

GlobalSCAPE® DMZ Gateway

User Guide

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/>

© 2004 GlobalSCAPE, Inc. All Rights Reserved

October 8, 2008

Table of Contents

The DMZ Gateway Server	5
Introduction to the DMZ Gateway Server	5
Peer Notification	5
Client Impersonation	6
DMZ Gateway Server Packet Forwarding	6
Securing DMZ Gateway Server Data	7
System Requirements for DMZ Gateway Server	8
Installing and Configuring DMZ Gateway Server	8
Installing DMZ Gateway in a Cluster	9
Prerequisites for DMZ Gateway in a Clustered Setup	10
Configure the DMZ Gateway Cluster	10
Set Up DMZ Gateways to Run in a Clustered Environment	11
Integrate DMZ Gateway into the Cluster	12
Complete Cluster Configuration and Test	12
Upgrading DMZ Gateway in a Cluster	13
Enabling DMZ Gateway in EFT Server	13
Managing DMZ Gateway Server	15
Routing Outbound Traffic through DMZ Gateway Server	16
Troubleshooting DMZ Gateway Server and EFT Server Communication	19

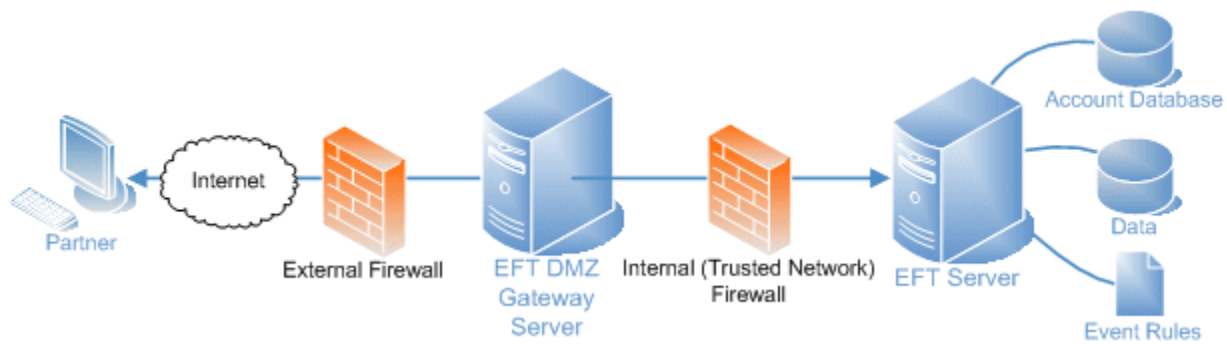
The DMZ Gateway Server

The topics below provide information for configuring and managing DMZ Gateway.

- [Introduction to DMZ Gateway](#)
- [Securing DMZ Gateway Data](#)
- [System Requirements for DMZ Gateway Server](#)
- [Installing and Configuring DMZ Gateway](#)
- [Enabling DMZ Gateway](#)
- [Managing DMZ Gateway](#)
- [Routing Outbound Traffic through DMZ Gateway Server](#)
- [Troubleshooting DMZ Gateway Server and EFT Server Communication](#)

Introduction to the DMZ Gateway Server

The DMZ Gateway Server is designed to reside in the demilitarized zone and provide secure communication with EFT Server behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ.



Peer Notification

EFT Server establishes peer notification channels with DMZ Gateway Server, and DMZ Gateway Server sends all data only through these channels. The peer notification channel (PNC) acts as a proxy for all transmission through DMZ Gateway Server; the result is that EFT Server behaves just as if it were in the DMZ, but it is actually safely behind the internal network firewall. The peer notification channel replaces the traditional inbound socket connection method for socket communications. EFT Server and DMZ Gateway Server communicate over a peer-notification channel using a proprietary protocol. Requests for client connectivity to DMZ Gateway Server are forwarded to EFT Server; EFT Server then opens connections to DMZ Gateway Server using a raw socket connection; the DMZ Gateway Server then pipes all data to the internal server using this socket without any translation. Thus, if the client is using HTTPS, then HTTPS traffic goes over that pipe.

There is no forwarding of client requests. The port that EFT Server and DMZ Gateway Server use to communicate with each other (4500 by default) is used for PNC communication and EFT Server -> DMZ Gateway Server sockets for the brokering of client connections. EFT Server specifies which ports on DMZ Gateway Server are used for the various protocols. For example, you could use port 21 for plaintext in the backend EFT Server using local traffic, but configure DMZ Gateway Server to listen to port 2112 for FTP

traffic. You could also enable ports and protocols on the backend server, but disable them on DMZ Gateway Server.

After restart or settings change, EFT Server determines whether a DMZ Gateway Server is configured. If so, EFT Server tries to establish a connection. After it connects, EFT Server assumes that DMZ Gateway Server exists and works correctly. In case of any error (e.g., connection refused, connection reset by peer, PNC protocol error) EFT Server reconnects.

