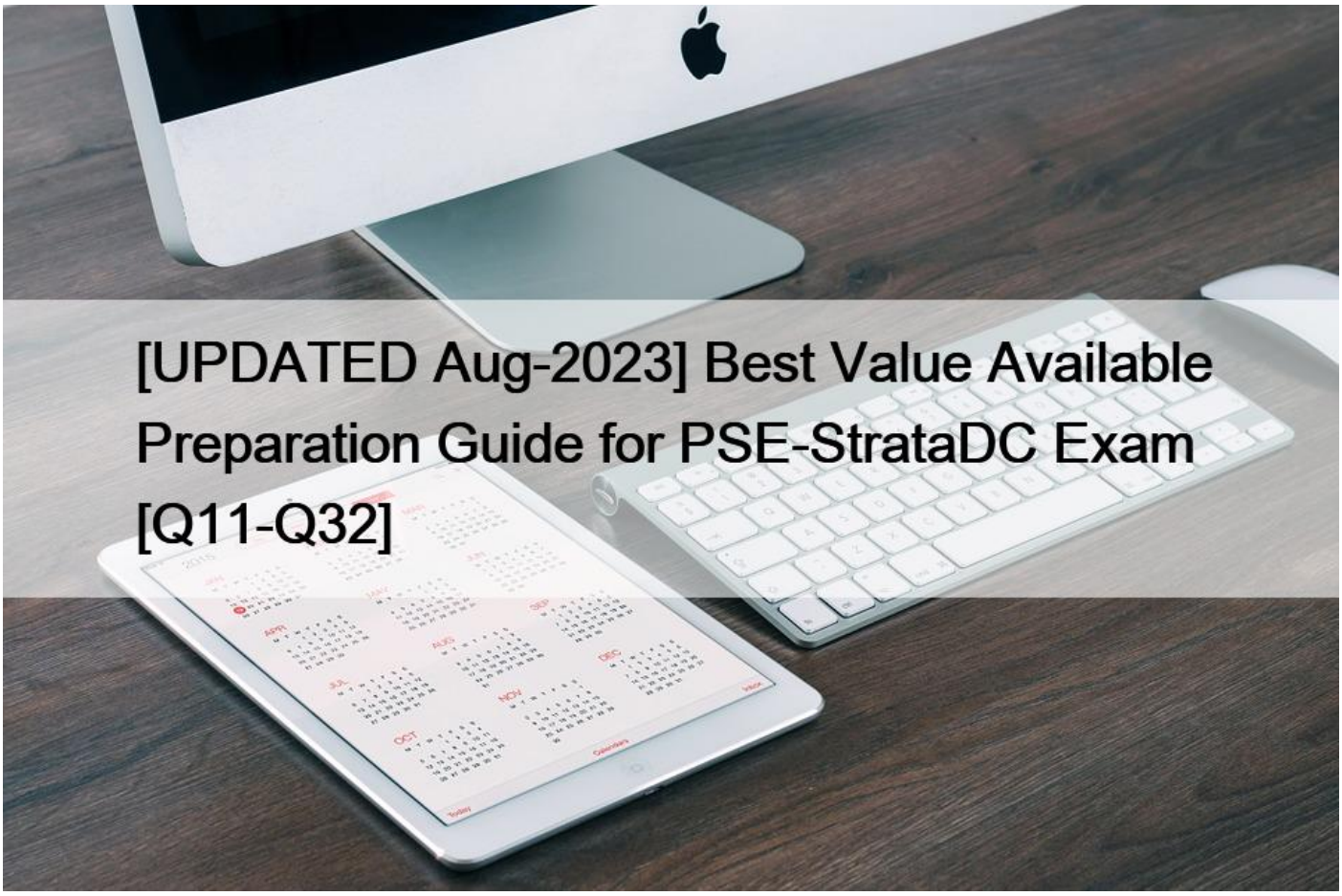
[UPDATED Aug-2023 Best Value Available Preparation Guide for PSE-StrataDC Exam [Q11-Q32



[UPDATED Aug-2023] Best Value Available Preparation Guide for PSE-StrataDC Exam
1 Full PSE-StrataDC Practice Test and 60 Unique Questions, Get it Now!

