Cisco SD-WAN
技術講座　第三回 rev2
導入とマイグレーション

Kohei Yamashita
SD-WAN Architect Viptela - Japan
2020/10

目次

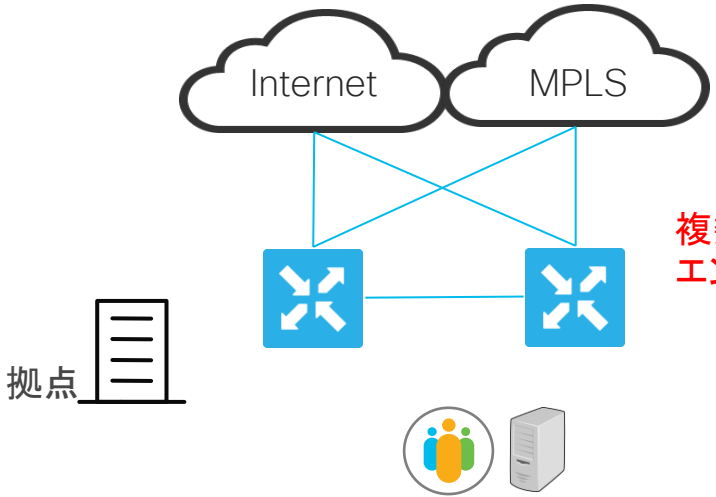
1. SD-WAN導入の前に
2. 基本設定とテンプレート設定
3. ネットワークポリシー　セキュリティポリシー
4. マイグレーション
5. セキュアクラウドとの接続(Umbrella/zScaler)
6. IaaSとの接続(AWS/Azure)

第一回　インターネットブレイクアウト　済
第二回　二重化構成とSIG連携　済
第四回　Cisco-SD-WAN 20.3/17.3 新機能とユースケース

SD-WAN導入の前に

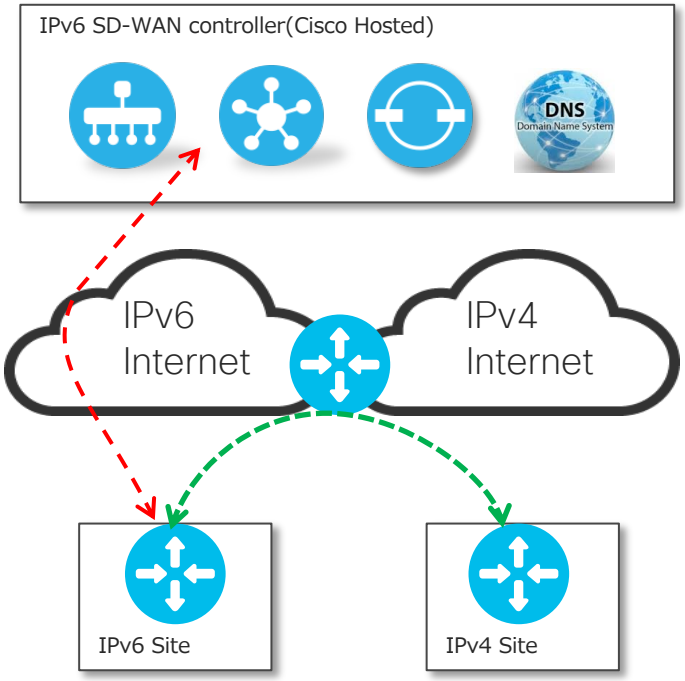
回線環境を確認する

Cisco-SD-WAN導入のまず確認すべきことは、利用する回線環境
日本では特にPPPoE環境での導入が多い
そのほかにもVLANタグが必要な回線、LTEなど多彩な環境に対応できる



複数の回線をどのように繋ぐかが
エンジニアの腕の見せ所

IPoEとSD-WAN　計画中



IPv6回線でのキャリアサービスはすでに展開中
https://business.ntt-east.co.jp/service/sd-wan/

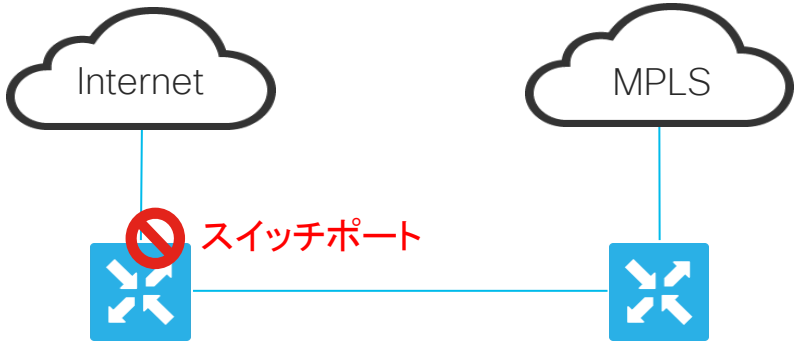
企業向けカスタマイズ可能な
IPv6対応CiscoSD-WANに向けて計画中

以下のいくつかの課題に順次対応していく予定

- IPv6コントローラ/AAAAレコード
- IPv6 ローカルブレイクアウト
- IPv4 over IPv6
- IPv4拠点とIPv6拠点とのSD-WAN接続

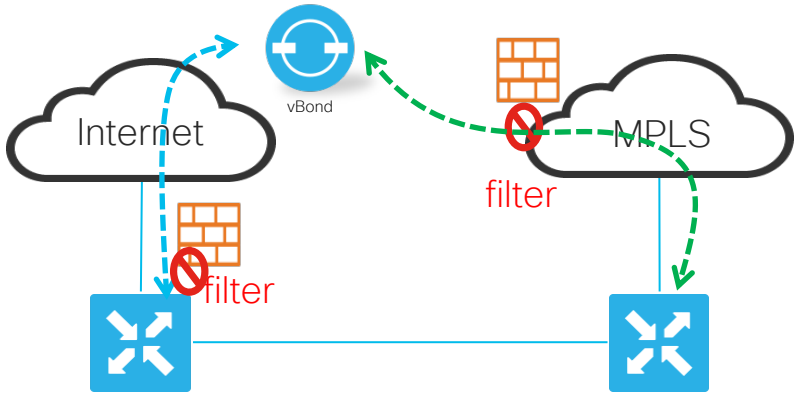
機器の物理ポート数

デバイスモデルによって収容できるWANリンク数、LANリンク数に差分がある
特に気を付けたいのはスイッチポート搭載の以下のモデル
　C1111-4P/C1111-8P
基本的にスイッチポートはWANリンクとしては使えない
＊裏技的にSVIをWANとして利用することができるがvManageテンプレートではサポート不可



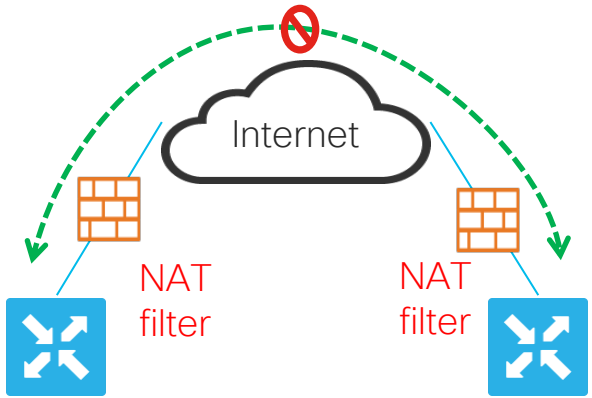
コントローラとの接続性　Firewallなど

全ての機器はコントローラとの接続が必要
接続経路上でコントローラとの接続を阻害する要因がないかをチェック
二重化MPLS利用の場合ではコントローラ通信をする場合に
ルーティング、フィルタリング等の調整が必要
フィルタリングについてはSD-WAN Firewall portを確認



FirewallとNATタイプ

CiscoSD-WANのIPsecはNAT配下でも動作するが
ただし特殊なNATタイプの場合にはIPsec通信ができない場合がある

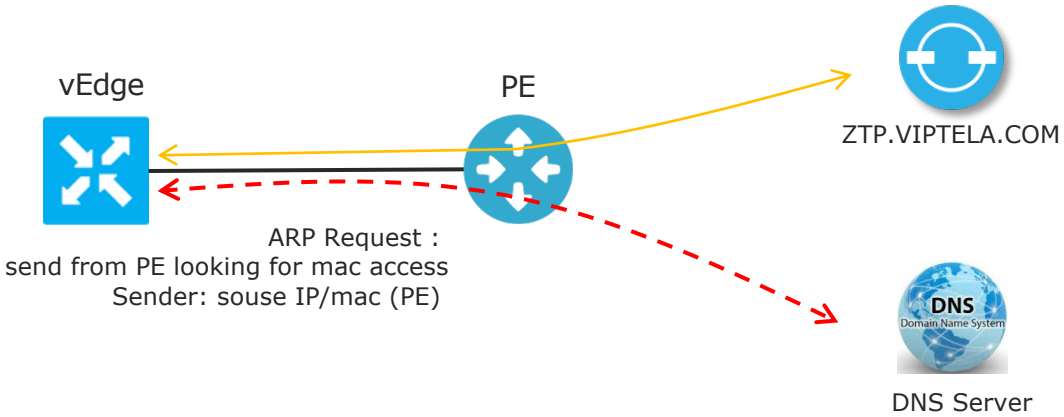


Side A	Side B	Tunnel Status
Public	Public	○
Full Cone	Full Cone	○
Full Cone	Port/Address Restricted	○
Port/Address Restricted	Port/Address Restricted	○
Public	Symmetric	○
Full Cone	Symmetric	○
Symmetric	Port/Address Restricted	NG
Symmetric	Symmetric	NG

