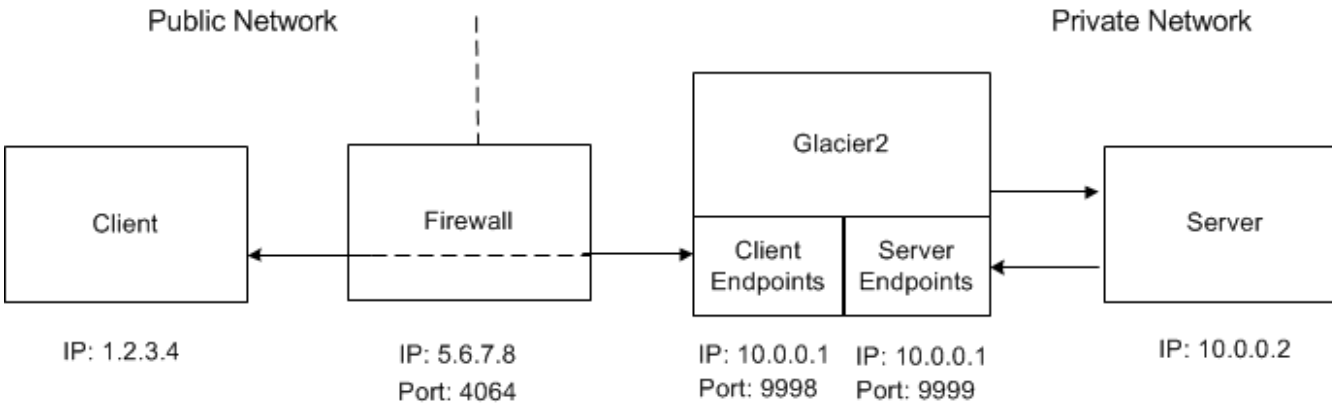
Configuring Glacier2 behind an External Firewall

The Glacier2 router requires only one external port to receive connections from clients and therefore can easily coexist with a network firewall device.

For example, consider the network shown in the following illustration:



The Glacier2 router in the example above has both of its endpoints in the private network and its host requires only one IP address, unlike the example we showed in the discussion of bidirectional connections in which the Glacier2 host straddled both networks.

We assume that the firewall has been configured to forward connections from port 4064 to the router's client endpoint at port 9998. Meanwhile, the client must be configured to use the firewall's address information in its router proxy, as shown below:

```
Ice.Default.Router=Glacier2/router:ssl -h 5.6.7.8 -p 4064
```

The Glacier2 router configuration for this example requires the following properties:

```
Glacier2.Client.Endpoints=ssl -h 10.0.0.1 -p 9998
Glacier2.Client.PublishedEndpoints=ssl -h 5.6.7.8 -p 4064
Glacier2.Server.Endpoints=tcp -h 10.0.0.1 -p 9999
```

We need to specify published endpoints for the client object adapter because the router is located behind a firewall. Without this property, any proxies that the router creates would use the endpoints specified in `Glacier2.Client.Endpoints`, but of course those endpoints are inaccessible to clients outside the firewall. The `PublishedEndpoints` property forces the Ice run time to use the given endpoints in proxies created by the client object adapter.

Note also that the server endpoint in this example includes a fixed port (`9999`), but a fixed port is not required in the server endpoint for the router to operate properly.

See Also

- Callbacks through Glacier2
- Object Adapter Endpoints
- Glacier2 Properties