It does not matter whether such errors occurred during connection initialization or later when transfers are taking place. That is, any connection error or PNC protocol error causes EFT Server to remove any existing connection objects and attempt to create a new PNC connection. This allows EFT Server to be independent of DMZ Gateway Server configuration. EFT Server starts working with DMZ Gateway Server as soon as DMZ Gateway Server is running and configured properly. EFT Server polls DMZ Gateway Server using the Connect() function while trying to maintain the PNC connection in a proper state. Any error causes a reconnect.

Client Impersonation

DMZ Gateway Server performs *client impersonation*, which means it replaces EFT Server's socket IP addresses and port settings with values taken from the connecting client socket. None of the sockets created through DMZ Gateway Server have the DMZ Gateway Server IP address and port; instead, all sockets created through DMZ Gateway Server have the IP address and port of the client connection. All information stored in logs or shown in the Administrator status pane have the actual connecting client IP addresses and ports.

Authentication is delegated to the backend EFT Server, as if the client were logging in directly to EFT Server from the internal network. DMZ Gateway Server essentially acts as a Layer 3 router and simply routes data from the client to EFT Server. Shown below is the general sequence. This sequence assumes that EFT Server has already established the Peer Notification Channel (PNC) to the DMZ Gateway Server.

1. Client makes socket connection to DMZ Gateway.
2. DMZ Gateway Server sends notification message to EFT Server using PNC.
3. EFT Server opens a new outbound connection to DMZ Gateway Server.
4. DMZ Gateway Server "glues together" the client socket with the EFT Server socket established in step 3.
5. DMZ Gateway Server routes data between client and EFT Server.
6. Client and EFT Server proceed as if the client were connected directly to EFT Server.

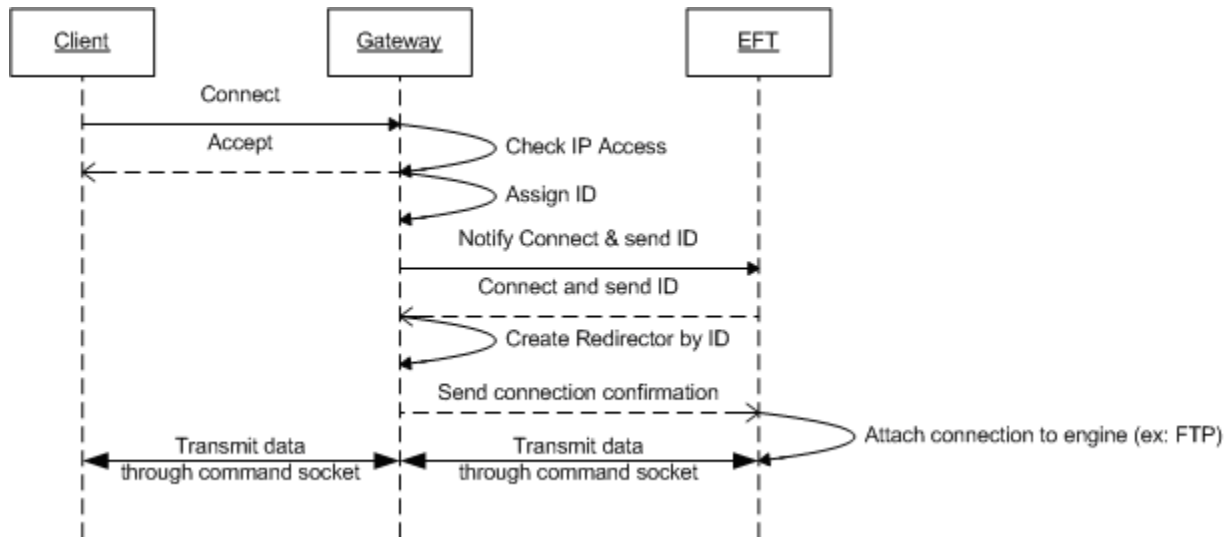
DMZ Gateway Server Packet Forwarding

DMZ Gateway Server is not a network hardware device like a bridge/router, so it does not "pass through" modified packets. The DMZ Gateway Server application (at the application layer) reads in a buffer full of data from the client TCP/IP stream (~4KB) and then sends that data over the server TCP/IP socket. They are completely different TCP/IP packets, with different source and destination locations. The headers, therefore, are different; depending upon the routes, the packet fragmentation, window size, and so on might be different, however, the payload is NOT changed at all.

Securing DMZ Gateway Server Data

DMZ Gateway Server allows or restricts incoming EFT Server Peer Notification Channel (PNC) connections based upon IP address. No username/password credentials are sent over the channel to establish the connection. The data over this channel is a binary header/payload message system with name/value pairs and serialized data. There is nothing sensitive contained in the PNC notifications that requires encryption.

