

GO TRANSIT BUILDS FOR THE FUTURE WITH JUNIPER NETWORKS SECURITY

Summary

Industry: Transportation

Challenge:

- Support high-volume e-commerce applications.
- Support for mobile workforce and devices.
- Gain visibility of malicious activity and mitigate network security risks.

Selection Criteria: GO Transit had a major network infrastructure initiative, aimed at enhancing security, reliability, and functionality of its systems that increasingly rely on the network.

Network Solution: Juniper security, switching and management products including the SSG320M, SA4500, EX4200, IDP250, STRM500, NSM, IC4500 and Junos Pulse.

Results:

- Enhanced reliability, capacity, and security of the Internet gateway to support mission-critical IP-based applications and services.
- Employees and contractors have anywhere, anytime secure access to corporate resources from an IP device.
- Proactive approach to security supported by comprehensive and collaborative suite of security solutions and managed services.

Serving almost 57 million passengers a year, GO Transit is Canada's first interregional transit system, linking the city of Toronto with the surrounding areas of the Greater Toronto Area through an extensive network of train and bus services that serves 7 million people in a region that spans more than 4,200 square miles. Since operations began in 1967, more than 1 billion people have taken the GO Train or the GO Bus.

Challenges

GO Transit provides transportation service to 217,000 passengers on a typical weekday. With ridership growing and exceeding expectations, the organization embarked on a multi-year plan to automate its business processes, modernize its applications, and consolidate multiple disparate networks to a scalable and efficient IP infrastructure. "The savings and efficiency costs of network consolidation were obvious," stated Robert Power, director of IT at GO Transit.

With IT systems becoming more strategic to GO Transit's operations, a critical step was to enhance and modernize its security posture, given the increasing number of new potential threats. The Internet gateway needed to keep pace with the increase in IP-based systems, services, and traffic.

At the same time, GO Transit was upgrading its point-of-sale (POS) system that customers use to purchase ride tickets, and it needed to migrate from a proprietary network to an IP-based infrastructure. That meant transaction processing would now flow through the corporate Internet gateway. With 96 percent of the organization's revenue processed through this POS system, the underlying network had to be highly available, highly reliable, and highly secure. "We needed reliable service to allow processing and application delivery to continue uninterrupted, even during peak sales times," said Power.

GO Transit wanted the extra assurance that its existing Internet gateway and managed services could keep pace with the new applications and uses. "We wanted to be ahead of the curve," continued Robert Power. "We needed something more solid and secure at the network for both business and security reasons."

A move to proactive security was also desired. GO Transit wanted to identify potential network vulnerabilities and enhance its ability to continue functioning if any malicious activity targeted its network. Armed with that insight, GO Transit's IT department took active measures to better equip the company against possible security attacks and mitigate risks. "We wanted further verification that our network was secure and the Internet gateway was doing its job to keep threats at bay," assured Power.

GO Transit also wanted to provide employees in the field with secure remote access, which would boost productivity and flexibility. "We are starting to equip field staff with laptops that have aircards, and they need access to their business applications through the public Internet. We estimate that 50% of GO's support vehicles will have network access within the next couple of years," predicted Power. Workers remotely access bus management, bus location, train management, and train location applications, among others.



While the organization's former VPN solution worked, GO Transit sought out a way to enhance the security for its dynamic environment. "Previously, we had an IPsec client and single-factor authentication, and we were looking to transition to SSL VPN and dual-factor authentication with tokens as well as boost network capacity to allow granular remote access for our staff in the field," explained Power.

Selection Criteria

GO Transit issued a detailed RFP for security elements, along with associated managed security services from a provider that had the expertise to configure, monitor, and diagnose the perimeter security domain. Respondents were judged on the quality, efficiency, and overall security of their design, as well as the cost to maintain it. "We were looking for the best possible integration of components to meet our business requirements," Power pointed out.

GO Transit chose a managed CPE services solution from Spyders—which included Juniper Networks security, infrastructure,

and management products—to protect its public-facing and internal Web, e-mail, e-commerce, and streaming media servers. "Juniper and Spyders had the best combination of products and services that gave us the constant monitoring, coordinated threat management, and the proactive security we needed," acknowledged Power.

Solution

GO Transit deployed Juniper Networks SSG Series Secure Services Gateways, IDP Series Intrusion Detection and Prevention Appliances, and EX Series Ethernet Switches at the Internet gateway. Secure remote and local access is provide by the SA Series SSL VPN Appliance, IC Series Unified Access Control Appliance, and the Juniper Networks Junos Pulse client. The company deployed NSM appliances for policy management and configuration, and Juniper Networks STRM Series Security Threat Response Managers for monitoring and reporting. Spyders provides ongoing management of the perimeter security domain.

