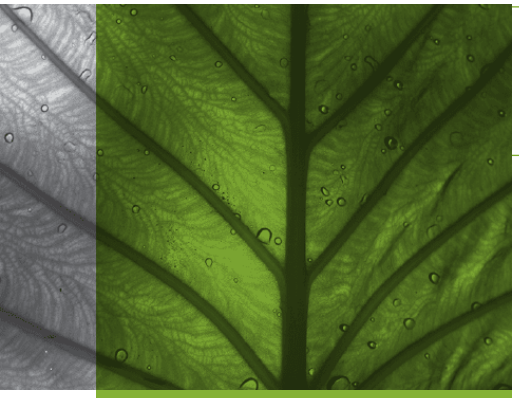

次世代ファイアウォールサービス

製品概要

ジュニパーネットワークスは、クライアントからクラウドまでの細部にわたる管理と可視性を提供する複数のハイパフォーマンス次世代ファイアウォールを提供しています。脅威を認識するネットワークでは、管理と可視化の両方が基本要素となります。ジュニパーは、既知および未知の脅威に対応するために、さらなるセキュリティを提供します。

- *アプリケーション識別*
- *ユーザー識別*
- *ネットワークやアプリケーションの不正利用から保護*
- *マルウェアの検出と防止*
- *悪意あるWebサイトのブロックを含むURLフィルタリング*
- *暗号化されたトラフィックの分析*

製品説明

アプリケーションの使用、ユーザーの行動、ネットワークインフラが絶え間なく変化する中で、企業はますます攻撃の対象となっています。ユーザーは、クラウドでホストされ、さまざまなデバイスで動作する増え続けるアプリケーションにアクセスする必要があります。エンドユーザーにとっては、これらのアプリケーションにシームレスにアクセスできることが不可欠ですが、セキュリティ面も考慮に入れる必要があります。アクセスによって組織のリスクが増えることがあってはなりません。

ユーザによるさまざまなデバイスから行われる新たなアプリケーションへのアクセスを維持しながら、これらの脅威に対抗するためには、さらなるセキュリティが必要です。ジュニパーネットワークス® の SRX シリーズのサービスゲートウェイは、アプリケーション認識、ユーザー識別、コンテンツ検査を備えた統合型次世代ファイアウォール（NGFW）プロテクションサービスを提供します。NGFW の機能に加え、SRX シリーズデバイスは侵入防御、SSL インスペクション、URL フィルタリング、未知の脅威検知も提供し、一般的なアーキテクチャの広範囲のセキュリティ要件に対応する単一のセキュリティ プラットフォームを提供します。

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、企業や MSP を絶え間ないサイバー攻撃から保護するための強力なプラットフォームとなるいくつかの主要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し、セキュリティポリシーを定義、管理および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 シリーズのデバイスは、Active Directory などのディレクトリサービスとの統合を通して、ネットワーク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。ポリシーは、個々のユーザーや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定義することができ、これにより強固でありながらもはるかにシンプルなセキュリティ管理が可能になります。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、ユーザーファイアウォールは、IP アドレスではなくユーザーレベルでアプリケーションの使用状況を可視化し、ネットワークを通過するアプリケーショントラフィックに対するパワフルな洞察力を提供します。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

アプリケーションは、従来のポートに基づく通信にはもはや結び付けられていません。新しいアプリケーションは、ポートやプロトコルが動的に変更されるように設計されています。HTTP Web トラフィックなど、一般的によく使用されている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。ユーザーにとって、これはアプリケーションをいつでもどこからでも使用できることを意味します。企業にとっては、アプリケーションを直接対象とし、従来のネットワークレイヤーの保護を通過するような、絶えず変化する脅威に対する防御を意味します。

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瞬時に認識し、ポート、プロトコル、暗号化方式に関わらず、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可視化します。

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 DPI（Deep Packet Inspection）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。

悪用からの保護：侵入検出と防御（IDP）

ジュニパーの侵入防止システム（IPS）は、Juniper 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緩和し、さまざまな攻撃から保護します。ジュニパーの IDP は、最新の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、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、検出のみまたはインラインモードで有効化し、悪意のあるトラフィックを直接ブロックする事が可能です。

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に、SecIntel を SRX に導入することで、ディープパケットの検査なしに悪意のある IP アドレスやドメインから発生する悪意のあるトラフィックを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、常に更新されています。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 はネットワークの負荷を軽減しながら、よりインテリジェントなセキュリティ保護を提供します。

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の悪意のあるファイルは、依然として複数の攻撃ベクトルから増え続けています。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。マルウェアや望ましくないファイルがエンドポイントに到達する前に、ネットワークレベルで検出してブロックすることが、ユーザー、アプリケーション、そしてインフラを攻撃から守るためには重要です。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 NGFW と組み合わせた SRX シリーズの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。その結果、数多くの既知の脅威に対して非常に効果的な境界防御が実現し、ユーザーやビジネスの速度を低下させることはありません。

