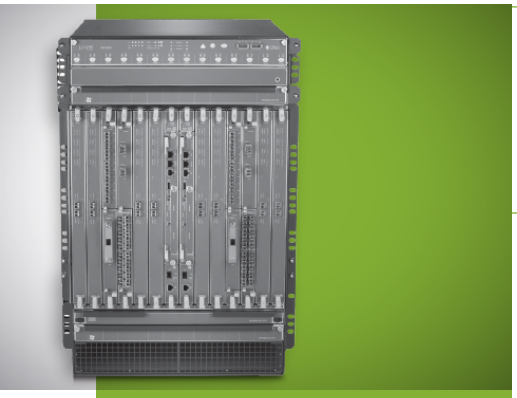

SRX5400、SRX5600、SRX5800 ファイアウォールデータシート

製品概要

SRX シリーズ次世代ファイアウォールは、大規模エンタープライズデータセンター、サービスプロバイダのインフラストラクチャ、および公共部門ネットワーク向けに構築されています。SRX シリーズファイアウォールは、モジュラー式のアーキテクチャと高性能なラインカードを備えた、オープンで拡張可能なセキュリティプラットフォームであり、柔軟な接続オプションとサービス統合を提供します。受賞歴のある SRX シリーズは、業界をリードする Junos OS を搭載しており、世界最大規模のデータセンターネットワークを利用可能、管理可能、かつセキュアな状態に保ちます。

製品説明

Juniper Networks® SRX5400、SRX5600、SRX5800 は次世代ファイアウォール（NGFW）であり、業界をリードする脅威からの保護、高性能、99.9999%の信頼性と可用性、拡張性、およびサービス統合を提供します。これらのデバイスは、次のような大規模なエンタープライズ、サービスプロバイダ、および公共部門ネットワークに最適です。

- 大企業のデータ センター
- クラウドおよびホスティング プロバイダのデータ センター
- モバイル通信事業者の環境
- マネージド サービス プロバイダ
- コア サービス プロバイダのインフラストラクチャ

SRX5400、SRX5600、SRX5800 ファイアウォールは、Juniper® Connected Security フレームワークに不可欠な要素であり、ネットワーク上のあらゆる接続ポイントにセキュリティを拡張して、アプリケーション、ユーザー、およびインフラストラクチャを高度な脅威から保護します。これらのプラットフォームは、悪用、マルウェア、コマンドアンドコントロール（C&C）通信に対する最高レベルの保護を提供しており、キャリアグレードの次世代ファイアウォールと、アプリケーションセキュリティ、侵入防御システム（IPS）、および統合脅威インテリジェンスサービスなどの高度なセキュリティサービスを特徴としています。

SRX5400、SRX5600、SRX5800 は、Juniper Security Director Cloud によって管理されており、現在の導入を将来のアーキテクチャ展開に結び付ける統一管理エクスペリエンスが得られます。Security Director Cloud は、単一のポリシーフレームワークを使用して、あらゆる環境全体にわたって一貫したセキュリティポリシーを実現し、エッジからデータセンターにいたるまでのネットワークのすべての部分にゼロトラストを拡大します。これにより、途切れることのない可視性、ポリシー構成、管理、および収集された脅威インテリジェンスがすべて実現できます。

SRX5000 シリーズでは、比類のない拡張性とパフォーマンスを提供します。各ファイアウォールは、サービス処理カード（SPC）および I/O カード（IOC）を追加することで拡張することができ、フル装備の SRX5800 では、最大 3.36Tbps のファイアウォールスループットをサポートすることができます。SPC は、さまざまなサービスをサポートするように設計されており、サービス固有のハードウェアを必要とせずに、将来の新しい機能をサポートできます。すべてのサービスで SPC を使用することで、アイドル状態のリソースが存在しなくなり、使用されている特定のサービスに基づいてハードウェアの利用率を最大限に高めることができます。

SRX5000 シリーズの拡張性と柔軟性は、同等の堅牢性を備えたインターフェイスにより支えられています。SRX5000 シリーズでは、モジュラー方式を採用しており、各プラットフォームに対して柔軟に任意の数の IOC を装備することができ、1GbE、10GbE、40GbE、100GbE インターフェイスを含めた複数の接続オプションが得られます。IOC は SPC と同じインターフェイススロットを共有するため、必要に応じてファイアウォールを設定し、処理と I/O の理想的なバランスをとることができます。したがって、SRX5000 シリーズの各導入を、特定のネットワーク要件に合わせて調整することができます。

