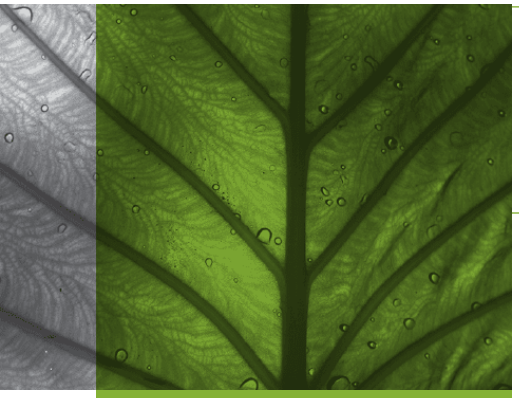

次世代ファイアウォールサービスのデータシート

製品概要

ジュニパーネットワークスでは、クライアントからワークロードにいたるまでの、詳細な制御と可視化を提供する高性能次世代ファイアウォールを複数提供しています。可視化、インテリジェンス、導入は、脅威認識型ネットワークを構成する基本要素です。ジュニパーでは、アプリケーションの識別、ユーザーの識別、ネットワークやアプリケーションの悪用からの保護、マルウェアの検出および防止、暗号化されたトラフィックのインサイト、悪意のあるウェブのブロックなどの URL フィルタリングなど、既知および未知の脅威に対抗するため、さらなるセキュリティを提供しています。

製品説明

労働環境の分散化が進むにつれて、ユーザーが必要な時に、必要なデータやアプリケーションに確実にアクセスできるようにするため、ネットワークエッジのセキュリティがこれまで以上に重要になっています。

リモートワーク環境の安全性を確保するにあたり、クラウドから提供されるセキュリティは十分ではありません。従業員を第一に考え、効率的に業務を行うために必要なデータやアプリケーションにセキュアにアクセスできるようにし、自社の合理化を支援する必要があります。クライアントからワークロードまでの途切れのない可視性、セキュリティアシュアランス、単一のポリシーフレームワークは、リモートワークの安全を確保するために不可欠なツールです。

アクセスによって、企業のリスクが増えることがあってはなりません。企業が直面する脅威の増加に対応しつつ、ユーザーがさまざまなデバイスから新しいアプリケーションにアクセスできる状態を維持するためには、セキュリティを追加する必要があります。Juniper Networks® SRX シリーズファイアウォールは、あらゆる物理的展開、仮想展開、コンテナ展開、as-a-service 展開に、アプリケーション認識、ユーザー ID、コンテンツ検査を備えた統合された次世代ファイアウォール（NGFW）保護サービスを提供します。さらに、SRX シリーズファイアウォールは、侵入防御、SSL 検査、スパム対策、アンチウイルス、URL フィルタリング、未知の脅威の検出も提供しており、一般的なアーキテクチャからさまざまなセキュリティ要件に対応する単一のセキュリティプラットフォームが得られます。

アーキテクチャと主要コンポーネント

SRX シリーズの NGFW サービスアーキテクチャには、絶えず進化する高度なサイバー攻撃から企業や MSP を保護する強力なプラットフォームを提供するため、複数の重要なコンポーネントが含まれています。

ユーザーの識別とアクセス制御：ユーザーファイアウォール

ユーザ識別は、ネットワーク要件のみならず、ビジネスニーズを反映したセキュリティポリシーを管理者が作成できるようにする次世代ファイアウォールのコア要件です。この柔軟性が、IP アドレスではなくユーザー ID に基づいてファイアウォールルールを作成することで、セキュリティポリシーを定義、管理、改良する強力なメカニズムを生み出します。ジュニパーのユーザーファイアウォール機能を通して、SRX はアクティブディレクトリなどのディレクトリサービスと統合することで、トラフィックを特定のユーザーに関連付けることができます。企業は、個々のユーザーまたはユーザーグループに基づいてアプリケーションの使用を許可するようにポリシーを定義することで、よりパワフルながらもシンプルなセキュリティ制御を実現できます。ユーザーファイアウォールでは、セキュリティポリシーをグループの観点から表現することができ、ユーザーがグループに追加されたり削除された場合でも、セキュリティポリシーを引き続き機能させることができます。さらに、IP アドレスの代わりにユーザーレベルでアプリケーショ

ンの使用に関する可視性を提供するため、ネットワークを通過するアプリケーションのトラフィックに関する強力なインサイトが得られます。セキュリティ管理者は、セキュリティポリシーを調整してアプリケーションの利用をセキュリティおよびビジネス上の必要性に合わせて調整することで、脅威のフットプリントを削減することができます。

