Cisco.300-415J.v2026-09-24.q252

試験コード：	300-415J
試験名称：	Implementing Cisco SD-WAN Solutions (300-415日本語版)
認証ベンダー：	Cisco
無料問題の数：	252
バージョン：	v2026-09-24
ページの閲覧量：	105
問題集の閲覧量：	2757

https://www.jpnshiken.com/shiken/Cisco.300-415J.v2026-09-24.q252.html

質問: **1**
4つのテナントを持つマルチテナント環境にvManagerをインストールする場合、いくつのvBondコントローラーをインストールする必要がありますか？
A. 1 つの vBond コントローラーがテナント間で共有されます。
B. マルチテナント展開には、3つのvBandコントローラが必要です。
C. 各テナントは冗長性のために 2 つの vBond コントローラーを必要とします。
D. 各テナントには専用のvBondコントローラーが必要です。
正解: (正解を表示します)
With Cisco SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco vManage.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20- x/systems-interfaces-book/sdwan-multitenancy.html

質問: **2**
NATの背後でTLOCが設定されている場合、どの色のタイプが割り当てられますか？
A. MPLS
B. private
C. blue
D. public
正解: (正解を表示します)
When a TLOC is configured behind NAT, the color type is assigned as public. This is because the TLOC is not accessible from the public internet, so it must use a public IP address to communicate with other TLOCs. The other color types, MPLS, private, and blue, are used for TLOCs that are accessible from the public internet.

質問: **3**
アクセス リストまたはルート マップを作成する前に、どの構成で関心グループを定義しますか?

A.



B.



C.



D.



正解: (正解を表示します)

To define groups of interest (such as prefixes, sites, VPNs) before creating an access list or route map, the correct configuration path in Cisco vManage is through the "Lists" option within "Centralized Policy" or "Localized Policy" under "Custom Options". This allows you to define specific elements such as IP prefixes or site lists that can later be referenced in access lists or route maps.

質問: **4**
顧客は音声トラフィックの信頼性を求めており、MPLS、ビジネスインターネット、およびパブリックインターネットのトランスポートを利用しています。どの制御ポリシー構成が、より優れたSLAを維持し、音声トラフィックのブラックホール化を回避できますか？

A.

```
policy
 sla-class VOICE_TRAFFIC
  latency 150
  loss 5
 !
app-route-policy
_vpn1_VOICE_TRAFFIC
 vpn-list vpn1
  sequence 1
   match
    app-list VOICE_Apps
   !
   action
    sla-class
VOICE_TRAFFIC preferred-color mpls
   !
  !
  default-action sla-class
VOICE_TRAFFIC
!
lists
 app-list VOICE_Apps
  app O365
 !
 site-list Site-10
  site-id 10
 !
 vpn-list vpn1
  vpn 1
 !
!
!
apply-policy
site-list Site-10
 app-route-policy
 _vpn1_VOICE_TRAFFIC
 default-action sla-class
VOICE_TRAFFIC
```

B.

```
policy
 sla-class VOICE_TRAFFIC
  latency 150
  loss 5
 !
app-route-policy
_vpn1_VOICE_TRAFFIC
 vpn-list vpn1
  sequence 1
   match
    app-list VOICE_Apps
   !
   action
    sla-class
VOICE_TRAFFIC preferred-color mpls
    backup-sla-preferred-color biz-
internet
   !
  !
 _vpn1_VOICE_TRAFFIC
!
lists
 app-list VOICE_Apps
  app audio-video
 !
 site-list Site-10
  site-id 10
 !
 vpn-list vpn1
  vpn 1
 !
!
!
apply-policy
site-list Site-10
 app-route-policy
 _vpn1_VOICE_TRAFFIC
 default-action sla-class
VOICE_TRAFFIC
```

jpnshiken.com

C.

```
sla-class VOICE_TRAFFIC
 latency 0
!
pp-route-policy _vpn1_VOICE_TRAFFIC
vpn-list vpn1
  sequence 1
   match
    app-list VOICE_Apps
   !
   action
    sla-class VOICE_TRAFFIC  preferred-
olor mpls strict
   !
  !
default-action sla-class VOICE_TRAFFIC
```

```
 app-list VOICE_Apps
  app audio-video
 !
 site-list Site-10
  site-id 10
 !
 vpn-list vpn1
  vpn 1
 !
!
!
apply-policy
site-list Site-10
 app-route-policy _vpn1_VOICE_TRAFFI
```

D.

```
olicy
 sla-class VOICE_TRAFFIC
  latency 150
  loss 5
 !
app-route-policy
_vpn1_VOICE_TRAFFIC
 vpn-list vpn1
  sequence 1
   match
    app-list VOICE_Apps
   !
   action
    sla-class
VOICE_TRAFFIC  preferred-color mpls
   !
  !
default-action sla-class
```

```
VOICE_TRAFFIC
!
lists
 app-list VOICE_Apps
  app audiovideo
 !
 site-list Site-10
  site-id 10
 !
 vpn-list vpn1
  vpn 1
 !
!
!
apply-policy
site-list Site-10
 app-route-policy
_vpn1_VOICE_TRAFFIC
```

正解: (正解を表示します)

質問: **5**

Cisco SD-WANデバイスでTLSプロキシが有効になっている場合、UTDに処理のために送信されるパケットの種類はどれですか？

A. 初期データパケット

B. サーバーハローパケット

C. TCP SYNパケット

D. クライアントハローパケット

正解: (正解を表示します)

When TLS proxy is enabled on a Cisco SD-WAN device with Unified Threat Defense (UTD), client hello packets are sent to UTD for inspection and action. The client hello packet is part of the initial handshake process in the TLS protocol, and it contains important information such as the client's supported ciphers and TLS version. Inspecting this packet allows the UTD service to perform actions such as decrypting, inspecting, or blocking traffic based on policy.

質問: **6**

データプレーンの復元力について、Cisco SD-WANソフトウェアは何を実装していますか？

A. BFD

B. vSmartコントローラーとWANエッジルーター間の親和性を確立する

C. 複数のvBondオーケストレーター
D. OMP
正解: (正解を表示します)
For data plane resilience, the Cisco SD-WAN software implements standard protocol mechanisms, specifically BFD, which runs on the secure IPsec tunnels between WAN Edge routers.
Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd- wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf

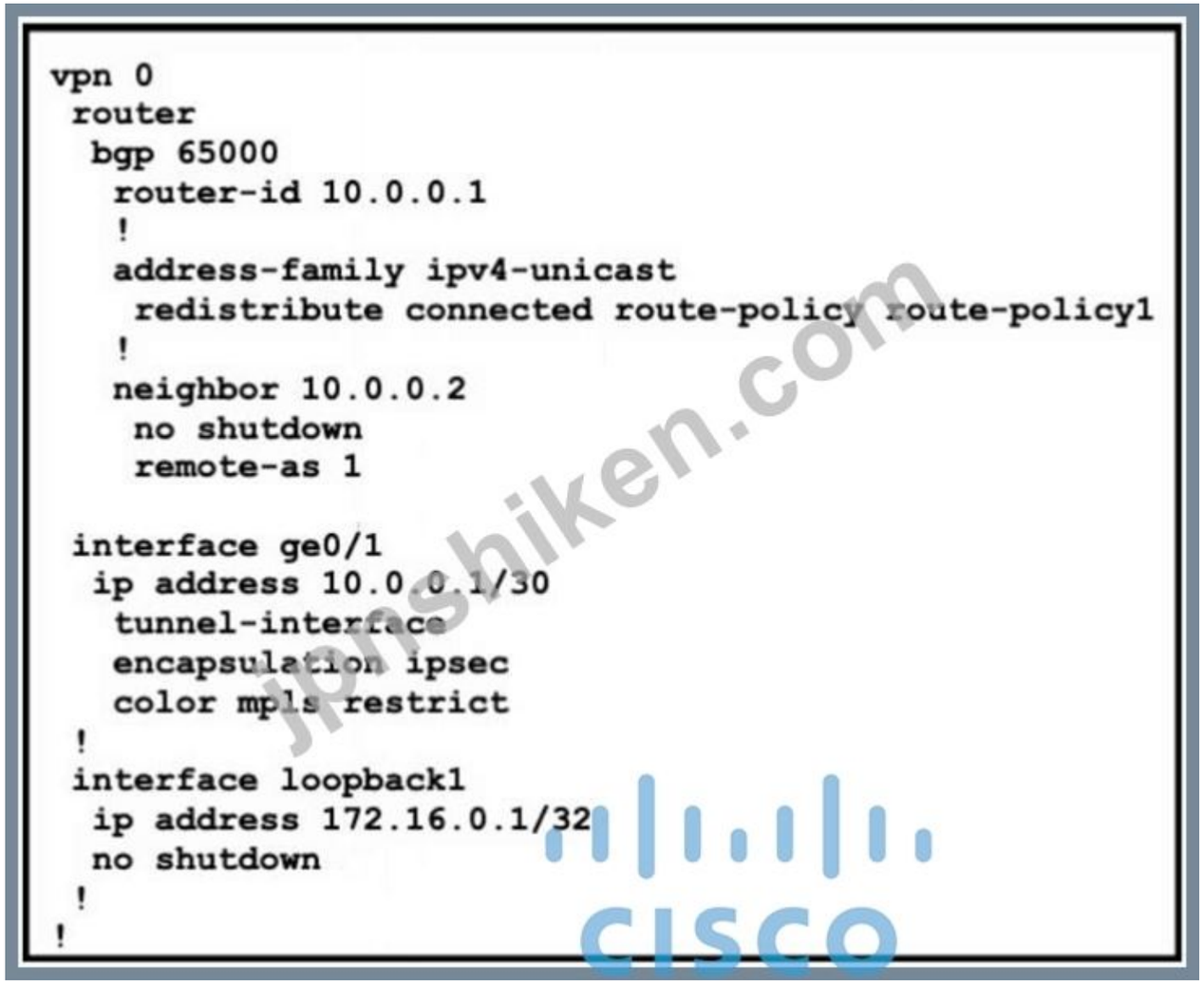
質問: **7**
管理者は、会社のプライベートネットワークからISPネットワークにトラフィックを転送するようにSD-WANを構成する必要があります。この目標を達成するためにどのような行動を取るべきですか？
A. 制御ポリシーを構成する
B. データポリシーを構成する
C. データセキュリティポリシーを構成する
D. アプリケーション対応ポリシーを構成する
正解: (正解を表示します)
Data policies are used to define routing and forwarding behavior based on various criteria, including destination, source, application, and other characteristics. You can create a data policy to specify the conditions under which traffic should be redirected from the private network to the ISP network.

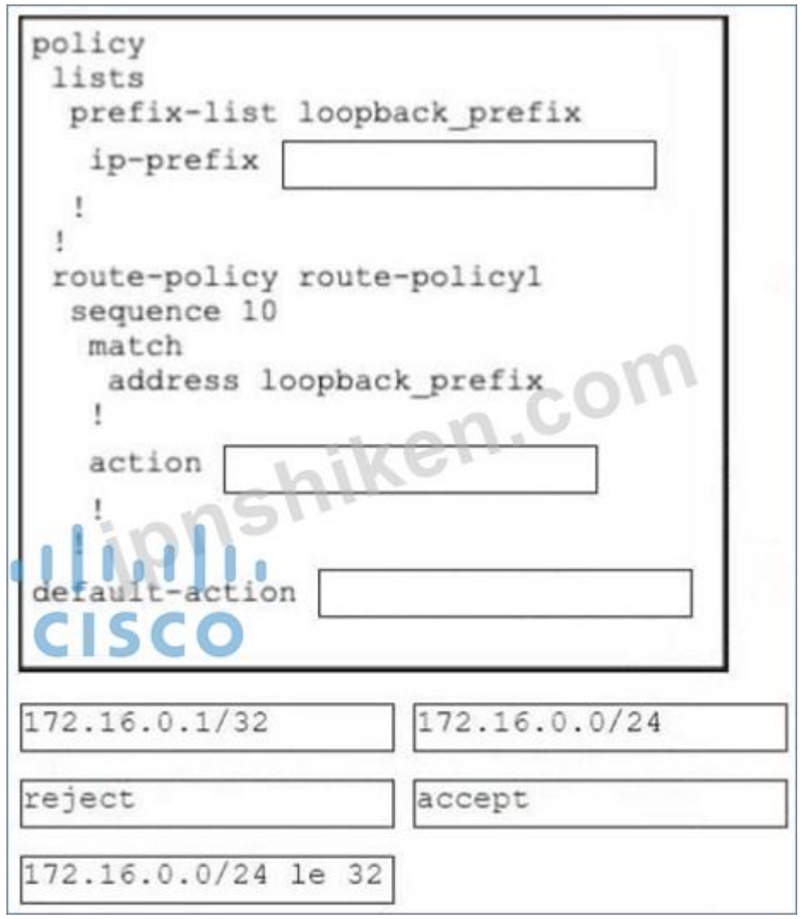
質問: **8**
どの設定で「local」という名前のデータポリシーが作成され、local_vpnsリストに含まれるVPNに関連付けられますか？
A. SD-WANコントローラー(config)# policy vpn-data-lists local
SD-WANコントローラー(config-lists)# data-prefix-list vpns
B. SD-WANコントローラー(config)# policy data-policy local
SD-WANコントローラー(config-data-policy-policy-name)# vpn-list local_vpns
C. SD-WANコントローラー(config)# policy vpn-data-policy local
SD-WANコントローラー(config-data-policy-policy-name)# vpn-list local_vpns
D. SD-WANコントローラー(config)# policy lists local
SD-WANコントローラー(config-lists)# data-prefix-list local_vpns
正解: (正解を表示します)
To create a data policy in Cisco SD-WAN, the correct configuration mode is vpn-data-policy. This command defines the policy name (in this case, local) and associates it with a specific VPN list using the vpn-list command (here, local_vpns). This is the valid syntax to apply a data policy to specified VPNs.

質問: **9**
分岐回路用に4GBのメモリを搭載したISR1Kを選択する際に、エンジニアが考慮すべき2つの機能は何ですか？(2つ選択してください。)
A. エンタープライズファイアウォール
B. URLフィルタリング
C. Cisco AMP および AMP 脅威グリッド
D. vSmartコントローラー
E. Cisco Umbrella DNSセキュリティ
正解: (正解を表示します)

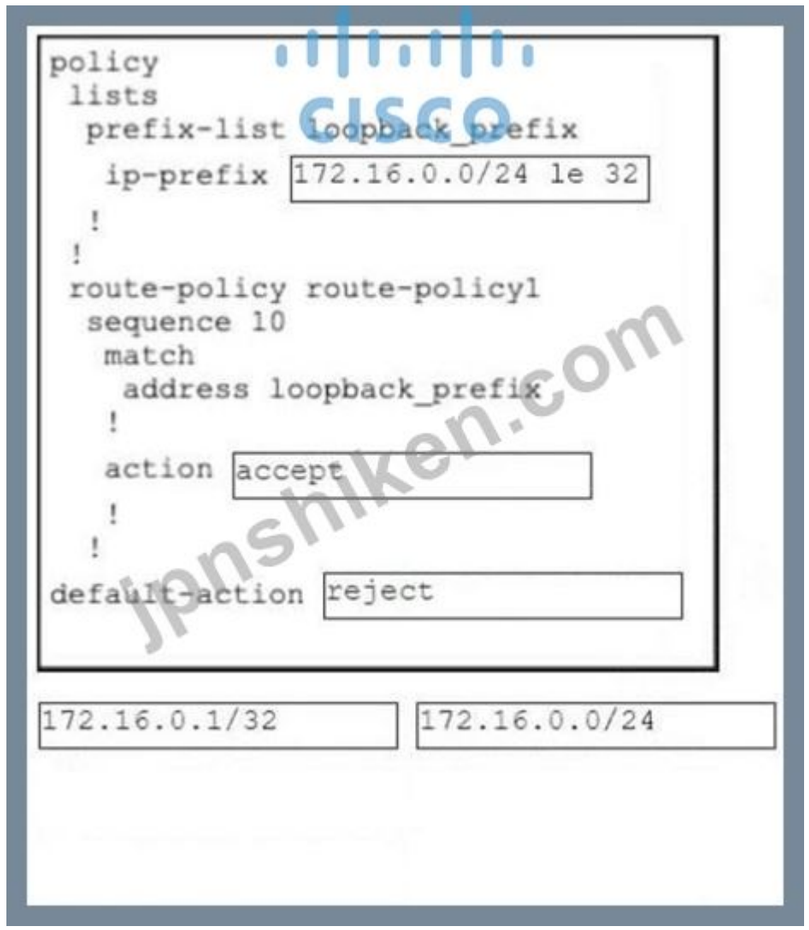
These features require sufficient resources, and with 4 GB of memory on the ISR1K, it's important to ensure that the device can handle the processing and memory demands of both enterprise firewall capabilities and URL filtering effectively.

質問: **10**
ドラッグアンドドロップ問題
顧客の支店には2台のルーターがあり、そのうちの1台のルーターで、トランスポートVPNで設定されたBGPにおいて、ループバック1アドレスをアドバタイズしたいと考えています。また、将来的にはループバック1サブネットからより多くのアドレスをアドバタイズするポリシーも必要です。要件を満たすように、下部にあるコードスニペットを構成内のボックスにドラッグアンドドロップしてください。すべてのオプションを使用するわけではありません。




policy
lists
prefix-list loopback_prefix
ip-prefix
!
!
route-policy route-policy1
sequence 10
match
address loopback_prefix
!
action
!
!
default-action
172.16.0.1/32
172.16.0.0/24
reject
accept
172.16.0.0/24 le 32

正解:



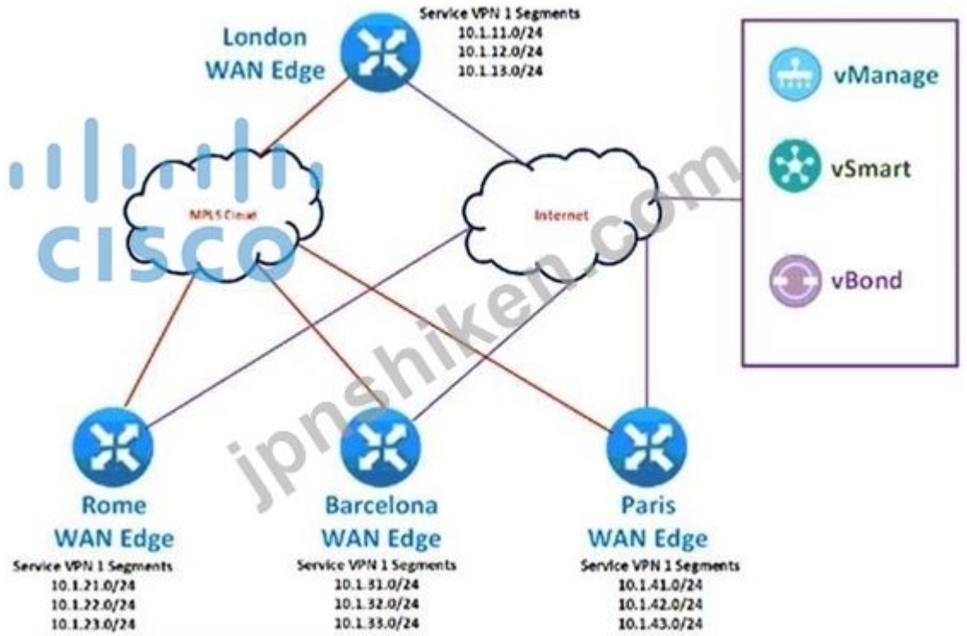
jpnshiken.com

質問: **11**
主要都市周辺に集中している、あるいは複数の国に分散している複数の支店を持つ企業に対し、各施設におけるルーティングサービスを地域ごとに最適化できるソリューションはどれでしょうか？
A. コロケーション向けクラウドオンランプ
B. SaaS向けクラウドオンランプ
C. IaaS向けクラウドオンランプ
D. マルチクラウド向けクラウドオンランプ
正解: **A** (コメントを発表する)
Cloud OnRamp for Colocation is a Cisco SD-WAN solution designed to regionalize routing services by colocating network and compute resources closer to distributed branch offices. This allows enterprises with multiple branch offices, especially those clustered around major cities or spread across different regions, to centralize and optimize their connections at colocation facilities. These facilities can then serve as regional hubs, improving performance and scalability for branch connectivity.

質問: **12**
BFDの基本設定におけるポーリング間隔のデフォルト値(ミリ秒単位)は何ですか？
A. 300,000
B. 600,000
C. 900,000

D. 1,200,000
正解: **(**正解を表示します**)**
https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Configuration/Templates/ BFD

質問: **13**
図を参照してください。SD-WANネットワークは、デフォルトのフルメッシュトポロジーで構成されています。SD-WANエンジニアは、パリのWANエッジで、MSN MessengerとAOL Messengerのトラフィックに対して、インターネットTLOCを優先TLOCとして使用したいと考えています。このタスクを実行するために、エンジニアはトラフィックを分類するためにどの構成を使用する必要がありますか？



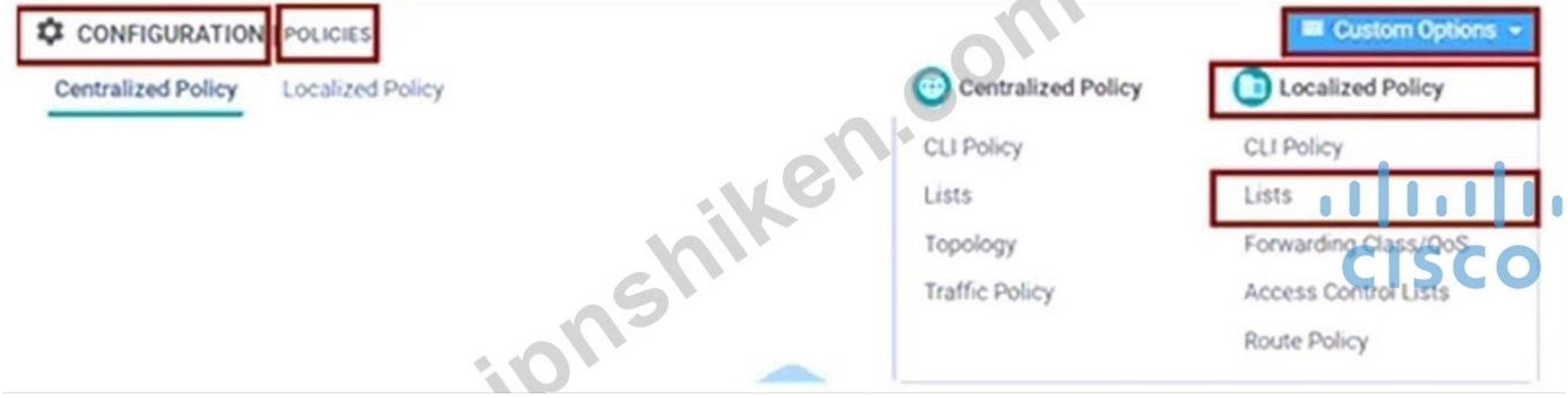
A.



B.


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

C.


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

D. 

正解: **(**正解を表示します**)**

To classify the traffic for MSN Messenger and AOL Messenger and configure the Paris WAN Edge to prefer the internet TLOC for this traffic, the engineer needs to define an Application List for the specific applications.

Chosen option includes the "Traffic Policy" option under the Centralized Policy section, which is necessary to classify the MSN Messenger and AOL Messenger traffic and direct it to the internet TLOC.

質問: **14**

どのCisco Catalyst SD-WAN機能プロファイルにBGPおよびOSPFの設定情報が含まれていますか？

A. CLIプロファイル

B. 輸送および管理プロファイル

C. ポリシープロファイル

D. サービスプロファイル

正解: **D (**コメントを発表する**)**

In Cisco Catalyst SD-WAN, the Service profile contains configuration details for routing protocols such as BGP and OSPF. This profile defines how services and routing are applied within VPNs, making it the correct place for dynamic routing configurations.

質問: **15**

SD-WANの高可用性vManageクラスタを構成する2つのアーキテクチャコンポーネントはどれですか？

(2つ選択してください。)

A. ネットワーク構成システム

B. WANエッジルーター

C. NATルーター

D. メッセージングサーバー

E. アプリケーションサーバー

正解: **(**正解を表示します**)**

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

質問: **16**
図を参照してください。管理者は、直接通信を行うべき2つのサイトに対して、既存のハブアンドスポークポリシーに加えて、新たなポリシーを設定しています。このポリシーはどのように設定されますか？



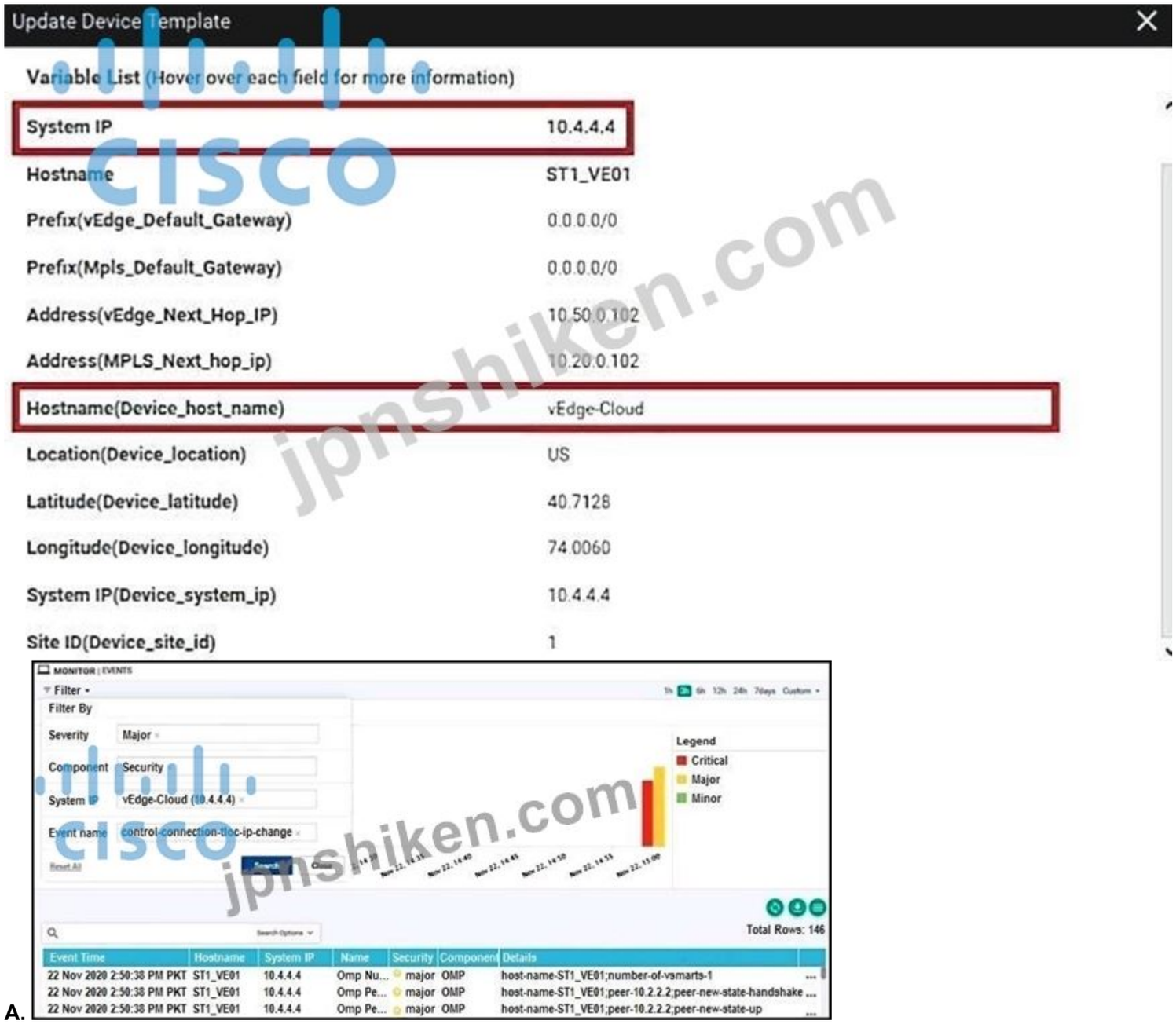
A. ハブアンドスポーク
B. メッシュ
C. 既存のトポロジーをインポートする
D. カスタム制御(ルートとTLOC)
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies- book/controlpolicies.html#id_107219

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
管理者は、回線ID 392318933を持つ特定のWANエッジデバイス上で、サービス側VPNから入ってくるトラフィックに対してACLを設定する必要があります。
このACLを設定するには、どのポリシーを使用する必要がありますか？
A. ローカルデータポリシー
B. 中央データポリシー
C. アプリ対応ポリシー
D. 中央制御ポリシー
正解: (正解を表示します)
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.

質問: **18**
図を参照してください。vManageのログは過去数か月分が利用可能です。重要なサイトでデバイス名の変更が誤って展開されました。運用チームと設計チームは、このデバイス名の変更をどのように追跡しますか？

A.



jpnshiken.com

B.



C.



D.

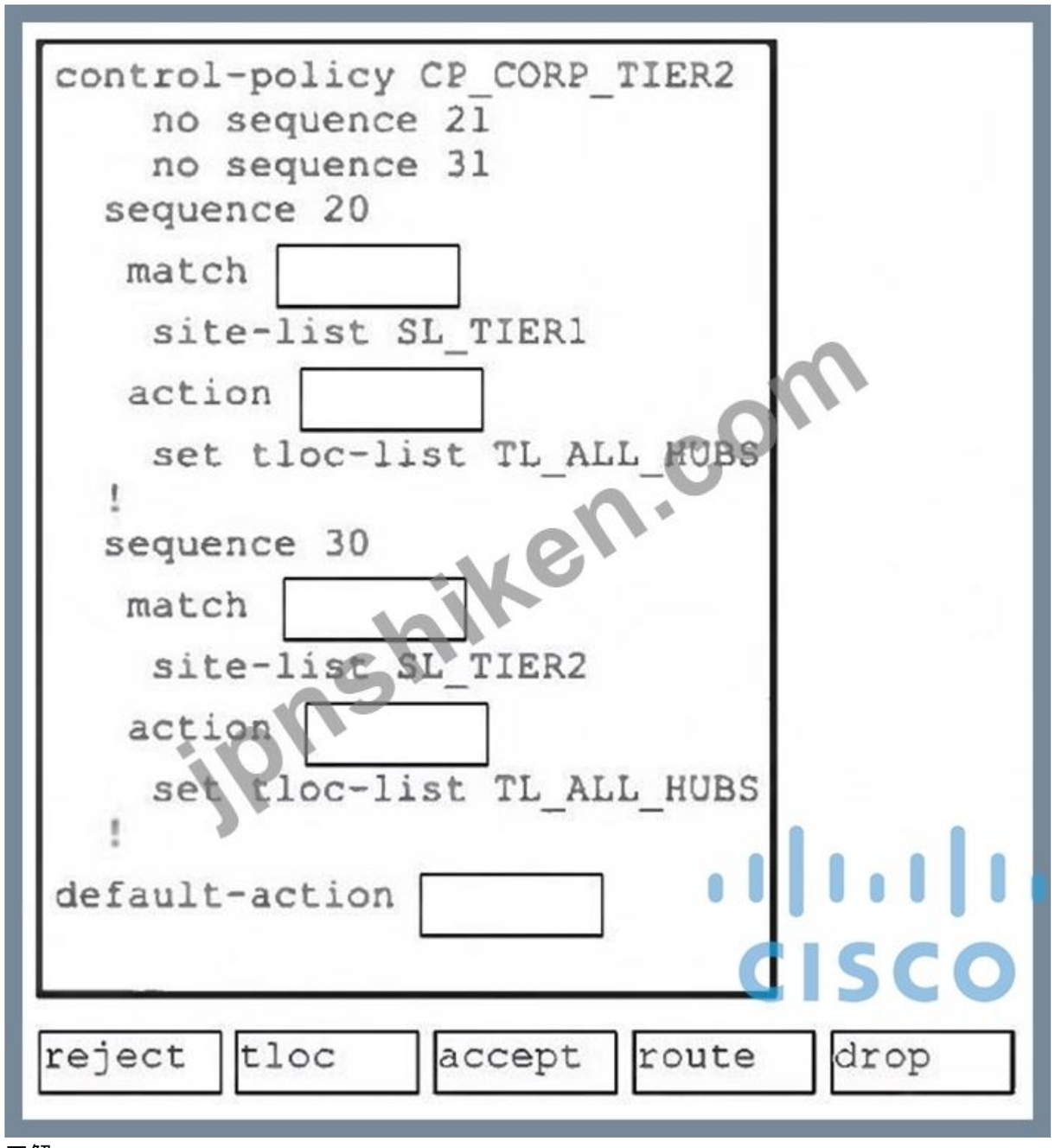


正解: **C** (コメントを発表する)

質問: **19**
顧客がGREよりもIPsecトンネルを選択する2つの理由は何ですか？(2つ選択してください。)
A. IPsecの障害検出が高速化されました。
B. 一般的に、トンネル接続に対してより高い帯域幅を提供します。
C. CFlowd が必要です。
D. WANエッジルーターがNATの背後にあります。
E. IPsecの方が安全です。
正解: **(正解を表示します)**
GRE tunnels require that the WAN Edge routers have public IP addresses. IPsec tunnels can be used with WAN Edge routers that are behind NAT.

質問: **20**
コントロールプレーン接続のデフォルトプロトコルは何ですか？
A. HTTPS
B. TLS
C. IPsec
D. DTLS
正解: **(正解を表示します)**
By default, the control plane uses DTLS as the protocol that provides privacy on all its tunnels.
DTLS runs over UDP.

質問: **21**
ドラッグアンドドロップ問題
企業では、Tier2サイトがハブ拠点を介してのみTier1およびTier2サイトと通信することを要求しています。さらに、Tier2はTier1およびTier2サイトとのBFDセッションを確立することを制限されています。要件を満たすように、下部にあるコードスニペットを構成内のボックスにドラッグアンドドロップしてください。すべてのオプションが使用されるわけではありません。一部のオプションは複数回使用されます。


control-policy CP_CORP_TIER2
no sequence 21
no sequence 31
sequence 20
match
site-list SL_TIER1
action
set tloc-list TL_ALL_HUBS
!
sequence 30
match
site-list SL_TIER2
action
set tloc-list TL_ALL_HUBS
!
default-action
reject
tloc
accept
route
drop

正解:

```
control-policy CP_CORP_TIER2
    no sequence 21
    no sequence 31
  sequence 20
   match route
    site-list SL_TIER1
   action accept
    set tloc-list TL_ALL_HUBS
  !
  sequence 30
   match route
    site-list SL_TIER2
   action accept
    set tloc-list TL_ALL_HUBS
  !
default-action drop
```

reject | tloc | accept | route | drop

ipnshiken.com

質問: **22**
TLOCはどのように定義されますか？
A. SD-WANアーキテクチャにおいてサイトを指定するための一意の識別子によって表されます。
B. マルチテナントvSMART展開におけるCisco SD-WANオーバーレイを指定します。
C. WANエッジルータに適用されるQoSポリシーのグループによって表されます。
D. これは、GREまたはIPsecカプセル化、リンクカラー、およびシステムIPアドレスの固有のコレクションです。
正解: (正解を表示します)

Each TLOC is uniquely identified by a 3-tuple comprising the system IP address, a color, and an encapsulation.
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/System- Interface/systems-interfaces-book-xe-sdwan/configure-interfaces.html

質問: **23**
図を参照してください。エンジニアが制御接続の問題をトラブルシューティングしています。
この "show control connections"出力における "connect"とはどういう意味ですか？

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. 制御接続が切断されました
B. 制御接続が確立されました
C. 制御接続試行が進行中です
D. 制御接続が接続されました
正解: **(**正解を表示します**)**
https://community.cisco.com/t5/networking-documents/sd-wan-routers-troubleshoot-control- connections/ta-p/3813237

質問: **24**
Cisco SD-WANネットワーク内のネットワークデバイスと通信するために、REST APIはどのプロトコルを使用しますか？
A. HTTP
B. SSL
C. IPsec
D. SSH
正解: **A (**コメントを発表する**)**
Rest API Monitoring uses HTTP requests to access and use data as the main protocol.
That data can be GET, PUT, POST AND DELETE data classification!
https://www.ciscopress.com/articles/article.asp?p=3145761&seqNum=6

質問: **25**
コントローラーをオンプレミスにインストールする利点は何ですか？
A. 自動的な地理的冗長性とセキュリティ
B. データプレーンとコントロールプレーンの完全な制御
C. 拡張性とコスト削減
D. 導入と管理の容易さ

正解: **(**正解を表示します**)**
Key benefices of on-premise systems
Greater security and privacy: On-premise systems are installed and operated on your premises,
■
so your data is always kept secure and private, as long as you harden your platform and keep them up to date.
More control and customization: On-premise systems give you more control over your security
■
system. You can customize it to meet your specific needs and requirements, whereas Cloud- based systems are more limited in customization options.
Higher performance: On-premise systems typically have higher performance than Cloud-based
■
systems, as they don't rely on the Internet connection or power outages.
Increased reliability: On-premise systems are less likely to experience downtime due to Internet
■
connection issues, as they don't rely on the Cloud for their functionality.
Disadvantages of on-premise systems
On-premise or legacy access control systems are becoming less secure every day. Legacy
■
systems are outdated and vulnerable to hackers who know how much time it takes for each server location or firm's IT department to have access control capabilities. Hackers can exploit these vulnerabilities because they're already familiar with the decades-old technology used in these legacy security methods, making them an easy target.
They can be expensive to purchase and maintain
■
It would be best to have a dedicated IT staff to manage them.
■
They can be challenging to scale up or down to meet your organization's needs.
■
They are less flexible than cloud-based systems.
■

質問: **26**
エンジニアは、サイト上でローカル冗長性を構成する必要があります。どの構成がこのタスクを達成しますか？
A. VPN 0
tloc拡張インターフェース
インターフェース名
B. VPN 0
インターフェース インターフェース名
tloc拡張機能インターフェース名
C. インターフェース インターフェース名
tloc拡張機能
D. tloc拡張インターフェース
インターフェース名
正解: **B (**コメントを発表する**)**

質問: **27**
エンジニアは、サイト上で集中管理型のポリシーを設定する必要があります。そのポリシーでは、HTTPトラフィックの損失率が10%未満の場合はすべてのHTTPトラフィックがパブリックインターネット回線を使用し、そうでない場合はMPLSを使用するように設定する必要があります。
この要件を満たす構成ウィザードはどれですか？
A. 関心のあるアプリケーションまたはグループを作成する > トラフィックデータを構成する > サイトと VPN にポリシーを適用する。

B. VPNメンバーシップの設定 > サイトとVPNへのポリシーの適用。
C. 関心のあるアプリケーションまたはグループを作成する > トラフィックルールを設定する > サイトと VPN にポリシーを適用する。
D. トポロジの構成 > サイトと VPN へのポリシーの適用。
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies- book/data-policies.html#id_107211

質問: **28**
インターネット経由でvManagerの地理情報画面を視覚化できるウェブサイトはどれですか？
A. *.globalstreetmaps.org
B. *.fullstreetmaps.org
C. *.callstreetmaps.org
D. *.openstreetmaps.org
正解: (正解を表示します)
https://www.cisco.com/c/dam/en/us/td/docs/cloud_services/cisco_modeling_labs/v110/installation
/guide/licensing/Open-Source-Used-in-Cisco-Modeling-Labs-1-1.pdf

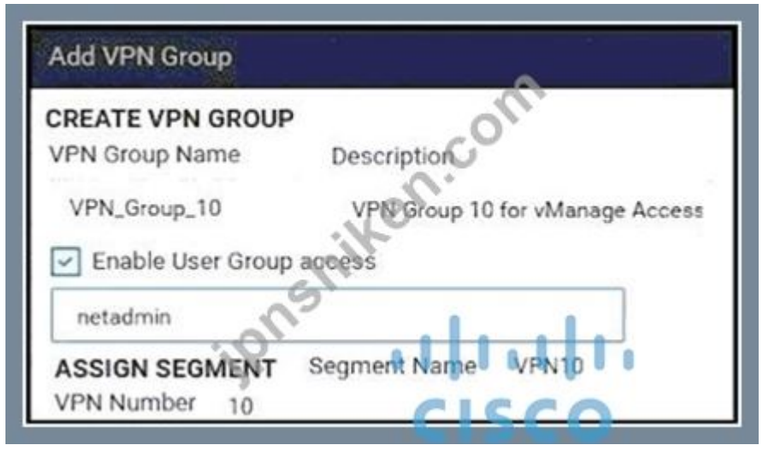
質問: **29**
vEdgeルーター上でTLOCごとのBFDセッション概要情報を表示するコマンドはどれですか？
A. bfd tloc-summary-list を表示
B. bfd履歴を表示
C. bfd の概要を表示します
D. bfdセッションを表示する
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/sdwan-cr- book_chapter_0100.html#wp5111537210

質問: **30**
エンジニアは、サイト上でローカルルーターの冗長性を設定する必要があります。この作業を完了するには、どの設定が必要ですか？
スドワン
A. インターフェース interface1-name
tloc拡張機能インターフェース2名
システム
B. インターフェースインターフェース名
tloc拡張機能インターフェース2名
システム
C. tloc拡張機能インターフェース名
インターフェース interface2-name
スドワン
D. tloc拡張機能インターフェース1名
インターフェース interface2-name
正解: (正解を表示します)

Local router redundancy in Cisco SD-WAN is implemented using TLOC extension, which allows one WAN Edge router to use the transport interface of another router at the same site. This is configured under the sdwan interface tunnel-interface configuration on the WAN Edge device.
The command tloc-extension interface2-name specifies the local interface used to reach the peer WAN Edge that provides the alternate transport, enabling redundancy for the transport connection.

質問: **31**
ある企業が、VPNグループ、セグメント、およびユーザーに基づいてCisco Catalyst SD-WAN Managerの機能へのアクセスを制限する新しいポリシーを導入しようとしています。この目的のためにuser1という名前でユーザーが既にプロビジョニングされている場合、どの構成でこのタスクを実行できますか？

A.



B.



C.



D.



正解: **A** (コメントを発表する)

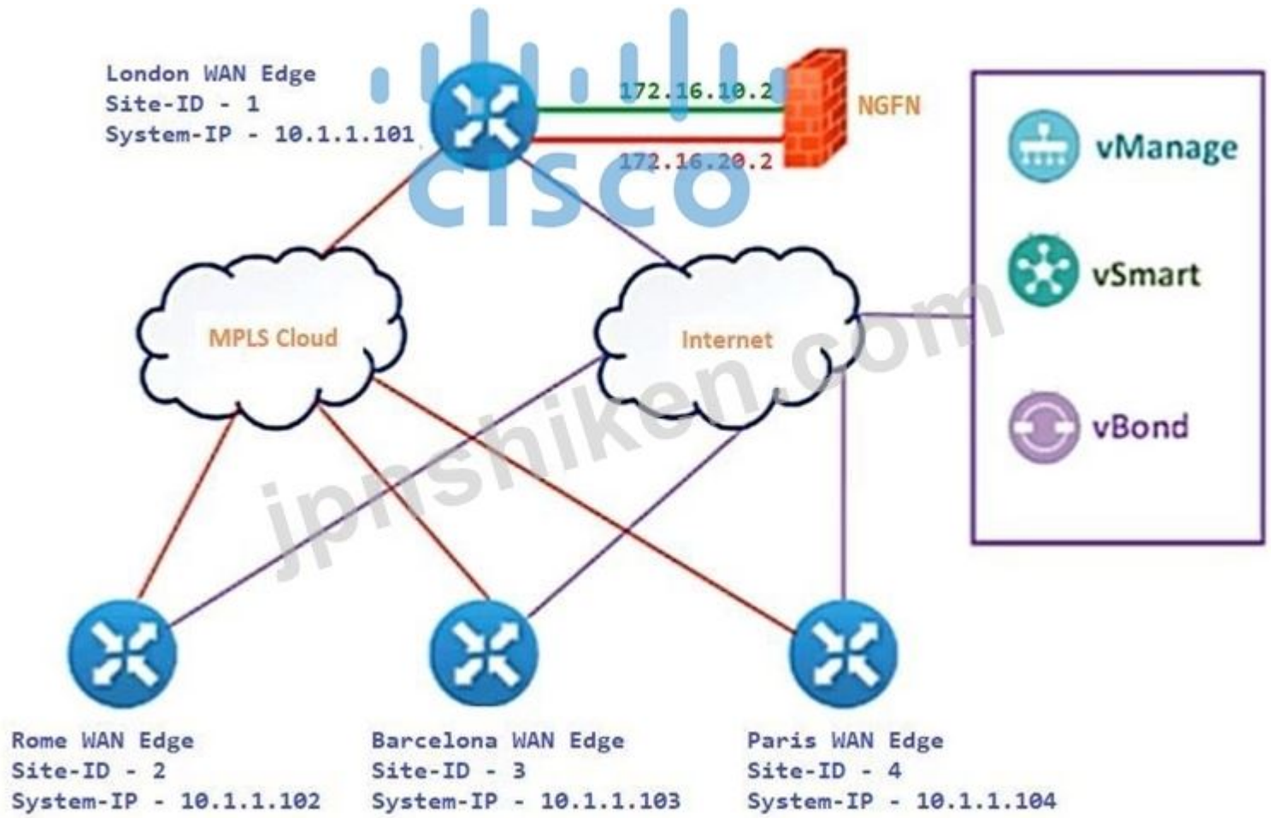
The company needs to restrict access to vManage features based on VPN groups, segments, and users.

In the correct option, the VPN group is assigned to the netadmin user group, which is typically the role with appropriate segmentation control capabilities. This setup ensures that only users in the netadmin group (like user1) have access to the defined VPN segment (VPN10), satisfying the access control policy.

