Cisco.300-540.v2026-06-29.q89

Exam Code:	300-540
Exam Name:	Designing and Implementing Cisco Service Provider Cloud Network Infrastructure
Certification Provider:	Cisco
Free Question Number:	89
Version:	v2026-06-29
# of views:	102
# of Questions views:	911
https://www.freecram.net/torrent/Cisco.300-540.v2026-06-29.q89.html	

NEW QUESTION: 1
Automatic fault management is crucial for:
A. Increasing manual monitoring efforts
B. Decreasing network uptime
C. Reducing network speed
D. Immediate identification and response to network issues
Answer: (SHOW ANSWER)

NEW QUESTION: 2
To ensure control plane high availability, deploying _____ instances across different physical servers is recommended.
A. isolated
B. single
C. duplicated
D. multiple
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which of the following are benefits of using streaming telemetry for network assurance? (Select two)
A. Real-time data collection
B. Reduced monitoring capabilities
C. Improved scalability and flexibility
D. Increased network latency

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 4
Zero-day exploits are:
A. Problems solved by restarting the system
B. Known vulnerabilities with existing patches
C. Vulnerabilities unknown to the software vendor
D. Issues only found in open-source software
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following is considered a virtualized Cisco platform?
A. Cisco IOS XRv
B. Cisco Aironet
C. Cisco Catalyst
D. Cisco Nexus
Answer: (SHOW ANSWER)

NEW QUESTION: 6
How does log management assist in meeting the requirements of cloud security regulatory compliance?
A. by supporting documentation and reporting processes
B. by streamlining resource allocation across cloud environments
C. by providing enhanced interoperability between cloud platforms
D. by boosting the security of cloud-based applications
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Cisco SP Cloud Network Infrastructure Security Knowledge Cloud security compliance frameworks (such as ISO 27001, PCI-DSS, GDPR, SOC 2, HIPAA) require:
* Evidence of security events
* Retention of logs for audit periods
* Ability to generate compliance reports
* Traceability and accountability
* Incident investigation support
Effective log management enables:
* Centralized collection of application, network, and system logs
* Storage of logs for mandated retention periods
* Generation ofaudit-ready reports
* Documentation required for compliance assessments

* Demonstration that monitoring and security controls are active and functioning Therefore, the role of log management in regulatory compliance is primarily aboutdocumentation, traceability, auditing, and reporting, which aligns only with Option A.
The other options do not directly serve regulatory compliance requirements:
* Brelates to resource optimization, not compliance.
* Crefers to interoperability, which is unrelated to regulatory auditing.
* Dimproves security but does not directly address compliance documentation.

NEW QUESTION: 7
A common DoS mitigation technique is:
A. Increasing bandwidth
B. Rate limiting
C. Using a single firewall
D. Removing all filters
Answer: (SHOW ANSWER)

NEW QUESTION: 8
SR-PM is related to:
A. Security risk performance management
B. Software redundancy performance metrics
C. Segment routing performance monitoring
D. Storage replication performance management
Answer: (SHOW ANSWER)

NEW QUESTION: 9
What is the main advantage of using container orchestration in application deployment?
A. Automated management of containers
B. Increased application latency
C. Manual scaling of applications
D. Reduced security
Answer: (SHOW ANSWER)

NEW QUESTION: 10
A large company's legacy network is set up with equipment from multiple vendors. The company engaged a network architect to optimize the network for virtualization. The architect must ensure robust and efficient operation, considering the company's immediate needs but also anticipating future network complexities and scalability requirements. The chosen strategy must be capable of integrating seamlessly with existing systems, while providing a pathway for innovation and growth. The solution must facilitate end-to-end service automation throughout the entire lifecycle, and the implementation must ensure the validation, execution, and abstraction of network configurations and services. Which action must be taken to meet the requirements?

A. Implement a service life-cycle approach with simplified monitoring that plans for post-deployment adjustments to be incorporated into the automation CI/CD pipeline.
B. Implement a configuration-management approach that allows for configuring each network device individually to optimize its performance.
C. Implement a flexible service-modeling approach that leverages automation for ongoing management and refinement as demands on the network evolve.
D. Implement a service-modeling approach with a static YANG one-size-fits-all model that includes the unique requirements of each different network element.
Answer: (SHOW ANSWER)
Cisco NSO-based orchestration principles in a multi-vendor environment require:
Service modeling using flexible, reusable YANG models
Abstraction of vendor-specific device differences
Transaction-safe configuration validation and execution
End-to-end automation across lifecycle stages (Day-0, Day-1, Day-N)
Scalability and adaptability for evolving requirements
Option C aligns perfectly with NSO service-modeling approaches:
Service models must be flexible, not rigid, enabling changes as technologies and needs evolve.
The architecture must support continuous refinement, enabling multi-vendor abstraction and lifecycle automation.
This ensures the network evolves seamlessly while remaining stable and automated.
Why the Other Options Are Incorrect
A - Simplified monitoring and post-deployment adjustments do not meet the core need for full lifecycle service modeling and abstraction.
B - Configuring devices individually contradicts the entire purpose of orchestration and abstraction.
D - A static YANG model cannot accommodate multi-vendor environments or future scalability.
Thus, only Option C matches full NSO-capable service modeling requirements.

NEW QUESTION: 11
In high availability design, DNS is used to ensure _____.
A. encryption
B. authentication
C. compression
D. redundancy
Answer: (SHOW ANSWER)

NEW QUESTION: 12
High availability design models often include:
A. Single points of failure
B. DNS, routing, and load balancers
C. Only physical redundancy
D. Decreased focus on redundancy

Answer: (SHOW ANSWER)

NEW QUESTION: 13
Virtual Machines and Containers are both used to virtualize resources.
Which statement is true?
A. Containers are less isolated than VMs.
B. VMs can be deployed faster than containers.
C. VMs are more lightweight than containers.
D. Containers virtualize the operating system, whereas VMs virtualize the hardware.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
The primary benefit of MACSEC is:
A. Filtering traffic based on content
B. Increasing the speed of network devices
C. Encrypting frames on a network
D. Authenticating users accessing the network
Answer: (SHOW ANSWER)

NEW QUESTION: 15
The main purpose of using IPsec VPN for WAN connectivity is to:
A. Simplify network management
B. Provide a secure encrypted tunnel over the internet
C. Increase the data transfer speed
D. Offer a dedicated physical connection to the internet
Answer: (SHOW ANSWER)

NEW QUESTION: 16
An engineer must design a cloud platform forevent-driven applications. The solution must allowmicro-sized atomic componentsto be built, deployed, and run code on demand. Which solution must be used?
A. Cisco+ Hybrid Cloud for Virtual Desktop Infrastructure
B. Cisco FaaS
C. Cisco+ Hybrid Cloud Virtualization
D. Cisco Intersight
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Cisco Cloud Architecture Knowledge Event-driven applications require:
* Stateless, micro-sized execution units
* Automatic scaling
* Code that runsonlywhen triggered

* No server or VM lifecycle management
This model is known asFunction-as-a-Service (FaaS).
Cisco FaaSprovides:
* Serverless execution
* Event-driven triggers
* Deployment of atomic micro-functions
* Automatic scaling and resource abstraction
* Ideal environment for microservices and cloud-native workloads
Why the others are incorrect:
* A. Cisco+ Hybrid Cloud for VDI# delivers desktops, not serverless compute
* C. Cisco+ Hybrid Cloud Virtualization# VM-based infrastructure, not event-driven micro-functions
* D. Cisco Intersight# operational management tool, not a serverless execution platform

NEW QUESTION: 17
Multi-homing is beneficial for:
A. Enhancing redundancy and resilience
B. Increasing dependency on a single ISP
C. Simplifying network architecture
D. Creating a single point of failure
Answer: (SHOW ANSWER)

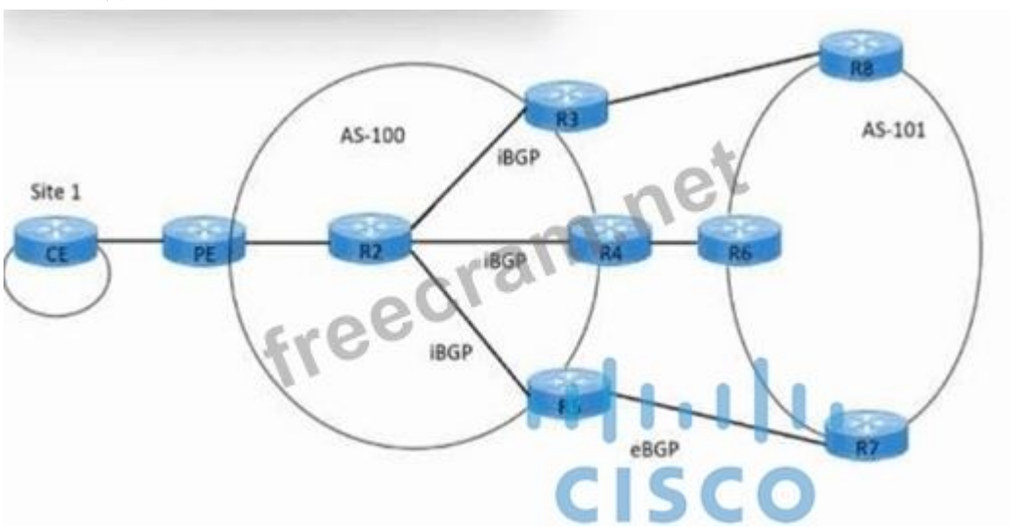
NEW QUESTION: 18
In the context of high availability, EVLAG is implemented to enhance _____.
A. speed
B. redundancy
C. latency
D. simplicity
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Streaming telemetry with gRPC and gNMI is used for:
A. Reducing network traffic

B. Real-time network monitoring
C. Physical network repairs
D. Data encryption
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
The use of Yang models in network configuration is to:
A. Replace XML-based data models
B. Provide a standardized data modeling language
C. Increase the complexity of network scripts
D. Simplify the parsing of binary data
Answer: (SHOW ANSWER)

NEW QUESTION: 21
What is a benefit of a carrier-neutral data center?
A. Reduction in foot traffic
B. Path diversity on multiple carriers
C. Lower electrical costs
D. Avoidance of a price lock-in
Answer: (SHOW ANSWER)
Carrier-neutral facilities allow customers to connect tomultiple telecom carriers, providing:
* Physical path diversity
* Redundancy
* Competitive options
* High availability for interconnects
Thus,path diversity on multiple carriersis the primary benefit.

