DUMPSQUEEN

VMware NSX-T Data Center 3.1 Security

VMware 5V0-41.21

Version Demo

Total Demo Questions: 10

Total Premium Questions: 70

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

Which esxcli command lists the firewall configuration on ESXi hosts?

A. esxcli network firewall ruleset list

B. vsipioct1 getrules -filter

C. esxcli network firewall rules

D. vsipioct1 getrules -f

ANSWER: A

Explanation:

This command allows you to display the current firewall ruleset configuration on an ESXi host. It will show the ruleset names, whether they are enabled or disabled, and the services and ports that the ruleset applies to.

For example, you can use the command "esxcli network firewall ruleset list" to list all the firewall rulesets on the host.

You can also use the command "esxcli network firewall ruleset rule list -r " to display detailed information of the specific ruleset, where is the name of the ruleset you want to display.

It's important to note that you need to have access to the ESXi host's command-line interface (CLI) and have appropriate permissions to run this command.

https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcli.ref.doc/esxcli_network_firewall_ruleset.html

QUESTION NO: 2

Which two are requirements for URL Analysis? (Choose two.)

A. The ESXi hosts require access to the Internet to download category and reputation definitions.

B. A layer 7 gateway firewall rule must be configured on the tier-0 gateway uplink to capture DNS traffic.

C. A layer 7 gateway firewall rule must be configured on the tier-1 gateway uplink to capture DNS traffic,

D. The NSX Edge nodes require access to the Internet to download category and reputation definitions.

E. The NSX Manager requires access to the Internet to download category and reputation definitions.

ANSWER: C D

Explanation:

The NSX Edge nodes require access to the Internet to download category and reputation definitions, and a layer 7 gateway firewall rule must be configured on the tier-1 gateway uplink to capture DNS traffic. This will allow the URL Analysis service

to analyze incoming DNS traffic and block malicious requests. For more information, please see this VMware Documentation article[1], which explains how to configure URL Analysis on NSX.

[1] https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_url_analysis/GUID-46BC65F3-7A45-4A9F-B444-E4A1A7E0AC4A.html

QUESTION NO: 3

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?

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 NO: 4

An administrator has configured a new firewall rule but needs to change the Applied-To parameter. Which two are valid options that the administrator can configure? (Choose two.)

A. DFW

B. rule

C. services

D. profiles

E. groups

ANSWER: A D

Explanation:

For further reading, see the VMware NSX-T Data Center Administration Guide (https://pubs.vmware.com/NSX-T-Data-Center/index.html#com.vmware.nsxt.admin.doc/GUID-704E1B2F-1E43-4E7F-97F2-59BBF8F6C9F6.html) for more information on configuring firewall rules.

QUESTION NO: 5

Which are two use-cases for the NSX Distributed Firewall' (Choose two.)

A. Zero-Trust with segmentation

B. Security Analytics

C. Lateral Movement of Attacks prevention
Software defined networking

D. Network Visualization

ANSWER: A C

Explanation:

Zero-Trust with segmentation is a security strategy that uses micro-segmentation to protect a network from malicious actors. By breaking down the network into smaller segments, the NSX Distributed Firewall can create a zero-trust architecture which limits access to only users and devices that have been authorized. This reduces the risk of a malicious actor gaining access to sensitive data and systems.

Lateral Movement of Attacks prevention is another use-case for the NSX Distributed Firewall. Lateral movement of attacks are when an attacker is already inside the network and attempts to move laterally between systems. The NSX Distributed Firewall can help protect the network from these attacks by controlling the flow of traffic between systems and preventing unauthorized access.

References: https://www.vmware.com/products/nsx/distributed-firewall.html
https://searchsecurity.techtarget.com/definition/zero-trust-network

QUESTION NO: 6

How does N5X Distributed IDS/IPS keep up to date with signatures?

A. NSX Edge uses manually uploaded signatures by the security administrator.

B. NSX-T Data Center is using a cloud based database to download the IDS/IPS signatures.

C. NSX Manager has a local IDS/IPS signatures database that does not need to be updated.

D. NSX Distributed IDS/IPS signatures are retrieved from updates.vmware.com.

ANSWER: D

QUESTION NO: 7

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

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 NO: 8

Which three security objects are provided as an output in a recommendation session in NSX Intelligence? (Choose three.)

A. context profiles
context profiles are not an output from a recommendation session in NSX Intelligence. It is used to define the context of the network traffic that is being analyzed, such as the type of device, the network location, or the user.

