CONNECTING TO A REMOTE HOST USING DMZ GATEWAY AS A PROXY

OVERVIEW

Most enterprise deployments of EFT Server place DMZ Gateway in the DMZ and EFT Server inside the network, with all inbound connections brokered by the DMZ Gateway. Occasionally it may be necessary for EFT Server's Event rules or Advanced Workflow Engine to connect to a remote host that is outside the network and DMZ. Because EFT Server resides within the network (as opposed to in the DMZ), it may be considered a security risk to connect directly from EFT to the remote host, and because the DMZ Gateway is already brokering inbound connections, it makes perfect sense to be able to route OUTBOUND connections though the DMZ Gateway, using it as a forward proxy. Fortunately, it is possible to do so both from EFT Server's Event rules and from within the Advanced Workflow Engine, as the DMZ Gateway is configured to act as a Socks5 proxy.

FIGURE 1 - SFTP TO REMOTE HOST VIA DMZ GATEWAY

PREREQUISITES

1. A copy of EFT Server Enterprise and the Advanced Workflow Engine (AWE) module
2. DMZ Gateway running on a separate host
3. A destination FTP/S or SFTP host, or another EFT Server somewhere in your network
4. Logon credentials for the destination server
5. Administrator access to EFT Server

EFT SERVER-INITIATED CONNECTIONS

Below are screenshots and instructions to guide you through the implementation of this technique.

1. Create an account on the remote (destination) host and note the host address, port, and login credentials. For this example we will use 74.125.227.180 over port 22 (SFTP), user:pass = roslin:test

2. In EFT Server, verify the DMZ Gateway is enabled and make note of the DMZ Gateway host address and port. For this example we will use 192.168.101.119 over port 44500
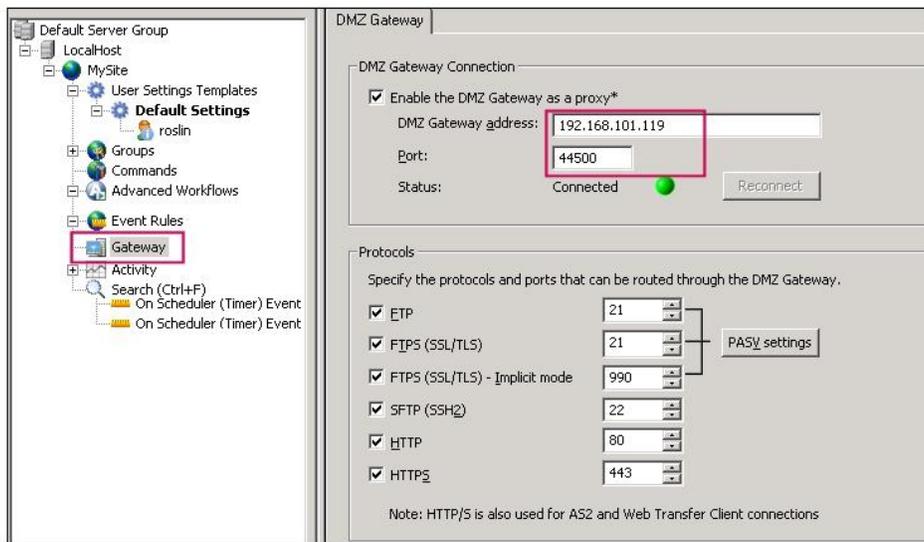
FIGURE 2 - EFT DMZ GATEWAY CONFIGURATION

3. Create a new rule in EFT Server and add a Copy/Move (offload) action, or modify an existing rule by selecting the Copy/Move action to bring up the Offload Wizard. (Refer to the *EFT Server User Guide* for instructions on how to create Event rules and Copy/Move actions if necessary.)
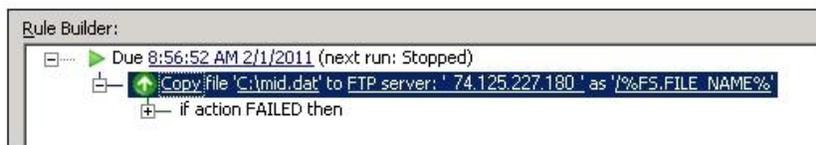
FIGURE 3 - EVENT RULE ACTION BUILDER

4. On the first page of the offload wizard, specify or verify the remote host (destination) address, login credentials, and protocol type.