NEW QUESTION: 22


Refer to the exhibit. An engineer working for a private service provider with an employee ID 5207:22:409 must configure iBGP multipath load sharing across the three paths. Which two commands must be run on the PE router? (Choose two.)

A. maximum-paths ibgp 3

B. ip load-sharing per-destination

C. ip load-sharing ibgp 3

D. router bgp 101

E. router bgp 100

Answer: (SHOW ANSWER)

In the diagram, thePE and R2, R3, R4, R5belong toAS 100. The PE router runs BGP processAS 100, so its BGP configuration must start with:

router bgp 100

To performiBGP multipath load sharingacross three equal-cost internal BGP paths, BGP must be instructed to keep and use multiple iBGP paths in the routing table. This is done with:

router bgp 100

maximum-paths ibgp 3

* maximum-paths ibgp 3 tells BGP to install up tothreeiBGP paths to the same prefix, enabling CEF to load-share across those paths.

* router bgp 100 is required because the PE is inAS 100, not 101.

Other options:

* ip load-sharing per-destination affects CEF behavior but does not enable BGP iBGP multipath by itself and is not specific to three iBGP paths.

* ip load-sharing ibgp 3 is not a valid IOS BGP command.

* router bgp 101 would configure the wrong AS and break the iBGP relationships shown in AS-100.

Thus, the correct commands on the PE to achieve iBGP multipath load sharing over the three internal paths are maximum-paths ibgp 3androuter bgp 100, corresponding toA and E.

NEW QUESTION: 23

What does enabling gRPC allow in Cisco NFVI Assurance and Monitoring?

A. telemetry streaming

B. IPFIX monitoring

C. Cisco IOS NetFlow monitoring

D. system logging

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation

In Cisco NFV Infrastructure (NFVI) Assurance and Monitoring, enabling gRPC activates the device's ability to support model-driven telemetry streaming.

Key points from Cisco SP Cloud/NFVI design principles:

gRPC is used as the transport protocol for model-driven telemetry.

Telemetry replaces traditional polling methods (SNMP, CLI scraping) with continuous, push-based updates.

It allows NFVI components to stream real-time operational data (CPU, memory, interfaces, VM metrics, fabric state) to collectors such as Cisco Crosswork, InfluxDB, Prometheus, or other analytic systems.
gRPC does not provide NetFlow/IPFIX export or syslog itself; those are separate subsystems.
Evaluation of options:
A). telemetry streaming - Correct. gRPC enables model-driven streaming telemetry.
B). IPFIX monitoring - Incorrect; IPFIX uses UDP exports, not gRPC.
C). Cisco IOS NetFlow monitoring - Incorrect; uses NetFlow export protocols.
D). system logging - Incorrect; syslog uses UDP/TCP, not gRPC.

NEW QUESTION: 24
TLS and mTLS are protocols used for:
A. Routing
B. Encryption and secure communication
C. Traffic shaping
D. Access control
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which of the following is NOT a purpose of implementing ACLs in network security?
A. To define routing protocols
B. To provide a layer of security
C. To restrict access to network resources
D. To filter network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Yang models are utilized in NFV for what purpose?
A. To manualize the configuration process
B. To decrease data model standardization
C. To increase the complexity of network configurations
D. To define network elements and configurations
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Cloud agents are deployed for:
A. Reducing data storage needs
B. Manual network configuration
C. Automated network and performance monitoring
D. Physical security
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
An engineer must add VNF implementation definitions and VNF service definitions to an OpenStack deployment data model to deploy virtual routers and firewalls to an enterprise network. After the virtual machine resources are prepared, which action must be taken next?
A. Specify the operational characteristics.
B. Create the initial configuration for day zero.
C. Configure key performance indicator monitoring.
D. Define the NFV network.
Answer: (SHOW ANSWER)
In an NFV environment following Cisco NFV Infrastructure and ETSI MANO architecture, the onboarding workflow for VNF deployment follows this high-level order:
* Define VNF descriptors (VNFD and NSD)- Includes implementation details and service definitions.
* Prepare virtual machine resources- Flavor, image, CPU/memory/storage, and placement.
* Define the NFV network- This step builds the underlay/overlay connectivity needed for the VNF.- It includes virtual network creation, interfaces, VLs (Virtual Links), connection points, and mapping into OpenStack (Neutron networks, subnets, ports).- No VNF can be deployed until the NFV service networks (management, control, data, HA) are defined.
* Apply Day-0 configuration- Bootstrapping/initial config.
* Apply Day-1 operational characteristics- Routing, services, policies.
* Configure operational monitoring (KPIs)- Performance and fault measurements.
Since the question states"after the VM resources are prepared", the next mandatory stage is defining the virtual network connectivity on which the VNFs will operate.

NEW QUESTION: 29


Refer to the exhibit. An engineer must configure dual-homing with single active redundancy in a BGP EVPN VXLAN fabric. Which command must be run on the leaf router to complete the EVPN Ethernet segment configuration?
A. redundancy single-active
B. default-gateway advertise
C. replication-type static
D. vlan configuration 101
Answer: (SHOW ANSWER)
In a BGP EVPN VXLAN multi-homing design, Ethernet Segment Identifiers (ESIs) are used to represent a set of links from one or more leaf switches to the same downstream device (such as a CE, firewall, or aggregation switch). By default, when multiple leafs share the same ESI, the EVPN

design supportsall-active redundancy, where all participating leafs can forward traffic for that Ethernet segment simultaneously.
However, some use cases-like connecting to devices that do not support multipath forwarding or for strict active/standby redundancy-requiresingle-activemulti-homing. In single-active mode, only one leaf in the Ethernet segment forwards traffic at any time; the other leaf(s) act as standby and only take over if the active node fails. This behavior is explicitly controlled in the EVPN Ethernet-segment configuration.
On Cisco platforms for EVPN VXLAN fabrics, this is configured under thel2vpn evpn ethernet-segment stanza using the command:
l2vpn evpn ethernet-segment 1
identifier type 0 01.01.01.10.10.10.10.10.10.10
redundancy single-active
* identifier type 0 ... defines the ESI for the multi-homed connection.
* redundancy single-active specifies that only one leaf in that ESI is allowed to be active at a time, thus enablingdual-homing with single-active redundancy.
The other options do not relate to Ethernet-segment redundancy mode:
* B. default-gateway advertiseis used in EVPN anycast gateway configurations to advertise the default gateway MAC/IP, not for ESI redundancy.
* C. replication-type staticis associated with multicast or ingress replication behavior for VXLAN VTEPs, not Ethernet-segment redundancy.
* D. vlan configuration 101is a VLAN configuration context command and has no effect on EVPN ESI redundancy.

NEW QUESTION: 30

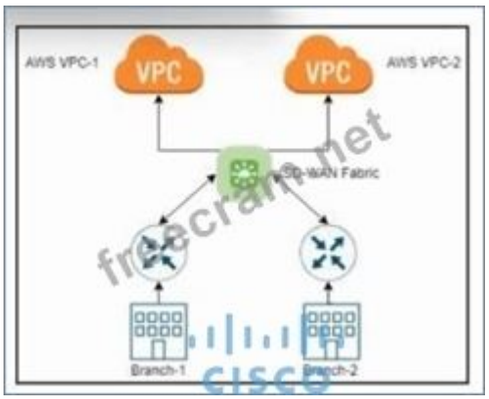
What is a capability of a Cisco NFVIS SNMP trap?

A. Monitors the activities of a network host
B. Controls the activities of a network host
C. Sends an unsolicited notification to the SNMP manager
D. Retrieves an SNMP object variable from the MIB
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
SNMP traps in Cisco NFVIS (and in SNMP generally):
* Areunsolicited notifications
* Sent from the NFVIS deviceto the SNMP manager
* Indicate alarms, changes, or significant operational events
* Donotrequire polling
Examples:
* Disk failures
* VM crashes
* Host status changes
* Resource alarms

Why the others are wrong:
* Adescribes SNMP monitoring (done by the manager with GET requests)
* BSNMP cannotcontrolhost activities
* DSNMP GET retrieves a variable, but traps sendunsolicitednotifications Thus, the correct answer isC.

NEW QUESTION: 31
What should be used to protect against lateral movements during a Cisco NFVI security breach?
A. Wi-Fi Protected Access
B. Web application firewall
C. Network segmentation
D. Data encryption
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
In Cisco NFVI security architecture, the primary defense againstlateral movement(an attacker moving from one compromised node to another) isnetwork segmentation.
Segmentation:
* Separates workloads (compute, storage, management, tenant networks)
* Prevents attackers from pivoting inside the NFVI
* Reduces blast radius during breaches
* Enforces micro-segmented virtual network boundaries
WPA protects Wi-Fi, not NFVI.
WAF protects web apps, not internal movement.
Data encryption protects confidentiality, not lateral movement control.
Thus,network segmentationis the correct solution.

