# INSTRUCTION FOR ISA SERVER ENTERPRISE 2000 - IV

The most frequently asked questions about ISA Clients are: What is the ISA Client, what are the types, and which are used? All of these questions are necessary when you work with a complex system like ISA server. The article provides an overview and how to deploy ISA Clients, exactly how

**ANALYSIS OF THE CLIENT ISA TYPE**

The most frequently asked questions about ISA Clients are: What is the ISA Client, what are the types, and which are used?All of these questions are necessary when you work with a complex system like ISA server.The article provides an overview and how to deploy ISA Clients, exactly how to work between ISA server and ISA clients to achieve the best performance.

There are 3 types of ISA clients: SecureNAT, Firewall and Web.The exact term when describing these Clients is 'Client request' rather than 'Client'.Why, because simply this description shows us how to work between Clients and ISA servers: These are requests from the ISA client to how ISA Server is responding.

A 'background' concept that you should keep in mind when deploying these Client types is LAT host (Loal Address Table host- Computers with IP addresses located in the internal address space, in order to distinguish them from External Computers).A LAT host can be configured to be SecureNAT, Firewall and Web client at the same time.
I would like to repeat some of the definitions presented in Part III
· ***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*** ) Service running on a Computer is responsible for responding to requests for name (hostname) to the IP address of Internet Servers.example of a name query, ISA Clients need to access towww.nis.com.vnormail.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*** ): This is the Computer name, indicating the logical structure of the Computer name associated with the 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, .).

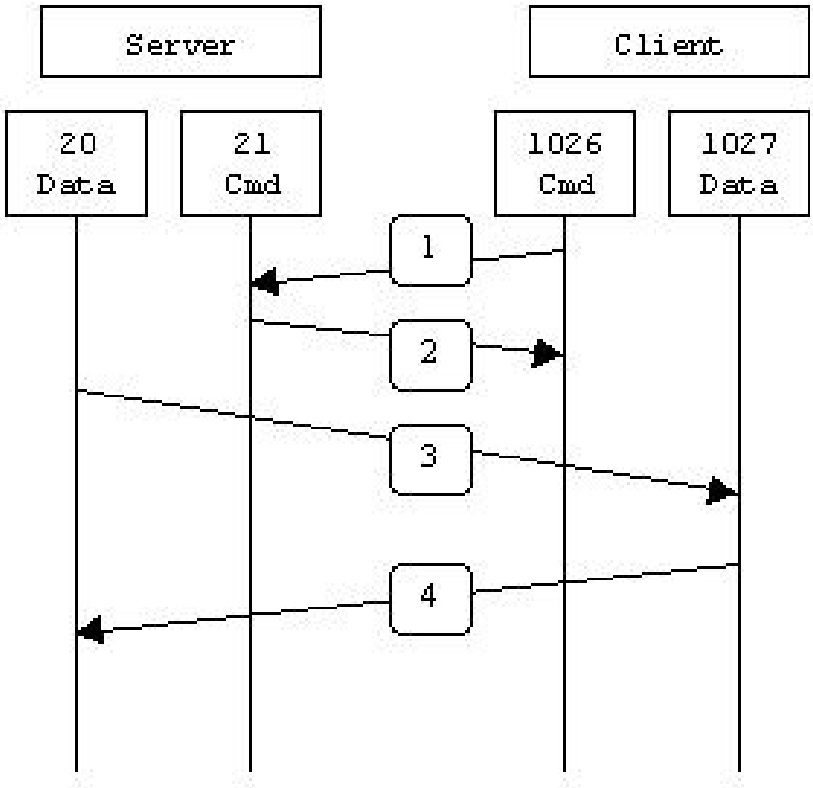
· ***LAT Host*** : The computers operating inside *the Intranet* are normally in the LAT (Local Address Table) list, helping the ISA server to distinguish it from the External Host.ISA server uses NAT to handle these LAT hosts (replacing the IP Addresses of LAT hosts with External IP addresses on ISA server), before the information is sent out.

· ***NetBIOS Name*** : Also called Computer Name, which is commonly used in Set Networks (the WORKGROUP model of computers often uses Netbios name to communicate with each other, not using Hostname - *note* :

*Hostname is* only used in 2 case: For 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 specifying a Host, a Mail server, a Web server or Domain Controller, etc., associated with IP address (or vice versa). write the previous IP adrress and Hostname later) of these Servers, and be 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 **)**




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 for you.

