Connect Offices to Each Other and the Internet Securely with Microsoft Virtual WAN

Microsoft Virtual WAN makes it easy to connect offices to each other and the Internet securely with Virtual WAN combined with iboss cloud.

Microsoft Virtual WAN with iboss cloud Overview

Microsoft Virtual WAN, or vWAN, can send traffic that is already destined to the Internet directly from branch locations to the cloud. 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 iboss cloud is natively integrated with Microsoft vWAN so that Internet security is applied to traffic as it is routed directly to the Internet from branch locations. The configuration is automatic and has massive scale so that branch office traffic can traverse directly to the Internet with low latency and high security while reducing management and configuration time.

- The iboss cloud is integrated natively with Microsoft Virtual WAN so that branch office traffic is automatically routed from Microsoft to iboss cloud for compliance, malware defense and data loss prevention

- One click configuration within iboss cloud connects Internet security to Microsoft Virtual WAN

- SaaS offering abstracts all of the complexities of configuring and implementing local branch Internet breakouts which substantially reduce data backhauling costs and increase speeds to cloud applications resulting in higher end user productivity

- Combining iboss cloud's horizontal scaling with Microsoft Virtual WAN, branch office to cloud tunneling capacity expands and scales to over 20 Gbps which is more than any other cloud security provider

- The iboss cloud gateway capacity lives directly within Microsoft Azure, ensuring fast and efficient connectivity that is close to the user

- Support for multiple Microsoft Hubs and regions to ensure data is scanned within country boundaries for GDPR compliance

- Optimized for Office 365 migrations with native Office 365 support features

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

Microsoft Virtual WAN provides a solution to connect offices together securely through Microsoft Azure cloud. Additionally, Microsoft Virtual WAN 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 iboss cloud is integrated with Microsoft Virtual WAN so that Internet bound traffic from users at branch offices is secured from Internet threats. This includes automatically routing data from Microsoft Virtual WAN through iboss cloud security. The iboss cloud automatically instructs Microsoft Virtual WAN how to route the data in addition to automatically scaling as bandwidth needs increase. The iboss cloud containerized gateway capacity lives directly within Microsoft Azure ensuring a direct connection between Microsoft Virtual WAN and iboss cloud for fast and efficient connections.

iboss cloud with Microsoft Virtual WAN

iboss and Virtual WAN – Secure Branch to Internet
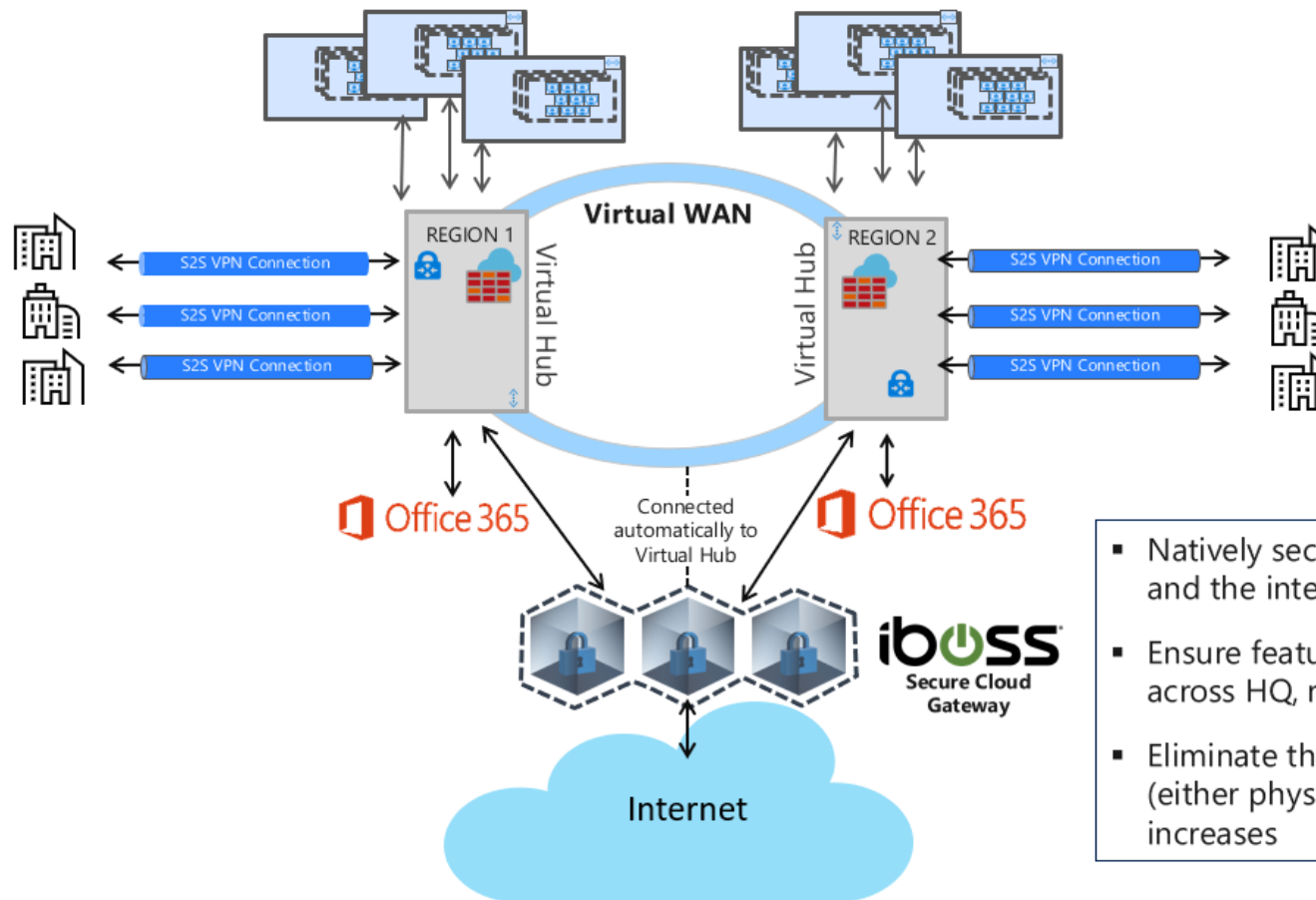
- Natively secure traffic between Virtual WAN and the internet without multiple hops
- Ensure feature parity and consistent security across HQ, remote offices and mobile
- Eliminate the need to manage appliances (either physical or virtual) as bandwidth increases

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

Enabling Microsoft Virtual WAN within iboss cloud will automatically route Internet destined traffic to iboss 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 iboss cloud 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 iboss cloud platform. Additionally, protect from data loss using deep file inspection capable of detecting PII and other sensitive information.

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

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

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 Microsoft Virtual WAN and natively integrated iboss cloud allows traffic to flow through the most optimized path directly to the Internet. This reduces load on MPLS 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.

Security That Lives Directly Inside Microsoft Azure

As traffic is routed between Microsoft Virtual WAN and iboss cloud, the containerized cloud gateway capacity that protects data Internet transfers lives directly inside Azure. This minimizes the amount of hops needed to apply Internet security to branch office data resulting in increased speeds and the best user experience. The iboss cloud extends across all of Microsoft Azure for maximum global reach and coverage.

Multiple Concurrent Microsoft Hub Support

Microsoft Virtual WAN relies on the concept of connecting branch offices to Microsoft Hubs. The Microsoft Hubs exists within different Microsoft data centers. The iboss cloud supports connecting multiple hubs and regions concurrently to gateway capacity within those regions so that Internet security can be applied to branch office traffic while ensuring compliance is met, such as GDPR.

Designed for Office 365

The power of Microsoft Office 365 requires bandwidth and fast connections. With iboss cloud living directly inside Azure, security lives next to the resources running Office 365 for fast connections. Best of all, the iboss cloud 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 iboss cloud security with Microsoft Virtual WAN is easy. To get started:

1. Get an active iboss cloud account
2. Log into your Microsoft Azure account or create one for free at https://azure.microsoft.com/en-us/free
3. Connect offices to Microsoft Azure and each other using Microsoft Virtual WAN
4. Enter your Microsoft Azure settings into the iboss cloud admin interface to enable vWAN connectivity
5. Connect a Microsoft Virtual WAN Hub to an iboss cloud Zone for protection

Enter Basic Azure Settings into the iboss cloud Admin Interface


To enable the Virtual WAN feature, enter your Microsoft Subscription ID, Client ID, Key and Tenant ID into the iboss cloud admin interface. The iboss cloud uses this to automatically configure all Virtual WAN routing and connections. IT staff do not have to worry about complex networking and routing configuration as this is completely abstracted by iboss cloud.

Connect an iboss cloud Zone to a Virtual WAN Hub
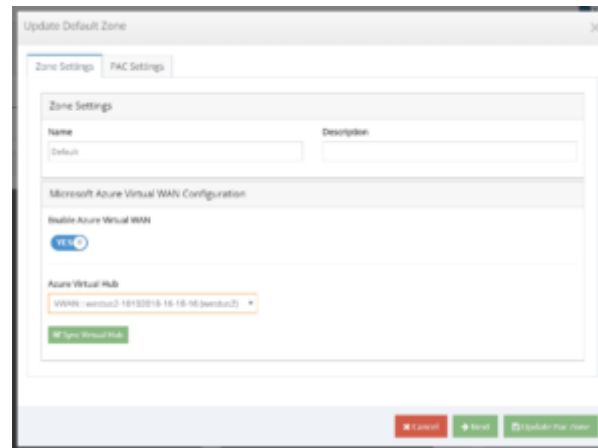
The iboss cloud allows IT administrators to create zones which represent users in offices or geographical regions. This also allows tight control of where data is processed for users within different regions for compliance, such as GDPR. Since Microsoft Virtual WAN relies on Virtual Hubs that exist within different regions, connecting an iboss cloud zone to a Microsoft Virtual Hub ensures traffic from users in that zone is automatically routed through iboss cloud security. This includes ensuring that traffic from that Microsoft Internet breakout point is scanned with iboss gateway capacity that exists within that region.

Once Virtual WAN is enabled for a zone, the iboss cloud automatically configures all routes and connections to Internet security with no IT intervention. Scaling is also automatic and can support tunnels between offices and the Internet in excess of 20 Gbps.

Pricing

Microsoft Virtual WAN Features

Microsoft Virtual WAN (vWAN) features are included with all iboss cloud subscriptions at no additional cost.

Contact Us

Learn More About Virtual WAN

To learn more about Virtual WAN, visit Microsoft's Virtual WAN home page at https://azure.microsoft.com/en-us/services/virtual-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