NEW QUESTION: 32



Refer to the exhibit. An engineer must design a solution that allows a user to choose which private Cisco Catalyst SD-WAN network they want to connect to AWS. The solution must automatically identify the AWS VPC and other cloud services based on the user credentials. What must be used?

A. AWS Direct Connect

B. Transit VPC for AWS

C. IPsec VPN

D. Segment routing

Answer: (SHOW ANSWER)

In Cisco Catalyst SD-WAN cloud integration, when the requirement is:

* Automatically discovering AWSVPCs
* Automatically identifying AWSservices
* Allowing the user to choose whichprivate SD-WAN networkconnects to the cloud
* UsingAWS credentials(Access Key / Secret Key) for automatic provisioning

...the Cisco-supported mechanism is theCisco SD-WAN Transit VPC solution.

Why Transit VPC is the correct answer:

* It is specifically designed to integrateCisco SD-WANwith AWS environments.
* Uses AWS APIs and user credentials to automatically discover:
* VPC IDs
* Subnets
* Regions
* Routing tables
* Automatically deploys and configures CSR1000v or Catalyst 8000V routers into the VPC.
* Provides a centralized "hub" in AWS to interconnect multiple SD-WAN sites.
* Enables the user to choose which SD-WAN segments connect to which VPCs.

This matches the requirement ofautomatic cloud resource identification based on user credentials.

Why the other options are incorrect

A). AWS Direct Connect

* This is a physical/private Layer 2 cloud connection.
* It doesnotauto-discover VPCs or integrate through credentials.
* It does not provide automated SD-WAN service provisioning.

C). IPsec VPN

* Works for connectivity but ismanual, not automated.

* Does not identify AWS cloud resources via credentials.
D). Segment routing
* A transport technology used inside SP networks, irrelevant to AWS API-based VPC discovery.
Thus, onlyTransit VPCprovides automatic AWS cloud discovery and integration with SD-WAN.

NEW QUESTION: 33
SNMP traps are utilized for which of the following purposes?
A. Monitoring network performance in real-time
B. Sending unsolicited alerts from network devices to a management station
C. Virtualizing network functions
D. Encrypting data packets
Answer: (SHOW ANSWER)

NEW QUESTION: 34
An engineer must configure NTP servers in Cisco Enterprise NFVIS. The primary NTP server has an IP address of 192.168.1.1 and the backup NTP server has an IP address of 192.168.2.1. Which two commands must be run to complete the configuration? (Choose two.)
A. system time ntp preferred_server 192.168.1.1
B. utils ntp server add 192.168.2.1 backup
C. system set-manual-time 192.168.1.1 192.168.2.1
D. utils ntp server add 192.168.1.1 primary
E. system time ntp backup_server 192.168.2.1
Answer: (SHOW ANSWER)
InCisco Enterprise NFVIS, time synchronization is configured using thesystem time ntpcommand structure.
NFVIS requires a primary and optionally a backup NTP server to maintain accurate system time for the hypervisor and guest VMs.
Correct NFVIS command syntax for NTP configuration:
* system time ntp preferred_server <IP>This command configures thepreferred (primary)NTP server used for system clock synchronization.
* system time ntp backup_server <IP>This command configures thebackupNTP server, which the system uses if the primary becomes unreachable.
These two commands match Cisco NFVIS time-configuration behavior described in NFV infrastructure design and implementation guidelines.
Why the Correct Answers Are A and E
Option A: system time ntp preferred_server 192.168.1.1
This properly configures the primary NTP server in NFVIS. The preferred server is always the first choice for time synchronization.
Option E: system time ntp backup_server 192.168.2.1
This correctly configures the backup NTP server. If the preferred server fails, NFVIS automatically falls back to the backup server.

Both commands directly match NFVIS's NTP command hierarchy and are the only ones that correctly apply to NFVIS.
Why the Other Options Are Not Correct
Option Buses utils ntp, which is not an NFVIS command.
Option Csets manual time and does not configure NTP servers.
Option Dalso uses the utils ntp syntax, which applies to other Cisco platforms but not NFVIS.

NEW QUESTION: 35
An engineer must implement a solution on a Cisco ASR 1000 Series router to protect against DDoS attacks.
DDoS traffic must be dropped by transmitting Flowspec attributes to edge routers, instructing them to generate an ACL via class-maps and policy-maps. The engineer already configured BGP neighbors. Which action must be taken next?
A. Configure Flowspec for the BGP address-family
B. Set the BGP routing process
C. Activate the BGP neighbors
D. Configure the route reflector
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
BGP Flowspec allows routers to distributetraffic-filtering rulesusing BGP NLRI.
To enable Flowspec, after neighbors are configured, the essential next step is:
#Activate the Flowspec address-family under BGP
Example:
router bgp 65000
address-family ipv4 flowspec
neighbor X.X.X.X activate
exit-address-family
This enables:
* FlowSpec NLRI exchange
* Distribution of drop rules (rate-limit, redirect, null route, etc.)
* Automatic ACL/class-map/policy-map generation on edge routers
Why the other options are incorrect:
* B. Set BGP routing process# already done when neighbors were configured
* C. Activate neighbors# only makes senseinsidean address-family; flowspec AF must be enabled first
* D. Configure route reflector# optional and not required for Flowspec to operate Thus, the correct next step isA. Configure Flowspec for the BGP address-family.

NEW QUESTION: 36
NSO in the context of virtualized architecture stands for:
A. Network Service Operator

B. Non-Secure Operations
C. Network Scale Optimization
D. Network Service Orchestrator
Answer: (SHOW ANSWER)

NEW QUESTION: 37
ACI's approach to data center management is unique because it:
A. Is application-centric, not just network-centric
B. Ignores the need for automation
C. Requires manual configuration for all network devices
D. Focuses on physical infrastructure over software
Answer: (SHOW ANSWER)

NEW QUESTION: 38
gRPC is used in network virtualization for:
A. Graphic rendering
B. High-performance remote procedure calls
C. Physical network connections
D. Decreasing network automation
Answer: (SHOW ANSWER)

NEW QUESTION: 39
An engineer must implement a public cloud solution that enables a company to place all its infrastructureand its end-user applications in the cloud, eliminating the need for software application management and maintenance. Which cloud service model must be used?
A. SaaS
B. PaaS
C. IaaS
D. FaaS
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (Cisco Cloud Model Knowledge)
The requirement states:
* All infrastructure in the cloud
* All applications delivered from the cloud
* No software management
* No maintenance by the customer
This matchesSoftware as a Service (SaaS).
SaaS provides:
* Fully managed applications
* No patching, upkeep, installation, or infrastructure maintenance
* End-to-end cloud delivery

PaaS and IaaS still require some software/application management.
FaaS is event-driven serverless compute, not full application hosting.
Therefore, the correct answer isA. SaaS.

NEW QUESTION: 40
When troubleshooting DCI solutions, which of the following tools or concepts are crucial? (Choose two)
A. SNMP for managing network devices
B. EVPN VXLAN for extending layer 2 services over a layer 3 network
C. IPsec VPN for enhancing physical security measures
D. ACI for centralized application-focused network policies
Answer: (SHOW ANSWER)

NEW QUESTION: 41
VNF workload optimization often involves:
A. Decreasing virtualization
B. Utilizing technologies like SR-IOV for performance
C. Ignoring software acceleration
D. Increasing physical network functions
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Automation in deploying NFV can reduce:
A. Network reliability
B. The speed of service delivery
C. Software-defined networking capabilities
D. The need for manual configuration
Answer: (SHOW ANSWER)

