Number: 5V0-41.21
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 5V0-41.21
Exam Name: VMware NSX-T Data Center 3.1 Security

Exam A

QUESTION 1
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

Correct Answer: C, D
Section:
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 2
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?

A. vSphere Firewall Policy
B. Endpoint Protection Rules
C. Network Introspection Policy
D. URL Analysis Attributes

Correct Answer: D
Section:
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 NSXT 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-releasenotes.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-releasenotes.html

QUESTION 3
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?

A. Discovered communication
B. Allowed communication
C. Blocked communication
D. Unprotected communication

Correct Answer: C
Section:
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 4
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

Correct Answer: D, E
Section:
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.
Reference: 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 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
D. Software defined networking
E. Network Visualization

Correct Answer: A, C
Section:
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.
Reference: https://www.vmware.com/products/nsx/distributedfirewall.html https://searchsecurity.techtarget.com/definition/zero-trust-network

QUESTION 6
An administrator wants to configure NSX-T Security Groups inside a distributed firewall rule. Which menu item would the administrator select to configure the Security Groups?

A. System
B. Inventory
C. Security
D. Networking

Correct Answer: C
Section:
Explanation:
To configure NSX-T Security Groups inside a distributed firewall rule, the administrator would select the "Security" menu item in the NSX-T Manager user interface.
Within the Security menu, the administrator would navigate to the "Groups" option, where they can create, edit, and manage security groups. These groups can then be used in the "Applied To" column when creating or editing firewall rules.
In the Security menu, administrator can also configure other security features such as firewall, microsegmentation, intrusion detection and prevention, and endpoint protection.
Reference:
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html
VMware NSX-T Data Center Security Groups documentation
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.groups.doc/GUID-8C8DDC52-0B91-4E9F-8D8EE1649D3C3BBD.html

QUESTION 7
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

Correct Answer: B
Section:
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.
Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/2.5/nsxt_25_admin_guide/GUID-E0CC7D8A-F9E6-4A6F-A6F8-6A3D7B3DC3EF.html#GUIDE0CC7D8A- F9E6-4A6F-A6F8-6A3D7B3DC3EF

QUESTION 8
A Security Administrator needs to update their NSX Distributed IDS/IPS policy to detect new attacks with critical CVSS scoring that leads to credential theft from targeted systems.
Which actions should you take?

A. • Update Distributed IDS/IPS signature database
   • Edit your profile from Security > Distributed IDS > Profiles
   • Select Critical severity, filter on attack type and select Successful Credential Theft Detected
   • Check the profile is applied in Distributed IDS rules
B. • Edit your Distributed IDS rule from Security > Distributed IDS/IPS > Rules
   • Filter on attack type and select Successful Credential Theft Detected
   • Update Mode to detect and prevent
   • Click on gear icon and change direction to OUT
C. • Create a new profile from Security > Distributed IDS > Profiles
   • Select Critical severity, filter on attack type and select Successful Credential Theft Detected
   • Check the profile is applied In Distributed IDS rules
   • Monitor Distributed IDS alerts to validate changes are applied
D. • Edit your Distributed IDS rule from Security > Distributed IDS/IPS > Rules
   • Filter on attack type and select Successful Credential Theft Detected
   • Update Mode to detect and prevent
   • Click on gear icon and change direction to IN-OUT

Correct Answer: A
Section:
Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_ids_ips/GUID-B2D6A7F6-

QUESTION 9
Which is an insertion point for East-West service insertion?

A. tier-1 gateway
B. Partner SVM
C. Guest VM vNIC
D. transport node

Correct Answer: C
Section:
Explanation:
East-West service insertion refers to the ability to insert security services, such as firewall and intrusion detection and prevention, between virtual machines (VMs) that are communicating within the same logical network. One of the insertion points for East-West service insertion is the virtual network interface card (vNIC) of the guest VM. The vNIC is the virtual representation of a physical NIC on a VM, and it connects the VM to the virtual network. By inserting security services at the vNIC level, traffic between VMs can be inspected and secured before it reaches the virtual switch.
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html
VMware NSX-T Data Center Security documentation
https://docs.vmware.com/en/VMware-NSX-TData-Center/3.1/com.vmware.nsxt.security.doc/GUID-8F7C8B70-F1A6-4F31-8D6CA0A9B9C9A9D3.html

QUESTION 10
An NSX administrator has been tasked with configuring a remote logging server (192.168.110.60) to send FW connections and packets logs to a remote logging server. The administrator is using this command syntax found in the NSX-T 3.1 documentation:

Which of the following commands does the administrator use to complete the configuration task?