SRX5000 シリーズでは、SPC と IOC の拡張性をカスタム設計のスイッチ ファブリックによって高めることができます。このファブリックのデータ転送は最大 960 Gbps まで対応しており、どのような構成でも処理能力と I/O 能力を最大限に引き出すことができます。SRX5000 シリーズは、このような最高クラスの拡張性と柔軟性によって、ネットワーク インフラストラクチャの将来的な拡張や発展を容易にし、比類なき投資保護を実現します。

SRX 5000 シリーズでの緊密なサービス統合を実現しているのが Junos®オペレーティングシステムです。SRX シリーズは、ステートフルファイアウォールや侵入防御システム (IPS)、サービス拒否 (DoS)、アプリケーションセキュリティ、VPN (IPsec)、ネットワークアドレス変換 (NAT)、コンテントセキュリティ、サービス品質 (QoS)、大規模なマルチテナント機能などの堅牢なサービス一式を提供します。各サービスのメリットに加え、SRX5000 シリーズは超低レイテンシソリューションを提供します。

Junos OS はまた、キャリアクラスの信頼性 (99.9999% のシステム可用性) も提供したことで、業界で初めて Telcordia による独立検証を達成しました。従来から、ジュニパーネットワークスのキャリアクラスのルーターとスイッチには単一ソース OS と単一統合型アーキテクチャが採用されており、SRX シリーズではそのメリットが十分に活かされています。

SRX5800

SRX5800 ファイアウォールは市場をリードするセキュリティソリューションであり、最大 3.36Tbps のファイアウォールスループットと、ステートフルファイアウォールで 32 マイクロ秒の遅延をサポートします。また、SRX5800 は 638Gbps IPS と 3 億 3800 万の同時セッションもサポートします。高度なセキュリティ サービスをすべて備えた SRX5800 は、大企業のホスト環境またはコロケーションのデータ センター、サービス プロバイダ コアおよびクラウド プロバイダのインフラストラクチャ、モバイル通信事業者の環境などのセキュリティ対策に最適です。SRX5800 は、最高のパフォーマンス、拡張性、柔軟性を備え、緊密に統合された処理環境に最適で、その高密度なサービスは、クラウド サービス プロバイダやマネージド サービス プロバイダにとって理想的なソリューションです。

SRX5600

SRX5600 ファイアウォールは SRX5800 と同じ SPC と IOC を使用し、最大 1.44Tbps のファイアウォールスループット、1 億 8200 万の同時セッション、245Gbps の IPS をサポートします。SRX5600 は、エンタープライズ データ センターのセキュリティ対策に加え、さまざまなセキュリティ ソリューションのアグリゲーションにも最適です。ゾーン単位で固有のセキュリティポリシーをサポートする機能やネットワークインフラストラクチャの拡大に柔軟に対応できる拡張性を備えた SRX5600 の導入は、大企業やサービスプロバイダー、モバイル通信事業者の環境においてサービスを統合するのに最適です。

SRX5400

SRX5400 ファイアウォールは、SRX5800 と同じ SPC および IOC を使用しており、最大 960Gbps のファイアウォールスループット、9,000 万回の同時セッション、および 172Gbps の IPS をサポートすることができます。SRX5400 は小型フットプリントの高性能ファイアウォールであり、大企業のキャンパスネットワークやデータセンターにおけるエッジまたはコアセキュリティ向けのセキュリティ対策に最適です。SRX5401 は、ゾーン単位で固有のセキュリティ ポリシーをサポートする機能を備え、優れた価格/パフォーマンス/設置面積率を実現しているため、大企業やサービス プロバイダ、モバイル通信事業者の環境でのエッジ サービスやデータ センター サービスに最適なソリューションです。

サービス処理カード

SPC は、SRX5000 シリーズを背後でコントロールする「ブレイン」として、プラットフォームで提供されるサービス全般を処理するよう設計されています。特定のサービスや機能を提供する専用ハードウェアを必要としないので、「一部のハードウェアに負荷が集中して、他のハードウェアがアイドル状態になる」という状況は起こりません。SPC は共にプール化できるよう設計されており、SRX5000 シリーズでは、SPC を増設することでパフォーマンスと処理能力を向上させ、管理に伴う費用や複雑さを大幅に軽減することができます。ハイパフォーマンス SPC3 カードは、SRX5400、SRX5600、SRX5800 ファイアウォールでサポートされています。

I/O カード

SRX5000 シリーズでは、SPC と IOC で同一のモジュラー式アーキテクチャを採用することによって、ソリューションの柔軟性を最大限に高めています。SRX5000 シリーズには 1 枚または複数枚の IOC を実装できるので、さまざまなインターフェイスを最適な組み合わせでサポートできます。また、空きスロットに IOC または SPC のどちらでも実装できる柔軟性を備えているので、SRX5000 シリーズは投資を保護しながら、最も要求の厳しい環

