# BAB V
# HASIL DAN PEMBAHASAN

Bab ini memaparkan hasil dari penelitian yang dilakukan serta pembahasan hasil dari penelitian. Berikut merupakan uraian dari hasil dan pembahasan dari penelitian ini.

## 5.1 Hasil

Setelah melakukan penelitian perbandingan dan analisis yang digunakan pada bab 4, serta diagram alur cara kerja dari masing-masing *platform* peneliti mendapatkan hasil sebagai berikut.

*Table 5.1. 1 Table Data Observasi*

| No. | Variabel | Proxmox Mail Gateway | Exchange Online Protection |
|---|---|---|---|
| 1. | Presentase keamanan | Pada *platform* ini Tingkat keamanan tidak dapat diprediksi namun didukung dengan fitur keamanan sebagai factor pertimbangan | Pada platform ini juga sama, yaitu tidak memberikan presentase tidak dapat diberikan secara angka, namun dapat melakukan peningkatan terhadap fitur yang ada pada *exchange online protection*. |
| 2. | Kemudahan penggunaan | Pada *platform* ini membutuhkan beberapa referensi yang kuat mengenai konfigurasi yang dilakukan. | Pada *platform* ini menawarkan beberapa kemudahan dalam penggunaan |
| 3. | Fleksibilitas | Pada *platform* ini Memiliki penyesuaian kompleks dalam kebutuhan pengguna | Pada *platform ini* pengguna dapat menyesuaikan beberapa kebutuhan yang unik sesuai keinginan |
| 4. | Ketersediaan Fitur | Pada *platform* ini menawarkan beberapa fitur untuk meningkatkan keamanan email dan manajemen pesan | Pada *platform* ini menawarkan beberapa fitur untuk meningkatkan keamanan email dan manajemen pesan |
| 5. | Biaya | Pada *platform* ini bersifat *Open-Source* namun terdapat penawaran harga untuk setiap fitur tambahan | Memiliki harga yang berbeda-beda namun sudah termasuk paket dalam office365 |
| 6. | Kinerja | *Platform* ini memiliki Tingkat kinerja yang optimal, hal ini didukung oleh factor pendukung | *Platform* ini memberikan Tingkat kinerja yang cepat |

*Table 5.1. 2 Analisis SWOT*

| No | SWOT | *Proxmox Mail Gateway* | *Exchange Online Protection* |
|---|---|---|---|
| 1. | *Strength* | Sumber terbuka (open source) yang dapat disesuaikan | Terintegrasi dengan Microsoft 365 secara mulus |
| | | Perlindungan keamanan yang kokoh untuk email | Alat manajemen yang kuat untuk administrator |
| 2. | *Weaknesses* | Memerlukan pengetahuan teknis yang lebih untuk konfigurasi awal | Biaya langganan yang mungkin tinggi untuk beberapa paket |
| | | Dukungan terhadap berbagai lingkungan mungkin kurang jelas | Bergantung pada koneksi internet yang stabil |
| 3. | *Opportunities* | Penyesuaian yang fleksibel sesuai kebutuhan organisasi | Penambahan fitur keamanan baru dari Microsoft secara berkala |
| | | Potensi pengembangan komunitas *open source* yang aktif | Integrasi yang lebih baik dengan ekosistem Microsoft 365 |
| 4. | *Threats* | Persaingan dengan produk serupa yang sudah mapan | Perubahan aturan keamanan yang tiba-tiba dari Microsoft |
| | | Ketidaktahuan pengguna akan opsi alternatif yang ada | Ancaman keamanan yang terus berkembang dan kompleks |

## 5.2 Pembahasan

### 5.2.1 Exchange Online Protection (EOP)

#### 1. Presentase tingkat keamanan pada Exchange Online Protection

*Exchange Online Protection* (EOP) adalah bagian dari layanan Microsoft 365 yang memberikan perlindungan keamanan untuk email. Namun, Microsoft atau penyedia layanan sejenis tidak selalu memberikan informasi rinci tentang presentase tingkat keamanan untuk layanan ini.

