Cisco SD−WAN アップデート
お役立ち機能と新型ルータのご紹介

Cisco Webinar

2020年11月26日

シスコシステムズ合同会社 / EN アーキテクチャー システムズ エンジニアリング
テクニカル ソリューションズ アーキテクト
吉野恵一

セッション概要

ビデオ会議やMS365などのクラウド活用が当たり前になりつつある現在において、アプリケーションのレスポンスタイムの速さは非常に重要な課題となっています。
このセッションでは、ユーザ体感を向上させるお役立ち機能をご紹介するとともに、10月下旬に発表されたばかりの新ルータもご紹介します。

Agenda

- Application Quality of Experience (AppQoE) とは?
  - Application Aware Routing (AAR)
  - Forward Error Correction (FEC) / Packet Duplication
  - TCP Optimization
  - SD-AVC Cloud Connector for MS365
- Cisco エンタープライズルータ新製品 Catalyst 8000 シリーズ

AppQoE (**App**lication **Q**uality **o**f **E**xperience)
アプリケーションレベルでの体感品質の向上

SD-WANにおけるApplication Quality of Experience (AppQoE)は、
以下のようなWANの問題を解決する**包括的な機能セット**です。

WAN回線上のパケットロス対策

最適化されていない帯域の利活用、高遅延回線への対応

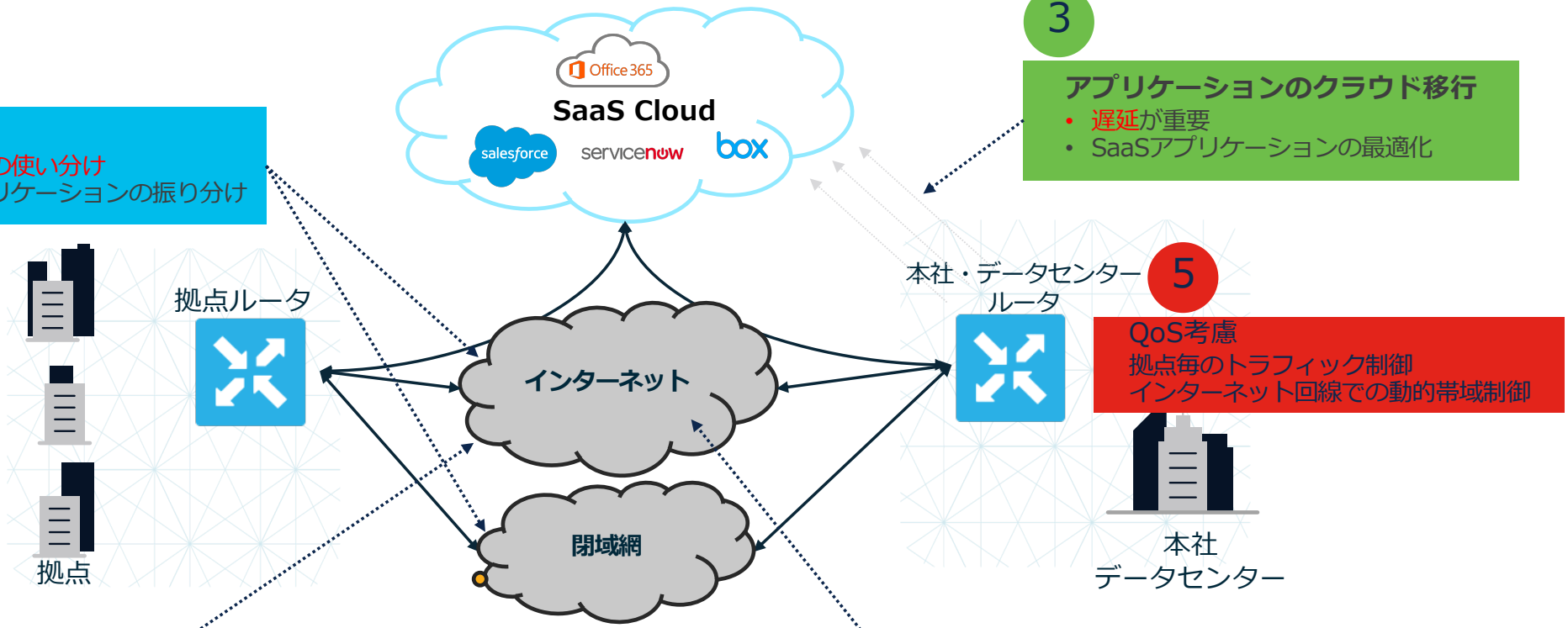
クラウドアプリケーションのパフォーマンス不足を解消

アプリケーションの可視化

SD−WANにおける新しいチャレンジ

1

With SD-WAN
- マルチパスによる回線の使い分け
- 回線品質に基づくアプリケーションの振り分け



3

アプリケーションのクラウド移行
- 遅延が重要
- SaaSアプリケーションの最適化

5

QoS考慮
拠点毎のトラフィック制御
インターネット回線での動的帯域制御

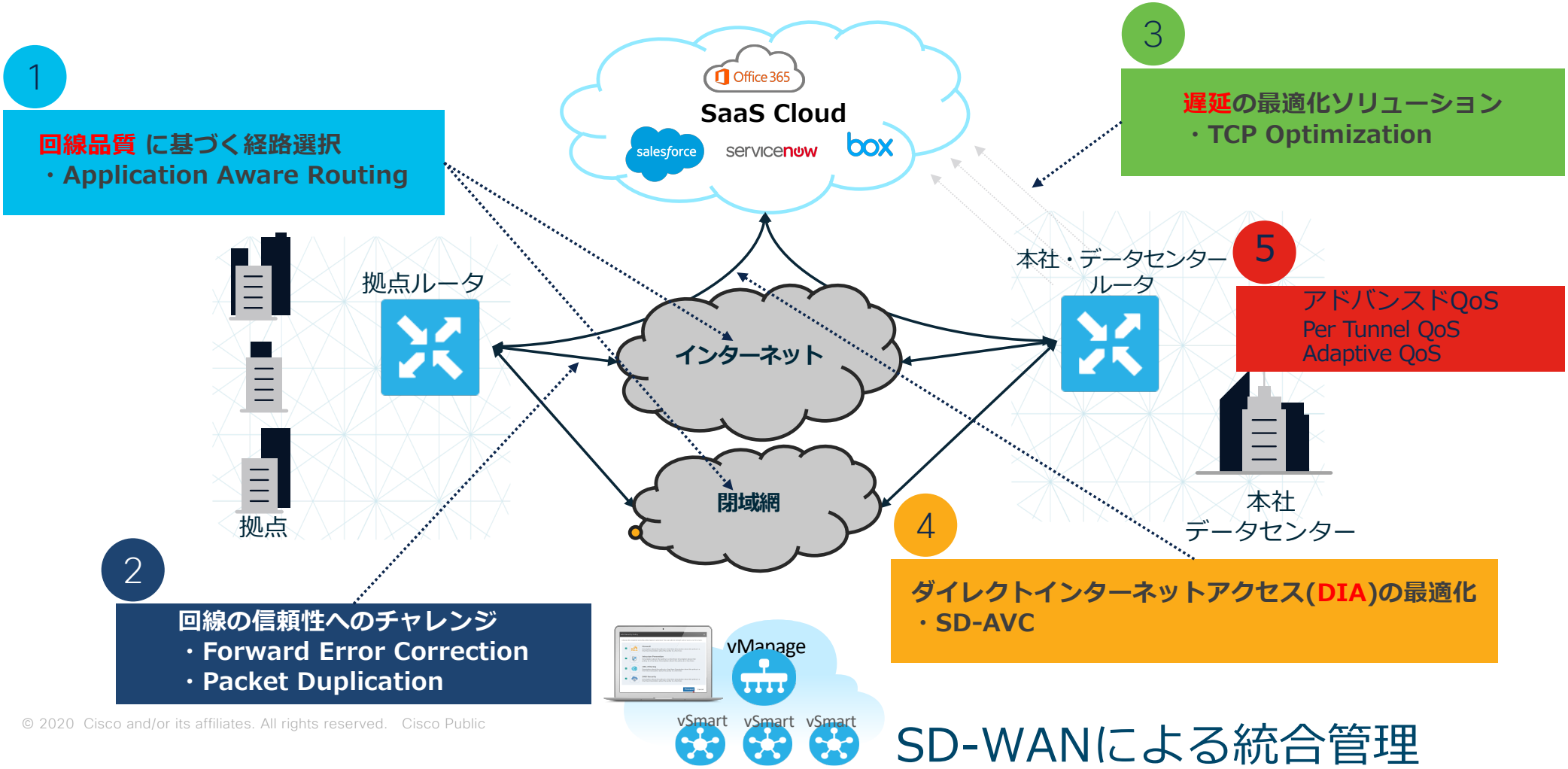
2

インターネット回線の重要通信への利用
- 回線の信頼性へのチャレンジ

4

インターネットトラフィックによる帯域消費
- DIAによるコスト削減

AppQoEによるソリューション



SD-WANによる統合管理

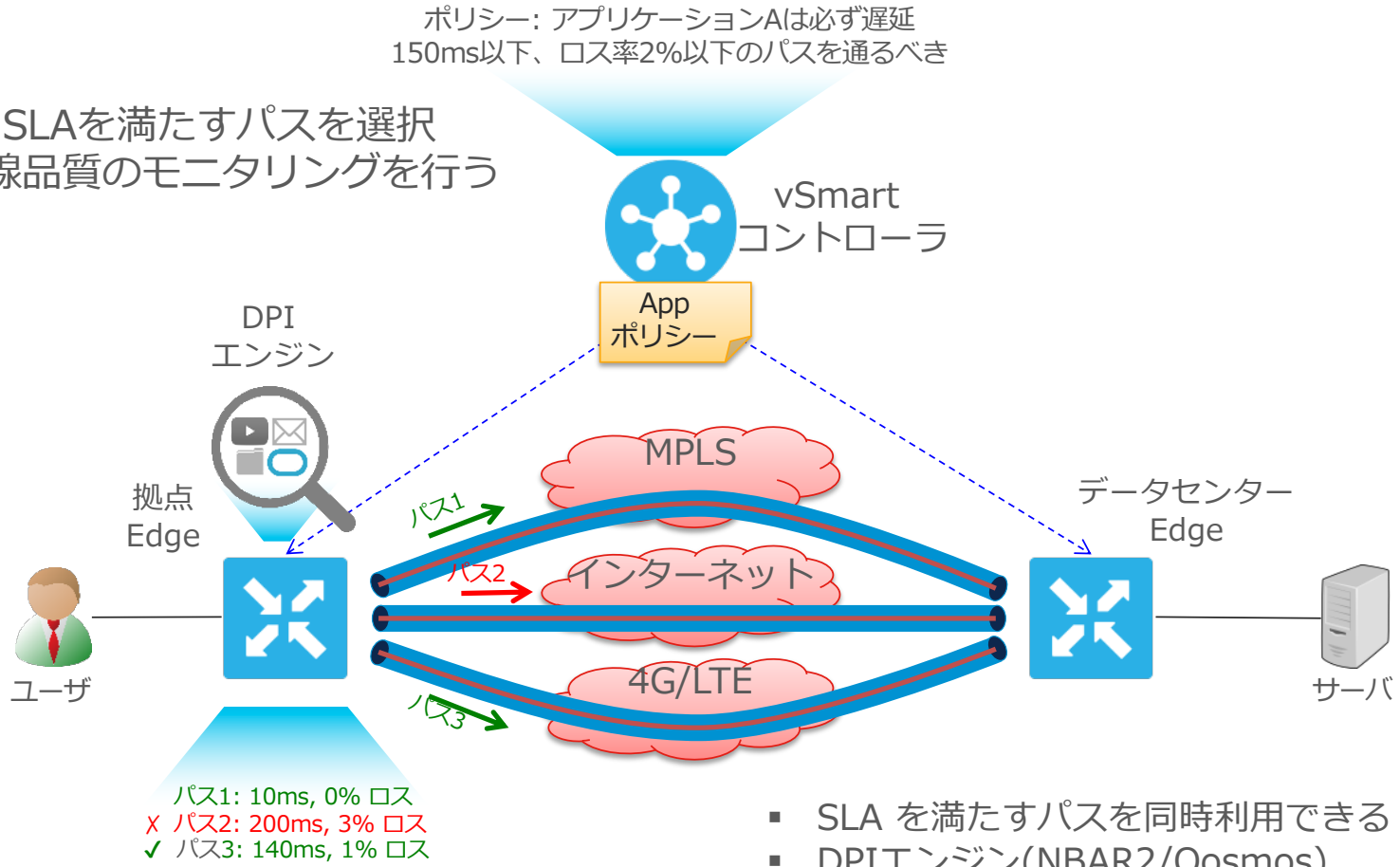
AppQoEによるソリューション

1. Application Aware Routing
2. FEC/Packet Duplication
3. TCP Optimization
4. SD-AVC Cloud Connector for O365
5. Per Tunnel QoS / Adaptive QoS