A. set logging-server 192.168.110.60 proto udp level info facility syslog message Id FIREWALLCONNECTION
B. set logging-server 192.168.110.60 proto udp level info facility syslog message!- monitor. Firewall
C. set logging-server 192.168.110.60 proto udp level info facility syslog message Id FIREWALLPKTLOG
D. set logging-server 192.168.110.60 proto udp level info facility syslog message Id system, fabric

Correct Answer: C
Section:
Explanation:
The administrator is using the command syntax found in the NSX-T 3.1 documentation to configure a remote logging server to send firewall connections and packets logs. In order to complete the configuration task, the administrator needs to use the correct options for the command.
The options used in the command are: logging-server: This option specifies the IP address or hostname of the remote logging server. In this case, the IP address of the remote logging server is 192.168.110.60. proto: This option specifies the protocol to be used to send the logs to the remote server. In this case, the protocol used is UDP. level: This option specifies the level of logging to be sent to the remote server. In this case, the level of logging is "info" facility: This option specifies the facility to be used for syslog messages. In this case, the facility used is "syslog" message Id: This option specifies the message Id that will be used for the logs. In this case, the message Id used is "FIREWALL-PKTLOG"
Reference:
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html
VMware NSX-T Data Center Logging documentation
https://docs.vmware.com/en/VMware-NSX-TData-Center/3.1/com.vmware.nsxt.logging.doc/GUID-2B9E9F8D-6CA9-4A1E-B7B1-8B8C7F0C2B2E.html

QUESTION 11
Which dot color indicates an on-going attack of medium severity in the IDS/IPS events tab of NSX-T Data Center?

A. blinking yellow dot
B. solid red dot
C. solid orange dot
D. blinking orange dot

Correct Answer: C
Section:
Explanation:
The dot color that indicates an on-going attack of medium severity in the IDS/IPS events tab of NSX-T Data Center is a solid orange dot. This indicates that the attack has been detected and is ongoing at a medium severity level.
Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_admin_guide/GUID-A8FAC8A1-F9F9-43EC-A822-F2F2CB5C5E5A.html#GUIDA8FAC8A1- F9F9-43EC-A822-F2F2CB5C5E5A
In the IDS/IPS events tab of NSX-T Data Center, different colors of dots are used to indicate the severity of an attack.
A solid red dot indicates a critical attack, which is the highest severity level.
A solid orange dot indicates a medium attack, which is a moderate severity level.
A solid yellow dot indicates a low attack, which is the lowest severity level.
In this case, a solid orange dot is used to indicate an on-going attack of medium severity in the IDS/IPS events tab of NSX-T Data Center.
It's worth noting that there is no blinking dots in this context, all the dots are solid.
Reference:
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html
VMware NSX-T Data Center Intrusion Detection and Prevention documentation
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.ids.doc/GUIDC4ED1F4D-4E4B-4A9C-9F5C-7AC081A5C5D5.html

QUESTION 12

An administrator needs to send FW connections logs to a remote server.
Which sequence of commands does the administrator need to apply on their ESXi Host?
A)

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
```

B)

```
esxcli network firewall ruleset set -r syslog -e true
esxcli network syslog config set --loghost=udp://<log server IP>:<port>
esxcli network syslog reload
```

C)

```
esxcli security firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
```

D)

```
esxcli system firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: C
Section:

QUESTION 13
There has been a confirmed case of virus infection on multiple VMs managed by Endpoint Protection. A security administrator wants to create a group to quarantine infected VMs in the future.
What criteria will be used to build this group?