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**

図を参照してください。Cisco SD-WANはデフォルトのトポロジを使用して展開されています。エンジニアは、ローマからパリへのすべてのデータトラフィックがロンドンにあるNGFWを経由して転送されるように、サービス挿入ポリシーを設定したいと考えています。サービスVPN IDが1であると仮定した場合、この要件を満たす構成はどれですか？


London WAN Edge
Site-ID - 1
System-IP - 10.1.1.101
172.16.10.2
172.16.20.2
NGFN
vManage
vSmart
vBond
MPLS Cloud
Internet
Rome WAN Edge
Site-ID - 2
System-IP - 10.1.1.102
Barcelona WAN Edge
Site-ID - 3
System-IP - 10.1.1.103
Paris WAN Edge
Site-ID - 4
System-IP - 10.1.1.104

A.

ROME WAN Edge
service FW address 10.1.1.101

PARIS WAN Edge
service FW address 10.1.1.101

vSmart Policy

```
policy
 lists
  site-list ROME
   site-id 2
  site-list PARIS
   site-id 4
 control-policy NGFW-SI
  sequence 1
   match route
    site-id ROME
   action accept
  sequence 2
   match route
    site-id PARIS
   action accept
  default-action accept
!
apply-policy
 site-list ROME control-policy NGFW-SI out
```

jpshiken.com

B.

London WAN Edge

```
vpn 1
  service netsvc1 address 172.16.10.2
  service netsvc2 address 172.16.20.2
```

vSmart Policy

```
policy
 lists
  site-list ROME
   site-id 2
  site-list PARIS
   site-id 4
 control-policy NGFW-SI
  sequence 1
   match route
    site-id ROME
   action accept
    set service netsvc1 vpn 1
  sequence 2
   match route
    site-id PARIS
   action accept
    set service netsvc2 vpn 1
  default-action accept
!
apply-policy
 site-list ROME
  control-policy NGFW-SI out
 !
 site-list PARIS
  control-policy NGFW-SI out
```

cisco
jpeshken.com

C.

London WAN Edge

```
vpn 1
  service netsvc1 address 172.16.10.2
  service netsvc2 address 172.16.20.2
```

vSmart Policy

```
policy
 lists
  site-list ROME
   site-id 2
  site-list PARIS
   site-id 4
 control-policy NGFW-SI
  sequence 1
   match route
    site-id ROME
   action accept
  sequence 2
   match route
    site-id PARIS
   action accept
  default-action accept
!
apply-policy
 site-list ROME control-policy NGFW-SI out
```

jpnshiken.com

ROME WAN Edge
service FW address 10.1.1.101

PARIS WAN Edge
service FW address 10.1.1.101

vSmart Policy
```
policy
 lists
  site-list ROME
   site-id 2
  site-list PARIS
   site-id 4
 control-policy NGFW-SI
  sequence 1
   match route
    site-id ROME
   action accept
    set service netsvc1 vpn 1
  sequence 2
   match route
    site-id PARIS
   action accept
    set service netsvc2 vpn 1
  default-action accept
!
apply-policy
 site-list ROME
  control-policy NGFW-SI out
 !
 site-list PARIS
  control-policy NGFW-SI out
```

D.

正解: **B** (コメントを発表する)

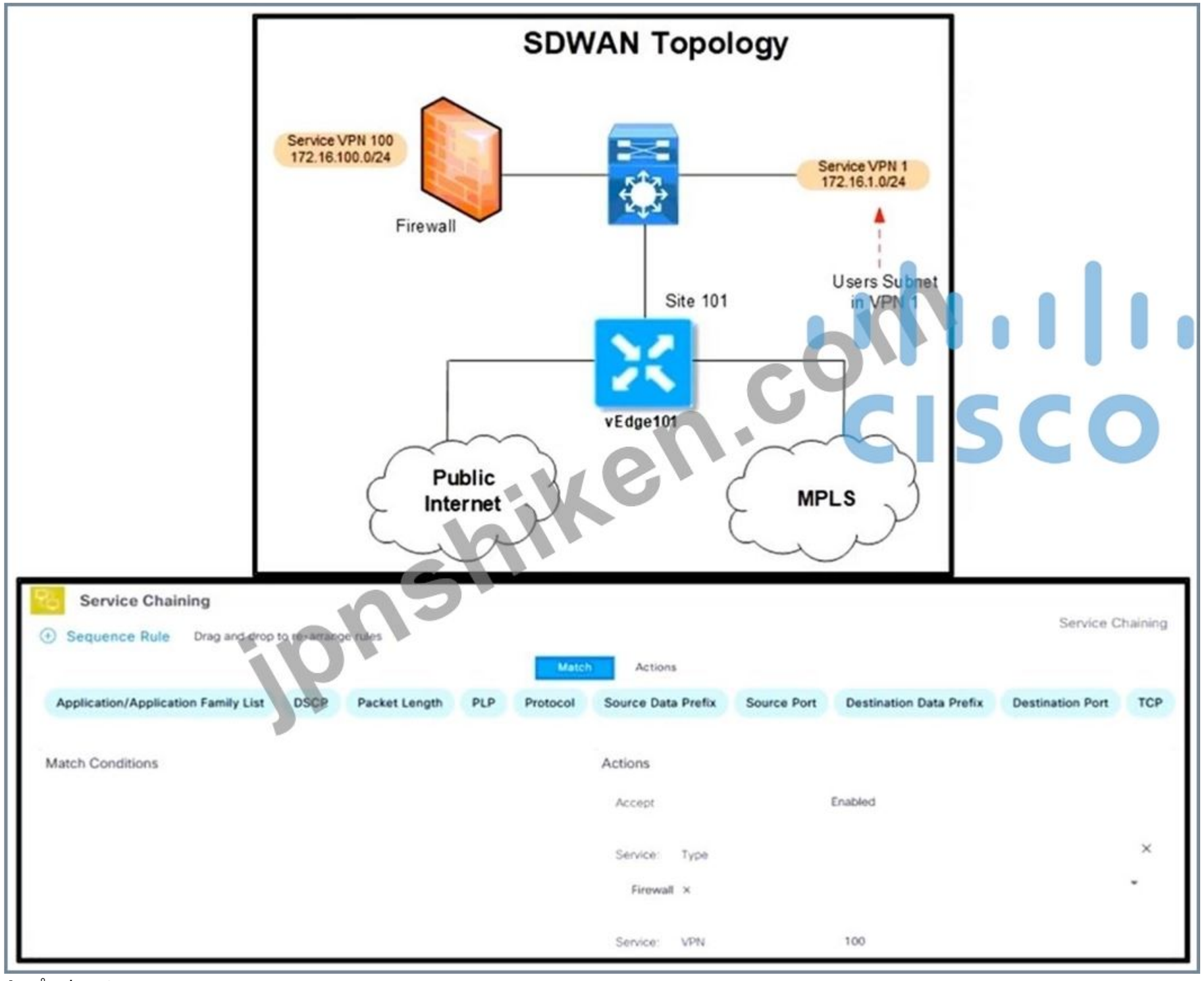
質問: **33**

図を参照してください。tloc-extensionコマンドを使用して作成されるバインディングは何ですか？



A. ポートタイプサービスのge 0/2.101とポートタイプサービスのge 0/0の間
B. ポートタイプ輸送のge 0/2.101とポートタイプサービスのge 0/0の間
C. ポートタイプサービス ge 0/2.101 とポートタイプ輸送 ge 0/0 の間
D. ポートタイプ輸送の ge 0/2.101 とポートタイプ輸送の ge 0/0 の間
正解**: (**正解を表示します**)**
The tloc-extension command in Cisco SD-WAN (vEdge) configuration is used to extend the Transport Locator (TLOC) from one interface to another. This is typically done to bind interfaces that might be on different physical networks but should be treated as if they are on the same transport.
Looking at the configuration in the exhibit:
- The interface ge0/2.101 is being configured.
- The tloc-extension ge0/0 command binds the TLOC of ge0/0 to ge0/2.101.
For the TLOC extension, the binding is typically between a transport interface and another interface that is not a transport interface. This allows the interface ge0/2.101 to utilize the TLOC of ge0/0 to communicate across the SD-WAN fabric.

質問**: 34**
エンジニアがVPN1ユーザー向けのポリシーを作成しています。サイト101におけるユーザーのスカベンジャートラフィックはファイアウォールを通過する必要があります。このポリシーを有効にするには、どの2つのマッチング条件を選択する必要がありますか？(2つ選択してください。)



A. プロトコル
B. アプリケーション/アプリケーションファミリー一覧
C. ソースデータ接頭辞
D. パケット長
E. 宛先ポート

正解: **B,C** (コメントを発表する)
To identify scavenger traffic (typically low-priority traffic like file sharing, streaming, etc.), matching based on application/application family list is appropriate.
The source data prefix ensures the traffic is coming from the user subnet in VPN 1 (172.16.1.0/24 at site 101), enabling precise policy targeting for firewall service chaining.

質問: **35**
図を参照してください。エンジニアリング部門は、74個の重要なサーバーネットワークのうち3個に、BGPピアにアドバタイズされた時点でできるだけ早くコミュニティタグを割り当てる必要があります。これらのサーバーネットワークは、AS外にアドバタイズされてはなりません。この要件を満たす構成はどれですか？



A.
```
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
```

B.
```
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
```

C.
```
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
```

D.
```
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
```

正解: **C** (コメントを発表する)

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.

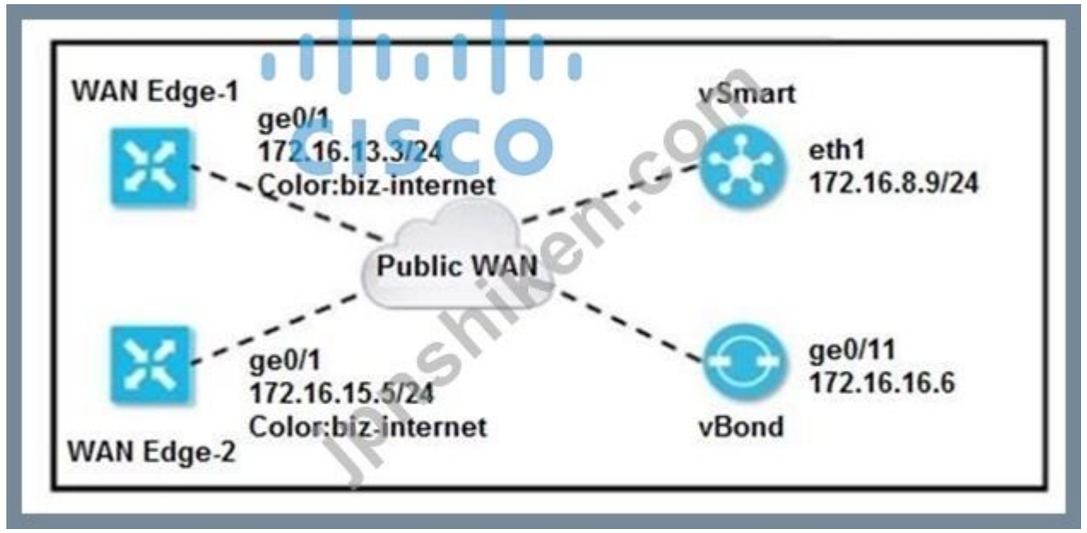
* local-as : Routes in this community are not advertised outside the local AS.

* 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.

質問: **36**

図を参照してください。両方のWANエッジルータにおけるトンネルインターフェースの設定を以下に示します。



WANエッジルーターのどの構成がインターネットに接続できますか？

```
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
```

A.
```
vpn 0
 interface ge0/1
  ip address 172.16.15.5/24
 !
ip route 0.0.0.0/0 172.16.13.1
```

B.
```
vpn 0
 interface ge0/1
  ip address 172.16.13.3/24
 !
ip route 0.0.0.0/0 172.16.13.1
```

C.

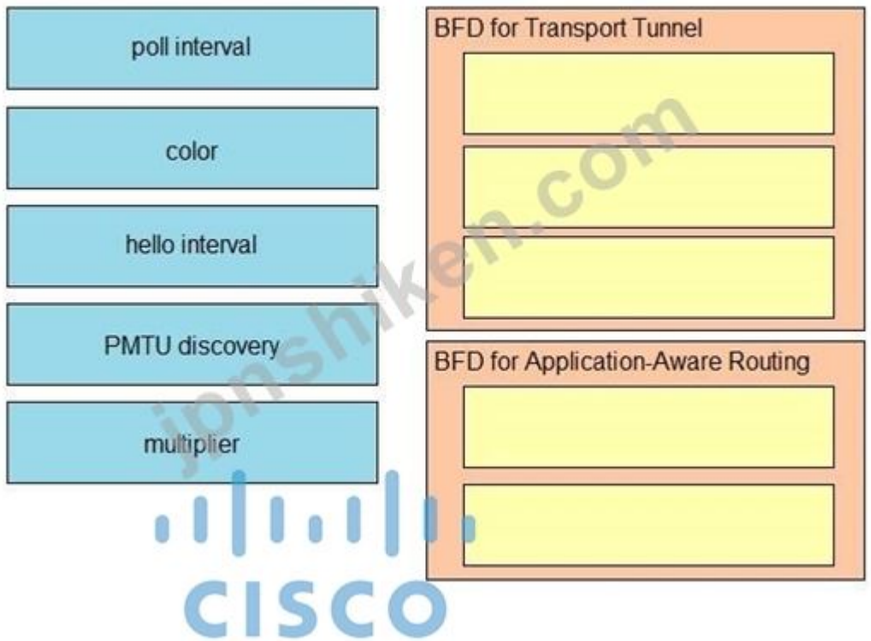

D.


正解: **B** (コメントを発表する)
The IP address on interface ge0/1 and the next hop should be in the same subnet.
https://sdwandocs.cisco.com/Product_Documentation/Software_Features/SDWAN_Release_16.3
/0 2System_and_Interfaces/07Network_Interface_Configuration_Examples

質問: **37**
UX 2.0でCisco SD-WANを構成するための構造化されたアプローチを使用して機能プロファイルを作成するコンポーネントはどれですか？
A. 特徴的な小包
B. デバイステンプレート
C. 設定グループ
D. 機能テンプレート
正解: (正解を表示します)

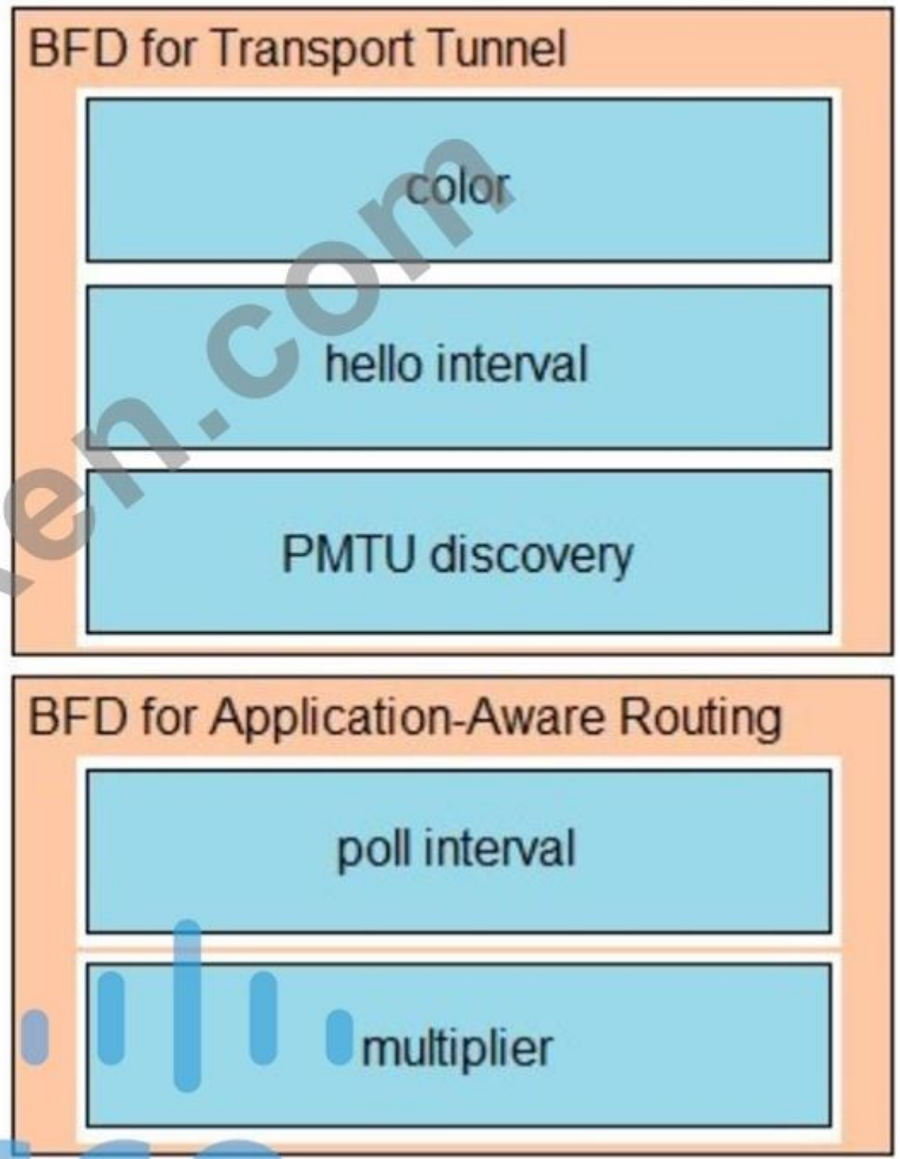
質問: **38**
ドラッグアンドドロップ問題
左側のBFDパラメータを右側のBFD設定にドラッグアンドドロップしてください。

Answer Area



正解:

Answer Area



jpnshiken.com
CISCO

質問: **39**
vBondオーケストレーターが提供するNATサーバー向けセッショントラバーサルユーティリティの役割は何ですか？
A. SD-WAN Edgeルーターが異なるサービスプロバイダー間のパブリックトランスポートとのセッションを確立することを防止します。
B. SD-WAN エッジ ルーターが NAT 対応ファイアウォールの背後に留まりながら、SD-WAN コントローラーのトランスポート アドレスが NAT されないようにします。

C. SD-WANルーターとコントローラーが、マッピングまたは変換されたIPアドレスとポート番号を検出できるようにします。
D. WANエッジルータがパブリックIPアドレスのみを使用してMPLS TLOC間でセッションを確立できるようにします。
正解: **C** (コメントを発表する)

質問: **40**
複数のデータセンターを持つ顧客小売ネットワークにおいて、ネットワーク管理者は地域ハブのトポロジーを作成するために何を使用しますか？
A. vSmart のアプリルーティングポリシー
B. vSmart のデータポリシー
C. vSmart の制御ポリシー
D. vManage の制御ポリシー
正解: (正解を表示します)
We configure the control policy at vManage and when we activate this policy, then the policy is applied and force on vSmart controller.

質問: **41**
vManageダッシュボードから監視するために、vSmart Control Connectionの統計情報を収集するために使用されるプレーンはどれですか？
A. 制御プレーン
B. データプレーン
C. 管理プレーン
D. オーケストレーションプレーン
正解: (正解を表示します)
The Management plane is responsible for collecting and displaying statistics, logs, and telemetry data from Cisco SD-WAN components, including vSmart Control Connection statistics. The vManage dashboard uses the management plane to monitor and gather information from the SD-WAN fabric, including control plane activities like vSmart connections.

質問: **42**
Cisco Cloud onRamp for Colocationは、次のうちどの2種類のサービス挿入をサポートしていますか？
A. CLIポリシー
B. ローカルポリシー
C. 制御ポリシー
D. OMPポリシー
E. データポリシー
正解: (正解を表示します)

質問: **43**
データセンター内のvManage、vBond、およびvSmartコントローラにWANエッジが到達するために必要な要件は何ですか？
A. OMP
B. IGP
C. QoS
D. TLS
正解: (正解を表示します)
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge- onboarding-deploy-guide-2020nov.pdf

質問: **44**
エンジニアが、複数のWANエッジデバイスが設置されているサイト上の単一のWANエッジデバイスに対して、IPv4プレフィックスのデータポリシーを設定しています。ポリシー設定ウィザードを使用して、このポリシーを追加するにはどうすればよいでしょうか？
A. vBond Orchestratorで、[構成] --> [ポリシー]画面を選択し、[ローカライズされたポリシー]タブを選択して、[ポリシーの追加]をクリックします。
B. vManage NMSで、[構成] --> [ポリシー]画面を選択し、[ローカライズされたポリシー]タブを選択して、[ポリシーの追加]をクリックします。
C. vSmartコントローラーで、[構成] --> [ポリシー]画面を選択し、[ローカライズされたポリシー]タブを選択して、[ポリシーの追加]をクリックします。
D. vManage NMSで、[構成] --> [ポリシー]画面を選択し、[集中ポリシー]タブを選択して、[ポリシーの追加]をクリックします。
正解: **(**正解を表示します**)**
vManage is the central management and orchestration platform for Cisco SD-WAN, and it provides a user-friendly interface for configuring policies. When creating a data policy specific to a WAN Edge device within a site, the "localized policy" tab is often the appropriate place to define site-specific policies.

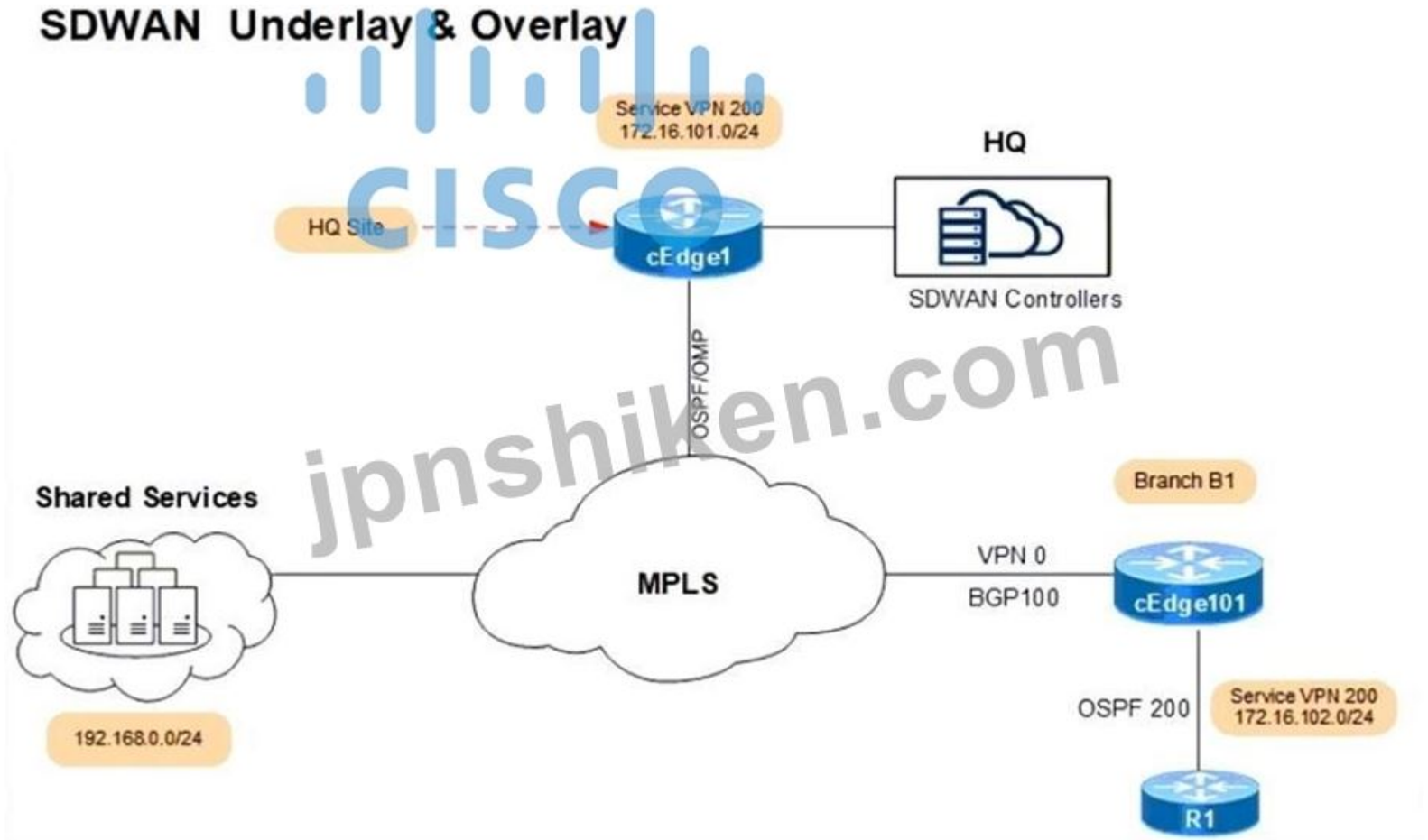
質問: **45**
vManageでユーザーグループに割り当てることができる権限の種類は、次のうちどれですか？(2つ選択)
A. 再起動
B. 消去
C. 読む
D. 管理する
E. 書き込み
正解: **C,E (**コメントを発表する**)**

質問: **46**
OMP が WAN エッジ ルータ間の TLOC ルートをアドバタイズするときに使用する識別子のセットはどれですか (2 つ選択してください)。
A. TLOC パブリックおよびプライベート アドレス、キャリア、および設定
B. 送信元と宛先の IP アドレス、MAC、サイト ID
C. システムIPアドレス、リンクカラー、カプセル化
D. VPN ID、ローカルサイトネットワーク、BGPネクストホップIPアドレス
E. TLOC パブリック アドレスとプライベート アドレス、トンネル ID、パフォーマンス
正解: **(**正解を表示します**)**
The identifiers that OMP carry when advertising TLOC routes to WAN Edge devices are:
- System IP address of the OMP speaker that originates the OMP route
- Color to identify the link type
- Encapsulation type on the transport tunnel
Origin (Source of the route, such as BGP, OSPF, connected, and static, and the metric associated with the original route).
Originator (OMP identifier of the originator of the route, which is the IP address from which the route was learned).
Preference (Degree of preference for an OMP route. A higher preference value is more preferred).
Service (Network service associated with the OMP route).
Site ID (Identifier of a site within the Cisco SD-WAN overlay network domain to which the OMP route belongs).

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
VPN 0 のどの vBond システム構成では、vBond オーケストレーターの DNS 名、ホスト名、または IP アドレスが省略されている場合でも、ルーティング可能なパブリック IP アドレスが使用できますか？
A. WAN
B. vbond専用
C. ローカル
D. DNS名
正解: (正解を表示します)

質問: **48**
図を参照してください。172.16.102.0/24 サブネットと 192.168.0.0/24 サブネット間の接続を確立する構成はどれですか？



CISCO
jpnshiken.com

A.
```
vrf definition 200
 address-family ipv4
   route-replicate from vrf global unicast bgp 100
```

B.
```
vrf definition 200
 address-family ipv4
  route-replicate from vrf global unicast ospf 200
```

C.
```
vrf definition 200
 global-address-family ipv4
   route-replicate from vrf global unicast ospf 200
```

D.
```
vrf definition 200
 global-address-family ipv4
  route-replicate from vrf 200 unicast bgp 100
```

正解: (正解を表示します)

To enable connectivity between the 192.168.0.0/24 shared services subnet (learned via BGP 100 in the global routing table) and the 172.16.102.0/24 subnet in VRF 200, the correct configuration is:

vrf definition 200

address-family ipv4

route-replicate from vrf global unicast bgp 100

This command replicates BGP routes from the global VRF into VRF 200, allowing the branch site to reach shared services.

質問: **49**

WANエッジルーターでSNMPv3モニタリングを構成するときに、ユーザーを認証する2つのアルゴリズムはどれですか。(2つ選んでください。)

A. AES-256

B. SHA-1

C. AES-128

D. MD5

E. SHA-2

正解: (正解を表示します)

https://sdwandocs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Configuratio n/Templates/SNMP



jpnshiken.com

質問: **50**

Cisco SD-WAN Cloud OnRampソリューションは、指定された経路を介して支店からクラウドへのSaaSアプリケーションのパフォーマンスをどのように評価しますか？

A. 優先度キューのパケット損失を監視します。

B. 体験の質スコアを計算します。
C. パスの遅延とジッターを測定します。
D. インターフェースエラーの数をカウントします。
正解: **B** (コメントを発表する)
The Cisco SD-WAN Cloud OnRamp solution rates the performance of a SaaS application by computing a quality-of-experience (QoE) score for each available path. This score is based on several factors, including delay, jitter, and packet loss, allowing the SD-WAN to intelligently route traffic to the optimal path for the best user experience.

質問: **51**
追加モジュールなしで、ティア3ライセンスで提供される最大帯域幅をネイティブにサポートするSD-WANデバイスはどれですか？
A. ISR 1100-6G
B. シスコ 4451
C. C8300-2N2S-4T2X
D. C8200L-1N-4T
正解: (正解を表示します)

質問: **52**
オーバーレイネットワークでは、個々のアプリケーションはユーザーごとにどのように監視されますか？
A. 利用可能性
B. 帯域幅
C. トンネル
D. パフォーマンス
正解: (正解を表示します)
In an overlay network, the performance of individual applications on a per-user basis is monitored to assess metrics such as latency, packet loss, and jitter. This allows network administrators to evaluate how well applications are performing for each user and identify any potential issues affecting application delivery.

質問: **53**
アプリケーション認識型エンタープライズファイアウォールポリシーは、同一のWANエッジルーター内でどのように適用されるべきでしょうか？
A. ゾーンペア内
B. ゾーン内およびゾーン間
C. 2つのVPNトンネル間
D. 2 つの VRF 間
正解: (正解を表示します)
Traffic flows that originate in a given zones are allowed to proceed to another zone based on the policy between the two zones. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones.
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-firewall-compliance- deploy-guide-2020sep.pdf

質問: **54**
Cisco SD-WAN環境でDREをサポートするために、どのような条件を満たす必要がありますか？
A. クライアント/サーバートポロジー
B. TCP最適化

C. ハブアンドスポーク型トポロジー
D. 流れの対称性
正解: (正解を表示します)
In a Cisco SD-WAN environment, DRE (Data Redundancy Elimination) requires flow symmetry to function properly. DRE is a WAN optimization feature that reduces bandwidth usage by eliminating redundant data patterns in traffic. For DRE to work effectively, the traffic must take the same path (symmetry) between two endpoints, ensuring that both directions of the traffic flow are optimized consistently.

質問: **55**
Cisco SD-WAN Cloud OnRampアーキテクチャにおいて、vManageはどのコンポーネントを自動的にデプロイしますか？
A. コア相互接続用のルーター2台
B. WANエッジ仮想ルーター
C. 仮想ネットワークとワークロード
D. リソースグループ
正解: (正解を表示します)
In a Cisco SD-WAN Cloud OnRamp architecture, vManage automatically deploys the WAN edge virtual router. This component is essential for extending the SD-WAN capabilities to cloud environments, enabling optimized performance and connectivity for applications running in the cloud.

質問: **56**
vSmartにアクセスできない場合、またはWAN EdgeからvSmartに接続できない場合、WAN Edgeデバイスはどのように動作しますか？
A. 通常通り運用を継続します。
B. 設定可能な時間、通常どおり動作し続けます。
C. 引き続き接続状況の更新情報を受け取ります。
D. データプレーンでのトラフィック転送を停止します。
正解: (正解を表示します)

質問: **57**
Cisco SD-WANノードのソフトウェアアップグレードにおける操作順序は？
A. vBond、vManage、vSmart、WAN Edge
B. vManage、vBond、vSmart、WAN Edge
C. vManage、vBond、WAN Edge、vSmart
D. vManage、vSmart、vBond、WAN Edge
正解: **B** (コメントを発表する)
When you upgrade a group of Cisco vBond Orchestrator, Cisco vSmart Controllers, and Cisco IOS XE SD-WAN devices or Cisco vEdge devices in either a standalone or Cisco vManage cluster deployment, the software upgrade and reboot is performed first on the Cisco vBond Orchestrator, next on the Cisco vSmart Controller, and finally on the Cisco IOS XE SD-WAN devices or Cisco vEdge devices.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And- Maintain/monitor-maintain-book/maintain.html

質問: **58**
エンジニアがVPN 10用のDIA向けデータポリシーを作成します。

```
data-policy DIA
 vpn-list VPN-10
  sequence 10
   match
    destination-data-prefix-list INTERNAL-NETWORKS
  !
  action accept
```

どのポリシーシーケンスが外部ネットワークのDIAを有効にしますか？

A.
```
sequence 20
 match
  destination-ip 0.0.0.0/0
 !
 action accept
  nat use-vpn
```

B.
```
sequence 5
 match
  source-ip 0.0.0.0/0
 !
 action accept
  nat use-vpn 0
```

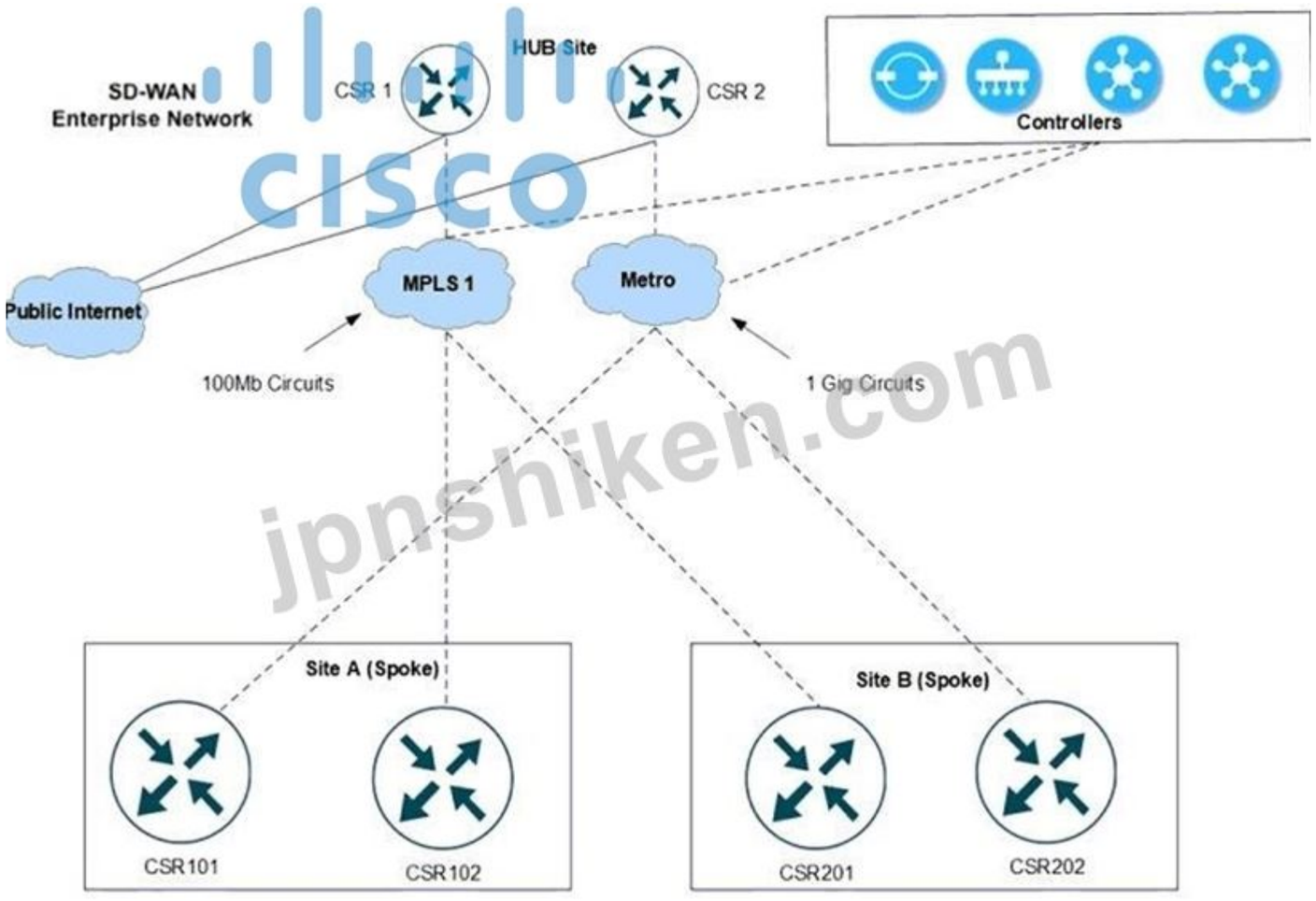
C.
```
sequence 5
 match
  destination-Ip 0.0.0.0/0
 !
 action reject
 !
!
default-action accept
```

D.
```
sequence 20
 match
  source-Ip 0.0.0.0/0
 !
 action reject
 !
 !
 default-action accept
```

正解: (正解を表示します)

質問: **59**

図を参照してください。Cisco SD-WANネットワークは複数の部門のトラフィックを伝送し、
サイトAとサイトBの支店には、MPLS1回線を介して複数のアプリケーションを使用する1200人のユーザーがいます。エンジニアは、バックアップ接続として、より帯域幅の広いオンデマンドのメトロ回線をプロビジョニングしています。
オンデマンドトンネルを実装するために、エンジニアはどの2つの構成を適用する必要がありますか？(2つ選択してください。)



A.
```
Spokes

omp
 no shutdown
 ecmp-limit 16

system
 on-demand enable
 on-demand idle-timeout 10
```

B.
```
Hubs

sdwan
  service TE vrf global
exit

system
  on-demand enable
  on-demand idle-timeout 10
```

C.
```
Hubs

sdwan
  service TE vrf global
exit
```

D.
```
Spokes

sdwan
  service TE vrf global
exit

omp
  no shutdown
  ecmp-limit 16
```

E.
```
Spokes

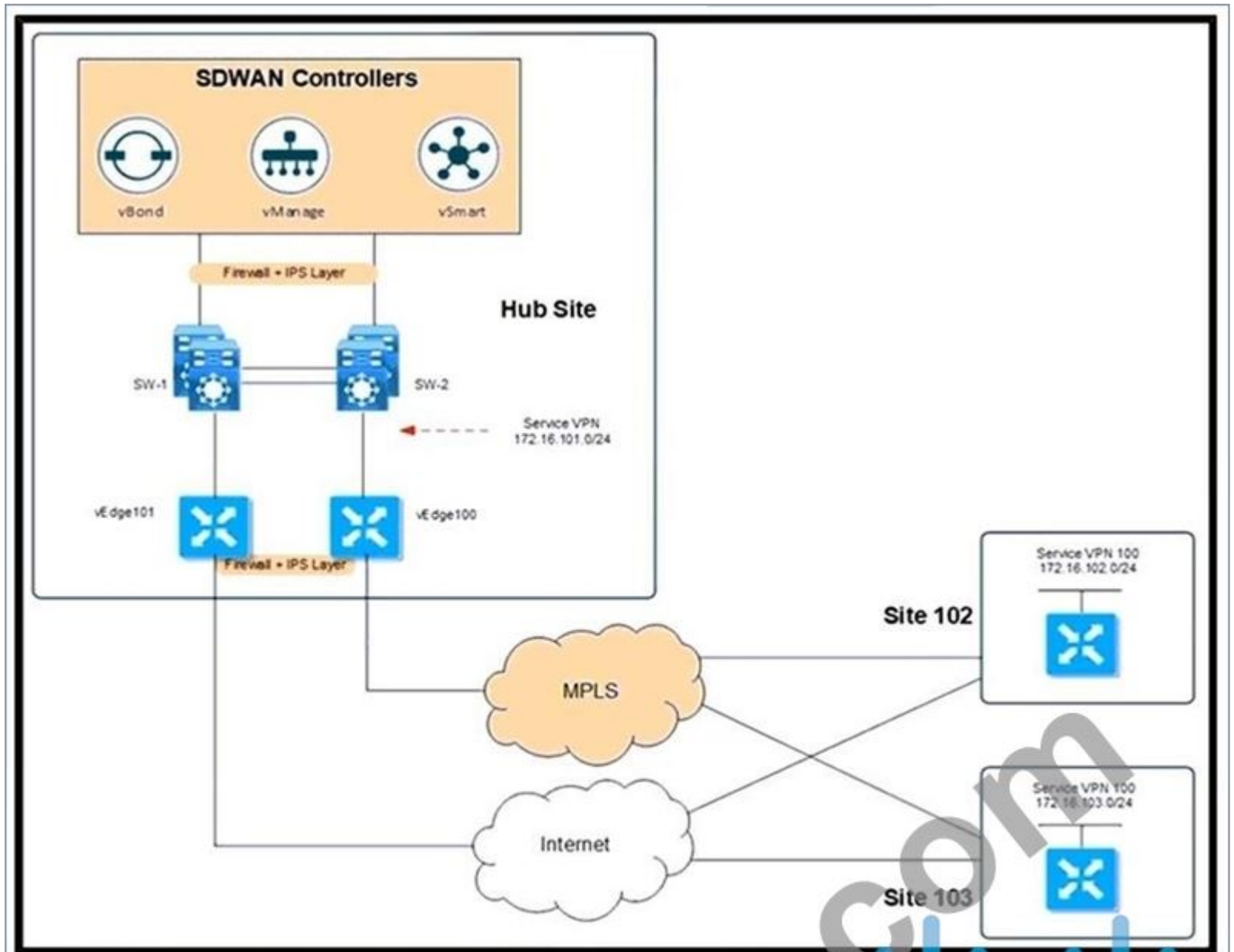
vpn 0
  service TE
  exit

omp
  no shutdown
  ecmp-limit 16
```

正解: (正解を表示します)

質問: **60**

図を参照してください。ある企業は、スポークサイト102と103が、サイト101(ハブサイト)によってアドバタイズされる172.16.101.0/24サブネット(サービスVPN 100)に到達するためにMPLS回線を使用することを要求しています。この要件を満たすポリシー構成はどれですか？

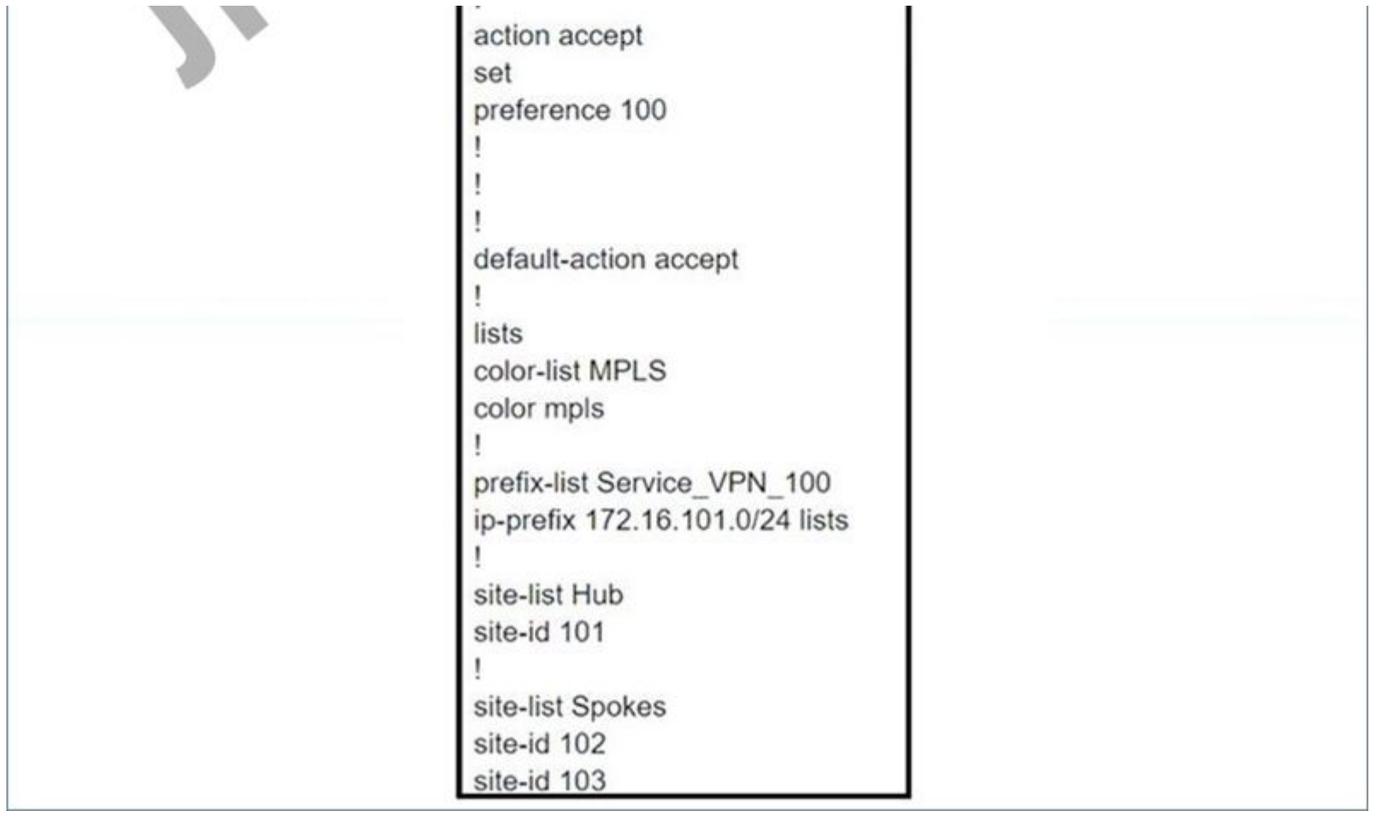



```
vEdge-Site102# show ip fib 172.16.101.0/24 | tab

ADDRESS OUT NEXTHOP NEXTHOP SA
VPN FAMILY ROUTE PATH IFNAME ADDRESS LABEL INDEX TLOC IP COLOR
-------------------------------------------------------------------------------
1 ipv4 172.16.101.0/24 1 ipsec 10.0.0.0 1 15 10.101.1.1 mpls
1 ipv4 172.16.101.0/24 2 ipsec 10.0.0.2 1 13 10.101.1.1 public-internet
```

```
viptela-policy:policy
control-policy Route-Policy
sequence 1
match route
color-list MPLS
prefix-list Service_VPN_100
!
```

ipnshiken.com
CISCO



A. ポリシー適用
サイトー覧 スポーク
制御ポリシー ルートポリシー
B. ポリシーを適用
サイトー覧 スポーク
コントロールポリシー ルートポリシー 出力
C. ポリシーを適用
サイトリストハブ
制御ポリシー ルートポリシー
D. ポリシーを適用
サイトリストハブ
コントロールポリシー ルートポリシー 出力
正解: **A** (コメントを発表する)
To ensure that spoke sites (102 and 103) prefer the MPLS path when reaching the
172.16.101.0/24 subnet from site 101 (Hub), the control policy must be applied inbound on the Spokes.
This way, vSmart modifies the route advertisements as they are sent to the spoke sites, setting higher preference (100) for the MPLS TLOC.

