EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

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. vSmart

C. vManage

D. vBond

Suggested Answer: *B*
Reference: https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/migration-guide/cisco-sd-wan-migration-guide.pdf

Community vote distribution
B (100%)

AJMD Most Recent 3 years ago
vSmart
upvoted 1 times

eric0430 3 years, 5 months ago
Do not buy from this website, this is a scam!
upvoted 3 times

Speirsington 4 years, 6 months ago
vSmart
upvoted 2 times

mimo1000 4 years, 11 months ago
The vSmart controller is the brain of the overlay network, establishing, adjusting, and maintaining the connections that form the fabric of the overlay network. In these functions, it oversees the control plane of the Cisco SD-WAN overlay network. The vSmart controller participates only in the overlay network and has no direct peering relationships with any of the devices that an edge router is connected to on the host-facing side.
upvoted 3 times

CCNPWILL 5 years, 3 months ago
First answer and question goes to me. Ive been studying this exam for about a month. Ive read the 13 chapters in the official press book and watched the udemy video for this exam. I also happen to be hands on with this technology. I'm not saying I know all the answers. I'm just doing my best here. Happy studies and good luck! oversees the control plane <<< vSmart. if you see control plane with NAT-T, think vBond.
upvoted 3 times

Question #2 *Topic 1*

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

A. ISR4000 series

B. ISR9300 series

C. vEdge-1000 series

D. ASR9000 series

E. ASR1000 series

Suggested Answer: *A, E*

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

Community vote distribution

AE (100%)

JoSharp Most Recent 1 year, 6 months ago

B,C,D is wrong answer, so the correct answer is A and E

upvoted 1 times

ManjeshM 1 year, 8 months ago

Options A & E are the correct answers. ASR-1K & ISR-4K platforms from the list.

upvoted 1 times

AJMD 3 years ago

Correct

upvoted 1 times

1984wolf 3 years, 1 month ago

The two hardware platforms that support Cisco IOS XE SD-WAN images are:

A. ISR4000 series B. ISR9300 series

Therefore, the correct answers are A. ISR4000 series and B. ISR9300 series.

upvoted 1 times

1984wolf 3 years, 1 month ago

The two hardware platforms that support Cisco IOS XE SD-WAN images are: A. ISR4000 series B. ISR9300 series Therefore, the correct answers are A. ISR4000 series and B. ISR9300 series.no such thing as an ISR 9300.

upvoted 1 times

colipto Highly Voted 3 years ago

no such thing as an ISR 9300.

upvoted 5 times

winder 4 years, 1 month ago

This question is asking which IOS XE SD-WAN images are supported, so it should fall into one of the following categories: 1. ISR/ASR/C8000/IR 2. ENCS 3. vEdge Cloud & CSR 1000v vEdge-1000 (or similar) is running Viptela OSWhat is your answer, please?

upvoted 2 times

winder 4 years, 1 month ago

This question is asking which IOS XE SD-WAN images are supported, so it should fall into one of the following categories: 1. ISR/ASR/C8000/IR 2. ENCS 3. vEdge Cloud & CSR 1000v vEdge-1000 (or similar) is running Viptela OS

upvoted 2 times

LanreDipeolu 2 years, 11 months ago

What is your answer, please?

upvoted 1 times

Mr_Cipher 5 years, 1 month ago

That's correct. Also, the new Cisco Catalyst 8X00 Series Edge Platforms do support.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/install-upgrade-17-2-later.html

upvoted 1 times

CCNPWILL 5 years, 3 months ago

i believe this is correct.

upvoted 3 times

Question #3 *Topic 1*

What is a default protocol for control plane connection?

A. HTTPS

B. TLS

C. IPsec

D. DTLS

Suggested Answer: *D*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/05Security/02Configuring_Security_Parameters

Community vote distribution

D (100%)

Aldebeer Most Recent 1 year, 9 months ago

DTLS is the right one

upvoted 2 times

Aldebeer 1 year, 9 months ago

OMP runs inside the DTLS

upvoted 1 times

eric0430 2 years, 5 months ago

Do not buy from this website, this is a scam!

upvoted 1 times

EGD 3 years, 8 months ago

If it is the correct answer - I like it when it is confirmed. It's possible that an answer is not confirmed because everyone is unsure - I assume that when there is no comment.

upvoted 2 times

mimo1000 3 years, 11 months ago

if it is the right answer why do you have to post something!

upvoted 3 times

Mr_Cipher 4 years, 1 month ago

By default, the control plane uses DTLS as the protocol that provides privacy on all its tunnels. DTLS runs over UDP. https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/05Security/02Configuring_Security_Parameters#:~:text=By%20default%2C%20the%20control%20plane,DTLS%20runs%20over%20UDP.

upvoted 2 times

ramjam 4 years, 2 months ago

TLS is the correct answer.

upvoted 1 times

ramjam 4 years, 2 months ago

TLS is the correct answer.DTLS I mean..

upvoted 1 times

ramjam 4 years, 2 months ago

DTLS I mean..

upvoted 2 times

CCNPWILL 4 years, 3 months ago

Correct

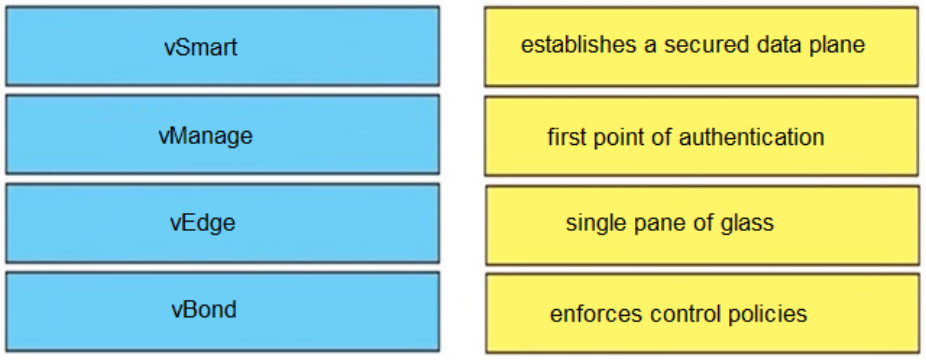
upvoted 3 times

Question #4 *Topic 1*

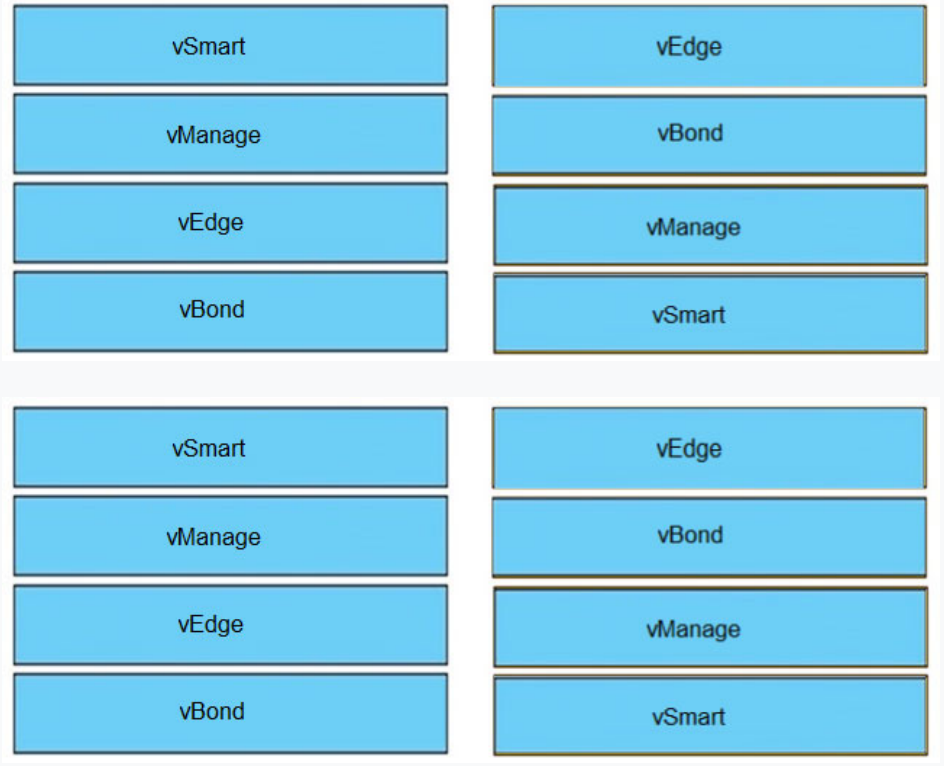
DRAG DROP -

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

Select and Place:



Suggested Answer:



Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/LTRCRS-3550.pdf slide 8

CCNPWILL Most Recent 1 year, 9 months ago

Correct

upvoted 2 times

Question #5 *Topic 1*

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

A. WAN Edge

B. vSmart

C. vBond

D. vManage

Suggested Answer: *C*

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

Community vote distribution

C (100%)

AJMD Most Recent 1 year, 12 months ago

vbond Correct

upvoted 2 times

milan74 4 years ago

Answer C, vBond needs a 1:1 public IP to be reachable for vEdge devices

upvoted 1 times

CCNPWILL 4 years, 3 months ago

Correct

upvoted 3 times

Question #6 *Topic 1*

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

A. ISR 1101

B. ASR 1001

C. CSR 1000v

D. vEdge 2000

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Aldebeer Most Recent 1 year, 9 months ago

one answer - one option

upvoted 1 times

Mr_Cipher 4 years, 1 month ago

The supported model is C1101-4PLTEPWX https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html

upvoted 1 times

CCNPWILL 4 years, 3 months ago

correct. i actually support these routers and the wifi for them full-time.

upvoted 3 times

Question #7 *Topic 1*

Refer to the exhibit. What does the BFD value of 8 represent?

Hostname	State	System IP	Reachability	Site ID	Device Model	BFD	Control
BR1-VEDGE1		10.3.0.1	reachable	300	vEdge Cloud	8	5

A. dead timer of BFD session

B. poll-interval of BFD session

C. hello timer of BFD session

D. number of BFD sessions

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Mfanelo Most Recent 1 year, 10 months ago

D it is.

upvoted 1 times

Alchobashko 3 years ago

correct

upvoted 2 times

CCNPWILL 4 years, 9 months ago

correct

upvoted 2 times

Question #8 *Topic 1*

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

A. DTLS or TLS tunnel with vSmart controller and IPsec tunnel with vBond controller

B. DTLS or TLS tunnel with vBond controller and IPsec tunnel with vManage controller

C. DTLS or TLS tunnel with vBond controller and IPsec tunnel with other WAN Edge routers

D. DTLS or TLS tunnel with vSmart controller and IPsec tunnel with other WAN Edge routers

Suggested Answer: *D*
Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf page 22

Community vote distribution
D (100%)

HAMPI Highly Voted 3 years, 11 months ago
D is the correct answer. 1. VBOND will make only DTLS connection, TLS connection will not happen between vBond and vEdge. 2. vBond connection is temporary 3. vEdges will make IPSec tunnels over data plane
upvoted 7 times

Mfanelo Most Recent 1 year, 10 months ago
I go with D.
upvoted 1 times

khanda 3 years, 9 months ago
vBond will only make a DTLS connection.
upvoted 3 times

akin5 3 years, 11 months ago
dear Team what is the solution to this Q 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?
upvoted 1 times

khanda 3 years, 11 months ago
C is the correct answer, the minimal config on the Edge device contains the vBond IP or DNS name, so first comms would be to the vBond through TLS/DTLS tunnel connection. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.htmlCorrect answer is D. vBond do not utilise TLS but DTLS.
upvoted 1 times

khanda 3 years, 11 months ago
C is the correct answer, the minimal config on the Edge device contains the vBond IP or DNS name, so first comms would be to the vBond through TLS/DTLS tunnel connection. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html
upvoted 1 times

khanda 3 years, 9 months ago
Correct answer is D. vBond do not utilise TLS but DTLS.
upvoted 1 times

serieus 4 years, 6 months ago
Technically C is also correct, but the DTLS tunnel to the vBond is torn down after the Edge receives the vManage & vSmart IP's. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.htmlHave to correct myself. The vBond is locked to DTLS only so C is NOT correct.
upvoted 1 times

serieus 4 years, 6 months ago
Technically C is also correct, but the DTLS tunnel to the vBond is torn down after the Edge receives the vManage & vSmart IP's. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html

upvoted 1 times

serieus 4 years, 6 months ago

Have to correct myself. The vBond is locked to DTLS only so C is NOT correct.

upvoted 2 times

ramjam 4 years, 8 months ago

Correct. https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/05Security/01Security_Overview

upvoted 2 times

CCNPWILL 4 years, 9 months ago

I believe this is correct a well.

upvoted 2 times

Question #9 *Topic 1*

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. vSmart

C. vBond

D. vManage

Suggested Answer: *D*

Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/cisco-sd-wan-certificates-deploy-2020aug.pdf page 14

Community vote distribution

D (100%)

Matt2727 Most Recent 2 years ago

vManage

upvoted 2 times

masaharu 4 years, 11 months ago

Correct.

upvoted 2 times

Question #10 *Topic 1*

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

A. 12344

B. 12345

C. 12347

D. 12346

Suggested Answer: *D*

Reference: https://community.cisco.com/t5/networking-documents/sd-wan-controller-setup-guide-on-prem-non-cloud-managed/ta-p/3921360

Community vote distribution

D (100%)

ManjeshM Most Recent 1 year, 10 months ago

Yes. Port 12346 is the right answer.

upvoted 1 times

AJMD 3 years ago

Correct

upvoted 1 times

CCNPWILL 5 years, 3 months ago

Correct. Straight from the press book.

upvoted 4 times

Question #11 *Topic 1*

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

A. Authenticate and authorize WAN Edge routers.

B. Configure and monitor WAN Edge routers.

C. Distribute route and policy information via OMP.

D. Distribute the IP address from DHCP server to WAN Edge routers.

E. Distribute crypto key information among WAN Edge routers.

Suggested Answer: *C, E*

Reference: https://codingpackets.com/blog/viptela-sdwan-overview/

Community vote distribution

CE (100%)

Aldebeer Most Recent 1 year, 9 months ago

thats all

upvoted 1 times

AJMD 1 year, 12 months ago

Correct

upvoted 1 times

Alchobashko 2 years, 6 months ago

Correct

upvoted 2 times

Question #12 *Topic 1*

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

A. vManage

B. vBond

C. OMP

D. APIC-EM

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

Adenismail Most Recent 2 years, 2 months ago
B. vBond When a WAN Edge device joins the Cisco SD-WAN overlay, the vBond Orchestrator is responsible for orchestrating the connection between the WAN Edge device and a vSmart controller. It authenticates new devices and facilitates their connection to the vSmart Controller, eliminating the need for manual processes
upvoted 1 times

Aldebeer 2 years, 9 months ago
quit agree with mr Chiper
upvoted 1 times

Mr_Cipher 5 years, 1 month ago
Correct. Cisco vBond resides in the orchestration plane. The vBond controller is largely responsible for the Zero-Touch Provisioning process as well as first-line authentication, control/management information distribution, and facilitating Network Address Translation (NAT) traversal.
upvoted 2 times

CCNPWILL 5 years, 3 months ago
Correct . Orchestration = vBond
upvoted 4 times

Question #13 *Topic 1*

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

A. Cloud OnRamp

B. Cloud app

C. vAnalytics

D. Network Designer

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Aldebeer Most Recent 1 year, 9 months ago

cloud-onramp

upvoted 1 times

Mr_Cipher 4 years, 1 month ago

Correct. Cisco SD-WAN Cloud OnRamp for IaaS extends enterprise WAN to public clouds.

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-742817.html

upvoted 3 times

ramjam 4 years, 2 months ago

Correct. - Cisco Software Defined Wide Area Networks (designing, Deploying, and Securing Your Next generation WAN with Cisco SD-WAN) by Joson, Dana Yanch, Dustin Schueman, and John Curran.

upvoted 1 times

CCNPWILL 4 years, 3 months ago

Correct.

upvoted 2 times

Question #14 *Topic 1*

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 instances of vSmart Cloud through the AWS online software store

B. Create GRE tunnels to AWS from each branch over the Internet

C. Install the AWS Cloud Router in the main data center and provide the connectivity from each branch

D. Create virtual WAN Edge devices Cloud through the AWS online software store

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Mr_Cipher Highly Voted 5 years, 1 month ago
Correct. With Cloud OnRamp for IaaS, vManage will automatically deploy SD-WAN edge virtual routers in a transit VPC, acting as virtual aggregation routers. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-742817.html
upvoted 7 times

Adenismail Most Recent 2 years, 2 months ago
C To extend the in-house Cisco SD-WAN branch network into AWS, the network architect can leverage Cisco Cloud onRamp for IaaS. Here's how it works: Cisco SD-WAN Cloud onRamp for IaaS: This solution automates and optimizes secure network connectivity from private network campus and branch locations to Amazon Web Services (AWS) virtual private clouds (VPCs). It streamlines the process and ensures a secure connection between your branches and AWS workloads. Deployment Steps: Verify prerequisites (ensure valid certificates for SD-WAN controllers). Deploy a transit VPC with Cisco Cloud onRamp for IaaS. Discover and map host VPCs to the transit VPC. Monitor Cisco Cloud onRamp for IaaS. Benefits: Fully automated extension of the Cisco SD-WAN fabric to AWS Cloud. Secure connectivity in minutes, replacing manual processes. Seamless integration with AWS workloads
upvoted 1 times

AJMD 3 years ago
Correct D
upvoted 1 times

ramjam 5 years, 2 months ago
correct.
upvoted 3 times

Question #15 *Topic 1*

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

A. Sun Enterprise M4000 Server running Sun Solaris

B. Sun SPARC Node running AIX

C. Cisco UCS

D. HP ProLiant DL380 Generation 10 running HP-UX

E. Cisco ENCS 5000 Series

Suggested Answer: *C, E*

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

Community vote distribution

CE (100%)

Speirsington Most Recent 2 years ago

UCS and ENCS

upvoted 3 times

Question #16 *Topic 1*

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 BGP across the enterprise routing for selecting optimal path

D. Implementation of a modern age core banking system

Suggested Answer: *A*
Official Answer: A

Community vote distribution
B (100%)

FlipCCNP Highly Voted 5 years, 2 months ago
This should be B. Ref below page 51 and 52 https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf
upvoted 18 times

RREVECO Most Recent 1 year, 10 months ago
CORRECT ANSWER "B" very textual and 90% similar to the case study of the link: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf page 51 and 52 and there is a change in: ""The Cisco SD-WAN solution is able to provide: • Quality of Service, including application prioritization and choosing the optimized path based on required SLAs for critical applications. • Circuit remediation for critical traffic, so as to improve the end-user experience for traffic traversing poor quality circuits. • Integration into cloud "SaaS and IaaS" (DOES NOT INDICATE PaaS) providers to offer the best possible application experience""
upvoted 1 times

Roger95 1 year, 10 months ago
- Improve customer experience for applications -Reduce overhead related to compliance and security. -->The chosen solution was a managed service built with Cisco SD-WAN which dramatically improved service delivery and quality of experience. -->Application performance improved due to dynamic SLA-based traffic routing over MPLS, internet, and LTE circuits. https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf (P51,52,53)
upvoted 1 times

KKK_9999 2 years ago
B is correct
upvoted 1 times

Seba_o_s 2 years, 6 months ago
Should be B option
upvoted 1 times

AJMD 3 years ago
B is right
upvoted 1 times

Tayeglow 3 years, 1 month ago
QoS including application prioritization and meeting critical applications SLA for selecting optimal path
upvoted 1 times

densma 3 years, 4 months ago
B is right. A isnt Key feature of cisco SD-WAN
upvoted 1 times

Alchobashko 3 years, 6 months ago
QoS and SLA for critical apps
upvoted 1 times

mumu2018 3 years, 6 months ago

i would go for B, thats the key important factors of SD WAN - Improve customer experience for applications -Reduce overhead related to compliance and security.

upvoted 1 times

Zdrobici 3 years, 7 months ago

should be B

upvoted 1 times

Jonycici 3 years, 8 months ago

B is correct

upvoted 1 times

wcorrea 3 years, 10 months ago

B is correct

upvoted 1 times

ccie_race 4 years ago

The answer should be B because this can be achieved via an SLA class and QoS.

upvoted 1 times

keefe23 4 years, 3 months ago

check this out and find Paas. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.html#Uniquecapabilities

upvoted 1 times

Baio 4 years, 7 months ago

This answer is should be B

upvoted 1 times

Xhizors 4 years, 7 months ago

This answer is should be B

upvoted 1 times

Question #17 *Topic 1*

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 an OSPF feature template to the AWS cloud Edge router template.

B. Attach the ג€AmazonCreateVPCג€ and ג€AmazonProvisionEC2ג€ permission policy to the IAM account.

C. Subscribe to the SD-WAN Edge router AMI in the AWS account.

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.

Suggested Answer: *C, D*

Official Answer: CD

Community vote distribution

CD (100%)

TheNetworkStudent Highly Voted 4 years, 11 months ago

C is confirmed via https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/Cisco_Cloud_onRamp_for_IaaS_AWS_Version2.html Under Procedure 1: " You must subscribe to the Cisco SD-WAN Edge router Amazon machine images (AMIs) in your account within the AWS Marketplace." D is confirmed via the Exam Guide or the Procedure 3 in the previous link. Exam Guide: "Configure a device template for the Cisco WAN Edge Cloud routers that will be used within the transit VPC" After this the guide specifies that you also need to deploy the template which I'm guessing also means "attach"ing it. So it's C & D

upvoted 8 times

Matt2727 Most Recent 2 years, 1 month ago

Agreed C & D

upvoted 1 times

pepegaston2021 3 years, 10 months ago

Yes its correct

upvoted 1 times

amitsir 4 years, 9 months ago

yes C and D

upvoted 1 times

Question #18 *Topic 1*

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

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

Matt2727 Most Recent 2 years, 1 month ago

B, vSmart

upvoted 1 times

Scav20 4 years ago

B is the correct answer

upvoted 1 times

Speirsington 4 years, 6 months ago

vSmart

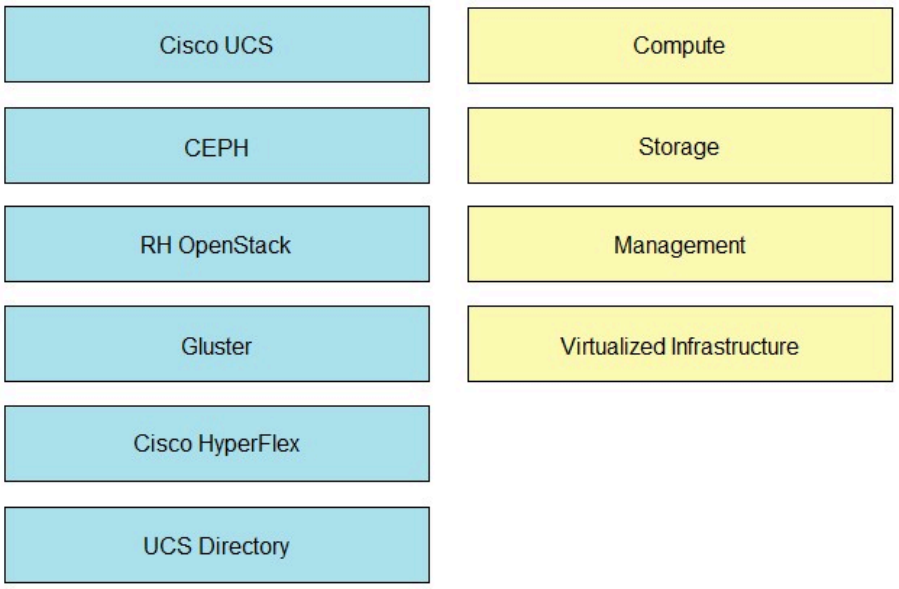
upvoted 1 times

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.

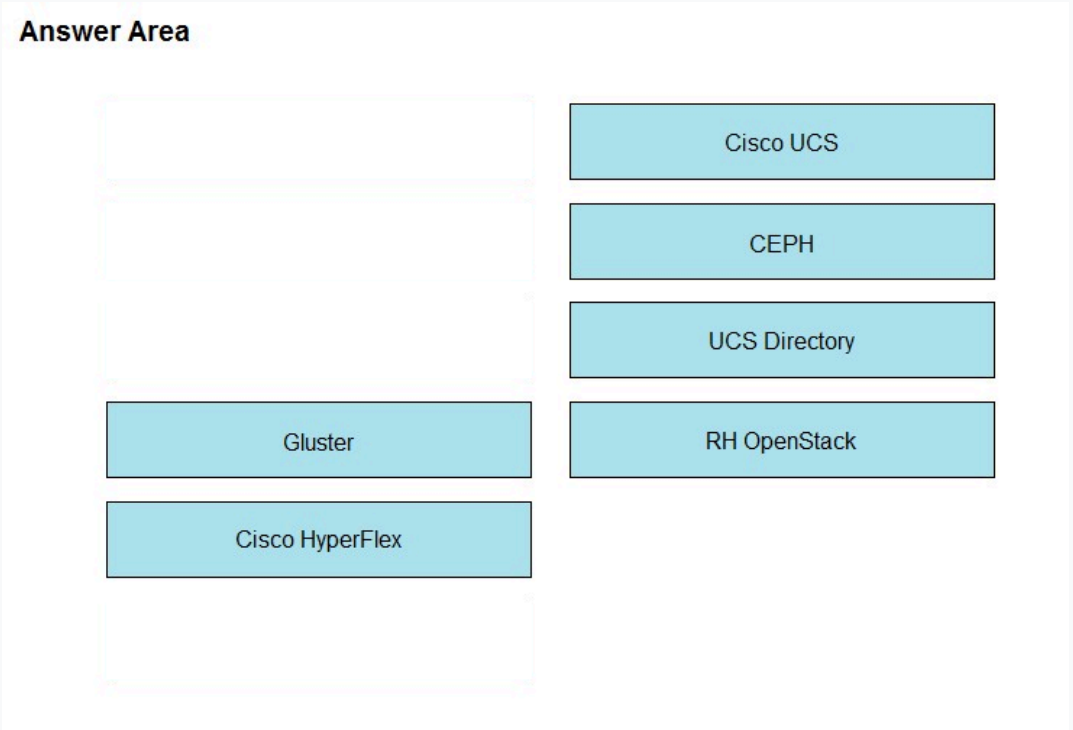
Select and Place:

Answer Area

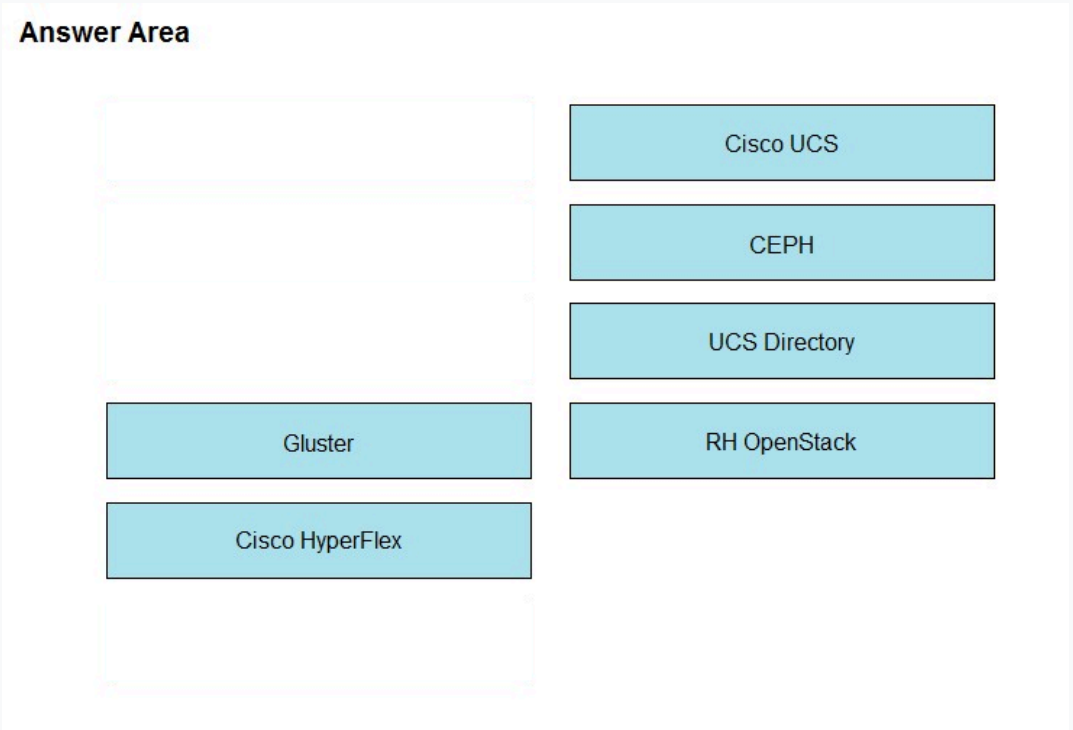


Suggested Answer:

Answer Area



Answer Area



TheNetworkStudent Highly Voted 1 year, 11 months ago

Correct, can be verified via: https://www.cisco.com/c/en/us/solutions/service-provider/network-functions-virtualization-nfv-infrastructure/at-a-glance.html#~nfvi Quick note: It's UCS Director, not Directory.... oh well.

upvoted 6 times

amitsir Most Recent 1 year, 9 months ago

yes, its correct

upvoted 1 times

Question #20 *Topic 1*

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

A. multiple vBond orchestrators

B. establishing affinity between vSmart controllers and WAN Edge routers

C. OMP

D. BFD

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Wippypradeep Most Recent 8 months, 4 weeks ago

Cisco SD-WAN data plane resiliency :- https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/optimization-ha/vedge/network-optimization-high-availability-book/high-availability.html

upvoted 1 times

thisisganesh1 2 years, 2 months ago

correct D.

upvoted 1 times

Ben_001 4 years, 7 months ago

For data plane resiliency, the Cisco SD-WAN software implements standard protocol mechanisms, specifically Bidirectional Forwarding Detection (BFD), which runs on the secure IPsec tunnels between routers. Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/optimization-ha/vedge/network-optimization-high-availability-book/high-availability.html

upvoted 2 times

Question #21 *Topic 1*

Refer to the exhibit. Which configuration configures IPsec tunnels in active and standby?

```
from-vsmart data-policy_1_ServiceIsertionIPSec
direction from-service
vpn-list 1
        sequence 1
        match destination-ip 64.102.6.247/32
        action accept
        set
        service netsvc1
        service local
        default-action accept
```

A. vpn 1 service netsvc1 interface ipsec1 ipsec2 from-vsmart lists vpn-list 1 vpn 1

B. vpn 0 service netsvc1 interface ipsec1 ipsec2 from-vsmart lists vpn-list 0 vpn 0

C. vpn 1 service netsvc1 interface ipsec1 ipsec2 vpn-list 1 count ServicePSec1_275676046 from-vsmart lists vpn-list 1 vpn 1

D. vpn 0 service netsvc1 interface ipsec1 ipsec2 vpn-list 1 count ServicePSec1_275676046 from-vsmart lists vpn-list 0 vpn 0

Suggested Answer: *C*

Official Answer: C

Community vote distribution

A (100%)

DBla Highly Voted 3 years, 4 months ago

A looks much better, why would we use a counter under vpn-list definition? A with a little bit of formating: vpn 1 service netsvc1 interface ipsec1 ipsec2 from-vsmart lists vpn-list 1 vpn 1

upvoted 12 times

eojedad Most Recent 7 months, 3 weeks ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#r_service_4005.xml

upvoted 1 times

JP4CCNP 1 year, 10 months ago

Right Answer is A. Because the Counter in Policys are limited to 20 Signs. In the Example there are 22 Signs.

upvoted 2 times

bearsaxman 2 years ago

Correct answer is A. No requirement for counters.

upvoted 2 times

Roger95 2 years, 2 months ago

"from-vsmart" is not command line it's included when proceed show policy command on vEdge. "A" should be the best choice (nothing related to counter here). and VPN ID should be 1

upvoted 1 times

Scav20 2 years, 6 months ago

A is correct

upvoted 1 times

testwinner 2 years, 11 months ago

Correct is A

upvoted 1 times

she_ccie 2 years, 11 months ago

Anyone with a c-edge that can test this in a lab or the documentation to validate the config? I can't find "from-vsmart" in anything but nat fall back.

upvoted 1 times

she_ccie 2 years, 11 months ago

Location of Service IP address of the the service device, or GRE interface through which the service is reachable. You can specify up to four IP address. The service is advertised to the vSmart controller only if the address (or one of the addresses) can be resolved locally, at the local site, and

not via routes learned through OMP. When configuring a GRE tunnel, specify the names of one or two GRE interfaces. If you configure two, the first interface is the primary GRE tunnel, and the second is the backup tunnel. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary GRE tunnel.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#wp5008346010

upvoted 1 times

she_ccie 2 years, 11 months ago

If the action you are configuring is a service, configure the required services on the Cisco SD-WAN devices so that the Cisco vSmart Controller knows how to reach the services: Device(config)# vpn vpn-id service service-name address ip-address Specify the VPN is which the service is located and one to four IP addresses to reach the service device or devices. If multiple devices provide the same service, the device load-balances the traffic among them. Note that the Cisco SD-WAN device keeps track of the services, advertising them to the Cisco vSmart Controller only if the address (or one of the addresses) can be resolved locally, that is, at the device's local site, and not learned through OMP. If a previously advertised service becomes unavailable, the Cisco SD-WAN device withdraws the service advertisement.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/control-policies.html#id_112053

upvoted 1 times

Question #22 *Topic 1*

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

A. Cloud onRamp for Colocation

B. Cloud onRamp for IaaS

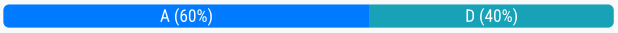
C. Cloud Services Platform

D. VNF Service Chaining

Suggested Answer: *A*

Official Answer: A

Community vote distribution



Loi2525 Most Recent 2 years, 1 month ago

RafaJohnston is correct, document explains it well.

upvoted 1 times

RafaJohnston76 2 years, 6 months ago

A is correct. Page 96 and 112 you can see the difference between Service-chaining and VNF ser ice chaining

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

upvoted 2 times

Networkchamp87 2 years, 7 months ago

Key word " regionalized" - Would say answer is A

upvoted 1 times

sus_007 2 years, 10 months ago

Cloud on-ramps are solutions designed to help organizations quickly and securely obtain cloud connectivity solutions.

upvoted 1 times

Clouddon 2 years, 10 months ago

A is correct

upvoted 1 times

timtgh 2 years, 11 months ago

VNF Service Chaining. (Virtual Network Function Service Chaining). The question asks how to provide service chaining to a network function. They practically put the answer in the question.

upvoted 2 times

Amitmanesar 4 years, 7 months ago

Service chaining ?

upvoted 1 times

Amitmanesar 4 years, 7 months ago

Service chaining ?I think that is correct

upvoted 1 times

timtgh 2 years, 11 months ago

I think that is correct

upvoted 1 times

EGD 4 years, 8 months ago

A: ? "With the Cisco SD-WAN Cloud onRamp for Colocation solution built specifically for colocation facilities, the solution routes the traffic to the best-permissible path from branches and remote workers to where all applications are hosted"

https://www.cisco.com/c/en/us/td/docs/routers/sdwan-cloud-onramp-for-colocation/solution-user-guide/cisco-sdwan-cloud-onramp-colocation-solution-guide-19_1/about-cisco-sd-wan-Cloud-OnRamp-for-Colocation-solution.html

upvoted 3 times

rockme27m 4 years, 10 months ago

Is correct

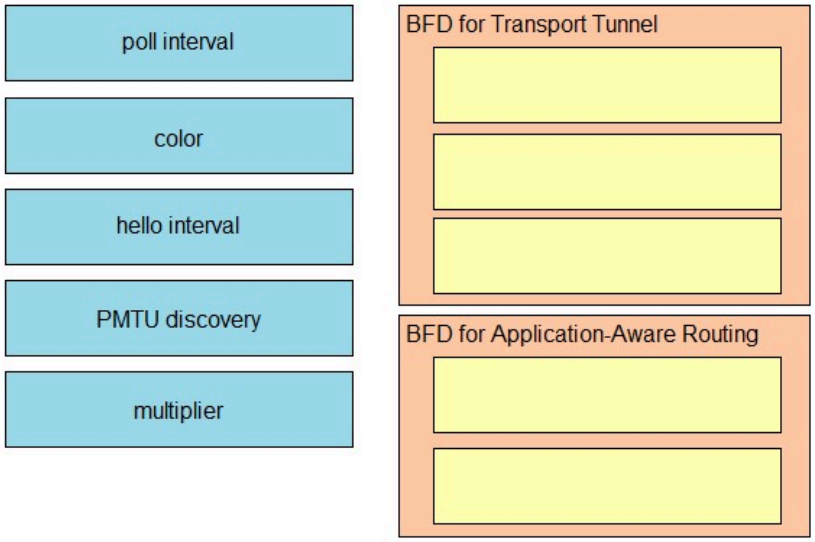
upvoted 1 times

DRAG DROP -

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

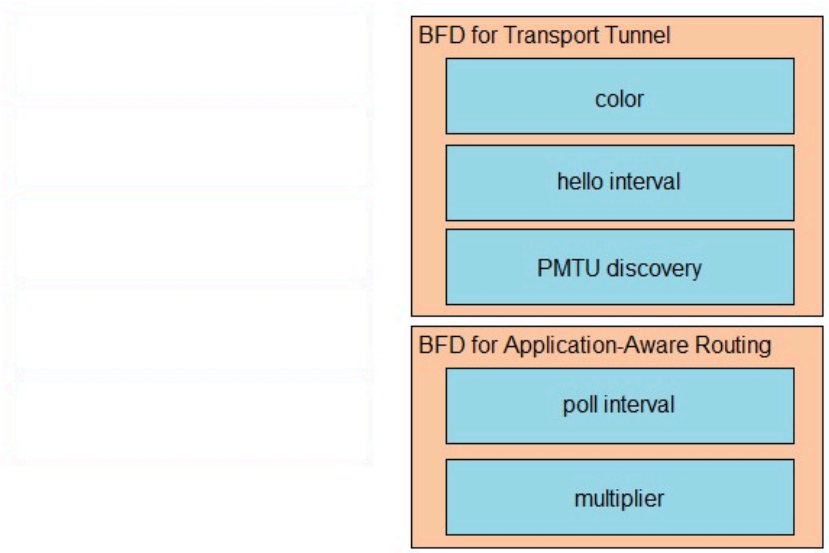
Select and Place:

Answer Area

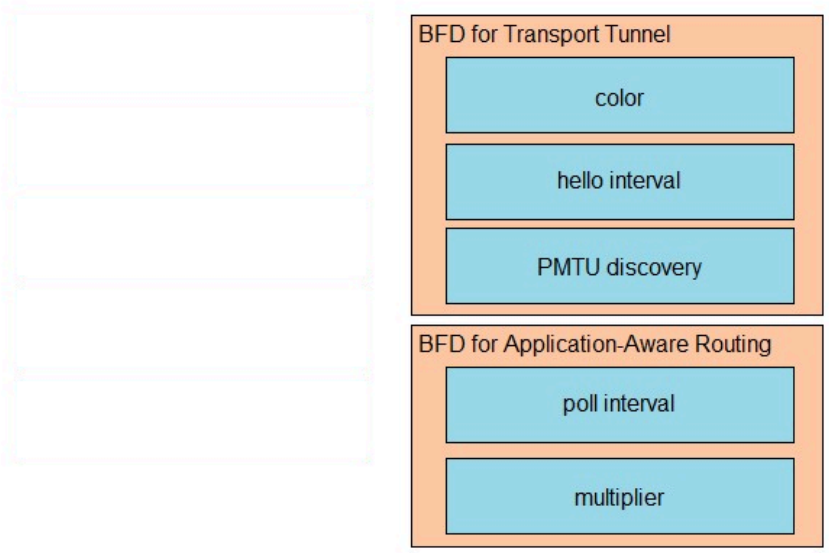


Suggested Answer:

Answer Area



Answer Area



wcorrea Most Recent 1 year, 10 months ago

multiplier could be also configured on bfd for ipsec tunnels https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Configuration/Templates/BFD#Configure_BFD_for_Application-Aware_Routing

upvoted 1 times

jablock2000 2 years, 9 months ago

https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Configuration/Templates/BFD#Configure_BFD_for_Application-Aware_Routing

upvoted 2 times

Question #24 *Topic 1*

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

A. WAN Edge Router

B. vSmart Controller

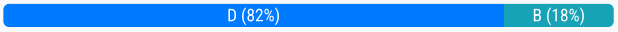
C. vManage

D. vBond Orchestrator

Suggested Answer: *D*

Official Answer: D

Community vote distribution



siang Most Recent 1 year, 9 months ago

D is correct

upvoted 1 times

RafaJohnston76 2 years, 2 months ago

vBond controller, or orchestrator, authenticates and authorizes the SD-WAN components onto the network. The vBond orchestrator takes an added responsibility to distribute the list of vSmart and vManage controller information to the WAN Edge routers.

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

upvoted 1 times

hamidreza0010 2 years, 9 months ago

D is correct

upvoted 2 times

bavaskan 3 years ago

Cisco vBond Orchestrator orchestrates the initial control connection between Cisco vSmart Controllers and edge routers

upvoted 2 times

timbo2000 3 years, 1 month ago

vBond is the gatekeeper and first point of contact, it then issues vsmart and vmanage ip addresses,

upvoted 1 times

heamgu 3 years, 1 month ago

Cisco vBond Orchestrator orchestrates the initial control connection between Cisco vSmart Controllers and edge routers.

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

upvoted 3 times

Roger95 3 years, 2 months ago

after Edges communicate with vBond and be authorized, communication between Edges, will be establish after vSmart share the TLOCs and key info to all Edges, then Edges establish the IPSec connection between them.

upvoted 2 times

she_ccie 3 years, 11 months ago

This question should not be worded "between Edge." Edge to controller is DTLS and vBond. Between the edges themselves is vSmart.

upvoted 1 times

Question #25 *Topic 1*

What is an attribute of TLOC?

A. tag

B. service

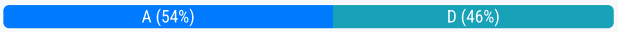
C. local preference

D. encryption

Suggested Answer: *A*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_17.1/06Policy_Basics/01Policy_Overview/01Viptela_Policy_Framework_Basics#:~:text=configured%20policy%20affects).-,TLOC%20Attributes% 20Used%20in%20Policies,address%2C%20color%2C%20and%20encapsulation

Community vote distribution



thepistol Most Recent 1 year, 3 months ago

Tag. question is explicitly asking what is an actual attribute. Encryption can be configured as encap-encrypt but there is not an 'encryption' literal attribute

upvoted 1 times

floydy 1 year, 4 months ago

Encryption is not the same as encapsulation, hence tag is the only match as per Cisco document.

upvoted 2 times

2e6bc5f 1 year, 5 months ago

System IP, Color and Encapsulation. Why is this even debated?

upvoted 1 times

Ma33 1 year, 7 months ago

In Cisco SD-WAN, the TLOC tag is indeed an optional attribute that can be associated with a TLOC, but its primary purpose is more about classifying or identifying transports rather than being a core attribute.

upvoted 1 times

Lloydyboy76 1 year, 7 months ago

Encryption is the answer as it is a feature of one of the two available encapsulation methods (GRE or IPSec)

upvoted 1 times

Matt2727 2 years, 1 month ago

TLOCS can have tags, i dont believe it is D as Encapsulation is not the same as Encryption. Encapsulation being ipsec or gre, gre is not encrypted.

upvoted 2 times

Rcont 2 years, 1 month ago

I´ll go with Encryption as a part of TLOC. Tag is an attribute of the OMP route, Not TLOC.

upvoted 2 times

Diegooo 2 years, 2 months ago

The tloc is defined by: System-ip Color Encapsulation.

upvoted 2 times

Kemofiv 2 years, 8 months ago

I agree

upvoted 1 times

brutusmail 3 years, 1 month ago

I believe that A and D are both correct as per Cisco documentation.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/policy-framework.html Am I see it correctly?

upvoted 3 times

khanda 4 years, 5 months ago

A is the correct answer, be careful not to confuse "local preference" with "preference" which is another TLOC attribute, local preference being a BGP attribute.

upvoted 4 times

Question #26 *Topic 1*

What is the behavior of vBond orchestrator?

A. It builds permanent connections with vSmart controllers.

B. It builds permanent connections with WAN Edge routers.

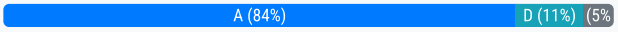
C. It updates vSmart of WAN Edge routers behind NAT devices using OMP.

D. It maintains vSmart and WAN Edge routers secure connectivity state.

Suggested Answer: *C*

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

Community vote distribution



MasiEB Most Recent 2 months ago

Control plane connection: Each Cisco SD-WAN Validator has a persistent control plane connection in the form of a DTLS tunnel with each Cisco Catalyst SD-WAN Controller in its domain. In addition, the Cisco SD-WAN Validator uses DTLS connections to communicate with edge routers when they come online, to authenticate the router, and to facilitate the router's ability to join the network. Basic authentication of an edge router is done using certificates and RSA cryptography. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html#%23c_Primary_SEN_Components_9291.xml

upvoted 1 times

AonDuine 2 months ago

I believe A is right. The question is regarding vBond's behavior not purpose.

upvoted 1 times

mikidvd51 1 year, 10 months ago

Also C could be correct. (google AI) 1. The WAN Edge router's real IP address and port are contained in a message. 2. The vBond controller receives the message and sends a notification to the WAN Edge router that it's behind a NAT. 3. The WAN Edge router updates its OMP TLOC route with the information and sends it to the vSmart controller. 4. The vSmart controller re-advertises the information across the overlay fabric. All WAN Edge routers in the fabric can use the correct IP and port values to establish communication.

upvoted 1 times

rubendrios 1 year, 11 months ago

To provide redundancy for the Cisco SD-WAN Validator, you can create multiple Cisco SD-WAN Validator entities in the network and point all edge routers to those Cisco SD-WAN Validators. Each Cisco SD-WAN Validator maintains a permanent DTLS connection with each Cisco Catalyst SD-WAN Controller in the network

upvoted 1 times

siang 2 years, 2 months ago

A is correct

upvoted 1 times

shadi_rizeq 2 years, 5 months ago

I think D is the correct answer, vBond establishes secure connections with all via IPSec, not only vSmart, but also vManage, WAN Edges, so Answer D is correct.

upvoted 1 times

nbvolz 3 years ago

We know which one is right, but which one would be on the exam..

upvoted 2 times

Tayeglow 3 years, 1 month ago

I believe it is D. It maintains vSmart and WAN Edge routers secure connectivity state.

upvoted 1 times

InjaYeGame 3 years, 4 months ago

I support A as correct. see below: "The DTLS connections with edge routers are temporary; once the Cisco vBond Orchestrator has matched a edge router with a Cisco vSmart Controller, there is no need for the Cisco vBond Orchestrator and the edge router to communicate with each other. The

Cisco vBond Orchestrator shares only the information that is required for control plane connectivity, and it instructs the proper edge routers and Cisco vSmart Controllers to initiate secure connectivity with each other. The Cisco vBond Orchestrator maintains no state."

upvoted 2 times

Roier 3 years, 5 months ago

A is correct The DTLS connections with Cisco vSmart Controllers are permanent so that the vBond controller can inform the Cisco vSmart Controllers as edge routers join the network. The DTLS connections with edge routers are temporary; once the Cisco vBond Orchestrator has matched a edge router with a Cisco vSmart Controller, there is no need for the Cisco vBond Orchestrator and the edge router to communicate with each other. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

upvoted 3 times

AW57 3 years, 8 months ago

A is correct

upvoted 2 times

Mohamedvibes 3 years, 8 months ago

vbond does not use OMP

upvoted 2 times

st1981 3 years, 8 months ago

A: Control plane connection: Each Cisco vBond Orchestrator has a persistent control plane connection in the form of a DTLS tunnel with each Cisco vSmart Controller in its domain. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

upvoted 1 times

wcorrea 3 years, 10 months ago

A is the correct answer

upvoted 1 times

nazars 3 years, 11 months ago

D is correct Vbond make secure connectivity between Vedge and vsmart

upvoted 2 times

aliciim 4 years ago

Selected Answer: D

Cisco vBond Orchestrator—The Cisco vBond Orchestrator automatically orchestrates connectivity between edge routers and Cisco vSmart Controllers. If any edge router or Cisco vSmart Controller is behind a NAT, the Cisco vBond Orchestrator also serves as an initial NAT-traversal orchestrator. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html

upvoted 1 times

phi5 3 years, 11 months ago

A is the correct answer, C is incorrect because vBond do not use OMP

upvoted 1 times

ccie_race 4 years ago

A seems correct because vBond maintains permanent connections with vSmart. vBond doesn't use OMP.

upvoted 2 times

Eliasmiranda 3 years, 11 months ago

A. Is correct. The major components of the Cisco vBond Orchestrator are: Control plane connection: Each Cisco vBond Orchestrator has a persistent control plane connection in the form of a DTLS tunnel with each Cisco vSmart Controller in its domain. In addition, the Cisco vBond Orchestrator uses DTLS connections to communicate with edge routers when they come online, to authenticate the router, and to facilitate the router's ability to join the network. Basic authentication of an edge router is done using certificates and RSA cryptography. NAT traversal: The Cisco vBond Orchestrator facilitates the initial orchestration between edge routers and Cisco vSmart Controllers when one or both of them are behind NAT devices. Standard peer-to-peer techniques are used to facilitate this orchestration. Load balancing: In a domain with multiple Cisco vSmart Controllers, the Cisco vBond Orchestrator automatically performs load balancing of edge routers across the Cisco vSmart Controllers when routers come online. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html#c_Components_of_the_Viptela_SEN_9290.xml

upvoted 2 times

Question #27 *Topic 1*

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

Suggested Answer: *D*

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

Community vote distribution

D (100%)

AJMD Most Recent 1 year, 12 months ago

Correct

upvoted 1 times

Speirsington 3 years, 6 months ago

Correct - OMP

upvoted 2 times

Question #28 *Topic 1*

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

A. OMP

B. IGP

C. QoS

D. TLS

Suggested Answer: *A*

Reference: https://www.lookingpoint.com/blog/cisco-sd-wan-omp

Community vote distribution



Almanac Highly Voted 4 years, 7 months ago

OMP is between vSmart to vEdge , and vSmart to vSmart only. I think tha answes is D: TLS. any comment?

upvoted 10 times

Almanac Highly Voted 4 years, 7 months ago

OMP is between vSmart to vEdge , and vSmart to vSmart only. I think tha answes is D: TLS. any comment?D seems correct.vEdge and vBond only use DTLS

upvoted 10 times

A_Wolf 4 years, 6 months ago

D seems correct.

upvoted 4 times

Seba_o_s 2 years, 6 months ago

vEdge and vBond only use DTLS

upvoted 1 times

Maurel 4 years, 6 months ago

vbond is never establish tls connection or OMP connection .

upvoted 5 times

Maurel 4 years, 6 months ago

vbond is never establish tls connection or OMP connection .at the time of bring up, there is a DTLS/TLS connection between vEdge and vBond, once the vEdge establishes connection to the vSart, the connection to the vBon is teared down.pg 180: https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=186

upvoted 5 times

A_Wolf 4 years, 6 months ago

at the time of bring up, there is a DTLS/TLS connection between vEdge and vBond, once the vEdge establishes connection to the vSart, the connection to the vBon is teared down.pg 180: https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=186

upvoted 1 times

A_Wolf 4 years, 6 months ago

at the time of bring up, there is a DTLS/TLS connection between vEdge and vBond, once the vEdge establishes connection to the vSart, the connection to the vBon is teared down.

upvoted 1 times

she_ccie 4 years, 5 months ago

pg 180: https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=186

upvoted 1 times

Wippypradeep Most Recent 8 months, 4 weeks ago

OMP is correct answer

upvoted 1 times

uzbin 1 year, 3 months ago

OMP, TLS all need underlay IGP. OMP only with vSmart. DTLS is the default, TLS is optional.

upvoted 1 times

Bajt 1 year, 6 months ago

D: TLS

upvoted 2 times

wasimtariq 1 year, 10 months ago

For a WAN Edge to effectively reach vManage, vBond, and vSmart controllers in a data center, the use of TLS is a critical requirement. This security protocol is vital for establishing secure and reliable connections within the SD-WAN architecture. Understanding these concepts is important for anyone pursuing a CCNA certification, as it covers fundamental networking principles and security measures in modern network design.

upvoted 2 times

tozcan 1 year, 10 months ago

The correct answer is D. TLS. Explanation: The WAN Edge devices must establish secure connections to the vManage, vBond, and vSmart controllers using TLS (Transport Layer Security). TLS is used to encrypt and secure communication between these components, ensuring data integrity and confidentiality. Without TLS, the WAN Edge devices would not be able to securely reach the controllers in the data center.

upvoted 1 times

merlow6674 2 years ago

A requirement for a WAN Edge to reach vManage, vBond, and vSmart controllers in a data center is: D. TLS Transport Layer Security (TLS) is essential for establishing secure communication channels between the WAN Edge routers and the controllers (vManage, vBond, and vSmart) in the Cisco SD-WAN architecture.

upvoted 1 times

Rcont 2 years, 1 month ago

inside DC, all devices (vmanage, vsmat, vbond, and Edges) need IGP to communicate with each other.

upvoted 1 times

siang 2 years, 2 months ago

A is correct

upvoted 1 times

Zamochit 2 years, 6 months ago

I think is IGP because Vbond doesn't use TLS? only DTLS on it. omp is only with vsmart and once the overlay is up.

upvoted 1 times

thomazmr 2 years, 6 months ago

correta B

upvoted 1 times

Aldebeer 2 years, 9 months ago

It can not be OMP. connecting with IGP is the most relevant answer to this question!

upvoted 1 times

Clouddon 2 years, 10 months ago

B is correct IGP

upvoted 1 times

AJMD 3 years ago

B is correct

upvoted 1 times

NetArch_Teck 3 years, 1 month ago

What is a requirement for a WAN Edge to reach vManage, vBond, and vSmart controllers in a data center? The question states the WAN Edge is in a data center, which mean's it is a bricks and mortar (Physical device) not a VM, so SD-WAN TLS, IGP and BGP is not valid here. OMP is required to connect to the overlay to the SD-WAN main controllers from a physical WAN Edge Device. Therefore the answer is A

upvoted 1 times

Tayeglow 3 years, 1 month ago

I think the answer is B

upvoted 1 times

Question #29 *Topic 1*

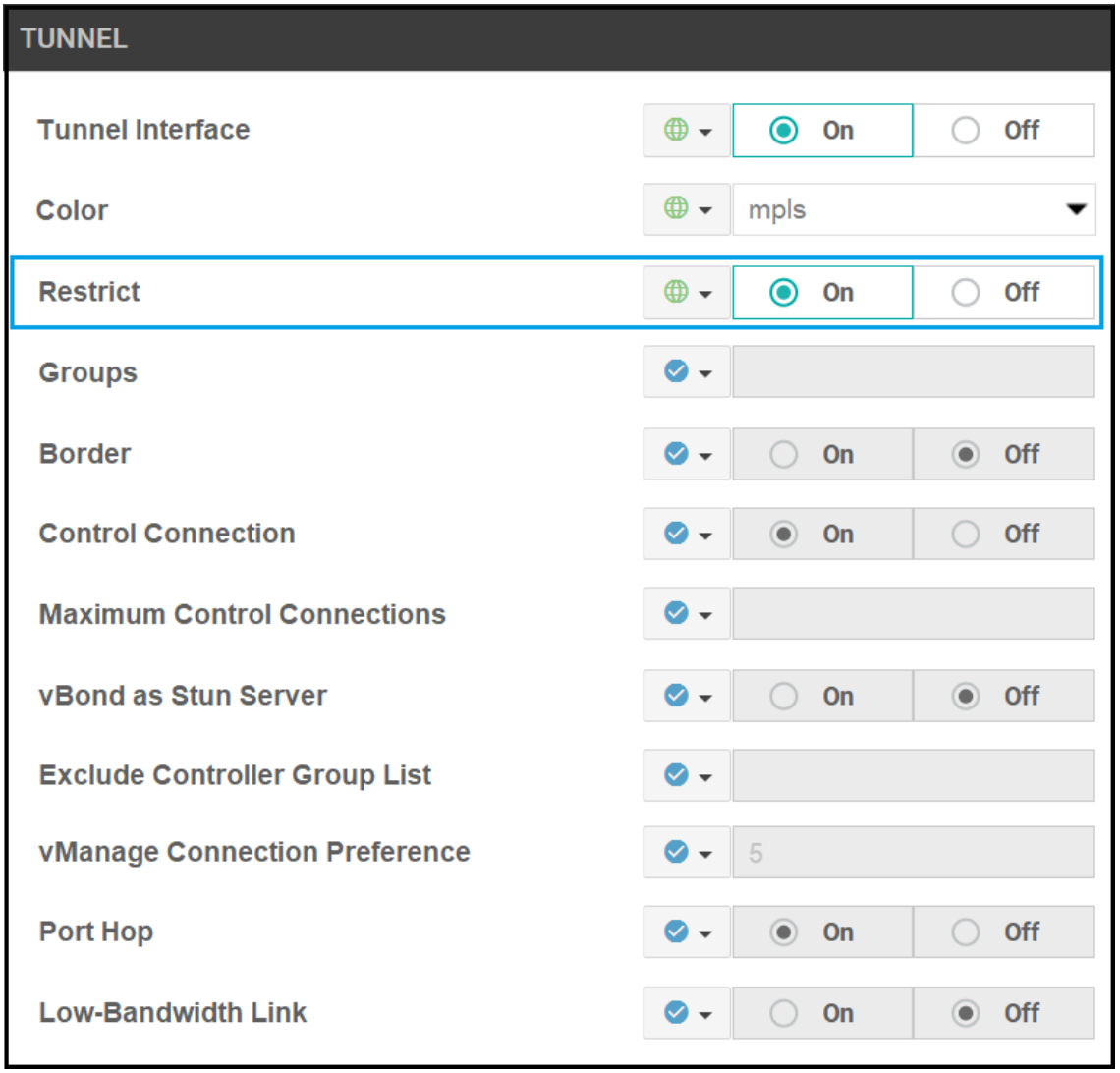
Company E wants to deploy Cisco SD-WAN with controllers in AWS. The company's existing WAN is on private MPLS without Internet access to controllers in
AWS. An Internet circuit is added to a site in addition to the existing MPLS circuit. Which interface template establishes BFD neighbors over both transports?

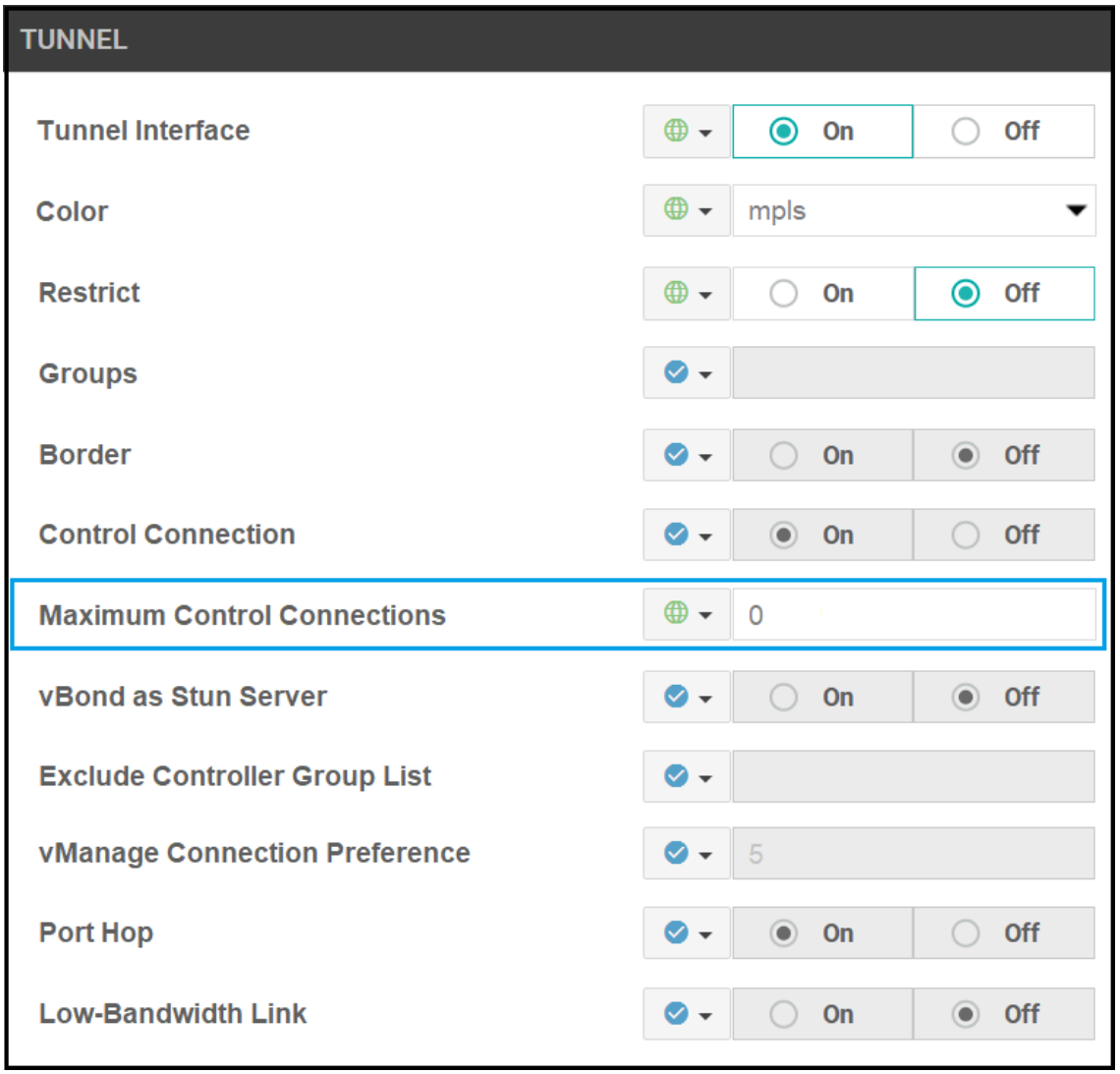
A.

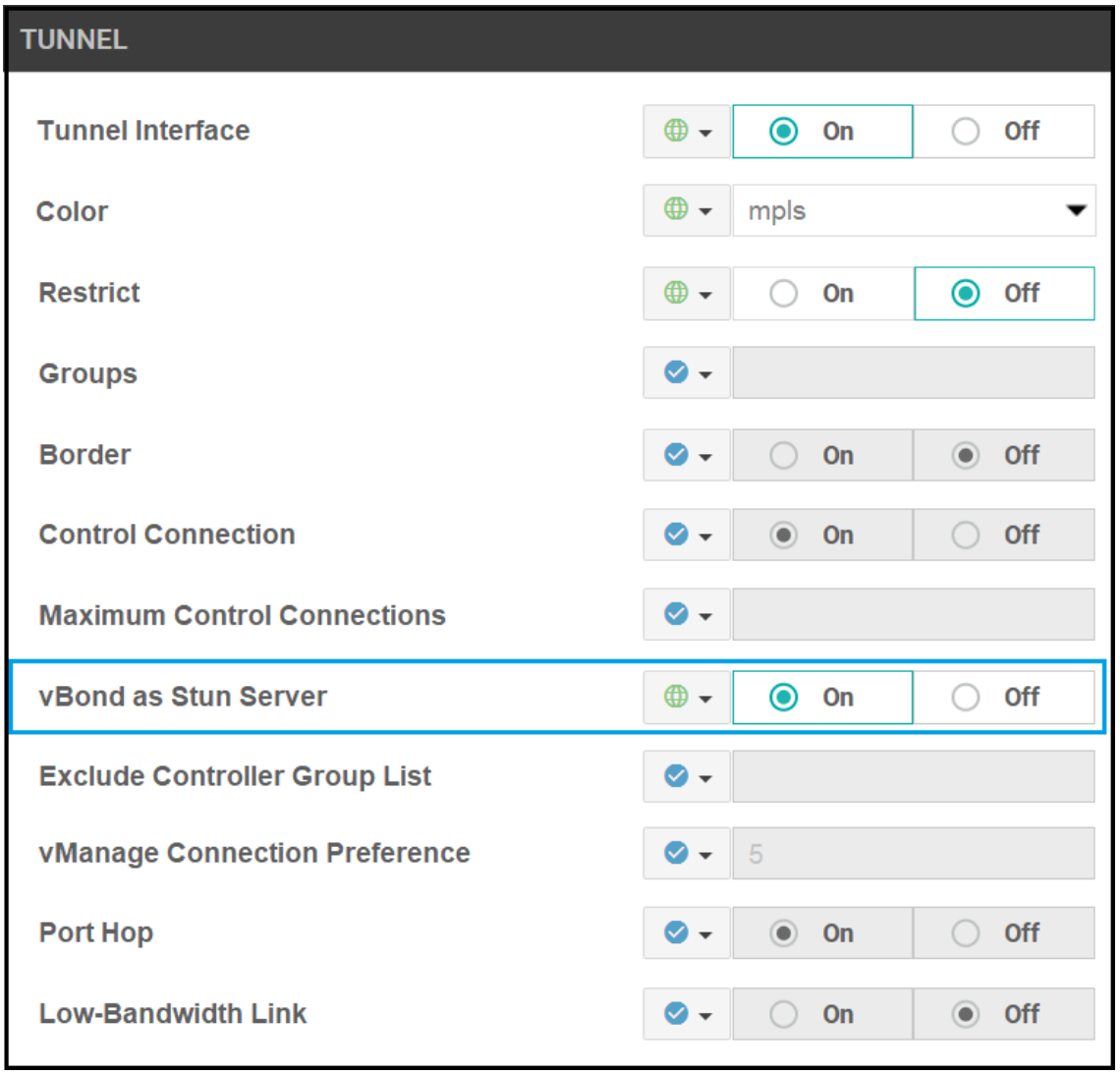
B.

