FREQUENTLY ASKED QUESTIONS

iPass

FAQ: Last Mile VPN Functionality

Q: Why should I use a VPN (Virtual Private Network) on my mobile device?

A: When a mobile device is used to access public Wi–Fi hotspots, all the information you send to and receive from the Internet is not secure. Web pages, emails, passwords, instant message traffic--absolutely everything that's not encrypted--is readable by anyone in the area.

The biggest threat to free Wi-Fi security is the ability for a hacker to position himself between a user and the Internet connection point. As the man in the middle, a hacker may get access to important emails, credit card information or even security credentials belonging to a user's company network. A hacker can also use an unsecured Wi-Fi connection to distribute malware. Finally, ISPs are also able to see what you are doing online and might even share your information with advertisers.

With a VPN, a "private tunnel" is created between you and the Internet, which encrypts all data that passes through the network. This can help prevent anyone lurking on the network from intercepting a user's data.

Q: What is iPass' solution for mobile data security over public Wi-Fi?

A: The iPass service includes last mile VPN functionality for data security while accessing Wi-Fi from a public hotspot. iPass traffic between a user and the Internet will be encrypted. iPass' VPN functionality prevents hackers, who may be connected between a user and the Internet, from spying on user activity online. iPass VPN functionality makes it difficult for hackers to read or steal private information.

The "last mile" refers to the distance between the user's device and the Internet, when the user is accessing public Wi-Fi. The last mile is

TABLE OF CONTENTS

traditionally the most vulnerable area in terms of data security. iPass uses industry–standard VPN technology to create a secure tunnel between a user's device and iPass' VPN servers at the edge of the Internet.

Q: Will the VPN service be a paid service or included in iPass Unlimited?

A: iPass' VPN service will be provided free of charge for iPass Unlimited customers. This is another way iPass brings value to its customers by providing an additional level of security and privacy.

Q: iPass' last mile VPN functionality is supported on what devices?

A: For the time being, our last mile VPN functionality will only be available on Android and iOS.

Q: What standards does last mile VPN functionality support?

A: iPass uses industry-standard VPN technology and supports IPSec (Internet Protocol Security) on iOS devices and OpenVPN on Android devices.

Q: What level of encryption does iPass VPN functionality use?

A: iPass uses IPsec AES 128 and AES 256-bit (Advanced Encryption Standard) encryption for iOS devices. For Android devices, iPass uses OpenVPN SSL (Secure Socket Layer) TLS (Transport Layer Security) and RSA Certificates.

Q: What does the free VPN service include?

A: Our last mile VPN service covers all user data from iPass hotspots to iPass VPN termination points around the world.

Q: If the service is secure now, wasn't it before?

A: Security is multi-layered. There are device, application, data, network and traffic layers to consider; no one app or operating system individually can secure all layers at once. The iPass service secures user credential information and works with service providers to ensure secure wireless network protocols are employed across our network.

The addition of last mile VPN functionality enhances user security by encrypting Internet traffic up to iPass VPN termination points around the world. Also, this implementation effectively hides user traffic from network administrators and other users, who may be present within the last mile of the user's Internet connection. No solution from any one provider can ensure 100% security, but last mile VPN functionality is widely considered a very strong solution.

Q: Which VPN options can the user configure in the client and/or at the profile level?

A: The user controls whether the last mile VPN functionality is enabled or not, whether the VPN connection should be set to "Manual" or "iPass-only" networks, and which VPN server locations to use.

Q: Will VPN functionality replace or complement my existing VPN?

A: Only one VPN solution can be used at a time, so if an iPass user connects to a corporate VPN, the iPass solution will switch off, and the user will instead connect to their corporate VPN solution for security.

Q: Where are the VPN endpoints located (Country/Region)? How is the endpoint chosen?

A: iPass will support the following endpoint locations.

- Europe (UK)
- Asia (Singapore)
- North America (USA)

Endpoint selection is automatic. The server gets selected based on the client's geo tag. For example, if the client request comes from the Asia Pacific and Australia region, the request will only go to the Asia Pacific server in Singapore. If the client request comes from the Europe region, the request will only go to the Europe server in the UK. And for the rest of world, the request will go to the US Server.

Q: Is a client update necessary before VPN functionality can work?

A: The user will need a client update, and the IT admin will need to add VPN functionality to the profile.

Q: When using a streaming app that goes from a Wi-Fi to a cellular connection will last mile VPN functionality carry over?

A: It will not carry over.

Q: When traveling between frequent hotspots, will you be able to keep the session running so that you do not have to log in again?

A: If the last mile VPN service is set to "iPass Networks," the iPass app (if running) will automatically reconnect to the iPass VPN server on behalf of the user each time the user changes iPass hotspots. But if the user has set the VPN service to "Manual," then they will need to secure each iPass Wi-Fi hotspot manually.

INTERNAL QUESTIONS

Q: What is the pricing model – is the last mile VPN functionality included in ULTD but chargeable otherwise? Does the cost vary depending on what networks the VPN service is allowed to protect?

A: The pricing model is still in discussion. iPass is using OpenSource Software, which is under GNU GPL v2 license. We must first ensure legal compliance, as per GPL v2.

Q: Is the VPN functionality for cellular data included?

A: At this point in time, VPN functionality is not supported for cellular data.

Q: Are we using Amazon Cloud Computing Services?

A: We are using Amazon Web Services (AWS) for VPN server termination.

Q: What are the issues regarding data privacy now that we route all traffic through iPass (or Amazon)?

A: There are no privacy issues, as all data is encrypted by iPass and opaque to Amazon.

Q: What data privacy and security statement do we have from Amazon?

A: This AWS Security Whitepaper describes Amazon's security posture.

https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

Q: Does the new release include integration with Microsoft VPN services (RAS Client)?

A: No, the VPN functionality is only available for Android and iOS devices at this time.

Q: If the user selects different break-out points, can he circumvent licensing laws (e.g., accessing US Netflix from other locations)?

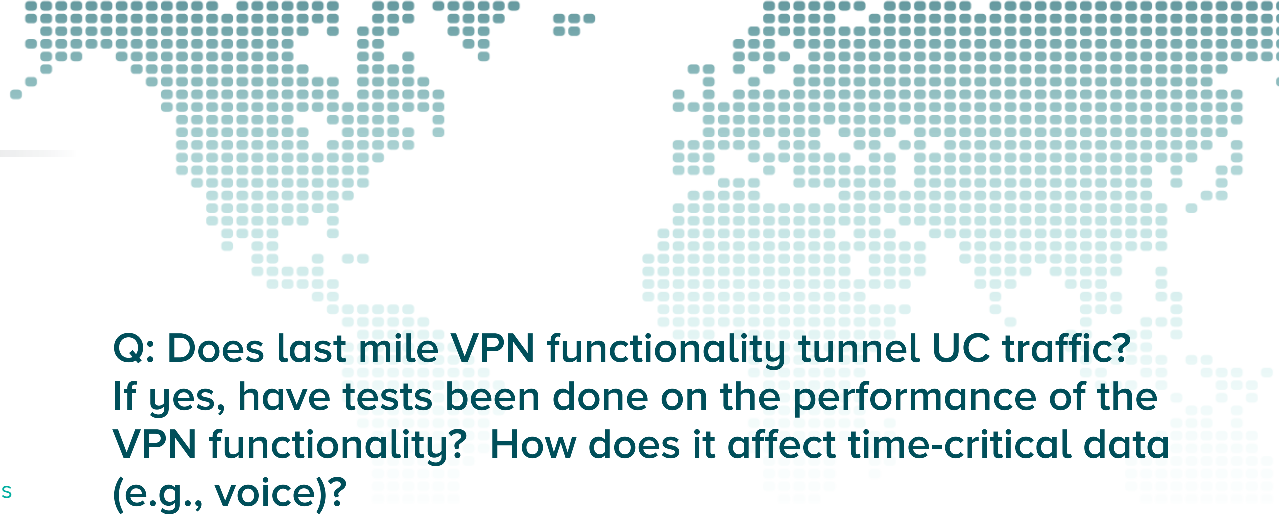
A: Yes, but that is not our intention. This subject should not be brought up externally.

Q: Is VPN functionality enforceable by IT or is it an opt-in by the end user?

A: Last mile VPN functionality is made available to the user through the IT profile, which is set up for the user. However, the user is responsible for turning it on and off. There is no existing functionality to designate the VPN as "always on."

Q: Is it possible for the user to select filtering rules on traffic (e.g., block Facebook traffic)?

A: No, filtering is not possible with last mile VPN functionality, but the user might use another method to filter traffic.



Q: Does last mile VPN functionality tunnel UC traffic? If yes, have tests been done on the performance of the VPN functionality? How does it affect time-critical data (e.g., voice)?

A: We do not recommend UC traffic. The encryption/decryption process can introduce jitter.

Q: What throughput are we offering with VPN functionality?

A: 10 Gigs; we are not advertising this number.

Q: What is the expected (additional) latency when using the VPN service?

A: The expected additional latency will be approximately 20ms in good conditions, further dependent on network quality.

ABOUT IPASS

iPass (NASDAQ: IPAS) is the world's largest Wi-Fi network, offering convenient, 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 will have 50 million hotspots in more than 100 countries by the end of 2015, 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.

Corporate Headquarters
iPass Inc.

3800 Bridge Parkway
Redwood Shores, CA 94065
+1 650-232-4100
+1 650-232-4111 fx
www.ipass.com

While every effort is made to ensure the information given is accurate, iPass does not accept liability for any errors or mistakes which may arise.

Specifications and other information in this document may be subject to change without notice.