Microsoft biasanya tidak memberikan angka pasti tentang presentase tingkat keamanan untuk layanan. Fokusnya lebih kepada penerapan berbagai fitur keamanan yang bertujuan untuk mengurangi kemungkinan serangan *phishing, malware,* dan *spam* email.

Meskipun tingkat keamanan tidak dapat diprediksi, Microsoft secara teratur memperbarui dan meningkatkan fitur keamanan *Exchange Online Protection*. Pembaruan ini mencakup definisi *anti-virus*, *filter spam*, deteksi ancaman, dan peningkatan teknologi keamanan.

Secara umum, EOP menawarkan perlindungan email yang kuat. Namun, perlu untuk di ingat bahwa tidak ada solusi keamanan yang 100% bebas dari risiko. Untuk melindungi data sensitif, selalu disarankan untuk menggunakan lapisan keamanan tambahan dan praktik keamanan yang baik.

**2. kemudahan penggunaan Exchange Online Protection**

*Exchange Online Protection* (EOP) dibuat untuk memberikan perlindungan keamanan email yang kuat sambil tetap mudah digunakan bagi pengguna bisnis. EOP menawarkan beberapa kemudahan penggunaan, seperti:

- **Integrasi Mudah dengan Microsoft 365:**

EOP terintegrasi dengan Microsoft 365, membuatnya mudah untuk diimplementasikan dan dikelola. Pengguna yang sudah terbiasa dengan microsoft akan dapat menggunakan fitur EOP dengan cepat tanpa perlu mempelajari platform baru secara menyeluruh.

- **Antarmuka Pengguna yang Intuitif:**

Melalui antarmuka pengguna yang bersih dan ramah pengguna, EOP memungkinkan *administrator* untuk mengatur kebijakan keamanan email, mengontrol pengaturan *filter*, dan melakukan tindakan perlindungan lainnya dengan mudah.

- **Otomatisasi dan Pemantauan:**

EOP menawarkan fitur otomatisasi yang membantu memantau email untuk mengidentifikasi ancaman keamanan seperti *malware, phishing,* dan spam. Ini membebaskan *administrator* dari tugas manual yang membosankan dan memungkinkan mereka untuk fokus pada penanganan kasus yang memerlukan perhatian khusus.

- **Pembaharuan Terjadwal:**

Microsoft secara teratur melakukan pembaruan keamanan dan fitur baru pada layanan EOP, memastikan bahwa solusi keamanan email selalu *update* dan dapat melindungi mereka dari ancaman terbaru.

- **Dukungan dan Sumber Daya:**

Untuk membantu administrator memahami dan menggunakan EOP dengan lebih baik, microsoft menyediakan berbagai sumber daya dukungan, dokumentasi, dan panduan, termasuk tutorial, forum komunitas, dan dokumentasi teknis yang terus diperbarui.

- **Konfigurasi yang Dapat Disesuaikan:**

EOP memberi *administrator* kemampuan untuk menyesuaikan kebijakan keamanan untuk memenuhi kebutuhan perusahaan. Pengguna dapat mengubah pengaturan *filter*, mengawasi daftar putih dan hitam, dan mengubah tingkat keamanan sesuai dengan preferensi organisasi.

*Exchange Online Protection* sangat bergantung pada integrasinya dengan *platform* Microsoft 365, antarmuka pengguna yang mudah digunakan, otomatisasi, dukungan, dan kemampuan untuk disesuaikan sesuai kebutuhan bisnis. Ini memastikan bahwa pengguna dapat mengelola keamanan email dengan mudah tanpa mengorbankan kemudahan penggunaan.

