The 2017
Guide to WAN Architecture & Design

Part 2: WAN Evolution

By Dr. Jim Metzler, Ashton Metzler & Associates
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Platinum Sponsors:

CATO NETWORKS

CLOUDGENIX
NETWORKS WITHOUT NETWORKING

cradlepoint

LiveAction™

nuagenetworks

TALARI Networks™

velocloud™

Table of Contents

Executive Summary

The wide area network (WAN) is a critically important topic for number of reasons. Those reasons include:

- The latency, jitter and packet loss that is associated with the WAN often cause the performance of applications to degrade;
- The WAN can be a major source of security vulnerabilities;
- Unlike most of the components of IT, the price/performance of WAN services doesn't obey Moore's Law;
- The outage of a WAN link often causes one or more sites to be offline;
- The lead time to either install a new WAN link or to increase the capacity of an existing WAN link can be quite lengthy.

A discussion of wide area networking is extremely timely for two reasons. One reason is that, for the first time in well over a decade, the wired WAN is the focus of considerable innovation which is leading to the deployment of a wide range of new WAN-related products and services. The second reason is that on a going forward basis, the WAN needs to support a new set of requirements such as providing connectivity to a growing number of mobile workers and public cloud providers as well as to the Internet of Things (IoT).

The primary goals of the 2017 Guide to WAN Architecture and Design (The Guide) are to make enterprise network organizations aware of the emerging alternatives to the traditional approaches to WAN architecture, management and security and to help them understand the key differences in those alternatives.

The Guide will be published both in its entirety and in a serial fashion. This document, Part 2, is the second of the serial publications. This document contains the description of a hypothetical company called NeedsToChange and it also contains how each of the sponsors suggests that NeedsToChange should evolve its WAN. In order to cover a wide array of technical and business environments, each sponsor was allowed to embellish the description of NeedsToChange to bring out any reasonable characteristics of the overall WAN environment.

The other sections of The Guide are:

- Part 1
  This section focused on providing insight into the current state of the WAN. This document contains the results of a survey that was distributed in May of 2016. Throughout The Guide the network professionals who completed the survey will be referred to as The Survey Respondents.

- Part 3
  This section will have two primary sub-sections. One sub-section will summarize the key WAN architecture, management and security considerations that were brought out in Part 2. The second sub-section will be a detailed call to action.

- Complete copy
  The final publication will consist of an executive summary and Parts 1 – 3 as described above.

Hypothetical Company: NeedsToChange

Each of the 7 sponsors was given the description of a hypothetical company: NeedsToChange. The goal was to present each sponsor with the description of a company that has a traditional WAN and ask them to provide their insight into how the company should evolve its WAN.

Even within the context of a traditional WAN, there is a wide breadth of options relative to a company's WAN topology, services, applications and goals. As a result of this breadth, it wasn't feasible to cover all possible options in a reasonably sized description of NeedsToChange's WAN. In order to limit the size of the description of NeedsToChange's WAN and yet still bring out a wide array of important WAN options, each sponsor was allowed to embellish the description of NeedsToChange's WAN. They could, for example, add additional data centers or key applications; vary the amount of traffic that was backhauled; prioritize the factors impacting NeedToChange's WAN or identify business drivers such as the need to support mergers and acquisitions.

Below is the description of NeedsToChange's WAN that each sponsor received.

1. **Data Centers**
   NeedsToChange has a class A data center in Salt Lake City, Utah. The site has two diversely routed T3 links into an MPLS network and a 100 Mbps link to the Internet.

2. **Traffic Prioritization**
   In the current environment, traffic is prioritized in a static manner; e.g., voice traffic always gets top priority and it receives a set amount of bandwidth.

3. **Business Critical Data Applications**
   Two of NeedsToChange's business critical applications are SAP and Product Data Management (PDM). PDM is NeedsToChange's most bandwidth intensive application, however it is widely understood that NeedsToChange runs its business on SAP and so the performance of SAP is critical. In addition to the applications that NeedsToChange uses to run its business, the company uses an Infrastructure as a Service (IaaS) provider for disaster recovery (DR).

4. **Public Cloud Computing Services**
   Other than its use of an IaaS site for DR, NeedsToChange currently makes relatively modest use of public cloud computing services. However, the company has started to implement Office 365 and the decision has been made that on a going forward basis, unless there is a compelling reason not to do it, any new application that the company needs will be acquired from a Software as a Service (SaaS) provider.

5. **Voice and Video**
   NeedsToChange supports a modest but rapidly growing amount of real time IP traffic, including voice, traditional video and telepresence.

6. **Internet Access**
NeedsToChange currently backhauls over half of its Internet traffic to its data center in Salt Lake City. The company is looking to enable direct Internet access from their branch offices but they are concerned about security. NeedsToChange is also concerned that it is supporting non-business related Internet traffic that is negatively impacting business traffic.

7. **Mobile Workers**
Roughly half of NeedsToChange's employees regularly work somewhere other than a company facility.

8. **Guest Workers**
NeedsToChange's network organization is considering offering guest WiFi access from at least some of its facilities.

9. **Branch Offices**
NeedsToChange categorizes its branch offices into three categories: small, medium and large.
    - A small office/site has between 5 and 25 employees. These sites are connected by an MPLS network with each site having either a single T1 link or multiple T1 links that are bonded. All of its Internet traffic is backhauled.
    - A medium office/site has between 25 and 100 employees. These sites are connected by an MPLS network with each site having capacity between a single T1 link and a link running at 10 Mbps. All of its Internet traffic is backhauled.
    - A large office/site has more than 100 employees. These sites are connected to an MPLS network either by using bonded T1 links or by a T3 link. They also have direct Internet connectivity which in most cases runs at 10 Mbps over DSL.

10. **Branch Office Availability**
NeedsToChange wants to improve the availability of the WAN access at its branch offices and has established a goal of 99.99% availability.

11. **IoT**
The company has begun a smart business initiative which the company believes is just the first in a number of initiatives that will quickly drive the need for them to support thousands, if not tens of thousands, of devices.

12. **Visibility**
In the majority of instances in which the performance of one of NeedsToChange's business critical applications begins to degrade, the degradation is noticed first by the end users. In addition, the time it takes to identify and resolve performance problems has been increasing.

13. **Regulations**
NeedsToChange is subject to PCI compliance. That is just one factor driving NeedsToChange to seek out ways to increase its security.

14. Factors Driving Change

While not in priority order, the following factors are driving NeedsToChange to seek alternative WAN designs:

- Improve application performance, notably for SAP;
- Reduce cost;
- Increase uptime;
- Reduce the time it takes to identify and remediate performance problems;
- Increase security;
- Reduce complexity;
- Provide access to public cloud computing services in general and Office 365 in particular;
- Provide better support for real time applications;
- Reduce the time it takes to implement new network services;
- Increased agility both in terms of supporting new facilities and in supporting growth within existing facilities

Balancing off the factors driving NeedsToChange to seek alternative WAN designs is the fact that NeedsToChange will not be allowed to increase the size of its network organization.

Vendor Responses

Below is a description of how each of the 7 sponsors suggests that NeedsToChange should evolve its WAN.

Introducing the Next Evolution of Wide Area Freedom

Overview of the NeedtoChange Network Environment

The constructs for wide area networking at NeedToChange (NTC) have remained stagnant for over 20 years. Network connectivity (such as a managed MPLS-based VPN service) is purchased from a Service Provider via a multi-year contract. Then, the networking team rolls out routers to the branch and applies a site-specific configuration that creates the network topology based on a hub-and-spoke (HQ-to-branch) architecture.

The workflow for these network rollouts is rigorously managed with formal project management, specialist personnel and change control processes to ensure any deployment or augmentation to the WAN happens with minimal disruption to the business.

WAN bandwidth is expensive and thus in limited supply, so the skill in WAN management is squeezing the last drops of performance out of a finite resource. At NTC this has been achieved with advanced configurations within the branch routers or the addition of network appliances — both approaches that increase network complexity.

How Cloud-Based IT Consumption is Affecting the Branch

Today's IT environment is being hampered by the rigidity of the wide area network. Historically, traffic has been client-to-server, so a hub-and-spoke WAN design fitted NTC's needs well. Remote branches were clients to the Utah datacenter servers. But now with Cloud IT, traffic patterns have changed. NTC has virtualized its Utah datacenter and the critical Customer Relationship Management (CRM) and Product Data Management (PDM) applications reside on virtualized compute systems.

