DMZ GATEWAY® v3.3

User Guide

globalscape™

GlobalSCAPE, Inc. (GSB)

Address:	4500 Lockhill-Selma Road, Suite 150 San Antonio, TX (USA) 78249
Sales:	(210) 308-8267
Sales (Toll Free):	(800) 290-5054
Technical Support:	(210) 366-3993

Web Support: http://www.globalscape.com/support/

Last Updated: December 7, 2012

Table of Contents

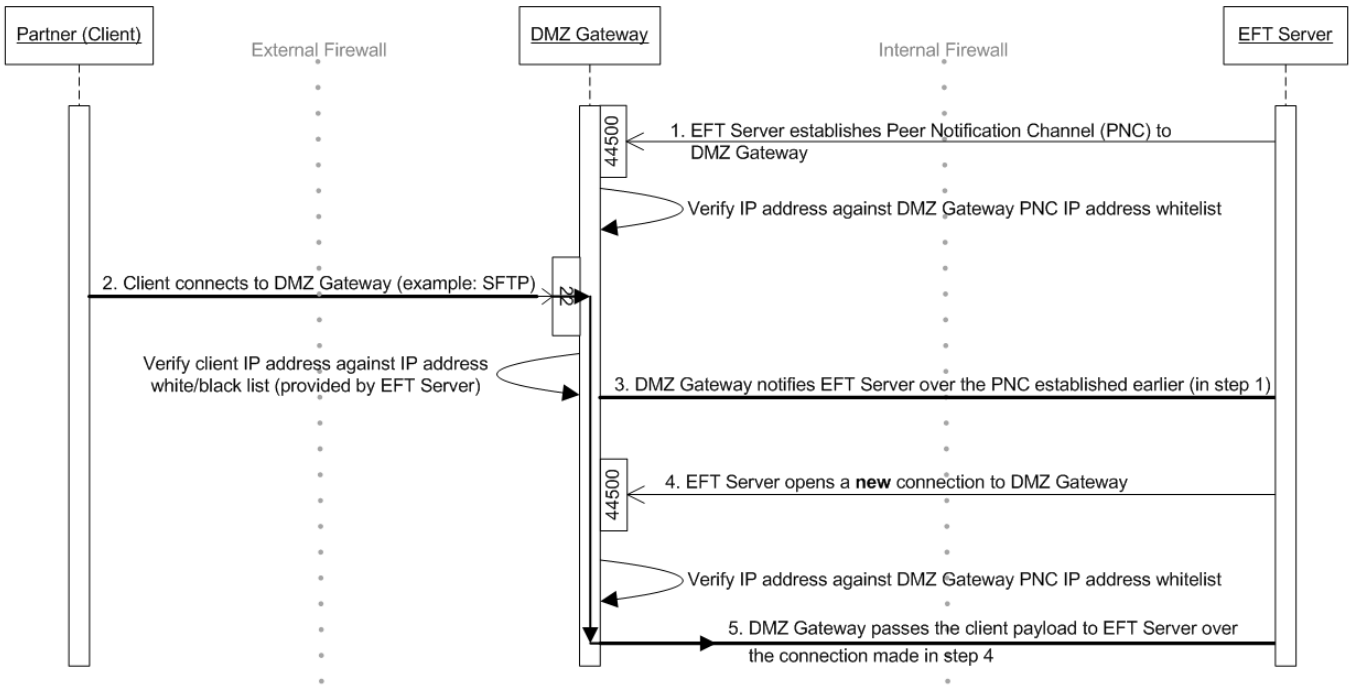
Introduction to DMZ Gateway® Server

DMZ Gateway® server is designed to reside in the demilitarized zone and provide secure communication with a server behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ, and with no sensitive data stored in the DMZ, even temporarily. Currently, DMZ Gateway is supported with Globalscape's EFT Server and Mail Express. DMZ Gateway supports connections to the servers using Profiles on page 32. Depending on the license purchased, you can have up to 15 Profiles (unique IP address:port connections).

How Does It Work?

1. When the connected server's service is started, it will establish (and maintain) an outbound connection to the DMZ Gateway. This proprietary, non-encrypted connection is called the Peer Notification Channel (PNC). The server and DMZ Gateway use the PNC to setup subsequent communications between the server and incoming client connections.
2. When a client (web browser, FTP client, etc.) connects to DMZ Gateway on a pre-approved port (21, 22, 80 443, etc.), DMZ Gateway will cross reference the client's IP with the IP access list (provided by the server over the PNC) before proceeding any further. (Mail Express currently only support HTTPS and does not use an IP ban/access list, as EFT Server does.
3. If the IP is accepted, DMZ Gateway will notify the server over the PNC of the new client connection, providing data such as the client's IP address and the port connected to.
4. The server will subsequently create a new outbound connection to the DMZ Gateway to the same port that is being used by the PNC for associating with the client connection made in step 2.
5. DMZ Gateway will then proceed to read the inbound payload data from the client and send the payload data along to the server for processing. DMZ Gateway will also read any outbound data communications from the server and send it along to the client.

The graphic below describes the flow in EFT Server (similar in Mail Express):



Technical FAQ

Does DMZ Gateway modify the client's packets?

DMZ Gateway effectively terminates the client's TCP/IP session at the DMZ Gateway. The client data contained within the payload of the TCP/IP packet is transmitted to the server over the independently established TCP/IP connection between the server and DMZ Gateway. No modifications are required or performed on the actual payload data, but rather the payload is sent as is to the server. Thus, if the client is using HTTPS, then the HTTPS payload is streamed on through to the server. Unlike a network hardware bridge/router device, the DMZ Gateway does not "pass through" modified packets by changing the TCP/IP or frame layer headers. Instead, the DMZ Gateway reads in a buffer full of data from the client TCP/IP stream (~64KB) and then sends that data over the TCP/IP socket established earlier by the server (see step 4 above). The result is a set of completely different TCP/IP packets with different source and destination locations but containing the original payload. Keep in mind that the original (source) location (IP address) is known by the server as it was provided to the server earlier by DMZ Gateway (see step 3 above).

Does DMZ Gateway forward client connections to the server?

The DMZ Gateway does not forward client connections. Only the payload (data) is forwarded or passed through to the server.

How do the server's listening ports affect DMZ Gateway?

EFT Server allows you to define two groups or sets of listening ports. When used with DMZ Gateway, the external listening ports (DMZ Gateway Internet facing) are specified in EFT Server's administration interface on the DMZ Gateway tab on page 47. EFT Server's second set of listening ports, defined on the Site's Connections tab, are ONLY used for establishing internal listening ports (server-network facing) for each supported (and enabled) protocol. These sets of ports can be the same or different (even for the same protocol). When DMZ Gateway is NOT being used (i.e., the server is residing in the DMZ or is being used for internal, network-facing transactions), then only a single set of ports is used, defined on the Site's **Connections** tab, for all incoming connections to EFT Server.

Mail Express only has one server port and one client HTTPS port. They are defined on the DMZ Gateway settings page on page 49 in the Mail Express Administration portal. When DMZ Gateway is not being used, Mail Express will only listen to the ip:port bindings defined on its General Settings page in the Administration portal.

How is the PNC created and maintained?

Once configured to work with DMZ Gateway, the server (when running) will always attempt to initiate, maintain, and, if necessary, reconnect to DMZ Gateway's PNC port. No further administrative action is required in the server to establish or maintain communication after the initial setup. From DMZ Gateway's perspective, if the PNC channel is broken, DMZ Gateway will refuse new (and existing) client connections until the server re-establishes a connection.

The server will "ping" the DMZ Gateway every 5 minutes. If a reply is not received within 10 seconds, the server considers the connection lost, severs the current connection, and then attempts to reconnect. DMZ Gateway also maintains its own awareness (ping/pong) of whether the server is connected. Every 30 seconds, DMZ Gateway determines whether it has received a pong message from the server since the last ping. If it has, it will ping again; if not, it drops the connection. This test allows it to free up ports if the server is not available (i.e., no longer responds to ping) and for error reporting. (Refer to the Knowledge Base article "How do EFT Server and DMZ Gateway Server communicate with each other?" for information about changing these defaults in EFT Server 6.2 and later and DMZ Gateway 3.0 and later.)

Is the PNC secure?

The PNC between the server and DMZ Gateway is not encrypted; however, the external client's encrypted session will be streamed all the way through to the server, so only the intercommunications between the server and the DMZ Gateway are in the clear, not the client session (assuming they used a secure protocol such as SFTP or HTTPS).

But won't an insecure PNC be vulnerable to a man-in-the-middle attack?

In order to usurp the PNC connection, the attacker would need full control over the internal systems on which the server is running. This access would indicate a far greater threat to Confidentiality, Integrity, and Availability (CIA) already in place in your network. Keep in mind that the internal firewall should be configured to allow only outbound connections from the server to DMZ Gateway via the PNC port. If configured as such, then the ability to usurp the control connection doesn't really gain the attacker much of an edge. Even if a connection were seized, the attacker would need to perform several other non-trivial steps, such as spoofing the server's IP address*, reverse engineering the protocol, opening ports on the firewall, altering the routing table, etc.

*DMZ Gateway provides an optional whitelist for IP addresses that are allowed to connect to the PNC port.

Isn't DMZ Gateway just giving users a way to bypass the firewall without providing any security functionality or filtering?

The DMZ Gateway is not designed to replace firewalls or content-inspection devices. The DMZ Gateway's main purpose is to allow network administrators to minimize the exposure surface area by allowing you to further lock down the internal firewall such that only outbound connections are needed, thus eliminating the need for inbound connections through your internal firewall to your directory server (for user authentication) or SQL/Oracle server (for transaction auditing). Furthermore, it eliminates the need to store file data in the DMZ. Essentially DMZ Gateway limits the attack vector to the server as opposed to multiple other internal servers. As far as filtering is concerned, it is important to note that DMZ Gateway does not replace any other sort of filtering mechanism, such as firewalls, web application firewalls, content inspection devices, and so on. DMZ Gateway is intended to work with and extend existing security mechanisms.

So then, any vulnerability in the server is essentially exposed to the Internet?

Assuming vulnerabilities exist then yes, those would be exposed to the Internet; however, the attack vector would be limited to attacks that could be accomplished over the network protocols that are proxied through the DMZ, as there would be no means for the attacker to establish inbound connections to the server directly, because of the server <> DMZ Gateway architecture.

What about Denial of Service attacks? Wouldn't it be trivial to pump traffic all the way through the DMZ to where EFT Server resides?

EFT Server is a file transfer server. It is meant to handle anything you can throw at it over the various listeners. EFT Server includes a number of DoS and flood-prevention mechanisms to mitigate these sorts of attacks. This would be the same if you stood up EFT Server (or any other FTP server) in the DMZ and terminated connections there. If EFT Server designates one or more IP addresses as needing to be blocked, it will add those IP addresses to its own internal IP Access Rules list and communicate that list to DMZ Gateway. DMZ Gateway will subsequently block all external clients with blacklisted IP addresses on the access list.

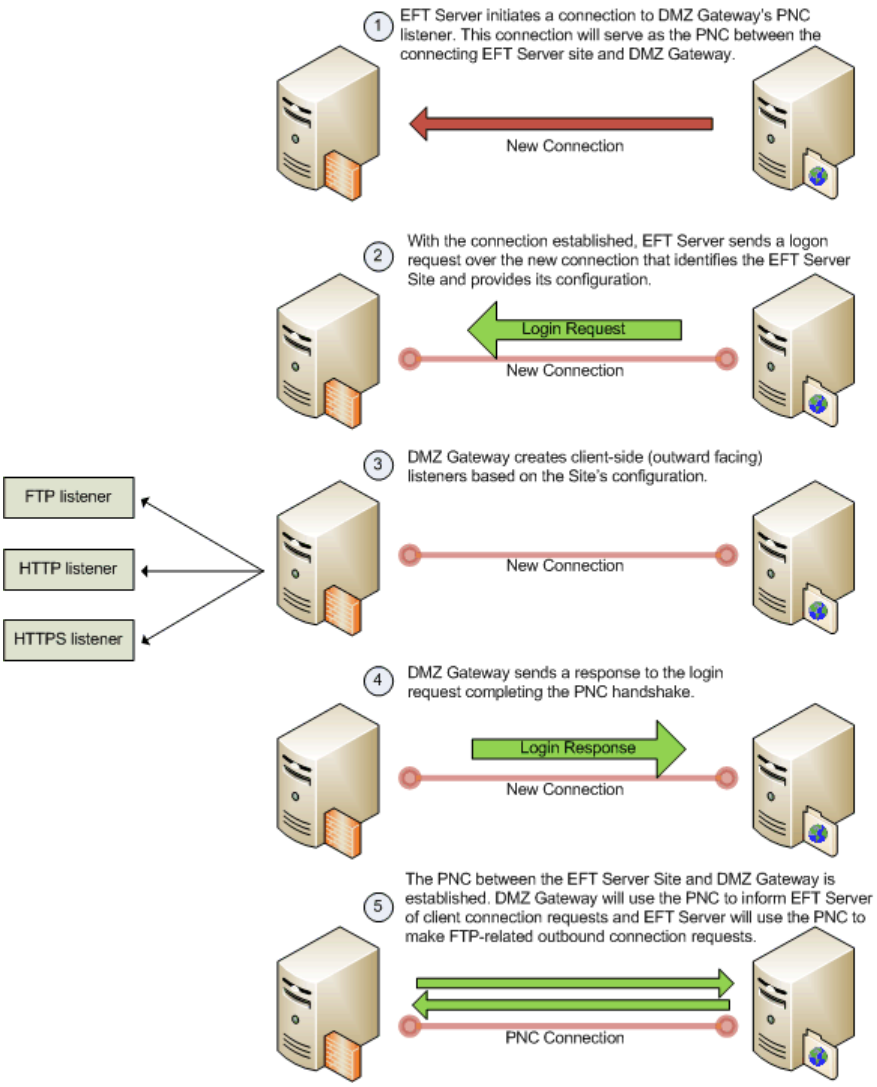
If there is a change to EFT Server's IP access rules, are the changes communicated immediately to the DMZ Gateway when those changes are applied?

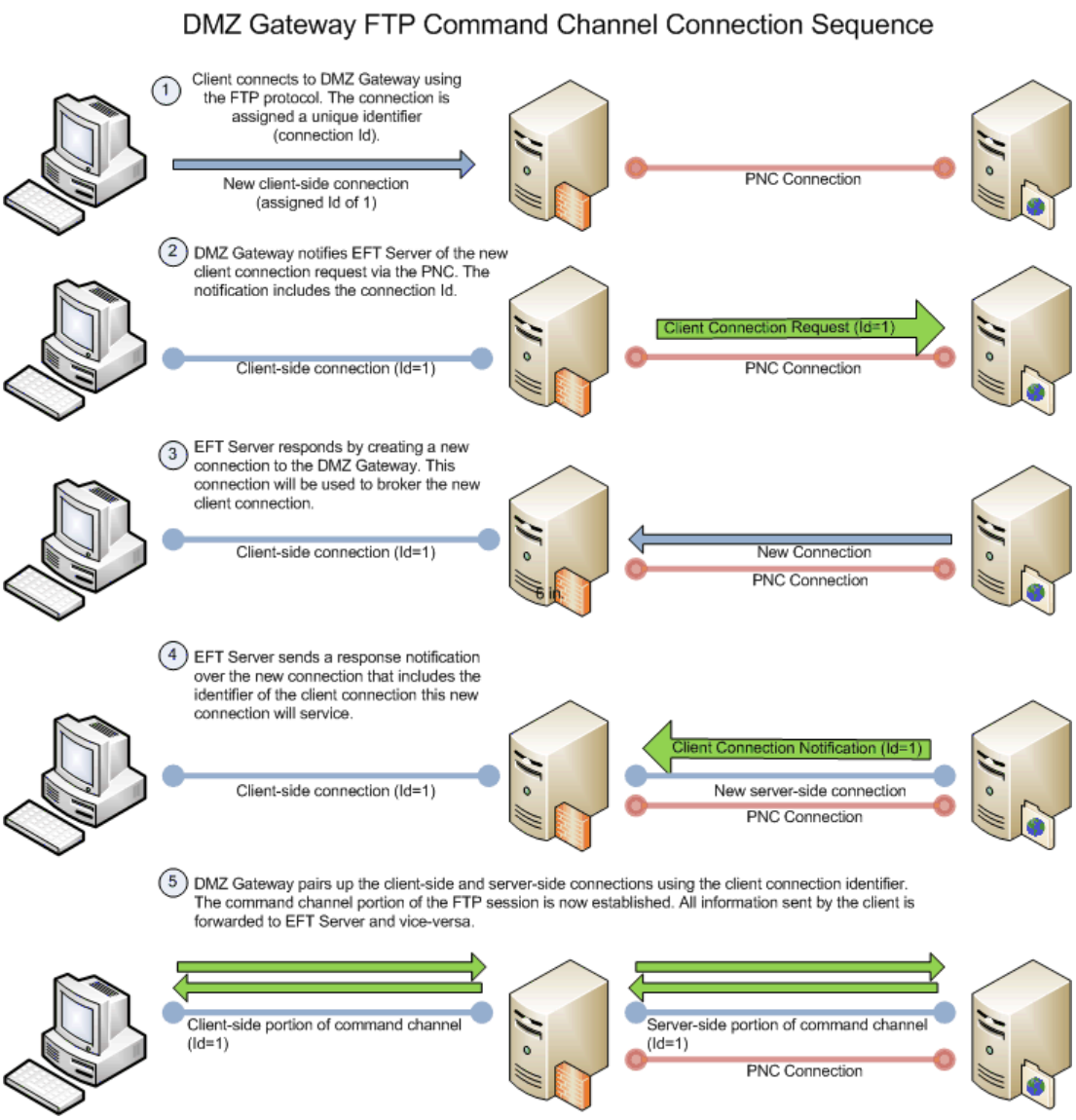
Yes, IP address access policy changes (whether manually initiated or as a byproduct of an auto-ban) are automatically propagated to the DMZ Gateway (v3.0 and later). (This does not apply to Mail Express.)

