Solution Brief

Secure and Assured Networking for Financial Services

Introduction

To increase competitiveness, financial institutions rely heavily on their networks to connect customers, employees, partners and suppliers to a range of internal applications. They are under constant pressure to ensure that these internal applications and data are always available and highly secure. Internal business initiatives and external regulations are adding to these challenges and are testing the capabilities of status quo networks. Though these networks were adequate in the past, they may no longer provide the level of service required for ongoing competitive advantage in the face of new business initiatives and regulatory compliance obligations. Juniper Networks is working with financial institutions worldwide to implement changes to their networks that enable application assurance and security as required by business initiatives including:

- Regulatory compliance
- IP Telephony
- Secure VPN initiatives
- Web applications and Web services
- Infrastructure consolidation and virtualization

Financial institutions use Juniper Networks' industry-leading routing, security and application acceleration solutions to update their networks to accommodate these new initiatives. Yet adding new applications and updating networks involves risk, including the exposure to new security issues, unplanned downtime and network conflicts. Mitigating risk requires an architecture that can deliver network predictability, pervasive security and application control. Juniper Networks offers a unique architecture for providing these benefits – the Enterprise Infranet – which enables financial institutions to secure and assure delivery of their most critical applications.

Enterprise Infranet

The foundation of secure and assured networking, the Enterprise Infranet, is an IP infrastructure that coordinates network, application and endpoint intelligence to control traffic across the entire network.

Enterprise Infranets operate as a service layer on top of the existing infrastructure, allowing financial institutions to deliver secure and assured applications over advanced networks while protecting their infrastructure investments.

Though there are a variety of products and solutions that comprise the Enterprise Infranet, benefits are delivered in three categories of capabilities: Delivery Control, Use Control and Threat Control.

Delivery Control

Delivery Control describes how network traffic is delivered, specifying the required levels of performance, predictability and integrity. It includes high availability, fault tolerance, quality of service, privacy and integrity of the connection.

Use Control

Use Control defines what network traffic is allowed or not allowed to traverse the network and explicitly dictates how the network, the application and information resources can be used and implicitly denies everything else.

> *"The Juniper Networks firewall is solid as a rock."*
>
> **Mark Price**
> **Commerce Bank**
> **Information Security Consultant**

Threat Control

Threat Control describes how traffic that is identified as malicious, behaving inappropriately or causing disruption to the network, is removed from the allowed traffic.

IP Telephony

Situation

Financial institutions are turning to IP telephony to reduce costs and enhancing productivity. Frequently, evaluation focuses on the PBX and handset features and does not consider the increased requirements for QoS and availability on the WAN. Additionally, installed networks often do not protect IP Telephony from traditional data attacks, or new IP telephony-specific abuse.

Solution

Juniper Networks delivers a standards-based approach that interoperates with best-in-class third-party hybrid/IP PBXs to create IP telephony solutions providing:

- Highly available voice service through stable systems, redundant hardware configurations and multiple network level resiliency mechanisms for fast sub-second recovery times
- Quality voice through high-performance designs that deliver predictable low latency and low jitter while performing complex packet processing functions as filtering, scheduling and voice encryption
- Secured voice from layered security to protect the network from voice related DoS exploits like multiple call requests from a single user, and voice-aware Application Layer Gateways (ALGs) for SIP and H.323 that allow only authorized sessions while limiting unauthorized use and exposure to threats
- Reduced bandwidth requirements through optimization of WAN capacity up to 70% and prioritization of voice

Network Predictability

According to Infonetics research, annual downtime and degraded service costs financial institutions an average of 16% of revenue in lost revenues and lost productivity. Gartner estimates that each hour of downtime can cost upwards of $6.45 million. Because of these incredibly high costs, financial institutions must ensure that applications are always available irrespective of internal downtime, malicious attack or external disaster. Furthermore, providing a high level of service is critical to remaining competitive. Poor performance and delays can cost financial institutions enormously in lost productivity and can drive away customers. Given the high total lifetime value of customers to many financial institutions, customer defections and negative publicity can result in long-term damage to the organization.

Network predictability – comprising high availability, high performance and network intelligence – is a hallmark of Juniper Networks solutions. Juniper Networks Delivery Control capabilities enable financial institutions to provision each network segment the appropriate high availability and resiliency required. They also ensure that the network is optimized to support all applications that traverse financial networks. Juniper Networks delivers unparalleled operational stability and performance across all product lines:

- Firewalls feature purpose-built hardware integrated with advanced software, operating at high speeds and providing sub-second failover
- Routers deploy the pioneering modular JUNOS router operating system architecture, which provides operational stability, QoS and supports MPLS for VPNs and traffic engineering
- Intrusion prevention with multimode detection significantly reduces false positives, ensuring that critical network resources can be reached even as attacks are stopped
- Application acceleration ensures the availability and optimization of application delivery through such capabilities as traffic redirection, HTTP compression and support for Compressed Real-Time Protocol (cRTP)

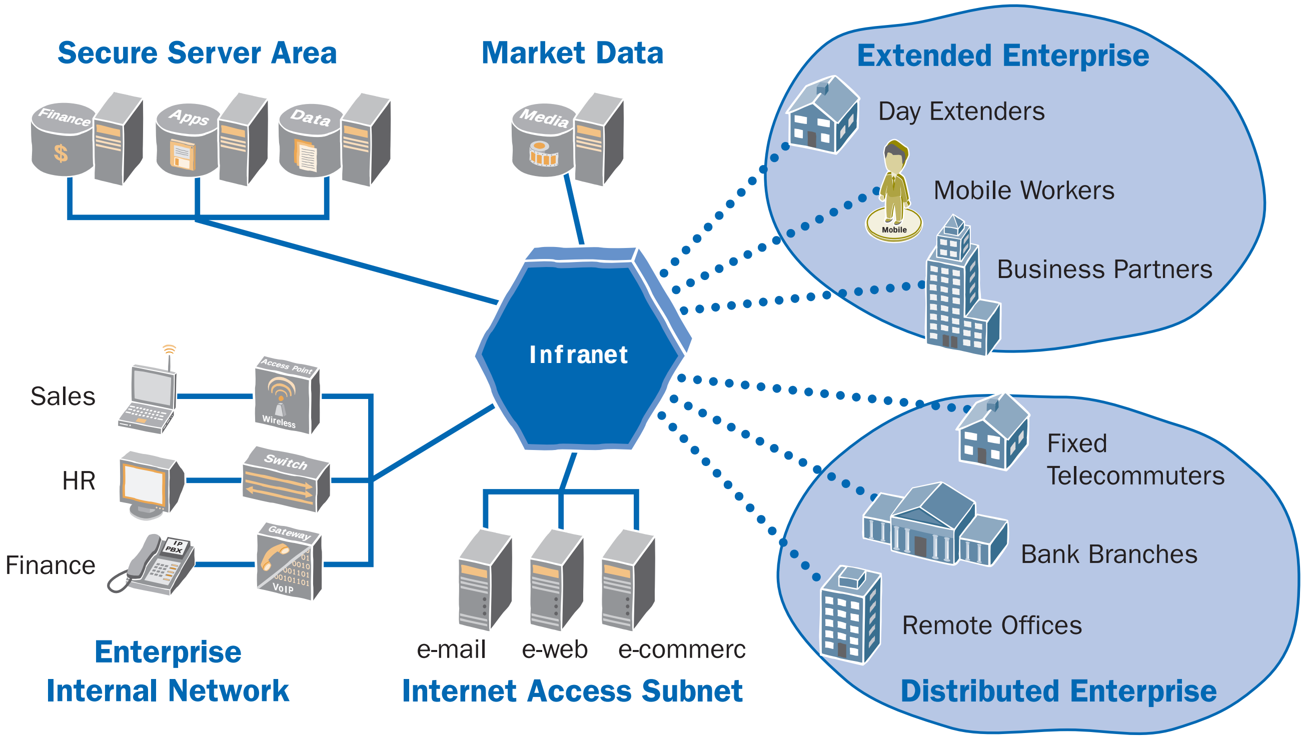

Figure 1: Enterprise Infranet provides secure and assured application delivery between all nodes across the network

Pervasive Security

More than most organizations, financial institutions must protect their networks, applications and data from a wide range of security threats. Viruses, worms, malware, denial of service attacks and increasingly sophisticated application layer intrusions of all kinds can cost financial institutions dearly in lost assets and expensive downtime. These intrusions and attacks originate both outside and within financial institutions' network perimeters. Like poor customer service, publicized intrusions can lead to erosion in trust in the financial institution on the part of customers. Also, financial institutions provide internal and external users secure and encrypted access to critical resources, while segregating these resources from unauthorized access. Juniper Networks provides rich feature sets that deliver Use Control, which ensures that internal applications are only accessed by authorized personnel from trusted networks, and Threat Control, which mitigates attacks and removes dangerous traffic from authorized traffic. Examples of pervasive security through Use Control and Threat Control include:

- Firewalls and routers preventing IP spoofing
- SSL VPN rules that allow conditional network access to specific users at an application level and rules that incorporate device state, such as verifying the installation of up-to-date virus protection, before allowing network access
- Intrusion detection and prevention signatures (updated daily) that remove known worms from the network, while ensuring the availability of applications to legitimate traffic
- Network-based anti-virus, deep inspection and URL filtering to ensure that no unauthorized software runs on the network

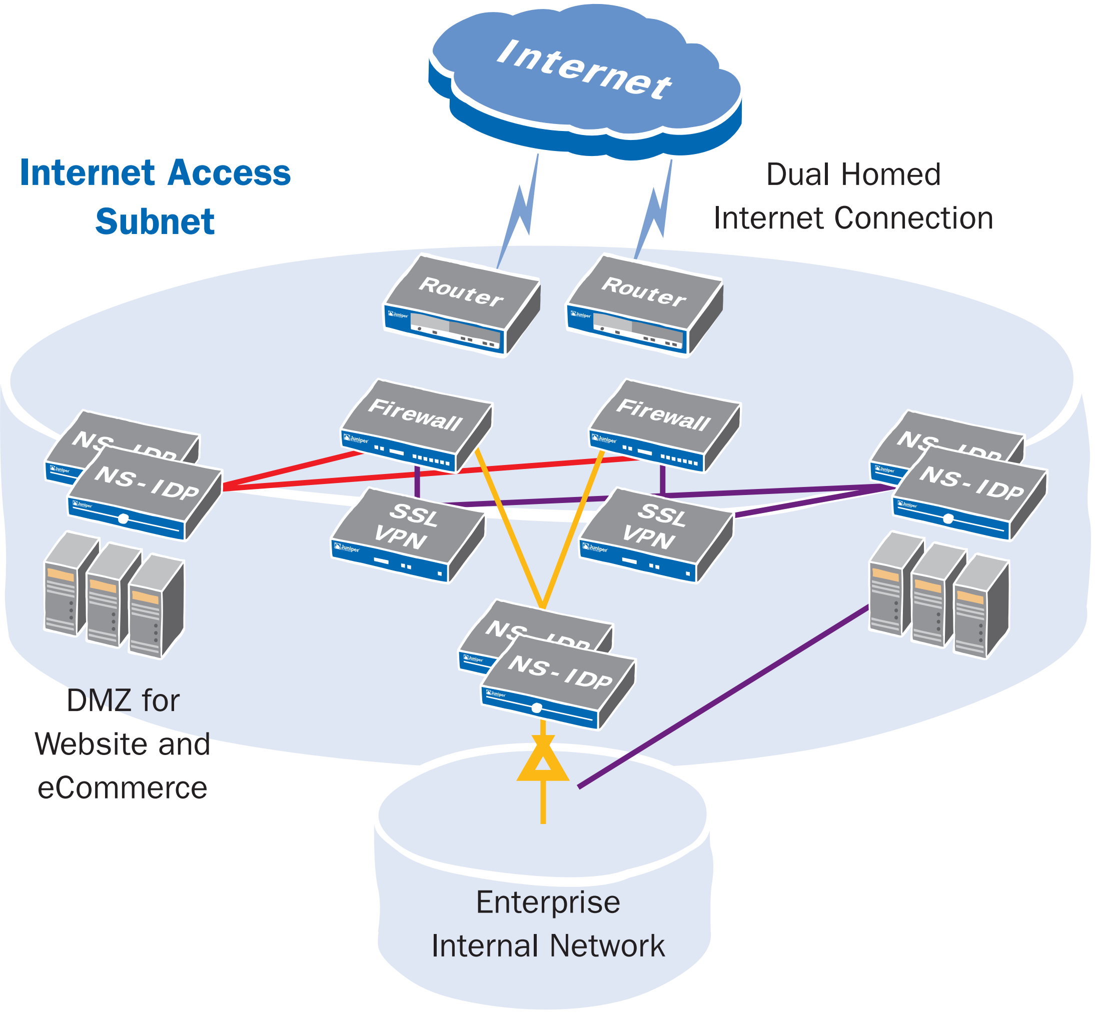

Figure 2: Downtime caused by ISP failures (12% of all downtime according to Infonetics) is eliminated by multihoming

Operations and Cost Control

Operational stability, pervasive security and high performance enable financial institutions to take control of their costs by consolidating resources and introducing operational efficiencies. For example, Juniper Networks offers an array of firewalls, available in different sizes for different areas of the network, enabling financial institutions to control security capacity and cost and enabling further control through consolidation. By deploying application acceleration solutions, financial institutions achieve greater performance and efficiencies from existing application and database servers, while centralizing data and backup systems. This eliminates the need to undergo costly and ineffective backup, restore and management in remote offices. Whether because of the reduction of operational expenditures afforded by simple code version maintenance, simpler operating system interfaces, or simpler management tools, financial institutions that rely on Juniper Networks enjoy greater control over operations and costs. Furthermore, by reducing the number of vendors within specific areas (for example, perimeter defense and connectivity), financial institutions simplify support processes, training, vendor approval and purchasing.

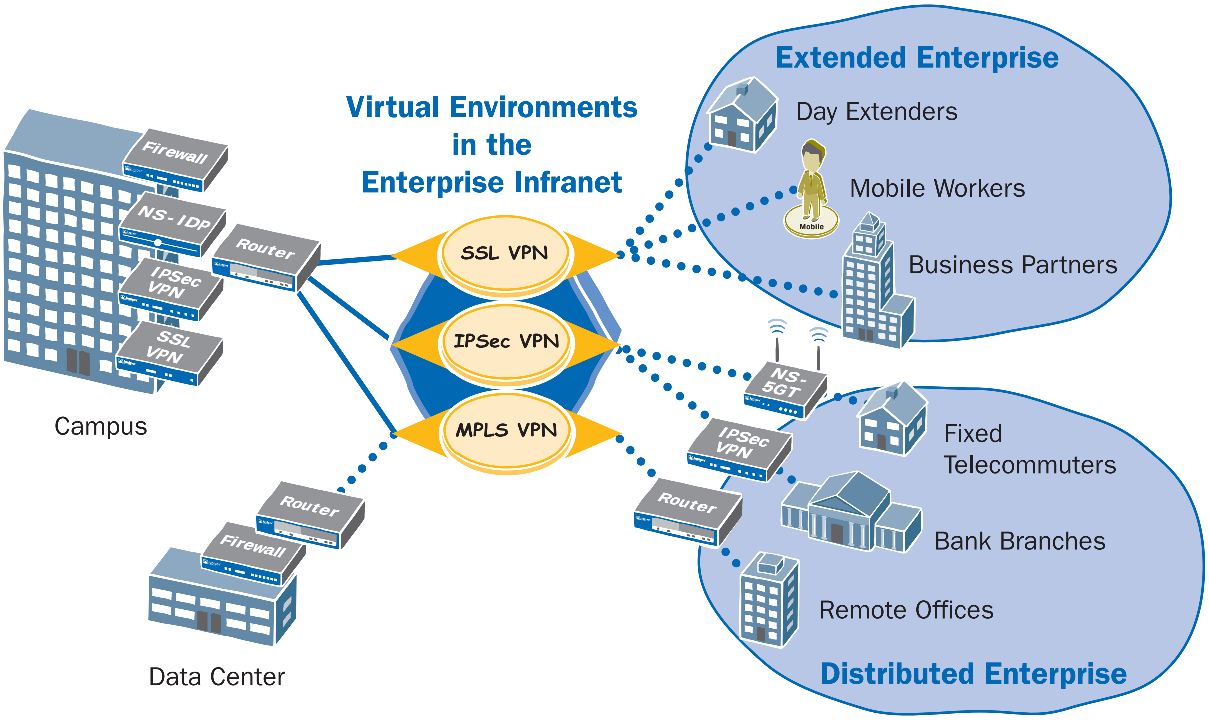

Figure 3: A broad offering of security solutions provides Delivery, Use and Threat Control for all applications, users and devices across the network.

Secure VPN Initiatives

Situation

Financial institutions are opening and extending their networks to allow remote users – including roaming employees, fixed telecommuters, branch offices, partners and customers – access to internal applications. Security concerns and regulatory compliance issues require that remote users only have access to applications for which they are approved. In addition, the financial institution must quarantine threats located in authorized network traffic originating from that user's device. At the same time, organizations must ensure that unauthorized users are denied access to sensitive information.

