vSRX – Virtual SRX
仮想化・クラウド環境のセキュリティ

ジュニパーネットワークス株式会社

2020年7月

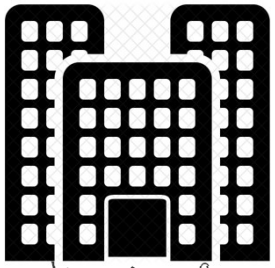
Juniper Networks | Engineering Simplicity

仮想化セキュリティー適用領域

ブランチ

セキュアSD-WAN

NFXにvSRXを実装



キャンパス

拡張性に優れたマルチコアvSRX

ハイパーバイザー:
- ESX
- KVM
- Hyper-V

データセンター

プライベートクラウド
マイクロセグメンテーション

SDN:
- NSX
- Contrail
- Nutanix

クラウド

クラウドセキュリティ

自動化

クラウド:
- AWS
- Azure
- IBM
- GCP

サービスプロバイダー

uCPE/vCPE

MEC

拡張性

NFV:
- OpenStack

vSRX – 唯一無二の仮想環境のセキュリティ

アドバンス・セキュリティと高性能ルーティングを兼ね備えた
オール・イン・ワン仮想アプライアンス

業界最速の仮想ファイアウォール (1コアあたりのスループット)

様々な利用要求に柔軟に対応 (DC・MSSP環境対応)

迅速な構築・運用をサポート (SDN統合と管理ポリシーの統合)

シンプル、拡張性、柔軟性を持つライセンス体系による
コストパフォーマンスの優位性

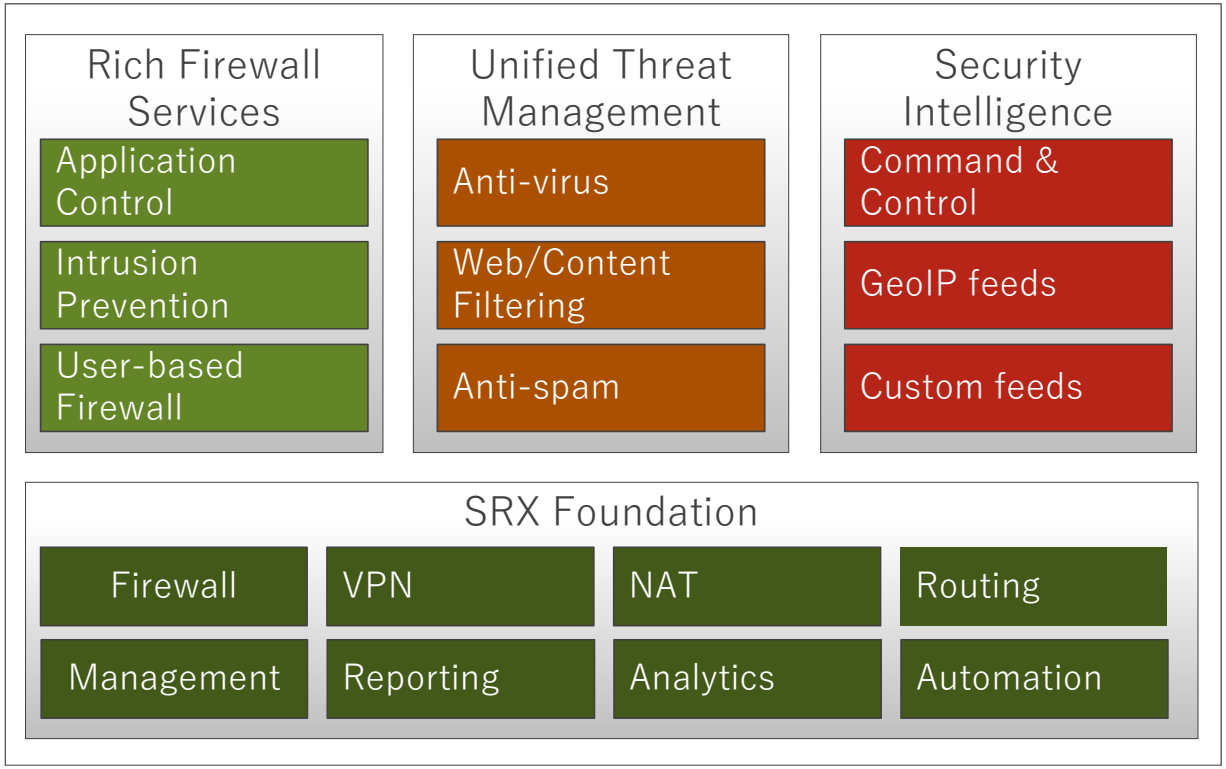
vSRX – 仮想アプライアンスとしてのSRX

SRXのVM版

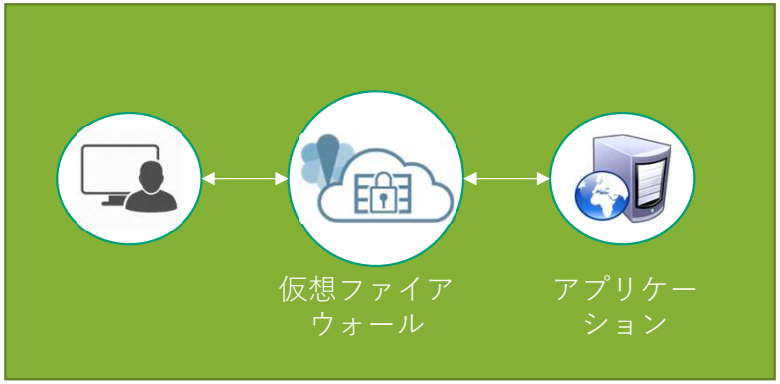
最もパフォーマンスがよく、
最もTCOが少ないFW

vCPU2コアで、ラージパケット
FWパフォーマンスは、18Gbps
IMIX FWパフォーマンスは、4Gbps

vCPU17コアで、ラージパケット
FWパフォーマンスは、100Gbps
IMIX FWパフォーマンスは、30Gbps



vSRX – 業界最速の仮想ファイアウォール



アプリケーションのパフォーマンスと遅延の解決はビジネスの最重要課題

- Highest Performance and Lowest TCO
- 2vCPUで18Gbps(ラージ) / 4Gbps(IMIX)ファイアウォールパフォーマンス
- 17vCPUで100Gbps(ラージ) / 30Gbps(IMIX)ファイアウォールパフォーマンス

オンプレミスへの導入	New AWS	Azure*
• DPDK • SRIOV	• Elastic Network Adapter	• Accelerated Networking

* ロードマップ

サポートプラットフォーム

インフラストラクチャーの選択はファイウォールの選択より優先される

ハイパーバイザー

- VMware ESXi 5.5, 6.0, 6.5, 6.7
- KVM – CentOS, Ubuntu, RedHat Enterprise Linux
- Microsoft – Hyper-V
- Nutanix - AHV

