TICVIC NETWORKS

Connect Secure Redundant Besilient

A Step to SD-WAN

Benefits of SD-WAN Briefed

<u>SDWAN</u>

- The primary advantage of SD-WAN is security. Provides an End-to-End Data protection.
- Key benefits such as visibility, scalability, performance, and control are enhanced.
- Enables central network control and traffic management as well as network automation. Single point of Control/Mgmt.
- Today's companies prefer network architectures that integrate security, policy, and orchestration, and SD-WAN covers those bases by unifying secure connectivity.
- SD-WAN comes with no bandwidth penalties. Customers can upgrade easily by adding new links, with no changes necessary to the infrastructure or network.
- Enables the ability to cost-effectively mix and match network links according to content type or priority.
- SD-WAN can benefit businesses by removing expensive routing hardware and instead provisioning connectivity using a bare metal device/x86 hardware/VM.
- When deploying SD-WAN through an NFV-based model, capacity can dynamically scale up or down without having to replace or add additional proprietary hardware.

Benefits of SD-WAN Briefed

SDWAN

- Application Intelligence -- SD-WAN has the ability to identify over 2800 specific applications and use that knowledge to apply a range of network and security policies to the traffic carrying them

- Multiple deployment options -- The SD-WAN can be deployed directly on bare metal x86 servers, white-box appliances, virtual machines (VMware ESXi, KVM) and containers.

Things to remember when selecting the Transport Layer for the SD-WAN Setup

- Expecting 1:1 (upload and download) bandwidth through Internet Broadband connection is not a good idea. This impacts the VoIP quality if the SD-WAN is built using only Internet Broadband Connections only.

- The End-to-End Bandwidth guarantee over Internet Broadband connection is not possible at least for now. We've to keep this in mind while designing the Transport layer for the SD-WAN.

- The MPLS provides 1:1 (upload and download) and End-to-End bandwidth guarantee with its cost in OPEX.

WAN And Evolving Application Requirements

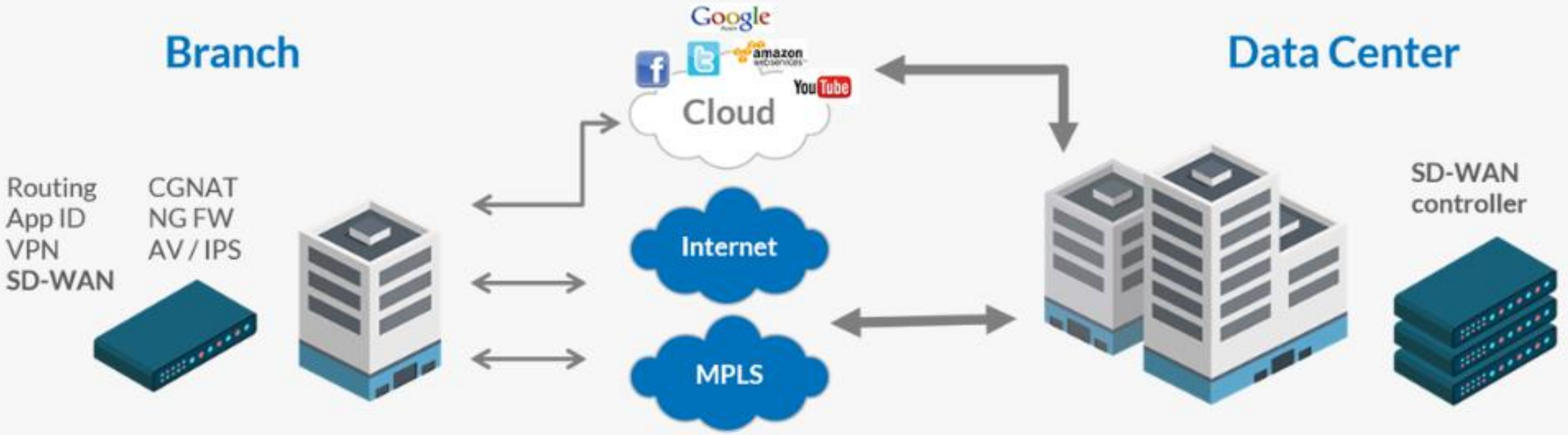
Day to day Usage of Cloud for Compute and storage, as well as core applications like CRM, HR and Microsoft Office are increasing rapidly. Yet Corporate WAN connectivity continue to use 20-year-old private line technology (MPLS) and expensive, proprietary networking hardware.

