Free Questions for 300-415 by certsdeals

Shared by Grimes on 22-07-2024

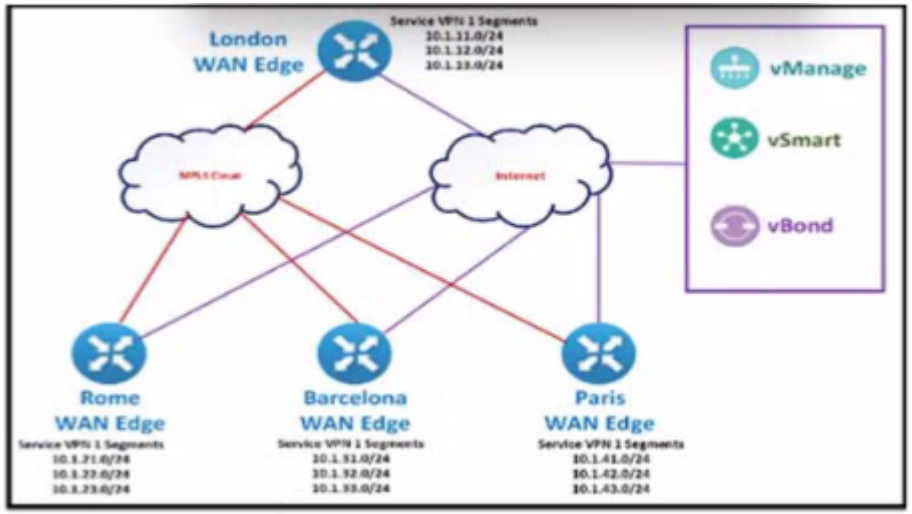
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

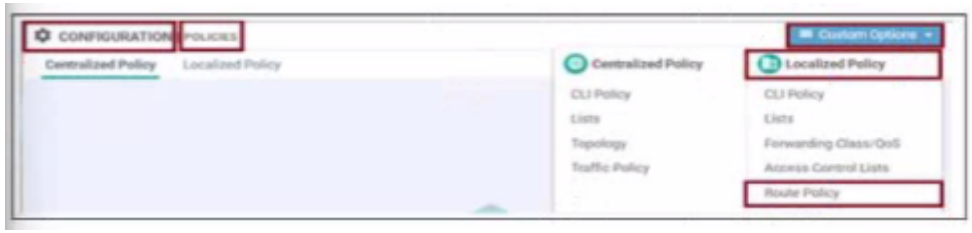
Question Type: MultipleChoice

Exhibit.



The SD-WAN network is configured with a default full-mash 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)


CONFIGURATION
POLICIES
Custom Options
Centralized Policy
Localized Policy
Centralized Policy
CLI Policy
Lists
Topology
Traffic Policy
Localized Policy
CLI Policy
Lists
Forwarding Class/QoS
Access Control Lists
Route Policy

B)


CONFIGURATION
POLICIES
Custom Options
Centralized Policy
Localized Policy
Centralized Policy
CLI Policy
Lists
Topology
Traffic Policy
Localized Policy
CLI Policy
Lists
Forwarding Class/QoS
Access Control Lists
Route Policy

C)

D)

Options:

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.

1.Understanding the Policy Requirements:

oCentralized 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.

oRoute Policy: Specifically, a route policy will be used to set the preferred path for traffic between sites, ensuring that it passes through London.

1.Option Analysis:

oOption A: Shows the configuration of a centralized policy with a focus on route policy, which is necessary to achieve the desired traffic flow manipulation.

oOther Options: Do not provide the necessary centralized policy or route policy configurations that are needed to control the routing paths between the sites.

1.Configuration Details:

oCentralized Policy: Define the policy under the centralized policy section in the vManage GUI.

oRoute Policy: Create and apply a route policy that specifies the desired routing behavior for traffic between Barcelona and Paris, ensuring it routes through London.

1.Reference:

oCisco SD-WAN Control Policy Configuration Guide

Cisco SD-WAN Centralized Policy Documentation

Question 2

Question Type: MultipleChoice

What is a requirement for deployment of on-premises vBond controllers through the Cisco Plug and Play Connect process?

Options:

A- a DNS name that identifies vBond

B- a defined controller profile

C- Internet connectivity from vManage

D- a CSV The that contains ail 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.

1.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.