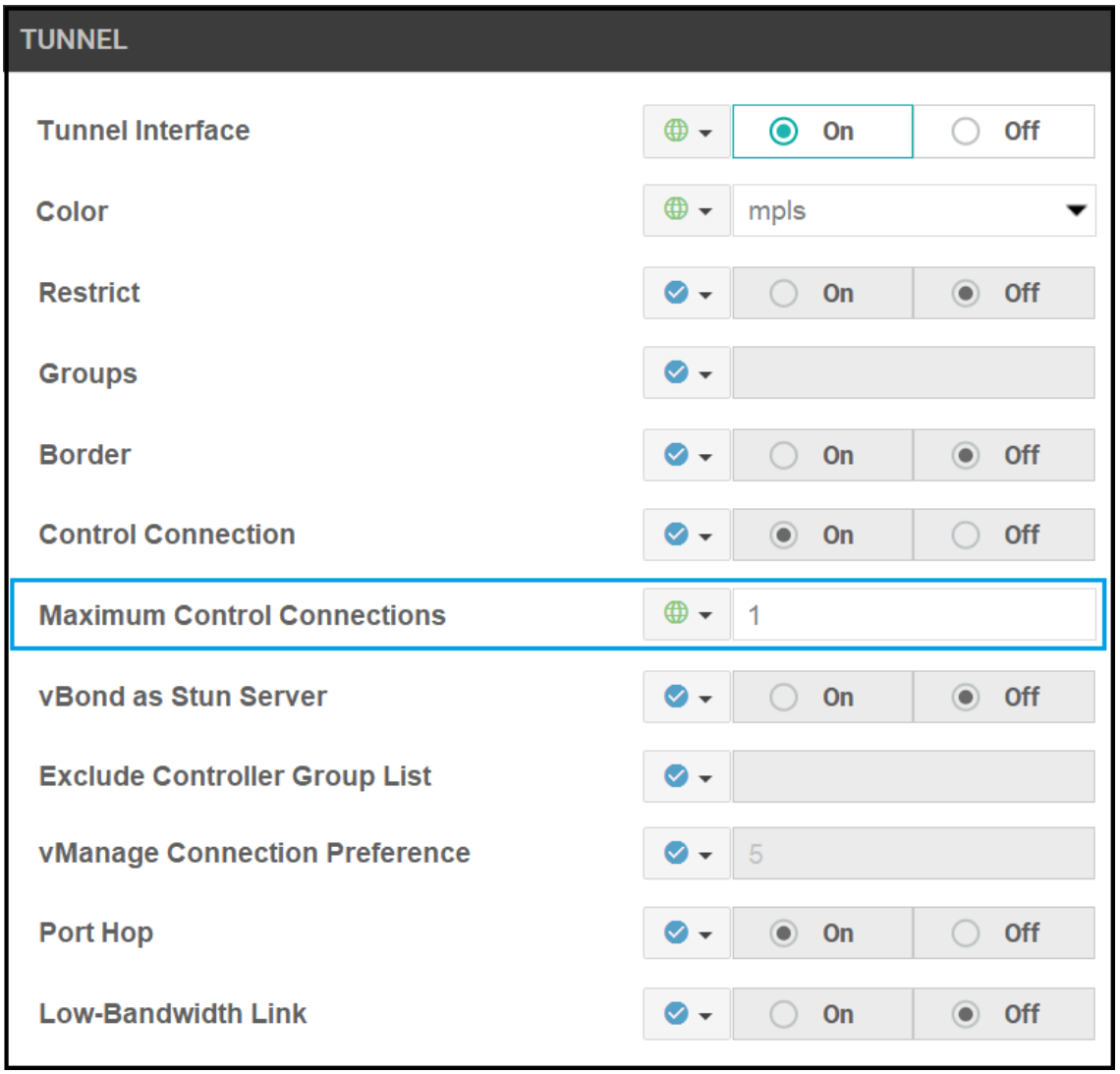
C.

D.




TUNNEL
Tunnel Interface
On
Off
Color
mpls
Restrict
On
Off
Groups
Border
On
Off
Control Connection
On
Off
Maximum Control Connections
0
vBond as Stun Server
On
Off
Exclude Controller Group List
vManage Connection Preference
5
Port Hop
On
Off
Low-Bandwidth Link
On
Off


TUNNEL
Tunnel Interface
On
Off
Color
mpls
Restrict
On
Off
Groups
Border
On
Off
Control Connection
On
Off
Maximum Control Connections
vBond as Stun Server
On
Off
Exclude Controller Group List
vManage Connection Preference
5
Port Hop
On
Off
Low-Bandwidth Link
On
Off



Suggested Answer:
Official Answer: A

Zizo_Yassin Most Recent 1 year ago

I think answer is B. From Cisco book and I quote: "It is important to note that with default settings, WAN Edge routers will attempt to establish control connections to SD-WAN Control Components over the MPLS transport. If such an attempt is unsuccessful, the router will not proceed to form data tunnels over it, and SDWAN will not use the transport. To address this, you should set the Maximum Control Connections option for the MPLS tunnel interface to 0. This tells the WAN Edge router that this TLOC is not expected to form control connections but still can build data tunnels" end of Quotation.

upvoted 1 times

Arsenal16 1 year, 6 months ago

I think B is correct. When the Restrict option is turned On, it may limit the traffic to only specific paths or interfaces, which can interfere with the establishment of BFD neighbors across both the MPLS and Internet links.

upvoted 2 times

John662266 1 year, 8 months ago

I think B is correct.

upvoted 3 times

ckdwa123 1 year, 10 months ago

I also believe it is B. https://community.cisco.com/t5/sd-wan-and-cloud-networking/cisco-sdwan-mpls-transport/td-p/4759812 It is similar thing and you force for max cc as 0 to not form control connections with controllers but you still force other tlocs to advertise this tloc in order to build data plane over it. "If that is true you can update the MPLS interface (under tunnel-interface) with "max-control-connections 0". This command will force the other two transports (gold, green) that can connect to the controllers to send the MPLS interface TLOC info to the controllers." If we choose vBond as Stun Server, it doesn't make sense as there is no NAT done in the MPLS circuit so how would it help? Private colors are not intended to be used with NAT. "On the other hand, private colors are intended for use on connections to clouds where NAT is not utilized"

upvoted 3 times

Vinay_Harish 2 years, 6 months ago

I suppose D is the correct answer, due to reasons below, 1. As per the question "which interface template establishes BFD neigh over both interface". Which means we need to allow at least 1 control connections on each of the links in-order to form the control connections and in-turn the BFD neigh.

upvoted 1 times

RafaJohnston76 2 years, 6 months ago

B is correct As per requirements of the question the only correct answer is B, here is what I found on a book: For transports that don't need to facilitate control connectivity to the controllers (such as with MPLS, wherein the controllers are only reachable via the Internet), you must restrict control connections via the max- control- connections 0 command. This command is applied to the transport tunnel interface.

upvoted 2 times

hamed4maf 2 years, 8 months ago

B is correct because MPLS is not used for control connection and must max-control-connection on this interface be 0 A is not correct, because restrict is one of the OMP attributes that using for data plane not control plane C is not correct, because vbond use as a stun server when other controllers alos put on cloud D is not correct, because when we use internet connection for vbond connectio, we must max-control-connection = 0 on MPLS

upvoted 2 times

Aldebeer 2 years, 8 months ago

B is correct

upvoted 2 times

Clouddon 2 years, 10 months ago

D is correct

upvoted 3 times

creaakz 2 years, 11 months ago

"Which interface template establishes BFD neighbors over both transports?" That immediately rules out the Restrict option. B is correct, you don't want to establish control connection through the MPLS link (since it doesn't reach the controllers).

upvoted 1 times

AJMD 3 years ago

B is correct

upvoted 2 times

begafas 3 years ago

B is the corect answer. If MPLS doesn't have access to the controllers, only max-control-connections to 0 will allow it to form BFD tunnels on MPLS link.

upvoted 2 times

NetArch_Teck 3 years, 1 month ago

A is the correct Answer. Please remember the question specifies an existing topology of an MPLS TLOC, so you want to restrict this to MPLS, and leave the maximum connections ticked. This would complete the question. I have also rolled out this policy to the controllers for a customer where they added two circuits to an existing topology being MPLS from a ISP.

upvoted 1 times

hamidreza0010 3 years, 2 months ago

D is the correct answer

upvoted 2 times

JP4CCNP 3 years, 2 months ago

B is the correct answer: - vBond isn`t reachable via MPLS (as explaint in the Text) -> so C can`t be the right answere - onyl 1 Controll Session make no sense, because vSmarts are also Controllers and not reachable vie MPLS (as explaint in the Text) -> So D can`t be the right answere - Answere A limits the IPSEC Tunnels to the color MPLS (but for this, the Controllers DTLS Session must be formed to learn and advertise OMP Routes) - Answere B can only the right Answere, because with setting the max. Controll Sesisons to 0 we told the Edge Device it is not possible to form Control Sessions about this MPLS link and the Edge Device advertise about the existing Internet Control Sessions the MPLS Color TLOCs to the vSmart. This Help to build IPSEC Tunnel over Private Links without creating Control Tunnels over this Cloud!

upvoted 4 times

JP4CCNP 3 years, 2 months ago

B is the correct answer: - vBond isn`t reachable via MPLS (as explaint in the Text) -> so C can`t be the right answere - onyl 1 Controll Session make no sense, because vSmarts are also Controllers and not reachable vie MPLS (as explaint in the Text) -> So D can`t be the right answere - Answere A limits the IPSEC Tunnels to the color MPLS (but for this, the Controllers DTLS Session must be formed to learn and advertise OMP Routes) - Answere B can only the right Answere, because with setting the max. Controll Sesisons to 0 we told the Edge Device it is not possible to form Control Sessions

about this MPLS link and the Edge Device advertise about the existing Internet Control Sessions the MPLS Color TLOCs to the vSmart. This Help to build IPSEC Tunnel over Private Links without creating Control Tunnels over this Cloud!The key here is the BFD neighbors

upvoted 4 times

Tuchi 3 years, 1 month ago

The key here is the BFD neighbors

upvoted 2 times

densma 3 years, 4 months ago

B is the only correct answer

upvoted 3 times

Question #30 *Topic 1*

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

A. DTLS

B. SSL VPN

C. IPsec

D. TLS

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

Wippypradeep Most Recent 8 months, 4 weeks ago

spoke to spoke or router to router connectivity through IPSec only, however router to controller uses DTLS

upvoted 2 times

nbvolz 1 year, 10 months ago

What good is this for if ALL questions are NEW.

upvoted 1 times

AJMD 1 year, 12 months ago

Correct

upvoted 1 times

ChrisCCNA 2 years, 11 months ago

C is correct

upvoted 1 times

Question #31 *Topic 1*

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

Suggested Answer: *B*

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

Community vote distribution

B (100%)

Aldebeer 2 years, 9 months ago

Selected Answer: B

it means 6 seconds

upvoted 1 times

Aldebeer 2 years, 9 months ago

it means 6 secondsyou mean 600 seconds or 10 minutes right?

upvoted 1 times

Rcont Most Recent 2 years, 1 month ago

you mean 600 seconds or 10 minutes right?

upvoted 1 times

AJMD 3 years ago

Correct

upvoted 1 times

Alchobashko 3 years, 6 months ago

correct

upvoted 1 times

Question #32 *Topic 1*

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

A. data

B. orchestration

C. management

D. control

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

John662266 Most Recent 1 year, 8 months ago

CP is correct.

upvoted 1 times

yuorsun 2 years, 3 months ago

D Control Plane

upvoted 1 times

Question #33 *Topic 1*

How is TLOC defined?

A. It is represented by a unique identifier to specify a site in a SD-WAN architecture.

B. It specifies a Cisco SD-WAN overlay in a multitenant vSMART deployment.

C. It is represented by a group of QoS policies applied to a WAN Edge router.

D. It is a unique collection of GRE or IPsec encapsulations, link color, and system IP address.

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Aldebeer Most Recent 1 year, 9 months ago

there is no another choice

upvoted 1 times

Question #34 *Topic 1*

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. WAN

B. local

C. dns-name

D. vbond-only

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

kent2612 1 year, 9 months ago
system configuration under VPN 0 so why is the answer 'local'? My understanding of under vpn0: vpn 0 interface ge0/0 ip address 1.1.1.1/24 ipv6 dhcp-client tunnel-interface encapsulation ipsec no allow-service bgp allow-service dhcp allow-service dns allow-service icmp no allow-service sshd no allow-service netconf no allow-service ntp no allow-service ospf no allow-service stun allow-service https
upvoted 3 times

kent2612 1 year, 9 months ago
system configuration under VPN 0 so why is the answer 'local'? My understanding of under vpn0: vpn 0 interface ge0/0 ip address 1.1.1.1/24 ipv6 dhcp-client tunnel-interface encapsulation ipsec no allow-service bgp allow-service dhcp allow-service dns allow-service icmp no allow-service sshd no allow-service netconf no allow-service ntp no allow-service ospf no allow-service stun allow-service httpsThe vBond Address would be specified in the system section of the configuration. With the addition "local" act the vEdge as vBond and not as a vEdge Device
upvoted 3 times

JP4CCNP Most Recent 1 year, 8 months ago
The vBond Address would be specified in the system section of the configuration. With the addition "local" act the vEdge as vBond and not as a vEdge Device
upvoted 1 times

kk_learn 2 years ago
B. Command 'local' makes vedge device to become vbond. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html
upvoted 2 times

Roger95 2 years, 3 months ago
system vbond x.x.x.x local
upvoted 1 times

EMAG86 2 years, 3 months ago
B local
upvoted 3 times

Question #35 *Topic 1*

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

A. centralized control and data plane

B. infrastructure as a service

C. management of SLA

D. centralized raid storage of data

E. distributed authentication policies

Suggested Answer: *A, C*

Official Answer: AC

Community vote distribution



mclk1234 Highly Voted 5 years ago

I think that is B and C, because A it's correct to the centralized control plane but not data planel can agree with B and C also.

upvoted 15 times

mclk1234 Highly Voted 5 years ago

I think that is B and C, because A it's correct to the centralized control plane but not data plane

upvoted 15 times

CCNPWILL 4 years, 9 months ago

I can agree with B and C also.

upvoted 3 times

siang Most Recent 1 year, 9 months ago

B and C are correct

upvoted 1 times

salmarin 2 years, 4 months ago

B and C

upvoted 1 times

speaktosen 3 years ago

B & C are correct. Data plane will be between edge routers

upvoted 2 times

khanda 3 years, 10 months ago

B and C are the correct answers.

upvoted 2 times

Baio 3 years, 12 months ago

IAAS and SLA B C are correct

upvoted 2 times

she_ccie 4 years ago

D, E I think this question is about CloudOps. What are the benefits of the cloud regardless of the solution being put in it? Redundancy and managed authentication...IMHO. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/knowledge-base/CloudOps/b-cisco-sdwan-cloudops/m-cloudops-overview.html

upvoted 3 times

A_Wolf 4 years ago

The data plane is composed by the vEdge (Branch, Head Offices, DC, etc) the data plane CANNOT be centralized. A is not correct. B,C are correct.

upvoted 1 times

juniper 4 years ago

B AND C

upvoted 2 times

ramjam 4 years, 8 months ago

BC... Book "Cisco SDWAN Defined Wide Area Networks" by Jason, Dana, Dustin, and JOhn

upvoted 4 times

FlipCCNP 4 years, 8 months ago

B and C IaaS is in question 19. Which two platforms for the Cisco SD-WAN architecture are deployable in a hypervisor on-premises or in IAAS Cloud?

upvoted 1 times

FLYT 4 years, 9 months ago

agree with B and C

upvoted 3 times

logo 4 years, 9 months ago

advantages of deploying cloud-based Cisco SD-WAN controllers? the question is about CONTROLLERS, I think A it´s not correct.

upvoted 1 times

TheNetworkStudent 4 years, 10 months ago

I'd say it's not A, B and E.... but I dont know if I agree with C and D.... this is a weird question.

upvoted 3 times

klaatu 5 years ago

I think it is not B IaaS since Cisco is deploying and managing all the controllers VMs over AWS/Azure, so it is consumed in the way of SaaS in fact. But I disagree also with A, given that it does not matter where the controllers are place (cloud or on-prem), the functionality and centralized control is just the same.

upvoted 3 times

klaatu 5 years ago

I think it is not B IaaS since Cisco is deploying and managing all the controllers VMs over AWS/Azure, so it is consumed in the way of SaaS in fact. But I disagree also with A, given that it does not matter where the controllers are place (cloud or on-prem), the functionality and centralized control is just the same.When you deploy your controllers in a cloud, it can be IaaS where the cloud provider gives you only the infrastructure and you need to build up your virtual hardware and software and you maintain both. That is IaaS if i'm not wrong. But the question in this form is still weird because how IaaS is an advantage of doing IaaS? Altough B is a better option than A for sure.

upvoted 3 times

spamke 4 years, 4 months ago

When you deploy your controllers in a cloud, it can be IaaS where the cloud provider gives you only the infrastructure and you need to build up your virtual hardware and software and you maintain both. That is IaaS if i'm not wrong. But the question in this form is still weird because how IaaS is an advantage of doing IaaS? Altough B is a better option than A for sure.

upvoted 1 times

Question #36 *Topic 1*

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

A. .nxos

B. .qcow2

C. .iso

D. .ova

E. .bin

Suggested Answer: *B, D*
Official Answer: BD

Han2022 Most Recent 3 years, 2 months ago

vEdge Cloud router viptela-x.x.x-edge-genericx86-64.ova (for ESXi Hypervisor) viptela-edge-genericx86-64.qcow2 (for KVM Hypervisor) Cisco vBond Orchestrator viptela-edge-genericx86-64.ova (for ESXi Hypervisor) viptela-edge-genericx86-64.qcow2 (for KVM Hypervisor) Cisco vSmart Controller viptela-smart-genericx86-64.ova (for ESXi Hypervisor) viptela-smart-genericx86-64.qcow2 (for KVM Hypervisor) Cisco vManage viptela-vmanage-genericx86-64.ova (for ESXi Hypervisor) viptela-vmanage-genericx86-64.qcow2 (for KVM Hypervisor)

upvoted 4 times

milan74 3 years, 10 months ago

Answer B,D: see link https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html

upvoted 3 times

ramjam 4 years, 2 months ago

correct..

upvoted 3 times

Question #37 *Topic 1*

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. ISR 4431

C. vEdge 100c

D. vEdge 2000

E. vEdge Cloud

Suggested Answer: *A, E*

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

EGD Most Recent 2 years, 1 month ago

1. Hardware platforms • Cisco vEdge (formerly Viptela vEdge) Routers running Viptela OS • Integrated Services Router (ISR) 1000 and 4000 Series running IOS® XE SDWAN Software • Aggregation Services Router (ASR) 1000 Series running IOS XE SD-WAN Software 2. Virtual platforms • Cloud Services Router (CSR) 1000v running IOS XE SD-WAN Software • vEdge Cloud Router running Viptela OS

upvoted 3 times

Question #38 *Topic 1*

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

A. Increase the bandwidth of the WAN link connected to the vManage

B. Increase licensing on the vManage

C. Deploy more than one vManage controllers on different physical server

D. Deploy multiple vManage controllers in a cluster

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Aldebeer Most Recent 1 year, 9 months ago

its more affordable

upvoted 1 times

MerlinTheWizard 2 years, 2 months ago

Correct.. C is advised, but not mandatory to the solution, A is also recommended for larger scale deployment

upvoted 2 times

ramjam 4 years, 2 months ago

Correct: See this link. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Step_2__Deploy_the_vManage_NMS_7856.xml

upvoted 3 times

CCNPWILL 4 years, 3 months ago

Correct

upvoted 2 times

Question #39 *Topic 1*

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

A. vSmart

B. WAN Edge

C. vManage

D. vBond

Suggested Answer: *C*

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

Community vote distribution

C (100%)

nbvolz Most Recent 1 year, 10 months ago

I thought this site was updated when there was new questions? I keep seeing posts on here that there is alot of new questions.

upvoted 2 times

MerlinTheWizard 2 years, 2 months ago

Not exactly control-plane as per the ENSDWI course, but still correct due to the certificates/templates

upvoted 1 times

Han2022 3 years, 2 months ago

You can use Cisco vManage to store certificate credentials, and to create and store configurations for all Cisco edge network components. As these components come online in the network, they request their certificates and configurations from Cisco vManage. When Cisco vManage receives these requests, it pushes the certificates and configurations to the Cisco edge network devices

upvoted 1 times

CCNPWILL 4 years, 3 months ago

Correct

upvoted 3 times

Question #40 *Topic 1*

An engineer is troubleshooting a vEdge router and identifies a `DCONFAIL `" DTLS connection failure` message. What is the problem?

A. memory issue

B. certificate mismatch

C. organization mismatch

D. connectivity issue

Suggested Answer: *D*

Reference: https://community.cisco.com/t5/networking-documents/sd-wan-routers-troubleshoot-control-connections/ta-p/3813237#toc-hId-340740870

Community vote distribution

D (100%)

bullett00th Most Recent 1 year, 9 months ago

D is correct. https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html DTLS Connection Failure (DCONFAIL) This is one of the common issues of control connectivity that does not come up. Probable causes include a firewall or some other connectivity issues.

upvoted 1 times

nbvolz 1 year, 10 months ago

Great! So what I paid for is nothing . Is it worth going over this or a waste?

upvoted 1 times

Roger95 2 years, 9 months ago

D DTLS Connection Failure (DCONFAIL) This is one of the common issues of control connectivity that does not come up. Probable causes include firewall or some other connectivity issues. https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html

upvoted 3 times

Scav20 3 years ago

D is the correct answer indeed

upvoted 1 times

Question #41 *Topic 1*

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

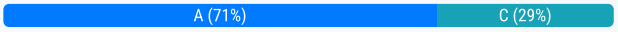
C. show certificate installed

D. show certificate status

Suggested Answer: *A*

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

Community vote distribution



siang Most Recent 1 year, 9 months ago

A is correct

upvoted 1 times

BrentL 2 years, 8 months ago

I'd go with A becuz it asks for certificates validity and this command shows both certificate and enterprise-cert validity.

upvoted 1 times

bearsaxman 3 years ago

A is the correct answer. The question specifically asks which command verifies the validity of the certificate. While validity information is shown in option C (show certificate installed), option A has a line that specifically states: certificate-validity Valid/Invalid. Option A is the best command for rapid troubleshooting by a technician.

upvoted 1 times

Seb82 3 years, 2 months ago

both commands run on a vEdge will show the cert validation and period

upvoted 3 times

Seb82 3 years, 2 months ago

both commands run on a vEdge will show the cert validation and periodsdwn01# show control local-properties certificate-not-valid-before Aug 09 09:25:19 2017 GMT certificate-not-valid-after Aug 09 09:25:19 2027 GMT ---------- sdwn01# show certificate validity The certificate is valid from Aug 9 09:25:19 2017 GMT (Current date is Wed Feb 1 11:36:51 GMT 2023) & valid until Aug 9 09:25:19 2027 GMTshow cert VALIDITY - not in the list of options..

upvoted 3 times

Alchobashko 3 years ago

sdwn01# show control local-properties certificate-not-valid-before Aug 09 09:25:19 2017 GMT certificate-not-valid-after Aug 09 09:25:19 2027 GMT ---------- sdwn01# show certificate validity The certificate is valid from Aug 9 09:25:19 2017 GMT (Current date is Wed Feb 1 11:36:51 GMT 2023) & valid until Aug 9 09:25:19 2027 GMT

upvoted 3 times

Alchobashko 3 years ago

sdwn01# show control local-properties certificate-not-valid-before Aug 09 09:25:19 2017 GMT certificate-not-valid-after Aug 09 09:25:19 2027 GMT ---------- sdwn01# show certificate validity The certificate is valid from Aug 9 09:25:19 2017 GMT (Current date is Wed Feb 1 11:36:51 GMT 2023) & valid until Aug 9 09:25:19 2027 GMTshow cert VALIDITY - not in the list of options..

upvoted 3 times

MerlinTheWizard 2 years, 9 months ago

show cert VALIDITY - not in the list of options..

upvoted 2 times

wcorrea 3 years, 3 months ago

For me "A" is correct since the question is about certificate on VEdge. The option "C" is related to certificate on controllers vsmar, vbond, vmanger. show certificate installed show certificate installed—Display the decoded certificate signing request installed on a vBond orchestrator, vManage NMS or vSmart controller. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/operational-cmd.html#r_show_certificate_installed_3978.xml

upvoted 3 times

Roger95 3 years, 3 months ago

troubleshoot validity of certificate, focus on certificate in detail. show certificate installed is the best choice

upvoted 2 times

EGD 4 years, 2 months ago

branch-vE1# show control local-properties personality vedge organization-name vIPtela Inc Regression certificate-status Installed root-ca-chain-status Installed certificate-validity Valid certificate-not-valid-before Sep 06 22:39:01 2018 GMT certificate-not-valid-after Sep 06 22:39:01 2019 GMT

upvoted 2 times

spamke 4 years, 4 months ago

'show certificate installed' also shows the validity of the certificate, so...

upvoted 3 times

Question #42 *Topic 1*

Refer to the exhibit. An engineer is troubleshooting a control connection issue. What does `connect` mean in this show control connections output?

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	CONTROLLER LOCAL COLOR	GROUP STATE	UPTIME	ID
vbond	dtls	-	0	0	1.3.25.25	12346	1.3.25.25	12346	gold	connect	0	
vbond	dtls	-	0	0	1.3.25.25	12346	1.3.25.25	12346	silver	connect	0	

A. Control connection is down

B. Control connection is up

C. Control connection attempt is in progress

D. Control connection is connected

Suggested Answer: *C*

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

Community vote distribution

C (100%)

siang Most Recent 1 year, 9 months ago

C is correct

upvoted 1 times

Xhizors 4 years, 1 month ago

Control connections might not come up if the overlay network has routing issues. If this is the case, the State column in the show control connections command output has a value of "connect", which indicates that a connection attempt is in progress. If the control connection is up, the State column shows a value of "up".

upvoted 3 times

Question #43 *Topic 1*

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

Suggested Answer: *D*

Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf page 16

Community vote distribution

D (100%)

Knowledge33 Most Recent 2 years, 1 month ago

D is correct

upvoted 1 times

Han2022 3 years, 8 months ago

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.

upvoted 3 times

Question #44 *Topic 1*

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

A. It carries control traffic over secure IPsec connections between vSmart controllers and vEdge routers, and between vEdge and vManager.

B. It carries control traffic over secure IPsec connections between vSmart controllers and vEdge routers, and between vSmart and vBond.

C. It carries control traffic over secure DTLS or TLS connections between vSmart controllers and vEdge routers, and between vSmart and vBond.

D. It carries out-of-band network management traffic among the Cisco SD-WAN devices in the overlay network.

Suggested Answer: *C*
Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_17.1/04Segmentation/02Configuring_Segmentation_ (VPNs)

Community vote distribution
C (100%)

Knowledge33 Most Recent 2 years, 1 month ago
C is correct
upvoted 1 times

Aldebeer 2 years, 2 months ago
C is the right answer!
upvoted 3 times

nbvolz 2 years, 4 months ago
VPN 0 or transport VPN carries control traffic over secure DTLS or TLS connections between vSmart controllers and vEdge routers, and between vSmart controllers and vBond orchestrators VPN 0 .
https://www.bing.com/ck/a?!&&p=5acc1b101683b550JmltdHM9MTY5NTUxMzYwMCZpZ3VpZD0xNGJjNzA4Mi1kODllLTZiYjQtMDIxZC02MzE3ZDkzNTZhZDcmaW5zaWQ9NTM0Mg&ptn=3&hsh=3&fclid=14bc7082-d89e-6bb4-021d-6317d9356ad7&psq=DTLS+and+TCP+connections+between+vsmart+and+vbond&u=a1aHR0cHM6Ly93d3cuY2lzY28uY29tL2MvZW4vdXMvdGQvZG9jcy9yb3V0ZXJzL3Nkd2FuL2NvbmZpZ3VyYXRpb24vc2VnbWVudGF0aW9uL3ZFZGdlLTIwLXgvc2VnbWVudGF0aW9uLWJvb2svc2VnbWVudGF0aW9uLmh0bWw&ntb=1
upvoted 2 times

NetArch_Teck 2 years, 7 months ago
VPN 0 on a WAN edge device is utilized to first connect to VBond to retrieve information through the REST-API (GET) procedure, via DTLS /TLS. Answer [B]
upvoted 1 times

colipto 2 years, 8 months ago
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20-x/systems-interfaces-book/configure-interfaces.html VPN 0—Transport VPN, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.
upvoted 1 times

A_Wolf 4 years ago
vEdges never build IP Sec tunnels to vSmart/vManage. IP Sec tunnels are stablished only between vEdges. A ad B are ruled out
upvoted 4 times

Question #45 *Topic 1*

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

A. control-policy

B. vpn-membership policy

C. app-route policy

D. cflowd-template

Suggested Answer: *A*

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

Community vote distribution

A (100%)

Knowledge33 Most Recent 2 years, 1 month ago

Correct is a

upvoted 1 times

NetArch_Teck 2 years, 7 months ago

Answer [A] A control policy is required when influencing a routing path via prefixes. The Cisco Link:-

fhttps://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/policy-overview.htmlerence

upvoted 1 times

aurelio123 3 years, 4 months ago

Asnwer A

upvoted 1 times

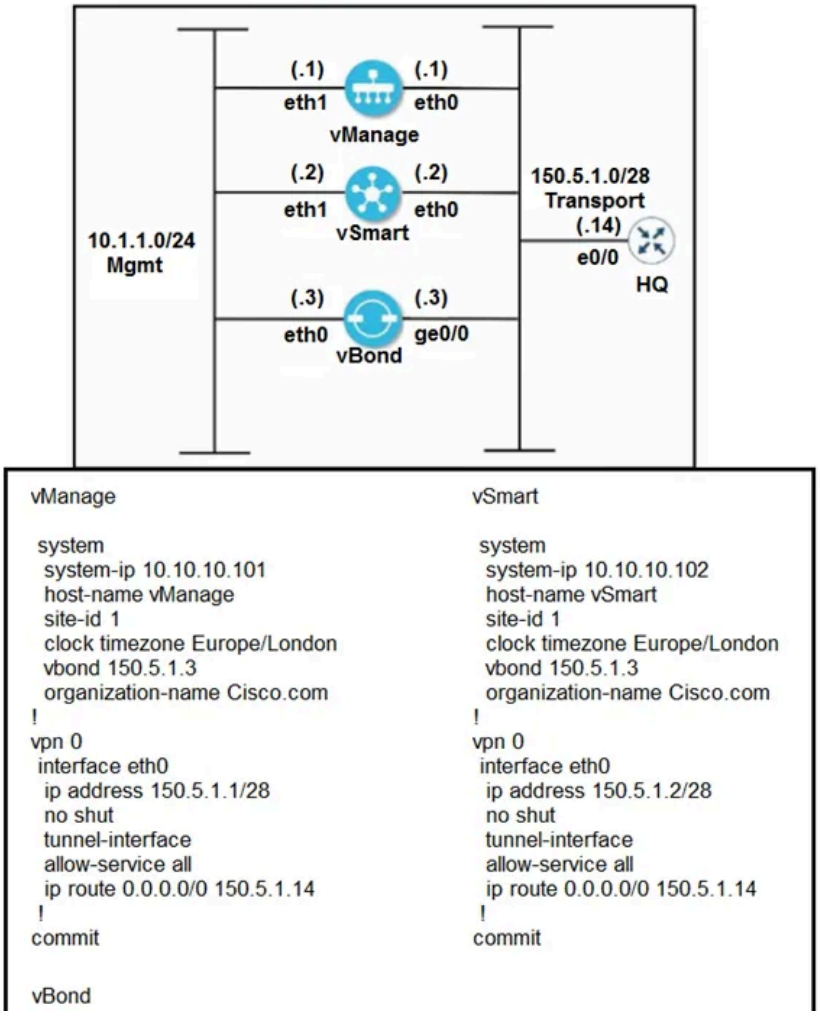
Scav20 3 years, 6 months ago

control-policy - is correct

upvoted 1 times

Question #46 *Topic 1*

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



A. Remove the encapsulation ipsec command under the tunnel interface of vBond

B. Reconfigure the vbond command on the vBond as vbond 150.5.1.3 local

C. Configure the tunnel interface on all three controllers with a color of transport

D. Configure encapsulation as IPsec under the tunnel interface of vManage and vSmart

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (71%) D (29%)

Nean Highly Voted 4 years, 6 months ago

vBond system system-ip 10.10.10.103 host-name vBond site-id 1 clock timezone Europe/London vBond 150.5.1.3 organization-name Cisco.com ! Vpn 0 Interface ge0/0 ip address 150.5.1.3/28 no shut tunnel-interface encapsulation ipsec allow-servide all ip route 0.0.0.0/0 150.5.1.14 ! commit

upvoted 16 times

ZeroBits Highly Voted 4 years, 8 months ago

This question is missing information in the exhibit

upvoted 7 times

thomazmr Most Recent 2 years ago

B is the correct answer, It is not necessary to define encapsulation in vManage and vSmart, only in vBond

upvoted 1 times

Knowledge33 2 years, 1 month ago

Answer is B

upvoted 1 times

hamidreza0010 2 years, 8 months ago

B is the correct answer

upvoted 1 times

eric0430 2 years, 11 months ago

Where is the vBond config in the exhibit?

upvoted 2 times

Mohamedvibes 3 years, 2 months ago

B is correct

upvoted 1 times

atiWok 3 years, 3 months ago

It's definetly B

upvoted 1 times

Eliasmiranda 3 years, 4 months ago

Answer is B vManage and vSmart do not use IPsec encapsulation, only vBond and SD-WAN Routers do.

upvoted 3 times

madcloud 3 years, 6 months ago

The given Answer is correct. People are being confused between setting up controlers and Edge routers. Tunnel Interface TYPE (Encapsulation IPSEC /(color in SCR) must be configured on the WAN edge router. On Vbond, Tunne interface is enabled by default. Configuring vBond Transport Interface Settings vBond VPN 0 ge0/0 interface: The VPN 0 interface is preconfigured for WAN transport (DHCP/IPsec). The tunnel interface configuration settings lock down the interface and also prevent incoming NETCONF and SCP/SSH connection. vManage establishes NETCONF and SCP connections with vBond over VPN 0. Recommendation: disable the tunnel-interface configuration while performing controller integration. Alternative: temporarily allow the NETCONF and sshd service

upvoted 1 times

RREVECO 3 years, 8 months ago

Answer: B is correct! A is WRONG , On page 27 it says you have to specify encapsulation ipsec on the tunnel interface of the vBond (and only for the vBond, neither for the vSmarts nor for the vManage) https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/LTRRST-2734-LG.pdf D is WRONG Vmanage use DTLS/TLS TUNNELS in the real vmanage devico no show ipsec PSEC tunnel is used to send out the data traffic between the vEdges/cEdges and as most of you already knew about the how secure is IPSEC tunnel. The parameters used in IPSEC tunnel is generally are Authentication and encryption Rekeying interval Replay window

upvoted 2 times

shanntorana 3 years, 10 months ago

Answer: D makes sence I believe Nean posted the missing piece of the exhibit. "Tunnel interfaces on vEdge routers must have an IP address, a color, and an encapsulation type:" The vManage and vSmart configurations are missing the encapsulation type. D. Configure encapsulation as IPsec under the tunnel interface of vManage and vSmart https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.2/02System_and_Interfaces/06Configuring_Network_Interfaces

upvoted 1 times

shanntorana 3 years, 10 months ago

agree with wolf

upvoted 1 times

A_Wolf 4 years ago

B without the vBond 150.5.1.3 LOCAL, the vBond would not act as a vBond "Note: vBond is actually the same image as a vEdge. We convert the personality by initiating the “vBond {ip-address} local” command."

upvoted 2 times

JTPRO 4 years, 1 month ago

Answer: D I believe Nean posted the missing piece of the exhibit. "Tunnel interfaces on vEdge routers must have an IP address, a color, and an encapsulation type:" The vManage and vSmart configurations are missing the encapsulation type. D. Configure encapsulation as IPsec under the tunnel interface of vManage and vSmart https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.2/02System_and_Interfaces/06Configuring_Network_Interfaces

upvoted 1 times

JTPRO 4 years, 1 month ago

Answer: D I believe Nean posted the missing piece of the exhibit. "Tunnel interfaces on vEdge routers must have an IP address, a color, and an encapsulation type:" The vManage and vSmart configurations are missing the encapsulation type. D. Configure encapsulation as IPsec under the tunnel interface of vManage and vSmart https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.2/02System_and_Interfaces/06Configuring_Network_Interfacesencap is only for the vEdge.

upvoted 1 times

A_Wolf 4 years ago

encap is only for the vEdge.

upvoted 3 times

TheNetworkStudent 4 years, 6 months ago

With the information missing, all answers are incorrect... but you can see vBond configuration should be in the bottom left of the exhibit. Guess B is correct then, assuming that the vbond is incorrect in the missing config.

upvoted 3 times

ramjam 4 years, 8 months ago

Requirements of Vbond. A connection should have TLOC.

upvoted 1 times

Question #47 *Topic 1*

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

```
                                                
```

Question #48 *Topic 1*

Refer to the exhibit. An engineer is troubleshooting tear down of control connections even though a valid CertificateSerialNumber is entered. Which two actions resolve the issue? (Choose two.)

```
PEER    PEER     PEER              SITE          DOMAIN
PEER            PRIVATE PEER                    PUBLIC                                  LOCAL   REMOTE      REPEAT
INSTANCE TYPE       PROTOCOL SYSTEM IP    ID          ID      PRIVATE IP        PORT      PUBLIC IP      PORT  REMOTE
COLOR    STATE              ERROR          ERROR    COUNT DOWNTIME
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
0           vbond       dtls    0.0.0.0                 0       0               192.168.0.231   12346   192.168.0.231   12346  default
tear_down       CRTREJSER NOERR    9       2019-06-01T19:06:32+0200
```

A. Enter a valid product ID (model) on the PNP portal

B. Match the serial number file between the controllers

C. Remove the duplicate IP in the network

D. Restore network reachability for the controller

E. Enter a valid serial number on the controllers for a given device

Suggested Answer: *A, C*

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

Community vote distribution

AE (88%) AB (12%)

Mr_Cipher Highly Voted 4 years, 7 months ago

I reckon it's A & E. The correct serial number and device model must be configured and provisioned on PnP portal (software.cisco.com) and vManage.

upvoted 15 times

juniper Highly Voted 4 years ago

A and E

upvoted 6 times

siang Most Recent 1 year, 9 months ago

A and E are correct

upvoted 2 times

hamidreza0010 2 years, 8 months ago

A and E are the correct answers

upvoted 2 times

ZeroBits 2 years, 9 months ago

A & E ..... BIDNTVRFD, CRTREJSER, SERNTPRES: Missing Serial Number Resolve the Problem Send the device's serial number to the controllers: 1. In vManage NMS, select the Configuration ► Certificates screen. 2. In the vEdge List tab, select the device whose serial number is missing. 3. Click Send to Controllers.

upvoted 3 times

Nandhujoe 2 years, 9 months ago

Answer is A & B

upvoted 1 times

AiltonDoria 3 years ago

if you have a look with the properly attention to this question we will be able to understand that's question is not about what meaning CRTREJSER, BIDNTVRFD. The question is: Focus in solve the issue, ***Which two actions resolve that behavior?*** based on it, the right options are: A: Enter a valid product ID (model) on the PNP portal E: Enter a valid serial number on the controllers for a given device Explanation and reference link: https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html#anc11 When you troubleshoot such a problem, ensure that the correct serial number and device model was configured and provisioned on the PnP portal (software.cisco.com) and vManage. In order to check the chassis number and the certificate serial number, this command can be used on vEdge routers: CRTREJSER - Challenge response rejected by peer. (peer reject because the serial number is not valid, that's why it generates this message.

upvoted 3 times

AiltonDoria 3 years ago

https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html#anc4

upvoted 1 times

kk_learn 3 years ago

A, E From provided document: "When you troubleshoot such a problem, ensure that the correct serial number and device model was configured and provisioned on the PnP portal (software.cisco.com) and vManage."

upvoted 3 times

theleftfoot 3 years ago

https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html#anc13

upvoted 1 times

moraist 3 years, 1 month ago

A and E makes sense for based on documentation. When you troubleshoot such a problem, ensure that the correct serial number and device model was configured and provisioned on PnP portal (software.cisco.com) and vManage.

upvoted 2 times

atiWok 3 years, 3 months ago

Check the link provided by FlipCCNP

upvoted 1 times

ccie_race 3 years, 6 months ago

A and E seems correct

upvoted 1 times

mac_tire 3 years, 10 months ago

E does not work, since the only two ways to upload the wan edge list is either to sync the smart account or upload the csv file to vManage and send that to the controllers. D does not make sense since it is able to talk to vbond and the error code is CTRREJSER, if it could not talk to vbond it would have DCONFAIL. C does not work either because if it was a duplicate IP it would have the code LISFD - Listener Socket FD Error - message. This leaves only A and B as the best/correct answersSerial Number(s) Not Present (CRTREJSER, BIDNTVRFD) Local error "CRTREJSER" is meaning If the serial number is not present on the controllers for a given device, the control connections fail. Reference: https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html#anc9

upvoted 1 times

mac_tire 3 years, 10 months ago

E does not work, since the only two ways to upload the wan edge list is either to sync the smart account or upload the csv file to vManage and send that to the controllers. D does not make sense since it is able to talk to vbond and the error code is CTRREJSER, if it could not talk to vbond it would have DCONFAIL. C does not work either because if it was a duplicate IP it would have the code LISFD - Listener Socket FD Error - message. This leaves only A and B as the best/correct answers

upvoted 1 times

Han2022 3 years, 8 months ago

Serial Number(s) Not Present (CRTREJSER, BIDNTVRFD) Local error "CRTREJSER" is meaning If the serial number is not present on the controllers for a given device, the control connections fail. Reference: https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html#anc9

upvoted 1 times

RickyDG 3 years, 11 months ago

For sure C is incorrect

upvoted 1 times

Baio 4 years ago

A & E should be correct

upvoted 2 times

Maurel 4 years ago

the correct answer is : AE

upvoted 3 times

Question #49 *Topic 1*

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

A. PnP Server

B. ZTP

C. HTTP

D. NETCONF

Suggested Answer: *B*

Official Answer: B

Community vote distribution

D (100%)

siang Most Recent 1 year, 9 months ago

D is correct

upvoted 1 times

RafaJohnston76 2 years ago

D is correct

upvoted 1 times

nbvolz 2 years, 6 months ago

On a test, would you go with the voted answer or the one they have as correct on here?

upvoted 3 times

jcms700 2 years, 7 months ago

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

upvoted 2 times

BGP65000 2 years, 8 months ago

Netconf and CLI: Netconf is a standards-based protocol used by Cisco vManage to provision a Cisco vSmart Controller. In addition, each Cisco vSmart Controller provides local CLI access and AAA.

upvoted 2 times

Eliasmiranda 3 years, 5 months ago

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

upvoted 1 times

ccie_race 3 years, 6 months ago

It should be D as vManage pushes the policies and config using Netconf which is similar to SNMP but more efficient.

upvoted 2 times

ChrisCCNA 3 years, 7 months ago

RickyDG is right page 518 of the Cisco Press SDWAN book

upvoted 1 times

testwinner 3 years, 9 months ago

Netconf

upvoted 1 times

RickyDG 3 years, 11 months ago

It is netconf. The answer is on page 518 in the Cisco SDWAN Press book.

upvoted 2 times

Baio 3 years, 11 months ago

Netconf is correct

upvoted 1 times

A_Wolf 4 years ago

D. NETCONF https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html "When any controller (vManage, vBond, or vSmart) is added to vManage, a vManage instance uses NETCONF to retrieve information from them and allows them to be added as

devices into the GUI" "If any controller reloads or crashes, then that controller uses NETCONF to communicate back to vManage before encrypted DTLS/TLS sessions are re-formed"

upvoted 1 times

Stiga 4 years, 1 month ago

netconfig

upvoted 1 times

Ben_001 4 years, 1 month ago

additional info: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf page 10

upvoted 1 times

Ben_001 4 years, 1 month ago

I believe "D" is correct -- The Edge then establishes a secure connection to the vManage and downloads the configuration using NETCONF.

upvoted 1 times

iamapie42 4 years, 3 months ago

D. Netconf.

upvoted 3 times

Almanac 4 years, 4 months ago

D. Netconf

upvoted 2 times

Question #50 *Topic 1*

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

A. RootCert

B. VeriSign

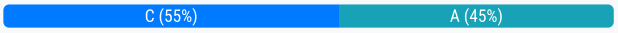
C. Microsoft

D. RADIUS

Suggested Answer: *A*

Reference: https://www.nterone.com/articles/cisco-sdwan-viptela-everything-you-wanted-to-know-about-certificates-deployment-but-were-afraid-to-ask

Community vote distribution



lecha3096 Highly Voted 3 years, 5 months ago

From SD-WAN book Should you choose to manage this functionality yourself, there are plenty of enterprise CA options available. Some common choices are Microsoft Certificate Services, OpenSSL, and even Cisco Identity Services Engine. Think it is C

upvoted 9 times

Jara2 Most Recent 2 months, 2 weeks ago

Several options for local CA follow: Customer's existing CA infrastructure Microsoft CA is most commonly used within enterprise environments. Most enterprises use Microsoft CA, which is supported by SD-WAN. Other CA solutions may work but must be tested.

upvoted 1 times

pipkin 11 months, 1 week ago

From SD-WAN book Should you choose to manage this functionality yourself, there are plenty of enterprise CA options available. Some common choices are Microsoft Certificate Services, OpenSSL, and even Cisco Identity Services Engine.

upvoted 3 times

siang 1 year, 8 months ago

A is correct.

upvoted 2 times

siang 1 year, 9 months ago

A is correct

upvoted 1 times

MerlinTheWizard 2 years, 9 months ago

C is the only possible option here. As per the ENSDWI 2.0 course, Section 2: Examining Cisco SD-WAN Deployment Options, Chapter 2.7: "Several options for local CA are as follows: - Customer's existing CA infrastructure ... Microsoft CA is most commonly used within enterprise infrastructure - Convenient CA setup for lab testing ... XCA ... TinyCA ... OpenSSL "

upvoted 1 times

Neil_Neo234 2 years, 10 months ago

B is also correct, because verisign also provides enterprise root ca?

upvoted 1 times

Zgana 3 years, 1 month ago

RootCert is not Enteprise CA Server, it shoul be C.

upvoted 1 times

fireman17 4 years ago

I believe is C, because you need an Enterprise Root CA.

upvoted 3 times

reza88 3 years, 1 month ago

A should be Ok

upvoted 1 times

fireman17 4 years ago

I believe is C, because you need an Enterprise Root CA.I don't think C is correct. What if the server is running on Linux OS?Then you would be using OpenSSL, which is not a answer option, hence C is correct

upvoted 3 times

DP 4 years ago

I don't think C is correct. What if the server is running on Linux OS?

upvoted 4 times

DP 4 years ago

I don't think C is correct. What if the server is running on Linux OS?Then you would be using OpenSSL, which is not a answer option, hence C is correct

upvoted 4 times

RafaJohnston76 1 year, 10 months ago

Then you would be using OpenSSL, which is not a answer option, hence C is correct

upvoted 1 times

Question #51 *Topic 1*

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

Suggested Answer: *D*

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

Community vote distribution

A (100%)

kentkyye Highly Voted 3 years, 7 months ago

correct answer will be A. reference:https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#Cisco_Concept.dita_818c0252-a9e5-4884-bf9a-ea70710eeb59

upvoted 13 times

kentkyye Highly Voted 3 years, 7 months ago

correct answer will be A. reference:https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#Cisco_Concept.dita_818c0252-a9e5-4884-bf9a-ea70710eeb59"In addition to the device serial and chassis numbers, the automatic validation and authentication procedure depends on having each device configured with the same organization name. You configure this name on Cisco vManage, and it is included in the configuration file on all devices. The organization name must be identical on all the devices that belong to a single organization (the name is case-sensitive). The organization name is also included in the certificate for each device, which is created either by Cisco SD-WAN or by an enterprise root CA. "

upvoted 13 times

Speirsington 3 years, 7 months ago

"In addition to the device serial and chassis numbers, the automatic validation and authentication procedure depends on having each device configured with the same organization name. You configure this name on Cisco vManage, and it is included in the configuration file on all devices. The organization name must be identical on all the devices that belong to a single organization (the name is case-sensitive). The organization name is also included in the certificate for each device, which is created either by Cisco SD-WAN or by an enterprise root CA. "

upvoted 3 times

Aldebeer Most Recent 1 year, 9 months ago

must be A

upvoted 1 times

hamidreza0010 2 years, 3 months ago

A is the correct answer

upvoted 2 times

Nandhujoe 2 years, 3 months ago

Correct Answer is A

upvoted 1 times

MiraGod 2 years, 11 months ago

A is the correct answer

upvoted 1 times

chubak 3 years ago

correct answer will be A.

upvoted 1 times

ccie_race 3 years ago

I think its should be A

upvoted 1 times

khanda 3 years, 4 months ago

A - is the correct answer

upvoted 1 times

Baio 3 years, 6 months ago

correct answer is A

upvoted 2 times

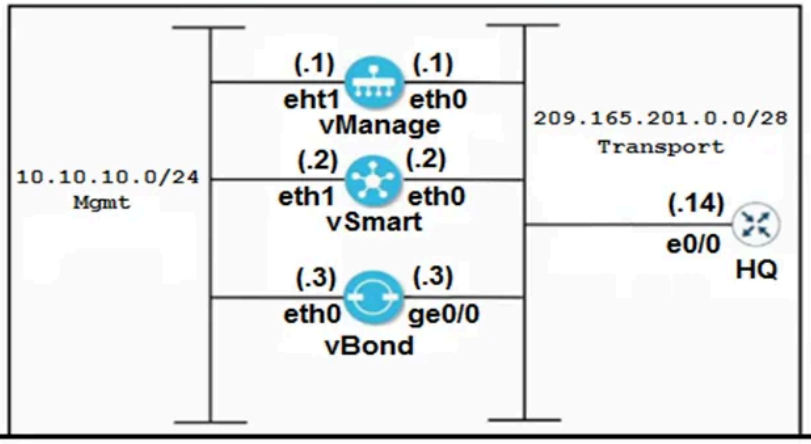
A_Wolf 3 years, 6 months ago

A. There is no such thing as a "vBond Domain" A domain is a logical grouping of vEdge routers and vSmart controllers that demarcates the span of control for the vSmartcontrollers. Each domain is identified by a unique integer, called the domain ID. Currently, you can configure only one domain in aViptela Overlay Network.Within a domain, vEdge routers can connect only with the vSmart controllers in their own domain. The vBond orchestratoris aware of which vSmart controllers are in which domain, so that when new vEdge routers come up, the vBond Orchestrator canpoint those routers to the vSmart controllers in the proper domain. However, the vBond orchestrator is never a member of adomain

upvoted 1 times

Question #52 *Topic 1*

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




```
vManage

system
  system-ip 10.10.10.101
  host-name vManage
  site-id 1
  clock timezone Europe/London
  vbond 209.165.201.3
  organization-name Cisco.com

!
vpn 0
 interface eth0
  ip address 209.165.201.1/28
  no shut
  tunnel-interface
  allow-service all
 ip route 0.0.0.0/0 209.165.201.14
!
commit
```

```
vBond

system
  system-ip 10.10.10.103
  host-name vBond
  site-id 1
  clock timezone Europe/London
  vbond 209.165.201.3 Local
  organization-name viptela.com

!
vpn 0
 interface ge0/0
  ip address 209.165.201.3/28
  no shut
  tunnel-interface
  encapsulation ipsec
  allow-service all
 ip route 0.0.0.0/0 209.165.201.14
!
commit
```

A. Change the organization name on both controllers to match viptela.com.

B. Configure the encapsulation ipsec command under the tunnel interface on vManage.

C. Reconfigure the system IPs to belong to the same subnet.

D. Remove the encapsulation ipsec command under the tunnel interface of vBond.

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html

Community vote distribution

A (100%)

testwinner Highly Voted 2 years, 5 months ago

Answer is A

upvoted 6 times

Erik_N Highly Voted 1 year, 8 months ago

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. Answer A

upvoted 5 times

Maurel 2 years, 6 months ago

Answer should A

upvoted 4 times

Question #53 *Topic 1*

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

```
PEER  PEER      PEER  SITE DOMAIN PEER         PRIVATE PEER               PUBLIC                          LOCAL REMOTE REPEAT
TYPE  PROTOCOL  SYSTEM  IP ID   ID PRIVATE IP      PORT    PUBLIC IP       PORT LOCAL COLOR   STATE      ERROR ERROR COUNT
-------------------------------------------------------------------------------------------------------------------------------
vbond dtls      -         0  0   209.165.200.230 12346 209.165.200.230 12346 biz-internet tear_down CTORGNMMIS NOERR 14
vbond dtls      -         0  0   209.165.201.137 12346 209.165.201.137 12346 biz-internet tear_down CTORGNMMIS NOERR 13
```

A. Configure a valid certificate on vSMART.

B. Configure a valid organization name.

C. Configure a valid serial number on the WAN Edge.

D. Configure a valid product ID.

Suggested Answer: *B*

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

Community vote distribution

B (100%)

Erik_N Most Recent 1 year, 8 months ago

Organization Mismatch (CTORGNMMIS) Organization Name is a critical component for bring up of the control connection. For a given overlay, the Organization name has to match across all the controllers and vEdges so that control connections can come up.
https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html#anc17 B is correct

upvoted 2 times

ChrisCCNA 2 years ago

B is correct

upvoted 2 times

Question #54 *Topic 1*

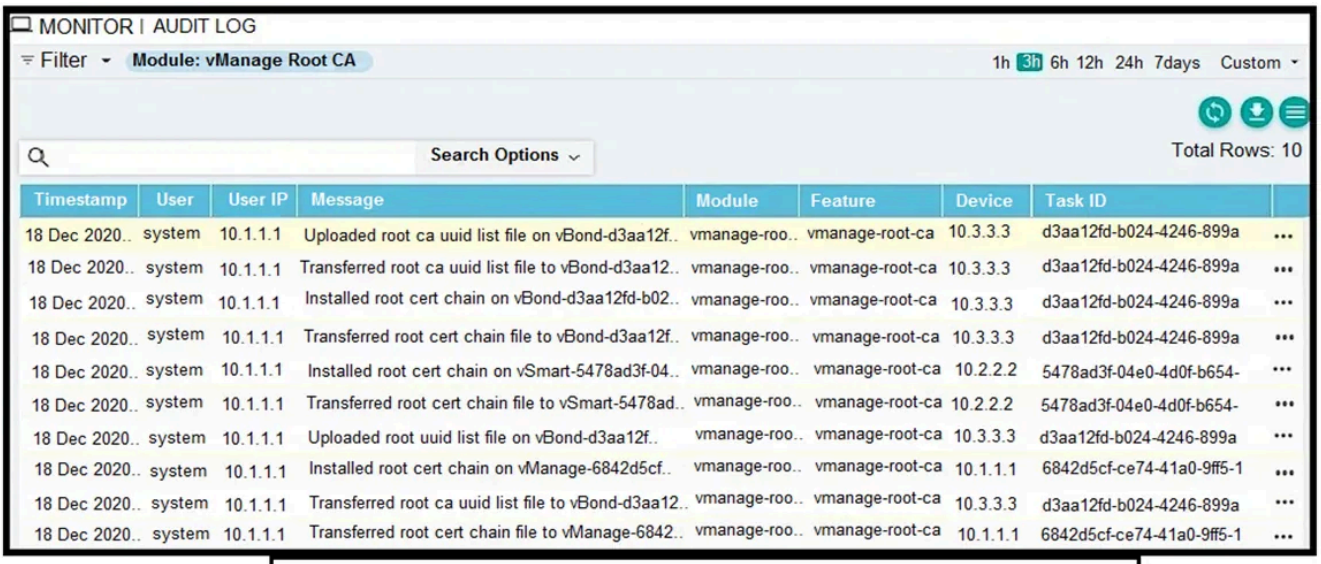
Refer to the exhibit. A small company was acquired by a large organization. As a result, the new organization decided to update information on their Enterprise
RootCA and generated a new certificate using openssl. Which configuration updates the new certificate and issues an alert in vManage Monitor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

A.

B.

C.

