WHITEPAPER

WORKING FROM HOME

Solutions featuring NComputing Products and Services

The COVID-19 pandemic is changing where we work. Shelter-in-place initiatives have starved businesses of their talent. Unable to properly continue business as usual, a harsh reality is setting in–working from home (WFH) is no longer a luxury; it's a necessity. Whether you're familiar with virtualization products or coming to this green, our focus here is to show the different ways to virtualize your office.

Introduction

Before we begin, a quick definition. The plans involved in this paper revolve around individuals working remotely. Requirements for their home office are simple - a keyboard, mouse, monitor (or two), and an access device. These devices can be physical hardware like PCs, laptops, or thin clients. They can also be software solutions. The use cases provided here will help you identify best-fit solutions for your needs.

NComputing offers comprehensive and flexible virtualization solutions to solve WFH initiatives. We built a line of products that both complement and complete the scenarios discussed here. We will start with simple, straight forward solutions like our vSpace Pro platform, and gradually work through Microsoft Windows Virtual Desktop (WVD), Remote Desktop Services (RDS), **VERDE VDI**, and Citrix.

NComputing has been providing desktop virtualization systems worldwide for 17 years. It's our specialty, so let's get started.

Why virtualization?

Managing employees' desktops and laptops is a costly and time-consuming reality for IT. Even with today's modern desktop management tools, applying patches, upgrading applications, onboarding new users, and maintaining appropriate levels of security on the desktop can be a significant headache. When those resources are not physically close, it further complicates. Desktop virtualization is a way to alleviate many of these issues.

NComputing®
Compute Smartly™

Benefits for end-users:

- **Increased flexibility and mobility:** Users can access their apps and virtual desktops from anywhere using various devices such as thin clients and home PCs without compromising performance.
- **Hardware independence:** Older computers still running legacy operating systems such as Windows XP can leverage the enhanced capabilities of modern operating systems such as Windows 10 running in a virtual environment on servers.
- **Business continuity and disaster recovery:** Business continuity can be enhanced by enabling rapid resolution of hardware failures and eliminating location requirements.

Benefits for IT:

- **Ease of deployment and management:** Administrators can easily manage virtual desktops from a central location and quickly provision them to users as-needed, eliminating the need for IT to manage each user device independently.
- **Cost reduction:** IT can save on hardware costs by using lower-cost thin clients with desktop virtualization instead of traditional PCs. Thin clients also consume less energy and require less maintenance, providing further savings on operational expenses.
- **Enhanced security:** Sensitive business data remains in the data center instead of being stored locally on end-user computers.
- **Data protection:** Since data is not locally stored, in case of any disaster data is quickly recoverable, improving uptime and the reliability of the system.

Virtualization types

There are two primary methods of virtualization: Server Based Computing (SBC) and Virtual Desktop Infrastructure (VDI). SBC are terminal-session based homogenous desktops for users with similar needs. For instance, kids in a school computer lab need access to the same operating system and application set. So would employees in a call center, or order tracking stations at a manufacturing facility.

VDI deployments are typically virtual machine (VM) based heterogeneous desktops, providing flexible computing environments for different types of users and needs. Employees in finance may need a different operating system and application set than software engineers or the marketing team. VDI provides the flexibility to meet all their needs.

The critical difference between SBC and VDI virtual desktop architectures is how the operating system exists within the virtual desktops. With VDI, each virtual desktop requires a complete, independent instance of the host operating system and provides one-to-one interaction between the virtualized Operating System (OS) and user.

With SBC virtualization, a single instance of the operating system supports multiple users. All of them have their personalized accounts within that instance, providing a one-to-many interaction of one OS and numerous users. While the performance and experience for the users are very similar, the administration experience is vastly different, and it is worthwhile to understand how the differences between the two architectures affect them.

SBC-based platforms

This architecture allows users to share one virtualized server desktop environment in the form of individual sessions instead of separate operating environments per user. This shared virtual desktop environment can run on servers in a central data center or on a physical PC in a workgroup, call center, or classroom. A hypervisor is not required for small user environments (less than 100), making it extremely simple to set up and deploy. In the case of larger deployments, the shared desktop environment can run inside a virtual machine on a server. Multiple VMs on multiple servers can scale a deployment to thousands of users.

- Multiple users share a single OS.
- Applications are on that single OS instance.
- Terminal session-based user isolation.

VDI-based platforms

This architecture uses a hypervisor to run a user's operating system in a virtual machine (VM), decoupling it from the PC host hardware. Typically multiple VMs run on servers in a central datacenter, isolating the user desktop environment from the physical device, enabling the user to access their virtual desktop from any PC, laptop, or thin client from any location. And since the computing resources are centralized, management and maintenance are made easier for IT.

- Each user has a personal OS (VM).
- Applications are on the individual OS (VM).
- VM-based user isolation.

Four platforms for discovery

The following four platforms will be looked at in-depth in our use cases. Here is a brief introduction of each and the role NComputing plays in them.

vSpace PRO

vSpace Pro is an end-to-end virtualization solution delivering Windows desktops to users. All data storage and computing tasks occur on servers, not local computers, but the experience from the user's standpoint is the same. Here, you're getting PC-like performance from server-based computing (SBC). vSpace Pro is a session virtualization system. Each user gets their workspace, and all workspaces from the server have the same operating system and applications.

This platform supports 11 popular Windows operating systems for use with *NComputing* thin clients, Chromebooks, and PCs running our LEAF OS software solution. Every platform needs a protocol to work on, and vSpace Pro uses the proprietary UXP protocol for all traffic.

vSpace Pro delivers a turnkey solution to manage all your user sessions and devices centrally. These services can exist on-premise or in the cloud.

Microsoft

Microsoft Windows Virtual Desktop (WVD) is a comprehensive desktop and application virtualization service managed by Microsoft and hosted in the Azure cloud. WVD delivers simplified management with multi-session Windows 10 support. *NComputing* is an official Windows Virtual Desktop partner for integrared Linux thin client solutions, verified by Microsoft.

Microsoft Remote Desktop Services (RDS) is a virtualization platform that serves sessions of individual applications or desktops. These services are either hosted on-premise or in the cloud. We provide thin clients for end-users and the software to manage them. They are designed and optimized specifically for Microsoft RDP and include support for Microsoft RD Gateway, Remote App and Desktop, Remote FX, and VPN connections. RDS works on the RDP protocol. We've also addressed the sub-standard multimedia performance of the standard RDS deployment through a server software package called SuperRDP, allowing for the improved streaming performance of HD video locally or from the web.

verde

VERDE VDI is purpose-built from the ground up on a secure Linux foundation. It connects to a wide range of endpoint devices, including PCs, thin clients, software clients, and HTML5-enabled browsers providing Windows or Linux desktops to users. Supported protocols include UXP, RDP, and SPICE.

VERDE VDI is a secure, easy-to-use, enterprise-grade virtual desktop infrastructure. It offers three important capability pillars:

- Windows and Linux clients are equal citizens.
- WAN latency is eliminated by decentralizing VDI processing to the edge of your organization.
- It spans the end-user computing fabric from on-premise to cloud-hosted, or hybrid using our unique Cloud Branch technology.

Prevention of malware, virus attacks, data leakage, and unauthorized access to the internal network are all cornerstones of **VERDE VDI** security protocols. In addition, all traffic is encrypted.

CITRIX

Citrix provides server, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing technologies.

NComputing has designed access devices optimized for Citrix HDX. They meet the performance, security, and manageability necessary for demanding Citrix users.

NComputing is a founding partner in the Citrix Ready Workspace Hub program aimed at accelerating workplace transformation and solving innovative use cases around enterprise IoT.

