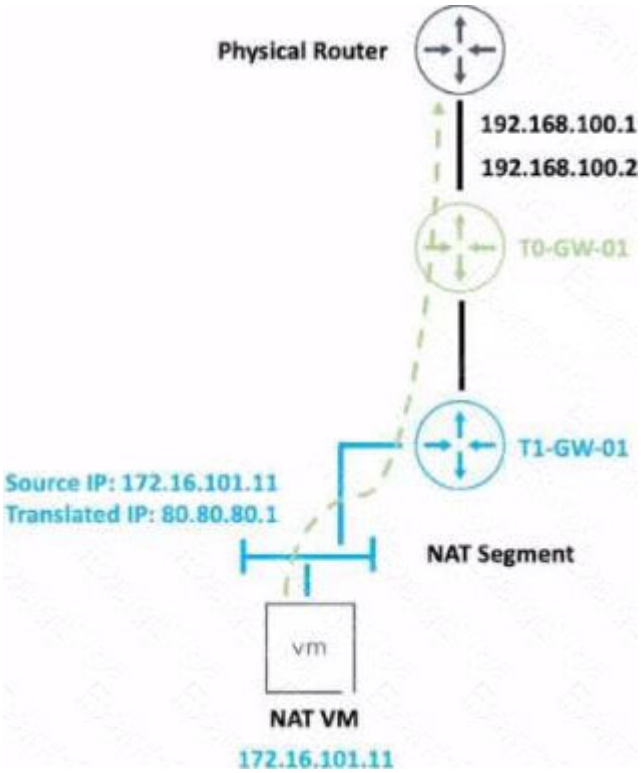
Exam : **2V0-41.23**

Title : VMware NSX 4.x Professional

Version : DEMO

1.Refer to the exhibit.



An administrator would like to change the private IP address of the NAT VM I72.l6.101.il to a public address of 80.80.80.1 as the packets leave the NAT-Segment network.
Which type of NAT solution should be implemented to achieve this?
A. DNAT
B. SNAT
C. Reflexive NAT
D. NAT64
Answer: B
Explanation:
SNAT stands for Source Network Address Translation. It is a type of NAT that translates the source IP address of outgoing packets from a private address to a public address. SNAT is used to allow hosts in a private network to access the internet or other public networks1
In the exhibit, the administrator wants to change the private IP address of the NAT VM 172.16.101.11 to a public address of 80.80.80.1 as the packets leave the NAT-Segment network. This is an example of SNAT, as the source IP address is modified before the packets are sent to an external network.
According to the VMware NSX 4.x Professional Exam Guide, SNAT is one of the topics covered in the exam objectives2
To learn more about SNAT and how to configure it in VMware NSX, you can refer to the following resources:
VMware NSX Documentation: NAT 3
VMware NSX 4.x Professional: NAT Configuration 4
VMware NSX 4.x Professional: NAT Troubleshooting 5
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-7AD2C384-4303-4D6C-A44A-DEF45AA18A92.html

2.Which two choices are solutions offered by the VMware NSX portfolio? (Choose two.)
A. VMware Tanzu Kubernetes Grid
B. VMware Tanzu Kubernetes Cluster
C. VMware NSX Advanced Load Balancer
D. VMware NSX Distributed IDS/IPS
E. VMware Aria Automation
Answer: C, D
Explanation:
VMware NSX is a portfolio of networking and security solutions that enables consistent policy, operations, and automation across multiple cloud environments1
The VMware NSX portfolio includes the following solutions:
- VMware NSX Data Center: A platform for data center network virtualization and security that delivers a complete L2-L7 networking stack and overlay services for any workload1
- VMware NSX Cloud: A service that extends consistent networking and security to public clouds such as AWS and Azure1
- VMware NSX Advanced Load Balancer: A solution that provides load balancing, web application firewall, analytics, and monitoring for applications across any cloud12
- VMware NSX Distributed IDS/IPS: A feature that provides distributed intrusion detection and prevention for workloads across any cloud12
- VMware NSX Intelligence: A service that provides planning, observability, and intelligence for network and micro-segmentation1
- VMware NSX Federation: A capability that enables multi-site networking and security management with consistent policy and operational state synchronization1
- VMware NSX Service Mesh: A service that connects, secures, and monitors microservices across multiple clusters and clouds1
- VMware NSX for Horizon: A solution that delivers secure desktops and applications across any device, location, or network1
- VMware NSX for vSphere: A solution that provides network agility and security for vSphere environments with a built-in console in vCenter1
- VMware NSX-T Data Center: A platform for cloud-native applications that supports containers, Kubernetes, bare metal hosts, and multi-hypervisor environments1
VMware Tanzu Kubernetes Grid and VMware Tanzu Kubernetes Cluster are not part of the VMware NSX portfolio. They are solutions for running Kubernetes clusters on any cloud3
VMware Aria Automation is not a real product name. It is a fictional name that does not exist in the VMware portfolio.
https://blogs.vmware.com/networkvirtualization/2020/01/nsx-hero.html/

3.When a stateful service is enabled for the first lime on a Tier-0 Gateway, what happens on the NSX Edge node'
A. SR is instantiated and automatically connected with DR.
B. DR Is instantiated and automatically connected with SR.
C. SR and DR Is instantiated but requites manual connection.
D. SR and DR doesn't need to be connected to provide any stateful services.

