NeoRouter is a cross-platform zero-configuration VPN solution that securely connects Windows, Mac and Linux computers at any locations into a virtual LAN and provides a networking platform for various applications like remote desktop, shared folders and printers, offsite backup, voice & video chat, games, etc. It is the ideal Remote Access and VPN solution for small businesses and homes.

Many small businesses or homes have high-speed Internet and multiple computers, and users are facing challenges like remote access, directory management and network security. To solve similar problems at large enterprises, skilled administrators can deploy very expensive and complex tools like VPN gateway, domain controller and corporate firewall. But small business or home users do not have the right tools that fit their needs. NeoRouter solves these challenges with a low-cost, integrated and user-friendly solution.
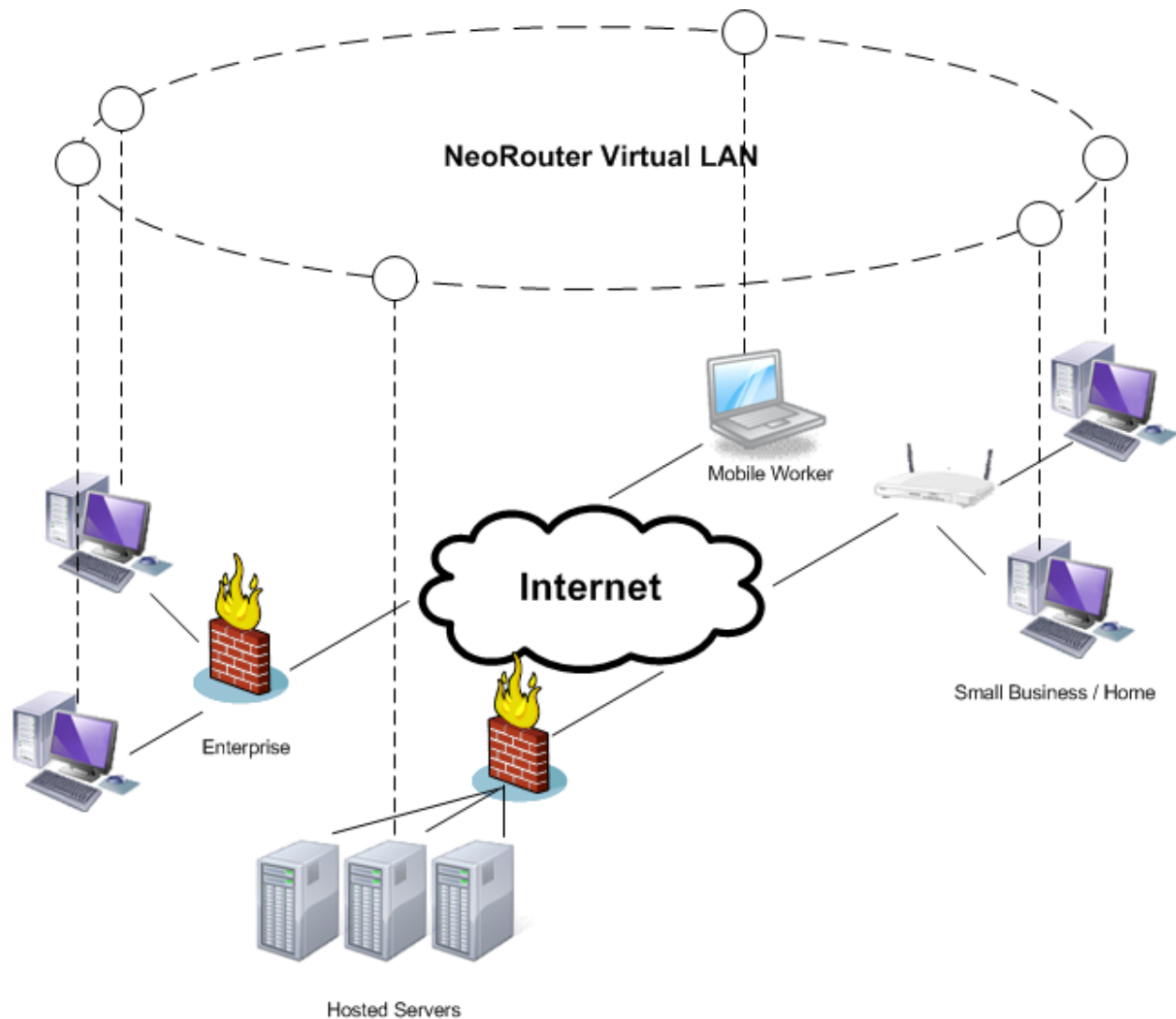
How it works

