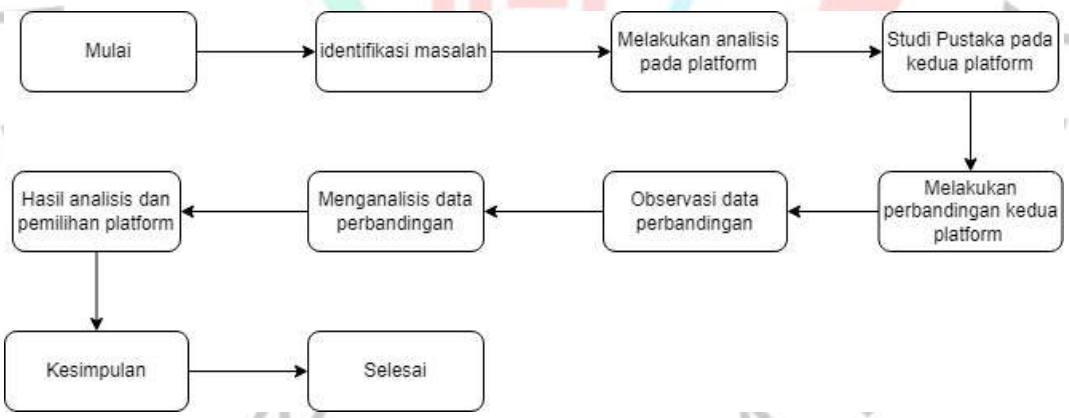
BAB IV
PERENCANAAN

Perencanaan pada penelitian ini terbagi menjadi dua, yaitu Langkah-langkah penelitian dan Rancangan pengujian yang dilaksanakan oleh peneliti. Langkah-langkah dan pengujian ini menjadi dasar saat melakukan penelitian hingga terlaksana dengan terstruktur.

4.1 Langkah-langkah Penelitian

Dalam melakukan penelitian ini terdapat Langkah-langkah yang dituliskan melalui laporan ini agar dapat berjalan dengan baik. Lalu Langkah-langkah ini juga dapat berguna sebagai gambaran maupun acuan bagi peneliti untuk melakukan penelirian. Berikut Langkah-langkah yang dimaksud oleh peneliti dalam bentuk diagram alur.



Gambar 4. 1 Flowchart langkah-langkah penelitian

Pada diagram alir yang tertera di **Gambar 4.1** diatas, dapat dijelaskan sebagai berikut :

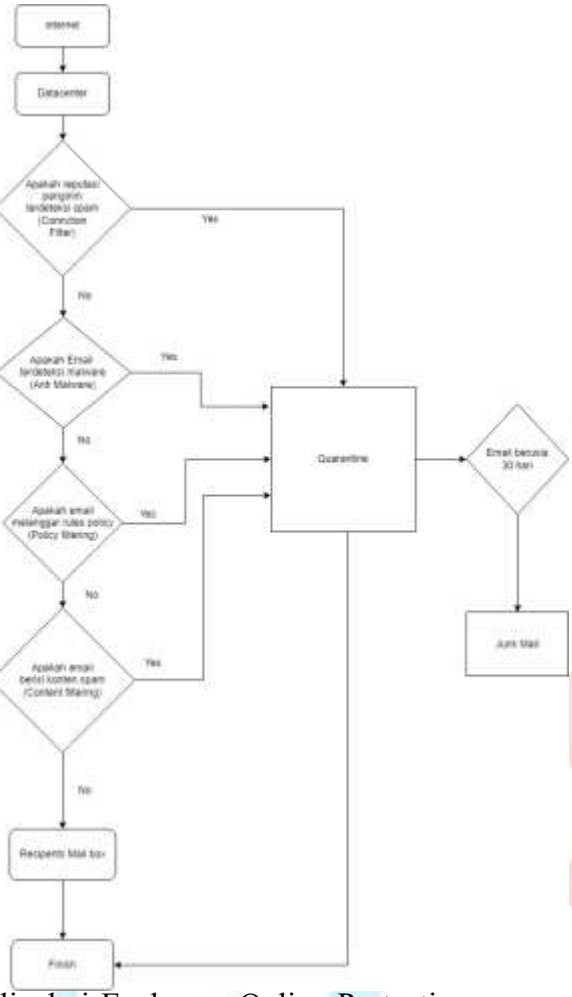
1. Identifikasi masalah menggambarkan tentang masalah dari topik yang sudah ditentukan. Pada tahapan ini, maka akan ditentukan batasan-batasan masalah pada penelitian sehingga bisa menemukan hasil yang bisa diprediksi.

2. Melakukan analisis pada *platform* yang akan digunakan seperti *proxmox mail gateway* dan *exchange online protection*.
3. Studi pustaka untuk menemukan penelitian terdahulu yang berkaitan dengan *proxmox mail gateway* untuk pengumpulan data.
4. Membandingkan kedua *platform* dengan beberapa variabel yang dapat sudah ditentukan oleh peneliti sebagai bukti pemilihan *platform*.
5. Observasi data perbandingan yaitu pengumpulan data yang sudah dibandingkan mengikuti beberapa variabel seperti presentase keamanan, kemudahan pengunaan, fleksibilitas *platform*, ketersediaan fitur, biaya dan kinerja.
6. Analisis data perbandingan dengan kekuatan (*Strength),* kelemahan (*Weaknesses)*, peluang (*Opportunitties*), dan ancaman (*Threats*).
7. Hasil analisis pada *platform* beserta pembahasannya yang berada pada observasi data dan analisis SWOT.
8. Kesimpulan dengan menjawab pertanyaan pada rumusan masalah dan penjelesan singkat mengenai hasil pemilihan *platform* yang ditentukan.

4.2 Rancangan Penelitian

Dalam sub bab ini rancangan penelitian dilakukan untuk menemukan gambaran seperti apa alur dari penelitian setiap kinerja dari platform. rancangan penelitian adalah bagian penelitian untuk membuat rancangan analisis data dan membantu menentukan sampel dalam penelitian (Wisadirana). Dengan menggunakan analisis SWOT dan metode pengumpulan data dengan menggunakan observasi.

4.2.1 Arsitektur Sistem Exchange Online Protection



Gambar 4.2.1 Alur Arsitektur Sistem Pengamanan Exchange Online Protection

Diagram alir dari Exchange Online Protection merupakan cara kerja dari fitur mail gateway dan dapat dilihat pada **Gambar 4.2.1** dibawah ini.

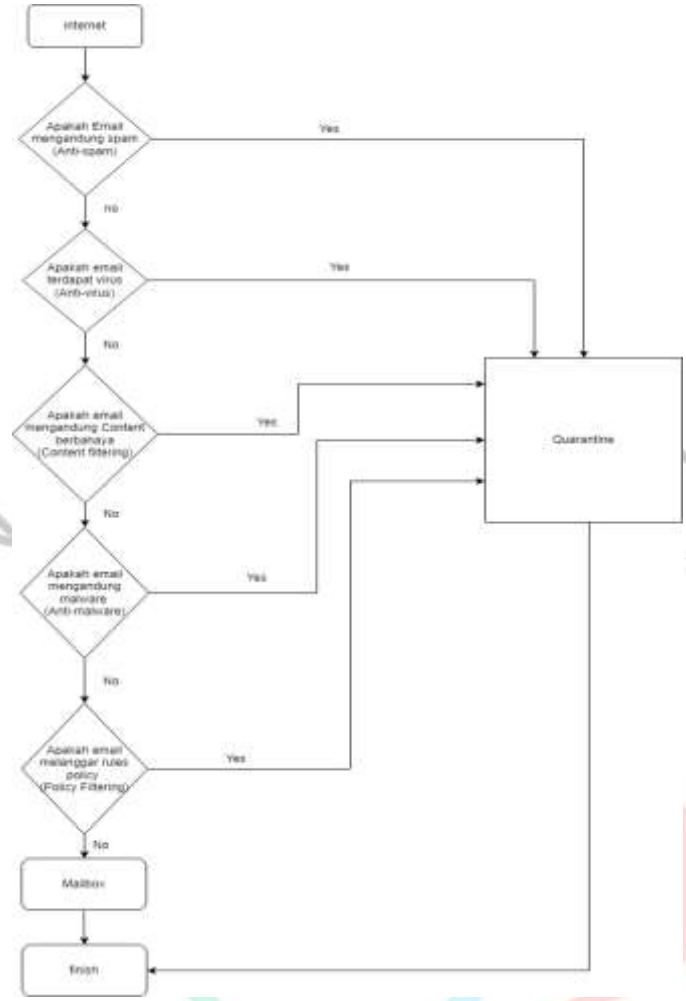
Berikut merupakan penjelasan diagram alur *Exchange Online Protection* diatas.

1. Pengiriman email melalui dengan internet melalui *Simple Mail Transfer Protocol* (SMTP).
2. Email akan sampai ke dalam *datacenter* dari office 365 yang disebut dengan *mail server*
3. Ketika pesan masuk memasuki EOP, pesan tersebut awalnya melewati penyaringan koneksi, yang memeriksa reputasi pengirim. Jika kondisi ini terdeteksi spam, maka secara otomatis akan dimasukkan ke dalam karantina.

4. Kemudian pesan tersebut diperiksa untuk mencari *malware*. Jika *malware* ditemukan dalam pesan atau lampiran pesan, pesan tersebut dikirim ke karantina. Secara default, hanya *administrator* yang dapat melihat dan berinteraksi dengan pesan *malware* yang dikarantina.
5. Pesan berlanjut melalui *mail flow rules-policy filtering*, pada aturan ini akan pasang beberapa kondisi di dalam *mail flow rules-policy filtering* ketika email terdeteksi ancaman maka akan di alirkan ke dalam spam, namun jika tidak terdeteksi maka akan dilanjutkan ke proses selanjutnya.
6. Pesan melewati *Content Filtering* (*anti-spam* dan *anti-spoofing*) di mana pesan berbahaya diidentifikasi sebagai spam, maka akan di alirkan ke dalam karantina secara otomatis. Pengguna dapat mengonfigurasi tindakan yang akan diambil terhadap pesan berdasarkan keputusan pemfilteran (karantina), dan apa yang dapat dilakukan pengguna terhadap pesan yang dikarantina menggunakan kebijakan karantina. Karantina email, pada langkah ini admin dapat mengelola pesan dan *file* ini, seperti melepaskan atau menghapus semua pesan yang dikarantina. Pengguna juga dapat menggunakan kebijakan karantina untuk menentukan apa yang dapat dilakukan pengguna terhadap pesan yang dikarantina.
7. Pesan yang dikarantina akan secara otomatis terhapus dan masuk ke dalam folder *junk mail* setelah berusia 30 hari.

4.2.2 Arsitektur Proxmox Mail Gateway

Diagram alir dari *Proxmox Mail Gateway* (PMG) merupakan cara kerja dari fitur *mail gateway* dan dapat dilihat pada **Gambar 4.2.2** dibawah ini.



Gambar 4.2.2 Arsitektur Sistem Proxmox Mail Gateway

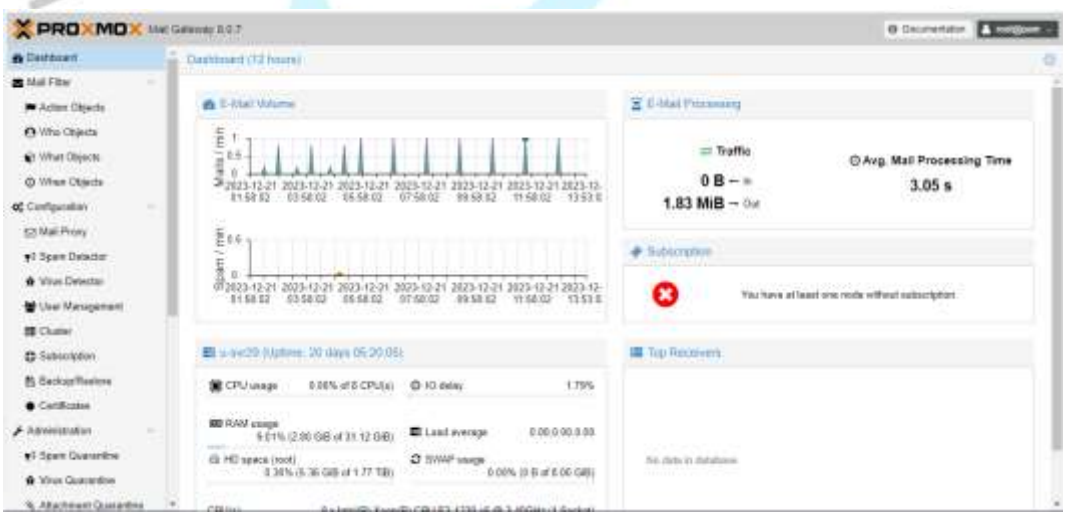
Berikut merupakan penjelasan diagram alur *Proxmox Mail Gateway* diatas diantaranya :

1. Pengiriman email melalui dengan internet melalui *Simple Mail Transfer Protocol* (SMTP).
2. Ketika email diterima, *Proxmox Mail Gateway* melakukan pemeriksaan terhadap email tersebut. Pemeriksaan tersebut yaitu *anti-spam*, email akan memasuki *filter anti-spam* untuk mengidentifikasi dan menyaring *spam*. Jika email terbukti sebagai *spam*, maka akan di masukkan ke dalam fitur karantina.
3. Gateway ini juga melakukan pemindaian terhadap lampiran dan konten email untuk mendeteksi virus, jika terbukti terdeteksi virus maka akan dimasukkan ke dalam fitur karantina.

