Software Defined WAN:

CloudGenix

A whitepaper by Ethan Banks and Drew Conry-Murray

PACKETPUSHERS

Where Too Much Networking Would ***NEVER*** Be Enough

Table of Contents

Introduction

Software-Defined WANs (SD-WANs) aim to simplify and enhance branch and remote office connectivity. SD-WANs use a central controller to enforce policies and direct specific application flows (not just packets) across the most appropriate connection as defined by administrator criteria, including performance and cost.

An encrypted overlay creates a unified fabric from a physical underlay that can include private circuits, low-cost Internet broadband, and even LTE. This gives engineers more physical connectivity choices and can speed deployments.

Last but not least, SD-WANs combine application awareness and analytics so that the controller can respond to changing traffic conditions within the fabric to meet application requirements. They also provide real-time and historical performance data to help administrators manage the WAN, identify and address service issues, and meet business demands.

An SD-WAN is not technology for technology's sake. It can provide meaningful, measurable benefits to both IT and the business.

CLOUDGENIX
NETWORKS WITHOUT NETWORKING

This white paper explores in detail the core concepts of SD-WAN technology. It also provides a comprehensive overview of CloudGenix's SD-WAN product.

What Is SD-WAN?

Organizations are just beginning to reap the benefits of software defined networking (SDN) as real-world, usable products have come to market and adoption is becoming more widespread. One such SDN product category gaining traction is the software-defined WAN (SD-WAN).

Four SDN elements are critical to an SD-WAN solution.

While not all SD-WAN product offerings have identical feature sets, a complete SD-WAN solution should include the following four critical components.

- **Policy manager.** SD-WANs treat the WAN as a unified fabric — one massive entity that can be managed centrally. Network operators use the policy manager software to define traffic classes, security parameters, QoS characteristics, and other settings that are applied to the WAN fabric.
- **Central controller.** The controller software acts as a unified network control plane. In SD-WAN, the controller tells the forwarders how to forward traffic.
- **Forwarders.** Traditional WANs terminate long-distance circuits with routers. In SD-WAN, a forwarder does the work of a router, sending traffic across the WAN.
- **Analytics.** SD-WAN reacts to changing network topology, link load, and circuit performance in real time. In addition, forwarders are aware of the applications flowing through them. The controller and an analytics engine use this data for reporting and to make real-time changes in WAN fabric forwarding.

Using these building blocks, SD-WAN takes on problems that are common in wide area networks, but hard to solve using legacy WAN tools. For example...

- **Virtualizing a network across a traditional built WAN is complex,** requiring VRFs and perhaps a number of overlays to maintain a security boundary. If security policy demands stateful inspection, a firewall may need be deployed at each branch site to meet this requirement.
- Hybrid WANs, which involve a variety of private and public carriers, physical access methods, and encryption strategies, are **difficult to manage.** Standards and procedures differ per carrier.

- **Organizations with SaaS or public cloud applications lose insight** into network performance beyond their borders.

Those familiar with SDN design principles aimed at the data center or LAN may have concerns about applying these principles directly to a WAN environment.

For example, there's the problem of latency between the controller and forwarders, which is exacerbated in a WAN context. And what happens when a forwarder loses touch with the central controller, something more likely to happen in a WAN than in a LAN? And how is transport security guaranteed, as this is not of paramount concern in LAN environments?

SD-WAN architectures address all of these concerns directly. We'll discuss them as we progress through this paper.

How SD-WAN Is Different from Legacy WANs

To skeptical networkers, SD-WAN might sound like a marketing gimmick that attaches SDN buzzwords to the traditional, staid WAN. While marketers have jumped on the software defined bandwagon, SD-WAN is indeed distinct from traditional WAN.

The Key Term: Software Defined

Some might think that SD-WAN is just another way to describe WAN orchestration, thus bringing nothing materially new to the market. SD-WAN is more than orchestration, however. The key is in the term "software defined."

- In an SD-WAN, software takes **analytic inputs from the WAN** as well as **policy inputs from operators**, and defines a flow forwarding scheme. That scheme is constantly adjusted based on new information. The software engine at the heart of SD-WAN sets it apart from mere orchestration systems.
- SD-WAN is also distinct in that it **abstracts the physical WAN**. The physical WAN becomes an underlay that connects SD-WAN forwarders, but requires little care and feeding beyond that. Once the physical WAN is up and basic IP forwarding established, the work is done.
- SD-WAN forwarders handle security, QoS, flow forwarding, and exception routing, as well as redundancy and resiliency. Some SD-WAN forwarders can even terminate Ethernet circuits directly, making it **technically possible to retire legacy routers**.
- **Central management** is another important part of SD-WAN. Businesses define how an application should be forwarded across the network, and the central controller distributes that policy to all forwarders. Operators do not have to build specific configurations for individual devices to implement a business policy, as they do with a traditional WAN.

Packets vs. Flows

SD-WAN's greatest distinction, however, is in how traffic is thought of. Traditional WANs think about **packets**. SD-WANs think about **flows**.

Different application flows have different needs. For example, the SIP flow used as the control channel to set up a voice conversation can tolerate jitter and latency well, while the RTSP flow used to carry a real-time voice conversation cannot. Delivering the entirety of a flow end-to-end across a wide area network, no matter how the WAN's characteristics change, is critical. SD-WAN considers flows across an infrastructure, as opposed to packets at junction points.

Emerging WAN Design & x86 for Network Computing

An interesting aspect of SD-WAN is that it wouldn't have been an especially compelling solution all that long ago. Only recently have three trends converged to make SD-WAN a technology that makes sense for WAN operators.

