SRX4300 ファイアウォール

製品概要

データセンターが従来のアーキテクチャから分散型アーキテクチャへと進化するにつれて、ファイアウォールの役割も拡大する必要があります。ファイアウォールは、境界テクノロジーではなく、ネットワーク全体に織り込まれたセキュリティファブリックの一部である必要があります。セキュリティファブリックにより、すべての接続ポイントでセキュリティが維持されます。

ジュニパーネットワークス SRX4300 次世代ファイアウォールは、この新しいアーキテクチャに不可欠であり、組織はネットワーク全体のセキュリティを運用できます。ネットワークを保護するために、この 1U の電力効率に優れたファイアウォールは、組み込みのゼロトラスト、イーサネット VPN-仮想拡張 LAN（EVPN-VXLAN）ファブリック統合、AI 予測による脅威防止を提供します。SRX4300 は、ワイヤスピード MACsec を備えた複数の 100 Gbps インターフェイスをサポートします。

製品説明

Juniper Networks® SRX4300 ファイアウォールは、エンタープライズキャンパス、データセンターエッジ、コアを保護するために設計された、高性能な次世代ファイアウォール（NGFW）です。ローミングと SD-WAN セキュアハブファイアウォールのユースケースもサポートします。キャリアグレードのルーティングと最先端のスイッチングを組み合わせたこのプラットフォームは、堅牢なセキュリティ、効果的な脅威検知、包括的な自動化と緩和機能を提供します。

図 1：ジュニパー SRX ファイアウォールは、CyberRatings と NetSecOpen によって、セキュリティ有効性において最高のスコアを獲得しました。

SRX4300 は、クラウド対応のエンタープライズネットワークとデータセンターの変化するニーズをサポートする NGFW 機能を提供します。エンタープライズキャンパス内での新しいサービスの展開、クラウドへのシームレスな接続、業界標準への準拠、運用効率の向上など、SRX4300 は、企業がビジネス目標を実現しながら、ゼロトラスト原則を大規模に運用することを可能にします。SRX4300 は、侵入防御システム（IPS）、ユーザーをフォローするアクセスポリシー、アプリケーションをフォローするアクセスポリシー、ジュニパーの AI 予測による脅威防止などの機能により、重要な企業資産を保護します。さらに、SRX4300 はジュニパーのクラウドセキュリティソリューションと連携して、ネットワーク全体の可視性と制御機能によりハイブリッドクラウド環境を保護し、オンプレミスとクラウド環境を一貫して保護します。

ネットワークアーキテクチャの分散化と非中央集権化が進む中、ジュニパーネットワークスの SRX シリーズファイアウォールは、他のジュニパーネットワークスおよびサードパーティのネットワーキングプラットフォームとのシームレスな 統合を保証します。同時に、NGFW はアーキテクチャの変革をサポートし、組織をオンプレミスからハイブリッドクラウド環境へとシームレスにコスト効率よく移行させます。SRX シリーズファイアウォールは、業界標準のイーサネット VPN（EVPN）タイプ 5 と仮想拡張 LAN（VXLAN）プロトコルをデータセンター環境に初めて実装した製品であり、SRX4300 をデータセンタースパインリーフアーキテクチャのセキュアなファブリック 認識型のリーフとして機能させることができます。

SRX4300 は、業界初の Connected Security 分散型サービスアーキテクチャを採用し、組織は水平方向に拡張可能で、弾力的なスケーリングを実現し、大規模なファイアウォールネットワークの運用管理を簡素化できます。このアーキテクチャにより、複数の SRX4300 プラットフォームを単一の大規模な論理ファイアウォールとして連携し、より高いパフォーマンスと拡張性でセキュリティを提供します。

SRX4300 は、世界最大のミッションクリティカルなエンタープライズネットワークとサービスプロバイダネットワークを支え、保護するのに役立つ Junos®オペレーティングシ

ステム（Junos OS）を搭載しています。組織の現在の導入を将来のアーキテクチャ展開に結び付けるジュニパーの統合管理エクスペリエンスである Juniper® Security Director Cloud によって管理されます。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、脅威インテリジェンスのすべてを一元的に提供します。

アーキテクチャと主要コンポーネント

SRX4300 ハードウェアおよびソフトウェアアーキテクチャは、コンパクトで拡張性の高い 1U フォームファクタでコスト効率の高いセキュリティを提供します。ネットワーク環境を保護するために構築された SRX4300 は、Junos OS 上に複数のセキュリティサービスとネットワーキング機能を組み込み、高度にカスタマイズ可能な脅威保護、自動化、統合機能を提供します。SRX4300 のクラス最高の高度なセキュリティ機能は、IMIX トラフィックパターンを使用したデータセンター、エンタープライズキャンパス、地域本部の導入に最適です。

