FORTINET

It's Time to Leave Branch Routers Behind

4 Big Advantages of Secure SD-WAN

More and more organizations are turning away from branch routers in favor of Secure SD-WAN to become cloud-ready and improve the user experience. Not only are Secure SD-WAN solutions simple to manage but they also simplify WAN operations overall.

Organizations should embrace Secure SD-WAN solutions to help branch users better leverage unified communications and collaboration, use critical SaaS applications, and easily access resources stored in the cloud. Here are four key advantages Secure SD-WAN offers over legacy branch routing architectures:

Secure SD-WAN solutions are easy to manage and simplify WAN operations overall.

1. Improved application agility

Routers operate based on packets. As a result, they are unable to provide deep visibility into applications. Because a majority of organizations have an investment in cloud applications and services, being unable to identify those business-critical applications and apply protocols to support their unique bandwidth and connectivity needs can degrade the user experience.

SD-WAN solutions can do anything a traditional router can do, such as provide advanced routing and WAN connectivity. Beyond traditional routing functions, however, SD-WAN solutions

- Identify and steer applications using dynamic path selection for consistent quality of experience
- Can identify applications and create SLAs for thousands of applications such as O365, Salesforce.com, and unified communications
- Have the ability to update business applications on a daily basis to ensure applications are identified accurately and taking the most desired path

2. Easy to scale, with considerable capex and opex savings

MPLS connection speeds and volumes are predetermined and expensive, which means that a sudden spike in traffic—such as multiple high-speed unified communications connections, or the need to process a large amount of data—can affect everyone. Adding new branch router sites is also a costly, time-consuming process.

SD-WAN solutions, however, can help customers migrate from MPLS to broadband (DSL, 4G/5G, Ethernet) and realize 40% savings in opex in many cases. SD-WAN enables organizations to dynamically and securely scale to tens of thousands of branches, seamlessly interoperate with existing physical and cloud infrastructures, and provide remote troubleshooting to eliminate costly physical interventions by skilled technicians. Secure SD-WAN also consolidates a range of point products—including routers, firewalls, and WAN optimization tools—into a single product, resulting in significant capex savings.

3. Simplified management and orchestration

Branch routers are often complex to install, upgrade, and maintain—even when they are supposed to be a "low-touch" solution. Configuration requires expertise with a router's command line interface (CLI), and because of its complexity, it can rarely be performed by anyone onsite at a branch location.

Centralized Secure SD-WAN management ensures that new services and policies are application-focused and that connectivity and security configurations and policy changes can be seamlessly propagated throughout the extended WAN—eliminating the need to configure or manage each device or service individually. Centralized Secure SD-WAN also provides rich analytics showing historic and real-time application performance, allowing teams to quickly troubleshoot and improve key performance metrics such as average time to respond.

4. Integrated security and networking

Branch routers are not fully integrated security and networking solutions by any means. When MPLS is supplemented with split tunneling to allow direct access to the internet, branch routers provide little to no management of links or connections. Even when traffic fails over or is moved to an alternative path, they lack the sub-second proactive steering required to avoid dropped connections, and don't have the ability to mitigate transport issues or provide things like dynamic jitter buffering. They are also unable to actively regulate traffic before congestion becomes an issue. Worse, because routers lack effective security, these non-MPLS connections expose your organization to additional risk.

But it's important to note that most SD-WAN solutions aren't without security challenges—indeed, one of the critical requirements for SD-WAN success is fully integrated security. Next-generation firewalls (NGFWs), whose key components include IPS, web filtering, SSL inspection, and anti-malware, are an example of an integrated solution. Without fully integrated security, SD-WAN becomes just another conduit for malware and cyber criminals to attack your network.

A true platform needs tools explicitly designed to interoperate as a single system, ideally with each element running on the same operating system and managed using a single-pane-of-glass interface. This ensures that transactions are all seen and inspected, and any threats or anomalous behaviors are shared between every solution for maximum protection. As part of such an integrated system, the networking and connectivity functionalities of an SD-WAN aren't just more closely associated with the security solutions installed on the platform. They're the same thing.

Next-stage considerations

It is essential not only to recognize the need to transition away from a traditional router-based WAN strategy but also to carefully select a Secure SD-WAN solution designed to provide the full spectrum of functionality and the broadest possible number of use cases. This helps ensure that your new SD-WAN deployment not only meets the needs of your organization today but that it can also adapt to your rapidly evolving requirements.

axient
Contact Us
sales@axient.com.au

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

June 1, 2020 4:06 PM

692249-0-0-EN

Macintosh HD:Users:bhoullhan:Documents:_Projects:Flyer:flyer - SD-WAN branch routers:flyer-SD-WAN-branch-routers