· ***WINS (Windows Internet Name Services*** ) Also Sevice specializes in resolving name search queries such as DNS, except that NAME is resolved on WINS as NETBIOS NAME (non-stratified name form such as Hostname, maximum length of 16 kg - The 16th character used to identify the service that Computer uses NETBIOS name is provided to other computers on the Network, for example 1 record registered in WINS server is **SERVER 20** >: Computer name is ***Server*** and character Hexa at the end of ***20*** , determine for the other

Computer on the Network to know 2 information: Computer name is ***Server*** and the service that this machine provides is ***Fire 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:**

1. ***SecureNAT*** : It is a LAT host (The client has an IP address configured inside 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.

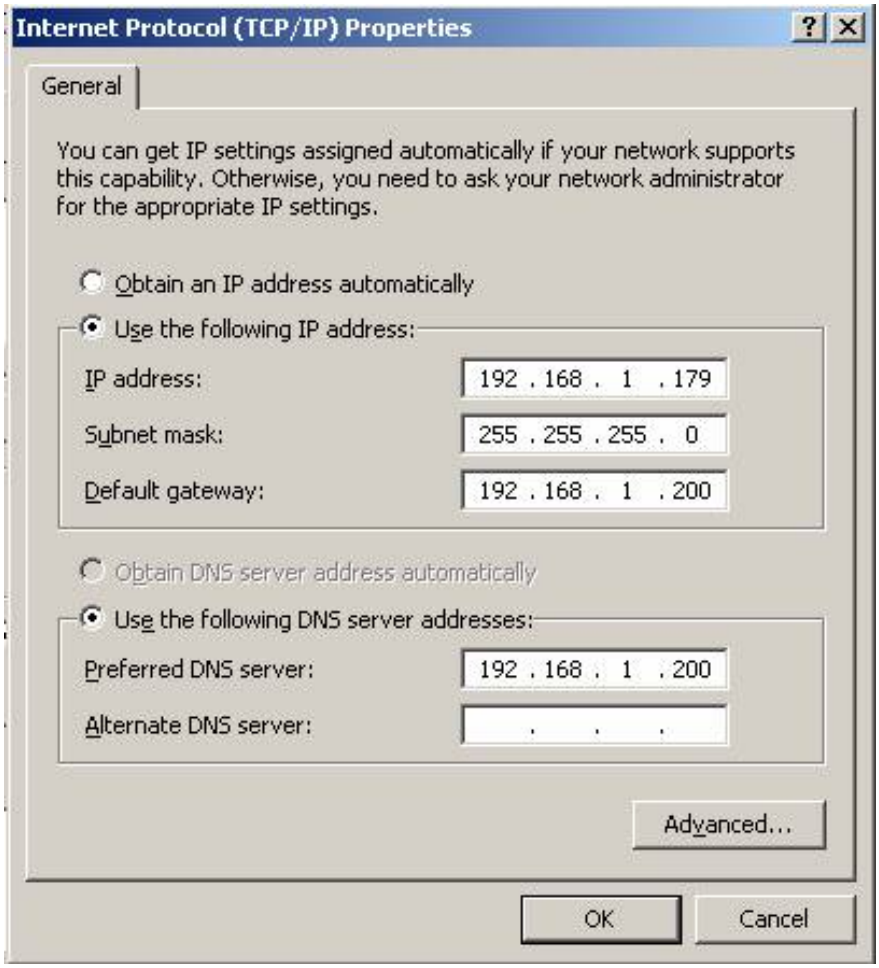



Figure 1: TCP / IP parameters when configuring a SecureNAT client

*Questions related to SecureNAT Client:*
- Is the SecureNAT client only need to set the IP address in Internal Networks (LAT host) and the Default Gateway parameter is ISA Internal IP?
Yes, in a Simple Network it is just like that, but if in a more complex Network, SecureNAT will choose Default Gateway as the IP address of a Router and then this Router needs routing to ISA Internal IP