DMZ Gateway Initialization and Connection Diagrams

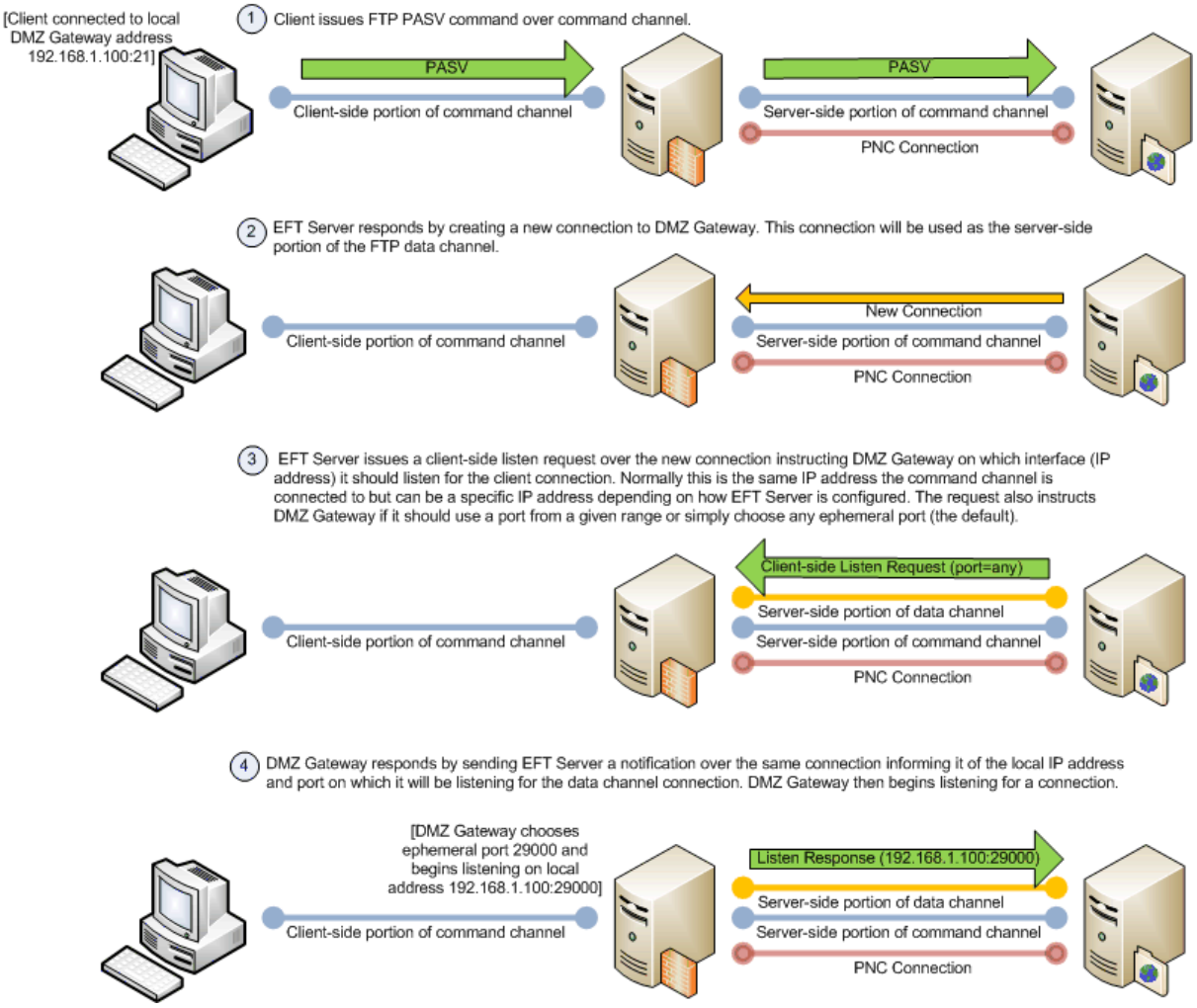
The diagrams below illustrate the initialization and connection sequences for DMZ Gateway and EFT Server™ communication.

DMZ Gateway Peer Notification Channel (PNC) Initialization Sequence




DMZ Gateway FTP Command Channel Connection Sequence
1
Client connects to DMZ Gateway using the FTP protocol. The connection is assigned a unique identifier (connection Id).
New client-side connection (assigned Id of 1)
PNC Connection
2
DMZ Gateway notifies EFT Server of the new client connection request via the PNC. The notification includes the connection Id.
Client-side connection (Id=1)
Client Connection Request (Id=1)
PNC Connection
3
EFT Server responds by creating a new connection to the DMZ Gateway. This connection will be used to broker the new client connection.
Client-side connection (Id=1)
New Connection
PNC Connection
4
EFT Server sends a response notification over the new connection that includes the identifier of the client connection this new connection will service.
Client-side connection (Id=1)
Client Connection Notification (Id=1)
New server-side connection
PNC Connection
5
DMZ Gateway pairs up the client-side and server-side connections using the client connection identifier. The command channel portion of the FTP session is now established. All information sent by the client is forwarded to EFT Server and vice-versa.
Client-side portion of command channel (Id=1)
Server-side portion of command channel (Id=1)
PNC Connection

DMZ Gateway FTP Passive Mode (PASV) Connection Sequence



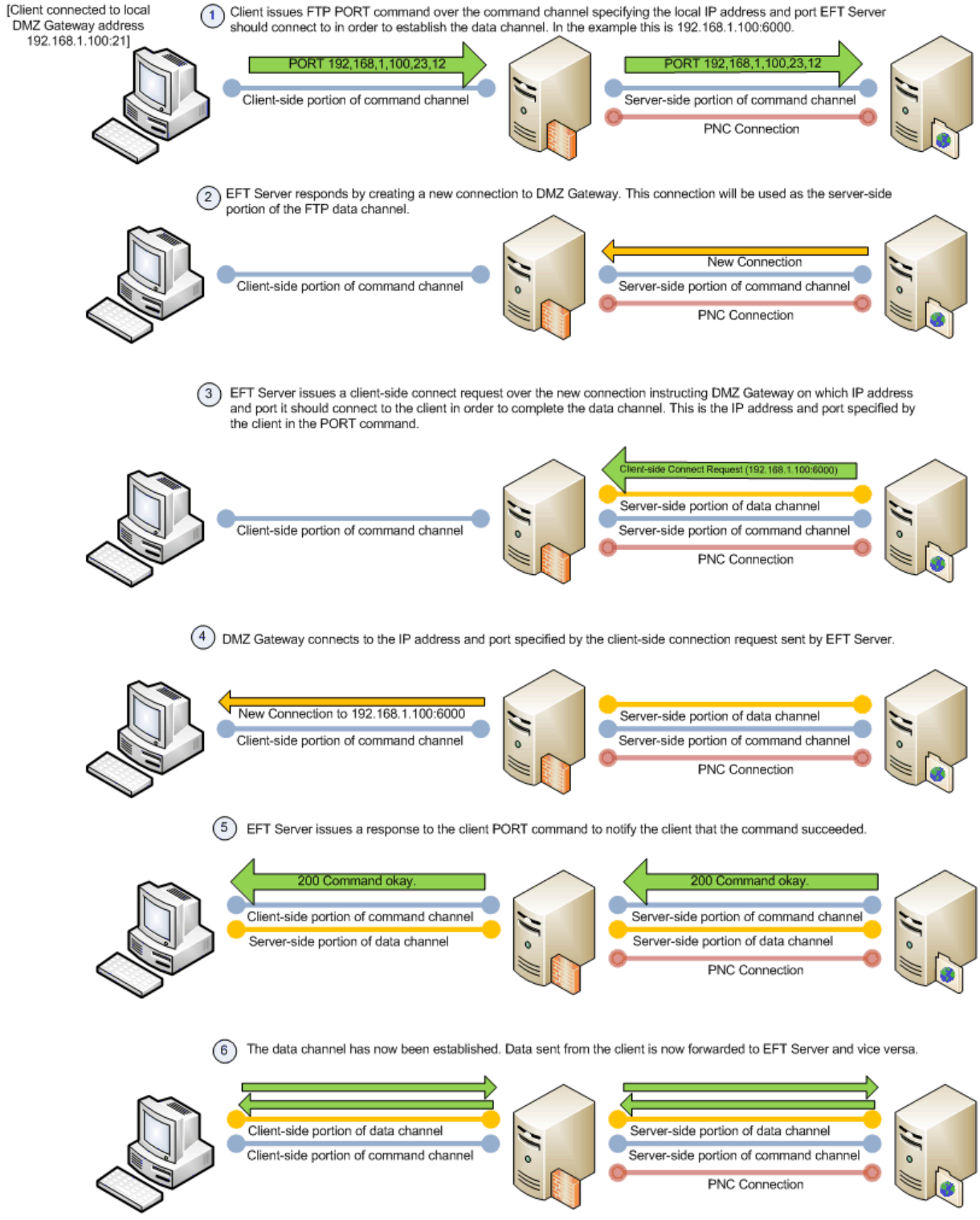
5 EFT Server responds to the client PASV command over the command channel. The response includes the IP address and port to which the client should connect in order to establish the data channel.

6 Client initiates a new connection to DMZ Gateway based on the PASV command response.

7 DMZ Gateway notifies EFT Server that it has accepted the client connection using the connection established for the data channel earlier.

8 The data channel has now been established. Data sent from the client is now forwarded to EFT Server and vice versa.

DMZ Gateway FTP Active Mode (PORT) Connection Sequence



What's New in DMZ Gateway®?

Changes in version 3.3 of DMZ Gateway include:

- Added support for IPv6 addressing when operating with Mail Express Server version 3.3 and later
- Added support for Unicode strings in the log files and XML-based configuration files
- Added support for Unicode strings in communications with EFT Server 6.5 and later
- Changed installer so that it now ensures the DMZ Gateway administration interface is not running prior to making modifications
- Fixed an issue that prevented binding to interfaces if IPv4 or IPv6 support was disabled in the operating system
- Fixed minor user interface issues in the DMZ Gateway administration interface
- Upgraded the embedded Java Runtime Environment to version 1.7.0_09.

Installing DMZ Gateway

The topics in this section provide instructions for installing DMZ Gateway.

System Requirements for DMZ Gateway v3

The Globalscape Quality Assurance team tests our products with a variety of operating systems, software, and hardware. It is possible for DMZ Gateway to function with other operating systems, software, and hardware, but is only tested and approved for use with the following:

- Accepts incoming connections from EFT Server Enterprise v6.2 and later, and EFT Server 6.2 and later. (Versions prior to v6.2 require DMZ Gateway v2.)
- Accepts incoming connections from Mail Express Server v3 and later
- Officially supported operating systems:
    - Windows Server 2003 R2 32-bit and 64-bit (IPv6 is not supported)
    - Windows Server 2008 R2 (Standard, Enterprise, and Datacenter editions)
    - Windows Server 2012
    - Red Hat Enterprise Linux release 6.3
    - SuSE Linux Enterprise Server release 11 SP2
    - Ubuntu 12.04 LTS
    - Solaris 11

    *"Internet Protocol Version 4 (TCP/IPv4)" must be installed on the operating system. If you are using "Internet Protocol Version 6 (TCP/IPv6)," "Internet Protocol Version 4 (TCP/IPv4)" may be disabled instead of uninstalled. (In the **Local Area Connection Properties** dialog box, clear the check box next to "Internet Protocol Version 4 (TCP/IPv4)".) Alternatively, you can have them both enabled at the same time.*
- x86-compatible processor (Itanium 64-bit processors are not supported)
- 1GB memory
- 1024x768 resolution or higher display (headless computer supported on non-Windows systems)
- Remote administration must be available.

- On Solaris and Linux-based systems, the administration interface will operate locally; therefore, if running on a headless operating system, you must:
    - Export the display to a remote X-Server to access the user interface.
    - Make available on the DMZ Gateway computer the subset of X11 libraries necessary for exporting the display.
    - Properly configure a remote X11 server.
    - Alternatively, the DMZ Gateway Server may be manually configured without the use of the administration interface.

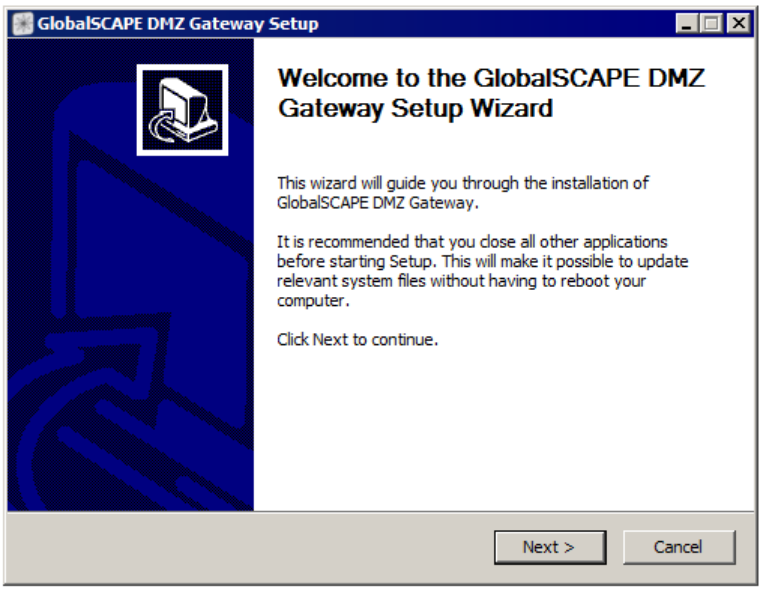
Installing DMZ Gateway on a Windows System

DMZ Gateway and the connecting server must be installed on separate computers.

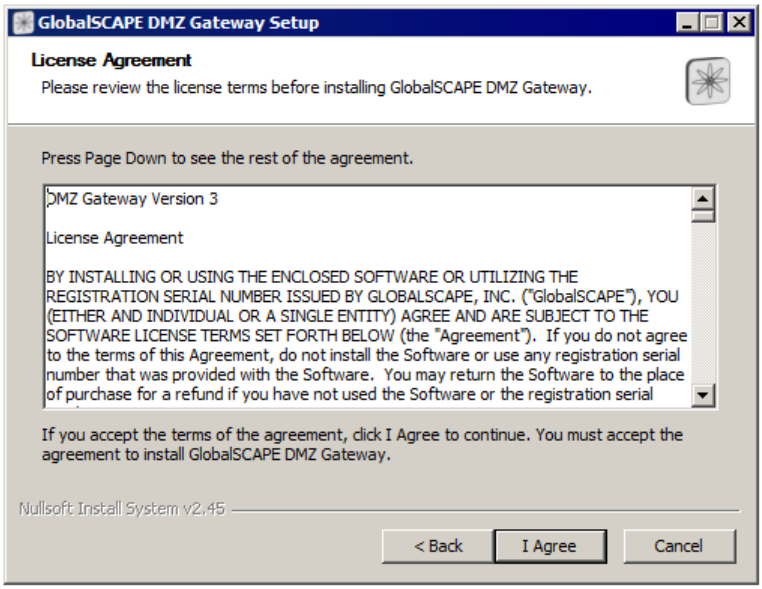
- If you are installing DMZ Gateway in a cluster configuration, refer to Installing DMZ Gateway in a Cluster.
- If you are upgrading, refer to Upgrading or Repairing DMZ Gateway on page 24.

