



Protexx Secure Internet Banking

The Problem:

The problem with the security of Internet banking is that it depends on the security of both client and server. Even if the bank's computer systems have all the security protection provisions in place internally a customer's personal computer is unprotected and can become infected with malicious software and susceptible to hacking and identity theft. Therefore all of their money is still at risk no matter what internal banking security policies exist. And unfortunately it is very difficult to maintain the security of a modern personal computer. If you are an expert in computer security, you know that you are only one mouse-click or one security hole away from allowing someone else to take control of your computer. If you aren't an expert in computer security, then the odds against you becoming a victim are even more overwhelming.

The security advice that banks give to customers on their websites is usually along the following lines:

- Be careful which websites you access.
- Be careful opening email attachments.
- Install your own personal data encryption software
- Install your own anti-virus software, firewall software, anti-spyware software.
- Don't forget to keep all your operating system software and application software up-to-date with security patches.

Even if you follow these best practices you are still just one click from disaster.

If you do your banking on your personal computer via the Internet, trouble can mean big trouble. When you type your user name and password into your computer to access your bank account online, you are giving your credentialing away and now your computer and all the software running on it has full access to that same bank account information. And if your Internet banking lets you withdraw money out of your bank account and send it to someone, then the opportunity for criminals to quickly and easily steal money from you can be devastating.

The Solution

Incredible as it may seem, there is a simple security solution that is available to almost all modern personal computers, which can be used to completely encrypt all of your data and to prevent further malicious attacks due to illegal access to your computer. The name of this security solution is **Protexx Safe Search**.

Its effectiveness arises from a few basic principles of how computers work:

- Most of us turn our computers on when we want to use them, and turn them off again when we have finished using them.
- When the power is off, the computer loses all the data in its working memory.
- Therefore, a computer must have built into it a security encryption process which operates when it starts up. This process loads a simple software, accessible from any web browser, and resides on your client, and this program then proceeds to create a secure tunnel allowing all additional connectivity to it protecting all of your "data in motion".
- By preloading encryption software on the client or through a biometric clip drive ensures the user that they are the only one who is authorized to access the transmitted data with up to three factor authentication.

But they may not be such a problem for those occasions where we need to use a computer for a task where security is more critical. For example, when we do our Internet banking.

The basis scenario or "use case" is as follows:

- You decide to do your Internet banking.
- If the computer is already on, you double click on the Protexx icon in your system tray enabling Protexx Safe Search. This instantly opens up a secure tunnel and provides you with a anonymous IP domain proxy making you invisible on the Internet to Hackers and Identity Thieves..
- With Protexx engaged you can now establish a secure connection to the Internet or tunnel directly to a secure server site (access to the secure server site could be limited to tunnel access only).
- You enter your URL
- You may now log into your account, and perform Internet banking functions securely through the tunnel.
- You log out.
- You either keep Protexx running protecting all of your "data in motion" or you can right click on the double icon in your system tray to temporarily disconnect Protexx encryption protection. We highly recommend keeping Protexx on at all times.

Fortunately Protexx has been especially designed for the purpose of secure Internet banking. Assuming that more can be achieved in the short term with maximum use and leverage of existing technology, the following are the design features which I think are most important to secure Internet banking:

- It should be based on Linux for OS and Mozilla for web browser.
- Both of these components should be "stripped down" to remove non-essential functionality.
- ISPs should provide configuration options to reduce user-specific configuration to zero. (A particular problem is that of static IP addresses which must typically be set on the user's computer. In contrast to this, DHCP gives automatic configuration, but is used in situations where IP addresses are not static. A solution might be to provide DHCP or some similar protocol which can work even for users that have static IP addresses.)
- Protexx provides the user with an IP address that is DHCPed from the Protexx tunnel server, an option to provide static IP is available and is based on the certificate.
- Banks should make sure that their websites can work with minimal web browser functionality, and in particular should not require the users to access their accounts with a proprietary web browser or other proprietary software.