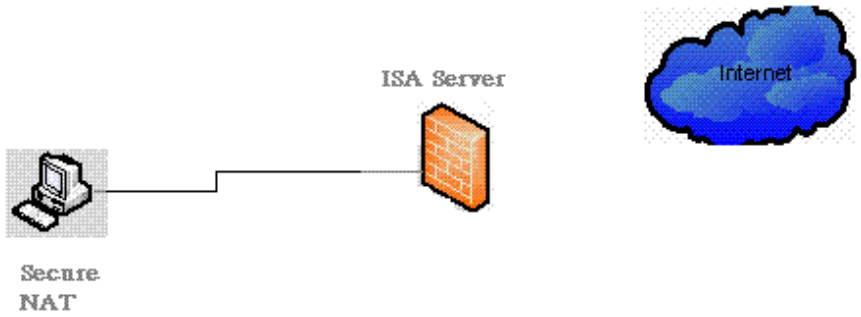



Figure 2: Simple Network Model

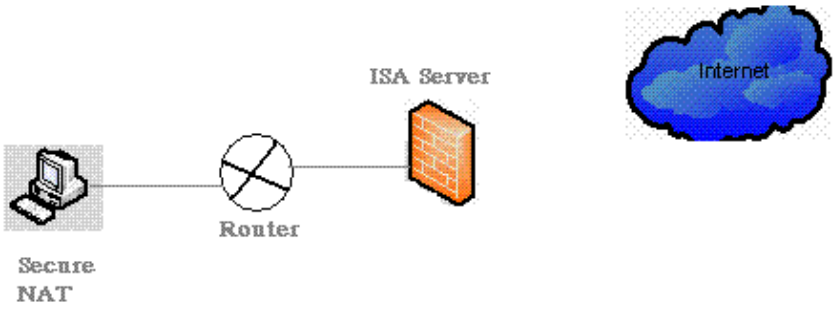



Figure 3: Complex Network Model

- Which modes of SecureNAT client work on ISA server?
? Firewall mode and Integrated mode.Note that Cache mode is not listed here.Because the SecureNAt client needs to use ISA server as a Router while this function does not exist with ISA server Cache mode.The Firewall service must be installed and operated on ISA server before the SecureNAT client can 'get out'.
- If the computers do not run Microsoft Operating System (non-Microsoft Host), can they become SecureNAT?
Yes, because of the simple non-Microsoft Hosts, only need to set to LAT Host and use the Default Gateway as ISA Internal IP
- Does SecureNAT Client have the feature to automatically update ISA Auto-Detect configuration?
? No
- What protocols can SecureNAT Client use?
C? Can use any simple-simple protocol (except for secondary connections).These protocols are listed in **Policy Elements** , **Protocol definitions** , and allowed (allow) in **Access Policy, Protocol Rules** ). These protocols are not restricted by **User** or **Group** in **Access policy, Site and Content rules** on ISA server.
- Can SecureNAT client use Secondary Protocol?
? No
- SecureNAT Client can be authenticated with non-client ISA Server?
, No, when the request from SecureNAT is sent to ISA server, you will not notice the pop-up authentication appears to fill in the authentication information, or 'failed' when making the connection.These are signs that the SecureNAT client is not authenticated by ISA server, the authentication depends on Application, or service when initiating the request to ISA Server and the authentication technique is applied to those requests.
- Does ISA server support DNS to resolve name queries for SecureNAT clients?
, No, when configuring the client machine's TCP / IP settings, you must enter the required DNS parameters (or you can multiply these parameters automatically from the DHCP server).Is it unfair for the SecureNAT client when Web Proxy Client and Firewall clients are supported to resolve DNS hostnames from ISA server through the *ISA Web Proxy / Firewall services' DNS "feature"* this question for Microsoft? Thus, the TCP / IP SecureNAT client configuration must specify which DNS, Internal DNS or External DNS will be used (from ISP). Whether using DNS must be approved by ISA server (allow) in the Protocol rule control policy. For example, administrators can create a Protocol rule called 'Internet DNS' and enable ***DNS queries*** and ***DNS zone transfer*** protocols. *Note not to select the Server versions for these protocols, because it is used for publishing the Server and not passing the query requests outside* .Figure 1 shows us that SecureNAT client uses DNS IP 192.168.1.200, which is installed on ISA (ISA server also does DNS server caching-only mechanism, meaning when receiving requests to find Hostname from SecureNAT will forward to other DNS servers present in the Forwarders list (usually ISP's DNS servers), and then retain the results in their DNS cache to serve the next query coming from the SecureNAT other clients.

2. ***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 hosts Proxy requests sent to the Outbound

web listener on ISA server to the Internet Requests from an ISA web proxy client are sent directly to ISA server Web proxy service, following rules and restrictions that Web Proxy service specified.

