



"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks.com

Warning: Keep connected with our support team for latest updates

Question: 1

What are the two advantages of deploying cloud-based Cisco SD-WAN controllers? (Choose two.)

- A. centralized control and data plane
- B. distributed authentication policies
- C. management of SLA
- D. infrastructure as a service
- E. centralized raid storage of data

Answer: C,D

Question: 2

An engineer is troubleshooting a certificate issue on vEdge. Which command is used to verify the validity of the certificates?

- A. show control local-properties
- B. show control summary
- C. show certificate installed
- D. show certificate status

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr->

book/operational-cmd.html#wp2835720000

Question: 3

What is a benefit of the application-aware firewall?

- A. It blocks traffic by MAC address
- B. It blocks traffic by MTU of the packet.
- C. It blocks traffic by application.
- D. It blocks encrypted traffic

Answer: C

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xr-16-9/sec-data-zbf-xr-16-9-book/sec-data-zbf-xr-16-9-book_chapter_0100100.html

Question: 4

When VPNs are grouped to create destination zone in Zone-Based Firewall, how many zones can a single VPN be part of?

- A. two
- B. four
- C. one
- D. three

Answer: C

Explanation:

Reference:

https://sdwandocs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/Enterprise_Firewall_with_Application_Awareness

Question: 5

Which attributes are configured to uniquely Identify and represent a TLOC route?

- A. system IP address, link color, and encapsulation
- B. firewall, IPS, and application optimization
- C. site ID, tag, and VPN
- D. origin, originator, and preference

Answer: A

Explanation:

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf>

Question: 6

Which device information is required on PNP/ZTP to support the zero-touch onboarding process?

- A. serial and chassis numbers
- B. interface IP address
- C. public DNS entry
- D. system IP address

Answer: A

Explanation:

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sd-wan-wan-edge-onboarding-deploy-guide-2020jan.pdf>

Question: 7

Which configuration step is taken on vManage after WAN Edge list is uploaded?

- A. Send the list to controllers
- B. Enable the ZTP process
- C. Verify the device certificate
- D. Set the device as valid

Answer: D

Explanation:

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf>

device state must be moved from staging to valid. In vManage under Configuration > Certificates > WAN Edge List, select the WAN Edge device(s) and change the state to valid under the Validity column and click Send to Controllers

Question: 8

When software is upgraded on a vManage NMS, which two image-adding options store images in a

local vManage software repository? (Choose two.)

- A. To be downloaded over a SMTP connection
- B. To be downloaded over a SNMP connection
- C. To be downloaded over an out-of-band connection
- D. To be downloaded over a control plane connection
- E. To be downloaded over an ICMP connection

Answer: C,D

Explanation:

Reference: <https://sdwan->

[docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Maintenance/Software_Repository](https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Maintenance/Software_Repository)

Question: 9

Which policy configures an application-aware routing policy under Configuration > Policies?

- A. Localized policy
- B. Centralized policy
- C. Data policy
- D. Control policy

Answer: B

Explanation:

Reference: [https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-](https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=451)

[4.pdf#page=451](https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=451)

Question: 10

What is a default protocol for control plane connection?

- A. IPsec
- B. HTTPS
- C. TLS
- D. DTLS

Answer: D

Explanation:

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-

[WAN_Release_16.3/05Security/02Configuring_Security_Parameters](https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/05Security/02Configuring_Security_Parameters)

Question: 11

Which logs verify when a device was upgraded?

- A. Audit
- B. Email
- C. ACL
- D. SNMP

Answer: A

Explanation:

Reference: https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Monitor/Audit_Log

Question: 12

Which command displays BFD session summary information per TLOC on vEdge routers?

- A. show bfd history
- B. show bfd summary
- C. show bfd sessions
- D. show bfd tloc-summary-list

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/sdwan-cr-book_chapter_0100.html

Question: 13

Which Cisco SD-WAN WAN Edge platform supports LTE and Wi-Fi?

- A. vEdge2000
- B. ASR1001
- C. CSR 1000v
- D. ISR 1101

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/dam/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/q-and-a-c67-739639.pdf>

Question: 14

Which component of the Cisco SD-WAN control plane architecture facilitates the storage of certificates and configurations for network components?

- A. vSmart
- B. vBond
- C. WAN Edge
- D. vManage

Answer: D

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html>

Question: 15

Which type of route advertisement of OMP can be verified?

- A. OMP, VPN, and origin
- B. Origin, TLOC, and VPN
- C. Origin, TLOC, and service
- D. OMP, TLOC and service

Answer: D

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-2.pdf#page=122>

Question: 16

Which OSPF command makes the WAN Edge router a less preferred exit from a site with a dual WAN Edge design?
A)

```
vpn vpn-id
router
ospf
area number
range prefix/length
```

B)

```
vpn vpn-id
router
ospf
max-metric
```

C)

```
vpn vpn-id
router
ospf
area number
no-summary
```

D)

```
vpn vpn-id tauter
O»pf a red numbes' n**a
no summary
```

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 17

Which two services are critical for zero touch provisioning on-boarding? (Choose two)

- A. SNMP
- B. DNS
- C. DHCP
- D. AAA

E. EMAIL

Answer: B,C

Explanation:

Reference: <https://www.grandmetric.com/2020/03/23/zero-touch-provisioning-ztp-cisco-sd-wan-work/>

Question: 18

Refer to the exhibit.

PEER TYPE	PEER PROTO UPTIME	PEER ID	PEER DOL	PEER SYSTE	SITE WIP ID	PEER DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PUBLIC PORT	CONTROLLER LOCAL COLOR	GROUP STATE
vbond	dtls	-	0	0	0	1.3.25.25	12346	1.3.25.25	12346	gold	connect	0
vbond	dtls	-	0	0	0	1.3.25.25	12346	1.3.25.25	12346	silver	connect	a

An engineer is troubleshooting a control connection Issue. What does "connect" mean in this how control connections output?

- A. Control connection is down
- B. Control connection is connected
- C. Control connection attempt is in progress
- D. Control connection is up

Answer: C

Explanation:

Reference: <https://community.cisco.com/t5/networking-documents/sd-wan-routers-troubleshoot-control-connections/ta-p/3813237>

Question: 19

Which hardware component is involved in the Cisco SD-WAN authentication process for ISR platforms?

- A. TPMD
- B. ZTP
- C. TPC
- D. SUDI

Answer: D

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf>

Question: 20

Which alarm setting is configured to monitor serious events that affect but do not shut down, the operation of a network function?

- A. Minor
- B. Major
- C. Medium
- D. Critical

Answer: B

Explanation:

Reference: https://sdwan-docs.cisco.com/Product_Documentation/vManage_How-Tos/Troubleshooting/Monitor_Alarms

Question: 21

Refer to the exhibit.

Hostname	State	System IP	Reachability	Site ID	Device Model	BFD	Control
BR1-VEEDGE1	✓	10.3.0.1	reachable	300	vEdge Cloud	8	5

What does the BFD value of 8 represent?

- A. number of BFD sessions
- B. hello timer of BFD session
- C. poll-interval of BFD session.
- D. dead timer of BFD session

Answer: A

Explanation:

Question: 22

How is the scalability of the vManage increased in Cisco SD-WAN Fabric?

- A. Increase licensing on the vManage
- B. Deploy multiple vManage controllers in a cluster
- C. Deploy more than one vManage controllers on different physical server.
- D. Increase the bandwidth of the WAN link connected to the vManage

Answer: B

Explanation:

Question: 23

Which component of the Cisco SD-WAN control plane architecture should be located in a public Internet address space and facilitates NAT-traversal?

- A. vBond
- B. WAN Edge
- C. vSmart
- D. vManage

Answer: A

Explanation:

Reference:

https://www.cisco.com/c/dam/global/da_dk/assets/pdfs/cisco_virtual_update_cisco_sdwan_viptela.pdf

Question: 24

Refer to the exhibit.

```
policy
  policer cnp
    rate 1000000
    burst 15000
    exceed drop
  !
access-list acl-guest
  sequence 1
  match
    source-ip 172.16.10.0/24
    destination-ip 172.16.20.0/24
    destination-port 20
    protocol 6
  !
  action accept
  policer cnp
  !
  !
default-action drop
```

Which QoS treatment results from this configuration after the access list acl-guest is applied inbound on the vpn1 interface?

- A. A UDP packet sourcing from 172.16.20.1 and destined to 172.16.10.1 is accepted
- B. A TCP packet sourcing from 172.16.10.1 and destined to 172.16.20.1 is dropped
- C. A UDP packet sourcing from 172.16.10.1 and destined to 172.16.20.1 is dropped.
- D. A TCP packet sourcing from 172.16.20.1 and destined to 172.16.10.1 is accepted

Answer: C

Explanation:

Question: 25

Which component of the Cisco SD-WAN architecture oversees the control plane of overlay network to establish, adjust, and maintain the connections between the WAN Edge devices that form the Cisco SD-WAN fabric?

- A. APIC-EM
- B. vManage
- C. vSmart
- D. vBond

Answer: C

Explanation:

Cisco vSmart Controller

The Cisco vSmart Controller oversees the control plane of the Cisco SD-WAN overlay network, establishing, adjusting and maintaining the connections that form the Cisco SD-WAN fabric.

Question: 26

Which command verifies a policy that has been pushed to the vEdge router?

- A. vEdge# show running-config data policy
- B. vEdge# show policy from-vsmart
- C. vSmart# show running-config policy
- D. vSmart# show running-config apply-policy

Answer: B

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book.pdf>

Question: 27

Which command on a WAN Edge device displays the information about the colors present in the fabric that are learned from vSmart via OMP?

- A. show omp tlocs
- B. show omp sessions
- C. show omp peers
- D. show omp route

Answer: A

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/sdwan-cr-book_chapter_0100.html#wp1675287742

Question: 28

Which template configures the out-of-band management VPN?

A)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Global	No
	Interface Name	Global	loopback0
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lo0_int_ip_addr/maskbits

B)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_mgt_int_mgmt0_or_gex/x
	Description	Global	Management Interface
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn512_mgt_int_ip_addr/maskbits

C)

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	512
	Name	Global	Management VPN
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn512_mgt_next_hop_ip_addr

D)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int2_shutdown
	Interface Name	Device Specific	vpn1_lan_int2_gex/x
IPv4 configuration	Description	Device Specific	vpn1_lan_int2_description
	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int2_ip_addr/maskbits

A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

Question: 29

Which protocol is used to measure loss latency, jitter, and liveliness of the tunnel between WAN Edge router peers?

- A. OMP
- B. IP SLA
- C. NetFlow
- D. BFD

Answer: D

Explanation:

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/TECCRS-2014.pdf>

Question: 30

DRAG DROP

Drag and drop the actions from the left into the correct sequence on the right to create a data policy to direct traffic to the Internet exit.

Apply data policy.	step 1
Enable NAT functionality.	step 2
Create centralized data policy.	step 3
Identify VPN and match criteria.	step 4

Answer:

Explanation:

Enable NAT functionality.
Create centralized data policy.
Identify VPN and match criteria.
Apply data policy.

Step 1 – Enable NAT Functionality Step 2 – Create centralized data policy Step 3 – Identify VPN and match criteria Step 4 – Apply data policy

Question: 31

An engineer is troubleshooting a vEdge router and identifies a “DCONFAL – DTLS connection failure”

message. What is the problem?

- A. certificate mismatch
- B. organization mismatch
- C. memory issue
- D. connectivity issue

Answer: D

Explanation:

<https://community.cisco.com/t5/networking-documents/sd-wan-routers-troubleshoot-control-connections/tap/3813237#toc-h1d-340740870>

Question: 32

Which on-the-box security feature supported by the Cisco ISR 4451 SD-WAN device and not on vEdge?

- A. Cloud Express service
- B. Enterprise Firewall with Application Awareness
- C. reverse proxy
- D. IPsec/GRE cloud proxy

Answer: B

Explanation:

<https://www.cisco.com/c/en/us/products/collateral/software/one-wan-subscription/guide-c07-740642.html#Step2SoftwareType>

Question: 33

When the VPN membership policy is being controlled at the vSmart controller, which policy disallows VPN 1 at sites 20 and 30?

A)

apply-policy

site-list 20-30

vpn-membership disallow-vpn 1

policy

lists

site-list 20-30

site-id 20

site-id 30

■
vpn-iist VPN 1

vpn 10

vpn 20

vpn-membership disallow-vpn 1 sequence 10

match

vpn-iist VPN 1

i ■

action reject

■
default-action accept

B)

policy

lists

site-list 20-30

site-id 20

site-id 30

■
prefix-list drop-list

ip-prefix 10.200.1.0/24

control-policy drop-unwanted-routes

sequence 10

match route

prefix-list drop-list

action reject

r

!

default-action accept

c)

apply-policy

site-list 20-30

vpn-membership disallow-vpn1

policy lists

site-list 20-30

site-id 20

site-id 30

vpn-membership disallow-vpn1

sequence 10

match vpn-id 1

action reject

i a

default-action accept

policy

lists

d)

site-list BP-Sites

site-id 10

site-id 20

vpn-list All-BPs

vpn 100

vpn 101

vpn-list Enterprise-BP

vpn 200

control-policy import-BPs-to-Enterprise sequence 10

match route

vpn-list All-BPs [

action accept

export-to vpn-list Enterprise-BP

default-action accept

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-17->

Question: 34

DRAG DROP

Drag and drop the route verification output from show omp tlocs from the left onto the correct explanations on the right.

shows if the route was chosen to enter the routing table or not	system ID
ENCAPSULATION	attribute of WAN link
COLOR	type of tunnel being used
TLOC IP	TLOC route status

Answer:

Explanation:

TLOC IP
COLOR
ENCAPSULATION
shows if the route was chosen to enter the routing table or not

Question: 35

Which configuration changes the packet loss priority from low to highly?

A)

```
policy
  policer ccnp-traffic
    rate 1000000
    burst 20000
    plp high
```

B)

```
policy
  policer ccnp-traffic
    rate 1000000
    burst 20000
    exceed remark
```

C)

```
policy
  policer ccnp-traffic
    rate 1000000
    burst 20000
    exceed drop
```

D)

```
policy
  policer ccnp-traffic
    rate 1000000
    burst 20000
    exceed high
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

we change the PLP from low to high (configured by the policer exceed remark command)

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/qos/vEdge-20-x/qos-book/forwarding-qos.html>

Question: 36

In which VPN is the NAT operation on an outgoing interface configured for direct Internet access?

- A. 1
- B. 10
- C. 512
- D. 0

Answer: D

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2019nov.pdf>

Question: 37

Which two platforms for the Cisco SD-WAN architecture are deployable in a hypervisor on-premises or in IAAS Cloud?
(Choose two.)

- A. CSR 1000v
- B. vEdge 100c
- C. vEdge Cloud
- D. vEdge 2000
- E. ISR 4431

Answer: A,C

Explanation:

Reference:

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf>

Question: 38

DRAG DROP

Drag and drop the devices from the left onto the correct functions on the right.

vSmart	establishes a secured data plane
vManage	first point of authentication
vEdge	single pane of glass
vBond	enforces control policies

Answer:

Explanation:

vEdge

vBond

vManage

vSmart

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/LTRCRS-3550.pdf>

Question: 39

When redistribution is configured between OMP and BGP at two Data Center sites that have Direct Connection interlink, which step avoids learning the same routes on WAN Edge routers of the DCs from LAN?

- A. Define different VRFs on both DCs
- B. Set same overlay AS on both DC WAN Edge routers

- C. Set down-bit on Edge routers on DC1
- D. Set OMP admin distance lower than BGP admin distance

Answer: B

Explanation:

Typically, there are more than one datacenters for HA redundancy requirements. After successful migration of the first datacenter, migrate the second datacenter in a similar method as explained in this section. Note that a routing loop can occur if there is a backdoor link between the datacenter sites and route advertisement is configured between the two datacenters. To avoid the loop, any of the three methods explained below can be used:

1. Use the same Autonomous System Numbers (ASN) on edge routers of the two datacenters. Because of the same ASN, the AS-PATH attribute will avoid learning the same prefixes on the edge routers that are advertised by the other datacenter towards the LAN side.
2. Use overlay-AS to insert Overlay Management Protocol (OMP) AS number when redistributing the routes from OMP into LAN side towards DC LAN. Configure all DC SD-WAN edge routers with the same overlay-as. This allows the edges to filter the routes advertised by the other DCs edge devices towards the LAN side and prevents redistributing the same routes back into OMP.
3. Use tags or communities to mark the prefixes at one datacenter when redistributing to DC LAN and filter on the edge of the other datacenter when learning advertisements from the LAN side.

Question: 40

Which value is verified in the certificates to confirm the identity of the physical WAN Edge device?

- A. Serial Number
- B. OTP
- C. System-IP
- D. Chassis-ID

Answer: A

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/manage-certificates.html>

Question: 41

Which configuration allows users to reach YouTube from a local Internet breakout?

- A)

VPN 10

```
ip route 0.0.0.0/0 vpn 0
```

B)

VPN 10

```
ip route 0.0.0.0/0 vpn 0
```

VPNO

```
interface Gig1/1
```

```
nat
```

C)

policy

data-policy DPI

vpn-list vpn 10

sequence 10 match

app-list YouTube destination-port 80 443 !

action accept count Youtube

|

default-action accept !

lists

vpn-list vpni 0

vpn 10

app-list YouTube app youtube app youtube_hd !

site-list Remote

site-id 14

site-id 15 r

|

|'

apply-policy

site-list Remote

policy

data-policy DPI vpn-list vpn10 sequence 10 match

app-list YouTube

action drop count Youtube

default-action accept

lists

vpn-list vpn10 vpn 10

app-list YouTube app youtube app youtube_hd

site-list Remote

site-id 14

site-id 15

apply-policy site-list Remote

data-policy DPI from-transport

vpn 10

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

As explained in figure 7, within the direct Internet model, segmentation is leveraged by deploying centralized data policies or a NAT DIA route to leak Internet traffic from the service-side VPN (VPNs 0 - 511,513 - 65530) into the Internet transport VPN (VPN 0), which allows traffic to exit directly to the Internet through the NAT-enabled interface in VPN 0.

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy->

2020aug.pdf

Question: 42

Which command disables the logging of syslog messages to the local disk?

- A. no system logging disk enable
- B. no system logging disk local
- C. system logging disk disable
- D. system logging server remote

Answer: A

Explanation:

Reference:

https://sdwandocs.cisco.com/Product_Documentation/Software_Features/SDWAN_Release_16.3/02System_and_Interfaces/08Configuring_System_Logging

Question: 43

Which API call retrieves a list of all devices in the network?

- A. https://vmanage_IP_address/dataservice/system/device/{{model}}
- B. http://vmanage_IP_address/dataservice/system/device/{{model}}
- C. http://vmanage_IP_address/api-call/system/device/{{model}}
- D. https://vmanage_IP_address/api-call/system/device/{{model}}

Answer: A

Explanation:

Display all available vEdge routers in the overlay network.

GET <https://vmanage-ip-address}/dataservice/system/device/vedges>

Question: 44

On which device is a service FW address configured to Insert firewall service at the hub?

- A. vEdge at the branch
- B. vSmart at the hub
- C. vEdge at the hub
- D. vSmart at the branch

Answer: C

Explanation:

Reference:

https://sdwandocs.cisco.com/Product_Documentation/Software_Features/Release_18.4/07Policy_Applications/02Service_Chaining/Service_Chaining_Configuration_Examples

Question: 45

Refer to the exhibit.

#Branch1-Edge1

vpn 0

interface ge0/1

ip address

172.17.113.241/28

tunnel-interface

encapsulation ipsec

color mpls restrict

no shutdown

interface ge0/2.704

ip address 10.113.4.2/30 tloc-extension

ge0/2

#Branch1-Edge2

vpn 0

interface ge0/2

no shutdown

interface ge0/2.704

ipaddress 10.113.4.1/30

tunnel-interface

encapsulation ipsec

color mpls restrict

mtu 1496

no shutdown

ip route 0.0.0.0/0 10.113.4.2

Which configuration change is needed to configure the tloc-extension on Branch1-Edge1?

A interface geO/2.704 ip address 10.113.4.1/30 tunnel-
interface encapsulation ipsec color mpls restrict no
shutdown

0 interface geO/2.704 ip address 10.113.4.2/30 mtu 1496
tloc-extension ge0/1

0 interface geO/2.704 ip address 10.113.4.2/30 mtu 1496
tloc-extension ge0/2

0 interface geO/2.704 ip address 10.113.4.1/30 tunnel-
interface encapsulation ipsec color mpls restrict mtu 1496
tloc-extension geO/2 no shutdown

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 46

Which two image formats are supported for controller codes? (Choose two.)

- A. .nxos
- B. .qcow2
- C. .ova
- D. .bin
- E. Tgz

Answer: B,C

Explanation:

Question: 47

Two sites have one WAN Edge each WAN Edge has two public TLOCs with no restriction configured. There is full reachability between the TLOCs. How many data tunnels are formed on each Edge router?

- A. 2

- B. 8
- C. 6
- D. 4

Answer: D

Explanation:

Question: 48

Which SD-WAN component is configured to enforce a policy to redirect branch-to-branch traffic toward a network service such as a firewall or IPS?

- A. vBond
- B. WAN Edge
- C. vSmart
- D. Firewall

Answer: C

Explanation:

Question: 49

Which two hardware platforms support Cisco IOS XE SD-WAN images" (Choose two)

- A. ASR1000 series
- B. ISR9300 series
- C. vEdge-1000 series
- D. ASR9000 series
- E. ISR4000 series

Answer: A,E

Explanation:

Reference: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white_paper-c11-741071.html

Question: 50

Which two mechanisms are used to guarantee the integrity of data packets in the Cisco SD-WAN architecture data plane? (Choose two)

- A. transport locations
- B. authentication headers
- C. certificates
- D. TPM chip
- E. encapsulation security payload

Answer: B,E

Explanation:

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/01Security_Overview/Data_Plane_Security_Overview

Question: 51

Which feature template configures OMP?

A)

Section	Parameter	Type	Variable/value
Authentication	Authentication Order	Drop-down	local
	Local	Device Specific	user_admin_passwd

B)

Section	Parameter	Type	Variable/value
Basic configuration	Number of paths advertised per prefix	Global	16
	Advertise	Global	Off
	Static	Global	Off

C)

Section	Parameter	Type	Variable/value
Server	Hostname/IP Address	Global	10.4.48.13
	VPN ID	Global	1
	Source interface	Global	loopback0

D)

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	512
	Name	Global	Management VPN
IPv4 Route	Prefix	Global	0000/0
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn5!2_mgt_next_hop_ip_addr

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

Question: 52

DRAG DROP

Drag and drop the policies from the left onto the correct policy types on the right.

strict hub-and-spoke topology

perform shaping on traffic

service firewall insertion

prefer voice and video via MPLS link

Control Policy

Data Policy

Answer:

Explanation:

Control Policy

strict hub-and-spoke topology

prefer voice and video via MPLS link

Data Policy

perform shaping on traffic

service firewall insertion

Question: 53

A voice packet requires a latency of 50 msec. Which policy is configured to ensure that a voice packet is always sent on the link with less than a 50 msec delay?

- A. centralized control
- B. localized data
- C. localized control
- D. centralized data

Answer: D

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/application-aware-routing.html>

Question: 54

A vEdge platform is sending VRRP advertisement messages every 10 seconds. Which value configures the router back to the default timer?

- A. 2 seconds
- B. 3 seconds
- C. 1 second
- D. 5 seconds

Answer: C

Explanation:

Reference:

https://sdwandocs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Templates/VPN_Interface_Ethernet

Question: 55

DRAG DROP

Drag and drop the functions from the left onto the correct templates on the right.

VPN 512	routing policy
VPN 0	transport VPN
route-map	management VPN
organization name	service VPN
VPN 10	system information

Answer:

Explanation:



Question: 56

Which pathway under Monitor > Network > Select Device is used to verify service insertion configuration?

- A. Real Time
- B. System Status
- C. ACL Logs
- D. Events

Answer: A

Explanation:

E. Using Cisco vManage:

View the configured services on the Real Time monitoring page (**Monitor > Network > hub-device > Real Time**) For Device Options, select OMP Services

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html>

Question: 57

At which layer does the application-aware firewall block applications on a WAN Edge?

- A. 3

- B. 7
- C. 5
- D. 2

Answer: B

Explanation:

Question: 58

Which combination of platforms are managed by vManage?

- A. ISR4321, ASR1001, ENCS, ISRV
- B. ISR4351, ASR1002HX, vEdge2000, vEdge Cloud
- C. ISR4321, ASR1001, Nexus, ENCS
- D. ISR4351, ASR1009, vEdge2000, CSR1000v

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sw-defined-wan-faq-cte-en.pdf>

Question: 59

Which scheduling method is configured by default for the eight queues in the cloud vEdge router1?

- A. low latency queue
- B. priority queue
- C. weighted random early detection
- D. weighted round robin

Answer: D

Explanation:

Reference:

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-

[WAN_Release_16.3/06Policy_Basics/05Localized_Data_Policy/Configuring_Localized_Data_Policy_for_IPv4](https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/06Policy_Basics/05Localized_Data_Policy/Configuring_Localized_Data_Policy_for_IPv4)

Question: 60

DRAG DROP

Drag and drop the vManage policy configuration procedures from the left onto the correct definitions on the right.

Create groups of interest.	Create the network structure to which the policy applies.
Configure traffic rules.	Create lists that group together related items that an engineer can call in the match or action components of a policy.
Configure topology.	Associate a policy with sites and VPNs in the overlay network.
Apply policies to sites and VPNs.	Create the match and action conditions of a policy.

Answer:

Explanation:

Configure topology

Create groups of interest

Apply policies to sites and VPNs

Configure traffic rules

Reference:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html>

Question: 61

Which platforms are managed by a single vManage dashboard?

- A. ISR4351, ASR1002HX, vEdge2000, vEdge Cloud
- B. ISR4321, ASR1001, Nexus, ENCS
- C. ISR4321, ASR1001, ENCS, ISRV
- D. ISR4351, ASR1009, vEdge2000, CSR1000v

Answer: C

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sw-defined-wan-faq-cte-en.pdf>

Question: 62

Which pathway under Monitor > Network > Select Device is used to verify service insertion configuration?

- A. System Status
- B. Troubleshooting
- C. Real Time
- D. Events

Answer: B

Explanation:

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/LABEN-2010-LG.pdf>

Question: 63

What is a benefit of the application aware firewall feature in the Cisco SD-WAN solution?

- A. application monitoring
- B. application malware protection
- C. application visibility
- D. control policy enforcement

Answer: C

Explanation:

[https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-](https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=242)

[4.pdf#page=242](https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=242)

The Application Firewall inspects and blocks traffic based on applications or application-family. This application-aware firewall feature provides the following benefits:

- **Application visibility** and granular control

Question: 64

A policy is created to influence routing path in the network using a group of prefixes. What policy application will achieve this goal when applied to a site List?

- A. vpn-membership policy
- B. cflowd-template
- C. app-route policy
- D. control-policy

Answer: D

Explanation:

Question: 65

Which component of the Cisco SD-WAN secure extensible network provides a single pane of glass approach to network monitoring and configuration?

- A. APIC-EM
- B. vSmart
- C. vManage
- D. vBond

Answer: C

Explanation:

Cisco vManage provides a single-pane-of-glass management to manage all controller components and both enterprise and extended enterprise WAN edge devices. The comprehensive vManage GUI has dashboard, monitor, configuration, tools, maintenance, administration, and analytics as the top-level menus.

Question: 66

A network administrator is configuring Qos on a vEdge 5000 router and needs to enable it on the transport side interface. Which policy setting must be selected to accomplish this goal?

- A. Cloud QoS Service side
- B. Cloud QoS
- C. NetFlow
- D. Application

Answer: B

Explanation:

9. Since the DC routers are vEdge 5000s, select the Cloud QoS checkbox to enable QoS on the transport side.

Question: 67

Which two algorithms authenticate a user when configuring SNMPv3 monitoring on a WAN Edge router? (Choose two.)

- A. AES-256
- B. SHA-1
- C. AES-128
- D. MD5
- E. SHA-2

Answer: A,B

Explanation:

Configure SNMPv3

Table 7. Feature History

Feature Name	Release Information	Description
Support for SNMPv3 AES-256 bit Authentication Protocol	Cisco SD-WAN Release 20.5.1	Support introduced for AES-256 bit Authentication Protocol called SHA-256.

To configure SNMPv3, in SNMP Version, click V3 For SNMPv3, you can configure groups, users, and trap information. Configure groups and trap information as described above. To configure SNMPv3 users, in the User section, click Add New User and enter the following parameters:

Table 8.

Parameter Name	Description
User	Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters.
Authentication Protocol	Select the authentication mechanism for the user. <ul style="list-style-type: none">• SHA-1 message digest• SHA-256 message digest. Note Starting from Cisco SD-WAN Release 20.5.1, SHA-256 authentication protocol was introduced. When you choose SHA-256 as the authentication protocol, you must set the security level as authPriv. Note MD5 authentication protocol is deprecated for Cisco SD-WAN Release 20.3.2 and later releases.

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/snmp/snmp-book.html>

Question: 68

In the Cisco SD-WAN solution, vSmart controller is responsible for which two actions? (Choose two.)

- A. Distribute crypto key information among vEdge routers
- B. Configure and monitor vEdge routers.
- C. Authenticate and authorize vEdge routers.
- D. Distribute the IP address from DHCP server to vEdge routers.
- E. Distribute route and policy information via OMP.

Answer: A,E

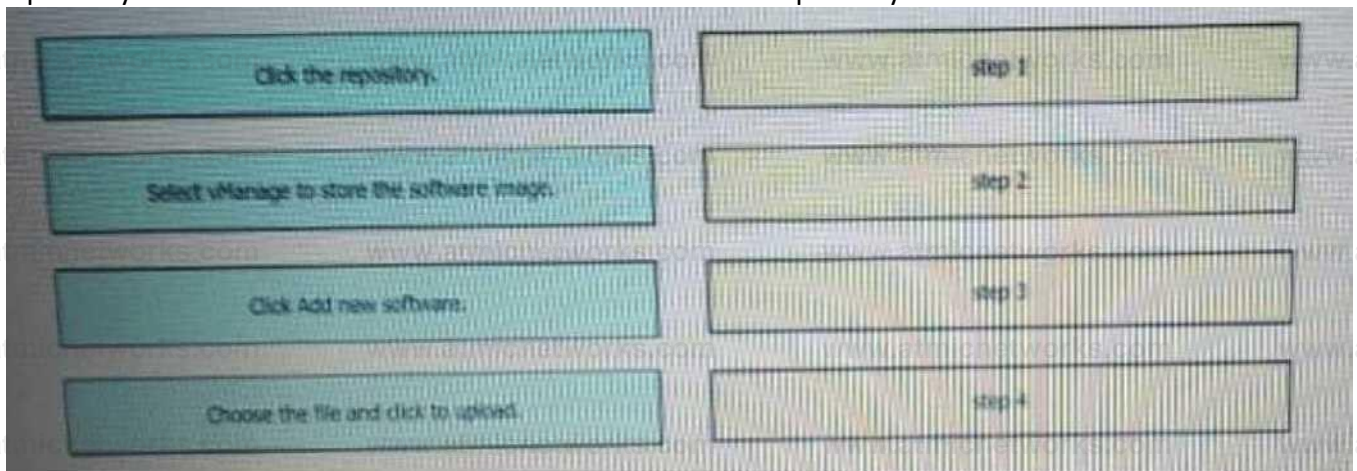
Explanation:

vSmart controller - This software-based component is responsible for the centralized control plane of the SD-WAN network. It maintains a secure connection to each WAN Edge router and distributes routes and policy information via the Overlay Management Protocol (OMP), acting as a route reflector. It also orchestrates the secure data plane connectivity between the WAN Edge routers by reflecting crypto key information originating from WAN Edge routers, allowing for a very scalable, IKE-less architecture.

Question: 69

DRAG DROP

Drag and drop the steps from the left into the order on the right to upload software on vManage repository that is accessible from maintenance > Software Repository.



Explanation:

Answer:

Click the repository

Click Add new software

Select vManage to store the software image

Choose the file and click to upload

Add an Image to the Software Repository

To add a software image to the software repository:

1. In Cisco vManage, click **Maintenance > Software Repository**.

2. Click **Add New Software** and select **vManage** from the drop-down menu
3. In the **Upload Software to vManage** dialog box:

- a. Click **Browse** and browse to the desired software image.

- b. Click **Upload**

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/maintain.html#c-Software_Upgrade-12330

Question: 70

In an AWS cloud, which feature provision WAN Edge routers automatically in Cisco SD-WAN?

- A. Cloud app
- B. Cloud OnRamp
- C. vAnalytics
- D. Network Designer

Answer: B

Explanation:

Cisco SD-WAN Cloud OnRamp for aaS, "Cloud OnRamp" for short, is a Cisco SD-WAN feature that automates provisioning of a Cisco SD-WAN virtual appliance routers (either vEdge Cloud or CSR (Cloud Services Router)) in the AWS cloud, after providing

Question: 71

What is the purpose of "vpn 0" in the configuration template when onboarding a WAN edge node?

- A. It carries control traffic over secure DTLS or TLS connections between vSmart controllers and vEdge routers, and between vSmart and vBond
- B. It carries control out-of-band network management traffic among the Viptela devices in the overlay network.
- C. It carries control traffic over secure IPsec connections between vSmart controllers and vEdge routers, and between vSmart and vManager
- D. It carries control traffic over secure IPsec connections between vSmart controllers and vEdge routers, and between vSmart and vBond

Answer: A

Explanation:

• VPN 0 is the transport VPN. It carries control traffic over secure DTLS or TLS connections between vSmart controllers and vEdge routers, and between vSmart controllers and vBond orchestrators. Initially, VPN 0 contains all a device's interfaces except for the management

interface, and all the interfaces are disabled. For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

Question: 72

Which device in the SD-WAN solution receives and categorizes event reports, and generates alarms?

- A. WAN Edge routers
- B. vSmart controllers
- C. vManage NMS
- D. vBond controllers

Answer: C

Explanation:

<https://sdwan->

[docs.cisco.com/Product_Documentation/vManage_Help/Release_17.1/vManage_NMS_Product_Hel p](https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_17.1/vManage_NMS_Product_Hel_p)

Question: 73

A network administrator is bringing up one WAN Edge for branch connectivity. Which types of tunnels form when the WAN edge router connects to the SD-WAN fabric?

- A. DTLS or TLS tunnel with vBond controller and IPsec tunnel with vManage controller.
- B. DTLS or TLS tunnel with vBond controller and IPsec tunnel with other WAN Edge routers.
- C. DTLS or TLS tunnel with vSmart controller and IPsec tunnel with other Edge routers.
- D. DTLS or TLS tunnel with vSmart controller and IPsec tunnel with vBond controller.

Answer: C

Explanation:

The WAN Edge routers form a permanent Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) control connection to the vSmart controllers and connect to both of the vSmart controllers over each transport. The routers also form a permanent DTLS or TLS control connection to the vManage server, but over just one of the transports. The WAN Edge routers securely communicate to other WAN Edge routers using IPsec tunnels over each transport. The Bidirectional Forwarding Detection (BED) protocol is enabled by default and runs

Question: 74

When a WAN Edge device joins the SD-WAN overlay, which Cisco SD-WAN components orchestrates the connection between the WAN Edge device and a vSmart controller?

- A. vManage
- B. vBond

- C. OMP
- D. APIC-EM

Answer: B

Explanation:

When a vEdge device comes up, how does it automatically discover Cisco vManage and Cisco vSmart Controller and establish connections with them? **It does so with help from Cisco vBond Orchestrator.**

Question: 75

An administrator needs to configure SD-WAN to divert traffic from the company's private network to an ISP network.

What action should be taken to accomplish this goal?

- A. configure the control policy
- B. configure the data policy
- C. configure the data security policy
- D. configure the application aware policy

Answer: B

Explanation:

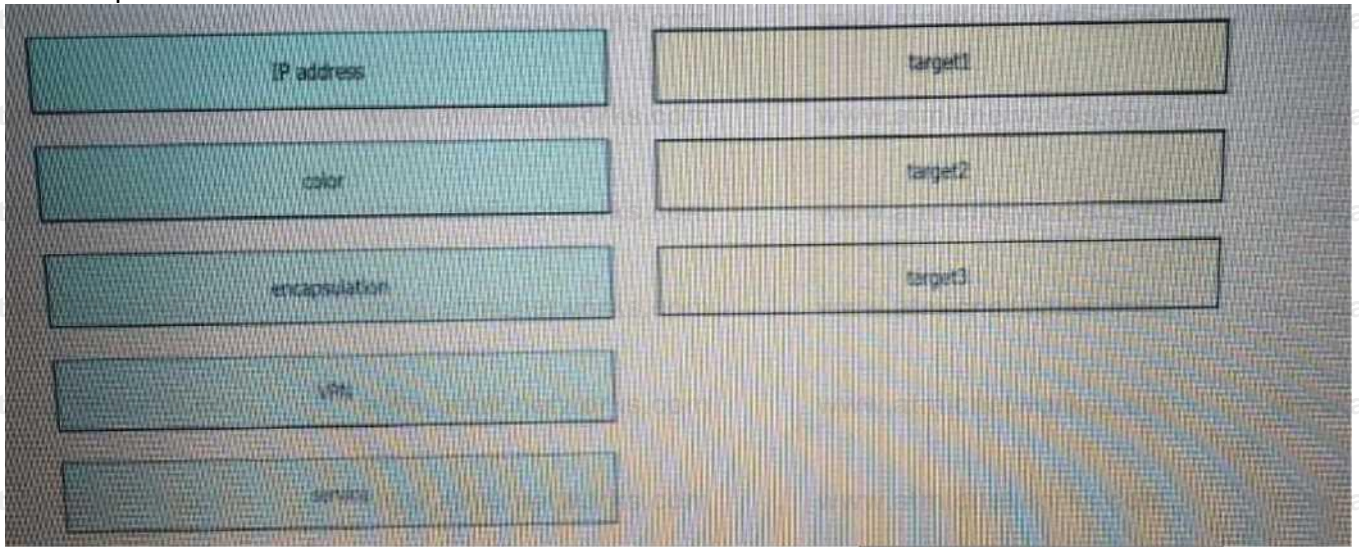
Data policy influences the flow of data traffic traversing the network

Question: 76

DRAG DROP

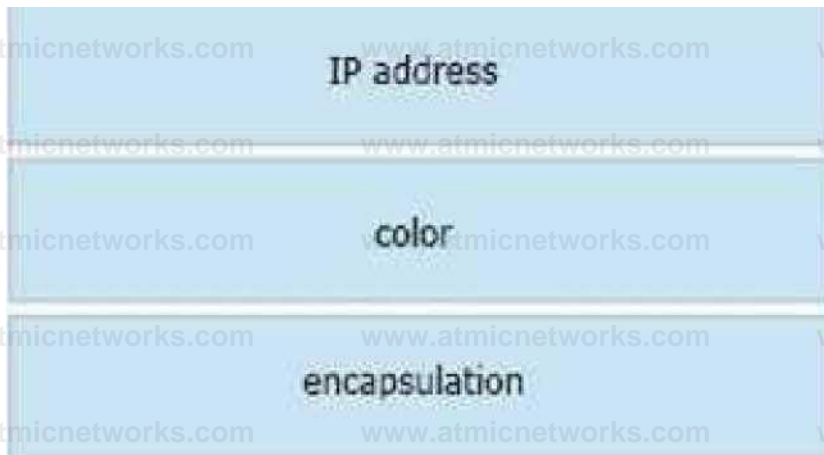
Drag and drop the attributes from the left that make each transport location unique onto the right.

Not all options are used



Answer:

Explanation:



A TLOC, or Transport Location, is the attachment point where a WAN Edge router connects to the WAN transport network. A TLOC is uniquely identified and represented by a three-tuple, consisting of **system IP address**, **link color**, and **encapsulation** (Generic Routing Encapsulation [GRE] or IPsec).

Question: 77

Refer to the exhibit.

```
vEdge-2(config-vpn-0)# interface ge0/2.101
vEdge-2(config-interface)# ip address 10.1.100.0/24
vEdge-2(config-interface)# tloc-extension ge0/0
vEdge-2(config-interface)# mtu 1496
vEdge-2(config-interface)# no shutdown
```

What binding is created using the tloc-extension command?

- A. between ge 0/2.101 of port-type service and ge 0/0 of port-type service
- B. between ge 0/2.101 of port-type transport and ge 0/0 of port-type service
- C. between ge 0/2.101 of port-type service and ge 0/0 of port-type transport
- D. between ge 0/2.101 of port-type transport and ge 0/0 of port-type transport

Answer: D

Explanation:

tloc-extension

Bind this interface, which connects to another vEdge router at the same physical site, to the local router's WAN [transport interface](#) (on vEdge routers only).

Question: 78

Answer:

grouping of VPNs where the data traffic flows terminate

grouping of VPNs where the data, traffic flows originate

matching condition that allows traffic flow between two zones

DRAG DROP

Drag and drop the definitions from the left to the configuration on the right.

grouping of VPNs where the data traffic flows originate	destination zone
grouping of VPNs where the data traffic flows terminate	source zone
matching condition that allows traffic flow between two zones	firewall policy
container that associates forwarding and blocking decisions	zone pair

Explanation:

container that associates forwarding and blocking decisions

- **Source zone**—A grouping of VPNs where the data traffic flows originate.
- **Destination zone**—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone
- **Zone-based firewall policy**—A data policy, similar to a localized data policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Zone-based firewalls can match IP prefixes, IP ports, and the protocols TCP, UDP, and ICMP. Matching flows can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default.
- **Zone pair**—A container that associates a source zone with a destination zone and that applies a zone-based firewall policy to the traffic that flows between the two zones.

Question: 79

A network administrator is configuring an application-aware firewall between inside zones to an outside zone on a WAN edge router using vManage GUI. What kind of Inspection is performed when the “inspect” action is used?

- A. stateful inspection for TCP and UDP
- B. stateful inspection for TCP and stateless inspection of UDP
- C. IPS inspection for TCP and Layer 4 inspection for UDP
- D. Layer 7 inspection for TCP and Layer 4 inspection for UDP

Answer: A

Explanation:

Cisco's Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

A firewall policy is a type of localized security policy that allows **stateful inspection** of TCP, UDP, and ICMP data traffic flows,

Question: 80

An engineer wants to track tunnel characteristics within an SLA-based policy for convergence. Which policy configuration will achieve this goal?

- A. App-route policy
- B. VPN membership policy
- C. Control policy
- D. Data policy

Answer: A

Explanation:

An **application-aware routing policy** matches applications with an SLA, that is, with the data plane tunnel performance characteristics that are necessary to transmit the applications' data traffic. The primary purpose of application-aware routing policy is to optimize the path for data traffic being transmitted by Cisco SD-WAN devices

Question: 81

A policy is created to influence routing in the network using a group of prefixes. What policy application will achieve this goal when applied to a site list?

- A. Vpn-membership policy
- B. Control-policy
- C. cflowd-template
- D. App-route policy

Answer: B

Explanation:

Control policy, which is similar to standard routing policy, operates on routes and routing information in the control plane of the overlay network. Centralized control policy, which is provisioned on the Cisco vSmart Controller, is the Cisco SD-WAN technique for customizing network-wide routing decisions that determine or influence routing paths through the overlay network. Local control policy, which is provisioned on a Cisco vEdge device, allows customization of routing decisions

Question: 82

In Cisco SD-WAN, what protocol is used for control connections between SD-WAN devices?

- A. DTLS
- B. OMP
- C. BGP
- D. OSPF

Answer: A

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html>

Question: 83

Which feature builds transport redundancy by using the cross link between two redundant WAN Edge routers?

- A. OMP
- B. zero-touch provisioning
- C. quality of service
- D. TLOC extension

Answer: D

Explanation:

Features like TLOC extension help to build transport redundancy by using the cross link between two redundant WAN Edge routers. Network level redundancy is implemented by multiple geo-redundant data centers.

Question: 84

What is a description of vManage NMS?

- A. It is accessible only from VPN 512 (the management VPN).
- B. A cluster requires device templates to be created on and attached to the same server
- C. It is a software process on a dedicated WAN Edge router in the network.
- D. A cluster consists of a minimum of two vManage NMSs

Answer: B

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/optimization-ha/vedge/network-optimization-high-availability-book/high-availability.html>

Question: 85

In which device state does the WAN edge router create control connections, but data tunnels are not created?

- A. valid
- B. backup
- C. active
- D. staging

Answer: D

Explanation:

Staging - In this state, the WAN Edge device establishes secure control plane connections to the SD-WAN controllers (vBond, vManage, and vSmart) only. It is important to note that no data plane connections are established with other WAN Edge devices in the overlay network.

Question: 86

Which VPN connects the transport-side WAN Edge interface to the underlay/WAN network?

- A. VPN 1
- B. VPN 511
- C. VPN 0

D. VPN 512

Answer: C

Explanation:

transport network and the transport network itself. The network ports that connect to the underlay network are part of VPN 0, the transport VPN. Getting connectivity to the Service Provider gateway in the transport network usually involves configuring a static default gateway (most

Question: 87

Which two WAN Edge devices should be deployed in a cloud? (Choose two.)

- A. vEdge 5000v
- B. ASR 1000v
- C. CSR 1000v
- D. vEdge 100wm
- E. vEdge cloud

Answer: C,E

Explanation:

2. Virtual platforms

- Cloud Sendees Router (CSR) 1000v running IOS XE SD-WAN Software
- vEdge Cloud Router running Viptela OS

Question: 88

Which port is used for vBond under controller certificates if no alternate port is configured?

- A. 12345
- B. 12347
- C. 12346
- D. 12344

Answer: C

Explanation:

vSmart and vManage are normally installed behind NAT device, so port hopping is not needed. vBond always uses to other Viptela devices using port 12346 and they never use port hopping.

Question: 89

An engineer is configuring a centralized policy to influence network route advertisement. Which controller delivers this policy to the fabric?

- A. vSmart
- B. vManage
- C. WAN Edge
- D. vBond

Answer: A

Explanation:

vSmart controllers are the centralized brain of the solution; they implement policies and connectivity between SD-WAN branches. The centralized policy engine in Cisco vSmart controllers provides policy constructs to manipulate routing information, access control, segmentation, extranets, and service chaining

Question: 90

A network administrator is configuring a tunnel interface on a branch Cisco IOS XE router to run TLOC extensions. Which configuration will extend a TLOC over a GRE tunnel to another router in the branch?

```
sdwan
interface g0/0
  extended-interface tloc-extension-gre-from 10 1 1 1
```

```
sdwan
interface g0/0
  gre-interface tloc-extension-gre-to 10 1 1 1
```

```
sdwan
interface g0/0
  tunnel-interface
    tloc-extension-gre-to 10 1 1 1
```

sdwan

interface g0/0

floc-interface

tloc-extension-gre-from 10.1.1.1

A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

Configure a tunnel interface over which to run TLOC extensions (on IOS XE routers only). TLOC extensions allow you to extend a TLOC, over a GRE tunnel, to another router in the branch.

Command Hierarchy

sdwan

interface interface-name

tunnel-interface

tloc-extension-gre-to extended-interface-ip-address

Question: 91

Which two products that perform lifecycle management for virtual instances are supported by WAN Edge cloud routers?
(Choose two.)

- A. OpenStack
- B. AWS
- C. VMware vCenter
- D. Azure
- E. IBM Cloud

Answer: A,C

Explanation:

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-07-cloud-router-data-sheet-cte-en.html>

The following figure illustrates Cisco vEdge Cloud router solution elements.



Question: 92

A network administrator is creating an OMP feature template from the vManage GUI to be applied to WAN edge routers. Which configuration attribute will avoid the redistribution of the routes back into the OMP from the LAN side?

- A. configure "Number of Paths Advertised per Prefix"
- B. configure "Overlay AS Number"
- C. configure "Send Backup Paths"
- D. configure "ECMP limit"

Answer: B

Explanation:

If you configure the same **overlay AS number** on multiple vEdge routers in the overlay network, all these routers are considered to be part of the same AS, and as a result, they do not forward any routes that contain the overlay AS number. This mechanism is an additional technique for **preventing BGP routing loops** in the network.

Question: 93

If Smart Account Sync is not used, which Cisco SD-WAN component is used to upload an authorized serial number file?

- A. WAN Edge
- B. vManage
- C. vSmart
- D. vBond

Answer: B

Explanation:

<https://sdwan->

docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Devices

Question: 94

An engineer is tasked to improve throughput for connection-oriented traffic by decreasing round-trip latency. Which configuration will achieve this goal?

- A. turn on "Enable TCP Optimization"
- B. turn off "Enhance ECMP Keying"
- C. turn off "Enable TCP Optimization"
- D. turn on "Enhance ECMP Keying"

Answer: A

Explanation:

TCP optimization fine-tunes the processing of TCP data traffic to decrease round-trip latency and improve throughput, <https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-2.pdf#page=530>

Question: 95

Which secure connection should be used to access the REST APIs through the Cisco vManage web server?

- A. HTTP inspector interface
- B. authenticated HTTPS
- C. authenticated DTLS
- D. JSON Inspector interface

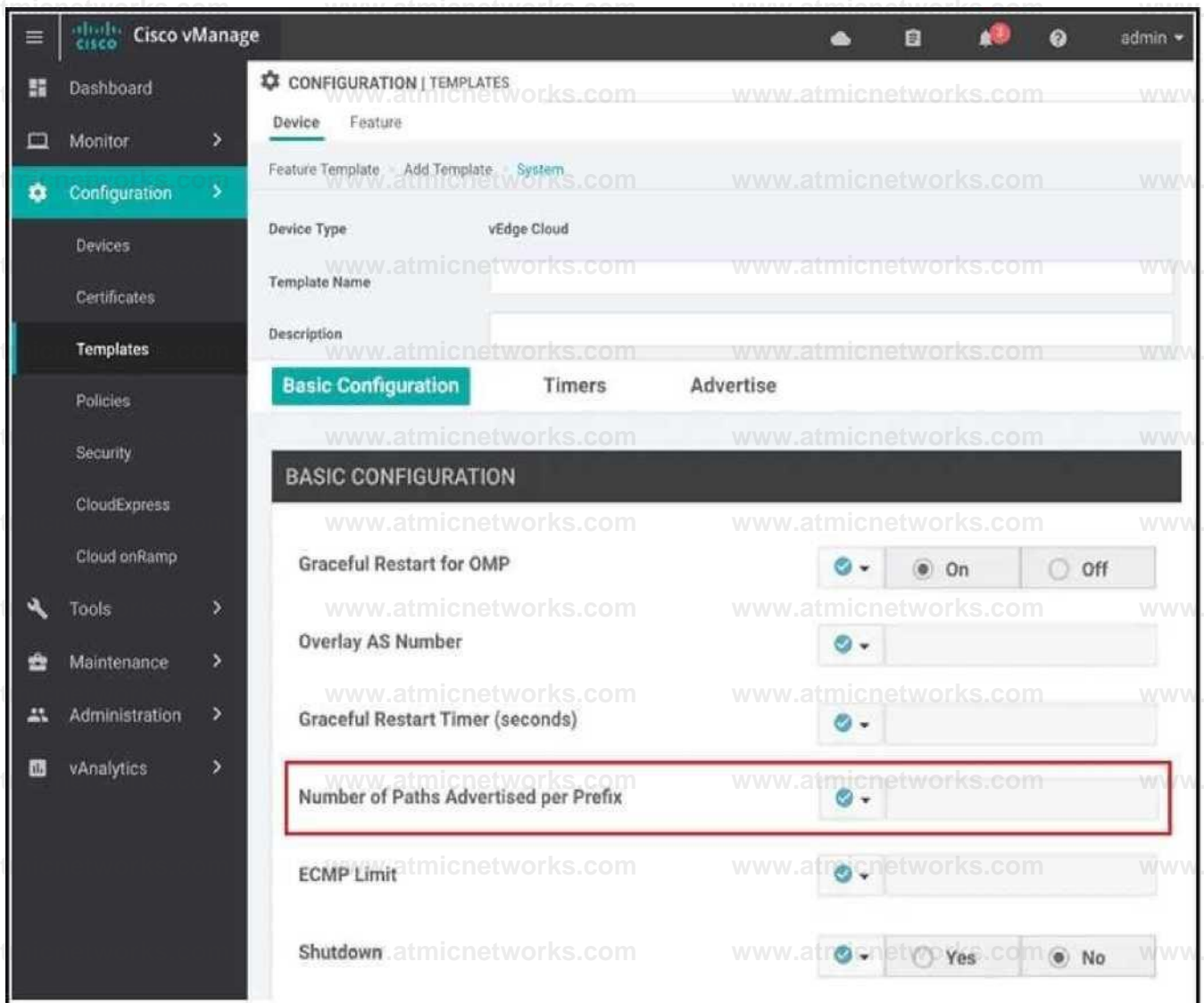
Answer: B

Explanation:

<https://documenter.getpostman.com/view/3224967/SVmpXhXd#ed9ccd34-cc5a-4258-bb6b-9b3848b7f650>

Question: 96

Refer to the exhibit.



A network administrator is configuring OMP in vManage to advertise all the paths for the same prefix from a site that has two WAN Edge devices. Each WAN Edge device is connected to three ISPs and two private MPLS transports. What is the minimum value for "Number of Paths advertised per Prefix" that should be configured?

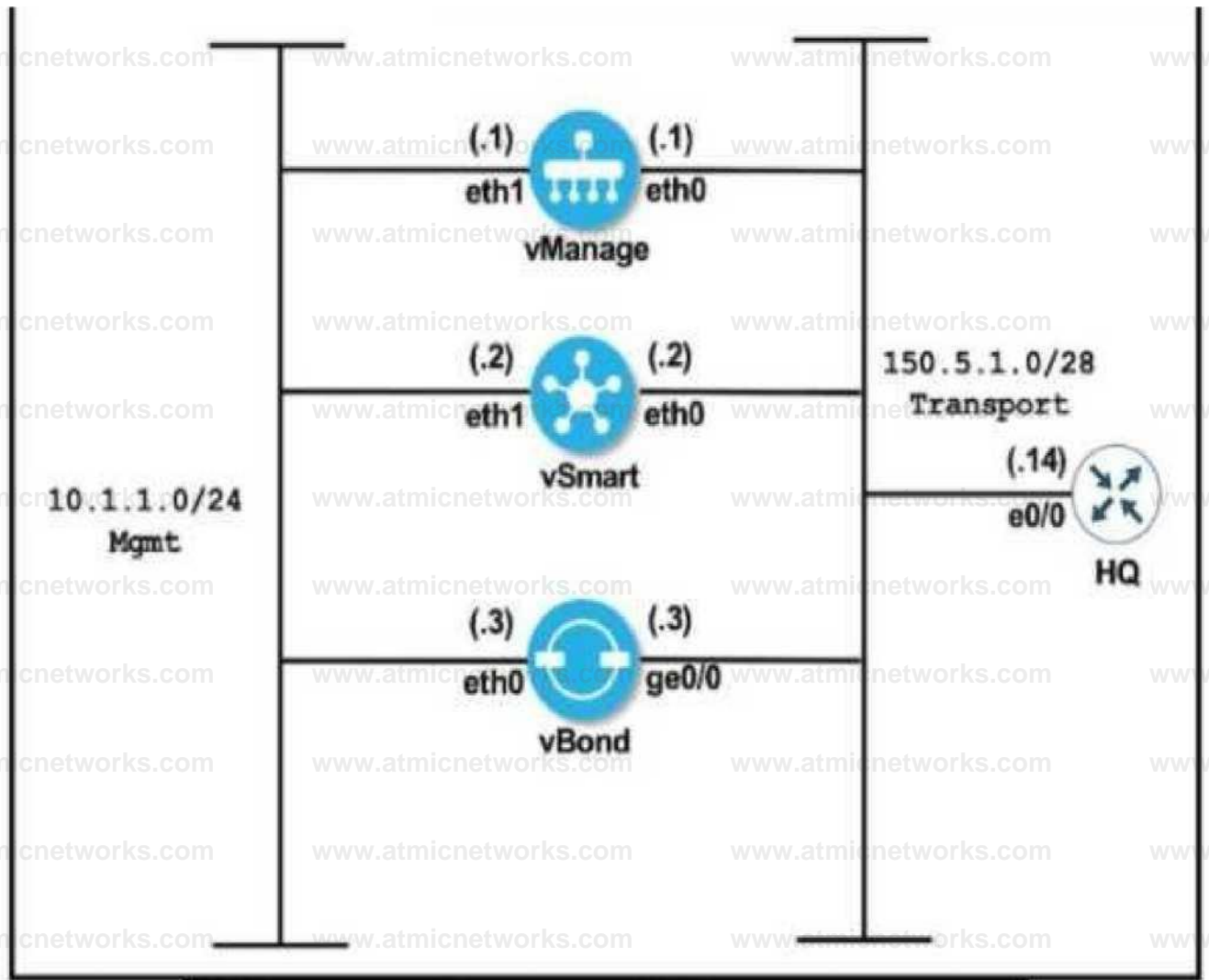
- A. 2
- B. 3
- C. 5
- D. 10

Answer: D

Explanation:

Question: 97

Refer to the exhibit.



dln*^

.Hnvi

lyitM

tyi*«-ip 15 10 Kittl

hc*t MJM rH*:i>j» «xt4~44 1

elicit T1**«CT« tu r-rpw ■'t^-^m vb.mi l» Stl

orgAnj K*tlon-nu4 Cisco co* I

apa a

littarU - MHO

Ip illt^a ISO.4 1.1/21

M ihut

buaiiai -1 nearC*c*

• 1L>* aarvlw ill 1* nata 4 4 0 0/0 iw.l

1 14

omm t

wQpnd

«ydr«s

ayaua ip ID 1| 10.103 he it-HUB vWond *it*ni i

41oe± l_11M£2U ±LucafM/Lo-ndfr.

4feM4 LM 5.1 J

bepuluUaH-hM* i. Litl- UH fl

'F' 0

mtarl.ua ftdl/0 ip AMrMI LH.I I /.■ m that t^imal kAtarfaea afW^MlaU^l ipl« allow isrrltw *11

ip Mt* P.O 4.0/4 1W 5 1 14 f

MttMt

iyvtvs ijiTii? ip ic i(j io t41 heat SWFW •

3F>■ r t Ht*-*4 1

riirh t^4w*M4 ■VTTI=« L^Adrn rtcu ISO 5

1 !

argsnlratiata-kMa CL Seo caw 1 vpa *

intii Fact sUifl ip Midm* 150.5.1 !/(• HA

kkiil kiural Lateftara AUPF MF*14a all

ip tusks | C 4 WO 150.5.1.14 1

«*aaii l

An engineer is troubleshooting an issue where vManage and vSmart have a problem establishing a connection to vBond. Which action fixes the issue?

- A. Reconfigure the vBond command on the vBond as vBond 150.5.1.3 local
- B. Configure the tunnel interface on all three controllers with a color of transport
- C. Remove the encapsulation IPsec command under the tunnel interface of vBond.
- D. Configure encapsulation as IPsec under the tunnel interface of vManage and vSmart

Answer: A

Explanation:

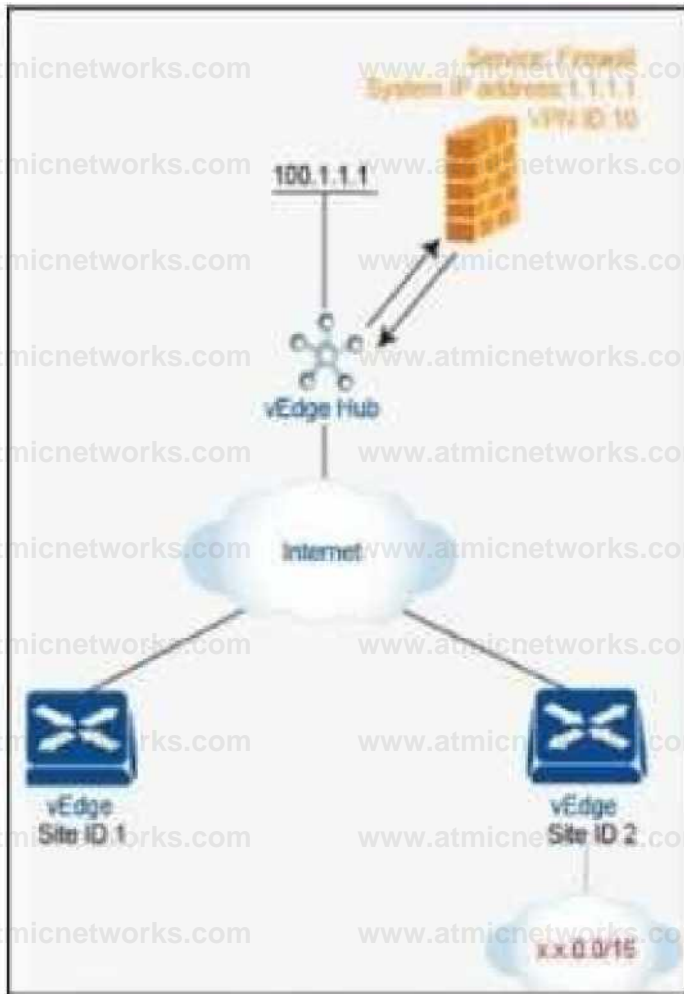
Configure the IP address of Cisco vBond Orchestrator. Cisco vBond Orchestrator's IP address must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach Cisco vBond Orchestrator:

```
vBond (config-system) Hvbond ip<address> local
```

In Releases 16.3 and later, the address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. A vBond orchestrator is effectively a vEdge router that performs only the orchestrator functions. The local option designates the device to be Cisco vBond Orchestrator, not a vEdge router. Cisco vBond Orchestrator must run on a standalone virtual machine (VM) or hardware router; it cannot coexist in the same device as a software or hardware vEdge router.

Question: 98

Refer to the exhibit.



An engineer is configuring service chaining. Which set of configurations is required for all traffic from Site ID 1 going toward Site ID 2 to get filtered through the firewall on the hub site?

A)

```
vpn 20
  vvic FWaddr 1.1.1.1
  policy
    iSt
    stte-llstfirewall-sites
    site id n
  control-policy firewall-service
  sequence 10
  match route
  iht4d 2
  action accept
  set service FW vpn 20
  default-action accept
  apply-policy
  ifMst flrewoH-sitH coturpi .policy 0Hwoll4>rvk4 out
```

B)

```
vpn 10
```



```

service FW address 1.1.1.1
policy
  list
  site-list firewall-sues
  site-id 1
control-policy firewall-service
sequence 16
match route
  site-id 2
action accept
  set Sarrica FW vpn 10
  cehnilt-action accept
apply-poky
site-fist firewall-sites control-policy firewall service out

```

C)

```

vpn 10
service FW address 1.1.1.1
policy
  lists
  site -11st frewall -sites
  site-id 1
control-policy firewall-service
sequence IQ
match route
  site-id 2
action accept
  set service FW vpn 20
  □ Btault-octori accept
apply-pcky
site .fi sc firewall-si res control-policy firewall -service out

```

D)

```

vpn 10
service FW address 1.1.1.2 policy
lists
  site-list firewall-SIUM site-rd 1
control-policy firewall-servac# sequence ID match route
  site-ld 1 acuon accept set service FW vpn 10 defaulwetion accept apply-pahcy
site-lut tire wall-sites control-policy firewall-service out

```

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/service-chaining.html>

Question: 99

In a Cisco SD-WAN architecture, what is the role of the WAN Edge?

- A. It provides orchestration to assist in automatic provisioning of WAN Edge routers and overlay
- B. It is the management plane responsible for centralized configuration and monitoring
- C. It is the control plane that builds and maintains network topology
- D. It is the data plane that is responsible for forwarding traffic

Answer: D

Explanation:

Cisco WAN Edge routers are responsible for establishing the network fabric and forwarding traffic. Cisco WAN Edge routers come in multiple forms, virtual and

Question: 100

A network administrator is configuring VRRP to avoid a traffic black hole when the transport side of the network is down on the master device. What must be configured to get the fastest failover to standby?

- A. lower timer interval
- B. prefix-list tracking
- C. higher group ID number
- D. OMP tracking

Answer: B

Explanation:

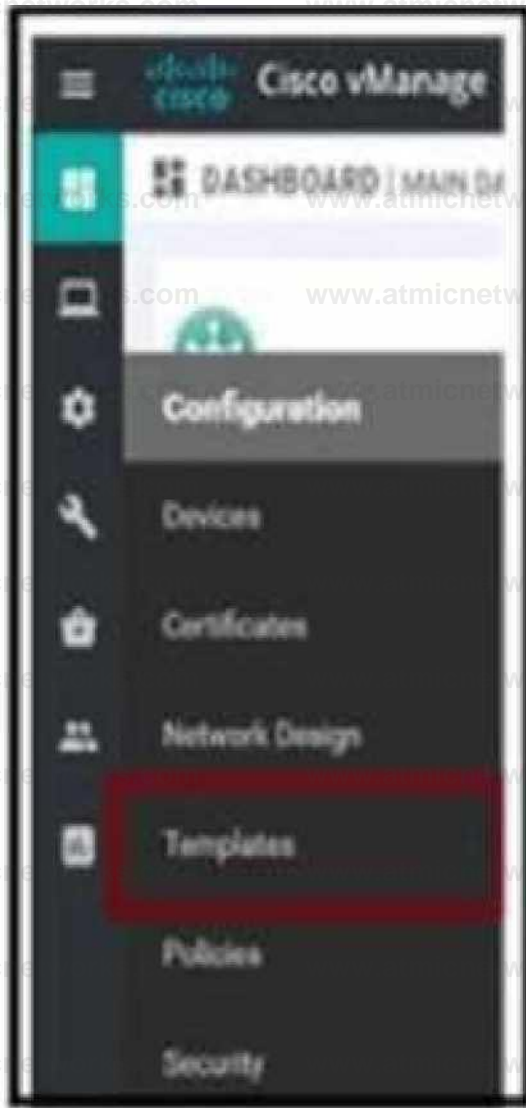
```
vEdge(config-vxrp)# track-prefix-list list-name
```

If all OMP sessions are lost, VRRP failover occurs as described for the track-omp option. In addition, if reachability to all the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP master.

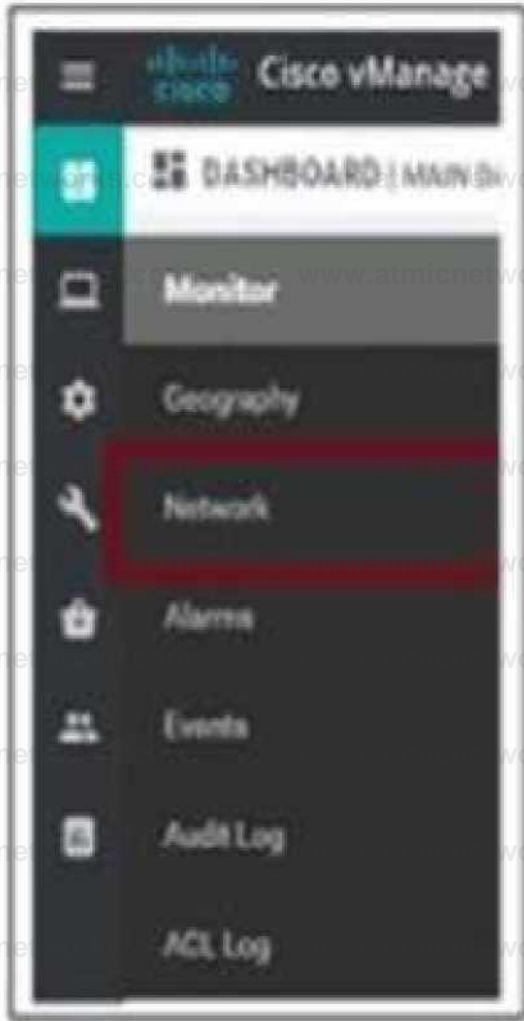
Question: 101

Company ABC has decided to deploy the controllers using the On-Prem method. How does the administrator upload the WAN Edge list to the vManage?

A)



B)



c)



D)



A. Option A B. Option B C. Option C D. Option D

Answer: D

Explanation:

[https://sdwan-](https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Devices)

[docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Devices](https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Devices)

Question: 102

Which two products are used to deploy Cisco WAN Edge Router virtual platforms? (Choose two.)

- A. HP ProLiant DL360 Generation 10 running HP-UX
- B. Cisco ENCS 5000 Series
- C. Sun SPARC Node running AIX

- D. Cisco UCS
- E. Sun Enterprise M4000 Server running Sun Solans

Answer: B,D

Explanation:

<https://www.cisco.com/c/en/us/products/collateral/routers/5400-enterprise-network-compute-system/datasheet-c78-738512.html>

Question: 103

Where on vManage does an engineer find the details of control node failure?

- A. Alarms
- B. Events
- C. Audit log
- D. Network

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/vManage_How-Tos/vmanage-howto-book/m-troubleshooting.html

Question: 104

An engineer is configuring a list that matches all IP prefixes with lengths from /1 to /16 in a centralized control policy. Which list accomplishes this task?

- A. 0.0.0.0/1 le 16
- B. 0.0.0.0/0 ge 1
- C. 0.0.0.0/0 le 16
- D. 0.0.0.0/16 ge 1

Answer: A

Explanation:

Question: 105

Which TCP Optimization feature is used by WAN Edge to prevent unnecessary retransmissions and large initial TCP window sizes to maximize throughput and achieve a better quality?

- A. SEQ
- B. SYN
- C. RTT
- D. SACK

Answer: D

Explanation:

TCP Optimization

The Cisco SD-WAN TCP Optimization feature uses TCP Selective Acknowledgement (SACK) to prevent unnecessary retransmissions and large initial TCP window sizes in order to maximize throughput and achieve a better quality of experience.

Question: 106

A large retail organization decided to move some of the branch applications to the AWS cloud. How does the network architect extend the in-house Cisco SD-WAN branch to cloud network into AWS?

- A. Create virtual WAN Edge devices Cloud through the AWS online software store
- B. Create virtual instances of vSmart Cloud through the AWS online software store
- C. Create GRE tunnels to AWS from each branch over the Internet
- D. Install the AWS Cloud Router in the main data center and provide the connectivity from each branch

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/Cisco_Cloud_onRamp_for_aaS_WS_Version2.html#_Toc54023359

Question: 107

Refer to the exhibit.

LOCAL	PEER	PEER	PEER	SITE	DOMAIN	PEER	PRIVATE	PEER	PEER
INSTANCE	REMOTE	REFEAT	SYSTEM	ID	ID	PRIVATE	PORT	PUBLIC	PUBLIC
TYPE	COLOR	STATE	IP	ERROR	COUNT	IP		IP	PORT
REMOTE			ERROR	ERROR	DOWNTIME				
0	vSmart	tls	1.1.1.3	100	1	100.1.1.3	23456	100.1.1.3	23456
default	trying		DOWNFAIL	NOERR	10001	2020-01-01T10:01:20+0000			

The control connection is failing. Which action resolves the issue?

- A. import vSmart in vManager
- B. Validate the certificates authenticity on vSmart
- C. Upload the WAN Edge list on vManage.
- D. Restore the reachability to the vSmart

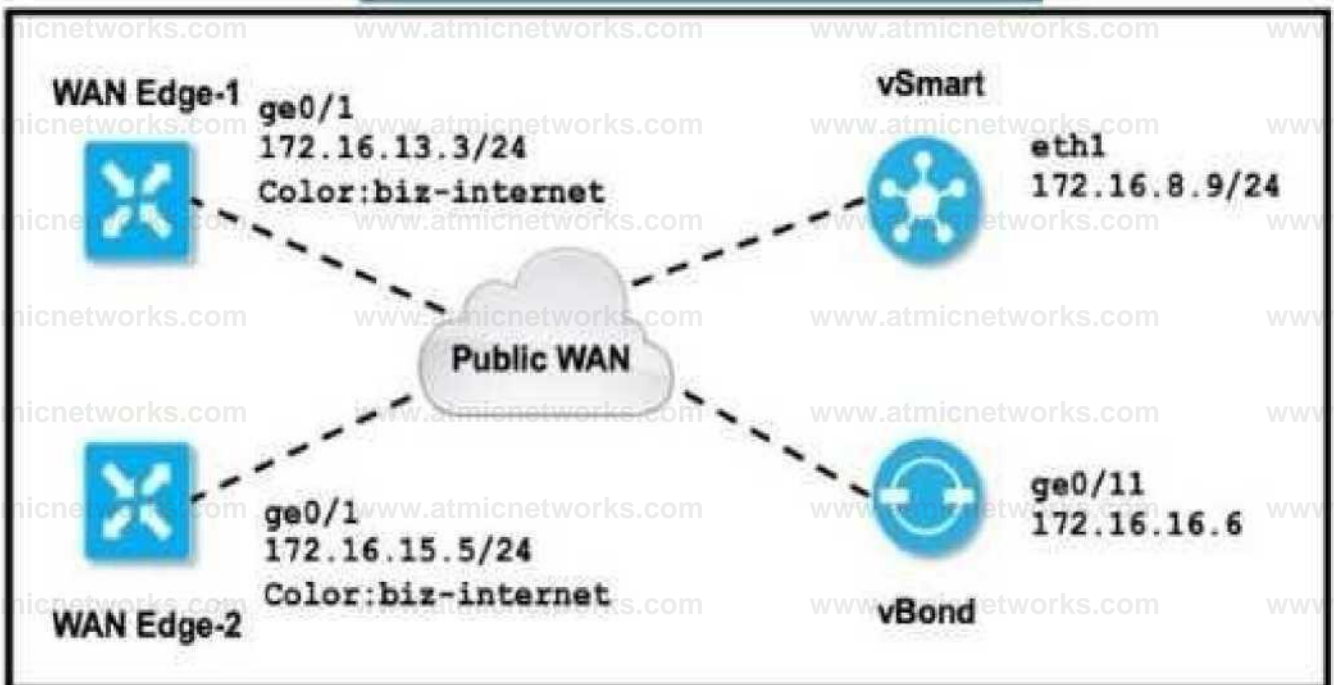
Answer: D

Explanation:

<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html>

Question: 108

Refer to the exhibit.



The tunnel interface configuration on both WAN Edge routers is:

```

vpn 0
interface QtC'i hinnel^nwrfce
encapsulation IpMC color bii-lmemet ■howwvict dhtp jlf aMMWYIH dnt a:low-service temp naaliow-service
jtitid no allow-service ntp no allow-iarvicE stun

```

no ihutdovm

Which configuration for WAN Edge routers will connect to the Internet?

```
vpn 0
interface ge0/1
ip address 172.16.13.1
ip route 0.0.0.0 0.0.0.0 172.16.13.1
```

```
vpn 0
interface ge0/24
ip address 172.16.13.3/24
^ routed 0.0.0.0 0.0.0.0 172.16.13.1
```

```
vpn 0
interface ge0/24
ip address 172.16.13.3/24
```

```
ip route 0.0.0.0 0.0.0.0 172.16.13.1
```

```
vpn 0
interface ge0/24
ip address 172.16.14.6/24
```

```
ip route 0.0.0.0 0.0.0.0 172.16.8.1
```

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/02System_and_Interfaces/07Network_Interface_Configuration_Examples

Question: 109

A network administrator is tasked to make sure that an OMP peer session is closed after missing three consecutive keepalive messages in 3 minutes. Additionally, route updates must be sent every minute. If a WAN Edge router becomes unavailable, the peer must use last known information to forward packets for 12 hours. Which set of configuration commands accomplishes this task?

```
omp
Timers
advertisement-interval 60
holdtime ISO
graceful-re start-timer 43200
```

**omp
timers
adverb semen:-interval 1
holdtime 180
graceful-re st art-timer 43200**

**omp
timers
advertisement-interval 1
holdtime 180
graceful-re start-timer 720**

**omp
timers
advertisement-interval 60
holdtime 60
graceful-re start-timer 720**

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_17.2/Configuration/Templates/OMP

Question: 110

An engineer is configuring a data policy for packets that must be captured through the policy. Which command accomplishes this task?

- A. policy > data-policy > vpn-list > sequence > default-action> drop
- B. policy > data-policy > vpn-list > sequence > action
- C. policy > data-policy > vpn-list > sequence > default-action> accept
- D. policy > data-policy > vpn-list > sequence > match

Answer: B

Explanation:

<https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=357>

Question: 111

A bank is looking for improved customer experience for applications and reduce overhead related to compliance and security. Which key feature or features of the Cisco SD-WAN solution will help the bank to achieve their goals?

- A. Integration with PaaS providers to offer the best possible application experience
- B. QoS including application prioritization and meeting critical applications SLA for selecting optimal path.
- C. implementation of a modem age core banking system
- D. implementation of BGP across the enterprise routing for selecting optimal path

Answer: B

Explanation:

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf>

Question: 112

Refer to exhibit.

PEER	PEER	PEER		SITE	DOMAIN					LOCAL	REMOTE	REPEAT	
INSTANCE	TYPE	PRIVATE	SYSTEM	IP	PUBLIC	ID	ID	PRIVATE	IP	PORT	PUBLIC	PORT	REMOTE
COLOR	STATE	ERROR	ERROR	COUNT	DOWNTIME								
0	vpn0	dlia	0.0.0.0	0	0	0	0	192.168.0.231	12346	192.168.0.231	12346	default	tea
P-down CTREJSEZ NOERR 0 2019-06-01T19:06:32+0200													

An engineer is troubleshooting tear down of control connections even though a valid Certificate Serial Number is entered Which two actions resolve the Issue? (Choose two)

- A. Enter a valid serial number on the controllers for a given device
- B. Remove the duplicate IP in the network.
- C. Enter a valid product ID (model) on the PNP portal
- D. Match the serial number file between the controllers
- E. Restore network reachability for the controller

Answer: C,D

Explanation:

<https://community.cisco.com/t5/networking-documents/sd-wan-routers-troubleshoot-control-connections/tap/3813237>

Question: 113

Refer to the exhibit.

```

vpn 0
interface ge0/0
ip address 10.1.15.15/24
tunnel-interface
color lte
allow-service dhcp
allow-service dns
allow-service icmp

no allow-service sshd
no allow-service ntp
no allow-service stun
!
no shutdown
shaping-rate

```

Which shaping-rate does the engineer use to shape traffic at 9 Mbps?

- A. 9

- B. 9000
- C. 90000
- D. 9000000

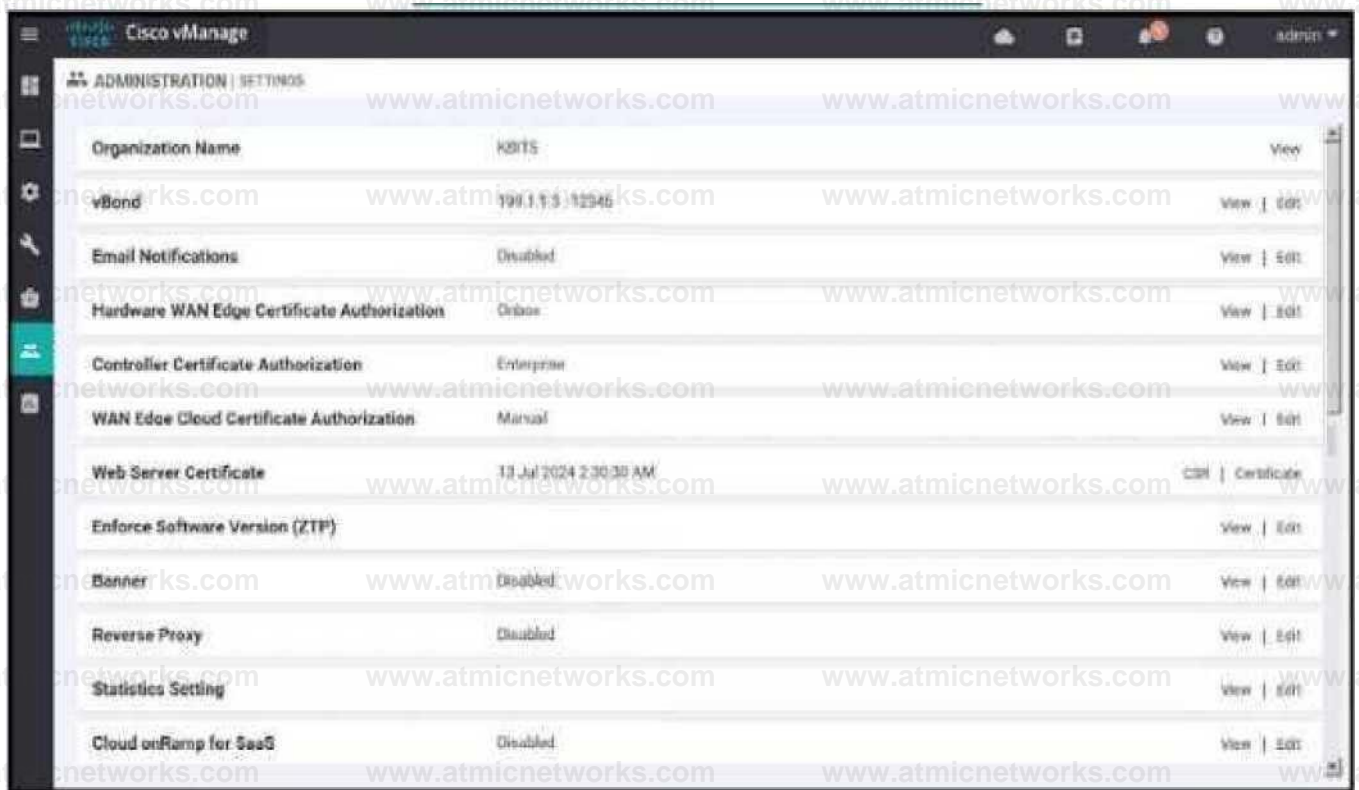
Answer: B

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#wp4217152133>

Question: 114

Refer to the exhibit.



Which two configurations are needed to get the WAN Edges registered with the controllers when certificates are used? (Choose two)

- A. Generate a CSR manually within vManage server
- B. Generate a CSR manually on the WAN Edge
- C. Request a certificate manually from the Enterprise CA server
- D. Install the certificate received from the CA server manually on the WAN Edge
- E. Install the certificate received from the CA server manually on the vManage

Answer: A,E

Explanation:

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/cisco-sd-wan-certificates-deploy-2020aug.pdf>

Question: 115

Refer to the exhibit.



Refer to the exhibit. The ge0/0 interface connects to a 30-MB link. A network administrator wants to always have 10 MB available for high priority traffic. When lower-priority traffic busts exceed 20 MB. Traffic should be redirected to the second WAN interface ge0/1. Which set of configurations accomplishes this task?

A)

```

interface ge0/0
  ip address 10.1.1.1 255.255.255.0
  bandwidth 30000
  class-map gold
    match ip dscp 54
  class-map silver
    match ip dscp 56
  class-map bronze
    match ip dscp 57
  policy-map p1
    class gold
      priority 10
    class silver
      priority 20
    class bronze
      priority 30
  service-policy p1

```

B)

```
policy
  policer bursty-traffic
    rate 100000
    burst 20000
    exceed continue
  access-list policer-bursty-traffic
    sequence 10
    match
      source-ip 56.0.1.0/24
    action accept
  policer bursty-traffic
    default-action accept
```

C)


```
policy
  policer bursty-traffic
    rate 1000000
    burst 20000
    exceed remark
  access-list policer-bursty-traffic
    sequence 10
    match
      source-ip 56.0.1.0/24
    action accept
  policer bursty-traffic
    default-action accept
```

D)

```
policy
  policer bursty-traffic
    rate 10
    burst 20
    exceed remark
access-list policer-bursty-traffic
  sequence 10
  match
    source-ip 56.0.1.0/24
  action accept
  policer bursty-traffic
  default-action accept
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

policy

```
policer bursty-traffic rate 1000000 burst 2000 0
```

```
exceed remark
```

```
access-list policer-bursty-traffic sequence 10
```

```
mat ch source-ip 55.0.1.0/24 action accept
```

```
policer bursty-traffic default-action accept
```

<https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=546>

Question: 116

An engineer is configuring a WAN Edge router for DIA based on matching QoS parameters. Which two actions accomplish this task? (Choose two.)

- A. Apply a QoS map policy.
- B. Configure a control policy.
- C. Configure a centralized data policy.
- D. Configure NAT on the transport interface.
- E. Apply a data policy on WAN interface.

Answer: C,D

Explanation:

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2020aug.pdf>

Question: 117

An administrator must configure an ACL for traffic coming in from the service-side VPN on a specific WAN device with circuit ID 391897770. Which policy must be used to configure this ACL?

- A. local data policy
- B. central data policy
- C. app-aware policy
- D. central control policy

Answer: A

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/Policy-basics.html>

Question: 118

What is an advantage of using auto mode versus static mode of power allocation when an access point is connected to a PoE switch port?

- A. It detects the device is a powered device
- B. All four pairs of the cable are used
- C. Power policing is enabled at the same time
- D. The default level is used for the access point

Answer: D

Explanation:

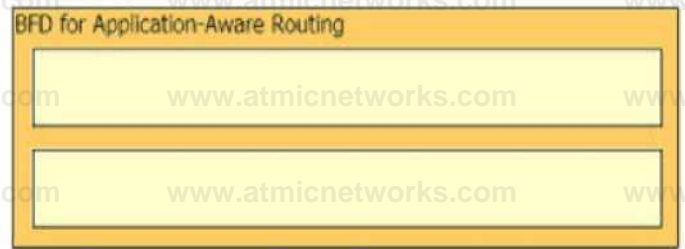
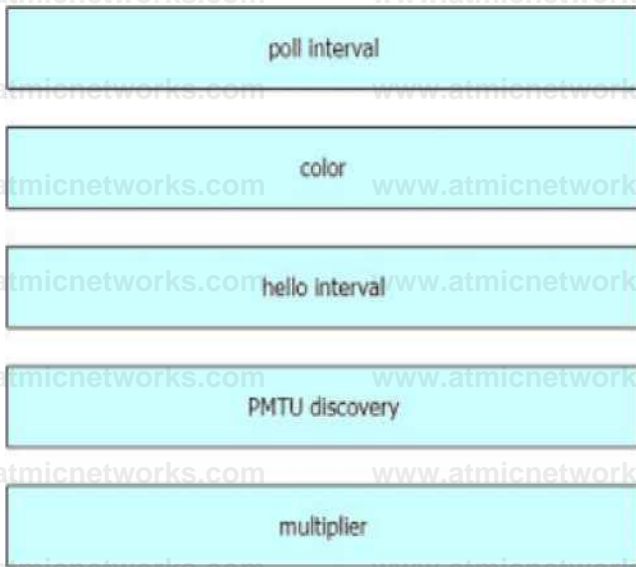
Use the auto setting on any PoE port. The auto mode is the default setting.

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011010.html

Question: 119

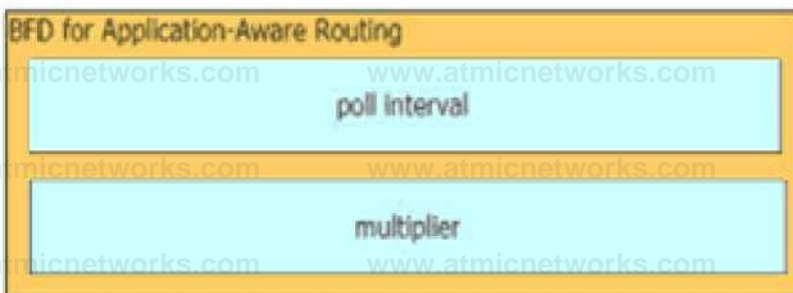
DRAG DROP

Drag and drop the BFD parameters from the left onto the BFD configurations on the right.



Answer:

Explanation:



https://sdwandocs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Configuration/Templates/BFD

Question: 120

Which plane assists in the automatic onboarding of the SD-WAN routers into the SD-WAN overlay?

- A. Data
- B. Orchestration

C. Management

D. Control

Answer: B

Explanation:

The Cisco SD-WAN solution is comprised of separate orchestration, management, control, and data planes.

- The orchestration plane assists in the automatic onboarding of the SD-WAN routers into the SD-WAN overlay.

Question: 121

Refer to the exhibit.

```
/Edge-C loud?
/Edge-cloud#
/Edge-Cloud# vshell
vEdge~Cloud:~$ cd /var/log/ vEdge-Cloud:/var/log$ /Edge-C 1 oud:/var/1 og$ ls -l total 28992
-rw-r--r--      1 root      root      1441700  NOV  22  15:13  auth.log
-rw-r--r--      1 basic      adm       0Aug    7 15:29  cloud-init.log
drwxr-xr-x      2 root      root      4096    NOV  22  14:49  confd
-rw-r--r--      1 root      root     1896486  NOV  22  14:57  kern.log
-rw-r--r--      1 root      root     292292  Aug   9  22:31  lastlog
-rw-r--r--      1 root      root     6197843  Nov   22  15:14  messages
-rw-r--r--      1 root      root     10512141 Aug  30  21:00  messages.1
drwxr-xr-x      2 root      root      4096    Nov   22  14:48  pdb
drwxr-xr-x      2 quagga    quagga    4096    Aug   7 15:29  quagga
-rw-r--r--      1 root      root      437     Nov   22  14:48  swscript^active.log
-rw-r--r--      1 root      root      382     Nov   22  14:48  sw_script_previous.lo
-rw-r--r--      1 root      root     2004    NOV  22  14:49  sw_script_syncddb.log
-rw-- .....    1 root      root     64064   Nov   22  15:07  tallylog
drwxr-xr-x      2 root      root      60      Nov   22  14:48  t nip log
-rw-r--r--      1. root      root     6841506  Nov   22  15:14  vconfd
-rw-r--r--      1 root      root     184602  Aug   7 15:29  vdebug
-rw-r--r--      1 root      root     2479511  Nov   22  15:14  vsyslog
-rwxr-xr-x      1 root      utmp     49536   Nov   22  15:07  wtmp
```

.'Edge-Cloud: /var/logS vEdoe-C loud: A ar loq\$

Refer to the exhibit. Which configuration stops Netconf CLI logging on WAN Edge devices during migration?

logs

audit disable

netcon (disable

logs

netconfdisable

logging

disk netconf-disable

logging

disk

audit-disable

np lr nn f-H i t ah IP

- A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#wp3867250313>

Syslog messages related to AAA authentication and Netconf CLI access and usage are placed in the auth.log and messages files. Each time Cisco vManage logs in to a Cisco vEdge device to retrieve statistics and status information and to push files to the router, the router generates AAA and Netconf log messages. So, over time, these messages can fill the log files. To prevent these messages from filling the log files, you can disable the logging of AAA and Netconf syslog messages:

```
Device(config) # system aaa logsViptela(config-logs) * audit-disableViptela(config-logs) ♦ netconf-disable
```

Question: 122

Refer to the exhibit.



Refer to the exhibit. An administrator is configuring a policy in addition to an existing hub-and-spoke policy for two sites that should directly communicate with each other. How is this policy configured?

- A. hub-and-spoke
B. mesh
C. import existing topology
D. custom control (route and TLOC)

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/controlpolicies.html#id_107219

Question: 123

An engineer is adding a tenant with location JD 306432373 in vManage. What is the maximum number of alphanumeric characters that are accepted in the tenant name field?

- A. 64
B. 128
C. 256

D. 8

Answer: B

Explanation:

In the Add Tenant window:

1. Enter a name for the tenant. It can be **up to 128 characters** and can contain only **alphanumeric characters**,

Question: 124

Which policy blocks TLOCs from remotes and allows TLOCs from the data center to form hub-and-spoke peering?

- A. localized control policy
- B. localized data policy
- C. centralized data policy
- D. centralized control policy

Answer: C

Explanation:

Centralized Policy

Centralized policy refers to policy provisioned on Cisco vSmart Controllers, which are the centralized controllers in the Cisco SD-WAN overlay network. Centralized policy comprises two components:

- Control policy, which affects the overlay network-wide routing of traffic
- Data policy; which affects the data traffic flow throughout the VPN segments in the network

Question: 125

For data plane resiliency, what does the Cisco SD-WAN software implement?

- A. BFD
- B. establishing affinity between vSmart controllers and WAN Edge routers
- C. multiple vBond orchestrators
- D. OMP

Answer: A

Explanation:

For data

plane resiliency, the Cisco SD-WAN software implements standard protocol mechanisms, specifically Bidirectional Forwarding Detection (BFD)

Question: 126

A network administrator is configuring a centralized control policy based on match action pairs for multiple conditions, which order must be configured to prefer Prefix List over TLOC and TLOC over Origin?

- A. highest to lowest sequence number
- B. nonsequential order
- C. deterministic order
- D. lowest to highest sequence number

Answer: D

Explanation:

A centralized control policy consists of a series of numbered (ordered) sequences of match-action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a route or TLOC matches the match conditions, the associated action or actions are taken and policy evaluation on that packets stops. Keep this process in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a route or TLOC matches no parameters in any of the sequences in the policy configure, it is, by default, rejected and discarded.

Question: 127

DRAG DROP

Drag and drop the Cisco SD-WAN components from the left onto their functions on the right.

vBond Orchestrator	IPsec key reflection and rekeying
vManage	first point of authentication
vSmart Controller	passes data plane traffic
WAN Edge Router	used to build configuration and policies

Answer:

Explanation:

vSmart Controller
vBond Orchestrator
WAN Edge Router
vManage

Question: 128

Which two features does the application firewall provide? (Choose two.)

- A. classification of 1400+ layer 7 applications
- B. blocks traffic by application or application-family
- C. numbered sequences of match-action pairs
- D. classification of 1000+ layer 4 applications
- E. application match parameters

Answer: A,B

Explanation:

This application aware firewall feature provides the following benefits:

- **Application visibility and granular control**
- **Classification of 1400- layer 7 applications**
- **Allows or blocks traffic by application, category, application-family or application-group**

Question: 129

Refer to the exhibit.

```
LAB-ROUTER#show ip route vrf 100
```

```
Gateway of last resort is 10.1.9.2 to network 0.0.0.0
```

```
m* 0.0.0.0/0 [251/0] via 10.1.9.2, 06:10:53
```

```
[251/0] via 10.1.9.3, 06:10:53
```

O 10.80.6.0/24

```
[110/300] via 172.19.75.78, 20:35:33, GigabitEthernet0/0/2.10
```

```
[110/300] via 172.19.75.66, lwo, GigabitEthernet0/0/1.11
```

O 10.80.56.0/24

```
[110/300] via 172.19.75.78, 20:35:33, GigabitEthernet0/0/2.10
```

```
[110/300] via 172.19.75.66, lwo, GigabitEthernet0/0/1.11
```

Refer to the exhibit. The network administrator has configured a centralized topology policy that results in the displayed routing table at a branch office. Which two configurations are verified by the output? [Choose two.]

- A. The routing table is for the transport VPN.
- B. The default route is learned via OMP.
- C. This routing table is from a cEdge router.
- D. The default route is configured locally.
- E. The configured policy is adding a route tag of 300 to learned routes.

Answer: B,C

Explanation:

Question: 130

Refer to the exhibit.

```
from-^mart data policy 1 ServirelseritnrnIPS^ direction fro ruse nice
```

```
Vpn lb I1
```

```
sequence 1
```

```
tu.itch destination ip 64.102.6.24" 52
```

```
■etna accept MI service aeUvcl servica local dpbiih-arlinn accept
```

Refer to the exhibit, which configuration configures IPsec tunnels in active and standby?

vpn 1
service nsvcl interface ipsec2

vpn-iist 1
count ServicePSed_275676046
from-vsmart Into vpn-iist i

vpn 1
vpn 0
service nsvcl interface ipsecZ

frotiHramirt lists vpn-iist 0
vpn 0

vpn1
service nsvcl interface ipsec2
fromvsmart lists vpn4l&t 1

vpn1
vpn 0
service nsvcl interface ipsec2

vpn-iist 1
ooount ^ivicAPSitd_775STfln4\$
frnm-vsmart fists vpn-iist 0
VDDJQ

A. Option A B. Option B C. Option C

D. Option D

Answer: C

Explanation:

Question: 131

Refer to the exhibit.

```
Site 1:  
vpn 10  
service FW address 1.1.1.1  
  
On vSmart  
policy  
lists  
site-list firewall-sites  
site-id 1  
  
apply-policy  
site-list firewall-sites control-policy firewall-service out
```

Refer to the exhibit, Which configuration routes Site 2 through the firewall in Site 1?

**control-policy firewall-service sequence ID match route site-id 2 action accept set
service local
default-action accept**

**On vSmart
control-policy firewall service sequence 10
match route site-id 2 action accept
set
service FW vpn 10 default-action accept**

**On vSmart
control-policy firewall-service sequence 10
match route site-id 2 action accept set
service FW vpn 10 service local
default-action accept**

**On vSmart
control-policy firewall-service sequence 10
match route site-id 2 action accept set service FW Vpn 10 default-action accept**

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html>

Here is the configuration procedure:

1. On the hub router, provision the firewall service, specifying the IP address of the firewall device. With this configuration, OMP on the hub router advertises one service route to the Cisco vSmart Controller. The service route contains a number of properties that identify the location of the firewall, including the TLOC of the hub router and a service label of svc-id-1, which identifies the service type as a firewall. (As mentioned above, before advertising the route, the device ensures that the firewall's IP address can be resolved locally.)

```
vpn 10  
service FW address 1.1.1.1
```

2. On the Cisco vSmart Controller, configure a control policy that redirects data traffic traveling from Site 1 to Site 2 through the firewall. Then, also on the Cisco vSmart Controller, apply this policy to Site 1.

```
policy  
lists site-list firewall-sites site-id 1  
control-policy firewall-service  
sequence 10 match route site-id 2 action accept set service FW vpn 10 default-action accept apply-policy site-  
list firewall-sites control-policy firewall-service out
```

Question: 132

A customer is receiving routes via OMP from vSmart controller for a specific VPN. The customer must provide access to the W2 loopback received via OMP to the OSPF neighbor on the service-side VPN, which configuration fulfils these requirements?

```
vpn 0
router
ospf
redistribute omp route-policy OSPFRoutePolicy area 0
interlace geO/2
exit
lists
prefix-list W2 Loopback
ip-prefix 10.10.10.5/24

route-policy OSPF_Route_Policy
sequence 1 match
address W2_Loopback

default action accept set
metric 100
metric-type typel
```

```
vpn 0
router
ospf
redistribute omp route-policy OSPF Route Policy area 0
interface geO/2 exit
lists
prefix-list W2 Loopback
ip-prefix 10.10.10.5/32
j
route-policy OSPF_Route_Policy
sequence 1
match
aHrirpcc W7 l nnnhark
```

metric-type typel

Wb l hl ft dipt ndhinbula mip rwh>p4Myi.0ltt Haute FoM tew 6

Interfit* uvUrf

*M

Mil

PfflifcJll WV kn^nh*rk iMttrti 10,1011 tell

fH*>potwM*P Rtfiiir Fuiitv

MquinM 1

MIkh tdrinwHI Loogbith

Mb* Mtfpi

■WHO IK

■wfnaJypt*tyP*!

vpp 10


```

UM *** IINIM WM M"1"
IIHWI
a»pi trihMbut>< anq rootofoha^ O#F ppute Foteev MN 4
intertill QIM IRll
MI
^TL! h> *3 k.UUUI^1
Mte* iirtubu

rwte'MKv O>w HIMW Fofcri
*tewM i
kMrit WT LMWIMI

Ulp
IMUtmftl rulni IMIW ^IIAy MFF RWfct PalkV m( interfit! Of 11J
■q
tali
piri.i i|n W; |X4«bH<l
UHllH i 10,1010^

touta-potea^ Dtn n^/aiify wqunH 1 nun
mditilhv.'mw&Mh

rtiwi K*MI
MI
Htta l#
■nitari rik» l^ptl

```

- A. Option A B. Option B C. Option C D. Option D E. Option E

Answer: D

Explanation:

Answer must start with VPN 10(service side) & should have metric-type 1 and not with VPN 0 (transport side)

Question: 133

An engineer wants to automate the onboarding process for a WAN Edge router with vManage. Which command will accomplish this?

- A. request vedge-cloud activate chassis-number <chassis-number> serial <serial>
- B. request vedge-cloud activate chassis-number <chassis-number> token <token-number>
- C. request vedge-cloud activate serial <serial> token <token-number>
- D. request vedge-cloud activate chassis-number <chassis-number> organization <organization>

Answer: B

Explanation:

```

vedge#
vedge> vedge request vedge-cloud activate chassis-number 19f2059b-5fd1-9027-a665-24c33d223247 token 22*eKb3a8c22d8269725dlcb495b718|

```

Question: 134

An administrator is configuring the severity level on the vManage NMS for events that indicate that an action must be taken immediately. Which severity level must be configured?

- A. warning
- B. error
- C. critical
- D. alert

Answer: D

Explanation:

- **Alert**— Action must be taken immediately (corresponds to syslog severity 1).

Question: 135

Which Cisco SD-WAN component the initial communication between WAN Edge devices to join the fabric?

- A. WAN Edge Router
- B. vSmart Controller
- C. vManage
- D. vBond Orchestrator

Answer: D

Explanation:

The Cisco **vBond Orchestrator** orchestrates the **initial control connection** between Cisco vSmart Controllers and vEdge routers. It creates DTLS tunnels to the Cisco vSmart Controllers and vEdge routers to authenticate each node **that is requesting control plane connectivity**. This authentication

Question: 136

In a Cisco SD-WAN network, which component is responsible for distributing route and policy information via the OMP?

- A. vManage
- B. vSmart Controller
- C. vBond Orchestrator

D. WAN Edge Router

Answer: B

Explanation:

The Cisco vSmart Controller maintains a centralized route table that stores the route information, called OMP routes, that it learns from the vEdge routers and from any other Cisco vSmart Controllers in the Cisco SD-WAN overlay network. Based on the configured policy, the Cisco vSmart Controller shares this route information with the Cisco vEdge network devices in the network so that they can communicate with each other.

Question: 137

DRAG DROP

Drag and drop the REST API calls from the left onto the functions on the right.

PUT

Retrieve or read.

GET

Update an object.

POST

Create an object.

DELETE

Remove an object.

Answer:

Explanation:

GET

PUT

POST

DELETE

GET: Get resource from the server.

POST: Create resource to the server.

PATCH or PUT: Update existing resource on the server.

DELETE: Delete existing resource from the server.

Question: 138

An engineer wants to change the configuration of the certificate authorization mode from manual to automated. Which GUI selection will accomplish this?

- A. Maintenance > Security
- B. Configuration > Certificates
- C. Administration > Settings
- D. Tools > Operational Commands

Answer: C

Explanation:

Runbook to Request and Install Cisco PKI Certificates

1. Verify that you have satisfied the prerequisites and that you have added the Smart Account credentials
2. Navigate to **Administration ► Settings ► Controller Certificate Authorization** and press Edit.
3. Select the **radio button Cisco Automated** (Recommended).

Question: 139

Which protocol is used for the vManage to connect to the vSmart Controller hosted in Cloud?

- A. PnP Server
- B. ZTP
- C. NETCONF
- D. HTTP

Answer: C

Explanation:

Netconf and CLI-Netconf is a standards-based protocol used by Cisco vManage to provision a Cisco vSmart Controller.

Question: 140

Which component is responsible for routing protocols such as BGP and OSPF in a Cisco SD-WAN solution?

- A. vSmart Controller
- B. vBond Orchestrator
- C. vManage
- D. WAN Edge Router

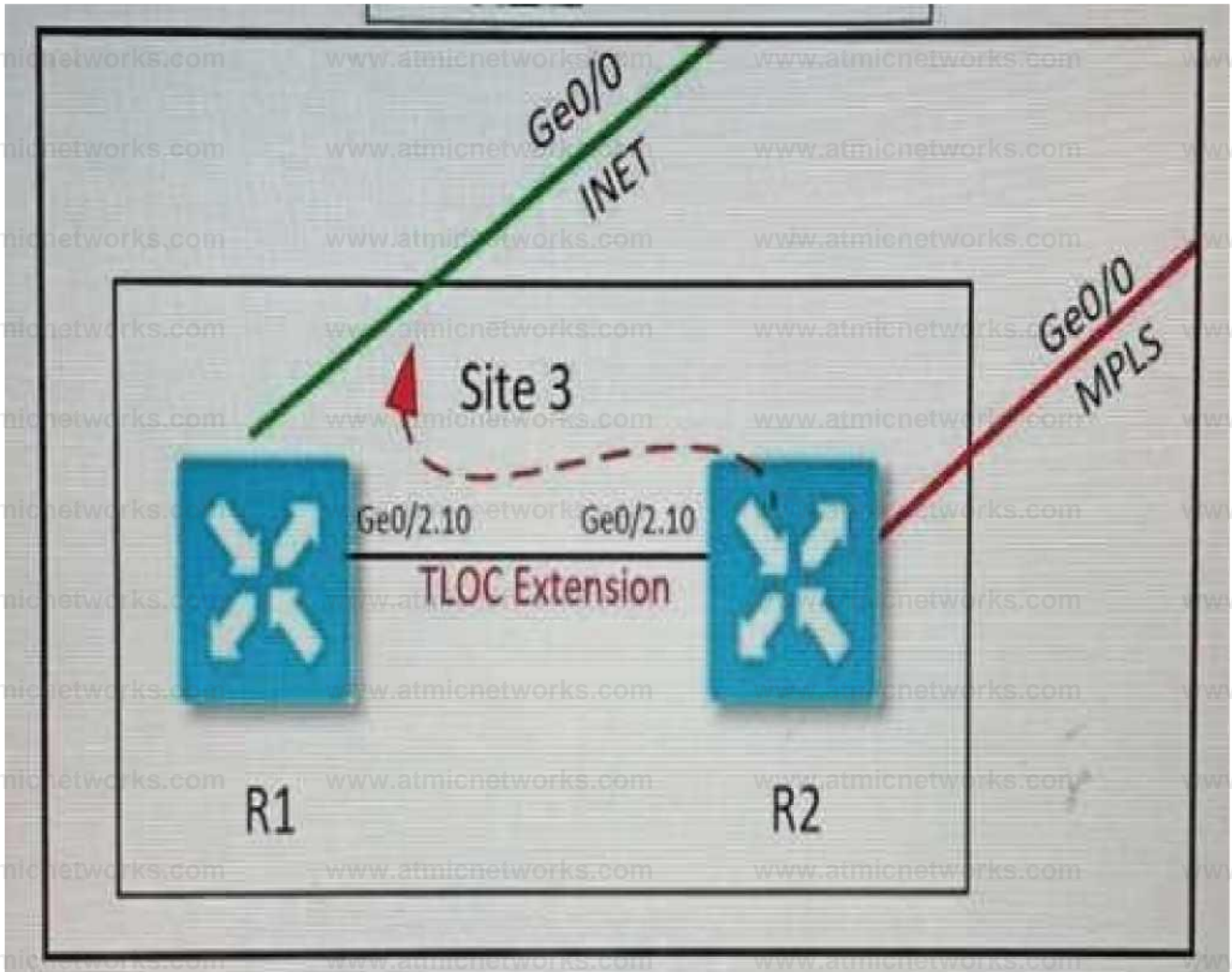
Answer: D

Explanation:

WAN Edge router - This device, available as either a hardware appliance or software-based router, sits at a physical site or in the cloud and provides secure data plane connectivity among the sites over one or more WAN transports. It is responsible for traffic forwarding, security, encryption, quality of service (QoS), routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), and more.

Question: 141

Refer to the exhibit.



Refer to the exhibit. Which configuration extends the INET interface on R1 to be used by R2 for control and data connections?

A)

```
R1
  ip interface virtual 100
    ip address 10.10.10.10/24
    ip address 10.10.10.10/24
```

```
R1
  ip interface virtual 100
    ip address 10.10.10.10/24
    ip address 10.10.10.10/24
```

```
R1
  ip interface virtual 100
    ip address 10.10.10.10/24
    ip address 10.10.10.10/24
```

```
Interfiled fl*O£ W i^iMwiiJa 43 43&N tiu-txtiMtan (fM
```

```
IM«rf»C« fr*O/2 n» ihutdown
```

```
Inttrf*c* f*W2 10 Ip *dd<»* 43 43 43 mil fist-sHenkleri fdM
```

B)

```
Ri iniBrfjc* p*W?
```

```
Interface g*0/2 10
```

```
Ip address 43 43 43,2130 do<»«xtMMton flvOC tunntHnterffr:*
```

```
color publte'IMdmM
```

```
interface 8*0/2
```

```
Interfax* g*0£ 10
```

```
|paHn»4343 43 lftO wnn«hIntorface
```

```
cst^r puhlwJNMH**1
```

C)

```
HI
```

```
ifrtdrfK* Qi#0J3 mlu 1604
```

Answer: C

Explanation:

<https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKRST-2091.pdf>

Subinterfaces require a physical, parent interface to be defined in VPN 0, and also require the subinterface MTU to be four bytes lower than the physical interface due to the 802.1q tag. It is recommended to configure the parent physical interface for an MTU of 1504 to take care of this requirement.

Question: 142

How does the replicator role function in cisco SD-WAN?

- A. WAN Edge devices advertise the rendezvous point to all the receivers through the underlay network.
- B. vSmart Controllers advertise the rendezvous point to all the receivers through the overlay network.
- C. WAN Edge devices advertise the rendezvous point to all receivers through the overlay network.
- D. vSmart Controllers advertise the rendezvous point to all the receivers through the underlay network.

Answer: B

Explanation:

Replicators

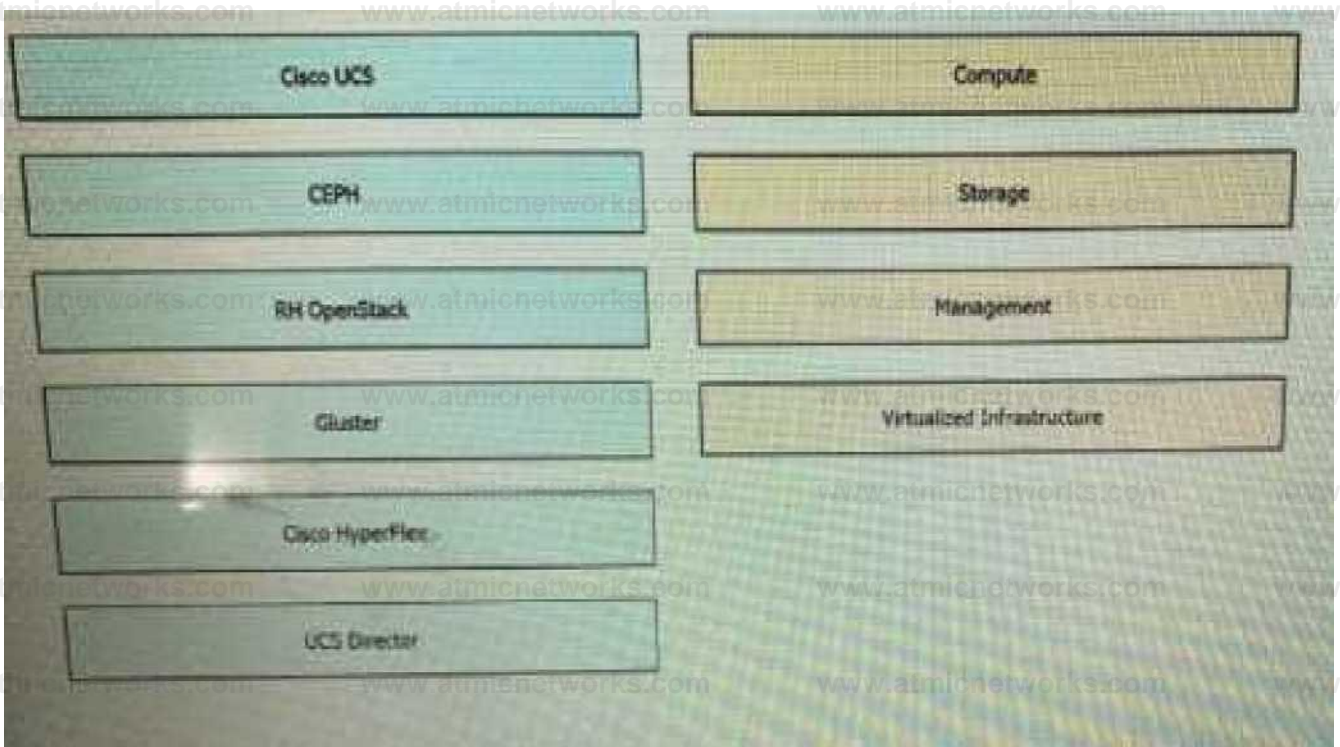
For efficient use of WAN bandwidth, strategic Cisco SD-WAN routers can be deployed and configured as replicators throughout the overlay network. Replicators mitigate the requirement for a Cisco SD-WAN router with local sources or the PIM-RP to replicate a multicast stream once for each receiver. As discussed above, replicators advertise themselves, using OMP multicast-autodiscover routes, to the Cisco vSmart Controllers in the overlay network. The controllers then forward the replicator location information to

the PIM-enabled Cisco IOS XE SD-WAN routers that are in the same VPN as the replicator.

Question: 143

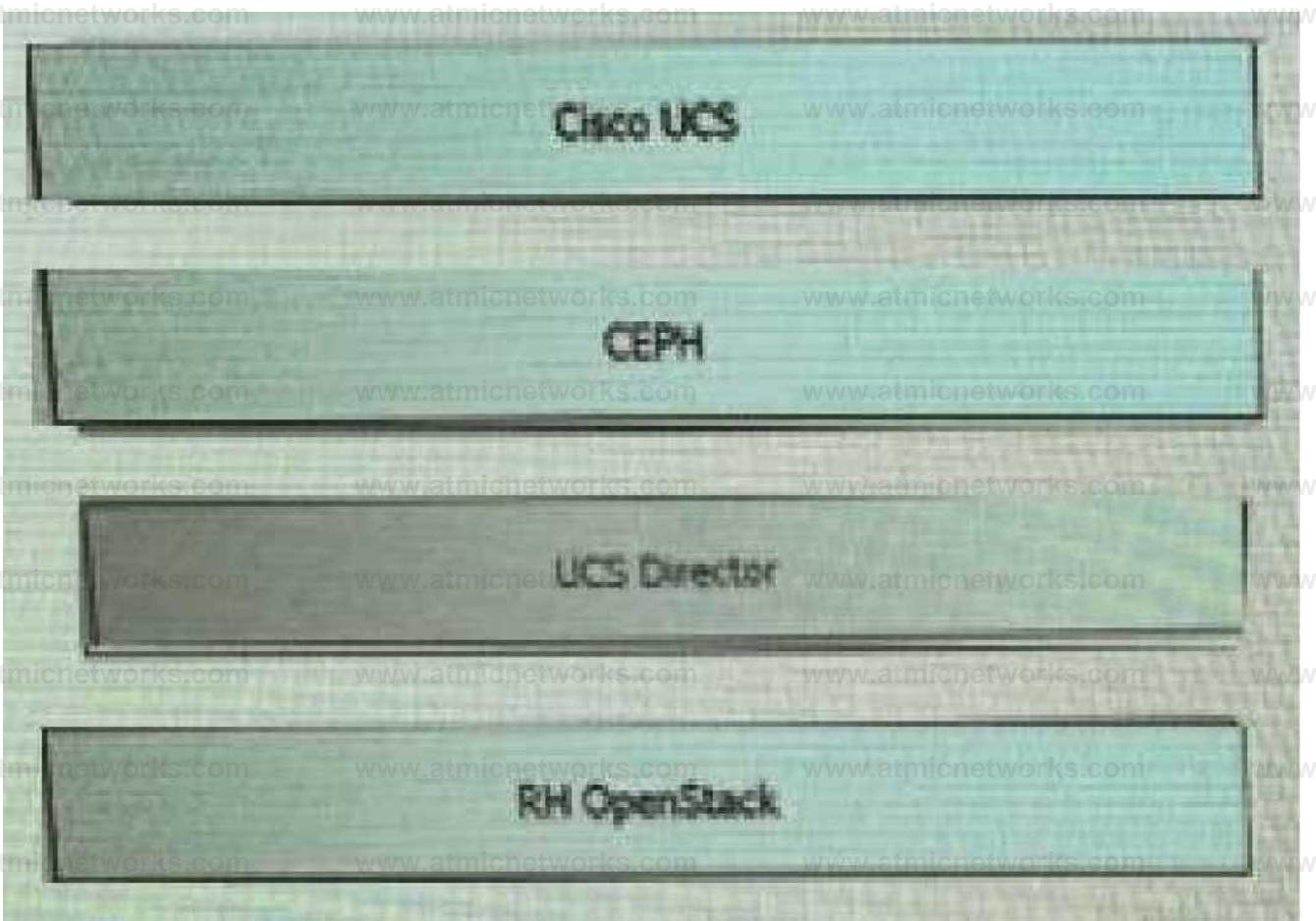
DRAG DROP

Drag and drop the components from the left onto the corresponding Cisco NFV infrastructure Building Blocks on the right. Not all options are used.



Answer:

Explanation:



Cisco NFV Infrastructure Building Blocks

- **Compute:** Cisco Unified Computing System™ (Cisco UCS®) for a carrier class and reliable compute infrastructure.
- **Storage:** Cisco UCS hardware and **CEPH provide** reliable storage. The user has the options to introduce additional storage as capacity needs grow.
- **Networking:** Cisco Nexus® 9000 series hardware provides high throughput, low latency, and rich feature sets.
- **Virtualized Infrastructure:** Fully integrated Red Hat Enterprise Linux and **Red Hat OpenStack** Platform runs on top of Cisco Unified Computing System™ (Cisco UCS®). It is open source yet hardened and mature.
- **Management:** Cisco **UCS Director** functions as a unified management tool across multiple virtual environments. SDN controller is optional.

Question: 144

Which two requirements must be met for DNS inspection when integrating with cisco umbrella? (Choose two)

- A. Upload the WAN Edge serial allow list to the Umbrella portal.
- B. Attach security policy to the device template.
- C. Configure the Umbrella token on the vManage
- D. Create and attach a System feature template with the Umbrella registration credentials.
- E. Register and configure the vManage public IP and serial number in the Umbrella portal.

Answer: B,C

Explanation:

<https://www.connection.com/~media/pdfs/brands/c/cisco/security/cnxx-cisco-sd-wan-and-umbrella.pdf?la=en>

Question: 145

Which feature allows reachability to an organization's internally hosted application for an active DNS security policy on a device?

- A. local domain bypass
- B. DHCP option 6
- C. DNSCrypt configurator
- D. data pokey with redirect

Answer: A

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/umbrella-integration.html>

• Local domain bypass list is global and each VRF can enable or disable the local domain bypass list. If enabled, the DNS packet will be matched against the local domain list.

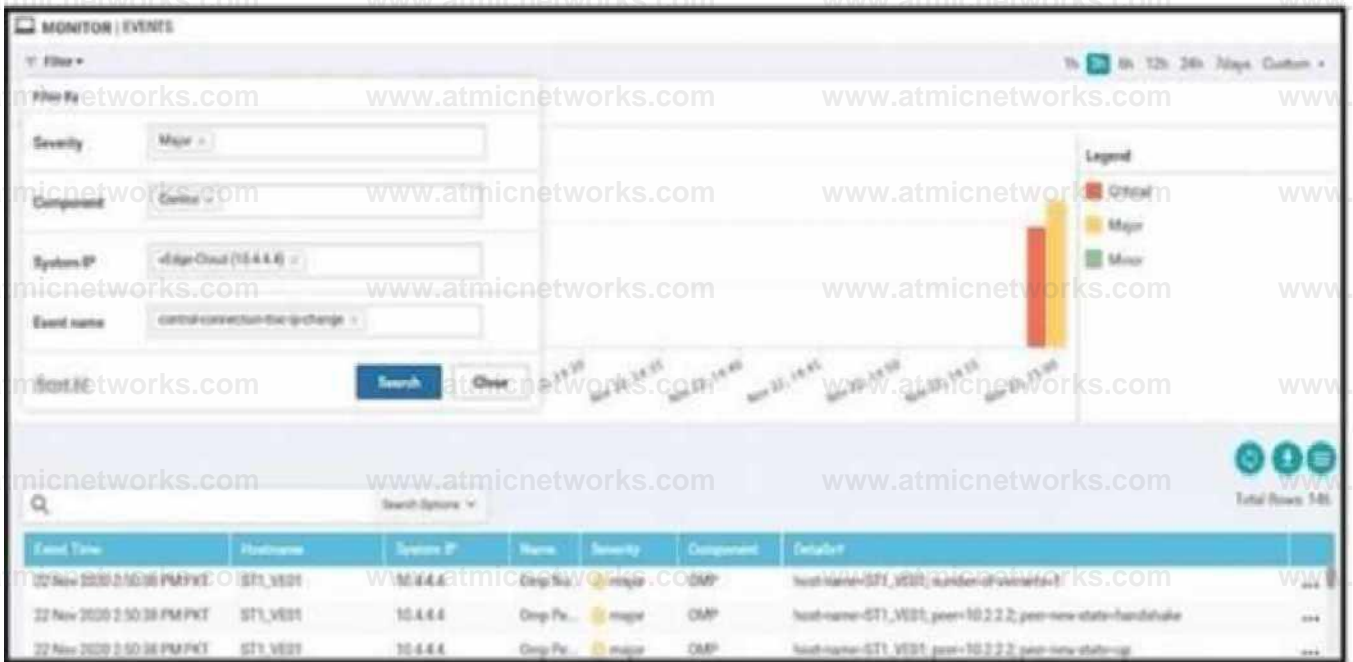
Question: 146

Refer to the exhibit.

