

# HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

How to configure ISA Server to work with three types of ISA Clients: SecureNAT Client, Web Proxy Client and Firewall Client. The instructions on how to configure ISA server and differentiate different types of ISA Clients, which can be used according to different circumstances, can help the Admin take advantage of ISA and deploy properly with love. bridge on your organization's Network system

Picture 1 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

How to configure ISA Server to work with three types of ISA Clients: SecureNAT Client, Web Proxy Client and Firewall Client. The instructions on how to configure ISA server and differentiate different types of ISA Clients, which can be used according to different circumstances, can help the Admin take advantage of ISA and deploy properly with love. bridge on your organization's Network system.

## **Some definitions:**

### · *Auto-detection* :

A feature on ISA server (WPAD), which allows Internet Explorer browser (version 5.0 and above), automatically updates the most appropriate configuration for you to work with ISA server

### · *DNS (Domain Name Services)*

The service that runs on a Computer is responsible for responding to requests for name (hostname) to the actual IP address of Internet Servers. example of a name query, ISA Clients need to access to www.nis.com.vn or mail.nis.com.vn (this is a hostname, and hostname is the only name type used to describe Computer providing services on the Internet)

### · *FQDN (Fully Qualified Domain Name)* :

Computer name, indicates the logical structure of the Computer name associated with that Computer Domain. For example: www.security.net is considered the following logical structure: 'Security.net' is the Domain name, 'www' is the name of the Computer that provides the Web service of that Domain. In addition, the .com, .net, .edu, .gov, .org, v.vv etc. are all provided by organizations that regulate Internet Domain Name (ICANN, .).

### · *LAT Host* :

Computers that work inside *the Intranet* are usually in the LAT (Local Address Table) list, which helps ISA server specifically separate from the External Host. ISA server uses NAT to handle these LAT hosts (replacing the IP Addresses of LAT hosts with External IP addresses on ISA server), before the information is sent out.

· **NetBIOS Name :**

Also called Computer Name, which is commonly used in Set-up Networks (the model WORKGROUP computers often use Netbios name to communicate with each other, do not use Hostname - *note : Hostname is only used in 2 cases: Cho servers providing services on the Internet, and in internal Domain systems, such as Microsoft Active directory domain*)

· **Record :**

In the DNS system, and in the DNS zone, records are a specific record that specifies a Host, a Mail server, a Web server or Domain Controller, etc. that are associated with IP address (or vice versa, write IP address before and Hostname later) of these servers, and are the main factor for name querying from clients.

· **Primary and Secondary Protocol :**

There are servers that provide only one Network Service when communicating, maybe the Service must be operated on multiple Ports (or in other words serve on multiple connections at the same time even if only providing 1 service. Example **Active FTP server** service , run simultaneously on 2 TCP ports: 21- set up connection, and 20- data transfer (other than **Passive FTP** only opens TCP Port 21 )

Picture 2 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

In the above example, the Primary connection on the Active FTP server is done via TCP Port 21, while Secondary connection is via TCP port 20. Thus TCP 21 is Primary Protocol, and TCP 20 is Secondary Protocol of the *Active FTP Server Application* .

· **TTL (Time to Live )**

There are units, calculated in seconds, that determine the time for a name record to exist in the DNS zone, before this name record must be refreshed, to update the new parameter exactly for you.

· **WINS (Windows Internet Name Services )**

Also Service specializes in resolving name search queries such as DNS, except that NAME is resolved on WINS as NETBIOS NAME (non-stratified name form like Hostname, has a maximum length of 16 characters - the 16th character used for determine the service that this computer uses NETBIOS name for other computers on the Network, for example 1 record registered in WINS server is **SERVER 20** >: Computer name is **Server** and the last Hexa character, identify the other Computer on the Network to know 2 information: Computer name is **Server** and the service that this machine provides is **File and Print Sharing**.

· **WPAD (Windows Proxy Auto Detection)**

A feature on ISA server uses support for Internet Explorer 5.0 (or higher).When properly configured, it allows IE to automatically update its configuration parameters.

**Operating modes of ISA server:**

· **Cache :**

The service is installed and operating is Caching Service.If ISA server only installs in this mode, the only ISA client object it serves is the Web Proxy client.And this mode also does not support H.323 Gatekeeper service.ISA server operates in this mode only need to provide Web cache, so only 1 NIC Card is needed.

· **Firewall :**

ISA server in this mode is a combination of Firewall Service and Web Proxy service, and has absolutely nothing to do with Web Cache service.All the main features of ISA Server are here and all types of ISA Clients are supported.ISA Server in this mode requires at least 2 NIC Cards - 1 External Card and 1 Internal Card for LAT.

· **Integrated :**

Package integration includes all the above services combined (Web Proxy, Firewall and Web Caching service).In fact, the difference keeps this mode and that Firewall is Intergrated with Web Caching service.

