vSRX 仮想ファイアウォール

製品概要

vSRX 仮想ファイアウォールは、高度なセキュリティ機能、堅牢なネットワーク機能と仮想マシン ライフサイクルの自動管理機能を含む、サービス プロバイダおよび企業向けの完全な仮想ファイアウォール ソリューションです。セキュリティ担当者は vSRX を使用することで、変動性の高い環境でもファイアウォールによる防御態勢を導入して拡張できます。

IPS、AppSecure、UTM など、高度なセキュリティ サービスを含む、vSRX 試用版のダウンロードは、www.juniper.net/jp/jp/dm/free-vsrx-trial/ からご利用いただけます。

製品説明

データ センターでは、サービスをこれまでになく迅速に効率的に提供するために、サーバーの仮想化に依存することが多くなってきています。その一方で、仮想データ センターには、物理的資産に求められる以上のセキュリティ上の配慮が必要とされます。

仮想データ センターの VM（仮想マシン）は、頻繁に行われる追加、移動、変更によって大きく変動する可能性があります。このことが、持続的な法令順守のために必要な、VM のインスタンス化におけるセキュリティ ポリシーの適用や VM の移動時のセキュリティ ポリシーの追跡を複雑にしています。つまり、動的で柔軟であるという仮想化の特性が原因で、物理的な世界では当然とされる可視性や制御性が容易に失われてしまうということです。

ネットワークやセキュリティの専門家は、組織のセキュリティを損なうことなく仮想化やクラウドの技術を活かすために、両方のバランスを慎重にとる必要があります。この課題に応えられるのは、進化する脅威に対抗しながら、信頼性、可視性、制御性を損なわずに仮想環境およびクラウド環境の俊敏性と拡張性にマッチするセキュリティ ソリューションだけです。

ジュニパーはこれらの課題に真正面から取り組み、受賞歴のある Juniper Networks® SRX シリーズ サービス ゲートウェイの機能に vSRX 仮想ファイアウォールを加えることで、仮想環境に対応しています。ジュニパーネットワークスの Junos® OS を備えた vSRX は、完全一体型の仮想セキュリティ ソリューションを提供しており、サービス プロバイダや企業向けの高度な L4-L7 セキュリティ サービス、堅牢なネットワーク、ライフサイクルの自動管理機能を備えています。

ネットワークとセキュリティ管理者は、仮想環境とクラウド環境の変化するニーズに応じて、vSRX の自動プロビジョニング機能を活用することで、ファイアウォール保護メカニズムを迅速かつ効率的に導入して拡張できます。管理者は、vSRX を Junos Space® Security Director の機能と組み合わせることによって、一元的な汎用プラットフォームから物理的資産と仮想資産の両方について、ポリシーの設定、管理、可視化の能力を大幅に向上させることができます。

仮想ネットワークおよびセキュリティ サービス用の vSRX 製品はネットワーク機能仮想化（NFV）の使用事例に幅広く対応しているため、サービスに特化したアプリケーションをソフトウェアに導入することを検討中のサービス プロバイダや組織に適しています。また、vSRX は ジュニパーネットワークス Contrail、ジュニパーネットワークス OpenContrail、その他のサード パーティー ソリューションにも対応しており、さらに OpenStack などの次世代のクラウド オーケストレーション ツールと直接または API を介して統合できます。