The brokered sockets that "glue together" client connections to EFT Server are not encrypted unless you are using SSL- or SSH-based protocols. You should use SSL- or SSH-based protocols to encrypt sensitive information. If a client is using a plain text protocol to communicate to the EFT Server, then the path from the client to DMZ Gateway Server is in clear text, and the data traveling over the WAN is vulnerable to malicious users. Securing the data on the short path from DMZ Gateway Server to EFT Server provides little added security, because the route from the DMZ Gateway Server to the EFT Server is owned by the same enterprise, and not likely to have threats; however, if the client is connecting to the EFT Server using SFTP or an SSL-based protocol (FTPS or HTTPS), then the data is encrypted when it is sent to the DMZ Gateway Server, and the bytes are passed through to the EFT Server and to the WAN in that same encrypted format.



DMZ Gateway Server configuration is obtained only from EFT Server and used until changed at EFT Server. The configuration tells DMZ Gateway Server on which ports and IP addresses it should listen (e.g., 21, 22, 80), and which IP addresses are allowed access. The ports and IP addresses can be configured for each Site independently. EFT Server sends new configuration to DMZ Gateway Server, which restarts the listening sockets if needed. The configuration is never stored on DMZ Gateway Server.

If the PNC connection is broken, DMZ Gateway Server stops listening on all sockets and waits until EFT Server reconnects to the PNC. All existing sockets are not closed and continue working normally. Once EFT Server reconnects, DMZ Gateway Server restarts all listening sockets and continues operation.

System Requirements for DMZ Gateway Server

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

- Windows 2000, Windows XP Pro, or Windows Server 2003
 - *DMZ Gateway Server has known issues with Windows Vista or 2008 (planned support by Q4-08)*
- x86 compatible processor (tested with 600 MHz dual zeon to 3Ghz dual core)
- 1GB memory
- 1024x768 resolution or higher display

Installing and Configuring DMZ Gateway Server

After you install and configure DMZ Gateway Server, refer to [Enabling DMZ Gateway](#) for details of enabling the DMZ Gateway Server service to connect to EFT Server. You cannot enable DMZ Gateway Server in the Administrator until you have installed and configured DMZ Gateway Server as described below.

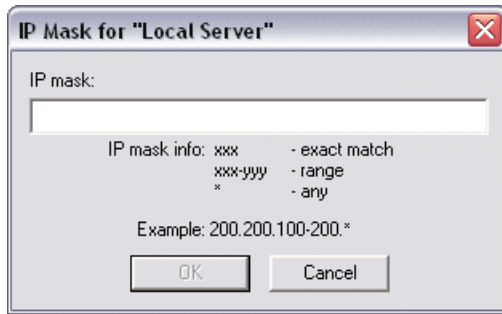


EFT Server and DMZ Gateway Server must be installed on separate computers.

To install and configure DMZ Gateway Server

1. Start the installation wizard (**EFTGateway.exe**) and follow the instructions in the wizard (i.e., accept the license agreement and specify an installation path if other than the default).
2. Click **Enter Serial Number** or **Enter Trial Serial Number** to provide the DMZ Gateway Server serial number, then click **Register**. The [EFT DMZ Gateway interface](#) appears.
3. In the **Server IP** box, specify the IP address the DMZ Gateway Server uses for connections with EFT Server or click **All Incoming**.
4. In the **Port** box, specify the port number that EFT Server and DMZ Gateway Server use to communicate with each other. The default is 44500. (For HS-PCI-enabled Sites, use a port number other than the default.)
5. In the **Client IP** box, specify the IP address the DMZ Gateway Server allows for client connections or click **All Incoming**.
6. In the **IP access rules for EFT Servers** area, you can limit which IP addresses can connect to the DMZ Gateway Server by granting or denying access to only one specific IP address or a range of IP addresses. By default, all IP addresses are granted access to EFT Server.
7. Do one of the following:
 - Click **Denied Access** to *allow* listed in the box below.
 - Click **Granted Access** to *deny* access to all peer EFT Servers except those listed in the box below.

- Click **Add**. The **IP Mask** dialog box appears.



- Type the IP address or range of IP addresses that you want to grant or deny access to EFT Server. You can also use wildcards to select ranges of IP addresses.
- Click **OK**.
- Click **Apply** to save the changes on DMZ Gateway Server. When you make changes to DMZ Gateway Server, you must [stop](#) and [restart](#) any Site connected to DMZ Gateway Server from EFT Server.

Installing DMZ Gateway in a Cluster

Set up DMZ Gateway in a clustered environment using Microsoft Clustering Services or GlobalSCAPE's monitoring utilities and achieve high availability through failover clustering.

If you have Microsoft Clustering Service (MSCS) deployed, you can use its built-in Resource Monitor to manage the availability of DMZ Gateway. MSCS can manage DMZ Gateway as a generic service.

