エンタープライズ セキュリティを パブリック クラウドとハイブリッド クラウドに拡張

ジュニパー セキュリティ – 絶え間なく進化する市場に対応

課題

エンタープライズ環境は急速な勢いでパブリック クラウドあるいはハイブリッド クラウドの導入へと移行しています。それに伴い、セキュリティ レベルを従来のネットワークから新しいクラウド ランドスケープへと拡張することが急務となっています。

ソリューション

物理および仮想ファイアウォールの幅広いポートフォリオ、単一画面での一元管理、そして脅威対策インテリジェンスをジュニパーネットワークスは提供します。シンプルでありながら包括的な保護メカニズムを絶え間なく進化する市場へ提供することにより、物理データ センター、プライベート クラウド、さらにはパブリック クラウドのセキュリティをシームレスに強化したい企業を支援します。

メリット

- 投資保護、TCO（総所有コスト）の削減、および学習コストの削減によって、設備投資と運用コストの大幅な削減を実現
- パブリック クラウドおよびハイブリッド クラウド全体のセキュリティ強化と監視を、シンプルかつ直感的な管理によって実現
- 物理データ センターで使用されるセキュリティ ポリシーと技術を、パブリック クラウド、ハイブリッド クラウドに拡張
- 導入および管理しなければならない、プロプライエタリで機能が制限されたパブリック クラウド エレメントの数を削減

パブリック クラウドへの移行は急速に拡大しています。Gartner は、パブリック クラウドのグローバル市場は 2016 年には 2040 億ドルに達すると予想しています。この急速な普及の主な要因は、柔軟性、拡張性、シンプルさ、そして従量課金モデルと低額の初期コストといった、パブリッククラウドの能力があらゆる地域間で導入可能であることと考えられます。ただし、プライベート データ センターに莫大な投資を行い、パブリック クラウドのセキュリティについて懸念を持つ企業は、ハイブリッドなアプローチを支持し、パブリック クラウドと既存の物理データ センターおよびプライベート クラウドの組み合わせを採用する傾向があります。しかし、クラウドへの移行は、今までとは異なるリスク モデルを生み出しており、組織のネットワークを確実に保護するためには、そのリスクに対応する必要があります。

課題

欠点が 1 つもない新技術は存在しません。これはクラウドについても言えることです。データがオンプレミスのファイアウォールの内側だけに存在するのではなくなった現在、パブリックおよびハイブリッド クラウドの世界では、考慮すべき新たなリスクが出現しています。

例えば、Amazon Web Services（AWS）は、57% のマーケットシェアを誇る、最も人気の高いパブリック クラウド プラットフォームですが、シンプルな IP レベルまたはポート レベルの制限アプローチを各インスタンス レベルで採用しています。しかし、これは、ネットワークおよびセキュリティ管理者が必要とし、物理環境で使用しているきめ細かな制御や高度なセキュリティ機能からはほど遠いものです。

パブリック クラウド

パブリック クラウドの飛躍の原動力となってきたものは、大部分において、ダイナミックかつ現実的な新興企業の存在です。今日、多くの新興企業や小規模企業にとって、専門の管理スタッフを配した物理データ センターを導入することは経済的に見て割が合いません。その代わりに彼らが選択するのは、定評のあるクラウド プラットフォームです。インフラストラクチャを導入し、従来のネットワーク セキュリティチームの代わりに、DevOps 担当者を採用します。

DevOps の担当者たちは開発と運用の経験を豊富に有していますが、セキュリティの専門知識は持っていません。彼らが期待されているのは、高いスクリプティングのスキルであり、通常、ソフトウェア ビルド マネージメントといった役割も任されます。ネットワーク セキュリティは職務のほんのごく一部にすぎないため、DevOps 担当者たちは、自ら構成し、監視し、更新できるようなシンプルなセキュリティ ソリューションを必要としています。Chef や Puppet などのインフラストラクチャ自動化プラットフォームの台頭により、プログラマビリティは DevOps チームにとって最大の関心事項となりつつあり、あらゆるセキュリティ プラットフォームにとって必須事項となってきています。

