Evolution of Wide Area Networking

The use of Software Defined Networking (SDN) in the datacenter has resolved the issues with application and workload placement but this hasn't reduced the complexity of delivering the application to users across the wide area.

To extend the dynamism of the cloud to remote employees, enterprises across the globe are looking at Software Defined Wide Area Networking (SDWAN) as the foundation for the future evolution of wide area networking.

This case study focuses on a typical nationwide enterprise we'll call Kromacom told from the perspective of their new CIO Alex Warner. Alex has joined Kromacom with the mandate from the CEO to change the IT environment.

Introduction

I'm Alex Warner and I joined Kromacom when they acquired the startup company I worked for. I was CIO at the startup and managed the IT environment as we grew from an idea to public listing and then through the growth period that led to the purchase by Kromacom. As a smaller company we used a lot of cloud-based IT and applications to ensure that our people had the right business information to do their jobs.

I was elated to be given the CIO role at Kromacom as the IT environment is more complex — and I love a challenge. The CEO was very clear though throughout the interview process: with the move to cloud IT Kromacom had outgrown its internal IT processes and systems. More of the same was not going to cut it. The IT department needed a fresh set of eyes and a change in approach to remove the constraints that were hindering business growth.

Kromacom IT Environment

Kromacom is based in Texas. It has a centralized datacenter and a mix of small, medium and large offices throughout the nation connected via a private IP-VPN service. Some cloud-based compute is used, primarily for IT dev-ops and for disaster recovery to the main datacenter.

The application mix is mainly in-house with an existing customer relationship manager (CRM) and finance systems both locally developed and hosted in the Texas datacenter. Recently, Kromacom rolled out salesforce.com as their first Software as a Service application.

Desktop applications are mainly client (branch) to server (datacenter). However Kromacom is in the middle of a rollout of advanced IP communication and collaboration tools that will add desktop instant messaging, IP voice and desk-to-desk video conferencing.

The constructs for wide area networking at Kromacom have remained the same for over 20 years. Network connectivity (such as the managed MPLS-based IP-VPN service) has been purchased from a service provider via multi-year contracts. Then, the networking team rolls out routers to the branches and via a site visit applies a location-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 as WAN managers, our challenge is to squeeze the last drops of performance out of a finite resource. To date, Kromacom achieved this with advanced configurations within the branch routers or the addition of network appliances — both approaches that increase network complexity, CAPEX and OPEX.

How Cloud-Based IT Consumption is Affecting the Branch

I found that Kromacom's IT environment was 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 Kromacom's needs well. Remote branches were clients to the Texas datacenter servers.

With Cloud IT, traffic patterns have changed. Kromacom has virtualized its Texas datacenter and the critical CRM and finance applications reside on virtualized compute systems.

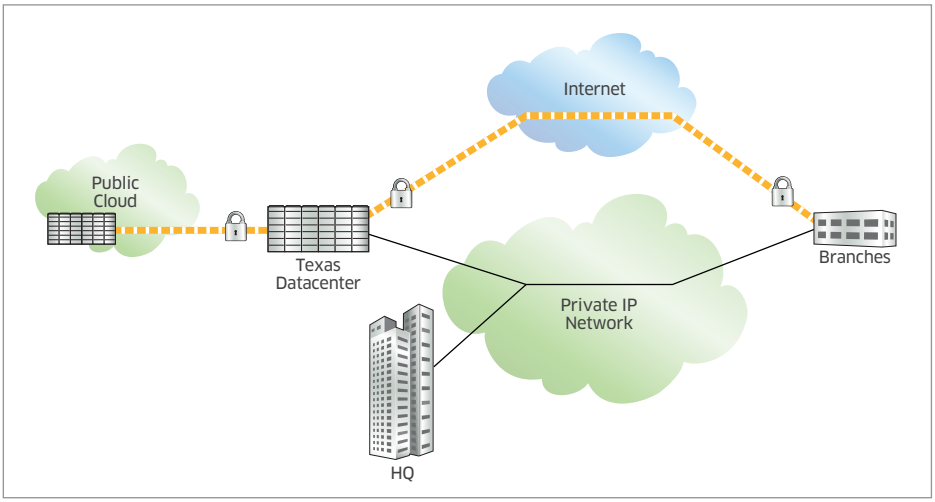
As the demand for these applications increases, the virtual compute environment flexes to accommodate the workload. This means that the application does not always reside in the same rack or row of the datacenter. In disaster recovery situations, for example, it would be relocated to a completely different datacenter in the cloud.