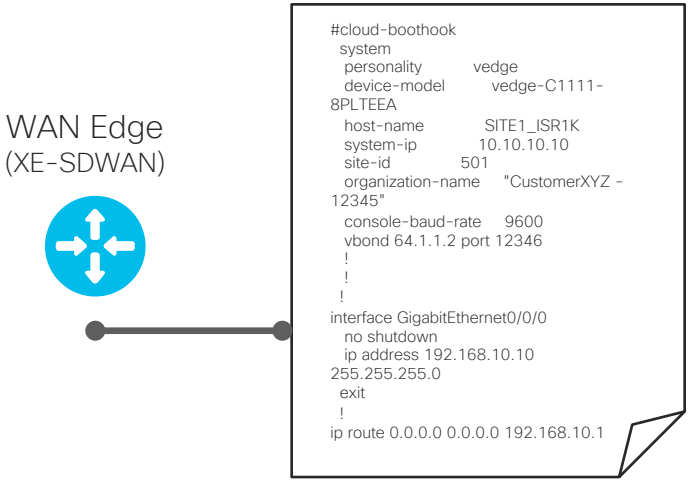
ZTPの代替手段

PPPoE、特殊LTE、MPLSなどZTPが行えない環境下でも複数の代替え手法がある

vEdge：Auto-IP

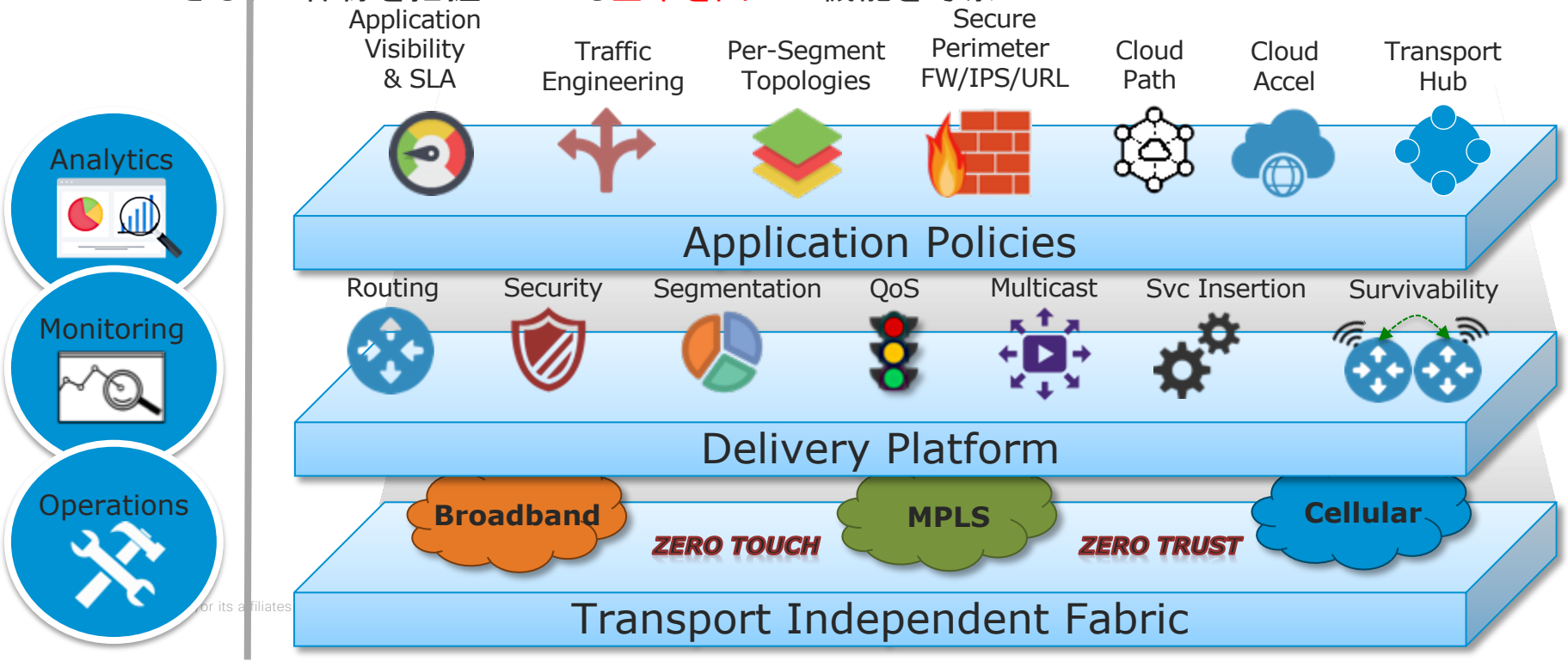


cEdge：USB



SD-WAN機能全体像を理解する

SD-WANはITインフラのベーシックな機能から付加機能まで、多数機能を使うことができる。全体像を把握しつつも基本を固めて機能を考察



基本設定とテンプレート管理

基本設定　コントローラ

Cisco-SD-WAN **コントローラ機器の基本設定は簡単にまとめると以下**
最低限上位3つの設定が必須

・システム設定
host-name / system-ip / site-id / organization-name / vbond-ip

・WAN側インタフェース
vpn 0 / interface**名** / ip address / Tunnel-interface(vbond**は不要**)

・ルータ機器シリアル一覧

・オプション
SNMP / SYSLOG　etc..

基本設定 ルータデバイス

Cisco-SD-WAN **ルータ機器の基本設定は簡単にまとめると以下**
最低限上位3つの設定が必須

- **システム設定**
  host-name / system-ip / site-id / organization-name / vbond-ip

- WAN**側インタフェース**
  vpn 0 (global-vrf) / interface**名** / ip address / Tunnel-interface

- LAN**側インタフェース**
  vpn X (vrf X) / interface**名** / ip address

- LocalPolicy
  ACL / Route-map / SNMP / SYSLOG / DPI/Netflow / Security

vEdge Factory Default Configuration

```
vEdge100b# show running-config
system
 vbond ztp.viptela.com
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password <文字列省略>
  !
 !
 logging
  disk
   enable
  !
 !
!
```

By default, vEdge connects to ztp.viptela.com for ZTP.
(You can skip the process of ZTP by replace ztp.viptela.com with the IP address or FQDN of vBond)

```
omp
 no shutdown
 graceful-restart
 advertise connected
 advertise static
!
security
 ipsec
  authentication-type ah-sha1-hmac sha1-hmac
 !
!
vpn 0
 interface ge0/4
  ip dhcp-client
  tunnel-interface
   encapsulation ipsec
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
  !
  no shutdown
 !
!
vpn 512
 interface ge0/0
  ip address 192.168.1.1/24
  no shutdown
 !
!
```

ge0/4 is configured with DHCP for ZTP.
tunnel-interface is also configured to allow for establishing connections in control plane and data plane.

cEdge Configuration *samplこれが工場出荷ではないので注意

```
system
 system-ip             172.27.1.7
 overlay-id            1
 site-id               11
 control-session-pps   300
 no admin-tech-on-failure
 sp-organization-name  "organization - xxxxx"
 organization-name     "organization - xxxxx"
 console-baud-rate     9600
 vbond 2.2.21.1 port 12346
!
vrf definition 1
 rd 1:1
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 description Transport VPN
 rd          1:512
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
ip route 0.0.0.0 0.0.0.0 2.2.28.1 1
```

VRF assignment

VRF configuration

```
interface GigabitEthernet0
 no shutdown
 vrf forwarding Mgmt-intf
 ip address dhcp client-id GigabitEthernet0
exit
interface GigabitEthernet0/0/0
 no shutdown
 ip address dhcp client-id GigabitEthernet0/0/0
exit
interface GigabitEthernet3
 no shutdown
 vrf forwarding 1
 ip address x.x.x.x 255.255.255.0
exit
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit
```

Tunnel assignment

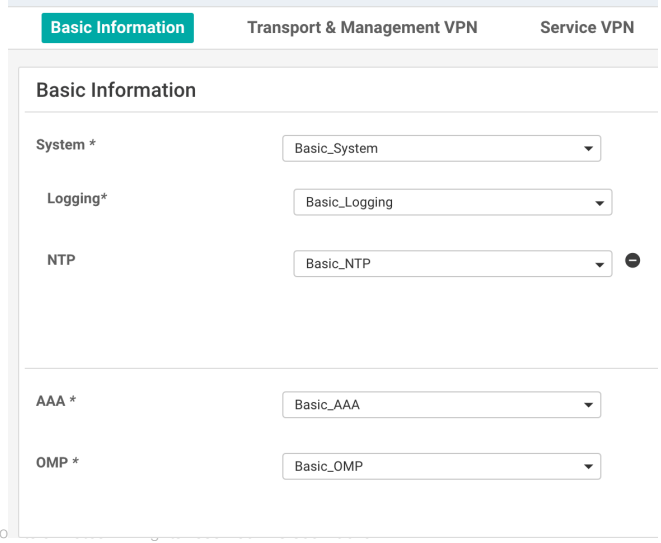
```
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec weight 1
   color gold
   no last-resort-circuit
   vmanage-connection-preference 5
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
  exit
 exit
 interface GigabitEthernet3
 exit
exit
policy
 no app-visibility
 no flow-visibility
 no implicit-acl-logging
 log-frequency        1000
!
```

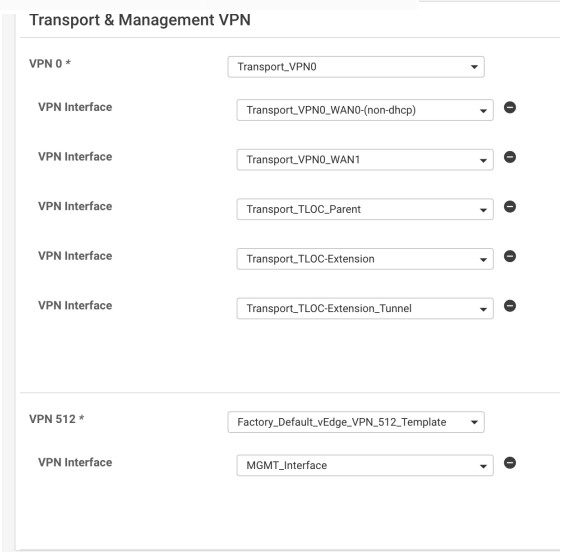

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html

Feature Template

完全GUIでのCofigurationが可能　Cisco固有のCLIを暗記する必要がない

Name	Description	Type	Device Model	Feature Templates	Devices Attached
Datacenters	DC, 2 WAN per router	Feature	vEdge Cloud	19	2
SItes_A	TLOC-Ext, 1 WAN	Feature	vEdge Cloud	19	0
Sites_C	Single vE, 2 WAN	Feature	vEdge Cloud	30	3
SItes_D	Single vE, 1 WAN	Feature	vEdge 1000	13	1





Device and Feature Template

拠点タイプや機種モデルに応じてテンプレートを作ることでパラメータ管理が楽になる

Datacenter
- System
- Logging
- NTP
- AAA
- OMP
- BFD
- Security

- Transport VPN 0
- VPN Interface
- VPN Interface

- Services VPN 1
- VPN Interface

- Services VPN 2
- VPN Interface

Remote_Type_A
- System
- Logging
- NTP
- AAA
- OMP
- BFD
- Security

- Transport VPN 0
- VPN Interface
- VPN Interface

- Services VPN 1
- VPN Interface

- Services VPN 2
- VPN Interface

Remote_Type_B
- System
- Logging
- NTP
- AAA
- OMP
- BFD
- Security

- Transport VPN 0
- VPN Interface

- Services VPN 1
- VPN Interface

- Services VPN 2
- VPN Interface

Remote_Type_C
- System
- Logging
- NTP
- AAA
- OMP
- BFD
- Security

- Transport VPN 0
- VPN Interface

- Services VPN 1
- VPN Interface

ネットワークポリシー
セキュリティポリシー

コントロールポリシー

Cisco SD-WANのコントロールポリシーはvSmartからルータに配信される
利用できるポリシーをまとめると以下

・コントロールポリシー *in/out制御はvSmartを主語として理解する
TLOC　IPsecトンネルの構成を変更する
Route　各拠点から収集したルート情報の配信フィルタリングやVRF間転送

・データポリシー
From-Service　LAN側から受信したトラフィックをコントロールする
From-Tunnel　IPsecトンネルから受信したトラフィックをコントロールする

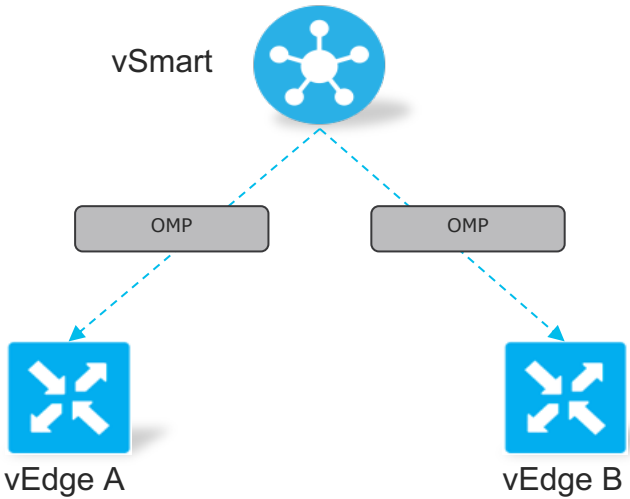
・App Aware Route(AAR)ポリシー
IPsecトンネル上のBFDによりロス・遅延・ジッタによる経路自動切り替え

・VPN Membershipポリシー
ルータが所属できるVPN（VRF）を制限することができる（拠点からのOMPルート制御）

コントロールポリシー概要と理解

Cisco SD-WANのコントロールポリシーを図解する
vSmartには大きく分けて2つのDBテーブルがある
- TLOCテーブル
- Routeテーブル

コントロールポリシーは2つのテーブルの受信ルール・送信ルールを制御する



TLOC

System-IP	Global-IP	Local-IP	Etc(color ..)
1.1.1.1(A)	x.x.x.x	xx.xx.xx.xx	gold
1.1.1.2(B)	y.y.y.y	yy.yy.yy.yy	gold
1.1.1.2(B)	z.z.z.z	zz.zz.zz.zz	silver

