Free Questions for 5V0-41.21 by ebraindumps

Shared by Olson on 16-01-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An NSX administrator has been tasked with deploying a NSX Edge Virtual machine through an ISO image.

Which virtual network interface card (vNIC) type must be selected while creating the NSX Edge VM allow participation in overlay and VLAN transport zones?

Options:

A- e1000

B- VMXNET2

C- VMXNET3

D- Flexible

Answer:

C

Explanation:

When deploying an NSX Edge Virtual Machine through an ISO image, the virtual network interface card (vNIC) type that must be selected is VMXNET3 in order to allow participation in overlay and VLAN transport zones. VMXNET3 is a high-performance and feature-rich paravirtualized NIC that provides a significant performance boost over other vNIC types, as well as support for both overlay and VLAN transport zones.

For more information on deploying an NSX Edge Virtual Machine through an ISO image, please refer to the NSX-T Data Center documentation:https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-deploy-config/GUID-A782558B-A72B-4848-B6DB-7A8A9E71FFD6.html

Question 2

Question Type: MultipleChoice

A customer has a requirement to achieve Zero-Trust Security and minimize operational overhead. Which VMware solution can be used by the customer to achieve the requirement?

Options:

A- NSX Manager

B- Tanzu Kubernetes Grid

C- Carbon Black Anti-Virus

D- NSX Intelligence

Answer:

D

Explanation:

NSX Intelligence is a security analytics solution from VMware that can be used to achieve Zero-Trust Security and minimize operational overhead. It provides an AI-driven security analytics platform that can detect and respond to threats in real-time, allowing organizations to quickly identify threats and respond to them before they can cause damage. Additionally, it also provides automated security operations and orchestration capabilities that can help reduce manual overhead and free up resources for more important tasks.

For more information on NSX Intelligence and how it can help achieve Zero-Trust Security and minimize operational overhead, please refer to the NSX-T Data Center documentation:https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-intelligence/GUID-C2B2AF2E-A76A-46B8-A67A-42D7A9E924A9.html

Question 3

Question Type: **MultipleChoice**

Which three are required to configure a firewall rule on a getaway to allow traffic from the internal to web servers? (Choose three.)

Options:

A- Create a URL analysis profile for web hosting category.

B- Create a firewall rule in System category.

C- Enable Firewall Service for gateway.

D- Create a firewall policy in Local Gateway category.

E- Add a firewall rule in Local Gateway category.

F- Disable the firewall rule in Default category.

Answer:

C, D, E

Explanation:

In order to configure a firewall rule on a gateway to allow traffic from the internal to web servers, the administrator needs to enable the Firewall Service for the gateway, create a firewall policy in the Local Gateway category, and add a firewall rule in the Local Gateway category. This firewall rule should specify the web servers as the destination and the internal network as the source.

For more information on how to configure firewall rules on a gateway, please refer to the NSX-T Data Center documentation:https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-firewall/GUID-3A79CA7A-9D5E-4F2B-8F75-4EA298E4A4D5.html

Question 4

Question Type: **MultipleChoice**

At which OSI Layer do Next Generation Firewalls capable of analyzing application traffic operate?

Options:

A- Layer 4

B- Layer 3

C- Layer 7

D- Layer 2

Answer:

C

Explanation:

Next Generation Firewalls are capable of analyzing application traffic at Layer 7 of the OSI model. Layer 7 is the Application Layer, which is where the application-level protocols, such as HTTP and FTP, are implemented. Next Generation Firewalls are able to inspect the application traffic and apply rules based on the content of the application-level packets.

For more information on the OSI model and Next Generation Firewalls, please refer to the following resources:

* OSI Model:https://en.wikipedia.org/wiki/OSI_model* Next Generation Firewalls:https://en.wikipedia.org/wiki/Next-generation_firewall

Question 5

Question Type: **MultipleChoice**

When configuring members of a Security Group, which membership criteria art permitted?

Options:

A- Virtual Machine, Physical Machine, Cloud Native Service Instance, and IP Set

B- Segment Port, Segment, Virtual Machine, and IP Set

C- Virtual Interface, Segment, Cloud Native Service Instance, and IP Set.