境のニーズに合わせて、インターフェイスと処理機能を最適な組み合わせで実装できます。

第 4 世代の IOC は、利用可能なすべてのラインカードの中でも最も高いスループットである最大 480Gbps を実現し、接続も 1G、10GbE、40GbE から 100GbE までの複数のオプションが用意されています。

ルーティングエンジン（RE3）と拡張システムコントロールボード（SCB4）

SRX5K-RE3-128G RE3 は、2000MHz で動作するマルチコアプロセッサを備えた SRX5000 シリーズ向けの RE 製品ファミリーの最新製品です。128 GB DRAM でパフォーマンス、スケーラビリティ、信頼性を向上させます。また、これには TPM モジュールが含まれています。SRX5K-SCB4 は、SCB あたり 480 Gbps のスループットを実現し、シャーシ内およびシャーシ間冗長性を構成できます。

特長とメリット

ネットワークとセキュリティ

SRX5000 シリーズファイアウォールは、堅牢なネットワーキングサービスで、業界をリードする脅威保護を提供するために設計されています。

特長	説明	メリット
専用プラットフォーム	ネットワークサービスおよびセキュリティサービス向けに設計された専用ハードウェア上に、新規構築されました。	他社製品を大きく上回るパフォーマンスと柔軟性を実現し、高速ネットワーク環境を保護します。
拡張可能なパフォーマンス	ジュニパーのダイナミックサービスアーキテクチャに基づいた拡張可能な処理能力。	新しいサービスと適切な処理能力を利用した、シンプルで経済性に優れたソリューションを提供します。
システムとネットワーク回復力	キャリアクラスのハードウェア設計と実績のある OS。	サービスを中断させることなく、重要な高速ネットワークの導入に求められる信頼性を提供します。マルチプロセッシングコア、およびデータプレーンとコントロールプレーンの分離に基づく独自のアーキテクチャ設計を採用しています。
高可用性（HA）	専用の高可用性インターフェイスを使用したアクティブ/パッシブ HA およびアクティブ/アクティブ HA 構成。	重要なネットワークに求められる可用性と耐障害性を実現します。
柔軟なインターフェイス	ダイナミックサービスアーキテクチャに基づくモジュラーカードを使用した、柔軟な I/O オプション。	要求の厳しいネットワーク環境で必要とされるポート密度の要件を満たす柔軟な I/O 構成と他に依存しない I/O 拡張性（1GbE、10GbE、40GbE、100GbE オプションを含む）を提供します。
ネットワークのセグメント化	管理者は、セキュリティゾーン、バーチャル LAN（VLAN）、バーチャルルーターにセキュリティポリシーを導入してサブネットワークを分離することで、重複する IP アドレス範囲を使用できます。	さまざまな内部、外部、および非武装地帯（DMZ）のサブグループごとに、セキュリティおよびネットワーキングに関する独自のポリシーを設定可能です。
堅牢なルーティングエンジン	専用のルーティングエンジンにより、データプレーンとコントロールプレーンを物理的/論理的に分離します。	ルーティングとセキュリティが統合されたデバイスの導入と、ルーティングインフラストラクチャのセキュリティの確保が、すべて専用の管理環境から可能です。
脅威からの高度な保護機能	IPS、アンチウィルス、アンチスパム、拡張 Web フィルタリング、Juniper Advanced Threat Prevention Cloud、暗号化されたトラフィックのインサイト、脅威インテリジェンスフィード、Juniper ATP Appliance。	• リアルタイムで IPS シグネチャを更新し、悪用や脅威から保護 • 業界最先端のアンチウィルスおよび URL フィルタリングを実装 • サードパーティー提供のフィードと統合した、オープンな脅威インテリジェンス プラットフォームを提供 • ゼロデイ攻撃から保護 • 不正なデバイスや侵害を受けたデバイスがマルウェアを拡散するのを阻止 • 完全な TLS/SSL 復号化の高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
AppTrack	バイト、パケット、およびセッション単位でネットワーク内のアプリケーションの容量/使用状況を詳細に分析します。	ネットワーク管理と制御の改善を目的として、アプリケーションの使用状況を追跡する機能を提供し、高リスクなアプリケーションの特定や、トラフィックパターンの分析を支援します。
AppQoS	ジュニパーの豊富な QoS 機能が、お客様のビジネスと帯域幅のニーズに基づいて、アプリケーションに優先順位を付けます。	アプリケーションとネットワーク全体のパフォーマンス向上を目的として、アプリケーションの情報や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を制限および確保する機能を提供します。
アプリケーション シグネチャ	3,000 を超すアプリケーション シグネチャで、アプリケーションとネストされたアプリケーションを特定するためのオープン・ シグネチャーライブラリーを利用できます。	アプリケーションを正確に特定して、結果の情報を可視化、ポリシー適用、制御、保護に利用できます。
SSL プロキシー（フォワードおよびリバース）	クライアントとサーバー間で SSL 暗号化と復号化を実施します。	アプリケーション識別との組み合わせにより、SSL 暗号化トラフィックに埋め込まれた脅威に対する可視化と防御を実現します。
ステートフル GPRS および SCTP インスペクション	携帯電話会社での General Packet Radio Service Tunneling Protocol（GTP）とストリーム制御伝送プロトコル（SCTP）ファイアウォールをサポートします。	SRX5000 シリーズでステートフルファイアウォール機能を使用することで、モバイル通信事業者のネットワークに接続されている重要な GPRS ノードを確実に保護できます。

