Sun Rich Converges Network and Security into Cato Cloud

Adam Laing
Systems Administrator

Background

Sun Rich is a provider of high-quality fresh-cut fruit to foodservice and retail markets in North America. Sun Rich has 150 users spread across four facilities. These facilities are strategically located in Richmond, BC, Brampton, ON, Corona, CA and Reading, PA with datacenters located in Canada and in the Microsoft Azure cloud.

The Appliance Patchwork

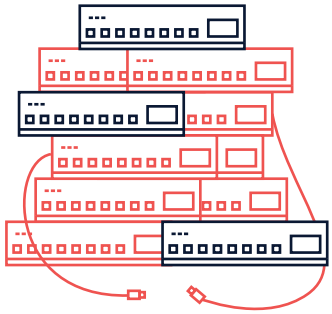
Like so many enterprises, Sun Rich's infrastructure became ever more complex with the growth of the organization. An MPLS network connected all facilities; Internet access was centralized in one location. Mobile users relied on a third-party service. Numerous security tools, such as firewalls and anti-malware, were needed to protect users. Connecting to Azure brought its own headaches. In short, Sun Rich was drowning in cost and complexity.

MPLS connections for the US sites were very expensive, limiting the amount of bandwidth to those locations. They also took far too long to deploy. "We looked at upgrading our WAN optimizer, but buying another expensive solution didn't make sense," says Adam Laing, systems administrator at Sun Rich.

The network architecture was impacting the business. Backhauling the Internet traffic to the datacenter coupled with the limited capacity at each location meant users experienced general "sluggishness" when accessing applications. "Today, you can't run a business on 3 Mbits/s connections to your branches," says Laing. "We ended up paying a lot of money for nothing."

They also struggled with reading and writing files to the shared file server at the datacenter. The company's ERP application requires the Remote Desktop Protocol (RDP). Users could also use RDP to access files from the share drives. The performance was slightly better than when the users accessed files directly from their desktops but if the files were complex, opening and saving work was challenging across the MPLS network. Employees resorted to copying large files to their desktops, circumventing sharing, security and backups. Printing was also impacted when executing the job from within the RDP environment. Requests were routed to the datacenter and then back to the local office printer, delaying print jobs.

Internet backhaul introduced other headaches. Connecting to Azure was difficult because "performance was not where it need to be," says Laing. "The limited performance would also have made migrating to Office 365 and SharePoint impossible", he says.



> “With an SD-WAN appliance, we could never remove MPLS because of Internet routing, things in the network, and things out of my control.”

SD-WAN Alone Not the Answer

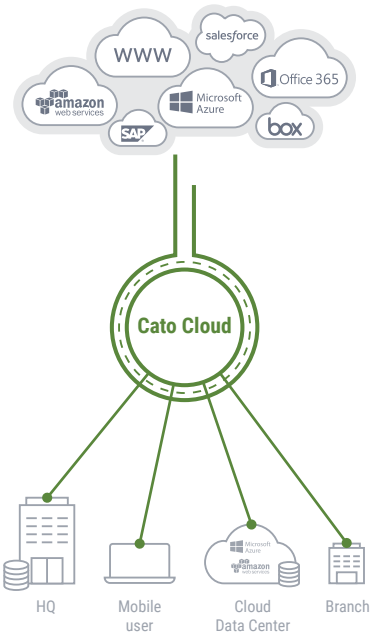
Sun Rich needed an alternative approach. Laing began by investigating SD-WAN appliances, connecting offices with multiple, active broadband connections. The US facilities were provided with direct Internet connections, secured with local firewalls, alongside their existing MPLS connections. The SD-WAN appliances directed internal traffic to the MPLS network and Internet traffic to the direct Internet connections.

Adding the appliance was effective for one site, but proved challenging for the other US location. The broadband connections did not have the same stability as the MPLS network. The lack of fiber meant Laing had to use DSL and eventually 100 Mbits/s cable to connect the location.

Internet routes, even in developed Internet regions, can underperform or perform erratically. To minimize the Internet’s impact, Laing followed SD-WAN best practice and connected his offices to multiple Internet links. No number of local links, though, could compensate for poor routing. The ISP bounced traffic from Sun Rich’s Pennsylvania office across 30 hops before reaching the datacenter.

Without control of the routing, the SD-WAN appliances were unable to improve the connection. “We opened a trouble ticket with the SD-WAN appliance vendor, but when the customer support agent saw our line speed met the committed rate, he said there was nothing he could do to help.” says Laing.

