Some new points in the network connection of Windows Server 2008 R2

In this article, I will show you some of the new networking issues of Windows Server 2008 R2.

In this article, I will show you some new things about the networking issues of Windows Server 2008 R2.

Windows Server 2008 R2 has been released for a while but there are many people who are still using Windows Server 2003 or maybe Windows Server 2008 for many different reasons. Each new release always comes with many new, interesting points if you have time to learn and exploit them. In Windows Server 2008 R2 too, it must be said that its new networking features are really interesting, and this article will cover that content.

Some features in Windows Server 2008 R2 will definitely appeal to you:

DirectAccess

VPN Reconnect

BranchCache

URL based QoS

Here we will take a look at these features.

DirectAccess

DirectAccess is a new remote access technique that allows domain member computers to connect to the local network without a VPN connection. You may have heard a lot of information about DirectAccess as a type of VPN connection, but in fact, DirectAccess is much more than a VPN. Microsoft has developed this technology as an alternative to VPN. So what's the difference here? Virtual Private Network allows your users to access the network when they want to access information here. In contrast, DirectAccess allows you to expand your network itself to all DirectAccess-enabled clients, so users will always connect to your local and IT networks that are always connected to DirectAccess clients. The big advantage is that, in contrast to VPN clients, DirectAccess clients are always in control, always up to date, and always comply with the desired configuration settings.

The only two ways to achieve that are to upgrade, because DirectAccess requires Windows Server 2008 R2 on the server side and Windows 7 Enterprise or Ultimate on the client side. You may or may not be able to upgrade the entire network infrastructure, depending on which DirectAccess form you deploy (we'll cover that in the next section).

DirectAccess is not a specific technique, it is a collection of available techniques and is combined together under a common name 'DirectAccess'. The main techniques in DirectAccess include:

Active Directory - The DirectAccess client and server must be members of the Active Directory domain to ensure authentication.

Group Policy Objects (GPOs) are used to distribute DirectAccess-related configuration settings to both DirectAccess servers and clients.

DNS - DirectAccess uses DNS to determine which connections will be sent via the DirectAccess connection, which will be sent directly to the server on the Internet.

PKI - DirectAccess uses computer certificate authentication and IPsec, PKI request techniques to deploy certificates.

IPsec - DirectAccess is a secure access solution that takes advantage of both IPsec tunnel mode and IPsec transport mode to secure remote connections from DirectAccess clients to DirectAccess server and to servers located in the intranet.

IPv6 - DirectAccess is a technology expected, this technology is built on IPv6 future network protocol. (However, with UAG, you don't need to have a native IPv6 network for DirectAccess to work on your current network.)

Some of these techniques are available in any Windows domain. Some may or may not be used in your network. All of these techniques can be used with previous versions of Windows Server, but are used in a discrete and only way in Windows Server 2008 R2, all of which are combined to create a DirectAccess solution. .

The important thing here is to understand that there are two types of DirectAccess, namely: Windows DirectAccess and UAG DirectAccess. The Windows DirectAccess format for small and medium-sized

businesses has only a few servers, but to use it, you must have an original Windows Server 2008 R2 domain and an IPv6 network. For large enterprise deployments, you need to use the UAG DirectAccess solution because this format is scalable and quite solid. In addition, UAG DirectAccess allows you to use DirectAccess even without deploying IPv6 and without Windows Server 2008 infrastructure (still having a Windows Server 2008 R2 machine on which UAG is installed).

VPN Reconnect

While DirectAccess is an alternative to VPN, VPN Reconnect, a new VPN technology included in Windows Server 2008 R2 is similar to other VPN protocols, such as PPTP and L2TP / IPsec. It uses the same VPN connectoID that is still used by these VPN protocols. However, the big difference between VPN and VPN Reconnect protocols is: with VPN Reconnect, the connection is automatically reset when the connection is lost. In the meantime, if the VPN connection is lost, the user will not receive a message saying that the connection is lost and asks if he wants to reconnect. Instead the software will reconnect them.

This method is very convenient for mobile users. For example, suppose you are using a Wireless WAN connection through an account. Now you're on the train and checking your email or working on something . Things are going on as expected, then the train goes through the tunnel section. In the Internet connection tunnel is broken because there is no radio wave. Although you are working with emails in Outlook at the same time, you still don't realize that your connection has failed (that is, VPN Reconnect connection). When the train goes out of the tunnel, the Internet is connected again and the VPN Reconnect connection is automatically reset. All of this happens in the background so users are unaware that their Internet connection is dropped during the train's passage.

