Muthithi Road, Westlands, Nairobi, Kenya

Deploying Cisco ASA Firewall Features

Duration: 5 Days Course Code: FIREWALL Version: 2.0

Overview:

This five-day course aims to provide network security engineers with the knowledge and skills needed to implement and maintain Cisco ASA adaptive security appliance-based perimeter solutions.
Delegates will be able to reduce risk to the IT infrastructure and applications using Cisco ASA adaptive security appliance features, and provide detailed operations support for the Cisco ASA adaptive security appliance.

Target Audience:

Anyone who implements and maintains Cisco ASA firewalls, Network security specialists and technicians, delegates seeking CCNP Security certification

Objectives:

- **After you complete this course you will be able to:**
- Evaluate the basic firewall technology, features, hardware models, and licensing options of the Cisco ASA security appliance
- Implement and troubleshoot basic Cisco ASA security appliance connectivity and device management plane features
- Configure and verify Cisco ASA security appliance network integration
- Configure and verify Cisco ASA security appliance policy
- Configure and verify high availability and virtualization on Cisco ASA security appliances

Prerequisites:

Attendees should meet the following prerequisites:

- CCNA Security Certification **ICND1** and **IINS** Required.
- Working knowledge of Microsoft Windows OS is an advantage.

Testing and Certification

Recommended preparation for exam(s):

- **642-618** - Deploying Cisco ASA Firewall Solutions

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

Follow-on-Courses:

The following courses are recommended for further study :

- **SECURE** - Securing Cisco Routers and Switches
- **VPN** - Deploying Cisco ASA VPN Solutions
- **IPS** - Implementing Cisco Intrusion Prevention System

The above courses along with FIREWALL make up the CCNP for Security Certification.

Delegates may also want to consider

- ICISE - Implementing Cisco Identity Services Engine.
- 802.1X - Introduction to 802.1X Operations for Cisco Security Professionals

Content:

Cisco ASA Adaptive Security Appliance Essentials

- Evaluating Cisco ASA Adaptive Security Appliance Technologies
- Identifying Cisco ASA Adaptive Security Appliance Families
- Identifying Cisco ASA Adaptive Security Appliance Licensing Options

Basic Connectivity and Device Management

- Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
- Managing Basic Cisco ASA Adaptive Security Appliance Network Settings
- Configuring Cisco ASA Adaptive Security Appliance Device Management Features

Network Integration

- Configuring Cisco ASA Adaptive Security Appliance NAT Features
- Configuring Cisco ASA Adaptive Security Appliance Basic Access Control Features
- Configuring Cisco ASA Adaptive Security Appliance Routing Features
- Configuring the Cisco ASA Adaptive Security Appliance Transparent Firewall

Cisco ASA Adaptive Security Appliance Policy Control

- Defining the Cisco ASA Adaptive Security Appliance MPF
- Configuring Cisco ASA Adaptive Security Appliance Connection Policy and QoS Settings
- Configuring Cisco ASA Adaptive Security Appliance Advanced Application Inspections
- Configuring Cisco ASA Adaptive Security Appliance User-Based Policies

Cisco ASA Adaptive Security Appliance High Availability and Virtualization

- Configuring Cisco ASA Adaptive Security Appliance Interface Redundancy Features
- Cisco ASA Adaptive Security Appliance Active/Standby High Availability
- Configuring Security Contexts on the Cisco ASA Adaptive Security Appliance
- Configuring Cisco ASA Adaptive Security Appliance Active/Active High Availability

Labs

- Lab 2-1: Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
- Lab 2-2: Configuring the Cisco ASA Adaptive Security Appliance for Secure Network Integration
- Lab 2-3: Configuring Management Features
- Lab 3-1: Configuring NAT
- Lab 3-2: Configuring Basic Cisco Access Control Features
- Lab 3-3: Configuring Transparent Firewall (Optional)
- Lab 4-1: Configuring MPF, Basic Stateful Inspections, and QoS
- Lab 4-2: Configuring MPF Advanced Application Inspections
- Lab 4-3: Configuring Cut-Through Proxy
- Lab 5-1: Configuring Active/Standby High Availability
- Lab 5-2: Configuring Active/Active High Availability

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/Email us on : - +254 713 027 191

KENYA - training.kenya@clclearningafrica.com

TANZANIA - training.tanzania@clclearningafrica.com

UGANDA - training.uganda@clclearningafrica.com

RWANDA - training.rwanda@clclearningafrica.com

BURUNDI - training.burundi@clclearningafrica.com

ETHOPIA - training.ethopia@clclearningafrica.com

Deploying Cisco ASA VPN Solutions

Duration: 5 Days **Course Code: VPN**

Overview:

The Deploying Cisco ASA VPN Solutions (VPN) course aims 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. Successful graduates will 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 Those seeking CCNP Security certification

Objectives:

- Upon completing this course, the learner will be able to meet these overall objectives:
- 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:

The knowledge and skills that a learner must have before attending this course are as follows:

- Cisco CCNA certification
- Cisco CCNA Security certification
- Familiarity with networking and security terms and concepts
- Working knowledge of the Microsoft Windows operating system

