実用的なJN0-637シュミレーション問題集 &合格スムーズJN0-637試験対策 |検証するJN0-637真実試験

無料でクラウドストレージから最新のJapancert JN0-637 PDFダンプをダウンロードする：https://drive.google.com/open?id=1UP60rEZpFYfQ3M7H5o6JZoQaN781ECXs

今、私たちJuniperは非常に競争の激しい世界に住んでいます。あなたがまともな仕事を見つけて高い給料を稼ぎたいなら、あなたは優れた能力と豊富な知識を所有していなければなりません。この状況では、JN0-637ガイドトレントを所有することは非常に重要です。特定の分野で優れた能力を習得し、仕事をうまく処理できるからです。私たちが提供するJN0-637試験準備は、JN0-637試験に合格し、簡単にJN0-637試験トレントを所有するという夢を実現するのに役立ちます。

Juniper JN0-637 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• 高度な IPsec VPN: ネットワーク プロフェッショナルに焦点を当てたこのパートでは、高度な IPsec VPN の概念を取り上げ、受験者は実際のアプリケーションでスキルを実証する必要があります。
トピック 2	• 自動化された脅威軽減: このトピックでは、自動化された脅威軽減の概念について説明し、脅威軽減戦略の実装と管理に重点を置いています。
トピック 3	• レイヤー 2 セキュリティ: レイヤー 2 セキュリティの概念をカバーし、関連するシナリオを構成または監視する必要があります。
トピック 4	• セキュリティ ポリシーとセキュリティ ゾーンのトラブルシューティング: このトピックでは、ログ記録やトレースなどのツールを使用してセキュリティ ポリシーとゾーンをトラブルシューティングおよび監視するネットワーク プロフェッショナルのスキルを評価します。
トピック 5	• マルチノード高可用性 (HA): このトピックでは、ネットワーク プロフェッショナルを目指す人がマルチノード HA の概念について知識を得ます。試験に合格するには、受験者は HA システムの構成または監視方法を習得する必要があります。

>> JN0-637シュミレーション問題集 <<

JN0-637試験対策、JN0-637真実試験

常にJuniper JN0-637試験に参加する予定があるお客様は「こちらの問題集には、全部で何問位、掲載されており

ますか？」といった質問を提出しました。心配なくて我々JapancertのJuniper JN0-637試験問題集は実際試験のすべての問題種類をカバーします。70%の問題は解説がありますし、試験の内容を理解しやすいと助けます。

Juniper Security, Professional (JNCIP-SEC) 認定 JN0-637 試験問題 (Q44-Q49):

質問 # 44
You have deployed automated threat mitigation using Security Director with Policy Enforcer, Juniper ATP Cloud, SRX Series devices, and EX Series switches.
In this scenario, which device is responsible for blocking the infected hosts?

- A. Policy Enforcer
- B. Juniper ATP Cloud
- C. EX Series switch
- D. Security Director

正解：A

解説：
Policy Enforcer interacts with other network elements like EX switches to enforce blocking of infected hosts based on threat intelligence from ATP Cloud and other sources.
In a Juniper automated threat mitigation setup involving Security Director, Policy Enforcer, Juniper ATP Cloud, SRX Series, and EX Series switches, the Policy Enforcer is the component responsible for blocking infected hosts.

質問 # 45
You want to bypass IDP for traffic destined to social media sites using APBR, but it is not working and IDP is dropping the session.
What are two reasons for this problem? (Choose two.)

- A. The APBR rule does a match on the first packet.
- B. IDP disable is not configured on the APBR rule.
- C. The application services bypass is not configured on the APBR rule.
- D. The session did not properly reclassify midstream to the correct APBR rule.