4. Pada tahap *content filtering*, *platform* akan melakukan pemeriksaan terhadap setiap konten yang ada pada email untuk mengidentifikasikan potensi konten yang berbahaya atau tidak pantas. Jika terdeteksi, maka email akan masuk ke dalam fitur karantina.
5. Pada tahap ini, *platform* akan melakukan pemeriksaan *malware* pada email, Jika *malware* ditemukan dalam pesan atau lampiran pesan, pesan tersebut dikirim ke karantina. Secara default, hanya *administrator* yang dapat melihat dan berinteraksi dengan pesan *malware* yang dikarantina.
6. Pada tahap ini, *platform* akan melakukan pemeriksaan berdasarkan kebijakan dan aturan yang telah ditentukan sebelumnya untuk memastikan kepatuhan terhadap kebijakan keamanan. Jika terbukti maka akan di masukkan ke dalam fitur karantina
7. Setelah dilakukan pengecekan dan terbukti tidak ada ancaman pada email, maka email bisa langsung masuk ke dalam *mail box*

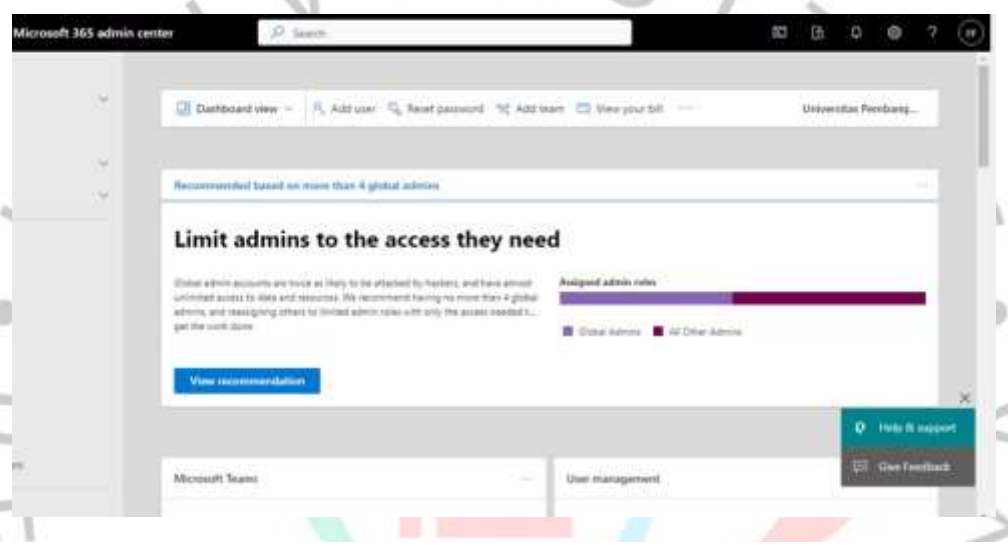
4.2.3 Perbedaan Platform

Proxmox Mail Gateway dan *Exchange Online Protection* (EOP) adalah dua solusi yang berbeda untuk manajemen keamanan email, namun keduanya memiliki fokus yang serupa yaitu melindungi email dari ancaman keamanan seperti *spam, malware, phishing,* dan serangan lainnya.



Gambar 4.2.3. 1 Dashboard Proxmox Mail Gateway

Proxmox mail gateway bersifat *open-source solution*, Dimana *platform* ini menyediakan beberapa fitur keamanan untuk melindungi email di tingkat *gateway. Proxmox mail gateway* ini berbasis *Virtual Environment* (VE), karena untuk integrasi dengan lingkungan virtualisasi. Pengguna memiliki kontrol lebih besar atas konfigurasi dan pengelolaan karena sifatnya yang *open-source*, memungkinkan kustomisasi yang lebih dalam. Melindungi email dengan *filter spam, anti-virus,* proteksi *phishing*, dan kontrol lanjutan di tingkat *gateway*.

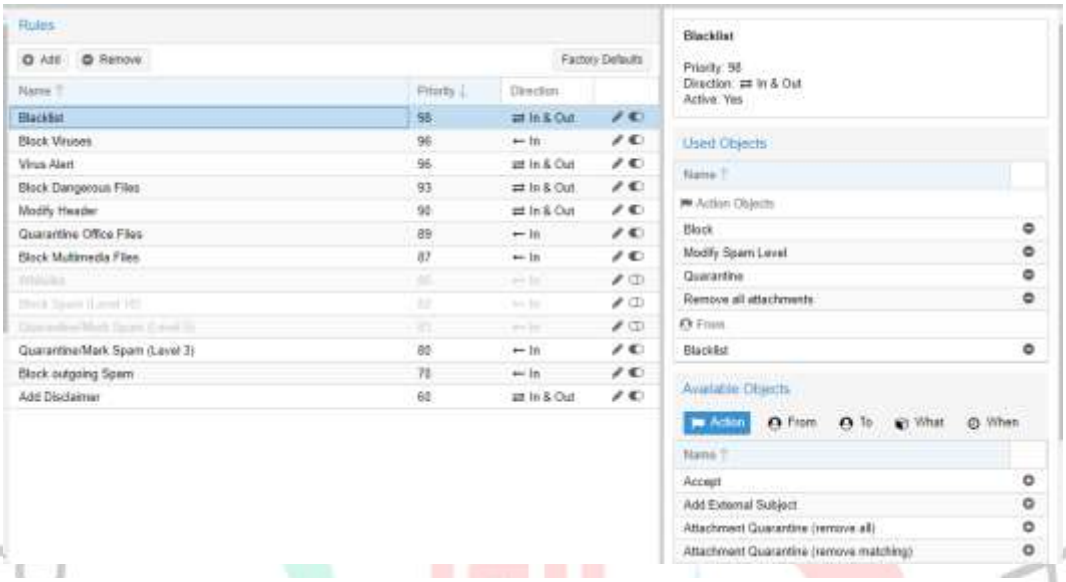


Gambar 4.2.3. 2 Tampilan dashboard security EOP

Pada Microsoft *Service* EOP adalah layanan keamanan email yang disediakan oleh Microsoft sebagai bagian dari layanan *Exchange Online* dalam paket Office 365. Lalu Terintegrasi dengan Office 365, Dirancang khusus untuk melindungi email yang menggunakan layanan Office 365, menyediakan perlindungan terintegrasi untuk pengguna Office 365. Kemampuan Microsoft mengelola layanan ini, memberikan kenyamanan dan dukungan yang kuat dari vendor dalam hal manajemen dan pemeliharaan. Selain perlindungan dasar seperti *filter spam* dan *anti-virus*, EOP juga dapat menyertakan fitur-fitur keamanan tambahan seperti proteksi terhadap serangan lanjutan, enkripsi email, dan kecerdasan buatan.

4.2.4 Metode Perbandingan

Dalam perbandingan akan di lakukan observasi terhadap monitoring dari setiap *platform*, metode yang dilakukan yaitu observasi. Berikut observasi yang dilakukan di kedua *platform* :



Gambar 4.2.4. 1 Monitoring mail filter

Pada monitoring di dalamnya, *mail filter* pada *Proxmox Mail Gateway* adalah komponen yang bertanggung jawab untuk memindai dan memeriksa email yang melewati gateway untuk memastikan keamanan, keandalan, dan kesesuaian dengan kebijakan yang telah ditetapkan. administrator dapat melakukan beberapa konfigurasi seperti pada *action Objects, who Objects, What Objects,* dan *When Objects*. Pada mail filter terdapat *rules* yang bisa dimodifikasi

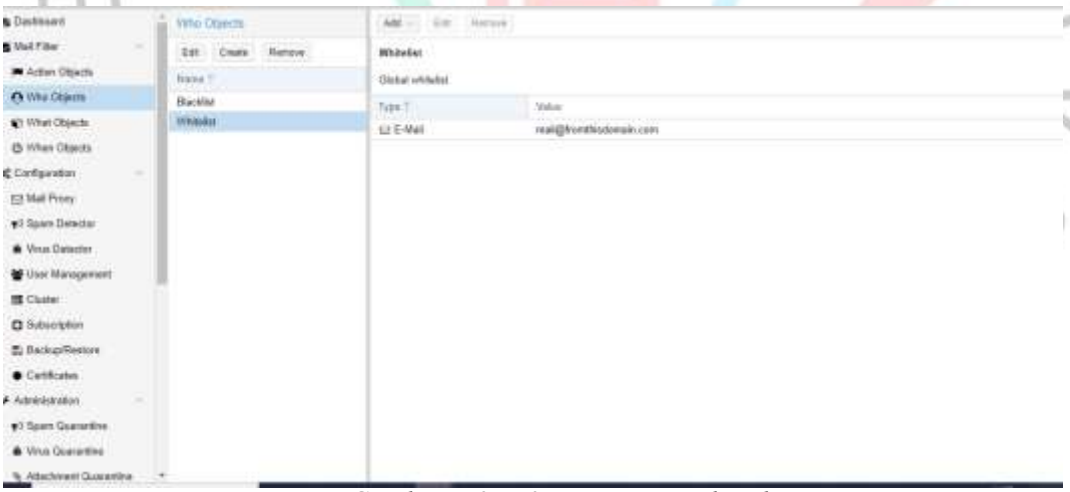
"*action objects*" merujuk pada kumpulan tindakan yang dapat diambil oleh sistem berdasarkan hasil dari filterisasi email. *Action objects* mengatur respons yang akan diambil ketika *filter* menemukan email yang memenuhi kriteria tertentu.

Beberapa *action objects* yang umumnya tersedia di *Proxmox Mail Gateway* termasuk:

- *Quarantine*: Email yang diidentifikasi sebagai berpotensi berbahaya atau tidak diinginkan dipindahkan ke area karantina sehingga tidak langsung diantarkan ke kotak masuk pengguna. Pengguna kemudian dapat memeriksanya dan mengambil tindakan lebih lanjut jika diperlukan.

- *Reject*: Email yang melanggar kebijakan keamanan atau tidak diinginkan ditolak oleh *gateway* dan tidak diantarkan ke penerima.
- *Tag*: Menandai email dengan label tertentu yang mengidentifikasikan jenis atau tingkat risiko dari pesan tersebut. Misalnya, menambahkan tag "[SPAM]" pada subjek email yang teridentifikasi sebagai *spam*.
- *Redirect*: Mengalihkan email ke alamat alternatif atau ke dalam sistem untuk penanganan lebih lanjut. Ini mungkin termasuk mengirim salinan pesan kepada *administrator* untuk peninjauan.
- *Quarantine & Notify*: Email dipindahkan ke karantina, dan penerima atau *administrator* diberi notifikasi tentang adanya email yang tertahan di sana.
- *Accept*: Membiarkan email melewati *filter* tanpa tindakan tambahan.

Action objects memungkinkan *administrator* untuk mengonfigurasi cara sistem harus menangani email yang lolos atau tidak lolos melalui *filter*. Dengan menggunakan kombinasi *action objects* yang sesuai, *administrator* dapat menyesuaikan tingkat keamanan dan kebijakan email sesuai dengan kebutuhan organisasi.



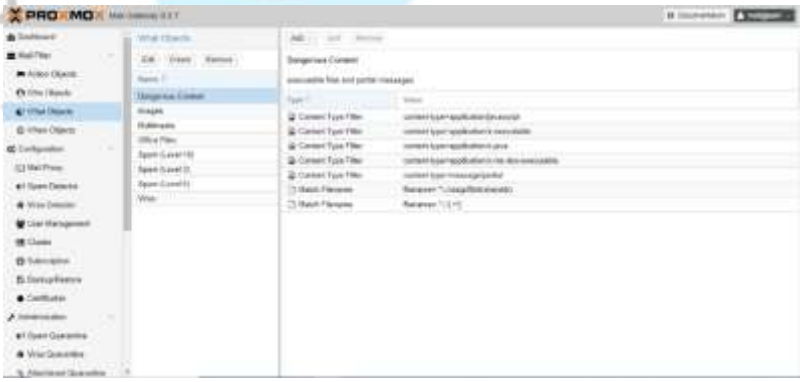
Gambar 4.2.4. 2 Monitoring who objects

Dalam *who objects*, *Proxmox Mail Gateway* biasanya merujuk pada kemampuan untuk mengelola dan menerapkan kebijakan keamanan berbasis identitas pengirim atau penerima email, bukan hanya berdasarkan alamat email tetapi juga berdasarkan identitas yang lebih spesifik.

Ini memungkinkan pengguna untuk membuat aturan yang lebih kompleks dan canggih terkait dengan pengiriman email, misalnya:

- Grup Pengguna: Menetapkan kebijakan keamanan tertentu untuk grup pengguna tertentu dalam organisasi. Sehingga, aturan dapat diterapkan secara spesifik untuk anggota departemen atau unit kerja tertentu.
- Pengenal IP atau Domain: Memberikan izin atau memblokir pengiriman email dari domain atau alamat IP tertentu, memungkinkan pengelolaan tingkat akses dari sumber yang telah dikenali.
- Pengenal Pengguna Individual: Memperbolehkan atau memblokir email dari pengirim atau penerima tertentu, memungkinkan kebijakan yang sangat spesifik berdasarkan identitas individu.
- Pengaturan Prioritas: Mengizinkan email dari sumber tertentu untuk memiliki prioritas yang lebih tinggi dalam pengiriman atau penerimaan, memberikan perlakuan khusus untuk email yang datang dari entitas yang telah ditetapkan.

