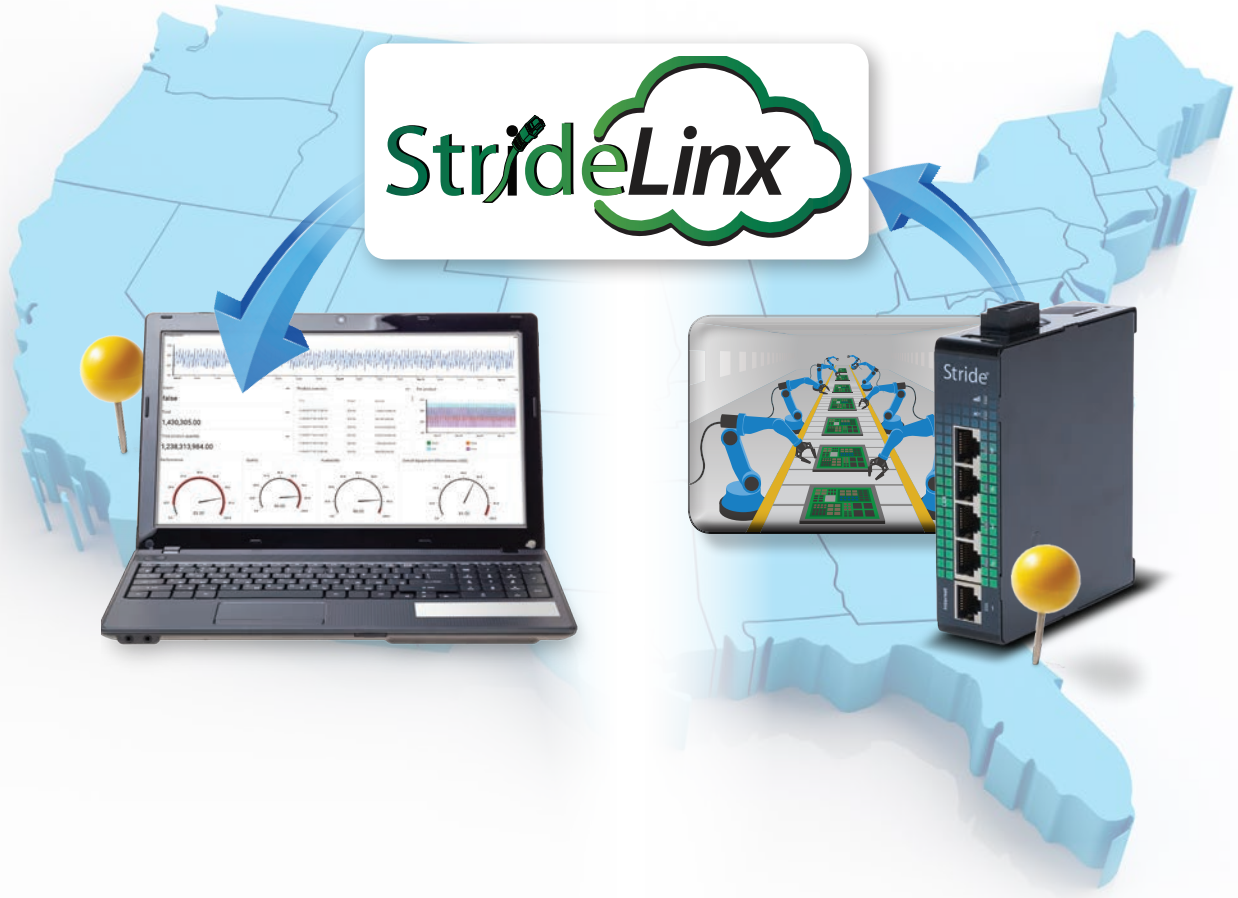
WHITE PAPER

Selecting the Best Remote Access Solution for Your Application

There are three router-based methods for establishing remote access to industrial systems via a PC or mobile device—with each providing a different level of security, required implementation effort and integrated features.

