Solution Brief

Migrating to Next Generation WANs

Secure, Virtualized Solutions with IPSec and MPLS

Migration Drivers for Ethernet and Virtual Private Networking

During the last several years, telecommunications growth has fueled demand for new solutions to increase performance while retaining the services offered with legacy technologies. These solutions must provide better and more dynamic control, richer feature content, and wider connection possibilities—while lowering the cost of implementation and operation. They must also integrate with other services, such as voice, video, Internet, Intranet/Extranet, ERP and other business applications.

Ethernet has emerged as the top choice for both an access technology and a WAN technology, replacing traditional ATM and Frame Relay (FR) access and WAN connectivity. FR and ATM technology is highly secure and reliable, and provides adequate QoS, yet is less flexible and generally more costly than Ethernet. Enterprises appreciate the higher bandwidth of Ethernet, and the fact that it is a familiar technology, optimized for IP and pervasive in the campus.

Virtual Private Network (VPN) options for next-generation WANs are secure enough to replace existing FR/ATM circuits, and are much more flexible and scalable. Next generation WANs reduce circuit costs with traffic consolidation; this includes a reduction in both the circuit count and the cost per megabit. Next generation WANs also reduce the number and types of network equipment and operating systems that must be supported, simplifying troubleshooting and IT support. The useful life of equipment can be extended due to scalability and a flexible feature set.

These benefits come from the ability to both encrypt (with IPSec) and virtualize (with Multiprotocol Label Switching or MPLS) the core network and separate its resources into discrete domains. Figure 1 illustrates virtualization in an MPLS network. MPLS VPNs (controlled by Virtual Routing and Forwarding tables or VRFs) across a core network map to VLANS or IPSec tunnels (which could in turn map to virtual routers or firewall zones) in the local loops to the enterprise sites. In Figure 1, the red and blue services are kept separate with the same reliability as if they were on different physical media.

Most enterprises can realize these benefits using existing WAN links, making these links instantly more useful. WAN connections can also be upgraded to take further advantage of the performance capabilities and scalability of these solutions.

Allowing the WAN to extend virtual security domains across the enterprise is a great competitive advantage, and MPLS VPNs are the ideal way to achieve this. Enterprises have long recognized the need to virtualize their networks, and many large enterprises carry hundreds of VLANs across their campus to keep services separate. VLANs are very useful in the campus, but they do not scale well, and are often difficult to manage. Extending policy-controlled security zones across wide area networks and enhancing the manageability of these zones with routing is a more secure and manageable solution than simply extending VLANs.

Juniper's virtualization solution for the WAN uses firewalls with virtual routers (VRs) and MPLS-optimized routers with Layer 3 VRF tables to propagate security domains. This solution allows you to maintain firewall policy between zones to control access between routing domains in specific predefined regions.

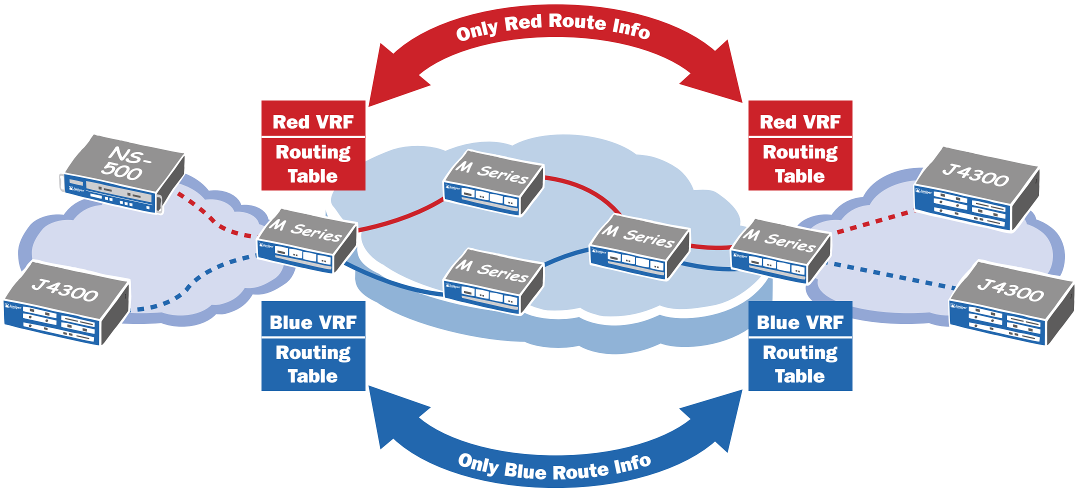

Figure 1: Virtualization with a Layer 3 (MPLS) VPN Network

Value Propositions for Next Generation WANs

Next generation WANs take you from the static, separate networks of FR and ATM into a consolidated and more flexible environment based on Ethernet and IP. Consolidating your traffic on a single network reduces circuit costs. Many financial institutions, health care companies and other enterprises have realized huge benefits in both circuit counts and bandwidth costs.

