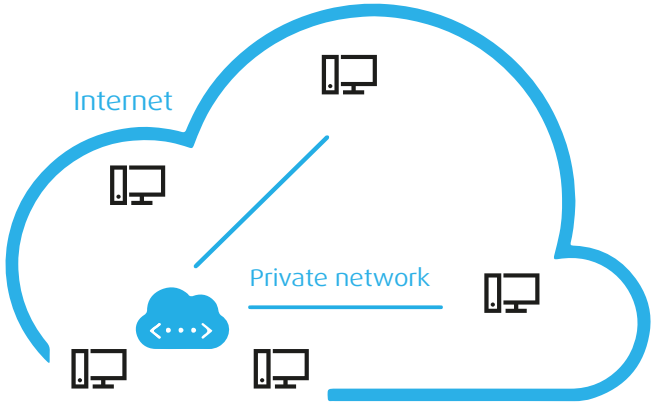

Remote Network Connection™
trust
CloudTrust
Microsoft
Azure
Certified

Overview

Remote Network Connection™ is a comprehensive VPN solution and platform that uses the SSL/TLS protocol to establish an encrypted channel. SSL/TLS is a protocol widely used on the Internet. Its best-known, ubiquitous application is HTTPS, which is used to encrypt the traffic of web sites. By default, HTTPS uses Port 443 for communication. This communication protocol is well known by all firewalls and proxy devices. It can also be managed and forwarded easily in a NAT environment.

Using a secure connection via the Internet, the Remote Network Connection™ VPN solution establishes a VPN session between the remote and the local virtual network adapters and forwards all Ethernet frames between the two networks. The Remote Network Connection™ VPN network consists of the Remote Network Connection™ server and multiple Remote Network Connection™ applications. The Remote Network Connection™ VPN solution guarantees a fully transparent connection between two or more network adapters – as if they were on the very same network segment.



Remote Network Connection™ VPN network over the Internet

Remote Network Connection™ application

The Remote Network Connection™ application is a service that maintains a continuous, self-reconfiguring connection to the Remote Network Connection™ server – meaning that it will keep trying to re-establish the VPN connection in case the Internet connection gets disrupted. The Remote Network Connection™ application opens a connection to the Remote Network Connection™ server only, through Port 443, using the local Internet connection. Therefore, no „incoming" protocols have to be allowed and no „incoming" ports have to be opened. VPN traffic is sent through this encrypted channel.

The Remote Network Connection™ application can also be run as a Windows service. This means that the local resources and services are available to the other members of the VPN even when there are no users logged in at the local computer.

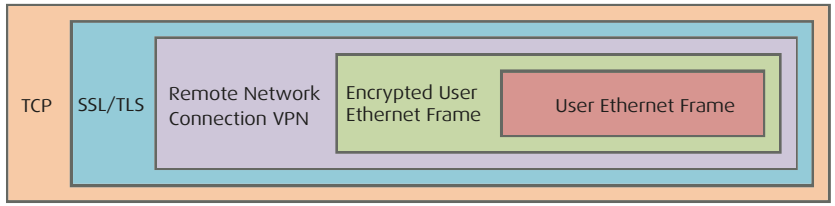
By default, the Remote Network Connection™ application only forwards traffic sent to its own network towards the Remote Network Connection™ server. All other traffic is sent to the local Internet gateway as usual (split tunneling). It is also possible to forward the whole amount of network traffic, or all the traffic related to a certain DNS provider towards the VPN network, and within that, a designated Remote Network Connection™ application. This can be enforced by creating local routing rules. In this case the remote VPN clients should use the Microsoft Internet Connection Sharing (ICS) feature or some other routing technique.

The Remote Network Connection™ application can be configured to filter protocols transmitted towards its own network – e.g. the unnecessary uPnP packets, or the multicast and broadcast messages.

Remote Network Connection™ server

The role of the Remote Network Connection™ server is to create a virtual network for the Remote Network Connection™ applications – including the dynamic allocation of IP addresses, managing sessions, providing routing features, and transmitting status information. The Remote Network Connection™ server only provides the Remote Network Connection™ VPN members with the services necessary to operate the infrastructure. It cannot be connected in any other ways.

The Remote Network Connection™ application encrypts the communication of the local virtual adapter with a pre-shared password – using standard-based, symmetric-key encryption – when sending it to another member of the network and decodes the traffic arriving from another member. It means that the communication within the SSL/TLS traffic on Port 443 is encrypted: the Remote Network Connection™ server, which is responsible for routing, cannot „peek into" the actual data content sent by the Remote Network Connection™ applications. In other words, this is real, point-to-point encrypted communication.



