安全なインターネットブレークアウトでクラウドアプリケーションのパフォーマンスを向上

First-packet iQ と Cloud Intelligence で、詳細なセキュリティーポリシーの実施が可能に

クラウドの採用が加速し続けています

企業は引き続きアプリケーションをクラウドに移行しています。ナレッジワーカーは現在、しばしば Office365、Salesforce、および Workday などの Software as-a-Service（SaaS）アプリケーションを使用し、クラウドでホスティングされたサービスから電子メールにアクセスし Box、Dropbox または同様のサービスに文書を格納し、バックアップとします。ERP ならびに CRM システムは、主にクラウドでホスティングされています。企業は、ますます IT アジリティを向上しながらのコスト低減に、Infrastructure as-a-Service（IaaS）ソリューションを選択しています。実際、IDC は、2018 年までに全仕事量の 78% がパブリックもしくはプライベートのクラウドデータセンターで処理されるだろうと予測しています*。

しかし、支店オフィスの従業員は一般的に、クラウドにホスティングされたアプリケーションの性能は、支店からよりも自宅からの方が良いと不満を持ちます。なぜでしょうか？自宅からの場合、SaaS アプリケーションと IaaS アクセスは 最大 100Mbps またはこれ以上のスピードのインターネットを直接介してのアクセスだからです。従来のルーターを中心とした支店の WAN エッジモデルでは、直接インターネットにアクセスしません。全てのインターネット行きのトラフィックは、会社を脆弱性から守るために追加のセキュリティ措置が実施される本社かハブサイトにバックホールされます。基本的な SD-WAN ソリューションは、インターネット行きのトラフィックの扱いに「100 かゼロか」のアプローチを採用、または全てのアプリケーションで、信頼される SaaS アプリケーションを直接インターネットに仕向けるための IP アドレスを特定するのに、全ての機器のアクセス制御リスト（ACL）の構成で手作業に依存しなければなりません。トラフィックバックホールが非効率であるだけでなく、潜在的に追加の、高価な帯域幅が必要であり、クラウドアプリケーションに悪影響を与えるレイテンシーも追加し、従業員の生産性と満足度が下がります。また、数日間で古くなってしまう SaaS アドレス ACL は、もう一度手動のプログラミングが必要です。

*IDC FutureScape: Worldwide Cloud 2016 Predictions, https://www.idc.com/promo/thirdplatform/RESOURCES/ATTACHMENTS/IDCFutureScapeExecSummary-Cloud.pdf

