APAC Cohesion Connected Security (CSEC)

SmartWall TDD 11.5 および Juniper Secure Edge のセキュリティアップデート

Tech Roundup Q4-2022

ジュニパーネットワークス株式会社

JUNIPER NETWORKS | Driven by Experience™

Agenda

- ジュニパーのセキュリティ戦略
- TDD 11.5 の新機能
  - PTX サポート
  - “絨毯爆撃” 攻撃からの保護
  - サービスポータル可視化の強化
  - ライセンス/パッケージの更新
- ジュニパーセキュアエッジ (JSE) の更新

デジタルの世界は変化している

進化するアーキテクチャの回復力とスケーラビリティ

現在 1 つの組織は平均して 2.6 のパブリッククラウドと 2.7 のプライベートクラウドを使用しています。

どこからでもすべてにアクセス

労働者の 75% が週に2~3日以上、自宅で仕事をすることになります。

サイバー攻撃の成功率が急増

企業の 63% が侵害され、ゼロデイエクスプロイトの使用は 2021 年に2倍以上になりました。

ネットワークは高度に分散されより複雑になっています

IT エグゼクティブの 75% は、自社のネットワークが複雑すぎて「懸念される」リスクがあると述べています。

Juniper Connected Security

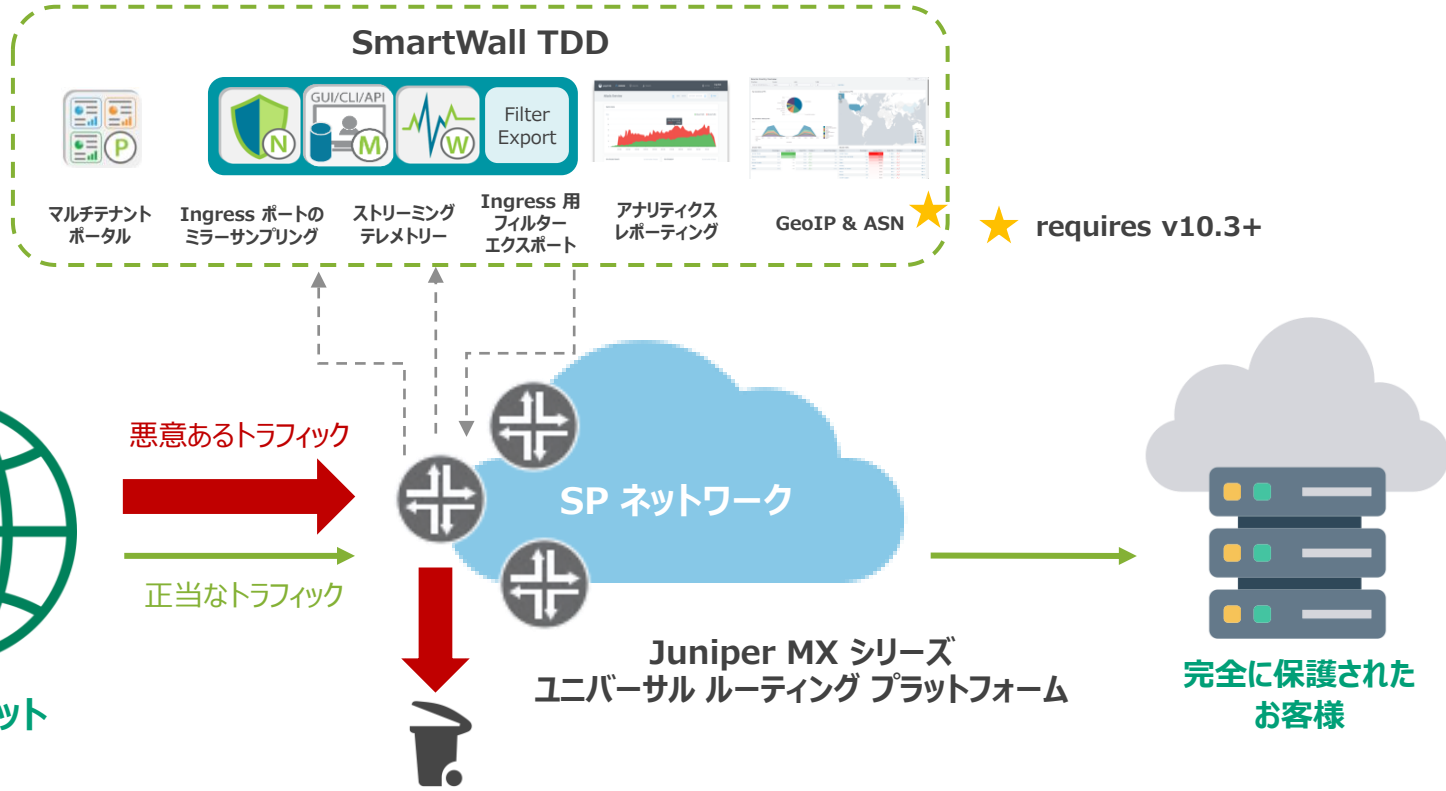
クライアントからワークロードまで、どこでも、どんな場所でも

ユーザー, **アプリケーション** および **インフラストラクチャ**
すべての接続ポイントを安全に保護

SmartWall TDD

50 G から 40 Terabits まで拡張可能な 10-20 秒以下の DDoS 防御を実現

- **MX シリーズと PTX シリーズの統合**
- **ミラートラフィックの継続的な監視**
- **数分ではなく、10-20 秒未満で検出し軽減**
- **Juniper Trio ASIC ベースのペイロードマッチング***