アプリケーションの識別と制御：AppSecure

従来のポートベースの通信に、アプリケーションを縛り付ける時代はとっくに終わっています。今日の新しいアプリケーションは、ポートやプロトコルを動的に変更するように設計されています。HTTP Web トラフィックなどのサービス上にトンネリングするように設計されているものもあります。つまり、ユーザーが必要なときに、どこからでもアプリケーションを使用できるということです。ユーザーがどこからでもアプリケーションにアクセスできるようにすることで、企業を保護するための従来のネットワーク層の保護を通過して、アプリケーションを直接標的にしようと試みる絶え間なく変化する脅威から保護するという課題が生まれます。

ジュニパーの NGFW サービスは、この課題を満たすだけの十分な機能を備えた強力なセキュリティプラットフォームを提供します。その中核にあるのが AppSecure で、ネットワーク上のアプリケーションに対する強力な可視性と管理性を提供します。

AppSecure はアプリケーションを迅速に認識し、ポート、プロトコルまたは暗号化方法に関係なく、アプリケーション名、サービスの説明、固有のリスクレベルを表面化します。

アプリケーションの詳細な可視化と制御を提供する AppSecure は、場所やデバイスに関係なく、アプリケーションの使用をユーザーに結びつけるコンテキストを提供します。さらに、AppSecure はアプリケーションの動作を理解して脆弱性を特定するため、管理者はリスクのあるアプリケーションが影響を与える前にブロックすることができます。AppSecure は、必要となるディープパケットインスペクションのレベルや、アクセスを許可するユーザーやグループなど、細部にわたるセキュリティポリシーの定義を可能にすることで、アプリケーションに対する脅威フットプリントを軽減します。

アプリケーション層にサービス品質（QoS）を適用し、アプリケーションに基づいてトラフィックを転送し、重要なアプリケーショントラフィックにマルチパスルーティング機能を提供します。

悪用からの保護：侵入検出および防止（IDP/IPS）

ジュニパーの侵入防御システム（IPS）は、ジュニパー SRX と緊密に統合されており、ネットワークやアプリケーションの悪用を軽減し、幅広い攻撃から保護します。ジュニパーの侵入検知システム（IDP）は、新しく発見された脆弱性情報と照らし合わせて新たな脆弱性を常に監視し、最新のサイバー攻撃に対するネットワーク保護を最新の状態に維持しながら、ネットワーク内に侵入を許す前の段階で阻止します。IDP シグネチャは検出専用モードまたはインラインで有効にして、悪意のあるトラフィックを直接ブロックすることができます。

カスタム署名は、既存の署名セットを使用して作成できます。事前に定義済みのポリシーテンプレートを使用するか、カスタムシグネチャに基づいてポリシーを作成し、ネットワークトラフィックを保護し続けることができます。ゾーン、ネットワーク、アプリケーションに基づいて、トラフィックの一部を一致させるポリシールールを定義し、そのトラフィックに対してアクティブまたはパッシブな予防措置を講じることができます。また、攻撃の前後にパケットキャプチャを行い、さらなる分析を行うこともできます。

リアルタイム保護：SecIntel

SecIntel は、ネットワーク全体にあるすべての接続ポイントに検証済みの脅威インテリジェンスを提供することで、悪意あるトラフィックをブロックし、脅威を認識するネットワークを構築します。リスクを軽減するため、SecIntel を SRX に導入して、悪意のある IP アドレスやドメインからの悪意のあるトラフィックを、ディープパケットインスペクションを必要とせずにブロックすることができます。SecIntel の脅威フィードは自動化されており、常時更新されます。さらに、これらのフィードは Juniper Threat Labs によってスクラブされ検証されているため、高い検出効果を維持し、誤った検出を軽減することができます。SecIntel は、ネットワーク上の負荷を軽減するのに役立ちます。

既知の脅威のブロック：ネットワークのマルウェア対策

ランサムウェアやアドウェアなど、複数の攻撃ベクトルから悪意のあるファイルが蔓延しています。これらの脅威は、ネットワークのエンドポイントを危険にさらし、認証情報や個人を特定できる情報（PII）などのデータが盗まれる脆弱性が生まれます。エンドポイントに侵入する前の段階で、ネットワークレベルでマルウェアや不要なファイルを検出してブロックすることは、ユーザー、データ、インフラストラクチャを攻撃から保護するために重要です。クラウドベースのファイルレピュテーションインテリジェンスとマルウェアシグネチャを SRX シリーズ NGFW と組み合わせたマルウェア対策により、軽量かつ高速なセキュリティを実現します。ユーザーやビジネスのスピードを落とすことなく、既知の脅威に対して非常に効果的な境界防御が得られます。NGFW が、軽量かつ高速なセキュリティを実現します。その結果、多くの既知の脅威に対処する非常に効果的な境界防御が完成し、ユーザーやビジネスのスピードが遅くなることもありません。

