KL 004.2.4:

Kaspersky SD-WAN

Featured products

Kaspersky SD-WAN 2.4

Course description

Kaspersky SD-WAN is an enterprise solution for centralized WAN management.

This course explains the architecture of the solution, introduces its capabilities and provides examples of how to configure it.

Our course consists of theoretical materials describing the principles of operation, configuration and troubleshooting, and hands-on labs to gain practical experience.

Upon successful completion of this course, participants will be able to:

- Understand the benefits of software-defined wide area networks over traditional networks
- Understand the specifics of different transport services
- Create new transport services and manage existing ones
- Configure channel selection rules based on the current state of all available channels
- Manage dynamic routing within an SD-WAN network and at its junction with a legacy network

Duration

2 days

Requirements for participants

The course is designed for technical support and pre-sales engineers. Attendees are required to possess:

- Basic understanding of networking technologies, such as TCP/IP, OSPF and BGP routing, VRRP, tunneling at the CCNP/HCNP level
- Understanding of how applications use HTTP/HTTPS and VoIP
- Basic knowledge of Windows and Linux administration
- Basic knowledge of information security principles

Contents

Labs

- Lab 1. Install and configure an SD-WAN server, perform initial configuration of the solution
  - 1.1. Turn on servers and virtual machines
  - 1.2. Install packages and set environment variables on the server
  - 1.3. Start SD-WAN installation using an Ansible playbook
  - 1.4. Open the Kaspersky SD-WAN management console and configure the environment
  - 1.5. Create a new tenant
- Lab 2. Create a physical network function template and deploy the SD-WAN service
  - 2.1. Upload the SD-WAN physical network function template
  - 2.2. Create an SD-WAN service template and deploy the SD-WAN service
- Lab 3. Prepare templates of client network devices and connect them to the Kaspersky SD-WAN service
  - 3.1. Upload the root certificate to Kaspersky SD-WAN
  - 3.2. Prepare and upload the gateway template
  - 3.3. Register the gateway with Kaspersky SD-WAN
  - 3.4. Prepare and upload templates of client network devices
  - 3.5. Register CPE1
  - 3.6. Prepare and import the CPE2_1 and CPE2_2 templates
- Lab 4. Configure Point-to-Multipoint (P2M) and Multipoint-to-Multipoint (M2M) services
  - 4.1. Configure a Point-to-Multipoint service and check its health
  - 4.2. Configure a Multipoint-to-Multipoint service and check its health
  - 4.3. Configure CPE time synchronization using NTP
  - 4.4. Configure dynamic routing via BGP in the WAN segment
  - 4.5. Speed up connectivity loss detection
- Lab 5. Configure connection with legacy networks
  - 5.1. Simulate a non-redundant L3 connection with BGP dynamic routing
  - 5.2. Configure dynamic allocation of IP addresses using DHCP
  - 5.3. Simulate an L3 connection with default gateway redundancy using VRRP
  - 5.4. Simulate a redundant L3 connection with dynamic routing using OSPF
- Lab 6. Test backup and automatic channel failover
- Lab 7. Enable connection quality monitoring and check channel failover when thresholds are exceeded
- Lab 8. Enable and test forward error correction
- Lab 9. Configure traffic management based on DPI
  - 9.1. Specify the "Last resort" setting for the links
  - 9.2. Enable DPI in the firewall CPE template
  - 9.3. Create a rule to classify SSH test traffic
  - 9.4. Create ACL service interfaces
  - 9.5. Create a dedicated transport service for priority traffic
- Lab 10. Migrate client networks to dedicated VRFs on CPE devices
  - 10.1. Configure VRF on GW and CPE1 via the orchestrator
  - 10.2. View settings via the CPE1 console
- Lab 11. Configure PBR between VRFs to organize local breakout
  - 11.1. Configure PBR on CPE1
  - 11.2. Add a default route to BGP on CPE1
- Lab 12. Use REST API to create a new tenant and tenant administrator