Create a Site-to-site VPN on ISA 2006 (Part 1)

One of the advanced improvements in the Enterprise Edition version of the ISA Firewall is the Branch Office Connectivity Wizard (used to connect branches with headquarters for companies). The latest version, ISA 2006 has re-integrated components n &

Configure a Site-to-site VPN virtual private network, using the Branch Office Connection Wizard connection program.

Branch Office Domain Controller

One of the advanced improvements in the Enterprise Edition version of the ISA Firewall is the Branch Office Connectivity Wizard (used to connect branches with headquarters for companies). In ISA 2000, the Site to Site VPN Wizard program has been integrated, making it easy to create a site-to-site virtual private network. But ISA 2004 ignores this functionality, making it difficult to create site-to-site VPNs between two ISA Firewall firewalls. Fortunately, the latest version, ISA 2006 has re-integrated this component under the name of the Branch Office Connectivity Wizard.

The Branch Office Connectivity Wizard uses the information contained in the Remote Site configuration at the headquarters, making it easier to create a Site to Site VPN virtual private network. When working with the Wizard, a file will be created so you can use the branch office ISA Firewall to create the site-to-site VPN virtual private network. The wizard also provides the option to create the ISA Firewall Domain Member Branch Office (the ISA Firewall for the domain member branch office), which is the most realistic ISA Firewall. The security issue of the ISA Firewall domain member is much more powerful, able to stand alone as a standalone ISA Firewall.

In this series on using the ISA Firewall Branch Office Connectivity Wizard to create this site-to-site virtual private network, the first part is the process of creating a site to site VPN connection using the Wizard. It will then create the Access Rules (ie the rules used), allowing the domain management server or domain member client to be located at the branch office and use the least privilege to work in this.

Figure below shows a high-level general illustration of the experimental network used in our series.

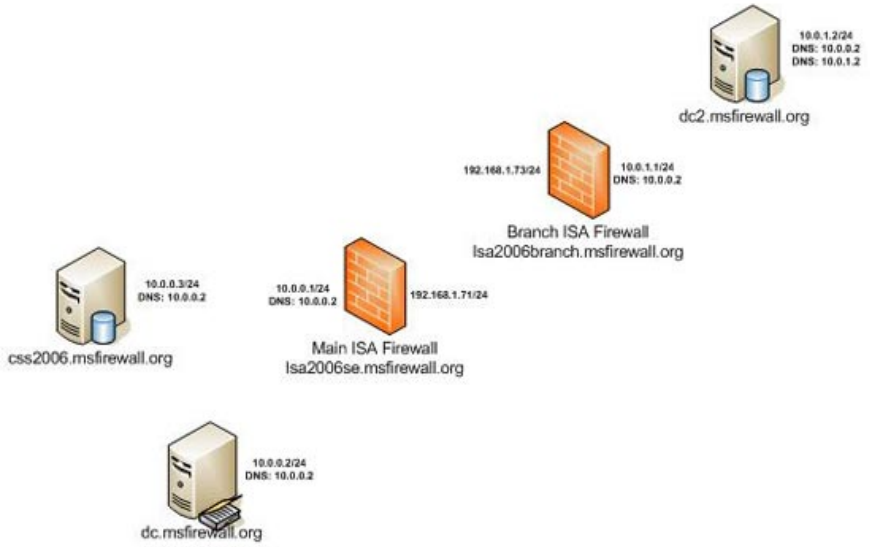
10.0.1.2/24
DNS: 10.0.0.2
DNS: 10.0.1.2
dc2.msfirewall.org
192.168.1.73/24
10.0.1.1/24
DNS: 10.0.0.2
Branch ISA Firewall
lsa2006branch.msfirewall.org
10.0.0.3/24
DNS: 10.0.0.2
10.0.0.1/24
DNS: 10.0.0.2
192.168.1.71/24
Main ISA Firewall
lsa2006se.msfirewall.org
css2006.msfirewall.org
10.0.0.2/24
DNS: 10.0.0.2
dc.msfirewall.org

Figure 1

There are 5 machines used :

• **Dedicated CSS (css2006.msfirewall.org)** : a dedicated CSS will be used to provide CSS shelter for ISA Enterprise Edition firewall arrays. There are two ISA Firewall arrays: one for the ISA Firewall array at the main office and one for the branch office. We cannot place the ISA Firewall firewall for the head office and branch office in the same array, because the internal communications for all members must be on the same network ID. This is not possible when an array member is on the branch office. However, you can apply this enterprise policy to all arrays in the same ISA Firewall Enterprise.

• **Domain Controller (dc.msfirewall.org)** : All machines in this case belong to the same domain, msfirewall.org.

• **Main office ISA Firewall (isa2006se.msfirewall.org)** : This machine is the **main office ISA Firewall** and belongs to an array named Main. This is a domain member, with internal and external interface.