Route

System-IP	Prefix	VPN(VRF)	Etc(Origin..)
1.1.1.1(A)	prefix/maskA	1	bgp
1.1.1.2(B)	prefix/maskB	1	ospf
1.1.1.2(B)	prefix/maskB	2	eigrp

データポリシー

Cisco SD-WANのデータポリシーもvSmartからルータに配信される
データポリシーの機能をまとめると以下

・トラフィックアプリ識別とマッチング
IPアドレス、ポート番号、DSCPなどの情報から
DPI/NBAR2のシグニチャーから

・NAT DIA
マッチしたトラフィックに対し、NATもしくはブレイクアウトアクションを実行

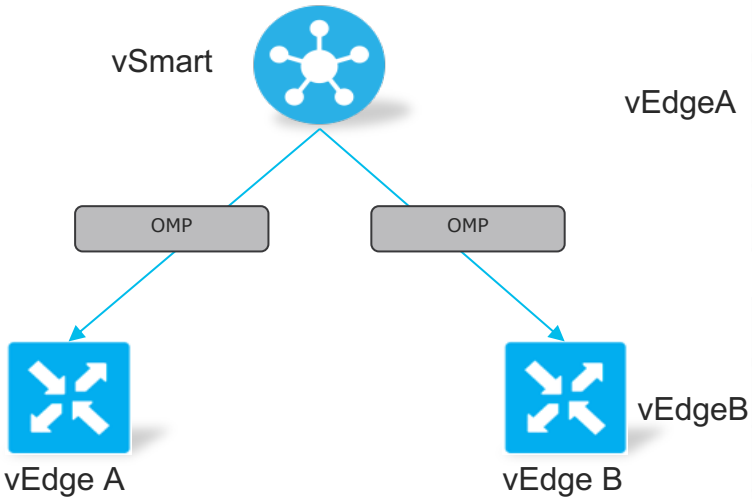
・QoS
マッチしたトラフィックに対し、クラシフィケーション、ポリシング、マーキング

・FEC / PAD
マッチしたトラフィックに対し、パケットロス対策

・etc (service-chaninng ..)

データポリシー概要と理解

Cisco SD-WANのデータポリシーを図解する
配信されたデータポリシーはルータのメモリ上（Configではない）に展開され
ルータが受信したトラフィックフローに対してアクションが実行される
ACLと同じように上からチェックする　上でヒットしたものは下のポリシーは見ない



vEdgeA

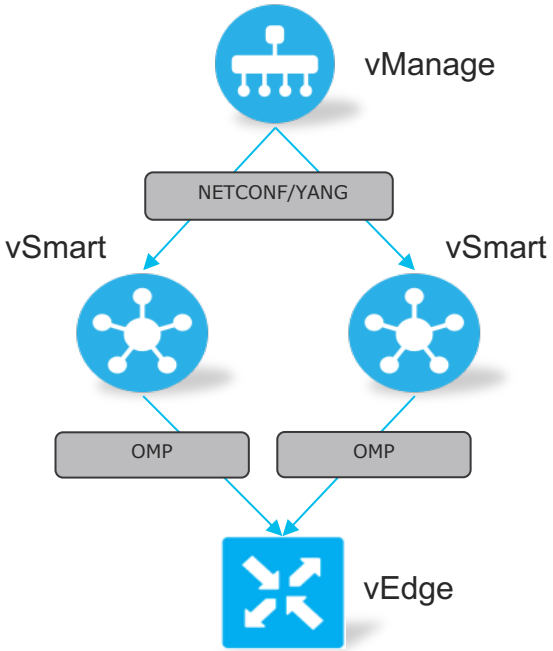
VPN	Match	Action	Etc(dia ..)
1	prefix/maskA	accept	-
1	Port 21	drop	-
1	youtube	accept	Dia(nat)

vEdgeB

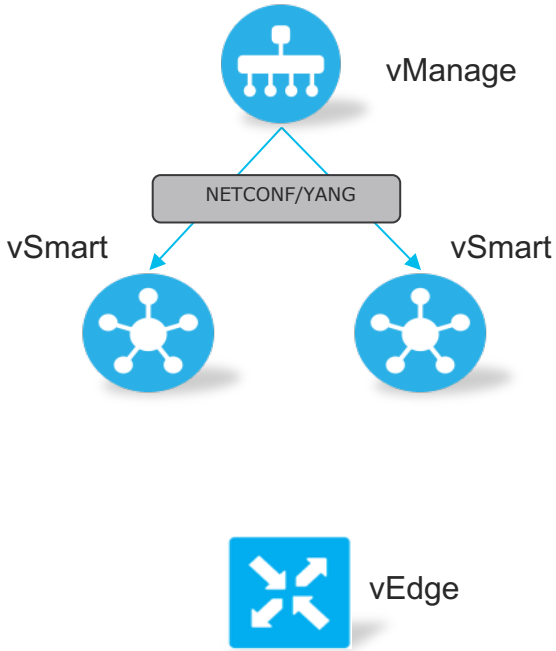
VPN	Match	Action	Etc(dia ..)
1	prefix/maskA	accept	-
1	Port 21	drop	-
2(Guest)	All	accept	Dia(nat)