特長	説明	メリット
IOC3	第 3 世代の I/O カードは、非常に高いレベルのファイアウォールスループットと低レイテンシを実現します。カードには 2 つのボードの選択肢があります。6 個の 40GbE インターフェイスと 24 個の 10GbE インターフェイス、または 2 個の 100GbE インターフェイスと 4 個の 10GbE インターフェイス。IOC3 は既存の SPC2/SPC3 と首尾よくペアリングさせることができ、あらゆる SRX5000 シリーズのファイアウォールでファイアウォールのパフォーマンスを最大限に高めます。	非常に優れた最高レベルの接続効率と記録破りの高スループット I/O インターフェイスを提供します。ファイアウォールに対するリンク アグリゲーションの必要性が低下し、Express Path を有効にして最大 2 Tbps の非常に高いファイアウォール スループットを実現します。
IOC4	第 4 世代の I/O カードは 2 つの種類が提供されています。まず、10 Gbe のインターフェイスを提供します。2 つ目は、選択した光ファイバーに応じて、48x10GbE、12x40GbE、または 100 Gbe のインターフェイスを提供します。	スロットあたりの最速スループットを実現し、Express Path と組み合わせて I/O カードあたり最大 480 Gbps のスループットを実現できます。
SPC3 カード	SPC2 サービス カードとの後方互換性を確保したパフォーマンスと拡張性を実現します。これらのカードはインサービス ソフトウェア アップグレードとインサービス ハードウェア アップグレードをサポートしています。	セキュリティを常に確保する回復力により、高まり続けるネットワークパフォーマンスのニーズに応えます。
AutoVPN	新規に追加したスポークを含め、すべてのスポークに対してサイト間 VPN のハブ構成を 1 回で行います。構成オプションには以下が含まれます。ルーティング、インターフェイス、Internet Key Exchange (IKE) 、IPsec。	IT 管理にかかる時間とコストを削減し、IPsec VPN ネットワークを簡単かつ自動的に導入できるようにします。
リモートアクセス/SSL VPN	Juniper Secure Connect により、セキュアで柔軟なリモートアクセス SSL VPN を提供します。	会社のリソースにどこからでも安全にアクセスできます。
マルチテナント機能	論理、大規模なセグメント化、セキュリティ機能の分離を提供します。	専用のセキュリティポリシー、ゾーン、その他の機能を使用して、独立した論理インスタンスを導入できます。複数の物理または仮想ファイアウォールを展開する必要がなくなります。

IPS 機能

ジュニパーネットワークスの IPS 機能は、最高レベルのネットワークセキュリティを確保するために、いくつかの独自機能を提供します。

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	この機能は、最も正確な検知方式を実現するとともに、誤検知を減らす効果があります。	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 8500 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 ノーマライゼーション	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既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、攻撃グループのシグネチャをジュニパーネットワークスのセキュリティ 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	アクティブ/アクティブ構成の SRX5000 シリーズ シャーシ クラスターで IPS モニタリングを実行します。	サービス内のソフトウェアアップグレードなどの高度な機能を含む、アクティブ/アクティブ IPS 監視をサポートします。
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。	周囲のトラフィックをさらに分析し、ターゲットを保護するためのさらなるステップを決定することができます。

コンテンツ セキュリティ機能

SRX5000 シリーズファイアウォールで提供されるコンテンツセキュリティサービスには、業界をリードするアンチウィルス、アンチスパム、コンテンツフィルタリング、およびその他のコンテンツセキュリティセキュリティサービスが含まれます。