質問: **61**
管理者は、アクションをすぐに実行する必要があることを示すイベントについて、vManageNMSで重大度レベルを構成しています。どの重大度レベルを構成する必要がありますか？
A. 警告
B. エラー

C. クリティカル
D. アラート
正解: **C** (コメントを発表する)
The "critical" severity level is typically used for events that require immediate attention or action.

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
エンジニアが、172.20.21.0/24 ネットワークから 172.20.41.0/24 ネットワークへの通信を防止するデータ ポリシーを作成しました。このタスクを実現する構成はどれですか？

A.

```
policy
 lists
  vpn-list VPN1
  vpn 1
 !
  data-prefix-list LosAngeles-Net1
   ip-prefix 172.20.21.0/24
  data-prefix-list Rome-Net1
   ip-prefix 172.20.41.0/24
!
data-policy FILTER-POLICY
 vpn-list VPN1
  sequence 1
   match
    source-data-prefix-list      LosAngeles-Net1
    destination-data-prefix-list Rome-Net1
    action drop
 !
 default-action accept
```

```
policy
  lists
    vpn-list VPN1
    vpn 1
 !
    data-prefix-list LosAngeles-Net1
     ip-prefix 172.20.21.0/24
    data-prefix-list Rome-Net1
     ip-prefix 172.20.41.0/24
!
  data-policy FILTER-POLICY
    vpn-list VPN1
     sequence 1
      match
       source-data-prefix-list     LosAngeles-Net1
       action drop
  !
     sequence 11
      match
       source-data-prefix-list     Rome-Net1
       action drop
!
  default-action accept
```

B.

jprishiken.com

```
policy
  lists
    vpn-list VPN1
    vpn 1
  !
    data-prefix-list LosAngeles-Net1
     ip-prefix 172.20.0.0/16
    data-prefix-list Rome-Net1
     ip-prefix 172.20.0.0/16
!
  data-policy FILTER-POLICY
    vpn-list VPN1
     sequence 1
      match
       source-data-prefix-list     LosAngeles-Net1
       destination-data-prefix-list Rome-Net1
       action drop
    !
    default-action accept
```

C.

```
policy
  lists
    vpn-list VPN1
    vpn 1
  !
    data-prefix-list LosAngeles-Net1
     ip-prefix 172.20.21.0/24
    data-prefix-list Rome-Net1
     ip-prefix 172.20.41.0/24
!
  data-policy FILTER-POLICY
    vpn-list VPN1
     sequence 1
      match
       source-data-prefix-list     LosAngeles-Net1
       destination-data-prefix-list Rome-Net1
       action accept
!
  default-action drop
```

D.

正解: (正解を表示します)

質問: **63**

SD-WANセキュリティソリューションにおいて、マルウェア、フィッシング、および不適切なリクエストをブロックし、ユーザーに高速なインターネットアクセスを提供する機能はどれですか？
A. SaaS利用制御
B. DNSレイヤーの強制適用
C. クラウド配信型ファイアウォール
D. 相関脅威情報
正解: (正解を表示します)
DNS-layer enforcement is a security feature that blocks requests to malicious sites, phishing domains, and other unwanted content at the DNS level. By intercepting and filtering DNS requests, it provides a faster response than inspecting full traffic flows, as it prevents harmful connections before they are fully established. This approach enhances security by stopping threats early and also contributes to faster internet access for users by reducing the amount of traffic that needs to be inspected further down the line.

質問: **64**
Smart Account Syncを使用しない場合、許可されたシリアル番号ファイルのアップロードに使用されるCiscoSD-WANコンポーネントはどれですか。
A. WANエッジ
B. vManage
C. vSmart
D. vBond
正解: (正解を表示します)
https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Devices

質問: **65**
ある銀行は、アプリケーションにおける顧客体験の向上と、コンプライアンスおよびセキュリティ関連のオーバーヘッド削減を目指しています。Cisco SD-WANソリューションのどの主要機能が、この銀行の目標達成に役立つでしょうか？
A. PaaSプロバイダーとの統合により、可能な限り最高のアプリケーションエクスペリエンスを提供します
B. 最適なパスを選択するためのアプリケーションの優先順位付けと重要なアプリケーションのSLAを満たすことを含むQoS。
C. 現代のコアバンキングシステムの導入
D. 最適なパスを選択するためのエンタープライズルーティング全体にわたるBGPの実装
正解: (正解を表示します)
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol- overview-cte-en.html#Uniquecapabilities

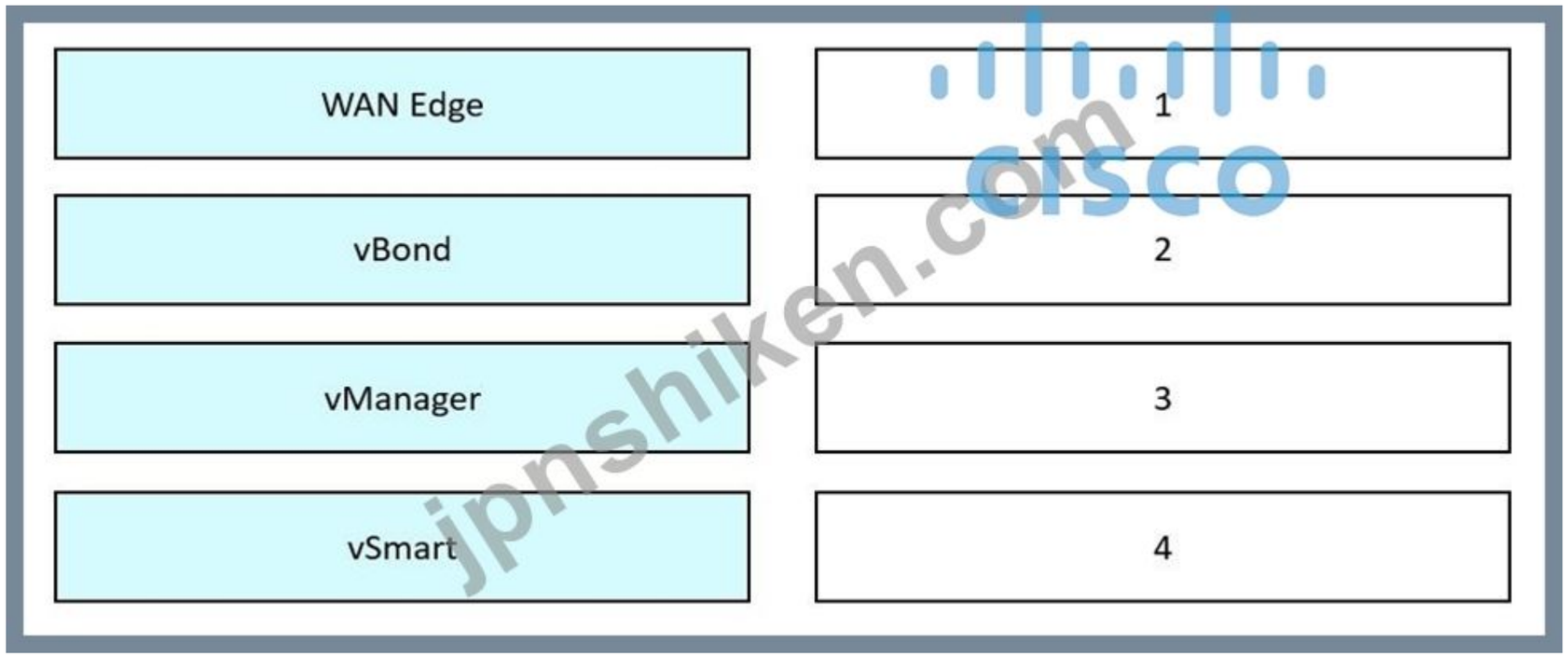
質問: **66**
SD-WAN Managerを使用してWANエッジルーターのソフトウェアをアップグレードする際に、リスクを最小限に抑え、ネットワークの安定性を確保するための最適なアプローチは何ですか？
A. ダウンタイムを最小限に抑えるため、全拠点のすべてのWANエッジルーターを同時にアップグレードします。
B. まずリスクの低いサイトのWANエッジルーターのごく一部をアップグレードし、その後残りのサイトを段階的にアップグレードします。
C. 利用可能な帯域幅が最も高いWANエッジルーターのアップグレードを優先します。
D. 1 つのサイトのすべての WAN エッジ ルーターを同時にアップグレードし、その後、サイトごとにそれを繰り返します。
正解: (正解を表示します)
The recommended and safest approach for upgrading WAN Edge routers is to start with a small, low-risk site to validate the upgrade process, verify stability, and catch potential issues early.

Once confirmed successful, you can proceed to upgrade additional sites gradually. This minimizes network disruption and overall risk.

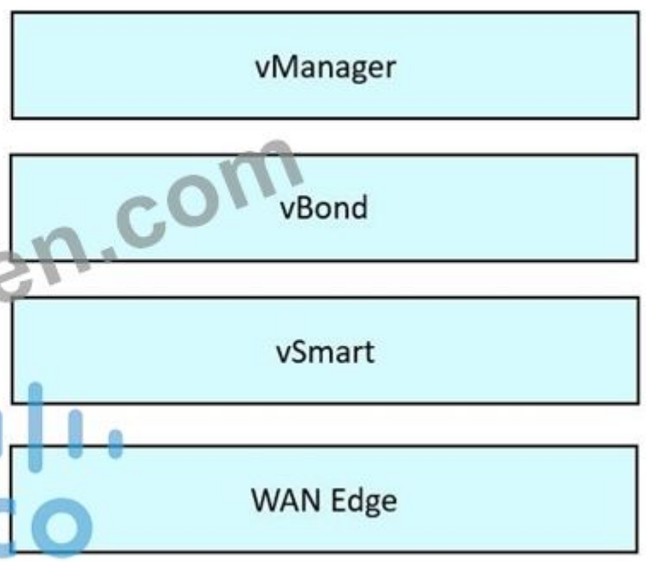
質問: **67**
アプリケーション認識型ファイアウォールを構成する2つの要素は何ですか？(2つ選択してください。)
A. デフォルトのアクション
B. シーケンス
C. ゾーンペア
D. リスト
E. ファイアウォールポリシー
正解: (正解を表示します)
Two components that are valid within the options here are:
- Zone Pair
- Firewall Policy
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge-20-x/security- book/ent-firewall-app-aware.pdf

質問: **68**
Cisco SD-WAN WAN Edgeプラットフォームのうち、LTEとWi-Fiをサポートしているのはどれですか？
A. vEdge 2000
B. CSR 1000V
C. ISR 1101
D. ASR 1001
正解: (正解を表示します)

質問: **69**
ドラッグアンドドロップ問題
ソフトウェアをバージョン19からバージョン20にアップグレードするには、左側のデバイスを右側の順番にドラッグアンドドロップしてください。



正解:



jpnshiken.com

質問: **70**

WANエッジルータは、IPsecトンネル作成時にデフォルト以外のオフセット値を使用するようにUDPポートオフセットを手動で設定します。オフセットの範囲はどのくらいですか？

A. 1-19

B. 0-18

C. 0-19

D. 1-18

正解: **(**正解を表示します**)**

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

質問: **71**
OMPエージェントおよびSD-WANサブシステムの「イベントトレース」を監視する主な目的は何ですか？
A. SD-WANマネージャとSD-WANサブシステム間のSD-WANトラッキングの診断を実行する機能を提供します。
B. Cisco IOS XE デバイスおよび SD-WAN サブシステムのイベント通知のサポートを追加します。
C. Cisco WAN EdgeルータおよびSD-WANサブシステムのイベントアラートのサポートを追加します。
D. SD-WANデーモンとSD-WANサブシステム間のSD-WANトレースをキャプチャする機能を提供します。
正解: (正解を表示します)
Event Trace is primarily used to capture detailed trace logs of communication and events occurring between SD-WAN daemons (like OMP agent) and other SD-WAN subsystems. This helps in deep troubleshooting and understanding the behavior of control plane processes.

質問: **72**
レプリケータの役割は、Cisco SD-WANでどのように機能しますか？
A. WANエッジデバイスは、アンダーレイネットワークを介してすべての受信者にランデブーポイントをアドバタイズします。
B. vSmartコントローラーは、オーバーレイネットワークを介してすべての受信者にランデブーポイントをアドバタイズします。
C. WANエッジデバイスは、オーバーレイネットワークを介してすべての受信者にランデブーポイントをアドバタイズします。
D. vSmartコントローラーは、アンダーレイネットワークを介してすべてのレシーバーにランデブーポイントをアドバタイズします。
正解: (正解を表示します)
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.

質問: **73**
AWSクラウドでは、Cisco SD-WANでWANエッジルーターを自動的にプロビジョニングする機能はどれですか。
A. クラウドアプリ
B. Cloud OnRamp
C. vAnalytics
D. ネットワークデザイナー
正解: (正解を表示します)



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

質問: **74**
Cisco Catalyst SD-WANネットワークにおいて、2つのストリームのマルチキャスト受信機の位置を取得するために、レプリケーターのアドレスをイングレスルータに送信するデバイスはどれですか？
A. SD-WAN検証

B. SD-WANマネージャー
C. SD-WANコントローラー
D. WANエッジ
正解: (正解を表示します)
In Cisco Catalyst SD-WAN multicast, the SD-WAN Controller (vSmart) is responsible for providing the ingress WAN Edge with the replicator addresses. This allows the ingress router to know where multicast receivers are located and forward the two streams accordingly.

質問: **75**
VPN2において、出力方向のブランチに割り当てられた制御ポリシーのうち、厳密なハブアンドスポーク型トポロジーを確立するのはどれか？

```
policy
 lists
  vpn-list VPN2
   vpn2
 !
site-list hub_sites
 site-id 1-2
 !
!
control-policy vpn_multi-topology
 sequence 10
  match route
  site-list hub_sites
  vpn-list VPN2
 !
  action accept
!
sequence 20
 match route
!
  action reject
!
```

A. default-action accept

```
policy
lists
 vpn-list VPN2
  vpn2
!
site-list branch_sites
 site-id 100-200
!

control-policy vpn_multi-topology
 sequence 10
  match route
   site-list branch_sites
   vpn-list VPN2
 !
  action accept
   set
   tloc 1.1.1.1 color red
   !
 !
```

B.

```
default-action accept
 policy
  lists
   vpn-list VPN2
    vpn2
  !
 site-list hub_sites
  site-id 1-2
  !
 !
 control-policy vpn_multi-topology
  sequence 10
   match route
   site-list hub_sites
    vpn-list VPN2
  !
   action accept
  !
  sequence 20
   match route
   vpn-list VPN2
  !
   action reject
  !
```

C.

```
default-action accept
```

D.

```
policy
 lists
  vpn-list VPN2
   vpn2
 !
site-list branch_sites
 site-id 1-100
 !
!
control-policy vpn_multi-topology
 sequence 10
  match route
   site-list branch_sites
   vpn-list VPN2
 !
 action accept
  set
  tloc 100.1.1.1 color mpls
  !
 !
!
default-action accept
```

正解: (正解を表示します)

質問: **76**

エンジニアは、クラス マップを作成し、それを WAN エッジ ルータ上の LLQ キューに割り当てることによって、QoS ポリシーを作成する必要があります。どの構成でこのタスクを達成できますか。

A.



B.



C.

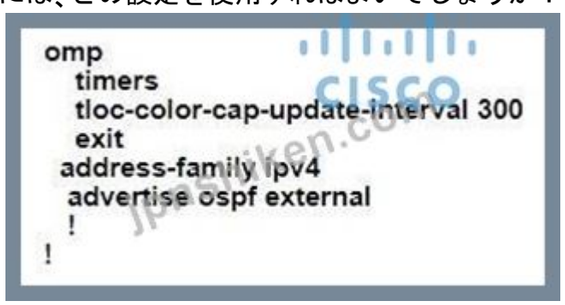

D.


正解: **D** (コメントを発表する)

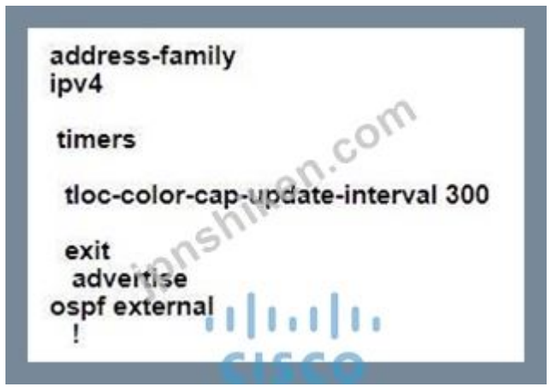
有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**

エンジニアは、OSPFで学習したルートをアドバタイズし、SD-WANデバイス上でTLOCカラーによるルートフィルタリングの更新間隔を300に変更する必要があります。このタスクを実行するには、どの設定を使用すればよいでしょうか？

A.


B.



C.

```
address-family ipv4
  advertise ospf external
  tloc-color-cap-update-interval 300
  !
```

D.

```
omp
 address-family ipv4
  advertise ospf external
  tloc-color-ca-update-interval 300
 !
!
```

正解: **A** (コメントを発表する)

Advertise OSPF-learned routes into OMP - the correct command is advertise ospf external under address-family ipv4.

Modify TLOC color capability update interval - this is set using tloc-color-cap-update-interval under the omp timers section.

質問: **78**

クラウドオンランプ環境におけるユーザーエクスペリエンス品質を計算するコンポーネントはどれですか？

A. WANエッジデバイス

B. SD-WANバリデーター

C. SD-WANコントローラー

D. SD-WANマネージャー

正解: (正解を表示します)

In a Cisco SD-WAN Cloud OnRamp environment, the Quality of Experience (QoE) for applications is measured and calculated by the WAN Edge device. The WAN Edge device monitors real-time network conditions, such as latency, jitter, and packet loss, and uses these metrics to calculate the QoE for applications. This information helps the SD-WAN system make intelligent routing decisions, ensuring optimal application performance based on network conditions.

質問: **79**

Cisco SD-WANアーキテクチャでは、WANエッジの役割は何ですか。

A. WANエッジルーターとオーバーレイの自動プロビジョニングを支援するオーケストレーションを提供します

B. 一元化された構成と監視を担当する管理プレーンです

C. ネットワークトポロジを構築および維持するのはコントロールプレーンです

D. トラフィックの転送を担当するのはデータプレーンです

正解: (正解を表示します)

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

質問: **80**
Cisco SD-WANコントロールプレーンアーキテクチャのどのコンポーネントが、ネットワークコンポーネントの証明書と構成の保存を容易にしますか？
A. vSmart
B. WAN Edge
C. vManage
D. vBond
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system- overview.html

質問: **81**
Cisco SD-WAN導入における構成グループの2つの利点は何ですか？(2つ選択してください。)
A. 個々のデバイスには複数のタグルールがあります。
B. 個々のデバイスは、共有構成に基づいてグループ化されます。
C. デバイスの一部がタグで識別されます。
D. 個々のデバイスが複数のグループに追加されます。
E. 個々のデバイスは、構成グループとデバイステンプレートに関連付けられています。
正解: (正解を表示します)

質問: **82**
Cisco UmbrellaリゾルバがDNSリクエストをインテリジェントプロキシに転送するトリガーとなるのは、どのような問題ですか？
A. ドメインはローカルで到達可能です。
B. ドメインがブロックリストに登録されています。
C. ドメインが存在しません。
D. ドメインがグレーリストに登録されています。
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge-20-x/security- book/cisco-umbrella-integration.pdf

質問: **83**
ネットワーク エンジニアは、本社にあるサービス チェーン ファイアウォールを介してすべてのブランチが相互に通信できるように構成する必要があります。
エンジニアがこのタスクを達成できる構成はどれですか?

A. 

B. 

C. 

D. 

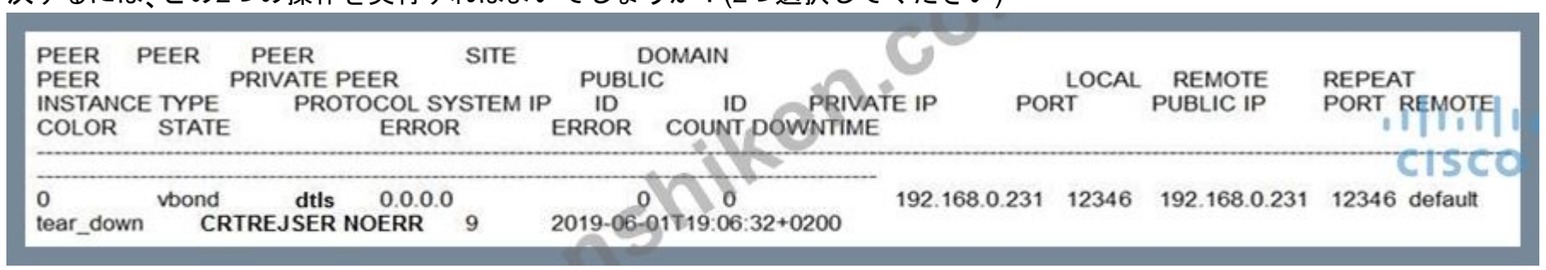
正解: (正解を表示します)

Centralized Policy applies to all sites branches.

- matches: braches's service LAN segment
- action: accept + set service route to FW (which is advertised from Hub site to vSmart)

質問: **84**

図を参照してください。エンジニアは、有効なCertificateSerialNumbreが入力されているにもかかわらず、制御接続が切断される問題のトラブルシューティングを行っています。この問題を解決するには、どの2つの操作を実行すればよいでしょうか？(2つ選択してください)

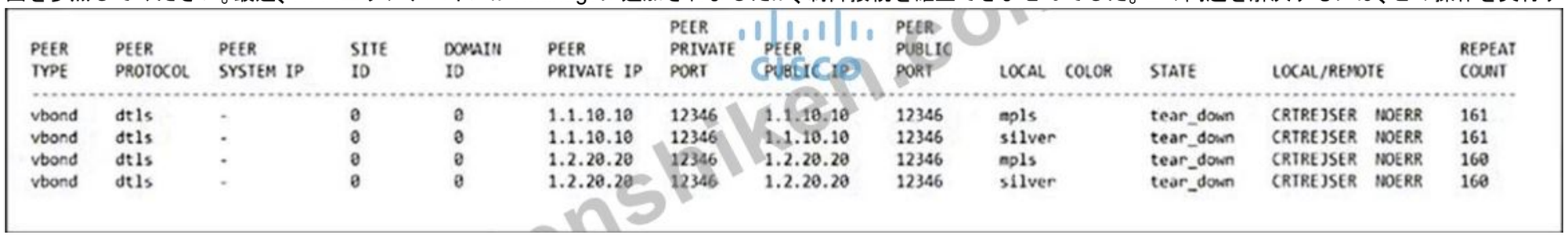


```
PEER    PEER    PEER            SITE       DOMAIN
PEER            PRIVATE PEER                PUBLIC                                  LOCAL   REMOTE      REPEAT
INSTANCE TYPE       PROTOCOL SYSTEM IP      ID         ID       PRIVATE IP          PORT    PUBLIC IP   PORT  REMOTE
COLOR    STATE                  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. 指定されたデバイスのコントローラーに有効なシリアル番号を入力してください
B. ネットワーク内の重複するIPを削除します。
C. PNPポータルで有効な製品ID(モデル)を入力してください
D. コントローラー間でシリアル番号ファイルを一致させる
E. コントローラのネットワーク接続性を復元します
正解: **A,C** (コメントを発表する)
https://community.cisco.com/t5/networking-documents/sd-wan-routers-troubleshoot-contro- connections/ta-p/3813237

質問: **85**
エンジニアはvManageのどこで制御ノードの障害の詳細を見つけますか？
A. アラーム
B. イベント
C. 監査ログ
D. ネットワーク
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/vManageHow-Tos/vmanage-howtobook/m- troubleshooting.html

質問: **86**
図を参照してください。最近、WANエッジデバイスがvManageに追加されましたが、制御接続を確立できませんでした。この問題を解決するには、どの操作を実行すればよいでしょうか？

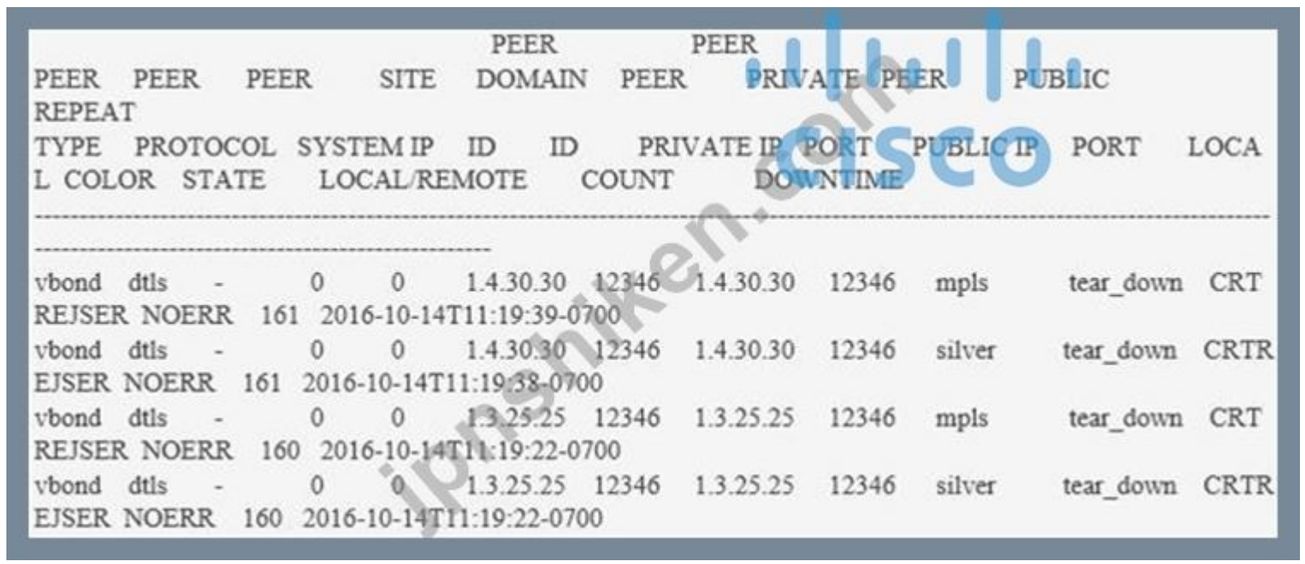


PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	LOCAL COLOR	STATE	LOCAL/REMOTE	REPEAT COUNT
vbond	dtls	-	0	0	1.1.10.10	12346	1.1.10.10	12346	mpls	tear_down	CRTREJSER NOERR	161
vbond	dtls	-	0	0	1.1.10.10	12346	1.1.10.10	12346	silver	tear_down	CRTREJSER NOERR	161
vbond	dtls	-	0	0	1.2.20.20	12346	1.2.20.20	12346	mpls	tear_down	CRTREJSER NOERR	160
vbond	dtls	-	0	0	1.2.20.20	12346	1.2.20.20	12346	silver	tear_down	CRTREJSER NOERR	160

A. WANエッジデバイス上のルートCA証明書の不一致を修正します。
B. ZTP の到達可能性を解決し、スマート アカウント認証情報の問題を修正します。
C. WAN Edge にブートストラップ コードをインストールし、CSR を確認します。
D. vManageコントローラからvBondにシリアル番号を送信します。
正解: **D** (コメントを発表する)
Problem Statement
A device's serial number is missing from the vSmart controllers.

Identify the Problem

Issue the show control connections-history command. In the Local Error column of the output, the values BIDNTVRFD, CRTREJSER, and SERNTPRES indicate a missing serial number. BIDNTVRFD indicates a missing serial number for vBond orchestrators. CRTREJSER indicates a missing serial number for vEdge routers and vSmart controllers. SERNTPRES on a vBond orchestrator indicates a serial number mismatch between vSmart controllers.



```
                                        PEER          PEER
PEER   PEER    PEER      SITE    DOMAIN   PEER      PRIVATE PEER      PUBLIC
REPEAT
TYPE   PROTOCOL SYSTEM IP  ID      ID     PRIVATE IP  PORT  PUBLIC IP   PORT    LOCA
L COLOR  STATE    LOCAL/REMOTE     COUNT      DOWNTIME
-------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------
vbond  dtls   -       0       0      1.4.30.30   12346  1.4.30.30   12346   mpls       tear_down   CRT
REJSER NOERR  161  2016-10-14T11:19:39-0700
vbond  dtls   -       0       0      1.4.30.30   12346  1.4.30.30   12346   silver     tear_down   CRTR
EJSER NOERR   161  2016-10-14T11:19:38-0700
vbond  dtls   -       0       0      1.3.25.25   12346  1.3.25.25   12346   mpls       tear_down   CRT
REJSER NOERR  160  2016-10-14T11:19:22-0700
vbond  dtls   -       0       0      1.3.25.25   12346  1.3.25.25   12346   silver     tear_down   CRTR
EJSER NOERR   160  2016-10-14T11:19:22-0700
```

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.

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

質問**: 87**

図を参照してください。証明書を使用する場合、WANエッジをコントローラに登録するために必要な設定はどれですか？(2つ選択してください)



A. vManageサーバー内でCSRを手動で生成する
B. WANエッジでCSRを手動で生成する
C. エンタープライズCAサーバーから証明書を手動で要求する
D. CAサーバーから受け取った証明書をWANエッジに手動でインストールします。
E. CAサーバーから受け取った証明書をvManageに手動でインストールします
正解: **(**正解を表示します**)**
https://www.cisco com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/cisco-sd-wan-certificates- deploy-2020aug.pdf

質問: **88**
クラウドベースのvSmartコントローラーには、どのサードパーティ製エンタープライズCAサーバーを使用する必要がありますか？
A. ルート証明書
B. VeriSign
C. マイクロソフト
D. RADIUS
正解: **A (**コメントを発表する**)**
https://www.nterone.com/articles/cisco-sdwan-viptela-everything-you-wanted-to-know-about- certificates-deployment-but-were-afraid-to-ask

質問: **89**
2つのサイトにはそれぞれ1つのWANエッジがあります。各WANエッジには、制限が設定されていない2つのパブリックTLOCがあります。TLOC間は完全に接続可能です。
各エッジルーター上で、いくつのデータトンネルが形成されますか？
A. 6
B. 2
C. 4
D. 8
正解: **(**正解を表示します**)**

jpnshiken.com

By default, WAN Edge routers try to form an overlay tunnel to every TLOC over each available WAN transport, including TLOCs that belong to other colors if there is IP reachability between the two transport networks.

質問: **90**
Cisco SD-WANネットワークにおいて、vManageとファブリック間の接続が失われた場合、どのような2つの影響がありますか？
(2つ選択してください。)
A. ポリシー変更の伝播が停止します。
B. テンプレートの作成は不可能です。
C. WANエッジデバイス間のBFDピアリングが確立されました。
D. 統計情報の収集が停止します。
E. WANエッジデバイス用のIPsecトンネルが切断されます。
正解: **(**正解を表示します**)**
When SD-WAN Manager loses connectivity to the fabric, it can no longer push policy changes to the WAN Edge devices (A) or collect statistics and monitoring data (D). This can impact the network's ability to adapt to changes and monitor its performance effectively.

質問: **91**
エンジニアがvManageにロケーションID399533345のテナントを追加しています。提出されたテナント名で受け入れられる英数字の最大数はいくつですか？
A. 64
B. 128
C. 256
D. 8
正解: **B (**コメントを発表する**)**
In the Add Tenant window:

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

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
vManageにおける集中型ポリシー展開の2つの構成要素は何ですか？(2つ選択してください。)
A. ポリシー定義
B. リスト
C. QoSマップ
D. ポリシーベースルーティング
E. ルートポリシー
正解: **(**正解を表示します**)**
Policy definition is the process of creating a policy that specifies the traffic that you want to control. The policy definition includes the following elements:

The source and destination of the traffic.
The protocol and ports that the traffic uses.
The action that you want to take on the traffic.
Lists are used to group objects together. For example, you can create a list of all the servers that you want to protect with a firewall policy.
QoS map, policy-based routing, and route policy are not components of centralized policy deployment in vManage.

質問: **93**
エンジニアは、収束に関するSLAベースのポリシーに基づいて、トンネルの特性を追跡したいと考えている。
どのポリシー設定がこの目標を達成しますか？
A. アプリルーティングポリシー
B. VPNメンバーシップポリシー
C. 制御ポリシー
D. データポリシー
正解: (正解を表示します)
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.
https://sdwan-
docs.cisco.com/Product_Documentation/Software_FeaturesSDWAN_Release_16.2/07Policy_Ap plications/01ApplicationAware_Routing/01Configuring_Application-Aware_Routing

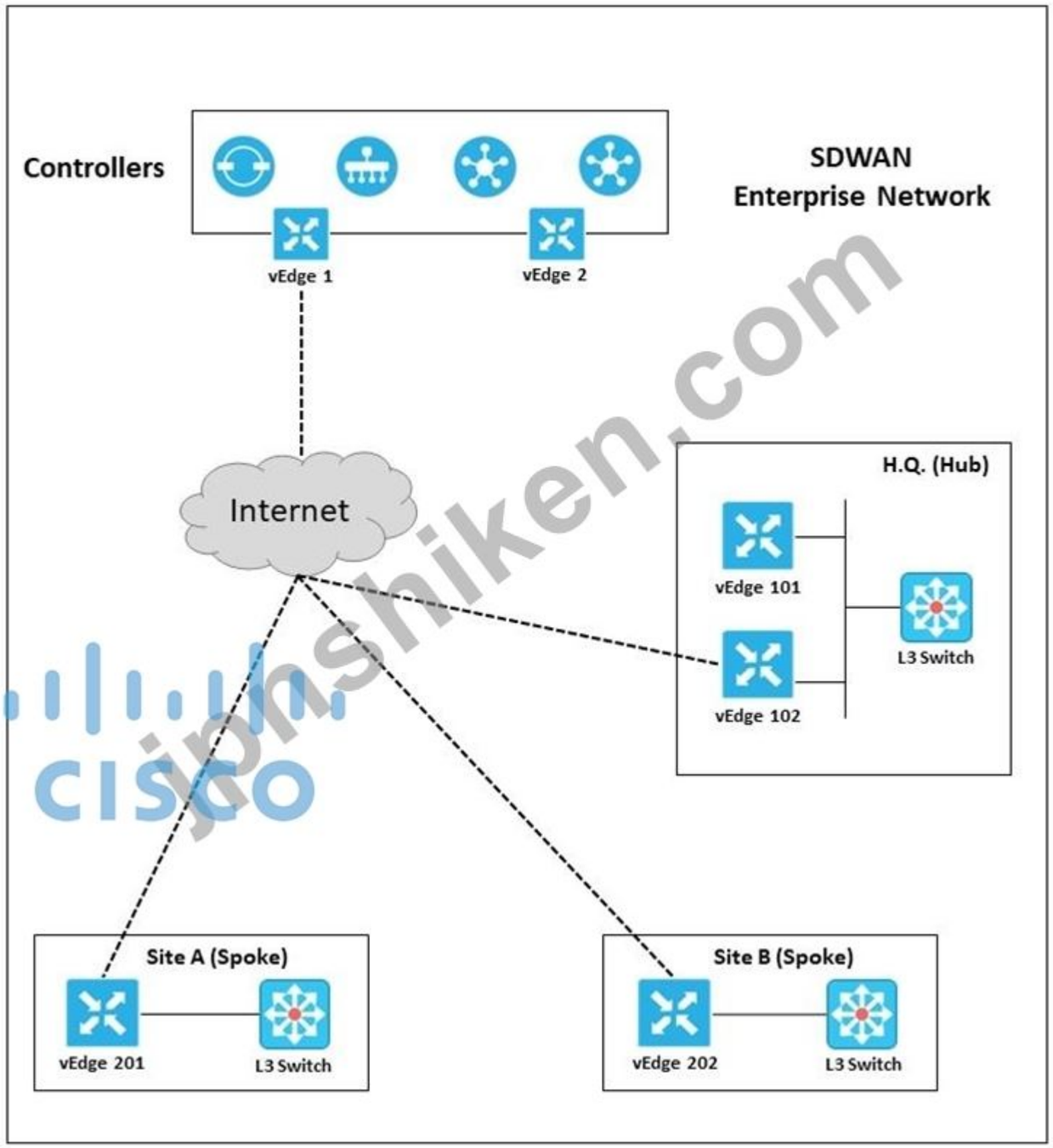
質問: **94**
図を参照して、どの構成がIPsecトンネルをアクティブ/スタンバイ状態に設定しているかを確認してください。



A. VPN 0
サービス netsvc1 インターフェース ipsec1 ipsec2
from-vsmartはvpn-list 0をリストします
VPN 0
B. VPN 1
サービス netsvc1 インターフェース ipsec1 ipsec2
VPNリスト 1
ServicePSec1_275676046 をカウントします
from-vsmartはvpn-list 1をリストします
VPN 1
C. VPN 0

サービス netsvc1 インターフェース ipsec1 ipsec2
VPNリスト 1
ServicePSec1_275676046 をカウントします
from-vsmartはvpn-list 0をリストします
VPN 0
D. VPN 1
サービス netsvc1 インターフェース ipsec1 ipsec2
from-vsmartはvpn-list 1をリストします
VPN 1
正解: **D** (コメントを発表する)

質問: **95**
図を参照してください。エンジニアは、ハブとサイトA(スポーク)間のQoSポリシーを標準的なインターネット回線上で設定する必要があります。このポリシーでは、利用可能な帯域幅に基づいてトラフィックシェーピングが調整されます。
どの構成が要件を満たしますか？


Controllers
SDWAN
Enterprise Network
vEdge 1
vEdge 2
Internet
H.Q. (Hub)
vEdge 101
vEdge 102
L3 Switch
Site A (Spoke)
vEdge 201
L3 Switch
Site B (Spoke)
vEdge 202
L3 Switch

A.

Site A (Spoke)

```
sdwan
 interface GigabitEthernet1
 qos-adaptive
  period 90
  downstream 8000
  downstream range 6000 10000
  upstream 8000
  upstream range 4000 16000
  exit
 tunnel-interface
  encapsulation ipsec weight 1
  color public-internet
  no last-resort-circuit
  vmanage-connection-preference 5
  allow-service all
```

B.

Site A (Spoke)

```
sdwan
 interface GigabitEthernet1
 qos-adaptive
  period 40
  downstream 10000
  downstream range 8000 12000
  upstream 9000
  upstream range 5000 16000
  exit
 tunnel-interface
  encapsulation ipsec weight 1
  color mpls
  no last-resort-circuit
  vmanage-connection-preference 5
  allow-service all
```

C.

```
Hub
sdwan
 interface GigabitEthernet1
 qos-adaptive
  period 90
  downstream 8000
  downstream range 6000 10000
  upstream 8000
  upstream range 4000 16000
  exit
 tunnel-interface
  encapsulation ipsec weight 1
  color public-internet
  no last-resort-circuit
  vmanage-connection-preference 5
  allow-service all
```

D.

