

DAG
disaggregatorの略。

VIPRIONでは、シャーシ内のブレード・サーバーを仮想化して1台に見せることで、運用性を高めている(図2-5)。

F5ネットワークスのVIPRIONは、同社のアプリケーション・スイッチであるBIG-IP8800とはほぼ同じ機能と処理能力をもつブレード・サーバーを、最大4枚搭載できるシャーシ型の製品である。

それぞれのブレード・サーバーにはCPUが四つ載っている。そして、各ブレード・サーバー間は、スイッチ・ファブリック同士がシャーシ内のバックプレーンを通じてメッシュ状につながる。こうすることで、すべてのブレード・サーバーが一体化しているように利用できる。

具体的な動きを見てみよう。クライアントからのパケットは、まずその通信ポートがつながっているブレード・サーバー内の「DAG」^①という部分で受け取る。DAGは、パケットの入出力を振り分けるスイッチに相当する部分だ。

DAGでは、過去のコネクション数やパケットのハッシュ値を元に、VIPRIONに搭載した全ブレード・サーバーの全CPUの中から、受け取ったパケットを処理させるCPUを決める。処理させるCPUを決めたら、バスやファブリック経由でDAGからCPUにパケットを送る。CPUで必要な処理をした後のパケットは、送信先のサーバーがつながっているブレード・サーバーのDAGに送る。受け取ったDAGは、送り先のサーバーにパケットを転送する。

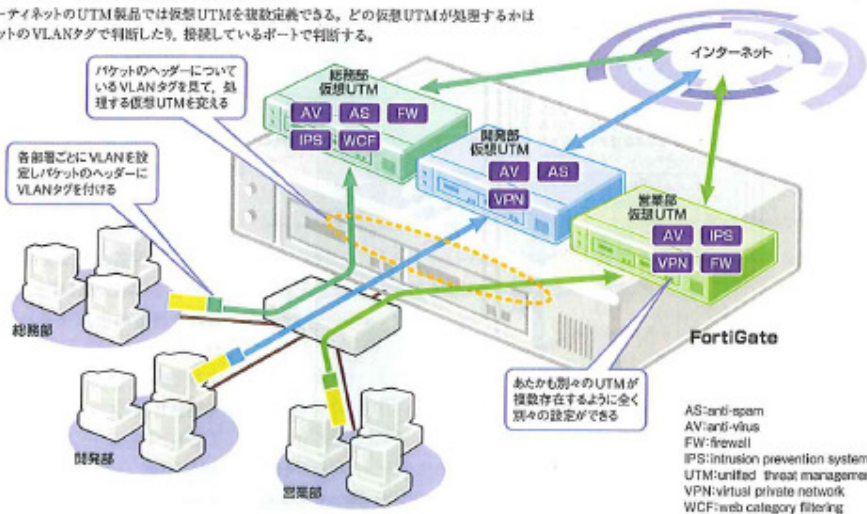
このような方式を採用することで、シャーシ内の能力全体を効率的に利用できることになる。物理的なブレード・サーバーの構成にとらわれずに、その時点で搭載しているすべてのCPUに処理を分散させられるからだ。そのため、ブレード・サーバーを追加していけば、シャーシ全体としての処理能力をリニアに増やせる。搭載するブレード・サー

バーを増やしても、同一のIPアドレスを使い続けるため、外部に登録しているDNSの設定などを変える必要もない。

一つの機器を仮想的に複数に分割
次は図2-1の③で示した「一つの機器の中に仮想的に複数の機器があるように見える」仮想化を見てみよう。こうした仮想化のメリットは、仮想的に複数の機器があるように見せかけることで、一つの機器だけを使いながらあたかも別々の機器を使っているようにサービスを提供できることである。

米フォーティネットのUTMの場合を例に見てみよう。フォーティネットのUTM機器であるFortiGateでは、こうした仮想化の機能を標準で提供している。この仮想化機能を使えば、セキュリティ・ポリシーの異なる部署が存在した場合に、各部署ごとに別々の仮想UTMがあるかのように、物理的には1台のUTM

図2-6 1台のネットワーク機器を複数存在するように見せる
フォーティネットのUTM製品では仮想UTMを複数定義できる。どの仮想UTMが処理するかはパケットのVLANタグで判断したり、接続しているポートで判断する。



を利用できる (p.57の図2-6)。

例えば、総務部には、アンチウイルス、アンチスパム、ファイアウォール、不正侵入防衛 (IPS)、Webカテゴリ・フィルタリングといった五つのUTM機能を一通り有効にする。その一方、開発部ではアンチウイルスやアンチスパムといった最低限の機能だけを有効にし、その代わりに外部から社内ネットに接続するためのVPN機能を有効にして動かす。機能の有効/無効だけでなく、それぞれの仮想UTMで使いたい値の設定を変えるなど設定を細かく使い分けることも可能である。

一つの物理的な機器を、仮想的な複数の機器に見せるネットワーク製品はほかにも登場してきている。

例えば、ノーテルはVSS (virtual switch system) 5000という製品で「仮想ラック」という機能を提供する。これは、文字通り1台のハードウェアの中に複数の仮想ラックを作るというものである。それぞれの仮想ラックに、やはりファイアウォールやIPS、VPNといった機能を個別に乗せて、あたかも別々のラックのように利用できる。

こうして定義した仮想UTMへの通信は、内部ではVLANの機能を活用して使い分ける。具体的には、パケットのヘッダー内に入っているVLANのタグを見て、どの仮想UTMが対象とする通信かを判別して処理している。

例えば、VLANグループ1のタグが付いていれば総務部のパケット、VLAN

グループ2のタグが付いていれば開発部のパケットといったように、UTMの内部で判別した上で、それぞれに定義した処理の内容を実行する。これらのVLANタグは、ノードやスイッチで付けたものをUTMで受け取って処理する方法と、UTMの物理的なポートごとに設定する方法のどちらも可能である。

仮想サーバーに合わせて環境を最適化

最後に、少し毛色の変わった仮想化製品を紹介しよう。Part1で見てきたように、サーバーの仮想化は急速な勢いで広がっている。このサーバーの仮想化を、ネットワーク機器としてサポートしようという製品だ。

米ブレード・ネットワーク・テクノロジーズの「SmartConnect」は、仮想サーバー環境を提供するサーバー群の前に配置する製品である。通信している相手を物理的に接続しているポートだけでなく、やりとりしているMACフレーム内の、あて先や送信元MACのMACアドレスを見て、どの仮想サーバーが通信しているものかを判別する (図2-7)。

SmartConnectには、仮想サーバーのグループごとに「VMビュー」を定義する。例えば、ファイル・サーバーはグループA、データベース・サーバーはグループB、基幹サーバーはグループCといったようにVMビューを設定する。

そして、同じVMビューに関連付けられた複数の仮想サーバーは、ネットワーク上では一つのサーバーに見える。ほかの機器からは同じIPアドレスまたは同じMACアドレスでアクセスできるようにする。その上で、例えば、基幹サーバーにはある程度の帯域を確保するが、ファイル・サーバーにはベスト・

