INTRODUCTION

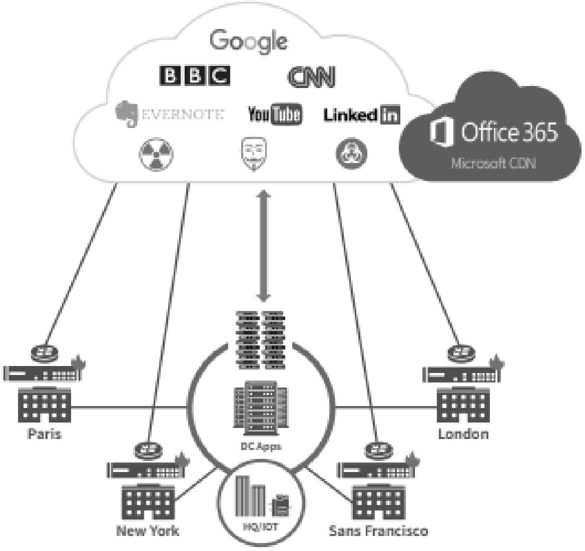
As enterprises rely more and more on cloud applications to run their businesses, they face challenges imposed by traditional hub-and-spoke architectures. When Microsoft Exchange servers and Office applications were on-premises, you had to backhaul traffic from remote sites and mobile users to the data center. It was the only way to provide connectivity. But now that these services have moved to the cloud in the form of Office 365, backhauling all your traffic to your data centers can create the kind of latency that can quickly lead to frustrated users and delayed deployments.

Today, the Instasafe Cloud Security Platform processes over terabytes of Office 365 traffic every month for customers around the world. And these numbers are growing rapidly.

With our customers, we've seen an average increase in network utilization of 40 percent, and that's because each user is now generating between 12 and 20 persistent connections. This increase can easily overwhelm firewalls and increase your transport budget. Therefore, Microsoft now recommends performing NGFW capacity assessments, WAN latency assessments and advised against using Skype for business when deploying Office 365 on a hub and spoke architecture.

DIRECT INTERNET CONNECTIVITY FOR OFFICE 365 – DIRECT INTERNET CONNECTION USING APPLIANCES

Office 365 was built to be accessed securely and reliably via a direct Internet connection and Microsoft has invested in a CDN to deliver a fast experience. Deploying appliances at each branch is better for the user experience, but it is expensive to buy, deploy and maintain.

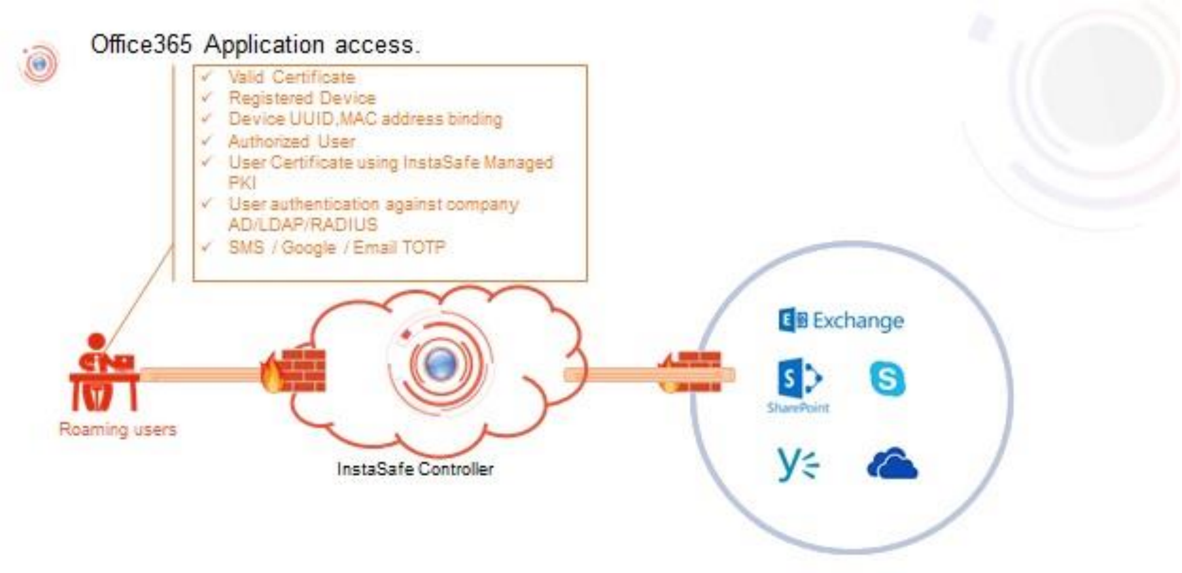


Challenges with appliances

- Requires constant firewall updates and missing an IP or URL update will cause connectivity issues
- Requires appliance capacity assessments to ensure they can handle the high number of long lived connections.
- Requires security tradeoffs in branches with only UTMs or firewalls for security.
- Requires local DNS.

How does it work?

InstaSafe makes Office 365 deployment easy. It provides your users with a fast Office 365 experience, while maintaining the highest level of security for Internet traffic. Simply point your Internet and Office 365 traffic to the closest InstaSafe data center. There is no hardware to deploy and manage and since traffic is routed locally, you can reduce your MPLS spend.


Office365 Application access.
✓ Valid Certificate
✓ Registered Device
✓ Device UUID,MAC address binding
✓ Authorized User
✓ User Certificate using InstaSafe Managed PKI
✓ User authentication against company AD/LDAP/RADIUS
✓ SMS / Google / Email TOTP
Roaming users
InstaSafe Controller
Exchange
SharePoint

Office 365 control using InstaSafe Secure Access.

Pre-Requisites:

- Office 365 customer needs to block access to users from unknown public IP address.
- InstaSafe provided public IP needs to be whitelisted in Office365 portal.
- Customer will get InstaSafe portal login details once signup with InstaSafe.

InstaSafe Approach:

- Using InstaSafe portal we will group all the applications (Skype, yammer, mail and OneDrive) with respective public subnet.
- After user on boarding to InstaSafe portal, administrator can create user based application access control rules.
- Administrator can define which device can be used for user login.
- Once access rules are created user can login and download the InstaSafe agent to connect office 365 applications outside his/her office network.

Self-Service Provisioning

Automatic configuration of user’s email, VPN and Wi-Fi settings eliminates help desk calls.

SSO Access

Certificate-based authentication and SSO give users easy access to Office 365 (MFS) and other cloud services (SAML).

Hostchecking

Compliance enforcement ensures that only secured devices can access Office 365 and other cloud services. Hostchecking can also be used with third party identity providers.

BYOD Container

Android and iOS container security encrypts data, controls app data sharing, selectively wipes data and supports per app connectivity policies.

Mobile App Management

Policy-based push of Word, Power point, Excel and other mobile apps boosts user productivity.