```
Hub
sdwan
 interface GigabitEthernet1
 qos-adaptive
  period 40
  downstream 10000
  downstream range 8000 12000
  upstream 9000
  upstream range 5000 16000
  exit
 tunnel-interface
  encapsulation ipsec weight 1
  color mpls
  no last-resort-circuit
  vmanage-connection-preference 5
  allow-service all
```

正解: **B** (コメントを発表する)

質問: **96**

エンジニアがROME-POLICYというデータポリシーを設定しました。どの設定が、ローマ内部ネットワークから他のサイトへのトラフィックフローを許可しますか？

A.
```
apply-policy
 site-list Rome
  data-policy ROME-POLICY from-tunnel
```

B.
```
apply-policy
 site-list Rome
  data-policy ROME-POLICY from-service
```

C.
```
site-list Rome
 control-policy ROME-POLICY in
```

D.
```
site-list Rome
 control-policy ROME-POLICY out
```

正解: **B** (コメントを発表する)

質問: **97**

図を参照してください。ネットワークエンジニアが支店のユーザー向けにインターネットへの直接アクセスを設定しています。

サブネット 10.10.0.0/24 および 10.20.0.0/24 のユーザーは、インターネットに直接アクセスできる必要があります。vManage の 関心のあるグループの作成」セクションで、エンジニアはどの構成を使用してこのタスクを実行する必要がありますか？



A. VPN

B. data prefix

C. policer

D. site

正解: (正解を表示します)

In Cisco SD-WAN, the "Create groups of interest" section in vManage is used to define specific network attributes or groups that policies will apply to. To configure direct internet access (DIA) for particular subnets, you would define these subnets (e.g., 10.10.0.0/24 and 10.20.0.0/24) as data prefixes. The data prefix setting allows you to specify IP address ranges to which policies, such as routing or DIA policies, can be applied. This setup enables those specific subnets to have direct access to the internet based on the configured policy.

質問: **98**

ABC 社は、オンプレミス方式を使用してコントローラを導入することを決定しました。管理者はどのようにして WAN エッジ リストを vManage にアップロードするのでしょうか?

A.



B.





C.

D. 

正解: **(**正解を表示します**)**

https://sdwan-docs.cisco.com/Product Documentation/vManageHelp/Release18.3/Configuration/Devices

質問: **99**

SD-WANデータプレーンのトラフィックを暗号化するために使用される暗号化アルゴリズムは何ですか？

A. AES-256 GCM

B. トリプルDES

C. AES-128

D. IPsec

正解: **A (**コメントを発表する**)**

In the Cisco Catalyst SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetric-key algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets

質問: **100**

パスの状態(アップ／ダウン)を検出し、損失／遅延／ジッターを測定し、IPsecトンネルのMTUの品質を測定するプロトコルはどれですか？

A. DTLS

B. BFD

C. OMP

D. IP-SLA

正解: **B (**コメントを発表する**)**

Bidirectional Forwarding Detection (BFD) runs via the DTLS session between the remote site and the regional hub. BFD is a detection protocol that provides fast forwarding path failure detection times between two adjacent routers. It is used in SD-WAN to determine path liveliness (up/down) and quality (loss/latency/jitter and IPsec tunnel MTU).

質問: **101**

Cisco Catalyst SD-WAN Cloud OnRampにおけるコロケーション施設の機能は何ですか？

A. ブランチルータはトラフィックを認識し、SD-WAN Manager 内のポリシーに基づいて、コロケーション施設の適切なネットワーク機能を使用してトラフィックをルーティングします。

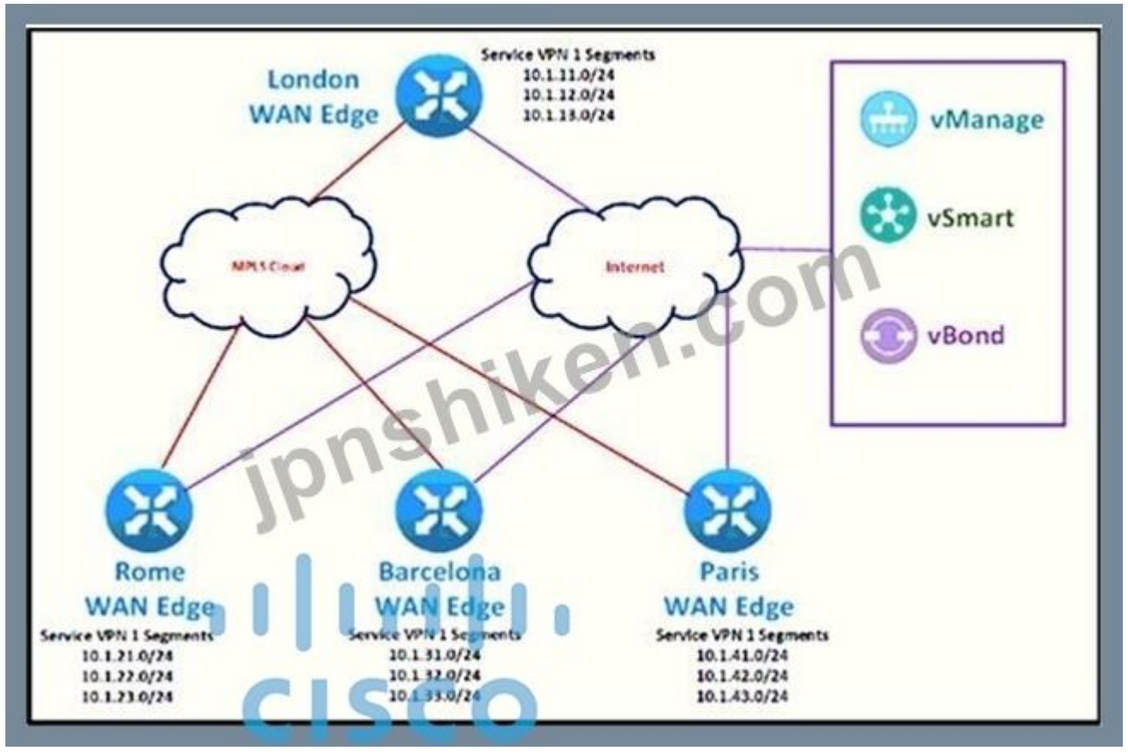
B. ユーザーは、SaaSプロバイダーのクラウドへの高速伝送を活用するために、遠隔地のコロケーションに効率的にトラフィックを転送します。

C. コロケーションソリューションでは、データトラフィックはコロケーション施設にルーティングされ、宛先に送信されてサービスを分散化します。

D. コロケーション クラスターは、SaaS プロバイダーのアプリケーションおよびインフラストラクチャに直接接続されていないコロケーションに配置されます。

正解: (正解を表示します)
In Cisco Catalyst SD-WAN Cloud OnRamp for Colocation, the colocation facility hosts virtualized network functions (VNFs) such as firewalls, IPS, or other security services. Traffic from branch sites is identified and steered by policy configured in SD-WAN Manager (vManage) so that it passes through the appropriate service hosted at the colocation site before reaching its destination. This enables service chaining using centralized network functions deployed in the colocation data center.

質問: **102**
図を参照してください。SD-WANネットワークは、デフォルトのフルメッシュトポロジーで構成されています。ネットワークエンジニアは、MPLSリンクが以下の特性を備えている限り、Rome WAN EdgeがTelnetトラフィックを転送する際に、優先TLOCとしてMPLS TLOCを使用するようにしたいと考えています。
損失 :5%
遅延時間 :100ms
ジッター: 100 ms
ネットワークエンジニアは、MPLSリンクの特性を分類するリストを作成するために、どの構成を使用する必要がありますか？



A.


Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN

B.


Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN

C.



D.



正解: (正解を表示します)

To configure a list that classifies the MPLS link characteristics (Loss: 5%, Latency: 100ms, Jitter:
100ms) in the Cisco SD-WAN environment, the network engineer should create an SLA class that defines these parameters.
Chosen option includes the necessary "SLA Class" option, which is what the engineer needs to define the acceptable loss, latency, and jitter thresholds for the MPLS TLOC.

質問: **103**
エンジニアは音声トラフィックの送信QoSを設定する必要があります。このタスクを実行するために、エンジニアはWANエッジルータでどのキューを設定する必要がありますか？
A. キュー 0
B. キュー 1
C. キュー 3
D. キュー 7
正解: **A** (コメントを発表する)
Queue 0 is reserved for Low Latency Traffic or (LLQ) in other words voice traffic.
Queues 1-7 are available for data traffic.
https://www.cisco.com/c/en/us/support/docs/routers/vedge-router/213408-implement-qos-in- cisco-sd-wan.html

質問: **104**
顧客は、AWSのトランジットVPC内に仮想SD-WANルーターをデプロイすることで、Cisco SD-WAN IaaSサービスにAWSを利用したいと考えています。トランジットVPCは、サイト間IPsecトンネルを介してAWSトランジットゲートウェイに接続されます。
どのトランジットVPCが、サイト間IPsecトンネルを介してAWSトランジットゲートウェイに接続しますか？
A. Cisco Cloud onRamp for SaaS
B. コロケーション向け Cisco Cloud onRamp
C. Cisco Cloud onRamp for IaaS
D. マルチクラウド向けCisco Cloud onRamp
正解: (正解を表示します)
Cisco Cloud OnRamp for IaaS is designed to simplify and optimize connectivity between on- premises locations, Cisco SD-WAN components, and public cloud environments like AWS.
The key components and functionalities of Cisco Cloud OnRamp for IaaS in this scenario include:
Transit VPC: The transit AWS VPC serves as a hub, where the virtual SD-WAN routers are deployed. These SD-WAN routers are responsible for efficiently connecting the customer's on-premises network with resources in the AWS cloud.
AWS Transit Gateway: The AWS Transit Gateway provides centralized routing and connectivity management for multiple Amazon VPCs, including the transit VPC and other VPCs within the AWS environment. It simplifies and streamlines the routing of traffic between the VPCs and the on-premises network.
Site-to-Site IPsec Tunnels: Site-to-site IPsec tunnels are used to secure the communication between the SD-WAN routers in the transit VPC and the AWS Transit Gateway, ensuring the confidentiality and integrity of data in transit.

質問: **105**
コントローラーの証明書認証モードをルート証明書を示すように設定するために必要な2つの操作はどれですか？(2つ選択してください。)
A. ドロップダウンメニューから有効期間を選択してください。
B. SSL証明書をvManageにアップロードします。
C. Ciscoが推奨するコントローラ証明書認証モードを選択します。
D. Cisco SD-WANファブリックの組織名を変更します。
E. 公開証明書署名機関ではなく、プライベート証明書署名機関を選択します。
正解: (正解を表示します)

質問: **106**
Cisco SD-WANファイアウォールポリシーにおいて、TCP、UDP、およびICMPフローのステートフルインスペクションに使用されるコンポーネントはどれですか？
A. サブネット
B. サイト
C. インターフェース
D. ゾーン
正解: (正解を表示します)
In Cisco SD-WAN firewall policies, zones are used for stateful inspection of TCP, UDP, and ICMP flows. Zones define groups of interfaces and subnets that share common security requirements and enable you to create firewall policies to control traffic between these zones.

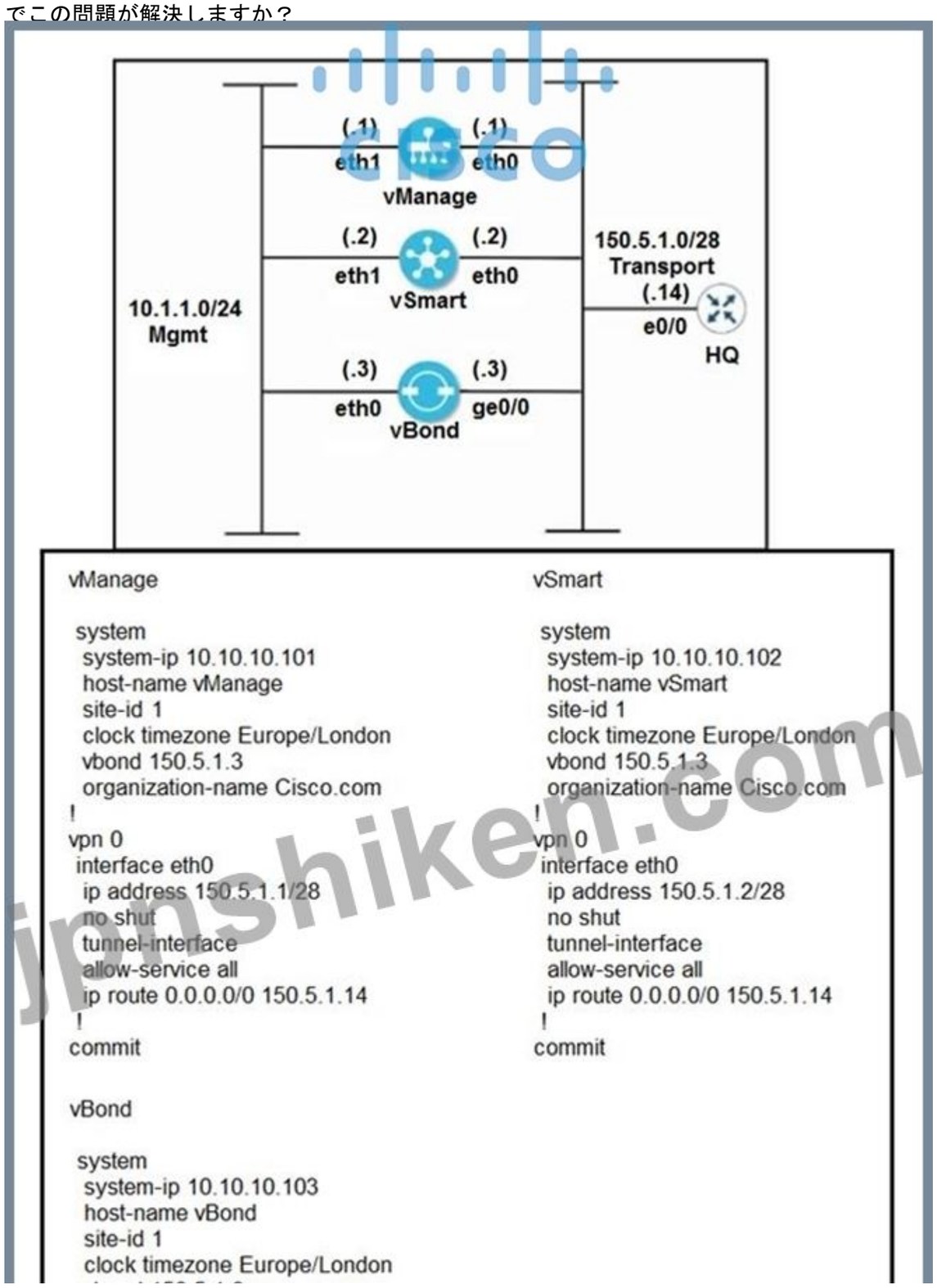
有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
ネットワーク管理者は、複数の条件の一致アクションペアに基づいて集中制御ポリシーを構成しています。TLOCよりもプレフィックスリストを優先し、オリジンよりもTLOCを優先するように構成する必要がある順序はどれですか。
A. 最高から最低のシーケンス番号
B. 非順次順序
C. 決定論的順序
D. 最小から最大のシーケンス番号
正解: (正解を表示します)
In a centralized control policy (such as Cisco SD-WAN), match-action pairs are evaluated in sequence. The order of preference is determined by the sequence numbers assigned to the policy statements:
- Lower sequence numbers are evaluated first.
- Once a match is found, the associated action is applied, and evaluation stops.
Therefore, to prefer Prefix List over TLOC and TLOC over Origin, you must configure the policy entries in ascending order (lowest to highest sequence number), so that Prefix List rules are checked before TLOC, and TLOC before Origin.

質問: **108**
RESTアプリケーションは、HTTPまたはHTTPSを介して通信し、ネットワークデバイス間で呼び出しを行います。
HTTPS標準規格に含まれるメソッドはどれですか？(2つ選択してください。)
A. POST
B. オブジェクト
C. 削除
D. スカラー
E. 配列
正解: (正解を表示します)

質問: **109**

図を参照してください。エンジニアが、SD-WAN ManagerとSD-WAN ControllerがSD-WAN Validatorへの接続を確立できないという問題のトラブルシューティングを行っています。どの操作でこの問題が解決しますか？



jpnshiken.com

```
 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-service all
  ip route 0.0.0.0/0 150.5.1.14
 !
commit
```

A. SD-WAN ManagerとSD-WAN Controllerのトンネルインターフェイスで、カプセル化をIPsecとして設定します。
B. SD-WANバリデーターでvbondコマンドをvbond 150.5.1.3 localとして再設定します。
C. 3 つのコントローラすべてで、トランスポートの色を使用してトンネルインターフェイスを設定します。
D. SD-WAN Validator のトンネルインターフェイスの下にある encapsulation ipsec コマンドを削除します。
正解: **B (**コメントを発表する**)**

質問: **110**
Cisco Catalyst SD-WAN Managerのどのコンポーネントを使用すると、ネットワーク管理者は設定グループをWANエッジルータに関連付けることができますか？
A. ワークフローライブラリ
B. 機能テンプレート
C. 構成グループワークフローをデプロイします
D. カスタム構成グループワークフロー
正解: **C (**コメントを発表する**)**
The "deploy configuration group workflow" in Cisco Catalyst SD-WAN Manager is used to associate configuration groups with WAN Edge routers. This workflow allows network managers to select a configuration group (made up of feature templates) and apply it to selected WAN Edge devices, ensuring consistent and scalable deployment.

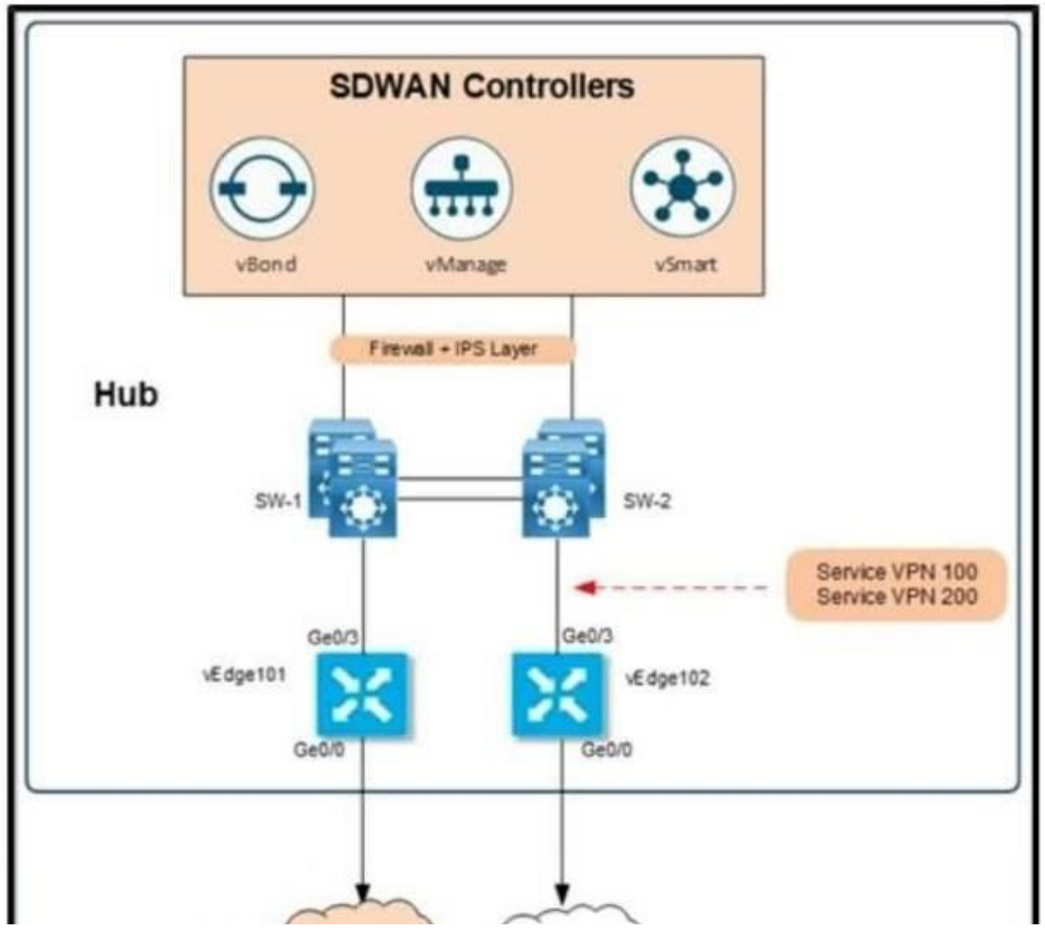
質問: **111**
vManageがすべてのコントローラを連携させるために使用される属性はどれですか？
A. vManage system-ip
B. リージョンID
C. 組織名
D. セキュアデバイスID
正解: **(**正解を表示します**)**
SD-WAN uses certificates to authenticate each other to the Root CA (VBond) to the other controllers including vEdge, ostensibly using the same design of a PKI.
The controllers authenticate the certificate fields which include the Organization name, this field along forms a union with the other controllers and devices.
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-controller-cert- deploy-guide.html

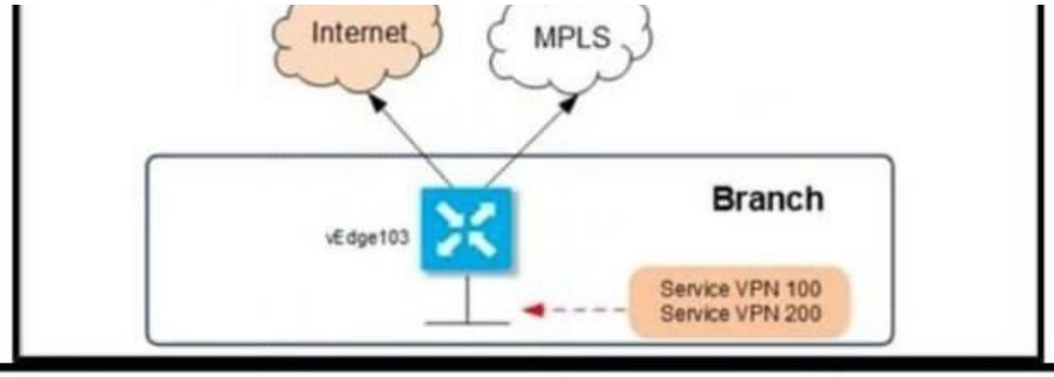
質問: **112**
ユーザーがWebブラウザ経由でvManageにアクセスするために、vManageにはどのタイプの証明書がインストールされますか？

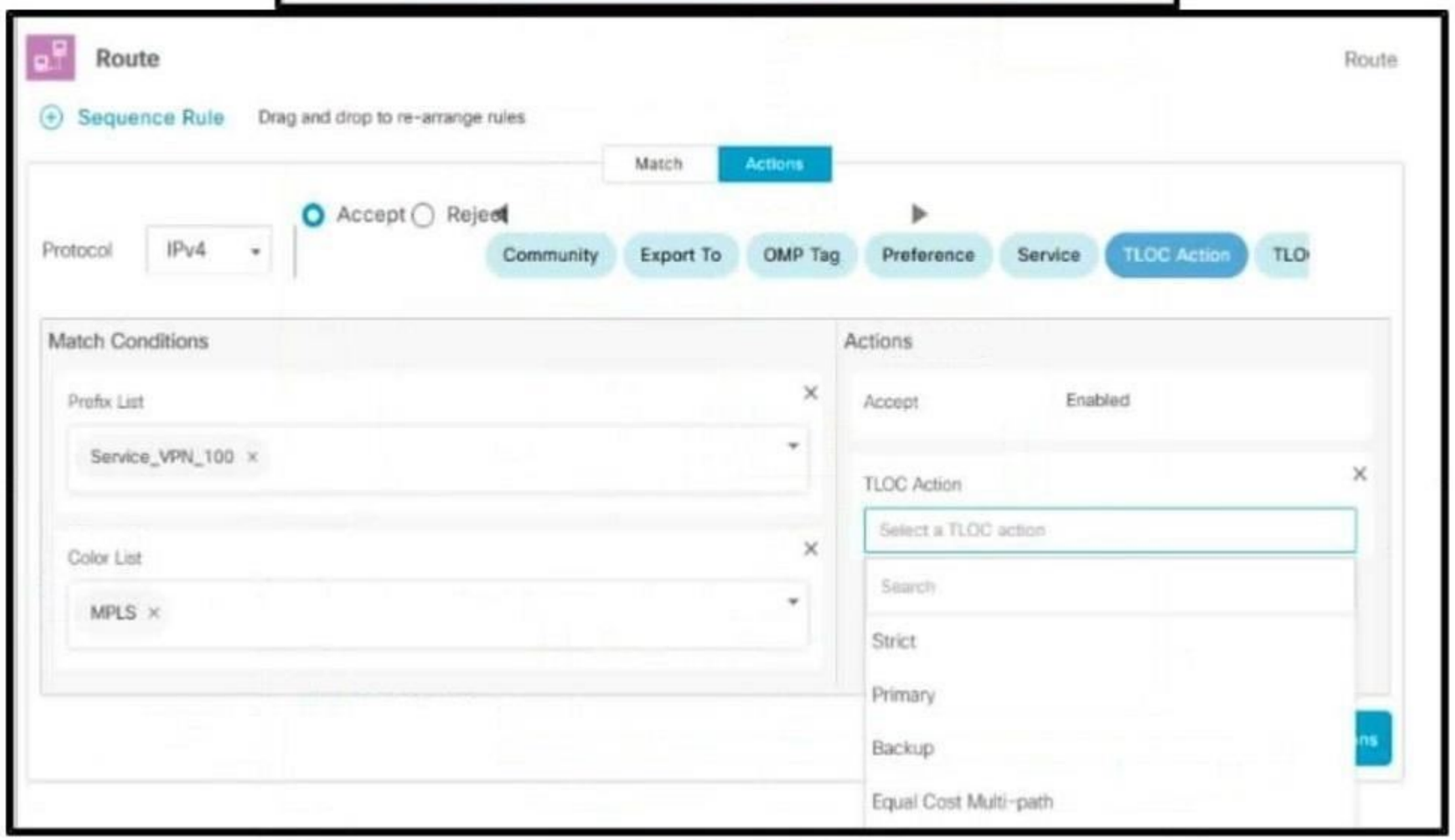
A. コントローラー証明書
B. Webサーバー証明書
C. SD-AVC証明書
D. WANエッジ証明書
正解: (正解を表示します)
Used for web access to the vManage. Cisco installs a self-signed certificate by default. A Self- signed certificate is a Secure Sockets Layer (SSL) certificate that is signed by its own creator.

質問: **113**
vSmartコントローラがルートリフレクタとして動作する場合、vSmartコントローラとWANエッジルータ間ではどのプロトコルが実行されますか？
A. DTLS/TLS 内の BGP
B. DTLS/TLS制御接続外のOMP
C. DTLS/TLS制御接続内のIPsec
D. DTLS/TLS制御接続内のOMP
正解: (正解を表示します)

質問: **114**
図を参照してください。vEdge103は、2つの異なる回線を使用して本社に接続されています。
MPLSとビジネスインターネット。サービスVPN 100はMPLS回線のみを使用し、MPLS回線が故障した場合はトラフィックを破棄する必要があります。この動作を実現するには、どのTLOCアクションを選択する必要がありますか？







A. 厳格
B. 等コストマルチパス
C. プライマリ
D. バックアップ
正解: **A** (コメントを発表する)
The "Strict" TLOC action is used to enforce that traffic only uses the specified TLOC (in this case, MPLS) and will drop the traffic if that TLOC is unavailable. By selecting "Strict," the policy will ensure that Service VPN 100 only uses the MPLS circuit, and traffic will not fail over to the Business Internet circuit if the MPLS connection goes down.

質問: **115**

アプリケーション認識型ファイアウォールの利点は何ですか？
A. パケットのMTUによってトラフィックをブロックします
B. 暗号化されたトラフィックをブロックします
C. アプリケーションによるトラフィックをブロックします
D. MACアドレスによるトラフィックをブロックします
正解: (正解を表示します)
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

質問: **116**
クイックコネクトワークフローを使用する場合、SD-WANオーバーレイの設定を完了するために、ワークフロー外で設定する必要があるVPNはどれですか？
A. サービス VPN
B. トランスポートVPN
C. サービスおよびトランスポートVPN
D. 管理用VPN
正解: (正解を表示します)
The Quick Connect workflow is limited to configuring WAN settings (VPN 0). To be able to complete the Cisco Catalyst SD-WAN overlay bring up process, you also need to configure service-side VPN templates

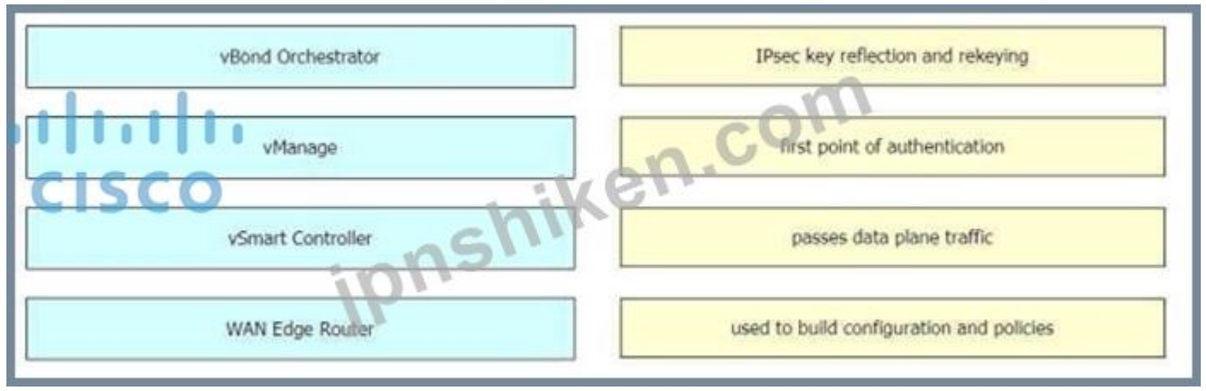
質問: **117**
OMP のグレースフル リスタート値を 24 時間に設定するには、エンジニアが IPsec キー再生成タイマーのどの値を設定する必要がありますか?
A. 6時間
B. 12時間
C. 36時間
D. 48時間
正解: (正解を表示します)
In Cisco SD-WAN, the recommended practice is to set the IPsec rekey timer to be half the value of the OMP graceful restart timer. This ensures that the IPsec security associations (SAs) are refreshed well before the OMP session timeout, providing seamless connectivity and avoiding downtime.
Since the OMP graceful restart timer is set for 24 hours, the IPsec rekey timer should be set to 12 hours (half of 24 hours) to ensure proper timing and avoid any interruptions in the IPsec connections.

質問: **118**
デバイス上のアクティブなDNSセキュリティポリシーについて、組織の内部でホストされているアプリケーションに到達できるようにする機能はどれですか？
A. ローカルドメインバイパス
B. DHCPオプション6
C. DNSCryptコンフィギュレーター
D. リダイレクト付きのデータポーキー
正解: (正解を表示します)
A local domain bypass allows reachability to an organization's internally hosted applications when an active DNS security policy is in place. It permits the device to bypass DNS security policies for specific domains or hosts, typically those that are hosted internally by the organization. This ensures that access to internal resources is not blocked or affected by DNS security policies.

質問: **119**

ドラッグアンドドロップ問題

左側のCisco SD-WANコンポーネントを、右側のそれぞれの機能にドラッグアンドドロップしてください。



正解:



質問: **120**

エンジニアは、vManageを使用してWANエッジルーターのオンボーディングプロセスを自動化したいと考えています。どのコマンドがこれを達成しますか？

A. リクエストvedge-cloudactivatechassis-number <chassis-number>シリアル<serial>

B. vedge-cloudアクティブ化シャーシ番号<chassis-number>トークン<token-number>を要求します

C. リクエストvedge-cloudアクティブ化シリアル<シリアル>トークン<トークン番号>

D. vedge-cloudアクティブ化シャーシ番号<chassis-number>組織<組織>を要求します

正解: **B** (コメントを発表する)

request vedge-cloud activate

Activate a vEdge Cloud router in the overlay network (on vEdge Cloud routers only). Before you can use this command, you must configure the organization name and the vBond orchestrator's IP address or DNS name on the vEdge Cloud router.

Command Hierarchy

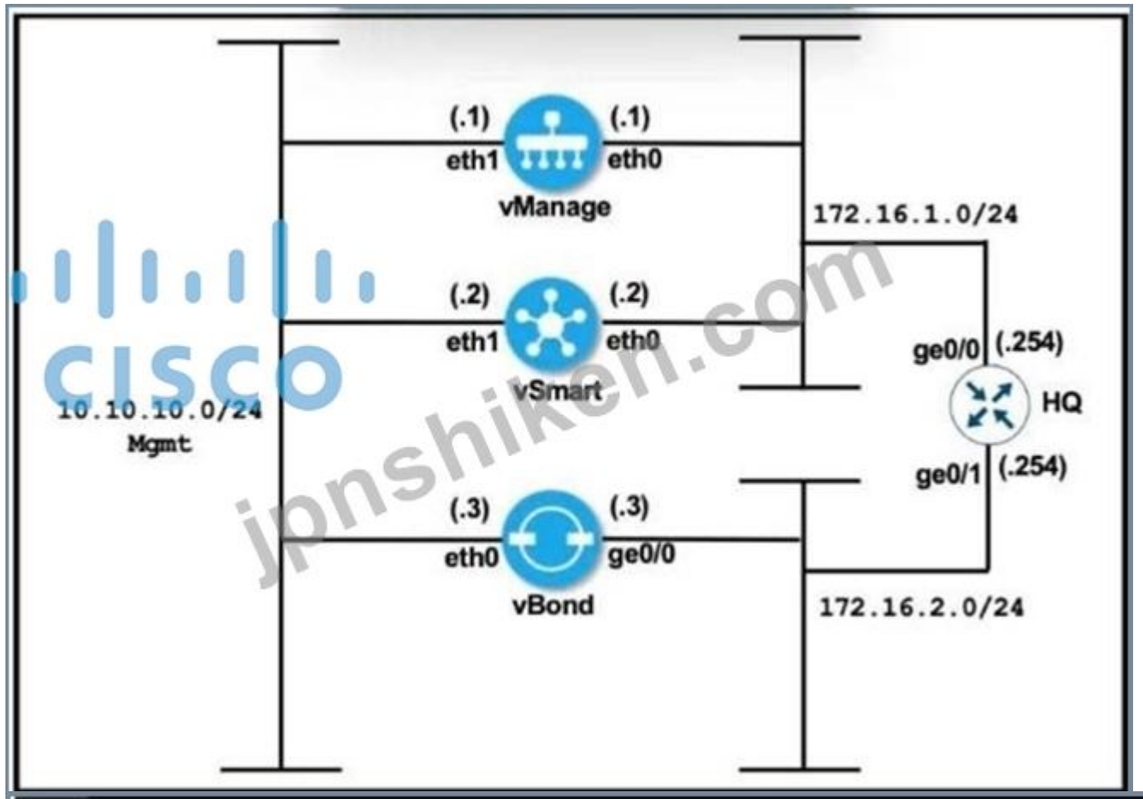
request vedge-cloud activate chassis-number number token token

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr- book/operational-cmd.html#wp1526475327

質問: **121**

図を参照してください。vManageとvBondは相互に接続を確立する際に問題が発生しています。

どの設定で問題が解決しますか？




```
vManage

system
 system-ip 10.10.10.101
 host-name vManage
 site-id 1
 clock timezone Europe/London
 vbond 172.16.2.1
 organization-name Cisco.com
!
vpn 0
 interface eth1
  ip address 172.16.1.1/24
  no shut
  tunnel-interface
  allow-service all
 ip route 0.0.0.0/0 172.16.1.254
!
commit
```

```
vBond

system
 system-ip 10.10.10.103
 host-name vBond
 site-id 1
 clock timezone Europe/Rome
 vbond 172.16.2.1 local
 organization-name Cisco.com
!
vpn 0
 interface ge0/0
  ip address 172.16.2.1/24
  no shut
  tunnel-interface
  encapsulation ipsec
  allow-service all
 ip route 0.0.0.0/0 172.16.1.254
!
commit
```

A. vBond のタイムゾーンを Europe/London に設定します。

B. vBond のトンネルインターフェイスの下にある encapsulation ipsec コマンドを削除します。

C. vManage のトンネル インターフェイスで encapsulation ipsec コマンドを設定します。

D. vBond 上に 172.16.2.254 を指すデフォルト ルートを設定します。
正解: (正解を表示します)

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
デバイスの身元を確認するために、証明書内で検証される値はどれですか？
A. シリアル番号
B. OTP
C. システムIP
D. シャーシID
正解: (正解を表示します)
Serial numbers are commonly used in certificates as a unique identifier for a specific physical device. When a device presents a certificate during authentication or key exchange, the serial number is one of the attributes used to verify the device's identity and authenticity.

質問: **123**
エンジニアはCiscoを通じて証明書の署名を自動化する必要がある。
このタスクを実現するには、どのvManage構成を使用すればよいですか？
A. VPN 0
DNS 208.67.222.222 プライマリ
allow-service dns
allow-service sshd
allow-service netconf
B. VPN 0
allow-service dns
allow-service sshd
allow-service netconf
C. VPN 512
DNS 208.67.222.222 プライマリ
allow-service dns
allow-service sshd
allow-service netconf
D. VPN 512
allow-service dns
allow-service sshd
allow-service netconf
正解: (正解を表示します)

Automated certificate signing through Cisco Systems
With this option, certificate signing requests are automatically sent to the Cisco PnP cloud service where the certificate is signed. The SD-WAN Manager then automatically retrieves the certificate and installs it. A DNS server needs to be configured to resolve the hostname, cloudsso.cisco.com and subsequently, apx.cisco.com. The SD-WAN Manager needs to reach both servers on TCP port 443.
Account credentials are configured before this certificate option can be configured.
Procedure 1: Verify Cisco server reachability
1. Ensure that a DNS server is defined for VPN 0 on SD-WAN Manager via SSH or console:
config terminal
vpn 0
dns 208.67.222.222 primary
commit and-quit

質問: **124**
Cloud OnRamp SaaSにおけるコロケーションの機能は何ですか？
A. Cloud OnRampは、リモートのクラウドアクセスポイントを選択することで、地域コロケーション施設を組み込みます。
B. Cloud OnRampのコロケーション施設では、セキュリティと最適化の仮想化において顧客は課題に直面しています。
C. Cloud OnRampでは、コロケーションはアクセス専用ロケーションの仮想化とコロケーションセンターの使用をサポートします。
D. コロケーションソリューションのクラウドオンランプは、Cisでオーケストレーションされるさまざまなvnfサービスチェーンの作成を制限します
正解: (正解を表示します)

質問: **125**
ネットワーク機能の動作に影響を与えるものの、停止させるほどではない重大な事象を監視するように設定されているアラーム設定はどれですか？
A. 重大
B. 中程度
C. メジャー
D. マイナー
正解: (正解を表示します)
https://sdwan-docs.cisco.com/Product_Documentation/vManage_How-Tos/Troubleshooting/Monitor_Alarms

質問: **126**
サイト間トラフィックをファイアウォール経由でルーティングするために、サービスチェーンIPアドレスを設定する必要があるデバイスはどれですか？
A. vSmart
B. スポークWANエッジ
C. ハブWANエッジ
D. ファイアウォール
正解: (正解を表示します)
https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD- WAN_Release_16.3/07Policy_Applications/02Service_Chaining/Service_Chaining_Configuration_Examples

質問: **127**

Cisco Umbrellaリゾルバ がDNSリクエストをインテリジェントプロキシに向けるようになるのは、どのような問題が原因ですか？
A. ドメインが存在しません。
B. ドメインがブロックリストに登録されています。
C. ドメインがグレーリストに登録されています。
D. ドメインはローカルで到達可能です。
正解: (正解を表示します)

質問: **128**
エンジニアは、一致するQoSパラメータに基づいてDIA用のWANエッジルーターを構成しています。このタスクを実行する2つのアクションはどれですか？ 2つ選択してください。）
A. QoSマップポリシーを適用します。
B. 制御ポリシーを構成します。
C. 一元化されたデータポリシーを構成します。
D. トランスポートインターフェイスでNATを構成します。
E. WANインターフェースにデータポリシーを適用します。
正解: (正解を表示します)
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2020aug.pdf

質問: **129**
1つのFECブロックにはいくつのパケットが含まれていますか？
A. データパケット4個、パリティパケット1個
B. データパケット1個、パリティパケット1個
C. データパケット1個、パリティパケット4個
D. この値はポリシーで設定可能です。
E. データパケット2個、パリティパケット1個
正解: (正解を表示します)

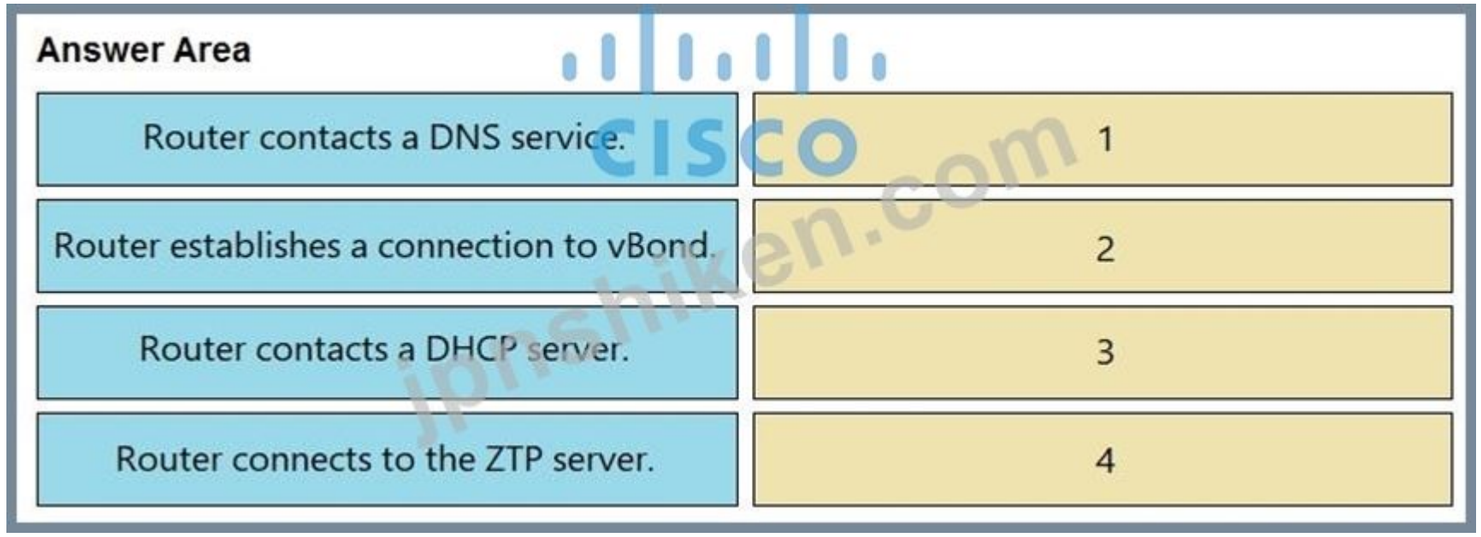
質問: **130**
図を参照してください。エンジニアは、WANエッジデバイス上で特定のサービスVPNからのFTPトラフィックをブロックする必要があります。この目的を達成するには、どの手順を実行すればよいでしょうか？



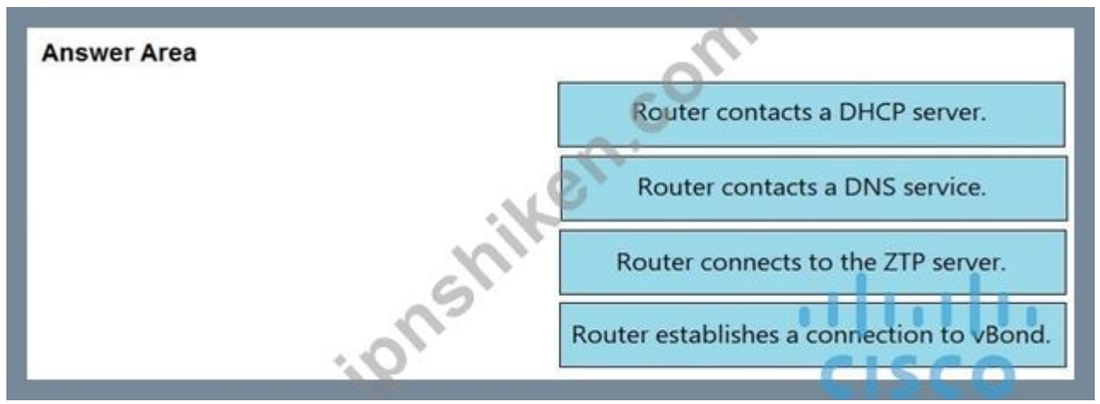
A. ローカライズされたポリシーを作成し、それをインターフェイス機能テンプレートに追加します。
B. ローカライズされたポリシーを作成し、それを VPN テンプレートに追加し、インターフェース機能テンプレートに ACL を追加します。
C. プレフィックスリストを作成し、それをローカライズされたポリシーに追加し、インターフェース機能テンプレートに追加します。
D. ローカライズされたポリシーを作成し、それをデバイステンプレートに追加し、インターフェイス機能テンプレートにACLを追加します。
正解: (正解を表示します)
The exhibit already shows a localized policy created in VManage, their is no need to create a new one. You only need to create an ACLthat block's FTP traffic (Port 20/21) ingress on an interface (in VManage add it to the localized, then interface feature).

質問: **131**
デバイスのアップグレード日時を確認できるログはどれですか？
A. ACL
B. メール
C. SNMP
D. 監査
正解: (正解を表示します)
Audit logs are often used to record significant events and actions related to device management, including activities like software upgrades. These logs can help track when an upgrade was performed, who initiated it, and other relevant details about the upgrade process.

質問: **132**
ドラッグアンドドロップ問題
電源投入後のWANエッジルーターでゼロタッチプロビジョニングを行うには、左側の手順を右側の手順にドラッグアンドドロップしてください。



正解:



質問: **133**
レプリケーターは、オーバーレイネットワーク内のSD-WANコントローラーに自身を通知するために、どの機能を使用しますか？
A. ランデブーポイント (RP) の送信元アドレス
B. vEdgeルーターはインターネットグループ管理プロトコル(IGMPv2)をリッスンします
C. オーバーレイ管理プロトコル (OMP) マルチキャスト自動検出ルート
D. マルチプロトコルBGP(MP-BGP)ルート
正解: **C (**コメントを発表する**)**
In Cisco SD-WAN multicast architecture, replicators automatically advertise themselves using OMP multicast-autodiscover routes. These routes are sent through the control plane to the SD-WAN controllers (vSmart), which then distribute the information to other WAN Edge routers. This allows receivers and sources to dynamically discover the appropriate replicator nodes that will replicate multicast traffic across the SD-WAN overlay.

質問: **134**
WAN エッジ デバイスがクラウド展開で機能するには、Azure VNet にいくつのサブネットが必要ですか?
A. CSR は、Microsoft クラウドでサポートされている WAN エッジ デバイスです。Microsoft アンダーレイ クラウド ファブリックが管理機能を実行します。
B. VNet には、管理、パブリック、サービスの 3 つのサブネットが必要です。
C. VNet には 1 つのパブリック サブネットが必要です。Microsoft アンダーレイ クラウド ファブリックは、WAN エッジのすべてのルーティング機能を実行します。

D. VNet にはパブリック サブネットとサービス サブネットが必要です。Microsoft アンダーレイ クラウド ファブリックが管理機能を実行します。
正解: (正解を表示します)
In an Azure cloud deployment of a WAN Edge device (like a Cisco CSR), you typically need at least two subnets within your Azure Virtual Network (VNet): one for public-facing traffic (public subnet) and another for internal services (services subnet). The Microsoft Azure cloud fabric handles the underlying management functions, so you don't need a separate management subnet. This configuration allows you to separate public-facing traffic from internal services and manage the WAN Edge device effectively.

質問: **135**
セキュリティのためにSD-WANでTLSプロキシを有効にする場合、トラフィックフローを設定する最初のステップは何ですか？
A. 送信者はデバイスと個々のユーザーを認証し、受信者は送信者の公開鍵を使用してメッセージを復号化することで署名を検証します。
B. TLSプロキシの認証局は、ホスト、ネットワークデバイス、ユーザーなどのすべてのエンティティの認証のために証明書を発行します。
C. クライアントとプロキシ間、およびプロキシとサーバー間でTCP接続が確立されます。
D. フローに対して復号ポリシーが有効になっている場合、Unified Threat Defense はクライアント ハロー パケットを受信して復号アクションを定義します。
正解: (正解を表示します)

質問: **136**
プレフィックスのグループを使用してネットワーク内のルーティングに影響を与えるポリシーが作成されます。サイトリストに適用すると、どのようなポリシーアプリケーションがこの目標を達成しますか？
A. VPNメンバーシップポリシー
B. 制御ポリシー
C. cflowd-template
D. アプリルートポリシー
正解: (正解を表示します)
Control policy, which is similar to standard routing policy, operates on routes and routing information in the control plane of the overlay network.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies- book/control-policies.html

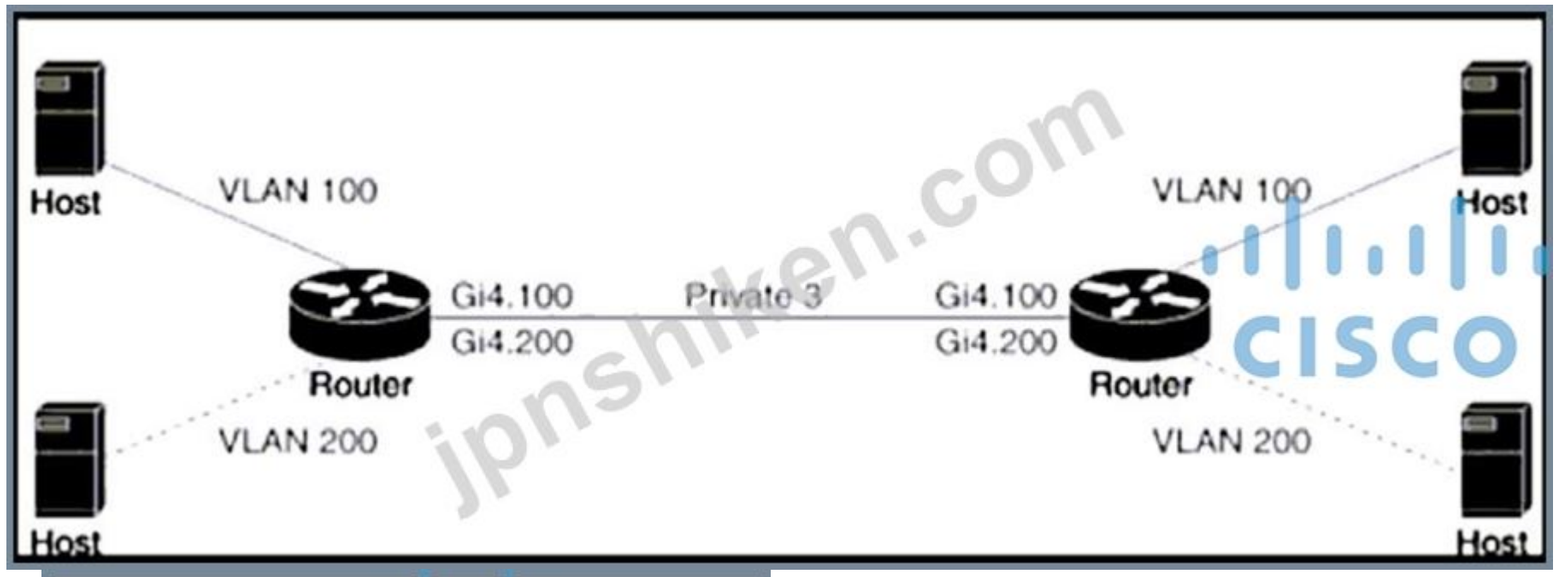
有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
Cisco IOS XE SD-WANイメージをサポートするハードウェアプラットフォームはどれですか？(2つ選択してください。)
A. ISR4000シリーズ
B. ISR9300シリーズ
C. vEdge-1000シリーズ
D. ASR9000シリーズ
E. ASR1000シリーズ
正解: (正解を表示します)
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white_paper-c11-741071.html

質問: **138**
アプリケーションチームは、業務上極めて重要な新しいアプリケーションをネットワークに展開する準備を進めている。
トラフィックを保護するために、ネットワークチームはQoSマップに別のキューを追加し、そのマップをファブリックに展開する必要があります。QoSマップにキューを追加して適用する前に、どの構成手順を完了する必要がありますか？
A. 新しいQoSクラスとハードウェアキューの関係は、vManageのローカルポリシーセクションの『リスト』ページから設定する必要があります。その後、QoSマップがWANインターフェイスに適用されます。
B. 新しいQoSクラスとハードウェアキューの関係は、vManageのローカルポリシーセクションの『リスト』ページから設定する必要があります。その後、QoSマップがサービス側のインターフェイスに適用されます。
C. 新しいQoSクラスとハードウェアキューの関係は、vManageの中央ポリシーセクションの『リスト』ページから設定する必要があります。その後、QoSマップがサービス側のインターフェイスに適用されます。
D. 新しいQoSクラスとハードウェアキューの関係は、vManageの集中ポリシーセクションの『リスト』ページから設定する必要があります。その後、QoSマップがWANインターフェイスに適用されます。
正解: **(**正解を表示します**)**
QOS is created in Local policies and needs to be applied on the WAN interface.

質問: **139**
クラウド環境において、Cisco SD-WANのオーケストレーションプレーンを管理するコントローラはどれですか？
A. シスコDNAセンター
B. vSmart
C. vBond
D. vManage
正解: **C (**コメントを発表する**)**
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.

質問: **140**
図を参照してください。エンジニアがサブインターフェース上のVLAN 100のトラフィックをシェーピングするためのQoSポリシーを設定しています。どのポリシー設定がこのタスクを実現しますか？



A.