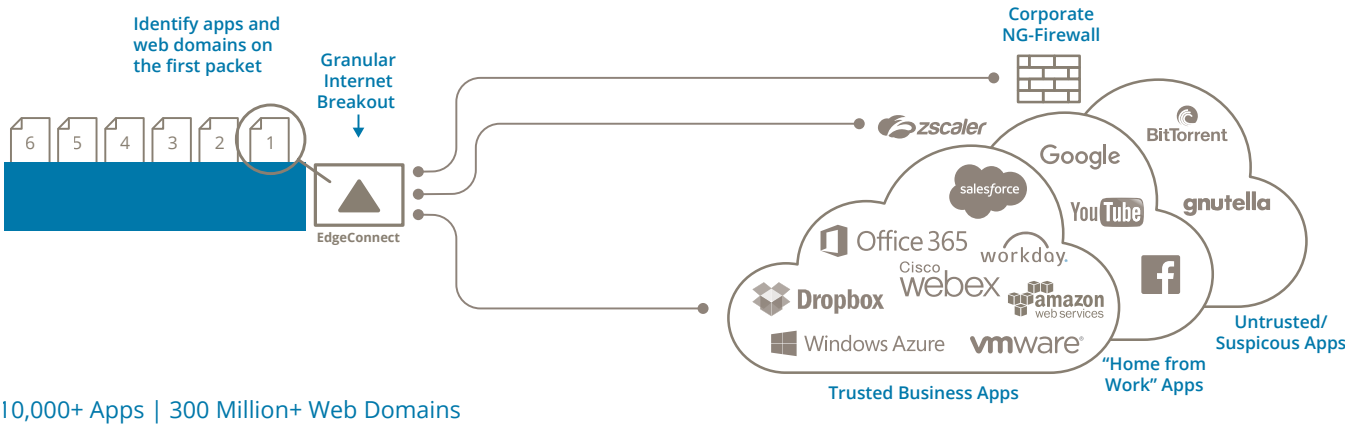

図 1：詳細なトラフィックステアリングでは、最初のパケットにアプリケーション分類が必要です。

使用事例：安全なインターネットブレークアウト

インターネットを介して支店からクラウドアプリケーションに直接アクセスすることで、最高のパフォーマンスが実現できます。しかし、全てのアプリケーションが同じというわけではなく、あるウェブトラフィックは会社をウイルス、トロイの木馬、DDoS 攻撃、およびその他の脆弱性にさらすかもしれません。従って、直接のクラウドブレークアウトもまた安全である必要があります。

SD-WAN が満たさなければならない課題は、アプリケーションごとでインターネット行きの HTTP と HTTPS トラフィックを、企業のセキュリティーポリシーに従って正しい方向へ細かく調整することです（図 1. 参照）例えば、セキュリティーポリシーは次のように定義されます：

- Office365、Salesforce、Workday、および Box など、全ての既知の、信頼されるビジネス SaaS トラフィックをインターネットに送る
- Facebook、Twitter、YouTube、Netflix などの「在宅勤務」レクリエーションアプリケーションを、Zscaler などの安全なウェブゲートウェイサービスに送る
- 全ての信頼できない、疑わしい、および未知のトラフィック、ピア ツー ピアのトラフィック、または会社が事業を行なっていない国へのトラフィックなどは、ハブもしくは本社に備える Palo Alto、Fortinet、または Check Point などの次世代ファイアーウォールに送る

ウェブアプリケーションに詳細なセキュリティーポリシーを実装するには、多くの HTTP ならびに HTTPS アプリケーションが同じ TCP ポートを共有するため、詳細なトラフィックステアリングが必要です。しかし、ステアリングは、アプリケーションの最初のパケットで判断されなければなりません。アプリケーションセッション、または流れが一度確立すると、別のパスに移動することはできません。

最初のパケットでトラフィックを詳細にステアリングするには 2 つの課題があり、この 2 つには次の機能が必要となります：

- トラフィックを正しい方向にステアリングするため、最初のパケットでアプリケーションを認識する機能
- これらのアドレスは連続的に変わるため、「インターネットの地図」とも言われる、SaaS アプリケーション IP アドレスデータベースの最新版を SD-WAN 機器に保持

課題 1：最初のパケットでアプリケーションを認識

従来のアプリケーション分類技術は、よく知られた IP アドレス、TCP/UDP ポート番号と、ディープ パケット インスペクション（DPI）の組み合わせを活用していました。DPI は、アプリケーションがポートを予期せず使用する場合や、同じ HTTP もしくは HTTPS ポートを共有するアプリケーションを区別する場合には便利です。しかし、DPI は、アプリケーションを最初のパケットで認識できないため、アプリケーションごとにトラフィックを特定の方向に、詳細にステアリングするには不十分です。DPI は、アプリケーション署名やヒューリスティックのライブラリに依存し、HTTP アプリケーションの認識には 2 から 6 個のパケットが、HTTPS アプリケーションの認識には 10 個以上のパケットが必要です。フローレポート、QoS マーキング、および接続のブロックにはこれは許容されますが、WAN 全体の細かなセキュリティーポリシーの実装に

