Installing and configuring the 2004 ISA Server Firewall - Chapter 4

The Windows Internet Name Service (WINS) when this Service is deployed on the Internal Network Domain, it will serve the Computer in the Network to resolve to find the same NetBIOS names.

Chapter 4: Installing and configuring Microsoft DHCP and WINS Server Services

The Windows Internet Name Service (WINS) when this Service is deployed on the Internal Network Domain, it will serve the Computer in the Network to resolve to find the same NetBIOS names, and a Computer A in this Network can through WINS server to solve. Determine the NetBIOS name of Computer B on another Network (of course the WINS system is normally only used to resolve the Netbios names in the Organization's Internal Network, to avoid confusion with how to resolve the DNS server's hostname - possibly ability to resolve the FQDN name (www.nis.com.vn) of the Internet or the Internal Network Domain.

You can refer to 'BUILDING NETWORK INFRASTRUCTURE ON MICROSOFT WINDOWS SERVER 2003', about to be released by me to better understand the role of a WINS server in Internal Network.

Computers on the Internal Network will be configured as WINS clients, registering their names (Netbios / Computer names) with WINS servers. WINS clients can also send name query requests to the WINS server to resolve Name to IP addresses. If in Internal Network there is no WINS Server, Windows clients will send broadcast messages to find Computer Netbios name to communicate. However, if these computers are located in another Network (with other Network IDs), then these Broadcast will be blocked (broadcast blocking is the default on the Router). So in the Internal Network of an Organization, including many Network Segments, the resolution is for Computer from Network 1 to find NetBios name of Computers in Network 2,3. Using WINS server is the ideal solution.

WINS server is also particularly important for VPN clients. VPN clients do not directly connect to the Internal Network, and thus cannot use broadcasts to resolve NetBIOS names of Computers within the Network. (Unless you use Windows Server 2003 and open the NetBIOS proxy function, the NetBIOS broadcast will be supported, but very limited). The VPN clients rely on WINS server to resolve NetBIOS names and use this information to search for Computers in My Network Places of the Internal Network.

Dynamic Host Configuration Protocol (DHCP) is used to automatically provide parameters related to IP address (TCP / IP settings) to DHCP clients. The DHCP server will be configured on the Internal Network server and not on the ISA Server 2004 Firewall itself. When we have configured the DHCP server on the Internal Network, ISA Server 2004 Firewall can automatically lease IP Addresses from the DHCP server and redistribute it to VPN Clients (these IP addresses are taken from a special address space on the DHCP server). The server, for example, has created a DHCP scope called 'VPN Clients Network.', this area contains IP addresses and parameters provided only for VPN Clients).

Access controls and routing relationships for these VPN Clients accessing the Internal Network can be configured between VPN Clients Network and Internal Networks defined in the LAT partition (Local Address Table managed by ISA Server 2004 Firewall.

In this section we will perform the installation of Microsoft WINS and DHCP services. We will then configure a DHCP scope with the proper DHCP scope options.

Install WINS Service

The Windows Internet Name Service (WINS) is used to resolve NetBIOS names to IP Addresses (simply because we are using Network TCP / IP, Network communicates with the number - IP address, Computer name is only a sub-element, and is communication habits, because names are easier to remember than numbers. In the new Network models today (eg Network Microsoft Windows 2000/2003) using the main name search solution is DNS service, WINS service deployment is an option, and absolutely not required). However, many Organizations want to use My Network Places to identify servers on the Network. We know that My Network Places works searching for Network Computers based on the Service Windows Browser. And the Windows Browser service resolves names based on broadcast (based service), if Network deploys Windows Browser WINS server on computers that will depend on WINS server to gather information about computers distributed throughout the Segment of Network. In addition, WINS service is also required to deploy when the VPN clients want to get a list of Computers in the Internal Network. The purpose of installing WINS server in this tutorial is to support resolving NetBIOS name and Windows browser service for VPN clients.