As the demand for these applications increases, the virtual compute environment flexes to accommodate the workload. This means that the application does not always reside in the same rack or row of the datacenter. In disaster recovery situations, for example, it is relocated to a completely different datacenter. Unfortunately, outside the datacenter, NTC's network architecture is static and cannot easily adapt to dynamic demand. To resolve this inflexibility with the current architecture NTC must either overbuild the network (inefficient and expensive) or reconfigure the network on the fly (manually intensive and high risk).

A similar shift in consumption is occurring on the client side of the network within the branch. Today any NTC employee connecting to the CRM is the client, but only for that application session. NTC has embarked on a new set of IP-based collaboration tools to improve workflow and communications across the organization, including instant messaging, desktop videoconferencing and IP voice. Now any employee in any branch can initiate a desktop video session to any employee in another branch. In this scenario, the employee's PC becomes the host or source of the traffic. This direct branch-to-branch communication is not handled efficiently in an HQ-to-branch (or hub-and-spoke) network architecture.

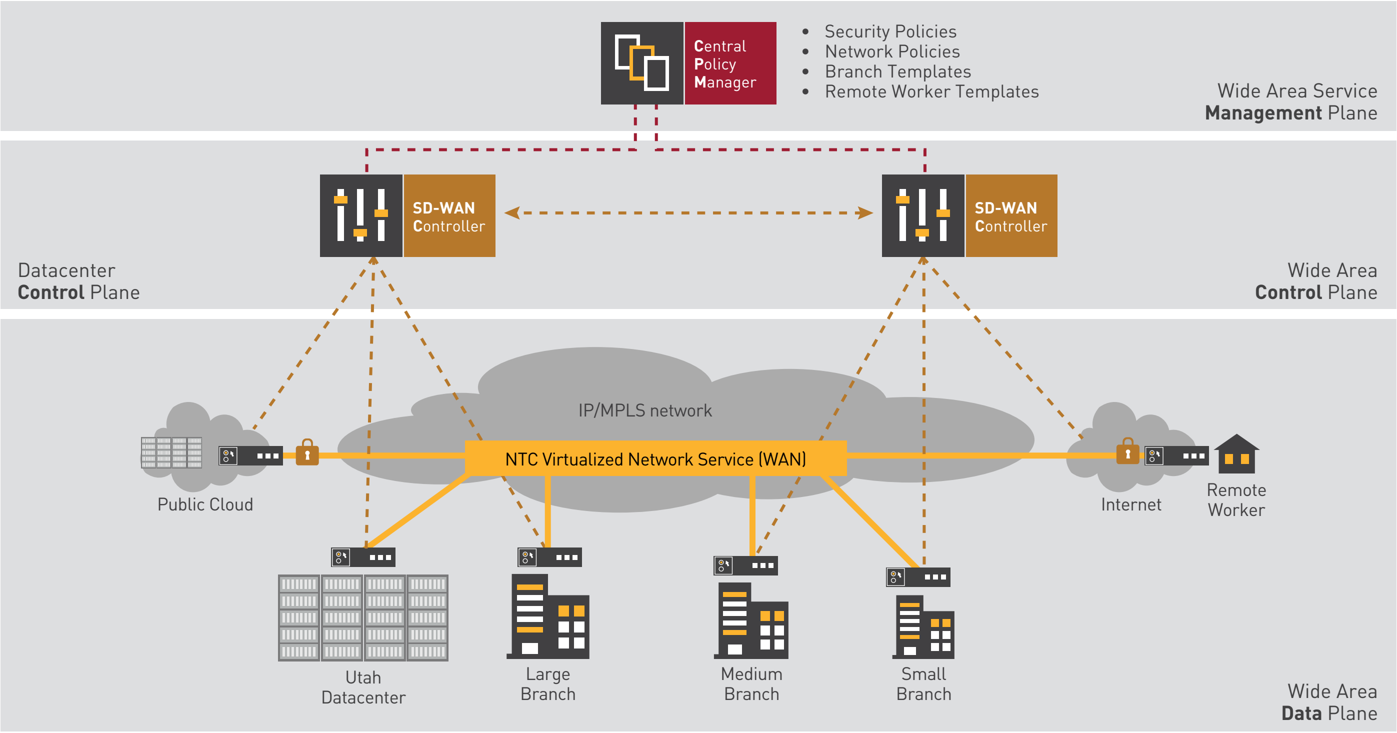
Unconstrained Networking, Datacenter to Branch

To address new business communication standards and Cloud-based IT, enterprises must re-examine what they need from the WAN. Some key areas of change that should be considered by NTC are:

- Change the network topology from hub-and-spoke to meshed network architecture to facilitate efficient branch-to-branch and branch-to-datacenter/cloud communications
- Manage premium bandwidth with secure Internet offload at the branch
- Reduce WAN operational overhead with centralized network policy enforcement
- Investigate alternative connectivity options on a per state, region or branch location basis
- Treat the datacenter and WAN at NTC as a single entity with common management, monitoring and reporting tools

In order to drive these benefits into its business NTC needs to deploy a virtualized network service WAN environment. This will deliver expansive wide area networking that matches the flexibility of cloud-based IT.

FIGURE 1. NTC virtualized network service architecture



With software defined wide area networking (SD-WAN) there are three key planes (or layers of network functionality) that will assist in this delivery (see Figure 1):

- **Service Management Plane:** A policy system that centrally administers the network templates and policies. This layer should provide the visibility and control of the NTC network via an intuitive GUI. Templates can be created per branch type and automatically deployed when the branch equipment is deployed. All visibility and control aspects of the NTC WAN are managed via this WAN service management layer.
- **WAN Control Plane:** This layer contains the SD-WAN-based controllers that manage the control plane of the NTC WAN. Predominantly deployed in pairs, these controllers manage the network connections between the endpoints (branches, Utah datacenter and public cloud) of the NTC network.
- **WAN Data Plane:** Open compute (x86-based) branch equipment is deployed at the remote branch locations and datacenter connection points, and at the public cloud interconnect to provide enterprise-wide control of the network. These "branch devices" should support both a virtual deployment option (in a public cloud or on an existing branch server) and a dedicated hardware form factor. In either case (virtual or physical) management is provided by the service management planes with data forwarding control provided by the WAN control plane (SD-WAN controllers).

Any-to-Any Network Connections

NTC can implement a fully meshed network architecture to facilitate branch-to-datacenter and branch-to-branch communications. This provides the flexibility to transport inter-site traffic across the most efficient path. Rich IT communication tools can be deployed to enhance the collaboration between branches without the constraints of the rigid hub-and-spoke architecture of the past.