• **Branch office ISA Firewall (isa2006branch.msfirewall.org)** : This machine is the branch **office ISA Firewall** , which is a member of the domain using the Branch Office Connectivity Wizard. This machine uses Windows Server 2003 and was originally a standalone server. ISA 2006 will be installed on the machine when it is a standalone server. After installing ISA 2006 Enterprise Edition, we will run the Branch Office Connectivity Wizard on this machine to create a site-to-site VPN virtual private network and incorporate the domain into the domain. The wizard will also connect the branch office ISA Firewall to the branch office array configured on the CSS at the main office.

• **Branch office Domain Controller** : This is the domain controller (Domain Controller - DC) in the branch office. Users at those branches will use it to authenticate the information. We will create custom Access Rules that allow DC to link to the DC at the headquarters.

We will also make changes to the DNS configuration (Domain Name System) of the branch office ISA Firewall so that we can use branch office DC after the configuration is complete.

Site-to-site By using a dedicated device and a wide-area security mechanism, each company can create connections with many sites over a public network such as the Internet.

Site-to-site VPN can be in one of two forms:

- ***Intranet VPN***
Applicable in case the company has one or more remote locations, each location has a LAN local area network. They can then build a virtual private network to connect local networks to a unified private network.

- ***Extranet VPN***
When a company has an intimate relationship with another company (for example, a partner, a support or a customer), they can build an extranet VPN to connect to a LAN with the network. LAN and allow such companies to work in an environment with shared resources.

The procedures include :

• Configure the headquarters DNS server to remove dynamic updates and add points to static DNS for the array

name and branch office ISA Firewall.

• Install CSS on a dedicated CSS machine.

• Install Firewall services on the main office ISA Firewall.

• Install local CSS and Firewall Services on the branch office ISA Firewall.

• Create an answer file at the main office ISA Firewall, which will be used in the Branch Office Connectivity Wizard.

• Run the Branch Office Connectivity Wizard on the branch office ISA Firewall.

• Create Access Rules that allow communication within the domain between domain controllers at the headquarters and branch offices.

• Install DC at the branch office.

• Create DNS changes at the branch office so that the ISA Firewall uses the branch office DC.

Some points to pay attention to Site to Site VPNs

One of the busiest areas of the ISA server.org website is the array of VPNs. In particular, the most mentioned problem is the site to site VPN connection. The reason is probably because many people do not understand how they work and do not know some of the basic prerequisites when they want to create them.

VPN Gateway is the router for virtual private network.

When the ISA Firewall is configured as a gateway for the site to site VPN, it becomes a router with network IDs located behind the remote VPN gateway. For example, suppose the head office is located on the network ID of 10.1.0.0/16 and the branch office IP addresses are located on network ID 10.2.0.0/16. When a host in the head office needs to connect to the remote network ID 10.2.0.0/16, it must perform through the virtual private network gateway at the head office.

To do this, the network clients at the main office must be configured with a gateway address that knows the direction to network ID 10.2.0.0/16. The ISA Firewall completes this functionality, so clients are configured to use the ISA Firewall as a default gateway. For client systems that do not use the default ISA Firewall, hosts must be configured to use a LAN router with the table entry routing function to send connections to the network ID 10.2.0.0/16 and their LAN IP address. ISA Firewall.

I see a lot of questions regarding how to 'fix' the problem encountered when the local and remote layers have the same network ID. Many people wonder if there is any way to handle this problem. The answer is NO, from a routing perspective. Because client systems that connect to the ID of the local network will never send a connection to the gateway address. So why do clients still send connections to local network IDs and gateways even if they are not required and violate all principles of TCP / IP routing rules?

Solution name

Another common problem in layer-based virtual private networks is the name solution. The clients at the branch office need to handle the computer names at the head office, and usually at the branch as well. If you want to do that, you need to have a proper DNS server infrastructure that can handle all names. In addition, you need to consider whether the branch office user can handle the Internet host name directly, or depending on the ISA Firewall at the head office or at the branch.

There are two main problems related to the name resolution at the branch office level: with or without Domain Controller (DC). If the company uses DC at branch offices, hosts at the branch office can use the local Domain Controller to log in and process the name. The machines can be configured as an Active Directory integrated DNS server. If there is no DC at the branch office, the clients at that office can be configured to use the headquarters's DNS server, handling names for servers in both the main office and the branch office.

Handling Internet host names is a separate issue. Some happy organizations allow clients to handle Internet host names themselves (for SecureNET clients). While some other organizations want to be able to control this issue only allow the ISA Firewall to handle the name on behalf of the clients.

There are many methods to handle Internet host names and it's hard to tell which method is best. The most commonly used way is to configure the ISA Firewall and host on the unified network, using Active Directory integrated with the DNS server. The first is to process the hostname, then configure the Active DNS integrated Directory to use the company-controlled sender.