ブラウジング防御：拡張 Web フィルタリング（EWF）

ユーザーは、インターネットの閲覧や Web ベースのツールの使用に、時間の半分以上を費やしています。Web トラフィックが、合法的かつ安全であることが重要です。同時に、オンラインバンキングや医療などの一部の Web アプリケーションでは、非公開性を保ち続ける必要があります。EWF では、管理者がギャンブルやマルウェアなどのサイトなど、望ましくない URL カテゴリーをブロックすることができ、ビジネスのトラフィックを脅威から保護するために部分的に復号化を有効にして、ユーザーの個人的なトラフィックの機密性を保つことができます。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。ただし、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端末にマルウェアを直接ダウンロードする可能性があります。組織は SSL 接続を認識していないため、HTTPS を介して自社の企業に送信される脅威を検知する事ができません。

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のゲートウェイとして動作することで HTTPS トラフィックを傍受し、暗号化トラフィックが企業に入る前に、暗号化トラフィックを終端させます。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プロアクティブなマルウェア 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。

ユーザーのプライバシ保護のため、SSL プロキシには特定の URL とのトラフィックが復号化されないように、除外項目を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。

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、高度なマルウェアの完全な検知および防止を実現します。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 シリーズサービスゲートウェイと統合することで、Juniper ATP はグローバル脅威データベースを活用して、脅威インテリジェンス、動的なマルウェア解析、暗号化トラフィックの洞察、適応型脅威プロファイリングを提供します。Juniper ATP は、クラウドベースのサービスまたはオンプレミスアプライアンスとして提供されています。

Juniper 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 の脅威から保護します。

特長とメリット

特長	必要となる Junos OS バージョン	説明	メリット
アプリケーション識別	15.1X49-D200 以上	最先端の分類エンジンを使用し、回避テクニックにより識別を回避することで知られるアプリケーションでも、ポートやプロトコルに関係なく、アプリケーションを正確に識別します。	IP アドレスではなく固有のアプリケーションを特定し、特定のビジネス要件に合わせて企業のセキュリティ ポリシーを適用することで、きめ細かい制御を可能にします。
アプリケーション分析	15.1X49-D100 以上	ネットワーク全体におけるアプリケーション量と使用状況を分析し、アプリケーションごとのバイト数、パケット数及びセッション数といった情報を可視化します。	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。
AppFirewall	18.2R1 以上 (ユニファイドポリシーを使用する場合)	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	18.2R1 以上 (ユニファイドポリシーを使用する場合)	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)	15.1X49-D60 以上	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	12.1X47-D10 以上	Active Directory などのディレクトリ サービスと統合して、特定のユーザーまたはグループに関連付けられたファイアウォール ポリシーを作成し、セキュリティ保護を適用します。	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	15.1X49-D30 以上	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終端し、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。
侵入防御システム (IPS)	15.1X49-D10 以上	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。	このソリューションは、新しく発見された脆弱性の新たな悪用を継続的に監視し、新しいサイバー攻撃方法に対してネットワーク保護を最新の状態に保ちます。

特長	必要となる Junos OS バージョン	説明	メリット
Juniper Advanced Threat Prevention	15.1X49-D80 以上	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。
セキュリティインテリジェンス（SecIntel）	15.1X49-D80 以上	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	20.2R1 以上	SRX シリーズのファイアウォールで、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、SSL/TLS 接続についての関連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 通信の復号による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。
適応型脅威プロファイリング	20.2R1 以上	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。
ネットワークのマルウェア対策	15.1X49-D100 以上（クラウドベース） オンボックス	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り、マルウェア、ウィルス、フィッシング攻撃、侵入、スパム、その他の脅威に対応します。	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	15.1X49-D40 以上	アプリケーションやセキュリティポリシーに組み込むことができる Web トラフィックの分類を提供します。	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	15.1X49-D60 以上	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。

Junos Space Security Director

ジュニパーネットワークス® Junos® Space Security Director は、すべての SRX サービスゲートウェイの一元管理マネージャーです。革新的で直感的で使いやすい Web ベースのインターフェイスを通じて、すべての物理的、論理的、および仮想的なファイアウォールセキュリティポリシー管理を実施する事で、新たな脅威と従来の脅威ベクターに対応したセキュリティを一元的に適用します。アプリケーションのパフォーマンスを詳細に可視化してリスクを低減するだけでなく、ユーザーは何かがおかしいことを「知っている」状態から、問題を解決するために「何かをする」状態に素早く移行することができます。

広範な拡張性、細部にわたるポリシー管理、ネットワーク全体へのポリシー幅を提供する Security Director は、管理者が一元化された Web ベースインターフェイスを介して、ステートフルファイアウォールや NGFW サービス向けのセキュリティポリシーのライフサイクルのすべての段階を管理するのに役立ちます。Security Director は、複数の環境タイプに対応しており、オンプレミスまたはクラウドサービスとして導入することができます。

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 シリーズの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 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、世界をつなぐ製品、ソリューション、サービスを通じて、ネットワークを簡素化します。エンジニアリングのイノベーションにより、クラウド時代のネットワークの制約や複雑さを解消し、お客様とパートナー様の日々直面する困難な課題を解決します。ジュニパーネットワークスは、世界に変革をもたらす知識の共有や人類の進歩のリソースとなるのはネットワークであると考えています。私たちは、ビジネスニーズにあわせた、拡張性の高い、自動化されたセキュアなネットワークを提供するための革新的な方法の創造に取り組んでいます。

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