Network Address Translation (NAT) in the SAP Environment
Copyright

Copyright © 2000 SAP AG. All rights reserved.

No part of this brochure may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

SAP AG further does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within these materials. SAP AG shall not be liable for any special, indirect, incidental, or consequential damages, including without limitation, lost revenues or lost profits, which may result from the use of these materials. The information in this documentation is subject to change without notice and does not represent a commitment on the part of SAP AG for the future.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft®, WINDOWS®, NT®, EXCEL® and SQL-Server® are registered trademarks of Microsoft Corporation.

IBM®, DB2®, OS/2®, DB2/6000®, Parallel Sysplex®, MVS/ESA®, RS/6000®, AIX®, S/390®, AS/400®, OS/390®, and OS/400® are registered trademarks of IBM Corporation.

OSF/Motif® is a registered trademark of Open Software Foundation.

ORACLE® is a registered trademark of ORACLE Corporation, California, USA.

INFORMIX®-OnLine for SAP is a registered trademark of Informix Software Incorporated.

UNIX® and X/Open® are registered trademarks of SCO Santa Cruz Operation.

ADABAS® is a registered trademark of SAP Software AG.

SAP®, R/2®, R/3®, R/3 Retail®®, R/3 Retail®, ABAP®, SAP ArchiveLink®, SAPaccess®, SAPmail®, SAPoffice®, SAP-EDI®, R/3 Retail®, SAP EarlyWatch®, SAP Business Workflow®, ALE/WEB™, Team SAP™, BAPI™, Management Cockpit™ are registered or unregistered trademarks of SAP AG.

Icons

The following icons are used in this document as visual aids.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚨</td>
<td>Caution</td>
</tr>
<tr>
<td>🎮</td>
<td>Example</td>
</tr>
<tr>
<td>📜</td>
<td>Note</td>
</tr>
<tr>
<td>💡</td>
<td>Recommendation</td>
</tr>
</tbody>
</table>

Version

Contents

INTRODUCTION.................................................................................................................. 5

Layout of this Document .................................................................................................... 5

NAT BASICS.................................................................................................................. 6

Using NAT......................................................................................................................... 6

NAT Functions.................................................................................................................. 7
    A) Static Address Translation ......................................................................................... 7
    b) TCP Port Address Translation (PAT) ........................................................................ 8

BASIC RULES FOR CONFIGURING NAT................................................................... 9

Implementation ................................................................................................................ 9

SAP Server....................................................................................................................... 9

Frontend Host .................................................................................................................. 9
    Alternative Configurations .......................................................................................... 10

PROBLEMS AND SOLUTIONS .................................................................................... 11

SAP Logon Load Balancing ............................................................................................. 11
    A) Defining an Additional Logon Group....................................................................... 12
        Procedure: ............................................................................................................... 12
        Restrictions ............................................................................................................ 12
    B) Using SAProuter..................................................................................................... 14

NAT and RFC .................................................................................................................... 15
Introduction

Layout of this Document

This document uses examples of configurations to describe the problems that can occur when SAP systems and frontends communicate with each other using NAT, and how you can solve these problems.

The \textit{NAT Basics} section (page 6) provides basic information about the functions and implementation of NAT.

The section entitled \textit{Basic Rules for Configuring NAT} (page 9) contains information about the instances where it makes sense to implement NAT, and those where other solutions are to be preferred.

In the \textit{Problems and Solutions} section (page 11), typical NAT configuration problems and their respective solutions are described using examples.
NAT Basics

Using NAT

When allocating IP addresses in the Internet, there is the problem that only a limited number of addresses are available worldwide, due to the 32-bit digit code. It is therefore necessary to assign official IP addresses that are valid worldwide as restrictively as possible.

Independent of that, private IP ranges can be defined in company networks. Since these private IP addresses are not transferred into the Internet using a router, no conflicts occur with IP addresses outside the company network.

If communication is to take place between a host in the private company network and a partner in the Internet, then the company-internal IP addresses must be translated into official IP addresses.

Network Address Translation (NAT) is a method that enables such a translation of IP addresses between different networks.

There are various reasons for implementing NAT:

- For a large number of hosts with private IP addresses, just a few official IP addresses are required, since external communication is dealt with using different ports. This is particularly an option if only a few computers are communicating externally at the same time.
- NAT enables you to connect communication partners who would otherwise be unable to reach each other directly due to address conflicts (overlapping IP ranges).