Unfortunately, outside the datacenter, Kromacom's network architecture is static and cannot easily adapt to dynamic demand. To resolve this inflexibility with the current architecture Kromacom 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 employee connecting to the CRM is the client, but only for that application session. Kromacom recently launched 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 by our HQ-to-branch (or hub-and-spoke) network architecture.

FIGURE 1. Kromacom proposed SDWAN architecture



Unconstrained Networking, Datacenter to Branch

To address new business communication standards and Cloud-based IT, I needed to re-examine what we need from the WAN. Some key areas of change that I identified 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
- Control the premium bandwidth costs with an augmented secure Internet offload at the branch for selected applications
- 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 as a single entity with common management, monitoring and reporting tools

To give Kromacom access to these benefits, I recommended that we deploy an SDWAN. Figure 1 shows the basic network topology with connections from the branch to the datacenters utilizing both private IP and Internet services.

The technologies around SDWANs significantly change the management and operation of the WAN environment. They use the key principles of SDN:

- **ABSTRACTION** of the business needs from the underlying network capabilities
- **AUTOMATION** of the deployment of network functionality via a centralized policy push model
- Increased **CONTROL** of the network environment and the ability to adapt to dynamic business requirements
- Enhanced **VISIBILITY** into the operation of the network and the performance of the business applications and network locations

There are a number of SDWAN solutions in the market so I approached a few vendors with my requirements. I liked the comprehensive solution from Nuage Networks called Virtualized Network Services (VNS).

Nuage Networks VNS covered my key requirements and provided a seamless solution that incorporated my datacenter, wide area and branch environments into a single operational domain.

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

Below is how Nuage Networks said they could deliver wide area networking that matches the flexibility of Cloud IT — just what we need.

Evolving the Wide Area Network with Nuage Networks

With the Nuage Networks VNS solution there are three key domains (or layers of network functionality) that will help me deliver a new SDWAN for Kromacom:

- **Service Management Plane:** A policy system that centrally administers the network templates and policies. Nuage Networks calls this the Virtualized Services Directory or VSD. This layer provides the visibility and control of the 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 WAN are managed via this WAN service management layer.
- **WAN Control Plane:** This layer contains the SDN-based controllers that manage the control plane of the WAN. Nuage Networks calls these the Virtualized Service Controllers or VSCs. Deployed in pairs, these controllers manage the network connections between the endpoints (branches, Texas datacenter and public cloud) of the Kromacom network.
- **WAN Data Plane:** Open compute (x86-based) Network Service Gateways or NSGs deployed at the remote branches and datacenter connection point, and at the public cloud interconnect to provide enterprise-wide control of the network. These branch devices support both a virtual deployment option (in a public cloud or on an existing branch server) and a dedicated hardware form factor (Nuage Networks 7850 NSG). In either case (virtual or physical) management is provided by the service management layer with data forwarding control provided by the WAN control plane (the VSCs).

Any-to-Any Network Connections

With this software defined wide area network in place Kromacom can implement either partial or full mesh network architectures to facilitate branch-to-datacenter and branch-to-branch communications. This provides us with the flexibility to transport inter-site traffic across the most efficient path. The rich IT communication tools we are deploying to enhance the collaboration between branch staff can be implemented without the constraints of the rigid hub-and-spoke architectures of the previous network architecture.