A. NSX Tags
B. Segment
C. vSphere Tags
D. VM Name

Correct Answer: C
Section:
Explanation:
vSphere Tags are labels that can be used to group and categorize virtual machines and other objects.
The security administrator can create a tag for quarantined VMs and assign it to any VMs that are confirmed to be infected. This will help identify and isolate the infected VMs more quickly and easily in the future.
Reference: https://docs.vmware.com/en/VMwarevSphere/7.0/com.vmware.vsphere.security.doc/GUID-2AAB1D7A-E6A6-47F7-9B28-F9C9DED1C6B7.html

QUESTION 14
A security administrator has configured NSX Intelligence for discovery. They would like to get recommendations based on the changes in the scope of the input entities every hour.
What needs to be configured to achieve the requirement?

A. Start a new recommendation.
B. Publish the recommendations.
C. Toggle the monitoring option on.

D. Adjust the time range to 1 hour.

Correct Answer: D
Section:
Explanation:
NSX Intelligence uses machine learning algorithms to analyze network traffic and provide recommendations for security and compliance. The administrator can configure the time range of the input entities to be analyzed, so that the recommendations are based on changes in the scope of the input entities over that period of time.
To achieve the requirement of getting recommendations based on the changes in the scope of the input entities every hour, the administrator needs to adjust the time range to 1 hour. This will ensure that the analysis and recommendations are based on the most recent hour of network traffic.
Reference:
VMware NSX Intelligence documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.intelligence.doc/GUID-F2F1D7E8-F6B2-4870-9E38-7C8D3D3F9B1E.html
VMware NSX Intelligence Configuration documentation
https://docs.vmware.com/en/VMware-NSXT-Data-Center/3.1/com.vmware.nsxt.intelligence.config.doc/GUID-7F44F3D3-3A3C-4EBE-A5D5-F1E3E3F59A8B.html

QUESTION 15
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.

Correct Answer: C
Section:
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.
1. 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.
Reference:
Zero Trust Networks, Forrester Research https://www.forrester.com/report/Zero+Trust+Networks/-/E-RES146810
Zero Trust Security: From Theory to Practice, NIST
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800

QUESTION 16
Which three security objects are provided as an output in a recommendation session in NSX Intelligence? (Choose three.)

A. context profiles
B. distributed firewall rules
C. security service
D. gateway firewall rules
E. security groups

Correct Answer: B, C, D
Section:
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:
Distributed Firewall Rules: Distributed firewall rules are used to control traffic between virtual machines within a logical network. NSX Intelligence can recommend new distributed firewall rules based on traffic patterns it observes in the network.

Security Service: Security services are used to protect virtual machines and networks from threats.
NSX Intelligence can recommend new security services to be deployed based on traffic patterns it observes in the network.
Security Groups: Security groups are used to group virtual machines and networks together for security and management purposes. NSX Intelligence can recommend new security groups to be created based on traffic patterns it observes in the network.
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.
Reference:
VMware NSX Intelligence documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.intelligence.doc/GUID-F2F1D7E8-F6B2-4870-9E
Top of Form
Bottom of Form

QUESTION 17
What must an administrator deploy to provide Linux based VMs with antivirus protection?

A. Antivirus Agent in NSX
B. Antivirus Agent in vCenter
C. Guest Introspection Thin Agent
D. Guest Customization Agent

Correct Answer: C
Section:
Explanation:
NSX provides a feature called Guest Introspection that allows administrators to provide security services to virtual machines, including antivirus protection. One of the components of Guest Introspection is the Guest Introspection Thin Agent, which must be deployed to provide Linux-based VMs with antivirus protection. The Thin Agent is a lightweight agent that runs inside the guest operating system of virtual machines and communicates with the NSX Manager to provide security services.
Once the Guest Introspection Thin Agent is deployed, the administrator can configure the antivirus service to scan virtual machines for malware and take action on any threats that are detected.
Reference:
VMware NSX Guest Introspection documentation https://docs.vmware.com/en/VMware-NSX-TData-Center/3.1/com.vmware.nsxt.guest_introspection.doc/GUID-A86FBAF1-A8D9-4E12-8F3D-04B3D89B8F7E.html
VMware NSX Guest Introspection Thin Agent documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.guest_introspection.doc/GUID-A86FBAF1-A8D9-4E12-8F3D-04B3D89B8F7E.html

QUESTION 18
A company's CTO has requested that all logging should be enabled for all NSX-T Data Center Distributed Firewall rules. What should be considered prior to executing this request?