Answer: A
Explanation:
The answer is A. SR is instantiated and automatically connected with DR.
SR stands for Service Router and DR stands for Distributed Router. They are components of the NSX Edge node that provide different functions1
The SR is responsible for providing stateful services such as NAT, firewall, load balancing, VPN, and DHCP. The DR is responsible for providing distributed routing and switching between logical segments and the physical network1
When a stateful service is enabled for the first time on a Tier-0 Gateway, the NSX Edge node automatically creates an SR instance and connects it with the existing DR instance. This allows the stateful service to be applied to the traffic that passes through the SR before reaching the DR2
According to the VMware NSX 4.x Professional Exam Guide, understanding the SR and DR components and their functions is one of the exam objectives3
To learn more about the SR and DR components and how they work on the NSX Edge node, you can refer to the following resources:
- VMware NSX Documentation: NSX Edge Components 1
- VMware NSX 4.x Professional: NSX Edge Architecture
- VMware NSX 4.x Professional: NSX Edge Routing

4.A company Is deploying NSX micro-segmentation in their vSphere environment to secure a simple application composed of web. app, and database tiers.
The naming convention will be:
• WKS-WEB-SRV-XXX
• WKY-APP-SRR-XXX
• WKI-DB-SRR-XXX
What is the optimal way to group them to enforce security policies from NSX?
A. Use Edge as a firewall between tiers.
B. Do a service insertion to accomplish the task.
C. Group all by means of tags membership.
D. Create an Ethernet based security policy.
Answer: C
Explanation:
The answer is C. Group all by means of tags membership.
Tags are metadata that can be applied to physical servers, virtual machines, logical ports, and logical segments in NSX. Tags can be used for dynamic security group membership, which allows for granular and flexible enforcement of security policies based on various criteria1
In the scenario, the company is deploying NSX micro-segmentation to secure a simple application composed of web, app, and database tiers.
The naming convention will be:
- WKS-WEB-SRV-XXX
- WKY-APP-SRR-XXX
- WKI-DB-SRR-XXX
The optimal way to group them to enforce security policies from NSX is to use tags membership. For example, the company can create three tags: Web, App, and DB, and assign them to the corresponding

VMs based on their names. Then, the company can create three security groups: Web-SG, App-SG, and DB-SG, and use the tags as the membership criteria. Finally, the company can create and apply security policies to the security groups based on the desired rules and actions2
Using tags membership has several advantages over the other options:
- It is more scalable and dynamic than using Edge as a firewall between tiers. Edge firewall is a centralized solution that can create bottlenecks and performance issues when handling large amounts of traffic3
- It is more simple and efficient than doing a service insertion to accomplish the task. Service insertion is a feature that allows for integrating third-party services with NSX, such as antivirus or intrusion prevention systems. Service insertion is not necessary for basic micro-segmentation and can introduce additional complexity and overhead.
- It is more flexible and granular than creating an Ethernet based security policy. Ethernet based security policy is a type of policy that uses MAC addresses as the source or destination criteria. Ethernet based security policy is limited by the scope of layer 2 domains and does not support logical constructs such as segments or groups.
To learn more about tags membership and how to use it for micro-segmentation in NSX, you can refer to the following resources:
- VMware NSX Documentation: Security Tag 1
- VMware NSX Micro-segmentation Day 1: Chapter 4 - Security Policy Design 2
- VMware NSX 4.x Professional: Security Groups
- VMware NSX 4.x Professional: Security Policies

5.When collecting support bundles through NSX Manager, which files should be excluded for potentially containing sensitive information?
A. Controller Files
B. Management Files
C. Core Files
D. Audit Files
Answer: C
Explanation:
According to the VMware NSX Documentation1, core files and audit logs can contain sensitive information and should be excluded from the support bundle unless requested by VMware technical support. Controller files and management files are not mentioned as containing sensitive information.
Reference: 1: Support Bundle Collection Tool - VMware Docs
Core files and Audit logs might contain sensitive information such as passwords or encryption keys.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-73D9AF0D-4000-4EF2-AC66-6572AD1A0B30.html