Intelligent Traffic Offload

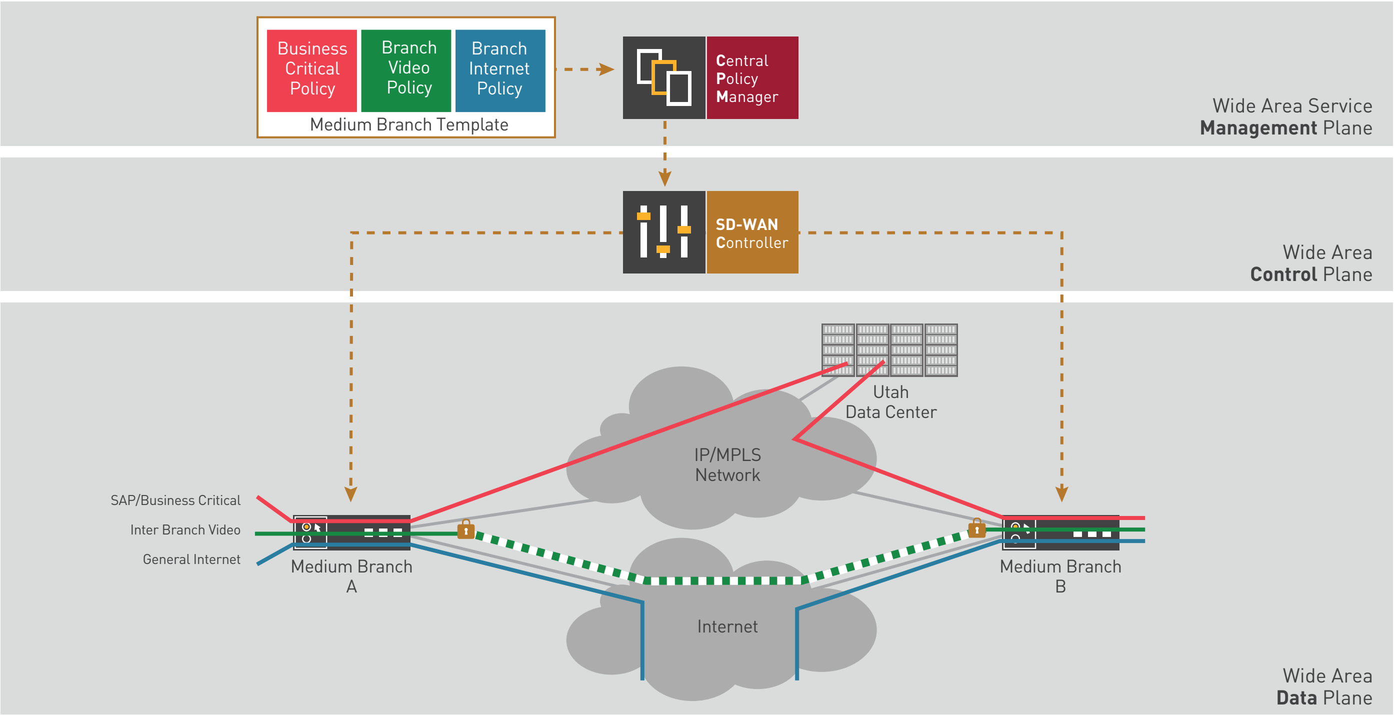
Via the central policy system, the NTC network team implements the network policy that securely offloads any Internet traffic at the branch (see figure 2). There are three key benefits of this feature. First, the limited IP-VPN bandwidth is only used for business critical voice and data, which maximizes its availability for critical data. Second, via this policy a secured inter-branch tunnel can be created to force high-bandwidth usage across an encrypted Internet path. The third benefit of the intelligent traffic offload feature is the ability to use the Internet connection as a backup link in case the IP-VPN circuit fails. Using the same template-based policy push from the central management system, all branch traffic can be encrypted and sent over the Internet to the Utah datacenter. This provides additional resiliency and enables NTC to improve network availability at the branch.

Policy-Based Network Management

With the right SD-WAN solution, management and monitoring of the NTC WAN environment can be simplified via a policy-based manager. The policy manager can create policies for NTC traffic at many levels and these policies can be simply grouped together into templates. The templates can be deployed automatically when an application changes (for example, if CRM is relocated to the disaster recovery

> Traditional hub-and-spoke WAN designs inhibit the efficiency of today's rich collaboration tools

FIGURE 2. Using policies to intelligently offload traffic



datacenter) or a new branch is added. These policies can be split into four key types:

- **Application policies:** These are the conditions each application needs to function across the network and can include specific security, quality of service and resiliency requirements. For instance, a policy for the CRM application may include QoS policies for interactive, batch and print traffic. This provides granular control of how individual flows are handled by the network. The CRM print traffic at the branch can be lower in priority to ensure that it doesn't affect the performance of the critical interactive traffic.
- **Branch policies:** These include the network functionality for specific or types of branches in the network. A branch may be a physical location or a virtual location, such as a public cloud interconnect where a new NTC application resides. NTC networking staff can deploy policies for the use of backup links, enforce encryption or automate equipment password changes across all branches.
- **Security policies:** User-based permission means network security can be managed by a specialty team. The security team can set the security policies on an application or branch level. For instance, the team can specify the mandatory time period for all branch device password changes or encryption keys exchanged. Once this policy is set it is called on by the operational team in the deployment of applications or branches. User-based permission functions ensure that the security policies are implemented, which guarantees compliance with NTC's security framework. And the single control point for policy enforcement reduces the complexity of regulatory/industry auditing.
- **Network policies:** These are the network wide policies that control the flow of traffic across the NTC network. Examples include the overall quality of service policy that prioritizes CRM, PDM and voice traffic over general inter-office traffic.

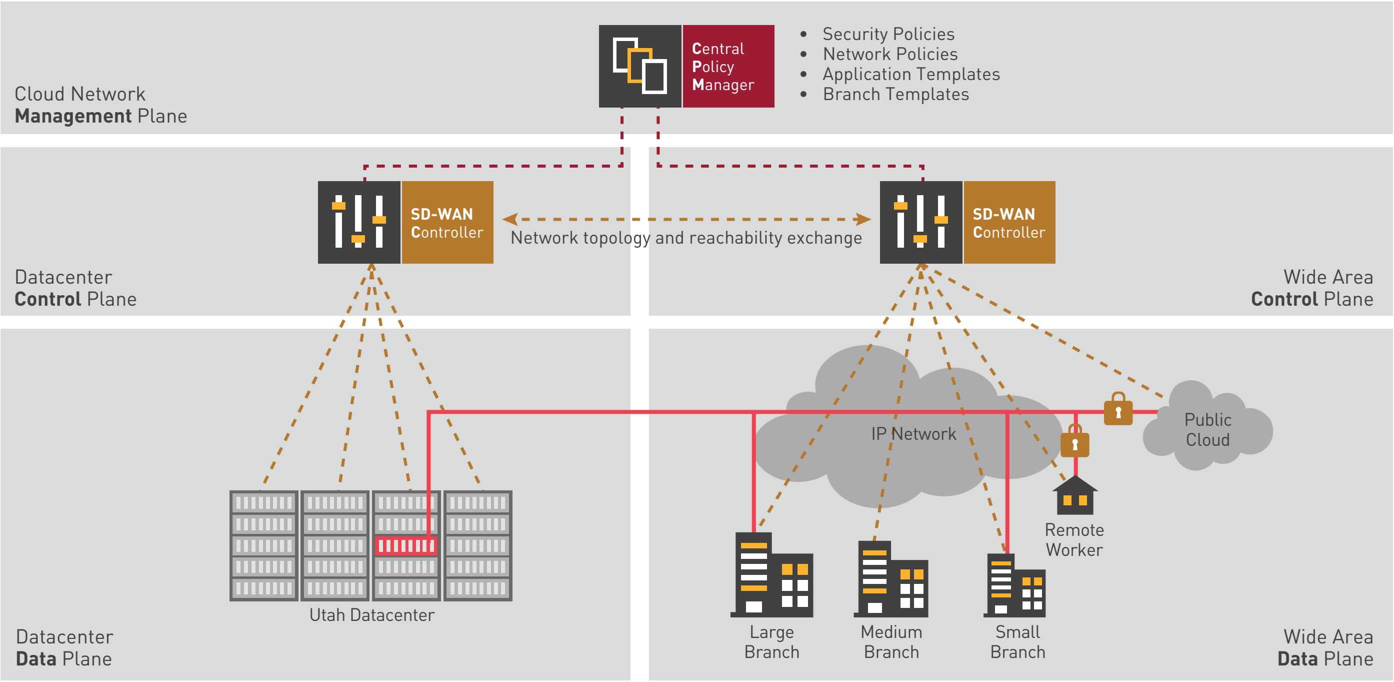
Using these policies, templates for deployments can be created, such as the Intelligence Traffic Offload example provided earlier. Any number of policies can be grouped into a template. For example, a template could be designed for all medium-sized branches. It could include a policy on application forwarding (the three colored flows shown in Figure 2) plus a standard security policy for equipment so encryption keys and passwords are changed in accordance with any regulatory or business requirement. These templates could be called on whenever a new site is added to the network.

Relying on templates reduces the need for specialized personnel to visit the branch location. The branch equipment can be couriered to the branch manager with simple instructions to connect to the WAN links. Once connected the device will "call home" to the policy manager, authenticate and the template configuration will be sent over the WAN to the device.

Network Functions Virtualization

SD-WAN also provides the opportunity to reduce the reliance on external network devices at the branch. For many enterprises the only option to enhance network performance and security has been to deploy high CAPEX physical devices (such as firewalls and WAN accelerators) at the branch. These point solutions increase CAPEX up front and increase network complexity, which in turn drives up OPEX for maintaining the WAN environment.

FIGURE 3. Seamless interworking with SD-WAN



Comprehensive SDN-based WAN solutions use Network Functions Virtualization (NFV) to provide this enhanced functionality. Software features are "chained" into the traffic flows to and from the branches. By adopting this approach, NTC could enable a more robust and dynamic end-to-end policy that inserts the right network functions into the right locations to ensure data integrity at the branch, without the large CAPEX drain of physical devices.

