Cato Networks Re-Architects NeedToChange (NTC) WAN to Boost Capacity, Availability, Performance and Security

Current State of NTC's WAN

The Wide Area Network (WAN) was built to connect static and physical locations, not today's fluid and dynamic networks. Like many other companies, NTC depends on expensive and limited MPLS-based WAN for remote branch connectivity. NTC backhauls internet traffic as their small and medium remote sites don't have a security stack in place, resulting in the "trombone effect" (high latency and poor user experience) when accessing a business application hosted on SaaS and IaaS platforms. NTC has no control and visibility for employees working outside a company facility, and the plan to adopt SaaS applications and to connect thousands of IoT devices requires a new architecture to support this business transformation.

NTC's Network Challenges
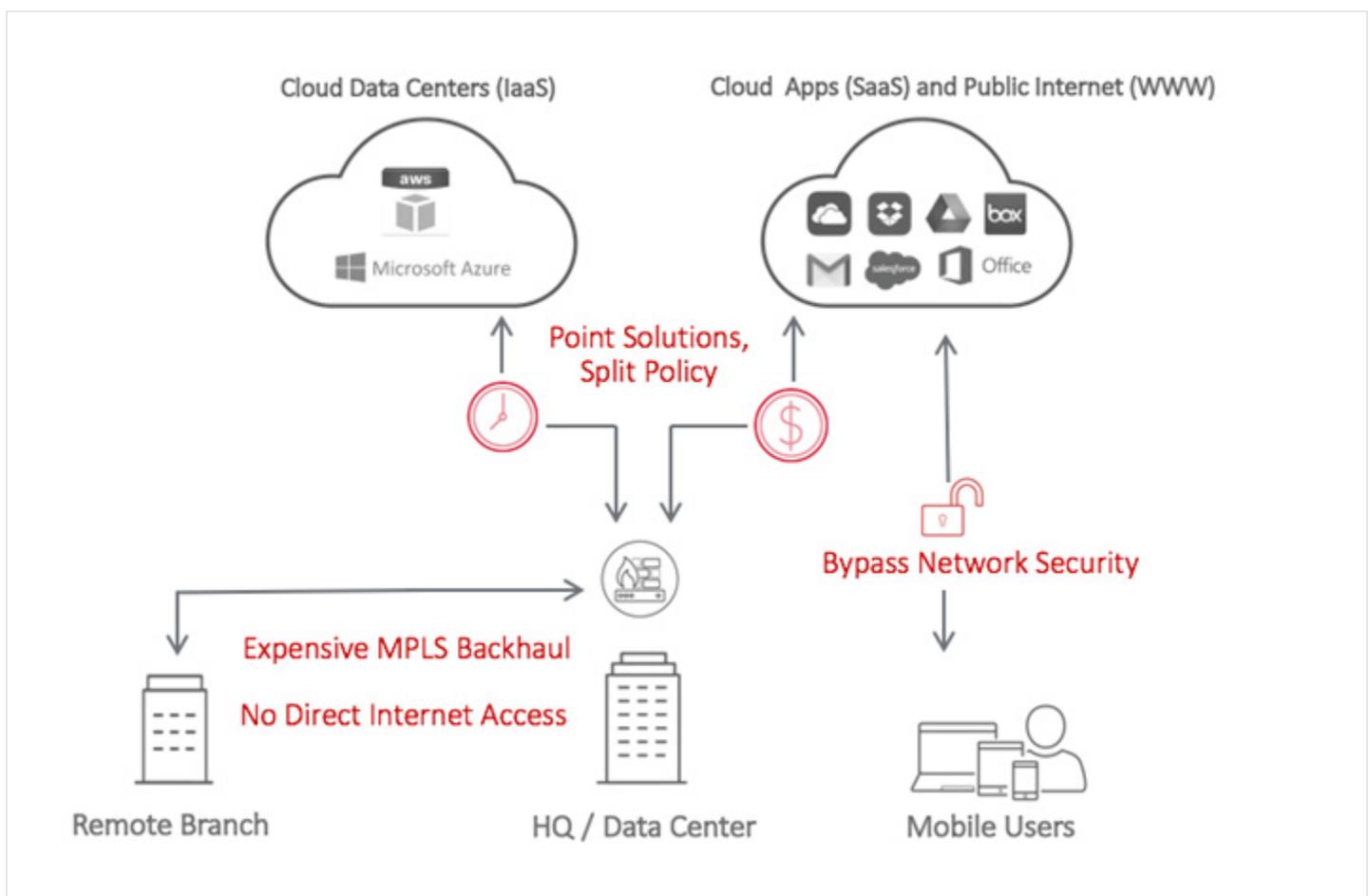
Cato Networks: Software-Defined and Cloud-Based Enterprise Network

