Reverse Proxy Configuration for Mobile Data Collection – On Premise Server Implementations

Last Modified on 08/02/2022 12:56 pm EDT

Q – Does PoliteMail need external connectivity (outside the firewall) to get mobile enabled?
A – No, however PoliteMail does require certain https traffic from the internet to reach the PoliteMail Server.

The bottom line is that HTTPS traffic originating from the mobile device has to reach the PoliteMail Server for it to be measured.

This **DOES NOT** require external connectivity from the PoliteMail Server to the internet, however it does require allowing certain https traffic from the internet to reach the PoliteMail Server.

Technically, this is accomplished using a **Split DNS** configuration with a **Reverse Proxy**.

These are not PoliteMail concepts or technologies. The details regarding the configuration of the Split DNS and Reverse Proxy is wholly dependent upon a **client's network topology**; local hostnames, IP addresses, and other information that PoliteMail cannot access.

Most customers will have an F5 or Netscaler device in the DMZ, which will be configured to handle the inbound traffic and function as the proxy.

Split DNS is a concept that allows a hostname to resolve to one IP address on the internal network, and another on the external network. The configuration of split DNS depends upon what you use for your DNS Server. Here is an article that explains one method of using Windows Server 2016 as your DNS server: https://blogs.technet.microsoft.com/networking/2015/05/12/split-brain-dns-deployment-using-windows-dns-server-policies/

Reverse Proxy is a concept that allows external traffic to reach an internal host, without exposing that host to the public internet.

- X = mobile device, or "client" computer on the internet
- Y = the reverse proxy web site, proxy.example.com
- Z = the PoliteMail Server website, pm.example.com

With direct web access, one would connect directly from X –> Z.

However, is it more secure for the administrator of Z to restrict or disallow direct access. Because you do not want to expose the PoliteMail Server and it's hosted content directly to the public – you will force external visitors to go through Y first.

So there is data being retrieved by Y –> Z on behalf of X, which chains as follows: X –> Y –> Z.

The user X does not know he is accessing Z, because the user X only sees he is communicating with Y. The server Z is invisible to clients and only the reverse proxy Y is visible externally. A reverse proxy requires no (proxy) configuration on the client side.

Additionally, firewall rules can be applied between Y and Z, to further limit the traffic to acceptable patterns and reject all other traffic.