Service Provider Independence

SDN provides the separation of the NTC WAN (overlay service) from the underlying IP transport (MPLS IP-VPN) network. With traditional WANs these are tightly integrated; with SD-WAN they can be completely separated. This separation delivers a new set of options for getting bandwidth across the WAN and into the branch. It means that NTC can procure the required IP connectivity services on a per-branch or per-region basis and use these links as an underlay network for the WAN. This gives NTC access to the world of competitive local carriers and alternative access technologies. If IP-VPN connections aren't available at a site then 4G/LTE mobile broadband, cable or DSL technologies can be deployed to provide the connection.

Summary

To gain maximum benefit from the move to SD-WAN, the operation and purpose of the network(s) in the enterprise need to be rethought. The network is there to connect the new cloud IT environment to business users regardless of their locations.

Implementing SDN in the datacenter and across the WAN is a great start. However, to drive a change across the whole business these two critical network islands need to operate in concert and that means removing any management boundaries that separate them.

The key to seamless interworking is the use of a single network policy framework that distributes business policies and network intelligence across both domains. SD-WAN provides the opportunity to achieve this. If SD-WAN is controlling the network that underpins cloud applications and is managing the connectivity across the WAN towards the applications' end users (employees and/or customers) then centralizing this intelligence onto an overarching policy and control framework makes sense.

With the right SDN-based WAN solution, NTC can achieve exactly this: unconstrained networking for the datacenter and beyond. To gain maximum benefit from the move to Cloud IT, NTC needs to centrally manage the datacenter and wide area networks with a single policy framework. This simplifies the overall network configuration. The enterprise can change a security policy once and have the network automatically roll that change out. Add a new application to the business and instantly deploy the updated network, branch and security policies. No more waiting for project rollouts, no more specialist personnel needed at the branch.

With this new network environment in place, NTC will get wide area networking on its terms.

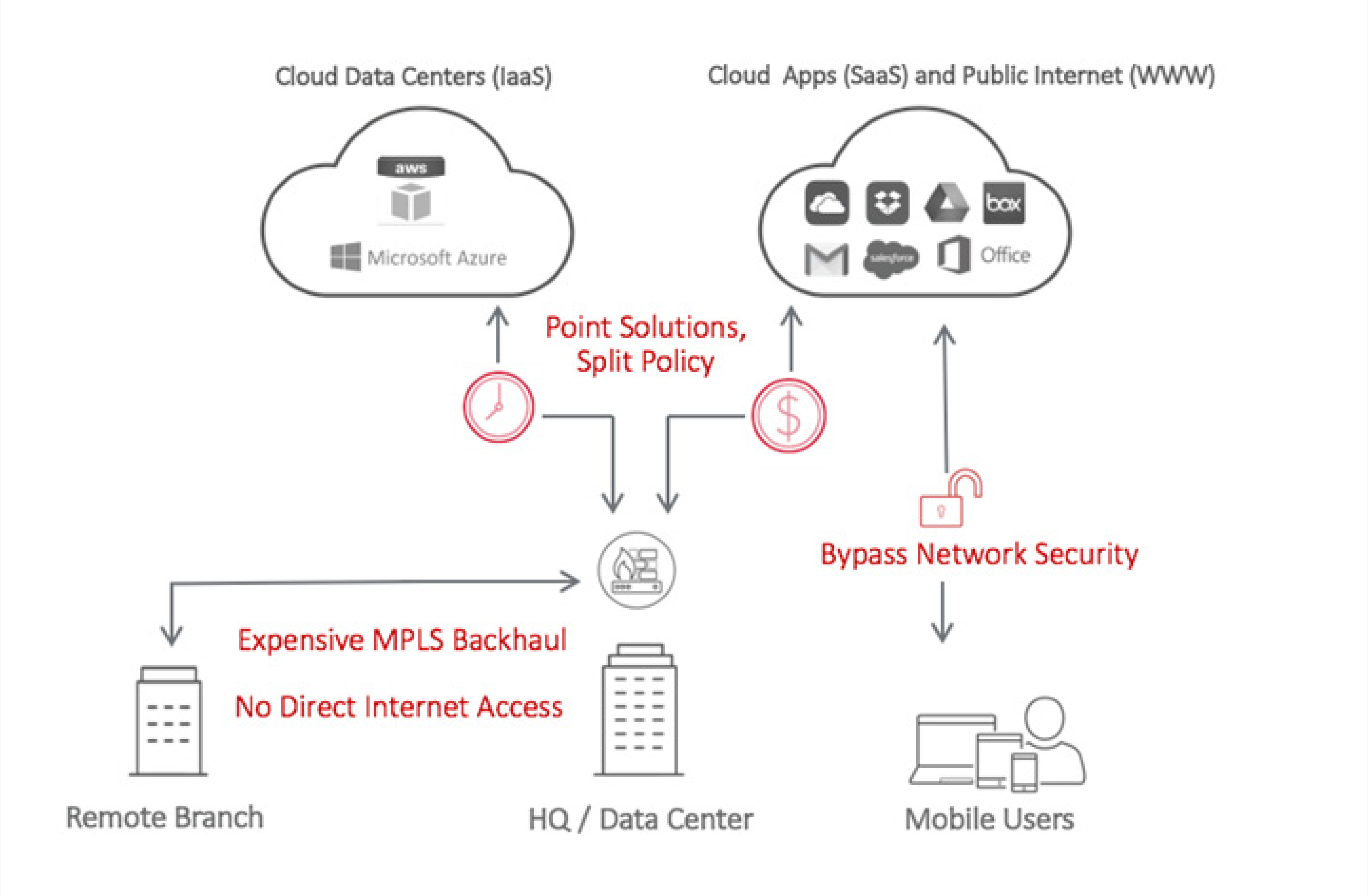
Automated policy-based networking significantly reduces the complexity of regulatory and industry compliance

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:

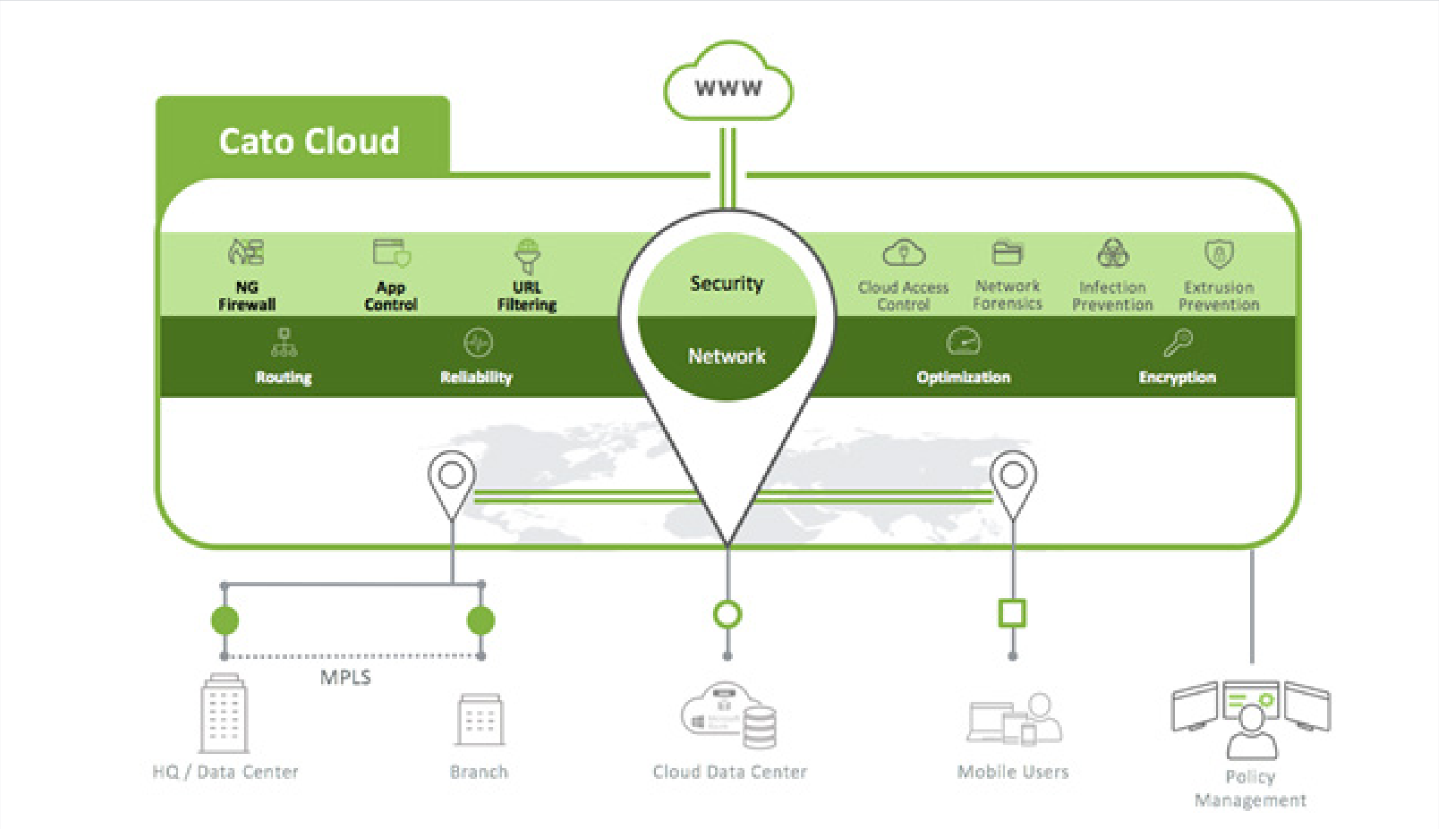
Cato Cloud Network

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.