Dengan *WHO Objects*, pengguna *Proxmox Mail Gateway* dapat melakukan manajemen kebijakan yang lebih terperinci, memungkinkan pengelolaan tingkat keamanan yang disesuaikan dengan identitas pengirim dan penerima email, serta sumber asal pesan. Ini membantu meningkatkan kontrol dan keamanan dalam pengelolaan email

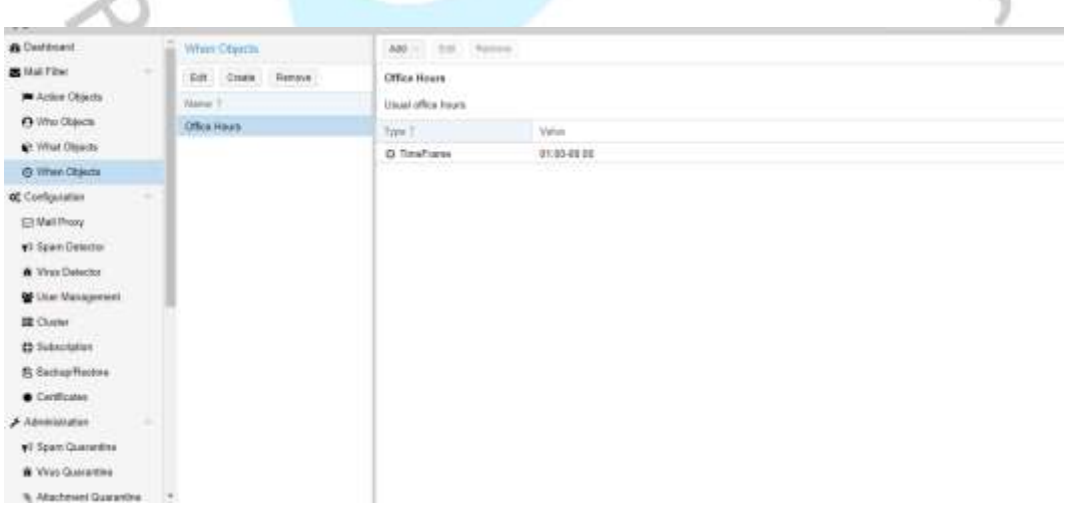


Gambar 4.2.4. 3 Monitoring what objects

Dalam konteks keamanan email, "*what objects*" bisa merujuk pada jenis-jenis filter atau kebijakan yang diterapkan pada isi atau jenis konten dari pesan email. Beberapa fitur umum yang mungkin termasuk dalam konsep "*what objects*" meliputi:

- Filter konten: Ini mencakup filterisasi berdasarkan isi pesan, seperti deteksi kata kunci tertentu, analisis pola teks, atau identifikasi konten berbahaya seperti gambar eksplisit atau tautan yang mencurigakan.
- Deteksi lampiran berbahaya: mengidentifikasi dan menangani lampiran yang berpotensi membawa virus atau *malware*.
- Pendeteksian pola data sensitif: menerapkan kebijakan untuk mengidentifikasi dan mengontrol email yang mengandung informasi sensitif seperti nomor kartu kredit, informasi pribadi, atau rahasia perusahaan.
- Pemfilteran berbasis tindakan: mengklasifikasikan jenis pesan berdasarkan tindakan yang dapat diambil, misalnya, apakah pesan tersebut adalah *spam, phishing,* atau email penting dari pihak internal.

Jika ada fitur spesifik yang dimaksudkan dengan "*what objects*" dalam konteks *Proxmox Mail Gateway* atau jenis filter konten yang lebih spesifik, Anda mungkin perlu merujuk ke dokumentasi resmi atau referensi *Proxmox Mail Gateway* untuk informasi yang lebih tepat dan terperinci.

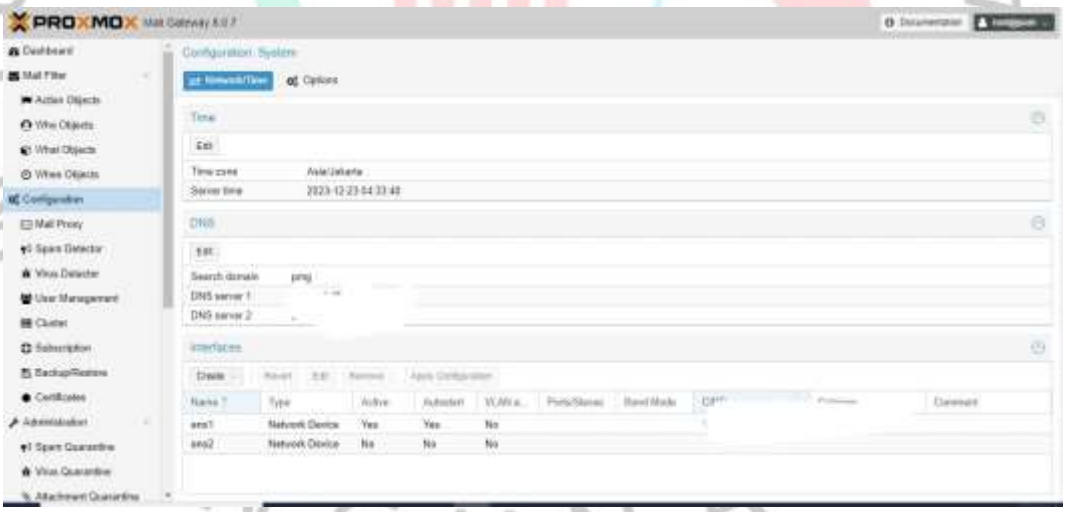


Gambar 4.2.4. 4 Monitoring when objects

Dalam *when objects*, fitur ini dapat melakukan *add time frame* dengan kata lain fitur ini mengatur waktu pelaksanaan kinerja proxmox mail gateway. beberapa fitur yang mungkin berkaitan dengan konsep "*when*" yang bisa berlaku:

- *Scheduling*: Mengatur kapan kebijakan keamanan email tertentu diterapkan atau diaktifkan. Misalnya, aturan tertentu untuk mengirim email ke karantina hanya diterapkan pada jam kerja, sementara pada akhir pekan email langsung diteruskan ke kotak masuk.
- Pengaturan waktu: penerapan kebijakan yang berbeda pada waktu-waktu tertentu. Misalnya, aturan ketat untuk *filter spam* yang diaktifkan selama waktu-waktu yang rawan serangan spam yang tinggi.

Jika "*when objects*" merujuk pada fitur yang lebih spesifik atau pengaturan terkait waktu dalam *Proxmox Mail Gateway*, merujuk ke dokumentasi resmi atau referensi spesifik terkait dengan *platform* tersebut akan memberikan informasi yang lebih tepat



Gambar 4.2.4. 5 Sistem Konfigurasi PMG

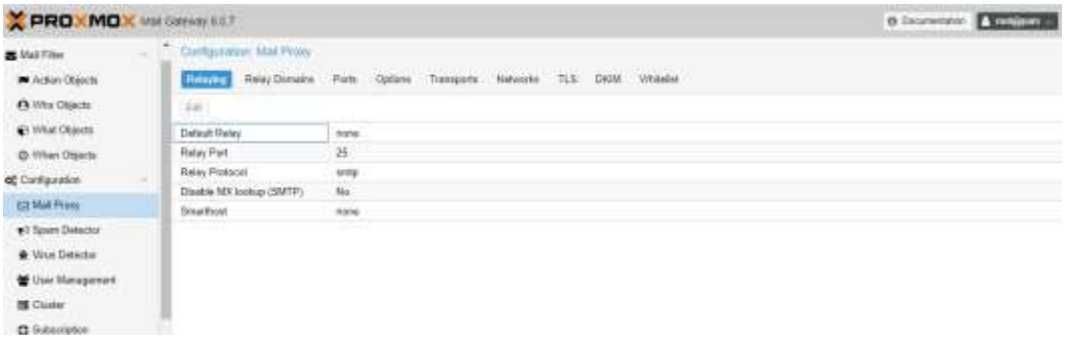
Menu konfigurasi pada *Proxmox Mail Gateway* (PMG) adalah sebuah menu konfigurasi yang digunakan untuk mengatur sebuah jaringan dan mengelola berbagai pengaturan yang ada pada *proxmox mail gateway*. Ini mencakup berbagai opsi dan pengaturan untuk mengontrol dan mengelola pengiriman email, keamanan, *filter*, integrasi dengan layanan eksternal, dan manajemen pengguna. Dalam menu konfigurasi ini, pengguna dapat menemukan opsi pertama pada fitur ini yaitu

pengaturan umum seperti pengaturan dasar yang berkaitan dengan domain, pengaturan jaringan, waktu, dan lain-lain.

Pada sistem konfigurasi terdapat beberapa konfigurasi yang diantaranya yaitu :

1. Pengaturan umum: pengaturan dasar yang berkaitan dengan domain, pengaturan jaringan, waktu, dan lain-lain.
2. Pengaturan *antivirus* dan *antispam*: konfigurasi untuk perlindungan terhadap virus dan spam, termasuk konfigurasi filter, daftar putih/hitam, pengaturan heuristic, dan integrasi dengan solusi antivirus eksternal.
3. Pengaturan keamanan: opsi untuk mengonfigurasi tindakan keamanan, seperti pembatasan koneksi, pengaturan SSL/TLS, dan kebijakan enkripsi.
4. Manajemen pengguna: untuk mengelola pengguna, grup, hak akses, serta aturan terkait otentikasi dan akses.
5. Log dan pelaporan: pengaturan terkait pemantauan, logging, dan pelaporan aktivitas email.
6. Integrasi eksternal: konfigurasi untuk integrasi dengan layanan eksternal, seperti LDAP, *Active Directory*, atau layanan lainnya yang mendukung otorisasi.

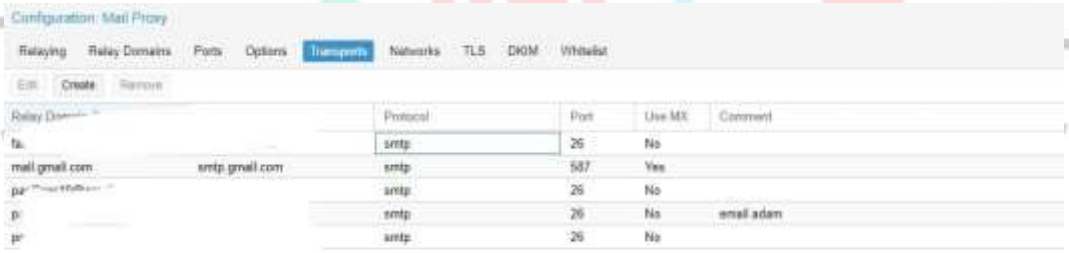
Menu konfigurasi ini memberikan kontrol yang luas kepada *administrator* untuk menyesuaikan pengaturan *gateway* email sesuai dengan kebutuhan dan kebijakan keamanan organisasi.



Gambar 4.2.4. 6 Konfigurasi pada mail proxy

Pada pengaturan *Antivirus* dan *Antispam proxmox mail gateway* terdapat *mail proxy*, Fitur ini pada *Proxmox Mail Gateway* memungkinkan perangkat ini untuk bertindak sebagai perantara atau *proxy* untuk lalu lintas email yang masuk dan keluar dari jaringan. Ini memungkinkan pengawasan, filterisasi, dan perlindungan tambahan terhadap email yang dikirim dan diterima. Dalam konfigurasi *mail proxy* terdapat *relay domain* yang berfungsi sebagai penyampain email yang masuk ke dalam aplikasi email berdasarkan domain yang digunakan pengirim.

Relay domain ini terhubung dengan *Simple Mail Transfer Protocol* (SMTP) merupakan protokol komunikasi standar yang digunakan untuk mengirim email di



Gambar 4.2.4. 7 Simple Mail Transfer Protocol

internet. Protokol ini menangani pengiriman pesan email dari satu server ke server lainnya dan memungkinkan pengguna untuk mengirim email dari klien email mereka ke server email penerima. SMTP berperan dalam mengatur proses pengiriman email, termasuk transfer pesan, verifikasi identitas, dan konfirmasi penerimaan pesan. Untuk pengiriman email tanpa enkripsi, SMTP menggunakan port standar 25, sedangkan port 587 (Submission) umumnya digunakan untuk pengiriman email yang terenkripsi, seperti yang dilakukan oleh TLS/SSL.

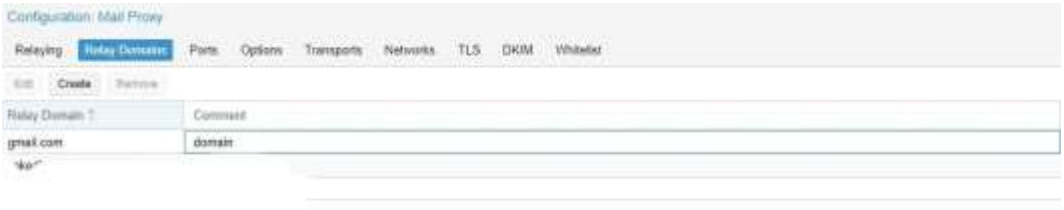
Activate Windows
Go to Settings to activate Windows.