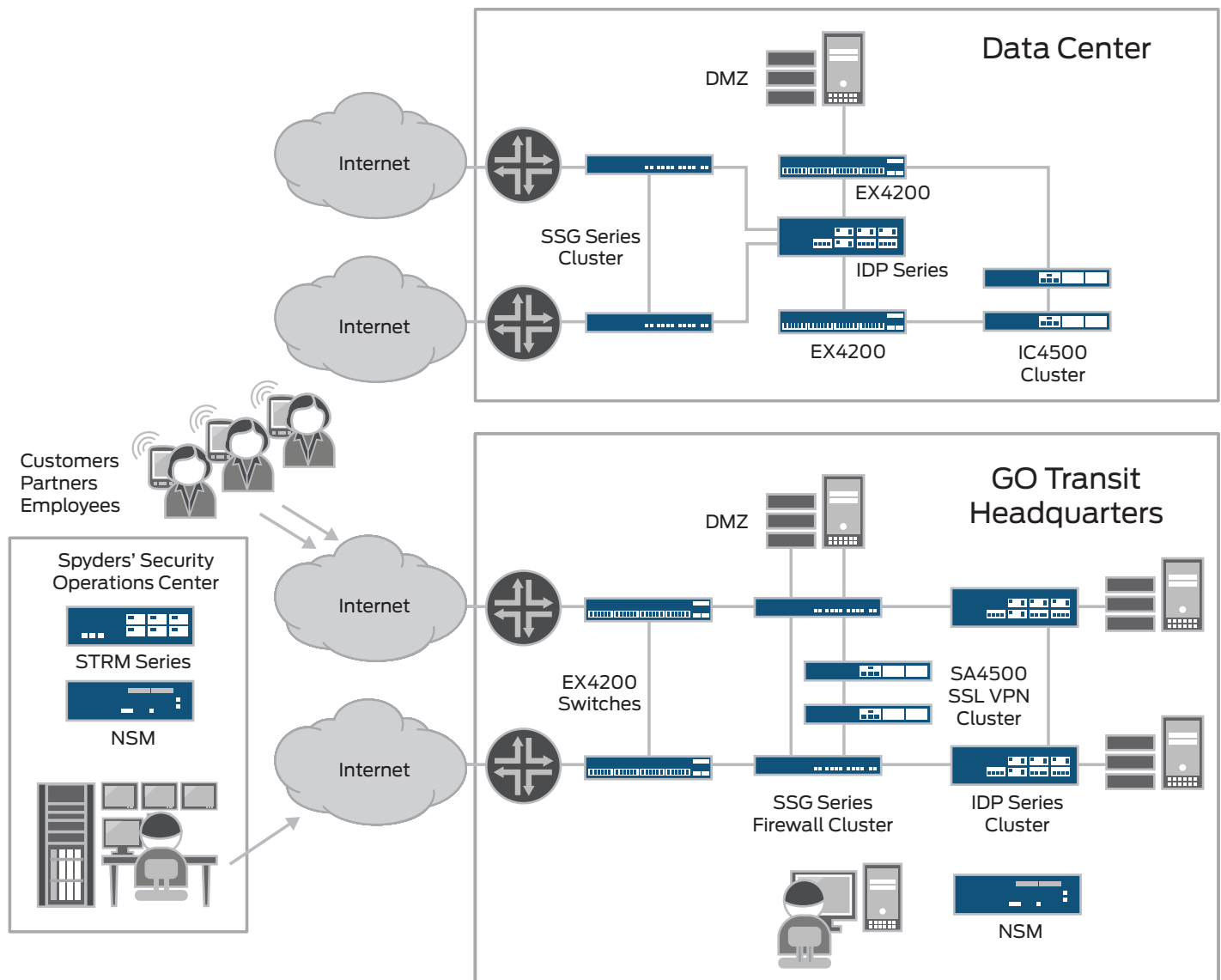


Figure 1: The new GO Transit comprehensive network.

Clusters of SSG Series Secure Services Gateways and standalone IDP Series appliances protect GO Transit's network perimeter. The SSG Series is a purpose-built, high-performance platform that delivers WAN connectivity and security, protects the LAN perimeter against external attacks, and identifies and stops application-level attacks and content-based attacks. Pairs of SSG Series Secure Services Gateways are set up in high availability mode, ensuring that the network meets the service levels necessary for high-volume e-commerce sales.

The IDP Series offers the latest capabilities in network intrusion prevention to protect the network against a wide range of attacks. It provides zero-day protection against worms, Trojans, spyware, and other malware. Not only does the IDP Series protect the network, it gives GO Transit the audit trail to verify that its security policy is effective.

"Juniper had the best combination of products that gave us the constant monitoring, coordinated threat management, and the proactive security we needed."