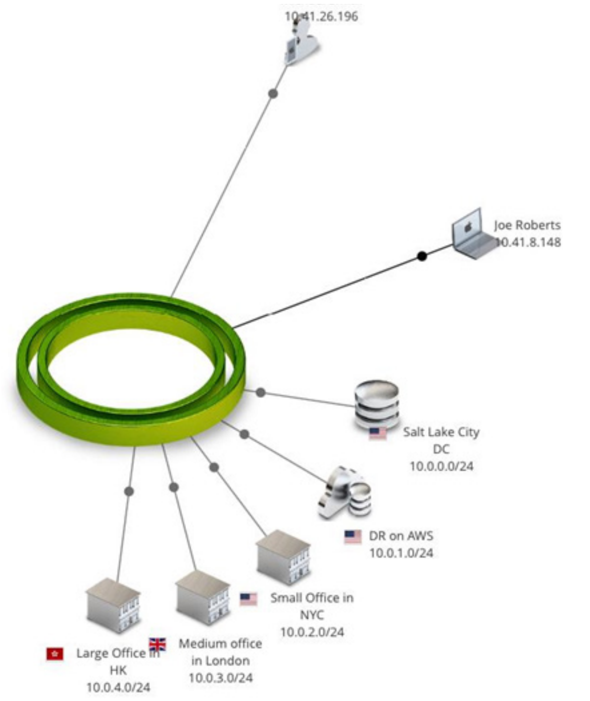
Step 3: Extend the WAN and Security to Cloud Data Centers and the Mobile Workforce

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.

TALARI Networks

NeedToChange WAN Refresh
Delivering a Failsafe Software Defined WAN

Overview

The NeedToChange WAN had served them well throughout the 2000s, but with company growth and the introduction of new services and applications, it was starting to show its age. Users were experiencing slowdowns while accessing critical applications such as SAP, PDM and Office 365, and complaints to the IT help desk were beginning to rise. Also, with the heavy use of VoIP and traditional applications as well as the increased use of cloud applications, complaints emerged that calls were not connecting and the voice quality was garbled while access to key applications was not meeting user expectations. Beyond application performance issues, some offices had experienced network outages that left them unable to function for periods of time.

The IT staff was starting to be stretched thin by the effort to maintain the existing network. Every time a new application was introduced, they were forced to manually update the existing infrastructure. The outages that occurred created an atmosphere of "manage by crisis." The IT staff was starting to reject or slow roll the introduction of new applications – harming the ability of NeedToChange to maintain its leadership position in the market.

NeedToChange decided to address these problems and update their WAN to support the company's future growth with Talari's Software Defined WAN solution which delivered a failsafe WAN that saved money, dramatically improved their users' experience, increased overall productivity, and best of all, stopped their IT team from lurching from one crisis to another.

Moving to a Network with Talari

As NeedToChange began the WAN research process, four requirements were clear going in:

- They would need more bandwidth at every branch office
- They couldn't expand their MPLS commitment due to cost constraints
- Direct access to cloud applications from the branch was required
- They needed to increase branch security to support access to external resources

This meant they had to use broadband Internet connections since they were the only option to cost-effectively increase available bandwidth. Also, the Internet connections served as the primary method to access cloud applications. The company quickly found a mixture of DSL and Cable providers and established an extra connection for the offices that didn't already have an Internet link. While the broadband connections were far less expensive than MPLS, they offered significantly more bandwidth.

They purchased Talari for each of their physical offices, selecting the Talari Virtual Appliance VT800 for the small offices, and the Talari Appliance E100 for the medium and large offices. In the Data Center, they installed a high-availability pair of Talari Appliance T3010s. Talari Aware, the centralized management system that gives IT staff the ability to configure, monitor, and analyze a Talari SD-WAN, was also deployed in the data center location.

They implemented in phases, starting with the Data Center and the offices that were reporting the most problems. The physical appliances leveraged Talari's Easy Install capability which allowed plug and play device deployment at the branch locations. This work was done by non-technical employees and eliminated the need for IT staff to travel to those offices during the SD-WAN rollout.

With the introduction of the Talari SD-WAN solution, the company decided to stop backhauling Internet traffic. Since each Talari appliance supported a stateful zone-based firewall and network address translation capabilities, the Talari solution delivered an easy and cost-effective method to deploy the incremental capabilities required for secure local Internet access.

The New Talari Software Defined WAN

The Talari SD-WAN built secure, full mesh, on-demand virtual connections between the offices, the data center, and the cloud. These encrypted connections are tunnels that are abstracted from the underlying network links. Each application uses a virtual connection, with the Talari network controller utilizing policy-driven decisions to ensure the highest possible performance for each specific application.

To make path decisions, the Talari solution collected data with every packet to determine the loss, latency, jitter and congestion of every possible path through the network in each direction. This collected information, based on real network traffic and not probe data or round trip pings, was combined with the centrally defined policies regarding prioritization, bandwidth share and security to make decisions about individual applications. Thus, the WAN became an intelligent network, able to accomplish the goals of the organization in the context of the actual real-time state of each WAN link.