各種ポリシーとルータのConfig

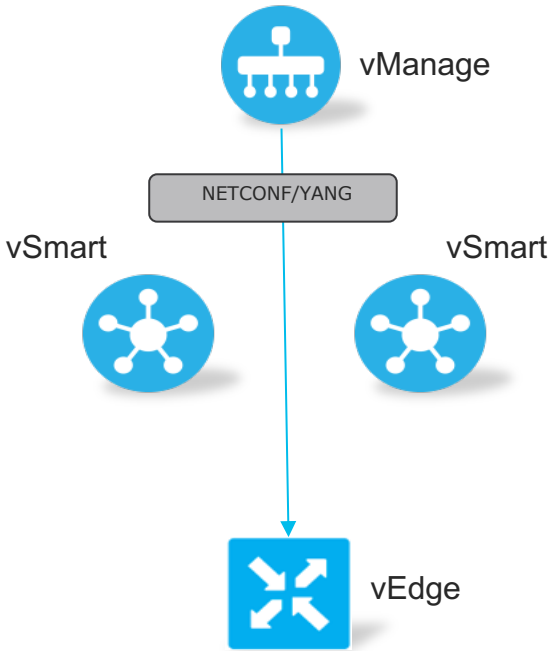
Data Policy
App Aware Routing Policy



Control Policy
VPN Membership Policy



Configuration/Local Policies



セキュリティポリシー

アプリケーション認識型のエンタープライズ ファイアウォール
（1400 以上のアプリケーション）

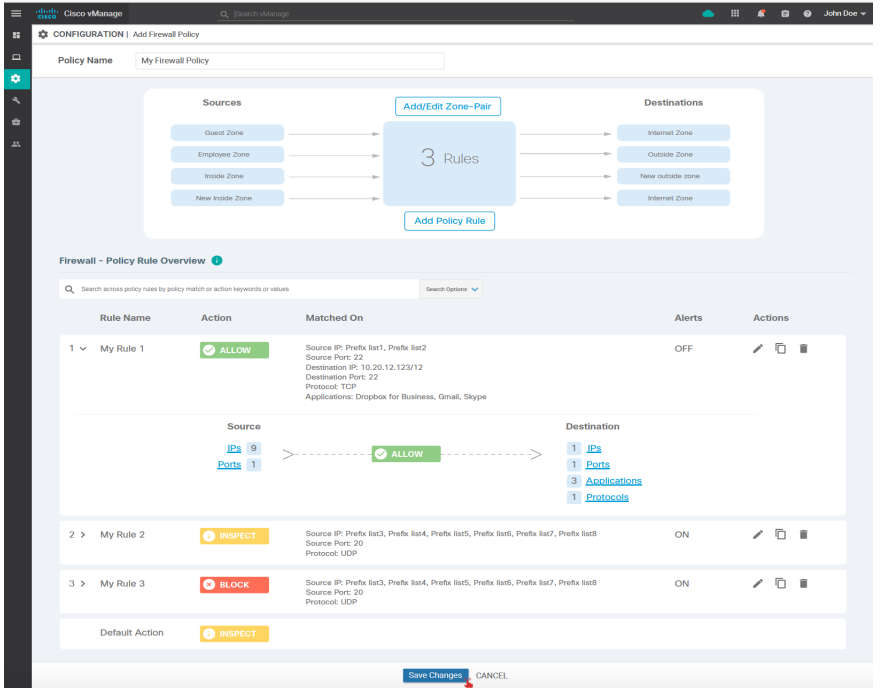
TALOS シグネチャに裏打ちされた IPS Snort エンジン

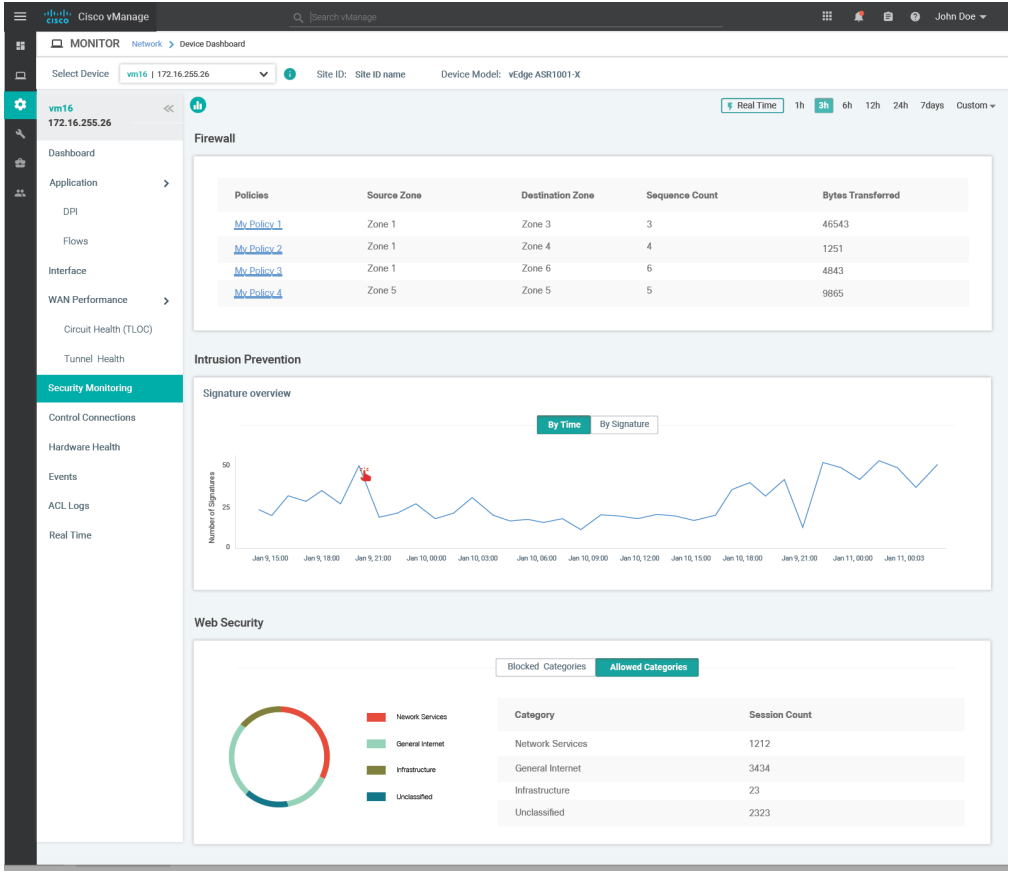
82 以上の Web カテゴリを使用する URL フィルタリング

Cisco Umbrella による防御の最前線

Talos を利用した高度なマルウェア防御（AMP と ThreatGRID）

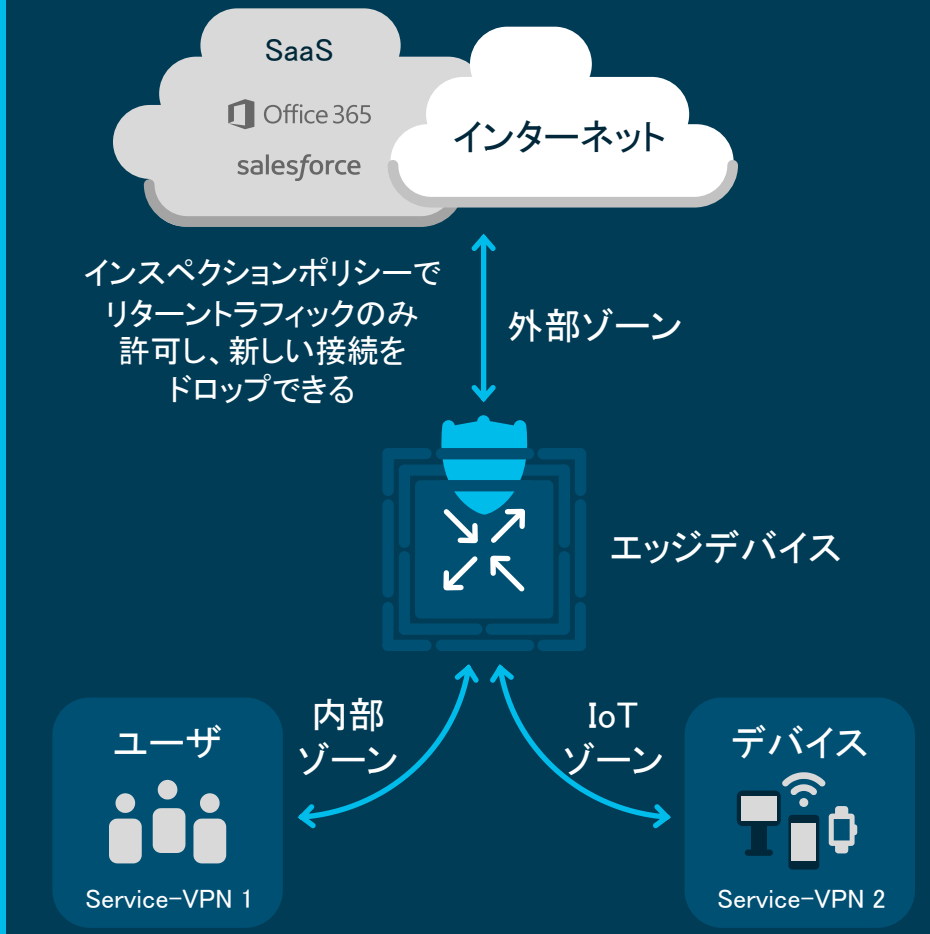
vManage GUIでの一括管理が可能





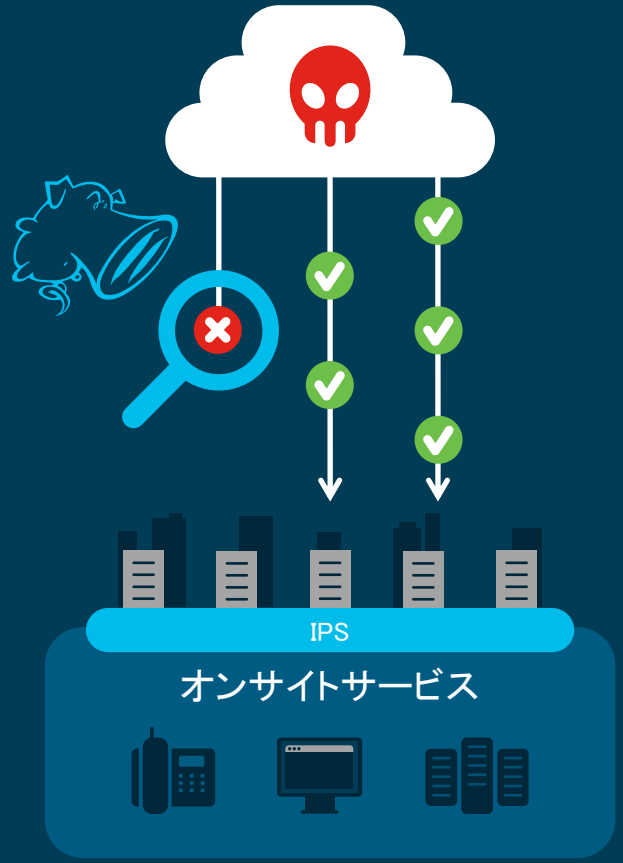
アプリケーション認識型ファイアウォール

- カテゴリまたは個々のアプリケーション別のアプリケーションの可視性ときめ細かい制御
- 1400 以上のアプリケーションを分類
- 脅威のラテラルムーブメントを防止（プリントサービスで従業員ネットワークへの新しい接続が確立されないなど）
- PCI コンプライアンス



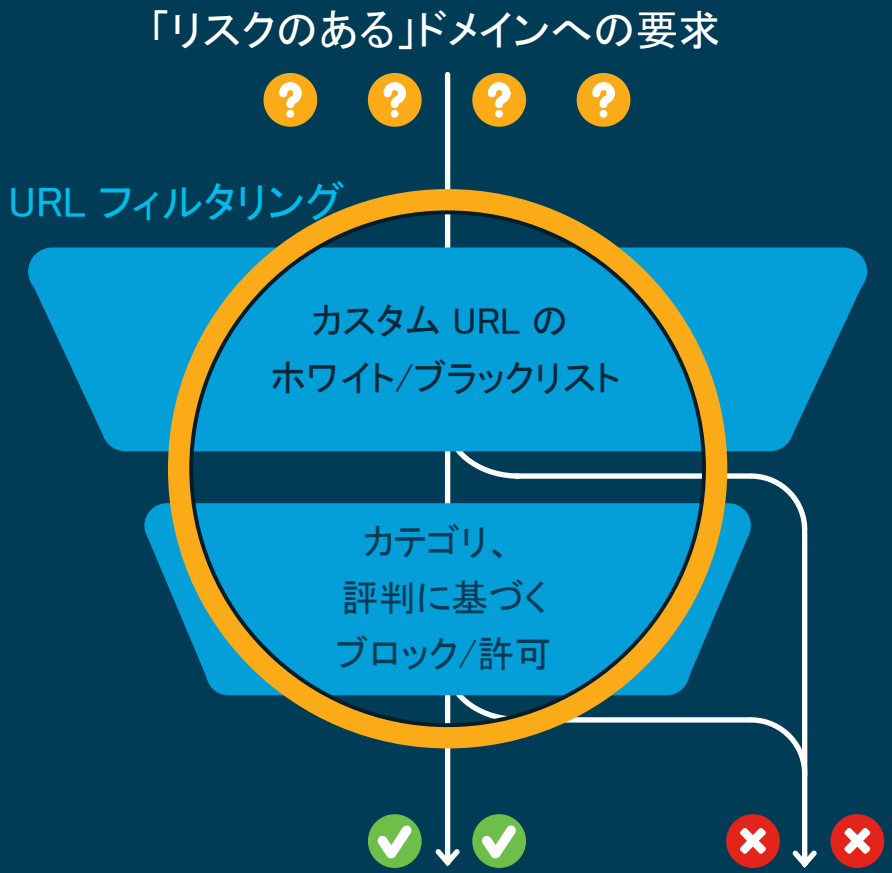
侵入防御（IPS）

- Snort IPS は世界中で最も広く導入されているエンジン
- 自動的に更新されたグローバル脅威インテリジェンス（TALOS）シグネチャで裏付けされている
- シグネチャホワイトリストのサポート
- リアルタイムのトラフィック分析
- PCI コンプライアンス



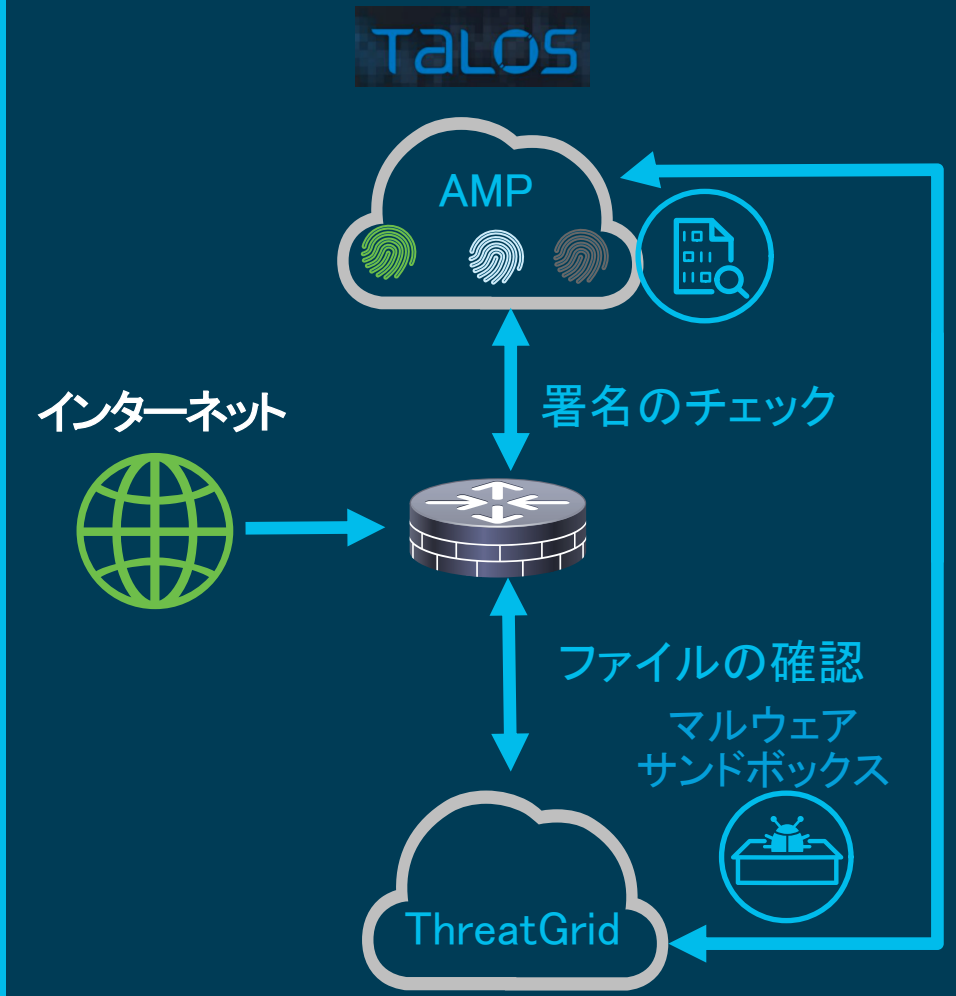
URL フィルタリング

- 82 以上の Web カテゴリと動的更新
- Web レピュテーションスコアに基づいたブロック
- カスタムのブラックリストとホワイトリストを作成
- カスタマイズ可能なエンドユーザ通知