Robert Power,
Director of IT, GO Transit

The EX Series Ethernet Switches provide high-performance, carrier-class performance. The EX Series switches are easy to deploy, reduce the amount of boxes needed to be deployed, can be managed by NSM, and consume less energy—allowing for more energy-efficient networks that reduce capital and operational expenses. GO Transit used Junos automated scripting to eliminate external load balancers by polling multiple ISP links and dynamically determining the best path for sessions.

GO Transit uses the Juniper Networks SA4500 SSL VPN Appliance to give an identified group of mobile and remote employees, contractors, and business partners access to corporate resources and applications. The SA4500 is designed to provide medium and large enterprises with remote access plus sophisticated partner and customer extranet features. With the SA4500, GO Transit can provide differentiated access to users based on their roles and groups, so that identified users have access only to authorized data. These users can gain anywhere, anytime access to their corporate resources using any web-enabled device.

GO Transit uses Secure Meeting, a feature of the SA Series, to improve helpdesk support for its users as well as to streamline troubleshooting for IT vendors. The In Case of Emergency (ICE) license option on the SA Series allows GO Transit to ensure business continuity in the event of an emergency such as a pandemic or other disaster. With ICE, GO Transit can instantly accommodate spikes in remote access demand from more concurrent users. This allows the company to maintain productivity and deliver customer service by using any web-enabled device such as employee's home PCs to access the network.

"Threat coordination among the IDP Series, IC Series Unified Access Control Appliances and SA Series SSL VPN is important to us," said Power. Juniper's solutions help GO Transit address its security and compliance requirements as a cooperative system that identifies, mitigates, and reports on the attacks in the distributed enterprise.

Junos Pulse allowed GO Transit to extend their perimeter security right into their field operations environment via the 3G network, allowing contractor and employee handheld BlackBerry and iPad devices to securely access to the GO intranet.

The IC Series UAC Appliances are used for access, authentication and enforcement for GO Transit employees as well as third party contractors and partners with guest accounts. The Junos Pulse client allows IT staff to enforce policy at the remote desktop/device level for user access. The authentication of BlackBerry devices with Junos Pulse and UAC in GO Transit's WiFi environment also reduces mobile airtime and associated telecom costs in the campus environment.

The STRM Series and NSM appliances provide GO Transit with the tools for a proactive security strategy. "The STRM and NSM are used for provisioning, monitoring, and correlation of information so that we can better understand relevant events and potential risks to the business," confirmed Power.

The STRM Series provides centralized alarm and event correlation from network and security devices, along with management reports pertaining to the Juniper security and switching infrastructure at the Internet gateway. The STRM Series provides GO Transit with network, security, application, and identity awareness necessary to achieve security in a proactive manner. This enables GO Transit to leverage the accounting capabilities of the management appliance to understand who accessed what information and from what location.

The technical staff from GO Transit and Spyders has access to the NSM appliances, so they have shared control and visibility of the security elements. With NSM, they can easily control device configuration, network settings, and security policy management for all aspects of the infrastructure—including switching, firewall/VPN, and IPS. Additionally, a complete set of investigative and reporting tools gives IT greater visibility for fine-tuning or compliance.

Results

According to Power, the first phase of the implementation has taken place on time, within budget and without incident. "We've had a graceful transition, which was as seamless as possible," he declared. "Spyders is an extension of our team."

Power has been pleased with the move to managed services. "We wanted managed services because it's critical to keep everything up to date," advised Power. "Once the security infrastructure is built, you have to keep it current to countermand the latest security threats."

Network simplification and comprehensive protection allow GO Transit to take a more proactive stance against any incoming attacks. GO Transit has greater visibility and control over the network, applications, and users. He continued, "We know more about what is going on, and we don't have to just assume that the security is working because we can see exactly what attacks are coming in, from where and targeted at which device."

With the new remote access capabilities, identified GO Transit employees can work productively from anywhere with an Internet connection. "They'll notice a much better service that's more ubiquitous, well managed, easier to use, and more convenient," boasted Power. "Our network allows us to extend our reach without compromising security." Not only is remote access more convenient for off-site workers, but IT can now give third-party consultants and contractors access to the resources they need with confidence.

While GO Transit's IT staff works with its managed service provider Spyders for day-to-day operations, the IT staff also completed Juniper's Fast Track security course. The curriculum allowed the IT staff to quickly gain proficiency with the new solution that is helping them achieve their security goals.

Next Steps and Lessons Learned

Looking ahead, the new infrastructure gives Power the capabilities he needs to set up information portals for GO Transit employees. "In the future, we'd also like to consider dealing directly with our customers through mobile devices, and our secure network will help us do that as well," he said.

Power offered up a bit of advice to those who might be considering a major network infrastructure overhaul—do the heavy lifting up front. "Do your homework, and put a lot of thought, planning, and research into the process," he concluded. "If you follow an RFP process, make sure you get it right and set it up to extract what you want out of the project."

For More Information

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

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.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

Copyright 2011 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. 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.