Policy Enforcer

製品概要

ジュニパーの Software-Defined Secure Network（SDSN）プラットフォームは、境界ファイアウォールだけでなくネットワーク全体を活用し、脅威の検知とセキュリティ維持を行います。Junos Space Security Director の Policy Enforcer コンポーネントは、ジュニパーのクラウドベース マルウェア検出ソリューション「Sky Advanced Threat Prevention」によって作成されたポリシーをオーケストレーションし、EX シリーズ、QFX シリーズ スイッチやジュニパーの仮想および物理 SRX シリーズ ファイアウォールに配信する機能を持っています。

製品説明

最近コーポレート ネットワークが次々と攻撃を受けていることから、従来の「境界のみ」のセキュリティ アーキテクチャの欠点が明らかになってきました。こうしたセキュリティ アーキテクチャでは完全で包括的な防御を実現するには不十分であることが分かってきたのです。境界のみのソリューションが不十分である理由はいくつかあります。

- 境界の内側で受けた攻撃はブロック不可能であるため、境界内の単一のアプリケーションのブリーチによってネットワーク全体が脆弱になる。
- ネットワークは内部攻撃に対して完全に脆弱である。
- 組織内の内部がラテラル攻撃を受けても、境界デバイスの可視化やインテリジェンスでは悪意のあるアクティビティがまったく検知できない。可視化がなければ、セキュリティ チームは効果的にネットワークをセキュアに維持することが不可能である。
- 境界ベースの制御はアプリケーションから遠すぎるため、マルウェアに感染したことが分かっているラップトップやサーバーを効果的に隔離またはブロックすることが不可能である。境界のみのアクティビティを隔離またはブロックしても north-south トラフィックしかブロックできず、east-west トラフィックは存在し続ける。

ジュニパーネットワークス Software-Defined Secure Network は、これらのセキュリティ上の課題に対処する包括的なアプローチを提供します。ジュニパーネットワークスの SDSN が提供する具体的な機能は以下のとおりです。

- **広範囲のセキュリティ：**ジュニパーの SDSN は、スイッチ、ルーター、セキュリティ デバイス（物理および仮想）を使用して、ネットワーク全体の広範囲なセキュリティをオンプレミス環境に提供します。その際、ジュニパーネットワークス Contrail などの SDN ソリューションを活用し、将来的にアプリケーションをクラウドでホストする場合など、必要に応じて、ネットワーク機能のオーケストレーションをすることができます。また各ネットワーク要素は、セキュリティ センサーとして動作可能であり、イントラネットおよび内部ネットワーク通信に可視化とインテリジェンスを提供します。
- **ユーザー インテントベース ポリシー:**ユーザー グループや位置情報、デバイス、サイト、テナント、アプリケーション、脅威などビジネス向けの項目をベースとするシンプルなポリシー フレームワークであるこのソリューションは、データやリソースを共有したり、ネットワーク内の修復操作をオーケストレーションしたりすることでスイッチ、ルーター、ファイアウォール、その他のネットワーク デバイスを連携させることが可能です。
- **脅威インテリジェンスの集約：**ジュニパーの SDSN は、複数のローカルからの情報（セキュリティ情報およびイベント管理など）、クラウドベース（Sky Advanced Threat Prevention など）、そしてサードパーティー製の脅威検知ソリューションからの情報を集約する能力があります。

Junos® Space Security Director のコンポーネントである Policy Enforcer は、よりシンプルなユーザー インテントベースの脅威管理ポリシーの修正および配信ツールであり、ジュニパーネットワークス EX シリーズ イーサネット スイッチ、QFX シリーズ スイッチ、そしてジュニパーの仮想および物理 SRX シリーズに配備されるポリシーの更新が可能です。

アーキテクチャと主要コンポーネント

セキュリティ強化ネットワーク

Policy Enforcer は、境界ファイアウォールを含む Secure Network と呼ばれる抽象化機能を持っています。また、アプリケーションとユーザーを繋ぐスイッチにもなります。Secure Network は、支社やその場所に配備されているセキュリティおよびネットワーキング デバイスなどの特定位置の表示、ネットワーク アクティビティの検知、特定されたポリシーの強制を実行するコヒーレント システムとして動作します。Policy Enforcement Groups と呼ばれる追加の抽象化機能は、ユーザーやアプリケーションなどの企業体やサポート ネットワーク全体内の独立ユーザー インテント志向のポリシーを表示します。

高度な脅威防止

ジュニパーのクラウドベース Sky Advanced Threat Prevention ソリューションは、複数の脅威フィードを提供します。例えば、

- コマンド アンド コントロール（C&C）- 既知の悪意のあるコマンドやコントロール サイトを特定する
- Geo IP - インターネット上の異なる組織の位置情報を取得する
- マルウェア - 既知のマルウェア脅威を特定する
- 感染したホスト - 高度な機械学習技術に基づいて感染した内部ホストのリストを提供する

Policy Enforcer は Sky Advanced Threat Prevention とネイティブに統合しており、セキュリティ ワークフローをオーケストレーションして境界のトラフィック保護とネットワーク内の脅威伝搬の阻止を行います。また、脅威の重大度に応じて自動修正アクションを実行するための細かい制御が可能なセキュリティ オペレータを搭載。トラフィックの拒否や記録などの境界ファイアウォール関連アクションや、感染したホストの隔離などのネットワーク関連アクションを実行することができます。