特長	説明	メリット
アンチウィルス	アンチウィルスにはレピュテーション対応を強化したクラウドベースのアンチウィルス機能が含まれており、POP3、HTTP、SMTP、IMAP、および FTP プロトコル上でスパイウェアやアドウェア、ウィルス、キーロガー、その他のマルウェアを検知してブロックします。このサービスは、セキュリティ専門会社の Sophos Labs との連携により提供されます。	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。
アンチスパム	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、スタンダードベースの S/MIME、Open PGP および TLS による暗号化、MIME タイプと拡張子に基づくブロッカーなどの機能は、セキュリティ専門会社の Sophos Labs との連携により提供されます。	高度な電子メール フィルタリングやコンテンツ ブロッカーを駆使することにより、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実現します。
拡張 Web フィルタリング	広範なカテゴリーの細分化 (95 種類以上のカテゴリー) や、Web セキュリティ専門プロバイダの Forcepoint が提供するリアルタイムの脅威スコアなどの拡張 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。

特長	説明	メリット
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 コマンドなどに基づく効果的なコンテンツ フィルタリング。	生産性の損失や、ネットワーク上に存在する外部コンテンツや悪意のあるコンテンツ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帯域幅の確保を支援します。

Advanced Threat Prevention

SRX5000 シリーズでは、高度なマルウェア、持続的な脅威、ランサムウェアから防御する Advanced Threat Prevention（ATP）ソリューションを利用できます。2 つのバージョンがご利用可能です。Juniper ATP Cloud（SaaS ベースのサービス）と Juniper ATP Appliance（オンプレミスのソリューション）があります。

特長	説明	メリット
高度なマルウェア検知および修復	マルウェアの分析とサンドボックスは、機械学習と行動分析に基づいています。	「ゼロデイ」の脆弱性を悪用する高度なマルウェアなど、悪意のある攻撃からエンタープライズユーザーを保護します。
包括的な脅威フィード（C2、GeoIP、カスタム）	厳選された実用的な脅威インテリジェンス フィードは、ほぼリアルタイムで SRX シリーズ デバイスに配信されます。	マルウェア通信チャネルを積極的にブロックし、ボットネット、フィッシング、その他の攻撃から保護します。
暗号化されたトラフィックのインサイト	SRX シリーズファイアウォールでは、使用された証明書、ネゴシエートされた暗号スイート、接続の動作など、TLS/SSL 接続についての関連データを収集します。この情報は Juniper ATP クラウドによって処理されます。ATP Cloud がネットワーク行動分析と機械学習を使用して、接続が無害が悪意のあるものなのかを判断します。SRX シリーズファイアウォールに設定したポリシーを使用して、悪意ありと判定されたトラフィックをブロックできます。	完全な TLS/SSL 復号化の高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。
HTTP、HTTPs、メール	Web ベースと電子メールベースの脅威（暗号化されたセッションなど）が分析されます。	電子メールなどのあらゆる主要脅威ベクトルからユーザーを保護します。電子メール用の柔軟なメッセージ処理オプションを提供します。Juniper ATP Appliance は、Office 365 や Google Mail などのクラウドベースの電子メールサービスをサポートし、SMB トラフィック内の脅威を検知します。
Security Director および JSA との統合	Juniper Secure Analytics（JSA）セキュリティ情報およびイベント管理（SIEM）は、脅威イベントを消費して関連付けることができます。Juniper ATP クラウドは、プロビジョニングと監視を行うため、Security Director Cloud と完全に統合されています。	Security Director Cloud と JSA を統合することで、統一された管理で、簡略化されたポリシーの適用と監視エクスペリエンスを提供します。

Juniper Advanced Threat Prevention 製品の詳細については、https://www.juniper.net/jp/ja/products/security/advanced-threat-prevention.html を参照してください。

一元管理

ジュニパー、Security Director Cloud は、すべての SRX シリーズファイアウォールの一元管理マネージャーです。革新的で直感的に使える一元化された Web ベースのインターフェイスを通して、すべての物理、仮想、およびコンテナ化されたファイアウォール向けセキュリティポリシー管理を提供し、新たな脅威ベクトルと従来の脅威ベクトル全体で強化します。アプリケーションパフォーマンスを詳細に可視化し、リスクを軽減し、ユーザーの診断を可能にし、問題を迅速に解決します。Juniper Security Director Cloud の詳細については、https://www.juniper.net/jp/ja/products/security/security-director-network-security-management.html をご覧ください。

