

InterwiseConnect™

Working with NAT

Version 7.2

Table of Contents

INTRODUCTION	3
Interwise Connect	3
APPLICATION ADJUSTMENTS.....	4
Preliminary Adjustments.....	4
Materials Editor	4
Participant.....	4
Install From The Web (IFTW)	4
Communications Center (ICC)	4
Server Manager (ISM)	4
Communications Server (ICS)	5
Push Server	5
EXAMPLE	5
DMZ NAT	5
ICC Browsing.....	5
Connecting to a Live Event.....	5

Introduction

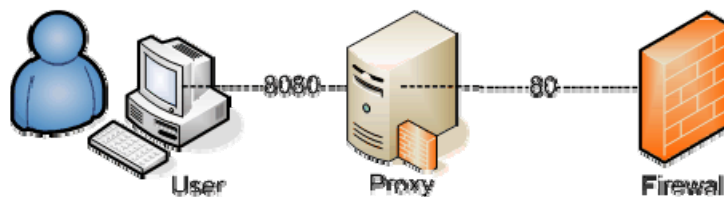
NAT (Network Address Translation) is the translation of one IP address to another IP address. Today NAT has become part of almost any network topology and there are several motivations for network administrators to use it.

The main reason for using NAT is the limited number of public IP addresses in comparison with the number of computers and devices in the company's network. NAT enables the organization to get round this by using a firewall or web proxy that translates the address of a private IP address to a public IP address before sending the request to the Internet (i.e. to a web site).

Other reasons for working with NAT:

- ◆ **Extended security offering:** An important reason for organizations to use NAT technology is the extended security it offers. NAT extends security by keeping the internal IP addresses of one network segment hidden from devices and users on another network segment (i.e. hiding LAN's IP addresses from users in the Internet).
- ◆ **Dynamic/Static NAT:** There are two different methods of using NAT: dynamic and static. In static NAT, given IP address is always mapped to another specific IP address whereas in dynamic NAT, an IP address is mapped dynamically when needed to an IP address out of a given pool of addresses. In dynamic NAT, the mapping takes place ad hoc when needed based on the availability of any IP address in the pool.
- ◆ **Port address translation (PAT):** Similar to address translation, there is an option to use port translation. This way, a connection is sent to a specific port that is routed in the way to another port by the device that implements the PAT (i.e. firewall, proxy or router).

The following diagram illustrates PAT from port 8080 to port 80 by a web proxy:



Interwise Connect

Interwise Connect is comprised of several client (e.g. Participant, Materials Editor, Outlook AddIn) and server (e.g. ICC, ISM, IPP, ICS) applications.

Organizations may choose to locate one or more Interwise Connect applications in a network environment that is configured to use NAT. Interwise Connect is fully supported when working in such an environment. The following section details the required configurations and settings that will enable it.

Application Adjustments

Preliminary Adjustments

- ◆ **ICC:** The IIS IP address of the ICC must have a DNS common name (FQDN) configured, published and accessible to all of the Interwise Connect users.
- ◆ **ISM:** The ISM should also have a DNS common name if it is located behind NAT.
- ◆ **IPP:** The IPP should also have a DNS common name if it is located behind NAT.



Note: Accessing the ICC should take place using the common name only (i.e. via browser and/or Outlook AddIn).

Materials Editor

The Participant application, when running the Materials Editor AddIn, holds the ICC parameters for uploading and downloading Event Materials. The ICC URL should be configured with its common name (DNS name).

Participant

The Participant application needs no special configuration to support NAT.

Install From The Web (IFTW)

The Install From The Web files may contain the ICC address for the My Interwise application. The ICC address should be configured using the computer name and not the IP address.

Search for all **Student.ini** files under \Interwise and edit each one of them as follows:

1. Open the file using Microsoft Notepad.
2. Under the [ICC_URL] section, edit the ICC_URL key.

Communications Center (ICC)

1. The IIS IP of the ICC must have a DNS name if located behind NAT as mentioned in the *Preliminary Adjustments* section above.
2. The ICS and its Push Server should be configured as mentioned in the *Communications Server* section below.
3. The Remote Controller should be configured with both the internal and external IP addresses in the ICC (**System Management > Application Parameters > Application Parameters > Install_Shield > Install_RC_Ip**).

Server Manager (ISM)

The ISM needs no special configuration other than having a DNS name if located behind NAT, as mentioned in the *Preliminary Adjustments* section above.

Communications Server (ICS)

1. The ICS should be configured to use the ISM common name if the ISM is installed behind NAT. These settings are applied while installing the ICS but can be changed later via the *Interwise Server Options* (**Start > Programs > InterWise > InterWise Server Options > ISM Properties**) and restarting the Interwise Services and processes.
2. The ICS should be configured with both its internal and external IP addresses in the ISM. The ISM is configured to support these two IP addresses.



Note: The internal IP address is an IP address which is actually assigned to that machine and is registered in the operating system whereas the external IP address may be defined only in the routing device (i.e. firewall).

Push Server

The Push Server should be configured manually to recognize the external IP address. Please refer to the *Defining PushOverrideIP and PushOverridePort* section in the *Installation Guide*.

Example

DMZ NAT

In this scenario, The ICC, ISM and ICS are located in a DMZ (Demilitarized Zone) which is accessible to users connecting behind the firewall (from the LAN) as well as users connecting from the Internet.

For security reasons, the organization has decided to hide the IP addresses of the ICC, ISM and ICS. Therefore, a DNS name is assigned to the ICC and another one to the ISM. The firewall is configured with a rule that applies NAT on the IP address of the ICS so it has both internal (real, defined in Windows) IP address and an external IP address (defined only in the firewall).

ICC Browsing

Users that want to access the ICC are using a DNS name that is mapped to an IP address accessible from the Internet. This external IP address is not the IP address that is assigned on the ICC machine in the IIS but rather an address that is later translated by the firewall to the real IP address. The solution guidelines are:

- ◆ This process is transparent to the users as they use the DNS common name.
- ◆ The organization achieves security value as the real IP address is not published to the outside world.
- ◆ The use of a DNS name is important for the scenarios where the ICC needs to send out links with its address (i.e. in mail invitations).

Connecting to a Live Event

Users receive the list of servers that are available for the Event. The ICS will appear in the list twice, once with its internal address and once with its external address.

The ISS will drop the internal address and establish the connection to the external address that will later be translated by the firewall to the real IP address.

The solution guidelines are:

- ◆ This process is transparent to the users as the ISS drops the IP addresses that are inaccessible to the user.
- ◆ The organization achieves security value as the real IP address is not published to the outside world.
- ◆ The use of the internal address enables the ICS to bind to this address and thus create a listening socket for the incoming requests.