Gambar 4.2.4. 8 Port Eksternal dan Port Internal

Pada *Proxmox Mail Gateway*, *port* eksternal dan *port* internal merujuk pada pengaturan koneksi ke perangkat itu sendiri. Ini seringkali terkait dengan konfigurasi *firewall* dan pengaturan jaringan yang digunakan untuk mengakses layanan yang ditawarkan oleh *Proxmox Mail Gateway*.

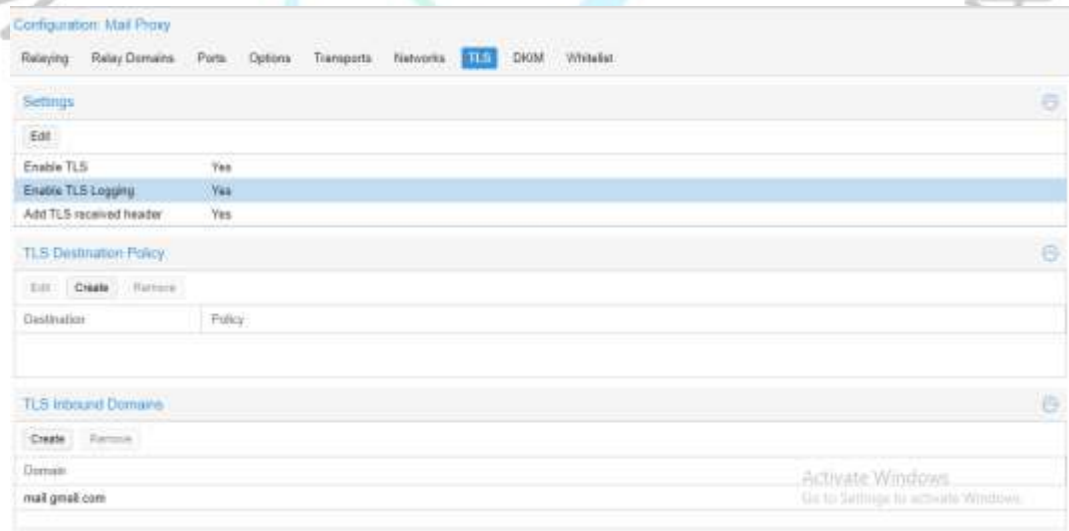
- *Port Eksternal* merujuk pada *port* yang digunakan untuk koneksi dari luar jaringan atau dari sumber eksternal yang ingin terhubung ke *Proxmox Mail Gateway*. Ini sering kali adalah port yang diekspos ke internet atau jaringan yang lebih luas untuk memungkinkan akses dari luar.
- *Port Internal* merujuk pada *port* yang digunakan di dalam jaringan atau di dalam infrastruktur yang terisolasi, biasanya jaringan lokal atau jaringan internal. Ini adalah *port* yang digunakan oleh *Proxmox Mail Gateway* untuk layanan internal, seperti layanan SMTP, POP3, IMAP, atau antarmuka manajemen web.

Secara umum, *port* eksternal akan terhubung dengan *port internal* melalui proses konfigurasi jaringan untuk mengalihkan lalu lintas dari port eksternal ke *port internal* yang sesuai pada *Proxmox Mail Gateway*. Hal ini memungkinkan komunikasi yang aman dan teratur antara sumber eksternal (seperti pengguna atau server lain di luar jaringan lokal) dan layanan yang ditawarkan oleh *Proxmox Mail Gateway* di dalam jaringan tersebut.



Gambar 4.2.4. 9 Relay Domain

Relay domain adalah domain yang diizinkan untuk menerima atau mengirim email melalui server email tertentu, meskipun domain tersebut sebenarnya tidak di-host atau dikelola oleh server email tersebut. Dalam konteks pengiriman email, relay domain mengacu pada konfigurasi di server email yang memungkinkan server tersebut untuk menerima email dari domain tersebut dan mengirim email atas nama domain tersebut. Pada *relay domain* terdapat nama *domain* dari google.com, jadi hal ini *domain* yang diperbolehkn untuk masuk ke dalam *proxmox mail gateway* (PMG) adalah domain tersebut.



Gambar 4.2.4. 10 Transport Layer Security (TLS)

Transport Layer Security (TLS) pada *Proxmox Mail Gateway* merupakan protokol keamanan yang digunakan untuk mengamankan komunikasi antara server

email pengirim dan server email penerima. Protokol ini mengenkripsi data yang dikirimkan antara server email, sehingga menjaga keamanan dan privasi informasi yang dikirim melalui email.

Dalam konteks *Proxmox Mail Gateway*, penggunaan TLS memiliki beberapa aspek yang meliputi Enkripsi Komunikasi *Transfer Layer* Protocol (TLS) yang digunakan untuk mengenkripsi lalu lintas email yang keluar dan masuk dari *Proxmox Mail Gateway*. Hal ini melindungi email dari penyadapan atau intersepsi oleh pihak yang tidak berwenang saat sedang berada dalam perjalanan di internet. Pengaturan Keamanan dapat mengonfigurasi *Proxmox Mail Gateway* untuk memerlukan koneksi TLS saat berkomunikasi dengan server email lainnya. Ini membantu memastikan bahwa koneksi antara server email lokal dan server tujuan dilakukan melalui kanal yang aman.

Activate Windows
Go to Settings to activate Windows.

Gambar 4.2.4. 11 Spam Detector

Spam detector pada *Proxmox Mail Gateway* adalah sebuah fitur atau mekanisme yang digunakan untuk mengidentifikasi dan memisahkan email yang dikategorikan sebagai spam atau pesan yang tidak diinginkan dari email yang valid dan diinginkan. Detektor spam ini menggunakan berbagai teknik dan algoritma untuk menganalisis konten email, *header,* dan perilaku pengirim untuk menentukan apakah suatu email kemungkinan besar merupakan spam.

Beberapa metode yang biasanya digunakan dalam *spam detection* di *Proxmox Mail Gateway* meliputi:

1. Filtering berbasis aturan: menggunakan seperangkat aturan yang telah ditentukan pengguna untuk mengidentifikasi dan memblokir email yang sesuai dengan kriteria tertentu, seperti daftar kata kunci, alamat pengirim, atau pola tertentu dalam email.

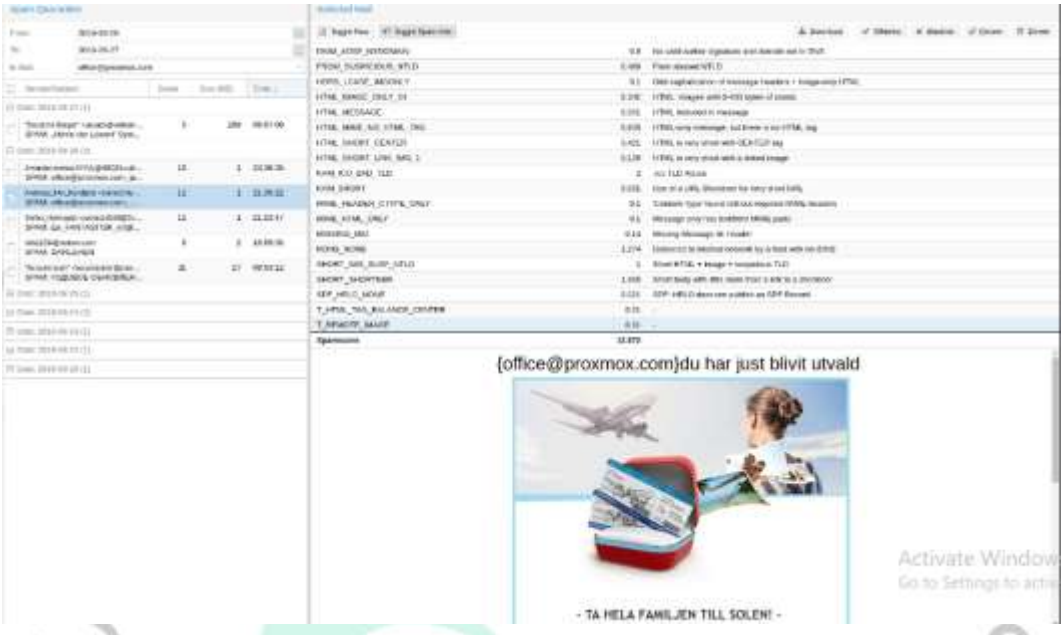
2. Penggunaan daftar hitam (*blacklist*) dan daftar putih (*whitelist*): membandingkan alamat pengirim dengan daftar hitam yang berisi alamat-alamat yang dikenal sebagai pengirim *spam*, serta daftar putih yang berisi alamat-alamat yang diizinkan.

3. Analisis heuristik: menggunakan analisis statistik dan pemodelan untuk mengidentifikasi pola umum dalam spam, seperti penggunaan kata-kata tertentu, struktur email yang tidak biasa, atau tanda-tanda lain yang mengindikasikan *spam.*

4. Pengenalan pola (*pattern recognition*): membandingkan konten email dengan pola atau tanda-tanda yang sering terkait dengan spam, seperti penipuan phishing atau promosi komersial yang tidak diinginkan.

5. Penggunaan teknologi pembelajaran mesin (*machine learning*): menerapkan algoritma pembelajaran mesin untuk secara otomatis mempelajari dan mengenali pola dari email yang valid dan *spam* berdasarkan data pelatihan.

Dengan kombinasi beberapa teknik ini, *Proxmox Mail Gateway* berusaha untuk secara efektif mengidentifikasi dan memblokir email yang masuk ke dalam kategori *spam*, membantu pengguna untuk mengelola kotak masuk mereka dengan lebih efisien dan mengurangi risiko dari serangan *phishing* serta *malware*.



Gambar 4.2.4. 12 Spam Quarantine

Spam Quarantine pada *Proxmox Mail Gateway* adalah fitur yang memungkinkan sistem untuk menahan email-email yang terdeteksi sebagai spam sebelum mereka mencapai kotak masuk pengguna. Email-email ini disimpan secara terpisah dalam area penyimpanan yang disebut "*quarantine*" untuk diperiksa lebih lanjut oleh pengguna atau administrator.

Dengan menggunakan fitur ini, email yang dianggap mencurigakan atau spam tidak langsung disampaikan kepada penerima, mengurangi risiko terpaparnya pengguna terhadap konten yang berpotensi berbahaya atau tidak diinginkan. Ini memberi kesempatan bagi administrator atau pengguna untuk memeriksa email yang ditahan tersebut dan memutuskan apakah email tersebut sebenarnya penting atau sebaiknya dibuang.

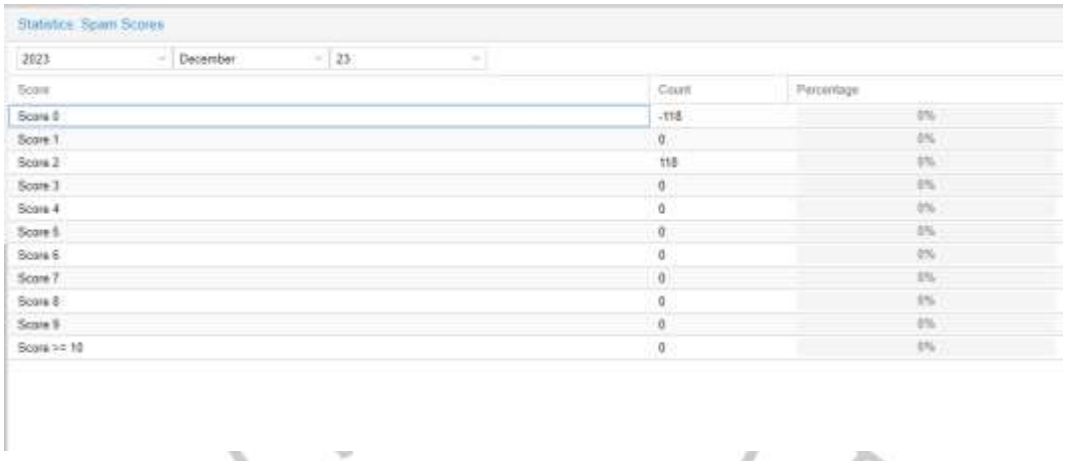
Quarantine pada *Proxmox Mail Gateway* memungkinkan pengguna atau *administrator* untuk melihat, mengelola, dan mengambil tindakan seperti melepaskan (mengizinkan email masuk ke kotak surat) atau menghapus email yang ditahan sebagai spam. Fitur ini membantu meningkatkan keamanan dan mengontrol arus email yang masuk ke jaringan.

Dalam *spam quarantine* terdapat sebuah pilihan Ketika email tersebut masuk ke dalam fitur *quarantine*, yaitu *administrator* dapat memilih apakah email tersbut masuk ke dalam *blacklist* atau *whitelist*. Pada fitur ini dijelaskan bahwa

Blacklist dan *whitelist* pada *Proxmox Mail Gateway* adalah mekanisme yang digunakan untuk mengontrol dan mengelola lalu lintas email yang masuk berdasarkan daftar yang telah ditentukan pengguna atau *administrator*.