### 3. Fleksibilitas dan Penyesuaian pada Exchange Online Protection

Untuk memenuhi kebutuhan keamanan email yang berbeda, *Exchange Online Protection* (EOP) menawarkan berbagai opsi fleksibilitas dan penyesuaian, seperti berikut:

- **Konfigurasi Kebijakan Keamanan yang Terperinci:**

*Administrator* memiliki kemampuan untuk menyesuaikan kebijakan keamanan email dengan EOP. *Administrator* dapat mengubah aturan *filter* untuk mengidentifikasi dan menangani ancaman seperti *phishing, malware,* atau *spam*. Ini termasuk mengubah tingkat keamanan yang dapat disesuaikan, mengatur tindakan yang diambil terhadap email yang dianggap mencurigakan, dan lainnya.

- **Filterisasi yang Disesuaikan:**

*Administrator* memiliki kemampuan untuk menyesuaikan *filter* untuk membedakan email yang dianggap *spam*, email yang berasal dari sumber yang tidak

diinginkan, atau pesan yang masuk ke dalam kategori tertentu. Filterisasi ini dapat disesuaikan dengan mempertimbangkan parameter seperti kata kunci, pengirim, atau lainnya.

- **Manajemen Daftar Putih dan Hitam:**

EOP memungkinkan untuk mengelola daftar putih dan hitam. Kedua daftar ini memungkinkan pengguna untuk mengidentifikasi pengirim yang diizinkan atau diblokir secara khusus. Ini memungkinkan untuk mengontrol lebih banyak email yang diterima atau ditolak.

- **Integrasi dengan Layanan Eksternal:**

Meskipun EOP termasuk dalam solusi Microsoft 365, namun EOP juga dapat diintegrasikan dengan layanan keamanan eksternal atau pihak ketiga tertentu. Ini memberikan fleksibilitas tambahan bagi organisasi yang ingin menggunakan solusi keamanan tambahan yang mungkin mereka miliki atau layanan yang lebih khusus untuk kebutuhan bisnis.

- **Audit dan Pelaporan yang Dapat Disesuaikan:**

Kemampuan yang dapat disesuaikan untuk audit dan pelaporan disediakan oleh EOP. Untuk mendapatkan pemahaman yang mendalam tentang keamanan email organisasi, administrator dapat memantau aktivitas email, menganalisis keamanan, dan membuat laporan sesuai kebutuhan.

- **Perlindungan Berbasis Kebutuhan Bisnis:**

EOP dapat menyesuaikan tingkat keamanan dengan kebutuhan bisnis. Ini memungkinkan organisasi untuk menyesuaikan kebijakan keamanan mereka untuk sesuai dengan risiko yang dihadapi dan kebijakan keamanan internal.

*Exchange Online Protection* dapat disesuaikan dengan mudah sehingga organisasi dapat mengatur keamanan email sesuai dengan kebutuhan dan kebijakan internal. Ini memberikan kontrol yang lebih besar atas perlindungan email yang diterima dan dikirim.

**4. Ketersediaan Fitur pada Exchange Online Protection**

Beberapa fitur penting *Exchange Online Protection* (EOP) adalah sebagai berikut:

- **Proteksi terhadap *Malware* dan Virus:**

EOP memindai email untuk menemukan dan menghapus lampiran atau pesan yang mungkin mengandung *virus* atau *malware* sebelum mencapai kotak masuk pengguna.

- **Deteksi dan Penanganan *Phishing*:**

Pengaturan kebijakan dan fitur pengenalan pola memungkinkan EOP untuk menemukan pola *phishing* pada email yang masuk dan mengambil tindakan yang sesuai.

- **Filterisasi dan Pengaturan Kebijakan *Spam*:**

EOP memiliki *filter* yang kuat yang dapat membedakan email yang dianggap spam atau berasal dari sumber yang tidak diinginkan. *Administrator* dapat mengubah kebijakan spam sesuai dengan kebutuhan bisnis.

- **Perlindungan Terhadap Email Berbahaya:**

Fitur EOP melindungi email yang berpotensi berbahaya, seperti email dengan tautan atau *attachment* yang mencurigakan.

