VSRX 仮想ファイアウォールデータシート

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 を使用展することで、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、コンテンツセキュリティのような高度のセキュリティサービスが含まれる vSRX のトライアル版のダウンロードをご希望の場合は、www.juniper.net/jp/ja/products/security/srx-series/vsrx-virtual-firewall-datasheet.html をご覧ください。

製品説明

データ センターは、サービスをこれまでになく迅速かつ効率的に提供するために、サーバーの仮想化にますます依存しています。しかし、仮想化されたデータセンターは、物理的資産に求められる以上のセキュリティ上配慮を必要とする新たな課題ももたらします。

VM（仮想マシン）は、仮想化されたデータセンターにおいて、頻繁に行われる追加、移動、変更によって、非常に動的で融通性の高いものになり得ます。この頻繁な変更が、法令遵守の継続に必要な、VM のインスタンス化へのセキュリティポリシーの取り付けや、VM の移動に伴うセキュリティポリシーの追跡の能力を妨げています。つまり、動的で柔軟である仮想化の特性が、可視性や制御を容易に失ってしまう原因となるのです。

ネットワークやセキュリティ専門家は、組織のセキュリティを損なうことなく、仮想化やクラウド技術の利益をもたらし、微妙なバランスを取る必要があります。この課題に応えられるのは、進化する脅威に対応しながら、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適合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、受賞歴を誇る Juniper Networks® SRX シリーズファイアウォールの機能に vSRX 仮想ファイアウォールを加えて仮想世界に拡張することで、この課題に正面から対応しています。ジュニパーは、あらゆるレベルでクラウドを保護することで、セキュリティを容易にします。それは、アプリケーション間、インスタンス間、そして環境全体に及びます。

ジュニパーネットワークスの Junos® オペレーティングシステムを搭載した vSRX は、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、自動ライフサイクル管理機能を含む、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 NFV（ネットワーク機能仮想化）のユースケース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企業に適しています。また、vSRX は Juniper Networks Contrail、OpenContrail および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、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も直接または豊富な API を介して統合することができます。

表 1. vSRX コンテンツセキュリティの特徴とメリット

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、評価の高いクラウドベースのアンチウィルス機能 • サーバ上またはクラウド上	• 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	• 幅広いカテゴリーオプション（90 以上のカテゴリー）やリアルタイムのスコアカードをはじめとする拡張 Web フィルタリング	• 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の確保を支援します。
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	• 多層のスパム防御、最新のフィッシング URL 検知、スタンダードベースの S/MIME、Open PGP と TLS 暗号化、MIME タイプ、および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頻繁に変化する脅威の状況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、コンテンツセキュリティ、IDP/IPS（不正侵入検知･防御）、および Juniper Networks AppSecure によるアプリケーションの制御と可視化サービスを含む用途の広い高度で優れたセキュリティサービスを提供します。

コンテンツセキュリティ

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の解析と、500 を超えるコンテキストに対応し、プロトコルの適切な使用を確実にします。	プロトコルの正確なコンテキストにより、シグネチャの精度を向上させます
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が提供されます。	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、新たに発見された脆弱性への同日対応が提供されます。	脆弱性への新たな攻撃に対しネットワークを守ります。
推奨ポリシー	ジュニパーセキュリティチームが、一般的なエンタープライズのために、攻撃シグネチャを特定します。	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 のモニタリングに対応します。
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、ターゲットを保護するさらな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、発信元、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、動的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許可または拒否します。	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キングします。	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し、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 シリーズファイアウォール向けの次世代型アプリケーションセキュリティスイートで、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 Prevention は、vSRX と連携して、既知のマルウェアや高度なゼロデイ脅威に対し動的な保護を自動的に提供することで、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。

