Combine Verizon Cloud Security with SD-WAN for Branch Office Internet Breakouts

Sending Internet bound traffic through private MPLS and SD-WAN links is unnecessary and results in latency and increased costs. Alleviate the load on private links by sending Internet bound traffic directly to the Internet through the Verizon Secure Cloud Gateway.

Using Verizon Secure Cloud Gateway with SD-WAN Overview

MPLS and SD-WAN are used to secure internal office-to-office communication. With cloud and SaaS changing the way applications are delivered from on-prem appliances to the cloud, the amount of Internet destined traffic is increasing by the day. Taking advantage of direct Internet breakouts for branch offices by sending Internet destined data directly to the Internet reduces the load on site-to-site links and in turn reduces costs and increases user experience. The Verizon Secure Cloud Gateway delivers Internet security in the cloud and secures traffic as it is routed directly to the Internet from branch locations. Combining Verizon Secure Cloud Gateway with MPLS and SD-WAN has substantial benefits:

- Firewalls and perimeter branch office equipment can be configured to only send internal traffic through private links while sending Internet traffic directly to Verizon Secure Cloud Gateway for compliance, malware defense and data loss prevention
- Reducing load on MPLS links and SD-WAN extends the useful life of existing branch office equipment as the majority of bandwidth increases are for traffic headed to the Internet which eliminates this burden on internal links and equipment
- SD-WAN can be used to push policies required to split traffic between internal traffic and Internet traffic destined to Verizon Secure Cloud Gateway
- Substantially reduce data back-hauling costs and increase speeds to cloud applications resulting in higher end user productivity
- The Verizon Secure Cloud Gateway's containerized design can easily be leveraged for horizontal scaling for massive tunnel capacity from branch offices to the cloud
- The Verizon Secure Cloud Gateway is designed for the mobile world with user experience and security being the same in the office or on the road
- The Verizon Secure Cloud Gateway is designed for Office 365, which requires fast and efficient connections with sufficient bandwidth

Typical Challenges Related to Cloud Adoption and Increasing Bandwidth

Migrating applications to the cloud and moving to a SaaS based delivery model can reduce management overhead and costs. An organization's strategy may also involve moving to a cloud first delivery model for all applications which reduces infrastructure management and eliminates data center footprints. With this cloud migration, however, various challenges emerge:

- The amount of bandwidth consumption for users increases exponentially as cloud application use surges
- Traditional models involving hairpinning traffic through centrally hosted gateway proxies for security increase strain on site to site bandwidth adding substantial costs to the IT budget
- The number of security appliances needed to secure bandwidth increases substantially resulting in high IT overhead and high infrastructure costs
- Meanwhile, the need to send some data between offices and data centers might still exist for internal resources

MPLS and SD-WAN provide solutions to connect offices together securely through private links. Additionally, branch office perimeter equipment has the ability to route traffic from branch offices directly to the Internet when accessing cloud applications. Before the traffic is routed to the Internet, the need to scan data for compliance, malware defense and data loss prevention is required to ensure safe access to the public Internet.

The Verizon Secure Cloud Gateway runs in the cloud so that Internet bound traffic from users at branch offices is secured from Internet threats even as it is routed directly to the cloud from the branch office. Immediately realize value by mitigating bandwidth increases through private links, eliminating the need to overhaul network design due to increased bandwidth loads, and increased productivity from end-users accessing cloud applications with speed and efficiency. The Verizon Secure Cloud Gateway runs in the cloud ensuring a direct connection between branch offices and cloud applications for fast and efficient Internet connections.

Verizon Secure Cloud Gateway paired with SD-WAN

Apply Compliance, Malware Defense and Data Loss Prevention to Internet Traffic from Branch Offices

Configure SD-WAN or on-prem perimeter equipment to automatically route Internet destined traffic to Verizon cloud security so that compliance, malware defense and data loss prevention can be applied to user Internet traffic as it moves between branch offices and the cloud. All of the capabilities of Verizon Secure Cloud Gateway can be leveraged, including the best malware defense comprised of industry leading malware engines and feeds. CASB controls for social media and cloud applications are also native within the Verizon Secure Cloud Gateway platform. Additionally, protect from data loss using deep file inspection capable of detecting PII and other sensitive information.

Eliminate Sending Unnecessary Internet Traffic Through Private Network Connections

When traffic is headed toward cloud applications such as Office 365, unnecessarily sending that traffic through private connections to centrally hosted security appliances is not only costly, but reduces user productivity substantially as Internet connections from branch offices are choked. Leveraging Verizon Secure Cloud Gateway allows traffic to flow through the most optimized path directly to the Internet. This reduces the load on MPLS and SD-WAN links and valuable network resources, including firewalls and routers. It also extends the useful life of existing network appliances which will not need to reach their maximum throughput capabilities due to the offloaded direct to Internet traffic. This results in substantial savings and reduced IT labor costs.

Ensure the Same Security and Policies Apply to Branch Offices and Mobile Users

Any policy applied to branch office Internet traffic will also apply to mobile users working on the road or at home. Users are always connected to Verizon cloud security which ensures any policies created for branch office traffic routed through the Verizon Secure Cloud Gateway will also apply to users wherever they roam.

Security That Lives Directly In the Cloud

As traffic is routed between branch offices and Verizon Secure Cloud Gateway, the containerized cloud gateway capacity that protects data Internet transfers lives directly inside the cloud next to where the applications run. This minimizes the amount of hops needed to apply Internet security to branch office data resulting in increased speeds and the best user experience.

