NewCytech Solutions for Working Remotely and Securely

1.Newcytech's Solutions

The Coronavirus outbreak changed our lives! One of the major changes imposed is working remotely from the office. Several organisations depend on a centralised infrastructure to distribute business assets (e.g. files, services). Their existing infrastructure may span across a standalone file server to a full rack of servers. Now that the workforce must access these sensitive resources remotely in order to complete everyday business tasks, several technical issues are raised. A critical update of the infrastructure must be performed by several organisations in order to continue offering the required tools and resources to their workforce and, therefore, ensure business continuity.

NewCytech offers turnkey solutions to assist small and medium enterprises work transparently and efficiently during this time of high distress. The proposed solutions are offered as an enhancement to your organisation's existing infrastructure, which can be implemented rapidly and enables the workforce to access the required resources remotely, securely and, most importantly, in a cost effective manner.

2.Solution Features

NewCytech offers complete network protection solutions with unique advantages that enable small and medium enterprises to adopt the necessary infrastructure functionalities with minimum effort and cost.

A distinct benefit of the solutions provided by NewCytech is the prompt delivery speed, even while the movement-restriction measures are imposed. This is accomplished by introducing virtual or software-based products, which can be deployed to your organisation's existing infrastructure without the need to visit your organisation's premises, or by having limited access.

NewCytech's network protection solutions are installed as a virtual or software appliance in order to:

- minimise the changes required to the existing infrastructure - run on existing desktops, laptops, servers, mobile devices;
- reduce delivery and deployment time - software and licenses delivered by NewCytech, installation and configuration may be performed by NewCytech or your IT department;
- minimise access to the physical premises – configuration and operation is accomplished remotely.

NewCytech can deploy the proposed solutions on any setup – on premises, public cloud, private cloud or hybrid, allowing your organisation to consolidate and make available its resources effectively, securely and transparently.

2.1 Advanced Networking and Protection

The Advanced Networking and Protection solutions provided by NewCytech extend the available networking functionalities of your organisation's infrastructure immediately after deployment. NewCytech offers advanced networking, security, privacy and performance-improvement functionalities that, amongst others, include:

- network routing;
- network bridging;
- zone segmentation;
- traffic shaping;
- traffic filtering;
- access control;
- application control;
- wireless control;
- encrypted communication;
- remote access;
- Data Loss Prevention (DLP);
- policy definition and enforcement;
- centralised management.

NewCytech's solutions protect your network traffic (web and internal), business applications and workloads, as well as email and data by applying the following features:

- advanced firewall;
- Intrusion Detection System (IDS);
- Intrusion Prevention System (IPS),
- dedicated antivirus;
- anti-malware;
- web protection;
- advanced threat protection

The aforementioned features and functionalities are customised according to your organisation's particular needs and existing infrastructure. As a result, the existing networking and protection functionalities are improved, despite the technical specifications of the infrastructure that sustains them.

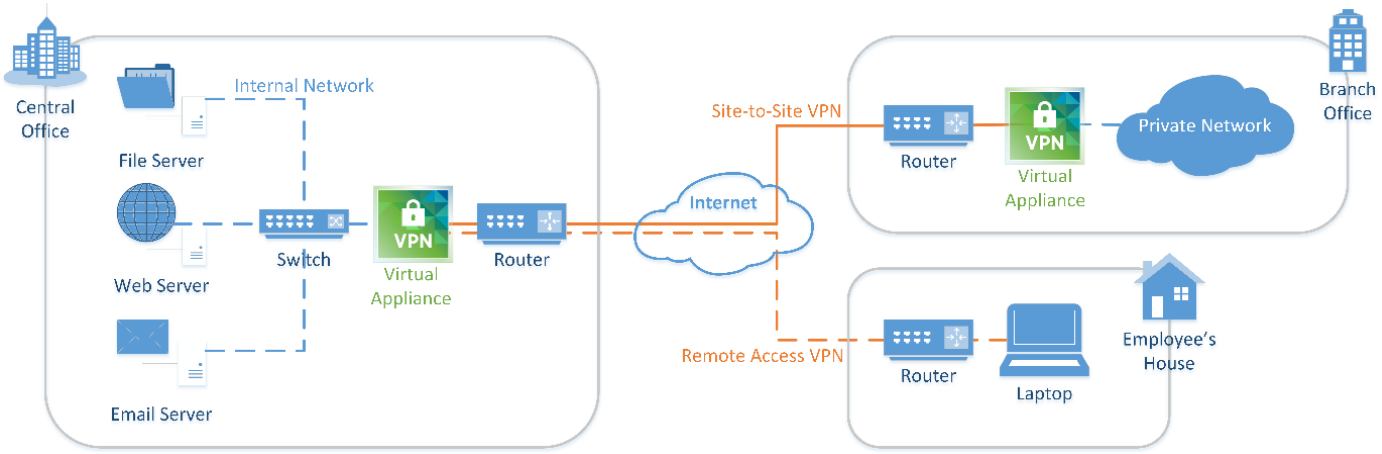
NewCytech's experts work closely with your organisation to identify the best possible solutions, configure them to operate on the existing infrastructure and manage their operation in order to minimise the effort required to be invested by your workforce.