- This results in slow provisioning times for new offices or even basic changes to configurations and functions.
- High costs for network equipment and WAN services.
- Complex branch architectures and high administrative overhead.

SD-WAN: Bringing Wan Flexibility, Control And Security

- Software based and multi-service approach to SD-WAN.
- Low cost WAN appliances vs proprietary network hardware.
- Provides full set of Integrated SD-WAN services (with the help of NFV).

- All the above allows enterprises to reduce the Capex and Opex of their WAN and branch networks, while increasing IT responsiveness to business needs.
- The time required to manage the network is minimized, and branch security is strengthened.



Branch

Routing
App ID
VPN
SD-WAN

CGNAT
NG FW
AV / IPS

Cloud

Internet

MPLS

Data Center

SD-WAN
controller

Low-cost appliance with **SD-WAN + Internet security**

Application-aware routing across MPLS and Internet

Centralized policy and control; other security functions

The Benefits of SD-WAN with Integrated Branch Security

Branch Networking Today – More Bandwidth, More Complexity

As traffic volumes have increased significantly due to video, cloud storage/collaboration and other high bandwidth applications, WAN bandwidth requirements have also increased.

Options include adding more capacity to the existing WAN circuit or introducing an Internet connection to the branch WAN architecture.

The Internet approach can help mitigate the overall congestion of the WAN, but also increases the complexity, security requirements and cost of designing and managing the branch network, requiring additional infrastructure, policies and management/oversight.

From a bandwidth management and allocation basis, traffic engineering to ensure available bandwidth for given applications requires time consuming manual mapping of specific traffic to specific circuits.

From a security perspective, adding Internet connectivity requires additional security infrastructure, policy creation and management.

Finally, when Internet connectivity is added, the ability to effectively monitor and obtain an overall view of the branch WAN becomes increasing complex, and ongoing issues are often difficult to mitigate.

Branch Network/WAN: Enterprise Challenges

Applications deployed everywhere

Today, applications not only run in corporate data centers, but also exist at SaaS and IaaS Cloud service providers.

If all traffic to/from the cloud must be routed through the corporate data center for security functions, end user experience & response times will be negatively
impacted.

At the same time, additional security functions (e.g. firewall, access control & filtering, anti-virus/malware, DNS, etc.) are required if cloud resources are accessed directly from the branch office.

Bandwidth growth & application performance

Video and cloud storage/collaboration continue to consume a growing amount of WAN traffic. Increasing the capacity of MPLS and leased lines can be expensive.

The addition of direct Internet connections and broadband circuits provides lower cost bandwidth, but also increases operational complexity and security requirements.

Additional challenges come with monitoring and troubleshooting network health across multiple circuits, communication service providers and an array of network & application performance tools.

Branch Network/WAN: Enterprise Challenges

Slow response to change and business needs

Agility when facing unexpected events or line of business requirements at the branch allows companies to gain competitive advantage.

Unfortunately, companies deploying new or upgraded branch network services experience long deployment times due to provisioning of new hardware devices, as

well as scheduling consultants or integrators to install, configure, integrate and test equipment.

This occurs both at initial deployments, but also when capacity upgrades are required (e.g. if a new or larger WAN circuit is provisioned, then a higher capacity router and/or firewall is required).

Making a change to the branch WAN can take weeks and even months.

Leveraging Software-Defined WAN (SD-WAN) and NFV

The use of software abstracted from the underlying hardware used in the delivery of network services is called Network Function Virtualization (NFV), evolving previously hardware-centric network and security technologies into software-based solutions running on Commodity off-the-shelf (COTS) hardware and white-box appliances.

A core element of NFV is the virtualized network function (VNF), which is a software-based or virtualized version of a specific function like routing, CGNAT or next-generation firewall.

Much more than just converting from point hardware or appliances to virtualized software instances, VNFs are centrally managed and policy orchestrated, zero-touch provisioned, and service-chained.

Deployment Time

Taking an example of SDWAN, imagine an enterprise with 400 branch offices that wants to utilize inexpensive, high throughput broadband connections as an element of its overall WAN architecture.

Using the legacy appliance-based approach and deploying them at the rate 20 per month (an aggressive schedule, at one installation per business day), it would take over 1.6 years to complete the project.

Leveraging SD-WAN NFV-approach, the enterprise or service provider can ship commodity white box appliances to 100 branches per month, and simultaneously activate and test 25 devices per week remotely, yielding a total project time of 4 months. The result is a time reduction of nearly 80%, coupled with a significantly lower cost of deployment (as no on-site specialists are required).

