# Free Sep-2023 UPDATED Cisco 350-701 Certification Exam Dumps is Online [Q181-Q202


**Free Sep-2023 UPDATED Cisco 350-701 Certification Exam Dumps is Online Cisco Exam 2023 350-701 Dumps Updated Questions**

Cisco 350-701: Implementing and Operating Cisco Security Core Technologies is an exam that tests the knowledge and skills of IT professionals in implementing and operating Cisco security solutions. 350-701 exam is designed to evaluate the ability of candidates to secure network infrastructure, identify and mitigate security threats, and maintain the confidentiality, integrity, and availability of data. 350-701 exam is a part of the CCNP Security certification program and is a requirement to earn the certification.

The Cisco 350-701 exam covers a wide range of topics related to core security technologies such as network security, cloud security, endpoint protection, secure network access, visibility, and automation. 350-701 exam also covers advanced security concepts and best practices for implementing and managing secure solutions.

**NO.181** What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?
* posture assessment
* CoA
* external identity source
* SNMP probe

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.

One of the settings to configure the CoA type is “Reauth”. This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.

One of the settings to configure the CoA type is “Reauth”. This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.

One of the settings to configure the CoA type is “Reauth”. This option is used to enforce reauthentication of an already authenticated endpoint when it is profiled.

Reference:

b_ise_admin_guide_sample_chapter_010101.html

b_ise_admin_guide_sample_chapter_010101.html

**NO.182** An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and dat a. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?
* Virtual routing and forwarding
* Microsegmentation
* Access control policy
* Virtual LAN

Zero Trust is a security framework requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

The Zero Trust model uses microsegmentation – a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network – to contain attacks.

**NO.183** Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)
* Patch for cross-site scripting.
* Perform backups to the private cloud.

* Protect against input validation and character escapes in the endpoint.
* Install a spam and virus email filter.
* Protect systems with an up-to-date antimalware program

Explanation : Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim’s machine.

**NO.184** What is a key difference between Cisco Firepower and Cisco ASA?

* Cisco ASA provides access control while Cisco Firepower does not.
* Cisco Firepower provides identity-based access control while Cisco ASA does not.
* Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.
* Cisco ASA provides SSL inspection while Cisco Firepower does not.

Explanation

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-firepowerservices/200451-Configure-Intrusion-

**NO.185** Refer to the exhibit. How does Cisco Umbrella manage traffic that is directed toward risky domains?

* Traffic is managed by the application settings, unhandled and allowed
* Traffic is allowed but logged
* Traffic is managed by the security settings and blocked.
* Traffic is proxied through the intelligent proxy

**NO.186** What is an advantage of network telemetry over SNMP pulls?

* accuracy
* encapsulation
* security
* scalability

**NO.187** What is managed by Cisco Security Manager?

* WSA
* ASA
* access point O
* ESA

https://www.cisco.com/c/en/us/products/collateral/security/security-manager/datasheet-C78-737182.html

**NO.188** An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

* Cisco Defense Orchestrator
* Cisco Secureworks
* Cisco DNA Center
* Cisco Configuration Professional

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.

Cisco Defense Orchestrator features:

….

Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.

Cisco Defense Orchestrator features:

….

Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.

Reference:

736847.html

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.

Cisco Defense Orchestrator features:

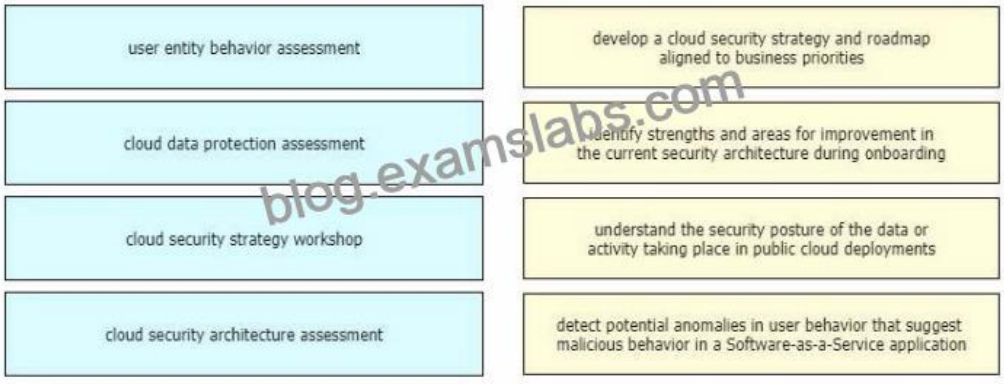
….

