iPass Last Mile VPN

iPass

CONTENTS

Anytime, anywhere mobility

Wi-Fi has become a basic business requirement, as mobile professionals require unlimited access to high-speed, high quality connectivity to get more done. But not all Wi-Fi is created equal. Although offering upfront cost savings, free Wi-Fi is anything but free. It comes with numerous risks to your company's mobile security, from man-in-the-middle attacks to packet sniffing and identity spoofing. If exploited, any of these threats can bring your business down. You need iPass to keep your company data safe and your mobile teams productive.

The big challenge is making unlimited connections that are invisible and everywhere. But being connected everywhere demands being secured on every connection, on every network and in every environment.

Implications of always-on connectivity

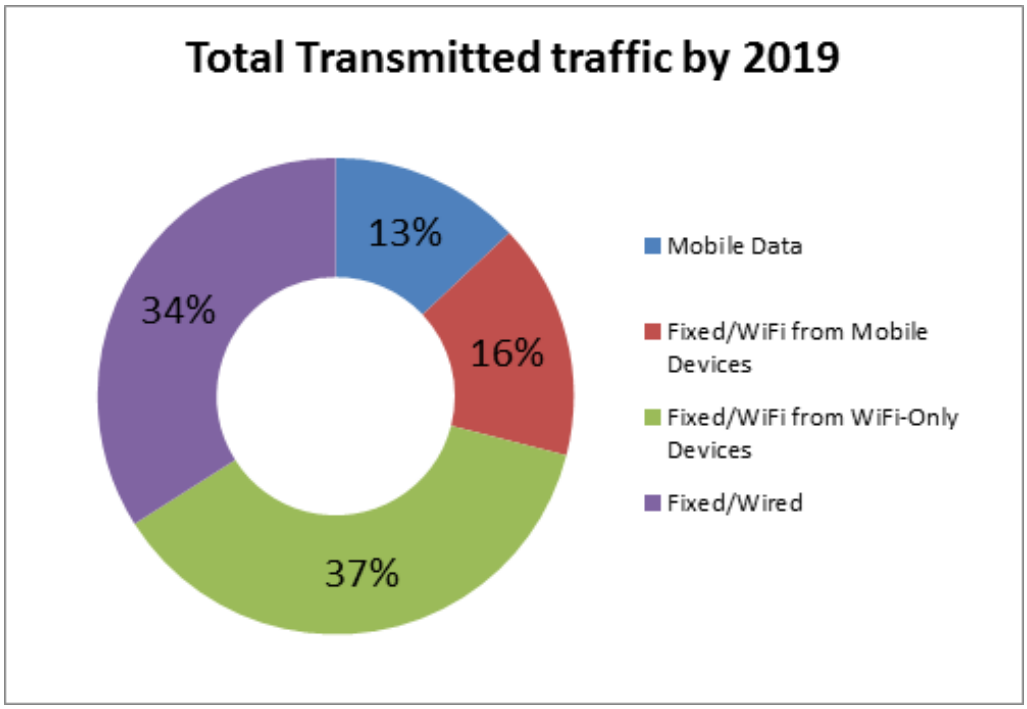
Companies and private users use their mobile devices in order to handle private and sensitive data with their own colleagues and contacts within their organizations. Smartphones can be used for internet browsing, accessing social networks, video conferencing, scheduling tasks, reading documents and phone calls. In addition, as individuals, we use our smartphones or mobile devices for accessing our bank accounts, to do online shopping, and other tasks.

Bring your own device (BYOD) is an increasingly common practice in many companies, so it's inevitable that a mobile device or laptop may include both personal data and business data.

Mobile devices are the first choice for all kinds of users. They can access any type of Wi-Fi network, including home networks, corporate networks, premium wireless services or unsecured, open Wi-Fi networks.

Wi-Fi is the most convenient and cost-effective way of staying connected everywhere; it operates in millions of homes, corporations, universities and public hotspots worldwide.

