Cisco SD-WAN Demo Script

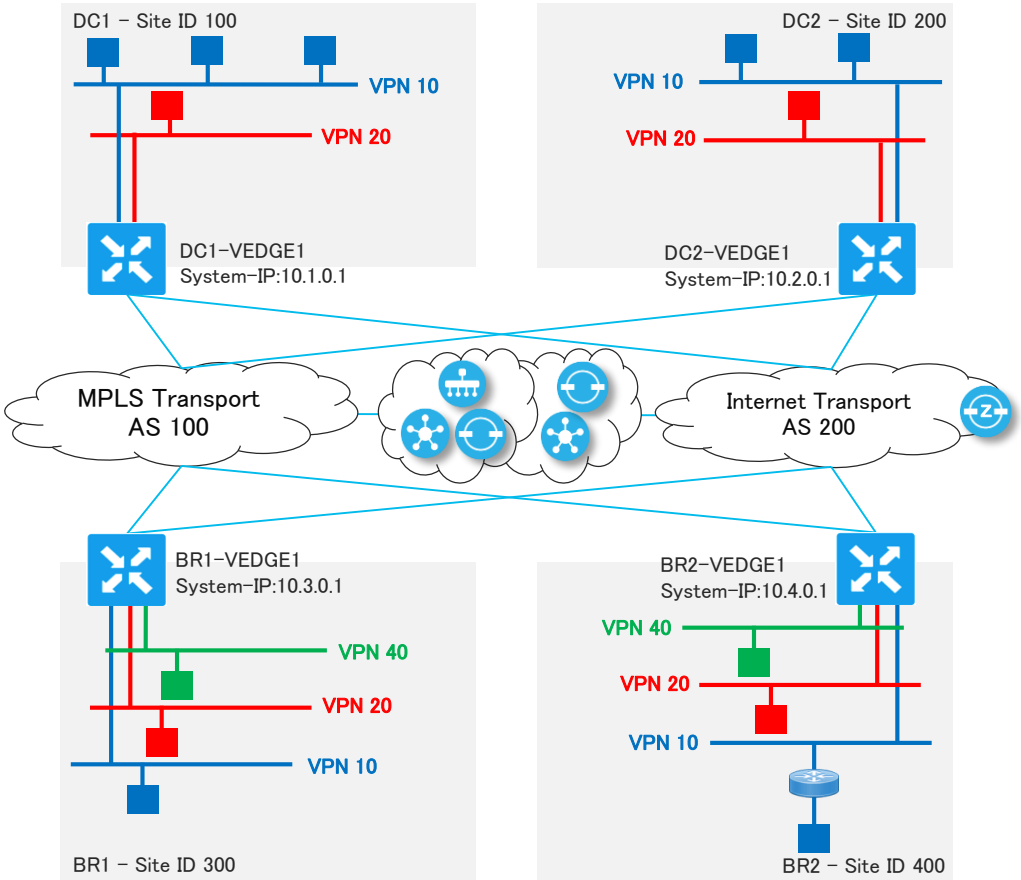
2018/6

シナリオ

- シナリオ1 – Cisco vManage ダッシュボードの概要 と ゼロタッチプロビジョニング（ZTP）機能に関するセクション。 工場出荷時設定を備えた vEdge ルータは、ゼロタッチプロビジョニングによる自動化を活用することで簡単にプロビジョニングすることが可能。 デバイスの展開の前に、設定のテンプレートを割り当てる。
- シナリオ2 –ポリシー適用によるトポロジ制御に関するセクション。ポリシーの設定による柔軟なトポロジの構成が可能。本シナリオでは、 CorporateおよびIOT/PCI VPNセグメントをハブアンドスポークトポロジを構成するポリシーを展開する。ブランチのゲストWi-Fi VPNは、DIAのみ許可。
- シナリオ3 – ポリシー適用によるマルチトポロジ制御に関するセクション。本シナリオでは、Coporate VPNはフルメッシュ構成、IOT/PCI VPNはハブアンドスポーク構成、とVPNセグメントごとに異なるトポロジ制御を行う。ブランチのゲストWi-Fi VPNは、DIAのみ許可。
- シナリオ4 – サービスチェインニングの機能に関するセクション。物理トポロジに依存せず、任意の拠点にネットワークサービス（FW、IPS、IDSなど）を展開可能。本シナリオでは、ネットワークにFWサービスを導入する。
- シナリオ5 – Application Aware Routing の機能に関するセクション。ネットワーク品質に基づいた動的なパスの選択が可能。
- シナリオ6 – リージョナルインターネットExitの設定を行うセクション。BRからのインターネット宛のトラフィックを特定のDCを優先して経由させる。
- シナリオ7 – Cloud OnRamp for SaaS(旧CloudExpress)に関するセクション。複数の出口が利用可能な場合に、パフォーマンスベースのパス選択を提供。本シナリオでは、ブランチ上の特定のSaaSアプリケーションに対してCloudExpressを有効にする。