**Configure at ISA server to support Web Proxy Client**

Open the ISA MMC and scroll down to Client Configuration.Right-click Web Browser and select Properties;Select the Direct Access tab you will see as shown in Figure 4. This is where we will have some settings related to Internet explorer at Connection tab.All of the settings here will be sent to IE as a Jscript (if the client's IE creates a request to update Web proxy parameters, will the following path be used http:////array.dll?Get.Routing.Script or http:////wpad.dat.

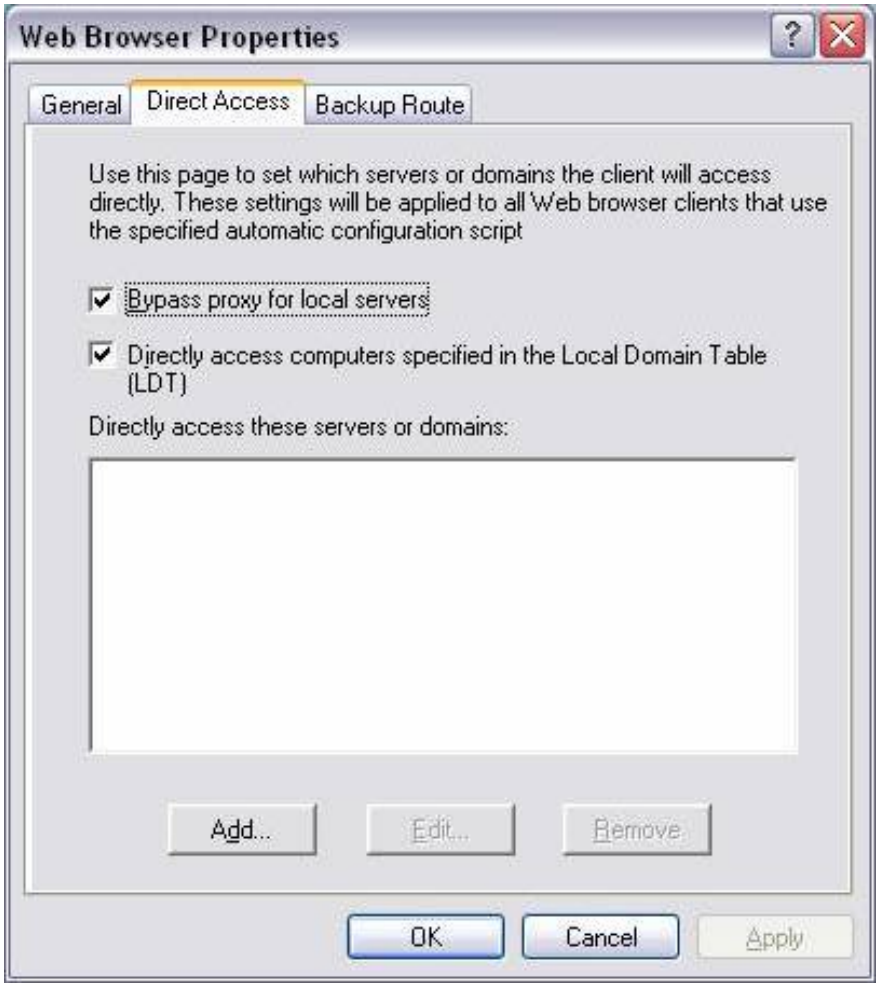


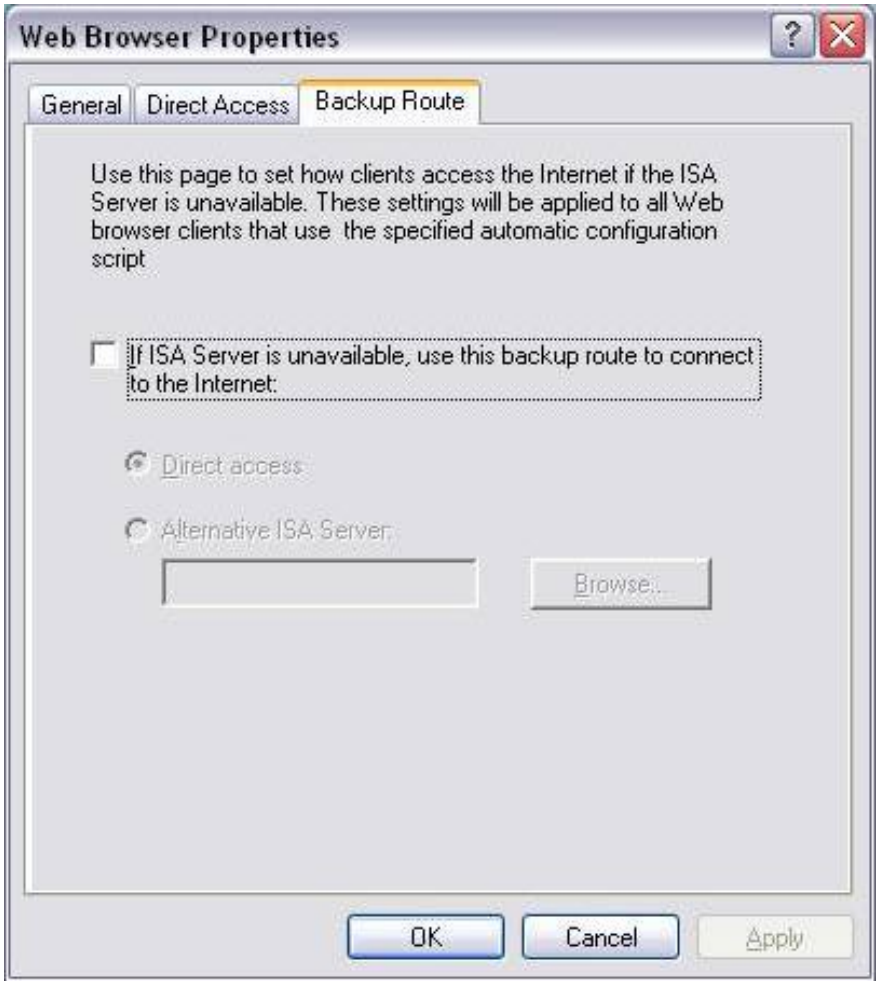

Figure 4: Configure the parameters provided for the Web proxy client on ISA Server

**Bypass proxy for local addresses -** Explained in **the Client machine configuration becomes a Web proxy client**

**Directly access computers specified in the Local Domain table (LDT ) -** If you do not check this setting, IE on the client will still send requests with 'proxy' to ISA Server Web proxy service before this service passes the request to Internal Host belongs to LDT- Local Domain table.Sometimes on an Internal Network mutual access between Internal Hosts will check here to establish access speed.

**Directly access these servers or domains** - This setting allows you to access specific servers / domains, in addition to the two rules set above (use the Add button to list), if these Servers / domains are located in outside your Network (internet) IE will expect the SecureNAT or Firewall Client to work for this request

Next, select Backup Route tab.This setting allows IE to use alternate means to go to the Internet in case the primary ISA server is not responding.There are 2 options:
**Direct Access** - This option allows IE to make requests such as a SecureNAT or Firewall client, of course in this particular case the Client machine has been configured as a SecureNAT / Firewall client.
**Alternative ISA Server -** This option allows ISA to use a secondary ISA if the Primary ISA fails




**Client machine configuration becomes a Web proxy client:**
Using Internet Expolorer 6.0 as an example of web proxy client configuration
Open Internet Expolorer 6.0 Tools Internet Options Connections LAN settings

