Appendix D: Configuring Firewalls and Network Address Translation

The configuration information in this appendix will help the network administrator plan and configure the network architecture for Everserve. This appendix describes two sample configurations and includes a troubleshooting section.

Introduction

This document describes the steps involved in using Everserve for systems that communicate over remote networks. This involves configuring Everserve communities in which some peers communicate across firewalls.

This document is not intended to describe every possible network configuration. Instead, it details two sample configurations and lists setup instructions for installing Everserve in this configuration.

This document is intended for the customer entering into lab trials or field trials with Everserve 2.01, build 2.12, or later.

Overview

Although Everserve is logically a "push" model, communication in an Everserve community is actually always initiated by the Target or Relay. This means that the Target or Relay needs to know how to route traffic to the servers. The information used to build a route, along with keys and other security information, is captured in a community seed file, named <*community*>.zip. The same seed file is used for all peers in the community, including:

- Servers behind the corporate firewall, including Community Managers, Publishers, and Relays.
- Targets behind the corporate firewall
- Targets outside the corporate firewall
- Targets who roam inside and outside the corporate firewall

Specifically, the seed contains the fully qualified hostname of the system running the Java Messaging Server (JMS) and the port used to connect to the JMS server. A fully qualified hostname would be, for example, `foxtrot.widgets.com`. In other words, the target system must be able to resolve to the IP address of the JMS machine, regardless of where the target is located. The DNS servers, firewalls and NAT servers must be able to route the traffic properly, regardless of origin.

Background: Firewalls, Proxies, and DNS servers

A firewall controls network traffic based on rules. Typically, a firewall is used to protect a network from traffic on other networks and/or the Internet.

When a firewall connects two or more networks, it is most often implemented with two or more Network Interface Cards (NICs). One NIC is connected to each network segment. Rules on the firewall then specify what traffic is allowed to flow from one segment to the other. The rules are typically based on the format of network packets, as well as IP addresses and ports.

Often, the two networks will use different IP addressing schemes. For example, a corporate network may use addresses matching 10.x.x.x, which is not routable over the Internet. The firewall can translate addresses so that external systems are unable to see or know about the internal IP addresses of machines. This is known as Network Address Translation (NAT).

A firewall with NAT uses forwarding rules to allow external systems to reach internal addresses. These rules say, for example, that all traffic directed to an address on the external side of the firewall should be directed to a different address on the internal side..

Here is an example using two networks:

The external IP addresses for www.synchronnetworks.com is 192.220.116.63. Internally, the Synchron Networks webserver uses IP address 10.148.100.50. The firewall might therefore contain the following rules (in pseudocode):

Incoming traffic (from the public Internet)

- If the target address is 192.220.116.63 on port 80, modify the traffic's target address to 10.148.100.50 and allow the traffic to pass on port 80.
- Block all other traffic

Outgoing traffic (from the protected network to the Internet)

- Modify the source address of all traffic from its 10.148.100.50 address to appear to originate from 192.220.116.63

Proxy servers are used to stand-in for another server. They often do this by accepting traffic intended for another machine, modifying the traffic in some way, and passing it on. For example, an outbound proxy might be configured to intercept requests for HTTP over port 80 and redirect them to a different HTTP server or require authentication.

Domain Name Servers, or DNS servers map host names to IP addresses and vice versa. Externally visible DNS servers provide name and address resolution services to the public Internet. Internal DNS servers provide host name and address resolution to a private network.

For example, one public DNS server reports that the IP address for `www.synchronnetworks.com` is 192.220.116.62. The internal DNS server reports that the name `otter` maps to 10.148.127.249.

Likewise, an external DNS server might report that the host name `foxtrot.widgets.com` maps to 192. 10.148.126.15, while an internal DNS server might resolve the same host name to an internal address of 192.168.2.100. This ability of different DNS servers to resolve the same host name to different addresses is the key to using NAT.

Using Everserve with Firewalls and NAT

Configuring your firewall and DNS

To configure Everserve to work on the Internet, you will need to know and be able to modify:

- The routing rules on your firewall
- The internal IP address of the host running the JMS server and the port number with which it was installed
- The external IP address and ports by which external clients would access the JMS server
- The DNS entry for an externally routable name. For example, `foxtrot.widgets.com`, and the IP address that this name maps to. In addition, the DNS server must support reverse lookup (also called PTR mode) to resolve the host name from the IP address.