**Types of ISA Clients :** (Will be analyzed in detail in **Part 4** )

· **SecureNAT :**

It is a LAT host (the client has an IP address configured in the Local Network).In a simple Network, SecureNAT Client has a unique route (default gateway) to the Internet via ISA server, and receives the Default Gateway which is the IP address of ISA server Internal NIC.In a more complex network it may be slightly different, SecureNAT Clients will receive the Default Gateway which is the Interface of the Router behind the ISA server, and the task of these Routers is to point to Internal Interface on ISA.

· **Firewall:**

As well as being a LAT host, installing the software **ISA Firewall client** , **enabled** and the client applications will use it later.

· **Web Proxy :**

Configured simply through an Application (IE or other Web browsers such as Netscape ., or web-enabled applications) such as Yahoo Messenger, etc., on LAT host use sent proxy requests to the Outbound web listener on ISA server to the Internet.

**Configure ISA Server:**

It is important that ISA server is properly configured to serve different types of ISA Client.If ISA Server has difficulty resolving the Client to find a Hostname, or accessing Internet services, all Clients can be

affected.Repeat the tests for ISA Server during the installation and configuration process, to make sure ISA Server is properly configured.Thus, changes in the configuration parameters will be strictly verified, and if there are mistakes, it will be easy to return to the original state.

· ***Outgoing Web Requests Listener:***

Function as a Web proxy.The Web proxy service (w3proxy) request must be active, Outbound Web Requests Listener must be configured and enabled.See and change this parameter, open ISA **Management MMC** , open **Servers and Arrays**,. Right-click and **select Properties** . Click **Outgoing Web Requests** tab.

Picture 3 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

By default ISA Server enables Proxy service on all **internal IP IPs** (in the previous examples, 192.168.1.200 and 127.0.0.1 (this is for ISA Server if it wants to become a Web Proxy Client of the Web Proxy Service itself). works on it ), at **port 8080**, **this** default setup of Proxy service is not related to the operation of other ISA Server modes such as Firewall, Integrated, Cache. To **disable the** Outgoing Web Requests listener, simply select **Configure listeners individually per IP address** and do not select any IP addresses for this.

· ***Auto Discovery listener*** : This is one of the "problems" for people who love ISA server, when they want to run IIS (web server) on ISA Server itself, even if IIS only uses Internal IPs.See the picture you will see

Picture 4 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

In this situation, we have 2 *applications / services* ( **WPAD functions** and **IIS Web service** ) for Clients on the same TCP Port, a competition occurs and any of these 2 Services may be 'disadvantaged'.Essentially TCP Port 80 is opened on ISA Server to provide ISA Client with Automatic Discovery (WPAD functionality, which means automatically detecting parameters to connect to Web Proxy Service or ISA firewall Service), but descriptions above will cause Admin to wonder a bit when using this feature.

If you do not want Auto Discovery, do not check **Publish automatic discovery information** .Thus Port 80 will be freed for Internal IPs on ISA Server

*Note:*ISA Server in Web proxy server mode only uses 1 NIC (Cache Mode)

· ***Site and Content Rules*** :

The rules set out here control the content related to HTTP and FTP when they move to Web Proxy Service (for example, when ISA Clients access 1 HTTP site, Site and Content rules are set.) Rules will look at whether the ISA clients' requests are valid, if valid for the content as well as the destination, the request will be forwarded to the Web Proxy service and to the Internet....) By default **Site and Content Rules Prohibit** any content (Audio, image, video, applications, compressed file .), and any Site when requesting to send to the Internet. By default, **Allow rules** are set.If you want to prevent Website / FTPsite Admin from executing Deny here, please set it correctly, otherwise it will be "closed down" all.

Picture 5 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

### · **Protocol Rules :**

One of the hubs of ISA Server. *Enabling LAT hosts (Internal Clients) access Internet resources through rules here* .The figure below defines a lot of Protocols that allow LAT hosts to use. For example, if I do not create a rule marked with red, my LAT hosts will not be able to access HTTP Sites.

Picture 6 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

### · **IP Routing :**

The next issue is to ensure that all traffic flows SecureNAT Clients are not blocked (of course, the rules in Protocol rules above must allow this). The default ISA Server is *disabled 'Enable IP Routing'* . When **Enable** New ISA Server allows **ICMP (pings) from LAT** to Internet.

