Compliments of CLOUDGENIX
NETWORKS WITHOUT NETWORKING

CloudGenix Special Edition

Software-Defined WAN

FOR DUMMIES®

A Wiley Brand

Learn:

- Best practices for implementing software-defined WANs
- Top benefits and expected ROI
- Ten considerations when deploying a software-defined WAN

Darril Gibson

Software-Defined WAN

FOR DUMMIES®
A Wiley Brand

CloudGenix Special Edition

by Darril Gibson

FOR DUMMIES®
A Wiley Brand

Software-Defined WAN For Dummies®, CloudGenix Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-09854-6 (pbk); ISBN: 978-1-119-09846-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Johnson
Editorial Manager: Rev Mengle
Acquisitions Editor: Steve Hayes
Business Development Representative: Karen Hattan
Production Editor: Kinson Raja
Special Help: Vijay Sagar, Aaron Edwards, Rebecca Salie

Introduction

Virtualization and hypervisor technologies have allowed many data centers to transition from hardware-based to software-based data centers (SDDCs). Now, a similar transition is occurring with wide area networks (WANs).

At the forefront is a need for hybrid connectivity for WANs. Traditional WANs use a single connectivity method such as Multiprotocol Label Switching (MPLS). A hybrid WAN dynamically supports MPLS, broadband Internet, cellular connections, and any other transport mechanism available to an enterprise.

Dynamically choosing the correct paths for traffic is exceedingly complex with traditional hardware. In contrast, this should be table stakes with a software-defined WAN (SD-WAN). As an example, the CloudGenix SD-WAN solution enable network managers to create policies using plain business language. These policies designate allowed paths for specific applications, users, and/or service level agreement (SLA) customers.

About This Book

Software-Defined WAN For Dummies, CloudGenix Special Edition, is designed to help you understand SD-WANs. This includes many of the benefits such as reduced cost, improved performance, an elastic security perimeter, and shorter deployment timelines. It

also outlines the requirements of a robust SD-WAN solution.

Icons Used in This Book

This book uses the following icons to call your attention to information you may find helpful in particular ways.

The information marked by this icon is important and therefore repeated for emphasis. This way, you can easily spot noteworthy information when you refer to the book later.

This icon points out extra-helpful information.

This icon marks places where technical matters, such as SD-WAN jargon, are discussed. Sorry, it can't be helped, but it's intended to be helpful.

Paragraphs marked with the Warning icon call attention to common pitfalls that you may encounter.

Chapter 1

Knowing What a Software-Defined WAN

In This Chapter

- Defining software-defined WANs
- Diving into software-defined everything
- Comparing SDNs for the data center and for the WAN

There's a revolution afoot in networking known as *software-defined networking* (SDN). Instead of complex hardware-based networking, organizations are moving toward simplified SDN. This chapter looks at the different software-defined capabilities that are emerging, with a focus on *software-defined wide area networks* (SD-WANs).

Defining SD-WANs

By leveraging the differences between SD-WANs and software-defined data centers (SDDCs), it's easier to define and create SD-WANs. SD-WANs use centralized controllers without relying on interactions with underlying provider transport solutions. De-coupling the data plane from the control plane, replacing Internetworking

protocols with APIs, and building policies based on application metrics rather than network metrics make this possible.

A WAN connects two or more local area networks (LANs) located in separate geographical locations. For example, a WAN can connect a LAN in a main office location in San Jose with a LAN in a remote office in San Francisco. With this in mind, the simplest definition of the SD-WAN is a WAN that utilizes software and virtualization technologies, instead of traditional hardware, such as routers, to connect remote locations.

However, that simple definition doesn't tell the whole story. Here's a more technical and complete definition: The SD-WAN utilizes software and virtualization technologies to create a WAN and includes the following three elements:

- Separates the network's data plane (or forwarding plane) from the network's control plane — you often see this process described as *decoupling* the data and control planes.
- Provides centralized control
- Is easily programmable

Transitioning to SDX

Software-defined everything (SDX) refers to the trend moving from systems that have tightly coupled software with proprietary hardware toward a model where software can be run as an application on commodity off the shelf x86 compute platforms.

One of the primary drivers that has encouraged SDX is virtualization. Organizations have virtualized their computer infrastructure and moved to a software-based

programmable and management model. The next logical step was to use these technologies in SDNs and SDDCs. Over 50 percent of server workloads are virtualized through companies such as VMware, Microsoft, and Citrix, especially in large data centers.

