DrayTek Whitepaper

Your reliable networking solutions partner

VPN Basic

Introduction

To enterprise, the security of confidential information is a great issue for a company. In modern society, mobile devices are popular and people who work with mobile devices also increase more and more. IT administrators not only assure the stability and convenience of the communication between business men and cooperative partners outside, but also maintain the security of remote access for the both sites. Therefore, how to protect the information is the big challenge for IT administrators.

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

VPN Types

The common VPN types are listed as below:

IPsec VPN

Before constructing the network connection, users must be authorized to ensure the information be encrypted and transmitted safely on both sites. Such type can provide a secure and cost effective method to assist the enterprises building remote connection securely all over the world. And it can offer a reliable network connection for the data exchange from site to site or clients to site. However, remote clients have to install relational IPSec software for the configuration of Windows IPSec will be complicated. In addition, the users must face the compatibility problem caused by NAT traversal constructed by IPSec application software, router and IPsec gateway. These are the disadvantages that the IPSec users must face.

PPTP VPN

The feature of PPTP (Point-to-Point Tunneling Protocol) tunneling technique is easy to configure, therefore, it is a protocol that is used widely by people. Through PPTP VPN, the user can use the network connection built in Windows operation system to establish a virtual private network.

PPTP will encapsulate the data with IP packets and transmit to the destination via Internet. The packets encapsulated will be regarded as common IP packets by any router, device or machine in network and be sent out. When the packets arrived to remote end of the VPN tunnel, the header of the IP packets encapsulated will be removed. The advantage of such technique is that the data with different protocols can be transmitted through any network media (e.g., Internet) supporting IP.

SSL VPN

SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. That's, it is a web-based and non-client software. It is not necessary for users to pre-install any VPN client software (e.g, SmartVPN). Meanwhile, it will not be restricted by network environment and it is easy to configure and simple to be maintained through webpages. Most important, it is cost saving. What advantages that SSL VPN have?

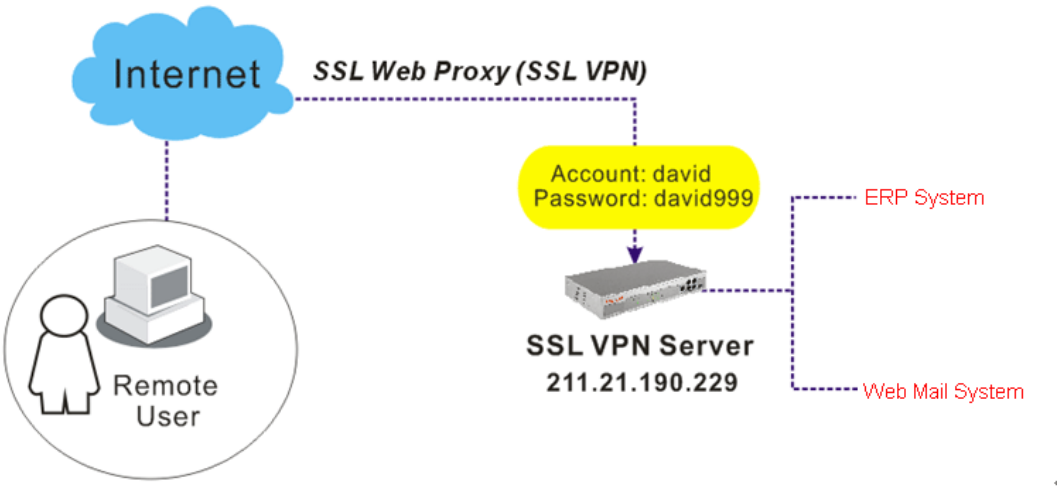
- First, general web browsers support such protocol. It is not necessary for users to install software to configure settings additionally. The management requirement fee can be reduced largely.
- Second, the administrator can configure several policies to make the remote clients accessing data via Internet safely.
- Finally, the application of browser will not be influenced or blocked by the firewall. Therefore, it can avoid the situation that VPN is unavailable due to the firewall application.

DrayTek VPN Solutions

At present, the models which support fully VPN functions contain Vigor2950, Vigor2930 and Vigor2930n. Here we focus on SSL VPN. The main applications for SSL VPN that DrayTek VPN solution provides are:

- **SSL Web Proxy**

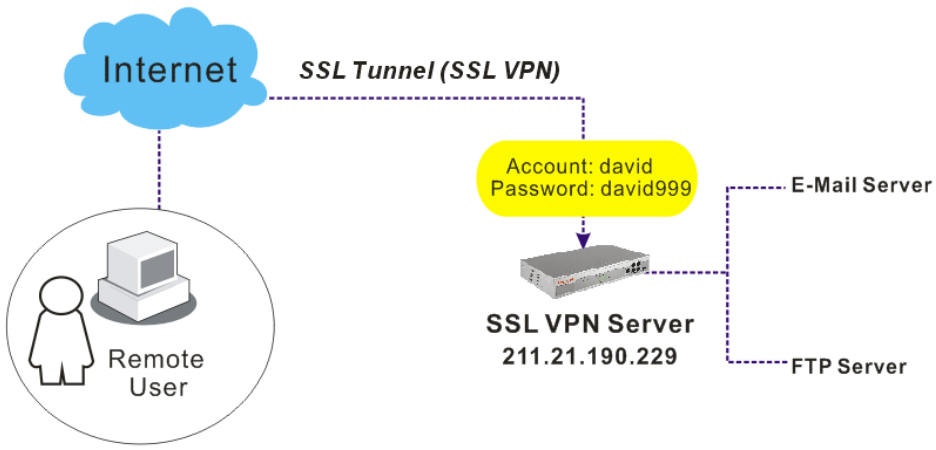
SSL Web Proxy will allow the remote user(s) to access into the internal system (e.g., ERP system, G-forge system, etc.) over HTTPS. Refer to the following figure for an example:



As shown in above figure, for the server end, the administrator must specify account(s) and password(s) for remote dial-in user and server profiles (URL); and for the remote user end, what he/she has to do is to obtain server IP address, account and password from system administrator.

- **SSL Tunnel**

It allows the remote users to make an SSL VPN Tunnel connection (which will not be blocked by any firewall or transferred by NAT) through Internet, suitable for the application through network accessing (e.g., e-mail server or FTP server). Refer to the following figure for an example:



• Access the desktop of a remote PC via SSL VPN

To access the desktop of a remote PC which is behind a NATed router, you have two options. One is by opening relative ports (e.g. TCP 5900 for VNC or TCP 3389 for RDP) on the router, the other is by connecting a VPN tunnel to the router. The former is easy but not secure as the router is exposed to the whole Internet. Furthermore it's hard to add security by using firewall policies to restrict the accessing IP addresses for mobility users. As for the latter method based on VPN connection, it provides security by requiring you to build a tunnel to the router before accessing the internal computers and the tunnel may be encrypted. There are three types of VPN connection:

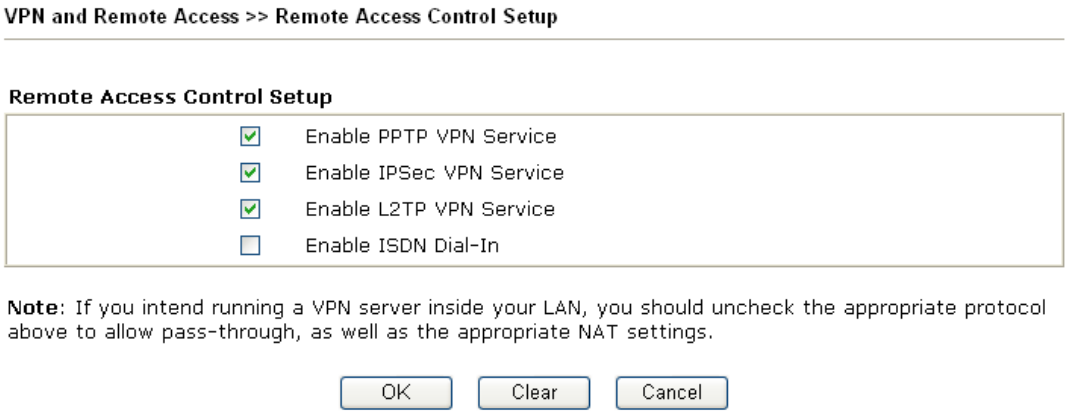
- Connect a tradition VPN connection to the office, such as PPTP, L2TP or IPSec.
- Connect a SSL Tunnel to the office.
- Connect a SSL VPN to the office.

With the above said method 1 and 2 you have full access to the whole office network, whereas with the method 3 you will be restricted to specific applications.

Vigor2950 now supports VNC and RDP applications and acts as VNC/RDP client. You can connect a computer to Vigor2950 via SSL VPN by using a web browser, such as IE or Firefox, then access the desktop of a computer connected behind Vigor2950 and running the VNC or RDP server.

• Remote Access Control

In remote access control setup, there are several VPN services provided by DrayTek routers and the operation is easy, too. Simply enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.



Conclusion

To sum up, SSL VPN resolutions provided by DrayTek can make people use the network resources more conveniently and safely. The remote users do not need to install any client software onto their computers additionally, and they can access the network for getting information via standard Internet browsers at any time. SSL VPN has the same advantage in data security as IPSec, however it does not own the shortcoming of IPSec. In addition, it can solve the compatibility problem caused by using NAT. Welcome visit DrayTek website to get more detailed product information: www.draytek.com.