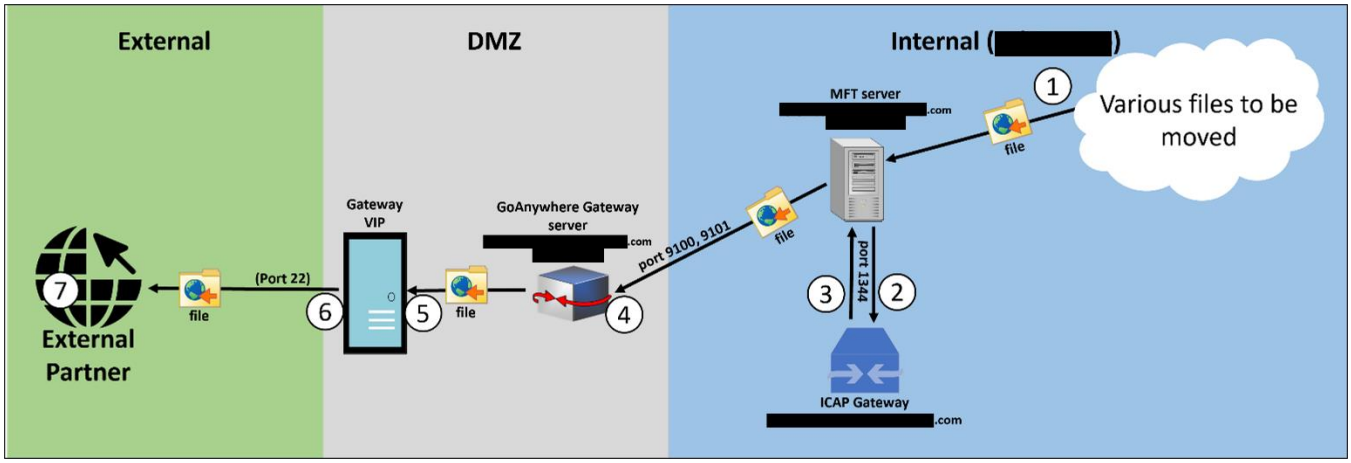
Workflow Automation Network Architecture

File Transfers

This section contains information and diagrams representing the *[REDACTED]* production environment and flow for the most common day-to-day file transfer scenarios.

Outbound

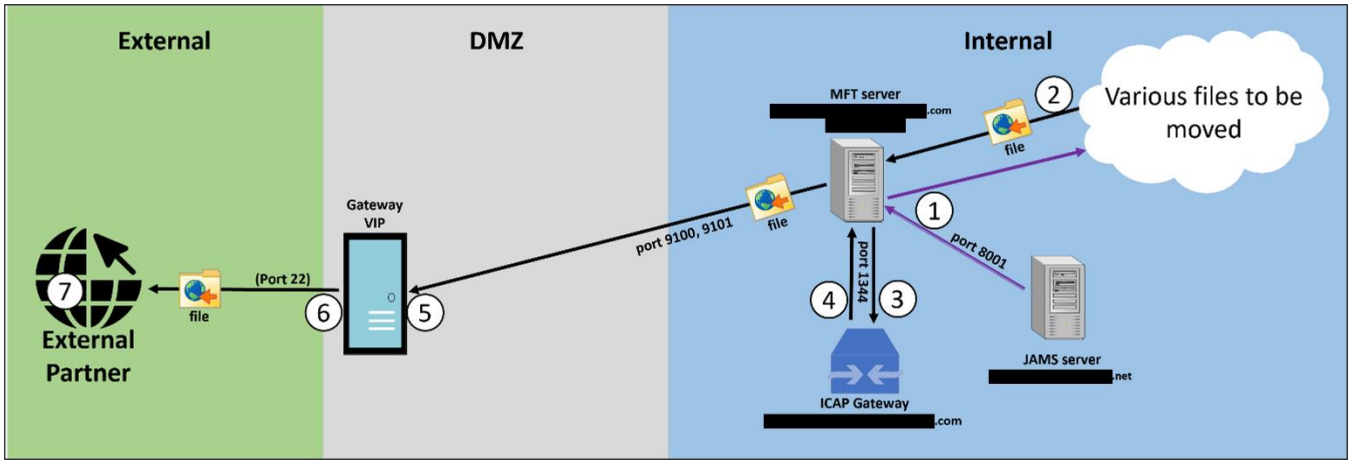
Scenario 1: An external partner pulls a file from [REDACTED]



