Implementing Cisco ACI Security

Duration: 4 Days **Course Code: N1_ACISEC** **Delivery Method: Virtual Learning**

Overview:

This 4 Day course provides in-depth knowledge and practical skills in implementing a comprehensive ACI security design.
Updated 09/08/2026

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

The primary audience for this course is as follows:
- Network administrators and engineers
- IT professionals working with Cisco ACI
- Individuals interested in Data Center security

Objectives:

- By the end of this course, participants will learn a comprehensive approach of implementing security in ACI. You will be proficient in managing and administering both internal and external security approaches in ACI. Upon completion, the learner will be able to meet these overall objectives:
- Proficient in managing and implementing a comprehensive Cisco ACI security solution
- Utilize all of the Cisco ACI built in security mechanisms
- Implement L4-L7 solutions into ACI
- Integrate NGFW features into an ACI security solution

Prerequisites:

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

- Basic knowledge of Cisco ACI infrastructure
- Recommend CCNP Certification or equivalent knowledge
- Understanding of networking and security fundamentals

Testing and Certification

- *N/A*

Follow-on-Courses:

- *None recommended*

Content:

Course Outlines

Module 1: Cisco ACI Software Defined Networking (SDN) Architecture

Objective: Gain comprehensive knowledge of the Cisco SDN Architecture implementation of hardware and software

- Lesson 1: ACI SDN Network Architecture
- Lesson 2: ACI Zero Trust Model and Security constructs
- Lesson 3: ACI Physical Server Integration
- Lesson 4: ACI Security for Physical or Virtual workloads
- Lesson 5: ACI L3Out external routing

Module 2: Secure Hypervisor integration with Cisco ACI

Objective: Understand the secure integration of leading hypervisors with Cisco Application Centric Infrastructure (ACI)

- Lesson 1: Nutanix AHV (Nutanix Acropolis Hypervisor)
- Lesson 2: VMware ESXi and vCenter
- Lesson 3: Microsoft Hyper-V with System Center Virtual Machine Manager (SCVMM)
- Lesson 4: Red Hat OpenStack
- Lesson 5: Google Kubernetes
- Lesson 6: Kernel-based Virtual Machine (KVM)

Module 3: Cisco ACI Native Access Control

Objective: Explore, configure, and evaluate all the native Cisco ACI access control mechanisms

- Lesson 1: ACI networking constructs of Bridge Domain and VRF.
- Lesson 2: ACI Zero Trust model objects of Tenant, EPG, Application Profile, Contract, Subject and Filters
- Lesson 3: Network Centric vs Application Centric Security Models
- Lesson 4: ACI zones
- Lesson 5: ACI VRF Policy Control Enforcement
- Lesson 6: ACI Preferred Groups
- Lesson 7: Configure ACI vzAny
- Lesson 8: Configure an ACI Allow List Model with Contracts and Filters
- Lesson 9: Stateful vs Stateless Contracts
- Lesson 10: ACI Tenant Span to analyze secure traffic flows
- Lesson 11: ACI EPG Shutdown
- Lesson 12: ACI contract logging

Objective: Master administration of ACI Physical Security

- Lesson 1: Remote Leafs
- Lesson 2: MACsec on ACI leafs
- Lesson 3: Enabling 802.1x on ACI leafs
- Lesson 4: NXOS Image signing and verification

Module 8: Cisco ACI Multidomain Security

Objective: Develop skills in understanding the value and approach of Cisco ACI and VMware NSX integration

- Lesson 1: Trustsec Policy Domain
- Lesson 2: Cisco Identity Services Engine (ISE) for a cohesive security policy
- Lesson 3: Trustsec Security Group to ACI External EPG security translation
- Lesson 4: Stealthwatch and ACI Integration
- Lesson 5: Cisco ACI and Cisco Secure Workload Integration
- Lesson 6: Cisco ACI and Cisco Secure Workload Rapid Threat Containment

Labs Outlines

Labs are designed to assure learners a whole practical experience, through the following practical activities:

Lab 0: Accessing the NterOne Lab Devices

- Basics of accessing and setting up the lab environment for Cisco ACI security exercises.

Lab 1: Validate Fabric Discovery

- Validate the pre-configured Cisco ACI Fabric

Lab 2: Create ACI Access Policies

- Setting up policies, profiles, pools and AEPs for device connectivity

Lab 3: Implement Cisco ACI Tenant Policies

- Configure the underlying managed objects to support ACI Security

Lab 4: Integrate APIC with Nutanix Acropolis Hypervisor (AHV)

- Hands-on experience in provisioning Cisco ACI and Nutanix AHV virtual machine manager (VMM) Integration

Lab 9: Configure ACI vzAny

- Configure a contract and filter and apply to vzAny within a VRF in your tenant.