1

Application Aware Routing (AAR)
回線の品質に基づく経路選択

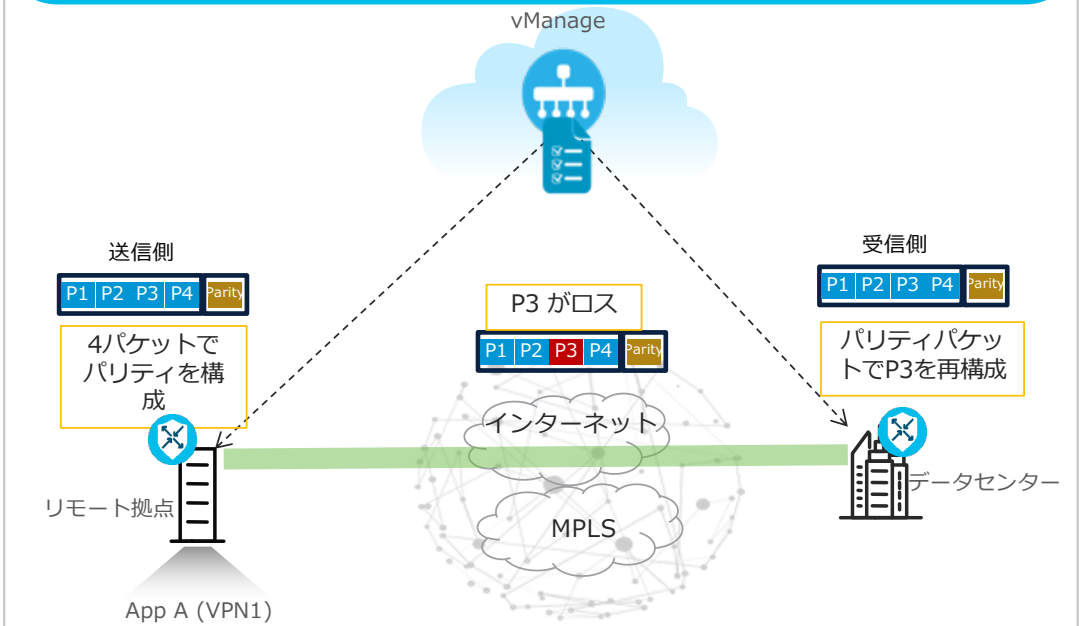
- アプリケーションごとにSLAを満たすパスを選択
- WAN Edge ルータが回線品質のモニタリングを行う
  - ロス率
  - 遅延
  - ジッター



- SLA を満たすパスを同時利用できる
- DPIエンジン(NBAR2/Qosmos)

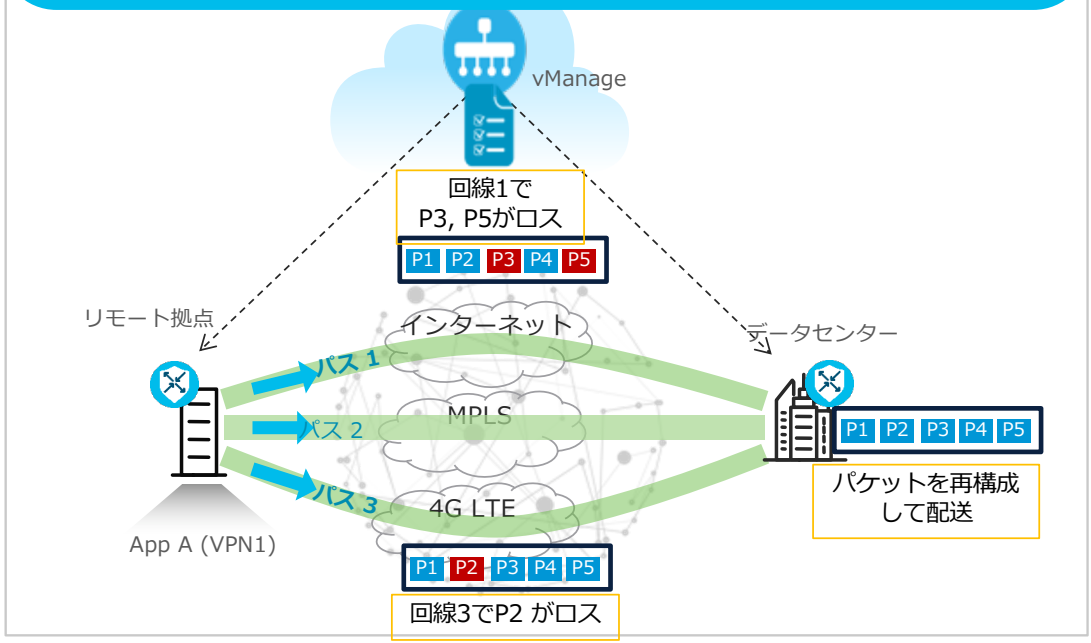
2 Forward Error Correction (FEC) / Packet Duplication
回線の信頼性向上 パケットロス対策

Forward Error Correction (FEC)



- 信頼性が不十分なWAN回線で、音声その他重要なトラフィックを安定的に配送したいときに
- 再送を削減し、スループット向上します

Packet Duplication



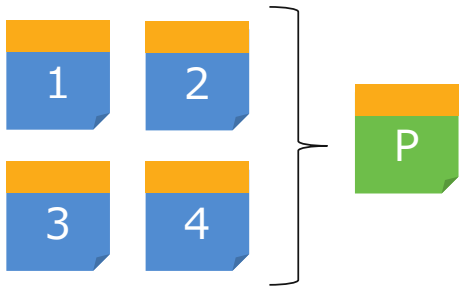
- 信頼性が不十分なWAN回線で、音声/ビデオの品質を向上したいときに
- パケットを複製して副系回線でも配送します

2

Forward Error Correction (FEC)

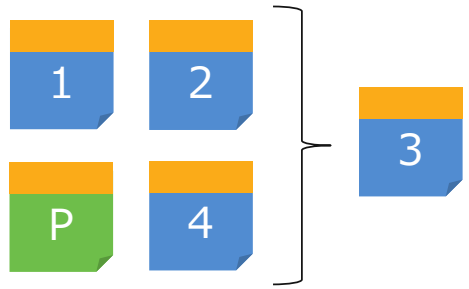
パケットロスをリストア

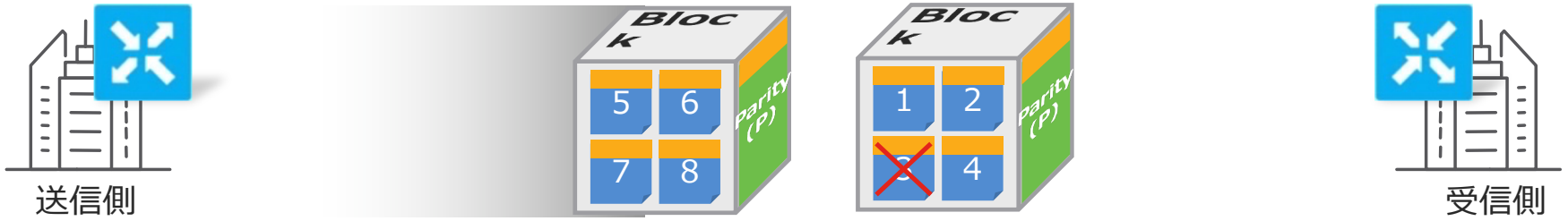
- パケットロスからデータを保護
- プロトコル(TCP/UDP)に依存せず有効
- トンネル毎に動作
- 複数のトランスポート対応
- 動的(必要な時だけ)発動も可能
- データポリシーで適用



注意:

- ユーザのデータトラフィックのみ適用し、BFDには適用されない
- パリティパケットのサイズはブロック中の最大サイズのパケットと同じ





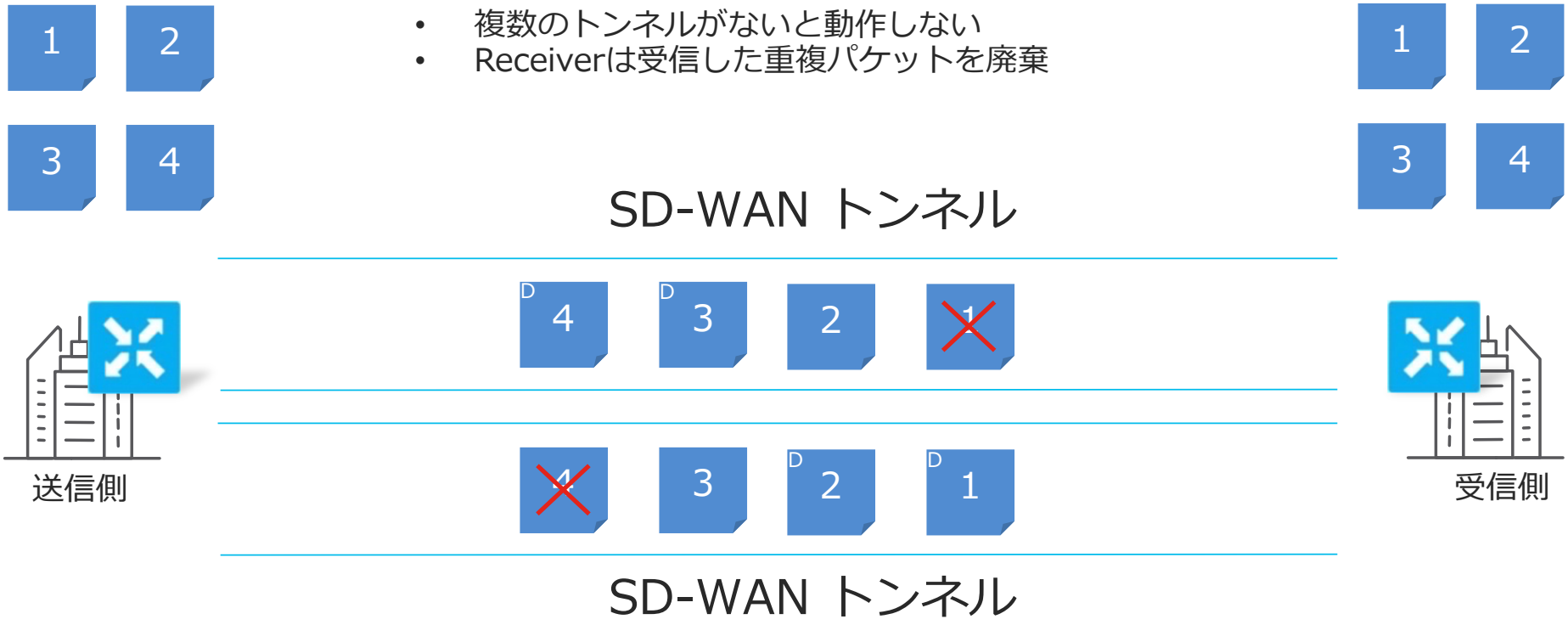
SD-WAN トンネル

FEC ヘッダー

2 Packet Duplication パケット複製

- パケットロスからデータを保護
- プロトコル(TCP/UDP)を問わず有効
- 複数のトンネルを跨いで動作
- データポリシーで適用

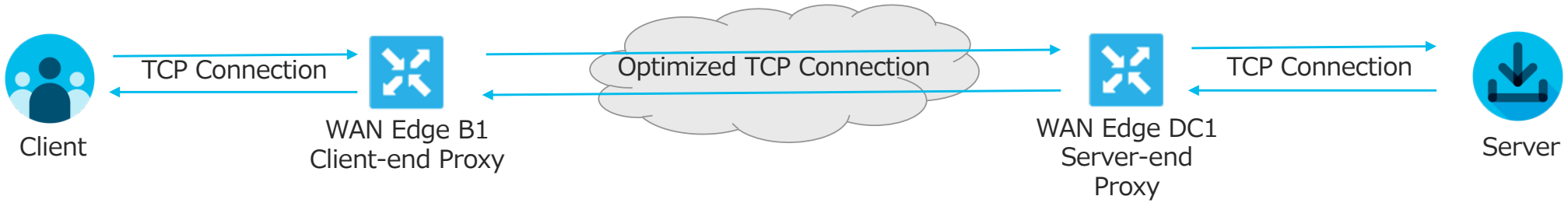
注意:
- 複数のトンネルがないと動作しない
- Receiverは受信した重複パケットを廃棄