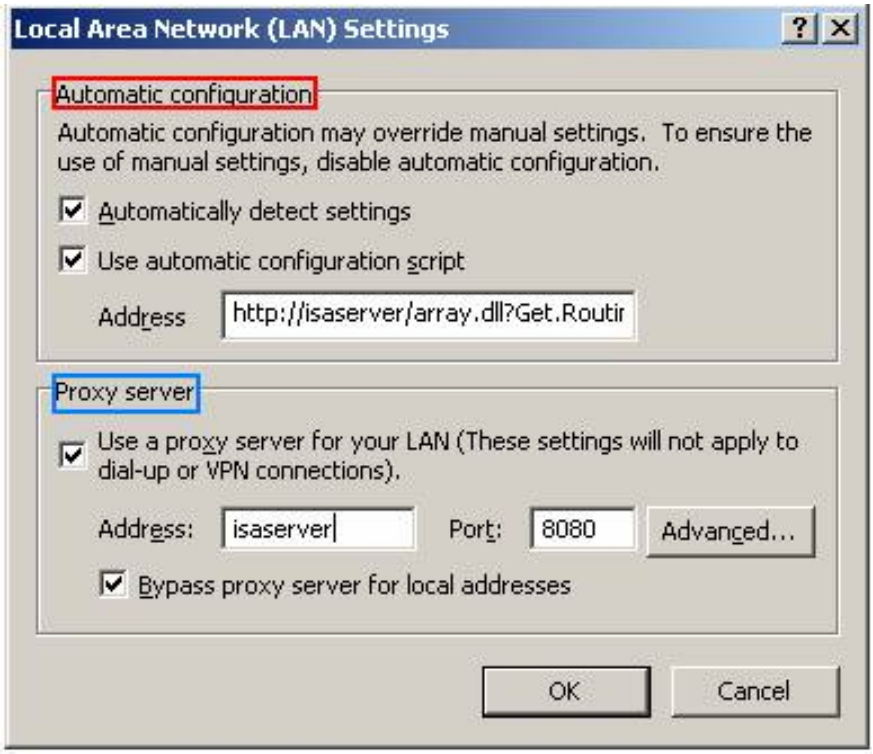



Figure 6: Description of configuration for a Web proxy client based on IE 6.0

As you can see, setting up the client to become a Web proxy client is not difficult.I temporarily separated into 2 sets and considered them independent of each other (the truth is so)
- **Automatic configuration** (section in Red frame): This section includes 2 settings for Automatic detect settings and Use automatic configuration script
**Automatic detect settings** : Completely dependent on the Auto Discovery feature when this feature is enabled, in addition to the WPAD entry in the internal DNS zone.If you do not have internal DNS or DHCP with the specified 252 option, this feature should be turned off.In addition, if you are using IE older than version 5.0, or other internet browsers, this feature will not work and also note that the Client cannot use the ISA Auto Detection feature until it can be resolved. ISA Server name (in the picture is isaserver), this is a prerequisite.
**Use automatic configuration script** : Allows the Browser to configure itself according to a script provided from ISA server. This JScript is formed from the configured parameters in LDT (local domain table), and the Web Proxy Client Configuration options. An example of a path to receive Jscript file parameters is as follows:
*http:///isaserver/array.dll? Get.Routing.Script or http://isaserver/wpad.dat*

- **Proxy Server** (Blue frame) includes setting Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections) and set up Bypass Proxy server for Local address.Using these settings is only used when Automatic settings settings are not available or set to blank (None)
**Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections) These settings will not apply to** dial-up or VPN connections
**Bypass Proxy server for Local addresses** the Client access to Internal Hosts without changing the request to Web proxy Service on ISA Server.Checking this setting can help clients access the Internal Host easily (without ISA Server Web proxy service control) and faster.

*Questions related to Web proxy Client:*

- What are the client client's Web proxies operating on ISA server?
? Works on all modes of ISA server (Firewall, Cache, Intergrated)
- Computer does not run Microsoft Operating System (non-Microsoft Host), can it become a Web proxy client?
Application Any application running on a LAT host can become a Web Proxy client if:
a.Applications (browser, FTP client, etc.) are compatible with CERN (CERN-compatible), which is simply a common method for Aplication to initiate proxy requests to Proxy Server service.
b.Provides a means to allow you to specify Computer name, IP address and -port port to serve proxy requests.
- Does the Web proxy client have the feature to automatically update ISA Auto-Detect configuration?
? ISA auto-detection for Web Proxy clients only supports Internet Explorer 5.0 or later versions.
- What protocols can Web proxies use?
Protocol The protocols used with Web proxy clients are quite limited, including HTTP, HTTPS and FTP download
- Is the Web proxy client using Secondary Protocol?
, No, only use the simple protocols
- Can Web proxy client be authenticated with non-Client ISA Server?
. Yes.
- Does ISA server support DNS to resolve name queries for Web proxy clients?
, Yes, thanks to the *ISA Web feature Proxy DNS "feature"*.This feature allows a LAT host as a Web proxy client to use DNS services provided by ISA Web proxies that do not need to configure DNS related parameters themselves.

3. ***Firewall*** : Also a LAT host, installed with the software ***ISA Firewall client*** , ***enabled*** and the client applications will use it later.
This type of client has most of the capabilities in working with ISA server, because it has the ability to perform on each application 'per-application' how it works and what information it will need for each application to operate.In addition, it is the only type of ISA client that can use the **secondary protocols** .Connection is required to use the secondary protocols for applications such as Instant Messaging (yahoo messenger .), streaming media, FTP, etc.And it is also the type of ISA client that makes it difficult for users to experience 'thoughts' when deploying.

