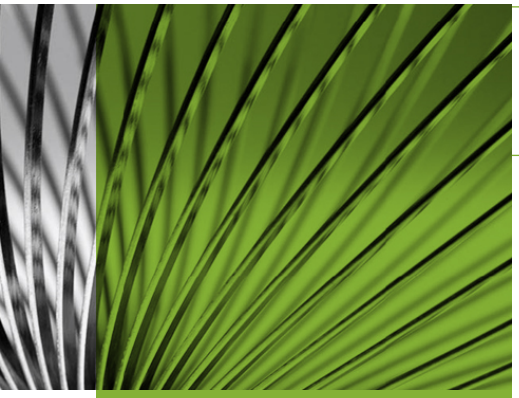

POLICY ENFORCER

製品概要

Juniper Connected Security 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脅威の検知とセキュリティの強化の領域として活用します。Junos Space Security Director のコンポーネントである Policy Enforcer は、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、EX シリーズおよび QFX シリーズスイッチ、MX シリーズルーター、サードパーティのスイッチと無線ネットワーク、Contrail や VMware NSX などのプライベートクラウド/ SDN ソリューション、およびパブリッククラウド導入において、脅威の修復とマイクロセグメンテーションのポリシーを実施します。Juniper ATP Cloud のクラウドベースのマルウェア検知、コマンドアンドコントロール、GeoIP 識別フィードと、信頼できるカスタムフィードは、Policy Enforcer の脅威検知メカニズムとして機能し、修復ワークフローをオーケストレーションします。

製品説明

企業ネットワークへの攻撃によって、従来の「境界線のみ」のセキュリティアーキテクチャの欠点を露呈し、完全かつ全体的な保護を提供するには不十分であることが証明されました。境界のみに対するソリューションが不適切である主な理由としてはいくつかあげられます。

- 境界内のアプリケーションやエンドポイントが 1 つでも侵害されると、境界内の攻撃はブロックできないため、ネットワーク全体が脆弱な状態になります。
- ネットワークは、インサイダー攻撃に対して非常に脆弱です。マルウェアに感染したエンドポイントは、ネットワーク接続元で隔離し、横方向の攻撃伝播の可能性を制限することが最適です。
- 内部攻撃が企業内で横方向に動き始めると、境界デバイスからの可視性とインテリジェンスでは、悪意のある活動の証拠が得られません。この可視性がなければ、セキュリティチームがネットワークを効果的に保護することはできません。

Juniper Networks® Connected Security は、これらのセキュリティ上の懸念に対応する包括的なアプローチを提供します。Juniper Connected Security が提供する具体的な機能は次のとおりです。

- **死角のないセキュリティ**：ジュニパーの Connected Security は、ネットワーク全体にわたる死角のないセキュリティを実現します。オンプレミスでは、物理スイッチおよび仮想スイッチの両方、ルーター、セキュリティデバイスをサポートし、ジュニパーネットワークスの Contrail や VMware NSX などの SDN ソリューションを活用して、必要に応じてネットワーク機能をオーケストレーションし、Amazon Web Services（AWS）や Microsoft Azure などのパブリッククラウドプラットフォームでホストされるアプリケーションと連動させます。また、各ネットワーク要素がセキュリティセンサーとして機能し、ネットワーク内およびネットワーク間の通信を可視化し、インテリジェンスを提供します。
- **ポリシーのオーケストレーション**：ユーザー、ユーザーグループ、地理的な位置、デバイス、サイト、テナント、アプリケーション、脅威などのビジネス指向の項目に基づいたシンプルなポリシーのフレームワークのソリューションで、スイッチ、ルーター、ファイアウォールおよびその他のネットワークデバイスがデータやリソースを共有しながら連携し、ネットワーク内で修復アクションをオーケストレーションできます。
- **SecIntel**：Juniper Connected Security は、複数のローカル（セキュリティ情報やイベント管理など）、クラウドベース（Juniper ATP Cloud など）、さらにはサードパーティの脅威検知ソリューションからの脅威情報を集約する機能を提供します。

Junos® Space Security Director のコンポーネントである Policy Enforcer は、より分かりやすく、ユーザーの意図に基づいた脅威管理ポリシーの修正および配布ツールとなります。ジュニパーネットワークスの EX シリーズイーサネットスイッチや QFX シリーズスイッチ、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、更新したポリシーを展開できます。

