



プロキシ環境でも容易に導入可能 エンタープライズSD-WANとは

～ Office 365をより快適に使うためのジュニパーのクラウド最適化ソリューション～

2019年12月3日

JUNIPER
NETWORKS

Engineering
Simplicity



SD-WANとは

ONUG SD-WAN評価

No	評価項目	可否	ジュニパーネットワークス
1	Active／Active構成で様々な回線・WANの制御が可能なこと	☐	Public WAN, Private WANのマルチホーミング(Active/Active)での利用ができます。
2	コモディティHW上で、仮想的にCPEを提供できること	☐	vSRX（バーチャルSRX)にてSRXの機能を仮想マシン形式のCPEとしてご利用いただけます。
3	アプリケーション等のポリシーに基づき、ダイナミック制御が可能なこと	☐	SRX、NFXのAppRoute（APBR）にてアプリケーションベースのダイナミックな制御が可能です。
4	個別のアプリに対して、可視化・優先順位付け、ステアリングが可能なこと	☐	アプリケーションの可視化、アプリケーションベースでの優先制御(QoS)が可能です。
5	可用性・柔軟性の高いハイブリッドなWANの構築が可能なこと	☐	複数のPrivate WAN, Public WANでの構成が可能で回線障害時も動的に切り替えが可能です。
6	L2／L3に対応	☐	SRX、NFXはL2/L3に対応します。
7	拠点、アプリケーション、VPN品質等をダッシュボードでレポートができること	☐	CSO / Sky Enterpriseでは各種ダッシュボード機能、パフォーマンスレポートの機能を備えております。
8	オープンなノースバウンドAPIを持ちコントローラーへのアクセスや制御ができること	☐	REST APIをはじめ各種スクリプトを提供、資料を公開しています。 https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration
9	ゼロタッチプロビジョニングに対応すること	☐	SRX、NFXはZTP(ゼロタッチプロビジョニング)に対応しております。 NFXはvSRX（バーチャルSRX)を標準搭載します。
10	FIPS-140-2(セキュリティ)を取得できること	☐	SRX、NFX250およびJunosはFIPS-140-2に対応しています。 https://www.juniper.net/documentation/en_US/junos/topics/reference/general/junos-fips-software-editions.html https://www.juniper.net/documentation/en_US/junos-fips12.1/topics/concept/understanding-junos-fips-mode.html https://www.juniper.net/documentation/en_US/junos-fips12.1/information-products/pathway-pages/security/security-fips-guide-12.1x46-d40.pdf https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3288



何故、SD-WANが必要なのか

SD-WANを検討するモチベーション

CAPEX/OPEXの 軽減

- WAN, LAN, Wi-Fi を一元管理
- テンプレート作成による簡単運用
- ZTPによる拠点構築

ユーザ体感の向上

- クラウドアプリケーションを利用するユーザの体感を改善
- 拠点間通信の最適化

収益モデルの構築

- サブスクリプションモデルにより、必要に応じてセキュリティサービスを追加
- カタログモデルの販売(3rd パーティVNFをオンデマンドで提供)

エンドユーザがSD-WANを必要とする理由

CAPEX/OPEXの 軽減

- WAN, LAN, Wi-Fi を一元管理
- テンプレート作成による簡単運用
- ZTPによる拠点構築

ユーザ体感の向上

- クラウドアプリケーションを利用するユーザの体感を改善
- 拠点間通信の最適化

収益モデルの構築

- サブスクリプションモデルにより、必要に応じてセキュリティサービスを追加
- カタログモデルの販売(3rd パーティVNFをオンデマンドで提供)

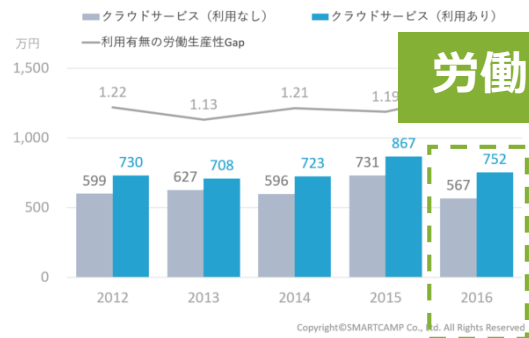
クラウドサービスの普及と課題

クラウドサービスの利用で労働生産性は向上 SaaS利用が急速に拡大している

クラウドサービスの利用による1社あたり労働生産性の向上

クラウドサービスを利用することで生産性向上を実現することが可能。
クラウドサービスを利用している企業は、利用していない企業に比べて労働生産性が約30%も高い。

SaaS
Software as a Service

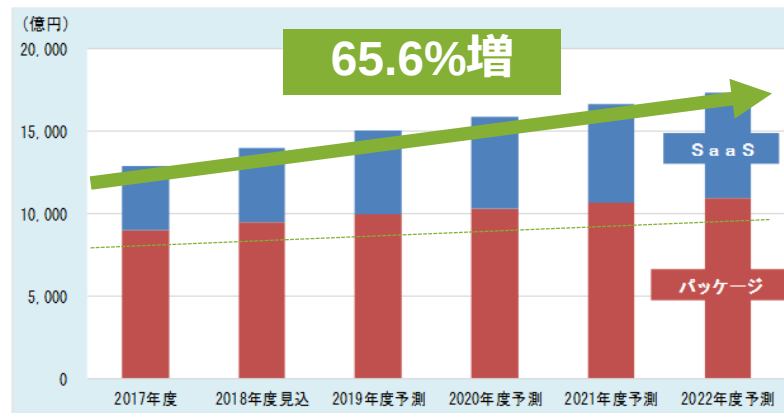


労働生産性 約30%高

出所 総務省「平成28年通信利用動向調査」
※ 調査にスマートキャンプが分析・作成
・ 営業利益、人件費、資本金、減価償却費およびクラウドサービスの利用の有無をすべてを回答した企業を対象
・ 労働生産性 = (営業利益 + 人件費 + 減価償却費) ÷ 従業員数
・ 比率はクラウドサービスの「利用あり」と「利用なし」の差異を表している

