

ზოგადი მოთხოვნები:

- სისტემა უნდა წარმოადგენდეს ვირტუალურ მანქანას.
- მხარდაჭერილი უნდა იყოს შემდეგი ვირტუალიზაციის პლატფორმები:
 - ESXi
 - Hyper-V
 - Xen
- სისტემას უნდა ჰქონდეს მინიმუმ 2 ვირტუალური ბირთვის მხარდაჭერა.
- სისტემას უნდა შეეძლოს დაიცვას არანაკლებ 1000 აქტიური მომხმარებელი.
- სისტემას უნდა ჰქონდეს შესაძლებლობა დაიცვას არანაკლებ 250 დომეინი.

სისტემას უნდა გააჩნდეს შემდეგი ტექნოლოგიების და ფუნქციონალის მხარდაჭერა:

- როგორც შემომავალი ასევე გამავალი წერილების დაცვა.
- ადრესატთან დაშიფრული მეილის გაგზავნა.
- ფუნქციონალის სხვადასხვა დონეზე კონფიგურირება(სისტემა, მომხმარებელი).
- მეილებზე 3 ტიპის მოქმედების განხორციელება: დაშვება, ბლოკირება, დაკარანტირება.
- მომხმარებელს უნდა შეეძლოს ელ-ფოსტის უსაფრთხოების გეითვეის ვებ ინტერფეისის საშუალებით საკუთარ კარანტირებული ელ. წერილების ნახვა.
- მომხმარებლის როლური დაშვების შესაძლებლობა: მომხმარებელი, დომეინის ადმინი, HELP Desk ადმინი.
- syslog სერვერთან ინტეგრაცია.
- სისტემას უნდა ჰქონდეს შესაძლებლობა DNSBL,RBL_ის დახმარებით ამოიცნოს “ცუდი“ სერვერები IP მისამართის მიხედვით და დაბლოკოს ისინი.
- დროის გარკვეულ მონაკვეთში ერთი IP მისამართიდან მიღებული მეილების რაოდენობის შეზღუდვის შესაძლებლობა.
- დაბლოკოს/დაუშვას ადმინისტრატორის მიერ შექმნილი IP მისამართების/ქსელების სია.
- დაადასტუროს გამომგზავნის ავთენტურობა (SFP,DKIM)
- მიმღების ვალიდურობის LDAP სერვერის დახმარებით(Active Directory, Novell eDirectory, Domino Directory,OpenLDAP) შემოწმების შესაძლებლობა.
- მიმავლებული ფაილების გაფართოების მიხედვით დაბლოკვის შესაძლებლობა.
- ისეთი არქივების ბლოკირების შესაძლებლობა, რომლებიც დაცულია პაროლით.
- მიღებული სურათების ანალიზის გაკეთების შესაძლებლობა(OCR).
- ე.წ. სპამ ელ.წერილების აღმოჩენის შესაძლებლობა ლინგვისტური ალგორითმის საფუძველზე ე.წ. Bayesian Analysis
- მეილების შეფასების სკალობრივი სისტემა(ე.წ. spam scoring), რომელიც შეაფასებს მეილში არსებულ საფრთხეს. ადმინისტრატორს უნდა ჰქონდეს შესაძლებლობა “ქულის“ მიხედვით განსაზღვროს დაბლოკოს თუ დაუშვას მეილი
- მეილ სერვერზე(MS Exchange) აგენტის ლოკალურად დაყენების შესაძლებლობა, იმეილ ტრაფიკის ლოკალურად დასაცავად.

- სისტემას უნდა იმართებოდეს ვებ ინტერფეისის საშუალებით(<http/https>).
- სისტემას უნდა გააჩნდეს, როგორც ლოკალურად, ასევე ვენდორის საიტის საშუალებით მართვის შესაძლებლობა(ე.წ. cloud control).