Your Trusted Premier IT Partner

The Ultimate Guide to Setting Up Remote Network Access During the CV19 Crisis

Critical Facts and Insider Secrets Every Small Business Owner Must Know Before Installing a 'Virtual Network' to Allow Employees to Work from Home

Author: Tom Donohue
Stryker Networks LLC
www.strykernetworks.com

The Ultimate Guide to Setting Up Remote Network Access During the CV19 Crisis

Critical Facts and Insider Secrets Every Small Business Owner *Must* Know Before Installing a 'Virtual Network' to Allow Employees to Work from Home

If you are the owner or manager of small to mid-sized business and have been forced to implement a "work from home" program for your employees – DON'T - until you read this eye-opening guide.

This report will explain in plain, non-technical terms, the best practices for setting up remote access for you and your staff, as well important questions you should ask to avoid making the most common, costly mistakes made when setting up technology for a work from home program.

You'll Discover:

- How to keep your staff productive despite the upheaval in today's workplace
- How to securely connect remote computers to your office network
- Three different methods for accessing your office network
- How to protect your office computers from outside attacks
- **How to get your FREE network review and "Home Office Action Pack" ($197 Value).**

Provided as an educational service by:

Stryker Networks LLC
1827 Walden Office Square
Suite 555
Schaumburg, IL 60173
847-908-3210
http://www.strykernetworks.com

Key Considerations for Implementing Remote Staffing

The challenge being faced by every business owner and manager today is how to best deliver quality goods and services in a socially distanced, distributed, and remote environment. These challenges can be broken down into categories:

Psychological: Providing your team a sense of "togetherness" and normalcy while implementing a new, abnormal workflow.

Security and compliance: Ensuring that you remain compliant (if you are regulated) and that corporate information is protected and private.

Communication: Implementing a distributed office in the most personable and accessible way possible.

Systems Access: Architecting a secure, practical, and efficient capability to access customer and business records.

Legal: Maintaining accurate policies and records to protect business assets.

Technology's Role in Supporting Employee Mental Health

Many people underestimate the impact that technology has on the psychological wellbeing of the workforce. Stress levels are well above average and feelings of loneliness, isolation, and disconnection are common. By providing a well-planned work from home strategy, businesses can maximize productivity while minimizing anxiety.

When planning a remote-work architecture, care should be taken to provide workflows and tools that are as close to the office environment as possible. Considerations include:

- Access to systems and data such that function, speed, and accessibility are optimized
- Problematic issues such as copy, print, fax, and scan are identified and resolved with new workflows
- Communication with staff is increased and personalized with video and phone calls rather than email and text
- Encouragement from management to maintain discipline and routine
- More frequent staff meetings.

Providing Access to Applications, Data, and Files

Regardless of whether applications are on a laptop, an office network, or in the cloud, remote users rely on these tools to complete their daily tasks.. Efficiently delivering application and data resources is essential for a productive distributed workflow.

Cloud Based Applications

Many Email systems are cloud based and there is a growing trend towards moving ERP systems to the cloud as well. Transitioning staff to remotely access these applications is relatively seamless. Minimally, the employee would require:

- Secure Internet Access
- A workstation or laptop computer to access the internet

Security, storage, and disaster recovery are all performed by the host so the user experience should not be disrupted. Care should be taken to address possible compliance and ancillary device issues such as home computers being shared by others and unsecured internet access.

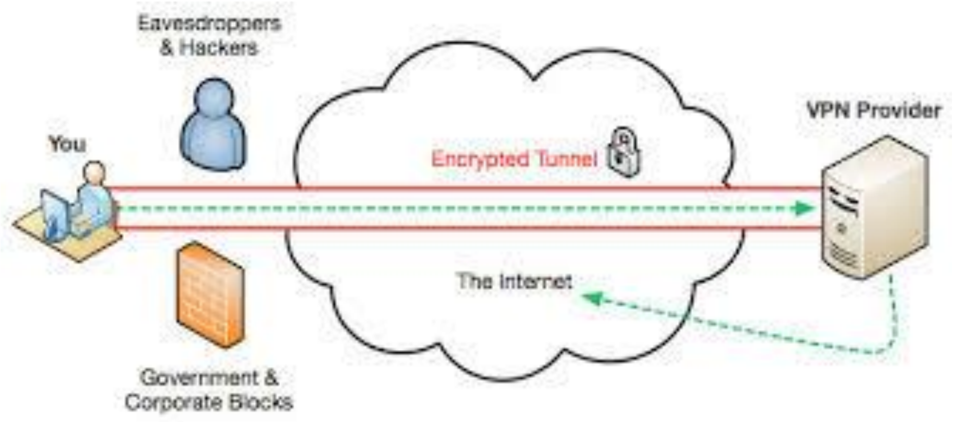
On-Premises Files and Applications.