Source : Smartcamp Co, Ltd <https://boxil.jp/mag/a5170/>

ソフトウェアの国内市場（パッケージ／SaaS）



Source : 富士キメラ総研ソフトウェアビジネス新市場 2018年版

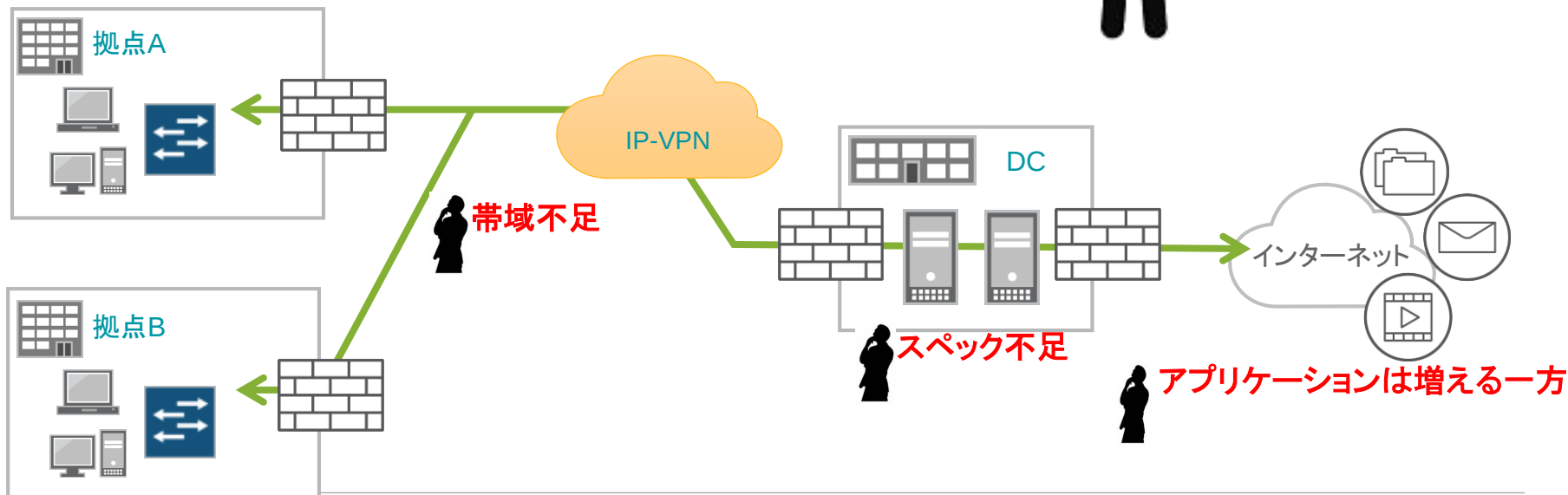
企業でのSaaS 利用は拡大

クラウドサービスの普及と課題

メールやアプリケーションサーバをクラウドに移行すると

ネットワークの帯域やFWへかかる負荷が増大

プロキシサーバを経由する場合はプロキシサーバの負荷が増大





アプリケーション制御による 課題の解決

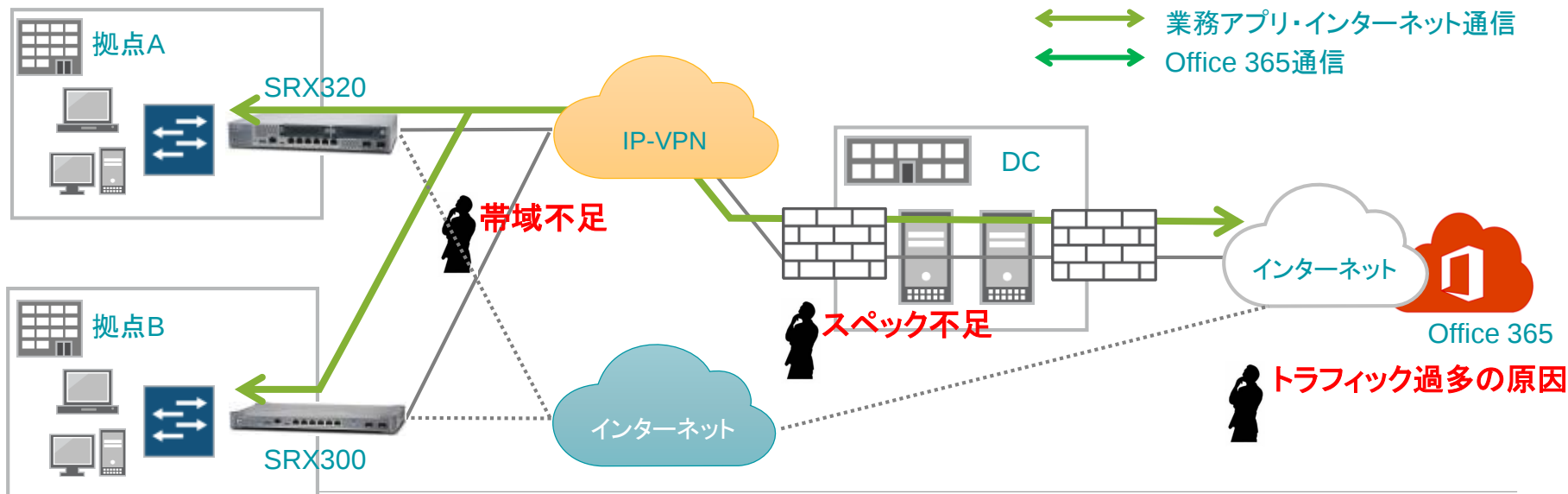
SRXを利用したネットワークが遅くなった原因の判別

アプリケーションの使用帯域、セッション数、使用したユーザを表示



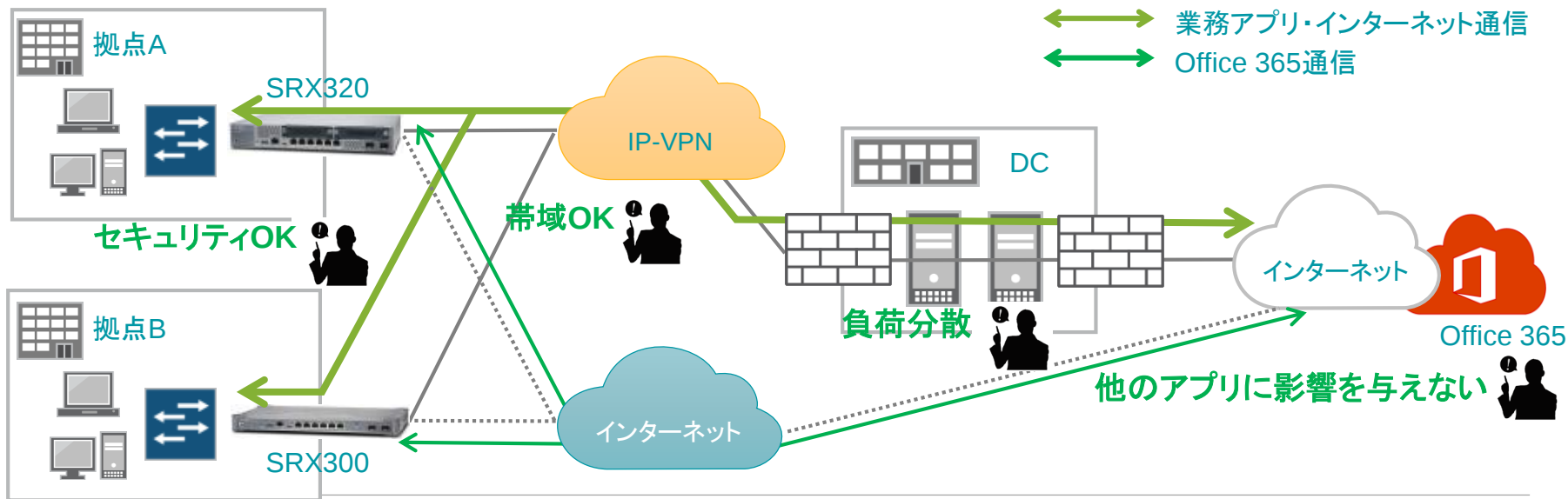
ローカルブレイクアウトの需要

- ✓ 帯域不足でファイルのダウンロードに時間が掛かる
- ✓ 今後のどれだけクラウドサービスを使用していくか不明瞭なため単純な回線増強ではすぐに頭打ちになってしまう。
- ✓ データセンタ側のFWに負荷が掛かり処理に時間が掛かる



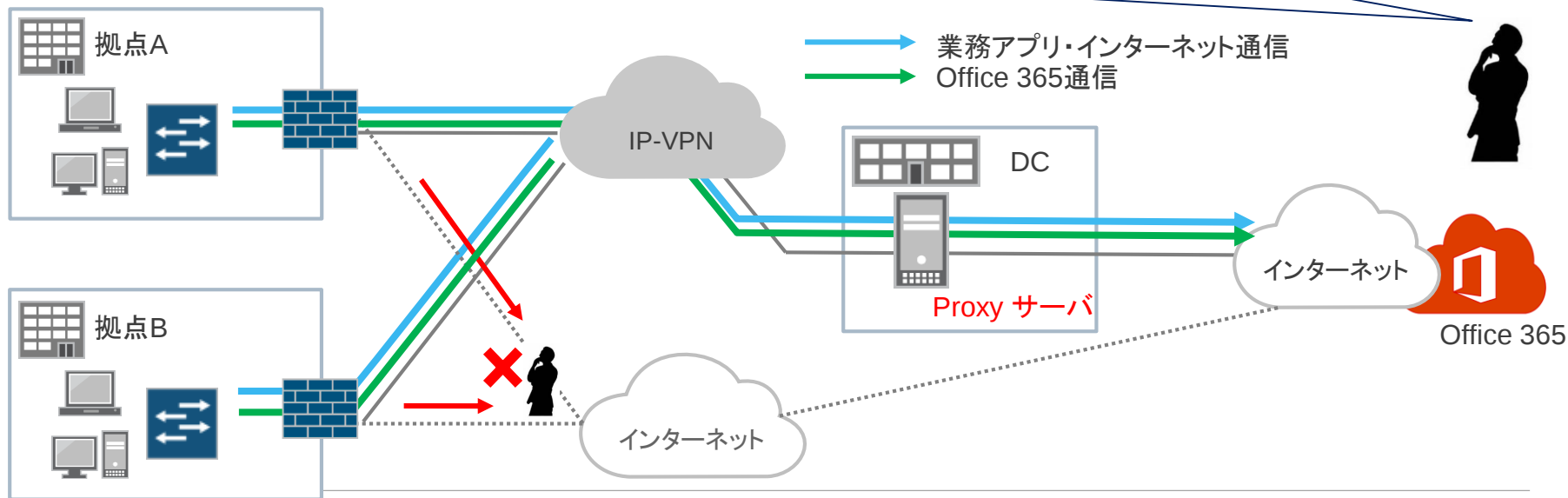
ローカルブレイクアウトの需要

- ✓ IP-VPN回線の増強は不要
- ✓ トラフィック過多の原因となっていたO365はインターネット回線から通信
- ✓ インターネットへのアクセスもFW経由なので問題なし