- **Enkripsi Email:**

EOP mendukung enkripsi email dengan menggunakan teknologi enkripsi yang kuat untuk melindungi informasi sensitif yang dikirim melalui email.

- **Pengaturan dan Konfigurasi Kebijakan yang Terperinci:**

*Administrator* memiliki kemampuan untuk menyesuaikan kebijakan keamanan yang sangat rumit. Ini termasuk mengatur aturan *filter*, mengubah cara menangani email yang mencurigakan, dan lainnya.

- **Manajemen Daftar Putih dan Hitam:**

*Administrator* dapat menyesuaikan daftar putih dan hitam untuk memberikan kontrol lebih lanjut atas email yang diterima atau ditolak serta mengizinkan atau memblokir pengirim tertentu.

- **Pelaporan dan Analisis Keamanan:**

EOP menyediakan alat untuk melacak dan menganalisis tren keamanan melalui laporan aktivitas email untuk mendapatkan pemahaman yang mendalam tentang keamanan email organisasi.

- **Integrasi dengan Layanan Keamanan Tambahan:**

Meskipun EOP merupakan bagian dari microsoft 365, itu dapat diintegrasikan dengan layanan keamanan eksternal atau pihak ketiga yang mungkin dimiliki oleh perusahaan.

- **Pembaruan Keamanan Berkala:**

Microsoft secara teratur melakukan pembaruan keamanan pada EOP untuk memastikan bahwa layanan ini tetap *update* dan aman dari serangan terbaru.

EOP dapat melindungi email organisasi dari berbagai risiko keamanan karena fitur yabg  disebutkan ini.

## 5. Biaya pada Exchange Online Protection

Harga *Exchange Online Protection* (EOP) berbeda-beda tergantung pada paket atau langganan microsoft 365 yang telah dipilih sebagian besar langganan microsoft 365 menyertakan *Exchange Online Protection* sebagai bagian dari paketnya.

Untuk mendapatkan informasi yang paling akurat tentang biaya EOP, sebaiknya langsung melihat halaman harga resmi dari Microsoft atau menghubungi tim penjualan mereka. Biaya EOP biasanya merupakan bagian dari biaya langganan Microsoft 365 yang mencakup berbagai layanan seperti *Exchange Online, SharePoint, OneDrive,* dan lainnya.

Perlu diingat bahwa biaya EOP bisa berbeda-beda tergantung pada paket microsoft 365 yang dipilih, jumlah pengguna, atau fitur tambahan yang mungkin perlukan. Microsoft juga sering kali memiliki opsi langganan yang berbeda untuk

bisnis kecil, perusahaan besar, atau institusi pendidikan yang bisa memiliki harga yang berbeda pula.

### 6. Kinerja dan Ketersediaan pada Exchange Online Protection

Salah satu komponen penting dari layanan email Microsoft dalam lingkup microsoft 365 adalah *Exchange Online Protection* (EOP). EOP dirancang untuk memberikan layanan email yang dapat diandalkan kepada pengguna dengan kinerja dan ketersediaan yang cukup baik.

- **Ketersediaan Layanan (*Availability*):**

Microsoft menunjukkan komitmennya terhadap ketersediaan layanan yang tinggi melalui kebijakan *Service Level Agreement* (SLA) yang menetapkan persentase ketersediaan layanan, biasanya sangat tinggi, seperti 99,9% atau lebih. Dengan demikian, Microsoft berkomitmen untuk memastikan bahwa layanan seperti exchange online protection tetap tersedia sepanjang waktu dengan sedikit gangguan atau waktu tidak aktif.

- **Performa dan Kecepatan:**

Secara umum, layanan EOP dirancang untuk memberikan kinerja yang cepat dan efisien dalam mendeteksi dan melindungi terhadap ancaman email seperti *malware, phishing,* dan *spam*. Meskipun ada beberapa faktor yang dapat mempengaruhi kinerja, seperti ukuran organisasi, tingkat lalu lintas email, dan konfigurasi jaringan, microsoft memiliki infrastruktur yang kuat untuk mengatasi permintaan yang tinggi dan mempertahankan kinerja yang baik.