Applications and data that are installed/stored at the business office (on-premise network) require additional forethought. There are different methods for accessing the network and each have their own cost/benefit. Regardless of the methods utilized, the network connection should be secure. This is accomplished with a Virtual Private Network (VPN).

A Virtual Private Network (VPN) is an encrypted link between the on-premises network and a remote user. The host network's firewall generates a unique piece of software (VPN client) which is installed on the remote workstation/laptop. When the remote user logs on to the VPN, they are establishing a secure tunnel between the business office and the remote workstation. Although data is transmitted through the internet, the data is encrypted and can only be read by the devices on either side of the VPN tunnel.

Beware! Once the VPN connection is made, the workstation is "on the network". This means that any virus, malware, or vulnerability on the workstation is now capable of reaching and infecting the office network. ***Only workstations that have proper***

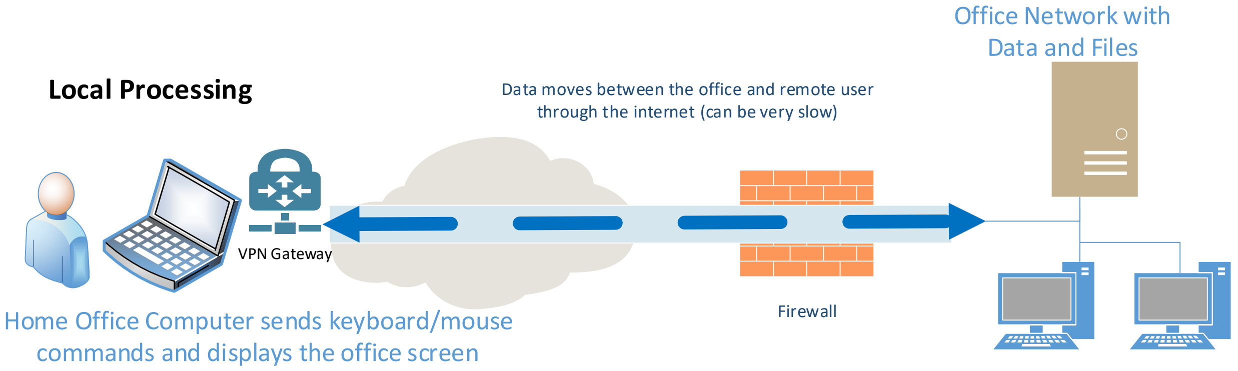
security, anti-virus, and patches should be permitted to access the practice office remotely.


Eavesdroppers & Hackers
You
Encrypted Tunnel
VPN Provider
The Internet
Government & Corporate Blocks

After a secure VPN connection has been established, there are several methods for utilizing network resources:

Local Processing at the Home Office

This is the simplest and most common method of network access. The home computer has programs such as Outlook, Excel, Word, and Acrobat which are installed and run on the local (home) machine. When the user requires files from the office system, they open them as they would if they were in the office. The VPN effectively creates a very long network cable connecting the home computer to the office network. Unfortunately, this very long cable (the internet) is not as fast as the office connection to the employee's desk in the office.