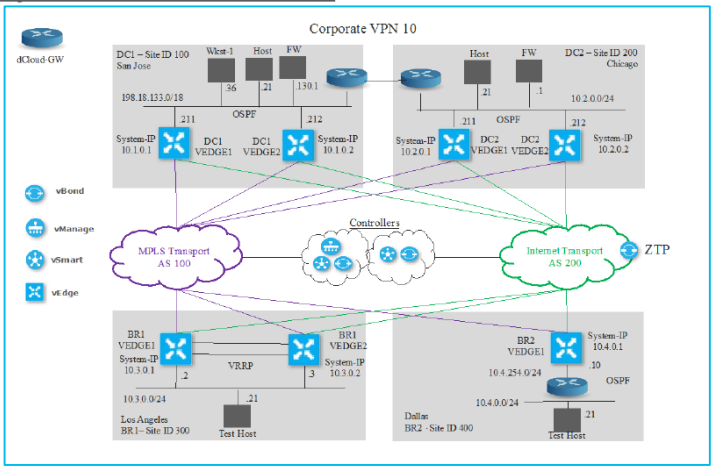
トポロジ

トポロジ（簡易版）

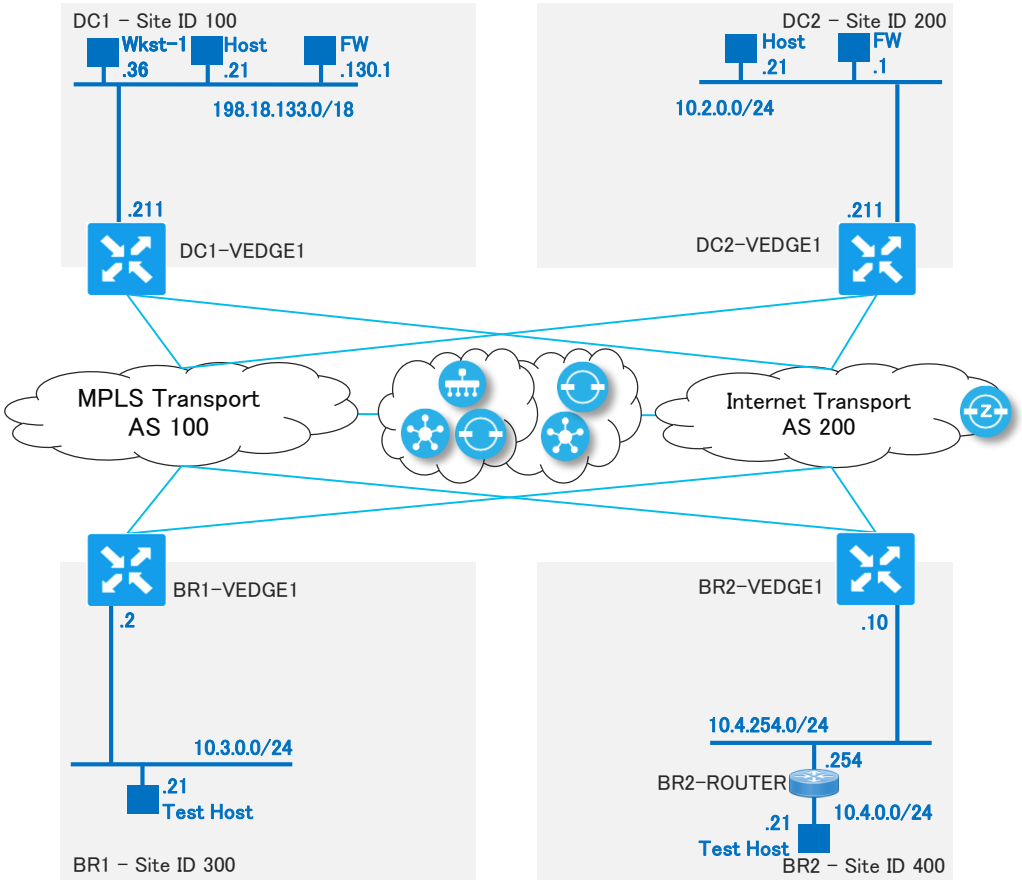


- ZTP Server
- vBond
- vSmart
- vManage
- vEdge

Viptela dCloud Lab in details

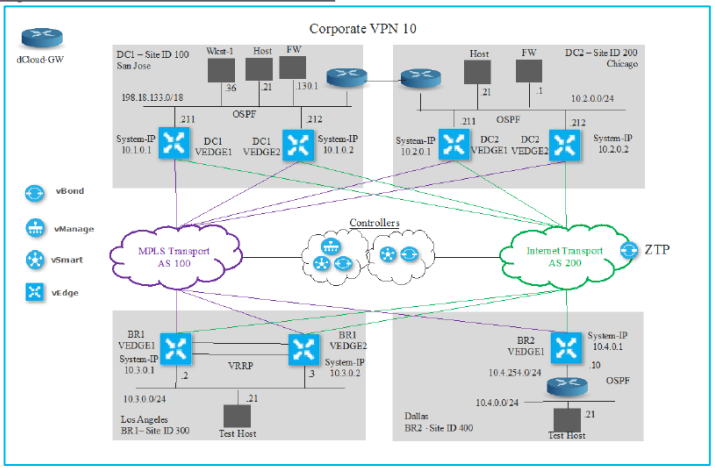


トポロジ（Corporate VPN 10）

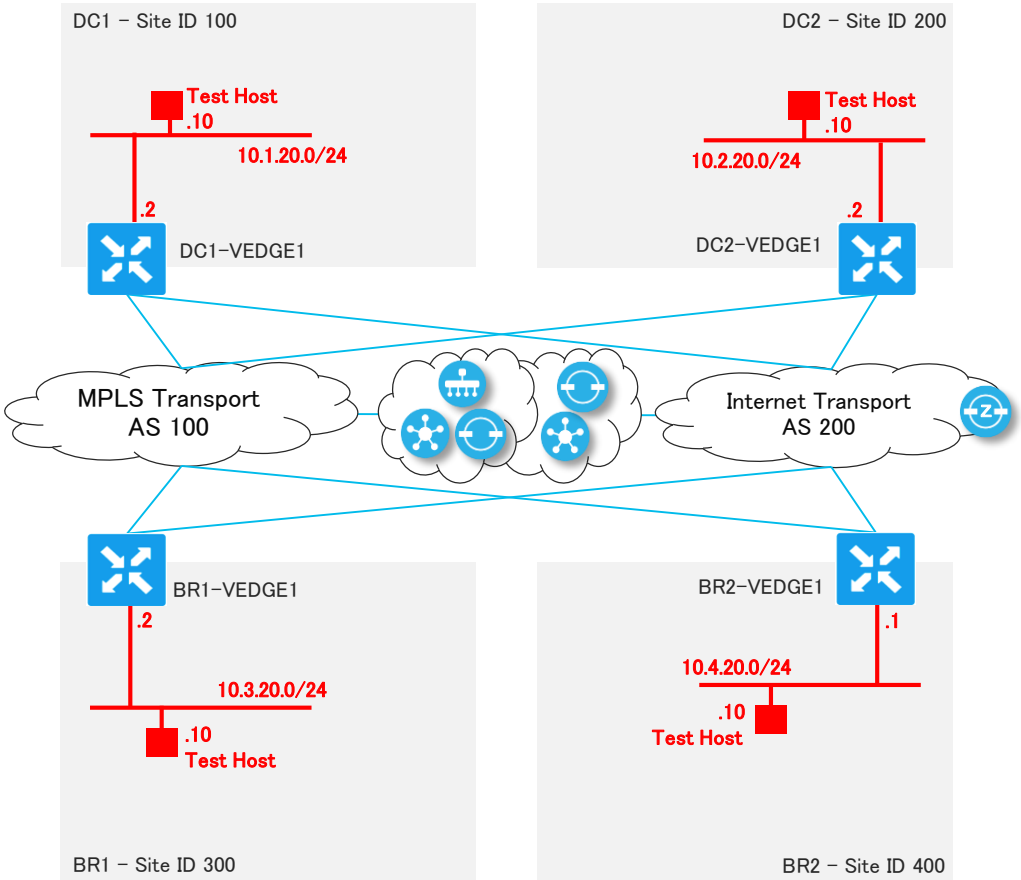


【データプレーンの疎通確認は以下のIPを使用】
DC1 : 198.18.133.21 (Host)
DC2 : 10.2.0.21 (Host)
BR1 : 10.3.0.21 (Test Host)
BR2 : 10.4.0.21 (Test Host)

Viptela dCloud Lab in details

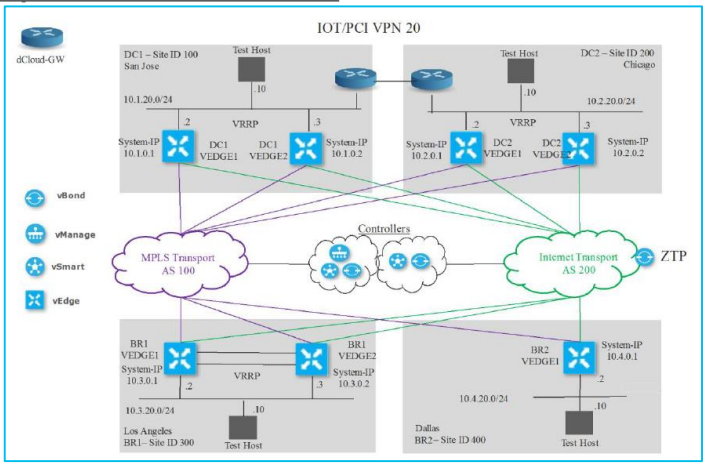


トポロジ（IOT/PCI VPN 20）

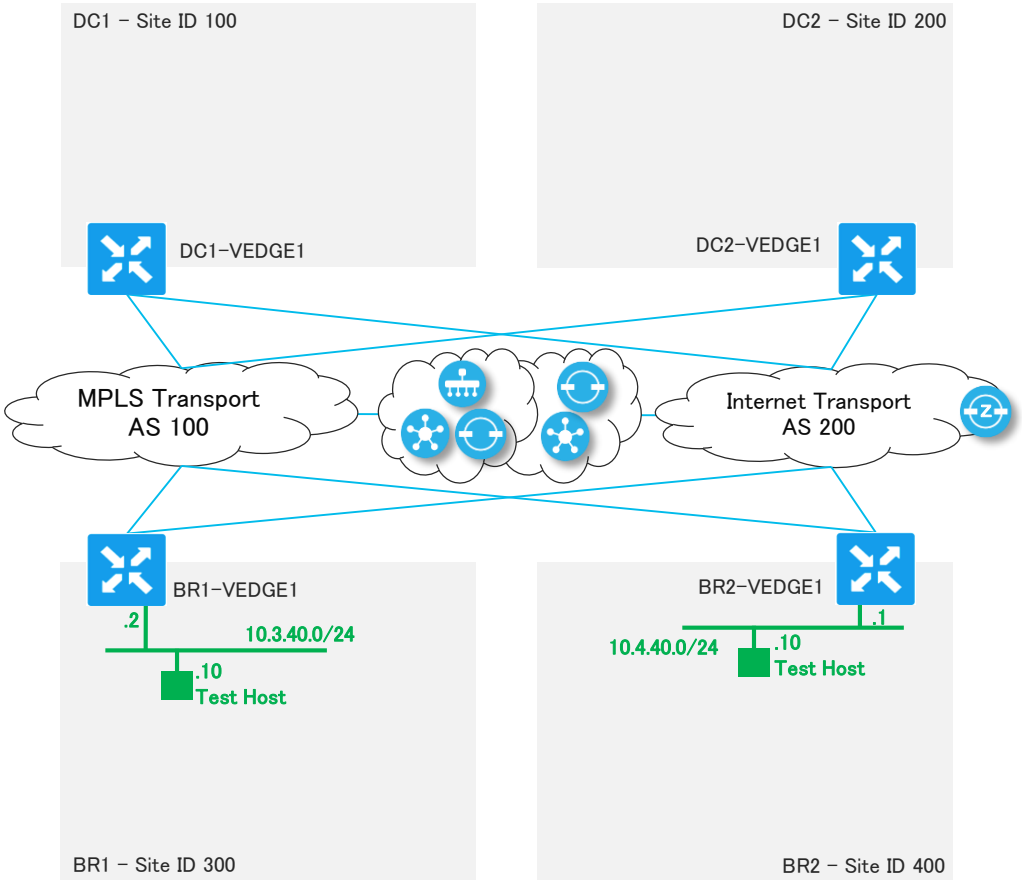


【データプレーンの疎通確認は以下のIPを使用】
DC1 : 10.1.20.10 (Test Host)
DC2 : 10.2.20.10 (Test Host)
BR1 : 10.3.20.10 (Test Host)
BR2 : 10.4.20.10 (Test Host)