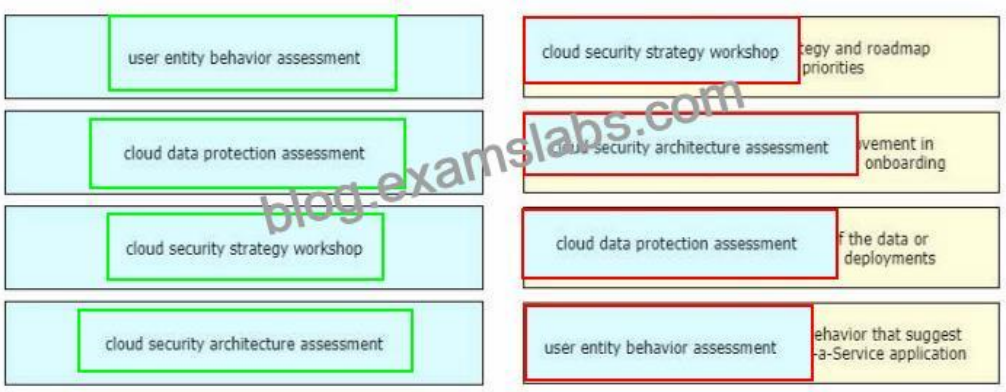
Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.

736847.html

**NO.189** What is a key difference between Cisco Firepower and Cisco ASA?
* Cisco ASA provides access control while Cisco Firepower does not.
* Cisco Firepower provides identity-based access control while Cisco ASA does not.
* Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.
* Cisco ASA provides SSL inspection while Cisco Firepower does not.
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-firepowerservices/200451-Configure-Intrusion-Policy-and-Signature.html

**NO.190** Drag and drop the cloud security assessment components from the left onto the definitions on the right.







**NO.191** Which type of dashboard does Cisco DNA Center provide for complete control of the network?
* service management
* centralized management
* application management
* distributed management

Cisco’s DNA Center is the only centralized network management system to bring all of this functionality into a single pane of glass.

Reference:

dna-center-faq-cte-en.html

**NO.192** How is Cisco Umbrella configured to log only security events?
* per policy
* in the Reporting settings
* in the Security Settings section
* per network in the Deployments section

The logging of your identities’ activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs. From the Policy wizard, log settings are: Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don’t Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on. Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management From the Policy wizard, log settings are:

Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don’t Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on.

The logging of your identities’ activities is set per-policy when you first create a policy. By default, logging is on and set to log all requests an identity makes to reach destinations. At any time after you create a policy, you can change what level of identity activity Umbrella logs. From the Policy wizard, log settings are: Log All Requests-For full logging, whether for content, security or otherwise Log Only Security Events-For security logging only, which gives your users more privacy-a good setting for people with the roaming client installed on personal devices Don’t Log Any Requests-Disables all logging. If you select this option, most reporting for identities with this policy will not be helpful as nothing is logged to report on. Reference:

https://docs.umbrella.com/deployment-umbrella/docs/log-management

**NO.193** An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization’s public cloud to send telemetry using the cloud provider’s mechanisms to a security device. Which mechanism should the engineer configure to accomplish this goal?
* mirror port
* NetFlow
* Flow
* VPC flow logs
Reference:

https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/q-and-a-c67-737402.html

**NO.194** A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment Which tool should be used to accomplish this goal?
* Security Manager
* Cloudlock
* Web Security Appliance
* Cisco ISE
Reference:

https://www.cisco.com/c/dam/en/us/products/collateral/security/cloudlock/cisco-cloudlock-cloud-data-securitydatasheet.pdf

**NO.195** Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?
* file access from a different user
* interesting file access
* user login suspicious behavior
* privilege escalation
The various suspicious patterns for which the Cisco Tetration platform looks in the current release are: + Shell code execution: Looks for the patterns used by shell code. + Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree. + Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks. + Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping). + User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods. + Interesting file access: Cisco Tetration platform can be armed to look at sensitive files. + File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user. + Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

+ Shell code execution: Looks for the patterns used by shell code.

+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.

+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts.

Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.

+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).

+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.