継続的な監視

・ネットワークエッジに展開された Juniper MX
・メトロ、ピアリングポイント、SP、クラウドコアにおける Juniper PTX[1]
・サンプルミラーを介し Ingress トラフィックを監視
・ミラーサンプルとストリーミングテレメトリーを Corero SmartWall TDD に転送

リアルタイム検出

・Corero TDD は、Juniper MX および PTX ルーターからのフィード 内のすべてのパケットを検査
・TDD は大量の DDoS 攻撃を数秒以内に自動的に検出

ラインレートの軽減と可視性

・TDD はファイアウォールフィルタを自動的に生成し、NETCONF を介して MX と PTX を構成して DDoS パケットをブロック
・TDD は Splunk を利用した分析により、攻撃前・攻撃中・攻撃後にわたって包括的な可視性を提供

* Trio chip set is specific to the MX Series routers

1 PTX support as of TDD v11.5+ with EVO based PTX devices

Juniper MX/PTX Joint DDoS Protection Solution

目的

Why – DDoS 攻撃の脅威の排除に努め、MX/PTX のお客様にさらなる価値を提供し、競争力を強化

How – ネットワークのエッジで動作する最新の技術を使って、リアルタイムで自動化された保護を提供

What – Juniper MX/PTX + TDD

従来のアプローチ

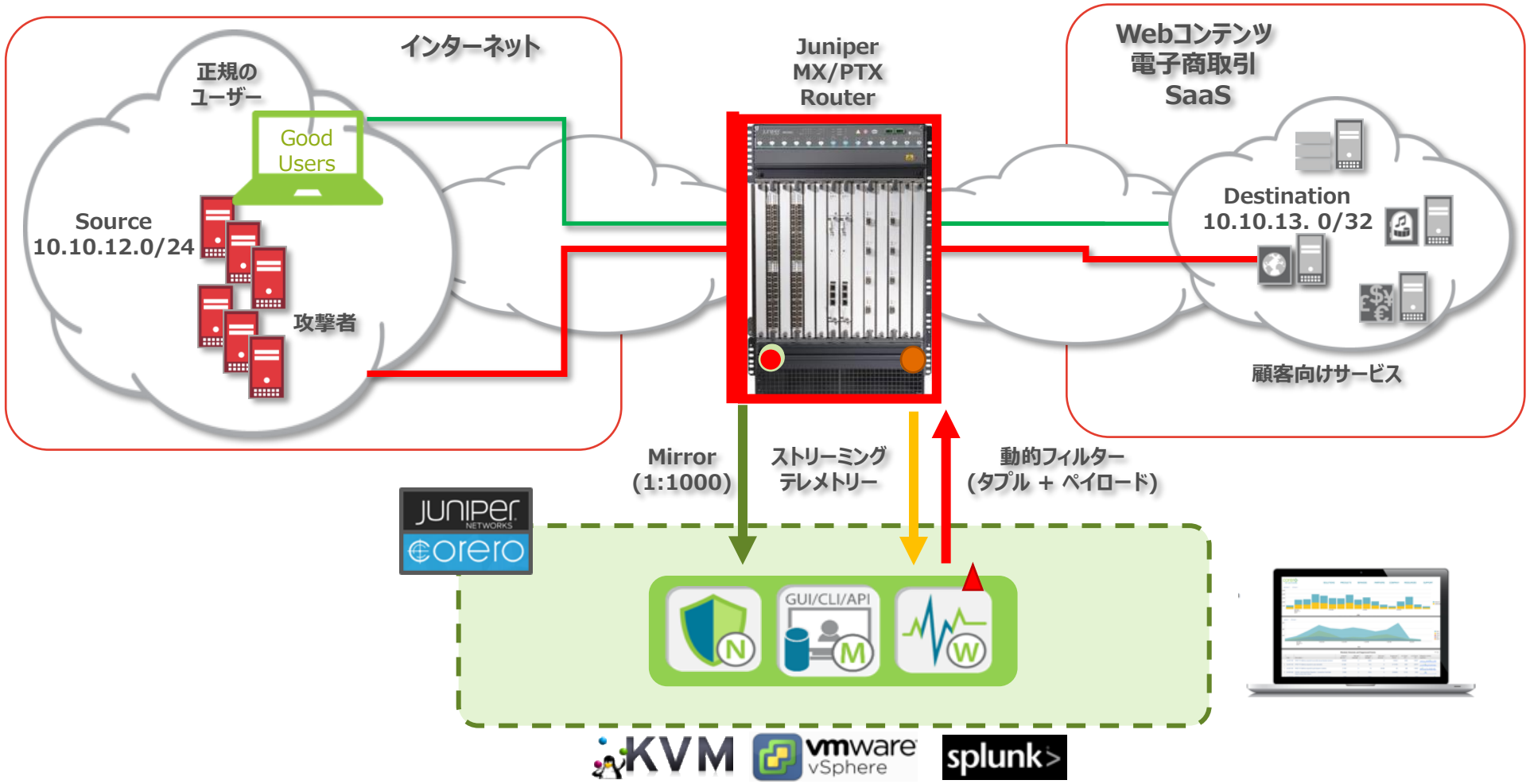
- Netflow や Flowspec といった時代遅れの技術やプロトコル
- 自動化されていない
- リアルタイムではない
- 数分間のサービス停止
- ネットワーク全体で悪意のあるトラフィックを転送
- 手動による介入
- 偽陽性率が高い
- コストが高い