SRX5400 Services Gateway　SRX5600 Services Gateway　SRX5800 Services Gateway

仕様

注：パフォーマンス、設定数、特長は、最適なラボ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。

	SRX5400	SRX5600	SRX5800
最大パフォーマンス/設定数 [1]			
テスト済みの Junos OS バージョン	Junos OS 21.2	Junos OS 21.2	Junos OS 21.2
ファイアウォール パフォーマンス、IMIX	960Gbps	1.44Tbps	3.36Tbps
シャーシあたりの最大パフォーマンス	960Gbps	1440 Tbps	3.36Tbps
次世代データセンターファイアウォールのパフォーマンス [2]	136Gbps	194Gbps	504Gbps
セキュア Web アクセスファイアウォールのパフォーマンス [3]	75 Gbps	107Gbps	277Gbps
レイテンシ（ステートフルファイアウォール）	~11µsec	~11µsec	~11µsec
IPsec VPN AES-256-GCM（IMIX）	188Gbps	269Gbps	699Gbps
最大 IPS パフォーマンス	172Gbps	245Gbps	638Gbps
最大同時セッション数	9100 万	1 億 8200 万	3 億 3800 万
新規セッション数/秒（持続、tcp、3 ウェイ、ファイアウォール NAT）	1.7/100 万	3.4/200 万	6.3/400 万
最大サポート ユーザー数	無制限	無制限	無制限
ネットワーク接続			
IOC4 オプション（SRX5K-IOC4-MRAT; SRX5K-IOC4-10G）	40x1GbE SFP+および 40x10GbE SFP+または 12xQSFP+/QSFP28 マルチレート		
IOC3 オプション（SRX5K-MPC3-100G10G; SRX5K-MPC3-40G10G）	2 x 100GbE CFP2 および 4 x 10GbE SFP+ または 6 x 40GbE QSFP+ および 24 x 10GbE SFP+		
ファイアウォール			
ネットワーク攻撃検知	○	○	○
DoS および DDoS（分散型サービス拒否）からの保護	○	○	○
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	○	○	○
IPsec VPN			
サイトツーサイトのトンネル数	15,000	15,000	15,000
トンネル用インターフェイス数	15,000	15,000	15,000
リモートアクセス/SSL VPN（同時）ユーザー数	25,000	40,000	50,000
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）		
インターネット重要な手がかり交換	IKEv1、IKEv2		
ペイロード設定	○	○	○

	SRX5400	SRX5600	SRX5800
IKE 認証アルゴリズム	MD5、SHA1、SHA-256、SHA-384、SHA-512		
IKE 暗号化アルゴリズム	プライム、DES-CBC、3DES-CBC、AEC-CBC、AES-GCM、SuiteB		
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)		
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, hmac-sha-384, hmac-sha-512		
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		
リプレイ攻撃防御	○	○	○
VPNs (GRE, IP-in-IP, MPLS)	○	○	○
VPN ゲートウェイ冗長化	○	○	○
侵入防御システム (IPS)			
シグネチャ ベースおよびカスタマイズ可能 (テンプレート使用)	○	○	○
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	○	○	○
ステートフル プロトコル シグネチャ	○	○	○
攻撃検知方式	ステートフル シグネチャ、プロトコル アノーマリ検知 (ゼロデイ対応) 、アプリケーション識別	ステートフル シグネチャ、プロトコル アノーマリ検知 (ゼロデイ対応) 、アプリケーション識別	ステートフル シグネチャ、プロトコル アノーマリ検知 (ゼロデイ対応) 、アプリケーション識別
攻撃対応方式	接続破棄、通信切断、セッションパケットログ、セッションサマリー、メール	接続破棄、通信切断、セッションパケットログ、セッションサマリー、メール	接続破棄、通信切断、セッションパケットログ、セッションサマリー、メール
攻撃通知方式	構造化システム ロギング	構造化システム ロギング	構造化システム ロギング
ワーム防御	○	○	○
推奨ポリシーによるインストールの簡素化	○	○	○
トロイの木馬防御	○	○	○
スパイウェア/アドウェア/キーロガー防御	○	○	○
高度なマルウェア防御	○	○	○
感染したシステムからの拡散防御	○	○	○
ポート スキャンの防御	○	○	○
リクエスト & レスポンス サイド攻撃防御	○	○	○
複合攻撃防御 - ステートフル シグネチャ検知とプロトコル アノーマリ検知の組み合わせ	○	○	○
カスタム攻撃シグネチャの作成	○	○	○
カスタマイズ可能なコンテキスト	600 以上	600 以上	600 以上
攻撃の編集 (ポート範囲など)	○	○	○
ストリーム シグネチャ	○	○	○
プロトコルしきい値	○	○	○
ステートフル プロトコル シグネチャ	○	○	○
アップデート頻度	毎日および緊急時	毎日および緊急時	毎日および緊急時
コンテンツセキュリティ			
アンチウィルス	○	○	○
コンテンツ フィルタリング	○	○	○
拡張 Web フィルタリング	○	○	○
リダイレクト Web フィルタリング	○	○	○
アンチスパム	○	○	○
AppSecure			
AppTrack (アプリケーションの可視化と追跡)	○	○	○
AppFirewall (アプリケーション名ごとのポリシー適用)	○	○	○
AppQoS (アプリケーション名ごとのネットワーク トラフィックの優先度設定)	○	○	○
ユーザーベースのアプリケーション ポリシー適用	○	○	○
GPRS セキュリティ			
GPRS ステートフル ファイアウォール	○	○	○
宛先ネットワーク アドレス変換 (NAT-Dst)			