The PSE-StrataDC exam tests the candidate's understanding of various topics such as data center architecture and design principles, cloud infrastructure and services, network virtualization, security technologies, automation, and management. Palo Alto Networks System Engineer Professional - Strata Data Center certification exam is suitable for individuals who have a strong background in networking, security, and virtualization technologies and want to advance their career in data center security. Achieving the PSE-StrataDC certification demonstrates the candidate's ability to design and implement secure data center solutions using Palo Alto Networks technologies.

Palo Alto Networks PSE-StrataDC (Palo Alto Networks System Engineer Professional - Strata Data Center) Exam is designed for IT professionals who are interested in validating their knowledge and skills related to the deployment and management of Palo Alto Networks technologies in a data center environment. Palo Alto Networks System Engineer Professional - Strata Data Center certification exam is specifically designed for system engineers and architects who work with Palo Alto Networks products and solutions.

NO.11 Is vulnerability analysis against images in the registry sufficient for security?
* Yes, containers do not have unique vulnerabilities.
* No, you should do vulnerability analysis only against the running containers, which are vulnerable.
* Yes, you are ensuring that the images the containers are based on are secure.
* No, you need to do analysis in the CI system, in the registry, and against instantiated containers

NO.12 Which task is required to create steering rules on NSX-V Manager?
* Select Steering Rules > 3rd Party Firewalls > Palo Alto Networks and then populate the object with the required details
* Configure the rule in Panorama and push it to NSX-V Manager.
* Select Fabric > Access Policies > Quick Start and follow the prompts
* Add a network introspective service and select Redirect to Service under Action.

NO.13 Which interface mode does an administrator use to generate the statdump file that can be converted into an SLR? Assume that the administrator wants to make the evaluation as unintrusive as possible
* Virtual Wire
* TAP
* Layer 2
* Layer 3

NO.14 Which feature removes the limitation of requiring the first interface to be management?
* Management interface swap
* Utilize a separate Load Balancer VM
* Utilize a separate NAT VM.
* Dataport interface switch

NO.15 How do Palo Alto Networks NGFWs integrate with an ACI architecture?
* SDN code hooks can help to detonate malicious file samples designed to detect virtual environments
* Traffic can be automatically redirected using static Address objects.
* VXLAN or NVGRE traffic is terminated and inspected for translation to VLANs.
* Controllers can program firewalls using a REST-based API.

NO.16 How are workloads protected in Prisma Cloud Enterprise and Prisma Cloud Compute”
* Prisma Cloud enterprise and Prisma Cloud Computes provides identical workload capabilities.
* Prisma Cloud Enterprise provides workload protection through integration with the NGFW.
* Prisma Cloud Compute offers agentless protection for all workload types.
* Prisma Cloud Enterprise does not offer workload protection because it is a SaaS based product and agentless

NO.17 Which VM-Series can be deployed on Amazon Web Services (AWS)?
* Can deploy any VM-Series except the VM-50
* Only VM-100, VM-200 and VM-300
* Any VM-Series model
* Any VM-Series model except the VM-700

NO.18 Which option describes Arista’s micro-segmentation?
* Arista and VMware are extending secure segmentation with an open API (RESTZJSON)-based exchange, which allows NSX to federate with CloudVision to extend the micro-segmentation policy for physical workloads.
* Arista and Kubernetes are extending secure segmentation with an open API (RESTVJSON)-based exchange, which allows Kubernetes to federate with CloudVision to extend the micro-segmentation policy for physical workloads.

* Arista’s micro-segmentation and macro-segmentation are identical concepts that can be used interchangeably
* Arista and VMware both perform identical functions for NGFW micro-segmentation

NO.19 What is the major decision factor that customers use when selecting a managed container platform such as AS/EKS/GKE?
* licensing costs
* enhanced capabilities not available in vanilla K8s
* no need to manage containers, just the application code.
* reduced operational costs and management overhead

NO.20 Which configuration is requiredto share NSX security groups as tags to be used by Dynamic Address Groups in a non-NSX firewall?
* notify device groups within VMware Services Manager
* a User-ID agent on a Windows domain server
* VMware Information Sources
* none, sharing happens by default

NO.21 A network administrator is working on a VMware NSX installation with VM-1000-HV firewalls The administrator has created a security group that is populated with VMs The administrator is trying to create a Dynamic Address Group in Panorama, but the security group is not showing.