3 TCP Optimization
WANの遅延とTCPスループットの最適化

WANリンクの遅延が大きいとアプリケーションのパフォーマンスが低下します。
高遅延によるスループット低下は、TCP最適化で改善することができます。
例: 大陸横断リンクや長距離リンク、高遅延の衛星リンクなど。

TCP最適化により、WANエッジルーターは、TCPフローを開始しているクライアントとフローをリッスンしているサーバーとの間でTCPプロキシとして機能します。

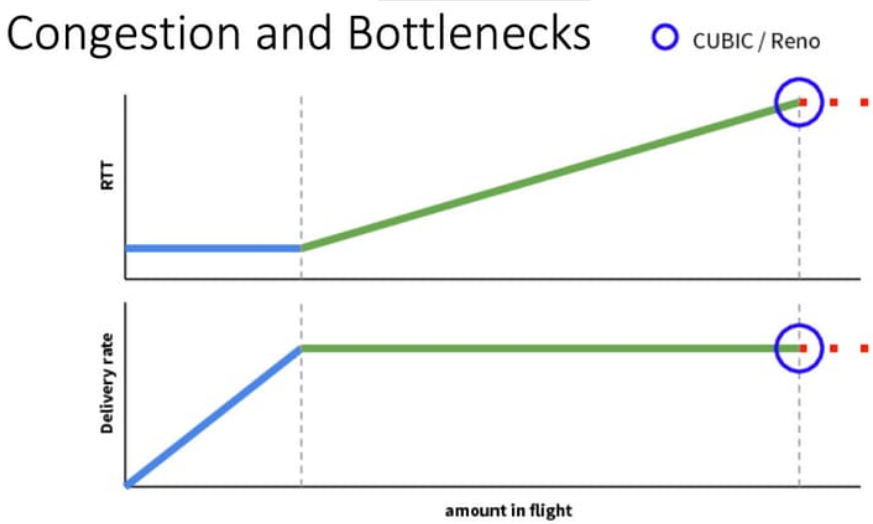


XE-SDWAN (cEdge)では BBRアルゴリズムを実装
Viptela OS (vEdge) では CUBICアルゴリズムを実装※

※vEdge1000,vEdge2000のみ

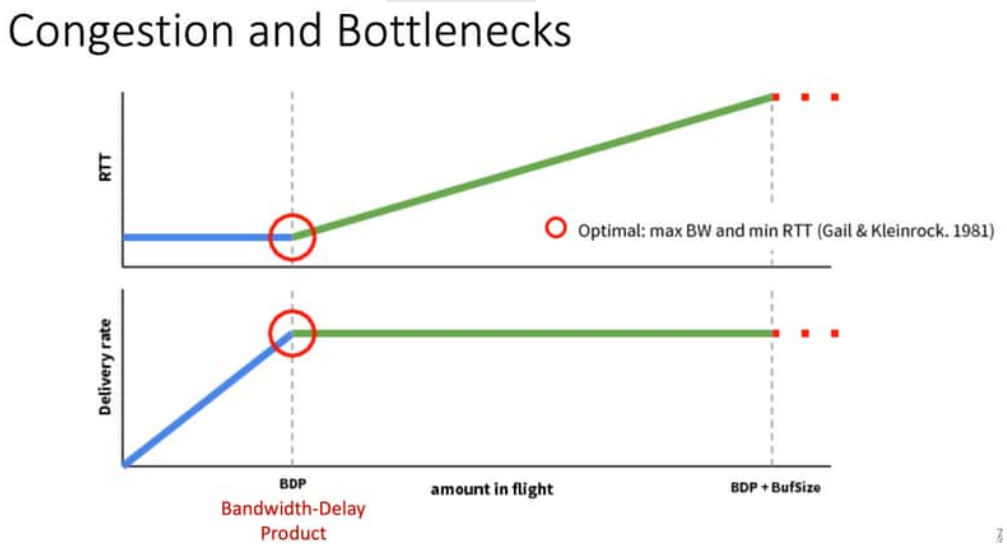
3 TCP Optimization BBR vs CUBIC

CUBIC



一般的なOSではRenoやCUBIC等のアルゴリズムが実装済み
これらを実装していない古いTCP/IPスタックを使用しているようなホストで有効

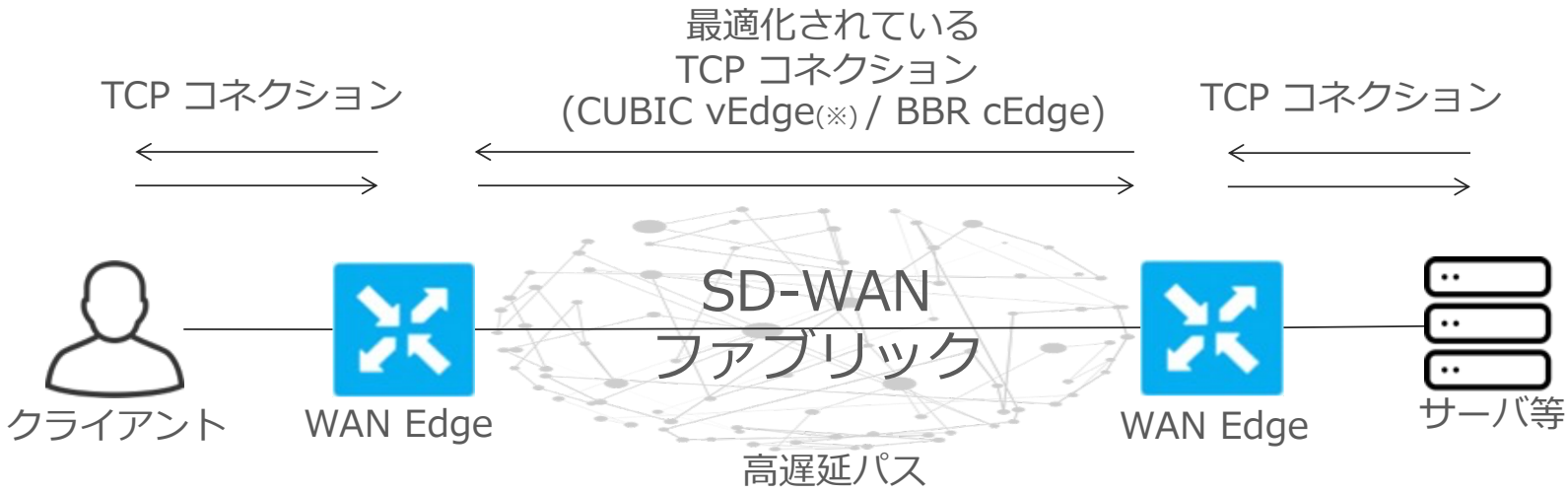
BBR



輻輳制御の開始ポイント
CUBIC ＝ Loss Based トリガー
BBR ＝ RTT/Latency トリガー

3

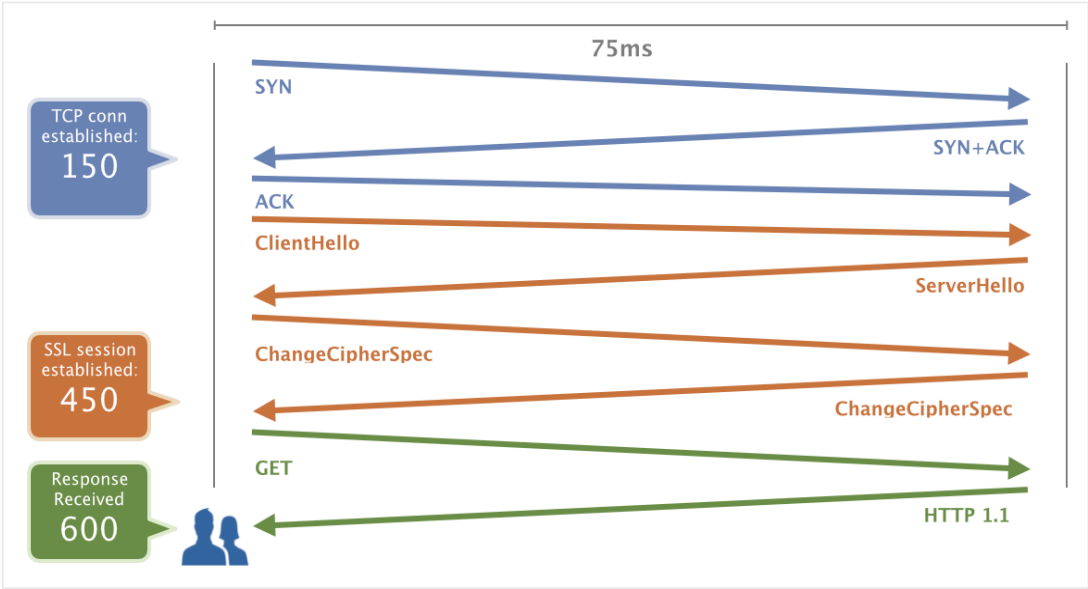
TCP 最適化

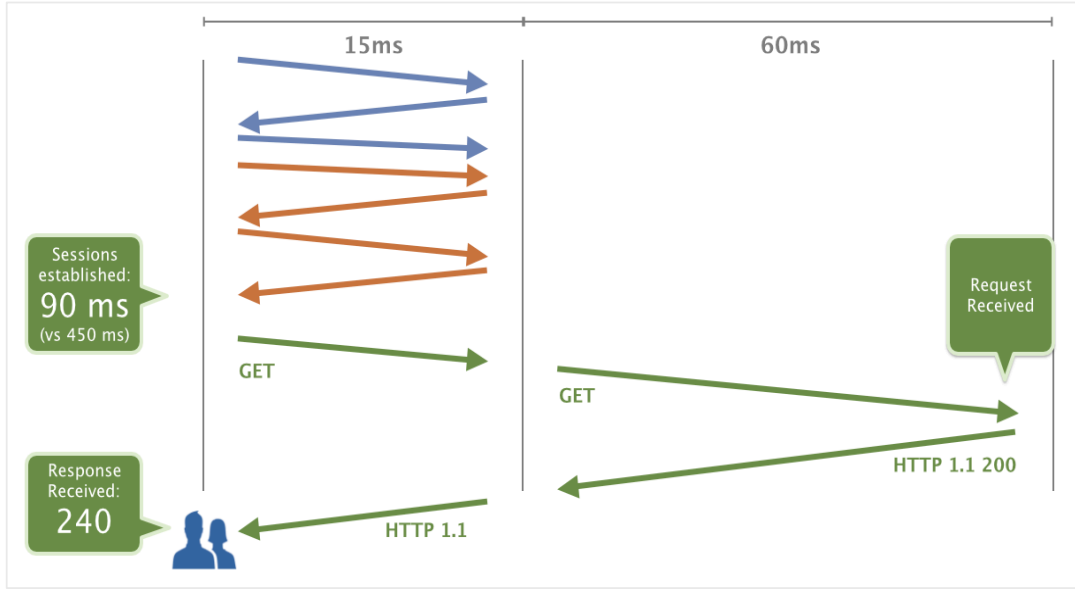


- TCP 最適化により拠点間遅延を減らしスループットを向上
- WAN Edge はクライアントとサーバ間の TCP Proxy として機能
- WAN Edge はローカルのクライアントおよびサーバの TCPコネクションを終端し、WAN Edge間でTCP最適化を行う
- ホストはエンドツーエンドの TCP ACK を待つ必要はなく、TCP の送信を一時停止する必要もない
- 最適化されたTCP接続では、不要な再送信や大きな初期 TCPウィンドウサイズが発生しないように、セレクティブ ACKを使用してスループットを最大化します

