クラウドアプリ時代に求められるネットワークセキュリティ(ファイアウォール)とは?

これまで企業セキュリティといえば、アンチウイルスツールをPCにインストールし、ファイアウォールのようなゲートウェイセキュリティで脅威が侵入しないようにする境界防御が中心だった。しかし、どんどん便利になるクラウドサービスの進化と普及、サイバー攻撃の高度化によって、従来の境界防御だけでは対応しきれなくなっているのが現状だ。テクノロジーの進化にともない企業のIT環境がますます複雑化する中、ファイアウォールを中心とした企業のネットワークセキュリティを今、見直す時期がきている。

クラウドトラフィックの急増にネットワークはどう対応できるか?

いまやクラウドサービスなくして、企業の業務、特にOA業務は成り立たないといっても過言ではないだろう。その一方で、クラウドサービスの浸透によって企業のネットワークは劇的に変化した。これまで社内を中心に格納されていた多くのデータがインターネットを経由してクラウド上のサーバーに保存され、ネットワークを流れるトラフィックの量は、従来とは比べものにならないほど増えた。

たとえばマイクロソフトのクラウドアプリケーションである「Office 365」の導入が多くの企業で進んでいるが、同時にネットワークのレスポンス低下に悩まされている企業も多いという。クラウドアプリを導入することで、社内PCとクラウド上のサーバーとの通信が増大し、それに合わせてインターネットトラフィックだけでなくセッション数も数倍に増大する。その結果、レスポンスの低下、クラウドとの接続切断が発生し、社内ユーザーのストレスにつながることがある。最近では電話に代わってVoIPを使ったコミュニケーションツールが普及しているが、WAN回線にバースト性のあるクラウドデータが流れ込むと、VoIPによる音声通信が影響を受けることがあり、業務効率の低下は避けられない。

また、サイバー攻撃の進化も無視できない状況だ。ターゲットとなる企業や組織に合わせてマルウェアや侵入方法をカスタマイズするのは当たり前で、これまでのシグネチャーを使ったファイアウォールやアンチウイルスでは検知できない脅威が急増している。企業のネットワークはこうした新手の脅威に対しても、必要な対策が求められている。

クラウドアプリの普及、高度なサイバー攻撃と、現代の企業ネットワークを取り巻く環境は大きく変化し、5年前のテクノロジーではもはや対応できない。ネットワークセキュリティの代表ともいえるファイアウォールはこれからも必須の対策だが、当然のことながら、今求められるファイアウォールの機能は5年前のそれとは大きく異なってくる。

こうした環境変化の中、これまで世界中の企業ネットワークセキュリティを担ってきた老舗のファイアウォールがその役割を終えようとしている。ジュニパーネットワークスの「NetScreen SSG」(SSGシリーズ)だ。SSGシリーズは2020年から2021年初頭にかけて市場から引退し、それに代わって同社の「新生」SRXシリーズが、今求められるファイフウォールとして現在の企業ネットワークのアプリケーション配信とセキュリティを担っていく。

