Cisco.350-701.v2021-01-29.q74

Exam Code:	350-701
Exam Name:	Implementing and Operating Cisco Security Core Technologies
Certification Provider:	Cisco
Free Question Number:	74
Version:	v2021-01-29
# of views:	1736
# of Questions views:	71669
https://www.freecram.net/torrent/Cisco.350-701.v2021-01-29.q74.html	

NEW QUESTION: 1

Refer to the exhibit.

What is a result of the configuration?

A. Traffic from the DMZ network is redirected

B. Traffic from the inside network is redirected

C. All TCP traffic is redirected

D. Traffic from the inside and DMZ networks is redirected

Answer: (SHOW ANSWER)

NEW QUESTION: 2

What is the purpose of the My Devices Portal in a Cisco ISE environment?

A. to manage and deploy antivirus definitions and patches on systems owned by the end user

B. to register new laptops and mobile devices

C. to provision userless and agentless systems
D. to request a newly provisioned mobile device
Answer: (SHOW ANSWER)
Explanation

Employees can use the My Devices portal to register and manage their personal devices. The My Devices portal includes online help that provides

NEW QUESTION: 3
In which two ways does a system administrator send web traffic transparently to the Web Security Appliance? (Choose two.)
A. use Web Cache Communication Protocol
B. configure policy-based routing on the network infrastructure
C. configure the proxy IP address in the web-browser settings
D. reference a Proxy Auto Config file
E. configure Active Directory Group Policies to push proxy settings
Answer: (SHOW ANSWER)

NEW QUESTION: 4
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?
A. Security Category Blocking
B. Application Control
C. File Analysis
D. Content Category Blocking
Answer: (SHOW ANSWER)

NEW QUESTION: 5
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?
A. LDAP injection
B. cross-site scripting
C. man-in-the-middle
D. insecure API
Answer: (SHOW ANSWER)
Explanation

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

NEW QUESTION: 6
What features does Cisco FTDv provide over ASAv?
A. Cisco FTDv runs on VMWare while ASAv does not

B. Cisco FTDv supports URL filtering while ASAv does not
C. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
D. Cisco FTDv runs on AWS while ASAv does not
Answer: (SHOW ANSWER)

NEW QUESTION: 7
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?
A. It provides stateless IP flow tracking that exports all records of a specific flow
B. It tracks the flow continuously and provides updates every 10 seconds.
C. It tracks flow-create, flow-teardown, and flow-denied events
D. Its events match all traffic classes in parallel.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?
A. interpacket variation
B. software package variation
C. process details variation
D. flow insight variation
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?
A. PSIRT
B. DEVNET
C. CSIRT
D. Talos
Answer: (SHOW ANSWER)
Explanation
https://talosintelligence.com/

NEW QUESTION: 10
A user has a device in the network that is receiving too many connection requests from multiple machines.
Which type of attack is the device undergoing?

A. SYN flood
B. slowloris
C. pharming
D. phishing

Answer: (SHOW ANSWER)
Explanation
https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html#~types-of-ddos-attacks

NEW QUESTION: 11
When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?
A. Common Vulnerabilities and Exposures
B. Common Exploits and Vulnerabilities
C. Common Security Exploits
D. Common Vulnerabilities, Exploits and Threats
Answer: (SHOW ANSWER)
Explanation
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cve/174/cve-addressed-1741.html