According to Cisco's *Global Data Traffic Forecast Update, 2015-2020*, in the year 2019, more than half of the total transmitted traffic (53%) worldwide will originate or terminate on Wi-Fi.



"In the era of hyper-connectivity…global proliferation of unsecured Wi-Fi networks and uneducated users can be a worrying combination."

Threats to constantly connected devices

Our mobile devices inevitably generate a significant amount of traffic, including sensitive data. Important professional and personal information such as usernames, passwords, session keys and personally identifiable information is often transmitted.

In the era of always-on connectivity, the increase in the number of mobile devices, global proliferation of unsecured Wi-Fi networks and uneducated users can be a worrying combination.

Users will tend to gravitate towards free internet access without knowing the level of security behind these services. Many public places, such as coffee shops and hotels, have wireless networks that lack any security for transient users that access these networks. As an example, a large number of coffee shops are more concerned with providing easy Wi-Fi access to their customers than a secure network environment.

The problem arises when a user is unaware of those vulnerabilities. Public Wi-Fi networks are almost always unencrypted, which means that a latent threat or threats can be embedded within this type of service.

Public networks can also be accessed by hackers looking for sensitive information. A third party can break into these unencrypted Wi-Fi public networks, and with commonly available software, they can access everything that is being sent over the network.

The *iPass Mobile Security Report* compiled responses from 500 organizations from the U.S., U.K., Germany and France. The report showed that 37% of the overall respondents stated that their biggest perceived security threat was free Wi-Fi hotspots.

Unsecured Wi-Fi can be compromised using several attack vectors:

- Man-in-the-middle attacks
- Sniffers
- Evil twin
- Sidejacking

The white paper, "The Hidden Dangers of Public Wi-Fi," published by *Private Wi-Fi* in October of 2014, explains that different hacks can occur while a user connects to a public Wi-Fi hotspot.

Many users also consider that if they connect to a paid network in a hotel or airport, they have access to a secure service. However, wireless attacks can happen on any public Wi-Fi network. Many users that lack data transmission security knowledge can be victims of attacks without even realizing they have been hacked. The responsibility of protecting themselves belongs to end users and their employers.

Mitigating the risks

Some countermeasures have been set in place to reduce the security threats present in the public free and paid Wi-Fi networks. However, according to the iPass Mobile Security Report, almost 50% of the organizations in the U.K. banned their employees from using public Wi-Fi with a company owned device, citing security concerns. But the question is still the same: what happens with a BYOD scenario?

Despite education, end users may well access public Wi-Fi networks with their own device, often transmitting personal information as well as work related data.

Antivirus and firewalls may be used for online safety although often these tools do not protect users from hackers performing attacks on public and private hotspots.

End users and company employees are also advised to rely on HTTPS in order to protect their online transactions. Hackers have found alternative routes to access this type of information, by using fake websites in order to collect any type of SSL certificate that can be exchanged with a simulated server. Therefore secured websites can also be a target and are not invulnerable to these types of attacks.

The threats mentioned above may lead to traffic interception, man-in-the-middle attacks or any other attacks performed by a hacker.

A safe alternative is to use tunnelling techniques such as a Virtual Private Network (VPN) in order to provide a proper traffic encryption.

"Almost 50% of the organizations in the United Kingdom have banned their employees from using public Wi-Fi with a company owned device citing security concerns."

Securing your devices with mobile VPNs

VPNs are designed to provide data integrity, authentication and encryption to assure the security of data over an unprotected network. The VPN creates a tunnel between the mobile device and an internet gateway or server connected to a corporate network.

A VPN encrypts all user data coming in and out of a mobile device or smartphone, while the two sides of the communication use a shared encryption algorithm and key pair.

Many different protocols are used to implement a VPN. In this document, we will describe the ones used for VPNs for mobile devices:

- Internet Protocol Security (IPsec): IPsec uses the Internet Key Exchange (IKE) protocol in order to establish a remote access VPN tunnel. This protocol offers a number of benefits such as automatic negotiation and authentication of the VPN creation as well as the ability to change the encryption keys during an IPSec session. (Making it harder to unencrypt the traffic).

  The tunnels can be created with different encryption methods such as AES, 3DES, DES, etc.

- Secure Socket Layer (SSL): SSL-based VPNs leverage the SSL protocol often referred to as Transport Layer Security Protocol. This protocol has been in existence since the early 1990s and was created by the IETF in order to consolidate the different SSL vendor versions into a common and opened standard.

  SSL/TLS prevalence relies on the ability for VPN users to remotely access different resources from anywhere. It secures the communication using cryptographic algorithm in order to offer confidentiality, authentication and integrity. Key exchange algorithms such as RSA and ECC rule the way the user's mobile device and the server determine the keys to be used during the VPN session.

Initially, VPNs were built for users to work from remote locations such as their homes, offices, hotels, airports or other premises as if they were directly connected to their corporate network.

The iPass Mobile Security Report explains that only 26% of organizations are fully confident that mobile workers access their enterprise systems via a VPN all the time.

The end-to-end connection paradigm changed when BYOD smartphones started to be the preferred device. Users need access to a secure channel that allows them to browse the internet, perform any online transaction, and access their IoT devices as well as using their corporate services.

There are limitations with the current mobile VPN solutions, and these are highlighted below:

- The VPN tunnel is only invoked once the connection is established to the enterprise VPN server. This can result in user login information being sent 'in the clear' on an unencrypted connection.

- Many enterprises are migrating their applications to the cloud and do not wish to route traffic to those services via their corporate networks, due to bandwidth and latency concerns. This has led many enterprises to implement split-tunnel VPNs. This approach routes traffic for the enterprise over an encrypted tunnel but leaves any traffic for destinations outside the enterprise unencrypted. This is a key flaw when using split tunnel VPNs on unsecured Wi-Fi. A user may think that they are protected for all traffic when in fact they aren't.

Mobile VPN Solutions

As highlighted before, Wi-Fi traffic will be 53% of total data traffic by 2019. With a forecasted 355 million public hotspots and 12 billion mobile devices (32% of which will be smartphones), only a relatively small number of connections need be compromised to represent vast proprietary information leakage.

A user should be able to access online services and applications as well as transmit traffic safe in the knowledge that his or her data is not being hacked. Mobile VPNs based on the IPSec or SSL should block any or all attack vectors.

The ideal security solution will support VPN traffic for every device independently of its operating system (OS) and can defeat multiple attack vectors. The ideal solution will also secure all traffic to and from a device, including login information, irrespective of the source or destination of the traffic.

iPass Last Mile VPN Solution

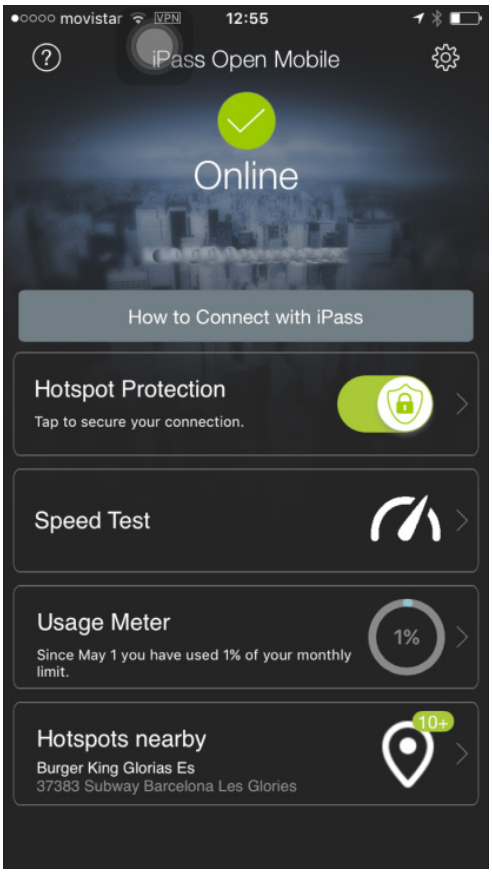
iPass delivers global mobile connectivity as a hosted cloud service, connecting its customers with the people and information that matter the most on all of the devices they choose to carry: smartphones, tablets and laptops. iPass is the world's largest Wi-Fi network, with more than 53 million hotspots in more than 120 countries in airports, hotels, aircraft, local businesses and public areas.

The iPass app provides global hotspot security with last-mile VPN functionality. The iPass client can initiate a secure VPN tunnel before user authentication takes place. The VPN connection initiated by the iPass app is established between the mobile device and a secure internet gateway hosted and managed by iPass. This allows user credentials as well as personal and company data to be fully secured and protected against attacks.

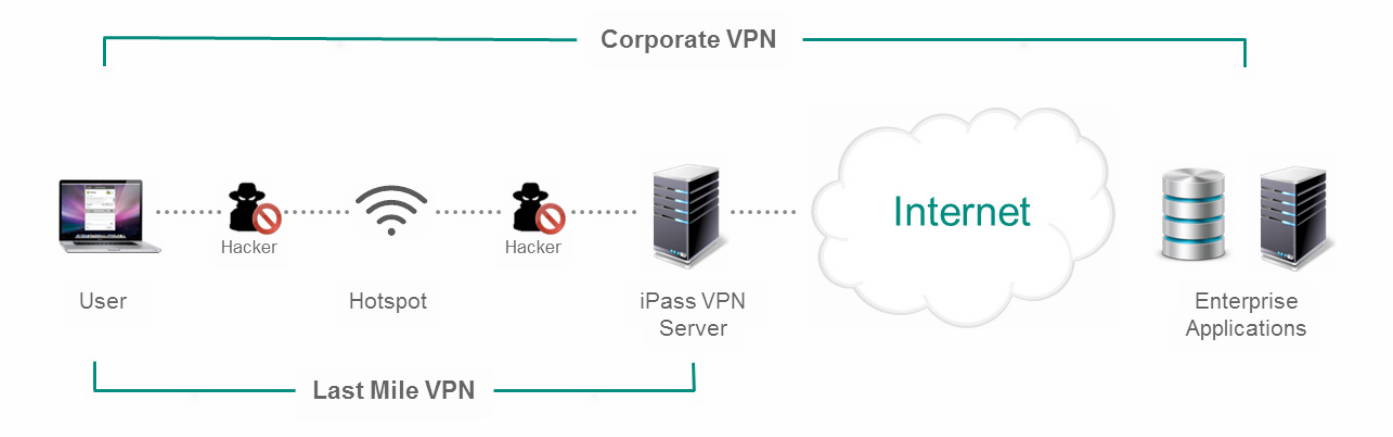
This capability is available for traffic over any Wi-Fi hotspot not just those in the iPass footprint. The user only has to be an iPass subscriber. This is a key capability when a user is connecting to a non-commercial hotspot, for example at a rental property.

As shown below, a user is able to activate the VPN feature manually. Alternatively, an enterprise IT admin can force a user's device to always activate the Last Mile VPN. To optimize latency, the iPass client will automatically connect to the nearest iPass hosted VPN gateway.

In the unlikely event that a VPN server is not available, the client will continue to send traffic to the Internet without the tunnel. The VPN indicator (a key icon on Android, or the letters VPN on IOS) at the top of the screen will not appear. Additionally, the user interface will indicate the tunnel is not in use.



The last mile VPN can be used in addition to or instead of a corporate VPN. It may seem counterintuitive to layer a VPN over a VPN, but the last mile VPN provides additional protection for user login credentials and for traffic that may not be routed via the corporate VPN as in the 'split-tunnel' scenario detailed above.



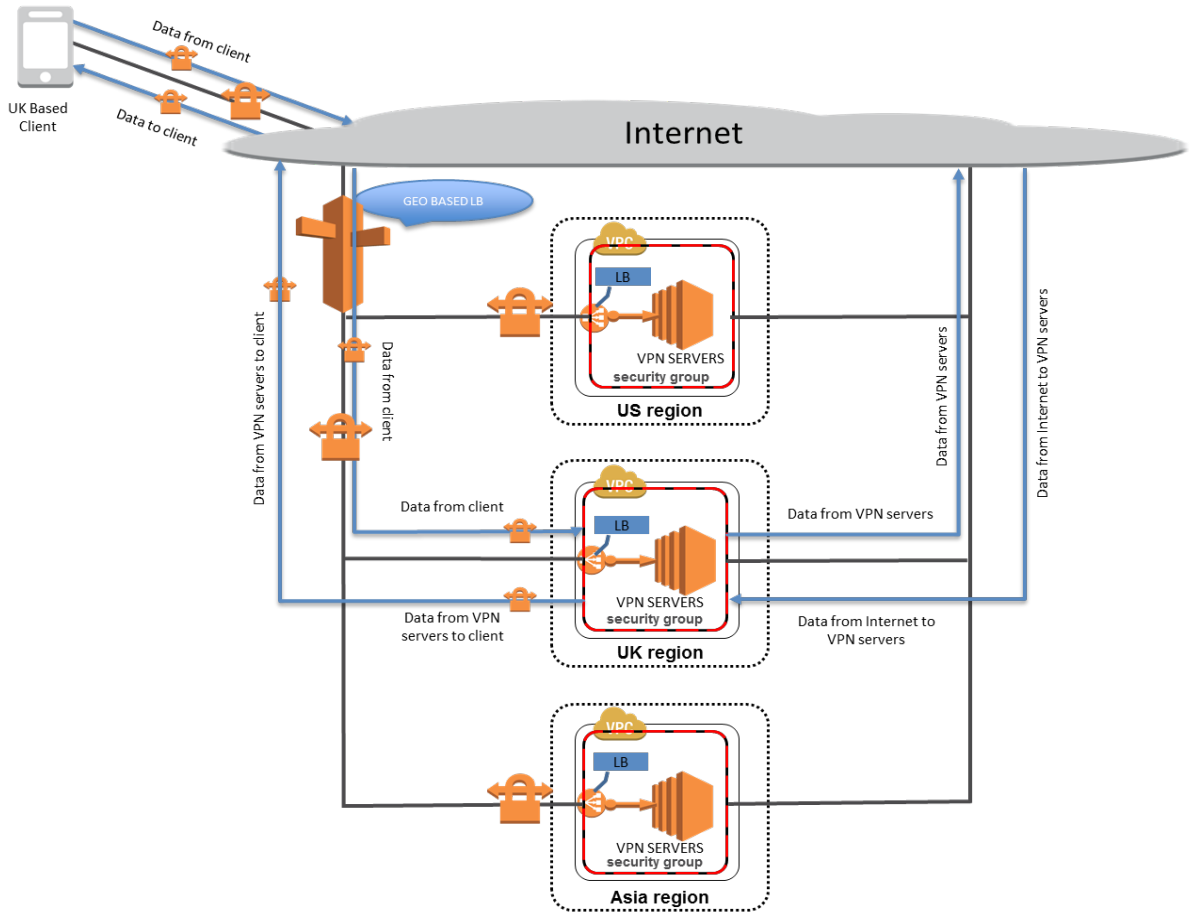
While latency can be a common issue when using a VPN, iPass eliminates this problem by distributing VPN gateways on different locations worldwide (see below). When connecting to any hotspot location, the application launches a VPN to the closest internet gateway, reducing the latency generated by connecting to a VPN endpoint that is abroad.