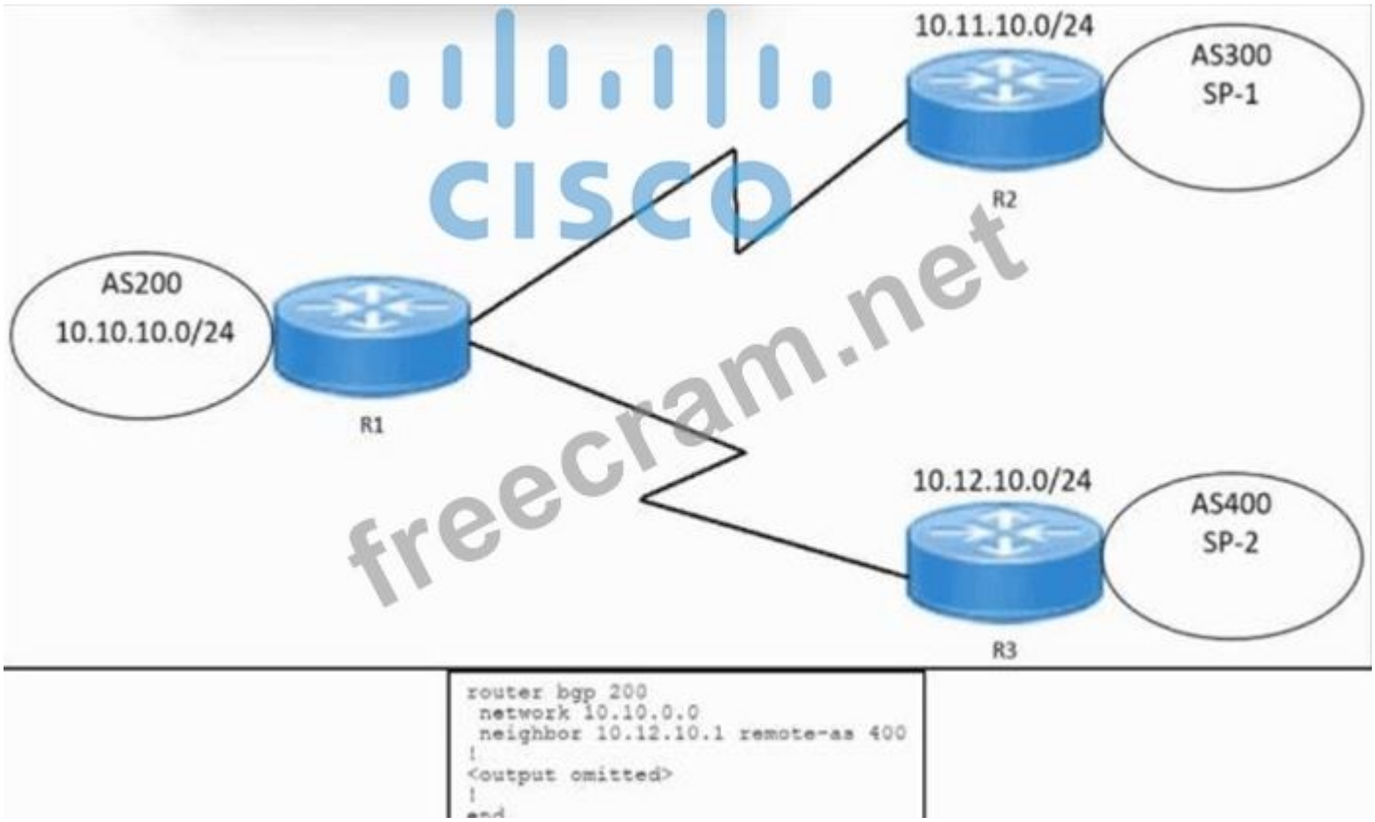
NEW QUESTION: 43
VIM control plane KPIs are important for:
A. Monitoring virtual infrastructure manager performance
B. Decreasing network traffic
C. Tracking physical server health
D. Manual network configurations
Answer: (SHOW ANSWER)

NEW QUESTION: 44
gNMI/gRPC are used in network management for:
A. Exclusively managing physical network devices
B. Simplifying manual network configuration tasks
C. Providing high-performance, bi-directional streaming of network state information

D. Reducing the efficiency of network operations
Answer: (SHOW ANSWER)

NEW QUESTION: 45
NFVI errors and events diagnosis is crucial for:
A. Reducing the efficiency of the network
B. Increasing network costs
C. Ensuring high network availability and reliability
D. Manual network configurations
Answer: (SHOW ANSWER)

NEW QUESTION: 46



Refer to the exhibit. An engineer must configure multihoming between router R1 and service provider SP-2.
Locally generated routes must be advertised to service provider SP-2. Which command must be run on R1 to complete the configuration?
A. network 10.0.0.0 route-map as200only out
B. neighbor 10.12.10.1 route-map localonly out
C. network 10.12.10.1 route-map as200only in
D. neighbor 10.0.0.0 route-map localonly out
Answer: (SHOW ANSWER)
On R1 (AS200), the requirement is:
* Advertiselocally generated routes(for example, 10.10.10.0/24 from AS200)

* Only towardSP-2, which peers on IP10.12.10.1
* Apply a policy (route-map) controlling what R1 advertises
In BGP, to controlwhich locally originated routesare sent to a specific neighbor, the correct configuration is:
neighbor <IP> route-map <map-name> out
This applies outbound policy filtering or permitting to the prefixes advertised.
Thus:
* The neighbor toward SP-2 is10.12.10.1
* The route-map must be appliedoutbound
* The command that accomplishes this is:
neighbor 10.12.10.1 route-map localonly out
Why the Other Options Are Incorrect
* A. network 10.0.0.0 route-map as200only outThe network command doesnotaccept route-map out.
This is invalid syntax.
* C. network 10.12.10.1 route-map as200only inIncorrect network, incorrect direction, and invalid syntax with in.
* D. neighbor 10.0.0.0 route-map localonly out10.0.0.0 is not a BGP neighbor; it's a network prefix.

NEW QUESTION: 47
Cloud edge facilities are designed to:
A. Centralize cloud operations in a single location
B. Provide backup power solutions for data centers
C. Reduce latency by bringing cloud resources closer to the end-user
D. Increase the physical storage capacity for cloud providers
Answer: (SHOW ANSWER)

NEW QUESTION: 48
For infrastructure security, which of the following is NOT typically a focus area?
A. Implementing ACLs for traffic filtering
B. Enhancing user interface designs
C. Encrypting data in transit with MACSEC

D. Hardening routers to prevent unauthorized access
Answer: (SHOW ANSWER)

NEW QUESTION: 49
API security is crucial for protecting:
A. Network cables
B. Physical devices only
C. Software interfaces
D. Data storage units
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which format is used by Cisco Container Platform for configuration files?
A. HTML
B. YAML
C. XHTML
D. XML
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
Cisco Container Platform (CCP), built on Kubernetes orchestration, usesYAMLfiles for:
* Cluster configuration
* Pod definitions
* Network settings
* Storage mappings
YAML is the industry-standard declarative syntax for Kubernetes and container orchestration platforms.
HTML, XHTML, and XML are not used for CCP configuration.

NEW QUESTION: 51
An engineer attempts to kill a NETCONF session. The session ID is equal to the current session. What is the effect of this action?
A. An invalid-value error is returned, and the current user is not logged out.
B. The session is terminated, and all the connected users are logged out.
C. The configuration is saved, and the current user is logged out.
D. The configuration is removed, and the current user is logged out.
Answer: (SHOW ANSWER)
NETCONF rules state:
* A user cannot terminatetheir own active session.
* Attempting to kill the same session returnsinvalid-valueerror.
* The session continues running normally.
Thus:

* No logout
* No termination
* No configuration impact
Therefore,Ais correct.

NEW QUESTION: 52
Secure NFVI control and management plane typically involves the use of:
A. Open and unsecured APIs
B. Strong authentication mechanisms
C. Hard-coded credentials
D. Unencrypted traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 53
The implementation of SR-IOV in VNF optimization primarily improves:
A. Manual network troubleshooting efforts
B. Physical device management
C. Virtual network function performance
D. Data encryption protocols
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54


Refer to the exhibit. An engineer must configure an IPsec VPN connection between site 1 and site 2. The indicated configuration was applied to router R1; however, the tunnel fails to come up. Which command must be run on R1 to resolve the issue?
A. ip route 0.0.0.0 0.0.0.0 10.1.1.2
B. crypto isakmp key vpnuser address 192.168.20.2
C. ip route 0.0.0.0 0.0.0.0 192.168.20.2
D. crypto isakmp key vpnuser address 10.1.1.2
Answer: (SHOW ANSWER)

For a site-to-site IPsec VPN, each peer must configure apre-shared keytied to thepublic IP address of the remote VPN peer:
crypto isakmp key <KEY> address <REMOTE_PUBLIC_IP>
From the diagram:
* R1 outside IP:192.168.10.1/24
* R2 outside IP:192.168.20.2/24# remote peer for R1
In the current R1 configuration, the ISAKMP key is incorrectly bound to192.168.10.2, which is a local next- hop/ISP address on R1's own subnet, not the R2 public IP. Because the pre-shared-key address does not match the source IP of R2's IKE packets, phase 1 negotiation fails and the tunnel never comes up.
The correct configuration on R1 must therefore be:
crypto isakmp key vpnuser address 192.168.20.2
Options A and C incorrectly change the default route (next hop must be the local ISP router, not R2's public IP or a LAN address). Option D uses an internal address (10.1.1.2), which is not the IP used for IKE on the Internet.