To install DMZ Gateway

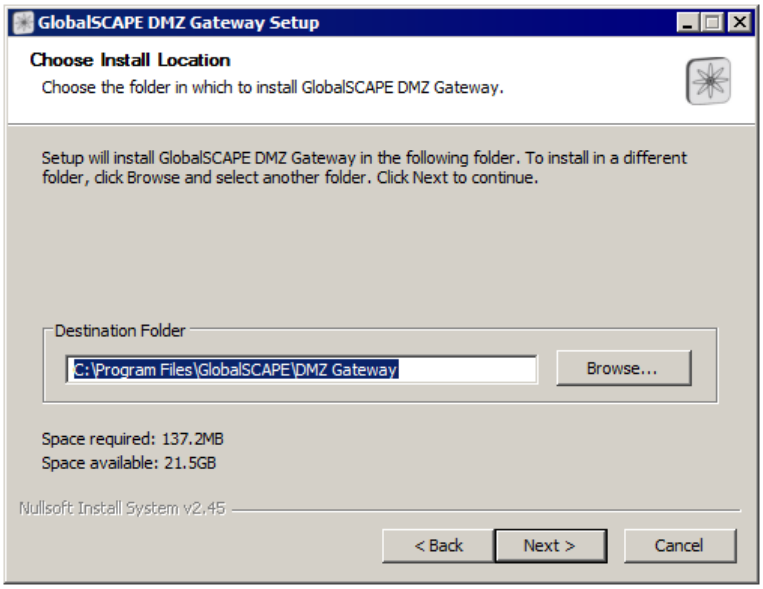
1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.
2. Start the installer. The **Welcome** page appears.



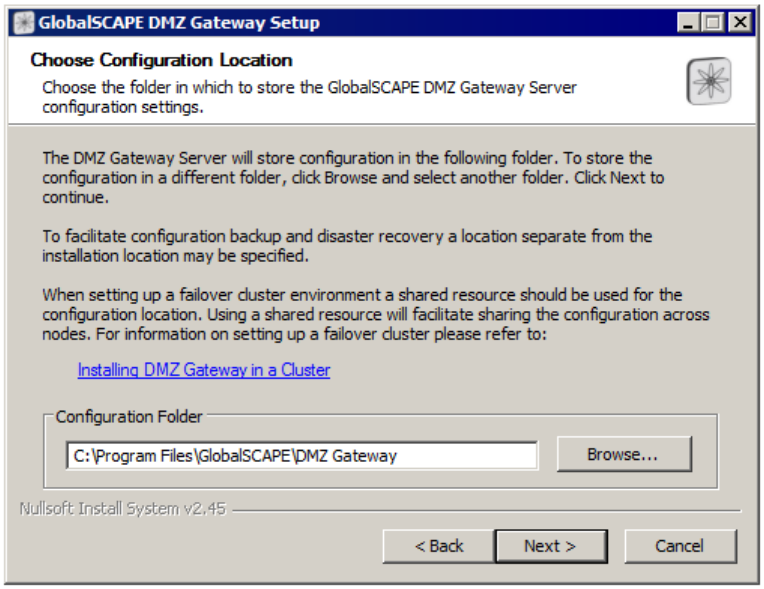
3. Click **Next**. The **License Agreement** appears.



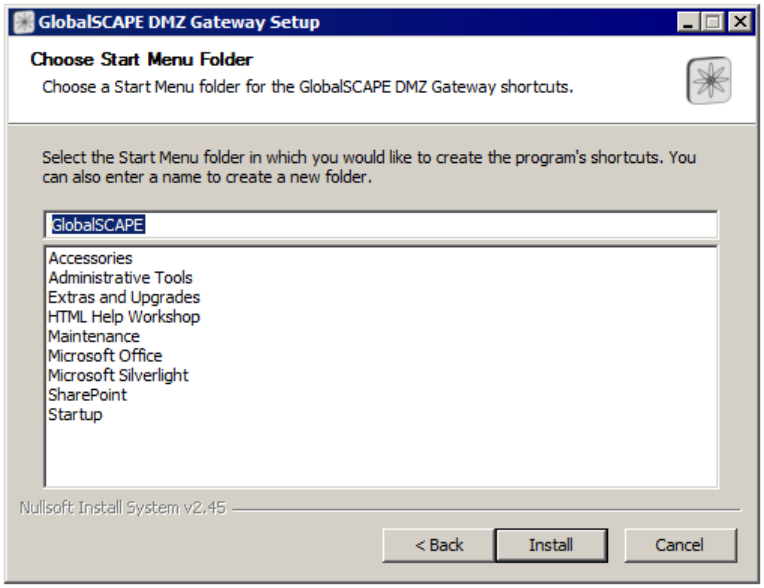
4. Read the license, then click **I Agree**.
5. If an existing installation is detected, refer to Upgrading or Repairing DMZ Gateway on page 24. Otherwise, the **Choose Installation Location** page appears.



6. The **Destination Folder** box displays the default location. Keep the default displayed in the box or click **Browse** to specify a different location. Also displayed is the amount of hard drive space required to install the program.
7. Click **Next**. The **Choose Configuration Location** page appears.

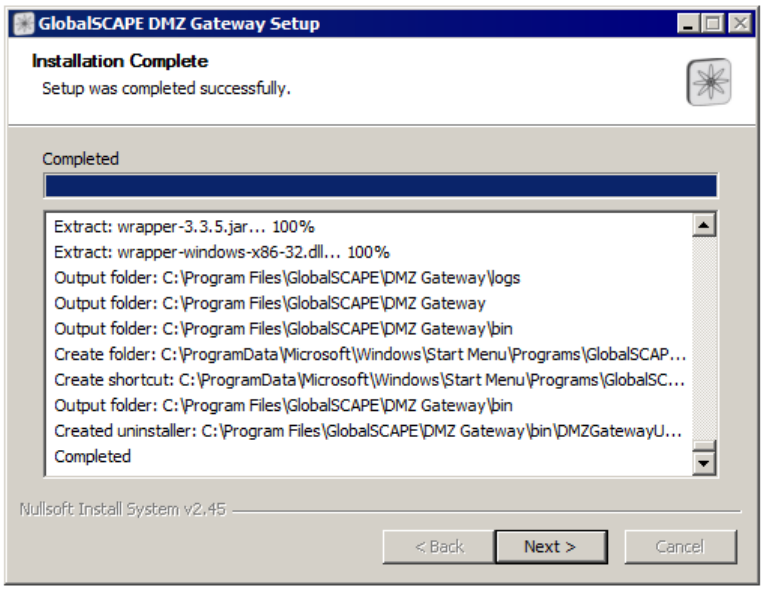


8. In the **Configuration Folder** box, specify the path at which to store configuration files for DMZ Gateway. The installation location is specified by default, but you can specify a separate location for backup and disaster recovery or for shared resources, such as with a cluster environment.
9. Click **Next**. The shortcuts page appears.

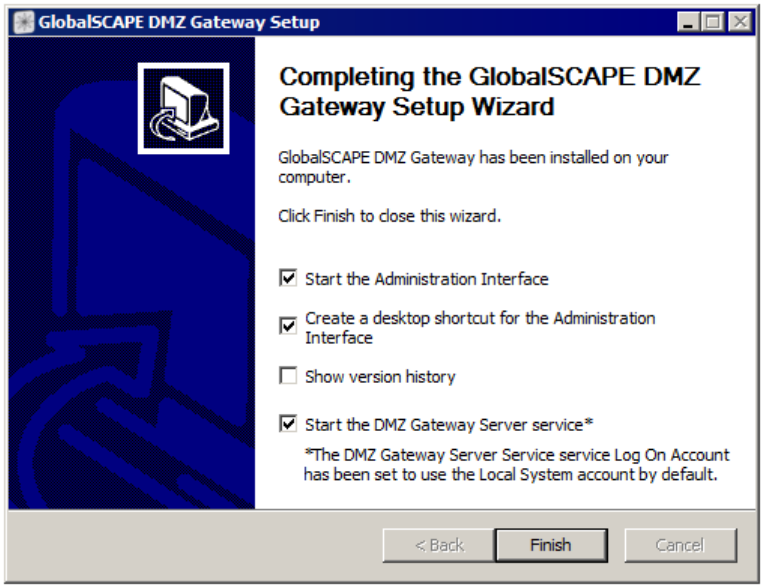


A shortcut to open the DMZ Gateway interface will be installed on the **Start** menu in a folder called **Globalscape**. You can keep this default location or specify a different location in which to install the shortcut.

10. Click **Install**. The product is installed and the installation log appears.



11. Click **Next**. The completed page appears.



The **Start the Administration Interface**, **Create a desktop shortcut**, and **Start the DMZ Gateway Server service** check boxes are selected by default. Select the **Show version history** check box if you want to read the release notes. (You can also access the release notes in the installation folder.)

12. Click **Finish**. If you left the **Start the Administration Interface** check box selected, the DMZ Gateway Administration Interface on page 28 appears.

A default Profile is defined that will listen on all IP addresses of the computer on which you installed DMZ Gateway. By default, it will listen for connections from servers on port 44500.

- Refer to Editing a Profile on page 34 to change the IP address/port assignments.
- Refer to Creating a Profile on page 32 to create new/additional Profiles.
- Refer to Controlling Access by IP Address on page 35 to specify which IP addresses or IP masks are allowed or denied connections.
-

Installing DMZ Gateway on a non-Windows System

The installation process on each non-Windows operating system is the same, with a few minor differences. The basic process of installation can be described as follows:

1. Copy the appropriate installer archive file (**.tgz**) to the target machine.
2. Extract the contents of the installer archive. The archive contains two files: an installation script and an archive of the actual program files.
3. Run the installation script as root and follow the prompts.

The process for supported non-Windows operating systems is described below. (For installation on Windows systems, refer to Installing DMZ Gateway on page 16.)

The installation script includes registering and starting the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). Alternately, you can start the server manually using the command `<InstallDir>/bin/dmzgatewayd start`. Refer to Manually Registering and Deregistering the DMZ Gateway Server Daemon on page 23 if you decide not to register the daemon during the installation process.

Installing DMZ Gateway on RedHat or SuSE Linux 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the appropriate DMZ Gateway Linux installer archive to a convenient directory on the target machine.
2. On the target machine, open a terminal window. The installation package must be run with root privileges. If not already logged on as the root user, change to root using the `su` command in the terminal window:

   ```
   su
   ```

3. Change to the directory containing the installer archive and perform the following:
   - On 32-bit systems:

     ```
     gunzip dmz-gateway-linux-x86-32.tgz
     tar xvf dmz-gateway-linux-x86-32.tar
     ./Install.sh
     ```

   - On 64-bit systems:

     ```
     gunzip dmz-gateway-linux-x86-64.tgz
     tar xvf dmz-gateway-linux-x86-64.tar
     ./Install.sh
     ```

4. Follow the prompts to complete the installation.
   - You are prompted to accept the license agreement, and to specify the installation and configuration directories (e.g., **/opt/dmzgateway**), etc.
   - After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
   - If you start the service, you can execute the DMZ Gateway Administration interface script (e.g., type: `/opt/dmzgateway/bin/DMZGatewayAdmin`).

Refer to the example below on page 22 for details of the installation process.

Installing DMZ Gateway on Ubuntu Linux 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the DMZ Gateway installer archive into a convenient directory on the target machine.
2. On the target machine, open a terminal window.
3. Change to the directory containing the installer archive and perform the following:
   - On 32-bit systems:
     ```
     gunzip dmz-gateway-linux-x86-32.tgz
     tar xvf dmz-gateway-linux-x86-32.tar
     sudo ./Install.sh
     ```
4. On 64-bit systems:
   ```
   gunzip dmz-gateway-linux-x86-64.tgz
   tar xvf dmz-gateway-linux-x86-64.tar
   sudo ./Install.sh
   ```
5. Follow the prompts to complete the installation.
   - You are prompted to accept the license agreement, and to specify the installation and configuration directories (by default, **/opt/dmzgateway**), etc.
   - After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
   - If you start the service, you can execute the DMZ Gateway Administration interface script (e.g., type: `/opt/dmzgateway/bin/DMZGatewayAdmin`).

Refer to the example below on page 22 for details of the installation process.

Solaris x86 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the appropriate DMZ Gateway installer archive to a convenient directory on the target machine.
2. On the target machine, open a terminal window. The installation package must be run with root privileges. If not already logged on as the root user, change to root using the `su` command in the terminal window:
   ```
   su
   ```
3. Change to the directory containing the installer archive and perform the following:
   - On 32-bit systems:
     ```
     gunzip dmz-gateway-solaris-x86-32.tgz
     tar xvf dmz-gateway-solaris-x86-32.tar
     ./Install.sh
     ```
   - On 64-bit systems:
     ```
     gunzip dmz-gateway-solaris-x86-64.tgz
     tar xvf dmz-gateway-solaris-x86-64.tar
     ./Install.sh
     ```
4. Follow the prompts to complete the installation.
   - You are prompted to accept the license agreement, and to specify the installation and configuration directories (e.g., **/opt/dmzgateway**), etc.
   - After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
   - If you start the service, you can execute the DMZ Gateway Administration interface script (e.g., type: `/opt/dmzgateway/bin/DMZGatewayAdmin`).

Refer to the example below on page 22 for details of the installation process.

Example of Installation Process

Below is an example of executing the Install.sh script on a Solaris x86 32-bit computer.

```
== License Agreement ==
OMITTED – End-user License Agreement
Do you agree to the above license terms? [yes or no]: yes [ENTER]
== Choose Install Location ==
Please specify the path into which the DMZ Gateway program files will be installed
or press "Enter" to accept the default.
Specify installation directory [/opt/dmzgateway]: [ENTER]
== Choose Configuration Location ==
Please specify the path in which to store the DMZ Gateway Server configuration
settings or press "Enter" to accept the default.
Specify configuration directory [/opt/dmzgateway]: /export/home/appdata [ENTER]
== Choose Installation Owner ==
Please specify the user account name to use as the owner of the installed files.
Specify owner [root]: [ENTER]
== Choose Installation Group ==
Please specify the user group name to use as the group of the installed files.
Specify group [root]: [ENTER]
== Confirm Settings ==
Installation directory:  /opt/dmzgateway Configuration directory:
/export/home/appdata Installation owner:      root Installation group:      root
Are these settings correct? [yes or no]: yes [ENTER]
Creating directory "/opt/dmzgateway"
Creating directory "/export/home/appdata"
Unpacking archive...
Extracting files...
OMITTED - Extracted Program File List
Unpacking JRE...
Extracting JRE...
OMITTED - Extracted Java Runtime Environment File List
Removing temporary files...
Updating permissions...
Updating ownership...
Updating configuration file...
== Register Service ==
The installation script can attempt to register the DMZ Gateway Server daemon
service (dmzgatewayd) for automatic startup and shutdown.
Register the DMZ Gateway Server daemon service? [yes or no]: yes
Creating symbolic link "/etc/init.d/dmzgatewayd"...
Registering system daemon...
ln -sf /etc/init.d/dmzgatewayd /etc/rc0.d/K99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc1.d/K99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc2.d/S99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc3.d/S99dmzgatewayd
== Start Service ==
The installation script can attempt to start the DMZ Gateway Server daemon service
(dmzgatewayd).
Start the DMZ Gateway Server daemon service? [yes or no]:  yes [ENTER]
Executing: /etc/init.d/dmzgatewayd start
-n Starting DMZ Gateway Server...
== Installation Complete ==
The Globalscape, Inc. DMZ Gateway is now installed.
The DMZ Gateway Server daemon service may be controlled using the "dmzgatewayd"
script:    /opt/dmzgateway/bin/dmzgatewayd
The DMZ Gateway Administration Interface may be started using the
script:    /opt/dmzgateway/bin/DMZGatewayAdmin
```

Activating DMZ Gateway

DMZ Gateway licensing is activated in the connecting server, not DMZ Gateway, which accepts connections from any licensed server. For example, a Single-Site license enables one EFT Server Site or a Mail Express Server to connect to any available DMZ Gateway. A Multi-Site license enables one or more Sites from EFT Server Enterprise to connect to any available DMZ Gateway. DMZ Gateway allows up to 15 Profile definitions to manage connections, but the license installed on the connecting server determines how many connections the server is allowed to make to DMZ Gateway.