Open **ISA Management MMC** , find **IP Packet Filtering** . Right-click, select **Properties** and you'll see the picture

Picture 7 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

See more information Enable IP Routing at: <http://support.microsoft.com/kb/q279347/>

### · **HTTP Redirector :**

This is where the Admin can control ISA Firewall Clients and SecureNAT Clients when these Clients require Web access. Open **ISA Management MMC**, select **Servers and Arrays** , **Extensions** , **Application Filters** . Right-click the **Redirector Filter HTTP** , select **Properties** . Select **Options** Admin tab will see as shown in Figure

Picture 8 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

So here, the Admin can determine how the SecureNAT & Firewall client's Web access requests will be controlled (Note: Normally SecureNAT clients and ISA Firewall Clients will work directly with the ISA Firewall Service for all requests to access all Internet services, but except for HTTP / FTP-Web requests, HTTP Redirector will transfer to Web Proxy service.

In the image above you also see the setting '*If the local service is unavailable* .' , this setting means that when Web Proxy Service on ISA Server does not work, transfer Web requests directly to the Web Server '*redirect requests to Requested Web Server*' This is convenient for SecureNAT and Firewall clients who still have access to the Internet without considering Web Proxy filtering which is **NO ANSWER REQUESTS** .

If Admin checks the **Send to requested Web Server** , SecureNAT and Firewall Clients bypass the Web proxy service for all Web requests, at all times.

However, check here will ignore all Proxy parameters set on IE / Netscape browser of Firewall and SecureNAT clients.

If check **Reject HTTP requests from Firewall and SecureNAT clients**, the Firewall and SecureNAT clients must set up Web proxy settings at the browser if they do not want to be banned from all Web requests.

### · **Local Domain Table :**

Table identifies Internal Domains. This is key information for both IE and Firewall client. Any domain name given and this table 1 of 2 possibilities can occur as follows:

1. If Web Proxy and Firewall clients use a DNS server to find the name, they will pass this DNS server to resolve without the related ISA service.
2. Web Proxy clients will make requests directly to any Server in that Domain, bypassing ISA proxy services.

*Note: Also prompt the Admin, to avoid the case that DNS cannot distinguish what is accessing the Internet domain and where to access the internal domain, when creating an Internal Domain to avoid using formats like Internet Domain For example, congty.com may be different instead: **int.Domain.tld** (here I set the domain name very specifically for my organization : **Int.Domain** with **.tld** instead of the current .com / net / edu / org on the Internet)*

Picture 9 of HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III

### · **Name Resolution :**

Determine the correct IP parameters for ISA server absolutely important. At least, Admin must provide a DNS server for ISA Server so that ISA can resolve Internet Servers for Web Proxy and Firewall clients, and should also provide it to ISA. An internal DNS server serves the Internal Network, if the Network is a Domain. ISA Server 2000 installs on Windows server 2000, and W2K Server is recommended by default to use DNS as the only name query solution, rather than using solutions that may cause headaches for later Administrators such as WINS ( NETBIOS name resolution), and how to resolve the 'classic' name NETBIOS Broadcast. ISA Server provides a solution to find DNS names for itself by creating a *DNS Lookup Packet Filter*. The Admin should not Disabled this function, because otherwise ISA Server may not correctly resolve Internet DNS names

### **Proxy Web Proxy and Firewall DNS cache :**

Web Proxy and Firewall services on ISA server provide a very basic DNS name resolution solution based on the TCP / IP settings that Admin has configured on the Network Card of ISA server. This basic function will address requests to search for Internet hostnames for Web and Firewall clients. The mechanism to keep resolved DNS names (DNS Name Cache) of ISA server is quite interesting, the existence time of cached DNS records (Time to Live of DNS Records) does not depend on the rules from the **remote The DNS server** that ISA server sends requests to resolves, that *TTL has been specified by ISA server for Web Proxy and Firewall DNS caches* has a total duration of *6 hours*. This is different from the working mechanism of **DNS caching servers**, these DNS servers when transferring the request to resolve names to other DNS servers, the TTL of the records is cached on it, depending on the TTL from the DNS servers. plays the role of a query solver and is merely storing (caching) what has been found by another DNS server. Administrators want to refer to the parameters of the DNS name cache mechanism of Web Proxy service and Firewall Service on ISA server. Use the REGEDIT command at the RUN menu and search for entries as follows

**Web Proxy:**

HKLM\SOFTWARE\Microsoft\FpcArrays {Array GUID} ArrayPolicyWebProxy  
" *msFPCDnsCacheSize* " = dword: 00000bb8  
" *msFPCDnsCacheTtl* " = dword: 00005460

**Firewall :**

HKLM\SOFTWARE\Microsoft\FpcArrays {Array GUID} ArrayPolicyProxy-WSP  
" *msFPCDnsCacheSize* " = dword: 00000bb8  
" *msFPCDnsCacheTtl* " = dword: 00005460

**WWW.NEWHORIZONS.COM (New Horizons Computer Learning Centers)**

**Ho Viet Ha**

**Training Manager**

**My Website ( NIS.COM.VN - Network Network *I have an security*, My Website Coming soon)**

You finished reading the article "**HOW TO INSTALL ISA SERVER ENTERPRISE 2000 - Part III**" 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.