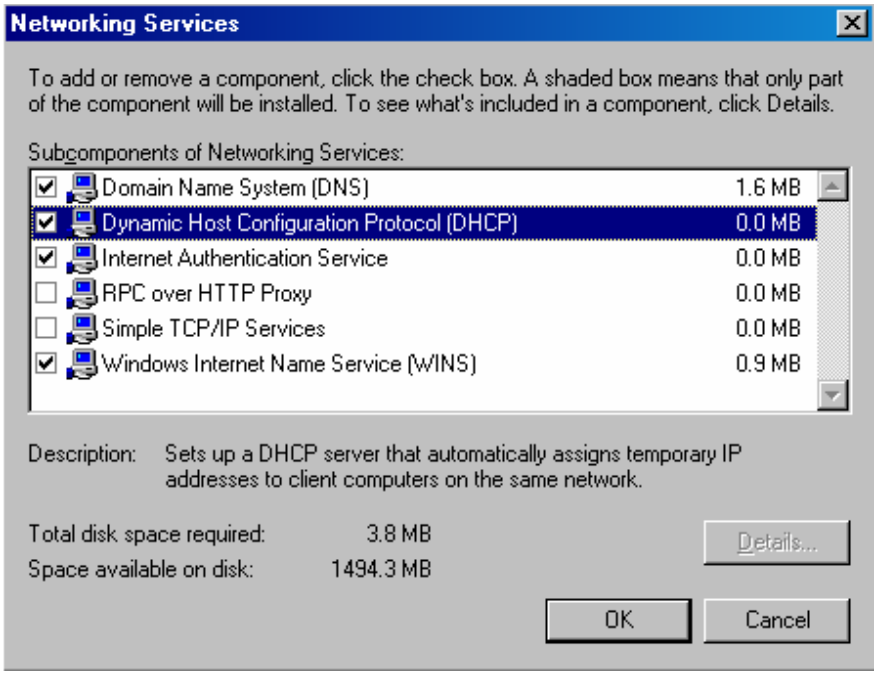
Proceed to the following steps to install WINS:

1. Click Start, Control Panel. Click Add or Remove Programs.

2. In Add or Remove Programs, click Add / Remove Windows Components

3. On the Windows Components page, scroll down to the Components list and select Networking Services entry. Click Details.

4. In the Network Services dialog box, check the Windows Internet Name Service (WINS) check box. Check the Dynamic Host Configuration Protocol (DHCP) check box. Click OK.



5. Click Next on the Windows Components page.

6. Click OK on Insert Disk dialog box. In Files Needed dialog box, insert the I386 folder path in Copy files from text box and click OK.

7. Click Finish on the Completing the Windows Components Wizard page.

8. Close Add or Remove Programs.

WINS server is ready to serve NetBIOS name registration immediately without any additional configuration. ISA Server 2004 Firewall, Domain controller, and Internal Network clients will all be configured as WINS Client and will register with WINS server in their TCP / IP setting (TCP / IP Properties settings)

Configure DHCP Service

Dynamic Host Configuration Protocol (DHCP) is used to automatically split IP related parameters