ハイブリッド クラウド

クラウドへ移行したいという意欲はあっても、これまで物理データ センターに莫大な投資を行ってきた企業の場合は、パブリッククラウドによる柔軟性と経済性を利用できるからです。これまで以上の管理を行う必要がありますが、パブリック クラウドの柔軟性と経済性の両方を確保できるからです。また、企業によっては、特定のデータをオンプレミスで保管することが義務付けられている場合もあります。ハイブリッドなアプローチでは、極めてセンシティブなデータはプライベート データ センターに保管し、それ以外のデータをすべてクラウドにオフロードすることができます。

しかし、ハイブリッド クラウドへの移行には、課題も付きまといます。新しいセキュリティーポリシーを設定する必要があるだけでなく、管理に伴う追加費用、物理データセンタとパブリッククラウドの違いなどを確認する必要があります。また、クラウドの専門家を採用したり、既存の職員向けにクラウド セキュリティのトレーニングを実施することによる、追加の時間や費用も必要になります。

ジュニパーネットワークスのパブリック クラウドとハイブリッド クラウド セキュリティ ソリューション

ジュニパーネットワークスでは、パブリックおよびハイブリッド クラウド環境のセキュリティを強化するためにそれぞれが連動する幅広い製品ポートフォリオを提供しています。このソリューションの主なコンポーネントは次のとおりです。

- 統合型の次世代機器と統合脅威管理（UTM）を搭載したジュニパーネットワークス® SRX シリーズ サービス ゲートウェイとジュニパーネットワークス vSRX 仮想ファイアウォール。以下の機能を備えています。
  - コアファイアウォール機能に加え、IPsec VPN や、NAT、ルーティングなどのネットワークサービスの豊富な実装
  - ネットワーク侵入を検知し、ブロックする侵入防御システム（IPS）2.0
  - ユーザーベースファイアウォールにより、ユーザーの役割とグループに応じてアクセスコントロールを行い、分析とログを出力
  - 統合型のジュニパーネットワークス AppSecure 2.0 によるアプリケーション コントロールと可視化。アプリケーションを安全に有効化するために、アプリケーション レベルの分析、優先度の設定、およびブロッキングを提供
  - ウィルス、スパム、悪意のある URL とコンテンツから保護するための、統合脅威管理（UTM）機能によるアンチウィルス、アンチスパム、Web およびコンテンツ フィルタリング
  - vSRX の Linux KVM、VMware、AWS プラットフォームのサポート
- Spotlight Secure 脅威インテリジェンスや Sky Advanced Threat Prevention (Sky ATP) によるクラウド内のセキュリティインテリジェンス
- Spotlight Secure 脅威インテリジェンスは、複数のソースから脅威フィードを集約することにより、SRX シリーズ ファイアウォールに対して、オープンかつ統合された、即座に使用可能なインテリジェンスを提供します。複数のインテリジェンス ソースを通じて攻撃パターンを学習し、その知識を SRX シリーズや vSRX 仮想ファイアウォールと共有して、脅威検知や高度なマルウェア制御を即座に行うためのオープンプラットフォームを提供します。
- Sky ATP は、巧妙なマルウェアから保護するための動的分析（サンドボックス）を採用したクラウドベースの高度なマルウェア対策サービスです。SRX シリーズおよび vSRX 仮想ファイアウォールと統合することにより、機械学習による検知の精度を高め、修復の時間を短縮します。
- ジュニパーネットワークスの Junos® Space Security Director は、単一画面管理を通じて一元化され、セキュリティ機能ならびにすべての SRX シリーズ、vSRX 仮想ファイアウォール間の導入、監視、構成を行います。Security Director には、詳細情報や脅威マップ、イベントログが表示されるカスタマイズ可能なダッシュボードが用意されており、かつてないレベルの可視化をネットワーク セキュリティにもたらします。Security Director は、Google の Android や Apple の iOS システムなどのモバイルアプリとしても利用でき、リモート モバイル監視も可能です。