Clustering setups vary between operating systems, hardware resources used, and various other factors. If you have never set up a server cluster before, please consult your Windows documentation or the Cluster Administrator help file for detailed instructions on setting up a server cluster prior to proceeding. The focus of these instructions is for setting up DMZ Gateway in a *pre-existing* clustered environment.

- To find out which hardware is compatible with MSCS, refer to Microsoft's hardware compatibility list at: <https://winqual.microsoft.com/default.aspx>
- To learn more about MSCS, search for "clustering" on the Microsoft Developer Network Library at: <http://msdn2.microsoft.com/en-us/library/default.aspx>
- For information about clustering on Windows 2003 Server, review the article "Introducing Microsoft Cluster Service (MSCS) in the Windows Server 2003 Family" at: <http://msdn2.microsoft.com/en-us/library/ms952401.aspx>
- Deploying DMZ Gateway in a clustered environment as described in this document is typically the most reliable method to achieve high availability and mitigate down time. For more information specific to clustering with DMZ Gateway, contact [GlobalSCAPE Customer Support](#).

Prerequisites for DMZ Gateway in a Clustered Setup

Operating System requirements

Microsoft Clustering Service as available on:

- Windows 2000 Advanced Server name service
- Windows Server 2003 R2 Enterprise Edition
- Windows Server 2003 Datacenter Edition

Hardware and resource requirements

- A complete system for each node of the cluster (minimum of two)
- A shared disk resource such as DAS, or SANS, preferably configured as a RAID-redundant array
- A disk quorum for disk and resource management; a minimum of two adapters per system (one for internal cluster communications, and another for public access)

Skill Set

A systems or network administrator familiar with the organization's structure and skilled in networking, Active Directory (AD), and cluster administration.

Configure the DMZ Gateway Cluster

Perform the steps below to configure clustering before setting up DMZ Gateway on the system.

1. Make sure the hardware is set up correctly and there is a shared disk resource, disk quorum, hub, or switch with Ethernet hookups between the two DMZ Gateways, as well as adapters for the crossover and for outside access, an adequate uninterruptible power supply (UPS) support for each device, and so on.
2. Make sure you install an operating system that supports clustering on each system. If available, give Internet access to each system because you will need to activate DMZ Gateway on each node. If you cannot provide Internet access, you will have to activate the product manually (see *Activating the Software*).
3. Install Active Directory (AD) and configure the domain name service (DNS) on the first node. Choose one of DMZ Gateways to be node 1. The administrator password cannot be left blank.
4. Create an account for the cluster in AD with a non-blank password and assign the account to the administrators group.
5. Join the second node to the AD domain as another domain controller. Both nodes must be domain controllers.
6. Reboot, then log in to the first node with the cluster account.
7. Launch the Cluster Configuration Manager from the **Add/ Remove Windows components** dialog box and create a new cluster.
8. Complete the new cluster creation wizard, providing a name for the cluster and cluster account credentials. Allow it to manage the disk, quorum, and other shared resources. Verify the quorum drive is correct, and select the private network option. Use one adaptor for the cluster nodes and the other for the public network. Specify the IP address for managing the cluster.

9. Run the cluster configuration tool on the second node and configure it to be an additional node in the cluster. You will need to provide the cluster name and appropriate cluster account credentials.
10. After you have completed the cluster configuration wizard, verify that the two nodes are set up properly from the cluster administrator dialog box. (To access the cluster administrator, click **Start > Programs > Administrative Tools > Cluster Administrator** .)
11. Select the **Resources** folder in the left pane, right-click, click **New > Resource** , then create the shared IP address on which the DMZ Gateways will listen. Note that DMZ Gateway captures the IP address when the DMZ Gateway service starts, so if the IP address is changed after that, the Service must be restarted to capture it.

Set Up DMZ Gateways to Run in a Clustered Environment



*If you are upgrading DMZ Gateway in a cluster, you **MUST bring down BOTH nodes BEFORE performing the upgrade. Refer to [Upgrading DMZ Gateway in a Cluster](#) instead of this topic.***

After you install and configure clustering on the system, perform the following procedure to configure DMZ Gateway in the cluster.

1. Install DMZ Gateway on the active node
2. Select the shared disk drive as the installation directory.
3. When the install completes, launch the product. Connect to DMZ Gateway using the Administrator account that you created during installation.
4. Activate the software in Full or Trial mode. Use your primary serial number if activating the primary node and your backup serial number if activating the backup node.
5. Once activated, exit the Administrator.
6. Open the **Services** dialog box (in Windows Administrative Tools), open the DMZ Gateway service **Properties** dialog box, then switch the startup mode from **Automatically** to **Manual** .
7. Stop the DMZ Gateway service, close the **Services** dialog box, and launch the Cluster Administrator.
8. In the Cluster Administrator, make the second node active: In the left pane, click **Groups** , right-click the appropriate cluster and disk groups, then click **Move Group** . All resources should move from the first node over to the second node so that the second DMZ Gateway installation succeeds. If not, the shared disk will lock for the second node. It may take a few moments for the resources to switch over.
9. Install DMZ Gateway on the second node once it is active (also to the shared directory), following steps above, and then exit the **Services** dialog box without stopping the DMZ Gateway service.
10. Launch the Administrator, connect to the DMZ Gateway service on the second node, and configure DMZ Gateway.

