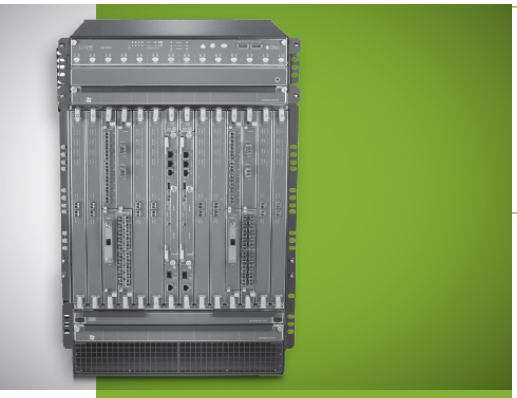

SRX5400、SRX5600、SRX5800 サービス ゲートウェイ

製品概要

SRX シリーズ サービス ゲートウェイは革新的なアーキテクチャをベースとした次世代のファイアウォールであり、圧倒的なパフォーマンス、拡張性、可用性、およびセキュリティ サービスの統合を可能にします。処理能力や I/O 能力の柔軟な拡張性、およびサービス統合に対応するカスタム設計により、SRX シリーズ サービス ゲートウェイはデータ センターの統合やサービス アグリゲーションに伴うセキュリティ要件を十分に満たしています。同様に、受賞歴のある SRX シリーズに搭載された Junos OS は業界屈指のオペレーティング システムであり、世界最大級のネットワークの可用性、管理、セキュリティ保護を維持します。

製品説明

ジュニパーネットワークス®の SRX5400、SRX5600、SRX5800 サービス ゲートウェイは次世代ファイアウォール（NG-FW）であり、優れた防御機能や、市場をリードするパフォーマンス、99.9999% の信頼性と可用性、拡張性、サービス統合を実現します。以下に示すようなサービス プロバイダ、大企業、公的機関などのネットワークに最適です。

- 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
- 大企業のデータ センター

SRX5400、SRX5600、SRX5800 は、高度な脅威からユーザー、アプリケーション、インフラストラクチャを保護するために構築された Juniper Connected Security フレームワークの不可欠な部分です。

これらのプラットフォームは、悪用、マルウェア、およびコマンド & コントロール（C&C）通信に対して最高レベルの保護を提供し、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、コンテンツ セキュリティ、侵入防御システム（IPS）、および統合型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 サービスを備えています。

また、さらに高度な保護機能として、SRX シリーズでは、クラウド上で動作するジュニパーの脅威インテリジェンス プラットフォームであるジュニパーネットワークスの Advanced Threat Prevention（ATP）を介した統合脅威インテリジェンス サービスを提供しています。Juniper ATP Cloud は、C&C 関連のボットネットや Web アプリケーションの脅威に対する高度な防御を可能にする実用的なセキュリティ インテリジェンスを SRX シリーズデバイスに提供するとともに、GeoIP データに基づいてポリシーを適用します。これらはすべて、ジュニパーネットワークスの提供するフィードに基づいて行われます。またお客様は、自身の顧客やサードパーティーのフィードを使い、自社のビジネス環境に特化した高度なマルウェアやその他の脅威から保護することができます。この高度な顧客関連の統合型脅威インテリジェンス サービスは、クラウドからオンプレミスの SRX シリーズに配信されます。

SRX5400、SRX5600、SRX5800 は、ジュニパーネットワークスセキュリティディレクターがサポートしており、新しいリスクベクトルと従来のリスクベクトル全体の適用を可能にする直感的な一元化されたインターフェイスを通じて、分散型セキュリティポリシー管理を可能にします。管理者は、直感的なダッシュボードとレポート機能を活用しながら、脅威、セキュリティを侵害されたデバイス、リスクのあるアプリケーションなどを把握できます。