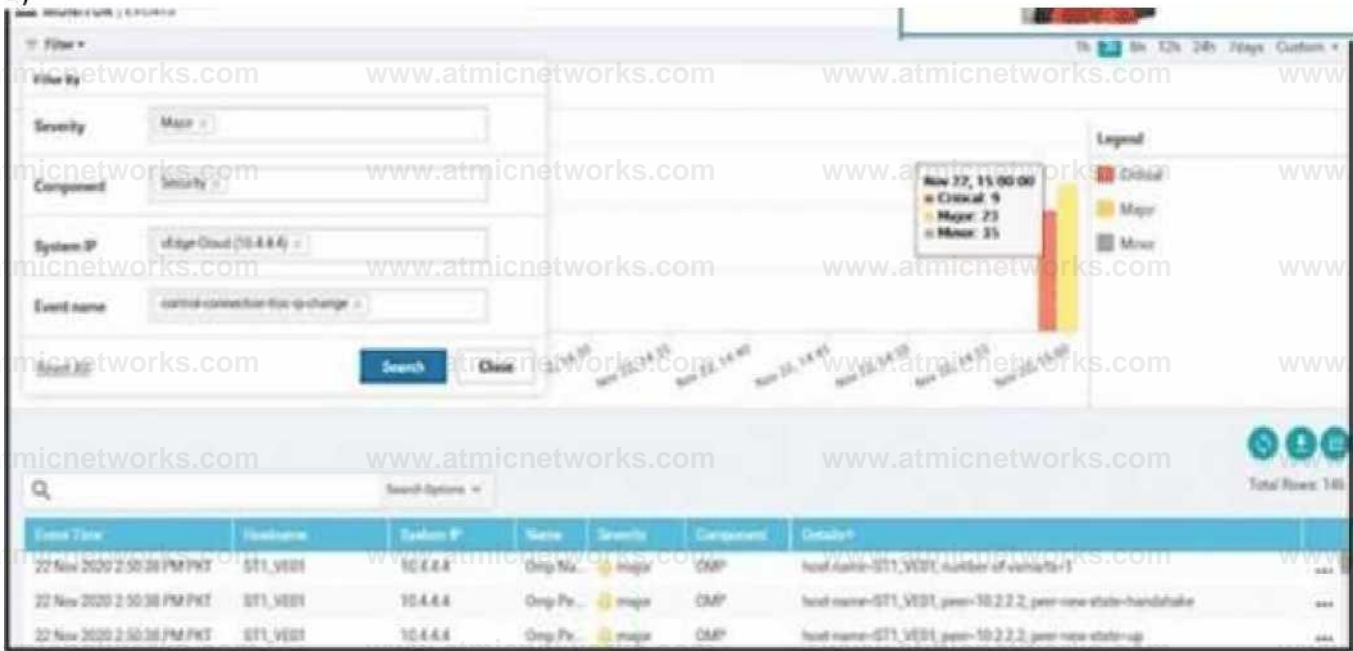
Variable List (Hover over each field for more information)	
System IP	10.4.4.4
Hostname	ST1_V101
Prefix(vEdge_Default_Gateway)	0.0.0.0/0
Prefix(Mpls_Default_Gateway)	0.0.0.0/0
Address(vEdge_Next_Hop_IP)	10.50.0.102
Address(MPLS_Next_hop_ip)	10.20.0.102
Hostname(Device_host_name)	vEdge-Cloud
Location(Device_location)	US
Latitude(Device_latitude)	40.7128
Longitude(Device_longitude)	74.0060
System IP(Device_system_ip)	10.4.4.4
Site ID(Device_site_id)	1

Refer to the exhibit. vManage logs are available for the past few months. A device name change deployed mistakenly at a critical site. How is the device name change tracked by operation and design teams?

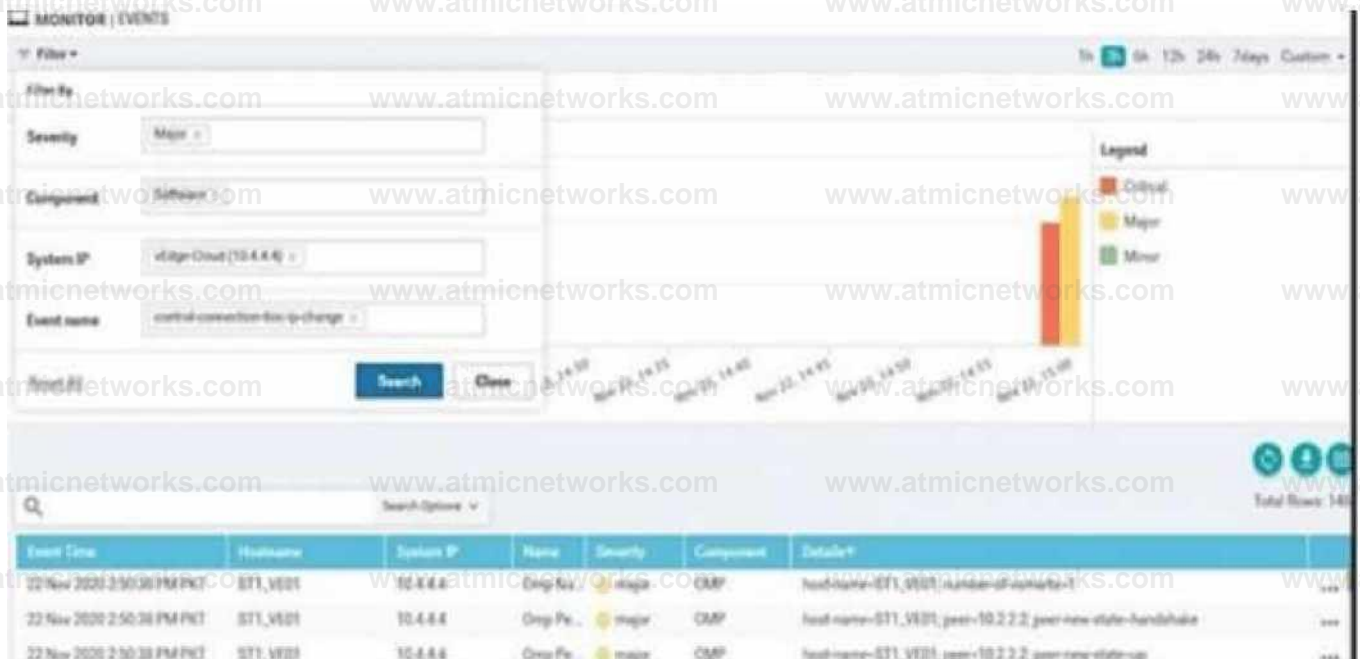
A)



B)



C)



A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 147

A customer must upgrade the cisco SD-WAN devices and controllers from version 19.2 to version 20.3. The devices include WAN Edge cloud, vManage, vSmart, and vBond. Which types of image files are needed for this upgrade?

- A. one file for vManage and one file for all other devices with extension tar.gz
- B. one file for vManage, one for vSmart and one for vBond + WAN Edge Cloud with extension .bin
- C. one file for vManaga, one for vSmart and one for vBond + WAN Edge Cloud with extension tar.gz
- D. one file for vManaga and one file for all other devices with extension .bin

Answer: C

Explanation:

<https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.3.1>

Question: 148

Which two prerequisites must be met before the Cloud onRamp for IaaS is initiated on vManage to expand to the AWS cloud? (Choose two)

- A. Attach the *AmazonCreateVPC* and "Amazon Provision EC2" permission policy to the IAM account
- B. Subscribe to the SD-WAN Edge router AMI in the AWS account
- C. Attach an OSPF feature template to the AWS cloud Edge router template
- D. Attach a device template to the cloud WAN Edge router to be deployed in the AWS
- E. Preprovision the transit VPC in the AWS region

Answer: B,D

Explanation:

The pre-requisites include verifying you meet the AWS prerequisites, including the necessary AWS credentials and subscriptions to the Amazon Machine Image (AMI) instances for Cisco SD-WAN Edge routers (Cisco CSR 1000v virtual routers or Cisco vEdge Cloud), verifying you have available tokens/licenses for at least two additional Cisco SD-WAN Edge Routers within Cisco vManage, and configuring and deploying device templates for the Cisco SD-WAN Edge routers that will be used within the transit VPCs.

Note that the creation of the customer host VPCs, shown in the figure above, is outside the scope of this document. It is assumed that one or more customer host VPCs have already been created.

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/Cisco_Cloud_onRamp_for_iaaS_AWS_Version2.html

Question: 149

An organization wants to use the Cisco SD-WAN regionalized service-chaining feature to optimize cost and user experience with application in the network, which allows branch routers to analyze and steer traffic toward the required network function. Which feature meets this requirement?

- A. Cloud Services Platform
- B. VNF Service Chaining
- C. Cloud onRamp for Colocation
- D. Cloud onRamp for IaaS

Answer: C

Explanation:

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf>

The solution provides enterprises with multiple distributed branch offices that are clustered around major cities or spread over several countries the ability to regionalize the routing services in colocation facilities.

Question: 150

What are the two protocols redistributed into OMP? (Choose two.)

- A. OSPF
- B. RIP
- C. LDP
- D. RSVP
- E. EIGRP

Answer: A,E

Explanation:

Supported Protocols

This section explains the protocols supported for unicast routing

- [OMP Routing Protocol](#)
- [BGP and OSPF Routing Protocols](#)
- [OSPFv3](#)
- [EIGRP](#)

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-unicast-routing.html>

Question: 151

An engineer is adding a tenant with location ID 399533345 in vManage. What is the maximum number of alphanumeric characters that is accepted in the tenant name field?

- A. 64
- B. 128
- C. 256
- D. 8

Answer: B

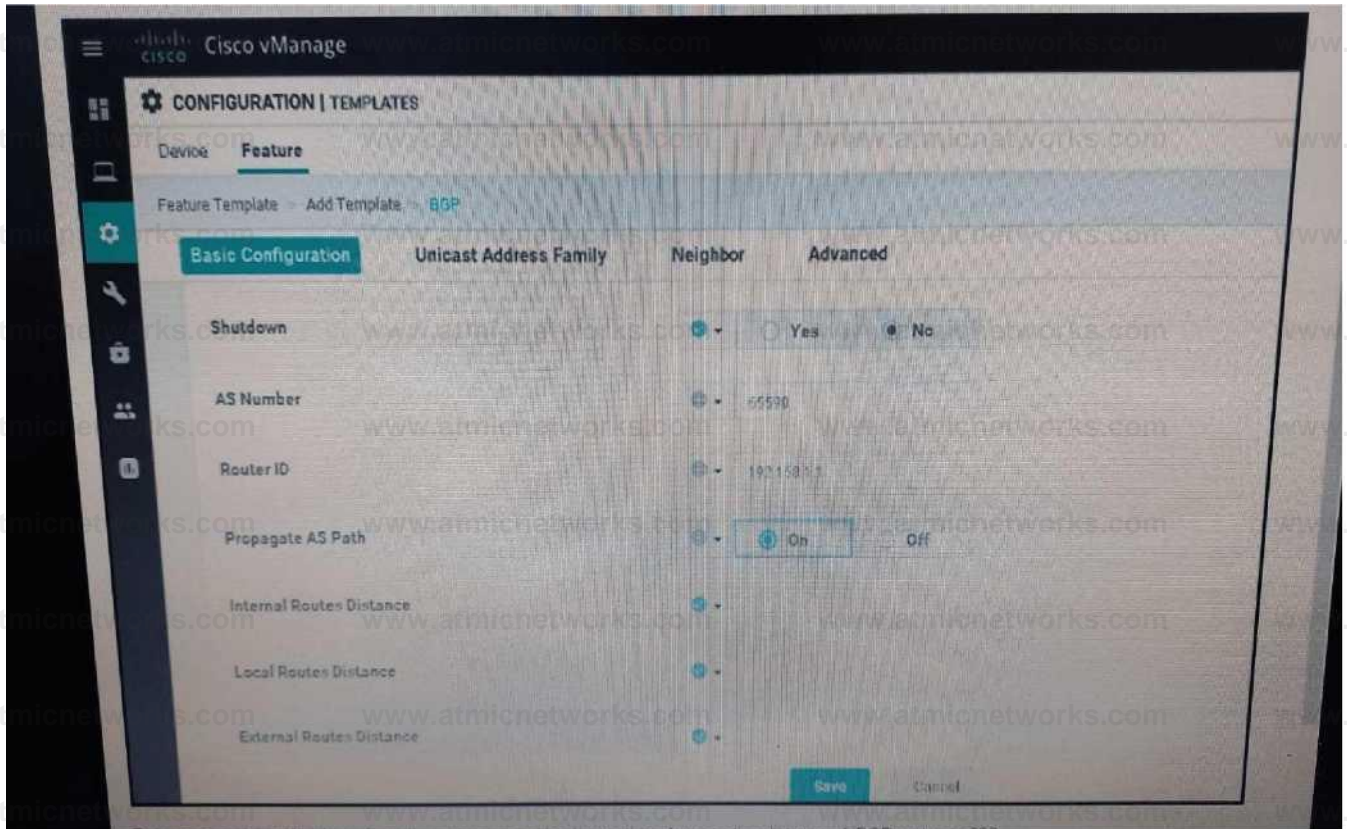
Explanation:

In the Add Tenant window:

- a. Enter a name for the tenant. It can be up to 128 characters and can contain only alphanumeric characters.

Question: 152

Refer to the exhibit.



Refer to the exhibit. Which configuration value is used to change the administrative distance of iBGP routes to 20?

- A. Configure internal Routes Distance to 20
- B. Configure Propagate AS Path to off
- C. Configure Local Distance to 20
- D. Configure External routes distance 20

Answer: C

Explanation:

Question: 153

Refer to the exhibit.

Timestamp	User	User IP	Message
MDOcZON	eyrtm	10.1.1.1	Upbade root ca umd het Me on /Bond
11 Dec 2020	q*M	101.11	T rendered nootca uud Ini Mo lo
WK 2020	m\$MH	10111	intiafAD tool cert cha<n on
ISOKXUO	system	101.11	Tiensteted root cel chan Me to »\$cnddIMI2'
1#Dvc 2030	MVlam	Will	imJaied root cert cnam on /Smart M/tad3t
ISOK2W0	rHwn	10.1.1.1	Twidrad root cart (fan U< io *SrMrl M/SM
ito*cnn	system	io T n	UpioaM root ca <«d M Ma on ^onSSLulK
11 Dec 2030	tylMm	l0l 1 1	imMM root cert cnam on /Manage b<&Mfcf
IS tec BN	t^las	101.1.1	lundMSMtc«M/MM»lo*>Mta>2
		10111	TmMMt cart Cn H, io MMsgHStt

vManage# show certificate installed

Server certificate

Certificate:

Data:

Version: 1 (0x0)

Serial Number:

dO:dl:fO:eO:63:52:c9:3a

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=UK, ST=ENG, L=London, O=ABC, CN=SDWAN.lab

Validity

Not Before: Jul 30 19:42:30 2020 GMT

Not After: Jul 30 19:42:30 2021 GMT

Subject: C=US, ST=California, L=San Jose, OU=ABC,

O=vIptela Inc, CN=vmanage-6842d5cf-ce74-41a0-9ff5-10e810f9ddab-

0.vm

Subiect Public Key Info:

Public Key Algorithm: rsaEncryption Public-Key: (2048 bit)

Refer to the exhibit A small company was acquired by a large organization As a result, the new organization decided to update information on their Enterprise RootCA and generated a new certificate using openssl Which configuration updates the new certificate and issues an alert in vManage Monitor | Events Dashboard?

Step1: Generate the RootCA Certificate

```
openssl x509 -req -in vmanage_csr \  
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \  
-out vmanage.crt -days 365 -sha256
```

Step2: Install the RootCA Certificate

vManage > Administration > Settings > Controller Certificate Authorization >
Enterprise Root Certificate

Step1: Generate the RootCA Certificate

```
openssl x509 -req -in vmanage_csr \  
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \  
-out vmanage.crt -days 365 -sha256
```

Step2: Install the RootCA Certificate

vManage > Administration > Settings > Controller Certificate Authorization >
Symantec Automated (Recommended)

Step1: Generate the RootCA Certificate

```
vManage:~$openssl req -x509 -new -nodes -key ROOTCA.key -  
sha256 -days 2000 \  
-subj "/C=UK/ST=ENG/L=London/O=XYZ/CN= SDWAN.lab " \  
-out ROOTCA.pem
```

Step2: Install the RootCA Certificate

vManage > Administration > Settings > Controller Certificate Authorization >
Enterprise Root Certificate

Stepn Gorwat* ht RMICA Certificate

```
Yttin|f*|<iptniil nq -xi&3 -nnw -nodfia -k*y lIOiJTtX icy -shn2Cfi  
-days 1H0 \  
-libJ */M!!/(tMn/IriIMd4II/(MIC/ate ^ DM AN 1 At - \  
-Mt FOCTCA pM
```

8hp2: install ire RaoEA Certificate

vManage > Adminitlra'jM > Sell nq& > Cunbctac Ctn^cjl0 Authonzai^n *
Symantec Alternated (RMonnwriwl)

- A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

7 Generate Root CA certificate named rootca.pem and sign it with rootca.key that was generated ON the previous step

```
vmanage:~/web$ openssl req -x509 -new -nodes -key rootca.key -sha256 -days 4000 -out rootca.pem
```

Question: 154

What is a requirement for a WAN Edge to reach vManage, vBond, and vSmart controllers in a data center?

- A. IGP
B. QoS
C. TLS
D. OMP

Answer: A

Explanation:

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf>

Question: 155

The network administrator is configuring a QoS scheduling policy on traffic received from transport side tunnels on WAN Edge 5000 routers at location 406141498 Which command must be configured on these devices?

- A. cloud-qos
B. service qos
C. cloud-mis qos
D. mis qos

Answer: A

Explanation:

Question: 156

Refer to the exhibit.

	tn XX I¹)		
	eth1 . eth0 vManage		
	(.2) XJk (.2) eth1 ^^		209.165.201.0.0/28 Transport
	vSmart		tn ^ . eO/Ok/V HQ
10.10.10.0/24 Mgmt	geO/O vBond		

```

vManage                                vBond
system                                 system
system-ip 10.10.10.101                 system-ip 10.10.10.103
host-name vManage                       host-name vBond
site-id 1                               site-id 1
clock timezone Europe/London           clock timezone Europe/London
vbond 209.165.201.3                     vbond 209.165.201.3 local
organization-name Cisco.com            organization-name viptela.com
!                                       !
vpn 0                                    vpn 0
interface eth0                          interface ge0/0
ip address 209.165.201.1/28             ip address 209.165.201.3/28
no shut                                  no shut
tunnel-interface                        tunnel-interface
allow-service all                       encapsulation ipsec
allow-service all                       allow-service all
ip route 0.0.0.0/0 209.165.201.14     ip route 0.0.0.0/0 209.165.201.14
!                                       !
commit                                  commit

```

Refer to the exhibit vManage and vBond have an issue establishing a connection with each other Which action resolves the issue?

- A. Reconfigure the system IPs to belong to the same subnet
- B. Change the organization name on both controllers to match vipteta.com.
- C. Remove the encapsulation ipsec command under the tunnel interface of vBond
- D. Configure the encapsulation ipsec command under the tunnel interface on vManage

Answer: B

Explanation:

<https://community.cisco.com/t5/sd-wan-and-cloud-networking/encapsulation-ipsec-on-vbond/td-p/4451149>
 "encapsulation" command under vBond tunnel-interface has no meaning and effect.

Question: 157

Refer to the exhibit.

```

vpn 1
service netsvd interlace ipsec1

```



```
from-vsmari data-paliqy 1 ServiceeelsenionIPSec
```

```
direction front-service
```

```
vpn4$ 1
```

```
sequence 1
```

```
match
```

```
destnafjon-ip 11 11/32
```

```
action accept
```

```
set
```

```
service netsvc1
```

```
default-action accept
```

```
from-vsmart lists vpn-list 1
```

```
vpn 1
```

Refer to the exhibit Which command allows traffic through the IPsec tunnel configured in VPN 0?

- A. service local
- B. service FW address 1.1.1.1
- C. service netsvc1 vpn 1
- D. service netsvc1 address 1.1.1.1

Answer: B

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html>

Question: 158

Which third-party Enterprise CA server must be used (or a cloud-based vSmart controller)?

- A. RootCert
- B. Microsoft
- C. RADIUS
- D. VeriSign

Answer: A

Explanation:

Question: 159

What is the behaviour of vBond orchestrator?

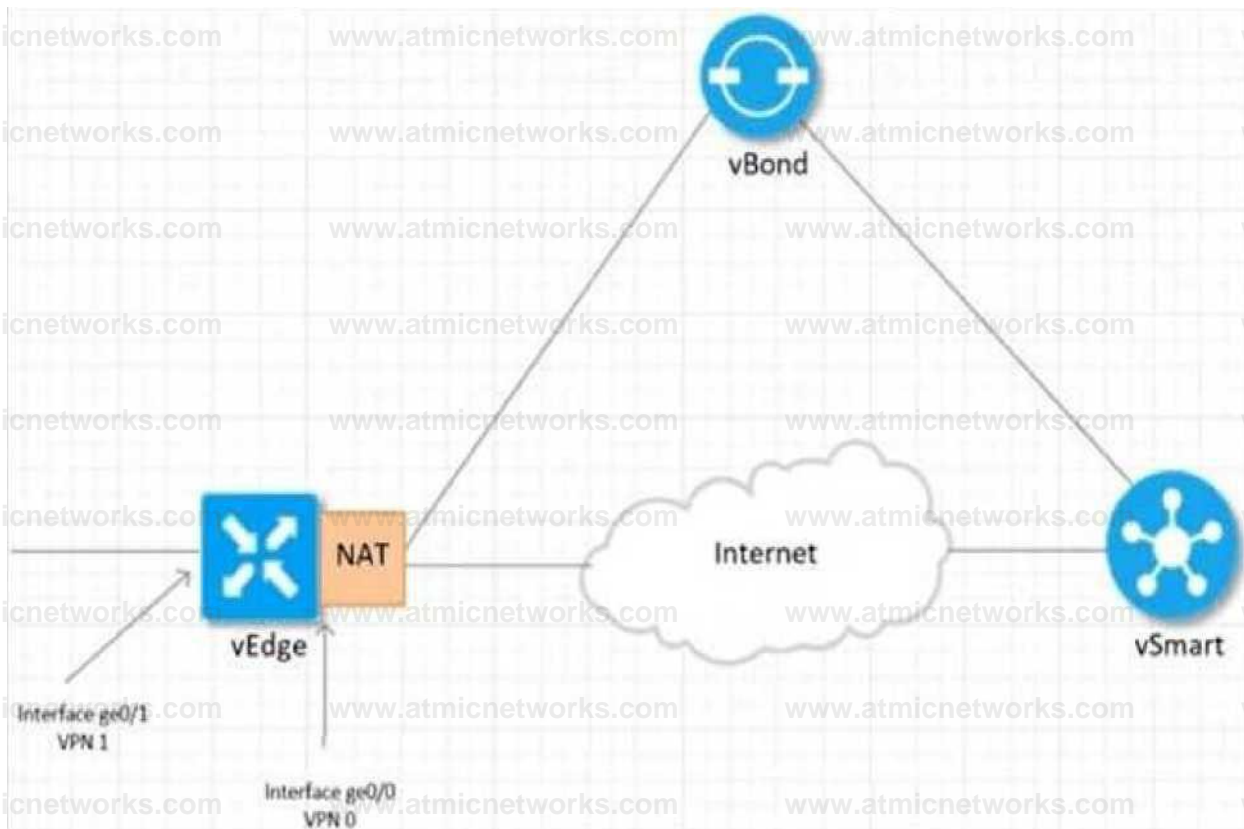
- A. It maintains vSmart and WAN Edge routers secure connectivity state
- B. it builds permanent connections with vSmart controllers
- C. it updates vSmart of WAN Edge routers behind NAT devices using OMP.
- D. It builds permanent connections with WAN Edge routers

Answer: A

Explanation:

Question: 160

Refer to the exhibit.



Refer to the exhibit Which configuration sets up direct Internet access for VPN 1?

vpn 1

interface grtH

nit

no shutdown

vpn0

ip route 0.0.0.0/0 vpn 1

vpn 1

interface ge(J/O nat

no shutdown

vpn 0

ip route 0-0 00 vpn 1

vpn 0

interface ge0!1

ip ML

no shutdown

vpn 1

ip route 0-0.0.0/0 vpn 0

□□XUXmiXIXIXIIXCXXXXXXXXXXCCXZIXZXXXXXIIIZI^MDDOHZXXXXXE0EXKISmniZEIIXXXXXXX

A. Option A B. Option B C. Option C

Answer: C

Explanation:

Question: 161

An engineer is configuring a shaping rate of 1 Mbps on the WAN link of a WAN Edge router Which configuration accomplishes this task'

vpn vpn-id interface interface-name
shaping-rate 1000 0 00

vpn vpn-id

interface interface-name shaping -rate 1000

interface interface-name vpn vpn-id
shaping-rate 1000 000

interface interface-name vpn vpn-id
shaping-rate 1000

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 162

Refer to the exhibit.

FIX* rm	FIX* MKWCot	MOA mnx	1X11 IF 10 ID	DOMAIN raft	PXIVATI IF rwr	FAJVATt	FIX# muc :r	tUBLIC iwr	LOCAL COW* >TA7X	LOCAL NILOTIC UFXAT we* mo* cowrr
vbcnd	dUa		0 0	204.1<S.2M.2M	12346	204,165 200.230	12346	bi e-internet	tear down	CTOMMMIS NOW 14
vbcnd	dtla	*	0 0	200 165 201.137	12346	204.165 201.137	12346	bia^intamet	tear-down	CTOASNMMIS NOXAX 13

Refer to the exhibit An engineer is getting a CTORGNMMIS error on a controller connection Which action resolves this issue?

- A. Configure a valid serial number on the WAN Edge
- B. Configure a valid organization name
- C. Configure a valid certificate on vSMART
- D. Configure a valid product ID

Answer: B

Explanation:

Question: 163

Which routing protocol is used to exchange control plane information between vSmart controllers and WAN Edge routers in the Cisco SD-WAN secure extensible network?

- A. BGP
- B. OSPF

- C. BFD
- D. OMP

Answer: D

Explanation:

Question: 164

How is multicast routing enabled on devices in the Cisco SD-WAN overlay network?

- A. The WAN Edge routers originate multicast service routes to the vSmart controller via OMP, which then forwards joins for requested multicast groups based on IGMP v1 or v2 toward the source or PIM-RP as specified in the original PIM join message.
- B. The vSmart controller originates multicast service routes to the WAN Edge routers via OMP, which then forwards joins for requested multicast groups based on IGMP v1 or v2 toward the source or PIM-RP as specified in the original PIM join message.
- C. The vSmart controller originates multicast service routes to the WAN Edge routers via OMP, which then forwards joins (or requested multicast groups based on IGMP v2 or v3 toward the source or PIM-RP as specified in the original PIM join message).
- D. The WAN Edge routers originate multicast service routes to the vSmart controller via OMP, which then forwards joins for requested multicast groups based on IGMP v2 or v3 toward the source or PIM-RP as specified in the original PIM join message.

Answer: A

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-multicast-routing.html>

Question: 165

What is an attribute of TLOC?

- A. encryption
- B. local preference
- C. tag
- D. service

Answer: C

Explanation:

Question: 166

An administrator must deploy the controllers using the On-Prem method while vManage can access the PnP portal from inside How are the two WAN Edge authorized allowed lists to be made available to vManage? (Choose two)



A. Option A B. Option B C. Option C D. Option D

Answer: A,B

Explanation:

https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Configuration/Devices

Question: 167

An engineer must configure a centralized policy on a site in which all HTTP traffic should use the Public Internet circuit if the loss on this circuit is below 10%. otherwise MPLS should be used Which configuration wizard fulfils this requirement?

- A. Create Applications or Groups of Interest > Configure Traffic Rules > Apply Policies to Sites and VPNs
- B. Configure VPN Membership > Apply Policies to Sites and VPNs
- C. Create Applications or Groups of interest > Configure Traffic Data > Apply Policies to Sites and

VPNs

- D. Configure Topology > Apply Policies to Sites and VPNs

Answer: A

Explanation:

Question: 168

An enterprise has several sites with multiple VPNs that are isolated from each other A new requirement came where users in VPN 73 must be able to talk to users in VPN 50 Which configuration meets this requirement?

```
policy
control-policy Route-Leaking
sequence 1 match route VPN_73 prefix-Net Jtoylpv^PrefixUrt action accept
sequence 11 match route vpndistWfOO pre fl a d i st _A ny l pvdPrefix List action accept
export-to vpn-Jist VPN_73 default-action accept
```

policy

```
control-policy Route-Leaking
sequence 1 match route VPN_73 prefix -1 i & t _Any l pvd Prefix Li BI export-to VPN_50
sequence 11 match route VPN_50 prefix diet .ArtylpydPrefiXLISt expOf-to VPNJ3
default-action accept
```

policy

```
control-policy Route-Leaking
```

```
sequence 1
match route
VPN-ALL
prefix-list_AnyIpv4PrefixList
action accept filter-xprt-to VPN_ALL
```

```
policy
control-policy Route-Leaking
```

```
sequence 1
match route
VPN-50 VPN-73
prefix-list_AnyIpv4PrefixList
action accept
export^ VFN_73VFN_50
```

A. Option A B. Option B C. Option C D. Option D

Answer: A

Explanation:

Question: 169

An engineer must use data prefixes to configure centralized data policies using the vManage policy configuration wizard. What is the first step to accomplish this task?

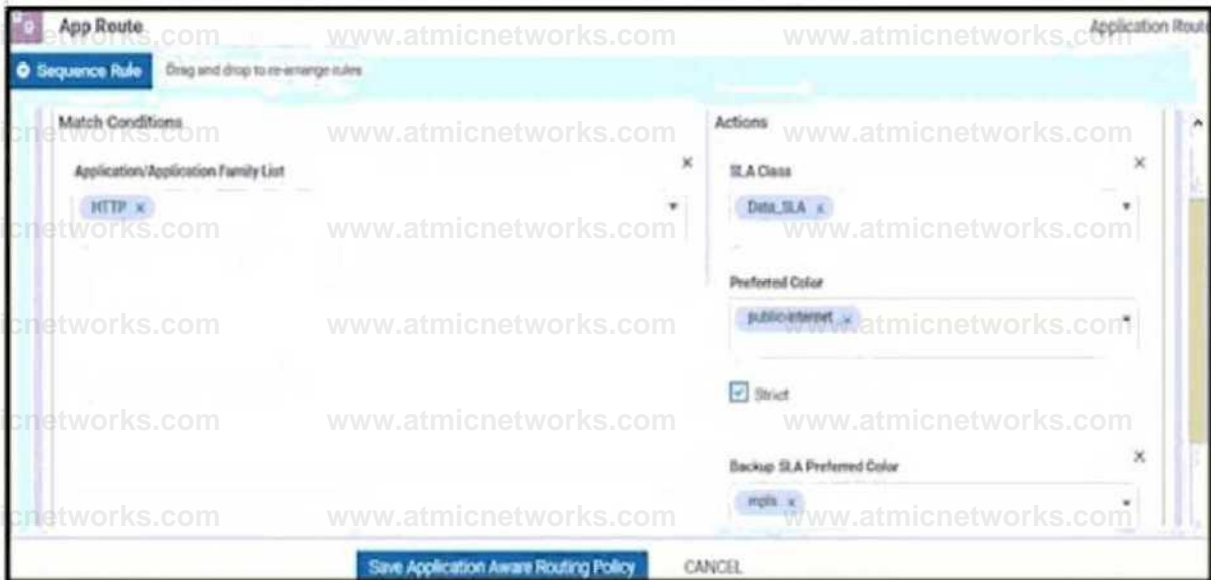
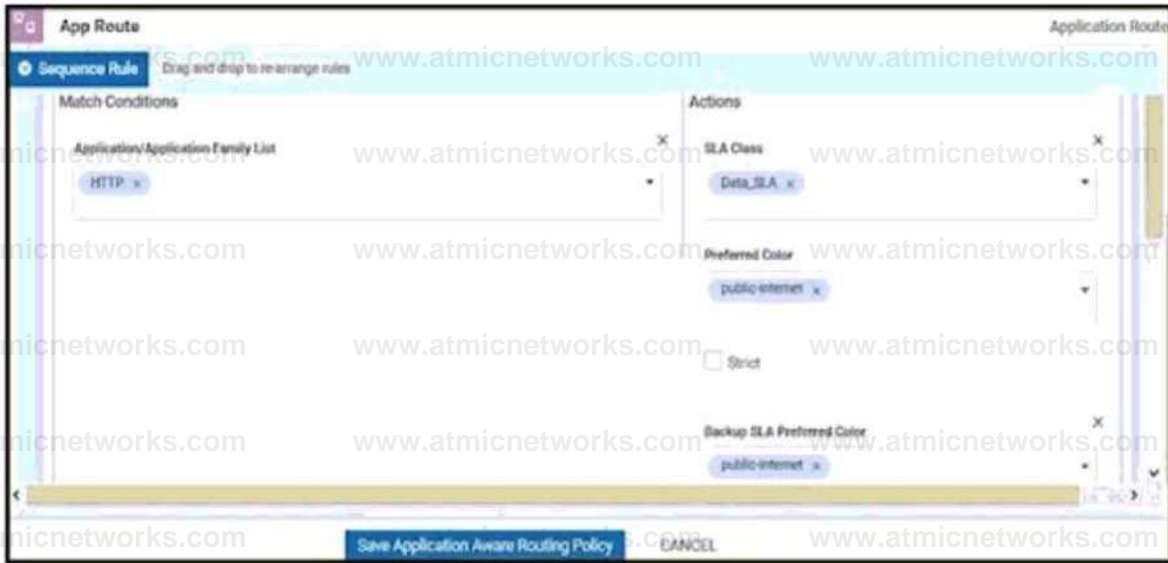
- A. Create groups of interest
- B. Configure network topology.
- C. Configure traffic rules.
- D. Apply policies to sites and VPNs.

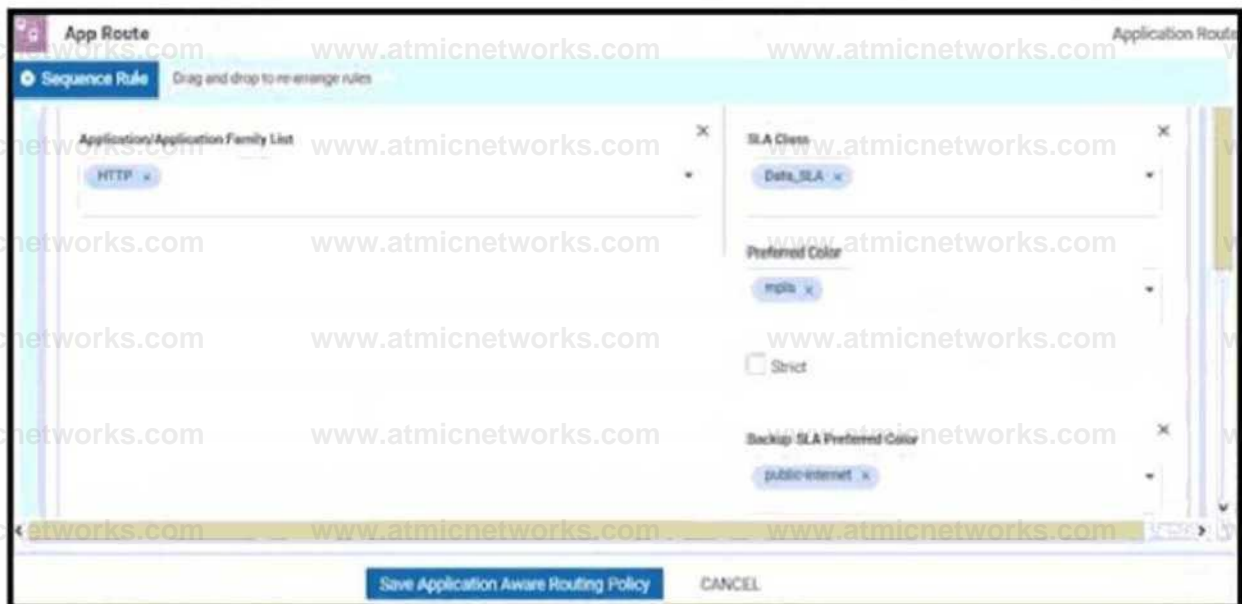
Answer: A

Explanation:

Question: 170

An engineer must improve video quality by limiting HTTP traffic to the Internet without any failover. Which configuration in vManage achieves this goal?





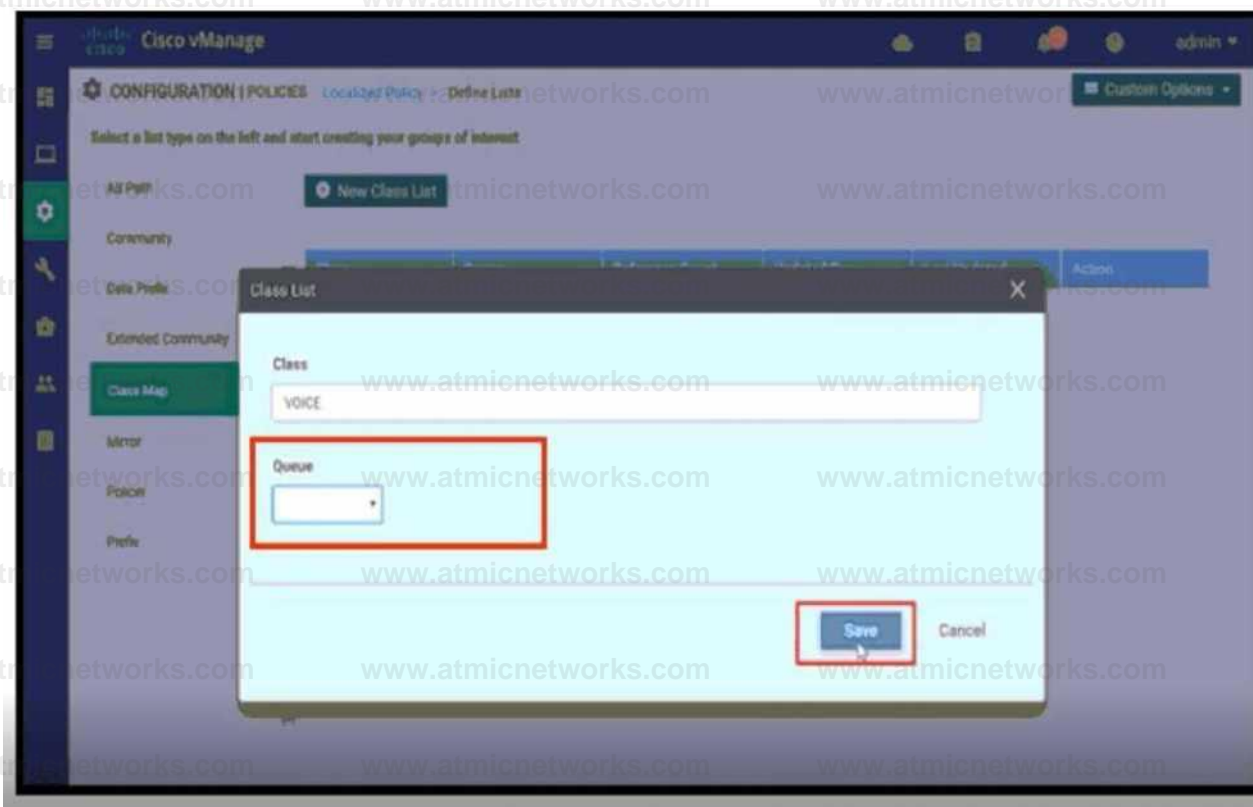
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 171

Refer to the exhibit.



Refer to the exhibit. A network administrator is setting the queuing value for voice traffic for one of the WAN Edge routers using vManager GUI. Which queue value must be set to accomplish this task?

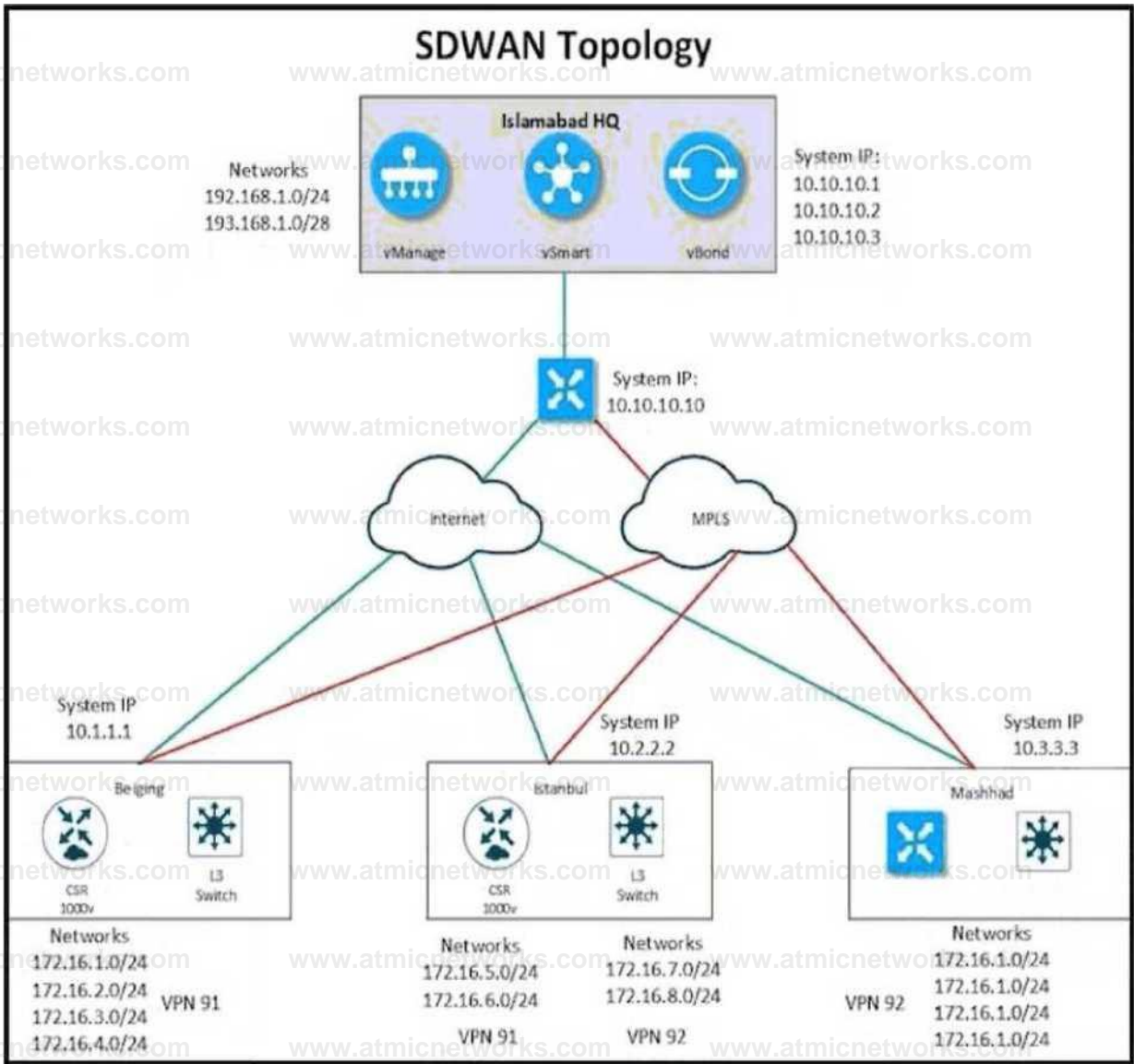
- A. 0
- B. 1
- C. 2
- D. 3

Answer: A

Explanation:

Question: 172

Refer to the exhibit.



Q Centralized Policy

O Localized Policy

CLI Policy

CLI Policy

Lists

Lists

Topology

Forwarding Class/QoS

Traffic Policy

Access Control Lists

Route Policy

Refer to the exhibit The Cisco SD-WAN network is configured with a default full-mesh topology. Islamabad HQ and Islamabad WAN Edges must be used as the hub sites. Hub sites MPLS TLOC must be preferred when forwarding FTP traffic based on a configured SLA class list. Which policy configuration does the network

engineer use to call the SLA class and set the preferred color to MPLS?

- A. Localized Policy, Route Policy
- B. Centralized Policy, Traffic Policy
- C. Localized Policy, Forwarding Class
- D. Centralized Policy Topology

Answer: B

Explanation:

Question: 173

Which set of elements are verified by the controller to confirm the identity of edge devices?

- A. certificates, organization name and serial number of the device
- B. organization name serial number and system IP of the device
- C. certificates, organization name, and vBond domain
- D. certificates, system IP, and vBond domain

Answer: A

Explanation:

Question: 174

WAN Edge routers are configured manually to use UDP port offset to use nondefault offset values when IPsec tunnels are created. What is the offset range?

- A. 1-19
- B. 0-18
- C. 0-19
- D. 1-18

Answer: C

Explanation:

Question: 175

An engineer configures policing with a rate of 125 Bps and a burst rate of 8000 bits, as shown here:

policy policer pl
rate

```
burst
exceed drop i
access-list acH
sequence 1
match
source-ip 2.2.0.0/16
destination^ 10.110/24 100.110/24
destination-port 20 30
protocol 6 17 23
```

```
action accept policer pl
```

```
default-action drop
```

```
vpn 1 t
interface geO 4
description Policy ID: B413:A88D:76G7::4
ip address 10.20.24.15/24
no shutdown
access-list acl out
```

Which configuration completes this task?

- A. Configure 125 for rate and 1000 for burst.
- B. Configure 1000 for rate and 64000 for burst
- C. Configure 125 for rate and 8000 for burst
- D. Configure 1000 for rate and 1000 for burst

Answer: D

Explanation:

Question: 176

A customer has MPLS and Internet as the TLOC colors An engineer must configure conrolLers with the Internet and not with MPLS Which configuration achieves this requirement on vManage?

A)

```
vpn 0 interface eLM
ip add res? 10.50.0.1/24 tunnel-interlace color mpis
```

B) vpn 0 interface eth1

```
ip address 10.50.0.1/24 tunnel-interface color public-Internet
```

C) vpn 0

```
I interface eth1
```

```
ip address 10.50.OT2*
```

```
tunnef-interface color Hi-Internet
```

D)

```
vpn 0
1 interface «h1
  ip address 10 M 0.1 24 tunnel-interface color default
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

Question: 177

Which plane builds and maintains the network topology and makes decisions on traffic flows?

- A. orchestration
- B. management
- C. control
- D. data

Answer: C

Explanation:

Question: 178

What is a benefit of using REST APIs?

- A. predefined automation and orchestration platform for event management and logging
- B. user-defined automation and integration into other orchestration systems or tools
- C. vAnalytics to simplify operational services integration and real-time event monitoring
- D. predefined SD-WAN controller with other platform integration for event management and logging

Answer: B

Explanation:

Question: 179

How is TLOC defined?

- A. It is represented by a unique identifier to specify a site in as SD-WAN architecture.
- B. It specifies a Cisco SD-WAN overlay in a multitenant vSMART deployment.

- C. It is a unique collection of GRE or iPsec encapsulation, link color, and system IP address.
- D. It is represented by group of QoS policies applied to a WAN Edge router.

Answer: C

Explanation:

Question: 180

Which two criteria are supported to filter traffic on a Cisco Umbrella Cloud-delivered firewall? (Choose two)

- A. tunnels
- B. site ID
- C. URL
- D. geolocation
- E. protocol

Answer: A,E

Explanation:

<https://docs.umbrella.com/umbrella-user-guide/docs/add-a-firewall-policy>

Question: 181

In a customer retail network with multiple data centers, what does the network administrator use to create a regional hub topology?

- A. control policy on vManage
- B. control policy on vSmart
- C. data policy on vSmart
- D. app route policy on vSmart

Answer: A

Explanation:

Question: 182

What is the default value (in milliseconds) set for the poll interval in the BFD basic configuration?

- A. 300,000
- B. 600,000

- C. 900,000
- D. 1,200,000

Answer: B

Explanation:

https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Configuration/Templates/BF D

Question: 183

A Cisco SD-WAN customer has a requirement to calculate the SHA value for files as they pass through the device to see the returned disposition and determine if the file is good, unknown or malicious. The customer also wants to perform real-time traffic analysis and generate alerts when threats are detected Which two Cisco SD-WAN solutions meet the requirements? (Choose two.)

- A. Cisco Trust Anchor Module
- B. Cisco Threat Grid
- C. Cisco Snort IPS
- D. Cisco AMP
- E. Cisco Secure Endpoint

Answer: C,D

Explanation:

Question: 184

Which vBond system configuration under VPN 0 allows for a routable public IP address even if the DNS name, hostname, or IP address of the vBond orchestrator are omitted?

- A. local
- B. vbond-only
- C. dns-name
- D. WAN

Answer: A

Explanation:

Question: 185

An engineering team must prepare a traffic engineering policy where an MPLS circuit is preferred for traffic coming from the Admin VLAN Internet should be used as a backup only. Which configuration fulfill this requirement?

A)

policy

data-policy TB vpn-list VPNJD sequence 1 match

s o u r e - d a l a - p r e f i l l i s t S C u r w . P r t f i x d e s t i n a t i o n * d a t a - p r e f i x * l i s t

D e \$ t _ P r e f i x a c t i o n a c c e p t

s e t v p n 1 0 d o c - l i s t H u b - I L O G i d e f a u l t - a c t i o n r e j e c t

t l o c - l i s t H u b _ T L O C s

t l o c 1 0 . 4 . 4 . 4 c o l o r m p l s e n e a p I p W C p r e f e r e n c e 3 0 0

t l o c 1 0 . 4 . 4 . 4 c o l o r p u b l i e - i n t e r n s t « n u p i p w c p r e f e r e n c e 6 0 0

B)

policy

data-policy TE

vpn-list VPN1

sequence 1 match

source-data-prefix-list Source_Prefix

destination-data-prefix-list Dest_Prefix

action accept

nat use-vpn 0

nat fallback

default-action reject

Uoc-ItMHub.TLOCs

tloc 10.4.4.4 color mpls encap ipsec preference 300

tloc 10.4.4.4 color public-internet encap ipsec preference 600

C)

policy

data-policy TE

vpn-list VPN.1D

sequence 1

match

source-data-prefix-list Source_Prefix

destination-data-prefix-list Dest_Prefix

action accept

set

vpn 10

tloc-list Hub_TLOCs

default-action accept

tloc-list Hub_TLOCs

tloc 10.4.4.4 color mpls encap ipsec preference 600

tloc 10.4.4.4 color public-internet encap ipsec preference 300

D)

policy

data-policy IE

vpn-list VPN JO

sequence 1 match

source-data-prefix-list Source_Prefix destination-data-prefix-list Dest_Prefix action accept set vpn 512 Hoc-list HubJLOCs default-action accept I tloc-list HubJLOCs Hoc 10.4.4.4 color mpls encap ipsec preference 600 tloc 10.4.4.4 color public-internet encap ipsec preference 300

A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

Question: 186

A company must avoid downtime at the remote sites and data plane to continue forwarding traffic between WAN Edge devices if the branch router loses connectivity to its OMP peers Which configuration meets the requirement?

A)

CONFIGURATION | TEMPLATES

Device Feature

Feature Template: Add Template: OMP

Basic Configuration Timers Advertise

Graceful Restart for OMP On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown Yes No

B)

Feature Template: Add Template: OMP

Basic Configuration Timers Advertise

Graceful Restart for OMP On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown Yes No

C)

CONFIGURATION | TEMPLATES

Device Feature

Feature Template: Add Template OMP

Basic Configuration Timers Advertise

Graceful Restart for OMP On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown Yes No

D)

CONFIGURATION | TEMPLATES

Device Feature

Feature Template: Add Template OMP

Basic Configuration Timers Advertise

Graceful Restart for OMP On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown Yes No

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

Question: 187

Which secure tunnel type should be used to connect one WAN Edge router to other WAN Edge routers?

- A. TLS
- B. DTLS
- C. SSL VPN
- D. IPsec

Answer: D

Explanation:

Question: 188

An engineer is configuring a data policy for IPv4 prefixes for a single WAN Edge device on a site with multiple WAN Edge devices How is this policy added using the policy configuration wizard?

- A. In vManage NMS, select the configure ► policies screen, select the localized policy tab and click add policy
- B. In vSmart controller, select the configure ► policies screen, select the localized policy tab. and click add policy
- C. In vManage NMS. select the configure ► policies screen select the centralized policy tab and click add policy
- D. In vBond orchestrator. select the configure ► policies screen, select the localized policy tab. and click add policy

Answer: A

Explanation:

Question: 189

Refer to the exhibit.

Which command-line configuration on a WAN Edge device achieves these results? A)

```

vpn 0
interface ge0/0
ip address 10.50.0.101/30
tunnel-interface encapsulation grt
color public-internet
restrict all allow-service all
ip route 0.0.0.0/0 10.50.0.102
    
```

B)

Protocol	Status	Jitter (ms)	Loss (%)	FEC Loss
IPSEC	↑			0
rac	↑			0
race	↑			0
IPSEC	↑			0

ip route 0.0.0.0/0 10.50.0.102

C)

```

vpn 0
interface ge0/0
ip address 10.50.0.101/30 tunnel-interface encapsulation ipsec allow-service none
ip route 0.0.0.0/0 10.50.0.102
    
```

D)

vpn 1

Interface ge0/0

ip address 10.50.0.105/30 tunnel-Interface encapsulation

ipsec color public-internet restrict How-service all

How-service netconf

ip route 0.0.0.0/0 10.50.0.102

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 190

Company E wants to deploy Cisco SD-WAN with controllers in AWS The company's existing WAN is on private MPLS without Internet access to controllers in AWS An Internet circuit is added to a site in addition to the existing MPLS circuit. Which interface template establishes BFD neighbors over both transports?

A)



B)



- C)
- Miss
- D)



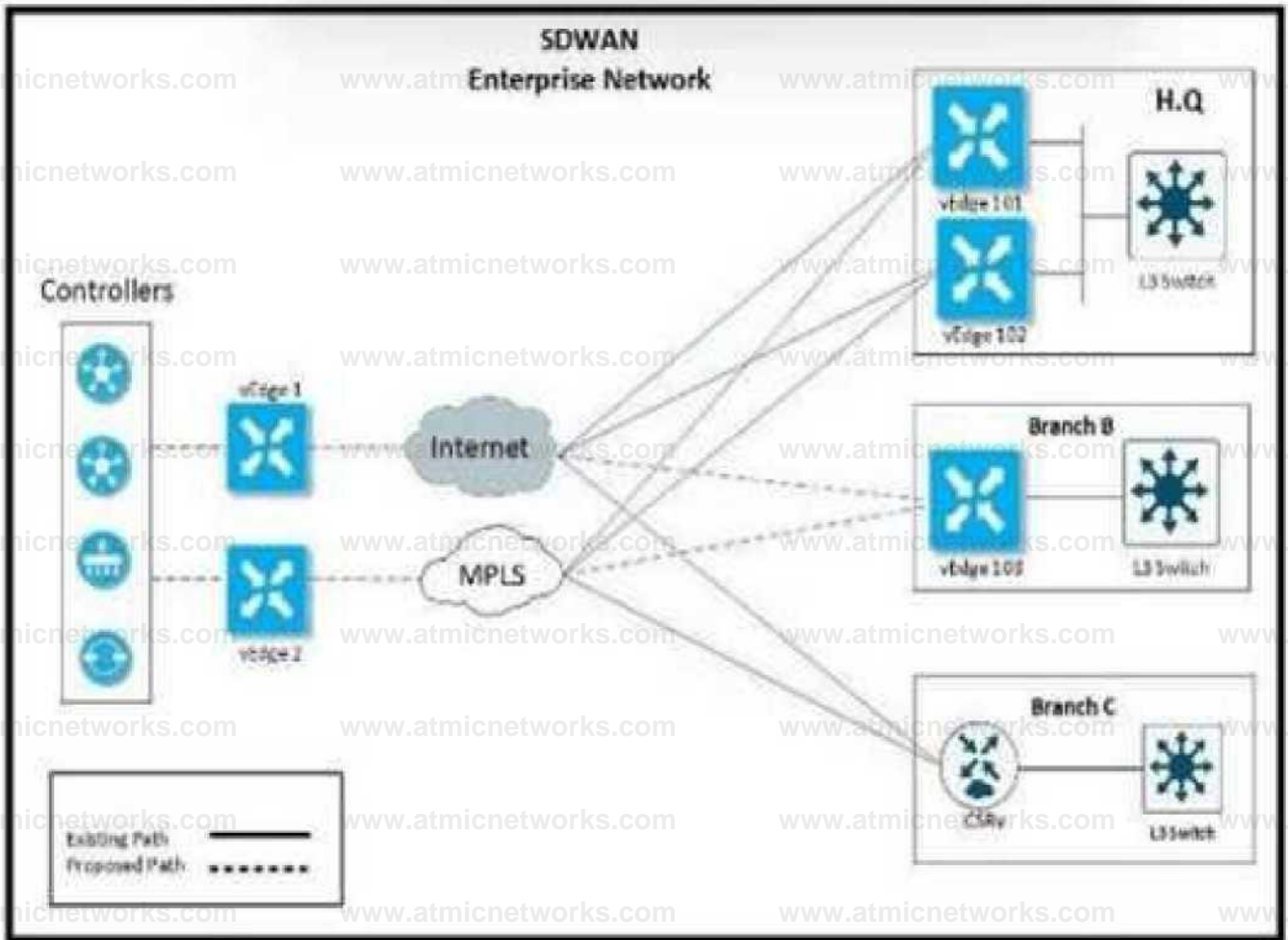
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 191

Refer to the exhibit.



The network team must configure branch B WAN Edge device 103 to establish dynamic full-mesh IPsec tunnels between all colors with branches over MPLS and Internet circuits. The branch is configured

with:

```

v ip>>h-1 y 5^rn:iyMc^
3flV CD n-|Qd*1 v»dg»-cfoud
lwt-iiiani ^Edgt-Cloud
iDCJt.as C
mtStWTFIp A 10.4 4 *
dWMin4d *M46 1

WQiniutijM-nMn* ABC (fork
imuo-x U$N«wy«rt vtoond
10 10.01 pe« 12146

amp
TO Shutdown jnafui-rttuit

```

```

wh M2 ini>rfa» »rhD
.p jddfHt IOLO.QLUN
l1Q tHutdbwfi

```

Which configuration meets the requirement?

A)

vpn 0

interface ge0/0

description 'Internet Circuit' ip

address 209.165.200.225/30 tunnel-
interface

encapsulation ipsec color public-

internet allow-service all

interface ge0/1

description '* MPLS ip address

10.10.0.101/30 tunnel-interface

encapsulation ipsec color mpls allow-
service all

B)

vpn 0

interface ge0/0

description 'Internet Circuit'

ipaddress 209.165.200.225/30 tunnel-
interface

encapsulation ipsec

color public-internet restrict allow-

service all

interface ge0/1

description ' MPLS ' ipaddress

10.10.0.101/30 tunnel-interface

encapsulation ipsec color mpls

restrict allow-service all