You can realize these benefits without wholesale changes to the existing network. For instance, many enterprise IT shops need to be more conservative about making changes, and they might want to keep their current access links, yet migrate on these links to a site-to-site IPSec VPN. This will offer them better use of their current WAN bandwidth. Application optimization, such as that offered by Juniper's WX and WXC application acceleration platforms, provides optimal use of their links.

With IPSec VPNs, mission-critical data is protected with cryptography. This solution offers low capital costs by leveraging the Internet and provider security for remote users from trusted endpoints. IPSec VPNs provide a centralized user security policy and have a unique high availability option in the form of dynamic route-based VPNs.

Other companies will be more aggressive about being able to upgrade their access links and WAN routers. For them, moving more quickly to MPLS solutions may make more sense, optionally partnering with a service provider to find the ideal solution.

The most pronounced benefits have been noted in organizations that can lease circuits and provide their own MPLS support. This reduces labor costs for operations and maintenance. The number of devices is reduced and the ability to support the network is greatly simplified. The useful life of equipment can also be extended due to the scalability of a converged MPLS network.

Flexible VPN Options from Juniper Networks

The next generation WAN employs VPNs using both IPSec and MPLS:

- IPSec VPNs optimize current WAN bandwidth and enhance overall security and reliability
- MPLS VPNs support next generation core routing capabilities
- Hybrid solutions provide additional flexibility and value.

MPLS is used to support a number of additional capabilities that are not provided by IPSec:

- Virtualization, to provide transparency for independent virtual network operation, including Layer 2 or Layer 3 VPNs to maximize flexibility
- Support for convergence and consolidation by enabling carrier-class routing protocols, different QoS policy sets, policy control on the high-speed backbones, and the collapsing of ATM infrastructures to dramatically reduce the quantity of connections
- Provision of high availability by including deterministic parallel paths and fast reroute options with 50 millisecond failover

Juniper Networks provides full MPLS implementations in which all capabilities are available to service providers.

IPSec is managed using the Juniper Networks VPN Monitoring capability, and the Layer 3 MPLS core can be deployed and managed either by enterprise IT staff or with a partnering service provider. Although IPSec is more commonly associated with the enterprise, and MPLS is generally a service provider technology, these are not in fact competing solutions. For instance, a service provider can bundle IPSec as a value-added service, either encrypting between provider edge (PE) devices or from the customer edge (CE) to the PE device, to protect the local loop.

Figure 2 shows the array of possibilities: the IPSec VPNs can run on all link types, and the encapsulation can be between either PE or CE devices.

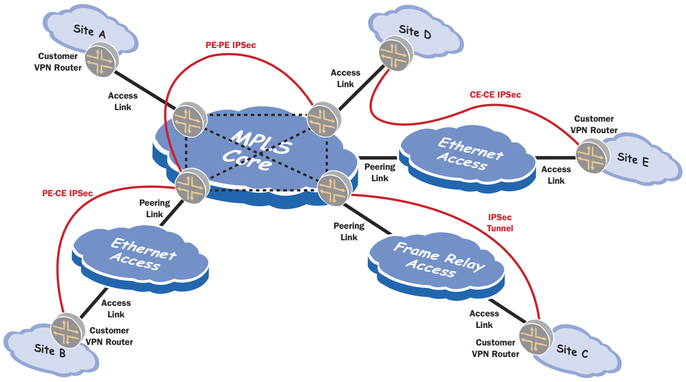

Figure 2: Layer 3 VPN and IPSec Tunnel Scenarios

Conversely, an enterprise customer can still run IPSec tunnels on top of the Layer 3 VPN. This decouples the routing from the security (providing virtualization) and provides policy-based IPSec and QoS for the encrypted traffic.

The following hybrid solution illustrates IPSec running over MPLS.