A. Large amounts of log information can fill up the vSphere Server database.
B. Logging can only be enabled for sections and not for single rules.
C. Once logging is enabled for all rules it cannot be disabled afterwards.
D. Large amounts of log information will likely affect performance.

Correct Answer: A
Section:

QUESTION 19
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

Correct Answer: A, D
Section:
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 20
Which of the following are the local user accounts used to administer NSX-T Data Center?

A. operator, admin, audit
B. admin, super, read-only
C. operator, admin, root
D. admin, audit, root

Correct Answer: A
Section:
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-4A4E9FBE-50B3-4F8F-B6C4-8527E7A08A67.html) for more information on user accounts andpermissions in NSX-T Data Center.

QUESTION 21
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

Correct Answer: C
Section:
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/GUIDA1A7F233-5F9F-4B2E-B3D3-0F8B593032F6.html) for more information on configuring theas the CVE filter can be used to filter out any events which are related to a specific vulnerability

QUESTION 22
Which two are used to define dynamic groups for an NSX Distributed Firewall? (Choose two.)

A. segment
B. physical servers
C. machine name

D. tags
E. segment's port

Correct Answer: C, D
Section:
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/GUIDBEDA8D9F-ACBC-42B1-B7F5-FEEF0E0D899C.html) for more information on configuring dynamicgroups.

QUESTION 23
What type of IDS/IPS system deployment allows an administrator to block a known attack?

A. A system deployed in SPAN port mode.
B. A system deployed inline with ALERT and DROP action.
C. A system deployed inline with ALERT action.
D. A system deployed in TERM mode.

Correct Answer: B
Section:
Explanation:
(https://pubs.vmware.com/NSX-T-Data-Center/index.html#com.vmware.nsxt.admin.doc/GUIDQuestionsand Answers PDF 16/38D9A6B1E7-FFCD-47A7-8E0C-FDD3DE6AC2B6.html) for more information on configuring an IDS/IPS system.

QUESTION 24
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.
E. VMs must be powered on.

Correct Answer: D, E
Section:
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 25
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

Correct Answer: D
Section:
Explanation:
Component Manager is used to deploy the Partner Service VM on every host of a cluster configured for guest introspection.
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/GUIDACB4CE1E-4F6E-4B4F-96BF-9FA9DFFF9229.html) for more information on configuring guestintrospection.

QUESTION 26
To which object can time based rules be applied?

A. Gateway Firewall only
B. DFW and Gateway Firewall both
C. DFW only
D. DFW or Gateway Firewall, but not both at the same time

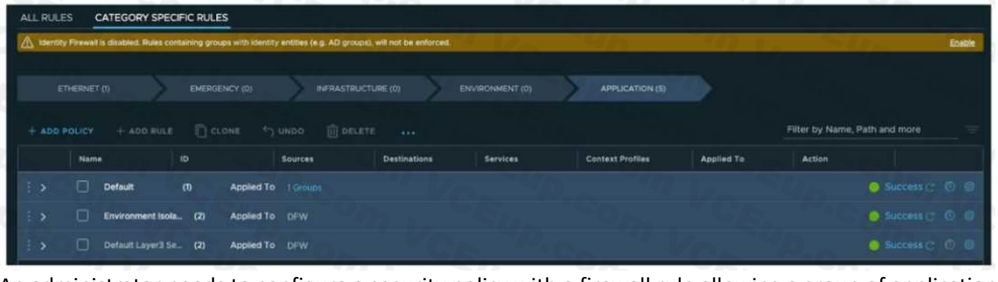
Correct Answer: C
Section:
Explanation:
For further reading, see the VMware NSX-T Data Center Administration Guide
(https://pubs.vmware.com/NSX-T-Data-Center/index.html#com.vmware.nsxt.admin.doc/GUID-8F9C6E9E-9C83-4CAD-BB3A-F4E4A25C6FE7.html) for more information on configuring time basedrules.

