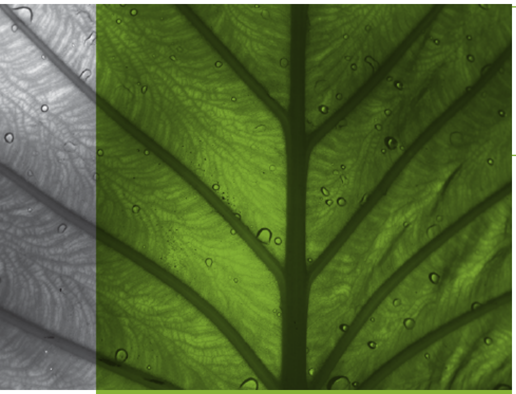

次世代ファイアウォール サービス

製品概要

ジュニパーネットワークスは、アプリケーションの可視化、ユーザー識別、そして詳細なコンテンツ インスペクションを組み合わせた、ハイパフォーマンスな次世代ファイアウォールを提供し、セキュリティ インフラストラクチャをきめ細かく制御できるようにします。

製品説明

アプリケーションの使用方法、ユーザーの行動、ネットワーク インフラストラクチャの絶え間ない変化のために、組織が引き続き広い攻撃対象にさらされる脅威の状況が生じ続けています。ユーザーは、ビジネスのセキュリティに関係なくさまざまなデバイス間で動作するアプリケーションへのアクセス要求を増やすことで、問題の一因を形成しています。

これらの脅威に対処し、異なるデバイス上の新しいアプリケーションへのユーザー アクセスを維持するには、新しいセキュリティ パラダイムが必要になります。Juniper Networks® SRX シリーズ サービス ゲートウェイは、アプリケーション認識、ユーザーの識別、コンテンツ インスペクションを利用して、統合された NGFW（次世代ファイアウォール）の保護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 NGFW サービス アーキテクチャには、企業を継続的な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を提供するいくつかの主要コンポーネントが含まれています。

アプリケーションの識別と制御：AppSecure

最新のアプリケーションは、従来のポートベースの通信に縛られなくなっています。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ことで、または Web トラフィックなどの一般的に使用されるサービスをトンネリングすることで、従来のファイアウォールを回避するように当初から設計されています。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、この課題に対応できる強力なセキュリティ プラットフォームを提供します。コアに置かれる AppSecure は、ネットワーク上で動作するアプリケーションの堅牢な可視化と制御を可能にします。AppSecure は強力なメカニズムを備えており、ポート、プロトコル、暗号化方法に関係なく、ネットワークを通過するアプリケーションの正確なアイデンティティを特定する識別技術を使用して、新しいアプリケーションでも即座に認識できます。

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リンクす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、脆弱性を特定して、アプリケーションによって発生したセキュリティの脅威をそれが損害を与える前に阻止します。

ネットワーク トラフィックが完全に分類されると、アプリケーション、コンテンツ、ユーザーごとにセキュリティ ポリシーを詳細に定義することで、脅威のフットプリントを削減できます。インスタント メッセージング、ピアツーピアのファイル共有、Web メール、ソーシャル ネットワーキング、IP 音声/映像コラボレーションなど、主に個人的なコミュニケーションを目的として設計されたユーザー中心のアプリケーションを、固有のアプリケーションに分類し、エンタープライズによって承認された特定のアクセス権を付与できます。

ユーザー識別：UserFirewall

ユーザー アイデンティティは、ネットワーク要件ではなくビジネス 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。これにより、IP アドレスではなくユーザー アイデンティティに基づいたファイアウォール ルールを定義することで、セキュリティ ポリシーを定義、管理、調整するための強力なメカニズムが形成されます。ジュニパーの UserFirewall 機能を使用して、SRX シリーズ デバイスは、Active Directory などのディレクトリ サービスとの統合によって、特定のユーザーにネットワーク トラフィックを関連付けることができます。ユーザーやグループに基づいてアプリケーションの使用を可能にするポリシーを定義して、より強力ながらシンプルなセキュリティ制御を実現できます。UserFirewall を介して、グループの観点からセキュリティ ポリシーを表現し、ユーザーがグループに追加されたりグループから削除されたりしてもセキュリティ ポリシーを引き続き機能させることができます。さらに、UserFirewall は、アプリケーションの使用状況に対する可視性を IP アドレスではなくユーザー レベルで提供し、ネットワークを通過するアプリケーション トラフィックに関する強力な洞察を提供します。セキュリティ管理者は、セキュリティ ポリシーを調整することで脅威のフットプリントを削減し、セキュリティとビジネスの実践によってアプリケーションの使用状況を調整できます。