By Jonathan Griffith
Product Manager, Automation Controls & Connectivity, AutomationDirect



AUTOMATIONDIRECT.com
The #1 Value in Automation.™

WHITE PAPER

In today's Internet of Things (IoT) world, remote mobile access is a necessity for many industrial applications. There are several ways of implementing this connectivity with routers and virtual private networks (VPNs). Three of the most popular methods are:

- standard router (without VPN)
- traditional VPN router
- cloud-hosted VPN router

The first solution is a standard router, and although it is not secure it is still widely used in many existing mobile HMI applications, and even in some newer ones. A primary attraction is its low cost, but this approach is discouraged because it poses significant cybersecurity risks when port forwarding is enabled in the firewall as this exposes the network to external threats.

The second solution is a traditional VPN router, which creates a secure tunnel from one location to another. This option requires significant IT skills and greater investment to implement and sustain than either of the two other options, but it offers a secure solution with some significant advantages.

The third solution is a cloud-hosted VPN router, which simplifies IT complexity by creating an encrypted connection from a local VPN router to a cloud-hosted VPN router via the internet. Remote users can then securely access the local components and systems via the cloud-hosted VPN router. This option provides a high degree of cybersecurity, along with relatively simple configuration and maintenance.

Each solution can support various PC-based remote access applications, along with access via smart phone and tablet apps, but with different levels of cybersecurity.

This White Paper will compare the three types of remote access solutions for both PCs and mobile devices, and it will examine the advantages and design considerations for each. The Table illustrates the differences among these options, which are discussed in detail below.

	Standard Router	Traditional Router	Cloud-Hosted VPN Router
PLC/HMI Programming from a PC	Not Secure	Secure	Secure
3rd Party Mobile App Support	Not secure due to port forwarding	Secure if mobile VPN is supported by router	Secure through mobile VPN (with StrideLinx)
Security Risk - PC	High	Low	Low
Security Risk - Mobile	High	Low	Low
Changes to Existing Firewall	Required	Required	Not Required
External Cost			
Initial	$	$$$$$	$$$
Sustaining	$	$	Bandwidth dependent
Internal Support Cost	$	$$$$$	$
Required Technical Expertise	Medium	High	Low
Data Dashboards & Alerts	Typically not available	Typically not available	Available through subscription

Table 1: Comparing Three Remote Access Solutions

WHITE PAPER

Standard Router Advantages and Design Concerns

In many industrial applications a standard router and firewall is used to protect the corporate and industrial plant network (Figure 1), requiring users to manually configure and manage all routing and firewall settings. This type of router does not usually have a VPN to encrypt data, but rather creates port forwarding "holes" in the firewall for remote users to access specific applications and components in the plant network.

