

St. George Bank Juniper Networks NetScreen-5200™ Security Appliances Protect National Financial Institution

Customer:

St. George is Australia's fifth largest bank and one of the country's top 15 publicly listed companies. Its national operations span all aspects of the financial industry, including retail banking, institutional and business banking, and wealth management.

www.stgeorge.com.au

Challenge:

Provide a secure firewall solution to meet the demanding requirements of a world-class financial institution.

Objectives

- Protect digital assets, while providing services to customers connected via the Internet.

- Lower total cost of ownership and increase ongoing return on investment.
- Maintain or increase security and performance, over the existing firewall solution.
- Reduce administration costs and equipment footprint.

Solution:

Deploy four Juniper Juniper Networks NetScreen-5200 network security appliances to protect the St. George network.

Benefits:

- Reduced total cost of ownership
- Increased network performance
- Reduced administrative overhead
- Reduced equipment footprint
- Increased network scalability

"By consolidating our security infrastructure with Juniper Networks NetScreen™ system, we enjoyed immediate savings in maintenance costs, administration costs, and equipment footprint."

Michael McCutcheon
Infrastructure Manager,
St. George Bank

About the Company

Founded in 1937 as a housing-based financial institution, St. George built a reputation as Australia's foremost building society, before achieving full banking status in July 1992. It is now Australia's fifth largest bank and one of the country's top 15 publicly listed companies. Its national operations span all aspects of the financial industry, including retail banking, institutional and business banking, and wealth management.

Minimize Overhead, Maximize Protection

St. George already had a workable security platform. They considered the Juniper Networks solution when they learned that the same level of performance and security could be achieved with less ongoing maintenance and administration.

A Secure Solution

St. George wanted to build out a more efficient solution—one with lower total cost of ownership, more flexible scalability, lowered equipment footprint, and satisfactory (or improved) performance. Network security, however, was the most important consideration for this financial institution, followed by high performance, because the bank provides online financial services for its customers over the Internet. The firewall deployment exercise also had to fall within budget.

Professional Protection

The Juniper Networks NetScreen-5200 security appliance is part of the Juniper Networks NetScreen-5000™ series of purpose-built security systems. Designed to deliver new levels of high performance for large enterprise, carrier, and data centre networks, the Juniper Networks NetScreen security appliances integrate firewall, DoS and DDoS protection, VPN, and traffic management functionality, in a low-profile modular chassis. These systems are built around Juniper Networks NetScreen's third-generation security ASICs (Application Specific Integrated Circuits) and distributed

system architecture. They employ a switch fabric for data exchange, with a separate multibus channel for control information to provide scalable performance for the most demanding environments. These systems offer excellent scalability and flexibility.

In early 2002, nMetrics Pty Ltd., an integration partner of Juniper Networks, introduced St. George's senior IT staff to the Juniper Networks NetScreen security technology. nMetrics chose to promote this technology because it believed there would be a marked paradigm shift in favour of innovative ASIC-based firewall appliances. Its in-house testing had also confirmed that Juniper Networks NetScreen series was the leading product in this crucial area.

When Stephen Urquhart, nMetrics director, first met with Mick McCutcheon, Senior Manager Infrastructure Architecture at St. George, he highlighted the features and benefits of ASIC-based firewall technology. These advantages were also recognized by Gartner Research in its "Magic Quadrant" analysis, which identified Juniper Networks NetScreen series as a market leader in this area, with both the vision and the capability to deliver ASIC-based firewalls. The bank readily saw how the technology could improve and drive its business performance, while underpinning security management.

In late 2002, nMetrics and St. George IT staff decided to verify the implications and business benefits of migrating from the bank's existing firewall platform to the Juniper Networks NetScreen solution. David Britt, nMetrics CTO, worked closely with St. George's IT staff to map out the design. Stringent proof-of-concept methodologies ensured that if the Juniper Networks NetScreen firewalls were purchased, the business would benefit as per the criteria specified in the planning documents.

Committed to sound migration procedures, Mick McCutcheon engaged the services of Scott Crane of ThinkSecure to provide a micro-design document, mapping out a migration plan to the new architecture that would not compromise security. nMetrics and St. George independently verified the plan, concluding that ThinkSecure's procedures would provide a smooth transition. With the full confidence to move forward, St. George ordered the security appliances from nMetrics and engaged it to implement two Juniper Networks NetScreen- 5200 security appliances at the two Sydney sites.

Implementing Innovation

Implementation of the Juniper Networks solution began in August of 2003 and was completed in January of 2004. nMetrics worked closely with Juniper Networks and St. George's IT staff to ensure the success of the project. A total of four Juniper Networks NetScreen-5200 security appliances were implemented, in paired redundant configuration: one pair at the Kogarah site and one pair at the Sydney city sites.

Juniper Networks unique Virtual Systems and Virtual Routers features were activated on the Juniper Networks NetScreen-5200 devices so that St. George could create independent administrative profiles that logically emulated 18 firewall zones and six virtual routers. The Virtual Systems feature allows a single Juniper Networks NetScreen security appliance to be logically partitioned into multiple security domains, with their own administrators, address books, user lists, custom services, Virtual Private Networks (VPNs), and policies. The Virtual Routers allow traffic to be isolated and securely routed, targeting different destinations. These features simplified St George's redundancy requirement, without compromising on footprint and administration requirements.

Roadmap to the Future

With the Juniper Networks 5200s now protecting its network, St. George has a variety of options for future needs. Scalability is as simple as adding additional Juniper Networks NetScreen appliances to the topology. If additional Virtual Servers or Virtual Routers are required, new profiles can quickly be created on the existing appliances, without any hardware implementation or modifications.

The high performance provided by the purpose-built ASICs in the Juniper Networks NetScreen-5200 appliances means that the St. George network performs better, in accordance with the company's business requirements. The network is securely protected by Juniper Networks, and quality of service and reliability have been enhanced for a better customer experience.



**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 2004, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESR E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XR, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. 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.