```

vpn 0
interface ye0/0
description..... Internet Circuit ****T1 ip address 209J6 5 200.22 5/30 tunnel-
interlace
encapsulation ipsec color public-internet restrict allow-service ail

```

```

interface ae0H description "MPLS
ip address 10.10.0.101/30 tunnel-interface
encapsulation ipsec color mpl$ restrict jllow-service all

```

C)

```

vpn 0
interface ge0/0 description..... Internet Circuit ipaddress 2 09.16
5.20 0.225/30 tunnel-in terface
encapsulation ipsec color public-internet al low-service a lf

```

```

vpn 1
interface ge0/1
description "" MPLS ""* ip address 10.100.1 ni/30 tunnel-interface
encapsulation ipsec color mnls

```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 192

What is the procedure to upgrade all Cisco SD-WAN devices to a recent version?

- A. The upgrade is performed for a group of WAN Edge devices first to ensure data-plabe availability when other controllers are updated.
- B. The upgrade is performed first on vManage, then on WAN Edge devices, then on vBond and finally ON vSmart The reboot must start from WAN Edge devices.
- C. Upgrade and reboot are performed first on vManage then on vBond then on vSmart. and finally on the Cisco WAN Edge devices.
- D. Upgrade and reboot are performed first on vBond. then on vSmart. and finally on the Cisco WAN Edge devices.

Answer: C

Explanation:

Question: 193

Refer to the exhibit.

The screenshot shows a configuration window with the following fields and controls:

- Address Family:** A dropdown menu with a globe icon, currently set to 'On' (radio button selected).
- Address Family:** A text input field containing 'ipv4-unicast' with a close button (X).
- Maximum Number of Prefixes:** A dropdown menu with a checkmark icon, currently set to 'On' (radio button selected).
- Route Policy In:** A dropdown menu with a checkmark icon, currently set to 'Off' (radio button selected).
- Route Policy Out:** A dropdown menu with a globe icon, currently set to 'On' (radio button selected).
- Policy Name:** A text input field containing 'eBGP_Community_Policy'.

The engineer must assign community tags to 3 of its 74 critical server networks as soon as that are advertised to BGP peers. These server networks must not be advertised outside AS. Which configuration fulfill this requirement?

- A)
- ```
policy
route-policy eBGP_Community_Policy
 wqutuct 1 match address Community^P refix action acctpt let
 Gommunity 99^6SW0 locabas
 default-action reject
Utts
prefin-1Kt Coinrnunity_Prefix
ip-prefix 2 0.20.20.0/24
ip-prefix 21 21.21.^24
ip-prefi(22.22.22.0/24
```
- B)
- ```
policy
fouie-pohcy oBGP_Cdmrnufi impolicy sequence 1 match
address COfnmur*iPty_P refill
```

```
action acctpt tel
cacrirnijnty 939 :S5M0 no-ex port
default-action accept
litis
prefixJM Community Prefix
^prefix Z0.K.20 NW
^prefix 21 21 21 9 24
ip-prefix 22 22,22,0'24
C)
policy
xouie-pollcy tBGP_C<ncommunity_Poficy
sequence 1
match
address Commumry^Prefix
action accept tel community 999:6 5030 focaku default-action reject
lists
prelix-lhf C<ifnrniunity_Prefix
bp-prefix 20.2C.20.0-24
ip-prefix 21.21.21.0/24
tp-prefix 22.22.22.0/24
```

```

policy
route-policy *BGP_ConriniGniTy_Polic
  wqueflCe 1
  march
  address CommunityJhvfli
  action, accept
  5*1
  community 99fl:E5W0 no-expon. default-action accept IEfts
  pretix-J^t Community Prefix
  ip-pr«fix 2d .20.20.0/24
  ip-prifix 21.21.21.0/24
  iP'prefix 22.22.22.0/24

```

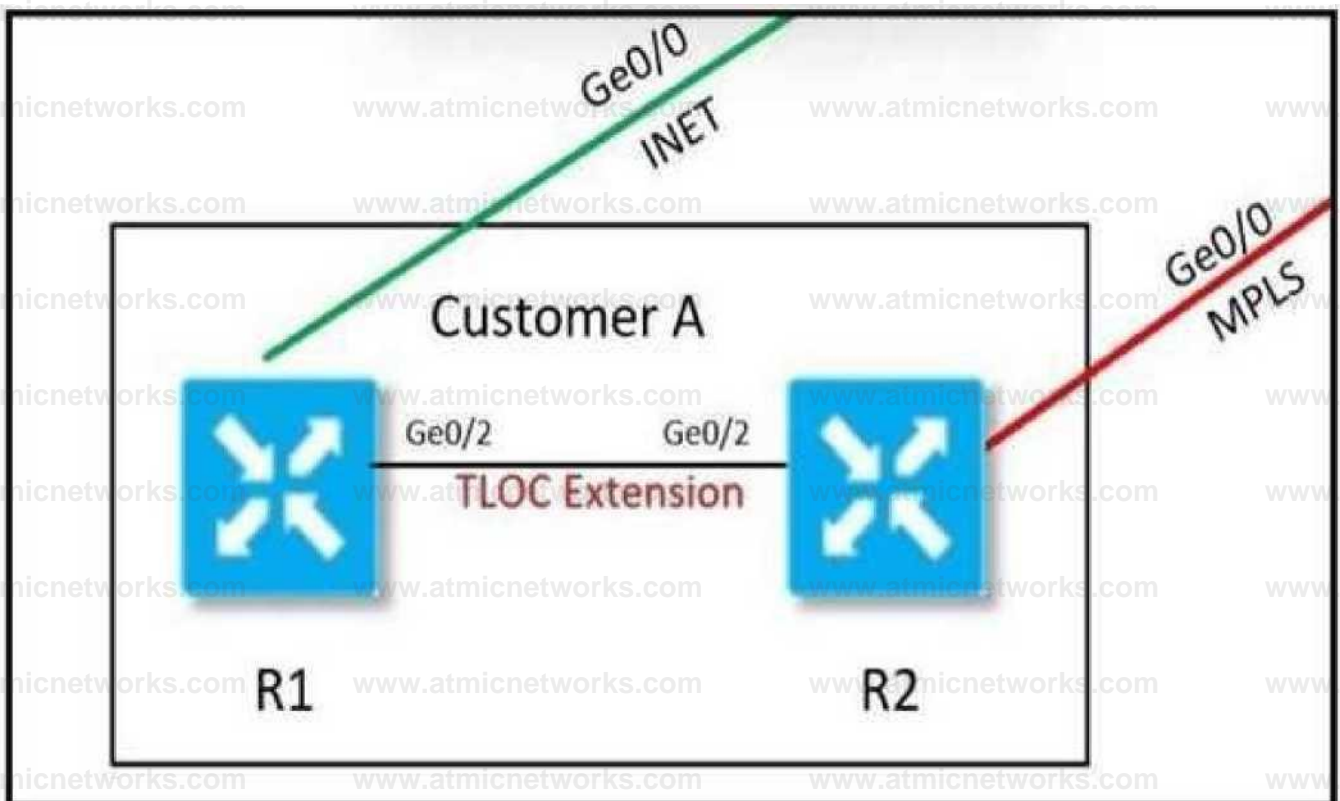
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation:

Question: 194

Refer to the exhibit.



An MPLS connection on R2 must extend to R1 Users behind R1 must have dual connectivity for data

traffic Which configuration provides R1 control connectivity over the MPLS connection?

A)

```
interface ge0/2
 ip address 34.34.34.1/30
 tunnel-Interface
 color mpls
```

m

```
interface ge0 2
 ip address 34.34.34.2/30
 doc-extension geG/D
 tunnel-Interface
 color public-1 memei
```

B)

```
interface ge0'2
 ip address 34.34.34 J00
 thc-extension gtfth
```

H2

```
interface geOIO
 ip address 34.34.34.2'30
 tunnel-Interface
 color mph
```

C)

```
vpn 0 router ospf
 redistribute omp route-polxy OSPF_Route_Poicy area 0
 Interface geQ'2 exit lists
 prefix-list W2 Loopback
 ip-prefix 10.10.10.5'32
 route-policy OSPF_Route_Policy
 sequence 1 match
 address W2_Loopback

action accept
 set
 metric 100
 metric-Type type!
```

D)

```
vpn 10
 name— Strvic* VPN 10 — router
 01 pf
 redistribute omp route-policy OSPF_Route_Policy
 area 0
 interface geO 2 exit
```


lists

```
prefix-list W2_Loopback
ip-prefix 10.10.10.5/32 i
route-policy OSPF_Route_Policy
sequence 1 match
address W2_Loopback
```

action acctot

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation:

Question: 195

What prohibits deleting a VNF image from the software repository?

- A. if the image is stored by vManage
- B. if the image is referenced by a service chain
- C. if the image is uploaded by a WAN Edge device
- D. if the image is included in a configured policy

Answer: D

Explanation:

Question: 196

Which two metrics must a cloud Edge router use to pick the optimal path for a SaaS application reachable via a gateway site? (Choose two.)

- A. HTTP loss and latency metrics to the SaaS application
- B. ICMP loss and latency metrics to the SaaS application
- C. BFD loss and latency metrics to the gateway site
- D. BFD loss and latency metrics to the SaaS application
- E. HTTP loss and latency metrics to the gateway site

Answer: A,C

Explanation:

-The gateway vEdge uses HTTP to obtain SaaS application performance information - The client vEdge will use BFD over the IPSec tunnel to the gateway site to obtain client>gateway path performance information

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Cloud-onRamp-for-SaaS-Deployment-Guide-2018JUL.pdf>

Question: 197

An enterprise needs DIA on some of its branches with a common location ID: A041:B70C: D78E::18 Which WAN Edge configuration meets the requirement?

A)

```
vpn 1
interface ge0/1
ip address 172.16.0.1/24
vpn 512
ip route 0.0.0.0/0 vpn 0
```

B)

```
vpn 1 ip route 0.0.0.0/0 vpn 1 Interface ge0/0
ip address 172.10.1.1/24
Mt
```

C)

```
vpn 0 interface ge0/0
ip address 172.16.0.1/24 net
vpn 1
ip route 0.0.0.0/0 vpn 0
```

D)

```
vpn 0 ip route 0.0.0.0/0 vpn 0 vpn 1 interface ge0/1 ip address 172.16.0.1/24 net
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 198

vManage

system

```
system^ 10.11.11.1
host-name vManage
site-id 1
dock hmezone Europe tendon
vbond 11 1 1 3
organization-name Cisco com
VDOO
Interface etni
Ip address 11.1.11/24
No shut
Tunnel-mterface
AJiow-servicc all
Ip route 00 0.0/0 11 1 1 254
```

vBand

system

```
system-ip 10.11.11 3
host-name vManane
site-id 1
dock timezone Europelondon
vbond 11111 local
organization-name Cisco com
VDOO
Interface geO'O
Ipaddress 11.1.13/28
No shut
Tunnel-interface
Encapsulation ipsec
Aiiow-service all
Ip route 0 0 0 0/0 11 1 1 254
```

v Smart

system

```
system-ip 1011111
host-name vSmart
Site-id 1
dock timezone Europe/Rome
vbond 11 1 1 3
organization-name Cisco com
VoriO
Interface ethl
Ip address 11.1.1 2/24
No shut
Tunnel-interface
Al low-service all
JP joute M 9^ 1 254
```

vManage and vSmart have an issue establishing a connection to vBond. Which configuration resolves the issue?

- A. Configure the tunnel interface on all three controllers with a color of transport.
- B. Change the timezone on the vSmart to Europe/London.
- C. Configure the (11.1.1.X/24) IP addresses on the elhO interfaces on vManage and vSmart.
- D. Reconfigure the system-ip parameter on vSmart to 11.1.1.2.

Answer: B

Explanation:

Question: 199

Which destination UDP port is used by WAN Edge router to make a DTLS connection with vBond Orchestrator?

- A. 12343
- B. 12345
- C. 12346
- D. 12347

Answer: C

Explanation:

Question: 200

Which policy is configured to ensure that a voice packet is always sent on the link with less than a 50 msec delay?

- A. localized data policy
- B. localized control policy
- C. centralized data policy
- D. centralized control policy

Answer: C

Explanation:

Question: 201

An organization requires the use of integrated preventative engines, exploit protection, and the most updated and advanced signature-based antivirus with sandboxing and threat intelligence to stop malicious attachments before they reach users and get executed. Which Cisco SD-WAN solution meets the requirements?

- A. Cisco Trust Anchor module
- B. URL filtering and Umbrella DNS security
- C. Cisco AMP and Threat Grid
- D. Snort IPS

Answer: D

Explanation:

Question: 202

What is the minimum Red Hat Enterprise Linux operating system requirement for a Cisco SD-WAN controller deployment via KVM?

- A. RHEL7.5
- B. RHEL 6.5
- C. RHEL4.4

D. RHEL 6.7

Answer: D

Explanation:

Question: 203

An engineer must automate certificate signing through Cisco. Which vManage configuration achieves this task?

A)

vpn 0

dn\$ 208.67.222.222 primary

allow-service dn\$

allow-service sshd allow-service netconf

B)

vpn 0

allow-service dns allow-service sshd allow-service netconf

C)

vpn 512

dn\$ 208.67.222.222 primary

allow-service dns allow-service sshd allow-service netconf

D)

vpn 512

allow-service dns

allow-service sshd

allow-service netconf

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Question: 204

Which issue triggers the Cisco Umbrella resolver to forward DNS requests to the intelligent proxy?
Which issue triggers the Cisco Umbrella resolver to forward DNS requests to the intelligent proxy?

- A. A domain is nonexistent.
- B. A domain is block-listed.
- C. A domain is locally reachable.
- D. A domain is grey-listed.

Answer: D

Explanation:

Question: 205

How many vCPUs and how much RAM are recommended to run the vSmart controller on the KVM server for 251 to 1000 devices in software version 20.4.x?

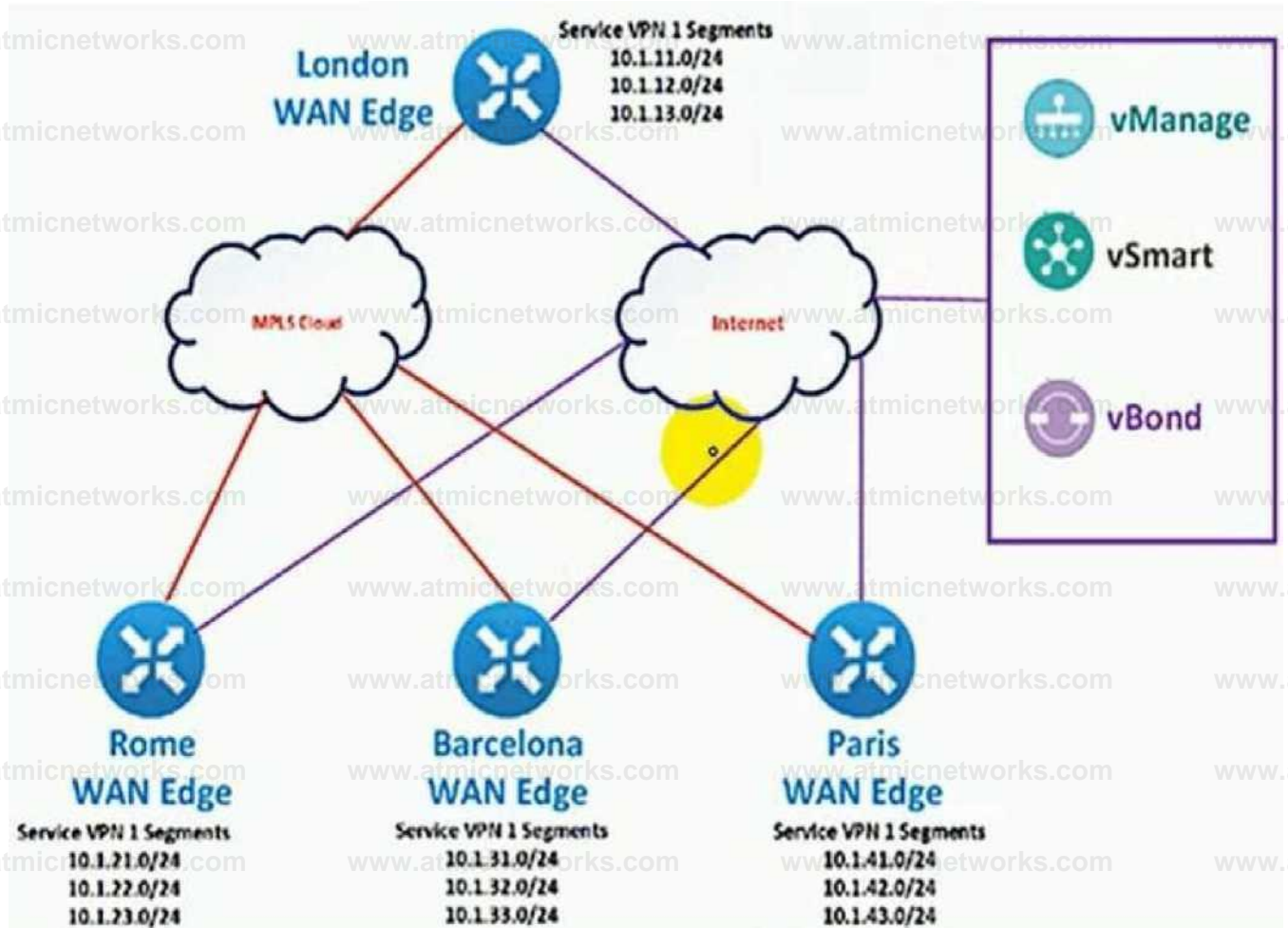
- A. 4vCPUs, 16 GB
- B. 4 vCPUs, 8 GB
- C. 8vCPUs, 16 GB
- D. 2vCPUs, 4GB

Answer: B

Explanation:

Question: 206

Refer to the exhibit.



The Cisco SD-WAN network is configured with a default full-mesh topology. An engineer wants Paris WAN Edge to use the Internet HOC as the preferred TLOC for MSN Messenger and AOL Messenger traffic.

Which policy achieves this goal?

A)



B)



C)



D)

Cw*iAi»4 p»*<y tacMrM^x



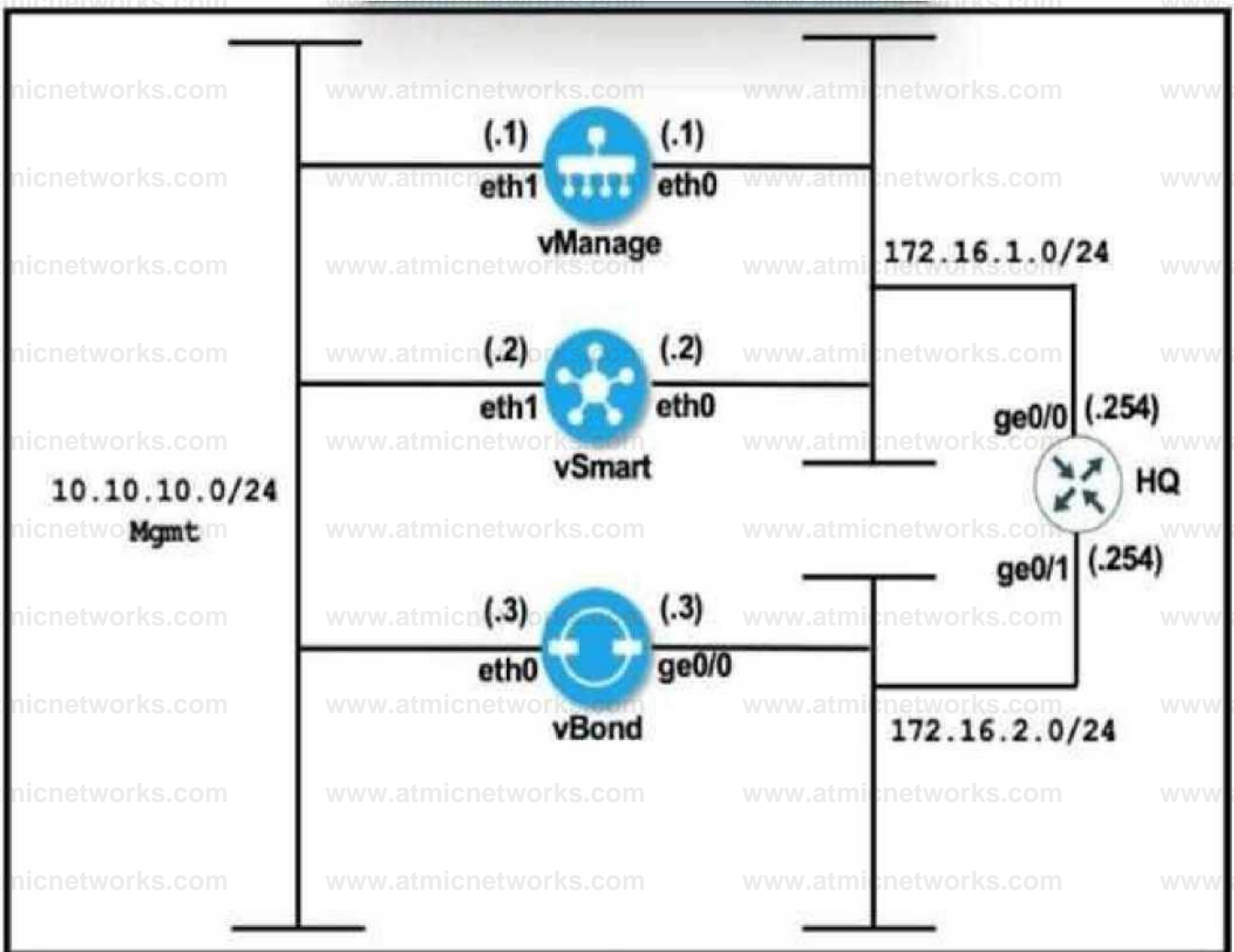
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 207

Refer to the exhibit.



vManage

Cisco.com

```

system
system-ip 10.10.10.101
host-name vManage
site-id 1
clock timezone Europe/London
vbond 172.16.2.1
organization-name Cisco.com

```

```

vpn 0 interface eth1
ip address 172.16.1.1/24 no shut
tunnel-interface
allow-service all
ip route 0.0.0.0/0 172.16.1.254
commit

```

vBond

```

system
system-ip 10.10.10.103 host-name
vBond site-id 1
clock timezone Europe/Rome vbond
172.16.2.1 local organization-name

```

```

vpn 0
interface ge0/0 ip address
172.16.2.1/24 no shut tunnel-
interface encapsulation ipsec
allow-service all
ip route 0.0.0.0/0 172.16.1.254 i
commit

```

vManage and vBond have an issue establishing a connection to each other. Which configuration resolves the issue?

- A. Configure the timezone on vBond to Europe/London.
- B. Configure the encapsulation ipsec command under the tunnel interface on vManage.
- C. Configure a default route on vBond pointing to 172.16.2.254.
- D. Remove the encapsulation ipsec command under the tunnel interface of vBond.

Answer: C

Explanation:

Question: 208

An engineer must deploy a QoS policy with these requirements:

- policy name: App-police
- police rate: 1000000
- burst: 1000000
- exceed: drop

Which configuration meets the requirements?

vpvfa WHIG sequence 1 match
A. aooini youtube acton acctpt wt
police? App-police

policy
data-policy policy-name vpfbUst ft
F sequence 1 action accept set
police? App-police

vpn 10 interface fleO Oi'O
C. set
police? App-polict In default action accept

policy
- action accept ' Mt
police? App-police

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 209

How is an event monitored and reported for an individual device in the overlay network at site ID:S4300T6E43F36?

- A. The device sends event notifications to vManage.
- B. The device sends notifications to vSmart that sends them to vManage.
- C. The device sends a critical alarm of events to vManage.
- D. The device sends a critical alarm to vSmart that sends it to vManage.

Answer: A

Explanation:

Question: 210

Refer to the exhibit.

```
policy
lists
!
tloc-list dc-preference-east
tloc 100.100.100.100 color mpls
encap ipsec preference 200
tloc 101.101.101.101 color mpls
encap ipsec preference 400
!
site-list sites-region-west
site-id 1-20
!
site-list sites-region-east
site-id 21-40
!
site-list dc-sites
site-id 100-101

control-policy adv-dc-preference-west
sequence 10
match route
site-list dc-sites
!
action accept
set
tloc-list dc-preference-east
!

!
default-action accept
!
control-policy adv-dc-preference-east
sequence 10
match route
site-list dc-sites
!
action accept
set
tloc-list dc-preference-east
!
!
default-action accept
!
!
apply-policy
site-list sites-region-west
control-policy adv-dc-preference-west
out
!
site-list sites-region-east
control-policy adv-dc-preference-east
out
!
!
```

A customer wants to implement primary and secondary Cisco SD-WAN overlay routing for prefixes that are advertised for both data centers. The east data center (TLOC 101.101.101.101) is primary for east sites, and the west data center (TLOC 100.100.100.100) is primary for west sites. Which configuration change achieves this objective?


```
tlloc-list dc-preference-east
```

```
tlloc 100.100.100.100 color mpis encap ipsec preference 400  
tlloc 101.101.101.101 color mpis encap ipsec preference 200
```

D.

```
control-policy adv-dc-preference-west  
sequence 10  
match route  
site-list dc-sites  
action accept  
set  
  soc-list dc-preference-west  
default-action accept
```

A. Option A B. Option B C. Option C D. Option D

Answer: A

Explanation:

Question: 211

DRAG DROP

Drag and drop the security terminologies from the left onto the PCI-compliant network features and devices on the right.

transport security

perimeter security

segmentation

attack prevention

IPS

zone-based firewall and VPNs

IPsec VPN

firewall

Answer:

Explanation:

attack prevention

segmentation

transport security

perimeter security

Question: 212

An engineer must apply the configuration for certificate installation to vBond Orchestrator and vSmart Controller. Which configuration accomplishes this task?

```
vpn 0 interface eth1 ip >d«HH mi.M^a A UfinMvIMtaa
```


alio^service uhd al low-service netconf M thtikfown

vpn Si J interface e*i \$ ip address 199 1 11/28 " tunnel-interface
allow-service »hd al low-service netconf

vpn 0 interface «ni ,- ip address lfii.T.L 1/20 ' tutwel-iHtorftn
ahoW'Service Hhd jl-aw-service nip

vpn M\$ Interfwe *tM ip AMfMI 199 1 1 1/28 D tunnel-interface
al low-service netconf no AIEpw-terVIH nio no al l ow-service stun

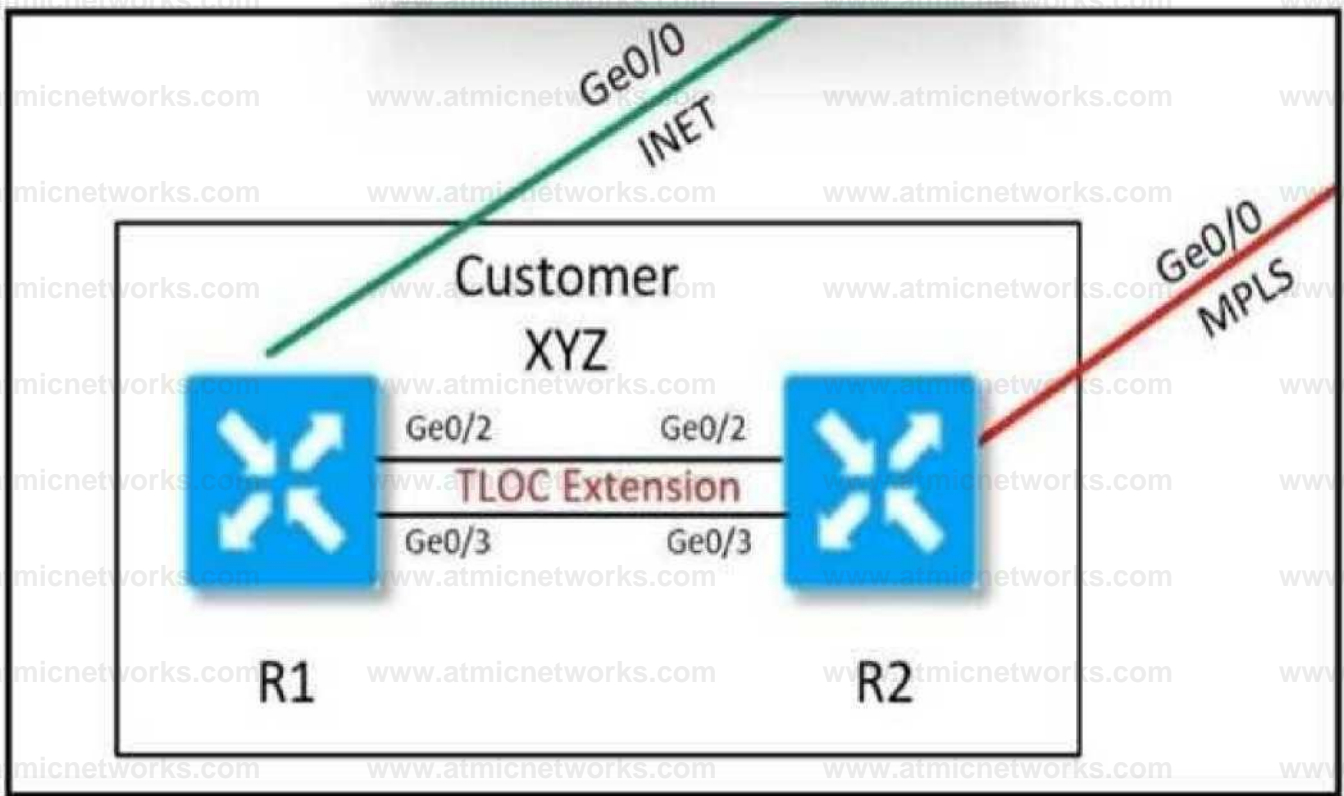
A. Option A B. Option B C. Option C D. Option D

Answer: A

Explanation:

Question: 213

Refer to the exhibit.



Customer XYZ cannot provision dual connectivity on both of its routers due to budget constraints but wants to use both R1 and R2 interlaces for users behind them for load balancing toward the hub site. Which configuration achieves this objective?

RI

fawta* QtOfS

ip addrtis 43 43 43 2,30

tiOMMftllM H+0 0

IntvfaM oeO'3

Ip iddrm 3 4.34 34 V30

tuRnaMntorfact

cdw mp4?

interface grt'2

Ip address « 43 43 1/30

tunr*HnIM^3w

color p4jhiic-1.fi temst

inttrfx* 0*0^3

ip addrtii 34.34 34.130

tiec-ultmioneaWO

RI

interface geO'I

Ip address 43.43.434/30 doc-ejcwmlw o#0'0

**Interface 0*0'3 ip address MM M UM
_ ti M-em n si on pt 0 ' 0**

**R2
Interface jaO 2
ip address 43.43.43.13* tunnel-Interface
tolgr public-internet**

interface ge0'3 ip address 34.MM 1/30

R1

Interface ge0/2

ip address 10.10.10.1 24

Interface p0/0

ip address 34.34.34.1 30

show ip interface ge0/0

R2

interface ge0/2

ip address 43.43.43.1 24

Interface s0/0/3

ip address 34.34.34.1 30

R1

Interface g0/2

ip address 43.43.43.100 24

interface ge0/0 ip address 34.34.34.1 30

D

R2

interface g0/2

ip address 4.3.4.3 24

ip address 4.3.4.3 24

interface s0/0/3 ip address 34.34.34.1 30

A. Option A B. Option B C. Option C D. Option D

Answer: A

Explanation:

Question: 214

Which protocol is configured on tunnels by default to detect loss, latency, jitter, and path failures in Cisco SD-WAN?

- A. TLS
- B. BFD
- C. OMP
- D. BGP

Answer: B

Explanation:

Question: 215

An administrator wants to create a policy to add a traffic policer called "politer-ccnp" to police data traffic on the WAN Edge. Which configuration accomplishes this task in vSmart?

A.

```
vpn 1
interface ge 0/4
policer policer-ccnp in
```

B.

```
policy
data-policy policy-ccnp
vpn-list list-ccnp
sequence number
action accept
set policer policer-ccnp
```

C.

```
policy
access-list list-ccnp
sequence number
action accept
policer policer-ccnp
```

D.

```
vpn 1
interface ge 0/4
policer policer-ccnp out
```

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 216

Which table is used by the vSmart controller to maintain service routes of the WAN Edge routers in the hub and local branches?

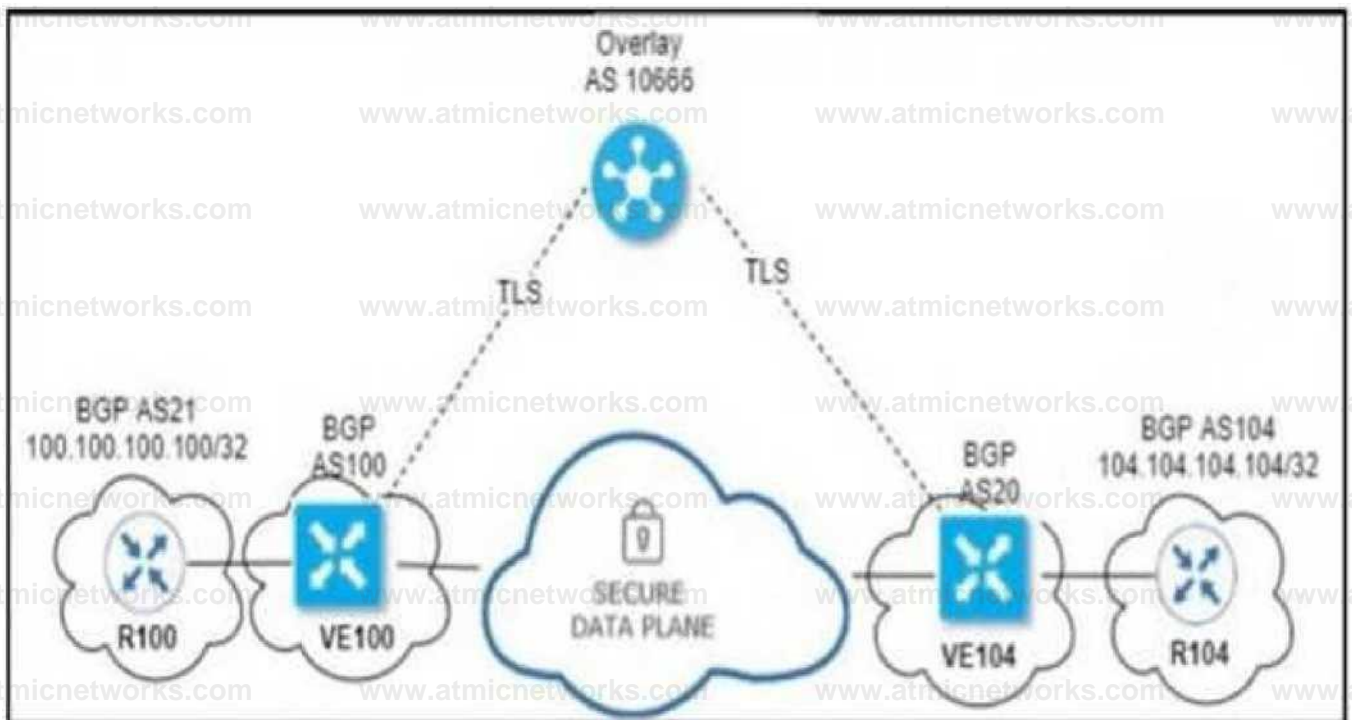
- A. RIB
- B. FIB
- C. OMP
- D. TLOC

Answer: C

Explanation:

Question: 217

Refer to the exhibit.



An engineer configured OMP with an overlay-as of 10666. What is the AS-PATH for prefix 104.104.104.104/32 on R100?

- A. 100 10666
- B. 100 20 104
- C. 100 10666 20 104
- D. 100 10666 104

Answer: A

Explanation:

Question: 218

Which policy tracks path characteristics such as loss, latency, and jitter in vManage?

- A. VPN
- B. control
- C. app-route
- D. data

Answer: C

Explanation:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/application-aware-routing.html>

Question: 219

Refer to the exhibit.

```
vEdge1# show control connections
```

PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP
vsmart	dtls	10.2.2.2	1	1	10.50.0.5	12446	10.50.0.5
vsmart	dtls	10.2.2.2	1	1	10.50.0.5	12446	10.50.0.5
vbond	dtls	0.0.0.0	0	0	10.50.0.9	12346	10.50.0.9
vbond	dtls	0.0.0.0	0	0	10.50.0.9	12346	10.50.0.9
vmanage	dtls	10.1.1.1	1	0	10.50.0.1	12446	10.50.0.1

An organization is testing a Cisco SD-WAN solution and decided to have the control plane established first and not the data plane at the time of migration. Which configuration achieves this goal?

CONFIGURATION | CERTIFICATES

WAN Edge List Controllers

Send to Controllers Click Send to Controllers to sync the WAN Edge list on all controllers

Search Options Total Rows: 20

Style	Device Model	Chassis Number	Hostname	IP Address	Serial No./Title	Validity		
	vEdge Cloud	1b0cfa0-a463-7d6c-e5...	vEdge1	10.10.10.1	BC42AE30	Expired	Expire	Valid
	vEdge Cloud	ec3baa6e-9d81-7e9d-f9...	vEdge2	10.10.10.2	E1F8764E	Expired	Expire	Valid
	vEdge Cloud	d7b14bb6-f718-b111-8...	vEdge3	10.10.10.3	F5DA8A8D	Expired	Expire	Valid
	vEdge Cloud	12b4f92b-daff-7a27-cl...	vEdge4	10.10.10.4	8D992D59	Expired	Expire	Valid
	vEdge Cloud	0183a420-e12e-41f7-af...	vEdge5	10.10.10.5	FA46CEE8	Expired	Expire	Valid

A.

CONFIGURATION | DEVICES

WAN Edge List Controllers

Change Mode Upload WAN Edge List Export Bootstrap Configuration Sync Smart Account

UI Inside Search Options Total Rows: 20

Style	Device Model	Chassis Number	Serial No./Title	Hostname	System IP	Site ID	Mode
	vEdge Cloud	1b0cfa0-a463-7d6c-e5...	BC42AE30	vEdge1	10.10.10.1	1	vManage
	vEdge Cloud	ec3baa6e-9d81-7e9d-f9...	E1F8764E	vEdge2	10.10.10.2	2	vManage
	vEdge Cloud	d7b14bb6-f718-b111-8...	F5DA8A8D	vEdge3	10.10.10.3	3	vManage
	vEdge Cloud	12b4f92b-daff-7a27-cl...	8D992D59	vEdge4	10.10.10.4	4	vManage
	vEdge Cloud	0183a420-e12e-41f7-af...	FA46CEE8	vEdge5	10.10.10.5	5	vManage

B.

CONFIGURATION | CERTIFICATES

WAN Edge List | Controllers

Send to Controllers

Click Send to Controllers to sync the WAN Edge list on all controllers

Search Options

CM*	1 <to*wtt*W*	jSMMiMAw	HMM*	I MIWMinAan		
2	it(* Oas#	t*0riM& *m & JOMk*&	Wopl	10 WM1	BC t.'A4 U	^#4
*	■CdQv Cu4	txM4rt>*ttit M4F*	(Up*	13 10 14 X	tnob#	■ - 1
	>(4*i 0*4	cw«t»<n*kin*	rfopj	1010103	»WJUJW3	r
2	•C4gaO«tf	HMfli»<W1 ta><3	J«V*	1010104	■QMNM	
	Kl* ODu4	01(3*41* «Or4V>'M	i* 4p*	1510 1311	IM MUI	

CONFIGURATION | CERTIFICATES

WAN 14v1M-1 | Controllers

Send to Controllers

Click Send to Controllers to sync the WAN Edge list on all controllers

Search Options

Total Rows: 20

State	GMM MM*4	1 OMM>MM»	< * «MM»	I PmMHm	M*IMnMM 144—
	44p0kMd	«MdkM«tUNK«t	U4p1	MIC 1*1	K4Mt*Q
	■MptM	u*dM*» «tot JrMH	U<ipT	ic wia;	III0HM
	44*00*4	«*14Mk4n**)H4	»t«pl	MNW»	ItfMMO
	U 1**C 1 -1	UMFW* *JM Tntd	H4p4	Will 134	Kvimo
		#1 M»4>*»)» 410#	vttart	MM1M	■MMIt*

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 220

Which two sets of identifiers does OMP carry when it advertises TLOC routes between WAN Edge

routers? (Choose two.)

- A. TLOC public and private address, carrier, and preference
- B. source and destination IP address, MAC, and site ID
- C. system IP address, link color, and encapsulation
- D. VPN ID, local site network, and BGP next-hop IP address
- E. TLOC public and private address, tunnel ID, and performance

Answer: A,C

Explanation:

Question: 221

How many subnets are necessary in Azure VNet for a WAN Edge device to function in the cloud deployment?

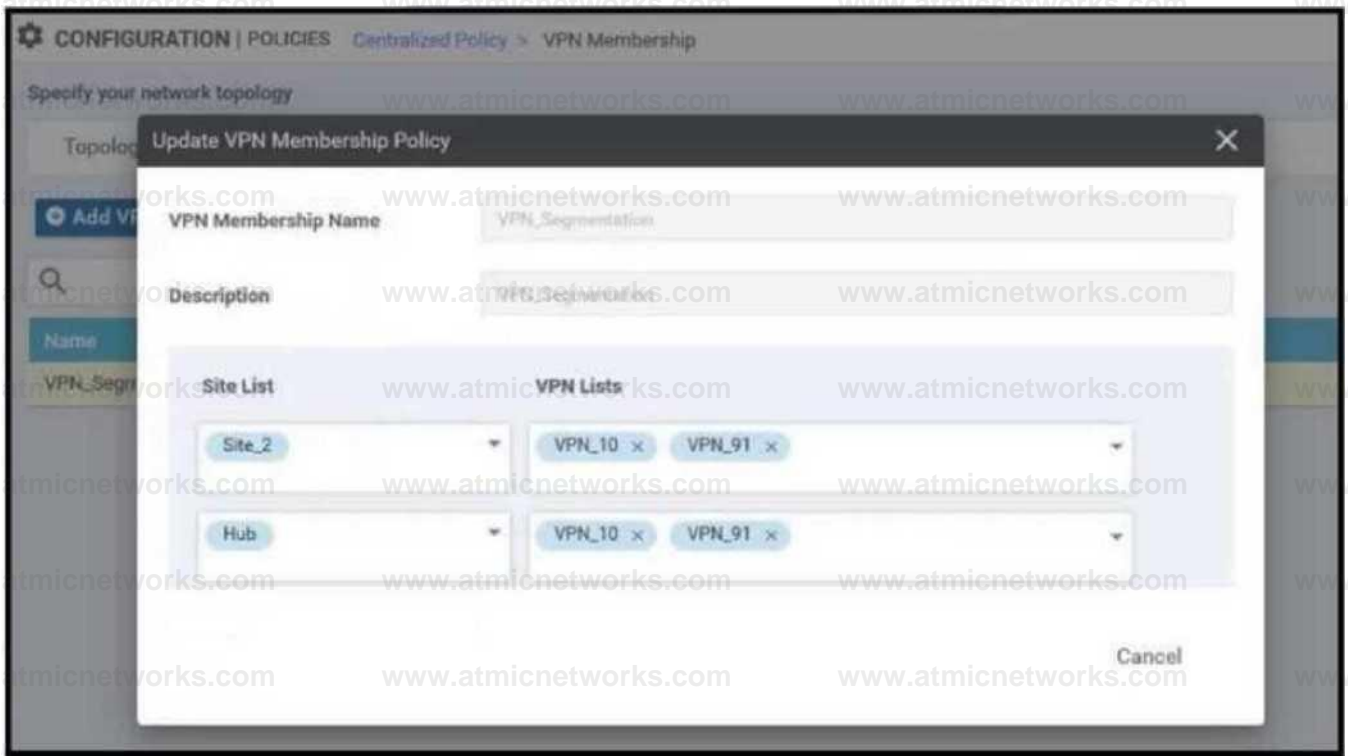
- A. CSR is the WAN Edge device that is supported in the Microsoft cloud. The Microsoft underlay cloud fabric performs the management function.
- B. There must be three subnets in VNet: management, public, and services.
- C. One public subnet is required in VNet. The Microsoft underlay cloud fabric performs all of the routing functions for WAN Edge.
- D. Public and services subnets are required in VNet. The Microsoft underlay cloud fabric performs the management function.

Answer: D

Explanation:

Question: 222

Refer to the exhibit.



An enterprise has hub and spoke topology where it has several VPNs. An engineer must allow users in VPN91 to reach users in VPN92 and VPN10 to reach VPN91 and VPN92. Which configuration meets these requirements?

Route

Sequence Rule Drag and drop to rearrange rules

Match Conditions	Actions
VPN List: VPN_01 VPN ID: [dropdown]	Accept Export To: VPN_02
Match Condition VPN List: VPN_02 VPN ID: [dropdown]	Accept Export To: VPN_01
Match Condition VPN List: VPN_01_and_VPN_02 VPN ID: [dropdown]	Accept Export To: VPN_00

Route

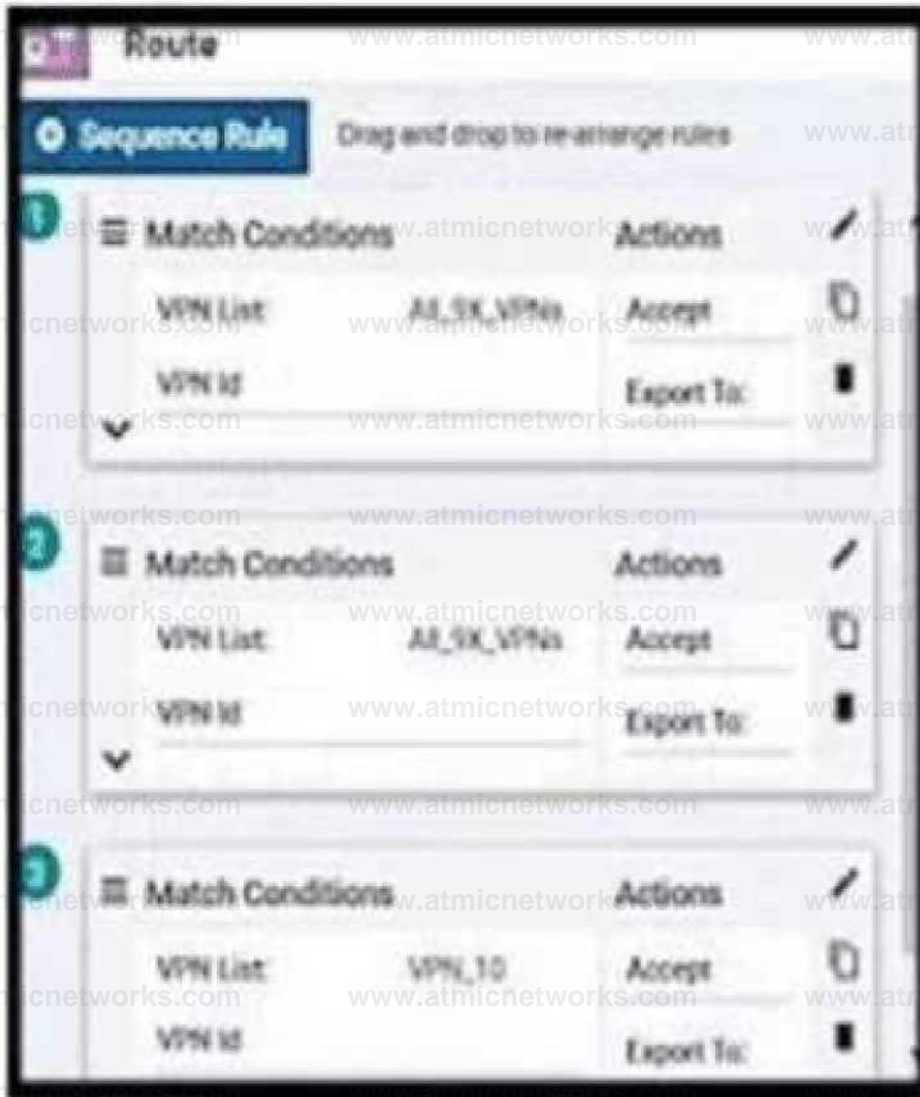
Sequence Rule Drag and drop to re-arrange rules

Match Conditions	Actions
VPN List: VPN_10 VPN ID: <input type="text"/>	Accept Export To: VPN_91 and VPN_92
VPN List: All_IX_VPNs VPN ID: <input type="text"/>	Accept Export To: All_IX_VPNs
VPN List: VPN_91 and VPN_92 VPN ID: <input type="text"/>	Accept Export To: VPN_10

C.

The screenshot displays a configuration interface for a Route, titled "Route". At the top, there is a "Sequence Rule" section with a sub-header "Drag and drop to re-arrange rules". Below this, three sequence rules are listed, each with a "Match Conditions" section and an "Actions" section. The rules are numbered 1, 2, and 3 on the left side.

Match Conditions	Actions
VPN List: VPN_10 VPN ID	Accept Export To: VPN_91_and_VPN_92
VPN List: VPN_91_and_VPN_92 VPN ID	Accept Export To: VPN_91_and_VPN_92
VPN List: VPN_91_and_VPN_92 VPN ID	Accept Export To: VPN_10



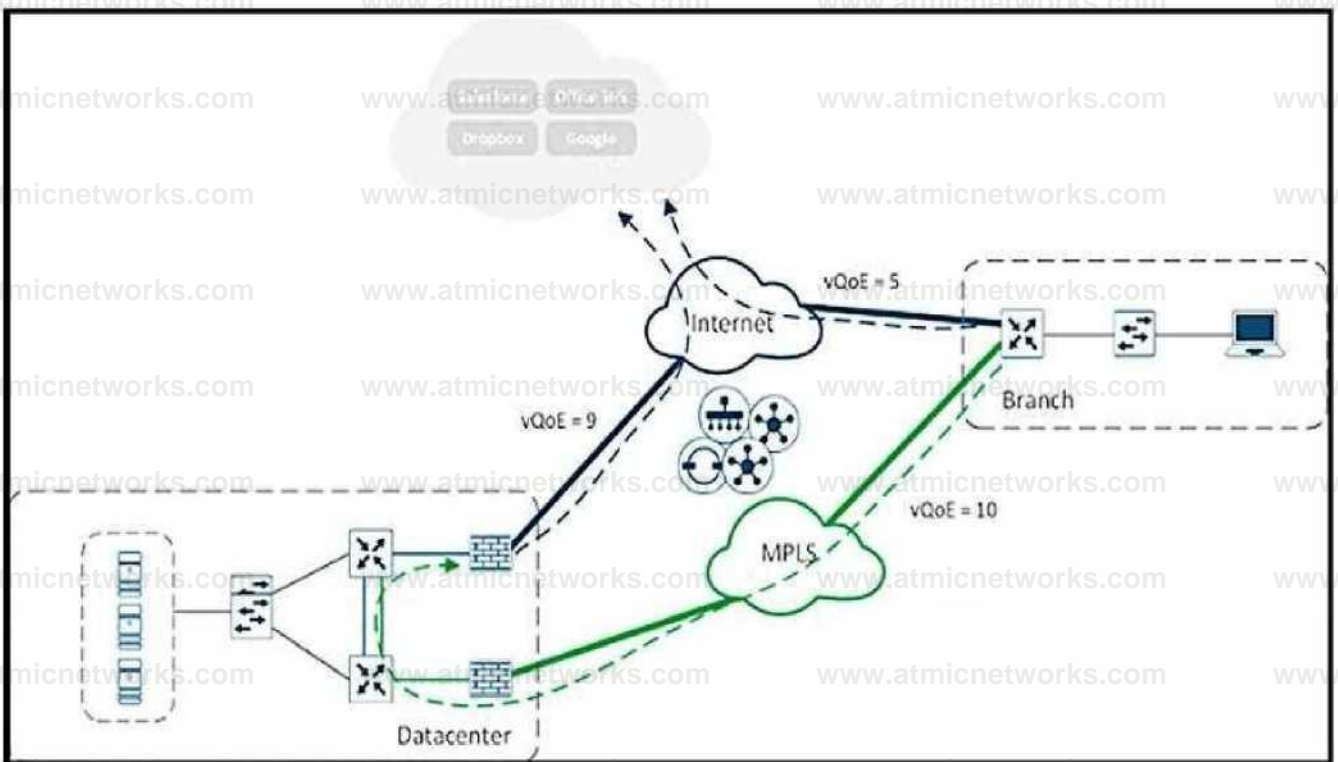
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 223

Refer to the exhibit.



Refer to the exhibit. A user in the branch is connecting to Office 365 for the first time. Over which path does the branch WAN Edge router traffic follow?

- A. routing table of the branch WAN Edge router
- B. DIA exit of the branch WAN Edge router
- C. forwarded to the gateway site
- D. dropped because the minimum vQoE score has not been met

Answer: B

Explanation:

Question: 224

Which type of lists are used to group related items via an application-aware routing policy under the policy lists command hierarchy on vSmart controllers?

- A. data prefix, site, and VPN
- B. OSCP value, application, and VPN
- C. data prefix, application, and SLA class
- D. DSCP value, site, and VPN

Answer: C

Explanation:

Question: 225

An engineer builds a three-node vManage cluster and then realizes that multiple nodes are unnecessary for the size of the company. How should the engineer revert the setup to a single vManage?

- A. Remove two nodes from the three-node vManage cluster
- B. Use the cluster conversion utility to convert to standalone vManage
- C. Restore vManage from the backup VM snapshot
- D. Leave the cluster as is and point to one vManage

Answer: B

Explanation:

Question: 226

Which routes are similar to the IP route advertisements when the routing information of WAN Edge routers is learned from the local site and local routing protocols?

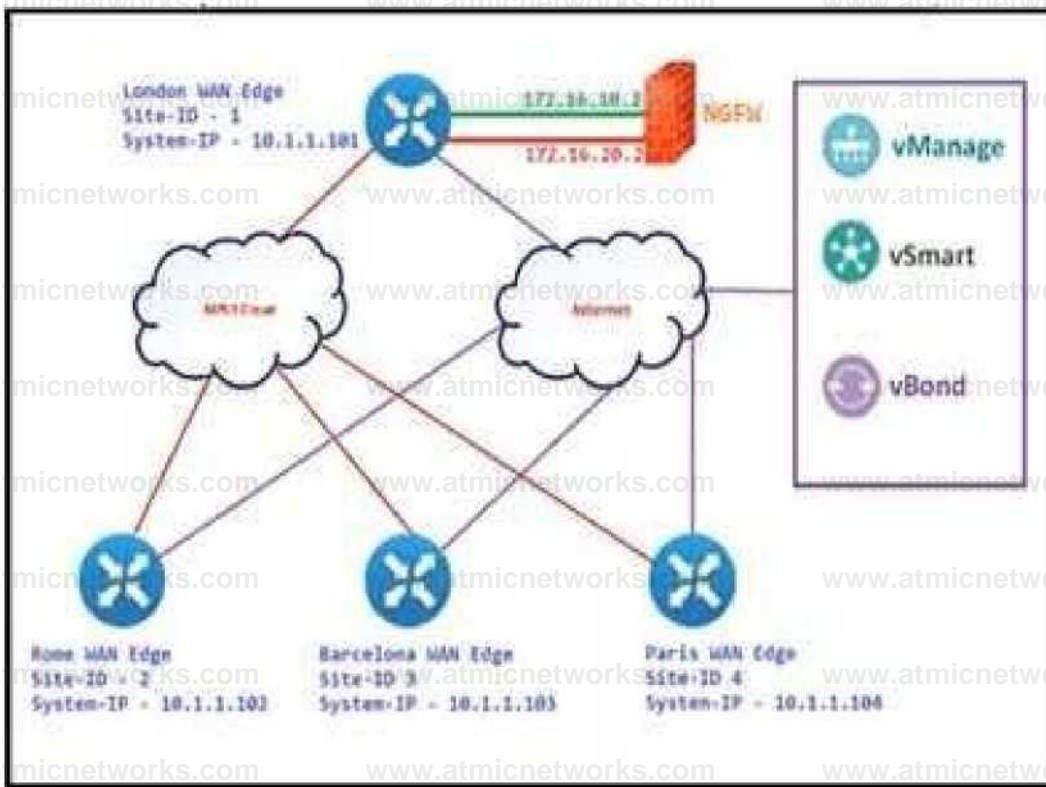
- A. service
- B. BGP
- C. TLOC
- D. OMP

Answer: D

Explanation:

Question: 227

Refer to the exhibit.



Refer to the exhibit. The Cisco SD-VYAN is deployed using the default topology. The engineer v/ants to configure a service insertion policy such that all data traffic between Rome to Paris is forwarded through the NGFW located in London. Which configuration fulfills this requirement, assuming that the Service VPN ID is 1?

A)

Lesion WAN L^c

vpn 1

service natsvol address 172 16 10.2

service n*tsvc2 address 172 16.20.2

pciky Oft*

site-list ROME

J it* 3 2

sits-list PARIS

sftHdi

cotitro"policy NGFW-SI

SWpjMWS 1 mitath rouh

site-id ROME

action accept

sit service netsvcl vpn 1

ieqii?ice 2

match routs

sitt-d PARIS

action accept MI unde* n«svc2 vpn 1 dsfautbaefflon acctpt

appi^poKcy i> legist ROME control-policy NGFW-S- out

stt»4st PARIS

control-policy NGFW-Si out

B)

LOfMOT '-Wi -
vpn 1

service neisvd adores 172 15.10 2
HT^W nmvcj tMtw* 172 15.20 2

uni

m-hit ROWE site-id 2 uta-liit PARIS nfe-d4 cchntcrf-pnlicy NATO'S!

WqUMU 1 match rauh site id ROME action act KT

uqLMnoi 2 match roule tito-M PARIS action ace apt default-action accept

aspl^pdrCy

liMlit ROME CMfrol-poflicy MSFW-SI «rt

C)

gO^t^ WAN E^e

ser/ice rW address 10.1.1.1 ' G1

PA-^{**1_}^

ittvlct fWid3r*5i i01 1 tOi

vSniaff

lists

>iW4*t ROME

ute-d 2

4,1«-liit PARIS

ti^di

control-policy NGFW-SJ

Mqutmt 1 match route

Hit-id ROWE

action Script

set service netsvcl vpn 1

tequenct2

match ro™ trtr

id PARIS

action accept

Mt iirvlc* nmyc2vpn 1 default-action accept

apply-pdicv

site-list ROME

ciwitrpl-policy NGFW-5I out

SitV^iSt PARI?

wntrol-pollcy NOFW-3I out

D)

HL L. -NLJ.
tablet FWaddreu 10X1.101
RAWS Wi Edo?
wvict FW ad&Mi 101 1 101
v^m^f ■ ■ ■ ■?
policy
lff&
tiffin «CW
sHaUd 2
iita-hst PARIS slt*4d4
wtrot-policf N0W5J
sequence 1 match rout* ill*-id ROME
ebon accept
MqtWKt 3 mJteh PMM site-id PARIS action
ucq>< default-action accept
appty-poUey
intuit! ROME cowol-pollcy NGFW*SI out

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 228

Which action is performed during the onboarding process when a WAN Edge router is connected to ZTP server ztp.viptela.com?

- A. The router is connected to WAN Edge Cloud Center
- B. The router is synced with vSmart Controller via an IPsec tunnel
- C. The router receives its vBond Orchestrator information
- D. The router is connected to vSmart Controller via a DTLSTLS tunnel

Answer: C

Explanation:

Question: 229

What are two attributes of vRoute? (Choose two)

- A. originator
- B. service
- C. encapsulation
- D. carrier
- E. domain ID

Answer: A,B

Explanation:

Question: 230

An engineer is configuring the branch office with a 172.16.0.0/16 subnet to use DIA for Internet traffic. All other traffic must flow to the central site or branches using the MPLS circuit Which configuration meets the requirement?

