

FINANCIAL SERVICES REGULATORY COMPLIANCE WITH JUNIPER NETWORKS FIREWALLS, VPNS AND INTRUSION DETECTION

Challenge

Financial Services Institutions (FSIs) networks were adequate in the past, but 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.

Solution

Juniper Networks high-performance firewalls, VPNs and intrusion detection and prevention solutions provide a collection of security control features that simplify FSI regulatory compliance while controlling costs.

Benefits

- Increased application and data security
- High performance for multicast traffic
- Granular network access control

Financial services institutions of every kind must comply with a broad collection of local, national and international regulations, and the adoption of additional regulations is expected. Today's regulatory environment is becoming increasingly complex, and keeping track of redundancies and reconciling apparent conflicts can be confusing. Sarbanes-Oxley, Gramm Leach Bliley, BASEL II, Markets in Financial Instruments Directive (MiFID), Check 21, and dozens of additional regulations require financial services organizations to implement internal controls to:

- Secure stored data.
- Control access to data.
- Ensure the availability and performance of data and applications.
- Monitor network events.

To facilitate the compliance process, financial services organizations often adopt widely used comprehensive standards, like Control Objectives for Information and related Technology (COBIT) or International Standards Organization (ISO) 17799, with broad collections of practices. Using standards, organizations can develop specific objectives that align best practices with business requirements and capabilities, and regulatory requirements.

The Challenge

To increase competitiveness, FSIs 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 related 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.

As FSIs update their networks to accommodate new and emerging regulatory initiatives, they face a number of challenges. Some regulations require that stored data must be secured from intrusions and attacks to ensure both integrity and privacy. Other regulatory requirements stipulate that access privileges should only be granted to appropriate personnel or that data needs to remain available on a timely basis. Some regulations require active monitoring and reporting of network events, while others require that applications deliver quick and secure services to users. In the end, FSIs need to meet relevant requirements, and also be able to demonstrate to auditors that their network implementation and controls enable them to meet all of their regulatory obligations.

Juniper Networks Networking Solutions for FSIs

Securing Stored Data

FSIs are required to securely store data to ensure both integrity and privacy.

- Juniper Networks® firewalls enable segmentation of the network into secure domains through virtualization technology. Each segment can have its own firewall, VPN and policy-based management, allowing financial institutions to implement layers of security to protect key applications and servers. High interface density allows for topographical flexibility.
- Juniper Networks IDP Series Intrusion Detection and Prevention Appliances stop application level attacks before they damage network devices and servers and can interfere with application delivery.

Controlling Access to Data

Not only must data be secured from attacks and intrusions, many regulations require that access be limited only to appropriate personnel.

- Juniper Networks stateful inspection firewalls control who and what has access to key areas of the network. Built-in user authentication can be performed against an internal user database, eliminating the need for an external user repository, or it can be performed against a variety of different directories and databases including:
 - RADIUS, SecurID, Lightweight Directory Access Protocol (LDAP), and Active Directory with support for redundant server definitions.
 - Firewall/VPN access control and authentication that also provides a Web-based authentication mechanism allowing users to be authenticated to access any network server via an Internet browser.
- VPNs encrypt customer and other sensitive data as they travel within the internal network, as well as to and from remote customers and partners.

Ensuring Data Availability and Performance

Many regulations require that data remain available on a timely basis. Other regulations stipulate that applications operate effectively and quickly.

Juniper Networks firewalls/VPNs are fully redundant and feature sub-second, stateful failover.

- Firewalls/VPNs are available with as many as 72 Fast Ethernet or 24 Gigabit Ethernet ports.

- Firewalls/VPNs support dynamic routing, which allows them to overcome network failures by automatically learning and updating network configurations and rerouting traffic and VPN tunnels as appropriate.
- Firewall/VPNs support multicast traffic, which ensures high performance for critical financial services applications.
- The IDP Series stops traffic generated by unauthorized software, including peer-to-peer, freeing bandwidth for critical applications.
- The IDP Series is available on a variety of purpose-built hardware platforms to accommodate a broad range of network requirements, and can be clustered for high availability (HA) and scalability.

Monitoring Network Events

In addition to implementing internal controls, organizations must be able to demonstrate the effectiveness of their controls to auditors. Furthermore, some regulations require active monitoring and reporting of network events.

- IDP Series provides deep visibility into network traffic content. Comprehensive forensic and reporting tools enable investigation, tracking and reporting of malicious activity across the network.
- Centralized, policy-based management of firewall, VPN and IDP Series devices simplify the configuration and deployment process while minimizing the possibility of errors.
 - Delegate administrative rights to control the number of people who can manage the firewall or VPN and the administrative tasks they are allowed to perform.
 - Monitor and report on security policies as well as session, event and device status for proof of compliance.
 - Export detailed log files to third-party reporting tools to satisfy auditor requests for proof of internal controls.
- Regulatory compliance, though not driven by pure business considerations, does not need to be a liability. The expenses associated with compliance can be leveraged to provide positive and measurable benefits to organizations in the form of increased productivity and better cost controls. Providing a double benefit, the capabilities delivered by Juniper Networks market-leading firewalls, VPNs and IDP Series solutions make them useful for compliance and also enable FSIs to increase productivity and better control their costs.

Solution Components

Juniper Networks firewall/VPN and IDP Series are available in a broad range of configurations including:

- Integrated firewall/VPN appliances with Deep Inspection firewall that are ideally suited for branch office deployments.
- Juniper Networks ISG Series Integrated Security Gateways combining high-performance firewall/VPN and comprehensive IDP functionality for central site and data center deployments.
- Juniper Networks SSG Series Secure Services Gateways that deliver firewall/VPN and Unified Threat Management (UTM) security features, powerful routing and modular LAN and WAN connectivity.
- Standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances supporting small, medium and large enterprises.
- Juniper Networks SA Series SSL VPN Appliances providing clientless VPN for remote workers, customers and partners.

Summary—High-Performance Networking for FSIs

Juniper Networks is an established and innovative networking and security company with a proven record of success in the global banking and financial services market. Our technology vision is backed by a portfolio of market-leading products, and our financial services customers rely on Juniper in developing and marketing their own competitive products and services. Juniper's high-performance platforms deliver the operational stability, security and performance that high performing FSIs need to increase customer acquisition and retention, consolidate business units and networks, control costs, meet current and emerging regulatory requirements, and increase return on assets.

Next Steps

For additional details about the many ways Juniper's routing, security and application platforms help financial institutions address business and networking issues, please visit www.juniper.net/financial-services.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

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

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airsides Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.