Juniper Security (JSEC) Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Overview

This five-day course covers the configuration, operation, and implementation of SRX Series Services Gateways in a typical network environment. Key topics within this course include security technologies such as security zones, security policies, Network Address Translation (NAT), IP Security (IPsec), and high availability clusters, as well as details pertaining to basic implementation, configuration, management, and troubleshooting.

Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring the Junos OS and monitoring device operations. This course uses Juniper Networks SRX Series Services Gateways and Security Director for the hands-on component. This course is based on Junos OS Release 15.1X49-D70.3 and Junos Space Security Director 16.1.

Prerequisites

Students should have basic networking knowledge and an understanding of the Open Systems Interconnection (OSI) reference model and the TCP/IP protocol suite. Students should also attend the Introduction to the Junos Operating System (IJOS) course, or have equivalent experience prior to attending this class

Who should attend

The course benefits operators of SRX Series devices. These operators include network engineers, administrators, support personnel, and reseller support personnel.

Juniper Security (JSEC) Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

• Describe traditional routing and security and the current trends in internetworking.
• Provide an overview of SRX Series devices and software architecture.
• Describe the logical packet flow and session creation performed by SRX Series
• devices.
• Describe, configure, and monitor zones.
• Describe, configure, and monitor security policies.
• Describe, configure, and monitor user firewall authentication
• Describe various types of network attacks.
• Configure and monitor Screen options to prevent network attacks.
• Explain, implement, and monitor NAT, as implemented on Junos security platforms.
• Explain the purpose and mechanics of IP Security (IPsec) virtual private networks (VPNs).
• Implement and monitor policy-based and route-based IPsec VPNs.
• Describe, configure, and monitor high availability chassis clusters.
• Describe how to deploy and manage vSRX.
• Describe and configure Group VPNs.
• Describe and configure ADVPNs.
• Troubleshoot chassis clusters, IPsec VPNs, zones, and Security Policies