The following steps explain the process for Scenario 1:

1. As a result of an external partner requesting to pull a file from *[REDACTED]* using SFTP, the requested file is moved from its current location at *[REDACTED]* and routed to the *MFT* server ([REDACTED].com) for transport via SFTP.
2. The *MFT* server routes the file to the ICAP Gateway ([REDACTED].com) for security validation.
3. The ICAP Gateway moves the validated file back to the *MFT* server.
4. The *MFT* server moves the file via SFTP to the *GoAnywhere* Gateway server ([REDACTED].com) in the DMZ.
5. The *GoAnywhere* Gateway server moves the file via SFTP to the Gateway VIP in the DMZ.
6. The Gateway VIP sends the file outside of the DMZ routed to the external partner.
7. The intended external partner receives the file.

Scenario 2: [REDACTED] pushes a file to an external partner

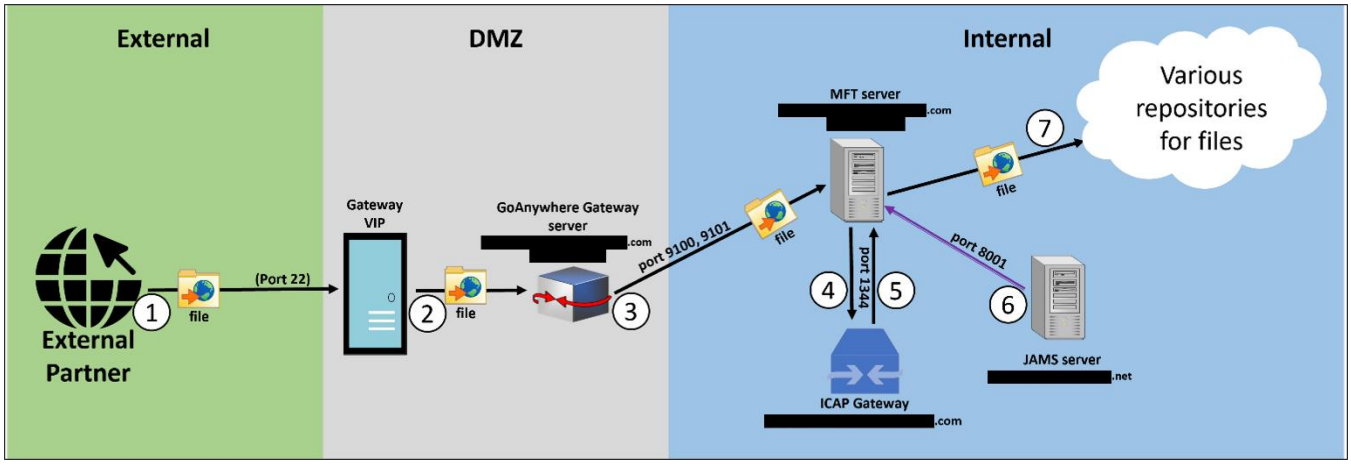


The following steps explain the process for Scenario 2:

1. *JAMS* ([REDACTED].com) triggers a job which instructs the *MFT* Server ([REDACTED].com) to move an outbound file from any one of several internal repositories to an external partner.
2. The *MFT* server locates the internal file and begins moving the file via SFTP protocol.
3. The *MFT* server routes the file to the ICAP Gateway ([REDACTED].com) for security validation.
4. The ICAP Gateway moves the validated file back to the *MFT* server.
5. The *MFT* server moves the file via SFTP to the Gateway VIP in the DMZ.
6. The Gateway VIP sends the file to the external destination.
7. The intended external partner receives the file.

