NetTech India

JNCIS-SEC Exam Objectives (Exam: JN0-332)

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

Junos Security Overview

- Identify concepts, general features and functionality of Junos OS security
  - Junos security architecture
  - Branch vs. high-end platforms
  - Major hardware components of SRX Series services gateways
  - Packet flow
  - Packet-based vs. session-based forwarding

Zones

- Identify concepts, benefits and operation of zones
  - Zone types
  - Dependencies
  - Host inbound packet behavior
  - Transit packet behavior
- Demonstrate knowledge of how to configure, monitor and troubleshoot zones
  - Zone configuration steps
  - Hierarchy priority (Inheritance)
  - Monitoring and troubleshooting

Security Policies

- Identify the concepts, benefits and operation of security policies
  - Policy types (default policy)
  - Policy components
  - Policy ordering
  - Host inbound traffic examination
  - Transit traffic examination
  - Scheduling
  - Rematching
  - ALGs
  - Address books
  - Applications
- Demonstrate knowledge of how to configure, monitor and troubleshoot security policies

- Policies
- ALGs
- Address books
- Custom applications
- Monitoring and troubleshooting

Firewall User Authentication

- Describe the concepts, benefits and operation of firewall user authentication
  - User Firewall
  - User authentication types
  - Authentication server support
  - Client groups

Screens

- Identify the concepts, benefits and operation of Screens
  - Attack types and phases
  - Screen options
- Demonstrate knowledge of how to configure, monitor and troubleshoot Screens
  - Screen configuration steps
  - Monitoring and troubleshooting

NAT

- Identify the concepts, benefits and operation of IPSec VPNs
  - Secure VPN characteristics and components
  - IPSec tunnel establishment
  - IPSec traffic processing
  - Junos OS IPSec implementation options
- Demonstrate knowledge of how to configure, monitor and troubleshoot IPSec VPNs
  - IPSec VPN configuration steps
  - Monitoring and troubleshooting

IPSec VPNs

- Identify the concepts, benefits and operation of IPSec VPNs
  - Secure VPN characteristics and components
  - IPSec tunnel establishment
  - IPSec traffic processing
  - Junos OS IPSec implementation options

- Demonstrate knowledge of how to configure, monitor and troubleshoot IPSec VPNs
  - IPSec VPN configuration steps
  - Monitoring and troubleshooting

High Availability (HA) Clustering

- Identify the concepts, benefits and operation of HA
  - HA features and characteristics
  - Deployment requirements and considerations
  - Chassis cluster characteristics and operation
  - Cluster modes
  - Cluster and node IDs
  - Redundancy groups
  - Cluster interfaces
  - Real-time objects
  - State synchronization
  - Ethernet switching considerations
  - IPSec considerations
  - Manual failover
- Demonstrate knowledge of how to configure, monitor and troubleshoot clustering
  - Cluster preparation
  - Cluster configuration steps
  - Monitoring and troubleshooting

Unified Threat Management (UTM)

- Identify concepts, general features and functionality of UTM
  - Packet flow and processing
  - Design considerations
  - Policy flow
  - Platform support
  - Licensing
- Describe the purpose, configuration and operation of antispam filtering
  - Methods
  - Whitelists vs. blacklists
  - Order of operations
  - Traffic examination
  - Configuration steps using the CLI
  - Monitoring and troubleshooting
- Describe the purpose, configuration and operation of antivirus protection
  - Scanning methods
  - Antivirus flow process
  - Scanning options and actions

- Configuration steps using the CLI
- Monitoring and troubleshooting

• Describe the concepts, benefits and operation of content and Web filtering

- Filtering features and solutions
- Configuration steps using the CLI
- Monitoring and troubleshooting