表 1：vSRX UTM の特長とメリット

特長	説明	メリット
アンチウィルス	• POP3、HTTP、SMTP、IMAP、および FTP プロトコル上でスパイウェア、アドウェア、ウィルス、キーロガーなどのマルウェアを検知してブロックする、評判の高まったクラウドベースのアンチウィルス機能 • アンチマルウェア技術のリーダーである Sophos Labs との提携により実現したサービス	• 一流のアンチウィルス専門家によって提供される高度な防御策により、データ漏えいや生産性の損失をもたらす可能性があるマルウェア攻撃に対抗します。
Web フィルタリング	• 広範なカテゴリー オプション（90 種類以上のカテゴリー）や、第 1 級の Web セキュリティ専門プロバイダである Forcepoint が提供するリアルタイムのスコアカードをはじめとした、拡張 Web フィルタリング機能	• 生産性の損失や、悪意のある URL による影響から保護すると同時に、ビジネスに不可欠なトラフィック用のネットワーク帯域幅を確保します。
コンテンツ フィルタリング	• MIME タイプ、ファイル拡張子、プロトコル コマンドに基づく効果的なインバウンド/アウトバウンド コンテンツ フィルタリング機能	• 不注意による、または悪意のあるファイル送信およびネットワーク上の悪意のあるコンテンツから保護し、侵害とデータ漏えいの危険を最小化します。
アンチスパム	• セキュリティ専門会社の Sophos Labs との連携により提供された、マルチレイヤー型のスパム防御、最新のフィッシング URL 検知、標準ベースの S/MIME、Open PGP、および TLS 暗号化、MIME タイプと拡張子に基づくブロッカーの機能	• 優れた電子メール フィルタリング機能とコンテンツ ブロッカー機能により、ソーシャル ネットワーキング攻撃や最新のフィッシング詐欺による高度で永続的な脅威に対する防御を行います。

アーキテクチャと主要コンポーネント

高度なセキュリティ サービス

今日の高度な攻撃に対抗することを目的として、従来のファイアウォール、個々のスタンドアロン アプライアンスやソフトウェアを中心に構築された、一体化されていないレガシー システムを導入する方法は、もはや適切とは言えません。ジュニパーの高度なセキュリティ パッケージでは、ユーザーが現代の組織による進化する個別のニーズや常に変化する脅威に合わせて複数の技術を導入できます。技術やポリシーなどのセキュリティ機能はリアルタイムで更新され、常に最新の状態に保たれます。

vSRX は、Unified Threat Management（UTM）、侵入検出および防止（IDP）、Juniper Networks AppSecure によるアプリケーション制御と可視化サービスを含む、用途の広い高度な優れたセキュリティ サービスを提供します。

統合脅威管理（UTM）

vSRX は、最高レベルのアンチウィルス、アンチスパム、Web フィルタリングとコンテンツ フィルタリングによる総合的なコンテンツ セキュリティ機能を有し、マルウェア、ウィルス、フィッシング攻撃、侵入、スパム、その他の脅威に備えています（表 1 を参照）。

侵入防御システム（IPS）

vSRX の IPS は、データを調査し、影響を受ける前に発生中の攻撃をブロックしたり、ファイアウォールで一連のルールを作成したりすることで、IT ネットワークへのアクセスを制御し、システムを攻撃から保護します。IPS はジュニパーのアプリケーション セキュリティ機能とネットワーク インフラストラクチャを密接に統合し、脅威を緩和してさまざまな攻撃や脆弱性を阻止します（表 2 を参照）。

表 2：vSRX IPS の特長とメリット

特長	説明	メリット
ステートフル シグネチャ インスペクション	適切なプロトコル コンテキストによって判別されたネットワーク トラフィックの関連部分に限定して、シグネチャが適用されます。	誤検知を最小限に抑え、柔軟なシグネチャ作成を可能にします。
プロトコル デコード	65 を超えるプロトコル デコードと、500 を超えるコンテキストに対応し、プロトコルが適切に使用されるようにします。	プロトコルの正確なコンテキストによって、シグネチャの精度が改善されます。
シグネチャ	異常や攻撃、スパイウェア、アプリケーションを特定するための 15,000 種類以上のシグネチャが存在します。	攻撃が正確に特定され、既知の脆弱性を悪用しようという試みが検知されます。
トラフィック正規化	再構築、正規化、プロトコル デコードに対応します。	難読化方式により、他の IPS 検知を迂回しようとする試みをシステムが無効にします。
ゼロデイ攻撃防御	プロトコル異常検知と、脆弱性が新しく発見された当日中の対応パッチの提供を実現します。	ネットワークは、新しい攻撃に対してもすでに保護された状態になります。
推奨ポリシー	一般的なエンタープライズ環境を保護する重要な対応として、攻撃のシグネチャをジュニパーのセキュリティ チームが特定します。	インストールとメンテナンスの簡素化と同時に、最高レベルのネットワーク セキュリティが確保されます。
アクティブ/アクティブ構成のトラフィック モニタリング	IPS モニタリングには、アクティブ/アクティブ構成の vSRX シャーシ クラスターが含まれます。	アクティブ/アクティブ構成の IPS モニタリングに対応しています。
パケット キャプチャ	IPS ポリシーにより、ルールごとにパケット キャプチャのログを記録します。	ユーザーは、関連トラフィックをさらに詳しく分析して、対象を保護する手順を決定できます。