ジュニパーネットワークス株式会社
技術統括本部
エンタープライズ技術第二本部
本部長 長田篤氏

人気のファイアウォールSSGを継承して生まれ変わった新しいSRX

ジュニパーネットワークス 技術統括本部 エンタープライズ技術第二本部 本部長の長田篤氏は、同社のファイアウォール製品の世代交代について、次のように話す。

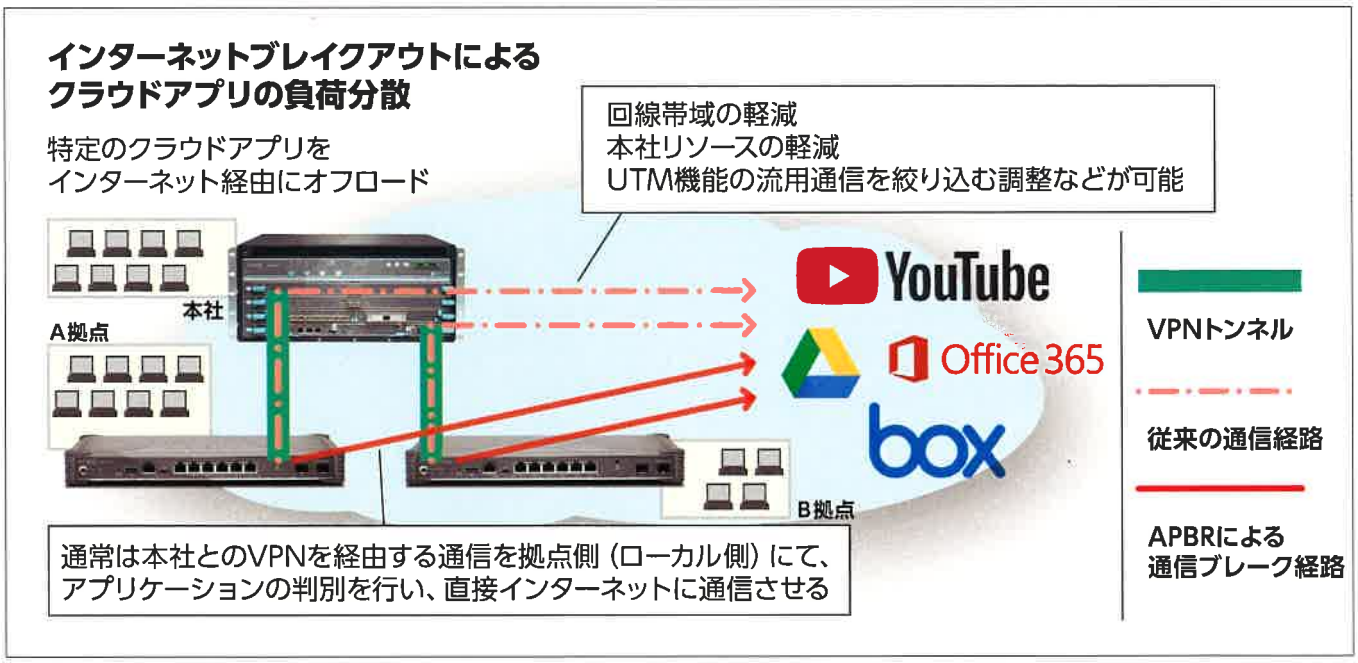
「当社のSSGシリーズはNetScreen社の買収後、販売を継続させていただいたファイアウォールですが、世界中で使われている人気製品です。強力なUTM（統合脅威管理）として、世界中のお客様のネットワークを守ってきました。そのSSGが2020年以降保守終了を迎えようとしています。後継となるSRXシリーズはSSGのDNAを引き継ぎ、さらにネットワーキング企業として強みを活かした『アプリケーション識別＋トラフィック制御』機能を強化しており、単なる境界防御ではなくネットワーク基盤の要として機能するファイアウォール（セキュアルータ）として販売しています。販売当初は機能の移植が十分でなくお客様に混乱を与えてしまいましたが、現在のSRX 300シリーズはSSGの使いやすさを引き継ぎつつ、安定してお客様にご利用いただいています。当社の強みであるルーティングおよびスイッチング機能が拡張され、クラウドアプリを最適化して配信する機能だけでなく、未知の脅威にも対応するセキュリティ機能が備わるなど、時代に合わせた進化を遂げています」

SRXの製品名を構成するSは「セキュリティ」、Rは「ルーティング」、Xは「スイッチング」を表している。「SRXは境界防御としてのファイアウォールにとどまらず、脅威対策のセンサーとしても機能する。さらに、BGPやMPLSのような重要なプロトコルに対応したトラフィック配信機能を持つ、ジュニパーネットワークスらしいセキュリティ製品」（長田氏）というわけだ。

