

Cisco CCNP Designing and Implementing Cloud Connectivity v1.0 (300-440 ENCC)

This intermediate Designing and Implementing Cloud Connectivity v1.0 (300-440 ENCC) training prepares network admins to design and implement cloud connectivity for a Cisco network, balancing architectural concerns with IPsec, SD-WAN, operation requirements, and design requirements.

[CBT Nuggets course material](#) →

WEEK 1

Introduction to Cloud Computing

154 min.

Cloud Computing Fundamentals	16
Cloud Deployment Models	11
More Cloud Deployment Models	10
Challenge	7

Exploring Cloud Service Models

Introduction	3
Infrastructure as a Service (IaaS)	11
Platform as a Service (PaaS)	11
Software as a Service (SaaS)	8
Anything as a Service (XaaS)	5
Overview of Public Cloud Providers	5
Challenge	3

Connecting to Cloud Providers over the Internet

Introduction	2
Introduction to IPsec	9
Discovering ESP and Data Integrity	6
Discovering Confidentiality (Encryption)	7
Discovering Key Management	9
Discovering Authentication and SAs	8
Challenge	8

Introduction to SD-WAN

Introduction	2
Discovering Cisco SD-WAN	8
The vManage Server	5

WEEK 2**152 min.**

The vSmart Controller	8
The vBond Server	5
WAN Edge Devices	8
Challenge	9

Connecting SD-WAN to Cloud Providers

Introduction	5
What is Cisco dCloud?	10
SD-WAN Overview	9
Cloud OnRamp for IaaS	7
Cloud OnRamp for Multi-Cloud - Cloud Gateway Design:	8
Cloud OnRamp for Multi-Cloud - Branch Connect Design:	5
Challenge	6

Using Private Connections to the Cloud

Introduction	5
Why Private Connectivity?	10
Understanding Transport Locators	12
Using AWS Direct Connection with SD-WAN	5
Using GCP Cloud Interconnect with SD-WAN	3
Using Azure ExpressRoute with SD-WAN	4
Challenge	6

Understand Colocations and Cloud Exchanges

Introduction	4
Examining Colocations	12
Cloud OnRamp for Colocation	11

WEEK 3**155 min.**

Understand Cloud Exchanges	4
Introduction to SDCI	7
Challenge	8

Connecting SD-WAN to SaaS Providers

Introduction	2
The Centralized Internet Gateway Design	17
The Direct Internet Access Design	7
Cloud OnRamp for SaaS	8
Using DIA Links at the Branches	6
Using DIA Links at a Gateway Site	7
Using DIA Links Through a Colocation	3
Challenge	10

Introduction to Cisco Umbrella

Introduction	2
What is Cisco Umbrella?	10
Understand Umbrella Traffic Flow	6
Understand Cisco's SASE Architecture	9
Integrating SD-WAN and SASE	8
Cloud OnRamp for SaaS with Umbrella	5
Challenge	7

Exploring Cisco Umbrella

Introduction	1
Cisco Umbrella Overview	7
Examining Security Reports	5
Managing Identities and Network Tunnels	7

Examining DNS Policies 9

WEEK 4

165 min.

Examining Web Policies 9

Examining Firewall Policies 6

Challenge 4

Performance and Redundancy for Cloud Connections

Introduction 3

Criticality of Performance and Redundancy 17

Exploring Redundancy Requirements 15

Redundancy with AWS 7

Redundancy with Azure 6

Redundancy with GCP 4

Challenge 9

Performance and Redundancy Technologies Part 1

Introduction 12

Using Timers and BFD 22

Perform Packet Captures 13

Challenge 10

Performance and Redundancy Technologies Part 2

Introduction 9

Monitor Connections with IP SLA 19

WEEK 5

153 min.

Using IP SLA and Tracked Objects 13

Using EEM to Stabilize IP SLA 14

Examining Load Sharing 10

Challenge: 7

Native Cloud Security Features

Introduction 1

Exploring Native Cloud Security 12

Traffic Control in the Cloud 13

AWS Security Features 10

Azure Security Features 8

GCP Security Features 4

Challenge 8

Describing IPsec Connectivity

Introduction 8

What is a VPN? 9

Configure a GRE Tunnel 9

IPsec Framework 8

Configure IKEv2 on IOS XE 11

Configure IPsec Components and the Tunnel 8

WEEK 6

159 min.

Verify IPsec and Connectivity 5

Challenge 11

Configure AWS VPC for IPsec VPN to IOS XE

Introduction 1

Putting Together Our Game Plan	9
Create the VPC and IP Subnet	6
Create and Attach Gateways	5
Create the VPN Connection on AWS	10
Create a Route Table and Security Group	6
Gathering Information for the IOS XE Configuration	6
Challenge	5

Configure IOS XE for IPsec VPN to AWS VPC

Introduction	1
Reviewing Our Game Plan	8
Configure IKEv2 Keychain	5
Configure IKEv2 Proposal, Policy, and Profile	10
Configure IPsec Transform Set and Profile	4
Configure Tunnel Interfaces	9
Testing Reachability	10
Challenge	5

Configure Redundancy with IOS XE and AWS

Introduction	6
Adding Trackability to our Tunnels	9
Dynamic Routing with BGP	11
Using an FHRP on the Redundant Edge	8
Edge Redundancy with Multiple Links	9

Challenge	13
-----------	----

158 min.