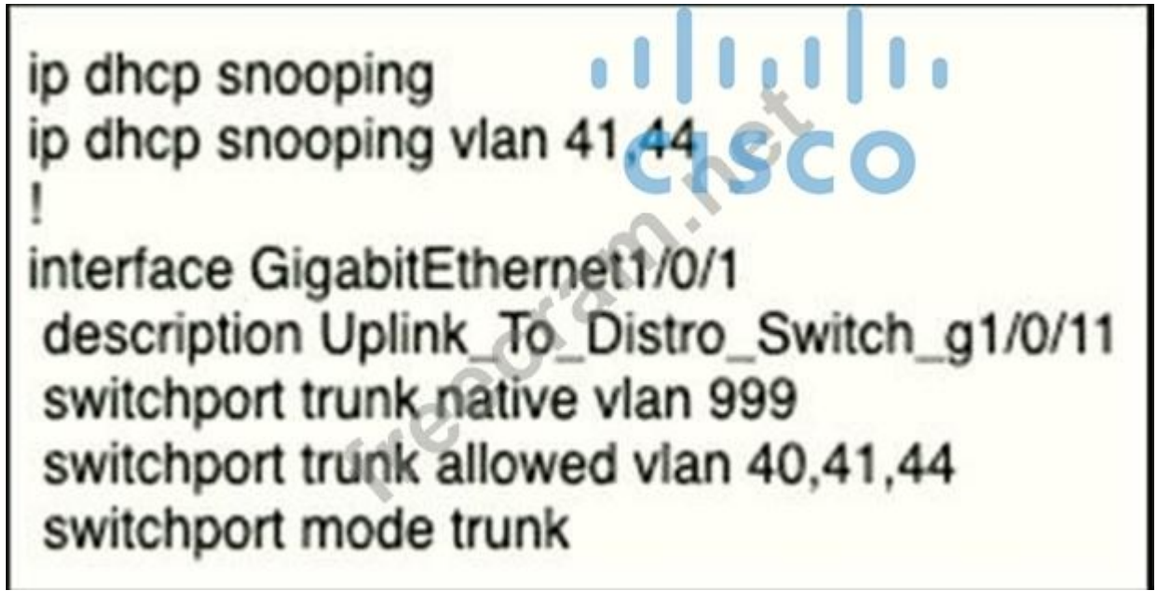
NEW QUESTION: 12
Which VPN technology can support a multivendor environment and secure traffic between sites?
A. SSL VPN
B. GET VPN
C. FlexVPN
D. DMVPN
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?
A. NGIPS
B. Cisco Firepower
C. Cisco Umbrella
D. Cisco Stealthwatch
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?
A. Firepower Threat Defense
B. Platform Exchange Grid
C. Multifactor Platform Integration
D. Advanced Malware Protection
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which two key and block sizes are valid for AES? (Choose two.)
A. 192-bit block size, 256-bit key length
B. 128-bit block size, 192-bit key length
C. 64-bit block size, 112-bit key length
D. 128-bit block size, 256-bit key length
E. 64-bit block size, 168-bit key length
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Refer to the exhibit.



An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?
A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust
Answer: (SHOW ANSWER)
Explanation
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp

NEW QUESTION: 17
What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an organization? (Choose two.)
A. single sign-on access to on-premises and cloud applications
B. identification and correction of application vulnerabilities before allowing access to resources
C. integration with 802.1x security using native Microsoft Windows supplicant
D. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes. and push notifications
E. secure access to on-premises and cloud applications
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two.)
A. SSL
B. SIP
C. inline normalization
D. modbus
E. packet decoder
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)
A. Protect systems with an up-to-date antimalware program
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Patch for cross-site scripting
E. Install a spam and virus email filter
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

A. auth-type all
B. ip device-tracking
C. aaa server radius dynamic-author
D. aaa new-model
Answer: (SHOW ANSWER)

NEW QUESTION: 21
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?
A. It decrypts HTTPS application traffic for authenticated users.
B. It provides enhanced HTTPS application detection for AsyncOS.
C. It decrypts HTTPS application traffic for unauthenticated users
D. It alerts users when the WSA decrypts their traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?
A. Use Bounce Verification
B. Configure incoming content filters.
C. Bypass LDAP access queries in the recipient access table.
D. Configure Directory Harvest Attack Prevention
Answer: (SHOW ANSWER)
Explanation

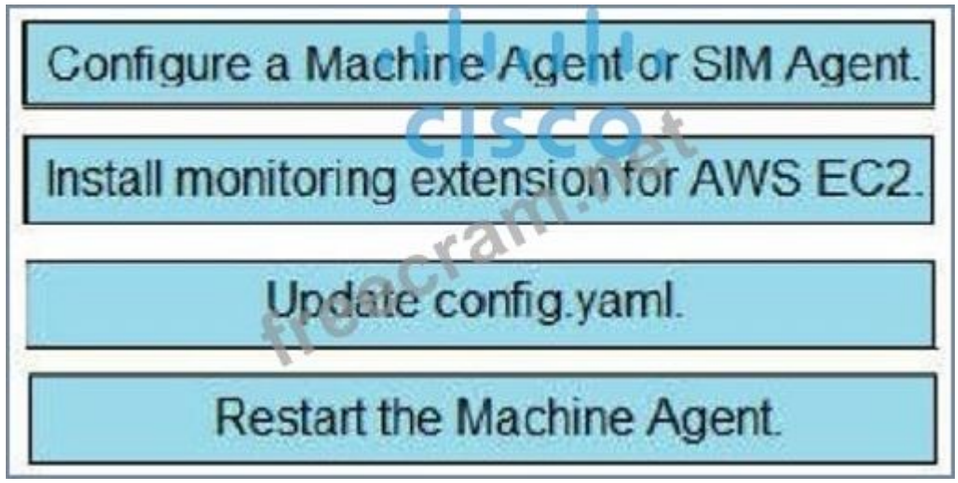
How do you create an LDAP group query on the ESA?

1. Create an LDAP group query under System Administration > LDAP.
2. Enable the group query for the listener under Network > Listener > {select the listener} > select the LDAP group query.
3. Go to Incoming Mail Policies.
4. Create a new policy for the group.
5. Add in the recipient matching the group.
6. Choose LDAP group query instead of email.
7. Select group query and put in the matching group name.
8. Configure new incoming mail policies. Anti-Spam, Anti-Virus, Content Filters, and Virus Outbreak Filters.

