Exam : 642-591

Title : Implementing Cisco NAC Appliance (CANAC)

Ver : 03-25-2009

QUESTION 1:

How does the Cisco NAM determine the presence of vulnerability without using the Cisco NAA on the client machine?

A. The end-user Cisco Trust Agent capability summary message does not match the defined role-based security policy requirement on the Cisco NAM.
B. The Cisco NAM receives a Cisco Security Agent vulnerability alert from the Cisco NAS
C. The Nessus network scan report matches a defined role-based or OS-based vulnerability on the Cisco NAM
D. The Cisco NAM will perform an agentless scan and interpret the results to determine if the client machines is vulnerable

Answer: C

QUESTION 2:

Exhibit:

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	MAC Notif.	Client MAC	Profile
Fa0/1	1	FastEthernet0/1			1	1			uncontrolled
Fa0/2	2	FastEthernet0/2			91	3	✔		Man91
Fa0/3	3	FastEthernet0/3			18	3	✔		controlled18
Fa0/4	4	FastEthernet0/4			1	1			Default [uncontrolled]
Fa0/5	5	FastEthernet0/5			1	1			Default [uncontrolled]

Your work as an network engineer at Certkiller .com. Please study the exhibit carefully. From a Drop-Down menu, profiles are applied to each managed port. Before a profile can be applied, where are the client access and authentication VLAN profile parameters to configured?

A. Controlled VLAN profile
B. Access Control profile
C. Switch Profile
D. VLAN Mapping Profile
E. Port Profile

Answer: E

QUESTION 3:

What is the local user account primarily used for?

A. For users who acquire temporary access or the normal login role
B. For users who acquire the quarantine access role
C. For Administrator access
D. For testing or for guest user accounts

Answer: D

QUESTION 4:

Which high-availability option is supported by a Cisco NAC Appliance Solution?

A. Cisco NAA Backup Server
B. Cisco NAS Backup Network Scanning
C. Cisco NAM and Cisco NAS redundancy
D. Cisco NAM and Cisco NAS load Balancing

Answer: C

QUESTION 5:

Which features must be configured to ensure that users can perform update and remediation?

A. Temporary Roles and Quarantines roles
B. Nessus Plug-ins and Antivirus Rules
C. Temporary and Quarantine network Remediation timer
D. Session timeouts and traffic controls policies

Answer: D

QUESTION 6:

What is the local user account primarily used for?

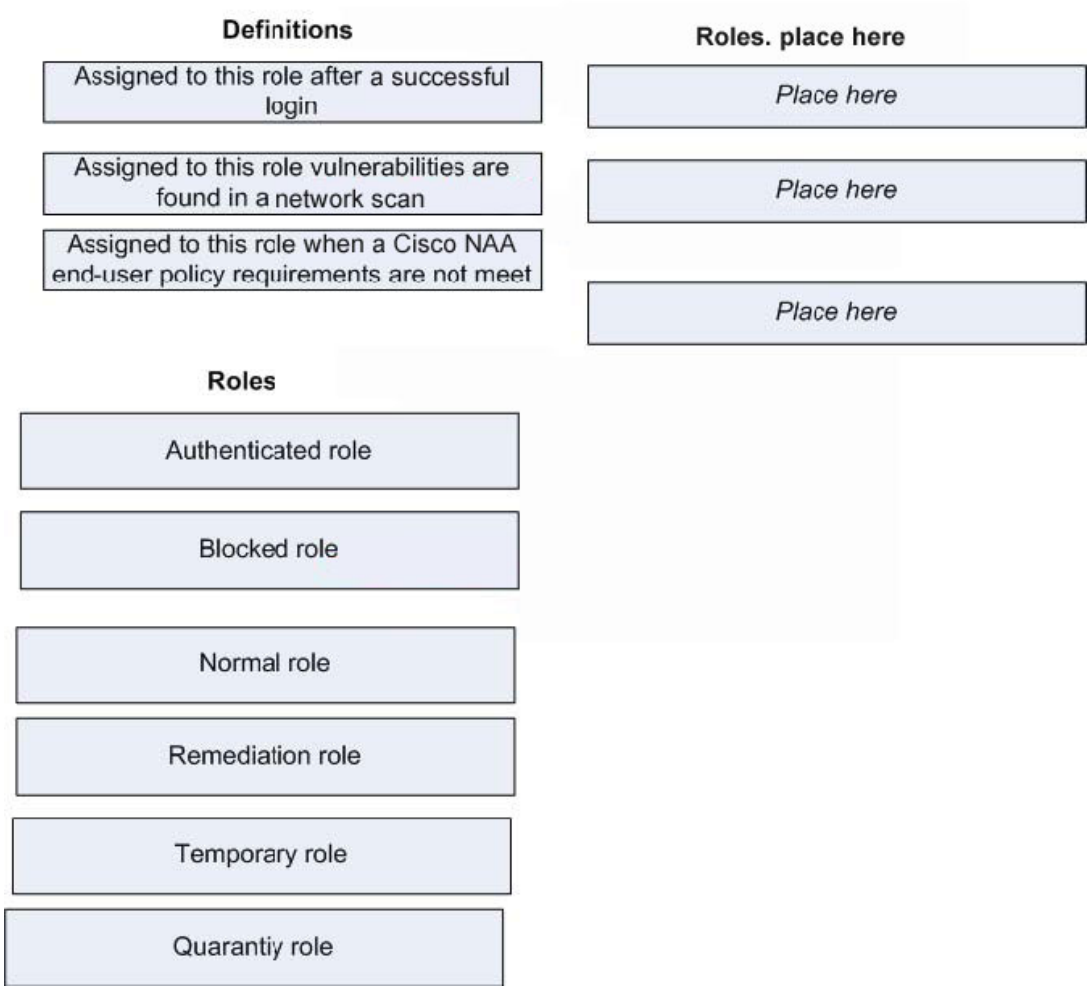
A. For testing or for guest user accounts
B. For users who acquire temporary access or the normal login role
C. For users who acquire the quarantine access role
D. For Administrator access