表 3：AppSecure for vSRX の特長とメリット

特長	説明	メリット
AppTrack	アプリケーション データを分析し、リスク レベル、ゾーン、送信元、宛先アドレスに基づいて分類します。	アプリケーションの使用状況を追跡し、高リスクなアプリケーションの特定とトラフィック パターンの分析を行うことにより、ネットワークの管理と制御能力を向上させます。
AppFW	アプリケーション コントロール ポリシーを作成し、アプリケーション名やグループ名に基づいてトラフィックを動的に許可または拒否できます。	従来のポートやプロトコルの分析ではなく、アプリケーションに基づいたセキュリティ ポリシーの作成と適用を可能にします。
AppQoS	管理者が設定したアプリケーション セキュリティ ポリシーに基づいて、トラフィックを計測してマークします。	ネットワーク全体のパフォーマンス向上を目的として、アプリケーション情報とコンテキストに基づいてトラフィックの優先度を設定するとともに、帯域幅の制限と確保を行います。

AppSecure によるアプリケーションの可視化と制御

AppSecure は、vSRX および SRX シリーズ サービス ゲートウェイ向けの次世代型アプリケーション セキュリティ パッケージで、脅威の可視化、脅威からの保護、ポリシーの適用、制御を行います。

Facebook のようなクラウドベースのアプリケーションにアクセスしているユーザーの数を毎日把握する必要がある場合でも、最も多くの帯域幅を使用しているアプリケーションを知る必要がある場合でも、AppSecure は高い可視性を提供し、アプリケーションの動きを継続して追跡できます。オープン シグネチャを使って特定のアプリケーション セットを監視し、計測し、コントロールすることで、組織のビジネス上の優先度に基づいてアプリケーションを適切に使用できます。

Juniper Advanced Threat Prevention

Juniper Advanced Threat Protection は、vSRX と連携して、既知のマルウェアや高度なゼロデイの脅威に対して動的かつ自動的な保護を提供し、その結果、ほぼ瞬時に対応します（表 4 を参照）。

セキュリティ ポリシーでは、1 つのゾーンから別のゾーンへのセッションの転送を許可するかどうかを決定します。vSRX はパケットを受信し、すべてのセッション、アプリケーション、ユーザーを継続して追跡します。VM は仮想環境またはクラウド環境内を移動しても、引き続き安全が確保された状態で、vSRX に処理の必要なパケットを送信します。