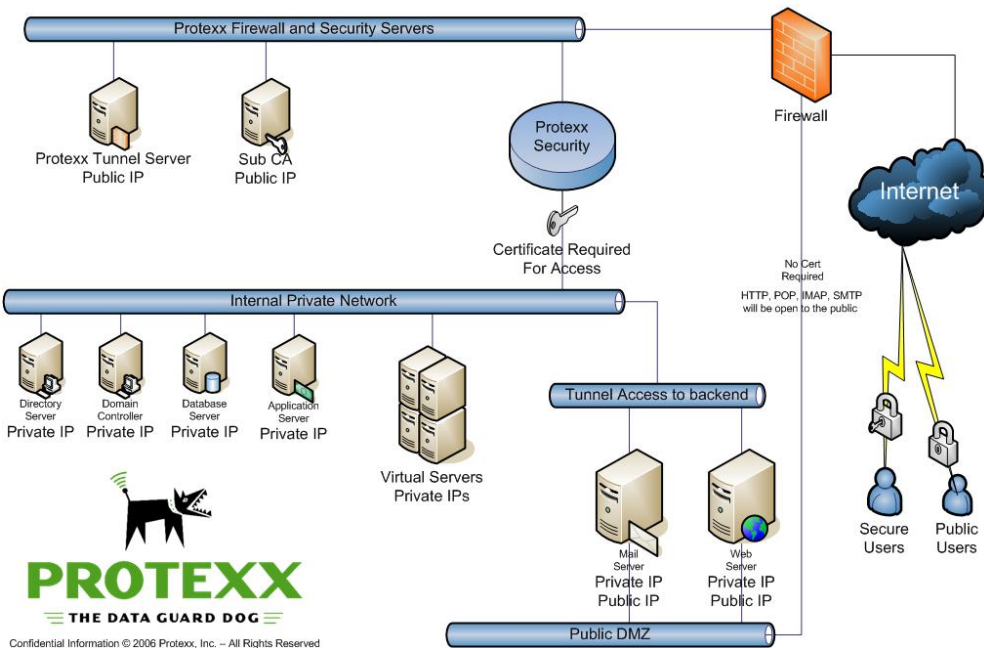
Issues

An encryption solution seems to be the only practical solution to the Internet banking security problem, and is certainly better than the "always be careful when surfing" advice given on banking websites. But it will not be an absolute guarantee of impregnable security, and there are a number of issues that need to be considered by those recommending such a solution, and which may require changes to its design:

- Not all Internet banking operations need to be made completely secure. Just browsing bank statements is not as security-critical as being able to transfer money to someone else's bank account in Florida. Banks should offer users multiple sub-accounts and premium services with different capability levels.
- Users might wish to print out a record of what they have done online. Accessing printers increases required boot time (although this could be deferred until something actually needs to be printed). One possible solution comes back to separation between security-critical and non-security-critical functionality: printing records of transactions performed could be done by access to a read-only sub-account.
- Computer compromises are caused by security holes, and even with the Protexx software enabled it is still likely that your system may contain inherent bugs, some of which will be security holes. The ability to exploit such holes is much more limited than when the system is running without encryption, because whoever or whatever manages to

break in to must take advantage of the break-in immediately, before the user completes their banking activity and logs off. The number of opportunities to break in is also much reduced. The user will not be installing any new software while doing their Internet banking, which leaves only security attacks based on the processing of untrusted data. Given that an Internet banking user only accesses known and trusted websites, the only possible source of malicious data is either raw IP packets, or something very tricky in the account detail itself.

Protexx Security Architecture



Stop living in fear of losing sensitive information to hackers, "Evil Twins", and man in the middle phishing attacks.

The Protexx Safe Search Offer



- Secure Your online Banking Transactions
- Secure Your Wi-Fi Hotspot Connections
- Secure Your Network Connections
- Secure Your Home and Office Cable and High Speed Access
- Secure Your email and File Transfers
- Become Anonymous on the Internet
- Safe and Encrypted Connections Between Your Computer and the Internet

What does Protexx do?

- Ensures your privacy when using online banking, Wi-Fi hotspots, Wireless, Cable, and Network connections by keeping your personal information safe and anonymous from hackers.
- Provides the highest level of encryption (up to 2048 bit) due to the recent security breaches cracking SSL, DES, 3DES, CDMA, WEP, WPA.
- Automatically encrypts all your inbound and outbound Internet traffic (emails, HTTP, FTP, Web, IM and VoIP calls, etc.)
- Provides Identity Management as *"Protexx knows you are who you say you are"* by the issuance of PKI Digital Certificates".
- Provides a personal firewall to block Wi-Fi, Wireless, Network and Cable hackers from using your connection to gain access to your computer and stealing confidential files or infecting your computer with viruses.