```
policy-map shape_GigabitEthernet4.100
    class class Queue0
     service-policy xyz_QoS-model
      shape average 100000000
!
interface GigabitEthernet4.100
   encapsulation dot1Q 200
   service-policy output shape_GigabitEthernet4.100
```

B.

```
policy-map shape_GigabitEthernet4.200
   class class-default
     service-policy xyz_QoS-model
     shape average 100000000
!
interface GigabitEthernet4.100
   encapsulation dot1Q 100
   service-policy output shape_GigabitEthernet4.200
```

C.

```
policy-map shape_GigabitEthernet4.100
    class class-default
     service-policy xyz_QoS-model
     shape average 100000000
!
interface GigabitEthernet4.100
   encapsulation dot1Q 200
   service-policy output shape_GigabitEthernet4.100
```

D.
```
policy-map shape_GigabitEthernet4.200
    class class Queue0
     service-policy xyz_QoS-model
      shape average 100000000
!
interface GigabitEthernet4.100
   encapsulation dot1Q 100
   service-policy output shape_GigabitEthernet4.100
```

正解: (正解を表示します)

Based on the configuration goal to shape traffic for VLAN 100 on a subinterface, the correct policy configuration should include a shaping policy applied to the subinterface corresponding to VLAN 100.

Chosen option is the correct configuration because it includes the correct encapsulation of dot1Q 100for VLAN 100 on GigabitEthernet4.100and applies the shaping policy with service- policy output shape_GigabitEthernet4.100.

質問: **141**

エンジニアは、以下の要件を満たすQoSポリシーを導入する必要があります。

- ポリシー名: アプリ警察

警察のレート :1000000

- バースト: 1000000

- 超過: 減少

どの構成が要件を満たしていますか？

A.
```
policy
 data-policy policy-name
  vpn-list 10
   sequence 1
    action accept
     set
       policer App-police
```

B.
```
vpn-list VPN10
 sequence 1
  match
   app-list youtube
  action accept
   set
    policer App-police
```

C.
```
policy
 action accept
  set
    policer App-police
```

D.
```
vpn 10
 interface ge0/0/0
  set
    policer App-police in
  default action accept
```

正解: (正解を表示します)

質問: **142**
Cisco Catalyst SD-WAN Managerサーバーのリポジトリにソフトウェアイメージを追加する手順を教えてください。
A. SD-WANマネージャサーバーは、SD-WANデバイスにアクセス要求を送信し、リモートファイルサーバーに接続してソフトウェアイメージをダウンロードします。
B. ソフトウェアイメージはローカルのSD-WANマネージャサーバーに保存され、帯域外管理接続を介してSD-WANデバイスにダウンロードされます。
C. SD-WAN デバイスは FTP URL を SD-WAN マネージャー サーバーに送信し、リモート ファイル サーバーに接続してソフトウェア イメージをダウンロードします。
D. ソフトウェアイメージは、データプレーン接続を介してSD-WANデバイスにダウンロードされた後、リモートのSD-WANマネージャサーバーに保存されます。
正解: **B (**コメントを発表する**)**
In Cisco SD-WAN, software images are typically uploaded and stored directly on the Cisco SD- WAN Manager server. Once the images are in the repository, SD-WAN Manager distributes them to SD-WAN devices via an out-of-band management connection, ensuring that software updates do not interfere with regular data plane traffic. This centralized management approach allows administrators to control and deploy updates efficiently across multiple devices.

質問: **143**
エンジニアが、VPN 115の既存のデータポリシーを、以下の追加要件を満たすように変更しています。
- 政府のウェブサイトを閲覧する際は、トラフィックは直接アクセスする必要があります
インターネット接続。
- サイトから出るトラフィックの送信元アドレス
政府のウェブサイトは、
国そのもの、特定のTLOC。

A.

```
vpn 0
 interface ge0/0.100
  ip address 198.51.100.2/30
  nat
 !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
 mtu 1496
 no shutdown
 !
 interface ge0/1.10
  ip address 10.254.254.2/30
 !
  tunnel-interface
   encapsulation ipsec
   color private1
 mtu 1496
 no shutdown
 !
ip route 0.0.0.0/0 198.51.100.1
ip route 0.0.0.0/0 10.254.254.1
!

data-policy DIA
  vpn-list VPN-115
    sequence 10
     match
      destination-data-prefix-list INTERNAL-NETWORKS
     !
     action accept
    sequence 20
     match
      destination-ip 0.0.0.0/0
     !
     action accept
      nat use-vpn 0
    !
   !
  default-action accept
 sequence 15
  match
   destination-data-prefix-list GOVERNMENT-WEBSITES
  !
  action accept
   set
    local-tloc-list
     color biz-internet
```

jpnshiken.com

B.
```
sequence 25
 match
  destination-data-prefix-list GOVERNMENT-WEBSITES
 !
 action accept
  nat use-vpn 0
```

C.
```
sequence 15
 match
  source-data-prefix-list GOVERNMENT-WEBSITES
 !
 action accept
  set
   local-tloc-list
    color private1
```

D.
```
sequence 30
 match
  destination-data-prefix-list GOVERNMENT-WEBSITES
 !
 action accept
  set
   local-tloc-list
    color biz-internet
```

正解: (正解を表示します)

質問: **144**

図を参照してください。vManage と同じエンタープライズ ルート CA 証明書を使用して、vBond コントローラがコントローラ リストに追加されました。2 つのコントローラは VPNO を介して相互に通信でき、同じ組織名を共有していますが、制御接続が開始されません。どの操作でこの問題を解決できますか？

```
vManage#show control local-properties
   personality                vmanage
   sp-organization-name       Cisco
   organization-name          Cisco
   system-ip                  10.1.1.10
   root-ca-chain-status       Installed
   certificate-status         Installed
```

A. vManage 上の WAN Edge リストをコントローラと同期します。

B. 両方のコントローラで NTP を設定して接続を確立します。

C. vManage 上で有効な vBond IP を設定します。

D. vBondコントローラに有効なシステムIPを設定します。

正解: (正解を表示します)

質問: **145**

デバイスがオンラインになる前にオンボーディングプロセスをサポートするために、WANエッジリストがアップロードされた後、vManageで実行される構成手順はどれですか？
A. デバイス証明書を検証します
B. ZTPプロセスを有効にする
C. デバイスを有効なものとして設定します
D. リストをコントローラーに送信する
正解: **C** (コメントを発表する)

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.**

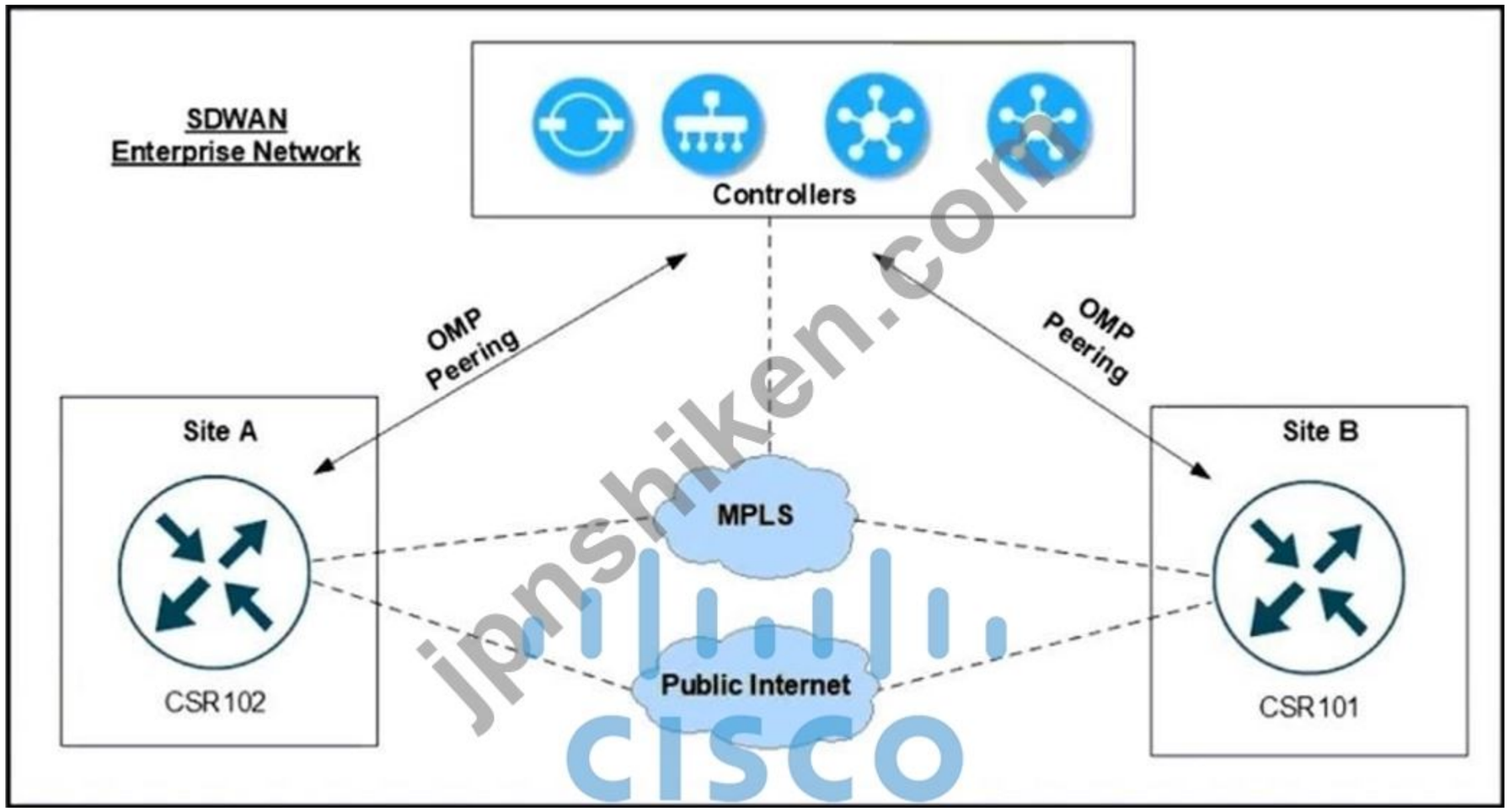
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf

質問: **146**
vSmartコントローラ上で、安全なDTLS/TLS接続の作成と維持を担当するコンポーネントはどれですか？
A. vdaemon
B. OMP
C. SNMP
D. NETCONF
正解: **A** (コメントを発表する)
A Cisco SD-WAN daemon running on each vSmart controller and router creates and maintains the secure DTLS or TLS connections between the devices. This daemon is called vdaemon .
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security- book/security-overview.html

質問: **147**
Cisco SD-WANソリューションにおいて、プロビジョニングと設定に使用されるコントローラはどれですか？
A. vManage
B. WANエッジルーター
C. vBond
D. vSmart
正解: (正解を表示します)

質問: **148**
Cisco Catalyst SD-WAN環境でTLSプロキシを設定する際に使用される認証局(CA)オプションはどれですか？
A. SD-WAN ManagerをCAとして使用
B. SD-WANコントローラをCAとして使用
C. vController を CA として使用
D. WANエッジをCAとして利用
正解: (正解を表示します)
When configuring a TLS proxy in a Cisco Catalyst SD-WAN environment, the SD-WAN Manager acts as the Certificate Authority (CA). It issues and manages the certificates used for proxying TLS sessions, enabling secure inspection and control of encrypted traffic.

質問: **149**
図を参照してください。エンドユーザーがCSR101経由でデータ トラフィックを送信できないようにするには、どのコマンドが必要ですか？



A. omp
no address-family ipv4
B. omp
no overlay-as
C. omp
no graceful-restart
D. omp
正解: (正解を表示します)
The command omp no address-family ipv4 disables the OMP route advertisements and reception for IPv4 on CSR101, effectively preventing it from participating in data plane traffic forwarding, while still allowing OMP peering to function. This stops end-user data traffic from being routed through CSR101.

質問: **150**
コントローラーコードでサポートされている画像フォーマットはどれですか？(2つ選択してください。)
A. .nxos
B. .qcow2
C. .iso
D. .ova
E. .tgz

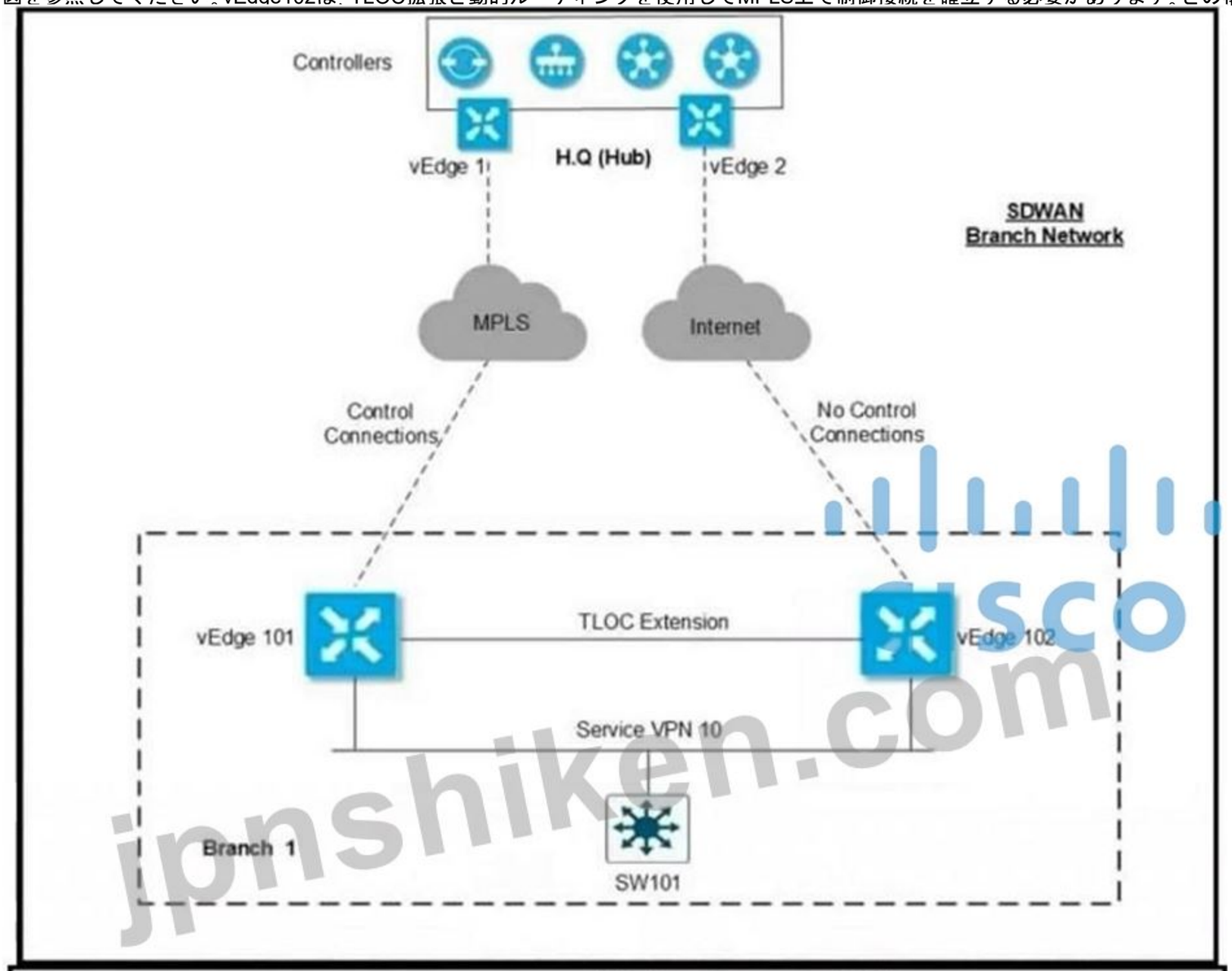
正解: **B,D** (コメントを発表する)

- Cisco Catalyst SD-WAN Controller
    - viptela-smart-genericx86-64.ova (for ESXi Hypervisor)
    - viptela-smart-genericx86-64.qcow2 (for KVM Hypervisor)

Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs- book/hardware-and-software-installation.html

質問: **151**

図を参照してください。vEdge102は、TLOC拡張と動的ルーティングを使用してMPLS上で制御接続を確立する必要があります。どの構成でこのタスクが達成されますか？



jpnshiken.com

vEdge101

```
interface ge0/0
```

```
vpn 0
  router
  bgp 65001
   neighbor 172.1.1.1
   no shutdown
   remote-as      65001
   neighbor 192.0.0.2
   remote-as      100
    no shutdown
```

```
  description "*MPLS Transport
Interface*"
  ip address 192.0.0.1/30
  tunnel-interface
   encapsulation ipsec
   color mpls restrict
   allow-service bgp

 interface ge0/1
  description    "TLOC Extension
Interface"
  ip address 172.1.1.2/30
  pmtu
  tloc-extension ge0/0
```

A.

```
vpn 0
  router
  bgp 65001
   neighbor 192.0.0.1
   no shutdown
   remote-as    65001

interface ge0/1
 description """ MPLS Interface """"
ip address 172.1.1.1/30
tunnel-interface
 encapsulation ipsec
 color mpls restrict
 allow-service all
no shutdown
```

passhiken.com
CISCO

```
vpn 0
  router
  bgp 65001
   neighbor 172.1.1.2
   no shutdown
   remote-as     65001
   neighbor 192.0.0.2
   no shutdown
   remote-as     100

 interface ge0/1
   description    "TLOC Extension Interface"
   ip address 172.1.1.1/30
   tloc-extension ge0/0
   no shutdown
```

B.

```
vpn 0
  router
  bgp 65001
   neighbor 172.1.1.2
   remote-as     65001
    no shutdown

 interface ge0/1
  description "*** MPLS Interface ***"
  ip address 172.1.1.1/30
  tunnel-interface
   encapsulation ipsec
   color mpls restrict
   allow-service bgp
  no shutdown
```

C.

```
vpn 0
  router
  bgp 65001
   neighbor 172.1.1.1
   no shutdown
   remote-as     65001

 interface ge0/0
  description    "TLOC Extension Interface"
  ip address 172.1.1.2/30
  tloc-extension ge0/0
  no shutdown
```

D.

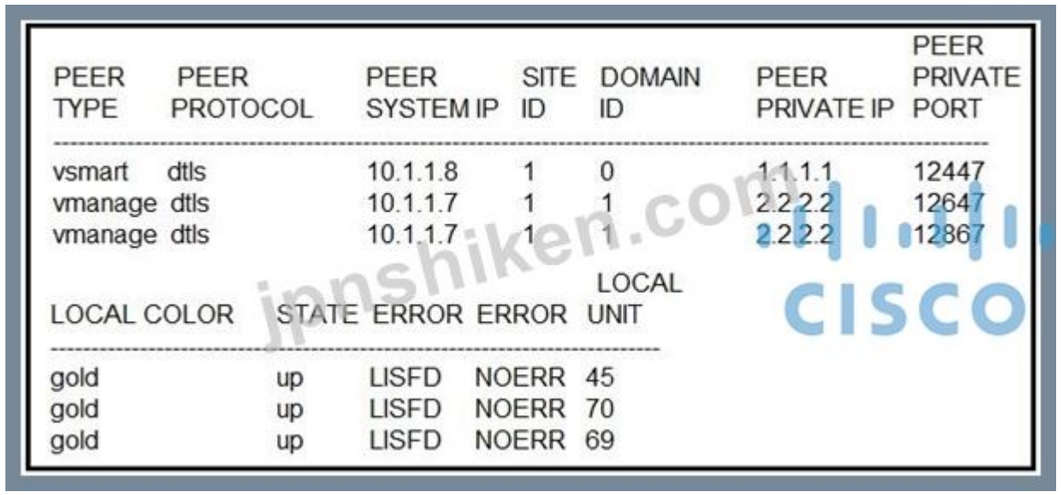
正解: (正解を表示します)
tloc-extension ge0/0 on ge0/1, which extends TLOC transport from vEdge101.
Dynamic routing BGP sessions with both 192.0.0.2 and 172.1.1.2.
This allows vEdge102 to utilize vEdge101's MPLS TLOC through the TLOC extension and form control connections dynamically as required.

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
ネットワーク管理者が、2つのWAN接続と2つのTLOCを備えたWANエッジルータを構成しています。TLOCのどの2つの属性を構成する必要がありますか？(2つ選択してください。)
A. グループID
B. サイトID
C. カプセル化
D. tloc-ip
E. 色
正解: (正解を表示します)
These attributes define how the TLOC operates within the SD-WAN architecture, with encapsulation specifying the type of encapsulation used for the transport and color representing the type of transport (e.g., MPLS, internet, LTE) for the TLOC.

質問: **153**
代替ポートが構成されていない場合、コントローラー証明書の下でvBondに使用されるポートはどれですか？
A. 12345
B. 12347
C. 12346
D. 12344
正解: **C** (コメントを発表する)
vSmart and vManage are normally installed behind NAT device, so port hopping is not needed. vBond always uses to other Viptela devices using port 12346 and they never use port hopping.

質問: **154**
図を参照してください。エンジニアが、ソケットエラーが表示されるWANエッジデバイスの制御接続の問題をトラブルシューティングしています。パケットキャプチャでは、2つのデバイス間で一部のICMPパケットがドロップされていることが示されています。どの操作で問題が解決しますか？

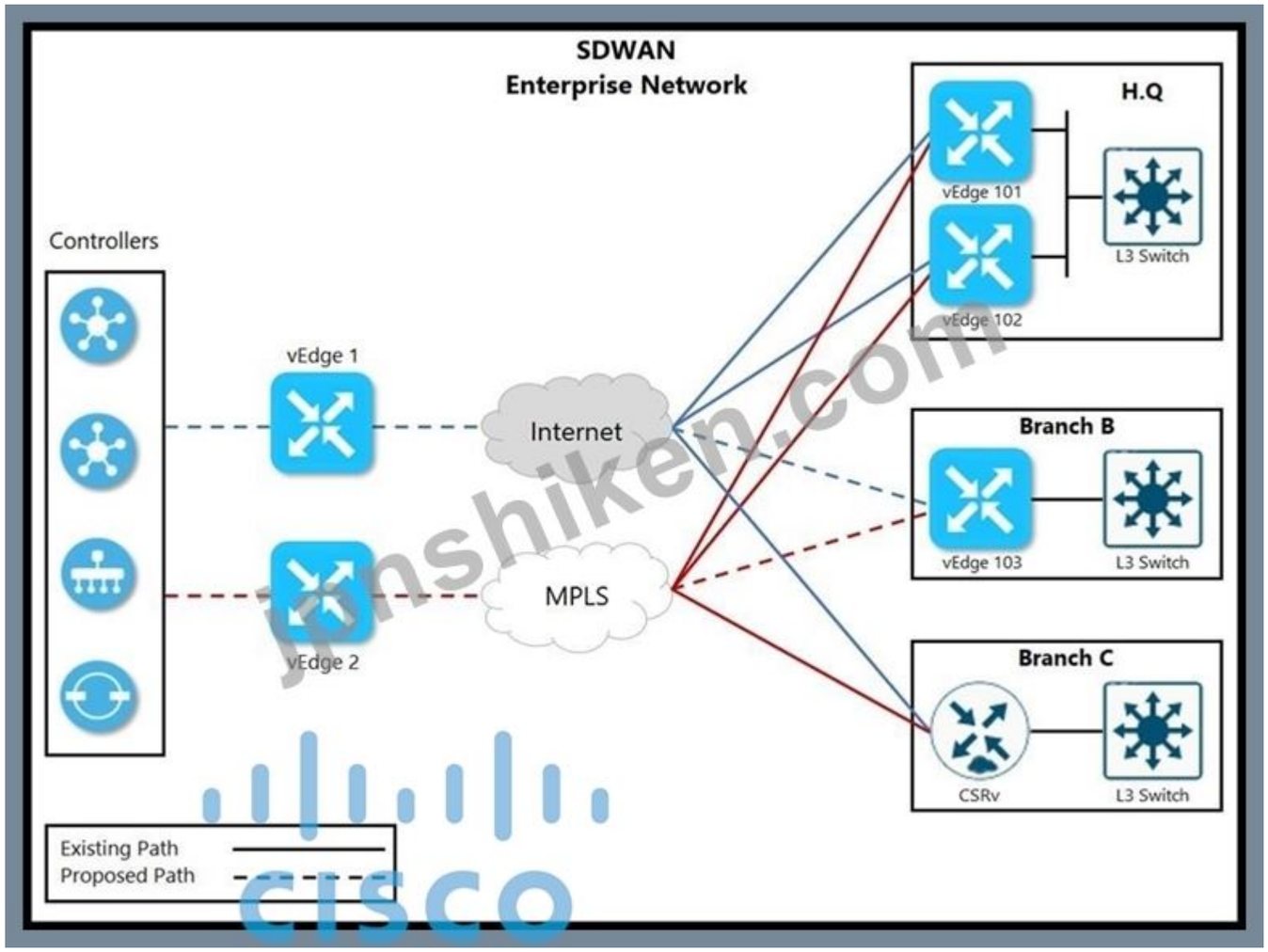


PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT
vsmart	dtls	10.1.1.8	1	0	1.1.1.1	12447
vmanage	dtls	10.1.1.7	1	1	2.2.2.2	12647
vmanage	dtls	10.1.1.7	1	1	2.2.2.2	12867

LOCAL COLOR	STATE	ERROR	ERROR	LOCAL UNIT
gold	up	LISFD	NOERR	45
gold	up	LISFD	NOERR	70
gold	up	LISFD	NOERR	69

A. ネットワーク内のIPアドレスの重複を削除し、一意のIPアドレスを設定します。
B. vBond を復旧するか、コントローラーのリロードを待ちます。これはリセットが原因である可能性があります。
C. 高可用性クラスタでダウンしている vManage コントローラを復旧します。
D. システムIPが変更された場合は、システムIPを変更するか、WANエッジを再起動してください。
正解: **A** (コメントを発表する)
The exhibit displays the LISFD error, (Socket Errors), the most common cause for these errors are due to Duplicate transport IPs. (LISFD) = Socket Errors!
https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control- connections.html#toc-hId-1996362298

質問: **155**
図を参照してください。ネットワークチームは、ブランチBのWANエッジデバイス103を設定し、MPLSおよびインターネット回線を介して、すべての色のブランチ間で動的なフルメッシュIPsecトンネルを確立する必要があります。



このブランチは以下のように構成されています。

```
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
```

どの構成が要件を満たしていますか？

A.

```
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
```

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

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

B.

```
/pn 0
nterface ge0/0
 description "*** Internet Circuit ***
 ip address 209.165.200.225/30
 tunnel-interface
  encapsulation ipsec
  color public-internet
  allow-service all

/pn 1
nterface ge0/1
 description "*** MPLS ***"
 ip address 10.10.0.101/30
 tunnel-interface
  encapsulation ipsec
  color mpls
  allow-service all
```

C.

```
nterface ge0/0
 description "*** Internet Circuit ***
 ip address 209.165.200.225/30
 tunnel-interface
  encapsulation ipsec
  color public-internet
  allow-service all

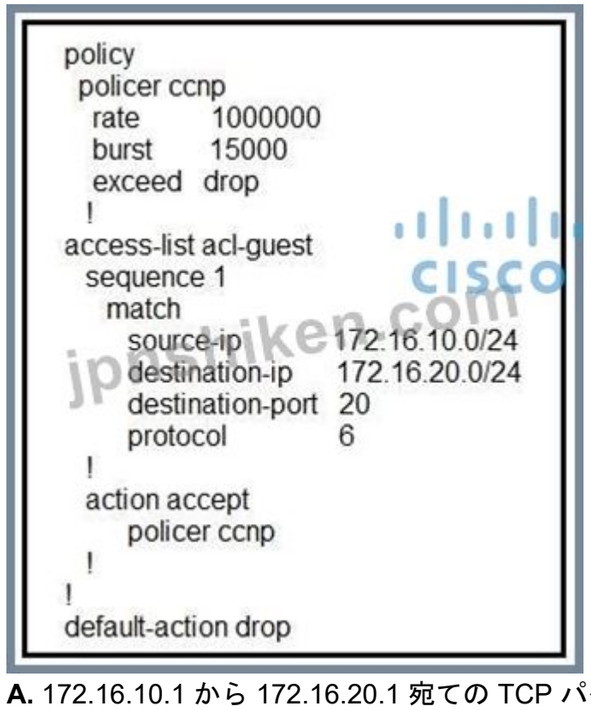
nterface ge0/1
 description "*** MPLS ***"
 ip address 10.10.0.101/30
 tunnel-interface
  encapsulation ipsec
  color mpls
```

D.

正解: (正解を表示します)

質問: **156**

図を参照してください。vpn1インターフェースにアクセスリストacl-guestをインバウンドで適用した後、この構成によってどのようなQoS処理が行われますか？



A. 172.16.10.1 から 172.16.20.1 宛ての TCP パケットが破棄されました
B. 172.16.20.1 から 172.16.10.1 宛ての UDP パケットが受け入れられます
C. 172.16.10.1 から 172.16.20.1 宛ての UDP パケットが破棄されました
D. 172.16.20.1 から 172.16.10.1 宛ての TCP パケットが受け入れられます
正解: (正解を表示します)
Protocol 6 is used for TCP.
Reference:
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

質問: **157**

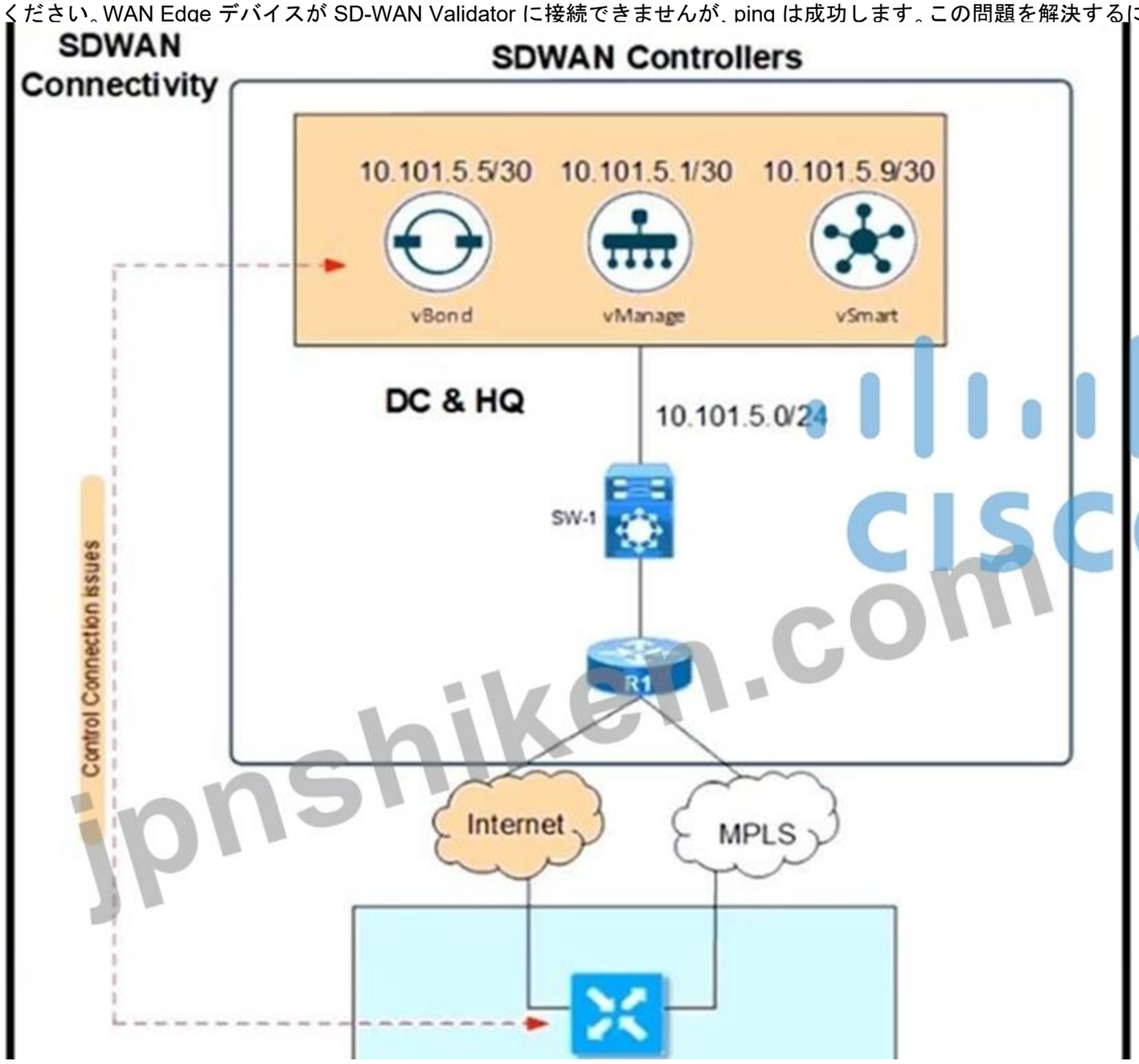
Cisco SD-WANにおける前方誤り訂正は、どのような問題に対処するのでしょうか？
A. インバウンドシェーパーによって発生する非効率的なトラフィック転送
B. サービス劣化に関連するアプリケーションパフォーマンスの低下を軽減
C. 特定の輸送手段において遅延が増加した交通の流れ
D. 時折無効なデータ入力があり、パフォーマンスが低いアプリケーション
正解: (正解を表示します)

質問: **158**

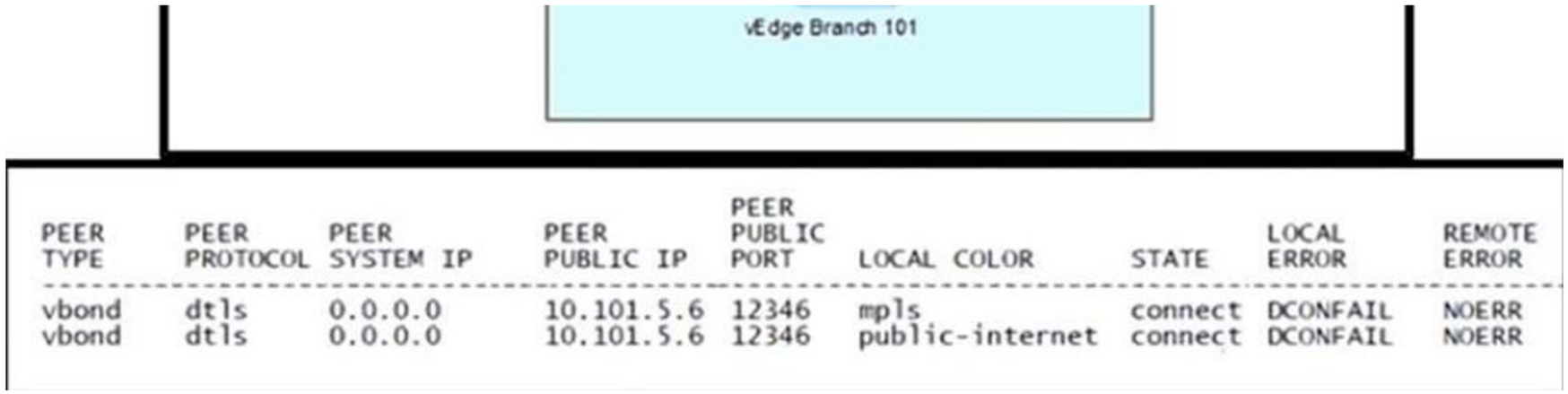
デバイス上で実行されたアクションのステータスを確認するREST API呼び出しはどれですか？
A. 管理者ステータス
B. トラブルシューティングステータス
C. 設定ステータス
D. モニターの状態

正解: **D** (コメントを発表する)
The monitor status REST API call returns the status of a specific action or a list of all actions that have been performed on a device. The status of an action can be one of the following:
Pending - The action has not yet been started.
Running - The action is currently running.
Completed - The action has completed successfully.
Failed - The action has failed.
The monitor status REST API call can be used to troubleshoot problems with actions that are not completing successfully.

質問: **159**
図を参照してください。WAN Edge デバイスが SD-WAN Validator に接続できませんが、ping は成功します。この問題を解決するには、どの操作を行うべきでしょうか？

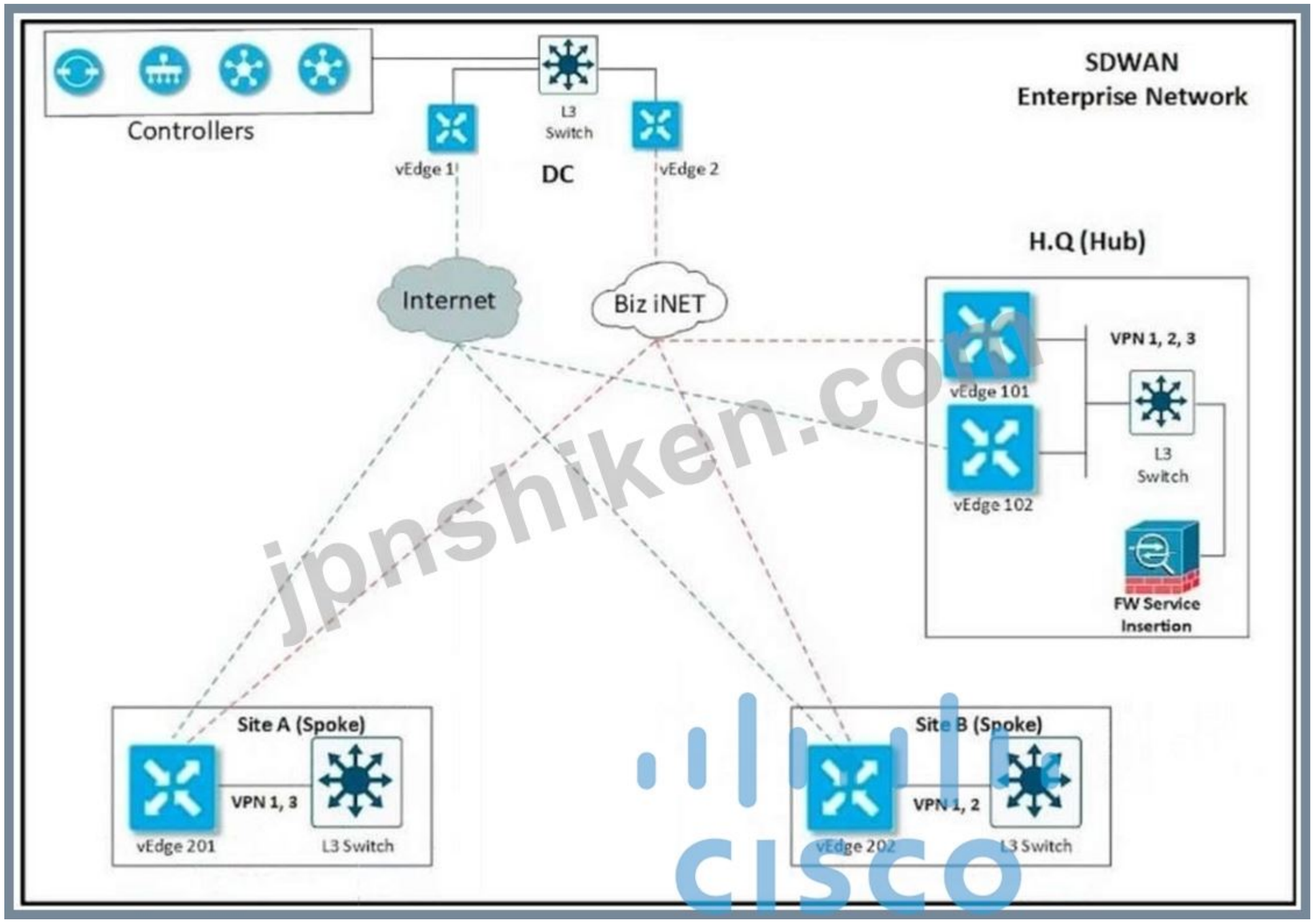


jpnshiken.com



A. SD-WANバリデーターのIPアドレスが正しいことを確認してください。
B. WANエッジ上のシステムIPを変更します。
C. WAN Edge に正しいルート証明書をインストールします。
D. ピアプロトコルをDTLSからTLSに切り替えます。
正解**: (**正解を表示します**)**
The vEdge device shows STATE: connect but LOCAL ERROR: DCONFAIL, which means DTLS connection was attempted but control connection failed - typically due to certificate/authentication issues. Since it can ping the vBond, IP reachability is fine. The most likely cause is a missing or incorrect root certificate, preventing proper TLS handshake and control channel establishment.

質問**: 160**
図を参照してください。顧客は、VPNからのトラフィックをHQでサービス挿入に展開したいと考えています。
1. 両拠点から本社への通信はファイアウォールを経由する必要があります。この通信では、経路漏洩は発生しません。本社における要件を満たす構成はどれですか？



jpnshiken.com
CISCO

A.

```
policy
  lists
    site-list device-1
      site-id 1
  control-policy firewall-service
    sequence 10
      match route
        vpn 1
      action accept
        set service FW
apply-policy
  site-list device-1 control-policy firewall-service out
vpn 1
  service FW address 10.0.0.2
 interface ge0/2.1
  description "*** vpn 1  ***"
  ip address 10.0.0.1/28
  no shutdown
 !
```

B.

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

C.

```
vpn 1
  service FW address 10.0.0.2
 interface ge0/2.1
  description "*** vpn 1 ***"
  ip address 10.0.0.1/28
  no shutdown
 vpn 11
  interface ge0/3.100
  description "*** vpn 11 FW  Inside Interface ***"
  ip address 1.1.1.1/29
  no shutdown
 vpn 12
  interface ge0/3.101
  description "*** vpn 12 FW  Outside Interface ***"
  ip address 2.2.2.1/29
  no shutdown
```

D.