1. *Blacklist* (Daftar Hitam): daftar ini berisi entitas yang dilarang atau diblokir dari pengiriman email. Ini bisa berupa alamat email, domain, atau bahkan alamat IP yang telah diidentifikasi sebagai sumber spam, malware, atau entitas yang tidak diinginkan lainnya. Email yang berasal dari entitas yang terdaftar dalam daftar hitam ini akan ditolak atau ditempatkan langsung ke dalam folder *spam/quarantine.*
2. *Whitelist* (Daftar Putih): sebaliknya, daftar putih adalah daftar yang berisi entitas yang diizinkan atau diberi akses untuk mengirim email tanpa batasan. Entitas yang ada dalam daftar putih ini akan melewati filter spam dan kebijakan lain yang diterapkan oleh *Proxmox Mail Gateway*. Ini bisa berupa alamat email, domain, atau IP yang diberikan izin khusus untuk mengirim email ke pengguna tanpa terhalang oleh filter keamanan.

Dengan menggunakan daftar hitam dan daftar putih ini, *administrator* dapat melakukan pengaturan yang lebih presisi terkait apa yang diizinkan atau diblokir dalam aliran email masuk. Ini membantu meningkatkan keamanan dan kehandalan sistem email, mengurangi kemungkinan penerimaan email yang tidak diinginkan atau berbahaya ke dalam kotak surat pengguna.



Gambar 4.2.4. 13 Spam Scores

Spam Scores pada *Proxmox Mail Gateway* (PMG) adalah nilai yang diberikan oleh sistem untuk menentukan seberapa mungkin sebuah email dianggap sebagai *spam*. Skor ini bisa didasarkan pada berbagai faktor seperti pengaturan aturan, analisis konten email, pengenal pengirim, dan karakteristik lainnya dari pesan email yang masuk. Umumnya, semakin tinggi skor spam, semakin besar kemungkinan email tersebut adalah *spam*.

PMG menggunakan berbagai teknik untuk menentukan skor spam, seperti filter bayesian, analisis header dan body email, deteksi pola, serta daftar hitam (*blacklist*) dan daftar putih (*whitelist*) untuk pengirim yang dikenal atau tidak dikenal.

Pengguna biasanya dapat mengatur ambang batas (*threshold*) di mana pesan akan ditandai sebagai *spam* atau diblokir berdasarkan skor yang diberikan. Dengan mengatur ambang batas yang sesuai, pengguna dapat mengelola seberapa ketat filter *spam* yang mereka inginkan.

Proxmox Mail Gateway (PMG) menggunakan skala nilai untuk menilai tingkat kecenderungan sebuah email menjadi spam. Cara membedakan skor spam dari 1 hingga 10 pada PMG dapat bervariasi tergantung pada konfigurasi spesifik dari sistem dan aturan yang diterapkan. Namun, umumnya, semakin tinggi nilai skor yang diberikan, semakin besar kemungkinan email tersebut dianggap sebagai spam.

skala skor *spam* pada PMG bisa dilihat sebagai berikut:

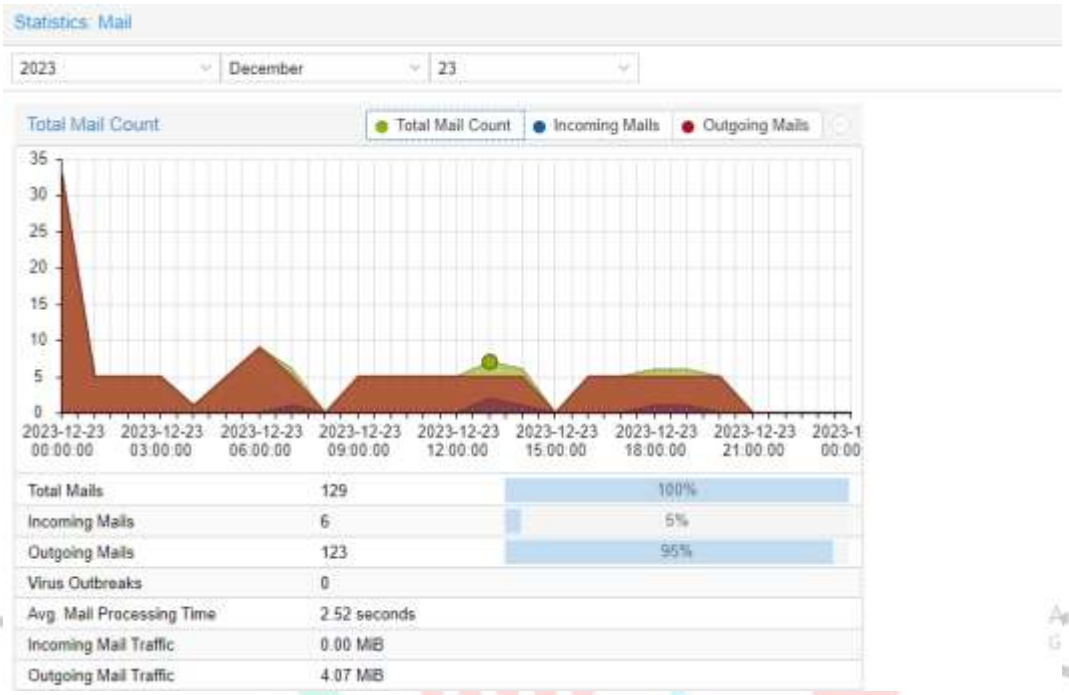
- Skor 1-3: Email yang kemungkinan besar bukan spam.
- Skor 4-6: Email yang memerlukan perhatian tambahan karena memiliki beberapa ciri yang mirip dengan *spam*.
- Skor 7-10: Email yang cenderung sangat mungkin menjadi *spam*.

Gambaran tentang bagaimana skor spam dari 1 hingga 10 mungkin diterapkan pada *Proxmox Mail Gateway*:

- Skor 1-3: sebuah email dari kontak yang sudah dikenal sebelumnya, misalnya, dari kolega kerja atau keluarga yang alamat emailnya terdaftar dalam daftar putih (*whitelist*) pengguna. Pesan ini mungkin berisi teks sederhana tanpa tautan eksternal yang mencurigakan atau lampiran yang berpotensi berbahaya. Sistem akan memberikan skor yang rendah karena email tersebut cocok dengan profil pengirim yang sudah dikenal dan tidak memiliki tanda-tanda *spam* yang jelas.
- Skor 4-6: sebuah email masuk yang berasal dari alamat yang belum pernah terlihat sebelumnya dan berisi beberapa tautan ke situs web yang tidak biasa atau menggunakan bahasa yang mencurigakan. Email ini mungkin mengandung beberapa kata kunci yang sering terkait dengan spam, seperti "diskon besar-besaran" atau "penawaran eksklusif", namun tidak memicu penandaan langsung sebagai spam. Skor di sini sedang, karena pesan ini memiliki beberapa ciri yang mirip dengan *spam*.
- Skor 7-10: sebuah email yang berasal dari alamat yang tidak dikenal atau terdaftar dalam daftar hitam (*blacklist*) sebagai pengirim yang sering terkait dengan aktivitas *spam*. Isi email ini penuh dengan tautan ke situs web yang tidak aman atau mencurigakan, dan mungkin juga mengandung lampiran yang terdeteksi sebagai berbahaya. Pesan ini memiliki banyak ciri-ciri yang sering terkait dengan , sehingga menerima skor tinggi di puncak skala.

Dalam kasus ini, skor spam yang diberikan pada PMG dapat bervariasi sesuai dengan kombinasi faktor-faktor seperti pengaturan aturan, analisis konten email, pengenal pengirim, dan karakteristik pesan email yang masuk. *Adjusting*

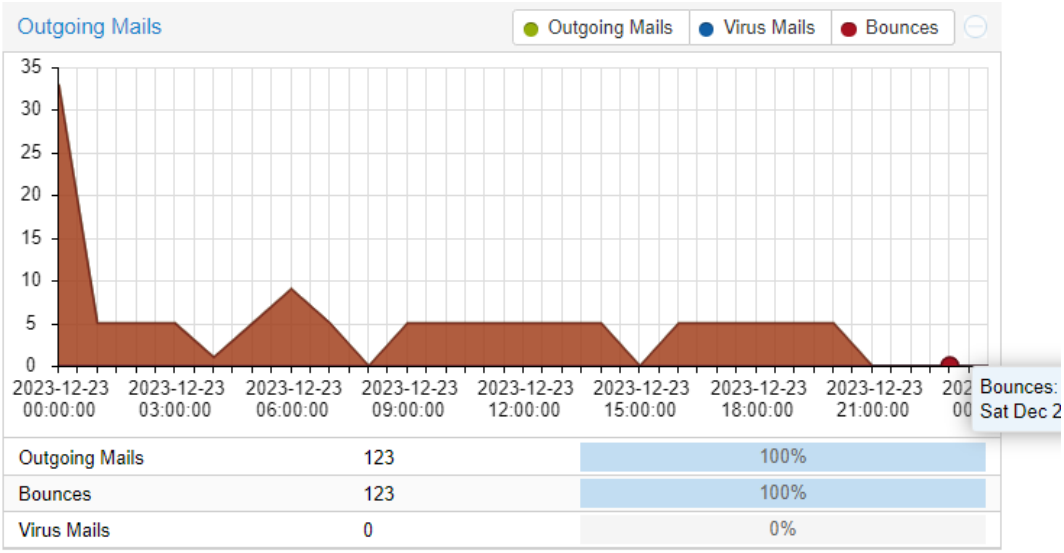
ambang batas (*threshold*) di mana pesan akan ditandai sebagai *spam* atau diblokir juga dapat mempengaruhi nilai skor yang diberikan pada sebuah email.



Gambar 4.2.4. 14 Statistic Mail

Statistic mail pada *Proxmox Mail Gateway* adalah fitur yang memberikan laporan dan analisis tentang lalu lintas email yang masuk dan keluar dari server. Fitur ini memberikan informasi terperinci tentang jumlah email yang diterima, jumlah yang diblokir karena *spam* atau *malware*, serta statistik tentang penggunaan sumber daya dan aktivitas email lainnya.

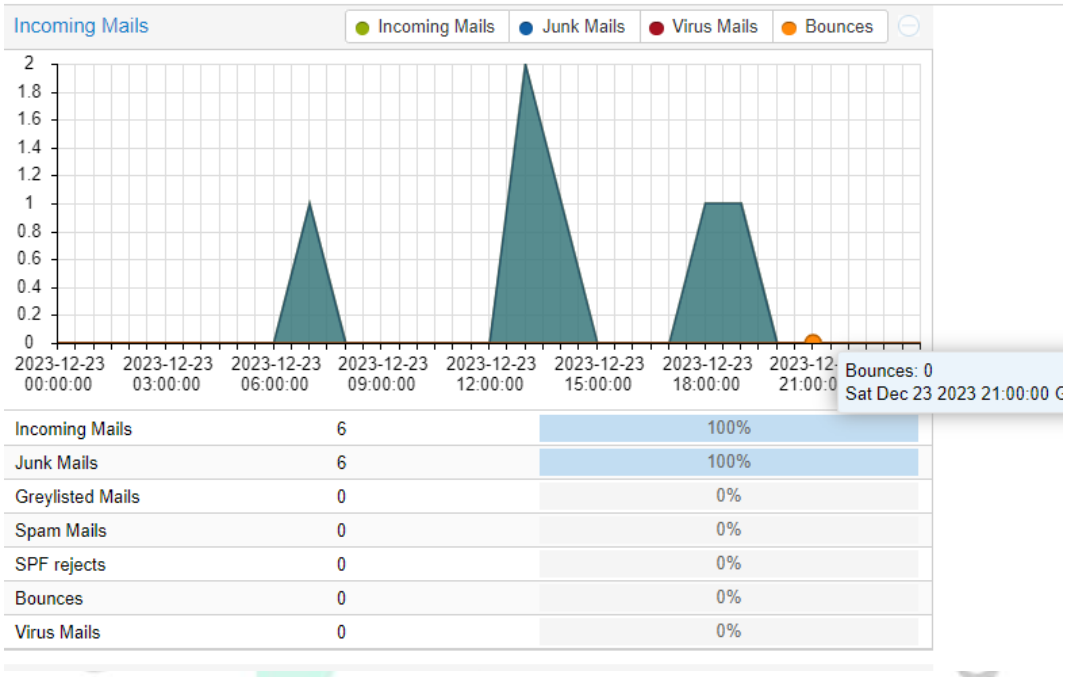
Dengan statistik email, pengguna dapat memantau kinerja sistem email mereka, mengidentifikasi pola yang mencurigakan (seperti peningkatan tiba-tiba dalam email *spam*), dan membuat keputusan berdasarkan data untuk meningkatkan keamanan dan efisiensi email. Ini memungkinkan *administrator* untuk melacak tren, memantau penggunaan sumber daya, dan mengoptimalkan konfigurasi sistem.



Gambar 4.2.4. 15 Outgoing Mails

Outgoing mail merujuk kepada email yang dikirim dari server atau sistem *Proxmox Mail Gateway* ke tujuan eksternal, seperti pengguna yang mengirim email ke alamat di luar domain atau sistem yang dijalankan oleh *Proxmox Mail Gateway.*

UPN PEMBANGUNAN JAYA



Gambar 4.2.4. 16 Incoming Mails

Incoming mail mengacu pada email yang masuk ke server atau sistem *Proxmox Mail Gateway* dari luar, dari pengirim eksternal atau sumber email eksternal.

Incoming mail dan *outgoing mail* pada *Proxmox Mail Gateway* merujuk kepada arah dari aliran email yang masuk dan keluar dari sistem.

