CASE STUDY

AUTOMATION CREATES NIMBLE SECURITY OPERATIONS AT LEADING FINANCIAL INSTITUTION

Summary

Company: Global Financial Institution

Industry: Financial services

Business Challenge:

- Use security automation to meet the demands of business units that require rapid response to fast moving opportunities

Technology Solution:

- Firefly Perimeter
- SRX5400 Services Gateway
- NSM4000 Network and Security Manager

Business Results:

- Deployed security automation at scale
- Reduced firewall changes from 40 to 5% of operating budget
- Rightsized protection with physical and virtual firewalls
- Migrated smoothly from ScreenOS to Junos OS
- Reduced hosting fees to internal customers by over 30%

Financial services firms must move swiftly to capture fast moving opportunities. Yet they are under constant attack from bad actors intent on cybercrime, business disruption, or corporate embarrassment. IT must be flexible enough to meet the demands of business without compromising security.

Business Challenge

This leading global financial institution found that manual security configuration consumed more than 40 percent of its security operations budget. Even worse, configuration changes could take weeks to approve and provision.

The firm needed a security solution that could be fully integrated into the custom workflows that permeated its physical and virtual networks. As it replaced its older Juniper Networks® NetScreen Series Security Systems, the company wanted an adaptive, intelligent security solution capable of full automation. The selected security solution had to work with the bank's VMware orchestration tools, which it had developed in-house. The bank also wanted a solution that would mesh with SDN and its growing cloud environment.

Technology Solution

The bank is migrating its internal customers from legacy firewalls like NetScreen Series to modern, more adaptive cloud solutions, including Juniper Networks Firefly Perimeter. It also deploys SRX Series Services Gateways for protecting high-performance, low-latency business-to-business and internal trading applications.

By deploying a combination of virtual and physical firewalls, the bank rightsized its security infrastructure without sacrificing performance and is now able to meet the aggressive service-level agreements (SLAs) of its business units. Security automation will replace dozens of fixed-configuration firewalls with Firefly Perimeter, eliminating the need to install and manage hardware in the bank's many locations around the world. Because Firefly Perimeter is a virtual firewall based on Juniper Networks Junos® operating system, the bank can fully secure its high-bandwidth applications with the identical automation used for cloud automation. Using Firefly Perimeter has permitted the bank to deploy more focused, granular protection for its internal networks to meet its audit requirements, while minimizing the workload when policy changes are required.

With Juniper's adaptive, intelligent security solutions, the financial institution can deploy security automation at scale while enforcing its highly specialized business requirements.

Since this financial institution has a large Juniper Networks ScreenOS® Software network, it required a management solution that could work with both legacy and modern firewalls, including for situations that couldn't be automated. The bank uses NSM4000 Network and Security Manager to provision and manage Firefly Perimeter, SRX Series, and NetScreen Series firewalls. As the bank further automates security operations, it will have an effective centralized management solution across its Juniper firewall estate without the need to deploy another management tool.

Results

This financial institution is delivering applications on time for its business units and will considerably reduce its cost of operations. With Juniper's adaptive, intelligent security solutions, the bank can deploy security automation at scale while enforcing its specialized business requirements.

The bank has reduced firewall changes from 40 percent to 5 percent of operating budget.

Ultimately, the ability to virtualize and automate security allows the bank to scale to tens of thousands of virtual firewalls. Critical to the success of automated security configuration is application profiling with pre-approved policies. Once an application is profiled and validated, an associated security policy can be created based on pre-approved templates. For example, IT could create templates for changes commonly requested by different departments, and then those changes could automatically be applied across the virtual and physical firewall infrastructure. There's no need to wait days or weeks for a security administrator to make manual configuration changes. Automation allows the bank to deliver on its security and compliance obligations while reacting with the agility and speed that its business units need—without the painstaking labor of security administrators.

By rightsizing and automating its network security, the bank is seeing significant CapEx and OpEx savings. Whereas 40 percent of the security operations budget was once devoted to firewall policy changes, the use of automation has slashed that number to 5 percent. As a result of these efficiencies, IT can pass that savings on to its business units with significant reduction in the cost of hosting.

The migration from ScreenOS to Junos OS continues to go smoothly. The bank is using Juniper-developed scripts and NSM to migrate many of the firewall configurations.

Next Steps

As the financial institution automates security operations for its internal networks, it is exploring the use of security automation for its external networks and cloud services.

For More Information

To find out more about Juniper Networks products and solutions, please visit www.juniper.net.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net.**

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

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

3520520-001-EN Oct 2014