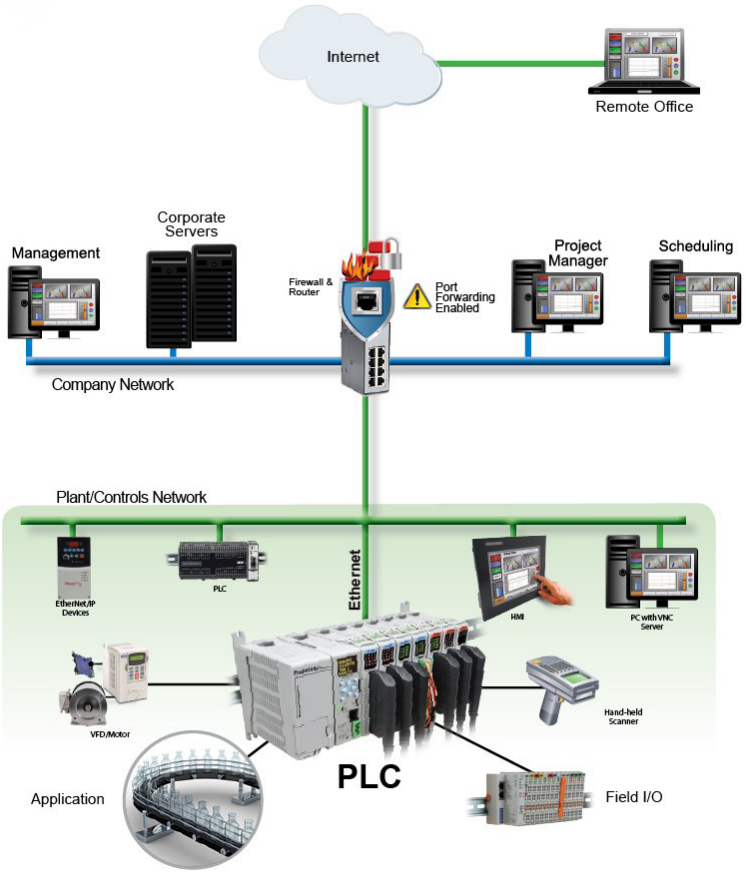


Figure 1: Remote access to local automation components using a standard router is not recommended due to cybersecurity risks.

Most HMI users want the same level of access whether they are remote or local. Laptops normally connect to the HMI web server for monitoring data and making changes to setpoints and other parameters, or they connect to the HMI with programming software to troubleshoot or make program changes.

In order to connect remotely using a standard router, port forwarding is usually configured to allow access to the HMI, or to a local PC running remote access software such as TeamViewer or VNC Connect. The local PC provides the remote user with the ability to run the HMI programming software.

HMI Mobile apps also require port forwarding so the remote user can access the local HMI for control or viewing data. These apps usually provide the same functionality as browser-based remote access, but via an app rather than a browser.

WHITE PAPER

The main concern with this approach is the security risk associated with port forwarding in both mobile and PC-based applications. It's not difficult for a hacker to determine which ports are open on a firewall, thereby gaining entrance to the corporate or plant network through the router.

While port forwarding can be extremely efficient and useful when done within a corporate or plant network, it is extremely dangerous to use this functionality at the internet-corporate interface. Organizations should avoid this standard router approach for new installations and should convert existing standard router installations to a more secure solution, such as a cloud-hosted VPN router.

Traditional VPN Router Advantages

This option is depicted in Figure 2 and requires a local VPN router (shown on the Plant/Controls Network in Figure 2) to connect through the internet via a secure VPN tunnel to a second remote VPN router or software client. Once connected, remote users can access automation components connected to the local router and all associated networked devices through the VPN tunnel, just as if they were connected directly at the plant/controls network.

