

Cisco SD-WAN Advanced Policy and Security

Download Whitepaper: Accelerate Your Modernization Efforts with a Cloud-Native Strategy
Get Your Free Copy Now

Course Number: SDWSEC-NTO

Duration: 3 days

Overview

Course Description

Take control of application experience and security at scalemaster advanced Cisco SD WAN policy and SASE integrations in just 3 days. Designed for engineers and architects, this intensive course dives deep into the SD WAN policy framework (centralized/local control & data policies, application aware routing, QoS, segmentation, and security policies, showing you how to harden the edge with SD-WAN integrated security (Firewall, IPS/IDS, Malware Protection and URL filtering). This course also covers the integration between SD-WAN and Cisco Umbrellas full stackDNS Security, Cloud Delivered Firewall, and Secure Internet Gateway. Through step by step design patterns and hands on labs, youll learn how to integrate, operate, and troubleshoot secure Cisco SD WAN across enterprise and service provider environments, enforcing zero trust principles while boosting performance and visibility. By the end, youll be able to build policy with intent, secure users and sites anywhere, and apply best practices that translate directly into reliable, high performing production deployments. The course qualifies for 24 Cisco Continuing Education Credits (CE).

Skills Gained

- Describe the Cisco SD-WAN architecture, explain its key concepts and identify the control components and their roles
- Explain the Secure Enterprise Network (SEN) approach with the secure control plane using DTLS tunnels and secure data plane using IPsec tunnels for a Zero trust networking
- Define Direct Internet Access (DIA) at branch locations in the SD-WAN infrastructure and identify the security challenges associated to it
- List the network security considerations when migrating enterprise applications and services to public cloud and summarize what is Cloud on Ramp and how it addresses security concerns in the context of SaaS and IaaS
- List the multiple security mechanisms included in the SD-WAN integrated security approach, including Zone Based Firewall, Intrusion Detection and Prevention, Advanced Malware Protection and URL filtering, and the use cases and scenarios where they are applied
- Design and deploy security policies with integrated services in SD-WAN infrastructures using SD-WAN Manager workflows
- Identify the security risks involved with the domain name resolution services (DNS) and what are the strategies to shield the DNS lookups
- Design, implement, verify, operate and support DNA security using Cisco Umbrella
- Describe the Secure Internet Gateway (SIG) approach to deploy security into SD-WAN solutions as a Cloud-based service and match the benefits of Cisco Umbrella as SIG solution
- Integrate SD-WAN with Cisco Umbrella for Cloud Firewall services
- Troubleshoot SD-WAN and Cisco Umbrella Integration, diagnosing and solving integration and security policy issues

Who Can Benefit

The primary audience for this course is as follows:

- Systems Engineers
- Technical Solutions Architects
- Field Engineers

Prerequisites

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

- Knowledge of WAN architectures and routing networking concepts
- High-level familiarity with basic network protocols and applications
- Familiarity with common application delivery methods
- Fundamental Understanding of perimeter security

- Basic Cisco SD-WAN familiarity

Audience

Course Details

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
- 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

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
- 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