Viptela dCloud Lab in details

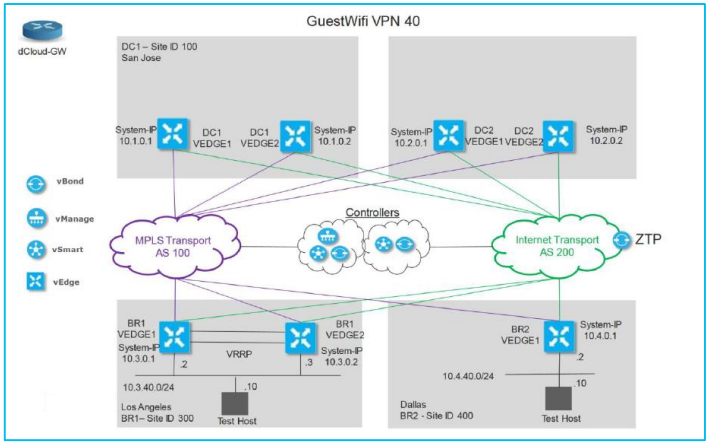


トポロジ（GuestWifi VPN 40）



【データプレーンの疎通確認は以下のIPを使用】
DC1 : X
DC2 : X
BR1 : 10.3.40.10 (Test Host)
BR2 : 10.4.40.10 (Test Host)

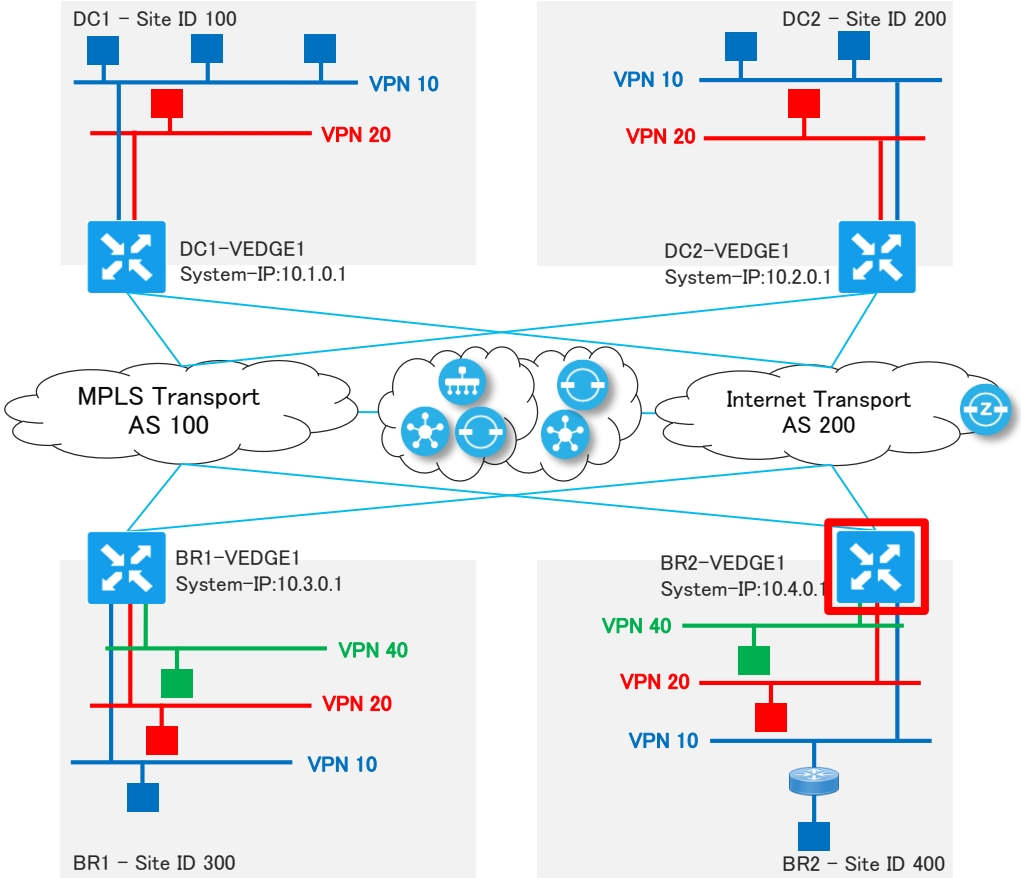
Viptela dCloud Lab in details



シナリオ1

シナリオ1 – 概要

Cisco vManage ダッシュボードの概要 と ゼロタッチプロビジョニング（ZTP）機能に関するセクション



【ゼロタッチプロビジョニング（ZTP）】
ゼロタッチプロビジョニングによる自動化を活用して、デバイスを安全に検出およびプロビジョニングします。

【シナリオ概要】
Cisco vManage にアクセスし、ネットワークやデバイスの状態を確認。

工場出荷状態のBR2のvEdgeのWANインターフェスを起動させ、ゼロタッチプロビジョニングを実行。

確認事項

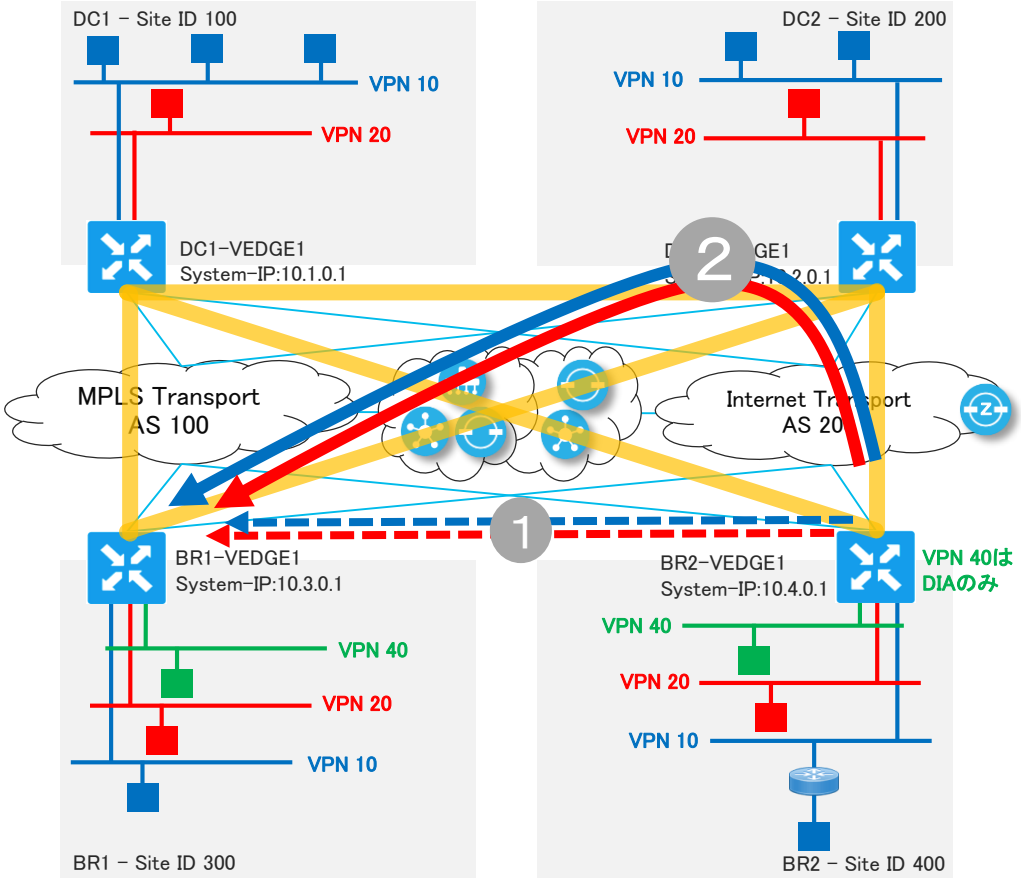
- BR2-VEDGE1をZTP後、vEdgeのUP状態とReachability
- コントロールコネクション
- Ping to

Site	VPN 10 Test IP	VPN 20 Test IP	VPN 40 Test IP
DC1	198.18.133.21	10.1.20.10	X
DC2	10.2.0.21	10.2.20.10	X
BR1	10.3.0.21	10.3.20.10	10.3.40.10
BR2	10.4.0.21	10.4.20.10	10.4.40.10

シナリオ2

シナリオ2 – 概要

ポリシー適用によるトポロジ制御に関するセクション

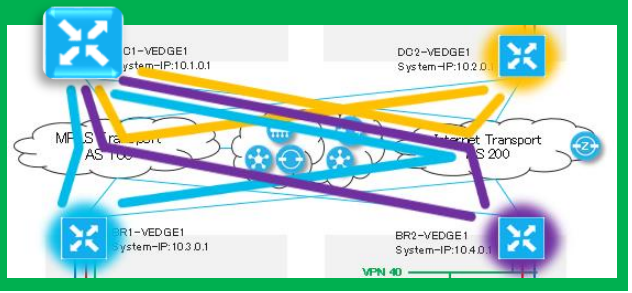


【トポロジの管理と制御】
Cisco SD-WAN では、ポリシー設定により、簡単にトポロジを制御することが可能です。ブランチにスケーラビリティとシンプルさが提供されます。