正解：C、D

解説：
* Explanation of Answer A (Session Reclassification):
* APBR (Advanced Policy-Based Routing) requires the session to be classified based on the specified rule, which can change midstream as additional packets are processed. If the session was already established before the APBR rule took effect, the traffic may not be correctly reclassified to match the new APBR rule, leading to IDP (Intrusion Detection and Prevention) processing instead of being bypassed. This can occur especially when the session was already established before the rule change.
* Explanation of Answer C (Application Services Bypass):
* For APBR to work and bypass the IDP service, the application services bypass must be explicitly configured. Without this configuration, the APBR rule may redirect the traffic, but the IDP service will still inspect and potentially drop the traffic. This is especially important for traffic destined for specific sites like social media platforms where bypassing IDP is desired.
Example configuration for bypassing IDP services:
bash
set security forwarding-options advanced-policy-based-routing profile <profile-name> application-services- bypass Step-by-Step Resolution:
* Reclassify the Session Midstream:
* If the traffic was already being processed before the APBR rule was applied, ensure that the session is reclassified by terminating the current session or ensuring the APBR rule is applied from the start.
Command to clear the session:
bash
clear security flow session destination-prefix <ip-address>
* Configure Application Services Bypass:
* Ensure that the APBR rule includes the application services bypass configuration to properly bypass IDP or any other security services for traffic that should not be inspected.
Example configuration:
bash

set security forwarding-options advanced-policy-based-routing profile <profile-name> application-services- bypass Juniper Security Reference:
* Session Reclassification in APBR: APBR requires reclassification of sessions in real-time to ensure midstream packets are processed by the correct rule. This is crucial when policies change dynamically or new rules are added.
* Application Services Bypass in APBR: This feature ensures that security services such as IDP are bypassed for traffic that matches specific APBR rules. This is essential for applications where performance is a priority and security inspection is not necessary.

質問 # 46
You are asked to control access to network resources based on the identity of an authenticated device.
Which three steps will accomplish this goal on the SRX Series firewalls? (Choose three)

- A. Apply the end-user-profile at the interface connecting the devices
- B. Reference the end-user-profile in the security policy.
- C. Reference the end-user-profile in the security zone
- D. Configure the authentication source to be used to authenticate the device
- E. Configure an end-user-profile that characterizes a device or set of devices

正解：B、D、E

解説：
To control access to network resources based on the identity of an authenticated device on the SRX Series firewalls, you need to perform the following steps:
A) Configure an end-user-profile that characterizes a device or set of devices. An end-user-profile is a device identity profile that contains a collection of attributes that are characteristics of a specific group of devices, or of a specific device, depending on the attributes configured in the profile. The end-user- profile must contain a domain name and at least one value in each attribute. The attributes include device-identity, device-category, device-vendor, device-type, device-os, and device-os-version1. You can configure an end-user-profile by using the Junos Space Security Director or the CLI2.
C) Reference the end-user-profile in the security policy. A security policy is a rule that defines the action to be taken for the traffic that matches the specified criteria, such as source and destination addresses, zones, protocols, ports, and applications. You can reference the end-user-profile in the source-end-user- profile field of the security policy to identify the traffic source based on the device from which the traffic issued. The SRX Series device matches the IP address of the device to the end-user-profile and applies the security policy accordingly3. You can reference the end-user-profile in the security policy by using the Junos Space Security Director or the CLI4.
E) Configure the authentication source to be used to authenticate the device. An authentication source is a system that provides the device identity information to the SRX Series device. The authentication source can be Microsoft Windows Active Directory or a third-party network access control (NAC) system.
You need to configure the authentication source to be used to authenticate the device and to send the device identity information to the SRX Series device. The SRX Series device stores the device identity information in the device identity authentication table5. You can configure the authentication source by using the Junos Space Security Director or the CLI6.
The other options are incorrect because:
B) Referencing the end-user-profile in the security zone is not a valid step to control access to network resources based on the identity of an authenticated device. A security zone is a logical grouping of interfaces that have similar security requirements. You can reference the user role in the security zone to identify the user who is accessing the network resources, but not the end-user-profile7.
D) Applying the end-user-profile at the interface connecting the devices is also not a valid step to control access to network resources based on the identity of an authenticated device. You cannot apply the end- user-profile at the interface level, but only at the security policy level. The end-user-profile is not a firewall filter or a security policy, but a device identity profile that is referenced in the security policy1.
Reference: End User Profile Overview Creating an End User Profile source-end-user-profile Creating Firewall Policy Rules Understanding the Device Identity Authentication Table and Its Entries Configuring the Authentication Source for Device Identity user-role

質問 # 47
Exhibit:
You are configuring NAT64 on your SRX Series device. You have committed the configuration shown in the exhibit. Unfortunately, the communication with the 10.10.201.10 server is not working. You have verified that the interfaces, security zones, and security policies are all correctly configured.
In this scenario, which action will solve this issue?