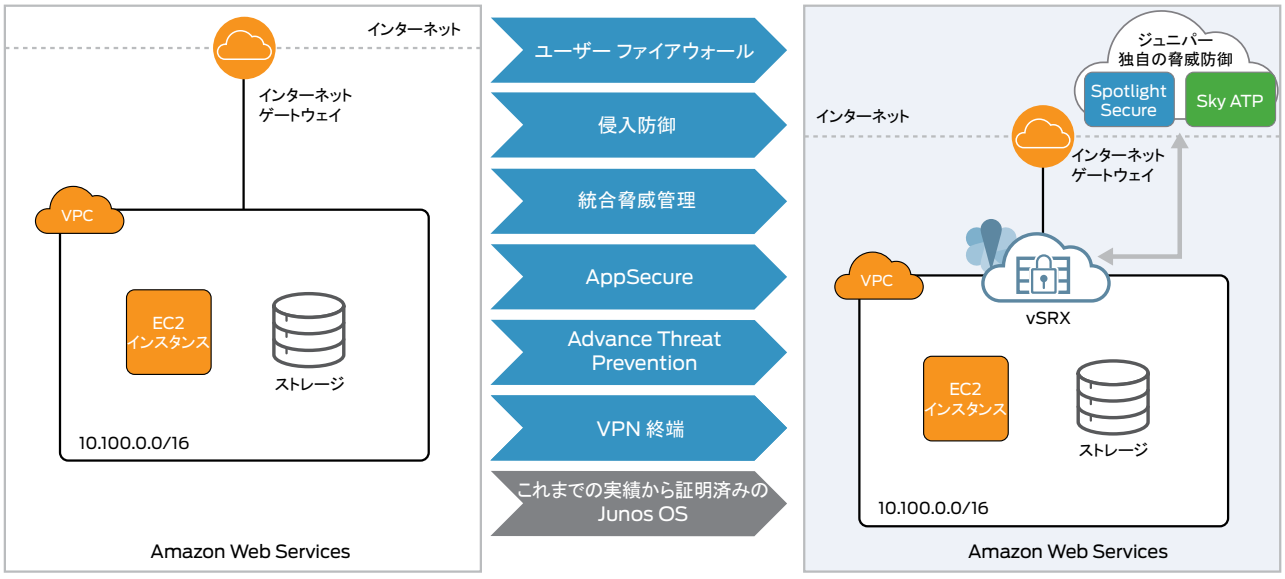

図 1：1 つの VPC からなるシンプルな AWS に vSRX を導入した場合

パブリック クラウド（AWS）の導入をセキュア化および簡素化するジュニパーネットワークスのソリューション

1 つのバーチャル プライベート クラウド（VPC）から成るシンプルな AWS の導入を見てみましょう。インターネット ゲートウェイと複数の EC2 インスタンスとともに、ジュニパーネットワークスのソリューションがどのように包括的なセキュリティ機能をクラウドに提供しているかを確認することができます。シンプルなクラウドの導入では、ジュニパーネットワークスの vSRX 仮想ファイアウォールをインターネット ゲートウェイと VPC の間に容易に組み込むことができ、包括的なセキュリティ機能と VPN サービスを利用することができます。

VPC を複数使用するようなもう少し複雑な AWS の場合は、vSRX によって専用ハードウェア コンポーネントの必要性が減り、これらのコンポーネントを統合して、管理を簡素なものにすることができます。例えば、複数の部門と数百名の従業員がいる企業を想像してください。専用の VPN を介して、ほぼ全員がインフラストラクチャ リソースにログインします。同じリソースを複数の部門が共有する場合もあれば、共有を必要としない部門もあります。AWS では、VPC 間の相互通信に専用のピアリング モジュールが必要です。デフォルトでは、VPC 内のすべての IP アドレスはプライベート スペース（10.X.X.X）にあります。内部リソースがインターネットにアクセスしようとする場合は、各 VPC に対する専用の NAT モジュールが必要となります。それに対して、AWS の vSRX は、マルチサイト VPN 環境での VPN の終端、NAT、VPC 間の相互接続のタスクを処理することができ、トポロジーを劇的に簡素化し、管理対象の数は削減し、VPC 間のセキュアできめ細かい制御を可能にします。（図 2 を参照）