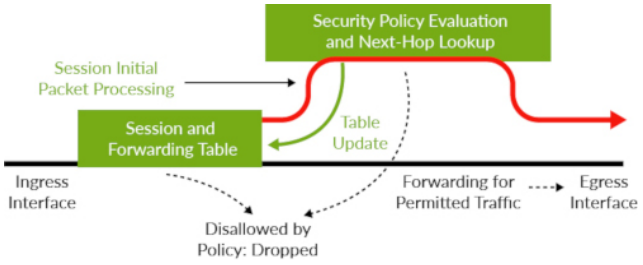

図 1：vSRX のセッションベース転送アルゴリズム

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/パッシブモードのシャーシクラスタリングに対応し、ミッションクリティカルな信頼性を提供します。HA 機能は、プロセス中のあらゆる接続と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を提供します。vSRX VM は、クラスターに設定されると、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をします。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。

Juniper Secure Connect

Juniper Secure Connect は、柔軟性に優れた SSL VPN アプリケーションであり、保護されたリソースから離れた場所で業務に取り組む従業員に、会社やクラウドのリソースへのセキュアなアクセスを提供します。Juniper Secure Connect は、Windows、Mac OS、Android、iOS などの OS を使用しているデスクトップおよびモバイルデバイスで使用できます。Secure Connect を SRX シリーズファイアウォールと組み合わせることで、企業はどこからでも、あらゆるデバイスに対して動的で柔軟かつ適応性の高い接続性を実現でき、可視化とポリシーの適用をユーザーからクラウドにまで拡大してリスクを軽減できます。

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、既知の脅威を迅速に特定するか、特に発見困難なマルウェアを探しだすために綿密なファイル分析をします。
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、豊富なレポートと分析ツールを提供し、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。
SecIntel	SecIntel からの動的脅威インテリジェンスフィードにより、脅威情報を 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。
コマンド＆コントロール（C&C）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。
暗号化トラフィックのインサイト（ETI）	完全な TLS/SSL 暗号化解除の重い負荷を発生させることなく、暗号化によって失われた可視性を復元します。

特長	メリット
適応型脅威プロファイリング	新たな脅威による継続的な攻撃に対処できるように、迅速な対応を可能にします。ATP クラウドの適応型脅威プロファイリングを使用すると、ネットワークに対する現在の攻撃者や攻撃方法の情報に基づいてセキュリティインテリジェンス脅威フィードを自動作成できます。

表 5. vSRX ファイアウォールの主要な性能メトリクス

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)	15.7Gbps	41 Gbps	73 Gbps	81 Gbps	17 Gbps	50 Gbps	79Gbps	141Gbps
ファイアウォール スループット、IMIX	3.2 Gbps	11.1Gbps	17 Gbps	27 Gbps	4.3 Gbps	12.5Gbps	22 Gbps	40Gbps
AES + GCM IPSec VPN スループット (1420B)	2.1 Gbps	3.8 Gbps	12 Gbps	13 Gbps	2.9Gbps	6.3Gbps	10.8 Gbps	14.9Gbps
アプリケーションの可視化と制御 [2]	3.7Gbps	10.8 Gbps	21 Gbps	39 Gbps	2.4 Gbps	10.8 Gbps	20.7Gbps	35.8Gbps
IPS 推奨シグネチャ	3.6 Gbps	11 Gbps	18 Gbps	39 Gbps	2.2 Gbps	12.6Gbps	20.8 Gbps	36.2Gbps
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	12/28M	512,000	2M	4M	12/28M
リモートアクセス/SSL VPN (同時) ユーザー数	500	500	500	500	500	500	500	500

[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になる場合もあります)。リストに示されたパフォーマンス、設定数、および特徴は、Junos OS 20.4R1 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#jd0e119 をご覧ください。

パフォーマンス

お客様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 インターフェイス 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。vSRX は仮想ファブリック内から運用され、仮想環境やクラウドベース環境への対応に必要な強固なセキュリティと、パフォーマンスの両方を提供します。

vSRX は、ソフトウェア受信側スケーリングの実装を活用して、新しいインスタンスイメージの認証なしで、同じインスタンスに、最小 2 つの vCPU を超える最大 32 の vCPU の追加のコア*を提供します。　1 つのソケットで 17 個の vCPU を使用して最大 98 Gbps のパフォーマンスを達成することが可能です。