Solution

Juniper Networks offers a number of solutions to financial institutions for overcoming challenges that arise as part of extending the network.

- Private MPLS networks for larger organizations to virtualize the network and separate user and application traffic in VPNs between offices.
- IPSec VPN for encrypted connectivity between fixed sites and branches using devices controlled by the financial institution
- SSL VPN for the extended enterprise of roaming employees, customers and partners who access with devices not necessarily controlled by the financial institution
- Flexibility through mixing and matching VPN technologies for different areas of the network and business requirements

Conclusion

Juniper Networks delivers the network predictability, security and control required by financial institutions to realize competitive advantage, contain costs and to comply with outside regulations. The Enterprise Infranet provides an architecture for delivering comprehensive Delivery Control, Use Control, and Threat Control capabilities into the network through a broad product portfolio. Juniper Network solutions include comprehensive support, services and strong partner relationships, and are designed and validated in the most demanding real-world scenarios. Whether the organization is a bank, investment firm or insurer, Juniper Networks exceeds the requirements for critical financial networks.

> *"When the Juniper Networks NetScreen-SA 5000 series came along, it blew us out of the water. It had everything we'd been waiting for."*

Gene Fredriksen, CISM
Chief Security Officer
Vice President, Information Risk Management
Raymond James Financial, Inc

Bloomberg

Commerce Bank
Member FDIC

st.george

Handelsbanken

You're worth more here.
LANDMARK CREDIT UNION

SWIFT

RAYMOND JAMES
Individual solutions
from independent advisors

ตลาดหลักทรัพย์แห่งประเทศไทย
The Stock Exchange of Thailand

SPACE COAST CREDIT UNION
SCCU.COM

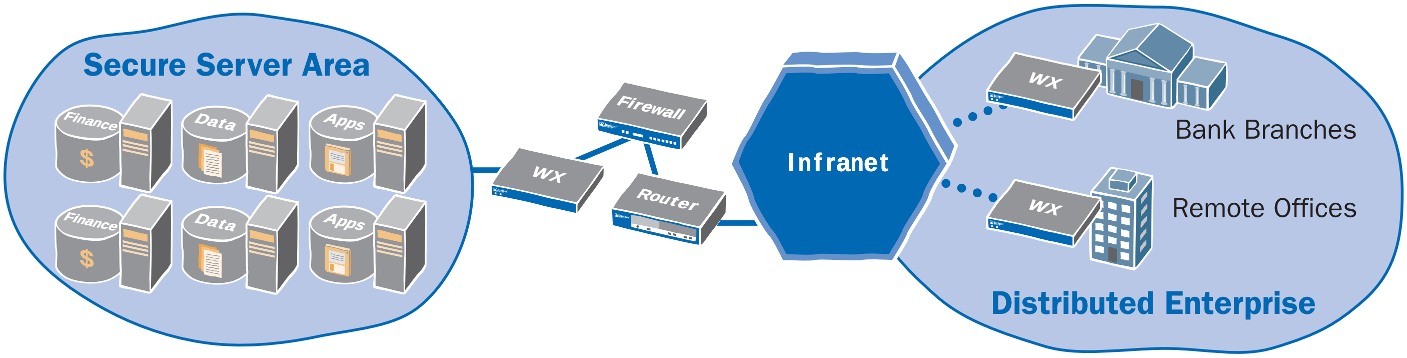

Figure 4 WAN optimization enables the removal of servers and data from remote and branch offices, reducing CapEx and OpEx

Enhancing and Simplifying Regulatory Compliance

Situation

Securing and protecting information is a top concern of financial institutions. Ensuring the integrity and availability of sensitive customer data is good business practice and is required by law. Banks, brokerages and insurance companies are required to implement security solutions that comply with a myriad of government regulations like the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes Oxley Act.

Solution

Juniper Networks solutions include routing, security and application acceleration to defend against a broad range of threats, protect privacy and provide features necessary to demonstrate regulatory compliance.

- Data encryption through multiple VPN technologies to ensure data privacy and integrity
- Separation through virtualization features across the products and solutions enable financial institutions to ensure that sensitive information is accessible only to appropriate agents
- Highly available communications through stable systems, redundant hardware configurations and multiple network-level resiliency mechanisms for fast sub-second recovery times
- Comprehensive logs for establishing audit trails and demonstrating compliance
- Compliance simplification through application acceleration to consolidate resources – particularly application servers and data storage – eliminating opportunities for error in backup and restore processes, and making them easier to secure

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