Exam : 642-567

Title : Advanced Security for Field Engineers

Ver : 10.12.07

QUESTION 1:

When issuing the show eou all command on a Cisco router acting as a NAD, you do not see any EOUoUDP sessions in the displayed output. Which, most likely, is the problem?

A. No clients have attempted access.
B. Clients are not configured to use EOUoUDP.
C. All NAC sessions have timed out.
D. The router is not properly configured.

Answer: D

QUESTION 2:

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 Clean Access Manager (CAM)?

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

Answer: B

QUESTION 3:

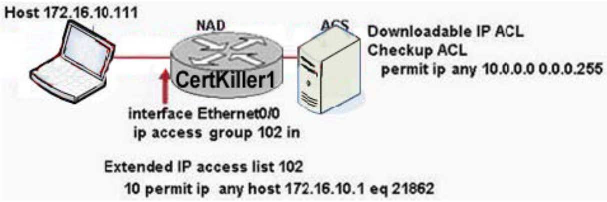
Which Cisco "all-in-one" security appliance automatically detects, isolates, and cleans infected and/or vulnerable devices that attempt to access a network?

A. Cisco Security Monitoring, Analysis and Response System (CS MARS)
B. Cisco Clean Access (CCA)
C. Security Device Manager (SDM)
D. Cisco Security Agent (CSA)

Answer: B

QUESTION 4:

Refer to the exhibit. The ACS server has the downloadable access list called "Checkup ACL" configured. If the host shown is granted access to the network, which access list (ACL) will be sent to the NAD and where will it be placed in the ACL? (Choose two.)
Exhibit:



```
Downloadable IP ACL
Checkup ACL
  permit ip any 10.0.0.0 0.0.0.255
```

```
interface Ethernet0/0
 ip access group 102 in
```

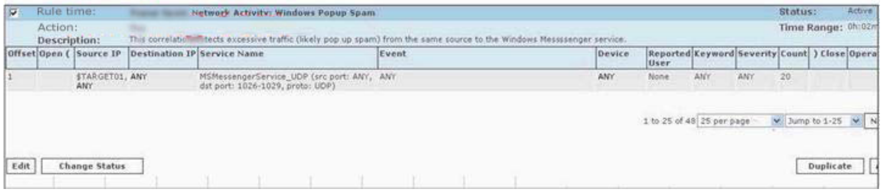
```
Extended IP access list 102
  10 permit ip  any host 172.16.10.1 eq 21862
```

A. permit ip any 10.0.0.0 0.0.0.255
B. permit ip host 172.16.10.111 10.0.0.0 0.0.0.255
C. permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255
D. The access control entry will be placed before the existing static ACL entries.
E. The access control entry will be placed after the existing static ACL entries.
F. Extended IP ACL 102 will be replaced with the named ACL, "Checkup ACL."

Answer: B,D

QUESTION 5:

Exhibit:



☑ Rule time: Network Activity: Windows Popup Spam
Status: Active

Action:
Time Range: 0h:02m

Description: This correlatio[redacted]tects excessive traffic (likely pop up spam) from the same source to the Windows Messsenger service.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Opera
1		$TARGET01, ANY	ANY	MSMessengerService_UDP (src port: ANY, dst port: 1026-1029, proto: UDP)	ANY	ANY	None	ANY	ANY	20		

1 to 25 of 48 25 per page Jump to 1-25

To configure the Mars appliance to send out an alert when the system rule fires, what should you fropm the MARS GUI screen shown?

A. Click on "Active" in the "Status" field, select the appropriate alerts, then apply.
B. Click on "None" in the "Action" field, select the appropriate alerts, then apply
C. Click "Edit" to edit the "Operation" field of the rule, select the appropriate alert option(s), then apply.
D. Click "Edit" to edit the "Event" field of the rule, select the appropriate alert option(s), then apply.
E. Click "Edit" to edit the "Reported User" field of the rule, select the appropriate alert option(s), then apply.

Answer: B

QUESTION 6:

When the maximum limit of 100 unauthorized non-responsive endpoints per NAD is reached, the router stops processing RADIUS requests for NAC to prevent DoS attacks on the ACS server. What then happens to legitimate users attempting access?

A. Users without CTA will be denied access.
B. Users with CTA will still receive posture validation tokens.
C. Users will have default network access (whatever is permitted by the access list [ACL]

of the router interface).
D. All users will be denied access and placed into an "unknown" status.

Answer: C

QUESTION 7:

When installing the Trend AV policy server for use with a Cisco NAC deployment, which two types of web servers can you install? (Choose two.)

A. IIS
B. Mozilla
C. Sun ONE
D. Linux
E. Apache 2.0

Answer: A,E

QUESTION 8:

What information will be displayed with the debug eou eap command when issued on a Cisco Catalyst switch acting as a NAD?

A. EAPoUPD packets
B. EAPoUPD posture validation information
C. all EOU and EAP packets
D. EAP state machine EOU messages

Answer: A

QUESTION 9:

Which two actions result when the access list shown below is applied to an interface of a Cisco router performing NAC? (Choose two.)access-list 102 permit udp any any eq 21862access-list 102 deny ip any any

A. EAPoUDP traffic is allowed.
B. All traffic other than UDP traffic destined to the DNS server is blocked.
C. Clientless host traffic is validated.
D. The rest of the traffic is blocked until it is validated.
E. NAD traffic is forwarded to the antivirus policy server prior to posture assessment.

Answer: A,D

QUESTION 10:

In the CCA Manager, which default administrative group has delete privileges?

A. Manager
B. Add/Edit
C. Full Control
D. Operator

Answer: C

QUESTION 11:

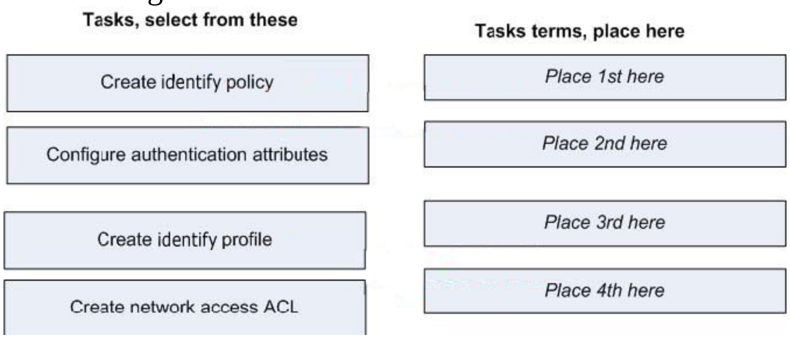
Regarding MARS Appliance rules, which three statements are correct? (Choose three.)

A. There are three types of rules: System Inspection Rules, User Inspection Rules, and Drop Rules.
B. Rules can be saved as reports.
C. Rules can be deleted.
D. Rules trigger incidents.
E. Rules can be defined using a seed file.
F. Rules can be created using a query.

Answer: A,D,F

QUESTION 12:

DRAG DROP
You work as a network technician at Certkiller .com. Your Certkiller trainee Sandra is curious about NAD configuration for clientless hosts. You must order the appropriate NAD configurations tasks.



Tasks, select from these

Create identify policy

Configure authentication attributes

Create identify profile

Create network access ACL

Tasks terms, place here

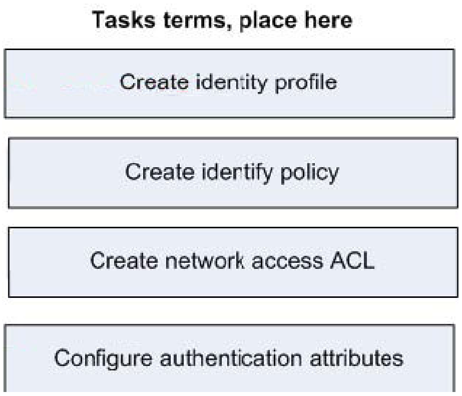
Place 1st here

Place 2nd here

Place 3rd here

Place 4th here

Answer:



Tasks terms, place here

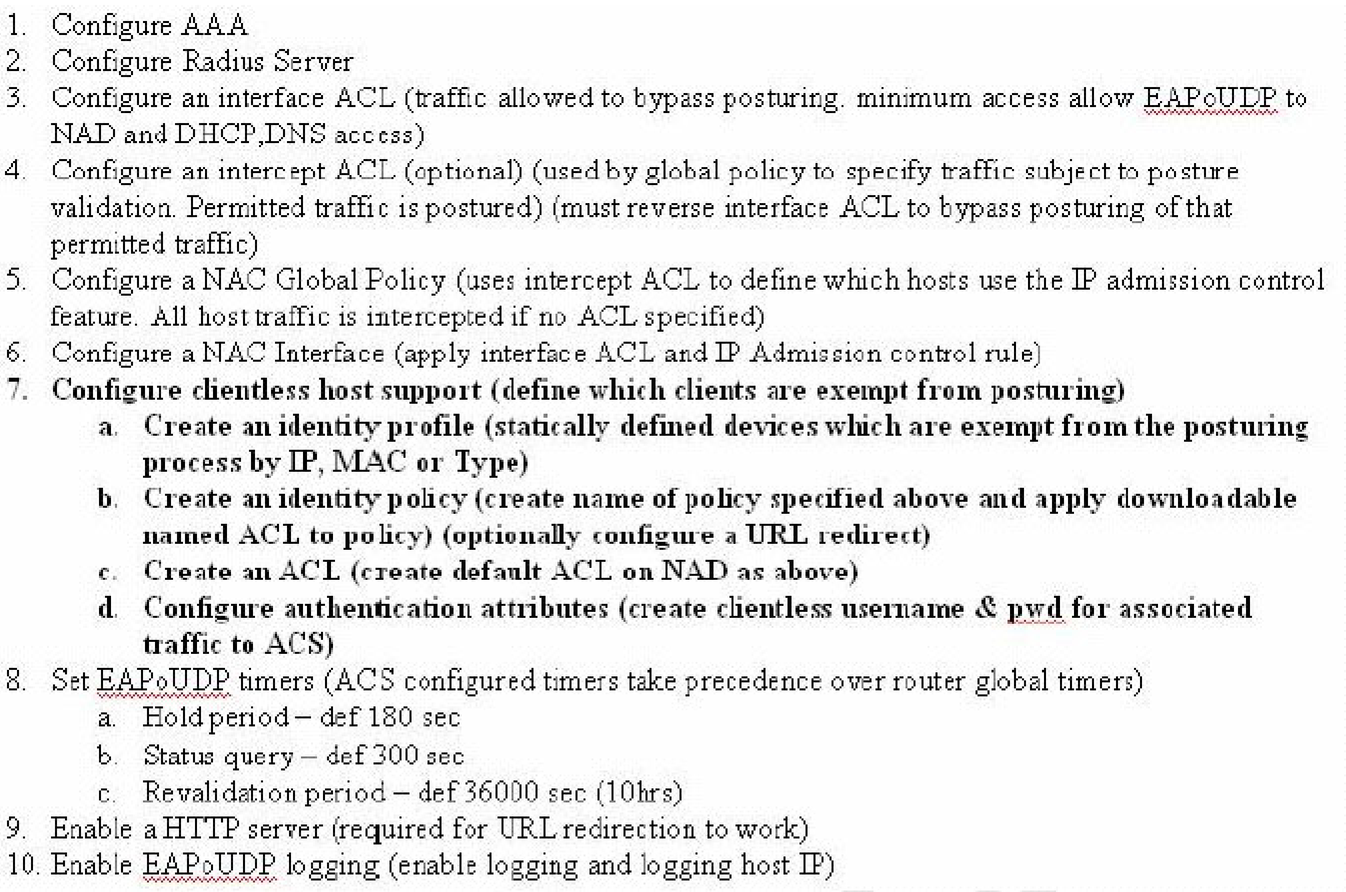
Create identity profile

Create identify policy

Create network access ACL

Configure authentication attributes

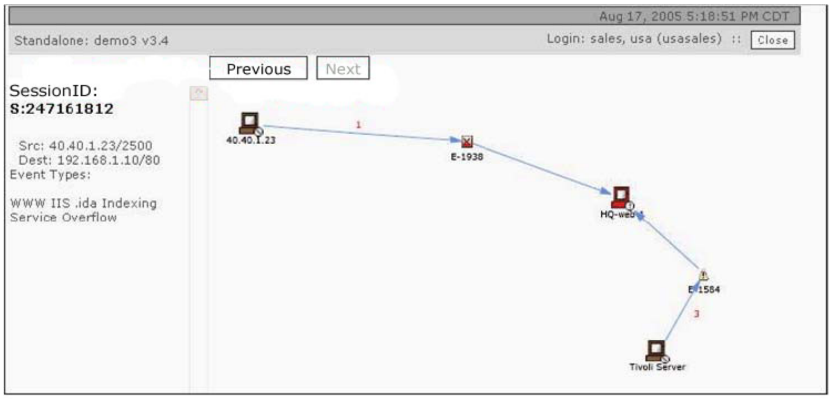
Explanation: ASFE Course Notes pg 1-129 Configuring Cisco IOS Routers for NAC:



1. Configure AAA
2. Configure Radius Server
3. Configure an interface ACL (traffic allowed to bypass posturing. minimum access allow EAPoUDP to NAD and DHCP,DNS access)
4. Configure an intercept ACL (optional) (used by global policy to specify traffic subject to posture validation. Permitted traffic is postured) (must reverse interface ACL to bypass posturing of that permitted traffic)
5. Configure a NAC Global Policy (uses intercept ACL to define which hosts use the IP admission control feature. All host traffic is intercepted if no ACL specified)
6. Configure a NAC Interface (apply interface ACL and IP Admission control rule)
7. **Configure clientless host support (define which clients are exempt from posturing)**
    a. **Create an identity profile (statically defined devices which are exempt from the posturing process by IP, MAC or Type)**
    b. **Create an identity policy (create name of policy specified above and apply downloadable named ACL to policy) (optionally configure a URL redirect)**
    c. **Create an ACL (create default ACL on NAD as above)**
    d. **Configure authentication attributes (create clientless username & pwd for associated traffic to ACS)**
8. Set EAPoUDP timers (ACS configured timers take precedence over router global timers)
    a. Hold period – def 180 sec
    b. Status query – def 300 sec
    c. Revalidation period – def 36000 sec (10hrs)
9. Enable a HTTP server (required for URL redirection to work)
10. Enable EAPoUDP logging (enable logging and logging host IP)

QUESTION 13:

Exhibit:



SessionID:
S:247161812

Src: 40.40.1.23/2500
Dest: 192.168.1.10/80
Event Types:

WWW IIS .ida Indexing
Service Overflow

Refering to the Incident Vector Graph shown on the MARS GUI screen, which three of the following statements are correct? Select three.

A. The port being attacked is port 80
B. This incident has two associated Event Types.
C. You can mitigate this attack by clicking on the device being attacked.
D. The device being attacked is the Tivoli Server
E. Click the Previous button to view any other Sessions related to this incident.

Answer: A, B, E

QUESTION 14:

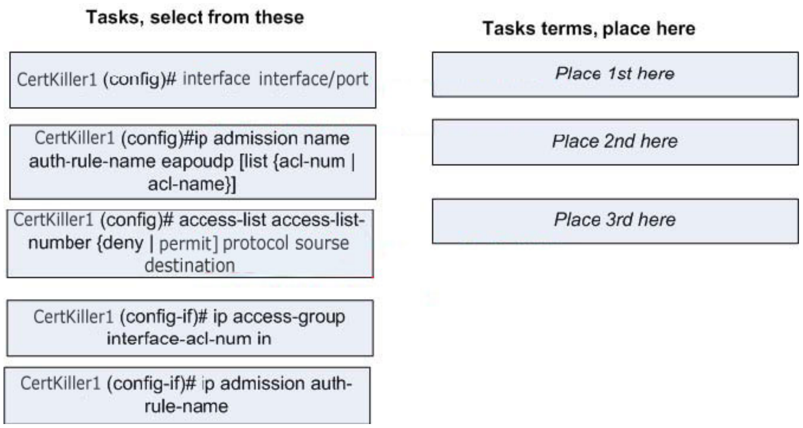
You have an external database configured for use in your NAC deployment. When the ACS forwards the credentials to the external database and does not receive a result in return, what action will the ACS take?

A. return a posture token of "unknown"
B. put the requesting device in the default group
C. automatically redirect the request to a remediation server
D. reject policy validation requests

Answer: D

QUESTION 15:

DRAG DROP
You work as a network technician at Certkiller .com. Your boss is curious about Cisco NAC configuration. Select the configuration tasks that are needed to configure a Cisco NAC switch interface.
You will not use all tasks.



Tasks, select from these

CertKiller1 (config)# interface interface/port

CertKiller1 (config)#ip admission name auth-rule-name eapoudp [list {acl-num | acl-name}]

CertKiller1 (config)# access-list access-list-number {deny | permit] protocol sourse destination

CertKiller1 (config-if)# ip access-group interface-acl-num in

CertKiller1 (config-if)# ip admission auth-rule-name

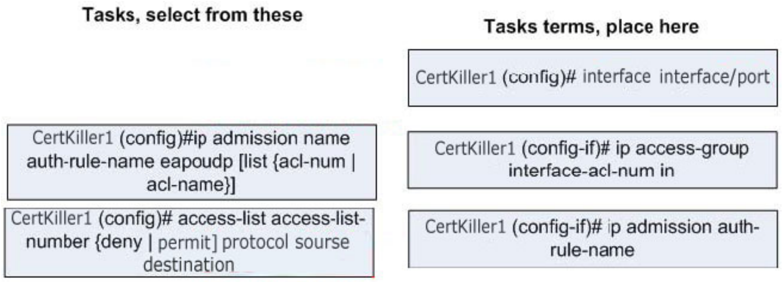
Tasks terms, place here

Place 1st here

Place 2nd here

Place 3rd here

Answer:



Tasks, select from these

CertKiller1 (config)#ip admission name auth-rule-name eapoudp [list {acl-num | acl-name}]

CertKiller1 (config)# access-list access-list-number {deny | permit] protocol sourse destination

Tasks terms, place here

CertKiller1 (config)# interface interface/port

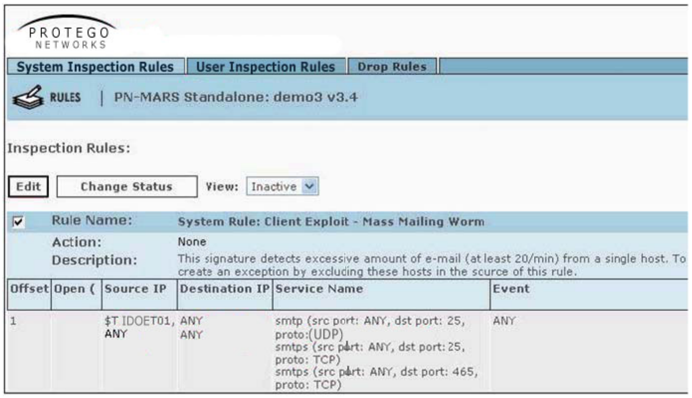
CertKiller1 (config-if)# ip access-group interface-acl-num in

CertKiller1 (config-if)# ip admission auth-rule-name

Explanation: ASFE Course Notes pg 1-161/162 (config)# interface fe0/1 (config-if)# ip access-group Interface_ACL in (config-if)# ip admission NAC_Rule

QUESTION 16:

Exhibit:



PN-MARS Standalone: demo3 v3.4

Inspection Rules:

View: Inactive

☑ Rule Name: System Rule: Client Exploit - Mass Mailing Worm

Action: None

Description: This signature detects excessive amount of e-mail (at least 20/min) from a single host. To create an exception by excluding these hosts in the scurce of this rule.

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$T IDOET01, ANY	ANY ANY	smtp (src port: ANY, dst port: 25, proto:(UDP) smtps (src port: ANY, dst port: 25, proto: TCP) smtps (src port: ANY, dst port: 465, proto: TCP)	ANY

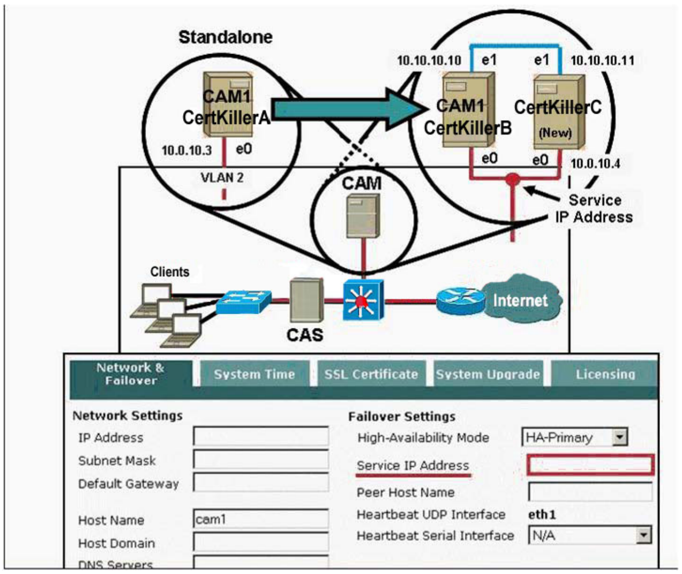
Referring to the System Inspection Rule shown on the MARS GUI screen, which one of the following statements is correct?

A. Click on "Add" to activate the rule.
B. Click on "Activate" to activate the rule.
C. Click on "Change Status" to activate the rule.
D. Click on "Edit". Then you can apply and activate the rule.
E. Click on "Duplicate" to archive the rule to a remote NAS.

