Free Questions for NSE7_ZTA-7.2 by dumpshq

Shared by Henson on 22-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which three statements are true about zero-trust telemetry compliance1? (Choose three.)

Options:

A- FortiClient EMS creates dynamic policies using ZTNAtags

B- FortiChent checks the endpoint using the ZTNAtags provided by FortiClient EMS

C- ZTNA tags are configured in FortiClient, based on criteria such as certificates and the logged in domain

D- FortiOS provides network access to the endpoint based on the zero-trust tagging rules

E- FortiClient EMS sends the endpoint information received through FortiClient Telemetry to FortiOS

Answer:

A, B, D

Explanation:

In the context of zero-trust telemetry compliance, the three true statements are:

A) FortiClient EMS creates dynamic policies using ZTNA tags: FortiClient EMS utilizes ZTNA (Zero Trust Network Access) tags to create dynamic policies based on the telemetry it receives from endpoints.

B) FortiClient checks the endpoint using the ZTNA tags provided by FortiClient EMS: FortiClient on the endpoint uses the ZTNA tags from FortiClient EMS to determine compliance with the specified security policies.

D) FortiOS provides network access to the endpoint based on the zero-trust tagging rules: FortiOS, the operating system running on FortiGate devices, uses the zero-trust tagging rules to make decisions on network access for endpoints.

The other options are not accurate in this context:

C) ZTNA tags are configured in FortiClient, based on criteria such as certificates and the logged-in domain: ZTNA tags are typically configured and managed in FortiClient EMS, not directly in FortiClient.

E) FortiClient EMS sends the endpoint information received through FortiClient Telemetry to FortiOS: While FortiClient EMS does process telemetry data, the direct sending of endpoint information to FortiOS is not typically described in this manner.

Zero Trust Telemetry in Fortinet Solutions.

FortiClient EMS and FortiOS Integration for ZTNA.

Question 2

Question Type: **MultipleChoice**

Which three statements are true about a persistent agent? (Choose three.)

Options:

A- Agent is downloaded and run from captive portal

B- Supports advanced custom scans and software inventory.

C- Can apply supplicant configuration to a host

D- Deployed by a login/logout script and is not installed on the endpoint

E- Can be used for automatic registration and authentication

Answer:

B, C, E

Explanation:

A persistent agent is an application that works on Windows, macOS, or Linux hosts to identify them to FortiNAC Manager and scan them for compliance with an endpoint compliance policy. A persistent agent can support advanced custom scans and software inventory, apply supplicant configuration to a host, and be used for automatic registration and authentication.Reference:=

Persistent Agent

Persistent Agent on Windows

Using the Persistent Agent

Question 3

Question Type: MultipleChoice

In which FortiNAC configuration stage do you define endpoint compliance?

Options:

A- Device onboarding

B- Management configuration

C- Policy configuration

D- Network modeling

Answer:

C

Explanation:

Endpoint compliance is defined in the policy configuration stage of FortiNAC. Endpoint compliance policies specify which endpoint compliance configuration and user/host profile are applied to a host based on its location, user, and device type. Endpoint compliance configurations define whether a host is required to download an agent and undergo a scan, permitted access with no scan, or denied access. The scan parameters and security actions are also configured in the endpoint compliance configurations.Therefore, to define endpoint compliance, you need to create and assign endpoint compliance policies and configurations in the policy configuration stage of FortiNAC.Reference:= https://docs.fortinet.com/document/fortinac/9.4.0/administration-guide/985922/endpoint-compliance-policies

https://docs.fortinet.com/document/fortinac/9.4.0/fortinac-manager/161887/endpoint-compliance-configurations