New

パブリッククラウド

- Amazon Web Services(AWS)
- Microsoft Azure
- IBM Cloud

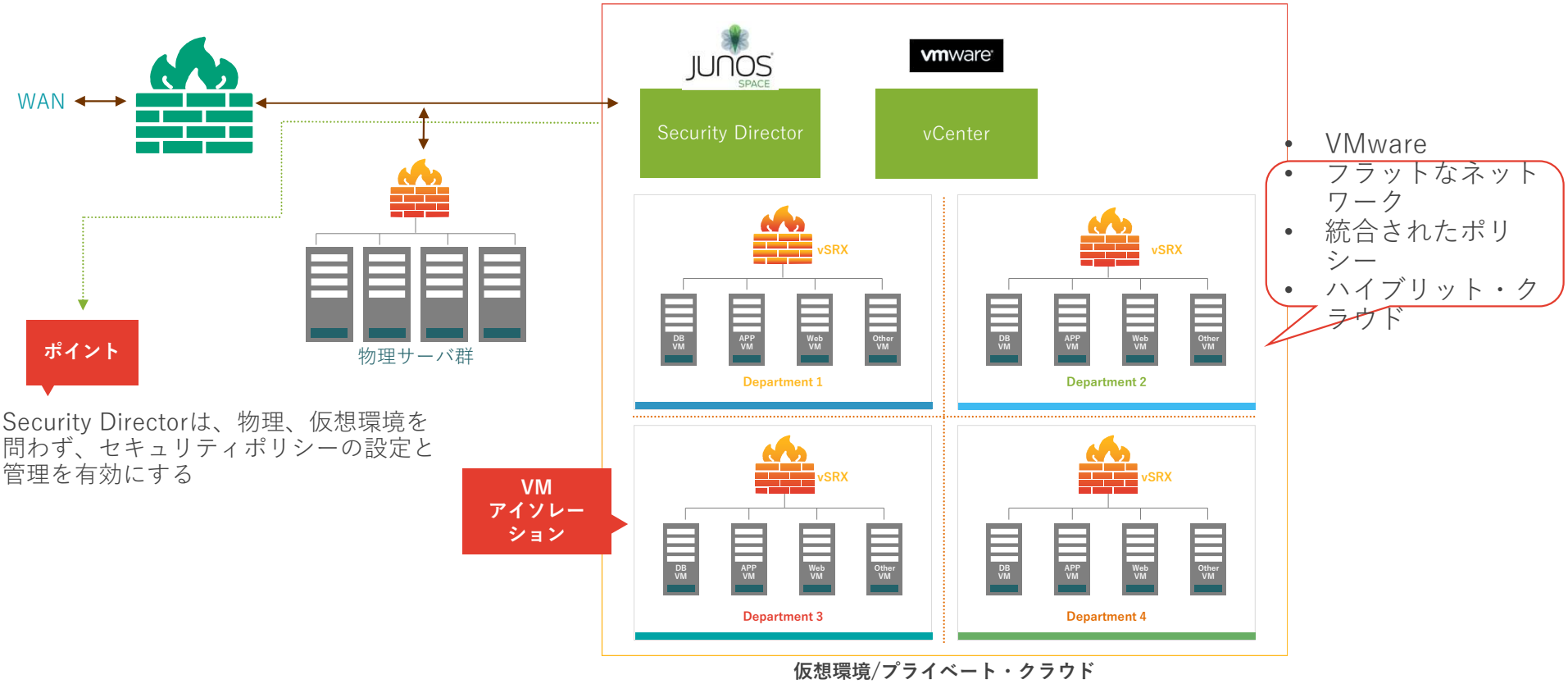
New

- Google Cloud
- Oracle Cloud

プライベートクラウド/SDNプラットフォーム

- VMware NSX-V
- OpenStack – Plugin
- Contrail Networking 3.x / 5.x

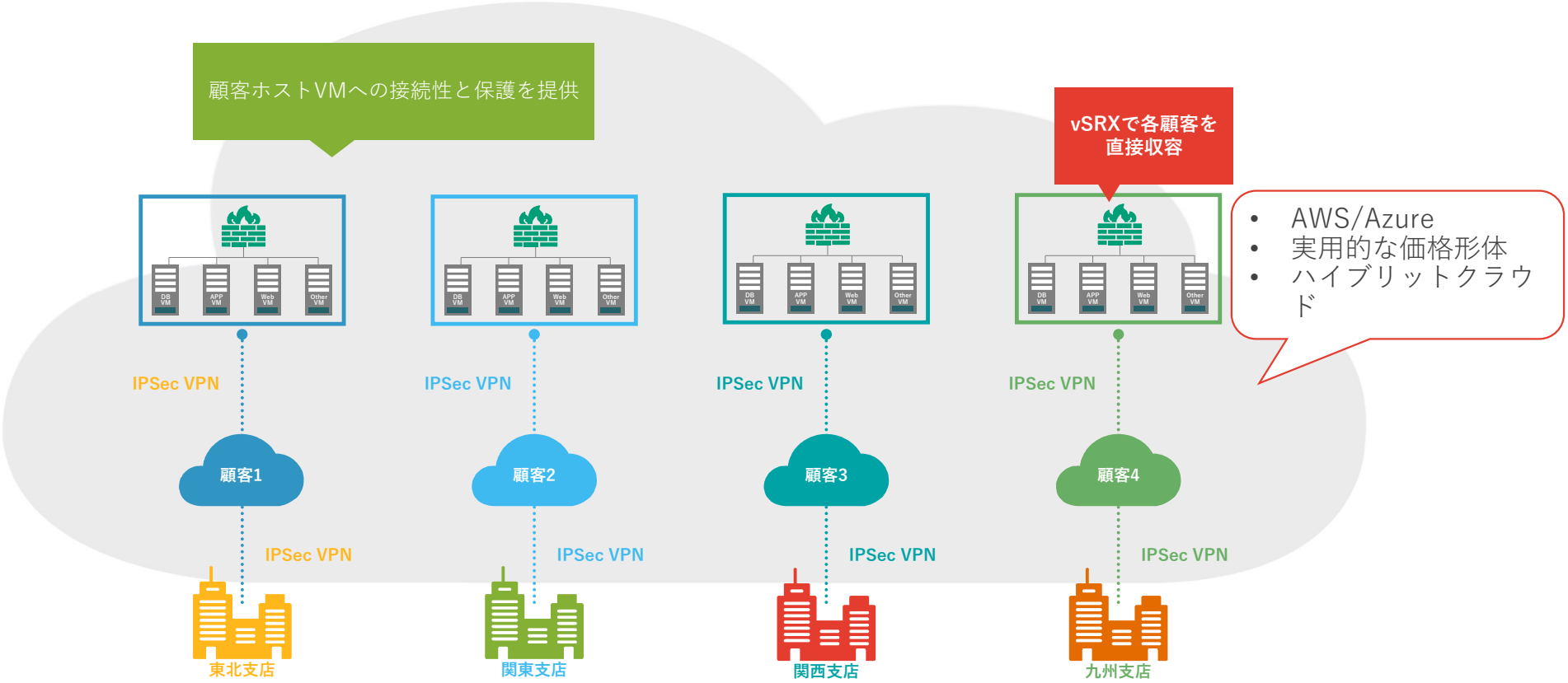
利用モデル #1: エンタープライズ・プライベート・クラウド



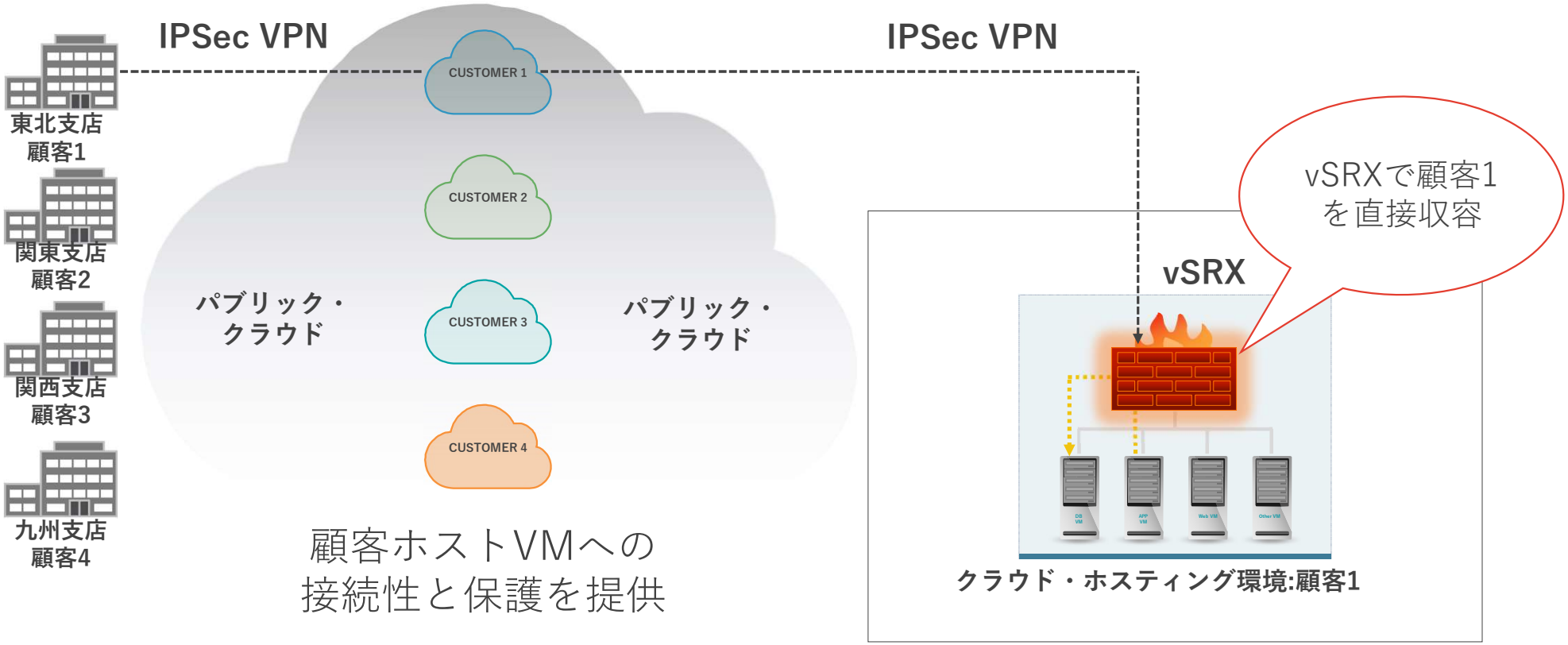
- VMware
- フラットなネットワーク
- 統合されたポリシー
- ハイブリット・クラウド

