POINT OF VIEW

Converge Networking and Security for a More Dependable SD-Branch

Executive Summary

There is a long history of building networks and adding security as an afterthought. This was no different for branch offices, mainly because, traditionally, all traffic went back to a central location for security inspection. Dedicated network lines (typically MPLS) connected branches to headquarters, and there was little perceived need to worry about security within the branch.

With the move to SD-WAN, branches are now directly connected to the internet, bringing security to the forefront. The remote nature of branches makes security inherently challenging. Often there is reduced visibility and direct knowledge about what is happening on the branch network and who and what devices are connecting to it.

From branch employees to IoT devices, cybercriminals have plenty of targets. But branches often have little to no dedicated on-site IT staff who can investigate when something suspicious occurs. As threats continue to evolve and target the lowest-hanging fruit, weakly secured branches can easily enter the larger corporate system. Branch security needs to be a priority, as branch locations are now far more vulnerable than they were in the past.

Many SD-Branch solutions focus on consolidation and ease of management (both important characteristics), but the dependability of a branch's network is directly related to its security. This means reliable security must be a top consideration of SD-Branch deployments.

WAN Security and Performance

The rise of SD-WAN has completely changed how branch traffic is routed. With SD-WAN, traffic no longer travels back to headquarters for security. Instead, to give the best quality of experience (QoE), traffic will often be routed to the internet directly at the branch. Therefore, SD-Branch solutions must inspect all traffic entering and exiting the branch, particularly those involving internet sources. To make matters worse, with the move to secure web-based Software-as-a-Service (SaaS) solutions, more and more traffic is encrypted. Not only does this traffic need to be inspected, but it also requires decryption beforehand then re-encryption. All this needs to occur without impacting the QoE that SD-WAN has been installed for. Without fast and secure analysis of all traffic (encrypted or decrypted), performance will suffer, either from the need to route packets back to HQ for inspection or slow decryption/inspection.

LAN Risks and Requirements

While the internet presents one class of risk to a branch, the LAN, where users and guests connect presents another. Bad actors try to access branch resources and launch greater attacks on the larger network via the LAN. The larger the number of branches (and fewer IT staff to cover them), the more important it becomes to have reliable, consistent, and pervasive security at the branch. LAN security must be tied into overall network security to ensure that the network continues operating at peak efficiency.

Breach locations and attack methods are unpredictable, so policies and settings across deployments need to be automated and enforced as close to the access point. Branch security needs to consider that the organization’s users are a potential problem in addition to outside threats. They may unwittingly compromise their machines at the branch or while away, so the LAN must also be protected. SD-Branch security solutions need a tight coupling of all equipment at the branch.

Being constantly vigilant for indicators of compromise on user devices and directly quarantining threats where they enter the network are also necessary. Integrated branch security will keep the network safe from breaches entering through endpoint devices, ensuring operations continue smoothly regardless of attack attempts.

IoT Device Challenges

The rising use of IoT devices within branches to drive important business outcomes has created a new issue that SD-Branch solutions must address. These devices are often highly vulnerable, lacking the security measures that higher-end client devices are capable of. Special care needs to be taken to secure IoT devices so they are not leveraged to launch an attack. The volume of IoT devices and the varied solution sets they look to address adds an additional level of challenge, as IT staff rarely directly interacts with every device being brought online in any branch.

Flexible and automated branch security is needed to remove IT from the critical deployment path for these technologies. Solutions that require manual intervention slow down business initiatives at the branch and impact overall performance. Instead, SD-Branch equipment must be able to onboard these devices securely, allowing operations to continue without unduly exposing the network.

For Optimal Performance, SD-Branch Must Converge Around Security

Above all else, SD-Branch solutions are deployed to improve overall performance at the branch. While manageability may account for the more obvious ROI benefits of SD-Branch, without security, branch operations can slow or even grind to a halt due to bad actors. A reliable SD-Branch solution needs to offer security, not as a mere add-on, but truly integrated into all equipment to best address all aspects of branch dependability. By leveraging security at the heart of SD-Branch, the WAN, LAN, and device edge are all kept to optimal performance. Converging SD-Branch components with security enables a common framework for all branch network components, driving the best ROI.

www.fortinet.com

March 13, 2024 2:43 PM

940960-A-0-EN