*コア数は、2+1 (すなわち、2n+1) のべき乗である必要があります。

表 6：vSRX のシステム要件

仮想 CPU コア数	メモリ (GB)	サポートされている NIC タイプ
2	4、8、16、20、32	VMXNET3、VIRTIO、82599 SR-IOV、I40E SR-IOV
5	8、16、20、32	VMXNET3、VIRTIO、82599 SR-IOV、I40E SR-IOV
9	16、32、50、64	I40E SR-IOV
17	32、50、64	I40E SR-IOV
32	64	I40E SR-IOV

Junos Space Security Director

Junos Space Security Director は、直感的な一元管理の Web ベース インター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、コンテンツセキュリティ、IPS、AppFW、VPN、NAT のセキュリティポリシーライフサイクルのあらゆるフェーズ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 クラウドおよびパブリッククラウド環境のセキュリティを強化します。
- SRX シリーズファイアウォールと同じ、一貫した高度なセキュリティとネットワーク機能 (IPsec VPN、NAT、QoS、フルルーティング機能) を活用します。

- 強力なコンテンツセキュリティ、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、包括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制御を強化します。
- Contrail や Tungsten Fabric 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。

Nutanix で使用可能

vSRX を Nutanix エンタープライズクラウドに展開すると、Nutanix AVH のオンプレミスリソース間に高度なネットワーク/アプリケーションセキュリティとセキュアな IPsec VPN 接続が提供されます。Junos Space Security Director を使用することで、お客様はキャンパス、データセンター、クラウドのすべてにわたり、SRX シリーズファイアウォールで一貫したセキュリティポリシーを維持および管理できます。vSRX は Nutanix 対応と認定されています。詳細は https://www.nutanix.com/partners/technology-alliances/juniper-networks をご覧ください。

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 を使用することで、お客様はオンプレミスおよび AWS VPC のすべてにわたり、SRX シリーズファイアウォール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、ご自身の vSRX ライセンスを持ち込むことも、使用量に応じた価格 (pay-as-you-go (利用時払い)、時間単位または年単位) で支払えます。

Microsoft Azure Marketplace で使用可能

vSRX は、Microsoft Azure Marketplace と Microsoft Azure Government で使用でき、安全な IPsec VPN 接続と高度な次世代セキュリティを Azure 仮想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 を利用者所有ライセンス (Bring-Your-Own-License) モードで使用できます。