Security Directorは、物理、仮想環境を問わず、セキュリティポリシーの設定と管理を有効にする

利用モデル #2: パブリックとハイブリット・クラウド

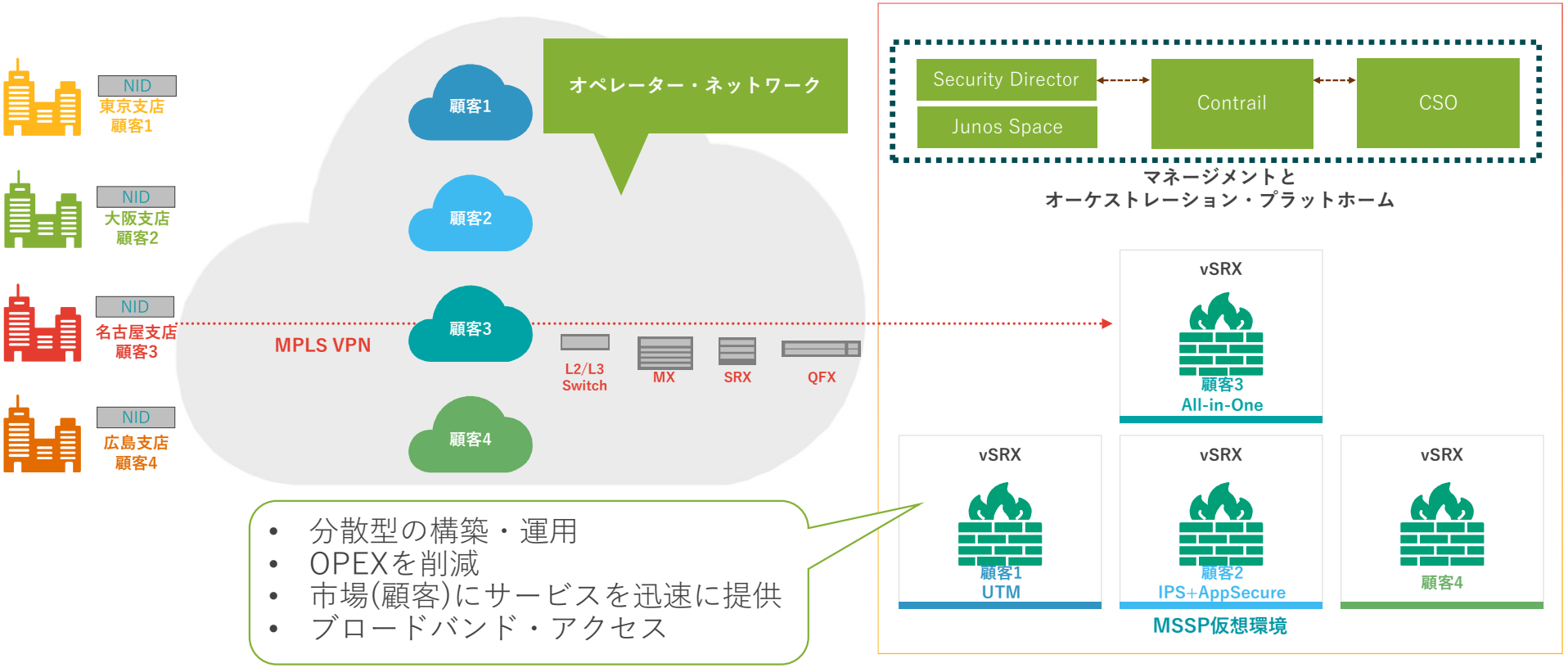


クローズアップ:クラウド・ホスティング・プロバイダーの利用例



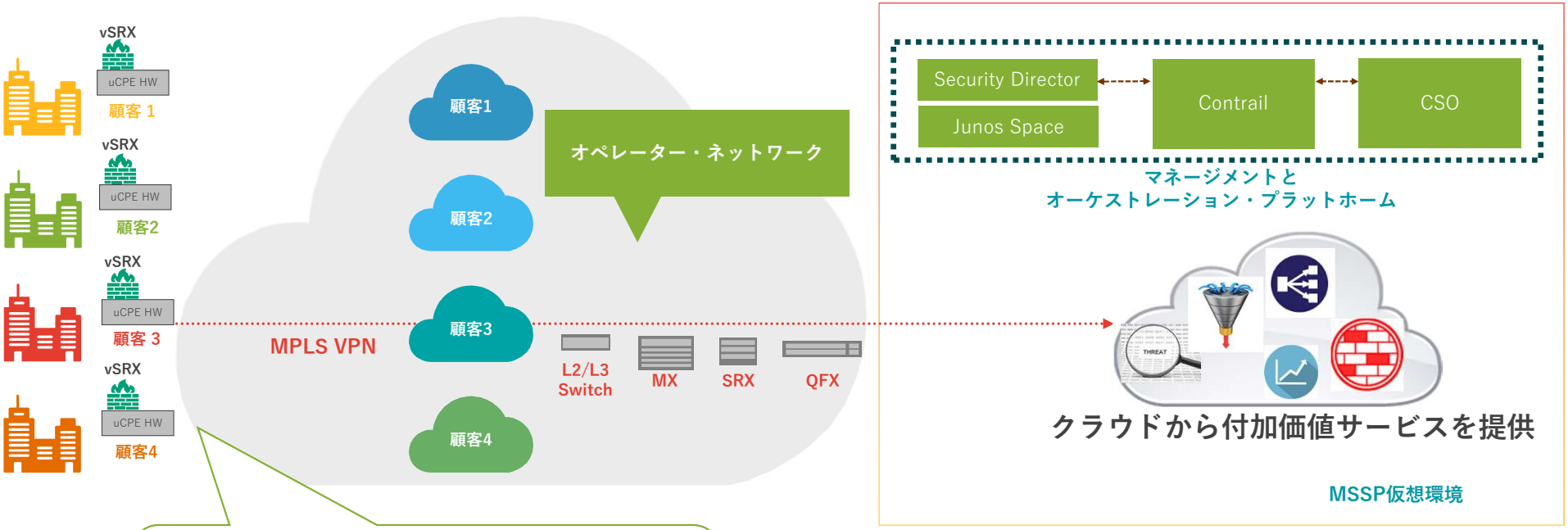
顧客ホストVMへの
接続性と保護を提供

利用モデル #3: サービス・プロバイダー・vCPE



- 分散型の構築・運用
- OPEXを削減
- 市場(顧客)にサービスを迅速に提供
- ブロードバンド・アクセス

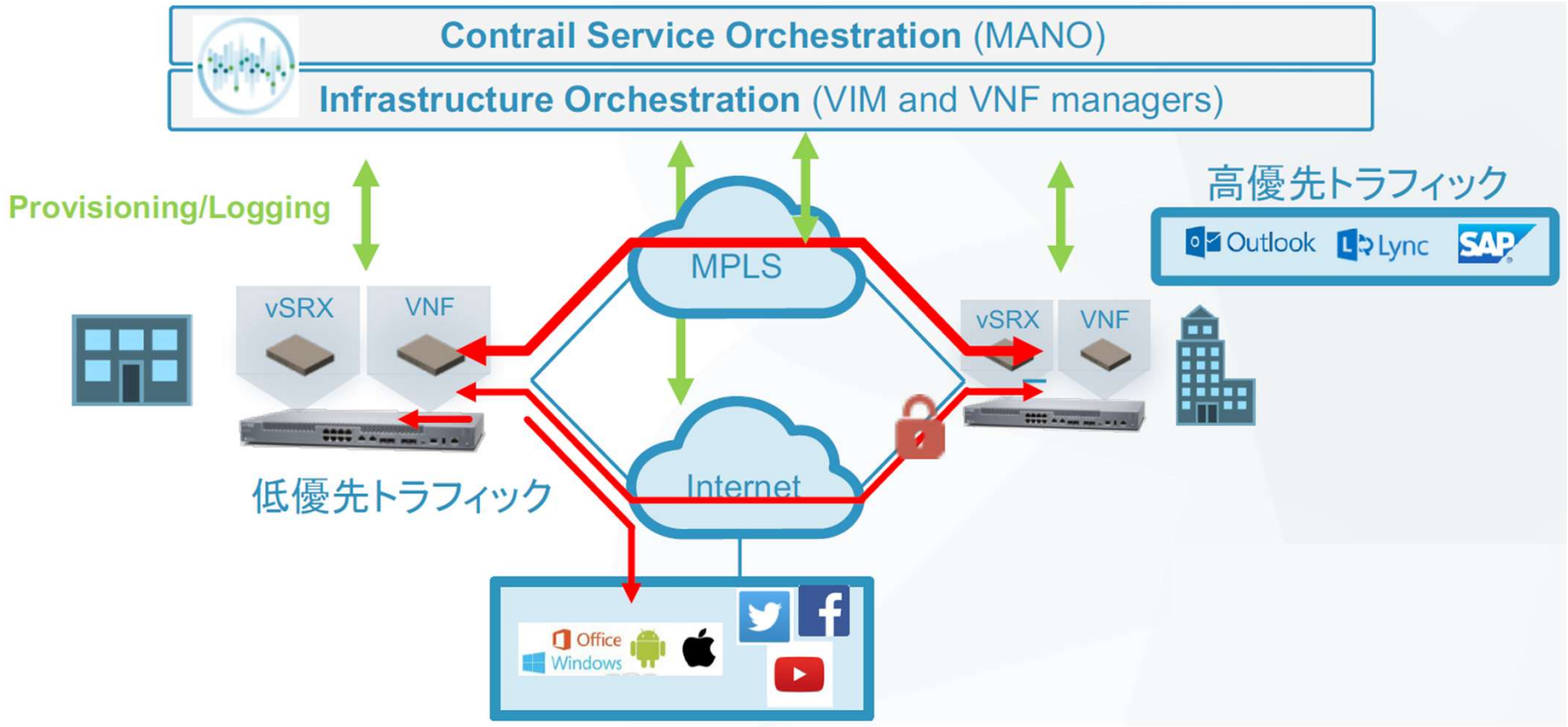
利用モデル #4: サービス・プロバイダー・uCPE



- 分散型の構築・運用
- OPEXを削減
- 市場(顧客)にサービスを迅速に提供
- コンプライアンス順守

利用モデル #5: サービス・プロバイダー SD-WANサービス

vSRXの機能により、アプリケーション・シグネチャベースのルーティングを提供

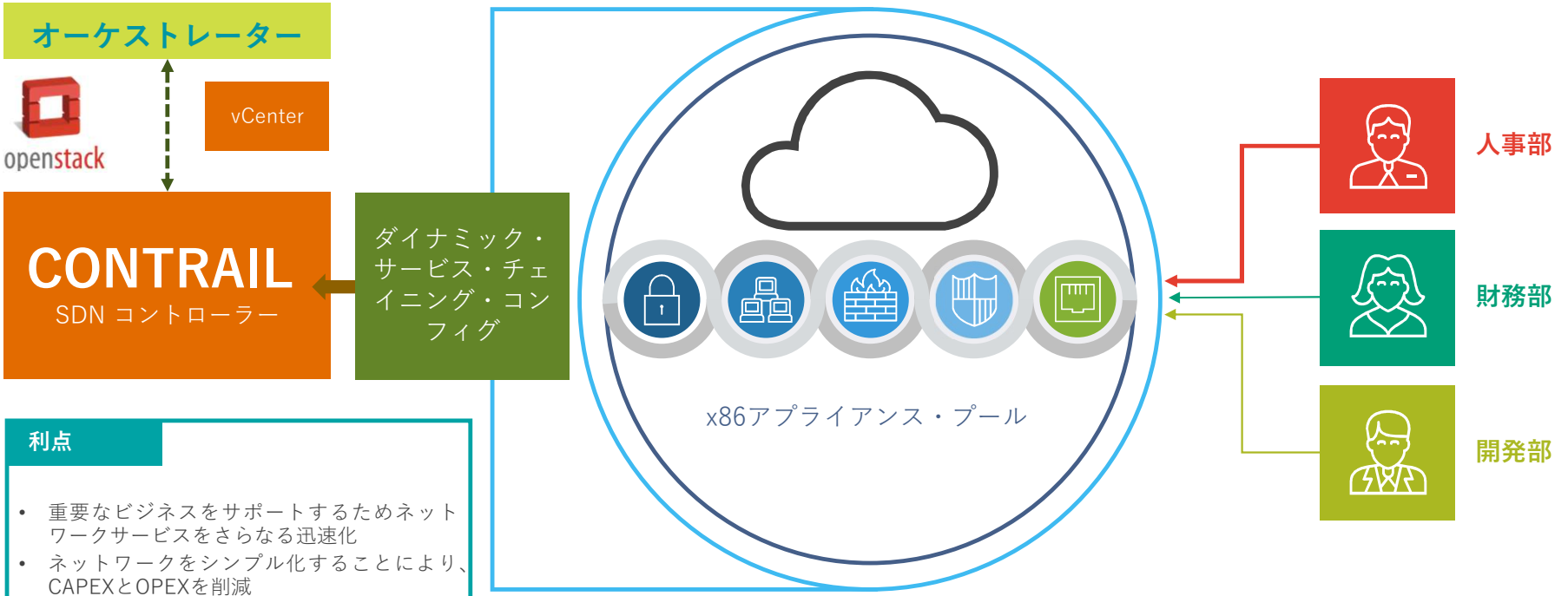


オーケストレーションとマネージメント

Junos Space Security Directorと仮想化

- 拡張性と迅速なセキュリティ管理を提供
- セキュリティポリシーの管理業務をより正確・容易に
- セキュリティポリシー・ライフサイクルを素早く、直感的なウェブベース管理で提供
- 仮想ファイアウォールのライフサイクル管理と大規模展開を支援