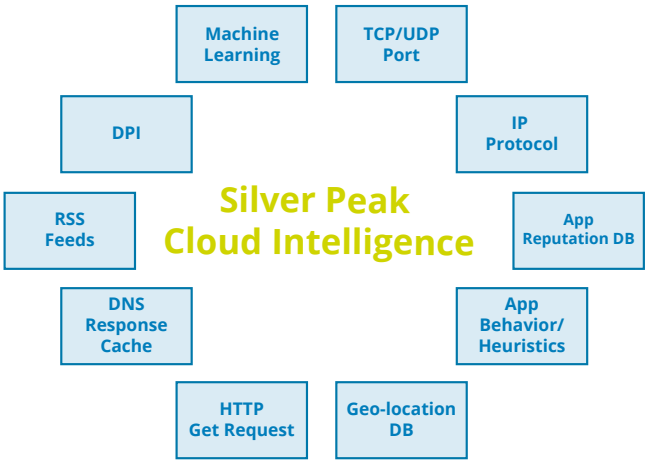

図 2：First-packet iQ は複数の技術を使用して、10,000 を超える SaaS ならびにウェブアプリケーション、および 3 億を超えるウェブドメインを分類します。

必要な、詳細なトラフィックステアリングに対応することはできません。

鉄道での例え

機関車と複数の貨車からなるいくつかの列車が、サンフランシスコから移動することを想像してみてください。デンバーの東に向かう必要のある家具を積んだ列車と、ロサンゼルスの南に向かう必要のある航空宇宙のコンポーネントを運ぶ必要のある列車です。しかし、その列車が運んでいる貨物については、機関車と 3 から 5 両の貨車が線路のスイッチを通過するまで判断することができません。

機関車は、TCP/IP の流れの最初のパケットを表し、貨車はその後に続くパケットを表します。列車がデンバーとロスアンゼルスへ向かう異なる線路に接続しているスイッチに近づくと、スイッチオペレーターは 5、3 両目、または 2 両目が通り過ぎるまで待つことができません。悲惨な結果を避けるために、列車の切り替えの判断は機関車がスイッチに到達する前に決定しなければなりません。従って、機関車がスイッチを通り過ぎる前に貨車の荷物を特定する技術が必要になります。

ソリューション：First-packet iQ アプリケーション分類

セキュリティーポリシーを適用するために正しいパスにトラフィックをステアリングするには、トラフィックは流れの最初のパケットで分類される必要があります。Silver Peak Unity EdgeConnect First-packet iQ は、10,000 以上のアプリケーションと 3 億以上のウェブアプリケーションを最初のパケットで認識します。First-packet iQ は、今日利用されている典型的な DPI やポートレベルのアプローチを超え、Cloud Intelligence を加えて SaaS アプリケーションが使用する IP アドレスデータベースを最新の状態に維持します。

First-packet iQ は、図 2 に示すように複数の技術を使用してアプリケーションを分類し、これまでにないアプリケーションの可視性と優れた識別信頼度を提供します。

課題 2：SaaS IP アドレスは毎日変わる

Office 365、Salesforce、Workday、Box、Dropbox などの人気の高い SaaS アプリケーションは、膨大な数のユーザーをサポートするために数百または数千の IP アドレスを使用します。これらの IP アドレスは静的ではありません。別の地域または別のアプリケーションに再割り当てすることができます。エンドユーザーの要求に対応するために、新しいアドレスが頻繁に追加されます。要するに、SaaS アプリケーションで使用される IP アドレスのプールはほぼ連続的に変化します。表 1 は、Skype for Business および Office365 の IP アドレスプールで削除されたアドレスと追加されたアドレスを示す、毎日の SaaS アプリケーションサブネット変更レポートの短い抜粋です。

一部の SD-WAN ソリューションは、最初のパケットでアプリケーションをステアリングし、これを ACL を使用して達成できるとしています。ただし、ACL は静的であり、手作業でプログラムする必要があります。セキュリティーポリシーは、構成した当初は適切に動作するかもしれませんが、SaaS アプリケーションの IP アドレス変更後数日、または数週間でうまくいかなくなります。ACL の IP アドレスを手作業で再プログラミングするのでは、SaaS アプリケーションの動的な性質に追いつくわけがありません。