アーキテクチャと主要コンポーネント

Policy Enforcer を備えることで、情報セキュリティはセキュリティソフトウェアによって制御および管理されます。他のソリューションのように IP アドレスを特定するのではなく、新しいデバイスが自動的にセキュリティポリシーの対象となります。このようなソフトウェアを定義する環境は、すでに導入されているセキュリティポリシーや制御に影響を与えることなく移動することができます。その他のメリットは次のとおりです。

- **向上した、より詳細にわたるセキュリティ**：ネットワークアクティビティの可視性を高めることで、複数のソースからの脅威インテリジェンスを活用し、サイバー脅威やその他のセキュリティインシデントをより迅速に検知し、対応することができます。
- **拡張性とコスト削減**：ソフトウェアベースのモデルにより、 購入と維持にコストがかかるハードウェアを追加または削減することなく、当面のニーズに応じて迅速かつ容易にセキュリティを拡大または縮小することができます。
- **よりシンプルなソリューション**：ハードウェアセキュリティアーキテクチャは、サーバーや特殊な物理デバイスが必要となるため、複雑なものになることがあります。ソフトウェアモデルでは、セキュリティはポリシーに基づいています。Policy Enforcer は、物理的な場所に関係なく、どこにいても情報を保護します。

特長とメリット

表 1. Policy Enforcer の特徴とメリット

特長	説明	メリット
感染したホストのブロック	SecIntel を通じて Juniper ATP Cloud から提供される脅威情報に基づき、トラフィックをブロックします	お客様は、境界ファイアウォールで感染したエンティティからのトラフィックをブロックするだけでなく、隔離などのネットワーク指向のアクションを取ることで、ネットワーク内部での脅威の横方向への動きを抑制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モビリティによって発生する、ネットワーク ID に関連したよくある課題の変化に対応します	感染したホストの基盤となるネットワーク ID (IP アドレスなど) が変更された場合でも、エンティティに対して一貫したセキュリティポリシーを実施します。セキュアネットワークがネットワーク全体の感染ホストの動きを追跡し、セキュリティ制御を回避しようとする試みを特定します。
カスタム脅威フィード	カスタム/サードパーティの脅威フィードを Connected Security フレームワークに統合し、自動化されたインシデントレスポンスを実現します	感染したホストの基盤となるネットワーク ID (IP アドレスなど) が変更された場合でも、エンティティに対して一貫したセキュリティポリシーを実施します。セキュアネットワークがネットワーク全体の感染ホストの動きを追跡し、セキュリティ制御を回避しようとする試みを特定します。
メタデータベースの動的なアクセス制御ポリシー	プライベートクラウドやパブリッククラウドの展開で一般的な俊敏なワークロードを可能にするクラウド対応ポリシーモデルを提供します	オンプレミスだけでなく、異なるクラウドの導入にも対応した一貫したセキュリティポリシーモデルを実装し、ドメインごとに異なるルールセットを維持するために必要となる運用コストを削減します。
プライベートクラウド展開向けのマイクロセグメンテーション	VMware NSX および Juniper Contrail SDN プラットフォームと統合し、プライベートクラウドのワークロードをセグメント化します	Juniper Contrail および VMware NSX プラットフォームとの統合により、プライベートクラウド上のアプリケーションのワークロードをきめ細かくセグメント化し、高度なセキュリティを提供します。
パブリックおよびプライベートクラウドのワークロードとメタデータの検出	クラウド固有のメタデータを含む動的なクラウドのワークロードを検出します	俊敏で動的なワークロードであっても、ファイアウォール上で最新のポリシーを提供し、クラウドワークロードのセキュリティをサポートするために必要となる時間を短縮します。
プライベートおよびパブリッククラウドの導入における脅威の緩和	AWS、Google Cloud、Microsoft Azure、VMware、KVM、Hyper-V、Juniper Contrail クラウドプラットフォームと統合し、マルチクラウドでの脅威修復を実現します	感染したアプリケーションのコンポーネントを、アプリケーションが動作している場所であればどこでも特定し、ネットワーク内部での脅威の横方向への伝搬を抑制します。
DDoS の緩和	Juniper MX シリーズルーターと統合します	MX シリーズルーターの BGP Flowspec を更新し、トラフィックをスクラビングセンターに転送したり、ネットワーク内の被害を受けたホストにトラフィックが到達しないようにブロックしたりして、アクティブな DDoS 攻撃を緩和します。
ダッシュボードの監視	ネットワーク全体の脅威の状況を容易に把握できる、脅威に関するダッシュボードを提供します	お客様は、ネットワークに侵入する脅威や感染したエンドポイントをいつでも確認することができます。
自動化向けの RESTful API	自動化ツールと組み合わせて使用する RESTful API を提供します	物理、論理および仮想 SRX シリーズデバイスの設定と管理と、EX シリーズと QFX シリーズスイッチのセキュリティ機能を自動化します。

