Free Questions for 5V0-41.21 by actualtestdumps

Shared by Haley on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

An administrator is reviewing NSX Intelligence information as shown in the exhibit.

What does the red dashed line for the UDP:137 flow represent?

Options:

A- Discovered communication

B- Allowed communication

C- Blocked communication

D- Unprotected communication

Answer:

C

Explanation:

The red dashed line for the UDP:137 flow in the NSX Intelligence information represents blocked communication. This indicates that the NSX Distributed Firewall has blocked the communication between the source and destination IP addresses on port 137.

For more information on NSX Intelligence and how to use it, 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 2

Question Type: MultipleChoice

A security administrator is verifying why users are blocked from sports sites but are able to access gambling websites from the corporate network. What needs to be updated In nsx-T to block the gambling websites?

Options:

A- vSphere Firewall Policy

B- Endpoint Protection Rules

C- Network Introspection Policy

D- URL Analysis Attributes

Answer:

D

Explanation:

In order to block the gambling websites, the security administrator needs to update the URL Analysis Attributes in NSX-T. URL Analysis Attributes are used to control access to web content, and can be configured to deny access to certain web destinations based on domain names or categories.

For more information on URL Analysis Attributes and how to configure them, please refer to the NSX-T Data Center documentation[1]:https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/nsx-t-3.0-url-profile/GUID-F8BA3F3F-4A27-4B4F-8D2A-

A013F68E1619.html

https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-703-release-notes.html

1.VMware vCenter Server 7.0 Update 3 Release Notes

https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-703-release-notes.html

Question 3

Question Type: **MultipleChoice**

Which two criteria would an administrator use to filter firewall connection logs on NSX?

Options:

A- FIREWALL MONITORING

B- FIREWALL-PKTLOG

C- FIREWALL RULE TAG

D- FIREWALL CONNECTION

E- FIREWALL SYSTEM

Answer:

C, D

Explanation:

An administrator can use the FIREWALL RULE TAG and FIREWALL CONNECTION criteria to filter the logs on NSX. The FIREWALL RULE TAG criteria allows the administrator to filter the logs based on the tag assigned to each rule, while the FIREWALL CONNECTION criteria allows the administrator to filter the logs based on the connection status (e.g. accepted or denied).

For more information on how to filter firewall connection logs on NSX, 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-B6B835F2-B6F2-4468-8F8E-6F7B9B9D6E91.html

Question 4

Question Type: MultipleChoice

A security administrator is required to protect East-West virtual machine traffic with the NSX Distributed Firewall. What must be completed with the virtual machine's vNIC before applying the rules?

Options:

A- It is connected to the underlay.

B- It must be connected to a vSphere Standard Switch.

C- It is connected to an NSX managed segment.

D- It is connected to a transport zone.

Answer:

C

Explanation:

In order to apply the rules, the vNIC of the virtual machine must be connected to an NSX managed segment. The NSX managed segment is a logical representation of the virtual network, and all rules are applied at this level.

For more information on NSX Distributed Firewall and how to configure it, 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-B6B835F2-B6F2-4468-8F8E-6F7B9B9D6E91.html

Question 5

Question Type: MultipleChoice

What is one of the main use-cases of NSX-T Endpoint Protection?

Options:

A- Use Network Security Services of a third party vendor

B- Agentless Antivirus

C- East-West Firewalling

D- North-South Firewalling

Answer:

B

Explanation:

NSX-T Endpoint Protection provides agentless antivirus protection for virtual machines running on VMware ESXi hosts. It uses the VMware vShield Endpoint API to scan the virtual machines without requiring the installation of antivirus agents. The service is integrated with third-party antivirus solutions, such as McAfee and Symantec, to provide real-time protection against malware and other threats.

For more information on NSX-T Endpoint Protection, 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-endpoint-protection/GUID-25C22F02-4B30-47D4-8F0C-3BC9F9C3AFD3.html

Question 6

Question Type: MultipleChoice

What is the default action of the Default Layer 3 distributed firewall rule?

Options:

A- Drop

B- Allow

C- Forward

D- Reject

Answer:

A

Explanation:

The Default Layer 3 distributed firewall rule is a system-defined rule in NSX-T Data Center that applies to all distributed firewall sections. By default, this rule is set to drop all traffic, meaning that any traffic that does not match a specific rule will be dropped.

For more information on the Default Layer 3 distributed firewall rule and how to configure it, 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-B6B835F2-B6F2-4468-8F8E-6F7B9B9D6E91.html