SRX5000 シリーズは、ジュニパーネットワークスのダイナミック サービス アーキテクチャをベースとし、比類なき拡張性とパフォーマンスを実現します。各サービス ゲートウェイは、サービス処理カード (SPC)、I/O カード (IOC) を追加することで、ほぼリニアに拡張でき、フル装備の SRX5800 では最高 1 Tbps のファイアウォール スループットに対応できます。SPC は広範なサービスに対応できるよう設計されており、将来的に最新の機能に対応する際も、サービス専用のハードウェアを追加する必要はありません。すべてのサービスに SPC を使用することで、特定サービスの使用によってアイドル状態のリソースが発生することはなく、ハードウェアを最大限に活用できます。

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 シリーズはモジュラー式アプローチを採用しており、各プラットフォームに IOC を柔軟に実装できるため、1GbE、10GbE、40GbE、100GbE インターフェイスを含む広範な接続オプションをご利用いただけます。IOC は SPC と同一のインターフェイス スロットを使用するため、必要に応じて処理と I/O の理想的なバランスを考慮してゲートウェイを構成できます。 したがって、SRX シリーズを導入する際、個々のネットワーク固有の要件に応じたカスタマイズが可能です。

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 シリーズの緊密なサービス統合は、ジュニパーネットワークス Junos® OS をベースにしています。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 シリーズは超低遅延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 サービス ゲートウェイは、ステートフル ファイアウォールで最大 1 Tbps のファイアウォール スループットと 32 マイクロ秒という低遅延をサポートする、市場をリードするセキュリティ ソリューションです。また、SRX5800 は 860 Gbps IPS スループット と 3 億 3800 万の同時セッションもサポートしています。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 サービス ゲートウェイは、SRX5800 と同じ SPC と IOC を使用し、最大 480 IMIX Gbps 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、および 460 Gbps IPS スループット をサポートできます。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、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 サービスゲートウェイは、SRX5800 と同じ SPC と IOC を使用し、最大 270 Gbps の IMIX ファイアウォール、9000 万の同時セッション、および 230 Gbps IPS スループット をサポートできます。SRX5400 はコンパクトな設置面積で高性能なゲートウェイを、エッジ領域またはコア領域のセキュリティ導入に対応し、大企業のキャンパス ネットワークやデータ センター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)

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 サービス ゲートウェイでサポートされています。

I/O カード (IOC)

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、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。

ジュニパーの IOC の第 3 世代である IOC3 は、100GbE、40GbE、高密度 10GbE インターフェイスなどの優れた接続オプションとともに、高いスループットを実現します。IOC3 カードは、SRX5400、SRX5600、SRX5800 でサポートされています。

第 4 世代の IOC は、最大 480 Gbps の利用可能なすべてのラインカードの中で最高のスループットを提供し、10GbE および 40GbE から 100GbE までの複数の接続オプションを提供します。IOC4 は、ラインカードあたり最大 480Gbps のハードウェア加速型のスループットを提供できます。

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 ルーティング エンジン (RE3) は、2000 MHz で動作するマルチコア プロセッサを搭載した SRX5000 シリーズ用の RE シリーズの最新製品です。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

サービス ゲートウェイのジュニパーネットワークス SRX5000 シリーズは、堅牢なネットワーク サービスとセキュリティ サービスを実現するために一から設計されました。

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 アーキテクチャをベースとした拡張可能な処理能力を提供します。	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 を提供します。	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 アーキテクチャをベースとしたモジュラー カードを使用した柔軟な I/O オプションを提供します。	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・脅威から保護 • 業界トップクラス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。
AppFirewall	きめ細かなアプリケーション コントロール ポリシーにより、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、アプリケーションとユーザー ロールに基づいたセキュリティ ポリシーの作成と適用が可能になります。
AppQoS	Juniper の豊富な QoS 機能を活用して、お客様のビジネスや帯域幅の必要性に応じてアプリケーションの優先順位付けを行います。	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。

特長	説明	メリット
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 暗号化および復号化を実行します。	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。
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 スループットと低遅延を実現します。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 と正常にペアリングして、SRX5000 サービス ゲートウェイ シリーズのいずれかでファイアウォールのパフォーマンスを最大化します。	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導入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。	インサービス 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/アクティブ構成の IPS モニタリングのサポートが含まれます。
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。	関連トラフィックをさらに詳しく分析して、標的を保護する手順を決定します。

