Vendor: VMware

Exam Code: 5V0-41.21

Exam Name: VMware NSX-T Data Center 3.1 Security

Version: DEMO

QUESTION 1
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.
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.
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.

QUESTION 2
Which vCenter component is used by the NSX Manager to deploy the Partner Service VM on every host of a cluster configured for guest introspection?

A. ESXi Agent Manager (EAM)
B. Auto Deploy
C. Update Manager (VUM)
D. Component Manager

Answer: D
Explanation:
Component Manager is used to deploy the Partner Service VM on every host of a cluster configured for guest introspection.

QUESTION 3
An organization wants to add security controls for contractor virtual desktops. Which statement Is true when configuring an NSX Identity firewall rule?

A. User Identity can be used in the both the Source and the Destination sections of the firewall rule.
B. User Identity can only be used in the Source section of the firewall rule.
C. User Identity cannot be used in Source or Destination sections of the firewall rule.
D. User Identity can only be used in the Destination Section of the firewall rule.

Answer: B
Explanation:
In NSX-T, Identity firewall rules allow you to specify security controls based on the identity of the user, rather than the IP address or other network-based attributes. User identity can be used as a source in the firewall rule.

QUESTION 4

Which is the port number used by transport nodes to export firewall statistics to NSX Manager?

A. 1235
B. 4789
C. 6081
D. 1234

Answer: B
Explanation:
The port number used by transport nodes to export firewall statistics to NSX Manager is 4789.

QUESTION 5
Where is a partner security virtual machine (Partner SVM) deployed to process the redirected North-South traffic in an efficient manner?

A. Deployed close to the Partner Manager.
B. Deployed close to the NSX Edge nodes.
C. Deployed close to the VMware vCenter Server.
D. Deployed close to the compute nodes.

Answer: B
Explanation:
This allows for the Partner SVM to be close to the compute nodes, allowing for faster processing of the traffic and improved security. Additionally, the Partner SVM is also deployed close to the Partner Manager for added security and ease of management.

QUESTION 6
Which two Guest OS drivers are required for the Identity Firewall to operate? (Choose two.)

A. NSX Network Introspection
B. vmxnet3
C. NSX File Introspection
D. Guest Introspection
E. e1000e

Answer: AD
Explanation:
The two Guest OS drivers that are required for the Identity Firewall to operate are NSX Network Introspection and Guest Introspection. NSX Network Introspection provides network-level visibility and control, while Guest Introspection provides kernel-level visibility and control. The other drivers listed, vmxnet3, NSX File Introspection, and e1000e, are not required for the Identity Firewall to operate.

QUESTION 7
Which two statements are true about NSX Intelligence? (Choose two.)

A. NSX Intelligence assists to build service insertion with Partner SVM.
B. NSX Intelligence supports planning of distributed firewall rules and policy.
C. NSX Intelligence can help to visualize network physical infrastructure.
D. NSX Intelligence can be used in conjunction with vRealize Network Insight.

E. NSX Intelligence supports planning of NSX-T Edge Firewall rules and policy.

Answer: AE
Explanation:
The two statements that are true about NSX Intelligence are that it assists to build service insertion with Partner SVM and that it supports planning of NSX-T Edge Firewall rules and policy. NSX Intelligence can be used in conjunction with vRealize Network Insight to provide visibility and insights into the network, but it cannot be used to visualize the physical infrastructure. Additionally, while it can help to plan firewall rules and policy, it does not support planning of distributed firewall rules and policy.

QUESTION 8
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.

QUESTION 9
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.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**