A)

```
data-policy SOW DIA
vpnJiji VPN 172
sequence 1
match
wurc#4p 172.16,0.01'16
destination-ip 172.16.0.0/16
```

```
sequence 2
```

```
match
```

```
5aurcfr^ataH5r«fix4^t DIA
```

```
action accept
```

```
nat uw-vpn 0
```

```
default-action accept
```

B)

```
daw-pclrcy SOW DiA vpn-JistVPN172 sequence 1 match
```

```
source-ip 172.16.0.0/16
```

```
action accept T
```

```
sequence 2 match
```

```
so uret-tfata-prefix-list DIA action accept nat use-vpn 0
```


default-action accept

C)

data-policy SOW DIA vpn-list VPN172 sequence 1
match

source-ip 172.16.0.0/16 destination-ip 172,16.0.0/16 action accept

sequence 2 match

source-data-prefix^1st DIA action accept nat use-vpo 0

i

default action accept

D)

data policy SOW DIA vpn-lists[VPN172 sequence 1
match

source-ip 172.16.0.0/16

destination-ip 172.16.0.0/16

Sequence 2 match

source-data-prefix^1st DIA action accept

default action accept

A. Option A

B. Option B

C. Option C

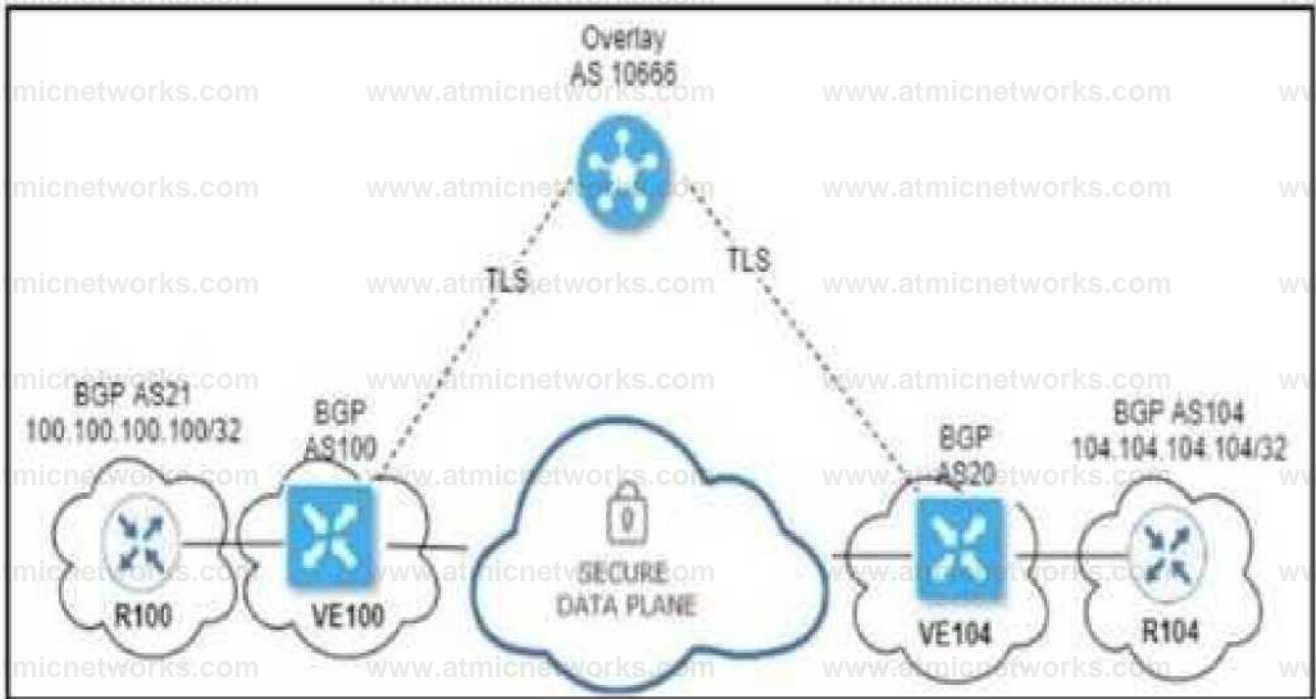
D. Option D

Answer: C

Explanation:

Question: 231

Refer to the exhibit.



Refer to the exhibit. An engineer configured OMP with an overlay-as of 10666. What is the AS-PATH for prefix 104.104.104.104/32 on R1007?

- A. 100 10666 104
- B. 100 10666
- C. 100 10666 20 104
- D. 100 20 104

Answer: A

Explanation:

Question: 232

Which Cisco SD-WAN component facilitates the initial communication between WAN Edge devices to join the fabric?

- A. vSmart Controller
- B. WAN Edge Router
- C. vManage
- D. vBond Orchestrator

Answer: D

Explanation:

Question: 233

An engineer must configure two branch WAN Edge devices where an Internet connection is available and the controllers are in the headquarters. The requirement is to have IPsec VPN tunnels established between the same colors. Which configuration meets the requirement on both WAN Edge devices?

WAN Edge 1

vpn0

interface ye 0/0

ip address 10.Q.0.1/24

ipv6 dhcp-client tunnel-interface color biz-internet restrict

encapsulation ipsec

WAN Edge 2

vpn 0

interface gfrWO

ip address 10.0 0.2/24

ipv6 dhcp -client tunnel-interface color default encapsulation ipsec

WAN Edge 1

Vpn 0

interface geO/0

ip address W.C,0.1/24

Ipv6 dhcp<hent tunnel-interface color default encapsulation ipsec

WAN Edge 2

vpn 0

interface geO/O

ip address 10,0-0.2/24

ipvg dhcp-ctfent

tunnel-interface

color default encapsulation ipsec

WAN Edge 1

vpn o

interface geO?O ip address 10.0,0,1/24 lp^ dticp-client tunnel -interface
color public-internet restrict encapsulation ipsec

WAN Edge 2

vpn 0

interface geOfO

ip address 10.0.0.2/24

ipvO dhcp-client tunnel-interface color gold restrict encapsulation ipsec

WAN Edge 1

vpn 0

interface ge(V0

ip addies 10.0.0.1/24

ipv6 ri hep-client tunnel-interlace color gold restrict encapsulation

ipsec

WAN Edge 2

vpn 0

Interface geO/O

ip address 1MA2/24 ipvG dhcp-clienl tunnel-interface color gold

restrict encapsulation ipsec

A. Option A B. Option B C. Option C

D. Option D

Answer: D

Explanation:

Question: 234

Which IP address must be reachable by a WAN Edge device for the ZIP process to work?

A. 10.1.1.1

B. 4.4.4.4

C. 172.16.1.1

D. 8.8.8.8

Answer: D

Explanation:

Question: 235

Which SD-WAN component detects path performance information in the organization to report the issue to the service provider at site ID:S4288T5E44F04?

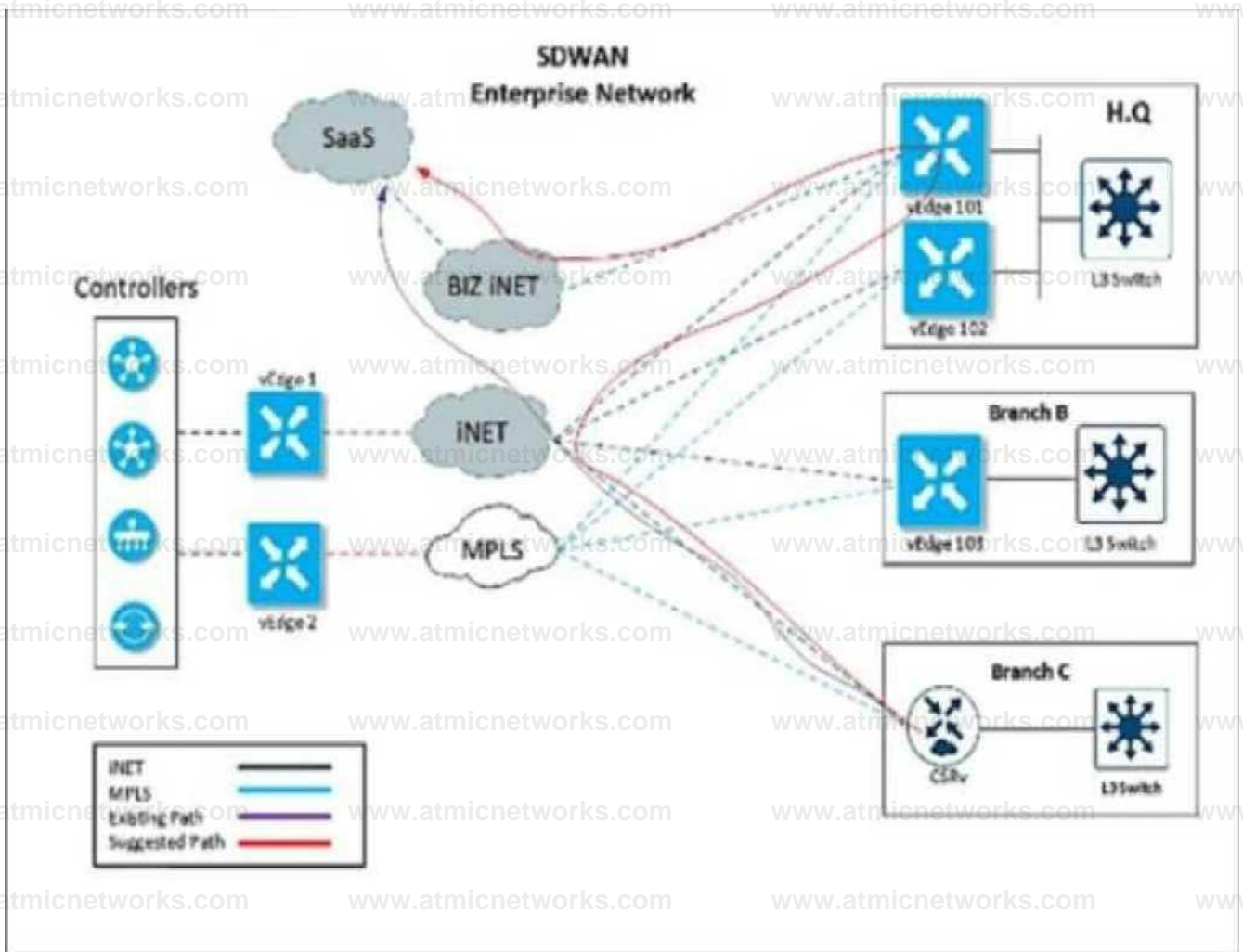
- A. vAnalytics
- B. vManage NMS
- C. vBond Orchestrator
- D. Cisco DNA

Answer: B

Explanation:

Question: 236

Refer to the exhibit.



Refer to the exhibit. An enterprise decides to use the Cisco SD-WAN Cloud onRamp for SaaS feature and utilize H.Q site Biz INET to reach SaaS Cloud for branch C. currently reaching SaaS Cloud directly. Which role must be assigned to devices at both sites in vManage Cloud Express for this solution to work?

- A. H.Q to be added as Gateway and Branch as DIA.
- B. Branch to be added as Client Sites and H.Q as DIA.
- C. Branch to be added as DIA and H.Q as Client Site.
- D. H.Q to be added as Gateway and Branch as Client Site.

Answer: B

Explanation:

Question: 237

Which protocol is used to measure jitter, loss, and latency on SD-WAN overlay tunnels?

- A. QoE
- B. OMP

- C. BGP
- D. BFD

Answer: D

Explanation:

Question: 238

Which protocol is used between redundant vSmart controllers to establish a permanent communication channel?

- A. IPsec
- B. HTTPs
- C. DTLS
- D. SSL

Answer: C

Explanation:

Question: 239

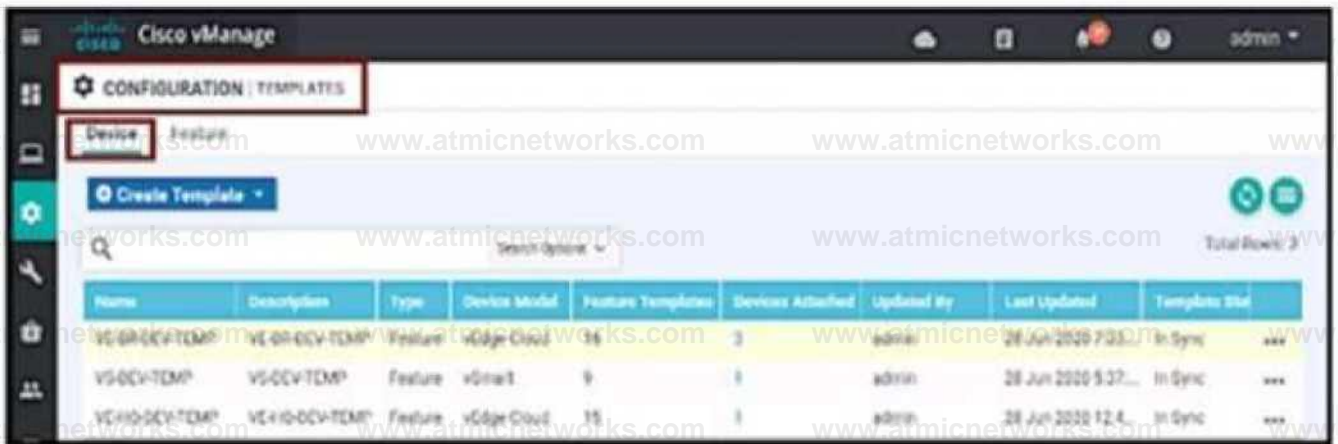
Which configuration defines the groups of interest before creation of the access list or route map? A)



B)



C)



D.



- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 240

Which controller is used for provisioning and configuration in a Cisco SD-WAN solution?

- A. vBond
- B. Manage
- C. WAN Edge router
- D. vSmart

Answer: B

Explanation:

Question: 241

Which policy configuration must be used to classify traffic as it enters the branch WAN Edge router to be put into the desired output queue?

A)

```
Policy
class-map
class pl queue 2
```

B)

```
qovmap QMap
qos-scheduler p1
```

C)

```
Policy
qos-schedulei QOS
class pl
bandwidth-percent 20
buffer-percent 20
drops red-dr op
```

D)

```
Policy access-list QoS sequence 1 match destination-ip 10,0.0.0/8
```

1

action accept class pt

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation:

Question: 242

Which routing protocol has the highest default administrative distance?

- A. OMP
- B. external EIGRP
- C. IS-IS
- D. IBGP

Answer: A

Explanation:

Question: 243

An engineer creates this data policy for DIA for VPN 10:

```
data-policy DIA
vpn hit VPN 10
sequence 10
match
```

```
d«1in^WKM4-prafiK4ifi INTERNAL NETWORKS
```

action accept

Which policy sequence enables DIA for external networks?

sequence 5 milch

Source-ip 0.0.0.0-0

**action accept
nat use-vpn 0**

**sequence 5
match
destination-ip 0 0 0 0/0**

action reject

default-action accept

**sequence 20 match
destination-ip 0 0 0 0/0**

**action accept
nat use-vpn 0**

**sequence 20
match
source-ip 0 0 0 0*0**

action reject

default-action accept

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 244

Which VPN must be present on at least one interface to install Cisco vManage and integrate it with WAN Edge devices in an overlay network site ID:S4307T7E78F29?

- A. VPN 512

- B. any VPN number selected
- C. services VPN range 0-511 D. VPNO

Answer: D

Explanation:

Question: 245

An enterprise is continuously adding new sites to its Cisco SD-WAN network. It must configure any cached routes flushed when OMP peers have lost adjacency Which configuration allows the cached OMP routes to be flushed after every 24 hours from its routing table?

Basic Configuration Timers Advertise

Graceful Restart for OMP On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown Yes No

Basic Configuration Timers Advertise

Graceful Restart for OMP On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown Yes No

Basic Configuration Timers Advertise

Graceful Restart for OMP On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown Yes No

Basic Configuration Timers Advertise

Graceful Restart for OMP On Off

Overlay AS Number

Graceful Restart Timer (seconds)

Number of Paths Advertised per Prefix

ECMP Limit

Shutdown Yes No

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

Question: 246

An engineer must configure the SD-WAN Edge router to identify DSCP 26 traffic coming from the router's local site and then change the DSCP value to DSCP 18 before sending it over to the SD-WAN fabric. What are the two ways to create the required configuration? (Choose two).





A. Option A B. Option B C. Option C D. Option D E. Option E

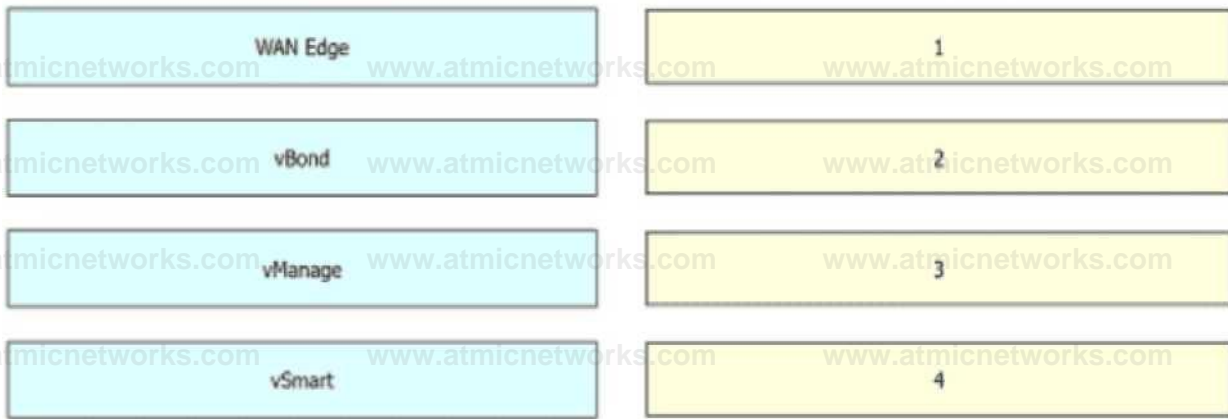
Answer: A,B

Explanation:

Question: 247

DRAG DROP

Drag and drop the devices from the left into order on the right to upgrade the software from version 19 to version 20.



Answer:

Explanation:



Question: 248

Which device information is required on PNP/ZTP to support the zero-touch onboarding process?

- A. interface IP address
- B. system IP address
- C. public DNS entry
- D. serial and chassis numbers

Answer: D

Explanation:

Question: 249

How must the application-aware enterprise firewall policies be applied within the same WAN Edge router?

- A. within and between zones
- B. between two VPN tunnels
- C. within zone pair
- D. between two VRFs

Answer: C

Explanation:

Question: 250

Which protocol is used to propagate multicast join requests over the Cisco SD-WAN fabric?

- A. ARP
- B. Auto-RP
- C. OMP
- D. IGMP

Answer: D

Explanation:

Question: 251

Which two REST API functions are performed for Cisco devices in an overlay network? (Choose two)

- A. distributing a Snort image among devices
- B. attaching a device configuration template
- C. managing connections for smart licensing
- D. monitoring device certificates
- E. querying a device and aggregating statistics

Answer: B,D

Explanation:

Question: 252

Which OMP route is selected for equal OMP route preference values on WAN Edge routers?

- A. route with higher TLOC preference value
- B. route with origin type of connected
- C. route with origin type of static
- D. route with lower TLOC preference value

Answer: A

Explanation:

Question: 253

Refer to the exhibit.



Refer to the exhibit A user has selected the options while configuring a VPN Interface Ethernet feature template What is the required configuration parameter the user must set in this template for this feature to function?

- A. The "IP MTU" field must be increased from the default value of 1500 to support the additional overhead.
- B. The "Shaping Rate (Kbps)" field must be configured with a value
- C. The "Adaptive QoS" field must be set to "on"
- D. The "Bandwidth Downstream" field must be configured with a value

Answer: B

Explanation:

Question: 254

REST applications communicate over HTTP or HTTPS to make calls between network devices. Which two HTTPS standard methods are included? (Choose two.)

- A. Array

- B. DELETE
- C. POST
- D. Scalar
- E. Object

Answer: B,C

Explanation:

Question: 255

Which set of platforms must be in separate VMS as of release 16.1?

- A. vSmart and WAN Edge
- B. WAN Edge and vBond
- C. vManage and vSmart
- D. vBond and vSmart

Answer: D

Explanation:

Question: 256

Which platform cannot provide IPS and URL filtering capabilities?

- A. Cisco CSR 1000V
- B. Cisco ISR 1000
- C. Cisco Catalyst 8300
- D. Cisco ISR 4000

Answer: B

Explanation:

Question: 257

An enterprise has these three WAN connections:

public Internet

business internet

MPLS

An engineer must configure two available links to route traffic via both links. Which configuration achieves this objective?

omp no shutdown route-limit 2

omp no shutdown send-path-limit 2

omp no shutdown Overlaps 2

omp no shutdown ecmp-bmit 2

A. Option B. Option C. Option D. Option

Answer: B

Explanation:

Question: 258

Which component is used for stateful inspection of TCP, UDP, and ICMP flows in Cisco SD-WAN firewall policies?

A. zones

B. sites

C. subnets

D. interfaces

Answer: A

Explanation:

Question: 259

Refer to the exhibit.

ni« rm	MIR PROIOCOI	Uli WIN IP	Mii ID	WAIN ID	Piii PRIVAIIP	PitVAVI PORI	HU MUC	IP P0H	MI* PUMK	UK* UKO*	SI AH	IRMO*	I RAM	IOC AI «UNI
	dtK	I# 144	1	.	1444	IW	14.1.1	1744/	go 14		Up	HMD	MM RI	4S
VMjrJ«C	dtB	IKI.I.7		1	? .» .»	1347	J. I. J.	1M0	gold		W>	HMD	MM RI	/»
vwr>fp	dtI*	io i.i ;	1	1	>444	DM/	>444	1714/	Itoi*		up	UVD	NOIM	00

Refer to the exhibit. An engineer is troubleshooting a control connection issue on a WAN Edge device that shows socket errors. The packet capture shows some ICMP packets dropped between the two devices. Which action resolves the issue?

- A. Recover the vManage controller that is down in a high availability cluster
- B. Change the system IP or restart the VWN Edge 4 the system IP is changed
- C. Remove IP duplication in the network and configure a unique IP address
- D. Recover vBond or wait for the controller to reload which could be caused by a reset

Answer: C

Explanation:

Question: 260

Which platform is a Cisco SD-WAN virtual platform?

- A. Cisco ISR 4000
- B. Cisco Nexus 1000V
- C. Cisco CSR 1000V
- D. Cisco ASR 1000

Answer: C

Explanation:

Question: 261

An organization wants to discover monitor and track the applications running on the WAN Edge device on the LAN. Which configuration achieves this goal?

1 CrW0VMjfWrt

n OtkltHfd

Q Maxtor

0 CatfxMorian

□ vAAii^ta

■ «JM^

3 DuJitoerd

MOTW

0 COHFIGURATION *Oicllt rr

MP^j

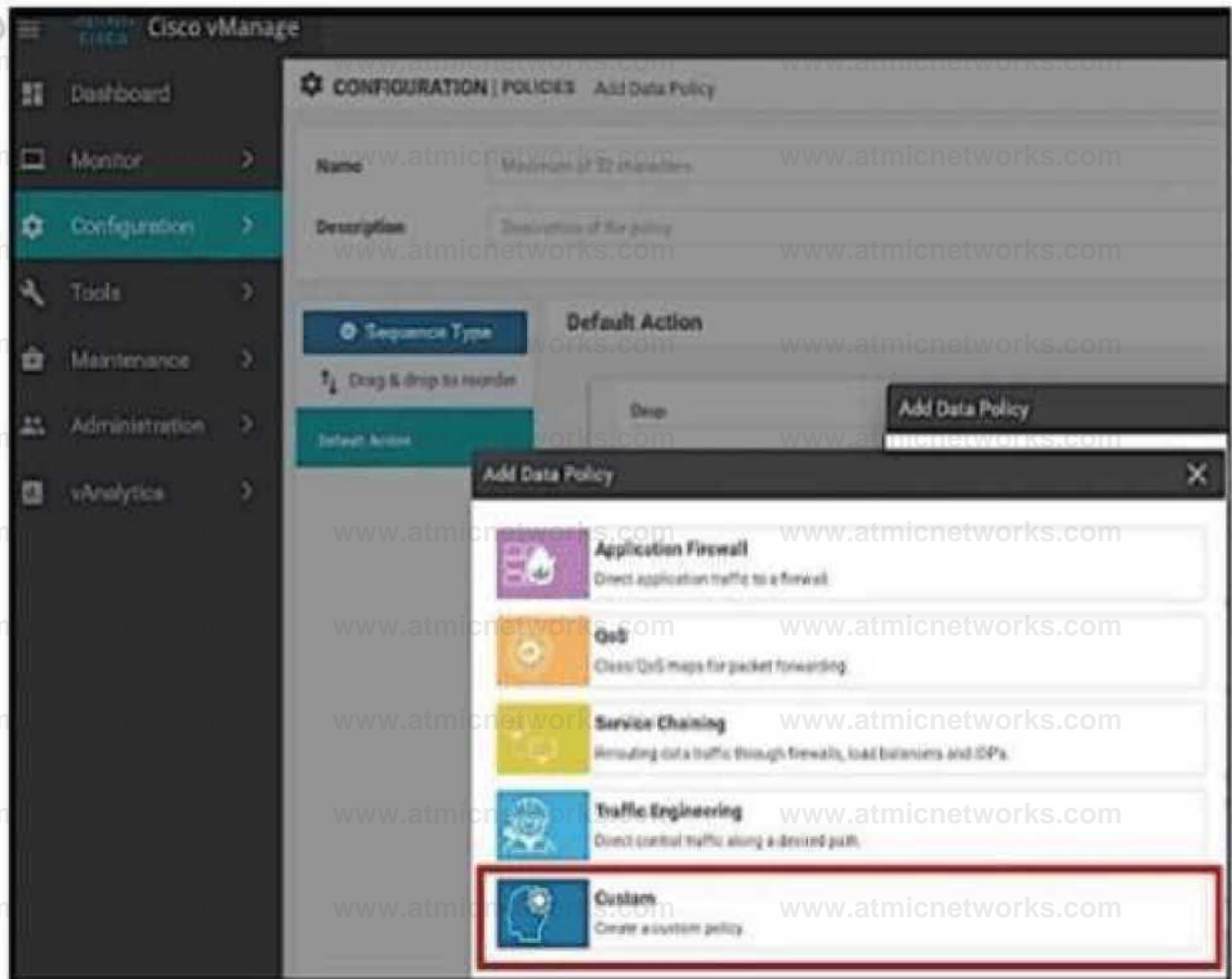
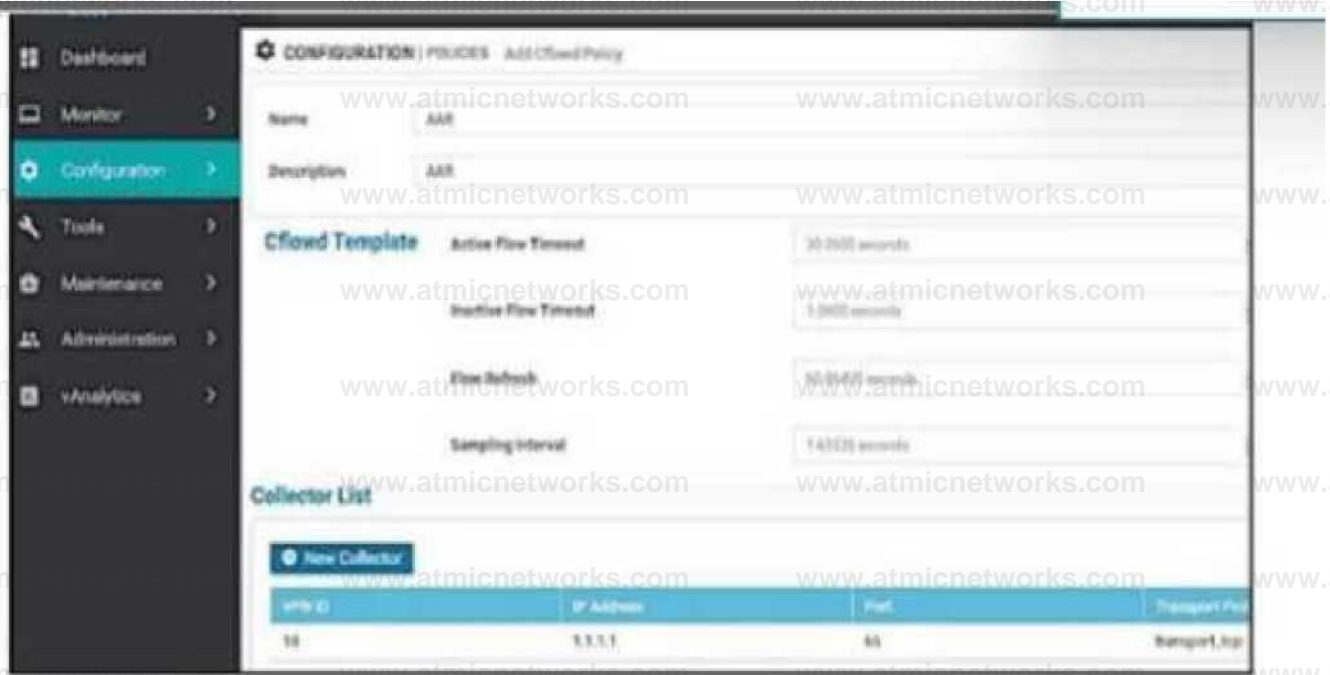
H^y
Jf-fLr bid

Q vA/wiybc*

Wil!*Wt

t





- A. Option A
- B. Option B
- C. Option C

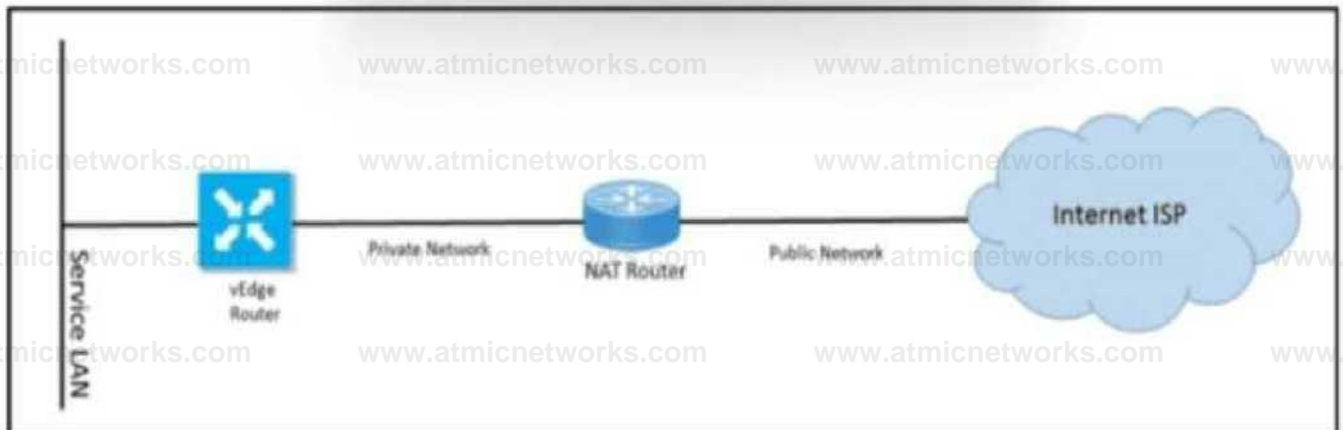
D. Option D

Answer: B

Explanation:

Question: 262

Refer to the exhibit.



Refer to the exhibit Which NAT types must the engineer configure for the vEdge router to bring up the data plane tunnels?

- A. Enable Full Cone NAT on the vEdge interface
- B. Use public color on the TLOC
- C. Use private color on the TLOC
- D. Enable Symmetric NAT on the vEdge interface

Answer: A

Explanation:

Question: 263

An engineer modifies a data policy for DIA in VPN 67. The location has two Internet-bound circuits.

Only the web browsing traffic must be admitted for DI

A. without further discrimination about which transport to use.

Here is the existing data policy configuration:

data-policy DIA

vpn-Hst VPN-67

sequence 10

match

destination-data-prefix 4ist IN TERN AL-NETWORKS

1

default-action drop

Which policy configuration sequence meets the requirements?

sequence 5

match

destination-port 80 443

destination-ip 0.0.0,0 0

action accept

nat use-vpn 0

sequence 20

match

destination-port 80 443

source-ip 0.0.0.0/0

J

action accept

set

locamloc-Nst

color blz-Internet

sequence 20

match

destination-port 80 443

destination-ip 0.0.0.0/0

action accept
nat use-vpn 0

(sequence 5

match

destination-port 80 443

source-ip 0.0.0.0/0

action accept
set

local-tloc-list

color blz-Internet

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 264

Which two vRoute attributes should be matched or set in vSmart policies and modified by data policies?
(Choose two.)

- A. site ID
- B. preference
- C. VPN

D. TLOC

E. origin

Answer: B,C

Explanation:

Question: 265

Which percentage for total memory or total CPU usage for a device is classified as normal in the WAN Edge Health pane?

- A. more than 80 percent usage
- B. less than 70 percent usage
- C. between 70 to 90 percent usage
- D. more than 90 percent usage

Answer: B

Explanation:

Question: 266

Which configuration component is used in a firewall security policy?

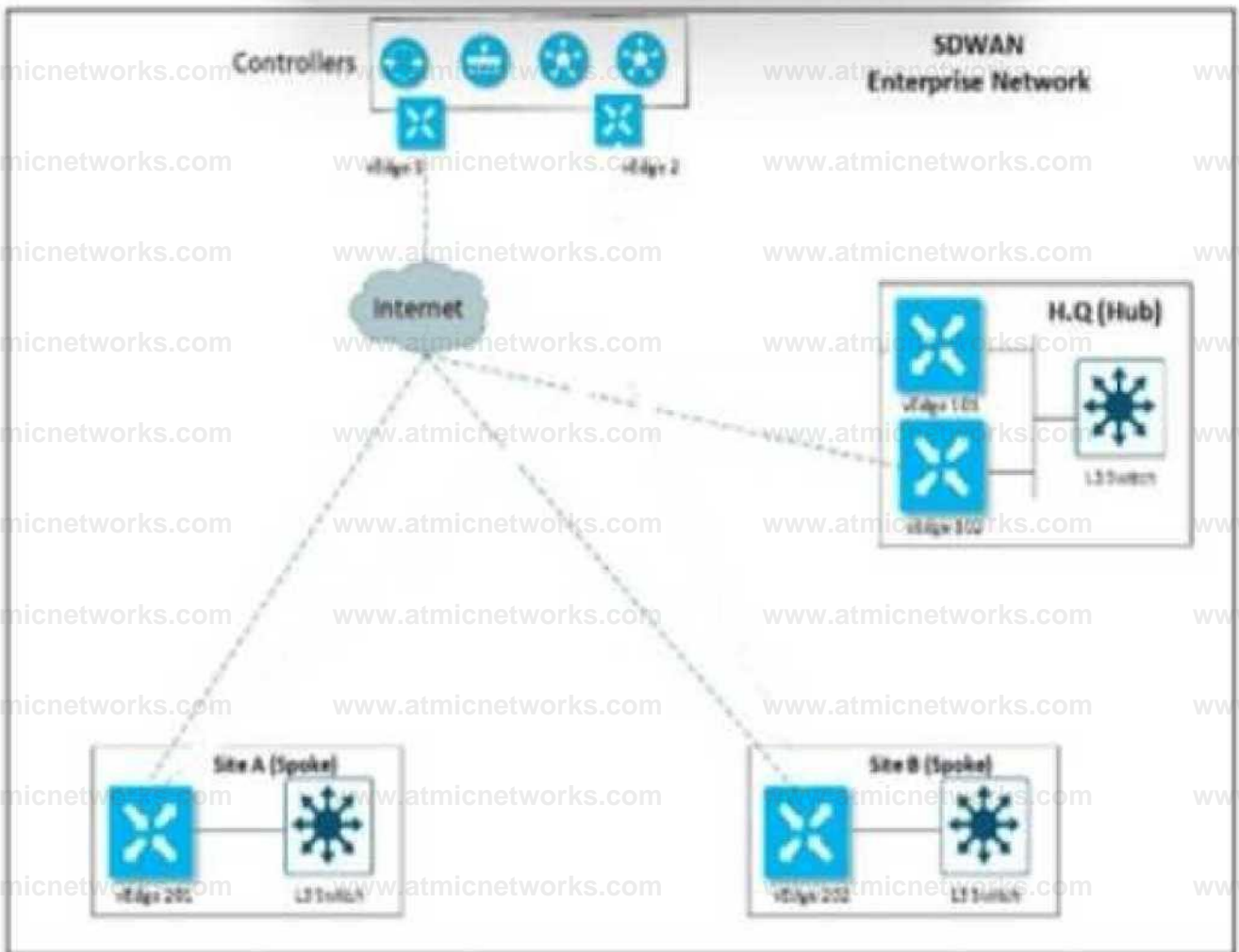
- A. numbered sequences of match-action pairs
- B. application match parameters
- C. URL filtering policy
- D. intrusion prevention policy

Answer: A

Explanation:

Question: 267

Refer to the exhibit.



Refer to the exhibit An engineer must configure a QoS policy between the hub and site A (spoke) over a standard internet circuit where traffic shaping is adjusted automatically based on available bandwidth. Which configuration meets the requirement?

- HHh sdwin Interact GlgabiiEth*mt1 qa£-jdjpu*e
- nenod 90
- dcwFiilrMm (NO
- downstream rifige Ei MO 1MM
- upttHOM GOOD
- upstream Wigt 4000 16000 nit
- TUrttieLttflirfacr
- n:jps Nation ipMC Wight I
- color pub ic-InTtmet
- Hp iitf-rwfitataUi
- VfTUFwgKdnnKtloft-prefmi'ce 5 illow-wrvice eU

^” iSpg^i

IntarfKB &Q#>i(BfrrMCI
qoi-oddpirvt
(wood 40
downstream 1Q0W
downitMMi w\$« MMO 12300
upstream 9000
upsiream rang* 5000 16000 uk
tiniri-irterfat*
•ncspsulsiion ipsec weight I optor mpls
(HI Ijit-rpwrt-Circuit
vrnariage-ctinrifctlon-preft'ence 6 dlwratnric* ai

Hub
ad wan
interface GigabitEthernet1 qos adaptive period 90
downstream 8000 downstream range 6000 10000 upstream
8000
upstream range 4000 16000 exit
tun net Interface
encapsulation ipsec weight 1
color public internet no las resort <kt urt vmanage-
connecon-preferenca 5 show-service all

Sly AISjiokvj

sdwen
interface GigabitEthernet1 qos-adaptive period 90
downstream LOGO
downstream range 6000 10 0 0 0
upstream 8000
upstream range 4000 16000 exit
tunnel-interface
encapsulation ipsec weight 1 color public internet no
lasbresort-circuit
vmanage-connecon-preterence 5 allow servtce all

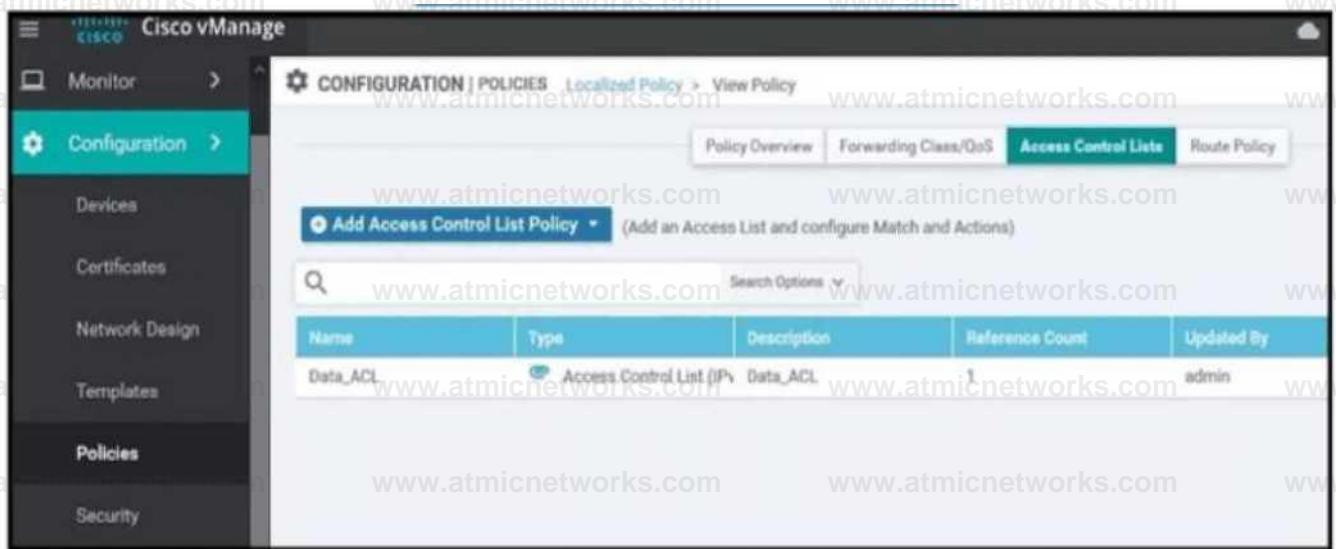
A. Option A B. Option B C. Option C D. Option D

Answer: D

Explanation:

Question: 268

Refer to the exhibit.



Refer to the exhibit. An engineer must block FTP traffic coming in from a particular Service VPN on a WAN Edge device Which set of steps achieves this goal?

- A. Create a localized policy and add it to (he interface feature template
- B. Create a localized policy add it to the device template and add an ACL to the interface feature template
- C. Create a prefix tat, add it to the localized policy and add it to the interface feature template
- D. Create a localized policy add it to VPN template and add an ACL to the interface feature template

Answer: C

Explanation:

Question: 269

A network administrator configures SNMPv3 on a Cisco WAN Edge router from CLI for monitoring purposes How many characters are supported by the snmp user <username> command?

- A. from 1 to 8
- B. from 1 to 16
- C. from 1 to 32
- D. from 1 to 48

Answer: C

Explanation:

Question: 270

Which two virtualized environments are available for a company to install the controllers using the On-premises model? (Choose two)

- A. VMware vSphere ESXi
- B. VMware Workstation
- C. kernel-based virtual machine
- D. OpenStack
- E. Microsoft Hyper-V

Answer: A,D

Explanation:

Question: 271

Which two performance data details are provided by Cisco SO-WAN vAnalytics? (Choose two)

- A. jitter loss and latency for data tunnels
- B. application quality of experience score from zero to ten
- C. detail on total cost of ownership for the fabric
- D. certificate authority status (health and expiration dates) for all controllers
- E. view devices connected to a vManage NMS

Answer: A,B

Explanation:

Question: 272

How are policies deployed on cloud-hosted Cisco SD-WAN controllers?

- A. Policies are created on vSmart and enforced by vSmart
- B. Policies are created on vSmart and enforced by vManage
- C. Policies are created on vManage and enforced by vManage.
- D. Policies are created on vManage and enforced by vSmart

Answer: A

Explanation:

Question: 273

A network administrator configures SNMPv3 on a Cisco WAN Edge router from CL I for monitoring purposes
How many characters are supported by the snmp user username command?

- A. from 1 to 8
- B. from 1 to 16
- C. from 1 to 32
- D. from 1 to 48

Answer: C

Explanation:

Question: 274

In which file format is a critical severity report downloaded from the MONITOR | ALARM tab in the vManage GUI?

- A. .txt
- B. .pdf
- C. csv
- D. xlsx

Answer: C

Explanation:

Question: 275

Refer to the exhibit.

Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate Serial
vBond	vBond	10.1.1.103	14 Jun 2021 3:49:50 PM +04	f16700...	Installed	1	615D8F69000000000005
vSmart	-	-	-	12aa1...	CSR Generated	-	No certificate installed
vManage	vManage1	10.1.1.101	14 Jun 2021 3:17:54 PM +04	ca64f9...	vBond Updated	1	61099683000000000002

Refer to the exhibit vManage and vBond have an issue establishing a connection to vSmart Which two actions does the administrator take to fix the issue? (Choose two)

Install the certificate received from the certificate server.

- A. Manually resync vManage and vBond
- B. Reconfigure the vSmart from CLI with the proper Hostname & System IP
- C. Delete and re-add vSmart Click Generate and validate CSR
- D. Request a certificate from the certificate server based on the CSR for the vSmart

Answer: C,D

Explanation:

Question: 276

What is the threshold to generate a warning alert about CPU or memory usage on a WAN Edge router?

- A. 70 to 85 percent
- B. 70 to 90 percent
- C. 75 to 85 percent
- D. 75 to 90 percent

Answer: C

Explanation:

Question: 277

How should the IP addresses be assigned for all members of a Cisco vManage cluster located in the same

data center?

- A. in the same subnet
- B. in overlapping IPs
- C. in each controller with a /32 subnet
- D. in different subnets

Answer: A

Explanation:

Question: 278

An engineer must avoid routing loops on the SD-WAN fabric for routes advertised between data center sites Which BGP loop prevention attribute must be configured on the routers to meet this requirement?

- A. same OMP overlay-as on WAN Edge routers of all data centers
- B. static routing on al WAN Edge routers instead of BGP
- C. same BGP AS between all WAN Edge routers and CE routers
- D. same BGP AS between all CE and PE routers

Answer: A

Explanation:

Question: 279

Which protocol advertises WAN edge routes on the service side?

- A. EIGRP
- B. OSPF
- C. BGP
- D. ISIS

Answer: B

Explanation:

Question: 280

A WAN Edge device has several service VPNs with no routing protocol configured in the service VPNs The device must be configured so that all connected routes are visible in OMP for VPN 10 Which configuration meets the requirement?

A)

vpn 10

nama — SoHrict VPN 10 ****“ omp

redistribute cwnocted

B)

omp no shutdown growfuHt start jav*rt]» connected

C)

omp

no shutdown pattU-rtnoH tedtur but* connoctta

D)

vpn 10

nam* — SoMct VPN IO omp

advortno connected

A. Option A B. Option B C. Option C D. Option D

Answer: D

Explanation:

Question: 281

What are the two functions of vSmart? (Choose two)

- A. It orchestrates connectivity between WAN Edge routers using policies to create network topology
- B. It ensures that valid WAN Edge routers can build the control pane connectivity
- C. It uses TLOCs to uniquely identify the circuit interface to control plane and data plane information D. It validates that the WAN Edge trying to join the overlay is authorized to join.
- E. It builds control plane connections with WAN Edge routers using ILS or UIIS

Answer: D,E

Explanation:

Question: 282

Which two actions are necessary to set the Controller Certificate Authorization mode to indicate a root

certificate? (Choose two)

- A. Select the Controller Certificate Authorization mode that is recommended by Cisco
- B. Change the organization name of the Cisco SO-WAN fabric.
- C. Upload an SSL certificate to vManage,
- D. Select a private certificate signing authority instead of a public certificate signing authority
- E. Select a validity period from the drop-down menu

Answer: C,D

Explanation:

Question: 283

Refer to the exhibit.

PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	REMOTE COLOR	STATE	LOCAL ERROR
10.0.2.73	23456	10.0.2.73	23456	default	trying	DCONFAIL

Refer to the exhibit Cisco SD-WAN is deployed with controllers hosted in a data center All branches have WAN Edge devices with dual connections to the data center one via Internet and the other using MPLS Three branches out of 20 have issues with their control connections on MPLS circuit The local error refers to Control Connection Failure Which action resolves the issue*?

- A. Rectify any issues with the underlay routing configuration
- B. Match the TLOC color on the controllers and all WAN Edge devices
- C. Match certificates for the DTLS connection and Root CA must be installed first on WAN Edge devices
- D. Update the system IP on vManage and then resend it to the controllers

Answer: A

Explanation:

Question: 284

Which encryption algorithm is used for encrypting SD-WAN data plane traffic?

- A. Triple DES
- B. IPsec

- C. AES-128
- D. AES-256 GCM

Answer: D

Explanation:

Question: 285

A customer has 1 to 100 service VPNs and wants to restrict outbound updates for VPN1 Which control policy configuration restricts these updates?

A)

>44

VPN7-1W fvpr 2-1IX;

MAM 10 lutTi rude vpiJII VPN?'WO r

--ir '4«1

il*tei!!-Ktan ««\$!>

B)

```
policy
lists
vpn-list VPN2-100
vpn 2-100
|
|
control-policy restrict_2-100
sequence 10
match route
vpn-list VPN2-100
|
action reject
|
default-action accept
```

C)

```
policy
lists
vpn-list VPN1
vpn 1
|
|
control-policy restrict_1
sequence 10
match route
vpn-list VPN1
|
action reject
|
default-action accept
```

D)

```
Policy
lists
vpn-list restricted_vpns
vpn 2-100
|
|
vpn-membership restrict_1
sequence 10
match vpn-list restricted_vpns
action reject
|
|
default-action accept
```

A. Option A

B. Option B C. Option C D. Option D

Answer: C

Explanation:

Question: 286

What happens if the intelligent proxy is unreachable in the Cisco SD-WAN network?

- A. The grey-listed domains are unresolved
- B. The Cisco Umbrella Connector locally resolves the DNS request
- C. The block-listed domains are unresolved
- D. The Cisco Umbrella Connector temporarily redirects HTTPS traffic

Answer: A

Explanation:

Question: 287

What are the two impacts of losing vManage connectivity to fabric in the Cisco SD-WAN network?

(Choose two)

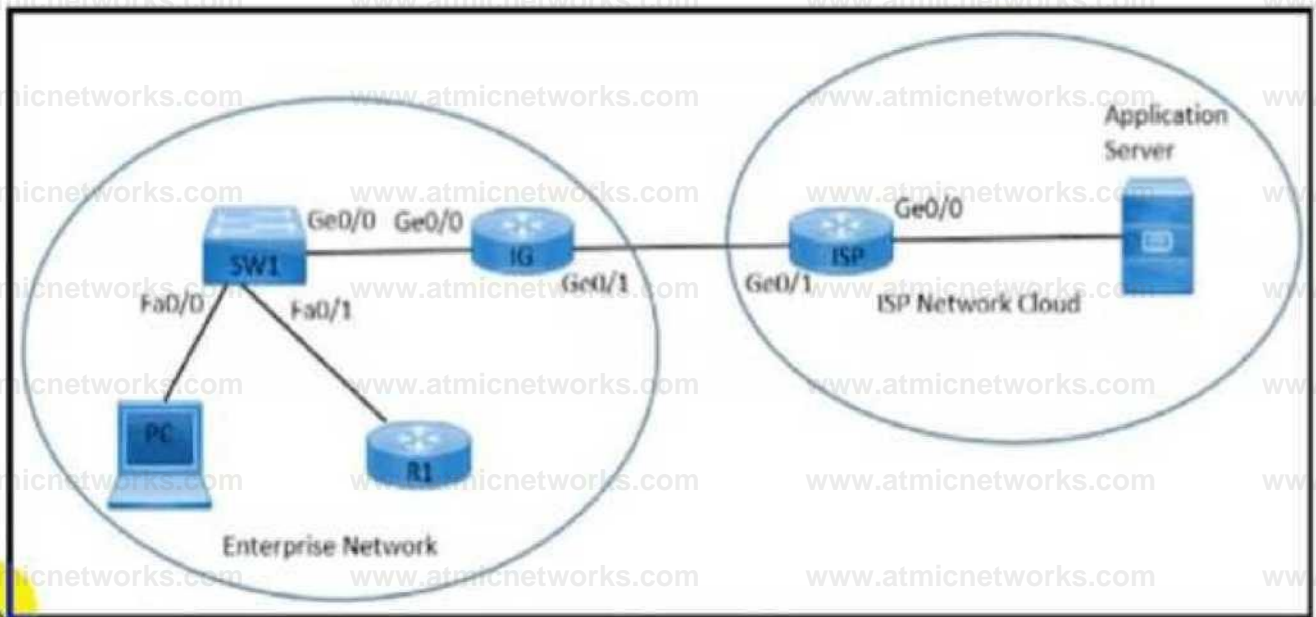
- A. Policy changes propagation stops
- B. Statistics collection stops
- C. BFD peering between WAN Edge devices are unestablished
- D. Creation of templates is impossible
- E. IPsec tunnels tear down for WAN Edge devices.

Answer: A,B

Explanation:

Question: 288

Refer to the exhibit.



Refer to the exhibit. An enterprise network is connected with an ISP network on an 80 Mbps bandwidth link. The network operation team observes 100 Mbps traffic on the 1Gig-ISP link during peak hours. Which configuration provides bandwidth control to avoid traffic congestion during peak hours?

A)

```

policy-map CUS PMAP
class CUS CHAP
police HOBoMQ 3 00000

```

```

interface gigabitethmrii 0/0
description ~ TO SW
ip address 100J0-5 25 5.255.25 5 0
se^ice-oobcy input CUSjPMAPd

```

B)

```

poHey-rrap SHAPE^MAP class dus-dtfadt
shape average 80000000

```

```

Interface gigabttthemet 0.1
description ' TO i SP
ip address 10 0 20 5 255 255 255 0
Mvktfrprllcy output SHAPE^MAP

```

C)

```

policy-map CUS PMAP
danCUS CMAP police #mmo 3 0 0000

interface g-gabitethemet 0/0

```

description " TO ISP*"
ip address 10.0.20.1 255 255 255 0
service policy input CUS_PMAP

D)

policy-map SHAPE_MAP class class-default
shape average 800000 0

Interface gigsbJtethemet 0/1
description" TO IGrack &4^5 A NJ J GT JU '

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 289

Which VManage dashboard is used to monitor the next-hop reachability between two devices traversing through OMP for a service VPN?

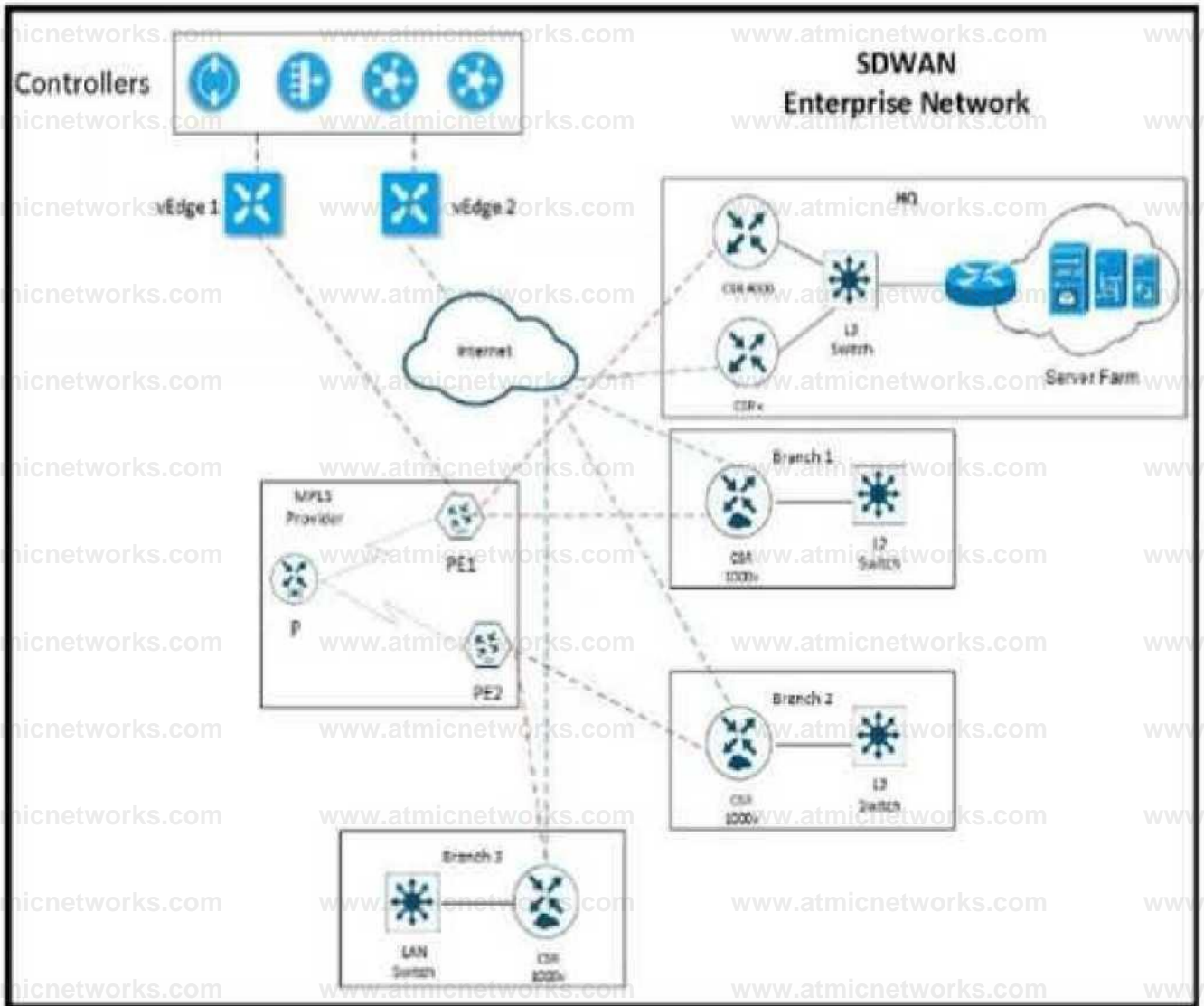
- A. Troubleshooting > App Route Visualization
- B. Troubleshooting > Tunnel Health
- C. Troubleshooting > Simulate Flows
- D. Troubleshooting > Packet Capture

Answer: C

Explanation:

Question: 290

Refer to the exhibit.



Refer to the exhibit The network team must configure EIGRP peering at HQ with devices in the service VPN connected to WAN Edge CSRv. CSRv is currently configured with

```

vlptela-system: system device-model vedge-cloud host-nam
                  CSRv
location          CA
system-ip         104.44
domain-id         1
site-id           1
organization-name ABC clock timezone US'Newyork vbond
10.10.0J port 12345

omp
no shutdown
graceful-restart

```

Which configuration on the WAN Edge meets the requirement*?

A)

```

vpn 0
interface pe0/0
description "Internet Circuit" ip address 165.200.229.30 tunnel-interface
encapsulation ipsec
color public-internet allow-service all

router
aw
address-family ipv4-unicast maximum-path paths 4 network 10.0.0.0/28
redistribute omp

vpn 312
interface eth0 shutdown

```

B)

```

vpn 0
interface eth0
description "Internet Circuit" ip address 500.16.5.200/30 tunnel-
interface
•ncaptutmlon ipra color public-internet allow-service all

router
•^T
address-family ipv4-unicast maximum-path paths 4 network 10.0.0.0/28

```

redistribute ospf

vpn 512

interface eth0 shutdown

C)

vpn 0

Interface ge0/0/24

description "Internet Circuit" ip address 10.0.0.1 255.255.255.0 tunnel-

interface encapsulation ipsec color pbbbc^nterrttt allow-service alt

vpn 1

router

•W

address-family ipv4 must maximum-paths 4 network 10.0.0.0/24
redistribute ospf

Interface ge0/0/24

ip address 10.0.0.1 255.255.255.0

vpn 512

Interface wi0 shutdown

D)

vpn 0

vpn 1

interface ge0/0/24

description "Internet Circuit" ip address 10.0.0.1 255.255.255.0 tunnel-

interface encapsulation ipsec color public -Internet Ai Foodservice a ll

router

•iflrp

address-family ipv4 unicast maximum-paths 4 network 10.0.0.0/24

redistribute ospf

interface ge0/0/24

ip address 10.0.0.1 255.255.255.0

vpn 512

interface eth0 shutdown

A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

Question: 291

What is the order of operations for software upgrades of Cisco SD-WAN nodes?

- A. vBond vManage vSmart WAN Edge
- B. vManage vBond WAN Edge. vSmart
- C. vManage vSmart, vBond, WAN Edge
- D. vManage vBond vSmart WAN Edge

Answer: D

Explanation:

Question: 292

What is the main purpose of using TLOC extensions in WAN Edge router configuration?

- A. creates hardware-level transport redundancy at the local site
- B. creates an IPsec tunnel from WAN Edge to vBond Orchestrator
- C. transports control traffic to a redundant vSmart Controller
- D. transports control traffic w remote-site WAN Edge routers

Answer: D

Explanation:

Question: 293

Which device should be configured with the service chain IP address to route intersite traffic through a firewall?