- **Redundansi dan Pemulihan Bencana:**

Microsoft mengurangi kemungkinan kegagalan sistem dengan membangun redundansi dan pemulihan bencana dalam infrastruktur mereka. Bahkan dalam situasi darurat atau kegagalan perangkat keras, mereka dapat memastikan bahwa layanan tetap tersedia dengan pusat data yang tersebar secara geografis.

- **Pembaruan Keamanan:**

Microsoft secara teratur melakukan pembaruan keamanan pada EOP untuk menanggapi ancaman keamanan baru dan melindungi sistem dari serangan siber yang terus-menerus.

- **Pengukuran Kinerja dan Pemantauan:**

Microsoft yang menangani pemantauan kinerja layanan seperti EOP melakukannya dengan menggunakan metrik dan alat pemantauan yang canggih untuk mengukur kinerja, mengidentifikasi ancaman, dan merespons masalah dengan cepat.

- **Ketersediaan Fungsionalitas:**

Dalam kondisi normal, fitur penting dari *Exchange Online Protection*, seperti deteksi *malware, filter spam*, perlindungan terhadap email berbahaya, dan pengaturan kebijakan keamanan, biasanya dapat diakses secara bebas.

Microsoft berupaya keras untuk menjaga kinerja dan ketersediaan *Exchange Online Protection* sebaik mungkin bagi penggunanya, meskipun EOP dan kinerjanya cenderung tinggi.

### 5.2.2 Proxmox Mail Gateway

**1. Presentase tingkat keamanan pada proxmox mail gateway**

*Proxmox Mail Gateway* adalah alat keamanan email yang kuat, tidak ada cara untuk memberikan gambaran yang jelas tentang tingkat keamanan *Proxmox Mail Gateway*, perlu dipertimbangkan beberapa faktor:

1. **Fitur Keamanan Bawaan:** Dilengkapi dengan berbagai fitur keamanan, *Proxmox Mail Gateway* memiliki perlindungan terhadap *spam, antivirus, filtering* konten, enkripsi, dan perlindungan terhadap ancaman *phishing*. Keefektifan setiap fitur dapat meningkatkan keamanan secara keseluruhan.
2. **Pembaruan dan Pemeliharaan:** Seberapa cepat *platform* seperti *Proxmox Mail Gateway* menangani ancaman baru sering dikaitkan dengan tingkat keamanan. Untuk mempertahankan tingkat keamanan yang tinggi,

pembaruan rutin, pemeliharaan keamanan, dan penambahan fitur baru sangat penting.

3. **Konfigurasi Pengguna:** Cara pengguna menggunakan *Proxmox Mail Gateway* dapat berdampak pada keamanannya. Keamanan keseluruhan dapat ditingkatkan dengan pengaturan yang tepat, penerapan praktik keamanan, dan pelatihan pengguna dalam mengidentifikasi ancaman.
4. **Keamanan Jaringan:** Keamanan jaringan tempat solusi *Proxmox Mail Gateway* digunakan sangat penting. Lapisan keamanan tambahan seperti firewall, penggunaan VPN, atau teknologi keamanan jaringan lainnya dapat meningkatkan keamanan sistem secara keseluruhan.

Karena keamanan adalah proses yang terus berubah, tingkat keamanan atau presentase pasti biasanya tidak dapat diberikan secara langsung. Namun, berkat kombinasi fiturnya dan perawatan yang baik, *Proxmox Mail Gateway* dapat menangkal serangan email yang signifikan. Evaluasi dan pembaruan keamanan terus-menerus sangat penting untuk memastikan tingkat keamanan yang optimal.