Remote Access

Every day we are dealing with multiple computers at work, home or other locations. It is often difficult to remotely connect to them because:

a) Corporate firewalls and residential routers segregate the network.

b) IP addresses are allocated dynamically and may change any time.

c) Port forwarding for every application is unsafe; some ISPs block certain ports.

NeoRouter can simplify this task by connecting all your computers at any locations into an overlay LAN-like network. These computers can communicate as if they were attached to the same network switch, so that user no longer needs to worry about the technical details of the underlying physical links. LAN-based protocols like NetBIOS/Samba and Bonjour can also work seamlessly over the virtual LAN. This overlay network is called a NeoRouter domain and you can create a friendly name to identify your domain.

neoROUTER

NeoRouter Virtual LAN

Mobile Worker

Internet

Enterprise

Hosted Servers

Small Business / Home

User can access a NeoRouter domain using the Network Explorer. After signing in with domain name and credential, you will see a list of computers in the domain. If you click on a computer, the launch pad dialog will pop up and it allows you to launch add-on applications and control the target computer remotely.

NeoRouter also provides a portable Network Explorer that you can run from a USB drive without installation. This feature is especially useful if you are using a computer that you do not have the privileges to setup new software, e.g. in a library or hotel.
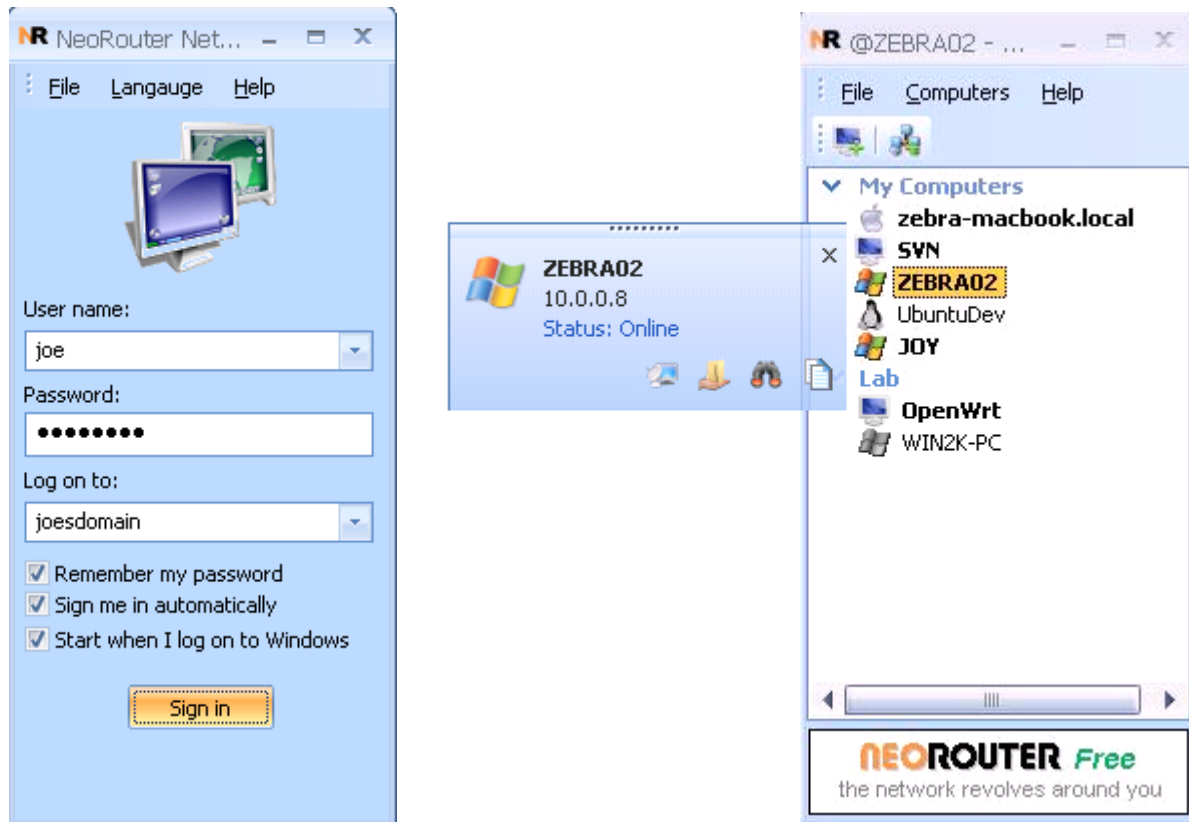
Directory Management