Advanced Malware Protection（AMP）

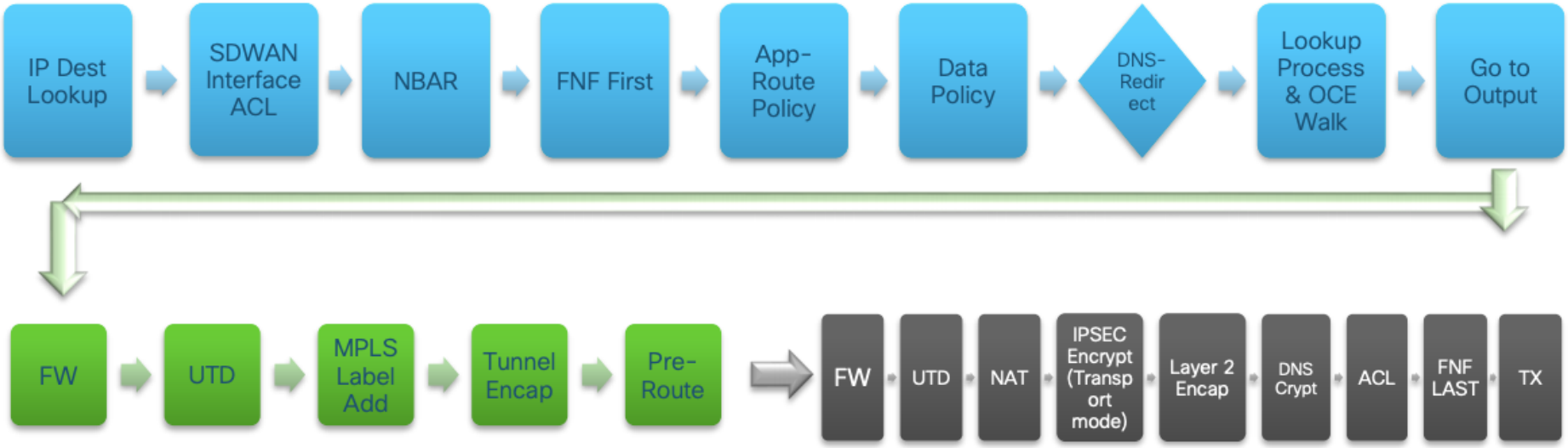
- AMP との統合
  - ファイルレピュテーション
  - ファイルレトロスペクション
- ThreatGrid との統合
  - ファイル分析
- 重要な脅威インテリジェンス（Talos）による裏付け



DNS セキュリティ/ セキュア インターネット ゲートウェイ

- DNS 要求に基づくブロックにより、マルウェア、フィッシング、および容認できない要求に対するセキュリティの有効性を実現
- DNScrypt をサポート
- ローカルのドメインバイパスオプション
- https 復号をサポート
- インテリジェントプロキシ

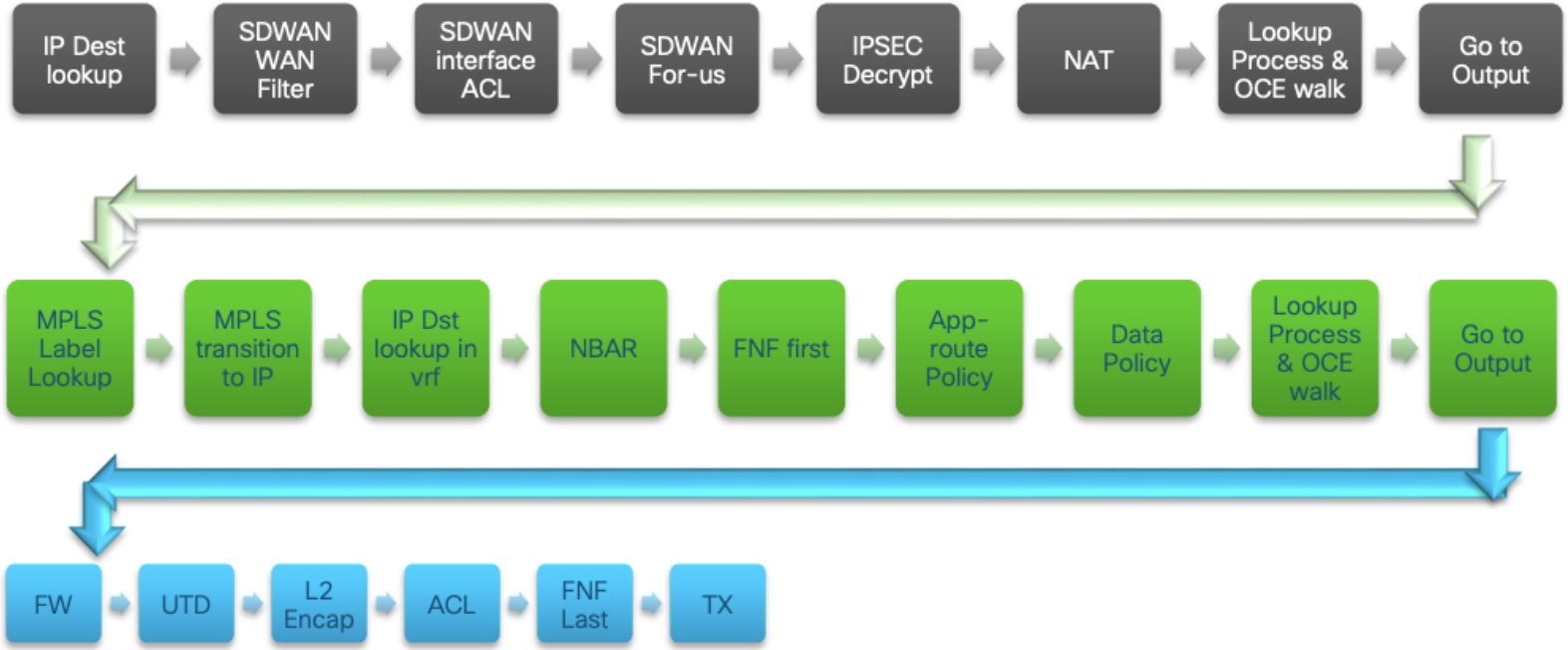
パケットの処理順序　LAN -> WAN



UTD: IPS->URL-F->AMP/TG *

Color Coding: LAN Interface | Tunnel Interface | WAN Interface

パケットの処理順序　WAN -> LAN



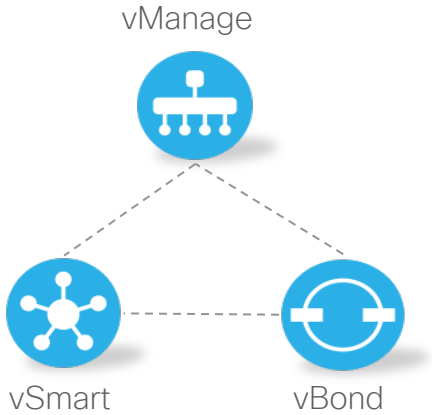
UTD: IPS->URL-F->AMP/TG *

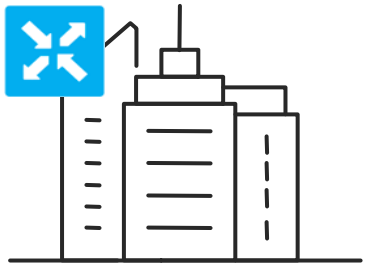
Color Coding: LAN Interface | Tunnel Interface | WAN Interface