QUESTION 27
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.

Correct Answer: B
Section:
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 28
Refer to the exhibit.



An administrator needs to configure a security policy with a firewall rule allowing a group of applications to retrieve the correct time from an NTP server. Which is the category to configure thissecurity policy and firewall rule?

A. Emergency
B. Application
C. Infrastructure
D. Environment

Correct Answer: C
Section:
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/GUIDD12A8AE7-B9E9-4C79-8FE4-7F4BECD4F71B.html) for more information on configuring firewall rules.

QUESTION 29
Which two statements are true about IDS/IPS signatures? (Choose two.)

A. Users can upload their own IDS signature definitions from the NSX UI.
B. IDS Signatures can be High Risk, Suspicious, Low Risk and Trustworthy.
C. Users can create their own IDS signature definitions from the NSX UI.
D. An IDS signature contains data used to identify known exploits and vulnerabilities.
E. An IDS signature contains a set of instructions that determine which traffic is analyzed.

Correct Answer: D, E
Section:
Explanation:
(https://pubs.vmware.com/NSX-T-Data-Center/index.html#com.vmware.nsxt.admin.doc/GUIDAFAF58DB-E661-4A7D-A8C9-70A3F3A3A3D3.html)

QUESTION 30
What is the NSX feature that allows a user to block ICMP between 192.168.1.100 and 192.168.1.101?

A. NSX Distributed Switch Agent
B. NSX Distributed IDS/IPS
C. NSX Distributed Routing
D. NSX Distributed Firewall

Correct Answer: D
Section:
Explanation:
NSX Distributed Firewall is used to create firewall rules to control traffic between networks.
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-4B6A4A87-F9C7-4AAB-923F-C6B84C33AF7D.html) for more information on configuring firewall rules.

QUESTION 31
Which three criteria help to determine the severity for a Distributed IDS/IPS? (Choose three.)

A. The type-rating associated with the classification type.
B. The Common Vulnerability Scoring System score specified in the signature.
C. The load balancer deployment type.
D. The Distributed Intrusion Detection and Intrusion Prevention rules.

E. The severity specified in the signature itself

Correct Answer: A, B, E
Section:
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/GUIDE6B25C6F-1F25-4B0F-B8AF-6B8C00F9C3A3.html) for more information on configuring the Distributed IDS/IPS.

QUESTION 32
Which is the port number used by transport nodes to export firewall statistics to NSX Manager?

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

Correct Answer: B
Section:
Explanation:
The port number used by transport nodes to export firewall statistics to NSX Manager is 4789.
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-15A2EBC2-C39D-45F3-B847-DC18F7B1E9B9.html) for more information on transport nodes and firewall statistics.

QUESTION 33
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.

Correct Answer: B
Section:
Explanation:
Reference:
[1] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmwarensx-data-center-for-vsphere-partner-svm-security-deploymentguide.pdf [2] https://pubs.vmware.com/NSX-6/index.jsp?topic=%2Fcom.vmware.nsx.admin.doc%2FGUID-A2A6B7F6-9020-4D4F-AFC6-7E6D2E6194DF.html
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 34
To which network operations does a user with the Security Engineer role have full access permission?

A. Networking IP Address Pools, Networking NAT, Networking DHCP
B. Networking Forwarding Policies, Networking NAT, Networking VPN
C. Networking Load Balancing, Networking DNS, Networking Forwarding Policies
D. Networking DHCP, Networking NAT, Networking Segments