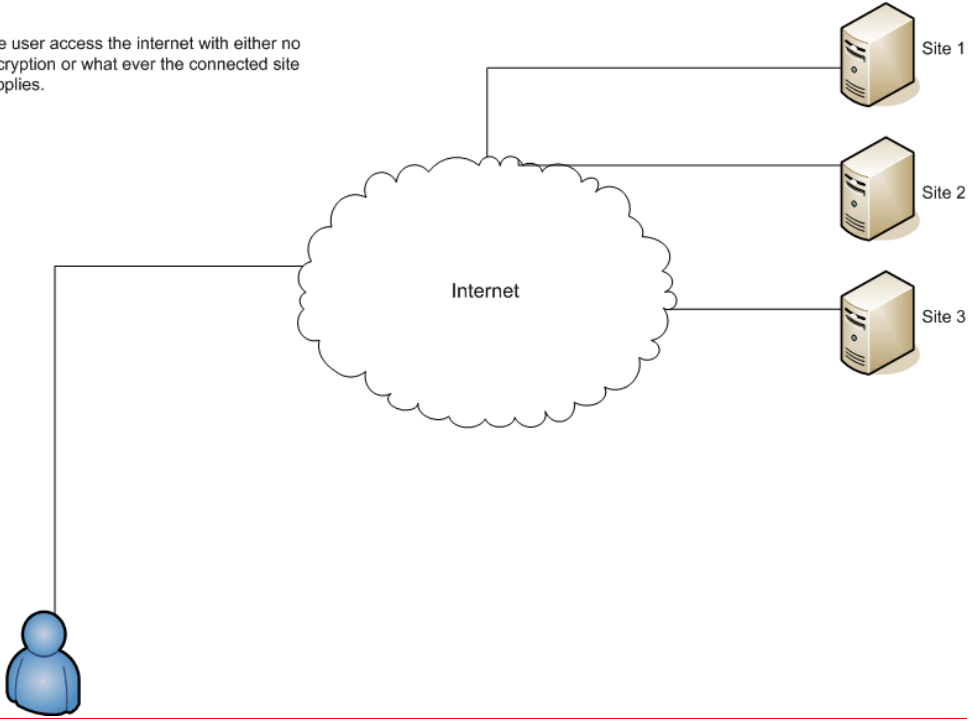
With all of the recent reports of identity theft and online fraud crippling businesses and putting extreme pressure both through legislative and litigation to protect data and intellectual property, corporate entities, private business owners, and everyone using the Internet for personal or for business needs protection.

The Protexx Safe Search adds a premium security service for you by offering encryption protection of all of your "data in motion".

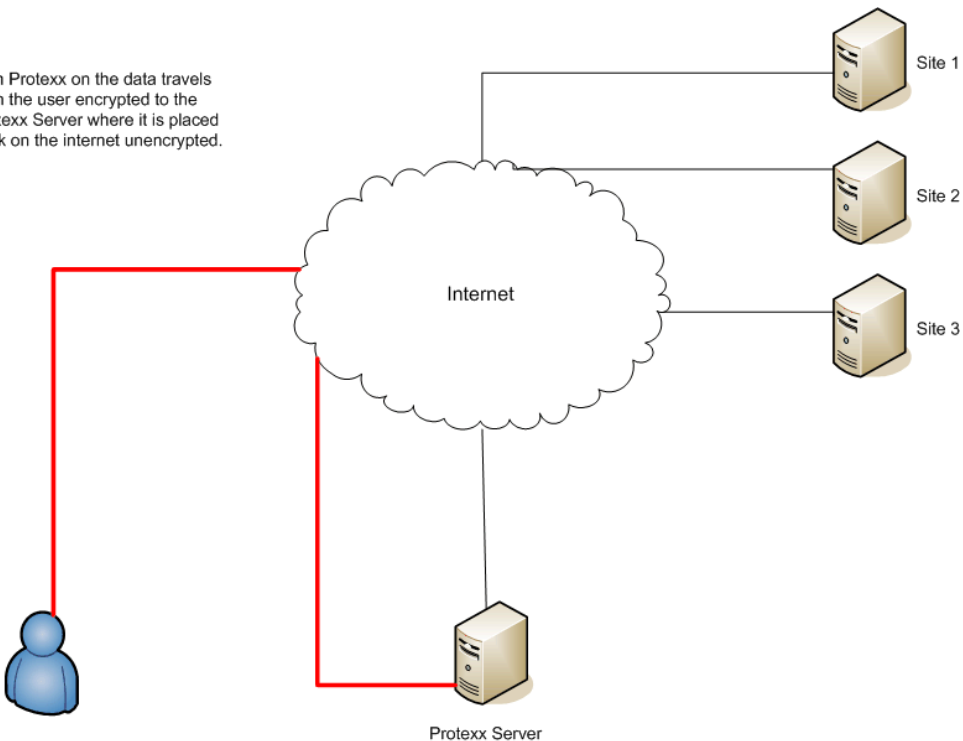
This Protexx Safe Search does it all as it is both versatile and economical and has the ability to secure online banking, Wi-Fi, Wireless, Network, Cable and Satellite transmissions with our Secure Information Transmission Highway (S.I.T.H) Digital Certificates. Protect your assets and customers from eavesdropping, hacking and identity theft now!