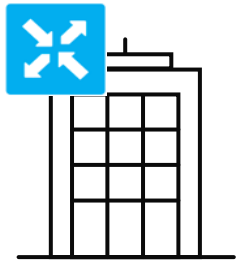
マイグレーション

マイグレーションシーケンス

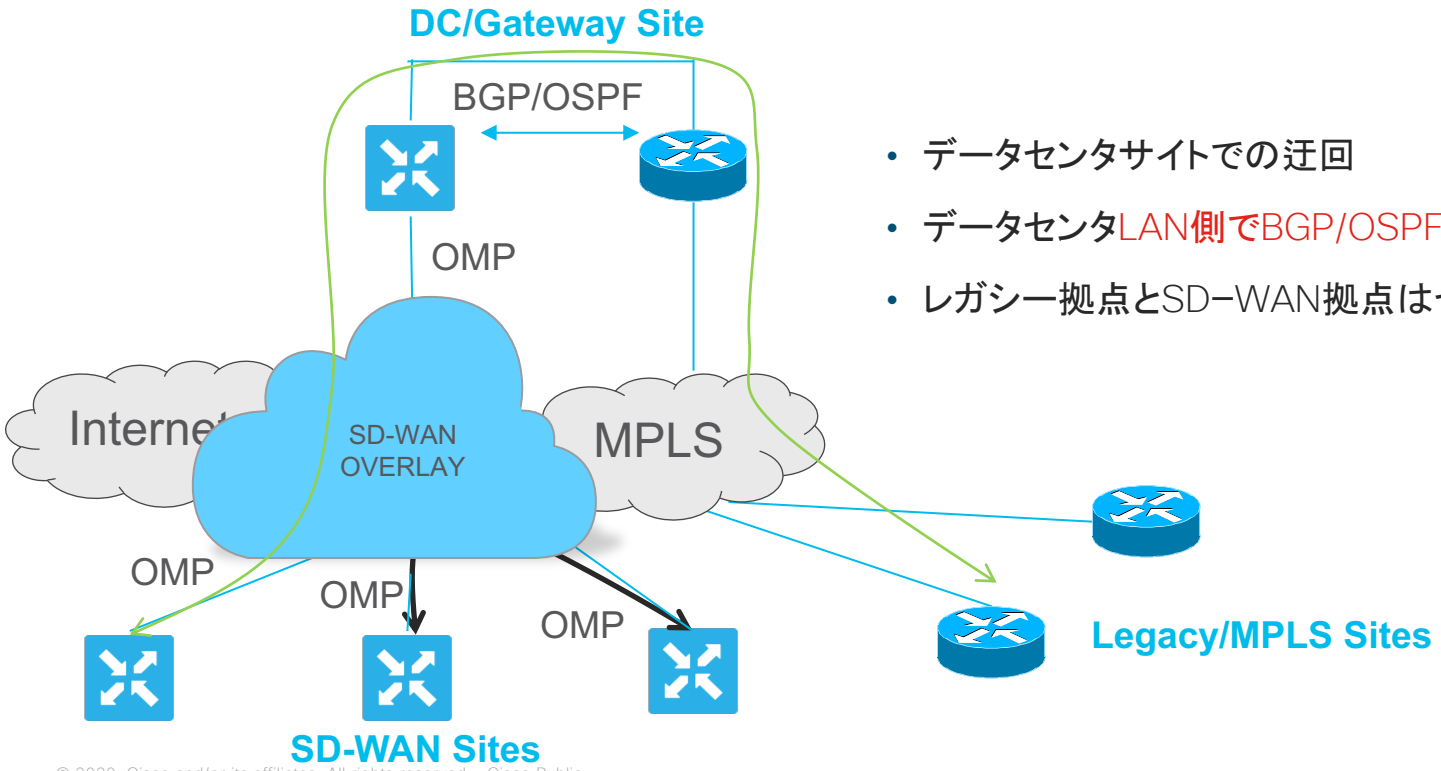
Controllers → Datacenter → Branches





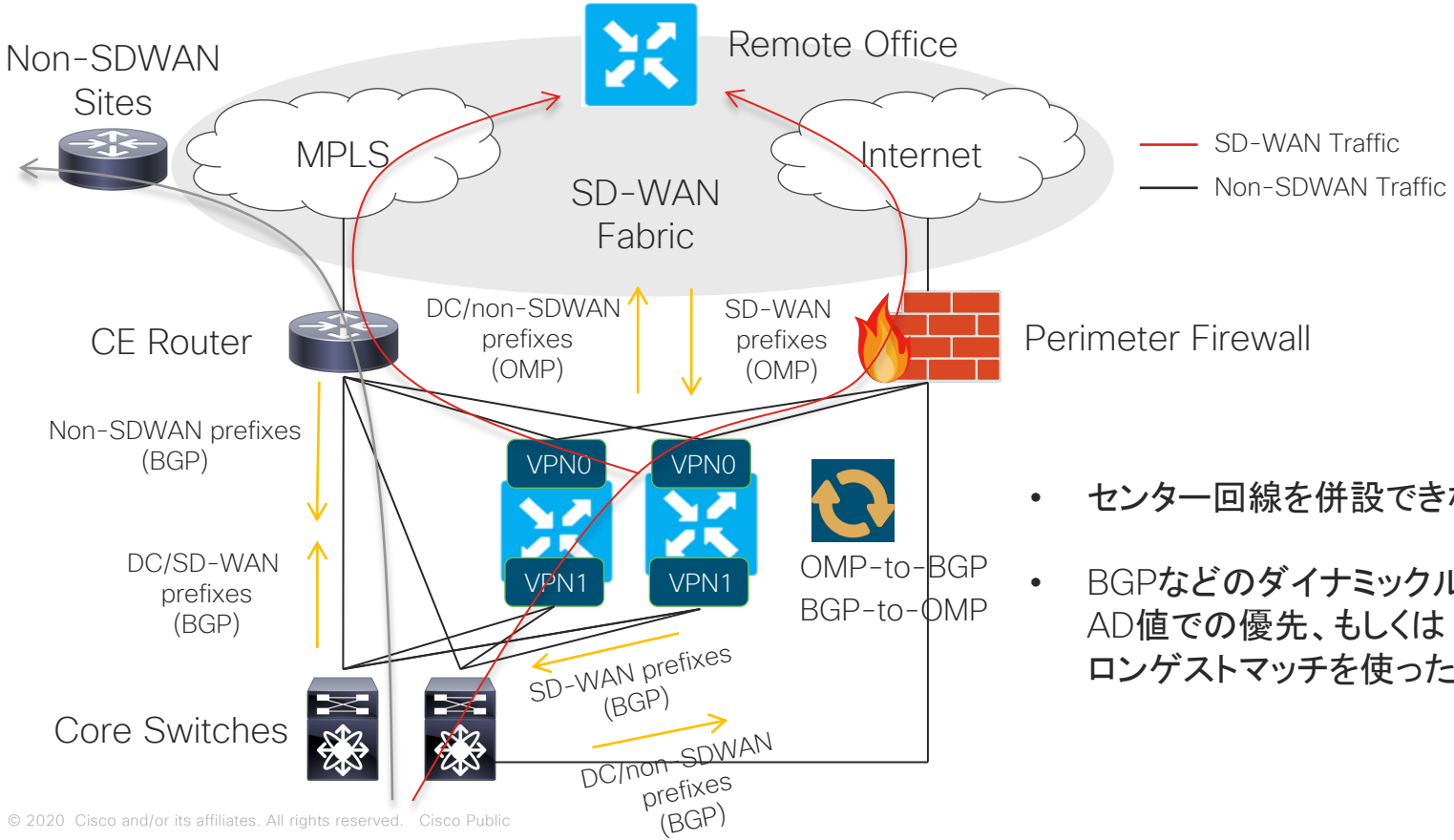


SD-WAN拠点とレガシー拠点との接続



- データセンタサイトでの迂回
- データセンタLAN側でBGP/OSPFによるHUB化
- レガシー拠点とSD-WAN拠点はセンタHUBを経由

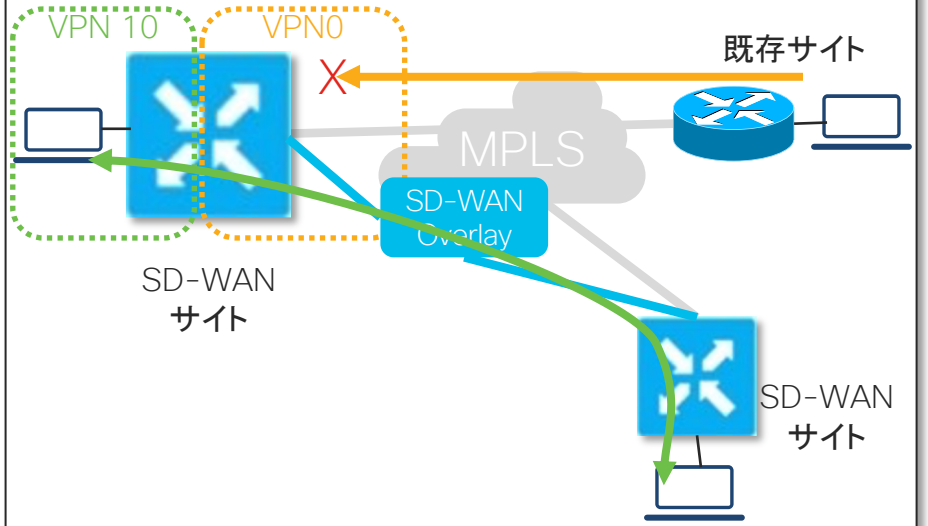
データセンタ



- センター回線を併設できない場合
- BGPなどのダイナミックルートの AD値での優先、もしくは ロンゲストマッチを使った構成

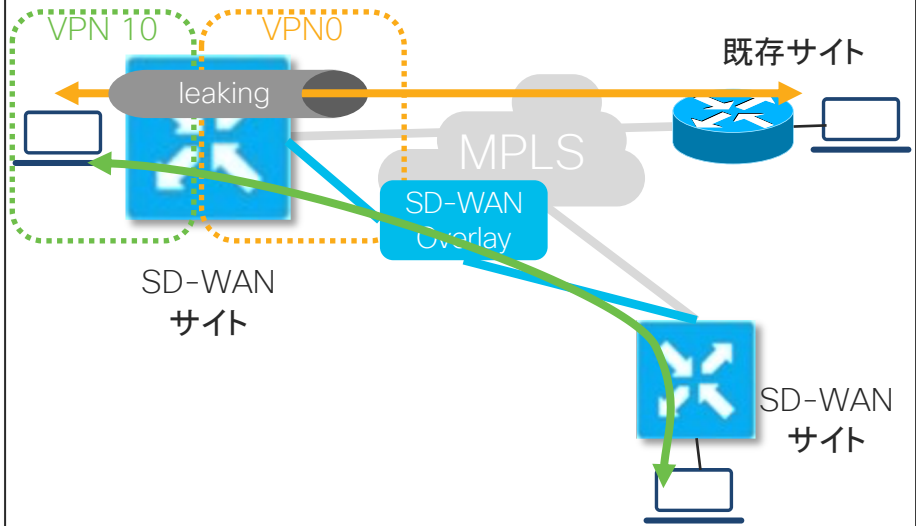
VPN0 route leaking機能

今までの課題



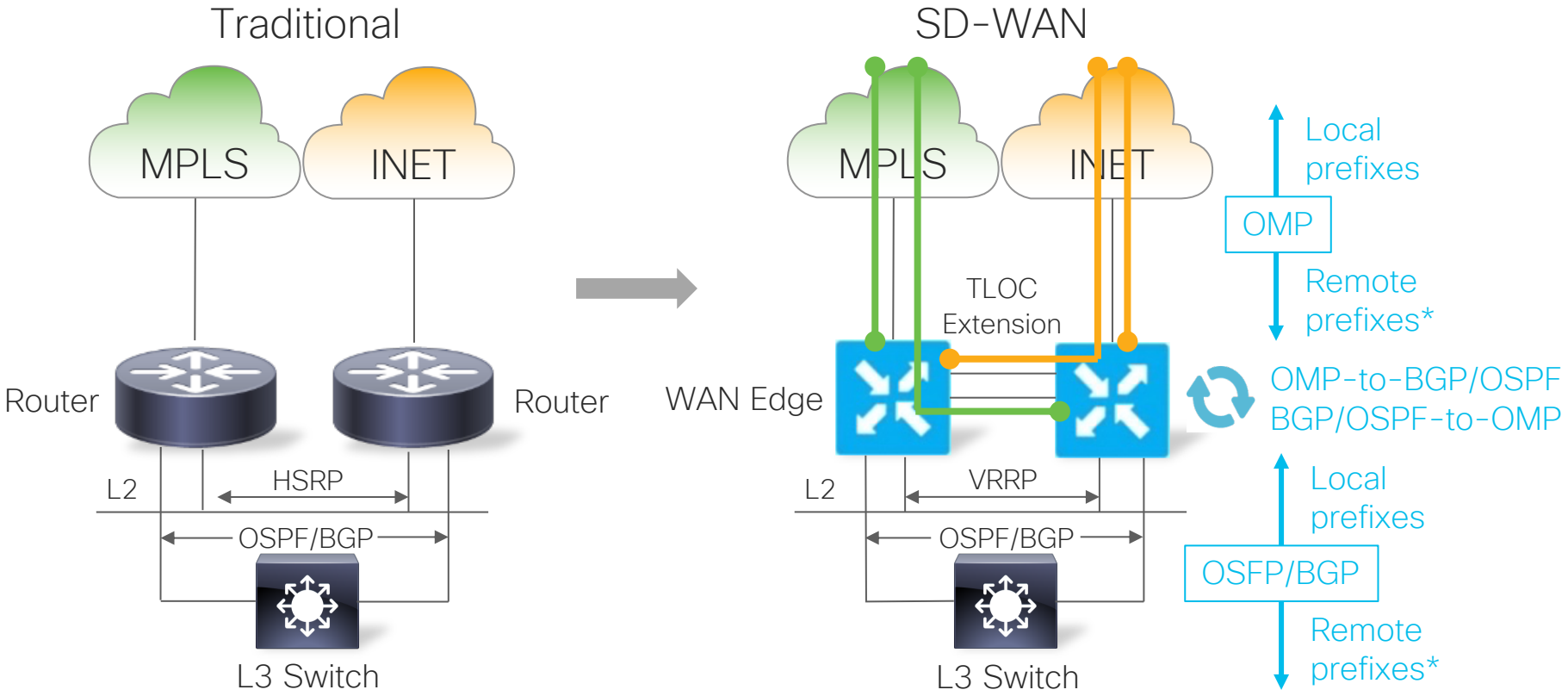
VPN0とVPN10はルーティングできないため、既存サイトとSD-WANサイトは通信が出来ない

VPN0 route leaking



route leakingによりVPN0とVPN10の間のルーティングを行い、既存サイトとSD-WANサイトは通信を実現

二重化拠点



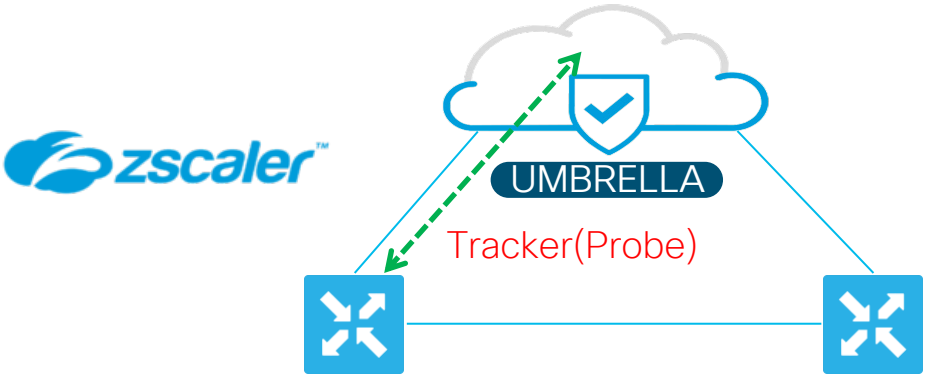
* SD-WAN and non-SDWAN

SD-WAN Tunnel

セキュアクラウドとの接続

Umbrella SIG接続

Cisco SD-WANとUmbreallaSIGとの接続は近日、自動接続がサポートされる
スタンダードIPsecの各種パラメータや接続先情報については以下URLを参照
vEdge
https://docs.umbrella.com/umbrella-user-guide/docs/add-a-tunnel-viptela
cEdge*修正予定
https://docs.umbrella.com/umbrella-user-guide/docs/add-a-tunnel-cisco-isr
ヘッドエンド（接続先）
https://docs.umbrella.com/umbrella-user-guide/docs/cisco-umbrella-data-centers