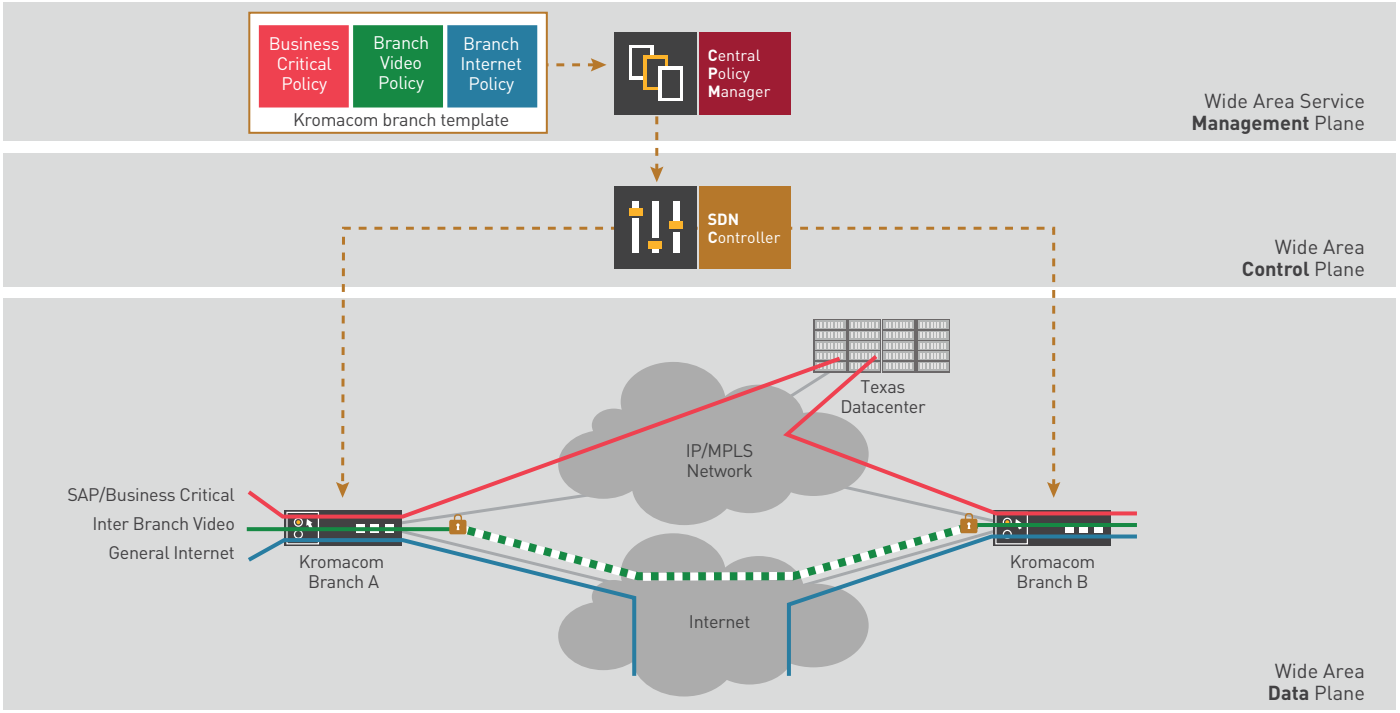
Intelligent Traffic Offload

Via the Virtualized Service Directory (VSD) and its central policy system, my IT team can implement a network policy to securely offload any Internet traffic at the branch.

This approach is going to be a big help to us in three ways. First, our 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 intelligently offloading traffic is that we can use the Internet connection as a backup link in case the primary (IP-VPN) circuit fails.

Using the same template-based policy push from the VSD, all branch traffic can be encrypted and sent over the Internet to the Texas datacenter. This provides additional resiliency and enables Kromacom to improve network availability at the branch. At the same time, we benefit from a per-bit cost advantage by using the Internet rather than adding additional premium VPN bandwidth to our primary connection.

FIGURE 2. Using policies to intelligently offload traffic



Policy-Based Network Management

With the Nuage Networks VNS solution and its VSD policy-based manager, management and monitoring of the Kromacom wide area environment can be simplified. The VSD can create policies for application traffic at multiple levels and these policies can be grouped together into templates. The templates can be deployed automatically when an application changes (for example, if CRM is relocated to the disaster recovery datacenter location) or a new branch is added. Policies can be split into four key types:

- **Application policies:** These are the conditions each application requires to function across the network and can include specific security, quality of service (QoS) and resiliency requirements for the application. For instance, a policy for the finance 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 finance print traffic at the branch can be lowered in priority to ensure that it doesn't affect the performance of the critical interactive traffic.
- **Branch policies:** These include the network configurations and features for specific or types of branches in the network. A branch may be a physical or virtual location, for instance a public cloud interconnect where a new application resides. My 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. This security team can set the security policies at 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 operations team and automatically pushed to the applications or branches. The user privilege functions of the VSD ensure that the policies are used/not changed so that compliance to Kromacom's security policies is enforced with a centrally managed audit path.
- **Network policies:** These are the network-wide policies that control the flow of traffic across the network. Examples include the overall QoS policy that prioritizes CRM, finance and voice traffic over general inter-office and Internet traffic.

Using these policies, templates for deployments can be created, such as the Intelligent 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 are then called on whenever a new site is added to the network.

Relying on templates reduces the need for my specialized personnel to visit branch locations. The branch equipment can be couriered to the branch manager with

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

simple instructions on how to connect to the WAN links. Once connected the device will "call home" to the VSD, authenticate and the template configuration will be sent over the wide area to the device.

Network Functions Virtualization

Nuage Networks VNS also provides us with an opportunity to reduce our reliance on external network devices at the branch. Historically the only option we've had 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 drive up network complexity, which in turn raises OPEX for maintaining the wide area environment.

With Nuage Networks VNS solution a number of network functions can be virtualized either at the branch or in the network path between the branch and datacenter. These network functions can be "chained" into the traffic flows to and from the branches. With this approach, a more robust and dynamic end-to-end policy that inserts the right network functions into the right locations will ensure data integrity at the branch, without the large CAPEX drain of physical devices.

Service Provider Independence

Nuage Networks VNS also makes it possible to separate Kromacom's wide area service from the underlying IP connectivity. With traditional WANs these are tightly integrated; with the Nuage Networks solution they can be completely separated.

This separation delivers a new set of options for getting bandwidth across the wide area and into the branch. It means that we can procure the required IP connectivity services on a per-branch or per-region basis and use these connections as an underlay network for the wide area. For instance, this gives my team 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 branch connection.

Kromacom's New Era in Branch Networking Freedom

The Nuage Networks VNS solution provides Kromacom with the wide area network this company needs and hits all the key functions I was looking for in an SDWAN solution. It opens up a world of possibilities that were unattainable with the existing WAN.

This isn't an exhaustive list, but here are some examples of new branch networking scenarios that my team can roll out.

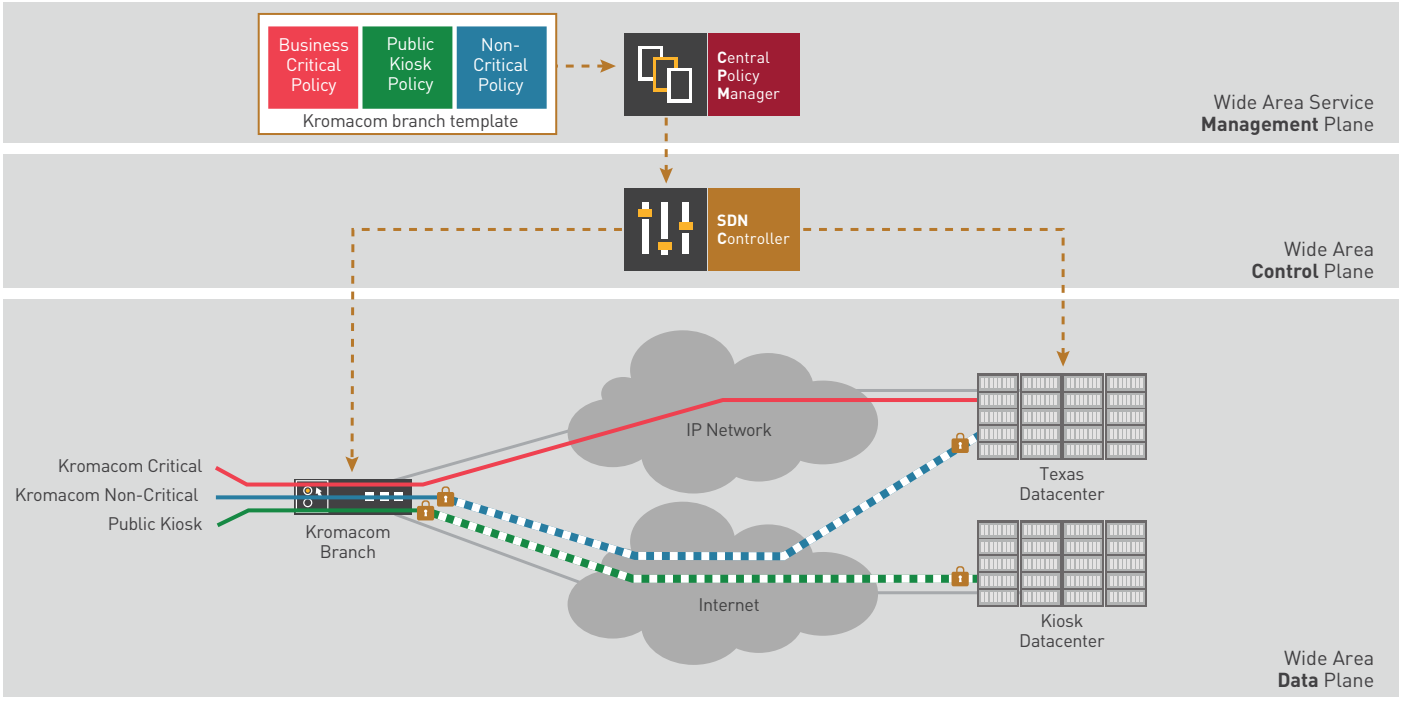
Intelligently offloading traffic at the branch