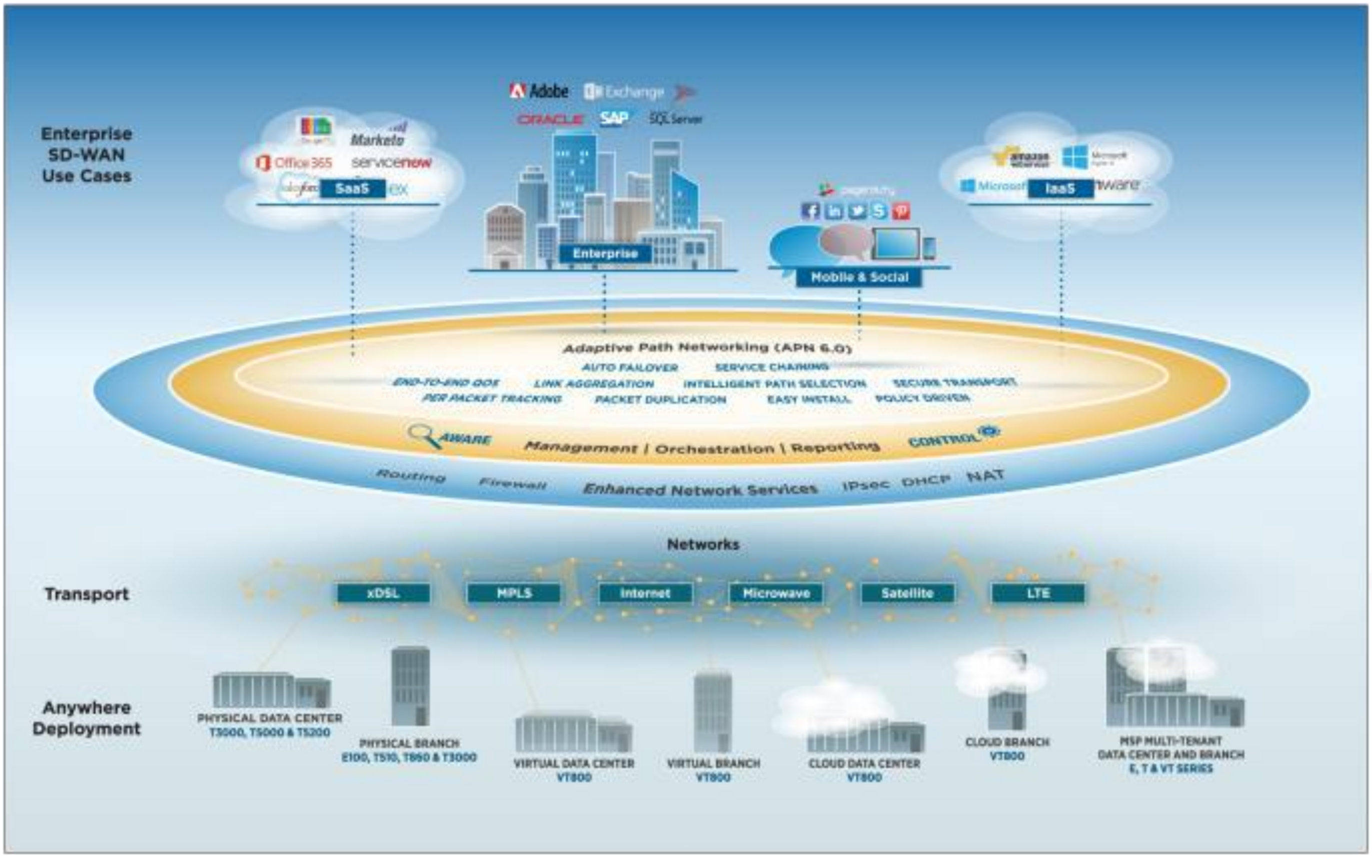


Figure #1, Talari Reference Architecture

Results for NeedToChange

The new WAN eliminated the problems that were plaguing the old network, improving the user experience while meeting the security goals of the organization and positioning them for the future. The key results realized with the new WAN included:

Cost Savings Coupled with Greater Capacity

Upon installation of the Talari SD-WAN solution, NeedToChange eliminated two large ongoing expenses. One was the maintenance on the firewalls in place at the large offices by replacing them with an integrated Talari Firewall. The second eliminated expense was due to the replacement of one of the MPLS circuits at the Data Center. While there had been much debate over whether they should scale back their MPLS commitment, the Talari solution proved it was more than able to convert broadband Internet links into a business class infrastructure.

Failsafe WAN Where Outages Go Unnoticed

By monitoring every path through the WAN, including to and from the cloud, the Talari solution detected link outages within a fraction of a second and automatically shift all WAN traffic to an alternate path. This prevented outages from disrupting offices; users now didn’t even notice when an outage occurred. Because error detection was so fast, even small spikes in latency or loss were detected and avoided, improving overall application performance. This approach allowed NeedToChange to deliver a business class WAN with better than 99.99% availability over a hybrid network comprised of commodity Internet and MPLS links.

Since VoIP was a key and growing application and voice traffic is latency and packet loss sensitive, voice packets were duplicated across two diverse WAN paths which ensured basically no loss for voice packets and the lowest possible latency. This resulted in an immediate improvement in voice quality and an elimination of dropped calls. And because of the broadband Internet links that had been added, there was an abundance of bandwidth available to support all applications.

Improved Application Performance

By forwarding direct traffic away from poor quality links and duplicating voice packets, the performance of business applications significantly improved. But more was needed, particularly during times of congestion when applications had to compete for available bandwidth. A combination of application prioritization and bandwidth reservation was used to ensure that critical applications such as SAP and PDM were given a share of network resources and were never choked out by lower priority applications.

While the default categorization could prioritize traffic, and assign the appropriate SD-WAN services to each type of application, specific rules were developed for some applications via the centralized configuration system. This allowed performance tuning on SAP and PDM traffic, decreased the share of bandwidth assigned to guest Wi-Fi access and public websites, and directed Internet traffic through the firewalls. This assured that during times of congestion, non-critical traffic would not choke out critical traffic. While the addition of the Internet links had reduced the likelihood of congestion, a link failure could quickly reduce the amount of bandwidth available to an office. The prioritization policies would immediately come into play if that occurred, preventing outages from impacting critical application availability and end user productivity.

Security Protocols - Uninterrupted and Reinforced

The new Talari SD-WAN conformed with NeedToChange's established stringent security policies. Since the Talari solution did not store any packets, worked with source encrypted packets, and did not provide external access to packets, the security protections that were already in place to achieve PCI compliance were left intact. All Talari destined WAN traffic was secured with the company choosing to use 256-bit encryption, header encryption, rotating encryption keys and trailing authentication checksums to ensure that data sent across Internet or MPLS links could not be read or spoofed. Also, the Talari stateful zone-based firewall delivered packet filtering and network address translation functions to further secure the branch sites.

Cloud Access When and Where Desired

NeedToChange was beginning to invest heavily in the cloud, including hosting their disaster recovery data center in AWS and mandating cloud options for new applications. Talari's SD-WAN solution allowed them to seamlessly incorporate the cloud into their WAN. Using the Talari Virtual Appliance VT800 as a Cloud Gateway, all traffic to and from the Internet used Talari's secure conduits. This created a secure and reliable connection to the cloud or co-location sites and eliminated any application performance problems caused by failed links or poor quality Internet connections.

By using the dynamic conduit feature of the Talari SD-WAN, the configuration of cloud and Internet access directly from each office was easy. With Talari's dynamic conduits feature, a secure tunnel is built to the cloud on demand when it is needed with no requirement to preconfigure anything. As additional offices were added, they automatically had a secure and reliable connection to the cloud with just the check of a box.

Performance and Cost-effective Scale to Deliver IoT

As NeedToChange proceeds with their IoT deployment, they will need a robust and secure infrastructure to link the sites that contain the thousands of IoT devices. This infrastructure will need to deliver the required bandwidth that will allow the IoT devices to effectively exchange information with the central control infrastructure which can be on-premises or in the cloud. The core capabilities that the Talari SD-WAN solution delivered to support the reliable, secure and performance requirements of user applications can easily be extended to support the IoT deployment in any location.

Segmentation to Support Guest Access

Talari comes with supports for VLANs, Virtual routing and forwarding (VRFs) and intelligent path selection which allowed for the secure handling of guest WiFi services within branch locations. These capabilities ensured that guest user traffic was isolated and restricted to accessing a limited set of public resources, such as the Internet.

Visibility and Actionable Analytics

While users didn't notice intermittent quality errors and link failures, the Talari management interface collected and displayed this information to the IT staff. They could see the performance of individual links and the aggregated performance of their telecom providers. This information was invaluable in helping them obtain support from the provider and to negotiate better rates. It also assisted with the troubleshooting of WAN and link issues. The benefit of a Talari SD-WAN was that it automatically and rapidly remediated the WAN when impediments were found, allowing IT staff to troubleshoot issues in a lower stress environment since they could address the network issues without having to deal with key applications being unavailable.

The correlated information on applications available from the management interface also helped the IT staff ensure they were meeting application SLAs and identify the root cause of WAN issues. By running reports on application performance across the WAN, they could show each business unit the quality score for their specific applications. This led to a more collaborative environment between IT and the other business groups, and helped IT tune the WAN to support the company's application mix and priorities.

Fast and Simple Implementation and Administration

One of the best results of the new Talari WAN was the ease of maintenance. Policies were centralized and changes were made in one location and easily pushed through the network, even outside of maintenance windows. By using Talari templates, IT staff reduced the time required to perform deployment changes while helping them maintain a consistent configuration. Also, new applications automatically used default behaviors and then were customized as needed. In addition, the increased visibility into network and application performance made it easy to identify areas for improvement. Beyond the central administration of the network, enabling a branch site was easy using Talari Easy Install. With this capability, appliances were staged by IT staff at the central controller and only required a non-technical person at the remote site to unbox and plug in the device to bring it online.

The End Result

With their new Talari-based failsafe WAN installed, the IT staff found themselves able to respond more quickly and positively to application requests from the business units. This gave them time to think proactively about new ideas that could help the company grow. Confident that their WAN was up to the challenge, they could add more video communications options, expand their use of SaaS applications, and push much of the needed infrastructure growth to the cloud. Also, they had budget to invest in these ideas with the decrease in telecom costs.

Best of all, the company and its employees noticed the difference. Productivity was up at offices as outages stopped interrupting work and access to important applications was always available and high quality. Finally, the Talari SD-WAN solution allowed the business to move quickly when opening new offices or acquiring new businesses.