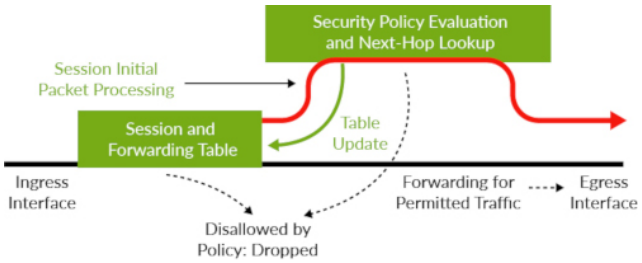

図 1：vSRX のセッションベース転送アルゴリズム

高可用性（HA）

vSRX はアクティブ/アクティブ モードとアクティブ/パッシブ モード両方のシャーシクラスリングに対応し、必要不可欠な信頼性を提供します。HA 機能は、処理中のあらゆる接続およびハイパーバイザーをつなぐクラスター メンバーに対し、完全なステートフル フェイルオーバー機能を提供します。vSRX VM がクラスター内で設定されると、VM は接続/セッションの状態とフロー情報、IPsec セキュリティ アソシエーション、ネットワーク アドレス変換（NAT）トラフィック、アドレス ブック情報、設定変更などの情報を同期します。この結果、フェイルオーバー中もセッションが維持されるだけでなく、セキュリティも損なわれることなく維持されます。また不安定なネットワークでは、vSRX はリンク フラッピングの発生も抑えます。

表 4：Juniper ATP for vSRX の特長とメリット

特長	メリット
綿密な調査と分析	侵害されたファイルを抽出してクラウドに送信し、特に見つけにくいのマルウェアを探すために、脅威を迅速に特定し、ファイルレベルで綿密な分析を行います。
攻撃をブロックするための即座の特定	マルウェアが検出されると、即座に特定して SRX シリーズ ファイアウォールに通達し、攻撃をブロックします。
豊富なレポートと分析ツールを備える Web ベースのポータル	設定、製品の更新といった管理タスク実行用に Web ベースのインターフェイスを提供します。また、さまざまなレポートと分析ツールにより、脅威や侵害されたホストを可視化します。
システムとホストの隔離	分析機能を使うと、管理者やセキュリティ スタッフはデータの分析と相互比較を行い、侵害を受けたシステムを特定したあと、その情報を SRX シリーズ ファイアウォールに供給して、システムを隔離できます。
Spotlight Secure との統合	Spotlight Secure 脅威インテリジェンス サービスと統合されているため、脅威の情報を SRX シリーズ ファイアウォールまで通知して即座の対応を可能にします。
C&C（コマンドおよびコントロール）データ	C&C データを SRX シリーズ ファイアウォールに供給します。侵害された内部システムが他のデバイスと通信することを防止します。
メールの分析と修復	悪意のあるマルウェアを分離して隔離し、攻撃ベクトルとしてメールが使用されるのを防ぎます。機械学習アルゴリズムがメール トラフィックを分析し、悪意のある添付ファイルを検出して、ファイルをファイアウォールでブロックします。
脅威インテリジェンス	高性能のオープン API を使用して、サードパーティー ベンダーとシームレスに統合し、複数の脅威インテリジェンス フィードを提供することで、攻撃対象領域を減らします。

表 5：vSRX サービス ゲートウェイの重要なパフォーマンス メトリック

パフォーマンス/設定数[1]	VMware				KVM			
vCPU	2	5.	9	17	2	5.	9	17
メモリ	4 GB	8GB	16 GB	32/64 GB	4 GB	8GB	16 GB	32/64 GB
ファイアウォール スループット、ラージ パケット（1514B）	9.5 Gbps	14 Gbps	73 Gbps	81 Gbps	14 Gbps	39 Gbps	68 Gbps	98 Gbps
ファイアウォール スループット、IMIX	2.4 Gbps	4.1 Gbps	17 Gbps	27 Gbps	3.2 Gbps	14 Gbps	16 Gbps	27 Gbps
AES + GCM IPSec VPN スループット（1420B）	2.2 Gbps	4.2 Gbps	12 Gbps	13 Gbps	1.1 Gbps	7 Gbps	10 Gbps	16 Gbps
アプリケーションの可視化と制御[2]	2.4 Gbps	7.2 Gbps	21 Gbps	39 Gbps	3.3 Gbps	10 Gbps	19 Gbps	38 Gbps
IPS 推奨シグネチャ	2.3 Gbps	7.1 Gbps	18 Gbps	39 Gbps	3 Gbps	10 Gbps	19 Gbps	36 Gbps
TCP 接続数/秒	55,000	166,250	351,250	537,660	69,000	239,380	360,000	612,660
最大同時セッション数[3]	512,000	2M	4M	12/24M	512,000	1M	1.5M	12/24M