Integrate DMZ Gateway into the Cluster

DMZ Gateway configuration should now be identical for both DMZ Gateways because both are using the same configuration file stored on the shared disk, are saving data to the same place, and share the same outside-facing IP.

To integrate DMZ Gateway into the cluster

1. Open the cluster administrator. In the left pane, right-click the **Resources** folder, click **New Resource**, expand the **Create New Resource** list, then click **Generic Services**.
2. Choose both nodes, select all resources as dependencies, then type the exact service name as displayed in the Windows **Services** dialog box (**GlobalSCAPE EFT Gateway**; It must be exact, including case.) Do not choose to replicate the registry settings.
3. Click **Finish** to add the service as a resource.

Complete Cluster Configuration and Test

You should now have both nodes configured with shared resources, including a shared IP address, disk array, quorum, and two DMZ Gateways. Perform tests to ensure the system was correctly configured.

1. In the Cluster Manager, right-click the "GlobalSCAPE EFT Gateway" service, then click **Bring online**.
2. Open the DMZ Gateway Administrator. Verify that it is online.
3. In the Cluster Manager, right-click "GlobalSCAPE EFT Gateway service" then click **Bring Offline**.
4. Verify in DMZ Gateway Administrator that the service is stopped (the play button for the service will become available).
5. Cause a failover to confirm the service can be started on each node automatically.
6. Configure EFT Server to connect to DMZ Gateway using the cluster IP address (IP address that the cluster shares).
7. Verify that the DMZ Gateway Administrator has a green light (to show that EFT Server is connected).
8. Verify that the failover allows EFT Server to continue to be connected to a DMZ Gateway in the cluster.

Your cluster setup is now complete.



If one DMZ Gateway goes down, you lose any transactions in progress until the failover goes online.

Upgrading DMZ Gateway in a Cluster

If you are upgrading a DMZ Gateway that is part of a cluster, follow the procedures below.

To upgrade DMZ Gateway in a cluster

1. Obtain new installation file(s)
2. Bring down the cluster (from within the cluster manager).
3. **It is critically important that DMZ Gateway service is STOPPED on both nodes! Verify that DMZ Gateway service is stopped by logging in to each node and inspecting the service control panel. For extra assurance you can change the startup type to Manual from Automatic. (Make sure to switch it back before you bring the cluster back up in step 8 below.)**
4. Run the installer on the first node and select **Repair** when prompted. (Do NOT click **Modify**.)
5. Run the installer on the second node and select **Repair** when prompted. (Do NOT click **Modify**.)
6. If you changed DMZ Gateway service startup to **Manual** in step 4, change it back to **Automatic**.
7. Bring the cluster back up.
8. Verify the upgrade was successful:
 - a. Verify that DMZ Gateway is running on the primary node.
 - b. Disable the primary node and verify secondary node starts up.
 - c. Open the DMZ Gateway Administrator interface and verify that the version number is the same on both nodes (click **Help**, then click **About**).

Enabling DMZ Gateway in EFT Server

In the [Site Setup wizard](#) for both standard and HS-PCI-enabled Sites, EFT Server displays the **Perimeter Security** configuration page that asks whether you will be using DMZ Gateway Server, and allows you to enter the DMZ Gateway Server IP address and port number. If **Connect this site to EFT Server's DMZ Gateway Server** is selected, EFT Server attempts to establish a socket connection to DMZ Gateway Server when you click **Next**.

Optional DMZ Gateway Configuration

PCI DSS requirement 1.3.4 explicitly forbids the storage of cardholder data in the demilitarized zone (DMZ). For security best practices, you should not store confidential data in your perimeter network.

GlobalSCAPE DMZ Gateway facilitates secure connections from the DMZ to your internal network, *never* storing data in the DMZ. If you are using DMZ Gateway, provide the listening IP address and port below:

Connect this Site to EFT Server's DMZ Gateway

IP Address: Port:

Continue without configuring the DMZ Gateway

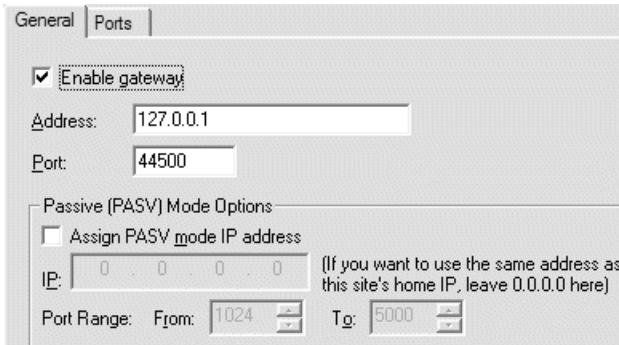
Note: Any explanation, justification, or compensating controls documented will be audited and included in EFT Server's PCI DSS compliance report.