Traditionally VPN solutions rely on a separate Domain Controller to manage user accounts and access controls. NeoRouter provides a unique solution that integrates directory management into the VPN itself. This design has the following advantages:

a) Roam user profile: You can sign in a domain from any computer using the same account and your profile, including the computer list and your preference, will roam with you.

b) Manage access control in one place: Administrator can create multiple users with different privileges, and grant accesses to a computer or a service individually.

c) Support special network configurations like hub-and-spoke, subnets and one-way access.

d) Support Windows home editions, Mac and Linux: You can add computers with various OS to a NeoRouter domain, while Windows Domain requires client computers to have professional editions or above.

Connection and Security

NeoRouter employs a hybrid P2P design. Each NeoRouter domain consists of one server and multiple clients. Server is responsible for authenticating users and client computers, as well as mediating direct P2P connections between clients. Client first connects to server (blue lines) in order to join the domain. Then client computers can establish direct P2P connections (green lines) on demand and use them as the transport for application network traffic. These highly optimized P2P connections can provide fastest data transfer speed.
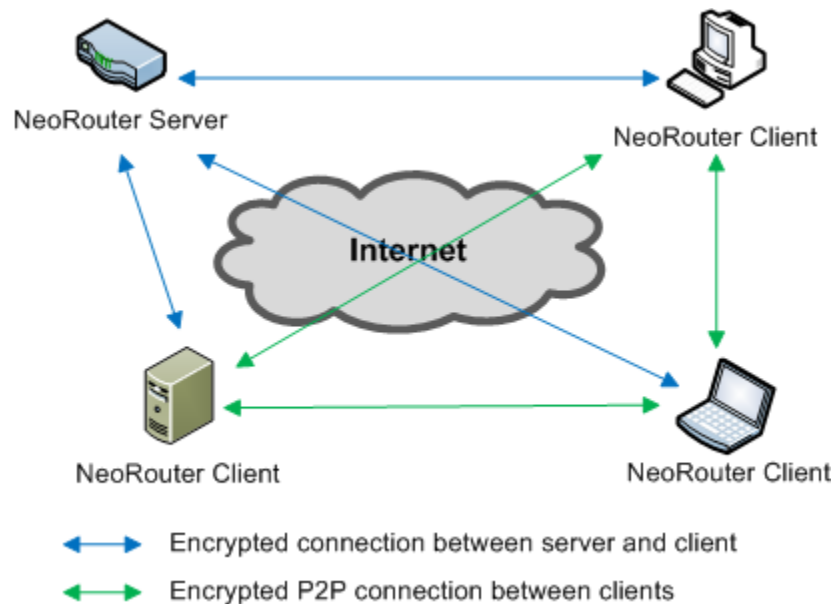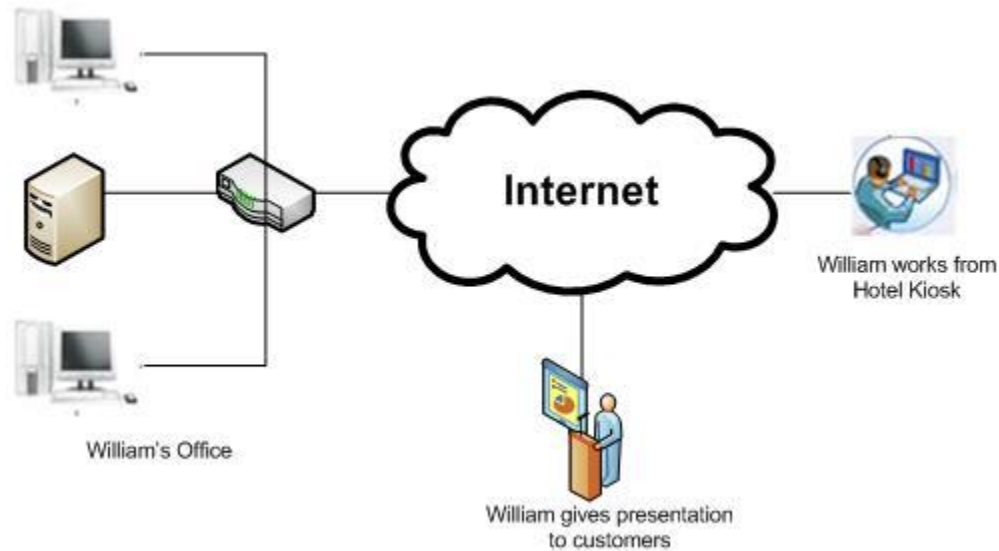
NeoRouter uses SSLv3 (AES-256) protocol to secure the communication channel between client and server and uses a suite of protocols (RSA 2048bit, DH and AES-256) to protect P2P connections among clients. This solution meets the industry's highest security standards.

For more information, please see User's Manual.

Use Scenarios

Work Remotely

William is a small business owner. He uses NeoRouter to connect all the computers in his office as well as the laptop that he travels with.

During the day, William gives a presentation at a customer's office and he needs to access sales reports on his office file server. William logs into the NeoRouter Network Explorer and his office computers appear in the computer list. He opens the shared folder on the file server, locates the reports and continues his presentation. The steps William uses to access his files are always the same regardless whether he is inside or outside his office; NeoRouter handles the network location differences.

At night, William goes back to hotel and the hotel offers computers with Internet access. William wants to remotely access his office computers, but he does not have the administrator privilege required to install software. He downloads the portable edition of the NeoRouter Network Explorer and launches it without installation. After log in, he sees the same computer list as usual and he can remotely connect to his office computers. When he finishes, he exits the NeoRouter Network Explorer Portable and no personal information will be left on the hotel computer.