After the 30-day trial has expired, you must activate DMZ Gateway by activating the serial number in the connecting server's administration interface. Refer to the EFT Server or Mail Express documentation for details of activating DMZ Gateway.

Manually Registering and Deregistering the DMZ Gateway Server Daemon (non-Windows Systems)

During the installation process, you are prompted to register the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). If you choose not to register the daemon during the installation process, use the procedure below to add or remove the DMZ Gateway Server daemon script, dmzgatewayd, from automatic system startup and shutdown.

There are multiple methods of configuring a daemon script for automatic startup/shutdown on Linux/Solaris. Ultimately, whatever method is used typically results in the creation of symbolic links in the **/etc/rc*** directories. These scripts are called at different startup and shutdown run levels of the operating system to start and stop the daemon.

RedHat Enterprise Linux

After creation of the /etc/init.d/dmzgatewayd symbolic link, the chkconfig command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:

  ```
  chkconfig --add dmzgatewayd
  ```

  (there are two dashes before `add`)

To deregister the script

- The following command may be used as root:

  ```
  chkconfig --del dmzgatewayd
  ```

  (there are two dashes before `del`)

SuSE Linux

After creation of the **/etc/init.d/dmzgatewayd** symbolic link, the **insserv** command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:

  ```
  insserv dmzgatewayd
  ```

To deregister the script

- The following command may be used as root:

  ```
  insserv -r dmzgatewayd
  ```

Ubuntu Linux

After creation of the **/etc/init.d/dmzgatewayd** symbolic link, the **update-rc.d** command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:

```
update-rc.d dmzgatewayd defaults
```

To deregister the script

- The **/etc/init.d/dmzgatewayd** symbol link must first be removed using the following command as root:

```
rm /etc/init.d/dmzgatewayd
```

To deregister the daemon

- The following command may be used as root:

```
update-rc.d dmzgatewayd remove
```

Solaris

On Solaris, after creation of the **/etc/init.d/dmzgatewayd** symbolic link you typically manually create the appropriate symbolic links in the **/etc/rc*** directories.

To register the script

- The following commands may be used as root:

```
ln -sf /etc/init.d/dmzgatewayd /etc/rc0.d/K99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc1.d/K99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc2.d/S99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc3.d/S99dmzgatewayd
```

To deregister the script

- Remove the symbolic links as root:

```
rm /etc/rc0.d/K99dmzgatewayd
rm /etc/rc1.d/K99dmzgatewayd
rm /etc/rc2.d/S99dmzgatewayd
rm /etc/rc3.d/S99dmzgatewayd
```

Upgrading or Repairing DMZ Gateway

Upgrades from version 2.x to version 3 of the DMZ Gateway are supported on Windows systems only. You must upgrade DMZ Gateway before upgrading EFT Server.

To upgrade or repair DMZ Gateway on non-Windows systems

- Perform the standard installation process on page 20 for the target operating system and use the same settings for installation path and configuration path. If the DMZ Gateway Server daemon service is running, you are prompted to stop it; if you do not stop it, the installer will abort.

To upgrade from DMZ Gateway 2.x on Windows systems

1. Close the Administration interface.
2. As a precaution, back up the existing installation directories and any other files you may have installed elsewhere.
3. Launch the installer and then click Next. The **License Agreement** appears.
4. Click **I Agree**. The installer will detect an existing installation.
5. The older version must be uninstalled. You can keep the existing configuration or use the (new) default configuration. Click one of the following, then click **Next:**
    - Keep existing configuration and uninstall the older version
    - Use a default configuration and uninstall the older version
6. Follow the prompts to finish the upgrade. Refer to Installing DMZ Gateway on page 16, if necessary.

During the upgrade process, the DMZ Gateway service **Log On As** account is set to use the **Local System** account.

To upgrade from DMZ Gateway 3.x on Windows systems

1. Close the Administration interface.
2. Launch the installer. The installer will detect an existing installation.
3. After accepting the End-User License Agreement, click **Upgrade DMZ Gateway**, then click **Upgrade**.
4. Follow the prompts to finish the upgrade. Refer to Installing DMZ Gateway on page 16, if necessary.

To reinstall DMZ Gateway 3.x on Windows systems

Reinstallation can be used to fix installations in situations where program files have been corrupted or accidentally deleted. During reinstallation, the installer will reinstall the original copies of corrupted or missing program files.

1. Close the Administration interface.
2. Launch the installer. The installer will detect an existing installation.
3. After accepting the End-User License Agreement, click **Reinstall DMZ Gateway**, then click **Reinstall**.
4. Follow the prompts to finish the reinstall. Refer to Installing DMZ Gateway on page 16, if necessary.

Uninstalling DMZ Gateway

Use the applicable procedure below to uninstall DMZ Gateway.

Uninstalling DMZ Gateway on a Windows System

Uninstall DMZ Gateway using Windows' **Add/Remove Programs** tool or via the shortcut on the **Start** menu.

Uninstalling DMZ Gateway on a non-Windows System

The installation process on each non-Windows operating system is the same with a few minor differences. The basic process of installation can be described as follows:

- Run the uninstallation script as root and follow the prompts. (The script is created during installation and is `<InstallDir>/bin/Uninstall.sh`)

RedHat Enterprise Linux, SuSE Linux, or Solaris x86 32-Bit or 64-Bit

You can uninstall DMZ Gateway using the Uninstall.sh script located in the `<InstallDir>/bin` directory.

To uninstall DMZ Gateway

1. On the target machine, open a terminal window. The uninstall script must be run with root privileges. If not already logged on as the root user, change to root using the su command in the terminal window:

   ```
   su
   ```

2. Run the Uninstall.sh script:

   ```
   /<InstallDir>/bin/Uninstall.sh
   ```

   For example:

   ```
   /opt/dmzgateway/bin/Uninstall.sh
   ```

3. Follow the prompts to complete uninstalling.

Ubuntu Linux 32-Bit or 64-Bit

You can uninstall DMZ Gateway using the Uninstall.sh script located in the <InstallDir>/bin directory.

To uninstall DMZ Gateway on Ubuntu Linux

1. On the target machine, open a terminal window.
2. Run the Uninstall.sh script:

   ```
   sudo /<InstallDir>/bin/Uninstall.sh
   ```

   For example:

   ```
   sudo /opt/dmzgateway/bin/Uninstall.sh
   ```

3. Follow the prompts to complete uninstalling.

Example of Uninstallation Process on Solaris

The following printout is a sample execution of the **Uninstall.sh** installation script run on Solaris x86 32-bit.

```
== Confirm Uninstallation == The uninstallation script will now uninstall the DMZ
Gateway from the following installation directory:

/opt/dmzgateway

Proceed with uninstallation? [yes or no]: yes [ENTER]

== Stop Service == The installation script has detected that the DMZ Gateway Server
daemon service (dmzgatewayd) is currently running. The service must be stopped
before proceeding. The script can now attempt to stop the service.

Stop the DMZ Gateway Server daemon service? [yes or no]: yes [ENTER]

Executing: /etc/init.d/dmzgatewayd stop Stopping DMZ Gateway Server... Stopped DMZ
Gateway Server.

== Deregister Service == The installation script can attempt to deregister the DMZ
Gateway Server daemon service (dmzgatewayd) from automatic startup and shutdown.

Deregister the DMZ Gateway Server daemon service? [yes or no]: yes [ENTER]

Removing /etc/init.d/dmzgatewayd symbolic link...

Deregistering system daemon:
rm /etc/rc0.d/K99dmzgatewayd rm /etc/rc1.d/K99dmzgatewayd rm
/etc/rc2.d/S99dmzgatewayd rm /etc/rc3.d/S99dmzgatewayd
Removing installation files...

== Uninstallation Complete ==
```

Administering DMZ Gateway

The topics in this section provide instructions for administering DMZ Gateway.

DMZ Gateway Components

DMZ Gateway consists of the following components:

- The main server component, the DMZ Gateway Server
- A launch and monitoring component, the DMZ Gateway Server Service
- A configuration and monitoring component, the DMZ Gateway administration interface

DMZ Gateway Server

The DMZ Gateway Server is the main Java-based functionality. An embedded Java Runtime Environment (JRE) is used to execute this functionality. (The JRE is installed with DMZ Gateway--you do not need to install or maintain the JRE.) The DMZ Gateway Server component is never executed directly, but rather controlled and monitored using the DMZ Gateway Server Service component.

DMZ Gateway Server Service

The DMZ Gateway Server Service component is responsible for properly initializing the JRE and launching the DMZ Gateway Server component. It then stays resident and provides watchdog monitoring functionality over the DMZ Gateway Server component. It also provides logging and diagnostic capabilities to facilitate troubleshooting any possible issues that may occur during server startup. (Refer to DMZ Gateway Logging on page 38 for detailed information.)

DMZ Gateway Administration Interface

The DMZ Gateway Administration Interface on page 28 is a Java-based thick client that provides graphical administration capabilities for the DMZ Gateway Server. The interface communicates with the DMZ Gateway Server via a local-only TCP/IP administration port.

The administration capabilities include:

- Creating and Configuring Profiles on page 32
- Viewing Statistics on page 36
- Controlling the Server Service/Daemon on page 29

DMZ Gateway System Files

The following file names can be observed when running DMZ Gateway:

On Windows Systems:

- In the Windows Services dialog box:
  - **DMZ Gateway Server** is the DMZ Gateway service on page 29.
- In the **Task Manager**:
  - **DMZGatewayServerService.exe** launches and monitors the DMZ Gateway Server.
  - **DMZGatewayServer.exe** is the DMZ Gateway Server.
  - **DMZGatewayAdmin.exe** is the administration interface on page 28.

On Non-Windows Systems:

- **dmzgatewayd** is the DMZ Gateway daemon on page 29.
- **DMZGatewayServer** is the DMZ Gateway Server.
- **DMZGatewayAdmin** is the DMZ Gateway administration interface on page 28.

You can view all running DMZ Gateway executables by typing:

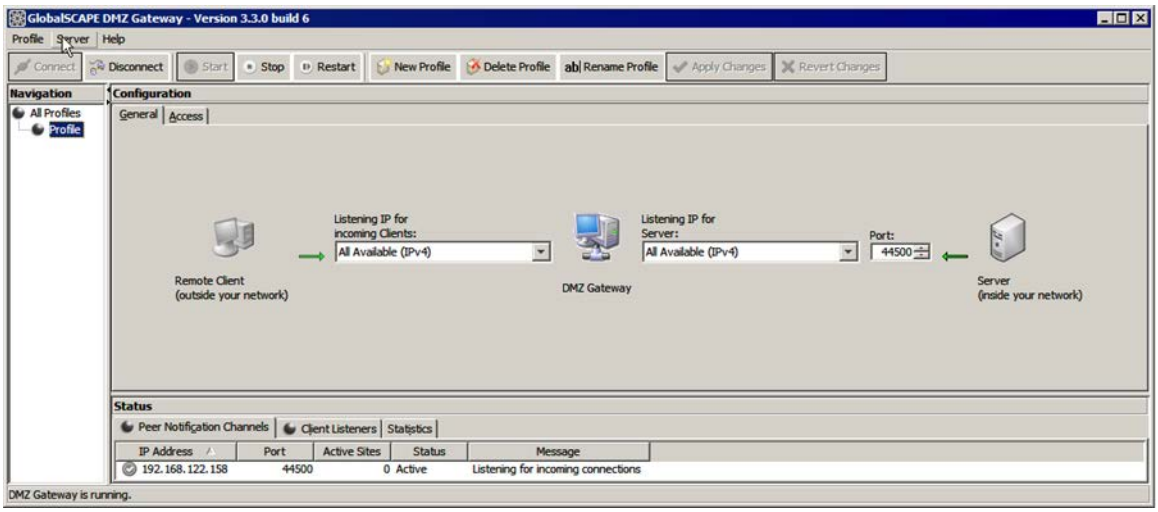
```
ps –ef | grep DMZGateway
```

The DMZ Gateway Interface

The DMZ Gateway interface is used for mapping and viewing DMZ Gateway connections. *Profiles* are used to define connections to DMZ Gateway.

To open the interface

- On Windows systems, double-click the DMZ Gateway shortcut on the desktop or **Start** menu.
- On non-Windows systems, after the server service has started, execute the DMZ Gateway administration interface script (e.g., `/opt/dmzgateway/bin/DMZGatewayAdmin`).
- The left pane displays each of the defined *Profiles* in an expandable/collapsible tree view. DMZ Gateway has a default Profile for which you define the listening IP address(es) and port for the connecting server, listening IP address(es) for connecting clients, and the IP address ban list. When DMZ Gateway connects, only the default Profile is displayed. The interface displays the configuration for the last Profile modified or viewed the last time the interface was opened or the first (default) Profile if no "last viewed" profile value is available.
- In the default view, with **All Profiles** selected, the right pane displays the status of the DMZ Gateway service and the status of all Profiles.
- When a Profile is selected, the right pane displays the configuration information and status of the selected Profile.



DMZ Gateway Administration Interface PID File

When the DMZGatewayAdmin executable is launched it will create the PID file <Installation Directory>\DMZGatewayAdmin.pid. This file contains the PID for the administration interface process. The timestamp of the file is updated every 10 seconds while the administration interface is running. When the application exits gracefully, it deletes the PID file.

This file is also used to prevent simultaneous execution of multiple copies of the administration interface. When the administration interface starts, it checks for the presence of the PID file. If the file exists and its timestamp has been updated in the last 20 seconds it will assume another copy of the user interface is running and exit.

Related Topics

- Refer to Creating a Profile on page 32 for information about Profile configuration.
- Refer to Controlling Access by IP Address on page 35 for information about granting or denying access to a specific IP addresses or an IP mask.
- Refer to Starting and Stopping the DMZ Gateway Server Service on page 29 for details of stopping and starting the DMZ Gateway server service.
- Refer to Viewing Statistics on page 36 for details of each of the tabs in the **Status** pane.

Starting and Stopping the DMZ Gateway Server Service

Typically, the DMZ Gateway server service is configured to start automatically when the computer is started. When the DMZ Gateway administration interface is launched, it determines whether the DMZ Gateway server service is running. If the DMZ Gateway server service is not running, a prompt appears asking if you want to start the DMZ Gateway service.

On Windows systems:

When you install DMZ Gateway, the service is configured to start automatically. You can start and stop the service in the Windows **Services** dialog box and in the DMZ Gateway Administration Interface on page 28.

On non-Windows systems:

The installation script includes registering and starting the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). Alternatively, you can start and stop the server manually using the following commands:

```
<InstallDir>/bin/dmzgatewayd start
<InstallDir>/bin/dmzgatewayd stop
```

In the DMZ Gateway administration interface:

In the DMZ Gateway administration interface, you can start and stop the service from the Server menu or using the toolbar controls. The status of the DMZ Gateway server service appears in the status bar at the bottom of the interface. (e.g., "DMZ Gateway is running.") You can start, pause, restart, or stop the DMZ Gateway service on the DMZ Gateway main menu or toolbar.

To start the DMZ Gateway

- On the DMZ Gateway main menu, click **Server > Start** or click **Start** on the toolbar.

To restart the DMZ Gateway

- On the DMZ Gateway main menu, click **Server > Restart** or click **Restart** on the toolbar.

To stop the DMZ Gateway

- On the DMZ Gateway main menu, click **Server > Stop** or click **Stop** on the toolbar.

DMZ Gateway Server PID Files

When the DMZ Gateway Server Service starts it will create the PID file **<Installation Directory>\DMZGatewayServerService.pid**. This file contains the process ID for the DMZ Gateway Server Service.

When the DMZ Gateway Server is started, the PID file **<Installation Directory>\DMZGatewayServer.pid** is created. This file contains the process ID for the DMZ Gateway Server.

DMZ Gateway Server Status Files

During the course of operation, the DMZ Gateway Server Service will create and update the status file **<Installation Directory>\DMZGatewayServerService.status**. This file will contain the current status of the DMZ Gateway Server Service. The possible contents are described at http://wrapper.tanukisoftware.org/doc/english/prop-statusfile.html.

During the course of operation the DMZ Gateway Server Service will create and update the status file <Installation Directory>\DMZGatewayServer.status. This file will contain the current status of the DMZ Gateway Server. The possible contents are described at http://wrapper.tanukisoftware.org/doc/english/prop-java-statusfile.html.