Answer: C

QUESTION 17:

When migrating from an existing standalone CAM to a High Availability CAM solution, what IP address should the administrator configure for the CAM1 service IP address?
Exhibit:



Network Settings
IP Address
Subnet Mask
Default Gateway
Host Name: cam1
Host Domain
DNS Servers

Failover Settings
High-Availability Mode: HA-Primary
Service IP Address
Peer Host Name
Heartbeat UDP Interface: eth1
Heartbeat Serial Interface: N/A

A. 10.10.10.3
B. 10.10.10.4
C. 10.10.10.5 (an unused IP address)
D. 10.10.10.252 (assigned by the system)

Answer: A

QUESTION 18:

Which CCA out-of-band solution statement is correct?

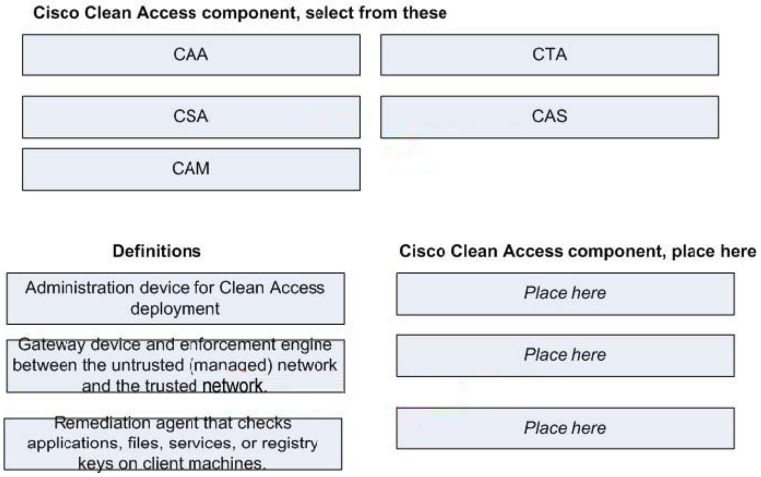
A. All client traffic flows through the CAS while access switch VLAN management is performed out of band.
B. Access switch to CAM configuration and status change messages are communicated via a proprietary protocol.
C. The switchport access and authentication VLAN information is sent to the access switch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

Answer: C

Explanation: ASFE Course Notes pg 2-178
Add the switches that you want to control to the NAM. When the switches are added and the ports on the switch are discovered, you can then configure the relevant switch ports to use the relevant port profiles. These profiles set up the ports to use the appropriate access and authentication VLANS to enable the client traffic to be routed temporarily through the NAS for authentication and certification before allowing this traffic on the trusted network.

QUESTION 19:

You work as a network technician at Certkiller .com. Your Certkiller trainee Sandra is curios Cisco Clean Access component. You need to match the component with the correct description.



Cisco Clean Access component, select from these

CAA

CTA

CSA

CAS

CAM

Definitions

Administration device for Clean Access deployment

Gateway device and enforcement engine between the untrusted (managed) network and the trusted network.

Remediation agent that checks applications, files, services, or registry keys on client machines.

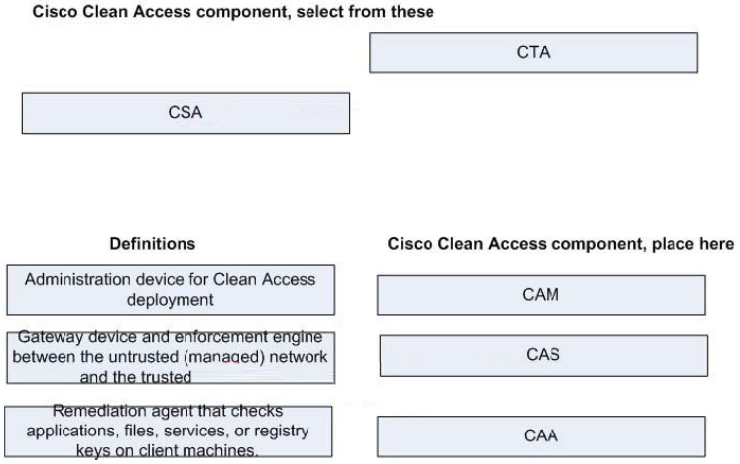
Cisco Clean Access component, place here

Place here

Place here

Place here

Answer:



Cisco Clean Access component, select from these

CTA

CSA

Definitions

Administration device for Clean Access deployment

Gateway device and enforcement engine between the untrusted (managed) network and the trusted

Remediation agent that checks applications, files, services, or registry keys on client machines.

Cisco Clean Access component, place here

CAM

CAS

CAA

QUESTION 20:

How does the Clean Access Manager (CAM) determine the presence of vulnerability?

A. The end-user CTA capability summary message does not match the defined role-based security policy requirement on the CAM.
B. The CAM receives a CSA vulnerability alert from the Clean Access Server (CAS).
C. The CAS network scan report matches a defined role- or OS-based vulnerability on the CAM.
D. The CCA scan report matches a role-based vulnerability signature on the CAM.

Answer: C

QUESTION 21:

You have installed the Cisco Trust Agent (CTA) on remote PCs for posture validation. However, CTA is not communicating properly with the validation server. What is a probable cause for this communication issue?

A. The redirect URL is not properly configured for remediation before allowing network access.
B. Incorrect credentials are being passed to the policy validation server.
C. A personal firewall is not configured to pass EAPoUDP.
D. The control services applet is not properly configured.

Answer: C

QUESTION 22:

Which three statements are correct about the MARS Global Controller? (Choose three.)

A. The Global Controller can correlate events from different Local Controllers into a common session.
B. One Global Controller can support multiple Local Controllers.
C. Each zone can have one Local Controller.
D. All Local Controllers events are propagated to the Global Controller for correlations.
E. The Global Controller and the Local Controllers can be running different MARS OS versions.
F. Based on a selected Local Controller, incidents on the Global Controller can be viewed.

Answer: B,C,F

QUESTION 23:

What are the three components that make up the Cisco Clean Access solution? (Choose three.)

A. Cisco Trust Agent (CTA)
B. Cisco Access Manager (CAM)

C. Cisco Security Agent (CSA)
D. Cisco Secure Access Control Server (ACS)
E. Cisco Access Server
F. Cisco Access Agent

Answer: B,E,F

QUESTION 24:

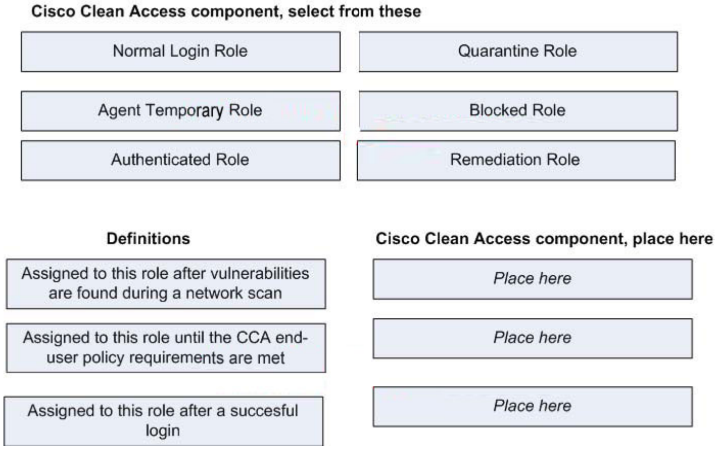
A Cisco Secure ACS evaluates a posture validation request using a NAC database that has 10 local policies and one external policy, but the external NAC servers associated with the external policy are not online. The 10 local policies all return security posture tokens (SPTs). The offline external policy is not returned because it is offline at the time of the request. What action will the ACS take?

A. The ACS will return the redirect URL token until it can validate the security posture.
B. The ACS will reject the posture validation request.
C. The ACS will return the valid SPTs with a posture validation of "checkup."
D. The ACS will check the application posture tokens (APTs) to determine the security posture status before returning a posture token.

Answer: B

QUESTION 25:

DRAG DROP
You work as a network technician at Certkiller .com. Your Certkiller trainee Sandra is curios Cisco Clean Access component. You need to match the component with the correct description.

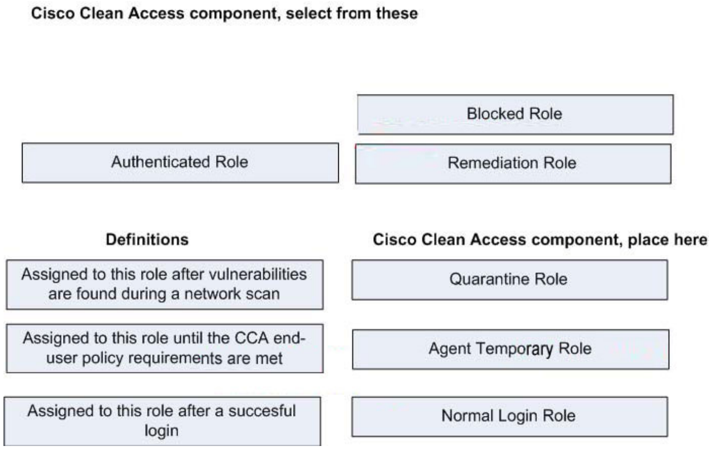


Cisco Clean Access component, select from these

Normal Login Role
Quarantine Role
Agent Temporary Role
Blocked Role
Authenticated Role
Remediation Role

Definitions	Cisco Clean Access component, place here
Assigned to this role after vulnerabilities are found during a network scan	Place here
Assigned to this role until the CCA end-user policy requirements are met	Place here
Assigned to this role after a succesful login	Place here

Answer:



Cisco Clean Access component, select from these

Blocked Role

Authenticated Role

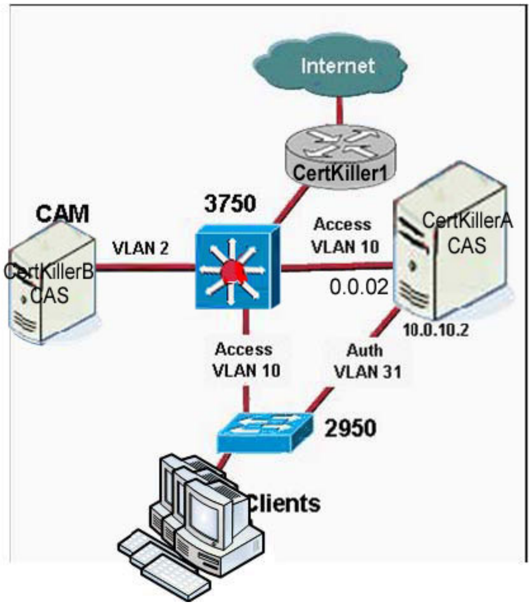
Remediation Role

Definitions	Cisco Clean Access component, place here
Assigned to this role after vulnerabilities are found during a network scan	Quarantine Role
Assigned to this role until the CCA end-user policy requirements are met	Agent Temporary Role
Assigned to this role after a succesful login	Normal Login Role

QUESTION 26:

Refer to the exhibit. The network represents which type of Cisco Clean Access deployment?