ローカルブレイクアウトソリューションの課題

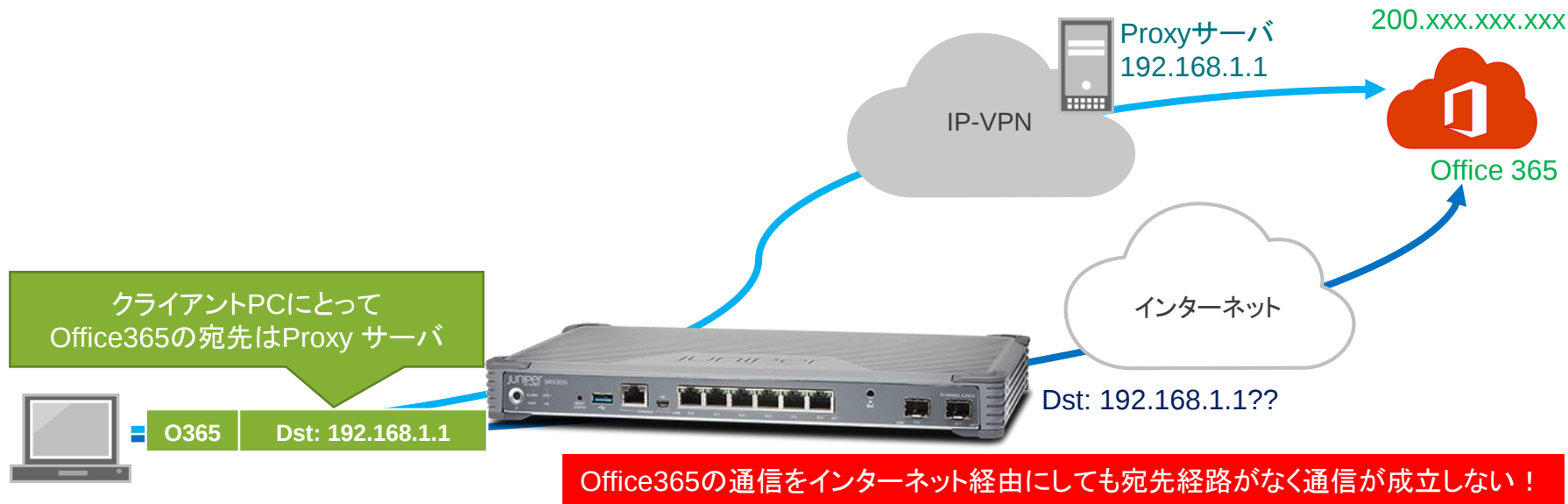
クラウド化が進む中で、DCに向かうトラフィック量が増大している。
インターネット回線を用意してトラフィックの負荷分散をしたいが、
セキュリティのためにProxyサーバを導入しており、一部のアプリケーションのみ
Proxyサーバを経由しない設計は困難。そのため、**ローカルブレイクのソリューションは導入できない**。



ローカルブレイクアウトソリューションを導入できない原因

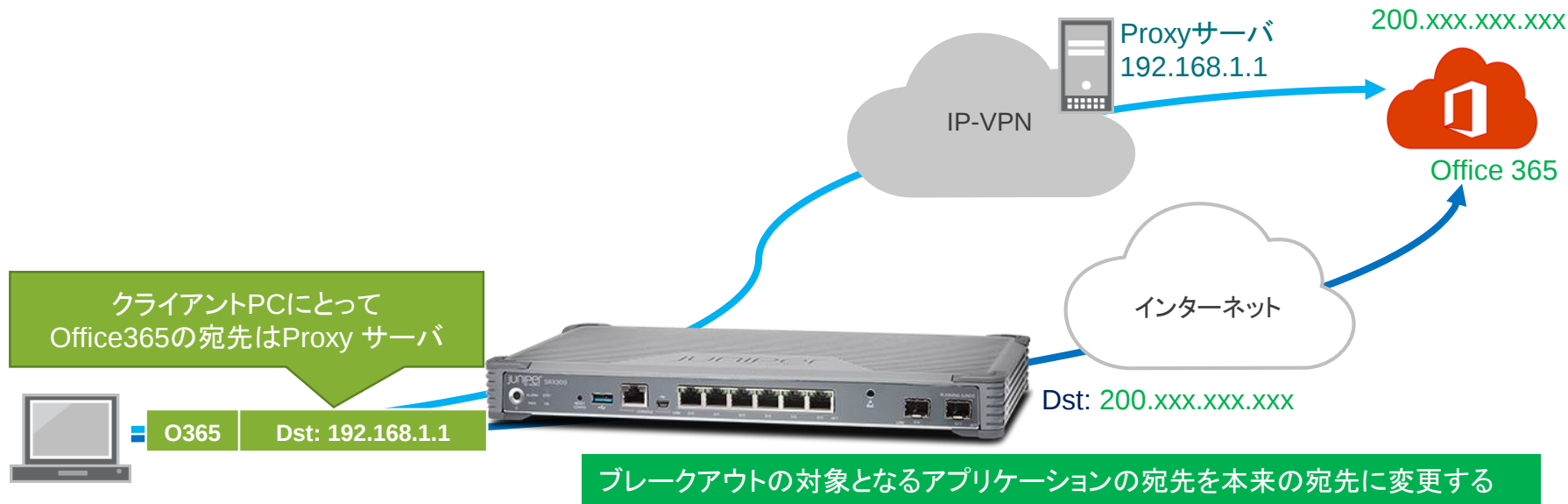
Proxyサーバを使用している環境ではクライアントはアプリケーションサーバのIPアドレスではなくProxyサーバのIPアドレスへ通信を開始する。