- Incoming Mail: ini merujuk pada email yang diterima oleh server atau *gateway* email dari luar ke dalam jaringan *local*. *Proxmox Mail Gateway* akan memeriksa, mem-*filter*, dan memproses email yang masuk ini untuk memastikan bahwa mereka aman, bebas dari *spam*, malware, atau ancaman lainnya sebelum disampaikan kepada pengguna di dalam jaringan *local*.
- *Outgoing Mail*: ini adalah email yang dikirim dari dalam jaringan *local* ke luar, menuju tujuan eksternal. *Proxmox Mail Gateway* juga dapat memantau dan memfilter email yang keluar untuk memastikan bahwa konten yang dikirimkan dari jaringan *local* sesuai dengan kebijakan yang ditetapkan, aman, dan tidak mengandung ancaman atau spam.

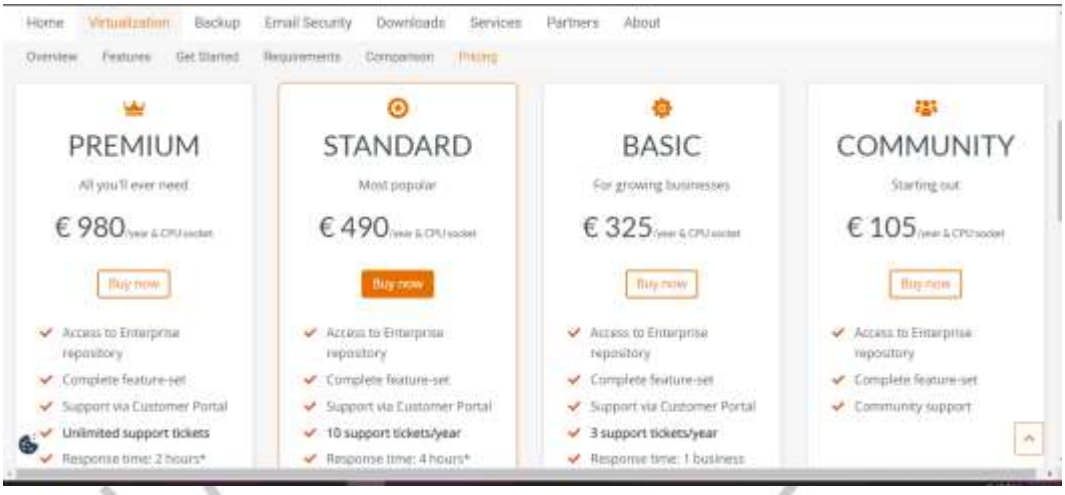
Kedua arah aliran email ini adalah bagian integral dari fungsi dari *Proxmox Mail Gateway* dalam memastikan keamanan dan keandalan komunikasi melalui email di dalam suatu jaringan.

Proxmox Mail Gateway memiliki beberapa opsi langganan berbeda yang dapat disesuaikan dengan kebutuhan bisnis dan jumlah pengguna yang diharapkan. Opsi langganan umumnya termasuk:

1. *Basic Subscription*: ini mungkin mencakup dukungan dasar dan pembaruan reguler untuk *platform Proxmox Mail Gateway*. Biasanya, ini adalah opsi terendah dalam hal fitur dan dukungan.
2. *Standard Subscription*: menawarkan dukungan yang lebih luas, pembaruan berkala, serta mungkin beberapa fitur tambahan seperti integrasi yang lebih baik, pemantauan yang diperkuat, atau keamanan tambahan.
3. *Enterprise Subscription*: jenis langganan ini biasanya memberikan akses ke semua fitur, dukungan prioritas yang lebih cepat, dan kadang-kadang layanan tambahan seperti konsultasi arsitektur, keamanan tambahan, atau integrasi khusus.

Biaya langganan dapat bervariasi berdasarkan beberapa faktor:

- Jumlah Pengguna/Domain: banyak model harga berbasis pada jumlah pengguna yang diatur atau domain yang dikelola.
- Level Dukungan: semakin tinggi level dukungan yang dipilih, semakin besar biayanya.



Gambar 4.2.4. 17 Subscription Pricing

Pemilihan antara langganan berbayar dan versi gratis Proxmox Mail Gateway tergantung pada kebutuhan dan prioritas spesifik Anda. Berikut adalah perbandingan umum antara keduanya:

Proxmox Mail Gateway Community Edition (Gratis):

- Biaya: tidak ada biaya lisensi; gratis untuk digunakan.
- Fitur Dasar: menyediakan fungsi dasar untuk perlindungan email, seperti perlindungan dari spam, virus, dan fitur dasar keamanan lainnya.
- Kustomisasi: keterbatasan dalam fitur dan kemampuan kustomisasi yang tersedia.
- Dukungan: dukungan komunitas mungkin tersedia melalui forum atau dokumentasi online, namun, tidak ada dukungan resmi dari Proxmox.

Proxmox Mail Gateway Subscription Edition (Berbayar):

- Biaya: berbayar, dengan harga beragam tergantung pada level langganan yang dipilih.
- Dukungan: mendapatkan dukungan teknis resmi dari tim *Proxmox*, termasuk pembaruan rutin, bantuan langsung, dan pemecahan masalah.
- Kustomisasi dan Skalabilitas: lebih banyak opsi untuk kustomisasi dan kemungkinan dukungan untuk skala bisnis yang lebih besar.

Exchange Online Protection (EOP) adalah layanan keamanan email yang disediakan oleh Microsoft sebagai bagian dari paket layanan *Office* 365. Fungsinya adalah untuk melindungi lingkungan email dari berbagai ancaman keamanan seperti *spam, malware, virus, phishing*, dan serangan siber lainnya.

Berikut adalah beberapa fitur utama dan fungsi dari *Exchange Online Protection*:

1. Filter Spam dan *Phishing*:

- Mendeteksi dan menyaring email yang dianggap *spam* atau *phishing* sebelum mencapai kotak masuk pengguna.
- Memiliki kemampuan untuk menandai, mengarahkan ke folder *spam*, atau memblokir email yang dianggap mencurigakan.

2. Perlindungan *Anti-Malware*:

- Mendeteksi dan menghapus *malware*, *virus*, atau konten berbahaya lainnya yang dapat menyebabkan kerusakan pada sistem.

3. Pencegahan kehilangan data (*Data Loss Prevention* - DLP):

- Melindungi data sensitif dengan mencegah pengiriman atau penerimaan email yang mengandung informasi rahasia.
- Memberikan kontrol untuk mengatur aturan yang melindungi data perusahaan.

4. Kebijakan *transport*:

- Memungkinkan organisasi untuk menerapkan aturan yang mengatur aliran email dalam organisasi, seperti pengalihan email, enkripsi, atau tindakan lainnya.

5. Analisis dan Pelaporan:

- Memberikan laporan terkait email masuk dan keluar, serta aktivitas keamanan lainnya untuk memungkinkan pemantauan dan analisis keamanan yang efektif.

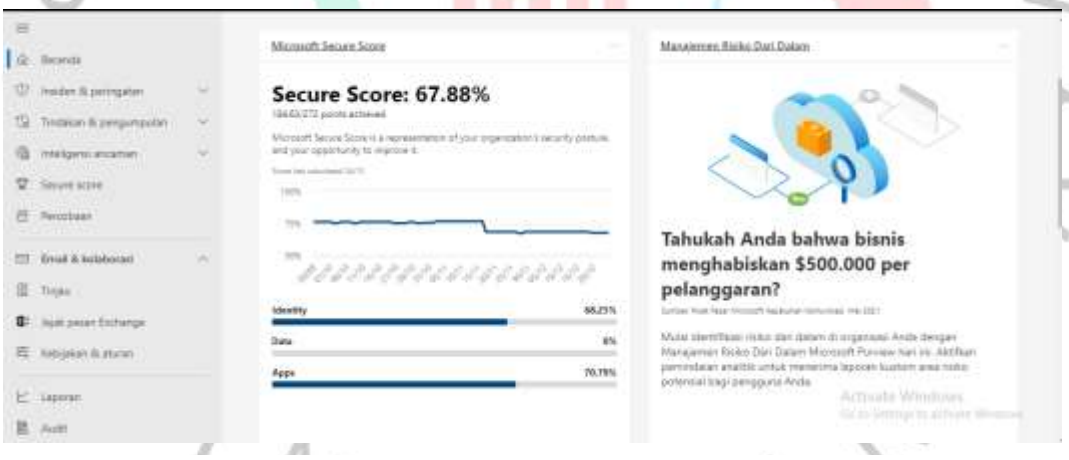
6. Integrasi dengan layanan *Office* 365:

- Menyediakan integrasi yang solid dengan layanan *office* 365 lainnya, memastikan keamanan email terintegrasi dengan solusi produktivitas Microsoft yang lain.

7. Skalabilitas dan ketersediaan tinggi:

- Dirancang untuk memenuhi kebutuhan organisasi dari skala kecil hingga besar dengan ketersediaan tinggi dan keandalan.

EOP adalah solusi yang fleksibel yang memungkinkan organisasi untuk mengelola dan mengkonfigurasi keamanan email sesuai dengan kebutuhan. Ini membantu melindungi organisasi dari berbagai ancaman keamanan email yang dapat mengganggu produktivitas dan keamanan sistem.



Gambar 4.2.4. 18 Secure Score

Microsoft secure score merupakan sebuah sebuah skor atau metrik yang digunakan untuk menilai tingkat keamanan Microsoft 365 (sebelumnya *office* 365) atau Azure. Skor ini menunjukkan seberapa baik organisasi atau perusahaan telah menggunakan berbagai fitur keamanan yang tersedia dalam layanan Microsoft.

Dalam upaya untuk meningkatkan keamanan sistem, skor *secure* menunjukkan seberapa baik suatu lingkungan telah mengikuti praktik keamanan terbaik yang direkomendasikan oleh Microsoft. Skor ini dapat membantu

administrator IT atau tim keamanan memahami area mana yang perlu diperbaiki atau ditingkatkan.

Dengan *secure score*, pengguna dapat melihat saran keamanan, solusi untuk meningkatkan skor keamanan, dan bagaimana setiap tindakan berdampak pada skor keamanan secara keseluruhan. Ini membantu organisasi mengelola ancaman keamanan dan meningkatkan perlindungan.

Konsep dasar *secure score* adalah memberikan poin kepada organisasi berdasarkan seberapa baik mereka menerapkan protokol keamanan yang disarankan Microsoft. Poin-poin ini diberikan kepada organisasi saat mereka mengaktifkan atau melakukan tindakan yang dapat meningkatkan keamanan lingkungan mereka.

Untuk meningkatkan skor keamanan, *secure score* biasanya menawarkan saran dan tindakan yang dapat dilakukan oleh admin IT atau tim keamanan. Ini dapat termasuk mengaktifkan fitur keamanan tambahan, mengubah kebijakan keamanan, memberikan pelatihan pengguna terkait keamanan, atau mengikuti praktik terbaik yang disarankan Microsoft.

Dengan *secure score*, pengelola dapat:

- Evaluasi Keamanan: berdasarkan rekomendasi keamanan Microsoft, menilai tingkat keamanan saat ini. Rekomendasi: Mendapatkan saran tentang tindakan yang dapat diambil untuk meningkatkan keamanan.
- Pemantauan Perubahan: melacak skor keamanan secara berkala untuk mengetahui apakah ada perubahan.
- Prioritas Tindakan: pilih langkah-langkah yang paling penting untuk meningkatkan keamanan.

Dengan memperoleh pemahaman yang lebih baik tentang kekurangan atau area infrastruktur IT yang perlu ditingkatkan, skor keamanan memungkinkan organisasi untuk lebih proaktif dalam mengelola ancaman keamanan.

Selain itu, *secure score* memberikan laporan dan informasi yang dapat membantu organisasi memahami dampak dari tindakan keamanan yang diambil terhadap keamanan secara keseluruhan. Ini membantu dalam pengambilan keputusan yang lebih terarah untuk meningkatkan pertahanan terhadap serangan siber.

Gambar 4.2.4. 19 Fitur Preview

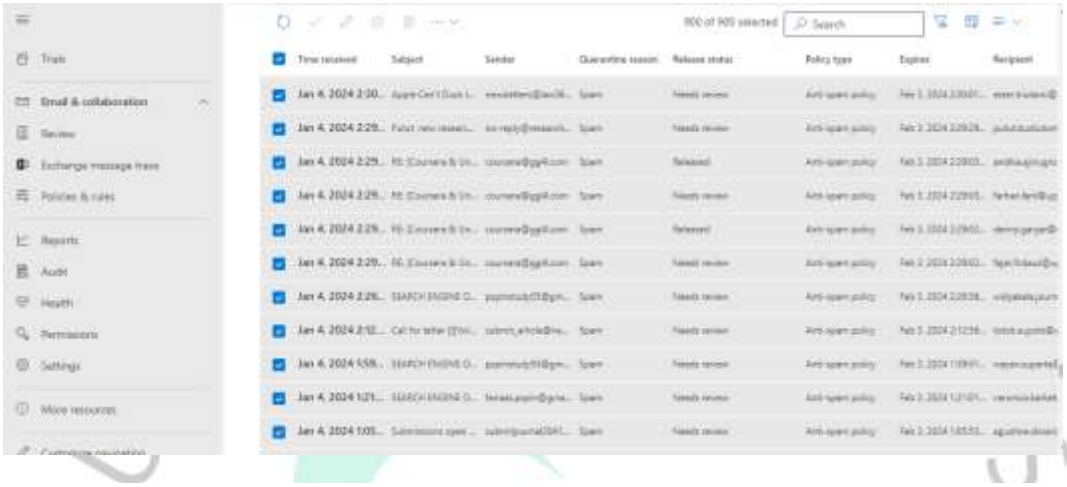
Fitur *preview* pada EOP (*Exchange Online Protection*) adalah kemampuan untuk melihat atau memeriksa pesan email yang masuk ke dalam sistem sebelum pesan-pesan tersebut benar-benar diserahkan ke kotak masuk pengguna. Fitur ini memungkinkan administrator atau pengguna untuk melihat cuplikan atau informasi dasar tentang email yang diterima, seperti subjek, pengirim, alamat email penerima, dan mungkin cuplikan dari isi pesan tersebut.