**2. kemudahan penggunaan proxmox mail gateway**

Beberapa faktor yang membuat *Proxmox Mail Gateway* (PMG) menarik bagi pengguna yang mencari solusi yang dapat diimplementasikan dengan mudah untuk mengelola keamanan email:

- **Antarmuka Pengguna yang Intuitif:** PMG memiliki antarmuka pengguna yang mudah digunakan dan mudah dipahami, dan panel kontrolnya dirancang untuk memudahkan pengguna dengan tingkat keahlian teknis yang berbeda.
- **Konfigurasi Awal yang Mudah:** *Proxmox Mail Gateway* menyediakan *wizard* konfigurasi awal yang memandu pengguna melalui langkah-langkah untuk mengatur sistem dengan cepat. Ini dapat membantu dalam pemasangan yang cepat dan mulus.

- **Manajemen Email yang Efisien:** PMG memudahkan pengelolaan email dengan fitur seperti penanganan ancaman, pengaturan kebijakan email, dan *filter spam* yang dapat dikonfigurasi.
- **Pemantauan dan Laporan:** Dengan sistem pemantauan yang terintegrasi, pengguna dapat melacak kinerja sistem dan mengetahui aktivitas email yang berpotensi berbahaya. Selain itu, laporan yang mudah dipahami dan terorganisir tersedia untuk memberikan informasi yang diperlukan.
- **Dokumentasi yang Baik dan Komunitas yang Aktif:** *Proxmox Mail Gateway* memiliki dokumentasi yang baik dan mendukung serta komunitas pengguna yang aktif. Ini sangat membantu dalam menemukan jawaban atas pertanyaan, menyelesaikan masalah, atau memperoleh saran dan tips dari pengguna lain.

Meskipun PMG sangat mudah digunakan, keamanan dan konfigurasi yang tepat masih sangat penting. Namun, dengan antarmuka yang ramah pengguna dan fitur-fitur bawaannya, PMG dapat menjadi pilihan keamanan email yang mudah digunakan.

### 3. Fleksibilitas dan Penyesuaian pada *proxmox mail gateway*

*Proxmox mail gateway* memberikan fleksibilitas yang cukup besar dan memiliki beberapa opsi untuk penyesuaian bagi para pengguna untuk memenuhi kebutuhan keamanan email. Berikut beberapa kebutuhan flesibilitas dan peneysuaian yang ditawarkan *proxmox mail gateway* (PMG) :

- **Pengaturan Kebijakan:** Pengguna dapat menyesuaikan sendiri kebijakan keamanan dengan PMG, seperti menetapkan aturan spam yang rumit, mengatur Tindakan yang diambil terhadapa email yang mencurigakan, dan membuat kebijakan khusus untuk penerimaan email.
- **Filtering yang Disesuaikan:** pengguna dapat menyesuaikan *filter* email yang memenuhi kebutuhan pengguna. Ini termasuk *filter* untuk *spam, antivirus,* dan *filter* konten yang dapat diatur untuk memenuhi standar keamanan yang diinginkan.

- ***Whitelisting* dan *Blacklisting*:** Pengguna dapat membuat daftar putih dan hitam untuk pengirim atau domain tertentu dengan PMG. Ini memungkinkan mereka untuk mengontrol secara langsung email yang diterima atau diblokir.

- **Integrasi dengan LDAP dan Active Directory:** PMG mendukung integrasi dengan layanan direktori seperti LDAP (*Lightweight Directory Access Protocol*) dan *Active Directory*, memungkinkan penyesuaian dengan infrastruktur IT yang ada.

- **Kustomisasi Notifikasi dan Tindakan:** Pengguna dapat mengatur pemberitahuan email dan tindakan yang diambil terhadapnya sesuai dengan kebutuhan yang di dapat, misalnya, mengarahkan email yang dianggap *spam* ke folder tertentu atau mengirimkan pemberitahuan kepada *administrator*.