NEW QUESTION: 23
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.

Answer:

Explanation



NEW QUESTION: 24

What is the benefit of installing Cisco AMP for Endpoints on a network?

A. It provides operating system patches on the endpoints for security.

B. It provides flow-based visibility for the endpoints' network connections.

C. It protects endpoint systems through application control and real-time scanning.

D. It enables behavioral analysis to be used for the endpoints.

Answer: (SHOW ANSWER)

Explanation

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/at-a-glance

NEW QUESTION: 25

The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

A. management console and the SDN controller

B. management console and the cloud

C. SDN controller and the cloud

D. SDN controller and the management solution

Answer: (SHOW ANSWER)

NEW QUESTION: 26

What are the two types of managed Intercloud Fabric deployment models? (Choose two.)

A. Public managed

B. Service Provider managed

C. Enterprise managed

D. User managed

E. Hybrid managed

Answer: (SHOW ANSWER)

Explanation

The Cisco Intercloud Fabric architecture provides two product configurations to address the following two consumption models:

- Cisco Intercloud Fabric for Business
- Cisco Intercloud Fabric for Providers

NEW QUESTION: 27

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))

response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

What does the API do when connected to a Cisco security appliance?

A. get the process and PID information from the computers in the network

B. create an SNMP pull mechanism for managing AMP

C. gather the network interface information about the computers AMP sees

D. gather network telemetry information from AMP for endpoints

Answer: (SHOW ANSWER)

NEW QUESTION: 28

Refer to the exhibit.

```
def add_device_to_dnac(dnac_ip, device_ip, snmp_version,
    snmp_ro_community, snmp_rw_community,
    snmp_retry, snmp_timeout,
    cli_transport, username, password, enable_password):
    device_object = {
        'ipAddress': [
            device_ip
        ],
       'type': 'NETWORK_DEVICE',
        'computeDevice': False,
        'snmpVersion': snmp_version,
        'snmpROCommunity': snmp_ro_community,
        'snmpRWCommunity': snmp_rw_community,
        'snmpRetry': snmp_retry,
        'snmpTimeout': snmp_timeout,
        'cliTransport': cli_transport,
        'userName': username,
        'password': password,
        'enablePassword': enable_password
    }
    response = requests.post(
        'https://{}/dna/intent/api/v1/network-
device'.format(dnac_ip),
        data=json.dumps(device_object),
        headers={
            'X-Auth-Token': '{}'.format(token),
       "     'Content-type': 'application/json'
        },
        verify=False
    )
    return response.json()
```

What is the result of this Python script of the Cisco DNA Center API?

A. receives information about a switch

B. adds authentication to a switch

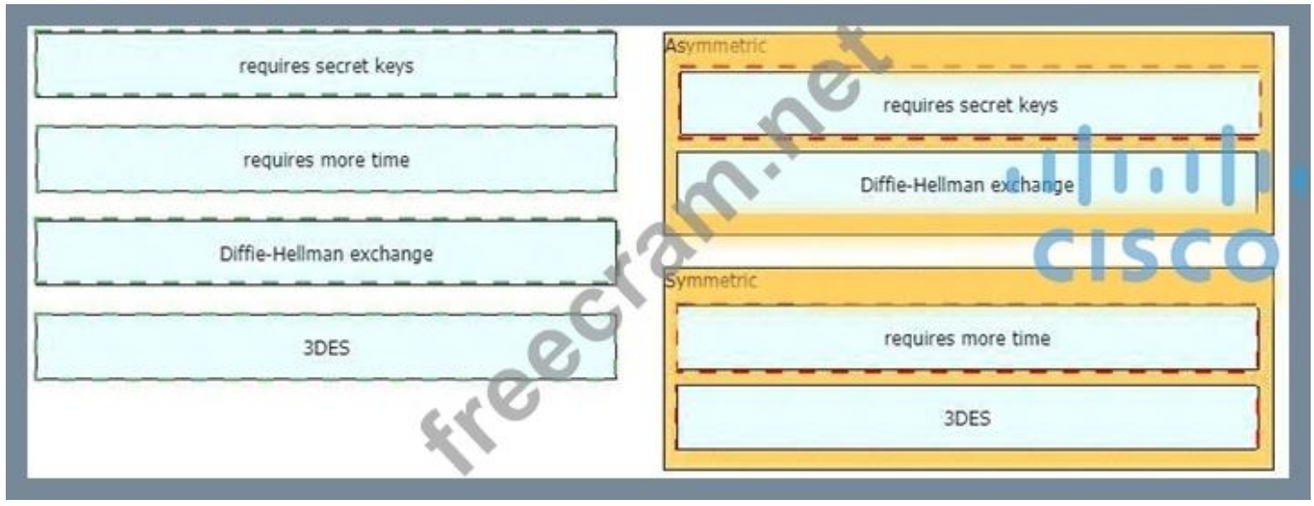
C. adds a switch to Cisco DNA Center

Answer: (SHOW ANSWER)