Cato will enable NTC to efficiently and securely connect all branch locations, the mobile workforce, physical and cloud data centers, into a global software-defined and cloud-based secure enterprise network. All outbound traffic, both WAN and internet, is consolidated in the Cato Cloud, where a set of elastic and agile security services are applied to protect access to enterprise applications and data, regardless of their location. The Cato Cloud service is comprised of the following pillars:

Cato Cloud Network

A global, geographically distributed, low-latency and SLA-backed network of PoPs, interconnected by multiple tier-1 carriers. NTC will connect to Cato over optimized and secured tunnels. Physical locations use the Cato Socket; a small, zero touch, tunneling device that controls and splits traffic across WAN links based on business policy. Traffic transmitted via the internet is encrypted and optimized end to end. Cloud data centers, like Amazon VPC, use a virtual version of the Socket (Cato vSocket). Lastly, mobile users use the Cato Client to establish a secure tunnel for laptops, tablets and smartphones.

Cato Security Services

A fully integrated suite of enterprise-grade and agile security services directly built into the cloud network. The services include a NG firewall, URL filtering, anti-malware and more, have no capacity constraints and are continuously updated to introduce new capabilities and adapt to emerging threats. The integrated network and security stack enables NTC to enforce its corporate policy on all traffic, WAN and internet, from all locations and users.