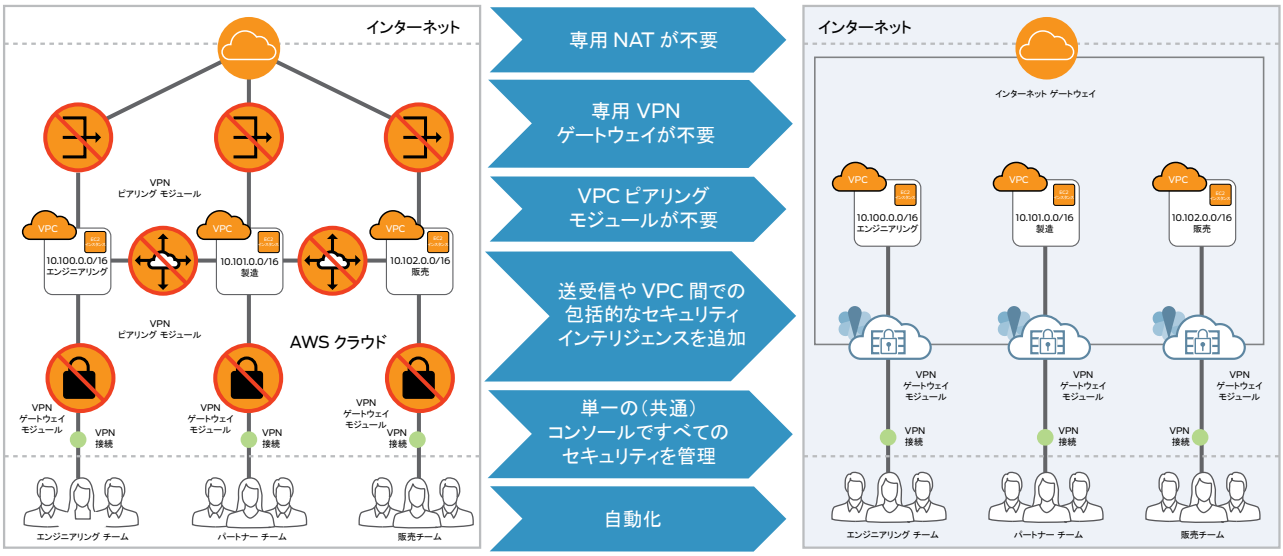

図 2：複数の VPC からなる AWS に対し、包括的に導入した場合

事例 1：エンタープライズ環境の拡張

別の場所に新しい支社を設置する

ある新規立ち上げの電子商取引企業はサンフランシスコに物理的なデータ センターを置いていますが、世界展開すべく海外にオフィスを構えることにしました。

- 要件：
  - ヨーロッパ、アジア、南米の各地域に新しいデータ センターを 1 つずつ設置する計画。
  - 従業員がそれぞれの地域から社内リソースにアクセスできる。
  - 顧客をそれぞれの地域へリダイレクトする必要がある。
  - メール、アクティブ ディレクトリ、ファイル サーバーといった必須のサービスは、すべてのデータ センターに複製され、データはリアルタイムで同期される。

事例 2：ワークロードの分散

地理的に離れた場所へワークロードを分散

米国東海岸のある映像配信会社では、11 月と 12 月の 夜 7 時から 10 時までの時間帯に視聴者数が増えると予測しています。年間を通して視聴者数が増えるわけではないので、物理データ センターを新たに導入したりプライベート クラウドに仮想データ センターをプロビジョニングしたりするのは、コストが高くつく可能性があります。

- 要件
  - 顧客のプライバシーを確実に守りつつ、コスト効率の高い方法で質の高いユーザー エクスペリエンスを提供することが不可欠。
  - コンテンツ データと顧客データを複製する必要がある。
  - データ センターの規模を需要の増減に合わせる必要がある。
  - 障害が発生することでサービスを停止するようなことは許されない。
  - 著作権のあるコンテンツや顧客の詳細情報が外部に漏れるようなことも許されない。