※vEdge-1000およびvEdge-2000でサポート

3 Session Persistence

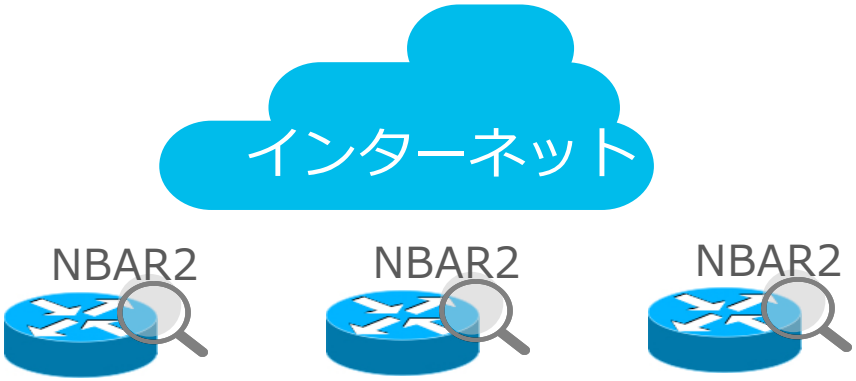




4 SD-AVC
(**S**oftware **D**efined **A**pplication **V**isibility and **C**ontrol)

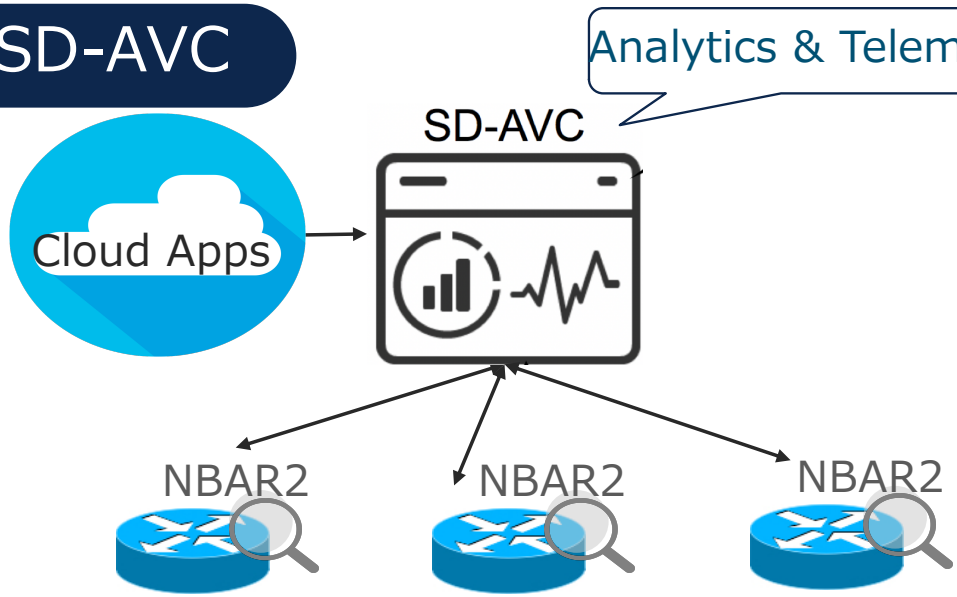
AVC = アプリケーションの可視化、分析する技術要素の総称

これまで



各ルータが個別に
アプリケーション識別

SD-AVC

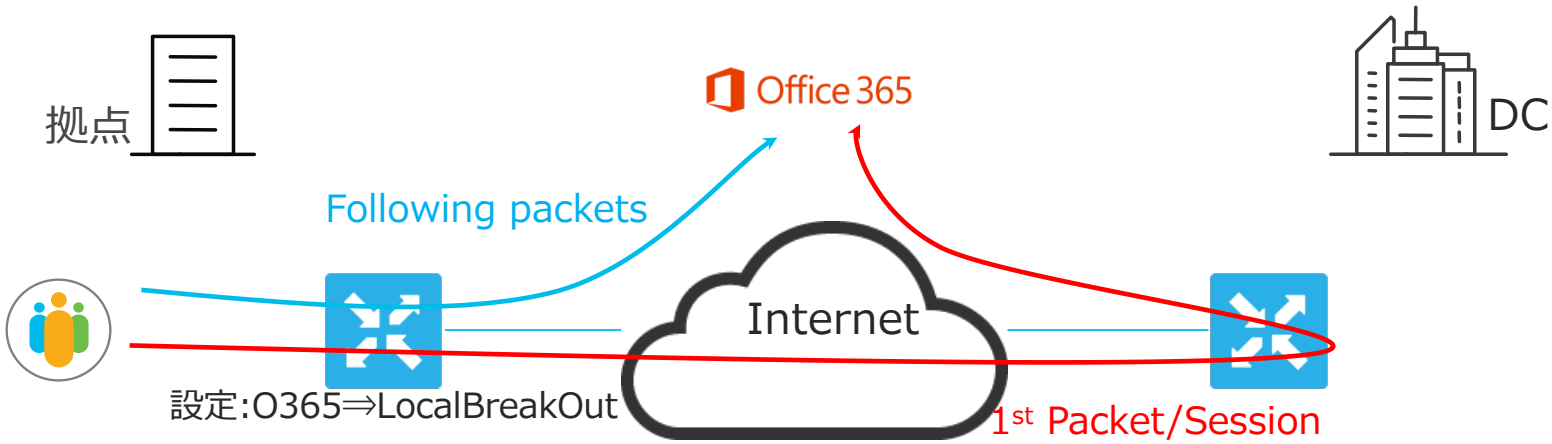


SD-AVCコントローラを中心に
外部ソースやルータと連携

4

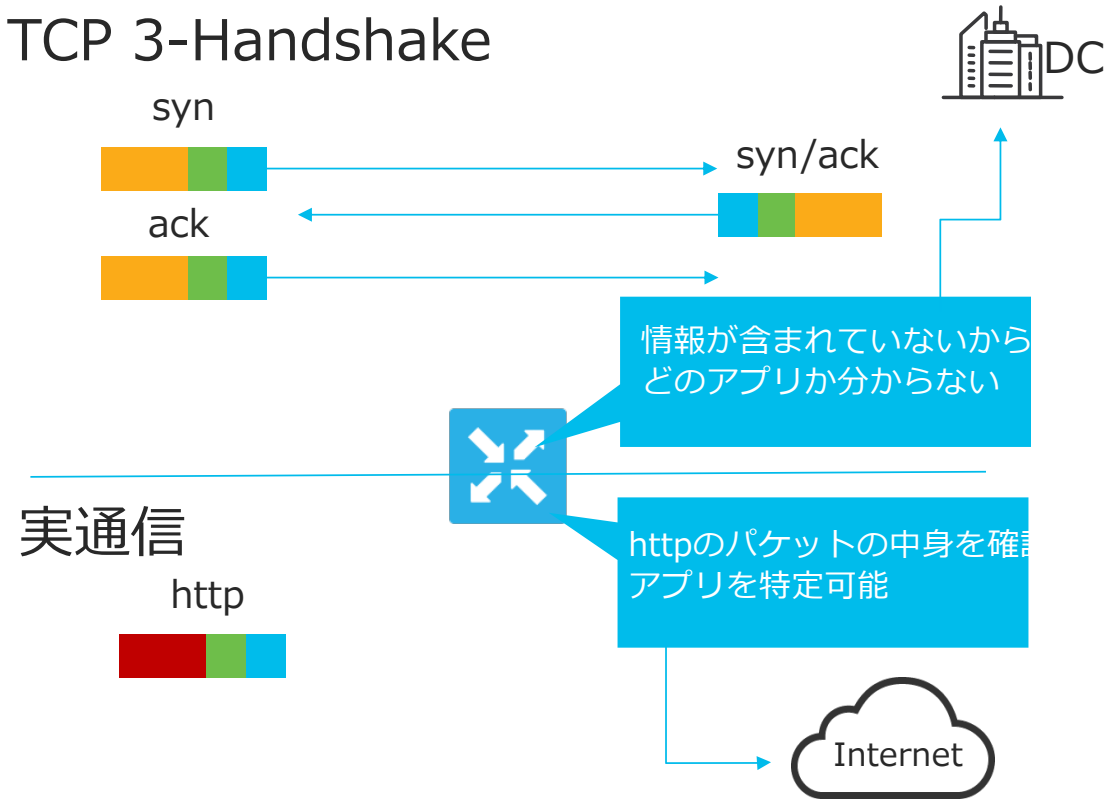
SD-AVC
DIA O365の最適化とファーストパケット対策

特定のクラウドへの通信を選択的にローカルブレイクアウトする際に
最初のパケットはローカルブレイクアウトされずに、
ハブ拠点を経由してインターネットへと抜けていってしまう



4

ファーストパケットがセンター経由になる理由



・特定のクラウドへの通信であることを識別するためにDPIが利用される

・DPIはパケットの中身を見て識別をする。ファーストパケットには識別に必要な情報が含まれていない

・ブレイクアウト対象のクラウド通信もファーストパケットは他のパケットと同様にセンター経由になってしまう

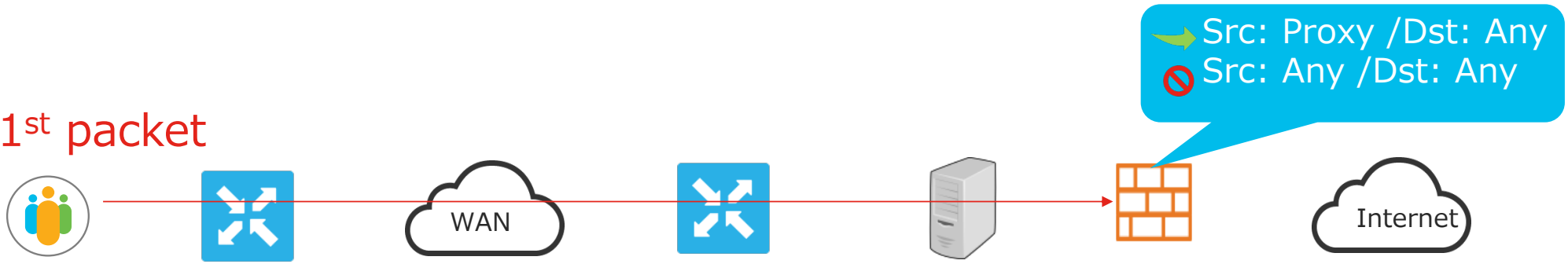
4

なぜファーストパケット問題が「問題」なのか

ファーストパケット問題が問題とされる要因＝

①プロキシの利用 ＋ ②ファイアウォールの設定

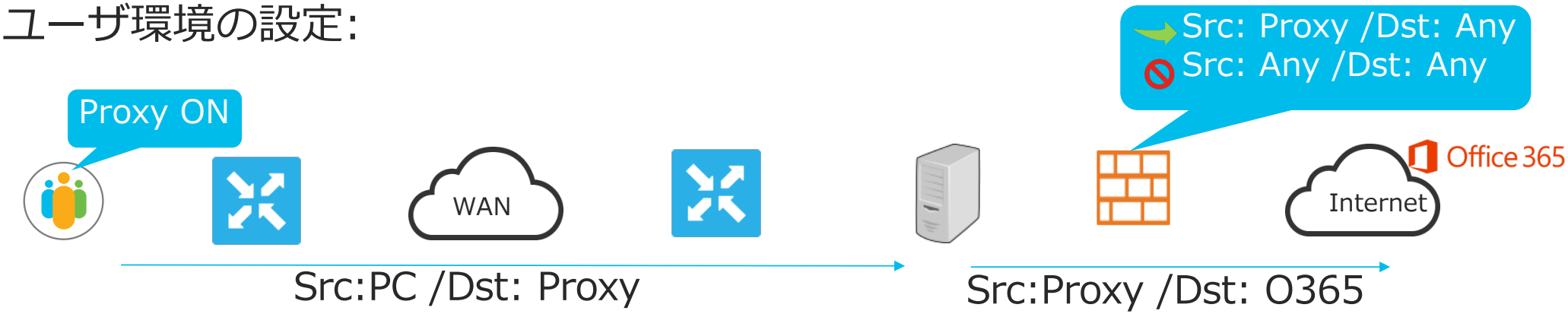
基本的にインターネットの通信はプロキシ経由としている場合、
ファイアウォールで送信元をプロキシに限定していることがほとんど。
その場合、ファーストパケットがファイアウォールにドロップされて
しまう。