D.




```
vManage# show certificate installed

Server certificate
------------------

Certificate:
    Data:
       Version: 1 (0x0)
       Serial Number:
         d0:d1:f0:e0:63:52: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
       Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
           Public-Key: (2048 bit)
```

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

```
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

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=ABC/CN= SDWAN.lab" \
   -out ROOTCA.pem
```

Step2: Install the RootCA Certificate

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

Suggested Answer:

Reference: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-controller-cert-deploy-guide.html

Mykhey 2 years, 3 months ago

I have tested this in a lab environment, B looks correct #RootCA openssl req -x509 -new -nodes -key ROOTCA.key -sha256 -days 2000 -subj "/C=UK/ST=Hampshire/L=Southampton/O=LAB-1/CN=roger.local" -out ROOTCA.pem This is from this lab: https://www.youtube.com/watch?v=X0yfM45sTyk&list=PLplGU0K93TA4oi8wcWGUUtdyJP9VNZ5Ce&index=6

upvoted 2 times

incog 2 years, 12 months ago

in doc this is an exmaple: OpenSSL> x509 -req -days 730 -in vmanage.csr -CA subca.crt -CAkey subca.key -set_serial 02 -out vmanage.crt which options matches this one?

upvoted 2 times

NetArch_Teck 3 years, 1 month ago

Correct Answer is B According to Cisco's published guides!

upvoted 2 times

Roger95 3 years, 1 month ago

https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/215103-how-to-generate-self-signed-web-certific.html#:~:text=vmanage%3A~%2Fweb%24%20openssl%20genrsa%20-out%20rootca.key%202048%20Generating%20RSA,is%2065537%20%280x10001%29%20vmanage%3A~%2Fweb%24%20ls%20rootca.key%20web_cert.csr%20vmanage%3A~%2Fweb%24

upvoted 1 times

hamidreza0010 3 years, 2 months ago

A is the correct answer

upvoted 1 times

hamidreza0010 3 years, 2 months ago

A is the correct answerB is correct. Step1 says - " generate RootCA Certificate" which matches with command syntax/attributes. In option A - the comand generates a "vmanage.crt" which is something else. (It will be needed later on)

upvoted 1 times

mikidvd51 Most Recent 1 year, 10 months ago

B is correct. Step1 says - " generate RootCA Certificate" which matches with command syntax/attributes. In option A - the comand generates a "vmanage.crt" which is something else. (It will be needed later on)

upvoted 1 times

Fireforwall 3 years, 2 months ago

B is correct

upvoted 2 times

MerlinTheWizard 3 years, 2 months ago

A is correct: Eliminate C/D due to using Symantec in step 2 - as per the question, it should be local enterprise CA as used in A/B The step 1 should specify 365 days, not 2000, so this eliminates B and leaves us with A.

upvoted 3 times

MerlinTheWizard 3 years, 2 months ago

A is correct: Eliminate C/D due to using Symantec in step 2 - as per the question, it should be local enterprise CA as used in A/B The step 1 should specify 365 days, not 2000, so this eliminates B and leaves us with A.There's no requirement for cert to be valid for 365 days. It may be valid for 2000 days. Also there's change in ORG name in option B. Plus according the reference which Roger95 provided syntax in option B is correct. I'll go with B.

upvoted 3 times

Outlaw_87 2 years, 7 months ago

There's no requirement for cert to be valid for 365 days. It may be valid for 2000 days. Also there's change in ORG name in option B. Plus according the reference which Roger95 provided syntax in option B is correct. I'll go with B.

upvoted 1 times

densma 3 years, 4 months ago

B is wrong

upvoted 1 times

alin93 3 years, 9 months ago

one thing that bodered me was the O value. The question say that the organization is changed, so the O value must change as well, from the old ABC to XYZ (new organization name)

upvoted 1 times

Idro 3 years, 9 months ago

A is correct

upvoted 2 times

cfx3175 3 years, 10 months ago

B ONLY - see for syntax below: student@student-vm:~/lolcalCA$ openssl req -x509 -newkey rsa:2048 -keyout myca.key- -out myca.crt - days 3650 - nodes

upvoted 1 times

cfx3175 3 years, 10 months ago

B ONLY - see for syntax below: student@student-vm:~/lolcalCA$ openssl req -x509 -newkey rsa:2048 -keyout myca.key- -out myca.crt - days 3650 - nodes3650 days is incorrect, also, it will not be generated on a vmanage. B option specified 2000 days, which is incorrectThere's no problem with 2000 days and it's not incorrect.

upvoted 1 times

MerlinTheWizard 3 years, 2 months ago

3650 days is incorrect, also, it will not be generated on a vmanage. B option specified 2000 days, which is incorrectThere's no problem with 2000 days and it's not incorrect.

upvoted 2 times

MerlinTheWizard 3 years, 2 months ago

3650 days is incorrect, also, it will not be generated on a vmanage. B option specified 2000 days, which is incorrect

upvoted 2 times

Outlaw_87 2 years, 7 months ago

There's no problem with 2000 days and it's not incorrect.

upvoted 1 times

khanda 4 years ago

B is correct.

upvoted 3 times

Baio 4 years, 5 months ago

B is the correct answer. the syntax of the command is: openssl req (without the "-") and than go to vManage > Administration > §Controller Certificate Authorization > Enterprise Root Certificatethe number of days does not correspond with the cert in question

upvoted 1 times

Baio 4 years, 5 months ago

B is the correct answer. the syntax of the command is: openssl req (without the "-") and than go to vManage > Administration > §Controller Certificate Authorization > Enterprise Root Certificate

upvoted 1 times

MerlinTheWizard 3 years, 2 months ago

the number of days does not correspond with the cert in question

upvoted 1 times

she_ccie 4 years, 5 months ago

In Releases 17.1 and later, Cisco vManage can act as a Certificate Authority (CA) and can automatically generate and installed signed certificates on vEdge Cloud router. Notice the top left corner. VManage Module RootCa

upvoted 1 times

Speirsington 4 years, 6 months ago

I lean towards A

https://stackoverflow.com/questions/10175812/how-to-generate-a-self-signed-ssl-certificate-using-openssl

upvoted 1 times

Speirsington 4 years, 6 months ago

I lean towards A https://stackoverflow.com/questions/10175812/how-to-generate-a-self-signed-ssl-certificate-using-openssll stand by B. The syntax is correct, A isn't. Also, Why would you want a RootCA only valid for 1 year?Because the cert in question is valid for 365 days, therefore B can't be valid no matter how you look at it

upvoted 1 times

Izeflexzz 4 years, 6 months ago

I stand by B. The syntax is correct, A isn't. Also, Why would you want a RootCA only valid for 1 year?

upvoted 1 times

Izeflexzz 4 years, 6 months ago

I stand by B. The syntax is correct, A isn't. Also, Why would you want a RootCA only valid for 1 year?Because the cert in question is valid for 365 days, therefore B can't be valid no matter how you look at it

upvoted 1 times

MerlinTheWizard 3 years, 2 months ago

Because the cert in question is valid for 365 days, therefore B can't be valid no matter how you look at it

upvoted 1 times

Izeflexzz 4 years, 6 months ago

The correct answer is B, not A. The syntax for OpenSSL is correct and has the right navigation to the enterprise root certificate directory rather than D.

upvoted 2 times

Izeflexzz 4 years, 6 months ago

The correct answer is B, not A. The syntax for OpenSSL is correct and has the right navigation to the enterprise root certificate directory rather than D.How can B be correct when the validity of the cert it generates is 2000 days and it uses O=XYZ, although the exhibit shows a cert with a validity of 365 day and O=ABC? In my opinion, A is the right answer.

upvoted 2 times

DP 4 years, 6 months ago

How can B be correct when the validity of the cert it generates is 2000 days and it uses O=XYZ, although the exhibit shows a cert with a validity of 365 day and O=ABC? In my opinion, A is the right answer.

upvoted 4 times

Maurel 4 years, 6 months ago

Right answer should be A

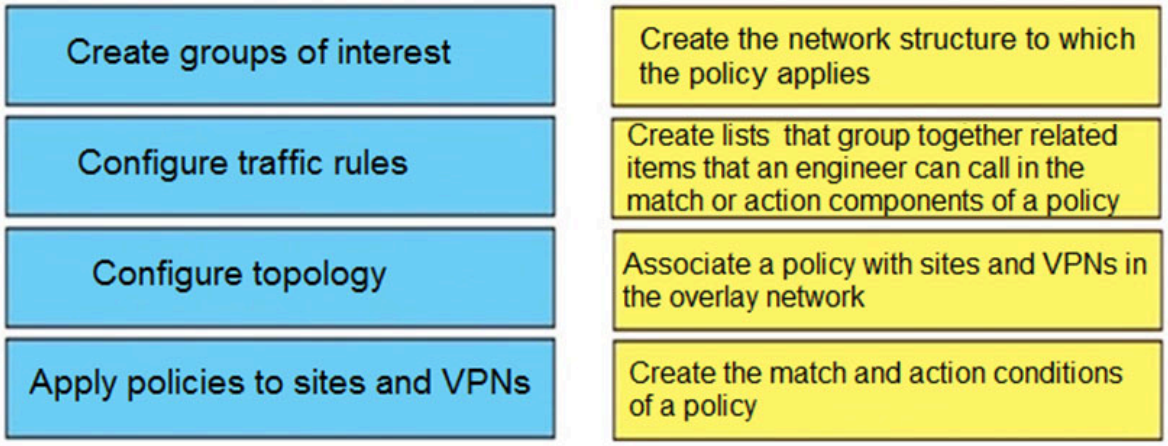
upvoted 2 times

Question #55 *Topic 1*

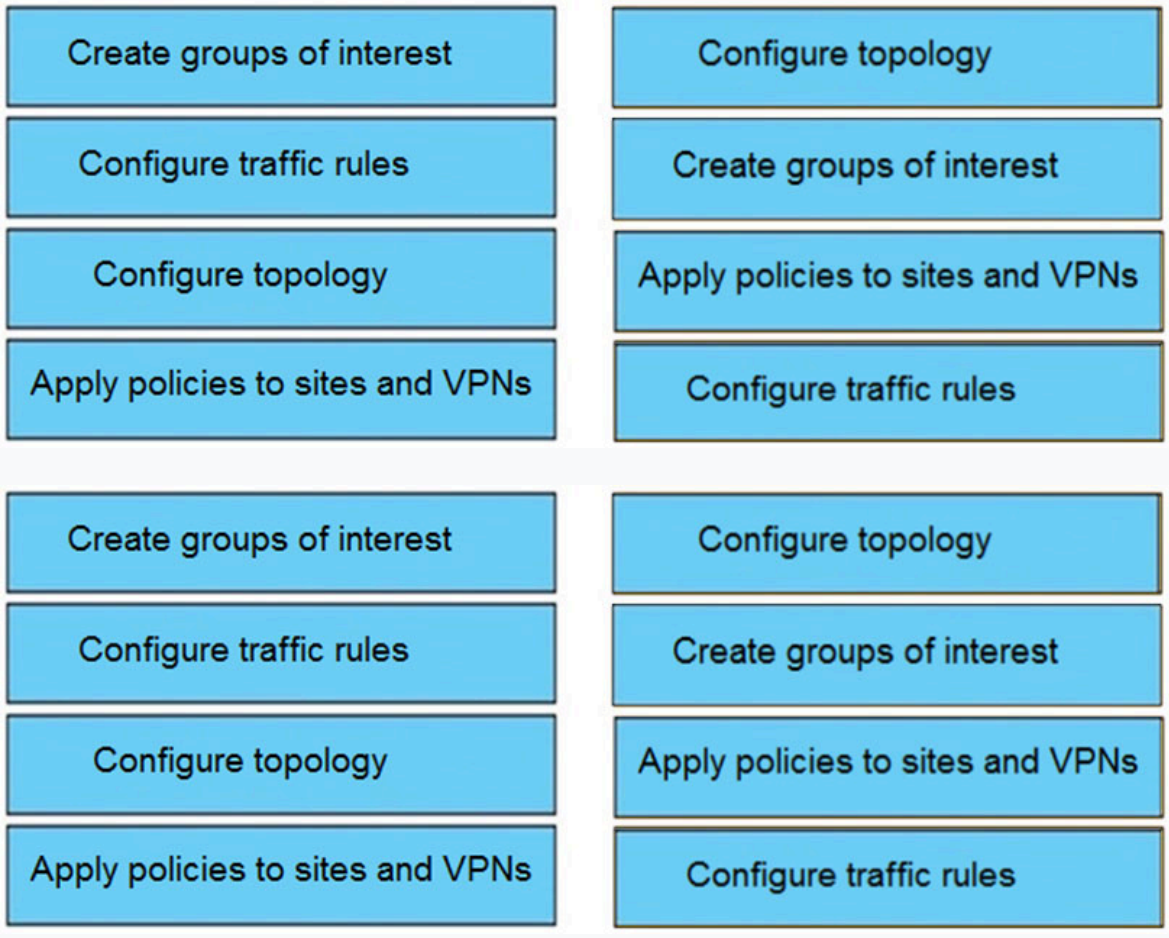
DRAG DROP -

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

Select and Place:



Suggested Answer:



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

Scav20 Most Recent 2 years ago

The order is correct: Configure topology Create group of interest Apply policies to sites and VPNs Configure traffic rules

upvoted 2 times

Question #56 *Topic 1*

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. 5 seconds

C. 1 second

D. 3 seconds

Suggested Answer: *C*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Templates/VPN_Interface_Ethernet

Community vote distribution

C (100%)

bullett00th Most Recent 1 year, 9 months ago

The VRRP advertisements are encapsulated in IP packets and sent to the IP v4 Multicast address assigned to the VRRP group. The advertisements are sent every second by default; the advertisement interval is configurable.

upvoted 1 times

milan74 3 years, 10 months ago

Answer C is correct, this is straight from the documentation: Specify how often the VRRP master sends VRRP advertisement messages. If slave routers miss three consecutive VRRP advertisements, they elect a new master. Range: 1 through 3600 seconds Default: 1 secondare these dumps still active ?

upvoted 2 times

milan74 3 years, 10 months ago

Answer C is correct, this is straight from the documentation:

Specify how often the VRRP master sends VRRP advertisement messages. If slave routers miss three consecutive VRRP advertisements, they elect a new master. Range: 1 through 3600 seconds Default: 1 second

upvoted 2 times

dybala10 3 years, 9 months ago

are these dumps still active ?

upvoted 2 times

Question #57 *Topic 1*

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

A.

B.

C.

D.

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

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

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

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

Suggested Answer:
Official Answer: A

Matt2727 Most Recent 2 years, 1 month ago

whilst max-metric would work... it would need the syntax with area number & router-lsa at the end, both are missing. C looks like the best bet here.

upvoted 2 times

konspali 2 years, 2 months ago

Stop thinking only about SDWAN commands and think of the Routing portion. By doing summarization we instantly make the router less preferred, as the other one will have more specific routes. Correct answer should be C.

upvoted 3 times

Stanleymahamadi 2 years, 2 months ago

Correct answer C

upvoted 2 times

incog 2 years, 12 months ago

A looks like the option: The OSPFv3 max-metric router LSA feature enables OSPFv3 to advertise its locally generated router LSAs with a maximum metric. The feature allows OSPFv3 processes to converge but not attract transit traffic through the device if there are better alternate paths.

upvoted 1 times

Jervv 3 years, 5 months ago

If you enter A and B on a vEdge, these commands are not accepted. Go for C

upvoted 1 times

Jervv 3 years, 5 months ago

If you enter A and B on a vEdge, these commands are not accepted. Go for Cvpn vpn-id --> router --> ospf --> max metric not accepted, only accepts if you write router-lsa after max-metric vpn vpn-id --> router --> ospf --> area number --> nssa --> no-summary is ACCEPTED in vEdge

upvoted 1 times

Outlaw_87 2 years, 7 months ago

vpn vpn-id --> router --> ospf --> max metric not accepted, only accepts if you write router-lsa after max-metric vpn vpn-id --> router --> ospf --> area number --> nssa --> no-summary is ACCEPTED in vEdge

upvoted 1 times

Idro 3 years, 9 months ago

A Is correct : https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Configuration/Templates/OSPFits not, doing "max-metric" will cause router to advertise it with infinite metric, even if primary path will be lost backup won't be installed since metric is infinite hence invalid to install. C is correct because you summarize prefix to make it less specific so it's not preferred when main route is installed but when the main is lost this summary will come into playA would be correct if there is "router-lsa" vEdge-INET-1# conf t Entering configuration mode terminal vEdge-INET-1(config)# vpn 1 vEdge-INET-1(config-vpn-1)# router vEdge-INET-1(config-router)# ospf vEdge-INET-1(config-ospf)# max-metric ----------^ syntax error: incomplete path vEdge-INET-1(config-ospf)# max-metric ? Possible completions: router-lsa Advertise own router LSA with infinite distance vEdge-INET-1(config-ospf)# max-metrictry with "area number "

upvoted 1 times

Idro 3 years, 9 months ago

A Is correct : https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Configuration/Templates/OSPF

upvoted 1 times

Precission21 3 years, 1 month ago

its not, doing "max-metric" will cause router to advertise it with infinite metric, even if primary path will be lost backup won't be installed since metric is infinite hence invalid to install. C is correct because you summarize prefix to make it less specific so it's not preferred when main route is installed but when the main is lost this summary will come into play

upvoted 1 times

Jervv 3 years, 5 months ago

A would be correct if there is "router-lsa"

vEdge-INET-1# conf t Entering configuration mode terminal vEdge-INET-1(config)# vpn 1 vEdge-INET-1(config-vpn-1)# router vEdge-INET-1(config-router)# ospf vEdge-INET-1(config-ospf)# max-metric ----------^ syntax error: incomplete path vEdge-INET-1(config-ospf)# max-metric ? Possible completions: router-lsa Advertise own router LSA with infinite distance vEdge-INET-1(config-ospf)# max-metric

upvoted 1 times

Jervv 3 years, 5 months ago

A would be correct if there is "router-lsa" vEdge-INET-1# conf t Entering configuration mode terminal vEdge-INET-1(config)# vpn 1 vEdge-INET-1(config-vpn-1)# router vEdge-INET-1(config-router)# ospf vEdge-INET-1(config-ospf)# max-metric ----------^ syntax error: incomplete path vEdge-INET-1(config-ospf)# max-metric ? Possible completions: router-lsa Advertise own router LSA with infinite distance vEdge-INET-1(config-ospf)# max-metrictry with "area number "

upvoted 1 times

Roger95 3 years, 1 month ago

try with "area number "

upvoted 1 times

Question #58 *Topic 1*

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

A. EMAIL

B. SNMP

C. AAA

D. DHCP

E. DNS

Suggested Answer: *D, E*
Official Answer: DE

izduk Most Recent 1 year, 10 months ago

D&E https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Prepare_vEdge_Routers_for_ZTP_9826.xml

upvoted 2 times

Scav20 2 years, 6 months ago

D & E are the correct answer

upvoted 4 times

Question #59 *Topic 1*

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

A. Set down-bit on WAN Edge routers on DC1

B. Define different VRFs on both DCs

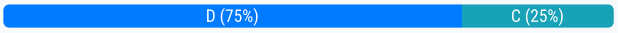
C. Set OMP admin distance lower than BGP admin distance

D. Set same overlay AS on both DC WAN Edge routers

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution



Hoon Highly Voted 5 years, 6 months ago

I think the answer is D. https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/215992-how-to-avoid-bgp-omp-routing-loop-in-sd.html

upvoted 17 times

ZeroBits Highly Voted 5 years, 2 months ago

By default, OMP is transparent to BGP even if propagate-aspath configured. overlay-as is a feature that prepends AS specified as a parameter of this command to BGP AS_PATH attribute of routes exported from OMP to BGP. If you configure the same overlay AS number on multiple devices in the overlay network, all these devices 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, hence routing loop will be prevented. As Hoon said, answer D

upvoted 6 times

Daniel_666 Most Recent 11 months, 2 weeks ago

C. Lowering OMP AD below BGP ensures that routes learned via OMP are preferred, avoiding re-learned routes via the DC interconnect.

upvoted 1 times

PandiyaGomathi 2 years ago

I think the answer is C

upvoted 1 times

siang 2 years, 2 months ago

D is correct.

upvoted 1 times

Aldebeer 2 years, 9 months ago

Only D:

upvoted 1 times

williancm19 3 years, 3 months ago

D for sure

upvoted 1 times

khanda 4 years, 1 month ago

Correct answer is D. https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/215992-how-to-avoid-bgp-omp-routing-loop-in-sd.html

upvoted 1 times

Baio 4 years, 6 months ago

correct answer is D

upvoted 1 times

Maurel 4 years, 6 months ago

Only D

upvoted 1 times

CesarVergaraGalindo 4 years, 10 months ago

Only D

upvoted 2 times

platin 5 years, 7 months ago

Which answer is right? B or D

upvoted 1 times

Question #60 *Topic 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

Suggested Answer: *A*

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

Community vote distribution

A (100%)

CCNPWILL Highly Voted 3 years, 3 months ago

correct

upvoted 8 times

khanda Most Recent 2 years ago

Correct answer.

upvoted 1 times

Question #61 *Topic 1*

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

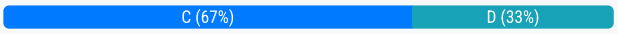
C. Set the device as valid

D. Send the list to controllers

Suggested Answer: *C*

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

Community vote distribution



mac_tire Highly Voted 4 years, 4 months ago

Correct answer is C, https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20-x/systems-interfaces-book/configure-devices.html in this document it states in section Upload WAN Edge Router Authorized Serial Number File To upload the WAN edge router authorized serial number file to Cisco vManage and then download it to controllers in the network: From the Cisco vManage menu, choose Configuration > Devices. Click WAN Edge List, and click Upload WAN Edge List. Under Upload WAN Edge List screen: Click Choose File and select the WAN edge router authorized serial number file you received from Cisco PnP. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the Validate the uploaded vEdge List and send to controllers check box is selected. If you do not select this option, you must individually validate each router in Configuration > Certificates > WAN Edge List. Click Upload. A list of routers in the network is displayed in the router table, with details about each router.

upvoted 8 times

Rosh8787 Most Recent 1 year, 10 months ago

Option C is correct. Initially by reading the question, option D looks very likely. But after reading it multiple times with more attention, Option C comes out as a correct answer.

upvoted 2 times

Stanleymahamadi 2 years, 2 months ago

correct answer D

upvoted 1 times

siang 2 years, 2 months ago

C is correct

upvoted 1 times

Outlaw_87 2 years, 7 months ago

vManage version 20.9 Configuration > Devices > Upload WAN Edge List Validate the uploaded vEdge List and send to controllers (there's only one option, not two)

upvoted 1 times

bullett00th 2 years, 9 months ago

I go with C See Page 18 https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf

upvoted 1 times

nbvolz 2 years, 10 months ago

To fully onboard the device, the 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.

upvoted 1 times

timtgh 2 years, 11 months ago

It's a poorly written question, because C and D are both required steps. Sending the list to the vSmart controllers is necessary, but it can be done without onboarding the devices at this time. Setting the devices as valid is what tells the vSmart to onboard those devices as soon as they come online.

upvoted 2 times

AJMD 2 years, 12 months ago

Selected Answer: D

D Question says: "to !!!support!!! the on-boarding process !!!before!!! the device comes online".

upvoted 1 times

AJMD 2 years, 12 months ago

D Question says: "to !!!support!!! the on-boarding process !!!before!!! the device comes online".C. Set the device as valid (to !!!support!!! the on-boarding process !!!before!!! the device comes online"). See the document linked below by CCNPCollab1297.

upvoted 1 times

timtgh 2 years, 11 months ago

C. Set the device as valid (to !!!support!!! the on-boarding process !!!before!!! the device comes online"). See the document linked below by CCNPCollab1297.

upvoted 1 times

bchrisb 3 years ago

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf : Technical Tip: A WAN Edge device within staging state will establish only control connections with the SD-WAN controllers. No data plane connections are established across WAN Edge devices. To fully onboard the device, the 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.

upvoted 1 times

kk_learn 3 years, 6 months ago

D Question says: "to !!!support!!! the on-boarding process !!!before!!! the device comes online". 'Support' and 'before online' says to us that device must be staged, since it is not online (doesn't send traffic), but we must control it (hence, support it). We can do that if we stage device and send list to controllers. When we validate device, it comes online (and question says before it comes online).

upvoted 2 times

Erik_N 3 years, 8 months ago

It is asking for a configuration task on vManage, so that would be C The whitelist will be shared automatically with other controllers. No need to configure anything for that.

upvoted 1 times

khanda 4 years ago

WAN Edge devices have to be known and authorized by all the SD-WAN controllers before allowing the device onto the network. D seems to be correct for me.

upvoted 1 times

khanda 4 years ago

WAN Edge devices have to be known and authorized by all the SD-WAN controllers before allowing the device onto the network. D seems to be correct for me.Yes you are right, but they need to be validated before, you can use the checkbox when uploading the list into the vManage, or you go to devices and validate them one by one and then you will share the valid list to the controllers. That is why when you do a show valid-vedges on the vSmart you will only see the ones that are valid and no the whole list.

upvoted 1 times

MiraGod 3 years, 11 months ago

Yes you are right, but they need to be validated before, you can use the checkbox when uploading the list into the vManage, or you go to devices and validate them one by one and then you will share the valid list to the controllers. That is why when you do a show valid-vedges on the vSmart you will only see the ones that are valid and no the whole list.

upvoted 3 times

immphoenix 4 years, 3 months ago

I am not sure vBond will be able to orchestra the devices with vmanage with having known the list. So the answer is very clear to me.

upvoted 1 times

DP 4 years, 6 months ago

C is the correct answer. The list has to be validated first before being sent to the other controllers.

upvoted 2 times

Izeflexzz 4 years, 6 months ago

I'd say C seems to be the likely answer based on Sky_Soul's link.

upvoted 1 times

juniper 4 years, 6 months ago

D is correct

upvoted 2 times

Question #62 *Topic 1*

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

A. vSmart at the branch

B. vEdge at the branch

C. vEdge at the hub

D. vSmart at the hub

Suggested Answer: *C*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/07Policy_Applications/02Service_Chaining/Service_Chaining_Configuration_Examples

Community vote distribution

C (100%)

ramjam Highly Voted 4 years, 2 months ago

correct. https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=472

upvoted 7 times

AJMD Most Recent 1 year, 11 months ago

Correct C

upvoted 1 times

Question #63 *Topic 1*

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

A. system IP address, link color, and encapsulation

B. origin, originator, and preference

C. site ID, tag, and VPN

D. firewall, IPS, and application optimization

Suggested Answer: *A*
Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.2/03Routing/01Unicast_Overlay_Routing_Overview#TLOC_Routes

kentkyye Most Recent 2 years, 1 month ago

A, A TLOC is denoted by a 3-tuple that consists of the system IP address of the OMP speaker, a color, and an encapsulation type

upvoted 1 times

CCNPWILL 2 years, 9 months ago

Correct!

upvoted 4 times

Question #64 *Topic 1*

Which type of route advertisement of OMP can be verified?

A. Origin, TLOC, and VPN

B. Origin, TLOC, and service

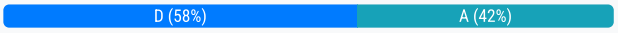
C. OMP, VPN, and origin

D. OMP, TLOC, and service

Suggested Answer: *D*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.2/03Routing/01Unicast_Overlay_Routing_Overview#OMP_Route_Advertisements

Community vote distribution



Decorations Most Recent 3 months, 3 weeks ago

This question say, what type of routes OMP advertising. Answer is OMP routes, TLoC routes and service route.

upvoted 1 times

Rbrahmi 9 months ago

OMP route advertisements that can be verified are OMP routes (or vRoutes), TLOC routes, and service routes. OMP routes represent reachability information from the site's local network, TLOC routes represent the transport location (physical connection to the WAN) and its properties, and service routes map network services (like firewalls) to their location.

upvoted 1 times

Rosh8787 1 year, 10 months ago

A is the correct answer

upvoted 4 times

Veeru_k23 1 year ago

D is the Correct Answer.

upvoted 1 times

Rosh8787 1 year, 10 months ago

A is the correct answerI think it's D. Question asks "which type of route" not "which attributes of routes"

upvoted 4 times

WarlockLV 1 year, 7 months ago

I think it's D. Question asks "which type of route" not "which attributes of routes"

upvoted 2 times

PandiyaGomathi 2 years ago

A is correct answer

upvoted 4 times

siang 2 years, 2 months ago

D is correct

upvoted 2 times

RafaJohnston76 2 years, 6 months ago

A is correct, there is no service information, however there is the VRF (VPN) to which the OMP routes belong https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-unicast-routing.html#:~:text=OMP%20advertises%20each%20TLOC%20separately,translated%20address%20of%20the%20TLOC.

upvoted 2 times

thomazmr 2 years, 6 months ago

Correct D

upvoted 2 times

AJMD 2 years, 12 months ago

Correct D

upvoted 1 times

eoin1907g 3 years ago

correct Ans is D

upvoted 1 times

williancm19 3 years, 2 months ago

Selected Answer: A

I guess A is correct.

upvoted 3 times

kup_rjds 3 years, 2 months ago

D https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/bridging-routing-segmentation-qos/vedge/bridging-routing-segmentation-qos-book/unicast-overlay-routing.html

upvoted 3 times

williancm19 3 years, 2 months ago

I guess A is correct.check this link... i have same doughts https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/bridging-routing-segmentation-qos/vedge/bridging-routing-segmentation-qos-book/unicast-overlay-routing.html

upvoted 3 times

kup_rjds 3 years, 2 months ago

check this link... i have same doughts https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/bridging-routing-segmentation-qos/vedge/bridging-routing-segmentation-qos-book/unicast-overlay-routing.html

upvoted 1 times

williancm19 3 years, 2 months ago

I think would be the letter A, as per the 'sh omp routes' output: vEdge120# show omp routes ---------- omp route entries for vpn 1 route 10.110.1.0/30 ---------- RECEIVED FROM: peer 1.1.1.30 path-id 1 label 1005 status C,I,R loss-reason not set lost-to-peer not set lost-to-path-id not set Attributes: originator 1.1.1.110 type installed tloc 1.1.1.110, mpls, ipsec ultimate-tloc not set domain-id not set overlay-id 1 site-id 110 region-id None region-path 65534 preference not set tag not set origin-proto connected origin-metric 0 as-path not set community not set unknown-attr-len not set

upvoted 3 times

ldro 3 years, 9 months ago

D - https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.2/03Routing/01Unicast_Overlay_Routing_Overview

upvoted 2 times

kentkyye 4 years, 7 months ago

OMP advertises the following types of routes: -OMP routes (also called vRoutes) -Transport locations (TLOCs) -Service routes

upvoted 2 times

lakatos 5 years, 3 months ago

I think it should be A. An OMP route has an Origin just like a BGP route, a TLOC as the next hop and a VPN assocaited with each route.

upvoted 1 times

d2001 5 years, 2 months ago

OMP routes (also called vRoutes)— TLOC • Service routes—Identifiers that tie an OMP route to a service in the network, specifying the location of the service in the network. Services include firewalls, Intrusion Detection Systems (IDPs), and load balancers.

upvoted 1 times

lakatos 5 years, 3 months ago

I think it should be A. An OMP route has an Origin just like a BGP route, a TLOC as the next hop and a VPN assocaited with each route.Correct answer is D. Read the link and it is plainly put. OMP routes (vRoute, TLOC, and service)

upvoted 1 times

CCNPWILL Highly Voted 5 years, 3 months ago

Correct answer is D. Read the link and it is plainly put. OMP routes (vRoute, TLOC, and service)

upvoted 10 times

Question #65 *Topic 1*

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

A. show bfd tloc-summary-list

B. show bfd history

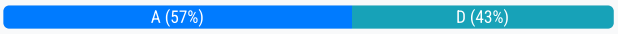
C. show bfd summary

D. show bfd sessions

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/sdwan-cr-book_chapter_0100.html#wp5111537210

Community vote distribution



LukaszCof Most Recent 6 months, 2 weeks ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/operational-cmd.html#r_show_bfd_tloc_summary_list_8976.xml show bfd tloc-summary-list—Display BFD session summary information per TLOC (on vEdge routers only).

upvoted 2 times

regissan 1 year, 7 months ago

TLOC = SYSTEM-IP + COLOR + ENCAP O comando que mostra os três é: SHOW BFD SESSIONS ENTÃO, "D" está correto.TLOC = SYSTEM-IP + COLOR + ENCAP The command that shows the three is: SHOW BFD SESSIONS THEN, "D" is correct.

upvoted 2 times

regissan 1 year, 7 months ago

Selected Answer: D

TLOC = SYSTEM-IP + COLOR + ENCAP O comando que mostra os três é: SHOW BFD SESSIONS ENTÃO, "D" está correto.

upvoted 2 times

regissan 1 year, 7 months ago

TLOC = SYSTEM-IP + COLOR + ENCAP The command that shows the three is: SHOW BFD SESSIONS THEN, "D" is correct.

upvoted 1 times

rubendrios 1 year, 9 months ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/operational-cmd.html#r_show_bfd_summary_5339.xml literally says, show bfd tloc-summary-list—Display BFD session summary information per TLOC (on vEdge routers only).

upvoted 4 times

jdisais23 1 year, 9 months ago

A is correct since question if Per TLOC vEdge# show bfd tloc-summary-list BFD TLOC Summary Information: ---------- TLOC IP Color Encapsulation State Sessions Up Down ---------- 192.168.1.1 biz-internet ipsec up 3 3 0 192.168.1.2 mpls ipsec up 4 4 0 192.168.1.3 public-internet ipsec down 2 0 2 10.1.1.1 lte ipsec up 1 1 0 ---------- Total Sessions: 10, Up: 8, Down: 2

upvoted 2 times

mikidvd51 1 year, 10 months ago

C8300-EDGE#sh sdwan bfd tloc-summary-list SESSIONS SESSIONS SESSIONS IF NAME ENCAP TOTAL UP FLAP ---------- TenGigabitEthernet0/0/4.3001 ipsec 50 50 134 TenGigabitEthernet0/0/4.3002 ipsec 50 50 282

upvoted 1 times

siang 2 years, 2 months ago

A is correct

upvoted 2 times

PureInertiaCopy 2 years, 5 months ago

This is the output for A: vEdge-Site2# show bfd tloc-summary-list IF SESSIONS SESSIONS SESSIONS NAME ENCAP TOTAL UP FLAP ---------- ge0/0 ipsec 3 3 0 ge0/1 ipsec 3 3 0 vEdge-Site2# Which leads me to vote D

upvoted 4 times

CCNPWILL 5 years, 3 months ago

Correct.

upvoted 1 times

Question #66 *Topic 1*

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

A.

```
VPN 10
ip route 0.0.0.0/0 vpn 0
VPN 0
interface Gig1/1
nat
```

B.

```
VPN 10
ip route 0.0.0.0/0 vpn 0
```

C.

```
policy
data-policy DPI
vpn-list vpn10
sequence 10
match
app-list YouTube
destination-port 80 443
!
action accept
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
```

D.

```
vpn 10
ip route 0.0.0.0/0 vpn 0
```

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

Suggested Answer:
Official Answer: C

TheNetworkStudent Highly Voted 5 years ago

Literally can't be anything but A, it's the only one not blocking youtube AND implementing a local breakout via NAT on VPN 0. B doesn't do anything usefull, C and D look impressive but C doesn't implement DIA and D blocks youtube. Conclusion: A is Correct.Thank you... I knew that the answer was incorrect.

upvoted 18 times

TheNetworkStudent Highly Voted 5 years ago

Literally can't be anything but A, it's the only one not blocking youtube AND implementing a local breakout via NAT on VPN 0.

B doesn't do anything usefull, C and D look impressive but C doesn't implement DIA and D blocks youtube.

Conclusion: A is Correct.

upvoted 18 times

PureInertiaCopy 2 years, 5 months ago

Thank you... I knew that the answer was incorrect.

upvoted 1 times

Mr_Cipher 5 years, 1 month ago

I think it's A. Design Considerations on using NAT DIA: • Along with the configuration of a NAT DIA route within the service-side VPN, ensure that you enable NAT on the Internet-facing interface within VPN 0, as Internet traffic is redirected based on the NAT DIA route from the service side to the NAT-enabled transport side interface. • If you are using one of the routing protocols on the service-side VPN, ensure that you redistribute the NAT DIA route into it. • In NAT DIA, it is assumed that NAT/PAT is configured on one or more interfaces in VPN 0. • By default, an IP static route has an administrative distance of 1, a NAT DIA route has a distance of 6, and OMP has a distance of 251. Therefore, the NAT DIA route overwrites the OMP advertised default to prefer the local Internet exit, instead of taking the remote data centre Internet exit within a VPN.

upvoted 6 times

Rosh8787 Most Recent 1 year, 10 months ago

Option C is correct because the question asks about YouTube. Option A is correct as well but for local internet breakout. With Option A, you open floodgates to internet to access anything and everything.

upvoted 1 times

Stanleymahamadi 2 years, 2 months ago

Correct answer A

upvoted 1 times

timtgh 2 years, 11 months ago

Absolutelty A. DIA can be done two ways: Using a default route for a VPN, or using centralized local policy. Options A and B use the default route method. A does it correctly, and B is missing the NAT command. C and D use the local policy method, but incorrectly. For DIA, the local policy has a nat command, and is applied on the service side, so Option C is wrong. Option D is obviously wrong on so many levels.

upvoted 1 times

timtgh 2 years, 11 months ago

Absolutelty A. DIA can be done two ways: Using a default route for a VPN, or using centralized local policy. Options A and B use the default route method. A does it correctly, and B is missing the NAT command. C and D use the local policy method, but incorrectly. For DIA, the local policy has a nat command, and is applied on the service side, so Option C is wrong. Option D is obviously wrong on so many levels.Correction (mistyped): should say "centralized data policy," not "centralized local policy."

upvoted 1 times

timtgh 2 years, 11 months ago

Correction (mistyped): should say "centralized data policy," not "centralized local policy."

upvoted 1 times

AJMD 2 years, 12 months ago

A is Correct

upvoted 1 times

AJMD 3 years ago

Answer: A

upvoted 1 times

NetArch_Teck 3 years, 1 month ago

Correct answer is C The question is specifically asking for traffic destined to youtube, not a default route to DIA.

upvoted 1 times

NetArch_Teck 3 years, 1 month ago

Correct answer is C The question is specifically asking for traffic destined to youtube, not a default route to DIA.This was suppose to say A "NOT C" "Big Lock Down FIngers"

upvoted 1 times

NetArch_Teck 3 years ago

This was suppose to say A "NOT C" "Big Lock Down FIngers"

upvoted 1 times

ccie_race 4 years ago

A because the main requirement is to enable nat on VPN0 and direct the service VPN default traffic to vpn0

upvoted 2 times

juniper 4 years, 6 months ago

A DIRECT INTERNET ACCESS

upvoted 3 times

Ben_001 4 years, 7 months ago

Is in question, which policy?

upvoted 2 times

CesarVergaraGalindo 4 years, 10 months ago

A is Correct

upvoted 2 times

Nean 5 years ago

1. Activate Network Address Translation (NAT) on the transport interface, where DIA should be used: vpn 0 ! interface ge0/0 description "DIA interface" ip address 192.168.109.4/24 nat <<<<==== NAT activated for a local DIA !

upvoted 1 times

Thor69 5 years, 1 month ago

A is correct the Answer: As explained in figure7,withinthe 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 theNAT-enabled interface in VPN 0.
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2020aug.pdf

upvoted 1 times

ramjam 5 years, 2 months ago

A. https://community.cisco.com/t5/sd-wan-and-cloud-networking/local-internet-breakout/m-p/4083996#M1992

upvoted 1 times

ramjam 5 years, 2 months ago

A. https://community.cisco.com/t5/sd-wan-and-cloud-networking/local-internet-breakout/m-p/4083996#M1992A. Is the answer.
https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/215022-how-to-select-a-particular-site-to-be-a.html?dtid=osscdc000283

upvoted 1 times

ramjam 5 years, 2 months ago

A. Is the answer. https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/215022-how-to-select-a-particular-site-to-be-a.html?dtid=osscdc000283

upvoted 1 times

FLYT 5 years, 3 months ago

C. local policy is required to do DIA.

upvoted 2 times

go_Corona_go 5 years, 3 months ago

notice local breakout

upvoted 1 times

Question #67 *Topic 1*

Which feature template configures OMP?

A.

B.

C.

D.

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

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

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

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

Suggested Answer:
Official Answer: A

amitsir Most Recent 2 years, 3 months ago
Answer A https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Configuration/Templates/OMP
upvoted 3 times

ramjam 2 years, 8 months ago
correct.
upvoted 4 times

ramjam 2 years, 8 months ago
correct.https://search.cisco.com/search?locale=enPH&query=feature%20template%20configures%20OMP&bizcontext=&mode=text&clktyp=enter&autosuggest=false&tareqid=1624135001062&pq=Cisco%20IOS%20XE%20:%20What%20route%20can%20you%20configure%20to%20enable%20local%20Internet%20breakout%20from%20the%20remote%20site%3F&pq_cat=DeepQA
upvoted 4 times

ramjam 2 years, 8 months ago

https://search.cisco.com/search?locale=enPH&query=feature%20template%20configures%20OMP&bizcontext=&mode=text&clktyp=enter&autosuggest=false&tareqid=1624135001062&pq=Cisco%20IOS%20XE%20:%20What%20route%20can%20you%20configure%20to%20enable%20local%20Internet%20breakout%20from%20the%20remote%20site%3F&pq_cat=DeepQA

upvoted 3 times

Question #68 *Topic 1*

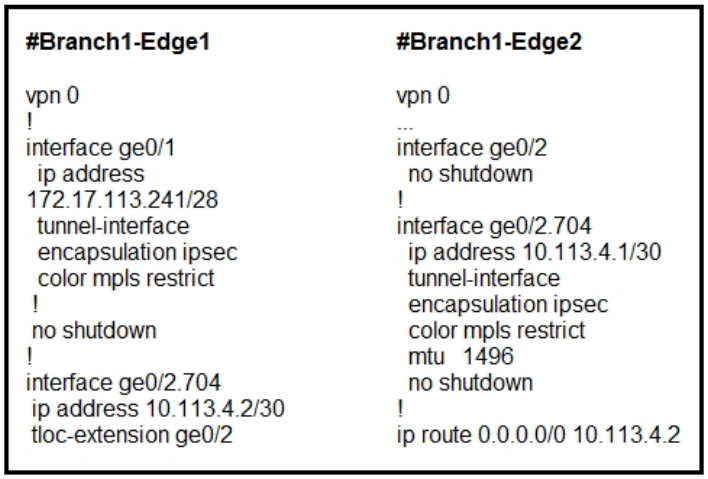
Refer to the exhibit. Which configuration change is needed to configure the tloc-extension on Branch1-Edge1?

A.

B.

C.

D.



#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
 ip address 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
```

```
interface ge0/2.704
  ip address 10.113.4.1/30
  tunnel-interface
   encapsulation ipsec
   color mpls restrict
   no shutdown

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

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

 interface ge0/2.704
   ip address 10.113.4.1/30
   tunnel-interface
    encapsulation ipsec
    color mpls restrict
    mtu 1496
    tloc-extension ge0/2
    no shutdown
```

Suggested Answer:
Official Answer: D

ccie_race Highly Voted 4 years ago

B is correct. D is incorrect because you dont need tunnel interface on g0/2.

upvoted 16 times

A_Wolf Highly Voted 4 years, 6 months ago

B is correct. the config shown on B shows the correct interface on the tloc-extension (ge0/1) and also has the correct ip address 10.113.4.2. Note that the default route on Edge2 points to 10.113.4.2 D is incorrect because: 1- has the incorrect address 10.113.4.1 2- the tloc-extension interface refers to the same interface where the tloc is being defined (ge0/2). That is not possible.

upvoted 8 times

Ma33 Most Recent 1 year, 7 months ago

B is correct. TLOC extension is done od Ge0/1 interface.

upvoted 1 times

Rosh8787 1 year, 10 months ago

B is the correct answer.

upvoted 1 times

siang 2 years, 2 months ago

B is correct.

upvoted 1 times

Fikie 2 years, 2 months ago

Answer B

upvoted 1 times

thomazmr 2 years, 6 months ago

B is correct.

upvoted 1 times

AJMD 2 years, 12 months ago

Correct B

upvoted 1 times

Nandhujoe 3 years, 3 months ago

B is correct answer

upvoted 3 times

Abbasym 3 years, 4 months ago

B IS THE RIGHT ANSWER.

upvoted 3 times

Idro 3 years, 9 months ago

B is correct

upvoted 5 times

kcobain87 3 years, 10 months ago

B for sure

upvoted 3 times

juniper 4 years, 6 months ago

B 100%

upvoted 4 times

Benzzyy 4 years, 7 months ago

I think "B" may be the correct answer. ge0/1 is the interface we are extending and B is the only answer referencing that interface.

upvoted 4 times

nihithp 4 years, 7 months ago

Ans B ? cehck tloc extn interface and the interface IP

upvoted 2 times

nihithp 4 years, 7 months ago

Ans B ? cehck tloc extn interface and the interface IP100% B With above configuration, only Branch1-Edge2 router sends traffic to Branch1-Edge1 router if the main route to MPLS fails (as only Edge2 has the default route to Edge1). Therefore we have to configure the TLOC Extension under subinterface ge0/2.704 of Branch1-Edge1 with the command “tloc-extension ge0/1”. Note: We change the mtu to 1496 to accommodate for the dot

upvoted 2 times

Speirsington 4 years, 7 months ago

100% B With above configuration, only Branch1-Edge2 router sends traffic to Branch1-Edge1 router if the main route to MPLS fails (as only Edge2 has the default route to Edge1). Therefore we have to configure the TLOC Extension under subinterface ge0/2.704 of Branch1-Edge1 with the command “tloc-extension ge0/1”. Note: We change the mtu to 1496 to accommodate for the dot

upvoted 4 times

Question #69 *Topic 1*

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

A. 6

B. 2

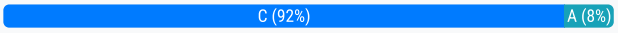
C. 4

D. 8

Suggested Answer: *A*

Official Answer: A

Community vote distribution



TheNetworkStudent Highly Voted 4 years, 5 months ago

1 vEdge with 2 TLOCs connects to 2 TLOCs for each of it's own TLOCs (so 2 * 2), which should be C = 4... right?

upvoted 13 times

SmartForNothing Highly Voted 4 years, 3 months ago

Like the previous comment said "1 vEdge with 2 TLOCs connects to 2 TLOCs for each of its own TLOCs (so 2 * 2), which should be C = 4"

upvoted 9 times

siang Most Recent 1 year, 8 months ago

C is correct

upvoted 1 times

eric0430 2 years, 12 months ago

C is correct since question is only "data tunnels on each Site".

upvoted 2 times

kcobain87 3 years, 3 months ago

C for sure

upvoted 3 times

phi5 3 years, 5 months ago

Answer is C, 1 edge each with two TLOCs each equals 4

upvoted 2 times

khanda 3 years, 6 months ago

4 is correct

upvoted 1 times

ccie_race 3 years, 6 months ago

4 is correct

upvoted 1 times

bender_the_offender 3 years, 8 months ago

each link builds one tunnel to each link on the other device which means (1*2)+(1*2) = 4

upvoted 1 times

ya9299 3 years, 10 months ago

C Correct

upvoted 1 times

khanda 3 years, 10 months ago

4 data tunnels

upvoted 1 times

paloncho06 3 years, 11 months ago

Essentially two transports per vEdge, ergo 4 tunnels.

upvoted 1 times

Khrysis 3 years, 11 months ago

C it is

upvoted 1 times

Khrysis 3 years, 12 months ago

Answer = C

upvoted 1 times

Hoosainsays 3 years, 12 months ago

The Answer is C

upvoted 1 times

Baio 4 years ago

data tunnels are 4

upvoted 1 times

Question #70 *Topic 1*

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 peers

B. show omp route

C. show omp sessions

D. show omp tlocs

Suggested Answer: *D*

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

Community vote distribution



RafaJohnston76 Most Recent 2 years ago

D is Correct #show omp tlocs | tab will get the color information because is in a table format

upvoted 1 times

BrentL 2 years, 8 months ago

Made a mistake on this: font was so large the screen wrapped and wasn't displsaying the color and tloc details. I thought something was off.. I'd agree show omp tlocs is the correct answer for this one....D

upvoted 1 times

BrentL 2 years, 8 months ago

If you run show omp tlocs like shown in the example it doesn't show the color. Show OMP route does although that's not the command without the S but works. I couldn't add a screen shot of show omp tlocs output but it's shown in example below and you can see there's no color label.Speirsington's comment below shows the show omp tlocs command, and you can see that it does show the color.

upvoted 1 times

BrentL 2 years, 8 months ago

If you run show omp tlocs like shown in the example it doesn't show the color. Show OMP route does although that's not the command without the S but works. I couldn't add a screen shot of show omp tlocs output but it's shown in example below and you can see there's no color label.

upvoted 1 times

timtgh 2 years, 5 months ago

Speirsington's comment below shows the show omp tlocs command, and you can see that it does show the color.

upvoted 1 times

Alchobashko 3 years ago

There is no correct answer actually: sdwn01# show omp tlocs detail (this is showing you learned colors) ---------- tloc entries for 1.1.1.2 biz-internet ipsec ---------- RECEIVED FROM: peer 0.0.0.0 uslav-colo-1fdc-sdwn01# show omp tlocs (not showing you colors) PUBLIC PRIVATE PSEUDO PUBLIC PRIVATE PUBLIC IPV6 PRIVATE IPV6 BFD FROM PEER STATUS KEY PUBLIC IP PORT PRIVATE IP PORT IPV6 PORT IPV6 PORT STATUS ---------- 0.0.0.0 C,Red,R 1 1.1.1.1 12387 1.1.1.1 12387 :: 0 :: 0 up

upvoted 1 times

mac_tire 3 years, 10 months ago

B is incorrect for this answer because the actual command is show omp routes not show omp route. therefore D should be the correct answer as it is the full command. this can be looked up on this page. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/operational-cmd.html#r_show_omp_tlocs_1923.xml

upvoted 1 times

Speirsington 4 years, 1 month ago

The answer is D: vEdge1# show omp tlocs ---------- tloc entries for 10.4.0.1 mpls ipsec ---------- RECEIVED FROM: peer 10.100.0.12 status C,I,R loss-reason not set lost-to-peer not set lost-to-path-id not set Attributes: attribute-type installed encap-key not set encap-proto 0 encap-spi 256 encap-auth sha1-hmac,ah-sha1-hmac encap-encrypt aes256 public-ip 172.31.14.2 public-port 12346 private-ip 172.31.14.2 private-port 12346

upvoted 3 times

Amitmanesar 4 years, 1 month ago

B should be the correct one , as it displays tloc and color information

upvoted 1 times

ramjam 4 years, 8 months ago

correct..

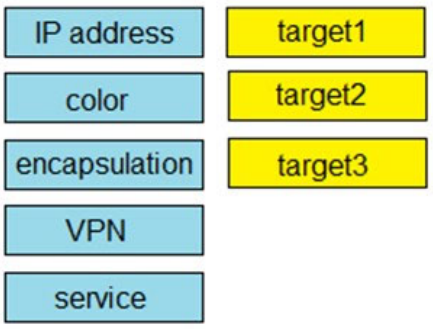
upvoted 1 times

Question #71 *Topic 1*

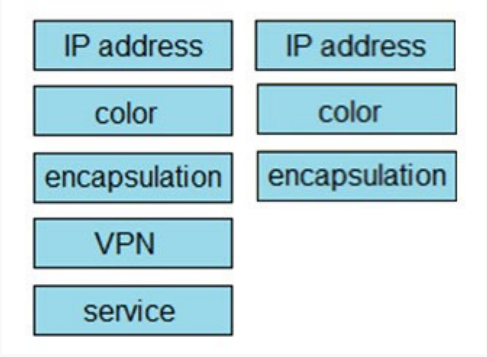
DRAG DROP -

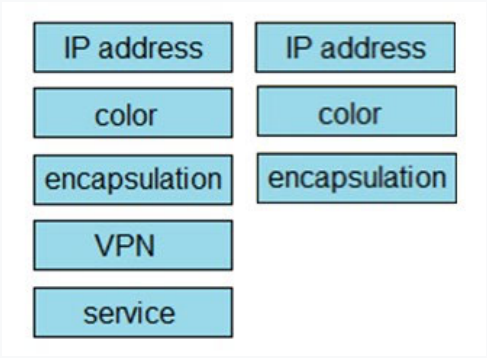
Drag and drop the attributes from the left that make each transport location unique onto the right. Not all options are used.

Select and Place:



Suggested Answer:





Reference: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

Speirsington Most Recent 2 years ago

IP colour enacp

upvoted 3 times

Question #72 *Topic 1*

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

A. ASR1000v

B. vEdge 100wm

C. CSR1000v

D. vEdge cloud

E. vEdge 5000v

Suggested Answer: *C, D*

Official Answer: CD

Community vote distribution

CD (100%)

ChrisCCNA Most Recent 2 years ago

CD are correct

upvoted 2 times

Question #73 *Topic 1*

Refer to the exhibit. Which binding is created using the tloc-extension command?

```
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
```

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

B. between ge 0/2.101 of port-type service 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

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Speirsington Highly Voted 4 years, 6 months ago

D - Transport to Transport

upvoted 9 times

Faridtnx Most Recent 6 months ago

TLOC extensions always occur between two transport-type ports in VPN 0. They do not involve "service-type" ports

upvoted 1 times

Scythe00 9 months, 2 weeks ago

In Cisco SD-WAN, interfaces are categorized as either: - Transport-type: Used for WAN connectivity (e.g., MPLS, Internet), and configured with tunnel-interface. - Service-type: Used for LAN or internal routing (e.g., VPN 1, VPN 10), and typically do not have tunnel-interface. When you apply the tloc-extension command to a service-type interface, you're telling the system: "This service interface will carry traffic that extends the transport reach of another WAN Edge device." But critically: - The interface itself does not become a transport interface. - It does not participate in control plane or data plane tunnel formation directly. - It simply acts as a bridge to extend the transport capabilities of another interface (usually on a different device)

upvoted 1 times

Loi2525 2 years ago

Zdrobici is correct. refer to Figure 7 in: https://www.networkacademy.io/ccie-enterprise/sdwan/connecting-to-the-wan-using-tloc-extension All required configuration is shown in figure 7 above. Once the config is applied, we can see that vEdge-2's ge0/0 is NOW A TRANSPORT interface and acts as a local TLOC marked with the "biz-internet" color.

upvoted 1 times

routingtable 2 years, 1 month ago

C is correct The primary function of tloc-extension is to extend the transport interface properties to a service interface. This means that after the configuration, ge0/2.101 can now use ge0/0's transport capabilities for overlay traffic. However, ge0/2.101 does not become a transport interface itself; it remains a service interface that can utilize the transport functions of ge0/0.

upvoted 4 times

siang 2 years, 2 months ago

C is correct

upvoted 1 times

thomazmr 2 years, 6 months ago

D - in the device template TLOCs (extension) are configured in the transport.

upvoted 2 times

Aldebeer 2 years, 8 months ago

I agree with the volks: D

upvoted 3 times

Zdrobici 3 years, 6 months ago

initially port type is SERVICE, after tloc-ext config is ADDED is becoming TRANSPORT. so we can say that the bound is done between TRANSP interfaces, because bound is done after tloc-ext cfg is added, wright? take a look on the cli outputs from https://www.networkacademy.io/ccie-enterprise/sdwan/connecting-to-the-wan-using-tloc-extension

upvoted 3 times

Alchobashko 3 years, 6 months ago

TLOC Ext interface is NOT service as it is connected to other WAN edge, no service/local network connections

upvoted 1 times

moraist 3 years, 6 months ago

D is correct. Reference: https://ccieme.wordpress.com/category/networking/sd-wan/tloc-extensions/ Go to the end of the page and see the TLOC-extension example diagram.

upvoted 3 times

Erik_N 3 years, 8 months ago

TLOCs are always in VPN0 which is Transport answer D

upvoted 2 times

atiWok 3 years, 9 months ago

It's C.. Check the "show interface| tab " in lab if you don't belive. +https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge/systems-interfaces-book/configure-interfaces.html

upvoted 2 times

Idro 3 years, 9 months ago

C Is correct , they are asking about the port-type not the VPN type ! https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20-x/systems-interfaces-book/configure-interfaces.html

upvoted 2 times

alin93 3 years, 9 months ago

the "extention" command can only be made between transport interfaces

upvoted 1 times

EMAG86 3 years, 10 months ago

transport to transport

upvoted 1 times

khanda 4 years ago

Correct Answer is C, I have tried it in the lab. Use show command : show interface description vpn 0 | tab* show interface vpn 0 | tab

upvoted 2 times

khanda 4 years ago

Selected Answer: C

Correct Answer is C, I have tried it in the lab. Use show command : show interface description vpn 0 | tab

upvoted 2 times

atiWok 3 years, 9 months ago

* show interface vpn 0 | tab

upvoted 1 times

Question #74 *Topic 1*

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?

A.

```
sdwan
  interface g0/0
    gre-interface
      tloc-extension-gre-to 10.1.1.1
```

B.

```
sdwan
  interface g0/0
    tunnel-interface
      tloc-extension-gre-to 10.1.1.1
```

C.

```
sdwan
  interface g0/0
    extended-interface
      tloc-extension-gre-from 10.1.1.1
```

D.

```
sdwan
  interface g0/0
    tloc-interface
      tloc-extension-gre-from 10.1.1.1
```

Suggested Answer:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/sdwan-cr-book_chapter_010.html#wp2314758100

Almanac Highly Voted 5 years, 4 months ago
yes B is the right answer sdwan nterface interface-name tunnel-interface tloc-extension-gre-to extended-interface-ip-addressYeah, as per the documentation link they are actually quoting
upvoted 29 times

Almanac Highly Voted 5 years, 4 months ago
yes B is the right answer sdwan nterface interface-name tunnel-interface tloc-extension-gre-to extended-interface-ip-address
upvoted 29 times

msstanick Most Recent 7 months, 1 week ago
Yeah, as per the documentation link they are actually quoting
upvoted 1 times

Speirsington 4 years, 7 months ago
B is correct - the rest aren't valid commands: vedge(config-vpn-0)# int g0/0 vedge(config-interface-g0/0)# gre-interface ----------^ syntax error: unknown command vedge(config-interface-g0/0)# extended-interface ----------^ syntax error: unknown command vedge(config-interface-g0/0)# tloc-interface ----------^ syntax error: unknown command vedge(config-interface-g0/0)# tunnel-interface vedge(config-tunnel-interface)#
upvoted 13 times

Kojy 11 months, 3 weeks ago
Official Cisco Documentation 1. Configure Layer 3 TLOC Extension Cisco provides a dedicated support document titled “Configure Layer 3 TLOC Extension” that details the setup for TLOC extension via GRE. It specifically describes the setup and syntax used to extend the transport location over a GRE tunnel. Cisco 2. Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide (IOS XE) In the System Interfaces Guide, Cisco explains that for TLOC extension, you bind the service-side physical interface to the GRE tunnel by using the following syntax under SD-WAN interface

configuration mode: sdwan interface GigabitEthernetX/Y gre-interface tloc-extension-gre-to This confirms that the correct command is tloc-extension-gre-to under a gre-interface, not under tunnel-interface or other variants. Cisco

upvoted 1 times

Adenismail 2 years ago

B is the correct answer

upvoted 1 times

thomazmr 2 years, 6 months ago

B is correct

upvoted 1 times

Aldebeer 2 years, 9 months ago

it should be B

upvoted 2 times

Clouddon 2 years, 10 months ago

Bis correct

upvoted 1 times

timtgh 2 years, 11 months ago

They worded the question badly. They ask which config is used to extend TLOC to another router. Worded that way, no answer is correct. Option B is the only answer without fake syntax, so it must be correct. But option B is not the config on the router that is extending the TLOC. It is the config on the other router, that the TLOC is being extended to. Still, the other answers are wrong on either router because they have fake syntax.

upvoted 1 times

AJMD 2 years, 12 months ago

Correct B vManage Feature Template For Cisco IOS XE routers only: Configuration ► Templates ► VPN Interface Ethernet Command Hierarchy sdwan interface interface-name tunnel-interface tloc-extension-gre-to extended-interface-ip-address

upvoted 1 times

hopatrickhk88 3 years, 1 month ago

Yes B is correct answer https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/220333-configure-layer-3-tloc-extension.html

upvoted 1 times

Idro 3 years, 9 months ago

B is correct : 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. sdwan interface interface-name tunnel-interface tloc-extension-gre-to extended-interface-ip-address https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#r_tloc_extension_gre_to_11940.xml

upvoted 1 times

kcobain87 3 years, 9 months ago

B is the right one

upvoted 1 times

khanda 4 years, 4 months ago

Correct answer is B. cEdge-4(config)# sdwan cEdge-4(config-sdwan)# interface GigabitEthernet2 cEdge-4(config-interface-GigabitEthernet2)# tunnel-interface cEdge-4(config-tunnel-interface)# tloc-extension-gre-to

upvoted 2 times

CesarVergaraGalindo 4 years, 10 months ago

B is correct

upvoted 1 times

TheNetworkStudent 5 years ago

I think tunnel-interface is the only command possible, which easily eliminates other options. So it's B.

upvoted 2 times

ramjam 5 years, 2 months ago

B. Correct Link: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/sdwan-cr-book_chapter_010.html#wp2314758100 sdwan interface tloc-extension-gre-to—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. sdwan interface tloc-extension-gre-from —Configure an interface as an extended interface, to channel TLOC traffic from a source branch router to the local WAN interface (on IOS XE routers only).

upvoted 3 times

CCNPWILL 5 years, 3 months ago

Also agree with B

upvoted 3 times

Question #75 *Topic 1*

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

A. TLOC extension

B. quality of service

C. zero-touch provisioning

D. OMP

Suggested Answer: *A*
Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf page 26

Scav20 Most Recent 2 years ago
Yes, TLOC extension is the correct answer
upvoted 3 times

Question #76 *Topic 1*

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

A. It provides orchestration to assist 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

Suggested Answer: *D*

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

Community vote distribution

D (100%)

siang Most Recent 1 year, 8 months ago

D is correct

upvoted 1 times

Tamer2022 3 years, 7 months ago

D is the correct answer.

upvoted 4 times

Question #77 *Topic 1*

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. SACK

B. SEQ

C. RTT

D. SYN

Suggested Answer: *A*

Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf page 47

Community vote distribution

A (100%)

siang Most Recent 1 year, 8 months ago

A is correct

upvoted 1 times

Speirsington 4 years ago

SACK is the answer

upvoted 2 times

Question #78 *Topic 1*

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

A. OMP tracking

B. higher group ID number

C. prefix-list tracking

D. lower timer interval

Suggested Answer: *D*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_17.1/02System_and_Interfaces/06Configuring_Network_Interfaces/Configuring_VRRP

Community vote distribution

C (100%)

MasterALX Highly Voted 4 years, 5 months ago

Correct answer is C: Track both the OMP session and a list of remote prefixes. list-name is the name of a prefix list configured with the policy lists prefix-list command on the vEdge router: vEdge(config-vrrp)# 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.

upvoted 13 times

siang Most Recent 1 year, 8 months ago

C is correct

upvoted 1 times

cytye 2 years, 10 months ago

Track Prefix List tracks both OMP and prefixes defined in the list and failover happens immediately.

upvoted 1 times

kcobain87 3 years, 3 months ago

C is correct

upvoted 1 times

khanda 3 years, 6 months ago

C is correct.

upvoted 2 times

ccie_race 3 years, 6 months ago

C is correct

upvoted 1 times

Punitkumar 3 years, 9 months ago

Why are you not updating correct answer on the site ?

upvoted 2 times

khanda 3 years, 10 months ago

Correct answer is - Track Prefix List tracks both OMP and prefixes defined in the list and failover happens immediately. https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Templates/VPN_Interface_Ethernet

upvoted 1 times

CesarVergaraGalindo 4 years, 4 months ago

C is correct

upvoted 3 times

TheNetworkStudent 4 years, 5 months ago

Practically the same question as another one, it's prefix tracking.

upvoted 3 times

Question #79 *Topic 1*

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?

A.

```
omp
 timers
  advertisement-interval 60
  holdtime 60
  graceful-restart-timer 720
```

B.

```
omp
 timers
  advertisement-interval 1
  holdtime 180
  graceful-restart-timer 43200
```

C.

```
omp
 timers
  advertisement-interval 1
  holdtime 180
  graceful-restart-timer 720
```

D.