- A. Configure proxy-ARP on the external IPv4 interface for the 10.10.201.10/32 address.
- B. Configure destination NAT to translate return traffic from the IPv4 address to the IPv6 address of your source device.
- C. Configure source NAT to translate return traffic from IPv4 address to the IPv6 address of your source device.
- D. Configure proxy-NDP on the IPv6 interface for the 2001:db8::1/128 address.

正解：B

質問 # 48
You are configuring advanced policy-based routing. You have created a static route with next hop of an interface in your inet.0 routing table

Referring to the exhibit, what should be changed to solve this issue?

- A. You should move the static route configuration to the main routing instance.
- B. You should move the inet. o table before the routing instance table in your rib-groups configuration.
- C. You should delete the interface-routes configuration under the routing-options hierarchy.
- D. You should change the routing instance type to virtual-router.

正解：B

質問 # 49
.....

10年以上のビジネス経験により、当社のJN0-637テストトレントは、顧客の購入体験を非常に重要視していました。電子製品の購入速度を心配する必要はありません。弊社では、JN0-637試験準備の信頼性を長期間にわたって評価および評価し、保証された購入スキームを提案するために尽力しています。

JN0-637試験対策: https://www.japancert.com/JN0-637.html

- 有難い-高品質なJN0-637シュミレーション問題集試験-試験の準備方法JN0-637試験対策 □ 「 www.passtest.jp 」で□ JN0-637 □を検索して、無料でダウンロードしてくださいJN0-637日本語版対策ガイド
- JN0-637日本語版対策ガイド □ JN0-637模擬試験最新版 □ JN0-637模擬試験サンプル □ 今すぐ➽ www.goshiken.com □を開き、“JN0-637 ”を検索して無料でダウンロードしてくださいJN0-637認定試験トレーリング
- 有難い-高品質なJN0-637シュミレーション問題集試験-試験の準備方法JN0-637試験対策 □ （ www.japancert.com ）から{ JN0-637 }を検索して、試験資料を無料でダウンロードしてくださいJN0-637日本語版トレーリング
- JN0-637試験問題 □ JN0-637認定試験トレーリング □ JN0-637日本語関連対策 □ ☀ www.goshiken.com □☀□サイトで▶ JN0-637 ◀の最新問題が使えるJN0-637テスト対策書
- JN0-637予想試験 □ JN0-637テスト参考書 □ JN0-637過去問無料 □ ➥ www.it-passports.com □には無料の「 JN0-637 」問題集がありますJN0-637認定試験トレーリング
- JN0-637日本語サンプル □ JN0-637資格認定試験 □ JN0-637日本語版対策ガイド □ ⇛ www.goshiken.com ⇚に移動し、✔ JN0-637 □✔□を検索して無料でダウンロードしてくださいJN0-637オンライン試験
- JN0-637テスト対策書 □ JN0-637学習関連題 □ JN0-637テスト参考書 □ ウェブサイト（ www.jpexam.com ）を開き、➡ JN0-637 □□□を検索して無料でダウンロードしてくださいJN0-637認定試験トレーリング
- JN0-637問題数 □ JN0-637過去問無料 □ JN0-637受験記 □ ➥ JN0-637 □の試験問題は【 www.goshiken.com 】で無料配信中JN0-637専門試験
- JN0-637受験記 □ JN0-637オンライン試験 □ JN0-637認定試験トレーリング □ ⇛ www.japancert.com ⇚から簡単に⇛ JN0-637 ⇚を無料でダウンロードできますJN0-637学習教材
- 実際的JN0-637｜ハイパスレートのJN0-637シュミレーション問題集試験｜試験の準備方法Security, Professional (JNCIP-SEC)試験対策 □ 時間限定無料で使える□ JN0-637 □の試験問題は□ www.goshiken.com □サイトで検索JN0-637認定試験トレーリング
- JN0-637日本語版対策ガイド □ JN0-637テスト難易度 □ JN0-637資格認定試験 □ ➠ www.mogiexam.com □で（ JN0-637 ）を検索して、無料で簡単にダウンロードできますJN0-637受験記
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,

2026年Japancertの最新JN0-637 PDFダンプおよびJN0-637試験エンジンの無料共有：https://drive.google.com/open?id=1UP60rEZpFYfQ3M7H5o6JZoQaN781ECXs