【シナリオ概要】
Cisco vManage から、「ハブアンドスポークを構成する」ポリシー（作成済）を適用する。

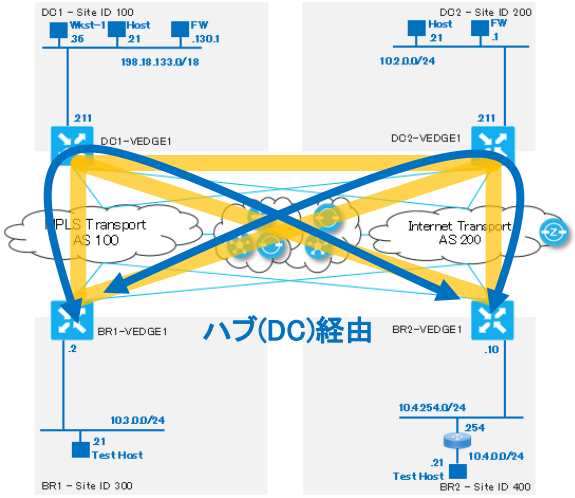
BR2のvEdgeからBR1のTestHost宛に、VPNセグメントごとにトレースルートを実行し、通信経路が変わっていることを確認する。

左図のIPsecトンネルの絵は簡略化していますが、厳密には同じvEdge宛にトランスポートごとに別のトンネルが確立されます。



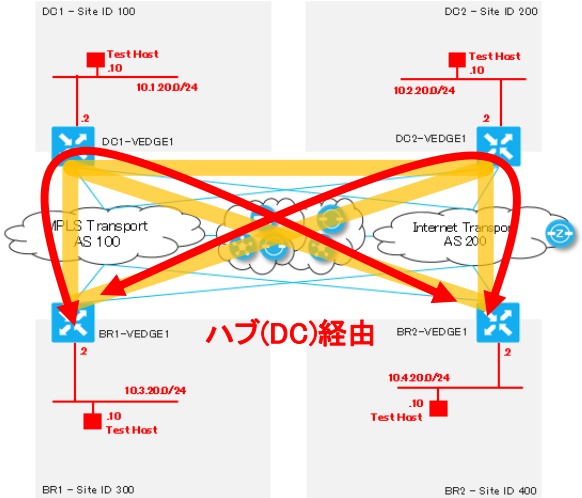
シナリオ2 – ポリシー概要

Corporate VPN 10



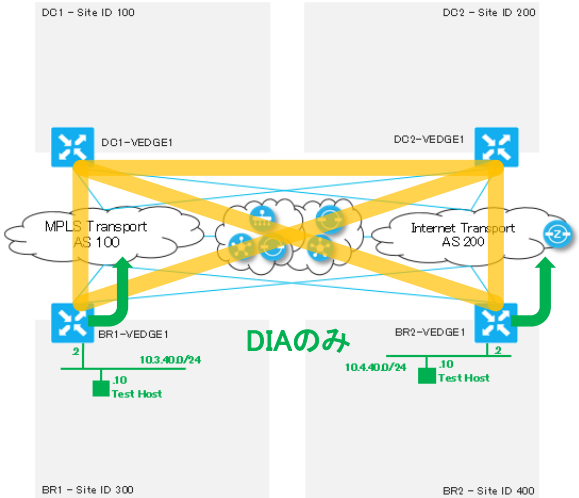
ハブ(DC)経由

IOT/PCI VPN 20



ハブ(DC)経由

GuestWifi VPN 40



DIAのみ

【ポリシー適用後…】

- IPsecトンネルはハブアンドスポーク構成
- Corporate VPN 10 と IOT/PCI VPN 20 では、BR間通信はハブ（DC）を経由する。
- GuestWifi VPN 40 はDIA（ダイレクトインターネットアクセス）のみ許可。

確認事項

- ポリシー適用前、フルメッシュ構成時の

Traceroute to 10.3.0.21(TestHost@BR1) VPN10 from BR2-VEDGE1

Traceroute to 10.3.20.10(TestHost@BR1) VPN20 from BR2-VEDGE1

- ポリシー適用後、ハブアンドスポーク時の

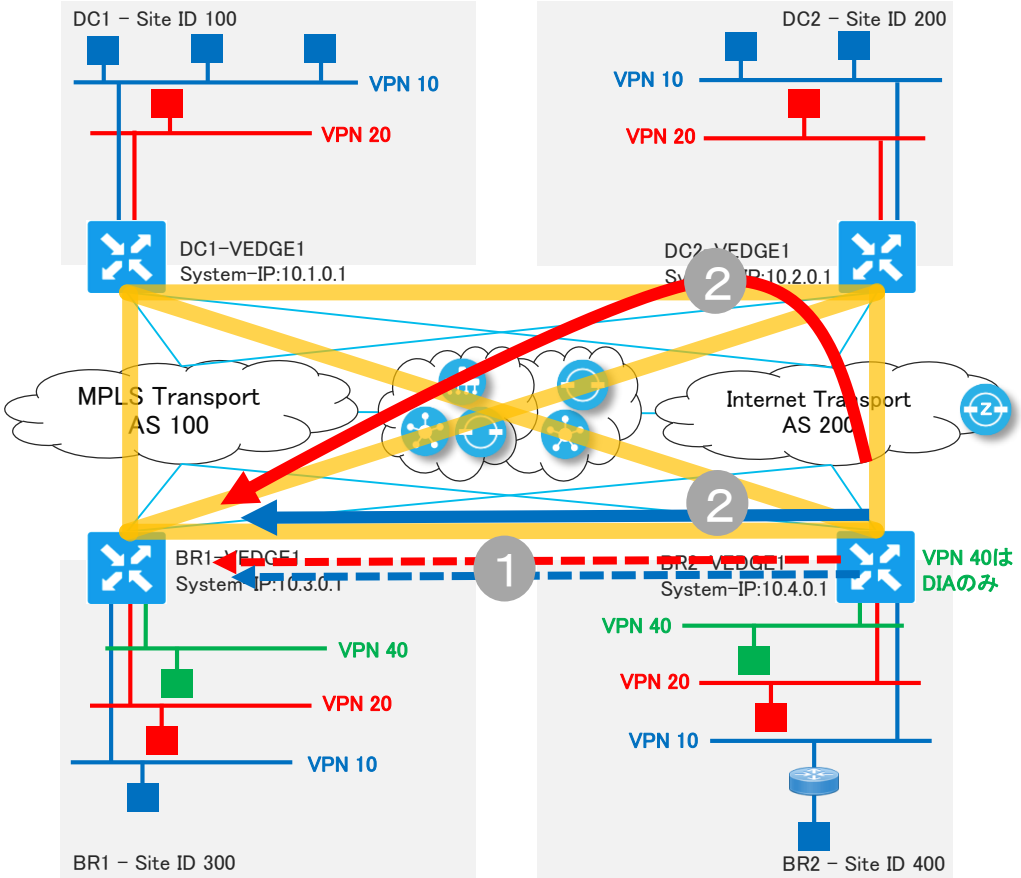
Traceroute to 10.3.0.21(TestHost@BR1) VPN10 from BR2-VEDGE1

Traceroute to 10.3.20.10(TestHost@BR1) VPN20 from BR2-VEDGE1

シナリオ3

シナリオ3 – 概要

ポリシー適用によるマルチトポロジ制御に関するセクション



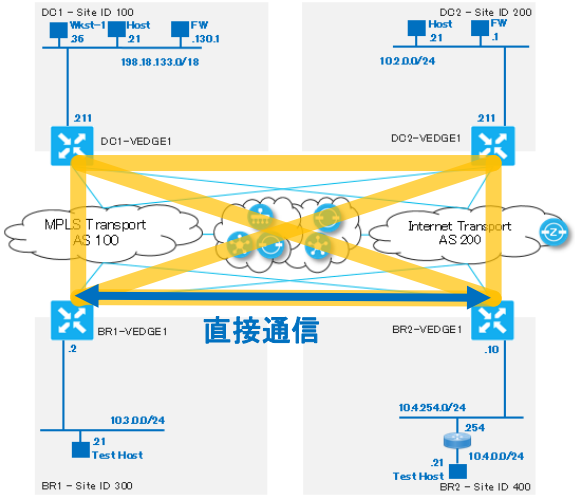
【マルチトポロジ構成】
Cisco SD-WAN では、ポリシー設定により、VPNセグメントごとに異なるトポロジを制御することが可能です。

【シナリオ概要】
Cisco vManage から、「マルチトポロジを構成する」ポリシー（作成済）を適用する。

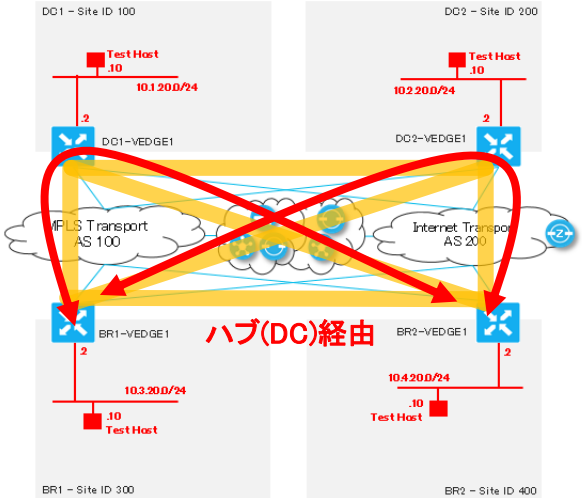
BR2のvEdgeからBR1のTestHost宛に、VPNセグメントごとにトレースルートを実行し、通信経路を確認する。