[1] すべてのパフォーマンス数値は「最大数値」であり、基盤のハードウェア構成によって変動します（一部のサーバー構成ではより高いパフォーマンスを示す場合もあります）。このリストに示しているパフォーマンス、設定数、および特長は、Junos OS 19.2R1 を実行する vSRX に基づいており、最適なテスト条件で測定したものです。実際の結果は、Junos OS リリースの種類や環境によって異なる可能性があります。

[2] トランザクション サイズ 44 KB の HTTP トラフィックに基づいたスループット数です。

[3] 最大同時セッション数は、vSRX のメモリ割り当てに応じて増加する場合があります。詳細については、https://www.juniper.net/documentation/en_US/vsrx/information-products/topic-collections/release-notes/19.2/topic-98044.html#jd0e107 をご覧ください。

パフォーマンス

ユーザーはこれまで拡張性とパフォーマンスのどちらかを選択する必要がありました。vSRX ソリューションは複数の仮想 CPU を活用するように最適化され、仮想環境におけるパケット処理と全体のスループットを最大化しています。各 vSRX VM にもさまざまな仮想ネットワークに接続可能な複数の仮想ネットワーク インタフェイス カード（vNIC）が搭載され、複数のネットワーク セグメントを同時に保護しています。仮想構造で運用される vSRX は、仮想環境やクラウドベース環境で必要とされる強固なセキュリティとパフォーマンスの両方を実現します。

スケールアップ モデルを利用可能な vSRX では、新しいインスタンスイメージを認証しなくても、同じインスタンスにコア*を追加するだけで、最小 2 つの vCPU の他に、仮想セキュリティ容量を柔軟にアップグレードできます。vSRX では 1 個のソケットで 17 個の vCPU を使用でき、最大 100 Gbps のパフォーマンスを実現します。

* コア数は 2 のべき乗 + 1（2n + 1）でなければなりません。

表 6：vSRX システム要件

コンポーネント	仕様			
CPU コア数	2	5.	9	17
メモリ	4 GB	8GB	16 GB	32 GB
ディスク容量	16 GB			
ネットワーク ドライバー - VMware ESXi	VMXNET3、SR-IOV on Intel X710/XL710 または X520/X540	VMXNET3	SR-IOV（Mellanox ConnectX-3/ConnectX-3 Pro および Mellanox ConnectX-4 EN/ConnectX-4 Lx EN）	
ネットワーク ドライバー KVM	Virtio、SR-IOV on Intel X710/XL710 または X520/X540	Virtio、SR-IOV on Intel X710/XL710	Virtio、SR-IOV on Intel X710/XL710（PCI-Passthrough 搭載） SR-IOV（Mellanox ConnectX-3/ConnectX-3 Pro および Mellanox ConnectX-4 EN/ConnectX-4 Lx EN）	

Junos Space Security Director

Junos Space Security Director は、直感的な一元管理の Web ベース インタフェイスを介したセキュリティ ポリシー管理機能を提供し、最近および従来のリスク要素に対してポリシーを適用します。Security Director は、Junos Space プラットフォームのアプリケーションとして、ネットワーク全体で広範なセキュリティ基準、きめ細かなポリシー制御、多様なポリシーを提供します。管理者はステートフル ファイアウォール、UTM、IPS、AppFW、VPN、NAT のセキュリティ ポリシー ライフ サイクルにおけるあらゆる段階を迅速に管理できます。

統合管理

管理者は、Junos Space Security Director の機能を活用することによって、一元的な汎用プラットフォームから物理的資産と仮想資産の両方について、ポリシーの設定、管理、可視化の能力を大幅に向上させることができます。

