CCIE Security Lab Bootcamp (CCIESL)

Duration 5 Days

COURSE CONTENT

It is an intense five day course designed to be challenging and give you the knowledge needed to achieve the CCIE Security certification. Over five long days you will learn and practice the topics from the CCIE Security blueprint. You will also have access to the instructor when you need personal mentoring. After each lecture you will be challenged with many hours of complex lab scenarios reinforcing the material you have covered at the start of the day. There will be a full lab on day five of the course.

COURSE OBJECTIVES

After you complete this course you will be able to:

- Understand what is required to pass the CCIE security lab exam.
- Find out how much work you still need to do.
- Become more knowledgeable about Cisco security.
- Become faster in your configuration of Cisco devices.

WHO SHOULD ATTEND

- Candidates preparing for the CCIE Security Lab exam who already possess most of the theoretical knowledge required for the exam.
- Candidates who have been preparing for the CCIE Security Lab exam who wish to assess their level of preparedness and who require additional practice

PREREQUISITES

Attendees should meet the following prerequisites:

- Candidates must have passed the CCIE written exam before attempting the lab boot camp
- CCIE Security Written Exam Boot Camp CCIESW
- Minimum of 3 - 5 years hands-on experience in respective field
- Ideally CCSP or CCNP Security Certified
- Determined attitude
- Patience
- Strong will

COURSE OUTLINE

Day 1

Section 1 - Firewalls, ASA and IOS

- Lab 1.1 – Basic ASA Setup
- Lab 1.2 - Static and Default Routing
- Lab 1.3 - Dynamic Routing
- Lab 1.4 - Object Groups
- Lab 1.5 – ACL
- Lab 1.6 – NAT and PAT
- Lab 1.7 – Connection limits and timeouts.
- Lab 1.8 – Management
- Lab 1.9 - Configuring Java, ActiveX and URL Filtering

Section 2 - Advanced ASA Setup

- Lab 2.1 - Protocol inspection
- Lab 2.2 - Modular policy framework
- Lab 2.3 - TCP Normalization
- Lab 2.4 - Advanced HTTP inspection
- Lab 2.5 - Advanced FTP inspection
- Lab 2.6 – URPF and fragments
- Lab 2.7 - Qos on the ASA

Section 3 - Failover, Contexts and Transparent mode

- Lab 3.1 - Multimode
- Lab 3.2 – Failover
- Lab 3.3 - Multicontext Transparent mode

Section 4 - Basic IOS Firewall Setup

- Lab 4.1 – Basic IOS FW setup
- Lab 4.2 – Tuning
- Lab 4.3 - Filtering of Java and URLs
- Lab 4.4 - Port application mapping (PAM)

Section 5 - Zone Based Firewall Setup

- Lab 5.1 – Creating a ZBF
- Lab 5.2 – ZBF advanced

Day 2

Section 1 - VPN using ASA and IOS

- Lab 1.1 – Basic ASA setup
- Lab 1.2 - ASA to ASA VPN
- Lab 1.3 – IOS to ASA VPN
- Lab 1.4 - Router to Router VPN using GRE
- Lab 1.5 - Router to Router VPN using VTI

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- Lab 1.6 – DMVPN
- Lab 1.7 – GET VPN
- Lab 1.8 – IOS CA

Section 3 - Remote access VPN

- Lab 3.1 - VPN Client to ASA
- Lab 3.2 - IOS to IOS with Dynamic VTI
- Lab 3.3 - ASA SSL VPN basic
- Lab 3.4 - ASA SSL VPN advanced

Day 3

Section 1 - IPS

- Lab 1.1 - Basic IPS Setup
- Lab 1.2 - Configuring Inline Mode
- Lab 1.3 - Signature Tuning
- Lab 1.4 – Event Action Overrides
- Lab 1.6 – Event reduction
- Lab 1.7 – Virtual sensors
- Lab 1.8 - Configuring SNMP
- Lab 1.9 – Creating a custom signature
- Lab 1.10 - Summarisation
- Lab 1.11 - IPS Authentication Attempt Limit

Section 2 - Catalyst Switch Security

- Lab 2.1 - Securing Spanning tree
- Lab 2.2 - Port Security
- Lab 2.3 - DHCP snooping
- Lab 2.4 - ARP inspection
- Lab 2.5 - VLAN Maps
- Lab 2.6 - Advanced features
- Lab 2.7 – 802.1x
- Lab 2.8 – Strom control
- Lab 2.9 – Private VLAN edge

Section 3 - Access Control Server (ACS)

- Lab 3.1 - AAA Clients
- Lab 3.2 - AAA Users and Groups
- Lab 3.3 - AAA on Routers
- Lab 3.4 - AAA on the ASA
- Lab 3.6 - Command authorization on IOS
- Lab 3.7 - Proxy Authentication on the ASA
- Lab 3.8 - Proxy Authentication on IOS

Section 4 - Advanced IOS Security Features

- Lab 4.1 – NTP
- Lab 4.2 - Time based ACL
- Lab 4.3 - TCP intercept
- Lab 4.4 – QOS
- Lab 4.5 – URPF
- Lab 4.6 – FPM
- Lab 4.7 – PBR and ICMP unreachable
- Lab 4.8 – Control plane security
- Lab 4.9 - Session Management
- Lab 4.10 - Management Processes Survival
- Lab 4.11 – Logging Class Maps
- Lab 4.12 - ACL IP Options Selective Drop
- Lab 4.13 – Router protection and notifications
- Lab 4.14 – IKE protection on router
- Lab 4.15 – Management protection
- Lab 4.16 – Advanced access lists
- Lab 4.17 – IKE pre shared key protection

Day 4

Section 1 - Putting it all together and troubleshooting - VPN

- Lab 1.1 - DMVPN through the ASA
- Lab 1.2 - IOS EZVPN with DVTI not working

Section 2 - Putting it all together and troubleshooting - FW

- Lab 2.1 - BGP through the ASA
- Lab 2.2 - AAA through IOS ZBF and ASA

Section 3 - Putting it all together and troubleshooting – Other

- Lab 3.1 - Routing Authentication
- Lab 3.2 - Cannot SSH to a device

Day 5

Full Lab

- Section 1- Core Configuration (20 points)
- Section 2- Firewalls (10 Points)
- Section 3: Cisco VPN (14 Points)
- Section 4: Cisco IPS (8 Points)
- Section 5: Identity Authentication (8 Points)
- Section 6: Control and Management Plane Security (18 Points)
- Section 7: Advanced Security (10 Points)
- Section 8: Network Attacks (12 Points)

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th