シナリオ3 – ポリシー概要

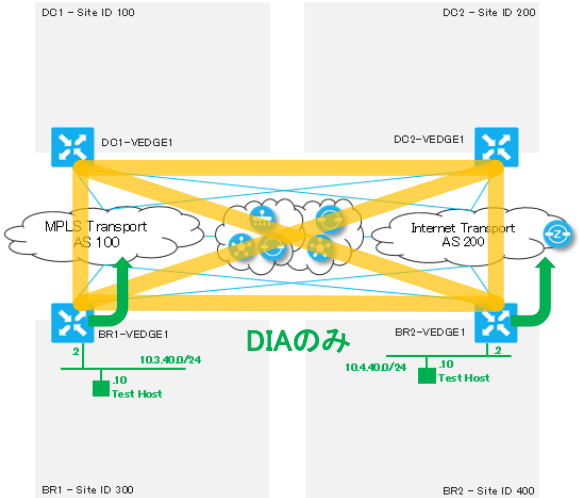
Corporate VPN 10



IOT/PCI VPN 20



GuestWifi VPN 40



【ポリシー適用後…】

- IPsecトンネルはフルメッシュ構成
- Corporate VPN 10 では、BR間も直接通信可能（フルメッシュ）
- IOT/PCI VPN 20 では、BR間通信はハブ（DC）を経由する（ハブアンドスポーク）
- GuestWifi VPN 40 はDIA（ダイレクトインターネットアクセス）のみ許可

確認事項

- ポリシー適用前、フルメッシュ構成時の

Traceroute to 10.3.0.21(TestHost@BR1) VPN10

Traceroute to 10.3.20.10(TestHost@BR1) VPN20

- ポリシー適用後、マルチトポロジ構成時の

デバイスダッシュボード > Tunnel

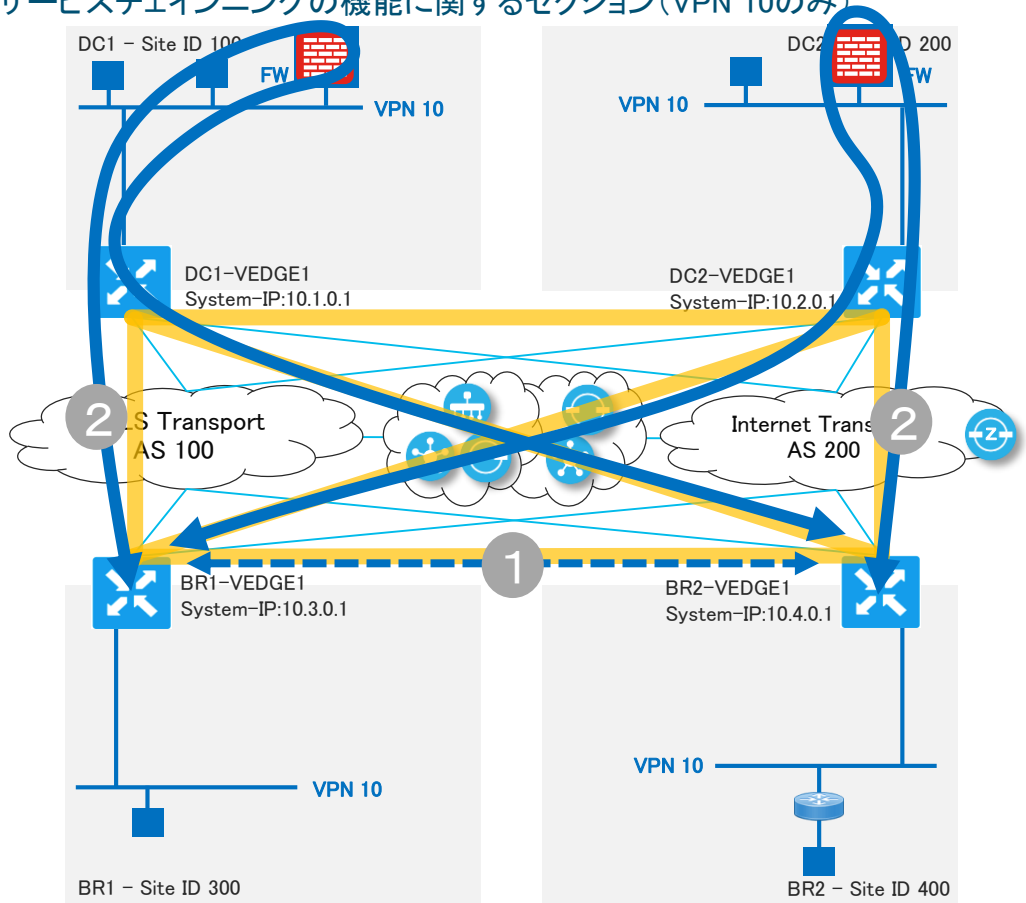
Traceroute to 10.3.0.21(TestHost@BR1) VPN10

Traceroute to 10.3.20.10(TestHost@BR1) VPN20

シナリオ4

シナリオ4 – 概要

サービスチェインニングの機能に関するセクション（VPN 10のみ）



【サービスチェインニング】
Cisco SD-WAN のサービスチェイニング機能を使うと任意のトラフィックの経路を変更して、様々なネットワークサービス（FW、IPS、IDSなど）を経由させることができます。何千台もあった拠点側 FW をデータセンター側の数十台のFW に集約し、大きくコストを削減することも可能です。

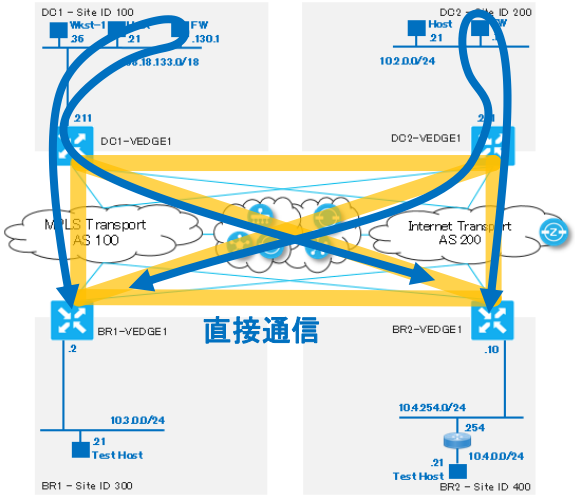
【シナリオ概要】
Cisco vManage から、「VPN10のBR間通信をDC1,2に収容された FW を経由させる」ポリシー（作成済）を適用する。

BR2のvEdge からBR1のTestHost宛にトレースルートを実行、通信経路を確認する。

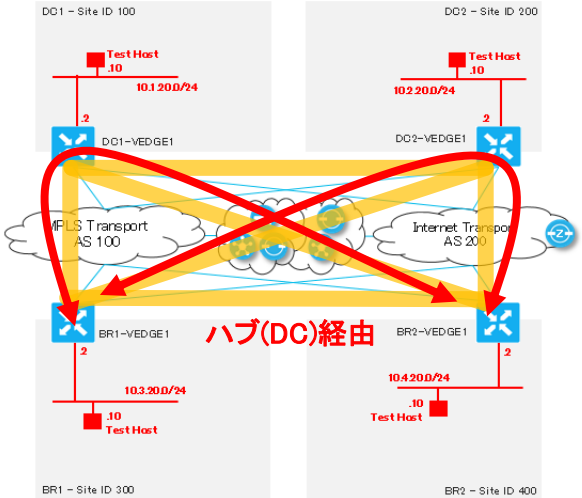
※IPsecトンネルはフルメッシュ構成
※DCのvEdgeのVPN10には、事前にFWサービスを定義している

シナリオ4 – ポリシー概要

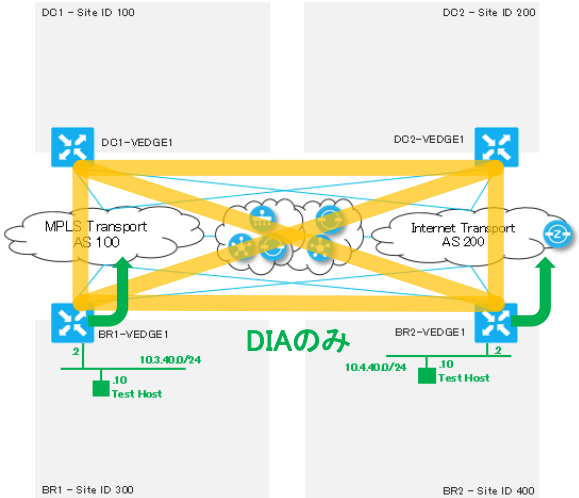
Corporate VPN 10



IOT/PCI VPN 20



GuestWifi VPN 40



【ポリシー適用後…】

- IPsecトンネルはフルメッシュ構成
- Corporate VPN 10 では、BR間はDC1のFW経由で通信（サービスチェインニング）
- IOT/PCI VPN 20 では、BR間通信はハブ（DC）を経由する（ハブアンドスポーク）
- GuestWifi VPN 40 はDIA（ダイレクトインターネットアクセス）のみ許可

