Course Outline

Securing The Edge with Cisco SASE
Course SDWSEC: 3 days Instructor Led

All Cisco courses are delivered by a Cisco Authorized Platinum Learning Partner

About this course
SDWSEC is a Cisco SASE (Secure Access Service Edge) training targeted to engineers and technical personnel involved in designing, deploying, operating, and securing Cisco Edge solutions both in enterprise and Service Provider environments. This training is specifically designed for partners and customers implementing secure Cisco SD-WAN integrated with the complete feature set of Cisco Umbrella including DNS Security, Cloud Based Firewall and Secure Internet Gateway. The course walks you through how each integration works and how to design and implement it step-by-step.

At course completion
After completing this course, students will be able to:

- Describe SD-WAN Architecture
- Design Cisco SD-WAN Branch Security
- Implement Cisco SD-WAN Secure Internet and Cloud Access
- Integrate and Troubleshoot Cisco SD-WAN with a SASE Solution

Course Outline

Module 1: Cisco SD-WAN Introduction

- High-level Cisco SD-WAN Deployment models
- Application-level SD-WAN solution
- Cisco SDWAN plan for HA and Scalability
- Cisco SD-WAN solution components: vManage NMS, vSmart Controller, vBond Orchestrator
- Edge Routers (cEdge, vEdge, and Catalyst 8K)
- Cloud Based Deployment vs On-Premises Deployment

Module 2: Zero Touch Provisioning

- Overview
- User Input Required for the ZTP Automatic Authentication Process
- Authentication between the vBond Orchestrator and WAN Edges
- Authentication between the Edge Routers and the vManage NMS
- Authentication between the vSmart Controller and the Edge Routers

Module 3: Cisco SD-WAN Solution

- Overlay Management Protocol (OMP)
- Cisco SD-WAN Circuit Aggregation Capabilities
- Secure Connectivity in Cisco SD-WAN
- Performance Tracking Mechanisms
- Application Discovery
- Dynamic Path Selection

SHI | TRAINING & ADOPTION

Course Outline

- Performance Based Routing
- Direct Internet Access
- Advanced Routing (OSPF, BGP, LISP, VXLAN, MPLS)
- Application Aware Routing
- Localized and Centralized Policies (Data and Control)
- Cisco SD-WAN In-built Security features: App Aware FW, Talos IPS, URL Filtering, Umbrella Integration, and Advanced Malware Protection
- Dynamic Cloud Access: Cloud On-Ramp for SaaS and IaaS (AWS, Azure & GPC)
- API and Programmatic Interaction via Python

Module 4: Deeper Insight into Cisco SD-WAN Security

- Designing Security Requirements within Cisco SD-WAN
    - DIA Security
    - Direct Cloud Access Security
    - Guest User Security
    - Compliance Requirements
- Security Implementation at the Branch Site
- Implementing Zone Based Firewalls on Cisco WAN Edge
- Implementing UTD on Cisco WAN Edge
    - Configuring URL Filtering
    - Configuring Snort IPS
    - Best Practices for UTD setup (Based on production deployment experiences)
- Implementing Advanced Malware Protection
    - Configuring AMP
    - Overview of integration with Threat Grid

Module 5: Designing and Implementing DNS Security

- Prerequisite check before integrating Umbrella with Cisco SD-WAN
    - Making sure you have the correct licensing
    - Platform support check
    - Internet Connectivity check
- Walking through the Umbrella Dashboard
    - Dashboard Overview
    - DNS Policy GUI Overview
    - Firewall Policy GUI Overview
    - Web Policy GUI Overview
    - Umbrella AD/SAML Integration Overview (optional)
- Integrating Cisco Umbrella for DNS Security
    - Umbrella API Integration
- Configuring the DNS Encryption Policy
    - Excluding the local domains
    - Configuring the Security Policy in vManage
    - Implementing the policy at the DIA Sites
- Verification
    - Checking the logs on Umbrella Dashboard
    - Checking the vManage Security Dashboard

Course Outline

Module 6: Cisco SD-WAN and Cisco Umbrella SIG Integration

- SIG Integration Overview
- Configuring Cisco vManage Templates for SIG Tunnel Creation
    - Using the pre-configured Feature Templates in vManage 20.X
- Adding the SD-WAN Routers and Sites in Umbrella Identities
    - Validate that the routers show up from the Umbrella Dashboard
- Designing and Configuring Policy for SIG Redirection
    - Setting up the vSmart Centralized Policies for SIG Redirection on DIA Traffic
- Verification
    - Checking the logs on Umbrella Dashboard
    - Checking the vManage Security Dashboard

Module 7: Cisco SD-WAN and Cisco Umbrella Cloud Firewall Integration

- Umbrella Cloud Firewall Integration Overview
- Configuring Cisco vManage Templates for Firewall Tunnel Creation
    - Using the pre-configured Feature Templates in vManage 20.X
- Adding the SD-WAN Routers and Sites in Umbrella Identities
    - Validate that the routers show up from the Umbrella Dashboard
- Designing and Configuring Policy for Firewall Redirection
    - Setting up the vSmart Centralized Policies for Umbrella FW Redirection on DIA Traffic
- Verification
    - Checking the logs on Umbrella Dashboard
    - Checking the vManage Security Dashboard

Module 8: Troubleshooting Umbrella Integration

- Troubleshooting DNS Security
    - API Integration not working
    - DNS for local domain failing
    - No redirection to Cisco Umbrella for external domains
- Troubleshooting SIG and Firewall
    - Making sure the IPSec Tunnels to Troubleshooting the vManage policies for redirection
    - Load balancing using vManage policies
    - Reviewing logs in Umbrella
- Checking Alarms and Notifications
    - Checking Alarms on vManage
    - Checking Alarms on Cisco Umbrella

Lab Outline:

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

- Onboard Edge
- Onboard Edge via ZTP
- Onboard vSmart Controller

SHI | TRAINING & ADOPTION

Course Outline

- AVC integration and Traffic Visibility
- Application Aware Routing Lab
- Local DIA and Regional DIA
- Backup and Restore using Python API
- Intra Zone Firewall
- Inter Zone Firewall
- UTD integration
    - URL Filtering
    - Snort IPS
- Umbrella Integration
    - DNS Policy
    - Web Policy
- SIG Tunnel Creation
- SIG Tunnel Redirection Policy
- Configuring Policy for Umbrella Firewall Redirection
- Trouble Ticket 1
- Trouble Ticket 2
- Trouble Ticket 3