Viability of Internet Links

- **Private WANs guarantee performance, reliability, and security, but at a high price.** To reduce that cost, organizations have turned to cheaper — and in many cases, higher bandwidth — Internet circuits to lower the dependence on private WAN. This has proven viable as Internet transport is increasingly reliable.
- The challenge comes in **managing connectivity across that public link.** Data encryption becomes a requirement. QoS is not easily solvable, as Internet service providers offer a best effort service only, and do not distinguish traffic classes.

The Rise of the Hybrid WAN

- Organizations have built **complex WAN topologies** that mix service providers, public and private transport, and access methods based on cost and availability at remote locations. This complicates management.

- **Different WAN device configurations** are required for every iteration of WAN access type. An LTE router configuration doesn't look the same as an Internet-facing router with a DMVPN termination.
- That configuration differs from a router configured for a private connection handed off by an MPLS service provider. Getting **identical end-to-end treatment of traffic** across that infrastructure is a configuration challenge.

x86 as a Network Computing Platform

While custom silicon still has advantages at massive scale, **at WAN scale x86 is more than adequate.** X86 offers plenty of computing power to fill gigabit Ethernet circuits and beyond. That positions x86 as a commodity platform on which to run SD-WAN controllers and forwarder software.

As these three trends — the operational complexity of hybrid WAN, the rise of x86 as a network computing platform, and the excessively high cost of operating a WAN — converge, SD-WAN finds its use-case.

Easy-To-Manage, Policy-Based Forwarding

SD-WAN offers a new way to provide secure, reliable communications among remote locations. The same basic services — forwarding, security, QoS, exception routing, resilience —are provided in completely different ways.

SD-WAN looks at traditional WAN forwarding and sees it as inflexible, which it is. WAN forwarding today is governed by routing protocols that were designed to do one thing: compute best path.

The problem with "best path" is twofold.

1. **Best path is computed based on unsophisticated metrics.** While different routing protocols use different formulas to calculate best path, ultimately the computation comes down to the fastest path - the lowest hop count, the most bandwidth, the least amount of delay, the fewest AS traversals, and so on. Even BGP, which can use complex policies to impact forwarding decisions, has no inherent system-wide awareness or ability to accommodate real-time conditions such as high link utilization.

2. **Best path is a one-size-fits-all computation.** In other words, best path is the same for all traffic bound for a particular destination prefix. Traditional routing protocols can't distinguish among the needs of different applications.

By contrast, SD-WAN forwarding is flexible.

Best path determination considers much more data than legacy routing protocols can.

- **SD-WAN forwarding considers application flows**, and not simply packets.
- **SD-WAN forwarding considers operator-defined policy** as applied to those flows. Does a flow require low latency? Low jitter? Stateful firewall traversal? Cheapest dollar cost? All of those (and more) can impact the path a flow takes through the SD-WAN. Different flows between the same source and destination address pair could end up taking different paths as a result.
- **SD-Data forwarding considers the real-time condition of paths** between forwarders. SD-WAN can react to situations such as brown-outs or congested links and make real-time changes to the forwarding topology.
- **SD-WAN forwarding allows for active/active link utilization.** While traditional routing protocols accommodate equal cost multi-path (ECMP) forwarding, ECMP is based on an equal cost as computed by simplistic best path metrics. SD-WAN has more subtle active/active link capabilities, allowing for flow forwarding through any and all paths available, and not eliminated from use simply because of inferior bandwidth.
- **SD-WAN forwarding automates exception routing in accordance with policy.** In a traditional WAN, policy based routing (PBR) forces traffic down unusual paths, but operators manage PBR policies device by device. SD-WAN makes whatever forwarding exceptions are required to ensure that applications flows meet with the defined business policies.

SD-WAN's flexible forwarding capability plays well in a modern, hybrid WAN environment. When implementing SD-WAN, the type of WAN circuit in use becomes less important than having a choice of paths and sufficient bandwidth. A site that might have used a combination of private WAN and public Internet as a backup path could now use two or three Internet links and achieve a service level that previously required a private carrier.

SD-WAN's flexible forwarding builds in the requirements of security, QoS, exception routing, and resilience.

Forwarding decisions driven by central business policy needs integrate these features that network operators used to treat separately.

- **Traffic between SD-WAN forwarders is encrypted, and no key management is required of the network operations team.** The SD-WAN solution manages keys automatically. Service chaining through firewalls or IDS/IPS devices is also supported, if stateful inspection or DPI is required.
- **QoS is built into the forwarding intelligence and real-time knowledge of the SD-WAN fabric.** Rather than configuring a one-size-fits-all QoS policy that aims to handle an unpredictable traffic mix during times of link congestion, SD-WAN knows in real-time exactly the path characteristics and can shape traffic flows as required to minimize congestion. It can swing certain flows to a path that meet business policy SLA, queue and prioritize flows, and account for some amount of path packet loss, resulting in a user experience that meets business policy.
- **Changes to the SD-WAN fabric topology are managed without the use of a routing protocol.** New paths between forwarders, as well as lost paths, are known immediately by the SD-WAN controllers. The forwarding topology is recalculated and deployed to the forwarders.

SD-WAN genuinely rethinks how a WAN is built and utilized, making no assumptions that "there must be a router" or "we have to use a traditional routing protocol." In fact, SD-WAN relies on industry-standard Ethernet & IP connectivity and little else. SD-WAN is an immediately useful tool for any organization using a WAN.

The CloudGenix SD-WAN Solution and Architecture

With a full complement of software features and a robust architecture, CloudGenix offers a complete SD-WAN solution. Let's look at the component parts and the critical features and functions that distinguish the CloudGenix's offering.

Central Controller

The CloudGenix Central Controller is software and can run in the cloud, as a VM in the local network or on a CloudGenix X86 box in the datacenter. Each form factor delivers the same functionality, while catering to the individual needs of the organization. As implied by the name, the CloudGenix Central Controller is the central point of control, management, policy setting, analytics and reporting for the SD-WAN fabric. The Central Controller is for control-plane functions solely, and is not in the data path. As such, latency concerns are minimal.