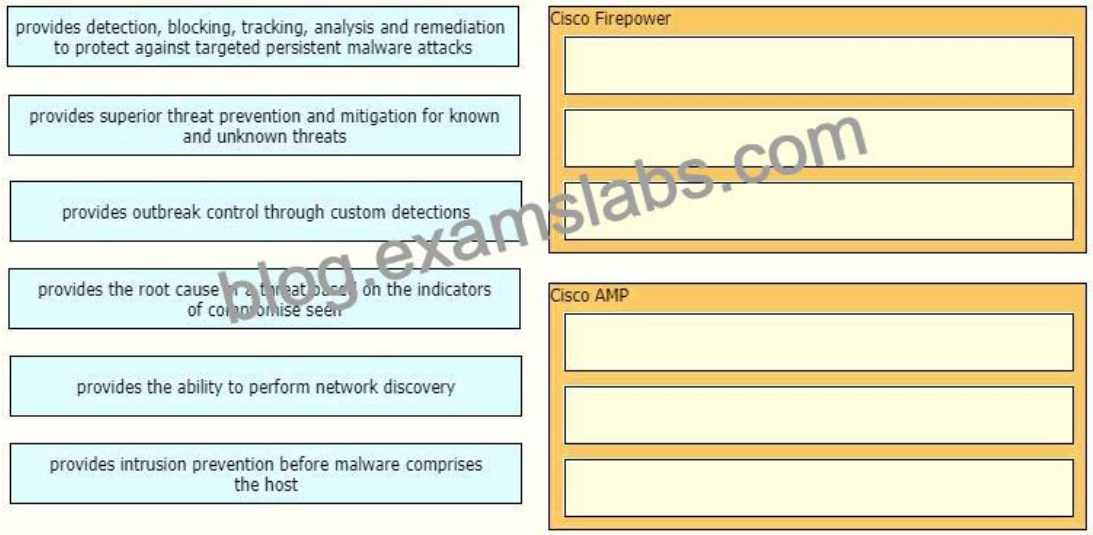
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.

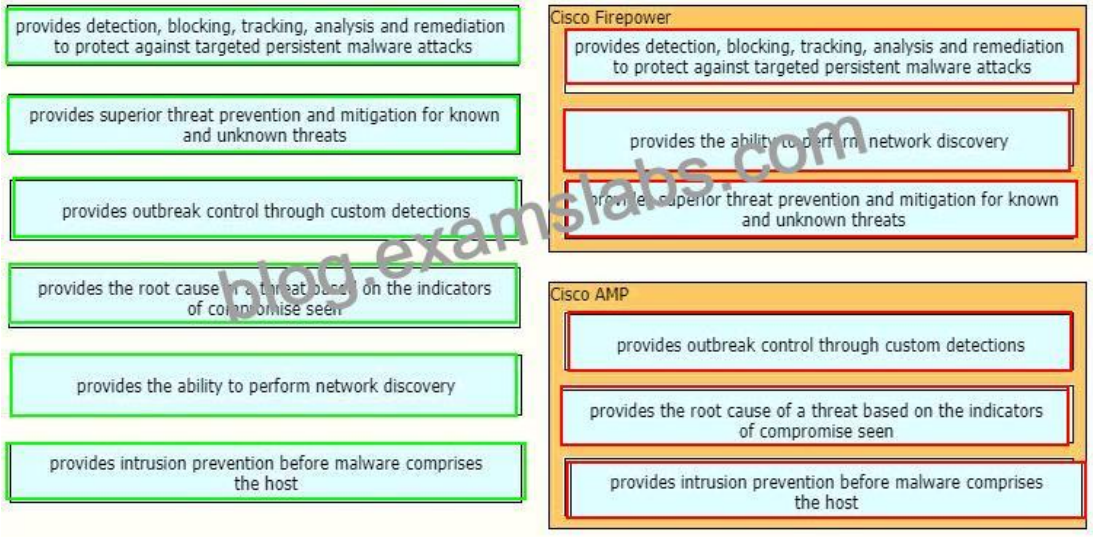
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.

+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform.

The various suspicious patterns for which the Cisco Tetration platform looks in the current release are: + Shell code execution: Looks for the patterns used by shell code. + Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree. + Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks. + Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping). + User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods. + Interesting file access: Cisco Tetration platform can be armed to look at sensitive files. + File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user. + Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

**NO.196** Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.



https://www.cisco.com/c/en/us/products/collateral/security/ngips/datasheet-c78-742472.html

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html

**NO.197** A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

* Use MAB with profiling
* Use MAB with posture assessment.
* Use 802.1X with posture assessment.
* Use 802.1X with profiling.