そのため、アプリケーションを判別して経路を変更しても通信が成立しない。

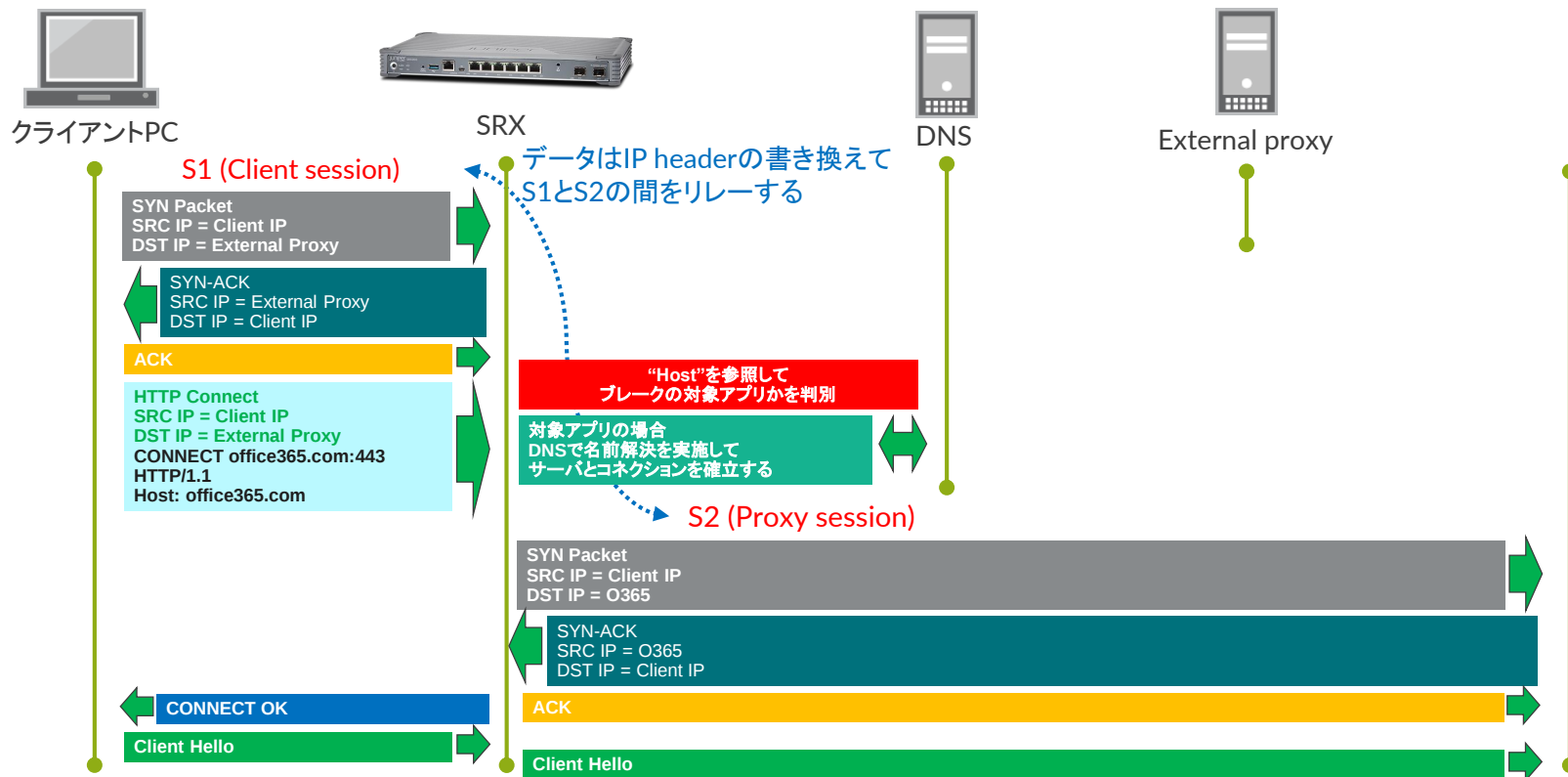


ローカルブレイクアウトソリューションを導入できない原因の解決

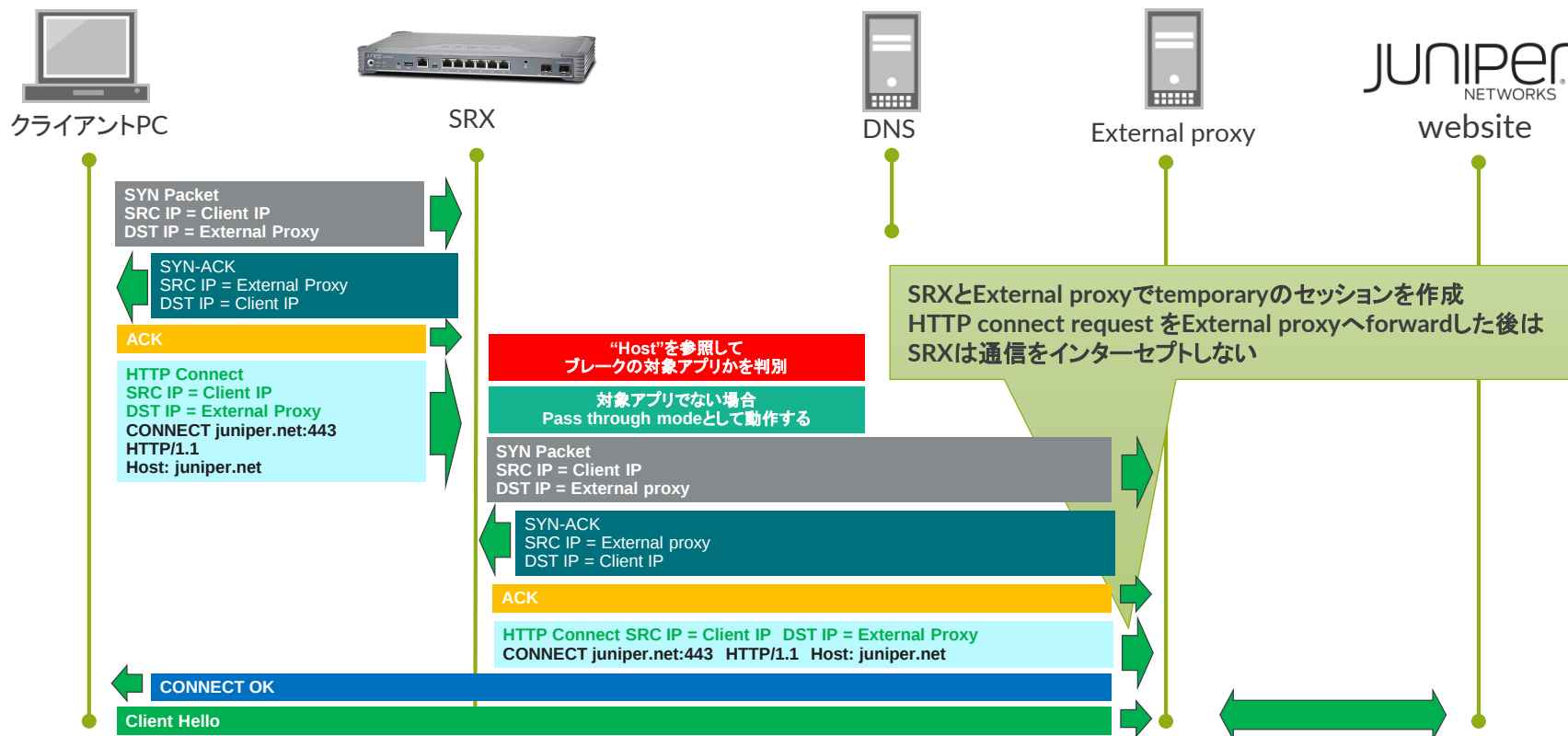
アプリケーションを判別した後、
ブレイクアウト対象のアプリケーション通信であれば**本来の宛先**に変更して通信させる。



ブレイクアウトを実施する際の動作



ブレイクアウトしない際の動作



SRXが提供するセキュリティ機能

次世代ファイアウォール機能

アプリケーションの
コントロールと可視化

侵入防御(IPS)

ユーザーベース
ファイアウォール

統合脅威管理(UTM)

アンチウイルス

アンチスパム

ウェブフィルタリング

最新のセキュリティ情報

ボットネット/C&C

GEO-IP

カスタムフィード&
ターゲット型攻撃

アンチマルウェア アンチゼロデイ

サンドボックス

回避型マルウェア防御

レポートニング&分析

SRX 基本サービス

ファイアウォール

NAT(アドレス変換)

VPN
(IPSec, SSL VPN)

冗長化
クラスタリング

ルーティング
(BGP, OSPF)

On Board GUI

MPLS

オートメーション

ブレイクアウトした通信ログの表示

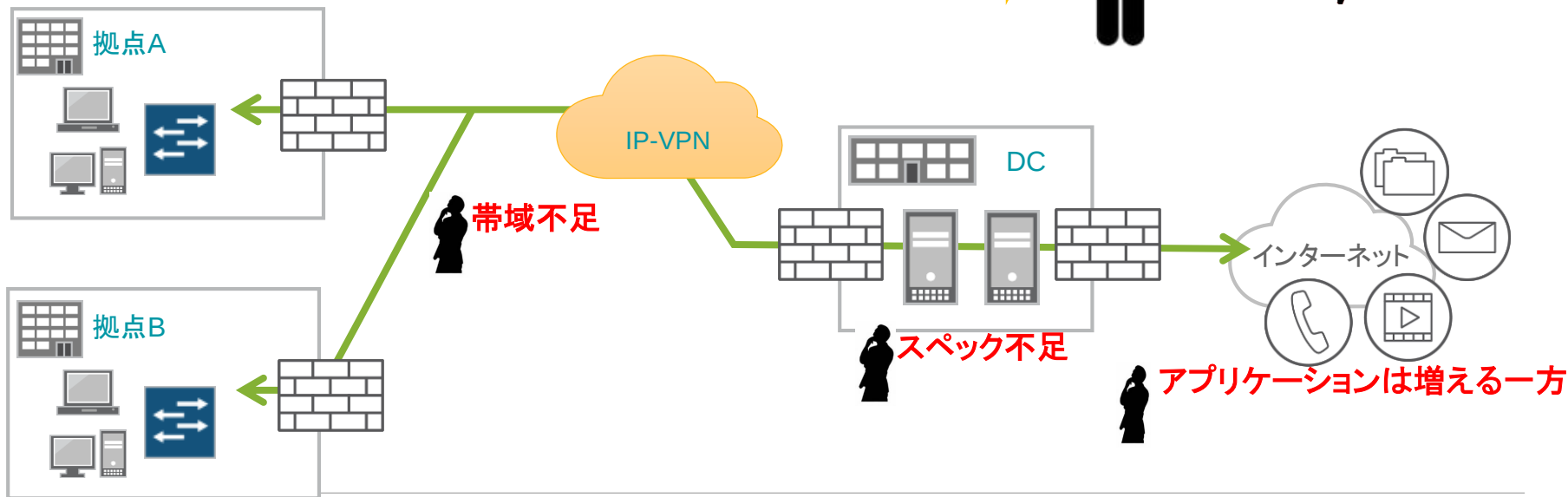
HTTPS(SSL)の通信でもアクセス先(URL)とユーザ名をログ出力することが可能。