ジュニパーネットワークスのソリューションを拡張して、ハイブリッド クラウドのセキュリティを強化：実際の環境での導入事例

以下のセクションでは、2 つの導入事例における課題とセキュリティ要件を見てみましょう。エンタープライズの拡張、そしてワークロードの分散を通して、ジュニパーネットワークスのソリューションがどのようにこれらのシナリオに対応したかを紹介します。

エンタープライズ環境の拡張とワークロード分散のためのシンプルでセキュアなジュニパーネットワークスのソリューション

ジュニパー セキュリティ ソリューションは、エンタープライズ環境の拡張やワークロードを分散するのに必要なセキュリティを導入することができます。

- vSRX 仮想ファイアウォールは、VPC 内のインスタンスとアプリケーションのセキュリティ強化を目的として、VPC と各 AWS のインターネット ゲートウェイの間にインストールされます。SRX シリーズ デバイスおよび vSRX 仮想のファイアウォールは、クラウド上で高度な脅威防衛システムである Sky ATP と接続しており、最新の脅威情報を取得し、巧妙なマルウェアの検知を行います。
- vSRX は、IPsec VPN 終端、マルチサイト VPN、および NAT ゲートウェイ機能としても使われており、AWS 導入の促進や補完に利用されています。
- リモート データ センターの支店にある vSRX ゲートウェイが、セキュアなデータ転送のために、IPsec VPN を通じて、本部の SRX シリーズ ファイアウォールに接続します。
- Junos Space Security Director は、インフラストラクチャ全体のすべてのセキュリティポリシーを一元的に管理します。リモート データ センターに導入された vSRX 仮想ファイアウォールは、本部にインストールされているか、またはクラウドにインストールされているかにかかわらず、Security Director に登録されます。
- セキュリティ ポリシーがいったんリモート vSRX にプッシュされると、アプリケーション データはすべてのデータ センター間で同期化されます。
- 新しいセキュリティ ポリシーは、Security Director から一元的に追加されるか、更新され、すべてのデータ センターで導入されます。

ジュニパー セキュリティ ソリューションがもたらす主なメリット

ジュニパー セキュリティ ソリューションは、パブリックまたはハイブリッド クラウド環境に次のメリットをもたらします。

1. 共通のインテリジェント セキュリティ
   - vSRX 仮想ファイアウォールは、単一のエンフォースメントポイントとなります。vSRX は、クラウドに搭載された Sky ATP などの高度な脅威インテリジェンス プラットフォームからのセキュリティ フィードを利用して、アプリケーション セキュリティや侵入防御システム、統合脅威管理（UTM）を強化しながら、既知および未知の脅威を検知します。
2. 一元化され、シンプルで直感的な管理
   - Junos Space Security Director は、ネットワーク全体でセキュリティを監視するために、直感的で一元的な管理を実現します。ユーザー インターフェイスがシンプルであるため、新規ユーザーでもすぐに熟達します。iOS および Android プラットフォームで利用可能なモバイルの Security Director アプリケーションは、自社のネットワークにおけるセキュリティ アップデートを遠隔操作で監視したいセキュリティ管理者や CIO（最高情報責任者）が利用できます。