4

なぜファーストパケット問題が「問題」なのか(1)

ユーザ環境の設定:



ローカルブレイクアウト用に設定変更:

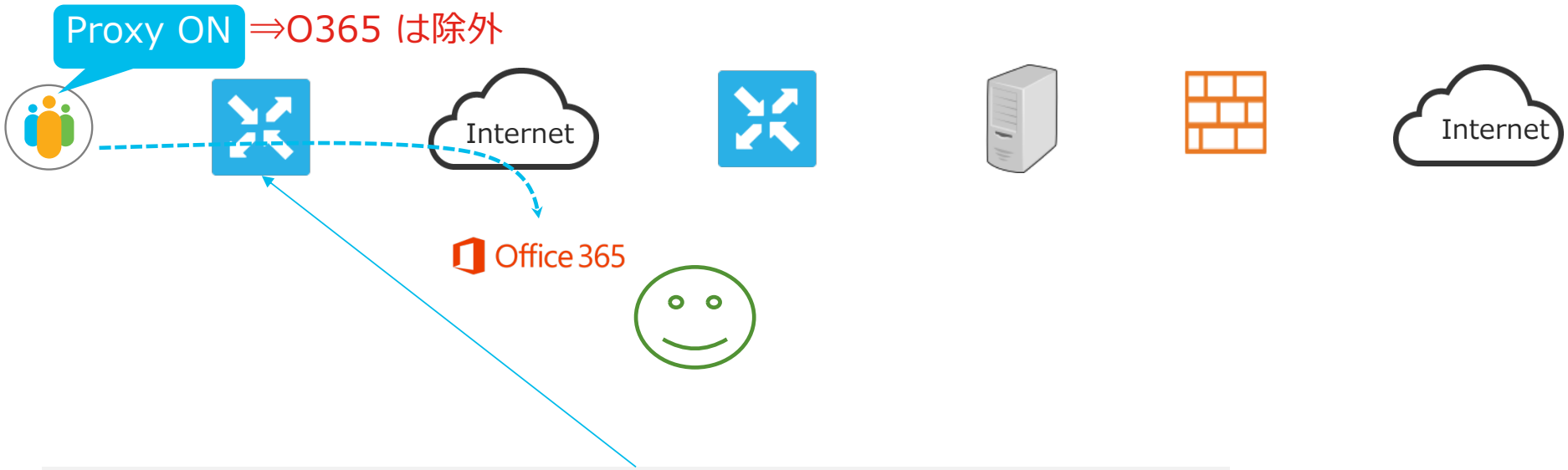
4

なぜファーストパケット問題が「問題」なのか(2)

ローカルブレイクアウト用に設定変更後:

4

では、どうすれば良いか？



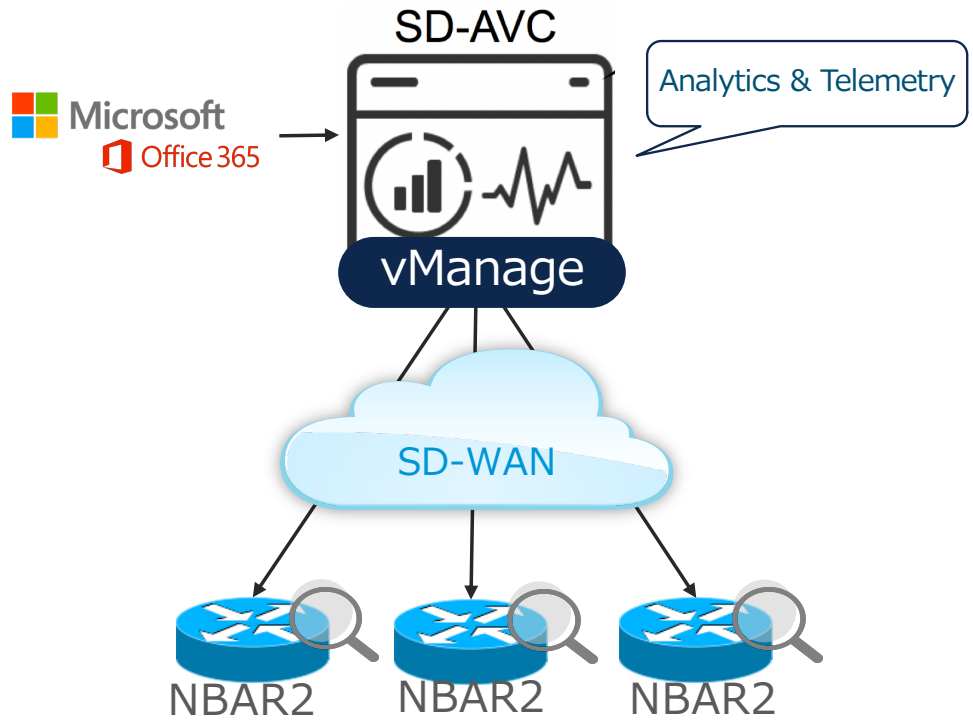
予め、O365 URL 向けの IPアドレス解決されたテーブルを
WAN Edge ルータ上に持ち、IPレベルでブレイクアウトする

4 SD-AVC
DIA O365の最適化とファーストパケット対策

SD-AVCではMicrosoft365と連携し、
事前にMS365のIPアドレス情報を
vManageが学習

ルールセットをNBAR2エンジンを搭載
した各WAN Edgeにプッシュ

ファーストパケットからローカルブレイ
クアウトが可能に



SD-AVCコントローラを中心に
外部ソースやルータと連携

4 WAN Edge側で NBARのキャッシュ

Service Internal が必要

```
BR10-C4351-01#config-transaction

admin connected from 127.0.0.1 using console on BR10-C4351-01
BR10-C4351-01(config)# service internal
BR10-C4351-01(config)# commit
Commit complete.
```

show ip nbar classification cache sync import last

```
BR10-C4351-01#sh ip nbar classification cache sync import last
Imported sockets
================

 id     | IP                                       | port        | L4  | vrf-id | vrf name | app-id | eng-id | sel-id   | app-name                | black | optimize    | allow      |
=============================================================================================================================================================================
      0 |                      139.219.156.0/22    |         443 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
      1 |          2001:489A:2204:C00::/54         |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |   TRUE [1] |        N/A |
      2 |                      23.103.160.0/20     |         143 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
      3 |                      13.107.18.10/31     |         143 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
      4 |                       51.5.64.0/23       |         443 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |   TRUE [1] |        N/A |
      5 |                      42.159.87.106/32    |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
      6 |                      52.238.118.132/32   |        3481 | UDP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |   TRUE [1] |        N/A |
      7 |                       103.9.8.0/22       |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
      8 |                       40.104.0.0/15      |         443 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |   TRUE [1] |        N/A |
      9 |                      180.210.229.0/24    |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
     10 |                      42.159.162.32/27    |         443 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |   TRUE [1] |        N/A |
     11 |                      209.177.86.0/24     |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
     12 |          2A01:111:F100:2002::8975:2D98/128       |         443 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
     13 |                  2A01:4180:2001::92/128          |         443 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
     14 |                  2603:10A6:800::/40              |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |   TRUE [1] |        N/A |
     15 |                      13.91.91.243/32     |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
     16 |                  2A01:4180:4040:7::/64           |        3478 | UDP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |   TRUE [1] |        N/A |
     17 |                      42.159.224.122/32   |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
     18 |                      51.5.145.122/32     |         443 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
     19 |                      42.159.4.200/32     |         443 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
     20 |                       51.4.80.0/27       |          25 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
```

最終行

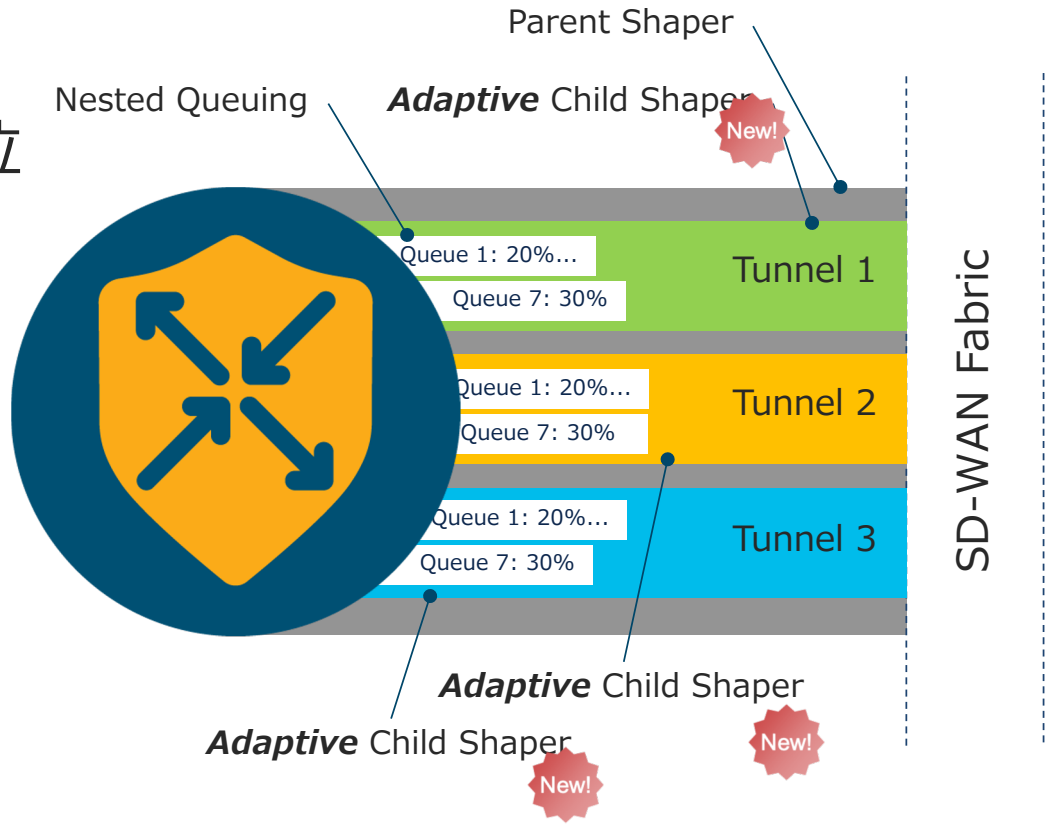

```
   1178 |                      168.63.252.62/32    |          80 | TCP | 65535  |      N/A |   1737 |     13 |      777 |             ms-services |    no |         N/A |   TRUE [1] |
```