1.Process:

oWhen a device comes online, it contacts the Plug and Play server to get the necessary information for connecting to the SD-WAN fabric.

oThe DNS name is used to resolve the vBond's IP address, enabling secure and reliable communication between the device and the vBond orchestrator.

1.Reference:

oCisco SD-WAN Plug and Play Connect Deployment Guide

oCisco SD-WAN vBond Orchestrator Configuration Documentation

Question 3

Question Type: **MultipleChoice**

Which two architectural components are part of an SD-WAN high availability vManage cluster? (Choose two.)

Options:

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.

1.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.

1.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.

3.Reference:

oCisco SD-WAN vManage Cluster Deployment Guide

oCisco SD-WAN High Availability Configuration Documentation

Question 4

Question Type: **MultipleChoice**

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)

B)

```
policy data-policy Srvc_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
```

C)

```
policy data-policy Srvc_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 Srvc_Plane_NAT
 vpn-list VPN1
  sequence 10
   match source-ip 10.0.0.1/32
   !
   action accept
    nat use-vpn 0
   !
  !
  default-action accept
 !
```

Options:

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.

1.NAT Configuration:

oSource 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.

oData Policy: A data policy must be created that matches the source IP addresses and applies the NAT pool to translate these addresses.

1.Option A Analysis:

oPolicy 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.

oInterface 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.

1.Reference:

oCisco SD-WAN NAT Configuration Guide

Question 5

Question Type: **MultipleChoice**

Which data policy configuration influences BGP routing traffic flow from LAN to WAN?

A)

```
policy
 route-policy BGP-AS-PREPEND
  sequence 10
   action accept
    set
     as-path prepend 10, 20
  !
  default-action accept

vpn 10
   router
     ospf
        route-policy BG-AS-PREPEND in
```

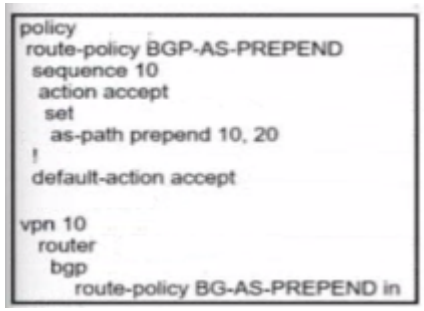
B)

```
policy
 route-policy BGP-AS-PREPEND
  sequence 10
   action deny
    set
     as-path prepend 10, 20
  !
  default-action accept

vpn 10
   router
     bgp
        route-policy BG-AS-PREPEND out
```

C)

```
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 out
```

D)



Options:

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.

1.AS-Path Prepending:

oAS-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.

oThis can be useful in directing traffic to take a different path by making certain routes appear longer.

1.Option C Analysis:

oPolicy Definition: The policy named BGP-AS-PREPEND includes a sequence that sets the AS-path to prepend the AS numbers 10 and 20.

oApplication: 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.

oThis ensures that the traffic flow from the LAN to the WAN is influenced by the AS-path prepending, making certain paths less preferred.

1.Reference:

oCisco SD-WAN Routing Configuration Guide

oCisco SD-WAN BGP Policy Configuration Documentation

Question 6

Question Type: **MultipleChoice**

Which TLOC color is used for site-to-site communication in a Google Cloud integration with Cisco SD-WAN?

Options:

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.

1.TLOC Color Assignment:

oFor 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.

1.Private1 for Site-to-Site Communication:

oThe 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.

1.Reference:

oCisco SD-WAN Cloud Integration Guide

oCisco SD-WAN Google Cloud Configuration Documentation

Question 7

Question Type: **MultipleChoice**

Which configuration allows VPN 10 traffic to have direct internet access locally from the WAN Edge device?

A)

```
policy                                  vpn 10
 data-policy DPI                         !
  vpn-list vpn10                         site-list Remote
   sequence 10                           site-id 14
    !                                    !
     action accept                      !
     nat use-vpn 0                     !
   default-action accept                apply-policy
  !                                      site-list Remote
  cflowd-template CFLOWD                 data-policy DPI from-service
 !                                       cflowd-template CFLOWD
 lists
  vpn-list vpn10                        vpn 10
                                        ip route 0.0.0.0/0 vpn 0
```