The intelligent traffic offload policies of Nuage Networks VNS provide Kromacom with the opportunity to centrally manage and deploy specific policies to route non-business-critical traffic away from the primary (constricted) premium IP circuit on to a secured Internet tunnel.

Other examples of how this functionality can be implemented include:

- **Guest Wi-Fi® Services:** Staff and guests can connect to the branch network and via policy be immediately directed to the local Internet connection (enabling a Bring Your Own Device (BYOD) capability). This provides a couple of benefits. First, office users are provided with Wi-Fi network connectivity so their traffic does not incur any mobile broadband changes. Second, the traffic is immediately routed to the local low-cost Internet connection and does not consume any premium branch office bandwidth. I also found this a quick and easy way to improve the relationship between branch staff and central IT.
- **Direct-to-Cloud Applications:** We can use this capability with the new salesforce.com application mentioned earlier. Network policies can direct the application traffic to the nearest Internet offload point, which removes it from the primary branch uplinks. It's great

FIGURE 3. Isolated local area networking in the branch



to know that we can implement similar over-the-top applications without impacting the premium bandwidth required to the branch.

- **Site-to-Site Bulk Traffic:** This is valuable for large file transfers such as branch server backups. The traffic can be directed via policy to use an encrypted Internet path. As this bandwidth will average a higher throughput rate than the premium branch connection the backup will conclude quicker or can even be scheduled during office hours without impacting network performance.

Branch network segmentation

The ability to segment and isolate portions of the branch network has traditionally been challenging with classic IP-VPN services. With Nuage Networks VNS this is deployable via the VSD's central policy functions. A business example of this could be the use of public kiosks for customers to come into the branch and conduct business.

With the Nuage Networks VNS network policies deployed, the kiosks (IP hosts on the network) could be isolated away from the physical (and logical) local area network used by branch staff. With no connection between these networks there is no possibility of customers accessing anything but the contained kiosk network.

This functionality can be used by public kiosk, or even as a way to securely share branch connectivity without compromising security. Another example could be co-location within the Kromacom branch with another company. The two organizations could share office location with completely isolated local area connections and centrally managed network policies to direct traffic to their respective central sites.

Summary

To gain maximum benefit from the move to SDN, the operation and purpose of the network(s) at Kromacom need to be rethought. The network needs to connect the new cloud IT environment to the business users regardless of their location.

Implementing SDN in the datacenter and across the wide area is a great start. However, to drive a change across the whole business these two critical network islands must operate in concert and that means removing any network 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. SDN provides the opportunity to achieve this.