Exhibit:



A. real IP gateway in-band
B. virtual gateway in-band
C. real IP gateway out-of-band
D. virtual gateway out-of-band

Answer: D

QUESTION 27:

What is the resulting action of the command eou timeout hold-period 60?

A. The EOU process will attempt to validate credentials (Accept-Reject) or EAPoUDP for a maximum of 60 seconds before quarantining the requesting client.
B. The hold timer will wait 60 seconds following a failed credential validation or an EAPoUDP association failure before a new association can be retried.
C. The EOU process will hold the client in an unknown state for 60 seconds maximum while the credential validation process is in progress.
D. Credentials will be considered valid for 60 minutes before a revalidation occurs.

Answer: B

Explanation:
ASFE Course Notes pg 1-172
EAPoUDPTimers:
HOLD-PERIOD: Wait specified seconds following a failed credential validation or EAPoUDP association failure before a new association can be retried. Default is 180 sec.
STATUS-QUERY: Once credential validation and security posture session is successfully established the NAD will send a status query to the client. If the NAD does not receive a response from the client it will wait the specified seconds before trying again. The timer is reset every time a response is received. Default is 300 sec.
REVALIDATION: Once credential validation and security posture session is successfully established the NAD will wait the specified seconds before revalidating the client credentials. Default is 36000 sec.

QUESTION 28:

Which two of the following are required to enable MARS level 3 operations? (Choose two.)

A. Global Controller
B. vulnerability scanning
C. Netflow
D. SNMP community string
E. username and password to log in to the device

Answer: D,E

Explanation: ASFE Course Notes pg 3-42
Level 3: is operational once you have entered the community string information for your network devices.
Username & password for device: (can't find a solid reference for this, but surmise the following:)
A fully enabled MARS has automated mitigation capability. The MARS only stores RO SNMP string so a logon username & pwd are required for full control of the network device.

QUESTION 29:

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?

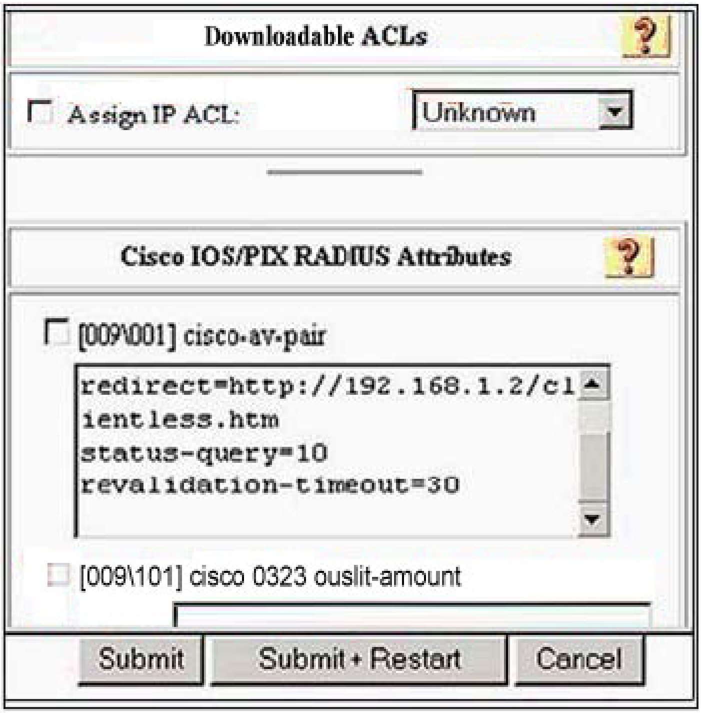
A. application-based exemption policy
B. IP-based traffic control policy
C. destination-based inclusion policy
D. role-based access policy

Answer: B

QUESTION 30:

Refer to the exhibit. You are troubleshooting a problem with a clientless host. It is showing up as 'unknown' or URL redirection is not working. You have determined that the problem lies in the Cisco ACS configuration. Which two parameters must be changed in order to correct this behavior? (Choose two)

Exhibit:



□ Assign IP ACL: Unknown

□ [009\001] cisco-av-pair

```
redirect=http://192.168.1.2/cl
ientless.htm
status-query=10
revalidation-timeout=30
```

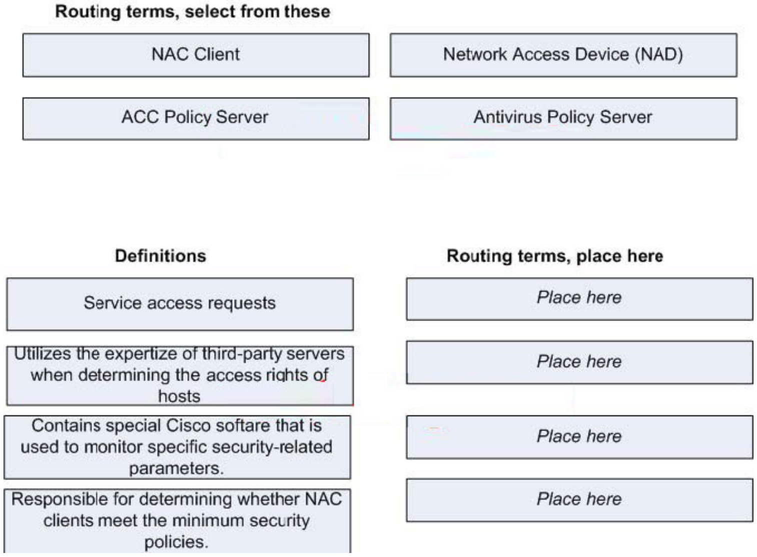
□ [009\101] cisco 0323 ouslit-amount

A. Check "Assign IP ACL."
B. Change the dropdown to "Healthy."
C. Check the "[0900\001] cisco-av-pair" box.
D. Change the redirect statement to http://192.168.1.2/healthy.htm.
E. Increase the status-query timer to 20 to help prevent a query timeout.

Answer: A,C

QUESTION 31:

DRAG DROP
Certkiller, your boss at Certkiller .com, asks you about NAC components. You must match the component with the appropriate function.

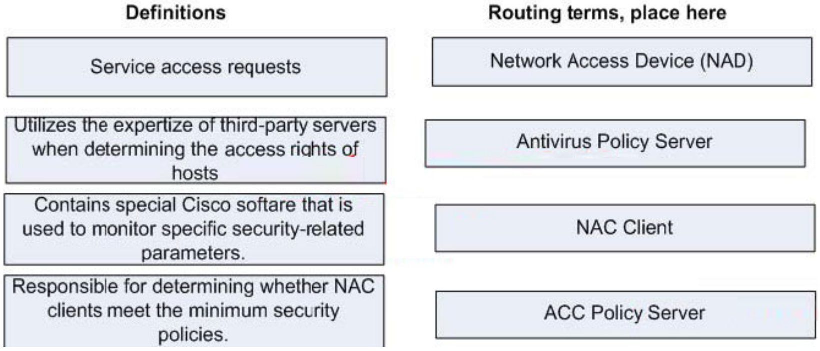


Routing terms, select from these

NAC Client
Network Access Device (NAD)
ACC Policy Server
Antivirus Policy Server

Definitions	Routing terms, place here
Service access requests	*Place here*
Utilizes the expertize of third-party servers when determining the access rights of hosts	*Place here*
Contains special Cisco softare that is used to monitor specific security-related parameters.	*Place here*
Responsible for determining whether NAC clients meet the minimum security policies.	*Place here*

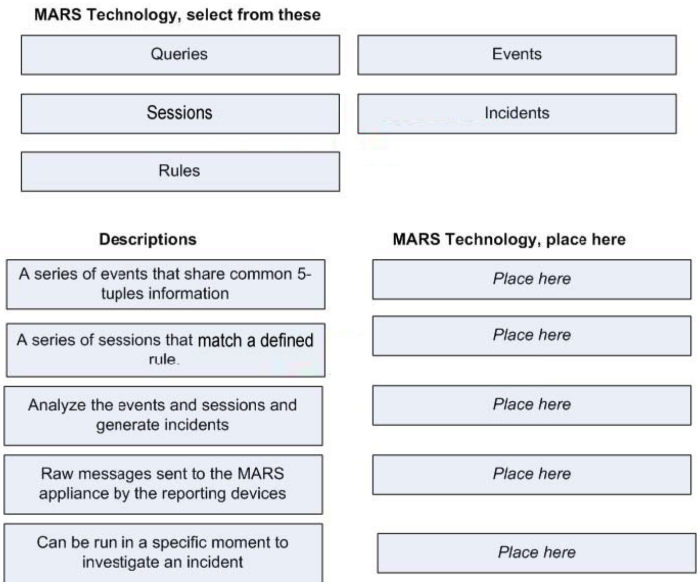
Answer:



Definitions	Routing terms, place here
Service access requests	Network Access Device (NAD)
Utilizes the expertize of third-party servers when determining the access rights of hosts	Antivirus Policy Server
Contains special Cisco softare that is used to monitor specific security-related parameters.	NAC Client
Responsible for determining whether NAC clients meet the minimum security policies.	ACC Policy Server

QUESTION 32:

DRAG DROP
Sandre, your Certkiller .com Trainee, asks you about the MARS terminology. You must match the component with the appropriate function.

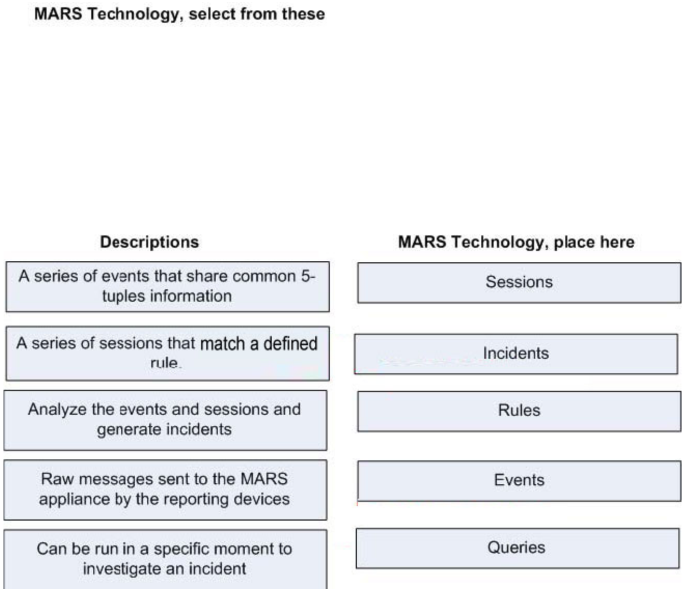


MARS Technology, select from these

Queries	Events
Sessions	Incidents
Rules	

Descriptions	MARS Technology, place here
A series of events that share common 5-tuples information	*Place here*
A series of sessions that match a defined rule.	*Place here*
Analyze the events and sessions and generate incidents	*Place here*
Raw messages sent to the MARS appliance by the reporting devices	*Place here*
Can be run in a specific moment to investigate an incident	*Place here*

Answer:



MARS Technology, select from these

Descriptions	MARS Technology, place here
A series of events that share common 5-tuples information	Sessions
A series of sessions that match a defined rule.	Incidents
Analyze the events and sessions and generate incidents	Rules
Raw messages sent to the MARS appliance by the reporting devices	Events
Can be run in a specific moment to investigate an incident	Queries

QUESTION 33:

Which two functions can a Cisco Clean Access Agent (CCA) be configured to perform? (Choose two.)