With virtualization you can often reduce the number of physical servers by a factor of ten. As an example, a data center hosting 500 physical servers can host the same number of virtual servers on 50 physical servers. This reduces operating costs and energy costs and can save an average of $3,000 annually for each virtualized server or, in this case, $1.35 million. With savings like that, it's no wonder so many organizations have fully embraced virtualization.

The next logical step was a transition from hardware to software on networks leveraging some of these same virtualization techniques. It first started in the SDDC and is now expanding to the WAN with SD-WAN.

SDN has grown exponentially in recent years. According to SDxCentral, the 2013 SDN market was estimated at about $1 billion and is expected to exceed $35 billion by 2018. While fundamental differences do exist between SDNs and SD-WANs, it shouldn't surprise anyone to see a similar growth spurt with SD-WANs.

Comparing SDNs for the Data Center and for the WAN

Just as SDNs use a controller to manage the network, SD-WANs also use controllers, but significant differences exist in the functions of these controllers.

As an example, consider the SDN used within a data center. A data center is a highly controlled environment with significant physical security, high bandwidth, and low latency. Signals sent between the controller and other systems typically arrive in ten milliseconds or less. Moreover, unless the network has a problem, the bandwidth and latency are constant.

In contrast, WAN connections have a high degree of variability. The controller is in a separate geographical location and may be thousands of miles, hundreds of milliseconds, away from branch locations with highly variable bandwidth and latency. Something as common as rain can disrupt signals sent between microwave links. The controller might enjoy 99.999 percent uptime, but it's highly unlikely that you'll enjoy the same uptime with the transport connections.

These issues aren't a concern for SDN controllers located in the data center, but SD-WAN controllers must tackle these issues. As an example, the CloudGenix SD-WAN controller doesn't assume good connectivity but instead constantly monitors the connections. If the controller gets disconnected from the rest of the WAN due to some extreme event, remote branch networks continue to operate. As long as the remote network still has connectivity to its transport connections (even if it doesn't have connectivity to the controller), users at the remote location won't experience any problems.

Some key differences between the data plane in a data center and the data plane in a WAN include the following:

- The centralized controller in the WAN is separated from the data plane, which is more distributed in a WAN than it is in a data center. This allows the

data plane at the remote locations of the WAN to enforce policies even if the WAN controller isn't accessible.

- An organization owns and manages the data plane in the data center, and it has consistent, tightly controlled characteristics. In contrast, a WAN has a variety of different transports that the organization doesn't own or control, and these different transports have very different characteristics.

The control plane is a collection of multiple protocols that administrators must deploy and configure. A WAN and a data center use different protocols. More, there are some key differences in these protocols:

- Within a data center, an organization fully manages the protocols. However, service providers manage these protocols in a WAN. The interdependencies between different protocols add another level of complexity, making them more difficult to manage.
- Protocols in a data center are relatively fast, constant, and predictable. In contrast, protocols in a WAN travel across great distances, resulting in huge latencies and various quality over the transport paths. The control plane within a data center uses metrics within link state and distance vector protocols, but these protocols are not ideal for determining the best path for application performance across a WAN.

While the control plane architecture used within the SDDC meets the needs of data centers, it doesn't meet the needs of SD-WANs. Instead, the ideal SD-WAN

control plane architecture needs to have the following characteristics above and beyond the SDDC control plane:

- The SD-WAN must be able to de-couple from provider protocols, allowing it to reduce the amount of protocol state data exchanged between the data plane endpoints. Ultimately, this allows the SD-WAN solution to remove routing protocols within the remote locations. SD-WAN solutions can instead replace these routing protocols with simpler and robust Application Programming Interfaces (APIs).
- Instead of traditional link state and distance vector protocol metrics, the SD-WAN solution supports new metrics for transport paths. These new metrics consider application performance requirements. This includes transaction time requirements for transactional applications, coding/decoding (CODEC) requirements for media and unified communications applications, and more.
- While you can reasonably expect SDDCs to have constant connectivity, you can't expect this in SD-WANs. Any communication disruptions between the SD-WAN controller and data plane elements must not prevent traffic flow. The remote sites should still be able to enforce policies and forward traffic.