確認事項

- ポリシー適用前、フルメッシュ構成時の

Traceroute to 10.3.0.21(TestHost@BR1) VPN10 from BR2-VEDGE1

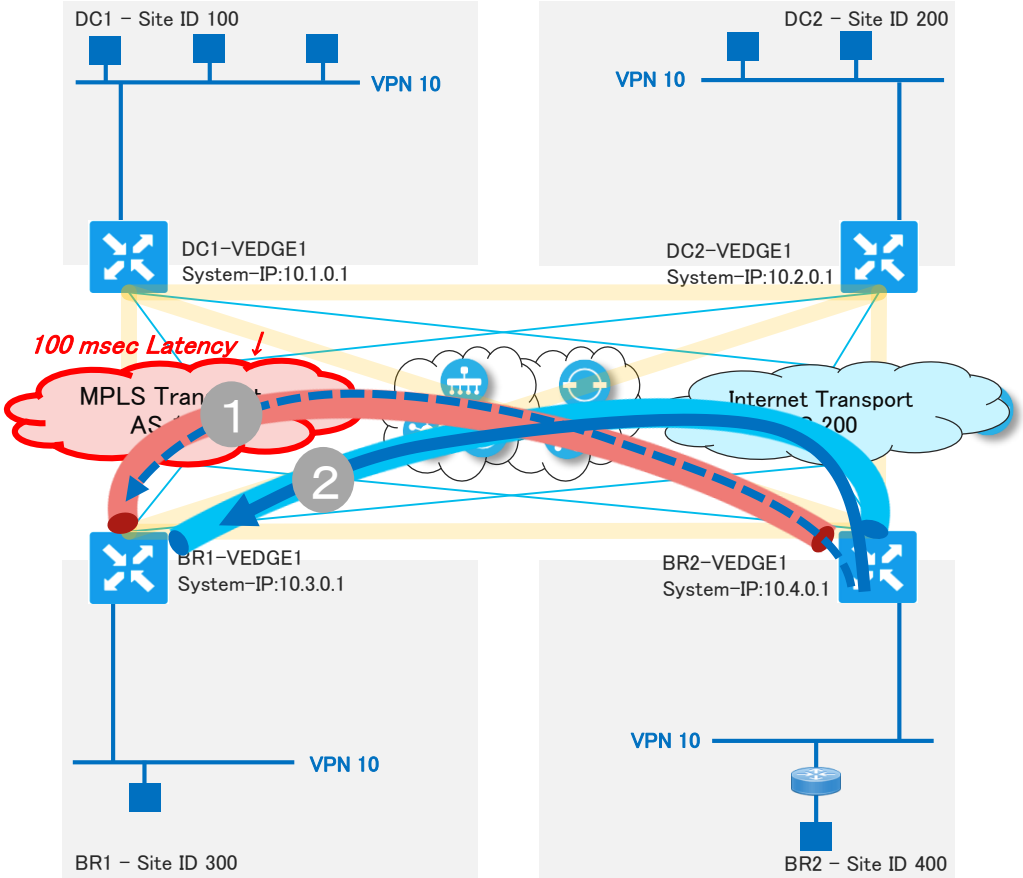
- ポリシー適用後、サービスチェインニング構成時の

Traceroute to 10.3.0.21(TestHost@BR1) VPN10 from BR2-VEDGE1

シナリオ5

シナリオ5 – 概要

Application Aware Routingの機能に関するセクション（VPN 10のみ）



【Application Aware Routing】
vEdge はアプリケーション単位で、ネットワーク品質に基づいた動的なパスの選択が可能です。最適な経路を使用した通信を提供します。

【シナリオ概要】

Cisco vManage から、「App：Office365 は 遅延：80msec以上でMPLS→Internet に切り替える、etc…」ポリシー（作成済）を適用する。