Dengan fitur *preview* ini, pengguna dapat memverifikasi email yang masuk untuk memastikan bahwa pesan tersebut aman sebelum membuka atau mengaksesnya sepenuhnya. Ini dapat membantu dalam mengidentifikasi email yang mencurigakan atau berpotensi berbahaya, seperti phishing atau malware, sebelum membuka pesan secara lengkap.

Pada fitur *preview* ini dibagi menjadi 2 bagian yaitu *Quarantine* dan Entitas terbatas, pada fitur *quarantine* terdapat beberapa email yang dianggap sebagai ancaman spam. Seperti pada gambar dibawah ini.

Karantina adalah fitur *Exchange Online Protection* (EOP) yang memungkinkan *administrator* untuk memindahkan email yang dianggap

mencurigakan atau berbahaya ke area terisolasi yang disebut karantina. Ini memberi mereka kesempatan untuk memeriksa email tersebut sebelum membuat keputusan apakah mengizinkannya atau mengambil tindakan tambahan.



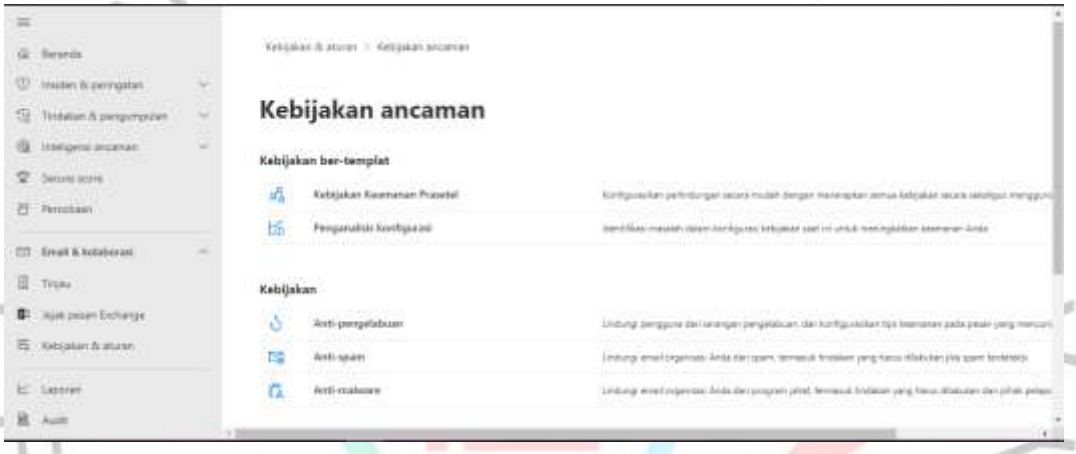
Gambar 4.2.4. 21 Quarantine

Gambar 4.2.4. 20 Entitas Terbatas

Pada entitas terbatas dijelaskan bahwa fitur ini merupakan sebuah fitur yang membuka pengguna email yang sebelumnya telah diblokir. Seperti pada gambar dibawah ini.

Kebijakan (*Policies*) dan Aturan (*Rules*) dalam *Exchange Online Protection* (EOP) adalah komponen penting yang memungkinkan pengguna untuk mengatur dan mengelola aliran email dengan lebih terperinci.

Kebijakan (*Policies*) dan Aturan (*Rules*) dalam *Exchange Online Protection* (EOP) adalah komponen penting yang memungkinkan pengguna untuk mengatur dan mengelola aliran email dengan lebih terperinci. Di dalam fitur *Policies* dan *Rules* terdapat fitur *Anti-spam* yang memungkinkan pengguna untuk membuat kebijakan anti-spam yang khusus untuk mengidentifikasi dan menangani pesan-pesan *spam*. Ini mencakup penyesuaian *filter*, tindakan yang diambil terhadap pesan yang diidentifikasi sebagai *spam*, dan penyesuaian level keparahan untuk *spam*.



Gambar 4.2.4. 22 Policies and Rule

Gambar 4.2.4. 23 Anti-Spam Policies

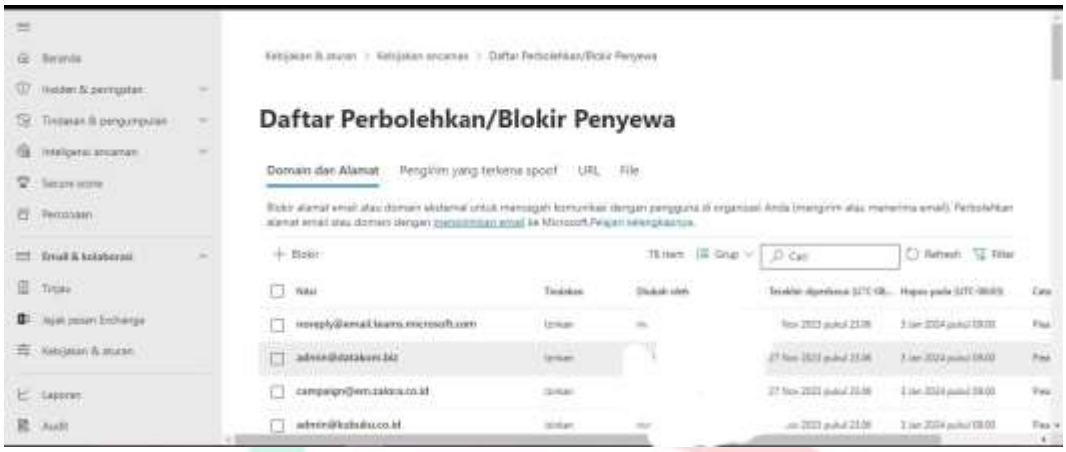
Anti-Spam Policies dalam *Exchange Online Protection* (EOP) adalah serangkaian fitur dan pengaturan yang memungkinkan pengguna untuk mengurangi jumlah pesan spam yang masuk ke lingkungan email organisasi mereka. Beberapa fitur kunci dari *Anti-Spam Policies* di EOP meliputi:

Inbound *Anti-Spam Policies* di *Exchange Online Protection* (EOP), tujuan *inbound* Melindungi lingkungan email organisasi dari pesan *spam*, *malware*, dan ancaman yang masuk dari luar organisasi. Fokus Utama dari EOP yaitu menyaring dan menangani pesan-pesan yang masuk ke kotak masuk pengguna.Fitur Utama:

- Penggunaan *filter* untuk mengidentifikasi dan memblokir pesan spam atau berbahaya.
- Konfigurasi daftar putih (*whitelist*) dan daftar hitam (*blacklist*) untuk mengizinkan atau memblokir pengirim tertentu.
- *Advanced Threat Protection* (ATP) untuk deteksi ancaman tingkat lanjut seperti *phishing* dan *malware*.
- Karantina pesan yang dicurigai untuk memungkinkan tinjauan lebih lanjut sebelum sampai ke pengguna akhir.

Outbound Anti-Spam Policies di *Exchange Online Protection* (EOP), tujuan *outbound* untuk mencegah email dari organisasi dikategorikan sebagai *spam* oleh penerima dan menjaga reputasi alamat IP organisasi. Fokus utama yaitu Memastikan email yang keluar dari organisasi mematuhi standar *anti-spam* dan tidak terblokir oleh penyaringan penerima. Fitur Utama:

- Melakukan pemindaian email yang akan dikirim dari organisasi untuk memastikan bahwa pesan tersebut tidak terdeteksi sebagai *spam*.
- Menerapkan kebijakan enkripsi jika diperlukan.
- Mencegah pengiriman email dari alamat IP yang teridentifikasi sebagai sumber *spam*.



Gambar 4.2.4. 24 Whitelist and blacklist

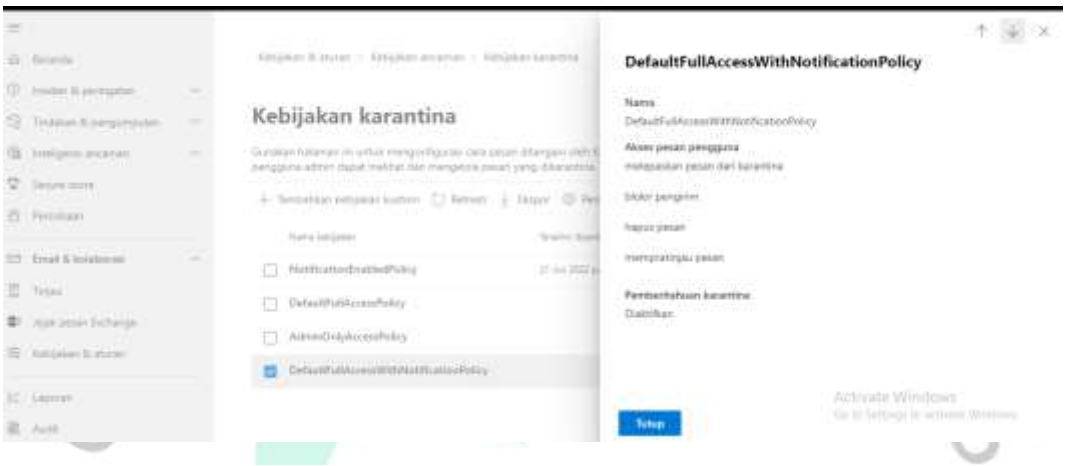
Fitur allow list dan *blacklist* pada *Exchange Online Protection* (EOP) digunakan untuk mengontrol dan mengelola email yang masuk ke dalam lingkungan email perusahaan.

1. *Allow List* (Daftar Putih): Ini memungkinkan pengguna untuk menentukan alamat email atau *domain* tertentu yang diizinkan untuk masuk ke dalam kotak masuk pengguna. Email dari alamat atau *domain* yang ada dalam daftar putih akan diterima secara otomatis tanpa ditolak atau diarahkan ke folder *spam*.

2. *Blacklist* (Daftar Hitam): Fitur ini memungkinkan pengguna untuk menentukan alamat email atau *domain* yang akan ditolak atau diarahkan secara otomatis ke *folder spam*. Email dari alamat atau domain yang ada dalam daftar hitam akan diblokir dan tidak akan masuk ke kotak masuk pengguna.

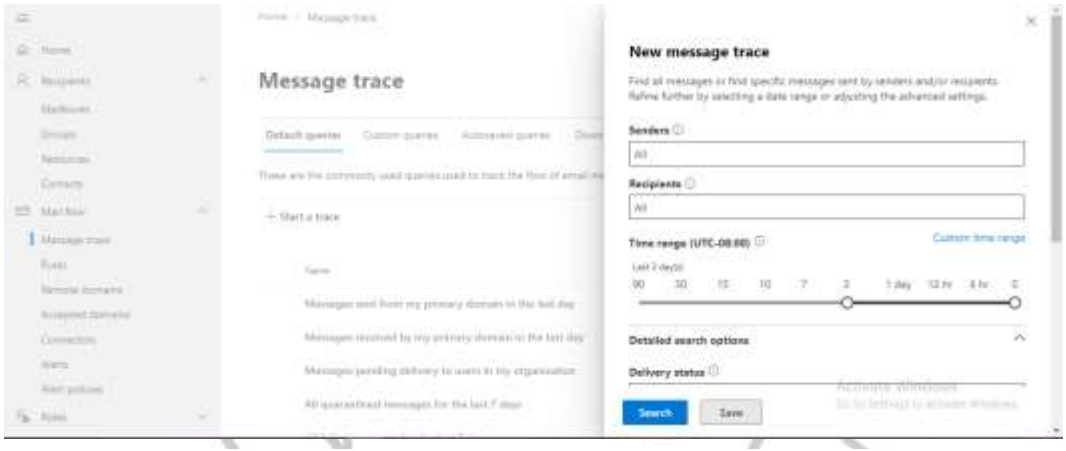
Dengan menggunakan kedua fitur ini, pengguna dapat meningkatkan keamanan email perusahaan dengan membatasi atau memperbolehkan email dari sumber yang

telah ditentukan. Ini membantu dalam mengurangi risiko menerima email berbahaya atau spam yang dapat merugikan lingkungan kerja.



Gambar 4.2.4. 25 Quarantine Policy

Quarantine Policy pada *Exchange Online Protection* (EOP) adalah aturan yang dapat dikonfigurasi untuk mengelola email yang dianggap mencurigakan atau berpotensi berbahaya. Ini merupakan salah satu fitur keamanan yang memungkinkan pengguna untuk memasukan email yang dianggap mencurigakan ke dalam karantina, sehingga tidak langsung pindah ke *folder* penerima.