Web Filtering Events ?					
Summary View Detail View					
				ユーザ名	アクセス先
Source Port	Destination Country	Destination IP	Destination Port	User Name	URL
370	 Singapore	111.221.29.254	443	katagiri	v10.vortex-win.data.microsoft.com
368	 Singapore	111.221.29.236	443	katagiri	array305-prod.do.dsp.mp.microsoft.com
367	 United States	40.96.3.210	443	katagiri	outlook.office.com
364	 United States	40.77.228.92	443	katagiri	watson.telemetry.microsoft.com
363	 Singapore	111.221.29.254	443	katagiri	v10.vortex-win.data.microsoft.com

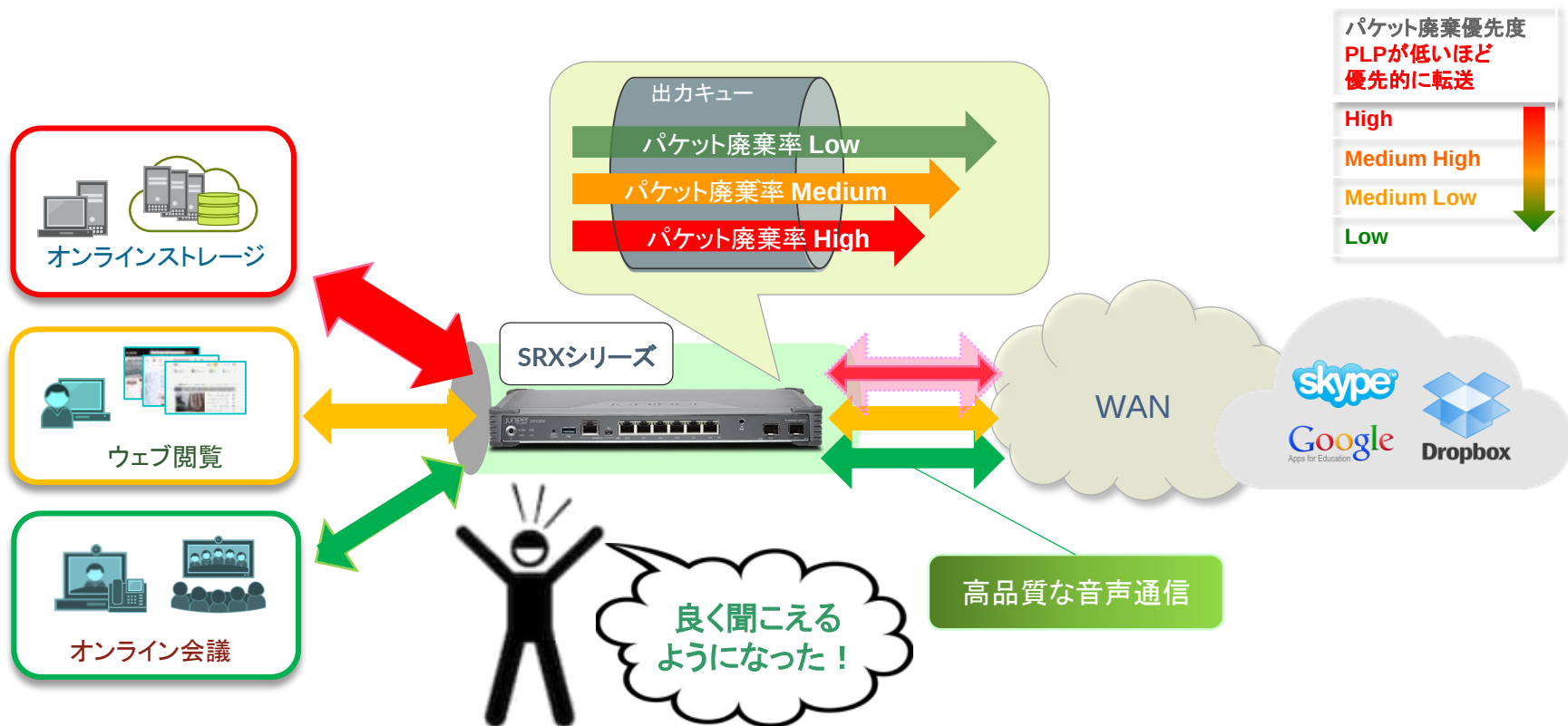
ビデオ動画や音声通話が品質劣化する要因

SaaSの普及に伴いWANに流れ込むトラフィック量が増大し
タイムクリティカルなアプリケーションが影響を受ける。

VoIPやオンライン会議の音声品質が低下し会話が聞き取り難くなる

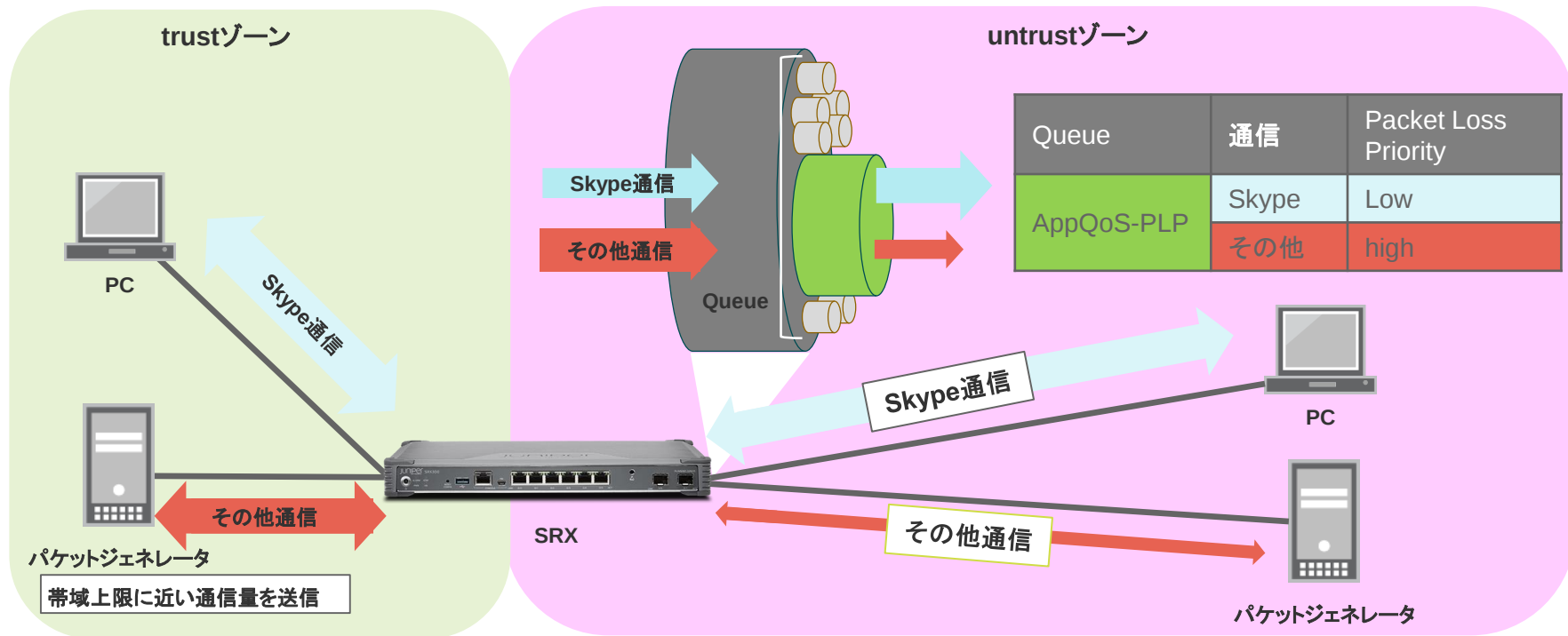


リアルタイム性の高いアプリケーションを最優先させ通信を制御



AppQoSデモ