Answer: A

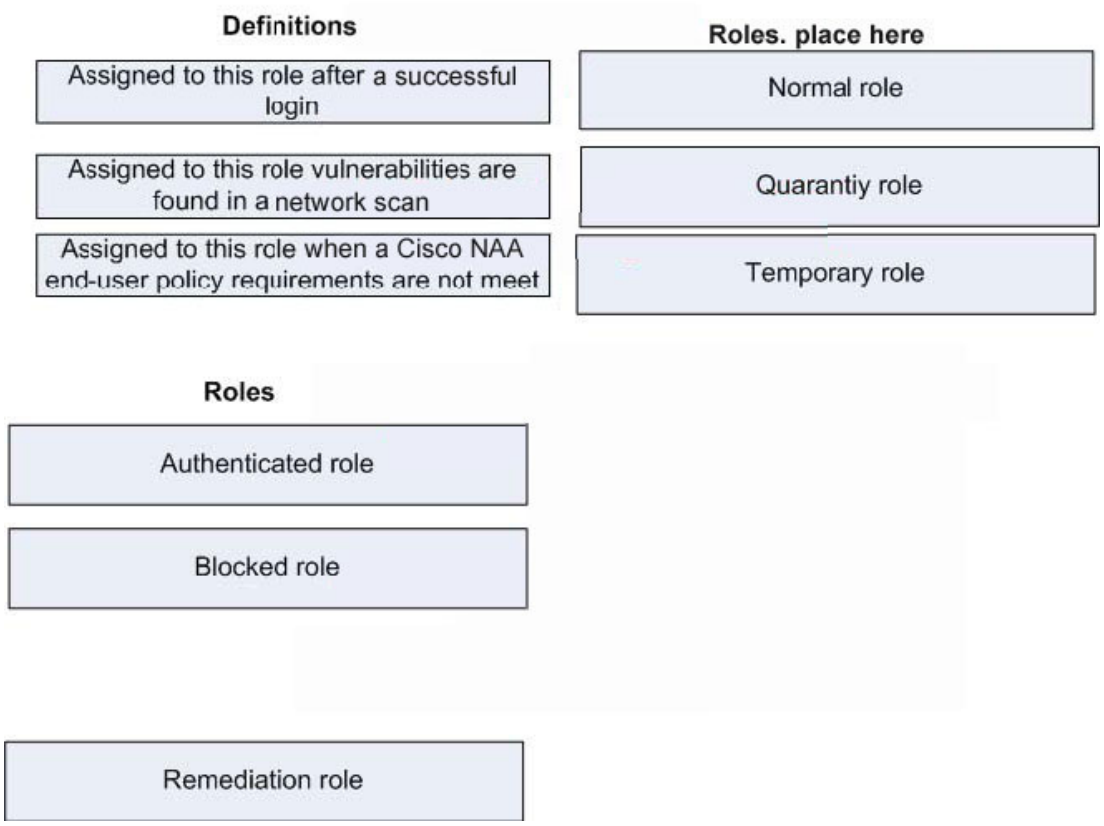
QUESTION 7:

DRAG DROP
You work as a network administrator at Certkiller .com. Your boss, Mrs. Certkiller, is interested in Cisco roles.

Match the descriptions with the appropriate roles.



Answer:



QUESTION 8:

What is an exempt device?

A. A device that does not require posture assessment each time it logs in to the network
B. A device that does not have to go through certification while its MAC address remains on the certified list
C. A multiuser device that is configured as a floating device so that recertification is not required at each login
D. A single or multiuser device that is only recertified when another user of the device logs out and accesses the network

Answer: B

QUESTION 9:

Which two functions can a Cisco NAC Appliance Agent be configured to perform? (Choose two.)

A. Check for up-to-date antivirus and antispam files
B. Detect the presence of worms and viruses before permitting network access to an end user

C. Perform registry, service and application checks
D. Initiate periodic Virus Scans

Answer: A,C

QUESTION 10:

In a Cisco NAM high-availability configuration, when does the secondary Cisco NAM take over?

A. When the timeout value is exceeded during data-mirroring activities
B. When the IP-based heartbeat signal fails to be transmitted and received within a certain time period
C. When the UDP heartbeat signal fails to be transmitted on the serial heartbeat connection between failover peers
D. When the UDP heartbeat signal is not transmitted and received within a certain time period

Answer: D

QUESTION 11:

Where is a local user validated?