Cost just \$9.95 per certificate per month or just \$59.00 annually.

The user access the internet with either no encryption or what ever the connected site supplies.

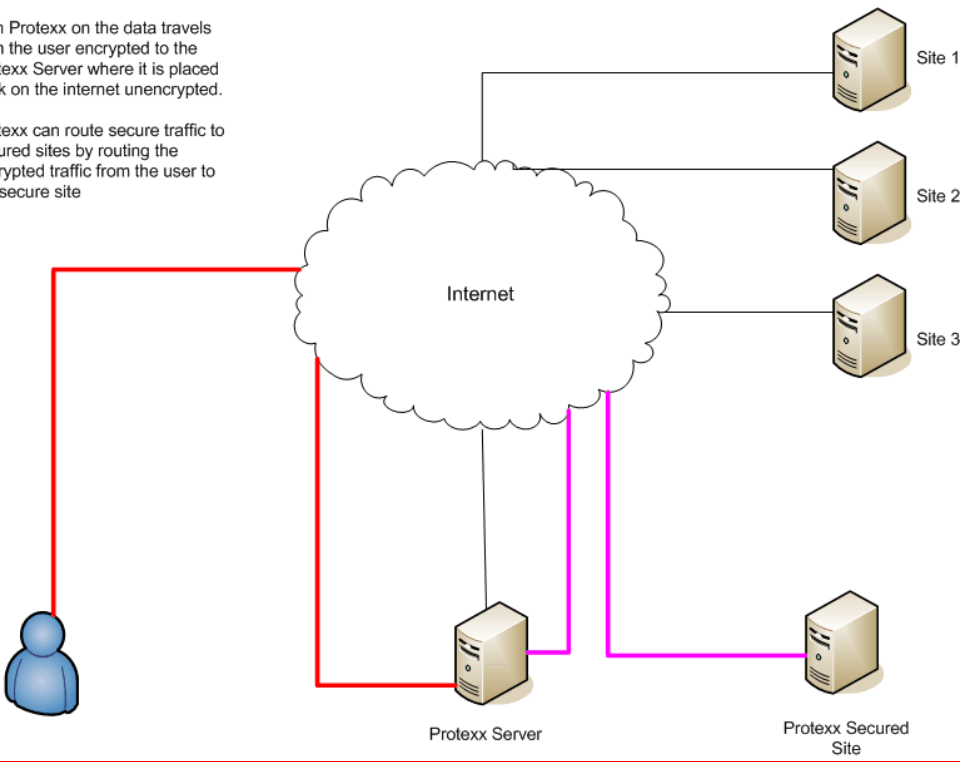


With Protexx on the data travels from the user encrypted to the Protexx Server where it is placed back on the internet unencrypted.



With Protexx on the data travels from the user encrypted to the Protexx Server where it is placed back on the internet unencrypted.

Protexx can route secure traffic to secured sites by routing the encrypted traffic from the user to the secure site



Private Secure Site, the user is only tunneled to the Private secure site all other traffic is open. This can give the user access to other systems behind the secure server.