WFH Solutions by Use Case Scenario

NComputing supports extensive and flexible work-from-home scenarios depending on the solution type. Below is a basic overview of the use case scenarios.

vSpace PRO	Microsoft	verde	CITRIX
EASY TO DEPLOY	EASY TO DEPLOY	EASY TO DEPLOY	EASY TO DEPLOY
FEATURE SET	FEATURE SET	FEATURE SET	FEATURE SET
BUDGET FRIENDLY	BUDGET FRIENDLY	BUDGET FRIENDLY	BUDGET FRIENDLY

On-premise deployment

- 1. VPN
- 2. Port forwarding

On-premise deployment

- 3. VPN
- 4. RD Gateway
- 5. Port forwarding

Azure Cloud deployment / Windows Virtual Desktop

- 6. Azure RD Gateway

Sessions only

- 10. VPN
- 7. Port forwarding

Remote PC only

- 11. VPN
- 8. Port forwarding

Sessions & Remote PC

- 12. VPN
- 9. Port forwarding

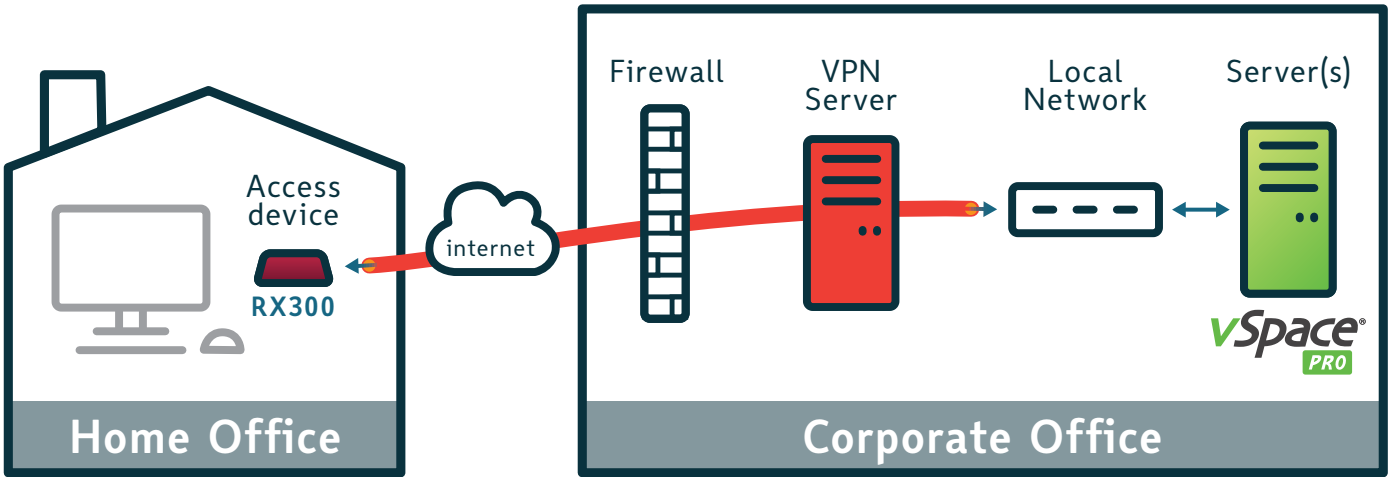
On-premise deployment

- 13. Netscaler/gateway

Citrix Cloud deployment

- 14. Citrix Gateway service

Scenario 1: vSpace Pro - VPN



Profile:

- Small to medium-sized office network
- Virtual Private Network (VPN) infrastructure
- Need access to internal resources

General description:

VPN allows individuals to establish secure connections with a remote computer network. They can access the protected resources on that network as if they connect directly to the network's servers. Customers who deploy vSpace Pro software can access their user sessions remotely via *NComputing* thin clients that support VPN.

Setup process:

1. Setup and initialize the VPN Server, including the VPN Server IP address, creating a DHCP pool to be used by connecting clients, and choosing the desired encryption type.
2. Create user accounts. Input a username, create a password for the user, and select if the user will have access to the local network or just to the router.
3. Configure thin clients to connect. Typically, all that is required is the VPN server address, username, and password.

Supported access devices:

- **RX300** thin client
- **RX-RDP**+ thin client
- **RX420**(RDP) thin client
- **LEAF OS** software
- **vSpace Pro Client** for Windows & Chromebook

Virtualization platforms:

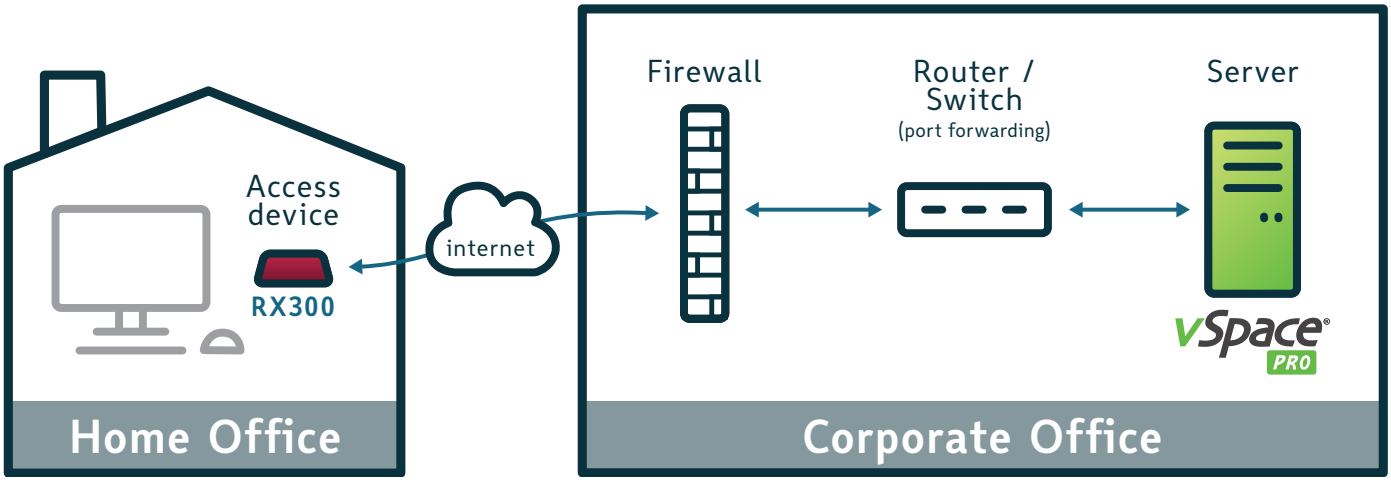
- **vSpace Pro Enterprise**

Implementation considerations:

- **VPN adds additional layers of protection:**
  - There is only one open port which is username and password protected.
  - All traffic to and from private network is encrypted.
  - Internal resources are password protected.
- Allows access to all deployed vSpace Pro servers and internal resources.
- Moderately simple configuration. User information is required, but no need for internal resource information.
- Older *NComputing* access device families (**L-series**, **M300**, **MX-series**) do not support VPN.
- Must have sufficient VPN seat licenses.
- Traffic to and from the internal network may be slightly slower due to the encryption process.

Additional resources: See Appendix A

Scenario 2: vSpace Pro - Port Forwarding



Profile:

- Small to medium-sized office network
- No Virtual Private Network (VPN) infrastructure
- Need access to internal resources

General description:

Customers who deploy vSpace Pro software can access their user sessions remotely via the router port forwarding method.

Port forwarding maps the port on your router's IP address (your public IP) to the port and IP address of the vSpace Pro server you want to access. The port forwarding rule intercepts the data traffic heading to your company's router public IP address and redirects it to the internal vSpace Pro server IP address. This allows *NComputing* thin clients in a public network to connect to the vSpace Pro server in the private network.

Typically your ISP uses Network Address Translation (NAT) to provide Internet connectivity through your router. Configuration changes to your router are usually required to enable the Port Forwarding option.

Setup process:

1. Find the internal IP address of your **vSpace Pro** server.
2. Find the public address of your router.
3. Create port forwarding rules (port 27605) in your router.
4. Optionally set up Dynamic DNS (DDNS) for the router IP address (i.e., don't need to worry about changing router public IP address by your ISP provider)
5. Configure the *NComputing* thin clients to connect to your router's public IP address and/or router's DDNS.

Warning: you're opening your PC up to the Internet – make sure you have a strong password set of your PC.