A. At the authentication Server
B. At the Cisco NAA
C. At the Cisco NAS
D. At the Cisco NAM

Answer: D

QUESTION 12:

In Cisco NAC Appliance Solutions, which statements is correct regarding devices on the certified list?

A. Device manually added to the certified device list are automatically deleted when the device list-clearing timer expires
B. Devices that pass the Cisco NAA requirements are automatically added to the exempt device list
C. To remove an exempt device from the certified list, click the clear Certified Device Button
D. A device is not required to be rescanned at the next login as long as it MAC address is in the certified list

Answer: D

QUESTION 13:

How do you ensure that the Cisco NAS has the most recent version of the Cisco NAA to install on user devices?

A. From the Cisco NAS web Admin Console, enable Cisco NAA autoupdate on the Administration->Software Update Form
B. The Cisco NAA is upgraded directly to each Cisco NAS using the upgrade server form available on the Cisco NAM web console GUI
C. Configure the Cisco NAS by selecting which Cisco NAA to upgrade in the Cisco NAA Upgrade form
D. Each Time the Cisco NAA is upgraded, the Cisco NAM automatically download the new version of Cisco NAA to all Cisco NAS Servers

Answer: D

QUESTION 14:

When trying to restrict a guest-role end user to a host that has multiple or dynamic IP Addresses; the administrator would create which type of policy?

A. Address-based inclusion Policy
B. Server-based exemption Policy
C. Host-based traffic Control Policy
D. IP-based Access Policy

Answer: C

QUESTION 15:

Custom login pages can be targeted to specific groups of end users. Which three target methods are supported by Cisco NAC Appliance? (Choose three.)

A. Operating System
B. Subnet
C. Network Access Method
D. End-user Role
E. VLAN ID
F. Device Type

Answer: A,B,E

QUESTION 16:

When configuring an in-band central-deployment virtual gateway on the Cisco NAS,

what must be configured to ensure that the interface traffic on the same Layer 2 switch does not create a loop?

A. In the network form, select the passthrough VLAN ID option for the untrusted and trusted management VLAN
B. Configure the first switch downstream of the Cisco NAS with Spanning Tree
C. In the managed subnet form, enter the IP address that is assigned to the Cisco NAS to route the subnet, not the calculated network address
D. In the VLAN mapping form, map the untrusted interface VLAN ID to a trusted network VLAN ID

Answer: D

QUESTION 17:

In an out-of-band Cisco NAC Appliance high-availability deployment, why must port security be disabled between the switch interfaces to which the Cisco NAS and Cisco NAM are connected?

A. Port Security interfaces with SNMP message delivery between Cisco NAM failover peers
B. Port Security interfaces with UDP heartbeat signals
C. Port Security creates time-based latency, causing erratic SSL communication
D. Port Security can interface with Cisco NAS high availability and DHCP delivery

Answer: D

QUESTION 18:

Which interface is always used by Cisco NAM failover peers to support inter-peer connections?

A. The eth1 interface
B. The Serial Connection
C. The Second Ethernet Port
D. The eth0 Interface

Answer: A

QUESTION 19:

What does the secondary Cisco NAM do after it reboots from its initial configuration?

A. Switches to active mode, enabling load sharing with the primary Cisco NAM
B. Automatically sends a message to all Cisco NAS Servers, identifying itself as the secondary Cisco NAM

C. Automatically Synchronizes its database with the primary Cisco NAM
D. Takes over as the active Cisco NAM if the secondary Cisco NAM has a higher priority

Answer: C

QUESTION 20:

Which NAC Appliance Component performs network scanning?

A. Cisco NAC Appliance Agent
B. Cisco NAC Appliance Server
C. Cisco NAC Appliance Manager
D. Cisco NAC Trust Agent

Answer: B

QUESTION 21:

In the Cisco NAM, under Administration-> User Pages -> Login Page, custom login pages can be created based on which three things? (Choose three.)

A. Operating System
B. User Role
C. Cisco NAS
D. Cisco NAM
E. VLAN
F. Subnet

Answer: A,E,F

QUESTION 22:

What must be done to upgrade a Cisco NAC Appliance implementation to take advantage of a major release of NAC Appliance?

A. Upgrade the Cisco NAM Servers. When the Cisco NAM servers come online, Cisco NAS upgrades will occur automatically
B. First upgrade the Cisco NAS servers, bring the Cisco NAS online and then upgrade the Cisco NAM Servers
C. First Upgrade the Cisco NAM Servers, Bring the Cisco NAM Serer online and then upgrade the Cisco NAS Servers.
D. Upgrade the Cisco NAM servers and Cisco NAS servers concurrently

Answer: D

QUESTION 23:

Network Topology Exhibit:

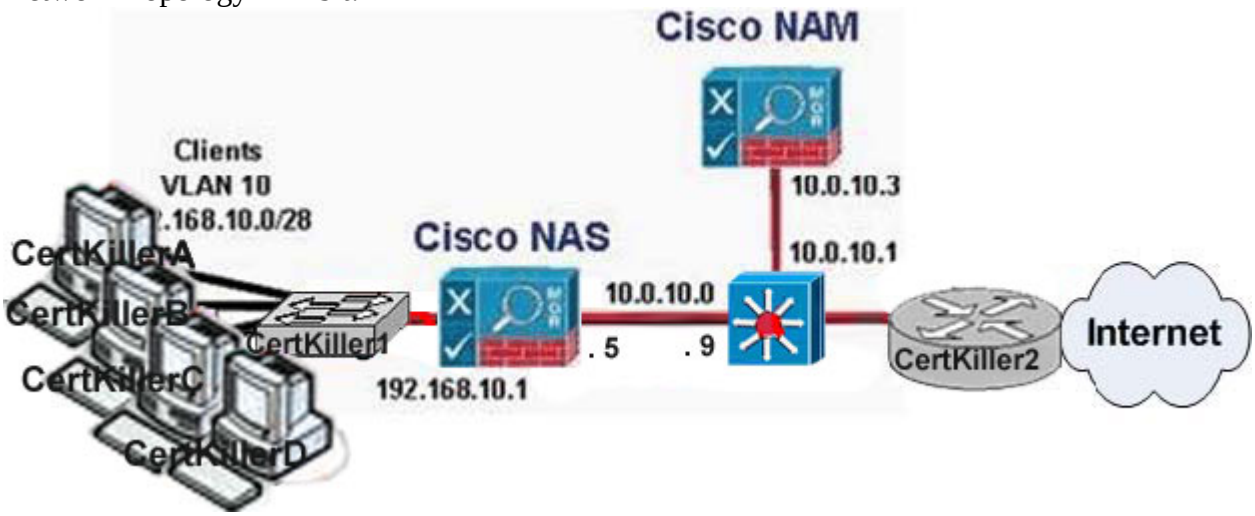
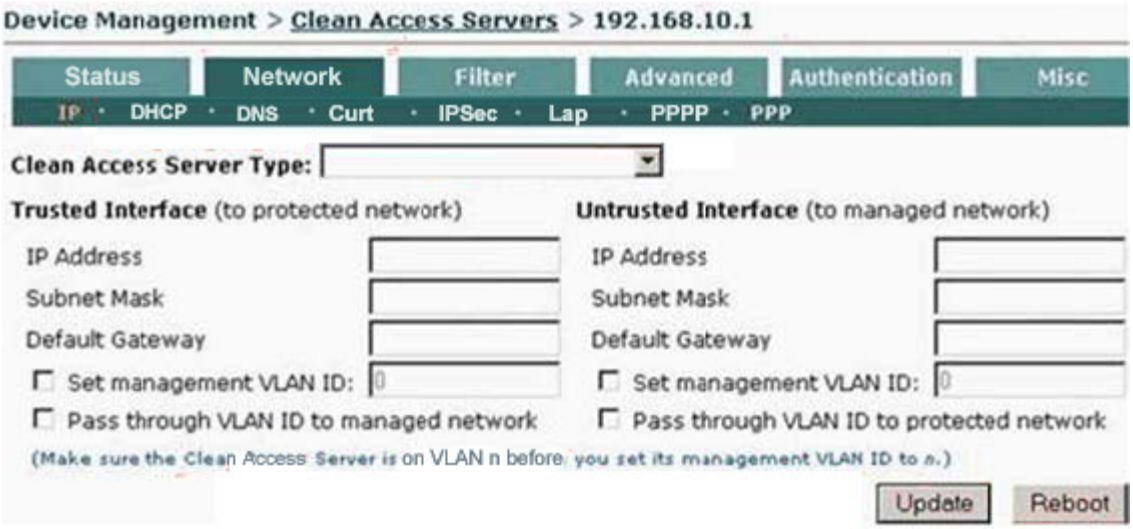


Exhibit #2:



Your work as a network engineer at Certkiller .com. Please study the exhibits carefully. A network Administrator is adding a Cisco NAC Appliance to a network. In the Clean Access Server Type Filed, which Cisco NAS mode should the administrator specify?

A. Out-of-band Virtual Gateway
B. NAT Gateway
C. Virtual Gateway
D. Real IP Gateway
E. Out-of-band real IP gateway

Answer: D

QUESTION 24:

When using Windows Active Directory Single-Sign-On (SSO), the Cisco NAA on the client machine will ask the client machine for a service Ticket (ST) with which username to communicate with the Cisco NAS?

A. The Cisco NAA username
B. The Cisco NAS username
C. The client username
D. The Microsoft Windows Active Directory Server username

Answer: B

QUESTION 25:

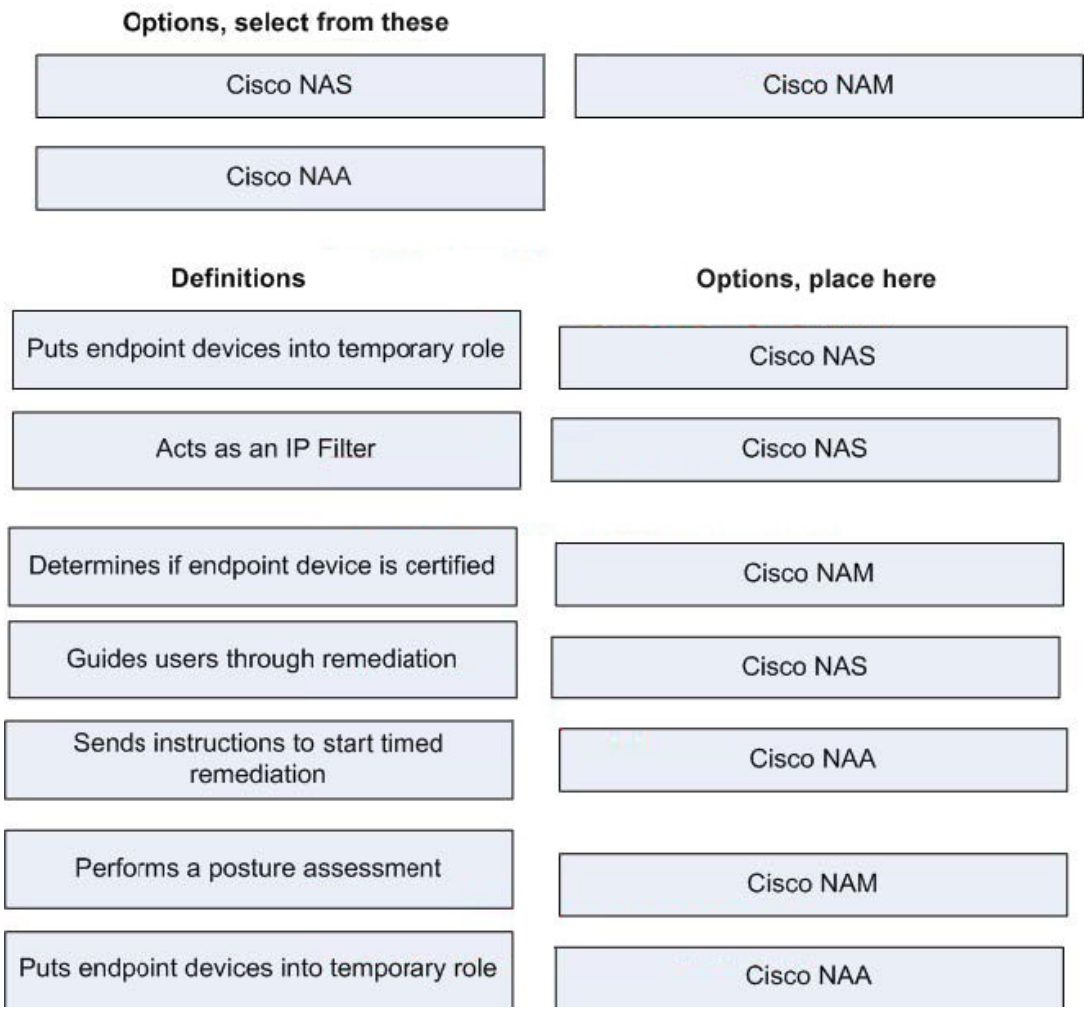
DRAG DROP
You work as a network administrator at Certkiller .com. Your boss, Mrs. Certkiller, is interested in Cisco NAC Appliance components. In particular she is interested of this subject in the context of an in-band deployment.
Match the descriptions with the appropriate components.
Each component may be used multiple times.

Options, select from these

Cisco NAS	Cisco NAM
Cisco NAA	

Definitions	Options, place here
Puts endpoint devices into temporary role	*Place here*
Acts as an IP Filter	*Place here*
Determines if endpoint device is certified	*Place here*
Guides users through remediation	*Place here*
Sends instructions to start timed remediation	*Place here*
Performs a posture assessment	*Place here*
Puts endpoint devices into temporary role	*Place here*

Answer:



QUESTION 26:

Why is critically important to maintain clock synchronization between Cisco NAC Appliance components?

A. Log Files will not show the actual time of system events
B. Cisco NAC Appliance Components communicate using SSL Certificates, which rely on accurate time to function correctly
C. Accurate time is required when performing vulnerability assessment and remediation
D. Cisco Switches that are being managed by SNMP messages need to be time synchronized to function

Answer: B

QUESTION 27:

How is Cisco NAC Appliance Network Scanning Configured?

A. Per NAS
B. Per user role
C. Per rule
D. Per Anti-X requirement

Answer: B

QUESTION 28:

What are two pairs of attributes of traffic policies? (Choose two.)

A. Standard and Extensible
B. Stateful and stateless
C. Global and local
D. Directional and hierarchical
E. Rule and requirement based

Answer: C,D

QUESTION 29:

If an administrator configures interfaces E0, E1 and S0 to support NAM high-availability failover, what information is exchanged over these interfaces?

A. NAM run-time data activities, UDP heartbeat signals, redundant heartbeat signals
B. NAM run-time data activities, UDP heartbeat signals and backup and recover database snapshots
C. NAM run-time data activities and UDP heartbeat signals
D. NAM run-time data activities and IP Based heartbeat signals

Answer: A

QUESTION 30:

Which Cisco NAC Appliance Component performs network scanning?

A. Cisco NAC Appliance Server
B. Cisco NAC Trust Agent
C. Cisco NAC Appliance Manager
D. Cisco NAC Appliance Agent

Answer: A

QUESTION 31:

When the Cisco NAS is configured for Windows Active Directory SSO to which component in a Cisco NAC Appliance solution does the client make a request for a Kerberos Service ticket?