ブラウジング防御：拡張 Web フィルタリング（EWF）

ユーザーは、半分以上の時間をインターネット閲覧や、Web ベースツールの使用に費やしています。Web トラフィックは、正当かつ安全なものでなければなりません。同時に、オンラインバ

ンキングやヘルスケアなどの特定の Web アプリケーションでは、プライベートを保つ必要があります。EWF を使用することで、管理者は、ギャンブルやマルウェアサイトなどの不要な URL カテゴリをブロックし、選択的な復号化で、トラフィックを脅威から安全に保護することができます。対照的に、ユーザー個人のトラフィックのプライベート性は維持されます。攻撃を軽減するために、EWF には 180 種類以上の URL カテゴリが含まれており、これらのカテゴリは SRX のセキュリティポリシーで使用できます。

暗号化された保護：SSL プロキシー

SSL は、Web サイトを認証し、Web クライアントと Web サーバーの間のトラフィックを暗号化するための汎用的な方法となっています。

SSL コンテンツは暗号化されるため、ユーザーはクライアントエンドポイントにマルウェアを直接ダウンロードすることができてしまいます。企業は、SSL 接続を可視化できないため、自社の企業クライアントに HTTPS を介して送信される脅威を検知することができません。

ジュニパーは、クライアントとサーバーの間の暗号化されたトラフィックの傍受、セッションの終了、宛先への接続の再開を行う強力なアプリケーション レベルの SSL プロキシーを提供しています。企業 LAN 上のユーザーとインターネットへのアクセスの間に位置する SSL「フォワード」プロキシーとして使用でき、クライアント端末を保護します。また、エンタープライズ境界でゲートウェイとして機能することで HTTPS トラフィックを傍受し、暗号化されたトラフィックを終了させます。そこでは、暗号化されていないトラフィックが即座に検査され、セキュリティ チームが設定したセキュリティ ポリシーに準拠しているかどうかが確認されます。その後、トラフィックは、即座にマルウェアをブロックする事前対応型マルウェアエンジンによって処理され、セキュリティ侵害を阻止します。

SSL プロキシは、ユーザーのプライバシー保護のため、特定の URL 間のトラフィックを復号化しないようにする除外項目を含めて設定することができます。除外項目は、ユーザーグループ、URL カテゴリ、またはカスタムカテゴリに基づいて設定できます。SSL プロキシは、ファイアウォールが保護するクライアントと Web サーバーの間にセキュリティを提供します。これは、外部接続と企業内で管理されている Web サーバーの間に設置される SSL「リバース」プロキシと呼ばれることもあります。

未知の脅威：Juniper Advanced Threat Prevention (ATP)

Juniper Advanced Threat Prevention (ATP) は、ジュニパーの脅威インテリジェンスハブであり、機械学習アルゴリズムを使用して完全かつ高度なマルウェア検出と防止を提供します。ATP は、復号化を破らずに、また侵害されたデバイスを表面化させることなく、脅威の検知をサポートします。SRX シリーズファイアウォールと統合することで、ジュニパー ATP は、世界的な脅威データベースを活用して、脅威インテリジェンス、動的マルウェア分析、暗号化されたトラフィックのインサイト、適応型脅威プロファイリングを提供します。ジュニパー ATP は、クラウドベースのサービスとして、またはオンプレミスアプライアンスとして提供されます。

ジュニパー ATP は、トロイの木馬、ワーム、ランサムウェア、ボットネット、IoT 脅威、ドメイン生成アルゴリズム (DGA) 生成ドメインや DNS トンネリングなどの DNS 脅威からの保護を提供します。