A. initiate periodic AV vendor virus scans
B. check for up-to-date AV files
C. detect presence of worms and viruses before permitting an end user network access
D. perform registry, service, and application checks
E. quarantine an end user until system is remediated

Answer: B,D

QUESTION 34:

If the CAS 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. 192.168.10.4
B. 192.168.10.5
C. 192.168.10.6
D. 192.168.10.7

Answer: C

Explanation:
ASFE Course Notes pg 2-109
Subnet /30 1 2 3
Network Address 192.168.10.0 192.168.10.4 192.168.10.8
Router Address 192.168.10.1 192.168.10.5 192.168.10.9
Client Address 192.168.10.2 192.168.10.6 192.168.10.10
Broadcast Address 192.168.10.3 192.168.10.7 192.168.10.11

QUESTION 35:

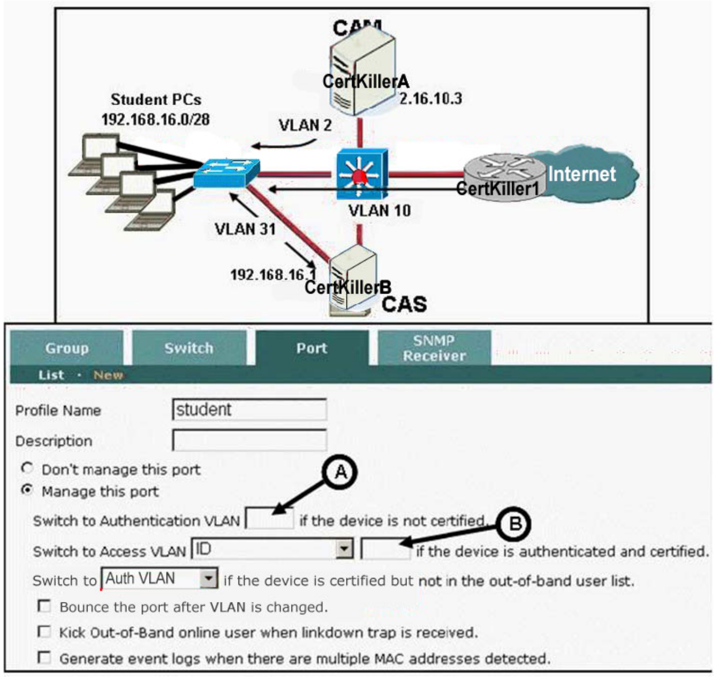
What enables the MARS Appliance to profile network usage and detect statistically significant anomalous behavior from a computed baseline?

A. MARS Global Controller
B. VMS
C. Netflow
D. CiscoWorks
E. MARS custom parser

Answer: C

QUESTION 36:

Refer to the exhibit. In an IP-routed, out-of-band solution, choose the correct VLAN number for callout A and B. (Choose two.)



Profile Name [student]

Description [ ]

○ Don't manage this port

● Manage this port

Switch to Authentication VLAN [ ] if the device is not certified.

Switch to Access VLAN [ID ▾] [ ] if the device is authenticated and certified.

Switch to [Auth VLAN ▾] if the device is certified but not in the out-of-band user list.

□ Bounce the port after VLAN is changed.

□ Kick Out-of-Band online user when linkdown trap is received.

□ Generate event logs when there are multiple MAC addresses detected.

A. A=(VLAN)2
B. A=(VLAN)10
C. A=(VLAN)31
D. B=(VLAN)2
E. B=(VLAN)10
F. B=(VLAN)31

Answer: C,E

QUESTION 37:

Which action enables the MARS Appliance to ignore false positive events by either dropping the events completely, or by just logging them to the database?

A. Creating System Inspection Rules using the Drop operation
B. Creating Drop Rules
C. Inactivating the Rules
D. Inactivating events
E. Deleting the false positive events from the Incidents > False Positives screen
F. Deleting the false positive events from the Management > Event Management screen

Answer: B

QUESTION 38:

Which command would you issue to view the current list of network admission entries on a Cisco switch acting as a NAD?

A. show ip nac hosts
B. show ip nac eou
C. show ip admission all
D. show ip admission cache

Answer: D

QUESTION 39:

What is the default SSL port number you will need to know when confirming the installation of a Trend Micro OfficeScan Server when both the OfficeScan and Policy Servers are installed on the same IIS virtual web site?

A. 1682
B. 1918
C. 4343
D. 8080

Answer: C

QUESTION 40:

Identify three ways an administrator can implement Cisco Clean Access (CCA) to protect a network. (Choose three.)

A. CTA only
B. CSA only
C. CAA only
D. CAA and network scan
E. network scan only
F. end-user scan only

Answer: C,D,E

QUESTION 41:

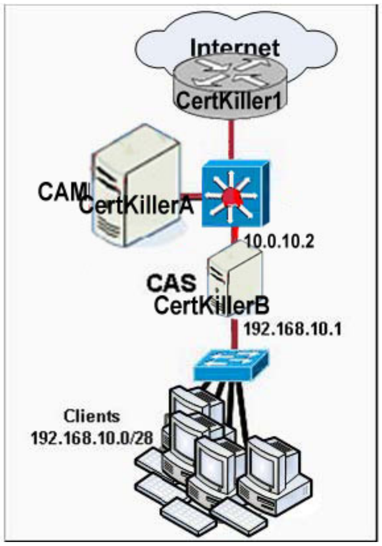
When adding a device to the MARS Appliance, what is the reporting IP address of the device?

A. the source IP address that sends syslog information to the MARS Appliance
B. the IP address MARS uses to access the device via SNMP
C. the IP address MARS uses to access the device via Telnet or SSH
D. the pre-NAT IP address of the device
E. the highest loopback IP address configured on the Cisco reporting device

Answer: A

QUESTION 42:

Refer to the exhibit. The network represents which type of Cisco Clean Access deployment?
Exhibit:



A. real IP gateway in-band
B. virtual gateway in-band
C. real IP Gateway out-of-band
D. virtual gateway out-of-band

Answer: A

QUESTION 43:

What is specified when the command ip radius source-interface is entered in the global configuration mode of a Cisco switch acting as a NAD?

A. the interface for all outgoing RADIUS packets
B. that all interfaces are sources for RADIUS authentication requests
C. that Layer 2 packets received are converted and passed to the RADIUS server as Layer 3 IP packets
D. the interface where the sourced RADIUS packets should be received at the switch

Answer: A

QUESTION 44:

A MARS Appliance cannot access certain devices through the default gateway.

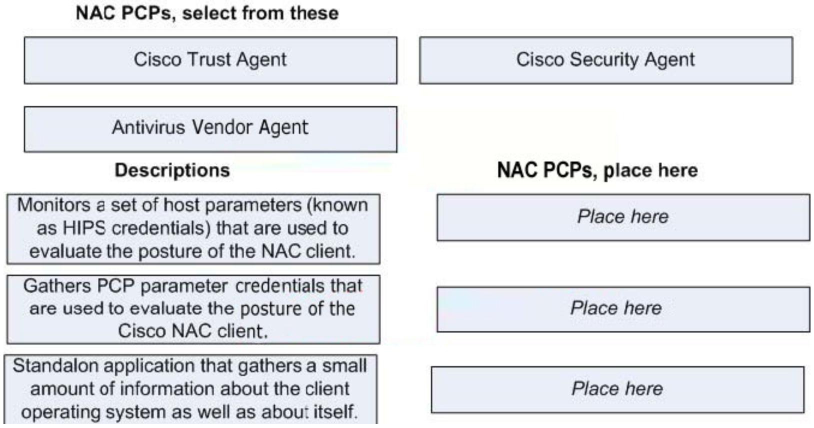
Troubleshooting has determined that this is a MARS configuration issue. Which additional MARS configuration will be required to correct this issue?

A. Use the MARS GUI to enable a dynamic routing protocol.
B. Use the MARS GUI to add a static route.
C. Use the MARS GUI to configure multiple default gateways.
D. Use the MARS CLI to enable a dynamic routing protocol.
E. Use the MARS CLI to add a static route.
F. Use the MARS CLI to configure multiple default gateways.

Answer: E

QUESTION 45:

DRAG DROP
You work as a network technician at Certkiller .com. Your Certkiller trainee Sandra is curious in NAC Posture Credentials Provider (PCP). You must order the NAC PCPs with the appropriate descriptions.

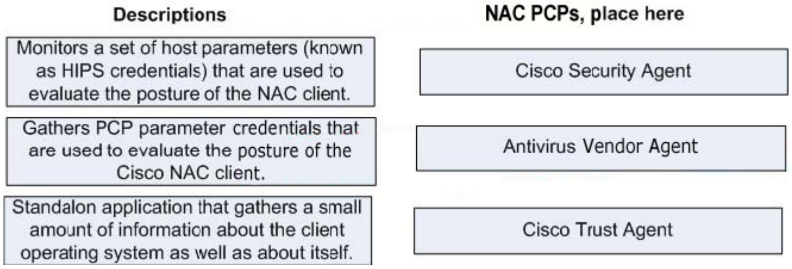


NAC PCPs, select from these

Cisco Trust Agent
Cisco Security Agent
Antivirus Vendor Agent

Descriptions	NAC PCPs, place here
Monitors a set of host parameters (known as HIPS credentials) that are used to evaluate the posture of the NAC client.	Place here
Gathers PCP parameter credentials that are used to evaluate the posture of the Cisco NAC client.	Place here
Standalon application that gathers a small amount of information about the client operating system as well as about itself.	Place here

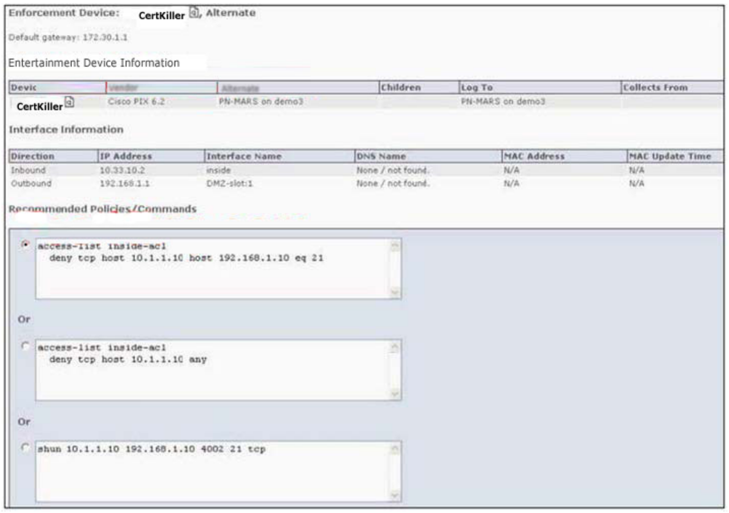
Answer:



Descriptions	NAC PCPs, place here
Monitors a set of host parameters (known as HIPS credentials) that are used to evaluate the posture of the NAC client.	Cisco Security Agent
Gathers PCP parameter credentials that are used to evaluate the posture of the Cisco NAC client.	Antivirus Vendor Agent
Standalon application that gathers a small amount of information about the client operating system as well as about itself.	Cisco Trust Agent

QUESTION 46:

Exhibit:



Enforcement Device: CertKiller, Alternate

Default gateway: 172.30.1.1

Entertainment Device Information

Devic	Vendor	Alternate	Children	Log To	Collects From
CertKiller	Cisco PIX 6.2	PN-MARS on demo3		PN-MARS on demo3	

Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time
Inbound	10.33.10.2	inside	None / not found.	N/A	N/A
Outbound	192.168.1.1	DMZ-slot:1	None / not found.	N/A	N/A

Recommended Policies/Commands

●
```
access-list inside-acl
  deny tcp host 10.1.1.10 host 192.168.1.10 eq 21
```

Or

○
```
access-list inside-acl
  deny tcp host 10.1.1.10 any
```

Or

○
```
shun 10.1.1.10 192.168.1.10 4002 21 tcp
```

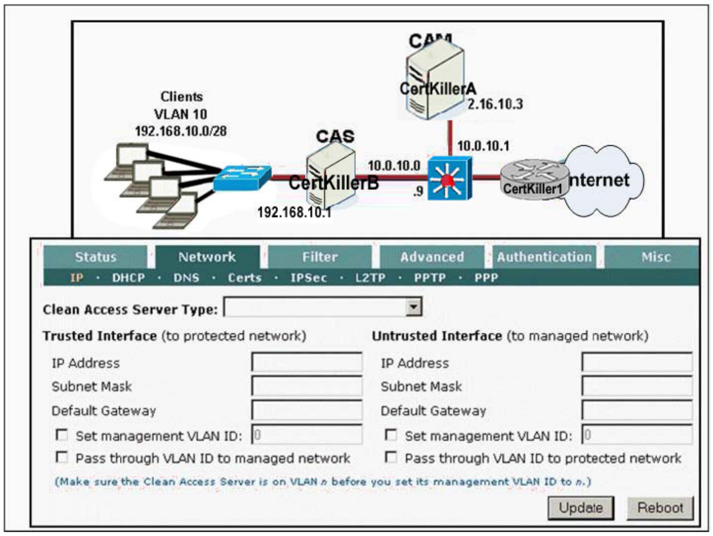
Referring to the exhibit shown on the MARS GUI screen, why is the Push function not enabled (greyed out)?

A. Because the Certkiller device is the alternate choke paint for mitigating this attack.
B. Because MARS cannot push commands to Layer 3 devices.
C. Because the Incident has not been confirmed by the administrator.
D. Because the Incident is a false positiove.
E. Because MARS is operating at level 2 and not at level 3.
F. Because the selected mitigation command is not support on the Certkiller device.

Answer: B

QUESTION 47:

Refer to the exhibit. A network administrator is adding a CAS to a network. In the Trusted and Untrusted IP Address fields, which IP addresses should they specify? (Choose two.)
Exhibit:



Clean Access Server Type:

Trusted Interface (to protected network)

IP Address

Subnet Mask

Default Gateway

□ Set management VLAN ID: 0

□ Pass through VLAN ID to managed network

Untrusted Interface (to managed network)

IP Address

Subnet Mask

Default Gateway

□ Set management VLAN ID: 0

□ Pass through VLAN ID to protected network

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

A. Trusted IP Address - 10.0.10.3
B. Trusted IP Address - 10.0.10.15
C. Trusted IP Address - 192.168.10.1
D. Untrusted IP Address - 10.0.10.3
E. Untrusted IP Address - 10.0.10.15
F. Untrusted IP Address - 192.168.10.1

Answer: B,F

QUESTION 48:

When restoring archived data to a MARS Appliance, which is the best practice to follow?

A. Use HTTPS to protect the data transfer.
B. Use secured FTP to protect the data transfer.
C. Use "mode 5" restore from the MARS CLI to provide enhanced security during the data transfer.
D. Use the Admin > System Maintenance > Data Archiving on the MARS GUI to perform restore operations online.
E. To avoid problems, only restore to a same or higher-end MARS Appliance.

Answer: E

QUESTION 49:

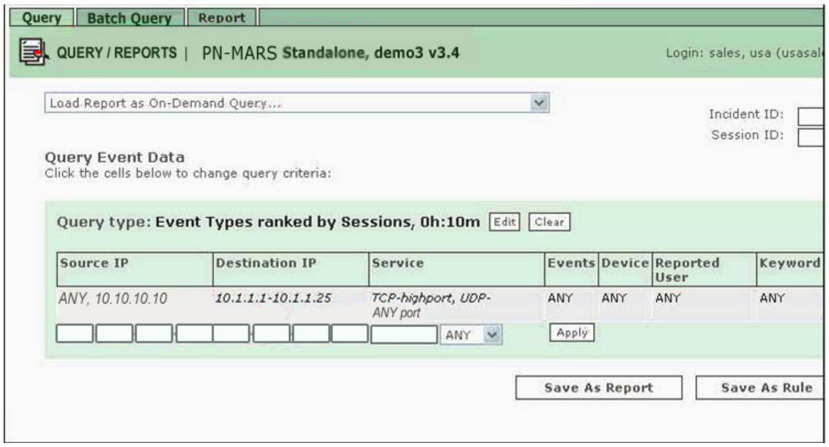
Cisco Clean Access (CCA) network scanning is performed by which of the following CCA components?

A. CAM
B. CAS
C. CAA
D. CTA

Answer: B

QUESTION 50:

Exhibit:



QUERY / REPORTS | PN-MARS Standalone, demo3 v3.4

Login: sales, usa (usasal

Load Report as On-Demand Query...

Incident ID:

Session ID:

Query Event Data

Click the cells below to change query criteria:

Query type: Event Types ranked by Sessions, 0h:10m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword
ANY, 10.10.10.10	10.1.1.1-10.1.1.25	TCP-highport, UDP-ANY port	ANY	ANY	ANY	ANY

ANY

Which three of the following statements are correct regarding the Query shown in the MARS GUI screen? Select three.

A. Query will match any source IP address.
B. Query will only match a source IP address of 10.10.10.10.
C. Query will only match a destination IP address range from 10.1.1.1 to 10.1.1.25
D. Query will only match a destination IP address of 10.1.1.1 or 10.1.1.25
E. Query will only match any services since both TCP-highPort and UDP-hihgPort service groups are specifided in the Service field.
F. Query will only match any service using the TCP-highPort OR UDP-highPort service groups.

Answer: A, C, F

QUESTION 51:

Which High Availability option is supported by Cisco Clean Access (CCA) solution?

A. CAA load balancing
B. CAM and CAS redundancy
C. CAA backup server
D. CAS backup network scanning

Answer: B

QUESTION 52:

Which of the following is a supported mitigation feature on the MARS Appliance?

A. Generating and pushing configuration commands to Layer 3 devices
B. Generating and pushing configuration commands to Layer 2 devices
C. Automatically dropping all suspected traffic at the nearest firewall
D. Automatically dropping all suspected traffic at the nearest IPS appliance

Answer: B

QUESTION 53:

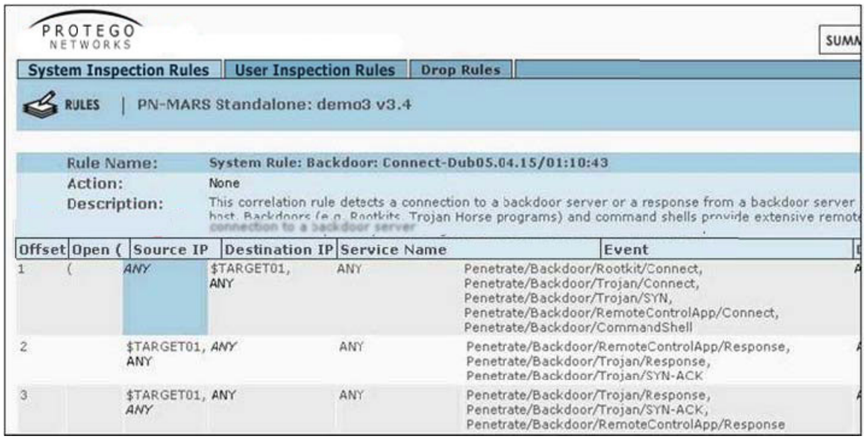
What will happen if you try to run a MARS query that will take a long time to complete?

A. After submitting the query, the MARS GUI screen will be locked up until the query completes.
B. The query will be automatically saved as a rule.
C. The query will be automatically saved as a report.
D. You will be prompted to "Submit Batch" to run the query in batch mode.
E. You will be prompted to "Submit Inline" to run the query immediately.

Answer: D

QUESTION 54:

Exhibit:



Rule Name: System Rule: Backdoor: Connect-Dub05.04.15/01:10:43
Action: None
Description: This correlation rule detects a connection to a backdoor server or a response from a backdoor server host. Backdoors (e.g. Rootkits, Trojan Horse programs) and command shells provide extensive remote connection to a backdoor server

Offset	Open (	Source IP	Destination IP	Service Name	Event
1	(	ANY	$TARGET01, ANY	ANY	Penetrate/Backdoor/Rootkit/Connect, Penetrate/Backdoor/Trojan/Connect, Penetrate/Backdoor/Trojan/SYN, Penetrate/Backdoor/RemoteControlApp/Connect, Penetrate/Backdoor/CommandShell
2		$TARGET01, ANY	ANY	ANY	Penetrate/Backdoor/RemoteControlApp/Response, Penetrate/Backdoor/Trojan/Response, Penetrate/Backdoor/Trojan/SYN-ACK
3		$TARGET01, ANY	ANY	ANY	Penetrate/Backdoor/Trojan/Response, Penetrate/Backdoor/Trojan/SYN-ACK, Penetrate/Backdoor/RemoteControlApp/Response

Referring to the rule shown in the MARS GUI screen, which two of the following statements are correct? Select two.

