Free Questions for 2V0-41.23 by go4braindumps

Shared by Lamb on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following exist only on Tler-1 Gateway firewall configurations and not on Tier-0?

Options:

A- Applied To

B- Actions

C- Profiles

D- Sources

Answer:

A

Explanation:

According to the VMware NSX Documentation, Applied To is a feature that exists only on tier-1 gateway firewall configurations and not on tier-0. Applied To allows you to specify which logical router ports or segments are affected by a firewall rule. This can help reduce the scope and improve the performance of firewall rules.

Question 2

Question Type: MultipleChoice

An NSX administrator is creating a Tier-1 Gateway configured In Active-Standby High Availability Mode. In the event of node failure, the failover policy should not allow the original tailed node to become the Active node upon recovery.

Which failover policy meets this requirement?

Options:

A- Non-Preemptive

B- Preemptive

C- Enable Preemptive

D- Disable Preemptive

Answer:

A

Explanation:

According to the VMware NSX Documentation, a non-preemptive failover policy means that the original failed node will not become the active node upon recovery, unless the current active node fails again. This policy can help avoid unnecessary failovers and ensure stability.

The other options are either incorrect or not available for this configuration. Preemptive is the opposite of non-preemptive, meaning that the original failed node will become the active node upon recovery, if it has a higher priority than the current active node. Enable Preemptive and Disable Preemptive are not valid options for the failover policy, as the failover policy is a drop-down menu that only has two choices: Preemptive and Non-Preemptive.

Question 3

Question Type: MultipleChoice

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:

```
sa-nsxedge-01> get gateways
Logical Router
UUID                                   VRF    GW-ID    Name              Type                        Ports
736a80e3-23f6-5a2d-81d6-bbefb2786666   0      0                          TUNNEL                      3
B10ef54e-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    6
```

Which two commands must be executed to check BGP neighbor status? (Choose two.)

Options:

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

Answer:

B, D

Explanation:

According to the image that you sent, the BGP neighbor is configured on the tier-0 gateway with the UUID 9f8e3a7c-5f9c-4d1a-bb6f-9c7f3d6f3d63 and the VRF ID 4. Therefore, to check the BGP neighbor status, you need to enter the VRF context of 4 and execute the get bgp neighbor command on the tier-0 service router (SR) node.

The other options are either incorrect or not applicable for this scenario. vrf 1, vrf 3, and sa-nexedge-01(tier1_dr)> get bgp neighbor are not related to the BGP neighbor configuration on the tier-0 gateway. sa-nexedge-01(tier1_sr> get bgp neighbor is also not relevant, as there is no BGP neighbor configured on the tier-1 gateway.

Question 4

Question Type: MultipleChoice

NSX improves the security of today's modern workloads by preventing lateral movement, which feature of NSX can be used to achieve this?

Options:

A- Network Segmentation

B- Virtual Security Zones

C- Edge Firewalling

D- Dynamic Routing

Answer:

A

Explanation:

According to the web search results, network segmentation is a feature of NSX that improves the security of today's modern workloads by preventing lateral movement. Lateral movement is a technique used by attackers to move from one compromised system to another within a network, exploiting vulnerabilities or credentials . Network segmentation prevents lateral movement by dividing a network into smaller segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot access other segments or resources . NSX enables network segmentation by using micro-segmentation, which applies granular firewall rules at the virtual machine level, regardless of the physical network topology .

Question 5

Question Type: MultipleChoice

Which troubleshooting step will resolve an error with code 1001 during the configuration of a time-based firewall rule?

Options:

A- Reinstalling the NSX VIBs on the ESXi host.

B- Restarting the NTPservice on the ESXi host.

C- Changing the lime zone on the ESXi host.

D- Reconfiguring the ESXI host with a local NTP server.

Answer:

B

Explanation:

According to the web search results, error code 1001 is related to a time synchronization issue between the ESXi host and the NSX Manager. This can cause problems when configuring a time-based firewall rule, which requires the ESXi host and the NSX Manager to have the same time zone and NTP server settings . To resolve this error, you need to restart the NTP service on the ESXi host to synchronize the time with the NSX Manager. You can use the following command to restart the NTP service on the ESXi host:

/etc/init.d/ntpd restart

The other options are not valid solutions for this error. Reinstalling the NSX VIBs on the ESXi host will not fix the time synchronization issue. Changing the time zone on the ESXi host may cause more discrepancies with the NSX Manager. Reconfiguring the ESXi host with a local NTP server may not be compatible with the NSX Manager's NTP server.

Question 6

Question Type: MultipleChoice

What needs to be configured on a Tler-0 Gateway lo make NSX Edge Services available to a VM on a VLAN-backed logical switch?

Options:

A- Downlink Interface

B- VLAN Uplink

C- Loopback Router Port

D- Service Interface

Answer:

D

Explanation:

A service interface is a logical interface on a tier-0 gateway that connects to a VLAN logical switch and provides NSX Edge services to the VMs on that switch.A service interface is required for services such as load balancing, VPN, NAT, and DHCP1. A downlink interface is used to connect a tier-0 gateway to a tier-1 gateway or an overlay logical switch. A VLAN uplink is used to connect a tier-0 gateway to the physical network.A loopback router port is used to assign an IP address to the tier-0 gateway for routing protocols or firewall rules2...

Question 7

Question Type: MultipleChoice

Which two of the following features are supported for the Standard NSX Application Platform Deployment? (Choose two.)

Options:

A- NSX Intrusion Detection and Prevention

B- NSX Intelligence

C- NSX Network Detection and Response

D- NSX Malware Prevention Metrics

E- NSX Intrinsic Security

Answer:

C, D

Explanation:

The NSX Application Platform Deployment features are divided into three form factors: Evaluation, Standard, and Advanced.Each form factor determines which NSX features can be activated or installed on the platform1.The Evaluation form factor supports only NSX Intelligence, which provides network visibility and analytics for NSX-T environments2.The Standard form factor supports both NSX Intelligence and NSX Network Detection and Response, which provides network threat detection and response capabilities for NSX-T environments3.The Advanced form factor supports all four features: NSX Intelligence, NSX Network Detection and Response, NSX Malware Prevention, and NSX Metrics1.

Question 8

Question Type: MultipleChoice

When configuring OSPF on a Tler-0 Gateway, which three of the following must match in order to establish a neighbor relationship with an upstream router? (Choose three.)

Options:

A- Naming convention

B- MTU of the Uplink

C- Subnet mask

D- Address of the neighbor

E- Protocol and Port

F- Area ID

Answer:

B, C, F

Explanation:

ccording to the VMware NSX Documentation, these are the three parameters that must match in order to establish an OSPF neighbor relationship with an upstream router on a tier-0 gateway:

MTU of the Uplink: The maximum transmission unit (MTU) of the uplink interface must match the MTU of the upstream router interface. Otherwise, OSPF packets may be fragmented or dropped, causing neighbor adjacency issues.

Subnet mask: The subnet mask of the uplink interface must match the subnet mask of the upstream router interface. Otherwise, OSPF packets may not reach the correct destination or be rejected by the upstream router.

Area ID: The area ID of the uplink interface must match the area ID of the upstream router interface. Otherwise, OSPF packets may be ignored or discarded by the upstream router.