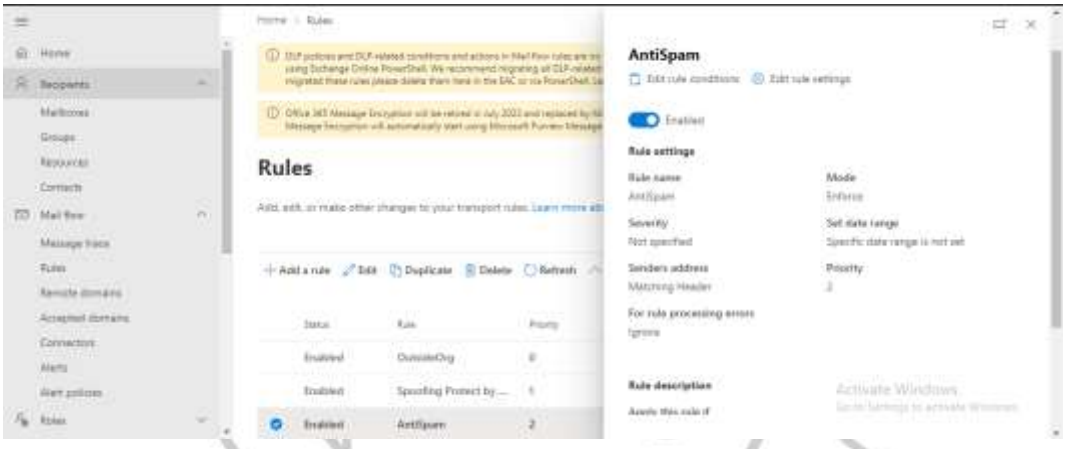


Gambar 4.2.4. 26 Message Trace

Message Trace pada *Exchange Online Protection* adalah fitur yang memungkinkan *administrator* untuk melacak perjalanan email melalui infrastruktur *exchange online*. Dengan menggunakan *message trace*, pengguna dapat melakukan pencarian dan pemantauan terhadap email yang masuk dan keluar dari organisasi. Fitur ini memungkinkan pengguna untuk menelusuri pesan berdasarkan beberapa kriteria seperti pengirim, penerima, rentang waktu, dan status pengiriman.

Cara mengatur *message trace* yaitu dengan melakukan pengaturan kriteria pencarian lalu menjalankan pengaturan untuk pencarian dan menemukan hasil pencarian. Berikut :

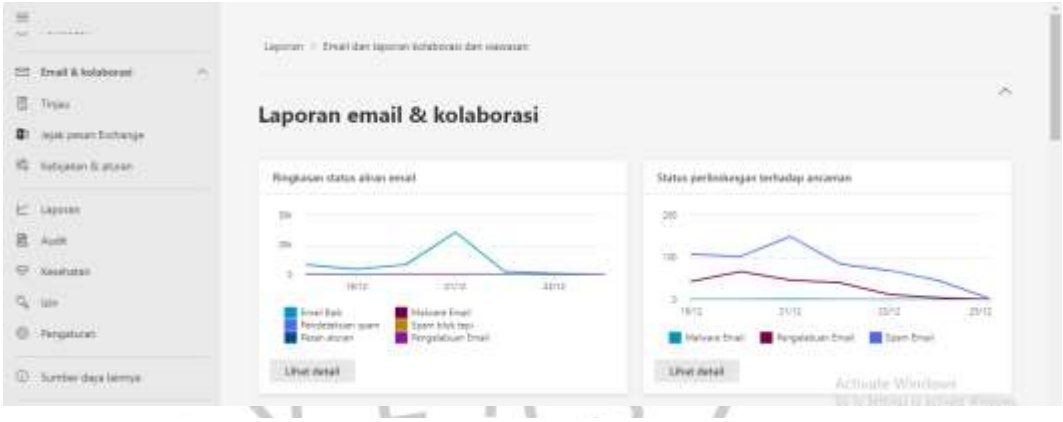
- Atur kriteria pencarian: pilih kriteria pencarian seperti rentang waktu, pengirim, penerima, subjek email, status pengiriman, dll.
- Jalankan pencarian: setelah mengatur kriteria pencarian, jalankan pencarian dengan mengklik "*Search*" atau "*Run Trace*".
- Lihat hasil pencarian: setelah pencarian selesai, hasil pencarian akan ditampilkan. Anda dapat melihat detail pesan yang sesuai dengan kriteria pencarian



Gambar 4.2.4. 27 Rules

Fitur *rules* pada EOP (*Exchange Online Protection*) merupakan kemampuan untuk membuat aturan atau kebijakan yang mengatur bagaimana pesan email dikelola, diarahkan, atau diperlakukan oleh sistem keamanan email. Contoh sebagai berikut :

- *Filtering Spam* dan *Malware*: *administrator* dapat membuat aturan untuk secara otomatis mengarahkan email yang diidentifikasi sebagai spam atau mengandung malware ke folder spam atau untuk ditandai sebagai email berbahaya.



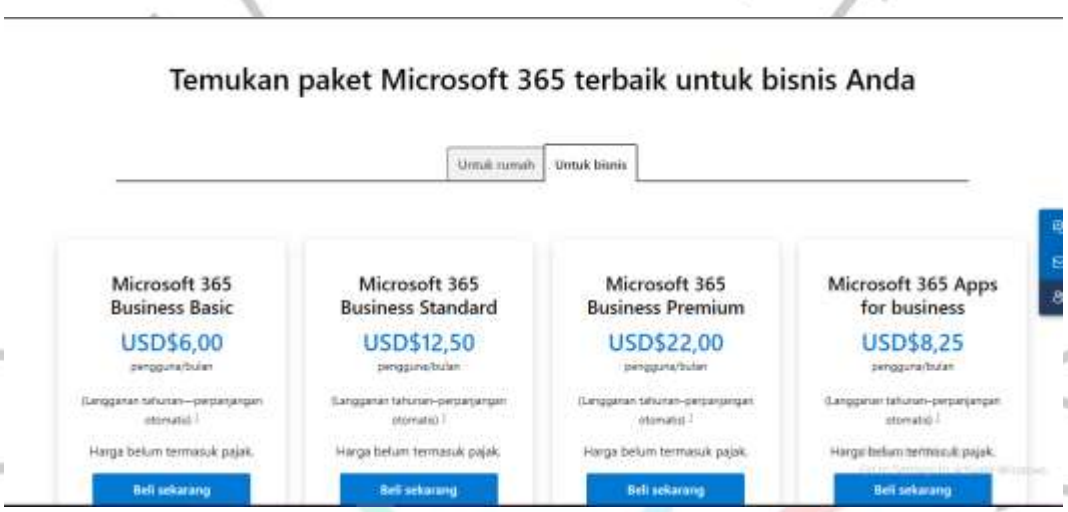
Gambar 4.2.4. 28 Laporan

Fitur Laporan pada *Exchange Online Protection* (EOP) memberikan informasi yang sangat berguna terkait keamanan email. Beberapa fitur laporan yang umumnya tersedia di EOP meliputi:

1. Laporan keamanan email: memberikan informasi tentang serangan email yang berhasil dicegah, seperti deteksi *malware, phishing,* atau serangan yang berpotensi membahayakan.
2. Ringkasan keamanan: menampilkan ringkasan aktivitas keamanan untuk email yang masuk dan keluar, termasuk jumlah email yang diblokir atau diizinkan, serta alasan-alasan di balik tindakan tersebut.
3. Laporan analisis keamanan: memberikan insight lebih mendalam tentang serangan yang terdeteksi, seperti bagaimana serangan itu dilakukan, siapa yang menjadi target, dan bagaimana sistem keamanan menanggapi serangan tersebut.
4. Laporan keandalan pengiriman email: menampilkan statistik tentang pengiriman email, meliputi email yang dikirim, diterima, ditolak, serta alasan penolakan pengiriman email.
5. Laporan manajemen risiko: memberikan informasi tentang risiko keamanan yang teridentifikasi dalam sistem, memberikan pandangan mengenai area mana yang memerlukan perhatian lebih lanjut untuk memperkuat keamanan.

6. Laporan kinerja sistem: memberikan informasi tentang kinerja sistem EOP, termasuk waktu respons, latensi, dan statistik kinerja lainnya untuk membantu dalam pemantauan dan peningkatan kinerja.

Laporan-laporan ini biasanya dapat disesuaikan dan dikonfigurasi sesuai kebutuhan perusahaan atau *administrator* IT yang mengelola *Exchange Online Protection*. Mereka memberikan pemahaman yang lebih baik tentang jenis ancaman yang dihadapi oleh sistem email dan membantu dalam pengambilan keputusan terkait dengan perbaikan keamanan.



Gambar 4.2.4. 29 Lisensi

Exchange Online Protection (EOP) termasuk dalam lisensi Microsoft 365 atau *Office* 365. EOP adalah bagian integral dari layanan email yang disediakan oleh Microsoft dalam paket langganan mereka.

Untuk mendapatkan akses ke *Exchange Online Protection*, umumnya perlu memiliki salah satu dari paket langganan berikut:

1. Microsoft 365 *Business Basic*: ini adalah paket dasar yang mencakup layanan email, aplikasi *web Office*, dan *Exchange Online Protection* untuk perlindungan email dasar.

2. Microsoft 365 *Business Standard*: paket ini mencakup semua fitur dari *Business Basic* dan menambahkan aplikasi *desktop Office* (*Word, Excel, PowerPoint, Outlook*) serta *Exchange Online Protection*.

3. Microsoft 365 *Enterprise Plans*: ada juga berbagai rencana *Enterprise* yang menawarkan layanan yang lebih canggih, seperti Microsoft 365 E3 atau E5, yang mencakup fitur-fitur keamanan yang lebih lanjut selain *Exchange Online Protection.*

4. *Exchange Online Plan* 1 dan *Plan* 2: jika hanya memerlukan layanan email dan perlindungan dasar, juga bisa mendapatkan akses ke EOP melalui rencana ini.

Setiap paket tersebut menawarkan tingkat akses yang berbeda terhadap *Exchange Online Protection*, dengan tingkat perlindungan yang sesuai. Lisensi tersebut memberikan akses ke fitur-fitur keamanan, laporan, dan kontrol yang terkait dengan EOP.

Penting untuk memilih paket yang sesuai dengan kebutuhan perusahaan Anda, karena berbagai paket ini menawarkan tingkat layanan dan keamanan yang berbeda. Hal ini bisa termasuk perbedaan dalam fitur perlindungan, tingkat akses terhadap laporan, dan kemampuan manajemen keamanan yang lebih canggih.

Table 4.2.4. 1Tabel data variabel yang dibutuhkan

No.	*Proxmox Mail Gateway*	*Exchange Online Protection*
1.	Presentase Tingkat Keamanan	Presentase Tingkat Keamanan
2.	Kemudahan dalam Penggunaan	Kemudahan dalam Penggunaan
3.	Fleksibilitas	Fleksibilitas
4.	Ketersediaan Fitur	Ketersediaan Fitur
5.	Biaya	Biaya
6.	*Performance*	*Performance*

4.2.6 Studi Pustaka

Dalam penelitian terdahulu salah satu studi literatur diatas memiliki kesamaan penelitian yang dilakukan dengan penelitian ini, kesamaan nya ada pada abstrak dari penelitian tersebut. Judul dari penelitian diatas yaitu *Design and Build Mail server Systems Using Zimbra 8.8.15 and Antispam on Proxmox Mail Gateway*.

Table 4.2.6. 1 Tabel studi pustaka perbandingan

Jurnal	Abstrak
Design and Build Mail server Systems Using Zimbra 8.8.15 and Antispam on Proxmox Mail Gateway.	Media email atau surat elektronik saat ini terus berkembang dan penggunanya pun semakin banyak. Namun kenyamanan dan keamanan berkomunikasi melalui email kini sudah sangat berkurang. Salah satu penyebab berkurangnya tingkat keamanan dan kenyamanan dalam menggunakan email adalah spam. Spam adalah email yang masuk ke email pengguna yang tidak pernah diminta dan diinginkan pengguna, jika spam dibiarkan di kotak masuk email maka akan membuat kapasitas penyimpanan penuh dan dapat membuat server email down. Untuk menghindari dan mencegah hadirnya email spam maka mail server Zimbra 8.8.15 memerlukan *anti spam* untuk dapat memblokir email spam yang akan masuk. *Anti spam* yang akan digunakan adalah Proxmox Mail Gateway 5.2 karena menggunakan fitur LDAP (Light Weight Directory Access Protocol)

Dalam *proxmox mail gateway* yang digunakan dalam penelitian ini yaitu menggunakan PMG *open source* yang tidak berbayar, lalu digunakan untuk membandingkannya dengan *exchange online protection*. Lalu untuk fitur yang ada tetap sama dan sesuai dengan yang ada pada arsitektur sistem yang ada pada gambar 4.2.1 dan 4.2.2.

Penelitian ini digunakan untuk membandingkan dengan *platform exchange online protection*, hal ini dilakukan karena minimnya penelitian terdahulu dengan menggunakan *proxmox mail gateway*. Dalam penelitian terdahulu di awali dengan membuat metode *research* dengan membuat rancangan jaringan usulan lalu dilakukan instalasi dan konfigurasi jaringan, instalasi dan konfigurasi ubuntu, Zimbra dan *proxmox mail gateway* lalu pengujian *mail server* dan pengujian *anti-spam proxmox mail gateway.*

Gambar 4.2.6. 1 Metode research penelitian terdahulu