組み込みのゼロトラスト

SRX4300 は、組み込みのトラステッドプラットフォームモジュール（TMP） 2.0 や暗号署名付きデバイス ID など、信頼を高め、運用を合理化するゼロトラストデバイス機能を搭載しています。

SRX4300 は、RFC 準拠のセキュアゼロタッチプロビジョニング（sZTP）をサポートしており、ネットワークに製品を効率的で迅速にリモートで展開することができます。さらに、SRX4300 はワイヤスピードで MACsec をサポートし、データの整合性と機密性を確保します。

Connected Security Distributed Services Architecture

SRX4300 は、ジュニパーの Connected Security 分散型サービスアーキテクチャの一部であり、データセンターセキュリティに革命を起こします。ジュニパーの Connected Security 分散型サービスアーキテクチャにより、複数のロケーションのトラフィックフォワーディングとセキュリティサービスを相互接続することで、ファイアウォールのパフォーマンスを水平方向に拡張できます。ジュニパーのソリューションは、フォワーディングコンポーネントと検査コンポーネントのフェイルオーバーとバックアップノードを自動化します。冗長性とロードバランシングに加え、ジュニパーの Connected Security 分散型サービスアーキテクチャにより、大規模なデータセンターファイアウォールネットワークの管理と運用を簡素化します。物理フォームファクタ、仮想化フォームファクタ、コンテナ化されたフォームファクタに追加されるファイアウォールエンジンの数に関係なく、1 つの論理ユニットとして管理できます。この一元化された管理により、従来のスケールアウトアプローチの意図しない結果であった複雑さを解消します。

特長とメリット

ビジネス要件	機能/ソリューション	SRX4300 のメリット
高性能	ハードウェアアクセラレーション暗号化/復号化	• CPU を大量に消費する暗号化/復号化タスクの負荷を軽減 • SSL と IPsec のパフォーマンスを向上させます。
高品質のエンドユーザーエクスペリエンス	アプリケーションの可視化と制御	• アプリケーションを継続的に更新し、カスタムアプリケーションをデコードします。 • アプリケーションおよびユーザーロールに基づいてトラフィックを制御し、優先度を設定 • Web と SaaS を含む、SSL 暗号化トラフィック内のアプリケーションを検査して検出します。
脅威からの高度な保護機能	NGFW サービス：IPS、アンチウィルス、アンチスパム、Web フィルタリング Juniper Advanced Threat Prevention Cloud：サンドボックス、暗号化されたトラフィックのインサイト、SecIntel の脅威インテリジェンスフィード	• 99.9%の有効性でエクスプロイトを防止します。シグネチャのリアルタイム更新 • 既知のマルウェアや、悪意のある Web と DNS トラフィックから保護します • iOS、Windows、Android、CentOS を含む複数の OS タイプにわたる未知のマルウェアのサンドボックス化 • オープンプラットフォームで脅威インテリジェンスを提供し、サードパーティの脅威フィードとカスタム脅威フィードに対応します。 • 復号化することなく、暗号化されたトラフィックに隠れた脅威を検出します。
ゼロデイ攻撃防御	ジュニパーの AI 予測による脅威防止	• AI を使用してパケットスニペットからの脅威を効果的に特定し、ラインレートでマルウェアを予測し防止 • 患者ゼロ感染を排除 • 攻撃ライフサイクル全体を通してアクティブな保護シグネチャを自動生成し、その後の攻撃からネットワークを安全に保ちます。
安全なデータ取引	Juniper Secure Connect：IPSec VPN、リモートアクセス/SSL VPN	• ハイパフォーマンスな IPsec VPN に専用の暗号化エンジンを提供 • リモートアクセスや動的なサイト間通信など、さまざまなネットワーク設計に多様な VPN オプションを提供 • 自動 VPN により、大規模な VPN 導入を簡素化 • ハードウェアベースの暗号化アクセラレーションを搭載 • セキュアで柔軟なリモートアクセス SSL VPN
高度なネットワーキングサービス	ルーティング、セキュア ワイヤ	• キャリアクラスの高度なルーティングおよび QoS（サービス品質）をサポート

