

ホワイトペーパー

ネットワーク・ソリューションの新たな設計方式 「ダイナミック・サービス・アーキテクチャ」

キャリアクラスの信頼性と可用性を実現しながら、スループットが劇的に向上



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408 745 2000
888 JUNIPER
www.juniper.net

ジュニパーネットワークス株式会社
〒163-1035 東京都新宿区西新宿 3-7-1
新宿パークタワー N 棟 35 階
電話 03-5321-2600
FAX 03-5321-2700
URL <http://www.juniper.co.jp>

目次

エグゼクティブサマリー.....	3
はじめに.....	3
ダイナミック・サービス・アーキテクチャ.....	4
従来のネットワーク・アプライアンスのアーキテクチャ.....	4
ありきたりなシャーシ方式とは一線を画する設計.....	5
スイッチファブリック、制御ボード、ルートエンジンの構成.....	5
サービス処理カード.....	5
I/Oカード.....	6
セッション分散・負荷分散.....	6
パケットフロー.....	7
統一されたモジュール式OS.....	8
ジュニパーネットワークスのサービスゲートウェイ「SRXシリーズ」.....	8
結びに代えて.....	9
ジュニパーネットワークスについて.....	9

エグゼクティブサマリー

新たなビジネスモデルやデータの集中管理に対応するため、ネットワーク管理者は、高度なアプリケーションや動的なサービスの導入を避けて通れなくなっています。しかし、こうした IT 投資の前提として、拡大するネットワークに耐えうる強力なセキュリティ、パフォーマンス、帯域を確保しなければなりません。拡大するネットワーク環境に対応する方法として、従来はアプライアンスやブレードを追加してきました。しかし、この方法では、IT 部門にとって環境が複雑になるばかりで、保守コストも増加の一途をたどります。

新登場の「ダイナミック・サービス・アーキテクチャ」は、並列コンピューティング方式を採用することで、従来のようなサブシステムやファイアウォールがいくつも混在する煩雑さを解消し、単一の強力なソリューションを実現します。この方式であれば、卓越したパフォーマンスでセキュリティサービスとネットワークサービスを実行する業界初のダイナミック・サービス・ゲートウェイが誕生します。また、パフォーマンスの低下を招かずにセキュリティ機能とネットワーク機能の統合環境を柔軟に拡張できるだけでなく、次世代の企業向け・個人向けのサービスやアプリケーションを迅速に導入できるようになります。

始めに

ほんの 1 年前には、一般的なネットワーク機能を考えるときに基準となるのは標準的な Web ブラウザでした。ところが最近ではシステムが大きく変わっています。P2P 通信やビデオ会議、地図閲覧ソフトなどのアプリケーションは複雑化、高機能化が進んでいるため、高速に利用できる可用性を確保しつつ、高度な相互作用を実現する必要があります。例えばビデオ会議の利用が増えただけでも、伝送遅延の許容度ゼロを実現するためにネットワークに負担がかかります。ネットワークを流れるトラフィック量が激増した結果、スループットの需要も爆発的に伸びています。そこで登場したのが、「ダイナミック・サービス・アーキテクチャ」です。これは、拡張性に優れたセキュリティとネットワークの統合機能を搭載し、高度なサービスやアプリケーションの導入を高速化するパフォーマンスを備えた画期的なモデルで、従来のネットワーク構築のあり方をがらりと変える斬新な設計が採用されています。

常に安定した可用性が確保できなければ、文字どおり“一か八か”のサービス提供になってしまいます。例えば、ケーブル TV 大手の米コムキャストでは、トラフィック増加の問題に対処しようと、使用量が飛び抜けて多いヘビーユーザーにトラフィック制限をかけ、不評を買ってしまいました。こうした状況からもわかるように、基本的なトラフィック管理の良し悪しでサービスの成否が大きく左右されます。

同時に、セキュリティ上の脅威、障害、サービス遅延の種類が増え、頻度が高まっており、管理者のきめ細かい対応が不可欠です。グローバルなネットワークへの依存が深まると、従業員や顧客による情報入手が困難になるような問題が起こりやすくなります。しかもこうした問題が大きな広がりを見せているのです。一例を挙げましょう。2008 年 8 月現在、報告のあった情報漏洩件数は、すでに前年の総数を上回る勢いです。個人情報盗難の防止に取り組む米カリフォルニア州サンディエゴの非営利団体 ITRC (Identity Theft Resource Center) によれば、情報漏洩の最大の原因は依然として「悪意ある攻撃」で、侵入者によるデータファイルの違法入手は全体の 13%を占めています。

多くの企業にとって無視できない問題がもう 1 つあります。それは、データセンターの集中化です。IT 部門は常に予算面の責任を負っている一方で、リモートアクセス、セキュリティ、コンプライアンス、管理は一層の強化が求められています。IT 担当者の多くは、この課題に対処するため、複数のデータセンターを統合して集中管理下に置き、保守作業の効率化、コスト削減、二酸化炭素の排出量削減を進めています。しかし、こうした対策の副作用として、ユーザーはインターネットや長距離の社内ネットワークを経由して集中管理下のアプリケーション (CRM、ERP など) にアクセスせざるを得ません。その結果、セキュリティリソース、トラフィックの優先処理、ストレージスペースを巡ってアプリケーション同士が競合し、伝送遅延が増大することもあります。

この原因は、従来のネットワーク設計がキャリアクラスの利用を念頭に置いていないことにあります。そのため、サービスプロバイダ、大企業、無線キャリア、CATV 事業者の間では、高度なインフラのニーズが高まっています。こうした最新型のインフラには、絶えず変化するパフォーマンス要件に対応するため、大容量で拡張性にも優れたセキュリティシステムが必要です。

この問題の解決策の 1 つとして、ネットワーク製品の開発にまったく新しい手法「ダイナミック・サービス・アーキテクチャ」を採用する方法が挙げられます。この画期的な手法により、現行のアーキテクチャ設計から脱却し、最新のネットワークづくりのニーズに沿った斬新なパラダイムが実現します。

ダイナミック・サービス・アーキテクチャ

この画期的な方式が必要になった理由を説明する前に、まず現行のアーキテクチャモデルについて考え、なぜ現行モデルでは近いうちにネットワークを十分にサポートできなくなるのか検証してみましょう。

従来のネットワーク・アプライアンスのアーキテクチャ

速度、処理能力、機能が飛躍的に向上したにもかかわらず、今日のネットワークやセキュリティのアーキテクチャは、IBM のパソコンが初めて登場した 1970 年代から設計がほとんど変わっていません。つまり、PC の心臓部である CPU 自体は、処理速度や処理能力が劇的に高まったものの、その CPU を核に PC を組み立てる際の前提条件が昔から変わっていないのです。アップグレードする場合には、新しい機能を追加するのではなく、搭載 CPU を高速のものに交換します。拡張性については、搭載スロットにメモリや拡張カード（モデムカード、グラフィックカード、ビデオカード、サウンドカードなど）を追加する方法で実現しています。ただし、スロット数が限られているうえ、カード自体の処理速度や最大搭載数が向上しても設計の基本特性は変わりません。

また、こうした従来型アーキテクチャは、現在出回っているほとんどのネットワーク・セキュリティ専用機（アプライアンス）に依然として採用されています。アプライアンスの場合、CPU の搭載数も固定されており、メモリ増設の可能性や拡張スロットの数も限られています。しかも、拡張スロットは I/O インタフェース用に限定されているのが一般的です。このため、多くのネットワーク・アプライアンスにも PC と同様の限界が見られることは、想像に難くありません。特にトラフィック量の多いネットワークに導入すると、この限界が如実に表れます。CPU は限界まで酷使され、処理能力増強の道もなく、あったとしても極めて限定的です。I/O インタフェースも、ネットワークが将来拡大した時のことを考えると、拡張性が十分とは言えません。この結果、導入環境によっては、I/O インタフェースに空きがあっても、CPU がトラフィックのボトルネックになる恐れがあります。逆に、CPU 利用率が低くても、I/O が足りなくなるケースも考えられます。

このような限界を克服する製品として、最近ではブレードシャーシが脚光を浴びました。ブレードシャーシは、筐体内に高速バックプレーンを備えており、ブレードと呼ばれるカードを搭載することで、多彩なセキュリティ機能を実現します。この方式は、ブレードを追加するだけで簡単に機能を増やせるメリットがあります。

しかし、この方には、ネットワーク・アプライアンスと同様の制約がいくつもあります。ほとんどのシャーシは、高速バックプレーン機能の実現を目的に設計されており、搭載したブレードを 1 つの統合システムとして管理する機能はほとんど考慮されていません。つまり、各種カードがただ集まっている状態に過ぎないのです。このため、ブレードの形をした複数のアプライアンスがシャーシという名のシェルに収容されているだけであって、個々のブレードレベルで見ると、依然として処理能力や I/O の制約が残っています。確かに新たにアプライアンスを追加購入することを考えれば、ブレードを追加する方式はあまり手間がかかりません。もっとも、この方式を積極的に選ぶメリットはごくわずかしかなかったり、ありません。

また、ソフトウェア面の拡張性強化に関しても、これまでにさまざまな取り組みが見られました。しかし、このような対策も、大きな成果を発揮するまでには至っていません。というのも、ハードウェア自体がこうした機能をサポートできる設計になっていないからです。このため、ソフトウェアをアップデートすると、システムが動かなくなったり、パフォーマンスが低下したりすることもあります。

このような問題を抱える IT 担当者にとって、唯一残されたソリューションがアプライアンスを追加購入する方法でした。アプライアンスを購入すれば、一定数の CPU やポート数が増えます。こうやって次々にアプライアンスを追加していけば、複雑で拡大の一途をたどるネットワーク環境が生まれますが、これは時間の無駄であり、保守にもコストがかかります。

当然のことながら、ネットワークのセキュリティを強化するために、アプライアンスを際限なく追加し続けることは不可能です。したがって、従来の設計から脱却して、まったく新しい角度からアーキテクチャを考え、拡張性に優れた動的なサービスを提供する環境づくりが重要課題になりました。そこで登場したのが、ダイナミック・サービス・アーキテクチャです。柔軟性と拡張性に優れたシステムを生かし、キャリアクラスの信頼性と可用性を実現すると同時に、スループットも劇的に向上させることができます。

ありきたりなシャーシ方式とは一線を画する設計

ダイナミック・サービス・アーキテクチャは、シャーシ方式をベースにしていますが、従来型のシャーシアーキテクチャとは抜本的に異なります。単に高速バックプレーン機能を搭載するのとは異なり、個々のブレードを統合して全体として強力なソリューションを実現するのに必要な管理機能や制御機能が備わっています。まったく異なる複数のカードがシャーシ内に收容されているのではなく、ダイナミック・サービス・アーキテクチャでは、各ブレードを追加するたびにリソースのプールが大きくなっていきます。このリソースプールの中から、トラフィックに合わせて最適な処理能力を確保します。

スイッチファブリック、制御ボード、ルートエンジンの構成

ダイナミック・サービス・アーキテクチャの心臓部となるのが、スイッチファブリック・制御ボード (SCB) です。この SCB によって、これまではブレードを收容するだけの筐体だったシャーシが、極めて実効性の高いメッシュ型ネットワークに姿を変えます。SCB があることで、シャーシ内の全ブレードは広大な帯域でトラフィックを流せるようになります。

ルートエンジン (RE) は、SCB の機能と高度に統合されており、このアーキテクチャのいわば中枢神経の役割を果たします。シャーシ内の制御プレーンに当たり、システム管理者が利用する総合的な管理・通信機能を担うほか、トラフィックのルーティング処理に用いるルーティングテーブルの計算処理も RE の仕事です。

シャーシの主要機能を担う OS も、この RE 上で動作します。ネットワーク機能やセキュリティ機能については、高度なルーティング、スイッチング、フローベース・セキュリティ、ゾーン別管理、スクリーンなどの機能が OS 上で利用できます。

サービス処理カード

RE がシャーシの中枢神経だとすれば、SPC (サービス処理カード) は脳に当たり、パケット処理という力仕事をこなす能力があります。シャーシ内では、最低でも 1 枚の SPC を動作させることとなります。

特にこの設計は、複数の SPC が搭載されているときに真価を発揮します。従来型のネットワーク・アーキテクチャの考え方であればシャーシに複数の“脳”ができることとなりますが、この設計では違います。SPC を追加した場合、あくまでも 1 つのシステムが大きくなり、単位時間内に処理できる仕事量が増えるのです。

この点は、ダイナミック・サービス・アーキテクチャが従来型アーキテクチャと決定的に異なる主要な特性の 1 つと言えます。ネットワーク管理者にとっては、ブレードごとに特定の仕事を処理するよう設定する必要がなくなります。システム自体は 1 つのままシャーシの処理能力を増やせるため、管理の手間を増やすことなく全体的な処理能力を連続的に拡張できます。

さらに、最高水準の信頼性を確保するため、SPC と RE は物理的にも論理的にも完全分離されています。つまり制御プレーンとデータプレーンを分離することにより、万が一いずれかの SPC が故障した場合でも、シャーシ全体の壊滅的な障害にはつながりません。

この方式は、DoS 攻撃などセキュリティ上の脅威に対しても強さを発揮します。攻撃が仕掛けられている最中でも、管理者によるシステム操作は通常トラフィックと一緒にされないため、即座に対応が必要な状況にもかかわらず、攻撃で急増しているデータと競合するようなこともありません。制御プレーンがトラフィックフローから切り離されているため、ネットワークが脅威にさらされたときに即座に対策を講じ、攻撃を阻止することができます。同時に、すべての SPC でネットワーク・トラフィックの処理が継続されます。

I/O カード

ダイナミック・サービス・アーキテクチャのシャーシスロットは、カードの種類を問わないという特長があります。ニーズに応じてシャーシ自体の限界までアーキテクチャ構成を自由に設定できます。例えば、軍事施設のように大きな処理能力が必要な組織では SPC が多め、I/O カード (IOC) が少なめの構成になるはずですが。一方、サービスプロバイダであれば、加入者のトラフィック用に I/O を多く確保し、生データ処理能力は少なめになります。ビジネス上の要件が変化したときには、IOC と SPC を手軽に追加してアーキテクチャの構成を自由に変更できます。

このようにスロットに制約がないため、IOC を自由に増減できます。空きスロットの数だけシャーシに IOC を搭載可能です (ただし、最低 1 スロットは SPC が必要)。その名のとおりダイナミックな特性を備えたアーキテクチャのため、新セッションが始まると、リアルタイムに各セッションを SPC に自動的にマッピングして処理します。

セッション分散・負荷分散

ダイナミック・サービス・アーキテクチャは、セッション分散方式に基づく高度なパフォーマンスと容量を備え、自動負荷分散に対応しています。これを可能にしているのがインテリジェントな IOC プロセッサ (前述の“脳”の部分) で、セッションの負荷を SPC の共用プール内で分散します。システム内の SPC はすべて同じサービスを実行し、同じ設定になっているからこそ、このような処理が可能なのです。IOC と SPC を 1 対 1 でマッピングする必要はありません。セッション生成時に個々のフローが動的にマッピングされるのです。

実際、SPC が 1 枚しか搭載されていない場合でも、ファイアウォール、VPN、侵入防御システム (IPS)、ルーティング、QoS、NAT などのあらゆるサービスを実行できます。さらに、SPC を追加すれば、システム構成を変更することなく、パフォーマンスと容量を増強できます。

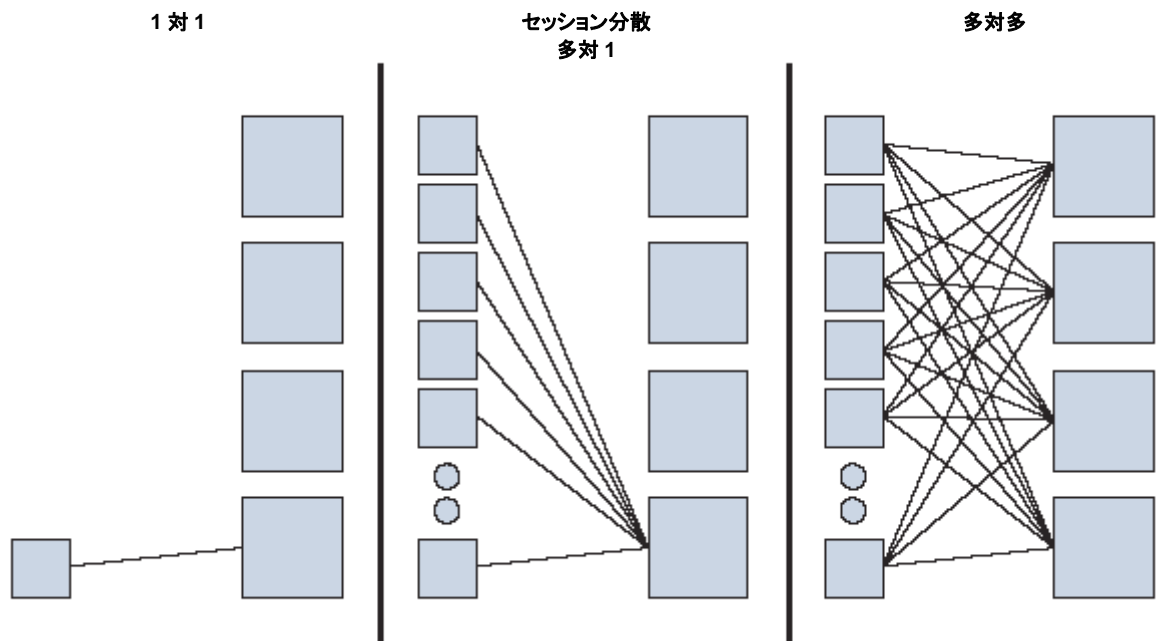


図 1: 基本的なセッションベースの負荷分散

例えば、図 1 の左側の構成(1 対 1)では、1 つの IOC と 1 つの SPC が対になってパケットを処理します。パケットは、この IOC から SPC に送出され、再び IOC から送り出されます。

図 1 の中央の構成(多対 1)では、複数の IOC があるものの、すべて 1 つの SPC に接続されています。この場合、システムは自動的に全 IOC からのトラフィックをすべて SPC に送り、別のポートからトラフィックを戻します。

一番右の構成(多対多)では、複数の SPC(図では 4 つ)にインテリジェントにセッションを分散させます。どのポートに入ってきたセッションであっても、セッションごとにシステム内の任意の SPC に転送できます。

この負荷分散は自動的に実行されるため、システム管理者による設定変更や監視は不要です。この仕組みとまったく逆なのが、従来のシャード型ソリューションで、各処理ブレードが独立したファイアウォールになっており、別々のトラフィックを扱い、設定やルーティングサポートもそれぞれに用意されます。

パケットフロー

ダイナミック・サービス・アーキテクチャでは、パケットフローも完全に統合されていて、管理もはるかに簡略化されています。管理者にしてみれば、トラフィック管理に関して、ブレードごとに別々の指示を与える必要がありません。システムを通過するパケットは、下記のように、基本的に共通の経路を通るからです。

1. 受信パケットは IOC のイーサネットポートに入ります。
2. IOC で処理された後、スイッチファブリックに渡されます。
3. SPC 上の 1 つの処理ユニットがパケットを受け取って、ファイアウォール、IPSec VPN、IPS などの処理を実行します。パケットを破棄する場合には SPC が処理し、通常はイベントをログに記録します。
4. パケットを通過させる場合には、スイッチファブリックを経由して IOC に渡します。その後、IOC プロセッサで処理し、必要に応じて QoS を適用します。
5. 次にイーサネットポートにパケットが送られ、システムから送出されます。

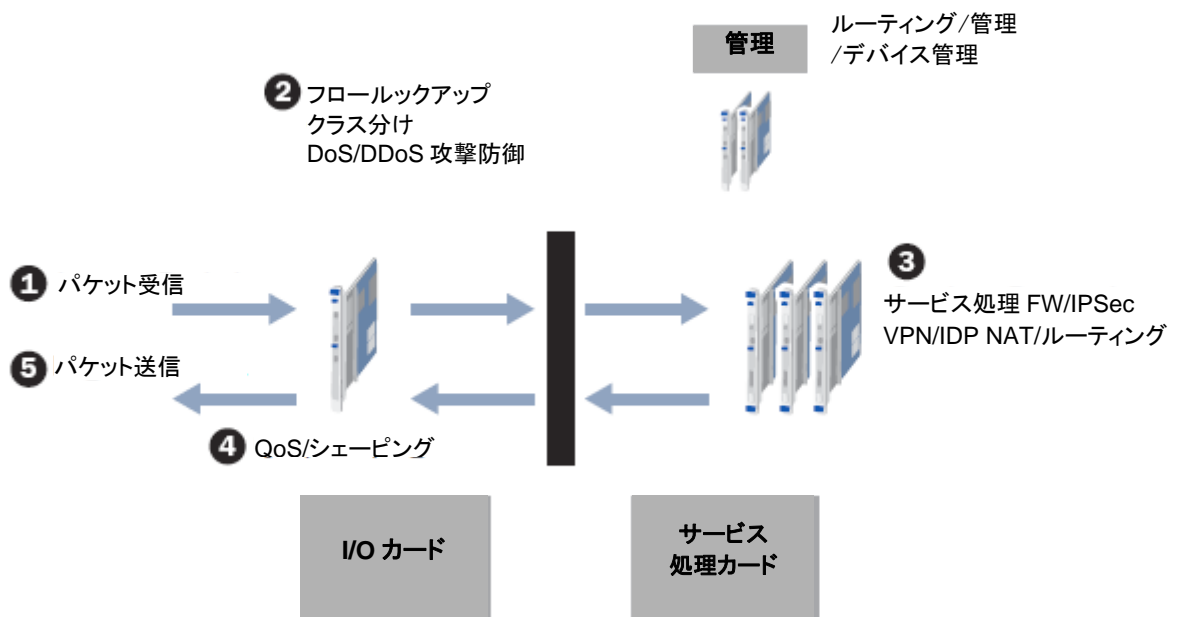


図 2: パケットフローの完全統合の例

ダイナミック・サービス・アーキテクチャでは、ポートとデータパケットの関係が一切固定されていないため、卓越した柔軟性を発揮します。問題のないトラフィックであれば、非常に高速に連続して流すことができます。さらに重要なポイントとして、SPCを追加しても、トラフィックの設定を変更する必要がなく、迅速な導入、管理作業の軽減、ネットワーク上でのトラフィック処理能力の低下防止につながります。

統一されたモジュール式 OS

ダイナミック・サービス・アーキテクチャは、ネットワークの統合管理に対応したモジュール式 OS を使用します。この OS には次のような特長があります。

- 1 つのソースコードに基づく統一性の高い OS—シャーンからルーティングまで、デバイス間で共通のツールを使って各種機能の設定・管理が可能のため、ネットワーク全体の監視・管理・アップデートが可能です。また、新機能の導入、ソフトウェアのアップグレード、その他の修正・変更作業が簡素化され、トレーニング時間の短縮やコスト削減につながるため、IT 部門の業務の効率化に寄与します。
- 厳格な品質基準と検証に基づき、開発時に新機能を安定的に実装できる定期的なリリース体系（リリース計画）—新バージョンは必ず前バージョンの完全な上位セットになっているため、前バージョンからの機能は新バージョンでも安定動作が保証されます。さらに、新バージョンはすべてのルーターとスイッチを対象に同時にリリースされます。この結果、予測不能な事態やサービス停止のリスク、コストのかかる検証作業、計画外の保守やアップグレードの面倒な事態を回避できます。
- 複数の機能を搭載しても柔軟性と安定性を両立する画期的なモジュール式アーキテクチャ—効率的な開発をサポートし、耐障害性やフェイルオーバーを強化します。問題点の切り分けが容易なため、迅速なトラブル・シューティングと問題解決が可能になり、高可用性を実現します。この結果、稼働率が向上すると同時に、攻撃プログラムや攻撃メールが広がるのを防止します。

このようなモデルでは、新機能の開発やソフトウェアのアップグレードが簡素化され、管理作業上のミスの発生を抑えることができます。また、定型作業の自動化ツールが用意されており、ダウンの可能性が大幅に排除され、管理作業の無駄もなくなります。