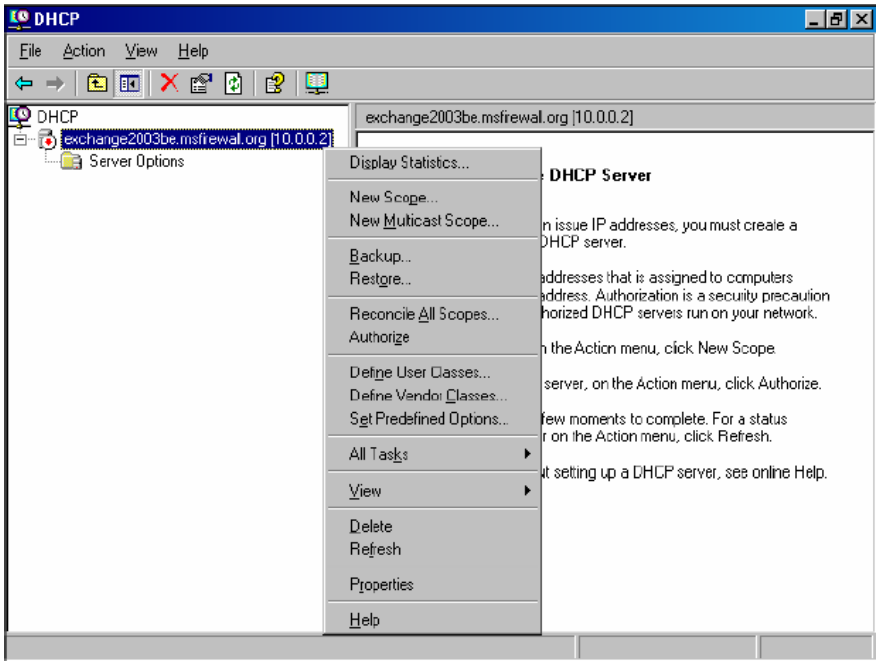
Address for Internal Network clients and VPN clients. In this Lab, the main purpose of a DHCP server is to allocate IP address parameters to the Network VPN clients. Note that, in the actual Network model of the Organizations, configuring the Computers to be DHCP clients, should not require a static IP address. (Of course there are exceptions, for example, using fixed IPs for Servers, or in a Network with a small number of computers, deploying a DHCP server creates a significant increase in costs, increasing Total Cost Ownership-TCO.)

DHCP server service has been installed according to the procedures outlined in Chapter 1. Next step, we will configure a DHCP scope (IP addresses area, with optional options - DHCP options). All of these parameters will be provided to DHCP Clients.

Perform the following steps to configure a DHCP scope:

1. Click Start, Administrative Tools. Click DHCP.

2. On a DHCP console, right click on the server name and click Authorize (this DHCP server validation works properly in the Domain, so all DHCP servers that are not Authorized will be disabled in the IP address provisioning).



3. Click the Refresh button. You will notice that the icon of the DHCP server changes from Red to Green, and DHCP is active

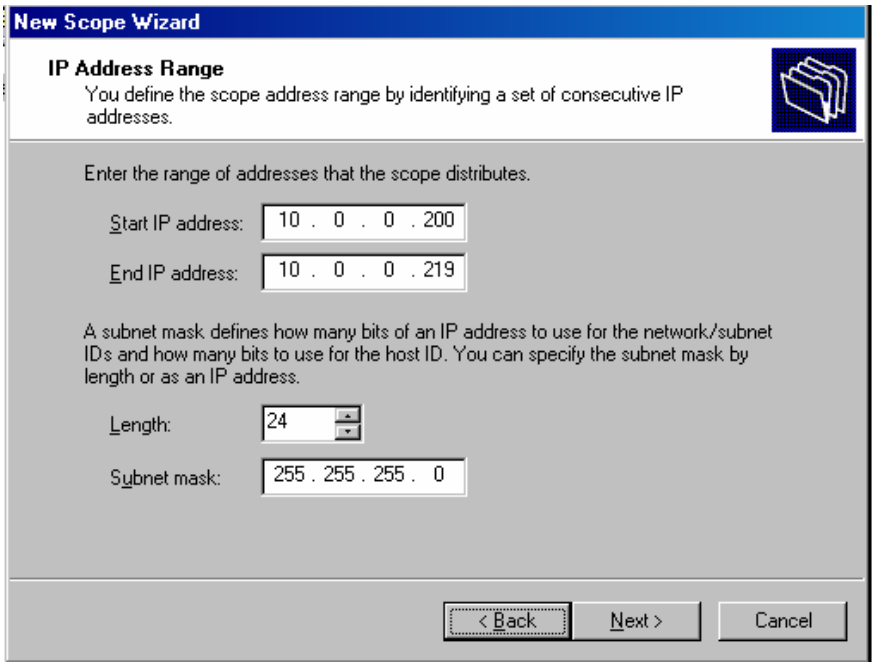
4. Right click on server name, click New Scope.

5. Click Next on Welcome to the New Scope Wizard page.

6. On the Scope Name page, name the scope in the Name text box and give the description in the Description text box. In this example, we'll name the scope scope 1 and not described in Description. Click Next.