Supported access devices:

- **RX300**, **RX-RDP+**, **L250**, **L300**, **L350**, **M300**, **MX100** thin clients
- **LEAF OS** software
- **vSpace Pro Client** for Windows & Chromebook

Virtualization platforms:

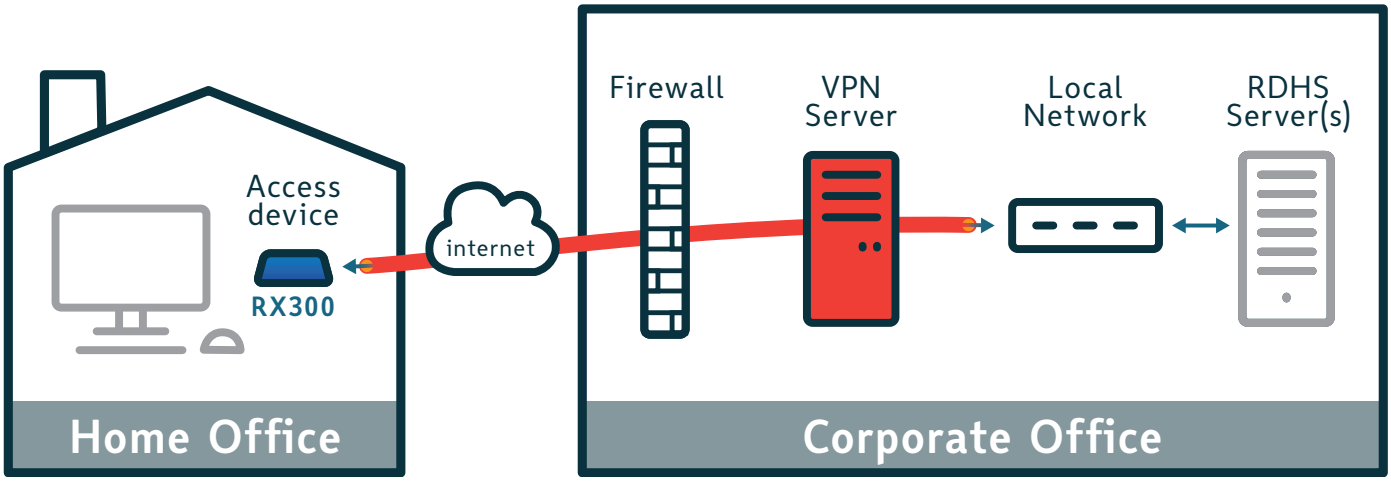
- **vSpace Pro Enterprise**

Implementation considerations:

- Easy to configure.
- Forwards the user to the private network without requiring a password.
- Works with Dynamic DNS.
- Supports all *NComputing* clients compatible with vSpace Pro.
- Safety depends on how good the router's firewall is; Must require a strong password set for your users' accounts.
- Not all traffic is encrypted.
- User session performance may be impacted by latency.
- Access to multiple vSpace Pro servers requires multiple port forwarding rules.

Additional resources: See Appendix A

Scenario 3: Microsoft RDS - VPN



Profile:

- Small to medium-sized office network
- No RD Gateway setup
- Virtual Private Network (VPN) infrastructure
- Need access to internal resources

General description:

Customers who deploy RDSH servers can access their user sessions remotely via *NComputing* thin clients that support VPN.

VPN allows individuals to establish secure connections with a remote computer network. They can access the protected resources on that network as if they connect directly to the network's servers.

Setup process:

1. Setup and initialize the VPN Server, including the VPN Server IP address, creating a DHCP pool to be used by connecting clients, and choosing the desired encryption type.
2. Create user accounts. Input a username, create a password for the user, and select if the user will have access to the local network or just to the router.
3. Configure thin clients to connect. Typically, all that is required is the VPN server address, username, and password.

Supported access devices:

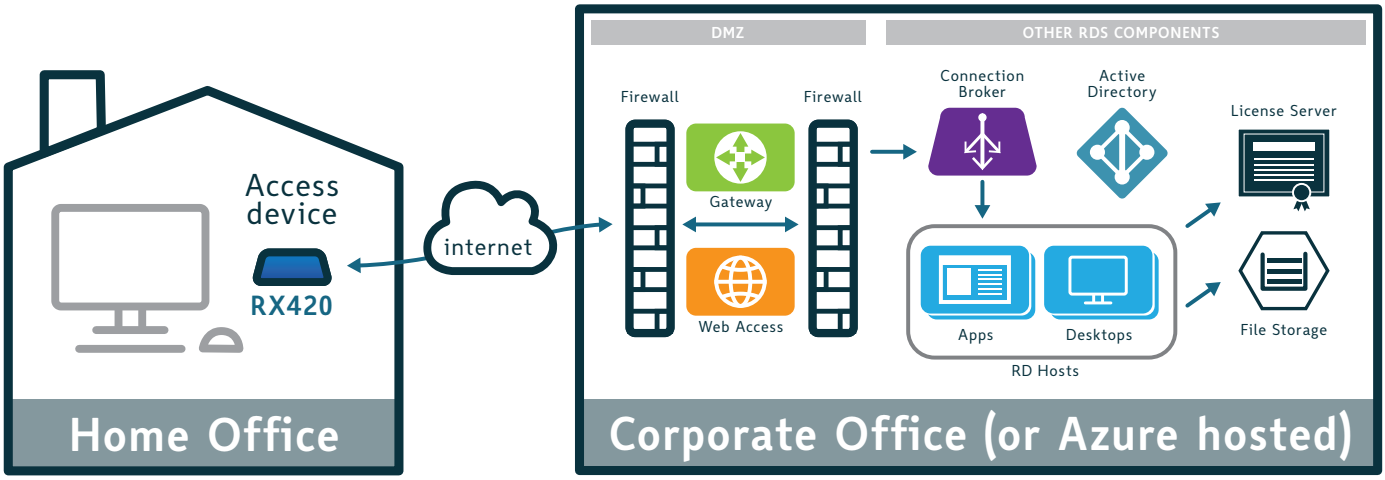
- **RX-RDP, RX420(RDP), RX300** thin clients.
- **LEAF OS** software

Implementation considerations:

- **VPN adds additional layers of protection:**
  - There is only one open port which is username and password protected.
  - All traffic to and from private network is encrypted.
  - Internal resources are password protected.
- Gain access to all deployed RDSH servers and internal resources.
- Moderately simple configuration. User information is required, but no need for internal resource information.
- Must have sufficient VPN seat licenses.
- Traffic to and from the internal network may be slightly slower due to the encryption process.

Additional resources: See Appendix A

Scenario 4: Microsoft RDS - RD Gateway



Profile:

- Small to medium-sized office network
- RD Gateway setup
- No Virtual Private Network (VPN) infrastructure
- Need access to internal resources

General description:

Remote Desktop Gateway is used to allow secure connections using HTTPS encryption from computers outside the corporate network. The configuration was simplified, beginning with Windows Server 2012.

Setup process:

1. Install the RD Gateway service in Windows Server (requires an existing RDS deployment).
2. Set up an SSL certificate for the RD Gateway server. (SSL certificates are used to encrypt communications between RDS thin clients and RD Gateway servers. The self-signed SSL certificate name must match the fully qualified domain name (FQDN) of the RD Gateway server.
3. Run RD Gateway Manager and setup both 'Connection Authorization policy' and 'Resource Authorization policy.'
4. Enable/forward TCP port 443 on your firewall to the RD Gateway server.
5. Export self-signed public certificates and copy them to supported thin clients.
6. Configure thin clients to talk to the RD Gateway by entering the FQDN name.

Supported access devices:

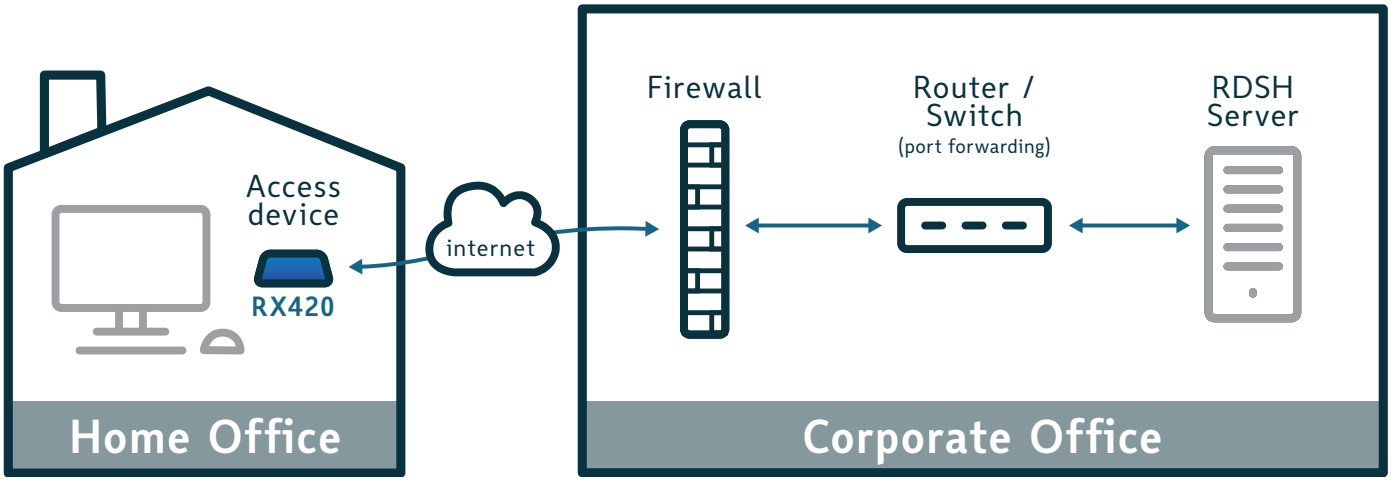
- **RX-RDP**, **RX-RDP+**, **RX420**(RDP), **RX300** thin clients
- **LEAF OS** software

Implementation considerations:

- No VPN required.
- Allows remote connections through the firewall (without opening port 3389).
- Supported by all *NComputing* RDP-ready clients.
- Flexible deployment (on-prem or Cloud).
- Extra steps to setup RD Gateway and certificate management.

Additional resources: See Appendix A

Scenario 5: Microsoft RDS - Port Forwarding



Profile:

- Small to medium-sized office network
- No RD Gateway setup
- No Virtual Private Network (VPN) infrastructure
- Need access to internal resources

General description:

Customers who deploy RDSH servers can access their user sessions remotely via the router port forwarding method. However, this approach can result in security vulnerabilities (port 3389 forwarding) and should be the last option if the customer does not have RD Gateway or VPN infrastructure. The admin should re-enforce a strong password set for accounts to help mitigate security vulnerability.

Port forwarding maps the port on your router's IP address (your public IP) to the port and IP address of the RDSH server you want to access. The port forwarding rule intercepts the data traffic heading to your company's router public IP address and redirects it to the internal RDSH server IP address. This allows *NComputing* thin clients in a public network to connect to the RDSH server in the private network.

Typically your ISP uses Network Address Translation (NAT) to provide Internet connectivity through your router. Configuration changes to your router are usually required to enable the Port Forwarding option.

Setup process:

1. Find the internal IP address of your RDSH Server.
2. Find the public address of your router.
3. Create port forwarding (port 3389) rules in your router.
4. Optionally set up Dynamic DNS (DDNS) for the router IP address (i.e., don't need to worry about changing router public IP address by your ISP provider)
5. Configure the *NComputing* thin clients to connect to your router's public IP address and/or router's DDNS.

Warning: you're opening your PC up to the Internet – make sure you have a strong password set of your PC.

Supported access devices:

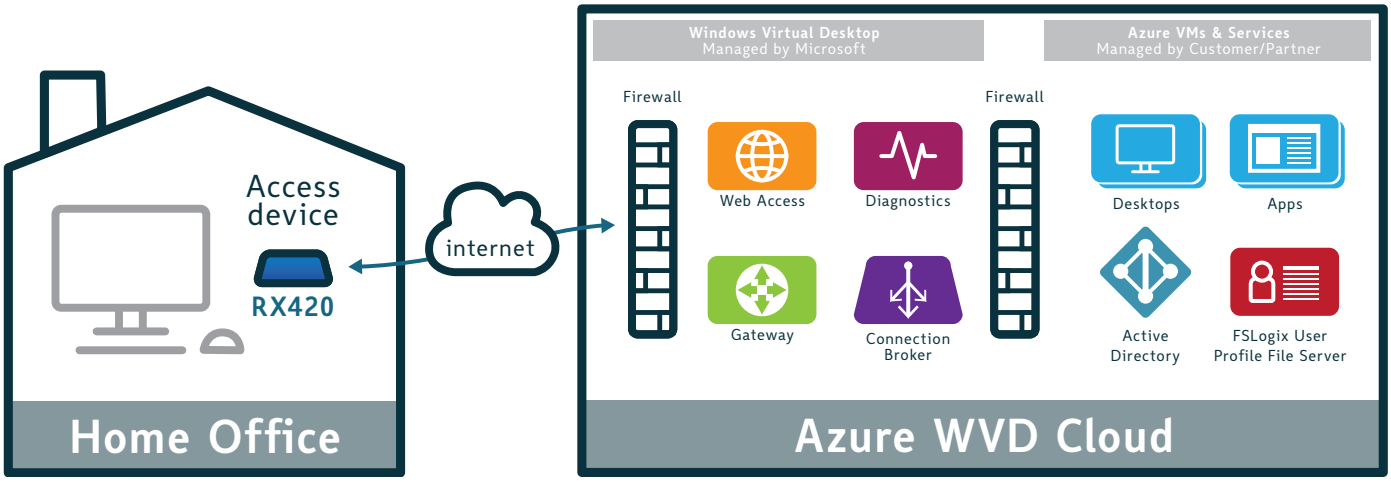
- **RX-RDP**, **RX-RDP+**, **RX420**(RDP), **RX300** thin clients
- **LEAF OS** software

Implementation considerations::

- Easy to configure.
- Only requires RDSH server address and port.
- Works with Dynamic DNS.
- Safety depends on the quality of the firewall;
- Requires strong user passwords (may be vulnerable to brute force attack).
- User session performance may be impacted by latency.

Additional resources: See Appendix A

Scenario 6: Microsoft Virtual Desktop (WVD) – Azure Cloud



Profile:

- Small to medium-sized office network
- Interested in DaaS (Desktop as a Service)
- No on-premise Microsoft RDS
- No Virtual Private Network (VPN) infrastructure
- Need access to internal resources

General description:

Windows Virtual Desktop (WVD) is a desktop and app virtualization service run and hosted by Microsoft on its Azure cloud. It allows the setup of multi-session Windows 10 desktops along with virtual office 365 ProPlus with eligible Microsoft licenses.

Setup process:

1. WVD initial setup with Azure and registration.
2. Prepare WVD environment with PowerShell & setup Windows Virtual Desktop tenant.
3. Configure Domain Controller and Virtual Machines (e.g. VM, disk, network configuration, etc.).
4. Set up VPN (resources, certificates, etc.).
5. Complete Windows Virtual Desktop configuration (e.g. Domain Controller, Azure AD, VMs, Assign Users, Publish Apps, etc.)

Supported access devices:

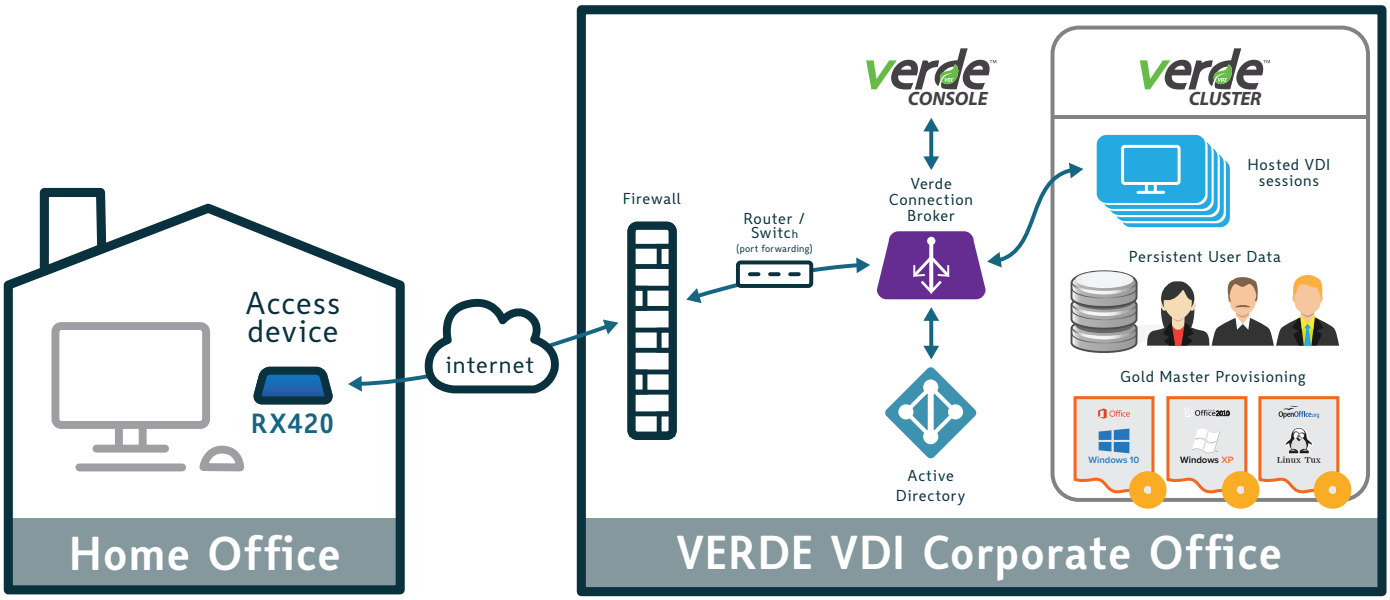
- **RX-RDP+**, **RX420**(RDP)
- **LEAF OS** software

Implementation considerations:

- Easy user accessibility from anywhere.
- Built-in security/firewall without VPN or port forwarding.
- Scalable and highly available by design.
- Data hosted by 3rd party (Microsoft), no local backup
- End user experience may be affected by Azure availability regions.
- Low start up cost, but higher cost of ownership over time.

Additional resources: See Appendix A

Scenario 7: VERDE VDI – VM Sessions only: port forwarding



Profile:

- Small to medium-sized office network
- No Virtual Private Network (VPN) infrastructure
- Need affordable VDI

General description:

The **VERDE VDI** desktop virtualization platform by *NComputing* is a purpose built, all-in-one solution that delivers a persistent, personalized desktop experience. **VERDE VDI** provides a secure, easy-to-use, enterprise-grade virtual desktop infrastructure at a very affordable price. **VERDE VDI** delivers Windows and Linux virtual desktops and is ideal for small-and medium-size business.

Customers who deploy **VERDE VDI** can access their VDI session remotely via the router port forwarding method.

Customers can optionally enable the VERDE Gateway Feature to provide an additional layer of security and control for remote access. The VERDE Gateway Feature comes with the **VERDE VDI** solution.

Setup process:

1. Setup & deploy VERDE VDI.
2. Find the internal IP address of your VERDE Connection Broker.
3. Find the public address of your router.
4. Create port forwarding rules 8443 and 48622 in your router.
5. Optionally setup Dynamic DNS (DDNS) for your router IP address (i.e., don't need to worry about changing router public IP address by your ISP provider).
6. *NComputing* thin clients connect to your router's public IP address and/or router's DDNS.

Supported access devices:

- **RX-RDP**, **RX420**(RDP), **RX300** thin clients
- **LEAF OS** software
- VERDE Windows client

Virtualization platforms:

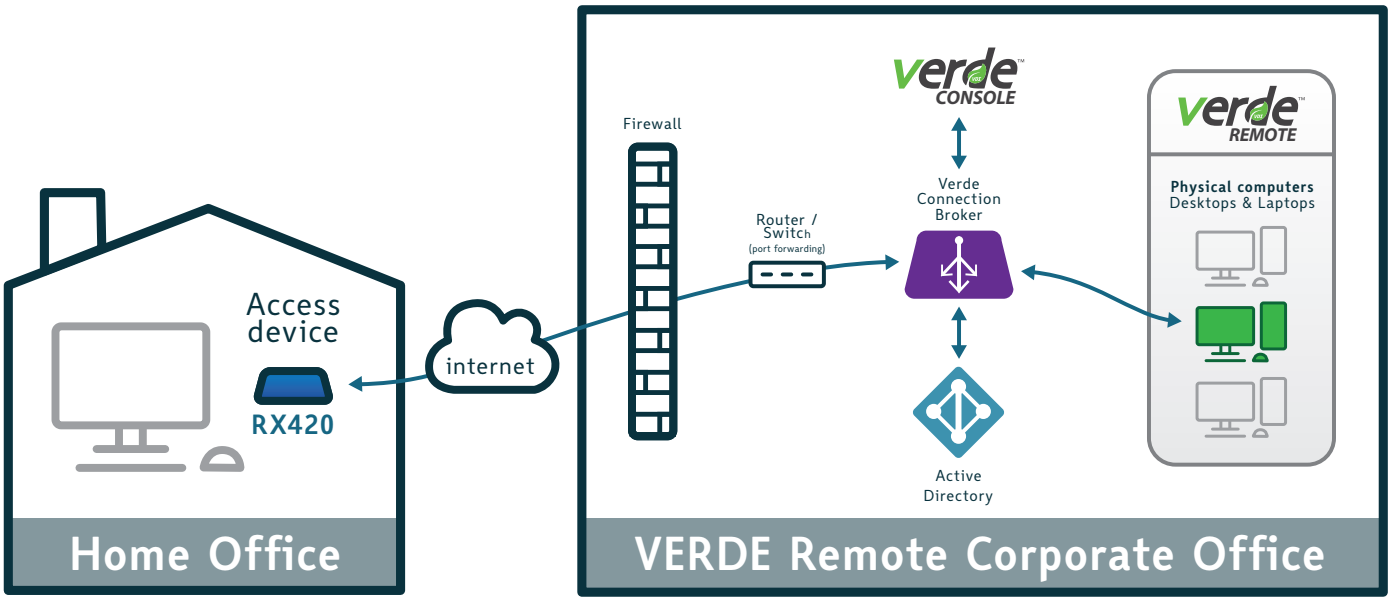
- VERDE VDI

Implementation considerations:

- End-to-end SSL encrypted traffic without VPN.
- True VDI solution, easier to setup and deploy.
- Costs less than other VDI solutions
- (Optional) VERDE Gateway feature provides an additional layer of security and control for remote access.
- VERDE Connection Broker may be exposed.

Additional resources: See Appendix A

Scenario 8: VERDE VDI – Remote PCs only: port forwarding



Profile:

- Small to medium-sized office network
- No Virtual Private Network (VPN) infrastructure
- Need access to existing physical PCs in the office.

General description:

VERDE Remote Access is an easy to deploy Linux virtual appliance that is installed in a customer's environment. It allows users at home to connect to their PC in the corporate office and use it as if they were sitting in front of it.

The VERDE Remote Access feature is configured by an administrator to define connection criteria. All data traffic is securely encrypted, protecting the physical PCs from unauthorized remote access.

The administrator can easily monitor connection status of the physical PCs and, if necessary, force a disconnection or shutdown.

Customers can also enable the VERDE Gateway Feature to provide an additional layer of security and control for remote access. The VERDE Gateway Feature is part of **VERDE VDI**.

Setup process:

1. Setup & deploy VERDE Remote Access.
2. Find the internal IP address of your VERDE Connection Broker.
3. Find the public address of your router.
4. Create port forwarding rules 8443 and 48622 in your router.
5. Optionally setup Dynamic DNS (DDNS) for your organization's router IP address (i.e. don't need to worry about changing router public IP address by your ISP provider)
6. Connect your thin clients to your router's public IP address and/or router's DDNS.

Supported access devices:

- **RX-RDP**, **RX-RDP+**, **RX420**(RDP), **RX300** thin clients
- **LEAF OS** software
- VERDE Windows client

Virtualization platforms:

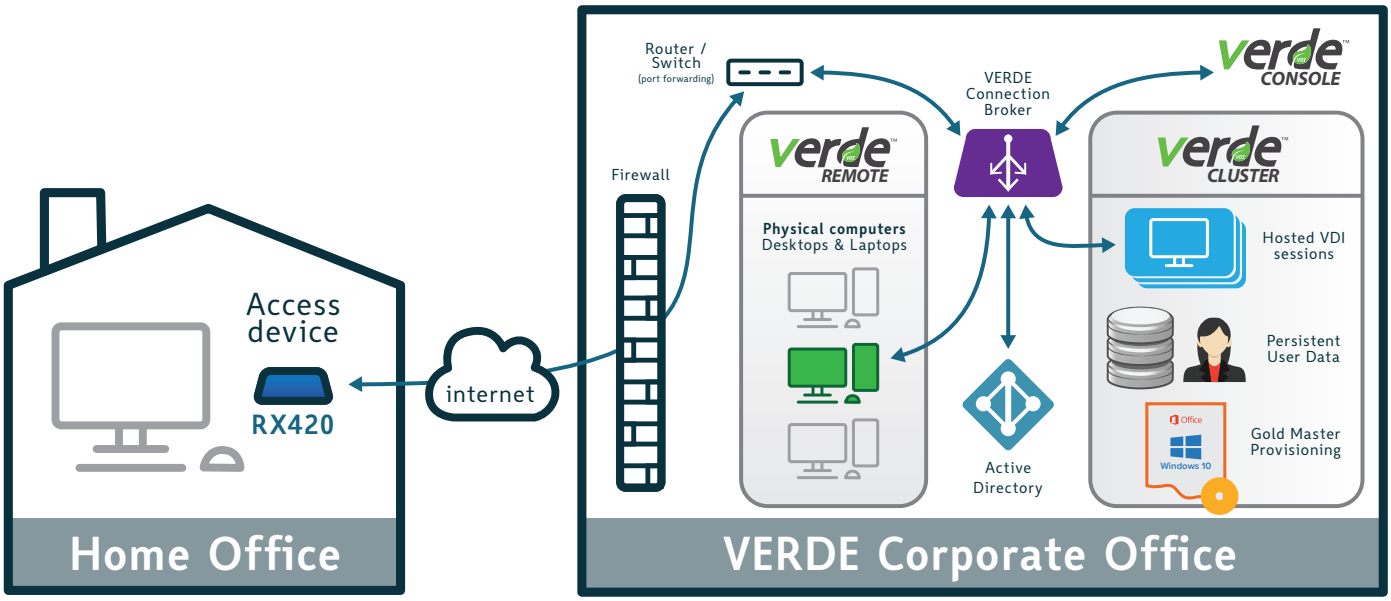
- VERDE VDI with Remote Access

Implementation considerations:

- Secure remote access. End-to-end SSL encrypted traffic between access device and physical PCs with no VPN.
- Minimal infrastructure required.
- (Optional) VERDE Gateway feature to provide an additional layer security and control for remote access.
- VERDE Connection Broker may be exposed.
- Remote PC must stay powered on.

