

顧客ユーザーにアプリケーション制御のセキュア通信を提供 「KDDI Wide Area Virtual Switch」で セキュアなインターネットサービスを実現

システムや業務データがデータセンターに集約されるデータセントリックな環境が進む企業ICTの運用ニーズに対応し、データセンターからアプリケーション、ネットワーク、宅内機器まで含めた、あらゆるICTサービスをワンストップで提供するためのプラットフォーム「KDDI Wide Area Virtual Switch」。この「広域仮想スイッチ」構想の中で、Virtualデータセンターの1つのメニューであるセキュア・インターネットサービスにおいて、仮想専用型ファイアウォール機能の提供のためにPA-4050が採用された。

Virtualデータセンターのメニューとして提供される仮想ファイアウォール

「KDDI Wide Area Virtual Switch」(以下、KDDI WVS)は、従来の広域イーサネットやIP-VPN型サービスとは異なり、文字通り「広域仮想スイッチ」という新しい概念を国内通信事業者として初めて導入した新型ネットワークサービスだ。広域イーサネット、IP-VPN、低価格VPN、宅内ルータの機能をすべて集約、レイヤ2/レイヤ3サービスを統合して、あたかも宅内のLANスイッチのように扱える、シンプルで柔軟な次世代広域ネットワークサービスだ。

KDDI WVSの特徴には、トラフィックが集中するデータセンター向け通信に対して、拠点における契約通信帯域に関わらず、回線終端装置のインタフェースの上限値まで通信帯域を拡張する「トラフィックフリー機能」、ブロードバンド回線を仮想的にイーサネットアクセス回線として利用できる「プラグイン機能」、拠点の利用形態に応じて異なるレイヤやアクセス回線を含むネットワークの一元化を可能にする「L2/L3マルチレイヤ」機能など多彩な特徴をそなえる。こうした機能の中に、2010年5月から提供される「セキュア・インターネット」サービスがある。ユーザー企業の各拠点から高速かつ安全なインターネット接続を可能にするために、1Gbpsのインターネットアクセス回線と仮想専用タイプのファイアウォール機能を標準で提供するもので、大容量バックボーンに直結したサーバ機能をユーザーのシステム構築なしで利用できる「Virtualデータセンター」のメニューの1つとして提供される。

「従来のWANサービスにおけるインターネット接続機能では、プロトコル制限などがありました。インターネットを介した取引会社との通信で業務系アプリケーションを自由に使いたいというお客様の要望に応えるために、広域ネットワークサービスの中でセキュアで高速なインターネット接続サービスを実現するものです。そのサービスでは、次世代広域ネットワークサービスであるKDDI WVSにふさわしい次世代ファイアウォール機能を仮想専用型で提供しようというのが大きなポイントです」。ソリューション商品企画本部プラットフォーム・セキュリティグループ課長補佐 和氣二朗氏は、PA-4050を採用した背景をこう述べる。

ユーザー自身の運用管理と高度なトラフィック制御に応える

ユーザー企業それぞれに論理的なファイアウォール機能を提供するためには、当然ながら仮想化技術を採用したファイアウォールが重要な要件。また、KDDI WVSの大きな特徴であるトラフィックフリー機能を活かすために、ワイヤースピードのファイアウォールスループットが求められた。PAシリーズには、マルチテナントサービス機能であるVSYS (仮想システム)があり、PA-4050では最大125の論理ファイアウォールを構成することができ、それぞれに管理権限が与えられ、個別にポリシー設定ができる。一方、パフォーマンスに関しては「シング

Designing The Future




KDDI 株式会社

東京都千代田区飯田橋 3-10-10 ガーデンエアタワー
<http://www.kddi.com/>

分野

電気通信事業

導入背景

- 広域ネットワークサービスにおいて、プロトコル制限のないセキュアなインターネット接続サービスを提供
- 顧客ユーザーが個別管理可能な仮想専用型ファイアウォールの実現
- アプリケーションレベルのトラフィック制御によるセキュアな通信を実現