```
omp
 timers
  advertisement-interval 60
  holdtime 180
  graceful-restart-timer 43200
```

Suggested Answer:

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.2/03Routing/02Configuring_OMP

ramjam Most Recent 2 years, 8 months ago

Correct.

upvoted 2 times

Question #80 *Topic 1*

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

A. centralized data policy

B. localized control policy

C. centralized control policy

D. localized data policy

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

siang Most Recent 1 year, 8 months ago

C is correct.

upvoted 1 times

MiraGod 3 years, 5 months ago

For topology changes you need to use a centralized control policy, correct answer is C

upvoted 1 times

ngabor 4 years, 1 month ago

Central Policy -> Custom control policy creates topology like hub and spoke

upvoted 2 times

nihithp 4 years, 3 months ago

• 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 Centralized control policy applies to the network-wide routing of traffic by affecting the information that is stored in the vSmart controller's route table and that is advertised to the vEdge routers. The effects of centralized control policy are seen in how vEdge routers direct the overlay network's data traffic to its destination. The centralized control policy configuration itself remains on the vSmart controller and is never pushed to local routers. Centralized data policy applies to the flow of data traffic throughout the VPNs in the overlay network. These policies can permit and restrict access based either on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol) or on VPN membership. These policies are pushed to the affected vEdge routers.

upvoted 1 times

nihithp 4 years, 3 months ago

Ans A ?

upvoted 2 times

Question #81 *Topic 1*

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

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

Barti1 Most Recent 1 year, 9 months ago

Orchestration assists

upvoted 2 times

Xhizors 3 years, 7 months ago

Correct!

upvoted 2 times

Question #82 *Topic 1*

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

A. vSmart Controller

B. WAN Edge Router

C. vManage

D. vBond Orchestrator

Suggested Answer: *B*
Official Answer: B

Xhizors Most Recent 2 years, 1 month ago

Correct!

upvoted 1 times

kentkyye 2 years, 1 month ago

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.

upvoted 2 times

Question #83 *Topic 1*

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

A. OSPF

B. RSVP

C. LDP

D. RIP

E. EIGRP

Suggested Answer: *A, E*

Official Answer: AE

Community vote distribution

AE (100%)

RREVECO Most Recent 1 year, 8 months ago

OK OSPF / EIGRP RIP is not available in OMP feature template (advertises)

upvoted 2 times

Xhizors 2 years, 1 month ago

Correct!

upvoted 1 times

Question #84 *Topic 1*

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

A. WAN Edge devices advertise the rendezvous point to all the receivers through the overlay network.

B. WAN Edge devices advertise the rendezvous point to all the receivers through the underlay network.

C. vSmart Controllers advertise the rendezvous point to all the receivers through the overlay network.

D. vSmart Controllers advertise the rendezvous point to all the receivers through the underlay network.

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

namashivaya Highly Voted 4 years, 9 months ago
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-multicast-routing.html 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. so IMHO, answer C is correct.No, look carefully it says replicators advertise themselves using OMP...to the vSmart controllers, its Wan edge devices that advertise themselves to vSmart and vsmart tells the rest of the network. Please read the above link carefully, Correct answer is A
upvoted 8 times

namashivaya Highly Voted 4 years, 9 months ago
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-multicast-routing.html 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.

so IMHO, answer C is correct.
upvoted 8 times

ASIMIS Most Recent 1 year, 10 months ago
No, look carefully it says replicators advertise themselves using OMP...to the vSmart controllers, its Wan edge devices that advertise themselves to vSmart and vsmart tells the rest of the network. Please read the above link carefully, Correct answer is A
upvoted 1 times

timtgh 2 years, 11 months ago
Replicator is most definitely a WAN Edge device. And it's an overlay function.
upvoted 1 times

khanda 4 years ago
C is the correct answer.
upvoted 1 times

Han2022 4 years, 2 months ago
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.
upvoted 1 times

Washiedread 4 years, 4 months ago
C is the correct answer , SD-WAN is an overlay network

upvoted 1 times

juniper 4 years, 6 months ago

Answer C

upvoted 1 times

Amitmanesar 4 years, 7 months ago

Ans B to me RP will be advertised by a VEdge because RP will be non cisco sdwan for sure. Vedge then sends this information through underlay

upvoted 2 times

amitsir 4 years, 9 months ago

Answer C https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-multicast-routing.html

upvoted 4 times

spamke 4 years, 10 months ago

I think the best answer is A but wording is weird again. 1. OMP runs in Overlay of course (Overlay Management Protocol..). Underlay is MPLS or Internet and SDWAN Fabric is built over the Overlay. 2. The answer should be that the WAN Edge routers with replicator function advertise the RP to the receivers over the overlay (so using OMP and actually vSmart advertises the OMP routes, etc. to the edges but the RP is advertised by the replicator WAN Edges) See: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-multicast-routing.html* SDWAN Fabric is built over the Underlay, sorry..

upvoted 1 times

spamke 4 years, 10 months ago

I think the best answer is A but wording is weird again.

1. OMP runs in Overlay of course (Overlay Management Protocol..). Underlay is MPLS or Internet and SDWAN Fabric is built over the Overlay. 2. The answer should be that the WAN Edge routers with replicator function advertise the RP to the receivers over the overlay (so using OMP and actually vSmart advertises the OMP routes, etc. to the edges but the RP is advertised by the replicator WAN Edges) See: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-multicast-routing.html

upvoted 1 times

spamke 4 years, 10 months ago

* SDWAN Fabric is built over the Underlay, sorry..

upvoted 1 times

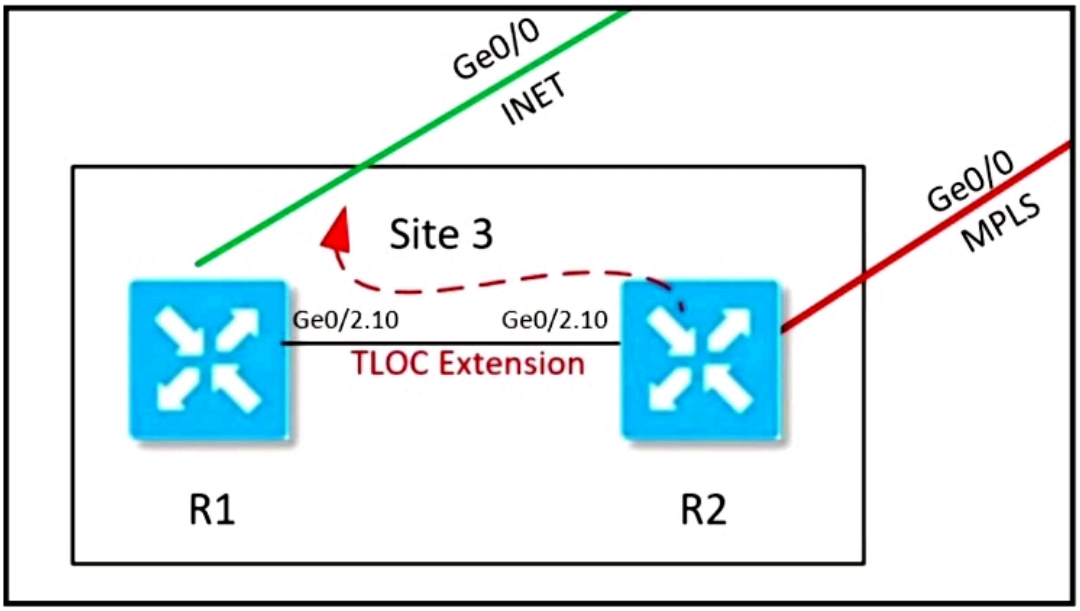
DBla 4 years, 10 months ago

Correct answer is D. But not rendezvous points. Replicators. Rendezvous points are not part of the SDWAN architecture and reside on the multicast source side. vSmart controllers doesn't participate in the overlay. Just in the underlay (VPN0). They are sending / advertising the replicator service routes in the overlay (the routes are in the overlay) via OMP and not through the overlay. OMP runs in underlay.

upvoted 1 times

Question #85 *Topic 1*

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



A. R1 interface ge0/2 interface ge0/2.10 ip address 43.43.43.2/30 tloc-extension ge0/0 tunnel-interface color public-internet R2 interface ge0/2 interface ge0/2.10 ip address 43.43.43.1/30 tunnel-interface color public-internet

B. R1 interface ge0/2 mtu 1504 no shutdown interface ge0/2.10 ip address 43.43.43.2/30 tunnel-interface color public-internet R2 interface ge0/2 mtu 1504 no shutdown interface ge0/2.10 ip address 43.43.43.1/30 tloc-extension ge0/0

C. R1 interface ge0/2 mtu 1504 no shutdown interface ge0/2.10 ip address 43.43.43.2/30 tloc-extension ge0/0 R2 interface ge0/2 mtu 1504 no shutdown interface ge0/2.10 ip address 43.43.43.1/30 tunnel-interface color public-internet

D. R1 interface ge0/2 no shutdown interface ge0/2.10 ip address 43.43.43.2/30 tloc-extension ge0/0 R2 interface ge0/2 no shutdown interface ge0/2.10 ip address 43.43.43.1/30 tloc-extension ge0/0

Suggested Answer: *C*
Official Answer: C

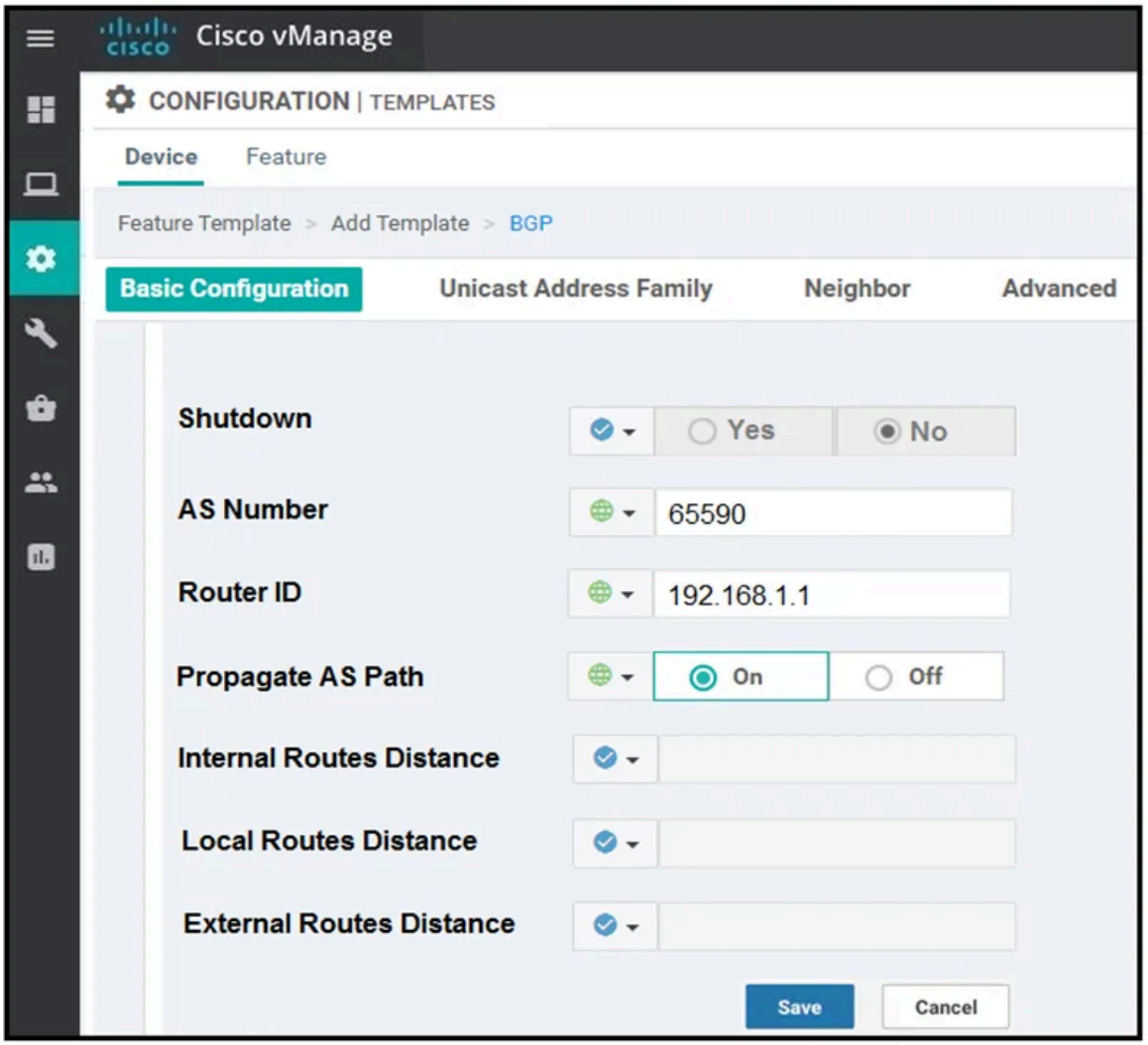
Community vote distribution
C (100%)

Khrysis Highly Voted 3 years, 7 months ago
C R1 interface ge0/2 mtu 1504 no shut ! interface ge0/2.10 ip address 43.43.43.2/30 tloc-extension ge0/0 ! R2 interface ge0/2 mtu 1504 no shut ! interface ge0/2.10 ip address 43.43.43.1/30 tunnel interface color public !
upvoted 6 times

AJMD Most Recent 1 year, 11 months ago
Correct C
upvoted 1 times

Question #86 *Topic 1*

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 Routes Distance to 20.

D. Configure External Routes Distance to 20.

Suggested Answer: *C*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-unicast-routing.html

Community vote distribution

A (52%) C (48%)

MikeG2055 Most Recent 8 months, 1 week ago

The question just asks about IBGP routes. If you change the "Internal Routes" the config that is adjusted is for what IBGP route distance is, not the local BGP routes. "distance bgp 20 XXX 20" . The description in the guides are very misleading but that is what the config does.

upvoted 3 times

1d03e21 10 months, 1 week ago

C is correct: Internal Routes Distance (EBGP): Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another. Range: 0 through 255 - Default: 200 Local Routes Distance (IBGP): Specify the BGP route administrative distance for routes within the local AS. By default, a route received locally from BGP is preferred over a route received from OMP. Range: 0 through 255 Default: 200 - External Routes

Distance: Specify the BGP route administrative distance for routes learned from other sites in the overlay network. Range: 0 through 255 Default: 20 https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-unicast-routing.html

upvoted 1 times

uzbin 1 year, 3 months ago

Internal routes = iBGP Local routes = Locally connected interface IP subnets External routes = eBGP

upvoted 3 times

Rcont 2 years ago

Correct ans is C Local route for iBGP Internal route for eBGP

upvoted 2 times

Loi2525 2 years ago

C is the correct answer here, NOT A. here is the reference document: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-unicast-routing.html summary of timtgh is correct.

upvoted 2 times

siang 2 years, 2 months ago

C is correct.

upvoted 1 times

hamed4maf 2 years, 8 months ago

I think C is correct Internal Routes Distance Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another. Local Routes Distance Specify the BGP route administrative distance for routes within the local AS. External Routes Distance Specify the BGP route administrative distance for routes learned from other sites in the overlay network.

upvoted 1 times

Clouddon 2 years, 10 months ago

Correct ans is C Local route

upvoted 3 times

timtgh 2 years, 11 months ago

Cisco's parameter names are really stupid, but we have to accept them: External = received from the overlay tunnel Internal = not from overlay tunnel, eBGP Local = not from overlay tunnel, iBGP

upvoted 4 times

eoin1907g 3 years ago

local routes distance is to change the AD of routes within the local AS

upvoted 2 times

Nandhujoe 3 years, 3 months ago

A. Configure Internal Routes Distance to 20.

upvoted 1 times

Nandhujoe 3 years, 3 months ago

Answer is A. Configure Internal Routes Distance to 20 is correct

upvoted 1 times

JP4CCNP 3 years, 4 months ago

Answer A ist correct: internal Route-Distance = internal BGP Routes (Routes learned from a other internal BGP Neighbor - the same AS external Route-Distance: external BGP Routes (Routes learned from a other external BGP Neighbor - differnet AS Locla-Route Distance: Routes local on this Router redistributed into BGP (somthing like BGP Weight)

upvoted 4 times

kk_learn 3 years, 6 months ago

C. Local Routes Distance Specify the BGP route administrative distance for routes within the local AS. By default, a route received locally from BGP is preferred over a route received from OMP.

upvoted 2 times

Alchobashko 3 years, 6 months ago

C is correct. Take a look at document and definition of those.

upvoted 3 times

Zdrobici 3 years, 7 months ago

I would go for A. Local routes means routes added via the network command under bgp process.

upvoted 1 times

Erik_N 3 years, 8 months ago

I would go for A, as they are internal BGP routes, received from another peer in same AS. Local I think are routes injected into BGP. The descriptions in the documentation is confusing and not clear.

upvoted 1 times

Question #87 *Topic 1*

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 v2 or v3 toward the source or PIM-RP as specified in the original PIM join message.

B. 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.

C. 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.

D. 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 v2 or v3 toward the source or PIM-RP as specified in the original PIM join message.

Suggested Answer: *A*

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

Community vote distribution

B (100%)

JTPRO Highly Voted 4 years, 6 months ago

Correct answer is A The question specifies "Cisco SD-Wan devices" which support IGMP V2 and V3. The old Viptela devices only support IGMP V1 and V2. Cisco bought Viptela and kept the name for a short time, but is phasing it out.

upvoted 6 times

John662266 Most Recent 1 year, 8 months ago

Option A is IGMP v2 or V3, only B is Correct...

upvoted 1 times

Clouddon 2 years, 10 months ago

A is the correct answer

upvoted 1 times

Oritopo 4 years, 2 months ago

Correct answer is A IOS XE supports both IGMNPv2 and IGMPv3 Viptela OS "listen" for both IGMPv1 and IGMPv2 group membership reports, but only "supports" IGMPv2 to send join request https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing-book/m-multicast-routing.html

upvoted 4 times

eoogengootoo 4 years, 7 months ago

Cisco SD-WAN overlay multicast routing supports the Internet Group Management Protocol (IGMP) version 2 (defined in RFC 2236). Cisco vEdge devices use IGMP to process receiver membership reports for the hosts in a particular VPN and to determine, for a given group, whether multicast traffic should be forwarded and state should be maintained. vEdge routers listen for both IGMPv1 and IGMPv2 group membership reports.It's A From the link... The Cisco IOS XE SD-WAN multicast overlay software extends Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) over the Cisco SD-WAN overlay using Overlay Management Protocol (OMP). Protocol Independent Multicast Sparse-Mode (PIM-SM) is deployed in the customer VPNs, and the Cisco IOS XE MVPN is used to integrate PIM in customer VPNs and OMP in the overlay. The OMP replicator is used in overlay multicast to optimize the multicast distribution tree across the overlay topology. The Cisco IOS XE SD-WAN router supports IGMPv2 and IGMPv3 reports and advertises receiver's multicast interest to remote Cisco SD-WAN routers using OMP. Depending on the level of optimization required, the Cisco SD-WAN routers join or prune to or from the replicators, and replicators use OMP to relay the join or prune to the Cisco SD-WAN router providing overlay connectivity to the PIM-RP or source.

upvoted 1 times

eoogengootoo 4 years, 7 months ago

Cisco SD-WAN overlay multicast routing supports the Internet Group Management Protocol (IGMP) version 2 (defined in RFC 2236). Cisco vEdge devices use IGMP to process receiver membership reports for the hosts in a particular VPN and to determine, for a given group, whether multicast traffic should be forwarded and state should be maintained. vEdge routers listen for both IGMPv1 and IGMPv2 group membership reports.

upvoted 1 times

Speirsington 4 years, 7 months ago

It's A From the link... The Cisco IOS XE SD-WAN multicast overlay software extends Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) over the Cisco SD-WAN overlay using Overlay Management Protocol (OMP). Protocol Independent Multicast Sparse-Mode (PIM-SM) is deployed in the customer VPNs, and the Cisco IOS XE MVPN is used to integrate PIM in customer VPNs and OMP in the overlay. The OMP replicator is used in overlay multicast to optimize the multicast distribution tree across the overlay topology. The Cisco IOS XE SD-WAN router supports IGMPv2 and IGMPv3 reports and advertises receiver's multicast interest to remote Cisco SD-WAN routers using OMP. Depending on the level of optimization required, the Cisco SD-WAN routers join or prune to or from the replicators, and replicators use OMP to relay the join or prune to the Cisco SD-WAN router providing overlay connectivity to the PIM-RP or source.

upvoted 1 times

eoogengootoo 4 years, 7 months ago

Should be B, as Viptela support only IGMP v1 and v2No it supports IGMP v2 and v3..so answer is A https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-multicast-routing.html

upvoted 1 times

eoogengootoo 4 years, 7 months ago

Should be B, as Viptela support only IGMP v1 and v2

upvoted 1 times

MajorSalieri 4 years, 7 months ago

No it supports IGMP v2 and v3..so answer is A https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-multicast-routing.html

upvoted 3 times

Question #88 *Topic 1*

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:

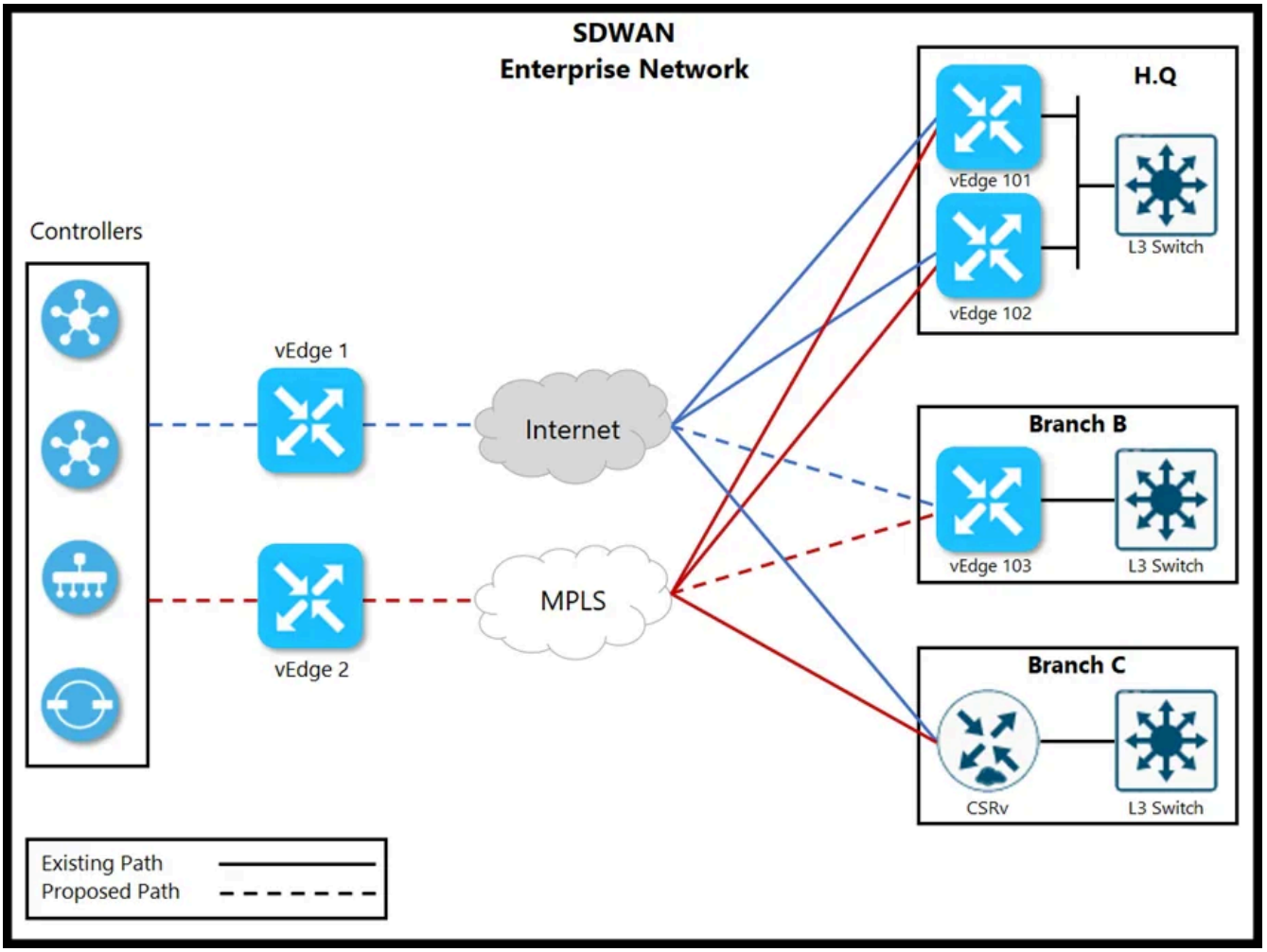
Which configuration meets the requirements?

A.

B.

C.

D.




```
viptela-system:system
 device-model      vedge-cloud
 host-nam                vEdge-Cloud
 location          CA
 system-ip               10.4.4.4
 domain-id               1
 site-id           1
 organization-name ABC
 clock timezone US/Newyork
 vbond 10.10.0.1 port 12346

omp
 no shutdown
 graceful-restart

vpn 512
interface eth0
 ip address 10.0.0.1/24
 no shutdown
```

```
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
```

```
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

vpn 1
interface ge0/1
  description “*** MPLS ***”
  ip address 10.10.0.101/30
  tunnel-interface
    encapsulation ipsec
    color mpls
    allow-service all
```

```
vpn 0
interface ge0/0
  description “*** Internet Circuit ***”
  ip address 209.165.200.225/30
  tunnel-interface
    encapsulation ipsec
    color public-internet restrict
    group 500
    allow-service all

interface ge0/1
  description “*** MPLS ***”
  ip address 10.10.0.101/30
  tunnel-interface
    encapsulation ipsec
    color mpls restrict
    group 50
    allow-service all
```

```
vpn 0
interface ge0/0
  description “*** Internet Circuit ***”
  ip address 209.165.200.225/30
  tunnel-interface
    encapsulation ipsec
    color public-internet restrict
    allow-service all

interface ge0/1
  description “*** MPLS ***”
  ip address 10.10.0.101/30
  tunnel-interface
    encapsulation ipsec
    color mpls restrict
    allow-service all
```

Suggested Answer:
Official Answer: D

tester2478 Highly Voted 3 years, 10 months ago
When a TLOC is marked as restricted, a WAN edge route router will attempt to establish an overlay tunnel to a remote TLOC only via its transport interfaces marked with the same color How can you say D is correct if question states The network team must configure branch B WAN Edge device 103 to establish dynamic full-mesh IPsec tunnels between all colors with branches
upvoted 24 times

5c1f681 Highly Voted 2 years, 2 months ago
Correct answer is A
upvoted 13 times

BECAUSE 2 years, 5 months ago
why not B? There is no front door VRF assigned to MPLS on the answer A?
upvoted 1 times

BECAUSE 2 years, 5 months ago
why not B? There is no front door VRF assigned to MPLS on the answer A?It has the second transport interface in a service VPN. VPN 1ahh yes, i missed that thank you!because both interfaces should be under vpn0
upvoted 1 times

PureInertiaCopy 2 years, 5 months ago
It has the second transport interface in a service VPN. VPN 1ahh yes, i missed that thank you!
upvoted 1 times

PureInertiaCopy 2 years, 5 months ago
It has the second transport interface in a service VPN. VPN 1
upvoted 1 times

BECAUSE 2 years, 5 months ago
ahh yes, i missed that thank you!
upvoted 1 times

Rosh8787 Most Recent 1 year, 10 months ago
because both interfaces should be under vpn0
upvoted 1 times

Networkchamp87 2 years, 6 months ago
correct answer is A
upvoted 5 times

Clouddon 2 years, 10 months ago
A is technically correct
upvoted 2 times

AJMD 2 years, 12 months ago
Correct A
upvoted 3 times

jcms700 3 years, 1 month ago
A is Correct because it does not have the word "restric" along tloc color name. Restric prevent to form IPsec Tunnels with different TLOC Colors
upvoted 2 times

johndoe22 3 years, 3 months ago
A coz between all colours, D if intra colors only.
upvoted 1 times

hamidreza0010 3 years, 3 months ago
Correct answer is A
upvoted 1 times

S__i__D 3 years, 11 months ago
There are no connections between the Internet and MPLS shown -> "restrict" will not affect the final data plane topology, but it will reduce the attempts to build tunnels between different colors. So I think D is correct.
upvoted 2 times

shoman 3 years, 11 months ago
correct Answer should be A

upvoted 3 times

phi5 3 years, 11 months ago

correct Answer should be A

upvoted 3 times

phi5 3 years, 11 months ago

Are sure its D, the question says, dynamic between all colours

upvoted 2 times

Question #89 *Topic 1*

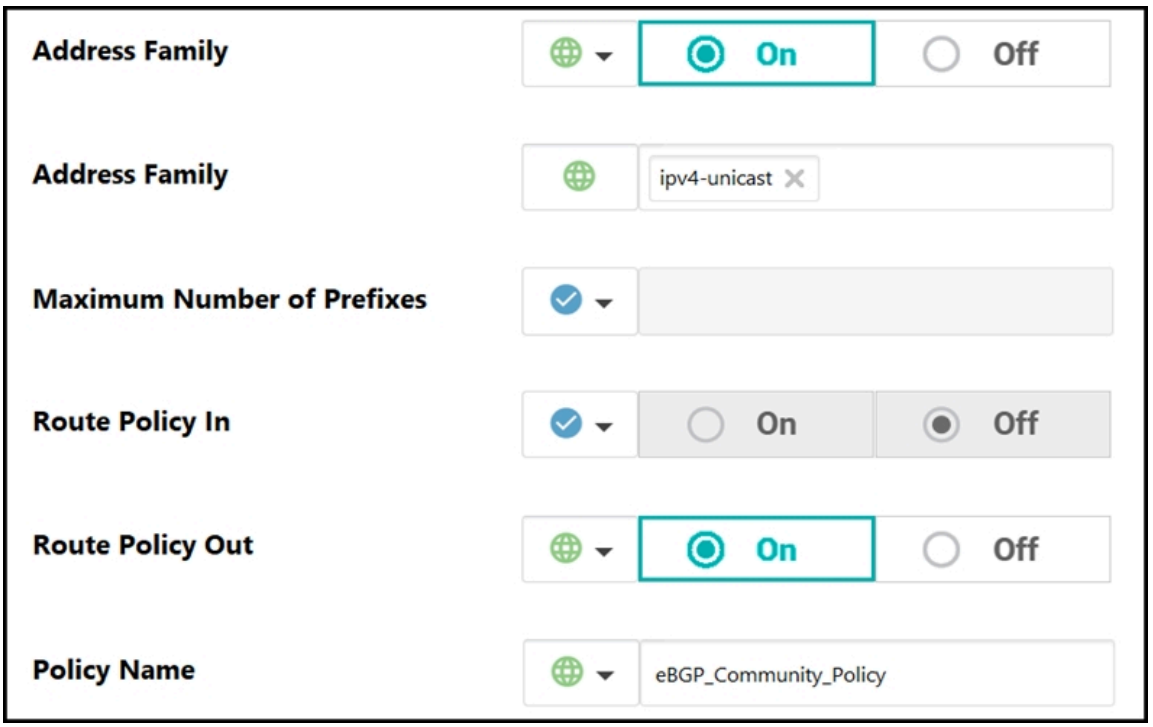
Refer to the exhibit. The engineering must assign community tags to 3 of its 74 critical server networks as soon as they are advertised to BGP peers. These server networks must not be advertised outside AS. Which configuration fulfills this requirement?

A.

B.

C.

D.




```
policy
 route-policy eBGP_Community_Policy
   sequence 1
    match
     address Community_Prefix
    action accept
     set
      community 999:65000 no-advertise
 default-action accept
lists
 prefix-list Community_Prefix
  ip-prefix 20.20.20.0/24
  ip-prefix 21.21.21.0/24
  ip-prefix 22.22.22.0/24
```

```
policy
 route-policy eBGP_Community_Policy
   sequence 1
    match
     address Community_Prefix
    action accept
     set
      community 999:65000 local-as
 default-action reject
lists
 prefix-list Community_Prefix
  ip-prefix 20.20.20.0/24
  ip-prefix 21.21.21.0/24
  ip-prefix 22.22.22.0/24
```

```
policy
 route-policy eBGP_Community_Policy
   sequence 1
    match
     address Community_Prefix
    action accept
     set
      community 999:65000 no-export
 default-action accept
lists
 prefix-list Community_Prefix
  ip-prefix 20.20.20.0/24
  ip-prefix 21.21.21.0/24
  ip-prefix 22.22.22.0/24

policy
 route-policy eBGP_Community_Policy
   sequence 1
    match
     address Community_Prefix
    action accept
     set
      community 999:65000 no-advertise
 default-action reject
lists
 prefix-list Community_Prefix
  ip-prefix 20.20.20.0/24
  ip-prefix 21.21.21.0/24
  ip-prefix 22.22.22.0/24
```

Suggested Answer:
Official Answer: B

ChrisCCNA Highly Voted 3 years, 11 months ago

I think this is C. Local-AS and no-export will both accomplish limiting the advertisements to the local as but the default action reject will stop all advertisements for the other 71 servers. • local-as : Routes in this community are not advertised outside the local AS. • no-advertise : Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • no-export : Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple community options, specifying one community in each option.

upvoted 26 times

MikeG2055 Most Recent 8 months, 1 week ago

B is wrong because it would not allow the other 71 to go through because of the default action reject. C is correct. Seriously why are all the answers that examtopics select wrong? You have to go into the discussion on every single question to get the correct input.

upvoted 2 times

mikidvd51 1 year, 10 months ago

The examtopics selected right answer as B is misleading. According to answers of testers. Why examtopic is misleading payed users ?

upvoted 1 times

BGP65000 3 years, 2 months ago

for me it's C, no-export filter advertise to external peers. no-advertise filter advertise internal and external peers.

upvoted 3 times

SACHK 3 years, 7 months ago

C is correct

upvoted 3 times

tester2478 3 years, 9 months ago

B is definitely wrong.... The local AS community is a well known BGP community and can be used for BGP confederations. It's basically the same as the no export community but this one works for within the sub-AS of a confederation. Prefixes that are tagged are only advertised to other neighbors in the same sub-AS, not to other sub-AS'es or eBGP routers

upvoted 2 times

Question #90 *Topic 1*

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

Suggested Answer: *C*

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/R6BGArNQ/TECSEC-2355.pdf

Community vote distribution

C (100%)

Roger95 Most Recent 1 year, 9 months ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#r_port_offset_3051.xml

upvoted 2 times

Question #91 *Topic 1*

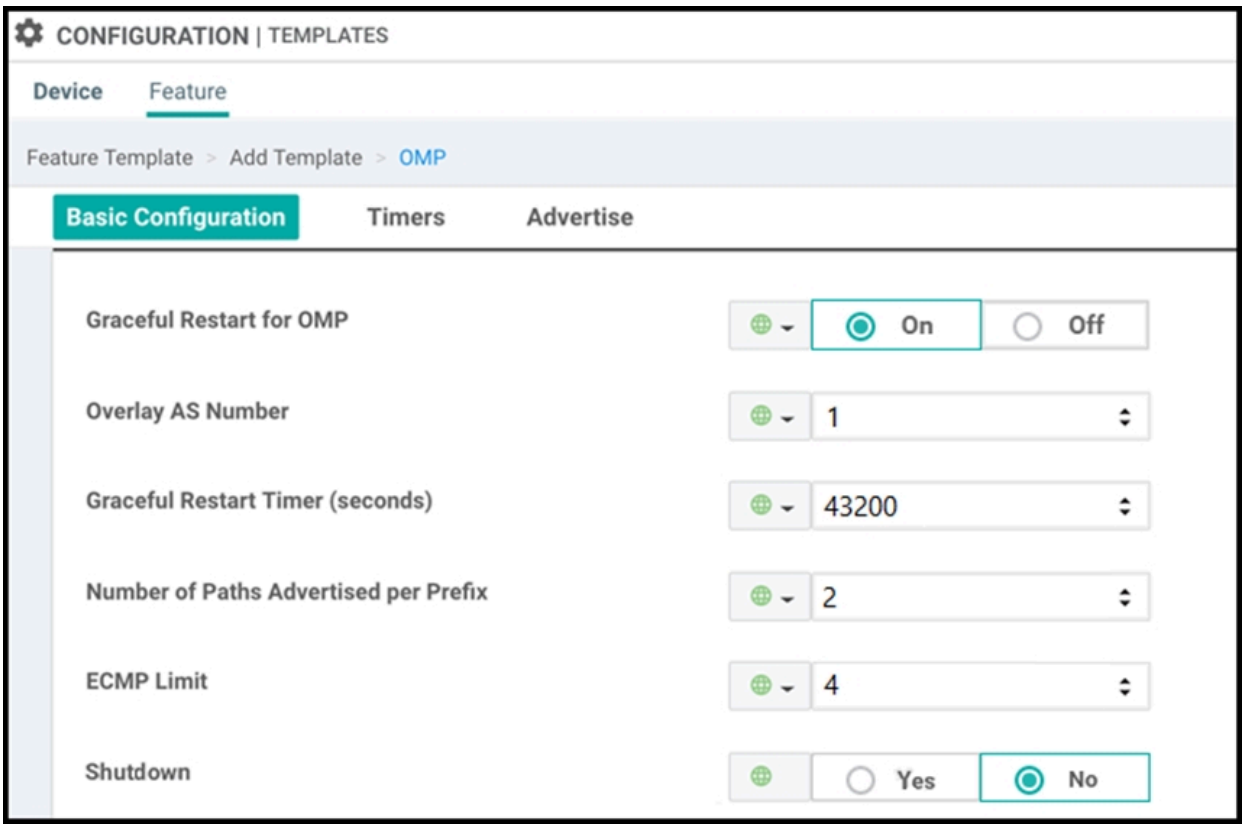
A company must avoid downtime at the remote sites and data plane to continue forwarding traffic between WAN Edge devices if the branch router loses connectivity to its OMP peers. Which configuration meets the requirement?

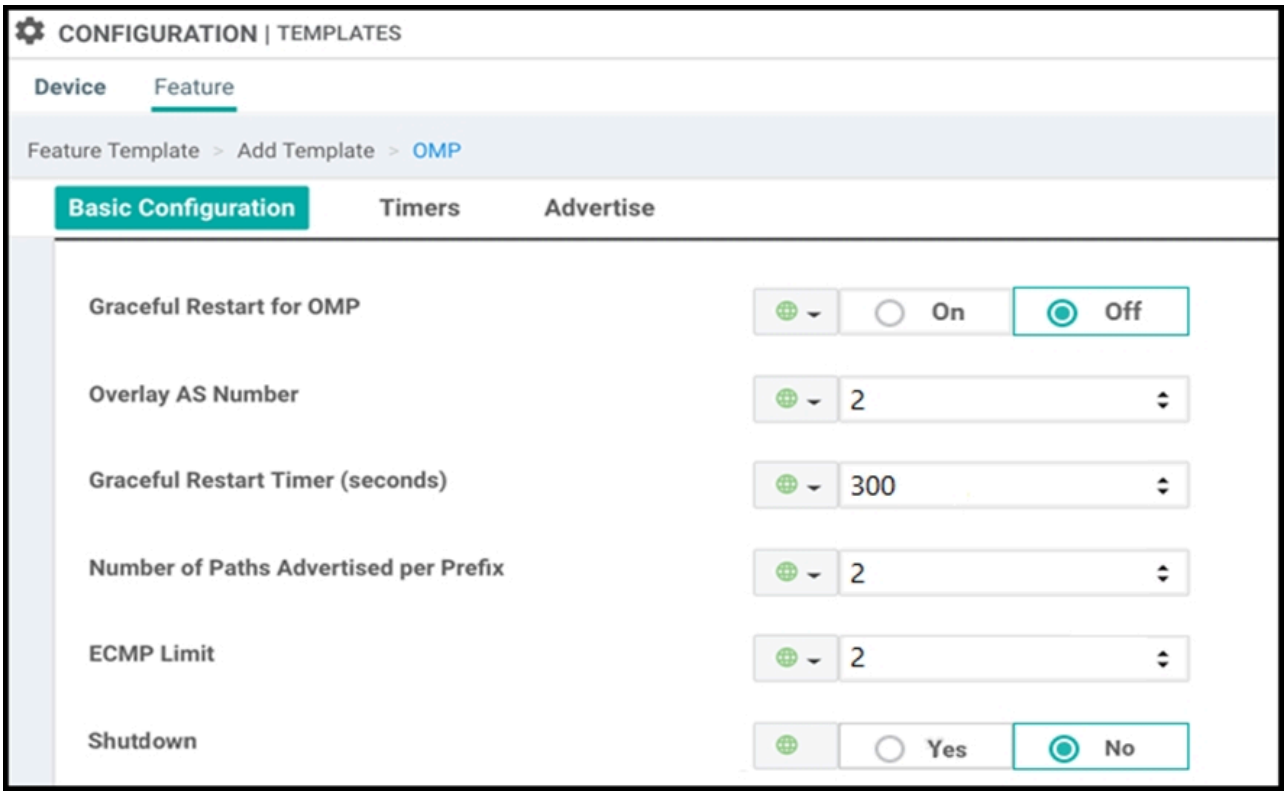
A.

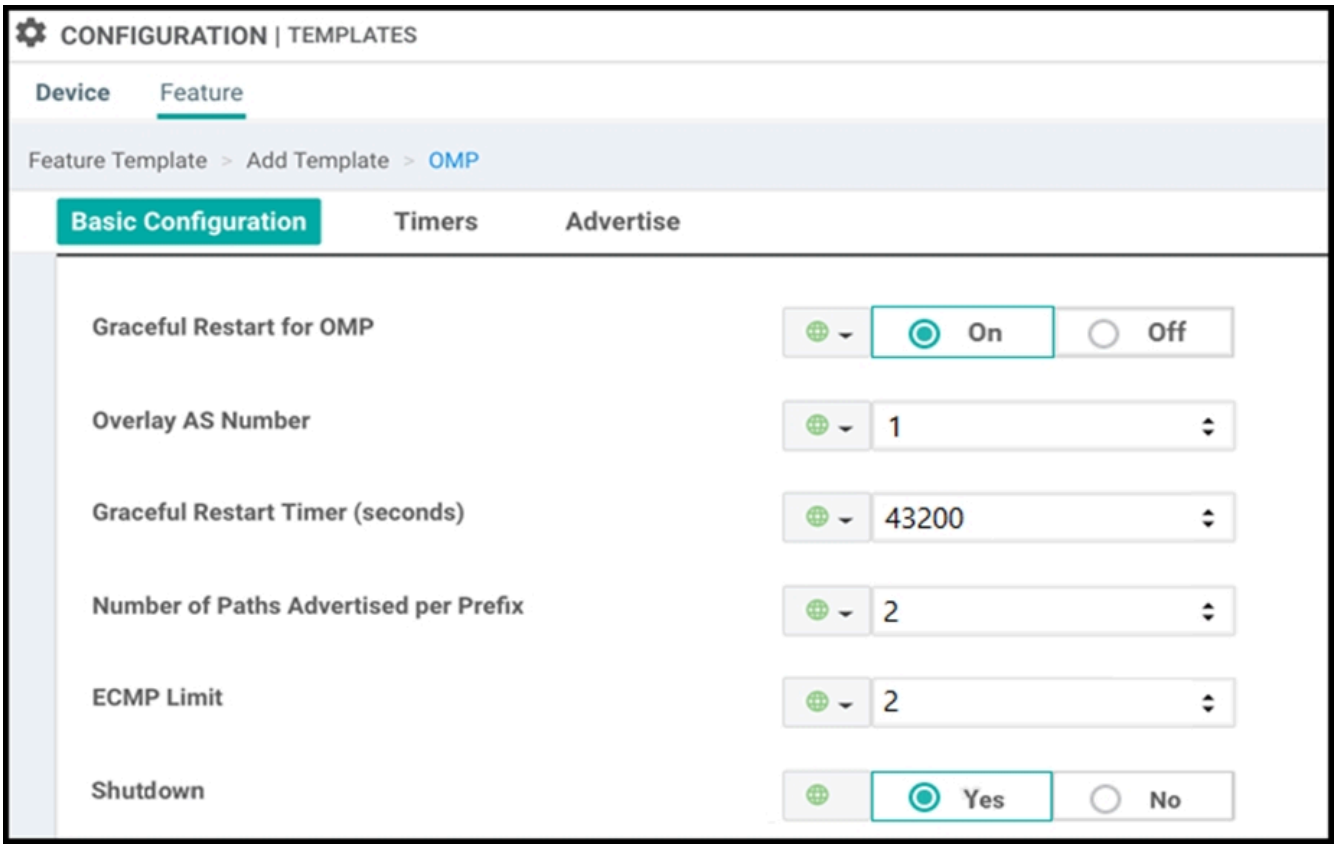
B.

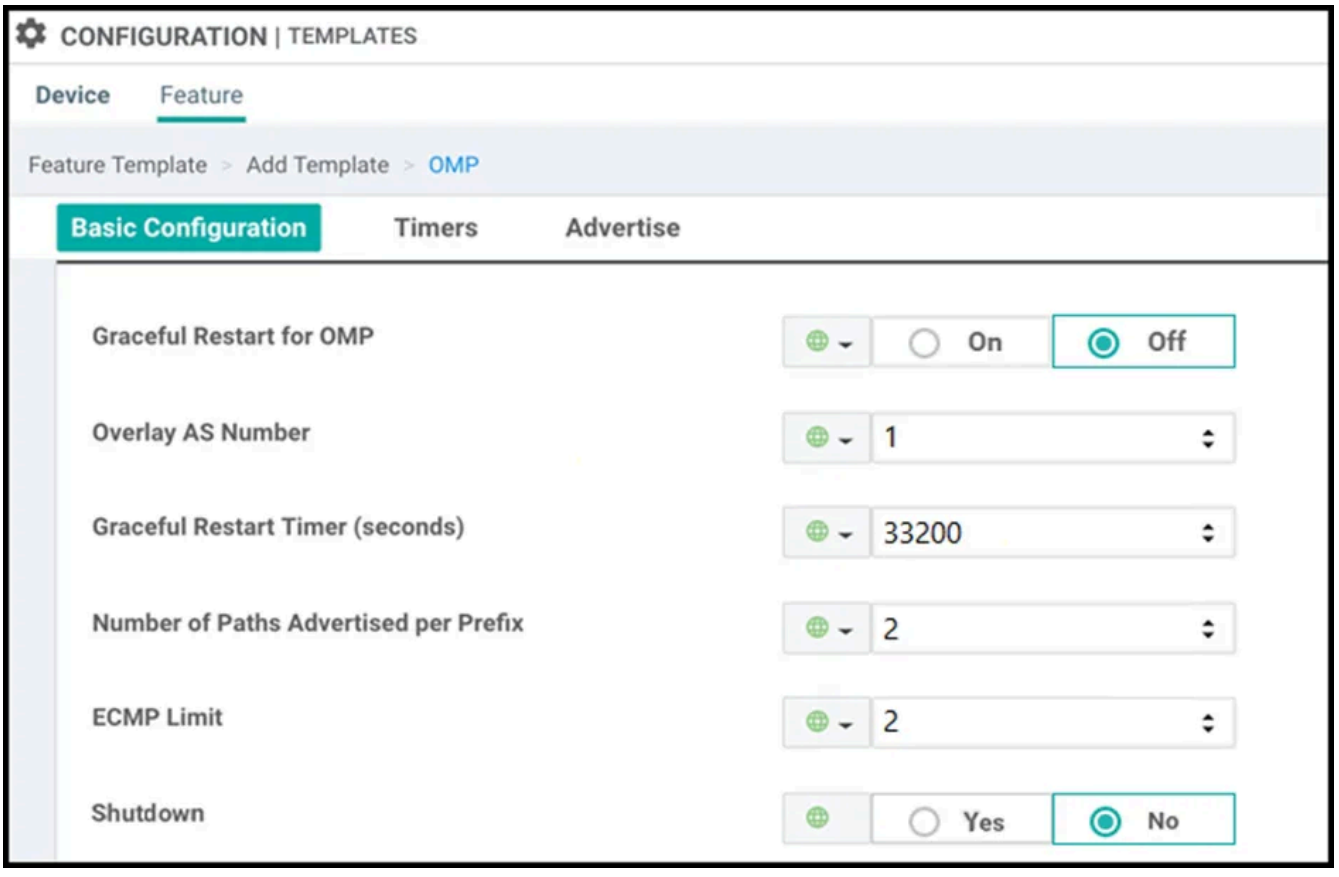
C.

D.









Suggested Answer:
Official Answer: A

ChrisCCNA Most Recent 1 year, 11 months ago

A is correct Graceful restart for OMP allows the data plane in the Viptela overlay network to continue functioning if the control plane stops functioning or becomes unavailable. With graceful restart, if the vSmart controller in the network goes down, or if multiple vSmart controllers go down simultaneously, the vEdge routers can continue forwarding data traffic. They do this using the last known good information that they received

from the vSmart controller. When a vSmart controller is again available, its DTLS connection to the vEdge router is re-established, and the vEdge router then receives updated, current network information from the vSmart controller.

upvoted 2 times

Question #92 *Topic 1*

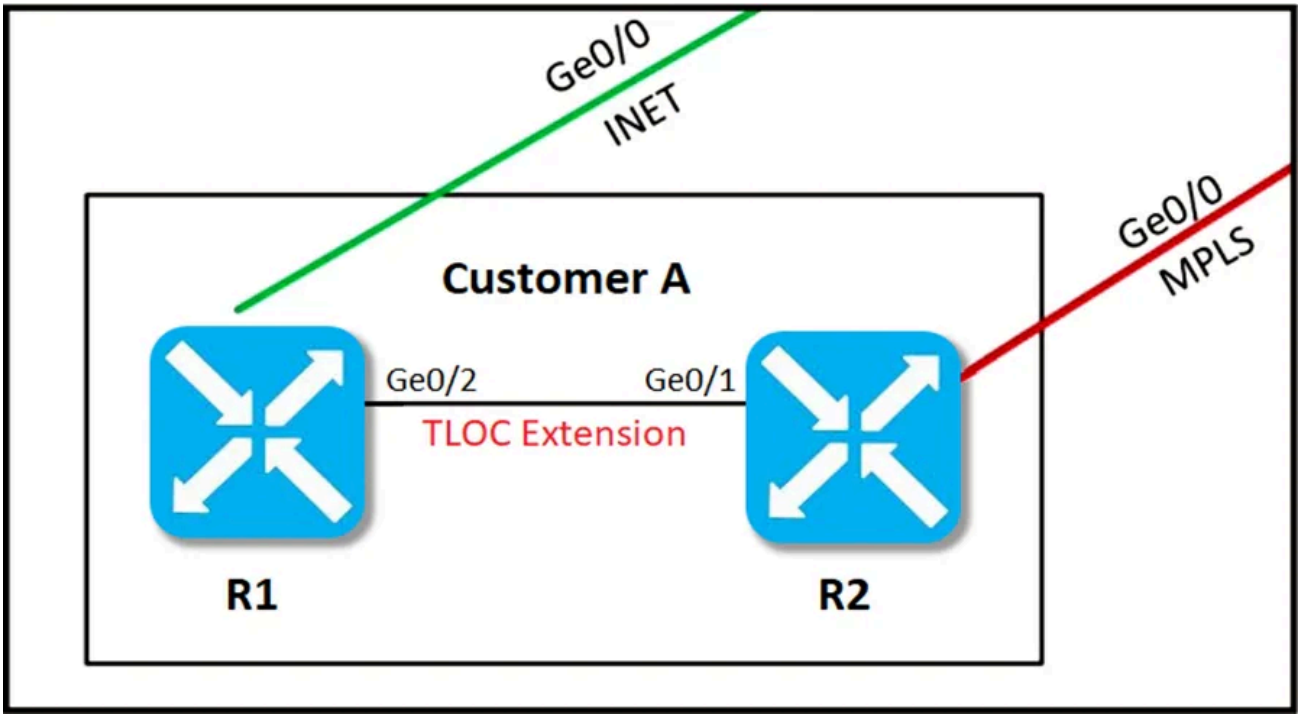
Refer to the exhibit. An MPLS connection on R2 must extend to R1. Users behind R1 must have dual connectivity for data traffic. Which configuration provides R1 control connectivity over the MPLS connection?

A.

B.

C.

D.



R1
```
interface ge0/2
 ip address 34.34.34.1/30
 tloc-extension ge0/1
```

R2
```
interface ge0/0
 ip address 34.34.34.2/30
 tunnel-interface
  color mpls
```

R1
```
interface ge0/2
 ip address 34.34.34.1/30
 tloc-extension ge0/1
 tunnel-interface
  color mpls
```

R2
```
interface ge0/2
 ip address 34.34.34.2/30
 tloc-extension ge0/0
 tunnel-interface
  color public-internet
```

R1
```
interface ge0/2
 ip address 34.34.34.1/30
 tunnel-interface
  color mpls
  control connection
```

R2
```
interface ge 0/2
  ip address 34.34.34.3/30
  tloc-extension ge0/0
```

R1
```
interface ge0/2
 ip address 34.34.34.1/30
 tunnel-interface
  color mpls
```

R2
```
interface ge0/2
  ip address 34.34.34.2/30
  tloc-extension ge0/0
```

Suggested Answer:
Official Answer: D

ChrisCCNA Highly Voted 2 years, 11 months ago

D is correct but there is a typo. Should be: R2 Interface G0/1

upvoted 9 times

Aldebeer Most Recent 1 year, 8 months ago

Option D is the correct config.

upvoted 1 times

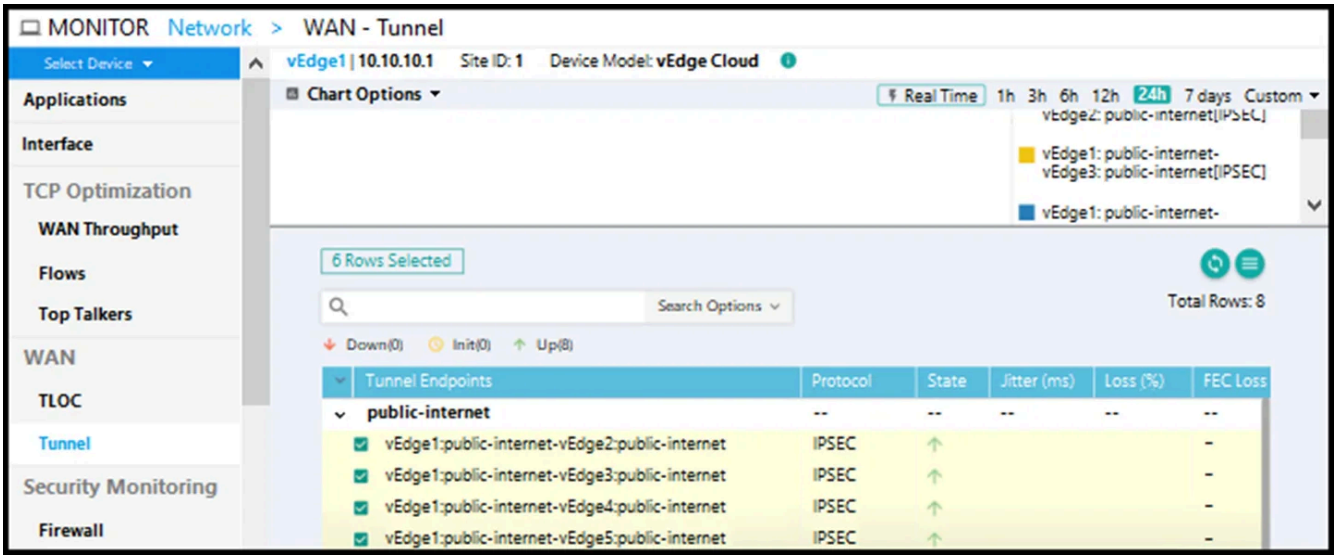
Refer to the exhibit. Which command-line configuration on a WAN Edge device achieves these results?

A.

B.

C.

D.




```
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
```

```
vpn 0
interface ge0/0
 ip address 10.50.0.101/30
 tunnel-interface
  encapsulation gre
  color public-internet
  allow-service ntp

ip route 0.0.0.0/0 10.50.0.102
```

```
vpn 0
interface ge0/0
 ip address 10.50.0.101/30
 tunnel-interface
  encapsulation ipsec
  color public-internet restrict
  allow-service all
  allow-service netconf

ip route 0.0.0.0/0 10.50.0.102
```

```
vpn 1
interface ge0/0
 ip address 10.50.0.101/30
 tunnel-interface
  encapsulation ipsec
  color public-internet restrict
  allow-service all
  allow-service netconf

ip route 0.0.0.0/0 10.50.0.102
```

Suggested Answer:
Official Answer: C

Myare Most Recent 1 year, 4 months ago

The trick of the question is to configure "restrict" under VPN0. the correct answer is C.

upvoted 1 times

ChrisCCNA 1 year, 11 months ago

C is correct. Configure VPN 0 tunnel interface. Encapsulate with IPSEC

upvoted 4 times

Question #94 *Topic 1*

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

A. 0

B. 512

C. 10

D. 1

Suggested Answer: *A*

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

Community vote distribution

A (100%)

dcastroHN Highly Voted 4 years, 1 month ago

Correct A, Transport VPN 0

upvoted 6 times

Vic_Malloy Most Recent 1 year, 6 months ago

Answer is A. VPN0 is Transport side and represents the the Underlay. That termination point for such transport (circuit, underlay) is known as the TLOC.

upvoted 1 times

Vic_Malloy 2 years ago

NAT is done on the Service Side which is VPN 0. Correct answer A

upvoted 1 times

Question #95 *Topic 1*

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

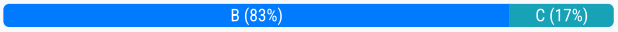
C. WAN Edge

D. Firewall

Suggested Answer: *B*

Official Answer: B

Community vote distribution



Faridtnx Most Recent 6 months ago

vSmart controller acts as the brains of the network (the control plane). It is responsible for implementing and enforcing centralized control policies, which include Service Chaining.

upvoted 2 times

d656971 1 year, 3 months ago

Keyword: ENFORCEMENTvEdge is the data plane devices. While they are the ones that actually forward the traffic, they only do so based on the instructions (policies) received from the vSmart.

upvoted 1 times

d656971 1 year, 3 months ago

Selected Answer: C

Keyword: ENFORCEMENT

upvoted 1 times

Faridtnx 6 months ago

vEdge is the data plane devices. While they are the ones that actually forward the traffic, they only do so based on the instructions (policies) received from the vSmart.

upvoted 1 times

vishalmayyahoo 2 years, 1 month ago

I think B. vSmart is correct. Service chaining is supported in both Control and Data Policies. Control policies can redirect traffic to a service by changing the next hop to the location of the service (e.g., a firewall or IDS/IPS). Data: The match criteria for data policies can include source and destination IP addresses, source and destination ports, DSCP values, and application information. Data policies can enforce actions such as NAT, QoS, mirroring, and service chaining by redirecting traffic to a service node.

upvoted 1 times

RafaJohnston76 2 years, 6 months ago

B is correct, Service-chaining is a Control-policy, and control policies are enforced on the V-Smart Centralized Control (Topology) policy is the most powerful form of policies which can be used to implement arbitrary overlay VPN topologies such as hub-and-spoke and partially-mesh, traffic engineering like preferring one site over another for a specific destination, service chaining by inserting a network service such as a firewall into the path of specific data traffic in an automated manner, and much more. Centralize control policies are defined on the vManage, configured and enforced on the vSmart Controllers affecting the control plane of the Cisco SD-WAN overlay fabric, whereas centralized data policies are defined on the vManage, configured on the vSmart Controllers, distributed by OMP to and enforced on the WAN Edge routers affecting the data plane of the overlay network.

upvoted 2 times

MerlinTheWizard 3 years, 2 months ago

CorrectThe component that is responsible for enforcing a policy to redirect branch-to-branch traffic toward a network service such as a firewall or IPS in Cisco SD-WAN is the WAN Edge.The WAN Edge is the component that is responsible for terminating the tunnels, providing secure connectivity between branch locations and the data center, and enforcing business policies. It is a multi-function device that includes routing, security, and application optimization capabilities. When it comes to redirecting branch-to-branch traffic toward a network service such as a firewall or IPS, the WAN Edge is responsible for enforcing the policy. It does this by using the service chaining feature, which allows traffic to be redirected to a service

device before being forwarded to its final destination. The WAN Edge intercepts the traffic, sends it to the specified network service, and then forwards it to its destination.

upvoted 1 times

MerlinTheWizard 3 years, 2 months ago

Selected Answer: B

Correct

upvoted 1 times

elninio13 2 years, 9 months ago

The component that is responsible for enforcing a policy to redirect branch-to-branch traffic toward a network service such as a firewall or IPS in Cisco SD-WAN is the WAN Edge.

upvoted 2 times

elninio13 2 years, 9 months ago

The WAN Edge is the component that is responsible for terminating the tunnels, providing secure connectivity between branch locations and the data center, and enforcing business policies. It is a multi-function device that includes routing, security, and application optimization capabilities. When it comes to redirecting branch-to-branch traffic toward a network service such as a firewall or IPS, the WAN Edge is responsible for enforcing the policy. It does this by using the service chaining feature, which allows traffic to be redirected to a service device before being forwarded to its final destination. The WAN Edge intercepts the traffic, sends it to the specified network service, and then forwards it to its destination.

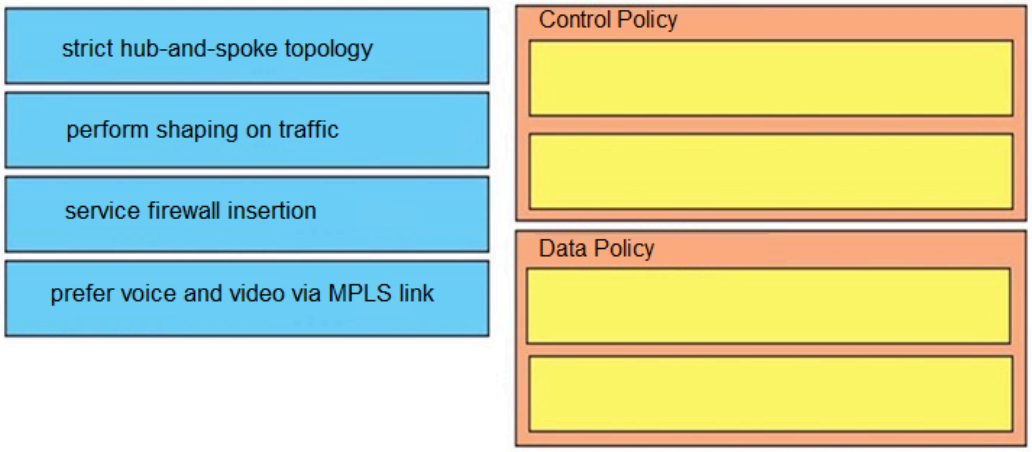
upvoted 1 times

Question #96 *Topic 1*

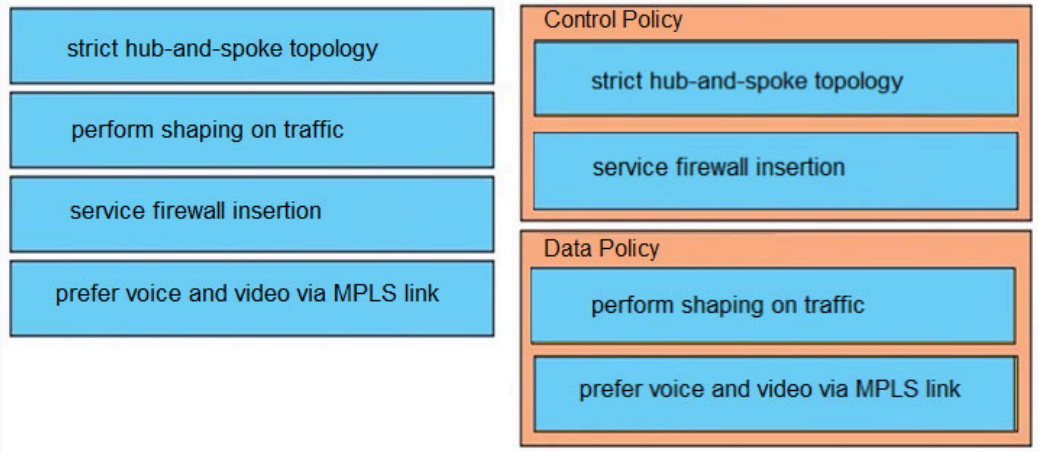
DRAG DROP -

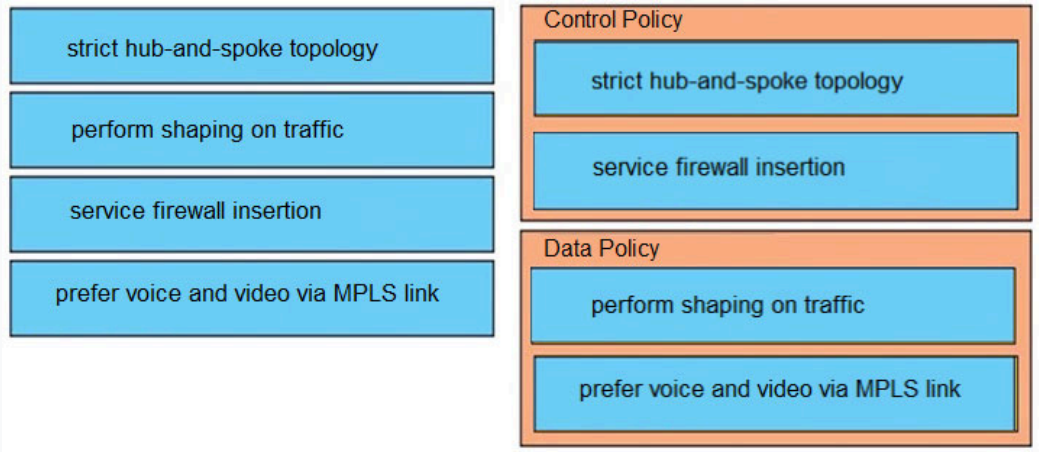
Drag and drop the policies from the left onto the policy types on the right.

Select and Place:



Suggested Answer:





Outlaw_87 Most Recent 2 years ago

service insertion or service chaining is the centralized control policy. reference: CBT Nuggets video course (instructor Knox Hutchinson).

upvoted 3 times

she_ccie 3 years, 11 months ago

how do you know if a service insertion is a data policy or a control policy? Documentation has it as both a data and control policy.

upvoted 3 times

she_ccie 3 years, 11 months ago

how do you know if a service insertion is a data policy or a control policy? Documentation has it as both a data and control policy.I didn't really look at the documentation, but from the ENSDWI course, it is a control policy. However, in this case, it's easy to sort the other answers leaving only a single option anywayI believe that when a policy influences the entire network topology, it could be categorized as a control policy. On the other hand, if a policy only has an impact on a single WAN device, it could be referred to as a data policy.

upvoted 3 times

MerlinTheWizard 2 years, 9 months ago

I didn't really look at the documentation, but from the ENSDWI course, it is a control policy. However, in this case, it's easy to sort the other answers leaving only a single option anyway

upvoted 1 times

TMT91 2 years, 5 months ago

I believe that when a policy influences the entire network topology, it could be categorized as a control policy. On the other hand, if a policy only has an impact on a single WAN device, it could be referred to as a data policy.

upvoted 3 times

Question #97 *Topic 1*

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

Suggested Answer: *D*

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

Community vote distribution

D (100%)

ramjam Highly Voted 4 years, 2 months ago

correct. Page 113 of the link

upvoted 5 times

bullett00th Most Recent 1 year, 9 months ago

D is correct To view the policy that has been pushed to the Cisco vEdge device, use the show policy from-vsmart command on the Cisco vEdge device. vEdge# show policy from-vsmart

upvoted 2 times

Question #98 *Topic 1*

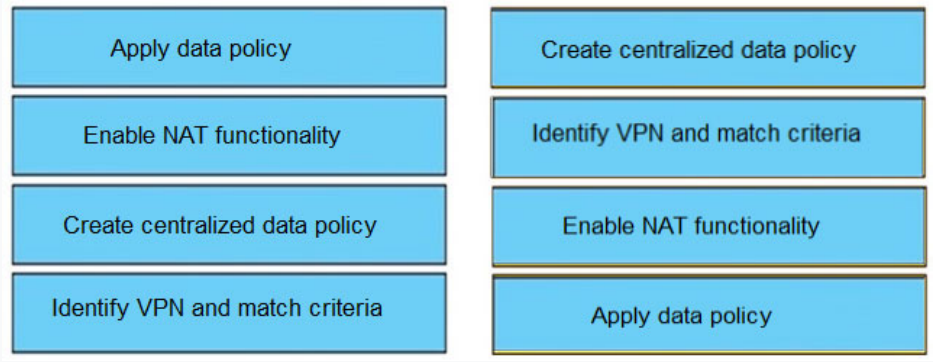
DRAG DROP -

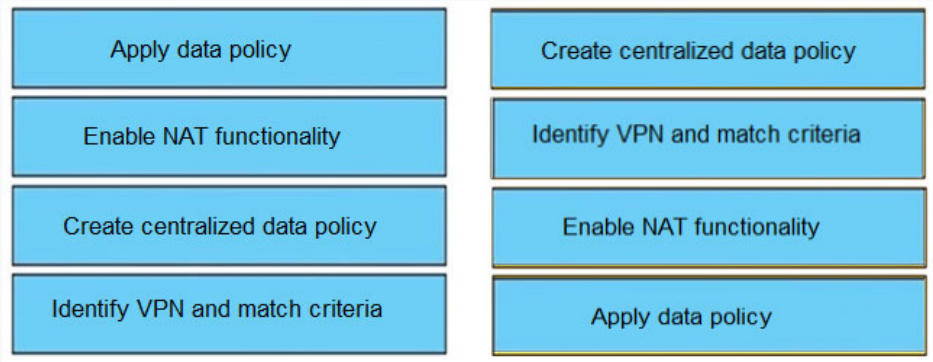
Drag and drop the actions from the left into the correct sequence on the right to create a data policy to direct traffic to the Internet exit.

Select and Place:



Suggested Answer:





Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/vEdge-as-NAT-device.html

Almanac Highly Voted 4 years, 10 months ago

i think B -C-D-A first you need to enable NAT first on the interface. then create central policy

upvoted 20 times

platin Highly Voted 5 years, 1 month ago

I think this answer is not correct. My opinion: B -> D-> C -> A

upvoted 10 times

platin 5 years, 1 month ago

I think this answer is not correct. My opinion: B -> D-> C -> AHow can you put D before C? You have to create the policy before you can add match rules to the policy.

upvoted 10 times

timtgh 2 years, 5 months ago

How can you put D before C? You have to create the policy before you can add match rules to the policy.

upvoted 1 times

Outlaw_87 Most Recent 2 years, 1 month ago

In the CBT Nuggets video course, the instructor (Knox Hutchinson) showed how it is (DIA) done. Steps: 1. Enable NAT 2. Create policy 3. Identify 4. Apply policy So, B > C > D > A

upvoted 2 times

timtgh 2 years, 5 months ago

Selecting NAT as the action in the policy is not the same thing as enabling NAT functionality. Enabling NAT functionality means configuring NAT on the WAN interface in VPN 0, and this is always the first step.

upvoted 2 times

JP4CCNP 2 years, 10 months ago

the given answer is correct. The Questions goes only for generating a Traffic-Data Policy with Direct Internet Access (DIA) and not regarding the native Interface Configuration on the Router. So the Steps in the actual Row are right from a Policy-Building Perspektive.

upvoted 3 times

Idro 3 years, 3 months ago

Given answer is correct, they are asking about the "Data Policy" steps

upvoted 2 times

ChrisCCNA 3 years, 5 months ago

I'm beginning to believe the given answer is correct. Speirsington explained correctly. First off this is Centralized Data policy configured via CLI. That is important. Create Centralized Data Policy (Match) Identity VPN and Match Criteria (Action) Enable NAT - this is done via "nat use-vpn 0" Apply Please reference page 307 of the Cisco SD-WAN configuration guide 18.4. "Rather than have a single exit point from the overlay network to the Internet, vSmart data-policy can provide local Internet exit from vEdge routers. You implement this using a data-policy that includes a NAT directive. The data-policy is configured on the vSmart controller, so local Internet exit is managed centrally."

upvoted 3 times

immphoenix 3 years, 9 months ago

the answer is correct if we are following the GUI configuration, however, it can be in different order if we are using CLI.

upvoted 1 times

Speirsington 4 years ago

The NAT function is configured on the transport side, on VPN 0 Ge0/1 using the following commands: vpn 0 interface ge0/1 nat The VPNs and site lists are configured, as always, in the lists as groups of interest. lists vpn-list guest-wifi vpn 2 site-list wifi-sites site-id 10-15 The actual policy is applied to the corresponding VPN list, and states that if the destination port is 80 or 443 (match), then (action) use the NAT function in VPN 0. data-policy wifi-dia vpn-list guest-wifi sequence 10 match destination-port 80 443 action accept nat use-vpn 0 ! default-action accept

upvoted 2 times

kentkyye 4 years, 1 month ago

Enable NAT Functionality in the WAN VPN The first step in setting up Internet exit on a Cisco vEdge device is to configure the router to act as a NAT device. You do this by enabling NAT functionality in VPNs that have interfaces that connect to a WAN transport network. By default, VPN 0 always connects to the WAN transport. Other VPNs in your network might also connect to WANs. so answer is : Enable NAT Created centralized policy. ID VPN and match. Apply data policy.

upvoted 2 times

Amitmanesar 4 years, 1 month ago

question talks about data policy construct :: so wrt to that seq is correct , create CENTRAL DATA policy> match (vpn and all)> action (nat) > apply policy ... offcourse nat should be enabled on the transport interface but that is out of scope from data policy construct

upvoted 2 times

nihithp 4 years, 3 months ago

Ans must be B,D,C,A To configure the Cisco vEdge device to act as a NAT device so that some traffic from the router can go directly to a public network, you do three things: Enable NAT in the transport VPN (VPN 0) on the WAN-transport–facing interface, which here is ge0/0. All traffic exiting from the Cisco vEdge device, going either to other overlay network sites or to a public network, passes through this interface. To direct data traffic from other VPNs to exit from the Cisco vEdge device directly to a public network, enable NAT in those VPNs or ensure that those VPNs have a route to VPN 0. On the vCisco vSmart Controller, create a centralized data policy the redirects the desired data traffic from the non-transport VPN to VPN 0, and then apply that data policy to the non-transport VPN. In this case, we apply the policy to VPN 1

upvoted 1 times

Lunap 4 years, 7 months ago

I think Isa1010 is correct. Question is about creating data policy Create centralised policy Create match conditions Action nat VPN 0 Apply policy

upvoted 3 times

isa1010 4 years, 7 months ago

It´s correct, Create centralized policy, then go to traffic-rules>traffic-data, add policy and select your "match" conditions and choose NAT VPN = 0 under ACTIONS column. finally apply said policy to vsmart.

upvoted 4 times

isaacmejia 4 years, 7 months ago

In order to create a centralized data policy you need to identify the vpns involved and match criteria first, i would go with -Identify vpn and match criteria -create the policy -enable nat -apply the policyAnother wrong answer. Just stop.

upvoted 2 times

isaacmejia 4 years, 7 months ago

In order to create a centralized data policy you need to identify the vpns involved and match criteria first, i would go with -Identify vpn and match criteria -create the policy -enable nat -apply the policy

upvoted 2 times

CCNPCollab1297 4 years, 6 months ago

Another wrong answer. Just stop.

upvoted 7 times

ramjam 4 years, 8 months ago

Correct: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/vEdge-as-NAT-device.html

upvoted 3 times

CCNPWILL 4 years, 9 months ago

To configure a Cisco vEdge device to be an Internet exit point, you enable NAT within a VPN on the Cisco vEdge device, and then you configure a centralized data policy on a Cisco vSmart controller. This policy splits the traffic within the VPN so that some of it is directed towards remote sites within the VPN, and hence remains within the overlay network, and other traffic is directed to the Internet or other destinations outside the overlay network. It is also possible to configure a Cisco vEdge device to forward data traffic directly to the Internet, by specifying the destination IP prefix.Enable NAT Created centralized policy. ID VPN and match. Apply data policy.

upvoted 6 times

CCNPWILL 4 years, 9 months ago

To configure a Cisco vEdge device to be an Internet exit point, you enable NAT within a VPN on the Cisco vEdge device, and then you configure a centralized data policy on a Cisco vSmart controller. This policy splits the traffic within the VPN so that some of it is directed towards remote sites within the VPN, and hence remains within the overlay network, and other traffic is directed to the Internet or other destinations outside the overlay network. It is also possible to configure a Cisco vEdge device to forward data traffic directly to the Internet, by specifying the destination IP prefix.

upvoted 6 times

CCNPWILL 4 years, 9 months ago

Enable NAT Created centralized policy. ID VPN and match. Apply data policy.

upvoted 9 times

Question #99 *Topic 1*

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

A. Data policy

B. Centralized policy

C. Localized policy

D. Control policy

Suggested Answer: *A*
Official Answer: A

Community vote distribution
B (100%)

tarq Highly Voted 4 years, 6 months ago
Its asking about the configuration option under Configure > Policies screen. Yes, it is centralized data policy but configuration option is named " Centralized Policy " so B is correct https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/application-aware-routing.html#id_114072 In Cisco vManage NMS, select the Configure > Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
upvoted 18 times

Aldebeer Most Recent 1 year, 8 months ago
centralized policy as from the question
upvoted 1 times

BGP65000 2 years, 2 months ago
application aware is a tab under centralized policy
upvoted 1 times

assili 2 years, 9 months ago
Configuration! Policies Centralized policy > application aware routing Policy
upvoted 1 times

khanda 3 years, 1 month ago
B CONFIGURATION | POLICIES Centralized Policy> Appliciation Aware Routing Policy
upvoted 4 times

majepiga 3 years, 3 months ago
I think is B
upvoted 3 times

khanda 3 years, 4 months ago
Configuration > Policies > Centralized Policy >
upvoted 1 times

JOHN818181 3 years, 5 months ago
Configuration > Policies > Centralized Policy
upvoted 1 times

Speirsington 3 years, 6 months ago
The procedure for AAR policy configuration using Cisco vManage GUI is as follows: In Cisco vManage GUI, navigate to Configuration > Policies > Centralized Policy and select Add Policy.
upvoted 3 times

CesarVergaraGalindo 3 years, 10 months ago
B is correct
upvoted 4 times

Adedayo 4 years, 7 months ago
I read in a documentation that this comes under a centralized data policy. Is option A still valid or should it be B?
upvoted 3 times

Adedayo 4 years, 7 months ago

I read in a documentation that this comes under a centralized data policy. Is option A still valid or should it be B?B is the correct answer buddy.

upvoted 3 times

CCNPWILL Highly Voted 4 years, 3 months ago

B is the correct answer buddy.

upvoted 8 times

Question #100 *Topic 1*

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

A.

B.

C.

D.