Talari Networks, Inc.,
1 Almaden Blvd, Suite 200
San Jose Ca, 95113

Phone: +1 408.689.0400

info@talari.com | www.talari.com

About Talari Networks

Talari Networks, the trusted SD-WAN technology and market leader, engineers the internet and branch for maximum business impact by designing failsafe WANs that deliver superior business-critical application reliability and resiliency, while unlocking the simplification and cost reduction benefits of branch consolidation.

Talari delivers a comprehensive solution, supporting a variety of network services in physical, virtual and cloud locations, which can be acquired through perpetual licensing, monthly subscription rates or as-a-service. Passionate and committed to their customers, Talari has incorporated eight years of innovation into five generations of product and is successfully deployed across thousands of sites in over 40 countries.

cradlepoint

SD-WAN for People, Places and Things at NeedsToChange Corp.

Introduction

This document outlines Cradlepoint's approach to a new SD-WAN for NeedsToChange Corporation (referred to as NTC). The guiding principle was to meet the NTC's operational, performance, and security requirements while significantly reducing one-time capital costs and recurring operational expense.

Cradlepoint Overview

Cradlepoint is the global leader in software-defined and cloud-delivered network solutions for connecting people, places, and things over wired and wireless broadband. More than 15,000 enterprise and government organizations around the world—including 75 percent of the world's top retailers and 50 percent of the Fortune 100—rely on Cradlepoint to keep critical sites, workforces, vehicles, and devices always connected and protected.

Cradlepoint NetCloud™

Cradlepoint NetCloud™ is a software-defined and cloud-delivered platform that powers and extends a portfolio of LTE-enabled routers with unified management, overlay networking, and virtualized network services. The NetCloud platform consists of the following elements:

NetCloud Manager (formerly Enterprise Cloud Manager) is a single-pane-of-glass cloud management platform that goes beyond ease-of-use to provide the "ease-of-scale" needed to connect hundreds of thousands of people, places, and things distributed around the globe. NetCloud Manager capabilities include:

- Simplified configuration with mass templating
- Zero-touch deployment capability
- Schedulable software and configuration updates
- LTE SIM and carrier management
- End-to-end policy management
- Orchestration and automation
- WAN analytics and health monitoring

NetCloud Engine is a cloud-based Network-as-a-Service that provides a private virtual overlay fabric across the public Internet. Its SDN architecture consists of a distributed data plane that runs on standard virtual machines within public cloud datacenters throughout the world. Each of these data plane entities, called ServicePoints, can host one or more virtual overlay networks, which are called Virtual Cloud Networks (VCNs). The ControlPoint is a collection of micro-services that together comprise the SDN control plane and provide orchestration, oversight, and management of the service. The ControlPoint also gives a VCN its self-organizing, self-optimizing, and self-healing properties.

ServicePoints also enable the integration of virtual network services utilizing Cradlepoint's Network Service Virtualization (NSV) technology. NSV is a distributed, micro-services form of NFV that runs each service function as a discreet process within a VCN's packet path. NSV can also provide a "last-in-chain" egress to external VNFs or cloud services, like firewalls or secure web gateways. A ServicePoint also can act as a Secure Cloud Gateway (SCG) to provide a secure egress point from a VCN to the Internet for connecting to public cloud, SaaS, and the web.

NetCloud Services provides a library of virtual network services based on Cradlepoint and third-party technologies. These services run within the VCN overlay—using NSV—or at the Edge on **NetCloud OS**, the Linux-based open network operating system that powers Cradlepoint routers. The following is a summary of available NetCloud Services:

- Carrier-grade NAT
- PKI-as-a-Service
- Overlay DNS with Active Directory integration
- Distributed next-gen firewall
- Micro-segmentation at the user, app, or device level
- Threat management with IPS/IDS
- App control—1,500+ business and SaaS apps
- URL/content filtering
- Network Access Control (NAC)

NetCloud Client and **NetCloud Gateway** provide an on-ramp to VCN overlays for standalone and router-attached resources, including PC, mobile, and IoT devices. NetCloud Client provides LAN over WAN services for seamlessly connecting mobile users and devices anywhere to private and public cloud applications and resources. It supports Windows, Mac, Linux, Android, and iOS operating systems. NetCloud Gateway provides the same functionality within Cradlepoint routers for IP-attached users and devices.

Cradlepoint Routers

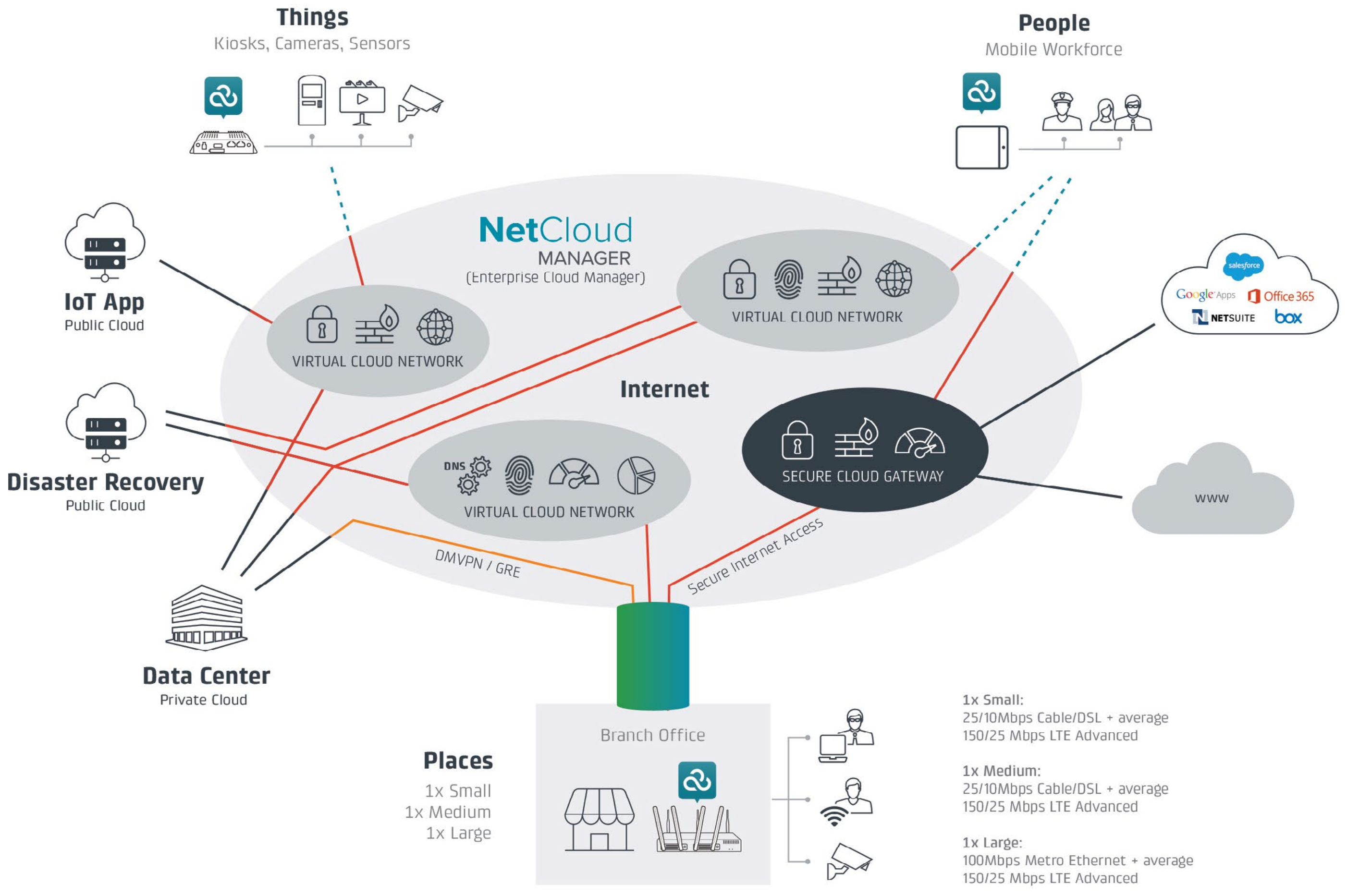
Cradlepoint offers an extensive portfolio of purpose-built, LTE-enabled routers for branch, in-vehicle, and IoT applications. For the NTC network, Cradlepoint has deployed the AER Series of converged, multi-WAN Edge routers and COR Series of IoT routers.