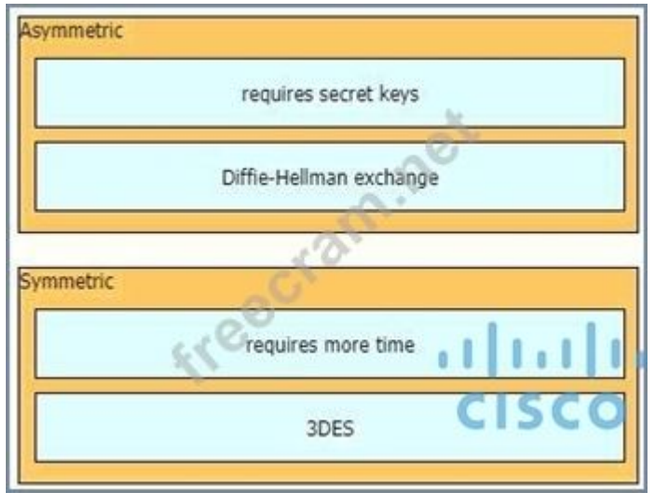
NEW QUESTION: 29

Drag and drop the descriptions from the left onto the encryption algorithms on the right.

Answer:



Explanation



NEW QUESTION: 30

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware?
(Choose two).

A. DLP

B. Sophos engine
C. outbreak filters
D. RAT
E. white list
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which two request of REST API are valid on the Cisco ASA Platform? (Choose two.)
A. Get
B. Connect
C. Put
D. Option
E. Push
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?
A. AnyConnect
B. Talos
C. AMP
D. DynDNS
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Refer to the exhibit.

```
snmp-server group SNMP v3 auth access 15
```

What does the number 15 represent in this configuration?
A. access list that identifies the SNMP devices that can access the router
B. interval in seconds between SNMPv3 authentication attempts
C. number of possible failed attempts until the SNMPv3 user is locked out
D. privilege level for an authorized user to this router
Answer: (SHOW ANSWER)

NEW QUESTION: 34
How is DNS tunneling used to exfiltrate data out of a corporate network?
A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
B. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.
C. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.
D. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
Answer: (SHOW ANSWER)

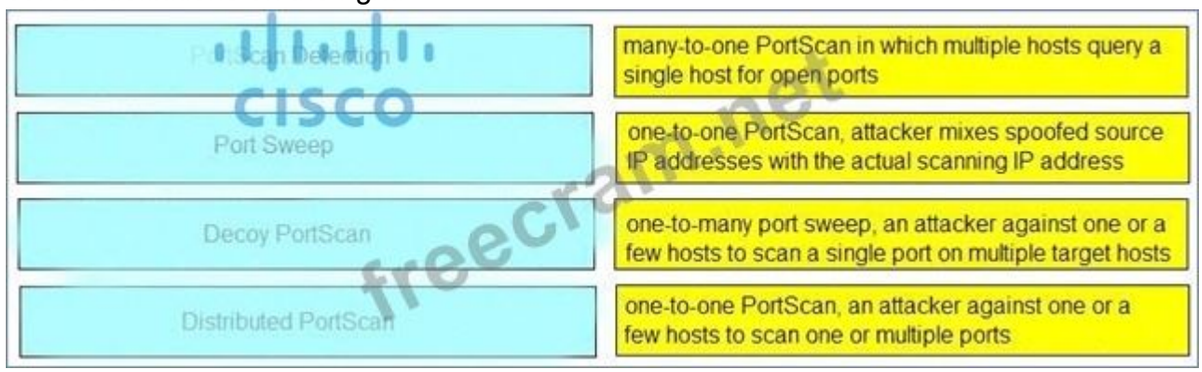
NEW QUESTION: 35
Which algorithm provides encryption and authentication for data plane communication?
A. AES-GCM
B. SHA-384
C. SHA-96
D. AES-256
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?
A. transparent
B. forward
C. redirection
D. proxy gateway
Answer: (SHOW ANSWER)

NEW QUESTION: 37
An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used.
However, the connection is failing. Which action should be taken to accomplish this goal?
A. Configure the port using the ip ssh port 22 command.
B. Enable the SSH server using the ip ssh server command.
C. Disable telnet using the no ip telnet command.
D. Generate the RSA key using the crypto key generate rsa command.
Answer: (SHOW ANSWER)
Explanation
https://learningnetwork.cisco.com/s/question/0D53i00000KsrhK/rsa-key

NEW QUESTION: 38

Drag and drop the Firepower Next Generation Intrustion Prevention System detectors from the left onto the correct definitions on the right.



