

Reduce or Eliminate Load on VPN Connections from Work From Home Users



Send Cloud Application Traffic from Remote Users Directly to the Cloud Reducing Load on VPNs and Increasing Remote User Productivity

Cloud application traffic from remote users is traditionally sent through slow and overloaded VPNs to provide network security for compliance, malware defense and data loss. This typically results in slow connections or down networks preventing users from working effectively in work from home scenarios. The problem is, cloud application traffic should NOT be sent through VPNs. If the traffic is destined to the cloud, why is it being sent back to the office?

With the iboss cloud platform, you can completely offload your VPN connections by sending cloud application traffic directly from work from home users to the cloud. All of the traffic is sent through the iboss cloud platform first, to ensure compliance, malware defense and data loss prevention. This immediately reduces or eliminates load from VPN connections bringing the network back up to normal operation and ensuring users are productive while working from home.



Reduce load on Office and Data Center Network Connections



Give your VPN a Break By Offloading Cloud Application Traffic to iboss cloud



Proxy Appliances Were Not Designed For Modern Cloud Applications

Reduce load on Office and Data Center Network Connections

The bandwidth available at the company data center or corporate office was designed and sized for the users within the office perimeter. When users work from home, the connection speeds available to them far exceed that of the corporate office. It is common for a user to have 100-500 Mbps of bandwidth from their home connection for a very small cost. When multiplied by the number of users working remotely, the amount of total bandwidth back to the data center is staggering.

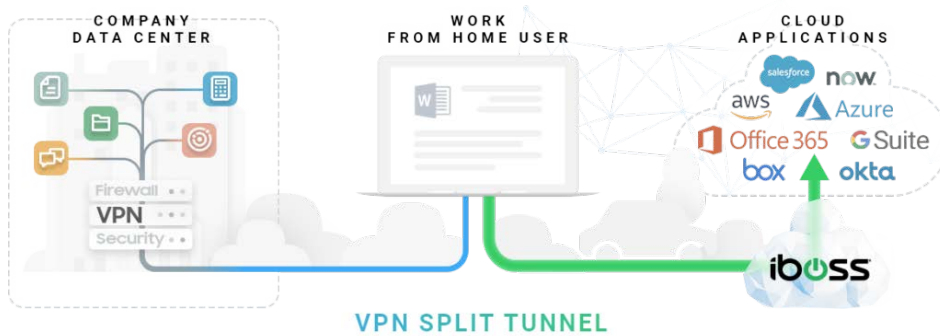


For example, one thousand remote workers with 100 Mbps connections at home is 100,000 Mbps (100 Gbps). It is very unlikely the corporate office or data center has that much bandwidth available. This results in slow or unusable connections to cloud applications making it impossible to work from home. With iboss, all of that traffic is eliminated from the data center and sent instead to iboss cloud. This immediately increases speeds and reduces costs as additional bandwidth does not need to be purchased to support these remote users.

Give your VPN a Break By Offloading Cloud Application Traffic to iboss cloud

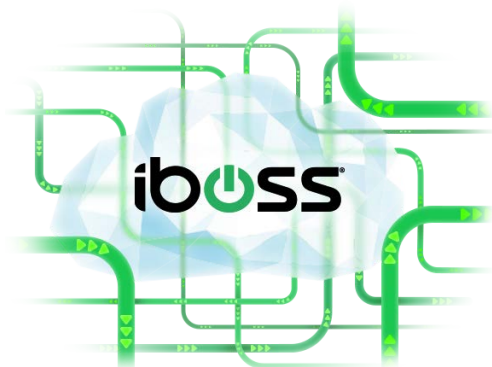
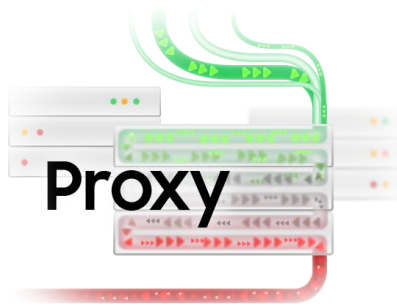
VPNs were designed to allow users to connect to applications sitting in the office. The problem is, those applications no longer sit at the office and have moved to the cloud. Microsoft Exchange has moved to Office 365 and can be accessed from anywhere, including work from home users. When the network load for cloud application traffic is sent through the VPN, it typically results in VPN infrastructure that is immediately overloaded. This results in downtime due to saturated VPN platforms or extremely slow and unusable connections for remote users.

Cloud application traffic should not be sent through the VPN as it will end up being sent to the cloud anyway. Send cloud application traffic through iboss cloud. This is easily accomplished by configuring a split-tunnel VPN configuration. This allows office traffic to go through the VPN and all other cloud application traffic to be sent directly to the cloud through iboss cloud. This can be configured in minutes and immediately solve slow connections or costly VPN upgrade projects.



Proxy Appliances Were Not Designed For Modern Cloud Applications

Proxy appliances are typically purchased and implemented to handle the bandwidth needs of the corporate office. They were not designed to handle the enormous bandwidth and encrypted traffic load from work from home users. On-prem proxy appliances will quickly become saturated as they do not have the compute capacity to scrub the large volume of data for compliance, malware defense or data loss prevention.



The iboss cloud lives in the cloud and has infinite compute capabilities. It can handle any bandwidth load, with its containerized horizontally scaling design. Instead of purchasing or renewing proxy appliances, switch instead to iboss cloud and get the same protection as a SaaS delivery model. This substantially reduces costs, labor and allows organizations to handle work from home user scenarios with ease.

Buy Now

The iboss cloud can secure user Internet access on any device, from any location, in the cloud. Best of all, you can start using it immediately to protect your users instantly.

What you get

- 🕒 In the cloud Internet security
- 🕒 Advanced Internet malware protection that follows users
- 🕒 Advanced cloud and SaaS controls
- 🕒 Web filtering and compliance controls
- 🕒 Internet security for in-office users without appliances
- 🕒 Branch office Internet security without data backhaul
- 🕒 And a lot more...

Contact Us

Get in touch with a technical specialist for a live demo.

North America Sales:
877-742-6832 X1
Contact local distributor or:
sales@iboss.com

International Sales:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com

EMEA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

CONTACT SUPPORT

Support Overview
Open a Ticket

North America Support:
877-742-6832 X3
support.na@ibosscloud.com

LATAM Support:
+52 (55) 41696270
support.latam@ibosscloud.com

EMEA Support:
+44 (0) 203 7908289
support.emeia@ibosscloud.com

APAC Support:
+63 (45) 4571057
support.apac@ibosscloud.com

CONTACT SALES

Request Demo
Request Information

North America Sales:
877-742-6832 X1
Contact local distributor or:
sales@iboss.com

International Sales:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com

EMEA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

iboss



Copyright © 2020
iboss. All Rights Reserved.