A. This rule will fire if the offset 1 condition occurs "OR" if the offset 2 condition occurs.
B. This rule will fire if the offset 3 condition occurs.
C. The expressions between cells are "AND" while expressions between items in the same cell are "OR".
D. This is a user-defined rule.
E. This rule can be deleted after changing its status to "inactive"

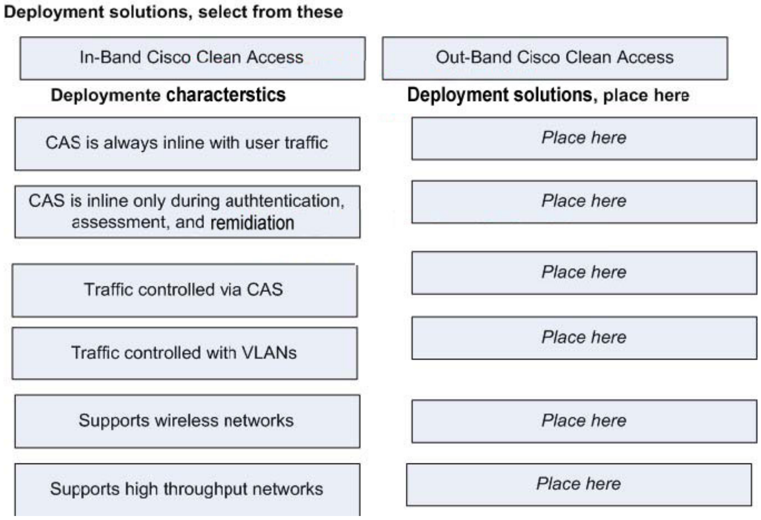
Answer: C, D

Explanation:
Expression between cells:
ASFE Course Notes pg 3-239
Rule logic is simple. You have a row. Every row has cells. The logical expressions

connecting different cells are "AND", while the expressions connecting items inside a cell are either "OR" or "AND NOT", depending which clause is chosen - the EQUAL TO or NOT EQUAL to.
User Defined Rule:
ASFE Course Notes pg 3-246
System rules can be copied and then become user rules that are fully editable.
When a system rule is copied the MARS system adds the date and time the rule was copied to the end of the rule name.

QUESTION 55:

DRAG DROP
You work as a network technician at Certkiller .com. You must match the appropriate deployment charecteristcs with the deployment solution.

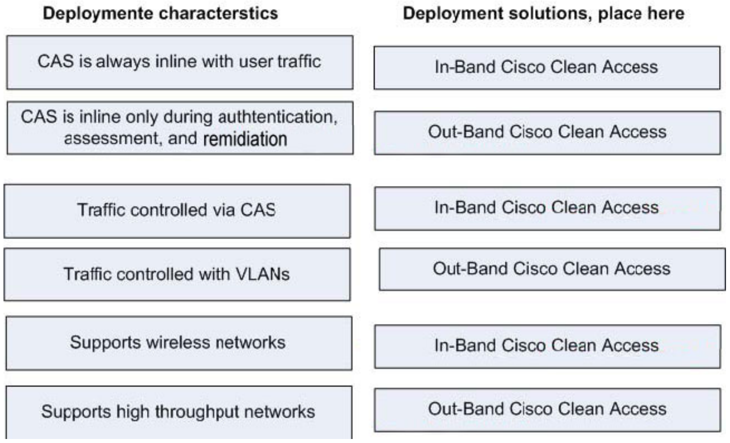


Deployment solutions, select from these

In-Band Cisco Clean Access
Out-Band Cisco Clean Access

Deploymente characterstics	Deployment solutions, place here
CAS is always inline with user traffic	Place here
CAS is inline only during authtentication, assessment, and remidiation	Place here
Traffic controlled via CAS	Place here
Traffic controlled with VLANs	Place here
Supports wireless networks	Place here
Supports high throughput networks	Place here

Answer:



Deploymente characterstics	Deployment solutions, place here
CAS is always inline with user traffic	In-Band Cisco Clean Access
CAS is inline only during authtentication, assessment, and remidiation	Out-Band Cisco Clean Access
Traffic controlled via CAS	In-Band Cisco Clean Access
Traffic controlled with VLANs	Out-Band Cisco Clean Access
Supports wireless networks	In-Band Cisco Clean Access
Supports high throughput networks	Out-Band Cisco Clean Access

QUESTION 56:

Refer to the partial output sample from a Cisco Trust Agent (CTA) ctad.ini configuration file. Which of the following is true based on the values shown?

[ServerCertDNVerification]TotalRules=2Rule1=CN*"server", ISSUER-CN*"Finance"Rule2=CN="Finance posture Cert", OU*"Finance", ISSUER-CN*" Certkiller "

A. Both Rule1 and Rule2 must be matched to allow the connection.
B. If either rule accepts the certificate, then the connection is permitted.
C. The issuer common name field in the Rule1 certificate must match "FINANCE" exactly.
D. The organizational unit in the certificate must match "Finance" exactly.
E. Certificates must be issued from both "Finance" and " Certkiller " to pass security posture validation.
F. Connections will not be permitted without the addition of a Distinguished Name (DN) field variable.

Answer: B

QUESTION 57:

Which of the following statements is correct regarding Cisco Clean Access (CCA) network scanning?

A. A default set of the available network scan plug-ins is loaded in the CAM at the factory.
B. The Cisco recommended list of plug-ins is selected by default.
C. Network scanning is performed on Windows-based operating systems only.
D. Network scanning is configurable by User Role.

Answer: D

QUESTION 58:

Which command can you use to verify operation between a Network Admission Control (NAC) agent and a Network Access Device (NAD)?

A. show eapoupd all
B. show eou all
C. show nac all
D. show nac access-list all

Answer: B

QUESTION 59:

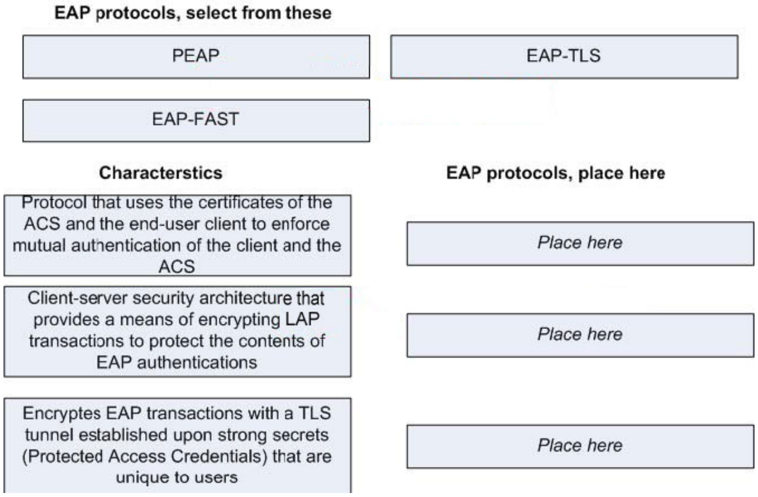
The MARS Appliance (running release 3.4.1) supports which protocol for data archiving and restoring?

A. NFS
B. TFTP
C. FTP
D. secured FTP

Answer: A

QUESTION 60:

DRAG DROP
You work as a network technician at Certkiller .com. Your Certkiller trainee Sandra is interested EAP protocols. You must match the protocol with the appropriate characteristics.



EAP protocols, select from these

PEAP

EAP-TLS

EAP-FAST

Characterstics

Protocol that uses the certificates of the ACS and the end-user client to enforce mutual authentication of the client and the ACS

Client-server security architecture that provides a means of encrypting LAP transactions to protect the contents of EAP authentications

Encrypts EAP transactions with a TLS tunnel established upon strong secrets (Protected Access Credentials) that are unique to users

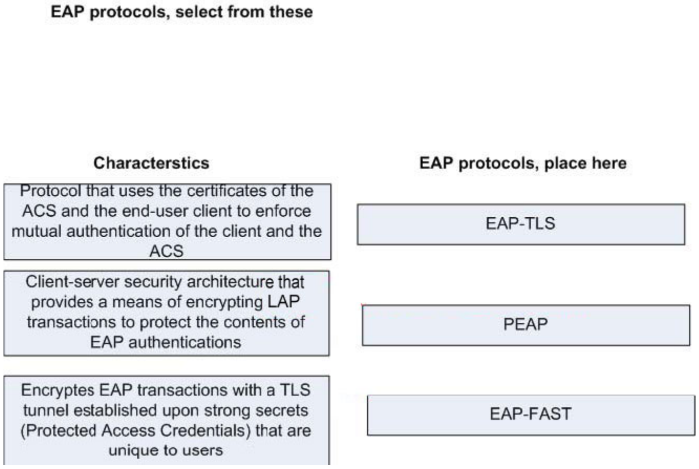
EAP protocols, place here

Place here

Place here

Place here

Answer:



EAP protocols, select from these

Characterstics

Protocol that uses the certificates of the ACS and the end-user client to enforce mutual authentication of the client and the ACS

Client-server security architecture that provides a means of encrypting LAP transactions to protect the contents of EAP authentications

Encrypts EAP transactions with a TLS tunnel established upon strong secrets (Protected Access Credentials) that are unique to users

EAP protocols, place here

EAP-TLS

PEAP

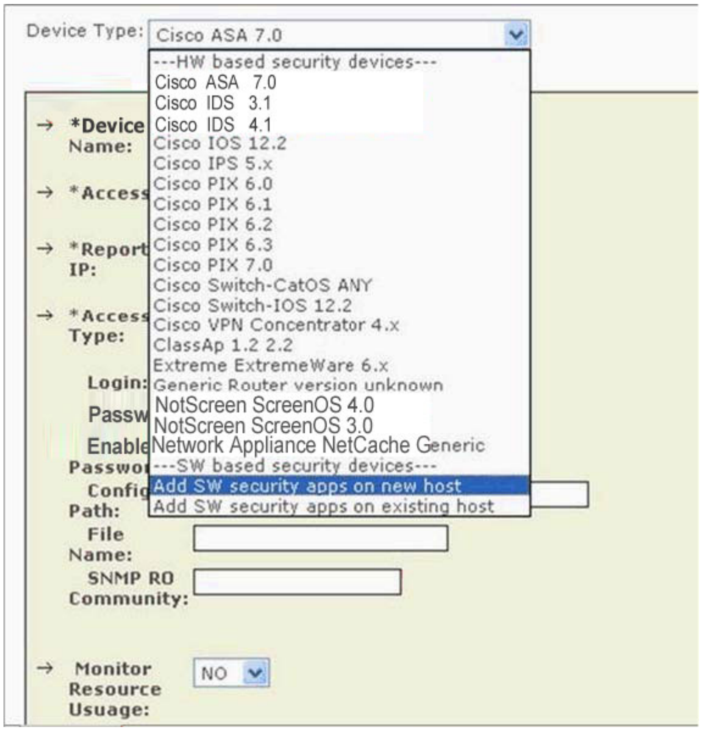
EAP-FAST

Explanation: EAP-TLS:
http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a00800b
EAP Transport Layer Security (TLS) (RFC2716) is a Microsoft-supported EAP

authentication algorithm based on the
TLS protocol (RFC2246). TLS is the current version of Secure Socket Layer (SSL) used
in most Web browsers for
secure Web application transactions.
PEAP:
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item0900aecd801764fa.shtml
PEAP works in two phases:
IN phase I,server-side TLS aurhentication is performed to create an encrypted tunnel
and achieve server-side authentication
in a manner similar to Web server authentication using Secure Sockets Layer (SSL), a
popular and trusted security method. Once
Phase 1 of PEAP is established, all data is encrypted, including all user-sensitive
information.
The framework for PEAP phase 2 Authenticationis extensible,and the client can be
authenticated using methods such as
EAP-GTC and Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2
within the TLS tunnel.
EAP-FAST :
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml
Cisco developed EAP-FAST to support customers who cannot enforce a strong password
policy and wish to deploy
an 802.1X EAP type that does not require digital certificates, supports a variety of user
and password database types, supports
password expiration and change, and is flexible, easy to deploy, and easy to manage. For
example, a customer using Cisco LEAP
who cannot enforce a strong password policy and does not want to use certificates can
migrate to EAP-FAST for protection from
dictionary attacks.
EAP-FAST uses symmetric key algorithms to achieve a tunneled authentication process.
The tunnel establishment relies on a
Protected Access Credential (PAC) that can be provisioned and managed dynamically by
EAP-FAST through the authentication,
authorization, and accounting (AAA) server.