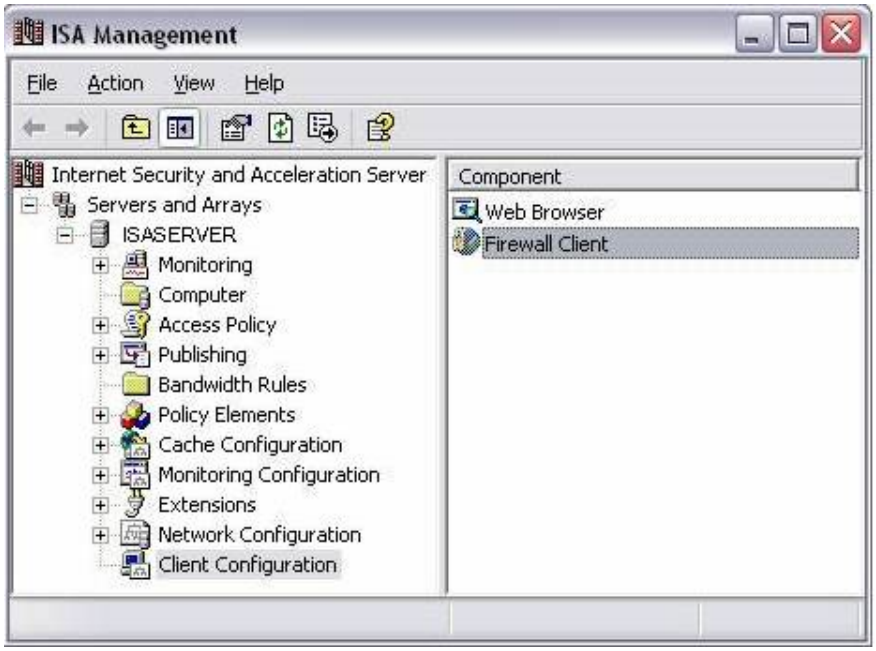
*Questions related to Firewall Client:*
- What types of modes does Firewall Client work on on ISA server?
? Firewall, Integrated.Note that Cache mode does not work with Firewall Client.Because ISA server installed in cache mode has absolutely no Firewall service- this service is required for Firewall and SecureNAT clients to function properly.
- Computer does not run Microsoft Operating System (non-Microsoft Host), can it become a Firewall Client?
? No.
- Does ISA server support DNS to resolve name queries for Firewall Client?
? Yes, a great thing.Firewall Clients have the ability to resolve hostnames through ISA Firewall service DNS on ISA server. If you do not want to use the ISA Firewall service DNS on ISA server, you can configure to resolve the Hostname like SecureNAT clients.
- What protocols can Firewall Client use?
? Firewall Clients can use all protocols with the condition:
**.** Allowed in **Access Policy, Protocol Rules**
**.** Not blocked by **Site and Content Rules**
**.**You can use secondary connections
- Is Firewall Client using Secondary Protocol?
. Yes
- Firewall Client can be authenticated with non-ISA Server Client Authentication?

? Firewall Clients, like Web Proxy clients, can authenticate with ISA server
- Does the Firewall Client have the feature to automatically update ISA Auto-Detect configuration?
. Yes

Firewall Client (FWC) and parameters:

**Configuration Files** - On Firewall Client LAT host includes 2 Files in Program FilesMicrosoft Firewall Clientinternal_setup 2 files that hold the settings for Firewall Client software and how to respond to Winsock requests from applications and services:
**- mspclnt.ini** ; This file contains most configuration data and presents the content of wspad.dat
- **msplat.ini** ; This file contains all entries created in Network Configuration, Local Address Table, and is located separately on the Client to maintain compatibility with the Proxy-2 form of the wspcfg.dat file. This file also contains 2 subnets including:
**224.0.0.0-255.255.255.254** standard multicast subnet. Since ISA server does not allow multicast transmission, this IP multicast area must be identified as Local addresses.
**127.0.0.0-127.255.255.255** This is the 'localhost' address.The address in this area is only valid for the host running, not valid for ISA server in managing clients.
Both files will be sent to ISA server during the installation of the *Firewall Client software* on the LAT host.
After installation is complete, User clicks on the **Update Now** button on *Firewall Client* configuration dialog, the next steps will occur:
**1.** If ' *Enable ISA Firewall automatic discovery in Firewall Client'* checkbox is selected, FWC will make a connection to http:///isaserver/wspad.dat to get the settings and save to **mspclnt.ini**
**2.** FWC then connected to ISA via TCP-1745 port to receive data for **msplat.ini** and get other data for **mspclnt.ini** at the same time.
Always pay attention to the solution to find the name of the ISA server to be complete, otherwise it will not receive configuration numbers for two files from ISA server.