Push Split Routing Policies with SD-WAN

SD-WAN can automatically push split routing policies to branch office perimeter network equipment so that internal traffic is routed over private links, while Internet bound traffic is routed through Verizon cloud security. With MPLS, the Internet Service Provider, such as Verizon, can configure this policy to offload Internet bound traffic from MPLS connections. This simplifies the configuration and deployment of cloud based Internet security to start realizing value immediately.

Designed for Office 365

The power of Microsoft Office 365 requires bandwidth and fast connections. The Verizon Secure Cloud Gateway lives in the cloud, where Office 365 lives, providing fast connections regardless of user location. Best of all, the Verizon Secure Cloud Gateway includes native features to ensure Office 365 traffic is always routed in the most optimized way possible and never interferes with Office 365 connections.

How It Works

Taking advantage of the Verizon Secure Cloud Gateway for direct branch office breakouts is easy. To get started:

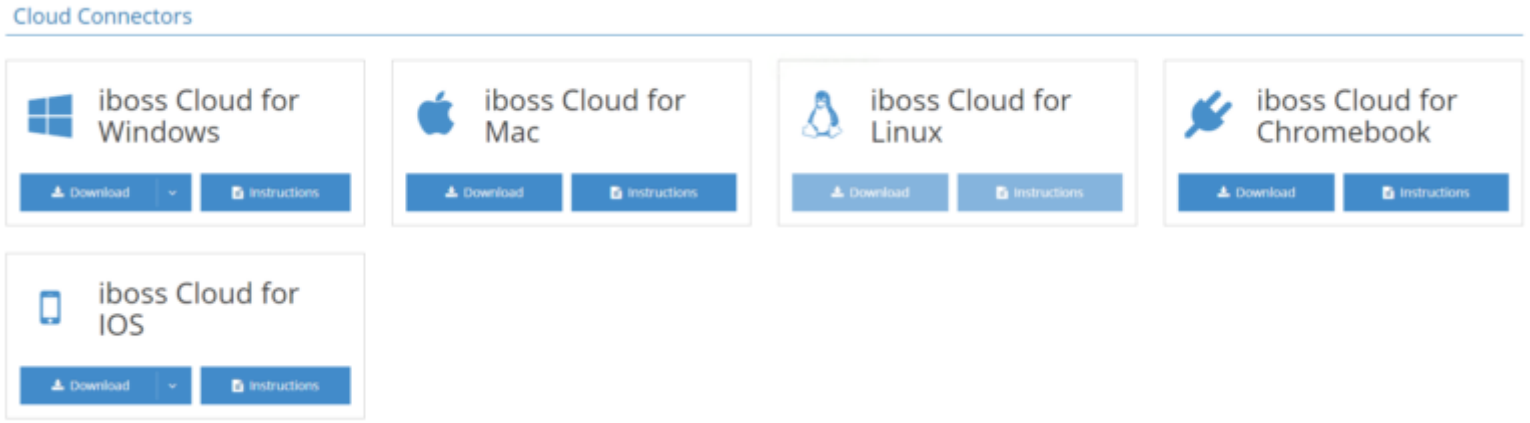
1. Get an active Verizon Secure Cloud Gateway account
2. Connect users to Verizon Secure Cloud Gateway using the Verizon SCG cloud connectors or branch office tunnels
3. Benefit from offloading traffic from internal private SD-WAN links for reduced costs and fast cloud connections

Feature Highlights

Branch Office Tunnel Support

The Verizon Secure Cloud Gateway supports both GRE and IPSec tunnels for connecting offices to the cloud. Virtually every type of branch office perimeter network device can be connected to Verizon cloud security so that Internet bound data is offloaded from internal MPLS and SD-WAN links. Example firewall configurations are also available.

Verizon SCG



The Verizon SCG connectors ensure users are connected to the Verizon cloud security at all times, regardless of location. The connectors take a mobile and cloud-first approach to connect users' devices to cloud security regardless of whether they are in the office or on the road. With the network perimeter eroding, the cloud connectors are a great choice for connecting users to Verizon cloud security. The connectors can also be used as an alternative to branch office GRE and IPSec tunnels as they will connect users to cloud security while users are in the office. SD-WAN and MPLS configuration can send any traffic with Verizon Secure Cloud Gateway destination IP Addresses directly to the Internet while sending all other traffic through private links. The containerized architecture of Verizon Secure Cloud Gateway allows for this advanced capability because the Verizon Secure Cloud Gateway IP Addresses are dedicated to the organization. These dedicated IP Addresses are what allow for policy routing configurations which offload Internet traffic from local office-to-office traffic.

Pricing

Branch Office Internet Breakouts	
The ability to configure MPLS and SD-WAN links for branch office Internet breakouts to Verizon cloud security is included with all Verizon Secure Cloud Gateway subscriptions at no additional cost.	Contact Us

Learn More About Pairing SD-WAN with Cloud Security

To learn more about branch office Internet breakouts and pairing MPLS and SD-WAN to cloud security, visit https://www.iboss.com/business/compliment-mpls-and-sd-wan.

About iboss

iboss is a cloud security company that provides organizations and their employees secure access to the Internet on any device, from any location, in the cloud. This eliminates the need for traditional security appliances which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture, iboss is designed to make transitioning from security appliances to cloud security a seamless process. iboss is trusted by more than 4000 organizations worldwide, spans over 100 points of presence globally and is backed by over 110 patents.

To learn more, visit https://www.iboss.com