WHITEPAPER

THE RIGHT APPROACH TO SECURING TODAY'S WAN

Why Software-Defined WAN Should Have Integrated Security Features

888-435-7986 | www.getgds.com

GLOBAL®
DATA SYSTEMS

INTRODUCTION

> End-users need an always-on, high-performance network that enables access to centralized applications, cloud services and remote data centers.

The only foolproof way to secure computer systems is to disconnect them from the network. That's obviously not feasible in today's hyper-connected business environment. End-users need an always-on, high-performance network that enables access to centralized applications, cloud services and remote data centers.

SD-WAN Reduced Telecom Costs

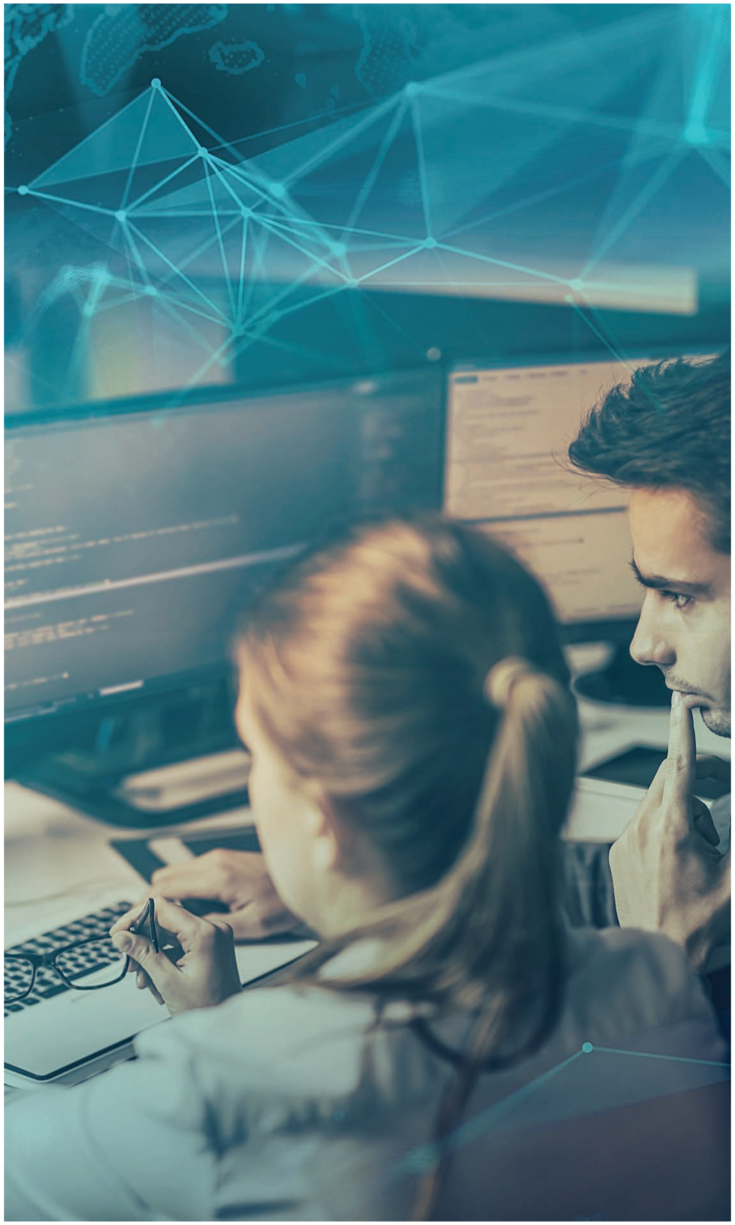
Organizations traditionally have provided that access through a highly secure Internet connection in the primary data center. Remote sites would connect to headquarters via dedicated carrier circuits or multiprotocol label switching (MPLS) services, and Internet traffic would be backhauled over these links. **As the volume of Internet traffic has skyrocketed, however, these legacy WAN architectures have become too costly and difficult to manage.**

Software-defined WAN (SD-WAN) has emerged as a means of reducing telecom costs, simplifying branch office connectivity and centralizing WAN management. An intelligent controller enables organizations to leverage cost-efficient broadband Internet services instead of legacy telco solutions while minimizing downtime and performance problems.

However, **connecting branch locations directly to the Internet brings significant security risks.** Organizations are faced with implementing multiple security tools at each branch to protect users and IT assets from Internet-borne risks. However, **many organizations already find it difficult to manage and maintain all of the security tools they have in place.** Adding more security point products only adds to this burden.

What You'll Learn

A better approach is to select an SD-WAN solution with integrated security capabilities. This whitepaper will explain the benefits of the integrated approach and what to look for when evaluating SD-WAN products.



A Closer Look at SD-WAN

SD-WAN solutions apply the principles of software-defined networking (SDN) to the network edge, bringing new levels of functionality to the WAN. Organizations can create a hybrid network that blends transport types such as broadband, 4G/LTE wireless and MPLS.

Traffic routing is automated by a central controller, making it possible to dynamically mix and match these connectivity options to maximize availability, optimize performance and control costs.

This would be virtually impossible using traditional WAN hardware. The configurations required to differentiate and segment traffic are complex and updated manually on each device in every remote location. That's why enterprise IT teams have tended to prefer MPLS for branch connectivity — it provides high levels of reliability and Quality of Service (QoS) without a lot of management overhead.

Benefits of SD-WAN

With SD-WAN, organizations can achieve these objectives while reducing reliance on costly MPLS services. SD-WAN solutions monitor WAN connectivity and automatically fail over to a backup broadband connection for maximum uptime. Adding 4G/LTE service protects against physical disruption of wired circuits and provides cost-efficient bandwidth for extremely remote locations.

Best-in-class SD-WAN solutions employ network traffic shaping with Layer 7 application visibility to prioritize mission-critical applications, users and groups. This ensures QoS for voice calls, videoconferencing and other interactive applications, even over broadband Internet links. Routing decisions are based upon defined policies and the current state of the network, providing the flexibility to adapt to changing conditions.

A More Agile WAN Solution

SD-WAN also creates a more agile WAN. Broadband Internet services can be provisioned quickly, while traditional telco services require 120 days or more to turn up. Many SD-WAN solutions offer zero-touch provisioning of on-premises appliances and simplified monitoring and management through a single interface.

Gartner's Definition of SD-WAN

According to Gartner, an SD-WAN solution must have these four characteristics:

- Support for multiple connection types
- Dynamic path selection and load sharing across connections
- Easy setup and simplified management and web gateways
- Support for third-party services such as VPNs, firewalls and web gateways

Understanding WAN Security

Inherently Secure

MPLS is inherently secure. The service provider carves out a separate data stream through the network core for each customer, creating a virtual private line. While it's theoretically possible for a hacker to infiltrate the network, the risk is negligible as long as the network is configured properly.

The public Internet, in contrast, is an insecure channel for exchanging data. Sensitive information can be intercepted, and malware and other threats can be delivered to vulnerable systems. At minimum, organizations must place a firewall between the LAN and the public Internet.

In the traditional WAN, security tools are deployed in the data center to protect the organization as a whole. Branch locations don't connect to the Internet directly — they gain Internet access via MPLS connections to the primary data center. With this hub-and-spoke architecture, IT doesn't have to worry much about WAN security at the branch.

WAN Can Be Costly

This design comes with high costs and performance bottlenecks, however, **leading more and more organizations to implement SD-WAN solutions**. Branch locations are now connecting directly to the Internet, which means that WAN security is now a major concern.

Unfortunately, very few SD-WAN products were designed with security in mind. When SD-WAN solutions don't have integrated security, organizations must deploy a third-party firewall or secure web gateway to protect the branch WAN, and ideally implement intrusion prevention, malware protection, content filtering and IP-SEC VPN tunneling. This increases costs, complexity and IT operational headaches.

THE SECURITY MANAGEMENT CHALLENGE

> Many organizations — particularly small to midsize businesses (SMBs) — are struggling to manage and maintain a growing array of network security tools.

Challenges for IT Staff

In a recent Spiceworks survey of IT decision-makers in businesses with 11 to 500 employees, respondents said they have implemented an average of seven network security tools, and nearly 80 percent said they manage these tools in-house.

However, these IT professionals are also responsible for ensuring the reliability and availability of three WANs on average as well as wired and wireless LANs, which means a large number of administrative tasks must be performed on a regular basis. That helps explain why 82 percent of survey respondents reported experiencing at least one type of network security threat in the past year despite having multiple layers of protections in place. It isn't only an SMB problem. Many enterprises have taken a best-of-breed approach to cybersecurity, implementing a fleet of point solutions to address specific threats. According to the 2018 State of Security Budgeting report, based upon a study conducted by research firm Vanson Bourne, 66 percent of respondents said they are having a hard time finding IT staff who are capable of managing these security products. This skills gap creates significant challenges for organizations with multiple remote sites.

80% say

THEY MANAGE SECURITY TOOLS IN-HOUSE

66% say

THEY HAVE A HARD TIME FINDING SKILLED IT STAFF

In a recent research note, Gartner recommended that organizations use cloud-based Security-as-a-Service solutions to relieve some of the complexities and management headaches associated with securing direct Internet connections in remote locations. A fully managed SD-WAN solution with integrated security offers an even better approach.

> **The SD-WAN market is growing quickly thanks to demand for more flexible and cost-efficient WAN architectures.**

According to IDC, SD-WAN sales grew from just $225 million in 2015 to $1.2 billion in 2017. The SD-WAN market is expected to see a 69 percent compound annual growth rate through 2021.

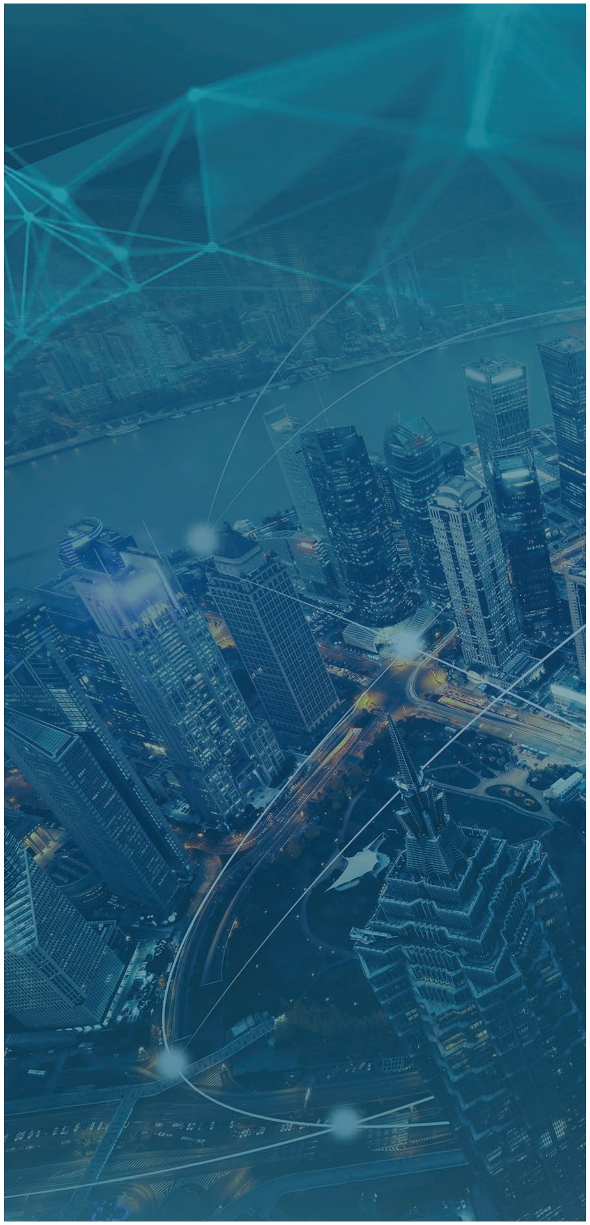
Many vendors have jumped onto the SD-WAN bandwagon, including manufacturers of traditional networking equipment and "pure play" SD-WAN providers. Only a handful of vendors have more than 10 percent market share, meaning that competition is fierce.

Intergrated Security is Key

Integrated security should be on the "must-have" feature list for organizations evaluating SD-WAN. Security functionality should include:

- **Stateful firewall:** The firewall protects the local Internet connection from external attack. Stateful packet filtering keeps track of all active connections and examines data packets as they attempt to enter the network. Potentially malicious traffic is blocked.
- **Intrusion prevention.** An intrusion prevention system (IPS) monitors the network for potentially malicious activity and security policy violations. The IPS blocks the malicious data packets and source address and sends an alert to network administrators.
- **Malware protection:** Antimalware solutions detect and block malware in real time. State-of-the-art solutions leverage threat intelligence and include sandboxing capabilities to identify emerging threats, and continuously monitor activity even after a file has been allowed to enter the network.
- **Content filtering:** Content filtering controls which websites users can access. This not only protects against malicious content but enforces acceptable use and security policies.
- **IP-SEC VPN tunneling:** A VPN tunnel uses robust, end-to-end encryption to protect data traveling over the Internet. In addition to preventing a data breach, VPN tunneling helps organizations meet regulatory requirements.

Ideally, these security tools and the WAN itself should be monitored around the clock and fully managed by the SD-WAN provider. The provider should employ security experts who follow industry best practices to ensure that upgrades, configuration changes and other maintenance tasks are performed in a timely manner. In addition to improving security, these services allow the customer's in-house IT team to focus on core business functions rather than monitoring and managing the WAN.



CONCLUSION

While SD-WAN enables organizations to use low-cost broadband Internet services instead of MPLS, it exposes branch locations and remote workers to Internet-borne threats. Organizations must deploy an array of security tools to protect sensitive systems and data.

Because it's difficult to manage multiple security appliances across branch locations, SD-WAN should incorporate strong security.

Integrating firewall functionality, intrusion prevention, malware protection, content filtering and IP-SEC VPN capabilities into SD-WAN helps to reduce risk without increasing operational complexity.

Best-in-class SD-WAN solutions are monitored and fully managed by the service provider to ensure robust protection.

GLOBAL DATA SYSTEMS

GDS can help you deploy SD-WAN Solutions

Contact Global Data Systems: 888-435-7986