Question 4

Question Type: **MultipleChoice**

exhibit.

```
[182:root:10]sslvpn_auth_check_usrgroup:2962 forming user/group list from policy.
[182:root:10]sslvpn_auth_check_usrgroup:3008 got user (0) group (0:1).
[182:root:10]sslvpn_validate_user_group_list:1850 validating with SSL VPN authentication
[182:root:10]sslvpn_validate_user_group_list:2864 got user (0:0), group (0:0) peer group
[182:root:10]fam_cert_send_req:1164 peer group 'SSL_VPN_Users' is sent for verification.
[182:root:10]fam_cert_send_req:1170 doing authentication for 1 group(s).
[2354] handle_req-Rcvd auth_cert req id=180791387, len=1111, opt=0
[974] __cert_auth_ctx_init-req_id=180791387, opt=0
[103] __cert_chg_st- 'Init'
[140] fnbamd_cert_load_certs_from_req-1 cert(s) in req.
[661] __cert_init-req_id=180791387
[710] __cert_build_chain-req_id=180791387
[257] fnbamd_chain_build-Chain discovery, opt 0x13, cur total 1
[273] fnbamd_chain_build-Following depth 0
[308] fnbamd_chain_build-Extend chain by system trust store. (good: 'CA_Cert_1')
[273] fnbamd_chain_build-Following depth 1
[87] fnbamd_chain_build-Self-sign detected.
[ ] __cert_chg_st- 'Init' -> 'Validation'
[1] __cert_verify-req_id=180791387
[32] __cert_verify-Chain is complete.
[457] fnbamd_cert_verify-Chain number:2
[471] fnbamd_cert_verify-Following cert chain depth 0
[533] fnbamd_cert_verify-Issuer found: CA_Cert_1 (SSL_DPI opt 1)
[471] fnbamd_cert_verify-Following cert chain depth 1
[675] fnbamd_cert_check_group_list-checking group with name 'SSL_VPN_Users'
[490] __check_add_peer-check 'student'
[366] peer_subject_cn_check-Cert subject 'CN = student'
[304] __RDN_match-Checking 'CN' val 'STUDENT' -- no match.
[397] peer_subject_cn_check-checking CN 'STUDENT' failed
[497] __check_add_peer-'student' check ret:bad
[191] __get_default_ocsp_ctx-def_ocsp_ctx=(nil), no_ocsp_query=0, ocsp_enabled=0
[867] __cert_verify_do_next-req_id=180791387
[99] __cert_chg_st- 'Validation' -> 'Done'
[912] __cert_done-req_id=180791387
[1663] fnbamd_auth_session_done-Session done, id=180791387
[957] __fnbamd_cert_auth_run-Exit, req_id=180791387
[1700] create_auth_cert_session-fnbamd_cert_auth_init returns 0, id=180791387
[1619] auth_cert_success-id=180791387
[1059] fnbamd_cert_auth_copy_cert_status-req_id=180791387
[833] fnbamd_cert_check_matched_groups-checking group with name 'SSL_VPN_Users'
```

User student is not able to log in to SSL VPN

Given the output showing a real-time debug: which statement describes the login failure?

Options:

A- Unable to verify chain of trust for the peer certificate

B- CN does not match the user peer configuration

C- student is not part of the usergroup SSL_VPN_Users.

D- Client certificate has expired

Answer:

C

Explanation:

Given the output showing a real-time debug, the statement that describes the login failure is:

C) student is not part of the usergroup SSL_VPN_Users: The debug log contains a line that says 'fnbam_cert_check_group_list-checking group with name 'SSL_VPN_Users'' followed by 'peer_check_add_peer_check_student' and later 'RDN_match-Checking 'CN' val 'STUDENT' -- no match.' This suggests that the certificate presented has a common name (CN) of 'student', which does not match or is not authorized under the 'SSL_VPN_Users' group expected for successful authentication.

Question 5

Question Type: MultipleChoice

With the increase in loT devices, which two challenges do enterprises face? (Choose two.)

Options:

A- Bandwidth consumption due to added overhead of loT

B- Maintaining a high performance network

C- Unpatched vulnerabilities in loT devices

D- Achieving full network visibility

Answer:

C, D

Explanation:

With the increase in IoT devices, enterprises face many challenges in securing and managing their network and data. Two of the most significant challenges are:

Unpatched vulnerabilities in IoT devices (Option C): IoT devices are often vulnerable to cyber attacks due to their increased exposure to the internet and their limited computing resources.Some of the security challenges in IoT include weak password protection, lack of regular patches and updates, insecure interfaces, insufficient data protection, and poor IoT device management12. Unpatched vulnerabilities in IoT devices can allow hackers to exploit them and compromise the network or data.For example, the Mirai malware infected IoT devices by using default credentials and created a massive botnet that launched DDoS attacks on internet services2.

Achieving full network visibility (Option D): IoT devices can generate a large amount of data that needs to be collected, processed, and analyzed. However, many enterprises lack the tools and capabilities to monitor and manage the IoT devices and data effectively. This can result in poor performance, inefficiency, and security risks. Achieving full network visibility means having a clear and comprehensive view of all the IoT devices, their status, their connectivity, their data flow, and their potential threats.This can help enterprises optimize their network performance, ensure data quality and integrity, and detect and prevent any anomalies or attacks3.

Question 6

Question Type: MultipleChoice

Exhibit.

Status	Host Name	Host Role	Operating System
w+	hr	Corporate	Windows Server 2019 ...

Which two statements are true about the hr endpoint? (Choose two.)

Options:

A- The endpoint application inventory could not be retrieved

B- The endpoint is marked as a rogue device

C- The endpoint has failed the compliance scan

D- The endpoint will be moved to the remediation VLAN

Answer:

B, C

Explanation:

Based on the exhibit, the true statements about the hr endpoint are:

B) The endpoint is marked as a rogue device: The 'w' symbol typically indicates a warning or an at-risk status, which can be associated with an endpoint being marked as rogue due to failing to meet the security compliance requirements or other reasons.

