Configure Windows Server 2008 to remotely access SSL VPN Server (Part 1)

Remote Access (Remote Access) is a very important issue today. As the number of people needing access to information is saved to home and work computers, the ability to access information from anywhere becomes a matter of utmost importance.

Thomas Shinder

Remote Access (Remote Access) is a very important issue today. As the number of people who need to access information is saved to work and home computers, the ability to access information from anywhere becomes an important issue. You can say ' *I will get information for you when I get into my computer* '. You will need that information if you want to compete in today's business environment.

In the past, the way to access remote information on a computer was done using a dial-up connection. RAS dial-up connections work on regular POTS (Plain Old Telephone Service) telephone lines and have speeds of about 56kbps. Speed ??is a big problem for dial-up RAS connections, but a bigger problem is the cost of connections for long distances required for access.

With the growth of the Internet, gradual dial-up RAS connections are no longer appropriate. That is due to the emergence of virtual private networks (VPNs). Virtual private network connections provide point-to-point connections that dial-up connections have provided, but with cheaper prices and much faster speeds, the speed of a virtual private network connection can be as fast as the connection. Internet connection and the cost of connection completely independent of the distance of the destination. The cost depends only on the Internet connection.

Virtual private network (VPN)

Connecting a virtual private network allows a computer to establish a *virtual* and *private* connection to a network on the Internet. The connection is *virtual* because when the computer establishes a VPN connection via the Internet, the computer creates connection operations such as a button that is directly connected in the network via an Ethernet cable. Users can access all possible resources, such as being connected directly to the network. However, in the case of connecting a VPN client to a VPN server, this connection is a *virtual* connection because there is no actual Ethernet connection to the destination network. The connection is unique because the contents of the moving data stream within the VPN connection are encrypted so that no one on the Internet can eavesdrop or read the contents of the moving data in the VPN link.

Windows Servers and clients have supported VPN connections since the early days of Windows NT and Windows 95. Windows clients and servers have been supporting VPN connections for decades, and the type of VPN support is growing. by the time. Windows Vista Service Pack 1 and Windows Server 2008 now support up

to 3 types of VPN connections:

1. PPTP
2. L2TP / IPSec
3. SSTP

PPTP is a point-to-point connection protocol. PPTP is the simplest method you can use to establish a VPN connection, but unfortunately, it also has the worst security. The reason is because important user information cannot be exchanged through a secure link. It can be said that the encryption of the VPN connection occurs after important information is exchanged. While important information is not transmitted between VPN clients and VPN servers, data can be attacked by sophisticated hackers accessing VPN servers and connecting to corporate networks.

A better security protocol is L2TP / IPSec. L2TP / IPSec is a collaborative development between Microsoft and Cisco. L2TP / IPSec is more secure than PPTP because there is an IPSec session set up before important information is sent over the signal line. Hackers cannot access important information of users and thus cannot steal or steal them for use for bad purposes. A more important point is that IPSec provides authentication mechanisms between computers, so unreliable computers will not be able to connect to L2TP / IPSec VPN gateways. IPSec also provides data integrity, reliability and non-repudiation. L2TP supports PPP and EAP authentication mechanisms for users, these mechanisms allow a high level of security for both user authentication and computer authentication are required here.

Windows Vista SP1 and Windows Server 2008 currently support a new VPN protocol - Secure Socket Tunneling Protocol or SSTP. SSTP uses SSL encrypted HTTP connections to establish a VPN connection to the VPN gateway. SSTP is a very secure protocol because important user information is not sent until a secure SSL 'tunnel' is established with the VPN gateway. SSTP is also known as PPP over SSL, so it also means that you can use PPP and EAP authentication mechanisms to ensure SSTP connections are more secure.

Private but does not mean good security

I need to remind you here that VPN connections are more about privacy than security. When I realized that privacy is a major component of secure communications, privacy itself does not provide security. VPN technologies provide communication privacy on the Internet, which prevents strangers from being able to read the content while you perform communications tasks. This technology also allows you to be secure because only authenticated users can connect to the network through the VPN gateway. However, privacy, authentication and authentication do not provide a comprehensive security solution.

For example, you have an employee and you want to recognize his VPN access. While the Windows Server 2008 VPN protocols support EAP user authentication, you decide to deploy smart cards to users and use the L2TP / IPSec VPN protocol. The combination of smart cards and L2TP / IPSec makes it safer for you to have good user and computer authentication. Smart card solutions and L2TP / IPSec work well and everyone is happy with it.

Everything is fine until one day when a user connects to the SQL server to access the salary information paid to the employee and expose that information to the employees. What is going to happen? Is the VPN connection secure in this case? We can affirm that it is security in some respects in terms of privacy, authentication, and authentication, but one thing that it does not provide is access control, which is an important aspect. Most important for computer security.

In order for the VPN solution to be truly secure, you need to make sure that the VPN gateway can perform access control based on users or groups to enforce minimum privilege access for users. . Advanced VPN gateways and firewalls like the ISA Firewall can fulfill this need for VPN connections. In addition, advanced firewalls such as the ISA Firewall can perform an inspection of the audited application and packet layer on the security status of VPN client connections.