最新のアプローチ: Juniper MX/PTX + TDD

- 最新技術 DPI、ソフトウェアドリブン
- エッジで攻撃を阻止
- 完全に自動化され、不良パケットを数秒で停止
- 瞬時のテレメトリと分析
- 誤検知ゼロ
- 効率的なコスト
- セルフサービスポータルとマルチテナンシーをサポート

Juniper Joint DDoS Solution (MX + TDD)

自動化ワークフロー　– その仕組み



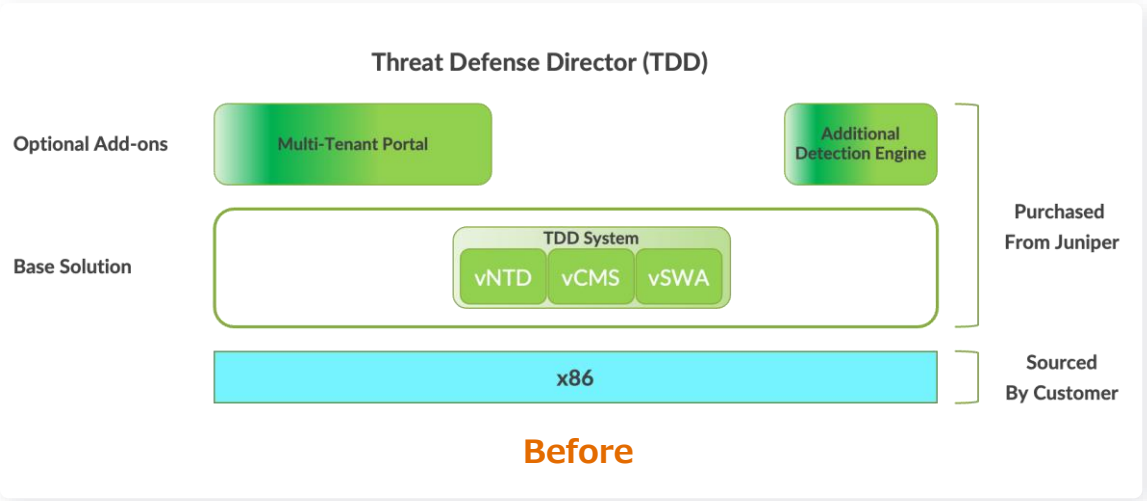
SMARTWALL TDD 11.5

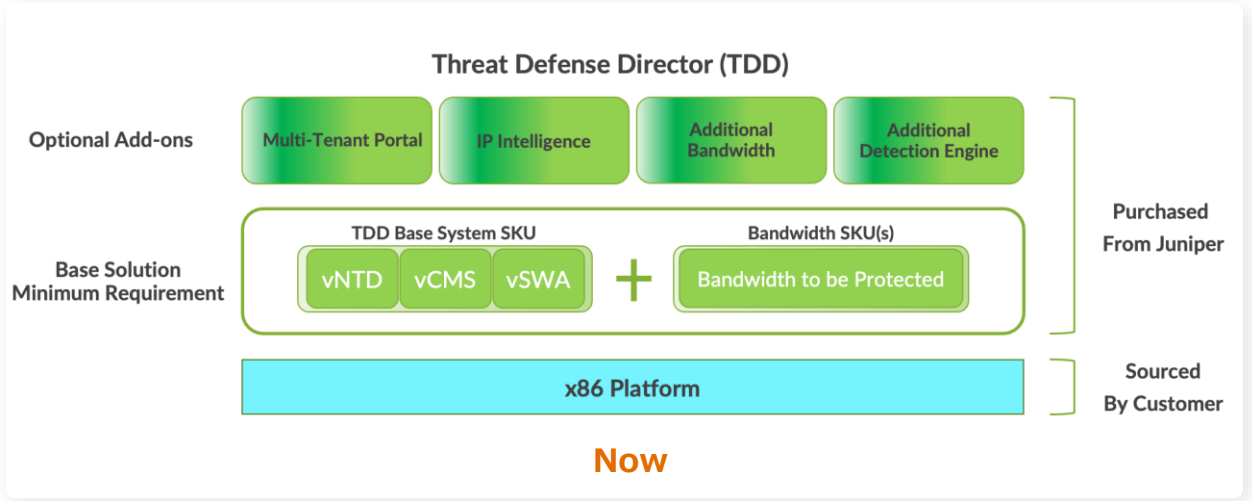
新着情報

JUNIPER NETWORKS

SmartWall TDD 11.5 Packaging Updates

パッケージの更新





新着情報：

- ✓新しい 50G 帯域幅（BW）オプション（現在、50G、100G、200G、500G、1T、10T、40T の BW 部分が利用可能）
- ✓TDD ベースシステムと帯域幅を別々に購入できるようになりました。
- ✓お客様は必要に応じて帯域を追加することが可能
- ✓マルチテナントポータルは、テナントの「シート」単位で購入できるようになりました。100、500、1000、2500 から最大 10K まで。
- ✓攻撃元の国（GeoIP）および攻撃元のネットワーク（ASN）の可視化
- ✓3 年間 10%、5 年間 15% のインセンティブを新たに設定

SmartWall TDD with MX Series

MX304

MX204

MX240, MX480, MX960

MX2008, MX2010, MX2020

MX10003, MX10008, MX10016

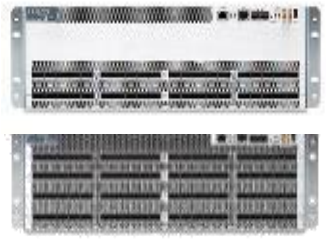
Supported with all System Packages on these MX Series routers

SmartWall TDD with PTX Series

Express 3 (ZX)

Express 4 (BT)

Junos EVO ベースの PTX モデル



PTX10003

PTX10003-80C-AC/DC
PTX10003-160C-AC/DC

PTX10001-36MR

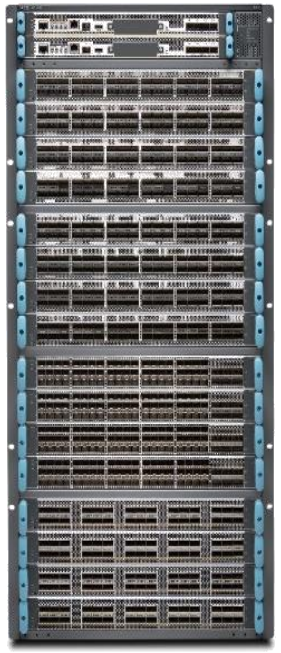
PTX10001-36MR-AC/DC
PTX10001-36MRLAC/LDC
PTX10001-36MR-AC-T