- A. vSmart
- B. firewall
- C. spoke WAN Edge
- D. hub WAN Edge

Answer: A

Explanation:

Question: 294

A customer wants to use AWS for Cisco SD-WAN IaaS services by deploying virtual SD-WAN routers in a transit AWS VPC. The transit VPC then connects via site-to-site IPsec tunnels to an AWS transit gateway. Which transit VPC connects via site-to-site IPsec tunnels to an AWS transit gateway?

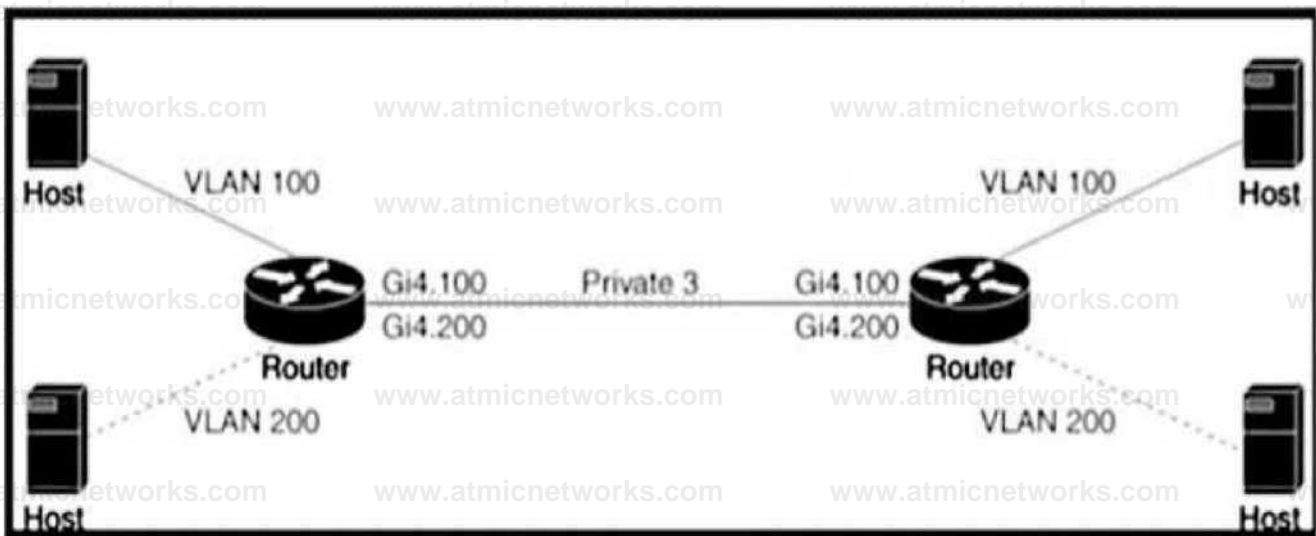
- A. Cisco Cloud onRamp for Multicloud
- B. Cisco Cloud onRamp for SaaS
- C. Cisco Cloud onRamp for Colocation
- D. Cisco Cloud onRamp for IaaS

Answer: D

Explanation:

Question: 295

Refer to the exhibit.



Refer to the exhibit. An engineer is configuring a QoS policy to shape traffic for VLAN 100 on a subinterface. Which policy configuration accomplishes the task?

- A)

```
int GigabitEthernet4/100
  service-policy Kft.GoS-TMdt
  fhrp vrf 100 100.0.0.0
```

```
int GigabitEthernet4/100
  nupiaTion dotIQ 200
```


service-policy output ^happ^GigstMeth^m?!* 100

B)

policy-map thapt.GlgabltEthfrnfUJOO

class-map match-all

match access-group name K/I OcS ^nMlfl

policy-map type qos

1

class-map match-all

match access-group name dotIQ 200

service-policy output ihap4_QiQ3bITE9h«rn*!4 10C

C)

policy-map shape_GigabitEtherne<4 200

class-map match-all

match access-group name xyi_Qo\$-mode.

shape average 100000000

interface GlgabitEihetneri 100

encapsulation dot1Q 100

service-policy output shape^GigabitEhmet* 200

D)

policy-map ihapt_nQfaabl&therhtt* JiDO dm dm QueutO

class-map match-all

match access-group name yz_QoS-rnode1

policy-map type qos

class-map match-all

match access-group name Uttan 4MiO 100

service-policy output ihapt^GIQabhEtherneU 100

A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

Question: 296

The Cisco SD-WAN engineer is configuring service chaining for a next-generation firewall located at the headquarters. Which configuration creates the service?

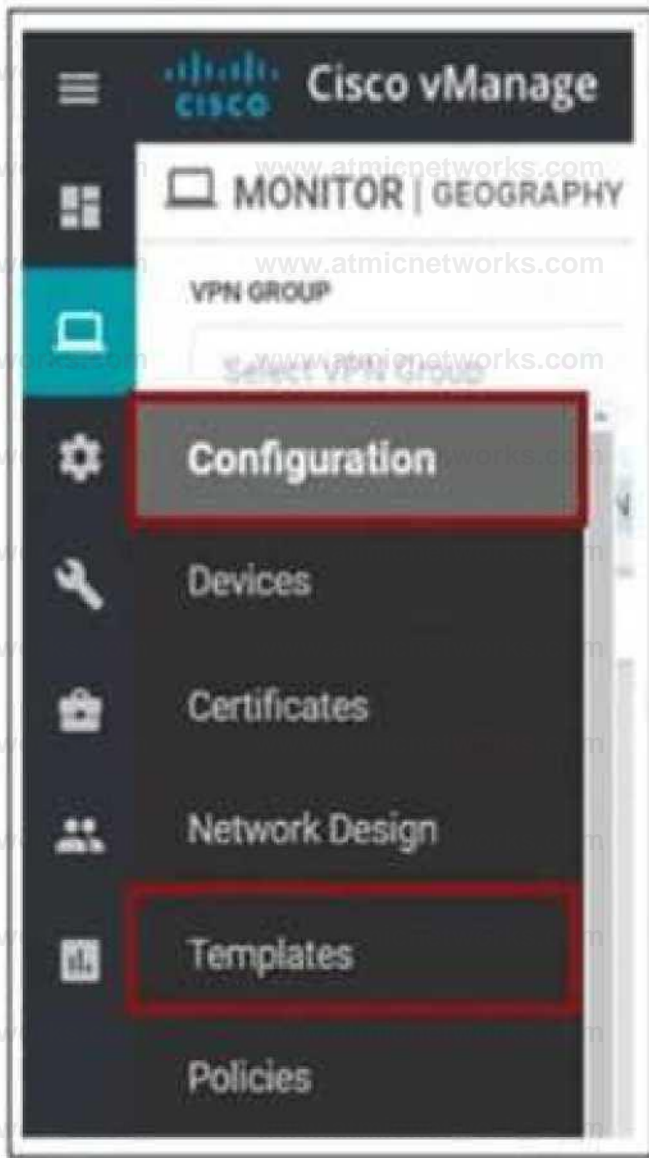
A)



B)



c)



D)



- A. Option A
- B. Option B
- C. Option C
- D. Option D

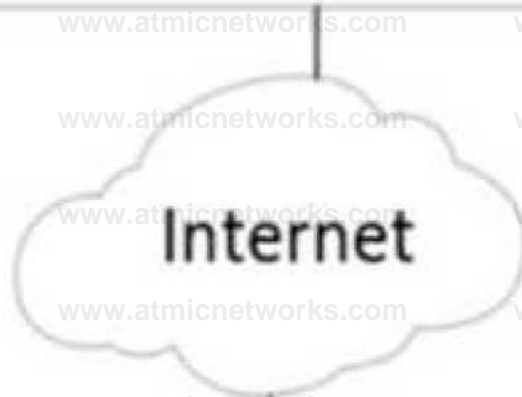
Answer: C

Explanation:

Question: 297

Refer to the exhibit.

SD-WAN Controllers (Cisco Hosted)



NAT Router



L2 Switch



Edge-1



Edge-2

Refer to the exhibit Which configuration must the engineer use to form underlay connectivity for the Cisco SD-WAN network?

A)

```
SI vpn 612 Jm+rf ac< rthO  
Ip Jddr*ss 10.0.0.21 "24 no  
shutdown
```

```
Ip rout* 0.0.0CO 10 0 0 254
```

```
von 512  
Interfiw vthD ip address 10X  
0.2'24 no shutdown
```

```
Ip rout* 0 0 0 CO 10,O.O.2M
```

B)

5!

```
vpn 10 interface 0*0*2  
Ip address 1Q 10.10 9 29 no  
Shutdown
```

```
Ip rout* 0.0 0 CO 10 10.10.11
```

```
TO vpn 10 Interne* 0*01 ip  
address 10.10.10 10/29 no  
shutdown t
```

```
Ip route 0 0.0 C O 10 10 10.11
```

81 von 0 Interface lflgtCO Ipaddrw 10.60,0 1'29 no shutdown

Ip rout® Q 0 Q CQ 10 M.O 3

£ vpn 0 Interfax IOgvOfO 1p address 10 50.01'29 ho Shutdown

Ip route C 0 C CO ID 50,0 3

C)

RI vpn 0 Imtrtat g+CO tp address 10 50 0 2 3 0 tunrMHmerfm

Ip route 3 0 0 0'0 10 50.0-4

Bl vpn 0 Interface geOt Ip xMrtu 10 50.0 3 30 tunnel interface

Ip route 0 0 0 CO 10 50 0 4

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 298

How many concurrent sessions does a vManage REST API have before it invalidates the least recently used session if the maximum concurrent session number is reached?

- A. 150
- B. 200
- C. 250
- D. 300

Answer: A

Explanation:

Question: 299

After deploying Cisco SD-WAN the company realized that by default, all sites built direct IPsec VPN tunnels to

each other in their previous topology all spoke sites used the head office as their next hop for the LAN segment that belongs to network 40.0.0.0/16. The company wants to deploy its previous policy, which allows the 40.0.0.0/16 network that originates at the hub to advertise to the spokes. Which configuration meets the requirement?

A)



B)



C)



D)



A. Option A B. Option B C. Option C D. Option D

Answer: D

Explanation:

Question: 300

An engineer configures an application-aware routing policy for a group of sites. The locations depend on public and private transports. The policy does not work as expected when one of the transports does not perform properly. This policy is configured:

policy

sla-class SULK-DATA loss 20 latency 300 jitter 100

sla-class TRANSACTIONAL_DATA loss 15 latency 50 jitter 100

**sla-class REALTIME loss 20
latency 100 jitter 30**

app-route-policy VPN-10_MPLS_AND_INET_SITES

vpn dis* VPN-10

sequence 1 match

**action backup-s la-preferred -color biz-internet sla-class
REALTIME preferred-color privatel i**

**sequence 11 match
dscp 34 i**

**action
backup-sla-preferred-color biz-internet
sla-class TRANSACTIONAL DATA preferred-color privatel**

which configuration completes the policy so that it works for all locations? A)

**s 3< 3M TRAN SAC T10NA ^_DATA lose 5
latency 50
jitter 100**

**subclass REALTIME
loss 2
latency 100 jitter 30**

B)

**t13<l«t THAN SAC TIONAL^DATA
loss 2
latency 100
jitter 30**

**siHlass REALTIME
loss 16
latency 100
jitter 100**

C)
***-diU BULKJJATA
IMS 10 latency 300 Jitter 100**

SiMlass REALTIME iOS* 2 latency 100 jitter 30

D)

>l1<l1M BULK_DATA

loss 15

latmcy 100

jitttr 100

QUESTION: 301 KIM TRANSACTIONAL JAIA hu 10 latency 300 jhtar 100

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 301

Which service VPN must be reachable from all WAN Edge devices and the controllers?

- A. VPNO
- B. VPN10
- C. VPN215
- D. VPN512

Answer: A

Explanation:

Question: 302

In which Cisco SD-WAN deployment scenario does Cisco Umbrella SIG deliver the most value?

- A. when a centralized Internet breakout solution is implemented
- B. when resource-intensive security operations are offloaded from entry-level WAN Edge devices
- C. when the identity of several WAN Edge devices is verified throughout the network

Answer: B

Explanation:

Question: 303

An engineer must create a QoS policy by creating a class map and assigning it to the LLQ queue on a WAN Edge router. Which configuration accomplishes the task?

A)



B)



C)



D)



A. Option A B. Option B C. Option C D. Option D

Answer: D

Explanation:

Question: 304

Which multicast component is irrelevant when defining a multicast replicator outside the local network without any multicast sources or receivers?

- A. PIM interfaces
- B. TLOC
- C. overlay BFD
- D. OMP

Answer: A

Explanation:

Question: 305

What is the role of the Session Traversal Utilities for NAT server provided by the vBond orchestrator?

- A. It facilitates SD-WAN toners and controllers to discover their own mapped or translated IP addresses and port numbers
- B. It prevents SD-WAN Edge routers from forming sessions with public transports among different service providers
- C. It facilitates SD-WAN Edge routers to stay behind a NAT-enabled firewall while the transport

addresses of the SD-WAN controller are unNAT-ed

D. It allows WAN Edge routers to form sessions among MPLS TLOCs using only public IP addresses

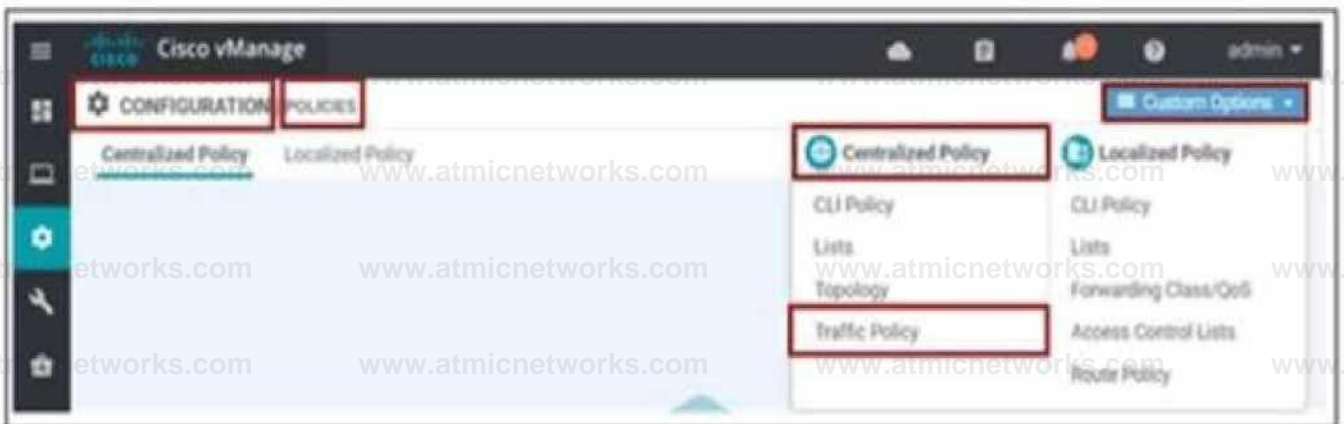
Answer: C

Explanation:

Question: 306

An engineer must create a QoS policy by creating a class map and assigning it to the LLQ queue on a WAN Edge router Which configuration accomplishes the task?

A)



B)



C)



D)



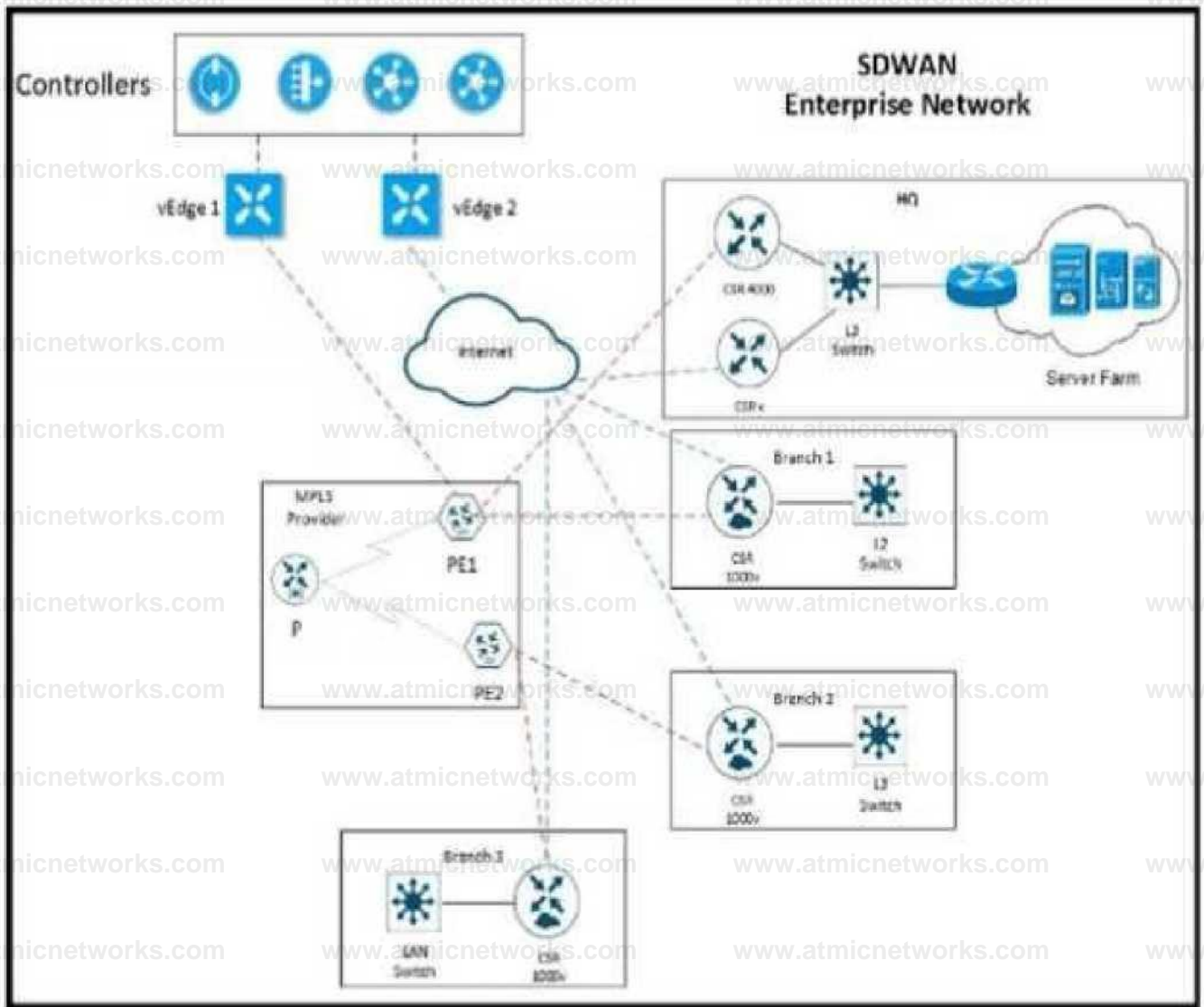
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation:

Question: 307

Refer to the exhibit.



Refer to the exhibit The network team must configure EIGRP peering at HQ with devices in the service VPN connected to WAN Edge CSRv. CSRv is currently configured with

**viptelMystem: system device-model vedge-cloud host-nam
CSRv**

location CA

system-ip 104.44

domain-id 1

site-id 1

organization-name ABC clock timezone US/Newyork vbond

10.10.0.1 port 12345

omp

no shutdown

graceful-restart

Which configuration on the WAN Edge meets the requirement*?

Which configuration on the WAN Edge meets the requiremnet

A)

vpn 0

router

eigrp

address-family ipv4-unicast

maximum-path paths 4 network 10.0.0.0/28

redistribute omp

interlace geO 0

description..... Internet Circuit

ip address 209.165 JOO.22 9'30

tunneHInterface

encapsulation ipsec

color public-internet allow-service all

vpn 512

interface ethO shutdown

B)

vpn 0 vpn 1 interface geO/O

description Internet Circuit ""L

Ip address 209.165.2 00.229 30 tunnel-interface

encapsulation ipsec color public-internet allow-service

all

router etgrp

address-family ipv4-unicast maximum-path paths 4

network 10.0.0 0 28 redistribute omp

interface ge0/1

Ip address 10 0 0 1/28

vpn 512 interface eth0 shutdown

vpn 0
interface ge0/0 description "Internet Circuit"
ip address 209.165.200.22 255.255.255.30
encapsulation ipsec tunnel-mode
allow-service all

vpn 1 router
eigrp
address-family ipv4-unicast maximum-paths 4
network 10.0.0.0/28 redistribute ospf

interface ge0/1
ip address 10.0.0.1/28

vpn 512
interface eth0 shutdown

D)

Q vpn 0

```
interface ge0/0 description "Internet Circuit" ip address
209.186.2.00-223/30 tunnel-mode interface
encapsulation ipsec color public-internet al low-service all
```

router

```
•t(jrp
address-family ipv4*unicast maximum-path paths 4 network
10.0.0.0/28 redistribute omp
```

vpn 512

```
interface eth0 shutdown
```

A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

Question: 308

An engineer configured a data policy called ROME-POLICY. Which configuration allows traffic flow from the Rome internal network toward other sites?

- A. apply-policy site-list Rome data-policy ROME-POLICY from-tunnel
- B. apply-policy site-list Rome data-policy ROME-POLICY from-service
- C. site-list Rome control-policy ROME-POLICY in
- D. site-list Rome control-policy ROME-POLICY out

Answer: A

Explanation:

Question: 309

DRAG DROP

Drag and drop the steps from the left into the order on the right to delete a software image for a WAN Edge router starting with Maintenance > Software Upgrade > Device list on vManage.

Click delete available software.	step 1
Click the checkbox next to the WAN Edge device.	step 2
Click WAN Edge in the title bar.	step 3
Select the version to delete and click delete.	step 4

Answer:

Explanation:

Click WAN Edge in the title bar.
Click the checkbox next to the WAN Edge device.
Click delete available software.
Select the version to delete and click delete.

Question: 310

Which two resource data types are used to collect information for monitoring using REST API in Cisco SD-WAN? (Choose two.)

- A. POST
- B. DELETE
- C. scalar

- D. array
- E. PUT

Answer: C,D

Explanation:

Question: 311

An enterprise deployed a Cisco SD-WAN solution with hub-and-spoke topology using MPLS as the preferred network over the Internet. A network engineer must implement an application-aware routing policy to allow ICMP traffic to be load-balanced over both the available links. Which configuration meets the requirement?

A)

```
app-route-policy VPN 10 AAR
vpn-list VPN_50
sequence 21
match
app-list ICMP
source-ip 0.0.0.0/0
i
action
sla-class ICMP SLA preferred-color public-internet sla-
class ICMP_SLA preferred-color mpls
```

B)

```
app-route-policy VPN IO AAR
vpn.list VPN_50~ " ~
sequence 21 match app-list ICMP source-lp 0.0.0.0/0
action sia-class ICMP SLA
```

C)

```
app-route-policy _VPN_1G.AAR
```

vpn-list VPN_50~ " "

sequence 21 match app-list ICMP source-ip 0.0.0.0/0

action

sla-class ICMP_SLA preferred-color mpls backup-

sla-preferred-color public-internet

D)

App-rOUU-pObCy VPH 10 AAR

vpn-HU VPN-50

sequence21

match

tMHfll ICMP

source^p 0 0 0 0 0

action

Uxlass iCMP SLA preferred* cok>r mpls public-internet

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 312

Which queue must an engineer configure for control and BFD traffic for convergence on a WAN Edge router?

- A. queue 0
- B. queue 1
- C. queue 2
- D. queue 7

Answer: C

Explanation:

Question: 313

Which storage format is used when vManage is deployed as a virtual machine on a KVM hypervisor?

- A. .iso
- B. .qcow2
- C. .ova
- D. .tgz

Answer: B

Explanation:

Question: 314

What are two benefits of installing Cisco SD-WAN controllers on cloud-hosted services? (Choose two.)

- A. utilizes well-known cloud services such as Azure, AWS, and GCP
- B. accelerates Cisco SD-WAN deployment
- C. allows integration of the WAN Edge devices in the cloud
- D. installs the controllers in two cloud regions in a primary and backup setup
- E. automatically implements zone-based firewalling on the controllers

Answer: B,D

Explanation:

Question: 315

Which protocol is used by the REST API to communicate with network services in the Cisco SD-WAN network?

- A. SSL
- B. HTTP
- C. IPsec
- D. SSM

Answer: B

Explanation:

Question: 316

What must an engineer consider when deploying an SD-WAN on-premises architecture based on ESXi hypervisor?

- A. Cisco must provision the backup and snapshots platform for the SD-WAN architecture
- B. The managed service provider must provision controllers with their appropriate certificates
- C. The IT team is required to provision the SD-WAN controllers and is responsible for backups and disaster recovery implementation
- D. The IT team will be given access by Cisco to a vManage for configuration templates and policies

Answer: C

Explanation:

Question: 317

Which feature delivers traffic to the Cisco Umbrella SIG cloud from a Cisco SD-WAN domain?

- A. L2TPv3 tunnel
- B. IPsec tunnel
- C. local umbrella agent
- D. source NAT

Answer: B

Explanation:

Question: 318

Which policy allows communication between TLOCs of data centers and spokes and blocks communication between spokes?

- A. centralized data policy
- B. centralized control policy
- C. localized control policy
- D. localized data policy

Answer: B

Explanation:

Drag and drop the steps from the left into the sequence on the right for a WAN Edge router after powering on for zero touch provisioning.

Router contacts a DNS service.	1
Router establishes a connection to vBond.	2
Router contacts a DHCP server.	3
Router connects to the ZTP server.	4

Answer:

Explanation:

Router connects to the ZTP server.
Router contacts a DNS service.
Router contacts a DHCP server.
Router establishes a connection to vBond.

Question: 320

What is the OMP graceful restart default value on vSmart controllers and WAN Edge routers?

- A. 21,600 seconds
- B. 43,200 seconds
- C. 86,400 seconds
- D. 604,800 seconds

Answer: B

Explanation:

Question: 321

How are custom application ports monitored in Cisco SD-WAN controllers?

- A. Customers add custom application ports in vAnalytics and vManage.
- B. Customers add custom application ports in vAnalytics and vSmart.
- C. Cisco adds custom application ports in vAnalytics and vManage.
- D. Cisco adds custom application ports in vAnalytics and vSmart.

Answer: A

Explanation:

Question: 322

How is the software managed in Cisco SD-WAN?

- A. Software upgrade operation in the group must include vManage, vBond, and vSmart.
- B. Software downgrades are unsupported for vManage.
- C. Software images must be uploaded to vManage through HTTP or FTP.
- D. Software images must be transferred through VPN 512 or VPN 0 of vManage.

Answer: A

Explanation:

Question: 323

Which website allows access to visualize the geography screen from vManager using the internet?

- A. *.opcnstreetmaps.org

- B. *.fullstreetmaps.org
- C. *.callstreelmaps.org
- D. *.globaistreetmaps.org

Answer: A

Explanation:

Question: 324

What is the default value for the number of paths advertised per prefix in the OMP feature template?

- A. 4
- B. 8
- C. 12
- D. 16

Answer: C

Explanation:

Question: 325

A network engineer must configure all branches to communicate with each other through the Service Chain Firewall located at the headquarters site. Which configuration allows the engineer to accomplish this task?

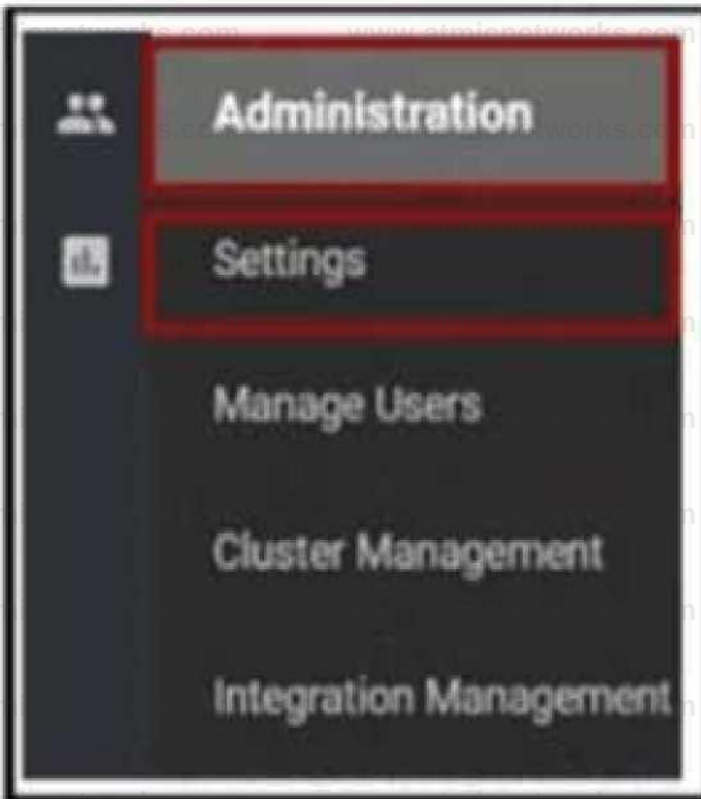
A)



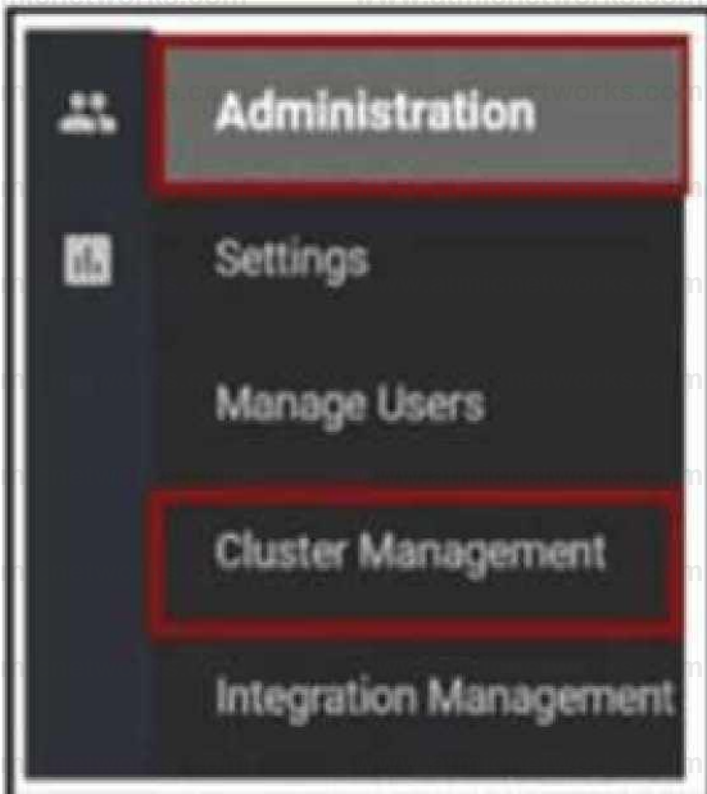
B)



C)



D)



A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 326

Which protocol detects path status (up/down), measures loss/latency/jitter, and measures the quality of the IPsec tunnel MTU?

- A. OMP
- B. IP-SLA
- C. BFD
- D. DTLS

Answer: C

Explanation:

Question: 327

What is the maximum number of IPsec that are temporarily created and converged on a new set of IPsec SAs in the pairwise keys process during a simultaneous rekey?

- A. 2
- B. 4
- C. 6
- D. 8

Answer: B

Explanation:

Question: 328

An engineer must configure local redundancy on a site. Which configuration accomplish this task?

- A. `vpn 0 interface interface-name`
- B. `tloc extension interlace nametloc extension interface interface name`
- C. `vpn 0 tloc extension interface`
- D. `interface-flame interface interface-name tloc-extension`

Answer: A

Explanation:

Question: 329

Which type of policy must be applied on a WAN Edge application-aware firewall to control traffic between two or more VPNs?

- A. service-insertion policy
- B. data policy
- C. firewall policy
- D. control policy

Answer: C

Explanation:

Question: 330

Refer to the exhibit.

Refer to the exhibit A WAN Edge device was recently added to vManage but a control connection could not be established Which action resolves this issue?

- A. Rectify the Rod CA certificate mismatch on WAN Edge devices
- B. Install the bootstrap code on WAN Edge and check for CSR
- C. Send the serial number to vBond from the vManage controller.
- D. Resolve the ZTP reachability and rectify smart account credentials issue

Answer: C

Explanation:

Question: 331

What are the default username and password for vSmart Controller when it is installed on a VMware ESXi hypervisor'?

- A. username Cisco password admin
- B. username admin password Cisco
- C. username Cisco password Cisco
- D. username admin password admin

Answer: D

Explanation:

Question: 332

Which SD-WAN component allows an administrator to manage and store software images for SD- WAN network elements?

- A. vGond controllers
- B. WAN Edge routers
- C. vSman controllers
- D. vManage NMS

Answer: D

Explanation:

Question: 333

An engineer is applying QoS policy for the transport-side tunnel interfaces to enable scheduling and shaping for a WAN Edge cloud router Which command accomplishes the task?

- A. cloud-qos-service-side
- B. qos-scheduler QOS_0
- C. qos-map QOS
- D. rewrite-rule QOS-REWRITE

Answer: C

Explanation:

Question: 334

Refer to the exhibit.



Refer to the exhibit The network team must configure application-aware routing for the Service VPN 50.0.0.0/16 The SLA must prefer MPLS for video traffic but the remaining traffic must use a public network What must be defined other than applications before the application-aware policy is create?

- A. SLA Class, Site VPN. Prefix
- B. Data Prefix, Site VPN TLOC C. Application, SLA VPN. Prefix
- D. Color, SLA Class, Sue, VPN

Answer: A

Explanation:

Question: 335

Which two different states of a WAN Edge certificate are shown on vManage? (Choose two.)

- A. inactive
- B. active
- C. staging
- D. invalid
- E. provisioned

Answer: B,E

Explanation:

Question: 336

Which two mechanisms are used by vManage to ensure that the certificate serial number of the WAN Edge router that is needed to authenticate is listed in the WAN Edge Authorized Serial Number Hst' (Choose two)

- A. Synchronize to the PnP
- B. Manually upload it to vManage
- C. The devices register to vManage directly as the devices come online
- D. The vManage is shipped with the list
- E. Synchronize to the Smart Account

Answer: B,E

Explanation:

Question: 337

Which protocol runs between the vSmart controllers and WAN Edge routers when the vSmart controller acts like a route reflector?

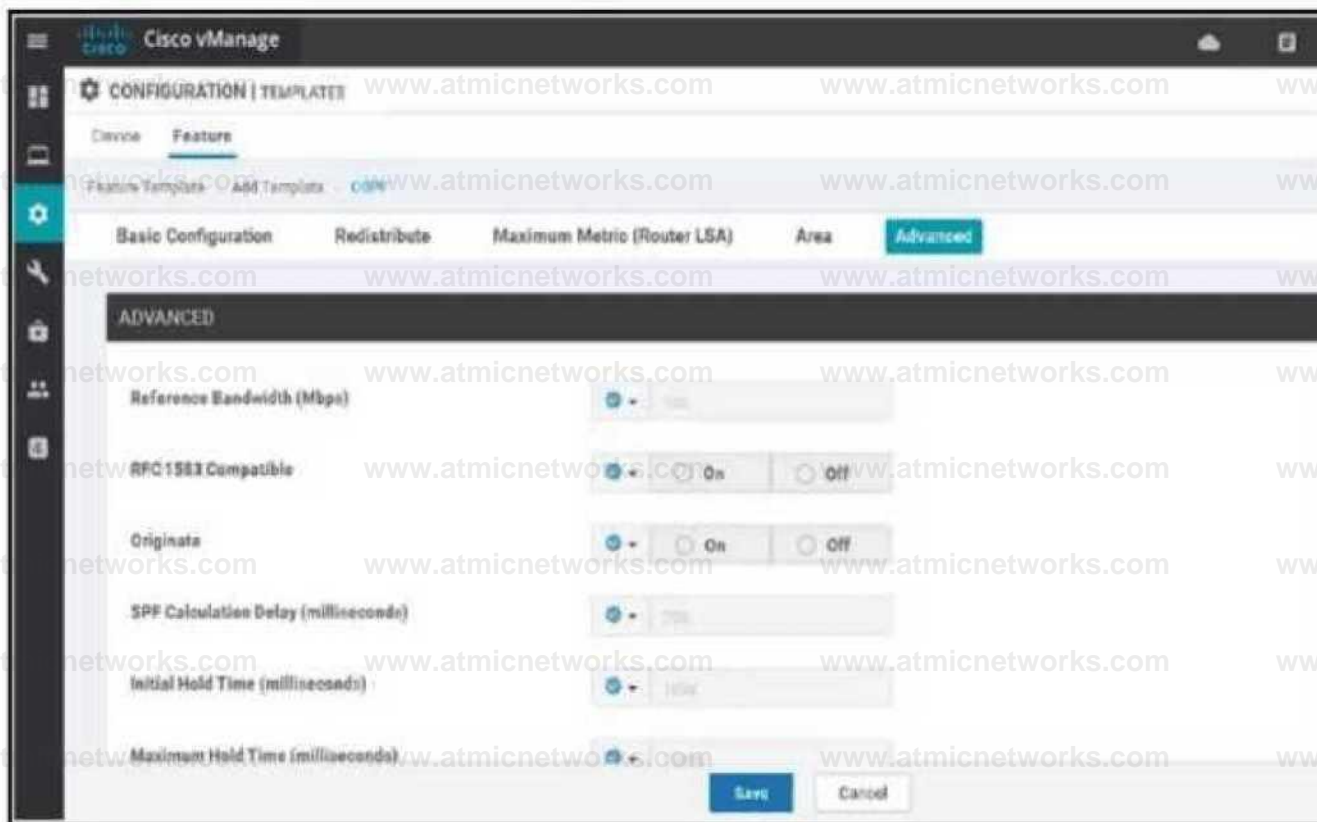
- A. OMP outside the DTLS/TLS control connection
- B. BGP inside the DTLS/TLS
- C. IPsec inside the DTLS/TLS control connection
- D. OMP inside the DTLS/TLS control connection

Answer: D

Explanation:

Question: 338

Refer to the exhibit.



Refer to the exhibit. A network administrator is configuring OSPF advanced configuration parameters from a template using the vManager GUI for a branch WAN Edge router to calculate the cost of summary routes to an ASBR. Which action achieves this configuration?

- A. Disable RFC 1583 Compatible
- B. Enable Originate
- C. Enable RFC 1M3 Compatible
- D. Disable Original

Answer: C

Explanation:

Question: 339

What is the result during a WAN Edge software upgrade process if the version of the WAN Edge software is higher than the one running on a controller device?

- A. The upgrade button is greyed out

- B. The upgrade proceeds with no warning message.
- C. The upgrade fails with a warning message
- D. The upgrade proceeds with a warning message

Answer: D

Explanation:

Question: 340

Refer to exhibit. An engineer is troubleshooting tear of control connection even though a valid CertificateSerialNumber is entered. Which two actions resolve Issue? (Choose two)

PEER	PEER	PEER	PEER	SITE	DOMAIN				LOCAL	REMOTE	REPEAT	REMOTE
INSTANCE	TYPE	PRIVATE	SYSTEM	IP	PUBLIC	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	REMOTE
COLOR	STATE	ERROR	ERROR	COUNT	DOWNTIME							
0	vpn	ssl	0.0.0.0	0	0	192.168.0.201	12345	192.168.0.201	12345	default	12345	12345
1	down	CERTIFICATE	ISSUE	5	2019-06-21T19:06:32+0200							

- A. Restore network reachability on the controller.
- B. Enter a valid serial number on the controller for a given device
- C. Enter a valid product ID (mode) on the PNP portal.
- D. Match the serial number file between the controller
- E. Remove the duplicate IP in the network

Answer: B,C

Explanation:

Question: 341

An engineer is configuring a data policy IPv4 prefixes for a site WAN edge device on a site with edge devices. How is this policy added using the policy configuration wizard?

- A. In vManage NMS select (he configure ► policies screen, select the centralized policy tab and click add policy
- B. In vBood orchestrator. select the configure > policies screen select the localized policy tab. and click add policy
- C. In vManage NMS. select the configure ► policies screen. select the localized policy tab- and click add policy
- D. In vSmart controller select tie configure ► policies screen, select the localized policy tab, and click add policy

Answer: C

Explanation:

Question: 342

Refer to the exhibit.

The screenshot shows a configuration panel with the following fields and values:

- Address Family:** A globe icon, a dropdown arrow, and radio buttons for **On** (selected) and **Off**.
- Address Family:** A globe icon, a dropdown arrow, and a text input field containing **ipv4-unicast** with a close 'X' button.
- Maximum Number of Prefixes:** A checkmark icon, a dropdown arrow, and a text input field.
- Route Policy In:** A checkmark icon, a dropdown arrow, and radio buttons for **On** and **Off** (selected).
- Route Policy Out:** A globe icon, a dropdown arrow, and radio buttons for **On** (selected) and **Off**.
- Policy Name:** A globe icon, a dropdown arrow, and a text input field containing **eBGP_Community_Policy**.

Refer to the exhibit The engineering must assign tags to 3 Of its 74 server networks as soon as they are advertised to peers These server network must not be advertised AS which configuration fulfil the requirement?

A)

policy

route-policy * BGPC cm munity ^Policy sequence 1 match

address C<xncommunity_Pr?fi>

action accept set

community 999 6 6000 no-advertise default action reject

lists

prefix-list Ccommunity_Prefix

Ip-prefix IC 20 20 0. 24

jp-prtfux 21 21.21 &24

ip-prrfi 22 22 22 0*24

B)

policy

route-policy 9GP_Community_PoHcy sequence 1 match

address Community^Preftx

action accept

set

community 999:65000 loeahas default action reject

lists

prefixes! Community Prefix

^prefix 20 2 0 20 0;24

p-prefn21 21 21 0.24

Ip-prefix 22 22 22 0,24

C)

policy

route-policy eOGP-Communniry-Policy sequence 1 match

addme Communnfy^Prefii

act or accept

Mt

community 991 6 5000 no-export

d<huf l action accept

lifts

prefix-lift Community_Prefix

Ip-prefix 20 20 20 0.24

Ip-prefix 21 21.21 0/24

^prefix 22 22 22 0 24

D)

policy

route-policy eBGP.Commumty _ Policy sequence 1

match

address Community .Prefix

action accept set

community 999 6 5000 no-adventa

default-action accept

lifts

prefixes! Comm unity .Prefix

ip-prefix 2C.20.20 0.24

ip-prefix 21.21.21 0:24

l f^ nr A A* 99 99 99 A 91

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation:

Question: 343

Which actions must be taken to allow certain departments to require firewall protection when interacting with data center network without including other departments? (Choose two.)

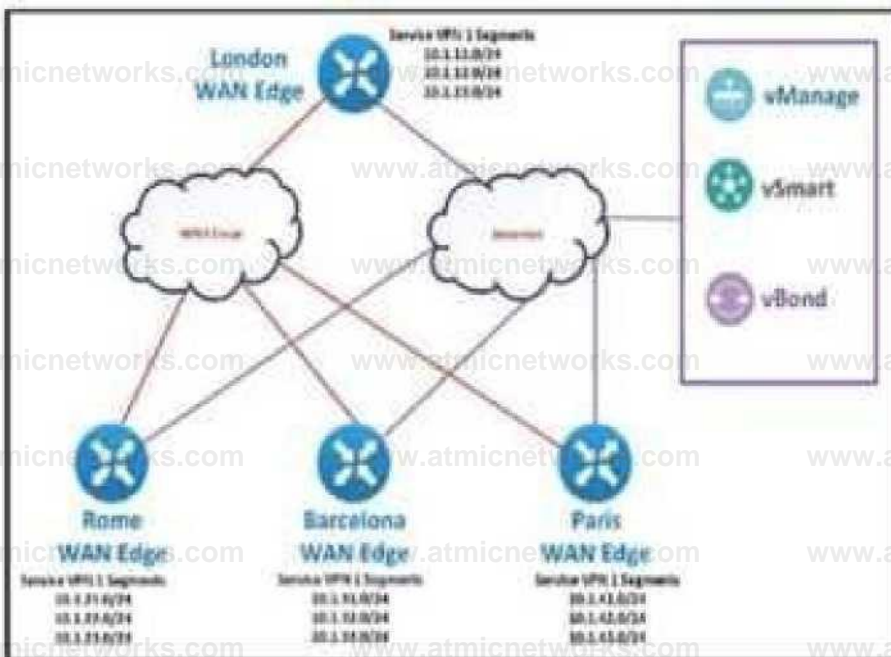
- A. Use classification policing and marking
- B. Apply data policies at vEdge.
- C. Deploy a service-chained firewall service per VPN
- D. The regional hub advertises the availability of the firewall service
- E. Advertise lo vSmart controllers

Answer: C,D

Explanation:

Question: 344

Refer to the exhibit.



The SD-WAN network is configured with a default full-mesh topology. The SD-WAN engineer wants the Barcelona WAN Edge to use MPLS TLOC as the preferred TLOC when communicating with Rome site. Which configuration must the

www.atmicnetworks.com www.atmicnetworks.com www.atmicnetworks.com www.atmicnetworks.com
www.atmicnetworks.com www.atmicnetworks.com www.atmicnetworks.com www.atmicnetworks.com
engineer use to create a list to select MPLS color toward the Rome TLOC?
A)

A)

Add Mesh Region

Name

Partial_Mesh

Description

Partial_Mesh

VPN List

ALL

Mesh Region Name

North

B)

Add Mesh Region

Name

Description

VPN List

Mesh Region Name

C)

Add Control Policy

 **TLOC**
Create a policy to apply to TLOCs

D)

Add VPN Membership Policy

VPN Membership Name

Site.to.Srte

Description

Site to. Site VPN List

Site List

VPN Lists

Spokes

ALL x

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 345

What problem happens on a device with two serial numbers, a unique device identifier (UDI), and secure unique device identifier (SUDI) when an engineer provisions ISR 4000 by PnP using only a UDI?

- A. It encounters spanning tree issues
- B. It faces interface buffer overflow patterns
- C. It encounters redirection problems.
- D. It encounters memory overload problems

Answer: D

Explanation:

Question: 346

Which type of connection is created between a host VNet and a transit VNet when configuring Cloud OnRamp for IaaS?

- A. Azure private endpoint
- B. GRE tunnel
- C. IPsec tunnel
- D. Azure peer link

Answer: C

Explanation:

Question: 347

How do WAN Edge devices operate when vSmart is inaccessible or fails to be reached by the WAN Edge?

- A. They cease to forward traffic in the data plane.
- B. They continue operation normally.
- C. They continue to receive reachability updates.
- D. They continue operating normally for a configurable time.

Answer: D

Explanation:

Question: 348

How is a TLOC uniquely identified from a WAN Edge router to the SD-WAN transport network?

- A. system IP address
- B. VPN ID
- C. OMP
- D. SD-WAN site ID

Answer: A

Explanation:

Question: 349

An engineer must apply the configuration for certificate installation to vBond Orchestrator and vSmart Controller. Which configuration accomplishes this task?

```
vpn 512 interface ath1 ip address 192.168.1.1 255.255.255.0 tunnel-mode interface allow-service netconf IM allow-service ntp no allow-service stun
```

```
vpn 0 interface eth1 ip address 140.1.1.1/28 tunnel-mode interface 8^hw allow-service ntp
```

```
vpn 512 interface eth1 ip address 1.1.1.1 255.255.255.0 tunnel-mode interface allow-service ntp allow-service natconf
```

```
vpn 0 interface s1/1/24 ip address 192.168.1.1 255.255.255.0 tunnel-mode interface allow-service ntp allow-service shutdown
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation:

Question: 350

What is the default value for the Multiplier field of the BFD basic configuration in vManage?

- A. 3
- B. 4
- C. 5
- D. 6

Answer: D

Explanation:

Question: 351

How is the software managed in Cisco SD-WAN?

- A. Software images must be uploaded to vManage through HTTP or FTP

- B. Software downgrades are unsupported for vManage
- C. Software images must be transferred through VPN 512 or VPN 0 of vManage
- D. Software upgrade operation in the group must include vManage, vBond, and vSmart.

Answer: B

Explanation:

Question: 352

An engineer creates a data policy to prevent communication from the 172.20.21.0/24 network to the 172.20.41.0/24 network. Which configuration accomplishes this task?

policy

lists

vpn-list VPN1

vpn 1

data-prefix-list LosAngeles-Net1

ip-prefix 172.20.21.0/24

data-prefix-list Rome-Net1

ip-prefix 172.20.41.0/24

data-policy FILTER-POLICY

vpn-list VPN1

sequence 1 match

source-data-prefix-list LosAngeles-Net1 action

drop i

sequence 11 match

source-data-prefix-list Rome-Net1

action drop

default-action accept

O policy lists vpn-list VPN1 vpn 1

**data-prefix-list LosAngeles-Net1 ip-prefix
172.20.21.0/24 data-prefix-list Rome-Net1 ip-
prefix 172.20.41.0/24**

**I data-policy FILTER-POLICY vpn-list VPN1
sequence 1 match**

**source-data-prefix-list LosAngeles-Net1
destination-data-prefix-list Rome-Net1 action
drop**

default-action accept

CJ policy lists vpn-list VPN1 vpn 1

!

**data-prefix-list LosAngeles-Net1 ip-prefix
172.20.0.0/16 data-prefix-list Rome-Net1 ip-prefix
172.20.0.0/16**

I data-policy FILTER-POLICY vpn-list VPN1

www.dumpsplanet.com TlldLn

O policy lists vpn-list VPN1 vpn 1

```
data-prefix-list LosAngeles-Net1 ip-prefix
172.20.21.0/24 data-prefix-list Rome-Net1 ip-
prefix 172.20.41.0/24
```

```
data-policy FILTER-POLICY vpn-list VPN1
sequence 1 match
```

```
source-data-prefix-list LosAngeles-Net1
destination-data-prefix-list Rome-Net1
action accept
! default-action drop
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

Question: 353

Which two protocols are supported for software image delivery when images are hosted on a remote server? (Choose two.)

- A. HTTPS
- B. SSL
- C. HTTP
- D. TFTP
- E. FTP

Answer: D,E

Explanation:

Question: 354

A company deploys a Cisco SD-WAN solution but has an unstable Internet connection. When the link to vSmart comes back up, the WAN Edge router routing table is not refreshed, and some traffic to the destination network is dropped. The headquarters is the hub site, and it continuously adds new sites to the SD-WAN network. An engineer must configure route refresh between WAN Edge and vSmart within 2 minutes. Which configuration meets this requirement?

**omp no shutdown graceful-
restart timers
eor-timer 120**

**omp
no shutdown
no graceful-restart**

**omp
no shutdown graceful-restart
timers
holdtime 120**

**omp
no shutdown
graceful-restart timers
advertisement-interval 120**

- A. Option A
- B. B
- C. Option B
- D.
- E. Option C
- F. Option D

Answer: A

Explanation:

Question: 355

Which controller is excluded from the process of checking against the authorized, allowed list?

- A. vBond
- B. PnP
- C. vSmart
- D. vManage

Answer: A

Explanation:

Question: 356

Refer to the exhibit.

```
vManage#show control local-properties
personality                vmanage
sp-organization-name       Cisco
organization-name         Cisco
system-ip                  10.1.1.10
root-ca-chain-status       Installed
certificate-status         Installed
```

Refer to the exhibit A vBond controller was added to the controller list with the same Enterprise Root CA certificate as vManage. The two controllers can reach each other via VPNO and share the same organization name, but the control connection is not initiated- Which action resolves the issue?

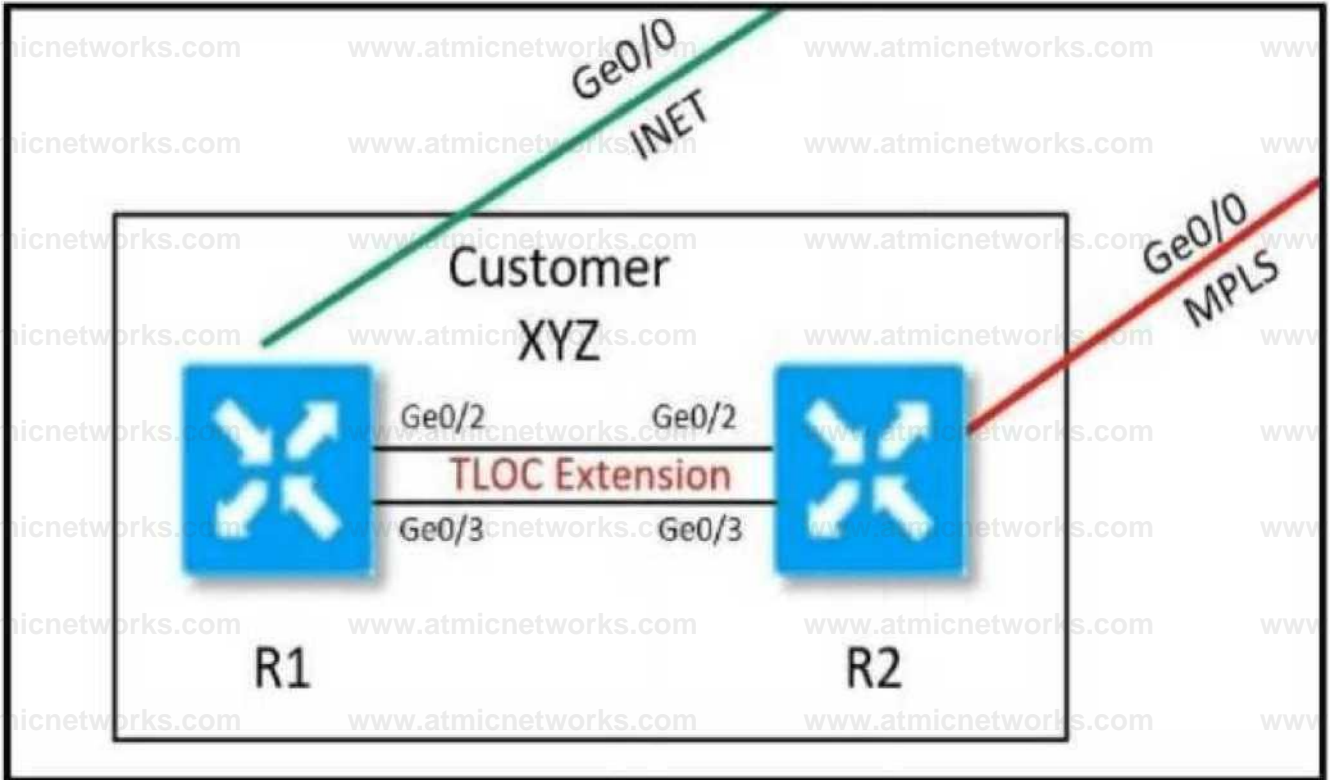
- A. Synchronize the WAN Edge list on vManage with controllers.
- B. Configure NTP on both controllers to establish a connection.
- C. Configure a valid system IP on the vBond controller.
- D. Configure a valid vBond IP on vManage.

Answer: D

Explanation:

Question: 357

Refer to the exhibit.



Customer XYZ cannot provision dual connectivity on both its routers due to budget constraints but wants to use both R1 and R2 interfaces for users behind them for load toward the hub site. Which configuration achieves this objective?