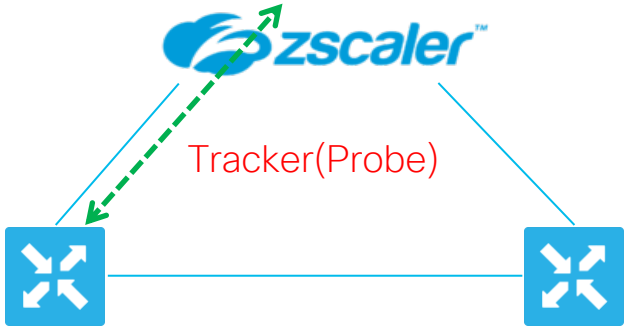


- vEdgeとcEdgeとでパラメータが違うので注意
- cEdgeは”Mutiplexing”設定に注意
  *17.2.x以降の用語
- 二重化と切り替え手法は
  Tracker(Probe)の利用を推奨

zScaler接続

Cisco SD-WANとzScalerとの接続も近日、自動接続がサポートされる予定
スタンダードIPsecの各種パラメータや接続先情報については以下URLを参照
vEdge/cEdge
https://www.zscaler.com/resources/solution-briefs/partner-viptela-cisco-sd-wan-deployment.pdf

ヘッドエンド（接続先）
https://ips.zscaler.net/cenr



- vEdgeとcEdgeとでパラメータが違うので注意
- cEdgeは”Mutiplexing”設定に注意
  *17.2.x以降の用語
- zScalerダウン検知専用のHTTP URIを利用
  http://<zsdomain>.zsccloud.net/vpntest

IaaS接続

Cloud onRamp for IaaS – Gateway VPC/VNET

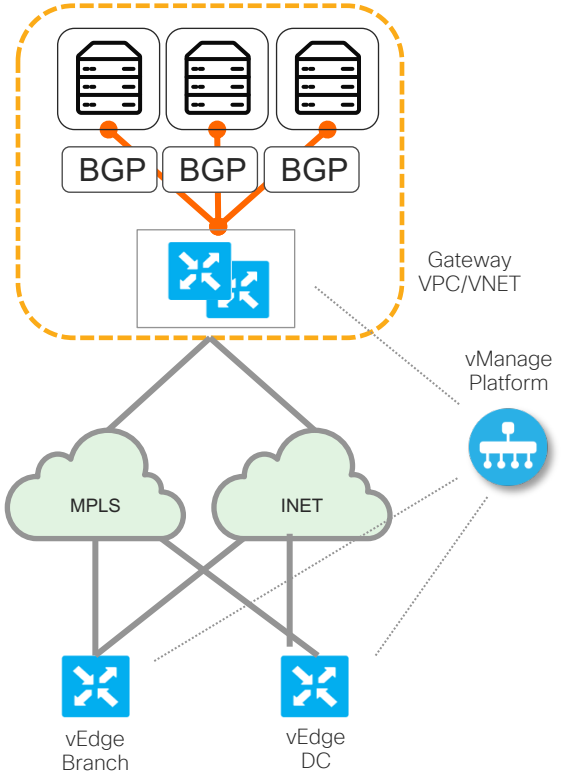
一対のvEdgeルーターインスタンスが
Amazon VPCまたはMicrosoft Azure VNETで展開

ゲートウェイVPC / VNET 標準IPSecトンネルが、
各ホストVPC / VNETに自動接続

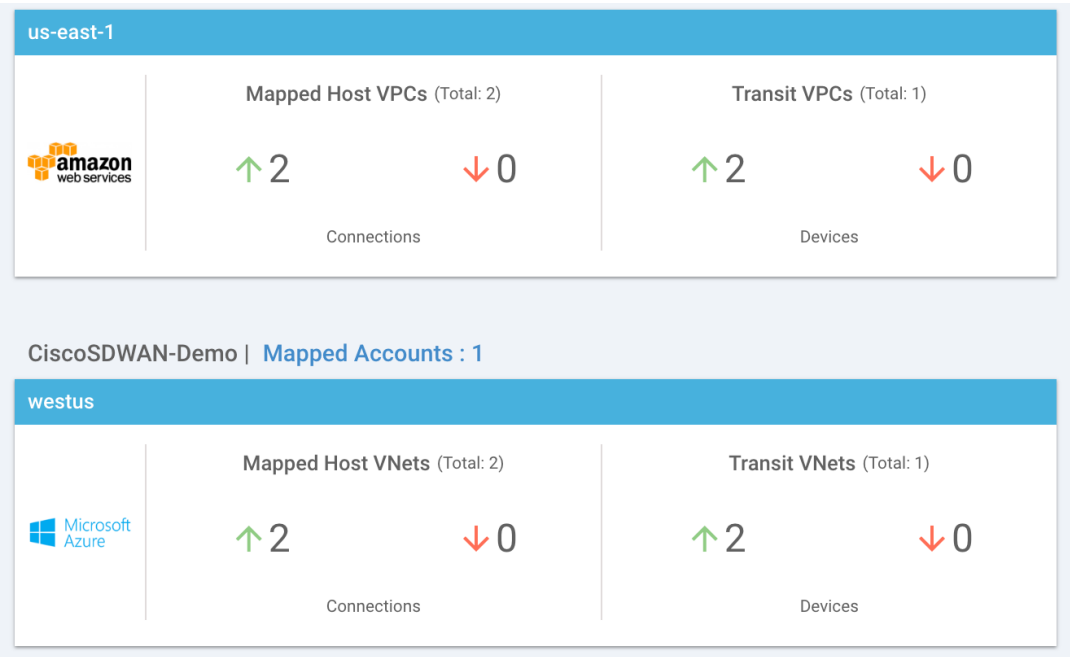
接続の冗長性にBGPが使用されIaaS内のルートは
OMPを経由してネットワーク全体に伝搬