	SRX5400	SRX5600	SRX5800
宛先 NAT と PAT (ポート アドレス変換)	○	○	○
ingress インターフェイス IP と同一サブネット内の NAT-Dst	○	○	○
NAT-Dst、多対 1、PAT あり (M：1P)	○	○	○
NAT-Dst、多対 1 (M：1)	○	○	○
NAT-Dst、多対多 (M：M)	○	○	○
送信元ネットワークアドレス変換 (NAT-Src)			
静的なソース NAT – IP 移行ダイナミック インターネット プロトコル (DIP)	○	○	○
NAT-Src、PAT あり、ポート変換	○	○	○
NAT-Src、PAT なし、固定ポート	○	○	○
NAT-Src、IP アドレス パーシステンス	○	○	○
ソース プールのグルーピング	○	○	○
ソース プールの利用率アラーム	○	○	○
インターフェイス サブネット外のソース IP	○	○	○
インターフェイス NAT-Src、インターフェイス DIP	○	○	○
要求が NAT プールを上回り、アドレス プールが枯渇したときは PAT にフォールバック	○	○	○
対称 NAT	○	○	○
NAT プールへの複数範囲割り当て	○	○	○
物理ポート用のプロキシー ARP (Address Resolution Protocol)	○	○	○
NAT-Src (ループバック グルーピング) - DIP (ループバック グルーピング)	○	○	○
ユーザー認証とアクセス コントロール			
組み込み (内部) データベース	○	○	○
RADIUS アカウンティング	○	○	○
Web ベースの認証	○	○	○
公開カギ基盤 (PKI) サポート			
PKI 証明書要求 (PKCS 7、PKCS 10、CMPv2)	○	○	○
自動証明書登録 (SCEP)	○	○	○
対応認証局	○	○	○
自己署名証明書	○	○	○
仮想化			
データプレーン分離によるカスタムルーティングインスタンス最大数	2000	2000	2000
最大セキュリティゾーン数	2000	2000	2000
データプレーンと管理用の分離 (論理/テナントシステム) による仮想ファイアウォール最大数	500	500	500
ジュニパーネットワークス vSRX 仮想ファイアウォール (VM ベース) による追加のオフプラットフォーム仮想ファイアウォールオプション	無制限	無制限	無制限
サポート VLAN 最大数	4096	4096	4096
ルーティング			
BGP インスタンス	1000	1000	1000
BGP ピア	2000	2000	2000
BGP ルート数	100 万	100 万	100 万
OSPF インスタンス	400	400	400
OSPF ルート数	100 万	100 万	100 万
RIP v1/v2 インスタンス	50	50	50
RIP v2 テーブル サイズ	30,000	30,000	30,000
ダイナミック ルーティング	○	○	○
スタティックルート	○	○	○
ソースベース ルーティング	○	○	○
ポリシーベース ルーティング	○	○	○
等コスト マルチパス (ECMP)	○	○	○
リバース パス フォワーディング (RPF)	○	○	○
マルチキャスト	○	○	○