- The DNS entries on your internal DNS server. You must provide a fully qualified name for the JMS server's IP address using the same name as used outside, such as `foxtrot.widgets.com`. The internal DNS server must support both forward and reverse lookup.

The external and internal names for the JMS server must be identical. For example, if you use the name `foxtrot.widgets.com` as your externally routable name, the internal DNS server must also have an entry or an alias for this name. The internal DNS server will give out the internal IP address. The external DNS server will give out an external IP address.

Your firewall must be configured to pass traffic from the externally designated port on this external IP address to port 1856 (or other non-default, if so configured) on the internal IP address of your JMS server. If you want to allow remote configuration via the Everweb interface from outside the firewall, open port 8443 for incoming traffic, or the port that you configured the Everweb interface to listen to for connections.

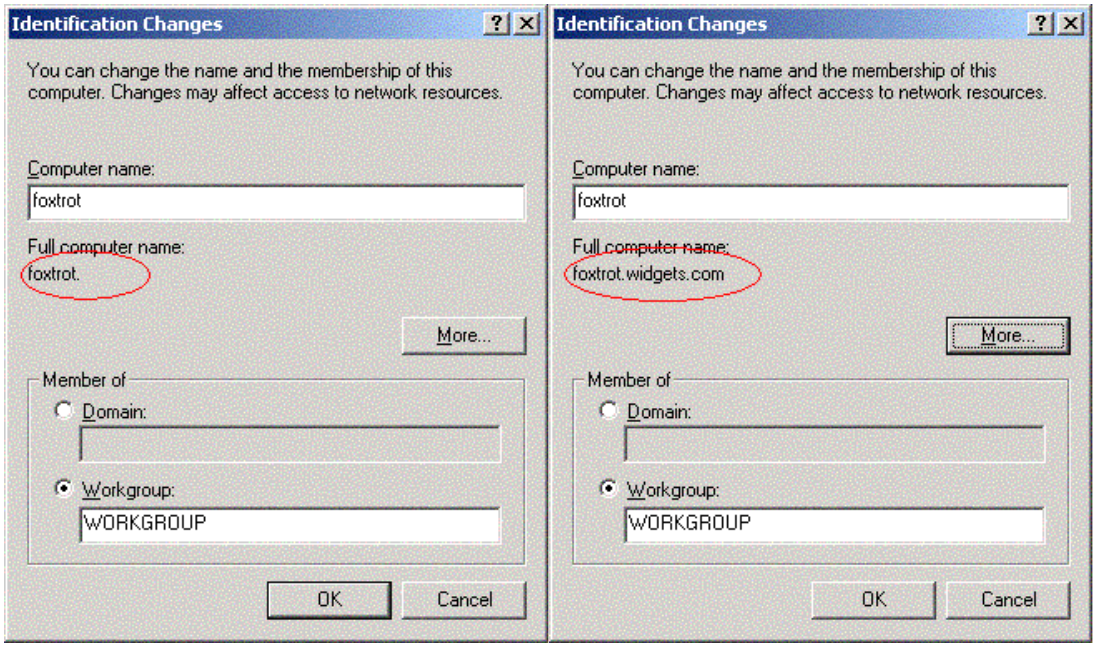
Installing and Configuring Everserve

Configuring Networking on the Server

The Everserve server needs to know its fully qualified domain name. If it has a local JMS server installed, it will use that name to open connections to the local server.

If you are using a static IP on your server, you will need to make sure that the machine name is fully qualified. To verify this on Windows 2000:

1. On the Windows desktop, right-click My Computer and choose Properties from the menu.
2. Click the Network Identification tab and look at the Full Computer name. If the fully qualified domain name is shown, you are finished.



Note that the fully qualified domain name is not displayed in the figure on the left,and it is present in the figure on the right.

3. If the fully qualified domain name is not shown, click Properties to open the "Identification Changes" window.

4. Click the "More…" button to open the "DNS Suffix and NetBIOS Computer Name" window.
5. Enter the domain name suffix in the box labeled "Primary DNS suffix of this computer" and click the OK button
6. Restart the computer when prompted.