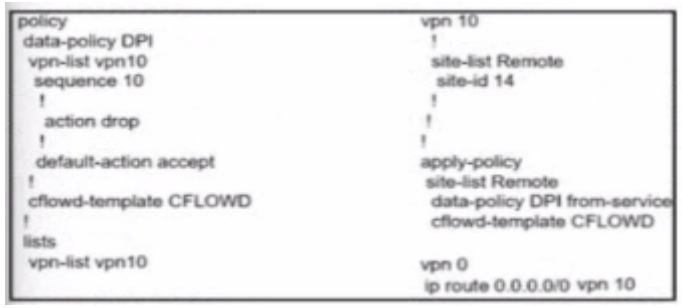
B)

```
policy                                  vpn 10
 data-policy DPI                         !
  vpn-list vpn10                         site-list Remote
   sequence 10                           site-id 14
    !                                    !
     action accept                      !
    !                                   !
   default-action accept                apply-policy
  !                                      site-list Remote
  cflowd-template CFLOWD                 data-policy DPI from-service
 !                                       cflowd-template CFLOWD
 lists
  vpn-list vpn10                        vpn 0
                                        ip route 0.0.0.0/0 vpn 10
```

C)

```
policy                                  vpn 10
 data-policy DPI                         !
  vpn-list vpn10                         site-list Remote
   sequence 10                           site-id 14
    !                                    !
     action drop                        !
    !                                   !
   default-action                       apply-policy
  !                                      site-list Remote
  cflowd-template CFLOWD                 data-policy DPI from-service
 !                                       cflowd-template CFLOWD
 lists
  vpn-list vpn10                        vpn 10
                                        ip route 0.0.0.0/0 vpn 0
```

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
```

Options:

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.

1.Policy Configuration:

oNAT 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.

oApply Policy: The policy should be applied in the outbound direction to the appropriate interface that connects to the internet.

1.Option A Analysis:

oThis 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.

oThe apply-policy command is correctly used to apply the policy to the site list and the data-policy DPI from-service.

1.Reference:

oCisco SD-WAN NAT Configuration Guide

Cisco SD-WAN Direct Internet Access (DIA) Configuration Documentation

Question 8

Question Type: **MultipleChoice**

Which control policy assigned to Drenches in the out direction establishes a strict hub-and-spoke topology tor VPN2?

A)

```
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
```

B)

```
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 branch_sites
   vpn-list VPN2
  !
  action accept
   set
    tloc 1.1.1.1 color red
  !
 !
!
default-action accept
```

C)

```
policy
 lists
  vpn-l
   vpn ist VPN2
  !      2
site-lis
 site-id t hub_sites
 !       l 1-2
!
contro
 sequel-policy vpn_multi-topology
  matcInce 10
   site-h route
   vpn-list hub_sites
  !      list VPN2
  actio
 !       n accept
  sequ
   matcence 20
   !      h route
   actio
!        n reject
defaul
         t-action accept
```

D)

```
policy
 lists
  vpn-list VPN2
   vpn 2
  !
site-list branch_sites
 site-id 1-100
 !
!
control-policy vpn_multi-topology
 sequence 10
  match route
   site-list branch_sites
   vpn-list VPN2
  !
  action accept
   set
    tloc 100.1.1.1 color mpls
  !
 !
!
default-action accept
```

Options:

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.

1.Control Policy Components:

oSite Lists: Define which sites are considered hubs and which are branches.

oVPN Lists: Identify the VPNs to which the policy applies.

oControl Policy: Use sequences to match routes and specify actions to accept or reject traffic based on the defined topology.

1.Policy Analysis:

oOption 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.

oOther options either incorrectly define the site lists or do not properly match and set the routes to enforce the strict hub-and-spoke topology.

1.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

1.Reference:

oCisco SD-WAN Control Policy Configuration Guide

oCisco SD-WAN Hub-and-Spoke Topology Deployment Guide

Question 9

Question Type: MultipleChoice

What do receivers request to join multicast streams in a Cisco SO-WAN network?

Options:

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.

1.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.

1.Process:

oWhen a multicast receiver wants to join a multicast stream, it sends an IGMP join request.

oThe WAN Edge device forwards this request to the vSmart controller.

oThe vSmart controller then updates the multicast service routes to include the new receiver, ensuring that multicast traffic is appropriately forwarded to the joining receiver.

1.Reference:

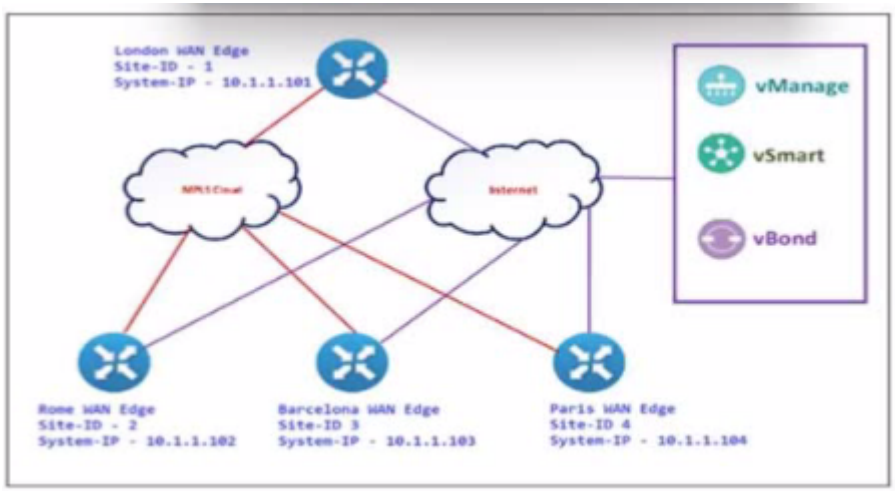
oCisco SD-WAN Multicast Configuration Guide

oCisco SD-WAN vSmart Controller Documentation

Question 10

Question Type: **MultipleChoice**

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-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
```

