

“We needed a network security solution that allows for scalability.”

Donnie Clemmons
asiGuardian
Vice President of Operations



Customer:

asiGuardian, a regional, layered-data protection company

Industry:

Managed services

Challenge:

Protect critical customer and corporate data from network attacks while accommodating performance and scalability needs

Solution:

Juniper Networks NetScreen firewall and IDP security solutions

Benefits:

- Increased network security and performance
- Simplified upgrade process because of centralized management
- Saved time and operating costs

asiGuardian was formed in October of 2002 to provide security and data-protection services for medium enterprises throughout Kentucky. Offering customers the option of managed services, professional services and infrastructure services, asiGuardian provides affordable business data protection, reliable data back-up and business recovery solutions. With the mission of “Online. All the time”, it is critical that asiGuardian work with a best-in-class network security solution provider that can provide a high level of stability and scalability.

asiGuardian originally implemented a Cisco firewall solution but when asiGuardian made available its new online backup offering in April of 2003, the company realized that the Juniper Networks network security solution’s layered approach was a better fit for what they were doing. “Using our previous internal firewall solution, we knew we couldn’t get where we wanted to go. We needed

a network security solution that allows for scalability,” said Donnie Clemmons, vice president of operations at asiGuardian.

The Solution

asiGuardian replaced its initial Cisco firewall solution with the Juniper Networks NetScreen network security solutions for its HaloPoint Secure Hosting offering.

asiGuardian selected and deployed, in active/passive mode, two Juniper Networks NetScreen-500 systems to serve as the company’s primary perimeter firewall solution. The NetScreen-500 system provides robust integrated firewall and virtual private network (VPN) functionality with up to 700 Mbps firewall performance and up to 250 Mbps of 3DES IPsec VPN throughput,

Juniper Networks NetScreen-IDP systems operate inline to accurately detect and drop malicious traffic, in real-time, before it reaches its victim.

The Juniper Networks NetScreen-IDP uses proprietary technologies and multiple detection methods to accurately identify attacks and minimize the number of false positives.

asiGuardian also purchased a Juniper Networks NetScreen-IDP 10 system and has it deployed at the asiGuardian Internet perimeter behind the NetScreen firewalls.

Additionally, a Juniper Networks NetScreen-IDP 100 is being used internally to monitor asiGuardian's securely hosted customer traffic. The NetScreen-IDP 100 provides up to 200 Mbps throughput and, using proprietary technologies and multiple detection methods, accurately identifies attacks and minimizes the number of false positives. With its high level of accuracy and ability to be deployed inline, Juniper Networks IDP customers can drop malicious packets or connections in real-time to minimize the cost and impact of attacks.

The Benefits

asiGuardian has seen many benefits since using the Juniper Networks solution. "No matter the size of our customer, we are now offering an effective means of securing their data without limiting the performance or scalability," Clemmons said.

Since deploying the Juniper Networks intrusion detection and prevention products, asiGuardian has been able to actively block, instead of simply monitor attacks. "We no longer have to worry about attack investigation and clean-up taking up valuable time. Juniper Networks' IDP products accurately block attacks from causing havoc in our internal network and those of our customers," said Tom Tipton, business development manager at asiGuardian.

Furthermore, Juniper Networks network security appliances are specifically designed for easy installation in a variety of environments. The intuitive and simple graphical user interface (GUI) and management features of the Juniper Networks devices allow asiGuardian to easily administer and maintain the solution.



**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

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

www.juniper.net

Copyright © 2003, Juniper Networks, Inc. All rights reserved. Juniper Networks is registered in the U.S. Patent and Trademark Office and in other countries as a trademark of Juniper Networks, Inc. ERX, ESP, E-series, Internet Processor, J-Protect, JUNOS, JUNOScript, JUNOSe, M5, M10, M20, M40, M40e, M160, M-series, NMC-RX, SDX, T320, T640, and T-series are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

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.