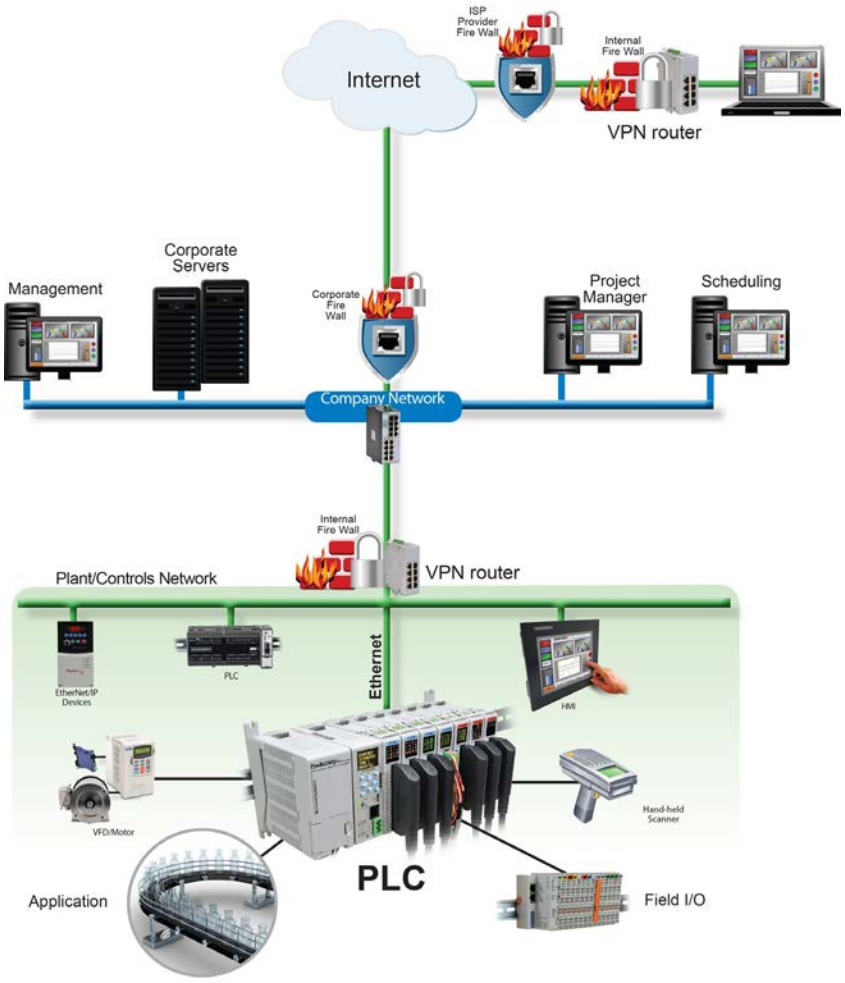


Figure 2: A traditional VPN solution using two routers is shown in this diagram. IT support is required both locally and at each remote site.

There are no cloud-hosted VPN servers between the two devices with either method of connection: VPN router to VPN router, or VPN router to VPN software client. This implementation is preferred when there are large amounts of data to be continuously exchanged between the local and remote sites, as with remote viewing of local video.

This solution is widely used, and it was the only method of secure two-way access prior to the introduction of cloud-based remote access solutions. It can be complex and costly in terms of internal resources required for support, both at the local and the remote site.

Traditional VPN Design Considerations

The main design consideration for this option is the capability and willingness of an IT team to support this solution at both the local and remote sites. For example, an OEM machine builder must consider every customer site and ensure all of its customers are willing to provide IT support. If not, the OEM will have to customize its remote access solution for each customer.

This solution is often more expensive upfront than a cloud-hosted VPN because of increased hardware cost and the IT resources required to configure the connection. Some companies have a dedicated IT staff to provide this support, but many smaller companies do not. Ongoing external costs are lower because there are no monthly cloud service fees, but internal costs are higher due to the need for IT support.

IT must open an inbound VPN port on the firewall. This provides full remote control and monitoring as it effectively creates one network joining local and remote users, but also presents a security concern as this port must be protected from unwanted access at all times. Ongoing security vigilance is required to ensure the router and VPN protocols remain up to date, and other technical considerations must also be addressed including:

- Firewall configuration may be challenging
- Subnet conflicts must be managed across sites with similar network design
- User management and access must be well controlled
- Event logging is not usually implemented and must be added if needed
- Security certificates must be created and managed
- Advanced networking knowledge is required
- Client configuration is needed for each connection point

Despite some drawbacks, this is the preferred VPN solution when the application requires high data bandwidth, or if there is a need to avoid reliance on a hosting vendor. IT staff must be available and willing to maintain security standards and make firewall changes.

WHITE PAPER

Cloud-Hosted VPN Router

Cloud-hosted VPN solutions provide a secure connection with simple setup and network configuration. Typical cloud-hosted VPN solutions include a local VPN router, a cloud-hosted VPN server, a VPN client and connected automation components (Figure 3).