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

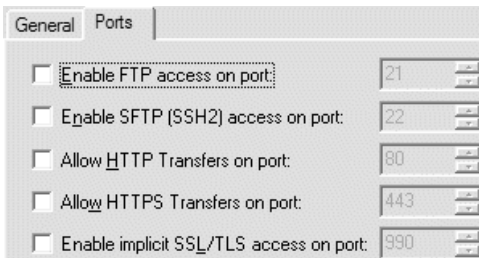
- If the socket connection is successful, EFT Server applies the settings and continues with Site setup.

To enable DMZ Gateway Server in EFT Administrator

1. In EFT Administrator, [connect to EFT Server](#) and click the **Server** tab.
2. Click the node of the Site you want to connect with the DMZ Gateway Server, then click **Gateway**.
3. In the right pane, click the **General** tab.



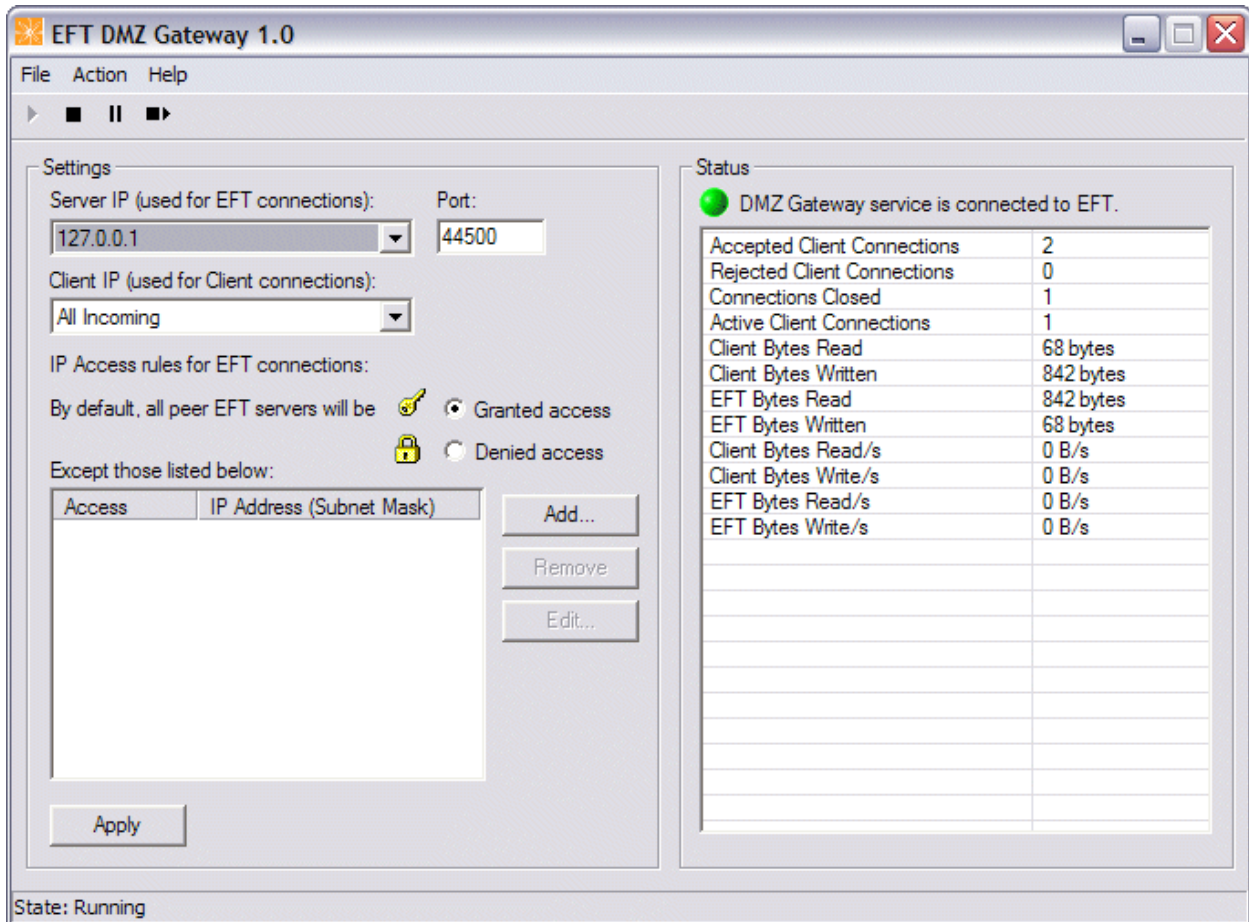
4. Select the **Enable Gateway** check box.
5. Type the IP address and the port number of the DMZ Gateway Server to which you are connecting.
6. Click the **Ports** tab.