A)

R1

interface ge0/2 ip address
43.43.43.2/30 tloc-extension ge0/0

interface ge0/3 ip address
34.34.34.2/30 tloc-extension ge0/0

R2 interface ge0/2 ip address
43.43.43.1/30

interface ge0/3 ip address
34.34.34.1/30

B)

BI interface ge0'2 ip address
43.43.43.2/30 tloc-extension ge0/0

interface ge0/3 ip address
34.34.34.1/30 tunnel-interface color
mpls

R2

interface ge0/2 ip address
43.43.43.1/30 tunnel-interface

color public-internet

interface ge0/3 ip address

34.34.34.2/30 tunnel-interface

C)

R1

interface ge0/2 ip address

43.43.43.2/30 tunnel-interface ge0/0

interface ge0/3 ip address

34.34.34.2/30

• tunnel-interface ge0/0

R2

interface ge0/2

ip address 43.43.43.1/30 tunnel-

interface

color public-internet

interface ge0/3 ip address

34.34.34.1/30 tunnel-interface

color mpls

D)

R1

```
interface ge0/2 ip address
43.43.43.2/30
```

```
tloc-extension ge0'0
```

```
interface ge0/3 ip address
34.34.34.1/30 tunnel-interface color
mpls
```

R2

```
interface ge0/2 ip address
43.43.43.1/30 tunnel-interface
color public-internet
```

```
interface ge0/3 ip address
34.34.34.2/30 tloc-extension ge0/2
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 358

Which timer specifies information in the cache after all OMP sessions are lost at location S0123T4E56F78?

- A. advertisement interval
- B. EOR timer

- C. graceful restart timer
- D. hold time

Answer: C

Explanation:

Question: 359

Which encryption algorithm secures binding exchanges Between Cisco TrustSec SXP peers?

- A. SEAL
- B. 3DES
- C. AES
- D. MD5

Answer: C

Explanation:

Cisco TrustSec (CTS) is a technology that enables secure access and dynamic role-based access control in the network. The Security Group Tag (SGT) Exchange Protocol (SXP) is used to propagate SGTs across network devices. To ensure the secure exchange of these tags, Cisco uses encryption algorithms.

AES (Advanced Encryption Standard): AES is widely used in many security protocols and standards because of its strong encryption capabilities. In the context of Cisco TrustSec, AES is the encryption algorithm used to secure binding exchanges between SXP peers. It provides robust encryption, ensuring the integrity and confidentiality of the data being exchanged.

Implementation: When configuring SXP peers, the AES encryption ensures that the SGT information transmitted is secure and cannot be intercepted or tampered with by unauthorized entities.

Cisco TrustSec Configuration Guide

Cisco's official documentation on TrustSec SXP deployment

Question: 360

What is a key element used in a vBond Orchestrator redundancy topology?

- A. fully qualified domain name
- B. DHCP server
- C. load-balancer with health probes
- D. stun server

Answer: A

Explanation:

In Cisco SD-WAN architecture, the vBond Orchestrator plays a crucial role in the initial device onboarding and control plane security. Ensuring redundancy for vBond Orchestrators is essential for maintaining high availability and reliability in the SD-WAN network.

Fully Qualified Domain Name (FQDN): The use of an FQDN is a key element in vBond Orchestrator redundancy. By configuring multiple vBond Orchestrators with the same FQDN, the SD-WAN devices can resolve this domain name to different IP addresses corresponding to the different vBond Orchestrator instances. This allows for automatic failover and load balancing among the vBond Orchestrators.

Redundancy Mechanism: The DNS mechanism will resolve the FQDN to a list of IP addresses, and in case one vBond is unreachable, another can be contacted. This approach ensures continuous availability and redundancy without requiring manual reconfiguration of the devices.

Cisco SD-WAN Design Guide

Cisco SD-WAN Configuration and Deployment Guide

Question: 361

Which application list is preconfigured?

- A. Google_Apps
- B. Cisco Apps
- C. Microsoft_Office365
- D. P2P_Apps

Answer: C

Explanation:

In Cisco SD-WAN, application lists are used to identify and manage specific types of application traffic.

Preconfigured application lists are provided by Cisco to simplify the management and configuration of common applications.

Preconfigured Application Lists: Among the preconfigured application lists provided by Cisco SD-WAN, Microsoft_Office365 is one of them. This list helps in easily identifying and managing traffic related to Microsoft Office 365 applications.

Usage: These preconfigured lists can be used in policies to ensure optimized routing and performance for critical applications like Microsoft Office 365, which are widely used in enterprise environments.

Cisco SD-WAN Application-Aware Routing Configuration Guide

Cisco SD-WAN Policy Framework Documentation

Question: 362

What does forward error correction addresses in Cisco SO-WAN?

- A. inefficient traffic forwarding caused by inbound shapers
- B. reduced application performance degradation rotated to service degradation
- C. applications with occasional invalid data input and poor performance
- D. traffic flows with increased delay over a particular transport

Answer: B

Explanation:

Forward Error Correction (FEC) is a technique used in networking to enhance data reliability and performance, particularly over unreliable or lossy networks.

Forward Error Correction (FEC): In Cisco SD-WAN, FEC helps in mitigating the effects of packet loss and service degradation by encoding redundant data, which can be used to reconstruct lost packets. This ensures that even if some packets are lost during transmission, the data can still be accurately reconstructed at the destination.

Addressing Performance Degradation: FEC specifically addresses reduced application performance degradation caused by packet loss and network impairments. By providing this error correction capability, FEC helps maintain the performance and reliability of critical applications over potentially unstable network paths.

Cisco SD-WAN Security and Quality of Service Configuration Guide Cisco SD-WAN Forward Error Correction Technical Whitepaper

Question: 363

What are the two components of an application-aware firewall? (Choose two.)

- A. zone pair
- B. sequence
- C. lists
- D. default action
- E. sequence action

F. firewall policy

Answer: B,D

Explanation:

An application-aware firewall in Cisco SD-WAN provides advanced security by allowing policies to be defined based on specific applications and their behaviors.

Sequence: In the context of an application-aware firewall, a sequence defines the order in which firewall rules

are evaluated. Each sequence can contain match conditions and corresponding actions to be taken if the conditions are met.

Default Action: The default action is a crucial component that specifies what action to take if none of the defined sequences match the traffic. This ensures that there is always a fallback action to handle unmatched traffic, providing a safety net for security policies.

Cisco SD-WAN Security Policy Configuration Guide
Cisco SD-WAN Firewall Policy Documentation

Question: 364

What is vBond reachability resolved by vManage?

- A. OMP
- B. DNS
- C. BGP
- D. IPsec

Answer: B

Explanation:

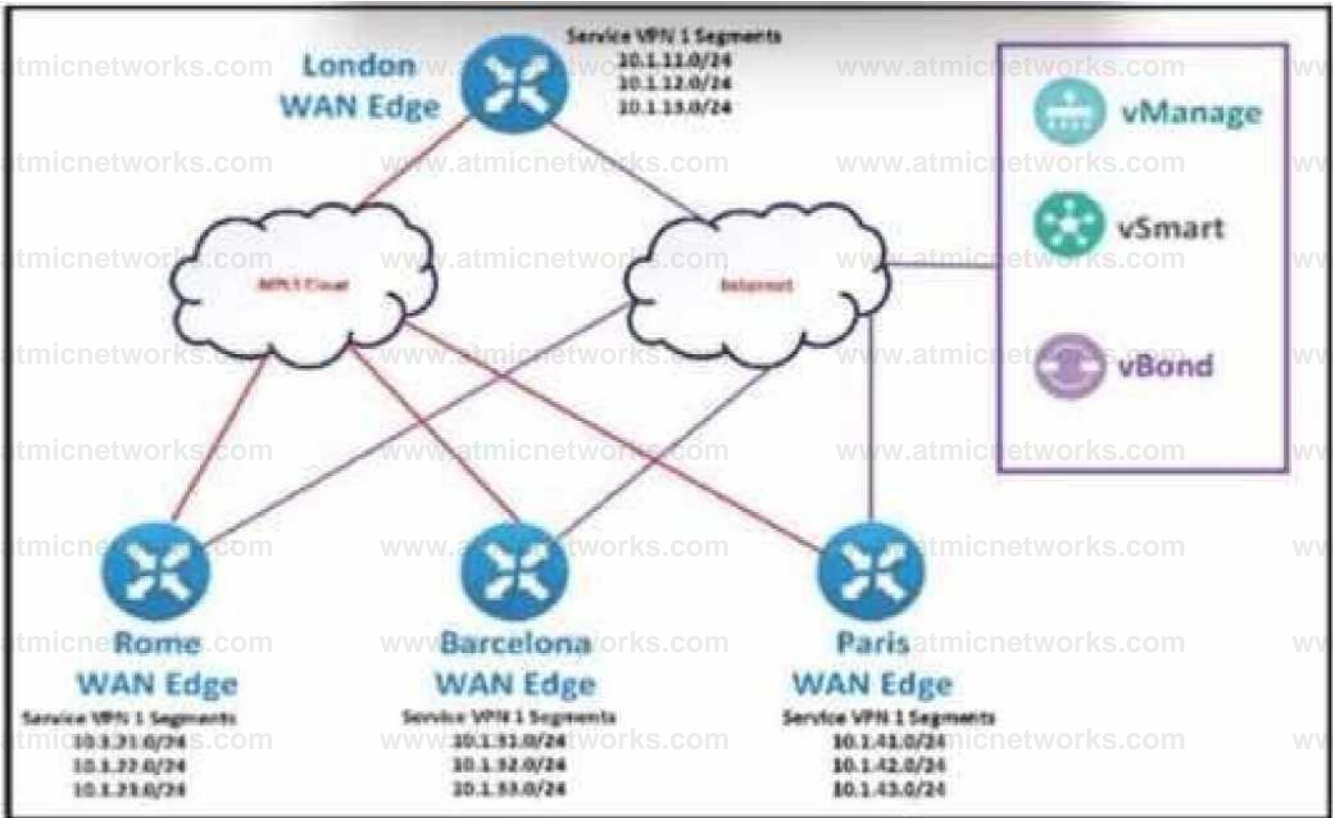
The vBond Orchestrator in Cisco SD-WAN is responsible for authenticating and orchestrating connectivity between the SD-WAN edge devices (vEdge routers) and the vManage and vSmart controllers. The reachability of vBond is crucial for the initial device onboarding and ongoing operations.

DNS (Domain Name System): vManage resolves the vBond reachability using DNS. By using a Fully Qualified Domain Name (FQDN) for the vBond orchestrator, the system can dynamically resolve the vBond's IP address, which allows for flexibility in managing the vBond's location and redundancy. Functionality: When a new edge device comes online, it contacts the vBond orchestrator using its FQDN. DNS resolution translates this FQDN into an IP address, allowing the device to establish a secure connection.

Cisco SD-WAN Deployment Guide
Cisco SD-WAN vBond Orchestrator Configuration Guide

Question: 365

Exhibit.



The SD-WAN network is configured with a default full-mesh topology. The network engineer wants the Rome WAN Edge to use the MPLS TLOC as the preferred TLOC when Telnet traffic as long as the MPLS link has these characteristics:

Loss: 5%

Latency: 100ms

Jitter: 100 ms

Which configuration must the network engineer use to create a list that classifies the MPLS link characteristics?

A)

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN

B)

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN

C)

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN

D)



A. Option B. Option C. Option D. Option

Answer: C

Explanation:

Configuration Analysis: The configurations provided in the images must be evaluated to determine which option correctly classifies the MPLS link based on the given criteria of loss, latency, and jitter. Preferred TLOC Configuration: The network engineer needs to configure the SD-WAN policy to prefer the MPLS transport for Telnet traffic, ensuring the link characteristics match the specified thresholds. Reference:

Cisco SD-WAN Policy Configuration Guide
 Cisco SD-WAN Transport and TLOC Configuration Guide

Question: 366

What is the advantage of instating the controller on-premises?

- A. ease of deployment and management
- B. full control of the data piano and the control plane
- C. automatic geographical redundancy and security

D. scalability and a cost-saving

Answer: B

Explanation:

Deploying the SD-WAN controller on-premises offers several advantages, particularly in terms of control and customization.

Full Control of the Data Plane and the Control Plane: When the controller is deployed on-premises, the organization maintains complete control over both the data plane (traffic forwarding) and the control plane (network management and configuration). This allows for more granular control over network policies, security configurations, and performance optimizations.

Customization and Security: On-premises deployment allows organizations to customize their SD-WAN setup to meet specific security and compliance requirements. Sensitive data remains within the organization's control, which can be crucial for industries with strict data privacy regulations. **Operational Flexibility:** Having the controller on-premises provides operational flexibility, enabling organizations to integrate the SD-WAN solution with existing network management tools and processes.

Cisco SD-WAN Deployment Guide

Cisco SD-WAN On-Premises Controller Configuration Documentation

Question: 367

An application team is getting ready to deploy a new business-critical application to the network. To protect the traffic, the network team must add another queue to the QoS map and then deploy the map to fabric

Which configuration step must be completed prior to adding the queue to the QoS map and applying it?

- A. The relationship between the new QoS class and the hardware queue must be configured from the 'lists' page of the Local Policy section of vManage. The QoS map is then applied to the WAN interface.
- B. The relationship between the new QoS class and the hardware queue must be configured from the 'lists' page of the Local Policy section of vManage. The QoS map is then applied to the serviceside interface.
- C. The relationship between the new QoS class and the hardware queue must be configured from the "lists" page of the Centralized Policy section of vManage. The QoS map is then applied to the WAN interface.
- D. The relationship between the new QoS class and the hardware queue must be configured from the "lists" page of the Centralized Policy section of vManage. The QoS map is then applied to the serviceside interface.

Answer: A

Explanation:

Adding a new QoS queue to handle business-critical application traffic involves several specific steps in Cisco SD-WAN's vManage:

Configure QoS Class and Hardware Queue Relationship:

Navigate to the 'lists' page within the Local Policy section of vManage.

Define the relationship between the new QoS class and the appropriate hardware queue. This step is crucial as it ensures that the new traffic class is mapped correctly to the underlying hardware resources, which are responsible for enforcing the QoS policies.

Applying the QoS Map:

Once the new QoS class and hardware queue relationship is configured, the updated QoS map must be applied to the relevant interfaces.

Specifically, the QoS map should be applied to the WAN interface. This ensures that the new QoS policies are enforced on the traffic as it traverses the WAN, which is typically where QoS management is most critical due to bandwidth constraints and variable network conditions.

- Cisco SD-WAN Quality of Service Configuration Guide
- Cisco SD-WAN vManage Policy Configuration Documentation

Question: 368

DRAG DROP

Drag and drop the alarm slates from the left onto the corresponding alarm descriptions on the right.

Critical (Red)	events that might diminish performance of network
Major (Yellow)	events that impair overlay network function
Medium (Blue)	events that affect operation of network function
Minor (Green)	events that might impair performance of network

Answer:

Explanation:

- Critical (Red): events that impair overlay network function
- Major (Yellow): events that might impair performance of network
- Medium (Blue): events that affect operation of network function
- Minor (Green): events that might diminish performance of network

Critical (Red): These are the highest severity alarms indicating events that can cause significant impairment to the overlay network's functionality. Immediate attention is required to prevent major network issues.

Major (Yellow): These alarms indicate events that could potentially impair network performance.

They are serious but not as critical as red alarms. They need prompt attention to prevent degradation in network performance.

Medium (Blue): These alarms are of medium severity and indicate events that affect the operation of the network function. They are important but do not require immediate action.

Minor (Green): These are the lowest severity alarms and indicate events that might diminish network performance. They are more informational and do not typically require urgent action.

- Cisco SD-WAN Monitoring and Troubleshooting Guide
- Cisco vManage Alarm Severity Levels Documentation

Question: 369

Which VPNs must be configured outside the workflow to complete the SD-WAN overlay setup when using the Quick Connect workflow?

- A. service and transport VPNs
- B. service VPNs
- C. transport VPNs
- D. management VPNs

Answer: D**Explanation:**

The Quick Connect workflow in Cisco SD-WAN simplifies the initial setup process by automating many configuration steps. However, certain configurations still need to be performed outside of this automated workflow to ensure a complete and operational SD-WAN overlay.

Management VPNs: Management VPNs, specifically VPN 512, are used for device management and are critical for the proper operation and management of the SD-WAN devices. These VPNs are typically configured outside of the Quick Connect workflow to ensure that all devices can be properly managed and monitored.

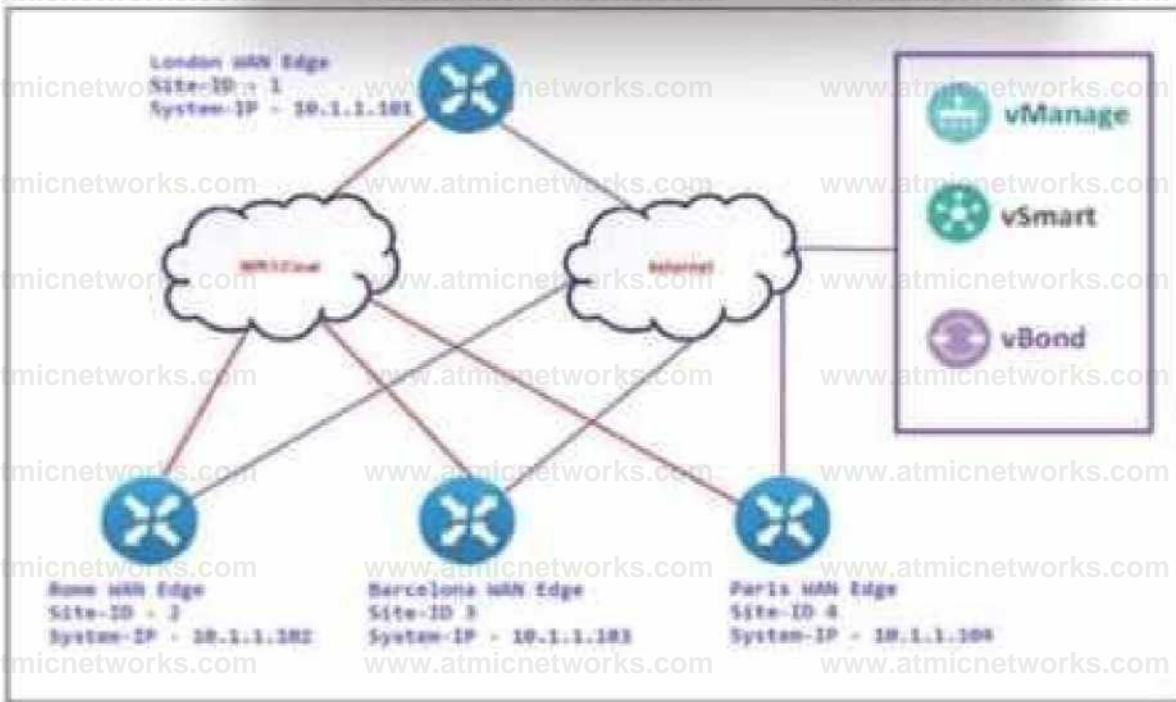
Service and Transport VPNs: While service and transport VPNs are also important, they are often included within the Quick Connect workflow, which sets up the necessary configurations to enable data transport across the SD-WAN fabric.

Cisco SD-WAN Quick Connect Guide

Cisco SD-WAN Management and Monitoring Guide

Question: 370

Refer to the exhibit.



An engineer configures Rome WAN Edge 10 use MPLS cloud as the preferred link to reach Paris WAN Edge and use biz-internet as a backup. Which policy configuration must be led in the outbound direction toward Rome to accomplish the task?

- A)


```

policy
lists
tloc-l is* TLOC-1
tloc 104.1 102 color nipsis encaps ipwc preference 500
Hoc 10.1.1.102 color biz-internet tncap ipsec preference 400
            
```
- B)


```

policy
Hals
Uccdist TLOC4
tloc 10.1.1.103 color mpls encaps ipsec preference 500
tloc 10.1.1.103 color biz-internet encaps ipsec preference 400
            
```
- C)


```

policy
lists
tioc&t TLOC-1
tloc 10.1.1.101 color mplsencap ipset preference 500
Hoc 10 1 1 101 color brz-internet encaps ipwe presence 400
            
```
- D)


```

policy
lists
rlqc ■l rat TLOC 4
tloc 10.1.1.104 color mptt encaps ipsec preference Soo
tloc 104.14 04 color Hz-^temtl encaps ipsec preference 400
            
```

- A. Option A B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

To configure Rome WAN Edge to prefer the MPLS cloud for reaching Paris WAN Edge, and use bizinternet as a backup, the policy must be set correctly to define the preference for each transport link. Understanding TLOCs (Transport Locator): TLOCs represent the transport network paths (MPLS, Internet, etc.) available for SD-WAN. The preference values assigned to TLOCs determine their priority. A lower preference value indicates a higher priority.

Policy Configuration Analysis:

Option A: This option correctly configures the TLOC list for the system IPs representing the MPLS and biz-internet links with the appropriate preferences (500 for MPLS and 400 for biz-internet).

Other options either repeat the TLOC configuration incorrectly or reference wrong system IPs.

Policy Configuration:

```
policy
```

```
lists
```

```
tloc-list TLOC-1
```

```
tloc 10.1.1.102 color mpls encap ipsec preference 500
```

```
tloc 10.1.1.102 color biz-internet encap ipsec preference 400
```

Cisco SD-WAN Policy Framework Guide

Cisco SD-WAN Transport Locator Configuration Documentation

Question: 371

What do receivers request to join multicast streams in a Cisco SO-WAN network?

- A. IGMP membership reports directly with a multicast router.
- B. Multicast service routes with the vSmart controller
- C. IGMP membership reports directly with the vBond orchestrator.
- D. PIM messages with the nearest neighboring multicast router.

Answer: B

Explanation:

In a Cisco SD-WAN network, multicast traffic management is handled differently compared to traditional IP multicast methods due to the nature of the overlay architecture.

Multicast Service Routes: In Cisco SD-WAN, multicast receivers use the vSmart controller to request multicast streams. This is done via multicast service routes which the vSmart controller manages. The vSmart controller is responsible for maintaining and distributing multicast routing information to all

edge devices in the network.

Process:

When a multicast receiver wants to join a multicast stream, it sends an IGMP join request.

The WAN Edge device forwards this request to the vSmart controller.

The vSmart controller then updates the multicast service routes to include the new receiver, ensuring that multicast traffic is appropriately forwarded to the joining receiver.

Cisco SD-WAN Multicast Configuration Guide

Cisco SD-WAN vSmart Controller Documentation

Question: 372

Which control policy assigned to Drenches in the out direction establishes a strict hub-and-spoke topology for VPN2?

A)

```
policy »M*
vpn OBI VPH2
vpn 2
```

```
Bit* .Not huh_ah»s sita-d 1-2 r
```

```
control policy Vpn_niulU topo'oro lequancB 10
match route D'ui Pal huQ-Hre^ «n.ji5t WMJ
```

```
action accept
```

```
M^MM* 34 match
route vpn fatvHia
```

```
action rw|Kt
default ncnon acc-ept
```

B)

```
policy lists vpn-Ust VPN? vpn 2
```

```
site-list hub_sites
Bite-id 1*2
```

```
cenwoFfjoiEty vpn_multi-topology sequence 10
match route
site-list brjncii .sites
```

```
vpn-list VPN2 '
```

```
action accept
set
tlcc 1.1.1.1 color mi
```

```
default-action accept
```

C)

```
policy
hats
vpn-l
```

```
vpn bl VPN2
```

```

1 2
site-lts
site-ict hub_sites
1 1-2

contra
sequel-policy vpn.multi-topology
matchlnc 10
site-h route
vpiHist hub_slts
! ikstVPN2
aetEOI
1 1 accept
aeqiH
matinee 20
1 h route actio
l n reject
defauT f-action accept

D)
policy Eiets
vpn-li<.t VPN2
vpn 2
ti^list brane fifties
site-id 1-100

contra l-policy vpn_muH!-topo1ogy
sequence 10
march route
■ft»4at br^neh +it»*
^iHitfVPNi '

action accept
*at
Ucc 100.1.1.1 color mpls t
l

defiulbKtlon accept
    
```

- A. Option
- B. Option
- C. Option
- D. Option

Answer: A

Explanation:

To establish a strict hub-and-spoke topology in Cisco SD-WAN for a specific VPN, such as VPN2, a control policy must be configured. This control policy dictates how traffic flows between sites, ensuring that all branch traffic is routed through the hub site.

Control Policy Components:

Site Lists: Define which sites are considered hubs and which are branches.

VPN Lists: Identify the VPNs to which the policy applies.

Control Policy: Use sequences to match routes and specify actions to accept or reject traffic based on the defined topology.

Policy Analysis:

Option A: Correctly defines site lists for hub sites (site-id 1-2) and creates a control policy that matches routes for VPN2, accepting routes from hub sites and rejecting routes from others. This ensures that traffic from branches (other sites) is only accepted if it routes through the hubs.

Other options either incorrectly define the site lists or do not properly match and set the routes to enforce the strict hub-and-spoke topology.

Policy Configuration:

policy

lists

```

vpn-list VPN2
vpn 2
site-list hub_sites
site-id 1-2
!
control-policy vpn_multi_topology
sequence 10
match route
site-list hub_sites
vpn-list VPN2
!
action accept !
sequence 20
match route
vpn-list VPN2 !
action reject !
default-action accept
    
```

Cisco SD-WAN Control Policy Configuration Guide
 Cisco SD-WAN Hub-and-Spoke Topology Deployment Guide

Question: 373

Which configuration allows VPN 10 traffic to have direct internet access locally from the WAN Edge device?

A)

```

p^y
mwbcf^M
vpn-Ad vpnio
MMjmHir.e IQ t
acton ancaut
ato M**A*pn •
otokjcaeton aeeapt
1
cfkw^terhfMala CRjQWD

bah
ton-M vpn 10
    
```

```

vpi ID.T
*to-kJ lfcawto
itoaj 14
t
apply-policy
hto-M Rarncaa dau-cM*eT DPI
honv-wv«« .*v*-a ta'iaMfB
C^LOrtD
    
```

```

ton 10
p rouijOOGtH) .pri y
    
```

B)

```

policy
data-policy DPI
vpn-list vpn10
sequence 10
  action accept
  default-action accept
  cflowd-template CFLOWD
lists
  vpn-list vpn10

vpn 10
  site-list Remote
  site-id 14
  apply-policy
  site-list Remote
  data-policy DPI from-service
  cflowd-template CFLOWD

vpn 0
  ip route 0.0.0.0/0 vpn 10
    
```

C)

```

pnir>
-'Jilt j-pau'. ■ DPI
vf#f-Q4 vpnIQ
*)JW** to T
  •coon arap

Jeijt-i't jcliun.

dlc*a-WHpiaw C FI M)

uta
tftHM vpn 10

vln -tn' RD TDln
  t*d 10

<0M»*Bf
E?tD-41I Rarn-|W
1«t* pt^~^j DPI taMt-MftMfl
dtaM>«*ttMta CROWD

¥pi ID
13 F&JfB D 0 CJ CH) rpr D
    
```

D)

```

policy
data-policy DPI
vpn-list vpn10
sequence 10
  action drop
  default-action accept
  cflowd-template CFLOWD
lists
  vpn-list vpn10

vpn 10
  site-list Remote
  site-id 14
  apply-policy
  site-list Remote
  data-policy DPI from-service
  cflowd-template CFLOWD

vpn 0
  ip route 0.0.0.0/0 vpn 10
    
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

To allow VPN 10 traffic to have direct internet access locally from the WAN Edge device, the configuration must ensure that the traffic is routed correctly and that NAT (Network Address Translation) is

applied to allow the traffic to exit to the internet.

Policy Configuration:

NAT Use: The configuration should include a directive to use NAT for the specific VPN (VPN 10 in this case). This ensures that the traffic originating from VPN 10 can be translated and routed to the internet.

Apply Policy: The policy should be applied in the outbound direction to the appropriate interface that connects to the internet.

Option A Analysis:

This option includes the nat use-vpn 0 directive, which instructs the system to use NAT for traffic in VPN 10, allowing it to access the internet directly.

The apply-policy command is correctly used to apply the policy to the site list and the data-policy DPI from-service.

Cisco SD-WAN NAT Configuration Guide

Cisco SD-WAN Direct Internet Access (DIA) Configuration Documentation

Question: 374

Which TLOC color is used for site-to-site communication in a Google Cloud integration with Cisco SD- WAN?

- A. Private1
- B. private2
- C. private3
- D. private4

Answer: A

Explanation:

In Cisco SD-WAN, TLOC (Transport Locator) colors are used to categorize and manage different types of transport networks. When integrating with cloud services such as Google Cloud, specific TLOC colors are designated for managing site-to-site communication within the cloud infrastructure.

TLOC Color Assignment:

For Google Cloud integration, Cisco SD-WAN uses specific TLOC colors to differentiate between various types of transport links and to ensure that traffic is routed appropriately between sites. **Private1 for Site-to-Site**

Communication:

The TLOC color private1 is specifically used for site-to-site communication within Google Cloud. This ensures that the traffic between different sites within the Google Cloud infrastructure is managed efficiently and securely.

Cisco SD-WAN Cloud Integration Guide

Cisco SD-WAN Google Cloud Configuration Documentation

Question: 375

Which data policy configuration influences BGP routing traffic flow from LAN to WAN?

- A)

PAAf

HMfiiMmiM 3GP-AS-PREFER

Mqu«fico W

□choc accept

Mt

AI path prepend 10, 20

ilttEMill-acton accept

vpn 10

RHA*

KHitKn^ty BOAS-PREPENO r

B)

policy

rcutv-Khty &&P-AS-PREPENP

sequence 10 acton tony w<

aMMth p<<wnd 10 20

dotautt-acton accept

vpn 10 ipm<

bOP

rwW pt*,j B&AS-FRERE NO <xrt

C)

poicy

route-policy BGP-A5-FREPENO

Mqwn 10 acton accept vet

at pnin cetypenti 10, JU

datiuii'Aoton accept

vpn 10 nxMr tv

D)

```

policy
  route-policy BGP-AS-PREPEND
  sequence 10
  action accept
  set
    as-path prepend 10, 20
  !
  default-action accept

vpn 10
router
  bgp
    route-policy BG-AS-PREPEND in

```

A. Option A B. Option B C. Option C D. Option D

Answer: C**Explanation:**

In Cisco SD-WAN, data policies can influence the routing traffic flow, particularly when using BGP (Border Gateway Protocol) to manage the traffic from the LAN to the WAN. This involves route manipulation techniques such as AS-path prepending to influence path selection.

AS-Path Prepending:

AS-path prepending is a technique used to manipulate the path selection process in BGP. By adding extra AS numbers to the AS-path attribute, you make a particular route less preferred.

This can be useful in directing traffic to take a different path by making certain routes appear longer.

Option C Analysis:

Policy Definition: The policy named BGP-AS-PREPEND includes a sequence that sets the AS-path to prepend the AS numbers 10 and 20.

Application: The policy is applied in the outbound direction of BGP, which means it will influence the BGP routes being advertised from the LAN to the WAN.

This ensures that the traffic flow from the LAN to the WAN is influenced by the AS-path prepending, making certain paths less preferred.

Cisco SD-WAN Routing Configuration Guide

Cisco SD-WAN BGP Policy Configuration Documentation

Question: 376

Customer has two branch silos with overlapping IPs How must the data policy be configured to establish communication between the sites and server to avoid overlapping?

A)


```

policy data-policy Svc_Plane_NAT
  vpn-list VPN2
  sequence 10
  match source-ip 10.0.0.1/32
  action accept
  nat pool 1
  default-action accept
  vpn 2
  interface natpool1
  ip address 192.168.1.1/32
  no shutdown

```

B)

```

policy data-policy Svc_Plane_NAT
  vpn-list VPN1
  sequence 10
  match source-ip 10.0.0.1/32
  action accept
  nat pool 1
  default-action accept

```

C)

```

policy data-policy Svc_Plane_NAT
  vpn-list VPN1
  sequence 10
  match source-ip 10.0.0.1/32
  action accept
  nat pool 1
  default-action accept

```

D)

```

policy data-policy Svc_Plane_NAT
  vpn-list VPN1
  sequence 10
  match source-ip 10.0.0.1/32
  action accept
  nat pool 1
  default-action accept

```

A. Option A

B. Option B C. Option C D. Option D

Answer: A**Explanation:**

When dealing with overlapping IP addresses in different branch sites, it's crucial to use NAT (Network Address Translation) to avoid IP conflicts and establish proper communication.

NAT Configuration:

Source NAT: This involves translating the source IP addresses of the packets as they leave a specific interface.

This can help avoid IP conflicts by ensuring that the IP addresses used within the network are unique.

Data Policy: A data policy must be created that matches the source IP addresses and applies the NAT pool to translate these addresses.

Option A Analysis:

Policy Definition: The data policy `Srvc_Plane_NAT` includes a sequence that matches the source IP `10.0.0.1/32` and accepts the action to apply NAT using `nat pool 1`.

Interface Configuration: The interface `ge0/0/0` is configured with the IP address `192.168.1.1/32` and is not shut down, ensuring it is active and can handle the NAT translation.

Cisco SD-WAN NAT Configuration Guide

Cisco SD-WAN Data Policy Configuration Documentation

Question: 377

Which two architectural components are part of an SD-WAN high availability vManage cluster? (Choose two.)

- A. WAN Edge router
- B. network configuration system
- C. NAT router
- D. messaging server
- E. application server

Answer: D,E**Explanation:**

In a Cisco SD-WAN high availability (HA) vManage cluster, several components work together to ensure redundancy and availability. The vManage cluster is responsible for network management and configuration and consists of multiple servers that handle different functions.

Application Server: This server handles the core functionalities of vManage, including processing user requests, managing configurations, and executing policies. In an HA setup, multiple application servers work together to provide redundancy and load balancing.

Messaging Server: The messaging server is responsible for inter-server communication within the cluster. It ensures that configuration changes, policy updates, and other important messages are propagated across all vManage servers in the cluster.

These components work in tandem to maintain the operational integrity and availability of the vManage system in an HA configuration.

Cisco SD-WAN vManage Cluster Deployment Guide
Cisco SD-WAN High Availability Configuration Documentation

Question: 378

What is a requirement for deployment of on-premises vBond controllers through the Cisco Plug and Play Connect process?

- A. a DNS name that identifies vBond
- B. a defined controller profile
- C. Internet connectivity from vManage
- D. a CSV The that contains all controllers

Answer: A

Explanation:

Deploying on-premises vBond controllers through the Cisco Plug and Play Connect process requires specific configurations to ensure proper identification and communication between the controllers and the devices.

DNS Name: A DNS name that identifies the vBond orchestrator is crucial. This DNS name allows devices to dynamically resolve the IP address of the vBond orchestrator. This is especially important in environments where IP addresses may change, ensuring that devices can always reach the vBond orchestrator through its DNS name.

Process:

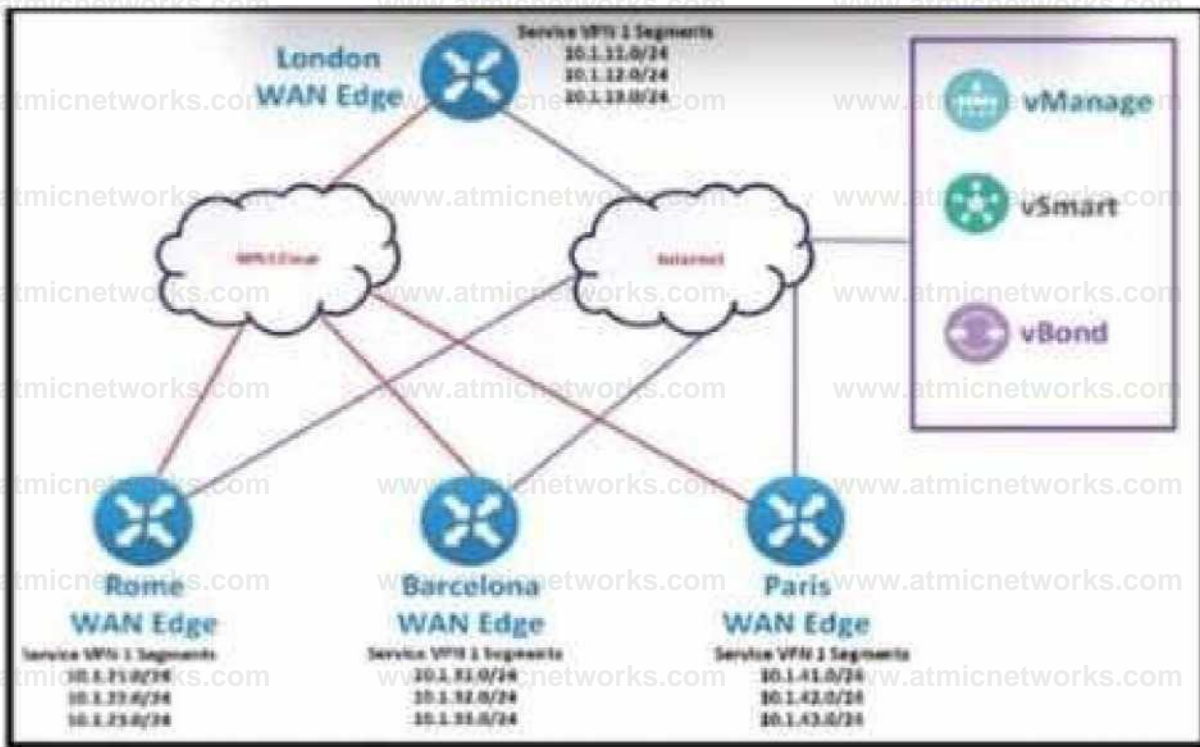
When a device comes online, it contacts the Plug and Play server to get the necessary information for connecting to the SD-WAN fabric.

The DNS name is used to resolve the vBond's IP address, enabling secure and reliable communication between the device and the vBond orchestrator.

Cisco SD-WAN Plug and Play Connect Deployment Guide
Cisco SD-WAN vBond Orchestrator Configuration Documentation

Question: 379

Exhibit.



The SD-WAN network is configured with a default full-mesh topology. An engineer wants Barcelona and Paris to communicate to each other through the London site using a control. Which control policy configuration accomplishes the task?

A)



B)



C)



D)



A. Option A B. Option B C. Option C D. Option D

Answer: A

Explanation:

To achieve communication between Barcelona and Paris through the London site, a control policy needs to be configured to force traffic from these two sites to pass through the London site. This setup involves manipulating the routing information such that London becomes a transit hub for traffic between Barcelona and Paris.

Understanding the Policy Requirements:

Centralized Policy: This type of policy is applied at the controller level and affects multiple devices in the SD-WAN fabric. It allows the control of routing behavior across the entire network.

Route Policy: Specifically, a route policy will be used to set the preferred path for traffic between sites, ensuring that it passes through London.

Option Analysis:

Option A: Shows the configuration of a centralized policy with a focus on route policy, which is necessary to achieve the desired traffic flow manipulation.

Other Options: Do not provide the necessary centralized policy or route policy configurations that are needed to control the routing paths between the sites.

Configuration Details:

Centralized Policy: Define the policy under the centralized policy section in the vManage GUI.

Route Policy: Create and apply a route policy that specifies the desired routing behavior for traffic between Barcelona and Paris, ensuring it routes through London.

Cisco SD-WAN Control Policy Configuration Guide
 Cisco SD-WAN Centralized Policy Documentation

Question: 380

What is the function of colocation in Cloud OnRamp SaaS?

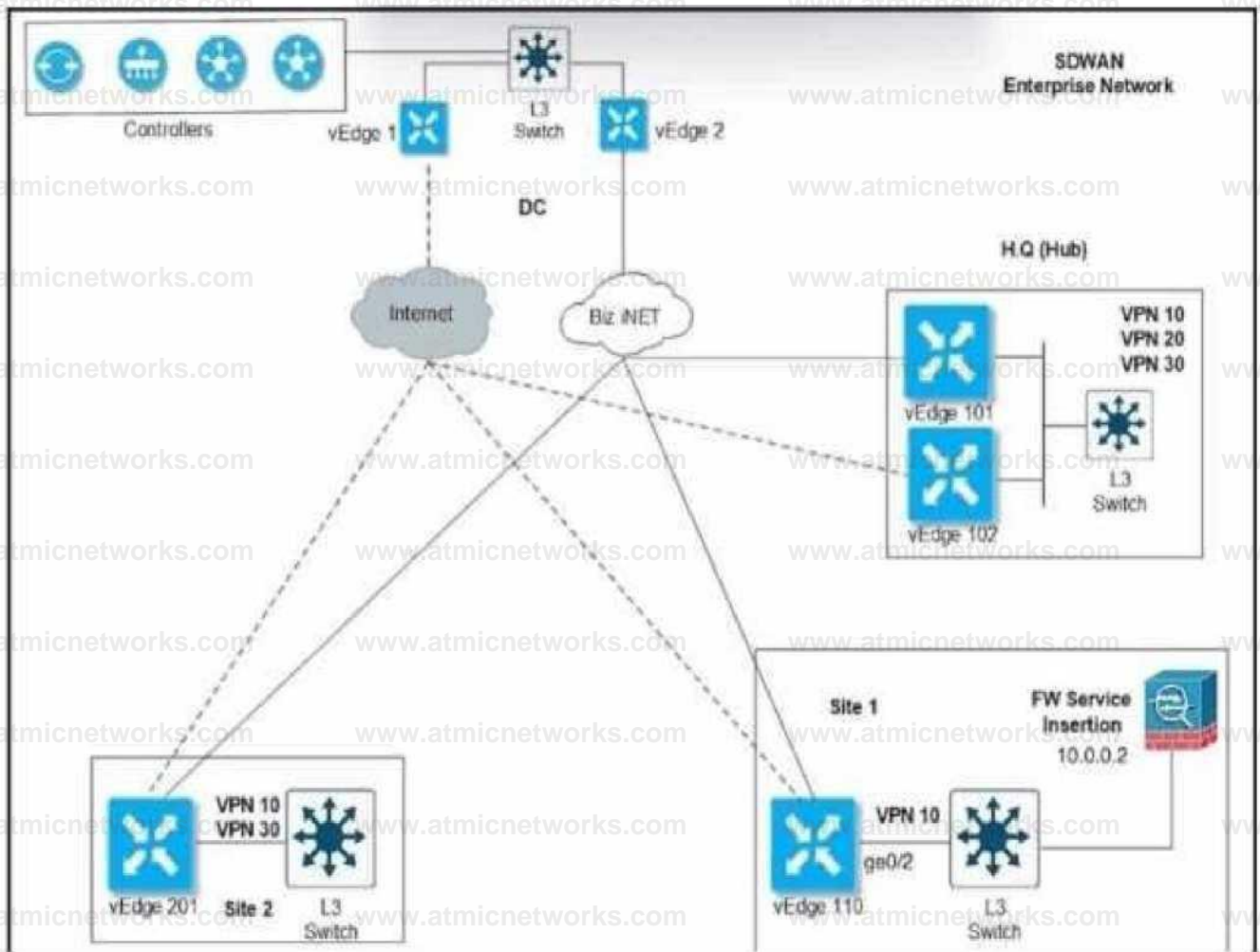
- A. Cloud OnRamp incorporates regional colocation facilities by choosing between cloud access points at the remote site and regional cloud access points at the colocation facilities.
- B. The Cloud OnRamp for colocation solution restricts the creation of different VNF service chains orchestrated in Cisco vManage and deployed on a cluster in a colocation facility.
- C. In Cloud OnRamp, colocation supports the capability of virtualizing access-only locations and using colocation centers that require the customer to extend to the cloud.
- D. With colocation facility in Cloud OnRamp, the customer faces challenges to virtualize the security and optimization infrastructure that influence traffic through network elements.

Answer: D

Explanation:

Question: 381

Refer to the exhibit.



Refer to the exhibit. A customer wants to deploy service insertion at site1. Which traffic from VPN 10 must route to this site through a firewall. A policy must be in place to route VPN 10 traffic from all sites toward this firewall. Which configuration must be on the vSmart controller to meet this requirement?

A.

```

policy
lists
site-list Site-1
site-ld 1
vpn-list vpn-10
vpn 10
data-policy FW-policy
vpn-list vpn-10
sequence 1 match
ip-destination 10.1.1.0/24
action accept
set next-hop 10.0.0.2
apply-policy
site-list Hub-1 data-policy netsvd -policy
    
```

B.

```

policy
 data-policy VPN JO FW
 vpn-list VPN JO
 sequence 1
 match
 destination-ip 10.1.1.0/24
 action accept
 set
 vpn 10
 Hoc 10.10.10.1 color mpls encap Ipsec default-action drop
 apply-policy
 site-list Sitel
 data-policy _VPNJO_FW from-service
    
```

C.

```

policy
 lists
 site-list Site-1
 site-ld 1
 control-policy firewall-service
 sequence 10
 match route
 vpn 1
 action accept
 set service FW
 apply-policy
 site-list device-1 control-policy custom-firewall-service out
    
```

D.

```

Policy
 control-policy FW_Policy
 sequence 1
 match route
 vpn 10
 prefix-list AnyIpv4PrefixList action accept
 export-to vpn-llst VPN10-VPN20 set
 service netsvcl
 default-action reject
 apply-policy
 site-list Sitel
 control-policy FW_Policy out
    
```

A. Option A

B. Option B

C. Option C

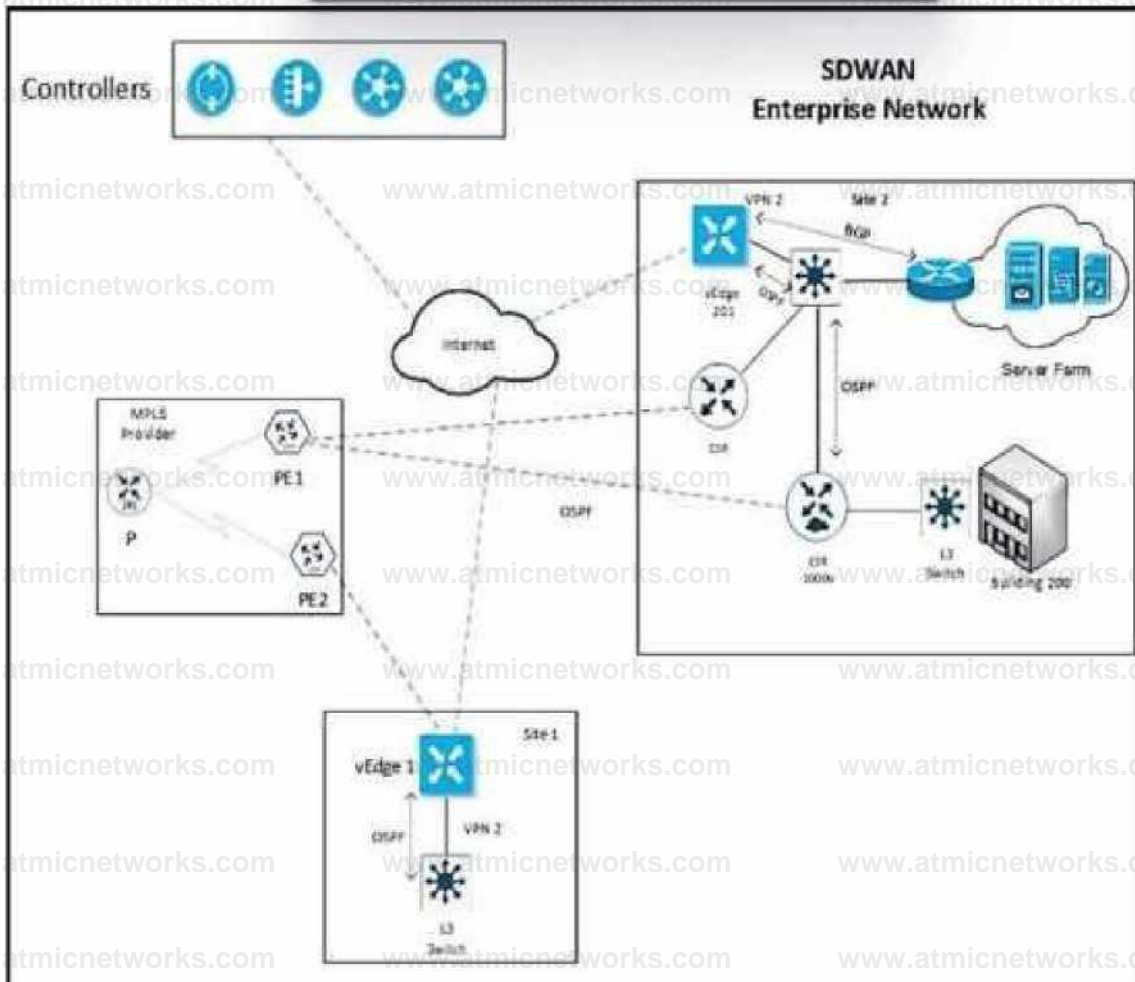
D. Option D

Answer: C

Explanation:

Question: 382

Refer to the exhibit.



Refer to the exhibit. Which configuration ensures that OSPF routes learned from Site2 are reachable at Stein and vice-versa?

A.

```
vpn 2 router ospf timers spf 200 1000 10000 redistribute natpool-outside redistribute omp area 0
interface gefl/0.200 exit
exit

omp
advertise ospf
```

B.

```
vpn 2 router oipf timers spf 200 1000 10000 redistribute omp atea 0
Interface ge0/0.200 exit exit

omp
advertise ospf external
```

C.

```
vpn 2 router ospf timers spf 200 1000 10000 redistribute connected redistribute omp area 0
```

Interface ge0/0.200 exit exit

omp
advertise ospf external
advertise connected

A. Option A

B. Option B

C. Option C

Answer: A

Explanation:

Question: 383

Which component is used to optimize the multicast distribution tree enabled through the multicast network?

- A. IGMP client
- B. vManage controllers
- C. VPN concentrator
- D. OMP replicator

Answer: D

Explanation:

Question: 384

Which capability does Cisco SD-WAN Multi-Region Fabric provide?

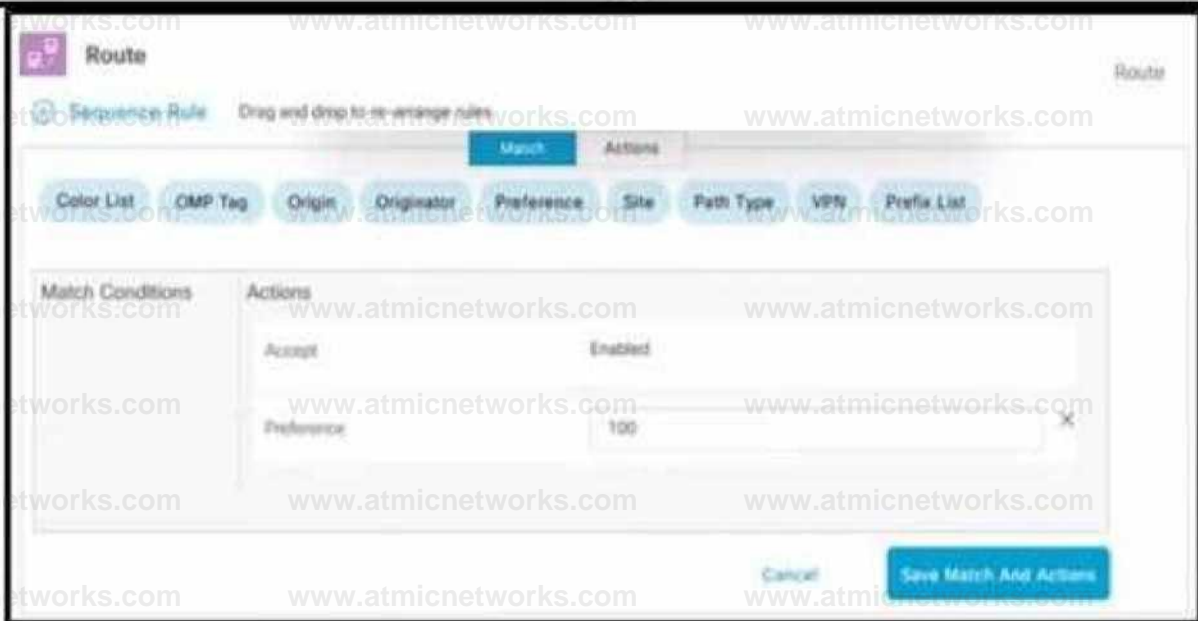
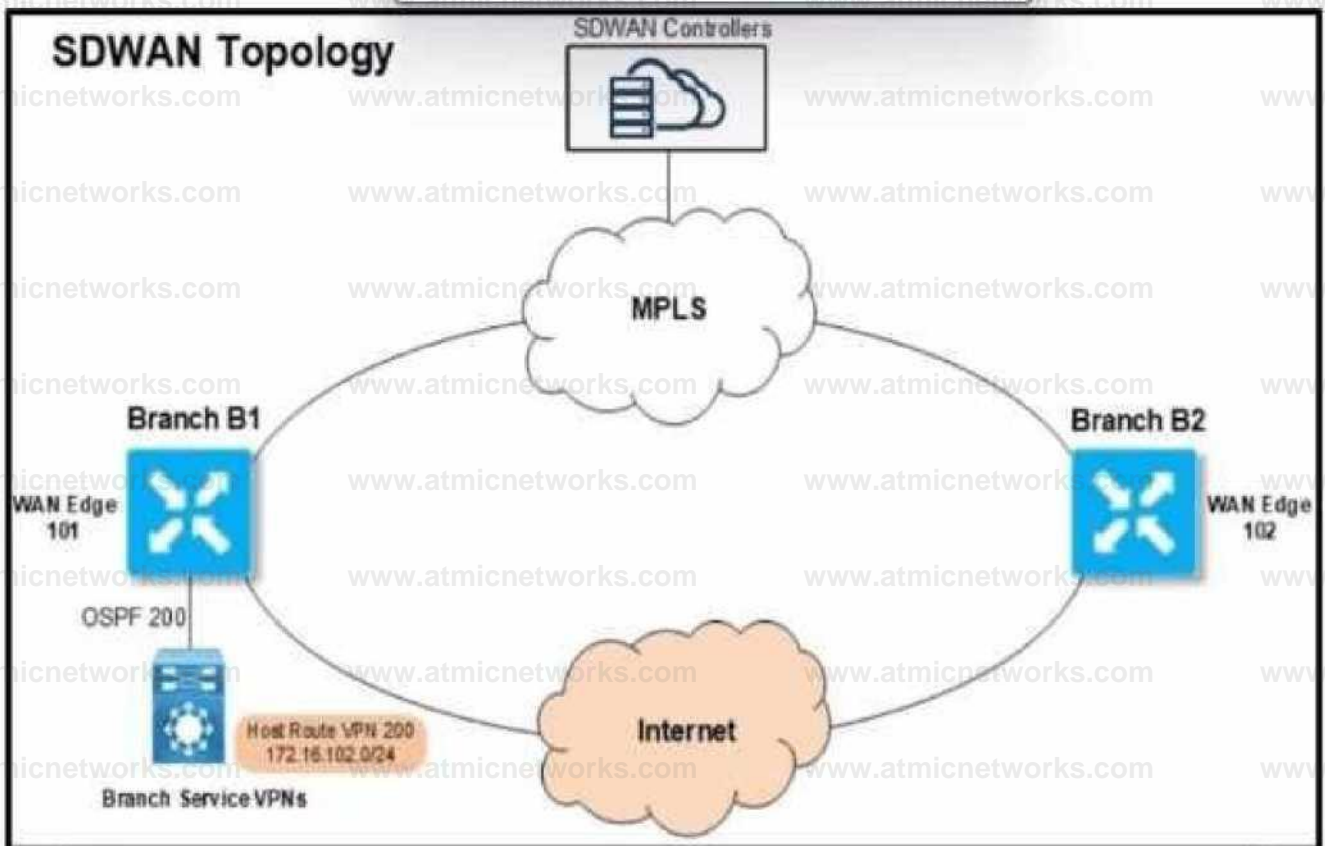
- A. end-to-end SLA-aware routing
- B. overlay support for IP multicast
- C. end-to-end encryption for inter-region traffic
- D. assignment of a single vSmart controller to handle region 0 and noncore regions

Answer: C

Explanation:

Question: 385

Refer to the exhibit.



Refer to the exhibit. An engineer must configure the Overlay Management Protocol route preference so that when B2 tries to reach host routes advertised by B1 it always chooses the MPLS circuit. Which two match conditions must be configured to accomplish this task? (Choose two.)

- A. VPN
- B. prefix list
- C. originator
- D. color list
- E. path type

Answer: D,E

Explanation:

Question: 386

An engineer modifies a data policy for DIA in VPN 200 to meet the requirements for traffic destined to these locations:

- * external networks; must be translated
- * external networks; must use a public TLOC color
- * syslog servers, must use a private TLOC color

Here is the existing data policy configuration:

```
data-policy DIA
vpn-l1st VPN-200
sequence 10
match
destination-data-prefix-l1st INTERNAL-NETWORKS !
action accept
sequence 20
match
destination-lp 0.0.0.0/0
|
action accept
nat use-vpn 0

default-action reject
```

Which policy configuration sequence set meets the requirements?

A.

```
sequence 15
match
destination-lp 0.0.0.0/10
|
action accept
set
local-tloc-l1st
color biz-Internet
sequence 30
match
destination-data-prefix-list SYSLOG-SERVERS
|
action accept
nat use-vpn 0
```

B.

```

sequence 15
match
  destination-data-prefix-list SYSLOG-SERVERS
action accept
set
  local-tloc-list
  color mpls
sequence 20
match
  destination-ip 0.0.0.0/10
[
action accept
set
  local-tloc-list color biz-Internet

```

C.

```

sequence 5
match
  source-ip 0.0.0.0/10
1
action accept
set
  local-tloc-list
  color biz-internet
sequence 30
match
  destination-data-prefix-list SYSLOG-SERVERS
[
action accept
set
  local-tloc-list
  color mpls

```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

Question: 387

An engineer must configure VRRP for redundancy on WAN Edge router1 running an earlier version than 20.6, considering WAN Edge router2 is configured correctly. Which configuration meets the requirement?

A.

vpn 177

Interface ge0/6 mtu 1504 vpn 177 !

Interface ge0/6.2

ipaddress 10.2.2.3/24 no shutdown vrrp 2

ipv4 10.2.2.1 track-prefix-list vrrp-prefix-list1 !

Interface ge0/6.3 ipaddress 10.2.3.5/24 shutdown vrrp 3 ipv4 10.2.3.11 track-prefix-list vrrp-prefix-list 1

B.

vpn0

Interface ge0/6 mtu 1500 vpn 177

interface ge0/6.2 ip address 10.2.3/24 mtu 14% no shutdown vrrp 2 ipv4 10.2.2.1 track-prefix-list vrrp-prefix-list1

interface ge0/6.3

ipaddress 10.2.3.5/24 mtu 1496 shutdown vrrp 3 ipv4 10.2.3.11 track-prefix-list vrrp-prefix-list1

C.

vpn 0

Interface ge0/6 mtu 1500 vpn 177 !

Interface ge0/6.2 ip address 10.2.2.3/24 no shutdown vrrp 2 ipv4 10.2.2.1 track-prefix-list vrrp-prefix-list1

Interface ge0/6.3 ip address 10.2.3.5/24 shutdown vrrp 3 IPV4 10.2.3.11 1

D.

vpn177

Interface ge0/6 mtu 1500 vpn 177 !

interface ge0/6.2

ipaddress 10.2.2.3/24 no shutdown vrrp 2 ipv4 10.2.2.1 track-prefix-list vrrp-prefix-list1

Interface ge0/6.3 ipaddress 10.2.3.5/24 no shutdown vrrp 3

ipv4 10.2.3.11 track-prefix-list vrrp-prefix-list1

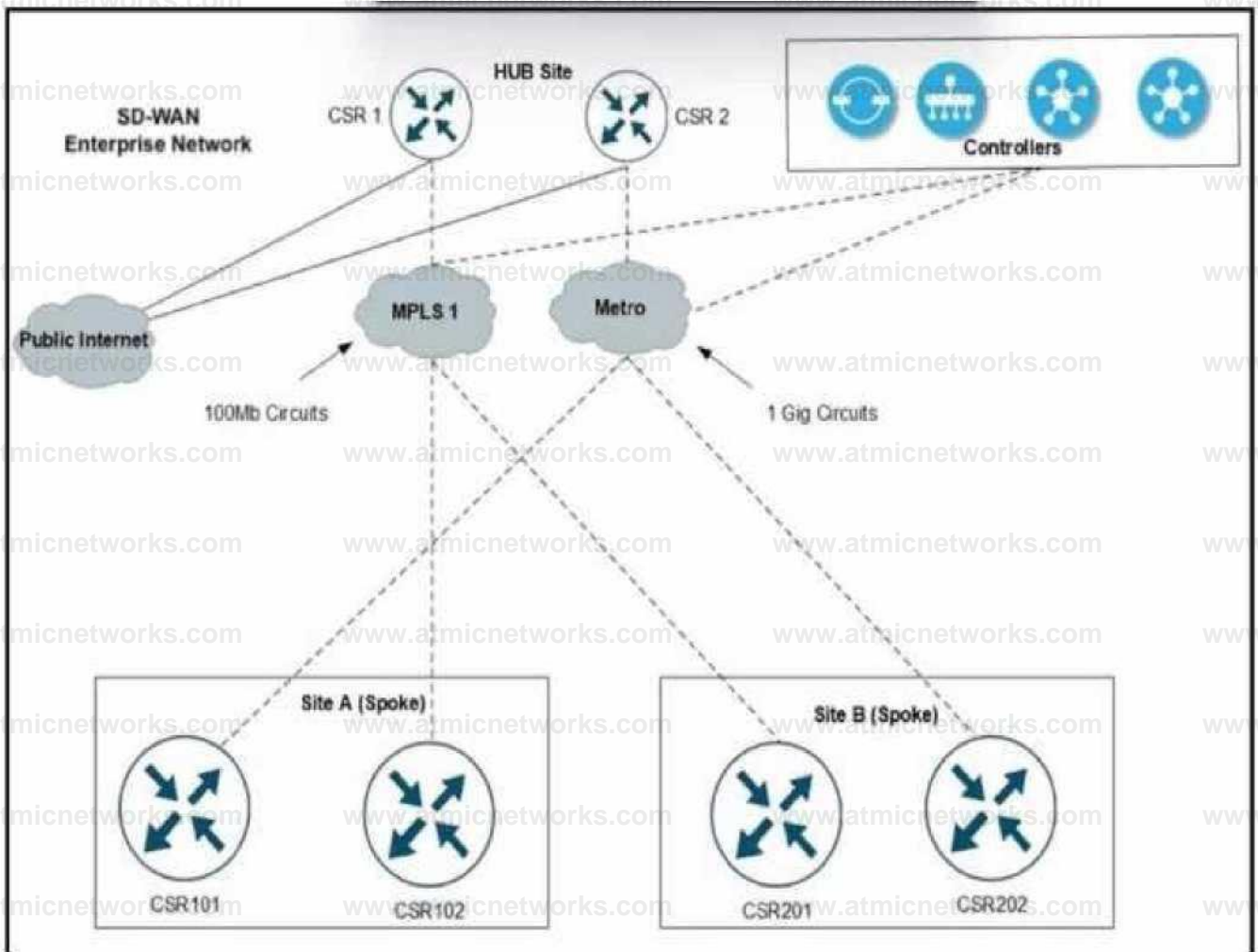
A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 388

Refer to the Exhibit.



Refer to the exhibit. A Cisco SD-WAN network carries traffic for several departments and over 1200 users with several applications at site A and site B branches over the MPLS1 circuit. An engineer is provisioning a higher bandwidth on-demand metro circuit as a backup connection. Which two configurations must the engineer apply to implement the on-demand tunnels? (Choose two.) A.

Spokes

- omp
- no shutdown
- ecmp-limit 16
- system
- on-demand enable
- on-demand idle-timeout 10

B.

Hubs

- sdwan
- service TE vrf global
- exit

C.

Spokes

```
sdwan
service TE vrf global
exit
```

```
omp
no shutdown
ecmp-limit 16
```

D.

Hubs

```
sdwan
service TE vrf global
exit
system
on-demand enable
on-demand idle-timeout 10
```

E.