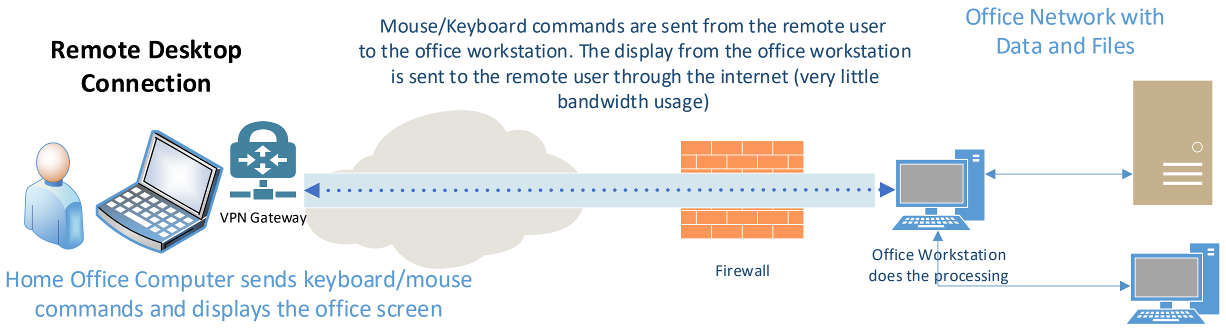

Office Network with Data and Files
Local Processing
Data moves between the office and remote user through the internet (can be very slow)
VPN Gateway
Firewall
Home Office Computer sends keyboard/mouse commands and displays the office screen

The available internet/Wi-Fi bandwidth and speed must be considered when processing files locally. Many data processing applications such as QuickBooks and MS Access move the data from the file server to the local machine for processing. While this is routine in an office with high speed cable connections, it can prove problematic with the limitations of internet and wireless connections. This solution is not recommended when the application connects to large data files or high definition images. Local processing is best used to add, edit, and delete small, individual files such as correspondence and spreadsheets. Typical uses would be the manipulation of Word and Excel documents.

As home computers are typically not included within a backup and disaster recovery plan, users should be instructed to save all files to the office network to ensure proper backup and security.

Remote Desktop Connection

If there is a workstation at the office that is accessible (powered on, connected to the network, and not in use by others) from the home office, the remote user could log on with a remote desktop connection (RDC). With RDC, the work, storage, and processing are done by the on-premises machine. The remote workstation merely relays keyboard/mouse commands and monitor output to/from the on-premises workstation/server.


Remote Desktop Connection
Mouse/Keyboard commands are sent from the remote user to the office workstation. The display from the office workstation is sent to the remote user through the internet (very little bandwidth usage)
Office Network with Data and Files
VPN Gateway
Firewall
Office Workstation does the processing
Home Office Computer sends keyboard/mouse commands and displays the office screen

This solution is preferred over the remote processing solution for the following reasons:

- Requires less internet bandwidth

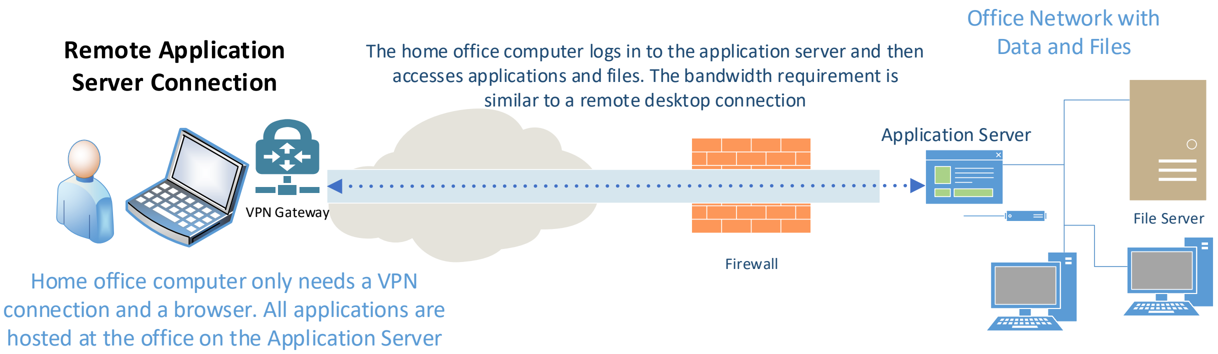
- Data and files are not transmitted or stored on the home workstation – only the screen image.
- The business' backup and disaster recovery policies are maintained
- Reduces the possibility of data corruption/compromise if the home workstation is used by non-authorized individuals.

While RDC is a preferred option, it does require an available office workstation/server. As with all remote options, printing and scanning may present challenges.

Application Server

An application server (Remote Apps) is much like the remote desktop connection with the following additional features and benefits:

- The application server provides the processing power, so an on-premises workstation is not required
- The business can decide which applications and restrictions will be provided to each remote user. Whereas a user may have had five different applications available at the office, they may only be given access to four of them for remote workflows.
- An additional layer of security exists between the remote user and the corporate network; further reducing the risk of a compromise.


Remote Application Server Connection
The home office computer logs in to the application server and then accesses applications and files. The bandwidth requirement is similar to a remote desktop connection
Office Network with Data and Files
Application Server
VPN Gateway
Firewall
File Server
Home office computer only needs a VPN connection and a browser. All applications are hosted at the office on the Application Server

While an application server is the preferred method for remote access, it requires additional hardware and licensing. This may prove impractical for some offices.

How To Protect Your Network From Insecure Home Devices

Once a computer has access to your network, every security breach, malware, and robot on that computer can infect your network!

Businesses run on their computer networks as ERP, Sales, billing, communication all depend upon a secure, reliable network. Not surprisingly, successful businesses make considerable investments in their IT infrastructure. Managed service providers or in-house staff are tasked with ensuring that precautions have been undertaken to avoid downtime, breaches, and data loss.

Many home users do not invest in the same level of maintenance and security as is performed on company computers. The lack of investment and management in home workstations can present security issues such as:

- Obsolete or insecure operating systems – i.e. Windows 7
- Missing security and performance patches
- Inadequate, outdated, or missing anti-virus and anti-malware software
- Home computers may be shared with other family members who may gain access to confidential company documents and Personal Identifier Information (PII) files.
- The Wi-Fi connection at the home/remote site may not be secure

You can minimize your risks of a data loss or compromise by

- ***Only permit remote access through a VPN***
- ***Provide a company computer for home use rather than rely upon the employee's home computer***
- ***If you cannot provide a company computer, add the company security software to the home computer and make sure it has been properly patched.***
- ***Insist that users only connect through secure (password protected) Wi-Fi networks when accessing the company network.***
- ***Deploy encryption software to secure data on the remote machine if it were to be stolen.***
- ***Implement written policies that prohibit the storage and/or access of confidential information by non-authorized individuals.***

The "Gotchas" When Setting Up a Remote Office.

So, you've set up your VPN. You've provided company owned laptops to some users and then secured and patched the personal computers of the remaining staff. Users have been trained on the different methods they can use to access the business management system(s), email, proposals, etc. Everyone knows the expectation and procedures to keep confidential information protected. The policy paperwork has been signed and returned. You're all set… right? Wrong!

The following is a list of commonly overlooked problems:

- Does the home office have a secure internet connection, and can the device connect?
    - Is the workstation Wi-Fi capable or do you need to purchase a Wi-Fi adapter?
    - Can the workstation be connected to the router with a patch cable? Does the user have a cable? Is it long enough?
    - If using Wi-Fi, is the connection password protected?
- Is there enough internet bandwidth to accomplish the required tasks?
    - A slow speed internet connection may be capable of handling small file transfers but not large documents or databases.
    - A cell phone can be used as an internet hot spot, but the bandwidth will limit capabilities
- Printing
    - Can the user access the office printer, or do they need to print at home?
    - Does the software support printing on a local machine or does it have to be connected to the network?
    - Does the user have the required stationary, checks, forms?
- Copy, Fax, and Scan
    - If the user is required to copy and scan documents, how do they accomplish this?
    - If a remote fax machine is impractical, can email to fax software be used to replace the fax machine?

Many users will resolve printing issues by emailing documents to another user for printing. While this is acceptable, users need to be trained to only use secure email when emailing documents with PII/PHI information.

Communication

Customers want to see their salesperson. Staff needs to feel connected to their co-workers. Mangers need to collaborate with their team. When establishing methods of communication there are certain best practices which should be followed:

Telephony

- Voice Over Internet Protocol (VOIP): A VOIP phone system uses the internet for connections and call routing. One key benefit of VOIP over an on-premises phone system is that VOIP provides full office functionality from any location. Consider implementing a VOIP system to provide robust features such as voice mail, extension transfer, conference calls, and call holds from any location. Users merely plug their office phones into their home network and have all the functionality they had at the office.
- Forwarding office phones to cell phones. Call quality can be unreliable and there is no ability to call forward to another coworker. This could be used for short term emergencies but should be avoided for extended remote workplaces.
- Forwarding office phone to home phones. Most homeowners have cancelled their land lines in favor of cell service. For employees that still maintain home service, the possibility of non-employees answering business calls can become problematic.