B)

```
policy
 lists
  tloc-list TLOC-1
   tloc 10.1.1.103 color mpls encap ipsec preference 500
   tloc 10.1.1.103 color biz-internet encap ipsec preference 400
```

C)

```
policy
 lists
  tloc-list TLOC-1
   tloc 10.1.1.101 color mpls encap ipsec preference 500
   tloc 10.1.1.101 color biz-internet encap ipsec preference 400
```

D)

```
policy
 lists
  tloc-list TLOC-1
   tloc 10.1.1.104 color mpls encap ipsec preference 500
   tloc 10.1.1.104 color biz-internet encap ipsec preference 400
```

Options:

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 biz-internet as a backup, the policy must be set correctly to define the preference for each transport link.

1.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.

1.Policy Configuration Analysis:

oOption 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).

oOther options either repeat the TLOC configuration incorrectly or reference wrong system IPs.

1.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

1.Reference:

oCisco SD-WAN Policy Framework Guide

oCisco SD-WAN Transport Locator Configuration Documentation

Question 11

Question Type: MultipleChoice

Which VPNs must be configured outside the workflow to complete the SD-WAN overlay setup when using the Quick Connect workflow?

Options:

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.

1.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.

1.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.

1.Reference:

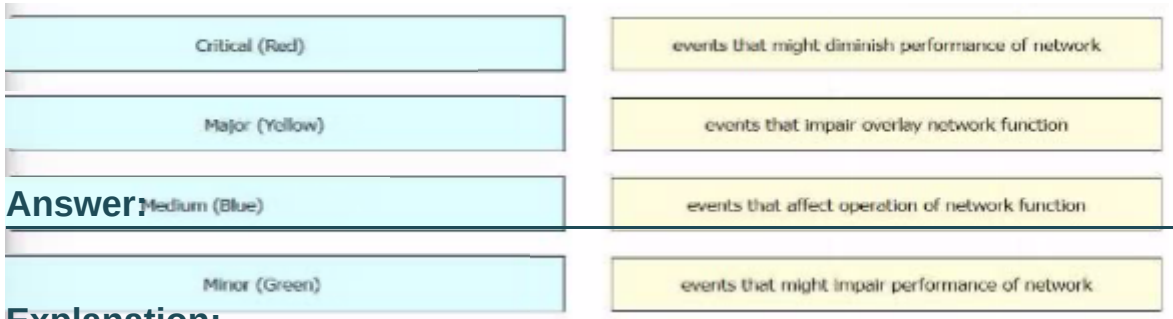
oCisco SD-WAN Quick Connect Guide

oCisco SD-WAN Management and Monitoring Guide

Question 12

Question Type: **DragDrop**

Drag and drop the alarm slates from the left onto the corresponding alarm descriptions on the right.



Answer:

Explanation:

*Cisco SD-WAN Monitoring and Troubleshooting Guide

*Cisco vManage Alarm Severity Levels Documentation