Answer:

Explanation

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/detecti

NEW QUESTION: 39

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

A. BAT
B. RAT
C. SAT
D. HAT
Answer: (SHOW ANSWER)

NEW QUESTION: 40
When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?

A. HSRP is used for fallover.
B. Traffic is distributed statically by default.
C. Multiple routers or VRFs are required.
D. Floating static routes are required.
Answer: (SHOW ANSWER)

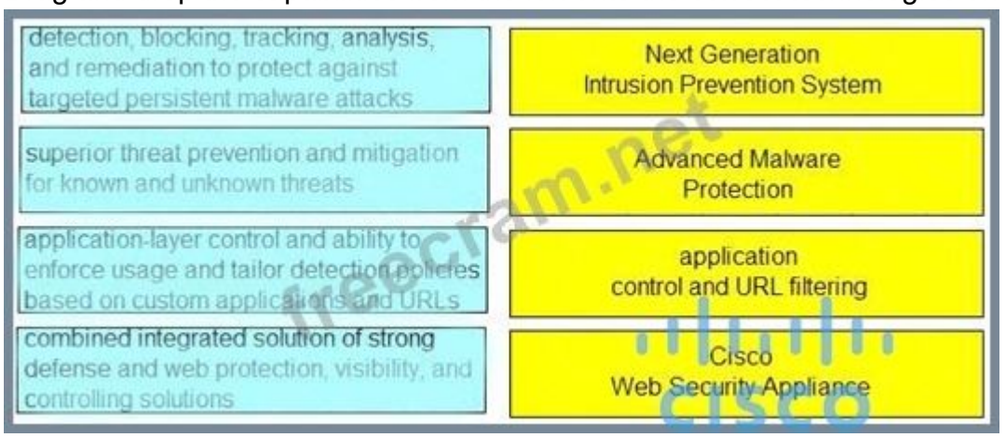
NEW QUESTION: 41
In which cloud services model is the tenant responsible for virtual machine OS patching?
A. UCaaS
B. SaaS
C. IaaS
D. PaaS
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two.)
A. eavesdropping
B. ARP spoofing
C. denial-of-service attacks
D. exploits
E. malware
Answer: (SHOW ANSWER)

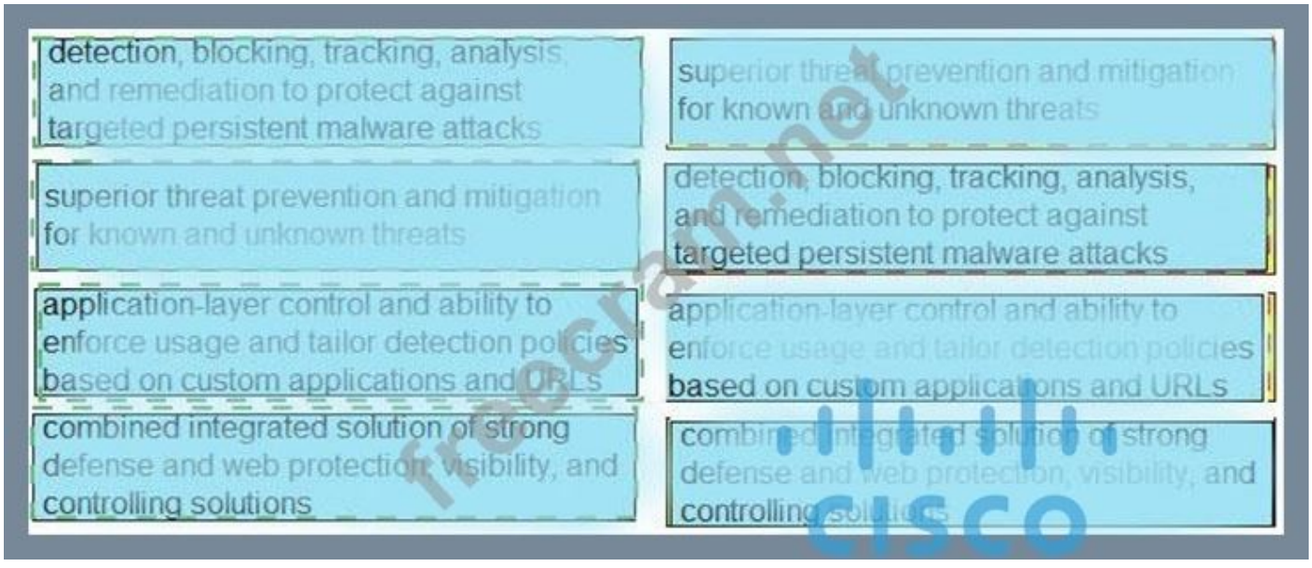
NEW QUESTION: 43
Which Dos attack uses fragmented packets to crash a target machine?
A. smurf
B. LAND
C. MITM
D. teardrop
Answer: (SHOW ANSWER)

NEW QUESTION: 44

Drag and drop the capabilities from the left onto the correct technologies on the right.