Customer Supports
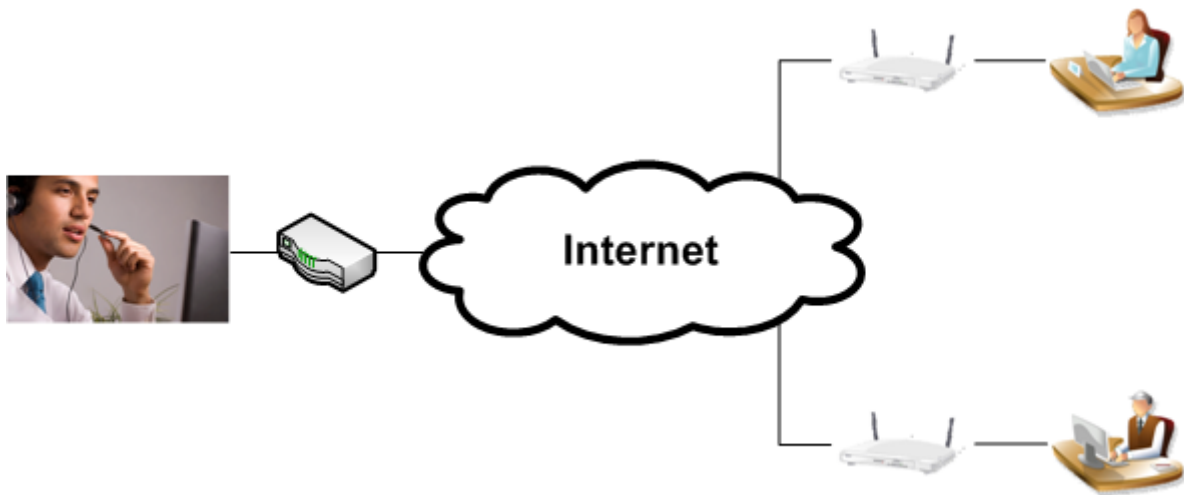
Jeff provides remote technical supports to his customers. He creates a NeoRouter domain and invites his customers to join. Then Jeff can use desktop sharing programs like VNC or Remote Assistance to connect to customer's computer and perform diagnosis.

Jeff configures the domain's access control list (ACL) following the hub-and-spoke template (see User's Manual). He will have full access to both customers' computers, but the customers are blocked from accessing each other's computer or Jeff's computer.