VPN Reconnect uses IKEv2, applies new features via IKEv2 mobile capabilities and multihoming techniques (techniques to increase reliability) described in RFC4555. You need to have Windows Server 2008 R2 and Windows 7 clients to use VPN Reconnect. Previous Windows versions do not have this feature.

There is a bit of similarity between DirectAccess and VPN Reconnect. Both of them allow connection in a way throughout the corporate network and they both automatically reconnect if the Internet connection is dropped. However, there are some significant differences:

DirectAccess requires DirectAccess clients to be domain members and VPN Reconnect does not require that.

DirectAccess allows connection to management servers before the user logs in, and VPN Reconnect starts when the user launches VPN connectoid to establish the initial connection.

DirectAccess is designed to support 'end-to-edge' and 'end-to-end' security, while VPN connectoid is only designed to support 'end-to-edge' security.

In general, you should use VPN Reconnect for non-domain members. As for domain members, managed computers, DirectAccess is the preferred remote access technique.

BranchCache

BranchCache is a new technology in Windows Server 2008 R2 and Windows 7, allowing users at branch offices to access information at the main office faster than ever. The biggest problem that users at branch offices encounter is access to data at the main office over a restricted WAN connection or site-to-site VPN to the main office. This problem sometimes leads to users avoiding access to information that can help them increase

productivity and add more value to the company.

BranchCache can be used to store the main office data at the branch office. When users connect HTTP (S) or SMB (CIFS) to resources located in the main office, that data will be stored at the branch office. When another user then tries to access that data, this data will be provided from the local cache stored at the branch office. This method significantly increases data access speed because it is provided at LAN speed at branch office (Gigabit Ethernet) instead of WAN speed (still within 10 Mbps).

BranchCache can be configured under either of the following modes:

Hosted Mode - In Hosted Mode, BranchCache works with a BranchCache server that holds cached data for all computers in the branch office. When the BranchCache client in the branch office requests data from the main office, it will access the data and then share this data with the BranchCache server. When the second host at the branch office creates a request with the same content, it will connect to the resource server at the main office to authenticate and receive the metadata to determine if the content has been changed. with what was previously cached or not. If nothing has changed, it can use data stored locally with LAN speed from Hosted Mode BranchCache at the branch office.

Distributed Mode - In Distributed Mode, there is no BranchCache server, instead Windows 7 clients will share cached data with each other. When a Windows 7 computer at the branch office receives data via SMB or HTTP (S) from the main office, it will cache this information locally. When another Windows 7 computer at the branch office makes the request with the same content, it will authenticate with the original server and receive the metadata, then receive the data at LAN speed from the Windows 7 client. required the same content before.

Distributed Mode is used when there are fewer than 50 computers in the branch office network. All computers need to be in the same network segment. If the branch office has more than 50 clients or has multiple network segments, you need to use Hosted Mode.

URL based QoS

Windows Server 2008 R2 and Windows 7 currently support Quality of Service (QoS) based URLs. This is the technology already in ISA Server and Threat Management Gateway (TMG) but now it is granted to clients and servers in the network.

What's new is that IP packets containing the Differentiated Services Code Point (DSCP) value, which is the value for routers configured with DSCP values ??can be checked to assign priority. When routers are busy, the packets will be queued and queues can be configured with the preceding high priority packets, the lower priority level.

With Windows Server 2008 R2 and Windows 7, you can use URL-based QoS to prioritize network traffic based on source URLs, add priorities based on IP addresses and ports. This method allows you to add control over network traffic and ensure that high priority web traffic is forwarded to low priority traffic, even when the traffic is allocated from same server. This is a big difference in performance.

For example, you will certainly have a large number of internal web servers that users need to access to perform their jobs. You can then assign these internal servers addresses with higher priority than external server addresses, so traffic to important internal resources will take precedence over With traffic to the server does not matter.

Conclude

In this article, I have shown you some of the new networking features available in Windows Server 2008 R2 and Windows 7. It's DirectAccess, a new remote access technology that helps extend your intranet. to any domain member computers no matter where these computers are located; VPN Reconnect, a great solution for non-domain member computers that need to have a VPN connection to the corporate network, allowing easy connection, without the hassle of having to reset VPN connections. ; BranchCache, a feature that allows clients at the branch office to receive content from the main office at the speed of a LAN instead of a slow WAN; URL-based QoS, which allows you to prioritize URL-based connections from which to make appropriate adjustments on web servers for network connectivity.