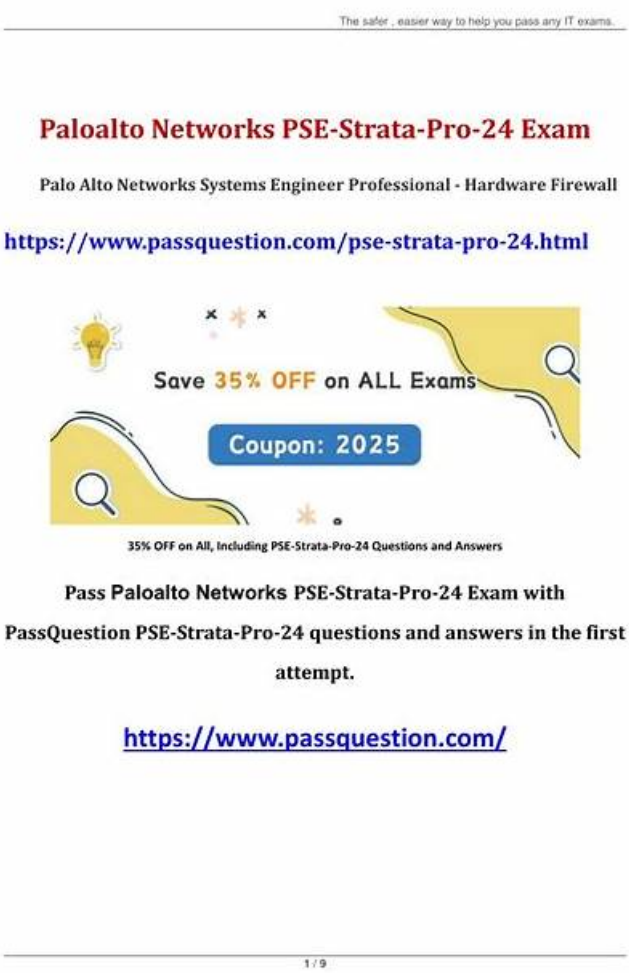
100% Pass Palo Alto Networks - Professional PSE-Strata-Pro-24 - Palo Alto Networks Systems Engineer Professional - Hardware Firewall Free Exam Questions



P.S. Free & New PSE-Strata-Pro-24 dumps are available on Google Drive shared by Real4test: https://drive.google.com/open?id=1-_AgTBEhefHAqebvzPQvsRN4nf4r8g-t

Do you want to obtain the latest information for your exam timely? Then you can choose us, since we can do that for you. PSE-Strata-Pro-24 study guide of us offers you free update for 365 days, so that you can get the latest information for the exam timely. And the latest version for PSE-Strata-Pro-24 exam materials will be sent to your email automatically. In addition, PSE-Strata-Pro-24 Exam Materials are compiled by experienced experts who are quite familiar with the exam center, therefore the quality can be guaranteed. We have online and offline service, and if you have any questions for PSE-Strata-Pro-24 exam dumps, you can consult us.

You can customize the time and Palo Alto Networks PSE-Strata-Pro-24 questions of our Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) practice exams according to your needs. Real Palo Alto Networks PSE-Strata-Pro-24 exam environment which our web-based and desktop PSE-Strata-Pro-24 Practice Exams create is beneficial to get accustomed to the real PSE-Strata-Pro-24 exam pattern.

>> PSE-Strata-Pro-24 Free Exam Questions <<

Quiz Palo Alto Networks - PSE-Strata-Pro-24 –Professional Free Exam Questions

The study material is available in three easy-to-access formats. The first one is PDF format which is printable and portable. You can access it anywhere with your smart devices like smartphones, tablets, and laptops. In addition, you can even print PDF questions in order to study anywhere and pass Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) certification exam.