ビジネス要件	機能/ソリューション	SRX4300 のメリット
データセンターファブリックに組み込まれたセキュリティ	EVPN-VXLAN（EVPN タイプ 5 ルート）	• レイヤー 4-7 セキュリティサービスにより、VXLAN カプセル化トラフィックのトンネル検査を強化 • BGP を通して Type 5 サポートで運用を簡素化 • EVPN-VXLAN トラフィックのカプセル化解除は不要
信頼性	シャーシクラスター、冗長電源	• ステートフル構成とセッション状態の同期を提供 • アクティブ/アクティブおよびアクティブ/バックアップの導入シナリオをサポート • PSU（冗長電源装置）および冗長ファン搭載の高可用性ハードウェアを提供
管理および拡張が容易	Juniper Security Director Cloud、オンボックス GUI	• ゼロタッチプロビジョニング（ZTP）、完全な可視化、インテリジェントなルール配置、簡略化されたポリシー設定と自動化など、ジュニパーの統合管理エクスペリエンスを介して一元化された管理を提供します。 • ネットワークアドレス変換（NAT）と、ウィザードによる自動 IPSec VPN 導入をサポート • オンボックス GUI をサポート
組み込みのゼロトラスト機能	TPM 2.0 モジュール付き DevID	• デバイスの信頼できる状態を簡単に検証します。 • ハードウェアとソフトウェア認証向けに RFC 準拠の sZTP をサポートする暗号署名付きデバイス ID を提供します。 • サプライチェーン攻撃のリスクを軽減します
TCO 低減	Junos OS	• 1 つのデバイスにルーティングおよびセキュリティ機能を統合 • Junos OS の自動化機能により運用コストを削減 • Juniper MX、PTX、ACX ルーターなどの Junos OS を実行する他のデバイス、EX および QFX スイッチ、クラウドネイティブの Contrail Networking（CN2）との自動統合

[1]CyberRatings の 2023 年エンタープライズファイアウォールテストレポートでテストされた、エクスプロイトブロック率の結果

図 2：SRX4300 ファイアウォール

ソフトウェアの仕様

ファイアウォールサービス

- ステートフルファイアウォールサービス
- ゾーンベースのファイアウォール
- スクリーニングおよび DDoS（分散型サービス拒否）からの保護
- 異常なプロトコルおよびトラフィックからの保護
- 統合型アクセスコントロール（UAC）
- Juniper Mist™ Access Assurance との統合

キャリアグレードネットワークアドレス変換（CGNAT）

- キャリアグレードのネットワークアドレス変換（大規模 NAT）
- IPv4 および IPv6 アドレス変換 NAT44、NAPT44、NAT66、NAPT66、NAT64、NAT46
- 静的および動的な 1-1 変換
- ソース NAT と PAT（ポートアドレス変換）
- 宛先 NAT と PAT（ポート アドレス変換）
- 永続的な NAT（EIM/EIF）
- ポートブロック割り当て（PBA）
- Deterministic NAT（DetNAT）
- ポートオーバーロード
- Twice-NAT44
- DS-lite

VPN 機能

- 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）
- Juniper Secure Connect：リモートアクセス/SSL VPN
- 設定ペイロード：◯
- IKE 暗号化アルゴリズム：Prime、3DES-CBC、AES-CBC、AES-GCM、Suite B
- 認証：事前共有カギおよび公開カギ基盤（PKI）（X.509）
- IPsec：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
- 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：Prime、DES-CBC、3DES-CBC、AEC-CBC、AES-GCM、Suite B
- 完全転送機密保持、アンチリプレイ
- Internet Key Exchange：IKEv1、IKEv2
- 監視：スタンダードベースのデッドピア検出、VPN モニタリング
- GRE over IPSec、IP-in-IP、MPLS

高可用性機能

- Virtual Router Redundancy Protocol（VRRP): IPv4 および IPv6
- Stateful high availability: デュアルボックスクラスタリング
  - アクティブ/パッシブ
  - アティブ/アクティブ
  - 設定同期
  - ファイアウォールセッション同期
  - デバイス/リンク検出
  - ISSU（インサービスソフトウェアアップグレード）
  - IP 監視によるルートとインターフェイスのフェイルオーバー
  - BFD 監視
- シャーシクラスター HA とマルチノード HA（MNHA）

アプリケーション セキュリティ サービス [2]

- アプリケーションの可視化と制御
- アプリケーション QoS
- 高度なアプリケーションポリシーベースのルーティング（APBR）
- Application Quality of Experience (AppQoE)
- アプリケーションベースのマルチパス ルーティング
- ユーザーベースファイアウォール