In the end, Laing was unable to achieve his goal. “We could never remove MPLS because of Internet routing issues,” he says. “Despite upgrading from 3 Mbits/s to 100 Mbits/s the users barely noticed a difference when connecting to the datacenter.”



Consolidate with Cato

With Cato, Laing found a solution that addressed all of his requirements. The Cato Cloud is an SLA-backed backbone that can replace MPLS by compensating for the latency, packet loss, and erraticness experienced across the Internet. Advanced security and network optimization functions run within the Cato Cloud, allowing Laing to simplify the network as it relates to firewalls, WAN optimization, routers, and SD-WAN appliances.

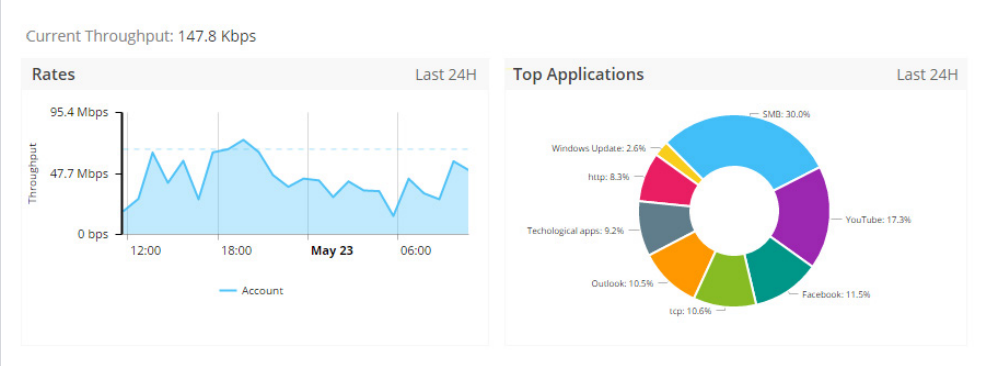
"When I saw Cato's presentation I literally thought to myself 'They're talking directly to me.'" Laing says. "Cato basically addressed every single issue on our network."

Sun Rich also gained far greater visibility and control with Cato. From a single management console, Sun RIch can see all of its cloud, site-to-site, and mobile traffic. No longer did Laing need to switch between different vendor products and services to understand network usage. Security policies can also be set for the entire network from Cato's management console, making updating and enforcing security that much easier.

> "When I saw Cato's presentation I literally thought to myself 'They're talking directly to me.' Cato basically addressed every single issue on our network."

Sun Rich's Azure experience improved for several reasons. Cato's PoPs share the same facilities as Azure, making application performance far faster than traversing the Internet. And by eliminating MPLS backhaul, Sun Rich reduced the latency for cloud applications. Migrating production workloads between the datacenter and Azure became much easier across the shared backbone. User experience also improved by no longer having to separately log into Sun Rich's datacenter and its Azure instance.

Finally, Cato's integrated approach is far more affordable. "Based on our size, our annual renewals on our appliances alone were nearly Cato's price, says Laing." Simplification also translates into better uptime. "You can troubleshoot faster with one provider than five providers," he says.



Sun Rich gained a comprehensive, detailed view of its network from the Cato management console.

> “ Cato has made our IT operation so much simpler and far more agile.”

Looking Ahead

Laing hopes to further simplify his network by connecting his mobile users with Cato’s mobile client. Public cloud applications and any new private cloud resources can be securely connected in the future, as needed.

CATO— NETWORKS

For more information:

www.CatoNetworks.com

@CatoNetworks

About Cato

Cato Networks provides organizations with a cloud-based and secure global SD-WAN. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people, and data. Cato Cloud cuts MPLS costs, improves performance between global locations and to cloud applications, eliminates branch appliances, provides secure Internet access everywhere, and seamlessly integrates mobile users and cloud datacenters into the WAN.

Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, co-founder of Check Point Software Technologies and Imperva, and Gur Shatz, co-founder of Incapsula.

Where do you want to start?

- SECURE CLOUD-BASED SD-WAN
- AFFORDABLE MPLS ALTERNATIVE
- BRANCH APPLIANCE ELIMINATION
- CLOUD DATACENTER INTEGRATION
- MOBILE ACCESS OPTIMIZATION
- SIMPLE NETWORK AUTOMATION

Global Backbone. Cloud-Based SD-WAN. Firewall as a Service. All in One