2.2 Secure Remote Access

NewCytech can help your organisation establish Virtual Private Networks (VPN), which are tunnels that carry business network traffic, from your office to a remote device (e.g. employee's home PC, mobile phone) over the Internet. This way, remote users can access and transfer data securely as if their devices were connected internally to the office network.

Secure connections can be established both between individual devices and between networks. Two scenarios that establish secure communications over VPN technology are presented in the following figure. They include:

- Site-to-Site connections between a branch office and the central office;
- Remote Access connections between off-site employees and the office network.

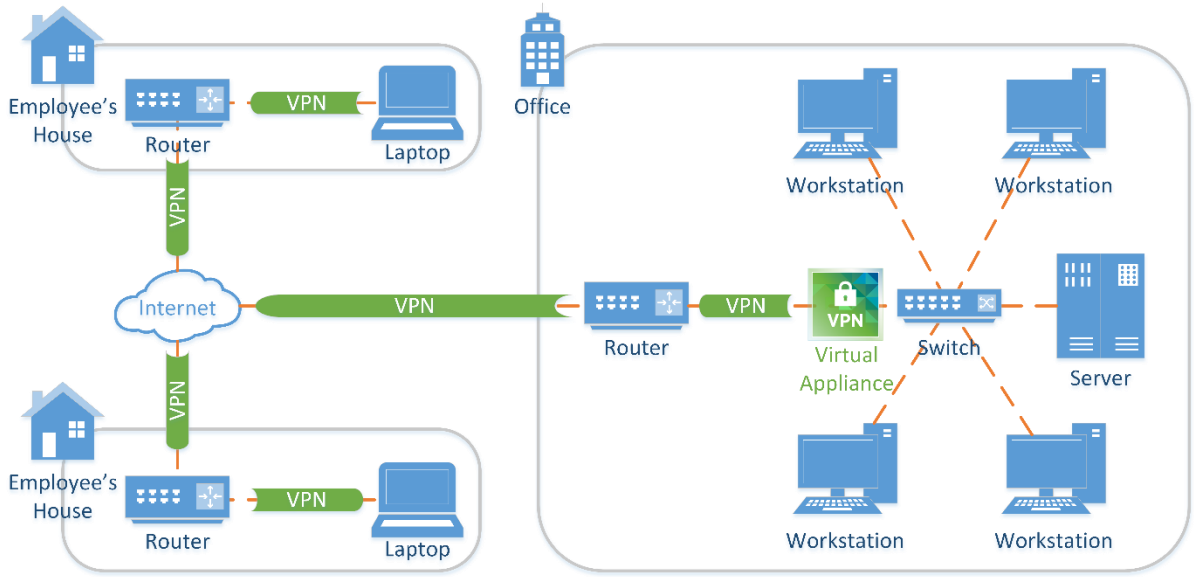


NewCytech enables your organisation to offer remote access through VPN according to the specific needs of your workforce. Therefore, NewCytech supports the most secure standards, including SSL, OpenVPN, IPSec (e.g. IKEv2), PPTP and L2TP as well as vendor-specific protocols.

Your workforce has several options to establish secure connections to the office network. They include:

- installing a dedicated VPN-client application at the endpoint (e.g. employee's home PC, mobile phone);
- configuring their devices' (e.g. mobile, laptop, desktop, server) operating system parameters.

The following figure presents how secure remote access to the office applications and data can be established from home by introducing a single virtual or software appliance at the office.



3.System Requirements

The configuration of the virtual and software appliances enables the network security to be implemented within the office infrastructure. These appliances deliver the full features of their equivalent hardware appliances. In case that the organisation is located at multiple offices, centralised management is available through dedicated add-on products.

Network protection appliances can be installed as a virtual appliance on most stacks, such as:

- VMware ESX and VMware ESXi;
- VMware NSX for vSphere;
- Microsoft Hyper-V;
- Microsoft AzureStack;
- Kernel-based Virtual Machine (KVM);
- Nutanix;
- VMware ESX and VMware ESXi;
- OpenStack;
- Citrix Xen;
- Open Source Xen;
- Cisco ACI / Cloud Services Platform;
- Other Hypervisor platforms (e.g. VirtualBox).
- OpenStack;

Network protection appliances can also be installed as a software suite on custom hardware over Windows and MacOS systems.

The minimum hardware requirements include:

- CPU: 1x core;
- RAM: 4 GB;
- HDD or SSD: 60 GB (for system and reporting);
- Network Interface Cards (NIC): 2x required (1x for LAN and 1x for WAN).

4. Licensing Options

The price of every network protection appliance includes a base license that offers basic functionalities. You can extend the functionalities according to your organisation's individual needs and deployment scenarios, by purchasing individual subscriptions or selecting one of the available bundles.

NewCyteh's network protection solutions include a free trial for a period of 30 days and may be provided free for home use

4. NewCytech's Services

- Warranty;
- Installation and Setup;
- Technical Support.
- Operational Support;
- Hardware Support;
- Corrective and Preventive Maintenance