脅威防御サービスおよびインテリジェントサービス [2]

- 侵入防御システム
- AI 予測による脅威防止
- アンチウィルス
- アンチスパム
- カテゴリー/レピュテーションベースの URL フィルタリング
- SSL プロキシ/インスペクション
- ボットネット（コマンド＆コントロール）からの保護
- GeoIP をベースにした適応型ポリシー適用
- ゼロデイ攻撃を検知してブロックする Juniper Advanced Threat Prevention（クラウドベースの SaaS サービス）
- 適応型脅威プロファイリング
- 暗号化されたトラフィックのインサイト
- SecIntel の脅威インテリジェンス
- Juniper ATP バーチャルアプライアンス、ゼロデイ攻撃を検出しブロックする分散型のオンプレミス Advanced Threat Prevention ソリューション

[2] 高度なセキュリティサブスクリプションライセンスとして提供。

ルーティングプロトコル

- IPv4、IPv6、スタティックルート、RIP v1/v2
- OSPF/OSPF v3
- BGP（ルートリフレクタ使用時）
- IS-IS
- マルチキャスト：IGMP v1/v2（インターネットグループマネージメントプロトコル）、PIM（プロトコルインディペンデントマルチキャスト）、SM（スパースモード）、SSM（ソーススペシフィックマルチキャスト）、SDP（セッションディスクリプションプロトコル）、DVMRP（ディスタンスベクターマルチキャストルーティングプロトコル）、MSDP（マルチキャストソースディスカバリープロトコル）、RPF（リバースパスフォワーディング）
- カプセル化：VLAN、PPPoE（Point-to-Point Protocol over Ethernet）
- 仮想ルーター
- ポリシーベースルーティング、ソースベースルーティング
- EVPN-VXLAN（EVPN タイプ 5 ルート）
- ECMP（等価コストマルチパス）

QoS 機能

- 802.1p、DSCP（DiffServ コードポイント）、EXP のサポート
- VLAN、DLCI（データリンクコネクション識別）、インターフェイス、バンドル、またはマルチフィールドフィルターに基づいた分類
- マーキング、ポリシング、およびシェーピング
- 分類およびスケジューリング
- WRED（Weighted Random Early Detection）保証および最大帯域幅
- ingress トラフィックのポリシング
- 仮想チャネル

ネットワークサービス

- ダイナミックホスト構成プロトコル（DHCP） クライアント/サーバー/リレー
- DNS（Domain Name System）プロキシ、DDNS（dynamic DNS）
- ジュニパーリアルタイムパフォーマンス 監視（RPM）および IP 監視
- フロー監視（J-Flow）

高度なルーティングサービス

- MPLS（RSVP、LDP）
- CCC（サーキットクロスコネクト）、TCC（トランスレーショナルクロスコネクト）
- L2/L2 MPLS VPN、pseudowires
- VPLS（仮想プライベート LAN サービス）、NG-MVPN（次世代マルチキャスト VPN）
- MPLS トラフィックエンジニアリングおよび MPLS 高速再ルート

管理、自動化、ログ記録、通知

- SSH、Telnet、SNMP-MIB、トラップ
- スマートイメージダウンロード
- ジュニパー CLI と Web UI、NetCONF、XML API、RMON
- Juniper Security Director Cloud
- Python
- Junos イベント、コミットおよび OP スクリプト
- アプリケーションおよび帯域幅の使用状況レポート
- デバッグおよびトラブルシューティングツール

