MQSeries and Firewalls

Paul F. Sehorne
IBM Certified Solution Expert - MQSeries
IBM Dallas Systems Center

General

MQSeries behaves just like many other TCPIP applications; e.g. HTTP. The ’caller’ selects a port at random. The ’callee’ listens on a fixed port.

- The sending MCA selects a port at random from available ports.
- The receiving MCA responds to the sending MCA by "initiating" a new conversation using local port 1414 and the remote port selected at random by the sending MCA.
- Rules must allow both the sending MCA and the receiving MCA to initiate conversations.

Sockets Conversations

- Each sockets conversation is identified by a unique combination of source and target ip address and port number
  - x.x.x.x(aaaa) y.y.y.y(bbbb)
- Only one conversation can exist on a network with a specific signature

Firewalls restrict conversations

Firewall products use the four objects and rules to

- uniquely identify a conversation
- allow or disallow specific hosts
- allow or disallow specific ports
- restrict who can initiate a conversation.

outside host	outside port	inside host	inside port	initiator
x.x.x.x	aaaa	y.y.y.y	bbbb	both,outside inside

All of the rules in this document allow conversations. Rules can also disallow conversations.

Wildcards may be used in rules

outside host	outside port	inside host	inside port	initiator
*	<1024	*	*	inside

This rule allows any inside host to initiate a conversation from any port to any outside host but only to ports less than 1024 (i.e., well known ports). This type of rule might be pre-configured in a firewall product.

MQSeries observed behavior - sender channel

- Sender channel selects at random a port number to use
  - greater than 1023
  - not already in use
  - not 1414 (already in use)

The term "observed behavior" is significant here. The explanations in this document were arrived at by observing behavior not by analyzing source code.

Example rule:
MQSeries rule #1

outside host	outside port	inside host	inside port	initiator
x.x.x.101	>1023	y.y.y.1	1414	outside

In this rule host x.x.x.101 outside the firewall may initiate a conversation from any port greater than 1023, but only to inside host number one in subnet y.y.y.0, and only to port number 1414.

This rule would allow the outside sender channel to request the initiation of a conversation to the queue manager at y.y.y.1 that is listening on port 1414. No conversation could be started with a queue manager at inside host y.y.y.1 that is listening on a port other than 1414.

To simplify this explanation, not shown here is the subnet mask that the firewall rule would use to identify both inside and outside hosts.

MQSeries observed behavior - receiver channel

- Receiver channel responds to the request from the sender channel by "initiating" a new conversation, i.e. it calls back
  - using local port 1414
  - to the sender channel’s randomly selected port
- The original conversation is only used to request that the receiver channel call back ("initiate").
- This requires a new rule that will allow a conversation to be "initiated" from inside the firewall using port 1414 to any outside port >1023 at host x.x.x.101

MQSeries rule #2

outside host	outside port	inside host	inside port	initiator
x.x.x.101	>1023	y.y.y.1	1414	inside

This rule allows an inside receiver channel to respond to a request from an outside sender channel. The receiver uses port number 1414 and communicates to the port number at the sender that was randomly selected.

MQSeries Rules #1 and #2

The two rules required to allow an outside sender channel to initiate a conversation with an inside receiver, and for the inside receiver to respond.

outside host	outside port	inside host	inside port	initiator
x.x.x.101	>1023	y.y.y.1	1414	outside
x.x.x.101	>1023	y.y.y.1	1414	inside

Some firewall products may allow these to be combined into one rule where "initiator" is "both". The firewall product used to do this research required two separate rules.

MQSeries Rules #3 and #4

Two similar rules are needed to allow an inside sender channel to start a conversation with an outside receiver.

outside host	outside port	inside host	inside port	initiator
x.x.x.101	1414	y.y.y.1	>1023	outside
x.x.x.101	1414	y.y.y.1	>1023	inside

Summary: Four Rules Are Needed

outside host	outside port	inside host	inside port	initiator
x.x.x.101	>1023	y.y.y.1	1414	outside
x.x.x.101	>1023	y.y.y.1	1414	inside
x.x.x.101	1414	y.y.y.1	>1023	outside
x.x.x.101	1414	y.y.y.1	>1023	inside

Using wildcards to combine the two rules that allow conversations to be initiated from inside hosts

outside host	outside port	inside host	inside port	initiator
x.x.x.101	>1023	y.y.y.1	1414	outside
x.x.x.101	1414	y.y.y.1	>1023	outside
*	*	*	*	inside

These rules would allow host x.x.x.101 outside the firewall to communicate with the MCA at inside host y.y.y.1. Conversations could be initiated from outside the firewall from any port greater than 1023 only to host y.y.y.1 on any port >1023.

On the other hand, any inside host using any port could initiate conversations to any outside host on any port.

Initiators and responders need different rules

- The rules that work for a receiver channel "should" work for any listening MCA; i.e. receiver, server.
- The rules that work for a sender channel "should" work for any requesting MCA; i.e. sender, requester, clntconn.
- Not all of these combinations have been tested; e.g. requester/sender.
- The combinations that have been tested are:
  - sender/receiver
  - clntconn/svrconn

Proxy Firewalls

- Although this document has not covered how a proxy firewall could be used to tighten security, with the information contained herein and knowledge of your proxy firewall product, it should be easy to establish any desired level of security by configuring sender channels to communicate only via specific ports through the proxy firewall.