MPLSに 100msec の遅延を発生させる。

BR2のvEdgeからBR1のTestHost宛へのトラフィックをシミュレートして通信経路（mpls→biz-internet）が変わることを確認する。

確認事項

- ポリシー適用後、遅延発生前、

デバイスダッシュボード > Troubleshooting > Simulate Flows から Office365トラフィックをシミュレート

- ポリシー適用後、遅延発生後、

デバイスダッシュボード > Troubleshooting > Simulate Flows から Office365トラフィックをシミュレート

- デバイスダッシュボード > TLOC > Latency/Jitterを指定、

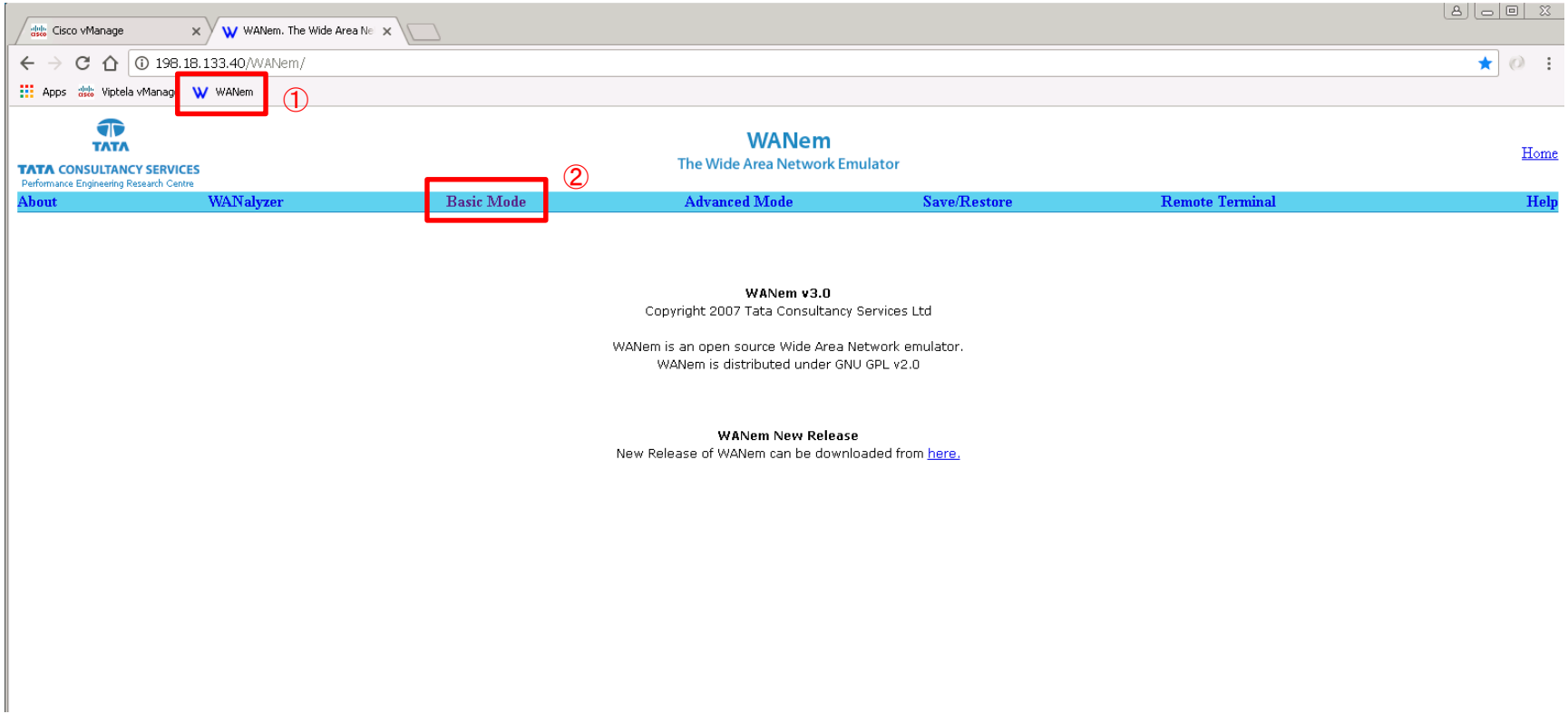
リアルタイムにTLOCごとの遅延を監視

- デバイスダッシュボード > Real Time > “App Route Statistics”、

TLOCごとの回線品質統計情報を確認

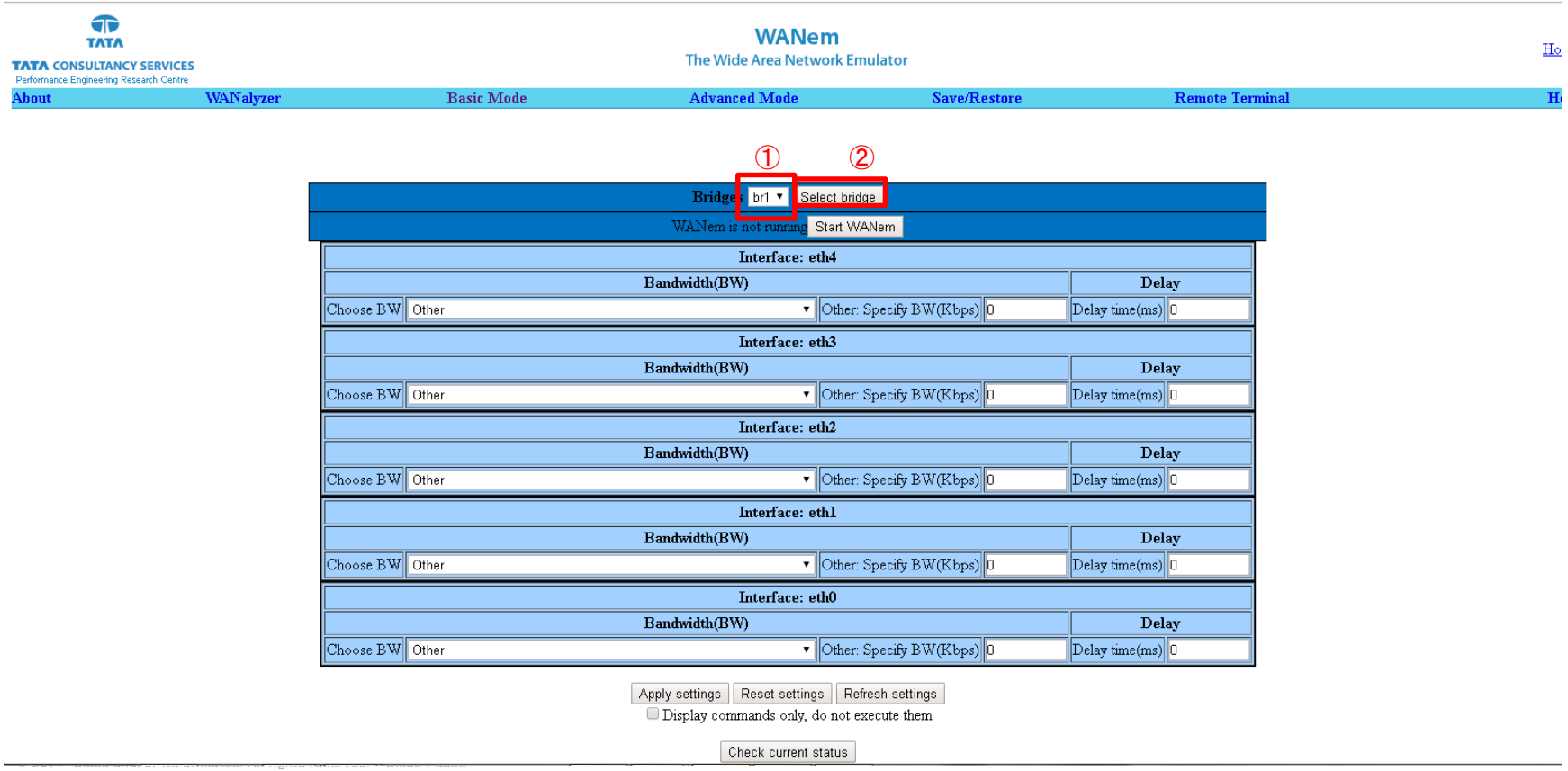
WANemの使い方

WANemソフトを使用し、MPLSに100msecの遅延を発生させます。
ブラウザの新しいタブを開き、ブックマークバーの「WANem」を開きます。「Basic Mode」をクリックします。
※vManageのタブは残しておきます。



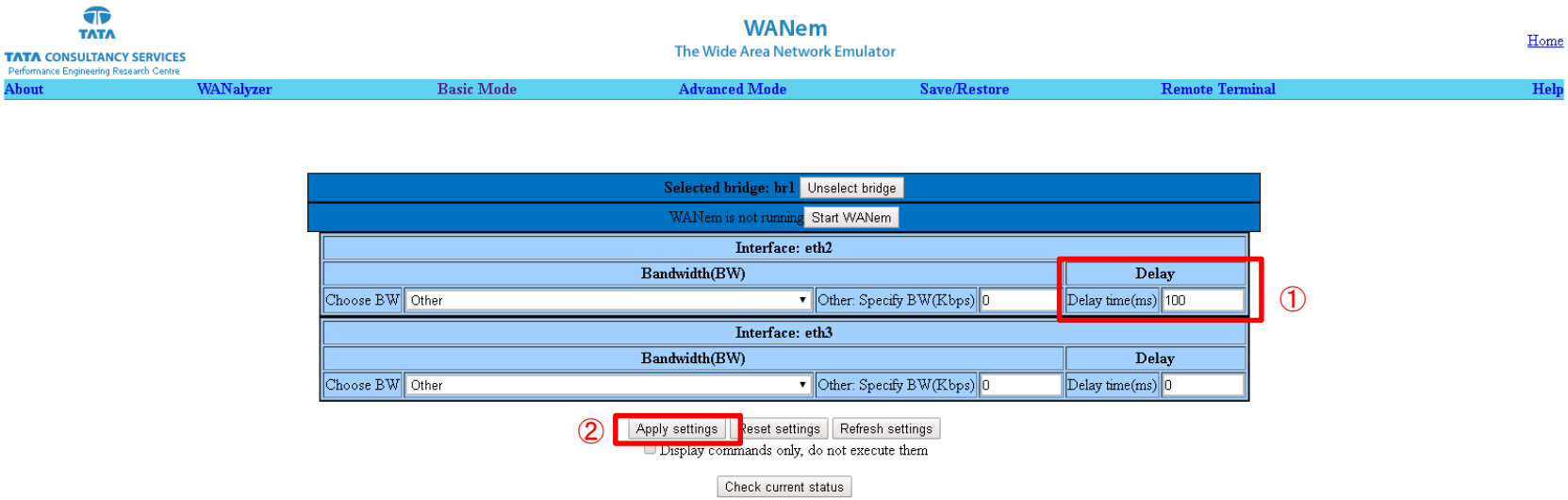
WANemの使い方

Bridgeで「br1」が選択されていることを確認し、「Select bridge」をクリックします。



WANemの使い方

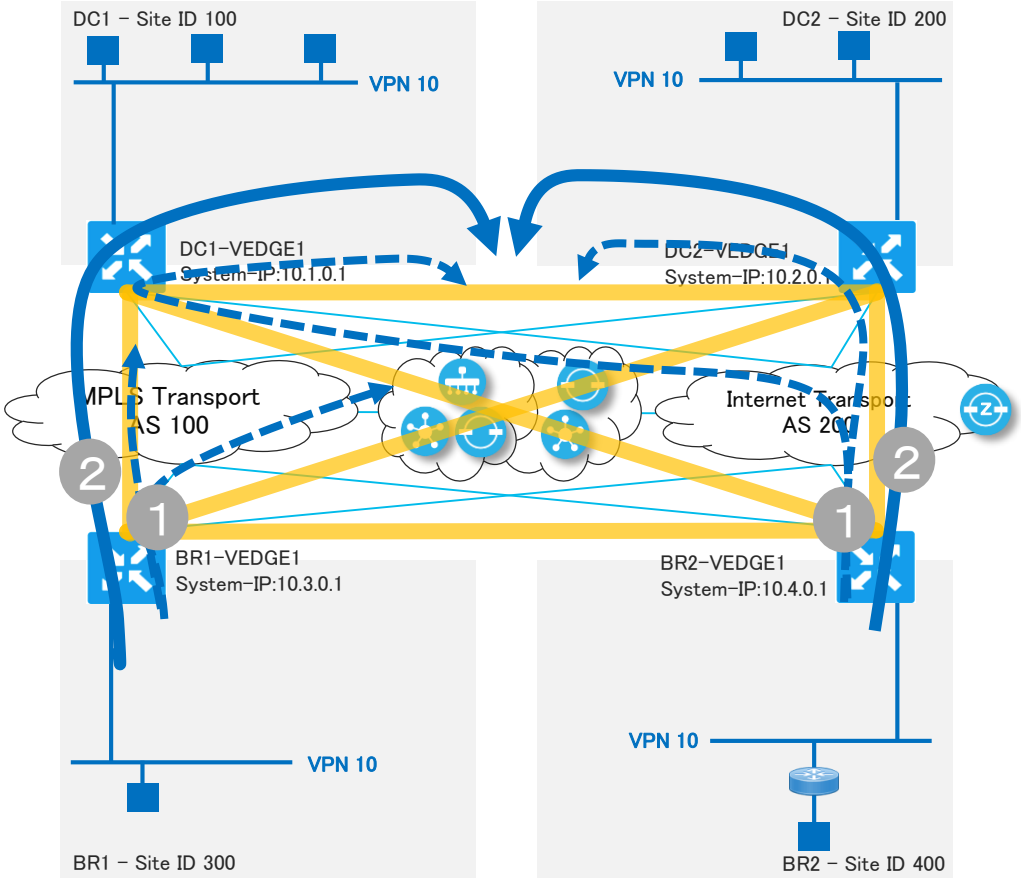
br1 の Interface eth2 の Delay欄に「100」と入力し、「Apply setings」をクリックします。



シナリオ6

シナリオ6 – 概要

リージョナルインターネットExitの設定に関するセクション（VPN10のみ）



【リージョナルインターネットExit】
Cisco SD-WAN では、ポリシー設定により、拠点ごとにインターネットExitとして使用する優先DCを設定可能です。