WEEK 7

Configure Native IPsec VPN to Azure

Introduction	1
Our Game Plan	12
Create the vNet and IP Subnets	9
Create Local and Virtual Gateways	8
Create the VPN Connection on Azure	8
Create a Route Table and SRV1	6
Configure IOS XE IPsec VPN on OnPrem_R1	8
Challenge	4

Configure Native IPsec VPN to GCP

Introduction	1
Our Game Plan	13
Create the VPC and IP Subnet	6
Create VPN and Peer VPN Gateway	11
Create SRV1	3
Configure IOS XE IPsec VPN on OnPrem_R1	9
Challenge	7

Deploying the Catalyst 8000v Edge Router into AWS

Introduction	5
Configuration Guidelines for the c8000v	9
Configuring the AWS VPC for the c8000v	7
Deploying the c8000v	10
Configuring the c8000v	8

Verifying Connectivity From Subnet 10	3
---------------------------------------	---

Verifying Subnet 10 from a Server	8
-----------------------------------	---

153 min.

WEEK 8

Challenge 7

Configure IOS XE Site-to-Site VPN in AWS

Introduction 10

Configure Both IKEv2 Key Rings 5

Configure Both IKEv2 PPPs (Proposals, Policies, and Profiles) 15

Configure Both IPsec TSs and Profiles 4

Configure Both Tunnel Interfaces 4

Deploy Dynamic Routing (OSPF) 6

Test Reachability Between Endpoints 2

Challenge 10

Configure IOS XE VPN Redundancy in AWS

Introduction 10

Deploy a Secondary c8000v 11

Configure Tunnel 2 on 'OnPrem_R2' 5

Configure Redundancy for the Tunnels 6

Configure a Traditional FHRP 8

Configure Redundancy for AWS 16

Verifying Failover and Reachability 6

Challenge 7

Deploying the Catalyst 8000v Router into Azure

Introduction 1

Our Game Plan 9

WEEK 9

152 min.

Configuration Guidelines for the c8000v 8

Prepare the Cloud Provider Network 17

Deploying the c8000v 12

Configuring the c8000v 3

Verifying Connectivity From Subnet 10 7

Verifying Subnet 10 from a Server 3

Challenge 6

Configure IOS XE Site-to-Site VPN in Azure

Introduction 1

Our Game Plan 9

Configure Both IKEv2 Key Rings 4

Configure Both IKEv2 PPPs 11

Configure Both IPsec TSs and Profiles 4

Configure Both Tunnel Interfaces 6

Deploy Dynamic Routing 6

Test Reachability Between Endpoints 3

Challenge 6

Deploying the Catalyst 8000v Router into GCP

Introduction 1

Our Game Plan 11

Configuration Guidelines for the c8000v 7

Prepare the Cloud Provider Network 10

Deploying the c8000v 13

Configuring the c8000v 4

WEEK 10

158 min.

Verifying Connectivity From Subnet 10 9

Challenge 3

Configure IOS XE Site-to-Site VPN in GCP

Introduction 1

Our Game Plan 10

Configure Both IKEv2 Key Rings 3

Configure Both IKEv2 PPPs 12

Configure Both IPsec TSs and Profiles 4

Configure Both Tunnel Interfaces 5

Deploy Dynamic Routing 6

Test Reachability Between Endpoints 2

Challenge 7

Preparing Our Lab for SD-WAN

Introduction 9

Prepare CML for Custom Images 6

Upload Controller Images 7

Import or Create Node Definitions 11

Import or Create Image Definitions 6

Deploy SD-WAN Nodes in Topology 4

Boot and Verify Image Versions 9

Challenge 6

Configure Our SD-WAN Environment

Introduction 7

Obtain a Network PnP File 10

Baseline Configuration and IP Connectivity 9

Configure Certificates 12

WEEK 11

156 min.

Challenge 7

Configure Our Controllers and Edge Devices

Introduction 7

Add Controllers and Issue Certificates 11

Configure VPN 0 and Verify Configuration 9

Add a c8000v as an Edge Device 21

Challenge 8

Preparing and Building Our Lab with CML 2.7+

Introduction 5

Deploy SD-WAN Nodes in Topology 12

Boot and Verify Image Versions 9

Baseline Configuration and IP Connectivity 7

Add Controllers and Issue Certificates 10

Add our c8000v Edge Devices 9

Challenge 8

Configure the On-Prem SD-WAN Edge

Introduction 8

Our Gameplan 3

Create the Device Template 12

Configure VPN 0 10

WEEK 12

151 min.