DMZ Gateway Server Monitoring

After starting the DMZ Gateway Server, the DMZ Gateway Server Service will stay resident and monitor the Server. If the Server crashes, the Service will wait 5 seconds and attempt to restart the Server.

DMZ Gateway Server Unix/Solaris Daemon

On Solaris and Linux-based system, the DMZ Gateway Server is started and controlled using the system daemon script **<Installation Directory>/bin/dmzgatewayd**. When necessary, this script will call the Java Service Wrapper utility **<Installation Directory>/bin/DMZGatewayServerServic**e to start and stop the **DMZGatewayServer** Java executable.

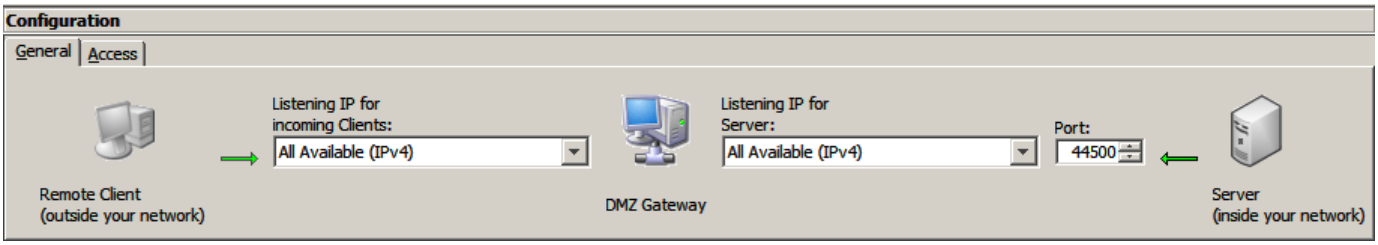
Per convention, if the user opted to register the service with the operating system during installation, a symbolic link **/etc/init.d/dmzgatewayd** will have been created. This symbolic link points to the **<Installation Directory>/bin/dmzgatewayd** script. Additionally, the appropriate symbolic links will have been created in the **/etc/rc.d** directories so that the DMZ Gateway Server will be started and stopped appropriately during system startup and shutdown.

You can control the system daemon by executing either /**etc/init.d/dmzgatewayd** or **<Installation Directory>/bin/dmzgatewayd**. The script accepts a set of command line options. Running the script without any command line options will display the set of available options, which are itemized below:

- console – Runs the DMZ Gateway Server as a console program as opposed to a system daemon.
- start – Starts the DMZ Gateway Server as a daemon process
- stop – Stops the DMZ Gateway Server daemon process, if running.
- restart – Stops the DMZ Gateway Server daemon process, if running, and then starts it.
- condrestart – Restarts the DMZ Gateway Server daemon process if it is currently running.
- status – Indicates if the DMZ Gateway Server daemon process is currently running or not.
- dump – Instructs the Java Virtual Machine to log the state of all active threads to the log.

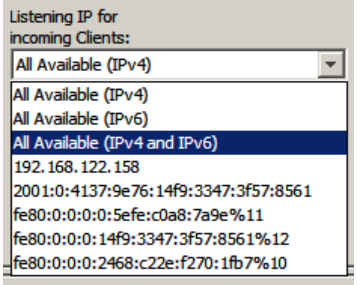
Specifying the Listening IP Addresses

For each DMZ Gateway Profile, you specify 2 IP addresses:



1. One address is used by client programs to connect. This is typically an external-facing address. When a Site configured at a peer server connects to the DMZ Gateway over the PNC, the DMZ Gateway reads the list of client ports configured in the Site. These ports are then combined with the client IP Address and it is on these client IP address/Site port combinations that the DMZ Gateway will listen for client connections.
2. The other address specifies the IP address on which to listen for connections from peer servers. The communications established using this address is known as the *Peer Notification Channel* or *PNC*. Typically, this IP Address will be an internal-facing address. This address is combined with the configured port value and it is on this IP Address/port combination that the DMZ Gateway will listen for connections from peer servers.

Each address is configured by selecting the IP address to use from a drop-down list. The list of IP addresses includes all IPv4 and IPv6 addresses present on the computer. Additionally, the list includes an **All Available** setting for both IPv4 and IPv6. (IPv6 connections to DMZ Gateway are not supported on Windows Server 2003.)



- In the **Listening IP for incoming Clients** box, click the down arrow to select one or more IP addresses for incoming clients. (Only the IP addresses defined on this computer appear in this box.) You can specify:
    - **All Available (IPv4)**—Listen for client connections on all IPv4 addresses.
    - **All Available (IPv6)**—Listen for client connections on all IPv6 addresses.
    - **All Available (IPv4 and IPv6)**—Listen for client connections on all IPv4 and IPv6 addresses.
    - **A specific IP address**—Listen for client connections on all on a specific IP address.
- In the **Listening IP for Server** box, click the down arrow to select one or more listening IP addresses for the server. (Only the IP addresses defined on this computer appear in this box.) **All Available** means that DMZ Gateway will listen on the IP address/port combination ONLY IF that IP address/port combination is not already being used by another Profile. Profiles configured with an explicit IP address have precedence over Profiles configured with **All Available**. You can specify:
    - **All Available (IPv4)**—Listen for server connections on all IPv4 addresses.
    - **All Available (IPv6)**—Listen for server connections on all IPv6 addresses.
    - **All Available (IPv4 and IPv6)**—Listen for server connections on all IPv4 and IPv6 addresses.
    - **A specific IP address**—Listen for server connections on all on a specific IP address.

  IMPORTANT:

  All Available means that DMZ Gateway will listen on the IP address/port combination ONLY IF that IP address/port combination is not already being used by another Profile. Profiles configured with an explicit IP address have precedence over Profiles configured with **All Available**.

What Does This Mean for the Peer Server Listeners?

Suppose you have three IP addresses on the computer: IP 1, IP 2, and IP 3, and you have two Profiles: Profile 1 and Profile 2.

- Both Profiles are configured to use the same Peer Server Listener Port 54321.
- Profile 1 is set to use **All Available**.
- Profile 2 is set to use IP 2.

Profile 1 will listen on **IP 1:54321** and **IP 3:54321**, and Profile 2 will listen on **IP 2:54321**.

Now, suppose you delete Profile 2, making **IP 2:54321** available. The DMZ Gateway will detect this and update the communications listeners so that Profile 1 will now listen on **IP 1:54321**, **IP 2:54321**, and **IP 3:54321**.

What Does This Mean for the Client Listeners?

Suppose you have three IP addresses on the computer: IP 1, IP 2, and IP 3, and you have two Profiles: Profile 1 and Profile 2. Profile 1 is set to use **All Available** and Profile 2 is set to use IP 2.

Now suppose you have two Sites configured on EFT Server. Both Sites are configured to connect to the DMZ Gateway and use FTP port 21. Site 1 is set to connect to Profile 1, and Site 2 is set to connect to Profile 2.

Once both Sites are connected, the DMZ Gateway will establish client listeners for Site 1 on **IP 1:21** and **IP 3:21** (because Site 1 used Profile 1, which uses all available IP/port combinations not currently in use). For Site 2 the DMZ Gateway will establish a client listener on **IP 2:21**.

If Site 2 should disconnect for some reason (perhaps it was deleted), **IP 2:21** is now considered available. The DMZ Gateway will detect this and update the communications listeners so that Profile 1 will listen for client connections on **IP 1:21**, **IP 2:21**, and **IP 3:21**.

Creating a Profile

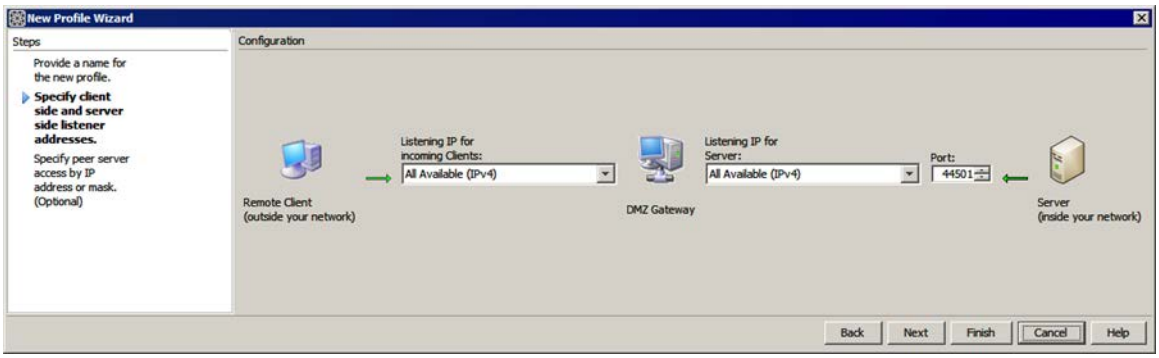
Creating a Profile includes specifying the listening IP address for incoming clients, specifying the listening IP addresses and port for the connecting server, and specifying the IP addresses that are allowed or denied access.

To create a Profile

1. Do one of the following:
   - Right-click in the **Profiles** tree, then click **New Profile**.
   - On the toolbar, click **New Profile**.
   - On the main menu, click **Profile > New**.

   The **New Profile Wizard** appears.

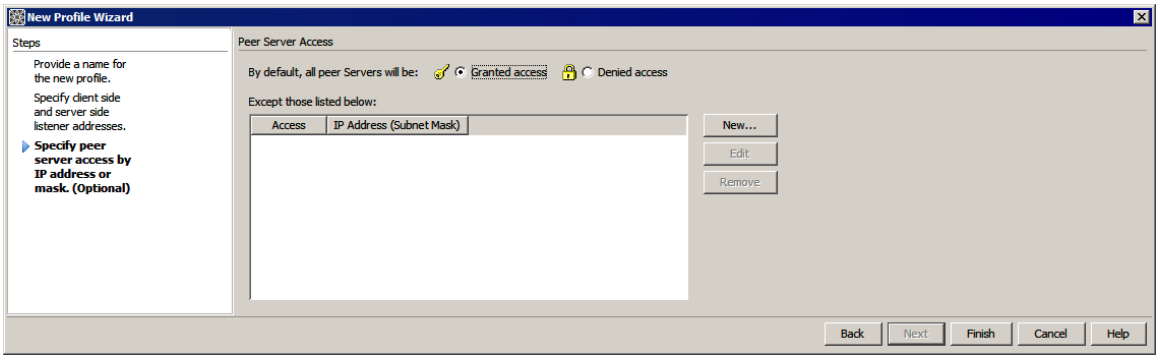
2. In the **Profile Name** box, provide a unique name for this Profile. The name will appear in the interface, logs, error messages, and reports.
3. Click **Next**. The **Configuration** page of the wizard appears.



4. In the **Listening IP for incoming Clients** box, click the down arrow to select one or more IP addresses for incoming clients. Refer to Specifying the Listening IP Addresses on page 30 for details.
5. In the **Listening IP for Server** box, click the down arrow to select one or more listening IP addresses for the server. Refer to Specifying the Listening IP Addresses on page 30 for details.
6. In the **Port** box, provide the port number over which connections are allowed.

> *The connection will be refused if the IP address is on the IP address ban list.*

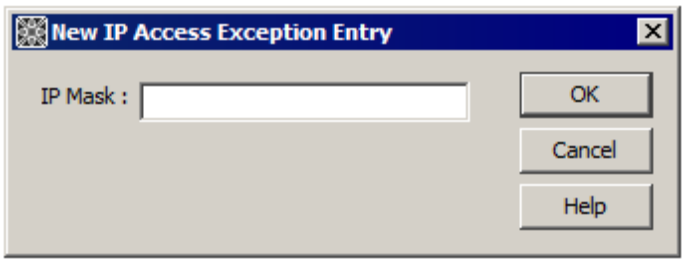
7. Click **Next**. The **Peer Server Access** page appears.



8. All IP addresses are granted access by default. To grant or deny access to specific IP addresses (optional):
9. Click **Granted access** or **Denied access**.
   - If most IP addresses are *allowed* access, click **Granted access**, then add the exceptions.
   - If most IP addresses are *denied* access, click **Denied access**, then add the exceptions.

> *For example, if you want to allow only 192.168.174.159 and block every other IP address, click **Denied access**, click **Add**, then type `192.168.174.159` in the **IP Mask** box. This will deny access to all IP addresses except 192.168.174.159.*

10. Click **New**. The **New IP Access Exception Entry** dialog box appears.



11. Specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.

12. Click **OK** to close the **New IP Access Exception Entry** dialog box.
13. Click **Finish**. The IP Mask appears in the exception list.

Renaming a Profile

The Profile name appears in statistics, logs, messages, and reports. You can change the name in the DMZ Gateway interface.

To change the name of a Profile

1. Click the Profile in the tree, then do one of the following:
   - Click the Profile name again.
   - Right-click the Profile name, then click **Rename Profile**.
   - On the toolbar, click **Rename Profile**.
   - On the main menu, click **Profile > Rename**.

   The name in the tree becomes editable.
2. Type a new name for the tree, then press ENTER.

Deleting a Profile

You can configure multiple Profiles. You can delete Profiles that you no longer use, but you cannot delete a Profile if it is the only Profile.

To delete a Profile

- Click the Profile in the tree, then do one of the following:
  - Right-click the Profile name, then click **Delete Profile**.
  - On the toolbar, click **Delete Profile**.
  - On the main menu, click **Profile > Delete Profile**.

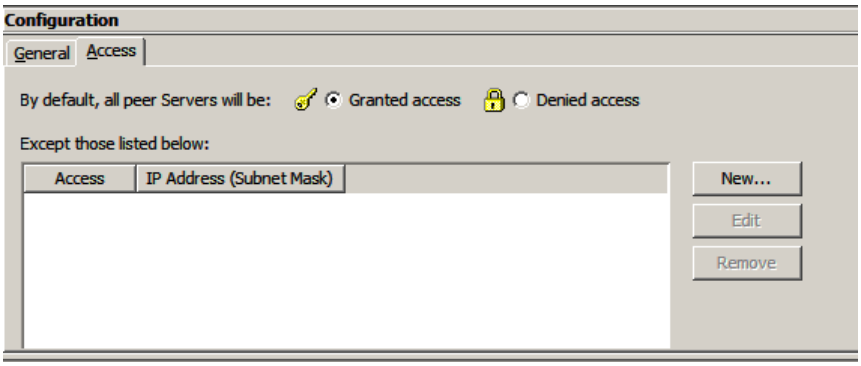
The Profile is deleted from the tree.

Editing a Profile

When you create a new Profile, you define the listening IP address for remote connecting clients, the listening IP address and port for the server inside your network, and any IP addresses exceptions on page 35. After the Profile is created, you can edit the Profile's configuration as necessary. You can also rename on page 34 or delete on page 34 the Profile. When you make a change to a Profile, before you click **Apply**, an asterisk appears in the tree next to the Profile that you are editing. You must define a unique IP address/port combination for each Profile.

To edit a Profile

1. In the **Navigation** pane, click the Profile that you want to edit.
2. In the **Configuration** pane, click the **General** tab.
3. Specify the **Listening IP for incoming Clients** box and the **Listening IP for Server**. Refer to Specifying the Listening IP Addresses on page 30 for detailed information.
4. In the **Port** box, provide the port number over which connections are allowed.
5. In the **Configuration** pane, click the **Access** tab.



6. Specify the IP addresses or IP mask of servers that are allowed or denied access on page 35.
7. In the toolbar, click **Apply Changes**. If the IP address and port are not unique, an error message appears; otherwise, the DMZ Gateway will allow the server to connect.

*If you have made multiple edits, you can revert to the last-saved state by clicking **Revert Changes** (undo) before clicking **Apply Changes**. However, once you click **Apply Changes**, you cannot go back.*

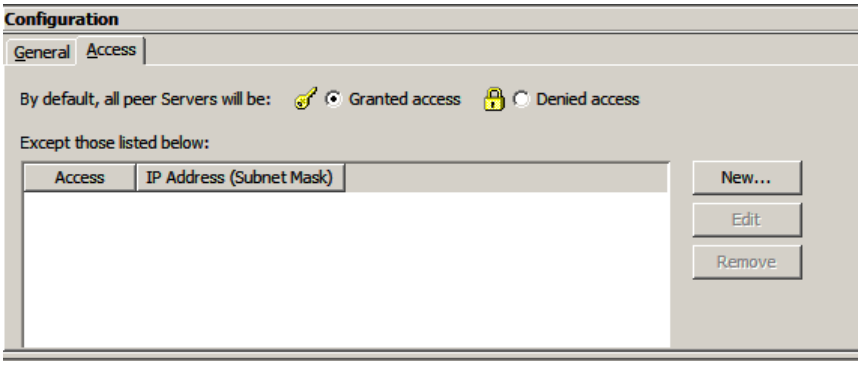
Controlling Access by IP Address

By default, all IP addresses are granted access to DMZ Gateway. You can grant access to only one specific IP address or a range of IP addresses, or deny access to one specific address or a range of addresses. You can define up to 100 IP address masks.

For example, if you want to allow only 192.168.174.159 and block every other IP address, click **Denied access**, click **Add**, then type `192.168.174.159` in the **IP mask** box. This will deny access to all IP addresses except 192.168.174.159.

To grant/deny access by IP Address

1. In the Profile tree, click the default **Profile** or create a new profile on page 32.
2. In the **Configuration** pane, click the **Access** tab. The exception list appears.



3. The **Access** tab displays the IP addresses that are granted or denied access. By default, all IP addresses are granted access, and no exceptions are displayed in the list.
4. To configure exceptions, click **Granted access** or **Denied access**.
   - If most IP addresses are *allowed* access, click **Granted access**, then add the exceptions (IP addresses that are not allowed access).
   - If most IP addresses are *denied* access, click **Denied access**, then add the exceptions (IP addresses that are allowed access).
5. Click **Add**. The **New IP Access Exception Entry** dialog box appears.
6. Specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.
7. Click **OK**. The IP address/mask appears in the exceptions list.

8. Click **Apply Changes** to save the changes on DMZ Gateway.

Viewing Statistics

In the DMZ Gateway administration interface, you can view a variety of statistics. Whether you click **All Profiles** or a specific Profile, the **Status** area displays information about Peer Notification on page 36 Channels and Client Listeners on page 36, as well as the size and speed of server and client data being transferred on page 37.

Your selections persist across Profiles; that is, if you click the **Client Listeners** tab in Profile 3, then click Profile 2, the **Client Listeners** tab is selected in Profile 2 also.

The status "bubbles up" to the **All Profiles** node. For example, if there is a problem in Profile 1 causing the icon to turn yellow, the **All Profiles** icon is also yellow.

In the Profile tree:

- A red icon indicates that an error exists (e.g. port conflict from external application, IP address no longer exists, etc.).
- A yellow icon indicates that the DMZ Gateway service is running, but port conflicts exist between connected sites, when at least two Sites are connected.
- A green icon indicates that the DMZ Gateway Service is running and at least one Site is connected.
- A gray icon indicates that there are no errors and no Servers are connected.

Peer Notification Channels

The **Peer Notification Channels** tab of the **Status** panel displays the IP address, port, number of active sites, channel status, and channel status message for each configured server-side IP address for a selected Profile or **All Profiles**. If **All Profiles** is selected, a Profile column displays the name of the applicable Profile. (For more about Peer Notification, refer to Introduction to Globalscape DMZ Gateway on page 7.)

The following icons provide an indication of channel status:

Active with connected servers

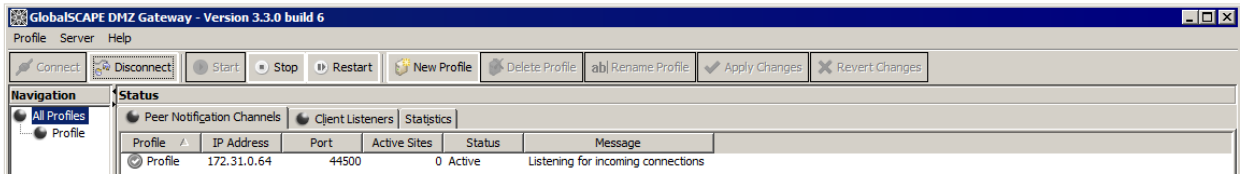
Active with no connected servers

Warning

Error

The following columns displayed on the tab can be sorted by clicking the column header:

- **IP address** - IP address on which Peer Notification Channels communicate
- **Port** - Port on which Peer Notification Channels communicates
- **Active Sites** - Number of Sites connected to DMZ Gateway
- **Status** - Active, Inactive, Warning, Error
- **Message** - More information regarding status (e.g., Listening for connections, Port already in use)



Client Listeners

The **Client Listeners** tab of the **Status** panel displays the PNC address, server IP address, server name, server type, Site name, listener IP address/port, status, and status message. If **All Profiles** is selected, the **Profile** column displays the name of the applicable Profile.

The following icons provide an indication of status:

- Listening
- Inactive
- Warning
- Error

The following columns displayed on the tab can be sorted by clicking the column header:

- **PNC Address** - Server-side IP address on which the server connected to DMZ Gateway
- **Server IP Address** - IP address of the remote server
- **Server Name** - user-assigned name of connected server
- **Server Type** - Type of server, e.g., EFT Server, EFT Server Enterprise, Mail Express Server
- **Site** - User-assigned name of Site
- **Listener IP Address** - Client-side IP address on which clients connect to DMZ Gateway
- **Listener Port** - Port of Listener
- **Status** - Active, Inactive, Error, Warning
- **Message** - More information regarding status (e.g., Listening for incoming connections, Unable to bind to port, Listener creation failure, Closed, Inactive, Listener IP/Port address already assigned)

Statistics

The **Statistics** tab of the **Status** panel displays the size and speed of server and client data being transferred. When **All Profiles** is selected, the aggregated data sizes are displayed, and the **Profile** column displays the name of the applicable Profile.

The **Statistics** tab is configured by default to refresh automatically every 15 seconds. You can change the refresh frequency or configure the interface to not refresh automatically. You can also refresh the display manually.

- To change the refresh frequency, in the **Refresh Interval** box, provide a new interval, in seconds, then click **Apply Refresh Interval**.
- To prevent the interface from refreshing automatically, clear the **Enable automatic refresh** check box.
- To refresh the interface manually, click **Refresh Now**.

The following columns displayed on the tab can be sorted by clicking the column header:

- **Server IP Address** - IP address of the server
- **Client Bytes Read/sec** - Number of bytes received from Clients
- **Client Bytes Written/sec** - Number of bytes sent to Clients
- **Server Bytes Read/sec** - Number of bytes received from Servers
- **Server Bytes Written/sec** - Number of bytes sent to Servers
- **Accepted Client Connections** - Number of successful client connections.
- **Rejected Client Connections** - Number of client connections attempted that were rejected.

DMZ Gateway Logging

All logging functionality in DMZ Gateway comes preconfigured with the optimal settings. The information below is provided to help you understand what is in the logs. When necessary, modifying the configuration for the logging functionality should only be performed with the aid of Globalscape Customer Support.

The following logs are created and populated during the operation of DMZ Gateway:

- DMZ Gateway Communications Activity Log on page 38 (**DMZActivity.log**)
- DMZ Gateway Server Diagnostics Log on page 39 (**DMZGatewayServer.log**)
- DMZ Gateway Server Service Diagnostics Log on page 39 (**DMZGatewayServerService.log**)
- DMZ Gateway Statistics Log on page 39 (**DMZStatistics.log**)
- DMZ Gateway Server Event Viewer on page 40 (Windows Operating Systems Only)
- DMZ Gateway Server Syslog on page 40 (Solaris/Linux-based Operating Systems Only)

DMZ Gateway Communications Activity Logging

The DMZ Gateway communications activity logging records messages relating to communications to a W3C Extended Log File-formatted file. By default, this log file is created as **<installation directory>\logs\DMZActivity.log**. The format of the log file consists of a header at the beginning of the file and subsequent lines for each communications message generated by the DMZ Gateway Server. (Not all fields will be populated for every message. More information on the W3C Extended Log File format is available on the W3C Web site at http://www.w3.org/TR/WD-logfile.html.)

(The examples below are for illustration only and do not necessarily reflect your version or installation of DMZ Gateway.)

The header is of the format:

```
#Software: DMZ Gateway Server Version: 3.0.0 build 4
#Version: 3.0
#Date: 2009-09-28 07:31:48
#Fields: time status rs-ip rs-comment s-ip s-comment c-ip c-comment
```

where:

- Software – Identifies the application that generated the log file. In this case, the DMZ Gateway Server. This line will also contain the application version and build number of the DMZ Gateway Server.
- Version – The version of the extended log file format used.
- Date – The date and time the log file was initially created.
- Fields – The field names for the fields included in each log message. The fields are defined as:
    - time – The date and time the log message was generated
    - status – The status of the message where a value of 0 indicates a failure or error and a value of 1 indicates success.
    - rs-ip – The remote server IP Address and Port number. This represents the peer server connected to the Peer Notification Channel. This will typically be the EFT Server or Mail Express Server.
    - rs-comment – Textual status message related to the remote server.
    - s-ip – The server IP Address and port. This represents the DMZ Gateway Server.
    - s-comment – Textual status message related to the DMZ Gateway Server.
    - c-ip – The client IP Address and port. This represents the FTP client connection.
    - c-comment – Textual status message related to the client.

The verbosity of messages written to the communications activity log is configurable via the DMZ Gateway administration interface. By default, verbose logging is not enabled. When set to false, only basic communications initialization and de-initialization messages are logged to the activity log. This includes messages concerning Peer Notification Channel listener startups and stops. When verbose logging is enabled, additional communications messages concerning client connections are logged.

Essentially, messages that may occur throughout the course of operating the DMZ Gateway Server are governed by the "Verbose Activity Logging" setting whereas messages that only occur during initial startup and shutdown are always logged. The DMZ Gateway Server appends the log during each run of the DMZ Gateway Server.

The log file will automatically archive itself when reaching 10 MB in size and maintains the last 10 log files in the form **DMZActivity.<X>** where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Server Diagnostics Logging

The DMZ Gateway Server diagnostics logging functionality provides diagnostic-level messages for the operation of the DMZ Gateway Server. This diagnostic information may be used to identify errors, warnings, and other information of interest that occur during the operation of the DMZ Gateway Server.

By default this functionality logs to the file **<installation directory>\logs\DMZGatewayServer.log**.

The DMZ Gateway Server appends the log during each run of the DMZ Gateway administration interface. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form **DMZGatewayAdmin.<X>** where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Server Service Diagnostics Logging

This logging records diagnostic information generated by the DMZ Gateway Server service executable. The diagnostic information may be used to identify errors or warnings that occur during startup of the DMZ Gateway Server. By default, this functionality logs to the following file:

<installation directory>\logs\DMZGatewayServerService.log.

The DMZ Gateway Server appends the log during each run of the DMZ Gateway Server. The log file automatically archives itself when it reaches 10 MB in size and maintains the last 10 log files in the form **DMZGatewayServerService.log.<X>** where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Statistics Logging

Statistics logging is disabled by default, because statistics are typically viewed through the DMZ Gateway administration interface. When enabled, this functionality records various statistical data in CSV format to the log file **<installation directory>\logs\DMZStatistics.log**. A header row is generated at the beginning of each file and then data rows are periodically added for each Profile/Peer Server connection.

The statistical data includes the following fields:

- Timestamp – the date and time the row was generated
- Profile – the Profile to which the row of statistical data pertains
- Server – the Peer Server (e.g. EFT Server) to which the row of statistical data pertains
- Client Received (B) – the total number of bytes received from clients for the specified Profile/Server.
- Client Sent (B) – the total number of bytes sent to clients for the specified Profile/Server.
- Server Received (B) – the total number of bytes received from the Server for the specified Profile/Server.
- Server Sent (B) – the total number of bytes sent to the Server for the specified Profile/Server.
- Client Receive Rate (Bps) – the number of bytes per second received from clients for the specified Profile/Server.

- Client Send Rate (Bps) – the number of bytes per second sent to clients for the specified Profile/Server.
- Server Receive Rate (Bps) – the number of bytes per second received from the Server for the specified Profile/Server.
- Server Send Rate (Bps) – the number of bytes per second sent to the Server for the specified Profile/Server.
- Connections Accepted – the total number of connections allowed for the specified Profile/Server.
- Connections Refused – the total number of connections refused for the specified Profile/Server.

The log is appended during each run of the DMZ Gateway service. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form **DMZGatewayServerService.log.<X>** where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Server Event Viewer (Windows Operating Systems Only)

On Windows operating systems, DMZ Gateway records significant events to the Windows Event Log. Events originating from the DMZ Gateway are recorded in the Application Event Log and by default include the following types of events:

- DMZ Gateway Service start
- DMZ Gateway Service stop
- DMZ Gateway Service restart
- DMZ Gateway Service startup failures
- All FATAL and ERROR level diagnostic log messages recorded in the DMZ Gateway Server Diagnostics Log

Additionally, the startup and shutdown activities originating from the Windows Service Control Manager are recorded in the System Event Log.

DMZ Gateway Server Syslog (Solaris/Linux-based Operating Systems Only)

On Solaris and Linux-based operating systems, DMZ Gateway can record significant events in the local Syslog. By default, messages will be logged with an indent of “DMZ Gateway Server” to the LOG_USER facility and include the LOG_PID option. (Refer to http://www.kernel.org/doc/man-pages/online/pages/man3/syslog.3.html for information on the syslog functionality or type “man syslog” in a terminal window.)

On Solaris systems, it may be necessary to configure the syslog daemon to include logging of the LOG_USER facility. Typically, you can edit the **/etc/syslog.conf**file as root and add a line such as:

```
user.info <tab> /var/admin/message
```

Replace <tab> with an actual TAB character. This will instruct the syslog daemon to log LOG_USER facility messages to the **/var/admin/message** log file. After saving your changes, you will need to restart the syslog daemon as root with a command such as:

```
svcadm restart system-log
```

DMZ Gateway Administration Interface Logging

The following log files are created and populated during the operation of the DMZ Gateway administration interface:

- DMZ Gateway Admin Diagnostics Logging on page 41
- DMZ Gateway Admin Launcher Diagnostics Logging on page 41

DMZ Gateway Administration Diagnostics Logging

The DMZ Gateway administration diagnostics logging provides diagnostic-level messages for the operation of the DMZ Gateway administration interface. This diagnostic information may be used to identify errors or warnings that occur during the operation of the administration interface.

By default this functionality records to the file:

<installation directory>\logs\DMZGatewayAdmin.log

The log is appended during each run of the DMZ Gateway administration interface. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form **DMZGatewayAdmin.<X>** where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Admin Launcher Diagnostics Logging

This logging records diagnostic information generated by the DMZ Gateway Admin Launcher executable, **<installation directory>\bin\DMZGatewayAdminLauncher(.exe)**. This executable is responsible for starting the Java Virtual Machine and launching the DMZ Gateway administration interface. The diagnostic information may be used to identify errors or warnings that occur during startup of the administration application. By default this functionality logs to the file **<installation directory>\logs\DMZGatewayAdminLauncher.log**. This file is overwritten during every execution of the utility.

DMZ Gateway Headless Administration

Configuration and administration of the DMZ Gateway is typically performed using the DMZ Gateway administration interface. This interface runs local to the DMZ Gateway Server and uses a local-only TCP/IP connection to configure the DMZ Gateway Server and to obtain status and statistical information. Administrators of headless systems have the following options for configuring and monitoring the DMZ Gateway:

- Use a remote X11 server to display the administration interface
- Manually configure and monitor the DMZ Gateway Server through the file system

X11 Server Method

While the exact steps required to display the administration interface remotely may differ from system to system, the following steps are typical:

1. Ensure the X11 Server is running on the host system on which the user interface will be displayed.
2. Allow the DMZ Gateway computer access to the X11 Server using the xhost command. For example, issuing the following command in a terminal window on the host system will allow access to all incoming IP addresses:
   ```
   xhost +
   ```
3. Log in to the DMZ Gateway computer as a user with the appropriate permissions to run the DMZ Gateway administration interface.
4. Export the display to the host X11 server by issuing the following command in a terminal window:
   ```
   EXPORT DISPLAY=<Host IP>:0.0
   ```
5. Execute the DMZ Gateway Administration Interface script in a terminal window:
   ```
   <Installation Directory>/bin/DMZGatewayAdmin
   ```
   For example:
   ```
   /opt/dmzgateway/bin/DMZGatewayAdmin
   ```

Note that some Unix-based installations come preconfigured in a pure headless fashion and may lack the necessary X11 libraries required to display the administration interface remotely. Please consult your operating system documentation for information on installing the necessary libraries.