Engineers who think of a WAN router's control-plane think of routing protocols. For example, OSPF runs locally on a traditional WAN router, peering with neighbors, and exchanging information about link state and possible destinations. OSPF populates the routing information base (RIB), which is then used to populate the forwarding information base (FIB). The router references the FIB when forwarding traffic.

The control-plane in the CloudGenix SD-WAN is quite different. There are no routing protocols whatsoever. Rather, the CloudGenix controller programs flow forwarding policy into the forwarders (what CloudGenix calls "ION Fabric") using APIs.

ION Elements

CloudGenix has branded parts of its SD-WAN solution "ION" for Instant-On Network. The CloudGenix ION Elements are flow forwarders. They are analogous to WAN routers in terms of function, but ION Elements are deployed as VMs on

commodity x86 devices, essentially simple PCs with several Ethernet interfaces and enough CPU and memory to handle traffic forwarding at multi-gigabit line rates. Customers can buy an ION appliance directly from CloudGenix or supply their own hardware and install it as a virtual machine. The ION Element can be installed at branches, headquarters, co-los, and public cloud (IaaS) locations.

ION Elements have several jobs.

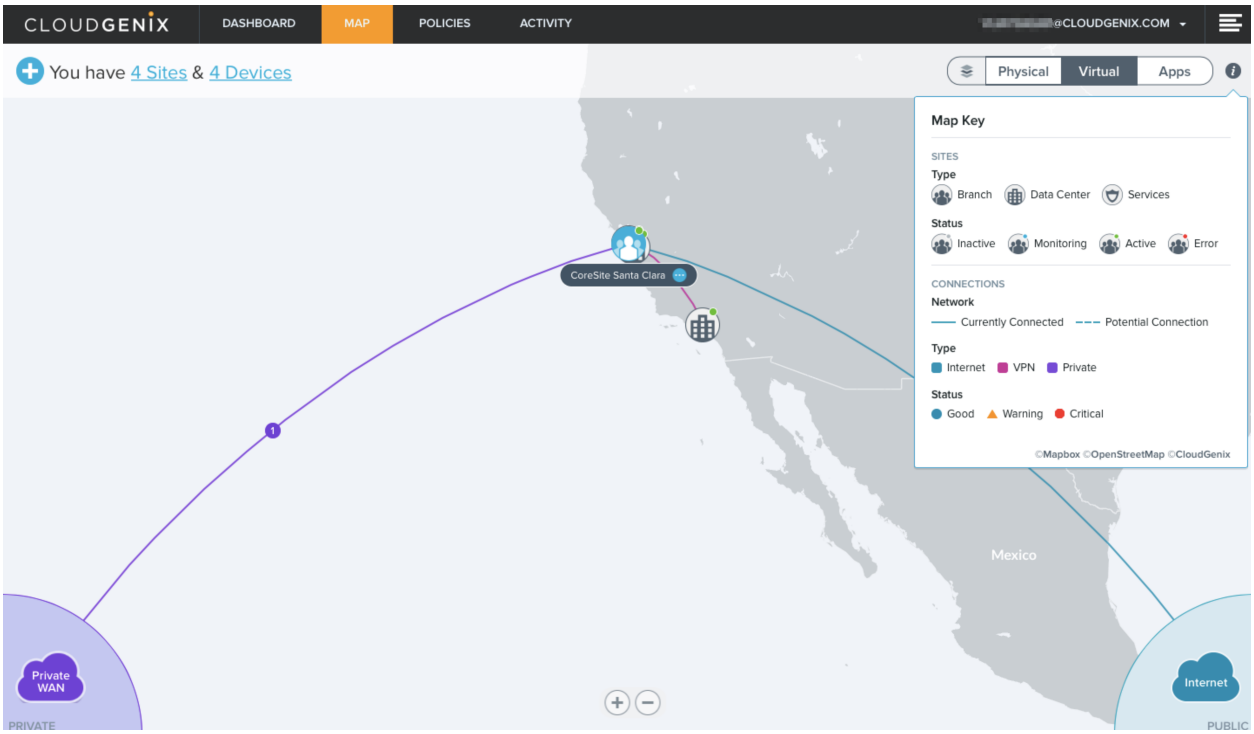
- **Flow forwarding.** First and foremost, the ION Element forwards application flows, similar to how a router forwards packets. However, since the Element is contextually forwarding flows and not simply packets, the way it makes a forwarding decision is markedly different from a WAN router. Instead of being focused on reachability and best/fastest path and low hop counts, the ION Element forwards application flows based on the ability of a link to deliver that application in accordance with a policy-defined service level agreement.
- **Topology change notification.** The ION Fabric monitors itself for availability. Each Element sees a connection to another Element as a path. When an Element can no longer communicate with another, that path is withdrawn, and the central controller notified. A path is a virtual construct, similar to the connectivity of a GRE tunnel between two routers. Elements might also be responsible for directly connected, physical WAN circuits, and will keep the controller notified of link status at all times.
- **Flow classification.** As traffic flows through the Element, the Element must determine what the flow actually is. CloudGenix flow identification distinguishes on-premises, cloud and SaaS applications down to the sub-application level. Correct flow identification ensures that the traffic will be subjected to the correct policy component.
- **Service level agreement (SLA) monitoring & enforcement.** Application flows will have specific performance characteristics as they traverse the SD-WAN fabric: transaction time, jitter, packet loss, and so on. The Element tracks these flow characteristics and compares them to the SLA as defined by the policy issued by the central controller. The Element places flows on the path that will best meet the SLA requirement at any given time. The path used by an Element for a given flow might change from one minute to the next, depending on path conditions.
- **Flow table maintenance.** For high availability, a flow table state must be maintained by the Element. The Element is aware of the state of all active application flows going

through it at all times. Flow table data is also used by the Element to maintain path symmetry, important when a path includes traversal of a stateful firewall, for instance.