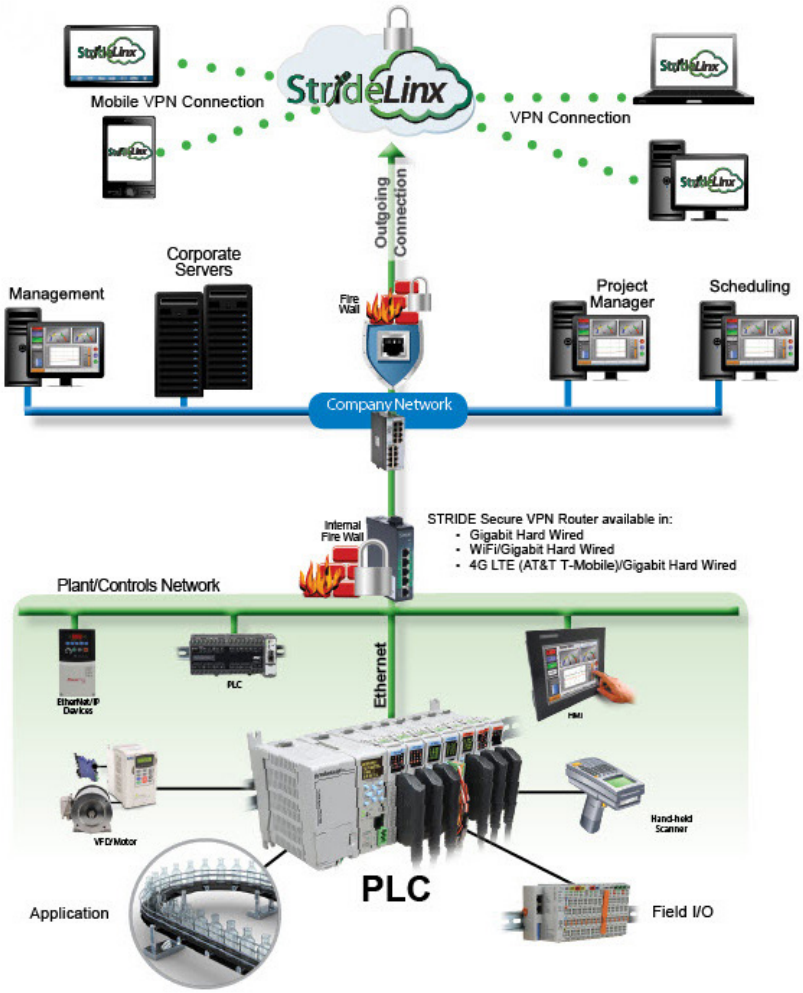


Figure 3: AutomationDirect's StrideLinx cloud-hosted VPN solution offers secure connectivity for mobile HMI applications hosted on laptops, smartphones and tablets.

A secure connection is established after the local router (at the Plant/Controls Network) and VPN client (software installed at the user's laptop or mobile device) each make a connection to the cloud-hosted VPN server. The local router makes this connection immediately upon startup, but a VPN client only connects upon a verified request from a remote user. Once both connections have been made, all data passing through this VPN tunnel is secure.

Most cloud-hosted VPN solutions provide a free monthly bandwidth allocation for basic operation and then throttle data access once this allocation is reached, and also offer a premium plan for additional bandwidth. For example, AutomationDirect's StrideLinx solution offers 5GB of VPN data exchange per month for free, sufficient for most troubleshooting, monitoring, and programming needs.

This solution has very low security risk as the local router initiates communication to the server via an outbound connection through standard ports that are typically open, such as HTTPS. This usually requires no changes to the corporate IT firewall and satisfies IT security concerns. For added security confidence, users should look for cloud hosted VPN solutions that have an industry-certified information security management system, such as ISO/IEC 27001:2013, as it indicates the supplier has implemented comprehensive security programs and controls.

Another advantage of a cloud-hosted VPN solution is extremely simple router configuration. Since the secure local router (Figure 4) will be connected to a predefined cloud server, the router comes preconfigured with complicated VPN networking settings in place, allowing non-IT staff to easily install this solution. All that's required is knowing the IP addresses of the automation components connected to the local area network, and whether their ISP or corporate wide area network router (not the cloud-hosted VPN router) provides IP addresses dynamically or statically.

Figure 4: These AutomationDirect StrideLinx VPN routers provide the pre-configured functionality needed for cloud-based connectivity, greatly simplifying implementation.

In addition to a wired LAN option, the cloud-hosted VPN router should include Wi-Fi and 4G LTE connectivity options. Wi-Fi provides access point or client connection, and it allows plant personnel to access the local router's LAN network wirelessly. This is safer and more convenient than opening the panel to access the physical LAN connection ports. 4G LTE connectivity provides access from remote locations without internet access, or from locations that don't have access to their corporate network.

Other advanced options included with some platforms are cloud data logging and alarm notification. These services allow users to log system data and receive customized critical alarms on their mobile devices or laptops, providing a convenient, web-based historical record of system performance available whenever needed.

Platform branding is helpful for an OEM looking to market its own Industry 4.0 solution by private labeling the StrideLinx platform. The OEM receives its own unique URL and home page logo, promoting its brand every time its customers access their machines.