Palo Alto Networks PSE-Strata-Pro-24 Exam Syllabus Topics:

Topic	Details
Topic 1	• Network Security Strategy and Best Practices: This section of the exam measures the skills of Security Strategy Specialists and highlights the importance of the Palo Alto Networks five-step Zero Trust methodology. Candidates must understand how to approach and apply the Zero Trust model effectively while emphasizing best practices to ensure robust network security.
Topic 2	• Deployment and Evaluation: This section of the exam measures the skills of Deployment Engineers and focuses on identifying the capabilities of Palo Alto Networks NGFWs. Candidates will evaluate features that protect against both known and unknown threats. They will also explain identity management from a deployment perspective and describe the proof of value (PoV) process, which includes assessing the effectiveness of NGFW solutions.
Topic 3	• Architecture and Planning: This section of the exam measures the skills of Network Architects and emphasizes understanding customer requirements and designing suitable deployment architectures. Candidates must explain Palo Alto Networks' platform networking capabilities in detail and evaluate their suitability for various environments. Handling aspects like system sizing and fine-tuning is also a critical skill assessed in this domain.
Topic 4	• Business Value and Competitive Differentiators: This section of the exam measures the skills of Technical Business Value Analysts and focuses on identifying the value proposition of Palo Alto Networks Next-Generation Firewalls (NGFWs). Candidates will assess the technical business benefits of tools like Panorama and SCM. They will also recognize customer-relevant topics and align them with Palo Alto Networks' best solutions. Additionally, understanding Strata's unique differentiators is a key component of this domain.

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q35-Q40):

NEW QUESTION # 35
Regarding APIs, a customer RFP states: "The vendor's firewall solution must provide an API with an enforcement mechanism to deactivate API keys after two hours." How should the response address this clause?

- A. Yes - This is the default setting for API keys.
- B. Yes - The default setting must be changed from no limit to 120 minutes.
- C. No - The PAN-OS XML API does not support keys.
- D. No - The API keys can be made, but there is no method to deactivate them based on time.

Answer: B

Explanation:
Palo Alto Networks' PAN-OS supports API keys for authentication when interacting with the firewall's RESTful and XML-based APIs. By default, API keys do not have an expiration time set, but the expiration time for API keys can be configured by an administrator to meet specific requirements, such as a time-based deactivation after two hours. This is particularly useful for compliance and security purposes, where API keys should not remain active indefinitely.
Here's an evaluation of the options:
* Option A:This is incorrect because the default setting for API keys does not include an expiration time.
By default, API keys are valid indefinitely unless explicitly configured otherwise.

* Option B:This is incorrect because PAN-OS fully supports API keys. The API keys are integral to managing access to the firewall's APIs and provide a secure method for authentication.
* Option C:This is incorrect because PAN-OS does support API key expiration when explicitly configured. While the default is "no expiration," the feature to configure an expiration time (e.g., 2 hours) is available.
* Option D (Correct):The correct response to the RFP clause is that the default API key settings need to be modified to set the expiration time to 120 minutes (2 hours). This aligns with the customer requirement to enforce API key deactivation based on time. Administrators can configure this using the PAN-OS management interface or the CLI.
How to Configure API Key Expiration (Steps):
* Access theWeb InterfaceorCLIon the firewall.
* Navigate toDevice > Management > API Key Lifetime Settings(on the GUI).
* Set the desired expiration time (e.g., 120 minutes).
* Alternatively, use the CLI to configure the API key expiration:
set deviceconfig system api-key-expiry <time-in-minutes>
commit
* Verify the configuration using the show command or by testing API calls to ensure the key expires after the set duration.
References:
* Palo Alto Networks API Documentation: https://docs.paloaltonetworks.com/apis
* Configuration Guide: Managing API Key Expiration

NEW QUESTION # 36
A customer has acquired 10 new branch offices, each with fewer than 50 users and no existing firewall.
The systems engineer wants to recommend a PA-Series NGFW with Advanced Threat Prevention at each branch location. Which NGFW series is the most cost-efficient at securing internet traffic?

- A. PA-600
- B. PA-500
- C. PA-200
- D. PA-400

Answer: D

Explanation:
ThePA-400 Seriesis the most cost-efficient Palo Alto Networks NGFW for small branch offices. Let's analyze the options:
PA-400 Series (Recommended Option)
* The PA-400 Series (PA-410, PA-415, etc.) is specifically designed for small to medium-sized branch offices with fewer than 50 users.
* It provides all the necessary security features, including Advanced Threat Prevention, at a lower price point compared to higher-tier models.
* It supports PAN-OS and Cloud-Delivered Security Services (CDSS), making it suitable for securing internet traffic at branch locations.
Why Other Options Are Incorrect
* PA-200:The PA-200 is an older model and is no longer available. It lacks the performanceand features needed for modern branch office security.
* PA-500:The PA-500 is also an older model that is not as cost-efficient as the PA-400 Series.
* PA-600:The PA-600 Series does not exist.
Key Takeaways:
* For branch offices with fewer than 50 users, the PA-400 Series offers the best balance of cost and performance.
References:
* Palo Alto Networks PA-400 Series Datasheet