感染したホストの追跡

境界のみの防御アーキテクチャの場合、感染エンドポイントが移動すると IP アドレスが変わるため、セキュリティが簡単に回避されてしまいます。Policy Enforcer なら、ユーザーの移動にともなってエンドポイント IP アドレスが再割り当てされても移動前後のホストの動きを追跡し続けるコヒーレント システムを提供するので、攻撃者はセキュリティ ポリシーの回避が難しくなります。

カスタム脅威フィード管理

政府や金融、小売、その他のセキュリティに敏感なお客様はさまざまなソースからのカスタム脅威フィードに登録し、絶えず変化する脅威状況に対応しています。加えて、Security Information and Event Management（SIEM）、ハニーポット、その他のセキュリティ分析ソリューションがセキュリティ チーム脅威フィードを提供しています。Policy Enforcer は、セキュリティ強化ネットワーク全体で関連制御を実行する際に、これらのカスタム フィードを利用可能な RESTful API を公開します。

特長とメリット

表 1：Policy Enforcer の特長とメリット

特長	説明	メリット
トラフィック ブロッキング	Sky Advanced Threat Prevention によって供給される脅威の情報に基づいてトラフィックをブロックします。	感染した組織のトラフィックをブロックするだけでなく、ネットワーク内の脅威のラテラル ムーブメントを隔離して阻止するなど、ネットワーク志向のアクションを実行することができます。
感染したホストの追跡	ユーザーやアプリケーションの機動力によるネットワーク アイデンティティ関連問題の変更に対処します。	内在するネットワーク アイデンティティ（IP アドレスなど）が感染したホストのために変更する場合に、組織のために一貫性のあるセキュア ポリシーを強制します。セキュリティ強化ネットワークは、感染したホストの動作をネットワーク全体で追跡し、セキュリティ制御を回避しようとする動きを特定します。
カスタム脅威フィード	自動インシデント応答のためにカスタム / サードパーティー製の脅威フィードを SDSN フレームに統合します。	顧客の既存投資を信頼されるサードパーティー製の脅威フィードに活用し、ジュニパーのソリューションを使用して制御を強制します。
ダッシュボードの監視	脅威関連のダッシュボードを提供して、ネットワーク全体の脅威の位置を簡単に特定します。	お客様はネットワークに侵入している脅威と感染したエンドポイントをいつでも明確に見ることができます。
RESTful APIs による自動化	自動化ツールと一緒に使用可能な RESTful API が提供されます。	物理、論理、仮想の SRX シリーズ デバイスの構成および管理、EX シリーズのセキュリティ機能、QFX シリーズ スイッチを自動化します。

仕様

サポートされるブラウザー

Security Director は次のブラウザーで最適に表示されます。

- Google Chrome v.33.x 以上
- Internet Explorer v.10.x 以上
- Firefox v.30.x 以上
- Safari v.7.x 以上

VMware のバージョン

Junos Space は VMware vSphere 4.0 以上と連携します。

Junos OS ソフトウェア

SRX シリーズ サービス ゲートウェイは Junos OS ソフトウェアで動作します。Junos Space Security Director は、Junos OS 10.3 以降のリリースを実行しているジュニパーのデバイス上で動作します。

Junos Space ネットワーク管理プラットフォーム

Junos Space Security Director 16.1 は Junos Space 16.1 で動作します。

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、高性能なサービス分野のリーダーであり、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。当社のサービスを利用することで、コストを削減し、リスクを最小限に抑えながら、生産性を最大限高め、より高速なネットワークを構築し、価値を高めることができます。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、卓越した運用を保証します。詳細については、www.juniper.net/jp/jp/products-services/ をご覧ください。

Policy Enforcer

Policy Enforcer ソフトウェアは、Secure Network で管理するネットワーキングおよびセキュリティ デバイスの数に基づいてライセンスが必要です。たとえば、最大 20 台の SRX シリーズ ファイアウォール、80 台の EX シリーズ スイッチを管理する場合、JS-SDSN-PO-100 のライセンスを 1 つ購入する必要があります。注：高可用性（HA）用に別途ライセンスを購入する必要はありません。

製品番号	説明
SDSN-PO-50	デバイス 50 台の Policy Enforcer ライセンス
SDSN-PO-100	デバイス 100 台の Policy Enforcer ライセンス
SDSN-PO-500	デバイス 500 台の Policy Enforcer ライセンス
SDSN-PO-1000	デバイス 1,000 台の Policy Enforcer ライセンス

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、ネットワークの経済性を一新する製品やソリューション、サービスを提供することで現状の課題に挑戦しています。当社のチームは顧客やパートナーと協力してイノベーションを促進し、拡張性とセキュリティに優れた自動ネットワークを開発して、俊敏性、パフォーマンス、価値を提供しています。詳細な情報は、ジュニパーネットワークスを参照するか、Twitter や Facebook からジュニパーにお問い合わせください。

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話：888.JUNIPER（888.586.4737）
または +1.408.745.2000
FAX：+1.408.745.2100
www.juniper.net

アジアパシフィック、ヨーロッパ、中東、アフリカ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話：+31.0.207.125.700
FAX：+31.0.207.125.701

ジュニパーネットワークスのソリューションの購入については、03-5333-7410 にお電話いただくか、認定リセラーにお問い合わせください。

1000602-001-JP 2016 年 10 月