Sender and Recipient Filtering Outbound

https://campus.barracuda.com/doc/39819728/

If any of the computers in your organization get infected with a botnet or other malware, it can send out spam emails, thereby possibly landing your domain(s) or IP address(es) on a blocklist, not to mention spreading the malware. Use the **BLOCK/ACCEPT > Sender Filters** page to control which domains and email addresses can send email out through the Barracuda Email Security Gateway. Note that both inbound and outbound email messages from whitelisted ("allowed") domains/subdomains bypass spam scoring as well as all other blocklists, but do go through virus checks.

> Adding your own domain to the sender whitelist is not allowed because spoofing the domain of the recipient is a frequently used spamming technique. Instead, add the IP address of your mail server(s) to the Allowed IP/Range list using the **BLOCK/ACCEPT > IP Filters** page.

Email addressed from specified email addresses and domains/subdomains can also be encrypted or redirected from the **BLOCK/ACCEPT > Sender Filters** page.

Outbound email addressed to specified email addresses (recipients) or domains/subdomains can also be allowed, blocked, encrypted or redirected from the **BLOCK/ACCEPT > Recipient Filters** page.

For more information about email encryption and redirection, see Encryption of Outbound Mail 6 and Above.