5 SD-WAN QoS
Per Tunnel QoS / Adaptive QoS

アドバンスドQoS機能

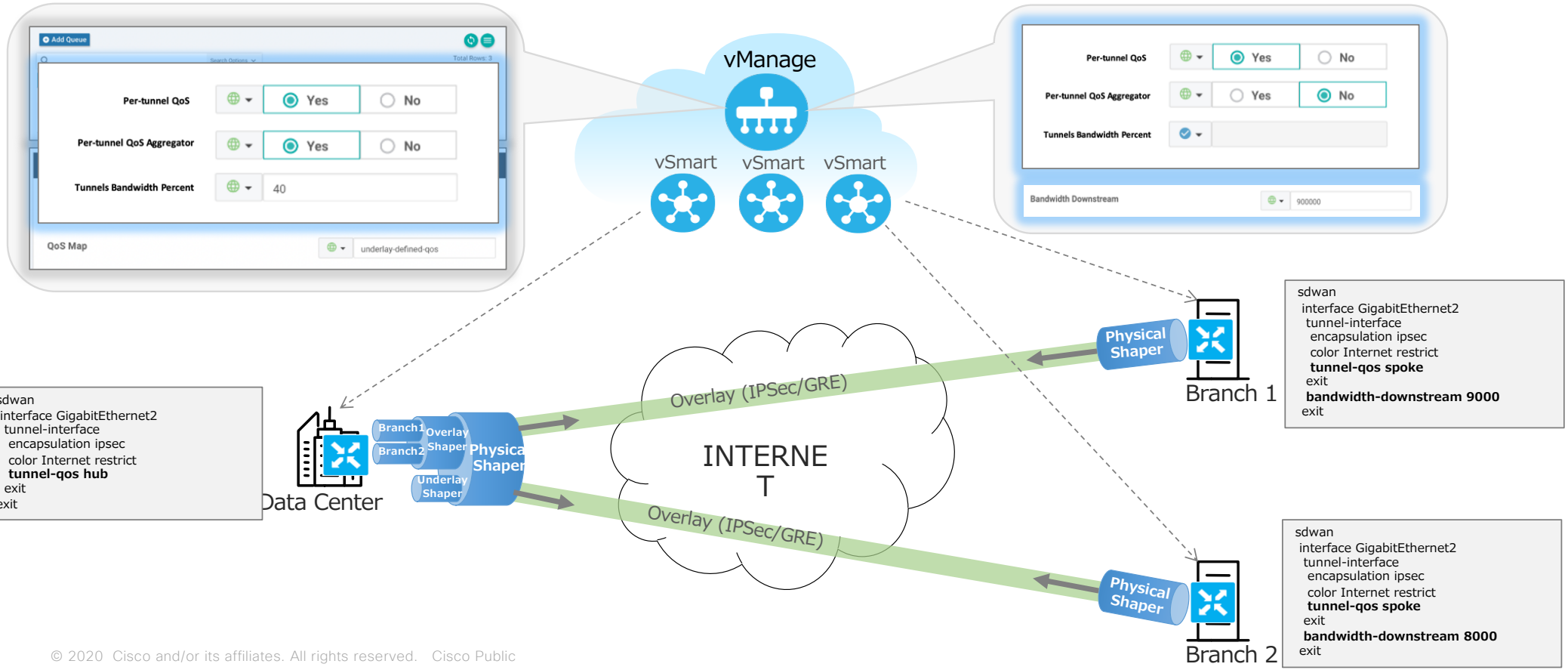
Per Tunnel QoS
Hub拠点によるトンネル(対地)単位によるShaping

Adaptive QoS
変化するWAN帯域を拠点毎に動的に調整



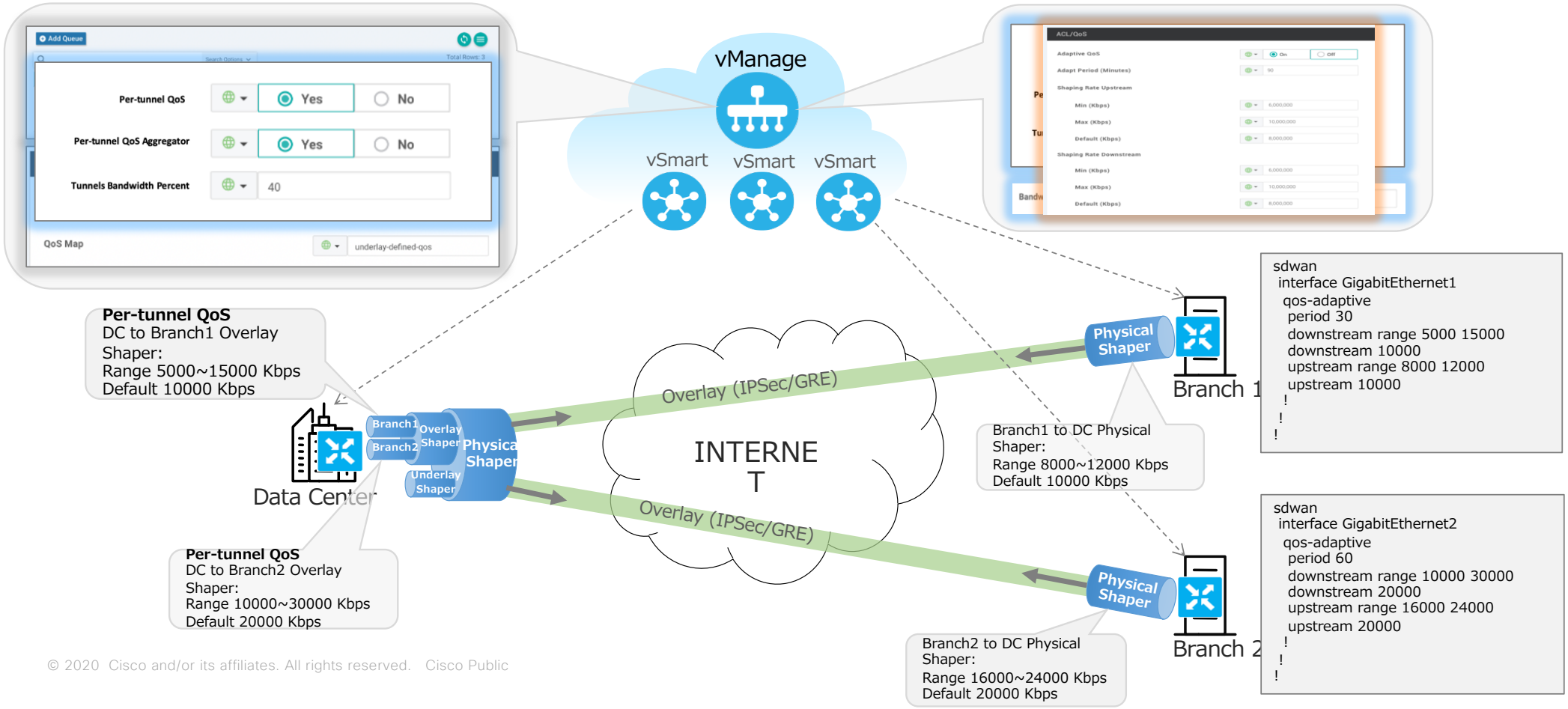
5 Per-Tunnel QoS

Per-Tunnel QoS は、ハブアンドスポーク構成で適用します。
ハブサイトではトンネル(スポークサイト)毎に子Shaperを持つ事ができます。



5 Adaptive QoS

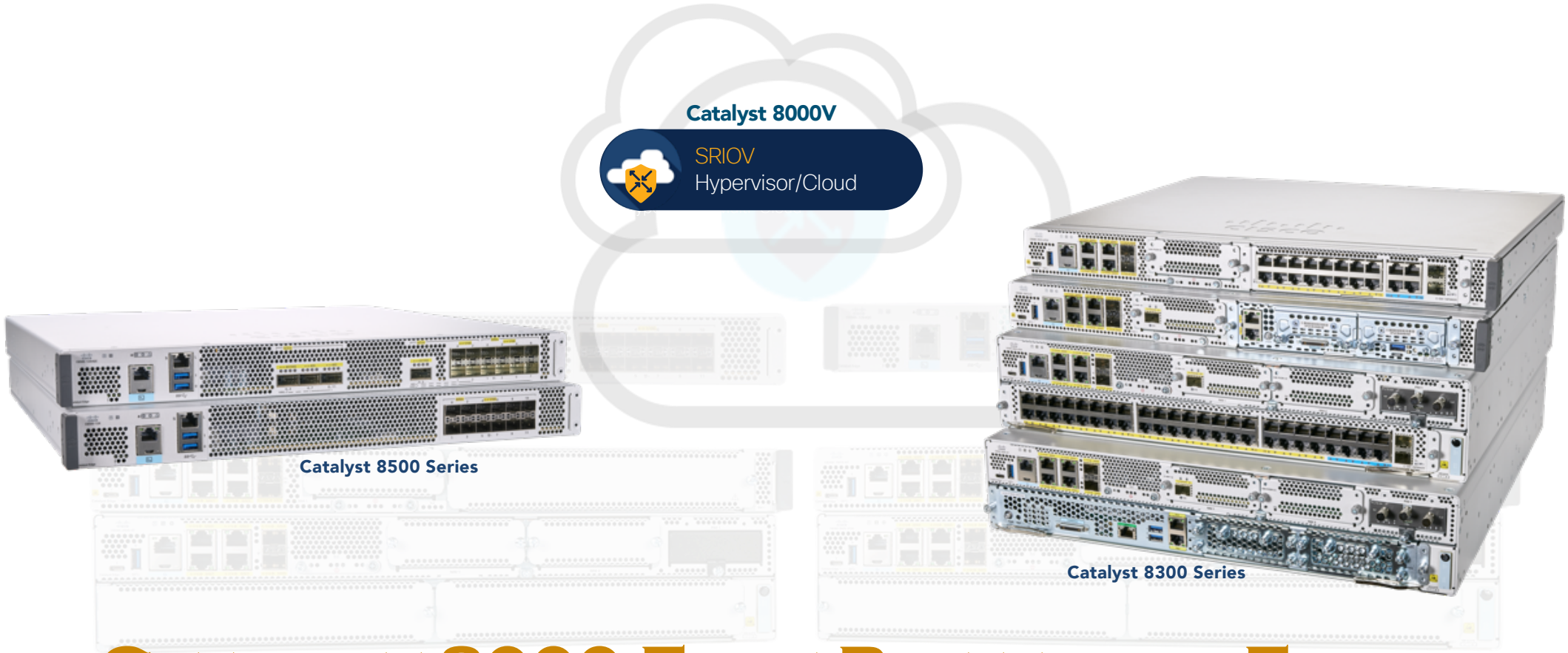
WAN回線の帯域幅を検出し、インターフェースShaperとEgress Queueを動的に更新する機能



AppQoEによるソリューション

1. Application Aware Routing
2. FEC/Packet Duplication
3. TCP Optimization
4. SD-AVC Cloud Connector for O365
5. Per Tunnel QoS / Adaptive QoS

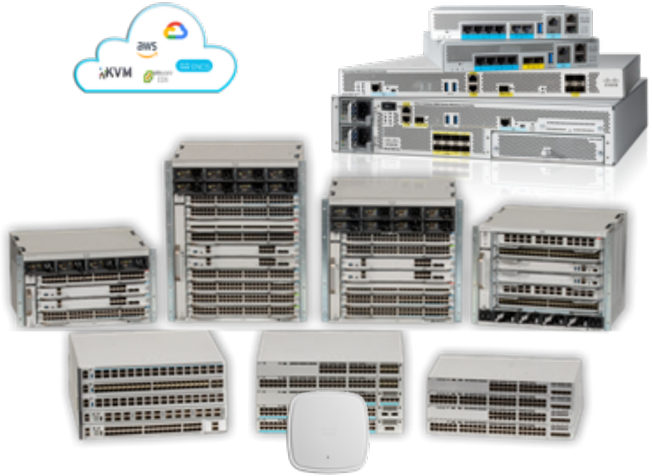
Catalyst 8000 Edge Platforms Family のご紹介