PTX10004

PTX10004-BASE3
PTX10004-PREM2
PTX10004-PREM3

PTX10008

PTX10008-BASE3
PTX10008-PREM2
PTX10008-PREM3

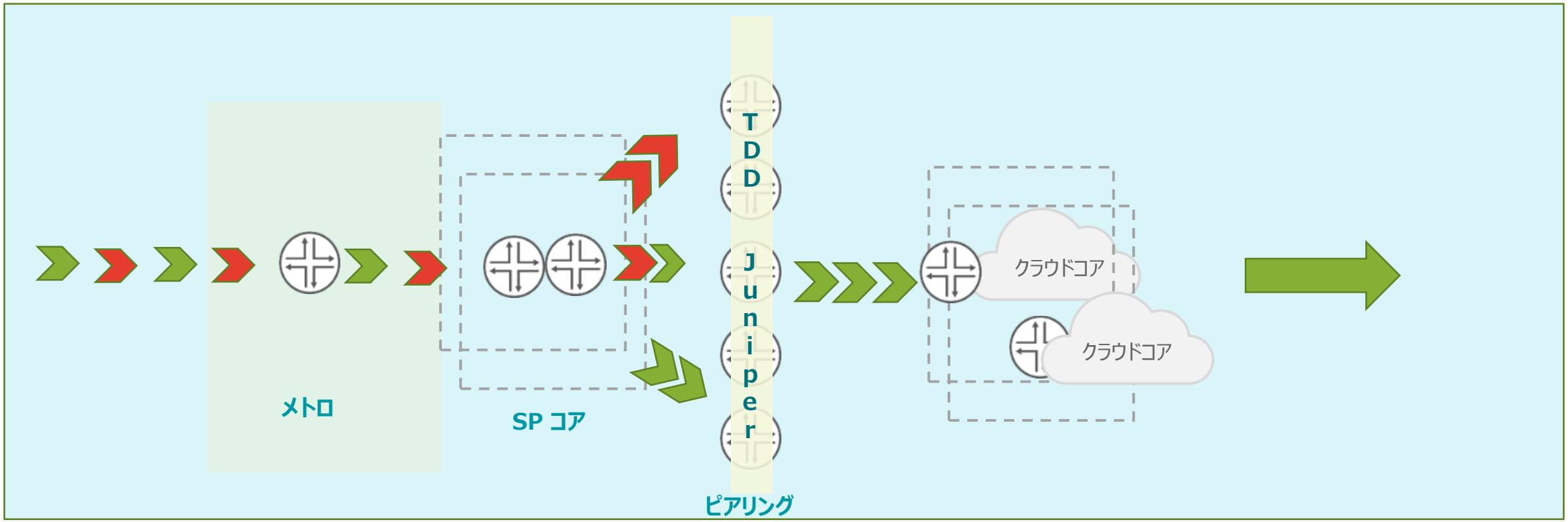


PTX10016

PTX10016-BASE3
PTX10016-PREM2
PTX10016-PREM3

SmartWall TDD 11.5 – PTX シリーズへのプラットフォーム対応を拡大

ピアリングサイトを保護する *TDD* 対応の *PTX*



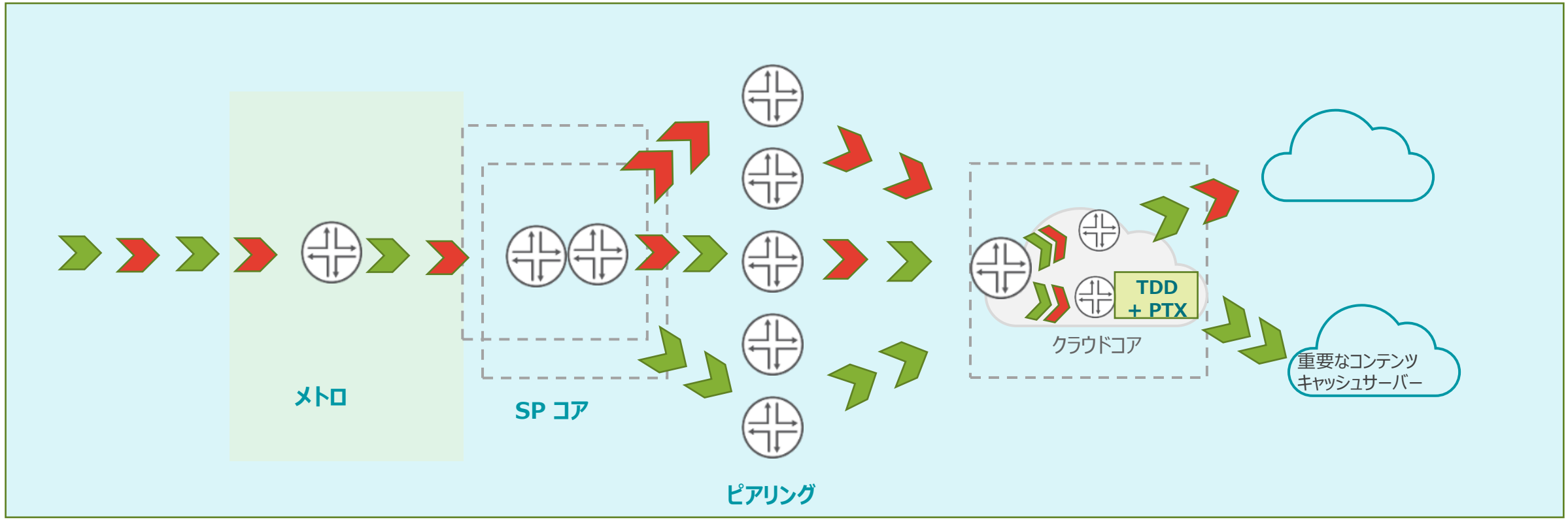
混合 Ingress トラフィック

DDoS を提供するPTX/TDD
保護 & 軽減

軽減された Egress トラフィック

SmartWall TDD 11.5 – PTX シリーズへのプラットフォーム対応を拡大

重要なコンテンツキャッシュサーバーを保護する *TDD* 対応の *PTX*



クラウドコアに到達する
混合 Ingress トラフィック

PTX/TDD による DDoS 対策
特定のトラフィックに対する
防御と緩和の提供

意図したクラウドへの有効な
Egressトラフィック

SmartWall TDD 11.5: 新機能