B. distributed firewall rules

C. security service

D. gateway firewall rules
gateway firewall rules are not an output from a recommendation session in NSX Intelligence. Gateway firewall rules are used to control traffic between logical networks, such as between a VLAN and a VXLAN, or between a logical network and the physical network.
References:
Top of FormBottom of Form

E. security groups

ANSWER: B C D

Explanation:

NSX Intelligence uses machine learning algorithms to analyze network traffic and provide recommendations for security and compliance. These recommendations include the following security objects:

A. context profiles are not an output from a recommendation session in NSX Intelligence. It is used to define the context of the network traffic that is being analyzed, such as the type of device, the network location, or the user.

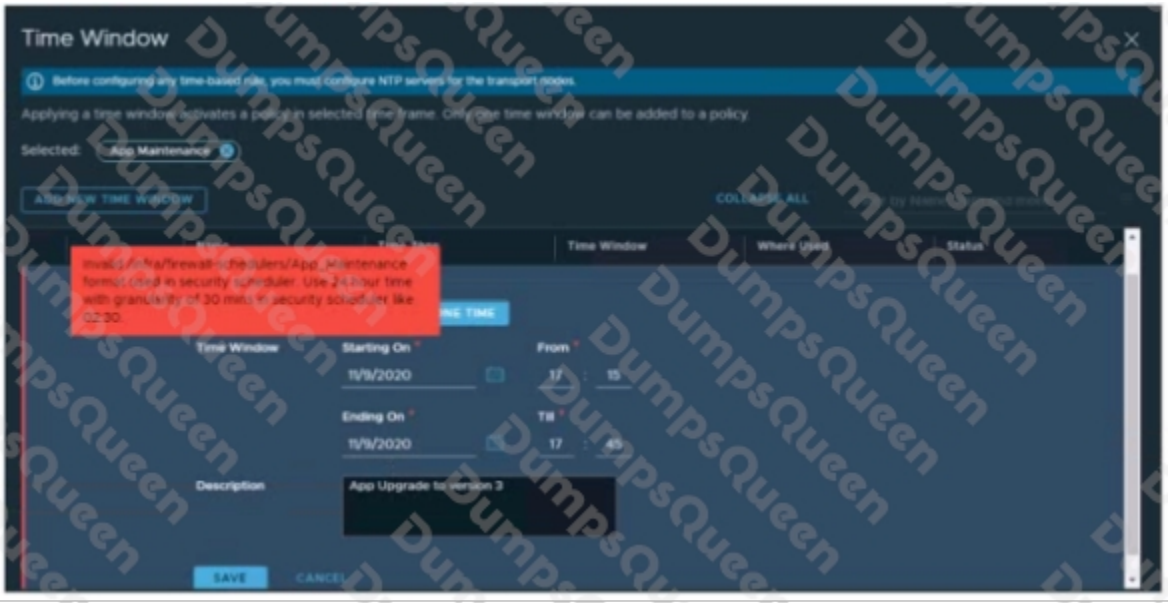
D. gateway firewall rules are not an output from a recommendation session in NSX Intelligence. Gateway firewall rules are used to control traffic between logical networks, such as between a VLAN and a VXLAN, or between a logical network and the physical network.

References:

Top of FormBottom of Form

QUESTION NO: 9

Refer to the exhibit.



A security administrator is configuring a time window to create a time-based distributed firewall rule. While configuring the time window, an error displayed as shown in the exhibit. Which action will resolve the problem?

A. Change the time window interval.

B. Restart me NTP service on the ESXI host.

C. Configure the ESXI host to use a remote NTP server.

D. Change the time windows frequency

ANSWER: C

Explanation:

The most likely action to resolve the problem is to configure the ESXi host to use a remote NTP server. The time window requires the ESXi host to be synchronized to a time source in order to properly calculate the time window, and the error is likely due to the ESXi host not being synchronized. Configuring the ESXi host to use a remote NTP server should ensure that the host is properly synchronized, and allow the time window to be configured correctly. References: [1]

https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-DD7F38A3-3D3B-47F1-92D7-9A4D4F3C44E1.html [2] https://www.vmware.com/support/vsphere/doc/vsphere-esxi-vcenter-server-601-configuration-maximums.html

QUESTION NO: 10

An NSX administrator has turned on logging for the distributed firewall rule. On an ESXi host, where will the logs be stored?

A. /var/log/esxupdate.log

B. /var/log/dfwpktlogs.log

C. /var/log/hostd.log

D. /var/log/vmkerntl.log

ANSWER: B

Explanation:

The NSX administrator has enabled logging for the distributed firewall rule, and the logs are stored in the /var/log/dfwpktlogs.log file on the ESXi host. This log file stores the packet logs for the distributed firewall rules, and the logs can be used for auditing and troubleshooting the distributed firewall.

References: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/2.5/nsxt_25_admin_guide/GUID-E0CC7D8A-F9E6-4A6F-A6F8-6A3D7B3DC3EF.html#GUID-E0CC7D8A-F9E6-4A6F-A6F8-6A3D7B3DC3EF