Course Outline

Juniper Networks | Education Services

Juniper Service Provider Edge Security

COURSE OVERVIEW

This three-day, intermediate-level 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. Additional topics include deploying MX-SPC3 card, configuring and verifying IPsec VPNs, and carrier-grade NAT, with unified services framework on MX Series platforms.

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.

COURSE LEVEL

Juniper Service Provider Edge Security is an intermediate course

AUDIENCE

Individuals responsible for implementing, monitoring, and troubleshooting Juniper security components.

PREREQUISITES

- Intermediate level of TCP/IP networking and security knowledge
- Completing the *Introduction to Juniper Security* course

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 devices.

Additional objectives for self-study:

- Describe SPC3 for MX Series platforms.
- Configure and verify IPsec VPN with unified services framework using MX-SPC3.
- Configure and verify carrier-grade NAT with MX-SPC3.
- Troubleshoot some common issues with MX-SPC3.

COURSE CONTENTS

DAY 1

Module 1: Course Introduction

Module 2: 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

Module 3: Juniper Networks Solutions for Service Providers

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

Module 4: Stateful Firewalls

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

Lab 1: Configure Stateful Firewalls

Module 5: 5G Architecture using SRX Devices

- Describe security insertion points
- Describe 5G network evolution

Module 6: Security Policy Options

- 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

Module 7: Carrier-Grade NAT

- Explain IPv4 address exhaustion
- Describe Source NAT
- Describe CGNAT
- Describe NAT64

Lab 3: CGNAT

Module 8: 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

Module 9: 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

Module 10: 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

Module 11: GPRS and GTP

- Describe how to secure GTP tunnels
- Describe the GPRS protocol
- Describe the GTP
- Explain how Roaming Firewall secures GTP

Module 12: SCTP

- Describe the SCTP Protocol

Module 13: 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 7: Configure control plane protections

Module 14: Securing the BGP

- Describe how to secure the BGP
- Describe BGP security features
- Describe BGP dampening

Lab 8: Configure BGP protections

SELF-STUDY MODULES

Module 15: SPC3 for MX Series Platforms

- Identify the main components of SPC3
- Describe the unified services framework

Module 16: IPsec VPN with SPC3 on MX Series Platforms

- Describe USF for IPsec
- Provide configuration and verification examples for the IPsec P2P mode
- Provide configuration and verification examples for the IPsec Traffic Selector mode
- Describe the software architecture of MX-SPC3
- Describe PowerMode IPsec

- Describe Fat Core
- Describe the unified services framework

Module 17: CGNAT with SPC3 on MX Series Platforms

- Describe carrier-grade NAT coverage on Juniper MX Series
- Configure and verify NAT for Next-Gen Services

Module 18: Troubleshooting MX-SPC3

- Describe some common problems and solutions related to MX-SPC3

JSPES20250404