An important issue in name processing in the branch office environment is WPAD entry points. As you know, both Web proxies and Firewall clients use WPAD entries to automatically detect the local address of the ISA Firewall, for Web proxies and Firewall client connections to the ISA Firewall. This problem can be problematic when you use a single DNS infrastructure for both branch offices and headquarters, because you cannot use a single WPAD entry for all areas whether you want hosts connect to the local ISA Firewall. But if you want to connect hosts to the Internet through a headquarters firewall array, you can use a single WPAD entry.

You can handle the problem by creating multiple WPAD entries, one for the main office and the other for each branch office, using netmask order on DNS servers. When the netmask order is allowed, the DNS servers will process the WPAD query to match the network ID from where the request was sent. That is, when a headquarters host sends a WPAD query to DNS, the return address is the one located near the network ID of the host at the head office. When the WPAD query is received by a host in the branch office, the return address will be the address closest to the branch's network ID.

The last DNS related issue you need to consider is the impact of DDNS subscriptions for the virtual private network (VPN) gateway. When DDNS is used on DNS server, Firewall RAS interface will register itself in DNS and create connection problems for Web proxy and Firewall cleint. They will try to connect to the RAS interface and not the real LAN address of the ISA Firewall. For that reason, in the issues discussed in this series, we will disable the DDNS function on the DNS server when creating the VPN gateway. We will also check to see if it is possible to disable the DDNS registration in the demail-dial interface using the RRAS console.

VPN protocols

ISA Firewall supports three VPN protocols for site-to-site virtual private networks: IPSec tunnel mode, L2TP / IPSec and PPTP.

IPSec tunnel mode was introduced with ISA 2004. With this protocol, the ISA Firewall can be used as a site-to-

site VPN gateway with third-party VPN gateways. This is only possible with IPSec tunnel modes, since this model is considered to be less secure and has less performance than L2TP / IPSec. In addition, routing support for IPSec tunnel mode is very difficult, heavy and limited.

L2TP / IPSec is the preferred site to site VPN protocol because both sides of the site-to-site virtual private network use the ISA Firewall and the third-party VPN gateway supports L2TP / IPSec. L2TP / IPSec supports pre-shared keys, so in a secure production environment, you can use certificate authentication information for both the machine account and the user account to authenticate the virtual private network 'tunnel' (VPN tunnel). This is a very safe configuration type, but most companies prefer to use non-EAP authentication mode for user-dial interface and certificate authentication for machine accounts.

PPTP is the easiest protocol to support site to site VPN connections. Without certification, PPTP 'only works and works'. One drawback is that PPTP is less secure than L2TP / IPSec because the hash of the authentication information is sent over an unencrypted channel. Therefore, the level of PPTP connection security provided depends greatly on the complexity of the password. PPTP does not provide rejection and protection functions during repetition like in L2TP / IPSec.

Using IPSec tunnel mode to connect to a third party virtual private network port is the easiest way. The first thing you should consider is the information on using the ISA Firewall with third party VPN gateways at the Microsoft website.

If this tutorial does not solve the problem, you need to consider IPSec. Make sure the IPSec parameters are correct on both sides. Even if you have the correct parameters, you may still encounter problems with the non-RFC dependent VPN gateway. For example, I have heard that some reports about the Sonicwall firewall do not work with the gateway to the ISA Firewall VPN. The reason is that they are not the RFC's essence and do not allow IKE to use the source port instead of UDP 500. Because the ISA Firewall is an entity of RFC, it can use an alternate port and therefore does not need to bind connect to the Sonicwall device. With the Sonicwall, you can use the software update to turn the device into RFC mode.

Another common problem is that site-to-site VPN user accounts are not correctly configured to match the demand-dial interface name. When this happens (there are times when the virtual private network is connected), there is no traffic going through the VPN gateway from one network to another. Or maybe you will find that connections are allowed, but not from another network. The reason is that the site-to-site VPN connection is not established. You can verify this by opening the RRAS console and checking the **Remote Access Clients** button in the left pane. If you see a remote access client connection for the remote VPN gateway, then the remote access VPN client connection has been made, not the site to site VPN connection. Remote access client connections will not allow routing through the VPN gateway.

For these reasons, I always recommend that ISA Firewall administrators should use L2TP / IPSec with a certificate authentication machine. However, most initial implementations install site-to-site virtual private networks that use a 'pre-shared' key to build a reliable solution to the solution and eliminate some of the complicated inheritance in PKI. After the site to site VPN solution completes the final test time, you should switch customers to a machine with certificate authentication and say goodbye to pre-shared keys.

Summary

This is the first part in a series of configuration site-to-site virtual private networks (VPN site to site) using the Branch Office Connectivity Wizard. With this model, an ISA Firewall will be set up at the office of the head

office and branch office, next to the Domain Controllers. In the following, we will look at how to use the Branch Office Connectivity Wizard in ISA 2006 Enterprise Edition to create a connection and then customize the Access Rules, DNS and some other configuration parameters, fully support the connection. Connect site to site VPN from branch office.

Create a Site-to-site VPN on ISA 2006 (Part 2)