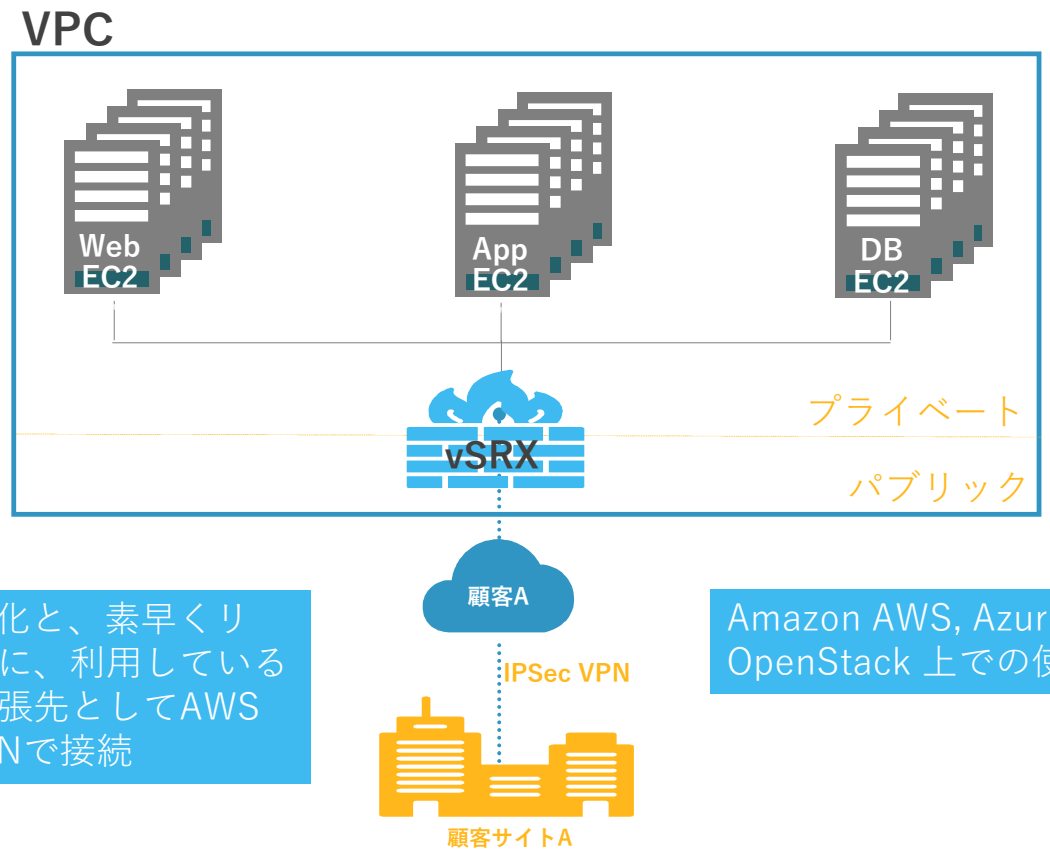
Contrailを利用したサービス・チェイニング



利点

- 重要なビジネスをサポートするためネットワークサービスをさらなる迅速化
- ネットワークをシンプル化することにより、CAPEXとOPEXを削減
- セキュリティと法令順守のため、シンプルにリソースを分割保護(マルチ・テナント)

IaaS・インテグレーション



Windows Azure

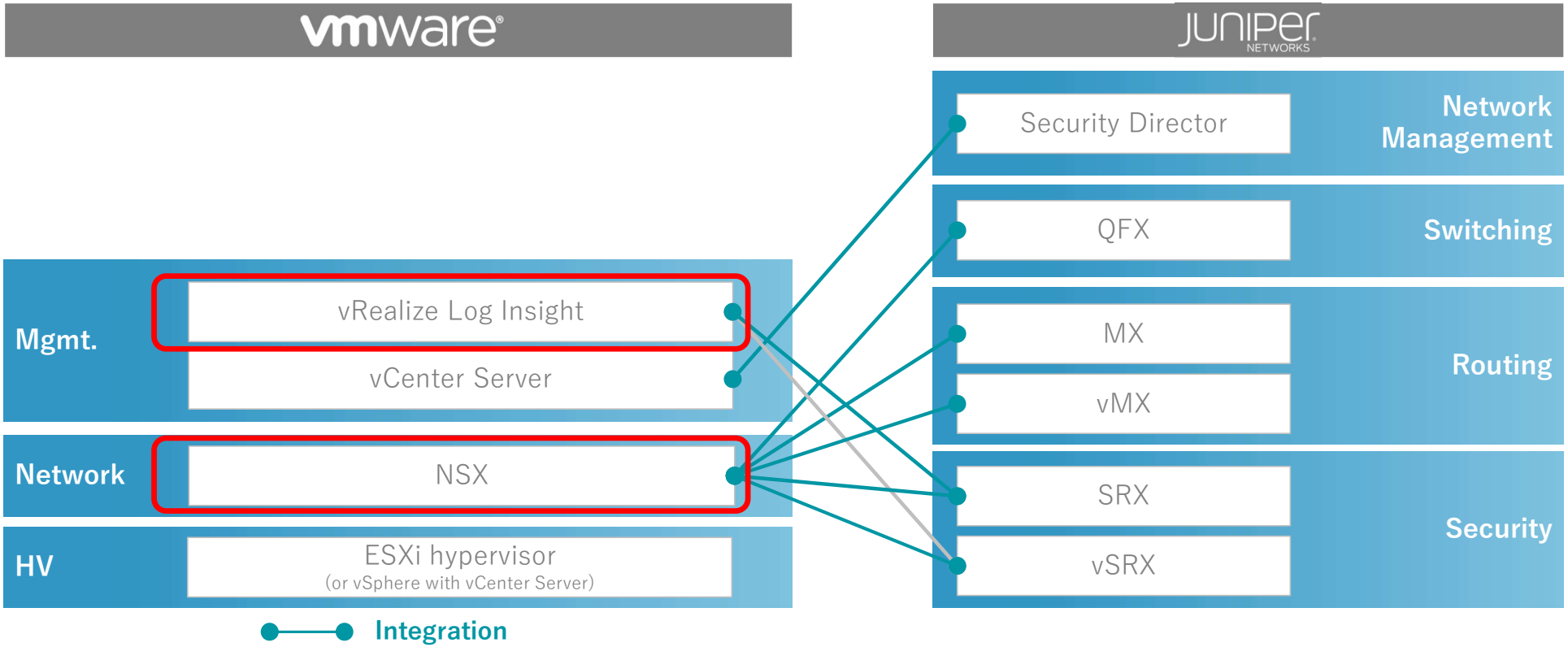
AWS

openstack

CAPEXとOPEXの最適化と、素早くリソースを拡張するために、利用しているオンプレミス環境の拡張先としてAWS VPCへvSRX IPSec VPNで接続

Amazon AWS, Azure に対応
OpenStack 上での使用をサポート

VMware 社製品とのインテグレーション



vSRX – NSX 連携

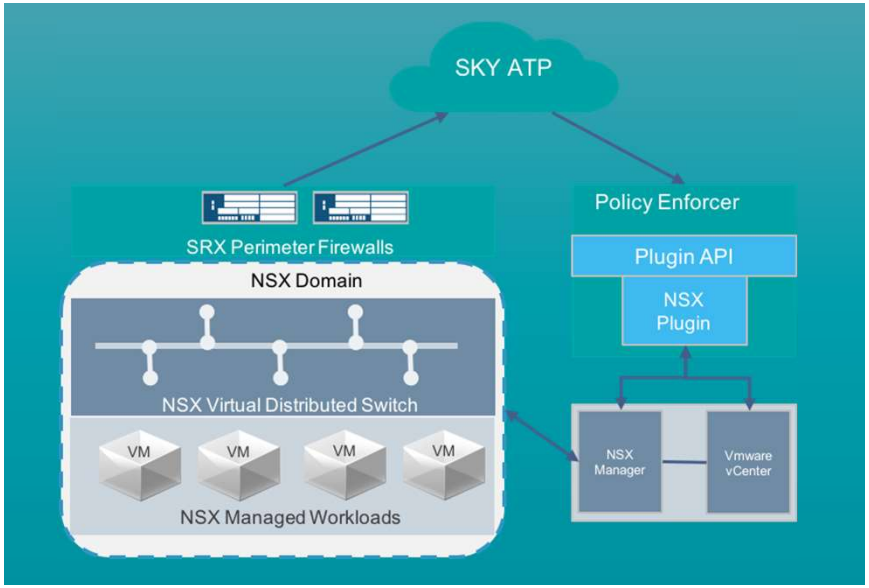
Use Case: NSXとvSRX連携で実現するマイクロセグメンテーション

ポリシーエンフォースメント

NSX ドメイン内でのマイクロセグメンテーション

- AppSecure (Layer-7 Firewall)
- IPS

管理機能の連携 (Policy Enforcer – NSX Manager)



鍵となる機能

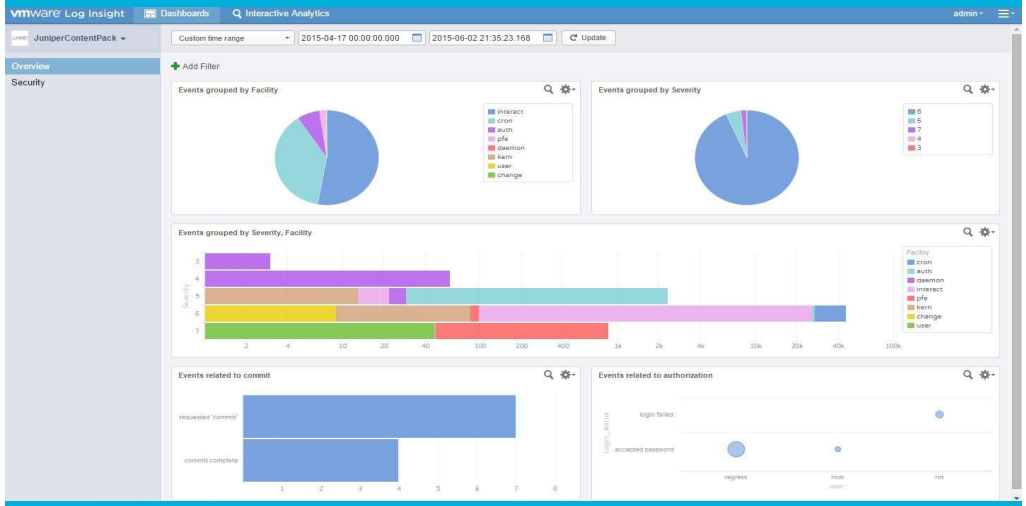
・ SD 上で、L7/IPS のポリシーがVM間通信、外部通信の両方で設定可能
・ ログ/レポートにVM名が含まれるようになり、閲覧時に容易な確認が可能
・ SDSNの対象として、NSXドメインも設定が可能 (SD 17.1以降)