Configure VPN 512 19

Configure Service VPN 10 13

Challenge 6

Configure the On-Prem SD-WAN Edge with CML 2.7+

Introduction 8

Our Gameplan 4

Create the Device Template 9

Configure VPN 0 12

Configure VPN 512 12

Configure Service VPN 10 12

Challenge 5

Preparing for Cloud OnRamp

Introduction 7

The GCP CPU Quota Issue 1

Reconfiguring Our SD-WAN Lab 7

Dealing with NAT Issues 10

Configure Templates for OnRamp 8

Verify OnRamp in SD-WAN Manager 9

Verify OnRamp from the CLI 9

WEEK 13

153 min.

Challenge 6

Cloud OnRamp for AWS

Introduction 1

Prepare the AWS Account for Cloud OnRamp 4

Configure AWS VPCs and Subnets 3

Deploy a VM into our VPC 5

Create an AWS Marketplace Subscription 5

Associate Your AWS Account with OnRamp 3

Configure the Global OnRamp Settings 6

Discover and Tag Desired Networks 2

Attach Template to 'Shadow' Routers 6

Create the Cloud Gateway 6

Verify OnRamp Deployment and Create VPN 6

Challenge 5

Cloud OnRamp for Azure

Prepare the Azure Account for Cloud OnRamp 3

Create an Azure Application 5

Configure vNets and Subnets 6

Deploy a VM into our vNet 5

Associate Your Azure Account with OnRamp 3

Configure the Global OnRamp Settings 6

Discover and Tag Desired Networks 2

Attach Template to 'Shadow' Routers 5

Create the Cloud Gateway 5

Verify OnRamp Deployment and Create VPN 5

Challenge 5

Cloud OnRamp for GCP

Introduction 1

Enable APIs and Create Service Account 8

Configure GCP VPCs and Subnets 5

Deploy a VM into our VPC 4

Associate Service Account with OnRamp 3

Configure the Global OnRamp Settings 5

Discover and Tag Desired Networks	2
Attach Template to 'Shadow' Routers	6
Create the Cloud Gateway	5
Verify OnRamp Deployment and Create VPN	6

WEEK 14

156 min.

Challenge	5
-----------	---

Manual SD-WAN Deployment to AWS

Introduction	1
Examine Our Game Plan	8
Prepare the Cloud Provider Network	13
Deploy the Catalyst 8000v	13
Create and Apply Our Device Templates	9
Verify Control Connections and IP Forwarding	7
Challenge	7

Manual SD-WAN Deployment to Azure

Introduction	1
Examine Our Game Plan	10
Prepare the Cloud Provider Network	13
Deploy the Catalyst 8000v	14
Create and Apply Our Device Templates	7
Verify Control Connections and IP Forwarding	6
Challenge	7

Manual SD-WAN Deployment to GCP

Introduction	2
--------------	---

Examine Our Game Plan	10
Prepare the Cloud Provider Network	9
Deploy the Catalyst 8000v	14

WEEK 15

152 min.

Create and Apply Our Device Templates	7
Verify Control Connections and IP Forwarding	5
Challenge	6

Introducing SD-WAN Policies

Introduction	2
SD-WAN Policy Structure	9
A Closer Look at Data Policies	11
A Closer Look at AAR	8
Configuring Policies	11
Put the Controller into vManage Mode	5
Challenge	7

Examining AppQoE

Introduction	2
AppQoE Overview	7
TCP Optimization	11
Data Redundancy Elimination	11
Packet Duplication	5
Forward Error Correction	13
Challenge	9

Troubleshooting IPsec Cloud Connectivity

Diagnose the Underlay Network 23

WEEK 16

153 min.

Diagnose the IPsec Tunnel 18

Common IPsec Errors 4

Challenge 6

Troubleshooting Cloud Gateways

Introduction 6

Troubleshoot the AWS VPN Gateway 27

Troubleshoot the Azure VPN Gateway 9

Troubleshoot the GCP VPN Gateway 7

Challenge 6

Troubleshooting Routing Protocols - OSPF

Introduction 4

Explore Our Topology 13

Examine OSPF 24

Troubleshoot OSPF 23

Challenge 6

WEEK 17

Troubleshooting Routing Protocols - BGP

157 min.

Introduction 4

Examine BGP 11

BGP Neighborships 17

BGP Path Selection 19

Troubleshoot BGP 18

Challenge 7

Troubleshooting Filtering and Redistribution

Introduction 1

Troubleshoot Filtering 22

Troubleshoot Redistribution 21

Challenge 7

Troubleshooting SD-WAN Cloud Connectivity

Introduction 9

Troubleshoot the SD-WAN Underlay 21

WEEK 18

30 min.

Troubleshoot the SD-WAN Overlay 15

Troubleshoot Cloud OnRamp 10

Challenge 5