NEW QUESTION # 37
Which two compliance frameworks are included with the Premium version of Strata Cloud Manager (SCM)? (Choose two)

- A. National Institute of Standards and Technology (NIST)
- B. Payment Card Industry (PCI)
- C. Center for Internet Security (CIS)
- D. Health Insurance Portability and Accountability Act (HIPAA)

Answer: A,B

Explanation:
Step 1: Understanding Strata Cloud Manager (SCM) Premium
Strata Cloud Manager is a unified management interface for Strata NGFWs, Prisma Access, and other Palo Alto Networks solutions. The Premium version (subscription-based) includes advanced features like:
* AIOps Premium: Predictive analytics, capacity planning, and compliance reporting.
* Compliance Posture Management: Pre-built dashboards and reports for specific regulatory frameworks.
Compliance frameworks in SCM Premium provide visibility into adherence to standards like PCI DSS and NIST, generating actionable insights and audit-ready reports based on firewall configurations, logs, and traffic data.
Reference: Strata Cloud Manager Documentation
"SCM Premium delivers compliance reporting for industry standards, integrating with NGFW telemetry to ensure regulatory alignment." Step 2: Evaluating the Compliance Frameworks Option A: Payment Card Industry (PCI) Analysis: The Payment Card Industry Data Security Standard (PCI DSS) is a mandatory framework for organizations handling cardholder data. SCM Premium includes a PCI DSS Compliance Dashboard that maps NGFW configurations (e.g., security policies, decryption, Threat Prevention) to PCI DSS requirements (e.g., Requirement 1: Firewall protection, Requirement 6: Vulnerability protection). It tracks compliance with controls like network segmentation, encryption, and monitoring, critical for Strata NGFW deployments in payment environments.
Evidence: Palo Alto Networks emphasizes PCI DSS support in SCM Premium for retail, financial, and e- commerce customers, providing pre-configured reports for audits.
Conclusion: Included in SCM Premium.
Reference: Strata Cloud Manager Premium Features Overview
"PCI DSS compliance reporting ensures cardholder data protection with automated insights." Option B: National Institute of Standards and Technology (NIST) Analysis: NIST frameworks, notably the NIST Cybersecurity Framework (CSF) and NIST SP 800-53, are widely adopted for cybersecurity risk management, especially in government and critical infrastructure sectors. SCM Premium offers a NIST Compliance Dashboard, aligning NGFW settings (e.g., App-ID, User- ID, logging) with NIST controls (e.g., Identify, Protect, Detect, Respond, Recover). This is key for Strata customers needing federal compliance or a risk-based approach.
Evidence: Palo Alto Networks documentation highlights NIST CSF and 800-53 mapping in SCM Premium, reflecting its broad applicability.
Conclusion: Included in SCM Premium.
Reference: Strata Cloud Manager AIOps Premium Datasheet
"NIST compliance reporting supports risk management and regulatory adherence." Option C: Center for Internet Security (CIS) Analysis: The CIS Controls and Benchmarks provide practical cybersecurity guidelines (e.g., CIS Controls v8, CIS Benchmarks for OS hardening). While Palo Alto Networks supports CIS principles (e.g., via Best Practice Assessments), SCM Premium documentation does not explicitly list a dedicated CIS Compliance Dashboard. CIS alignment is often manual or supplementary, not a pre-built feature like PCI or NIST.
Evidence: No direct evidence in SCM Premium feature sets confirms CIS as a standard inclusion; it's more commonly referenced in standalone tools like CIS-CAT or Expedition.
Conclusion: Not included in SCM Premium.
Reference: PAN-OS Administrator's Guide (11.1) - Best Practices
"CIS alignment is supported but not a native SCM Premium framework."
Option D: Health Insurance Portability and Accountability Act (HIPAA)
Analysis: HIPAA governs protected health information (PHI) security in healthcare. While Strata NGFWs can enforce HIPAA-compliant policies (e.g., encryption, access control), SCM Premium does not feature a dedicated HIPAA Compliance Dashboard. HIPAA compliance is typically achieved through custom configurations and external audits, not a pre-configured SCM framework.
Evidence: Palo Alto Networks documentation lacks mention of HIPAA as a standard SCM Premium offering, unlike PCI and NIST.
Conclusion: Not included in SCM Premium.
Reference: Strata Cloud Manager Documentation
"HIPAA compliance is supported via NGFW capabilities, not SCM Premium dashboards." Step 3: Why A and B Are Correct A (PCI): Directly addresses a common Strata NGFW use case (payment security) with a tailored dashboard, reflecting SCM Premium's focus on industry-specific compliance.
B (NIST): Provides a flexible, widely adopted framework for cybersecurity, integrated into SCM Premium for broad applicability across sectors.
Exclusion of C and D: CIS and HIPAA, while relevant to NGFW deployments, lack dedicated, pre-built compliance reporting in SCM Premium, making them supplementary rather than core inclusions.
Step 4: Verification Against SCM Premium Features
SCM Premium's compliance posture management explicitly lists PCI DSS and NIST (e.g., CSF, 800-53) as supported frameworks, leveraging NGFW telemetry (e.g., Monitor > Logs > Traffic) and AIOps analytics.
This aligns with Palo Alto Networks' focus on high-demand regulations as of PAN-OS 11.1 and SCM updates through March 08, 2025.