Which task should the administrator perform first?
* Go into vCenter/NSX and push the objects to Panorama
* Delete and re-add the security group.
* Go into Panorama and synchronize the Address objects with NSX
* Check the NSX Security policy to ensure the security group has been used in a policy.

NO.22 Which three software components have integration for deploying a VM-Series firewall in OpenStack? (Choose three)
* Mirantis OpenStack distribution
* Nuage VSP SDN controller
* VMWare NSX for OpenStack
* Cisco ACI
* Contrail SDN controller

NO.23 A single VM runs a web server and a DNS server A separate VM needs to access the DNS server, but is not allowed to access the web server What network control functionality is necessary to enforce this security posture’?
* can use a Palo Alto Networks NGFW for this requirement, but not a port filter firewall.
* can use either a Palo Alto Networks NGFW or a port filler firewall for this requirement.
* can use a port filter firewall for this requirement but not the Palo Alto Networks NGFW.
* can use a specialized VM with advanced threat protection for this requirement

NO.24 What are two types of security that can be implemented across every phase of the Build, Ship, and Run lifecycle of a workload? (Choose two)
* Runtime Security
* Firewalling
* Vulnerability Management
* Compliance or Configuration Management

NO.25 How is traffic directed to a Palo Alto Networks firewall integrated with Cisco ACI?
* by creating an access policy
* through a policy-based redirect (PBR)

* contracts between EPGs that send traffic to the firewall using a shared policy
* through a virtual machine monitor (VMM) domain

NO.26 How does the Palo Alto Networks NGFW integrate with Arista Networks Macro-Segmentation Service?
* Arista supports all hardware models of the Palo Alto Networks NGFW natively.
* Arista allows standalone non-HA firewalls to be attached to a service leaf switch. You must configure an Elastic Load Balancer to obtain fault tolerance.
* Arista CloudVision obtains relevant rules from Panorama through API and programs the Arista switches to steer intercepted east-west traffic to the Palo Alto Networks NGFW.
* Arista owns the Security policy. It can extend the concept of fine-grained intra-hypervisor security for VMs by enabling dynamic insertion of services for virtualized devices such as firewalls

NO.27 Describe the Automated Deployment of the NSX VM-Series firewall for NSX Solution’?
* When a new ESXi host is added to a cluster, a new VM-Series firewall is automatically deployed, provisioned and available for immediate policy enforcement without any little manual intervention
* When a new ESXi host is added to a cluster, a new VM-Series firewall is automatically deployed, provisioned and available for immediate policy enforcement without any manual intervention
* When a new ESXi host is added to a cluster, a new VM-Series firewall is automatically deployed provisioned and after manually retrieving licenses available for immediate policy enforcement.
* When a new ESXi host is added to a cluster, a new VM-Series firewall is automatically deployed and after manually adding licenses available for policy enforcement

NO.28 Which are two use cases for HSCI ports on the SMC module on PA-7000 Series? (Choose two)
* HA1 backup link in active/active HA
* HA1 link in active/passive HA
* HA3 link in active/active HA
* HA2 link in active/passive HA

Explanation

https://docs.paloaltonetworks.com/hardware/pa-7000-hardware-reference/pa-7000-series-module-and-interface-c

NO.29 Which two options describe use cases of internal and external tags in Panorama? (Choose two.)
* device group membership
* template membership
* Dynamic Address Group membership
* rule grouping

NO.30 In PAN-OS, which three NSX features can be pushed from Panorama? (Choose three)
* user IP mappings
* steering rules
* multiple authorization codes
* security group assignments of VMs
* security groups

NO.31 How does Palo Alto Networks VM orchestration help service providers automatically provision security instances and policies on demand? (Choose two.)
* Aperture Orchestration Engine (AOE)
* Support for Dynamic Address Groups
* Fully instrumented API
* VM Orchestration Policy Editor

NO.32 Which three steps are valid for deploying a VM-Series firewall on NSX? (Choose three)
* create steering policies to redirect traffic to the VM-Series firewall
* create a vDC and a vApp that includes the VM-Series firewall
* register the VM-Series firewall as a service
* obtain the AMI from market place
* enable communication between Panorama and the NSX Manager

Explanation

https://docs.paloaltonetworks.com/vm-series/8-1/vm-series-deployment/set-up-the-vm-series-firewall-on-vmwar