QUESTION 61:

Exhibit:



Device Type: Cisco ASA 7.0

Monitor Resource Usage: NO

Which three of the following reporting devices can be added to the MARS appliance using the "Add SW security apps on new host"? Select three.

A. Cisco ACS
B. Netflow
C. SNORT
D. FWSM
E. Generic web server

Answer: A, C, E

Explanation: ASFE Course Notes pg 3-91, 3-137, 3-148

QUESTION 62:

Which browser plug-in is required to view the charts and graphs on the MARS Appliance?

A. Macromedia Flash Player
B. Sun Microsystems Java
C. Microsoft PowerPoint
D. Adobe SVG Viewer

Answer: D

Explanation: ASFE Course Notes pg 3-172

To see diagrams you need the Adobe SVG viewer plug-in. The Adobe SVG viewer plug-in should automatically install.

QUESTION 63:

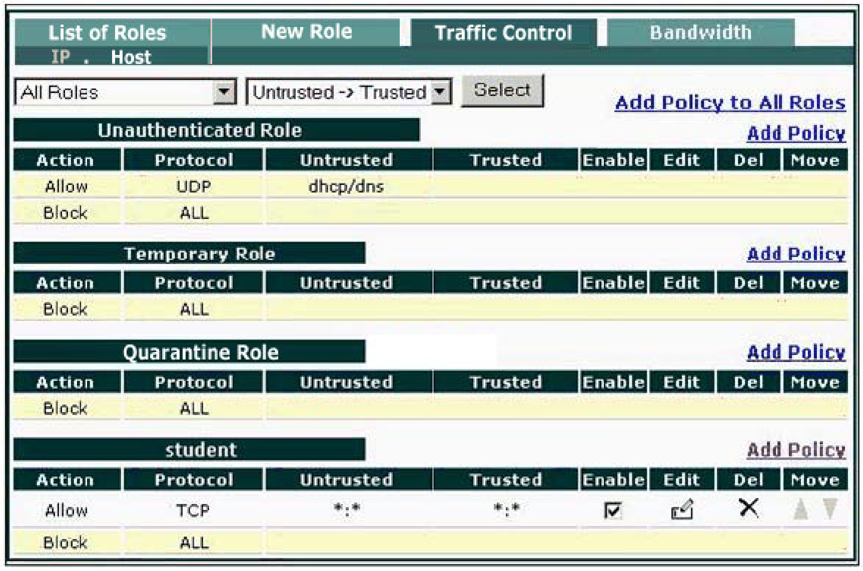
What are three benefits in deploying MARS Appliances using the Global and Local Controllers' architecture? (Choose three.)

A. A Global Controller can provide a summary of all Local Controllers information (network topologies, incidents, queries, and reports result).
B. A Global Controller can provide a central point for creating rules and queries, which are applied to multiple Local Controllers simultaneously.
C. The architecture provides redundancy in case one of the MARS Local Controllers failed within a zone.
D. Users can seamlessly navigate to any Local Controllers from the Global Controller GUI.
E. A Global Controller can correlate events from multiple Local Controllers to perform global sessionizations.

Answer: A,B,D

QUESTION 64:

Refer to the exhibit. When new students attempt to access the college network, the Clean Access Agent (CCA) informs the students that their PCs violate the college security policy because they are missing some required files and software applications on their PCs. To grant students FTP access to the files and applications on an internal remediation server, the administrator must take which of the following courses of action?
Exhibit:



Unauthenticated Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	UDP	dhcp/dns					
Block	ALL						

Temporary Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Block	ALL						

Quarantine Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Block	ALL						

student

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*:*	*:*	☑	✎	✕	▲ ▼
Block	ALL						

A. Add to the Unauthenticated Role an allow policy for FTP access to the internal

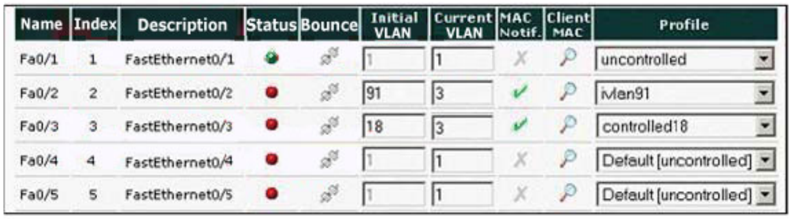
remediation server.
B. Add to the Temporary Role an allow policy for FTP access to the internal remediation server.
C. Add to the Quarantine Role an allow policy for FTP access to the internal remediation server.
D. Add to the Student Role an allow policy for FTP access to the internal remediation server.

Answer: B

Explanation: ASFE Course Notes pg 2-42
Temporary Role: This role is assigned to allow a user to download and install required packages. Full network access is denied till the requirements are met. If the requirements are met but the client is found to have vulnerabilities during the network scanning, then the client is transferred from the Temporary role to the Quarantine role, where the client is given network access to resources needed to fix the vulnerability.

QUESTION 65:

Refer to the exhibit. From a dropdown menu, profiles are applied to each managed port. Before a profile can be applied, where are the client access and authentication VLAN profile parameters configured?
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	✓	🔍	iMen91
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]

A. controlled VLAN profile
B. access control profile
C. port profile
D. User Role profile

Answer: C

Explanation:
ASFE Course Notes pg 2-173/191/207
The port profile determines whether a port is managed or unmanaged and which authentication and access vlan's to use when switching the client port. You will need to add a port profile for each set of authentication and access vlans that you configure on the switch.
When configuring switch ports, the profile column provides a drop down menu for each switch port and is used to assign the appropriate port profile to the port.

QUESTION 66:

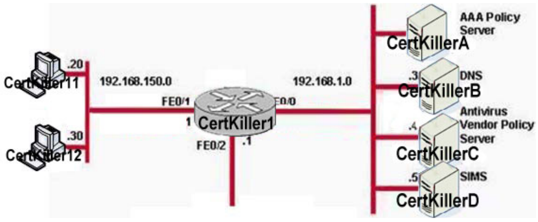
When configuring Cisco ACS users and groups, and the user configuration has an attribute configured differently from the same attribute in the group profile, what will the result be?

A. The user setting will override the group setting.
B. The group setting will be applied.
C. The specific user cannot be placed into a group to avoid conflicts.
D. A unique group must be configured and the user placed into that group.

Answer: A

QUESTION 67:

Refer to the exhibit. Network Admission Control (NAC) has been configured on router Certkiller1;however,end systems are not being properly validated for the correct security posture when accessing external networks. You have determined that the proper intercept ACL has not been applied. What would the correct intercept ACL and admission statement to apply be to correct this problem?
Exhibit:



A. access-list 199 permit ip any 192.168.1.0 0.0.0.255ip admission name bluemoon eapoudp list 199
B. access-list 10 permit upd any 192.168.150.0 0.0.0.255ip admission name nac1 eapoudp list 10
C. access-list 101 permit ip any 192.50.0.0 0.0.0.255 ip admission name greentree eapoudp list 101
D. access-list nac1 permit udp any anyip admission name nac1 eapoudp list 1

Answer: C

Explanation: ASFE Course Notes pg 1-124
The intercept ACL mirrors the interface ACL by denying traffic that was specifically permitted in the interface ACL and permitting traffic that was specifically denied in the interface ACL. Doing this subjects the specified traffic to the posture validation process. The Intercept ACL is not applied to a particular NAD interface, but instead applied to the NAC global policy.
In the Interface ACL one needs to deny EAPoUDP traffic to the NAD to enable the posture validation process to work, and sometimes also allow posture bypass for DNS & DHCP traffic. This permitted traffic should then be denied in the Intercept ACL.

If we assess the answers:
A) The syntax is correct, however we assume that we do not want to posture traffic to these servers as these are used for the posturing process and the question states external network.
B) This has 2 problems, First the ACL number is 10 which contradicts the syntax and secondly it is only looking at UDP traffic, we would want to posture all traffic.
C) The syntax is correct, however the diagram does not show us the IP address of the external network. If the external network IP range is 192.50.0.x then this is the correct answer. Without the external IP range information, by a process of elimination this is the most correct answer out of the options available.
D) The syntax for this ACL is incorrect for a named ACL.

QUESTION 68:

Which is a benefit of using the dollar variable (like $TARGET01) when creating queries in MARS?

A. The dollar variable enables multiple queries to reference the same common 5-tuples information using a variable.
B. The dollar variable ensures that the probes and attacks that are reported are happening to the same host.
C. The dollar variable allows matching of any unknown reporting device.
D. The dollar variable allows matching of any event type groups.
E. The dollar variable enables the same query to be applied to different reports.

Answer: B

QUESTION 69:

Exhibit:
After manually adding the Certkiller 1 device shown in the MARS GUI screen, what additional steps do you need to perform?

A. Click "Activate" to enable the device.
B. Click "Submit" to enable the device.
C. Click "Submit" to test access to the device. When access is successful, click "Activate" to activate the device.
D. Click "Activate" to activate the device, then click "Submit" to save the device configuration.
E. Click "Discover" to initiate manual discovery. When discovery is completed, click "Submit", then "Activate.

Answer: E

QUESTION 70:

Once you have installed the Cisco Trust Agent (CTA), you want to verify that the agent is operating properly and communicating with the antivirus policy server. Which could you do to verify that status?

A. Issue the show eou all command on the intermediate NAD device.
B. From the endpoint device, ping the AV server. If this is successful, CTA is installed correctly.
C. If an "unhealthy user" pop-up window on the endpoint device is not displayed, the agent is working properly.
D. Check CTA activity logs for security posture validation messages.

Answer: A