7. On the IP Address Range page, put in an IP address starting Start IP address) and an IP Adrress Last (End IP address) in text boxes. And this is the IP address space that you want to be available to DHCP Clients. In this example, we will set up the following: Start address is 10.0.0.200 and End address is 10.0.0.219. This contains 20 IP Address for DHCP Clients. Then we will configure ISA Server 2004 Firewall to allow VPN clients to simultaneously perform 10 VPN connections, and therefore can lose up to 10 of these 20 IP addresses for VPN Clients. ISA Server 2004 Firewall can require more than 10 IP Addresses from the DHCP server, if that is really necessary. Next we will put the subnet mask parameter into Length text box or Subnet mask. In the example here, we confirm the value 24 in Length text box. The Subnet mask value also changes automatically after you

have entered Length. Click Next.



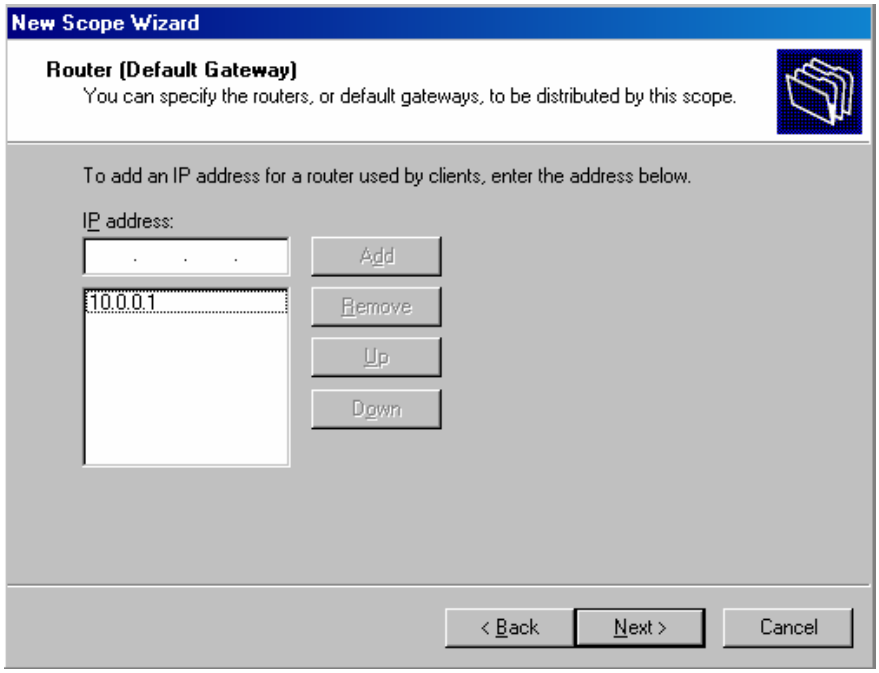
8. Not define any exclusions (intended to reserve for future IP addresses needs, or to avoid allocating IPs that are being used permanently on the Network for devices like Routers, Network Printers .), on the Add Exclusions page. Click Next.

9. Accept the address rental period (lease duration) of 8 days at the Lease Duration page. Click Next.

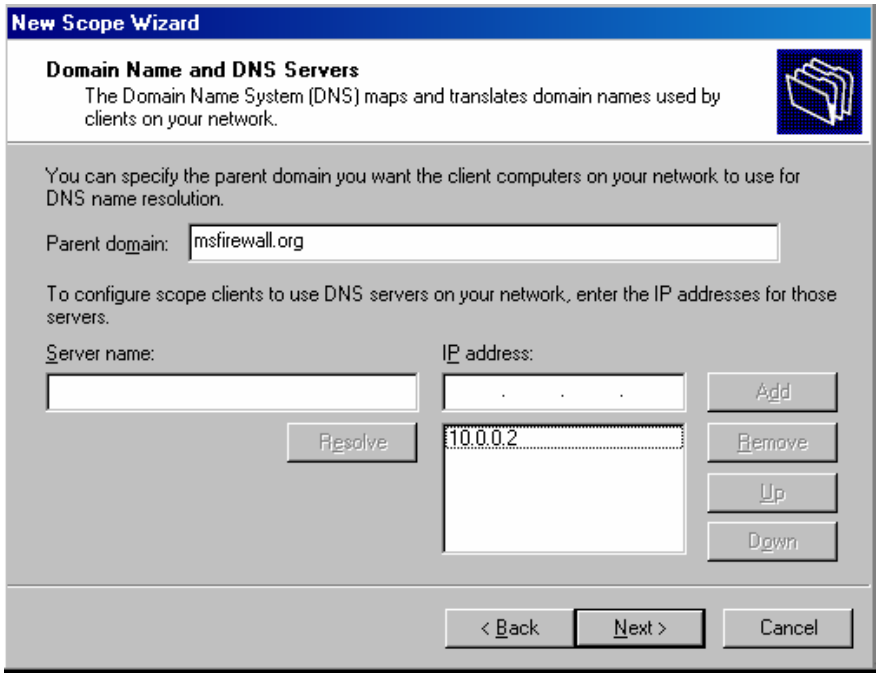
10. On the Configure DHCP Options page, select Yes, I want to configure these

