Cisco Meraki SD-WAN: Advanced Policy, Security and Programmability

Duración: 3 Días **Código del Curso: N1_SDWMER**

Temario:

This course is hands-on training on Cisco Meraki SD-WAN implementations, basic and advanced Cisco Meraki SD-WAN Security features that are available on Meraki MX routers. Deep dive into capabilities like Firewall and Traffic, Application Aware Firewall, AMP Integration, Content Filtering, Threat Protection, and many other advanced features are covered as a part of this training. This course also provides hands-on training on Cisco Meraki SD-WAN Programmability features.

Dirigido a:

The primary audience for this course is as follows:
- Systems Engineers
- Technical Solutions Architects

Objetivos:

- Upon completing this course, the learner will be able to meet these overall objectives:
- Introduction to Cisco Meraki SD-WAN Solution and Products/Components
- Understand key concepts of Cisco Meraki SD-WAN
- Implement Meraki SD-WAN Solution
- Understand Cisco Meraki SD-WAN Security Features
- Implement Firewall and IPS Policies
- Understand Cisco SD-WAN Programmability features
- Script APIs to automate Cisco SD-WAN vManage configurations

Prerequisitos:

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

- Basic networking concepts
- Familiarity with basic network protocols and applications
- Familiarity with common application delivery methods

Contenido:

Module 1: Introduction to Meraki SD-WAN and Meraki Key Concepts

- Meraki Centralized Dashboard
- Meraki key concepts

- Meraki Concentrator Modes

- VPN Topology

- Split Tunnel and Full Tunnel

- Hub and Spoke and VPN Mesh

- Meraki Connection Monitor
- Data Center Redundancy (DC-DC Failover)
- Warm Spare for VPN Concentrators

Module 2: Meraki SD-WAN Deployment Models

- Introduction
- Data Center Deployment
- MX Deployment Considerations

- MX Deployment Considerations

- Upstream DC Switching Considerations

- Routing Considerations

- Firewall Considerations

- Branch Deployment

- AutoVPN at the Branch

- Hub and Spoke VPN Deployment

- Hub Priorities and Design considerations

Module 3: Meraki SD-WAN Security

- Exploring the SD-WAN and Security Dashboard
- Site-to-site VPN Deep Dive
- Client VPN Technologies
- Access control and Splash Page
- NAT and Port Forwarding
- Firewall and Traffic Shaping
- Content Filtering and Threat Protection
- Meraki and Cisco Umbrella Integration

Module 4: Firewall and Traffic Shaping Policies

- MX Firewall Settings

- Outbound Rules

- Appliance Services

- Layer 7 Firewall Rules

- Forwarding Rules

- IP Source Address Spoofing Protection

- Overview and Key Terms

- NAT Modes Implementation

- Supported Deployment Topologies

- SD-WAN and Traffic Shaping

- Uplink Configurations

- Uplink Selections

- Global Bandwidth Limitations

- Traffic Shaping Rules

- Web Cache

Module 5: SD-WAN Security – Content Filtering and Threat Protection

- MX and Active Directory Integrations
- Content Filtering Implementations and Troubleshooting
- Cisco AMP Integrations and Threat Protection
- Threat Grid Integrations

Module 6: Programmable API

- Meraki Dashboard API with Postman
- Meraki Organization and Networks Import into Postman
- Meraki Devices into the appropriate Networks using APIs
- Troubleshooting Meraki using APIs

- Dashboard

- Device Dashboard

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid