Hosting Controller
Hybrid Cloud Automation

Non-VPN Access for Active Directory

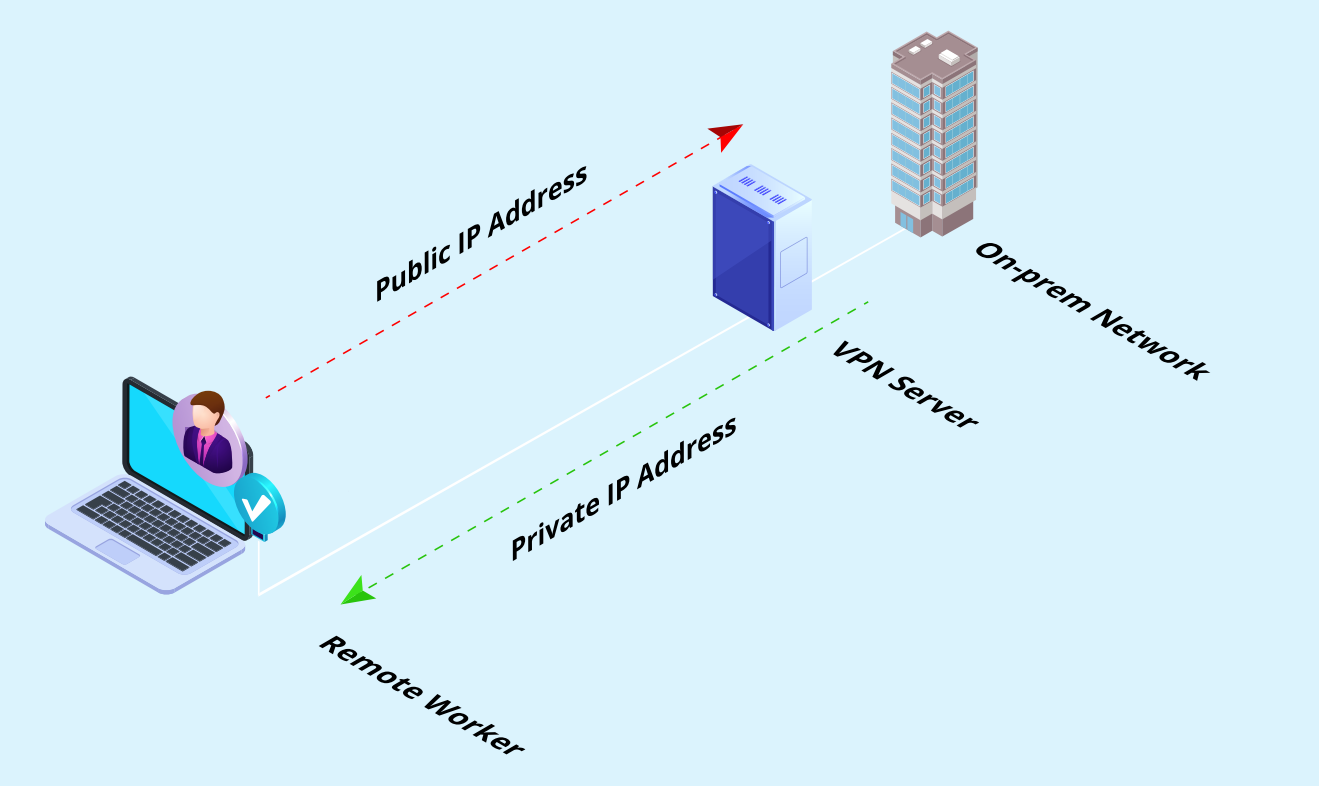
WHITE PAPER

Hosting Controller

www.hostingcontroller.com

For an organization running an on-premise Active Directory server, all users need to login to the Active Directory in order to gain access to required applications and resources.

The on-premise Active Directory is kept on a very secure network with controlled access from any location outside the office's trusted networks. Any remote workers need to be first granted network access to the on-premise network before they can login to the Active Directory servers. This is typically done using VPN Servers.



Such VPN connections have many problems attached to them:

A Security Loophole
Private networks are created to keep access from the public networks and all its related problems out of the way. Most of it is out of scope of this short document but a VPN server grants a private IP address outside the strictly controlled network.

An Administration Overhead
User accounts for all individuals working remotely need to be created. They are always only as secure as their VPN passwords or other authentication credentials. They need to be expired and changed periodically. When a user leaves or is not required to have remote access, the user accounts need to be disabled or removed.

A Security Monitoring Problem
With the same VPN server giving access to many different types of users, its a problem to use automated tools to monitor what data is being accessed by whom.

One Solution: Cloud Hosted Active Directories

Many cloud hosted service providers including Amazon AWS offer pre-configured hosted services for Active Directory server. If such a server is available, then the remote workers do not need to connect any VPN connections. The active directory is already available on a public IP address and the users only need to have a basic Internet connection to access that.

The hosted active directory needs to be synchronized with the on-premise directory. This can be done either using the built-in replication tools and configuring it as an 'Additional Domain Controller' or a third party tool like Hosting Controller's AD Connect Sync utility.

Major benefit of AD Connect Sync utility in this scenario is that it enables to only copy the required parameters to the cloud including the passwords.

Major cloud vendor like AWS and GCP have their own Active Directory offers like:

https://aws.amazon.com/directoryservice/
https://cloud.google.com/managed-microsoft-ad

Once an AD instance has been acquired in the cloud, one way replication can be setup between source AD which is usually on-premises and may be on a private IP subnet to the cloud based AD which is always available on a public IP address.

Hosting Controller's AD Connect Sync utility can then be used to copy only the required data selectively into the cloud AD. This will also include the user's passwords.

All remote workers can then easily login without any need for VPN connections.

Address
Hosting Controller Inc. Suite 401, 50 Burnhamthorpe Road W.
Mississauga, ON, L5B 3C2 Canada

+1 (647) 799-1000

sales@hostingcontroller.com
www.hostingcontroller.com