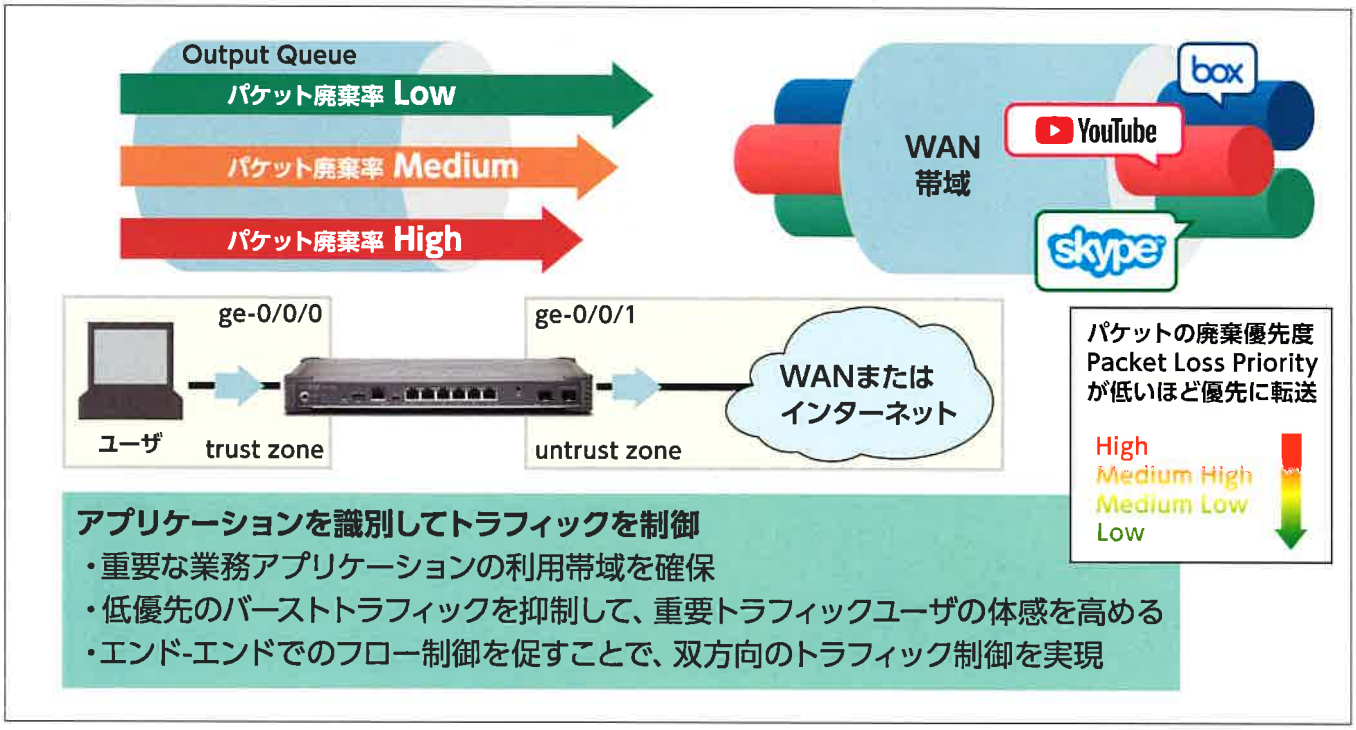
セキュリティ機能としては、IPSといったUTM機能、IPsecやSSL VPNといった暗号通信機能だけでなく、通信されるトラフィックに未知のマルウェアが含まれていないかクラウドで解析するサンドボックス機能の追加も可能になっている。SSGの基本機能はしっかりと継承し、現在のネットワーク環境に求められる新しいテクノロジーも実装されている、それが今のSRXである。

「Office 365 を入れたら遅くなった」にならないためのファイアウォール

ルーティング機能を備えたファイアウォール＝セキュアルータとして、SRXがその強みを発揮するのがクラウドアプリのセキュアかつ最適な配信だ。



クラウドアプリ最適化により、特定のアプリケーションの経路変更が可能



アプリケーションの優先制御によりユーザー体感を最適化

多数のセッションを同時に張るOffice 365では、通信量が多く、インターネットと社内との間のトラフィックが激増する。そのため、社内ユーザーからみると遅い、通信が切れるといった使い勝手の低下につながる。

SRXは3,600種類以上のアプリケーションを識別・可視化し、特定のアプリケーションの経路変更や優先度を変更できるルーティング機能を備えている（AppRouteおよびAppQoS）。ファイアウォールでありながら、ルーターとしてアプリケーションごとに細かな制御ができるというわけだ。

AppRouteを使えば、Office 365といった特定のアプリケーションを、拠点のユーザーは本社を経由せずに直接インターネットに接続し、クラウドアプリのサーバーと通信させることができる（インターネットブレイクアウト）。直接インターネットと通信するといっても、SRXのトラフィックは暗号化されているため、セキュリティ上の懸念はない。こうしてOffice 365が発生する膨大なトラフィックを本社・拠点で分け、本社・拠点を結ぶ高価な回線の帯域の負荷を軽減するとともに、ユーザーのレスポンスを向上できる。ファイアウォールとルーターの機能を兼ね備えたSRXならではの使い方だ