ソリューション：Cloud Intelligence は連続して変化する SaaS IP アドレスに足並みを揃えます

Silver Peak Cloud Intelligence は、一元化されたアプリケーションデータベース、または先述のアプリケーション分類技術に基づいて継続的に更新される「イン

App Name	Status	Subnet	Old Reachable Ip	Old Port	New Reachable Ip	New Port
skypeForBusiness	deleted	104.41.210.140/32	104.41.210.140	80		None
skypeForBusiness	deleted	207.46.156.136/32	207.46.156.136	80		None
skypeForBusiness	deleted	23.97.72.141/32	23.97.72.141	80		None
skypeForBusiness	deleted	40.113.16.205/32	40.113.16.205	80		None
skypeForBusiness	deleted	40.76.24.177/32	40.76.24.177	80		None
skypeForBusiness	deleted	40.76.24.32/32	40.76.24.32	80		None
skypeForBusiness	deleted	52.233.29.169/32	52.233.29.169	80		None
skypeForBusiness	deleted	52.233.30.121/32	52.233.30.121	80		None
office365	new	51.140.46.150/32		None	51.140.46.150	443
office365	new	52.169.109.48/32		None	52.169.109.48	80
intuit	new	12.5.80.64/26		None	12.5.80.67	443
office365Exchange	changed	40.97.28.0/24	40.97.28.22	443	40.97.28.114	80
microsoftTeams	new	52.185.146.154/32		None	52.185.146.154	443
microsoftTeams	deleted	104.41.210.140/32	104.41.210.140	80		None
microsoftTeams	deleted	13.64.106.229/32	13.64.106.229	443		None
microsoftTeams	deleted	13.64.240.95/32	13.64.240.95	80		None

表 1：ここで Office365 や Skype-for-Business に見られる IP アドレスの日次の変更には、継続的に更新されるインターネットマップが必要です。

ターネットの地図」を維持します。図 3 に示すように、EdgeConnect SD-WAN アプライアンスは、常駐アプリケーションのアドレスデータベースを更新して、SaaS アドレスと Web IP アドレスの変化に合わせて、最新の状態を維持します。この更新プロセスは、コンピューターウイルス保護アプリケーションで採用されているのと同様のものです。

統合化されたゾーンベースのステートフルファイアーウォール

統合化されたゾーンベースのステートフルファイヤーウォールは、完全で、安全なクラウドブレークアウトソリューションで、直接インターネットへの接続性を、支店オフィスからの信頼できる SaaS アプリケーションと IaaS に与えます。EdgeConnect のゾーンベースのファイアーウォールは、不必要な、または許可されていないトラフィックの支店ネットワークへの侵入をブロックすることで、エンタープライズ WAN を強化します。唯一許可されるインバウンドセッションは、支店内から開始された通信へ、または信頼されたインバウンド通信のためにホワイトリストもしくは開かれたポートへの応答で、例えば、遠隔で管理されたプリンターや会議システムなどがあります。

シンプルで、一元化されたセキュリティポリシーの管理と自動更新

完全な SD-WAN ソリューションの主な利点は、シンプルで、一元化されたオーケストレーションです。直感的なグラフィッフィカル ユーザー インターフェース（GUI）を 通 じ て、Silver Peak Unity Orchestrator は EdgeConnect SD-WAN ファブリック上にある全ての機器へのセキュリティーポリシーの構成と配信を合理化します。これにより、大きな運用コストの削減だけでなく、人為的エラーによって不適切にアプリケーションを扱ってしまう可能性を低減します。Orchestrator は、電子メール、音声、およびビデオなどのトラフィックの種類、およびオークション、自動車、航空、教育、ファンタジースポーツ、ソーシャルメディアなど（図 4）業界標準のグループ化を活用し、セキュリティーポリシーの定義をさらに簡易化します。先にも説明した通り、EdgeConnect 機器へのアプリケーション IP アドレスデータベースの自動日次更新は、SaaS とウェブアドレスの変更に対応します。