7. Select the check boxes for the protocols and the ports that DMZ Gateway Server will use. This is a separate configuration from the ports that EFT Server uses. For example, you can use port 21 for FTP traffic for EFT Server, but port 1465 for FTP traffic through the DMZ Gateway Server.
8. Click **Apply** to save the changes on EFT Server.
9. Re-establish a new connection with EFT Server by stopping and restarting connected Sites.

Managing DMZ Gateway Server

After DMZ Gateway Server is installed and configured, you can view statistics of the DMZ Gateway service in the **Status** pane. The **Status** pane in the DMZ Gateway Server interface shows the size of items transferring through DMZ Gateway Server, and indicates if DMZ Gateway Server is connected, not connected, running, or not running.



Other statistics displayed include:

- Accepted Client Connections
- Rejected Client Connections
- Connections Closed
- Active Client Connections
- Client Bytes Read
- Client Bytes Written
- EFT Bytes Read
- EFT Bytes Written
- Client Bytes Read/s
- Client Bytes Written/s
- EFT Bytes Read/s
- EFT Bytes Written/s

You can start, pause, restart, or stop the DMZ Gateway Server service on the DMZ Gateway Server main menu or toolbar.

In the Windows **Services** dialog box, the service is called **GlobalSCAPE EFT Gateway**, and in the Task Manager, it is called **GWService.exe**. The DMZ Gateway interface is called **GWAdmin.exe** in the Task Manager.



When you make changes to DMZ Gateway, you must [stop](#) and [restart](#) any Site connected to the Gateway.

To start the DMZ Gateway Server

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

To pause the DMZ Gateway Server

- On the DMZ Gateway main menu, click **Action > Pause** or click **Pause ||** on the toolbar.

To restart the DMZ Gateway Server

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

To stop the DMZ Gateway Server

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

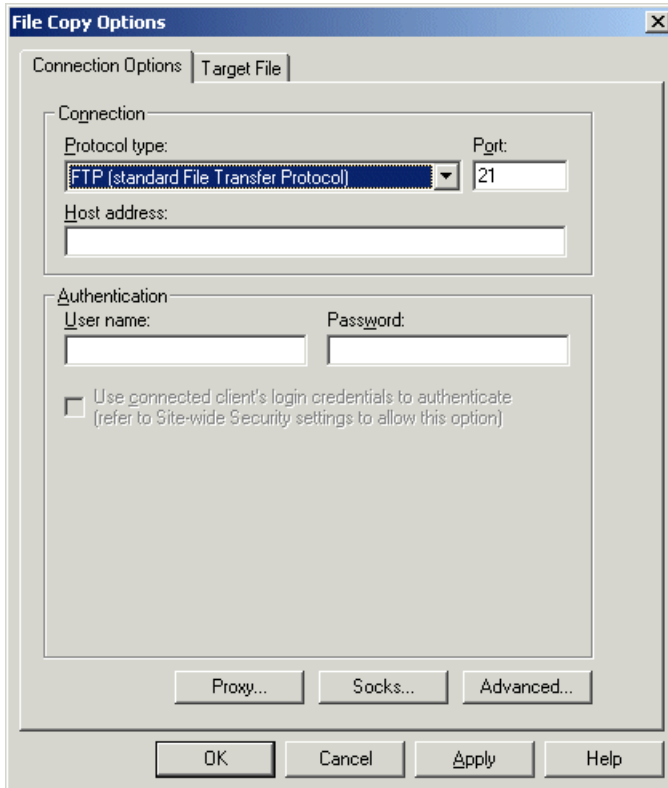
Routing Outbound Traffic through DMZ Gateway Server

DMZ Gateway Server's primary use is as an inbound proxy. Outbound connections that originate from EFT Server 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 Server as an outbound proxy.

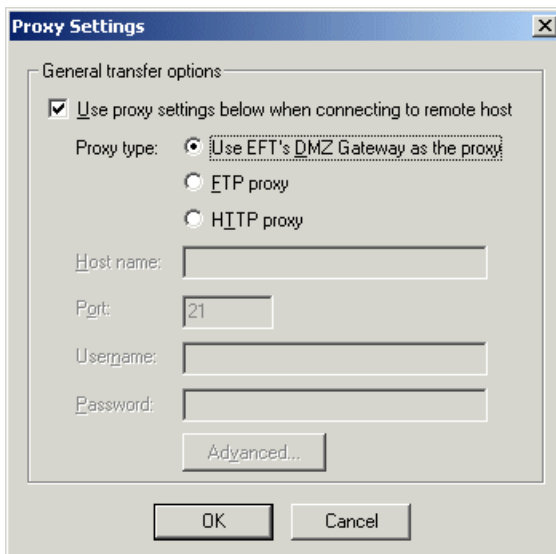
To configure an Event Rule to use DMZ Gateway Server as an outbound proxy

1. In the EFT Administrator, create an Event Rule, such as a [Scheduler \(Timer\) Event](#).
2. Add the [Copy/Move File to Host Action](#).