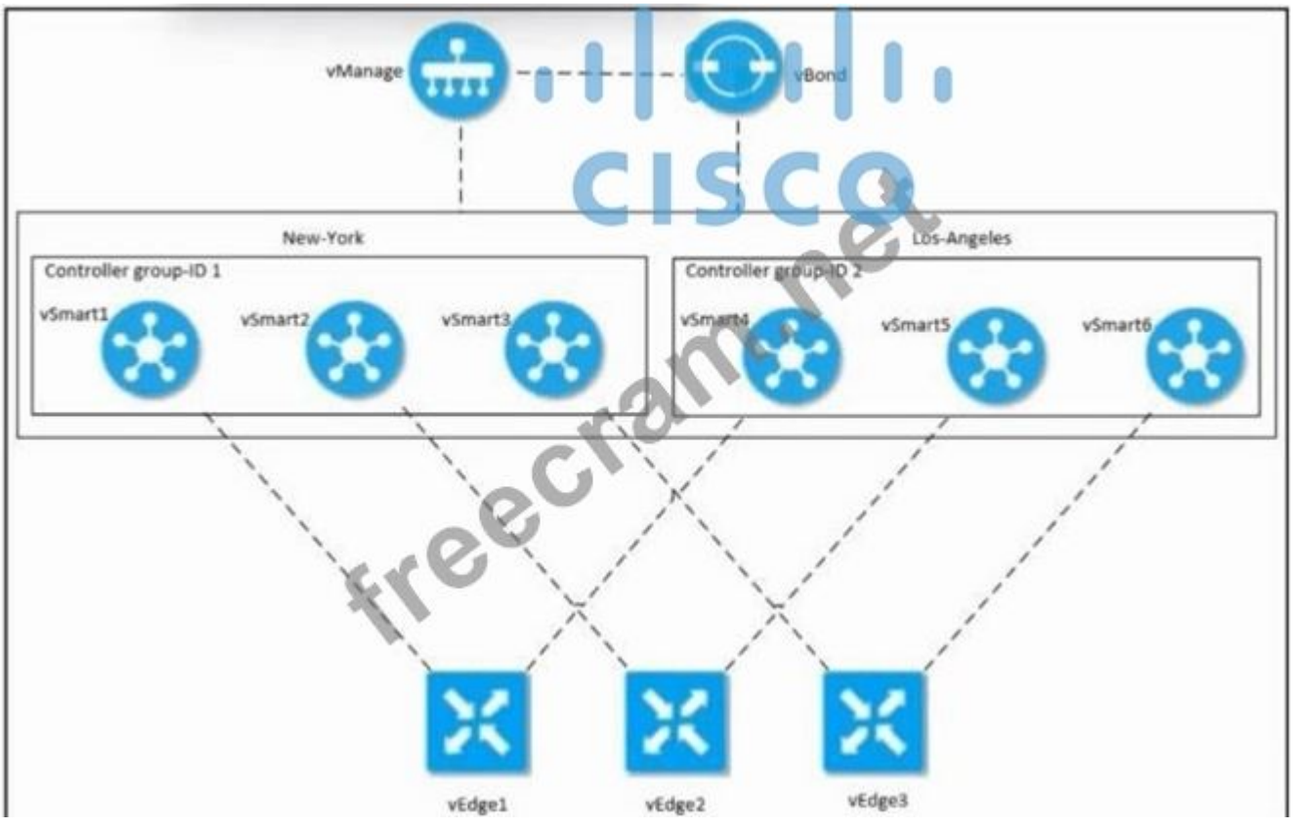
NEW QUESTION: 55
Which two tools should be used to manage container orchestration? (Choose two.)
A. Docker
B. VMware vCenter
C. Cisco vManage
D. Kubernetes
E. Cisco vSmart
Answer: A,D (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract from my knowledge of Designing and Implementing Cisco Service Provider Cloud Network Infrastructure Outlines without Any External URL or Links:
Container orchestration is the automated management of container lifecycle tasks such as deployment, scaling, failover, and updates. In Cisco cloud and NFV design guidance, typical orchestration platforms includeDocker (with Swarm)andKubernetes, which integrate with Cisco networking and security for cloud- native workloads.
* Dockerprovides the container runtime and can also perform basic orchestration through Docker Swarm mode, managing multi-container, multi-host deployments.
* Kubernetesis a full-featured orchestration system that automates deployment, scaling, and operations of application containers across clusters. It is the de-facto standard used with Cisco Container Platform and other Cisco cloud solutions.
VMware vCenter, Cisco vManage, and Cisco vSmart focus on virtual machines or SD-WAN control, not container orchestration. Therefore, the correct tools areDocker and Kubernetes (A, D).

NEW QUESTION: 56
What is used to protect against an API logic flaw?

A. SSH encryption at rest
B. Data encryption at rest
C. Remediation of vulnerabilities
D. Data encryption in transit
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation
AnAPI logic flawis a weakness in the API'sbusiness logic- not in encryption or transport security. It occurs when:
* API functions are misused
* Business rules are bypassed
* Security validation is missing
* Workflow logic is incorrect
These issues cannot be solved through encryption (at rest or in transit). They require:
#Vulnerability remediation
#Fixing API code logic
#Updating API validation, flow control, and authentication logic
Thus the correct answer isC. Remediation of vulnerabilities.

NEW QUESTION: 57
Which cloud provider connection permits BGP peering?
A. Azure S2S VPN
B. Azure Bastion
C. AWS Direct Connect
D. AWS-managed VPN
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation
Cloud interconnects that support BGP peering must provide a routed Layer-3 adjacency capable of exchanging routing information dynamically. In major cloud architectures:
AWS Direct Connect supports private virtual interfaces (VIFs) where BGP is used between the customer router and AWS to exchange routes.
Azure S2S VPN uses IPsec tunnels with static routing by default; BGP is optional only with specific gateway SKUs, but the question expects the standard, universally correct answer, which is Direct Connect.
Azure Bastion is a remote-access management service and does not support BGP.
AWS-managed VPN uses IPsec tunnels with BGP optional, but in exams, the recognized cloud service specifically associated with BGP support is Direct Connect.
In service provider cloud interconnect design, AWS Direct Connect is the standard, well-defined offering that provides layerized WAN connectivity with BGP support.

NEW QUESTION: 58



Refer to the exhibit. An engineer must configure redundancy by deploying three Cisco vSmart Controllers in each data center. Which two actions must be taken to configure controllers vSmart1 and vSmart4? (Choose two.)

A. Run the max-control-connections 2 command on vSmart4.

B. Run the max-control-connections 2 command on vSmart1.

C. Run the system controller-group-id 2 command on vSmart4.

D. Run the system controller-group-id 1 command on vSmart1.

E. Run the system controller-group-id 4 command on vSmart4.

Answer: (SHOW ANSWER)

In Cisco SD-WAN,vSmart controllers must be assigned to controller groupsso that edge routers can form redundant control-plane connections. Each data center in the diagram has its own group:

* New York DC # Controller group-ID 1(vSmart1, vSmart2, vSmart3)

* Los Angeles DC # Controller group-ID 2(vSmart4, vSmart5, vSmart6)

To configure the controllers correctly:

vSmart1

It resides in theNew York DC, so it must be assigned tocontroller-group 1.

Required command:

system controller-group-id 1

This corresponds toOption D.

vSmart4

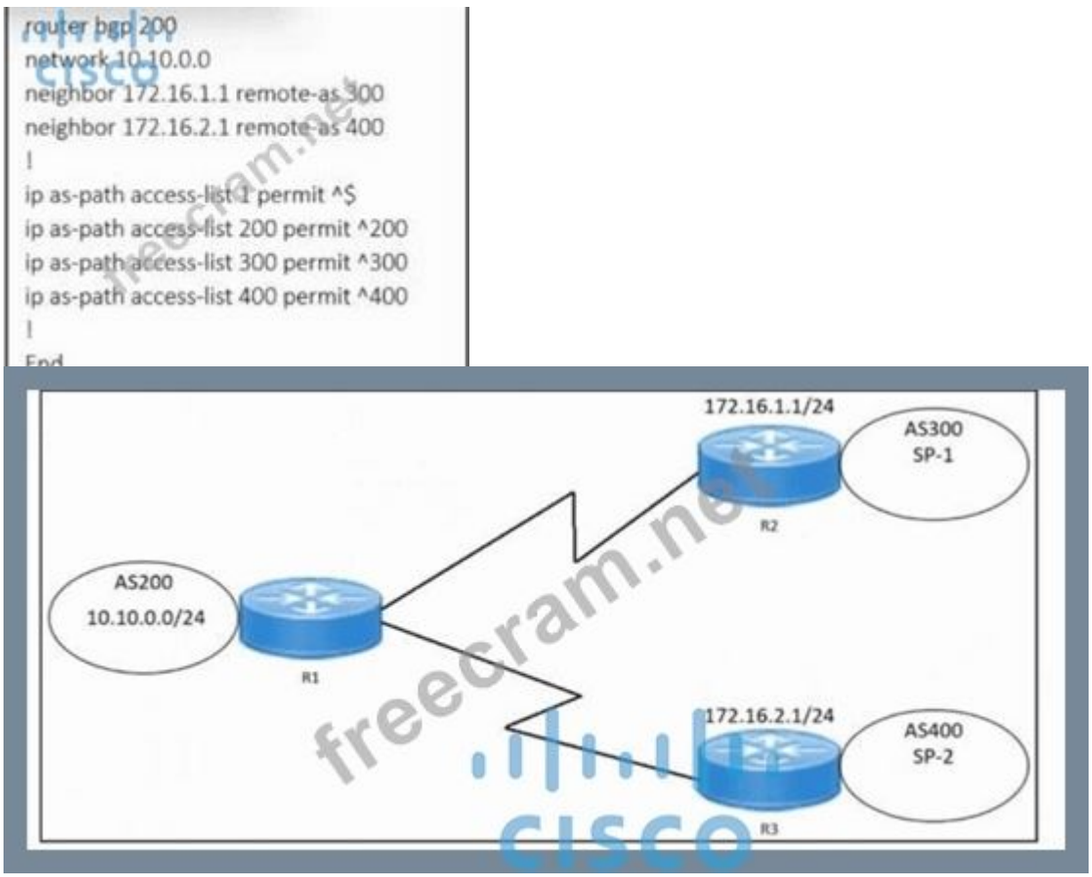
It resides in theLos Angeles DC, so it must be assigned tocontroller-group 2.

Required command:

system controller-group-id 2

This corresponds toOption C.
Why Other Options Are Incorrect
* A and B:The command max-control-connections is configured onedge routers, not vSmart controllers.
* E:Controller-group-id 4 does not exist in this design; only group 1 and group 2 are shown.