Spokes

```
vpn 0
service TE
exit
```

```
omp
no shutdown
ecmp-limit 16
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B,C

Explanation:

Question: 389

Which two advanced security features are available on the Cisco SD-WAN WAN Edge (vEdge) device?
(Choose two.)

- A. URL filtering
- B. snort intrusion prevention system
- C. Cisco Umbrella DNS Security
- D. Cisco AMP and AMP Threat Grid
- E. Enterprise Firewall

Answer: B,E

Explanation:

Question: 390

Which Cisco SD-WAN configuration provides the advantages of day-zero deployment and reusable configuration components?

- A. CLI-based templates
- B. configuration groups
- C. configuration via the vBond controller
- D. configuration through a Cisco Prime server

Answer: A

Explanation:

Question: 391

What is the size of SGT data in the metadata header?

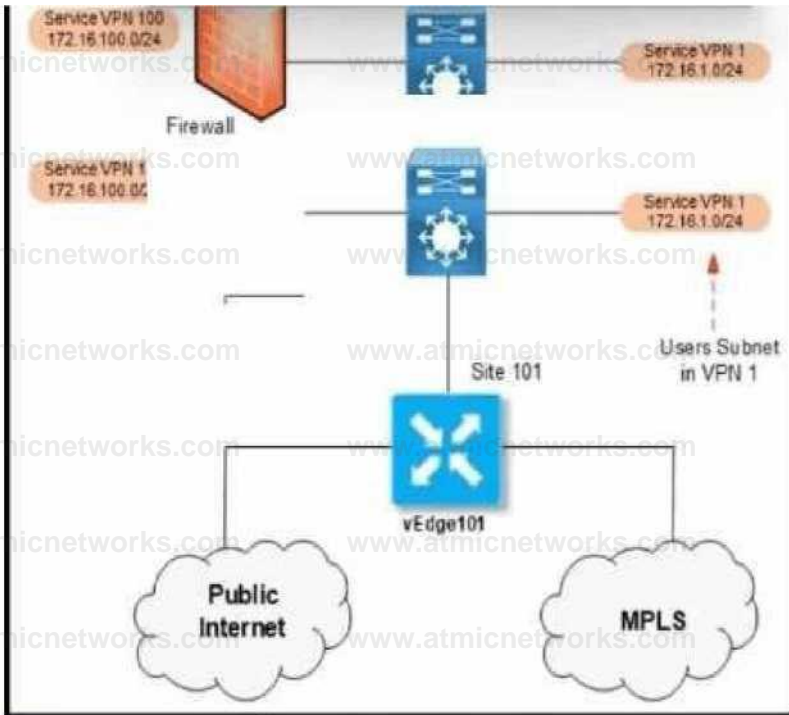
- A. 8 bits
- B. 16 bits
- C. 24 bits
- D. 32 bits

Answer: B

Explanation:

Question: 392

Refer to the Exhibit.



An engineer is creating a policy for VPN1 users. Their scavenger traffic at site 101 must pass through a firewall. Which two match conditions must be selected to enable this policy? (Choose two.)

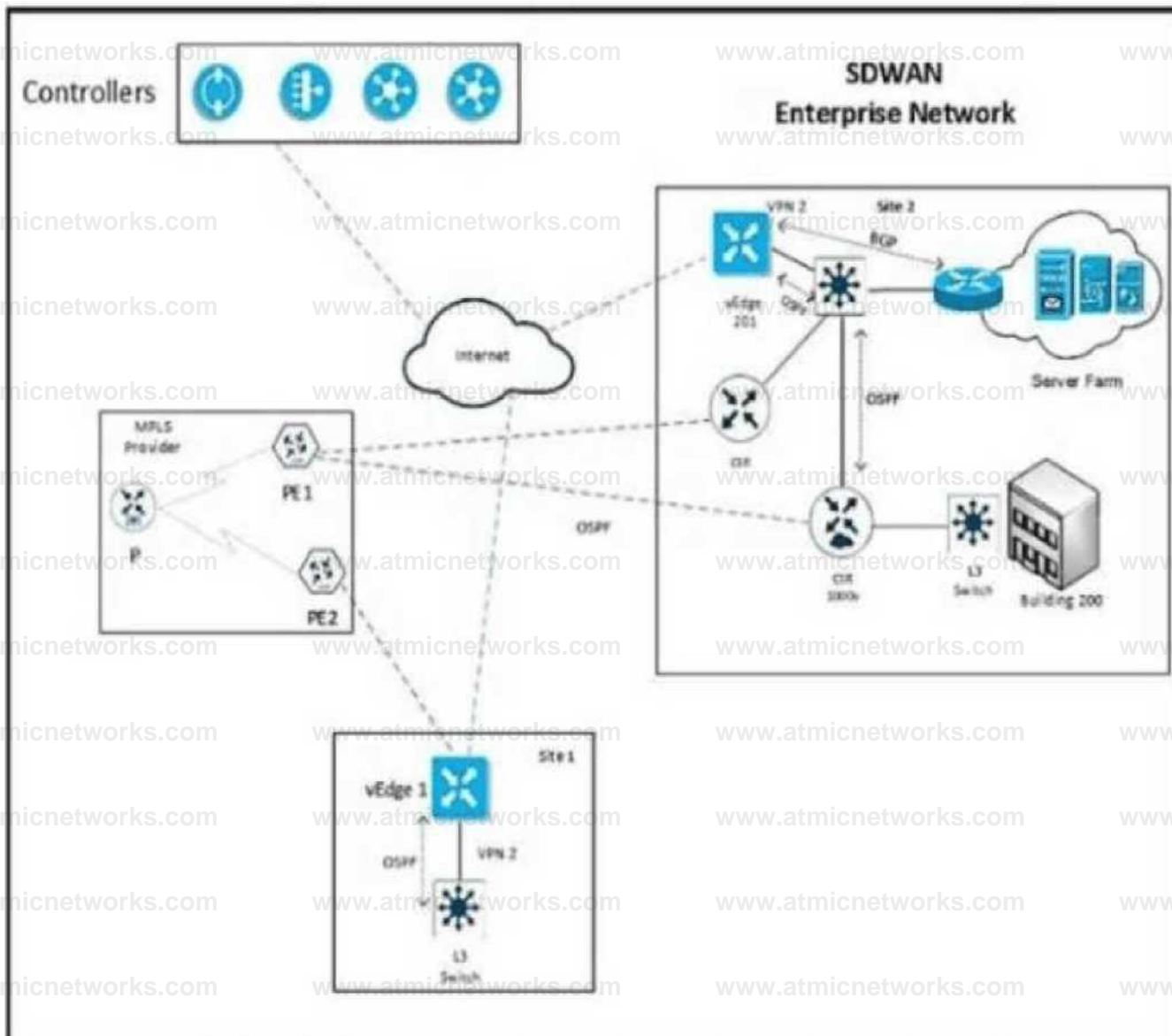
- A. destination port
- B. source data prefix
- C. packet length
- D. protocol
- E. application/application family list

Answer: D,E

Explanation:

Question: 393

Refer to the Exhibit.



Refer to the exhibit Which configuration ensures that OSPF routes learned from Site2 are reachable at Site1 and vice-versa?

```
vpn 2
router
```

```
ospf
```

```
timers spf 200 1000 10000
```

```
redistribute natpool outside
```

```
redistribute connected
```

```
area 0
```

```
interface ge0/0.2 0
```

```
exit
```

```
exit
```

```
omp
```

```
advertise connected
```

```
advertise ospf
```

```
vpn 2
```

```
router
```

```
ospf
```

```
timers spf 200 1000 10000
```

```
redistribute connected redistribute
```

```
omp
```

```
area 0
```

```
interface ge0/0.200
```

```
exit
```

```
exit
```

```
vpn 2 router ospf timers spf  
200 1000 10000 redistribute  
omp area 0  
interface ge0/0.200 exit  
exit
```

```
omp  
advertise ospf external
```

vPn2

```
router ospf timers spf 200  
1000 10000 redistribute  
natpool-outside redistribute  
omp  
area 0  
interface ge0/0.200 exit
```

A. Option A B. Option B C. Option C D. Option D

Answer: D

Explanation:

Question: 394

What is the ZTP workflow for Cisco IOS XE-based devices?

0 The WAN Edge performs the PNP process

The WAN Edge device queries devicehelper1.per.cisco.com The DNS server resolves the PNP server.

The WAN Edge performs the PNP process. The WAN Edge device queries devicehelper.cisco.com The DNS server resolves the ZTP server.

C The WAN Edge performs the ZTP process.

The WAN Edge device queries ztp.vlptela.com
The DNS server resolves the ZTP server.

The WAN Edge performs the ZTP process.
The WAN Edge device queues ztp.vipLela.com.
The DNS server resolves the PNP server

A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

Question: 395

Which cloud based component in cisco SD-WAN is responsible for establishing a secure connection to each

WAN edge router and distributes routers and policy information via omp?

- A. vBond
- B. vManage
- C. vSmart
- D. WAN Edge

Answer: C

Explanation:

Question: 396

Which configuration change allows direct internet access at the branch site for YouTube traffic?

```
policy
data-policy DPI
vpn-list vpn10
sequence 10
match
app-list YouTube
!
action
count Youtube
!
default-action accept
!
!
lists
vpn-list vpn10

vpn 10
!
app-list YouTube
app youtube
app youtube_hd
!
site-list Remote
site-id 14
!
!
!
apply-policy
site-list Remote
data-policy DPI from-service
```

```
policy
data-policy DPI
vpn-list vpn10
sequence 10
match
app-list YouTube
!
action drop
count Youtube
!
default-action accept
!
!
lists
vpn-list vpn10

vpn 10
!
app-list YouTube
app youtube
app youtube_hd
!
site-list Remote
site-id 14
!
!
!
apply-policy
site-list Remote
data-policy DPI from-transport
```




```
policy
data-policy DPI
vpn-list vpn10
sequence 10
match
app-list YouTube
!
action
count Youtube
nat vpn 0
!
default-action accept
!
lists
!
vpn-list vpn10
vpn 10
!
app-list YouTube
app youtube
app youtube_hd
!
site-list Remote
site-id 14
!
!
apply-policy
site-list Remote
data-policy DPI from-service
```



```
policy
data-policy DPI
vpn-list vpn10
sequence 10
match
app-list YouTube
!
action
count Youtube
nat vpn 0
!
default-action accept
!
lists
!
vpn-list vpn10
vpn 10
!
app-list YouTube
app youtube
app youtube_hd
!
site-list Remote
site-id 14
!
!
apply-policy
site-list Remote
data-policy DPI from-transport
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

Question: 397

Refer to the exhibit.

```
interface ge0/U
tunnel-interface
encapsulation ipsec
color metro-ethernet
group 100
```

The network design team has advised to use private IP addresses and private colors over the SP circuit for the data plane connections. The Public IP should be used for control connections. Which configuration should be applied at SiteA to achieve this task?

vpn 0

interface geO/O

description * TO ISP CID 64:ff9b:1:4376:89ff:34ff:76f5:2f1f *****

tunnel-Interface

encapsulation ipsec

color lte

group 101

vpn 0

interface geO/O

description * TO ISP CID 64:ff9b:1:4376:48ff:56ff:50f8:7f8f *****

tunnel-interface

encapsulation ipsec

color mpls

group 100

vpn 0

interface ge0/0

description *** TO ISP CID 64:ff9b:1:4376:24ff:93ff:81f7:6f5f ***

tunnel-Interface

encapsulation ipsec

color custom1

group 101

vpn 0

Interface ge0/0

description *** TO ISP CID 64:ff9b:1:4376:65ff:34ff:21f9:8f7f ***

tunnel-interface

encapsulation ipsec color biz-internet group 100

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 398

Which Cisco router provides a distributed multicore architecture optimized for SD-WAN branch support?

- A. Cisco 1000 ISR series
- B. Cisco 2900 ISR series
- C. Cisco Catalyst 3850 series
- D. Cisco 3900 ISR series

Answer: A

Explanation:

Question: 399

What is a restriction when configuring a tunnel interface?

- A. Up to six tunnel interfaces are configurable on a vSmart.
- B. it is manually assigned when using vWanage feature template.
- C. It must be configured for the interface under aft VPNs
- D. Up to six tunnel interfaces are configurable on a WAN Edge

Answer: B

Explanation:

Question: 400

An engineer provisions a WAN Edge router. Which command should be used from the WAN Edge router to activate it with vManage?

- A. request vedge-cloud activate serial <serial> token <token-number>
- B. request vedge-cloud activate chassis-number <chassis-number> organization <organization>
- C. request vedge-cloud activate chassis-number <chassis-number> token <token-number>
- D. request vedge-cloud activate chassis-number <chassis-number> serial <:serial>

Answer: A

Explanation:

Question: 401

The SD-WAN network is configured with a default full-mesh topology. The SD-WAN engineer wants the Barcelona WAN Edge to use the MPLS TLOC when forwarding Telnet traffic based on a configured SLA class list. Which configured must the engineer use to create a policy to call the SLA class and set the preferred color to MPLS?

- A)



B)



C)



D)



- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 402

Refer to the Exhibit.

```
interface GigabitEthernet0/0/1
description TO WAN - MPLS
no shutdown
ip address 209.165.202.129/27
no ip redirects
!
sdwan
!
interface GigabitEthernet0/0/1
tunnel-interface
encapsulation ipsec
color private1
port-hop

no allow-service all
!
```

Refer to the exhibit. An engineer is enabling command line access via MPLS for in-band management. Which command completes the partial SD-WAN interface configuration with the highest degree of security?

sdwan

```
interface OigabitEthernetO/O/1 atiw-service sshd
```

sdwan

```
interface GigabitEthernetO/O/1 attow-service https
```

sdwan

```
interface Gigabl£theneW/O/1 a!i<M*ser¥ice all
```

sdwan

```
Interface GigabitEtherneWO/I allo ^service temp
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

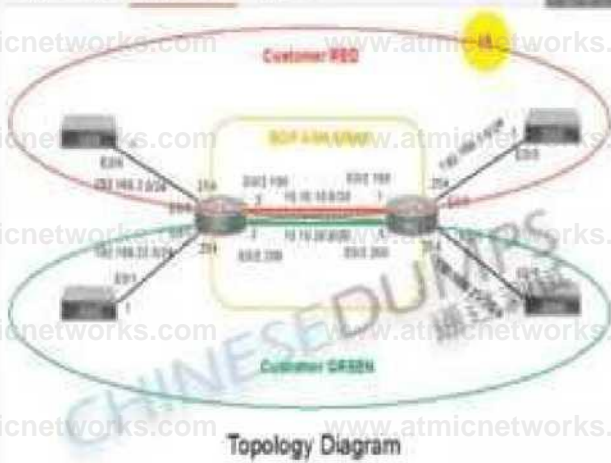
Question: 403

SIMULATION

Configure individual VRFs for each customer according to the topology to achieve these goals :

Comment

Guidelines Topology Tasks



R1 R2 SW1 SW2 SW3 SW4

```
R1>  
R1>  
R1>  
R1>  
R1>
```

Guidelines Topology Tasks



R1 R2 SW1 SW2 SW3 SW4

```
R1>  
R1>  
R1>  
R1>  
R1>
```

CAuty'u L-in>I iI4VHf<*-HJ11. il>ni<M ..m!': P' tw tapuMij

la Kiara* taw yiat

Balti i<Mm ** (Mittir^mwci Mti f M3<M*ng W* and

&3P.Dv roc um
J WF'Cu-OnHKri.^

3 DLiPo^rOulHI RI U ^™i<i RI Him

4 BE*P'I WIW R? paPtUMM VRF ffiuM^ bMNMra
ntKJW RI Vid fo

4 IARtalA>l<t*adiiifci*tRlw<wl>8Wt *4*M3tn URF'

LUTVJ ^v l—A*-. BW? Md EW4 /> VRF cuvaec' M
MrtrPai «* #acontl#t#Mt


```
R1 R2 SW1 SW2 SW3 SW4
R1 >
R1> I NESE DUMPS
R1>      sains
R1>
R1>en
RUsh run
Building configuration

Current configuration : 1353 bytes
!
version 15.a
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RI
!
boot-start marker
boot end marker
!
, EDUMPS
no aaa new-model
!
```

R1 R2 SW1 SW2 SW3 SW4

CHIN ESEDUMPS
aiSWK



```
ip vrf cu -green rd 65000:200
```

```
ip vrf cu~red rd 65000:100
```

```
| I
```

```
I
```

```
no ip domain lookup
```

```
ip cef
```

```
no ipv6 cef
```

```
■ t WES EDUMPS
```

```
multilink bundle-ndmb 'Authenticated |
```

```
i ■
```

CHINESE DUMPS
aasoK

R1

R2

SW1

SW2

SW3

SW4

CHINESEDUMPS

通过测试

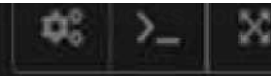
```
interface Loopback0
 ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.1.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.20.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 duplex auto
!
interface Ethernet0/2.100
 encapsulation dot1Q 100
 ip address 10.10.10.1 255.255.255.252
!
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.1 255.255.255.252
```

R1 R2 SW1 SW2 SW3 SW4

```
interface Ethernet0/2.200 encapsulation ip address
```

```
10
```

```
dot10 200  
DUMPS 55.255.255.252
```



```
interface
```

```
Ethernet0/3 no ip address shutdown duplex auto
```

```
router bgp 6500V * bgp log neighbor changes no  
bgp default ipv4-unicast
```

```
ip forward protocol nd
```

DUMPS

```
no ip http server
```

```
no ip http secure-server
```

```
ipv6 ioam timestamp i
```

DUMPS

```
control plane F
```

R2

R1 R2 SW1 SW2 SW3 SW4

```
R2>en
R2#Show run
Building configuration...
Current configuration : 1353 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
```



CHINESEDUMPS
通过测试

RI R2 SW1 SW2 SW3 SW4

ESEDUMPS

```
Ip vrf cu-greon rd 65000:200
```

```
ip vrf cu-red rd 65000:100
```

ESf DUMPS

```
j
```

```
no ip domain lookup
```

```
ip cot
```

```
no iPv6 cof 0U\|pS
```

```
multilink bundle-name authenticated
```

R1

R2

SW1

SW2

SW3

SW4

CHINESEDUMPS

通过测试

```
interface Loopback0
  ip address 10.10.2.2 255.255.255.255
```

```
interface Ethernet0/0
  ip address 192.168.2.254 255.255.255.0
  duplex auto
```

```
interface Ethernet0/1
  ip address 192.168.22.254 255.255.255.0
  duplex auto
```

```
interface Ethernet0/2
  no ip address
  duplex auto
```

```
interface Ethernet0/2.100
  encapsulation dot1Q 100
  ip address 10.10.10.2 255.255.255.252
```

```
interface Ethernet0/2.200
  encapsulation dot1Q 200
  ip address 10.10.20.2 255.255.255.252
```

CHINESEDUMPS

通过测试

RI R2 SW1 SW2 SW3 SW4

```
interface Ethernet0/2.200  
encapsulation dot1Q 200  
ip address 192.168.1.255 255.255.255.252
```

```
interface Ethernet0/3 no ip  
address shutdown duplex  
auto
```

```
router bgp 65000  
bgp log-neighbor changes  
no bgp default ipv4-unicast
```

```
ip forward-protocol nd
```

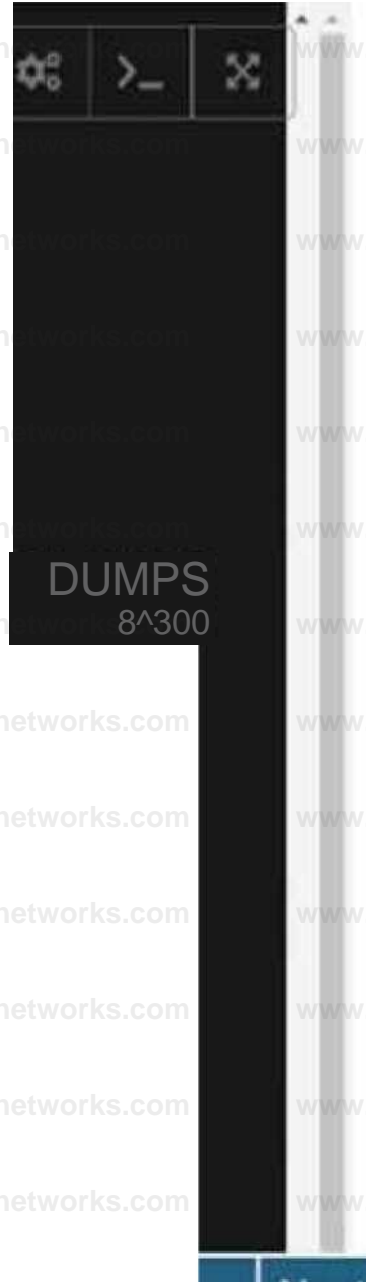
```
no ip http server  
no ip http secure-server
```

```
ipv6 ioam timestamp
```

```
; DUMPS
```

```
control-plane
```

SW1



R1 R2

SW1 SW2 SW3

SW4

```
SW1>en
SW1#sh run | J^MPS
Building configuration...

Current configuration : 942 bytes
!
• Last configuration change at 04:43:09 PST Sat May 7 20 22
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config

hostname SW1

boot-start-marker boot-end marker

! CHINESEDUMPS no aaa now-model ^ - '^ clock timezone PST -
80
```



DUMPS
^;®

R1 R2 SW1 SW2 SW3 SW4

```
spanning-tree mode pvst
spanning-tree extend system-id
```

通过测试

CHINESEDUMPS

通过测试

```
interface Ethernet0/0
no switchport
ip address 192.168.2.1 255.255.255.0

interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
```

Next

```
R1 R2 SW1 SW2 SW3 SW4
no switchport
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.2.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
control-plane
!
```

SW2

R1 R2 SW1 SW2 SW3 SW4

```
SW2>
```

```
WRI JESEDUMPS
```

```
SW2*n SiMjW
```

```
SW2|show run
```

```
Building configuration...^
```

```
Current configuration : 944 bytes
```

- Last configuration change at 04:43:09 22

```
version 15.2
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
no service password'encrypt ion
```

```
service compress-config
```

```
hostname SW2
```

```
boot start-marker
```

```
boot-end-marker
```

```
' CHINESEDUMPS
```

```
i asms
```

```
no aaa new model
```

PST Sat May 7 20

JESEDUMPS

R1 R2 SW1 SW2 SW3 SW4

```
spanning-tree mode pvst
spanning-tree extend system-id
```

CHINESEDUMPS
通过测试



CHINESEDUMPS
通过测试

```
interface Ethernet0/0
!
interface Ethernet0/1
no switchport
ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
```

R1 R2 SW1 SW2 SW3 SW4

```
interface EthennetOX Li nr
no switchpoit
ip address 192.166.2271 255 .255.255.0
interface Ethernet0/2
interface Ethernet0/3
ip forward-protocol nd
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.160.22.254 ssh server
ip algorithm encryption aes!28 -ctr aes192-ctr
  aos256-ctr p
ssh client algorithm encryption aes128-ctr aes192-ctr
  acs256 ctr
control-plane
```

SW3

RI R2 SW1 SW2 SW3 SW4

```
SW3>
SW3>en
SW3|show run
Building configuration

Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version IS.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption service
compress config
!
hostname SW3
!
boot start-marker boot
end marker
; < E DUMPS
, aa«
no aaa now model clock
timezone PST -8 0
```

RI R2 SW1 SW2 SW3 SW4

```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Ethernet0/0
 no switchport
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
```



通过测试

CHINESEDUMPS
通过测试

R1 R2 SW1 SW2 SW3 SW4

```
no switchport
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
control-plane
!
```

R1 R2 SW1 SW2 SW3 SW4

```
SW4>en
SW4#show run
Building configuration...

Current configuration : 944 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW4
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!
```

RI

SW1 SW2 SW3 SW4

```
spanning tree mode pvst
spanning trcf ^Xj^nl. system id
```

I

ES EDUMPS
iff t3IW

```
interface EthernetO/O
interface EthernetO/1
ip address 192.168.20.1 255.255.255.0
```

ZHINESEDUMPS

```
interface Ether netO/^i.
```

```
interface EthernetO/3
```

R1 R2 SW1 SW2 SW3 SW4

```
interface Ethernet0/24
 no switchport
 ip address 192.168.20.1 255.255.255.0
 interface Ethernet0/3
 ip forward-protocol nd
```

```
ip http server
```

```
ip http secure-server
```

```
ip route 0.0.0.0 0.0.0.0
```

CHINESE DUMPS
192.168.20.254

```
ip ssh server algorithm encryption aes128 ctr aes192 ctr aes256ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256ctr
```

CHINESE DUMPS

```
control plane
```

```
WWW
```

Guidelines Topology Tasks tF

Configure individual j/RFs for each customer according to the topology to achieve these goals

1. VRF "cu-red" has interfaces on routers R1 and R2 Both routers are preconfigured with IP addressing, VRFs. and BGP. Do not use the BGP network statement for advertisement.
2. VRF "cu-green" has interfaces on routers R1 and R2.
3. BGP on router R1 populates VRF routes between router R1 and R2.
4. BGP on router R2 populates VRF routes between router R1 and R2.
5. LAN to LAN is reachable between SW1 and SW3 for VRF cu-red and between SW2 and SW4 for VRF "cu-green All switches are preconfigured.

Answer: See the solution below in Explanation.

Explanation:

Solution:

Use cu-red under interfaces facing SW1 & SW3:

On R1:

```
interface Ethernet0/0 ip vrf forwarding cu-red
ip address 192.168.1.254 255.255.255.0
```

Check reachability to SW1:

```
R1#ping vrf cu-red 192.168.1.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

On R2:

```
interface Ethernet0/0
```

```
ip vrf forwarding cu-red
```

```
ip address 192.168.2.254 255.255.255.0
```

Check reachability to SW3:

```
R2#ping vrf cu-red 192.168.2.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: !!!!!

Use vrf cu-green for SW2 & SW4:

On R1:

```
interface Ethernet0/1
```

```
ip vrf forwarding cu-green
```

ip address 192.168.20.254 255.255.255.0

Test reachability to SW2:

R1#ping vrf cu-green 192.168.20.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

On R2:

interface Ethernet0/1

ip vrf forwarding cu-green

ip address 192.168.22.254 255.255.255.0

Test reachability to SW4:

R2#ping vrf cu-green 192.168.22.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

On R1:

interface Ethernet0/2.100

mpls ip !

interface Ethernet0/2.200

mpls ip !

Configure BGP:

router bgp 65000

neighbor 10.10.10.2 remote-as 65000

neighbor 10.10.20.2 remote-as 65000 !

address-family vpnv4

neighbor 10.10.10.2 activate

neighbor 10.10.20.2 activate exit-address-family

!

address-family ipv4 vrf cu-green redistribute connected

exit-address-family !

address-family ipv4 vrf cu-red redistribute connected exit-address-family

!

R1(config)#ip vrf cu-red

R1(config-vrf)#route-target both 65000:100 !

R1(config)#ip vrf cu-green

R1(config-vrf)#route-target both 65000:200

On R2:

interface Ethernet0/2.100

mpls ip !

interface Ethernet0/2.200

mpls ip !

```
router bgp 65000
neighbor 10.10.10.1 remote-as 65000
neighbor 10.10.20.1 remote-as 65000 !
address-family vpnv4
neighbor 10.10.10.1 activate
neighbor 10.10.20.1 activate exit-address-family
!
address-family ipv4 vrf cu-green redistribute connected
exit-address-family !
address-family ipv4 vrf cu-red redistribute connected exit-address-family
```

```
R2(config)#ip vrf cu-red
R2(config-vrf)#route-target both 65000:100 !
R2(config)#ip vrf cu-green
R2(config-vrf)#route-target both 65000:200
```

Verification:

From SW1 to SW3:

```
SW1#ping 192.168.1.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

But can't Reach SW2 or SW4 in VRF cu-green:

```
SW1#ping 192.168.22.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds: U.U.U

Success rate is 0 percent (0/5)

```
SW1#ping 192.168.20.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds: U.U.U

Success rate is 0 percent (0/5)

Same Test for SW2:

From SW2 to SW4:

```
SW2#ping 192.168.20.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

But can't Reach SW3 or SW1 in VRF cu-red:

```
SW2#ping 192.168.1.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: U.U.U

Success rate is 0 percent (0/5)

```
SW2#ping 192.168.2.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

U.U.U

Success rate is 0 percent (0/5)

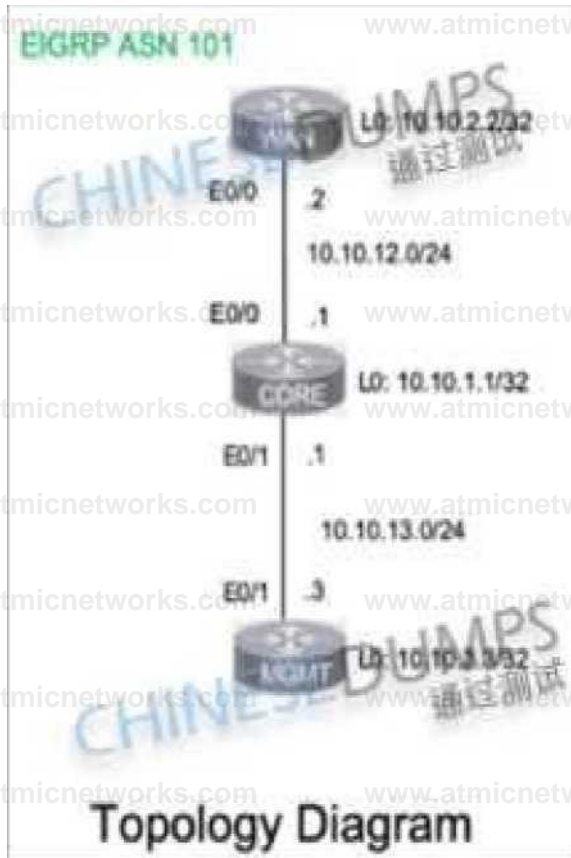
Both R1 & R2 has separate tables for VRFs cu-red and cu-green.

Question: 404

SIMULATION

A network is configured with CoPP to protect the CORE router route processor for stability and DDoS

protection. As a company policy, a class named class-default is preconfigured and must not be modified or deleted. Troubleshoot CoPP to resolve the issues introduced during the maintenance window to ensure that:



Guidelines Topology Tasks

A network is conjured with CoPP to protect the CORE router route process and DDoS protection. As a company policy, a class named class-default is preconfigured and must not be modified or deleted. Troubleshoot CoPP to resolve the issues introduced during the maintenance window to ensure that:

1. Dynamic routing policies are under CoPP-CRITICAL and are allowed only from the 10.10.x.x range.

2. Telnet, SSH, and ping are under CoPP-IMPORTANT and are allowed strictly to/from 10.10.x.x to the CORE router (Hint: you can verify using Loopback 1).

3. All devices ping (UDP) any CORE router interface successfully to/from the 10.10.x.x range and do not allow any other IP address.

NORMAL (Hint: Traceroute port range 33434-33464)

WAN

```
CHINESEDUMPS
interface Loopback0
ip address 10.10.2.2 255.255.255.255

interface Loopback1
ip address 172.16.2.2 255.255.255.255
CHINESEDUMPS
```

```
WA CORE MGMT
interface Loopback0
ip address 10.10.2.2
255.255.255.255
interface Loopback1
ip address 172.16.2.2
255.255.255.255

interface Ethernet0/0
ip address 10.10.12.2 255.255.255.0
duplex auto

interface Ethernet0/1 no ip
shutdown duplex auto

interface Ethernet0/2
no ip address shutdown duplex
auto

interface Ethernet0/3 no ip address shutdown
duplex auto

router ospf 101
network 10.10.0.0
0.0.255.255 network
area 0 router-id 10.10.2.2
```

```
router# show run | grep -E "eigrp|network|router-id"
eigrp 1
network 10.10.0.0 0.0.255.255
network 172.16.2.0 0.0.0.255
eigrp router-id 10.10.2.2
```

CORE

```
class-map imfhpnbfaRfy^ITICAL
match access-group 122
class-map match-all W^I NORMAL
match access-group 122
class map match-all COPP-IMPORTANT
match access-group 122

policy-map CoPP
class CuPP-CRITICAL
  police 1000000 50000 50000 conform action transmit exceed
  action drop
class CePP IMPORTANT
  police 100000 20000 20000 conform action transmit exceed- action drop
class COPP NORMAL
  police 64000 6400 64000 conform action transmit exceed action drop
class class-default
  police 8000 1500 1500 conform action drop
```



CHINESEDUMPS

```
interface Loopback0  
ip address 10.10.1.1 255.255.255.255
```

```
interface Ethernet0/0  
ip address 10.10.12.1 255.255.255.0  
duplex auto
```

```
interface Ethernet0/1  
ip address 10.10.13.1 255.255.255.0  
duplex auto
```

```
duplex auto  
interface EthornetO/2  
no ip address Shutdown duplex auto
```

```
interface EthornetQ/3 no ip address  
shutdown duplex auto
```

```
router eigrp 10] network  
10.10-0.0 0.0.255.255 eigrp  
router-id 10.10.1.1
```

CHINESEDUMPS
aaaira

```
ip forward protocol nd
```

```
!  
no ip http server  
no ip http secure server  
!
```

```
ipv6 ioam timestamp
```

```
!
CHINESEDUMPS
access-list 120 remark *** ACL for CoPP-Critical ***
access-list 121 remark *** ACL for CoPP-IMPORTANT
access-list 122 remark *** ACL for CoPP-NORMAL
!
control-plane
service-policy input CoPP
!
CHINESEDUMPS
通过测试
```

MGMT

WAN CORE MGMT

interface Loopback0

amMfii^

interface Loopback0

ip address 172.16.3.3 255.255.255.0

interface Ethernet0/0 no

ip address shutdown

duplex auto

interface Ethernet0/1

ip address 10.10.13.3 255.255.255.0 duplex

auto

interface Ethernet0/2 no

ip address shutdown

duplex auto

interface Ethernet0/3 no

ip address shutdown

duplex auto

router cigrp LCIDUMPS

nos work 10.10.13.0 255.255.255.0

network 172.16.3.0 0.0.0.255

router-id 10.10.13.3

CHINESE

EDUMPS
ISSMH

WAN CORE MGMT

```
no ip address shutdown  
DUMPS duplex auto iSOa
```

```
router eigrp 101  
network 10.0.0.0/24  
network 172.16.3.0/24  
eigrp router-id 10.3.3
```

```
ip forward-protocol nd
```

```
no ip http server  
no ip http secure-server
```

```
ipv6 ioam timestamp
```

```
control plane  
-CHIMESEDUMPS
```

.EDUMPS
iSHSH

**Answer: See
the
solution below in**

Explanation:

CORE

```
policy-mao CoPP  
class CoPP-CRITICAL  
police 1000000 50000 50000 conform-action transmit exceed-action transmit
```



```

:[] .!-'S.. I i r.t 2^pwJ-U' ACL for CoPP-Critical '* 11^^11 ^ 10.10.0.0
■itc^sn likt i*0.255.255 any 120 peift^^lmgrp any any
access-list 20 permit ip any 10.10.0*0 0.0,255.255
access-list 21 permit ienn; 10*10*0.0 0*0,255.255 any
access-list .21 permit tep ID. 10.0.0 0.0.255.255 any eq 22
access-list 21 permit tsp LO.IO.O.p 0.0.255.255 any eq toIne
access List t
access list 22 remark ■*■ ACL for COPP NORMAL
access-list 22 permit trip 10.10.0.0 0.0.255.255 any
access list 22 permit udp any 10*10.0.0 0.0.255.255
access-list 22 permit trip any 10/ ^.n "-M^MPS »
434 33464 22 permit trip 10.10,0.0 0*0.255.255 an^H^e 33
access List
434 33464
plane
service-: policy BtJA^^S
SI^tS

```



A screen shot of a computer AI-generated content may be incorrect. Text Description automatically generated with medium confidence

CORE# Copy run start

TESTING: -

CORE

```

CORE#sh ip -algrr no lghbrs
ELGRP-IPV4 Neighbour Mod AS (101)
通过测试
H Address Interface Hold Opti
me SRTT RTO Q Seq (sec)
(ms) Cnt Num
0 10.10.13.3 Et0/1 11 00:0
3:15 5 100 0 35
1 10.10.12.2 Et0/0 CHINESEDUMPS:0
3:24 7 100 0 33 通过测试
CORE#copy run star

```

A screen shot of a computer AI-generated content may be incorrect. Graphical user interface Description automatically generated with medium confidence

MGMT

```
MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ... Connection refused by remote host
通过测试

MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ... Open

Password required, but none set

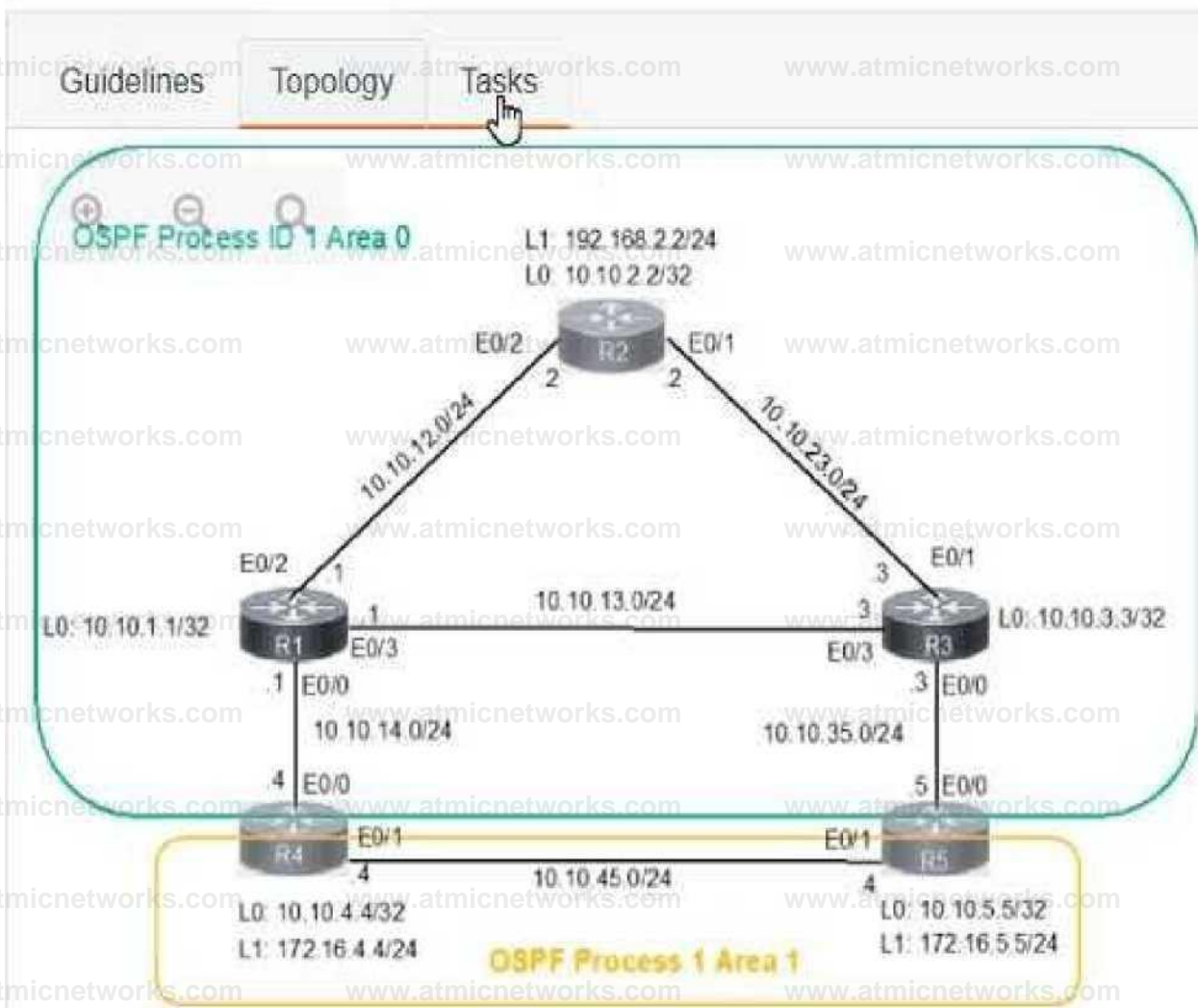
[Connection to 10.10.13.1 closed by foreign host]
MGMT#
```

A screenshot of a computer AI-generated content may be incorrect. Graphical user interface, text Description automatically generated

Question: 405

SIMULATION

A network is configured with IP connectivity, and the routing protocol between devices started having problems right after the maintenance window to implement network changes. Troubleshoot and resolve to a fully functional network to ensure that:



Topology Diagram

Guidelines Topology Tasks

A network is configured with IP connectivity, and the routing protocol between devices started having problems right after the maintenance window to implement network changes. Troubleshoot and resolve to a fully functional network to ensure that:

1. Inter-area links have link authentication (not area authentication) using MD5 with the key 1 string CCNP.
2. R3 is a DR regardless of R2 status while R1 and R2 establish a DR/BDR relationship.
3. OSPF uses the default cost on all interfaces. Network reachability must follow OSPF default behavior for traffic within an area over intra-area VS inter-area links.
4. The OSPF external route generated on R4 adds link cost when traversing through the network to reach R2. A network command to advertise routes is not allowed.

R2^>en

R2\$

R2f

R2 | r

R2 | 1

R2 |

R2f

R2lsh run

Building configuration...

Current configuration : 1279 bytes 1
version IS.9

service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption i

hostname R2

boot-start-marker boot-end-marker 1 1

!

no aaa new-model j i

clock timezone PST -8 0 mmi polling-interval 60 no
mmi auto-confignis

Activate Windc

Gc io Seungs *0 ac

R2 R4 R5

```
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
 ip ospf 1 area 0
!
interface Loepback1
 ip address 192.168.2.2 255.255.255.0
 ip ospf 1 area 0
!
interface EthernetO/O no
 ip address shutdown
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.23.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
!
interface EthernetO/2
 ip address 10.10.12.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/3 no ip
 address shutdown duplex
 auto
!
router ospf 1
 passive-interface default no passive-
 interface EthernetO/1 no passive-interface
 EthernetO/2
```

R2 R4 R5

```
interface EthernetO/3 no ip address shutdown duplex auto
```

```
router ospf "1"
  passive-interface default
  no passive-interface Ethernet 0/1
  no passive-interface Ethernet 0/2
```

```
ip forward-protocol nd
```

```
no ip http server
no ip http secure-server
```

```
ipv6 ioau? time stamp
```

```
control-planes
```

```
I
```

```
i
```

```
|  
lineconJ?
```

Activate
GcroSerij

R4

```
R2 R4 R5
R4>
R4>
R4>
R4>
R4>en
R4#sh run
Building configuration...

Current configuration : 1479 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
--More--
```

Activate V
Go to Setting

R2

R4

R5

```
key chain CCNP
key 1
  key-string ecnp
  cryptographic-algorithm md5
!
!
!
!
!
!
ip address 172.16.4.255 255.255.255.0 I interface
Ethernet0/0
ip address 10.10.14.4 255.255.255.0 ip ospf
authentication key-chain CCNP in ospf 1 area 0
duplex auto
!
interface Ethernet0/1
ip address 172.16.45.4 255.255.255.0 ip ospf 1 area
I duplex auto
J
interface Ethernet0/2 no ip address shutdown duplex
auto
interface Ethernet0/3 no ip address shutdown duplex
auto
```

Activate
Go to Settings

R2 M R5

```
router ospf 1
 redistribute connected subnets route-map to-ospf
 passive-interface default
 no passive-interface EthemetO/O
 no passive-interface Ethernet0/1
```

```
ip forward-protocol nd i
```

```
1
 no ip http server
 no ip http secure-server

 ipv6 ioam timestamp

 route-map to-ospf permit 10
 match interface Loopback1
```

```
|
 control-planes
```

```
!
```

```
|
```

```
i
 line coin 0
 logging synchronous
 line aux 0
```

Activate W
Go to Settings

R5

R2 R4 R5

```
RS>
R5>
Rb>en
R5i
RSI j
R5fsh run
Budding configuration...

Current configuration : 1496 bytes
version 15.3
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption I hostname 35

boot-start-marker boot-end-marker 1 [ 1
no aaa new-model
E
!
clock timezone EST -8 0
mmi polling-interval 60
no oii aut^configure
no mmi pvc
—Mora— |
```

Activate W

Go to

R2 R4 R5

```
I  
I  
I I no ip domain Lookup ip cef no ipv6 cef  
multilink bundle-name authenticated  
i  
i
```

```
key chain CCKP key 1  
  key-string CCNP  
  
  cryptographic-algorithm md5 i  
1  
Ac
```

R2

R4

R5

```
!
!
!
interface Loopbackd
 ip address 10.10.5.5 255.255.255.255
 ip ospf 1 area 1
!
interface Loopbackl
 ip address 172.16.5.5 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.35.5 255.255.255.0
 ip ospf authentication key chain CCNP
 ip ospf 1 area 0 duplex auto r
interface EthernetO/1
 ip address 172.16.45.5 255.255.255.0
 ip ospf 1 area 1
 ip ospf cost 60 duplex auto ■
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3 no ip
 address
```

R2 R4 R5

```
!
router ospf 1
 redistribute connected subnets route-map to-ospf
 passive-interface default
 no passive-interface Ethemet0/0 no passive-inter face EthemetO/1
```

```
ip forward-protocol nd
|
no ip http server
no ip http secure-server
ipv6 ioam timestamp
route-map to-ospf permit 10 match interface Loopback1

control-plane
| [
!
line con 0
 acn
 logging synchronous
Line aux Q
```

Activate Window
Go to Settings co

**Answer: See the solution
below in Explanation.**

Explanation:

```
R4
Int range et0/0 – 1
Ip ospf authentication message-digest
Ip ospf message-digest-key 1 md5 CCNP
```

```

Router ospf 1
Redistribute connected subnets route-map to-ospf metric-type 1
Copy run start

```

```

R5
Int range et0/0 – 1
Ip ospf authentication message-digest
Ip ospf message-digest-key 1 md5 CCNP

```

```

Interface eth 0/1
Ip ospf cost 10
Copy run start

```

VERIFICATION:-

```

R2#show ip ospf nei
R2#show ip ospf neighbor

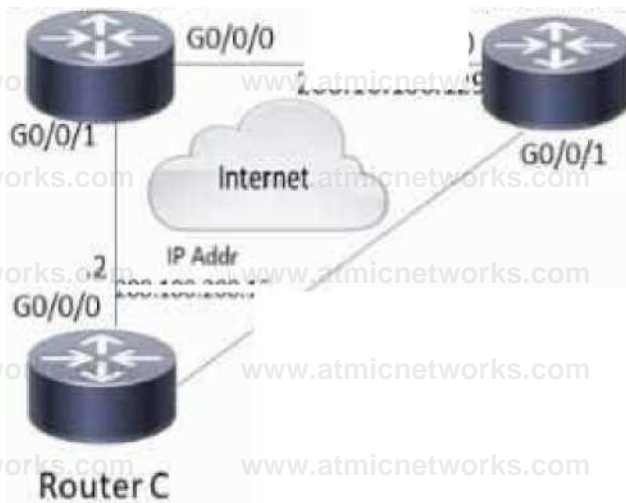
Neighbor ID      Pri   State           Dead Time   Address
Interface
10.10.1.1        1    FULL/BDR        00:00:38   10.10.12.1
theme t0/2
10.10.3.3        1    FULL/BDR        00:00:30   r i \ IQ.10I. 23c3\ E Go io
themetO/I
R2#

```

A black screen with white text AI-generated content may be incorrect. Graphical user interface, text, application Description automatically generated

Question: 406

Refer to the exhibit.



Router A

Network

190.100.200.220

Router B

Network

200.10.1
200.10.2

GO/O/

200.10:100.1

Refer to the exhibit. An engineer configures a hub-and-spoke SD-WAN topology with the requirement that traffic from router A branch to router B branch is guaranteed to flow through the network hub, router C. Which configuration meets the requirement for router A?

policy

COO 100

lists

prefix-list branch-B

In.*Mw#v 'inn <n eTe t \ni

match route

prefix-list branch-b

site-id 20

action accept

set tloc 200 10.100 129 color gold encap ipsec

apply-policy

site branch-b control-policy hub-n-spoke out

policy

lists

prefix-list branch-B

.p-prefix 200.10 172 0/27

site-list branch-A

site-rd 10

control-policy hub-n-spoke

sequence 10

match route

prefix-list branch-b

site-id 20

action accept

set tloc 200 100 200 129 color gold encap ipsec apply-policy

site branch-A control-policy hub-n-spoke out

oasdi drata p|o8 JOJOS 631 002 001 003 **|* >“

iddCCC UOQQC

03 p>-aiis qnpuuq isii-xyaxi

amoj qsjciu

01 acuanbas aipda-u-qnq Aoi|od-|aj|uoc

01 PhWS y qouejq isif-aus ZMrZZIOtOOZxa®*^! g-qouaq isil-*ijajd 'i'll

Ab||od

mo aHods-u-qnq Aogod-pAuoo q-qouuq «q* Aoifod-Aiddc idaooc uonoc

02 P' «'S q-qouuq mi-xyaxl ainoj qsicui 01, aouanbas a^ods*u*qnij

A3i|od-|ouuio3 0l Chaus V qouwq istf-aus

22/0 20 0 k002 xyaxMi Q'lpucjq is^iyaid n«ll Aoipd

A. Option A B. Option B C. Option C D. Option D

Answer: D

Explanation:

Question: 407

An engineer is modifying an existing data policy for VPN 115 to meet these additional requirements: When browsing

government websites, the traffic must use direct internet access.

The source address of the traffic leaving the site toward the government websites must be set to an IP range associated with the country itself, a particular TLOC.

The policy configuration is as follows:

```
vpn 0
 interface eeOO.100
   ip address 198.51.100.2/30 nat
   !
   tunnel-interface
     encapsulation ipsec
     color biz-internet
     mtu 1496
     no shutdown

 interface geO*1.10
   ip address 1Q.254.2M.2.30
   1
   tunnel-interface
     encapsulation ipsec
     color phvotel
     mtu 1496
     no shutdown
   ip route 0.0.0.0/0 198.51.100.1
   ip route 0.0.0.0/0 10.254.254.1
```

Which policy sequence meets the requirements without interfering with other destinations?

A.

```
sequence 30
 match
 destination-data-prefix-list GOVERNMENT-WEBSITES
 !
 action accept
 set
 local-tloc-list
 color biz-internet
```

B.

```
sequence 25
 match
 destination-data-prefix-list GOVERNMENT-WEBSITES
 action accept
 nat use-vpn 0
```

C.

```
sequence 15
 match
 source-data-prefix-list GOVERNMENT-WEBSITES
 action accept
 set
 local-tloc-list
 color private1
```

D.

```
sequence 15
 match
 destination-data-prefix-list GOVERNMENT-WEBSITES
 !
 action accept
 set local-tloc-list
```

color biz-internet

Answer: D

Explanation:

Question: 408

What is the function of the AppNav Controller in the Cisco SD-WAN AppNav solution?

- A. It accelerates specific traffic based on preconfigured policies.
- B. It provides information about configured optimization policies on SD-WAN edge devices.
- C. It provides configuration and monitoring for WAAS nodes.
- D. It intercepts and distributes network traffic based on configured policies.

Answer: D

Explanation:

Question: 409

How many vManage NMSs should be installed in each domain to achieve scalability and redundancy?

- A. two instances
- B. two clusters
- C. three or more in a cluster
- D. two or more in a cluster

Answer: C

Explanation:

Question: 410

Which component of the Cisco SD-WAN network assures that only valid customer nodes are participating in the overlay network?

- A. vBond
- B. vManage
- C. vSmart
- D. WAN Edge

Answer: A

Explanation:

Question: 411

Which type of route represents prefixes received from a local site via an SD-WAN Edge router in a Cisco SD-WAN architecture?

- A. TLOC routes
- B. Service routes
- C. Multicast routes
- D. vRoutes

Answer: D

Explanation:

Question: 412

How many cloud gateway instance(s) can be created per region when provisioning Cloud OnRamp for Multicloud from AWS in a multiregion environment?

- A. one
- B. two
- C. three
- D. four

Answer: B

Explanation:

Question: 413

Which value of the IPsec rekey timer must be set by the engineer for an OMP graceful restart value set for 24 hours?

- A. 6 hours
- B. 12 hours
- C. 36 hours

D. 48 hours

Answer: C

Explanation:

Question: 414

Which behavior describes a WAN Edge router running dual DIA when its DPI engine has identified a cloud SaaS application?

- A. Application traffic flows are routed over best performing DIA circuit, which makes the routing decision based on the best performing path.
- B. The gateway WAN Edge router DPI engine accepts the DNS query for SaaS applications, and DNS queries for noncloud applications follow the explicit path.
- C. Existing flows change the path and drop the traffic when the performance of the chosen path degrades.
- D. The WAN Edge DPI engine never selects a subperforming DIA circuit for the first application, and the WAN Edge router finds the SaaS application.

Answer: A

Explanation:

Question: 415

Which statement describes the requirement of integrating a secure internet gateway (SIG) with a Cisco SD-WAN Edge device?

- A. Attached to SIG tunnels, trackers monitor the respective SIG endpoints.
- B. Credentials for a smart account are required.
- C. A Cisco umbrella organization ID is needed to establish the SIG.
- D. Based on routing or policy, all customer internet traffic must be forwarded to the SIG.

Answer: B

Explanation:

Question: 416

Which two types of SGT propagation are supported by Cisco TrustSec? (Choose two.)

- A. reconciliation

B. SXP

C. offline tagging

D. key chain

E. inline tagging

Explanation:

Answer: B, E

Question: 417

Which attribute identifies the type of a vRoute?

A. tag

B. encapsulation

C. originator

D. origin

Answer: D

Explanation:

Question: 418

An engineer must advertise OSPF-learned routes and modify the update interval for route filtering by TLOC color to 300 on an SD-WAN device. Which configuration accomplishes this task?

```
address-family ipv4 advertise ospf external tloc-color-cap-update-interval 300
```

```
omp
```

```
address-family ipv4 advertise ospf external tloc-color-ca-update-interval 300
```

```
omp
```

```
timers
```

tloc-color-cap-update-Interval 300 exit
address-family ipv4
advertise ospf external

leujepce jdso
esrpeapp

MX®

00£)eAJe4ui-ejepdn-dB3-JO|o>ooB

SJdWU

FAd| A||ujpj-
sseippe

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Question: 419

How does the Cisco SD-WAN Cloud OnRamp solution rate the performance of a SaaS application from a branch office to the cloud via a given path?

- A. It computes a quality-of-experience score.
- B. It monitors the packet loss of priority queues.
- C. It counts the number of interface errors.
- D. It measures the delay and jitter of the path.

Answer: A

Explanation:

Question: 420

The branch users of an organization must be prevented from accessing malicious destinations, and the local files on users' systems must be protected from malware. Which two Cisco products must the organization deploy?

(Choose two.)

A. Cisco Stealthwatch

B. Cisco Umbrella

C. Cisco AMP

D. Cisco Cloudlock

E. Cisco SecureX

Answer: B, C

Explanation:

Question: 421

Which component is responsible for creating and maintaining the secure DTLS/TLS connection on the vSmart controller?

A. SNMP

B. vdaemon

C. NETCONF

D. OMP

Answer: B

Explanation:

Question: 422

What are the two requirements for plug-and-play provisioning on Cisco IOS XE SD-WAN devices?

(Choose two.)

A. The gateway router for the WANEdge device must be able to reach devicehelper.cisco.com.

B. The gateway router for the WANEdge device must be able to reach public DNS servers.

C. The gateway router for the WANEdge device must be able to reach ztp.viptela.com.

D. Devices at branch offices must be able to reach the Cisco SD-WAN vSmart controller at the headquarters site.

E. The WAN Edge device must have a valid certificate.

Answer: D, E

Explanation:

Question: 423

Which Cisco SD-WAN feature propagates packets with SGTs through the network?

- A. TrustSec Inline Tagging
- B. SGT Enforcement
- C. QoS
- D. SXP

Answer: A

Explanation:

Question: 424

Which compression algorithm does DRE use in a Cisco SD-WAN environment?

- A. run-length encoding
- B. Lempel-Ziv-Welch encoding
- C. Ziv Huffman encoding
- D. Huffman encoding

Answer: B

Explanation:

Question: 425

Refer to the exhibit.

PEER LOCAL	PEER REMOTE	PEER REPEAT	SITE	DOMAIN	PEER PRIVATE	PEER PUBLIC	PEER LOCAL COLOR		
TYPE	PROTOCOL	SYSTEM IP	ID	ID	PRIVATE IP	PORT	PUBLIC IP	PORT	LOCAL COLOR
STATE	ERROR	ERROR	COUNT	DOWNTIME					
vbond	dtls		0	0	189.1.11.40	12346	189.1.11.40	12346	his-internet
tear_down		CYORONHIS	NOERR	110	2020-01-01T01:10:20+0000				

Refer to the exhibit. Which issue is shown, and which action must an engineer take to resolve the issue?

- A. An IPsec issue; verify and resolve the tunnel configurations on devices.

- B. An organization name issue; verify and correct the configuration on the devices.
- C. A certificate issue; verify and correct the certificate attributes.
- D. A connectivity issue; verify and resolve the reachability to the controller.

Answer: B

Explanation:

Question: 426

Which protocol is used by the REST API to communicate with network devices in the Cisco SD-WAN network?

- A. SSL
- B. IPsec
- C. SSH
- D. HTTP

Answer: D

Explanation:

Question: 427

A network engineer sets tags in OMP for routes that were originated in the Service VPN. Which monitoring tab must be used to verify tags on the next hop?

- A. Realtime > OMP Received TLOCs
- B. Troubleshooting > Simulate Flows
- C. Realtime > OMP Received Routes
- D. Troubleshooting > Tunnel Health

Answer: B

Explanation:

Question: 428

What are the two advantages of configuration groups in a Cisco SD-WAN deployment? (Choose two.)

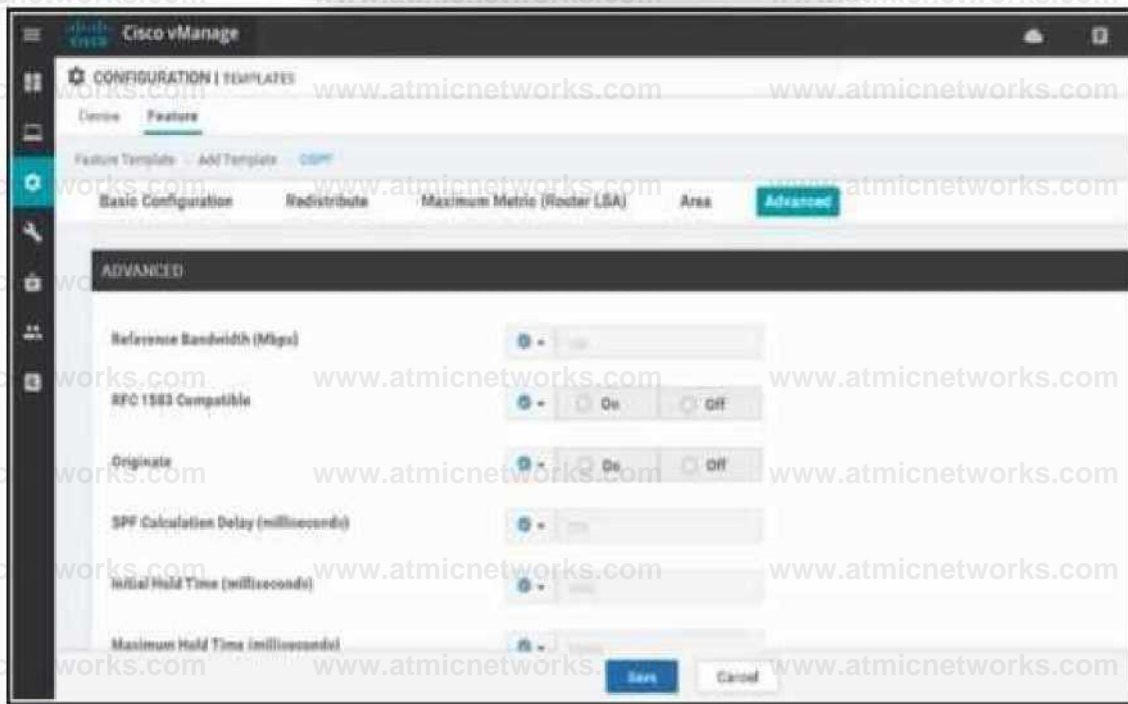
- A. Individual devices are associated with a configuration group and a device template.
- B. Individual devices are added to multiple groups.
- C. Individual devices are grouped based on a shared configuration.
- D. A subset of devices is identified with tags.
- E. An individual device has multiple tag rules.

Answer: C, D

Explanation:

Question: 429

Refer to the exhibit.



Refer to the exhibit. A network administrator is configuring OSPF advanced configuration parameters from a template using the vManager GUI for a branch WAN Edge router to calculate the cost of summary routes to an ASBR.

Which action achieves this configuration?

- A. Enable Originate.
- B. Disable Originate.
- C. Enable RFC 1583 Compatible.
- D. Disable RFC 1583 Compatible.

Answer: C