PTXシリーズへプラットフォーム対応機種を拡大	• ジュニパーコネクテッドセキュリティは、接続のあらゆるポイントにセキュリティを拡張するものです • MXシリーズの「Joint DDoS」ソリューションは、その有効性が実証されています。 • 今回、同じ実績のあるソリューションを PTX シリーズに拡張することで、選択肢が増え、より包括的な保護が可能になります • 特に、重要なコンテンツ・キャッシュ・サーバーやデータセンターの相互接続用ピアリングサイトを DDoS 攻撃から保護するなどの用途に適しています
「絨毯爆撃」攻撃からの自動保護	• 近年、複数の宛先 IP にまたがる「絨毯爆撃」的な DDoS 攻撃が急増しています • 従来のソリューションは、単一の宛先 IP への攻撃を想定して構築されていたため、これらの攻撃を検知、緩和することは困難であり、見逃してしまう可能性が高い • 最新のソリューションでは、サブネットレベルで、サブネット内の複数の宛先 IP を同時に、かつ自動的に監視および保護する必要があります • 手動分析による従来のアプローチでは時間がかかりすぎる　ダウンタイム ＝ $$$ の損失
サービスポータルの強化された可視性	• サービスポータルにより、プロバイダーは DDoS Protection as a Service を提供可能 ・攻撃/緩和 -フィルタまたは BGP/イベント/テナント別チャート/サービスレベル • GTP-U の認識、モバイルオペレーターにリアルタイムで詳細なトラフィック洞察を提供 • 国およびネットワーク自律システム番号による攻撃のソース