```
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
```

```
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
```

```
 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

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
```

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

RafaJohnston76 Most Recent 2 years, 2 months ago

C https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/segmentation/vEdge-20-x/segmentation-book/segmentation.html

upvoted 1 times

Zgana 3 years, 1 month ago

C is correct.

upvoted 1 times

khanda 3 years, 6 months ago

C is correct. vSmart-1# config Entering configuration mode terminal vSmart-1(config)# policy vpn-membership dissallow-vpn-1 vSmart-1(config-vpn-membership-dissallow-vpn-1)# sequence 10 vSmart-1(config-sequence-10)# match vSmart-1(config-match)# ? Possible completions: vpn VPN ID vpn-list Name of VPN list ---

upvoted 3 times

AK654321 3 years, 9 months ago

Guys, C is the right answer because, vpn-id was an older option available in Cisco SD-WAN which now has been removed.
upvoted 1 times

www 3 years, 10 months ago
cant be A because the VPN list that matches VPN 10 and 20 is being rejected. the default action is accept so, it is accepting anything but 10 and 20s the given answer is correct C for me
upvoted 2 times

www 3 years, 10 months ago
cant be A because the VPN list that matches VPN 10 and 20 is being rejected. the default action is accept so, it is accepting anything but 10 and 20
upvoted 2 times

majepiga 3 years, 9 months ago
s the given answer is correct C for me
upvoted 1 times

Khrysis 3 years, 11 months ago
A is the most appropriate answer among the given choices, even if it has the wrong VPNs of 10 & 20 instead of 1 (whether a typo or intentional, I can't tell)
upvoted 1 times

she_ccie 3 years, 12 months ago
C: there are 2 ways to configure the vpn membership. With a policy as shown in C, or by identifying them in the same line as the sites under apply-policy like this "vSmart (config-apply-policy)# site-list 20-30 vpn-membership 1. The doc is not wrong, its just the original way of configuring the policy and identifying the vpn group of interest. Which is VPN1 in this scenario.
https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-17-2.pdf#
upvoted 1 times

Maurel 4 years ago
A is the correct answer
upvoted 1 times

DBla 4 years, 4 months ago
C isn't correct either. match vpn-id 1 is not a correct configuration command. The correct one would be match vpn 1. Unfortunately even the config guide contains this faulty line (https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-17-2.pdf#page=190), but vedge will drop an error if you try it. For the exam, however, C should be marked.
upvoted 2 times

DBla 4 years, 4 months ago
C isn't correct either. match vpn-id 1 is not a correct configuration command. The correct one would be match vpn 1. Unfortunately even the config guide contains this faulty line (https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-17-2.pdf#page=190), but vedge will drop an error if you try it. For the exam, however, C should be marked.Perfect!!
upvoted 2 times

stepstranger 4 years, 2 months ago
Perfect!!
upvoted 1 times

ramjam 4 years, 8 months ago
correct.yes, ok
upvoted 3 times

ramjam 4 years, 8 months ago
correct.
upvoted 3 times

stepstranger 4 years, 2 months ago
yes, ok
upvoted 1 times

Question #101 *Topic 1*

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. centralized control policy

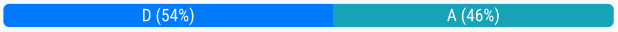
C. localized control policy

D. centralized data policy

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Afshan Most Recent 10 months, 3 weeks ago

Since the policy is Network wide and not to specific Edge, I believe it is Centralized. And since the policy is on the traffic I believe it is a Data Policy.

upvoted 2 times

Kojy 11 months, 2 weeks ago

CORRECT IS D .....LOCALIZED DATA POLICY DON'T ENFORCE SLA

upvoted 1 times

Myare 1 year, 4 months ago

the QoS configuration process is to assign traffic flows coming from the service-side to the appropriate forwarding classes. We can do this with either a centralized data policy on a per-VPN basis or with a localized data policy on a per-interface basis. Classification and Marking can be done at different network layers: Layer 2: 802.1q, MPLS EXP Layer 3: IP precedence, DSCP, IP ECN, Source/Destination IP Layer 4: TCP/UDP ports Layer 7: DPI/NBAR

upvoted 2 times

John662266 1 year, 8 months ago

it should be use centralized data policy configure forward policy. local data policy is for QoS ..

upvoted 2 times

mikidvd51 1 year, 9 months ago

granular QOS for app or prefixes is configured on - localized data policy

upvoted 4 times

thomazmr 2 years, 6 months ago

D is correct

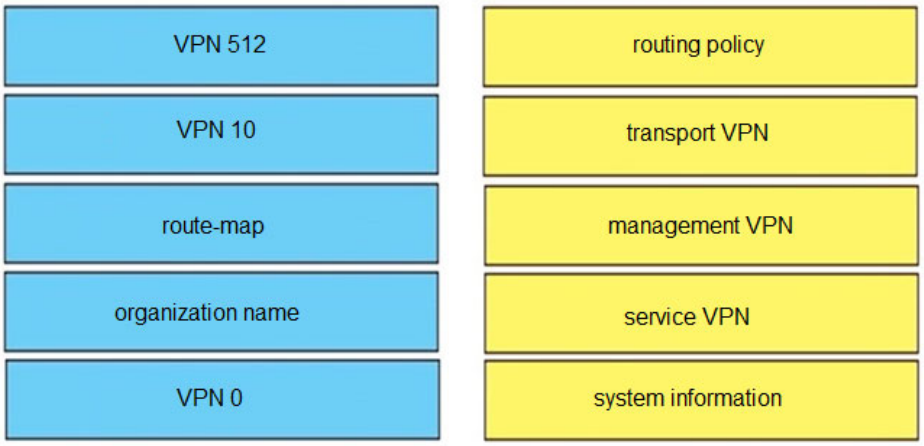
upvoted 2 times

Question #102 *Topic 1*

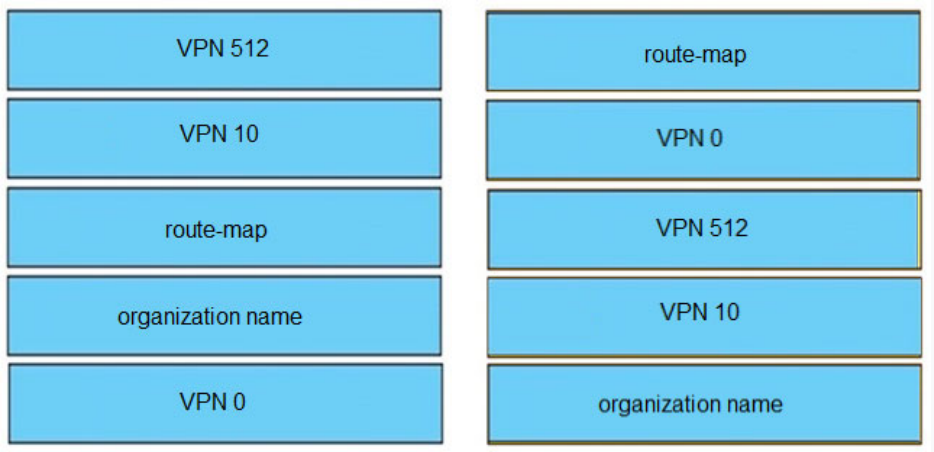
DRAG DROP -

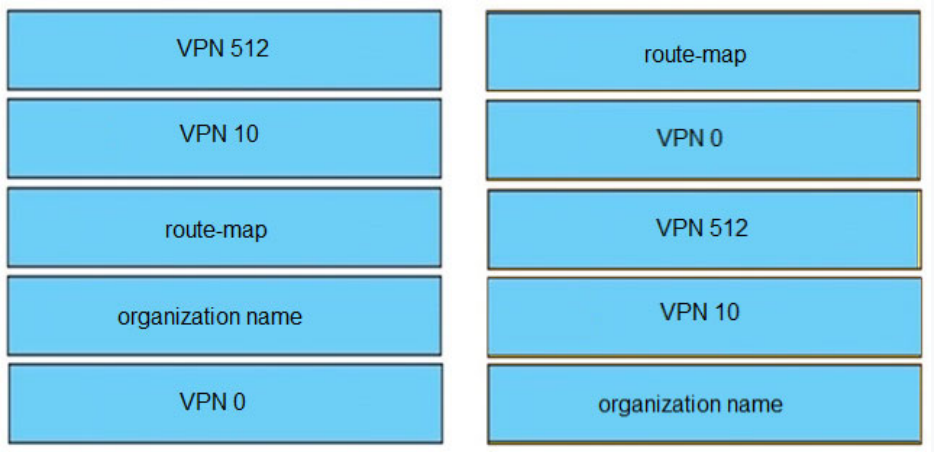
Drag and drop the functions from the left onto the correct templates on the right.

Select and Place:



Suggested Answer:





heavncong Most Recent 2 years, 1 month ago

correct

upvoted 1 times

ramjam 3 years, 8 months ago

correct.

upvoted 4 times

Question #103 *Topic 1*

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

Suggested Answer: *C*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/Enterprise_Firewall_with_Application_Awareness

Community vote distribution

C (100%)

khanda Most Recent 2 years ago

A VPN can be part of only one zone.

upvoted 2 times

JTPRO 2 years, 7 months ago

Given answer is correct https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=242

upvoted 2 times

Question #104 *Topic 1*

An engineer wants to track tunnel characteristics within a 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

Suggested Answer: *D*
Official Answer: D

Community vote distribution
A (100%)

venkat0594 Highly Voted 4 years, 11 months ago
correct answer should be A https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/application-aware-routing.html
upvoted 14 times

venkat0594 Highly Voted 4 years, 11 months ago
correct answer should be A https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/application-aware-routing.htmlI agree. Answer is A . 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.
upvoted 14 times

CCNPWILL 4 years, 9 months ago
I agree. Answer is A . 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.
upvoted 3 times

siang Most Recent 1 year, 8 months ago
A is correct
upvoted 1 times

Alchobashko 3 years ago
SLA based tracking is in APP route policy
upvoted 1 times

SlyNZ99 3 years, 2 months ago
Totally A vSmart1(config)# policy ? Possible completions: app-route-policy Configure application-aware routing policy cflowd-template Configure cflowd template control-policy List of control policies data-policy Configure data policy lists Configure lists policer Configure policer sla-class Configure SLA classes for application-aware routing vpn-membership List of VPN membership policies
upvoted 1 times

khanda 3 years, 6 months ago
A is the correct answer.
upvoted 2 times

Baio 3 years, 12 months ago
correct answer should be A
upvoted 1 times

juniper 4 years ago
A 100%
upvoted 1 times

Ben_001 4 years, 1 month ago
• Control Policies are applied at vSmart: Tailors routing information advertised to WAN endpoints • App-Route Policies are applied at WAN Edge: SLA-driven path selection for applications • Data Policies are applied at WAN Edge: Extensive Policy driven routing

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/BRKRST-2791.pdf page 6

upvoted 3 times

namashivaya 4 years, 3 months ago

I will go with D , Cisco's word game. app-route policy is not the correct naming, it should have been app-aware routing, which is in essence a centralized data policy.and even more the question is tricky, they said that the engineer wants to configured SLA for a future use in app-aware

upvoted 4 times

namashivaya 4 years, 3 months ago

I will go with D , Cisco's word game. app-route policy is not the correct naming, it should have been app-aware routing, which is in essence a centralized data policy.

upvoted 4 times

majepiga 3 years, 9 months ago

and even more the question is tricky, they said that the engineer wants to configured SLA for a future use in app-aware

upvoted 1 times

CesarVergaraGalindo 4 years, 4 months ago

D is correct

upvoted 1 times

TheNetworkStudent 4 years, 6 months ago

Application aware routing policy is a data policy so this question is a bit... dirty. But the book also specified this is done via an app-route policy. A is correct.

upvoted 3 times

TheNetworkStudent 4 years, 6 months ago

Application aware routing policy is a data policy so this question is a bit... dirty. But the book also specified this is done via an app-route policy. A is correct.Exactly what you say, tricky question this. You reach the right policy via Centralized -> Application Aware Routing. 'app-route' isn't mentioned anywhere in the GUI I think. I'll answer this with D since data policy is an actual term Cisco uses.but it is "app-route-policy" in the CLII think it's under centralized policy when you select sequences... but I'm not 100% sure

upvoted 3 times

serieus 4 years, 6 months ago

Exactly what you say, tricky question this. You reach the right policy via Centralized -> Application Aware Routing. 'app-route' isn't mentioned anywhere in the GUI I think. I'll answer this with D since data policy is an actual term Cisco uses.but it is "app-route-policy" in the CLII think it's under centralized policy when you select sequences... but I'm not 100% sure

upvoted 1 times

serieus 4 years, 6 months ago

Exactly what you say, tricky question this. You reach the right policy via Centralized -> Application Aware Routing. 'app-route' isn't mentioned anywhere in the GUI I think. I'll answer this with D since data policy is an actual term Cisco uses.

upvoted 1 times

spamke 4 years, 3 months ago

but it is "app-route-policy" in the CLI

upvoted 1 times

TheNetworkStudent 4 years, 5 months ago

I think it's under centralized policy when you select sequences... but I'm not 100% sure

upvoted 1 times

Question #105 *Topic 1*

An administrator needs to configure Cisco SD-WAN to divert traffic from the company's private network to an ISP network. Which action should be taken to accomplish this goal?

A. configure the security policy

B. configure the control policy

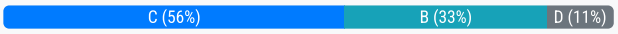
C. configure the data policy

D. configure the application aware policy

Suggested Answer: *C*

Official Answer: C

Community vote distribution



AonDuine Most Recent 2 months ago

Correct answer: C. The key phrase is: divert traffic from the company's private network to an ISP network means the administrator wants to steer/redirect data traffic from one path/transport to another — for example, from MPLS/private transport toward Internet/ISP transport.

upvoted 1 times

Scythe00 9 months, 1 week ago

To divert traffic from a private WAN to an ISP network in Cisco SD-WAN, you use an application-aware routing policy, which is part of the centralized data policy framework. This allows traffic steering based on performance metrics and application type. □ Why Application-Aware Policy Is the Right Choice - Direct Internet Access (DIA): Application-aware routing enables traffic to bypass the private WAN and use the ISP link directly, especially for SaaS or public internet-bound traffic. - Performance-Based Steering: You can define SLA thresholds (e.g., latency, jitter, loss) and steer traffic to the best-performing path, including ISP links. - Granular Control: Policies can match specific applications (e.g., Office 365, YouTube) and route them over the internet instead of MPLS or private WAN

upvoted 1 times

elbruno 2 years ago

C is correct The key word is Divert Traffic which you do with data policy.

upvoted 1 times

siang 2 years, 2 months ago

B is correct

upvoted 1 times

Networkchamp87 2 years, 3 months ago

Correct Answer B

upvoted 2 times

JP4CCNP 3 years, 4 months ago

I think the intention of this question is, to forward traffic from the LAN-Side to the Service-Provider (Underlay). This configuration would be done in a Traffic-Data-Policy. Answer C can be the only option. The AAR-Policy is only for SLA-Routing Side-To-Side

upvoted 4 times

Zdrobici 3 years, 6 months ago

maybe the question is related to another ISP to an external ISP that is not in the overlay and NAT is needed so thats why "centralized data policy" can work also (answ C)

upvoted 2 times

Erik_N 3 years, 8 months ago

Not sure what the intention is of the question. A control policy can be used to prefer ISP color over private network color for the whole topology.

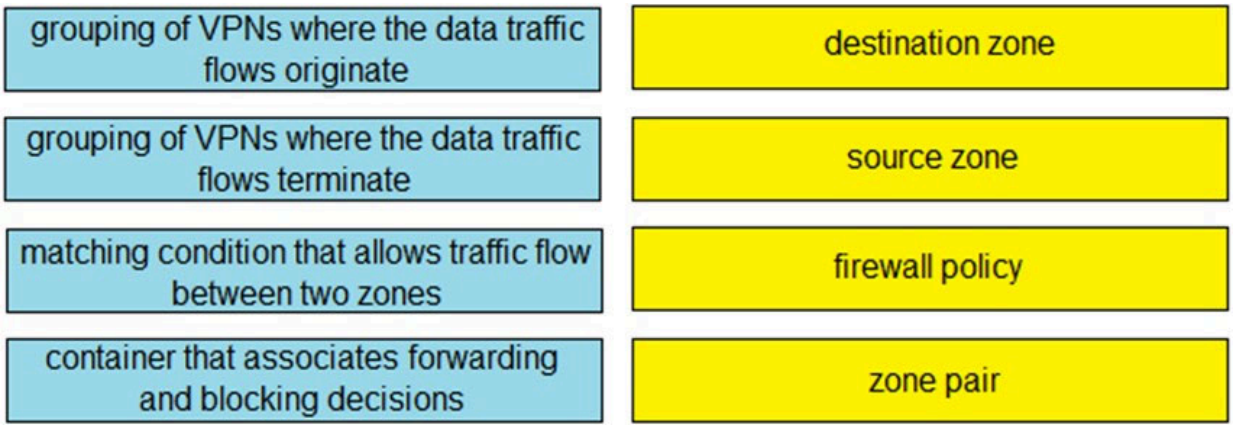
upvoted 4 times

Question #106 *Topic 1*

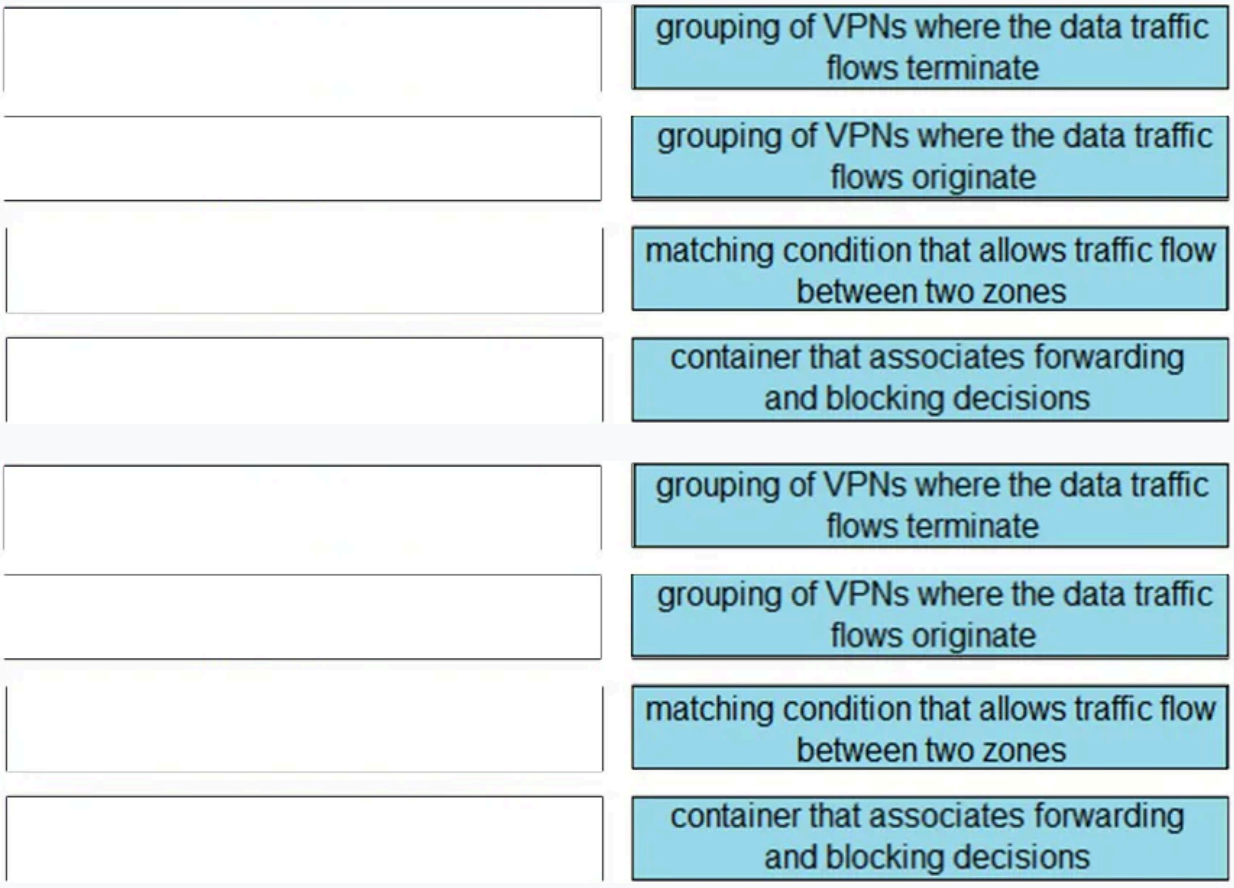
DRAG DROP -

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

Select and Place:



Suggested Answer:



Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/ent-firewall-app-aware.html#:~:text=Source%20zone%E2%80%94A%20grouping%20of,part%20of%20only%20one%20zone.&text=A%20VPN%20can%20be%20part%20of%20only%20one%20zone.,-Firewall% 20policy%E2%80%94A

Faridtnx Most Recent 6 months ago

Answer is wrong. Correct order is BADC Zone Pair: This is the specific directional relationship between two zones (e.g., Source_Zone to Destination_Zone). It acts as the "matching condition" because the firewall only examines traffic that matches a defined pair. • Firewall Policy: This is the actual "container" where you define your inspect, pass, or drop actions. It is applied to a zone pair to dictate the forwarding and blocking decisions for that specific traffic path.

upvoted 2 times

timbo2000 2 years ago

given answer is correct as cisco docs- Firewall policy—A security policy, similar to a localized security 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. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied. Zone pair—A container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

upvoted 3 times

bsk 2 years ago

I will go with the given answer, as per the link Zone configuration consists of the following components: Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone. Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone. Firewall policy—A security policy, similar to a localized security 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. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP. Matching flows for prefixes, ports, and protocols 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 firewall policy to the traffic that flows between the two zones.

upvoted 1 times

heavncong 2 years, 1 month ago

Given answer mixed up firewall policy and zone pair I will go for B -> A -> D -> C as well

upvoted 1 times

Erik_N 2 years, 2 months ago

Given answer is correct

upvoted 1 times

Roger95 2 years, 3 months ago

https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-2.pdf#page=474

upvoted 1 times

Roger95 2 years, 3 months ago

should be B -> A -> D -> Cyes agree

upvoted 3 times

Roger95 2 years, 3 months ago

should be B -> A -> D -> C

upvoted 3 times

Tan_Singh 2 years, 1 month ago

yes agree

upvoted 2 times

Question #107 *Topic 1*

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

A. vSmart

B. vBond

C. vManage

D. WAN Edge

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/policy-overview.html

Community vote distribution

A (100%)

BGP65000 Most Recent 2 years, 2 months ago

vsmart is the component that deploy policies to WAN Edges.

upvoted 1 times

Question #108 *Topic 1*

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

A. VPN 1

B. VPN 0

C. VPN 512

D. VPN 511

Suggested Answer: *B*
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/R6BGArNQ/TECRST-2191.pdf page 13

Fikie Most Recent 1 year, 9 months ago
Agree with given answer.
upvoted 1 times

go_Corona_go 4 years, 9 months ago
right answer
upvoted 4 times

Question #109 *Topic 1*

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. 0.0.0.0/0 le 16

B. 0.0.0.0/1 le 16

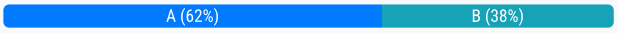
C. 0.0.0.0/0 ge 1

D. 0.0.0.0/16 ge 1

Suggested Answer: *B*

Official Answer: B

Community vote distribution



FlipCCNP Highly Voted 4 years, 8 months ago

This should be A. • 0.0.0.0/0—Match any prefix–length pair. • 0.0.0.0/0 le length—Match any IP prefix whose length is less than or equal to length. For example, ip-prefix 0.0.0.0/0 le 16 matches all IP prefixes with lengths from /1 through /16. https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/06Policy_Basics/03Localized_Control_Policy/Configuring_Localized_Control_Policy

upvoted 13 times

FlipCCNP Highly Voted 4 years, 8 months ago

This should be A. • 0.0.0.0/0—Match any prefix–length pair. • 0.0.0.0/0 le length—Match any IP prefix whose length is less than or equal to length. For example, ip-prefix 0.0.0.0/0 le 16 matches all IP prefixes with lengths from /1 through /16. https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/06Policy_Basics/03Localized_Control_Policy/Configuring_Localized_Control_PolicyA is correct. Directly from your link: "For example, ip-prefix 0.0.0.0/0 le 16 matches all IP prefixes with lengths from /1 through /16."

upvoted 13 times

CCNPCollab1297 4 years, 6 months ago

A is correct. Directly from your link: "For example, ip-prefix 0.0.0.0/0 le 16 matches all IP prefixes with lengths from /1 through /16."

upvoted 4 times

gladpark Most Recent 1 year, 5 months ago

0.0.0.0/0 le 16 matches all IP prefixes with lengths from /0 to /16. The question asks for /1 to /16.

upvoted 3 times

colipto 2 years, 6 months ago

Option A (0.0.0.0/0 le 16) also matches the criteria but it includes all IP prefixes up to /16, including those longer than /16 (e.g., /17, /18, etc.), which may not be desired. BOption B is a ridiculous answer, as it only matches routes where the first bit is a 0.Why would you think that? You even said, "up to /16." So that does NOT include /17, /18, etc. That's what up to /16 means. The mask is not longer than /16.

upvoted 1 times

colipto 2 years, 6 months ago

Option A (0.0.0.0/0 le 16) also matches the criteria but it includes all IP prefixes up to /16, including those longer than /16 (e.g., /17, /18, etc.), which may not be desired.

B

upvoted 1 times

timtgh 2 years, 5 months ago

Option B is a ridiculous answer, as it only matches routes where the first bit is a 0.

upvoted 1 times

timtgh 2 years, 5 months ago

Why would you think that? You even said, "up to /16." So that does NOT include /17, /18, etc. That's what up to /16 means. The mask is not longer than /16.

upvoted 1 times

khanda 3 years, 6 months ago

Correct answer is A.

upvoted 2 times

Han2022 3 years, 8 months ago

This should be A as well. • 0.0.0.0/0 le length—Match any IP prefix whose length is less than or equal to length. For example, ip-prefix 0.0.0.0/0 le 16 matches all IP prefixes with lengths from /1 through /16. Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/06Policy_Basics/03Localized_Control_Policy/Configuring_Localized_Control_Policy

upvoted 1 times

immphoenix 3 years, 9 months ago

Technically A is flawed becasue A match the default route 0.0.0.0/0, of which the prefix-length is arguably 0.

upvoted 3 times

Baio 3 years, 11 months ago

Corretto A Explanation in FlipCCNP comment

upvoted 1 times

MajorSalieri 4 years ago

B is correct. le denotes any range between 0-16(inclusive)

upvoted 1 times

Speirsington 4 years ago

A is correct

upvoted 2 times

spamke 4 years, 3 months ago

A is correct of course, but 0.0.0.0/1 le 16 is also matching all prefixes from /1 to /16, so.. interesting..no, 0.0.0.0/1 le 16 does not match "all prefixes", the /1 tells to check the first bit of the network, thus NOT all prefixes.

upvoted 1 times

spamke 4 years, 3 months ago

A is correct of course, but 0.0.0.0/1 le 16 is also matching all prefixes from /1 to /16, so.. interesting..

upvoted 1 times

A_Wolf 4 years ago

no, 0.0.0.0/1 le 16 does not match "all prefixes", the /1 tells to check the first bit of the network, thus NOT all prefixes.

upvoted 1 times

CesarVergaraGalindo 4 years, 4 months ago

A is correct

upvoted 2 times

isaacmejia 4 years, 7 months ago

The question clearly says from /1 to /16, 0.0.0.0/0 match everything Broadcast addr is 255.255.255.255. 0.0.0.0/1 Broadcast addr is 127.255.255.255 dont get confused isnot the same. i would go with B

upvoted 2 times

isaacmejia 4 years, 7 months ago

The question clearly says from /1 to /16, 0.0.0.0/0 match everything Broadcast addr is 255.255.255.255. 0.0.0.0/1 Broadcast addr is 127.255.255.255 dont get confused isnot the same. i would go with BPlease stop giving wrong answers in each question's comments.

upvoted 2 times

CCNPCollab1297 4 years, 6 months ago

Please stop giving wrong answers in each question's comments.

upvoted 6 times

ramjam 4 years, 8 months ago

Agree. It should be A. example, ip-prefix 0.0.0.0/0 le 16 matches all IP prefixes with lengths from /1 through /16.

upvoted 4 times

ramjam 4 years, 8 months ago

Agree. It should be A. example, ip-prefix 0.0.0.0/0 le 16 matches all IP prefixes with lengths from /1 through /16.A is the correct answer as the majority agreed because the le length up to /16 only

upvoted 4 times

Elmaestro 2 years ago

A is the correct answer as the majority agreed because the le length up to /16 only

upvoted 1 times

Question #110 *Topic 1*

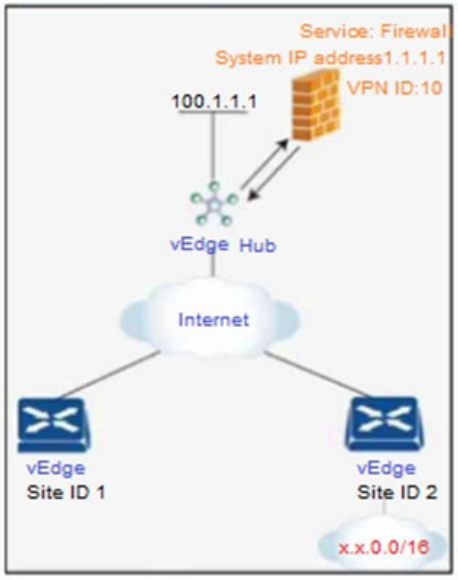
Refer to the exhibit. An engineer is configuring service chaining. Which set of configurations is required for all traffic from Site ID 1 going toward Site ID 2 to get filtered through the firewall on the hub site?

A.

B.

C.

D.




```
vpn 10
 service FW address 1.1.1.1
policy
 lists
  site-list firewall-service
   site-id 1
control-policy firewall-service
 sequence 10
  match route
   site-id 2
  action accept
   site service FW vpn 20
 default-action accept
apply-policy
 site-list firewall-sites control-policy firewall-service out
```

```
vpn 10
 service FW address 1.1.1.1
policy
 lists
  site-list firewall-sites
   site-id 1
control-policy firewall-service
 sequence 10
  match route
   site-id 2
  action accept
   site service FW vpn 10
 default-action accept
apply-policy
 site-list firewall-sites control-policy firewall-service out
```

```
vpn 20
 service FW address 1.1.1.1
policy
 lists
  site-list firewall-sites
   site-id 1
control-policy firewall-service
 sequence 10
  match route
   site-id 2
  action accept
   site service FW vpn 20
 default-action accept
apply-policy
 site-list firewall-sites control-policy firewall-service out


vpn 10
 service FW address 1.1.1.2
policy
 lists
  site-list firewall-sites
   site-id 1
control-policy firewall-service
 sequence 10
  match route
   site-id 2
  action accept
   site service FW vpn 10
 default-action accept
apply-policy
 site-list firewall-sites control-policy firewall-service out
```

Suggested Answer:
Official Answer: B

spamke Highly Voted 3 years, 9 months ago
it should be 'set service ...' and not 'site service ...' but otherwise B is correct
upvoted 5 times

Xhizors Highly Voted 3 years, 7 months ago
Notice the FW address and VPN id. Correct answer is BAccurate for fast response TKS!
upvoted 5 times

Xhizors 3 years, 7 months ago
Notice the FW address and VPN id.

Correct answer is B
upvoted 5 times

RREVECO 3 years, 2 months ago
Accurate for fast response TKS!
upvoted 2 times

NetArch_Teck Most Recent 2 years, 1 month ago
In order to forward traffic to Site ID 2 and to get filtered through the hub firewall The VPN 10 service address needs to be defined 1.1.1.1 (system ip)
Also the control-policy firewall-service would need to forward traffic out of VPN 10 with a route-map to filter traffic. Option B facilitates the request
upvoted 1 times

she_ccie 3 years, 6 months ago
B - this is pulled right from a policy config guide for v20. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html
upvoted 3 times

Question #111 *Topic 1*

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 > accept

B. policy > data-policy > vpn-list > sequence > match

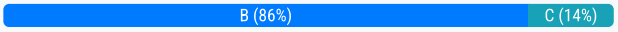
C. policy > data-policy > vpn-list > sequence > action

D. policy > data-policy > vpn-list > sequence > default-action > drop

Suggested Answer: *C*

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

Community vote distribution



ramjam Highly Voted 4 years, 8 months ago

C. Actions - Whether to accept or reject (and drop) matching packets, and how to process matching packets.

upvoted 9 times

uzbin Most Recent 1 year, 3 months ago

You have to MATCH before you can ACTION.

upvoted 1 times

RafaJohnston76 2 years ago

I believe is B, because the question is " packets that must be captured through the policy", my understand of the question is that a specific set of packets needs to be captured, and Match would be need it to define which packets will be captured

upvoted 1 times

Xiaolonguk 2 years ago

I believe its C as its clearly shown here https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=358

upvoted 1 times

Aldebeer 2 years, 3 months ago

In my optic, it is C.

upvoted 1 times

AJMD 2 years, 5 months ago

capture the packet. Answer B

upvoted 1 times

Neil_Neo234 2 years, 10 months ago

How about log packets after the match condition is satisfied? It will come under C, right?
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html

upvoted 1 times

Zdrobici 3 years ago

I would choose B because you always have the default action by default.

upvoted 1 times

khanda 3 years, 6 months ago

vSmart-1(config-vpn-list-1)# sequence 1 vSmart-1(config-sequence-1)# ? Possible completions: action Accept or drop match Match criteria

upvoted 1 times

khanda 3 years, 6 months ago

B is correct if you will be explicitly matching on something, also C is correct if you match "any"

upvoted 2 times

shanntorana 3 years, 10 months ago

i looked at this from JTPRO https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKRST-2791.pdf#page=72 B does seem to be the best answer or am i reading this incorect

upvoted 2 times

Nyck 3 years, 11 months ago

A centralized data policy based on source and destination prefixes and on headers in IP packets consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy. "match-action" Meaning ? Action or match ? LOL

upvoted 1 times

Nyck 3 years, 11 months ago

A centralized data policy based on source and destination prefixes and on headers in IP packets consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy. "match-action" Meaning ? Action or match ? LOLThe command is Match. So B ?

upvoted 1 times

Nyck 3 years, 11 months ago

The command is Match. So B ?

upvoted 1 times

Almanac 4 years ago

I think its B. Because match is always come first after sequence sequence > match > action > default action

upvoted 2 times

JTPRO 4 years ago

answer = B Look here under "Data Policy Structure" . Page 72 https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL-BRKRST-2791.pdf#page=72

upvoted 3 times

DBla 4 years, 4 months ago

I would choose B. Capturing is not an action type and here it means, in my opinion, packets that are interesting for the use case.

upvoted 4 times

RexChen 4 years, 8 months ago

B or C?

upvoted 1 times

Question #112 *Topic 1*

An administrator must configure an ACL for traffic coming in from the service-side VPN on a specific WAN Edge device with circuit ID 123456789. 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

Suggested Answer: *D*
Official Answer: D

Community vote distribution
A (100%)

takhira Highly Voted 3 years, 9 months ago
I would say that it is local data policy that took only specific device. The answer is A
upvoted 18 times

heamgu Most Recent 2 years, 1 month ago
Correct answer is A.
upvoted 3 times

AW57 2 years, 2 months ago
A (LOcal data policy) should correct answer
upvoted 1 times

khanda 2 years, 6 months ago
Correct answer is A. Localized data policy. Documentation in the comments.
upvoted 2 times

Baio 2 years, 12 months ago
A is correct
upvoted 2 times

she_ccie 2 years, 12 months ago
Localized data policy controls the flow of data traffic into and out of interfaces and interface queues on a vEdge router. This type of data policy is provisioned locally, on the vEdge router, using access lists. It allows you to classify traffic and map different classes to different queues. It also allows you to mirror traffic and to police the rate at which data traffic is transmitted and received.
https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf
upvoted 1 times

she_ccie 2 years, 12 months ago
Localized data policy controls the flow of data traffic into and out of interfaces and interface queues on a vEdge router. This type of data policy is provisioned locally, on the vEdge router, using access lists. It allows you to classify traffic and map different classes to different queues. It also allows you to mirror traffic and to police the rate at which data traffic is transmitted and received.
https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdfData policy influences the flow of data traffic traversing the network based either on fields in the IP header of packets or the router interface on which the traffic is being transmitted or received. Data traffic travels over the IPsec connections between vEdge routers, shown in purple in the adjacent figure. 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 vSmart controller, is the Viptela 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 vEdge router, allows customization of routing decisions made by BGP and OSPF on site-local branch or enterprise networks.
upvoted 1 times

she_ccie 2 years, 12 months ago
Data policy influences the flow of data traffic traversing the network based either on fields in the IP header of packets or the router interface on which the traffic is being transmitted or received. Data traffic travels over the IPsec connections between vEdge routers, shown in purple in the adjacent figure. 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 vSmart controller, is the Viptela 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 vEdge router, allows customization of routing decisions made by BGP and OSPF on site-local branch or enterprise networks.

upvoted 1 times

juniper 3 years ago

A is correct

upvoted 2 times

stepstranger 3 years, 2 months ago

CONFIGURATION | POLICIES Localized Policy> Access Control Lists Policy> Add IPV4 ACL Policy

upvoted 3 times

mullo 3 years, 2 months ago

Clearly this answer is A

upvoted 1 times

CesarVergaraGalindo 3 years, 4 months ago

A is correct

upvoted 1 times

serieus 3 years, 6 months ago

Sounds like A to me as well mentioning the single specific device.

upvoted 1 times

Maurel 3 years, 8 months ago

agree with you , correct answer should be A

upvoted 3 times

Question #113 *Topic 1*

Refer to the exhibit. The tunnel interface configuration on both WAN Edge routers is:

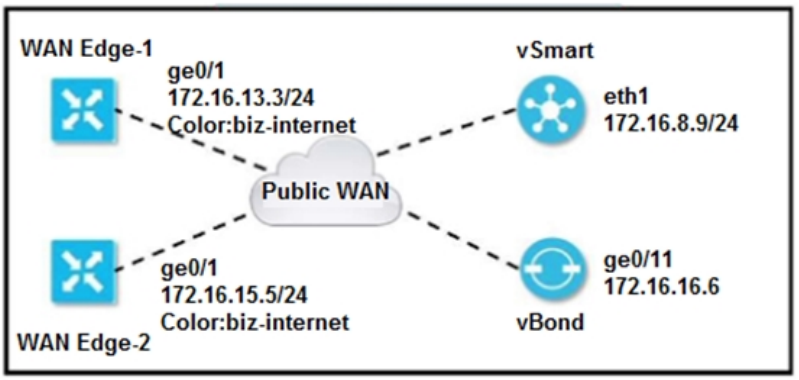
Which configuration for WAN Edge routers will connect to the Internet?

A.

B.

C.

D.




```
vpn 0
 interface ge0/1
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service ntp
   no allow-service stun
  !
  no shutdown
```

```
vpn 0
 interface ge0/1
  ip address 172.16.15.5/24
 !
ip route 0.0.0.0/0 172.16.8.1
```

```
vpn 0
 interface ge0/1
  ip address 172.16.15.5/24
 !
ip route 0.0.0.0/0 172.16.13.1
```

```
vpn 0
 interface ge0/1
  ip address 172.16.13.3/24
 !
ip route 0.0.0.0/0 172.16.13.1
```

```
vpn 0
 interface ge0/1
  ip address 172.16.13.3/24
 !
ip route 0.0.0.0/0 172.16.8.1
```

Suggested Answer:
Official Answer: B

Mr_Cipher Highly Voted 5 years, 1 month ago
I think it's C. It's the only logical answer since the Interface IP and GW are in the same subnet
upvoted 23 times

Aldebeer Highly Voted 2 years, 9 months ago
I go for C. the only one which senses.
upvoted 5 times

Rosh8787 Most Recent 1 year, 10 months ago
Correct answer C.
upvoted 4 times

hopatrickhk88 3 years, 1 month ago
It is important to understand “configuration for WAN Edge routers“ That means you choose the answer for two router VPN 0. The answer is B because VPN 0 interface ge 0/1 ip address 172.16.15.5/24 is the configuration for WAN edge-2 and vpn 0 ip route 0.0.0.0/0 172.16.13.1 is to configure default route in vpn 0 of WAN edge-1.No. Since every answer given has a single IP configuration, it's clear that each answer is just showing the config of a single router. Poorly worded, but that is clearly the intention. Option C is correct if applied to Edge-1, and the other three options are not correct on either router.agree with tim
upvoted 3 times

hopatrickhk88 3 years, 1 month ago
It is important to understand “configuration for WAN Edge routers“

That means you choose the answer for two router VPN 0. The answer is B because VPN 0 interface ge 0/1 ip address 172.16.15.5/24 is the configuration for WAN edge-2 and vpn 0 ip route 0.0.0.0/0 172.16.13.1 is to configure default route in vpn 0 of WAN edge-1.
upvoted 3 times

timtgh 2 years, 11 months ago
No. Since every answer given has a single IP configuration, it's clear that each answer is just showing the config of a single router. Poorly worded, but that is clearly the intention. Option C is correct if applied to Edge-1, and the other three options are not correct on either router.agree with tim
upvoted 3 times

timtgh 2 years, 11 months ago
No. Since every answer given has a single IP configuration, it's clear that each answer is just showing the config of a single router. Poorly worded, but that is clearly the intention. Option C is correct if applied to Edge-1, and the other three options are not correct on either router.
upvoted 3 times

Loi2525 2 years ago
agree with tim
upvoted 2 times

NetArch_Teck 3 years, 1 month ago
The question can be misleading but when utilizing networking basics of logical addressing scheme and hierarchy, the main configuration takes place on the primary devices first (or WAN Egde-1) then to other devices. The default route is clearly via WAN Edge-1 due to the 172.16.13.0/24 Class B subnet C VPN 0 interface ge0/1 ip address 172.16.13.3/24 ip route 0.0.0.0/0 172.16.13.1
upvoted 1 times

carlovalle 4 years ago
How can be B If default gw is not in the same subnet
upvoted 1 times

khanda 4 years ago
C is the correct answer, check IP addressing.
upvoted 2 times

assili 4 years ago

The correct answear is C

upvoted 1 times

Hoosainsays 4 years, 6 months ago

The Answer Would be B if the question is referring to WAN Edge 2

upvoted 1 times

juniper 4 years, 6 months ago

C is 100%

upvoted 1 times

CesarVergaraGalindo 4 years, 10 months ago

C is correct

upvoted 2 times

serieus 5 years ago

First of all the question isn't even a complete sentence.. Going by the addressing only C makes some sense

upvoted 3 times

CCIEINFRA 5 years, 1 month ago

Look at the interface configuration and the given default route in each option.

upvoted 3 times

Almanac 5 years, 3 months ago

the correct answer is C.

upvoted 4 times

go_Corona_go 5 years, 3 months ago

can anyone explain what will be the correct answer and why ? for me even the question looks strange

upvoted 2 times

Question #114 *Topic 1*

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

A.

B.

C.

D.

```
Site 1:
vpn10
      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
```

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


control-policy firewall-service
 sequence 10
  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
```

Suggested Answer:
Official Answer: C

msstanick Most Recent 7 months, 1 week ago

My control firewall policy looks as below - I would go with A then, but this question is quite vague vSmart1# show running-config policy control-policy sequence 21 policy control-policy BRANCH-VPN10-VIA-DC sequence 21 match route prefix-list _AnyIpv4PrefixList site-list BRANCHES-SOUTH vpn-list SERVICE-VPN-10 ! action accept set service FW vpn 10 tloc-list DC-TLOC-SOUTH

upvoted 1 times

RafaJohnston76 2 years ago

C is correct, look at this link the example is exactly the question
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/service-chaining.html

upvoted 3 times

soltani 2 years, 1 month ago

A is correct sequence 21 match route site-list SPOKES ! action accept set service FW ! !

upvoted 4 times

timtgh 2 years, 5 months ago

A and C are identical, except that A has the word "set" on its own line, which is an optional style and is acceptable. It's ridiculous that they would have it both ways, which are both correct, and expect us to choose one.

upvoted 3 times

timtgh 2 years, 5 months ago

A and C are identical, except that A has the word "set" on its own line, which is an optional style and is acceptable. It's ridiculous that they would have it both ways, which are both correct, and expect us to choose one.I think that's where they are trying to trip you up. the "set" parameter is meant to be in line with the FW service

upvoted 3 times

PureInertiaCopy 1 year, 11 months ago

I think that's where they are trying to trip you up. the "set" parameter is meant to be in line with the FW service

upvoted 1 times

khanda 3 years, 6 months ago

I'd go for answer A, C is technically correct as well. policy control-policy Firewall-service sequence 10 match route site-id 2 ! action accept set service FW vpn 10 ! ! ! default-action accept ! !

upvoted 2 times

Almanac 4 years ago

A and C are both correct. from cisco digital learning it is A https://ondemandelearning.cisco.com/cisco-cte/ensdwi20/sections/9/pages/7 . but on the preview from vManage on dCloud its letter C viptela-policy:policy control-policy Test_Service_Chaingin sequence 1 match route site-list Site300 vpn-list VPN10 prefix-list _AnyIpv4PrefixList ! action accept set service FW vpn 10 ! ! ! default-action accept ! lists site-list Site200 site-id 200 ! site-list Site300 site-id 300 ! vpn-list VPN10 vpn 10 ! prefix-list _AnyIpv4PrefixList ip-prefix 0.0.0.0/0 le 32 ! ! ! apply-policy site-list Site200 control-policy Test_Service_Chaingin out ! !

upvoted 1 times

juniper 4 years ago

C is correct

upvoted 1 times

Jimmy3848 4 years, 4 months ago

The SD-WAN book literally teaches that ‘set’ and ‘service’ are on 2 separate lines. Therefore, ‘A’ is the correct answer. Based on the 2021 book. Although, you can find online where ‘C’ is also referenced. Typical Cisco ambiguity.

upvoted 2 times

DBla 4 years, 4 months ago

A is also correct. set and service commands don't need to be in the same line.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html

upvoted 1 times

milan74 4 years, 4 months ago

IMO answer is C. This is a snippet of an example config: 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 So answers A and D are not correct, as in the syntax an extra "set" is used. Answer B is incorrect bc it does not include the vpn and service name FW in the command.

upvoted 1 times

Question #115 *Topic 1*

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 fulfills these requirements?

A.

B.

C.

D.

```
vpn 10
 name "*** Service VPN 10 ***"
 router
  ospf
   redistribute omp route-policy OSPF_Route_Policy
  area 0
   interface ge0/2
   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 type1
```

```
vpn 0
router
 ospf
  redistribute omp route-policy OSPF_Route_Policy
 area 0
  interface ge0/2
  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 type1
```

```
vpn 0
router
 ospf
  redistribute omp route-policy OSPF_Route_Policy
 area 0
  interface ge0/2
  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 type2
```

```
vpn 10
 name "*** Service VPN 10 ***"
 router
  ospf
   redistribute omp route-policy OSPF_Route_Policy
  area 0
   interface ge0/2
   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 type1
```

Suggested Answer:
Official Answer: D

Nalla123 Highly Voted 2 years, 11 months ago

Answer -A Question says --> W2 loopback received via OMP to the OSPF neighbor on the service-side VPN, so here service side VPNS come into 1-511. Option -A 1.) has mentioned with VPN 10 2.) Loopback set with /32 3.) After default action accept there wont be any set commands. In option A it says ACTION ACCEPT

upvoted 15 times

Nalla123 Highly Voted 2 years, 11 months ago

Answer -A Question says --> W2 loopback received via OMP to the OSPF neighbor on the service-side VPN, so here service side VPNS come into 1-511. Option -A 1.) has mentioned with VPN 10 2.) Loopback set with /32 3.) After default action accept there wont be any set commands. In option A it says ACTION ACCEPTYes, and even if set commands were allowed in the default action, putting the set commands there would not limit them to that loopback as needed.

upvoted 15 times

timtgh Most Recent 1 year, 11 months ago

Yes, and even if set commands were allowed in the default action, putting the set commands there would not limit them to that loopback as needed.

upvoted 1 times

TheNetworkStudent 3 years, 11 months ago

key differences are the VPN number and that the loopback address is a /24 or /32. I think it should be VPN 10 and /32, which would make A correct.

upvoted 8 times

NetArch_Teck 2 years, 1 month ago

I concur with the network group. Loopback addresses are /32 normally when setting up peer to peer interfaces. VPN 0 is a transport WAN service , so option B and C are not correct VPN 10 - is within the range of service VPN's (besides 512 and 0 which are dedicated management and transport exclusive VPN services) Set commands are no longer accepted to the interface once the default-action command is imitated! Option A is the only answer that accommodates the request.

upvoted 1 times

RREVECO 3 years, 2 months ago

The answer is A: EXPLANATION if we see the link: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/control-policies.html DETAIL 01 LOOPBACK = /32 and not /24 DETAIL 02 in answer D A) it says "default action" and not "default-action" = misspelled command B) even if it was good, the metric attributes are applied in the default option and not in the sequence 1 Detail 03: Question says: Which configuration fulfills these requirements? (ALTERNATIVE A is the most correct) if we see the link: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/control-policies.html the structure is: Structural Components for Localized Control Policy

upvoted 5 times

Sky_Soul 3 years, 5 months ago

Answer is A There is no possibility to SET something within the Default-Action configuration mode. Structural Components for Localized Control Policy policy lists as-path-list list-name as-path path-list community-list list-name community [aa:nn | internet | local-as | no-advertise | no-export] ext-

community-list list-name community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)] prefix-list list-name ip-prefix prefix/length route-policy policy-name sequence number match match-parameters action reject accept set parameters default-action (accept | reject) vpn vpn-id router bgp local-as-number neighbor address address-family ipv4-unicast route-policy policy-name (in | out) vpn vpn-id router ospf route-policy policy-name in redistribute (bgp | connected | nat | omp | static) route-policy policy-name

upvoted 2 times

Crazy_Creator 3 years, 6 months ago

Answer = D Do you see lack of word default in A answer ? The correct CLI syntax should be default action accept not accept action. They did it this way for the purpose hehe ... Another one tricky question, hard to find but once captured easy to see.D is missing the "-" making it an invalid command. The correct syntax would be " default-action accept " . I think that makes answer A more correct because " action accept " is a valid command.

upvoted 1 times

Crazy_Creator 3 years, 6 months ago

Answer = D Do you see lack of word default in A answer ? The correct CLI syntax should be default action accept not accept action. They did it this way for the purpose hehe ... Another one tricky question, hard to find but once captured easy to see.

upvoted 1 times

JTPRO 3 years, 6 months ago

D is missing the "-" making it an invalid command. The correct syntax would be " default-action accept " . I think that makes answer A more correct because " action accept " is a valid command.

upvoted 2 times

simo_2020 3 years, 8 months ago

Answer must start with VPN 10(service side) & should have metric-type 1 and not with VPN 0 (transport side) so the answer is AI agree that it's A, for several reasons. But why the requirement for metric-type 1? The question doesn't seem to mention anything that would require using metric-type 1.

upvoted 2 times

simo_2020 3 years, 8 months ago

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

upvoted 2 times

timtgh 1 year, 11 months ago

I agree that it's A, for several reasons. But why the requirement for metric-type 1? The question doesn't seem to mention anything that would require using metric-type 1.

upvoted 1 times

sysarf 3 years, 9 months ago

Answer A is correct

upvoted 1 times

Jimmy3848 3 years, 10 months ago

Answer is A. 'A' has a 'match & action accept' pair, whereas answer 'D' has a 'match' without an 'action accept,' but rather the 'default-action' which makes the subsequent 'set…' action incorrect syntax.

upvoted 3 times

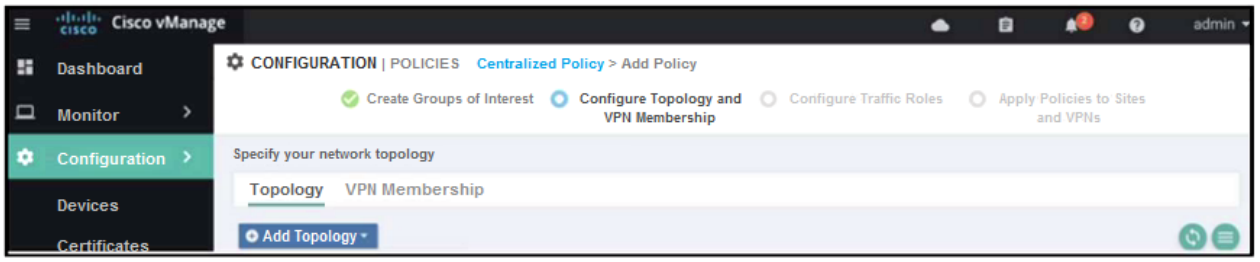
JasonNH 3 years, 11 months ago

The Answer should be A?

upvoted 2 times

Question #116 *Topic 1*

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. mesh

B. custom control (route and TLOC)

C. hub-and-spoke

D. import existing topology

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

DBla Highly Voted 3 years, 10 months ago
No. The policy has to allow TLOCs and routes from that site, which is filtered out by the existing hub and spoke topology. Custom control policy is the correct one.
upvoted 9 times

ChrisCCNA Highly Voted 3 years ago
B - Custom control
upvoted 5 times

timtgh Most Recent 1 year, 11 months ago
D is a ridiculous answer because it's too general. An imported topology still has to have a type, such as mesh or custom. And obviously it's not C.
upvoted 1 times

NetArch_Teck 2 years ago
Answer is [B] Please refer to Cisco's own guide:- https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/control-policies.html#id_107222
upvoted 1 times

Fireforwall 2 years, 1 month ago
Ans: A - Mesh
upvoted 1 times

khanda 3 years ago
Correct answer is D. Take note of "in addition to an existing hub-and-spoke policy"
upvoted 3 times

CesarVergaraGalindo 3 years, 10 months ago
D is Correct
upvoted 2 times

Question #117 *Topic 1*

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

A. data policy with redirect

B. local domain bypass

C. DNSCrypt configuration

D. DHCP option 6

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

khanda Most Recent 2 years ago

B is correct, check Page 377 on the official Cisco press book.

upvoted 2 times

khanda 2 years ago

B is correct. "If the DNS query is for a local domain, it forwards the query without changing the DNS packet to the DNS server in the enterprise network" ----> https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/umbrella-integration.html

upvoted 3 times

milan74 2 years, 10 months ago

I think answer B too. Link: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge-20-x/security-book/cisco-umbrella-integration.html

upvoted 2 times

Question #118 *Topic 1*

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. deterministic order

B. lowest to highest sequence number

C. highest to lowest sequence number

D. nonsequential order

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (75%) C (25%)

PandiyaGomathi Most Recent 2 years ago
answer is c
upvoted 1 times

Zamochit 2 years, 6 months ago
question says, which order. Like for prefix list, acl, in your control policy, data policy etc, always your specifics match must be on the lower sequences, you have to go to specific till general ones, if not the specific ones will never match. In the same way, if you want to match first prefix list, so you use lower seq for this, next for tloc and so on. I hope it helps.
upvoted 3 times

RafaJohnston76 2 years, 6 months ago
I am confused, because the question says "Prefer", and preference set is the highest to lowest, which would make C correct
upvoted 1 times

timtgh 2 years, 11 months ago
How can they both be correct? There is no mention of the word "order" in those options. Both B and C refer to sequence number. B says lowest to highest, and C says the reverse. Only one can be correct.
upvoted 1 times

hopatrickhk88 3 years, 1 month ago
B. lowest order to highest sequence number C. highest order to lowest sequence number Are both B and C correct ??
upvoted 1 times

Question #119 *Topic 1*

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.)

```
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, 1w0d, 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, 1w0d, GigabitEthernet0/0/1.11
```

A. The default route is configured locally.

B. This routing table is from a cEdge router.

C. The configured policy is adding a route tag of 300 to learned routes.

D. The default route is learned via OMP.

E. The routing table is for the transport VPN.

Suggested Answer: *A, B*

Official Answer: AB

Community vote distribution

BD (80%) AD (20%)

tester2478 Highly Voted 4 years, 11 months ago

since AD is 251 (default for cisco sd wan router) and route is M (leraned via OMP) B and D should be correctcorrect.

upvoted 23 times

tester2478 Highly Voted 4 years, 11 months ago

since AD is 251 (default for cisco sd wan router) and route is M (leraned via OMP) B and D should be correct

upvoted 23 times

Almanac 4 years, 7 months ago

correct.

upvoted 2 times

lollo1234 4 years, 11 months ago

Correct answers are B and D. B because it uses "vrf" and not "vpn". D because is a "m" route and the AD is 251.You may be right, but be aware that Cisco is planning to deprecate the "vpn" syntax and use "vrf" for all models.

upvoted 13 times

lollo1234 4 years, 11 months ago

Correct answers are B and D. B because it uses "vrf" and not "vpn". D because is a "m" route and the AD is 251.

upvoted 13 times

timtgh 2 years, 11 months ago

You may be right, but be aware that Cisco is planning to deprecate the "vpn" syntax and use "vrf" for all models.

upvoted 1 times

Loi2525 Most Recent 2 years ago

B and D!

upvoted 1 times

Zamochit 2 years, 6 months ago

show ip route vrf, so Cedge. Then you can see m for your default route, so you are learning it through OMP , who is anouncing it is system ip 10.1.9.2 and 10.1.9.3 , system ips of the remote site announcing df GW.

upvoted 1 times

izduk 3 years, 1 month ago

Originally OMP has 250 AD value in vEdge platforms. For cEdge it is 251, because NHRP has 250 AD which exists in Cisco OS before SD-WAN. m* shows routes learned from OMP

upvoted 2 times

jcms700 3 years, 1 month ago

B--> routing table is from an Edge Router for sure. D--> default and prefered route 0.0.0.0/0 is being learn by OMP protocol(m*)

upvoted 1 times

hamidreza0010 3 years, 3 months ago

B and D are correct

upvoted 2 times

kcobain87 3 years, 9 months ago

B/D for sure

upvoted 2 times

khanda 4 years ago

Correct answer is B and D

upvoted 2 times

Baio 4 years, 5 months ago

ISR because is VRF and not VPN in the show default route is learned from OMP because "m" in the show ip route is for OMP

upvoted 2 times

CesarVergaraGalindo 4 years, 10 months ago

B, D is Correct

upvoted 5 times

TheNetworkStudent 4 years, 11 months ago

Can anyone explain this? No clue why this should be A and B...

upvoted 1 times

Question #120 *Topic 1*

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 fulfills this requirement?