Cradlepoint SD-WAN Solution

BRANCH OFFICE WAN

For NTC's three branch offices, the Cradlepoint AER Series Advanced Edge Routers provide an "all-in-one" solution for WAN, LAN, guest WiFi, and IoT connectivity. The high-end AER3100 routers used in the NTC network cost less than $2,000 each and includes:

- Multi-WAN – MPLS, MetroE, Cable/DSL, WiFi, and LTE
- 12 Ethernet ports including four ports with PoE support
- 802.11ac WiFi – 3x3 MIMO, dual-band concurrent
- Up to two integrated 4G LTE modems, each with dual SIMs



🟦 4G LTE
🟩 Broadband
🟥 VCN Overlay
🟧 DMVPN Overlay
▨ Hybrid WAN (LTE + Cable / DLS)

● **Virtual Cloud Network (VCN):** Virtual overlay network with LAN emulation & policy-based network services.

● **Secure Cloud Gateway (SCG):** Virtual gateway to Internet with policy-based security services.

Replace MPLS with Broadband: Cradlepoint has replaced NTC's MPLS network with a hybrid WAN consisting of pooled wired and wireless broadband connections supporting both primary and failover requirements. The price for MPLS copper connections can range from $300 to $600 per Mbps/month, while business-class wired broadband access (cable or DSL) is typically less than $5 per Mbps/month — a savings of more than 90 percent. Given the price/performance advantage, a 25Mbps downstream and 10Mbps upstream wired broadband link is used for the small and medium NTC branches at $99/month a site. For the Large NTC branch, which has more than 100 users, a 100Mbps Metro Ethernet connection is used at a cost of $10 per Mbps/month.

LTE for Primary and Failover WAN: In addition to wired broadband, Cradlepoint has deployed Advanced 4G LTE as part of the hybrid WAN connection pool for both primary and failover uses. Cradlepoint's support of LTE Category 6 enables up to 300Mbps download and 50Mbps upload throughput speeds on networks such as Verizon's Advanced LTE. However, real-word speeds likely average 150/25Mbps.

Virtual Overlay Networks: Cradlepoint's SD-WAN capabilities include several forms of virtual overlay networks. For NTC's network, corporate intranet traffic flowing from the branch to the private cloud datacenter uses a DMVPN/GRE overlay. Internet-bound traffic headed to public cloud, SaaS applications, and the web utilizes a VCN overlay. While both overlay methods support point-to-point and meshed topologies, VCN has the added value of integrated DNS, LAN emulation, and AD integration.

Intelligent WAN Selection and Steering: Cradlepoint routers provide several policy-based traffic management and steering mechanisms that enable Quality of Service (QoS) and intelligent selection across both the wired and wireless broadband links that comprise the branch hybrid WAN connection pool. Using the mechanisms summarized below, specific QoS and traffic steering polices have been set to ensure the performance of NTC's business-critical SAP and PDM applications, control VoIP latency, and shape video traffic to avoid saturating links or over-consuming LTE data plans.

Intelligent WAN Selection & Steering: Cradlepoint provides several policy-based traffic management and steering mechanisms that enable quality of service (QoS) and intelligent selection across both the wired and wireless broadband links that compose a hybrid WAN connection pool.

- Policy-based QoS: App-enabled prioritization, bandwidth allocation, and traffic shaping for traffic traversing the router in each direction.
- WAN Diversity™: Ability to combine multiple wired and wireless WAN links into a hybrid WAN connection pool in primary and failover roles.
- WAN Affinity™: Traffic steering policies that control WAN link selection based on specific algorithms, including round-robin, load balancing, most available bandwidth, and LTE data usage.
- Intelligent LTE Failover: Complete policy control over the apps and traffic allowed to utilize the LTE link if one or more primary links fail.
- Data Plan Protection: Analytics-driven policies that automatically suspend or reduce LTE usage within the hybrid WAN connection pool as monthly data plan consumption reaches a set threshold.

High Availability: AER Series routers are configured with two LTE modems, each with dual SIM cards. This allows each router to be "dual-homed" on multiple LTE carriers in either redundant carrier (dual SIM) or concurrent carrier (dual modem) mode. With this approach, NTC can achieve 99.99% availability of its branch WAN. For the utmost in high availability and fault tolerance, NTC can deploy routers in tandem using VRRP to enable full hardware, WAN, and LTE carrier redundancy.

Guest WiFi: AER Series routers support advanced WiFi capabilities to enable secure guest access at each branch location. Guest network users can be micro-segmented from WiFi-to-WAN to isolate them from trusted branch networks. Moreover, the intelligent WAN selection and steering polices have been configured to ensure guest traffic does not interfere with business users and applications and does not utilize the LTE links. For added security and compliance, guest traffic also uses Secure Internet Access as described below.

Secure Internet Access: The new Cradlepoint SD-WAN achieves significant bandwidth savings for NTC by implementing Secure Internet Access (SIA) for branch employees and guest WiFi users. This direct access approach eliminates the backhauling of Internet traffic and avoids the cost and complexity of installing branch-based security appliances. Within each Edge router, the NetCloud Gateway provides an encrypted overlay to the nearest ServicePoint where traffic is securely routed through the NetCloud Engine SCG service to the Internet. NTC network admins can use NetCloud Manager to set the desired app, users, and device security policies, which in turn will automatically provision the appropriate virtual network services to be used for SIA traffic such as next-gen firewall (refer to NetCloud Services above for a listing of other available security functions).

Secure SaaS Access: SIA also provides branch employees with secure SaaS access from any device, including tablets and phones. NTC network admins can set user and device policies to allow or block the use of specific SaaS and web applications, such as Salesforce.com, Microsoft Office 365, or DropBox. For example, NTC may choose to allow access to all SaaS apps from any corporate-owned device but restrict access to only Salesforce.com for users of BYOD devices, like an Android tablet.

Public Cloud DR: The enclosed diagram illustrates how branch-level disaster recovery (DR) is provided using the NetCloud Engine service. At each branch, a separate disaster recovery VCN provides always-on connectivity to the public cloud DR site. In the event of a primary datacenter outage, or even loss of a single application or data store, the AER router can steer affected traffic over the DR-designated VCN.

MOBILE WORKFORCE WAN

Cradlepoint NetCloud extends the SD-WAN value proposition to NTC's mobile workforce, giving employees a secure, LAN-like connection to private and public cloud apps and files from anywhere and any device. As shown in the enclosed diagram, the NetCloud Client runs on each device and provides a persistent encrypted connection to a VCN overlay set up specifically for mobile access.

To address the security concerns around BYOD and public WiFi access, the mobile access VCN has been configured with NetCloud Services that provide NAC, micro-segmentation, next-gen firewall, and app control so that devices are isolated from one another and access is only granted to specific servers and applications at the datacenter and public cloud DR site. Mobile employees also are configured for SIA to provide secure and compliant access to SaaS applications and the web.

IoT WAN

Cradlepoint NetCloud and routers are optimized for IoT deployments in the field or within a branch. The ruggedized COR Series IoT router can support NTC's future field IoT deployments, such as kiosks, vehicles, digital signage, and surveillance cameras. It supports WiFi (for LAN or WAN), Ethernet and 4G LTE interfaces, DMVPN/GRE and VCN overlays, and the full suite of NetCloud Services. Within the branch, the AER3100 router with integral PoE can connect, protect, and power IoT devices such as cameras and sensors.

SINGLE-PANE-OF-GLASS MANAGEMENT

NetCloud Manager enables zero-touch branch and field deployments of AER Series and COR Series routers and utilizes a proprietary Stream management protocol that's 700 times more WAN-efficient than SNMP. Stream allows fine-grain management and control of routers, WAN interfaces, LTE carriers, and policies without the overhead of traditional management approaches, which can consume up to 30 percent of bandwidth.

Summary

With more than 15,000 customer deployments in some of the world's most demanding enterprise and IoT networks, and recognized leadership in 4G LTE solutions, Cradlepoint brings a unique pedigree to the SD-WAN market.

Cradlepoint NetCloud and router platforms provide a versatile SD-WAN solution that utilizes a single virtual overlay fabric to connect people, places and things, with advanced security and single-pane-of-glass management. For NTC, this all translates to a new software-defined and cloud-delivered WAN that makes its network more agile, secure, efficient, and extensible than ever before.

TO LEARN MORE, VISIT **CRADLEPOINT.COM**.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim's current interests include cloud networking and application delivery.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.