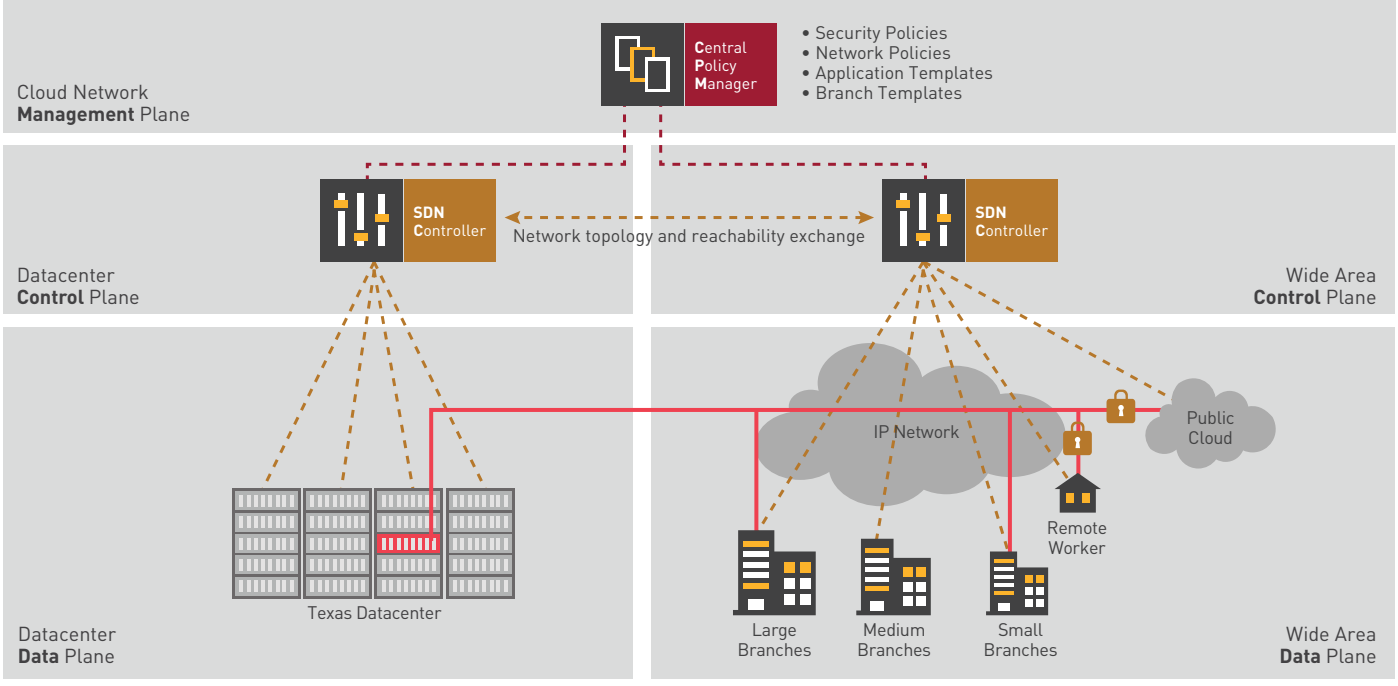
If SDN is controlling the network that underpins cloud applications in the datacenter and is managing the connectivity across the wide area towards the applications' end users (employees and/or customers) then centralizing this intelligence onto an overarching policy and control framework makes sense.

With Nuage Networks I can achieve exactly this: unconstrained networking for the datacenter and beyond.

We can maximize the benefits of moving to Cloud IT. My team can centrally manage the datacenter and wide area networks with a single policy framework, which simplifies the overall network configuration. We can change a security policy once and have the network automatically roll that change out. We can add a new application in the Texas datacenter and deploy the updated network, branch and security policies so it's instantly available to all users.

No more waiting for project rollouts, and no more specialist personnel needed at the branch. With this new network environment in place, I get to deliver the end-to-end network Kromacom needs — on my terms.

FIGURE 4. Seamless interworking with Nuage Networks SDN solution



nuagenetworks
From Nokia