NEW QUESTION: 59
What is the primary focus of NFVI MANO in network assurance?
A. Direct hardware access for applications
B. Physical network configurations
C. Encrypting user data
D. Managing network functions virtualization infrastructure
Answer: (SHOW ANSWER)

NEW QUESTION: 60


Refer to the exhibit. An engineer must configure multihoming between router R1 and service providers SP-1 and SP-2. Locally generated routes must be advertised to the service providers, and should prevent the risk that the local autonomous system becomes a transit AS for Internet traffic. Which two commands must be run on R1 to complete the configuration? (Choose two.)
A. neighbor 172.16.1.1 filter-list 300 out
B. neighbor 172.16.2.1 filter-list 400 out
C. neighbor 172.16.1.1 filter-list 1 out

D. neighbor 172.16.2.1 filter-list 1 out
E. neighbor 172.16.1.1 filter-list 200
Answer: (SHOW ANSWER)
R1 (AS 200) is multihomed to:
* SP-1 in AS 300 via neighbor172.16.1.1
* SP-2 in AS 400 via neighbor172.16.2.1
R1 must:
* Advertiseonly locally originated prefixes(its own network 10.10.0.0/24).
* NOTbecome atransit AS-i.e., R1 mustnotadvertise routes learned from one provider to the other.
The configuration includes AS-path access-lists:
ip as-path access-list 1 permit ^$
ip as-path access-list 200 permit ^200
ip as-path access-list 300 permit ^300
ip as-path access-list 400 permit ^400
* ^$ in AS-path ACL1matcheslocally originated routes(empty AS-path).
* ACLs 200, 300, and 400 match routes whose first AS in the path is 200, 300, or 400 respectively (used if we needed to match those provider or customer routes).
To ensure each upstream provider only receiveslocally originatedroutes, we apply AS-path ACL1as an outbound filter-liston each external BGP neighbor:
router bgp 200
neighbor 172.16.1.1 remote-as 300
neighbor 172.16.1.1 filter-list 1 out # only advertise local prefixes to SP-1 neighbor 172.16.2.1 remote-as 400 neighbor 172.16.2.1 filter-list 1 out # only advertise local prefixes to SP-2 This way:
* Routes learned from SP-1 (AS 300) willnotbe advertised to SP-2 (AS 400) because their AS-path will begin with 300, not empty, so they fail ACL 1.
* Similarly, routes from SP-2 will not be sent to SP-1.
* Only R1's own prefixes are exported, preventing AS 200 from becoming a transit network.

NEW QUESTION: 61
Logging with syslog is important for:
A. Network performance tuning
B. Collecting and analyzing system events
C. Enhancing user experience
D. Direct packet routing
Answer: (SHOW ANSWER)

NEW QUESTION: 62
What is used to protect a web server against a DDoS attack?
A. Web Application Firewall
B. Device Authorization Control
C. Network Access Control
D. Wi-Fi Protected Access
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation
AWeb Application Firewall (WAF)protects HTTP/HTTPS applications against:
* DDoS attacks (layer 7)
* Bot traffic
* Request floods
* SQL injection, XSS, OWASP Top 10 threats
Other options:
* Device Authorization Control # device authentication, not DDoS
* NAC # endpoint authorization, not DDoS
* WPA # Wi-Fi protection, irrelevant to web servers
Thus, the correct protection mechanism for web servers isA. Web Application Firewall.

NEW QUESTION: 63
Which of the following is an advantage of using RESTCONF over NETCONF for network configuration?
A. RESTCONF provides more robust security features than NETCONF.
B. RESTCONF operates over HTTP, making it more web-friendly than NETCONF.
C. RESTCONF uses binary data encoding, making it faster than NETCONF.
D. NETCONF supports more data models than RESTCONF.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Direct Connect offers which of the following advantages over traditional internet connections?
A. Higher latency
B. Increased security
C. More consistent network performance
D. Reduced bandwidth
Answer: (SHOW ANSWER)

NEW QUESTION: 65

Refer to the exhibit. An engineer must configure an IPsec VPN connection between site 1 and site 2. The ISAKMP policy for the phase 1 negotiations of the tunnel must use AES and SHA-256. This configuration was applied to both PE routers; however, the tunnel fails to come up:

crypto isakmp policy 10
encryption 3des
hash md5
authentication pre-share
group 12

Which two commands must be run on router PE1 to resolve the issue? (Choose two.)

A. group 10
B. encryption aes
C. encryption sha256
D. hash aes
E. hash sha256

Answer: (SHOW ANSWER)

Phase 1 of an IPsec tunnel (ISAKMP/IKE) must havematching proposalson both peers for:

* Encryption algorithm
* Hash (integrity) algorithm
* Authentication method
* DH group

The requirement states thatAESandSHA-256must be used. The current configuration uses:

* encryption 3des # incorrect (must be AES)
* hash md5 # incorrect (must be SHA-256)

To meet the requirement, we must modify the ISAKMP policy:

crypto isakmp policy 10
encryption aes # change 3DES to AES
hash sha256 # change MD5 to SHA-256
authentication pre-share
group 12

Therefore, the necessary commands on PE1 are:

* encryption aes# optionB
* hash sha256# optionE

Options C and D are invalid syntax (encryption sha256 and hash aes are not supported). Changing the DH group (A) is not required by the problem statement and would not by itself fix the mismatch related to encryption and hash algorithms.

NEW QUESTION: 66
Virus detectors are used to:
A. Identify and eliminate malware
B. Manage user access
C. Monitor network bandwidth
D. Encrypt traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 67


Refer to the exhibit. An engineer must configure an IPsec VPN connection between site 1 and site 2. The indicated configuration was applied to router R1; however, the tunnel fails to come up. Which command must be run on R1 to resolve the issue?
A. set peer 10.1.0.1
B. set peer 192.168.20.2
C. set peer 192.168.10.1
D. set peer 10.2.0.1
Answer: (SHOW ANSWER)
For asite-to-site IPsec VPN, each peer must point to thereachable IP address of the remote VPN endpoint
-that is, the IP address on the WAN/Internet-facing interface of the remote router.
From the diagram:
* R1 outside (toward Internet):192.168.10.1
* R2 outside (toward Internet):192.168.20.2
* Inside LANs:
* Site 1:10.1.0.0/24
* Site 2:10.2.0.0/24
The crypto map on R1 uses:
crypto map mymap 10 ipsec-isakmp
set transform-set myset

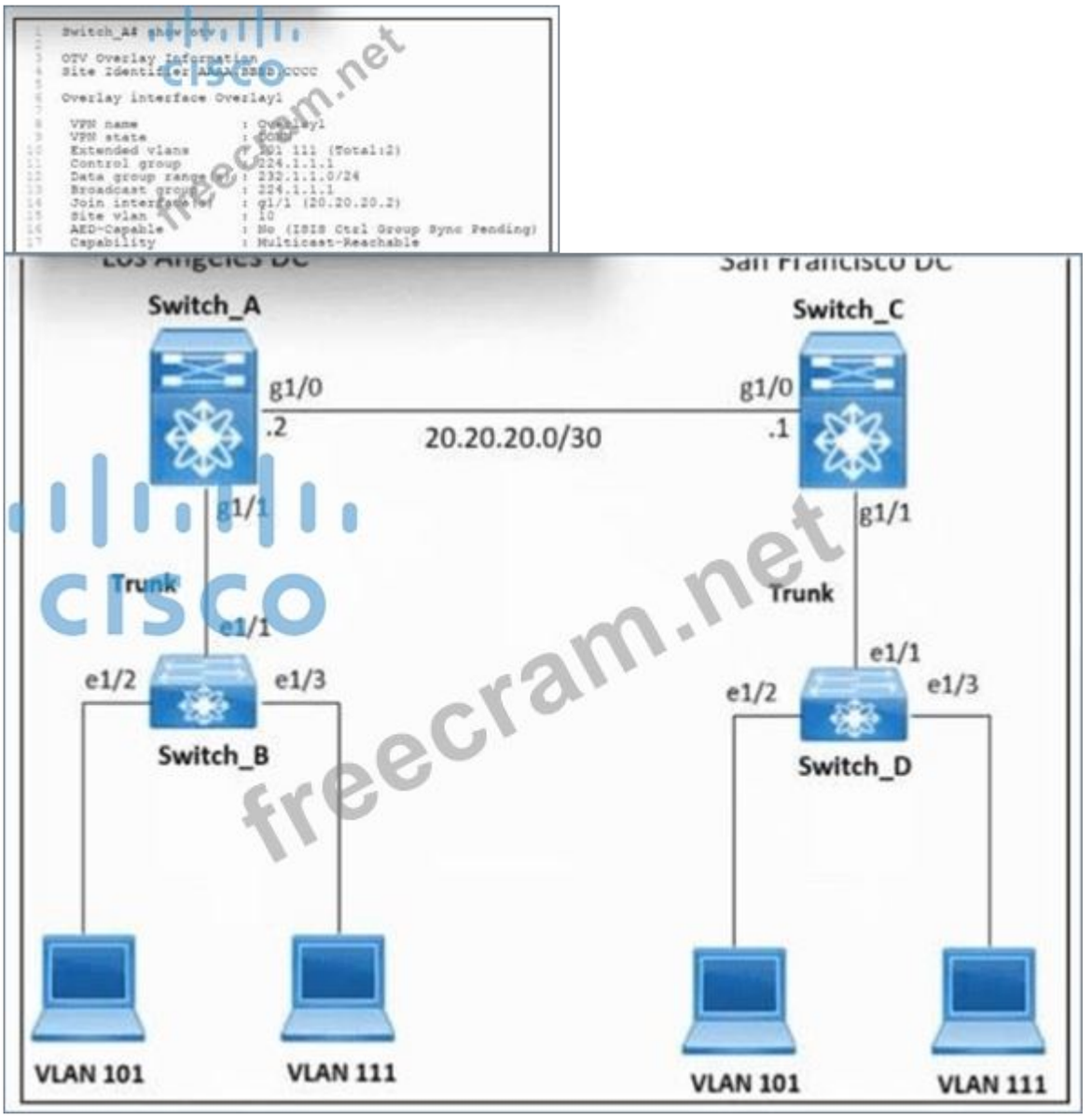
match address 101
set peer <REMOTE_PEER_IP>
The <REMOTE_PEER_IP> must be the IP address where R1 can actually reach the IPsec peer, which is R2's Internet-facing interface192.168.20.2.
If the peer were configured with a LAN IP such as 10.2.0.1 (site 2's internal gateway), IKE packets would never reach the remote router because that address is not routable over the Internet.
Therefore, the correct command to bring up the VPN is:
set peer 192.168.20.2
* Option A (10.1.0.1)- local LAN IP (R1's side), not the remote endpoint.
* Option C (192.168.10.1)- R1's own WAN IP, not the remote peer.
* Option D (10.2.0.1)- remote LAN IP, not reachable directly over the Internet.