Leveraging Software-Defined WAN (SD-WAN) and NFV

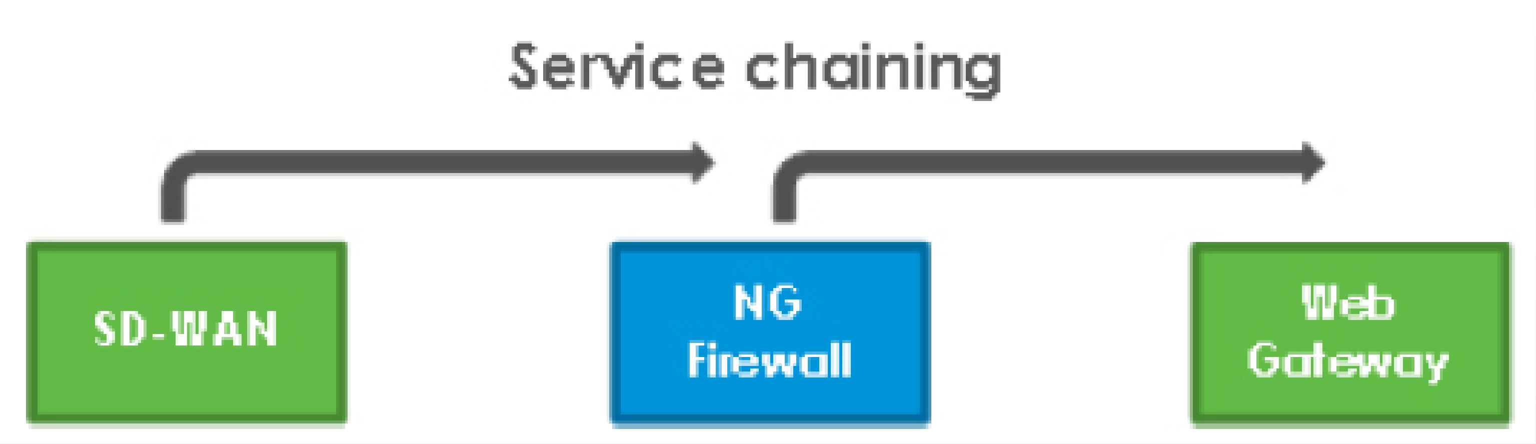
Service Chain

Another key aspect of SD-WAN using NFV is the ability to service chain security functions to easily achieve an SD-WAN with on-premises security to meet compliance and data protection requirements.

For example, specialized security functions like a secure web gateway can be service-chained to the SD-WAN to enable secure direct Internet access from the branch.

Service creation, service definition and service-chain rules utilize templates and provide programmable, API driven delivery of the service via centralized orchestration and management tools.

This automated approach enables each branch office SD-WAN to be deployed in hours, instead of days or even months.



Other benefits of SD-WAN with NFV

Application intelligence

SD-WAN has the ability to identify applications and use that knowledge to apply a range of network and security policies to the traffic carrying them.

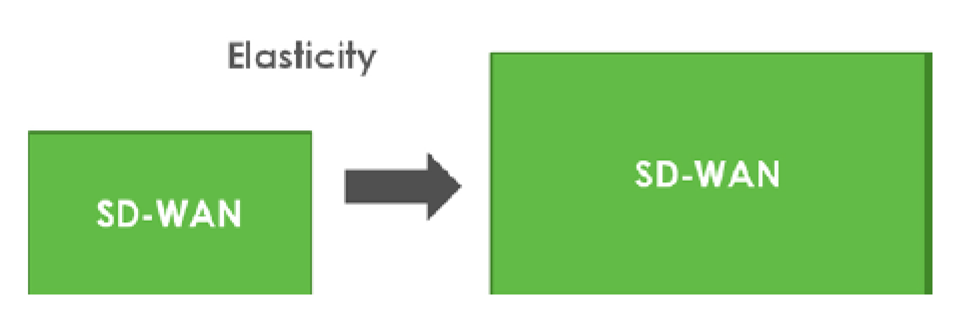
This includes mapping applications to particular WAN connections (e.g. core business applications to MPLS and consumer web traffic to broadband), application prioritization, per application security policy and enforcement (e.g. blocking certain types of web content), etc.

Elasticity

When deploying SD-WAN through an NFV-based model, capacity can dynamically scale up or down without having to replace or add additional proprietary hardware.

For example, branch bandwidth can be doubled in minutes either automatically or using commands from the central provisioning portal, with no truck roll or appliance swap-out.

