Requirements and Recommendations

- Hermes SEG should be behind a network perimeter firewall for best security.
- Network Firewall rule to allow inbound traffic to Hermes SEG IP address over TCP/25 (SMTP), TCP/80 (HTTP) and TCP/443 (HTTPS)
- Network Firewall rule to allow the Hermes SEG IP address outbound Internet access over the following Ports:
- UDP/53 (DNS)
- TCP/53 (DNS)
- TCP/80 (HTTP)
- TCP/443 (HTTPS)
- TCP/25 (SMTP)
- TCP/2703 (Cloudmark)
- UDP/6277 (DCC Antispam)
- TCP/123 (NTP)
- UDP/123 (NTP)
- TCP/873 (Rsync)
- UDP/873 (Rsync)
- TCP/24441 (Pyzor)
- TCP/2703 (Razor)
- 8 GB of RAM and at least 4 CPUs
- At least 275 GB of storage space on virtual host. Hermes SEG Appliance hard drives are thin provisioned. The 275 GB of storage will be needed once the email archive starts filling up. The rate the archive fills up greatly depends on the amount of email traffic. For low to medium email traffic a 5 year email retention is not out of the question.
- Your e-mail users will inevitably use the **Junk** and **Not Junk** buttons in their Outlook to report Spam and Ham to Microsoft. This is undesirable because it will create frustration with your users since no action will be taken with those reports as it relates to Hermes SEG. The best way to deal with this problem is to create rules in Hermes SEG to intercept e-mails destined for the following Microsoft e-mail addresses:

1. junk@office365.microsoft.com
2. phish@office365.microsoft.com
3. not_junk@office365.microsoft.com

and redirect them to e-mail address(es) of your choice so that you can take action.

More information on this topic can be found in the article below:

Take Action on E-mail Based on Headers in Hermes SEG

Revision #8
Created 22 November 2020 01:55:25 by Dino Edwards
Updated 24 September 2023 10:32:46 by Dino Edwards