帯域上限に近いトラフィックを送信し、Skypeビデオ映像の乱れを比較



AppQoSデモ

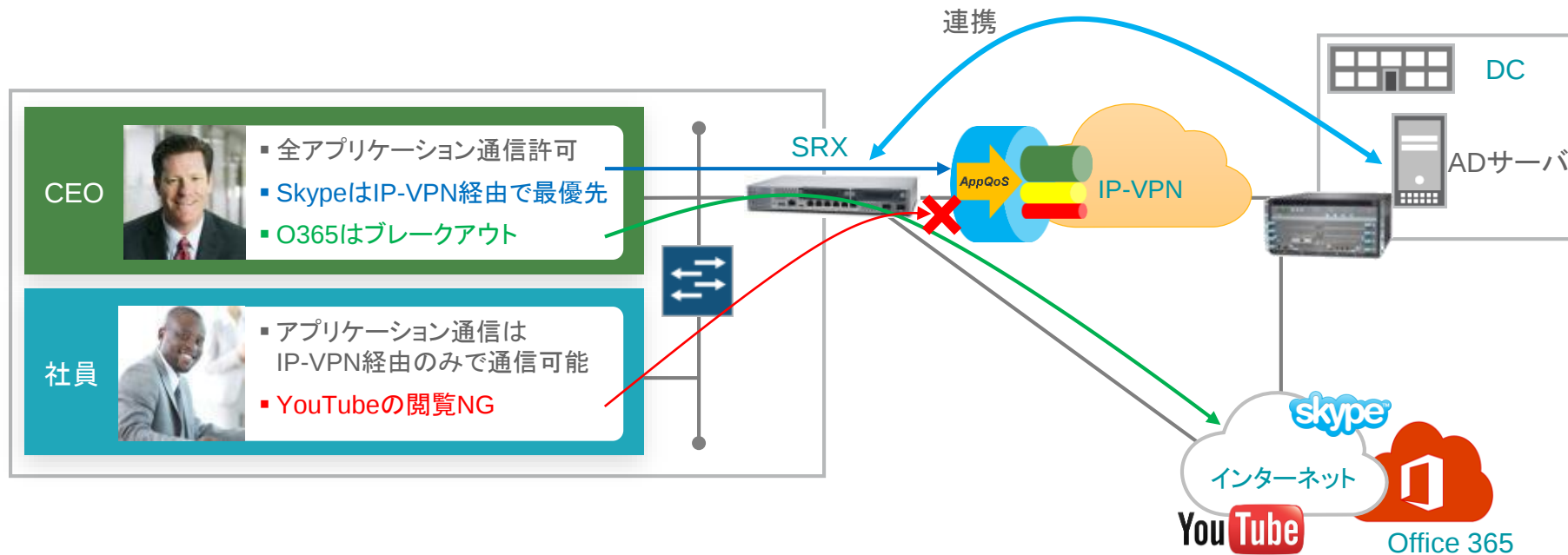
動画のリンクは下記を参照

<https://www.juniper.net/jp/jp/dm/security/>



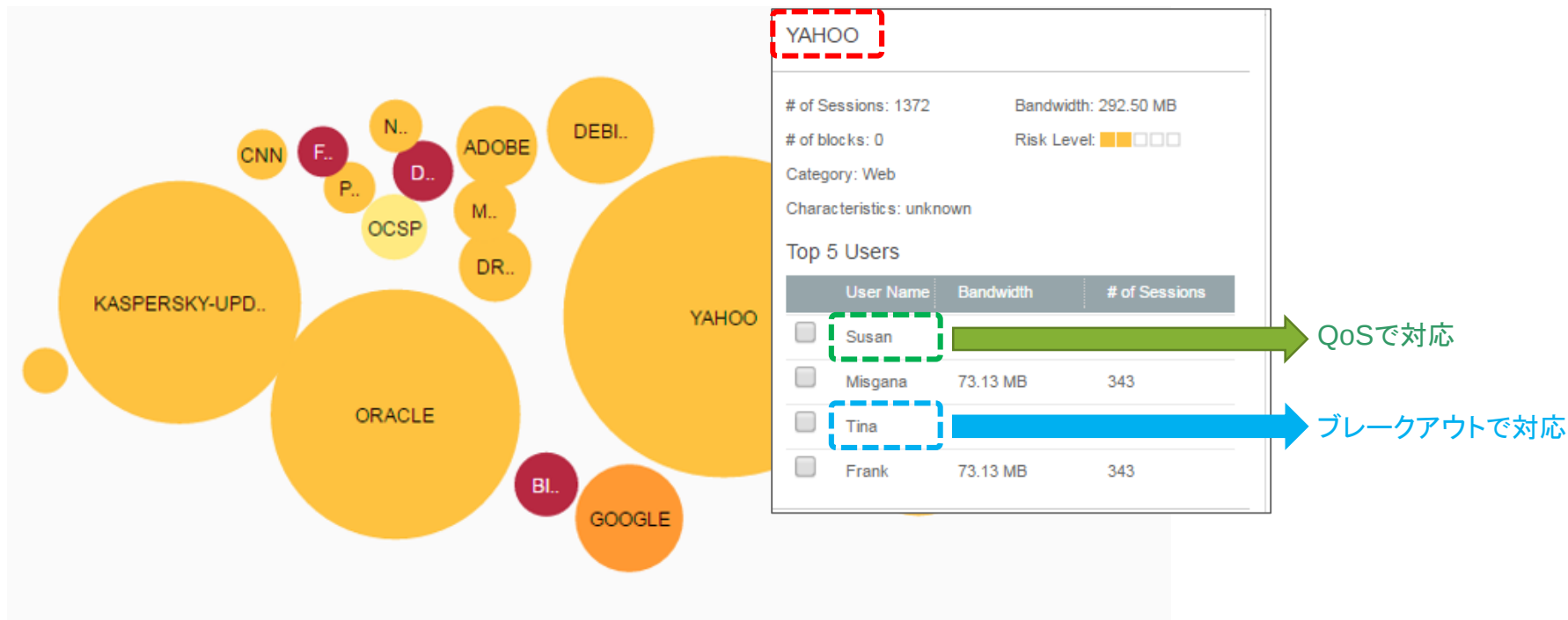
ユーザベースのアプリケーション制御

ユーザ属性とアプリケーションを条件に通信を制御



ユーザベースのアプリケーション制御

ユーザ属性とアプリケーションを条件に通信を制御

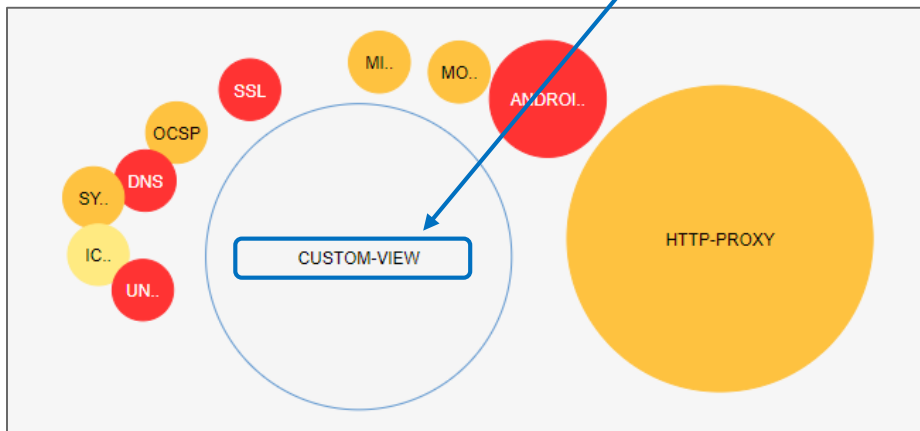


カスタムアプリケーション

Juniper Networksが定義していないアプリケーションもユーザ側で個別に定義して制御することが可能



```
set services application-identification application CUSTOM-VIEW over SSL signature s1 member m01 context ssl-server-name
set services application-identification application CUSTOM-VIEW over SSL signature s1 member m01 pattern ".*\juniper.net*"
set services application-identification application CUSTOM-VIEW over SSL signature s1 member m01 direction client-to-server
```