適用によるメリット

・ 各NSXホストにvSRXを自動でプロビジョニング可能
・ VM間通信、外部通信を問わず、あらゆるトラフィックに対して、一貫したポリシー適用が可能に

Juniper's VMware vRealize Log Insight Management Pack

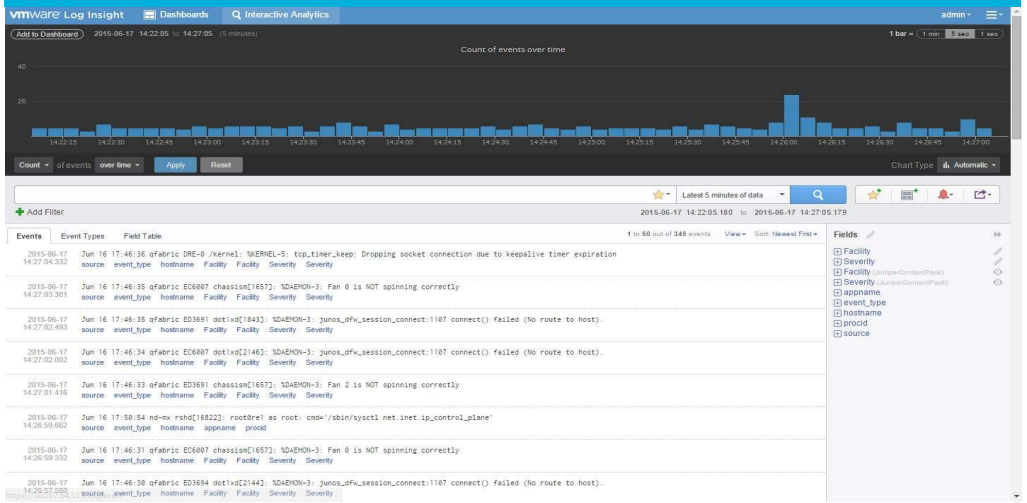
イベントオーバービューとセキュリティダッシュボード



Overview Dashboard Charts:
- Syslog by facility or severity
- Commit and authorization

Security Dashboard Charts:
- Analysis of FW Traffic Logs
- Drill Down to Virus

集約されたイベントとsyslog



Interactive drill down from charts into
- Security events and logs
- Syslog events and logs

- View tables of structured syslog extracted fields

vSRXのアップデート

vSRX 2.0

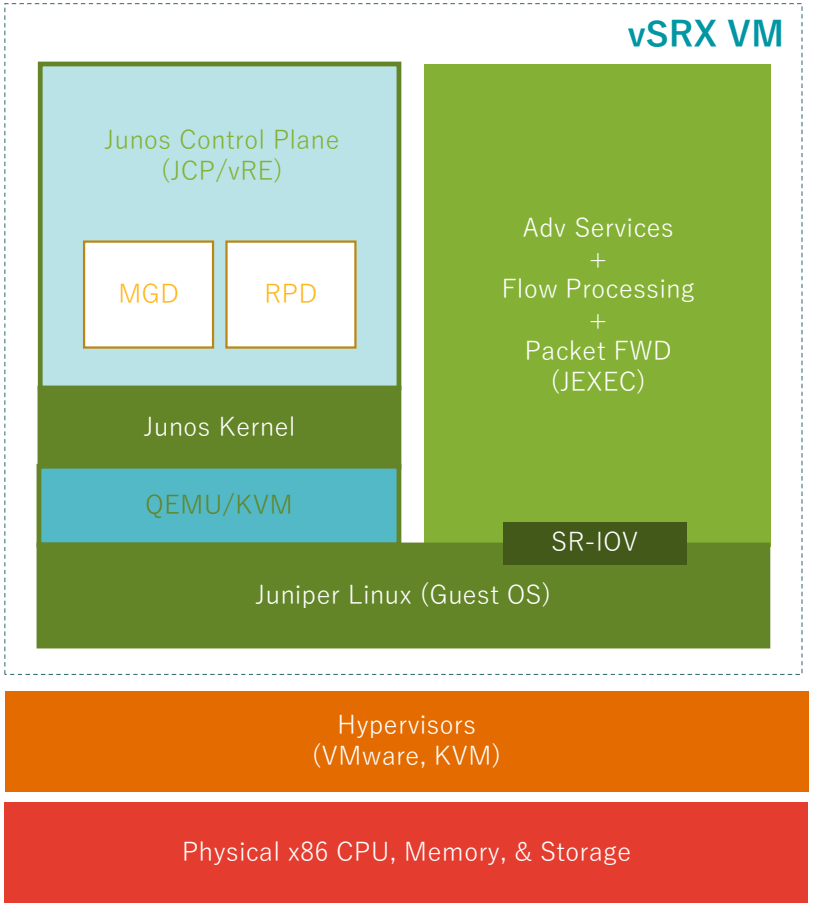
DPDKやSR-IOVに対応したことで、
パケット・フロー処理が向上した

プラットフォーム

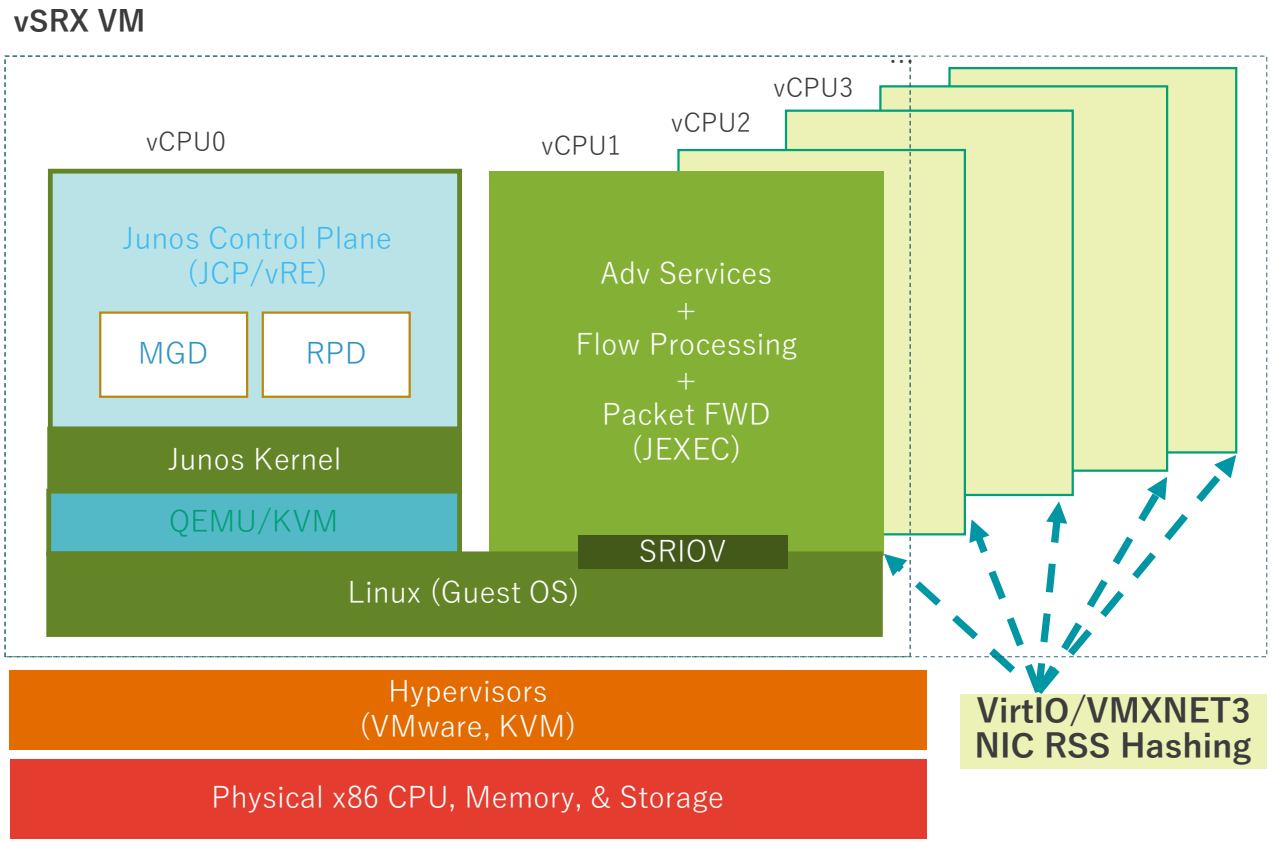
- VMware 5.1,5.5, 6.0, 6.5
- Ubuntu 14.04, 16.04, 18.04 (KVM)
- CentOS 7.2, 7.6, 7.7 (KVM)
- RHEL 7.6, 7.7(KVM)
- Contrail