- **Pengelolaan Perangkat Lunak dan Pembaruan:** PMG memungkinkan pengguna untuk mengelola perangkat lunak yang diinstal dan menyesuaikan jadwal pembaruan, memberikan kontrol penuh atas pembaruan perangkat lunaknya.

- **Skalabilitas dan Ketersediaan Tinggi:** PMG dirancang untuk skalabilitas dan ketersediaan tinggi, memungkinkan penyesuaian infrastruktur sesuai dengan kebutuhan pengguna, baik dalam hal peningkatan kapasitas maupun redundansi untuk mengatasi kegagalan perangkat keras.

Pengguna dapat menyesuaikan solusi keamanan email sesuai dengan kebutuhan bisnis dan keamanan dengan PMG, yang memungkinkan adaptasi yang kuat terhadap berbagai lingkungan IT dan memungkinkan pengguna untuk menyesuaikan kebijakan keamanan sesuai dengan berbagai situasi.

### *4.* Ketersediaan Fitur pada *proxmox mail gateway*

Untuk meningkatkan keamanan email dan manajemen pesan, *Proxmox Mail Gateway* (PMG) menawarkan banyak fitur, termasuk beberapa fitur penting berikut:

- ***Filtering Spam* dan *Antivirus*:** Dengan filter spam dan antivirus yang kuat, PMG melindungi sistem email dari ancaman yang berbahaya. Ini termasuk deteksi dan blok *spam, phishing, malware*, dan virus yang dapat merusak.
- **Penanganan Konten:** Dengan fitur ini, pengguna dapat mengatur dan mengelola konten email yang dianggap tidak diinginkan atau tidak layak. Fitur-fitur ini termasuk pengaturan kebijakan untuk konten tertentu, pembatasan lampiran, dan filter konten sensitif.
- **Proteksi Terhadap Anak Panah (*Spear Phishing*) dan *URL Filtering*:** Dengan mengidentifikasi dan memblokir email yang mencurigakan serta memfilter URL yang berpotensi berbahaya, PMG dapat melindungi pengguna dari serangan spear phishing.
- ***Encryption* dan Penandatanganan Email:** Pengguna dapat menandatangani dan mengenkripsi email dengan fitur ini untuk meningkatkan keamanan komunikasi.
- **Manajemen Kebijakan Email:** Pengguna dapat mengatur kebijakan pengiriman dan penerimaan email dengan PMG, yang mencakup pembatasan pengiriman email berdasarkan domain, pengguna, atau grup.
- **Pemantauan dan Laporan:** Dengan fitur ini, pengguna dapat melacak email yang masuk dan keluar, memantau kinerja sistem secara real-time, dan menghasilkan laporan keamanan yang rinci.
- **Integrasi dengan LDAP/*Active Directory*:** Untuk manajemen pengguna dan otentikasi yang terpusat, PMG mendukung integrasi dengan layanan direktori seperti LDAP dan *Active Directory*.
- ***Dashboard* dan Manajemen GUI:** Dengan antarmuka pengguna yang mudah digunakan, konfigurasi keamanan email dapat diatur dengan mudah.
- **Proteksi DDoS:** Dengan mengubah aturan pengaturan lalu lintas email, PMG dapat melindungi sistem email dari serangan DDoS (*Distributed Denial of Service*).

Fitur-fitur ini memiliki cakupan yang luas dan kuat untuk melindungi, mengelola, dan memantau sistem email. Kombinasi berbagai fitur ini dapat disesuaikan dengan kebutuhan khusus perusahaan untuk meningkatkan keamanan email secara keseluruhan.

