



Vendor: Cisco

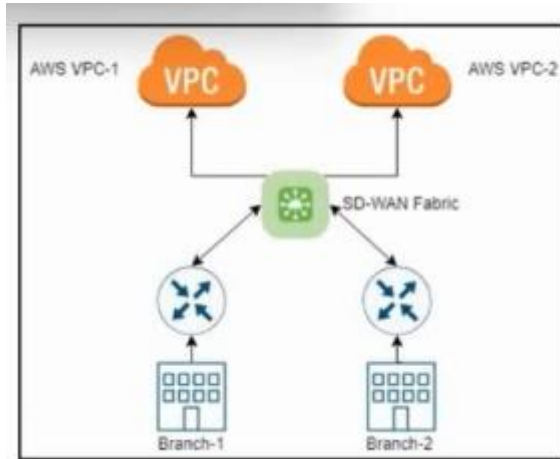
Exam Code: 300-540

Exam Name: Designing and Implementing Cisco Service
Provider Cloud Network Infrastructure

Version: DEMO

QUESTION 1

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: B

Explanation:

It is specifically designed to integrate Cisco SD-WAN with 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 of automatic cloud resource identification based on user credentials.

QUESTION 2

An engineer must design a cloud platform for managing IaC. The solution must be flexible, integrate with APIs, and allow for automation. What must be used?

- A. Cloud-based sandboxes
- B. Cisco with Terraform
- C. Cisco ThousandEyes
- D. Cisco AppDynamics

Answer: B

Explanation:

Infrastructure as Code (IaC) requires:

Declarative configuration

Automation

API-driven workflows

Multi-cloud capability

Integration with orchestration and provisioning tools

Terraform is a widely adopted IaC platform supporting:

Cloud automation (AWS, Azure, GCP, private clouds)

Cisco infrastructure provisioning (Nexus, ACI, IOS-XR, NSO, SD-WAN, etc.)

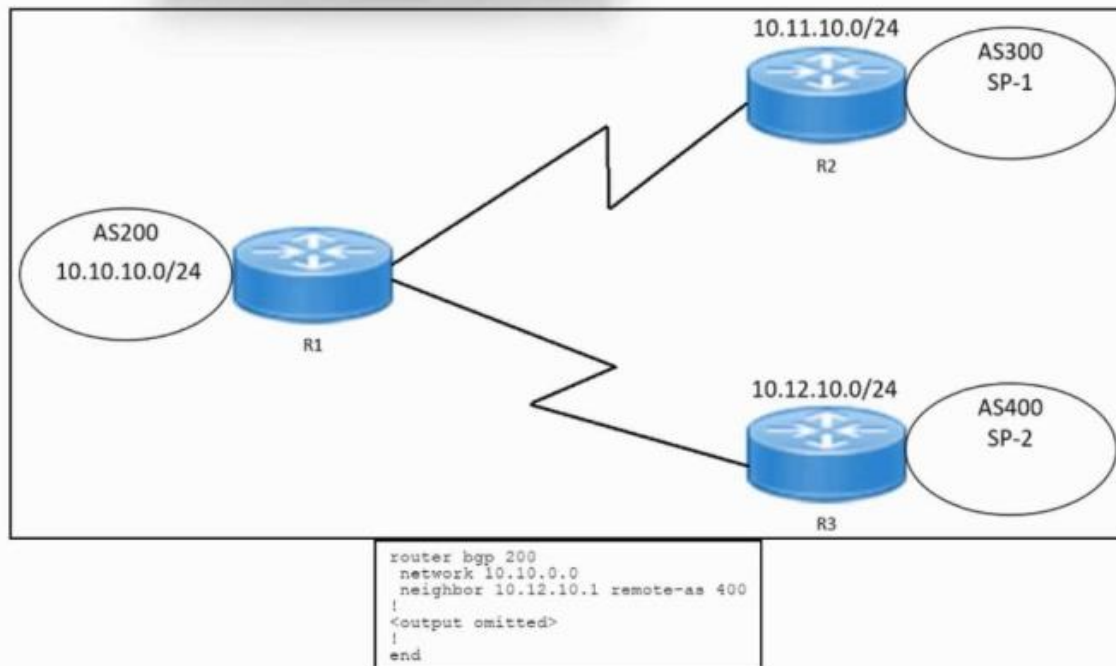
REST APIs and providers for programmability

Cisco provides official Terraform providers for multiple platforms, enabling full IaC operations.

This aligns exactly with SP cloud automation design principles.