ハイライト

- Junos 15.1- ベース
- DPDK 2.1
- SR-IOV
- VMXNET3とVirtIO (ドライバー・アップデート)
- Linux Base OS
- 64Bit Flowd
- 独立した管理I/Fサポート
- SCSI サポート
- SNMP拡張
- VMware Tools
- 最小構成 4G vRAM / 8G HD



vSRX 2.0アーキテクチャ



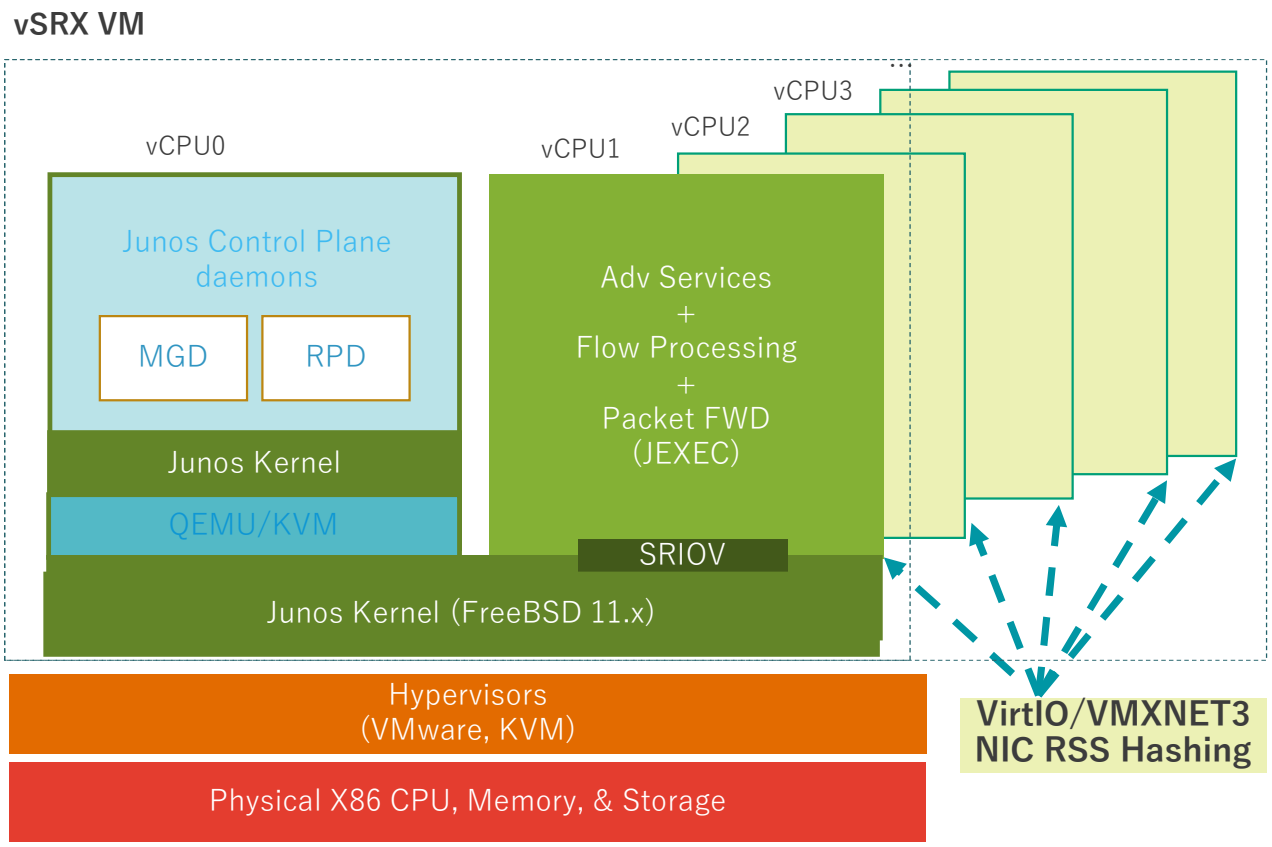
vSRX Flavor	vSRX-S	vSRX-M	vSRX-L	vSRX-XL
vCPUs	2 (1CP+1DP)	5 (1CP+4DP)	9 (1CP+8DP)	17 (1CP+16DP)
CPU Type	x86_64 multicore CPU Note: DPDK requires Intel Virtualization VT-x/VT-d support in the CPU.			
RAM	4G	8G	16G	32G
HDD	16GB			
Physical Interface	Intel X710/XL710, X520/540, or 82599 physical NICs for SR-IOV on vSRX Intel XL710 physical NICs for PCI passthrough support on vSRX			
Virtual Interface	SR-IOV VMXNET3 VirtIO		PCI-Passthrough	

vSRX 2.0 から vSRX 3.0 へ

vSRX 2.0の課題を解決した vSRX 3.0

- ハイパーバイザーにネステッドVMのサポートが必要
- 起動時間が遅い
- イメージサイズが大きい： 2 OSイメージ(LinuxとFreeBSD)
- JunosVMへの接続に管理ポート上でプロミスキャスモードが必要
- Live Migration(vMotion)が動作しない

vSRX 3.0アーキテクチャ



vSRX Flavor	vSRX-S	vSRX-M	vSRX-L	vSRX-XL
vCPUs	2 (1CP+1DP)	5 (1CP+4DP)	9 (1CP+8DP)	17 (1CP+16DP)
CPU Type	x86_64 multicore CPU Note: DPDK requires Intel Virtualization VT-x/VT-d support in the CPU.			
RAM	4G	8G	16G	32G
HDD	20GB			
Physical Interface	Intel X710/XL710, X520/540, or 82599 physical NICs for SR-IOV on vSRX Intel XL710 physical NICs for PCI passthrough support on vSRX			
Virtual Interface	SR-IOV VMXNET3 VIRTIO		PCI-Passthrough	
Image Size *	~~2.8GB~~ 700MB			
Boot time *	~~>8 minutes~~. ~1 minute			

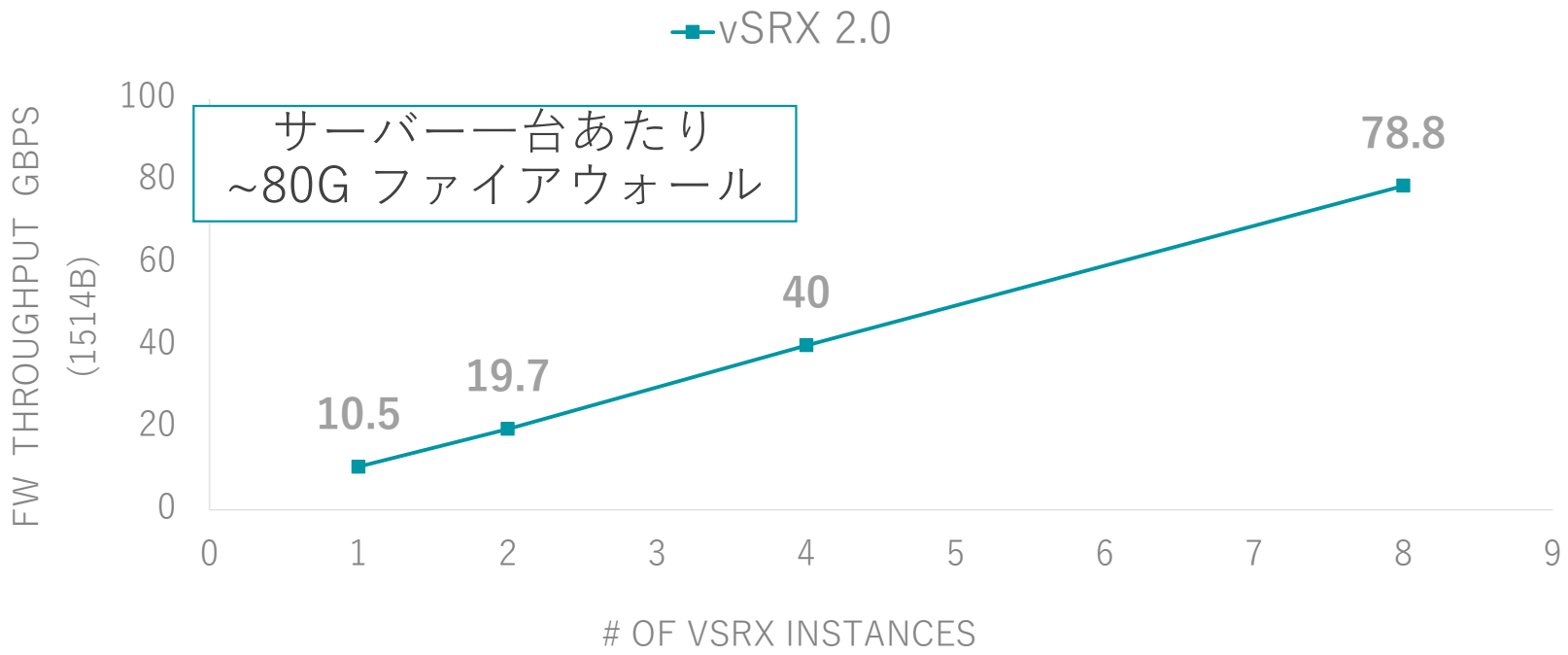
* Targeted numbers. Actual may be different

vSRX 2.0 (15.1X49-D70)パフォーマンス

Performance and Capacity	VMware VMXNET3		KVM VirtIO with OVS-DPDK	
vCPUs	2	5	2	5
Memory	4 GB	8 GB	4 GB	8 GB
Firewall throughput, large packet (1514B)	8 Gbps	20 Gbps	17 Gbps	20 Gbps
Firewall throughput, IMIX	2 Gbps	5.4 Gbps	4 Gbps	5.4 Gbps
AES+GCM IPSec VPN throughput (1420B)	2.7 Gbps	7 Gbps	2.7 Gbps	7 Gbps
Application visibility and control	2.9 Gbps	8.3 Gbps	2.9 Gbps	8.3 Gbps
IPS recommended signatures	1.8 Gbps	5.2 Gbps	1.8 Gbps	5.2 Gbps
TCP connections per second	50,000	60,000	50,000	60,000
Maximum concurrent sessions	512,000	1,000,000	512,000	1,000,000

Reference platform for performance: HP DL580 Gen 9 E7-8890 v3, 72 CPU * 2.493 Ghz; HT: Disabled with Intel 82599 NIC ixgbe version: 4.21; firmware version: 0x80000208; VMware version: 6.0; build: 3620759; KVM: Ubuntu 16.04 OpenVSwitch (OVS): 2.7.0.
All performance numbers are “up to” and will depend on underlying hardware configuration (some serverconfigurations may perform better).
Performance, capacity and features listed are based on vSRX running Junos OS 15.1X49-D70 release and are measured under ideal testing conditions.
Actual results may vary based on Junos OS releases and by deployments

vSRX 2.0 密度試験 (VMware 5.5 SRIOV有効)