### 5. Biaya pada *proxmox mail gateway*

Harga atau biaya untuk *Proxmox Mail Gateway* dapat bervariasi tergantung pada beberapa faktor, termasuk lisensi, dukungan, dan skala implementasi yang diinginkan. *Proxmox Mail Gateway* tersedia dalam dua versi:

- **Versi Berbayar (*Subscription-Based*):** *Proxmox Mail Gateway* menawarkan model langganan (*subscription*) yang mencakup berbagai fitur tambahan dan dukungan teknis. Biaya langganan umumnya bervariasi berdasarkan jumlah pengguna atau perangkat yang diinginkan, serta fitur tambahan yang dibutuhkan.
- **Versi Komunitas (*Community Edition*):** *Proxmox Mail Gateway* juga memiliki versi komunitas yang gratis untuk digunakan. Versi ini biasanya memiliki sebagian fitur inti, tetapi mungkin tidak termasuk fitur-fitur lanjutan atau dukungan teknis yang diberikan dalam versi berbayar.

Biaya langganan untuk *Proxmox Mail Gateway* dapat meliputi:

- **Lisensi Berlangganan:** Berlangganan untuk mendapatkan akses ke fitur-fitur tambahan dan pembaruan perangkat lunak.
- **Dukungan Teknis:** Layanan dukungan yang ditawarkan secara langsung oleh tim Proxmox untuk membantu dalam instalasi, konfigurasi, dan masalah teknis lainnya.
- **Pembaruan Perangkat Lunak:** Akses ke pembaruan rutin dan fitur-fitur baru yang diperbarui secara berkala.

Penting untuk menghubungi perusahaan Proxmox atau perwakilan resmi untuk mendapatkan informasi yang lebih akurat tentang harga dan opsi langganan yang sesuai dengan kebutuhan spesifik. Harga dapat berubah berdasarkan perubahan

pada fitur, dukungan, atau jumlah pengguna yang diinginkan, oleh karena itu, penting untuk mengetahui detail spesifik dari tim penjualan Proxmox.

### *6.* Kinerja dan Ketersediaan pada *proxmox mail gateway*

Kinerja dan ketersediaan *Proxmox Mail Gateway* (PMG) sangat penting untuk memastikan sistem email beroperasi dengan baik dan aman. Beberapa faktor yang mempengaruhi kinerja dan ketersediaan PMG meliputi:

- **Skalabilitas:** PMG didesain untuk skala yang dapat ditingkatkan, memungkinkan pengguna menyesuaikan kapasitas sistem untuk merespons penggunaan email yang lebih besar.
- **Ketersediaan Tinggi:** PMG dapat dikonfigurasi untuk ketersediaan tinggi, termasuk opsi untuk redundansi dan penanganan otomatis terhadap kegagalan perangkat keras.
- **Pembaruan dan Pemeliharaan:** Untuk mempertahankan kinerja dan keamanan sistem, Proxmox selalu memberikan pembaruan perangkat lunak secara berkala.
- **Monitoring dan Manajemen Kinerja:** PMG menyediakan alat pemantauan yang memungkinkan pengguna untuk memantau kinerja sistem secara real-time dan menanggapi perubahan yang diperlukan.
- **Optimisasi Konfigurasi:** Konfigurasi PMG yang tepat, yang mencakup manajemen pengguna, kebijakan keamanan, dan pengaturan filter, dapat berdampak pada kinerja dan keandalan sistem.
- **Proteksi Terhadap Serangan:** Kemampuan PMG untuk melindungi sistem dari serangan DDoS, serangan phishing, dan ancaman keamanan email lainnya adalah faktor lain yang memengaruhi kinerjanya.

Untuk memahami berbagai faktor, seperti konfigurasi, lingkungan jaringan, volume email, dan pengaturan kebijakan keamanan, dapat memengaruhi kinerja dan ketersediaan PMG. Memahami teknik terbaik untuk penggunaan PMG dan melakukan pemeliharaan rutin akan membantu memastikan kinerja yang optimal.

Dalam hal ketersediaan PMG, menerapkan ketersediaan tinggi atau redundansi dalam konfigurasi infrastruktur PMG dapat membantu menjaga ketersediaan layanan, meminimalkan waktu tidak tersedia, dan meningkatkan keandalan sistem secara keseluruhan.