Cato Cloud High Level Architecture
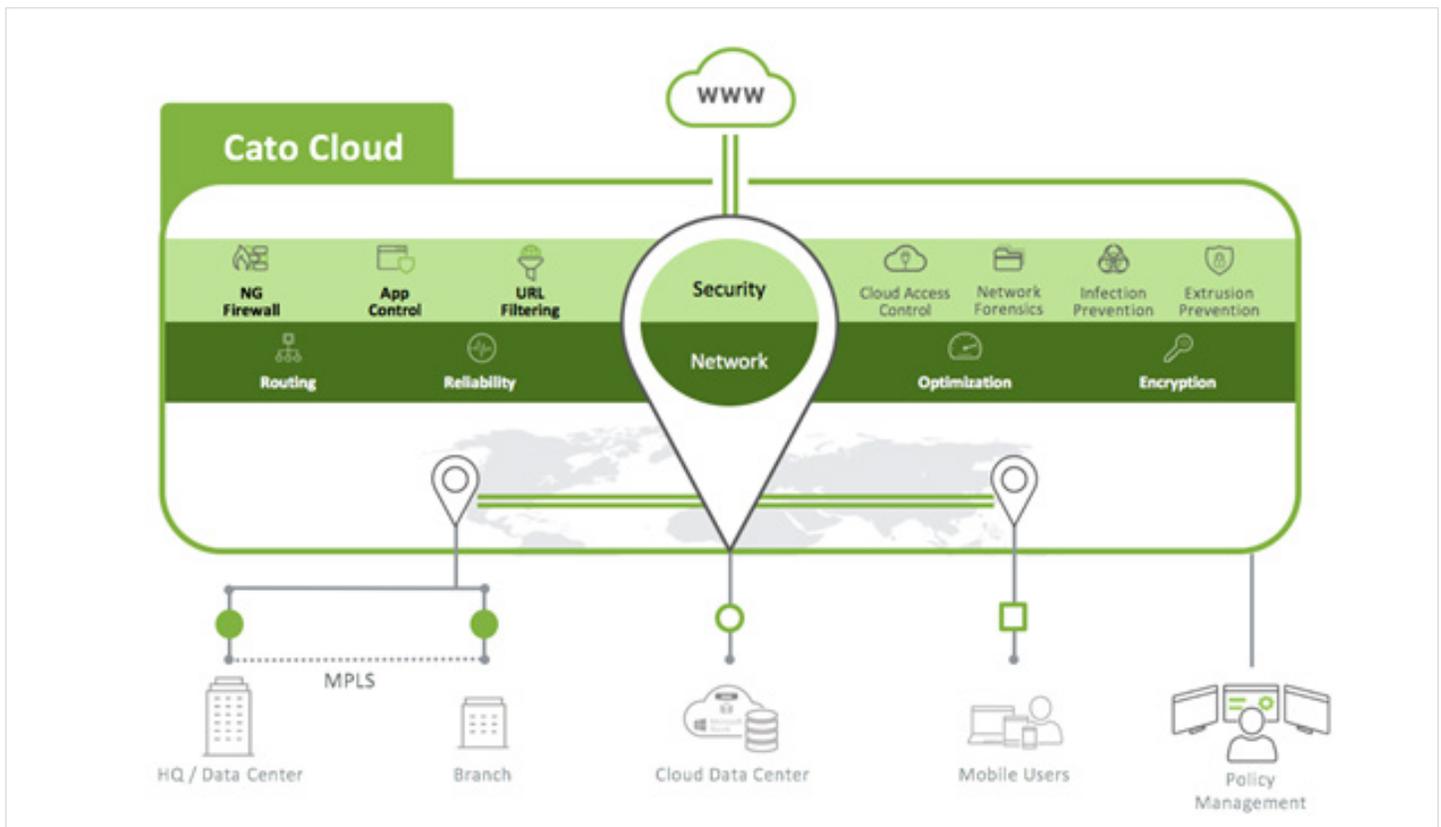
Recommendation:
Migrate to Cloud-Based SD-WAN with Built-in Security

To meet NTC's business needs and to future-proof the network, Cato recommends a cloud-based SD-WAN architecture that connects, secures, and simplifies NTC's global WAN following the 3 steps below.

Step 1: Expand WAN Capacity and Availability, and Add Policy-Based Routing to Meet Application Delivery Goals

Last Mile extension
NTC should deploy additional internet links in the locations currently served only by MPLS. Cato suggests NTC considers replacing MPLS with Cato, dual ISP links and optional 4G/LTE backup per below. Ultimately all sites will have either MPLS+Internet or 2 Internet links.

Policy-based routing
NTC will deploy a Cato Socket at each branch location and connect it to the available MPLS, internet and 4G links. Specifically, the internet links will connect the branch to the nearest available Cato PoP. Cato classifies and dynamically allocates traffic in real time to the appropriate link based on application policies and link quality (availability, utilization, latency, packet loss). NTC will specify these policies for SAP, PDM, Voice and Video to set prioritization and required service levels. With Cato, even the "internet leg" enjoys SLA-backed latency compared with the unmanaged public internet so it can offload more traffic off the MPLS link.

High availability, resiliency and quality
The Cato Socket can drive the WAN links in Active/ Active mode to boost overall capacity and reach 99.99% availability. Forward Error Correction (FEC) is intelligently applied to reduce the impact of packet loss on latency and quality.

Latency control for WAN and cloud locations
Unlike appliance-based approaches, Cato's SLA-backed backbone guarantees latency and availability over the long haul WAN (for national and global locations). The Cato backbone is fully redundant across servers, PoPs and regions and is co-located with Microsoft Azure and Office 365 datacenters for optimized access.

