IN THIS ISSUE:
~ VPN (IPSec vs. SSL)

COMING NEXT MONTH:
~ Terminal Server

READY NET GO … NEWS

March 2006 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

Browser Wars Continue

Nearly everyone needs a program to surf the web and fortunately we have choices outside of Internet Explorer (note: IE is required for some tasks such as accessing Outlook Web Access). Two good programs to use that currently don't have as many security concerns and offer advanced features:

1) Firefox has a new update which includes new security features. Download version 1.5.0.1 http://www.mozilla.com

2) Opera has released a no ad version of its free browser. Download 8.5 here:

http://www.opera.com

NOTE: IE 7.0 (currently in beta) will be debuting in 2006 and will be shipping with Windows Vista. Download the new version when it becomes available to consumers if you don't have plans to upgrade to Vista immediately.

New features in IE 7.0 include:

1) New interface – no more bulky toolbars.
2) Tabbed browsing allows you to have more than one webpage open without cluttering your taskbar with individual pages.
3) Search box at the top of the screen is always available. You can even choose which search engine you want to use.
4) RSS feeds – easy to subscribe and read current feeds.
5) Increased security measures alert you to known Phishing sites and malicious programs that may download without your knowledge.

Remote Access with VPN's

VPN's – **Virtual Private Networks** – are increasingly becoming more popular. The technology allows people to work away from the office either at home, on business trips and even in extreme cases, on vacation, all through a secure connection. Setting up a VPN can be time consuming and requires maintenance but the benefits are far reaching given the increasing need for remote access by multiple users.

A VPN is a **secure way to access files on a network** over an Internet connection or other public or private network. A VPN is similar to an intranet (a password protected network set up for internal company use) except that a VPN can be accessed from outside the confines of the office. An example: set up a VPN between your home PC and your work PC and you can access work files without the need to transfer files with an external flash drive or disc. Other users on your network then have immediate access to the updated files.

How VPN's Work

Here are the basic steps involved in setting up a VPN:

1. Install a VPN-enabled router and/or firewall on a network (for IPSec VPN's also install VPN client software on a remote computer);
2. From the remote computer, initiate an SSL VPN session by logging in with a username and password & secondary credentials if required – for an IPSec VPN, just click a preconfigured icon;
3. After the VPN firewall/router authenticates you as a secure user, you will have access to designated areas of the network;
4. When you are finished, disconnect from the VPN to close your session.

WWW (Websites Worth Watching)

1. www.garden.org – Gardening tips for beginners and experts – includes info on individual species.
2. www.chanticleergarden.org – Get inspired for this season's gardening (located in Wayne, PA).
3. www.upenn.edu/arboretum - More inspiration at the Morris Arboretum in Philadelphia.

Three parts to a VPN

1. Tunneling – a secure channel between two endpoints; the originating data cannot be altered during transmission because of encryption.
2. Encryption – the VPN appliance encrypts or scrambles the data so it is unintelligible to outsiders, which serves as a security measure. This is an extremely important step because the data is traversing the public network. Only the VPN appliance on the other end can decode the data to its original state.
3. Authentication – Process in which a VPN appliance ensures that the data it has received is from a known good source.

There are three types of VPNs - IPSec, Site-to-Site IPSec, and SSL

1) **IPSec** – IP Security – a type of protocol in which a **VPN appliance** (router or hardware firewall) communicates with VPN client software installed on remote computers. IPSec is best employed if users need full access to network resources and files; user rights policies will always take precedence however. **Downfall to this type of VPN** is that client software must be installed, configured, and maintained by users or administrators.

2) **Site to Site** (or point to point) – a type of IPSec VPN in which a VPN device at one branch office is configured to receive and send communication to a VPN device in another branch office. This type of configuration works well for departments in different locations that need to share information regularly. **VPN-enabled routers or hardware firewalls** handle the encryption and authentication necessary for secure point-to-point transmissions. No client PC configurations are necessary.

3) **SSL** – Secure Socket Layer – a type of protocol in which a user communicates with a VPN appliance over a **secure Internet connection**. You may already be familiar with SSL. When you make a purchase through an online retailer, you should see a lock icon in the task bar and the address of the site changes to https:// – this means that the site is using an encrypted SSL connection to ensure that your personal information cannot be tampered with during transmission.

   In regards to VPN's, the **SSL protocol** is similar to an IPSec protocol except that **client software is not required** to be installed on the remote PC. This makes SSL VPN's a preferable solution when the remote PC is not controlled by the user such as at Internet cafes, kiosks, or in hotel business centers. Because users can log on with a username and password from any computer, this type of protocol is advantageous to implement in large organizations that have numerous users (hundreds or thousands of people) or for businesses that do not want to purchase laptops for their employees. **Downfall to SSL** is that a user may not be able to access network resources remotely using public terminals (User policies on remote terminals may prevent individuals from installing components because they will need to logon as an administrator to do so). The initial cost of setting up an SSL VPN is also much higher than with an IPSec VPN.

New features in VPN appliances

Unified Threat Management (UTM) and multi-layer inspection devices increase protection by inspecting packets of information for viruses, spyware and spam before allowing the data into the network. Devices with these capabilities built-in reduce the need and potential conflicts of employing third party software to achieve comprehensive protection. These types of devices are expected to grow in popularity over the coming years as businesses continue to seek ways to secure data and improve productivity.