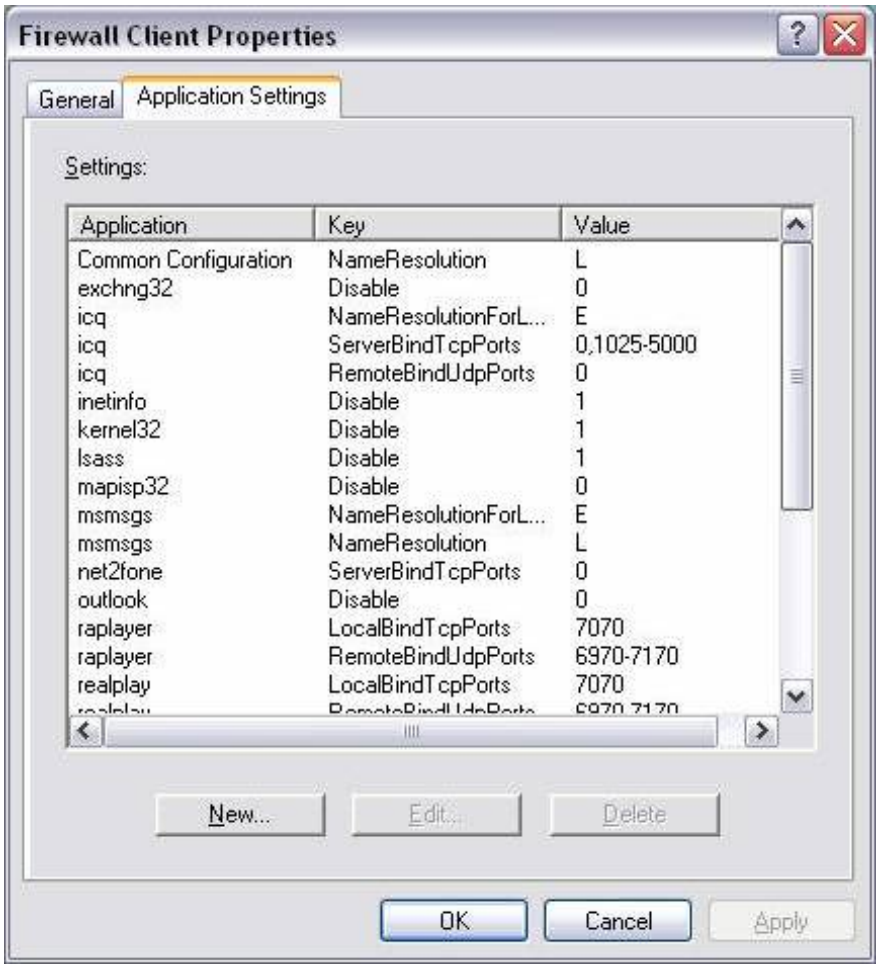
The settings on ISA Server support Firewall Client *:*
The settings in this section are important to provide the Firewall Client and its applications with appropriate parameters when working with the ISA server.
First of all, open **Client Cnfiguration Firewall Client** .Here is all you need to set up to specify how to work between applications of Client and ISA server through Firewall Client software:




double-click on **Firewall Client**

This is where we can create or interrupt functions of the ISA Firewall Client.Everything you set here is defined as the *default settings* for the *Firewall Client when you complete the installation of the* FWC software on the LAT host, as well as this data will be transferred to the *Firewall Client* when it requests to update the new parameters from the ISA server. (refresh)
**DNS name:** NetBIOS name of ISA server is entered by default.You should not interfere with this established default name. Unless you have installed a round-robin DNS model to improve server load balancing (internal load balancing).

- **IP address:** Instead of using a name, you can set up using the IP address of ISA server if you don't have any internal name search solutions like (WINS, DNS).
- **Enable ISA Firewall automatic discovery in Firewall Client -** Actually this setting does not control the Firewall Client task auto-detect ISA server, this setting can be changed from the Firewall Client side.
- Next, click on the 'Application Settings tab;Here you can create or stop applications that are compatible with Winsock (Winsock-compatible applications with ISA Server Firewall Client




(out of part 4)

**Ho Viet Ha**
Training Manager of New Horizons Vietnam (Computer Learning Center)
E-mail:hvha@newhorizons.com.vn

for similar articles on tips and guides. Thank you for reading and for following us regularly.