The translation of private IP addresses into official IP addresses (or the other way round) takes place predominantly in the IP protocol layer and, in some cases, also in the TCP layer:

TCP/IP Reference Model

You can always anticipate problems and restrictions with NAT if, in the application layer, data from the subordinate layers is sent. In particular, this affects transmission of IP addresses and TCP ports in application data.

The following describes the NAT translation process in greater detail.
A) Static Address Translation

The translation of IP addresses is usually performed by a router. This acts as a gateway between both networks and, since it has a routing table, it is able to replace IP addresses from the private IP range with official IP addresses and transfer these to the other network.

The communication partner, which is located outside of the private company network, can use the address translation to communicate with the host in the internal network as if it were in the same IP range.

The following graphic shows the process:

```
Host 10.1.1.2 is located in a company network that has private IP addresses (blue area), whereas host 198.1.1.2 belongs to a network in the official IP range. The router that performs the address translation has two NICs (Network Interface Cards). An IP address in the private network is assigned to one of the NICs (10.1.1.1), and an official IP address is assigned to the other NIC (198.1.1.1). The communication now proceeds as follows:

1. Host 10.1.1.2 attempts to contact host 198.1.1.2 and sends IP packets with the following header information:
   
   S: 10.1.1.2
   D: 198.1.1.2
```
"S" (Source) refers to the IP address of the source host and "D" (Destination), the IP address of the target host.

2. The IP packets are sent to the router (10.1.1.1) that acts as a default gateway for the 198.1.2.x network. The router now performs a mapping and assigns an official IP address for the host from the company network: 198.1.2.3. Using this address, the host can now be contacted from the outside. The router enters this address as a source in the header of the IP packet and transfers it to the 198.1.1 network:

   S: 198.1.2.3
   D: 198.1.1.2

   The information that belongs to the primary source (10.1.1.2) may still be included in the application data.

3. The IP packets reach host 198.1.1.2, which analyzes the packet information. The host sends back a packet whose target is the IP address of the company-internal host. This IP address comes from the mapping.

   S: 198.1.1.2
   D: 198.1.2.3

4. The IP packets arrive at the router. The router performs another mapping and replaces the official IP address of the target host with the original company-internal IP address (10.1.1.2).

   S: 198.1.1.2
   D: 10.1.1.2

   Using this information, the packet finds its way back to the original host.

b) TCP Port Address Translation (PAT)

The static translation of IP addresses (page 7) has the disadvantage that, for every internal IP address, an additional, officially valid IP address must be assigned (1:1 ratio). In the area of server communication there is often no alternative for such a procedure, since a unique assignment of collective communication partners must be possible at all times.

In the area of frontend communication, however, it makes sense to connect a larger number of SAP GUI PCs to an SAP system using a single official IP address.

In addition to the IP address, an individual TCP port is also assigned to distinguish between the connections. The TCP/IP packet header contains the following information:

   S: IP, Port(n)
   D: IP, Port(n)

The actual communication stages correspond to the procedure mentioned in a), but the unique characterization of a connection occurs through the use of an IP address and port. This means that for each host that opens a connection to the outside, the same official IP address and a private local port is assigned, which is allocated for the entire duration of the communication. Once the communication is finished, this port is released again after a certain waiting time. It can then be used for another connection. One restriction of this procedure is that the communication partners are no longer able to identify the starting point of the connection, since the IP address is identical for all connections. However, such an identification is not usually required.
Basic Rules for Configuring NAT

Implementation

There are can be different scenarios where NAT configurations make sense. Some of the most frequent examples of use are:

- Connecting SOHOs ("small office - home office" environments) to a company network.
- ASP connection (ASP, Application Service Provider).
- Access to a common network for subsidiaries.
- SAP GUI access using the Internet.

When you configure NAT scenarios of this nature, note the following basic rules:

SAP Server

- For access in the Intranet, you have the option of using official registered IP addresses for the server, or private unregistered IP addresses.
- If you use private IP addresses for the server, then access from the public network (Internet) has to take place using a SAProuter.
- There must always be a direct network connection between the servers of an SAP system (no NAT and usually no routing).

Frontend Host

Private, unregistered IP addresses are usually used for frontends. For connections over the Internet and for overlapping IP addresses, NAT or SAProuter is suitable.

The following graphic shows a NAT configuration that fulfils the basic rules described above.
Alternative Configurations

If the frontend hosts of the company network have to communicate only with the hosts in the official network as SAP frontends (SAP GUI) that is, if the frontends do not require any Web access, then use a SAProuter as opposed to NAT. A SAProuter simply passes on SAP data streams and must not be confused with a TCP/IP router.