Meeting application delivery goals
With all the enhancements above, NTC will improve access to SAP, PDM and Office 365 and is in a great position to eliminate MPLS even for latency sensitive applications like voice and video.

Step 2: Eliminate Internet-Bound Traffic Backhauling with Secure Direct Internet Access

With all branches connected to Cato Cloud, NTC employees can directly access the internet and cloud applications (i.e. office 365) behind Cato's enterprise grade and cloud-based security services. These services protect branch and mobile employees against threats, and can restrict access to critical applications as well as applications that violate corporate policies. All security capabilities are delivered without dedicated branch security appliances or regional co-location facilities.

Step 3: Extend the WAN and Security to Cloud Data Centers and the Mobile Workforce

NTC will use Cato vSockets to connects any IaaS platform (Such as AWS and Azure) to the Cato Cloud, making it an integrated part of the network. Instead of backhauling DR traffic over MPLS, NTC will use direct internet access to route traffic via the Cato Cloud between the data center and the DR location. NTC mobile users will deploy Cato Clients to connect Windows, Mac, iOS and Android devices to the the nearest Cato Cloud PoP. Users gain secure and latency-optimized access to NTC's physical and cloud datacenters as well as public cloud applications.

Transformation Done:
NTC's New Secure and Software-Defined WAN

With full migration to the Cato Cloud, NTC will achieve the following:

- All NTC's data centers, branches and users are connected to a high capacity, redundant, optimized, affordable and secure WAN.

- Full protection of all traffic for both datacenter, cloud and internet resources that seamlessly scales to accommodate growth and adapt to emerging threats.

- Central management of all policies including full site-to-site mesh, network segmentation, access control, and security.

- Instant deployment of new sites with Cato Socket 10-minutes self provisioning.

- Full visibility into the network usage and security events for every location, application and user that simplify end-to-end troubleshooting of performance and security issues.

Network View in Cato Management Application
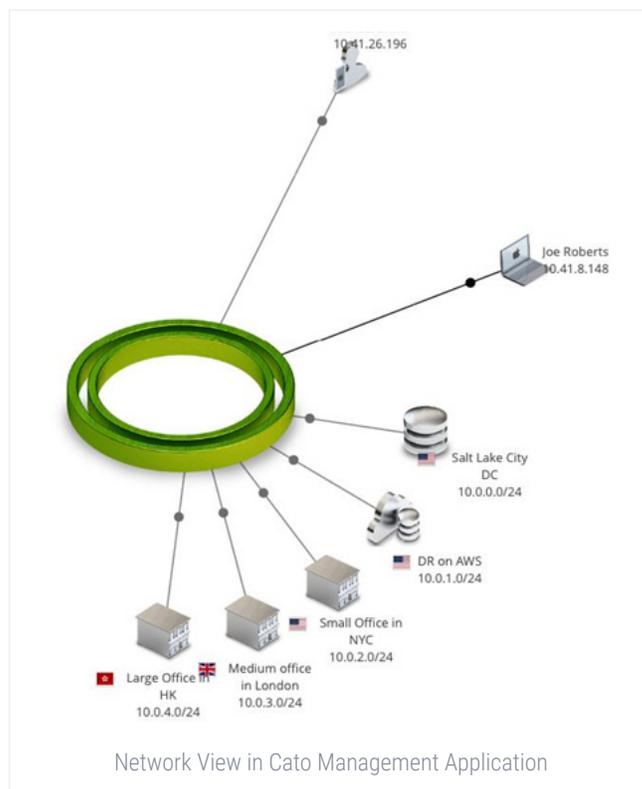
Summary

Cato provides NTC a flexible, software-defined WAN with built-in secure direct internet access, a SLA-backed global backbone, and seamless integration of cloud infrastructure and mobile users. By moving to Cato, NTC eliminates complexity, reduces costs, streamlines day-to-day operations and ensures scalability for the enterprise's future growth.