IT Management
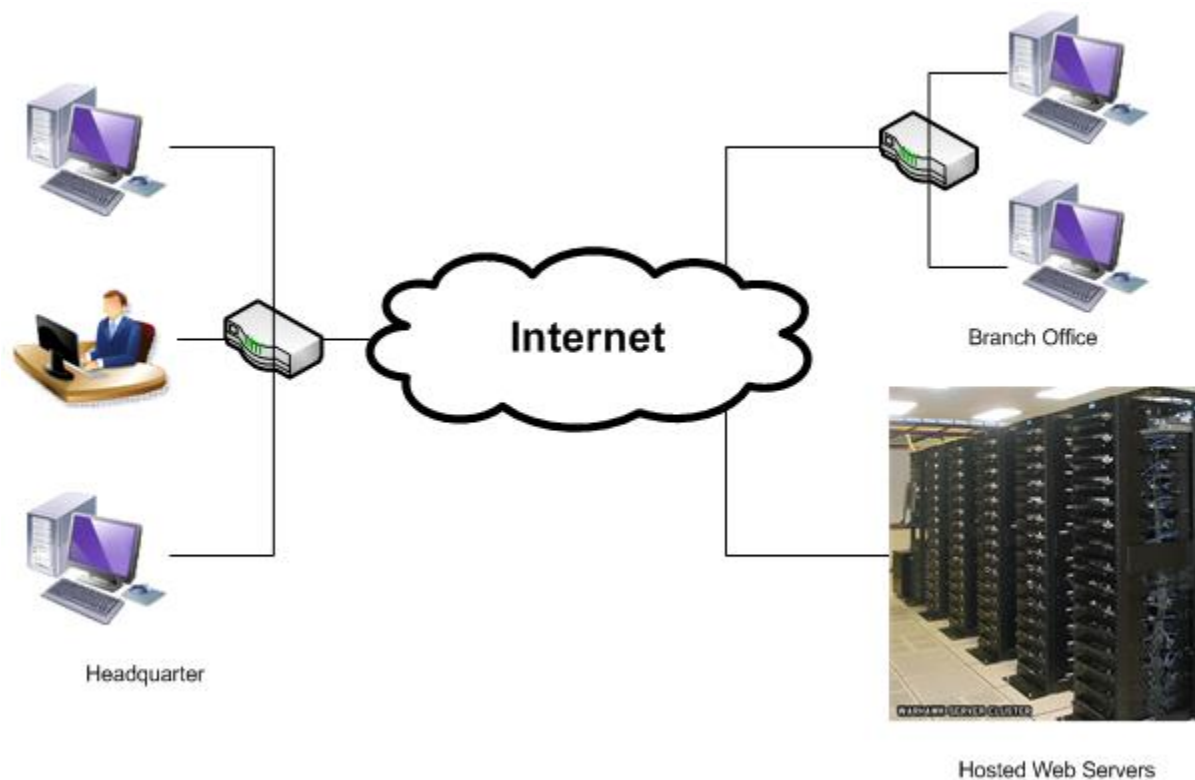
Mike is an IT manager responsible for deploying security patches and software updates to computers at company headquarter and branch offices. He setup a NeoRouter domain and connects computers at different locations to the domain. Then Mike can install updates and reboot the remote computers from his office. Because NeoRouter runs as a system service (daemon), the computers will reconnect to the virtual network automatically after reboot.