Answer:



Explanation

superior threat prevention and mitigation for known and unknown threats
detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions

NEW QUESTION: 45
Refer to the exhibit.

```
Info: New SMTP ICID 30 interface Management (192.168.0.100)
   address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
   DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
   AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
   DEFAULT in the outbound table
```

Which type of authentication is in use?
A. POP3 authentication
B. LDAP authentication for Microsoft Outlook
C. SMTP relay server authentication
D. external user and relay mail authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 46
For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two.)
A. computer identity
B. Windows firewall
C. Windows service

D. user identity
E. default browser
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Refer to the exhibit.

A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status What is the problem according to this command output?
A. authentication key mismatch
B. interesting traffic was not applied

C. encryption algorithm mismatch
D. hashing algorithm mismatch
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Refer to the exhibit.

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?
A. show authentication method
B. show authentication registrations
C. show dot1x all
D. show authentication sessions
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent? (Choose two.)
A. Traffic is encrypted, which prevents visibility on firewalls and IPS systems.
B. An exposed API for the messaging platform is used to send large amounts of data.
C. Outgoing traffic is allowed so users can communicate with outside organizations.
D. Messenger applications cannot be segmented with standard network controls.
E. Malware infects the messenger application on the user endpoint to send company data.
Answer: (SHOW ANSWER)

NEW QUESTION: 50

An engineer needs a solution for TACACS+ authentication and authorization for device administration. The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth.
Which product meets all of these requirements?

A. Cisco AMP for Endpoints
B. Cisco Identity Services Engine
C. Cisco Stealthwatch
D. Cisco Prime Infrastructure
Answer: (SHOW ANSWER)

NEW QUESTION: 51
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)
A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.
B. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically
C. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device
D. The IPsec configuration that is set up on the active device must be duplicated on the standby device.
E. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which type of algorithm provides the highest level of protection against brute-force attacks?
A. HMAC
B. PFS
C. SHA
D. MD5
Answer: (SHOW ANSWER)

NEW QUESTION: 53
What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?
A. posture assessment
B. CoA
C. external identity source
D. SNMP probe
Answer: (SHOW ANSWER)

NEW QUESTION: 54

What is the function of SDN southbound API protocols?

A. to enable the controller to make changes

B. to allow for the dynamic configuration of control plane applications

C. to enable the controller to use REST

D. to allow for the static configuration of control plane applications

Answer: (SHOW ANSWER)

Explanation

Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs.

NEW QUESTION: 55

Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

A. network address translations

B. intrusion policy

C. quality of service

D. time synchronization

Answer: D (LEAVE A REPLY)

NEW QUESTION: 56

Which two mechanisms are used to control phishing attacks? (Choose two.)

A. Define security group memberships

B. Enable browser alerts for fraudulent websites

C. Revoke expired CRL of the websites

D. Use antispyware software

E. Implement email filtering techniques

Answer: (SHOW ANSWER)

NEW QUESTION: 57

An organization has two systems in their DMZ that have an unencrypted link between them for communication. The organization does not have a defined password policy and uses several default accounts on the systems. The application used on those systems also have not gone through stringent code reviews.

Which vulnerability would help an attacker brute force their way into the systems?

A. weak passwords

B. missing encryption

C. lack of file permission

D. lack of input validation

Answer: (SHOW ANSWER)