For more information about using SAProuter, see the section Using SAProuter (page 14).
Problems and Solutions

SAP Logon Load Balancing

The following explains which NAT configurations in the SAP environment are problematic and how possible communication problems can be resolved.

- The following graphic shows an SAP GUI frontend host that belongs to a network in the official IP address space.
- The SAP systems are located in a company network with private address space.
- *Logon Load Balancing* is to be supported when logging on to the SAP systems.

1. The SAP GUI host connects to the message server. The requests of the SAP GUI are forwarded to the private IP network using the router.
2. The message server (10.1.1.4) analyzes these requests and delivers the internal IP addresses of the application server back to the SAP GUI where the logon takes place. In this example, this is the application server with the IP address 10.1.1.2.

The problem is that the SAP GUI in the remote network tries to perform a direct logon on the application server using its private IP address (10.1.1.2) and therefore runs idle. For the SAP GUI, the IP address proposed by the message server ("use 10.1.1.2") is always conclusive. For the logon to be successful,
however, the message server must send the instruction "use 198.1.2.2", since this is the only IP address that is known outside of the company network.

There are two ways of solving this problem:

- You can define an additional logon group (see page 12)
- You can implement a SAProuter between the company network and the public IP range (see page 14).

A) Defining an Additional Logon Group

You can use the following procedure to define a new logon group on the message server, which includes the officially valid IP address of the application server (198.1.2.2).

Procedure:

1. Log on to the system.
2. Call transaction SMLG.
3. Choose Create Entry.
4. Specify a name for the new logon group (for example, EXT).
5. In the Instance field, enter a valid instance name. This is structured as follows: <HOSTNAME>_<SID>_<SYSTEMNUMBER> (for example, hw1234_CBA_00).
6. Choose Attributes and enter the official IP address that the application server has from the viewpoint of the frontend host (in our example: 198.1.2.2).

7. Choose Copy and then save.

Restrictions

The effort required for manual maintenance can increase considerably – particularly if there are a large number of networks with frontend hosts. In such cases, proceed as described below.
B) Using SAProuter

Since maintaining logon groups (page 12) for a pure NAT solution often means high maintenance effort, it usually makes more sense to control the communication between SAP GUI and SAP servers using a SAProuter. For reasons of security, SAProuter is usually located in the Demilitarized Zone (between firewall and router). Note that SAProuter is not an IP router; it is a router for transporting SAP data.

The communication process contains the following steps:

1. The SAProuter (198.2.1.5), which acts as a gateway to the private network, is entered in the SAP router string of the frontend SAP GUI: `/H/198.2.1.5`
2. The SAProuter performs a routing to the message server (10.1.1.4).
3. The message server determines an application server and sends the information "use 10.1.1.3" to the SAP GUI.
4. An entry for the application server is made in the SAProuter string of the frontend: `:/H/198.2.1.5/H/10.1.1.3`. This information enables a connection to the application server, since the SAProuter knows the internal address.

When you plan such a configuration, note the following points:

- Host names are also tolerated in the SAProuter string.
- You must avoid using dynamic IP addresses in the SAP server network.
If the communication between SAP GUI frontend and message server takes place over a WAN, then it may be advisable to install a SAProuter in both networks. This makes sense, for example, if TCP/IP problems occur over the WAN, and they are connected with the TCP/IP stack of the frontend host.

**NAT and RFC**

RFC is a method of executing a function on a remote host. First the *importing parameters* are transferred to the remote host, then the function is started, and then the result (*exporting parameters*) is transferred back. A gateway is usually used to start an RFC server.

If you use RFC interfaces, particular configuration requirements arise in the NAT environment, since the translation of IP addresses using NAT is only possible at the TCP/IP level (see *Introduction*, page 5).

A problem that is often seen in the NAT environment occurs when the RFC client in a network is located in the official IP range, and the gateway, as well as the RFC server, lie in a private IP range:

1. A setup connection takes place from RFC client to the gateway (10.1.1.3).
2. The gateway checks the target address of the data and recognizes that it is not the target of the connection. It attempts to reconnect to IP address 198.2.1.3 but fails to recognize that this IP address corresponds to its own host.

You can solve this problem in the following way: expand the `gw/alternative hostnames` entry in the instance profile of the SAP System (see SAP Note 0148832). This ensures that the IP address that is assigned by the router (198.2.1.3) is identified as its own host.