2V0-41.23Q&As

VMware NSX 4.x Professional

Pass VMware 2V0-41.23 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/2v0-41-23.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: CD

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/

QUESTION 2

Which field in a Tier-1 Gateway Firewall would be used to allow access for a collection of trustworthy web sites?

A. Source

B. Profiles-> Context Profiles

C. Destination

D. Profiles-> L7 Access Profile

Correct Answer: D

The field in a Tier-1 Gateway Firewall that would be used to allow access for a collection of trustworthy web sites is Profiles-> L7 Access Profile. This field allows the user to create a Layer 7 access profile that defines a list of allowed or blocked URLs based on categories, reputation, or custom entries1. The user can then apply the L7 access profile to a

firewall rule to control the traffic based on the URL filtering criteria1. The other options are incorrect because they are not related to URL filtering. The Source field specifies the source IP address or group of the firewall rule1. The Destination field specifies the destination IP address or group of the firewall rule1. The Profiles-> Context Profiles field allows the user to create a context profile that defines a list of application signatures or attributes that can be used to identify and classify network traffic1. References: Gateway Firewall

QUESTION 3

An administrator wants to validate the BGP connection status between the Tier-O Gateway and the upstream physical router.

What sequence of commands could be used to check this status on NSX Edge node?

A. set vrf show logical-routers show bgp

B. show logical-routers get vrf show ip route bgp

C. get gateways vrf get bgp neighbor

D. enable get vrf show bgp neighbor

Correct Answer: C

The sequence of commands that could be used to check the BGP connection status between the Tier-O Gateway and the upstream physical router on NSX Edge node is get gateways, vrf , get bgp neighbor. These commands can be executed on the NSX Edge node CLI after logging in as admin6. The first command, get gateways, displays the list of logical routers (gateways) configured on the Edge node, along with their IDs and VRF numbers7. The second command, vrf , switches to the VRF context of the desired Tier-O Gateway, where is the VRF number obtained from the previous command7. The third command, get bgp neighbor, displays the BGP neighbor summary for the selected VRF, including the neighbor IP address, AS number, state, uptime, and prefixes received8. The other options are incorrect because they either use invalid or incomplete commands or do not switch to the correct VRF context. References: NSX-T Command-Line Interface Reference, NSX Edge Node CLI Commands, Troubleshooting BGP on NSX-T Edge Nodes

QUESTION 4

A customer has a network where BGP has been enabled and the BGP neighbor is configured on the Tier-0 Gateway. An NSX administrator used the get gateways command to retrieve this Information: Which two commands must be executed to check BGP neighbor status? (Choose two.)

```
sa-nsxedge-01> get gateways

Logical Router

UUID                                   VRF    GW-ID     Name              Type                        Ports
736a80e3-23f6-5a2d-81d6-bbefb2786666   0      0                           TUNNEL                      3
810ef54e-d5f3-49e5-99b7-8a51366d0592   1      1025      SR-T1-LR-01       SERVICE_ROUTER_TIER1        8
5a5ddd63-3764-4d28-b82e-ee4c964a0dfd   3      2049      SR-T0-LR-01       SERVICE_ROUTER_TIER0        6
0E0784db-511f-fa72-ae0b-1ccaa0262ad2   4      7         DR-T0-LR-01       DISTRIBUTED_ROUTER_TIER0    4
```

A. vrf 1

B. vrf 4

C. sa-nexedge-01(tier1_sr> get bgp neighbor

D. sa-nexedge-01(tier0_sr> get bgp neighbor

E. sa-nexedge-01(tier1_dr)> get bgp neighbor

F. vrf 3

Correct Answer: DF

BGP will be configured on the T0 SR. Connect to the VRF for the T0 SR and run get bgp neighbor once connected to it. https://docs.vmware.com/en/VMware-Validated-Design/5.1/sddc-deployment-of-vmware-nsx-t-workload-domains-withmultiple-availability-zones/GUID-8BD4228A-75C6-4C60-80B4-538D4297E11A.html For the BGP configuration on NSX-T, the Tier-0 Service Router (SR) is typically where BGP is configured. To check the BGP neighbor status:

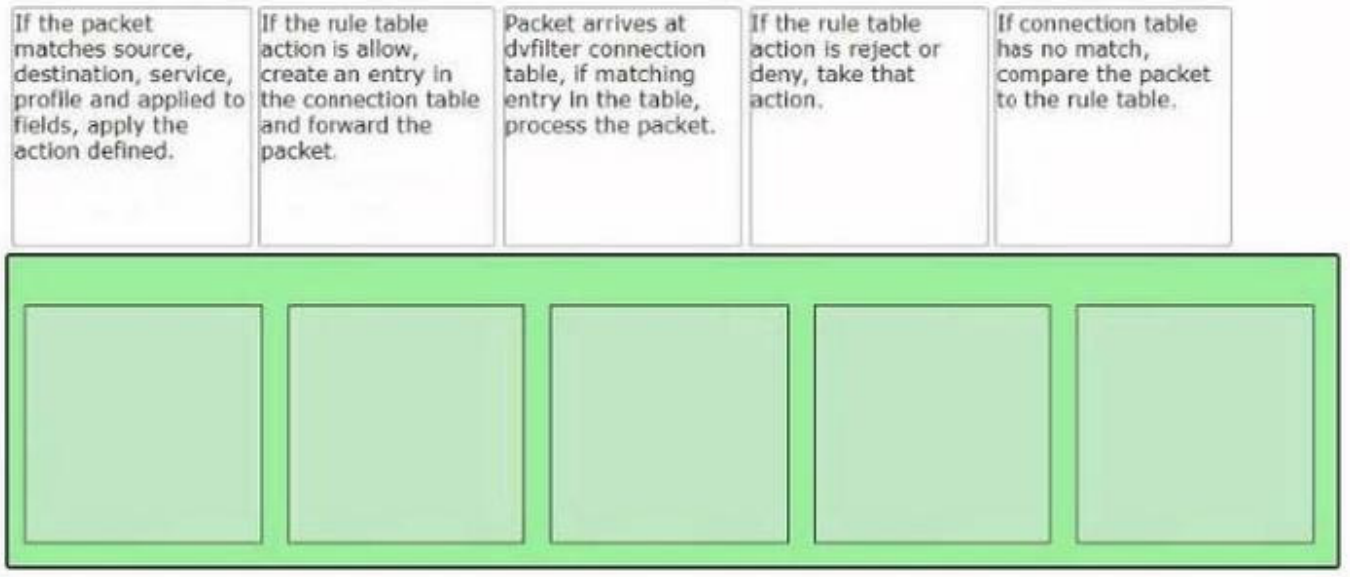
Connect to the VRF for the T0 SR, which is VRF 3 based on the provided output. Run the command to get BGP neighbor status once connected to it.

QUESTION 5

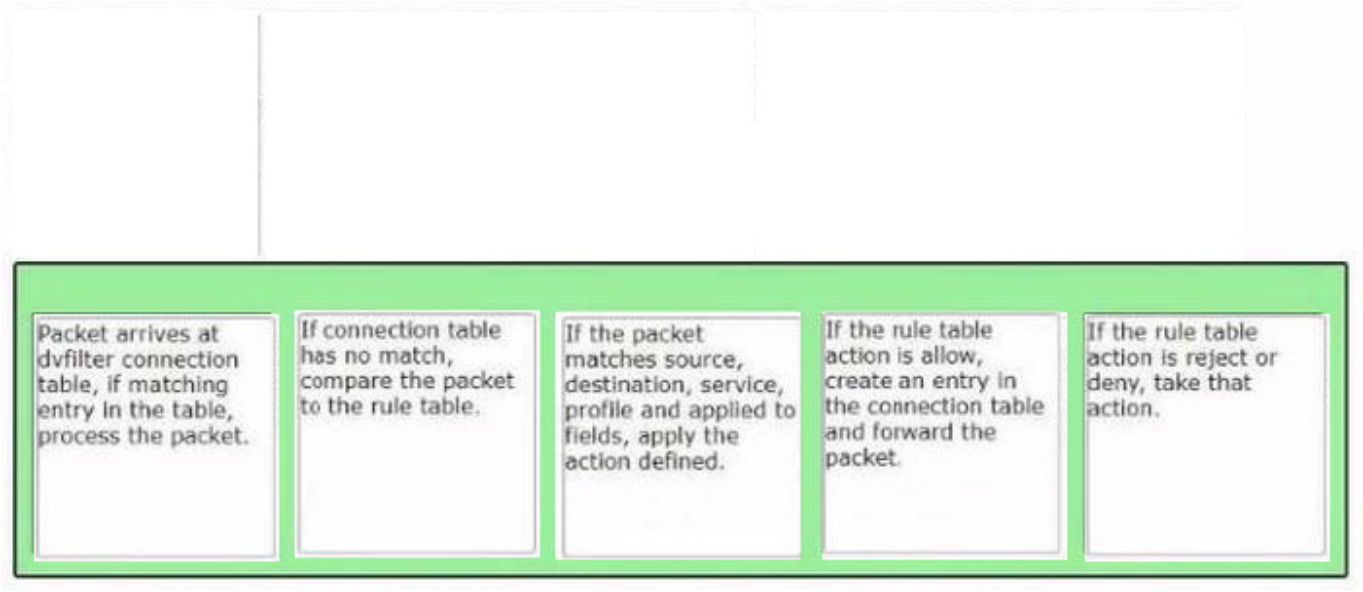
DRAG DROP

Sort the rule processing steps of the Distributed Firewall. Order responses from left to right.

Select and Place:



Correct Answer:



The correct order of the rule processing steps of the Distributed Firewall is as follows:

Packet arrives at vfilter connection table. If matching entry in the table, process the packet.

If connection table has no match, compare the packet to the rule table. If the packet matches source, destination, service, profile and applied to fields, apply the action defined.

If the rule table action is allow, create an entry in the connection table and forward the packet.

If the rule table action is reject or deny, take that action. This order is based on the description of how the Distributed Firewall works in the web search results1. The first step is to check if there is an existing connection entry for the packet in

the vfilter connection table, which is a cache of flow entries for rules with an allow action. If there is a match, the packet is processed according to the connection entry. If there is no match, the packet is compared to the rule table, which

contains all the security policy rules. The rules are evaluated from top to bottom until a match is found. The match criteria include source, destination, service, profile and applied to fields. The action defined by the matching rule is applied to

the packet. The action can be allow, reject or deny. If the action is allow, a new connection entry is created for the packet and the packet is forwarded to its destination. If the action is reject or deny, the packet is dropped and an ICMP

message or a TCP reset message is sent back to the source.