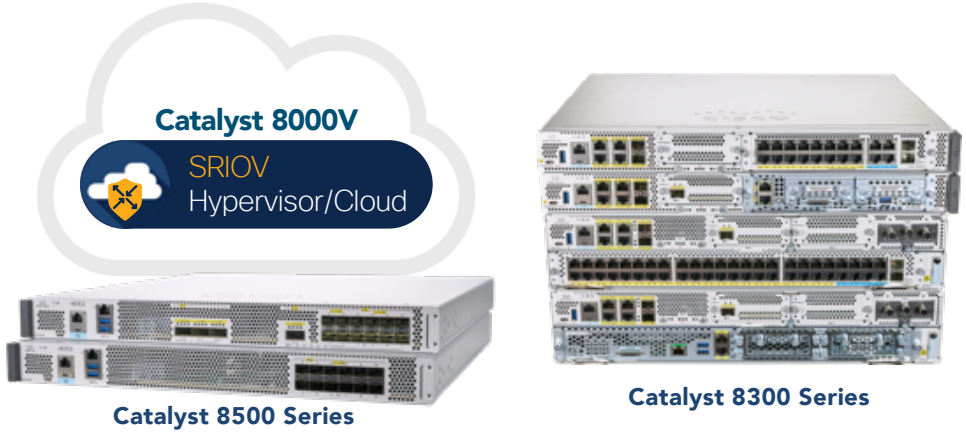


Catalyst 8000 Edge Platforms Family

インテントベースWANの新時代に向けて

Catalyst Everywhere





Catalyst 9K
企業 キャンパス ネットワーク

Catalyst 8K
企業 WAN ネットワーク

Cisco Catalyst 8000 エッジ プラットフォーム

クラウド

VNF

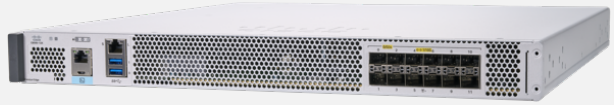
Catalyst 8000V

SRIOV
Hypervisor/Cloud

ヘッドエンド

QFP

Catalyst 8500



User Centric Design

ブランチ

x86

Catalyst 8300

IOS XE
共通 ソフトウェア アーキテクチャー

x86, QFP
スケーラブル ハードウェア アーキテクチャー

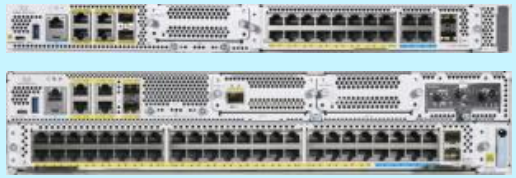
Catalyst 8000 シリーズが発表されました

今回発表されたのは以下3種類

ターゲット
リリース:
17.4.1

Catalyst 8500シリーズ エッジ プラットフォーム

Catalyst 8300シリーズ エッジ プラットフォーム



Catalyst 8000V エッジ ソフトウェア

SRIOV
Hypervisor/Cloud

後継元機種

ASR 1001/2-HX

アグリゲーション

ISR 4400

モジュラーアクセス

CSR 1000V

クラウド/バーチャル

Secure Cloud-scale SD-WAN により、SASEに最適なプラットフォーム

Catalyst 8500

Aggregation Redefined

Cisco Catalyst 8500シリーズエッジプラットフォーム

業界で最も強力なSD-WANヘッドエンド

豊富なサービスを統合

NBAR 2、NAT、ファイアウォール、QoSなど。
業界をリードするサービス・エッジ・プラットフォーム

エッジインテリジェンス

Compute
コンテナベースのアプリケーション

スケール

最大**8000**のSD-WANトンネル集約
高速**100/40**ギガビットイーサネットポート
高密度10/1ギガビットイーサネットポート

マルチレイヤセキュリティ

ハイスループットMACsecおよびIPsec
信頼できるソリューション
Umbrella SIG

内蔵ポートの柔軟性

ハイライト

- すべてのポート組み込み
- WAN MACsec
- 第3世代 QFP
- 最大200 Gbpsの CEF
- 5G対応

管理性

- 仮想管理
- DNA Center
- オープンAPI
- 分析

Catalyst 8500 シリーズ
以下2つの型番でリリース

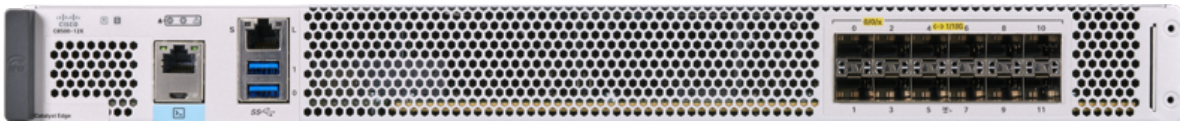
100G, 40G
‘C’ ‘Q’

C8500-12X4QC

2 QSFP28, 2 QSFP
12 SFP+

10G, 1G
‘X’

C8500-12X



12 SFP+

CEF で最大 200 Gbps,
高性能 IPsec

第3世代の QFP,
ハードウェアアクセラレーションサービス

ユーザ中心設計, RFID,
ラベルトレイ, FRU

C8500-12X4QC ポート仕様

業界初の 100G, 40G ポート SD-WAN 1RU プラットフォーム

オプション	ポートスピード	最大ポート構成
1	100G	2x100G
2	100/40G	1x100G + 3x40G
3	40/10G	4x40G + 8x10G
4	100/40/10G	1x100G + 1x40G + 8x10G
5	10G	12x10G
6	1G	12x1G

Note: 1/10G port's speed is detected based on SFP/SFP+ used in the port

Catalyst 8500シリーズポートの柔軟性

High Speed 100 G、40 Gオプション

Option 1 2 x 100G

Option 3 4 x 40G + 8 x 10G

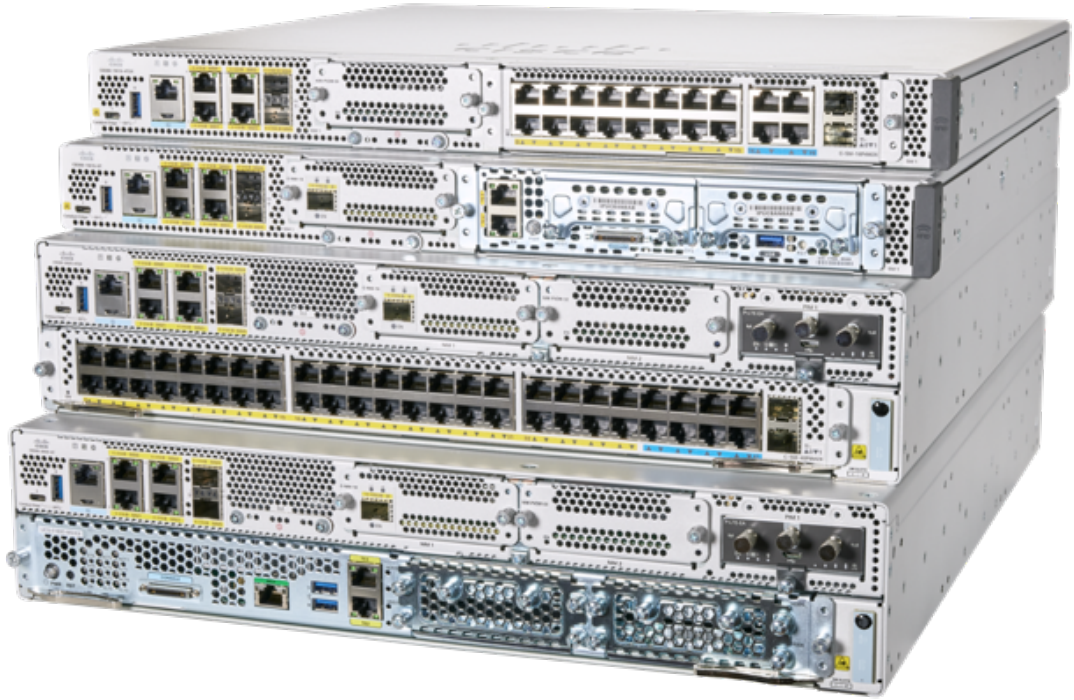
Option 2 1 x 100G + 3 x 40G Ports

Option 4 1 x 100G + 1 x 40G + 8 x 10G

高密度10 G/1 Gオプション

Option 5,6 **C8500-12X:** 12 x 1/10G

Option 5,6 **C8500-12X4QC:** 12 x 1/10G



Catalyst 8300

New Age Branch

Cisco Catalyst 8300シリーズエッジプラットフォーム
Secure Cloud Scale SD-WANブランチの基盤

豊富なサービスを統合
音声サバイバビリティ、転送エラー訂正
パケット複製、TCP最適化

エッジインテリジェンス
Compute
コンテナベースのアプリケーション

スケール
最大5倍のIPsecおよびIP CEFパフォーマンス
3~4倍のサービス・パフォーマンスを実現する
コアの可用性

マルチレイヤセキュリティ
SSLアクセラレーション
アプリケーションファイアウォール
IPS/IDS、URLフィルタリング
AMP、Threat Grid
Umbrella SIG

YESモジュラリティ

接続性
- WANポート密度の向上
- デフォルト8 G DRAM
- 10 G w/MACsec
- プラグ可能なNVMeストレージ
- 5G対応

管理性
- 仮想管理
- DNA Center
- オープンAPI
- 分析

Catalyst 8300 シリーズ
10G モデルが2型番、1G モデルが2型番リリース

10G WAN Ports 'X'
& 5G IPsec

C8300-2N2S-4T2X

C8300-1N1S-4T2X

4 RJ45
2 SFP+

1G WAN Ports 'T'
& 2G IPsec

C8300-2N2S-6T

C8300-1N1S-6T

4 RJ45
2 SFP

M.2 USB/ NVMe
ストレージ

UADPベース スイッチ
10G WAN モジュール

ユーザ中心設計
(RFID, QRラベル, FRU)

高効率の AC
および DC電源

Catalyst 8300 サポートモジュール

LAN

NIM-ES2-8
NIM-ES2-8-P
C-SM-40G8M2X
C-SM-16G4M2X

Async

NIM-16A
NIM-24A
SM-X-64A

WAN

C-NIM-1X
NIM-1T
NIM-2T
NIM-4T
SM-X-1T3/E3*
NIM-2BRI-S/T*
NIM-4BRI-S/T*

WAN + Voice:
NIM-1MFT-T1/E1
NIM-2MFT-T1/E1
NIM-4MFT-T1/E1
NIM-8MFT-T1/E1
NIM-1CE1T1-PRI*
NIM-2CE1T1-PRI*
NIM-8CE1T1-PRI*

LTE

NIM-LTEA-EA
NIM-LTEA-LA
P-LTE-VZ
P-LTE-NA
P-LTE-US
P-LTE-JN
P-LTE-GB
P-LTE-IN
P-LTE-AU
P-LTEA-EA
P-LTEA-LA
P-LTEAA-EA
P-LTEAP18-GL
CAT18 CGW*

5G

(1H, CY21 : Roadmap)

5G sub-6GHz CGW
5G sub-6GHz PIM

Voice

SM-X-PVDM-3000
SM-X-PVDM-2000
SM-X-PVDM-1000
SM-X-PVDM-500
SM-X-24FXS/4FXO
SM-X-16FXS/2FXO
SM-X-8FXS/12FXO
SM-X-72FXS

NIM-2FXSP
NIM-4FXSP
NIM-2FXS/4FXOP
NIM-2FXO
NIM-4FXO
NIM-4E/M*
NIM-2BRI-NT/TE*
NIM-4BRI-NT/TE*
NIM-PVDM-32
NIM-PVDM-64
NIM-PVDM-128
NIM-PVDM-256

