AT&T Secure Web Gateway

For protection of SD-WAN deployments

The challenge

Many organizations are implementing SD-WAN as part of their strategy to modernize their network, enhancing its performance and resiliency. Most often, businesses are connecting their branch offices directly to the internet using commodity network links and then using SD-WAN to manage the data flows while preserving their MPLS (Multiprotocol Label Switching) lines for high-priority traffic between branch locations and the data center.

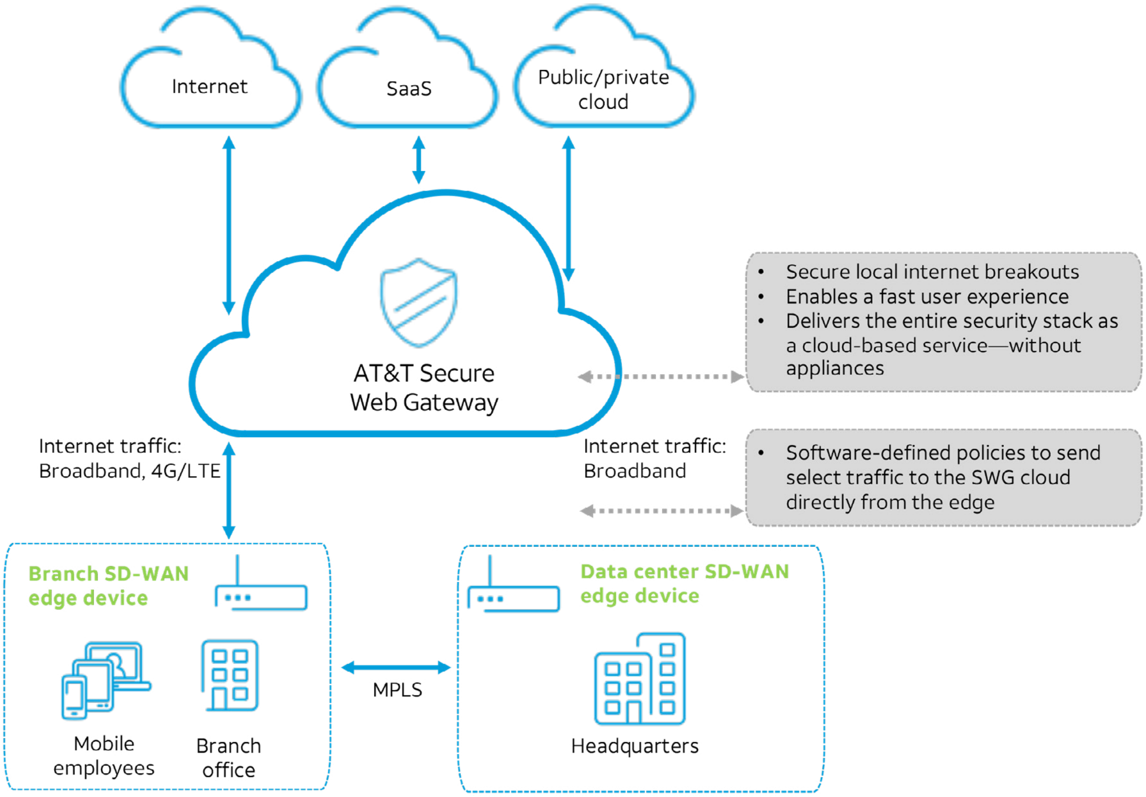
However, connecting branch offices to the internet exposes them to all of the web-based threats that had previously been defended only at their data center. One study from Enterprise Management Associates showed that enterprises with completed SD-WAN implementations were 1.3x more likely to experience a branch office security breach than those without one.[1] Why?

As mentioned above, connecting these branch offices to the Internet adds additional gateways in and out of the network that can be exploited. In addition, it is likely that many of these organizations falling victim to breach are relying solely on the security features native to their SD-WAN device, which in most cases will not be sufficient to protect branch offices against all modern attacks. Most SD-WAN devices will have highly secure tunneling and even stateful firewall functions (to monitor the full state of active network connections), but lack next-generation firewall capabilities, intrusion prevention, and data loss prevention (DLP). These are weak points that need to be shored up.

[1] Shamus McGillicuddy, Research Director, Enterprise Management Associates

The AT&T solution

AT&T Secure Web Gateway provides organizations with a way to apply unified policies across all of their users, virtually anywhere they are conducting business. With this solution administrators have the ability to extend the security and acceptable-use policies that had been enforced at their data center to all of their branch office locations. This will help protect users against web-based threats, and provide visibility and management of all locations through one pane of glass. Some editions of AT&T Secure Web Gateway offer additional functionality such as DLP or cloud access security broker (CASB) capabilities, which can offer more layers of protection without the need to purchase or manage dedicated appliances.


Internet
SaaS
Public/private cloud
AT&T Secure Web Gateway
Secure local internet breakouts
Enables a fast user experience
Delivers the entire security stack as a cloud-based service—without appliances
Internet traffic: Broadband, 4G/LTE
Internet traffic: Broadband
Software-defined policies to send select traffic to the SWG cloud directly from the edge
Branch SD-WAN edge device
Mobile employees
Branch office
MPLS
Data center SD-WAN edge device
Headquarters

Contact an AT&T account manager to get more information on how AT&T Secure Web Gateway can help protect SD-WAN deployments.

About AT&T Cybersecurity

AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our Software-as-a-Service (SaaS)-based solutions with advanced technologies (including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™), and our relationship with more than 40 best-of-breed vendors help accelerate your response to cybersecurity threats. Our experienced consultants and Security Operations Center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.