Lab 10: Configure an ACI Allow List Model with Contracts and Filters

- Configure a comprehensive security allow list in ACI incorporating one way and bidirectional traffic flows. Demonstrate EPG Shutdown and Contract Logging

Lab 11: Configure Tenant Span to analyze security

- Configure Tenant Span to analyze ACI Security traffic flows with Wireshark

Lab 12: Contract Inheritance with EPG Contract Master

- Configure the inherit contract relationship configuration of master EPG

Lab 13: Configure an ASAv in a ACI Service Graph in Unmanaged Mode

- Configure an ASAv firewall to integrate within the ACI allow list security model.

Lab 14: ACI Endpoint Security Groups (ESGs)

- Configure the new segmentation method available in Cisco ACI that allows creating security groups across multiple bridge domains (BDs)

Lab 15: ACI Micro segmented EPG (uEPG)

- Configure the dynamic uEPG and explore advanced isolation within an EPG

Lab 16: Configure a NGFW Firepower firewall in a ACI with Policy Based Routing (PBR)

- Configure an NGFW Firepower firewall to integrate within the ACI with PBR.

Lab 17: Configure Threat Detection with IDS and IPS in the ACI Integrated NGFW Firepower Security virtual machine

- Configure IDS and IPS L4-L7 integration within your tenant

Lab 18: Enabling 802.1X in ACI

- Configure 802.1X in Cisco ACI to control port-based access control to the leafs.

Lab 19: Monitoring and Diagnosing ACI

- Lesson 13: Contract Inheritance with EPG Contract Master
- Lesson 14: ACI Micro segmented EPG (uEPG) for Intra-EPG communications
- Lesson 15: ACI Endpoint Security Groups (ESGs)
- Lesson 16: VRF Leaking
- Lesson 17: Designing a secure ACI Data Center

Module 4: Cisco ACI L4-L7 Service Graphs for Secure Device Integration

Objective: Develop skills in L4-L7 service graphs to extend ACI security with external devices

- Lesson 1: ACI L4-L7 Service Graph
- Lesson 2: ACI Service Graph Template
- Lesson 3: Concrete Object
- Lesson 4: Service Chaining with multiple highly available devices
- Lesson 5: Managed vs Unmanaged L4-L7 ACI Integration
- Lesson 6: Integrating Cisco ASAv
- Lesson 7: Transparent vs routed mode security device integration
- Lesson 8: Contracts to insert security services into ACI
- Lesson 9: L3Out routing integration with security devices

Module 5: Cisco ACI and NGFW Integration

Objective: Develop skills in understanding the value and approach of Cisco ACI and NGFW integration

- Lesson 1: Next Generation Firewall (NGFW) Integrated Security Architecture
- Lesson 2: Cisco Secure Firewall Management Center (FMC)
- Lesson 3: Cisco Secure Firewall Threat Defense Virtual (formerly FTDv/NGFWv) and Cisco Secure Firewall Management Center (FMC) enabling on Nutanix AHV
- Lesson 4: Firepower Management Center Endpoint Update App for the Cisco Application Centric Infrastructure (ACI)
- Lesson 5: NGFW Routed, switch or inline interface mode
- Lesson 6: ACI L4-L7 Policy Based Redirect (PBR) to security service
- Lesson 7: ACI PBR for micro-segmentation
- Lesson 8: Extend PBR security services to ACI Multi-Pod
- Lesson 9: Cisco NGFW zone-based policies in FMC
- Lesson 10: Threat detection with Cisco intrusion detection systems (IDS) to ACI Insertion
- Lesson 11: Threat detection with Cisco intrusion prevention systems (IPS) to ACI

Lab 5: Enable a Bare Metal Device in your Tenant

- Configure a Bare Metal Device to demonstrate ACI security methodologies for physical servers along with Nutanix Virtual Machines.

Lab 6: Configure External Layer 3 (L3Out) Connection

- Setting up an OSPF L3Out in your tenant to integrate external connectivity with a secure ACI architecture

Lab 7: ACI VRF Policy Control Enforcement

- Configure VRF Policy Control Enforcement and verify connectivity within your Tenant

Lab 8: Configure ACI Preferred Groups

- Creating VRF based Preferred Groups and verify connectivity and isolation within your Tenant

Security

- Enable and analyze ACI security diagnostic information

Lab 20: Configure RBAC using Local and RADIUS Users

- Configure role-based access control (RBAC) to be used for both local and RADIUS user authentication

Insertion
- Lesson 12: Cisco ACI Integration with SPAN for IDS and IPS
- Lesson 13: Distributed Denial of Service (DDoS) Services Insertion
- Lesson 14: Cisco DC App ACI Endpoint Update to push endpoint information to the ASA or FMC

Module 6: Application Policy Infrastructure Controller (APIC) Security and Hardening

Objective: Learn method of adding security to the APIC for all management and programmatic functions

- Lesson 1: APIC Hardening
- Lesson 2: APIC Northbound Protocols
- Lesson 3: APIC Northbound Authentication
- Lesson 4: ACI Role Based Access Control (RBAC) for secure access
- Lesson 5: Audit logs for ACI changes
- Lesson 6: Certificate based authentication
- Lesson 7: Two factor authentication

Module 7: Administering Physical ACI Security

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo