

Solution Brief

# How Juniper Networks FW/VPN Solutions Facilitate Gramm-Leach-Bliley Compliance

---

Matt Keil  
Product Marketing Manager



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

Part Number: 351124-001 Aug 2005

---

## Contents

Introduction .....	3
Key Security Related Components .....	3
How Juniper Networks FW/VPN Solutions Can Facilitate GLB Compliance .....	4
Conclusion .....	5

## Introduction

In addition to reforming the financial services industry, the Gramm-Leach-Bliley Act of 1999 (GLBA) addressed concerns relating to consumer financial privacy. Recommendations on how financial institutions should protect customer data are made within Section 501 of the Act with additional details outlined within the Safeguards Rule. The Safeguards Rule dictates that Financial Institutions need to make a concerted effort to maintain the confidentiality of their customers' personal information such as their names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.

The Safeguards Rule applies to businesses, regardless of size, that are "significantly engaged" in providing financial products or services to consumers. This includes check-cashing businesses, data processors, mortgage brokers, non-bank lenders, personal property or real estate appraisers, professional tax preparers, courier services, and retailers that issue credit cards to consumers. The Safeguards Rule also applies to financial companies, like credit reporting agencies and ATM operators that receive information from other financial institutions about their customers. In addition to developing their own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

## Key Security Related Components

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution should consider all areas of its operation, particularly those that are critical to information security such as employee management and training; information systems; and managing system failures.

- **Employee Management and Training:** The success or failure of an information security plan depends largely on the employees who implement it. Firms should exercise best practices for hiring that might include extensive reference/background checks, strict enforcement of security policies such as password strength and refresh periods and limiting access to sensitive data and encrypting it data during transmission.
- **Information Systems:** Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. The Safeguards Rule makes suggestions along accepted industry practices on how to maintain security throughout the life cycle of customer information - that is, from data entry to data disposal. Recommendations include safe and secure storage for both hard copy as well as electronic data, limiting access to sensitive data stored electronically, protecting data during transmission, proper disposal of all data when appropriate.
- **Managing System Failures:** Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Recommendations within the Safeguards Rule follow well known processes and procedures such as regular back up of data, written policies and procedures to address security breaches, diligent software vendor vulnerability follow-up, implementation and maintenance of up-to-date security solutions such as strong authentication, firewalls and anti-virus that are centrally managed, prompt customer notification in the event that their personal information has been lost.

## How Juniper Networks FW/VPN and IDP Solutions Facilitate GLBA Compliance

Outside of recommending that firewalls and anti virus be used to protect customer data, the Safeguards Rule does not go into implementation specifics, instead focusing on a series of recommendations and best practices to protect private data. To help ensure that they are able to comply with the Safeguards Rule, financial institutions can use Juniper Networks broad range of firewall/VPN and intrusion detection and prevention products and services to implement a layered security solution that helps to protect their network and the sensitive customer data that resides on it. Specific FW/VPN and IDP functionality that can help financial institutions protect customer data include:

- Implementation of a Stateful inspection firewall to 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, LDAP and Active Directory with support for redundant server definitions
  - XAUTH support to allow authentication of dial-up user in addition to IPSec authentication
  - FW/VPN access control and authentication also provides a Web-based authentication mechanism that allows a user to be authenticated to access any network server via an Internet browser.
- Deployment of a Deep Inspection firewall or IDP to stop application level attacks before the damage the network.
  - Use forensic and reporting tools within IDP to investigate, track and report on malicious activity across the network.
- Segmentation of the network into secure domains through high interface density and virtualization functionality. Each segment can have its own firewall, VPN and policy-based management, allowing financial institutions to implement additional layers of security to protect key applications and servers.
- Encryption of customer and other sensitive data as it travels across the network internally as well as to and from the customer.
- Centralized, policy-based management of firewall, VPN and IDP to simplify configuration and deployment process while minimizing the possibility of errors that could lead to security holes.
  - Delegation of administrative rights with NetScreen-Security Manager 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 via NetScreen-Security Manager.
  - Export detailed log files to 3<sup>rd</sup> party reporting tools to satisfy auditor requests for proof of internal controls.
- Utilize Juniper Networks implementation expertise to first determine your exact security and networking requirements and then implement the solution that is most appropriate for your needs.

## Conclusion

Compliance with GLBA or any other regulatory act is a combination of products, best practice implementation, monitoring and ultimately, a 3<sup>rd</sup> party audit. Without each of these pieces, a company can struggle to achieve the necessary governmental compliance. The Juniper Networks FW/VPN and IDP offerings can help address the areas within the GLBA legislation that involve protecting the network and the customer data that traverse it. And with professional services assistance from either Juniper Networks or a certified channel partner, customers can utilize security best practices to implement a solution that can lead to GLBA compliance.

For more information on the FW/VPN and IDP product lines, please visit [www.juniper.net](http://www.juniper.net)

Information on GLBA and the Safeguards Rule was paraphrased from the following websites:

<http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html>

[http://www.ftc.gov/privacy/privacyinitiatives/safeguards\\_educ.html](http://www.ftc.gov/privacy/privacyinitiatives/safeguards_educ.html).

---

Nothing in this document should be considered legal advice with respect to state or federal laws or regulations. Readers should consult with their attorney for appropriate interpretation

Copyright © 2005 Juniper Networks, Inc. All rights reserved

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.

1194 N. Mathilda Ave. Sunnyvale, CA 95014 ATTN: General Counsel