NEW QUESTION: 68
Which cloud service model would best suit an organization looking to host its own web applications?
A. FaaS
B. PaaS
C. IaaS
D. SaaS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 69
Direct connect and MPLS differ in that:
A. Direct connect offers private connectivity to cloud services, while MPLS provides a protocol for efficient network routing
B. MPLS offers direct access to cloud providers
C. Direct connect is a routing protocol
D. MPLS can only be used in public internet connections
Answer: (SHOW ANSWER)

NEW QUESTION: 70
uRPF is utilized to combat which type of security threat?
A. DDoS attacks
B. Viruses
C. Insider threats
D. Spoofing attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 71



Refer to the exhibit. An engineer is troubleshooting an issue where Cisco switch Switch_A fails to establish OTV connectivity to Cisco switch Switch_C. What is the cause of the issue?

A. The broadcast group must be 232.1.1.0.

B. The join interface must be g1/0.

C. The control group must be 232.1.1.0.

D. The join interface must be e1/1.

Answer: (SHOW ANSWER)

In Cisco Overlay Transport Virtualization (OTV), thejoin interfaceis the Layer 3 interface that connects the edge device to thetransport network(the routed core / WAN) where multicast groups (control, data, broadcast) are reachable.

From the topology:

* Interfaceg1/0on Switch_A is connected to the routed 20.20.20.0/30 link toward Switch_C (the transport

/ WAN).

* Interfaceg1/1is a trunk toward Switch_B and carries extended VLANs (101, 111), so it belongs to the internal site-facing side, not the transport.
In the show otv output, the join interface is incorrectly configured asg1/1 (20.20.20.2), which is an internal trunk and not the correct routed interface to the OTV transport network. Because the join interface does not face the multicast-enabled transport, OTV cannot establish adjacency and the VPN state remains DOWN.
Correct configuration should use:
otv join-interface GigabitEthernet1/0
Options A and C about group addresses are not the issue; addresses shown (224.x for control/broadcast and
232.x for data group range) are valid multicast ranges. Option D (e1/1) is also an internal access/trunk interface and not the WAN transport interface.

NEW QUESTION: 72
Troubleshooting ACI involves understanding:
A. Basic routing protocols only
B. The application-centric policies and their impact on network behavior
C. Only the physical layer of the network
D. The brand of hardware being used
Answer: (SHOW ANSWER)

NEW QUESTION: 73
What is the purpose of VNF data plane redundancy?
A. To decrease network performance
B. To increase the cost of infrastructure
C. To simplify network management
D. To ensure data plane resiliency through placement and network resiliency
Answer: (SHOW ANSWER)

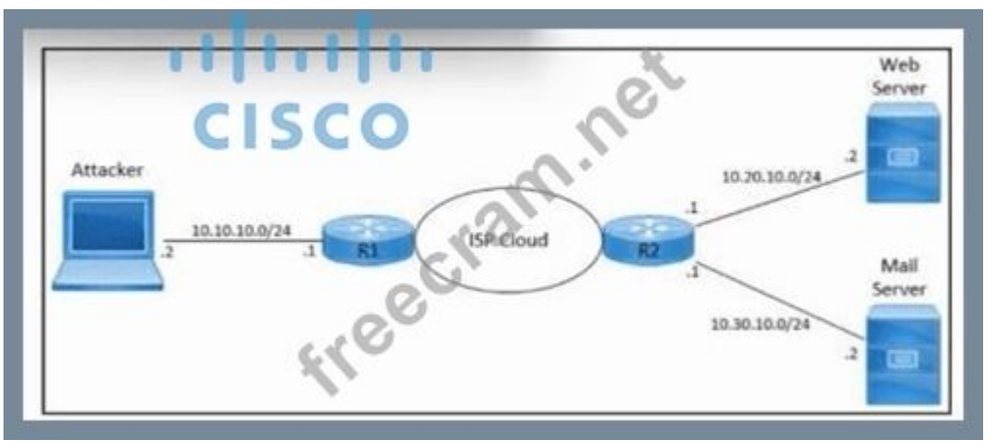
NEW QUESTION: 74
Which of the following statements accurately describes the difference between NFV and VNF?
A. NFV focuses on the deployment of network functions, while VNF refers to the specific network functions being deployed.
B. NFV is a software update mechanism, whereas VNF is a hardware-based function.
C. NFV refers to network failures, while VNF refers to the virtualization of those failures.
D. VNF and NFV are the same and can be used interchangeably.
Answer: (SHOW ANSWER)

NEW QUESTION: 75
What role does NFVI MANO play in service assurance?
A. Decreasing automation in network deployment

B. Reducing data storage capabilities
C. Managing physical network infrastructures only
D. Orchestrating resources and network services
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following are key components of network assurance? (Select two)
A. Manual network configurations
B. Physical network mapping
C. NFVI MANO
D. VNF workloads
Answer: (SHOW ANSWER)

NEW QUESTION: 77
A zero-day exploit refers to:
A. A bug that is fixed immediately upon discovery
B. An attack that occurs on the same day a security patch is released
C. A flaw that has been known for at least a day
D. A vulnerability that the attacker discovers before the developer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78


Refer to the exhibit. An engineer must stop DDoS attacks on web and mail servers by using an ACL. Which two commands must be run on router R17? (Choose two.)

A. access-list 101 deny ip 10.10.10.2 255.255.255.255 10.20.10.2 255.255.255.255

B. access-list 101 deny ip 10.0.0.0 0.255.255.255 10.10.0.2 0.0.0.0

C. access-list 101 deny ip 10.10.10.2 255.255.255.255 10.30.10.2 255.255.255.255

D. access-list 101 deny ip 10.10.10.2 0.0.0.0 10.20.10.2 0.0.0.0

E. access-list 101 deny ip 10.10.10.2 0.0.0.0 10.30.10.2 0.0.0.0

Answer: (SHOW ANSWER)

The attacker's IP is:

* 10.10.10.2

The servers under attack are:

* Web Server:10.20.10.2

* Mail Server:10.30.10.2

We must denytraffic from attacker # servers.

Correct ACL format useshost wildcards (0.0.0.0):

deny ip 10.10.10.2 0.0.0.0 10.20.10.2 0.0.0.0

deny ip 10.10.10.2 0.0.0.0 10.30.10.2 0.0.0.0

These matchD and E.

NEW QUESTION: 79

Software accelerated virtual switch technologies like DPDK and VPP aim to:

A. Decrease network security

B. Slow down packet processing

C. Increase physical network dependency

D. Improve network function virtualization performance

Answer: (SHOW ANSWER)

NEW QUESTION: 80

Refer to the exhibit. An engineer must deploy a standalone Cisco NFVIS. These configurations were performed already:

Deployed the virtual machine

Configured the hostname and IP address

Configured dual WAN support

When the engineer attempts to access the NFVIS portal, the API returns a 401 Unauthorized error. What is the cause of the issue?

A. The default admin password must be reset.

B. Portal access must be enabled via SSH.

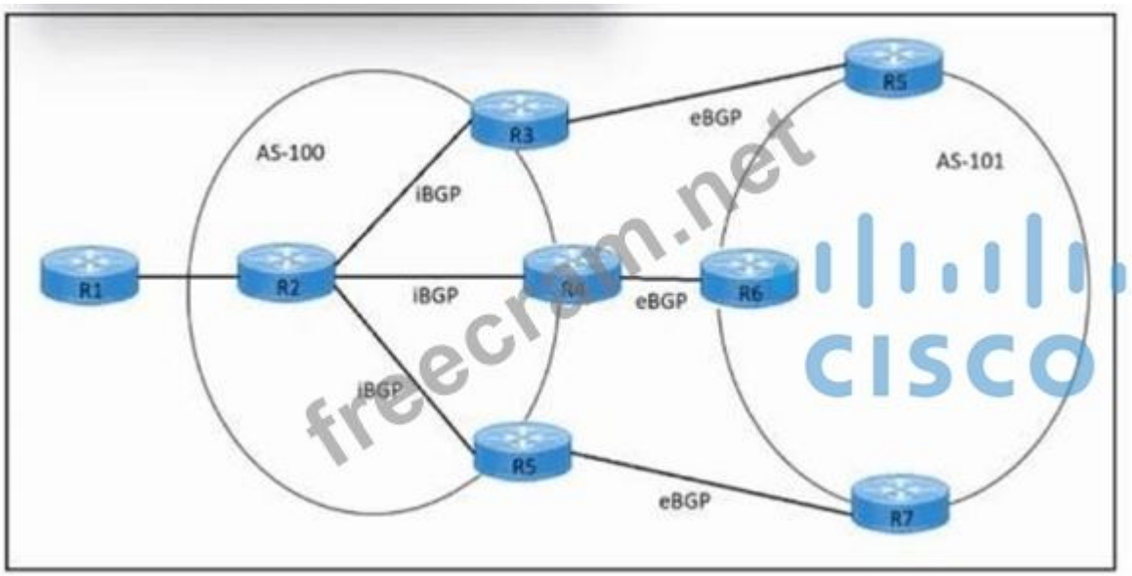
C. The Tomcat service must be restarted.
D. The browser certificate must be renewed.
Answer: (SHOW ANSWER)
Cisco NFVIS follows strict security controls. After a fresh deployment:
* Thedefault admin credentials are considered insecure.
* NFVIS requires the administrator toreset the default password on first login(typically via console or SSH).
* Until the password is changed,REST API and web-portal access are denied, and attempts to access the portal or API returnHTTP 401 Unauthorized, even if the default credentials are provided.
This mechanism prevents use of factory-default passwords in production and is explicitly documented as a mandatory post-install step.
The other options are not the cause of a 401 error:
* Enabling portal via SSH (B) is not required; HTTPS access is enabled by default once credentials are valid.
* Restarting Tomcat (C) would address service availability issues (e.g., 5xx errors), not authentication.
* Browser certificates (D) affect trust warnings (e.g., HTTPS certificate errors), not 401 Unauthorized.