特長とメリット

特長	説明	メリット
アプリケーション識別およびポリシーベースの制御	アプリケーション識別 (AppID) では、ポートやプロトコルに関係なくアプリケーションを識別する洗練された分類エンジンを提供します。識別を回避するために回避技術を使用することで知られているものも識別できます。ネットワーク全体のバイト、パケット、セッションに基づいて、アプリケーションのボリュームと使用状況を詳細に分析することができます。アプリケーションの使用状況を追跡してリスクの高いアプリケーションを特定し、トラフィックパターンを分析して、ネットワークの管理と制御を改善します。アプリケーション ファイアウォール (AppFW) は、アプリケーションシグネチャに基づく、ポリシーベースの強化とトラフィックの制御を提供します。	IP アドレスではなく、固有のアプリケーションを識別することで、運用チームがより粒度の細かい制御をできるようにすることで、特定のビジネス要件に合致した企業セキュリティポリシーを適用します。アプリケーションの使用状況を追跡してリスクの高いアプリケーションを特定し、トラフィックパターンを分析して、ネットワークの管理と制御を改善します。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	ジュニパーの豊富な QoS 機能を活用して、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ユーザーに提供します。
高度なポリシーベースのルーティング (APBR)	アプリケーションに基づいてセッションを分類し、設定されたルールを適用してトラフィックの経路を変更します。	異なる WAN リンク上でトラフィックをルーティングし、ビジネスに不可欠なアプリケーションに高い優先度を割り当てる機能を提供します。
ユーザーファイアウォール	アクティブディレクトリなどのディレクトリサービスと統合して、特定のユーザーやグループに関連するファイアウォールポリシーを作成し、セキュリティ保護を強化します。	強力かつ簡素化されたセキュリティ コントロールにより、より正確できめ細かいセキュリティ ポリシーを実現します。
SSL プロキシー	クライアントとサーバーの間でやりとりされる暗号化されたトラフィックを傍受してセッションを中断させ、宛先に向けて接続を再度開始します。クライアント端末を保護するための SSL「フォワード」プロキシとして使用することができます。	暗号化されたトラフィックに隠されたマルウェアを、ユーザーが直接クライアント端末にダウンロードしないように防ぎます。

特長	説明	メリット
侵入検知システム/侵入防御システム（IDS/IPS）	アプリケーション、データベース、オペレーティング システムにおける既知のセキュリティのさまざまな悪用に対する包括的な保護を提供します。	新たに発見された脆弱性と照らし合わせて新しい悪意ある攻撃を常に監視し、最新の攻撃サイバー手法に対してネットワーク保護が最新の状態に保たれるようにします。
Juniper Advanced Threat Prevention	強力な機械学習アルゴリズムを通した高度なマルウェア検出を実施して、これまでに見えなかったセキュリティの脅威を特定するクラウドベースのサービスを提供します。	従来の方法を回避するこれまで発見されなかった未知のマルウェアを正確に特定し、完全な保護を保証します。
SecIntel	攻撃者の IP、C&C、GeoIP、感染したホスト、動的アドレスグループが含まれる脅威フィードを生成します。	Juniper スイッチ、ルーター、ファイアウォールが潜在的な脅威を特定してブロックし、リスクを軽減します。
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が、セッションを復号化することなく、悪意のあるトラフィックをブロックできるようにします。使用される証明書、ネゴシエートされた暗号スイート、接続の動作などを含めた、関連する SSL/TLS 接続データを収集します。 Juniper ATP がこの情報を処理し、ネットワーク動作分析と機械学習を使用し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のポリシーを使用して、悪意ありと判定された暗号化トラフィックをブロックできます。	完全な TLS/SSL 復号化を実行することで大きな負担をかけることなく、暗号化によって失われた可視性を復元します。
適応型脅威プロファイリング	組織は、ネットワーク上で発生するリアルタイムイベントに基づいて、既存のインフラを活用してセキュリティインテリジェンスフィードを構築することができます。各組織に固有のこれらのフィードは、セキュリティポリシーに基づいて設定することができ、ネットワークの他のポリシー適用ポイントで活用して脅威を検出し、リアルタイムでインフラクチャを更新して潜在的な攻撃をブロックすることができます。	リアルタイムで脅威情報を取得し、ネットワーク全体のすべてのポイントにプッシュすることで、脅威への対応時間を改善します。
アンチマルウェア	アンチウイルス、アンチスパム、Web およびコンテンツフィルタリングを通じて、マルウェア、ウイルス、フィッシング攻撃、侵入、スパムおよびその他の脅威から保護します。	リアルタイムのセキュリティ防御を実装して、企業が最新シグネチャを維持し、世界中の脅威を可視化します。
URL フィルタリング	アプリケーションに組み込むことができる Web トラフィックカテゴリを提供します。	Web で発生する脅威や、望ましくない閲覧行為を防ぎます。
Security Director	すべての NGFW を一元的に管理することで、運用を合理化します。	使いやすい GUI によって、複雑なセキュリティ ポリシーの管理と実装を簡素化し、時間を節約し、生産性を向上させます。
Juniper Secure Edge	FWaaS、SWG、DLP を備えた CASB、ZTNA、Advanced Threat Protection を含むフルスタックの SSE 機能を提供し、Web、SaaS、オンプレミスアプリケーションへのアクセスを保護して、ユーザーがどこにいてもセキュリティを提供します。	必要とされている高速で、信頼性の高いセキュアなアクセスで、あらゆる場所にいる従業員を保護します。ジュニパーはお客様の現状を把握して、今あるものを活用し、ゼロトラストの取り組みをクラウド配信型のアーキテクチャに拡張することで、多額のコストをかけたり運用チームに支障をきたすことなく、お客様の望む方向へと導きます。

