AdRoll Transforms Mobile VPN Access to Amazon AWS with Cato

Background

AdRoll provides a marketing platform for creating personalized advertising campaigns using an advertiser's website data.

The company has approximately 500 employees spread across six main locations around the globe and 350 offsite contractors. A cloud-centric business, the company has three datacenters in Amazon AWS.

Traditional Mobile VPN Challenges

Like many companies, AdRoll saw networking pains grow as the company matured. Internet performance was a problem for the company's offsite contractors. They had to establish virtual private network (VPN) connections to the company's San Francisco firewall and from there they connected to the Internet and AWS. The traffic backhaul created a chokepoint, adding latency and saturating the San Francisco Internet connection.

Redundancy was also an issue. Locations were equipped with dual firewalls for local redundancy, but there was no geo-redundancy. Should the San Francisco site become inaccessible, the contractors were unable to work. "It puts a lot of stuff in one basket,'" says AdRoll's Global Director of IT, Adrian Dunne, "Once, the VPN on our primary firewall rebooted. Suddenly, 100 engineers couldn't work anymore."

Onboarding new users was cumbersome, particularly for contractors whose machines AdRoll did not control. Dunne and his team had to send them configuration instructions for their VPN clients. "Using the Mac's management software to push out VPN configurations to users was a pain," he says.

There were also security issues as the VPN required users be granted access to all network resources not specific applications. Nothing prevented a user who only needed access to the company's Web application, for example, from using SSH to connect to the company's routers. "Traditional VPNs meant opening the door to everything," says Dunne.

Ultimately, Dunne found the appliance-centric approach to mobile connectivity constrained his operation. "When we moved our San Francisco office, we had to treat our firewall relocation like an organ transplant," he says, "We ran down the stairs with the firewall, jumped into a running car, drove across the city, and ran it up the stairs to minimize downtime. That's not scalable or how I want to live my life."

Cato Globally Optimized and Secure Mobile Access

Dunne and his team had already experienced the value of cloud services with AWS. It provided his broader IT efforts with redundancy, geo coverage, and backhaul elimination. He wanted to mirror that success with his VPN solution, which is why he turned to Cato.

Cato Cloud provides a global, SLA-backed backbone that connects remote mobile workers and branch offices to corporate resources, such as cloud datacenters, and enforces granular access policies.

With Cato, Dunne solved his contractors' latency problems. Instead of backhauling their traffic to San Francisco, contractors now run the Cato mobile client and connect to Cato Cloud. The company's Amazon AWS datacenter connected to the Cato Cloud using a Cato initiated IPsec tunnel. With both users and datacenters connected to Cato, a single network is formed. Traffic from mobile users is sent across the optimized backbone directly to AWS. Eliminating the San Francisco chokepoint also reduced the congestion on the San Francisco Internet line.

Onboarding new users became much simpler. "With Cato, we just send a user an invite to install the client," he says, "It's very much like a consumer application, which makes it very easy for users to install." Perhaps the best measure of his success has been what users haven't said. "From our users, we have peace and quiet," he says, "Nobody will come and say, 'Thank you for the VPN.' They expect it to work, but silence is gold."

One converged, global WAN now connects AdRoll's cloud resources, locations, and mobile users.

Improved Security Posture is Good for Business

Cato also gave AdRoll better control over permissions for mobile users, determining the resources they can access at a very granular level. "With Cato, we can control what VPN access looks like for our contractors, sales people, and locations and that really spoke to us," says Dunne. "Now there's no concern about users getting into our routers," he says.

Dunne and his team have also gained deeper insight into cloud usage. "Now we can see who's connecting when and how much traffic is being sent, information that was unavailable with our previous VPN provider," he says. "Correct oversight and monitoring of logs ties directly into the bigger security conversation."

But more than providing "just" better management, Cato has helped AdRoll attract larger customers. "Fortune 500 customers do their due diligence and ask about access control, data flows, log review, and stuff like that in their RFPs," he says, "Cato gives us the ability to tick the "yes" box and shorten the time to get in front of the customer. There was a direct impact on our bottom line."
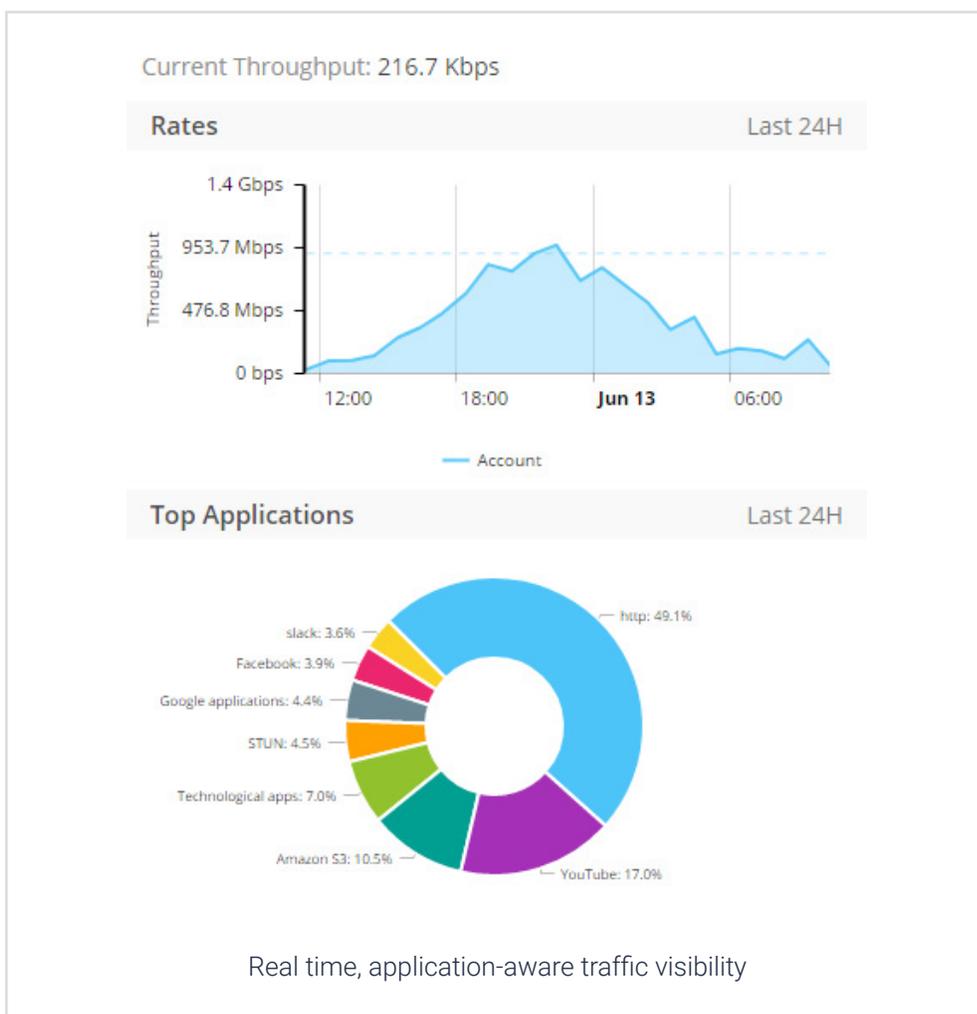

Real time, application-aware traffic visibility

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.

For more information:

🌐 www.CatoNetworks.com

🐦 @CatoNetworks

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