A. Cisco NAS
B. Cisco NAM
C. Microsoft Windows Active Directory Server
D. Cisco NAA

Answer: C

QUESTION 32:

What are the two types of traffic policies that apply to user roles? (Choose two.)

A. Host-Based
B. Server-Based
C. IP-Based
D. Manager-Based
E. VLAN-Based
F. Peer-Based

Answer: A,C

QUESTION 33:

Which Cisco NAS Appliance out-of-band solution statement is correct?

A. The switchport access and authentication VLAN information is sent to the Access switch from the Cisco NAM
B. As a laptop device accesses the Cisco NAC Appliance network, the access switch sends the device MAC address to the Cisco NAS
C. Access switch to Cisco NAM configuration and status change messages are communicated via a proprietary protocol
D. All Client traffic flows through the CAS while access switch VLAN management is performed out of band

Answer: A

QUESTION 34:

What method is used to pass traffic from the client to the Cisco NAS in an in-band Virtual-Gateway L2 deployment?

A. Use VLAN traffic to aggregate the traffic from the client subnets and configure VLAN mapping between the auth and Access VLANS

B. Use Policy-Based Routing
C. Use static routes
D. User the Cisco NAM downloadable ACLs to allow or block traffic at the access switch
E. Use different DHCP addressing and port bouncing to allow or block client traffic

Answer: A

QUESTION 35:

Which two functions can a Cisco NAC Appliance Agent be configured to perform? (Choose two.)

A. Perform registry, service and application checks
B. Detect the presence of worms and viruses before permitting network access to an end user
C. Initiate periodic virus scans
D. Check for up-to-date antivirus and antispam files
E. Quarantine an end user until the client machine complies with company policy

Answer: A,D

QUESTION 36:

Which default Administrator group has delete permissions?

A. Admin
B. Full-Control
C. Help-Desk
D. Add-Edit

Answer: B

QUESTION 37:

What does the secondary Cisco NAM do after it reboots from its initial configuration?

A. Takes over as the active Cisco NAM if the secondary Cisco NAM has a higher priority
B. Automatically sends a message to all Cisco NAS Servers, identifying itself as the secondary Cisco NAM
C. Automatically Synchronizes its database with the primary Cisco NAM
D. Switches to active mode, enabling load sharing with the primary Cisco NAM

Answer: C

QUESTION 38:

Exhibit:

Your work as a network engineer at Certkiller .com. Please study the exhibit carefully. When logging in to a Cisco NAC Appliance solution, an end user is prompted for a username, password and provider. What should be entered in the provider drop-down filed shown in the exhibit?

A. The authentication NAS
B. The Authorization NAM
C. The external Authenticating server
D. The name of the ISP

Answer: C

QUESTION 39:

When Configuring the Cisco NAM to implement Cisco NAA requirement checking on client machines, what is the next step after configuring checks and rules?

A. Map rules to requirement
B. Configure Requirements
C. Configure Session Timeout and traffic policies
D. Require the use of the Cisco NAA
E. Retrieve updates

Answer: B

QUESTION 40:

What is an advantage of a Layer 2 out-of-band virtual gateway deployment using port-based VLAN assignment?

A. Manages bandwidth and session time for users during authentication
B. Supports IP Telephony for end users who are multi-hops away

C. Improves security as the Client IP address must change when the port is changed form the authentication VLAN to the access VLAN
D. Simplifies implementation as client IP addresses are not changed
E. Supports wireless LAN networks providing bandwidth throttling

Answer: D

QUESTION 41:

Which type of certificate is recommended in a high-availability Cisco NAM configuration for the service IP Address?

A. SSL private Certificate
B. SSL public Certificate
C. Temporary Certificate
D. CA-signed Certificate

Answer: D

QUESTION 42:

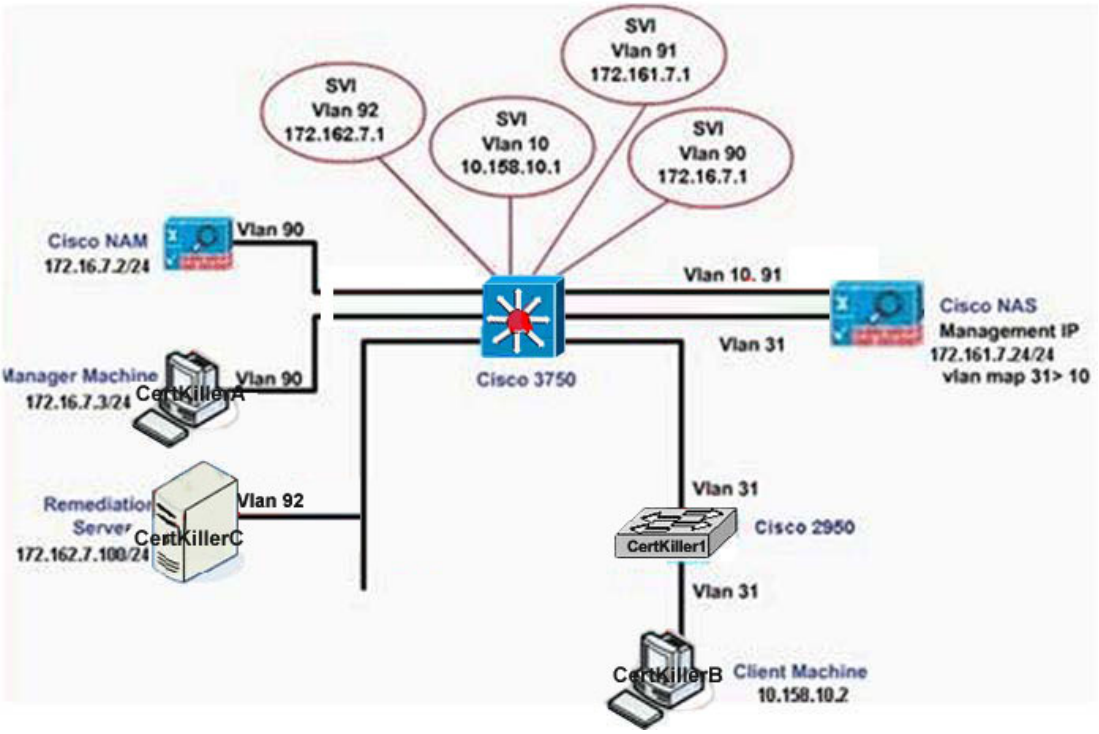
Which three components compromise a Cisco NAC Appliance Solution? (Choose three.)

A. A Linux Server for in-band or out-of-band network admission control
B. A Linux Server for Centralized Management of network admission servers
C. A NAC-enabled Cisco Router
D. A Read-only Client Operating on an endpoints devices
E. A NAC-enabled Cisco Switch

Answer: A,B,E

QUESTION 43:

SIMULATION
Network topology exhibit:



Cisco Clean Access Manager Exhibit:

You work as a network engineer at Certkiller .com. Please study the topology exhibit carefully. Also examine the Cisco Clean Access Manager Exhibit. Certkiller .com has implemented a Cisco NAC Appliance solution. The internal server Certkiller C has been set up to provide HTTP and HTTPS services only. These services are only available for Certkiller .com internal users.

Your boss, Mrs. Certkiller, has asked you to provide the following configuration tasks:

* define a NAC Appliance IP-based traffic policy for the "Temporary Role"

* configure the policy so that it is able to access this remediation server over HTTP and HTTPS for clients on the 10.158.10.0, 255.255.255.0 subhet.
* after the configuration has been completed you must be able to launch the link to access the remediation server from the Certkiller B client computer.

Answer:

Explanation:
1.) Select "User Roles"
2.) At "Temporary Role" klick "Add Policy"
3.) Enter the Following Values:
Priority: 1
Action: Allow
State: Enabled
Category: IP
Protocol: TCP / 6 (see http://www.iana.org/assignments/protocol-numbers/)
Untrusted: 10.158.10.0 / 255.255.255.0 / *
Trusted: 172.162.7.100 / 255.255.255.255 / 80,443
Klick "Add Policy"

QUESTION 44:

A search of available switches has been performed and a list of switches is presented. Which two SNMP attributes need to match what is configured in the Cisco switch profile for a listed switch to be added to the Cisco NAM? (Choose two.)

A. SNMP Trap
B. SNMP write community String
C. SNMP Write Version
D. SNMP read version
E. SNMP read community String

Answer: D,E

QUESTION 45:

After you implement a network scan and view the report, you notice that a plug-in did not access any of it's dependent plug-ins. What did you forget to do?

A. Install dependent plug-ins when you updated the Cisco NAC Appliance plug-in library
B. Configure dependent plug-on support when you mapped the Nessus scan check to the Nessus plug-in rule
C. Load the dependent plug-ins for that plug-in in the Plug-in updates form
D. Enable the Dependent Plug-in check box on the General Tab form

Answer: C

QUESTION 46:

In a Cisco NAM high-availability configuration, when does the secondary Cisco NAM take over?

A. When the IP-based heartbeat signal fails to be transmitted and received within a certain time period
B. When the UDP heartbeat signal fails to be transmitted on the serial heartbeat connection between failover peers
C. When the UDP heartbeat signal is not transmitted and received within a certain time period
D. When the timeout value is exceeded during data-mirroring activities

Answer: C

QUESTION 47:

When the Cisco NAS is configured for Windows Active Directory SSO to which component in a Cisco NAC Appliance solution does the client make a request for a Kerberos Service ticket?

A. Microsoft Windows Active Directory Server
B. Cisco NAM
C. Cisco NAS
D. Cisco NAA

Answer: A

QUESTION 48:

You are implementing switch management in a Cisco NAM for out-of-band deployment. Once communication between the switch and the Cisco NAM has been verified, what is configured next?