Chapter 2

Understanding Why You Need the SD-WAN

In This Chapter

- Working with hybrid network challenges
- Expanding the security perimeter
- Recognizing the emergence of the cloud
- Taking apps into consideration

As companies begin to implement and realize cost savings and organizational efficiencies, they have begun to rapidly implement virtualization. Similarly, IT directors and CIOs are learning about software-defined wide area networks (SD-WANs), so they're realizing the need to embrace this technology, too. This chapter outlines why many enterprises need an SD-WAN.

Hybrid Networking Challenges

Enterprises can use many transport methods: Multiprotocol Label Switching (MPLS), Internet, and

Long Term Evolution (LTE). Ideally, the WAN should be able to use all paths and dynamically choose the best path for users and applications for the best service level agreement (SLA). Enterprises used to only use MPLS, but now even if they bring in another transport method, they often use it only as a backup. The reason is it's extremely complicated with traditional WAN technology and routing protocols to use them together.

In contrast, SD-WANs can easily use multiple transport mechanisms. For example, the CloudGenix solution is transport agnostic and can use MPLS, 3G, 4G, LTE, broadband Internet, or any other transport mechanism. Additionally, all of these paths are active-active. *Active-active* means applications are load-balanced across all available paths. When a failure or slowdown occurs on a node, another node in the network takes its place. The system can dynamically choose the best path based on policies (which is fastest, cheapest, or so on) created by business managers.

SD-WAN solutions should be transport agnostic to ensure the enterprise isn't tied to any specific vendor and can adopt new transports as they become available. With SD-WANs, you can add multiple different transports into the mix. SD-WAN technologies enable you to manage them as a single fabric instead of separate and distinct networks. This allows you to realize the benefits of hybrid WAN's increased complexity. Those benefits include lower cost and higher application performance. As an example, the CloudGenix solution increases utilization of all available paths and provides price/performance gains between 10 and 100 times greater when compared to legacy WANs.

Expanding Security Perimeters

As traffic patterns and usage patterns have changed with more and more apps being delivered from cloud and Software as a Service (SaaS) providers in addition to traditional data centers, as well as being delivered across multiple public transport networks, your security perimeter is no longer just your data center's demilitarized zone (DMZ). In fact, it' your entire WAN surface area that's expanding and dynamic. Recent history has shown that exploits are increasingly focused on the WAN. Traditional networking and VPN topologies are static in nature, which makes them brittle, complex to manage, and slow to deploy. With SD-WAN technologies, because policies are delivered from a central controller via an Application Program Interface (API) to your entire WAN edge, security services such as encryption and app firewalling can be rapidly and reliably deployed to the entire WAN edge.

The Changing Nature of Applications

Historically, applications were client-server apps. Today, apps are much richer and more varied with a mix of collaborative, voice, video, and business transactions increasing over HTTP. Apps are being delivered from the cloud and SaaS providers. IT needs to simultaneously extend and manage secure connectivity and application performance for things that they don't directly own. Apps and app initiatives, such as

omni-channel, are increasingly leveraged to drive incremental revenue streams, upping the ante on app performance and availability.

Omni-channel retail applications detect the user's platform and automatically deliver the content in the best format. For example, content is delivered differently for smartphones, tablets, and desktop systems.

Each of these applications can have multiple substreams (for example, webex voice, video and share, and Virtual desktop infrastructure (VDI) with multiple individual channels) that have their own requirements in terms of SLAs. Couple this with the fact that people expect high-quality performance everywhere all the time, and it's important to be able to granularly identify the applications and directly measure the true end-user application experience. This includes coding/decoding (CODEC) conformance for media apps and application transaction time for transactional apps. SD-WAN enables you to replace traditional routing metrics with these business performance metrics as a basis for path selection.

While legacy hardware-based WANs can't adapt to these changing patterns, SD-WANs that use hybrid networking can, which enables them to increase mobility at the remote locations and easily and securely deliver new apps, including high-definition video, collaboration apps, and omni-channel applications.

Chapter 3

Recognizing Current Network Limitations

In This Chapter

- Reviewing legacy hardware-based WANs
- Choosing the best path
- Understanding technology and hardware limitations

Traditional hardware-based wide area networks (WANs) are often unable to meet the needs of remote offices. They're complex and rigid, which requires a significant amount of management and administration.

Understanding Legacy WANs

Legacy (hardware-based) WANs are extremely complex and brittle and require a significant amount of infrastructure to support remote offices. Some of the issues with them are

- **Reliance on traditional routing protocols:** A lot of protocols and protocol instances need to be configured and managed, including Multiprotocol

Label Switching (MPLS), interior Border Gateway Protocol (iBGP), open shortest path first (OSPF), next hop resolution protocol (NHRP), and the list goes on. Each of these protocols requires interaction and significant exchange of state between themselves and other Internetworked elements. Any change to topology or segmentation requires re-tuning at best or re-design at worst of your routing protocols. And many of these routing protocols interact with service provider routing protocols, which further adds complexity and reduces business responsiveness. Add to this the fact that the routing protocols were really designed to provide reliable connectivity at the network level as opposed to optimal performance at the application level.

- **Inability to easily gain visibility into cloud and SaaS apps:** You can't manage what you can't see. IT personnel need the ability to view performance metrics when troubleshooting. For example, if employees are experiencing problems with a cloud-based application such as Office365, IT personnel need the ability to view the different elements of the application. The problem could be due to an in-house networking fault, a connectivity issue with an Internet service provider, or a problem with Microsoft's cloud service. In a traditional network transport and cloud, services are outside of the network and therefore can't be monitored. You can purchase some tools on the market to try to bandage this issue, but they're incomplete and sometimes impossible to implement, adding complexity to an already brittle system. Tools provide the needed visibility of each these elements.

- **Rapidly securing the WAN:** The surface area of the WAN edge is growing and changing. The type and criticality of applications that are traversing the public Internet is changing as well. Traditional networking technologies aren't well suited to dynamically implementing new security posture based on changing topology or threat. They're also challenged in terms of the ability to differentiate and provide differentiated security services based on application type and context without deploying unwieldy and expensive hardware boxes to each branch.
- **Vendor and budget lock-in:** Legacy networks are generally built with one vendor's proprietary switches and routers. Every three to five years these need to undergo a refresh — meaning budget often in the hundreds of thousands of dollars needs to go toward this, including support and maintenance costs.

  Many organizations estimate they spend 70 to 80 percent of their IT budget just keeping the lights on. But when you reduce IT maintenance and support spend, you can repurpose the funds for transformation or innovation initiatives that will advance the business rather than merely keeping it functioning.
- **Difficulty reporting on how IT is supporting business:** Historically, IT organizations have been measured based on cost control as well as network connectivity SLAs. (Carrier class 99.999 percent used to be the Holy Grail.) Cost control and network connectivity are now taken for granted. IT organizations are increasingly being measured on their ability to deliver against application

performance SLAs that are rapidly enabled to and actually *enhance* new business initiatives. Traditional WAN networking tools don't even have the concept of what an application is because they think in terms of packets instead of apps, so it's difficult, if not impossible, to meet this.

- **No verifiable model for security and compliance:** Legacy WANs have multiple hardware elements that are difficult to monitor continuously. Administrators configure them with specific settings for security and compliance, but time-consuming audits are required to ensure these configurations haven't been modified.

Finding the Best Path

While the shortest path between two points is a straight line, it's not necessarily the best path for traffic. Or the quickest. Imagine Rebecca wants to drive from Pasadena to San Diego. She could look at a map and pick the direct path thinking it will also be the quickest. Unfortunately, the direct path could be slow due to construction or vehicle accidents.

What if Rebecca's car had access to a central control center? It would act as a central brain with a rich understanding of traffic conditions and could modify the recommended path in real time. If Rebecca followed the modified path, she would arrive in San Diego quicker than she would have if she just used the direct path.

Compare this to a hybrid WAN with multiple transport mechanisms such as Multiprotocol Label Switching (MPLS), broadband Internet, 3G/4G, and Long Term

Evolution (LTE). Ideally, you would be able to configure the WAN to use all these protocols and identify the best path by using the appropriate protocol. Unfortunately, this process is extremely complex in legacy WANs. Instead, legacy WANs typically use one active transport path and one or more backup paths. Enterprises pay for transport paths that they rarely use or underutilize because they have no way to adjust in real time.

Most software-defined WAN (SD-WAN) solutions can utilize all of the transport paths as an active/active model. Further, they can evaluate multiple variables and choose the best path for any type of traffic in real time.

Looking at Technology and Hardware Limitations

Ideally, IT goals and business goals would always be in harmony. Unfortunately, this is often not the case. The truth is that IT at the speed of the business is a myth when using legacy WANs even with the advances in cloud services and other technologies. However, it's not the fault of IT personnel. Often, technology and hardware limitations along with security concerns prevent them from fully meeting business needs, at least within the timeframe that the business wants them.

Some of the reasons why IT often can't meet business needs in a timely manner include the following:

- Change and configuration management processes slow them down
- Significant lag time between the initial concept and arrival of necessary hardware

- Manual processes, requiring personnel to touch the hardware
- The inability to "see" and react to what they're being held accountable to deliver, which are apps that meet performance SLAs

Chapter 4

Looking at the Changes that Make Software-Defined WANs Possible

In This Chapter

- De-coupling hardware from software
- Reducing costs by managing SLAs

Software-defined wide area networks (SD-WANs) haven't always been possible. Some important changes that make them possible today include virtualization and the exponential growth in processing power, increase in reliable transport options, and the implementation of IT governance methods to ensure IT goals match business goals.

Doubling with Moore's Law

In 1965, Gordon E. Moore, co-founder of the Intel Corporation, was asked to predict the future of semiconductor components. He predicted that the number of components on integrated circuits would double

every year for at least the next ten years. He was correct. In 1975, he modified his prediction, saying that this doubling will likely only occur every two years, and experts in the field dubbed this "Moore's Law." Later, Intel executive David House noted that CPUs were getting faster along with having twice as many transistors. He predicted chip performance to double every 18 months.

While only a prediction, many people consider Moore's Law a self-fulfilling prophecy. It has been accurate for so long that chip manufacturers use it as a guide. They expect their competitors to meet the prediction, so they set their manufacturing goals to do so too. The impact of Moore's Law is faster processors that run on smaller computer chips. These advances have also enabled the explosion of virtualization on x86-based systems and their ability to host virtual networks.

Originally, x86-based systems were used mainly for general-purpose software. Applications needing speed and scale required creation of an application-specific integrated circuit (ASIC), but these ASICs were expensive and inflexible. Significant fixes or feature improvements often required complete replacement of the system or ASIC itself. With the benefit of Moore's Law, over several years x86-based systems became able to easily replace and surpass ASIC systems in many cases.

A myth that some networking professionals sometimes repeat is that software routing simply isn't adequate for a current network. Instead, they stress that the only way to meet network requirements is with application-specific integrated circuit (ASIC) routers. This blanket statement isn't true for many networks, and is especially not true for WANs.

It is true that a well-designed ASIC system can route packets faster than a commercial off-the-shelf (COTS) x86-based system running software-defined networking (SDN) software. However, that doesn't mean that x86-based systems aren't adequate, especially when talking about SD-WANs. When comparing an x86-based solution against an ASIC solution, it's important to ask a simple question: How fast is fast enough for any given application?

A highly connected network within a data center might enjoy speeds in the multiple hundreds of Gbps per second. An x86-based system may have trouble keeping up with these speeds, so ASIC-based routers are typically more appropriate within the data center, but typical business WAN speeds are much slower. T-1 lines only provide 1.544 Mbps. If an organization can afford T-3 lines, it can get speeds as high as 45 Mbps, but T-3 lines are cost-prohibitive for most organizations.

Even consumer Internet speeds are much slower. Digital subscriber line (DSL) speeds top out at about 3 Mbps. Cable and cellular 4G speeds top out at about 100 Mbps for downloads. Even high-end fiber systems typically only provide 1Gbps bandwidth to the end-user.

All of these speeds are much slower than the multiple hundreds of Gbps/sec speeds in data center networks. In WAN networks, an x86-based solution can easily match the performance of ASIC solutions.

Current x86-based systems are not only powerful enough to encrypt and deliver data at WAN speeds, but also they're powerful enough to provide centralized control for SD-WANs.

Virtualization on COTS x86-based systems is a key reason why SD-WANs are now possible.

Managing for Business SLAs

When enterprises have IT governance processes in place, they're more successful at aligning business and IT goals. One IT governance control is service level agreement (SLA) management. With the explosion of the cloud and cloud services, enterprises often outsource many services, and SLAs help ensure they're receiving the services they purchase.

Consider the SD-WAN with a hybrid network. It has multiple transport paths, and enterprises pay for bandwidth on each path. If the enterprise exceeds bandwidth usage, it has to pay more. If it only uses 10 percent of purchased bandwidth, it doesn't get a refund. One way to reduce costs is to ensure you purchase the bandwidth you need, but no more.

Typically, enterprises use 60 to 65 percent of their available bandwidth. With the SD-WAN, they can increase that to 95 percent, which saves them tens, if not hundreds, of thousands of dollars. While that sounds simple enough, it has been difficult for enterprises to monitor transport paths, but it's possible to measure transport paths today, and many SD-WAN solutions include built-in tools to monitor their performance.

Chapter 5

Recognizing Software-Defined WAN Benefits

In This Chapter

- Looking at replacing your hardware
- Gaining centralized control with software
- Saving money with accelerated rollout times

The Open Networking User Group voted software-defined wide area networks (SD-WANs) as the top use case for software-defined networking (SDN) two years in a row. They did so for many reasons, including reduced capital expenses (CAPEX), reduced operational expenses (OPEX), increased security, higher scalability, and overall better service quality. This chapter digs a little deeper into how SD-WANs bring these benefits.

Replacing Hardware with Software

At the top of the list of benefits from the SD-WAN is that it enables an organization to focus on what the business

values — applications. Instead of just worrying about the physical network and connectivity, organizations put applications first. SD-WANs make it possible to build an application network.

This new concept — the application-driven network — delivers multiple related applications and services over a WAN, which allows administrators for the first time to tie applications, users, policies, and security together across the network.

The ability to replace networking hardware with software is another benefit. Replacing the hardware with software reduces costs. For example, you no longer need to purchase new branch-location routers using a standard three- to five-year refresh cycle. This reduces CAPEX. And, without routers at remote locations, you don't need technicians there to administer and maintain them. This reduces OPEX. With SD-WANs, organizations can redirect much of these expenses to advance the business instead of just keeping it functioning with another refresh cycle.

With the CloudGenix SD-WAN solution, you no longer need physical routers to direct traffic on your WAN. It can handle all the routing needs of remote offices without the networking hardware. That might sound scary to all of the administrators that spent the last ten years of their IT careers honing their skills with ACLs and routing tables, but it's great news for administrators, the CFO, and the business.

Gaining Centralized Control

The SD-WAN provides centralized control of all enterprise-owned components. One of the primary benefits is the ability to monitor all service level agreement (SLA) transport paths. Centralized control provides a deep view of enterprise SD-WAN performance and allows managers to monitor all the transport paths. Managers can ensure the providers are meeting SLA requirements and that they're using the bandwidth they've purchased. If they notice that a path is over-provisioned, they can save costs by reducing the purchased bandwidth.

Another benefit is the ability to manage all of the SD-WAN policies from a central location. Business managers create the policies once and publish throughout the organization instantaneously.

By using SD-WAN solutions, such as one from CloudGenix, business managers can create policies using plain business language. This allows them to identify allowed transport paths for specific users, applications, and SLA customers. Additionally, CloudGenix uses Cloud Fast, a proprietary technology. It identifies the best path traffic should take based on several variables and helps increase WAN utilization.

Centralized control also supports strong security by creating a dynamic security perimeter that implements enterprise-level security at the branch locations. Because the security perimeter is implemented with software, it allows managers to verify compliance with security requirements at any time.

Decreasing Rollout Times

One of the biggest challenges with IT solutions is the long deployment times. It's not unusual to take six months or longer to deploy many new hardware solutions. Software solutions significantly reduce deployment times. This allows managers to focus on business initiatives and goals.

As an example, imagine your enterprise has the SD-WAN implemented for branch locations and then decides to roll out a new omni-channel application. The challenge is ensuring that the application will use different transport paths when employees use it with different devices, such as smartphones, tablets, or desktop computers. If you use a legacy WAN, this process would be lengthy, involving in-depth research from technicians and administrators. It might even require the purchase of additional hardware. However, by using the SD-WAN solution, managers can deploy it in minutes. It often only requires a simple point-and-click action.