仕様

表 2 は、Policy Enforcer の最新リリースで、Juniper ATP Cloud を通じて提供され、さまざまな Juniper SRX シリーズファイアウォールでサポートされている Juniper SecIntel 脅威フィードの概要を示しています。

表 2. SRX シリーズデバイスでサポートされる Juniper SecIntel 脅威フィード

モデル/プラットフォーム	サポートされている脅威フィード
vSRX：2 VCPU、4 GB RAM（サーバー要件）	CC、アンチマルウェア、感染ホスト、GEO IP
SRX4100、SRX4200	
SRX4600	
SRX340, SRX345, SRX380, SRX550M, SRX1500	
SRX5400、SRX5600、SRX5800	
SRX300、SRX320 CC	CC、GEO IP

同様に、表 3 に示すように、他の Juniper EX シリーズおよび QFX シリーズスイッチプラットフォームでも、さまざまな Policy Enforcer の導入がサポートされています。

表 3. EX シリーズおよび QFX シリーズデバイスでサポートされている Policy Enforcer 導入モード

モデル	サポートされる Policy Enforcer モード
EX2200、EX3300、EX4200、EX4300、EX9200、EX2300、EX3400、QFX5100、QFX5200、vQFX	PE を使用する Juniper ATP クラウド（ファブリックの一部）

Policy Enforcer は、表 4 に示すように、サードパーティのスイッチプラットフォームに接続されたエンドポイントでの脅威の修復をサポートしています。

表 4. サポートされているサードパーティスイッチプラットフォーム*

モデル	サポートされる Policy Enforcer モード
Cisco ISE	PE を使用する ATP クラウド（ファブリックの一部）
HP Aruba Clearpass	
Forescout CounterAct	

* NAC ソリューションの機能に基づく一部のスイッチおよび無線デバイス。

Policy Enforcer と VMware NSX との統合には、表 5 に記載されている以下のコンポーネントが必要です。

表 5. VMware NSX サポート

モデル	サポートされる Policy Enforcer モード
VMware NSX	vSRX を使用したマイクロセグメンテーションと脅威の修復
VMware vCenter および ESXi	
vSRX バージョン	

Policy Enforcer と Juniper Contrail との統合には、表 6 に記載されている以下のコンポーネントが必要です。

表 6. Juniper Contrail サポート

モデル	サポートされる Policy Enforcer モード
Juniper Contrail	vSRX を使用したマイクロセグメンテーションと脅威の修復
vSRX バージョン	

パブリッククラウド向け Policy Enforcer には、表 7 に記載されている以下のコンポーネントが必要です。

表 7. AWS サポート

モデル	サポートされる Policy Enforcer モード
vSRX バージョン	ワークロードディスカバリに基づく vSRX ポリシー

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、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、www.juniper.net/jp/ja/products-services をご覧ください。

注文情報

Junos Space アプライアンス

Junos Space バーチャルアプライアンスには、Junos OS オペレーティングシステムだけでなく、Junos Space ソフトウェアパッケージ一式が含まれています。アプライアンスを展開するためには、ユーザーが仮想マシンを作成する必要があります。バーチャルマシンの推奨仕様は、物理アプライアンスの仕様と同等です。www.juniper.net/documentation/product/en_US/security-director を参照してください。ご注文情報については、ジュニパーの営業担当者にお問い合わせください。

Policy Enforcer

Policy Enforcer ソフトウェアは、セキュアなネットワークで管理するネットワークとセキュリティデバイスの数に基づいてライセンスされます。例えば、管理するデバイスが SRX シリーズのファイアウォール 20 台、EX シリーズのスイッチ 80 台までの場合は、SDSN-PE-100 を 1 ライセンス購入することになります。AWS の場合、vSRX をゲートウェイとして活用する各 VPC に対して、脅威の修復とワークロードの検出シナリオに対応するため、vSRX 用と VPC 自体の 2 つのデバイス単位が使用されます。

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。ご注文情報については、ジュニパーの営業担当者にお問い合わせください。

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、ネットワークを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
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