主な特長とメリット

- ステートフルなパケット処理とアプリケーションレイヤーのゲートウェイ機能をもつファイアウォールを仮想マシン形式で提供することで、マルチテナントのプライベート クラウドおよび公開クラウド環境のセキュリティを強化します。
- SRX シリーズ サービス ゲートウェイの同一で一貫した高度なセキュリティおよびネットワーク機能（IPsec VPN、NAT、QoS、フル ルーティング機能）を活用します。
- 強力な UTM、IPS、アプリケーションの可視化とコントロール機能を統合し、総合的な脅威管理フレームワークを実現することにより、ますます巧妙化する脅威に対抗します。
- オープン RESTful API でサードパーティー管理ツールやクラウド オーケストレーション ツールとの統合を可能にし、管理上の柔軟性を高めることができます。

- Junos Space Security Director を活用して、仮想環境と物理環境全体におけるファイアウォール セキュリティ ポリシーの設定と管理状況に対する可視性とコントロールを強化します。
- Contrail や OpenContrail などのサードパーティー ソリューションとの統合により、SDN と NFV に対応します。

Amazon Web Services Marketplace で使用可能

vSRX は、AWS (Amazon Web Services) Marketplace で使用でき、高度なネットワークおよびアプリケーション セキュリティと、AWS VPC、プライベート クラウド、およびオンプレミス リソースへのセキュアな IPsec VPN 接続を提供します。vSRX 3.0 では、AWS の自動拡張機能を活用して、容量を動的に増やすと同時に、安定したパフォーマンスを最小限のコストで維持できます。Junos Space Security Director を使用すると、オンプレミスおよび AWS VPC のすべてにわたり SRX シリーズ サービス ゲートウェイで一貫したセキュリティ ポリシーを維持して管理できます。AWS で vSRX を使用しているお客様は、独自の vSRX ライセンスを購入することも、使用量に応じた価格 (時間単位または年単位) を利用することもできます。

Microsoft Azure Marketplace で使用可能

vSRX は、Microsoft Azure Marketplace だけでなく、Microsoft Azure Government でも使用でき、セキュアな IPsec VPN 接続と高度な次世代のセキュリティを Azure 仮想化ネットワークに提供します。Junos Space Security Director を使用すると、オンプレミスや Azure の仮想化ネットワークに導入されている SRX シリーズ 次世代ファイアウォールに対して、一貫したセキュリティ ポリシーを維持して管理できます。Microsoft Azure Marketplace および Microsoft Azure Government では、vSRX を個人所有ライセンス (BYOL) モードで使用できます。

Google Cloud Platform Marketplace で使用可能

vSRX は、Google Cloud Government だけでなく、Google Cloud Platform Marketplace でも使用でき、セキュアな IPsec VPN 接続と高度な次世代の UTM セキュリティ機能を Google 仮想化ネットワークに提供します。Junos Space Security Director を使用すると、オンプレミスや Google の仮想化ネットワークに導入されている SRX シリーズ 次世代ファイアウォールに対して、一貫したセキュリティ ポリシーを維持して管理できます。ジュニパーは、Google Cloud Platform および Google Cloud Government で、個人所有ライセンス (BYOL) および 従量制 (PAYG) ライセンスのオプションを提供しています。

ジュニパーネットワークスのサービスとサポート

ジュニパーネットワークスは、高性能なサービス分野のリーダー的存在であり、高性能ネットワークの高速化、拡張、最適化を目指しています。当社のサービスをご利用いただくと、コストを削減し、リスクを最小限に抑えながら、業務効率を最大限に高めることが可能となり、ネットワークへの投資から早期に利益を得ることができます。また、ネットワークを最適化することで、必要な性能レベルや信頼性、可用性を維持し、卓越した運用を実現します。詳細については、www.juniper.net/jp/jp/products-services をご覧ください。