Reference: Strata Cloud Manager Release Notes (March 2025)
"Premium version includes PCI DSS and NIST compliance dashboards for automated reporting." Conclusion The two compliance frameworks included with the Premium version of Strata Cloud Manager are A.
Payment Card Industry (PCI) and B. National Institute of Standards and Technology (NIST). These are verified by SCM Premium's documented capabilities, ensuring Strata NGFW customers can meet regulatory requirements efficiently.

NEW QUESTION # 38
A prospective customer wants to validate an NGFW solution and seeks the advice of a systemsengineer (SE) regarding a design to meet the following stated requirements:
"We need an NGFW that can handle 72 Gbps inside of our core network. Our core switches only have up to
40 Gbps links available to which new devices can connect. We cannot change the IP address structure of the environment, and we need protection for threat prevention, DNS, and perhaps sandboxing." Which hardware and architecture/design recommendations should the SE make?

- A. PA-5430 or larger to cover the bandwidth need and the link types; Architect aggregate interface groups in Layer-3 mode that include 40Gbps interfaces on both sides of the path.
- B. PA-5445 or larger to cover the bandwidth need and the link types; Architect aggregate interface groups in Layer-3 mode that include 40Gbps interfaces on both sides of the path.
- C. PA-5445 or larger to cover the bandwidth need and the link types; Architect aggregate interface groups in Layer-2 or virtual wire mode that include 2 x 40Gbps interfaces on both sides of the path.
- D. PA-5430 or larger to cover the bandwidth need and the link types; Architect aggregate interface groups in Layer-2 or virtual wire mode that include 2 x 40Gbps interfaces on both sides of the path.

Answer: C

Explanation:
The problem provides several constraints and design requirements that must be carefully considered:
* Bandwidth Requirement:
* The customer needs an NGFW capable of handling a total throughput of 72 Gbps.
* The PA-5445 is specifically designed for high-throughput environments and supports up to81.3 Gbps Threat Prevention throughput(as per the latest hardware performance specifications).
This ensures the throughput needs are fully met with some room for growth.
* Interface Compatibility:
* The customer mentions that their core switches support up to40 Gbps interfaces. The design must include aggregate links to meet the overall bandwidth while aligning with the 40 Gbps interface limitations.
* The PA-5445 supports40Gbps QSFP+ interfaces, making it a suitable option for the hardware requirement.
* No Change to IP Address Structure:
* Since the customer cannot modify their IP address structure, deploying the NGFW inLayer-2 or Virtual Wire modeis ideal.
* Virtual Wire modeallows the firewall to inspect traffic transparently between two Layer-2 devices without modifying the existing IP structure. Similarly, Layer-2 mode allows the firewall to behave like a switch at Layer-2 while still applying security policies.
* Threat Prevention, DNS, and Sandboxing Requirements:
* The customer requires advanced security features likeThreat Preventionand potentially sandboxing(WildFire). The PA-5445 is equipped to handle these functionalities with its dedicated hardware-based architecture for content inspection and processing.
* Aggregate Interface Groups:
* The architecture should includeaggregate interface groupsto distribute traffic across multiple physical interfaces to support the high throughput requirement.
* By aggregating2 x 40Gbps interfaces on both sides of the pathin Virtual Wire or Layer-2 mode, the design ensures sufficient bandwidth (up to 80 Gbps per side).
Why PA-5445 in Layer-2 or Virtual Wire mode is the Best Option:
* Option Asatisfies all the customer's requirements:
* The PA-5445 meets the 72 Gbps throughput requirement.
* 2 x 40 Gbps interfaces can be aggregated to handle traffic flow between the core switches and the NGFW.
* Virtual Wire or Layer-2 mode preserves the IP address structure, while still allowing full threat prevention and DNS inspection capabilities.
* The PA-5445 also supports sandboxing (WildFire) for advanced file-based threat detection.
Why Not Other Options:
Option B:
* The PA-5430 is insufficient for the throughput requirement (72 Gbps). Itsmaximum Threat Prevention throughput is 60.3 Gbps, which does not provide the necessary capacity.
Option C:

* While the PA-5445 is appropriate, deploying it inLayer-3 modewould require changes to the IP address structure, which the customer explicitly stated is not an option.
Option D:
* The PA-5430 does not meet the throughput requirement. Although Layer-2 or Virtual Wire mode preserves the IP structure, the throughput capacity of the PA-5430 is a limiting factor.
References from Palo Alto Networks Documentation:
* Palo Alto Networks PA-5400 Series Datasheet (latest version)
* Specifies the performance capabilities of the PA-5445 and PA-5430 models.
* Palo Alto Networks Virtual Wire Deployment Guide
* Explains how Virtual Wire mode can be used to transparently inspect traffic without changing the existing IP structure.
* Aggregated Ethernet Interface Documentation
* Details the configuration and use of aggregate interface groups for high throughput.

NEW QUESTION # 39
Which two statements correctly describe best practices for sizing a firewall deployment with decryption enabled? (Choose two.)

- A. Rivest-Shamir-Adleman (RSA) certificate authentication method (not the RSA key exchange algorithm) consumes more resources than Elliptic Curve Digital Signature Algorithm (ECDSA), but ECDSA is more secure.
- B. SSL decryption traffic amounts vary from network to network.
- C. Large average transaction sizes consume more processing power to decrypt.
- D. Perfect Forward Secrecy (PFS) ephemeral key exchange algorithms such as Diffie-Hellman Ephemeral (DHE) and Elliptic-Curve Diffie-Hellman Exchange (ECDHE) consume more processing resources than Rivest-Shamir-Adleman (RSA) algorithms.

Answer: B,D

Explanation:
When planning a firewall deployment with SSL/TLS decryption enabled, it is crucial to consider the additional processing overhead introduced by decrypting and inspecting encrypted traffic. Here are the details for each statement:
* Why "SSL decryption traffic amounts vary from network to network" (Correct Answer A)?SSL decryption traffic varies depending on the organization's specific network environment, user behavior, and applications. For example, networks with heavy web traffic, cloud applications, or encrypted VoIP traffic will have more SSL/TLS decryption processing requirements. This variability means each deployment must be properly assessed and sized accordingly.
* Why "Perfect Forward Secrecy (PFS) ephemeral key exchange algorithms such as Diffie-Hellman Ephemeral (DHE) and Elliptic-Curve Diffie-Hellman Exchange (ECDHE) consume more processing resources than Rivest-Shamir-Adleman (RSA) algorithms" (Correct Answer C)?PFS algorithms like DHE and ECDHE generate unique session keys for each connection, ensuring better security but requiring significantly more processing power compared to RSA key exchange. When decryption is enabled, firewalls must handle these computationally expensive operations for every encrypted session, impacting performance and sizing requirements.
* Why not "Large average transaction sizes consume more processing power to decrypt" (Option B)?While large transaction sizes can consume additional resources, SSL/TLS decryption is more dependent on the number of sessions and the complexity of the encryption algorithms used, rather than the size of the transactions. Hence, this is not a primary best practice consideration.
* Why not "Rivest-Shamir-Adleman (RSA) certificate authentication method consumes more resources than Elliptic Curve Digital Signature Algorithm (ECDSA), but ECDSA is more secure" (Option D)?This statement discusses certificate authentication methods, not SSL/TLS decryption performance. While ECDSA is more efficient and secure than RSA, it is not directly relevant to sizing considerations for firewall deployments with decryption enabled.
Reference: Palo Alto Networks SSL Decryption Best Practices outlines considerations for sizing deployments with decryption, including variability in SSL traffic and the impact of encryption algorithms like ECDHE.