To gain the prerequisite skills and knowledge, Cisco strongly recommends the knowledge of the following courses:

- Interconnecting Cisco Networking Devices Part 1 (ICND1)
- Interconnecting Cisco Networking Devices Part2 (ICND2)
- Implementing Cisco IOS Network Security (IINS)
- Securing Networks with Cisco Routers and Switches (SECURE)
- Deploying Cisco ASA Firewall Solutions (FIREWALL)

Testing and Certification

Recommended as preparation for:

- 642-647 - Deploying Cisco ASA VPN Solutions (Last day to test 28th May 2012)
- 642-648 - Deploying Cisco ASA VPN Solutions

VPN is one of four courses required for the **Cisco Certified Network Professional (CCNP) Security** Certification

Follow-on-Courses:

- Implementing Cisco Intrusion Prevention System (IPS)

Content:

Cisco ASA Adaptive Security Appliance VPN Architecture and Common Components

- Evaluating the Cisco ASA VPN Subsystem Architecture
- Evaluating the Cisco ASA 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

Further Information:

For More information, or to book your course, please call us on +254 713 027 191

training@clclearningafrica.com

www.clclearningafrica.com

Computer Learning Centre 2nd Floor Museum Hill Centre, Muthithi Road, Westlands, Nairobi, Kenya

Implementing Cisco Intrusion Prevention System

Duration: 5 Days **Course Code: IPS**

Overview:

The Implementing Cisco Intrusion Prevention System (IPS) course is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. It is a five-day instructor-led course aimed at providing network security engineers with the knowledge and skills needed to deploy Cisco IPS-based security solutions. Successful graduates will be able to reduce risk to the IT infrastructure and applications using Cisco IPS features, and provide detailed operations support for the Cisco IPS.

Target Audience:

This course is designed for:Channel Partner / Reseller Customer Employee

Objectives:

- Upon completing this course, the learner will be able to meet these overall objectives:
- Evaluate products and deployment architectures for the Cisco IPS product line.
- Perform an initial implementation of a Cisco IPS sensor.
- Implement an initial security policy using a Cisco IPS sensor according to local policies and environmental requirements.
- Deploy customized policies to adapt Cisco IPS traffic analysis and response to the target environment.
- Implement a basic Cisco IPS data management and analysis solution.
- Implement complex Cisco IPS policy virtualization, high availability, and high performance solutions according to
- policy and environmental requirements.
- Perform the initial setup of, and maintain specific Cisco IPS hardware.

Prerequisites:

The knowledge and skills that a learner must have before attending this course:

- Working knowledge of the Microsoft Windows operating system

To gain the prerequisite skills and knowledge, Cisco strongly recommends the knowledge of the following courses:

- Interconnecting Cisco Network Devices 1 (ICND1)
- Interconnecting Cisco Network Devices 2 (ICND2)
- Implementing Cisco IOS Network Security (IINS)

Testing and Certification

Recommended as preparation for:

- 642-627 - Implementing Cisco Intrusion Prevention System

IPS is one of the courses required for the **Cisco Certified Network Professional (CCNP) Security** Certification.

Follow-on-Courses:

- Securing Networks with Cisco Routers and Switches (SECURE)
- Deploying Cisco ASA Firewall Solutions (FIREWALL)
- Deploying Cisco ASAVPN Solutions (VPN)

Content:

Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices

- Evaluating Intrusion Prevention and Intrusion Detection Systems
- Choosing Cisco IPS Software, Hardware, and Supporting Applications
- Evaluating Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-Evasive Countermeasures
- Choosing a Network IPS and IDS Deployment Architecture

Installing and Maintaining Cisco IPS Sensors

- Integrating the Cisco IPS Sensor into a Network
- Performing the Cisco IPS Sensor Initial Setup
- Managing Cisco IPS Devices

Applying Cisco IPS Security Policies

- Configuring Basic Traffic Analysis
- Implementing Cisco IPS Signatures and Responses
- Configuring Cisco IPS Signature Engines and the Signature Database
- Deploying Anomaly-Based Operation

Adapting Traffic Analysis and Response to the Environment

- Customizing Traffic Analysis
- Managing False Positives and False Negatives
- Improving Alarm and Response Quality

Managing and Analyzing Events

- Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors
- Managing and Investigating Events Using Cisco IPS Manager Express
- Using Cisco IME Reporting and Notifications
- Integrating Cisco IPS with Cisco Security Manager and Cisco Security MARS
- Using the Cisco IntelliShield Database and Services

Deploying Virtualization, High Availability, and High Performance Solutions

- Using Cisco IPS Virtual Sensors
- Deploying Cisco IPS for High Availability and High Performance

Configuring and Maintaining Specific Cisco IPS Hardware

- Configuring and Maintaining the Cisco ASA AIP-SSM and AIP-SSC-5 Modules
- Configuring and Maintaining the Cisco ISR IPS AIM and IPS NME Modules
- Configuring and Maintaining the Cisco IDSM-2

Further Information:

For More information, or to book your course, please call us on +254 713 027 191

training@clclearningafrica.com

www.clclearningafrica.com

Computer Learning Centre 2nd Floor Museum Hill Centre, Muthithi Road, Westlands, Nairobi, Kenya