If DMZ Gateway Server hands all traffic to EFT on the inside network, wouldn’t this be seen as a risk and defeat the objective of having the DMZ Gateway broker connections?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT (All Versions)
- DMZ Gateway

QUESTION

If DMZ Gateway Server hands all traffic to EFT on the inside network, wouldn’t this be seen as a risk and defeat the objective of having the DMZ Gateway broker connections?

ANSWER

If you configure the **IP Access Restriction list** on EFT, DMZ Gateway blocks the traffic on those IP addresses, including IP addresses added to the "Auto-Ban" list for traffic sensitivity. In other words, on EFT, if you block IP addresses (or if they automatically get added to the blocked list for banned IPs), DMZ Gateway blocks the traffic at the gateway and does NOT forward the "garbage" traffic on to EFT Server. In this way, DMZ Gateway supports the "Anti-DOS/Flooding" capability of EFT.

DMZ Gateway only restricts connections based on IP address. Any other form of packet analysis requires decrypting the traffic at the DMZ Gateway, thereby negating the advantage of End-to-End security between client and server. DMZ Gateway is a connection broker, not a firewall, packet inspector, IPS (Intrusion Prevention System), or anything like that.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10367/If-DMZ-Gateway-Server-hands-...