【シナリオ概要】
Cisco vManage から、「リージョナルインターネットExit」ポリシー（作成済）を適用する。

BR1とBR2のvEdgeで、ルーティングテーブルを参照し、デフォルトルート（インターネット宛）を確認する。

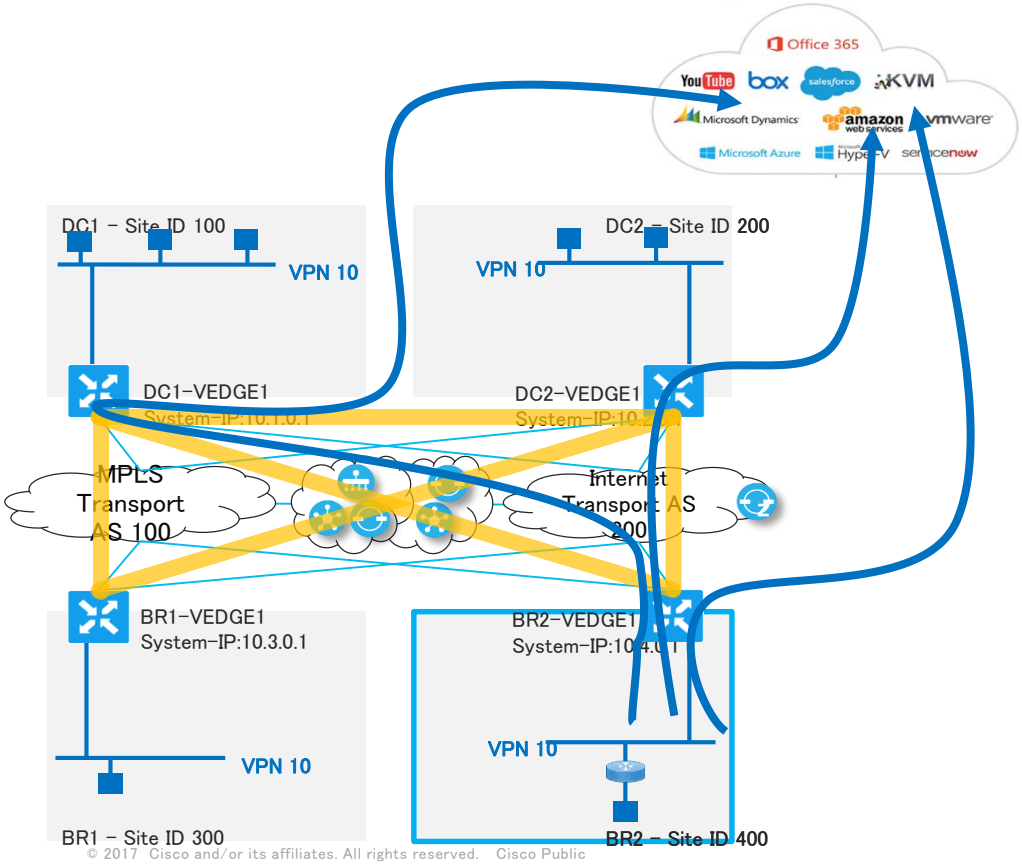
確認事項

- ポリシー適用前、デバイスダッシュボード > Real Time > “IP Routes” で VPN10, 0.0.0.0/0 とフィルターしルートを表示
- ポリシー適用後、デバイスダッシュボード > Real Time > “IP Routes” で VPN10, 0.0.0.0/0 とフィルターしルートを表示

シナリオ7

シナリオ7 – 概要

Cloud OnRamp for SaaS（旧Cloud Express）に関するセクション（VPN 10のみ）



【Cloud OnRamp for SaaS（旧Cloud Express）】
Office365、Salesforce、Dropbox、GoogleなどのSaaSアプリケーションの利用が増加し続けている中、Cisco SD-WANではアプリケーションごとに、最適なパスを提供します。

【シナリオ概要】

Cisco vManage から、Cloud Expressダッシュボードを確認。

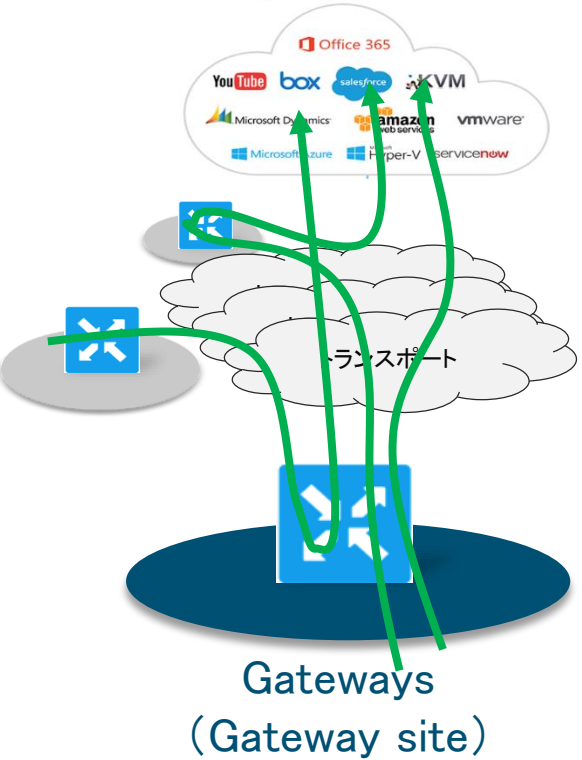
BR2のvEdgeのVPN10セグメントで、Office365 SaaSアプリケーションに対してCloud Expressを有効にします。

※本シナリオは設定フローを確認します。
Cloud Expressの機能を確認することはできません。

シナリオ7 – 補足

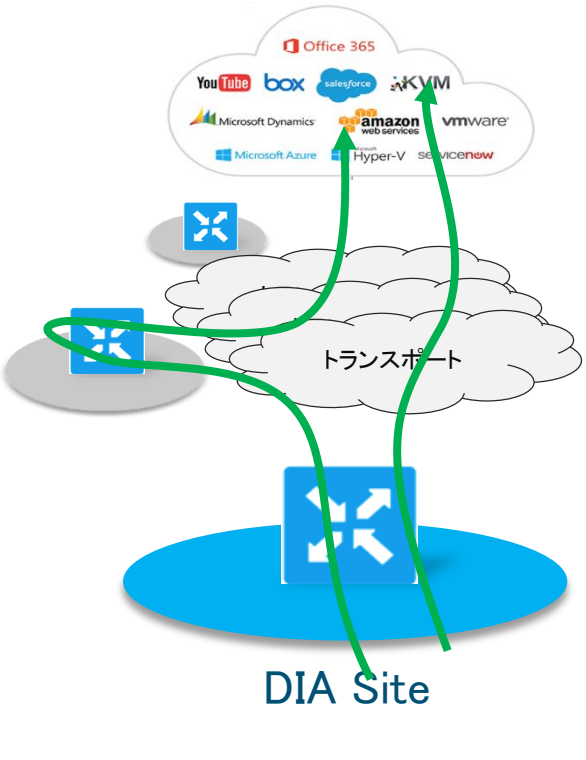
Cloud OnRamp for SaaS（旧Cloud Express）における3つのサイトの役割

他のサイトに対してGatewayとなることができるサイト
自サイトのトラフィックについては、Local Exitと他のGatewayを自動選択



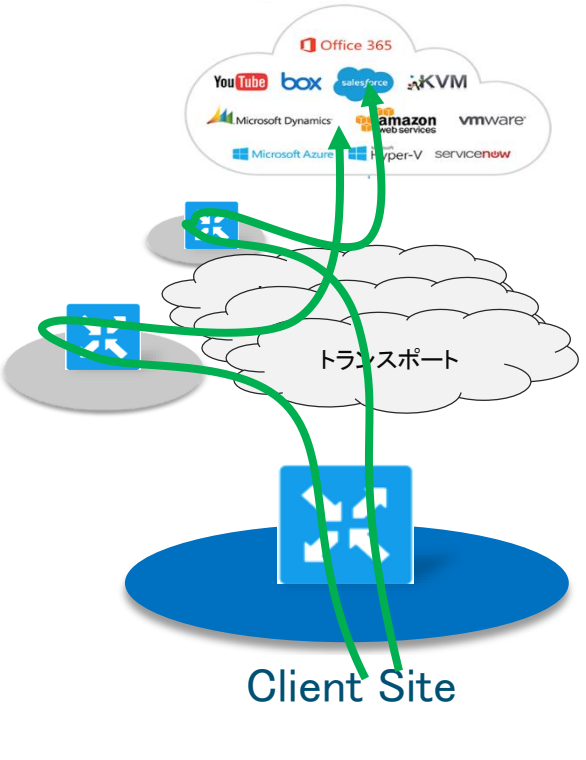
Gateways
（Gateway site）

Local ExitとGatewayを自動選択するサイト
他のサイトのGatewayとして使用されることはない



DIA Site

Local Exitがなく、必ずGatewayを経由してインターネットに接続するサイト



Client Site


CISCO