DUMPSARENA

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://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

What component in a transport node receives the firewall configuration from the central control plane?

A. nsx-ccp

B. nsx-appl-proxy

C. nsx-mpa

D. nsx-proxy

ANSWER: C

Explanation:

The component in a transport node that receives the firewall configuration from the central control plane is the NSX-MPA (Management Plane Agent). The NSX-MPA runs on each transport node and is responsible for connecting to the NSX-T central control plane and receiving the configuration for the transport node. It is also responsible for pushing the configuration down to the other components on the transport node, such as the NSX-Proxy, NSX-Appl-Proxy, and NSX-CCP. References: [1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-8C33F5B5-1B98-4A5F-B5B1-D70BE45F9FAD.html [2] https://docs.vmware.com/en/VMware-NSX-T/3.0/com.vmware.nsxt.install.doc/GUID-C129F7F0-E6F8-4A14-B2B0-9D6F3A7A3F62.

QUESTION NO: 2

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: 3

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: 4

Which of the following describes the main concept of Zero-Trust Networks for network connected devices?

A. Network connected devices should only be trusted if they are issued by the organization.

B. Network connected devices should only be trusted if the user can be successfully authenticated.

C. Network connected devices should only be trusted if their identity and integrity can be verified continually.
Network connected devices should only be trusted if their identity and integrity can be verified continually. This is the main concept of Zero-Trust Networks, every device that wants to access the network should be authenticated and verified its identity and integrity.
References:

D. Network connected devices should only be trusted if they are within the organizational boundary.

ANSWER: C

Explanation:

Zero-Trust Networks is a security concept that assumes that all devices, users, and networks are untrusted until they can be verified. This means that all network-connected devices must be verified for their identity and integrity before they are granted access to resources. This is done continually, meaning that devices are verified every time they try to access a resource, rather than being trusted permanently.

C. Network connected devices should only be trusted if their identity and integrity can be verified continually. This is the main concept of Zero-Trust Networks, every device that wants to access the network should be authenticated and verified its identity and integrity.

References:

QUESTION NO: 5

Information Security Management (ISM) describes a set of controls that organizations employ to protect which properties?

A. confidentiality, integrity, and availability

B. confidentiality, interoperability, and availability

C. configuration. Integrity, and availability

D. confidentiality. Integrity, and accessibility

ANSWER: A

Explanation:

Information Security Management (ISM) describes a set of controls that organizations employ to protect confidentiality, integrity, and availability. Confidentiality ensures that data is protected from unauthorized access or disclosure, integrity ensures that data is not modified without authorization, and availability ensures that data is accessible when it is needed. ISM is a crucial component of any organization's security strategy and is used to protect against threats such as data theft, data loss, and system outages. References: [1] https://searchsecurity.techtarget.com/definition/information-security-management [2] https://www.iso.org/standard/45170.html [3] https://www.bsigroup.com/en-GB/iso-27001-information-security/

QUESTION NO: 6

At which two intervals are NSX-T IDS/IPS updates through VMware's cloud based internet service provided for threat signature files? (Choose two.)

A. weekly periodic updates

B. off-schedule for 0-day updates

C. monthly periodic updates

D. daily periodic updates

E. bi-weekly periodic updates

ANSWER: B D

Explanation:

The NSX-T IDS/IPS updates are provided through VMware's cloud-based internet service at two different intervals: daily periodic updates, and off-schedule for 0-day updates. Daily periodic updates are provided on a daily basis to ensure the latest threat signature files. Off-schedule updates are provided as needed when a 0-day threat is identified, allowing customers to have the most up-to-date protection from the latest threats. References: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_ids_ips/GUID-D0F3F66C-FF83-4B3C-B0A3-C12F19D7A8AD.html https://blogs.vmware.com/networkvirtualization/2020/02/nsx-t-ids-and-ips-threat-protection.html

QUESTION NO: 7

An administrator wants to use Distributed Intrusion Detection. How is this implemented in an NSX-T Data Center?

A. As a distributed solution across multiple ESXi hosts.

B. As a distributed solution across multiple KVM hosts.

C. As a distributed solution across multiple NSX Managers.

D. As a distributed solution across multiple NSX Edge nodes.

ANSWER: D

Explanation:

An administrator can implement Distributed Intrusion Detection as a distributed solution across multiple NSX Edge nodes in an NSX-T Data Center. This allows for real-time monitoring of network traffic, as well as detection and prevention of malicious activity. Additionally, it can be used to identify, investigate, and respond to potential security threats. References: [1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-1F8741C0-D1CD-4EA3-A2BB-98CEF7F8D1DA.html [2] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-nsx-data-center-for-vsphere-distributed-intrusion-detection-deployment-guide.pdf

QUESTION NO: 8

A security administrator is verifying the health status of an NSX Service Instance.

Which two parameters must be functioning for the health status to show as Up? (Choose two.)

A. VMs must have at least one vNIC.

B. VMs must not have existing endpoint protection rules.

C. VMs must have virtual hardware version 9 or higher.

D. VMs must be available on the host.
VMs must be available on the host - The VMs that are associated with the service must be present on the host and able to communicate with the NSX Manager. If a VM is not available on the host, the service will not be able to function properly.

E. VMs must be powered on.
VMs must be powered on - The VMs that are associated with the service must be powered on and running. If a VM is not powered on, the service will not be able to function properly.

ANSWER: D E

Explanation:

The health status of an NSX Service Instance is an indicator of the overall health and functionality of the service.

For an NSX Service Instance to show as Up, the following two parameters must be functioning:

D. VMs must be available on the host - The VMs that are associated with the service must be present on the host and able to communicate with the NSX Manager. If a VM is not available on the host, the service will not be able to function properly.

E. VMs must be powered on - The VMs that are associated with the service must be powered on and running. If a VM is not powered on, the service will not be able to function properly.

QUESTION NO: 9

Which two are the insertion points for North-South service insertion? (Choose two.)

A. Partner Service VM

B. Uplink of tier-1 gateway

C. Transport Node NIC

D. Guest VM vNIC

E. Uplink of tier-0 gateway

ANSWER: D E

Explanation:

The tier-0 gateway is the entry point of the NSX-T Data Center network, and it is where the North-South service insertion takes place. The uplink of the tier-0 gateway is the point of connection between the NSX-T Data Center network and the external network.

The guest VM vNIC is the interface card inside the guest virtual machine, which is used to connect the guest VM to the NSX-T Data Center network. North-South services can be inserted at this point as well.

References: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_admin_guide/GUID-A3A6C7E1-8F5E-4A17-9B79-A3D836E3A6D3.html https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt

QUESTION NO: 10

As part of an audit, an administrator is required to demonstrate that measures have been taken to prevent critical vulnerabilities from being exploited. Which Distributed IDS/IPS event filter can the administrator show as proof?

A. Attack Type

B. CVSS

C. CVE

D. Signature ID

ANSWER: C

Explanation:

For further reading, see the VMware NSX-T Data Center Administration Guide (https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.admin.doc/GUID-A1A7F233-5F9F-4B2E-B3D3-0F8B593032F6.html) for more information on configuring the

as the CVE filter can be used to filter out any events which are related to a specific vulnerability