Installing Everserve

It is important that this process begin with the installation of Everserve, because the transport properties are read out of a file and moved into the database the first time Everserve is started. Consequently, it is important to make these changes ***before*** Everserve has been allowed to run even once. The steps are:

7. Install MySQL and run {mysqlhome}\bin\winmysqladmin to initialize it. This is just the normal way you would install mySql with Everserve.
8. Install Everserve. Choose "Full Install" from the install page or run setup.exe from the *\installers\windows\WinNTCustomInstall* directory on the CD.
9. When prompted for role capabilities, select the roles for this server. If
10. Ask to "Create New Databases" during installation.
11. When prompted for the "Transport Provider Hostname," be sure to specify the fully qualified domain name (FQDN), such as `foxtrot.widgets.com`.
12. At the last step of the installation, check "Reboot Later" before proceeding. This step is critical. You must alter the configuration before rebooting, because Everserve will auto-start on reboot. Everserve caches most of the configuration data when it runs the first time.

Modifying the JMS Server Configuration

Once Everserve has been installed in a Publisher, Community Manager, or combination Pub/CM role,, but ***before*** the installer has rebooted, do this:

1. Use a text editor to edit the file *ConnectionManager.xml*. This file is typically found in the directory:

   \Program Files\Synchron Networks\Everserve\FioranoMQ5\bin

2. Locate the line containing:

   `<URL>http://localhost:1856</URL>`

   and change it to

   `<URL>http://`*`FullyQualifiedHostName`*`:1856</URL>`

   where *FullyQualifiedHostName* is the host name that resolves correctly in both the external and internal DNS servers. For example,

   `<URL>http://foxtrot.synchronnetworks.com:1856</URL>`

3. If you want to enable remote administration to the JMS server from a Community Manager or Publisher peer outside the firewall, locate the line containing

   `<URL>http://localhost:1857</URL>`

   and change it to

   `<URL>http://`*`FullyQualifiedHostName`*`:1857</URL>`

   where *FullyQualifiedHostName* is the host name that resolves correctly in both the external and internal DNS servers. Note that you only have to allow remote administration to the JMS

server if you have a Community Manager or Publisher outside the firewall that will be using your internal JMS server. It is not necessary to open port 1857 to run the Everweb administration tool outside the firewall.

4. Save the *ConnectionManager.xml* file and exit the editor.
5. You may now reboot this machine and begin to use Everserve

Using Port Address Translation (PAT)

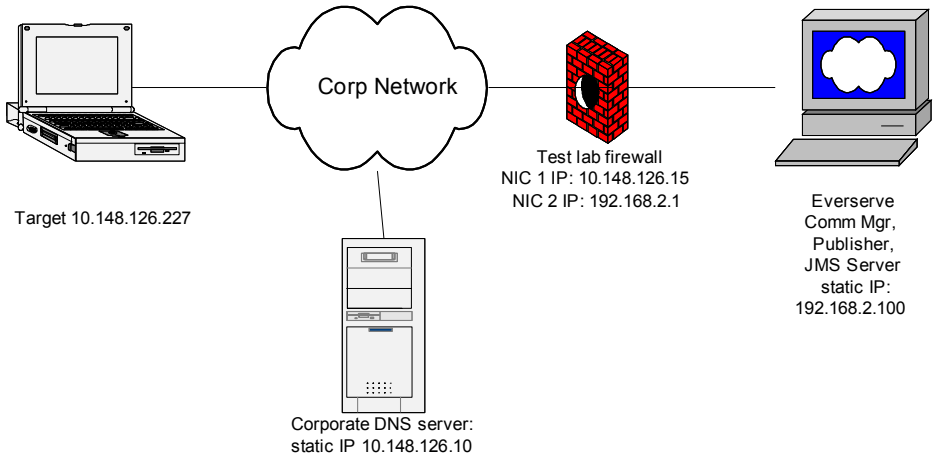
It may be desirable to use Port Address Translation, or PAT, in your network configuration. A router configured with PAT may modify the port numbers of packets as they pass through it. For example, a client may begin transmit a packet with a destination port of 12000. A PAT server may receive the packet, modify the header to change the port number to 800, and forward the packet to the receiver.

It is possible to modify the *ConnectionManager.xml* file to change the port number for the ConnectionFactory. However, the client must be able to find the Everserve server to obtain the ConnectionFactory.

Recall, however, that the JMS client must be able to connect to the serverserver from all locations on the network. For this reason, using PAT is not recommended on an Everserve community.

Sample Configurations

Everserve in a test lab with a single firewall



In this case, the Everserve server is called `foxtrot.widgets.com`. The test lab has a firewall which protects the rest of the Corporate Network from the test lab. The firewall has two NICs: one on the corporate network with a 10.148.126.15 address, and one on the test network, with a 192.168.2.1 address. The corporate DNS server returns the address 10.148.126.15 (the IP of the firewall) when queried for the address for `foxtrot.widgets.com`. Everserve was installed using the standard ports: 1856 for JMS, 1857 for JMS administration, and 8443 for the Everweb administrative interface.