The ION Element never punts data packets to the central controller and awaits further instructions; the central controller is never in the data path. Even if the ION Element is unable to communicate with the controller for some period of time, it is still able to forward flows. In the case of such a separation, the Element will forward in accordance with the last policy update it received. When connectivity to the controller is restored, the Element will be refreshed with any new policy changes.

ION Fabric

CloudGenix ION Fabric is the overlay mesh of ION Elements. The ION Fabric contains one or more virtual networks that abstract the physical hybrid WAN they ride on top of. By default, all traffic flowing across the fabric (i.e. between ION Elements) is encrypted with AES-256 IPSEC.



While ION Fabric abstracts the physical network underlay, ION Fabric also manages other complexities of the traditional WAN, making it simpler to operate.

- **The security perimeter becomes flexible.** ION Fabric lets you pass remote office traffic through central firewalls, rather than deploying firewalls to every branch office. Because the overlay encapsulates traffic, branch traffic that needs to traverse a firewall can be sent to an Element at a data center site, and then delivered to a firewall for inspection.
- **Virtual WAN creation becomes automated.** ION Fabric can create several different virtual fabrics, each with its own business policy. Organizations can create policies for specific applications defining priority, available paths, and security. These can be further defined by user or user group, location, and/or sub-application. This is done via policy, and does not require the creation of unique VRFs coordinated with the carrier. Instead, virtual fabrics are managed as separate overlays by CloudGenix.
- **Public key infrastructure (PKI) becomes simple.** Inside of the ION fabric, IPSEC is used to encrypt traffic between Elements. Key management is therefore a concern. CloudGenix manages PKI automatically, using unique keys that are rotated hourly with no human intervention.

Application Fingerprinting

CloudGenix has taken a unique approach to application fingerprinting amongst other SD-WAN providers. The approach uses sessions flowing between endpoints to identify applications, rather than using signatures or deep packet inspection (DPI). In the context of application fingerprinting, DPI is difficult to rely upon due to the increasing number of encrypted application payloads found in modern networks.

By using application sessions, CloudGenix is able to accurately identify not only applications but sub-applications as well. For instance, unified communication endpoints might have several different sessions flowing between them for signaling, voice, video, chat, and screen sharing traffic. By observing the flows that make up each of these sessions, CloudGenix can identify each sub-application specifically. This is key when considering business policy. Different sub-applications may have different security or QoS requirements. As a result, different sessions

sessions could be sent down different paths through the network as an ION Element determines how best to meet security and SLA requirements.

CloudGenix has developed a large database of known applications, and updates that database as new application session data comes in from organizations using CloudGenix. This is not in lieu of commonly available application identification databases, which CloudGenix might leverage. However, these more generic databases often lack the sub-application granularity that CloudGenix is convinced is key to network operators and business policy creators.

Sophisticated Path Selection

In the CloudGenix forwarding approach, there are no routing protocols. That is to say, **within the ION Fabric, routing protocols are not employed** to determine best path between one ION Element and another. The underlying physical WAN might still use routing protocols, but this is only if required for ION Elements to forward traffic between each other.

Put another way, ION Fabric doesn't care how encapsulated overlay traffic between Elements is delivered, in the same way that VPN tunnel peers have no knowledge of the network infrastructure between them.

Inside the ION Fabric, path selection is handled in a nuanced way that places no configuration burden

APPLICATION PERFORMANCE VS. LINK PERFORMANCE

Determining the performance of a link is useful, but potentially misleading without application context. Why? Different applications react to changing link conditions in different ways.

A link might be lossy or high latency, but still an adequate performer for some applications. A link could be running WAN optimization that only impacts certain applications.

Therefore, only by testing individual application & sub-application performance across a specific link does it become clear how best to forward specific traffic classes across the WAN.

on network operators. A complex metric is calculated to determine the best Element-to-Element path to send traffic down that includes the following elements.

- **Link goodput.** Goodput is the real-world throughput of a link after subtracting for retransmissions and other network overhead that is not part of valid payload delivery. CloudGenix tests links constantly to determine real-time goodput of a link. This takes the guesswork out of actual performance for links with ambiguous speed promises, such as an ISP offering "up to" a certain data rate.
- **Link capability.** Beyond goodput, links have characteristics such as latency and loss that ION Elements monitor.
- **Application performance.** ION Elements know how an application must perform to be in compliance with policy, and monitor actual application performance in real-time.

The resulting "best path" decision takes into consideration link goodput, link capability, and application performance requirements. The decision is never simple, nor makes generalizations such as, "High latency links should be avoided."

TRANSPORT AGNOSTICISM VS. TOPOLOGY AGNOSTICISM

Hybrid WAN coupled with an overlay delivers ***transport agnosticism***. Traffic might be delivered over public or private transport; it largely doesn't matter which, so long as the traffic is delivered.

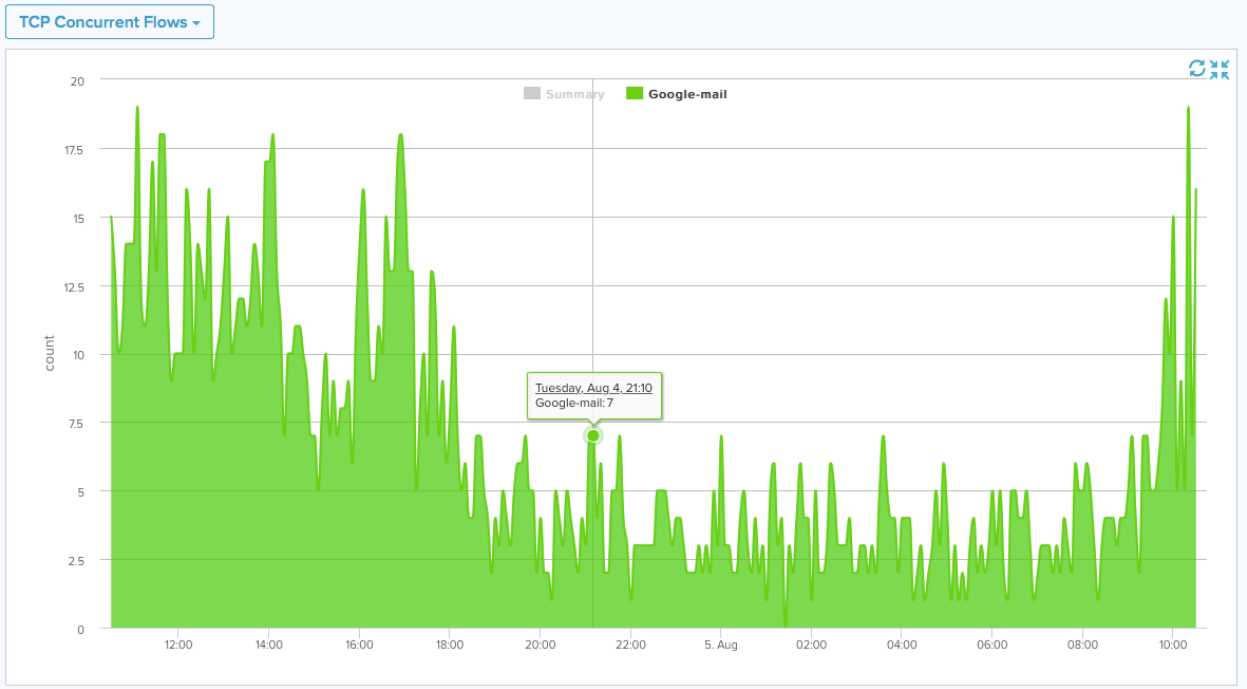
The progression beyond transport agnosticism is ***topology agnosticism***, where traditional routing protocols are removed from the SD-WAN overlay, and business policy dictates arbitrary WAN topology such as a regional hub model, or integration with network resources located in the public cloud.

Some applications are not greatly impacted by high round trip times and may perform sufficiently across a high latency link. CloudGenix path selection takes real-time path capability into account along with the specific needs of individual application sessions, and make forwarding decisions on a flow-by-flow basis.

Path selection is never an either-this-or-that choice. **All paths are available for use — "active/active" is normal in an ION Fabric.** The real-time monitoring is also critical to best path, as brownouts can happen due to congestion or a temporarily lossy link

that negatively impacts performance.

Path selection might also include traffic shaping. Shaping makes sure that other application flows have enough bandwidth to meet their SLA requirements, a useful feature especially in the face of links with unpredictable amounts of maximum bandwidth, such as ISPs that do not guarantee link throughput. This is an improvement over one-size-fits-most QoS schemes that presume a specific amount of available bandwidth, and can't react to changing bandwidth availability.



Management

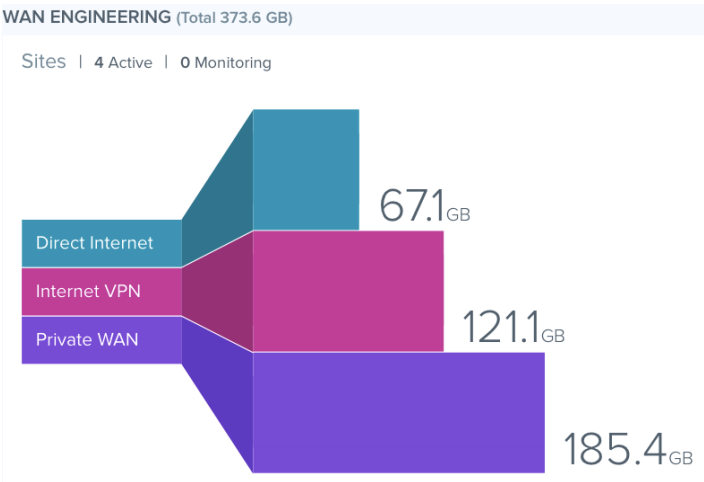
A CloudGenix component alluded to several times but not yet discussed is that of policy. The CloudGenix policy manager is where network operators describe how applications are to be treated as they traverse the ION Fabric. The policy manager is designed for simplicity. Rather than operators having to know nuanced network details to write a policy, CloudGenix abstracts away as much of the detail as possible. This allows policy elements to be written with the following nomenclature.

> Connect (users) to (resources) with (priority) ensuring (security/compliance).

The CloudGenix policy manager expresses complex network goals in a simplified, business-oriented way. Humans can read and understand a completed policy.

Traffic Analytics

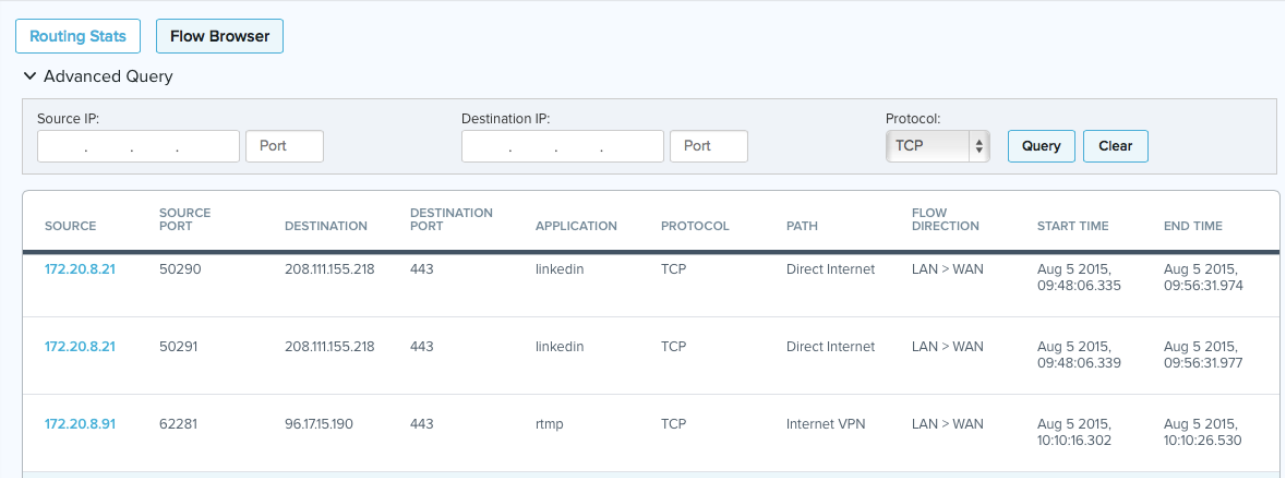
As a cloud-based controller, CloudGenix collects statistics from the ION Elements of all customers. Aggregating these statistics provides CloudGenix with a global view of key data points. This is useful for detecting problems affecting large numbers of customers in certain parts of the Internet, at specific data center colocation facilities, or with SaaS providers. Customers can opt out of the compilation of aggregated global statistics.

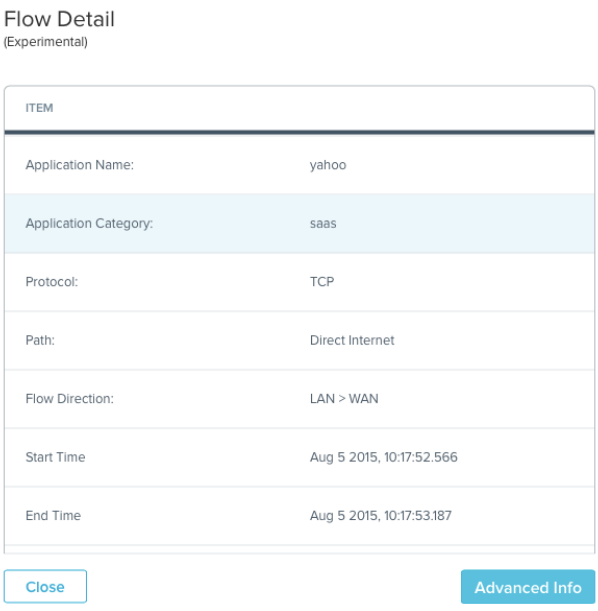


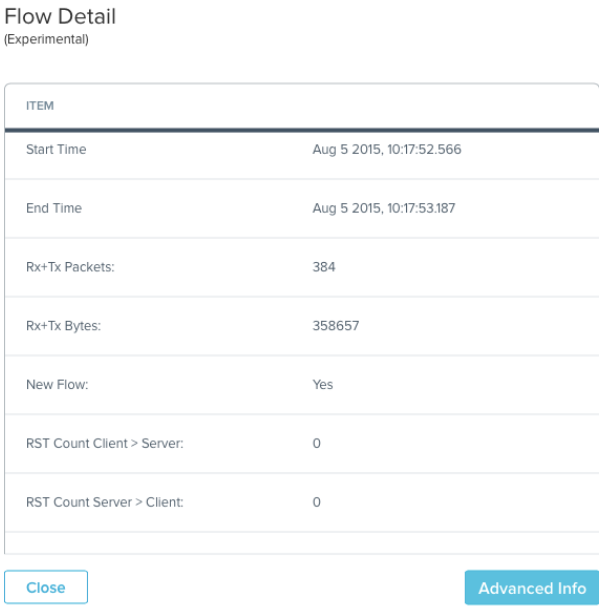
Whether opting in or out of global statistics, the customer's specific CloudGenix controller tracks local

application flow statistics, ION Fabric performance, and compliance with service level agreements. This granular data offers insight into application and sub-application performance over time.

Practically speaking, this approach is an advance over SNMP and log-based network management stations (NMS). An NMS can gather any number of statistics by polling SNMP OIDs or parsing log entries, but leaves data interpretation up to the network operator. The CloudGenix traffic analytics system shows specific application flow information and provides performance and compliance reports that are immediately useful to a business.







Getting Started with CloudGenix

Moving ahead with SD-WAN might seem daunting. At a glance, the architecture seems unfamiliar. There's a controller to get going, and ION Elements to bring online — somehow. New networking is often a risky, time-consuming endeavor. Time and risk tolerance are two things network engineers have little of. The CloudGenix architecture minimizes both with a number of deployment features to help organizations get started.

Zero touch provisioning

When ION Elements ship from CloudGenix, they are pre-configured to automatically come online, grab a DHCP address, and register with the controller. ION Elements ship with a manufacturer certificate that includes the location of the cloud controller and a security key. The registration process tells the controller about the ION Element device, including the customer that bought it. The controller places the ION Element into that customer's inventory. Before the Element can begin forwarding traffic, the customer must claim the device.

Using this system, customers do not have to preconfigure ION Elements before shipping them to remote locations. The Elements come online with enough knowledge to connect to a controller in the appropriate customer context, be approved by the customer, download policy, and start forwarding flows.

Service insertion for the data center

Bringing ION Elements online does not necessitate that all sites participate in the ION Fabric at once. Rather, it is possible to add sites to the fabric gradually. Let's assume a data center is a central location that most remote sites in the WAN need to communicate with. How is the ION Element inserted into the WAN traffic flow of the data center?

