WHITE PAPER

Secure Cloud Printing:

How to Ensure Complete Security in the Cloud

One of the key tenets of cloud computing is the reduction of hardware and software ownership and maintenance which allows organizations to focus on their core business strategies and strengths. We are already seeing this trend with organizations consolidating remote print servers to centralized data centers in the form of serverless printing.

While the financial and operational benefits are obvious and similar, cloud computing goes one step further by eliminating the burden of infrastructure management altogether and enabling organizations to quickly align information technology to business strategies through on-demand provisioning.

However, by adopting a cloud service, organizations must be willing to give up direct control of whichever system they are moving to the cloud and this naturally spawns concerns over security. This document will address common security concerns organizations have regarding moving their printing infrastructure to the cloud and how UniPrint Infinity ensures security when it comes to cloud printing.

Accessing On-Premise Printers from Microsoft Azure

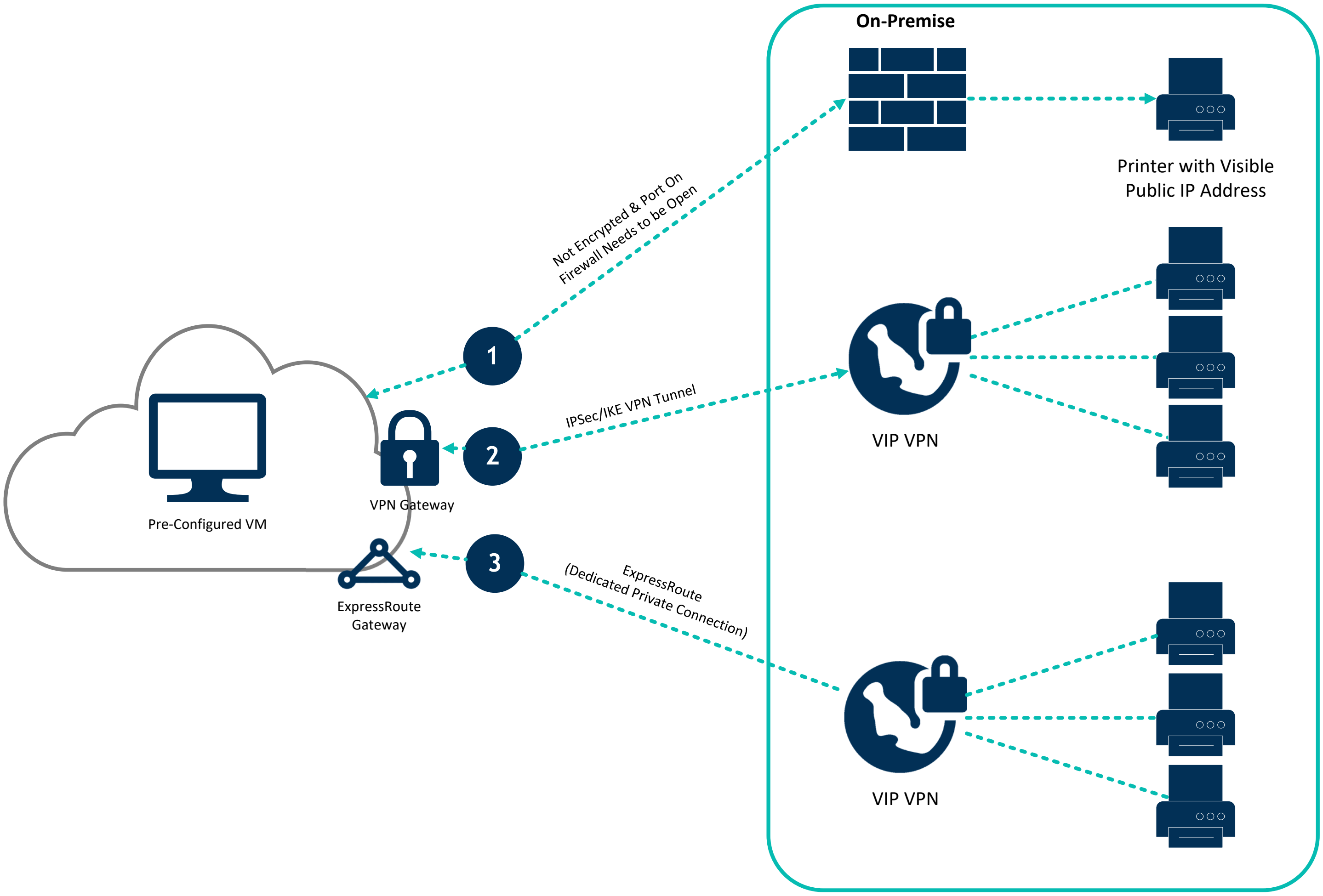
On-Premise
Printer with Visible Public IP Address
Not Encrypted & Port On Firewall Needs to be Open
1
IPSec/IKE VPN Tunnel
2
VIP VPN
Pre-Configured VM
VPN Gateway
ExpressRoute Gateway
3
ExpressRoute (Dedicated Private Connection)
VIP VPN

FIGURE 1: Current Site-to-Site connection methods between Azure and an organization's on-premise network.

One functionality that most organizations seek, is the ability to print from an application, that is hosted on an Azure virtual machine (VM), to a network or local printer on-premise. To do this, a connection between the Azure virtual network and the on-premise network needs to be established. Currently, there are 3 common methods to do this. One of which is not secure and therefore not recommended and the other 2 cost extra through Microsoft Azure.

For Route 1 (Figure 1), a port needs to be opened on the firewall exposing it to the public and an on-premise printer needs to have a public IP address assigned to it. The data transfer between Azure and the on-premise firewall is over the Internet and is not encrypted. This opens up an opportunity to sniff the print job before it reaches the corporate firewall allowing hackers to view any documents sent to on-premise printers. The exposed port and public IP address for the printer are also an open door into an organization's network. This route is not recommended due to grave security concerns.

For Route 2, an encrypted connection is established between the Azure VPN Gateway and the on-premise VPN device. Multiple on-premise sites can be connected to a single VPN Gateway and each on-premise VPN device must have a public IP address. While creating a virtual network in Azure is free, connecting it to an on-premise network securely is not free. The cost of most of these Azure resources, unless otherwise stated, are based on the amount of time they are provisioned and available. Depending on the bandwidth and speed requirements a VPN Gateway can cost anywhere from $0.04 per hour to $1.25 per hour and each VPN tunnel can cost up $0.015 per hour per tunnel. Also depending on the zone that the Azure data center is located, the outbound traffic can cost up to $0.035 per GB. For more information on pricing, visit the Azure marketplace for VPN gateway.

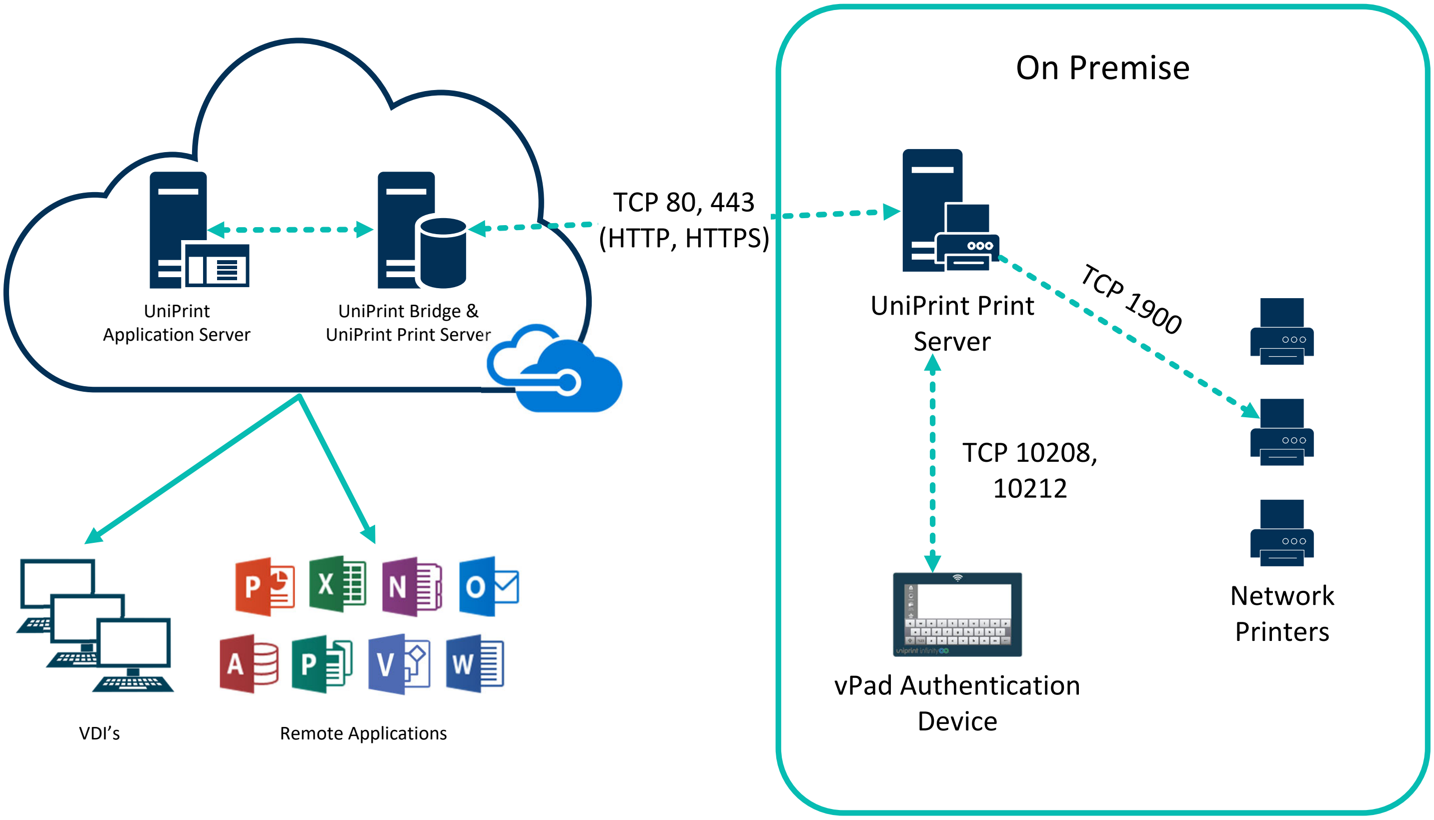
On Premise
UniPrint Application Server
UniPrint Bridge & UniPrint Print Server
TCP 80, 443 (HTTP, HTTPS)
UniPrint Print Server
TCP 1900
TCP 10208, 10212
Network Printers
vPad Authentication Device
VDI's
Remote Applications

FIGURE 2: UniPrint Infinity deployed in Microsoft Azure. *Default ports used by standard deployments.

Route 3 is the most secure out of the current connection methods, but it is also the most expensive. Azure ExpressRoute creates a dedicated private connection between the on-premise network and the Azure virtual network through an ExpressRoute partner. This is more secure since data traffic does not traverse the Internet. ExpressRoute is similar MPLS, but is specific to Microsoft Azure. Depending on the bandwidth and the speed required, ExpressRoute can cost any where from $55 to $51,300 per month plus the cost of the ExpressRoute VPN Gateway which ranges from $0.19 per hour to $1.87 per hour. There may also be additional costs from the ExpressRoute provider. For more information on pricing, visit the Azure marketplace for ExpressRoute.

While Microsoft ensures security within the Azure cloud environment, it doesn't secure against print data breaches between the Azure virtual network and the on-premise network, nor within the on-premise network. And while they provide features such as the VPN Gateway and ExpressRoute to help secure connectivity, these are provided at an additional cost. This is where UniPrint Infinity can help. UniPrint Infinity is deployed as a pre-configured virtual machine (VM) within Microsoft Azure. This deployment is available through the Microsoft Azure Marketplace and enables mobile printing, secure pull printing and network printing from anywhere in the cloud.

The connection between the Azure virtual network and the on-premise network is secure due to encryption. However, UniPrint Infinity goes one step further by helping to avoid print data breaches on-premise.

On-premise data breaches most often occur at the printer itself. This is where users tend to leave or forget to pick up their sensitive documents. These documents can be inadvertently taken or viewed by unauthorized personnel. For example, a user may not get to the printer in time to intercept their print job which could result in a different user inadvertently picking up their printed documents. Most users would just assume the print job didn't go through or that they forgot to click Print. So, they return to their workstation and send another print job which they manage to pick up before anyone else sees it. The user who initially picked up the first print job, realizes that it doesn't belong to them and returns it to the printer. This initial print job ends up sitting on the printer for all to see and may never be picked up by its owner.

The aforementioned scenario is unfortunately all too common, but it can be prevented by ensuring users are more conscious of their printing habits. This is where UniPrint SecurePrint and pull printing can help.

With SecurePrint, the user must initially password protect the print job with a SecurePrint password before they click Print. Their print job is then sent to and stored on the SecurePrint server awaiting release. It does not automatically go through to the print server, where it is rendered, and then sent on to the selected network printer. This gives the user time to make their way over to the printer, where the UniPrint vPad authentication device is installed. The user must enter their domain user name and then the print job's associated SecurePrint password before their print job is released to the printer for printing.

For additional security, SecurePrint and the vPad series support multifactor authentication whereby the user is required to tap their RFID or HID card and also enter a SecurePrint password before their print job is released for printing. SecurePrint is also compatible with Imprivata OneSign.

Conclusion

With UniPrint Infinity deployed in Azure, organizations can reap the benefits of cloud computing by reducing the amount of server and software ownership and management in addition to maintaining a cost effective and secure, end-to-end printing infrastructure. While Microsoft is responsible for securing their cloud infrastructure, by ensuring their data center is secure and ensuring each customer's data is isolated, they don't secure data that is transferred between Azure and the on-premise network.

However, UniPrint SecurePrint along with the UniPrint vPad authentication device, extends the security provided by Microsoft Azure, by ensuring the data transferred between the Azure and on-premise network is also secure. UniPrint SecurePrint also helps to avoid on-premise data breaches by ensuring sensitive documents are not left on shared printers and enforces users to print consciously.

For additional security, multifactor authentication can also be employed to securely release user print jobs for printing. Since SecurePrint easily integrates with Active Directory and is also compatible with Imprivata OneSign, the UniPrint vPad is available with a built-in RFID or HID reader. Alternatively, external card readers are also available for purchase. Since the vPad is compatible with any printer make and model, standardizing an existing printer fleet is not necessary.

Whether an organization is moving their entire IT infrastructure to the cloud, or just their printing infrastructure, UniPrint Infinity has a secure printing solution that is easy to integrate with any pre-existing printer fleet and with minimal configuration.

Try UniPrint InfinityCloud for a FREE
30-day trial and see how easy cloud printing can be

About Process Fusion

Process Fusion is a software company and a cloud solution provider. We help organizations transform inefficient, paper (labor) intensive business processes into a secure, automated, mobile ready Digital First experience for all participants.

Contact:
3250 Bloor Street West
Suite 1000, East Tower
Toronto, Ontario, Canada
M8X 2X9

uniprint.net
processfusion.com

Universal. Unified. Unique.

Process Fusion