ハードウェアの仕様

表 1. SRX4300 ハードウェア仕様

仕様	SRX4300
接続性	
オンボードポート	8 x 1 GbE/2.5 GbE/5 GbE/10 GbE BASE-T
オンボード小型フォームファクタプラガブルプラス（SFP+）トランシーバーポート	8 x 1 GbE/10 GbE SFP+ 4 x 1 GbE/10 GbE/25 GbE SFP28 6 x 40 GbE/100 GbE QSFP28
OOB（アウトオブバンド）管理用ポート	1 x 1 GbE G（RJ-45）
専用の HA（高可用性）ポート数	2 x 1 GbE SFP
コンソール	1（RJ-45）
USB 3.0 ポート（タイプ A）	1
ストレージ	
ストレージ (SSD)	1 x 120 GB（プライマリ）、1 x 960 GB（セカンダリ + ログディスク）
寸法と電源	
筐体	1U
サイズ（幅 x 高さ x 奥行き）	43.89 x 4.42 x 46.23 cm （17.28 x 1.74 x 18.20 インチ）
重量（デバイスおよび電源ユニット）	2 つの AC PSU を搭載したシャーシ：20.2 ポンド（9.2kg） 2 つの DC PSU を搭載したシャーシ：20.5 ポンド（9.3kg） パッケージ付きシャーシ：36.6 lb (16.6 kg)
冗長構成の電源ユニット	1+1
電源	2 x 850W AC PSU 冗長構成 2 x 850W DC PSU 冗長構成
平均発熱量	1 x DC PSU（40V）：1221.5 BTU/h 2 x DC PSU（40V）：1224.9 BTU/h 1 x AC PSU（110V）：1206.2 BTU/h 1 x AC PSU（230V）：1175.5 BTU/h 2 x AC PSU（110V）：1228.4 BTU/h 2 x AC PSU（230V）：1206.2 BTU/h
最大消費電流	4.67 A（110 V AC PSM 用） 2.188 A（230 V AC PSM 用） 11.53 A（-40 V DC 電源用）
最大突入電流	AC1 サイクル用 40 A（AC PSM） 40 A-pk（DC PSM）
環境規制	
気流/冷却	フロントツーバック
動作時温度	32～104° F（高度 6000 フィートで 0～40° C）
動作時湿度	5%～90%の非結露
平均故障間隔（MTBF）	100,000 時間以上（12 年間）
FCC 分類	クラス A
RoHS コンプライアンス	RoHS 6

仕様	SRX4300
パフォーマンスと拡張性	
ファイアウォールスループット[3]（IMIX）（Gbps）	7,000 万
ファイアウォールスループット[3]（1518B）Gbps	98
IPSec VPN スループット[3]（IMIX）（Gbps）	40
IPSec VPN スループット[3]（1400B）、Gbps	94
アプリケーションセキュリティパフォーマンス（TPS##）、単位：（Gbps）	85/45
次世代ファイアウォール（TPS##）[4] 単位：Gbps	83/24
セキュア Web アクセスファイアウォール（CPS**）、単位：Gbps	21
Advanced Threat (CPS**)[6] インチ Gbps	11
1 秒あたりの接続数（64B）	800,000
1 秒あたりの SSL 接続数	10,000
最大同時セッション数（IPv4 または IPv6）	1,000 万
ルーティングテーブルのサイズ（RIB/FIB）（IPv4）	200 万/120 万
IPsec VPN トンネル	4,000

[3] スループット値は UDP パケットおよび RFC2544 テスト方法に基づく
[4] 次世代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 を有効にして測定
[5] 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て測定
[6] 高度な脅威パフォーマンスは、ファイアウォール、アプリケーションセキュリティ、IPS、SecIntel、URL フィルタリング、マルウェア保護を有効にして測定
##TPS メソッド：平均的な HTTP セッションのスループットパフォーマンス
**CPS メソッド：短時間セッション

Juniper Mist WAN Assurance と AI ネイティブ運用

または、SRX4300 ファイアウォールは、Juniper Mist Cloud を通じて運用とオーケストレーションが可能です。Mist AI は、人工知能、機械学習アルゴリズム、データサイエンスの技術を組み合わせて、これまでにない自動化を実現し、時間の節約、IT 生産性の最大化により、デジタルユーザーに最高のエクスペリエンスを提供できます。

Juniper Mist WAN Assurance は、Juniper Mist Cloud 上に構築されており、エンドユーザーのエクスペリエンスに焦点を当てた AI ネイティブのインサイト、自動化された速度テスト、ダイナミックパケットキャプチャ（dPCAP）、異常検知、根本的原因の特定など、ライフサイクル管理と運用をフルで提供します。Day 0 および Day 1 の運用では、WAN Assurance は SRX4300 のオーケストレーション、管理、ZTP も提供します。詳細については、WAN Assurance のデータシートをご覧ください。

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、早期に収益を図ることができます。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。

注文情報

ジュニパーネットワークス SRX シリーズファイアウォールの注文や、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、単なる接続性は優れた接続エクスペリエンスと同じではないと考えています。ジュニパーの AI ネイティブネットワーキングプラットフォームは、AI を活用し、エッジからデータセンター、クラウドにいたるまで、最高かつ安全で持続可能なユーザーエクスペリエンスを実現することを目的に、ゼロから構築されています。詳細については、ジュニパーネットワークス（www.juniper.net/jp/ja）をご覧ください。また、X（Twitter）、LinkedIn、Facebook でジュニパーのフォローをお願いいたします。

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/