SmartWall TDD 11.5: “絨毯爆撃”からの自動保護

複数の宛先 IP に分散して攻撃されるケースが増加

(“絨毯爆撃” “サブネット” “スペクトラム拡散” 攻撃として知られることが多い)

- 利用可能なツールセットにより、サイバー犯罪者がそのような攻撃を容易に生成できるようになった
- 従来の保護機能は、単一の宛先 IP への攻撃を想定して構築されていた
- 複数の宛先 IP やサブネット全体に対する攻撃は見落とされる可能性が高い

効果的な保護には迅速な対応が必要 - 自動化が重要

- TDD の次世代有効性モデルでは、すべての DIP（宛先IPアドレス）ベースのルールに、以下の保護機能が追加されました
- カスタム定義とフラグメントは、サブネットの認識としきい値を持つようになりました

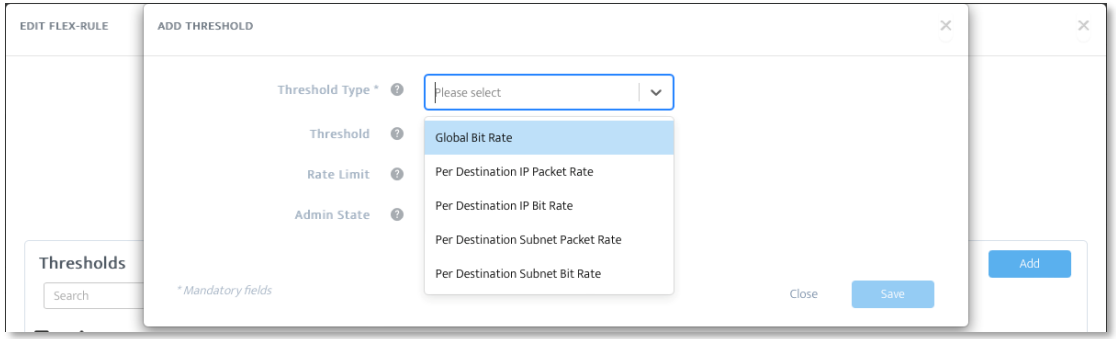
SmartWall TDD 11.5: “絨毯爆撃”からの自動保護

カスタムルールは、特定の保護機能を外科的な精度で提供します

- システムデフォルトの Flex-Rule BPF-フィルタは、DDoS パケットをより正確にブロックすることができます

Flex-Rules には、強化された宛先追跡が追加されました

- 宛先 IP に依存しない攻撃フィルタが追加されました
- 個々の IP、サブネット、またはグローバルにマッチしたパケットレートに基づいてルールをトリガすることができます
- 新しい/新興のベクターに対するルールを作成し、永続的に適用することが可能です