A. Configure the Switches to use the appropriate SNMP settings
B. Configure group, switch and port profiles on the Cisco NAM
C. Add the switches that you want to control to the Cisco NAM domain
D. Configure the Cisco NAM SNMP receiver settings

Answer: A

QUESTION 49:

Based on the Boolean order of precedence, how would Cisco NAC Appliance evaluate the following rule?
AdAwareLogRecent&(NorAVProcesslsActiveymAVProcesslsActive)

A. (The Norton Antivirus is active and there is a recent Ad Aware log entry) or (The Symantec antivirus process is active)
B. There is a recent Ad ware log entry, the Norton Antivirus is active and the Symantec antivirus process is active
C. There is a recent Ad Aware log entry or the Norton Antivirus is active or the Symantec Antivirus Process is active
D. (Either the Norton Antivirus or the Symantec Antivirus process is active) and (there is a recent Ad Aware log entry)

Answer: D

QUESTION 50:

A small public library wants to implement network admission control for their public wireless network and their internal wired network. Their network contains switches from a variety of vendors. Which Cisco NAC Appliance solution would best suit this client?

A. An out-of-band Cisco NAS deployment with a Cisco NAM Cluster
B. A Hybrid solution using in-band Cisco NAS for the wireless and out-of-band Cisco NAS for the wired Deployment
C. An in-band Cisco NAS deployment and a Cisco NAM
D. A Combination of an out-of-band and an in-band Cisco NAS deployment with a Cisco NAM Cluster

Answer: C

QUESTION 51:

Which Cisco NAC appliance out-of-band solution statement is correct?

A. Access switch to Cisco NAM configuration and status change messages are communicated via a proprietary protocol
B. The Swichport Access and authentication VLAN information is sent to the access switch from the Cisco NAM
C. As a laptop device accesses the Cisco NAC Appliance network, the access switch sends the device MAC address to the Cisco NAS
D. All client traffic flows through the CAS while access switch VLAN management is performed out of band

Answer: B

QUESTION 52:

In an edge deployment of an in-band virtual-gateway Cisco NAC Appliance solution, how does the Cisco NAS ensure that authenticated client traffic arrives at the correct default gateway?

A. Managed subnets ensure that devices on different untrusted VLANs arrive at the correct default gateways on the trusted side
B. After authentication, the Cisco NAA using its cached IP Addresses, supplies the IP Address of the Correct gateway to the Cisco NAS
C. VLAN trunks are used to aggregate the traffic form the managed subnets to the Cisco NAS before forwarded to their respective gateways on the Layer 3 switch or router
D. Cisco NAS interface are connected to trunked ports to provide VLAN passthrough to the correct gateway

Answer: D

QUESTION 53:

Why are managed subnets configure in out-of-band virtual gateway mode?

A. Configures the Cisco NAS to map the managed subnet to the proper access VLAN
B. Configure the Cisco NAS with an IP Address in the untrusted VLAN that Cisco NAS can use to send ARP request in that particular VLAN
C. Configure the Cisco NAM management subnet so that all the Cisco NAM initiated traffic will be sent out on the proper management subnet
D. Configure the Cisco NAS management subnet so that all the Cisco NAS initiated traffic will sent out of the proper management subnet

Answer: B

QUESTION 54:

A CA-signed certificate is returned from the CA authority and the private key on which the CA certificate is based no longer matches the one in the Cisco NAS. What should the administrator do?

A. Regenerate the certificates based on the FQDN rather than using the service ip address of the NAM
B. Import the single root CA or intermediate CA to .chain.crt in the admin console
C. Edit the Certificate files directly in the file system
D. Reimport the old private key and then install the CA-signed certificate

Answer: D

QUESTION 55:

In a Cisco NAC Appliance Windows Active Directory SSO Deployment, what are the cached credentials and Kerberos TGT from the client-machine Windows login used for?

A. They are used to validate the user authentication and access with the Cisco NAM
B. They are used to validate the user with the Cisco NAS
C. They are used to validate user access with the Cisco NAA
D. They are used to validate the user authentication with eh backend Windows Active Directory Server

Answer: D

QUESTION 56:

A college network administrator wants to restrict access to specific; targeted subnets by role such as student, administration, faculty and guest roles. How would this be accomplished using the Cisco NAM?

A. Define a bandwidth policy for each role that specifies the target subnets
B. Define extended Access-Control-list templates and apply each template to a specific user role
C. Define a host-based traffic control policy for each role that specifies the target subnets
D. Define an IP-Based traffic Control Policy for each role that specifies the target subnets

Answer: D

QUESTION 57:

When trying to restrict a guest role to a specific library server using a specific protocol, such as HTTP, the administrator would create which type of policy?

A. Application-based Access Policy
B. IP-Based Traffic Control Policy
C. Role-Based Access Policy
D. Host-Based Control Policy
E. Host-Based Traffic Policy

Answer: B

QUESTION 58:

In a Layer 3 out-of-band deployment, which Cisco NAC Appliance component provides the Client-Machie IP Address to MAC address mapping?

A. Cisco NAS

B. Cisco Trust Agent
C. Cisco NAM
D. Cisco Security Agent
E. Cisco NAA

Answer: E

QUESTION 59:

The NAS is configured to autogenerate an IP Address pool of 30 subnets with a netmask of /30, beginning at address 192.168.10.0. Which IP Address is leased to the end-user host on the second subnet?

A. 192.168.10.6
B. 192.168.10.5
C. 192.168.10.4
D. 192.168.10.7

Answer: A