Create VNP Site to Site with the ISA 2006 Firewall Branch Office Connection Wizard - Part 1

In this series, I will show you how to configure a site to site virtual private network (VPN) using the Branch Office Connectivity Wizard in the ISA 2006 Firewall.

In this series, I will show you how to configure a site to site virtual private network (VPN) using the Branch Office Connectivity Wizard in the ISA 2006 Firewall.

Virtual Private Network (VPN) - Virtual private network is a technology that allows to expand the scope of LANs (Local Area Networks) without any separate lines. VPN is used to connect geographically dispersed branches into a single network and allow remote use of application programs based on company services.

Domain Controller script for branch office

One of the improvements included in the Enterprise version of the 2006 Firewall ISA is the Branch office connectivity wizard. In ISA 2000, we already have a **site to site VPN wizard** that can easily create a site to site VPN. Although in ISA 2004, this popular **site to site VPN wizard** has disappeared, but people will not encounter any problems in making a site to site VPN work between the two ISA Firewalls. The ISA Firewall development team has made improvements so that we have an interesting site to site VPN wizard, the Branch Office Connectivity Wizard is the name reset.

The Branch Office Connectivity Wizard uses the information contained in the Remote Site configuration you create at the main office and uses that information to help make creating a site to site VPN easier. When you finish the wizard, a file will be created so you can take it to the branch office ISA Firewall to create a site to site VPN. In addition to creating a site to site VPN connection, the wizard also lets you get the option to create the ISA Firewall at a domain member's branch office, which is really the best way of ISA Firewall for comprehensive security. of a domain member is much more powerful than a standalone ISA Firewall.

In this series on using the ISA Firewall Branch Office Connectivity Wizard to create a site to site VPN, first we'll cover the process of creating a site to site VPN connection using the Wizard, after creating a site to VPN site. site, we will create Access Rules for the *domain controller* (*domain controller*) of the branch office, domain member clients at the branch office and use the minimum privileges to perform this.

The figure below shows an overview of the lab network used in this series.

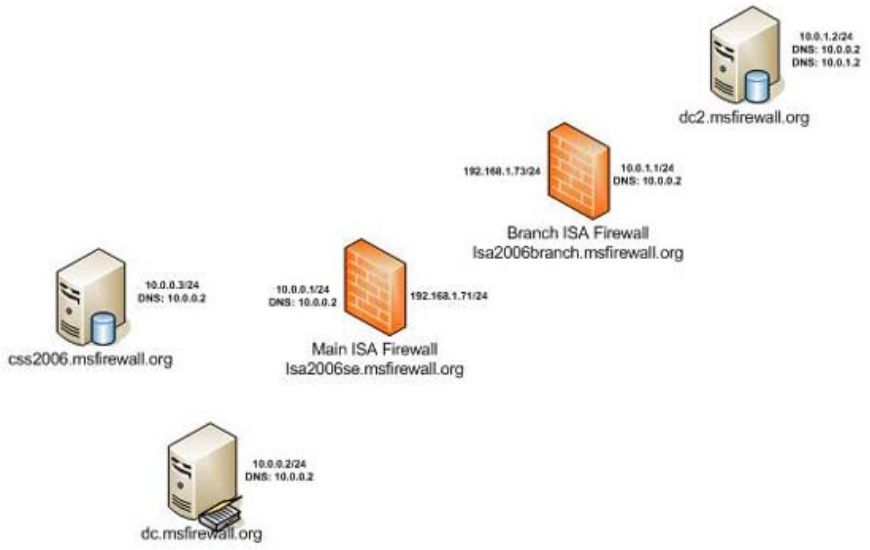

Figure 1

There are 5 computers used in this scenario:

- **Dedicated CSS (css2006.msfirewall.org)** A dedicated CSS will be used to manage CSS for ISA Enterprise Edition firewall arrays. There will be two ISA Firewall arrays: one for the main office ISA Firewall and one for the branch office. We cannot place the branch office and main office ISA Firewalls in the same array because the internal array communication addresses for all array members must be on the same network ID, and that is not when array members are located at branch offices. However, we can use enterprise policy for all arrays in the same ISA Firewall Enterprise.
- **Domain Controller (dc.msfirewall.org)** All computers in this scenario belong to the same domain, msfirewall.org.
- **Main office ISA Firewall (isa2006se.msfirewall.org)** This computer is the main office ISA Firewall and will belong to the network array called **Main** . This machine is a domain member, and has an internal and external interface.
- **Branch office ISA Firewall (isa2006branch.msfirewall.org)** This computer is the branch office ISA Firewall and will be set as a domain member using the branch office connectivity wizard. Windows Server 2003 is installed on this computer and it was originally a standalone server. ISA 2006 will also be installed on this computer when it is a standalone server. After ISA 2006 Enterprise Edition is installed on the machine, we will run the Branch Office Connectivity Wizard on this machine, create the site to site VPN and join the domain. The wizard will also connect the branch office ISA Firewall to the branch office array configured in the main office CSS.
- **Branch office Domain Controller** This is a **branch office domain** controller that users will use for authentication. We will create custom Access Rules to allow DC to communicate with the DC at the main office.