ソリューション

- App-IDによるアプリケーションの可視化と制御
- 仮想システム (VSYS) 機能による顧客ユーザーごとの仮想ファイアウォール管理

「次世代広域ネットワークサービス『KDDI WVS』の提供において、他社キャリアとの差別化を目的で『次世代ファイアウォール』を標榜しているPAシリーズが最もふさわしいと考えました」



和氣二朗氏
KDDI 株式会社
ソリューション商品企画本部
ソリューション商品企画部
商品企画1グループ
課長補佐

ル パスパラレルプロセッシング (SP3) アーキテクチャ」により、ポリシーマッチングやアプリケーション識別、コンテンツスキャンを、指定されたトラフィックに対して並列処理を行う個別専用のプロセッサを実装しており、スループットを最大化している。

こうした要件を満たす機能は選定候補に上った他社製品にも見られたが、その中でPA-4050が採用された理由を和氣氏は次のように指摘する。

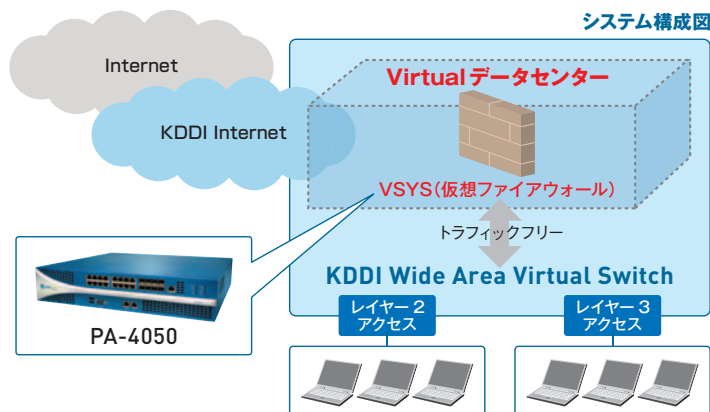
「他のキャリアもKDDI WVSと同様のネットワークサービスを提供してくる中、差別化を図る目的で『次世代ファイアウォール』を標榜しているPAシリーズが、次世代広域ネットワークサービスに位置付けているKDDI WVSにふさわしいと考えたからです。具体的には、アプリケーション、ユーザー、コンテンツを可視化してポリシーベースで制御するとともに脅威を防御するという点を高く評価しました」(和氣氏)。

あらゆるP2P型ファイル共有ソフトのブロックはもちろん、取引会社間での業務系トラフィックを確実に識別してセキュアな通信環境を確保するために、PAシリーズのアプリケーション識別・制御能力の優位性が評価されたもの。和氣氏は、「(セキュリティアプライアンスによる)アプリケーション制御はIPS (不正侵入防御) 技術を応用したものが多く中で、PAシリーズが独自のテクノロジーで実現していること。また、誰が何のアプリケーションを使い、どこで通信しているか、さらにそのリスクが高いのか低いのかを一目瞭然にできることは、お客様にとって非常にメリットが高いと感じています」と強調する。

ユーザー認証基盤と連携したきめ細かなトラフィック制御も実施

PAシリーズの管理インターフェースは、コマンドライン、Webベース、あるいは集中管理ソリューションを使用した管理が可能だが、KDDIでは顧客ユーザーがより簡便に操作できるように設定・管理項目を絞った独自のインターフェースを開発して提供する。

今後はMicrosoft Active Directoryや各種LDAPとの連携により、個別ユーザー情報に基づいたアプリケーションとコンテンツ監視のサービスも提供していく他、DMZ機能もVirtualデータセンターの中で利用できるようにしていく。「Virtualデータセンターという大きな機能の枠の中に様々なメニューをそろえて、『所有する』から『利用する』という環境を提供していきます。その構想の中で『次世代ファイアウォール』は、市場認知の拡大とともに大きな役割を果たすでしょう」(和氣氏)と期待を込める。



パロアルトネットワークス

E-mail: InfoJapan@paloaltonetworks.com

www.paloaltonetworks.jp