REMOTE ACCESS

Many companies including several of the world's largest enterprises such as Google, Amazon, and Microsoft are moving towards work from home with on-premise workforces to a distributed remote workplace.
miniOrange and many organizations, part of this strategy include recommending and enabling employees to work from home in response to the continually developing COVID-19 crisis. This decision is based on ensuring the safety of their employees and the prevention of exposure to the Coronavirus, it comes with the additional challenges of securing digital assets and business-critical resources.

How does working from home prevent COVID-19?

The basic and important parameter for preventing it is to **Maintain Social distancing**.

Reason:
When someone coughs or sneezes they spray small liquid droplets from their nose or mouth which may contain the virus. If you are too close, you can breathe in the droplets, or can accidentally touch the surface and pick up the virus including the Covid-19 if the person coughing has the disease.
Once Contaminated, hands can transfer the virus to your eyes, nose or mouth. From there, the virus can enter your body and can make you sick.

To read more information about protective measures for employee safety refer to WHO Article.

Different Ways to provide secure access to Work from Home to employees

1. Secure Access to OnPremise Resources / Servers:

a. **Restrict Access with VPN:** This restricts employees to log in into your on-premise network from their home with secure VPN credentials. Those users will have access to all the resources and your data is still secure even if using the public wifi network.

Employees can connect to the office network and access all the resources without compromising the security using the Remote Access with VPN.

Remote Access VPN has two main components:

- **Network Access Server (NAS)** - NAS allows you to connect to VPN using the username and password and does the authentication process using its own method or separate authentication server on the network.

- **VPN Client Software** - The client needs to install the software to connect the server when out of the office.

The Client software connects to NAS using the tunneled connection and also maintains the encryption to keep it more secure.

You can read later in the article how miniOrange provides the Remote Access VPN.

b. **Multi-factor or 2-Factor Authentication:**

miniOrange provides easy to use 2-factor authentication to secure VPN access to your network. It replaces insecure passwords and adds a second layer of security to your site.

Adding MFA also helps you gain visibility into all devices.

2. **Secure Access to Cloud Resources / Servers :**

Companies provide their employees remote access to the office network resources that are hosted on the cloud. Security is an important concern while remotely accessing these resources. Other than employees, no other third person should be able to access those resources and misuse them.
So this needs a protective login which provides access to only those who are authorized to it. This protective login can be done using Risk-Based Authentication(RBA).

What is Risk-Based Authentication?

It is an advanced method for Authentication that adds the layer to the traditional security of usernames and passwords. It is based on Location, Device and Time.
This Authentication can be enhanced depending on the level of the risk. In some cases, the user shows the suspicious activity continuously will be forced out of the system. Or in other cases, users have to provide the answer to determined questions or have to do multifactor authentication including biometrics, Verification through OTP, etc.
The objective of this is to reduce the burden of providing the additional credentials and providing better experience while maintaining strong authentications.

You can read later in the article how miniOrange provides the Remote Access VPN.

Which is more suitable for your Company -

Either or both could be the right choice for your company. Cloud computing and VPN use aren't mutually exclusive nor is one automatically superior to the other. Cloud computing is a much simpler solution, and it can do a great deal for your company besides making

remote work more streamlined and intuitive. On the other hand, if you have very serious security concerns, you probably *need* a VPN. For instance, a VPN will better protect your users' machines from potential malicious actions while using public WiFi signals. With a cloud computing network, your employees would need to connect via a portable WiFi hotspot to stay secure.

miniOrange offering to organizations for their work from the home environment

Single Sign-On (SSO) and MFA for VPN Apps and Cloud Environment

miniOrange will allow you enabling your secure access to apps and cloud resources with secure RADIUS protocol which is supported by all VPN servers and validating against any user store such as Active Directory.
miniOrange provides the ***Multifactor Authentication*** to provide an additional layer of security.
Click here for more details

Risk-Based Authentication

miniOrange provides the RBA based on the above-mentioned factors Device, IP, Location and Time by allowing the authentication connection with any external user store whether it is Active Directory or an External Identity Provider.
It also allows the user to securely login to any application without understanding the complexity inside it and do their work.
For example, if a user wants to access the resources from an unregistered location then he may have to perform the authentication based on the risk level. In this case, if the user has registered the new location also then he will be able to access it without any obligations.

Click here for more details.

Benefits to work with miniOrange

- **Secure your resources**
- **To gain visibility into all devices and employee access**
- **Setup guides for all pre-integrated Apps**.
- **Expertise Support**
- **And Many More.**