	SRX5400	SRX5600	SRX5800
IPv6			
ファイアウォール/ステートレス フィルター	○	○	○
デュアル スタック IPv4/IPv6 ファイアウォール	○	○	○
RIPng	○	○	○
BFD、BGP	○	○	○
ICMPv6	○	○	○
OSPFv3	○	○	○
サービスクラス (CoS)	○	○	○
動作モード			
レイヤー 2 (透過) モード	○	○	○
レイヤー 3 (ルートおよび/または NAT) モード	○	○	○
IP アドレス割り当て			
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	○	○	○
トラフィック管理サービス品質 (QoS)			
最大帯域	○	○	○
IPv4 の RFC2474 IP Diffserv	○	○	○
COS 用ファイアウォール フィルター	○	○	○
分類	○	○	○
スケジューリング	○	○	○
シェーピング	○	○	○
インテリジェント ドロップ メカニズム (WRED)	○	○	○
3 つのレベルでのスケジューリング	○	○	○
スケジューリングの各レベルでの WRR (Weighted Round Robin)	○	○	○
ルーティング プロトコルの優先度	○	○	○
ハードウェアでのトラフィック管理/ポリシー実行	○	○	○
高可用性 (HA)			
アクティブ/パッシブ、アクティブ/アクティブ	○	○	○
統合型インサービスソフトウェアアップグレード (統合型 ISSU)	○	○	○
設定同期	○	○	○
ファイアウォール/IPsec VPN のセッション同期	○	○	○
ルーティング変更によるセッション フェイルオーバー	○	○	○
デバイス障害検知	○	○	○
リンクおよびアップストリームの障害検知	○	○	○
デュアル コントロール リンク	○	○	○
インターフェイス リンク アグリゲーション/リンク アグリゲーション コントロール プロトコル (LACP)	○	○	○
冗長ファブリックリンク	○	○	○
管理			
WebUI (HTTP および HTTPS)	○	○	○
コマンドライン インターフェイス (コンソール、telnet、SSH)	○	○	○
Juniper Security Director Cloud	○	○	○
運用管理			
ローカル管理者データベース サポート	○	○	○
外部管理者データベース サポート	○	○	○
管理者ネットワーク	○	○	○
Root Admin、Admin、Read Only の各ユーザー レベル	○	○	○
ソフトウェア アップグレード	○	○	○
設定のロールバック	○	○	○

	SRX5400	SRX5600	SRX5800
ログ収集/モニタリング			
構造化された syslog	○	○	○
SNMP (v2 および v3)	○	○	○
Traceroute	○	○	○
認定資格			
安全規格	○	○	○
電磁気適合性規格 (EMC)	○	○	○
RoHS2 準拠 (EU 指令 2011/65/EU)	○	○	○
NIST FIPS-140-2 レベル 2	○	○	○
コモン クライテリア NDPP+TFFW EP + VPN EP	○	○	○
USGv6	○	○	○
寸法と電源			
外形寸法 (幅 x 高さ x 奥行き)	44.3 x 22.1 x 62.2 cm (17.45 x 8.7 x 24.5 インチ)	44.5 x 35.6 x 60.5 cm (17.5 x 14 x 23.8 インチ)	44.5 x 70.5 x 59.7 cm (17.5 x 27.8 x 23.5 インチ)
重量	フル装備の場合 128 ポンド (58.1kg)	フル実装時: 81.7 kg (180 ポンド)	フル実装時: 151.6 kg (334 ポンド)
電源 (AC)	100 ~ 240 VAC	100 ~ 240 VAC	200 ~ 240 VAC
電源 (DC)	-40 ~ -60 VDC	-40 ~ -60 VDC	-40 ~ -60 VDC
最大消費電力	4,100 ワット (AC 大容量)	4,100 ワット (AC 大容量)	8,200 ワット (AC 大容量)
標準消費電力	1540 ワット	2440 ワット	5015 ワット、10200 ワット (AC/DC)、200-305VAC、200-410VDC
環境規制			
動作時温度範囲 (長期間)	5 ~ 40°C (41 ~ 104°F)	5 ~ 40°C (41 ~ 104°F)	5 ~ 40°C (41 ~ 104°F)
湿度範囲 (長期間)	5 ~ 85% (結露しないこと)	5 ~ 85% (結露しないこと)	5 ~ 85% (結露しないこと)
湿度範囲 (短期間)	5 ~ 93% (結露しないこと)。ただし、水蒸気 0.026 kg/乾燥空気 1 kg を超えないこと	5 ~ 93% (結露しないこと)。ただし、水蒸気 0.026 kg/乾燥空気 1 kg を超えないこと	5 ~ 93% (結露しないこと)。ただし、水蒸気 0.026 kg/乾燥空気 1 kg を超えないこと

[1] このリストに示しているパフォーマンス、設定数、特長は、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 リリースの種類や展開方法によって異なります。
[2] 次世代データセンターファイアウォールのパフォーマンスは、ファイアウォール、アプリケーションセキュリティおよび IPS を有効にした状態で、64KB トランザクションを使用して測定したものです。
[3] セキュア Web アクセスファイアウォールのパフォーマンスは、ファイアウォール、アプリケーションセキュリティ、IPS、SecIntel および URL フィルタリングを有効にした状態で、64KB のトランザクションを使用して測定したものです。

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、ネットワークの高速化、拡張、最適化を実現する高度なパフォーマンスサービスに対応するリーダーです。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、運用効率を最大化します。詳細については、https://www.juniper.net/jp/ja/products.html をご覧ください。

注文情報

ジュニパーネットワークス SRX シリーズのファイアウォールのご注文や、ソフトウェアライセンス情報へのアクセスをご希望の場合は、ご購入方法ページ (https://www.juniper.net/jp/ja/how-to-buy/form.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/