```
vpn 1
  service FW address 10.0.0.2
 interface ge0/2.1
  description "*** vpn 1 ***"
  ip address 10.0.0.1/28
  no shutdown
 !
 interface ge0/3.100
  description "*** vpn 1 FW  Inside Interface ***"
  ip address 1.1.1.1/29
  no shutdown
 !
 interface ge0/3.101
  description "*** vpn 1 FW  Outside Interface ***"
  ip address 2.2.2.1/29
  no shutdown
```

正解: (正解を表示します)

Configuration of the firewall service address.

A control-policy named firewall-servicethat matches VPN 1 and sets the firewall service (set service FW).

Application of this policy to the specific device list, ensuring traffic from VPN 1 is directed through the firewall at HQ.

質問: **161**

ある顧客が、100の支店向けにCisco Catalyst SD-WANソリューションを導入しようとしています。各支店は、MPLS回線のみを使用してハブサイトに接続しています。ネットワークチームは、どのような構成を実装すべきでしょうか？

A.


Route
Sequence Rule
Drag and drop to re-arrange rules
1
Match Conditions
Actions
VPN List: All-VPNs
Accept
VPN Id
TLOC List: Hub_TLOC_MPLS

B.


CONFIGURATION | POLICIES
Add Hub-and-Spoke Policy
VPN List
VPN10
Add Hub-and-Spoke Sites
Add Hub Sites
Add Spoke Sites
Site Lists
Spokes
Hub

C.


Add VPN Membership Policy
VPN Membership Name
HQ-Policy
Description
HQ VPN Membership Policy
Site List
VPN Lists
All
VPN10
VPN_92
Add List

D.



正解: **A** (コメントを発表する)

The first image shows a TLOC-based route policy that directs all VPN traffic to use the Hub_TLOC_MPLS, which is exactly what's needed when branches reach the hub only over MPLS. This policy ensures that traffic from branches is routed via the MPLS circuit toward the hub site.

質問: **162**

OMP を構成する機能テンプレートはどれですか?

A.



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

B.

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

C.

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

D.

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

正解: (正解を表示します)

質問: **163**

Cisco SD-WAN を導入した後、この会社は、デフォルトですべてのサイトが相互に直接 IPsec VPN トンネルを構築していることに気付きました。以前のトポロジでは、すべてのスポーク サイトが、ネットワーク 40.0.0.0/16 に属する LAN セグメントのネクスト ホップとして本社を使用していました。この会社は、ハブから発信される 40.0.0.0/16 ネットワークがスポークにアドバタイズできるようにする以前のポリシーを導入したいと考えています。

どの構成が要件を満たしていますか?

A.



B.



C.



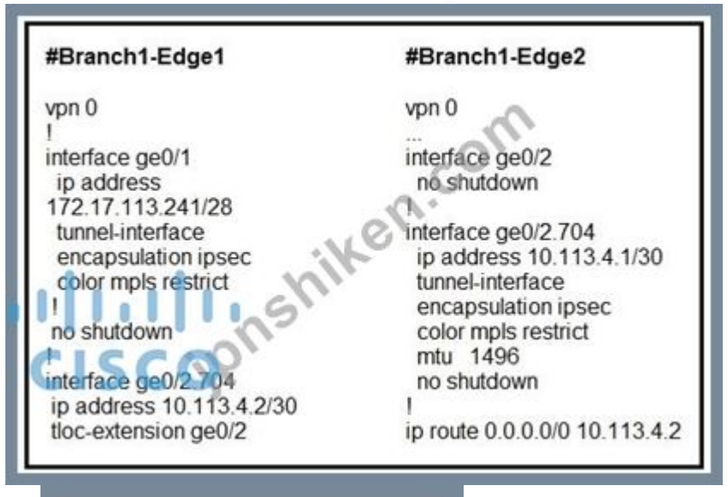
D.



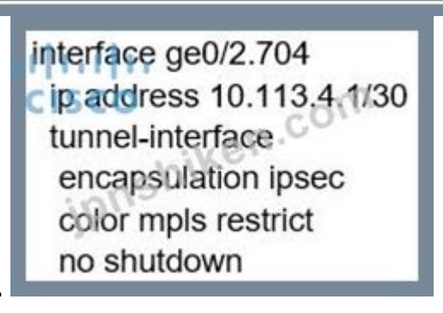
正解: (正解を表示します)

質問: **164**

図を参照してください。Branch1-Edge1 で tloc-extension を構成するには、どの構成変更が必要ですか？



A.



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

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

D.
```
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
```

正解: (正解を表示します)

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 dot1q tag.

質問: **165**

クラウドに導入する必要がある2つのWANエッジデバイスはどれですか？ （2つ選択してください。）

A. vEdge 5000v

B. ASR 1000v

C. CSR 1000v

D. vEdge 100wm

E. vEdgeクラウド

正解: (正解を表示します)

2. Virtual platforms

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

質問: **166**

TLOCルートを一意に識別し、表現するために設定されている属性はどれですか？

A. システムIPアドレス、リンクカラー、およびカプセル化

B. 起源、発信者、および好み

C. サイトID、タグ、VPN

D. ファイアウォール、IPS、およびアプリケーションの最適化
正解: (正解を表示します)
https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.2/03Routing/01Unicast_ Overlay_Routing_Overview#TLOC_Routes

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
SD-WANルーターのSD-WANオーバーレイへの自動オンボーディングを支援するプレーンはどれですか？
A. データ
B. オーケストレーション
C. 管理
D. コントロール
正解: (正解を表示します)
The Cisco Catalyst SD-WAN solution is comprised of separate orchestration, management, control, and data planes.
- The orchestration plane assists in the automatic onboarding of the SD-WAN routers into the SD- WAN overlay.
- The management plane is responsible for central configuration and monitoring.
- The control plane builds and maintains the network topology and makes decisions on where traffic flows.
- The data plane is responsible for forwarding packets based on decisions from the control plane.

質問: **168**
vEdgeルーターにプッシュされたポリシーを検証するコマンドはどれですか？
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
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book.pdf

質問: **169**
vSmart コントローラおよび WAN エッジ ルータの OMP グレースフル リスタートのデフォルト値は何ですか?
A. 21,600秒
B. 43,200秒
C. 86,400秒
D. 604,800秒
正解: **B** (コメントを発表する)
Graceful Restart Timer: default is 12hours (43200 sec)

Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart.
Range: 0 through 604800 seconds (168 hours, or 7 days) Default: 43200 seconds (12 hours)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing- book/m-unicast-routing.html#concept_rjl_sc2_b3b

質問: **170**
TLOC拡張インターフェースの目的は何ですか？
A. 隣接するWANエッジルーターのトランスポートへのアクセスを提供します
B. 隣接するWANエッジルーターと設定を同期します
C. ビジネスインターネットへのアクセスを提供します
D. 接続された輸送手段への代替接続を形成します
正解: **(**正解を表示します**)**

質問: **171**
KVM 経由で Cisco SD-WAN コントローラを導入する場合の Red Hat Enterprise Linux オペレーティング システムの最小要件は何ですか?
A. RHEL 7.5
B. RHEL 6.5
C. RHEL 4.4
D. RHEL 6.7
正解: **A (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/compatibility-and-server- recommendations.pdf

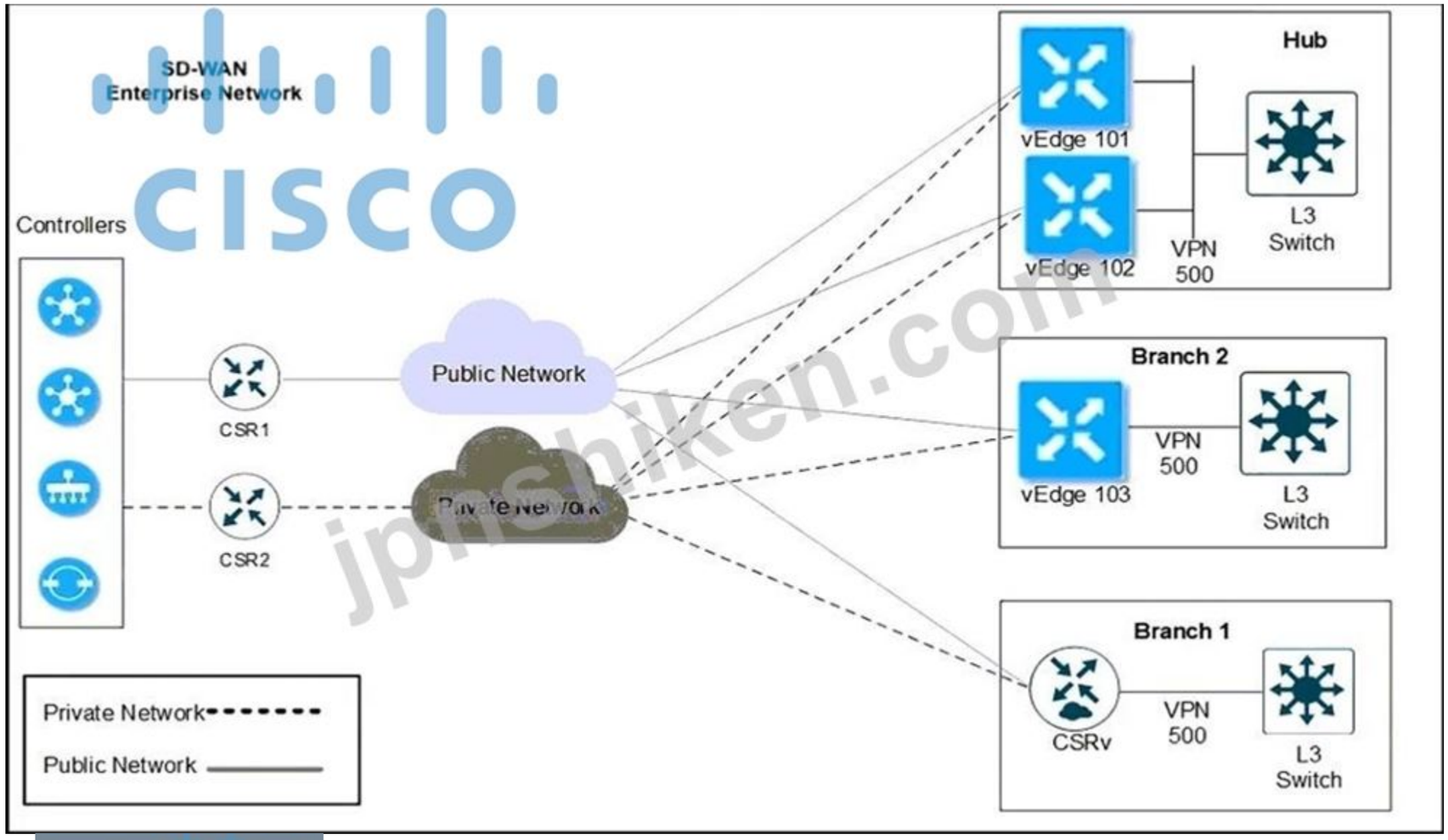
質問: **172**
OMP 機能テンプレートのプレフィックスごとにアドバタイズされるパスの数のデフォルト値は何ですか?
A. 4
B. 8
C. 12
D. 16
正解: **A (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/vEdge-20-x/routing- book/m-unicast-routing.html A Cisco vSmart Controller learns the same OMP route, 10.10.10.0/24, from two Cisco vEdge devices in the same site. If all other parameters are the same, both routes are chosen and advertised to other OMP peers. By default, up to four equal-cost routes are selected and advertised.

質問: **173**
Cisco SD-WANコントローラでは、カスタムアプリケーションポートはどのように監視されますか？
A. お客様は、vAnalytics および vSmart にカスタム アプリケーション ポートを追加します。
B. CiscoはvAnalytisとvManageにカスタムアプリケーションポートを追加しました。
C. お客様は、vAnalytics および vManage にカスタム アプリケーション ポートを追加します。
D. CiscoはvAnalyticsとvSmartにカスタムアプリケーションポートを追加しました。
正解: **(**正解を表示します**)**
Custom Application Ports Created in VManage is activated immediately for application visibility functionality only (Monitoring Traffic).
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies- book/m-custom-applications.pdf

質問: **174**
オーバーレイネットワークサイトID:S0123T4E56F78において、Cisco vManageをインストールし、WANエッジデバイスと統合するには、少なくとも1つのインターフェースにどのVPNが存在する必要がありますか？
A. VPN 512
B. 選択されたVPN番号
C. VPNサービス範囲 0-511
D. VPN 0
正解: (正解を表示します)
Cisco vManage is a centralized management platform for Cisco SD-WAN. It uses VPN 0, also known as the transport VPN, to communicate with WAN Edge devices. Therefore, VPN 0 must be present on at least one interface of the vManage VM in order to install it and integrate it with WAN Edge devices.

質問: **175**
REST API を使用する利点は何ですか?
A. イベント管理とログ記録のための定義済みの自動化およびオーケストレーション プラットフォーム
B. ユーザー定義の自動化と他のオーケストレーション システムまたはツールへの統合
C. 運用サービスの統合とリアルタイムのイベント監視を簡素化する vAnalytics
D. イベント管理とログ記録のための他のプラットフォーム統合を備えた定義済み SD-WAN コントローラ
正解: (正解を表示します)
One of the key benefits of using REST APIs (Representational State Transfer Application Programming Interfaces) is their flexibility and the ability for users to define their own automation and integrate systems or tools according to their specific needs. REST APIs allow for the creation of custom scripts and applications that can interact with different services and platforms, making it a powerful tool for automation and integration in various contexts, including software development and system administration.

質問: **176**
図を参照してください。エンジニアが、データセンターでCisco Catalyst SD-WANソリューションに移行する前に、WAN vEdge101デバイスを構成して概念実証を行っています。どの構成でこのタスクが達成されますか？



A.

```
vpn 0
 interface ge0/0
  ip address 99.0.0.1/30
  tunnel-interface
   encapsulation ipsec
   group 101
   color silver
interface ge0/1
  ip address 192.0.0.1/30
  tunnel-interface
   encapsulation ipsec
   group 101
   color gold
```

B.
```
vpn 0
 interface ge0/0
  ip address 99.0.0.1/30
  tunnel-interface
   encapsulation ipsec
   group 101
   color public-internet
interface ge0/1
 ip address 192.0.0.1/30
 tunnel-interface
  encapsulation ipsec
  group 102
  color custom1
```

C.
```
vpn 0
 interface ge0/0
  ip address 99.0.0.1/30
  tunnel-interface
   encapsulation ipsec
   group 101
   color mpls
 interface ge0/1
  ip address 192.0.0.1/30
  tunnel-interface
   encapsulation ipsec
   group 102
   color metro-ethernet
```

D.
```
vpn 0
 interface ge0/0
  ip address 99.0.0.1/30
  tunnel-interface
   encapsulation ipsec
   group 101
   color mpls
interface ge0/1
  ip address 192.0.0.1/30
 tunnel-interface
  encapsulation ipsec
  group 102
  color green
```

正解: (正解を表示します)

The goal is to test SD-WAN connectivity over public and private transport (as shown in the diagram with Public and Private Network clouds) Color silver is a valid SD-WAN transport color often mapped to internet.

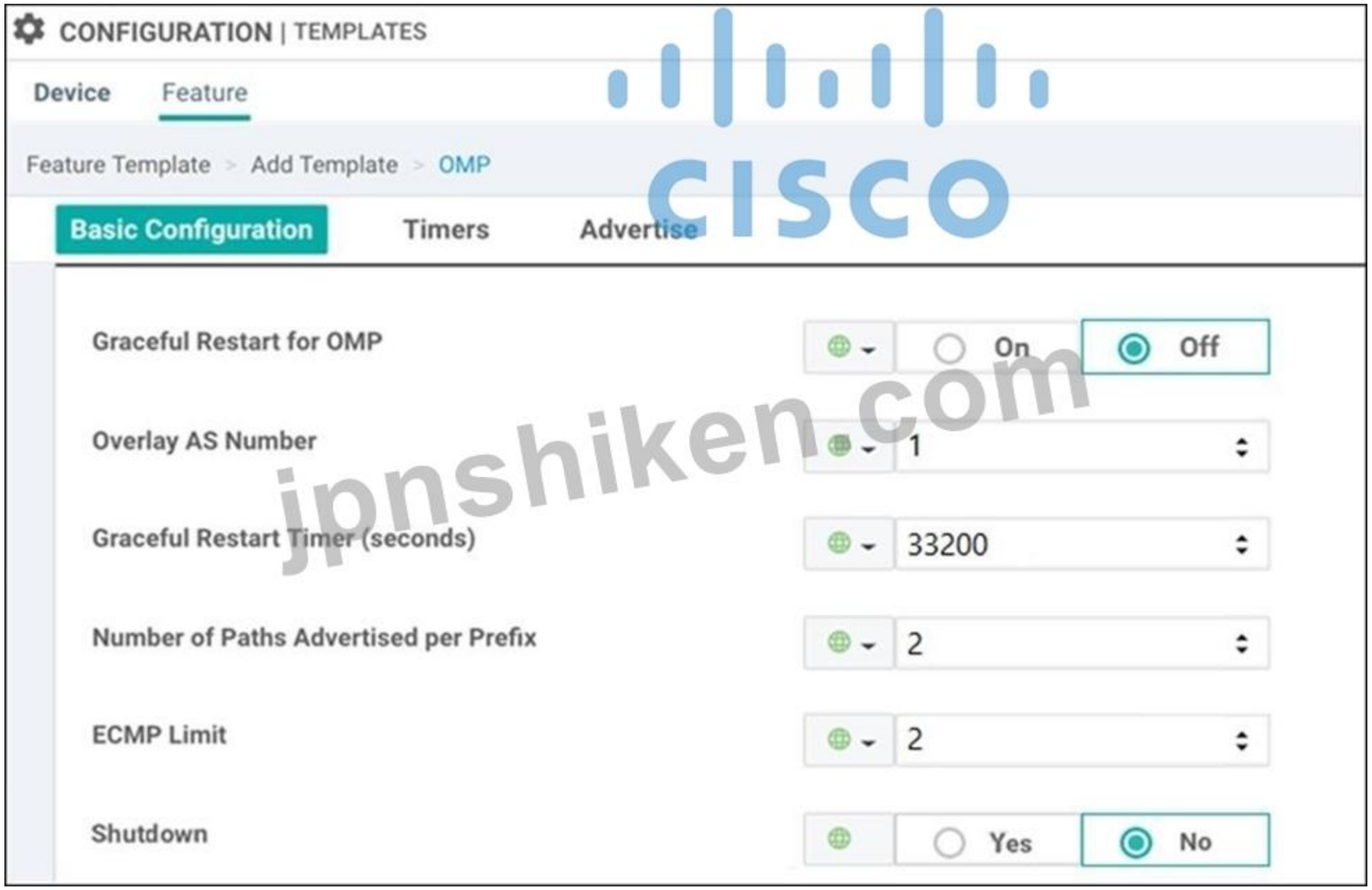
Color gold is used for private WAN (MPLS).

This matches the proof-of-concept topology and is appropriate for standard SD-WAN transport scenarios, unlike custom or undefined colors shown in other options.

質問: **177**

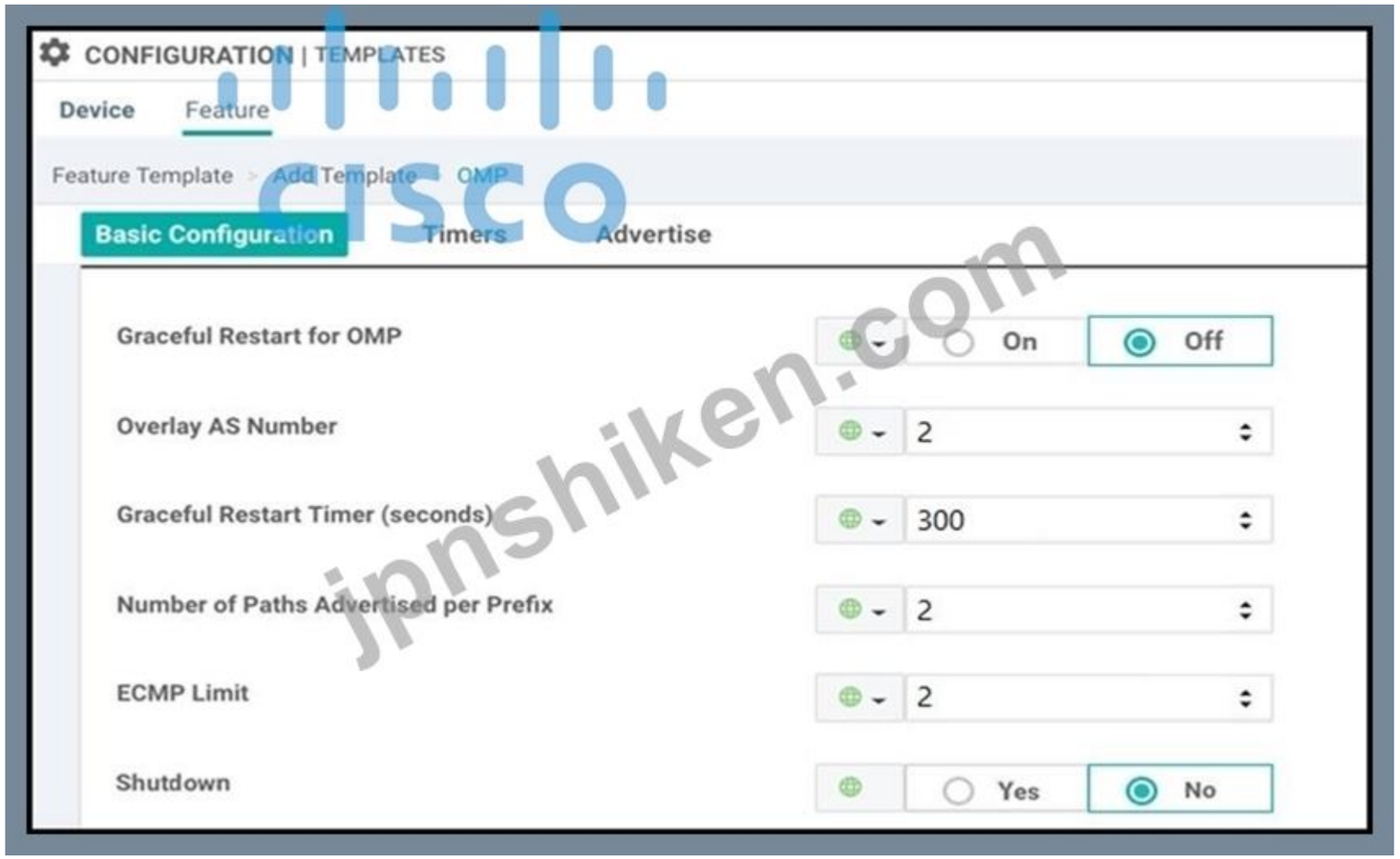
ブランチ ルータが OMP ピアとの接続を失った場合に、企業が WAN エッジ デバイス間のトラフィック転送を継続するには、リモート サイトとデータ プレーンでのダウンタイムを回避する必要があります。どの構成が要件を満たしていますか。

A.



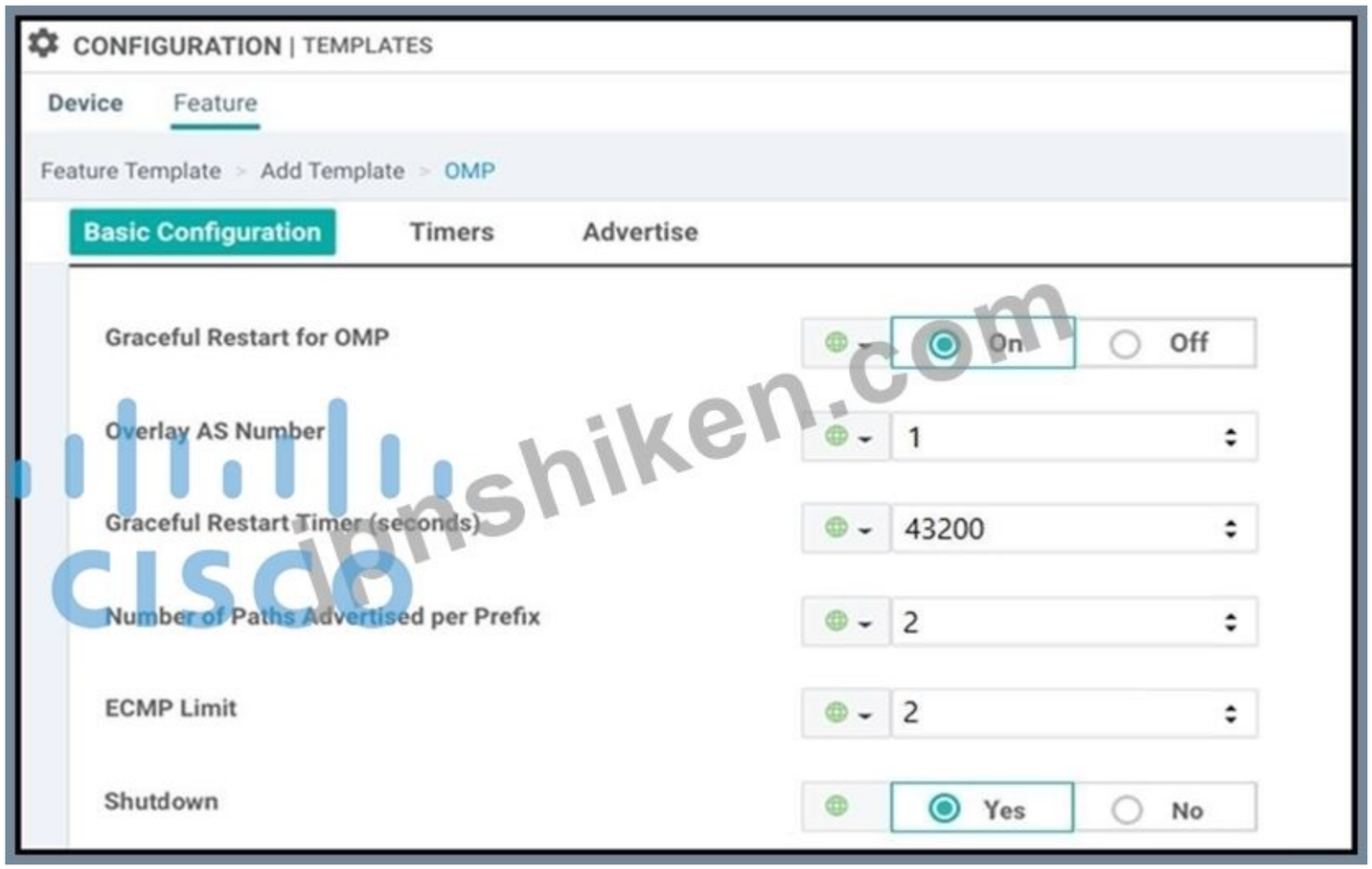
jpnshiken.com

B.

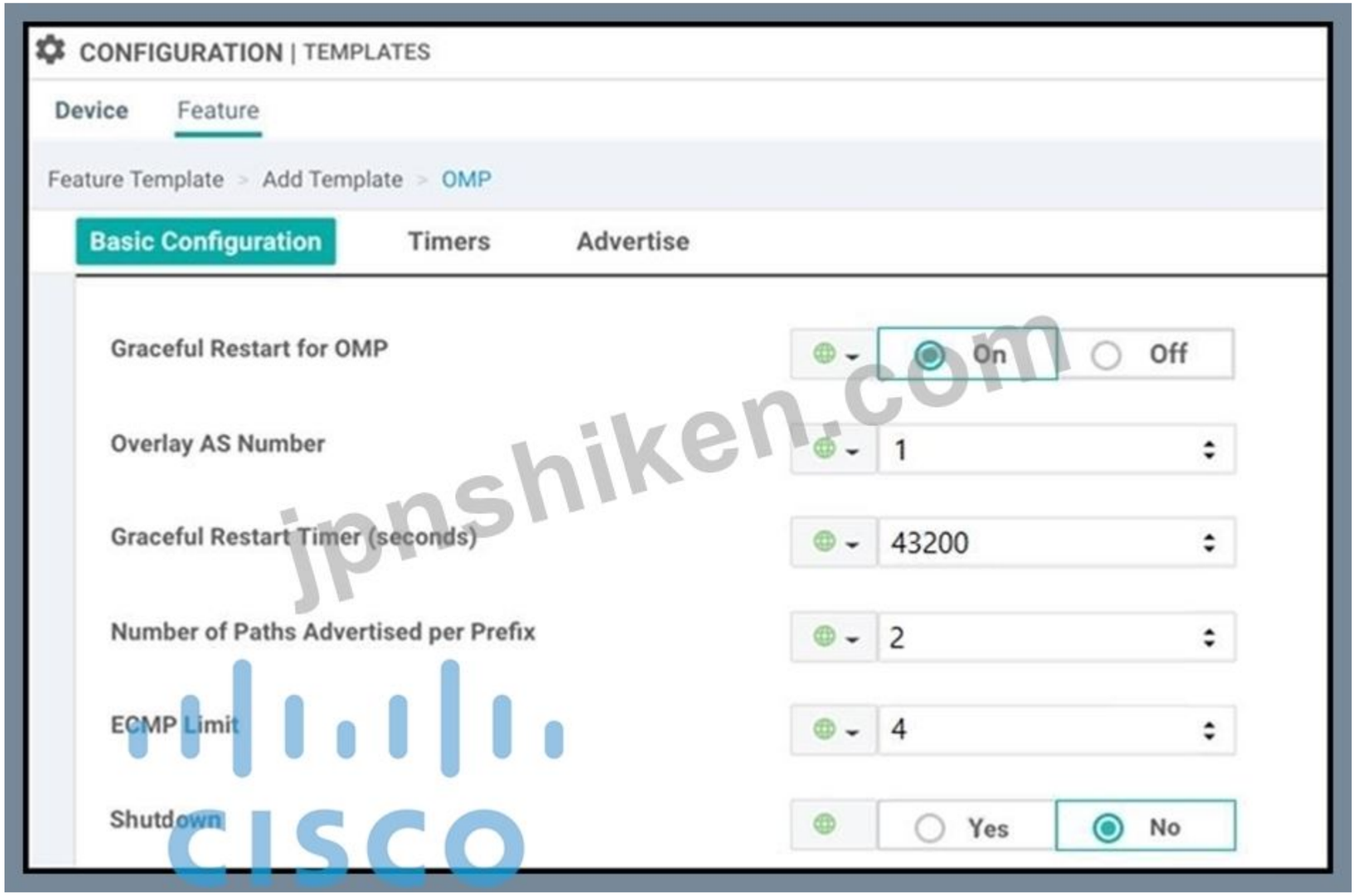


cisco
jpnshiken.com

C.


CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > OMP
Basic Configuration
Timers
Advertise
Graceful Restart for OMP
On
Off
Overlay AS Number
1
Graceful Restart Timer (seconds)
43200
Number of Paths Advertised per Prefix
2
ECMP Limit
2
Shutdown
Yes
No

D.



正解: (正解を表示します)

質問: **178**

Cisco V-Edgeルーターは、QoSトラフィック分類をどこで実行しますか？

A. VPNごと

B. vEdgeごと

C. イングレスインターフェース

D. 出力インターフェース

正解: **C** (コメントを発表する)

質問: **179**

Cisco SD-WAN WAN Edge (vEdge) デバイスで利用できる高度なセキュリティ機能はどれですか？(2つ選択してください。)

A. エンタープライズファイアウォール

B. URLフィルタリング

jpnshiken.com

C. Cisco AMP および AMP 脅威グリッド
D. 鼻を鳴らす侵入防止システム
E. Cisco Umbrella DNSセキュリティ
正解: **(**正解を表示します**)**

質問: **180**
Cisco Umbrella SIGは、どのCisco SD-WAN導入シナリオにおいて最も大きな価値を発揮しますか？
A. Cisco IOS XE SD-WAN デバイスがネットワーク全体に展開されている場合
B. リソース集約型のセキュリティ操作がエントリーレベルのWANエッジデバイスからオフロードされる場合
C. 複数のWANエッジデバイスのIDがネットワーク全体で検証される場合
D. 集中型インターネットブレイクアウトソリューションが実装された場合
正解: **(**正解を表示します**)**

質問: **181**
企業は以下の3つのWAN接続を持っています。
- 公共インターネット
- ビジネスインターネット
- MPLS
エンジニアは、利用可能な2つのリンクを両方経由してトラフィックをルーティングするように構成する必要があります。どの構成がこの目的を達成しますか？
A. omp
シャットダウンなし
ecmp制限2
B. omp
シャットダウンなし
send-path-limit 2
C. omp
シャットダウンなし
オーバーレイとして 2
D. omp
シャットダウンなし
ルート制限 2
正解: **A (**コメントを発表する**)**
If you want to route traffic (which means to send packets on a different links), you need to use ecmp-limit, because it affects the data plane. The question does not mention advertising prefixes (which is configured with send-path-limit). Send-path-limit would advertise two prefixes to vSmart and it would pass them to other EDGEs, so they could load balance, but only if they have ecmp- limit >= 2.

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**

エンジニアがWANエッジルーターをプロビジョニングします。WANエッジルーターからvManageでアクティブ化するには、どのコマンドを使用すればよいですか？
A. vedge-cloud のシャーシ番号トークンの有効化をリクエスト
B. vedge-cloud のシャーシ番号組織の有効化をリクエストします
C. vedge-cloud のシャーシ番号シリアルの有効化をリクエスト
D. vedge-cloud のシリアルトークンの有効化をリクエストします
正解: **(**正解を表示します**)**

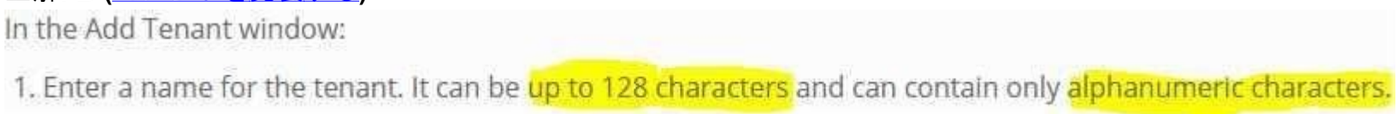
質問: **183**
Cisco Catalyst SD-WANでは、ソフトウェアプロセスはどのように管理されますか？
A. コントローラのソフトウェアアップグレード操作には、SD-WAN Manager、SD-WAN Validator、および SD-WAN を含める必要があります。
B. SD-WAN Manager GUI を介したソフトウェアのダウングレードはサポートされていません。
C. ソフトウェアイメージは、HTTP または FTP を介して SD-WAN Manager にアップロードする必要があります。
D. ソフトウェアイメージは、SD-WAN Manager の VPN 512 を介して転送されます。
正解: **D (**コメントを発表する**)**
From the Cisco vManage menu, choose Maintenance > Software Repository.
For the desired remote server, click ...
To view the remote server settings, click View Details.
To edit the remote server settings, click Edit. Edit any of the following settings as necessary and click Save.
Note
You cannot edit the remote server settings if you have added locations of any software images on the remote server to the Cisco vManage software repository. If you wish to edit the remote server settings, remove the software image entries from the software repository and then edit the settings.
Server Info
Server Name: Enter a name for the server.
Server IP or DNS Name: Enter the IP address or the DNS name of the server.
Protocol: Choose HTTP or FTP.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And- Maintain/monitor-maintain-book/maintain.html#concept_flr_scg_5rb

質問: **184**
ネットワーク管理者が監視目的で、Cisco WAN EdgeルータのCLIからSNMPv3を設定します。snmp userコマンドでサポートされる文字数はいくつですか？
A. 1から8まで
B. 1から16まで
C. 1から32まで
D. 1から48まで
正解: **C (**コメントを発表する**)**
In Cisco SD-WAN Solution, when configuring SNMPv3 on a Cisco WAN Edge router from the CLI, the "snmp user <username>" command supports a password length of 1 to 32 characters.

質問: **185**
Google Cloud と Cisco SD-WAN の統合におけるサイト間通信にはどの TLOC カラーが使用されますか?
A. プライベート1
B. プライベート2
C. プライベート3

D. プライベート4
正解: **(**正解を表示します**)**
On enabling site-to-site connectivity within each of the cloud gateways, an additional WAN tunnel interface is automatically created and added through the Cloud onRamp workflow with its color automatically set to private1. This interface is associated with the Site-to -Site VPC (s2s-enb- solutions-21615) and is assigned a private IP address.

質問: **186**
エンジニアがvManageでロケーションID 306432373のテナントを追加しています。テナント名フィールドに入力できる英数字の最大文字数はいくつですか？
A. 64
B. 128
C. 256
D. 8
正解: **B (**コメントを発表する**)**



質問: **187**
CiscoSD-WANセキュアエクステンシブルネットワーク内のvSmartコントローラとWANエッジルータ間でコントロールプレーン情報を交換するために使用されるルーティングプロトコルはどれですか。
A. BGP
B. OSPF
C. BFD
D. OMP
正解: **(**正解を表示します**)**
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco- sd-wan-ebook-cte-en.pdf

質問: **188**
エンジニアは、VPN 200のDIAのデータポリシーを修正し、以下の場所宛てのトラフィックの要件を満たすようにします。
- 外部ネットワーク; 翻訳が必要
- 外部ネットワーク。パブリックTLOCカラーを使用する必要があります。
- syslogサーバーでは、プライベートTLOCカラーを使用する必要があります
既存のデータポリシー設定は以下のとおりです。

```
data-policy DIA
 vpn-list VPN-200
  sequence 10
   match
    destination-data prefix-list INTERNAL-NETWORKS
 !
 action accept
sequence 20
 match
  destination-ip 0.0.0.0/0
!
action accept
 nat use-vpn 0
 !
!
default-action reject
```

どのポリシー構成シーケンスセットが要件を満たしていますか？

```
   natch
   destination-data-prefix-list SYSLOG-SERVER

   action accept
   set
    local-tloc-list
    color mpls
   sequence 20
    match
      destination-ip 0.0.0.0/0
   !
   ction accept
   set
    local-tloc-list
```

A. color biz-internet

jpnshiken.com

B.

```
sequence 25
 match
  destination-ip 0.0.0.0/0
 !
 action accept
  set
   local-tloc-list
   color biz-Internet
 sequence 30
  match
   destination-data-prefix-list SYSLOG-SERVERS
 !
action accept
 set
 local-tloc-list
  color mpls
```

```
sequence 15
match
 destination-ip 0.0.0.0/0
!
action accept
 set
  local-tloc-list
  color biz-Internet
sequence 30
 match
  destination-data-prefix-list SYSLOG-SERVER
!
action accept
```

C. nat use-vpn 0

D.

```
sequence 5
 match
  source-ip 0.0.0.0/0
 !
 action accept
 set
  local-tloc-list
   color biz-internet
sequence 30
 match
   destination-data-prefix-list SYSLOG-SERVERS
 !
 action accept
 set
  local-tloc-list
   color mpls
```

jpnshiken.com

正解: **A** (コメントを発表する)

質問: **189**

SD-WANソリューションのどのデバイスがイベントレポートを受信して分類し、アラームを生成しますか？

A. WAN Edge routers

B. vSmart controllers

C. vManage NMS

D. vBond controllers

正解: (正解を表示します)

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And- Maintain/monitor-maintain-book/m-alarms-events-logs.html

https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/vmanage/vmanage-how- tos-18-4-1.pdf

質問: **190**

ゼロタッチオンボーディングプロセスをサポートするために、PNP/ZTPではどのデバイス情報が必要ですか？

A. シリアル番号とシャーシ番号

B. インターフェースIPアドレス

C. パブリック DNS エントリ

D. システムIPアドレス

正解: (正解を表示します)

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

質問: **191**

どのアプリケーションリストが事前設定されていますか？

A. Microsoft_Office365

B. Cisco_Apps
C. Google_Apps
D. P2Pアプリ
正解: (正解を表示します)

質問: **192**
エンジニアリングチームは、管理VLANからのトラフィックにはMPLS回線を優先的に使用するというトラフィックエンジニアリングポリシーを作成する必要があります。インターネットはバックアップとしてのみ使用する必要があります。この要件を満たす構成はどれですか？

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
```

正解: (正解を表示します)

Prefer route with highest TLOC preference.

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/TECRST-2191.pdf

質問: **193**

SD-WANのオーバーレイネットワーク全体におけるマルチキャストパケット配信を最適化するには、エンジニアはどのようにすればよいでしょうか？

A. マルチキャストソースに接続されているWANエッジルーター上のパケット複製を無効にします。

B. WANエッジルータがマルチキャストソースのIPアドレスを学習できるように、共有ツリーを構築します。

C. ラストホップルータがマルチキャストソースのIPアドレスを学習できるように、共有ツリーを構築します。

D. マルチキャストソースに接続されているイングレスルータでのパケット複製を無効にします。

正解: (正解を表示します)

To optimize multicast packet distribution in Cisco SD-WAN, packet replication should be eliminated on the ingress router (the WAN Edge connected to the multicast source). Instead, replication is offloaded to replicator routers in the overlay, improving bandwidth efficiency and reducing processing load.

質問: **194**

どのVPNにおいて、発信インターフェース上のNAT操作は、インターネットへの直接アクセス用に構成されていますか？

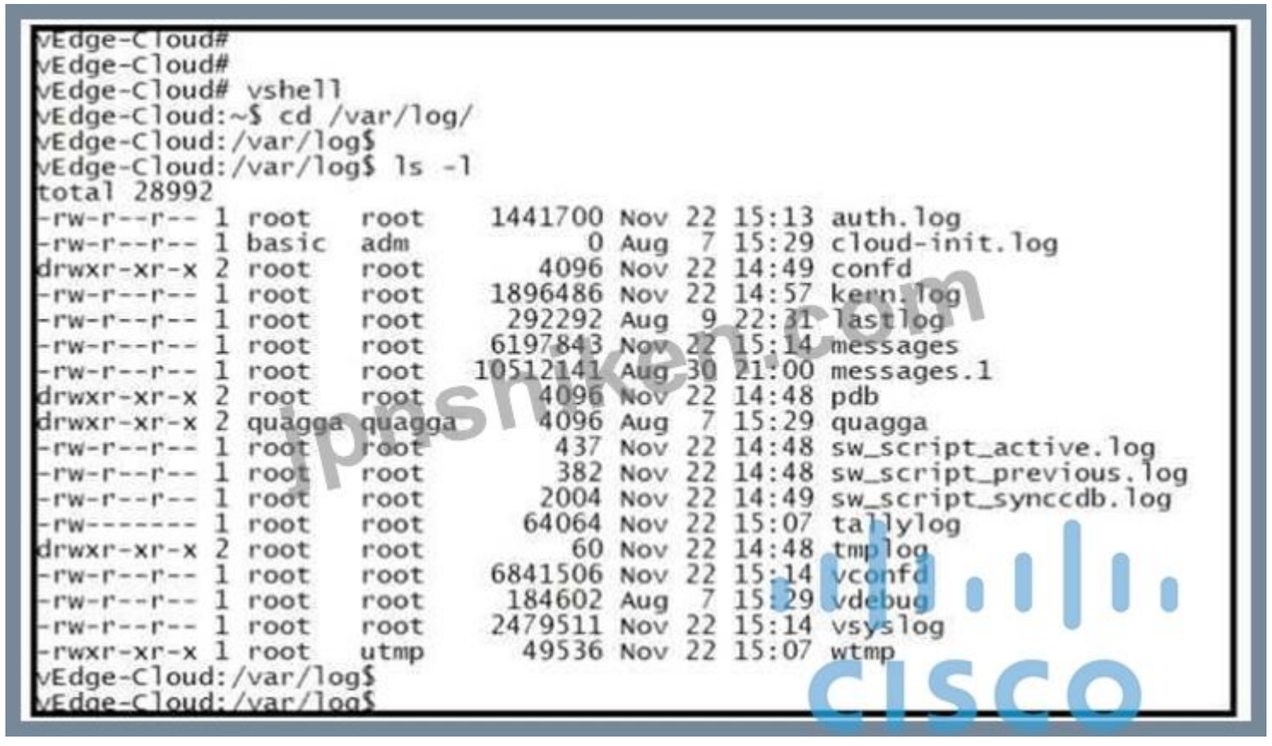
A. 0

B. 512

C. 10
D. 1
正解: (正解を表示します)
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2019nov.pdf

質問: **195**
vSmartの構成要素を2つ挙げてください。(2つ選択してください。)
A. モニタリング
B. デバイステンプレートの作成
C. NATトラバーサル
D. キーリフレクション
E. ポリシーエンジン
正解: (正解を表示します)

質問: **196**
図を参照してください。移行中にWANエッジデバイスでのNetconf CLIログ記録を停止する設定はどれですか？





A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: (正解を表示します)

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

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

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

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

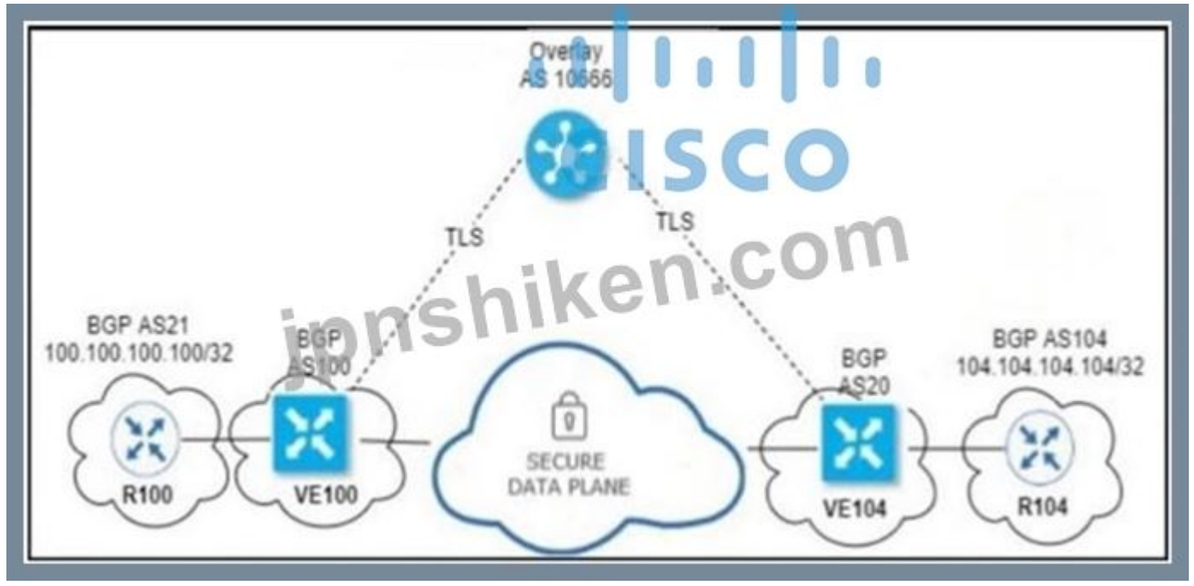
質問: **197**
SD-WANソリューションの機能として適切なものはどれですか？(2つ選択してください。)
A. 管理プレーン、制御プレーン、データプレーンを分離して水平スケーリングを可能にする
B. トラックで出動する支線が立ち上がり、容易な供給と新規設置が可能になる。
C. クラウドホスト型またはオンプレミス型の完全冗長管理および制御プレーン機能
D. 補完的な製品やアプリケーションとセキュリティを提供および統合する能力
正解: (正解を表示します)

質問: **198**
どのサービス VPN がすべての WAN エッジ デバイスとコントローラから到達可能である必要がありますか?
A. VPN0
B. VPN512

C. VPN10
D. VPN215
正解: **A (**コメントを発表する**)**

質問: **199**
エンジニアは、集中制御ポリシーで、長さが/ 1から/ 16までのすべてのIPプレフィックスに一致するリストを設定しています。どのリストがこのタスクを実行しますか？
A. 0.0.0.0/1 le 16
B. 0.0.0.0/0 ge 1
C. 0.0.0.0/0 le l6
D. 0.0.0.0/16 ge 1
正解: **(**正解を表示します**)**
* 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

質問: **200**
添付資料を参照してください。エンジニアがオーバーレイAS 10666を使用してOMPを構成しました。
R100 上でプレフィックス 104.104.104.104/32 の AS PATH は何ですか？



A. 100 10666
B. 100 20 104
C. 100 10666 20 104
D. 100 10666 104
正解: **A (**コメントを発表する**)**

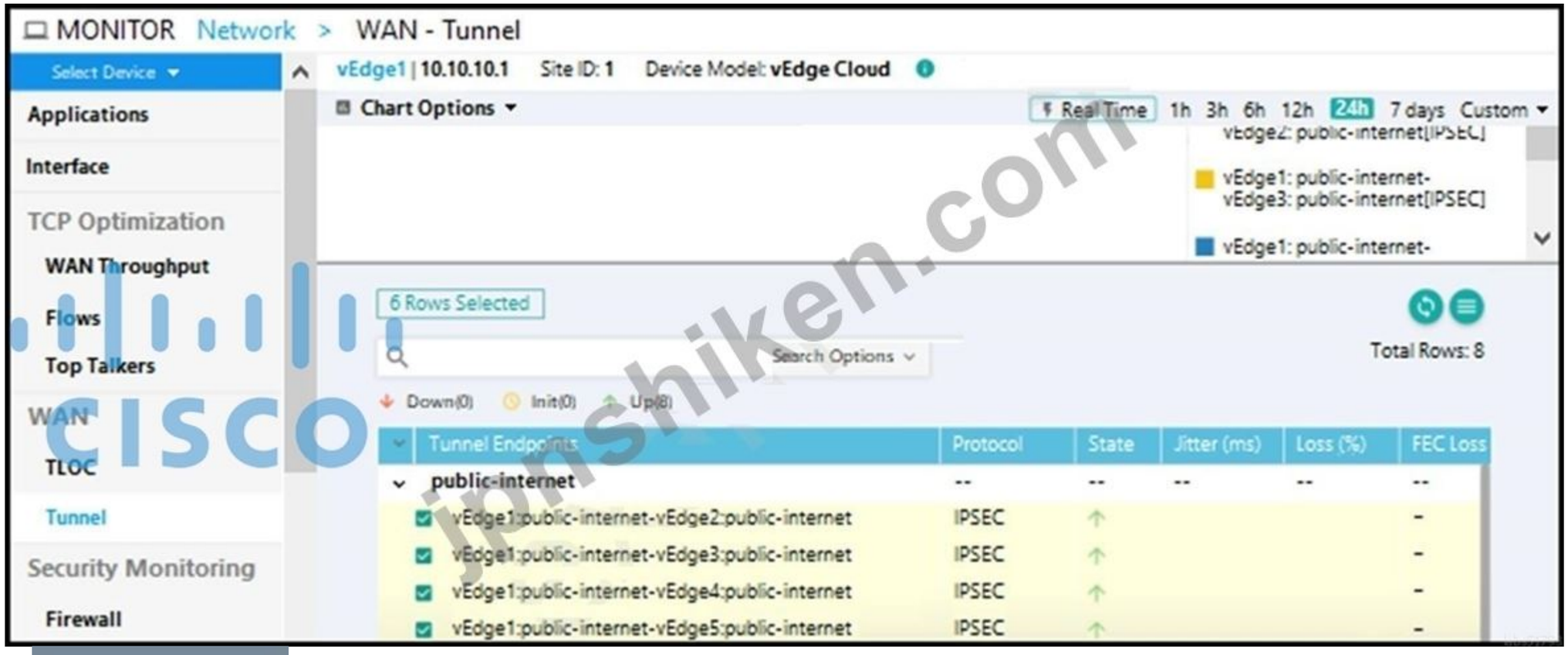
質問: **201**
データトラフィックがSLAクラスに一致する場合に、特定の種類のトンネルを選択するために使用されるキーワードは何ですか？

A. sia-preferred-color
B. 優先色
C. デフォルト
D. 厳密
正解: **B (**コメントを発表する**)**
The keyword preferred-color is used to choose a specific type of tunnel when SLA class is matched by the data traffic. The keyword sia-preferred-color is not a valid keyword. The keywords default and strict are used to specify the default tunnel and the strict tunnel, respectively.