C) The endpoint has failed the compliance scan: The 'w' symbol can also signify that the endpoint has failed a compliance scan, which is a common reason for an endpoint to be marked as at risk.

Question 7

Question Type: MultipleChoice

Which statement is true about FortiClient EMS in a ZTNA deployment?

Options:

A- Uses endpoint information to grant or deny access to the network

B- Provides network and user identity authentication services

C- Generates and installs client certificates on managed endpoints

D- Acts as ZTNA access proxy for managed endpoints

Answer:

A

Explanation:

In a ZTNA (Zero Trust Network Access) deployment, FortiClient EMS:

A) Uses endpoint information to grant or deny access to the network: FortiClient EMS plays a critical role in ZTNA by using information about the endpoint, such as its security posture and compliance status, to determine whether to grant or deny network access.

The other options do not accurately represent the role of FortiClient EMS in ZTNA:

B) Provides network and user identity authentication services: While it contributes to the overall ZTNA strategy, FortiClient EMS itself does not directly provide authentication services.

C) Generates and installs client certificates on managed endpoints: Certificate management is typically handled by other components in the ZTNA framework.

D) Acts as ZTNA access proxy for managed endpoints: FortiClient EMS does not function as an access proxy; its role is more aligned with endpoint management and policy enforcement.

FortiClient EMS in Zero Trust Network Access Deployment.

Role of FortiClient EMS in ZTNA.

Question 8

Question Type: MultipleChoice

An administrator wants to prevent direct host-to-host communication at layer 2 and use only FortiGate to inspect all the VLAN traffic
What three things must the administrator configure on FortiGate to allow traffic between the hosts? (Choose three.)

Options:

A- Configure proxy ARP to allow traffic

B- Block intra-VLAN traffic in the VLAN interface settings

C- Add the VLAN interface to a software switch

D- Configure static routes to allow subnets

E- Configure a firewall policy to allow the desired traffic between hosts

Answer:

B, D, E

Explanation:

To prevent direct host-to-host communication at layer 2 and use only FortiGate to inspect all the VLAN traffic, an administrator must configure:

B) Block intra-VLAN traffic in the VLAN interface settings: This setting prevents direct communication between hosts within the same VLAN, forcing traffic to be routed through FortiGate for inspection.

D) Configure static routes to allow subnets: By setting up static routes, the administrator ensures that traffic between different subnets is correctly routed through the FortiGate for inspection and policy enforcement.

E) Configure a firewall policy to allow the desired traffic between hosts: Firewall policies on the FortiGate will dictate what traffic is permitted between hosts, ensuring that only authorized traffic is allowed.

The other options are not typically required for this setup:

A) Configure proxy ARP to allow traffic: Proxy ARP is not necessary for this scenario as it involves answering ARP requests on behalf of another host, which is not relevant to blocking intra-VLAN traffic.

C) Add the VLAN interface to a software switch: This would create a switch-like environment on the FortiGate, which is counterproductive to the goal of preventing direct host-to-host communication at layer 2.

FortiGate VLAN Configuration Guide.

Blocking Intra-VLAN Communication in FortiGate.

Question 9

Question Type: MultipleChoice

What are the three core principles of ZTA? (Choose three.)

Options:

A- Verity

B- Be compliant

C- Certify

D- Minimal access

E- Assume breach

Answer:

A, D, E

Explanation:

Zero Trust Architecture (ZTA) is a security model that follows the philosophy of "never trust, always verify" and does not assume any implicit trust for any entity within or outside the network perimeter. ZTA is based on a set of core principles that guide its implementation and operation. According to the NIST SP 800-207, the three core principles of ZTA are:

A) Verify and authenticate. This principle emphasizes the importance of strong identification and authentication for all types of principals, including users, devices, and machines. ZTA requires continuous verification of identities and authentication status throughout a session, ideally on each request. It does not rely solely on traditional network location or controls. This includes implementing modern strong multi-factor authentication (MFA) and evaluating additional environmental and contextual signals during authentication processes.

D) Least privilege access. This principle involves granting principals the minimum level of access required to perform their tasks. By adopting the principle of least privilege access, organizations can enforce granular access controls, so that principals have access only to the resources necessary to fulfill their roles and responsibilities. This includes implementing just-in-time access provisioning, role-based access controls (RBAC), and regular access reviews to minimize the surface area and the risk of unauthorized access.

E) Assume breach. This principle assumes that the network is always compromised and that attackers can exploit any vulnerability or weakness. Therefore, ZTA adopts a proactive and defensive posture that aims to prevent, detect, and respond to threats in real-time. This includes implementing micro-segmentation, end-to-end encryption, and continuous monitoring and analytics to restrict unnecessary pathways, protect sensitive data, and identify anomalies and potential security events.

1: Understanding Zero Trust principles - AWS Prescriptive Guidance

2: Zero Trust Architecture - NIST