A. Create Applications or Groups of Interest > Configure Traffic Data > 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 Rules > Apply Policies to Sites and VPNs.

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

Suggested Answer: *C*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html#id_107211

Community vote distribution

C (100%)

Outlaw_87 Most Recent 2 years, 1 month ago

C is correct. Application Aware Routing is under Configure Traffic Rules in vManage. Reference: SD-WAN CBT Nuggets video course (instructor Knox Hutchinson).

upvoted 2 times

she_ccie 3 years, 12 months ago

To configure centralized policies using Cisco vManage, use the steps identified in the procedures that follow this section. Start the Policy Configuration Wizard Configure Groups of Interest for Centralized Policy Configure Topology and VPN Membership Import Existing Topology Create a VPN Membership Policy Configure Traffic Rules Match Parameters - Control Policy Match Parameters - Data Policy Action Parameters - Control Policy Action Parameters - Data Policy Apply Policies to Sites and VPNs Activate a Centralized Policy

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/centralized-policy.html

upvoted 2 times

Speirsington 4 years, 1 month ago

Create Applications or Groups of Interest > Configure Traffic Rules > Apply Policies to Sites and VPNS.

upvoted 3 times

Question #121 *Topic 1*

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. Configure network topology.

B. Apply policies to sites and VPNs.

C. Configure traffic rules.

D. Create groups of interest.

Suggested Answer: *D*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html#id_107211

Community vote distribution

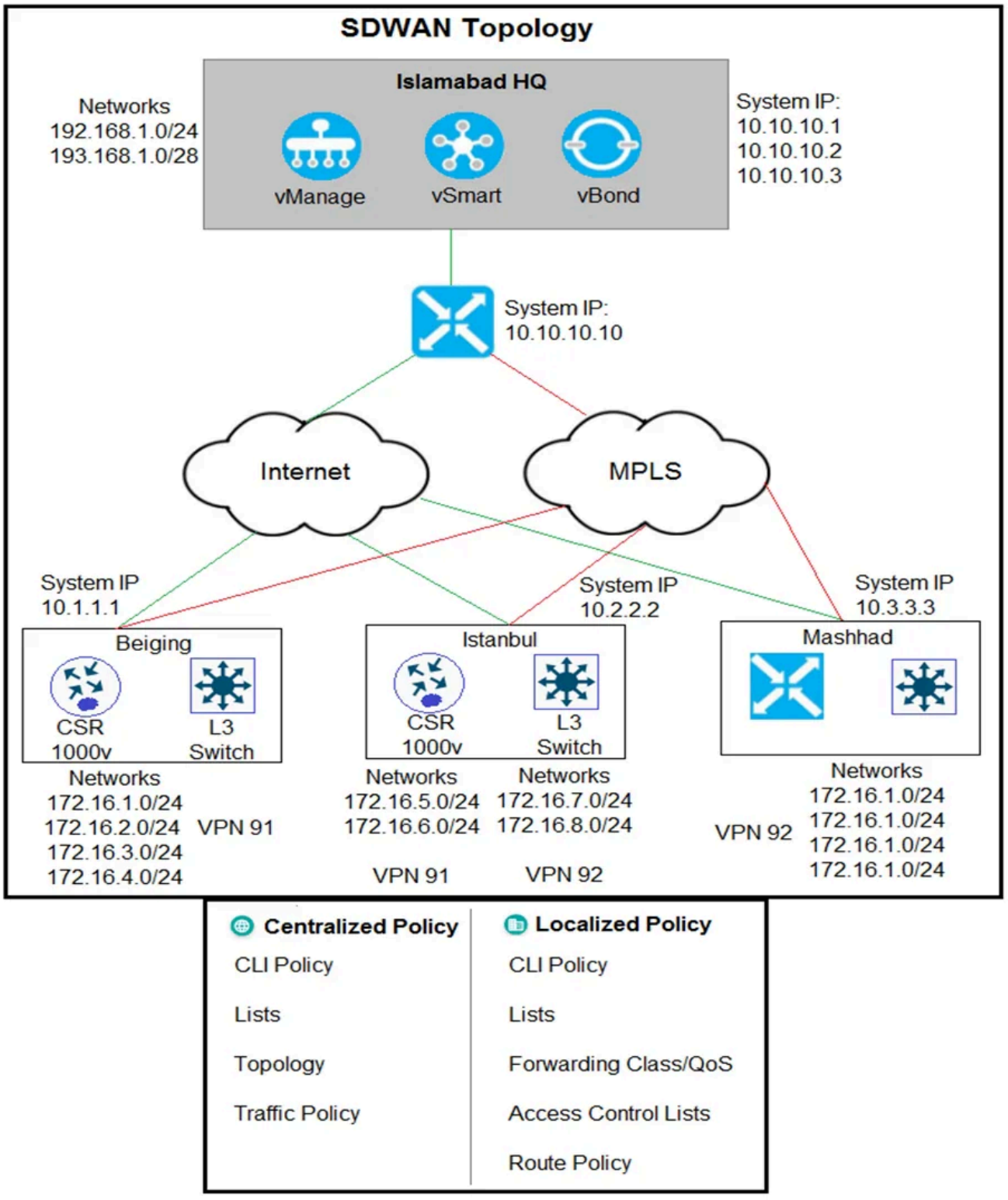
D (100%)

Maurel Highly Voted 2 years, 1 month ago

Should be D

upvoted 5 times

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. Centralized Policy, Traffic Policy

B. Centralized Policy, Topology

C. Localized Policy, Forwarding Class

D. Localized Policy, Route Policy

Suggested Answer: *B*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/centralized-policy.html#Cisco_Concept.dita_d31f22cb-f54f-41df-966a-0ae1ca3c398a

Community vote distribution

A (100%)

thomazmr Most Recent 2 years ago

Correct A

upvoted 1 times

Aldebeer 2 years, 2 months ago

the best answer is A

upvoted 1 times

AJMD 2 years, 5 months ago

Correct A

upvoted 1 times

hopatrickhk88 2 years, 7 months ago

Question is asking for "Which policy configuration does the network engineer use to call the SLA class and set the preferred color to MPLS?" To fulfil the requirements, AAR and data traffic policy should be used and hence Centralized policy, Traffic Policy is the answer.

upvoted 1 times

carlovalle 3 years, 6 months ago

An SLA Class list only can be added via AAR policy. AAR policy is part of Traffic-Rules, not traffic-Policy, so I think that best answer would be Centralized-Traffic Rules (doesnt exists)

upvoted 1 times

khanda 3 years, 6 months ago

CONFIGURATION | POLICIES - Centralized Policy> Data Policy This will be AAR to call the SLA list and pin traffic to MPLS color.

upvoted 2 times

carlovalle 3 years, 6 months ago

I think A and B should be correct IF it's multiple options Topology for HUb and Spoke and Traffic for AAR

upvoted 1 times

khanda 3 years, 6 months ago

CONFIGURATION | POLICIES - Centralized Policy> Data Policy

upvoted 1 times

Han2022 3 years, 8 months ago

The answer should be A

upvoted 4 times

she_ccie 3 years, 11 months ago

I just worked on this in my lab. You cannot match FTP in a Topology policy. You must move to the Traffic Data in "Configure Traffic Rules" to be given the opportunity to match on "FTP protocol." Also - the topology is not being changed. This is more of an old fashioned PBR that is changing the direction of FTP traffic. IMHO

upvoted 1 times

she_ccie 3 years, 11 months ago

I just worked on this in my lab. You cannot match FTP in a Topology policy. You must move to the Traffic Data in "Configure Traffic Rules" to be given the opportunity to match on "FTP protocol." Also - the topology is not being changed. This is more of an old fashioned PBR that is changing the direction of FTP traffic. IMHOYou can create individual policy components directly and then use them or import them when you are using the policy configuration wizard: In the title bar, click the Custom Options drop-down. For centralized policies, select the Centralized Policy tab and then select a policy component: CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard. Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard. Topology—Create a hub-and-spoke, mesh, or custom topology or a VPN membership to import in the Topology screen in the policy configuration wizard. Traffic Policy—Create an application-aware routing, traffic data, or cflowd policy to import in the Traffic Rules screen in the policy configuration wizard.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/Policy-basics.html

upvoted 1 times

she_ccie 3 years, 11 months ago

You can create individual policy components directly and then use them or import them when you are using the policy configuration wizard: In the title bar, click the Custom Options drop-down. For centralized policies, select the Centralized Policy tab and then select a policy component: CLI policy—

Create the policy using the command-line interface rather than the policy configuration wizard. Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard. Topology—Create a hub-and-spoke, mesh, or custom topology or a VPN membership to import in the Topology screen in the policy configuration wizard. Traffic Policy—Create an application-aware routing, traffic data, or cflowd policy to import in the Traffic Rules screen in the policy configuration wizard.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/Policy-basics.html
upvoted 1 times

Almanac 4 years ago
Correct answer is A. it should be configure on App Aware., Under Traffic Rule matching the FTP application and action select the" SLA class list" preferred color MPLS
upvoted 2 times

juniper 4 years ago
A is correct
upvoted 2 times

Speirsington 4 years, 1 month ago
Centralised policy > Topology https://www.networkacademy.io/ccie-enterprise/sdwan/lab2-allowing-hub-to-spoke-routingWhy should it be "Centralized Policy > Topology"? "Centralized Policy > Traffic Policy" is also a valid option in vManage.
upvoted 3 times

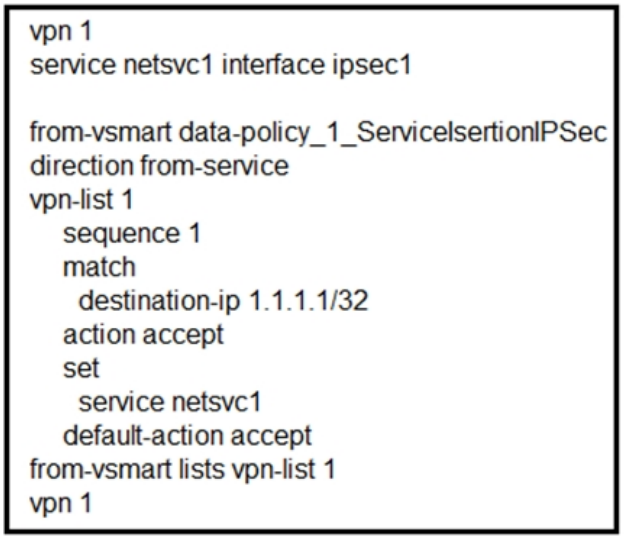
Speirsington 4 years, 1 month ago
Centralised policy > Topology

https://www.networkacademy.io/ccie-enterprise/sdwan/lab2-allowing-hub-to-spoke-routing
upvoted 3 times

JTPRO 4 years, 1 month ago
Why should it be "Centralized Policy > Topology"? "Centralized Policy > Traffic Policy" is also a valid option in vManage.
upvoted 2 times

Question #123 *Topic 1*

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



```
vpn 1
service netsvc1 interface ipsec1

from-vsmart data-policy_1_ServiceIsertionIPSec
direction from-service
vpn-list 1
    sequence 1
    match
      destination-ip 1.1.1.1/32
    action accept
    set
      service netsvc1
    default-action accept
from-vsmart lists vpn-list 1
vpn 1
```

A. service netsvc1 vpn1

B. service netsvc1 address 1.1.1.1

C. service FW address 1.1.1.1

D. service local

Suggested Answer: *A*

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

Community vote distribution

B (100%)

she_ccie Highly Voted 3 years, 5 months ago

Half the battle is understanding the layout of this question. The question they are asking is "what is the next line in the config after the VPN1 configuration command at the bottom of the snippet" "From-vSmart" means configure this on vSmart. Service insertion requires configs on several devices. A service config needs to go on the edge router to advertise the service. The second config is done on the vSmart controller. Baio's doc is a good reference to learn the order of operation.Baio's doc ?

upvoted 9 times

she_ccie Highly Voted 3 years, 5 months ago

Half the battle is understanding the layout of this question. The question they are asking is "what is the next line in the config after the VPN1 configuration command at the bottom of the snippet" "From-vSmart" means configure this on vSmart. Service insertion requires configs on several devices. A service config needs to go on the edge router to advertise the service. The second config is done on the vSmart controller. Baio's doc is a good reference to learn the order of operation.

upvoted 9 times

Aldebeer Most Recent 1 year, 8 months ago

Baio's doc ?

upvoted 1 times

Baio 3 years, 5 months ago

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/07Policy_Applications/02Service_Chaining/Service_Chaining_Configuration_Examples

upvoted 5 times

kentkyye 3 years, 7 months ago

For me it shud go to either service fw address 1.1.1.1 or service netsvc1 address 1.1.1.1 Here is the configuration procedure: Configure the firewall service on Hub-1. With this configuration, OMP on the Hub-1 router advertises a 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. vpn 10 service fw address 1.1.1.1The is not fw configuration on the policy the correct answer should be B, it would be C if they were using fw but they are using netsvcAgreed I go for B - https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=476 vpn 10 service netsvc1 address 2.2.2.2Just to add service netsvc1 VPN1 isn't valid vEdge1(config-vpn-1)# service netsvc1 vpn1 ----------^ syntax error: expecting address - IPv4 address interface - Interface tracker - Enable tracker for this Service

upvoted 1 times

kentkyye 3 years, 7 months ago

For me it shud go to either service fw address 1.1.1.1 or service netsvc1 address 1.1.1.1 Here is the configuration procedure: Configure the firewall service on Hub-1. With this configuration, OMP on the Hub-1 router advertises a 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.

vpn 10 service fw address 1.1.1.1

upvoted 1 times

MiraGod 2 years, 11 months ago

The is not fw configuration on the policy the correct answer should be B, it would be C if they were using fw but they are using netsvc

upvoted 1 times

Speirsington 3 years, 7 months ago

Agreed I go for B - https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=476

vpn 10 service netsvc1 address 2.2.2.2

upvoted 3 times

Speirsington 3 years, 7 months ago

Agreed I go for B - https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=476 vpn 10 service netsvc1 address 2.2.2.2Just to add service netsvc1 VPN1 isn't valid vEdge1(config-vpn-1)# service netsvc1 vpn1 ----------^ syntax error: expecting address - IPv4 address interface - Interface tracker - Enable tracker for this Service

upvoted 3 times

Speirsington 3 years, 7 months ago

Just to add service netsvc1 VPN1 isn't valid vEdge1(config-vpn-1)# service netsvc1 vpn1 ----------^ syntax error: expecting address - IPv4 address interface - Interface tracker - Enable tracker for this Service

upvoted 3 times

Question #124 *Topic 1*

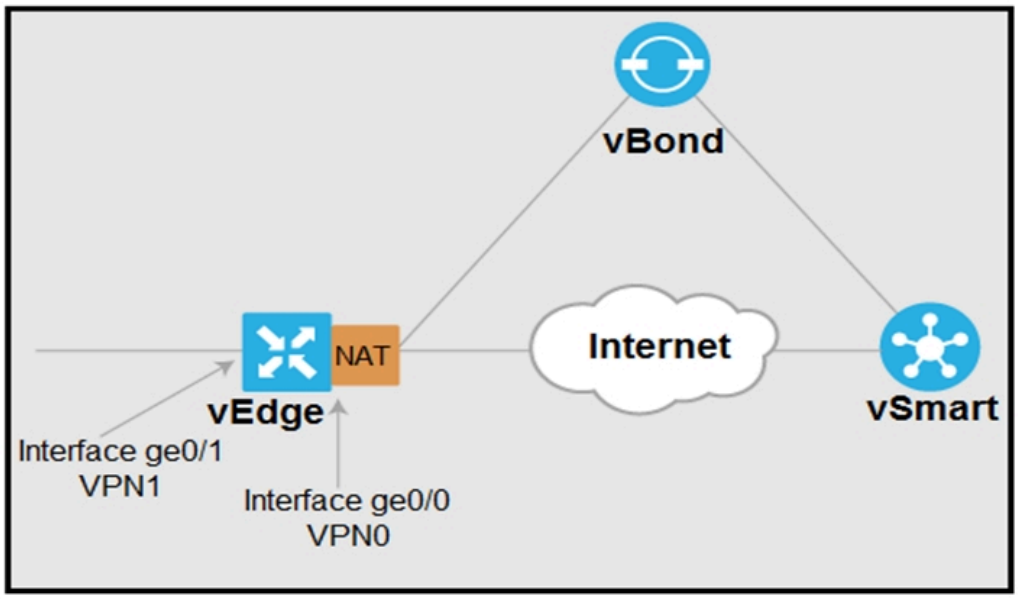
Refer to the exhibit. Which configuration sets up direct Internet access for VPN 1?

A.

B.

C.

D.




```
vpn 1
 ...
 interface ge0/0
   nat
 !
 no shutdown
...
vpn 0
 ....
 ip route 0.0.0.0/0 vpn 1
```

```
vpn 0
   .....
   interface ge0/0
        nat
  !
   no shutdown
...
vpn 1
   ...
    ip route 0.0.0.0/0 vpn 0
```

```
vpn 1
   .....
   interface ge0/1
    ...
     nat
  !
   no shutdown
...
vpn 0
   ...
    ip route 0.0.0.0/0 vpn 1
```

```
vpn 0
   …..
   interface ge0/1
    …
    ip nat
   !
   no shutdown
…
vpn 1
   …
    ip route 0.0.0.0/0 vpn 0
```

Suggested Answer:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/vEdge-as-NAT-device.html

NetArch_Teck Highly Voted 3 years, 1 month ago
Which configuration sets ip direct internet access for VPN-1 This is a straight forward question VPN 0 - [WAN Transport for TLOCs] interface ge0/0 - [Interface associated with VPN 0] nat - [Network Address Translation defined] no shutdown - [Administratively in a up state] VPN 1 - [VPN-1 is defined for DIA] ip route 0.0.0.0/vpn 0 - [Default route to WAN VPN 0] OPTION B Fulfils the request!
upvoted 8 times

thomazmr Highly Voted 2 years, 6 months ago
B is correct
upvoted 5 times

Rosh8787 Most Recent 1 year, 10 months ago
B is the correct answer
upvoted 3 times

Loi2525 2 years ago
B ofcourse!
upvoted 2 times

agkyawsoe 3 years, 6 months ago
It's definitely B.
upvoted 2 times

AW57 3 years, 8 months ago
B should correct
upvoted 4 times

AW57 3 years, 8 months ago
B should be correct
upvoted 2 times

Idro 3 years, 9 months ago
It should be B
upvoted 2 times

kcobain87 3 years, 9 months ago
B is correct
upvoted 2 times

ChrisCCNA 3 years, 11 months ago
B is correct
upvoted 2 times

MiraGod 3 years, 11 months ago
Correct answer should be B? The C is configuring the NAT on the VPN 1 and is sending the traffic from vpn 0 to 1, that is backwards
upvoted 1 times

Question #125 *Topic 1*

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?

A.

```
policy
control-policy Route_Leaking
  sequence 1
  match route
    vpn-list VPN_73
    prefix-list_AnyIpv4PrefixList
    action accept
    export-to-vpn-list VPN_50
  sequence 11
    match route
    vpn-list VPN_50
    prefix-list_AnyIpv4PrefixList
  action accept
    export-to vpn-list VPN_73
  default-action accept
```

B.

```
policy
control-policy Route_Leaking
  sequence 1
  match route
    VPN_50 VPN_73
    prefix-list_AnyIpv4PrefixList
    action accept
    export-to VPN_73 VPN_50
```

C.

```
policy
control-policy Route_Leaking
  sequence 1
  match route
    VPN_ALL
    prefix-list_AnyIpv4PrefixList
    action accept
    export-to VPN_ALL
```

D.

```
policy
control-policy Route_Leaking
  sequence 1
  match route
    VPN_73
    prefix-list_AnyIpv4PrefixList
    export-to VPN_50
  sequence 11
  match route
    VPN_50
    prefix-list_AnyIpv4PrefixList
    export-to VPN_73
default-action accept
```

Suggested Answer:
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/latam/docs/2018/pdf/BRKCRS-2186.pdf

PureInertiaCopy Most Recent 1 year, 11 months ago

You can't match vpn-lists with the syntax "match VPN_73" & or "match VPN_50". You MUST specify "vpn-list" before specifying the vpn-list {NAME} (e.g. vpn-list VPN_75) So the correct syntax is match route vpn-list VPN_75 (and or) vpn-list VPN_50 So B and D can't be correct. C is incorrect because it looks like it's selecting ALL VPNs.

upvoted 3 times

soltani 2 years, 1 month ago

D is incorrect because there is a syntax missing in VPN_73 under match route i think A is correct

upvoted 3 times

Damlouf 2 years, 6 months ago

B is the correct answer. A and C are incorrect due to wrong syntax of export-to. D is incrorrect too because the "action accept" is missing between the criteria and the actionB has ridiculous made-up syntax. A as the correct syntax, except the first "export-to" command has an incorrect hyphen, but we can assume that is a typo, since no other answer comes close.

upvoted 1 times

Damlouf 2 years, 6 months ago

B is the correct answer. A and C are incorrect due to wrong syntax of export-to. D is incrorrect too because the "action accept" is missing between the criteria and the action

upvoted 1 times

timtgh 2 years, 5 months ago

B has ridiculous made-up syntax. A as the correct syntax, except the first "export-to" command has an incorrect hyphen, but we can assume that is a typo, since no other answer comes close.

upvoted 2 times

khanda 3 years, 6 months ago

Answer A is correct.

upvoted 1 times

ngabor 4 years, 1 month ago

export-to vpn-list is the right syntax

upvoted 4 times

Question #126 *Topic 1*

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 vBond orchestrator, select the configure --> policies screen, select the localized policy tab, and click add policy.

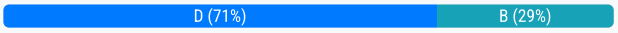
B. In vManage NMS, select the configure --> policies screen, select the localized policy tab, and click add policy.

C. In vSmart controller, select the configure --> policies screen, select the localized policy tab, and click add policy.

D. In vManage NMS, select the configure --> policies screen, select the centralized policy tab, and click add policy.

Suggested Answer: *B*
Official Answer: B

Community vote distribution



Faridtnx Most Recent 6 months ago
Since the requirement is to target a single device at a site with multiple devices, a localized policy is the only way to achieve that granular control.
upvoted 1 times

D3n1s 6 months, 2 weeks ago
localized data policy --> security, QoS, acl and manipulate service protocols.... Nothing related with the question
upvoted 1 times

Rachant 1 year, 1 month ago
Agree with Myare
upvoted 1 times

Myare 1 year, 4 months ago
Centralized data policies are configured through the Cisco vManage policy wizard. It guides you through four sequential screens that define different parts of the policy construct: Create Groups of Interest — At this step, we create lists of interesting items that will later be called in the match or action statements in the policy. Configure Traffic Rules — At this point, we specify the match and action conditions. Apply Policies to Sites and VPNs — At this step, we associate the policy with a site list and VPNs.
upvoted 3 times

AJMD 1 year, 11 months ago
Correct
upvoted 1 times

Jervv 2 years, 5 months ago
Given answer is correct "for a single WAN Edge device on a site with multiple WAN Edge devices."
upvoted 4 times

Diegooo 2 years, 6 months ago
Centralized polycy= B
upvoted 1 times

Diegooo 2 years, 6 months ago
Centralized polycy= BTypo, centralized policy =D
upvoted 1 times

Diegooo 2 years, 6 months ago
Typo, centralized policy =D
upvoted 2 times

Question #127 *Topic 1*

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 fulfills this requirement?

A.

```
policy
 data-policy _TE
  vpn-list VPN_10
   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
 !
  tloc-list Hub_TLOCs
  tloc 10.4.4.4 color mpls encap ipsec preference 300
  tloc 10.4.4.4 color public-internet encap ipsec preference 600
```

B.

```
policy
 data-policy _TE
  vpn-list VPN_10
   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
```

C.

```
policy
 data-policy _TE
  vpn-list VPN_10
   sequence 1
    match
     source-data-prefix-list Source_Prefix
     destination-data-prefix-list Dest_Prefix
    action accept
     set
      vpn 512
     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 _TE
  vpn-list VPN_10
   sequence 1
    match
     source-data-prefix-list Source_Prefix
     destination-data-prefix-list Dest_Prefix
    action reject
     set
      vpn 10
      tloc-list Hub_TLOCs
  default-action accept
!
 tloc-list Hub_TLOCs
 tloc 10.4.4.4 color mpls encap ipsec preference 300
 tloc 10.4.4.4 color public-internet encap ipsec preference 600
```

Suggested Answer:
Official Answer: A

wcorrea Highly Voted 3 years, 9 months ago
I think B is correct. Higher TLOC preference is chose. C is incorrect since this use VPN 512 (management) TLOC Preference. Prefer route with highest TLOC preference. https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/TECRST-2191.pdf pag.42
upvoted 23 times

Aldebeer 2 years, 9 months ago
I am quit agree with B!
upvoted 2 times

NetArch_Teck 3 years, 1 month ago
Option D fulfils the request! The configuration should not include the management VLAN 512. (This VLAN is designated to backhaul traffic via the controllers using DLTS/TLS traffic) The default action should be to accept Consequently this eliminates Options A and C to from the answer. Leaving B and D as options. The question requires that TLOC MPLS to be preferred and public internet as backup The preference with the lowest value is chosen within a tloc-list. To associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book.pdf {Page 288}Answer A, due to the fallback requirementFor each TLOC, specify its address, color, and encapsulation. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the highest preference value is used. If two or more of TLOCs have the highest preference value, traffic is sent among them in an ECMP fashion.
upvoted 2 times

NetArch_Teck 3 years, 1 month ago
Option D fulfils the request!

The configuration should not include the management VLAN 512. (This VLAN is designated to backhaul traffic via the controllers using DLTS/TLS traffic) The default action should be to accept

Consequently this eliminates Options A and C to from the answer. Leaving B and D as options.

The question requires that TLOC MPLS to be preferred and public internet as backup The preference with the lowest value is chosen within a tloc-list.

To associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book.pdf {Page 288}
upvoted 2 times

colipto 3 years ago
Answer A, due to the fallback requirement
upvoted 1 times

mohammad 1 year, 11 months ago

For each TLOC, specify its address, color, and encapsulation. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the highest preference value is used. If two or more of TLOCs have the highest preference value, traffic is sent among them in an ECMP fashion.

upvoted 1 times

agkyawsoe 3 years, 6 months ago

It's B.Admin Vlan is not Management and I think Management VPN (VPN512) doesn't pass on WAN link.

upvoted 2 times

Jonycici 3 years, 8 months ago

Correct answer is B. Higher TLOC preference is chosen, also VLAN should be 10 and not 512.

upvoted 4 times

Roger95 3 years, 9 months ago

as ChrisCCNA's explanation, Admin Vlan = VPN 512. C is correct

upvoted 2 times

Roger95 3 years, 9 months ago

as ChrisCCNA's explanation, Admin Vlan = VPN 512. C is correctwho said to associate admin vlan to management vlan lol

upvoted 2 times

Jervv 3 years, 5 months ago

who said to associate admin vlan to management vlan lol

upvoted 3 times

ChrisCCNA 3 years, 11 months ago

This question has been bugging me for days. I just passed the exam an hour ago and this question was on it. Here's the issue, the given answers here are incorrect I believe its a typo because on the exam the answer was obvious. So here's the correct details to look for: Mpls must have the lower priority. TLOC prefers lower. Action must equal accept in order to 'set' the tloc list Don't choose the one with NAT fallback or VPN 512 The default action is irrelevant Answer D I believe is the correct intended answer however I presume "action reject" is a typo. Action Accept is required.Even though, you assume "action accept", but in TLOC list: MPLS preference is 300 and internet is 600, so internet is preferred. D is not corect.B meets all the requirements, including action accept. D has action reject but also has wrong preference. Higher is better. Not sure why you said TLOC prefers lower. See Table 4 on this page: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/policy-overview.html

upvoted 2 times

ChrisCCNA 3 years, 11 months ago

This question has been bugging me for days. I just passed the exam an hour ago and this question was on it. Here's the issue, the given answers here are incorrect I believe its a typo because on the exam the answer was obvious. So here's the correct details to look for: Mpls must have the lower priority. TLOC prefers lower. Action must equal accept in order to 'set' the tloc list Don't choose the one with NAT fallback or VPN 512 The default action is irrelevant

Answer D I believe is the correct intended answer however I presume "action reject" is a typo. Action Accept is required.

upvoted 2 times

luctieuphung 3 years, 7 months ago

Even though, you assume "action accept", but in TLOC list: MPLS preference is 300 and internet is 600, so internet is preferred. D is not corect.

upvoted 1 times

timtgh 2 years, 11 months ago

B meets all the requirements, including action accept. D has action reject but also has wrong preference. Higher is better. Not sure why you said TLOC prefers lower. See Table 4 on this page: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/policy-overview.html

upvoted 3 times

ChrisCCNA 3 years, 11 months ago

I think this is C. MPLS needs to have a higher preference so that eliminates A and D. Admin traffic hints at VPN 512. There's information about Traffic Engineering in the SDWAN configuration guide 18.4 page 301.

upvoted 1 times

ChrisCCNA 3 years, 11 months ago

I think this is C. MPLS needs to have a higher preference so that eliminates A and D. Admin traffic hints at VPN 512. There's information about Traffic Engineering in the SDWAN configuration guide 18.4 page 301.Disregard my comment. TLOC preference prefers the lowest value. You cannot include VPN 512 in a data policy. Only "action accept" packets are eligible to be modified by extra parameters.TLOC preference prefers the highest value.

When a router has multiple available TLOCs (tunnel endpoints), it will choose the TLOC with the highest preference value to send traffic through. If multiple TLOCs share the same highest preference value, traffic is distributed equally among them using Equal-Cost Multi-Path (ECMP)

upvoted 1 times

ChrisCCNA 3 years, 11 months ago

Disregard my comment. TLOC preference prefers the lowest value. You cannot include VPN 512 in a data policy. Only "action accept" packets are eligible to be modified by extra parameters.

upvoted 1 times

ChrisCCNA 3 years, 11 months ago

Disregard my comment. TLOC preference prefers the lowest value. You cannot include VPN 512 in a data policy. Only "action accept" packets are eligible to be modified by extra parameters.TLOC preference prefers the highest value. When a router has multiple available TLOCs (tunnel endpoints), it will choose the TLOC with the highest preference value to send traffic through. If multiple TLOCs share the same highest preference value, traffic is distributed equally among them using Equal-Cost Multi-Path (ECMP)

upvoted 1 times

Rbrahmi Most Recent 9 months ago

TLOC preference prefers the highest value. When a router has multiple available TLOCs (tunnel endpoints), it will choose the TLOC with the highest preference value to send traffic through. If multiple TLOCs share the same highest preference value, traffic is distributed equally among them using Equal-Cost Multi-Path (ECMP)

upvoted 1 times

Question #128 *Topic 1*

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

A. app route policy on vSmart

B. data policy on vSmart

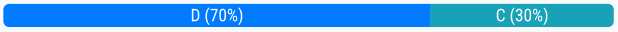
C. control policy on vSmart

D. control policy on vManage

Suggested Answer: *C*

Official Answer: C

Community vote distribution



Alchobashko Highly Voted 3 years, 6 months ago

No policy config on vSmart. Policies are configured on vManage!vManage has the user interface and accepts the config, but pushes it to vSmart. Therefore the policy is in the vSmart configuration, and surely that is what the question refers to, or the answer to everything would always be vManage, the GUI where everything is configured.Actually it could go either way, depending on how they mean their wording. They could be referring to the admin using vManage as the config GUI, or they could mean using a policy which resides on vSmart.

upvoted 8 times

Alchobashko Highly Voted 3 years, 6 months ago

Selected Answer: D

No policy config on vSmart. Policies are configured on vManage!

upvoted 8 times

timtgh 2 years, 11 months ago

vManage has the user interface and accepts the config, but pushes it to vSmart. Therefore the policy is in the vSmart configuration, and surely that is what the question refers to, or the answer to everything would always be vManage, the GUI where everything is configured.Actually it could go either way, depending on how they mean their wording. They could be referring to the admin using vManage as the config GUI, or they could mean using a policy which resides on vSmart.

upvoted 1 times

timtgh 2 years, 11 months ago

vManage has the user interface and accepts the config, but pushes it to vSmart. Therefore the policy is in the vSmart configuration, and surely that is what the question refers to, or the answer to everything would always be vManage, the GUI where everything is configured.

upvoted 1 times

timtgh 2 years, 11 months ago

Actually it could go either way, depending on how they mean their wording. They could be referring to the admin using vManage as the config GUI, or they could mean using a policy which resides on vSmart.

upvoted 1 times

ChrisCCNA 3 years, 11 months ago

Kind of an awkward question since you can create the centralized control policy on vmanage or vsmart. I still think the correct answer is vsmart since its a centralized control policy being created.Vsmat enforce policies (make it happened, send ot to the edges) the vmanage is the one creating policies, is the one with the data base, and send it to vsmart for the further distrubution to the right devices

upvoted 5 times

ChrisCCNA 3 years, 11 months ago

Selected Answer: C

Kind of an awkward question since you can create the centralized control policy on vmanage or vsmart. I still think the correct answer is vsmart since its a centralized control policy being created.

upvoted 5 times

Diegooo 3 years, 6 months ago

Vsmat enforce policies (make it happened, send ot to the edges) the vmanage is the one creating policies, is the one with the data base, and send it to vsmart for the further distrubution to the right devices

upvoted 4 times

msstanick Most Recent 7 months, 1 week ago

This is so so so stupid and cisco style... It is obvious policies are only created on vManage while then pushed to vSmart and enforced to c/vEdges, but the the question is where the policy gets created - and this is vManage. This not a matter of knowledge but good anticipation of what the question author had in mind :/

upvoted 1 times

uzbin 1 year, 4 months ago

Q is what does the Admin use... He uses vManage to create the policy.

upvoted 2 times

mohammad 1 year, 11 months ago

All configuration is via vmanage but the question is about where the policy exists. So first you need to understand which pilocy should be used to have regional hub topology which is Centralized Policy and it is on vsmart. In case of Localized Policy , it is done through template or CLI which mostly vmanage is responsible. Centralized Policy The centralized control policy configuration itself remains on the Cisco SD-WAN Controller and is never pushed to local devices. Localized Policy Localized policy refers to a policy that is provisioned locally through the CLI on the Cisco IOS XE Catalyst SD-WAN devices, or through a Cisco SD-WAN Manager device template.

upvoted 1 times

Mykhey 2 years, 3 months ago

I think the key word is 'USE', answer should be vManage

upvoted 1 times

bullett00th 2 years, 9 months ago

I'll go wih D. You do the configuration on the vManage which then pushes it to vSmart

upvoted 2 times

M_Ryu 2 years, 11 months ago

I think the answer is C. Source (you can also go to the section on control polices and it's all about vSmart too: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/policy-basics-CLIs.htmlAlso you can google: "where do you create hub and spoke topology cisco sdwan" and the PDF document "Cisco SD-WAN Policy Guide Hub & Spoke Topology" will come up where it says "Management plane (vManage): Responsible for central configuration and monitoring. Control plane (vSmart): Builds and maintains the network topology and makes decisions on where traffic flows."Exactly, the question is "what does the network administrator use to create a regional hub topology?" and here is your answer vManage is responsible for central Configuration D is correct answer

upvoted 2 times

M_Ryu 2 years, 11 months ago

I think the answer is C. Source (you can also go to the section on control polices and it's all about vSmart too: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/policy-basics-CLIs.html

upvoted 2 times

M_Ryu 2 years, 11 months ago

Also you can google: "where do you create hub and spoke topology cisco sdwan" and the PDF document "Cisco SD-WAN Policy Guide Hub & Spoke Topology" will come up where it says "Management plane (vManage): Responsible for central configuration and monitoring.

Control plane (vSmart): Builds and maintains the network topology and makes decisions on where traffic flows."

upvoted 1 times

M_Ryu 2 years, 11 months ago

Also you can google: "where do you create hub and spoke topology cisco sdwan" and the PDF document "Cisco SD-WAN Policy Guide Hub & Spoke Topology" will come up where it says "Management plane (vManage): Responsible for central configuration and monitoring. Control plane (vSmart): Builds and maintains the network topology and makes decisions on where traffic flows."Exactly, the question is "what does the network administrator use to create a regional hub topology?" and here is your answer vManage is responsible for central Configuration D is correct answer

upvoted 1 times

RafaJohnston76 2 years, 6 months ago

Exactly, the question is "what does the network administrator use to create a regional hub topology?" and here is your answer vManage is responsible for central Configuration D is correct answer

upvoted 2 times

LP92 3 years ago

C. Control Policy on vSmart , also verified on many other websites

upvoted 1 times

hamidreza0010 3 years, 1 month ago

D is the correct answer

upvoted 3 times

OstravaT2guy 3 years, 3 months ago

The key word here is "USE". We as engineers dont use control policy on vSmart. We can only use vManage to control policies. vManage can then push said policies to vSmart.

upvoted 2 times

theleftfoot 3 years, 6 months ago

take a look --> https://swat-sdwanlab.github.io/mydoc_regional_hub.html

upvoted 3 times

timbo2000 3 years, 7 months ago

COnfiguration done on vmanage Mesh In the Add Topology drop-down, select Mesh. Enter a name for the mesh region policy component. Enter a description for the mesh region policy component. In the VPN List field, select the VPN list for the policy. Click New Mesh Region. In the Mesh Region Name field, enter a name for the individual mesh region. In the Site List field, select one or more sites to include in the mesh region. Click Add. Repeat these steps to add more mesh regions to the policy. Click Save Mesh Topology.

upvoted 1 times

network_nick 3 years, 7 months ago

Centralized policies are configured on vManage and pushed down to vSmart. A centralized control (topology) policy would achieve this, and since the question asks what the admin would use to create the topology, it should be D.

upvoted 2 times

Jonycici 3 years, 8 months ago

policies are confirgured on vsmart

upvoted 1 times

Jevza 3 years, 9 months ago

Correct Answer should be D, vManage send it it to vSmart

upvoted 2 times

Question #129 *Topic 1*

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

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

Community vote distribution
A (100%)

Aldebeer Most Recent 1 year, 9 months ago
By default is 8
upvoted 1 times

imarin 2 years, 1 month ago
"For Cisco vEdge devices, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for control traffic, and queues 1, 2, 3, 4, 5, 6 and 7 are available for data traffic. The scheduling method for all eight queues is WRR. LLQ is not supported."
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/localized-policy.html#:~:text=The%20default%20scheduling%20method%20for,all%20eight%20queues%20is%20WRR.
upvoted 1 times

kentkyye 3 years, 7 months ago
answer is A. For hardware vEdge routers, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for low-latency queuing(LLQ), so any class that is mapped to queue 0 must be configured to use LLQ. The default scheduling method for all is weighted roundrobin (WRR).The question says cloud router, which is not a hardware router. Possibly a typo, since it says eight queues.
upvoted 4 times

kentkyye 3 years, 7 months ago
answer is A. For hardware vEdge routers, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for low-latency queuing(LLQ), so any class that is mapped to queue 0 must be configured to use LLQ. The default scheduling method for all is weighted roundrobin (WRR).
upvoted 4 times

timtgh 1 year, 11 months ago
The question says cloud router, which is not a hardware router. Possibly a typo, since it says eight queues.
upvoted 1 times

serieus 4 years ago
a Cloud vEdge only ha 4 queues to begin with. Besides that queue 0 is always configured as LLQ, while the remaining ones are WRRIn vEdges as you mentioned are only 4 queues but keep in mind that vEdges dont support LLQ, only the cEdges with their 8 queues.Still, virtual images do not have 8 queues whether they are cisco or viptela
upvoted 4 times

serieus 4 years ago
a Cloud vEdge only ha 4 queues to begin with. Besides that queue 0 is always configured as LLQ, while the remaining ones are WRR
upvoted 4 times

MiraGod 2 years, 11 months ago
In vEdges as you mentioned are only 4 queues but keep in mind that vEdges dont support LLQ, only the cEdges with their 8 queues.Still, virtual images do not have 8 queues whether they are cisco or viptela
upvoted 1 times

MiraGod 2 years, 11 months ago
In vEdges as you mentioned are only 4 queues but keep in mind that vEdges dont support LLQ, only the cEdges with their 8 queues.

upvoted 1 times

MerlinTheWizard 2 years, 2 months ago

Still, virtual images do not have 8 queues whether they are cisco or viptela

upvoted 1 times

Question #130 *Topic 1*

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

A. 3

B. 5

C. 2

D. 7

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Horsefeathers Most Recent 11 months, 4 weeks ago

The application layer in the OSI model is layer 7.

upvoted 1 times

Roger95 1 year, 9 months ago

Application Firewall The Application Firewall blocks traffic based on applications or application-family. This application-aware firewall feature provides the following benefits: Application visibility and granular control Classification of 1400+ layer 7 applications Blocks traffic by application or application-family

upvoted 1 times

she_ccie 2 years, 5 months ago

You can create lists of individual applications or application families. A sequence that contains a specified application or application family list can be inspected. This inspect action is a Layer 4 action. Matching applications are blocked/denied. - If a match condition contains an Application or Application Family List, the action must be Inspect. This inspect action is a Layer 4 action. The action for a specific application is block/deny. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/enterprise-firewall.html

upvoted 3 times

Question #131 *Topic 1*

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

Suggested Answer: *C*

Reference: 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

Community vote distribution

C (100%)

ChrisCCNA Most Recent 2 years ago

C is correct

upvoted 1 times

Question #132 *Topic 1*

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

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

Almanac Highly Voted 4 years, 10 months ago

correct answer is C. TCP will be allower sourcing from 172.16.10.0. Letter A. TCP allowed from 172.16.20 so Letter A is wrong

upvoted 5 times

Almanac 4 years, 10 months ago

correct answer is C. TCP will be allower sourcing from 172.16.10.0. Letter A. TCP allowed from 172.16.20 so Letter A is wrongLetter A is wrong because TCP is dropped with a correct source and destination

upvoted 5 times

Almanac 4 years, 10 months ago

Letter A is wrong because TCP is dropped with a correct source and destination

upvoted 2 times

Knowledge33 Most Recent 2 years ago

C is correct. Be careful, It's a negative question.

upvoted 4 times

Zahid111 3 years, 4 months ago

First of all it can be A or C based on the prefix pair (172.16.10.x to 172.16.20.x). However there is another condition match which is protocol 6 (tcp). So, the TCP traffic will not drop bus pass. UDP traffic will drop. Hence C is correct answer.

upvoted 2 times

ChrisCCNA 3 years, 6 months ago

UDP will be dropped by default action.

upvoted 2 times

carlovalle 3 years, 6 months ago

Maybe there is missing information in the question.

upvoted 1 times

khanda 3 years, 6 months ago

C is correct. Protocol 6 being TCP will be allowed, so any other traffic will be dropped, UDP traffic in this case.

upvoted 1 times

she_ccie 3 years, 12 months ago

TCP Port 20 is FTP. FTP traffic is policed and if exceeds the rate it is dropped. The accept function means to police the FTP traffic and only the policer will drop the traffic. The default action is for all other traffic.@she_ccie, As per your comment, Answer should be --> A TCP packet sourcing from 172.16.10.1 and destined to 172.16.20.1 is Accepted and after policer if it exceeds the value, it should drop. But this option is not present in given answers right ?As there is default-action drop, out of 4 options Answer C matches and is Correct

upvoted 1 times

she_ccie 3 years, 12 months ago

TCP Port 20 is FTP. FTP traffic is policed and if exceeds the rate it is dropped. The accept function means to police the FTP traffic and only the policer will drop the traffic. The default action is for all other traffic.

upvoted 1 times

Nalla123 3 years, 5 months ago

@she_ccie, As per your comment, Answer should be --> A TCP packet sourcing from 172.16.10.1 and destined to 172.16.20.1 is Accepted and after policer if it exceeds the value, it should drop. But this option is not present in given answers right ?

upvoted 1 times

Nalla123 3 years, 5 months ago

@she_ccie, As per your comment, Answer should be --> A TCP packet sourcing from 172.16.10.1 and destined to 172.16.20.1 is Accepted and after policer if it exceeds the value, it should drop. But this option is not present in given answers right ?As there is default-action drop, out of 4 options Answer C matches and is Correct

upvoted 1 times

Nalla123 3 years, 5 months ago

As there is default-action drop, out of 4 options Answer C matches and is Correct

upvoted 1 times

juniper 4 years ago

It is C

upvoted 2 times

juniper 4 years ago

Correct Answer : C

upvoted 2 times

Speirsington 4 years, 1 month ago

A UDP packet sourcing from 172.16.10.1 and destined to 172.16.20.1 is dropped Protocol 6 is TCP as you can see here:
https://www.cisco.com/c/en/us/td/docs/cable/serv_exch/serv_control/broadband_app/protocol_ref_guide/protocol_ref_guide/03_IP.pdf

upvoted 2 times

tester2478 4 years, 5 months ago

sould be C because TCP traffic is allowed from 10.x to 20.x

upvoted 3 times

go_Corona_go 4 years, 9 months ago

correct answer C

upvoted 4 times

ZeroBits 4 years, 10 months ago

Protocol 6 is TCP. A is correct

upvoted 3 times

ZeroBits 4 years, 10 months ago

Protocol 6 is TCP. A is correctnvm default-action drop. Means only tcp would be allowed and udp will be dropped. answer is correct

upvoted 3 times

ZeroBits Highly Voted 4 years, 10 months ago

nvm default-action drop. Means only tcp would be allowed and udp will be dropped. answer is correct

upvoted 6 times

Question #133 *Topic 1*

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
```

Suggested Answer:
Official Answer: B

daniccs8 Highly Voted 4 years, 4 months ago
Correct answer D. Apply a policer with exceed remark. PLP High or Low is just for matching
upvoted 14 times

Decorations Most Recent 3 months, 2 weeks ago
These questions aren't from blueprint.
upvoted 1 times

uzbin 1 year, 4 months ago
D is correct. Only C & D are options in the CLI.
upvoted 1 times

nbvolz 1 year, 11 months ago
Answer: D in the case of PLP..https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/localized-policy.html
upvoted 2 times

AJMD 1 year, 11 months ago
Correct D
upvoted 1 times

Speirsington 3 years, 7 months ago
"exceed is the action to take when the burst size or traffic rate is exceeded. action can be drop (the default) or remark. The drop action is equivalent to setting the packet loss priority (PLP) bit to low. The remark action sets the PLP bit to high" 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

upvoted 3 times

CesarVergaraGalindo 3 years, 10 months ago

D is correct

upvoted 1 times

TheNetworkStudent 4 years ago

Basic QoS knowledge, not sure what PLP is set as correct, should indeed be remark. D is correct.

upvoted 1 times

Rayan1122 4 years ago

yes, the correct answer is remark

upvoted 1 times

isaacmejia 4 years, 1 month ago

correct answer D, Specify the packet loss priority (PLP) (high | low)By default, packets have a PLP value of low. To set the PLP value to high, apply a policer that includes the exceed remark option.

upvoted 2 times

Almanac 4 years, 4 months ago

the correct answer is D. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html

upvoted 2 times

Question #134 *Topic 1*

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

A. IPsec/GRE cloud proxy

B. reverse proxy

C. Enterprise Firewall with Application Awareness

D. Cloud Express service

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

Outlaw_87 Most Recent 2 years, 1 month ago

The Cisco 4451-X Integrated Services Router revolutionizes the delivery of application-aware services in a branchoffice environment. This new member of the Cisco ISR Family provide extensive Layer 7 services hosted internally to the branch office while maximizing operating expenses(OpEx) savings. The Cisco 4451-X offers encryption acceleration, voice- and video-capable architecture, application firewall, call processing, and embedded services. https://www.cisco.com/c/dam/global/en_vn/solutions/smb/velocity/Downloads/isr4400_datasheet.pdf

upvoted 1 times

Diegooo 3 years ago

ISR4000 series supports SDWAN with Security

upvoted 1 times

Question #135 *Topic 1*

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

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution

CD (100%)

Adedayo Highly Voted 4 years, 7 months ago

Should be Authentication headers and encapsulation security payload (CD) https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/01Security_Overview/Data_Plane_Security_Overview

upvoted 28 times

Barti1 Most Recent 1 year, 8 months ago

These are corrects: cd

upvoted 2 times

stayfoolish 1 year, 9 months ago

CD is correct

upvoted 1 times

hopatrickhk88 2 years, 1 month ago

Two mechanisms used to guarantee the integrity of data packets in the Cisco SD-WAN architecture data plane are encryption and authentication.

Answer should C and D

upvoted 1 times

MerlinTheWizard 2 years, 2 months ago

Without reading about this topic, I'd be lost.. encryption was always for confidentiality, not integrity

upvoted 2 times

Idro 2 years, 9 months ago

C and D

upvoted 1 times

kcobain87 2 years, 9 months ago

CD are the correct

upvoted 1 times

ChrisCCNA 2 years, 11 months ago

Correct answer is AH and ESP. Answer can be found in the SDWAN Config guide 18.4 page 189

upvoted 1 times

carlovalle 3 years ago

C and D They are protocols that provides, integrity, authentication and anti reply

upvoted 1 times

khanda 3 years ago

C and D

upvoted 1 times

aliciim 3 years ago

C, D is correct

upvoted 1 times

CesarVergaraGalindo 3 years, 10 months ago

C,D is Correct

upvoted 2 times

tester2478 3 years, 11 months ago

i think C and D are correct https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-4.pdf#page=242 beside TLOC (transport location) in son related with integrity

upvoted 2 times

vicopo 4 years, 1 month ago

A number of components contribute to the integrity of data packets in the Viptela data plane: • ESP, which is the standard IPsec encryption protocol, protects (via encryption and authentication) the inner header, data packet payload, and ESP trailer in all data packets. • AH, which is the standard IPsec authentication protocol, protects (via authentication) the entire data packet, including the inner and outer headers, data packet payload, and ESP trailer

upvoted 2 times

Question #136 *Topic 1*

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

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

hopatrickhk88 Most Recent 2 years, 1 month ago

The identity of the physical WAN Edge device is confirmed by verifying the **certificate serial number Source: Conversation with Bing, 7/9/2023 (1) Cisco SD-WAN: WAN Edge Onboarding Deployment Guide. https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf. (2) Cisco SD-WAN Certificates Explained | NetworkAcademy.io. https://www.networkacademy.io/ccie-enterprise/sdwan/cisco-sd-wan-certificates-explained.

upvoted 1 times

NetArch_Teck 2 years, 1 month ago

A WAN Edge is identified by the Chassis-ID & Certificate Serial Number. The question is specifically asking how a WAN device is identified in a certificate, the Answer would therefore be A

upvoted 1 times

ChrisCCNA 2 years, 11 months ago

A is correct

upvoted 3 times

Question #137 *Topic 1*

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

A. ZTP

B. OTPC

C. SUDI

D. TPMD

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

nihithp Highly Voted 4 years, 9 months ago

- Hardware-based vEdge device certificate is stored in the on-board Tamper Proof Module (TPM) chip installed during manufacturing. - Hardware-based Cisco IOS-XE SD-WAN device certificate is stored in the on-board SUDI chip installed during manufacturing. - Virtual platform or Cisco IOS-XE SD-WAN devices do not have root certificates (such as the ASR1002-X platform) preinstalled on the device. For these devices, a One-Time Password (OTP) is provided by vManage to authenticate the device with the SD-WAN controllers.

upvoted 19 times

nihithp Highly Voted 4 years, 9 months ago

- Hardware-based vEdge device certificate is stored in the on-board Tamper Proof Module (TPM) chip installed during manufacturing. - Hardware-based Cisco IOS-XE SD-WAN device certificate is stored in the on-board SUDI chip installed during manufacturing. - Virtual platform or Cisco IOS-XE SD-WAN devices do not have root certificates (such as the ASR1002-X platform) preinstalled on the device. For these devices, a One-Time Password (OTP) is provided by vManage to authenticate the device with the SD-WAN controllers.Great, thanks

upvoted 19 times

stepstranger 4 years, 8 months ago

Great, thanks

upvoted 2 times

DiskRoot16 Most Recent 1 year, 3 months ago

SUDI stands for Secure Unique Device Identifier, and it plays a key role in the authentication process for Cisco SD-WAN on ISR (Integrated Services Router) platforms.

upvoted 2 times

Rosh8787 1 year, 10 months ago

Option C is the correct answer

upvoted 1 times

Rcont 2 years, 1 month ago

the selected answer is correct. TPMD does not exist. it only exists TPM.

upvoted 1 times

sdwanlove 3 years, 4 months ago

Cisco SD-WAN: WAN Edge Onboarding Deployment Guide,p6. Hardware-based vEdge device certificate is stored in the on-board Tamper Proof Module (TPM) chip installed during manufacturing. - Hardware-based Cisco IOS-XE SD-WAN device certificate is stored in the on-board SUDI chip installed during manufacturing. - Virtual platform or Cisco IOS-XE SD-WAN devices do not have root certificates (such as the ASR1002-X platform) preinstalled on the device. For these devices, a One-Time Password (OTP) is provided by vManage to authenticate the device with the SD-WAN controllers Correct answer is C.

upvoted 2 times

Question #138 *Topic 1*

A network administrator is configuring QoS on a WAN Edge 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

B. Netflow

C. Application

D. Cloud QoS Service side

Suggested Answer: *A*
Reference: https://www.coursehero.com/file/p5ai4be5/There-are-a-few-steps-to-take-when-configuring-QoS-on-vEdge-router-hardware-1/

EGD Highly Voted 2 years, 1 month ago

From that link: For vEdge 5000 routers (and vEdge cloud routers), use the cloud-qos command to enable QoS scheduling and shaping for the transport-side tunnel interfaces. Use the cloud-qos-service-side command to enable QoS scheduling and shaping for the service-side interfaces. This is configured within the localized policy.

upvoted 12 times

Question #139 *Topic 1*

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

A. application visibility

B. control policy enforcement

C. application monitoring

D. application malware protection

Suggested Answer: *A*
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/ent-firewall-app-aware.html#:~:text=Application%20Firewall&text=This%20application%2Daware%20firewall%20feature,of%201400%2B%20layer%207%20applications

she_ccie Most Recent 1 year, 11 months ago
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/enterprise-firewall.html Application visibility and granular control Classification of 1400+ layer 7 applications Blocks traffic by application or application-family
upvoted 4 times

DBIa 2 years, 4 months ago
Correct. https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/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.xml
upvoted 3 times

Question #140 *Topic 1*

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

A. turn off ز€Enable TCP Optimizationز€

B. turn on ز€Enhance ECMP Keyingز€

C. turn on ز€Enable TCP Optimizationز€

D. turn off ز€Enhance ECMP Keyingز€

Suggested Answer: *C*
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/optimization-ha/ios-xe-16/network-optimization-high-availability-book-xe/m-tcp- optimization.html

NetArch_Teck Most Recent 2 years, 1 month ago

This is the only option would be for TCP optimization to occur to improve throughout across a link. C. turn on Enable TCP Optimization

upvoted 1 times

Question #141 *Topic 1*

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 data policy on WAN interface

B. Configure a control policy

C. Apply a QoS map policy

D. Configure NAT on the transport interface

E. Configure a centralized data policy

Suggested Answer: *A, E*

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

Community vote distribution

DE (63%) AD (21%) CD (16%)

vanoone1 Highly Voted 4 years, 3 months ago

nat on transport + centralize data policy

upvoted 14 times

Mr_Cipher Highly Voted 4 years, 1 month ago

Should be D & E. NAT for DIA + Centralised data policy for QoS config

upvoted 10 times

PepaZdepa33 Most Recent 2 years, 1 month ago

agree with network_nick answer should be D and E

upvoted 1 times

network_nick 2 years, 7 months ago

Must configure NAT on the transport interface for DIA to function (D) A centralized data policy can be used to match based on DSCP markings. Question specifies the DIA policy is based on matching QoS parameters, which is equivalent to matching on DSCP markings, accomplished via a centralized data policy (E).

upvoted 3 times

AW57 2 years, 8 months ago

D & E should be correct answers.

upvoted 2 times

Idro 2 years, 9 months ago

A- QOS Policy for this specific WAN Edge Router D- Nat for DIA

upvoted 4 times

kcobain87 2 years, 9 months ago

These are the correct ones

upvoted 2 times

khanda 3 years ago

D and E

upvoted 3 times

khanda 3 years ago

For QoS you would utilize "Localized" Data Policy so I believe option E is not an option for QoS config, but for DIA. You would also need NAT and qos-map on the egress transport interface so my choice is C and D.After reading this again, the Correct answer is D and E. Centralized Data Policy can be used to configure QoS.

upvoted 3 times

khanda 3 years ago

Selected Answer: CD

For QoS you would utilize "Localized" Data Policy so I believe option E is not an option for QoS config, but for DIA. You would also need NAT and qos-map on the egress transport interface so my choice is C and D.

upvoted 3 times

khanda 3 years ago

After reading this again, the Correct answer is D and E. Centralized Data Policy can be used to configure QoS.

upvoted 2 times

RREVECO 3 years, 2 months ago

ANSWER D & E ARE CORRECTS! https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2020aug.pdf PAGE 13

upvoted 3 times

gem 3 years, 4 months ago

I guess A&D is correct answer: - you are question to enable the policy on a specific router (not central) - NAT must be enabled on transport interface for DIA

upvoted 1 times

juniper 3 years, 6 months ago

Correct Answer : D/E

upvoted 1 times

EGD 3 years, 7 months ago

I think A & E From the reference: Centralized data policies are used in configuring application firewalls, service chaining,traffic engineering, and quality of service (QoS). These policies include ApplicationAware Routing to apply SLAs for applications and traffic steering as well as activating AppQoE features such as packet duplication.

upvoted 2 times

CesarVergaraGalindo 3 years, 10 months ago

C, E is correct

upvoted 1 times

Question #142 *Topic 1*

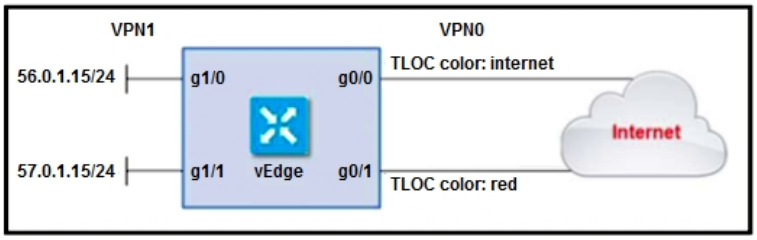
Refer to the exhibit. The ge0/0 interface connects to a 30-MB link. A network administrator wants to always have 10 MB available for high priority traffic. When lower-priority traffic bursts exceed 20 MB, traffic should be redirected to the second WAN interface ge0/1. Which set of configurations accomplishes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

A.

B.

C.

D.