D- Virtual Interface, Segment, Physical Machine, and IP Set

Answer:

A

Explanation:

When configuring members of a Security Group, the permitted membership criteria are Virtual Machine, Physical Machine, Cloud Native Service Instance, and IP Set.

For more information on configuring members of a Security Group, please refer to the NSX-T Data Center documentation:https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-security/GUID-C0F9A9A7-9A1E-41D9-A237-FED7A6F20A0A.html

Question 6

Question Type: **MultipleChoice**

An NSX administrator has been tasked with deploying a NSX Edge Virtual machine through an ISO image.

Which virtual network interface card (vNIC) type must be selected while creating the NSX Edge VM allow participation in overlay and VLAN transport zones?

Options:

A- e1000

B- VMXNET2

C- VMXNET3

D- Flexible

Answer:

C

Explanation:

When deploying an NSX Edge Virtual Machine through an ISO image, the virtual network interface card (vNIC) type that must be selected is VMXNET3 in order to allow participation in overlay and VLAN transport zones. VMXNET3 is a high-performance and feature-rich paravirtualized NIC that provides a significant performance boost over other vNIC types, as well as support for both overlay and VLAN transport zones.

For more information on deploying an NSX Edge Virtual Machine through an ISO image, please refer to the NSX-T Data Center documentation:https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-deploy-config/GUID-A782558B-A72B-4848-B6DB-7A8A9E71FFD6.html

Question 7

Question Type: **MultipleChoice**

At which OSI Layer do Next Generation Firewalls capable of analyzing application traffic operate?

Options:

A- Layer 4

B- Layer 3

C- Layer 7

D- Layer 2

Answer:

C

Explanation:

Next Generation Firewalls are capable of analyzing application traffic at Layer 7 of the OSI model. Layer 7 is the Application Layer, which is where the application-level protocols, such as HTTP and FTP, are implemented. Next Generation Firewalls are able to inspect the application traffic and apply rules based on the content of the application-level packets.

For more information on the OSI model and Next Generation Firewalls, please refer to the following resources:

* OSI Model:https://en.wikipedia.org/wiki/OSI_model* Next Generation Firewalls:https://en.wikipedia.org/wiki/Next-generation_firewall

Question 8

Question Type: **MultipleChoice**

Which three are required to configure a firewall rule on a getaway to allow traffic from the internal to web servers? (Choose three.)

Options:

A- Create a URL analysis profile for web hosting category.

B- Create a firewall rule in System category.

C- Enable Firewall Service for gateway.

D- Create a firewall policy in Local Gateway category.

E- Add a firewall rule in Local Gateway category.

F- Disable the firewall rule in Default category.

Answer:

C, D, E

Explanation:

In order to configure a firewall rule on a gateway to allow traffic from the internal to web servers, the administrator needs to enable the Firewall Service for the gateway, create a firewall policy in the Local Gateway category, and add a firewall rule in the Local Gateway category. This firewall rule should specify the web servers as the destination and the internal network as the source.

For more information on how to configure firewall rules on a gateway, please refer to the NSX-T Data Center documentation:https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-firewall/GUID-3A79CA7A-9D5E-4F2B-8F75-4EA298E4A4D5.html

Question 9

Question Type: **MultipleChoice**

A customer has a requirement to achieve Zero-Trust Security and minimize operational overhead. Which VMware solution can be used by the customer to achieve the requirement?

Options:

A- NSX Manager

B- Tanzu Kubernetes Grid

C- Carbon Black Anti-Virus

D- NSX Intelligence

Answer:

D

Explanation:

NSX Intelligence is a security analytics solution from VMware that can be used to achieve Zero-Trust Security and minimize operational overhead. It provides an AI-driven security analytics platform that can detect and respond to threats in real-time, allowing organizations to quickly identify threats and respond to them before they can cause damage. Additionally, it also provides automated security operations and orchestration capabilities that can help reduce manual overhead and free up resources for more important tasks.

For more information on NSX Intelligence and how it can help achieve Zero-Trust Security and minimize operational overhead, please refer to the NSX-T Data Center documentation:https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-intelligence/GUID-C2B2AF2E-A76A-46B8-A67A-42D7A9E924A9.html

20%
DISCOUNT