In the event that a branch needs more capacity due to a network traffic spike, the SD-WAN can automatically scale up to meet the demand. When the network spike subsides, the SD-WAN will scale down as needed.

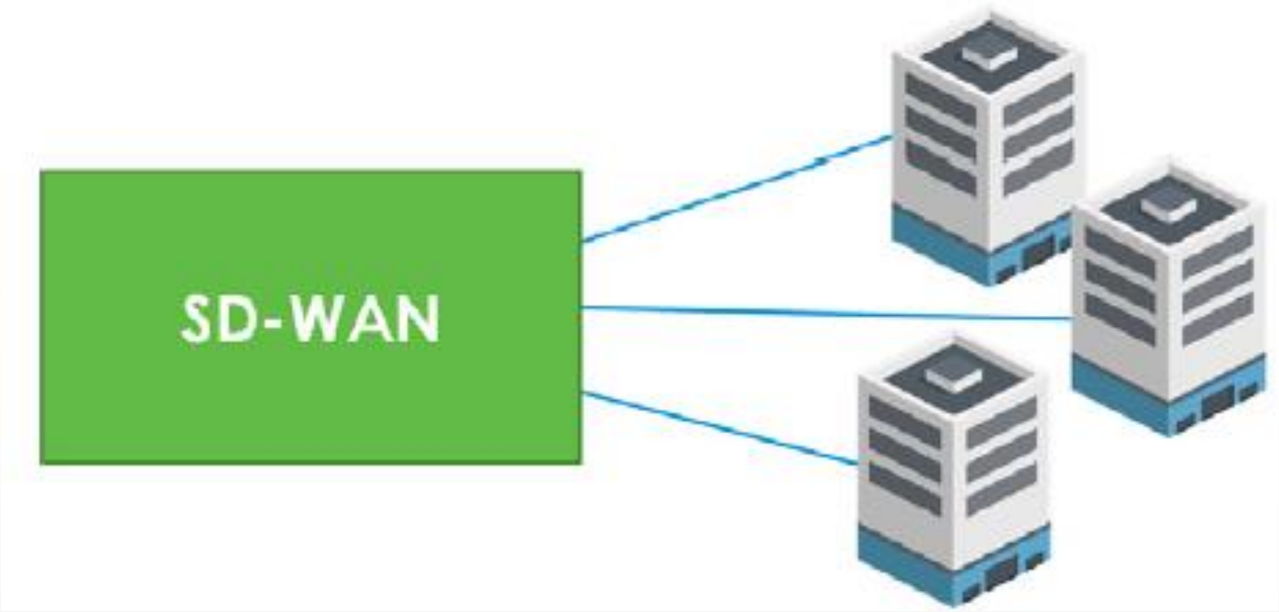


Other benefits of SD-WAN with NFV

Multi-Tenancy

SD-WAN is designed as a Carrier-Grade solution with full Multi-Tenancy support at both the head-end and branch.

Service providers operating SD-WAN managed services, as well as large enterprises operating different SD-WANs for separate business entities, can leverage this feature. The result is much lower infrastructure costs and more agile service delivery.



Other benefits of SD-WAN with NFV

Multiple deployment options

The SD-WAN can be deployed directly on bare metal x86 servers, white-box appliances, virtual machines (VMware ESXi, KVM) and containers.

Customers can select the best infrastructure for their SD-WAN deployment at both the data center/PoP and branch offices without being constrained by SD-WAN vendor proprietary hardware options, resulting in significantly lower CapEx and design flexibility.

Other benefits of SD-WAN with NFV

Flexible and distributed service architecture

With the advent of NFV, service providers and large enterprise have the capability (and flexibility) to decide where to deploy and run each layer of network or security
function – either on-premises in the branch office or centrally in the data center, at a provider’s point-of-presence (PoP).

For example, compute intensive services such as anti-virus and IPS can run centrally, while services that are key in the branch, like application identification, SDWAN, routing and firewall can be run locally.

Centralized, Automated Operations

A software-defined and NFV based approach to the WAN also provides a way to provision SD-WAN equipment and deliver network and security services from a single point of control, avoiding the need for skilled personal available on-site to deploy and configure the solution.

Instead, SD-WAN services can be deployed, bandwidth and service capacity increased or enhanced with additional functions automatically, all without requiring any on-site presence, hardware refreshes or manual interaction.

Thank You

TICVIC
NETWORKS
Connect Secure Redundant Besilient

Thank You

https://www.ticvic.com