WHITE PAPER

Cloud-Hosted VPN Design Considerations

The hosted VPN solution does not require an IT team for support because it's simple to implement and maintain, and it is accepted as secure by most companies. Those companies that would not accept a cloud-hosted VPN solution for security reasons would likely not accept a traditional VPN either because of its required firewall changes.

The simplicity of this solution comes at the cost of limiting some of the advanced routing features that may be required for sophisticated networks such as machine-to-machine networking, advanced NAT configuration and access control lists. However, for most users these advanced features are not required.

Other design considerations depend on specific features offered by the cloud-hosted VPN vendor. Inclusion of these key features address these issues, while exclusion may present problems. These key features include data logging, widgets for configuring remote access screens, a web-based platform for router configuration and a digital input for enabling/disabling remote access.

The traditional VPN solution requires supply and configuration of a third-party HMI, either PC-based or embedded, to provide data logging and widgets for configuring remote access screens. Instead, the cloud-hosted VPN option may provide data logging functionality in the form of collection, storage and display of data via a cloud-based platform. This allows users to log and access a virtually unlimited amount of data while only paying for the required capacity. Users can start with a small number of data points and then scale up as needed.

Some cloud-hosted VPN solutions provide widgets for users to configure dashboards for data visualization (Figure 5) on their PC or mobile device. If this feature is not provided, the additional software and effort required for designing remote access viewing screens can be cumbersome.

Figure 5: AutomationDirect's StrideLinx cloud-hosted VPN solution provides widgets for users to configure dashboards for remote access viewing on their PC or mobile device.

Cloud-based data logging typically requires an additional license or subscription from the cloud-hosted VPN vendor to collect and store the data in the cloud, and this cost must be considered, particularly since it doesn't exist with the traditional VPN option.

Cloud-based notifications provide mobile push notifications or email alerts, for example when a process parameter exceeds its limits or when process steps are completed. This is an important advantage because alerts and notifications can be quickly configured in the cloud platform to inform users when parameters fall outside a predefined range.

Those considering this solution must have a high level of trust in the hosted VPN vendor as it will be responsible for securely storing data and making it available to only those who need it. Monthly costs incurred for data bandwidth exceeding the free limit must also be considered, particularly compared to the relatively much lower cost, approaching zero in some cases, for a traditional VPN solution.

A web-based platform provides quick and easy configuration of the VPN router, often as simple as registering an account, configuring and downloading router settings, and installing a secure client on a PC. One of the main advantages of a web-based platform over PC-based configuration is that platform features can be updated without the user reinstalling a new version. This is particularly useful in the cases where new features are added on a regular basis.

An important safety feature for the VPN router is a digital input for a switch to locally enable or disable communications, preventing remote control of a machine during maintenance periods. If this option is not provided, it should be added on, which will add cost and design time.

Mobile App-Based Remote Access

Industrial HMI and PLC components are increasingly supported with mobile apps, providing users with remote access anytime from anywhere, with both monitoring and control capability. In order to securely access industrial equipment, the mobile device must also employ VPN technology to encrypt the data from the mobile device to the plant network. Without mobile VPN, the firewall ports at the plant will need to be opened, creating a similar scenario to the standard router solution and leaving the plant network vulnerable to a cyber-attack.

The solution is to use a traditional or hosted VPN solution providing a secure VPN connection for both laptops and mobile devices. Once securely connected to the plant network through the mobile VPN app, the third-party HMI or PLC app can then be opened and used to connect to the local HMI and PLC components as if the mobile user was on-site, because he or she is there virtually.

Traditional mobile VPN solutions are relatively easy to implement on the mobile user side, but they again require IT staff to deploy and support.

Hosted VPN solutions are significantly easier to deploy, but only available from a limited number of industrial VPN suppliers. AutomationDirect's StrideLinx routers provide a hosted VPN solution with VPN connections for both laptops and mobile devices. Both iOS and Android mobile device apps are available, providing users a secure connection from any device to the plant network.