- In the Action that you added to the rule, click **Copy**. The **File Copy Options** dialog box appears.

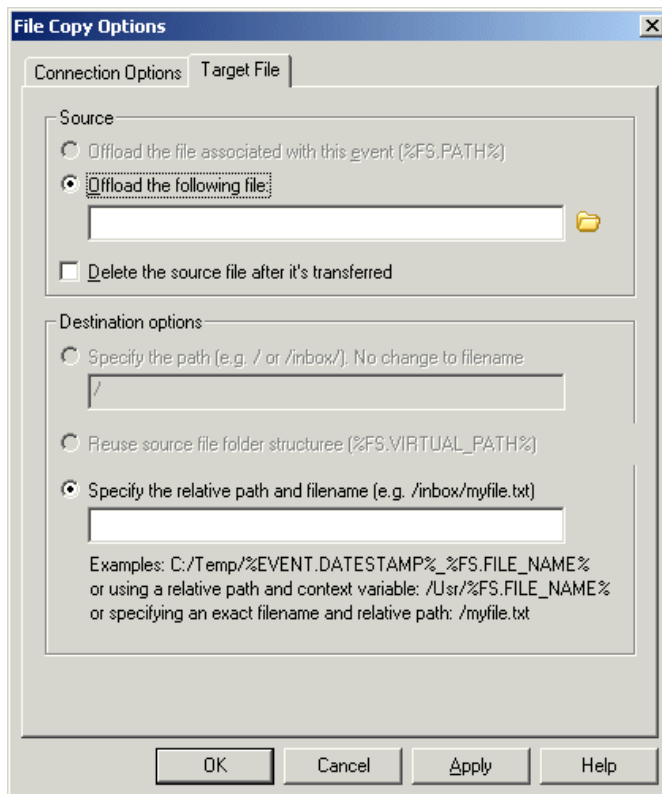


- In the **Host address** box, type the address of the remote host to which you want to offload files.
- In the **Authentication** area, type the **User name** and **Password** required to access the remote host.
- Click **Proxy**. The **Proxy Settings** dialog box appears.



- Select the **Use proxy settings below when connecting to remote host** check box, click **Use EFT's DMZ Gateway as the proxy**, then click **OK** to close the **Proxy Settings** dialog box.

8. In the **File Copy Options** dialog box, click the **Target File** tab.



9. In the **Offload the following file** box, type or click the open icon to specify the file that you want to copy to the remote host. Optionally, click the **Delete the source file after it's transferred** check box.
10. In the **Destination options** area, specify the relative path and filename or variable.
11. Click **OK**.
12. Optionally, add an [e-mail Notification Action](#) to notify you when the Rule is triggered.
13. Click **Apply** to save the Rule on the Server.

Troubleshooting DMZ Gateway Server and EFT Server Communication

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

1. Verify the services for both EFT Server and DMZ Gateway Server are started. (Look in the Services dialog box in the Windows Control Panel or the Task Manager.)
2. If you make changes in DMZ Gateway Server, make sure to click **Apply**. If necessary, stop and then restart the service after making changes.
3. Verify the IP address for EFT Server is not blocked in DMZ Gateway Server's **IP Access Exception** list. By default all IP addresses are granted access until you block or allow specific addresses. (Refer to [Installing and Configuring DMZ Gateway](#) for the procedure for blocking/unblocking IP addresses.)
4. Verify EFT Server can reach the IP address that DMZ Gateway Server is listening on.
5. 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 the Gateway remains enabled.
6. Verify the [DMZ Gateway Server settings in EFT Server](#) have the proper IP address and port for the gateway and that the allowed protocols and ports have been defined for allowed incoming client connections to DMZ Gateway Server.

If a connection between EFT Server and DMZ Gateway is indicated, but clients cannot connect to EFT Server through the Gateway, check the following:

1. Verify that you can connect to EFT Server using a client account from within your network.
2. If successful, it indicates something is not configured properly in the DMZ Gateway settings, either in DMZ Gateway Server or in EFT Server. Verify that EFT Server and DMZ Gateway Server are connected (see above) and that, in the EFT Server 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 the gateway. If no protocol is enabled or the wrong port is defined, clients will not be able to connect to the gateway.
3. If it fails, then it is a configuration issue in EFT Server. Review your configuration of [user accounts](#) and [connection settings](#).