NEW QUESTION: 58

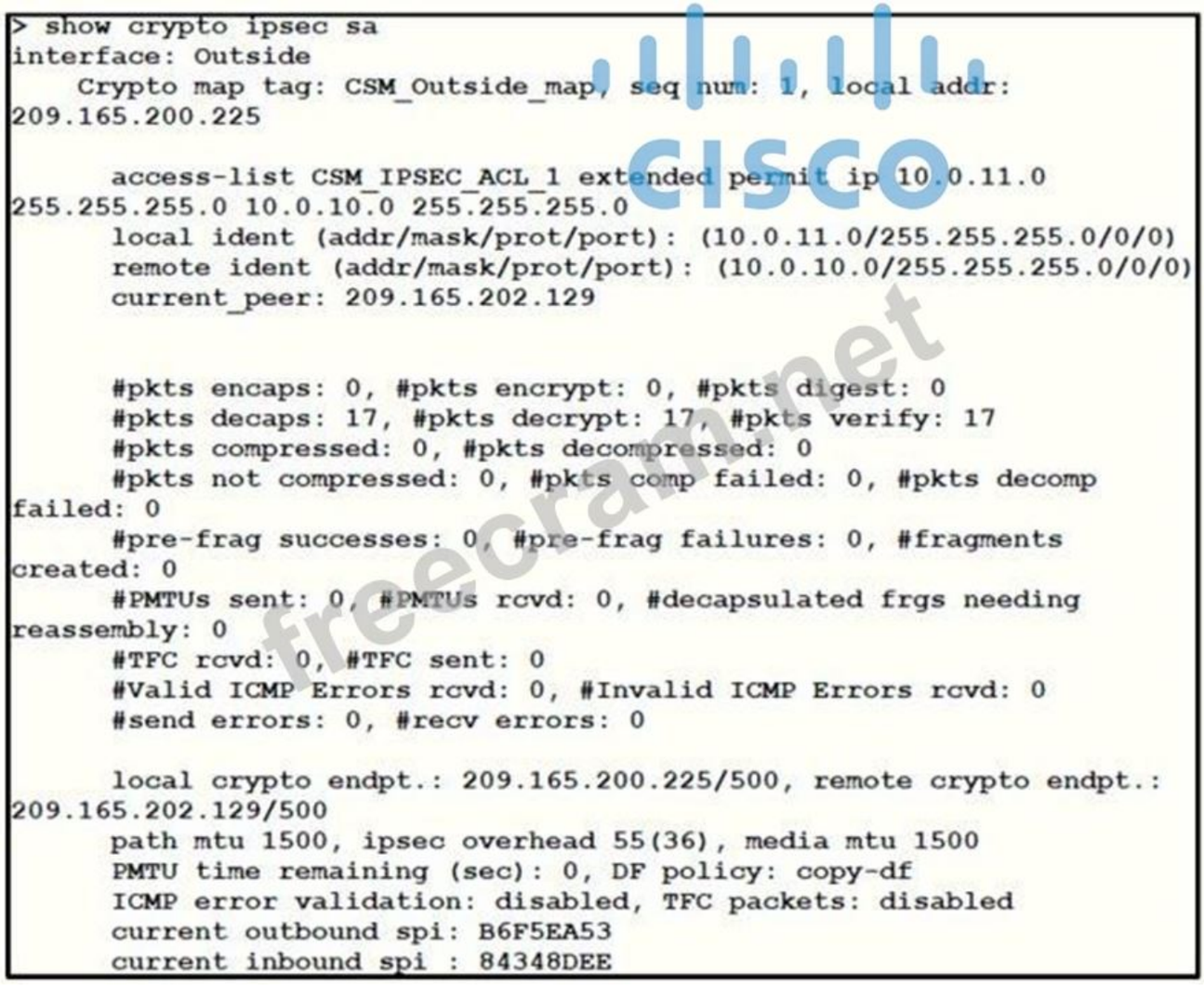
What is managed by Cisco Security Manager?

A. WSA
B. ASA
C. access point O
D. ESA
Answer: (SHOW ANSWER)
Explanation
https://www.cisco.com/c/en/us/products/collateral/security/security-manager/datasheet-C78-737182.html

NEW QUESTION: 59
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?
A. Destination Lists
B. SafeSearch
C. File Analysis
D. SSL Decryption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
Under which two circumstances is a CoA issued? (Choose two.)
A. A new Identity Source Sequence is created and referenced in the authentication policy
B. A new Identity Service Engine server is added to the deployment with the Administration persona
C. An endpoint is deleted on the Identity Service Engine server
D. A new authentication rule was added to the policy on the Policy Service node
E. An endpoint is profiled for the first time
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Refer to the exhibit.



Traffic is not passing through IPsec site-to-site VPN on the Firepower Threat Defense appliance. What is causing this issue?

A. No split-tunnel policy is defined on the Firepower Threat Defense appliance.

B. Site-to-site VPN peers are using different encryption algorithms.

C. The access control policy is not allowing VPN traffic in.

D. Site-to-site VPN preshared keys are mismatched.

Answer: (SHOW ANSWER)