We will also make changes to the DNS configuration of the branch office ISA Firewall so that it can use the branch office DC after the configuration is complete.

The procedures include:

- Configure the main office DNS server to reject dynamic updates, *add* static DNS entries for arrays and branch office ISA Firewall.
- Installing CSS on Dedicated CSS Machine
- Installing services of the Firewall on the main office ISA Firewall (Main office ISA Firewall)
- Installing internal CSS and Firewall Services on the branch office ISA Firewall (Branch office ISA Firewall)
- Create an answer file at the main office ISA Firewall to allow the branch office connectivity wizard to use
- Run the Branch Office Connectivity Wizard on the branch office ISA Firewall
- Create Access Rules to allow domain communication between DC offices of the branch office.
- Install DC at the branch office
- Create DNS changes at the branch office so that the ISA Firewall uses the branch office DC

Notes on Site to Site VPN

One of the busiest parts on ISAserver.org must include VPN sections and it is often site to site VPN issues. The reason for this is that many people don't understand how site to site VPN connections work and some basic requirements for those connections to work.

VPN Gateway is a VPN Router

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

To work, clients in the main office network must be configured with a gateway address to know the route to the network ID 10.2.0.0/16. The ISA Firewall knows the route well, so clients configured to use the ISA Firewall as their default gateway will be able to access the remote network through the ISA Firewall's VPN gateway.

We see a lot of questions mentioning how to 'fix' problems encountered when local and remote sites are addressed with the same network ID. They want to know if there is any way to 'fix' this problem. The answer is that there really is no way to 'fix' this problem from a routing point of view, because client systems connected to intranet IDs will never forward connections to a location. only port. Why would clients forward connections to intranet IDs to a gateway when not required and violate all tenets of TCP / IP routing rules?

Remember name identification

Another common problem with site to site VPNs is name identification. Clients at the branch office need to be able to identify computer names at the main office, and at the branch office. To do this, an appropriate DNS server infrastructure must be identified that can identify all names. In addition, you also need to think whether users at the branch office should assign Internet hostnames directly or depend on the ISA Firewall at branch offices or main offices to identify their on-behalf hostnames. .

There are two main scenarios related to name identification at the branch office: one is to have a domain controller at the branch office and the other is to have no domain controller at the branch office. If the company keeps the DCs at the branch office, the hosts at the branch office can use their local domain controller to log in to

name identification, because the computer can be configured as a server. Integrated DNS Active Directory. If there is no domain controller at the branch office, the clients at the branch offices can be configured to use the DNS server at the main office for the purpose of identifying domain names for servers at the office. branch office and main office.

Internet hostname identification is another problem. Some organizations prefer for clients to be able to identify Internet hostnames (the process required for SecureNET clients), while others want strict control over Internet hostname identification. and only allow the ISA Firewall to identify names as clients.

There are many ways to accomplish this delineation process, but I cannot provide you with a formula to identify the best way. However, what I usually do is configure the ISA Firewall and hosts on the corporate network to use Active Directory integrated DNS servers to identify hostnames, and then configure these DNS servers to use one. The relay is controlled by the company to identify Internet hostnames.

An important issue in name identification in branch office environments involves WPAD entries. As you know, both Web proxies and Firewall clients use WPAD entries to automatically detect the internal address of the ISA Firewall to use for Web proxy and Firewall client connections with the ISA Firewall. This can be a bit confusing when you use a separate DNS infrastructure for branch and main office offices, because you cannot use a WPAD entry for all locations, assuming you want the The host can connect to the internal ISA Firewall. In other words, if you want all hosts to connect to the Internet through a main office firewall array, you can use a WPAD entry.

You can solve the problem by creating multiple WPAD entries, one for the main office and one for each branch office, then activating *netmask ordering* on the DNS servers. When *netmask ordering* is enabled, the DNS servers identify WPAD queries to match the received network ID. That means that when a host at a main office sends a WPAD query to DNS, the returned address will be the closest address to the network ID of the host at the main office and when the WPAD query is received by a host at the branch office, the address returned will be the address closest to the network ID where the branch office is located.