Chapter 6

Ten Considerations When Deploying a Software-Defined WAN Solution

In This Chapter

- Recognizing qualities of robust SD-WANs
- Identifying questions to ask SD-WAN vendors

If you've read this book from the beginning, you've discovered many changes that make software-defined wide area networks (SD-WANs) possible today, along with many of the differences between software-defined networking (SDN) and SD-WANs. When evaluating any SD-WAN solution, consider these benefits:

- **Ease of Management:** Implementing SD-WAN solutions should make it easier to manage the network and reduce the workload. Clearly, WANs support the business, but traditional WANs require intense administrative workload.
- **Application-driven network:** SD-WAN solutions should be application-driven, instead of

application-aware. They should also allow administrators to create policies for specific users, applications, and service level agreement (SLA) customers.

- **Plain intuitive business language:** SD-WAN solutions should allow administrators and managers to use plain business language to create policies. One of the great benefits of a software-defined solution is that software developers can simplify the interface. This isn't to say the solution is simple — far from it. However, the software handles the complexity and presents network admins with an easy-to-use interface.
- **No routing protocols:** SD-WAN solutions should be able to eliminate routing protocols used on the internal network. They should also be transport- and carrier-agnostic. One of the great strengths of a robust SD-WAN solution is that it can use any transport mechanism, such as Multiprotocol Label Switching (MPLS), 3G, 4G, Long Term Evolution (LTE), or a traditional VPN. This helps ensure it isn't tied to any specific vendor and that you're ready for the next big thing, such as 5G or another transport technology that some Silicon Valley genius is thinking up right now.
- **Ability to use COTS (x86) hardware:** SD-WAN solutions should be able to run using commercial off-the-shelf (COTS) hardware. The last thing you want to do is tie yourself by a single vendor for your hardware to using a software-defined solution. COTS hardware is cheaper than proprietary hardware, and software-defined solutions can program the solution to do more than a proprietary Application Specific Integrated Circuit (ASIC).

- **Intelligent Automated Path Selection:** SD-WAN solutions should enable the hybrid WANs. Legacy WANs typically only support a single active connection with one or more backup connections in an active/backup configuration. True hybrid WANs support multiple active connections that they can use simultaneously based on application attributes defined in business policies, rather than being defined in rules that analyze packets. This also allows the solution to evaluate transport availability and performance metrics, and choose the best WAN path for users, applications, and/or SLA customers.
- **High-performance data plane:** Remote networks should remain operational even if they lose connectivity to the SD-WAN controller. Remote locations shouldn't depend on the SD-WAN controller for operation.

The CloudGenix SD-WAN solution locates the controller in the cloud, and remote locations connect to it via the Internet. If a remote location loses connectivity to the controller, it remains operational. Even if the controller lost connectivity due to a disaster, remote locations continue to operate normally for extended periods.

- **Ability to have a dynamic security perimeter:** SD-WAN solutions should provide a high level of security and create a dynamic security perimeter reaching to the remote sites. Additionally, they should reduce attack vectors by reducing the number of open ports. Because data traverses public networks, they should also support strong encryption mechanisms.

- **Dynamic tools to monitor SD-WAN:** The SD-WAN solution includes tools to give personnel a rich view of the SD-WAN components. For example, the CloudGenix solution provides a dashboard to monitor latency and reliability of transport mechanisms and applications. This provides IT personnel the ability to monitor and report on the performance of applications, the network, and WAN utilization. Personnel can view performance in real-time, which helps them identify trends.
- **Variable bandwidth and latency:** SD-WAN solutions should be able to handle variable bandwidth and latency. A robust SD-WAN solution doesn't assume good connectivity, but instead it continuously monitors all available paths, adjusts to changes in bandwidth and latency times, and directs traffic based on previously defined policies. This strategy with the right vendor can safely increase WAN utilization from typical levels of 60 to 65 percent to 95 percent.

Understand why you need a software-defined WAN

There's a revolution afoot in networking known as software-defined WAN (SD-WAN). New technology can be daunting, but once you realize cost savings and organizational efficiencies, the tide will quickly turn. Software-defined wide area networks (SD-WANs) are a part of new technology to embrace now.

- ***Understand why you might need a software-defined WAN* — enable hybrid networking and let applications drive your network**
- ***Enjoy the benefits and expected ROI of a software-defined WAN* — see the advantages of software, central control, and cost and efficiency savings**
- ***Discover ten considerations when deploying a software-defined WAN* — ensure you're getting the best solution for your needs**

Open the book and find:

- **Ways to manage application SLAs to reduce costs**
- **Qualities of robust software-defined WANs**
- **Questions to ask software-defined WAN vendors**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-09854-6
Not for resale