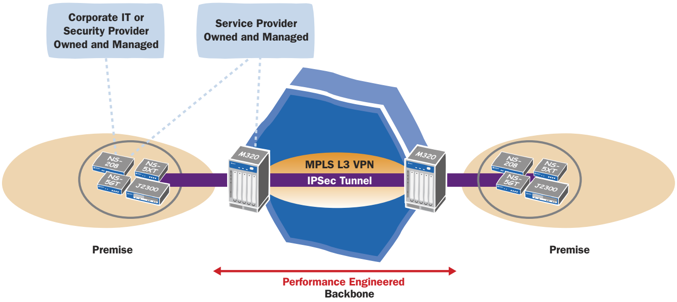

Figure 3: IPSec over MPLS

In this solution, enterprises can use IPSec to tunnel into the service provider network, and then these encrypted tunnels are routed through the service provider infrastructure over an MPLS VPN. This type of deployment is ideal when enterprises have very stringent requirements for security, and want not only traffic separation but encryption as well.

There are two possible deployment scenarios. The first is where the service provider owns and manages the CPE equipment as well the PE routers in the network infrastructure. The service provider configures and maintains the mesh of IPSec tunnels. In the second scenario, the service provider owns the PE router, and the enterprise (or a third party such as a security provider) owns and manages the CPE routers.

In the following hybrid VPN, the IPSec connections terminate on the router that begins the MPLS VPN connection. Again, notice that either the service provider or the enterprise can be managing the equipment on either end of the IPSec tunnel.

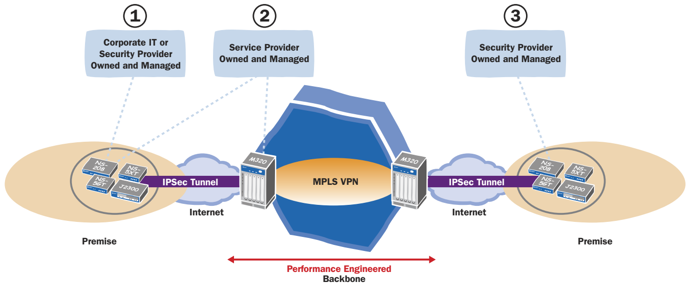

Figure 4: Hybrid VPNs, IPSec into MPLS VPN

This solution illustrates a variation with IPSec VPNs and MPLS VPNs deployed in a hybrid scenario. In this example, the enterprise has IPSec tunnels running from the CPE to the PE router in the service provider's network. The customer's data is then transported over the service provider's backbone in an MPLS VPN.

Selecting VPN Options

As the preceding discussion illustrates, there are a variety of factors that will play into the VPN choices for the next-generation WAN. The following table provides some high-level guidelines on how to choose the right VPN for different enterprise requirements.

Platforms	Site Characteristics
Pure MPLS VPN Solution	A large number of sites, thus the need to scale routing Willing to outsource, not interested in building in-house expertise
Pure IPSec VPN Solution	Strong security requirements In-house IP and security expertise No specific QoS expectations from the provider
Hybrid: MPLS/IPSec Solution	Large scaling requirements that push customer to a network based VPNs Decoupling (virtualizing) routing and security provides better scaling of CPE control plane Policy based IPSec (not every site or application needs it) QoS requirements

Of course, the requirements are in fact more diverse than this, as the following figure shows.

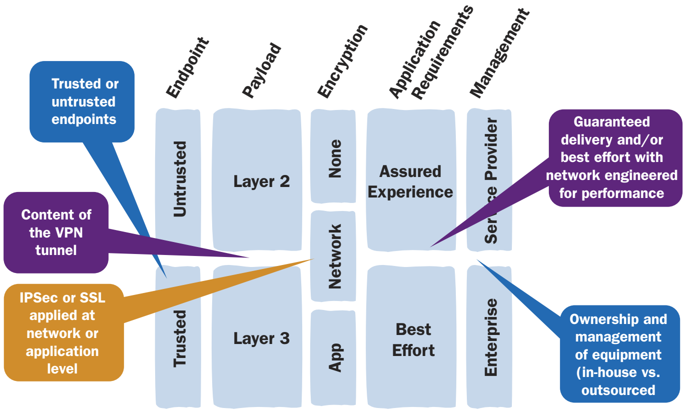
Endpoint
Payload
Encryption
Application Requirements
Management
Trusted or untrusted endpoints
Content of the VPN tunnel
IPSec or SSL applied at network or application level
Untrusted
Trusted
Layer 2
Layer 3
None
Network
App
Assured Experience
Best Effort
Service Provider
Enterprise
Guaranteed delivery and/or best effort with network engineered for performance
Ownership and management of equipment (in-house vs. outsourced)

Figure 5: Diverse Requirements

The choice of a next-generation WAN incorporates a diverse set of requirements to meet current and projected future user needs. These requirements are specifically related to the presence of different endpoint types (trusted or untrusted), payload visibility (Layer 2 or Layer 3), need for encryption (none, network level or application level), application types (best effort or assured experience) and management (enterprise or service provider) provisions.

There is no one right answer, but these considerations give you some good rules of thumb to help choose the right technology for your needs.

Key Components of the Juniper Solution

Juniper's IP VPN solution for WANs includes a number of key components, which collectively enable optimization of its overall effectiveness:

- Availability of a comprehensive suite of products that enables Juniper to offer the broadest VPN portfolio in the industry
- Full support for MPLS in the service provider and enterprise networks
- Design of IPSec support into all Juniper platforms to facilitate network and remote access user protection
- Incorporation of flexible security provisions, including firewalls, antivirus protection and Intrusion Detection and Prevention (IDP)
- Use of carrier-class routing protocols, HA features, and QoS/CoS
- Use of WX/WXC Application Flow Acceleration products (see below)
- Incorporation of flexible management tools, such as J-web and JUNOScript for JUNOS device management, and NetScreen Security Manger (NSM).

Juniper products contributing to a next generation WAN include:

- MPLS Support: M- and J-Series series routers, and NetScreen Firewalls
- IPSec Support: All NetScreen ScreenOS Devices and Firewalls, J-series support with license, M-series support through ASP and the ASM (M7i)

Implementations

Juniper Networks has implemented a large next-generation WAN solution for a number of major retailers. Although there are several reference designs for this solution, a typical one is shown in the Figure 6.

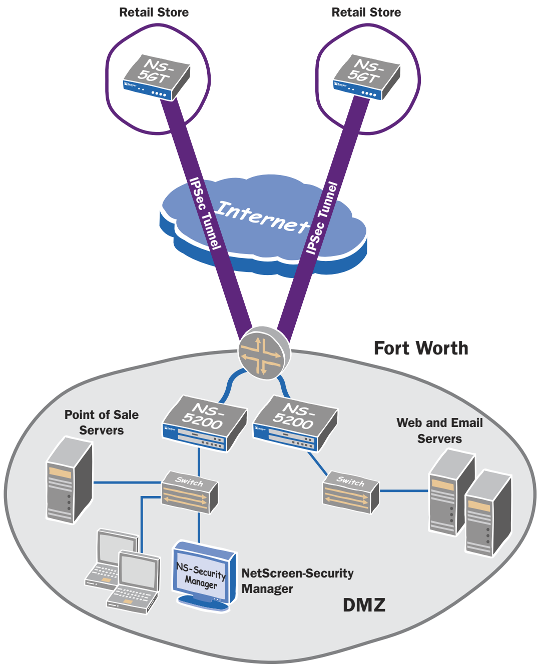

Figure 6: Retail Reference Design for CPE-Based IPSec

This scalable solution offers VPN services and Anti-Virus protection. The network leverages the primary benefits of IPSec (data protection, security, reliability, low capital cost, etc.) and capitalizes on a number of related advantages. The additional advantages that are provided by the Juniper solution include service assurance (VPN monitor), virtualization (virtual routers and zone architecture), flexibility (dynamic VPNs and dual untrust) and management (NSM).

The following application is an excellent example of where it is appropriate to implement MPLS in the core. This university application, with far-flung campuses and numerous departments, needed high performance routing, a separate VRF for each department, and the ability to delegate administrative control.

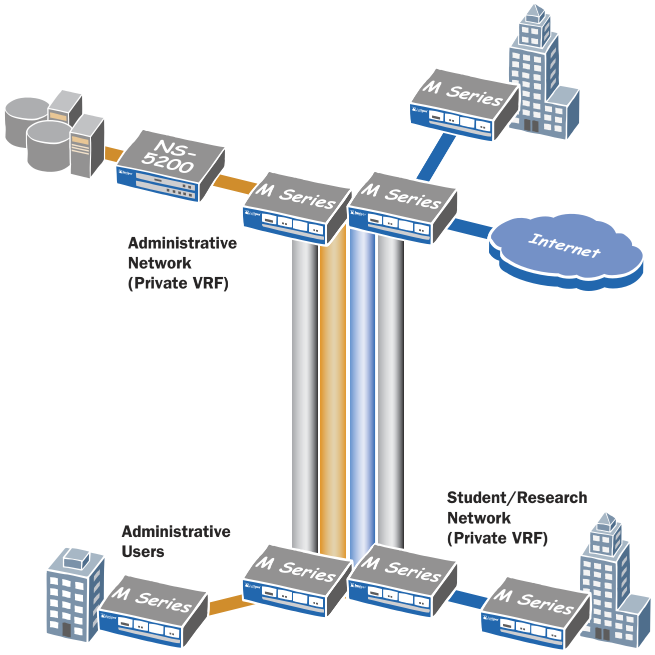

Figure 7: MPLS Core for University Application

This network requires policy-based security, which is enforced by a firewall. Since data confidentiality is not a primary concern, IPSec is not implemented (however, it can be added later while maintaining the MPLS core).

For another next-generation WAN example, see the For More Information section below.

Application Acceleration: WX and WXC Platforms

Juniper has application acceleration products – the WX and WXC platforms – to improve the performance of WAN links whether or not a full next generation WAN can be implemented. Of course, these technologies greatly improve the performance of the next generation WAN as well. They increase the speed of applications across the WAN by performing compression and caching, TCP and application-specific acceleration (Microsoft Exchange, file services, Web services) and QoS along with other application control mechanisms.

These platforms enable enterprises to deliver superior quality application performance over the WAN. The WX hardware and software is optimally used for increasing WAN capacity, accelerating transmission, facilitating QoS implementation and bandwidth allocation, and supporting intelligent multipath operation.

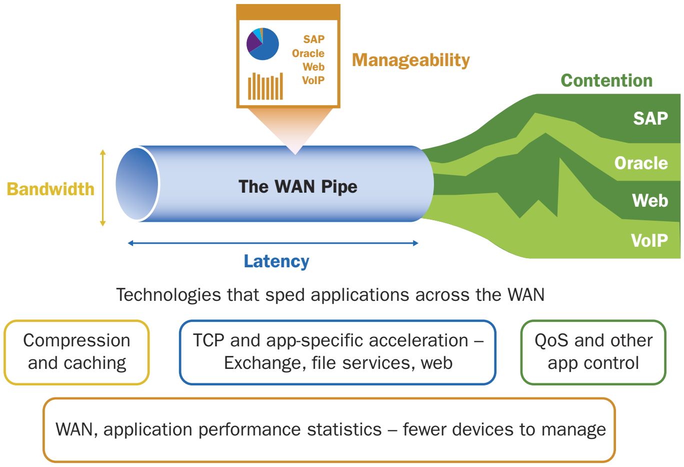
SAP
Oracle
Web
VoIP
Manageability
Contention
SAP
Oracle
Web
VoIP
Bandwidth
The WAN Pipe
Latency
Technologies that sped applications across the WAN
Compression and caching
TCP and app-specific acceleration – Exchange, file services, web
QoS and other app control
WAN, application performance statistics – fewer devices to manage

Figure 8: Improving Application Performance across the WAN with WX/ WXC Platforms

Infranet Initiative and the Enterprise Infranet

The Next Generation WAN is an integral part of Juniper's Infranet Initiative. This effort merges business and network demands so that business-critical services can be profiled by both enterprises and consumers, and can thus be delivered profitably to end users by enterprise network IT and network operators.

Enterprises in particular are demanding more out of their network infrastructure. They need their networking environment to support and optimize services that meet the different needs of all their users, so they can improve productivity and gain a competitive edge. Towards this end, Juniper has developed a reference architecture for an Enterprise Infranet, enabling enterprises to create an IP infrastructure that coordinates network, application and endpoint intelligence to control network traffic -- providing secure and assured delivery of applications.

For more information on the Enterprise Infranet, see the white paper entitled An Architectural Framework to Achieve an Enterprise Infranet at:

http://www.juniper.net/solutions/infranet

Conclusion

Juniper Networks provides an ideal solution set for next-generation WAN design and implementation:

- Comprehensive IPSec VPN solutions
- Industry-leading MPLS solutions
- Support for industry standards
- All key components needed for successful WAN implementation
- Flexible WAN optimization products for improving application performance

Juniper Networks leads the industry in providing a complete portfolio of products needed for creating advanced, reliable next-generation WANs. Customers can be assured that this comprehensive product base and Juniper's services capabilities will enable us to provide the most cost-effective, flexible and future-safe WAN solutions available.

For More Information

For a detailed reference design of a proven next generation WAN, see the application note entitled *Building a Secure and Virtualized Enterprise Core* at:

http://www.juniper.net/solutions/literature/app_note/350068.pdf

This tutorial describes a distributed enterprise core network that utilizes IPSec and MPLS to create a scalable secure virtualized core that can run any number of wide area services. The design illustrates the integration and virtualization capabilities of both the JUNOS and the ScreenOS operating systems, and details the seamless interoperability of security zones, virtual routers, and VRFs. The use of an MPLS core eliminates any scaling restrictions while retaining all the requisite security needs of the services.

The diagram for this network is shown in Figure 9; the application note details its configuration, and discusses how to build a next-generation WAN.

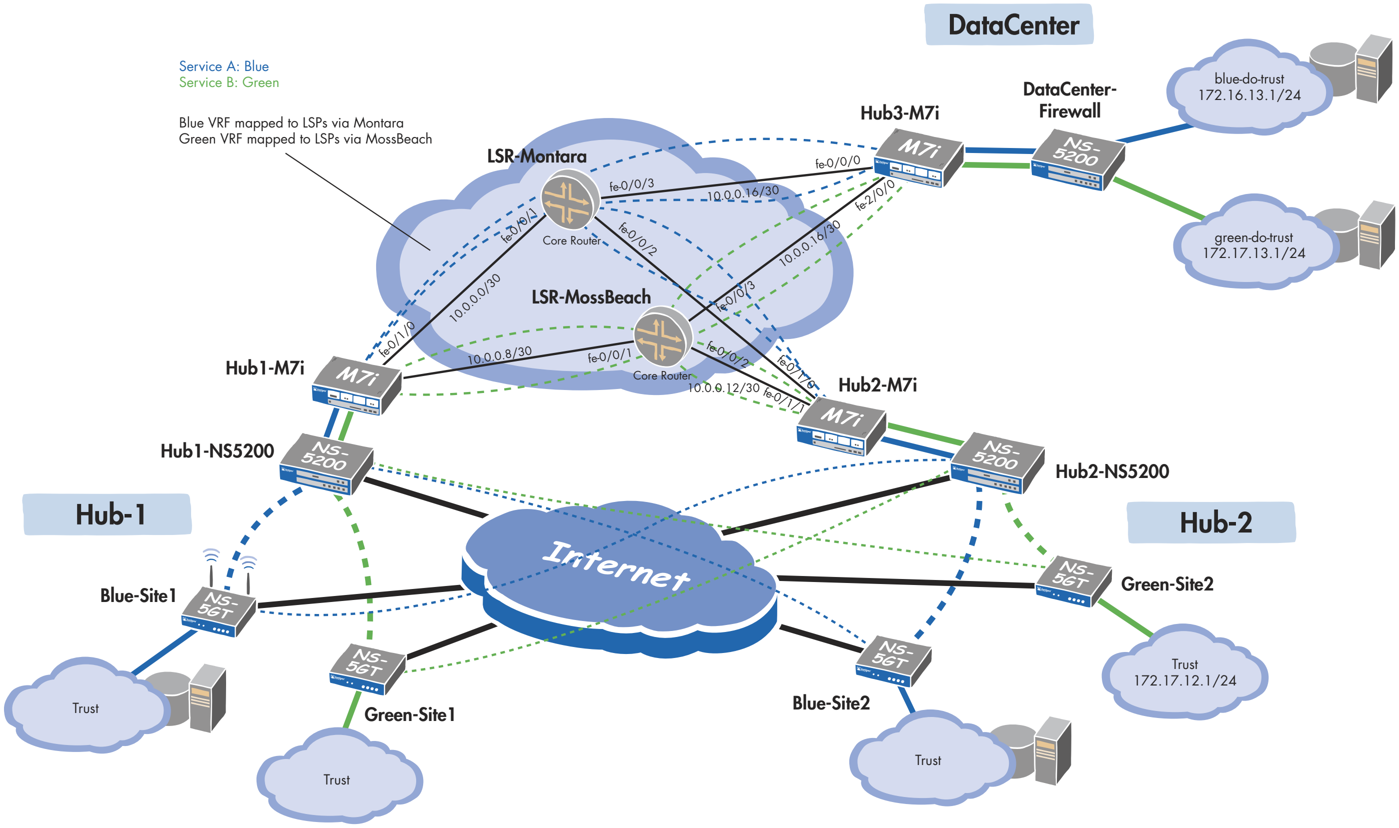

Figure 9: Secure and Virtualized Enterprise Core

Juniper® NETWORKS

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100

www.juniper.net

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

351108-001 July 2005