NEW QUESTION # 40
.....

Experience □ Enter ☀ www.prep4sures.top □☀□ and search for ✔ PSE-Strata-Pro-24 □✔□ to download for free □ □New PSE-Strata-Pro-24 Test Experience

- Test PSE-Strata-Pro-24 Questions □ New PSE-Strata-Pro-24 Exam Book □ Test PSE-Strata-Pro-24 Questions ～ Search for ➤ PSE-Strata-Pro-24 □ and download exam materials for free through ✔ www.pdfvce.com □✔□ □PSE-Strata-Pro-24 Exam Success
- Free PDF Quiz Palo Alto Networks - Efficient PSE-Strata-Pro-24 - Palo Alto Networks Systems Engineer Professional - Hardware Firewall Free Exam Questions □ Search for ▸ PSE-Strata-Pro-24 ◂ and download it for free on ➥ www.exams4collection.com □ website □PSE-Strata-Pro-24 Reliable Real Test
- PSE-Strata-Pro-24 Free Download □ PSE-Strata-Pro-24 Exam Success □ Valid PSE-Strata-Pro-24 Exam Tutorial □ Open website 「 www.pdfvce.com 」 and search for ▸ PSE-Strata-Pro-24 ◂ for free download ☮Valid PSE-Strata-Pro-24 Exam Tutorial
- 100% Pass Quiz 2025 Palo Alto Networks PSE-Strata-Pro-24: Marvelous Palo Alto Networks Systems Engineer Professional - Hardware Firewall Free Exam Questions □ Search for ➠ PSE-Strata-Pro-24 □ and download it for free immediately on ➥ www.passcollection.com □ ☣Valid PSE-Strata-Pro-24 Exam Tutorial
- PSE-Strata-Pro-24 Reliable Real Test □ PSE-Strata-Pro-24 Reliable Exam Pattern □ PSE-Strata-Pro-24 Reliable Real Test □ Search for ▹ PSE-Strata-Pro-24 ◃ and obtain a free download on 「 www.pdfvce.com 」 □Test PSE-Strata-Pro-24 Questions
- PSE-Strata-Pro-24 Test Torrent □ PSE-Strata-Pro-24 Test Pattern □ PSE-Strata-Pro-24 Free Download □ （ www.testsdumps.com ） is best website to obtain [PSE-Strata-Pro-24] for free download □Exam PSE-Strata-Pro-24 Answers
- 100% Pass 2025 PSE-Strata-Pro-24: Palo Alto Networks Systems Engineer Professional - Hardware Firewall Fantastic Free Exam Questions □ Go to website □ www.pdfvce.com □ open and search for 《 PSE-Strata-Pro-24 》 to download for free □New PSE-Strata-Pro-24 Test Experience
- Unparalleled Palo Alto Networks - PSE-Strata-Pro-24 - Palo Alto Networks Systems Engineer Professional - Hardware Firewall Free Exam Questions □ Simply search for ⇛ PSE-Strata-Pro-24 ⇚ for free download on ➠ www.pass4leader.com □ □Latest PSE-Strata-Pro-24 Practice Materials
- Valid PSE-Strata-Pro-24 test answers - Palo Alto Networks PSE-Strata-Pro-24 exam pdf - PSE-Strata-Pro-24 actual test □ Download { PSE-Strata-Pro-24 } for free by simply entering 「 www.pdfvce.com 」 website □Latest PSE-Strata-Pro-24 Practice Materials
- PSE-Strata-Pro-24 Relevant Answers □ PSE-Strata-Pro-24 Guaranteed Success □ PSE-Strata-Pro-24 Relevant Answers □ Open ➽ www.prep4pass.com □ and search for 《 PSE-Strata-Pro-24 》 to download exam materials for free □PSE-Strata-Pro-24 Relevant Answers
- www.stes.tyc.edu.tw, 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, study.stcs.edu.np, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ncon.edu.sa, marciealfredo.pointblog.net, tutorxpert.com.au, 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, aynwlqalam.com, Disposable vapes

P.S. Free & New PSE-Strata-Pro-24 dumps are available on Google Drive shared by Real4test: https://drive.google.com/open?id=1-_AgTBEhefHAqebvzPQvsRN4nf4r8g-t