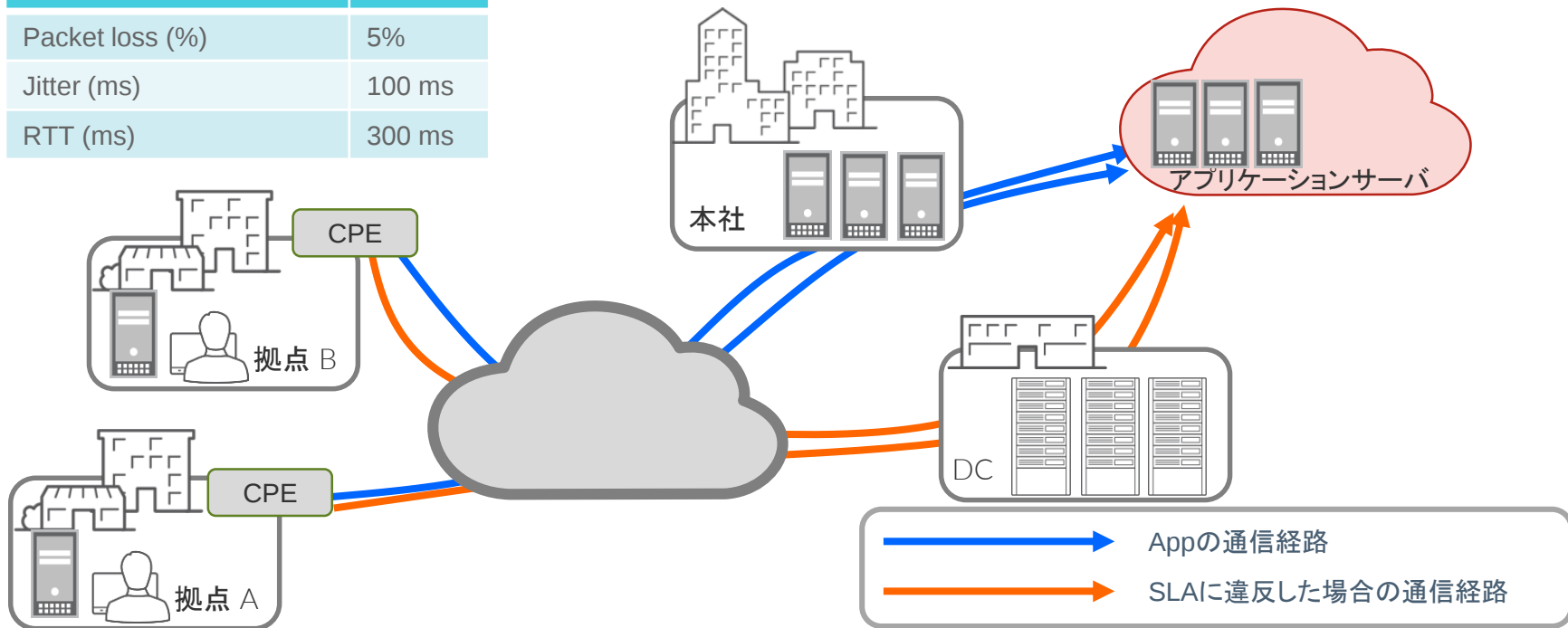


アプリケーション通信の最適化

アプリケーション単位でSLAを定義して経路を動的に変更するAPPQOE

該当するアプリケーションがSLAに違反した場合、経路を変更する

SLA	Value
Packet loss (%)	5%
Jitter (ms)	100 ms
RTT (ms)	300 ms



アプリケーション単位でSLAを定義して経路を動的に変更するAPPQOE

SLAを定義

SLA-Based Steering Profiles 🔍 Watch and Learn						
SLA Profiles List More ▾ 🔍 🔍 ⋮						
	Name	Traffic Type Profile	Packet Loss (%)	Jitter (ms)	RTT (ms)	Created By
☐	CSO-Sec	INTERNET	5 %	100 ms	300 ms	System
☐	CSO-Email	PREMIUM-INTERNET	5 %	100 ms	300 ms	System
☐	CSO-Productive	PREMIUM-INTERNET	5 %	100 ms	300 ms	System
☐	CSO-FileShare	INTERNET	5 %	100 ms	300 ms	System
☐	CSO-AV	VOICE-VIDEO	1 %	30 ms	150 ms	System