Configuration

Firewall

The test lab firewall has the following rules:

Incoming

- Allow all incoming connections with a target of 10.148.126.15 and a port of 8443, 1856, or 1857, and redirect them to 192.168.2.100
- Reject all other incoming traffic.

Outgoing

- Reject all traffic

Configuration Files

The file *ConnectionManager.xml* in the directory

\Program Files\Synchron Networks\Everserve\FioranoMQ5\bin

was modified. The <FMQConnectionFactories> section was modified to include the text in **bold**.

```
<FMQConnectionFactories>
        <ClientConnectionFactories>
                <ConnectionFactoryInfo type='SUN_SSL'>
                        <URL>http://foxtrot.widgets.com:1856</URL>
```

Corporate DNS Server

The corporate DNS server was configured to map the hostname `foxtrot.widgets.com` to the IP address 10.148.126.15 in its forward and reverse (PTR) lookup tables.

How it works

All connections are initiated by the target. When the Target tries to initiate a connection, it queries its DNS server for the IP address of the Everserve server using the host name in the seed file, which is `foxtrot.widgets.com`. The corporate DNS server returns the IP address 10.148.126.15. which is the IP address of the firewall. The Target then confirms the server name by asking the DNS server for a reverse lookup of the IP address, and the answer is returned as `foxtrot.widgets.com`.

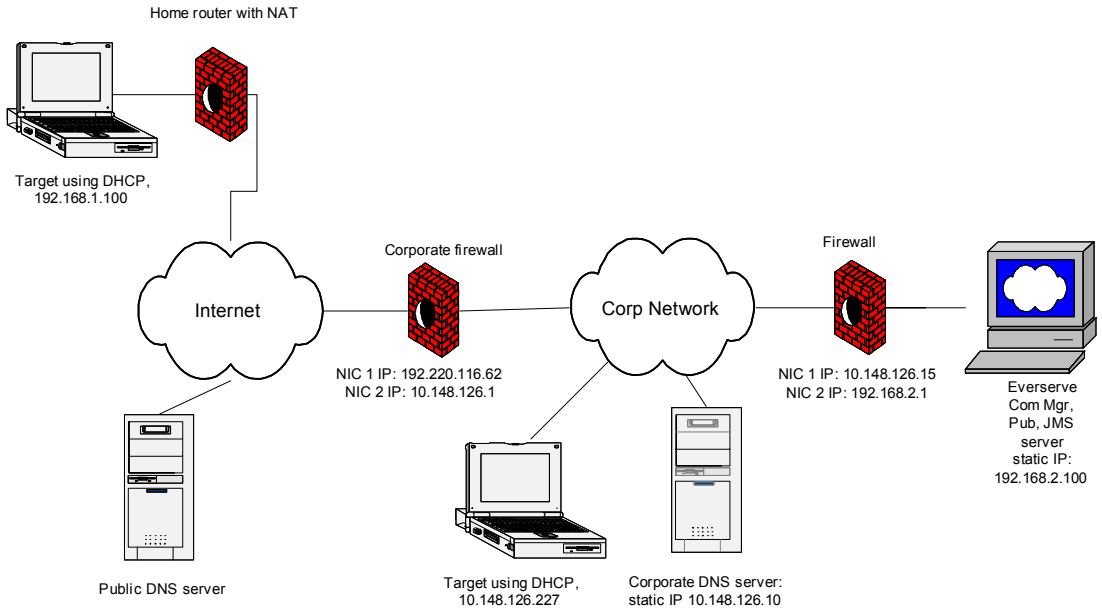
The Target then opens a connection to the machine using the address 10.148.126.15 over port 1856. The firewall server receives the connection request and verifies the port number. The firewall's routing rules say to forward those requests to the Everserve server at 192.168.2.100.

The JMS server receives the connection request and returns a ConnectionFactory to the JMS client in the Target. The ConnectionFactory contains information that the client needs to connect back to the JMS server In this case, the client is told to connect back using the host name `http://foxtrot.widgets.com` and port 1856 because of the settings that were modified in ConnectionMgr.xml.

The client then queries the DNS server to get the IP address for the host name returned in the ConnectionFactory. The corporate DNS server returns the address 10.148.126.15, and the client opens a connection back to the JMS server, using the same firewall rules as before.