For more information on how to do this, you can refer to the article by Stefaan Pouseele here.

The last DNS issue you need to consider is the impact of DDNS subscriptions for VPN gateways. When DDNS is enabled on the DNS server, the RAS interface (RAS interface) of the ISA Firewall will register itself in DNS and generate connection problems for the Web proxy and Firewall clients, as they will attempt to connect to the server. RAS interface and not the actual LAN address of the ISA Firewall. For this reason, in the scenario discussed in this article series, we will disable DDNS on DNS servers when creating a VPN gateway and then investigate it to disable registry issues. DDNS in the demand-dial interface using the RRAS interface.

VPN protocols

ISA Firewall supports three VPN protocols for VPN site sites: IPSec tunnel mode, L2TP / IPSec and PPTP.

IPSec tunnel mode support is introduced in ISA 2004 so that ISA Firewall can be used as a site to site VPN gateway with third-party VPN gateways. This is just a scenario you should use IPSec tunnel mode, because IPSec tunnel mode is still considered to be a less secure protocol and less efficient than L2TP / IPSec. In addition, IPSec tunnel mode routing support is very difficult and limited.

L2TP / IPSec is a popular VPN site to site protocol when both sides of the site to site VPN are using the third-party ISA Firewall or VPN gateway that supports L2TP / IPSec. Because L2TP / IPSec supports pre-shared

keys, in a secure environment, you must use certificate authentication for both the computer account and the user account that was used to verify the tunnel. VPN. While this is a very secure configuration, most of the companies I come across often use non-EAP authentication for user accounts with demand-dial interfaces and use certificate authentication for machine accounts. count.

PPTP is the easiest protocol to support site to site VPN connections. No certificate is required and most ISA Firewall administrators will find that PPTP is 'working only'. The disadvantage of PPTP is that it is less secure than L2TP / IPSec because the credentials hash is sent on an insecure channel. Therefore, the security level of the PPTP connection can provide depending primarily on the complexity of the password. In addition, PPTP does not provide non-repudiation features and *replay* protection that L2TP / IPSec provides.

When using *IPSec tunnel mode* to connect to third party VPN gateways, there's no easy way to do it. The first thing you should try is information about using the ISA Firewall with third-party VPN gateways at Microsoft's website.

If the tutorial doesn't match the deployment scenario, you'll have to go back to your understanding of IPSec and ensure that all IPSec parameters are correct on both sides. Even if you see the IPSec parameters correctly on both sides, you may still encounter problems with VPN gateways that do not have RFC compliance (non-RFC compliant). For example, there are some reports about the Sonicwall firewalls that do not work with the ISA Firewall VPN gateway because they do not have RFC compliant RFC and do not allow certain source ports for IKE outside of UDP 500. Due to ISA The firewall has RFC compliance, so it can use a different port and therefore does not connect to the Sonicwall device. In the case of the Sonicwall, a software upgrade may create RFC compliance for the device.

Another common problem with site to site VPN is that user accounts are not configured to meet demand-dial interface name (*Note:* Interface name on this side is the username on the other side!). When this happens, there may be times when the site to site VPN is connected, but there is no traffic from one network to another through VPN gateways, or it may be like the connections are given. permission from a network, but not from another network. The reason for this is because the site to site VPN connection is not set up. You can confirm that by opening the RRAS interface and checking the **Remote Access Clients** entry in the left pane. If you see a remote access client connection for the remote VPN gateway, you will know that the remote access client's VPN connection has been created without connecting to the site to site VPN. Remote access client connections will not allow routing through VPN gateways.

With experience, we always encourage ISA Firewall administrators to use L2TP / IPSec with machine certificate authentication. In most cases, though, during the initial deployment process, we will set up site to site VPN with a pre-shared key, to build confidence in the solution and remove some of the complexities. in a PKI. After the site to site VPN solution is implemented, we will move on to authenticate the machine certificate and remove the pre-shared keys.

Conclude

This is the first part of a series on how to configure a site to site VPN using the branch office connectivity wizard. In this scenario, there will be ISA Firewalls as well as domain controllers located in the main offices and branches. In the following sections, I will show you how to use branch office connectivity wizard included in ISA 2006 Enterprise Edition for you to create connections and then customize access rules. NDS and other configuration parameters to fully support the site to site VPN connection from the branch office.

following us regularly.