Manual Configuration Method

The DMZ Gateway Server may be configured by manually editing the DMZ Gateway Configuration file **gwconfig.xml**. For details on the configuration file, refer to DMZ Gateway Server Configuration File Reference on page 42.

It is highly recommended that the configuration be edited while the DMZ Gateway Server is ***not*** running; changes made to the configuration file will not take effect until the DMZ Gateway Server is restarted.

DMZ Gateway Server Configuration File (gwconfig.xml) Reference

The DMZ Gateway Server configuration file, **gwconfig.xml**, contains the main configuration settings governing communications through the DMZ Gateway Server.

The configuration file is in XML format and its contents are verified against a document type definition (DTD) file **gwconfig.dtd**.

Typically, the configuration items specified in **gwconfig.xml** will be edited via the DMZ Gateway administration interface. However, it is possible to edit the configuration settings using a text editor. Additionally, some advanced configuration items are not available via the DMZ Gateway administration interface and thus will require manual editing to configure.

Changes made to the configuration via manual editing will not take effect until the DMZ Gateway Server is restarted. Thus, the following steps should be followed:

1. Stop the DMZ Gateway Server service/daemon. on page 29
2. Edit the **gwconfig.xml** file using a text editor.
3. Save changes to the file.
4. Start the DMZ Gateway Server service/daemon on page 29.
5. Verify the DMZ Gateway Server has started and verify that no ERROR or FATAL messages are present in the DMZGatewayServer.log on page 39 diagnostics log file.

Configuration Validation

During startup, the DMZ Gateway Server will load the configuration file and validate its structure against the definition in the DTD file. It will also validate the various data constraints governing each element. If the configuration file format is invalid or the configuration violates any constraints, the DMZ Gateway Server will log an appropriate error message in the diagnostics log DMZGatewayServer.log on page 39 and shut down.

Configuration Elements

Please refer to the DTD file for the valid structure of the configuration file. The following describes the configuration elements available in the **gwconfig.xml** file.

- **ConfigurationVersion**

  The internal version number used to track the configuration file format. ***Do not edit.***

- **AdminPort**

  The DMZ Gateway administration interface communicates with the DMZ Gateway Server via a local-only TCP/IP communications port to conduct administrative tasks. This configuration item specifies the port to use for this communication path. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 0 to 65525.

  Setting the port to 0 instructs the operating system to randomly select an available port from its ephemeral port range.

  Setting the port to 1 through 65535 specifies an exact port. Care should be taken to ensure the specified port is not in use on the system.

  Default value: 0

- **AdminPortEnabled**

  The DMZ Gateway administration interface communicates with the DMZ Gateway Server via a local-only TCP/IP communications port to conduct administrative tasks. This configuration item allows the user to disable this communication path. Note that disabling the administration port will prevent use of the DMZ Gateway Administration Interface. The DMZ Gateway Server inherently only allows local connections via the administration port. This setting provides an additional level of security by allowing the operator to disable the administration port altogether once initial configuration has been completed. This setting is not configurable via the user interface and must be edited manually.

  Valid values:

  true - enable the administration port.

  false – disable the administration port.

  Default value: true

- **VerboseLoggingEnabled**

  Enables or disables verbose log messages in the DMZ Gateway Server communications activity log file, DMZActivity.log on page 38. This setting is configurable via the user interface.

  Valid values:

  true - enable verbose log output

  false – disable verbose log output

  Default value: false

- **GlobalPNCKeepalivePeriod**

  When a Peer Server application, such as the EFT Server, is connected to the DMZ Gateway Server via a Peer Notification Channel, keepalive functionality is used to verify that the communications channel is valid and alive. The keepalive functionality verifies the validity of the channel by periodically sending a message to the peer server and verifying that it receives a reply. This setting governs how often this check is performed for all Profiles. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 1 to 2^63 – 1, in milliseconds

  Default value: 30000
  (30 seconds)

- **StatisticsLoggingEnabled**

  The DMZ Gateway Server is capable of periodically logging statistical information to a statistics log file on page 39. This setting enables this logging functionality. This setting is not configurable via the user interface and must be edited manually.

  Valid values:

  true - enable statistics logging

  false – disable statistics logging

  Default value: false

- **StatisticsLoggingPeriod**

  This setting governs how often the current set of statistics within the DMZ Gateway Server is recorded in the statistics log file on page 39. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 1 to 2^63 – 1, in milliseconds

  Default value: 300,000(5 minutes)

- **Profiles**

  This element encloses 0 to 15 Profile elements. If no Profiles are specified in the configuration file, the DMZ Gateway Server will automatically create a default Profile during startup. If more

than 15 Profiles are defined, the DMZ Gateway Server will log the error during startup and subsequently shut down.

- **Profile**

  This enclosing element contains the configuration items defining a Profile. Profiles are configurable via the administration interface.

- **ProfileName**

  This is the name of the enclosing Profile. The name must be unique among all defined profiles. If the name is not unique, the DMZ Gateway Server will log the error during startup and subsequently shut down. Profile Names are configurable via the administration interface.

  Valid values: From 1 to 260 alphanumeric characters.

  Default value: Profile

- **ServerIP**

  This the IP Address of a local network adapter on which to listen for connections from peer servers on a peer notification channel. Server Listener IPs are configurable via the administration interface.

  Valid values: All or a specific IP address. When "All" is specified, the DMZ Gateway Server will listen on all IP address/port combinations on the local computer that are not already in use.

  Default value: All

- **ServerPort**

  This is the port to use with the IP address(es) specified in the ServerIP element to fully define the IP Address:Port combination on which to listen for connections from peer servers. Server listener ports are configurable via the administration interface.

  Valid values: 0 to 65535. When set to 0 the operating system will randomly select an available port from its ephemeral port range

  Default value: 44500

- **ClientIP**

  This the IP address of a local network adapter on which to listen for connections from clients. Client Listener IPs are configurable via the administration interface.

  Valid values: All or a specific IP address. When "All" is specified, the DMZ Gateway Server will listen on all IP address/port combinations on the local computer that are not already in use.

  Default value: All

- **PNCKeepalivePeriod**

  This element allows optional overriding of the GlobalPNCKeepalivePeriod on a per-Profile basis. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 1 to 2^63 – 1, in milliseconds

  Default value: 30000 (30 seconds)

- **NetworkAccessPolicy**

  This enclosing element contains the configuration settings for the IP access policy used to validate connections to the Peer Notification Channels of the enclosing Profile. The Network Access Policies for each Profile are configurable via the administration interface.

- **DefaultAccessPolicy**

  This is the policy to use by default when validating connections to the Peer Notification Channels of the enclosing Profile. The Default Access Policy for each Profile is configurable via the administration interface.

  Valid values:

  Grant – by default all connections will be granted access.

  Deny – by default all connections will be denied access.

  Default value: Grant

- **GrantPolicyExceptions**

  This element encloses 0 or more Exception elements that act as exceptions to the Grant All policy. Thus, they define what will be denied access. A maximum of 100 Exception elements may be defined. If more than 100 are defined, the DMZ Gateway Server will log the error during startup and subsequently shut down. The Grant Policy Exceptions for each Profile are configurable via the administration user interface.

- **DenyPolicyExceptions**

  This element encloses 0 or more Exception elements that act as exceptions to the Deny All policy. Thus, they define what will be granted access. A maximum of 100 Exception elements may be defined. If more than 100 are defined, the DMZ Gateway Server will log the error during startup and subsequently shut down. The Deny Policy Exceptions for each Profile are configurable via the administration user interface.

  Exception

  This element defines an exception to the enclosing Policy type. Exceptions are implemented as IP address masks that allow definition of masks that may be used to match the IP Address of a connecting peer server. The exceptions are configurable via the administration interface.

  Valid values: IP Address Masks match against IPv4 or IPv6 IP addresses

File Location

For new installs, the configuration file is created the first time the DMZ Gateway Server is started. When the configuration file is created, the corresponding DTD file is also created. By default, the configuration and DTD files are created in the DMZ Gateway installation directory. However, to facilitate sharing of configuration data in high availability clustered installs, an alternate shared data location may be specified.

Shared Configuration Location

An alternate shared data location may be specified either during the installation process or by subsequently editing the **DMZGatewayServerService.conf** file.

To specify the shared data location:

1. Stop the DMZ Gateway Server Service/Daemon. on page 29
2. Edit the **<Installation Directory>\conf\DMZGatewayServerService.conf** file using your preferred text editor.
3. Locate the following line in the file:

   ```
   set.DMZ_SHARED_CONFIG_DIRECTORY=""
   ```

4. Edit the line and enter the shared data location within the quotes, for example:

   ```
   On Windows: set.DMZ_SHARED_CONFIG_DIRECTORY="\\jupiter\DataShare\DMZGateway"
   On Solaris/Linux: set.DMZ_SHARED_CONFIG_DIRECTORY="/export/share/dmzgateway"
   ```

5. Save the changes to the file.
6. If you want to reuse the settings in the existing **gwconfig.xml** configuration file, move the file to the new location.
7. Start the DMZ Gateway Server Service/Daemon. on page 29

Please ensure that the operating permissions governing the DMZ Gateway Server service/daemon are set such that the process is able to access the specified shared configuration directory.

Note that the DMZ Gateway Server will automatically (re)generate the **gwconfig.dtd** DTD file in the specified shared data location. Additionally, for convenience, the file will also be generated in the installation directory.

Communicating with EFT Server or Mail Express Server

The topics in this section provide details of communication between DMZ Gateway and EFT Server or Mail Express Server.

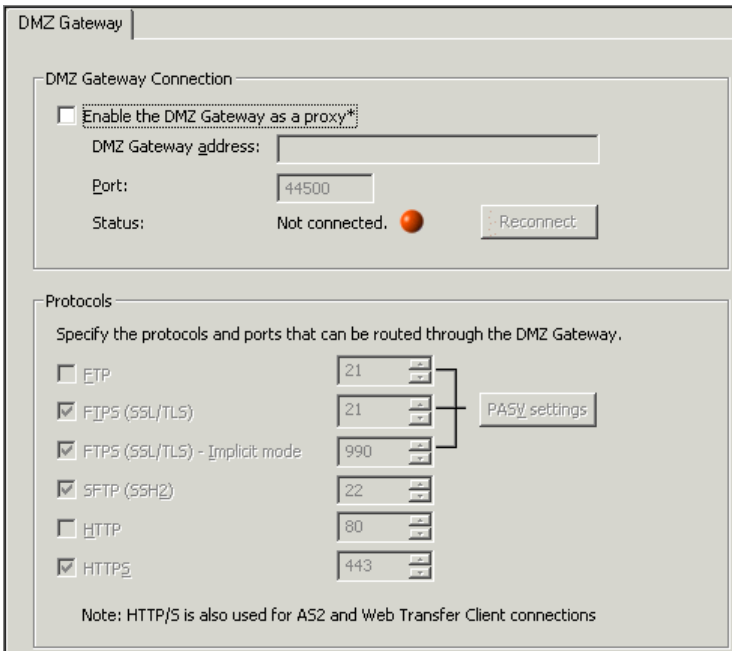
Enabling DMZ Gateway in EFT Server

You can enable DMZ Gateway when you create the Site or enable it later in the EFT Server administration interface. In the Site Setup wizard for both standard and High Security Sites, EFT Server displays the **Perimeter Security** configuration page that asks whether you will be using DMZ Gateway, and allows you to enter the DMZ Gateway IP address and port number. If **Connect this site to EFT Server's DMZ Gateway** is selected when you are creating a Site in the Site Setup wizard, EFT Server attempts to establish a socket connection to DMZ Gateway when you click **Next**.

- If the socket connection fails, a message appears in which you are allowed to provide the DMZ Gateway information again or disable DMZ Gateway and continue without it. (You can attempt to configure it again later.)
- If the socket connection is successful, EFT Server applies the settings and continues with Site setup.

To enable DMZ Gateway in EFT Server administration interface

1. In the EFT Server administration interface, connect to EFT Server and click the **Server** tab.
2. Expand the node of the Site you want to connect to DMZ Gateway, then click the **Gateway** node.
3. In the right pane, the **DMZ Gateway** tab appears.

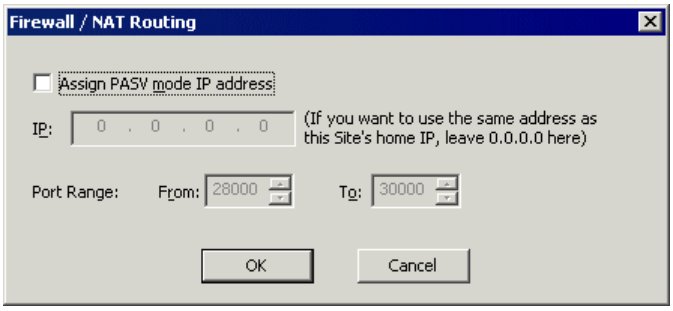


4. Select the **Enable the DMZ Gateway as a proxy** check box.
5. In the **DMZ Gateway address** box, specify the IP address of the DMZ Gateway to which you are connecting.
6. In the **Port** box, specify the port number over which EFT Server is to connect to DMZ Gateway. The default port is 44500.

   The connection will be refused if the IP address is on the server's IP Access\Ban list.
7. In the **Protocols** area, select the check boxes for the protocols and the ports that DMZ Gateway will use. These settings are separate from the ports that EFT Server uses. For example, you

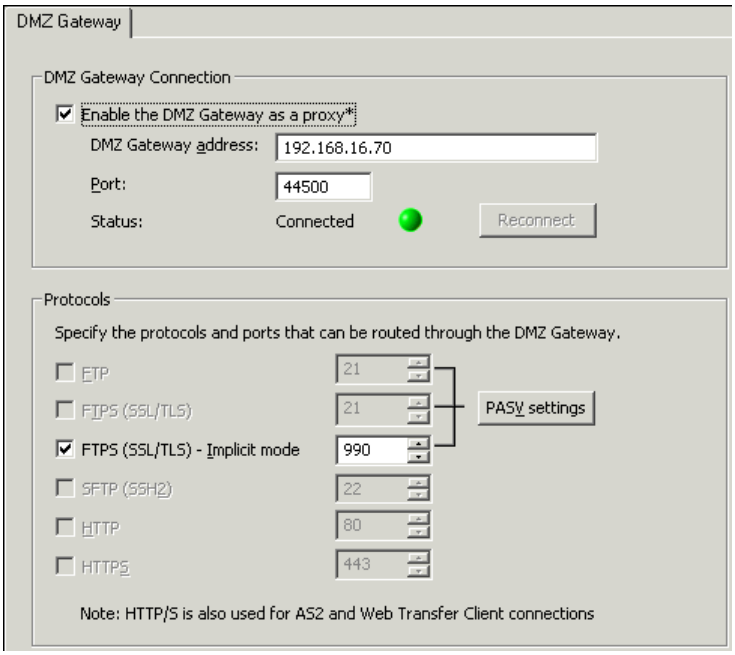
could use port 21 for FTP traffic directly to EFT Server, but port 14421 for FTP traffic through the DMZ Gateway.

8. If you are using DMZ Gateway with a PASV mode IP address, click **PASV settings**. The **Firewall/NAT Routing** dialog box appears.



   a. Select the **Assign PASV mode IP address** check box, then specify the IP address and port range.
   b. Click **OK**.

9. Click **Apply** to save the changes on EFT Server. If the settings are correct and the DMZ Gateway is configured properly, the connection status changes to **Connected** with a green icon.



If EFT Server cannot connect to DMZ Gateway, ensure that the EFT Server computer can connect to the DMZ Gateway computer by pinging it. Verify that the DMZ Gateway firewall is not blocking incoming connections.

10. You may need to establish a new connection with EFT Server by stopping and restarting connected Sites.
   a. In the left pane, click the Site node.
   b. In the right pane, click the **General** tab.
   c. Click **Stop**. The **Site Status** area displays "Stopped" with a red ball icon.
   d. Click **Start**. The **Site Status** area displays "Running" with a green ball icon.

Configuring the DMZ Gateway Connection in Mail Express

Using DMZ Gateway with the Mail Express Server allows administrators to limit access by allowing only outbound connections from the Mail Express Server via the firewall configuration. DMZ Gateway is designed to reside in the demilitarized zone and provide secure communication with the Mail Express Server behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ, and with no sensitive data stored in the DMZ, even temporarily. When configured to use DMZ Gateway, Mail Express functions normally, giving no indication to end users of the system that the additional piece has been added to the network. (Version 3.1 of Mail Express Server can connect to a network protected by DMZ Gateway v3.0.1 and later.)