Although Windows Server 2008 VPN does not provide user / group access control issues, there are a number of ways that you can enforce access control on the data servers yourself if you do not want to lose money to pay for Preferred firewall and VPN gateway. In this article, we only focus on the VPN server component.

Why need a new VPN protocol?

Microsoft already has two VPN protocols that allow users to connect to the corporate network, so why introduce a third protocol? SSTP is a great for VPN users because SSTP does not have problems with firewalls and NAT devices that PPTP and L2TP / IPSec still suffer from. For PPTP to work via a NAT device, this device needs to support PPTP through a PPTP 'NAT editor'. If there is no NAT editor for PPTP on a NAT device, then PPTP connections will fail.

L2TP / IPSec also has problems with NAT and firewall devices because the firewall requires L2TP port UDP 1701 open outbound, IPSec IKE port, UDP 500 open outbound, and IPSec NAT traversal port, UDP 4500 open outbound (L2TP port is required when using NAT-T). Most firewalls in public places such as hotels, conference centers, restaurants and other locations only allow a small number of open outbound ports, such as HTTP, TCP port 80 and HTTPS (SSL), TCP port 443. If you need support for protocols other than HTTP and SSL when you leave the office, you are very risky.

In contrast, SSTP VPN connections create a tunnel over SSL with TCP port 443. When all firewalls and NAT devices have TCP port 443 open, you will be able to use SSTP anywhere. This has been amazingly simple for life for 'on the road' employees, who really need to use VPN connections to the office to work and it also makes life a lot easier. much for corporate administrators who need support for employees on the road, as well as assistants at service providers who provide Internet access for hotels and associations seminars and other public places.

SSTP connection process

Below is how the SSTP connection process works:

1. SSTP VPN client establishes a TCP connection with the SSTP VPN gateway between a random TCP source port on the SSTP VPN client and TCP port 443 on the SSTP VPN gateway.

2. SSTP VPN client sends an SSL Client-Hello message, this message indicates that SSTP VPN client wants to establish an SSL session with the SSTP VPN gateway.

3. SSTP VPN gateway sends a computer certificate to the SSTP VPN client.

4. SSTP VPN client validates this certificate by checking its trusted certificate root repository repository to see if the CA certificate is placed in that repository. SSTP VPN client then determines the encryption method for the SSL session, creates an SSL session key and encrypts it with the public key of the SSTP VPN gateway, and then sends the encrypted session of the SSL session key to the SSTP VPN gateway.

5. SSTP VPN gateway decodes the encrypted SSL session key with its own key. All subsequent communications between the SSTP VPN client and the SSTP VPN gateway are encrypted using an encrypted method and an SSL session key.

6. SSTP VPN client sends an HTTP request message on SSL (HTTPS) to the SSTP VPN gateway.

7. SSTP VPN client negotiates an SSTP tunnel with the SSTP VPN gateway.

8. SSTP VPN client negotiates PPP connection with SSTP server. This negotiation involves verifying user certificates using standard PPP authentication (or even EAP authentication) and configuring settings for Internet Protocol version 4 (IPv4) or Internet Protocol traffic. version 6 (IPv6).

9. The SSTP VPN client now starts sending IPv4 or IPv6 traffic on the PPP link.

If you are interested in the characteristics of the VPN protocol architecture, then you can see in the picture below. Note that SSTP has an additional header compared to the previous two VPN protocols. This is because HTTPS encapsulation adds to the SSTP header. L2TP and PPTP do not have application layer headers in communication packaging.

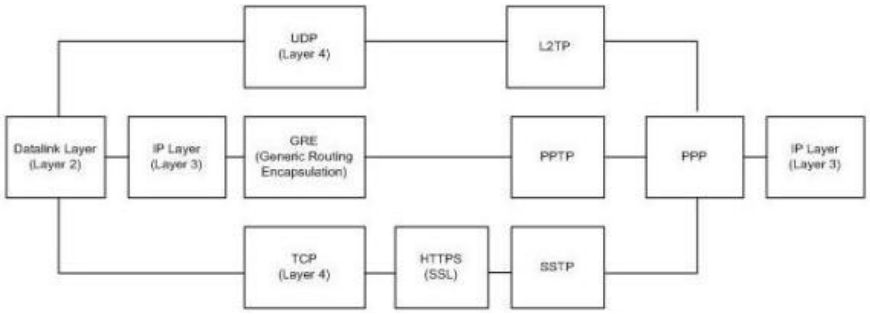


Figure 1

We will use a simple three-computer network example to show how SSTP works. The names and characteristics of the three computers here are:

Vista :
Vista Business Edition
Vista Service Pack 1
Members are not in the domain

W2008RC0-VPNGW :
Windows Server 2008 Enterprise Edition
Two NICs - Internal and External
Domain member

WIN2008RC-DC :
Windows Server 2008 Enterprise Edition
Domain Controller of MSFIREWALL.ORG domain

DHCP Server
DNS Server
Certificate Server (Enterprise CA)

Note that you must use Vista Service Pack 1 for the VPN client. Although there have been previous discussions about Windows XP Service Pack 3 in supporting SSTP, this is not important. We recently installed a version of the 'candidate' candidate for Windows XP Service Pack 3 on test computers and found nothing about SSTP support. This is indeed a pity because many laptops are currently installing Windows XP and most people have the idea that Vista runs too slowly for laptops. Perhaps Vista's effect issues will be modified in Vista Service Pack 1.