Explanation Explanation As the new device does not have a supplicant, we cannot use 802.1X. MAC Authentication Bypass (MAB) is a fallback option for devices that don’t support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device’s MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x. Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles. Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone. Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456 Explanation As the new device does not have a supplicant, we cannot use 802.1X.

MAC Authentication Bypass (MAB) is a fallback option for devices that don’t support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device’s MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x.

Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles.

Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing

the network from their personal iPhone.

Explanation Explanation As the new device does not have a supplicant, we cannot use 802.1X. MAC Authentication Bypass (MAB) is a fallback option for devices that don’t support 802.1x. It is virtually always used in deployments in some way shape or form. MAB works by having the authenticator take the connecting device’s MAC address and send it to the authentication server as its username and password. The authentication server will check its policies and send back an Access-Accept or Access-Reject just like it would with 802.1x. Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Chromebooks, and so on), desktop operating systems (for example, Windows, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles. Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone. Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456

**NO.198** An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?
* single interface
* multi-context
* transparent
* two-interface

**NO.199** A network engineer is configuring DMVPN and entered the crypto is akmp key cisc0380739941 address

0.0.0.0 command on host A The tunnel is not being established to host B. What action is needed to authenticate the VPN?
* Enter the same command on host B.
* Enter the command with a different password on host B.
* Change isakmp to ikev2 in the command on host A.
* Change the password on host A to the default password.

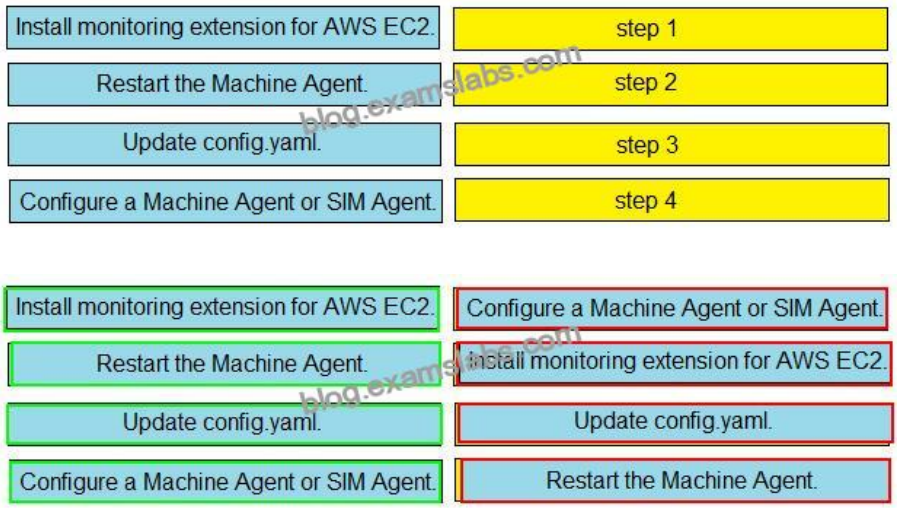
**NO.200** What is the primary role of the Cisco Email Security Appliance?
* Mail Submission Agent
* Mail Transfer Agent
* Mail Delivery Agent
* Mail User Agent

Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. Cisco ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay.

Reference:

Cisco_SBA_BN_EmailSecurityUsingCiscoESADeploymentGuide-Feb2013.pdf

**NO.201** Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.




**NO.202** An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?

* monitor
* allow
* block
* trust

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/access_control_using_intrusion_and_file_policies.html#:~:text=File%20Policies-,Access%20Control%20Traffic%20Handling%20with%20Intrusion%20and%20File%20Policies,-The%20following%20diagram the first three access control rules in the policy-Monitor, Trust, and Block-cannot inspect matching traffic. Monitor rules track and log but do not inspect network traffic, so the system continues to match traffic against additional rules to determine whether to permit or deny it

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/access_control_rules.html#:~:text=Rule%20Blocking%20Actions-,Access%20Control%20Rule%20Allow%20Action,network%20discovery%20policy%3B%20additionally%2C%20application%20discovery%20is%20limited%20for%20encrypted%20sessions.,-Related%20Concepts

**Cisco Certified 350-701 Dumps Questions Valid 350-701 Materials:**
https://www.examslabs.com/Cisco/CCNPSecurity/best-350-701-exam-dumps.html]