- **Vendor: Cisco**
- **Exam Code: 300-415**
- **Exam Name: Implementing Cisco SD-WAN Solutions (ENSDWI)**
- **New Updated Questions from Braindump2go (Updated in Jan/2021)**

QUESTION 1
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 2
Which configuration step is taken on vManage after WAN Edge list is uploaded to support the on-boarding process before the device comes online?

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

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

QUESTION 3
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. vSmart
C. WAN Edge
D. Firewall

Answer: B

QUESTION 4
Which command verifies a policy that has been pushed to the vEdge router?

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

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

QUESTION 5
Which policy configures an application-aware routing policy under Configuration > Policies?

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

Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/application-aware-routing.html
“An application-aware routing policy is a type of centralized data policy: you configure it on the vSmart controller, and the controller automatically pushes it to the affected Cisco SD-WAN devices”.

QUESTION 6
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-list VPN 1
  vpn 10
  vpn 20
 !
!
 vpn-membership disallow-vpn 1
   sequence 10
    match
     vpn-list VPN 1
    !
    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
   !
  !
  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
   !
  !
  default-action accept
```

D.
```
policy
   lists
    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
```

Answer: C
Explanation:
https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_17.2/04Segmentation/03Segmentation_(VPN)_Configuration_Examples

QUESTION 7
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. localized data
B. centralized control
C. localized control
D. centralized data

Answer: D
Explanation:
Centralized data policy: policy that is configured on a Cisco vSmart Controller (hence, it is centralized) and that affects data traffic being transmitted between the routers on the Cisco
SD-WAN overlay network. They affect traffic flow across the entire network. This will also help in controlling to send specific application traffic over specific tunnel based on jitter, delay, latency.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html

QUESTION 8
When VPNs are grouped to create destination zone, how many zones can a VPN be part of?

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

Answer: C
Explanation:
https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/Enterprise_Firewall_with_Application_Awareness

QUESTION 9
Which scheduling method is configured by default for the eight queues in the cloud vEdge router?

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

Answer: A
Explanation:
https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.1/06Policy_Basics/05Localized_Data_Policy/Configuring_Localized_Data_Policy_for_IPv4

QUESTION 10
At which layer does the application-aware firewall block applications on a WAN Edge?

A. 3
B. 5
C. 2
D. 7

Answer: D

QUESTION 11
What is a benefit of the application-aware firewall?

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

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

QUESTION 12
Refer to the exhibit. Which QoS treatment results from this configuration after the access list acl-guest is applied inbound on the vpn1 interface?

```
policy
 policer ccnp
  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 ccnp
 !
!
default-action drop
```

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

QUESTION 13
Which configuration changes the packet loss priority from low to high?

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

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

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

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

Answer: D
Explanation:
We change the PLP from low to high (configured by the policer exceed remark command).
https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=546

QUESTION 14
Which software security feature is supported by the Cisco ISR 4451 router?

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

Answer: C

QUESTION 15
Which two mechanisms are used to guarantee the integrity of data packets in the Cisco SD-WAN architecture data plane? (Choose two.)

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

Answer: CD
Explanation:
The data plane provides the infrastructure for sending data traffic among the vEdge routers in the Viptela overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The Viptela data plane implements the key security components of authentication, encryption, and integrity in the following ways:
+ Authentication – As mentioned above, the Viptela control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:
++ RSA encryption with 2048-bit keys.
++ Two standard protocols from the IPsec security suite framework, Encapsulation Security Payload (ESP) and Authentication Header (AH), are used to authenticate the origin of data traffic.
Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/01Security_Overview/Data_Plane_Security_Overview