ION Elements for the data center are able to connect to the DC fabric using eBGP. The Element peers with the core router (or possibly the headend WAN routers) and attracts traffic using traditional routing. The idea is that the Element will announce to the data center core network specific address blocks that it is ready to handle. Those address blocks might be for remote branches that also have ION Elements, or for specific applications. In this way, CloudGenix can add value on a selected branch or application basis.

This process leaves the business in control of when traffic will begin to traverse the ION Fabric. Specific applications can be tried. Specific branches can be tried. Backing out is relatively easy.

Service insertion for the branch

CloudGenix has three options for inserting an ION Element into the traffic flow of a branch location. Each option builds on the other, allowing for a gradually deeper involvement of ION Elements into branch office WAN traffic patterns.

1. **Analytics mode.** In analytics mode, an ION Element sits in the data path between the switch and the WAN edge router. An operator tells the ION Fabric which IP blocks are local to that branch. The CloudGenix system then learns the applications flowing from the branch into the WAN, how they are performing, and creates traffic profiles. In this mode, there is no flow forwarding of traffic via the ION Fabric. Analytics mode is used for learning and analyzing the network, providing visibility into the application performance, and charting baselines. This data can be used for troubleshooting performance issues and verifying regulatory compliance and security paths, as well as identifying where CloudGenix ION Elements should be placed initially.
2. **Router interoperability mode.** In router interoperability mode, an ION Element once again sits in the data path between the branch switch and WAN router. An operator tells the ION Fabric which IP blocks are local to that branch. Internet circuits are terminated on the ION Element, although private MPLS circuits are not. Flow forwarding via sophisticated path selection is enabled, allowing for the ION Element to decide whether traffic should flow across the private WAN or public Internet. This is a halfway step that enables the full functionality of the CloudGenix system, but allows existing WAN routers to stay in play. Organizations that have yet to fully depreciate the WAN edge routers or

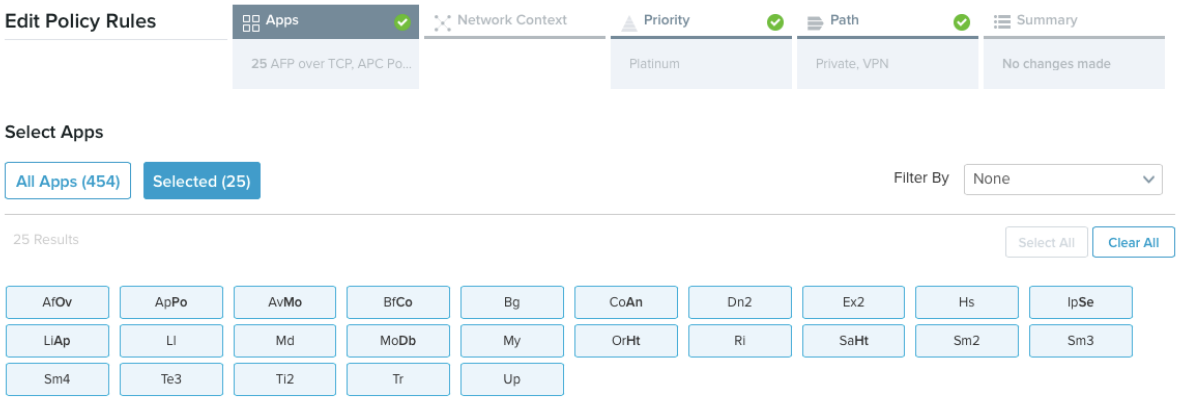
who have specific operational processes built around their WAN routers are likely to take advantage of this mode.

3. **Full router replacement mode.** When fully replacing a WAN router with an ION Element, all circuits are terminated on the CloudGenix box directly. The site fully participates in ION Fabric as in router interoperability mode. Terminating all circuits on an ION Element is possible assuming all circuits are Ethernet. For TDM circuits such as T1/E1, a WAN router will remain in use solely as a routed bridge between Ethernet and TDM interfaces.

Policy creation & maintenance

As ION Elements come online and the ION Fabric forms, network operators can compose policy. This policy will dictate how to handle flows across the fabric. The policy is written in a declarative language, where business intent is described in plain speech. In short, an operator will need to define the following key policy elements.

- **Applications of interest.** Each network has a somewhat unique application mix. Operators can select applications already known to CloudGenix out of the box. Operators can also define their own applications.
- **Users of interest.** CloudGenix lets organizations track to the user level.
- **Allowable paths.** In a hybrid WAN, several paths may be available between ION Elements, such as a public Internet path and private MPLS path. DMVPN or Internet-based IPSEC are also options.
- **Services.** Operators must define service requirements, such as traversing a firewall, for application flows.



With all of these definitions established, an organization can then use the defined elements to build the declarative language policy.

Another advantage of the centralized policy management is the ability to make policy changes without necessarily having to go through change control approval.

From a certain point of view, there is no system change being made. There is no IP re-addressing, no circuit turn up or turn down, no routing configuration change, no network device configuration change required to effect a policy change. Rather, a policy change is made and distributed to ION Elements with no disruption of service required. This means that changes as simple as application flow QoS handling or as complex as instantiating a new virtual ION Fabric can be done with a minimum of process overhead.