WHITE PAPER

App-Based Access in Action

As mentioned earlier, some cloud-hosted VPN vendors go beyond secure VPN remote access and also provide app-based access to data logging software running in the cloud, along with widgets for configuring customized dashboards to be viewed remotely.

Figure 6: StrideLinx mobile VPN connectivity allows control and data viewing on third-party mobile apps, like AutomationDirect's C-more Remote HMI.

This built-in cloud logging would be particularly effective for an OEM machine builder with thousands of machines installed worldwide at hundreds of different locations, each with multiple users. The OEM would simply provide a VPN router for each machine, pre-configured to log data and including customized dashboards for remote viewing on an Android or iOS app. No effort would be required by the OEM's customers to configure, install or maintain remote access software—other than installing an app on their smart phone or tablet.

For more comprehensive access beyond dashboards, remote users could securely access local HMIs and PLCs via apps using the mobile VPN provided by the hosted VPN supplier (Figure 6). For example, AutomationDirect's C-more HMI mobile app works securely when used in conjunction with the StrideLinx VPN router. And of course, local equipment could also be securely accessed remotely by a PC for programming, monitoring or troubleshooting.

Conclusion

This White Paper examined the three router-based methods for establishing remote access to industrial systems via a PC or mobile device: standard router, traditional VPN and hosted VPN.

Standard router solutions are not cybersecure, and therefore should not be used for new applications, and should be replaced in any existing applications.

Traditional VPN solutions are difficult to configure and support, with cybersecurity primarily the responsibility of the end user. But when properly deployed, these solutions can be used for secure remote access by mobile devices and PCs, although PC-based access does require firewall modifications, which may not be supported or even allowed by all of an OEM's customers.

WHITE PAPER

Hosted VPN solutions are ideal for machine builders and small/medium businesses looking for a simple way to deploy and maintain a secure remote access solution across multiple industrial locations. The router supplier provides most of the required configuration and support for both mobile device and PC access. Since this implementation usually does not require firewall modifications, it is acceptable for deployment at nearly all plant or OEM-customer locations.

Sidebar: Decision Tree

The decision tree (Figure 7) shown below can be used when deciding between a traditional and a cloud-hosted VPN solution as it factors in both PC and mobile device remote access. As mentioned earlier, it is strongly recommended to avoid implementation of a standard router solution as it leaves a network exposed to cyber security threats.

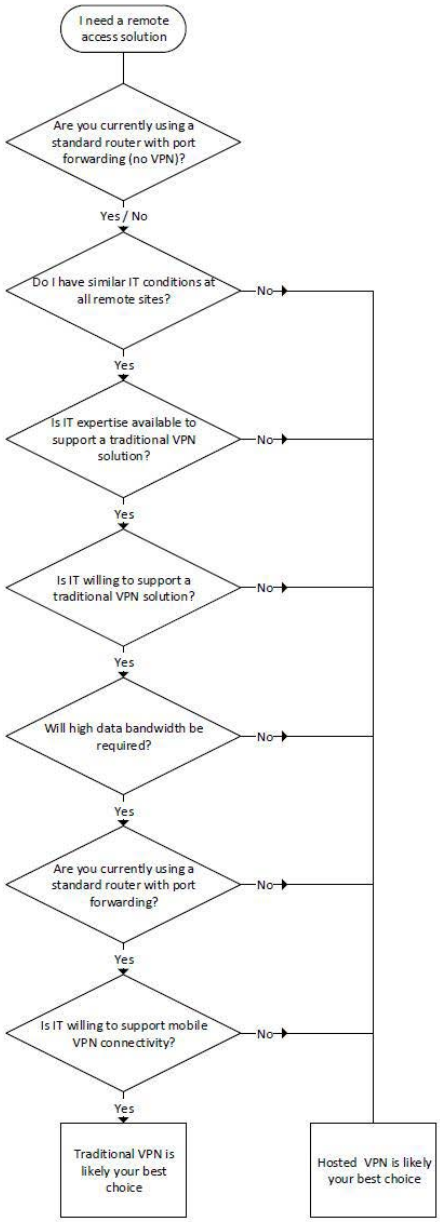


Figure 7: Comparing Traditional to Cloud-Hosted VPN