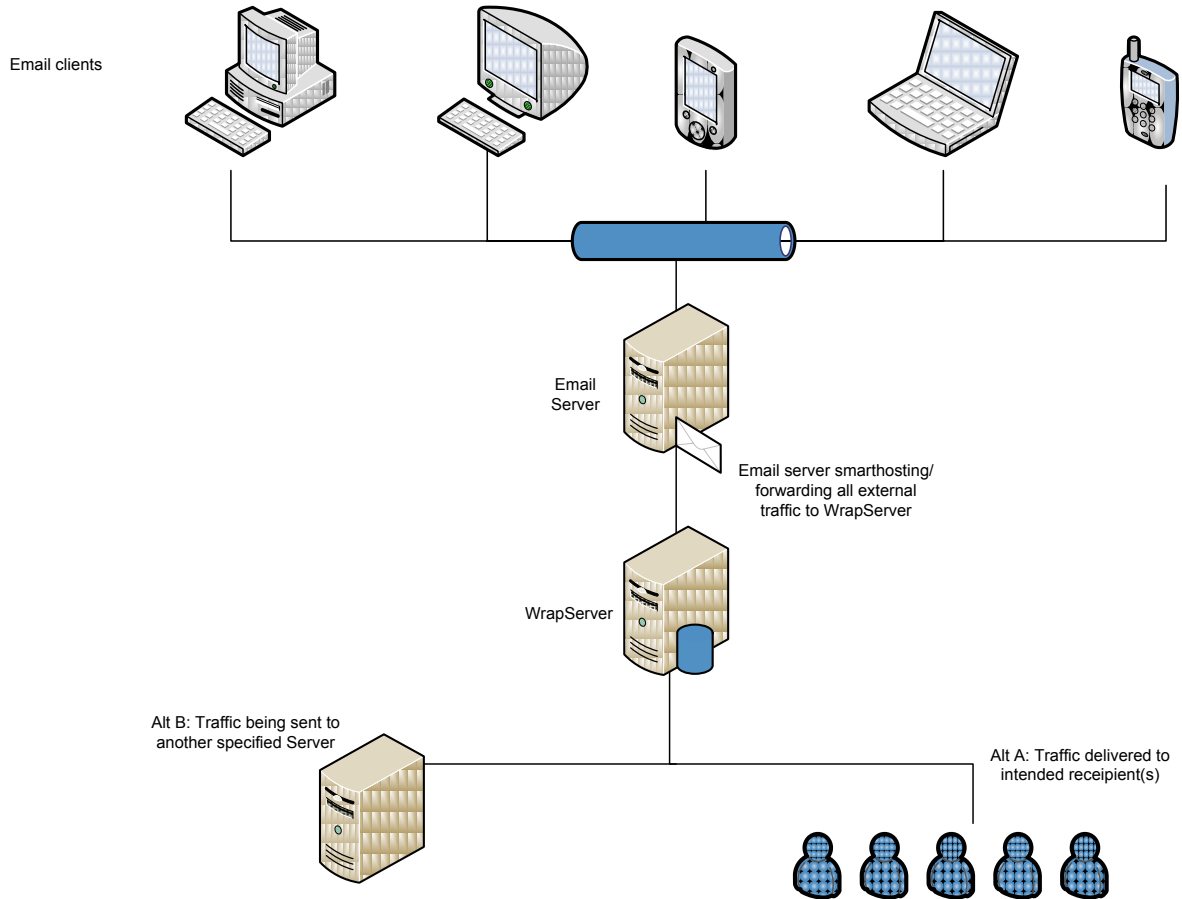


WrapMail Enterprise Overview



Explanation:

Emails originate from a user on any device capable of sending an email. Users do not change anything in their email client. All emails go to the Email Server which is set up to forward all **external** emails to a WrapServer. The WrapServer adds the appropriate “wrap” and either forwards the email to the next server in the chain (client choice) or delivers the email directly to the intended recipient(s).

WrapServer:

The dedicated WrapServer is hosted by client or in WrapMail’s hosting center (option). WrapMail does not provide hardware unless hosted by WrapMail. **Requirements for the WrapServer are 1GB RAM and 60GB HDD (allocated if a virtual server) and Windows 2003 Server Software.**

For clients with multiple Email servers there should be a 1:1 relationship between Email servers and WrapServers.