NEW QUESTION: 81
What is Virtualized Architecture primarily used for in the context of IT infrastructure?
A. Decreasing system security
B. Increasing physical hardware costs
C. Simplifying legal compliance
D. Reducing the need for physical hardware
Answer: (SHOW ANSWER)

NEW QUESTION: 82
What does Cisco Always-On Cloud DDoS use to protect against DDoS attacks?
A. Load balancing
B. Botnet zombies
C. Traffic mirroring
D. Scrubbing centers
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Cisco SP Security Knowledge Cisco Always-On Cloud DDoS Protection is a cloud-based, carrier-grade security service used by service providers to protect customers from volumetric and application-layer DDoS attacks.
Its core protection mechanism is the use ofglobal scrubbing centers, which:
* Receive diverted attack traffic
* Scrub (clean) malicious packets
* Forward clean traffic back to the customer

* Use behavioral analysis and real-time detection
* Protect against volumetric, TCP state-exhaustion, and application-layer attacks Why other answers are incorrect:
* Load balancing (A)doesnotmitigate DDoS attacks; it distributes traffic across servers.
* Botnet zombies (B)aresourcesof DDoS attacks, not protection.
* Traffic mirroring (C)is used for analysis and monitoring, not active DDoS protection.

NEW QUESTION: 83
Which type of cyberattack does Cisco Umbrella DNS-layer security effectively help mitigate?
A. Phishing and malware-based attacks
B. DDoS attacks targeting specific servers
C. Brute force attacks on user accounts
D. Advanced persistent threats and zero-day exploits
Answer: (SHOW ANSWER)
Cisco Umbrella DNS-layer security:
* Blocks malicious domains used inphishing,malware,C2 communications, andransomware
* Stops threatsbeforeconnections are made
* Uses DNS-based filtering and threat intelligence
It doesnotmitigate:
* DDoS (needs scrubbing centers)
* Brute force login attempts
* Zero-day exploits directly
Thus,Ais correct.

NEW QUESTION: 84


Refer to the exhibit. An engineer must configure iBGP multipath load sharing across three paths. Which two commands must be run on router R2? (Choose two.)
A. router bgp 100

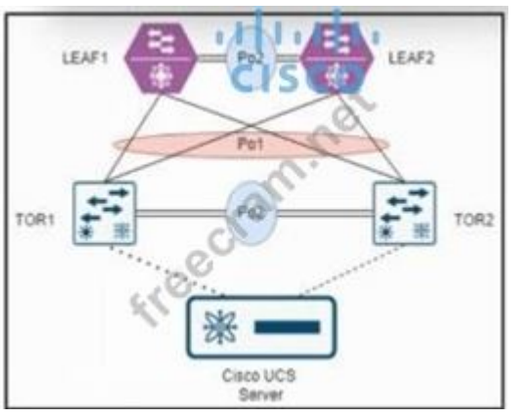
B. ip load-sharing ibgp 3
C. maximum-paths ibgp 3
D. router bgp 101
E. ip load-sharing per-destination
Answer: (SHOW ANSWER)
RouterR2is insideAS 100and has three iBGP paths (via R3, R4, R5) toward AS 101. To performiBGP multipathacross these three equal-cost paths, BGP must:
* Run the correct BGP process forAS 100
* Allow installation of multiple iBGP paths in the routing table
This is done with:
router bgp 100
maximum-paths ibgp 3
* router bgp 100- enters the BGP process for AS 100 (correct AS per diagram).
* maximum-paths ibgp 3- tells BGP to keep up to 3 iBGP paths to the same destination, enabling CEF to load-share across them.
Other options:
* ip load-sharing ibgp 3- not a valid command.
* router bgp 101- wrong AS number.
* ip load-sharing per-destination- controls CEF hashing but does not enable BGP to install multiple iBGP paths by itself.

NEW QUESTION: 85
Software-accelerated virtual switches like DPDK and VPP enhance VNF performance by:
A. Lowering network throughput
B. Increasing network latency
C. Reducing the need for high availability
D. Improving packet processing speed
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Which command must be run on a Cisco IOS device to configure six parallel iBGP and eBGP routes that can be installed into a routing table?
A. maximum paths bgp 6
B. multipath eibgp 6
C. maximum paths bgp routers 6
D. maximum-paths eibgp 6
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Cisco SP Core Optimization Knowledge Cisco IOS supportsBGP Multipathfor installing multiple equal-cost BGP routes (both iBGP and eBGP) into the routing table. The correct global BGP command syntax to set the number of allowable parallel BGP paths is:

maximum-paths <number>
For BGP specifically, the form is:
maximum-paths bgp <number>
This enables the router to install up to the specified number of equal-cost BGP routes (iBGP and eBGP) into the RIB and then potentially into the FIB.
Setting:
maximum-paths bgp 6
allowssixparallel ECMP paths learned via BGP-this matches the requirement in the question.
Why the other options are incorrect
* B. multipath eibgp 6Not a valid Cisco IOS command.
* C. maximum paths bgp routers 6Invalid syntax.
* D. maximum-paths eibgp 6The correct keyword isbgp, noteibgp.Cisco does not use "eibgp" in this context; IOS supports BGP multipath across iBGP/eBGP automatically when configured under maximum-paths bgp.

NEW QUESTION: 87



Refer to the exhibit. An engineer must connect switch TOR1 and switch TOR2 to switch LEAF1 and switch LEAF2 by using double-sided vPCs. LEAF1 and LEAF2 are already configured as vPC peers. Which action must be taken next to complete the configuration?
A. Add all the switches to the fabric.
B. Configure peering between LEAF1 and LEAF2 and TOR1 and TOR2.
C. Configure MSTP between TOR1 and TOR2.
D. Configure a vPC between TOR1 and TOR2.
Answer: (SHOW ANSWER)
In Cisco data center and cloud-scale designs, adouble-sided vPC(also called vPC-to-vPC) is used when both ends of a Layer 2 port channel are formed by a pair of switches that operate as vPC peers. In this model:
* On the aggregation or leaf side, two switches (in this case,LEAF1 and LEAF2) form a vPC domain with a vPC peer-link and keepalive.
* On the access or ToR side, two switches (in this case,TOR1 and TOR2) must also form their ownvPC domainwith a peer-link and vPC keepalive.

* The port-channel that interconnects the two vPC domains is then configured as a vPC on both sides, creating a vPC-to-vPC topology.
The problem statement specifies thatLEAF1 and LEAF2 are already configured as vPC peers. For a double-sided vPC to work, the other side (TOR1 and TOR2) must also behave as a single logical entity for the downstream Cisco UCS server and for the upstream vPC connection towards LEAF1 and LEAF2. This is only achieved when TOR1 and TOR2 are configured as vPC peers with:
* A vPC domain ID
* A vPC peer-link between TOR1 and TOR2
* vPC member port-channels towards LEAF1 and LEAF2 and towards the Cisco UCS server
Therefore, the next required step is to configure avPC between TOR1 and TOR2.
Evaluation of the options:
* Option A, "Add all the switches to the fabric," is generic and not specific to vPC configuration. It does not address the technical requirement to form a vPC domain on the ToR side.
* Option B, "Configure peering between LEAF1 and LEAF2 and TOR1 and TOR2," is incorrect because vPC peering is only configured between the two switches that form each vPC domain (LEAF1-LEAF2 and TOR1-TOR2), not across all four switches together.
* Option C, "Configure MSTP between TOR1 and TOR2," is not required for establishing a double-sided vPC. vPC designs rely on the vPC control plane and the peer-link, not on spanning-tree between the vPC peers for normal operation.
* Option D, "Configure a vPC between TOR1 and TOR2," correctly describes configuring TOR1 and TOR2 as a vPC pair (vPC domain with peer-link), which is the mandatory step to create a double-sided vPC topology with LEAF1 and LEAF2.

NEW QUESTION: 88
Evaluating WAN infrastructure connectivity, one should consider:
A. The scalability and flexibility of MPLS/segment routing
B. The availability and performance requirements of the application
C. The cost and complexity of IPsec VPNs only
D. The exclusive use of Direct Connect for all scenarios
Answer: (SHOW ANSWER)

NEW QUESTION: 89
BGP flowspec is primarily used for:
A. Encrypting data traffic
B. Distributing traffic flow specifications
C. Access control
D. Authentication
Answer: (SHOW ANSWER)