



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

CODE:	LENGTH:	PRICE:
JUN_JSPES	24 Hours (3 days)	£2,395.00

Description

This three-day course discusses edge security concepts for the service provider network.

It discusses security for 5G networks on the main GPRS interfaces.

Key topics include deploying an SRX Series device in different parts of the service provider network, implementing CGNAT, DDoS, malware inspection, command-and-control prevention, IPsec tunnels, 5G security, control plane hardening, and BGP hardening.

Students will gain experience in configuring, testing, and troubleshooting the Junos OS through demonstrations and hands-on labs.

This course is based on Junos OS 21.1R1.11.

The Juniper Service Provider Edge Security (JSPES) is an intermediate-level course. Relevant Juniper Product

- Junos OS • SRX Series

Objectives

- Define the general security architecture for 4G and 5G networks.
- Configure data plane security protections.
- Explain DoS and DDoS attacks.
- Describe BGP Flowspec in protecting against DDoS attacks.
- Explain the Corero solution for DDoS attacks.
- Describe the use of stateful firewalls.
- Explain the use of ALGs in stateful security firewalls.
- Explain how to secure BGP on Junos devices.
- Describe how to use IPsec to secure traffic.
- Explain the new IoT threat to networks.
- Describe AutoVPN IPsec architectures.
- Explain the use and configuration of CGNAT on SRX Series devices.

Audience

This course benefits those responsible for implementing, monitoring, and troubleshooting Juniper security components.

Prerequisites

- Intermediate level of TCP/IP networking and security knowledge.
- Attend the Introduction to Juniper Security (JSEC) course before attending this class.

Programme

Day 1 Course Introduction Security Challenges for Service Providers • Describe limitations of security devices

- Describe DDoS attack threats • Describe BGP security threats • Explain IP address depletion challenges

- Describe 5G security challenges Juniper Networks Solutions for Service Providers

- Describe Juniper Networks' security solutions for the service provider challenges Stateful Firewalls

- Describe stateless firewall filters • Describe stateful firewall policies • Describe screens and ALGs • Explain asymmetrical routing

Lab 1: Configure Stateful Firewalls 5G Architecture using SRX Series Devices • Describe security insertion points

- Describe 5G network evolution DDoS Protection • Explain DDoS history and common protections

- Describe SRX DDoS protection • Describe BGP FlowSpec • Describe Corero with MX DDoS protection Lab 2: DDoS Protection

Day 2 Carrier-Grade NAT • Explain IPv4 address exhaustion • Describe Source NAT • Describe CGNAT • Describe NAT64

Lab 3: CGNAT Juniper Connected Security for Service Providers • Explain Juniper Connected Security • Describe SecIntel feeds

- Describe a use case for IoT protection Lab 4: Implementing Juniper Connected Security IPsec Overview

- Describe the IPsec and IKE protocols • Configure site-to-site IPsec VPNs • Describe and configure Proxy IDs and Traffic selectors

- Monitor site-to-site IPsec VPNs • Describe IPsec use with gNodeB devices Lab 5: Site-to-Site IPsec VPN Scaling IPsec

- Describe and implement PKI certificates in Junos OS • Describe AutoVPN • Describe SecGW firewall use case for scaling IPsec

Lab 6: Configuring AutoVPN Day 3 GPRS and GTP • Describe how to secure GTP tunnels • Describe the GPRS protocol

- Describe the GTP • Explain how Roaming Firewall secures GTP SCTP • Describe the SCTP

Lab 7: Video about Implementing the Roaming Firewall (Demo) Securing the Control Plane

- Explain how to secure the control plane on Junos devices • Describe how the loopback filter works to secure the control plane

- Explain how to protect the control plane from DDoS attacks • Describe how to secure the IGP against attacks

Lab 8: Configure Control Plane Protections Securing the BGP • Describe how to secure the BGP • Describe BGP security features
• Describe BGP dampening Lab 9: Configure BGP protections

Session Dates

On request. Please [Contact Us](#)

Additional Information

[This training is also available as onsite training. Please contact us to find out more.](#)