The high-level configuration of the example network can be seen immediately in the figure below.

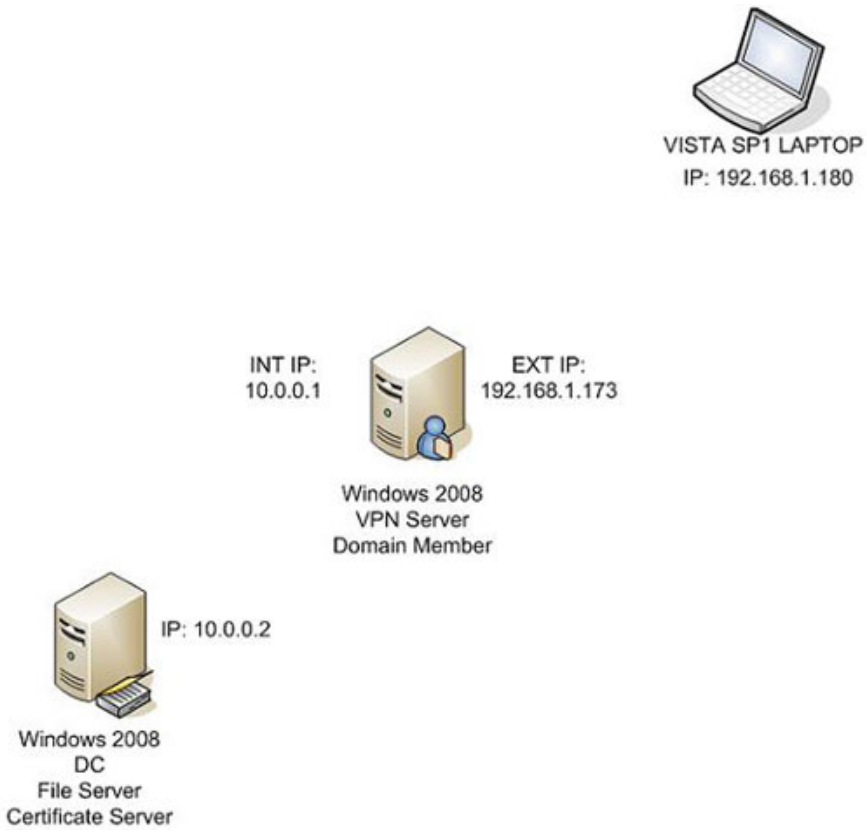
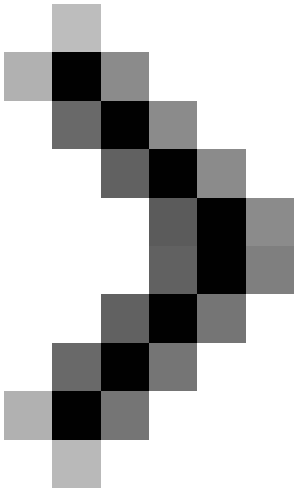


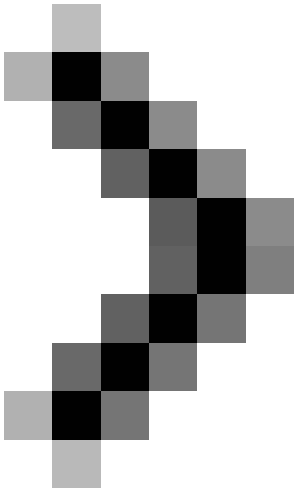
Figure 2

Conclude

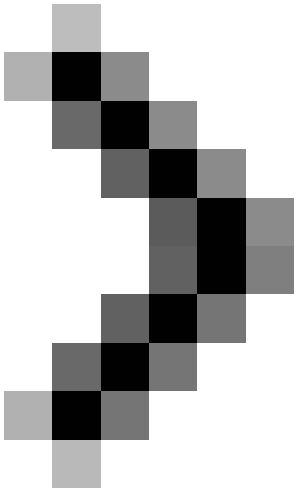
In this article, I have shown you a bit of history about remote access communications for computer networks. We then introduced the mainly supported VPN protocols in Windows Server and clients, introducing some security issues to previous VPN protocols. Introducing how SSTP addresses these problems with the previous two types of protocols, PPTP and L2TP / IPSec. Finally, we also introduced a simple example network that will be used in the next article to introduce more simple SSTP VPN client and server solutions with Windows Server 2008 and Windows Vista Service Pack 1.



Configure Windows Server 2008 to remotely access SSL VPN Server (Part 2)



Configure Windows Server 2008 to remotely access SSL VPN Server (Part 3)



Configure Windows Server 2008 to remotely access SSL VPN Server (Part 4)

You finished reading the article "**Configure Windows Server 2008 to remotely access SSL VPN Server (Part 1)**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