Google Cloud Platform Marketplace で使用可能

vSRX は、Google Cloud Platform Marketplace と Google Cloud Government で使用でき、安全な IPsec VPN 接続と高度な次世代とコンテンツセキュリティ機能を Google 仮想ネットワークに提供します。ジュニパーは、Google Cloud Platform および Google Cloud Government で、利用者所有ライセンス (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、高性能サービス市場をリードし、サービス導入の高速化、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、早期にネットワーク投資の価値を高めることができます。ジュニパーネットワークスは、必要なレベルのパフォーマンス、信頼性、および可用性を維持するようにネットワークを最適化することで、オペレーショナルエクセレンスを確保します。詳細については、https://www.juniper.net/jp/ja/products.html 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 Connectionless Netwrok service（CLNS）	• 静的	• ファイアウォール	• RPM（リアルタイム パフォーマンス監視）	• VMware ESXi 5.5、6.0、6.5、7.0 KVM/QEMU*：
• スタティックルート	• 動的ホスト構成プロトコル（DHCP）	• ファイアウォール、ゾーン、スクリーニング、ポリシー	• セッション、パケット、帯域幅の使用量	- CentOS 7
• RIPv2 +v1	• 内部 DHCP サーバー、DHCP リレー	• 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	• IP 監視	- Ubuntu 16.04、16.10、18.04
• OSPF/OSPFv3	• アドレス変換	• ネットワーク攻撃検知	• ログ作成	- RHEL 7.7
• BGP	• ソース NAT と PAT（ポートアドレス変換）	• 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）	• システム ロギング	- Oracle Linux 7.3
• IS-IS	• 静的 NAT	• リプレイ攻撃の防御、アンチリプレイ	• Traceroute	• Hyper-V 2012、2012R2、2016
• マルチキャスト（Internet Group Management Protocol, PIM, Session Description Protocol）	• ディスティネーション NAT と PAT	• 統合型アクセス コントロール（UAC）	• 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	• Nutanix AHV：
• MPLS	• 永続的 NAT、NAT64	• 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	• Junos Space Security Director に対応	- AOS：5.15 LTS
• VPLS	• カプセル化	• 総当たり攻撃緩和	• Juniper Networks Secure Analytics	
	• イーサネット	• Syn Cookie 防御	• Juniper Networks Advanced Insight Solution に対応	
	• 802.1Q VLAN サポート	• ゾーンベース IP スプーフィング	• 管理者用外部データベース（RADIUS、LDAP、SecureID）	
		• 異常パケット攻撃防御	• 自動構成	
		• VPN	• 設定のロールバック	
		• トンネル：サイトツーサイト、ハブアンドスポーク、動的エンドポイント、AutoVPN、ADVPN、グループ VPN（IPv4/IPv6/デュアルスタック）	• ボタンによるレスキュー設定	
		• インターネット鍵交換（IKE）：IKEv1/IKEv2	• 変更のための commit confirm	
		• ペイロード設定	• 診断自動記録	
		• IKE 認証アルゴリズム：MD5、SHA1、SHA-256、SHA-384	• ソフトウェア アップグレード	
		• IKE 暗号化アルゴリズム：プライム、DES-CBC、3DES-CBC、AEC-CBC、AES-GCM、SuiteB	• J-Web	
		• 認証：事前共有カギおよび公開カギインフラストラクチャ（PKI X.509）	• CLI	
		• IPsec（インターネットプロトコルセキュリティ）：認証ヘッダー（AH）/カプセル化セキュリティペイロード（ESP）プロトコル		
		• 完全転送機密保持		
		• IPsec 認証アルゴリズム：hmac-md5、hmac-sha-196、hmac-sha-256		
		• IPsec 暗号化アルゴリズム：プライム、DES-CBC、3DES-CBC、AEC-CBC、AES-GCM、SuiteB		
		• 監視：スタンダードベースのデッドピア検出（DPD）、VPN 監視		
		• VPNs（GRE, IP-in-IP, MPLS）		
		• Microsoft Azure 専用ハードウェアセキュリティモジュール（HSM）		
		• IPv6		

*ハイパーバイザーサポートは定期的に更新されます。サポートされているハイパーバイザーバージョン一覧は、KVM ページの vSRX をご覧ください。

ICSA ラボのファイアウォール認証

ジュニパーネットワークスの vSRX 仮想ファイアウォールは、ICSA ラボのファイアウォール安全検査の、Baseline と Corporate 双方の基準ドキュメント上の要件をすべて満たし、ICSA ラボのファイアウォール認定を受けています。レポートのコピーをダウンロードは https://www.icsalabs.com/product/vsrx-virtual-firewall から行えます。

注文情報

ジュニパーネットワークスの vSRX 仮想ファイアウォールの詳細については、 www.juniper.net/jp/ja/products/security/srx-series/vsrx-virtual-firewall.htm 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、https://www.juniper.net/ja/jp/dm/download-next-gen-vsrx-firewall-trial.html 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、ネットワーク運用を劇的に簡素化し、エンドユーザーに最上のエクスペリエンスを提供することに注力しています。業界をリードするインサイト、自動化、セキュリティ、AI を提供する当社のソリューションは、ビジネスで真の成果をもたらします。つながりを強めることにより、人々の絆がより深まり、幸福、持続可能性、平等という世界最大の課題を解決できるとジュニパーは確信しています。

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
日本, 東京本社
ジュニパーネットワークス株式会社
〒 163-1445 東京都新宿区西新宿 3-20-2
東京オペラシティタワー 45 階
電話番号： 03-5333-7400
FAX：03-5333-7401
www.juniper.net/jp/ja/