The firewall allows traffic to pass on port 1857 to allow future expansion of the community by allowing Everserve Publishers to be placed outside the firewall.

Everserve available to the Internet



This configuration is very similar to the preceding configuration. The Everserve Pub/CM server is known by the externally visible name `foxtrot.widgets.com`. There are two firewalls on the corporate network, and the user has an additional firewall at her residence.

There is a DNS server on the Internet which knows about the externally visible subdomain `foxtrot` on the `widgets.com` domain. The authoritative DNS record for this subdomain returns the IP address 192.220.116.62. The reverse, or PTR, record was configured to return the hostname `foxtrot.widgets.com` for the address 192.220.116.62.

Everserve was installed using the standard ports: 1856 for JMS, 1857 for JMS administration, and 8443 for the Everweb administrative interface.

Configuration

Firewall

The company's **external** firewall has the following rules on this connection:

Incoming

- Allow all incoming connections with a target of 192.220.116.62 and a port of 1856, and redirect them to 10.148.126.15 (the address of the firewall in front of Everserve)
- Reject all other incoming traffic.

Outgoing

- Reject all traffic

The **internal** firewall in front of Everserve has the same configuration as in the previous example:

Incoming

- Allow all incoming connections with a target of 10.148.126.15 and a port of 8443, 1856, or 1857 and redirect them to 192.168.2.100
- Reject all other incoming traffic.

Outgoing

- Reject all traffic

Configuration Files

The file *ConnectionManager.xml* is configured as in the previous example.

Corporate DNS Server

The corporate DNS server was configured to map the hostname `foxtrot.widgets.com` to the IP address 10.148.126.15 in its forward and reverse (PTR) lookup tables.

How it works

This configuration works almost exactly the same as the previous example. All of the communications start with the hostname of the target machine. The location of the target determines which DNS server it will use, either authoritative (external) or corporate (internal). If it queries an external DNS server, it will get back an external IP address, and if it queries the internal DNS server, it will get back the internal address.

The rest of the routing is the responsibility of the firewalls and NAT servers. Traffic that originates on the Internet is first routed to the company's external firewall. This firewall forwards traffic to the internal firewall in front of the Everserve server, which routes traffic on to the Everserve and JMS server.

Since all traffic originates with the Target, both firewalls can be configured to block traffic originating at the server. This offers protection to the corporate network from attacks on the Everserve server.

Note that the external firewall is configured to block traffic on port 8443. Since the internal firewall passes port 8443, administrators inside the corporate network are able to access the Everweb administrative interface. However, since the external firewall blocks port 8443, external users will be unable to access the Everweb administrative interface. Target users will only access the Everserve server on port 1856.

Troubleshooting

Symptom	Things to try
1. The Everserve service fails to start on a Windows 2000 server with a static IP address.	• Verify that the Full Computer Name in the System Properties dialog box is fully qualified with the primary DNS suffix. For example, the Full Computer name should be `foxtrot.widgets.com`, not `foxtrot`.

2. Users can't "join" a community	• Verify that the user can resolve the name of the Everserve from their DNS server. Use "nslookup *servername*".
	• Verify that the internal DNS server has the correct reverse or PTR record for the host name. Try this from a shell or DOS prompt at the user's location.
	`C> nslookup`
	`nslookup> servername`
	`nslookup> set type=PTR`
	`nslookup> IP_address`
	Verify that the name returned matches the hostname in the first query. If it doesn't match or an error is returned, the Everserve client won't be able to find the server. Update the DNS server to correct the error.
	• Verify that the firewall is set to accept traffic on port 1856 (or whatever port Everserve was configured to use) and forward that traffic to the Everserve server.

3. Users can't "ping" the Everserve server.	• Firewalls are often set up to block ICMP, or "ping" packets. To verify connectivity, use telnet instead: `C> telnet servername 1856` If the screen clears, you have a good connection. Press <return> a few times to close the connection, until you see the message "Connection to host lost.
4. Initial "join" command from a client takes a long time.	• The join command exchanges a significant amount of information between the client and server. In addition, it creates a private key for the client and exchanges public keys with the server. This process may take up to 3 minutes to complete.
5. Users are able to "join" the community from the corporate network but not from the Internet.	• Verify that the public DNS server is properly resolving the subdomain. Use the "nslookup" command to check the forward and reverse entry lookups, as in #1, above. Make sure to do this from the user's location. • DNS records may take up to 24 hours to propagate. Try using a different DNS server.