



JUNIPER JN0-636

Juniper JNCIP Security Certification Questions & Answers

Exam Summary – Syllabus – Questions

JN0-636

[Juniper Networks Certified Professional Security](#)

65 Questions Exam – Variable (60-70% Approx.) Cut Score – Duration of 90 minutes

Table of Contents:

Know Your JN0-636 Certification Well:	2
Juniper JN0-636 JNCIP Security Certification Details:	2
JN0-636 Syllabus:	3
Juniper JN0-636 Sample Questions:	5
Study Guide to Crack Juniper JNCIP Security JN0-636 Exam:	9

Know Your JN0-636 Certification Well:

The JN0-636 is best suitable for candidates who want to gain knowledge in the Juniper Junos Security. Before you start your JN0-636 preparation you may struggle to get all the crucial JNCIP Security materials like JN0-636 syllabus, sample questions, study guide.

But don't worry the JN0-636 PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the JN0-636 syllabus?
- How many questions are there in the JN0-636 exam?
- Which Practice test would help me to pass the JN0-636 exam at the first attempt?

Passing the JN0-636 exam makes you Juniper Networks Certified Professional Security. Having the JNCIP Security certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Juniper JN0-636 JNCIP Security Certification Details:

Exam Name	Security Professional
Exam Code	JN0-636
Exam Price	\$400 USD
Duration	90 minutes
Number of Questions	65
Passing Score	Variable (60-70% Approx.)
Recommended Training	Advanced Juniper Security
Exam Registration	PEARSON VUE
Sample Questions	Juniper JN0-636 Sample Questions
Practice Exam	Juniper Networks Certified Professional Security Practice Test

JN0-636 Syllabus:

Section	Objectives
Firewall Filters	<ul style="list-style-type: none"> - Describe the concepts, operation, or functionality of firewall filters. <ul style="list-style-type: none"> • Selective packet processing • Troubleshooting with firewall filters • Filter-based forwarding - Given a scenario, demonstrate how to configure, troubleshoot, or monitor firewall filters.
Troubleshooting Security Policy and Zones	<ul style="list-style-type: none"> - Given a scenario, demonstrate how to troubleshoot or monitor security policies or security zones. <ul style="list-style-type: none"> • Tools • Logging/tracing • Other outputs
Advanced Threat Protection	<ul style="list-style-type: none"> - Describe the concepts, operation, or functionality of Juniper Advanced Threat Prevention (on-premises appliance or Cloudbased service). <ul style="list-style-type: none"> • Collectors • Custom rules • Mitigation - Given a scenario, demonstrate how to configure or monitor Juniper Advanced Threat Prevention.
Edge Security	<ul style="list-style-type: none"> - Describe the concepts, operation, or functionality of edge security features. <ul style="list-style-type: none"> • Hardware support • Security Intelligence (SecIntel) • Intrusion prevention system (IPS) • Corero DDoS Mitigation • Advanced threat prevention (ATP)
Compliance	<ul style="list-style-type: none"> Describe the concepts or operation of security compliance. <ul style="list-style-type: none"> • Role-based access control (RBAC) • Junos Space® Security Director

Section	Objectives
	<ul style="list-style-type: none"> • Authentication, Authorization, and Accounting (AAA) and Security Assertion Markup Language (SAML) integration
Threat Mitigation	<ul style="list-style-type: none"> - Describe the concepts, operation, or functionality of the logical systems. <ul style="list-style-type: none"> • Administrative roles • Security profiles • Logical systems (LSYS) communication - Describe the concepts, operation, or functionality of the tenant systems. <ul style="list-style-type: none"> • Master and tenant admins • Tenant systems (TSYS) capacity
Logical and Tenant Systems	<ul style="list-style-type: none"> - Describe the concepts, operation, or functionality of the logical systems. <ul style="list-style-type: none"> • Administrative roles • Security profiles • Logical systems (LSYS) communication - Describe the concepts, operation, or functionality of the tenant systems. <ul style="list-style-type: none"> • Master and tenant admins • Tenant systems (TSYS) capacity
Layer 2 Security	<ul style="list-style-type: none"> - Describe the concepts, operation, or functionality of Layer 2 security. <ul style="list-style-type: none"> • Transparent mode • Mixed mode • Secure wire • Media Access Control Security (MACsec) - Given a scenario, demonstrate how to configure or monitor Layer 2 security.
Advanced Network Address Translation (NAT)	<ul style="list-style-type: none"> - Describe the concepts, operation, or functionality of advanced NAT functionality. <ul style="list-style-type: none"> • Persistent NAT • Domain name system (DNS) doctoring

Section	Objectives
	<ul style="list-style-type: none"> • IPv6 NAT - Given a scenario, demonstrate how to configure, troubleshoot, or monitor advanced NAT scenarios.
Advanced IPsec	- Describe the concepts, operation, or functionality of advanced IPsec applications. <ul style="list-style-type: none"> • Remote access VPNs • Hub-and-spoke VPNs • Public Key Infrastructure (PKI) • Auto Discovery VPNs (ADVPNs) • Routing with IPsec • Overlapping IP addresses • Dynamic gateways • IPsec class of service (CoS) - Given a scenario, demonstrate how to configure, troubleshoot, or monitor advanced IPsec functionality.