Inbound

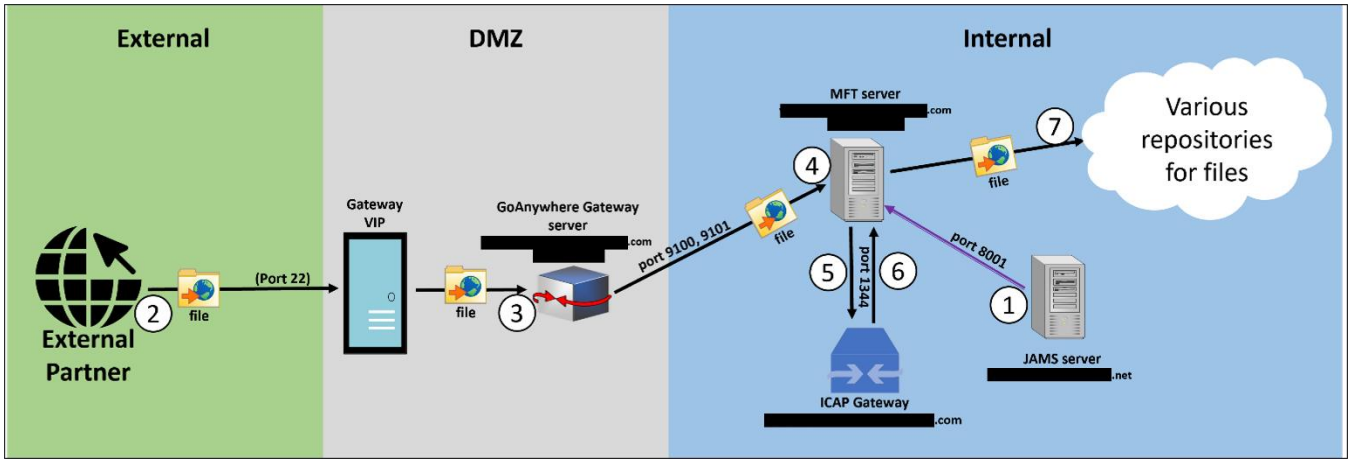
Scenario 3: An external partner pushes a file to [REDACTED]



The following steps explain the process for Scenario 3:

1. An external partner routes a file to the DMZ Gateway VIP via SFTP.
2. The Gateway VIP sends the file through the *GoAnywhere* Gateway server ([REDACTED].com).
3. The *GoAnywhere* Gateway server sends the file out of the DMZ to the *MFT* server ([REDACTED].com) at *[REDACTED]*.
4. The *MFT* server routes the file through the ICAP Gateway ([REDACTED].com) for security validation.
5. The ICAP Gateway validates the file and sends it back to the *MFT* server.
6. The *JAMS* server ([REDACTED].com) kicks off a scheduled job instructing the *MFT* Gateway to send the file to its intended repository destination.
7. The *MFT* Gateway sends the file to its intended destination within *[REDACTED]*.

Scenario 4: [REDACTED] pulls a file from an external partner



The following steps explain the process for Scenario 4:

1. The *JAMS* server kicks off a scheduled job instructing the *MFT* server to pull a particular file from a particular external partner.
2. Since *[REDACTED]* is whitelisted, the external partner allows the specified file to be routed to the Gateway VIP in the DMZ via SFTP.
3. The Gateway VIP routes the file through the *GoAnywhere* Gateway in the DMZ.
4. The *GoAnywhere* Gateway routes the file out of the DMZ and to the *MFT* server at *[REDACTED]*.
5. The *MFT* server sends the file to the ICAP server for security validation.
6. The ICAP Gateway validates the file and sends it back to the *MFT* server.
7. The *MFT* server sends the file to its intended repository destination at *[REDACTED]*.