DSL

NIM-VAB-A
NIM-VA-B
NIM-VAB-M
NIM-4SHDSL-EA

Storage

SSD-M2NVME-600G
M2USB-16G
M2USB-32G

ADAPTOR

C-SM-NIM-ADPT

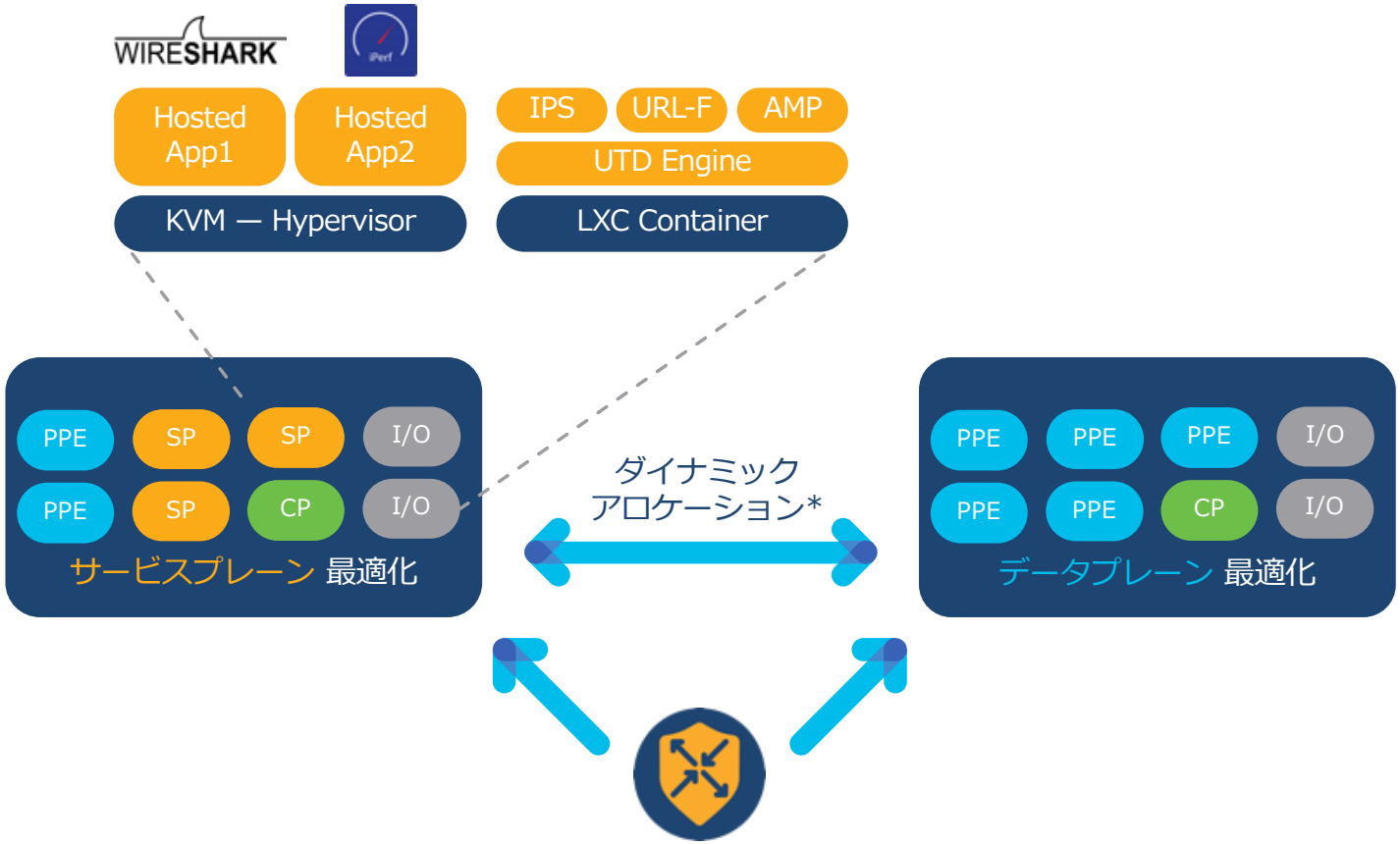
UCS-E

UCS-E160S-M3/K9
UCS-E1120D-M3/k9
UCS-E180D-M3/K9

* IOS XE はサポート済で SD-WAN は 17.4 よりサポート
青色： 未リリース

Catalyst 8000 エッジプラットフォーム— SoC

X86 Multi-core CPU



* Available in XE 17.4 release

ダイナミック・コア・アロケーション — スループットとサービス要求に対応

Catalyst 8300 シリーズ エッジ プラットフォーム
デフォルト コア アロケーション XE 17.3

Default Optimized Core Allocations*

	SD-WAN	IOS-XE
C8300-2N2S-4T2X 	CP-1, DP-6, SP-5	
C8300-2N2S-6T 	CP-1, DP-4, SP-3	
C8300-1N1S-4T2X 	CP-1, DP-4, SP-3	
C8300-1N1S-6T 	CP-1, DP-4, SP-3	

* Dynamic Core allocation available in XE 17.4 release

Catalyst
8000V

Catalyst 8000V

Future of Cloud

17.4 Release

Cisco Catalyst 8000V エッジ ソフトウェア

企業ユースのネットワーキング・セキュリティに対応するx86ベースのVNF

マルチサービス サポート

Feature-rich IOS XE and XE-SD-WAN software
Supported features such as NAT, Firewall, NBAR QoS, etc.
Runs on any x86 VM platform

クラウド インテグレーション

Extends connectivity, visibility, security into public and private clouds
Auto-Scaling capability
Integration with Azure vWAN and AWS TGW
Supports wide variety of cloud instances

パフォーマンスの弾性

CPU Hypervisors: 1 – 8 vCPU

Cloud Providers: 1- 16 vCPUs
Memory Scale: 4 – 16Gb

マルチレイヤー セキュリティ

Secure object storage

High Throughput IPsec
IPS/IDS, URLF, AMP&TG, TLS Proxy

Catalyst 8000V
Virtual Switch/SRIOV
Hypervisor/Cloud

ハイライト

- Up to 10 Gbps IPsec in cloud
- ENCS NIM support
- TGW and vWAN integration
- DPDK IO
- SD-WAN in AWS, Azure, and GCP

マネージメント

- vManage
- Multi-tenant
- Open APIs
- Analytics

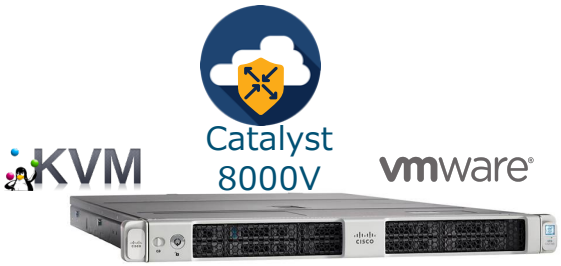
Cisco Catalyst 8000V エッジ ソフトウェア

多様なネットワーク接続オプション

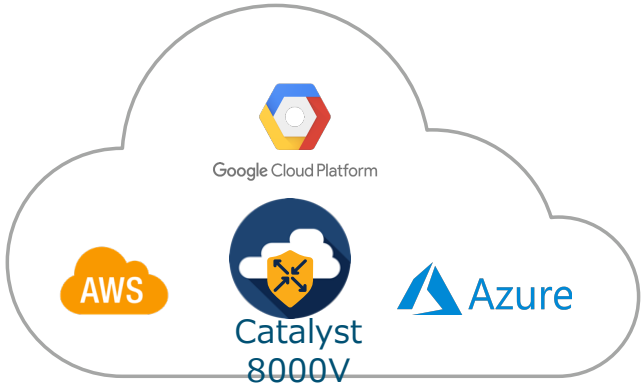
クラウド上でのシームレスなSD-WAN拡張

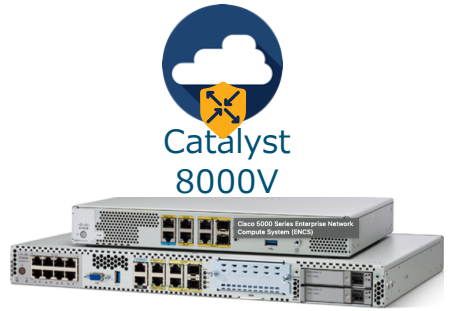
インフラに非依存

サービスの充実



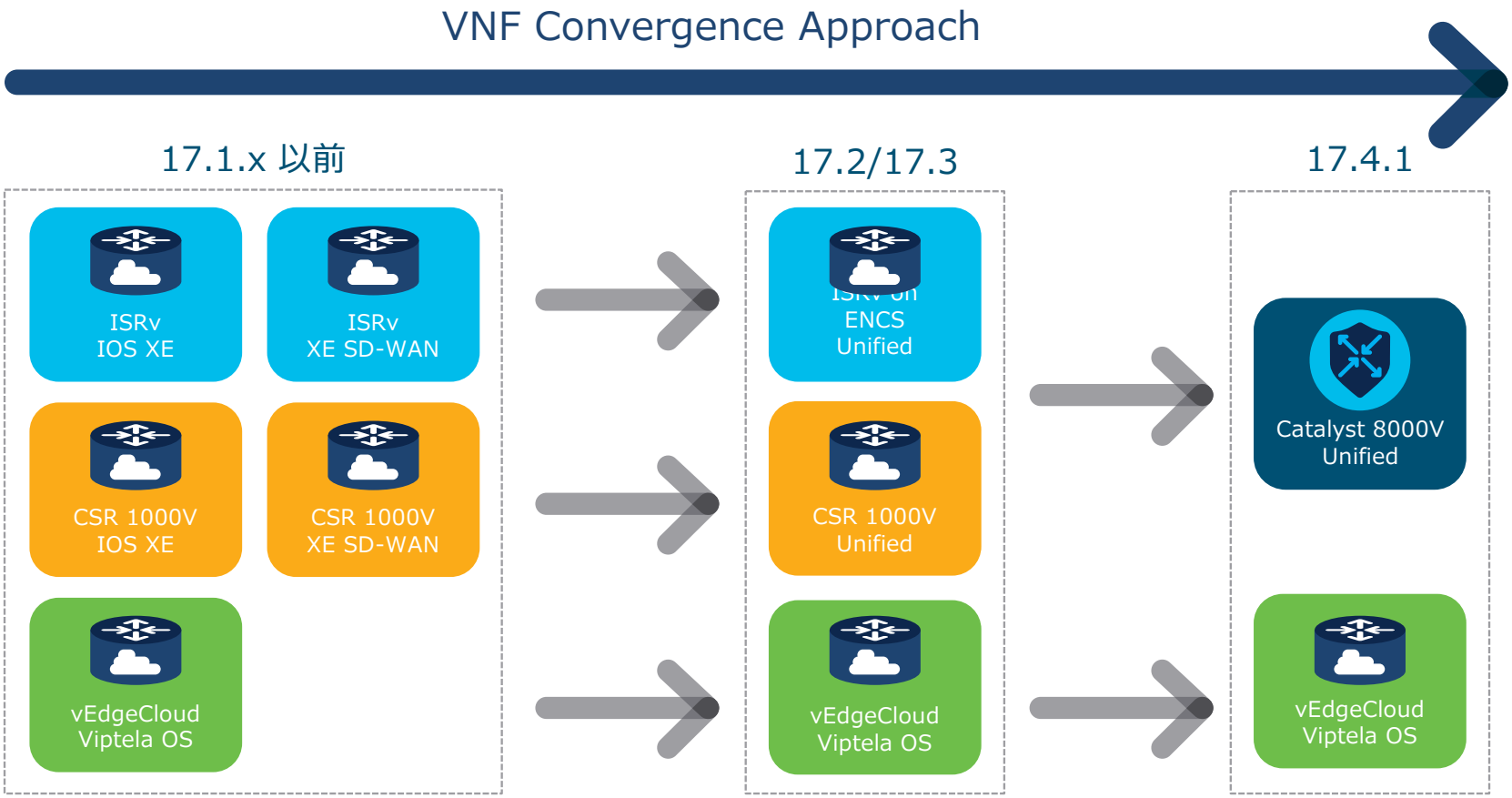
Hypervisor
On x86 server





NFVIS
on ENCS

仮想ルータのコンバージェンス



Catalyst 8000V vs CSR 1000V

Catalyst 8000V		CSR 1000V
✓	Secure Object Store	✗
✓	ENCS NIM Support	✗
✓	SD-WAN on Google Cloud	✗
✓	Azure Virtual WAN Integration	✗
DNA Licensing	Licensing	Classic + DNA licensing

Catalyst 8000V

SRIOV Hypervisor/Cloud

aws

up to 10G*

SD-WAN vHub

up to 2G*

まとめ

AppQoE
パケロス対策
アドバンスドQoS
WAN最適化 TCP最適化機能
ローカルブレイクアウト O365最適化　SD-AVC

Cat8k イントロ


CISCO