Video Conferencing

- There are a number of providers including Microsoft Teams (Skype), Zoom, and Doxy.me
- Best practices for the use of video conferencing services:
  - ✓ Always use a password protected session
  - ✓ Use a “waiting room” feature so that the host must admit each user into the session.
  - ✓ Have a backup plan in case your primary video conferencing software experiences a problem
  - ✓ Review your surroundings to ensure that everything visible to the camera is appropriate and professional.
  - ✓ Keep the meeting private. Don’t have family members within visual or earshot of the meeting.

Email

- Not all Email is secure. Sending PII and PHI information over an unsecure email connection can be a regulatory violation.
    - Examples of secure services: O365+, proton, gsuites
    - Non-compliant services: aol, gmail, yahoo.com
- Run anti-malware scans on email. Most security breaches come from email.
- Continue to train staff on the safe use of email and the avoidance of phishing scams.

Security

A security breach is not only expensive, it can destroy your reputation and close your business. Your work-from-home security policies should be an extension of your office policies.

Here are some best practices for security regardless of where the employees are located:

Electronic/Computers

- **Anti-Virus/Anti-Malware**: software should be installed on all workstations and servers. Definition files should be kept current.
- **Encryption:** The hard drives of any laptop or workstation that is removed from the office should have encryption software applied to protected data. Encryption software makes data unreadable to thieves.
- **VPN:** A virtual private network should be used when accessing the business network remotely.
- **Password Policy:** Passwords should be changed regularly. Complex passwords or pass phrases should use a combination of upper and lower case as well as numbers and special characters. Easy to guess passwords such as “password”, “123”, your child’s name should be avoided.
- **Dark Web Monitoring:** The odds are that some of your credentials are already for sale on the Dark Web – the part of the internet where criminals trade your information. Subscribe to a monitoring service to alert you so that you can change passwords should they become compromised.
- **Prepare and Implement a Business Continuity Plan:** Ensure that your data is backed up, checked, and accessible for restore in the event of an emergency or system failure.

Physical

- Equipment should be stored in a secure, locked location
- Workspaces should be private enough to avoid third party eavesdropping or visual access to PHI and PII information
- Workspaces should be clean, neat, and safe for the required tasks

Legal Documentation

While we are neither attorneys nor providing legal advice, we should address some basic legal issues when setting up a work-from-home network. By providing clear, consistent, written documentation at the beginning, you are protecting the business and your associates from misunderstandings and potential legal issues. **Request our complimentary network review and Home Office Action Pack for sample documentation.**

Company Assets: Provide a list of all assets, owned by the business, that are being provided to the remote employee. A detailed record of assets including, description, age, condition, and serial numbers establishes a paper trail of equipment that will one day need to be returned or destroyed.

Company Policies: This document has provided numerous recommendations and best practices for building a work-from-home network. While you may not implement everything discussed, you should document and share the policies that you have adopted.

Termination Policy: Employees change jobs. Workers are terminated. Offices are closed. Don't add to the stress of a termination by implementing an ad hoc policy. Advise your staff now as to your expectations of the return and/or destruction of business assets, PII, PHI, and other intellectual property.

What to Do Now

Our world changed almost overnight and the Coronavirus has impacted our personal and professional lives in ways we have yet to understand. This is the first pandemic where technology can have a significant affect. While the prospect of shifting to a skeleton office crew and a work-from-home office staff can be daunting, it is being done successfully in small and mid-sized businesses throughout the country. By following some simple best practices, you can guide your business through these difficult times and deliver quality goods and services to your customers. You don't have to do it alone! Stryker Networks has been assisting businesses like yours for over twenty years.

Regardless of whether you have a full IT staff, a current managed service provider, or are struggling with delivering technology to your staff, we would like to offer you a complimentary network review. There is no obligation and you may find additional peace of mind.

To request your Free Remote Access Consultation and Home Office Action Pack (which includes sample policy documentation and a remote office checklist), simply email your request along with your company name, address, and phone number to tdonohue@strykernetworks.com or call us at 847-908-3210. We will then schedule a convenient time for your network review.