ジュニパーネットワークスのサービスゲートウェイ「SRX シリーズ」

ダイナミック・サービス・アーキテクチャを採用する代表的な製品として、ジュニパーネットワークスから新発売のサービスゲートウェイ「SRX シリーズ」があります。「SRX 5000 シリーズ」は、並列コンピューティング・アーキテクチャを用いた統合インフラとなり、従来のように複数のサブシステムが混在する複雑な状況から脱却できます。あくまでも 1 つの強力なシステムのため、新型の高度なネットワーク・セキュリティ管理機能をいち早く利用できるだけでなく、パフォーマンスの飛躍的な向上も期待できます。

SRXシリーズは、シングルソースに基づくモジュール式ネットワークOSとして定評あるジュニパーの「JUNOS®ソフトウェア」を採用しています。他社製品と異なり、統一されたOS、バージョンの分岐・派生のない一貫した機能強化、単一のモジュール式アーキテクチャに基づく開発方針を特長としています。このように効率的で無駄のない手法を採用するメリットは明らかです。例えば、先頃、米調査会社レイクパートナーズが 120 社以上のネットワーク事業者を対象に実施した調査によれば、JUNOSソフトウェアを利用する事業者の多くは、競合製品を利用する事業者に比べて、一般的なネットワーク運用の作業にかかる時間が平均 25%も短いことがわかりました。さらに、トラブル・シューティングや突発的なイベントへの対応にかかる時間もJUNOSソフトウェアのほうが平均 54%少ないことが明らかになっています。

SRX 5000 シリーズの特長

- ベンチマークテストでファイアウォールのスループットは 100Gbps 以上、IPS のスループットは 30Gbps を達成し、業界最高のパフォーマンスを誇るセキュリティ・ソリューションの座を獲得
- 最新のアプリケーションのセキュリティ確保に不可欠なセッション数と高速セットアップをサポート（同時セッション数 400 万、接続セットアップ速度は 35 万/秒）
- ファイアウォール、IPS、バーチャル VPN、DoS 攻撃ブロックングサービス、NAT、QoS をネイティブに統合
- キャリアクラスの信頼性と可用性を実現

SRX シリーズの設計がもたらすメリット

- 拡張性とパフォーマンスが飛躍的に向上
- モジュール式アーキテクチャに基づく柔軟性が高まり、IT 担当者の操作性が向上し、作業負担も軽減
- アプリケーションのパフォーマンスとユーザーの使い心地が向上
- 統一アーキテクチャで単一のネットワーク OS を実行するため、TCO が減少

結びに代えて

ダイナミック・サービス・アーキテクチャは、拡張性に優れたセキュリティとネットワークの統合機能を搭載し、高度なサービスやアプリケーションの導入を高速化するパフォーマンスを備えた画期的なモデルです。従来のネットワーク構築のあり方をがらりと変える斬新な設計が採用されています。

柔軟な拡張性、高度な統合環境、卓越したパフォーマンスを特長とする SRX シリーズは、ダイナミック・サービス・アーキテクチャならではのメリットが見事に活かされています。IT 部門にとっては、常に安定した拡張性と優れたパフォーマンスを引き出し、管理も手間がかからず、しかも総合的なセキュリティ環境をユーザーに提供できます。さらに、業界トップクラスのパフォーマンスを維持しつつ、運用コストを削減し、IT 投資を最大限に生かすことができます。

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、ハイ・パフォーマンス・ネットワーキングのリーダーです。サービスおよびアプリケーションの一元化されたネットワークにおける展開を加速するのに不可欠な、即応性と信頼性の高い環境を構築するハイ・パフォーマンスなネットワーク・インフラストラクチャを提供するジュニパーネットワークスは、お客様のビジネス・パフォーマンスの向上に貢献します。ジュニパーネットワークスに関する詳細な情報は、以下の URL でご覧になれます。www.juniper.co.jp

Copyright © 2008, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Juniper Networks のロゴは、米国及びその他の国の Juniper Networks, Inc. の登録商標です。その他記載されているすべての商標、サービスマーク、登録商標、登録サービスマークは、各所有者に所有権があります。これらの仕様はすべて予告なく変更される場合があります。本資料の記載内容に誤りがあった場合、あるいは記載内容を更新する義務が生じた場合も、ジュニパーネットワークスは一切責任を負いません。ジュニパーネットワークスは、本発行物を予告なく変更、修正、転載、または改訂する権利を有します。