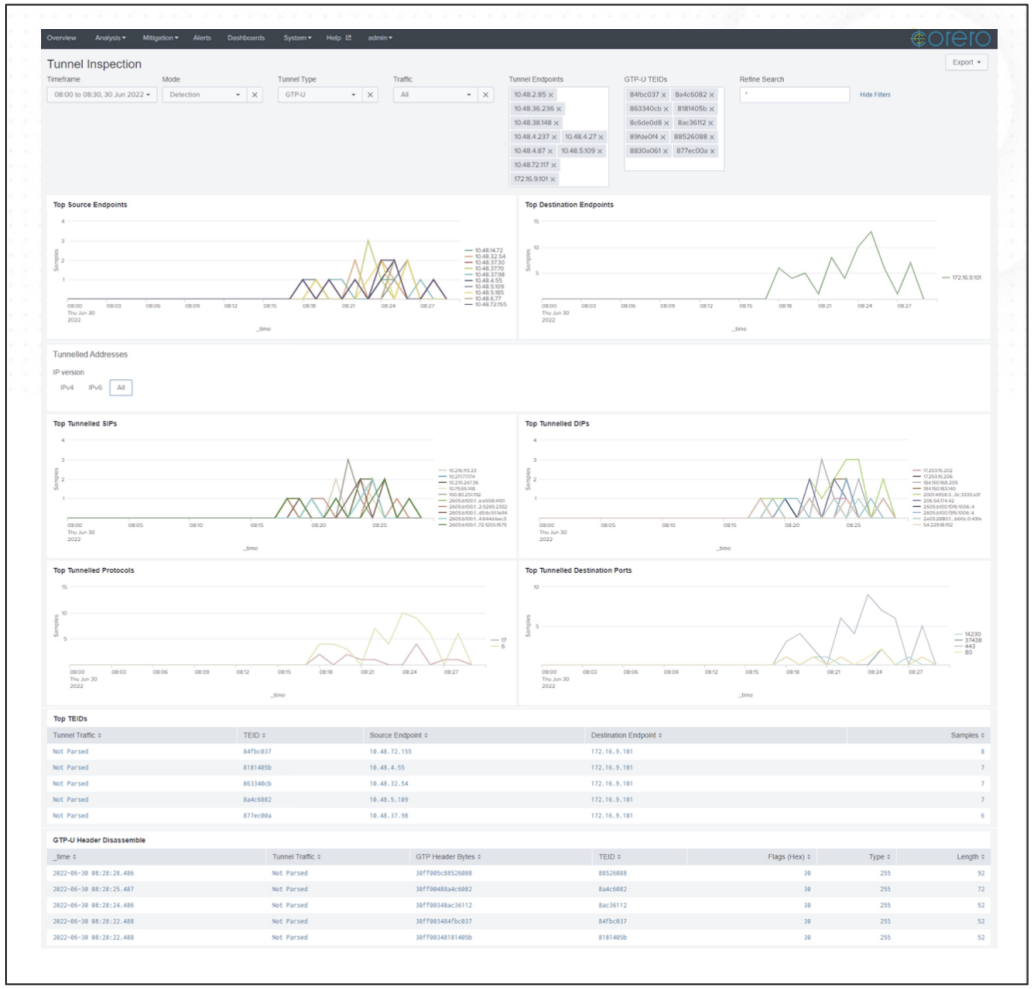
SmartWall TDD 11.5: サービスポータルの強化された可視性

サービスポータルにより、プロバイダーはDDoS Protection as a Service を提供することができます

- 攻撃/緩和 -フィルタまたは BGP/イベント/テナント別チャート/サービスレベル

GTP-U の認識により、モバイルオペレーターにリアルタイムで詳細なトラフィックインサイトを提供します

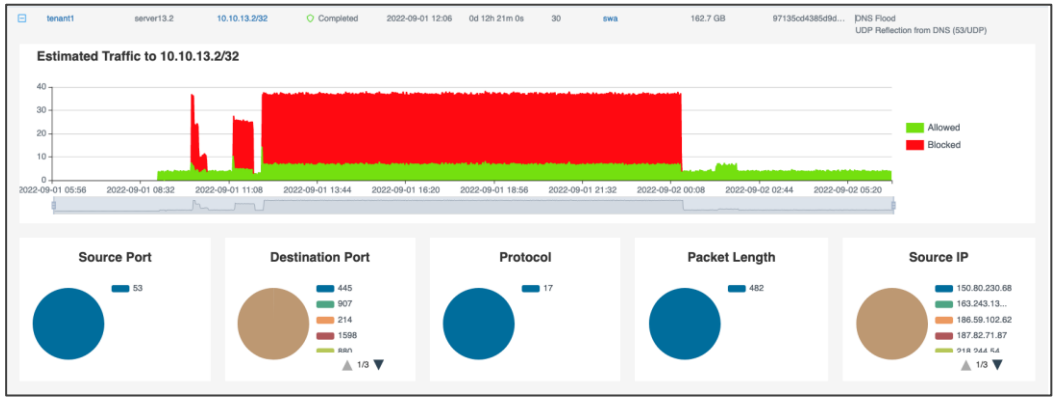
国およびネットワーク自律システム番号による攻撃のソース



SmartWall TDD 11.5: 新機能

TDD 11.5 では、TDD 製品群に有用な新機能が追加されました：

- ✓ JunOS EVO 22.3 以降で **PTX に対応**
- ✓ **Carpet Bomb**（別名：絨毯爆撃）攻撃**対策**
- ✓ **Service Portal 2.0 の統合**により、レポート、攻撃分類、トラフィック処理の区別が改善されました
- ✓ **TCP ACP SmartRule** の機能強化
- ✓ 混乱を減らすため、TDS のみの機能を TDD のお客様には非表示にしました
- ✓ TDD ユーザー向けの新しいデフォルトポリシー既定設定
- ✓ 新規インストール時のデフォルトの TDD Attack Alert の追加
- ✓ **GTP-U ダッシュボード** の改善
- ✓ 複数の改善と修正



セキュアアクセス サービスエッジ（SASE）とは何ですか?

JUNIPER NETWORKS

SASE が取り組むべき課題とは?