The Remote Network Connection™ VPN tunnels the Ethernet frames in SSL/TLS traffic

The Remote Network Connection™ server can be configured to allow network traffic towards IP addresses and hosts within its own VPN network; or to allow specific types of traffic – e.g. broadcast messages, route traffic – to the endpoints.

Highlights of Remote Network Connection™

Remote Network Connection™ application

- it can run in the background as a digitally signed (code signing certificate) and timestamped Windows service and application framework
- using a digitally signed (driver signing certificate) and timestamped virtual adapter, it maintains a separated, private network traffic
- it opens an SSL/TLS communication channel (TLS 1.2) from inside, towards the Remote Network Connection™ server (so that firewalls allow the returning, incoming traffic)
- it tries to keep the connection alive, continuously, in a self-reconfiguring way: changing the Internet provider or a short disruption in the connection is transparent to the user
- it manages the password-based or open proxy connection of the local Internet connection, and it confirms the hash of the Remote Network Connection™ server to avoid man-in-the-middle attacks
- it provides its own virtual network adapter
- it receives and transmits all network Ethernet frames (Layer 2)
- using a standard-based (AES 256) encryption, it encrypts and decrypts the network traffic, resulting in real point-to-point encrypted communication (other, custom encryption algorithms can also be used)
- it allows limiting the bandwidth of the traffic sent to the Remote Network Connection™ server
- it can be used with Windows 7, 8, 8.1 and 10 (32- and 64-bit) operating systems, furthermore with Windows Server 2008, 2012 and 2016 server OS

Remote Network Connection™ server

- it provides the Remote Network Connection™ applications with an SSL/TLS communications channel (TLS 1.2)
- it provides the Remote Network Connection™ applications with a session
- it can manage the connections of the Remote Network Connection™ application endpoints from their source IP addresses, and it can be configured to require endpoint SSL authentication certificates when establishing the SSL/TLS communications channel (identity authentication)
- one Remote Network Connection™ server can serve multiple, mutually independent virtual networks at the same time
- it assigns virtual IP addresses dynamically to the Remote Network Connection™ applications
- maintains the Remote Network Connection™ applications and provides them with occasional information
- receives and forwards the encrypted communication arriving from and to be sent to the Remote Network Connection™ applications
- measures the amount of traffic sent and received by the Remote Network Connection™ applications, and monitors the validity period of the VPN network connection

Part of the Remote Network Connection™ server is the Remote Network Connection SSL Offloading component, which is responsible for establishing and managing the SSL/TLS connection. The Remote Network Connection™ server supports implementing a high-availability, central server architecture.

vmware READY Microsoft Hyper-V Server ORACLE VIRTUALIZATION

Benefits

Benefits of using the Remote Network Connection™ solution:

- it can be used in a heterogeneous environment, with multiple Internet service providers – it can use any kind of business, retail, mobile, public Wi-Fi, etc. Internet connection
- even on a heterogeneous infrastructure, served by multiple ISPs, it provides a homogeneous solution, perfectly fitting the applications
- instead of hardware devices installed at the endpoints, you can use a centralized hardware solution, there is no deprecation related to endpoint hardware devices
- you can eliminate the time needed to manage the hardware devices installed at the endpoints and on-site visits
- less time is needed to manage and maintain the endpoint network, it can be centralized
- the Remote Network Connection™ members only forward traffic within their own network towards the Remote Network Connection™ server
- the Remote Network Connection™ members can be managed remotely
- the solution is transparent to the users, it gives them the same user experience they are used to but which required physical attendance
- it can be used to implement either continuous or ad hoc (or time-limited) access
- it fully supports telecommuting; it also supports performing work in an ad hoc manner
- it can be perfectly be operated as an infrastructure-as-a-service (IaaS) or software-as-a-service (SaaS) solution
- by using the Remote Network Connection™, the efficiency of teamwork is increased and there is less downtime because of service outages
- the total of the services provided by Remote Network Connection™ cannot be matched by hardware-based solutions – not even with a much greater investment and a significantly longer implementation time
- the Remote Network Connection™ application can be used on Windows To Go devices

Interconnection with other networks

There are several ways to extend the virtual network segment created by the Remote Network Connection™ VPN solution, depending on the usage needs and the requirements of the applications to be used:

- Internet Connection Sharing (ICS)
- IP Routing
- Port Forwarding and
- Routing and Remote Access Service (RRAS) can all be used.