WrapMail ports (preferably via VPN) the WrapMail Software onto the WrapServer.

The WrapServer has monitoring programs installed as part of the WrapMail solution and these programs have alarms as far as heartbeat (60 seconds) and queue size (queue size alarms settings are set based upon historic traffic data). Alarms are sent via both SMS and Email.

In an unforeseen situation where the WrapServer does not respond then Emails should not be lost as they will queue up on the Email server. The typical solution is to reverse the smarthost/forwarding so all the emails get delivered through the clients SMTP while WrapMail staff solves any issues.

WrapMail's hosting center is located in the same building as the WrapMail headquarter and sits on a city-grid as far as power. There's redundancy in the form of dual-drives and dual power in each server and double back-up level for each. The hosting center is further hooked to natural gas and a diesel generator with 2 weeks capacity in the case of a Power **and** gas outage. Co-location in Denver, Colorado.

Management of the WrapMail solution:

This is typically done by marketing staff as they are in charge of branding. WrapMail urges clients to inform all staff before starting the wrapping process so all is aware of benefits and potential hurdles. WrapMail has formulated a suggested letter to all employees for this purpose. This and other instructions are found in the support section of the Customer Control Panel.

Email security:

There really is no such thing as a secure email unless it is encrypted and decrypted with non-standard encryption technology and this is not done by regular corporations anywhere. When an email leaves the email server it travels through at least two ISP's and often through other "boxes" such as routers and switches. All this equipment is accessible by the employees of the organizations that own this equipment and thus emails could be jeopardized. WrapMail's WrapServer is another link in this chain but WrapMail does not keep any body-text of any email. WrapMail does keep the subject, time sent, sender and recipient(s) for the sole purpose of reporting back to the client as the emails are clicked by recipient(s).

Email deliverability:

WrapMail strongly suggest clients setting SPF statements (see www.openspf.org) authorizing the WrapMail servers to deliver the email on behalf of client. WrapMail's servers all have reverse DNS in place.

Emails between people who know each other where reverse DNS and SPF is in place should always be delivered directly to the Inbox (or a folder set up by recipient using rules in their email system). We all know this does not always happen, sometimes we get emails from people we communicate with on a regular basis and they end up in Spam or Junk for no apparent reason. This can also happen to wrapped emails. Wrapmail has been sending wrapped emails since October 2005 and have not encountered anything out of the ordinary as far as email delivery.

The WrapMail solution includes an email delivery assurance program which can be turned on or off.

If this program is activated then the system is designed to send every **new** recipient of an email a request that the recipient 'whitelist' or 'safe list' your email address. When recipients take this action all following emails from you, or from that senders domain, will be delivered directly to the inbox whether it contains images, links, attachments and/or certain key words.

The feature of sending the whitelist request can be turned on or off and can even be repeated at any time (just in case someone did not read the whitelist request email the first time).

This one-time email, coming **from** the WrapMail client (not coming from WrapMail) to each NEW recipient **with the same subject as the wrapped email** and is worded as follows:

Outlook/Windows/Lotus & Mac users will receive the following:

Hello,

I just sent you an email with an interactive letterhead. If you received the wrapped message in your INBOX do nothing. IF the email I sent you went to the J U N K folder please see below.

Outlook 2007/2003, Outlook Express, Windows Mail & Lotus Notes

In the list of emails in the junk folder right click my email and then chose "Junk E-mail" and then click "Add Senders Domain (@example.com) to Safe Senders List."

Entourage & Mac Mail

Look in your Junk E-mail folder for the wrapped message. Select the message, then click the button for "Not Junk."

GMAIL/Yahoo/AOL users will receive the following:

Hello,

I just sent you an email with an interactive letterhead. If you received the wrapped message in your INBOX do nothing. IF the email I sent you went to your S P A M folder please check the box on the left side of the message and then click above where it says NOT S P A M.

Furthermore, WrapMail constantly works with ISP's to get "whitelisted" which in essence means that the emails coming from these know senders/IP addresses/domains shall be delivered through any and all filters.