分散した従業員に必要なアプリとデータへの優れたアクセスを提供

会社のユーザーとリソースを保護

どこから接続しているかに関係なく、ユーザーとリソースを攻撃から保護

運用チームはどこでも完全な可視性と制御が可能に ― 例外はありません

お客様の SASE アーキテクチャーが…

最適なパスを提供し、ネットワークがそれ自体を最適化できたら

どこからでもユーザー アクセスを保護し、会社のリソースを保護できたら

統一された可視性とポリシー管理をすべて単一の UI 内で提供できたら

ビジネスに最適なペースでクラウド型セキュリティ に移行できたら

ジュニパーセキュアエッジの概要

主な機能

安全なアクセス制御:
- ウェブ
- クラウド
- プライベートアプリ
- データセンタ

脅威の防止

データセキュリティ

セキュリティ監視

コアサービス

Firewall as a Service

セキュア Web ゲートウェイ

クラウドアクセスセキュリティブローカー（CASB）

データ損失防止

高度な脅威対策

ゼロトラストネットワークアクセス

施行

クラウドサービス経由のインライン:
- オンプレミスデバイス
- エージェント

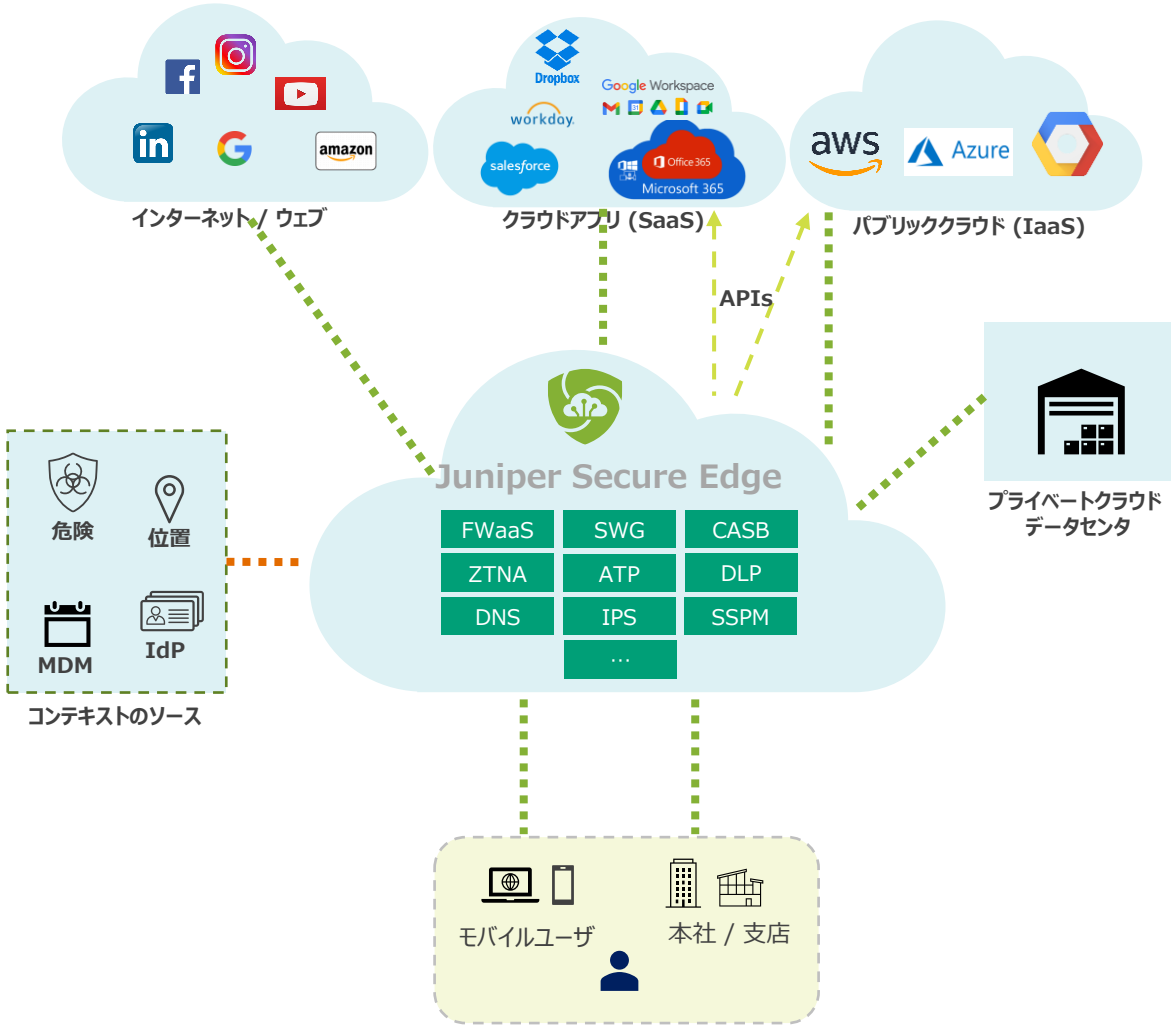
帯域外 (APIs)
- SaaS
- IaaS
- …

出展: Gartner MQ for Security Service Edge, 2022 年 4 月

ジュニパーセキュアエッジ

ジュニパーセキュアエッジの概要

クラウドで実現するセキュリティ



可視性

- オンプレミスとクラウドを完全に可視化する Security Director Cloud
- 許可された、または許可されていない クラウドアプリケーション、SaaS の状態、…

アクセス コントロール

- インラインおよびアウトオブバンドの エンフォースメント
- 統一されたポリシー
  - 環境: オンプレミス (SRX)、 クラウド (Secure Edge、ATP)
  - サービス FWaaS、SWG、IPS など

脅威防止

- ATP クラウドと完全に統合
- 脅威のフィード
- DNS セキュリティ、サンドボックス、 暗号化トラフィックインサイト

データ保護

- 移動中および静止中のデータ用
- コンテンツフィルタリング
- DLP
- クラウドデータディスカバリー

THANK YOU

Juniper Networks | Driven by Experience™