Running DMZ Gateway as non-root user in Linux

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- DMZ Gateway, version 3.0.0 and later

DISCUSSION

By default, DMZ Gateway installed on Linux runs as **root**, because the install script must itself be run as root. Good security practices require each server to run as its own user account, though, to isolate and protect sensitive information and services.

Although the installer prompts for optional user information during the installation process, this is ***not*** altering the user account under which the service runs; instead, it is simply setting the group and owner for the installed files.

To run the DMZ Gateway as non-root user after installing the DMZ Gateway:

1. Create a non-root user account on the server (be sure to set up a home folder for that user account as well). Establish a strong password for that user account. (e.g., a user "dmzgatewayserver" with home folder "/home/dmzgatewayserver")
2. Locate the installation folder (default "/opt/dmzgateway") and change ownership to the user account you created in step #1 (e.g., "sudo chown dmzgatewayserver /opt/dmzgateway")
3. Ensure that the owner has write access to that folder (required to create .pid and log files) (e.g., "sudo chmod 744 /opt/dmzgateway")
4. Edit the server daemon init script, "dmzgatewayd" (e.g., "sudo vi /opt/dmzgateway/dmzgatewayd")
5. Find the line reading "#RUN_AS_USER=" and remove the initial comment marker, "#", and append the name of the user created in step #1 above after the equals sign (e.g., the line becomes ("RUN_AS_USER=dmzgatewayserver")
6. Now you may start (or restart) the DMZ Gateway Server service to have it run as the designated user (e.g., "sudo service dmzgatewayd start"). If you encounter any errors, look in the log files found in the "Logs" subfolder of the installation directory.

NOTE!!!!

When you run the DMZ Gateway Server service as a non-root user, the server can no longer bind to low number ports like 21, 22, 80, and 443. If the paired EFT Server attempts to direct the DMZ Gateway to listen on those ports, it will fail.

Running DMZ Gateway as non-root user in Linux

To resolve this, you must:

1. Configure iptables on the DMZ Gateway machine to listen on the desired public facing TCP ports (like 21, 22, 80, and 443) and redirect them to high number ports on which DMZ Gateway can listen (e.g., 8021, 8022, 8080, and 8443).

   For example,

   iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8443

   (this works under Linux kernel 2.3, 2.4, 2.5 and 2.6)
2. Configure the EFT DMZ Gateway options to direct the DMZ Gateway to listen on those higher number ports to receive client traffic (e.g., 8021, 8022, 8080, and 8443). Be sure that you configure both **iptables** and EFT DMZ Gateway options to have the same port numbers.

This will cause the Linux OS to redirect traffic on the low ports to those ports DMZ Gateway is listening on, resulting in traffic properly routing to/from the EFT Server.

Refer to https://kb.globalscape.com/KnowledgebaseArticle11201.aspx for other DMZ Gateway configuration settings.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11206/Running-DMZ-Gateway-as-non-r...