攻撃の緩和：侵入防御システム

ジュニパーの IPS（侵入防御システム）はジュニパーの NGFW と密接に統合され、脅威を緩和し、さまざまな攻撃や脆弱性から保護します。Juniper Sky™ Advanced Threat Prevention（Sky ATP）との連携により、既知および未知の脅威に対して包括的な防御を提供し、ゼロデイ攻撃がネットワークに侵入する前に防御します。このソリューションは、最近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。クライアントおよびサーバー システムの脆弱性に対するネットワークから生じる攻撃は、損害が発生する前に直ちにブロックされます。

不明なマルウェア：Juniper Sky ATP

Juniper Sky ATP は、高度なマルウェア防御を提供するクラウドベースのサービスです。Juniper Sky ATP は、SRX シリーズ ファイアウォールとの統合により、変化の激しい脅威に対応する動的なマルウェア対策ソリューションを提供し、強力な機械学習のアルゴリズムを使用して Web と電子メール ファイルを動的に分析するクラウドベースのサービスを提供し、新しい未知のマルウェアを迅速に特定します。判別されると、その決定は SRX シリーズ NGFW に送信されて適用されます。Juniper Sky ATP では、Microsoft（.docx、.xls、.ppt）、pdf、APK（Android Application）を含むすべての主要なファイル タイプがサポートされます。

既知の脅威のブロック：マルウェア防御

複数の攻撃ベクトルからの悪意のあるアクティビティが急増しており、企業の境界は、ネットワークに侵入する前に脅威をブロックするための最初の防御ラインになります。マルウェア防御は、クラウドベースのレピュテーション インテリジェンスと SRX シリーズ NGFW のデバイス ベースの処理能力を組み合わせて、軽量かつ高速の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：悪意のある URL のフィルタリング

スピアー フィッシングは、多くの場合に企業内の重大な侵入につながる、よく使われる攻撃方法です。無防備なユーザーは、高度な持続的攻撃の前提となる悪用ルートキットをインストールする悪意のある URL をクリックすることで、貴重な企業データが盗まれるお膳立てをしてしまいます。攻撃者は一般的に人気のある Web サイトを侵害し、ユーザーが無意識にユーザー パスワードを提供するように仕向けます。ジュニパーの URL フィルタリング モジュールは常にリアルタイムで更新されており、世界中で絶えず発見されている悪質な URL の最新のデータベースを提供し、ユーザーの侵害を防止します。

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、ユーザーはエンド クライアント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に対して盲目的になります。

ジュニパーは、クライアントとサーバーの間に置かれて、暗号化トラフィックの傍受、セッションの終了、エンド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、エンド クライアントを保護します。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エンタープライズに入る前に、暗号化トラフィックを終了させます。その時点では、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。

特長とメリット

成果物	成果物の説明	メリット
AppSecure	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。
User-Firewall	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。
侵入防御システム（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。	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。
Juniper Sky ATP	これまで検出されなかったセキュリティ上の脅威を特定する強力な機械学習アルゴリズムによって、洗練された高度なマルウェア検知を提供するクラウドベースのサンドボックス サービスです。	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。
アンチマルウェア フィルタリング	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、その他の脅威に備えています。	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できるようにします。
Junos Space 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。

SRX シリーズ プラットフォームのサポート

表 2 に、NGFW サービスをサポートする SRX シリーズ プラットフォームの詳細と、必要な Junos の最小リリースを示します。

表 2：次世代ファイアウォール サービスのサポート

プラットフォーム	サポートされる Junos リリース
SRX300 シリーズ	15.1X49-D100 以降
SRX550	15.1X49-D100 以降
SRX1500	15.1X49-D100 以降
SRX4000 シリーズ	15.1X49-D100 以降
SRX5000 シリーズ	15.1X49-D100 以降
vSRX	15.1X49-D100 以降

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、高性能なサービス分野のリーダー的存在であり、高性能ネットワークの高速化、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、ネットワークへの投資から早期に利益を得ることができます。また、ネットワークを最適化することで、必要な性能レベルや信頼性、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/jp/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、www.juniper.net 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、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、お客様およびパートナーの皆様が日々直面してい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

Engineering
Simplicity

Copyright 2019 Juniper Networks, Inc. All rights reserved. Juniper Networks、Juniper Networks ロゴ、Juniper、Junos は、米国およびその他の国における Juniper Networks, Inc. の登録商標です。その他すべての商標、サービス マーク、登録商標、登録サービス マークは、各所有者に所有権があります。ジュニパーネットワークスは、本資料の記載内容に誤りがあった場合、一切責任を負いません。ジュニパーネットワークスは、本発行物を予告なく変更、修正、転載、または改訂する権利を有します。