```
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
```

```
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
```

```
policy
 policer bursty-traffic
  rate 10000
  burst 20000
  exceed drop
 access-list policer-bursty-traffic
  sequence 10
    match
      source-ip 56.0.1.0/24
    action accept
      policer bursty-traffic
    default-action accept
```

```
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
```

Suggested Answer:
Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_17.1/08Forwarding_and_QoS/03Forwarding_and_QoS_Configuration_Examples

ngabor Highly Voted 4 years, 1 month ago
C - check the number of zeroes
upvoted 6 times

NetArch_Teck 2 years, 7 months ago
The answer is [D} even though their are typo's everywhere, Policy rate is measured in bps (bits per second) Burst rate is measured in bytes. In order to achieve 10MB for the rate, the bps would need to be 10,000,000, not 1,000,000 This must be a type, however it is the closest answer out of the options. Answer [D] Cisco white paper:- https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/data-policies.html
upvoted 4 times

steph_lora66 2 years, 9 months ago
D is correct, same example if the followiung link: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/qos/vEdge-20-x/qos-book/forwarding-qos.htmlthe example on this link is exactly the question
upvoted 2 times

steph_lora66 2 years, 9 months ago
D is correct, same example if the followiung link: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/qos/vEdge-20-x/qos-book/forwarding-qos.html
upvoted 2 times

RafaJohnston76 Most Recent 2 years ago
the example on this link is exactly the question
upvoted 1 times

Jonycici 3 years, 2 months ago
C is wrong, it says 'exceed drop'
upvoted 3 times

Idro 3 years, 3 months ago
D is correct
upvoted 1 times

DP 4 years ago
D is the correct answer. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/qos/vEdge-20-x/qos-book/forwarding-qos.html
upvoted 2 times

Xhizors 4 years, 1 month ago
Wrong ngabor, rate are set in bps
upvoted 4 times

Xhizors 4 years, 1 month ago
Wrong ngabor, rate are set in bpsIn that case, none of the options are correct since D would be 1 MbpsI think someone just wrote wrong number of zeroes
upvoted 4 times

MerlinTheWizard 2 years, 8 months ago
In that case, none of the options are correct since D would be 1 Mbps

upvoted 2 times

MerlinTheWizard 2 years, 8 months ago

In that case, none of the options are correct since D would be 1 MbpsI think someone just wrote wrong number of zeroes

upvoted 2 times

Precission21 2 years, 7 months ago

I think someone just wrote wrong number of zeroes

upvoted 1 times

Question #143 *Topic 1*

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

```
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
```

A. 9

B. 9000

C. 90000

D. 9000000

Suggested Answer: *B*

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

Community vote distribution

B (100%)

EGD Highly Voted 2 years, 7 months ago

vpn vpn-id interface interface-name shaping-rate kbps

upvoted 5 times

khanda Most Recent 2 years ago

kilobits per second (kbps)

upvoted 1 times

RREVECO 2 years, 2 months ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#wp4217152133 Command Hierarchy vpn vpn-id interface interface-name shaping-rate kbps Syntax Description -> kbps Traffic Shaping Rate: Rate at which to transmit traffic, in kilobits per second (kbps).

upvoted 1 times

Question #144 *Topic 1*

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

Suggested Answer: *B*

Official Answer: B

Community vote distribution

C (100%)

nihithp Highly Voted 3 years, 9 months ago

C. Administration > Settings

upvoted 10 times

lollo1234 Highly Voted 3 years, 11 months ago

C. WAN Edge Cloud Certificate Authorization by default is Automated (vManage signed).

upvoted 7 times

bullett00th Most Recent 1 year, 8 months ago

C is correct See Screenshots under https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-controller-cert-deploy-guide.html

upvoted 1 times

jcms700 2 years, 1 month ago

C. Administrations > Settings

upvoted 1 times

Nandhujoe 2 years, 3 months ago

C. Administration > Settings

upvoted 1 times

kcobain87 2 years, 9 months ago

C is correct

upvoted 1 times

ChrisCCNA 2 years, 11 months ago

Admin Settings

upvoted 1 times

khanda 3 years ago

Administration > Settings

upvoted 1 times

majepiga 3 years, 3 months ago

I already did this, answer is C

upvoted 1 times

CesarVergaraGalindo 3 years, 10 months ago

C is Correct

upvoted 4 times

Question #145 *Topic 1*

Which two requirements must be met for DNS inspection when integrating with Cisco Umbrella? (Choose two.)

A. Attach security policy to the device template.

B. Create and attach a System feature template with the Umbrella registration credentials.

C. Register and configure the vManage public IP and serial number in the Umbrella portal.

D. Upload the WAN Edge serial allow list to the Umbrella portal.

E. Configure the Umbrella token on the vManage.

Suggested Answer: *A, E*

Official Answer: AE

Community vote distribution

AE (100%)

NetArch_Teck Most Recent 2 years, 1 month ago

You need to configure the Umbrella API Token as the 1st step, then attach a DNS Security Policy to the device in order to initiate integration from Cisco Umbrella! A & £ Attach Security Policy to device Template Configure the umbrella Token to VManage REF LINK https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/umbrella-integration.html#id_117963

upvoted 1 times

ChrisCCNA 2 years, 11 months ago

AE correct

upvoted 1 times

khanda 3 years ago

Correct Answer: AE

upvoted 1 times

Xhizors 3 years, 6 months ago

Correct

upvoted 4 times

Question #146 *Topic 1*

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

A. blocks traffic by application or application-family

B. numbered sequences of match-action pairs

C. classification of 1000+ layer 4 applications

D. application match parameters

E. classification of 1400+ layer 7 applications

Suggested Answer: *A, E*

Official Answer: AE

Community vote distribution

AE (100%)

Aldebeer Most Recent 1 year, 9 months ago

approved by the docs.

upvoted 1 times

Matt2727 1 year, 10 months ago

Evidence provided by Rita7

upvoted 1 times

Rita7 3 years, 1 month ago

This document describes how Zone Based FireWall policy is defined based on the applications that NBAR can detect and make Zone Based FireWall application aware. The Application FireWall inspects the traffic and blocks traffic based on applications, category, application-family or application-group. 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

upvoted 4 times

JTPRO 3 years, 7 months ago

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.pdf

upvoted 3 times

Question #147 *Topic 1*

The network administrator is configuring a QoS scheduling policy on traffic received from transport side tunnels on WAN Edge 5000 routers at location:405608122. Which command must be configured on these devices?

A. mls qos

B. cloud-qos

C. service qos

D. cloud-mls qos

Suggested Answer: *B*
Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/SD-WAN-End-to-End-Deployment-Guide.pdf page 153.

khanda 2 years, 6 months ago
The correct command would be: cloud-qosservice-side B is the closest to that, even though that's for transport sided.B is correct. And cloud-qos service-side is for service side, not for transport side
upvoted 2 times

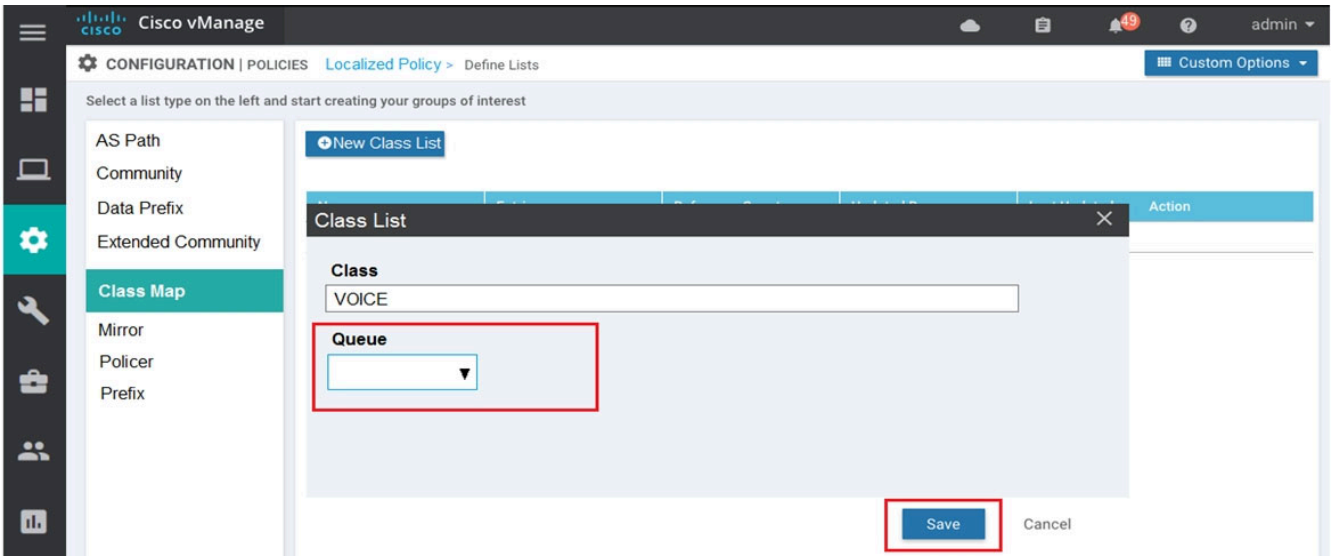
khanda 2 years, 6 months ago
The correct command would be: cloud-qosservice-side B is the closest to that, even though that's for transport sided.
upvoted 2 times

heavncong Most Recent 2 years, 1 month ago
B is correct. And cloud-qos service-side is for service side, not for transport side
upvoted 1 times

Rita7 2 years, 7 months ago
For vEdge cloud and vEdge 5000 routers, to enable QoS scheduling and shaping for the transport-side tunnel interfaces, you must use the cloud-qos command in the policy. In addition, to enable QoS scheduling and shaping for the service-side interfaces, you must use the cloud-qosservice-side command in the policy.
upvoted 3 times

Question #148 *Topic 1*

Refer to the exhibit. A network administrator is setting the queueing 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

Suggested Answer: *A*

Reference: https://www.cisco.com/c/en/us/support/docs/routers/vedge-router/213408-implement-qos-in-cisco-sd-wan.html

Community vote distribution

A (100%)

Knowledge33 Most Recent 2 years ago

a is correct

upvoted 1 times

sdwanlove 2 years, 10 months ago

Found new information: Repeat the last three steps to add more class lists as required. The following are example class lists and queue mappings: Table 1. Class List and Queue Mappings Class Queue VOICE 0 CRTICAL_DATA 1 BULK 2 CLASS_DEFAULT 3 INTERACTIVE_VIDEO 4 CONTROL SIGNALING 5 https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/qos/ios-xe-17/qos-book-xe/forwarding-qos.html#:~:text=Cisco%20SD%2DWAN%20Forwarding%20and%20QoS%20Overview,-Forwarding%20takes%20the&text=It%20specifies%20the%20interface%20through,IPsec%20connections%20between%20the%20routers. Also found this following cisco live: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRRST-2457-LG.pdf Page 25 Given answer is correct --> 0 disregard my last comment.

upvoted 2 times

sdwanlove 2 years, 10 months ago

On Cisco vEdge devices and Cisco IOS XE SD-WAN devices, each interface has eight queues, which are numbered 0 to 7. Queue 0 is reserved, and is used for both control traffic and low-latency queuing (LLQ) traffic. For LLQ, any class that is mapped to queue 0 must also be configured to use LLQ. Queues 1 to 7 are available for data traffic Queue 0 is reserved for control plane traffic and voice traffic would fall under the data traffic segment which is from 1 to 7. Answer should be B -1It's A, queue 0, LLQ .. voice with control traffic are the most critical

upvoted 1 times

sdwanlove 2 years, 10 months ago

On Cisco vEdge devices and Cisco IOS XE SD-WAN devices, each interface has eight queues, which are numbered 0 to 7. Queue 0 is reserved, and is used for both control traffic and low-latency queuing (LLQ) traffic. For LLQ, any class that is mapped to queue 0 must also be configured to use LLQ.

Queues 1 to 7 are available for data traffic

Queue 0 is reserved for control plane traffic and voice traffic would fall under the data traffic segment which is from 1 to 7.

Answer should be B -1

upvoted 1 times

MerlinTheWizard 2 years, 8 months ago

It's A, queue 0, LLQ .. voice with control traffic are the most critical

upvoted 1 times

Question #149 *Topic 1*

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

A.

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

B.

```
interface interface-name
  vpn vpn-id
    shaping-rate 1000000
```

C.

```
vpn vpn-id
  interface interface-name
    shaping-rate 1000000
```

D.

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

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

Nalla123 Highly Voted 3 years, 11 months ago
Answer is D vpn vpn-id interface interface-name shaping-rate kbps
upvoted 19 times

Arsenal16 1 year, 6 months ago
Answer is D based on https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#r_shaping_rate_3056.xml the answer should be vpn vpn-id interface interface-name shaping-rate kbps
upvoted 2 times

mikidvd51 1 year, 9 months ago
why cisco uses on some commands bps , on some Bps, and on some kbps This is a MESS.
upvoted 2 times

Rosh8787 1 year, 10 months ago
Option D is the correct answer. Below is the correct format for defining shaping rate. vpn vpn-id interface interface-name shaping-rate kbps
upvoted 1 times

Rosh8787 1 year, 10 months ago
Option D is the correct answer https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#r_shaping_rate_3056.xml
upvoted 1 times

Vic_Malloy 2 years ago
C: is correct. To set the shape rate to 1Mbps you need t9 specify 1,000,000 b8ts per second.
upvoted 1 times

sull3y 2 years, 2 months ago
Answer is D Command Hierarchy vpn vpn-id interface interface-name shaping-rate kbps
upvoted 2 times

bullett00th 2 years, 8 months ago
I would choose D!! shaping-rates are in Kpbs???!!
upvoted 1 times

NetArch_Teck 3 years, 1 month ago

The rate in which data is transmitted is in Kbps, meaning 1000 Kbps = 1MB The Syntax Hierarchy is VPN-"VPN-ID" Interface Interface Name Shaping-rate kbps The only correct option that fulfils the question is option D.

upvoted 1 times

BGP65000 3 years, 2 months ago

I agree should be C, because shaping-rate is expressed in kbits, 1mbits=1000kbits.

upvoted 1 times

BGP65000 3 years, 2 months ago

I agree should be C, because shaping-rate is expressed in kbits, 1mbits=1000kbits.So It's D hh

upvoted 1 times

Rbrahmi Most Recent 9 months ago

So It's D hh

upvoted 1 times

kcobain87 3 years, 9 months ago

It should be D

upvoted 3 times

ChrisCCNA 3 years, 11 months ago

This should be kbps

upvoted 4 times

Question #150 *Topic 1*

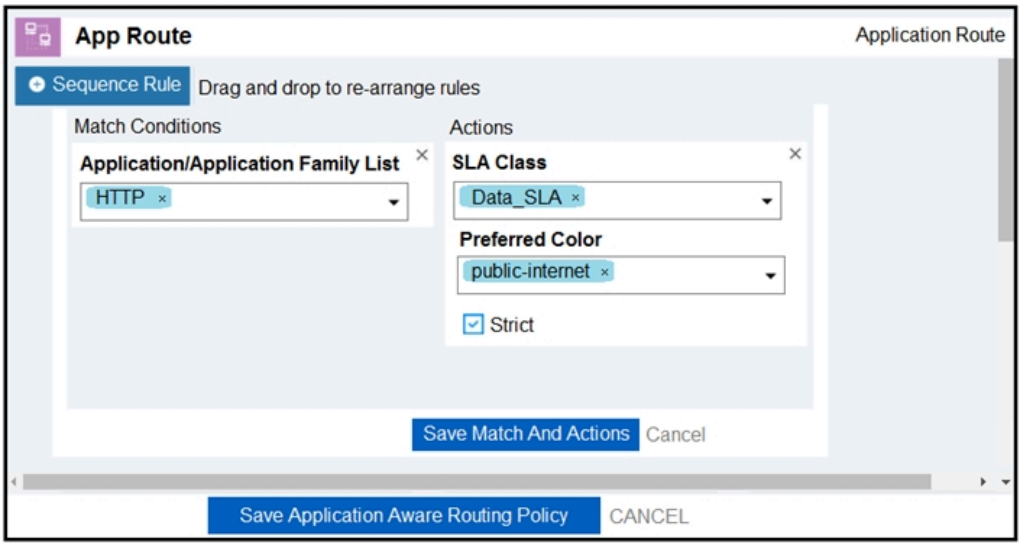
An engineer must improve video quality by limiting HTTP traffic to the Internet without any failover. Which configuration in vManage achieves this goal?

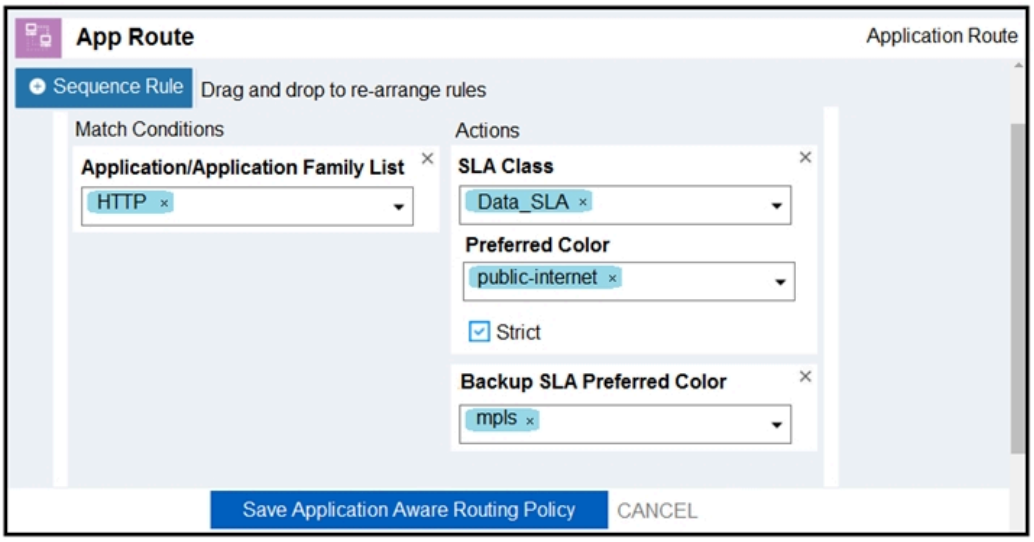
A.

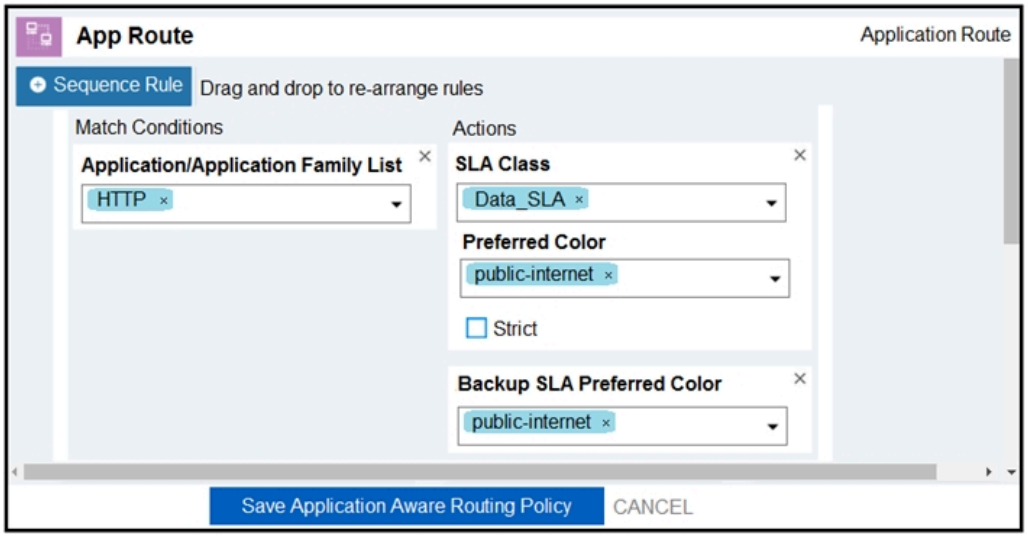
B.

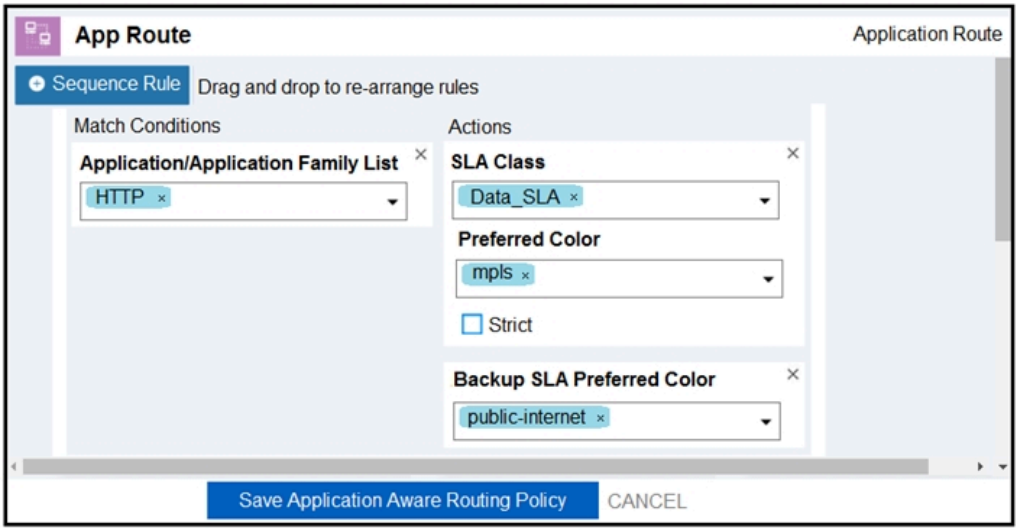
C.

D.









Suggested Answer:
Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.2/07Policy_Applications/01Application- Aware_Routing/01Configuring_Application-Aware_Routing

Aldebeer Most Recent 1 year, 9 months ago

without failover means no backup. answer A i correct

upvoted 1 times

Question #151 *Topic 1*

An engineer configures policing with a rate of 125 Bps and a burst rate of 8000 bits, as shown here:
Which configuration completes this task?

```
policy
 policer p1
 rate
 burst
 exceed drop
!
access-list acl1
 sequence 1
 match
 source-ip 2.2.0.0/16
 destination-ip 10.1.1.0/24 100.1.1.0/24
 destination-port 20 30
 protocol 6 17 23
!
action accept
 policer p1
!
default-action drop
!
vpn 1
interface ge0/4
 description Policy ID: B412:A29D:65G3::5
 ip address 10.20.24.15/24
 no shutdown
 access-list acl1 out
!
```

A. Configure 125 for rate and 1000 for burst.

B. Configure 125 for rate and 8000 for burst.

C. Configure 1000 for rate and 1000 for burst.

D. Configure 1000 for rate and 64000 for burst.

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (71%) A (29%)

Idro Highly Voted 3 years, 9 months ago
The required rate is 125 Bps= 1000 bps , and the required burst is 8000 bits = 1000 bytes
upvoted 18 times

Strewth Highly Voted 3 years, 10 months ago
I believe the answer is A. Rate is in bits and burst is in Bytes (1000 Bytes = 8000 bits)And that's why rate is 1000 bps and burst 1000 Bps.. The question states the rate should be 125 Bps - 1000 bpsThe burst rate is measured in BYTES. 8000 BITS make 1000 BYTES. The burst rate is 1000. The 125 rate sets a rate of 125 BITS. So nothing to change or convert there.
upvoted 8 times

Strewth 3 years, 10 months ago
Selected Answer: A
I believe the answer is A. Rate is in bits and burst is in Bytes (1000 Bytes = 8000 bits)
upvoted 8 times

MerlinTheWizard 3 years, 2 months ago
And that's why rate is 1000 bps and burst 1000 Bps.. The question states the rate should be 125 Bps - 1000 bps
upvoted 1 times

MerlinTheWizard 3 years, 2 months ago

And that's why rate is 1000 bps and burst 1000 Bps.. The question states the rate should be 125 Bps - 1000 bpsThe burst rate is measured in BYTES. 8000 BITS make 1000 BYTES. The burst rate is 1000. The 125 rate sets a rate of 125 BITS. So nothing to change or convert there.

upvoted 1 times

PureInertiaCopy 2 years, 5 months ago

The burst rate is measured in BYTES. 8000 BITS make 1000 BYTES. The burst rate is 1000. The 125 rate sets a rate of 125 BITS. So nothing to change or convert there.

upvoted 1 times

eojedad Most Recent 8 months ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/localized-policy.html section Configure Localized Policy for IPv4 Using the CLI Define policing parameters: vEdge(config)# policy policer policer-name vEdgeconfig-policer)# rate bandwidth (bps) vEdge(config-policer)# burst bytes vEdge(config-policer)# exceed action rate = 125 Bytes/s × 8 = 1000 burst = 8000 bits / 8 = 1000

upvoted 1 times

ManjeshM 1 year, 8 months ago

The correct answer is C. Police rate is in bits per second (bps) and burst rate is in bytes. 125 Bps (125 Bytes per second) = 1000 bits per second (125 x 8). 8000 bits = 8000/8 Bytes (1000 Bytes).

upvoted 1 times

NetArch_Teck 3 years, 1 month ago

The Correct Answer is C "rate = 1000, Burst = 1000" Rate is measured in bits per second and Burst is measured in Bytes per seconds. 1 Byte = 8 bits 8 bits = 1 Byte So configuring a rate of 125 Bytes per second and a Burst of 8000 Bits translates into:- 125 Bytes = 1000 Bits "Rate is calculated in bits" 8000 bits would be = 1000 Bytes "Rate is calculated by Bytes"

upvoted 3 times

BGP65000 3 years, 2 months ago

for me it's C, in policer's burst is expressed in bytes and rate in bits. Check the following link: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/localized-policy.html

upvoted 1 times

Luke538 3 years, 3 months ago

Exactly what Idro says, take care of the units. The given units are in bytes per second (Bps) and bits per second (bps) respectively. Rates are set in bits, and burst in bytes.

upvoted 2 times

eVo3000 3 years, 4 months ago

From: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_17.1/08Forwarding_and_QoS/03Forwarding_and_QoS_Configuration_Examples Here "policer p1" is configured to have a maximum traffic rate of 1,000,000 bits per second and a maximum burst-size limit of 15000 bytes : policy policer p1 rate 1000000 burst 15000 exceed drop ! So same unit for rate 125 bits per second. You need to convert 8000 bits => 1000 bytes Answer is A

upvoted 1 times

DameeL 3 years, 6 months ago

The answer should be C. ============================ vsmart(config-policer-1)# rate ? Description: Bandwidth for 1g interfaces: bps; for 10g interfaces: bps Possible completions: rate is in bps [125*8=1000] vsmart(config-policer-1)# burst ? Description: Burst rate, in bytes Possible completions: burst is in bytes [8000/8=1000]

upvoted 3 times

agkyawsoe 3 years, 6 months ago

It should be same unit ... 125Bps, brust is 1000Bps and if 1000bps, burst should be 8000bps ... notice the Bytes and bits ...

upvoted 2 times

Jonycici 3 years, 8 months ago

answer is C. 125 Bps = 1000 bps

upvoted 2 times

Question #152 *Topic 1*

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 Threat Grid

B. Cisco Trust Anchor Module

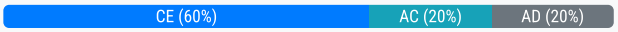
C. Cisco AMP

D. Cisco Secure Endpoint

E. Cisco Snort IPS

Suggested Answer: *A, C*
Official Answer: AC

Community vote distribution



eojedad Most Recent 8 months ago
CE is the correct answer
upvoted 1 times

jawad_khalife 1 year, 8 months ago
Cisco AMP (formerly) is now Cisco Secure endpoint so A and D
upvoted 1 times

Rosh8787 1 year, 10 months ago
CE is the correct answer
upvoted 1 times

BECAUSE 2 years, 3 months ago
Selected Answer: AC
A and C i would say are the answers. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/malware-protection.html
upvoted 1 times

BECAUSE 2 years, 3 months ago
A and C i would say are the answers. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/malware-protection.htmlSorry C and E after further research
upvoted 1 times

BECAUSE 2 years, 3 months ago
Sorry C and E after further research
upvoted 1 times

M_Ryu 2 years, 11 months ago
I think it's C and E Cisco Amp: "File Reputation: The process of using a 256-bit Secure Hash Algorithm (SHA256) signature to compare the file against the Advanced Malware Protection (AMP) cloud server and access its threat intelligence information. The response can be Clean, Unknown, or Malicious." Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/malware-protection.html Cisco Snort IPS: "Snort is an open source network IPS that performs real-time traffic analysis and generates alerts when threats are detected on IP networks." Source: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16-12/sec-data-utd-xe-16-12-book/snort-ips.pdf
upvoted 1 times

colipto 3 years ago
Cisco Threat Grid (Option A): Cisco Threat Grid is a cloud-based malware analysis and threat intelligence platform. It allows the customer to calculate the SHA value for files as they pass through the SD-WAN devices. The files are then submitted to Threat Grid for analysis. The platform analyzes files using various sandboxing techniques to determine if the files are good, unknown, or malicious. This provides real-time threat detection and enables the customer to take appropriate actions when threats are detected.

Cisco AMP (Advanced Malware Protection) (Option C): Cisco AMP is a comprehensive security solution that provides advanced malware detection, prevention, and response capabilities. It offers file reputation services, file analysis, and sandboxing to identify and block advanced malware and threats. In a Cisco SD-WAN deployment, AMP can be integrated with the SD-WAN devices to perform real-time traffic analysis. This helps in detecting and blocking threats in real-time and generating alerts when malicious activities are identified.

upvoted 3 times

colipto 3 years ago

Cisco Threat Grid (Option A): Cisco Threat Grid is a cloud-based malware analysis and threat intelligence platform. It allows the customer to calculate the SHA value for files as they pass through the SD-WAN devices. The files are then submitted to Threat Grid for analysis. The platform analyzes files using various sandboxing techniques to determine if the files are good, unknown, or malicious. This provides real-time threat detection and enables the customer to take appropriate actions when threats are detected. Cisco AMP (Advanced Malware Protection) (Option C): Cisco AMP is a comprehensive security solution that provides advanced malware detection, prevention, and response capabilities. It offers file reputation services, file analysis, and sandboxing to identify and block advanced malware and threats. In a Cisco SD-WAN deployment, AMP can be integrated with the SD-WAN devices to perform real-time traffic analysis. This helps in detecting and blocking threats in real-time and generating alerts when malicious activities are identified.Options B (Cisco Trust Anchor Module), D (Cisco Secure Endpoint), and E (Cisco Snort IPS) do not directly meet the specified requirements for calculating SHA values for files passing through the SD-WAN devices and performing real-time traffic analysis with threat detection and alerts. In summary, Cisco Threat Grid and Cisco AMP are the two Cisco SD-WAN solutions that provide the required capabilities for SHA value calculation and real-time traffic analysis with threat detection and alerting.

upvoted 3 times

colipto 3 years ago

Options B (Cisco Trust Anchor Module), D (Cisco Secure Endpoint), and E (Cisco Snort IPS) do not directly meet the specified requirements for calculating SHA values for files passing through the SD-WAN devices and performing real-time traffic analysis with threat detection and alerts. In summary, Cisco Threat Grid and Cisco AMP are the two Cisco SD-WAN solutions that provide the required capabilities for SHA value calculation and real-time traffic analysis with threat detection and alerting.

upvoted 1 times

nilkanthy 3 years, 8 months ago

Correct answer is C and E confirmed with Cisco documents.C for Calculate SHA value for files. E for real time traffic analysis and generate alerts.

upvoted 2 times

nilkanthy 3 years, 8 months ago

Correct answer is C and E confirmed with Cisco documents.

upvoted 2 times

nilkanthy 3 years, 8 months ago

C for Calculate SHA value for files. E for real time traffic analysis and generate alerts.

upvoted 4 times

PiyKac 3 years, 9 months ago

CE. https://www.cisco.com/c/en/us/support/docs/routers/xe-sd-wan-routers/217641-configure-sdwan-advanced-malware-protect.html https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16/sec-data-utd-xe-16-6-book/snort-ips.html.xml

upvoted 1 times

atiWok 3 years, 9 months ago

correct answer is AChttps://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/malware-protection.html

upvoted 1 times

atiWok 3 years, 9 months ago

correct answer is AC

upvoted 1 times

atiWok 3 years, 9 months ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/malware-protection.html

upvoted 1 times

aafonya 3 years, 9 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16-12/sec-data-utd-xe-16-12-book/snort-ips.pdf "Snort is an open source network IPS that performs real-time traffic analysis and generates alerts when threats are detected on IP networks. "

upvoted 2 times

Question #153 *Topic 1*

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

A. geolocation

B. site ID

C. URL

D. protocol

E. tunnels

Suggested Answer: *C, D*

Official Answer: CD

Community vote distribution

DE (100%)

aafonya Highly Voted 2 years, 9 months ago

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

upvoted 6 times

AJMD Most Recent 1 year, 11 months ago

Protocol and Tunnel

upvoted 1 times

PepaZdepa33 2 years, 1 month ago

from the link tat aafonya shared step 4. Choose the rule's criteria. a. Protocol b. Source Tunnels c. Source CIDR IP Addresses d. Source Ports e. Destination CIDR IP Addresses f. Destination Ports g. Applications

upvoted 2 times

heavncong 2 years, 7 months ago

Agree with aafonya. It can filter protocol, ports, tunnels, ip, applications

upvoted 1 times

Question #154 *Topic 1*

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

A. no system logging disk local

B. system logging server remote

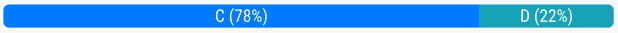
C. no system logging disk enable

D. system logging disk disable

Suggested Answer: *C*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/02System_and_Interfaces/08Configuring_System_Logging

Community vote distribution



Jonycici 2 years, 2 months ago

answer is C

upvoted 2 times

atiWok 2 years, 3 months ago

as Khanda said: vEdge-5(config)# no system logging disk enable vEdge-5(config)# commit Commit complete.

upvoted 2 times

ChrisCCNA 2 years, 6 months ago

Khanda posted the command

upvoted 3 times

khanda 2 years, 6 months ago

Correction: Answer is C

upvoted 3 times

khanda 2 years, 6 months ago

Selected Answer: D

vEdge-5(config)# no system logging disk enable vEdge-5(config)# commit Commit complete.

upvoted 2 times

khanda 2 years, 6 months ago

vEdge-5(config)# no system logging disk enable vEdge-5(config)# commit Commit complete.Your command is correct but seems your selected answer goes wrong... ...

upvoted 2 times

heavncong Most Recent 2 years, 1 month ago

Your command is correct but seems your selected answer goes wrong... ...

upvoted 2 times

Question #155 *Topic 1*

Which combination of platforms is managed by vManage?

A. ISR4351, ASR1002HX, vEdge2000, vEdge Cloud

B. ISR4321, ASR1001, Nexus, ENCS

C. ISR4321, ASR1001, ENCS, ISRv

D. ISR4351, ASR1009, vEdge2000, CSR1000v

Suggested Answer: *C*

Official Answer: C

Community vote distribution

A (88%) C (12%)

Cert_freak Highly Voted 5 years, 5 months ago

C is wrong only 1001-X is supported - A is the right answer https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/datasheet-c78-731632.html

upvoted 12 times

Adedayo Highly Voted 5 years, 7 months ago

ISRv is integrated services virtual router which can be used in the SDWAN fabric. Answer is validl agree, C is correct.ASR1001 is not support , should be -X, eg 1001-X https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKARC-2001.pdf page 38

upvoted 5 times

Adedayo 5 years, 7 months ago

ISRv is integrated services virtual router which can be used in the SDWAN fabric. Answer is valid

upvoted 5 times

CCNPWILL 5 years, 3 months ago

I agree, C is correct.

upvoted 3 times

RexChen 5 years, 2 months ago

ASR1001 is not support , should be -X, eg 1001-X https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKARC-2001.pdf page 38

upvoted 2 times

Rcont Most Recent 2 years, 1 month ago

why C is incorrect?

upvoted 1 times

thomazmr 2 years, 6 months ago

A. ISR4351, ASR1002HX, vEdge2000, vEdge Cloud

upvoted 1 times

soltani 2 years, 7 months ago

A is correct Product portfolio ASR1000 series: Cisco ASR 1001-X Router (Figure 2) ● Cisco ASR 1002-X Router ● Cisco ASR 1001-HX Router (Figure 3) ● Cisco ASR 1002-HX Router (Figure 4) ● Cisco ASR 1004 Router ● Cisco ASR 1006 Router ● Cisco ASR 1006-X Router ● Cisco ASR 1009-X Router ● Cisco ASR 1013 Router ASR 1000 is not include upper product

upvoted 1 times

Nandhujoe 3 years, 3 months ago

A. ISR4351, ASR1002HX, vEdge2000, vEdge Cloud

upvoted 1 times

Nandhujoe 3 years, 3 months ago

Correct Answer is A. ISR4351, ASR1002HX, vEdge2000, vEdge Cloud

upvoted 1 times

Neil_Neo234 3 years, 4 months ago

Check the compatibility matrix below : https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/compatibility/sdwan-device-compatibility.html#device-compat-isr4k

upvoted 2 times

khanda 4 years ago

Correct Answer is A

upvoted 1 times

jfernando_perezj 4 years, 1 month ago

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

upvoted 1 times

The_Real_StarLord 4 years, 3 months ago

C is correct : " New device models—for example, the Cisco 4331 ISR and the Cisco Integrated Services Virtual Router (ISRv) have been introduced in vManage." https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white_paper-c11-741071.html

upvoted 1 times

peerouter 4 years, 5 months ago

C Physical ● Branch: Cisco IOS® XE and Viptela OS-based devices. ● Branch: Cisco Catalyst® 8300 Series Edge Platforms and Cisco 1000, 1100, or 4000 Series Integrated Services Routers (ISR). ● Branch, regional hub, or data center: Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers (ASR). Virtual ● SD-Branch: Cisco 5000 Series Enterprise Network Compute System (ENCS) and Integrated Services Virtual Router (ISRv). ● Network hub, colocation facility, or data center: Cisco Cloud Services Platform 5000, Catalyst 8000V Edge Software, and Cloud Services Router (CSR) 1000V Series

upvoted 1 times

Baio 4 years, 5 months ago

A is the correct one https://www.cisco.com/c/en/us/products/collateral/software/one-wan-subscription/guide-c07-740642.html

upvoted 2 times

DP 4 years, 6 months ago

The answer C is correct. In the OCG book in Chapter 2, on page 30, Table 2-1 shows a list of current SD-WAN supported platforms that includes Cisco ENCS amongst others.ENCS 5K

upvoted 1 times

DP 4 years, 6 months ago

The answer C is correct.

In the OCG book in Chapter 2, on page 30, Table 2-1 shows a list of current SD-WAN supported platforms that includes Cisco ENCS amongst others.

upvoted 1 times

she_ccie 4 years, 5 months ago

ENCS 5K

upvoted 1 times

CesarVergaraGalindo 4 years, 10 months ago

A is Correct

upvoted 1 times

serieus 5 years ago

So all models in A & C are supported in SD-WAN, however the ISRv is managed from DNA-center. A is correct.

"Cisco vEdge Cloud is deployed by Cisco DNA Center and then controlled, provisioned, and managed by Cisco vManage, whereas Cisco ISRv is deployed, provisioned, and managed by Cisco DNA Center." https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white_paper-c11-741071.html

upvoted 3 times

serieus 5 years ago

So all models in A & C are supported in SD-WAN, however the ISRv is managed from DNA-center. A is correct. "Cisco vEdge Cloud is deployed by Cisco DNA Center and then controlled, provisioned, and managed by Cisco vManage, whereas Cisco ISRv is deployed, provisioned, and managed by Cisco DNA Center." https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white_paper-c11-741071.htmlNoticed the whitepaper dates from 2019, not sure if it's still accurate..

upvoted 3 times

serieus 5 years ago

Noticed the whitepaper dates from 2019, not sure if it's still accurate..

upvoted 1 times

Lunap 5 years ago

Answer should be A. all the models in answer A are SDWAN supported.

upvoted 1 times

Question #156 *Topic 1*

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

A. Critical

B. Medium

C. Major

D. Minor

Suggested Answer: *C*
Reference: https://sdwan-docs.cisco.com/Product_Documentation/vManage_How-Tos/Troubleshooting/Monitor_Alarms

kentkyye Highly Voted 2 years, 1 month ago

Critical (red)—Serious events that impair or shut down the operation of an overlay network function. • Major (yellow)—Serious events that affect, but do not shut down, the operational of a network function. • Medium (blue)—Events that might impair the performance of a network function. • Minor (green)—Events that might diminish the performance of a network function

upvoted 8 times

Han2022 Most Recent 1 year, 8 months ago

Alarm States Cisco vManage alarms are assigned a state based on their severity: Critical (red)—Serious events that impair or shut down the operation of an overlay network function. Major (yellow)—Serious events that affect, but do not shut down, the operational of a network function. Medium (blue)—Events that might impair the performance of a network function. Minor (green)—Events that might diminish the performance of a network function.

upvoted 2 times

Question #157 *Topic 1*

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

A. System Status

B. Troubleshooting

C. Real Time

D. Events

Suggested Answer: *C*

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

Community vote distribution

C (100%)

Almanac Highly Voted 4 years, 10 months ago

base on the link given its. Troubleshootingthis question is repeated in Q#101 and there too answer is Real time. Surprisingly there 'troubleshooting' is not an option even ! I just checked in sandbox and looks like "troubleshooting" is the right answer. confusing :(

upvoted 8 times

Almanac Highly Voted 4 years, 10 months ago

base on the link given its. Troubleshooting

upvoted 8 times

go_Corona_go 4 years, 9 months ago

this question is repeated in Q#101 and there too answer is Real time. Surprisingly there 'troubleshooting' is not an option even ! I just checked in sandbox and looks like "troubleshooting" is the right answer. confusing :(

upvoted 1 times

Kiprotich Most Recent 1 year, 11 months ago

From the Cisco SD-WAN Manager menu: View the configured services on the Real Time monitoring page (Monitor > Devices > hub-device > Real Time). For Device Options, select OMP Services. Cisco vManage Release 20.6.x and earlier: View the configured services on the Real Time monitoring page (Monitor > Network > hub-device > Real Time). For Device Options, select OMP Services.

upvoted 1 times

nbvolz 2 years, 3 months ago

Same question #164.

upvoted 1 times

Speirsington 4 years, 1 month ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html#monitor-service-chaining-vmanage Realtime On a hub device, view the configured services From the Cisco vManage menu: View the configured services on the Real Time monitoring page (Monitor > Devices > hub-device > Real Time) Troubleshooting On a spoke device, view the details of the service chain path. Using Cisco vManage: View the service chain path on the Traceroute page (Monitor > Devices > spoke-device > Troubleshooting > Connectivity > Trace Route). Enter the destination IP, VPN, and source interface for the desired path.

upvoted 3 times

DBla 4 years, 4 months ago

Actually, both looks good to me: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html

upvoted 1 times

vicopo 4 years, 7 months ago

Maybe the trick is in the "service insertion configuration", under troubleshooting you can verify if its running properly but under the real-time you can send several commands ...

upvoted 1 times

alphatag 4 years, 9 months ago

With Troubleshooting option you can verify the path trough service insertion doing a traceroute, but traceroute isn't the only option inside Troubleshooting, because Ping is inside Troubleshooting too. If you go trough Monitor>Network>[select_device]>Real Time>OMP Services and see Service Column you can watch for example FW service. For me the correct answer is Real Time

upvoted 2 times

Question #158 *Topic 1*

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}}

Suggested Answer: *A*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/Command_Reference/Command_Reference/vManage_REST_APIs/vManage_REST_APIs_Overview/Using_the_vManage_REST_APIs

Community vote distribution

A (100%)

GoForCCNP Most Recent 1 year, 11 months ago

Given answer is correct. "Every data service API request begins with the following Base URI: https:// /dataservice"

https://developer.cisco.com/docs/sdwan/#!summary

upvoted 2 times

Question #159 *Topic 1*

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

A.

B.

C.

D.

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

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

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

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

Suggested Answer:
Official Answer: B

lakatos Highly Voted 3 years, 4 months ago

B is the management interface, C is the management vpn configuration.Agree. C is correct.

upvoted 18 times

lakatos Highly Voted 3 years, 4 months ago

B is the management interface, C is the management vpn configuration.

upvoted 18 times

CCNPWILL 3 years, 3 months ago

Agree. C is correct.

upvoted 14 times

kcobain87 Most Recent 1 year, 9 months ago

C is the correct one

upvoted 3 times

Eliasmiranda 1 year, 11 months ago

C is correct. OOB management vpn configuration which is vpn512. vpn is configured first before you configure your interface.

upvoted 2 times

khanda 2 years ago

C is the correct answer.

upvoted 2 times

CesarVergaraGalindo 2 years, 10 months ago

C is Correct

upvoted 2 times

Question #160 *Topic 1*

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 an ICMP connection

B. To be downloaded over a SNMP connection

C. To be downloaded over a control plane connection

D. To be downloaded over an out-of-band connection

E. To be downloaded over a SMTP connection

Suggested Answer: *C, D*

Reference: https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Maintenance/Software_Repository

Community vote distribution

CD (100%)

PureInertiaCopy Most Recent 1 year, 11 months ago

The Cisco vManage software repository allows you to store images in three ways: On the local Cisco vManage server, to be downloaded over a control plane connection: Here, the software images are stored on the local Cisco vManage server, and they are downloaded to the Cisco SD-WAN devices over a control plane connection. The receiving device generally throttles the amount of data traffic it can receive over a control plane connection, so for large files, the Cisco vManage server might not be able to monitor the software installation on the device even though it is proceeding correctly.On the local Cisco vManage server, to be downloaded over an out-of-band connection: Here, the software images are stored on the local Cisco vManage server, and they are downloaded to the Cisco SD-WAN devices over an out-of-band management connection. For this method to work, you specify the IP address of the out-of-band management interface when you copy the images to the software repository. This method is recommended when the software image files are large, because it bypasses any throttling that the device might perform and so the Cisco vManage server is able to monitor the software installation.On a remote server: From Cisco vManage Release 20.7.1, you can store software images on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the Cisco vManage server sends this URL to the Cisco SD-WAN device, which establishes a connection to the file server to download the software images. In a multitenant Cisco SD-WAN deployment, only the provider can register a remote server with Cisco vManage and add locations of software images on the remote server to the Cisco vManage repository. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/maintain.html#concept_lpv_ggg_5rb

upvoted 2 times

PureInertiaCopy 1 year, 11 months ago

The Cisco vManage software repository allows you to store images in three ways:

On the local Cisco vManage server, to be downloaded over a control plane connection: Here, the software images are stored on the local Cisco vManage server, and they are downloaded to the Cisco SD-WAN devices over a control plane connection. The receiving device generally throttles the amount of data traffic it can receive over a control plane connection, so for large files, the Cisco vManage server might not be able to monitor the software installation on the device even though it is proceeding correctly.

upvoted 2 times

PureInertiaCopy 1 year, 11 months ago

On the local Cisco vManage server, to be downloaded over an out-of-band connection: Here, the software images are stored on the local Cisco vManage server, and they are downloaded to the Cisco SD-WAN devices over an out-of-band management connection. For this method to work, you specify the IP address of the out-of-band management interface when you copy the images to the software repository. This method is recommended when the software image files are large, because it bypasses any throttling that the device might perform and so the Cisco vManage server is able to monitor the software installation.On a remote server: From Cisco vManage Release 20.7.1, you can store software images on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the Cisco vManage server sends this URL to the Cisco SD-WAN device, which establishes a connection to the file server to download the software images. In a multitenant Cisco SD-WAN deployment, only the provider can register a remote server with Cisco vManage and add locations of software images on the remote server to the Cisco vManage repository. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/maintain.html#concept_lpv_ggg_5rb

upvoted 2 times

PureInertiaCopy 1 year, 11 months ago

On the local Cisco vManage server, to be downloaded over an out-of-band connection: Here, the software images are stored on the local Cisco vManage server, and they are downloaded to the Cisco SD-WAN devices over an out-of-band management connection. For this method to work, you specify the IP address of the out-of-band management interface when you copy the images to the software repository. This method is recommended when the software image files are large, because it bypasses any throttling that the device might perform and so the Cisco vManage server is able to monitor the software installation.

upvoted 2 times

PureInertiaCopy 1 year, 11 months ago

On a remote server: From Cisco vManage Release 20.7.1, you can store software images on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the Cisco vManage server sends this URL to the Cisco SD-WAN device, which establishes a connection to the file server to download the software images. In a multitenant Cisco SD-WAN deployment, only the provider can register a remote server with Cisco vManage and add locations of software images on the remote server to the Cisco vManage repository.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/maintain.html#concept_lpv_ggg_5rb

upvoted 2 times

Aldebeer 2 years, 2 months ago

yes its correct

upvoted 1 times

khanda 3 years, 6 months ago

Answer is correct, doc link provided in the question.

upvoted 2 times

Question #161 *Topic 1*

Which logs verify when a device was upgraded?

A. ACL

B. Email

C. SNMP

D. Audit

Suggested Answer: *D*
Official Answer: D

CCNPWILL Most Recent 2 years, 1 month ago

Monitor > AuditLog. Correct

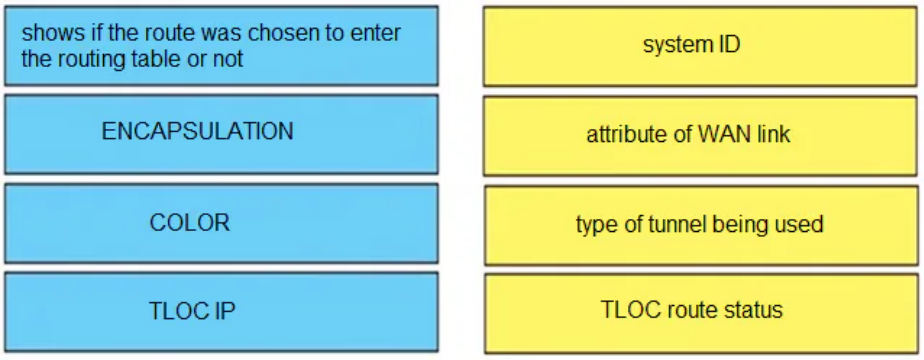
upvoted 3 times

Question #162 *Topic 1*

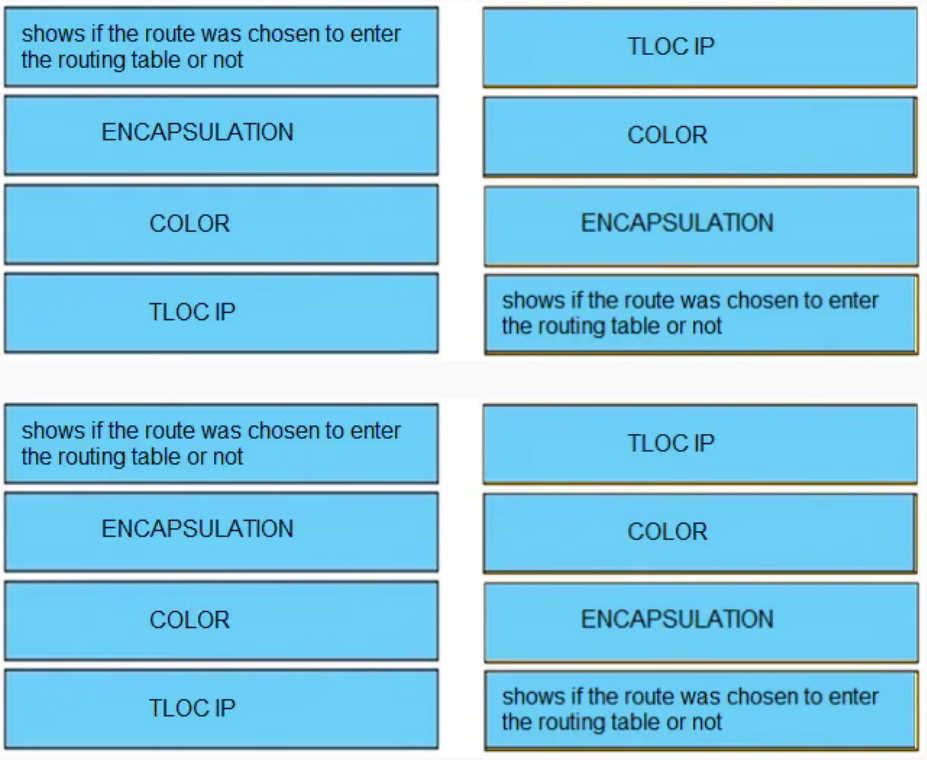
DRAG DROP -

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

Select and Place:



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #163 *Topic 1*

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

A. OMP

B. NetFlow

C. BFD

D. IP SLA

Suggested Answer: *C*

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

Community vote distribution

C (100%)

Matt2727 Most Recent 2 years, 1 month ago

BFD is the correct protocol

upvoted 1 times

CCNPWILL 4 years, 8 months ago

Correct.

upvoted 4 times

Question #164 *Topic 1*

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

A. System Status

B. ACL Logs

C. Real Time

D. Events

Suggested Answer: *C*
Official Answer: C

nbvolz Most Recent 1 year, 9 months ago
Same question #157
upvoted 1 times

Speirsington 3 years, 7 months ago
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html#monitor-service-chaining-vmanage Realtime On a hub device, view the configured services From the Cisco vManage menu: View the configured services on the Real Time monitoring page (Monitor > Devices > hub-device > Real Time) Troubleshooting On a spoke device, view the details of the service chain path. Using Cisco vManage: View the service chain path on the Traceroute page (Monitor > Devices > spoke-device > Troubleshooting > Connectivity > Trace Route). Enter the destination IP, VPN, and source interface for the desired path.
upvoted 2 times

CCNPWILL 3 years, 8 months ago
Monitor Service Chaining You can monitor different aspects of service chaining on hub and spoke devices Configuring a service device to operate as part of the service chain is called service insertion. On a hub device, view the configured services.

From the Cisco vManage menu:

View the configured services on the Real Time monitoring page (Monitor > Devices > hub-device > Real Time). For Device Options, select OMP Services.
upvoted 1 times

CCNPWILL 3 years, 8 months ago
Monitor Service Chaining You can monitor different aspects of service chaining on hub and spoke devices Configuring a service device to operate as part of the service chain is called service insertion. On a hub device, view the configured services. From the Cisco vManage menu: View the configured services on the Real Time monitoring page (Monitor > Devices > hub-device > Real Time). For Device Options, select OMP Services.C is correct. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html
upvoted 1 times

CCNPWILL 3 years, 8 months ago
C is correct. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/service-chaining.html
upvoted 1 times

Question #165 *Topic 1*

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

A. AES-256

B. MD5

C. SHA-2

D. AES-128

E. SHA-1

Suggested Answer: *B, E*

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

Community vote distribution



CCNPWILL Highly Voted 5 years, 3 months ago

Authentication Protocol

Select the authentication mechanism for the user:

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.

upvoted 9 times

CCNPWILL Highly Voted 5 years, 3 months ago

Authentication Protocol Select the authentication mechanism for the user: 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.Correct, but B and E are correct in this case.Note MD5 authentication protocol is deprecated for Cisco SD-WAN Release 20.3.2 and later releases.This is correct. but the valid answer is still. B&E

upvoted 9 times

khanda 4 years ago

Correct, but B and E are correct in this case.

upvoted 4 times

CCNPWILL 5 years, 3 months ago

Note MD5 authentication protocol is deprecated for Cisco SD-WAN Release 20.3.2 and later releases.

upvoted 2 times

Almanac 5 years, 3 months ago

This is correct. but the valid answer is still. B&E

upvoted 5 times

CesarVergaraGalindo 4 years, 10 months ago

B, C is Correct

upvoted 6 times

eojedad Most Recent 7 months, 3 weeks ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/snmp/snmp-book/m-snmp.html#Cisco_Concept.dita_Configure-SNMPv3-on-IOS-XE-Devices-Using-Cisco-vManage

upvoted 2 times

Rachant 1 year, 1 month ago

SNMP v3: Add User Name* Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters. Authentication Protocol Choose the authentication mechanism for the user: md5 sha

upvoted 1 times

Myare 1 year, 4 months ago

SNMP v3: Add User Name* Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters. Authentication Protocol Choose the authentication mechanism for the user: md5 sha Authentication Password Enter the authentication password either in cleartext or as an AES-encrypted key. Privacy Protocol Choose the privacy type for the user. aes-cfb-128: Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key. This is a SHA-1 authentication protocol. Correct anser is B &E

upvoted 2 times

mikidvd51 1 year, 9 months ago

Cisco should avoid such questions if authentication protocols changes over time. It just causes a misunderstanding a uncertainty .

upvoted 1 times

rubendrios 1 year, 10 months ago

SHA-1 message digest SHA-256 message digest Note: MD5 authentication protocol is deprecated for Cisco Catalyst SD-WAN Release 20.3.2 and later releases.

upvoted 1 times

Mykhey 2 years, 3 months ago

Table 20 in the link below https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/snmp/snmp-book/snmp-book_2.html#Cisco_Concept.dita_Configure-SNMPv3-on-IOS-XE-Devices-Using-Cisco-vManage

upvoted 1 times

Networkchamp87 2 years, 6 months ago

When configuring SNMPv3 monitoring on a WAN Edge router, the two algorithms commonly used for user authentication are: B. MD5 C. SHA-2 These algorithms are used to ensure the integrity and authenticity of SNMP messages exchanged between the SNMP manager (such as vManage NMS) and the managed device (WAN Edge router).Ignore my post - the answer is B and E.

upvoted 1 times

Networkchamp87 2 years, 6 months ago

When configuring SNMPv3 monitoring on a WAN Edge router, the two algorithms commonly used for user authentication are:

B. MD5 C. SHA-2

These algorithms are used to ensure the integrity and authenticity of SNMP messages exchanged between the SNMP manager (such as vManage NMS) and the managed device (WAN Edge router).

upvoted 1 times

Networkchamp87 2 years, 6 months ago

Ignore my post - the answer is B and E.

upvoted 1 times

soltani 2 years, 7 months ago

Choose the authentication mechanism for the user: *MD5 digest. (deprecate for release 20.3.2 and later) *SHA-1 message digest. *SHA-256 message digest.(start from release 20.5.1) according to these types and question. there is not sha-256 between options and must accept B&E

upvoted 1 times

bullett00th 2 years, 8 months ago

I'll go for SHA-1 and MD5 See Authentication Protocol https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/snmp/snmp-book/snmp-book_2.html#Cisco_Concept.dita_Configure-SNMPv3-on-IOS-XE-Devices-Using-Cisco-vManage

upvoted 1 times

Aldebeer 2 years, 8 months ago

To confirm my fellow specialists

upvoted 1 times

nbvolz 2 years, 10 months ago

Everyone is all over the place. One big guessing game we have here. More lost now than when started with all this

upvoted 1 times

M_Ryu 2 years, 11 months ago

B and E for me Section "Configure SNMPv3 on Cisco vEdge Devices Using Cisco SD-WAN Manager" Table 12 says: "Choose the authentication mechanism for the user: MD5 digest. SHA-1 message digest. SHA-256 message digest." For the sake of the test I'm assuming it doesn't matter that MD5 isn't used anymore because AES-128 and AES-256 are used for encryption and SHA-2 isn't an option. Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/snmp/snmp-book/snmp-book_2.html#Cisco_Concept.dita_Configure-SNMPv3-on-IOS-XE-Devices-Using-Cisco-vManageCorrection *SHA-2 isn't found on the page and SHA-256 isn't an option

upvoted 1 times

M_Ryu 2 years, 11 months ago

B and E for me

Section "Configure SNMPv3 on Cisco vEdge Devices Using Cisco SD-WAN Manager" Table 12 says: "Choose the authentication mechanism for the user: MD5 digest. SHA-1 message digest. SHA-256 message digest."

For the sake of the test I'm assuming it doesn't matter that MD5 isn't used anymore because AES-128 and AES-256 are used for encryption and SHA-2 isn't an option.

Source: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/snmp/snmp-book/snmp-book_2.html#Cisco_Concept.dita_Configure-SNMPv3-on-IOS-XE-Devices-Using-Cisco-vManage

upvoted 1 times

M_Ryu 2 years, 11 months ago

Correction *SHA-2 isn't found on the page and SHA-256 isn't an option

upvoted 1 times

NetArch_Teck 3 years, 1 month ago

Answer is B & C according to Cisco white papers!

upvoted 1 times

Chefff 3 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/snmp/snmp-book/snmp-book_2.html Choose the authentication mechanism for the user: MD5 digest. SHA-1 message digest. SHA-256 message digest. SHA-256 - introduced in 20.5.1 MD5 - depracated 20.3.2 Official Cisco SD-WAN course: https://www.cisco.com/c/en/us/training-events/training-certifications/training/training-services/courses/implementing-cisco-sd-wan-solutions-ensdwi.html The course lab environment is built using Cisco vEdge Cloud routers and Cisco SD-WAN 20.3 code. They use 20.3, so SHA-256 has not been there yet, I would go with MD5 and SHA-1, but IMO every combination SHA1/SHA2/MD5 is correct, it depends on the software version that you choose, so this question is really dumb and very Cisco-way of making exams.

upvoted 2 times

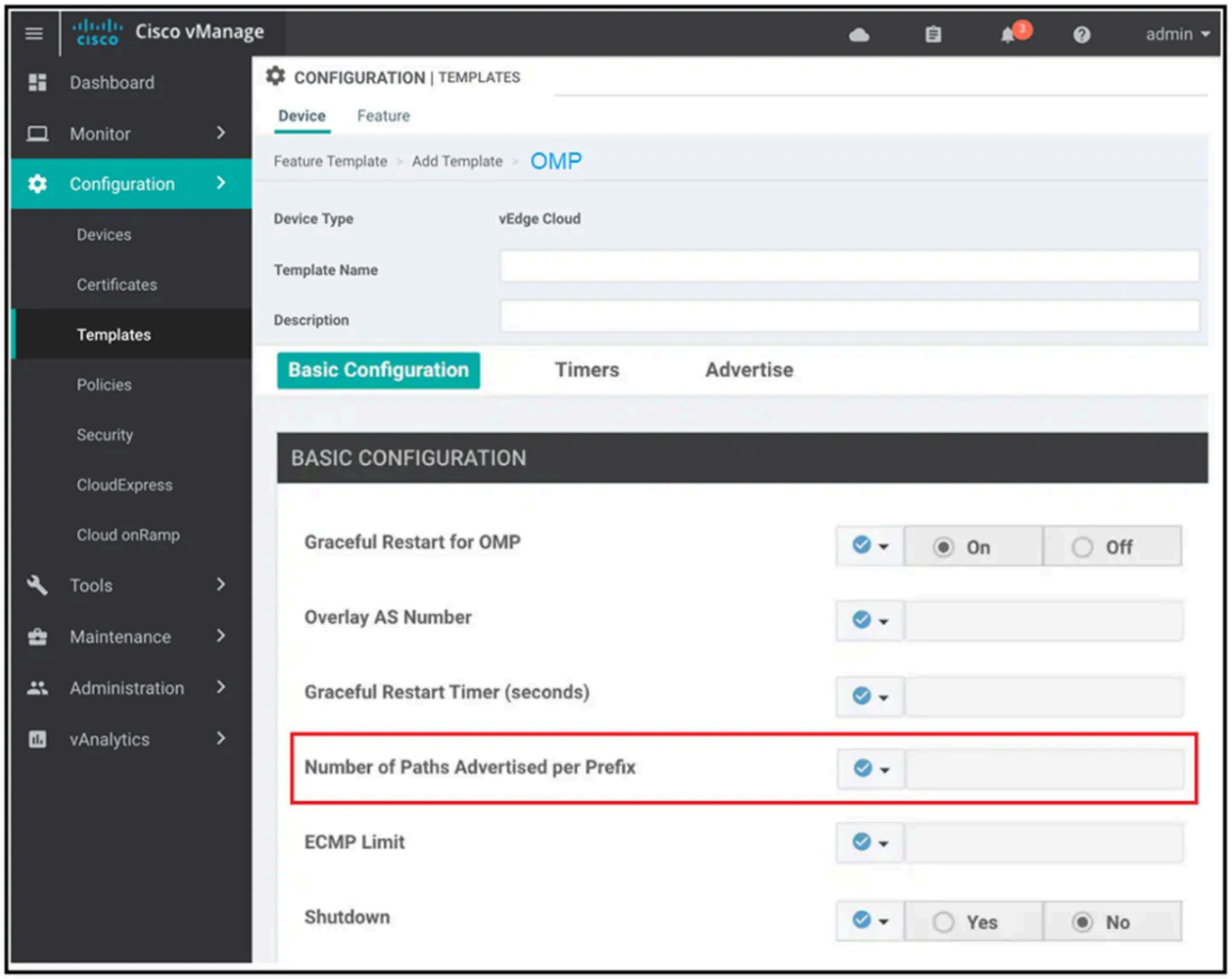
rajeshkumargs 3 years, 6 months ago

Answer is A & E, FYI MD5 is deprecated for cisco SDWAN release 20.3.2

upvoted 1 times

Question #166 *Topic 1*

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

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (64%) C (36%)

PiyKac Highly Voted 4 years, 6 months ago
Answer should be 5, can anyone confirm?I agree, because you configure the template on vManage and then it gets applied to each wan edge device.This reasoning makes alot of sense, since the configuration is made on the vManage
upvoted 10 times

PiyKac Highly Voted 4 years, 6 months ago
Answer should be 5, can anyone confirm?

upvoted 10 times

JTPRO 4 years, 5 months ago

I agree, because you configure the template on vManage and then it gets applied to each wan edge device.

upvoted 2 times

Mykhey 2 years, 3 months ago

This reasoning makes alot of sense, since the configuration is made on the vManage

upvoted 1 times

kcobain87 3 years, 9 months ago

D is the correct answer - See the documentation Number of Paths Advertised per Prefix Specify the maximum number of equal-cost routes to advertise per prefix. vEdge routers advertise routes to vSmart controllers, and the controllers redistribute the learned routes, advertising each route-TLOC tuple. A vEdge router can have up to four TLOCs, and by default advertises each route-TLOC tuple to the vSmart controller. If a local site has two vEdge routers, a vSmart controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised. Range: 1 through 16 Default: 4 https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Templates/OMP

upvoted 7 times

d656971 Most Recent 1 year, 3 months ago

Since 20.5, the range has been 1-16, default 4. Correct answer is 1, but not listed. I think Cisco is looking for 5, because it's the next step up from default if you wanted to increase the value

upvoted 1 times

mikidvd51 1 year, 9 months ago

C is correct The "number of paths" setting is per DEVICE

upvoted 2 times

mikidvd51 1 year, 9 months ago

5 per device

upvoted 1 times

NetArch_Teck 3 years, 1 month ago

The Answer is C Only 4 Paths can be advertised per prefix in the Overlay Management Protocol. The customer alludes to having 3 ISP circuits and 2 Private. The singular prefix would require at least 5 (4 by default, 1 advertisement to the Private Networks)

upvoted 2 times

majepiga 4 years, 3 months ago

I think the given answer is good because if they said that the remote site have 2 vedges and they has 5 links, so as minimum 1 prefix/vedge and there are 2 vedges 2x5 = 10vSmart pushes config for each individual vEdge device , thus 5 routes per device is correct answer

upvoted 3 times

majepiga 4 years, 3 months ago

I think the given answer is good because if they said that the remote site have 2 vedges and they has 5 links, so as minimum 1 prefix/vedge and there are 2 vedges 2x5 = 10

upvoted 3 times

gem 4 years, 3 months ago

vSmart pushes config for each individual vEdge device , thus 5 routes per device is correct answer

upvoted 1 times

takhira 4 years, 4 months ago

Should be C because by default it is 4.

upvoted 2 times

Question #167 *Topic 1*

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

A. BGP

B. DTLS

C. OSPF

D. OMP

Suggested Answer: *D*

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html#:~:text=The%20Overlay% 20Management%20Protocol%20is,described%20in%20Overlay%20Routing%20Overview .

Community vote distribution

B (100%)

TheNetworkStudent Highly Voted 4 years, 6 months ago

In the reference link under the 'Control Plane Authentication' part, you can find the following: Then, during the automatic authentication process, as pairs of devices (routers and controllers) are establishing DTLS control connections, each device compares the serial numbers (and for routers, the chassis numbers) to those in the files installed on the router. DTLS is the connection that facilitates the exchange of OMP information between the devices. In vManage the number of control connections also shows the amount of DTLS connections to/from a device. OMP is not the control connection, it's the control plane management protocol. B is correct, DTLS

upvoted 9 times

Mykhey Most Recent 1 year, 9 months ago

Both DTLS and OMP are true since the specific devices have not been mentioned! The wording of the question should be reviewed

upvoted 1 times

elninio13 2 years, 3 months ago

Why the owners dont correct the answers???

upvoted 2 times

ChrisCCNA 3 years, 5 months ago

B due to the way the question is asked. Poor wording. If it said exchange routing information then I'd say omp.

upvoted 2 times

khanda 3 years, 10 months ago

DTLS is correct

upvoted 1 times

Nyck 3 years, 11 months ago

"which protocol is used". Otherwise they would have said : Routing protocol. So, DTLS is the only one possible. B

upvoted 1 times

Nyck 3 years, 11 months ago

"which protocol is used". Otherwise they would have said : Routing protocol. So, DTLS is the only one possible. BDont be so sure they would have said it like that.. questions are written by global community participating in the Cisco SME program and not dedicated Cisco employees anymore. Typos and other mistakes are often overlooked when reviewing the questions before they are released into the exam pool

upvoted 1 times

MerlinTheWizard 2 years, 8 months ago

Dont be so sure they would have said it like that.. questions are written by global community participating in the Cisco SME program and not dedicated Cisco employees anymore. Typos and other mistakes are often overlooked when reviewing the questions before they are released into the exam pool

upvoted 1 times

A_Wolf 4 years ago

DTLS – between vSmarts, vManage and vBond permanently DTLS – between vSmart to vEdge permamently (DTLS or TLS). DTLS – between vBond to vEdge temporarily during vEdge onboarding. OMP – Only carries routing information between vSmart and vEdges and vSmart to vSmart vBond orchestrators always use DTLS tunnels to establish control connections with other devices, so they always use UDP. The UDP port is 12346

upvoted 2 times

Speirsington 4 years, 1 month ago

DTLS: "vpn 0 interface tunnel-interface control-connections—Attempt to establish a DTLS or TLS control connection for a TLOC (on vEdge routers only). This is the default behavior. " https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#wp4894365670

upvoted 2 times

CCNPWILL 4 years, 2 months ago

Not a good question. I would go with B though. vManage directly to edge device is NOT OMP for example when distributing a localized policy. All devices have at minimum DTLS connection to one another. Excluding the vBond after the edge gets authenticated.

upvoted 1 times

CesarVergaraGalindo 4 years, 4 months ago

B is correct

upvoted 4 times

isaacmejia 4 years, 7 months ago

A simple "show control connection" from a Vedge will answer this question, in my opinion is taking about connection from vedges to controlllers, So we are taking DTLS

upvoted 2 times

mithradel 4 years, 9 months ago

OMP (Overlay Management Protocol)—The OMP protocol is a routing protocol similar to BGP that manages the Cisco SD-WAN overlay network. OMP runs inside DTLS control plane connections and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the Cisco vSmart Controller and the vEdge routers and carries only control plane information. The Cisco vSmart Controller processes the routes and advertises reachability information learned from these routes to other vEdge routers in the overlay network.

upvoted 2 times

Maddy80 4 years, 9 months ago

The control connection means " Vsmart to Vedge " Communication , so OMP is the correct Answer .Agree. The keyword is "CONTROL". OMP is the one.There is a difference between Control Connection and Control Protocol...

upvoted 2 times

Maddy80 4 years, 9 months ago

The control connection means " Vsmart to Vedge " Communication , so OMP is the correct Answer .

upvoted 2 times

Mr_Cipher 4 years, 7 months ago

Agree. The keyword is "CONTROL". OMP is the one.

upvoted 1 times

Mr_Cipher 4 years, 7 months ago

Agree. The keyword is "CONTROL". OMP is the one.There is a difference between Control Connection and Control Protocol...

upvoted 1 times

Nalla123 3 years, 4 months ago

There is a difference between Control Connection and Control Protocol...

upvoted 1 times

Almanac 4 years, 9 months ago

DTLS is also a valid answer. because OMP is only running between vSmart to vSmart and vEdge to vSmart not across SD-WAN Devices.

upvoted 3 times

Question #168 *Topic 1*

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

A. AWS

B. Azure

C. VMware vCenter

D. OpenStack

E. IBM Cloud

Suggested Answer: *C, D*

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

Community vote distribution



nbvolz Most Recent 1 year, 10 months ago

Lifecycle management: VMware vCenter, OpenStack

upvoted 3 times

MikeyPher 2 years, 6 months ago

C and D

upvoted 2 times

khanda 3 years ago

Lifecycle management: VMware vCenter, OpenStack

upvoted 2 times

A_Wolf 3 years, 6 months ago

C & D A and B are not lifecycle management products. C and D is the correct answer. See table 2 (last line in the table) in the referenced document.

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

upvoted 3 times

CCNPWILL 3 years, 8 months ago

Correct

upvoted 2 times

DBla 3 years, 10 months ago

A and B are not lifecycle management products. C and D is the correct answer. See table 2 (last line in the table) in the referenced document.

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

upvoted 2 times

CesarVergaraGalindo 3 years, 10 months ago

A, B is CorrectLifecycle management VMware vCenter, OpenStack

upvoted 1 times

CesarVergaraGalindo 3 years, 10 months ago

A, B is Correct

upvoted 1 times

nihithp 3 years, 9 months ago

Lifecycle management VMware vCenter, OpenStack

upvoted 3 times

CCNPCollab1297 4 years, 1 month ago

A & B. AWS and Azure are supported by WAN Edge cloud routers. Read the link above.

upvoted 1 times

CCNPCollab1297 4 years, 1 month ago

A & B. AWS and Azure are supported by WAN Edge cloud routers. Read the link above.I tried to retract this but couldn't, C & D are correct.

upvoted 1 times

CCNPCollab1297 4 years ago

I tried to retract this but couldn't, C & D are correct.

upvoted 3 times

go_Corona_go 4 years, 3 months ago

Given Answer is correct. Check on the provided link. Dont get it confused with the supported Hypervisor (VMware ESXi and KVM) it runs on !!

upvoted 3 times

Question #169 *Topic 1*

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

A. authenticated DTLS

B. authenticated HTTPS

C. JSON Inspector interface

D. HTTP inspector interface

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

Eliasmiranda Most Recent 1 year, 11 months ago

B is the answer https://developer.cisco.com/docs/sdwan/#!authentication/how-to-authenticate

upvoted 1 times

A_Wolf 2 years, 6 months ago

GET https://{vmanage-ip-address}/dataservice/device/

upvoted 2 times

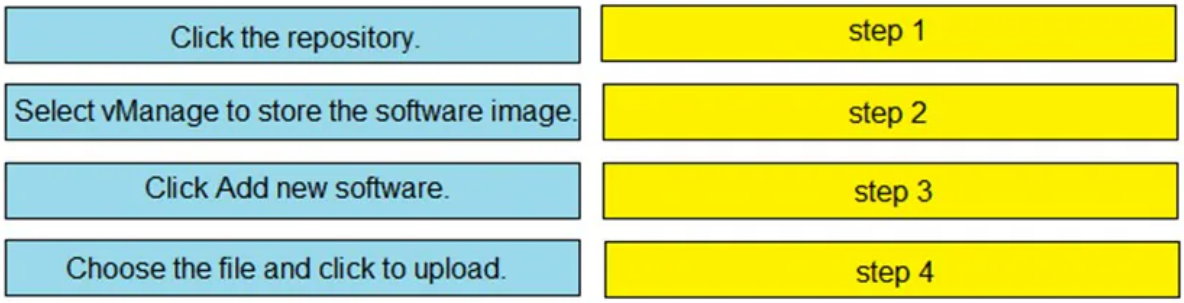
Question #170 *Topic 1*

DRAG DROP -

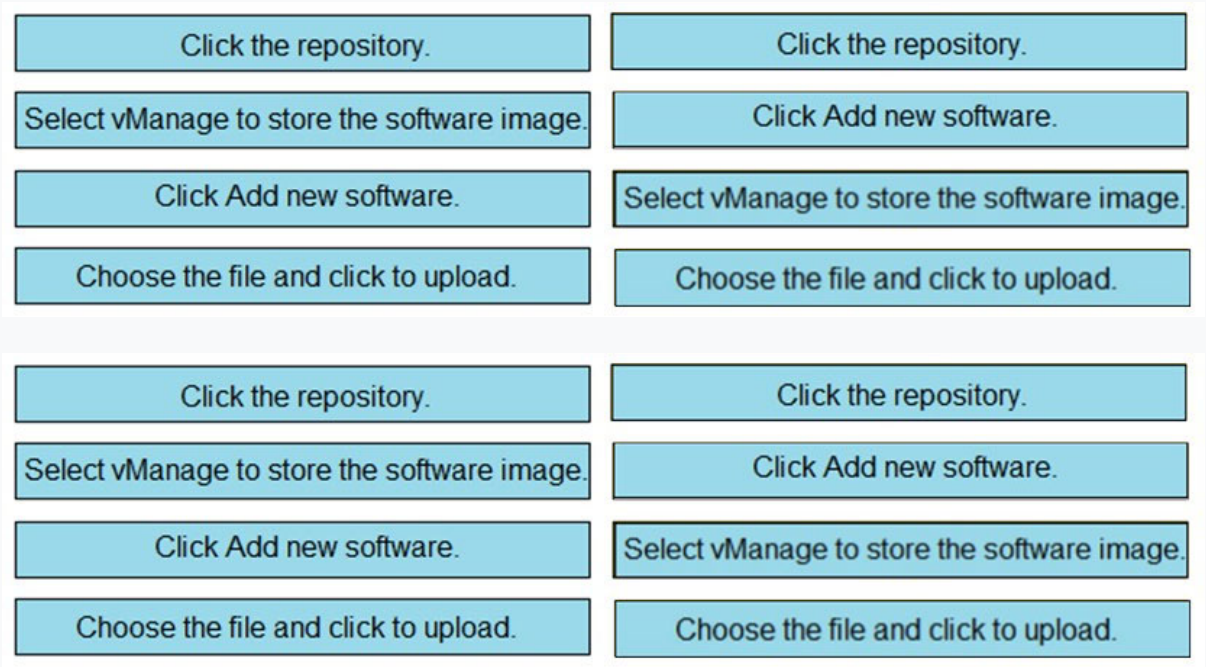
Drag and drop the steps from the left into the order on the right to upload software on vManage repository that is accessible from Maintenance > Software

Repository.

Select and Place:



Suggested Answer:



Reference: https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/vManage-Help/vmanage-help-17-2.pdf

CCNPWILL Highly Voted 5 years, 3 months ago

1. Click the Repository button located in the title bar. 2. Click Add New Software 3. Select the location to store the software image: 4. Click Upload to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.the answer presented is correct

upvoted 8 times

CCNPWILL Highly Voted 5 years, 3 months ago

1. Click the Repository button located in the title bar. 2. Click Add New Software 3. Select the location to store the software image: 4. Click Upload to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.

upvoted 8 times

CCNPWILL 5 years, 3 months ago

the answer presented is correct

upvoted 3 times

mikidvd51 1 year, 9 months ago

What the hack is this drag-n-drop question about ? Should I memorize GUI menus and submenus and where is which button? This is stupid cisco approach.Once they change menu and buttons after OS version upgrade, do they update also CERT quesitons?

upvoted 4 times

mikidvd51 1 year, 9 months ago

What the hack is this drag-n-drop question about ? Should I memorize GUI menus and submenus and where is which button? This is stupid cisco approach.

upvoted 4 times

mikidvd51 Most Recent 1 year, 9 months ago

Once they change menu and buttons after OS version upgrade, do they update also CERT quesitons?

upvoted 1 times

khanda 4 years ago

Answer presented is correct.

upvoted 1 times

Question #171 *Topic 1*

A network administrator is configuring an application-aware firewall between inside zones to an outside zone on a WAN Edge router using vManage GUI. Which kind of inspection is performed when the `inspect` action is used?

A. Layer 7 inspection for TCP and Layer 4 inspection for UDP

B. stateful inspection for TCP and stateless inspection of UDP

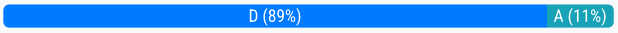
C. IPS inspection for TCP and Layer 4 inspection for UDP

D. stateful inspection for TCP and UDP

Suggested Answer: *D*

Official Answer: D

Community vote distribution



msstanick Most Recent 7 months, 1 week ago

Another "clever" question. The app-aware is due to DPI, while question is only about ZBFW inspection - which is just a stateful inspection for TCP and UDP so D

upvoted 1 times

uzbin 1 year, 4 months ago

AAR FW inspects at layer 7 so must be A...

upvoted 1 times

5c1f681 2 years, 1 month ago

D answer

upvoted 1 times

Barti1 2 years, 8 months ago

D is correct answer

upvoted 1 times

Nandhujoe 3 years, 3 months ago

D. stateful inspection for TCP and UDP

upvoted 1 times

Roger95 3 years, 8 months ago

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/enterprise-firewall.html

upvoted 4 times

gambit_777 4 years, 7 months ago

Looks to be correct one.

upvoted 1 times

Question #172 *Topic 1*

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

A. WAN Edge routers

B. vSmart controllers

C. vBond controllers

D. vManage NMS

Suggested Answer: *D*
Official Answer: D

Currently there are no comments in this discussion, be the first to comment!

Question #173 *Topic 1*

What is a description of vManage NMS?

A. A cluster consists of a minimum of two vManage NMSs.

B. It is a software process on a dedicated WAN Edge router in the network.

C. A cluster requires device templates to be created on an attached to the same server.

D. It is accessible only from VPN 512 (the management VPN).

Suggested Answer: *D*

Official Answer: D

Community vote distribution

C (100%)

RexChen Highly Voted 4 years, 2 months ago

I think it's C https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Step_2__Deploy_the_vManage_NMS_7856.xmlIt is not only accessible from VPN 512, this can also be accessed from VPN 0

upvoted 14 times

RexChen Highly Voted 4 years, 2 months ago

I think it's C https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Step_2__Deploy_the_vManage_NMS_7856.xml

upvoted 14 times

NetArch_Teck 2 years, 1 month ago

It is not only accessible from VPN 512, this can also be accessed from VPN 0

upvoted 1 times

CCNPCollab1297 4 years, 1 month ago

C is correct. From the link above: "Note that you must configure each Cisco vManage in the cluster individually, from that vManage server itself. You cannot create a vManage configuration template on one vManage server and attach other Cisco vManage to that device template."

upvoted 12 times

Aldebeer Most Recent 1 year, 8 months ago

It is C

upvoted 1 times

nbvolz 2 years ago

I love how we still don't know. C? D?

upvoted 1 times

NetArch_Teck 2 years, 1 month ago

A Cluster requires device templates to be created on at least 3 instances for Redundancy | HA | Uptime Talking from experience, VManage NMS heavily relies on templates to be attached to server instances within a cluster, otherwise the instances would not be able to form said cluster. The other three are invalid:- A minimum of 3 instances are needed for a cluster VManage NMS does not operate on a WAN Edge Router VPN 0 and VPN 512 can access the VManage NMS Option C is the only valid choice here!

upvoted 4 times

bsk 2 years, 6 months ago

As per RexChen and CCNPCollab, the Answer is C only. Because you need 3 instance minimum for VManage cluster, and it can be accessed by VPN 0 or VPN 512. That makes A and D incorrect. Also VManage is not a software process running on WAN Edge device. This makes B incorrect. So I am going with C as you require templates to configure VManage.

upvoted 2 times

Eliasmiranda 2 years, 11 months ago

D is correct. Nowhere in the documentation does it state that a device template associated with vManage is required to create a cluster. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-741440.html https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.1/Administration/Cluster_Managementno...it's not D as it can be accessed by Transport as wellC may be worded poorly, and doesn't mean templates are required. It means that if a template is used, the template must be attached only to the same vManage server that it was created on. All other answers are definitely wrong, and this seems to be what they meant.

upvoted 2 times

Eliasmiranda 2 years, 11 months ago

D is correct. Nowhere in the documentation does it state that a device template associated with vManage is required to create a cluster. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-741440.html https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.1/Administration/Cluster_Management

upvoted 2 times

Mookz 2 years, 10 months ago

no...it's not D as it can be accessed by Transport as well

upvoted 2 times

timtgh 1 year, 11 months ago

C may be worded poorly, and doesn't mean templates are required. It means that if a template is used, the template must be attached only to the same vManage server that it was created on. All other answers are definitely wrong, and this seems to be what they meant.

upvoted 1 times

khanda 3 years ago

C is close but not quite: "You cannot create a vManage configuration template on one vManage server and attach other Cisco vManage to that device template."

upvoted 1 times

Rita7 3 years, 1 month ago

You can access the vManage NMS from VPN 0 (the WAN transport VPN) and from VPN 512 (the management VPN). https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_17.1/vManage_NMS_Product_Help

upvoted 2 times

gem 3 years, 3 months ago

I think A is simple and correct

upvoted 2 times

gem 3 years, 3 months ago

I think A is simple and correcthttps://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/manage-cluster.html Above says that a cluster has a minimum of 3 servers, not 2.

upvoted 2 times

JoeMomma1126 3 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/manage-cluster.html Above says that a cluster has a minimum of 3 servers, not 2.

upvoted 2 times

Almanac 3 years, 7 months ago

C is not correct. it negates the statement on the link you guys provided. So D still the closest correct answer

upvoted 1 times

Stiga 3 years, 7 months ago

D: You can access the vManage NMS from VPN 0 (the WAN transport VPN) and from VPN 512 (the management VPN

upvoted 2 times

Stiga 3 years, 7 months ago

D: You can access the vManage NMS from VPN 0 (the WAN transport VPN) and from VPN 512 (the management VPND says 512 only, so it is incorrect.

upvoted 2 times

ngabor 3 years, 7 months ago

D says 512 only, so it is incorrect.

upvoted 4 times

DBla 3 years, 10 months ago

I have to correct myself. Since my last post I was able to log in to vManage on vpn 0 as well (after removing a well hidden acl from the lab). C isn't correct either, but it is the closest to be.:)

upvoted 2 times

DBla 3 years, 10 months ago

vManage can operate without templates attached to itself. You can configure them from CLI too. I wasn't able to access our vManage even if I used allow-service on the vpn0 interface.

upvoted 1 times

CesarVergaraGalindo 3 years, 10 months ago

C is Correct

upvoted 2 times

RexChen 4 years, 2 months ago

if you set allow-service in vpn 0 ,it's also accessible

upvoted 1 times

Question #174 *Topic 1*

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 ɹ€ECMP limitɹ€

B. configure ɹ€Send Backup Pathsɹ€

C. configure ɹ€Number of Paths Advertised per Prefixɹ€

D. configure ɹ€Overlay AS Numberɹ€

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

cwauch Most Recent 1 year, 4 months ago

Overlay AS Path: Adding an overlay AS path can help verify that routes learned over the fabric are not sent back into the fabric unless redistributed to a protocol that doesn't carry AS path. https://www.google.com/search?q=How+to+avoid+LAN+routes+from+being+redistributed+back+into+OMP&rlz=1C1CHBF_enUS860US860&oq=How+to+avoid+LAN+routes+from+being+redistributed+back+into+OMP&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQIRiPAjIHCAIQIRiPAtIBCjE1OTE0ajFqMTWoAgiwAgHxBZnj131ko-lb&sourceid=chrome&ie=UTF-8

upvoted 1 times

Question #175 *Topic 1*

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

A. Alarms

B. Events

C. Audit log

D. Network

Suggested Answer: *D*

Official Answer: D

Community vote distribution

A (100%)

ramjam Highly Voted 5 years, 2 months ago

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

upvoted 12 times

elninio13 2 years, 9 months ago

I dont understand why so basic questions are answered wrongly and nobody corrected them yet....I think this is why they can advertise this reviewer website openly to the public, IYKYK

upvoted 2 times

elninio13 2 years, 9 months ago

I dont understand why so basic questions are answered wrongly and nobody corrected them yet....

upvoted 2 times

Loi2525 Most Recent 2 years ago

I think this is why they can advertise this reviewer website openly to the public, IYKYK

upvoted 1 times

MANDY13 3 years, 1 month ago

Alarms

upvoted 1 times

khanda 4 years ago

It's under "Alarms", lab tested.

upvoted 4 times

rockme27m 4 years, 9 months ago

should be alarm

upvoted 1 times

nihithp 5 years ago

1.Alarms

upvoted 4 times

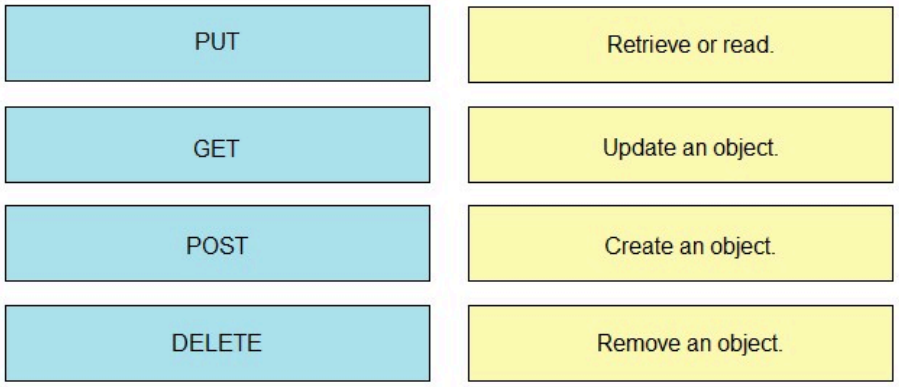
Question #176 *Topic 1*

DRAG DROP -

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

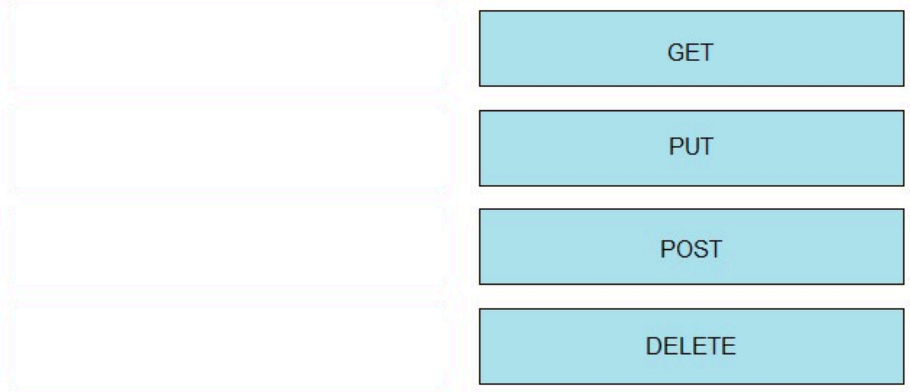
Select and Place:

Answer Area

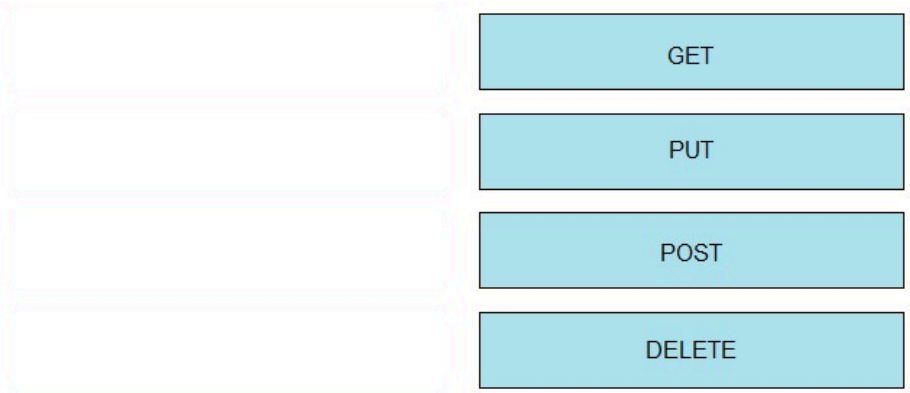


Suggested Answer:

Answer Area



Answer Area



incog Most Recent 1 year, 12 months ago

anser is correct: https://restfulapi.net/rest-put-vs-post/#:~:text=The%20POST%20method%20is%20used,PUT%20method%20is%20idempotent.

upvoted 1 times

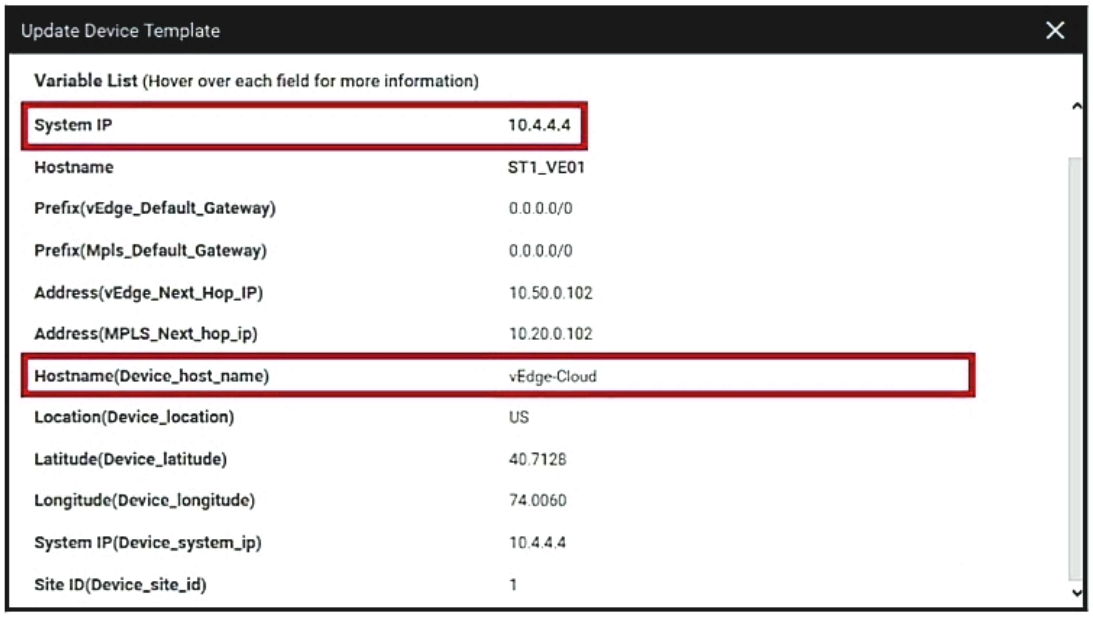
Refer to the exhibit. vManage logs are available for the past few months. A device name change was deployed mistakenly at a critical site. How is the device name change tracked by operations and design teams?

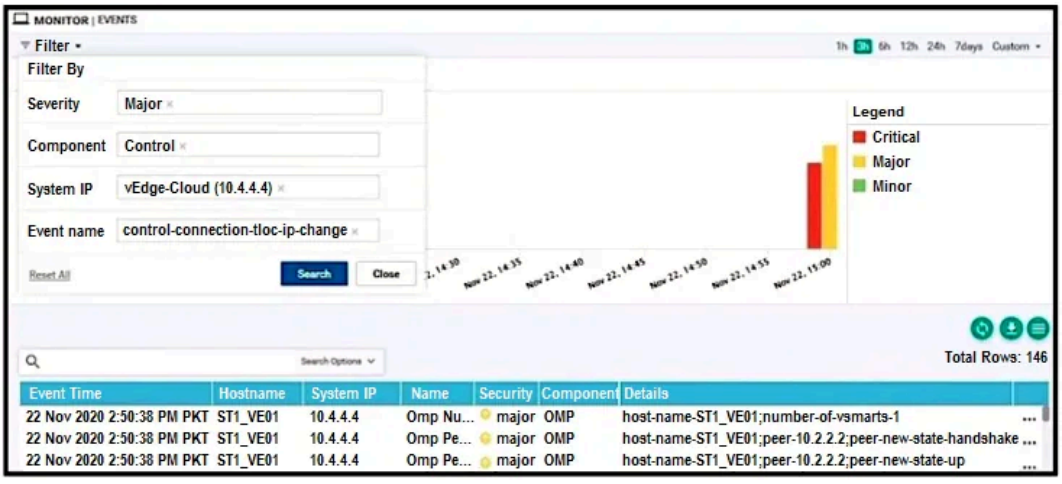
A.

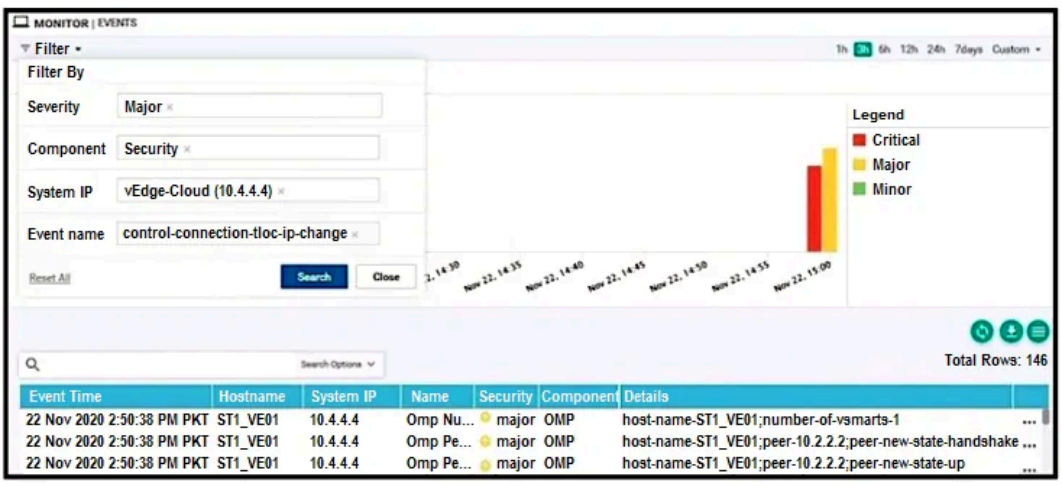
B.

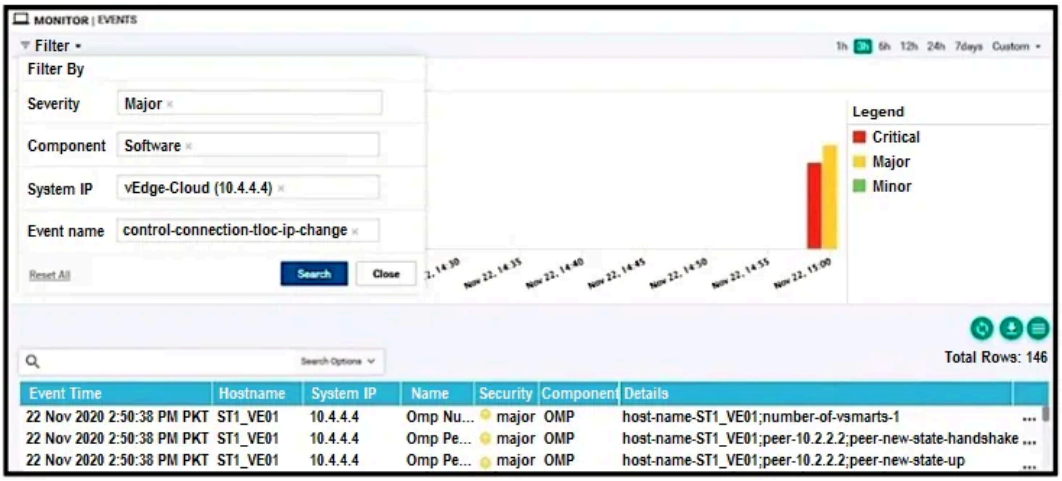
C.

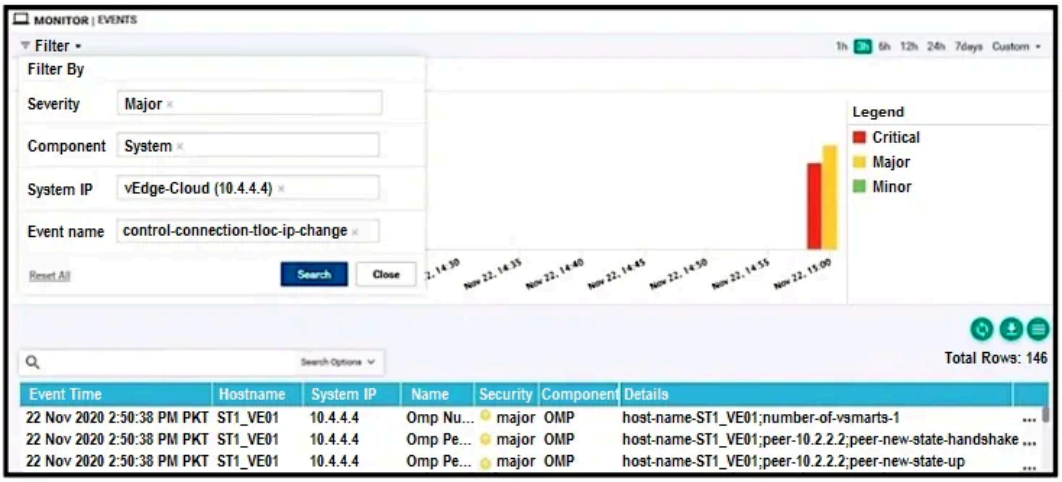
D.











Suggested Answer:
Official Answer: B

John662266 Most Recent 1 year, 8 months ago

D is correct..

upvoted 1 times

Rosh8787 1 year, 10 months ago

Option D is the correct answer since Hostname is part of System configuration

upvoted 2 times

Aldebeer 2 years, 9 months ago

Aha, the pictures are the same what are you discussing about ?

upvoted 2 times

NetArch_Teck 3 years, 1 month ago

The Device Name is tracked by the System Field. This field holds details about the ID of said device. D is the only option that displays this... B is incorrect!

upvoted 3 times

Bone02 3 years, 5 months ago

Something is wrong. Every picture are the same.Take a closer look. Component is different. Should be System -> DIt is the same picture, at least at the time of writing

upvoted 4 times

Bone02 3 years, 5 months ago

Something is wrong. Every picture are the same.

upvoted 4 times

Alchobashko 3 years, 5 months ago

Take a closer look. Component is different. Should be System -> D

upvoted 4 times

Alchobashko 3 years, 5 months ago

Take a closer look. Component is different. Should be System -> DIt is the same picture, at least at the time of writing

upvoted 4 times

MerlinTheWizard 3 years, 2 months ago

It is the same picture, at least at the time of writing

upvoted 1 times

AW57 3 years, 8 months ago

D should be correct one

upvoted 2 times

khanda 4 years ago

D is the correct answer, tested it.

upvoted 3 times

RREVECO 4 years, 2 months ago

ANSWER "D" -System I did this on REAL ENVIRONMENT Name: System Confirmation Severity: minor Component: System

upvoted 4 times

jeremiahwolfe 4 years, 4 months ago

D - System I did this in my lab. Name: System Commit Severity: minor Component: System

upvoted 2 times

Speirsington 4 years, 7 months ago

100% System - I tested it on my own vmanage. Severity is only minor

upvoted 3 times

DBla 4 years, 10 months ago

They are filtering for the control-connection-tloc-ip-change event. Tloc Ip change causes control connection reset, which should be under Control component.

upvoted 1 times

CesarVergaraGalindo 4 years, 10 months ago

D is CorrectThe Component is System - verified in a Sandbox. But changing the Device Name only generates an event of Severity MinorTo clarify on my comments above, two System events were generated for the name change - a Severity Major for "Pseudo Commit Status" and a Severity Minor for "System Commit"

upvoted 1 times

CesarVergaraGalindo 4 years, 10 months ago

D is Correct

upvoted 1 times

JS71 4 years, 10 months ago

The Component is System - verified in a Sandbox. But changing the Device Name only generates an event of Severity MinorTo clarify on my comments above, two System events were generated for the name change - a Severity Major for "Pseudo Commit Status" and a Severity Minor for "System Commit"

upvoted 3 times

JS71 4 years, 10 months ago

The Component is System - verified in a Sandbox. But changing the Device Name only generates an event of Severity Minor

upvoted 3 times

JS71 4 years, 10 months ago

To clarify on my comments above, two System events were generated for the name change - a Severity Major for "Pseudo Commit Status" and a Severity Minor for "System Commit"

upvoted 2 times

lollo1234 4 years, 11 months ago

Don't get it. I tried making a hostname change and the Component should be System with name "Pseudo Commit Status" and severity Major. So maybe D?

upvoted 1 times

Question #178 *Topic 1*

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 .bin

B. one file for vManage, one for vSmart, and one for vBond + WAN Edge Cloud with extension .bin

C. one file for vManage and one file for all other devices with extension tar.gz

D. one file for vManage, one for vSmart, and one for vBond + WAN Edge Cloud with extension tar.gz

Suggested Answer: *D*
Official Answer: D

Community vote distribution
C (100%)

JS71 Highly Voted 4 years, 10 months ago
C is correct - verify this via https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.4
upvoted 9 times

regissan Most Recent 1 year, 7 months ago
https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html
upvoted 1 times

rubendrios 1 year, 9 months ago
C is correct. the question says UPDATE. in software.cisco.com.co > SDWAN> SD-WAN Software Update is the answer.
https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.2
upvoted 1 times

merlow6674 2 years ago
D. one file for vManage, one for vSmart, and one for vBond + WAN Edge Cloud with extension tar.gz This is because, typically, the SD-WAN controllers and devices each require their own specific software images, and the .tar.gz format is commonly used for Cisco SD-WAN software upgrades.
upvoted 1 times

thomazmr 2 years, 6 months ago
Correta C
upvoted 1 times

wcorrea 3 years, 9 months ago
C is correct
upvoted 2 times

ldro 3 years, 9 months ago
C is correct
upvoted 3 times

khanda 4 years ago
C is correct, documentation on the comments.
upvoted 3 times

kcobain87 4 years, 1 month ago
C for sure
upvoted 2 times

majepiga 4 years, 3 months ago
C - I did it some months ago in our production sdwan devices
upvoted 2 times

Almanac 4 years, 7 months ago
correct answer is C. Letter D is when you deploy the sdwan for the first time
upvoted 2 times

MajorSalieri 4 years, 7 months ago
C is Correct according to Cisco documentation https://software.cisco.com/download/home/286320995/type/286321394/release/20.3.4

upvoted 2 times

CesarVergaraGalindo 4 years, 10 months ago

C is Correct

upvoted 1 times

MasterALX 4 years, 11 months ago

In the SD-WAN 2.0 (ENSDWI20) course Lab 13: Perform Cisco SD-WAN Software Upgrade there was 1 image for vManage and 1 image for vSmarts, vBonds and vEdges. Therefore I would say C is the correct answer.

upvoted 1 times

Question #179 *Topic 1*

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 serial

B. request vedge-cloud activate chassis-number token

C. request vedge-cloud activate serial token

D. request vedge-cloud activate chassis-number organization

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

JS71 Highly Voted 4 years, 10 months ago

B is correct - see https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/operational-cmd.html#wp1526475327

upvoted 5 times

Rosh8787 Most Recent 1 year, 10 months ago

As per below syntax, option B is the correct answer request vedge-cloud activate chassis-number number token token

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/operational-cmd.html#r_request_vedge_3137.xml

upvoted 1 times

Erik_N 3 years, 8 months ago

For physical device: request vedge [add | delete] serial-num chassis-num For cloud router: request vedge-cloud activate chassis-number token

upvoted 3 times

khanda 4 years ago

B is correct.

upvoted 1 times

Question #180 *Topic 1*

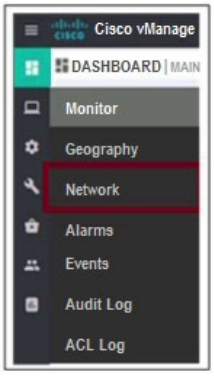
Company ABC has decided to deploy the controllers using the On-Prem method. How does the administrator upload the WAN Edge list to the vManage?

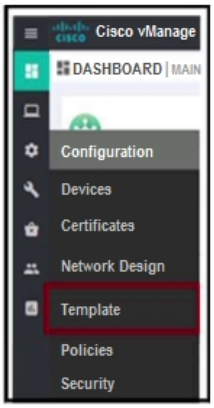
A.

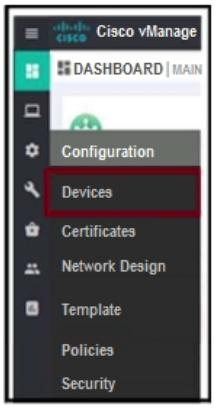
B.

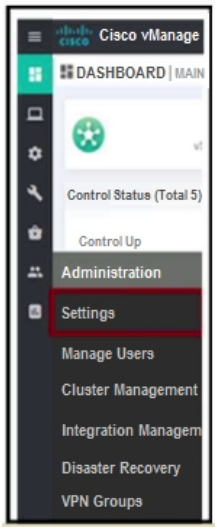
C.

D.









Suggested Answer:
Official Answer: C

CCNPWILL 4 years, 8 months ago
Configuration > Devices > Upload WAN Edge List. .. CorrectExcept they are talking about Controllers, but it's the same thing and place, just need to change tab to Controllers and add Controller.
upvoted 1 times

CCNPWILL 4 years, 8 months ago
Configuration > Devices > Upload WAN Edge List. .. Correct
upvoted 1 times

konspali Most Recent 2 years, 1 month ago
Except they are talking about Controllers, but it's the same thing and place, just need to change tab to Controllers and add Controller.
upvoted 1 times

Question #181 *Topic 1*

An engineer is adding a tenant with location ID 123456789 in vManage. What is the maximum number of alphanumeric characters that is accepted in the tenant name field?

A. 8

B. 256

C. 128

D. 64

Suggested Answer: *C*
Official Answer: C

MerlinTheWizard Highly Voted 1 year, 8 months ago
A perfect question that accurately portraits our understanding and ability to deploy and operate sdwan
upvoted 15 times

spamke 3 years, 3 months ago
correct, 128, but proper link is: https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Administration/Tenant_Management
upvoted 2 times

JS71 3 years, 4 months ago
Maximum characters is 128 - see https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html#wp4742550630
upvoted 1 times

Question #182 *Topic 1*

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-plane availability when other controllers are being updated.

B. Upgrade and reboot are performed first on vManage, then on vBond, then on vSmart, and finally on the Cisco WAN Edge devices.

C. 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.

D. Upgrade and reboot are performed first on vBond, then on vSmart, and finally on the Cisco WAN Edge devices.

Suggested Answer: *B*

Reference: https://community.cisco.com/t5/networking-documents/cisco-sd-wan-software-upgrade-best-practices/ta-p/4101848

Community vote distribution

B (100%)

Aldebeer Most Recent 1 year, 9 months ago

it is B

upvoted 1 times

kk_learn 2 years, 6 months ago

B. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html#best-practices-for-software-upgrades

upvoted 1 times

Idro 2 years, 9 months ago

B is correct

upvoted 2 times

Question #183 *Topic 1*

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

A.

B.

C.

D.

