

Solution Brief

How Juniper Networks FW/VPN and IDP Solutions Facilitate Sarbanes-Oxley Compliance

Matt Keil
Product Marketing Manager

Sarah Sorensen
Product Marketing Manager



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

Part Number: 351035-001

Contents

Background Information on Sarbanes-Oxley	3
Key Security Related Provisions	3
How Juniper Networks Integrated FW/VPN Facilitates Sarbanes-Oxley Compliance	4
How Juniper Networks IDP Facilitates Sarbanes-Oxley Requirements	5
Conclusion	6

Background Information on Sarbanes-Oxley

The Sarbanes-Oxley Act (SOX) was a direct fallout of a series of financial scandals with the most obvious result being that CEOs and CFOs must certify in writing that their financial disclosures complete and accurate. The lesser known result of the SOX legislation is that it requires all public companies to certify through 3rd party audit that they have enacted "disclosure controls and procedures" to ensure the reporting accuracy and security of material information affecting the company.

Key Security Related Provisions

The SOX legislation includes two key provisions Act where security products can help companies achieve SOX compliance.

- Section 302 - Corporate Responsibility For Financial Reports: This section makes the corporate executive team responsible for the accuracy of the Company's financial statements. As part of the reporting process, the internal controls over financial reporting that encompass IT controls over financial applications, and protection of those applications, are audited in conjunction with the financial statements and a separate audit report issued covering the Company's internal controls. Any significant deficiencies in internal controls are to be noted in this report filed with the SEC and available to the public.
- Section 404 - Management Assessment Of Internal Controls: While regulations defining aspects of Section 404 are in process, disclosure of significant weaknesses in internal controls will be required, which includes weaknesses related to access and protection of a company's financial applications. These access controls are considered pervasive so any weaknesses may be considered significant. External auditors will also be looking for appropriate security measures to protect the financial systems from fraud.

It is important to note that provisions outlined above do not call out any specific security related products or features. This means that companies need to interpret the provisions and in conjunction with best practices, implement the appropriate levels of security. Once the appropriate SOX security (and non-security) related measures have been implemented, a company will only achieve compliance after a 3rd party auditor has evaluated the implementation.

How Juniper Networks Integrated FW/VPN Facilitates Sarbanes-Oxley Compliance

As described in the above section, the SOX legislation does not call specify any security features or products. Based upon the language within the provisions, the following firewall/VPN features can help organizations as they work towards becoming Sarbanes-Oxley compliant.

- Implementation of Juniper Networks Stateful inspection firewall to control who and what has access to key areas of the network. Juniper Networks 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
 - Juniper Networks 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.
- Utilize Juniper Networks Deep Inspection firewall to protect against application level attacks delivered across common protocols such as HTTP, SMTP, IMAP, POP, FTP, DNS MS-RPC, P2P, IM, and NetBIOS/SMB.
 - Protect against inadvertent download of malicious programs such as Spyware and Adware through the implementation of URL/web filtering policies to keep employees from visiting common download sites.
- Segment 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 public companies 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.
- Use NetScreen-Security Manager to perform centralized, policy-based management of the security solutions to simplify configuration and deployment process while minimizing the possibility of errors that could lead to security holes.
 - Delegate administrative rights with Juniper Networks 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.
 - Proactively monitor and generate detailed reports on security policies as well as session, event and device status for proof of compliance via NetScreen-Security Manager.
- Utilize Juniper Networks implementation expertise to first determine the exact SOX related security and networking requirements and then implement the solution that is most appropriate.

How Juniper Networks IDP Facilitates Sarbanes-Oxley Requirements

In addition to the controls and security that Juniper Networks integrated firewall/IPSec VPN solutions enable organizations to deploy, the Juniper Networks IDP product line can also help organizations struggling to address the challenges laid out by Sarbanes-Oxley. In brief, the IDP provides network and application level attack protection and advanced logging capabilities that provide a detailed audit trail to help meet SOX requirements.

Sarbanes-Oxley requires corporations to prove that they are taking steps to proactively prevent fraudulent activity, insider trading, etc. IDP is the most sophisticated, proactive tool on the market, in that it combines the most attack detection mechanisms in a single solution to identify both known and unknown vulnerabilities, with multiple response mechanisms, including dropping the malicious packet or connection from the network. Leveraging Juniper Networks Stateful Signatures, Protocol Anomaly Detection, unique Backdoor detection capabilities (for interactive Trojan and Worm detection), Traffic Anomaly Detection, Network Honeypot, etc. adds further credibility to security audits, demonstrating that the organization is doing everything that it can to maximize its attack protection coverage.

As liability for preventing abuse of the network now rests at the "C level," the ability to immediately detect unauthorized change is paramount. IDP can identify changes on the network that might represent policy violations or malicious behavior, with the release of Enterprise Security Profiler - which is the intrusion detection industry's most advanced security posture assessment tool. Only IDP gives Network/Security managers a comprehensive, real-time view of the activity on the network tied to an intrusion prevention security policy that can be used to lock down unauthorized activity.

Juniper Networks IDP continuously learns about the network and stores that information in a searchable database, so administrators can quickly find the information they need to understand exactly what is going on in the network. Administrators can see what hosts are on the network, who is talking to whom, what services/ports are being used, and even what transpired during the interaction, such as what commands were issued or what file was downloaded. Administrators can achieve a holistic view of all servers, clients, users and applications on the network to ensure all appropriate security measures can be put in place. Plus, administrators can quickly drill into the details they need, including complete packet captures, to identify exactly what happened during a security event. This information can be used to close out the incident and potentially aid in other investigations.

There is a requirement in Sarbanes-Oxley that all communication into and out of the network (intra and extra corporate) is logged and held for 5 years. With Juniper Networks IDP, administrators can determine how many packets they want to capture before and after an event that triggers an alarm. The Juniper Networks IDP product line and the Juniper Networks Secure Access series works with the Network Intelligence correlation engine, which can be used to burn CD's of all the data that needs to be archived for storage.

Conclusion

While the Act itself does not call for any specific security features or functionality, it does require that appropriate internal controls be in place to contain and detect fraud (section 404). And it requires a company CFO and CEO to sign off on those controls as part of the periodic reporting process (Section 302). It is important to note that all technologies need to be supported by a strong corporate security policy to meet the overall requirements of Sarbanes-Oxley, but companies can utilize Juniper Networks security functionality to assist in their efforts to comply with Sarbanes-Oxley:

Information on Sarbanes-Oxley Act was paraphrased from the following website: www.sarbanes-oxley.com.

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