options now option and click Next.

11. On the Router (Default Gateway) page, fill in the IP address of the internal interface (10.0.0.1) on the ISA Server 2004 Firewall computer in the IP address text box and click Add. Click Next.



12. On the Domain Name and DNS Servers page, enter the Domain name of the Internal Network in the Parent domain text box. This is the Domain name used by DHCP clients, based on this, they will identify the Network environment that they are operating, and facilitate the Administrators later, when configuring parameters such as wpad entry, It serves for Web Proxy and Firewall clients to automatically detect, and work with Firewall Service or Web Proxy Service (two Services operating on ISA Server 2004) this function is called Autodiscovery. In this example, you will include the Domain name MSFirewall.org in the text box. In the IP address text box, enter the IP address of DNS server (10.0.0.2) on the Internal Network. Note that domain controllers are also internal DNS servers, as defined in the previous sections. Click Add. Click Next.



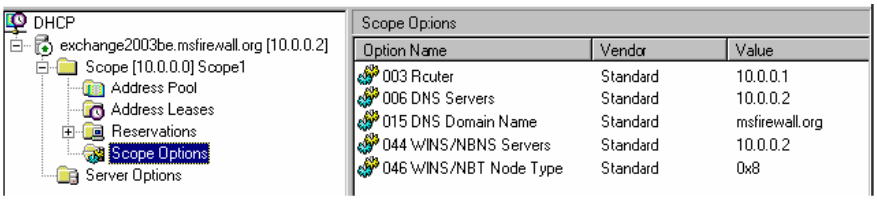
13. On the WINS Servers page, enter the IP address of WINS server (10.0.0.2) and Click Add

14. On the Activate Scope page, select Yes, I want to activate this scope now option

and click Next.

15. Click Finish on the New Scope Wizard page.

16. In the DHCP console, expand Scope 1 node, click Scope Options node. You will be presented with a list of options that you have configured.



17. Close the DHCP console.

At this point the DHCP server is ready to serve the IP address related parameters for DHCP clients on the Internal Network, and also the VPN Clients belonging to VPN clients Network. However, ISA Server 2004 Firewall will not provide these IP parameters for VPN Clients when the Admin has not allowed to deploy Service VPN (VPN server) on Firewall.

Conclude:

In this chapter, we discussed using Microsoft WINS and DHCP servers, installing both of these services on the Domain controller, and configuring a DHCP Scope on the DHCP server. In the following, we will talk about how these services will support VPN clients.

Welcome to **Chapter 5: Configuring DNS and DHCP to support Autodiscovery for Web Proxy and Firewall Client** will be released:

1. Installing and configuring ISA Server Firewall 2004 - Chapter 1 -
2. Installing and configuring the 2004 ISA Server Firewall - Chapter 2 Installing Certificate Services -
3. Installing and configuring ISA Server Firewall 2004 - Chapter 3 -

Thank you - Ho Viet Ha - sent articles about ISA Server Firewall
Network Information Security Vietnam, Inc.
http://nis.com.vn

Email: networksecurity@Nis.com.vn