Internet Connection Sharing (ICS) and Routing and Remote Access Service (RRAS) are both based on network address translation (NAT). The second one is aimed at enterprise environments, while the first one is practical for small or home offices (SOHO).

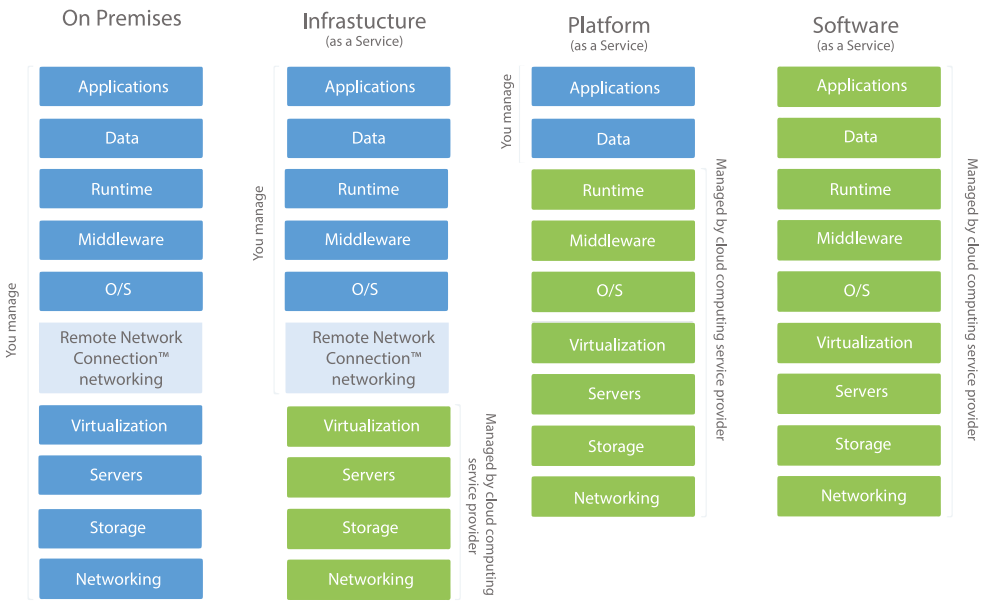
The Remote Network Connection™ VPN solution can be extended using other, classic, standard network solutions – e.g. L2TP/IPSec server connections.

To select the best way to connect to the other networks, you may need to investigate the usage patterns, and you may need to analyze the operation and the traffic patterns of the applications to be used.

The Remote Network Connection™ VPN solution can be used to build point-to-point, point-to-site and even site-to-site connections.

Supporting various operation and service models

The Remote Network Connection™ VPN solution can be served as infrastructure (IaaS) and can also be used on premises without any problems.



Connections of the Remote Network Connection™ operational model with own (on-premises) or Microsoft Azure environments

Infrastructure-as-a-service (IaaS) is an immediately available processing infrastructure that can be provisioned and managed via the Internet. The service provider offers virtual hardware, and all software on it is installed and maintained by the user. It can be quickly scaled in both directions according to needs, and its fees are typically based on the amount of usage.

Using IaaS, you can avoid the costs and complex tasks related to purchasing and managing your own physical servers and other data center infrastructure.

The Remote Network Connection™ VPN solution is capable to serve both infrastructu-re-as-a-service (IaaS) and on-premises operational models.
When using the infrastructure-as-a-service (IaaS) model, you can implement an own network layer beside the operating system (OS) layer, one that is independent from the provider. Thus the cloud provider cannot see its traffic – and you can mitigate the risks resulting from using public cloud services.

The Remote Network Connection™ VPN solution protects the data traffic between your organization and the cloud, between the resources in the cloud and between the cloud and other external providers. It protects against eavesdropping and modification, and it also takes care of the availability of the network connections and their expected transfer speeds.

Remote Network Connection™ supporting various public cloud service providers

The Remote Network Connection™ VPN solution encrypts the data traffic of the service and protects its integrity. Besides the potential line encryption and integrity protection provided by the cloud or telecommunication providers, it uses its own encryption, a custom VPN solution: it authenticates the devices and users taking part in the communication, it guarantees the high availability of the network connections, and the network bandwidths necessary for proper operation.

The Remote Network Connection™ VPN solution supports similar operational models both in hybrid and self-operated operating environments.

Available at: https://rnc.services

trust
CloudTrust