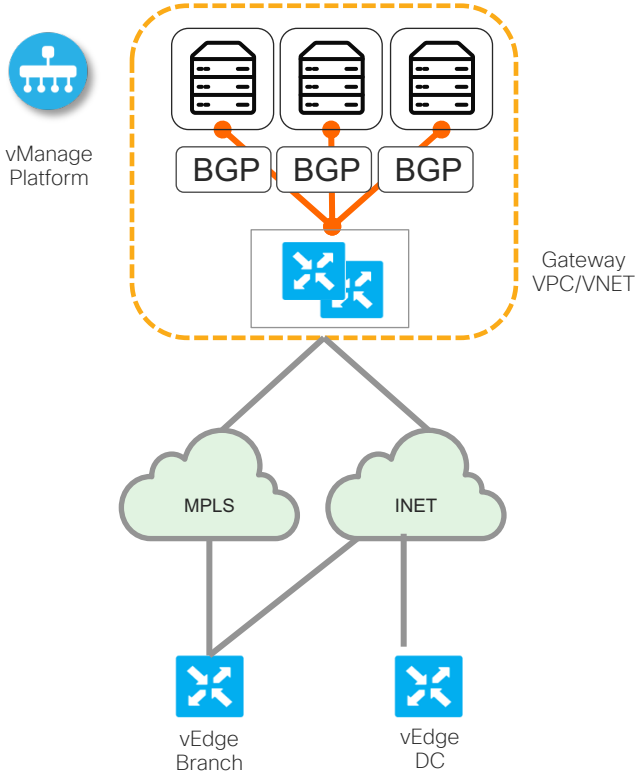
上記の一連の設定がvManage上のGUIで自動化

AWS /Azure　の認証情報(API-key)を事前に確認

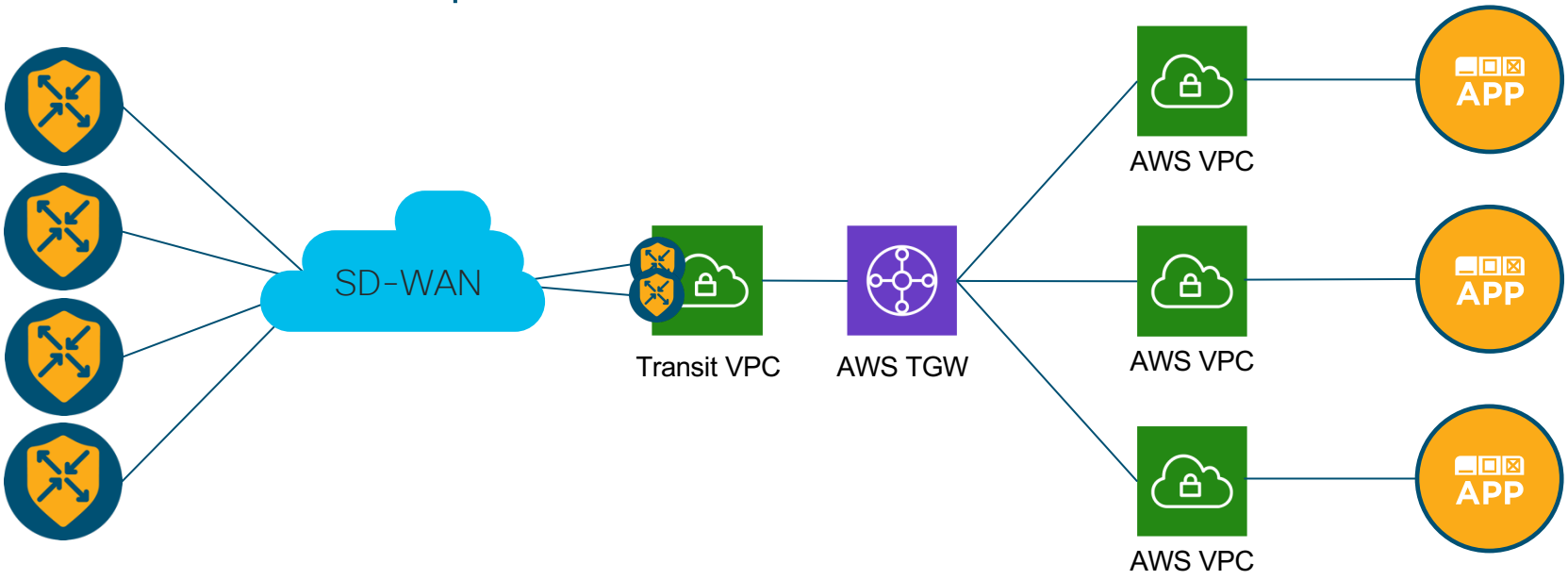


Cloud onRamp for IaaS GUI





Cloud on Ramp IaaS AWS TGW collab

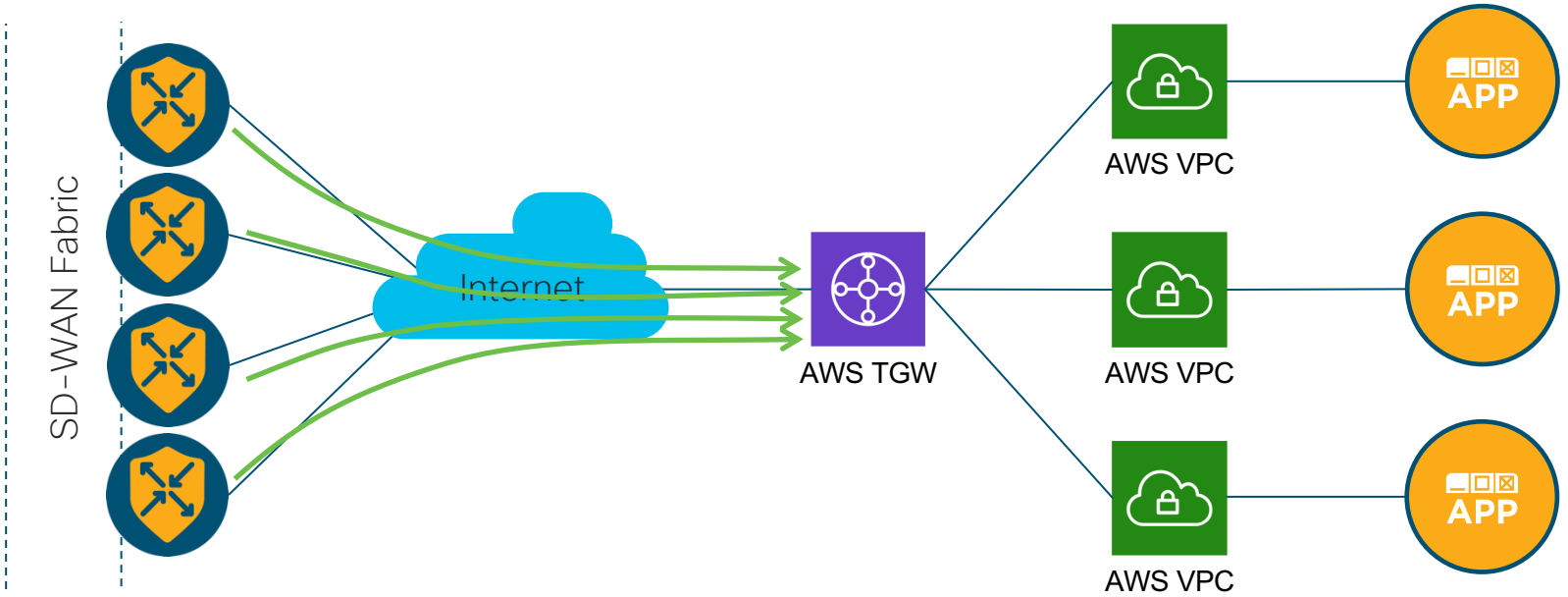


拠点ルータが新規に作成されたVPC経由でAWS TGWに直接接続するパターン

ルータはSD-WAN-IPsecによって接続されるためAppQoEなど高速化機能が利用できパフォーマンスに優れる

Target: 17.4

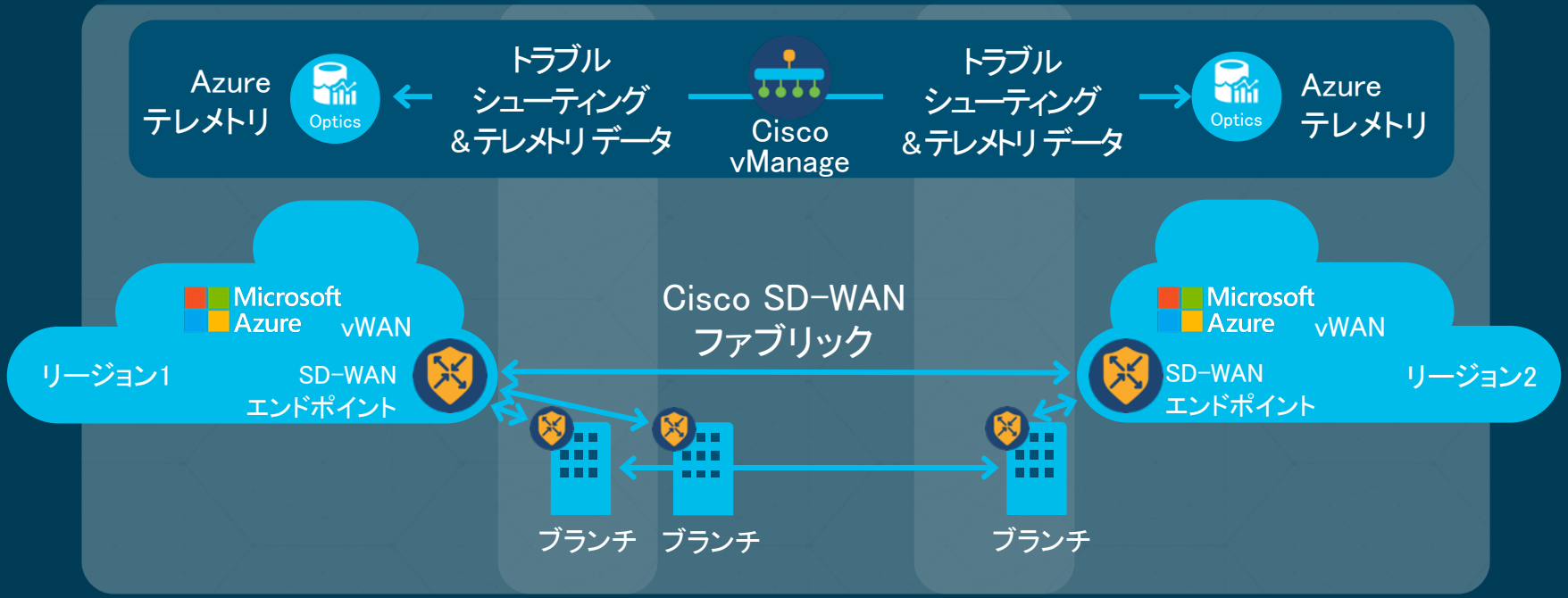
Cloud on Ramp IaaS AWS Direct TGW



拠点ルータがAWS TGWに直接接続するパターン

ルータにはスタンダードIPsecのConfigが自動で適用される

Cloud on Ramp IaaS Azure

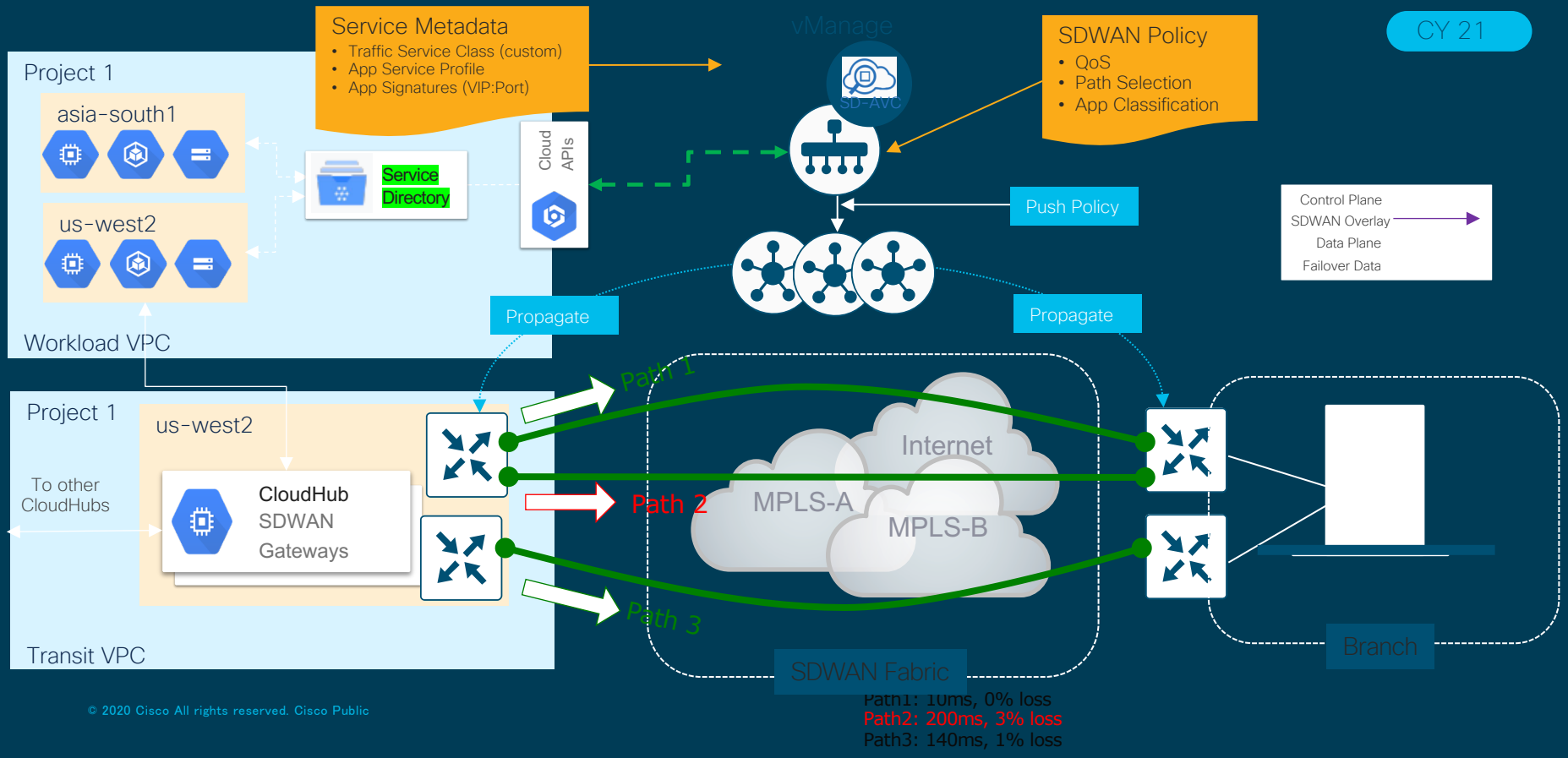


vWANハブ上の
CSR SD-WAN エンドポイント

vWAN ハブとの
自動ピアリング

vWAN と vManage 間のポリシー同期

Cloud on Ramp IaaS GCP

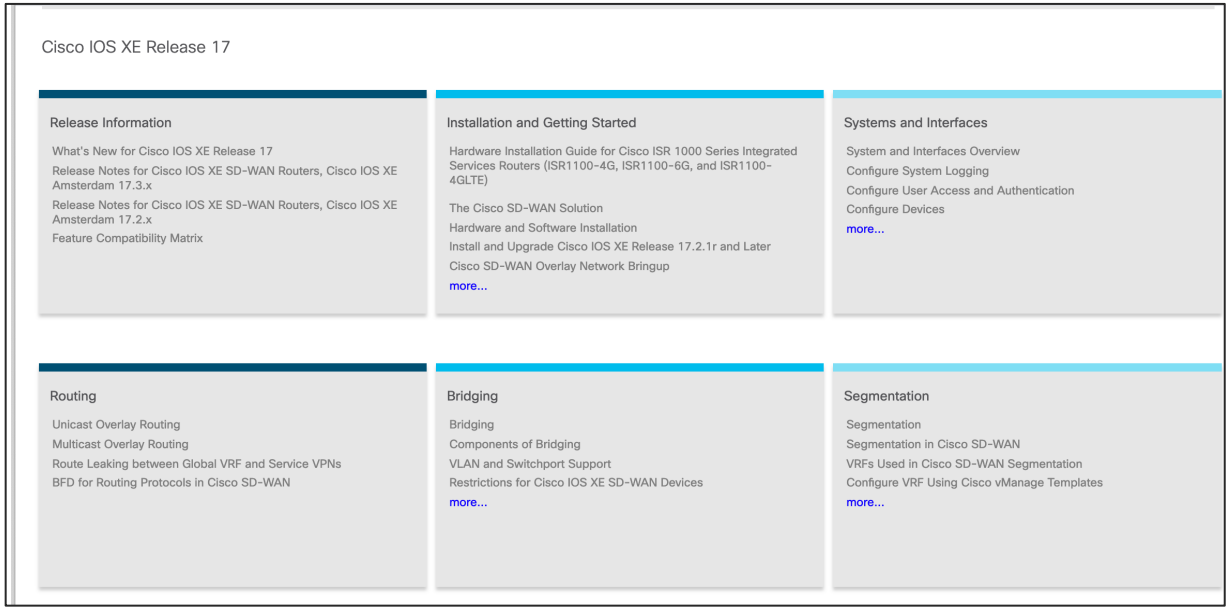


Q&A

SD-WANのマニュアルが見やすくなりました

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/config/ios-xe-sdwan17.html

※設定マニュアルはこちらをご参照ください




CISCO