Mike is also responsible for managing the company's web servers (either blade servers or VPSs) at a Web Hosting Provider (WHP). The WHP allows SSH, FTP and remote desktop to the servers, but opening service ports through WHP's firewall is often difficult and unsafe. The WHP blocks the access to other services like database management, file sharing or custom tools. An easy solution is to add the web servers to a NeoRouter domain, so that Mike can access them as if they were in the same LAN. Mike can always trust NeoRouter to protect the network traffic to these servers.

My Digital Life (Home User)
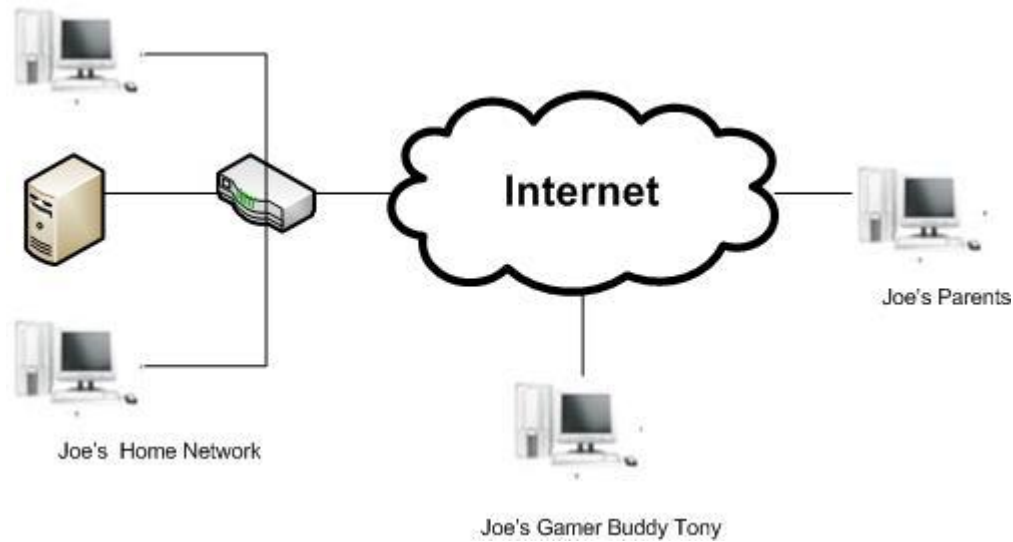
Joe likes to play video games with his buddy Tony over the network. He launches the NeoRouter Configuration Explorer and created an account for Tony. Tony installs the NeoRouter client on his computer and log into the Network Explorer using the account Joe created for him. Now Tony's computer is connected to Joe's domain and they can start playing games.

Joe also loves travel and photography. After a recent trip, he wants to share the photos with his parents. He creates an account for his parents and puts the photos in a shared folder on his computer so that the parents can browse remotely.

But Joe does not want to share the photos with his gamer friend Tony. Joe can use the NeoRouter Configuration Explorer to limit the computers and programs that Tony can access. In the access control dialog, Joe turned on the firewall for Tony and allows him to access games only. This change will not affect how Joe's parents access the network.