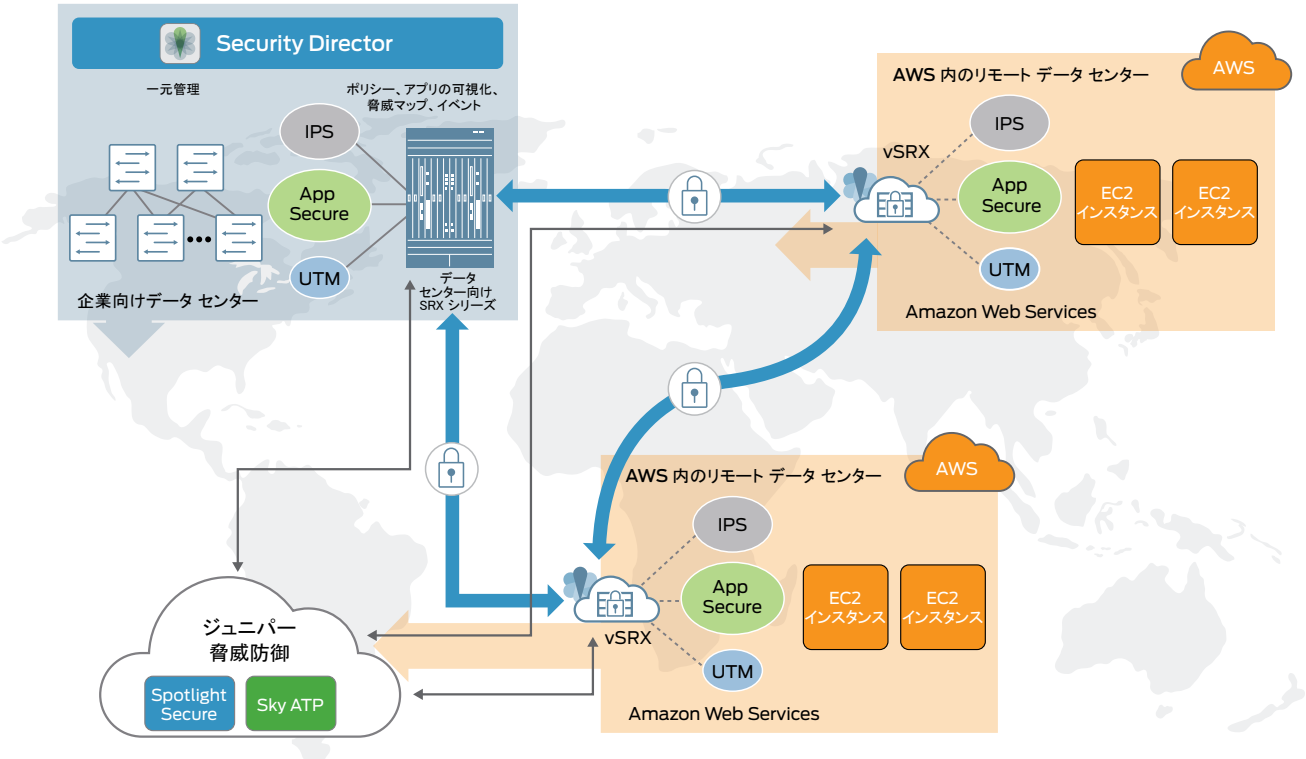

図 3：エンタープライズ環境の拡張やワークロードの分散のために、ジュニパー セキュリティ ソリューションをハイブリッド クラウドで展開した事例

3. プログラマビリティ

- ジュニパーネットワークス Junos オペレーティング システムでサポートされている幅広いプログラミング API により、シンプルなスクリプトを通じて容易に導入と管理アクティビティを自動化し、DevOps のリソースを活用して全体のワークフローを合理化することができます。

4. コストの削減と学習曲線の短縮

- 物理データ センターで使用されている、馴染みのある既知のセキュリティ ポリシーを拡張できることは、最も重要なメリットの 1 つです。企業は、これによって既存の管理者にクラウド インフラストラクチャの管理を任せられるようになります。クラウドのエキスパートを新たに採用する必要はありません。

まとめ

ジュニパーネットワークスのソリューションでは、柔軟性と管理方式の面で妥協することなく、パブリック クラウド、ハイブリッド クラウド間をシームレスに拡張できます。ジュニパーネットワークスは、高度に進化したセキュリティ インテリジェンス、シンプルな管理の集中化、そして自動化ツールによって、既存および新規のデータ センター全体のセキュリティの監視と強化を容易にします。

次のステップ

ジュニパーネットワークスのソリューションの詳細については、www.juniper.net/us/en/products-services/security をご覧いただき、ジュニパーネットワークス営業担当者にご相談ください。

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、ネットワークの経済性を変革する製品、ソリューション、サービスを通じて、現状打破に挑んでいます。ジュニパーのチームは、顧客やパートナーとの共同イノベーションにより、俊敏性、性能、そして価値のある、自動化され、拡張性に優れ、セキュアなネットワークを提供しています。詳細な情報については、ジュニパーネットワークスを参照してください。また、Twitter と Facebook もご覧ください。

米国本社
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
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
電話番号：+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。

3510567-003-JP 2017 年 3 月