NetTech India

JNCIP-SEC Exam Objectives (Exam: JN0-633)

This list provides a general view of the skill set required to successfully complete the specified certification exam. Topics listed are subject to change.

Application-Aware Security Services

- Describe the concepts, operation and functionality of AppSecure
  - AppSecure traffic processing
  - AppID
  - AppTrack
  - User FW
  - SSL proxy
  - AppFW
  - AppQoS
- Given a scenario, demonstrate knowledge of how to configure, monitor and troubleshoot the various AppSecure modules

Virtualization

- Describe the concepts, operation and functionality of various virtualization components on SRX Series Services Gateways
  - Routing instances
  - RIB groups
  - Routing between instances
  - Logical systems (LSYS)
  - Intra-LSYS and Inter-LSYS communication
- Given a scenario, demonstrate knowledge of how to configure, monitor and troubleshoot the various elements of virtualization
- Given a scenario, describe and implement filter-based forwarding (FBF)

Advanced NAT

- Describe the concepts, operation and functionality of various types of NAT
  - NAT traffic processing
  - Destination NAT
  - Source NAT
  - Persistent NAT
  - Static NAT
  - Double NAT

- NAT traversal
- DNS doctoring
- IPv6 NAT (Carrier-grade NAT) - NAT64, NAT46, NAT444, DS-Lite
- Routing
- NAT and FBF
- NAT and security policy

• Given a scenario, demonstrate knowledge of how to configure, monitor and troubleshoot advanced NAT implementations

Advanced IPSec VPNs

• Describe the concepts, operation and functionality of various IPSec VPN implementations

- IPSec traffic processing
- Site-to-site VPNs
- Hub-and-spoke VPNs
- Group VPNs
- Dynamic VPNs
- Routing over VPNs
- VPNs and NAT
- Public key infrastructure (PKI) for IPSec VPNs
- Traffic Selectors
- VPNs and dynamic gateways

• Given a scenario, demonstrate knowledge of how to configure, monitor and troubleshoot advanced IPSec VPN implementations

Intrusion Prevention

• Describe the concepts, operation and functionality of Junos Intrusion Prevention System (IPS) for SRX Series Services Gateways

- IPS packet inspection process
- IPS rules and rulebases
- Signature-based attack detection
- Reconnaissance scans and fingerprinting
- Flooding, attacks and spoofing

• Describe how to perform setup and initial configuration for SRX Series Services Gateways with IPS functionality

- IPS deployment options and considerations
- Network settings
- Attack database

- Given a scenario, demonstrate knowledge of how to configure mechanisms to detect and protect against scans and attacks
  - Custom signatures
  - Scan prevention

Transparent Mode

- Describe the concepts, operation and functionality of various transparent mode implementations
  - High Availability
  - VLAN translation
  - Layer 2 security
  - IRB
  - Bridge groups
  - Spanning tree traffic processing
- Given a scenario, demonstrate knowledge of how to configure, monitor and troubleshoot transparent mode implementations

Troubleshooting

- Given a scenario, demonstrate knowledge of how to troubleshoot Junos OS security issues
  - Flow analysis
  - SNMP
  - show commands
  - Logging and syslog
  - Tracing, including flow traceoptions
  - Policy flow
  - Packet capture