Correct Answer: A
Section:
Explanation:
A user with the Security Engineer role has full access permission to Networking IP Address Pools, Networking NAT, Networking DHCP, Networking Forwarding Policies, Networking VPN, Networking Load Balancing, Networking DNS, and Networking Segments. These operations allow the Security Engineer to configure and manage the necessary networking components to ensure a secure network environment. For example, Networking IP Address Pools allows the Security Engineer to create and manage IP address pools for assigning IP addresses to nodes on the network, Networking NAT allows the Security Engineer to configure Network Address Translation to improve security and privacy, and Networking Forwarding Policies allows the Security Engineer to configure policies for routing traffic between different networks. Reference: [1] https://docs.vmware.com/en/VMware- NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-ACA9C0F2-2F2E-43E3-A3C3- DEEECB7CFE8F.html [2] https://docs.vmware.com/en/VMware-NSX-T/2.5/vmware-nsx-t-25

QUESTION 35
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

Correct Answer: A, D
Section:
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 36
An administrator has enabled the "logging" option on a specific firewall rule. The administrator does not see messages on the Logging Server related to this firewall rule. What could be causing the issue?

A. The logging on the firewall policy needs to be enabled.
B. Firewall Rule Logging is only supported in Gateway Firewalls.
C. NSX Manager must have Firewall Logging enabled.
D. The logging server on the transport nodes is not configured.

Correct Answer: A
Section:

QUESTION 37
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.

Correct Answer: D
Section:

QUESTION 38
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.

Correct Answer: A, E
Section:
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 39
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.

Correct Answer: D
Section:
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. Reference:
[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-deploymentguide.pdf

QUESTION 40
Reference the CLI output.

```
[root@sa-esxi-03:~] vsipioctl getfwconfig -f nic-266154-eth0-vmware-sfw.2
ruleset mainrs {
rule 3054 at 1 (s) inout protocol tcp strict from addrset 6a966fb0-6388-42d7-9585-03acee45028e to addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf port
8443 accept;
rule 3055 at 2 (s) inout protocol tcp strict from addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf to addrset c104b8af-4de9-4779-8d00-aa329991305a port
80 accept;
rule 3056 at 3 inout protocol any from addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 to addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 reject;
}

addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf {
ip 172.16.20.11,
}
addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 {
ip 172.16.10.11,
ip 172.16.20.11,
ip 172.16.30.11,
}
addrset 6a966fb0-6388-42d7-9585-03acee45028e {
ip 172.16.10.11,
ip 172.16.10.12,
}

addrset c104b8af-4de9-4779-8d00-aa329991305a {
ip 172.16.30.11,
}
```

What is the source IP address in the distributed firewall rule to accept HTTP traffic?

A. 172.16.30.11
B. 172.16.10.12
C. 172.16.10.11

D. 172.16.20.11

Correct Answer: C
Section:

QUESTION 41
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

Correct Answer: C
Section:
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. Reference:
[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-NSXT/3.0/com.vmware.nsxt.install.doc/GUID-C129F7F0-E6F8-4A14-B2B0-9D6F3A7A3F62.

QUESTION 42
What needs to be configured on each transport node prior to using NSX-T Data Center Distributed Firewall time-based rule publishing?

A. DNS
B. NTP
C. PAT
D. NAT

Correct Answer: B
Section:
Explanation:
In order to use NSX-T Data Center Distributed Firewall time-based rule publishing, the NTP (Network Time Protocol) needs to be configured on each transport node. This ensures that the transport nodes have accurate time synchronization, which is required for time-based rule publishing. Additionally,
DNS (Domain Name System) and PAT (Port Address Translation) may also need to be configured oneach transport node, depending on the desired configuration. Reference:
[1] https://docs.vmware.com/en/VMware-NSX-T/2.5/com.vmware.nsxt.admin.doc/GUID-E9F8D8AD-7AF1-4F09-B62C-6A17A6F39A6C.html [2] https://docs.vmware.com/en/VMware-NSXT/2.4/com.vmware.nsxt.admin.doc/GUID-E9F8D8AD-7AF1-4F09-B62C-6A17A6F39A6C.html