コンテンツ セキュリティ機能

SRX5000 シリーズ サービス ゲートウェイで提供されるコンテンツ セキュリティ サービスには、業界屈指のアンチウィルス、アンチスパム、コンテンツ フィルタリング、および追加のコンテンツ セキュリティ サービスが含まれています。

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、標準ベースの 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。
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。Juniper ATP Cloud がこの情報を処理し、ネットワーク動作分析と機械学習に基づいて接続が無害なものか悪意のあるものかを判定します。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。
セキュリティ・ディレクターおよび JSA との統合	ジュニパーネットワークス Secure Analytics ポートフォリオ（JSA シリーズ）セキュリティ情報およびイベント管理（SIEM）は、脅威イベントを使用し、相関付けることができます。また、ジュニパー ATP クラウドは、プロビジョニングや監視のために Security Director と完全統合されています。Juniper ATP Appliance は管理コンソールが組み込まれており、Security Director と統合されていません。	Security Director と JSA シリーズの統合による単一パネル管理により、シンプルなポリシー適用とモニタリングを実現します。

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

一元管理

ジュニパーネットワークス®セキュリティ・ディレクターは、すべての SRX シリーズサービスゲートウェイの中央マネージャーです。革新的で直感的で一元化された Web ベースのインターフェイスにより、すべての物理、論理、および仮想ファイアウォールにセキュリティ ポリシー管理を提供し、新興および従来の脅威ベクトル全体の適用を実行します。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。ジュニパーネットワークスのセキュリティ・ディレクターの詳細については、https://www.juniper.net/jp/ja/products/security/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	IOC4 あたり 480Gbps	IOC4 あたり 480Gbps	IOC4 あたり 480Gbps
シャーシあたりの最大パフォーマンス	960 Gbps	1440 Tbps	3.36 Tbps
次世代ファイアウォールのパフォーマンス	100 Gbps	210 Gbps	400 Gbps
遅延（ステートフル ファイアウォール）	~11µsec	~11µsec	~11µsec
IPsec VPN AES-256-GCM（IMIX）	140 Gbps	280 Gbps	530 Gbps
最大 IPS パフォーマンス	230 Gbps	460 Gbps	860 Gbps
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）	40 x 10GbE SFP + または 12 x QSFP+/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		
構成ペイロード	○	○	○
IKE 認証アルゴリズム	MD5、SHA1、SHA-256、SHA-384、SHA-512		

	SRX5400	SRX5600	SRX5800
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	事前共有重要な手がかりおよび公開重要な手がかり基盤（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		
Perfect forward secrecy（PFS）	○		
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	標準ベースのデッドピア検出（DPD）、VPN 監視		
リプレイ攻撃防御	○	○	○
VPN（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	○	○	○

	SRX5400	SRX5600	SRX5800
宛先ネットワーク アドレス変換 (NAT-Dst)			
宛先 NAT と PAT (ポート アドレス変換)	○	○	○
イングレスインターフェイス 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	○	○	○
公開鍵基盤 (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 Virtual Firewall (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)	○	○	○

	SRX5400	SRX5600	SRX5800
マルチキャスト	○	○	○
IPv6			
ファイアウォール/ステートレス フィルター	○	○	あり
デュアル スタック IPv4/IPv6 ファイアウォール	あり	○	○
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)	○	○	あり
3 つのレベルでのスケジューリング	あり	○	○
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)	○	○	○
Junos Space Security Director	○	○	○

	SRX5400	SRX5600	SRX5800
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	○	○	○
設定ロールバック	○	○	○
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
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

‡ 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。

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、ネットワークへの投資から早期に収益を図ることができます。また、ネットワークを最適化することで、必要なパフォーマンスレベルや信頼性、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/ja/products-services 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 サービス ゲートウェイを注文し、ソフトウェア ライセンス情報にアクセスするには、https://www.juniper.net/jp/jp/how-to-buy/ の「購入方法」ページにアクセスしてください。

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大幅に簡素化し、エンドユーザーに優れたエクスペリエンスを提供することを目指しています。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で、真のビジネス成果をもたらします。つながりを強めれば、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信じています。

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