質問: **202**
Cisco SD-WAN仮想プラットフォームはどれですか？
A. Cisco CSR 1000V
B. Cisco ASR 1000
C. Cisco Nexus 1000V
D. Cisco ISR 4000
正解: **(**正解を表示します**)**

質問: **203**
オーバーレイネットワーク内のCiscoデバイスに対して実行されるREST API関数はどれですか？(2つ選択してください。)
A. デバイス構成テンプレートを添付します
B. デバイスにクエリを実行して統計情報を集計する
C. デバイス間でSnortイメージを配布する
D. 監視デバイス証明書
E. スマートライセンスのための接続管理
正解: **A,B (**コメントを発表する**)**
In a Cisco SD-WAN overlay network, the REST APIs provided by the vManage NMS are used to interact with devices and manage policies, configurations, and monitoring.
Attaching a device configuration template
- REST APIs allow you to push configuration templates to devices.
- This is a core function of centralized device management in SD-WAN.
Querying a device and aggregating statistics
- REST APIs are frequently used to pull operational data and statistics (CPU, memory, interface stats, application performance, etc.) from devices and aggregate them for monitoring and analytics.

質問: **204**
図を参照してください。WANエッジデバイスでこれらの結果を実現するコマンドライン設定はどれですか？



A.

```
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
```

B.

```
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
```

C.
```
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
```

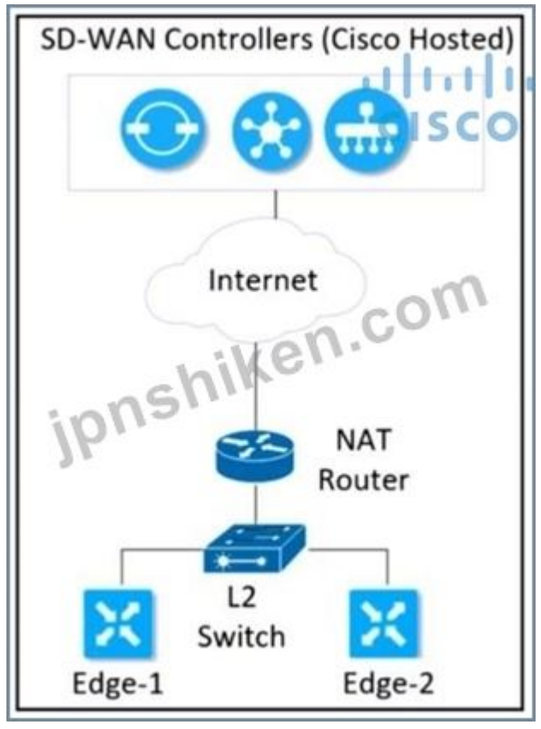
D.
```
vpn 0
interface ge0/0
  ip address 10.50.0.101/30
  tunnel-interface
    encapsulation ipsec
    color public-internet restrict
    allow-service all
    allow-service netconf

ip route 0.0.0.0/0 10.50.0.102
```

正解: **D** (コメントを発表する)

質問: **205**

図を参照してください。Cisco SD-WANネットワークのアンダーレイ接続を確立するために、エンジニアはどの構成を使用する必要がありますか？



A.

```
R1
vpn 0
interface ge0/0
ip address 10.50.0.2/30
tunnel-interface
!
Ip route 0.0.0.0/0 10.50.0.4

R2
vpn 0
interface ge0/0
ip address 10.50.0.3/30
tunnel-interface
!
Ip route 0.0.0.0/0 10.50.0.4
```

B.

```
R1
vpn 512
interface eth0
ip address 10.0.0.21/24
no shutdown
!
Ip route 0.0.0.0/0 10.0.0.254

R2
vpn 512
interface eth0
ip address 10.0.0.2/24
no shutdown
!
Ip route 0.0.0.0/0 10.0.0.254
```

cisco
ipnshiken.com

C.

```
R1
vpn 0
interface 10ge0/0
ip address 10.50.0.2/29
no shutdown
!
lp route 0.0.0.0/0 10.50.0.3

R2
vpn 0
interface 10ge0/0
ip address 10.50.0.1/29
no shutdown
!
lp route 0.0.0.0/0 10.50.0.3
```

D.

```
R1
vpn 10
interface ge0/2
ip address 10.10.10.9/29
no shutdown
!
lp route 0.0.0.0/0 10.10.10.11

R2
vpn 10
interface ge0/2
ip address 10.10.10.10/29
no shutdown
!
lp route 0.0.0.0/0 10.10.10.11
```

正解: (正解を表示します)

質問: **206**

Cisco IOS XE SD-WANデバイスでプラグアンドプレイプロビジョニングを行うための2つの要件は何ですか？(2つ選択してください。)

A. 支店のデバイスは、本社にある Cisco SD-WAN vSmart コントローラにアクセスできる必要があります。

B. WAN Edge デバイスのゲートウェイ ルータは devicehelper.cisco.com にアクセスできる必要があります。
C. WAN Edge デバイスのゲートウェイ ルーターは、パブリック DNS サーバーにアクセスできる必要があります。
D. WAN Edge デバイスのゲートウェイ ルーターは、ztp.viptela.com に到達できる必要があります。
E. WANエッジデバイスには有効な証明書が必要です。
正解: **D,E** (コメントを発表する)
ztp.viptela.com: This is the Zero Touch Provisioning (ZTP) server that Cisco SD-WAN devices must reach during plug-and-play provisioning. ZTP automates the device onboarding process by fetching configuration and certificates from the vManage and vBond controllers.
Valid certificate: The WAN Edge device must have a valid certificate to authenticate itself with the Cisco SD-WAN controllers (vSmart, vBond, and vManage). Without this certificate, the device cannot join the SD-WAN fabric.

質問: **207**
SD-WANコントローラは、どのような2つの機能を提供しますか？(2つ選択してください。)
A. 認証管理
B. テンプレートを使用したデバイス構成管理
C. ポリシー管理(ポリシーの作成、管理、適用を含む)
D. ポリシー、ルーティング情報、暗号化キーの動的配布
E. ネットワーク全体におけるポリシーの適用
正解: (正解を表示します)
The SD-WAN Controller (vSmart) acts as the central control plane and dynamically distributes OMP routes, policies, and encryption keys to WAN Edge devices so that the overlay network can establish secure and optimal paths.
The controller is responsible for policy enforcement across the SD-WAN fabric, ensuring that centralized control policies are applied consistently throughout the network when routes and policies are distributed to WAN Edge routers.

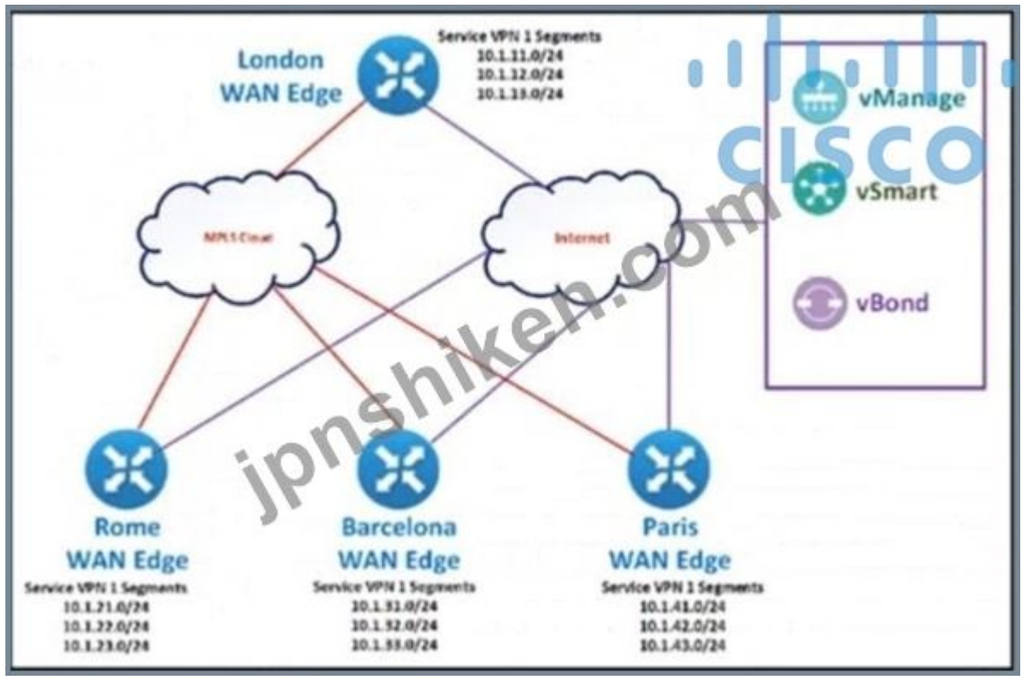
質問: **208**
ZTPプロセスが機能するために、WANエッジデバイスから到達可能なIPアドレスはどれである必要がありますか？
A. 4.4.4.4
B. 172.16.1.1
C. 8.8.8.8
D. 10.1.1.1
正解: (正解を表示します)
During the Zero Touch Provisioning (ZTP) process, the WAN Edge device must reach the IP address 4.4.4.4. This IP is often used as a placeholder to facilitate the initial connection and provisioning of the device, allowing it to download the necessary configuration files and firmware updates.

質問: **209**
VMware ESXiハイパーバイザーにvSmart Controllerをインストールした場合、デフォルトのユーザー名とパスワードは何ですか？
A. ユーザー名 admin パスワード admin
B. ユーザー名 admin パスワード cisco
C. ユーザー名 cisco パスワード admin
D. ユーザー名 cisco パスワード cisco
正解: (正解を表示します)
The default username and password for a vSmart Controller when it is installed on a VMware ESXi hypervisor typically follow the same default credentials used in the Cisco SD-WAN

environment. These default credentials are provided during the initial setup or installation of the vSmart Controller, and they are typically as follows:
Default Username: admin
Default Password: admin

質問**: 210**
SD-WAN Managerによって管理されるプラットフォームの組み合わせはどれですか？
A. ISR4351、ASR1009、vEdge2000、CSR1000v
B. ISR4351、ASR1002HX、vEdge2000、vEdge Cloud
C. ISR4321、ASR1001、ネクサス、ENCS
D. ISR4321、ASR1001、ENCS、ISRv
正解**: (**正解を表示します**)**
Cisco SD-WAN Manager (vManage) supports both vEdge (vEdge2000, vEdge Cloud) and IOS- XE SD-WAN-capable platforms like ISR4351 and ASR1002HX. These are officially supported SD-WAN devices that can be fully managed via SD-WAN Manager.

質問**: 211**
図を参照してください。SD-WANネットワークは、デフォルトのフルメッシュトポロジーで構成されています。SD-WANエンジニアは、バルセロナのWANエッジがローマサイトと通信する際に、優先TLOCとしてMPLS TLOCを使用するようにしたいと考えています。エンジニアは、ローマTLOCへのMPLSカラーを選択するリストを作成するために、どの構成を使用する必要がありますか？



jpnshiken.com

A.


Add Control Policy
Route
Create a policy to apply on a OMP

B.


Add Mesh Region
Name
Partial_Mesh
Description
Partial_Mesh
VPN List
ALL
Mesh Region Name
North
Site List
Spokes

C.





D.

正解: (正解を表示します)

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu **473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **212**

Cisco SD-WANソリューションでBGPやOSPFなどのルーティングプロトコルを担当するコンポーネントはどれですか？

A. vSmartコントローラー

B. vBond Orchestrator
C. vManage
D. WANエッジルーター
正解: (正解を表示します)
WAN Edge router - This router is responsible for running routing protocols, such as BGP and OSPF, to exchange routing information and make intelligent routing decisions. This enables efficient data forwarding within the SD-WAN network.

質問: **213**
どのデータ ポリシー構成が LAN から WAN への BGP ルーティング トラフィック フローに影響しますか?

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

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

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

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

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

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

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

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

正解: **D** (コメントを発表する)

The influence is from LAN to WAN not WAN to LAN. Therefore the policy is to be applied in the OUT direction.

質問: **214**

エンジニアは、インターネット接続が利用可能で、コントローラが本社にある2つのブランチWANエッジデバイスを設定する必要があります。要件は、同じ色のデバイス間でIPsec VPNトンネルを確立することです。どちらのWANエッジデバイスでも、この要件を満たす構成はどれですか？

A.

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
```

B.

WAN Edge 1

```
vpn 0
 interface ge0/0
  ip address 10.0.0.1/24
  ipv6 dhcp-client
  tunnel-interface
   color biz-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 default
   encapsulation ipsec
```

C.

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
```

D.

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
```

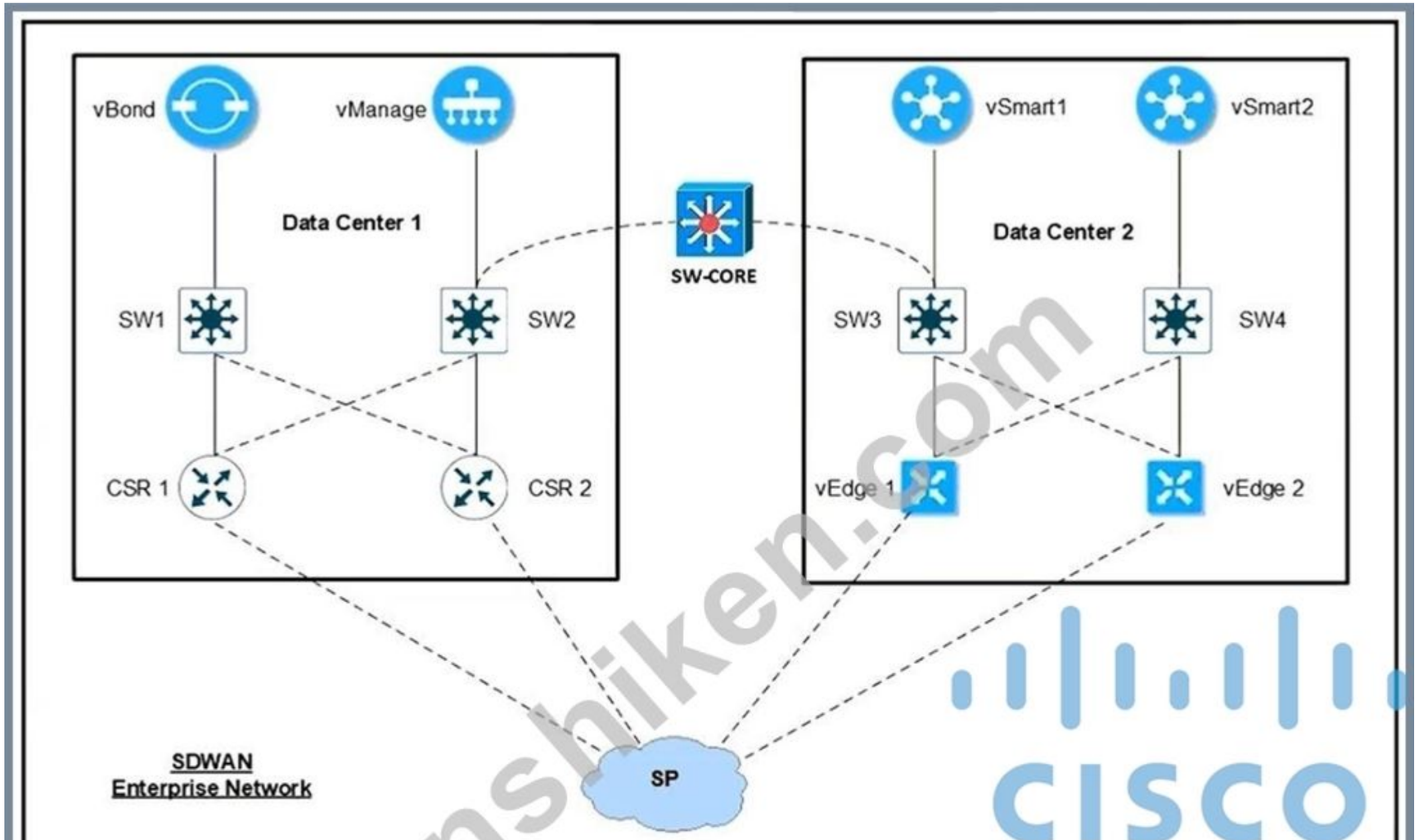
WAN Edge 2

```
vpn 0
 interface ge0/0
  ip address 10.0.0.2/24
  ipv6 dhcp-client
  tunnel-interface
   color gold restrict
   encapsulation ipsec
```

正解: **A** (コメントを発表する)

質問: **215**

図を参照してください。SW-COREデバイスはデータセンター1のコントローラとデータセンター2を接続し、データセンター1のWANエッジには受信ACLが設定されています。Cisco Catalyst SD-WANコントローラのDTLS接続を復元するには、どのACL構成を使用すればよいでしょうか？




```
vSmart1# ping vManage
Ping in VPN 0
PING vManage (10.101.1.2) 56(84) bytes of data.
64 bytes from vManage (10.101.1.2): icmp_seq=1 ttl=60 time=11.2 ms
64 bytes from vManage (10.101.1.2): icmp_seq=2 ttl=60 time=10.0 ms

vSmart1# tools nping vpn 0 10.101.1.2 options "--udp -p 12346 -g 12346 --source-ip 10.102.1.2 --df --data-length 1300"
Nping in VPN 0

Starting Nping 0.7.60 ( https://nmap.org/nping ) at 2022-01-12 14:20 UTC
SENT (0.0173s) UDP 10.102.1.2:12346 > 10.101.1.2:12346 ttl=64 id=37742 iplen=1328
RCVD (0.2127s) ICMP [172.16.1.25 > 10.102.1.2 Communication administratively prohibited by filtering (type=3/
code=13) ] IP [ttl=253 id=359 iplen=56 ]
SENT (1.0178s) UDP 10.102.1.2:12346 > 10.101.1.2:12346 ttl=64 id=37742 iplen=1328
RCVD (1.0446s) ICMP [172.16.1.25 > 10.102.1.2 Communication administratively prohibited by filtering (type=3/
code=13) ] IP [ttl=253 id=360 iplen=56 ]
```

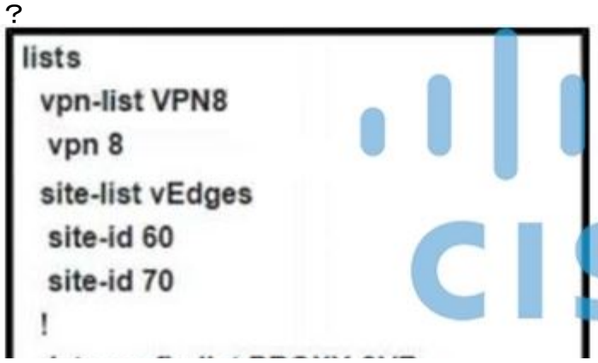
A. permit udp any eq 12346 any
TCP 任意の 23456 任意のポートを許可する
B. permit udp any eq 12446 any
tcp any eq 23556 any を許可します

C. udp 任意の範囲 12346 12446 を許可します
TCP 任意の範囲 23456 23556 を許可する
D. udp 任意の範囲 12346 12446 を許可します
TCP 任意の範囲 23456 23756 を許可する
正解: **(**正解を表示します**)**
DTLS (used for control connections in SD-WAN) communicates over UDP port 12346, while TCP port 23456 is used for TLS control connections.
The Communication administratively prohibited by filtering message in the output confirms that an ACL is blocking these ports.
Allowing UDP 12346 and TCP 23456 restores required SD-WAN controller connectivity.

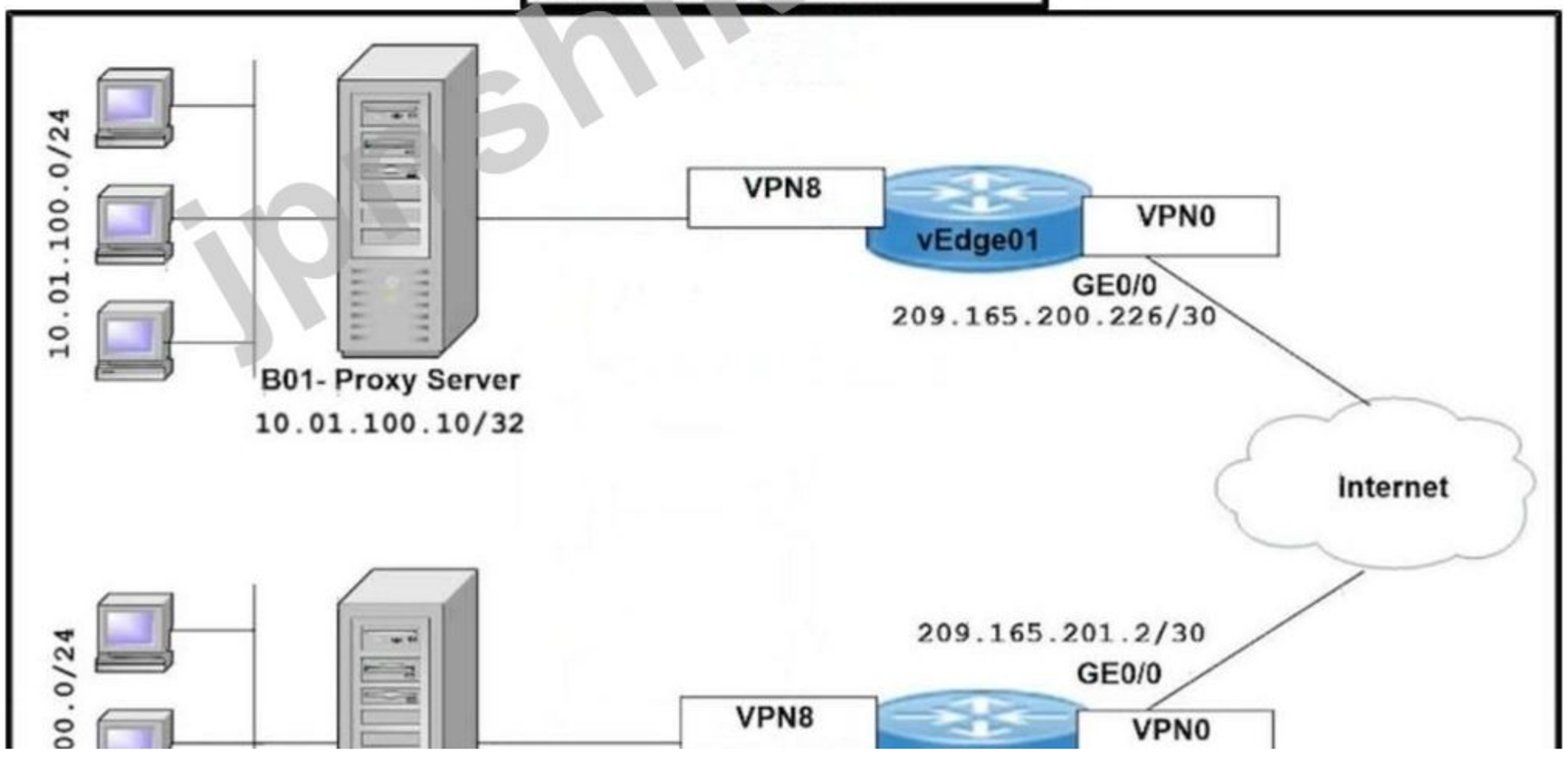
質問: **216**
Cisco SD-WANを導入していないものの、自社サイトにSD-WANルーティングアプライアンスを設置することなく顧客との接続が必要なパートナーやベンダーが利用するCloud OnRampソリューションはどれですか？
A. IaaS向けクラウドオンランプ
B. マルチクラウド向けクラウドオンランプ
C. コロケーション向けクラウドオンランプ
D. SaaS向けクラウドオンランプ
正解: **C (**コメントを発表する**)**
Cloud OnRamp for Colocation is designed for partners and vendors who do not have Cisco SD-WAN appliances but still need to connect to their customers without installing SD-WAN routing appliances at their own sites. This solution allows third-party providers to colocate SD- WAN virtual appliances in shared data centers, enabling connectivity to customer sites via SD- WAN without deploying SD-WAN hardware directly at the partner's or vendor's location.

質問: **217**
Cisco TrustSecがサポートするSGT伝播方式は、次のうちどれですか？(2つ選択してください。)
A. インラインタグ付け
B. 和解
C. SXP
D. キーホルダー
E. オフラインタグ付け
正解: **(**正解を表示します**)**

質問: **218**
図を参照してください。エンジニアが、集中型データポリシーを使用して、1つのプロキシサーバーからのインターネットアクセスのみを許可して、支店でのインターネットアクセスを構成しています。どのコマンドで構成が完了しますか？



```
 data-prefix-list PROXY-SVR
  ip-prefix 10.01.100.10/32
  ip-prefix 10.02.100.10/32
 !
!
data-policy DATA-POLICY-TO-vEdges
 vpn-list VPN8
  sequence 11
   match
    source-data-prefix-list PROXY-SVR
   !
   action accept
    nat use-vpn 0
     count TRAFFIC-FROM-PROXY-SVR
   !
  !
  default-action accept
 !
apply-policy
 site-list vEdges
```



ipmshken.com



A. データポリシー DATA-POLICY-TO-vEdges from-service
B. データポリシー TRAFFIC-FROM-PROXY-SVR from-service
C. app-route-policy DATA-POLICY-TO-vEdges
D. app-route-policy TRAFFIC-FROM-PROXY-SVR
正解: **A (**コメントを発表する**)**
The configuration in the exhibit shows a data policy named DATA-POLICY-TO-vEdgesthat matches traffic from specified proxy servers (defined in the data-prefix-list PROXY-SVR) and applies NAT within VPN 0 to direct the traffic to the internet. To complete this configuration and ensure that it is applied to the traffic coming from the proxy servers, the command data- policy DATA-POLICY-TO-vEdges from-serviceshould be used. This command applies the data policy in the outbound direction to allow the defined traffic to reach the internet.

質問: **219**
エンジニアは、vSmartコントローラを設定して、初期段階の最適ではないルートセットをvEdgeルータに送信するようにしています。オーバーレイ管理プロトコルで、この要件を満たすために必要な設定コマンドはどれですか？
A. バックアップパスを送信
B. send-path-limit 10
C. コントローラー送信パス制限 10
D. バックアップパスを送信
正解: **A (**コメントを発表する**)**
The send-backup-paths command under OMP configuration on the vSmart controller enables it to advertise non-best (backup) routes to vEdge routers. This allows the vEdge to have standby paths ready for failover or application-aware routing decisions. It is essential for ensuring resiliency and optimizing path selection.

質問: **220**
Cisco SD-WANマルチリージョンファブリックは、どのような機能を提供しますか？
A. IPマルチキャストのオーバーレイサポート
B. 地域間トラフィックのエンドツーエンド暗号化
C. 領域0と非コア領域を処理するための単一のvSmartコントローラの割り当て
D. エンドツーエンドのSLA対応ルーティング
正解: **(**正解を表示します**)**

質問: **221**
DNSクエリ内のFQDNがグレーリストに登録されているドメインのいずれかである場合、Cisco Umbrellaはクライアントに対してどのように応答しますか？
A. コンテンツプロバイダのIPアドレスを返します。
B. インテリジェントプロキシのユニキャストIPアドレスを返します。
C. ブロックされたランディングページのIPアドレスを返します。
D. 応答が送信されません。トラフィックがブロックされています。

正解: **B** (コメントを発表する)
When a DNS query is made for a grey-listed domain (a domain that is potentially suspicious but not definitively malicious), Cisco Umbrella responds with the IP address of its intelligent proxy. This approach allows Cisco Umbrella to proxy the traffic and monitor the connection more closely, providing additional filtering and inspection without outright blocking the domain. This enables Cisco Umbrella to make a more informed decision about allowing or blocking the traffic based on real-time analysis.

質問: **222**
図を参照してください。管理者は、TACACS+サー バーにアクセスできなくなった場合でも、デバイスに設定された認証情報を使用してユーザーが認証されるようにルーターを設定します。
このタスクを達成するには、どの構成が適切でしょうか？

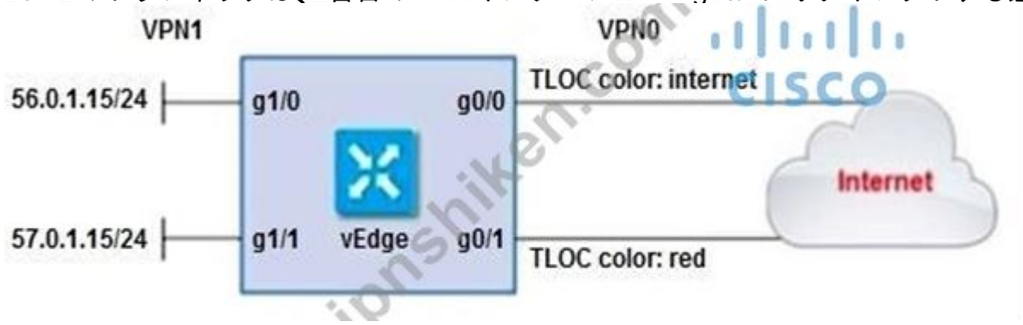


A. aaa 認証ログインデフォルトグループ CISCO-TACACS if-authenticated
B. aaa 認証ログインデフォルトグループ CISCO-TACACS 有効化
C. aaa 認証ログイン デフォルト ローカル
D. aaa 認証ログインデフォルトグループCISCO-TACACSローカル
正解: (正解を表示します)
The AAA authentication method list determines the order of authentication mechanisms. Using group CISCO-TACACS local instructs the router to first attempt authentication with the TACACS + server group. If the TACACS+ server becomes unreachable, the router falls back to the local user database configured on the device. This ensures administrators can still authenticate using locally configured credentials when the TACACS+ server is unavailable.

質問: **223**
ネットワーク管理者がvEdge 5000ルーターでQoSを設定しており、トランスポート側のインターフェースでQoSを有効にする必要があります。
この目標を達成するには、どの政策設定を選択すべきでしょうか？
A. アプリケーション
B. ネットフロー
C. クラウドQoSサービス側
D. クラウドQoS
正解: (正解を表示します)
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/configcmd.html#wp6721725270
policy cloud-qos-Enable QoS scheduling and shaping for traffic on WAN interfaces (applicable to Cisco vEdge Cloud, Cisco vEdge 5000, and Cisco ISR1100 routers).
policy cloud-qos-service-side-Use this command along with the policy cloud-qos command to enable QoS scheduling and shaping for traffic on LAN interfaces (applicable to Cisco vEdge Cloud, Cisco vEdge 5000, and Cisco ISR1100 routers).

質問: **224**

図を参照してください。ge0/0インターフェースは30MBのリンクに接続されています。ネットワーク管理者は、優先度の高いトラフィック用に常に10MBの帯域幅を確保したいと考えています。優先度の低いトラフィックのバーストが10MBを超えると、
20MBのトラフィックは、2番目のWANインターフェースge0/1にリダイレクトする必要があります。



このタスクを達成するには、どの設定の組み合わせが適切ですか？

```
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
```

A.

```
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
```

B.

C.
```
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
```

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

正解: **A** (コメントを発表する)