Juniper Security Director Cloud

Security Director Cloud は、単一の UI で提供されるジュニパーのシンプルかつシームレスな管理エクスペリエンスであり、お客様の現在の導入を将来のアーキテクチャ展開に結び付けます。Juniper Connected Security 戦略は管理を中心としたもので、企業はネットワーク上のあらゆる接続ポイントを保護してユーザー、データ、およびインフラストラクチャを保護することができます。

企業は、オンプレミス、クラウドベース、クラウド配信、ハイブリッドなどの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でアーキテクチャを保護し、エッジからデータセンター、アプリケーションやマイクロサービス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することができます。Security Director Cloud では、企業は途切れることのない可視性、ポリシー構成、管理、収集した脅威インテリジェンスをすべて 1 つの場所から利用できます。

ジュニパーは、お客様が移行のどの段階にいるのであれ要件を満たして、既存の投資を活用できるようにサポートし、Security Director Cloud で移行を自動化することで、お客様のビジネスに最適なペースで、希望するアーキテクチャに移行できるようにします。

Juniper Secure Edge

Juniper Secure Edge は、必要とされている高速で、信頼性の高いセキュアなアクセスで、あらゆる場所にいる従業員を保護します。FWaaS、SWG、DLP を備えた CASB、ZTNA、Advanced Threat Protection を含むフルスタックの SSE 機能を提供し、Web、SaaS、オンプレミスアプリケーションへのアクセスを保護して、ユーザーがどこにいてもセキュリティを提供します。ジュニパーはお客様の現状を把握して、今あるものを活用し、ゼロトラストの取り組みをクラウド配信型のアーキテクチャに拡張することで、多額のコストをかけたり運用チームに支障をきたすことなく、お客様の望む方向へと導きます。

Security Director Cloud によって管理される Juniper Secure Edge では、単一のポリシーフレームワークを採用しており、セキュリティポリシーを一度作成すれば、ユーザー、デバイス、データがどこにいるのであれ同じポリシーを適用することができます。お客様はクラウド配信セキュリティを採用する際に、最初から始める必要はありません。3 回のクリックで完了するウィザードで、既存のキャンパスエッジポリシーを活用して、SSE ポリシーへと簡単に変換することができます。導入モデルに関係なく、単一のポリシーフレームワークを使用するため、Secure Edge では、従来の導入からクラウド配信モデルへと、わずか数回のクリックで既存のセキュリティポリシーを適用することができ、誤設定やリスクを軽減することができます。

保護する対象がリモートユーザーであれ、キャンパスおよび支社/拠点、プライベートクラウド、パブリッククラウド、またはハイブリッドクラウドデータセンターであれ、ジュニパーはすべてのアーキテクチャに統一された管理と途切れることのない可視化を提供します。これにより、運用チームは、現在の投資を SASE などの将来のアーキテクチャ目標へと容易かつ効果的にブリッジできます。お客様は、オンプレミスであれ、クラウド内またはクラウドからであれ、どこからでもセキュリティを管理することができ、あらゆる場所にいるユーザー、デバイス、データに適用されるセキュリティポリシーを、単一の UI から管理することができます。

ユーザーには、必要なデータやリソースへの高速で、信頼性の高いセキュアなアクセスを提供することで、優れたユーザーエクスペリエンスを確保できます。IT セキュリティチームは、既存の投資を活用しながら、ネットワーク全体をシームレスに可視化することができるようになり、自分のペースでクラウド配信アーキテクチャへと移行できます。

Juniper Secure Edge からあらゆる場所のユーザー、デバイス、データに一貫したセキュリティポリシーが提供され、ルールセットをコピーしたり再作成したりする必要がありません。クラウド配信アプリケーション制御、侵入防御、コンテンツおよび Web フィルタリング、効果的な脅威防衛も、可視化やセキュリティの施行を損なうことなく簡単に導入できます。

ジュニパーは、過去 4 年間にわたって、複数のサードパーティ試験で、市場で最も効果的なセキュリティ技術として検証され続けており、すべてのユースケースで 100%のセキュリティ効果を発揮しています。

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、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については、https://www.juniper.net にある**購入方法**ページをご覧ください。

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/

JUNIPER NETWORKS | Driven by Experience™