Juniper JN0-636 Sample Questions:

Question: 1

You installed the IPS license on the SRX Series device and need to download the IPS signature database. What must you do?

- a) Run the request security idp security-package install command; the signature database will be downloaded from Juniper Networks and installed.
- b) Run the request security idp security-package download command followed by the request security idp security-package install command.
- c) Run the request security idp security-package download command; the signature database will be downloaded from Juniper Networks and installed.
- d) Download the signature database from Juniper Networks and run the request security idp security-package download <IP address> to use TFTP to transfer the file from your laptop and install it on the SRX Series device.

Answer: b

Question: 2

Which two methods can be categorized under the reconnaissance phase?

(Choose two.)

- a) using information from the target company website
- b) Xmas attack
- c) ping of death
- d) war dialing scan

Answer: a, d

Question: 3

Your enterprise requires a remote access solution and wants the installation of the VPN client software to be automated and linked to users as they log in to the VPN server.

Which client VPN feature meets this requirement?

- a) Purchase SSL VPN feature licenses and add them to the SRX Series device
- b) Install the Junos Pulse client on the Windows devices at login
- c) Deploy the group VPN SRX Series device feature 1
- d) Deploy the dynamic VPN on the SRX Series device

Answer: d

Question: 4

You are asked to separate several remote branch locations by attaching them to separate SRX Series devices.

You have only one SRX Series device and must accomplish this objective virtually. You are required to have separate routing tables, and each interface must be in different logical devices.

Which type of routing-instance must you use to accomplish this objective?

- a) virtual-router
- b) non-forwarding
- c) policy-based
- d) forwarding

Answer: a

Question: 5

You want to add the IDP attack database to your SRX device. Which two tasks are required to complete this goal?

(Choose two.)

- a) Download the IDP security package.
- b) Download the IDP sensor database.
- c) Install the IDP sensor database.
- d) Install the IDP security package.

Answer: a, d

Question: 6

Your company wants to scale to 200 branches across the globe. Dynamic routing over the VPNs is required and you want to minimize the chance of compromising the keys.

Which type of VPN implementation should you use?

- a) policy-based VPN with preshared key authentication
- b) route-based VPN with preshared key authentication
- c) policy-based VPN with certificate-based authentication
- d) route-based VPN with certificate-based authentication

Answer: d

Question: 7

A security administrator wants to establish a certificate-based VPN between SRXA and SRXB. SRXA receives a certificate from certificate authority CA-A and SRXB receives a certificate from certificate authority CA-B.

Which type of certificates are needed on SRXA to establish the VPN tunnel?

- a) SRXA's local certificate, and SRXA's CA certificate issued by CA-A
- b) SRXA's local certificate, and SRXB's CA certificate issued by CA-B
- c) SRXA's local certificate, and SRXB's local certificate
- d) SRXB's local certificate, SRXA's CA certificate issued by CA-A, and SRXB's CA certificate issued by CA-B

Answer: b

Question: 8

A large company with different partners wants to establish a VPN among the various sites using certificates. One partner receives a certificate from a different CA server than does corporate headquarters.

Which type of certificate format is used on the SRX Series device to establish this VPN?

- a) PKCS10
- b) PKCS7
- c) PKCSS
- d) PKCS12

Answer: b

Question: 9

You have configured DNS doctoring on your SRX device to allow your internal Web server traffic to respond to www.targethost.com. You now want to verify proper DNS doctoring behavior.

Which action allows you to perform this task?

- a) Initiate a ping from an internal host to www.targethost.com.
- b) Initiate a ping from an external host to www.targethost.com.
- c) Initiate a ping from the internal Web server to an external host.
- d) Verify that the DNS ALG is enabled.

Answer: b

Question: 10

You want to configure system security resources for logical systems on SRX devices. Which statement is true regarding the system behavior of security profiles?

- a) They are defined by user administrators within an LSYS.
- b) Up to 512 profiles can be configured.
- c) One security profile can be applied to multiple LSYSs.
- d) Configured limitations of type maximum guarantees system resources.

Answer: c

Study Guide to Crack Juniper JNCIP Security JN0-636 Exam:

- Getting details of the JN0-636 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the JN0-636 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Juniper provided training for JN0-636 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the JN0-636 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on JN0-636 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for JN0-636 Certification

Make NWExam.com your best friend during your Security Professional exam preparation. We provide authentic practice tests for the JN0-636 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual JN0-636 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the JN0-636 exam.

Start Online practice of JN0-636 Exam by visiting URL

<https://www.nwexam.com/juniper/jn0-636-juniper-security-professional-jncip-sec>