また、SRXではアプリケーションを識別することでアプリケーションごとに優先度をつけられる。遅延の影響を受けやすい音声やビデオアプリは最優先で転送する。音声通話は少しでもノイズがあると会話が成り立たないからだ。ファイルのダウンロードやアップロードは、数秒程度の遅延であれば気にならないので、帯域競合が発生した場合にはトラフィックを廃棄して再送を促す。またActive Directoryと連携させれば、ユーザーごとにアプリケーションを制御することも可能だ。こうすることで、アプリケーションに応じてユーザーの体感を向上させられるわけだ。

ネットワークを面で守るセキュリティ

従来のセキュリティの考え方は、あくまでもインターネットと社内の境界を守る境界防御となる。そのため、異なるテクノロジーのセキュリティシステムを多段で導入し、外部からの侵入を可能なかぎりブロックできるようにする。しかし、いったん社内に侵入されてしまうと、ネットワークでは社内で起こる侵害を阻止できない。

ジュニパーネットワークスのSRXは、ネットワークにおける脅威センサーとして機能し、vやスイッチといったそれ以外のネットワーク機器と連携して、ネットワークを面で守る仕組みがある。SRXには、未知のマルウェアの侵入をクラウド上の仮想実行環境で検知するSky ATPを搭載できる。Sky ATPでは各種のセキュリティ機関で共有される脅威インテリジェンスを基に、高度な解析を実施し、脅威が検知されたらそれをネットワークにフィードバックする。

具体的には、SRXは検知した脅威に関する情報を、ネットワークセキュリティのポリシーを管理するSecurity Directorのポリシーエンフォーサーへ伝達し、即座にセキュリティポリシーを変更、その脅威が再び侵入することを阻止する。またポリシーコントローラはネットワーク上のスイッチを制御して、感染した端末をネットワークから隔離し、脅威の拡大を防ぐ。ジュニパーネットワークスでは、脅威の状況に応じて迅速かつ柔軟にセキュリティポリシーを変更して、セキュリティを強化するこの仕組みを「SDSN（Software-Define Security Network)」と呼ぶ。

「最近では、セキュリティ対策の弱いIoT機器を狙う攻撃も増えています。SDSNであればエージェントをインストールできないIoT機器やエージェントに対応しない古いPCがマルウェアに感染した場合でも、脅威の拡散を防止できます。将来的には、ポリシーコントローラをSRXに組み込む計画で、さらにシンプルなSDSN環境を実現できるようになります」（長田氏）

クラウド時代に求められるファイアウォールへの移行

前述したように、ジュニパーネットワークスは多くのお客様にご利用いただいるSSGから、クラウド時代にふさわしい新生SRXへの移行を進めている。セキュリティは境界防御の対策から、クラウドアプリの安全で最適な配信、高度なサイバー脅威の検知とリアルタイムの対応（SDSN）といった対策が不可欠になっているためだ。

またSRXシリーズでは、仮想アプライアンスとして稼働する「vSRX」も提供されている。VMwareやKVM、Hyper-Vといった主要なハイパーバイザーのほか、AWSやAzure、Google Cloudのようなパブリッククラウドでも利用でき、まさにクラウド時代に求められるファイアウォールとなっている。

いまや企業のネットワークは、従来のセキュリティシステムを見直しする時機に差しかかっている。そこで、ジュニパーネットワークスではSSGをご利用のお客様がスムーズにSRXへ移行できるよう、販売パートナーとともにリプレースキャンペーンを実施している。今後クラウドの活用が計画されていて、またご利用中のファイアウォールがクラウドのパワーを十分に引き出せないのであれば、こうしたキャンペーンを利用して、ファイアウォールのリフレッシュを検討してみてはいかがだろうか。

JUNIPER NETWORKS

ジュニパーネットワークス 株式会社

本社 Tel: 03-5333-7410
https://www.juniper.net/jp/jp/
E-Mail: inquiry-jp@juniper.net