Working with NATs and Firewalls

.NET Framework (current version)

The client and server of a network connection frequently do not have a direct and open path for communication. Packets are filtered, routed, analyzed, and transformed both on the endpoint machines and by intermediate machines on the network. Network address translations (NATs) and firewalls are common examples of intermediate applications that can participate in network communication.

Windows Communication Foundation (WCF) transports, and message exchange patterns (MEPs) react differently to, the presence of NATs and firewalls. This topic describes how NATs and firewalls function in common network topologies. Recommendations for specific combinations of WCF transports and MEPs are given that help make your applications more robust to NATs and firewalls on the network.

How NATs Affect Communication

NAT was created to enable several machines to share a single external IP address. A port-remapping NAT maps an internal IP address and port for a connection to an external IP address with a new port number. The new port number allows the NAT to correlate return traffic with the original communication. Many home users now have an IP address that is only privately routable and rely on a NAT to provide global routing of packets.

A NAT does not provide a security boundary. However, common NAT configurations prevent the internal machines from being directly addressed. This both protects the internal machines from some unwanted connections and makes it difficult to write server applications that must asynchronously send data back to the client. The NAT rewrites the addresses in packets to make it seem like connections are originating at the NAT machine. This causes the server to fail when it attempts to open a connection back to the client. If the server uses the client's perceived address, it fails because the client address cannot be publicly routed. If the server uses the NAT address, it fails to connect because no application is listening on that machine.

Some NATs support the configuration of forwarding rules to allow external machines to connect to a particular internal machine. The instructions for configuring forwarding rules varies among different NATs, and asking end users to change their NAT configuration is not recommended for most applications. Many end users either cannot or do not want to change their NAT configuration for a particular application.

How Firewalls Affect Communication

A *firewall* is a software or hardware device that applies rules to the traffic passing through to decide whether to allow or deny passage. You can configure firewalls to examine incoming and/or outgoing streams of traffic. The firewall provides a security boundary for the network at either the edge of the network or on the endpoint host. Business users have traditionally kept their servers behind a firewall to prevent malicious attacks. Since the introduction of the personal firewall in Windows XP SP2, the number of home users behind a firewall has greatly increased as well. This makes it likely that one or both ends of a connection have a firewall examining packets.

Firewalls vary greatly in terms of their complexity and capability for examining packets. Simple firewalls apply rules based on the source and destination addresses and ports in packets. Intelligent firewalls can also examine the contents of packets to make decisions. These firewalls come in many different configurations and are often used for specialized applications.

A common configuration for a home user firewall is to prohibit incoming connections unless an outgoing connection was made to that machine previously. A common configuration for a business user firewall is to prohibit incoming connections on

all ports except a group specifically identified. An example is a firewall that prohibits connections on all ports except for ports 80 and 443 to provide HTTP and HTTPS service. Managed firewalls exist for both home and business users that permit a trusted user or process on the machine to change the firewall configuration. Managed firewalls are more common for home users where there is no corporate policy controlling network usage.

Using Teredo

Teredo is an IPv6 transition technology that enables the direct addressability of machines behind a NAT. Teredo relies on the use of a server that can be publicly and globally routed to advertise potential connections. The Teredo server gives the application client and server a common meeting point at which they can exchange connection information. The machines then request a temporary Teredo address, and packets are tunneled through the existing network. Teredo support in WCF requires enabling IPv6 and Teredo support in the operating system. Windows XP and later operating systems support Teredo. Windows Vista and later operating systems support IPv6 by default and only require the user to enable Teredo. Windows XP SP2 and Windows Server 2003 require the user to enable both IPv6 and Teredo. For more information, see the Teredo Overview.

Choosing a Transport and Message Exchange Pattern

Selecting a transport and MEP is a three-step process:

1. Analyze the addressability of the endpoint machines. Enterprise servers commonly have direct addressability, while end users commonly have their addressability blocked by NATs. If both endpoints are behind a NAT, such as in peer-to-peer scenarios between end users, then you might need a technology such as Teredo to provide addressability.

2. Analyze the protocol and port restrictions of the endpoint machines. Enterprise servers are typically behind strong firewalls that block many ports. However, port 80 is frequently open to permit HTTP traffic, and port 443 is open to permit HTTPS traffic. End users are less likely to have port restrictions but might be behind a firewall that permits only outgoing connections. Some firewalls permit management by applications on the endpoint to selectively open connections.

3. Compute the transports and MEPs that the addressability and port restrictions of the network permit.

A common topology for client-server applications is to have clients that are behind a NAT without Teredo with an outbound-only firewall and a server that is directly addressable with a strong firewall. In this scenario, the TCP transport with a duplex MEP and an HTTP transport with a request-reply MEP work well. A common topology for peer-to-peer applications is to have both endpoints behind NATs and firewalls. In this scenario, and in scenarios where the network topology is unknown, consider the following recommendations:

- Do not use dual transports. A dual transport opens more connections, which reduces the chance of connecting successfully.

- Support establishing back channels over the originating connection. Using back channels, such as in duplex TCP, opens fewer connections, which increases the chance of connecting successfully.

- Employ a reachable service for either registering endpoints or relaying traffic. Using a globally reachable connection service, such as a Teredo server, greatly increases the chance of connecting successfully when the network topology is restrictive or unknown.

The following tables examine the one-way, request-reply, and duplex MEPs, and the standard TCP, TCP with Teredo, and standard and dual HTTP transports in WCF.

Addressability	Server Direct	Server Direct with NAT traversal	Server NAT	Server NAT with NAT traversal
Client direct	Any transport and MEP	Any transport and MEP	Not supported.	Not supported.
Client direct with NAT traversal	Any transport and MEP.	Any transport and MEP.	Not supported.	TCP with Teredo and any MEP. Windows Vista has a machine-wide configuration option to support HTTP with Teredo.
Client NAT	Any non-dual transport and MEP. Duplex MEP requires TCP transport.	Any non-dual transport and MEP. Duplex MEP requires TCP transport.	Not supported.	Not supported.
Client NAT with NAT traversal	Any non-dual transport and MEP. Duplex MEP requires TCP transport.	All but dual HTTP and any MEP. Duplex MEP requires TCP transport. Dual TCP transport requires Teredo. Windows Vista has a machine-wide configuration option to support HTTP with Teredo.	Not supported.	TCP with Teredo and any MEP. Windows Vista has a machine-wide configuration option to support HTTP with Teredo.

Firewall restrictions	Server open	Server with managed firewall	Server with HTTP-only firewall	Server with outbound-only firewall
Client Open	Any transport and MEP.	Any transport and MEP.	Any HTTP transport and MEP.	Not supported.
Client with managed firewall	Any non-dual transport and MEP. Duplex MEP requires TCP transport.	Any non-dual transport and MEP. Duplex MEP requires TCP transport.	Any HTTP transport and MEP.	Not supported.
Client with HTTP-only firewall	Any HTTP transport and MEP.	Any HTTP transport and MEP.	Any HTTP transport and MEP.	Not supported.

Client with outbound-only firewall	Any non-dual transport and MEP. Duplex MEP requires TCP transport.	Any non-dual transport and MEP. Duplex MEP requires TCP transport.	Any HTTP transport and any non-duplex MEP.	Not supported.

;