Service chaining

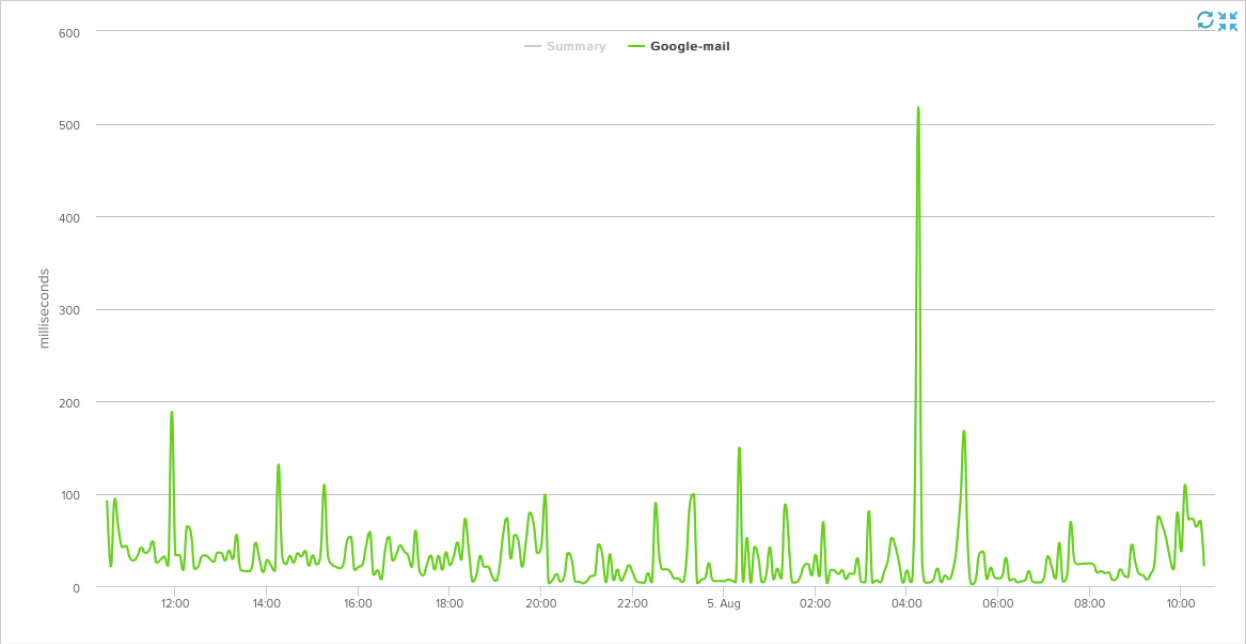
Service chaining sends traffic through a series of devices to result in some outcome. For instance, traffic might be chained to flow through a load balancer, firewall, and DPI device. There are many emerging SDN solutions that manage service chaining, although no one single solution has emerged as an industry reference model. CloudGenix interoperates with any service chaining model a customer has deployed.

CloudGenix uses the idea of a service hub to denote a service. A firewall cluster known to exist on the network by a particular ION Element is an example of a service hub. When a service hub is required by a policy element for a particular application flow, the ION Element will forward it to the service hub. Traffic will traverse the service hub and return to the ION Element for final forwarding to the ultimate destination.

Reporting

Once the ION Fabric is up and running, the controller gathers data application flows. CloudGenix uses this data, among other information, to generate reports. Many different reports are available. Here are a few examples.

- **Application transaction times.** Application transactions are broken down by their component parts (DNS lookup, SSL setup, HTTP load time, and so on.).
- **Verifiable compliance.** This means that applications traversing the ION Fabric demonstrate compliance with regulatory standards. For instance, an application can be shown to be subject to encryption, traversal of a firewall, and so on. This is an easier way to demonstrate compliance than handing over a pile of device configurations to an auditor.
- **Application availability.** Availability is an indicator of up time that shows when an application was reachable via the ION Fabric.



Understanding ROI and Operational Impact

It's one thing to understand the technology behind SD-WAN in general and a specific vendor's solution. It's another to understand the value of the technology. Let's consider a couple of factors that help determine whether SD-WAN is an appropriate investment.

Hard cost savings for an SD-WAN are straightforward to calculate.

There are obvious savings in the physical WAN infrastructure.

- Leveraging encryption and active/active paths, organizations can take increase adoption of public Internet links while reducing their use of private WAN circuits.
- On the assumption that private WAN costs are among the most significant of any IT budget, ROI calculation becomes a math exercise. Subtract the SD-WAN private WAN cost from the legacy private WAN cost.
- Eventually retiring routers within the WAN as refreshes approach can lead to both short-term savings and accrued long-term savings through reduced capex.

Soft cost savings are less straightforward to compute.

You can calculate the benefits of simplified IT operations, though it's more difficult to assign a dollar cost here. That said, with a centrally managed SD-WAN solution in place, the following statements that bear on opex are true.

- Network operators do not need to configure individual WAN routers to change policy.
- Routine changes do not need to be handled by network engineers with deep, specialized knowledge. This frees up engineering staff to work on business enriching projects, reduces human error, brings policy changes to bear more quickly, and improves system availability.
- Reports and network data is readily available and easy to consume, allowing organizations to spot issues and resolve them quickly.

IT's focus is shifting from delivering vertical functions (storage, security, virtualization, networking) to delivering applications. All IT systems work together to deliver reliable applications that perform well for business users that need them. A centrally managed business policy that guarantees application performance to remote locations positions SD-WAN in a critical role in IT's application delivery mission.

Conclusion: The Real Goal of SD-WAN

A wave of 'software-defined' technologies and architectures is flooding the network landscape. IT leaders and network engineers need to pay careful attention to the technical details behind new hardware and software products because those details affect your infrastructure and operations.

But even as you immerse yourself in control planes, configurations, and fabrics, don't lose sight of the overarching goal: to provide robust connectivity to applications and users for the right price with the right performance.

A good SD-WAN product should deliver clear and measurable value to the organization. It should help the business link up new branch and remote offices faster. It should simplify the WAN topology by abstracting multiple physical circuits into a centralized, policy-driven, application-aware fabric that's responsive to real-time network conditions. And it should help reduce costs by enabling lower-cost connectivity options and streamlining deployment and operations.

The details of an SD-WAN product matter, but first and foremost it should solve real business problems. Start with that perspective as you investigate this emerging technology category.