```
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
```

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

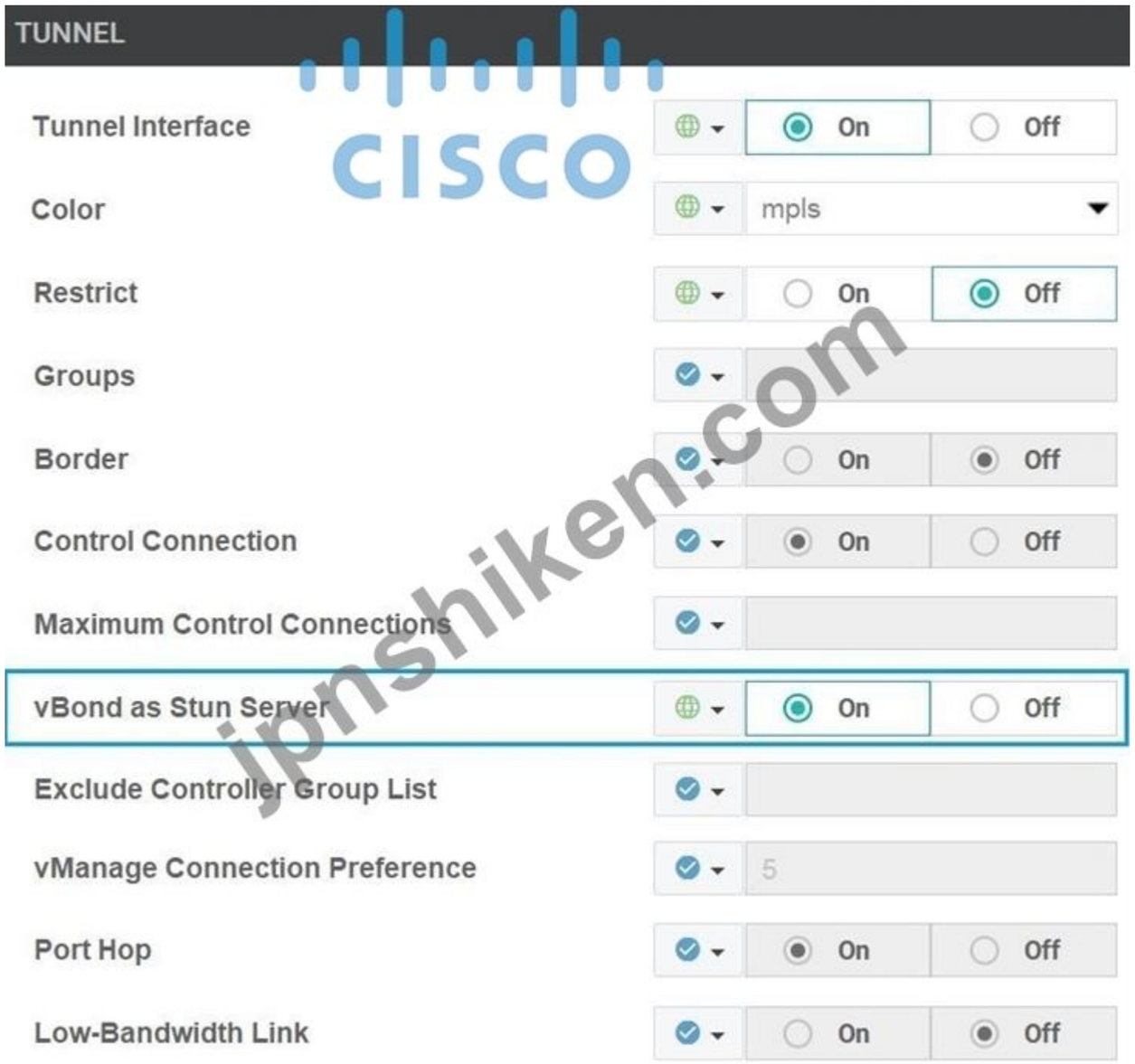
質問: **225**

エンジニアは、WAN エッジ ルータでのコンバージェンスのために、制御トラフィックと BFD トラフィック用にどのキューを設定する必要がありますか?

A. キュー 0
B. キュー1
C. キュー2
D. キュー7
正解: **(**正解を表示します**)**
Queue 0 is always configured as a low-latency queue and is the only queue that supports Low Latency Queuing. Additionally, all control traffic that is originated by the WAN Edge router, including DTLS/TLS, BFD probes, and rout-ing protocol traffic, is automatically mapped to queue
0.

質問: **226**
E社は、AWS上にコントローラを設置したCisco SD-WANを導入したいと考えています。同社の既存のWANはプライベートMPLS回線で、AWS上のコントローラへのインターネットアクセスはありません。既存のMPLS回線に加えて、サイトにインターネット回線が追加されます。
どのインターフェーステンプレートが、両方のトランスポート上でBFDネイバーを確立しますか？

A.



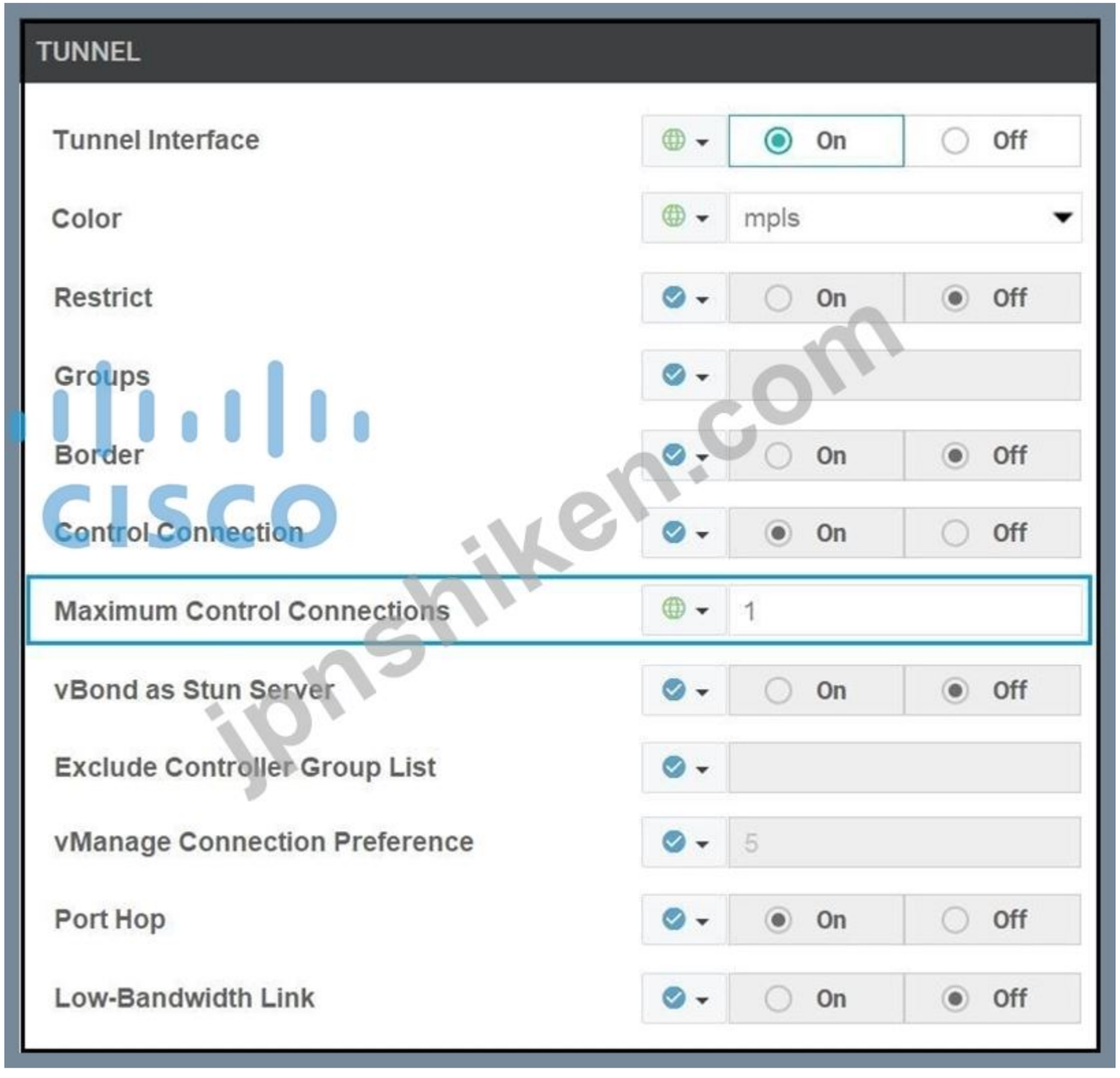
jpnshiken.com

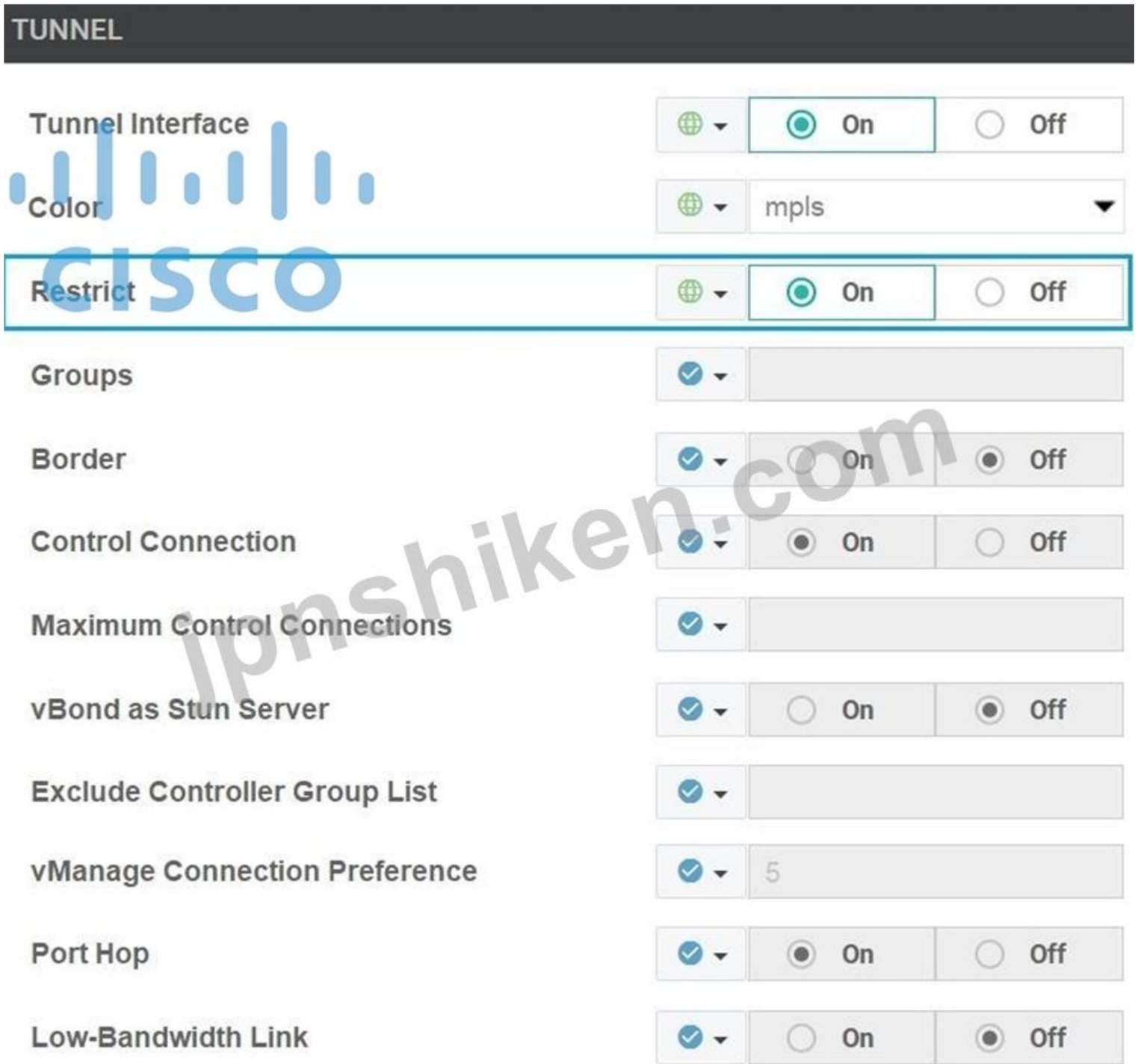
B.



jpnshiken.com

C.


TUNNEL
Tunnel Interface
On
Off
Color
mpls
Restrict
On
Off
Groups
Border
On
Off
Control Connection
On
Off
Maximum Control Connections
1
vBond as Stun Server
On
Off
Exclude Controller Group List
vManage Connection Preference
5
Port Hop
On
Off
Low-Bandwidth Link
On
Off



D.

正解: (正解を表示します)

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **227**
マルチキャストネットワークを介して有効になるマルチキャスト配信ツリーを最適化するために使用されるコンポーネントはどれですか？
A. OMPレプリケーター
B. vManageコントローラー
C. VPNコンセントレータ
D. IGMPクライアント
正解: **(**正解を表示します**)**
The OMP replicator is used in overlay multicast to optimize the multicast distribution tree across the overlay topology.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing- book-xe/m-multicast-routing.html

質問: **228**
vRouteのタイプを識別する属性はどれですか？
A. 発信者
B. タグ
C. 起源
D. カプセル化
正解: **(**正解を表示します**)**
Triggers to TLOC Disabled messages can be due to these probable causes:
Clear Control Connections.
Change the color on TLOC.
Change in the System IP.
https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control- connections.html

質問: **229**
Cisco Plug and Play Connectプロセスを通じてオンプレミスのvBondコントローラを導入するための要件は何ですか？
A. vBondを識別するDNS名
B. 定義済みのコントローラプロファイル
C. すべてのコントローラーを含むCSVファイル
D. vManageからのインターネット接続
正解: **A (**コメントを発表する**)**

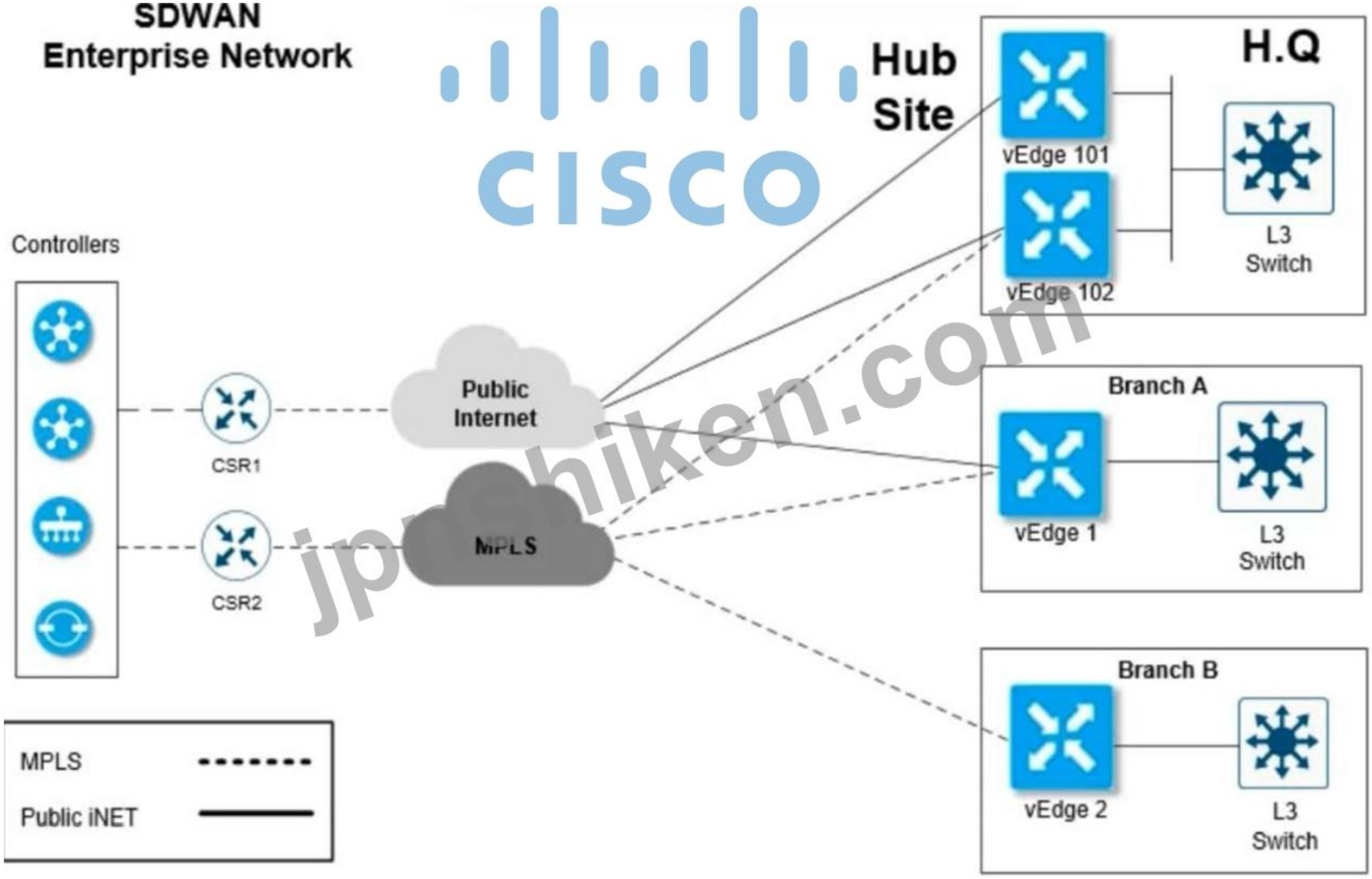
質問: **230**
vBond Orchestratorの冗長トポロジーで使用される重要な要素は何ですか？
A. ヘルスプローブを備えたロードバランサー
B. 完全修飾ドメイン名
C. スタンサーバー
D. DHCPサーバー
正解: **B (**コメントを発表する**)**

質問: **231**
どのCisco SD-WANコンポーネントがポリシー設定を一元管理しますか？

A. WANエッジ
B. vSmart
C. シスコDNAセンター
D. vBond
正解: **B (**コメントを発表する**)**

質問: **232**
ISRプラットフォームにおけるCisco SD-WAN認証プロセスに関与するハードウェアコンポーネントはどれですか？
A. ZTP
B. OTPC
C. SUDI
D. TPMD
正解: **(**正解を表示します**)**
The hardware component involved in the Cisco SD-WAN authentication process for ISR (Integrated Services Router) platforms is the SUDI (Signed Unique Device Identifier).
SUDI is a mechanism used for device authentication and is often employed in Cisco SD-WAN deployments. It helps verify the authenticity of the device and is part of the secure onboarding process.

質問: **233**
図を参照してください。ユーザーは、ビデオ通話中に直接通信するために、ブランチAとブランチBの間にトンネルを確立します。通話終了後、トンネルは切断されなければなりません。この要件を満たすために、スポークに適用する必要がある2つの構成はどれですか？(2つ選択してください。)



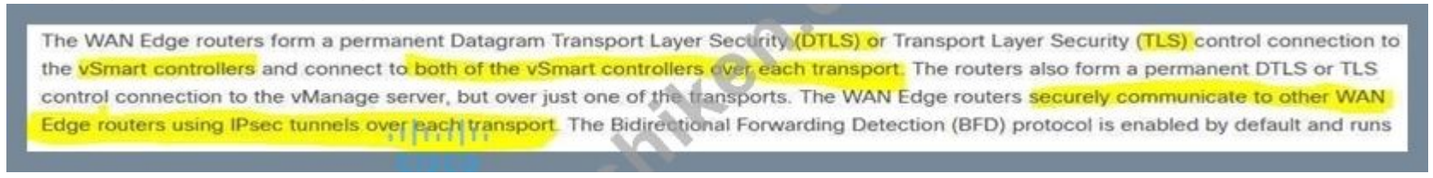
ipcisshiken.com

A. VPN 0
TEサービス
B. システム
オンデマンドアイドルタイムアウト 10
C. システム
オンデマンドで有効化
D. omp

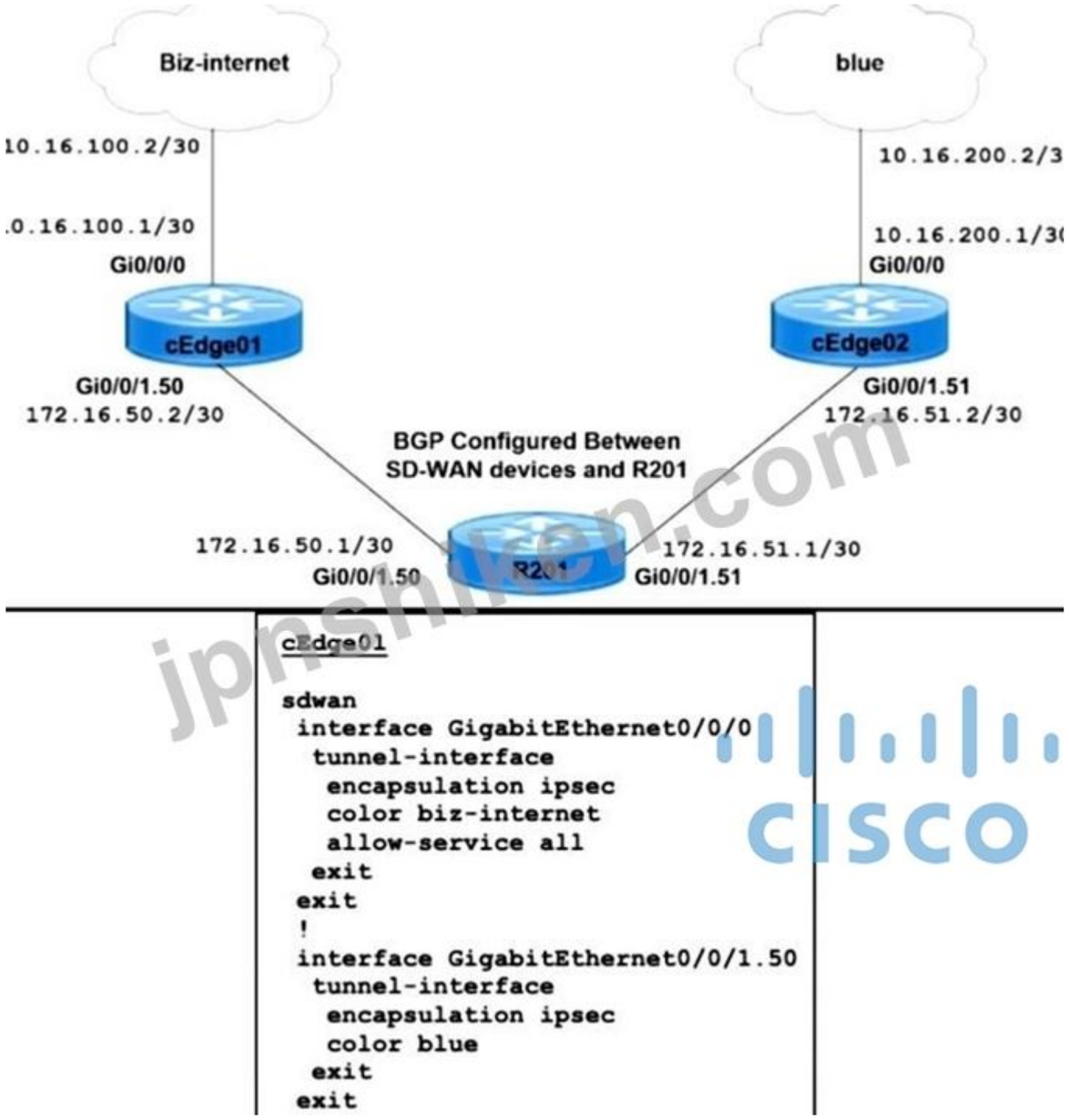
ecmp制限 16
E. omp
send-path-limit 16
正解: **(**正解を表示します**)**

質問: **234**
Cisco SD-WANのどの構成が、導入初日からの展開と再利用可能な構成コンポーネントという利点を提供しますか？
A. Cisco Primeサーバーを介した設定
B. 構成グループ
C. vBondコントローラによる設定
D. CLIベースのテンプレート
正解: **(**正解を表示します**)**

質問: **235**
ネットワーク管理者が、ブランチ接続用にWANエッジルータを1台起動しています。WANエッジルータがCisco SD-WANファブリックに接続すると、どのような種類のトンネルが形成されますか？
A. vBondコントローラを使用したDTLSまたはTLSトンネル、およびvManageコントローラを使用したIPsecトンネル。
B. vBondコントローラとのDTLSまたはTLSトンネル、および他のWANエッジルータとのIPsecトンネル。
C. vSmartコントローラとのDTLSまたはTLSトンネル、および他のエッジルーターとのIPsecトンネル。
D. vSmartコントローラを使用したDTLSまたはTLSトンネル、およびvBondコントローラを使用したIPsecトンネル。
正解: **C (**コメントを発表する**)**



質問: **236**
図を参照してください。トランスポート冗長性を確保するために、cEdge01ルータのSD-WANインターフェイスGigabitEthernet0/0/1.50にどの設定を適用する必要がありますか？



A. sdwan
インターフェース GigabitEthernet0/0/1.50
トンネルインターフェース
tloc-extension-gre-to 172.16.50.1
出口
出口

B. sdwan
インターフェース GigabitEthernet0/0/1.50
トンネルインターフェース
tloc-extension-gre-to 172.16.51.2
出口

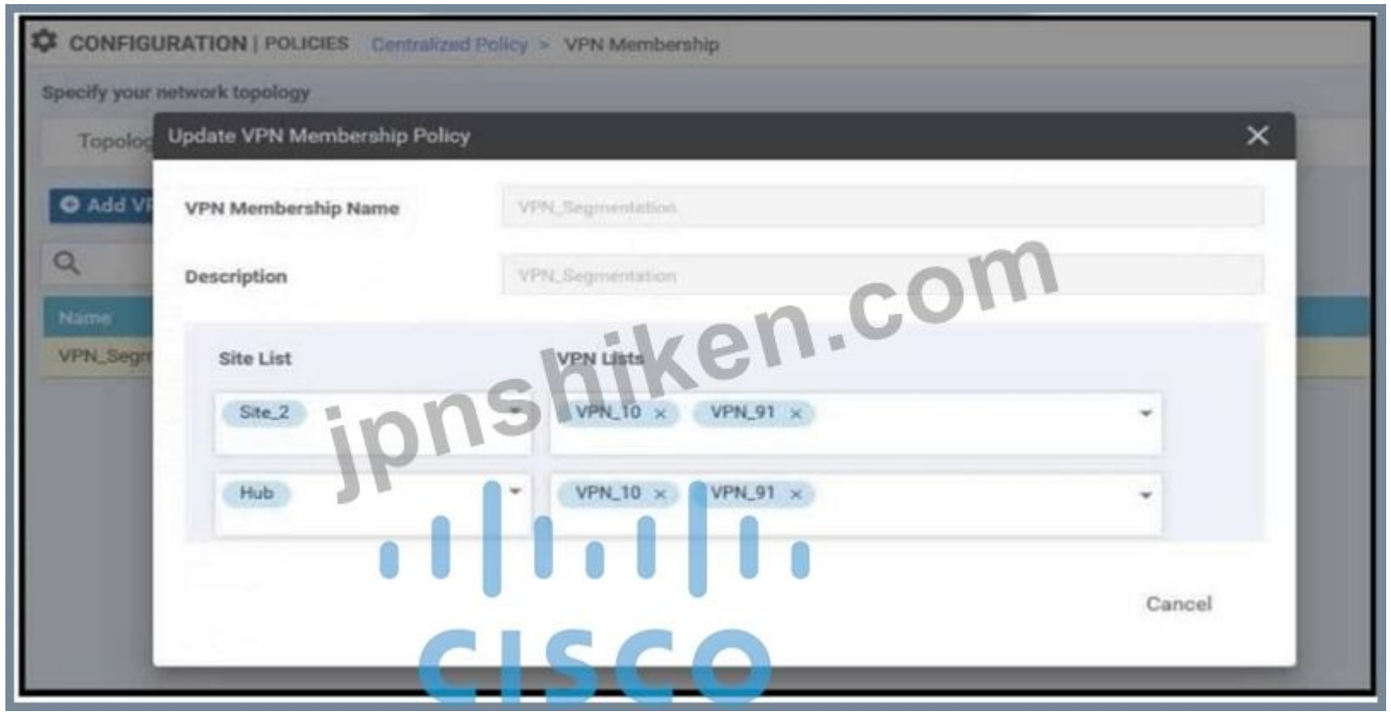
出口
C. sdwan
インターフェース GigabitEthernet0/0/1.50
トンネルインターフェース
すべてのサービスを許可する
出口
出口
D. sdwan
インターフェース GigabitEthernet0/0/1.50
トンネルインターフェース
tloc拡張機能 GigabitEthernet0/0/0
出口
出口
正解: (正解を表示します)
In Cisco Catalyst SD-WAN, transport redundancy between two WAN Edge routers connected through a LAN is implemented using TLOC extension, not GRE. GRE TLOC extension is used in specific designs when a non-SD-WAN device is in the path. In this topology, the extension is between two SD-WAN interfaces on the same router, so the correct mechanism is the standard TLOC extension command referencing the WAN interface.
The WAN transport on cEdge01 is:
GigabitEthernet0/0/0
color biz-internet
The LAN-facing subinterface GigabitEthernet0/0/1.50 connects to R201. To allow this interface to use the WAN transport and provide redundancy, the configuration must extend the TLOC to the WAN interface:
sdwan
interface GigabitEthernet0/0/1.50
tunnel-interface
tloc-extension GigabitEthernet0/0/0
This allows the router to share the transport of Gi0/0/0, enabling redundant SD-WAN tunnels.

質問: **237**
VPNをグループ化して宛先ゾーンを作成する場合、1つのVPNはいくつのゾーンに属することができますか？
A. 2つ
B. 4つ
C. 1つ
D. 3つ
正解: (正解を表示します)
https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/Enterprise_Fi rewall_with_Application_Awareness

質問: **238**
拡張性と冗長性を実現するために、各ドメインにいくつのvManage NMSをインストールする必要がありますか？
A. 2つのクラスター

B. 2 つのインスタンス
C. クラスター内の2つ以上
D. クラスター内に3つ以上
正解: **D** (コメントを発表する)
A highly available Cisco SD-WAN network contains three or more vManage NMSs in each domain. This scenario is referred to as a cluster of vManage NMSs, and each vManage NMS in a cluster is referred to as a vManage instance. Each vManage instance or device in a cluster can manage approximately 2000 devices, so a cluster of three vManage devices can manage up to 6000 devices. The vManage devices automatically load-balances the devices that they manage.
With three devices, the vManage cluster remains operational if one of the devices in that cluster fail.

質問: **239**
図を参照してください。ある企業は、複数のVPNを持つハブアンドスポーク型のトポロジーを採用しています。エンジニアは、VPN91のユーザーがVPN92のユーザーにアクセスできるようにし、VPN10がVPN91とVPN92の両方にアクセスできるようにする必要があります。これらの要件を満たす構成はどれですか？

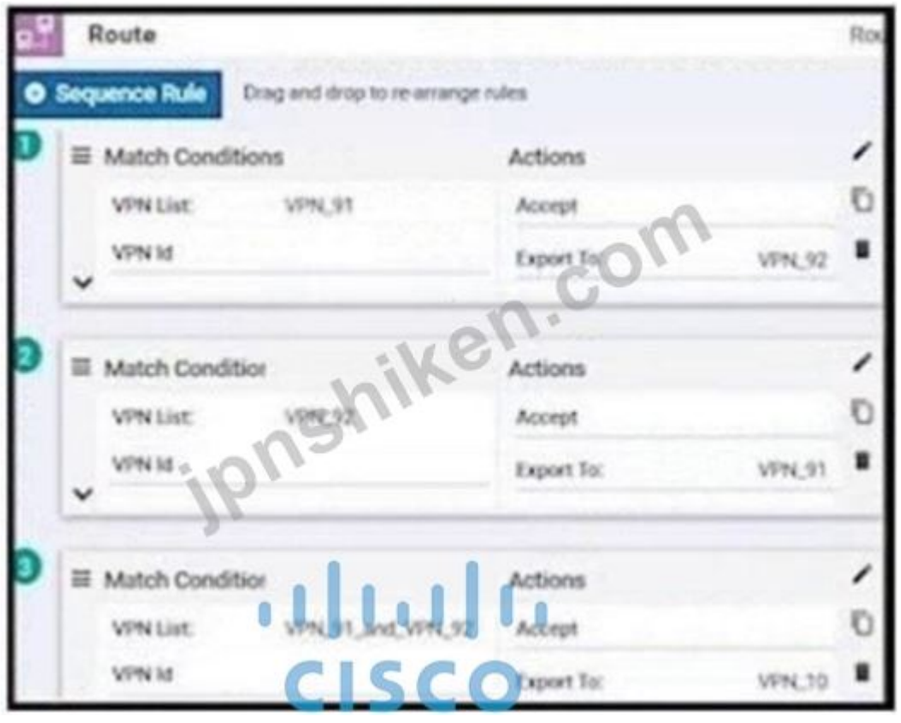


jpnshiken.com
CISCO

A.


Route
Sequence Rule
Drag and drop to re-arrange rules
Match Conditions
Actions
VPN List: VPN_10
VPN Id
Accept
Export To: VPN_91_and_VPN_92
Match Conditions
Actions
VPN List: VPN_91_and_VPN_92
VPN Id
Accept
Export To: VPN_91_and_VPN_92
Match Conditions
Actions
VPN List: VPN_91_and_VPN_92
VPN Id
Accept
Export To: VPN_10

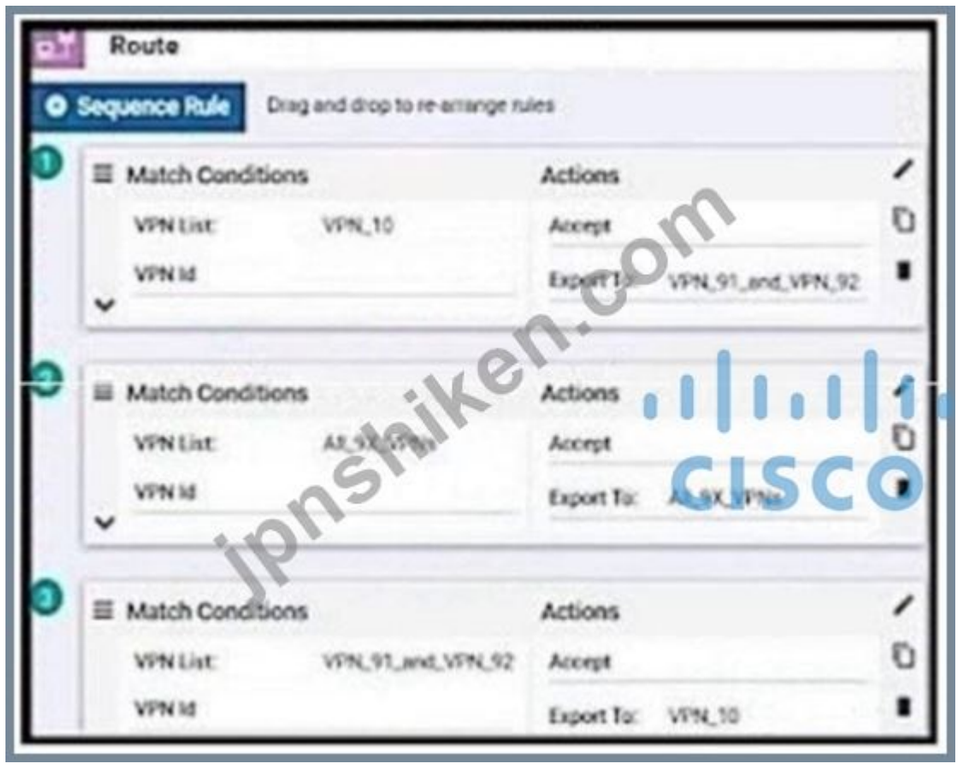
B.


Route
Sequence Rule
Drag and drop to re-arrange rules
Match Conditions
Actions
VPN List: VPN_91
VPN Id
Accept
Export To: VPN_92
Match Conditior
Actions
VPN List:
VPN Id
Accept
Export To: VPN_91
Match Conditior
Actions
VPN List:
VPN Id
Accept
Export To: VPN_10

C.



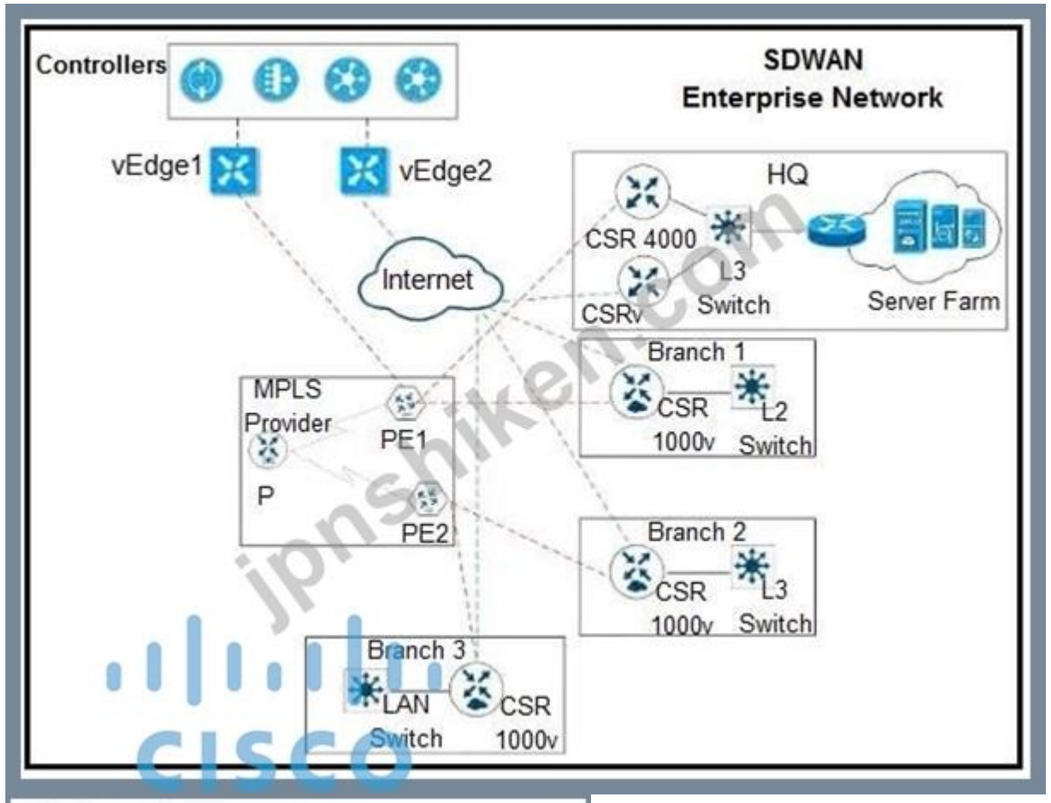
jpnshiken.com

D. 

正解: **A** (コメントを発表する)

質問: 240

図を参照してください。ネットワークチームは、本社でEIGRPピアリングを設定し、WANエッジCSRvに接続されたサービスVPN内のデバイスと接続する必要があります。CSRvは現在、以下のように設定されています。




```
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
```

WANエッジのどの構成が要件を満たしますか？

A.

```
vpn 0
 router
  eigrp
   address-family ipv4-unicast
    maximum-path paths 4
    network 10.0.0.0/28
    redistribute omp

interface ge0/0
   description "***Internet Circuit***"
   ip address 209.165.200.229/30
   tunnel-interface
    encapsulation ipsec
    color public-internet
    allow-service all

vpn 512
interface eth0
  shutdown
```

B.

```
vpn0
interface ge0/0
   description "***Internet Circuit***"
   ip address 209.165.200.229/30
   tunnel-interface
    encapsulation ipsec
    color public-internet
    allow-service all

router
  eigrp
   address-family ipv4-unicast
    maximum-path paths 4
    network 10.0.0.0/28
    redistribute omp


vpn 512
interface eth0
 shutdown
```

```
vpn0
vpn1
interface ge0/0
  description "***Internet Circuit***"
  ip address 209.165.200.229/30
  tunnel-interface
   encapsulation ipsec
   color public-internet
   allow-service all

router
 eigrp
  address-family ipv4-unicast
   maximum-path paths 4
   network 10.0.0.0/28
   redistribute omp

interface ge0/1
 ip address 10.0.0.1/28

vpn 512
interface eth0
 shutdown
```

C.

正解: **A** (コメントを発表する)

質問: **241**

vEdgeプラットフォームが10秒ごとにVRRPアドバタイズメントメッセージを送信しています。ルーターをデフォルトのタイマーに戻すには、どの値を設定すると良いでしょうか？

A. 2秒

B. 5秒

C. 1秒

D. 3秒

正解: **C** (コメントを発表する)

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

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu　**473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **242**

エンジニアがWANエッジルーターのWANリンク上で、1Mbpsのシェーピングレートを設定している。

このタスクを達成するには、どの構成が適切でしょうか？

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
```

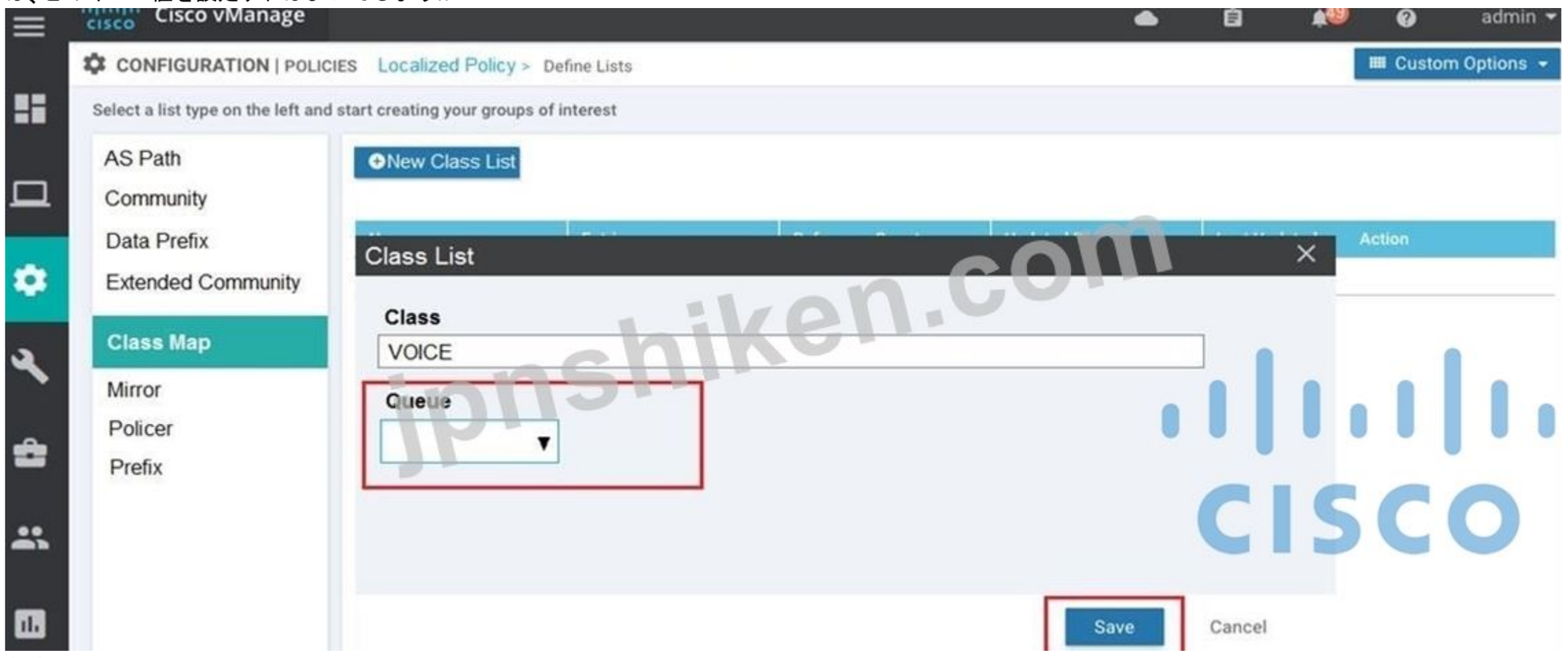
正解: (正解を表示します)

Shaping rates are configured in Kbps. 1 Mbps = 1000 Kbps

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/qos/ios-xe-17/qos-book- xe/per-vpn-qos.html

質問: **243**

図を参照してください。ネットワーク管理者が、vManager GUIを使用して、WANエッジルータの1つにおける音声トラフィックのキューイング値を設定しています。このタスクを実行するには、どのキュー値を設定すればよいでしょうか？



A. 0

B. 1
C. 2
D. 3
正解: **A (**コメントを発表する**)**
https://www.cisco.com/c/en/us/support/docs/routers/vedge-router/213408-implement-qos-in- cisco-sd-wan.html

質問: **244**
アプリケーションファイアウォールが提供する2つの機能はどれですか？ （2つ選択してください。）
A. 1400以上のレイヤー7アプリケーションの分類
B. アプリケーションまたはアプリケーションファミリによってトラフィックをブロックします
C. マッチアクションペアの番号付きシーケンス
D. 1000以上のレイヤー4アプリケーションの分類
E. アプリケーション一致パラメーター
正解: **(**正解を表示します**)**
The application firewall in Cisco SD-WAN provides the following features:
- Blocks traffic by application or application-family: The application firewall allows you to define policies that block or permit traffic based on specific applications or application families. This enables granular control over the types of traffic that are allowed or denied.
- Classification of 1400+ layer 7 applications: The application firewall classifies a wide range of layer 7 (application layer) applications, which allows you to create policies based on specific applications and their characteristics. This extensive classification database provides detailed application awareness for traffic management and security.

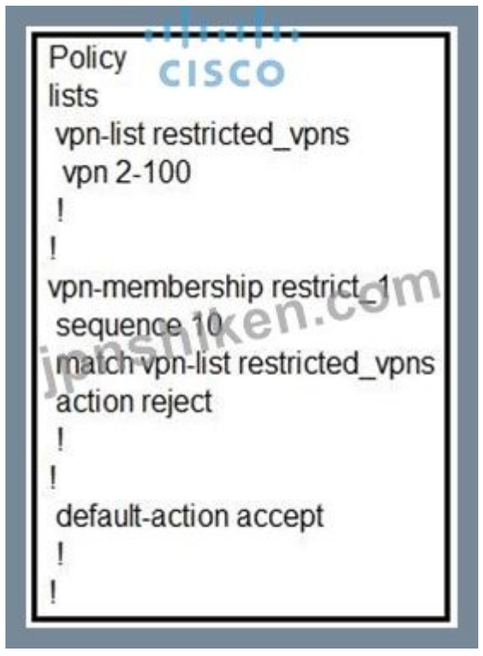
質問: **245**
「設定」＞「ポリシー」で、アプリケーション対応ルーティングポリシーを設定するポリシーはどれですか？
A. データポリシー
B. 中央集権的なポリシー
C. ローカライズされたポリシー
D. 制御ポリシー
正解: **B (**コメントを発表する**)**
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies- book/application-aware-routing.html
"An application-aware routing policy is a type of centralized data policy: you configure it on the vSmart controller, and the controller automatically pushes it to the affected Cisco SD-WAN devices".

質問: **246**
パケットの複製にはどのような利点がありますか？
A. パケットデータポリシー保護
B. セッションセキュリティ
C. パケット損失に対する保護
D. フレーム損失の防止
正解: **(**正解を表示します**)**
Packet duplication in Cisco SD-WAN sends duplicate packets over multiple paths to ensure delivery even if one path experiences loss. This enhances application reliability by mitigating the impact of packet loss, particularly for real-time or mission-critical traffic.

質問: **247**
Cisco SD-WAN Edge デバイスにセキュアインターネットゲートウェイ (SIG) を統合する要件を説明しているのは、次のうちどれですか？
A. ルーティングまたはポリシーに基づいて、すべての顧客インターネットトラフィックはSIGに転送する必要があります。
B. スマートアカウントの認証情報が必要です。
C. SIGを設立するには、Ciscoの傘下組織IDが必要です。
D. SIGトンネルに接続されたトラッカーは、それぞれのSIGエンドポイントを監視します。
正解: (正解を表示します)
When integrating a Secure Internet Gateway (SIG), such as Cisco Umbrella, with a Cisco SD- WAN Edge device, a Cisco Umbrella organization ID is required. This organization ID is used to authenticate and establish the connection between the SD-WAN Edge device and Cisco Umbrella's SIG services.

質問: **248**
WANエッジルーターの設定において、TLOC拡張機能を使用する主な目的は何ですか？
A. リモートサイトのWANエッジルーターに制御トラフィックを転送します
B. WAN EdgeからvBond OrchestratorへのIPsecトンネルを作成します
C. ローカルサイトでハードウェアレベルのトランスポート冗長性を作成します
D. 冗長vSmartコントローラに制御トラフィックを転送します
正解: (正解を表示します)
TLOC extensions allow a WAN Edge router to communicate over the WAN transport connected to the adjacent WAN Edge router through a TLOC-extension interface. This provides redundancy in case one of the WAN transports fails.

質問: **249**
顧客は 1 ～ 100 のサービス VPN を所有しており、VPN1 のアウトバウンド更新を制限したいと考えています。これらの更新を制限する制御ポリシー構成はどれですか。



A.
```
policy
lists
 vpn-list VPN2-100
  vpn 2-100
 !
!
control-policy restrict_2-100
sequence 10
 match route
  vpn-list VPN2-100
 !
 action reject
!
 default-action accept
```

B.
```
policy
lists
 vpn-list VPN1
  vpn 1
 !
!
control-policy restrict_1
 sequence 10
  match route
  vpn-list VPN1
 !
 action reject
!
 default-action accept
```

C.
```
Policy
lists
 vpn-list restricted_vpns
  vpn 1
 !
!
vpn-membership restrict_1
sequence 100
  match vpn-list restricted_vpns
  action reject
  !
 !
default-action accept
 !
!
```

D.

正解: (正解を表示します)
The configuration references VPN 1 to be matched and the action to reject traffic.
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies- book/centralized-policy.html

質問: **250**
図を参照してください。リスナーソケットFDエラー(LISFD)による制御接続障害を示しているのは、どの問題ですか？

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	LOCAL COLOR	PEER LOCAL STATE	REMOTE ERROR	REPEAT ERROR	COUNT
vbond	dtls	-	0	0	203.0.113.21	12346	203.0.113.21	12346	defaul	up	LISFD	NOERR	0

A. WANエッジでのメモリの問題
B. 最大伝送単位の不一致
C. 証明書エラー
D. 重複したトランスポートIP
正解: (正解を表示します)
A listener socket FD (file descriptor) error occurs when two WAN Edge devices attempt to use the same transport IP address on the same interface. This causes the socket to fail, preventing control connections from establishing. The issue is directly tied to duplicate transport IPs.

質問: **251**
エンジニアは、サイト グループに対してアプリケーション対応ルーティング ポリシーを構成します。場所は、パブリック トランスポートとプライベート トランスポートに依存します。トランスポートの 1 つが正常に動作しない場合、ポリシーは期待どおりに機能しません。このポリシーは次のように構成されます。

```
policy
 sla-class BULK_DATA
  loss   20
  latency 300
  jitter  100
 !
 sla-class TRANSACTIONAL_DATA
  loss   15
  latency 50
  jitter  100
 !
 sla-class REALTIME
  loss   20
  latency 100
  jitter  30
 !
 app-route-policy VPN-10_MPLS_AND_INET_SITES
  vpn-list VPN-10
   sequence 1
    match
     dscp 46
    !
    action
     backup-sla-preferred-color biz-internet
     sla-class REALTIME preferred-color private1
    !
   !
   sequence 11
    match
     dscp 34
    !
    action
     backup-sla-preferred-color biz-internet
     sla-class TRANSACTIONAL_DATA preferred-color private1
    !
   !
   sequence 21
    match
     dscp 24
    !
    action
     backup-sla-preferred-color biz-internet
     sla-class TRANSACTIONAL_DATA preferred-color private1
    !
   !
  !
 !
```

どの構成でポリシーが完成し、すべての場所で機能するようになりますか?

A.

```
sla-class TRANSACTIONAL_DATA
 loss   2
 latency 100
 jitter  30
!
sla-class REALTIME
 loss   15
 latency 100
 jitter  100
!
```

B.
```
sla-class BULK_DATA
 loss   10
 latency 300
 jitter  100
!
sla-class REALTIME
 loss    2
 latency 100
 jitter  30
!
```

C.
```
sla-class BULK_DATA
 loss    15
 latency 100
 jitter  100
!
sla-class TRANSACTIONAL_DATA
 loss    10
 latency 300
 jitter  100
!
```

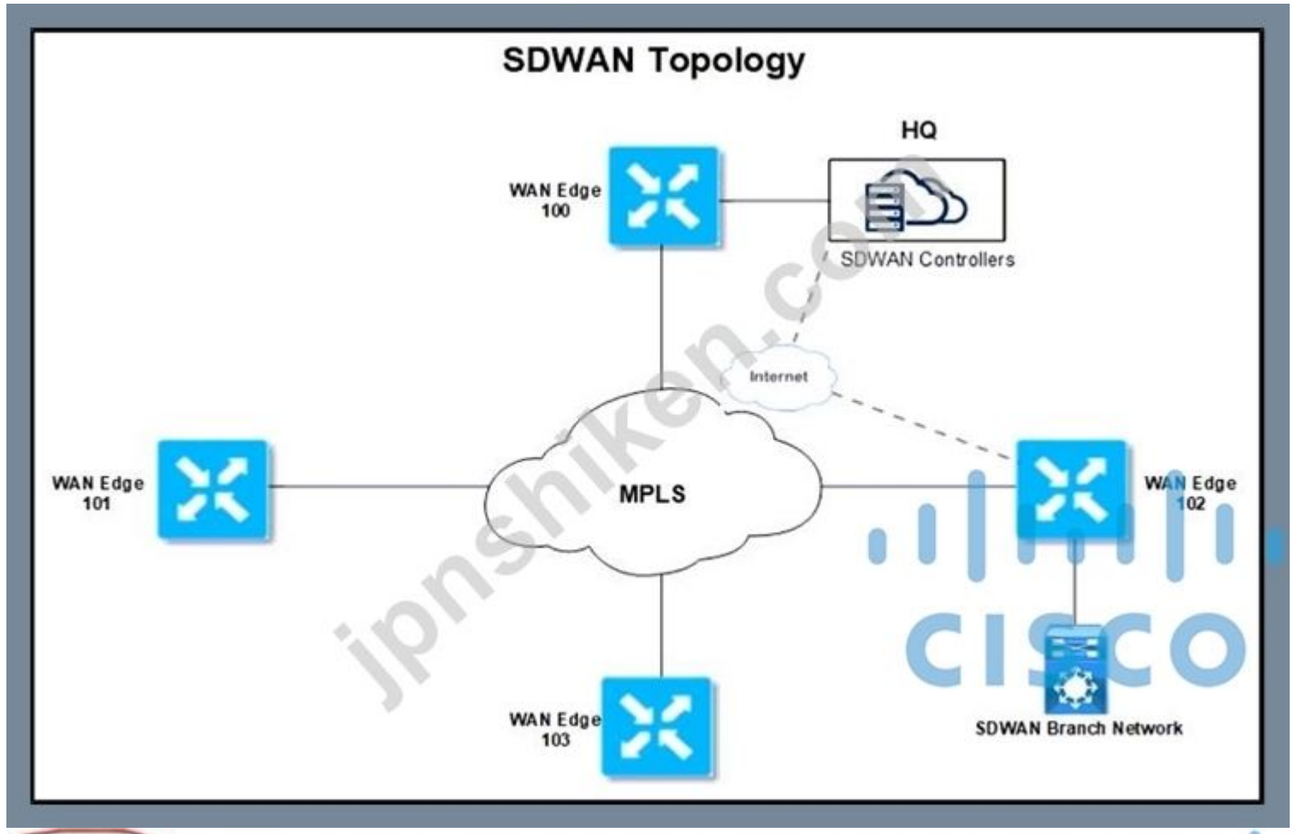
D.
```
sla-class TRANSACTIONAL_DATA
 loss    5
 latency 50
 jitter  100
!
sla-class REALTIME
 loss    2
 latency 100
 jitter  30
!
```

正解: **D** (コメントを発表する)

質問: **252**

図を参照してください。ある企業では、WAN Edge 102 から発信される OMP プレフィックスに到達する際に、すべての拠点がパブリック インターネット回線を優先的に使用するように設定する必要があります。エンジニアは、今後サイト 102 に追加されるデバイスに影響を与えずに、受信トラフィックに適用されるポリシーを Manage で設定する必要があります。

このポリシーを設定するには、「一致」タブのどの条件を選択する必要がありますか？





A. TLOC
B. 発信者
C. カラーリスト
D. サイト
正解: (正解を表示します)

有効的な**300-415J**問題集はJPNTest.com提供され、**300-415J**試験に合格することに役に立ちます！JPNTest.comは今最新**300-415J**試験問題集を提供します。JPNTest.com 300-415J試験問題集はもう更新されました。ここで**300-415J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/300-415J-mondaishu **473**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」