```
vpn 0
 interface eth1
  ip address 10.50.0.1/24
  tunnel-interface
   color default
```

```
vpn 0
 interface eth1
  ip address 10.50.0.1/24
  tunnel-interface
   color biz-internet
```

```
vpn 0
 interface eth1
  ip address 10.50.0.1/24
  tunnel-interface
   color public-internet
```

```
vpn 0
 interface eth1
  ip address 10.50.0.1/24
  tunnel-interface
   color mpls
```

Suggested Answer:
Official Answer: A

D3n1s Most Recent 6 months, 2 weeks ago

A, B and C cover the requirement based on Public colors logic

upvoted 1 times

Arsenal16 1 year, 6 months ago

Use biz-internet for business or enterprise-grade Internet connections. Use public-internet for general public Internet connections.

upvoted 1 times

Aldebeer 1 year, 8 months ago

B and C both correct, it depends on how you name your Internet feed?

upvoted 1 times

pachosinfortuna 1 year, 11 months ago

Colors are already named as MPLS and Internet. So the only option that matches one of these colors is option D, but D does not fulfil the rest of the requirements. I would go with A in this case.

upvoted 1 times

NetArch_Teck 2 years ago

Answer [A] Leaving the TLOC color as the default is still one of the public colors (meaning you don't need to define a preferred color, unless required or stated in the question) The default color tunnel can still build controlled connections (DTLS) to other SD-WAN devices, Options B and C are practically the same, this lead me to believe neither of those are valid for the question. Further Info - Link:- https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214148-configure-connectivity-between-different.html

upvoted 1 times

BrentL 2 years, 2 months ago

I can't make sense of this question really. B and C are basically same thing and they said not MPLS. So I'd go with A even though you actually don't configure color on the vManage or controllers normally. There are control connections established using the colors defined on remote end so if default is used on controllers I think it would be just like not having anything on them but won't have my lab spun back up for a few weeks to verify.

upvoted 2 times

moraist 2 years, 6 months ago

I agree with A, because the engineer is configuring the controller not a WAN Edge. In the controllers we don't use colors.From design guide (https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html): "The color attribute applies to WAN Edge routers or vManage and vSmart controllers". So, controllers are using colors.Also, there is no color default.The default color exists and is used by the controller when a specific color is not set. If you have a lab or real environment, please check your controller's VPN 0 configuration. The controller supports color, but it is not considered best practice to change it. This is an example of vSmart's control connection. 0 vmanage 10 0 223.1.1.12 12346 223.1.1.10 12346 1.1.1.10 dtls default default 223.1.1.10

upvoted 3 times

moraist 2 years, 6 months ago

I agree with A, because the engineer is configuring the controller not a WAN Edge. In the controllers we don't use colors.

upvoted 3 times

kk_learn 2 years, 6 months ago

From design guide (https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html): "The color attribute applies to WAN Edge routers or vManage and vSmart controllers". So, controllers are using colors.

upvoted 1 times

kk_learn 2 years, 6 months ago

From design guide (https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html): "The color attribute applies to WAN Edge routers or vManage and vSmart controllers". So, controllers are using colors.Also, there is no color default.The default color exists and is used by the controller when a specific color is not set. If you have a lab or real environment, please check your controller's VPN 0 configuration. The controller supports color, but it is not considered best practice to change it. This is an example of vSmart's control connection. 0 vmanage 10 0 223.1.1.12 12346 223.1.1.10 12346 1.1.1.10 dtls default default 223.1.1.10

upvoted 1 times

kk_learn 2 years, 6 months ago

Also, there is no color default.The default color exists and is used by the controller when a specific color is not set. If you have a lab or real environment, please check your controller's VPN 0 configuration. The controller supports color, but it is not considered best practice to change it. This is an example of vSmart's control connection. 0 vmanage 10 0 223.1.1.12 12346 223.1.1.10 12346 1.1.1.10 dtls default default 223.1.1.10

upvoted 2 times

kk_learn 2 years, 6 months ago

Also, there is no color default.

upvoted 2 times

moraist 2 years, 2 months ago

The default color exists and is used by the controller when a specific color is not set. If you have a lab or real environment, please check your controller's VPN 0 configuration. The controller supports color, but it is not considered best practice to change it. This is an example of vSmart's control connection. 0 vmanage 10 0 223.1.1.12 12346 223.1.1.10 12346 1.1.1.10 dtls default default 223.1.1.10

upvoted 1 times

kk_learn 2 years, 6 months ago

B. https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html The public colors are 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, public-internet, red, and silver.Reading this again, it could be C also (per my posted citation).

upvoted 1 times

kk_learn 2 years, 6 months ago

B. https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html The public colors are 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, public-internet, red, and silver.

upvoted 1 times

kk_learn 2 years, 6 months ago

Reading this again, it could be C also (per my posted citation).

upvoted 1 times

Jonycici 2 years, 8 months ago

correct is B

upvoted 1 times

Jonycici 2 years, 8 months ago

correct is Bwhy not "color public-internet" ?public internet is called biz-internet in SDWAN.No. Actually on sdwan environment, we have public-internet and biz-internet also.Ensdwi course used biz-internet. Several questions in exam used public-internet, both are public and both represent internet.. stupid question

upvoted 1 times

Eliasmiranda 2 years, 8 months ago

why not "color public-internet" ?

upvoted 1 times

Eliasmiranda 2 years, 8 months ago

why not "color public-internet" ?public internet is called biz-internet in SDWAN.No. Actually on sdwan environment, we have public-internet and biz-internet also.Ensdwi course used biz-internet. Several questions in exam used public-internet, both are public and both represent internet.. stupid question

upvoted 1 times

Tan_Singh 2 years, 7 months ago

public internet is called biz-internet in SDWAN.

upvoted 1 times

Tan_Singh 2 years, 7 months ago

public internet is called biz-internet in SDWAN.No. Actually on sdwan environment, we have public-internet and biz-internet also.Ensdwi course used biz-internet. Several questions in exam used public-internet, both are public and both represent internet.. stupid question

upvoted 1 times

williancm19 2 years, 2 months ago

No. Actually on sdwan environment, we have public-internet and biz-internet also.

upvoted 1 times

MerlinTheWizard 2 years, 2 months ago

Ensdwi course used biz-internet. Several questions in exam used public-internet, both are public and both represent internet.. stupid question

upvoted 1 times

Question #184 *Topic 1*

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.)

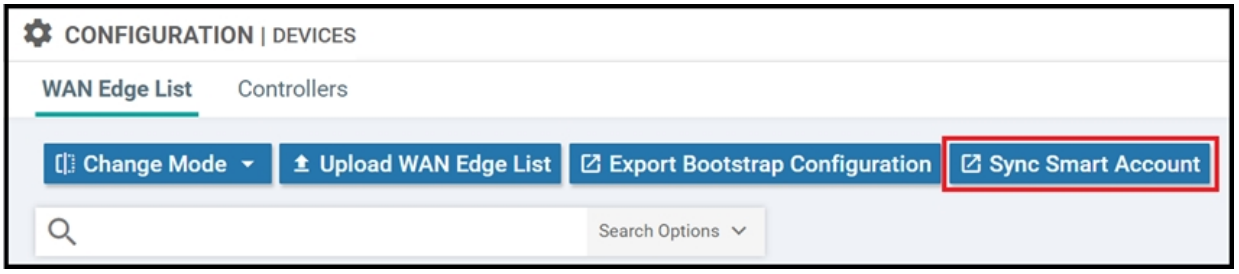
A.

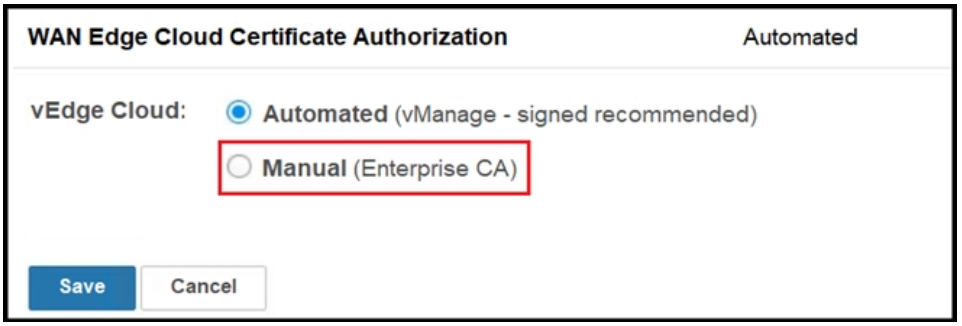
B.

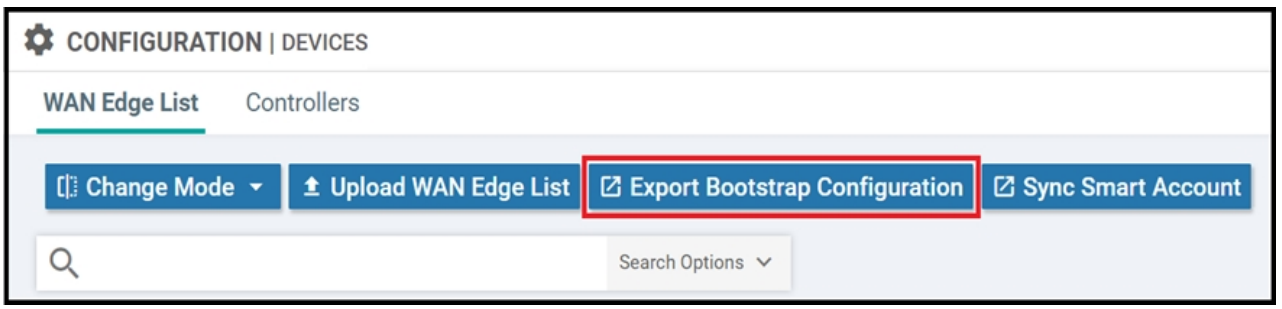
C.

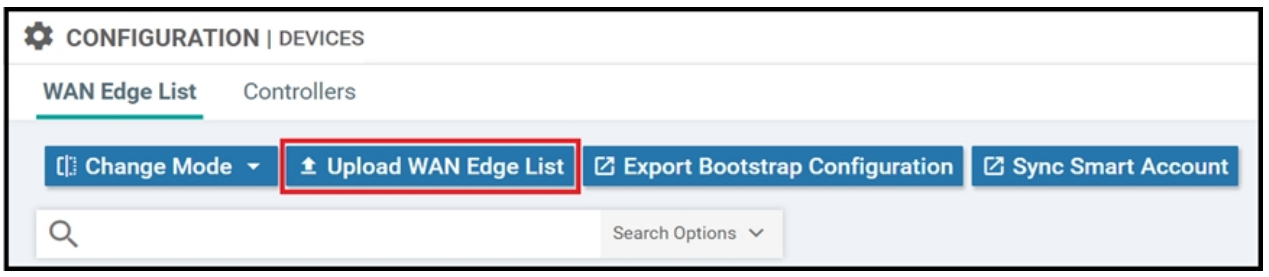
D.

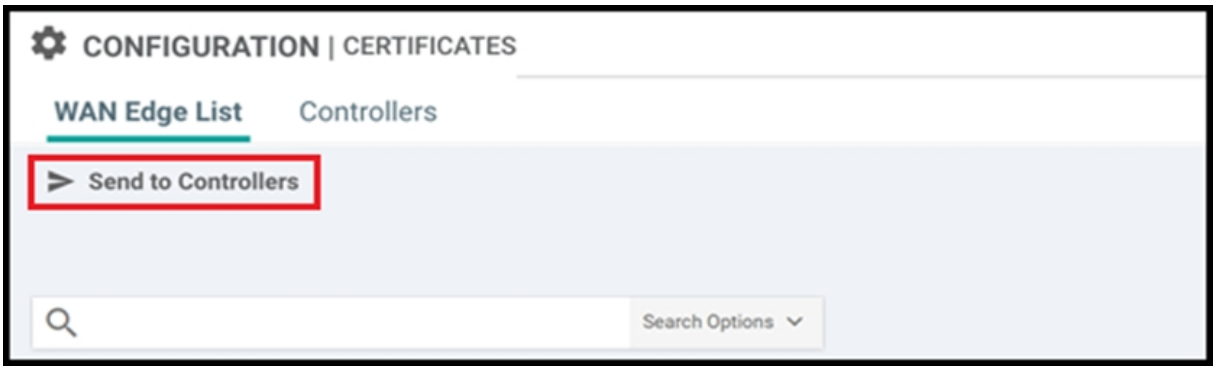
E.











Suggested Answer:
Official Answer: AD

MerlinTheWizard Highly Voted 3 years, 2 months ago
Briliant wording.. I got furious with these questions at the exam..
upvoted 7 times

AonDuine Most Recent 2 months, 1 week ago
Make WAN Edge list available to vManage = Sync Smart Account or Upload WAN Edge List Send to Controllers = after that
upvoted 1 times

34b33cd 1 year, 8 months ago
Can someone confirm the right answer?
upvoted 1 times

mikidvd51 1 year, 9 months ago
Great! We have here group saying AE , group of saying DE and group of saying it is AD. What a straight forward question and procedure! One would say.. Thank You cisco!
upvoted 1 times

mohammad 1 year, 10 months ago
A,E PnP portal is cisco poral, so " from inside" or "on-prem" is not related to PnP. so we have 2 options : 1. Device list using PnP will be sync via smart account 2. Manually upload device list To transfer device information from Cisco PnP portal to Cisco SD-WAN Manager, sync your Smart Account or Virtual account in Cisco SD-WAN Manager. You need Cisco credentials of the Virtual Account administrator role for this step. For more information about uploading the WAN Edge router serial numbers, see Upload WAN Edge Router Serial Numbers from Cisco Smart Account.
upvoted 1 times

Stanleymahamadi 2 years, 2 months ago
D and E are correct
upvoted 2 times

Networkchamp87 2 years, 3 months ago
Typo below : "sync to smart account"
upvoted 1 times

Knowledge33 2 years, 6 months ago
D&E are correct. Did it in LAB. We don't need to sync smart account. We don't need the vmanage to access internet.
upvoted 1 times

Networkchamp87 2 years, 3 months ago
D&E are correct. Sync to smart controller doesn't bring down the WAN edge list, Auto Sync Option: Admin> settings > PnP Connect sync would be correct.
upvoted 1 times

Knowledge33 2 years, 6 months ago
D&E are correct. Did it in LAB. We don't need to sync smart account. We don't need the vmanage to access internet.There are two ways, that you say is one but the key word it is that the vManage can access to PnP portal. The D options it is the manual way but you can upload the cEdge list from PnP and then send to controller so A and E are correct
upvoted 1 times

Seba_o_s 2 years, 6 months ago
There are two ways, that you say is one but the key word it is that the vManage can access to PnP portal. The D options it is the manual way but you can upload the cEdge list from PnP and then send to controller so A and E are correct
upvoted 3 times

Outlaw_87 2 years, 7 months ago
It says "on-prem method" and "pnp portal from inside". So why do we need "sync smart account"? I'll go with D and E.
upvoted 1 times

Seba_o_s 2 years, 6 months ago
A and D are correcto for me. The question say "while vManage can access the PnP portal from inside", so the vManage has access to PnP, that mean that can update the cEdge list manually and automatically
upvoted 2 times

Outlaw_87 2 years, 7 months ago
It says "on-prem method" and "pnp portal from inside". So why do we need "sync smart account"? I'll go with D and E.The key word is that the vManage has access to PnP, so you can upload the cEdge list directly from PnP and then send to controllersnot sure with the reply (If you give

internet acceso to vManage, also you can update the list in that way

upvoted 1 times

Seba_o_s 2 years, 6 months ago

The key word is that the vManage has access to PnP, so you can upload the cEdge list directly from PnP and then send to controllers

upvoted 1 times

Outlaw_87 2 years, 6 months ago

not sure with the reply (

upvoted 1 times

Seba_o_s 2 years, 6 months ago

If you give internet acceso to vManage, also you can update the list in that way

upvoted 1 times

colipto 3 years ago

D and E?

upvoted 1 times

Question #185 *Topic 1*

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

Suggested Answer: *B*
Official Answer: B

Currently there are no comments in this discussion, be the first to comment!

Question #186 *Topic 1*

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 included in a configured policy

D. if the image is uploaded by a WAN Edge device

Suggested Answer: *A*

Official Answer: A

Community vote distribution

B (100%)

MiraGod Highly Voted 2 years, 11 months ago

Correct answer is B, you can look at the following link for reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/maintain.html#task_hbp_kmd_ffb "If the VNF image is referenced by a service chain, it can't be deleted."

upvoted 12 times

alin93 Highly Voted 2 years, 9 months ago

If the VNF image is referenced by a service chain, it can't be deleted.

upvoted 5 times

AJMD Most Recent 1 year, 11 months ago

Correct B

upvoted 1 times

Question #187 *Topic 1*

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. Cisco AMP and Threat Grid

C. URL filtering and Umbrella DNS security

D. Snort IPS

Suggested Answer: *C*

Official Answer: C

Community vote distribution

B (100%)

ChrisCCNA Highly Voted 3 years, 5 months ago

B. Threat Grid is the only answer offering sandboxing.

upvoted 6 times

thomazmr Most Recent 2 years ago

B. Cisco AMP and Threat Grid

upvoted 1 times

NetArch_Teck 2 years, 7 months ago

The Correct Answer is B Threat Grid and Cisco AMP is based is the only answer here to fulfil the question!

upvoted 1 times

Nandhujoe 2 years, 9 months ago

B. Cisco AMP and Threat Grid

upvoted 1 times

wcorrea 3 years, 3 months ago

https://blogs.cisco.com/networking/enabling-amp-in-cisco-sd-wan NEW: Malware defense and sandboxing with Cisco AMP and AMP Threat Grid

upvoted 4 times

Question #188 *Topic 1*

An enterprise needs DIA on some of its branches with a common location ID: A042:B49C:D02E::72.
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 172.16.0.1/24 nat

C. vpn 0 ip route 0.0.0.0/0 vpn 0 vpn 1 interface ge0/1 ip address 172.16.0.1/24 nat

D. vpn 0 interface ge0/0 ip address 172.16.0.1/24 nat vpn 1 ip route 0.0.0.0/0 vpn 0

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

ChrisCCNA Highly Voted 2 years, 11 months ago
D is correct. Enable NAT on the transport interface. VPN 0 Create static route in the service VPN to direct traffic out of the NATed transport.
upvoted 6 times

NetArch_Teck Most Recent 2 years, 1 month ago
The Service VPN (1) has a default route to VPN 0 (WAN Transport) which requires NAT to be enabled to forward public/private traffic from WAN to LAN and vice versa Option D is the only answer here!
upvoted 2 times

Question #189 *Topic 1*

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

A. RHEL 7.5

B. RHEL 4.4

C. RHEL 6.7

D. RHEL 6.5

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Idro Most Recent 1 year, 9 months ago

A - https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/compatibility-and-server-recommendations.pdf

upvoted 2 times

ChrisCCNA 1 year, 11 months ago

A is correct

upvoted 2 times

Question #190 *Topic 1*

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?

A.

B.

C.

D.

WAN Edge 1

```
vpn 0
 interface ge0/0
  ip address 10.0.0.1/24
  ipv6 dhcp-client
  tunnel-interface
   color default
   encapsulation ipsec
```

WAN Edge 2

```
vpn 0
 interface ge0/0
  ip address 10.0.0.2/24
  ipv6 dhcp-client
  tunnel-interface
   color default
   encapsulation ipsec
```

WAN Edge 1

```
vpn 0
 interface ge0/0
  ip address 10.0.0.1/24
  ipv6 dhcp-client
  tunnel-interface
   color public-internet restrict
   encapsulation ipsec
```

WAN Edge 2

```
vpn 0
 interface ge0/0
  ip address 10.0.0.2/24
  ipv6 dhcp-client
  tunnel-interface
   color public-internet restrict
   encapsulation ipsec
```

WAN Edge 1

```
vpn 0
 interface ge0/0
  ip address 10.0.0.1/24
  ipv6 dhcp-client
  tunnel-interface
   color gold restrict
   encapsulation ipsec
```

WAN Edge 2

```
vpn 0
 interface ge0/0
  ip address 10.0.0.2/24
  ipv6 dhcp-client
  tunnel-interface
   color gold restrict
   encapsulation ipsec
```