VMインスタンスの数で、vSRX 2.0は、リニアにスケール

All the Above numbers are tested on Dell servers

- *VMware5.5+SRIOV-2.4Ghz Server – R820- 24 cores *2.393Ghz*

パブリッククラウド

AWSでサポートされているインスタンス(20.1以降)

インスタンスタイプ	vCPU	メモリ(GB)	vSRX3.0	RSSタイプ
c4.xL	4	7.5	VSRX-4CPU-7G memory	SW RSS
c4.2xL	8	15	VSRX-8CPU-15G memory	SW RSS
c4.4xL	16	30	VSRX-16CPU-30G memory	SW RSS
c4.8xL	36	60	VSRX-36CPU-60G memory	SW RSS
c5.L	2	4	VSRX-2CPU-3G memory	HW RSS
c5.2xL	8	16	VSRX-8CPU-15G memory	HW RSS
c5.4xL	16	32	VSRX-16CPU-31G memory	SW RSS
c5n.2xL	8	21	VSRX-8CPU-20G memory	HW RSS
c5n.4xL	16	42	VSRX-16CPU-41G memory	HW RSS
c5n.9xL	36	96	VSRX-36CPU-93G memory	HW RSS

Azureでサポートされているインスタンス

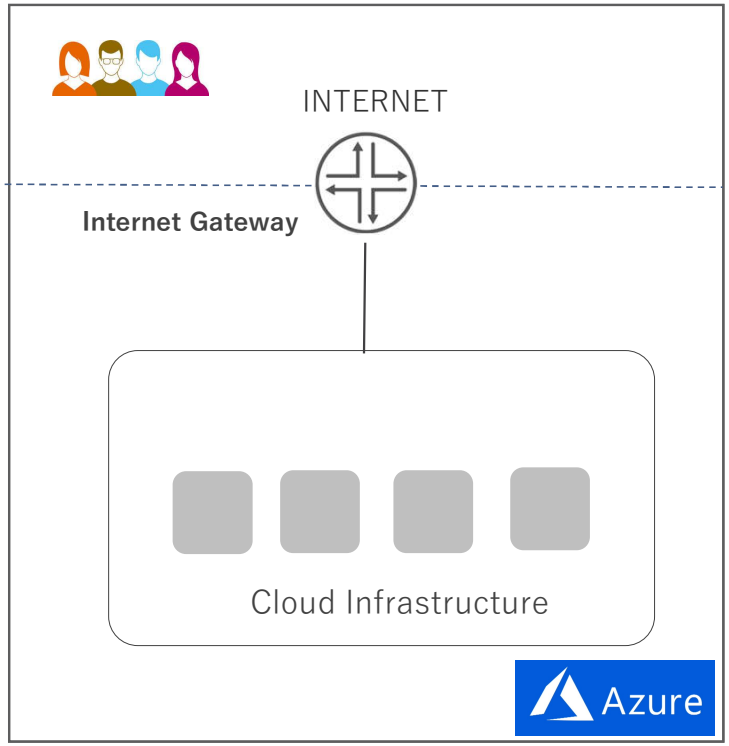
インスタンスタイプ	vCPU	メモリ (GB)	vSRX3.0	RSSタイプ
Standard_DS3_v2	4	14	VSRX-4CPU-14G memory	HWRSS
Standard_DS4_v2	8	28	VSRX-8CPU-28G memory	HWRSS
Standard_DS5_v2	16	56	VSRX-16CPU-56G memory	HWRSS

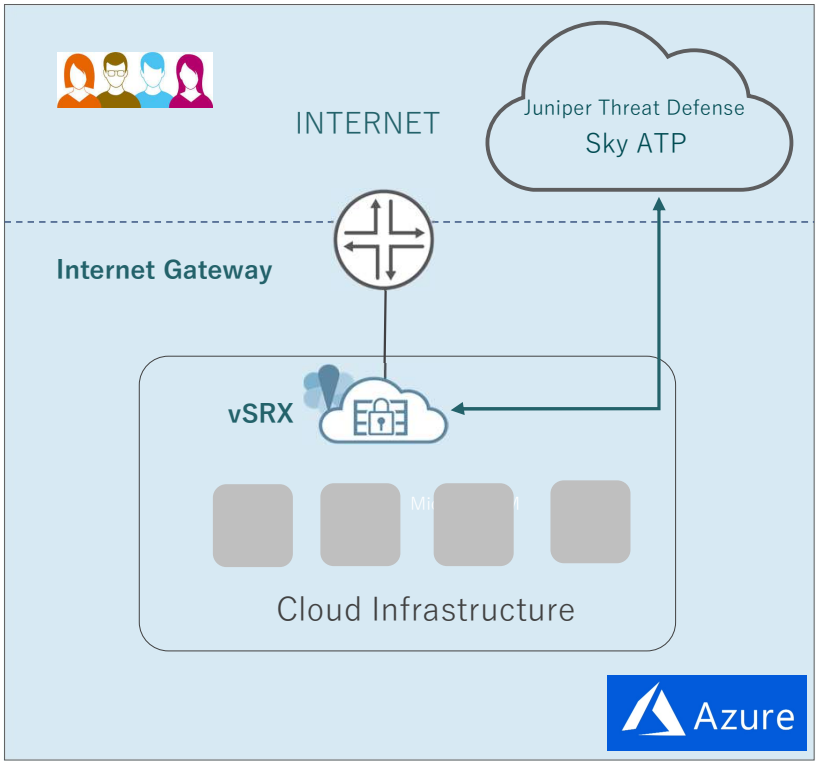
GCPでサポートされているインスタンス

インスタンスタイプ	vCPU	メモリ (GB)	vSRX3.0 Flavor Shows As	RSSタイプ
N1-standard-2	2	7.5	VSRX-2CPU-7G memory	HWRSS
N1-standard-4	4	15	VSRX-4CPU-15G memory	SWRSS
N1-standard-8	8	30	VSRX-8CPU-30G memory	SWRSS
N1-standard-16	16	60	VSRX-16CPU-60G memory	SWRSS

vSRX on Azure

vSRXを利用するメリット

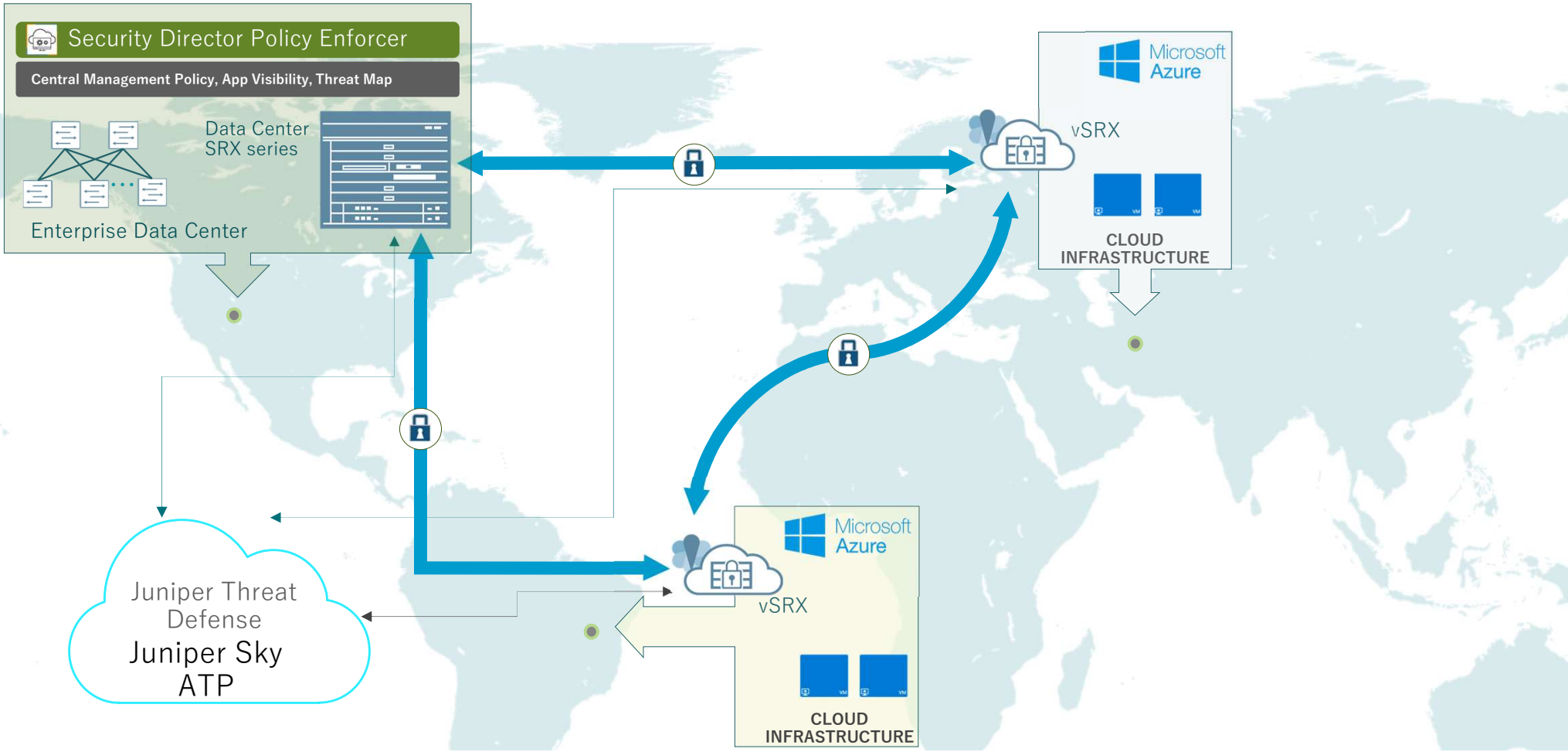




Hybrid Cloud	安全なオンプレネットワークをAzureクラウド内へ拡張 https://azuremarketplace.microsoft.com/en-us/marketplace/apps/juniper-networks.vsrx-security-gateway?tab=Overview
Management	CLI、APIとAzureマーケットプレースからSecurity Gateway Solution Template
Connectivity	Amazon AWSと同様にAzure vNET間でも暗号化トンネルの生成が可能
Deployment	AzureマーケットプレースからSecurity Gateway Solution Template https://www.juniper.net/documentation/en_US/vsrx/topics/task/multi-task/security-vsrx-security-gateway-solution-template-azure-marketplace-deploying.html
Transit VPC	従来の方式または、Transit VPCの利用が可能