図 3：アプリケーション IP アドレスデータベースは毎日すべての EdgeConnect 機器に更新されます。

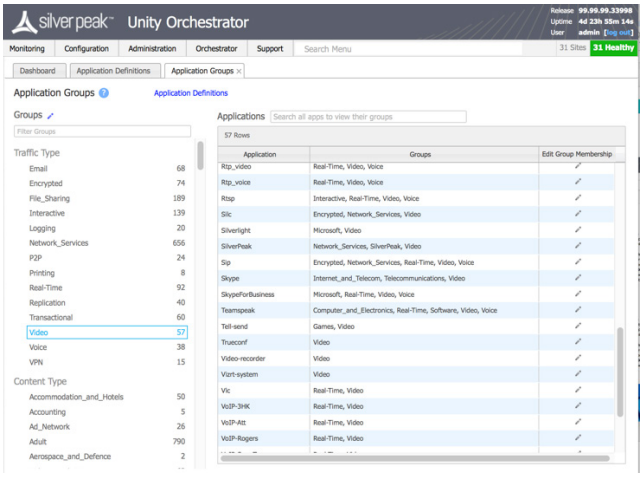

図 4：アプリケーションのグループ化により、セキュリティポリシー管理が簡素化されます。

バックホールトラフィックのための最適化されたイグレスルーティング

支店からの直接のインターネットブレークアウトにより、高度な SaaS アプリケーションならびに IaaS パフォーマンスを提供します。しかし、インターネット接続が提供されていない事業所、または企業のセキュリティーポリシーが、追加のセキュリティー検査のために SaaS アプリケーションのバックホールを必要とする場合には、Silver Peak Cloud Intelligence は、ベストパフォーマンスのために最適にトラフィックをルーティングする情報を含みます。Silver Peak SaaS 最適化 機能は、EdgeConnect デバイスから SaaS プロバイダーのデータが提供される物理的イグレスポイントまでのロス、レイテンシー、およびその他の指標を測定します。この情報は、EdgeConnect SD-WAN の機器に継続的に更新され、最適化されたエント ツーエンドパスを SaaS アプリケーションのどのユーザーにも提供します。

ビジネスの成果

企業がクラウドへの移行を続けるにつれ、多くの会社に明白なビジネス上の利益を実現する、高レベルの SaaS アプリケーションならびに IaaS パフォーマンスを提供するため、ますます「クラウドファースト」の SD-WAN アーキテクチャーを採用するようになっています。First-packet iQ や Cloud Intelligence を備えた Silver Peak EdgeConnect SD-WAN ソリューションは、クラウドファーストの企業に高いパフォーマンスを実現し、支店オフィスを不要な脅威や脆弱性から保護します。

EdgeConnect ソリューションの利点	ビジネスの成果
SaaS アプリケーションと IaaS のパフォーマンスと可用性の向上	従業員とビジネスの生産性を高める
予測可能な SaaS アプリケーションのパフォーマンス	顧客満足度の向上
First-packet iQ によって可能になる、詳細なアプリケーション主導のセキュリティポリシー	セキュリティーリスクを軽減
自動化された SaaS IP アドレステーブルとインターネットマップの更新	運用効率の向上と人為的ミスの軽減
統合化されたゾーンベースのステートフルファイアーウォール	セキュリティーリスクを軽減

表 2：Silver Peak Unity EdgeConnect SD-WAN ソリューションは、明確な利益とビジネス成果をもたらします。

住所

Silver Peak Systems, Inc.
（シルバーピークシステムズ・インコーポレーテッド）
2860 De La Cruz Blvd.
Santa Clara, CA 95050

電話とファックス

電話：+1 888 598 7325
ローカル：+1 408 935 1800

オンライン

電子メール：info@silver-peak.com
ウェブサイト：www.silver-peak.com