QUESTION 3

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: B

Explanation:

On R1 (AS200), the requirement is:

Advertise locally generated routes (for example, 10.10.10.0/24 from AS200) Only toward SP-2, which peers on IP 10.12.10.1

Apply a policy (route-map) controlling what R1 advertises

In BGP, to control which locally originated routes are 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 is 10.12.10.1

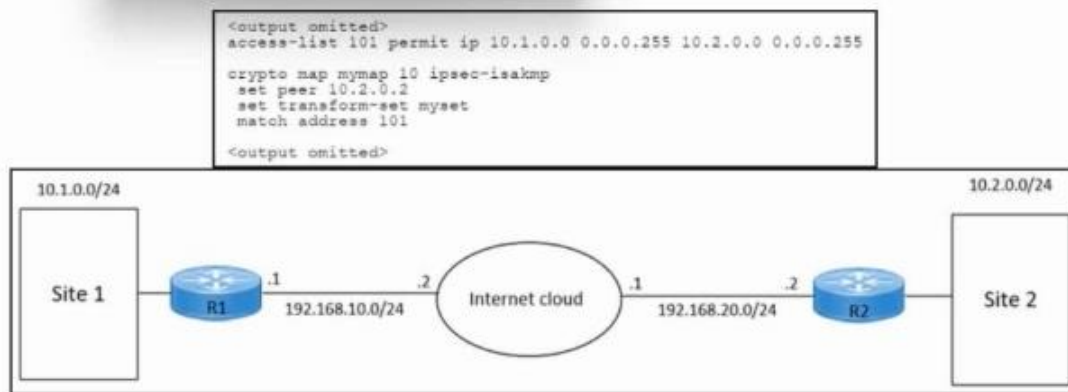
The route-map must be applied outbound

The command that accomplishes this is:

neighbor 10.12.10.1 route-map localonly out

QUESTION 4

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: B

Explanation:

For a site-to-site IPsec VPN, each peer must point to the reachable 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 interface 192.168.20.2.

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:

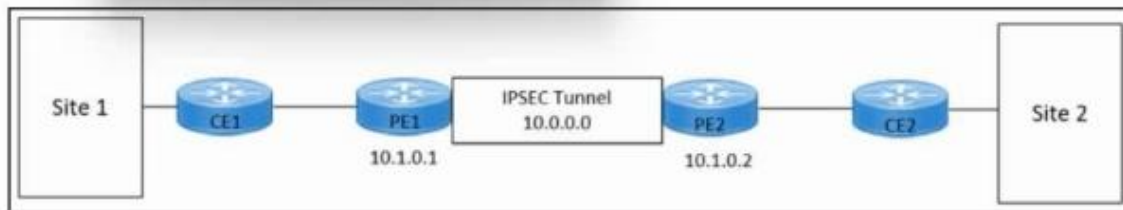
set peer 192.168.20.2

QUESTION 5

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: BE

Explanation:

Phase 1 of an IPsec tunnel (ISAKMP/IKE) must have matching proposals on both peers for:

Encryption algorithm
Hash (integrity) algorithm
Authentication method
DH group

The requirement states that AES and SHA-256 must 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 option B
```

```
hash sha256 option E
```

QUESTION 6

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: D

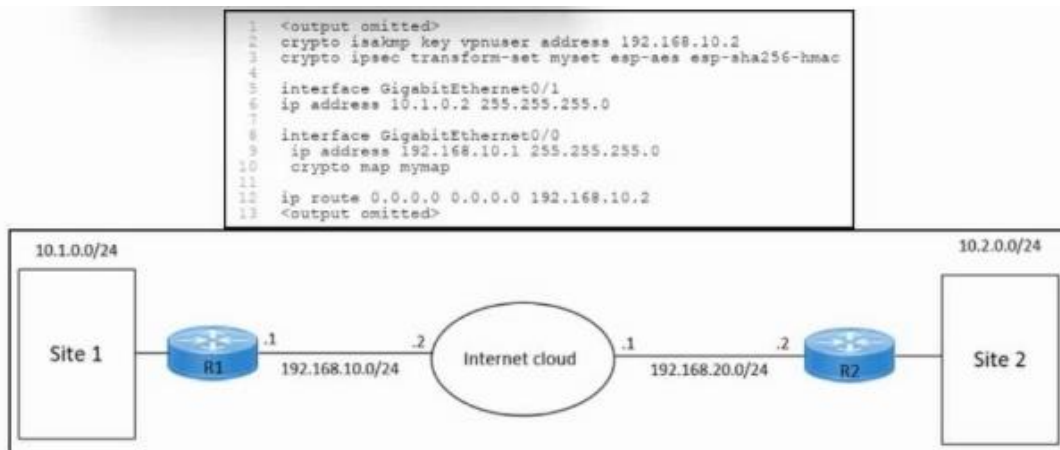
Explanation:

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 of global 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

QUESTION 7

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: B

Explanation:

For a site-to-site IPsec VPN, each peer must configure a pre-shared key tied to the public 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 to 192.168.10.2, 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

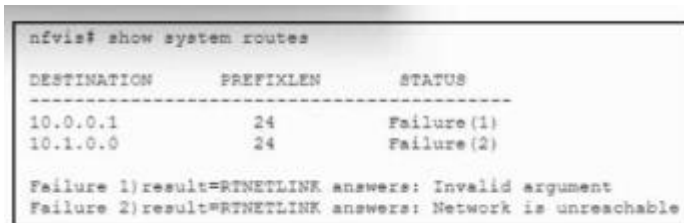
QUESTION 8

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?



DESTINATION	PREFIXLEN	STATUS
10.0.0.1	24	Failure(1)
10.1.0.0	24	Failure(2)

Failure 1) result=RTNETLINK answers: Invalid argument
Failure 2) result=RTNETLINK answers: Network is unreachable

- 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: A

Explanation:

Cisco NFVIS follows strict security controls. After a fresh deployment:

The default admin credentials are considered insecure.

NFVIS requires the administrator to reset 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 return HTTP 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.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14