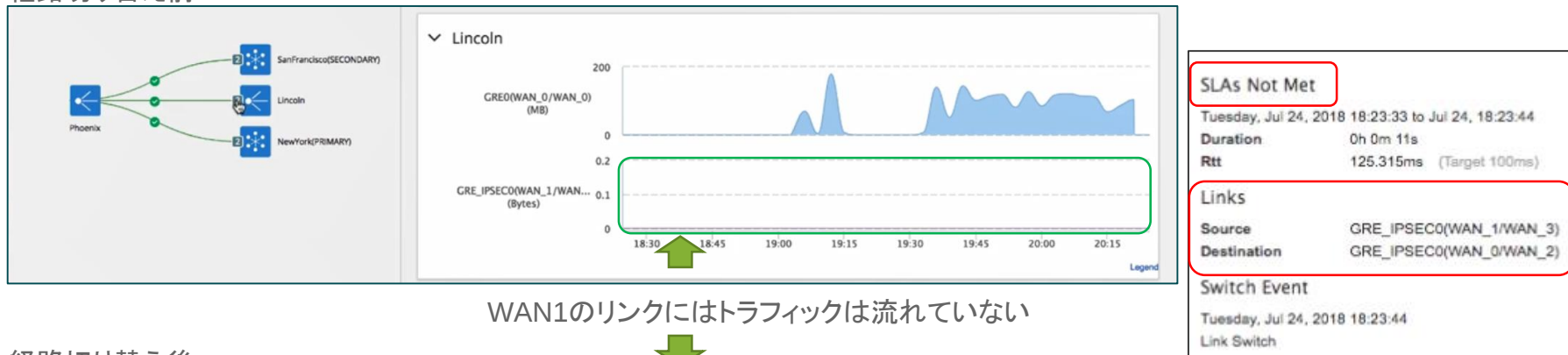
該当する通信に紐づける

30

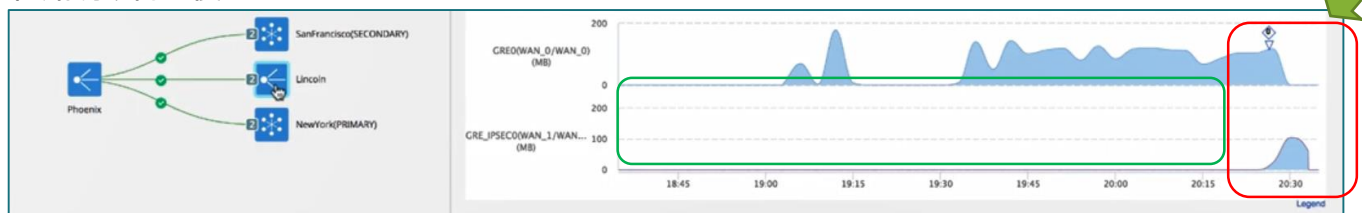
アプリケーション単位でSLAを定義して経路を動的に変更するAPPQOE

SLA違反を検知すると経路が切り替わる

経路切り替え前



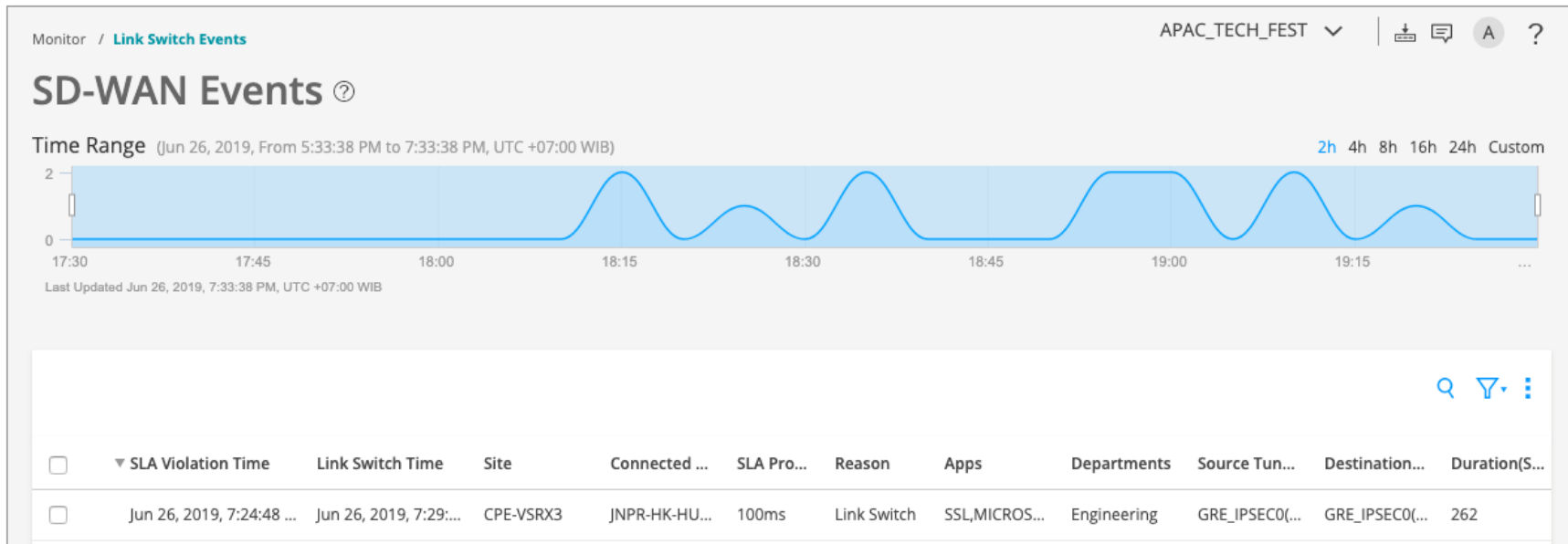
経路切り替え後



SLA違反のためWAN1からWAN2に切り替えて通信を開始

アプリケーション単位でSLAを定義して経路を動的に変更するAPPQOE

SLA違反は時系列で確認可能



アプリケーション単位でSLAを定義して経路を動的に変更するAPPQOE

動画のリンクは下記を参照

https://www.youtube.com/playlist?list=PLGvolzhkU_gR34Kxk_Qh5ONMtHXdDPEwk



JUNIPER NETWORKSが提供するアプリケーション制御

- 可視化したトラフィックをほぼ100%有効活用できる。
- Proxy環境であってもブレイクアウトのソリューションを展開できる。
- お客様の環境、例えばProxyサーバのアドレスをSRXに変更する、などの変更は不要
- アプリケーションを識別するシグネチャをユーザ側で定義することができる
 - 4000種類以上あるアプリケーションで定義していない通信もユーザ側で個別に定義して制御することが可能
- アプリケーションコントロールはSRX単体が保有する機能。
そのため、SD-WANコントローラーはあくまでオプション。
- SD-WANを検討したい場合、用途、規模に応じてコントローラーを選択できる
 - 簡易SD-WAN by Sky Enterprise, Full SD-WAN by CSO

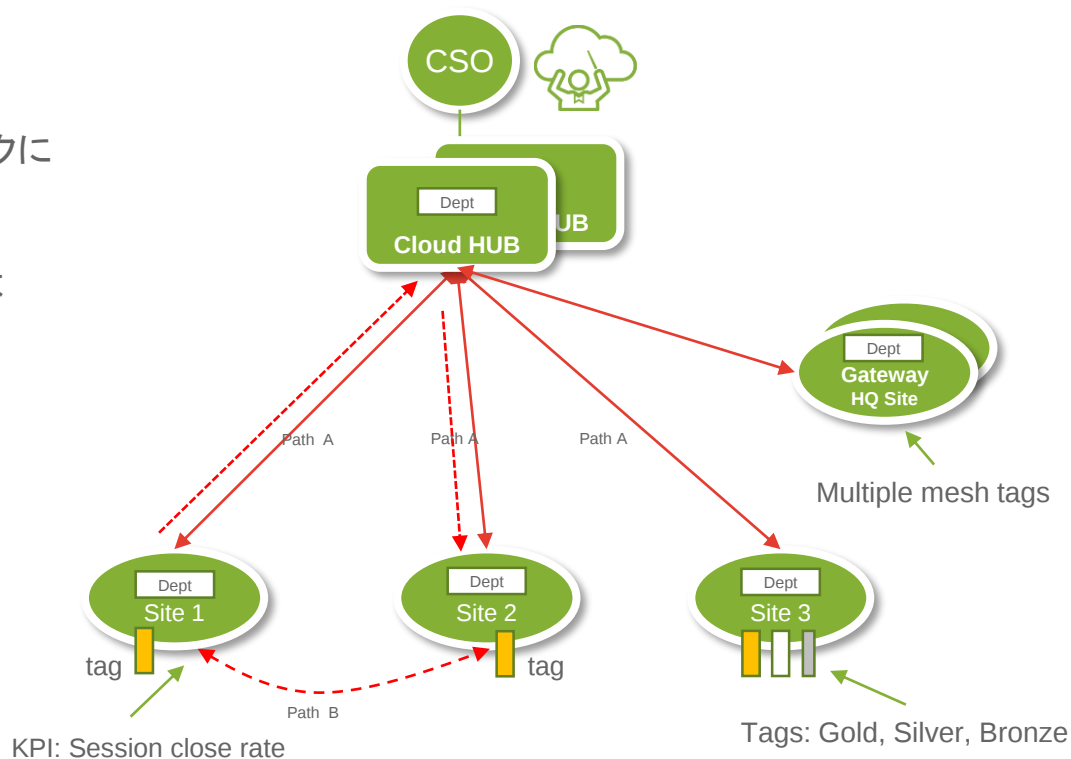


Appendix

拠点間通信の最適化

拠点間の通信を最適化するダイナミックVPN

1. 拠点間通信はデフォルトではハブを経由
2. セッション数が閾値を超えるとダイナミックに拠点間でトンネルを自動作成
3. セッション数が閾値を下回るとトンネルは自動消滅



拠点間の通信を最適化するダイナミックVPN

動画のリンクは下記を参照

https://www.youtube.com/playlist?list=PLGvolzhkU_gR34Kxk_Qh5ONMtHXdDPEwk





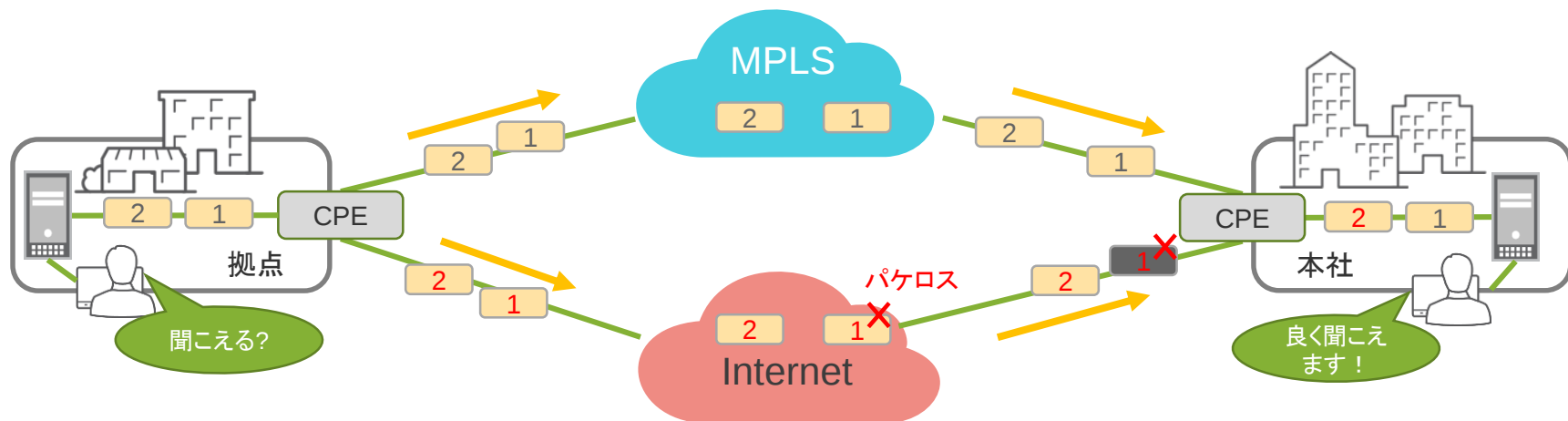
Appendix

拠点間通信の品質向上

パケットを複製して品質を高めるMULTI PATHING SUPPORT

該当するアプリケーションを複製してデータ遅延、欠損を補完する。

- パケットロスが発生した場合、欠損したパケットを補完する
- 同じパケットを複数受信した場合は2番目に受信したパケットを捨てる



A low-angle, upward-looking photograph of several modern skyscrapers with curved, glass-and-steel facades. The image is partially covered by a semi-transparent green rectangular overlay in the center. The sky is a pale, overcast grey.

THANK YOU

JUNIPER
NETWORKS | Engineering
Simplicity