Additional resources: See Appendix A

Scenario 9: VERDE VDI – VM Sessions & Remote PCs: port forwarding



Profile:

- Small to medium-sized office network
- No Virtual Private Network (VPN) infrastructure
- Need access to existing physical PCs in the office
- Need access to internal resources
- Need affordable VDI

General description:

VERDE VDI can also be deployed to provide hybrid VDI sessions and remote computer access to through the same secure VERDE Connection Broker.

VERDE VDI provides a secure, easy-to-use, enterprise-grade virtual desktop infrastructure. **VERDE VDI** delivers Windows and Linux virtual desktops.

VERDE Remote Access feature can be configured by an administrator to define connection criteria allowing a remote user to connect to their physical PC, Desktop or Laptop in the corporate office. All data traffic is securely encrypted and transmitted through the VERDE Remote Access appliance thereby protecting the physical PCs from unauthorized remote access.

Extensive monitoring and control for IT admins can be done with VERDE Console.

Customers can optionally enable the VERDE Gateway Feature to provide an additional layer of security and control for remote access. The VERDE Gateway Feature is part of **VERDE VDI**.

Setup process:

Refer to steps from Scenario 7 & 8.

Supported access devices:

- **RX-RDP**, **RX-RDP+**, **RX420**(RDP), **RX300** thin clients
- **LEAF OS** software
- VERDE Windows client

Virtualization platforms:

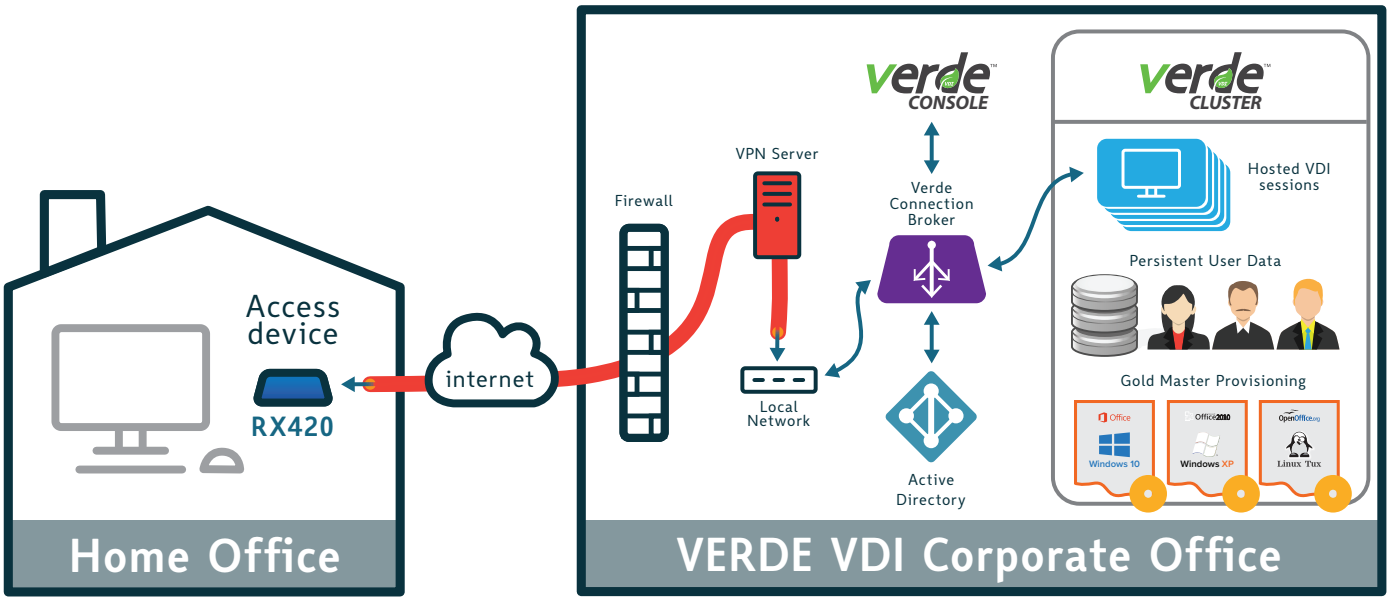
- VERDE VDI with Remote Access*

Implementation considerations:

- Fully SSL encrypted traffic from *NComputing* access device to VERDE.
- Flexible deployment with hybrid VDI sessions and remote access to physical computers.
- Extensive monitoring and control for IT admins using VERDE Console.
- (Optional) VERDE Gateway feature to provide an additional layer security and control for remote access.
- VERDE Connection Broker may be exposed
- Remote PC must stay on

Additional resources: See Appendix A

Scenario 10: VERDE VDI – VM Sessions only: VPN



Profile:

- Small to medium-sized office network
- Virtual Private Network (VPN) infrastructure
- Need affordable VDI

General description:

The **VERDE VDI** desktop virtualization platform by *NComputing* is a purpose built, all-in-one solution that delivers a persistent, personalized desktop experience across popular *NComputing* thin clients and software clients. **VERDE VDI** provides a secure, easy-to-use, enterprise-grade virtual desktop infrastructure at a very affordable price. **VERDE VDI** delivers Windows and Linux virtual desktops and ideal for small-and medium-size business.

Customers who deploy **VERDE VDI** can access their VDI session remotely to the VERDE Connection Broker via *NComputing* clients with VPN support.

VPN (Virtual Private Network) allows individual users to establish secure connections with a remote computer network. Those users can access the secure resources on that network as if they were directly plugged in to the network's servers. *NComputing* clients with integrated VPN enables employees to securely access their **VERDE VDI** virtual desktops in the private network.

Setup process:

1. Prerequisite – setup & deploy VERDE VDI - Online Setup Guide
2. **Setup and initialize the VPN Server:** This step includes setting the VPN Server IP address, creating a DHCP pool to be used by connecting clients, and choosing the desired encryption type.
3. **Create user accounts:** Input a username, create a password for the user, and select if the user will have access to the local network or just to the router.
4. Configure supported *NComputing* thin client with integrated VPN client. Typically, all that is required is VPN server address, username, and password.

Supported access devices:

- **RX-RDP**, **RX-RDP+**, **RX420**(RDP), **RX300** thin clients
- **LEAF OS** software
- VERDE Windows client

Virtualization platforms:

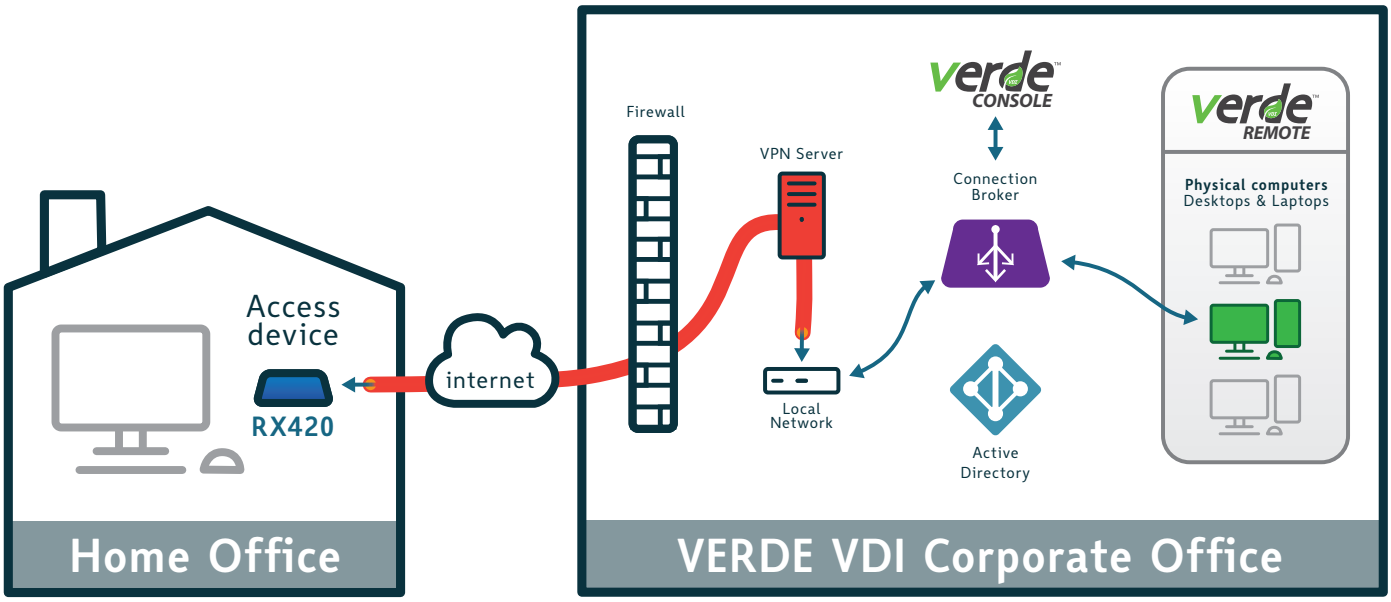
- VERDE VDI

Implementation considerations:

- Full access to local network resources.
- Additional security layers of protection through VPN tunnel.
- True VDI solution, easier to setup and deploy
- Costs less compared to other VDI Solutions.
- Need to have sufficient VPN license seats

Additional resources: See Appendix A

Scenario 11: VERDE VDI – Remote PCs only: VPN



Profile:

- Small to medium-sized office network
- Virtual Private Network (VPN) infrastructure
- Need access to existing physical PCs in the office

General description:

VERDE Remote Access feature is an easy to deploy Linux virtual appliance software installed in a customer's environment.

The VERDE Remote Access feature can be configured by an administrator to define connection criteria allowing a remote user to connect to their physical PC, Desktop or Laptop in the corporate office. All data traffic is securely encrypted and transmitted through the VERDE Remote Access appliance thereby protecting the physical PCs from unauthorized remote access.

The administrator can easily monitor connection status of the physical PCs and, if necessary, force a disconnection or shutdown of the PC.

One of the primary benefits of the VERDE Remote Access feature is that there is no requirement for extensive hardware infrastructure when compared to a standard VDI deployment.

Customers who deploy VERDE Remote Access can securely access their physical PC/laptop remotely to the VERDE Connection Broker via *NComputing* clients with VPN support.

Setup process:

1. Setup & deploy VERDE VDI
2. **Setup and initialize the VPN Server:** This step includes setting the VPN Server IP address, creating a DHCP pool to be used by connecting clients, and choosing the desired encryption type.
3. **Create user accounts:** Input a username, create a password for the user, and select if the user will have access to the local network or just to the router.
4. Configure supported *NComputing* thin client with integrated VPN client. Typically, all that is required is VPN server address, username, and password.

Supported access devices:

- **RX-RDP**, **RX-RDP+**, **RX420**(RDP), **RX300** thin clients
- **LEAF OS** software
- VERDE Windows client

Virtualization platforms:

- VERDE VDI with Remote Access*

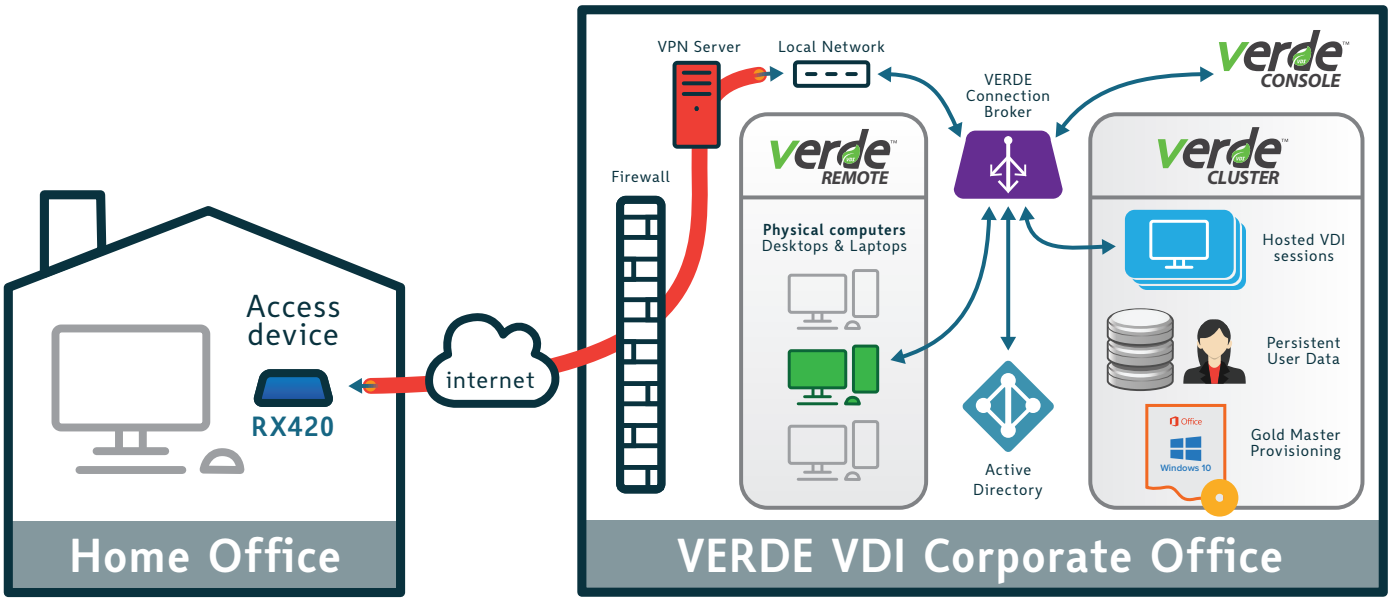
Implementation considerations:

- Full access to local network resources.
- Additional security layers of protection through VPN tunnel.
- Minimal infrastructure compared to full VDI.
- Need to have sufficient VPN license seats
- Remote PC must stay on

*

Additional resources: See Appendix A

Scenario 12: VERDE VDI – VM Sessions & Remote PCs: VPN



Profile:

- Small to medium-sized office network
- Virtual Private Network (VPN) infrastructure
- Need access to existing physical PCs in the office
- Need access to internal resources
- Need affordable VDI

General description:

VERDE VDI can also be deployed to provide hybrid VDI sessions and remote computer access to through the same secure VERDE Connection Broker, with VPN infrastructure.

VERDE VDI provides a secure, easy-to-use, enterprise-grade virtual desktop infrastructure. **VERDE VDI** delivers Windows and Linux virtual desktops.

VERDE Remote Access feature can be configured by an administrator to define connection criteria allowing a remote user to connect to their physical PC, Desktop or Laptop in the corporate office. All data traffic is securely encrypted and transmitted through the VERDE Remote Access appliance thereby protecting the physical PCs from unauthorized remote access.

Extensive monitoring and control for IT admins can be done with VERDE Console.

Setup process:

Refer to setup steps for Scenario 10 & 11.

Supported access devices:

- **RX-RDP**, **RX420**(RDP), **RX300** thin clients
- **LEAF OS** software
- VERDE Windows client

Virtualization platforms:

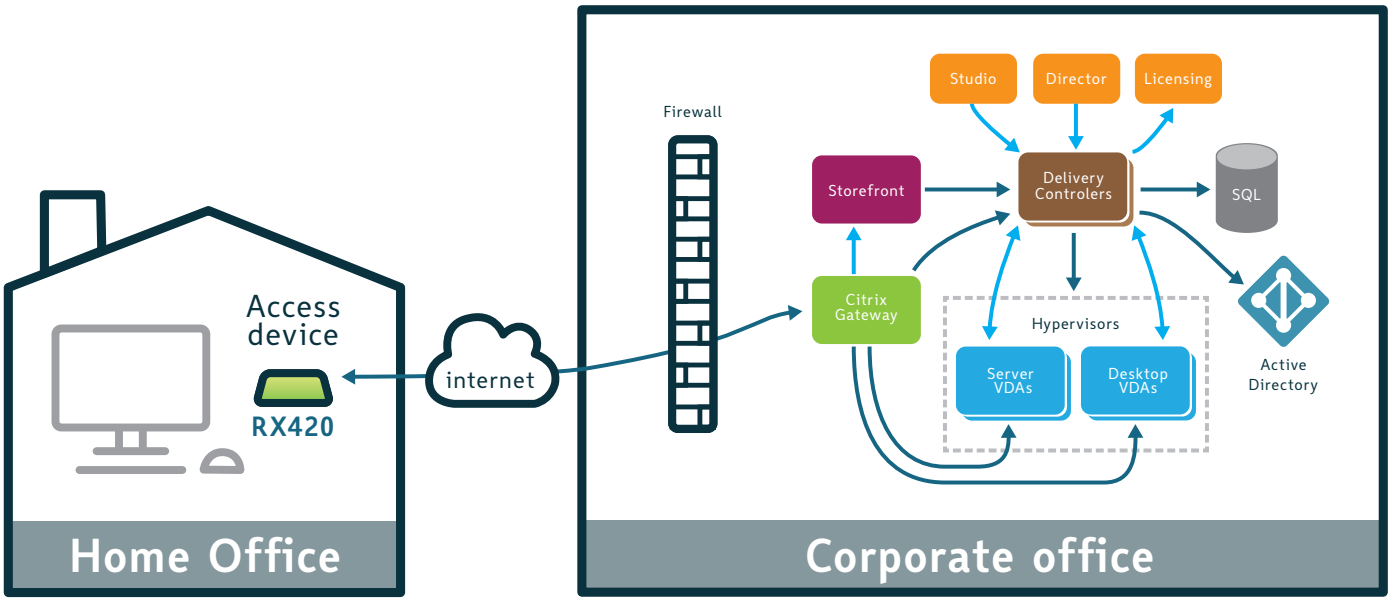
- VERDE VDI with Remote Access*

Implementation considerations:

- Full access to local network resources.
- Additional security layers of protection through VPN tunnel.
- Flexible deployment with hybrid VDI sessions and remote access to physical computers.
- Minimal infrastructure compared to full VDI.
- Extensive monitoring and control for IT admins using VERDE Console.
- Need to have sufficient VPN license seats
- Remote PC must stay on

Additional resources: See Appendix A

Scenario 13: Citrix VDI –On-premise



Profile:

- Medium and large organizations
- On-premise Citrix VDI deployment
- Need remote access to Virtual Apps & Desktops or Citrix Workspace.

General description:

A traditional Citrix deployment for apps and desktops consists of delivery controllers, StoreFront servers, a highly available SQL database, Studio and Director consoles, a License Server, and Citrix Gateway. These components are part of the management plane or control plane for the environment and are deployed at a data center or cloud that is a customer or partner-managed.

Citrix Gateway consolidates remote access infrastructure to provide single sign-on across all applications whether in a datacenter, in a cloud, or delivered as SaaS. It allows people to access any app, from any device, through a single URL. Citrix Gateway is easy to deploy and simple to administer. The most typical deployment configuration is to locate the Citrix Gateway appliance in the DMZ. *NComputing* RX-HDX, RX-HDX+, RX420(HDX) and EX400 thin clients are optimized for Citrix deployment.

Supported access devices:

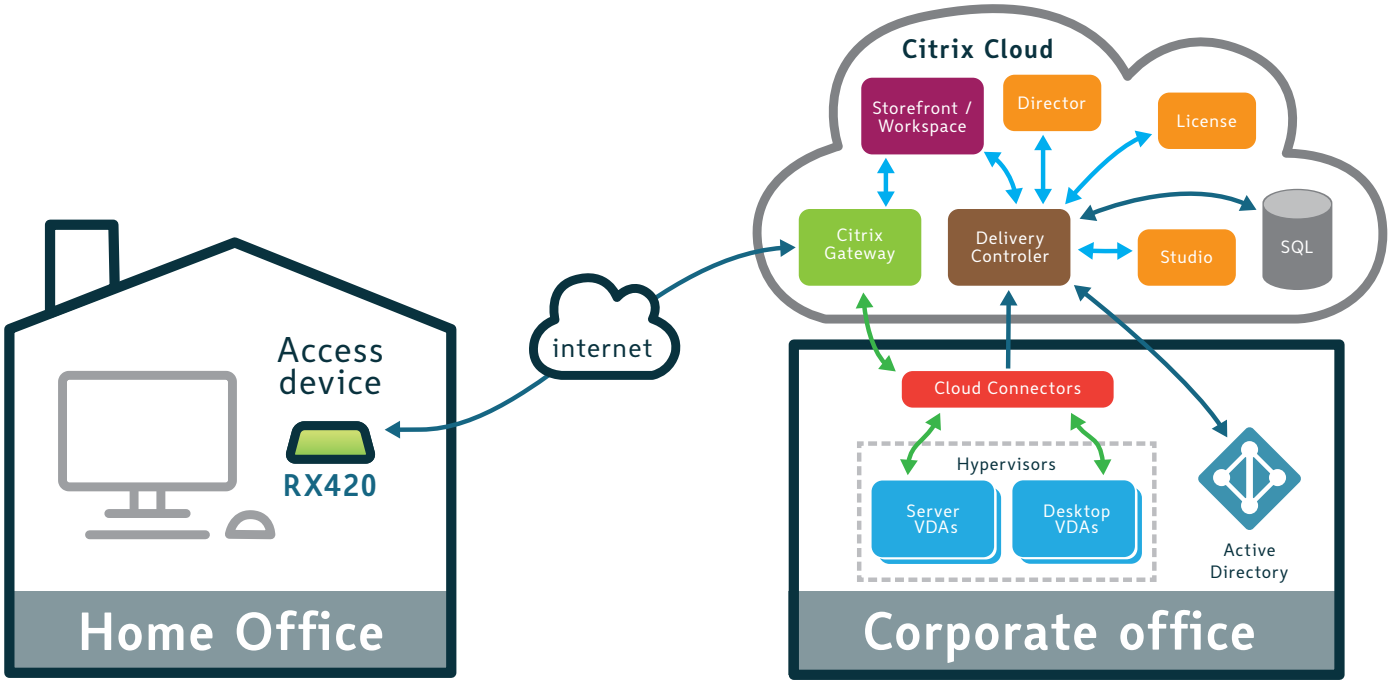
- **RX-HDX**, **RX-HDX+**, **RX420**(HDX), **RX420**(STDK), EX400 thin clients

Implementation considerations:

- Secure access through Citrix Gateway; VPN or port forward not required.
- *NComputing* clients have the Integrated Citrix Workspace App to provide Virtual Apps & Desktops support for on-premise or cloud deployment.
- Simple *NComputing* device setup.
- More complex to setup, deploy and maintain back-end infrastructure.
- Higher Cost; significant CAPEX investment.

Additional resources: See Appendix A

Scenario 14: Citrix – Citrix Cloud



Profile:

- Medium and large organizations
- Hyprid cloud or Citrix Cloud deployment
- Need remote access to Virtual Apps & Desktops or Citrix Workspace.

General description:

Citrix Cloud is a cloud-based platform comprised of various service offerings. Many of these services function as a management plane that is kept evergreen by Citrix with the workloads and data residing in the data center or cloud of the customer's choice. This approach allows customers to focus on the most strategic part of IT and resource delivery with the security, availability, and functionality that business demands.

In this case, customers don't handle the core product installation, setup, configuration, upgrades, monitoring, or scaling of the management plane as that is all left to Citrix to manage and maintain.

The customer can either deploy Citrix Gateway on-premise or in Citrix Cloud. Citrix Gateway allows employees to access any app, from any device, through a single URL. *NComputing* RX-HDX, RX-HDX+, RX420(HDX) and EX400 thin clients are optimized for Citrix deployment, regardless if it is on-premise, hybrid cloud or Citrix Cloud deployment.

Supported access devices:

- **RX-HDX**, **RX-HDX+**, **RX420**(HDX), EX400 thin clients

Implementation considerations:

- Key Citrix software managed and hosted by Citrix Cloud
- Secure access to Citrix Gateway service from anywhere.
- Easier setup & deployment
- Simple *NComputing* device setup.
- Low start-up cost, but higher cost of ownership over time.

Additional resources: See Appendix A

Appendix A: Additional Resources

NComputing access device compatibilities:

- NComputing access device comparison matrix
- vSpace Pro compatibility matrix
- VERDE VDI compatibility matrix

Scenarios 1, 3, 10, 11, 12:

- 3rd party OpenVPN access server & hosting solution (not affiliated with *NComputing*)
  - https://openvpn.net/virtual-appliances/
  - https://www.turnkeylinux.org/openvpn
  - https://doc.zentyal.org/en/vpn.html

Scenario 2:

- **KB article:** How to access vSpace Pro host machines with port forwarding

Scenario 4:

- Microsoft guide on Deploy your Remote Desktop environment

Scenario 5:

- **KB article:** How to access RDSH host machines with port forwarding

Scenario 6:

- Windows Virtual Desktop overview
- Getting started with Windows Virtual Desktop
- WVD Walkthrough guide

Scenarios 7, 9:

- VERDE VDI datasheet
- VERDE VDI installation guide
- VERDE VDI documentation

Scenario 13:

- Citrix Gateway documentation
- Citrix Virtual Apps and Desktops Technical Overview

Scenario 14:

- Citrix Virtual Apps and Desktops Service Reference Architecture and Deployment Methods