仕様

以下の表に、仕様の概要を示します。完全なリストについては、製品マニュアルを参照してください。

表 7：vSRX 仮想ファイアウォールの仕様

プロトコル	IP アドレスの管理	セキュリティ	SLA、測定、監視	ハイパーバイザー
• IPv4、IPv6、MPLS、ISO コネクションレス型ネットワーク サービス（CLNS） • スタティック ルート • RIPv2 +v1 • OSPF/OSPFv3 • BGP • IS-IS • マルチキャスト（インターネット グループ管理プロトコル、PIM、セッション記述プロトコル） • MPLS • VPLS	• 静的 • 動的ホスト構成プロトコル（DHCP） • 内部 DHCP サーバー、DHCP リレー • アドレス変換 • ソース NAT と PAT（ポート アドレス変換） • 静的 NAT • ディスティネーション NAT と PAT • 永続的 NAT、NAT64 • カプセル化 • イーサネット • 1q VLAN サポート	• ファイアウォール • ファイアウォール、ゾーン、スクリーニング、ポリシー • ステートフル ファイアウォール、ステートレス フィルター • ネットワーク攻撃検知 • DoS と DDoS（分散型 DoS）攻撃からの防御態勢をチェック（異常検知） • リプレイ攻撃の防御、アンチリプレイ • 統合型アクセス コントロール（UAC） • フラグメント パケット攻撃防御のための TCP パケット再構築 • 総当たり攻撃緩和 • Syn Cookie 防御 • ゾーンベース IP スプーフィング • 異常パケット攻撃防御 • VPN • トンネル（一般ルーティングのカプセル化、IP-IP） • IPsec、DES（データ暗号化規格）（56 ビット）、3DES（トリプル データ暗号化規格）（168 ビット）、AES（次世代標準暗号）（128 ビット）による暗号化 • Message Digest 5（MD5）、SHA-1、SHA-128、SHA-256 による認証 • IPv6	• RPM（リアルタイム パフォーマンス監視） • セッション、パケット、帯域幅の使用量 • IP 監視 • ログ作成 • システム ロギング • Traceroute • コントロール プレーンとデータ プレーンの広範な構造化/非構造化システム ログの管理 • Junos Space Security Director に対応 • Juniper Networks Secure Analytics • Juniper Networks Advanced Insight Solution に対応 • 管理者用外部データベース（RADIUS、LDAP、SecureID） • 自動構成 • 設定ロールバック • ボタンによるレスキュー設定 • 変更コミット確認 • 診断自動記録 • ソフトウェア アップグレード • J-Web • CLI	• VMware ESXi 5.5、6.0、6.5、KVM/QEMU： - CentOS 7.1 - Ubuntu 14.04、16.04、16.10 - RHEL 7.3 • Hyper-V 2012、2012R2、2016

注文情報

ジュニパーネットワークス vSRX 仮想ファイアウォールの詳細は、www.juniper.net/jp/jp/products-services/security/srx-series/vsrx をご覧いただくか、お近くのジュニパーネットワークスの営業担当者にお問い合わせください。vSRX 無料トライアルについては、www.juniper.net/jp/jp/dm/free-vsrx-trial/をご覧ください。

ジュニパーネットワークスについて

ジュニパーネットワークスは、世界をつなぐ製品、ソリューション、サービスを通じて、ネットワークを簡素化します。エンジニアリングのイノベーションにより、クラウド時代のネットワークの制約や複雑さを解消し、お客様およびパートナーの皆様が日々直面している困難な課題を解決します。ジュニパーネットワークスは、世界に変革をもたらす知識の共有や人類の進歩のリソースとなるのはネットワークであると考えています。私たちは、ビジネス ニーズにあわせた、拡張性の高い、自動化されたセキュアなネットワークを提供するための革新的な方法の創造に取り組んでいます。

Corporate and Sales Headquarters
Juniper Networks, Inc. 1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号：888.JUNIPER (888.586.4737)
または +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V. Boeing
Avenue 240 1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.0.207.125.700