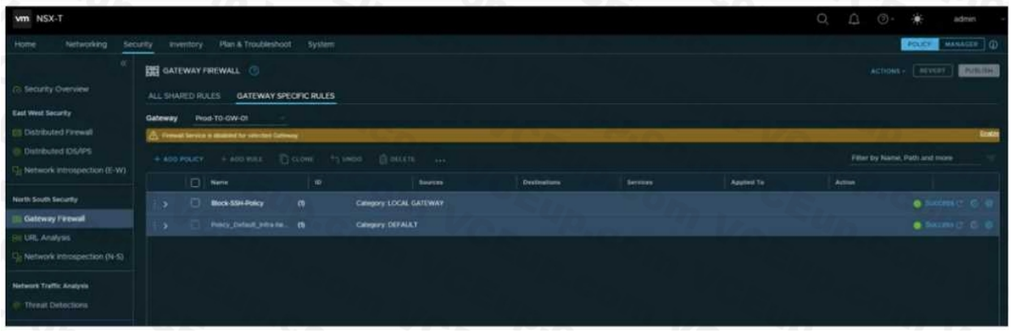
QUESTION 43
Which are the four use cases for NSX Tags?

A. Accountability, Third-party sharing/context sharing. Security, and Logging
B. Manageability, Third-party sharing/context sharing, Security, and Troubleshooting (Traceability)
C. Accountability, Third-party sharing/context sharing, Security, and Troubleshooting (Traceability)
D. Manageability, Third-party sharing/context sharing. Security, and Logging

Correct Answer: C

Section:
Explanation:
The four use cases for NSX Tags are Manageability, Third-party sharing/context sharing, Security, and Troubleshooting (Traceability). NSX Tags provide an easy way to organize, document, and manage virtual networks and can be used to track changes and enforce security policies. They can also be used to share context between third-party providers, such as cloud service providers, to ensure that security policies are adhered to. Additionally, NSX Tags can be used for logging and troubleshooting by providing traceability and making it easier to debug network issues. Reference:
[1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-2F3E7A3F-3C85-48E1-8F7E-2A2F7C2F8FCC.html [2] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-data-center-for-vsphere-tag-based-security-guide.pdf

QUESTION 44
Refer to the exhibit.



An administrator configured a firewall rule on their Edge Gateway to allow access to web servers.
What is missing in the Gateway Firewall policy to have the firewall rule applied?

A. Firewall service needs to be enabled on gateway.
B. Firewall rule needs to be moved to Default category.
C. Firewall rule needs to be enabled.
D. Firewall rule needs to be published

Correct Answer: B
Section:

QUESTION 45
What is one of the main use-cases of NSX-T Endpoint Protection?

A. Use Network Security Services of a third party vendor
B. Agentless Antivirus
C. East-West Firewalling
D. North-South Firewalling

Correct Answer: B
Section:
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-endpointprotection/ GUID-25C22F02-4B30-47D4-8F0C-3BC9F9C3AFD3.html

QUESTION 46

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?

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.

Correct Answer: C
Section:
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 47
When configuring members of a Security Group, which membership criteria art permitted?

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

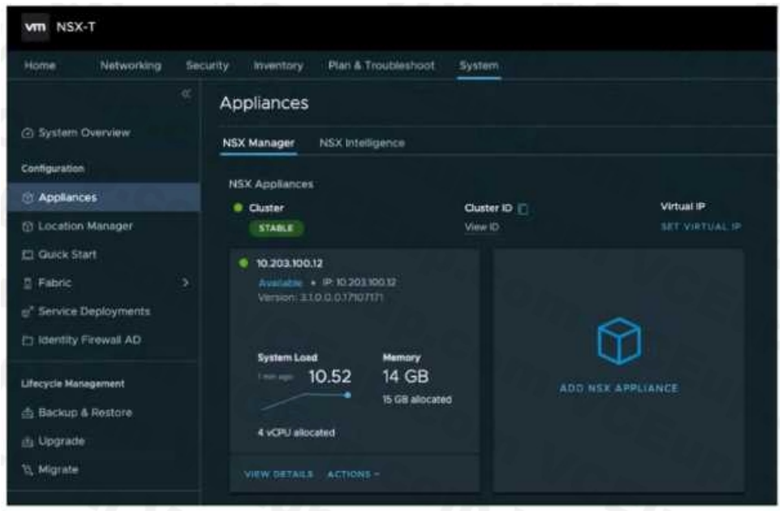
Correct Answer: A
Section:
Explanation:
When configuring members of a Security Group, the permitted membership criteria are Virtual Machine, Physical Machine, Cloud Native Service Instance, and IP Set.
For more information on configuring members of a Security Group, please refer to the NSX-T Data Center 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 48
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.