5. Click Proxy, and then select the **Use proxy settings** check box and **Use EFT Server's DMZ Gateway as the proxy**. Click **OK** then click **Next** in the wizard, completing the standard source/destination file information.
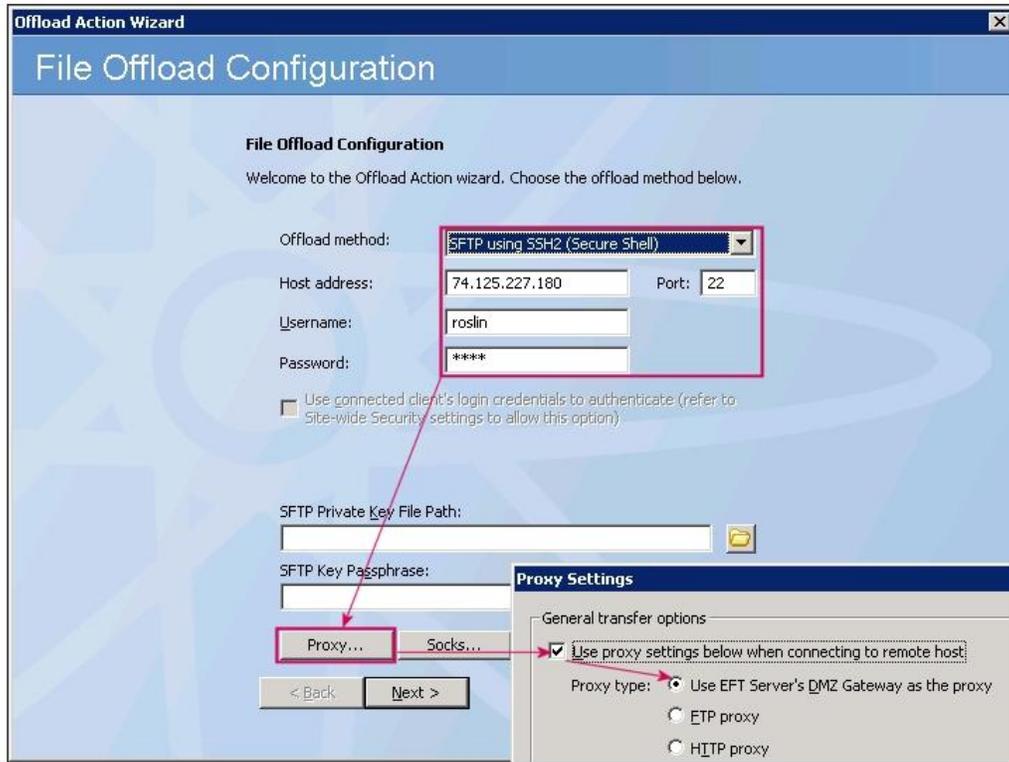
FIGURE 4 - COPY/MOVE ACTION WIZARD

6. The next time the rule is executed, EFT Server will route the connection through the DMZ Gateway residing at 192.168.101.119 over port 44500, en route to the destination address of 74.125.227.180:22

You can see the connection occur by observing the DMZ Gateway's real time logs:

FIGURE 5 - DMZ GATEWAY STATS VIEW

AWE-INITIATED CONNECTIONS

You can use the Advanced Workflow Engine's FTP/S and SFTP client actions to broker connections the DMZ Gateway by using AWE's Socks5 proxy option. (EFT 6.2 (AWE 7) only supports FTP/S through Socks5. EFT 6.3 (AWE 8) supports both FTP/S and SFTP through Socks5.)

1. Create a new Advanced Workflow or modify an existing workflow. (Refer to the *EFT Server User Guide* for instructions on how to create Event rules and Copy/Move actions if necessary.)
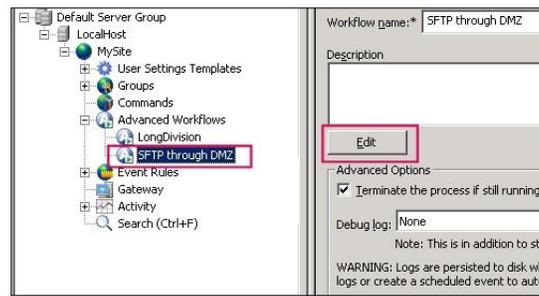
FIGURE 6 - MODIFY WORKFLOW

2. Inside the workflow editor, create a new Network -> FTP task (action) or modify the final destination host information, the desired protocols, and DMZ Gateway host address and port as Socks5 proxy parameters:
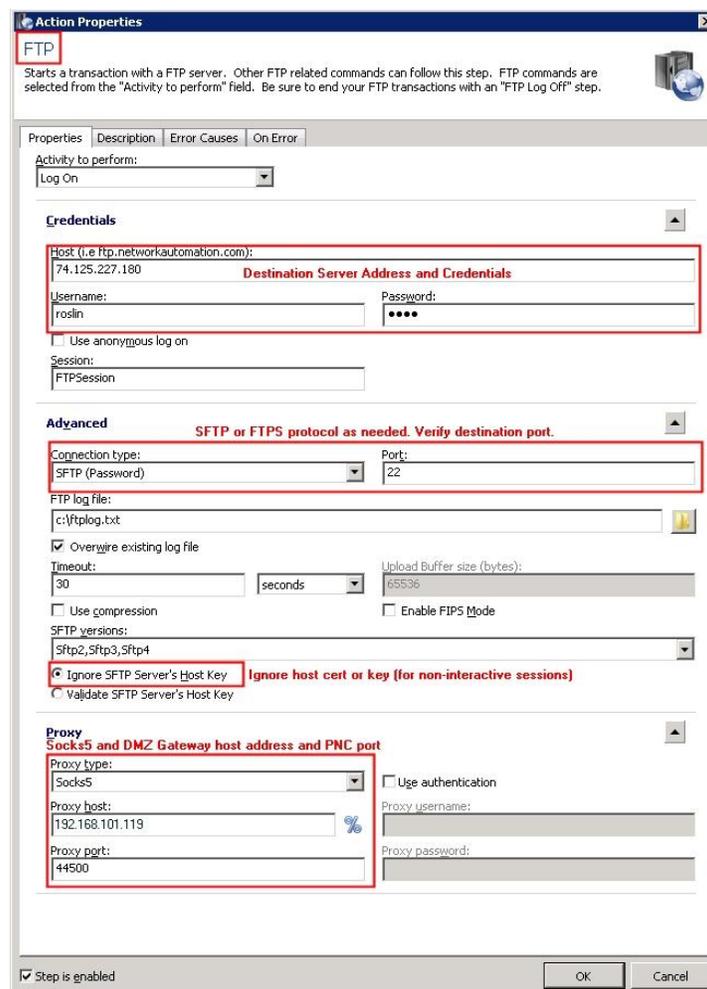
FIGURE 7 - AWE S/FTP/S SETTINGS

3. Save your task and test it. Check AWE, DMZ Gateway, or remote host logs to troubleshoot if necessary.