The connection between Mail Express and DMZ Gateway is configured in the Mail Express administration portal. You must enable an outbound port from Mail Express Server to DMZ Gateway over which Mail Express Server is to connect to DMZ Gateway. By default, the Mail Express Server will connect to DMZ Gateway using port 44500. Mail Express only communicates over HTTPS, which uses port 443 by default for client-side connections.

In the DMZ Gateway interface, the Mail Express Server is considered a "Server" and the Mail Express DMZ Protocol Handler is considered a "Site" (e.g., in the DMZ Gateway **Status** pane). In the DMZ Gateway version 3.1.0, when communicating with Mail Express Server, "Mail Express Server" appears in the **Server Type** column. In earlier releases of DMZ Gateway, “[Unknown]” appears in the **Server Type** column.

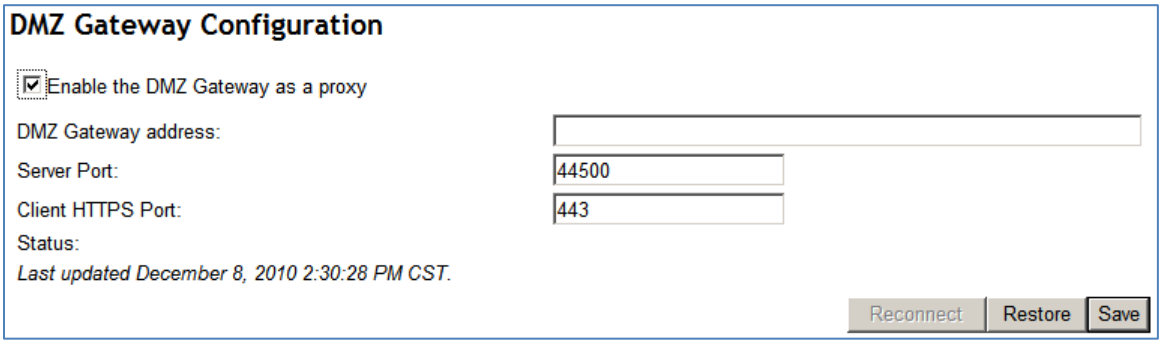
DMZ Gateway events are logged in the Mail Express Event log.

Before you can use DMZ Gateway with Mail Express Server, you have to provide Mail Express with the DMZ Gateway connection information.

To configure the DMZ Gateway information

1. In the Mail Express left navigation pane or on the Mail Express **Status** page, click **DMZ Gateway**. The **DMZ Gateway Configuration** page appears.

2. Select the **Enable the DMZ Gateway as a proxy** check box. The page expands to display more options.



3. In the **DMZ Gateway** address box, specify the hostname or IP address of the DMZ Gateway.
4. In the **Server Port** box, specify the port number used for server connections by DMZ Gateway (44500 by default).
5. In the **Client HTTPS Port** box, specify the port on which DMZ Gateway listens for incoming client connections. In the case of Mail Express, client connections will typically include external recipients picking up files via the Pick-Up portal and external users dropping off files via the Drop-Off portal.

- While the DMZ Gateway supports use of client ports other than port 443, it is highly recommended to use the default HTTPS port of 443 as this is the industry standard for HTTPS communications. When using the standard port, users will not have to specify a port value in the browser's URL if they are manually typing the URL to connect to a portal such as the Drop-Off portal.
- Using a non-standard client HTTPS listener port will require either adding the port to the **General Configuration** Hostname so that the port is included on links generated by the Mail Express system, or the networking infrastructure must be configured using port forwarding to redirect external HTTPS traffic to the configured Client HTTPS port on the DMZ Gateway computer.

6. Click **Save** to save the changes or click **Restore** to return to the previous settings.

If the connection to DMZ Gateway was lost (e.g., due to network errors), you can click **Reconnect** or wait 30 seconds for the Mail Express Server to automatically try to reconnect.

Routing AS2 Traffic through DMZ Gateway

Using the DMZ Gateway as proxy is available only in EFT Server Enterprise.

You can configure Event Rules to cause AS2 traffic to route through the DMZ Gateway using the **AS2 Send file to host** Action. You can use the **AS2 Send File to host** Action in the Folder Monitor, Timer, and all file-based Events.

To route AS2 traffic through DMZ Gateway

1. Create a new Event Rule, such as a File Uploaded event. (If necessary, refer to "Creating Event Rules" in the EFT Server documentation.)
2. Add the **AS2 Send file to host** Action to the Rule, then click the file or host link. The **AS2 Send File** dialog box appears.
3. In the **AS2 Send File** dialog box, specify trading partner profile to use or define the trading partner options.
4. Add the **Copy/Move File to Host** Action to the Rule.

5. In the **Rule** pane, click one of the undefined parameters (e.g., '%FS.PATH%'). The **Offload Action Wizard** appears.
6. Follow the instructions in Using DMZ Gateway as an Outbound Proxy on page 50 to define the Rule.

Using DMZ Gateway as an Outbound Proxy

DMZ Gateway's primary use is as an inbound proxy. Outbound connections that originate from EFT Server Enterprise will route through normal network mechanisms to reach the destination; however, it is possible to configure EFT Server's Event Rules using the **Copy/Move file to host** Action to use the DMZ Gateway Enterprise as an outbound proxy.

For instructions for configuring an Event Rule to use DMZ Gateway as an outbound proxy, refer to "Routing Outbound Traffic through a Proxy" in the EFT Server help documentation.

Testing the Configuration

After you have installed DMZ Gateway (on page 15), created and configured a Profile (on page 32), and enabled DMZ Gateway in EFT Server (on page 47) or Mail Express (on page 49), you can test your configuration by connecting to the server via DMZ Gateway and transferring a few files.

To test your configuration

Suppose your server is at IP address 192.168.174.176 and DMZ Gateway is at IP address 192.168.174.142, and you have configured DMZ Gateway in the server to allow connections over the HTTPS port 443.

1. Open a browser and in the address bar type `https://192.168.174.142` (the IP address of DMZ Gateway), then press ENTER.
2. You should be prompted to log in. Type the login credentials from a user defined on the server to which you want to connect.
3. Transfer a few files.
4. On the **Status** tab, you should see the numbers increase in the **Client Bytes Read**, **Client Bytes Written**, **Server Bytes Read**, and **Server Bytes Written** columns. Click **Refresh**, if necessary. (Note that if you connect to the server's IP address to transfer files, you are not going through the DMZ Gateway and, therefore, will not see any statistics change.)
    - With EFT Server, in the folder for the account that you used to log in (e.g., **C:\Inetpub\EFTRoot\GSSite\Usr\<username>**), you should see the files that you transferred.
    - With Mail Express, your recipient should receive a link in an email to the files you uploaded to Mail Express.
5. If you are not able to connect, refer to Troubleshooting DMZ Gateway Communication on page 51.

Troubleshooting DMZ Gateway Communication

Various configurations can prevent the server and DMZ Gateway from communicating. For example, if the DMZ Gateway computer's firewall is blocking connections, the server will not be able to connect to DMZ Gateway.

If the status icon in DMZ Gateway does not change color to green indicating a successful connection, verify the following:

1. Verify that the services for the server and DMZ Gateway are started.
2. If you make changes in DMZ Gateway, make sure to click **Apply Changes**. If necessary, in the server, stop and then restart the service (and/or the Site in EFT Server) after making changes.
3. If you made configuration changes in EFT Server, especially connection settings (protocols allowed, ports, etc.), make sure to stop and then restart the EFT Server service. Once restarted, make sure EFT Server is running (listening for new connections) and that DMZ Gateway remains enabled.
4. Verify that the IP address for the server is not blocked in DMZ Gateway's **IP Access Exception** list. By default, all IP addresses are granted access until you block or allow specific addresses. (Refer to Controlling Access by IP Address on page 35 for the procedure for blocking/unblocking IP addresses.)
5. Verify that the DMZ Gateway settings in the server on page 47 have the proper IP address and port and that the allowed protocols and ports have been defined for allowed incoming client connections.
6. Try pinging from the server computer to the DMZ Gateway computer and from the DMZ Gateway computer to the server computer. If you cannot connect, verify that there is no firewall that would block connections.

If a connection between the server and DMZ Gateway is indicated, but clients cannot connect to the server through DMZ Gateway:

Verify that you can connect to the server using a client account from within your network.

If connection is successful, but clients cannot connect through DMZ Gateway, something is not configured properly in the DMZ Gateway settings, either in DMZ Gateway or in the server. Verify that the server and DMZ Gateway are connected (see above) and that, in the server <--> DMZ Gateway configuration settings, the correct protocols and ports are specified for incoming client connections to the Gateway. These are the ports on which external clients will connect to DMZ Gateway. If no protocol is enabled or the wrong port is defined, clients will not be able to connect.

If connection fails, there is a configuration issue in the server. Review your configuration of user accounts and connection settings.

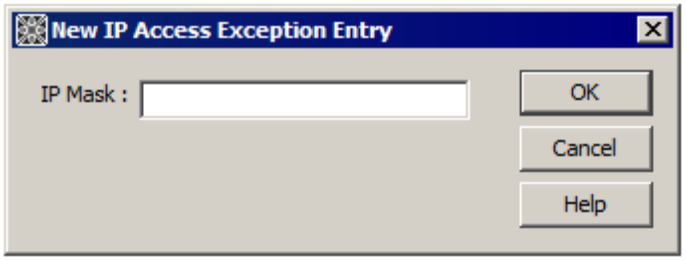
Interface Reference

The topics in this section describe the dialog boxes in DMZ Gateway that have **Help** buttons and provide a list of frequently used commands.

IP Access Exception Entry Dialog Box

Use the **New IP Access Exception Entry** dialog box and the **Edit IP Access Exception Entry** dialog box to provide a specific IP address (e.g., 192.168.43.201) or an IP address mask using wildcards (e.g., 192.168.43.*).

For example, if you want to allow only 192.168.174.159 and block every other IP address, click **Denied access**, click **Add**, then type `192.168.174.159` in the **IP mask** box. This will deny access to all IP addresses ***except*** 192.168.174.159.



To specify the IP address or mask

1. In the **IP Mask** box, specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.
2. Click **OK**. The IP address/mask appears in the exceptions list on the **Access** tab.

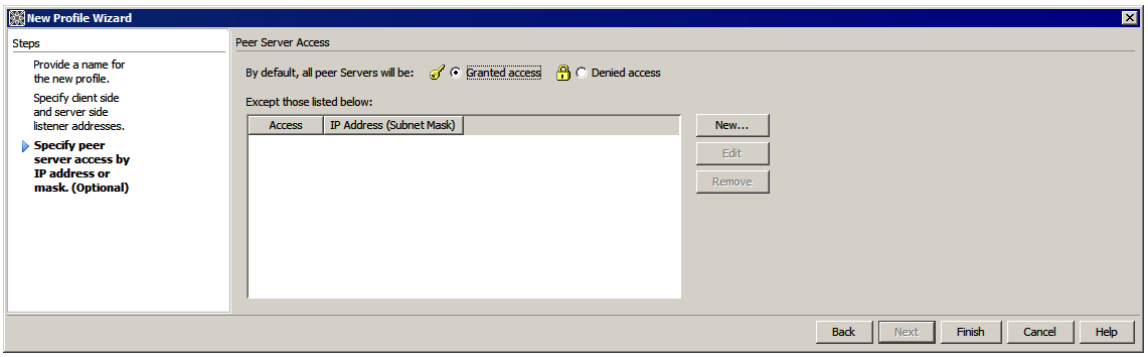
New Profile Wizard--Profile name

The New Profile Wizard is used to define a new Profile.

In the **Profile Name** box, provide a unique name for this Profile. The name will appear in the interface, logs, error messages, and reports.

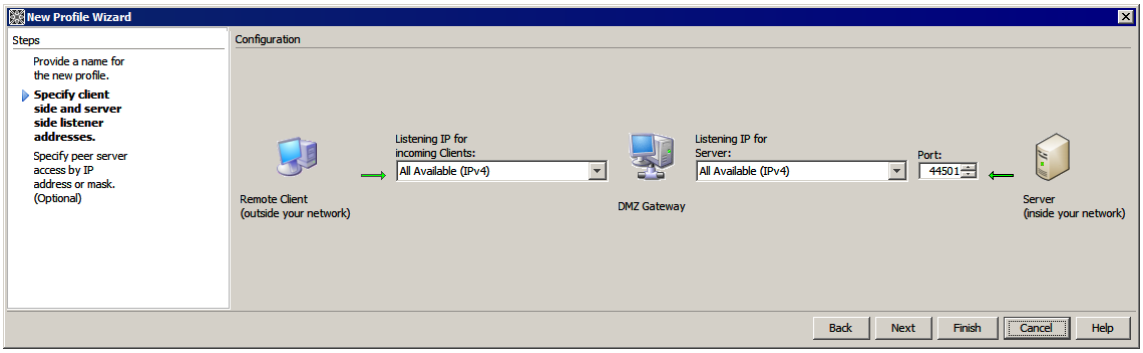
New Profile Wizard--Peer Server Access

Use the **Peer Server Access** page to specify the IP addresses or IP masks of peer servers who are allowed or denied access to DMZ Gateway. All IP addresses are granted access by default. Refer to IP Access Exception Dialog Box on page 53 for details.



New Profile Wizard--Configuration

Use the **Configuration** page of the wizard to specify which IP address/port combination on the DMZ Gateway computer should be used as the listening IP addresses.



To specify the client side and server side listening addresses

1. In the **Listening IP** boxes, click the down arrow to select the IP address or leave the default of **All Available**. Refer to Specifying the Listening IP Addresses on page 30 for detailed information.
2. In the **Port** box, specify the port on which DMZ Gateway communicates with the server. The default is **44500**. The connection will be refused if the IP address is on the IP address ban list.

Frequently Used Commands (non-Windows)

The table below describes several commands that you use to administer DMZ Gateway on non-Windows platforms. The commands are described in the applicable procedures in more detail; this table is provided only as a quick reference.

In the examples below, *your file and path names may differ.*

- Install on page 20

  Platform: All

  Example:

  ```
  gunzip dmz-gateway-linux-x86-32.tgz
  tar xvf dmz-gateway-linux-x86-32.tar
  ./Install.sh
  ```

- Register the script on page 23

  Platform: Redhat

  Example:

  ```
  chkconfig --add dmzgatewayd
  ```

  Platform: Suse

  Example:

  ```
  insserv dmzgatewayd
  ```

  Platform: Ubuntu

  Example:

  ```
  update-rc.d dmzgatewayd defaults
  ```

  Platform: Solaris

  Example:

  ```
  ln -sf /etc/init.d/dmzgatewayd /etc/rc0.d/K99dmzgatewayd
  ln -sf /etc/init.d/dmzgatewayd /etc/rc1.d/K99dmzgatewayd
  ln -sf /etc/init.d/dmzgatewayd /etc/rc2.d/S99dmzgatewayd
  ln -sf /etc/init.d/dmzgatewayd /etc/rc3.d/S99dmzgatewayd
  ```

- Deregister the script on page 23

  Platform: Redhat

  Example:

  ```
  chkconfig --del dmzgatewayd
  ```

  Platform: Suse

  Example:

  ```
  insserv -r dmzgatewayd
  ```

  Platform: Ubuntu

  Example:

  ```
  rm /etc/init.d/dmzgatewayd
  update-rc.d dmzgatewayd remove
  ```

  Platform: Solaris

  Example:

  ```
  rm /etc/rc0.d/K99dmzgatewayd
  rm /etc/rc1.d/K99dmzgatewayd
  ```

```
rm /etc/rc2.d/S99dmzgatewayd
rm /etc/rc3.d/S99dmzgatewayd
```

- Uninstall on page 25

  Platform: All
  Example:

  ```
  /opt/dmzgateway/bin/Uninstall.sh
  ```

- Open the DMZ Gateway Interface on page 28

  Platform: All
  Example:

  ```
  /opt/dmzgateway/bin/DMZGatewayAdmin
  ```

- Start DMZ Gateway Server service on page 29

  Platform: All
  Example:

  ```
  /opt/dmzgateway/bin/dmzgatewayd start
  ```

- Stop DMZ Gateway Server service on page 29

  Platform: All
  Example:

  ```
  /opt/dmzgateway/bin/dmzgatewayd stop
  ```

Licenses, Copyrights, and Release Notes

DMZ Gateway Release Notes

The DMZ Gateway release notes document is available in the installation folder as README.txt.

DMZ Gateway EULA

The license agreement is available in the installation folder as license.txt.

Index