Correct Answer: C, D
Section:
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 49
Refer to the exhibit.



Referencing the exhibit, what is the VMware recommended number of NSX Manager Nodes to additionally deploy to form an NSX-T Manager Cluster?

A. 4
B. 3
C. 2
D. 5

Correct Answer: B
Section:

QUESTION 50
In a brownfield environment with NSX-T Data Center deployed and configured, a customer is interested in Endpoint Protection integrations. What recommendation should be provided to the customer when it comes to their existing virtual machines?

A. Virtual machine must be protected by vSphere HA.
B. Virtual machine hardware should be version 10 or higher.
C. A minimum installation of VMware tools is required.
D. A custom install of VMware tools is required to select the drivers.

Correct Answer: D
Section:
Explanation:
Endpoint Protection (EPP) integrations with NSX-T Data Center typically involve installing a security agent on the virtual machines (VMs) in the environment. This agent communicates with the NSX-T Data Center platform to provide security features such as antivirus and intrusion detection.
In order for the agent to work properly, it is important that the correct drivers are installed on the VMs. Typically, this is done by installing VMware tools on the VMs, which provides the necessary drivers. However, in a brownfield environment, the VMs may already have VMware tools installedand the drivers may not be the correct version for the agent to work properly. In this case, it isrecommended to perform a custom install of VMware tools and select the drivers specifically for theagent.
Reference:
VMware NSX-T Data Center Endpoint Protection documentation
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.epp.doc/GUIDC6F7F8C3-2F7B-4D5C-974F-F9C9E5BD5C5F.html
VMware Tools documentation
https://docs.vmware.com/en/VMwarevSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-D2F7D8C9-9D05-4F0F-A717-C4B4D4F4E4E4.html

QUESTION 51
Which two are true of the NSX Gateway Firewall? (Choose two.)

A. Firewall rules in System category cannot be edited.
B. Firewall rules in Pre Rule category are applied to all gateways.
C. NAT service can be configured in NSX Gateway Firewall policy.
D. Security Groups can be used in Applied-To column.
E. Applied-To can be configured at Firewall Policy level.

Correct Answer: B, D
Section:
Explanation:
NSX Gateway Firewall is a distributed firewall that provides security for east-west traffic within a virtual environment.
1. Firewall rules in Pre Rule category are applied to all gateways. This category contains systemdefined rules that are always applied first to all gateways and cannot be modified. These rules include the default deny all rule and others that control basic connectivity.
2. Security Groups can be used in Applied-To column. Security groups allow you to group together VMs that have similar security requirements and then apply firewall policies to those groups. This way you can apply the same security rules to multiple VMs at once, instead of configuring the rules on each individual VM.
Reference:
VMware NSX-T Data Center documentation https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html
VMware NSX-T Data Center Gateway Firewall documentation
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/com.vmware.nsxt.firewall.doc/GUID-4C5D5A5F-8FDF-4F2A-9C5A-2C1903A3E5A5.html

QUESTION 52
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

Correct Answer: B, D
Section:
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-todate protection from the latest threats.
Reference: https://docs.vmware.com/en/VMware-NSX-TData- 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-ipsthreat-protection.html

QUESTION 53
At which OSI Layer do Next Generation Firewalls capable of analyzing application traffic operate?

A. Layer 4
B. Layer 3
C. Layer 7
D. Layer 2

Correct Answer: C

Section:
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 rulesbased 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 GenerationFirewalls: https://en.wikipedia.org/wiki/Next-generation_firewall

QUESTION 54
Which three are required to configure a firewall rule on a getaway to allow traffic from the internal to web servers? (Choose three.)

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.

Correct Answer: C, D, E
Section:
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