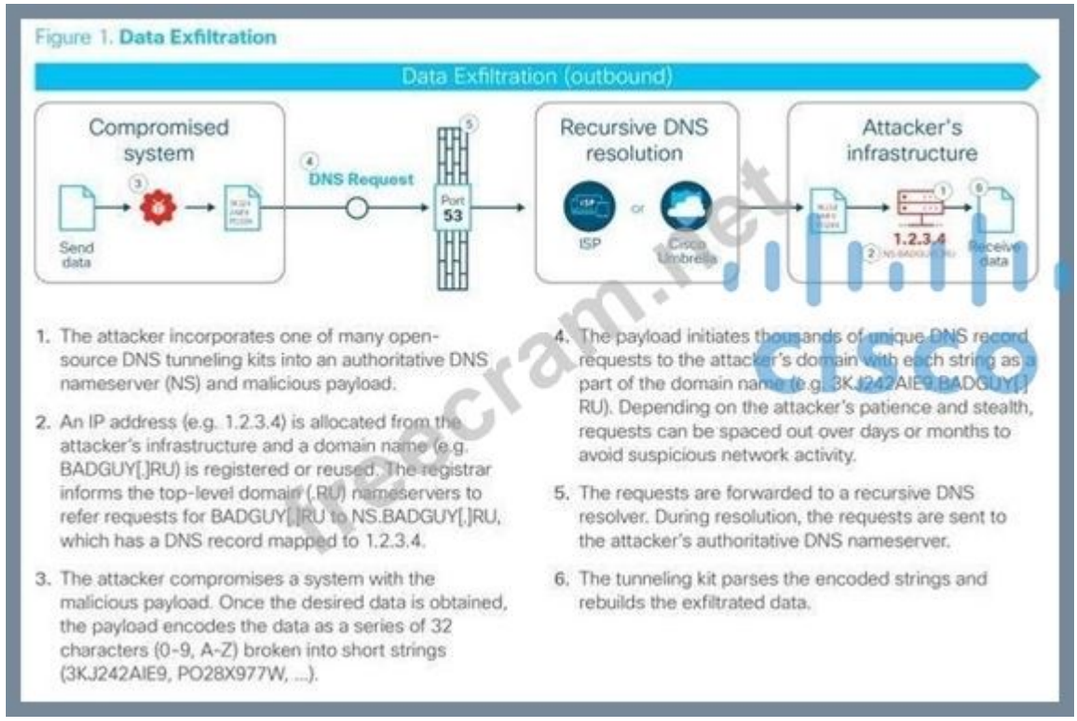
NEW QUESTION: 62

Which functions of an SDN architecture require southbound APIs to enable communication?
A. SDN controller and the network elements
B. management console and the SDN controller
C. SDN controller and the cloud
D. management console and the cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?
A. It allows CoA to be applied if the endpoint status is compliant.
B. It allows the endpoint to authenticate with 802.1xor MAB.
C. It verifies that the endpoint has the latest Microsoft security patches installed.
D. It adds endpoints to identity groups dynamically.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
What is a feature of the open platform capabilities of Cisco DNA Center?
A. domain integration
B. intent-based APIs
C. application adapters
D. automation adapters
Answer: (SHOW ANSWER)

NEW QUESTION: 65
How does DNS Tunneling exfiltrate data?
A. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection.
B. An attacker opens a reverse DNS shell to get into the client's system and install malware on it.
C. An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order to poison the resolutions.
D. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.
Answer: A (LEAVE A REPLY)
Explanation



NEW QUESTION: 66
What are two functions of secret key cryptography? (Choose two.)
A. provides the capability to only know the key on one side
B. utilization of different keys for encryption and decryption
C. key selection without integer factorization
D. utilization of large prime number iterations
E. utilization of less memory
Answer: (SHOW ANSWER)

NEW QUESTION: 67
What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?.
A. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
C. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX
D. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
Answer: B (LEAVE A REPLY)

NEW QUESTION: 68
A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?
A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.
B. The file is queued for upload when connectivity is restored.
C. The file upload is abandoned.
D. The ESA immediately makes another attempt to upload the file.

Answer: (SHOW ANSWER)

Explanation

- The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html

NEW QUESTION: 69

Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

A. Google Cloud Platform

B. Red Hat Enterprise Visualization

C. VMware ESXi

D. Amazon Web Services

Answer: (SHOW ANSWER)

Explanation

Cisco Firepower NGFWv in Amazon Web Services (AWS) or Microsoft Azure must be managed by a Cisco Firepower Management Center (FMC) residing in AWS or on-premises. The virtual FCM can be deployed on VMware ESXi, on KVM, and in AWS. Figure 1 shows the various FMC dashboards.

NEW QUESTION: 70

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services?
(Choose two.)

A. single sign-on

B. central web auth

C. local web auth

D. multiple factor auth

E. TACACS+

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 71

Which two services must remain as on-premises equipment when a hybrid email solution is deployed?
(Choose two.)

A. antivirus

B. DLP

C. antispam

D. encryption

E. DDoS

Answer: (SHOW ANSWER)

NEW QUESTION: 72

What are two list types within AMP for Endpoints Outbreak Control? (Choose two.)

A. simple custom detections

B. URL

C. command and control

D. blocked ports
E. allowed applications
Answer: (SHOW ANSWER)

NEW QUESTION: 73
What is a benefit of using Cisco FMC over Cisco ASDM?
A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
B. Cisco FMC provides centralized management while Cisco ASDM does not.
C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices
Answer: (SHOW ANSWER)
Explanation
https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html

NEW QUESTION: 74
After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from happening in the future?
A. Modify an access policy.
B. Modify identification profiles.
C. Modify outbound malware scanning policies
D. Modify web proxy settings
Answer: (SHOW ANSWER)
Explanation