SIMPLE & INTELIGENT SECURITY WHEREVER THE NETWORK GOES

セキュア・ハイブリット/マルチクラウド展開



サマリー

Carrier-class security and routing	JUNOSのルーティング、セキュリティ機能を付与
Better TCO	vSRXの低価格化とリソース要件の削減は、クラウドインフラの運用コストの削減に直結する
Unified Management	シンプル、セキュリティポリシーをシームレスに拡張するための直感的な管理、パブリッククラウドとハイブリットクラウド間のセキュリティ監視強化
Investment Protection	コンテナやJuniper Connected Securityへ移行可能な包括的な機能実装
Programmability	柔軟性の高いプログラミング機能実装は、DevOpには必要不可欠

SIMPLE & INTELIGENT SECURITY WHEREVER THE NETWORK GOES

vSRXコンテンツ紹介

GitHub:

https://github.com/Juniper/vSRX-Azure

vSRXソリューション紹介:

http://www.juniper.net/assets/us/en/local/pdf/solutionbriefs/3510617-en.pdf

動画とケーススタディ:

https://www.youtube.com/watch?v=3kTq0xJmNtM

https://www.juniper.net/us/en/solutions/pcm/public-cloud-security/

ライセンスと価格体系

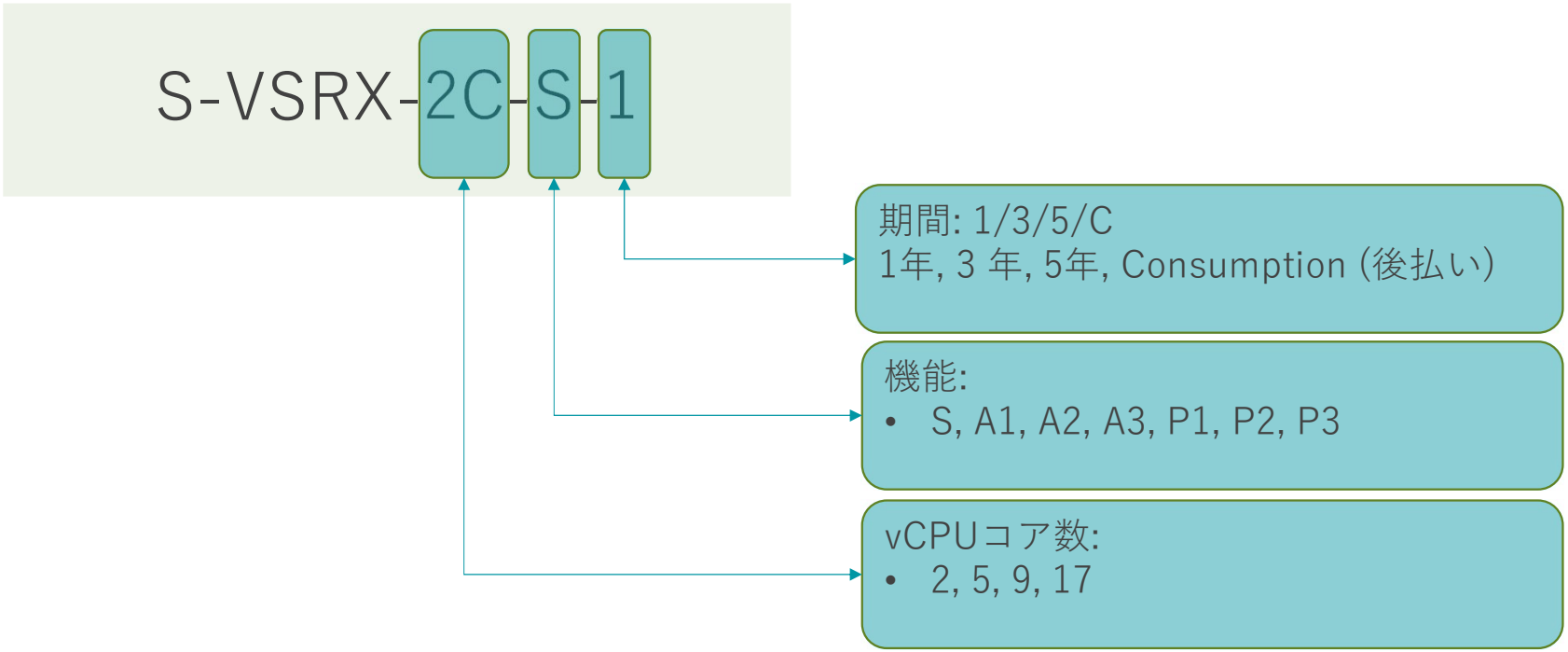
vSRXオーダリングガイドライン

- vSRXの価格は、vCPUコア数と機能バンドルライセンスの組み合わせで決まる
- All vSRX SKUs are bundled into Advanced and Premium tier which are subscription based only.
- Subscription SKU: 1年, 3年および 5年のサブスクリプションSKUにはサポートとメンテナンス/アップグレードが含まれる
- ライセンスのスタッキングが可能
- SKUは価格表を参照

vSRXライセンス体系

Premium-1	DC Security + ATP Cloud	Advanced-1 + ATP Cloud
Premium-2	NG Firewall + ATP Cloud	Advanced-2 + ATP Cloud
Premium-3	NG Firewall + ATP Cloud	Advanced-3 + ATP Cloud
Advanced-1	DC Security	Standard + IPS および AppSecure
Advanced-2	NG Firewall w/Sophos	Standard + IPS, AppSecure, URL Filtering, Cloud AVおよび Anti-Spam
Advanced-3	NG Firewall w/Avira	Standard + IPS, AppSecure, URL Filtering, On-box AVおよび Anti-Spam
Standard Software SKU	ファイアウォール機能 （ルーティング, ファイアウォール, NAT, VPN, スイッチング, MPLS）	

vSRX – SKU詳細



vSRX SKUマイグレーションマッピング

	既存SKU例		新規SKU例 (Flex)		
パフォーマンス	期間(年)	サブスクリプション	CPUコア	期間(年)	サブスクリプション
100M, 4G, 10G, 20G	Perpetual	Standard	2C, 5C, 9C,17C	1, 3, 5	Standard-Premium
	1, 3	ASEC-B App-Secure Bundle (STD + IPS + AppSecureを含む)			Advanced-1を購入
	1, 3	CS-B Content Security Bundle (STD + AppSecure, AV (Avira/Sophos), AS, EWF, Content Filteringを含む)			Advanced-2 or 3を購入
	1, 3, 5	ATP-B SkyATP bundle (STD + AppSecure, Content Security + ATP Cloudを含む)			Premium-2 or 3へアップグレード

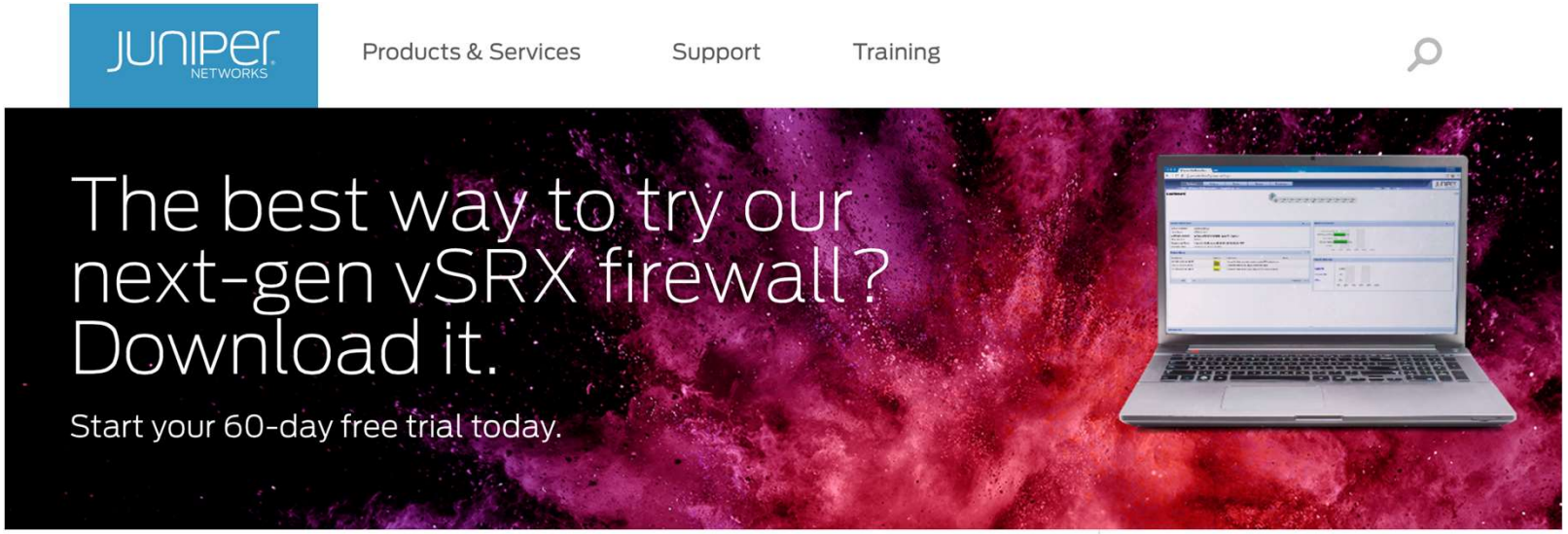
vSRX月額後払いモデル

- 月末のvSRXインスタンス使用数に応じて支払うモデル
- ハートナー・リセラーを通じて提供
- 個別の契約が必要
- 顧客は決められた請求期間の終わりに使用数を報告することが必要
  請求のこの報告に基づいて行われる
- 詳細についてはJuniper営業担当者に確認

検証ライセンスとデモ

vSRXとアドバンス・セキュリティ・サービスの評価ライセンス

- http://www.juniper.net/us/en/dm/free-vsrx-trial/
- vSRX標準ファイアウォールサービスは、60日間評価可能
- アドバンス・サービス(IPS, AppSecure, UTM)は、30日間評価可能



vSRX アドバンス・セキュリティ機能デモ

http://youtu.be/dOF6n-V7P00


Thank you
JUNIPER NETWORKS
Engineering Simplicity