Enterprise IT admins with data sovereignty concerns can force any or all of their users' clients to connect to a specific VPN gateway.

Available VPN tunnel termination points are located in the following locations:

- Americas (USA)
- Europe (UK)
- Asia (Singapore)

The diagram below shows how iPass routes VPN traffic.

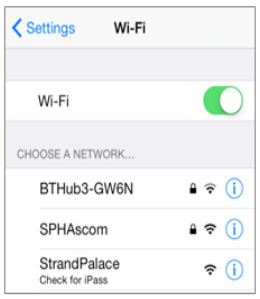


Last mile VPN functionality can be supported with Android, iOS and Windows devices. The encryption methods on the iPass Last Mile VPN differ by device OS:

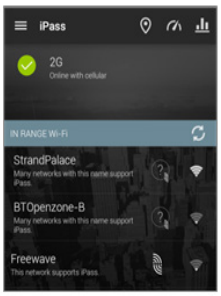
- IOS: IPsec AES 128 and AES 256-bit
- Android: 256-bit and 160-bit OpenVPN SSL/TLS+RSA Certificates
- Windows: 256-bit and 160-bit OpenVPN SSL/TLS+RSA Certificates

How to connect with the iPass Last Mile VPN

1. Ensure that Wi-Fi is activated.
2. Select a hotspot (for optimum user experience use an iPass hotspot) with a strong signal.



iOS Network Selection

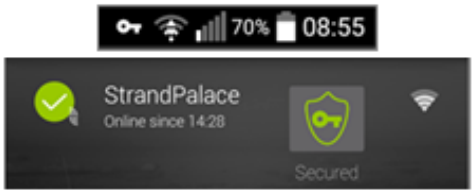


Android Network Selection

3. Launch the iPass app and confirm that it logged in automatically. If it did not, tap on Log In.

4. Activate the Hotspot Protection (VPN) feature (may be automatically activated). Once the VPN is enabled the padlock icon will be shown closed and VPN or Key will appear at the top of your screen (depending on your mobile device operating system.)

iOS



Android

Conclusion

- BYOD is becoming increasingly popular, making it almost inevitable that a mobile device will be both used for personal and business purposes, comingling personal and business data.
- With the rise of public Wi-Fi hotspots and the new capabilities on smartphones, users need to make sure that all of their traffic is protected.
- Using a secure VPN that establishes an encrypted tunnel from the mobile device to a secure gateway makes attacks such as MITM, Evil Twins, Sniffers and Sidejacking far harder to accomplish.
- With a footprint of over 53 million hotspots, iPass secures end users credentials and data by providing a solution that encrypts and transmits the traffic from the mobile device into a secured VPN Internet Gateway.

Sources

- iPass Mobile Security Report – iPass Inc.
- Defending mobile devices for high level officials and decision-makers – NATO Cooperative Cyber Defence Centre of Excellence
- Smartphone Security – European Union Agency for Network and Information Security
- Global Data Traffic Forecast Update, 2015-2020 - Cisco

About iPass

iPass (NASDAQ: IPAS) is the leading provider of global mobile connectivity, offering simple, secure, always-on Wi-Fi access on any mobile device. Built on a software-as-a-service (SaaS) platform, the iPass cloud-based service keeps its customers connected by providing unlimited Wi-Fi connectivity on unlimited devices. iPass is the world's largest Wi-Fi network, with more than 53 million hotspots in more than 120 countries, at airports, hotels, train stations, convention centers, outdoor venues, inflight, and more. Using patented technology, iPass SmartConnect™ takes the guesswork out of Wi-Fi, automatically connecting customers to the best hotspot for their needs. Customers simply download the iPass app to experience unlimited, everywhere, and invisible Wi-Fi.

iPass Corporate Headquarters
3800 Bridge Parkway
Redwood Shores, CA 94065

main: +1 650-232-4100
support: +1 650-232-4300

www.ipass.com