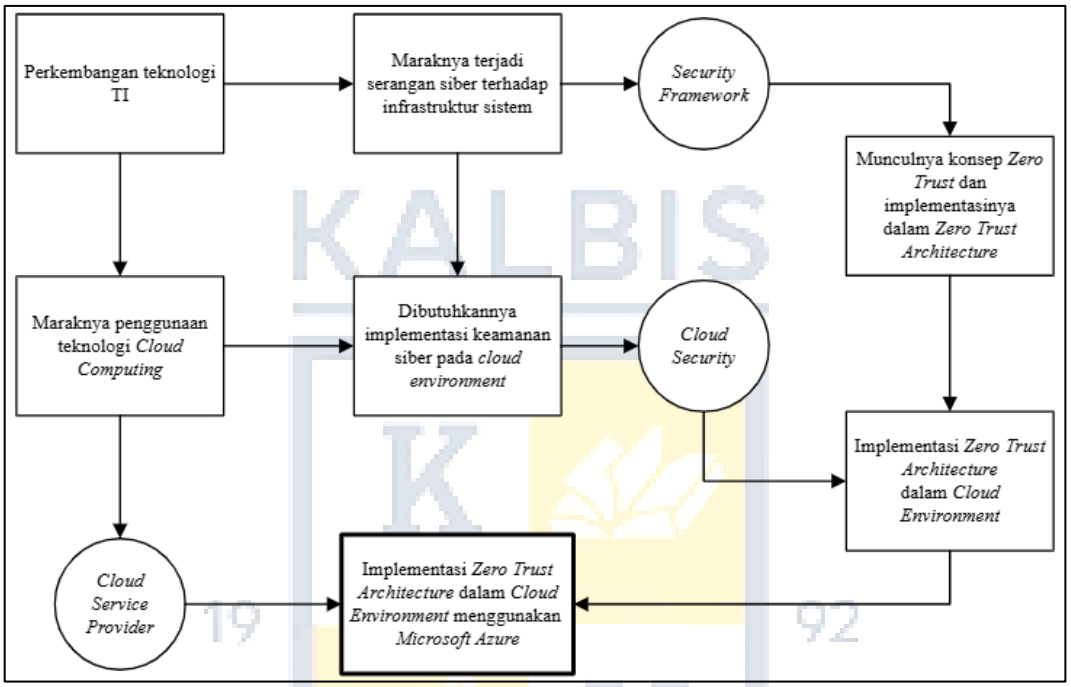
# BAB 3

# METODOLOGI PENELITIAN

## 3.1 Kerangka Pemikiran




**Gambar 3.1: Diagram Kerangka Pemikiran**

Kerangka pemikiran yang digunakan oleh penulis dalam melakukan penelitian ini didasari oleh perkembangan teknologi informasi yang sudah menjadi standar industri di masa sekarang. Teknologi *cloud computing* adalah perkembangan yang menjadi fokus dalam penelitian ini. Seiring berkembangnya teknologi yang ada, serangan siber terhadap infrastruktur sistem juga semakin marak terjadi. Hal ini memicu bertumbuhnya permintaan atas implementasi keamanan siber dalam *cloud environment* yang merupakan dasar munculya sektor *cloud security*.Atas permintaan tersebut, terciptalah sektor *Cloud Security*. Maraknya serangan siber juga memicu dibuatnya standarisasi kerangka keamanan yang digunakan (*Security Framework*), salah satunya adalah penggunaan konsep *Zero Trust Architecture*. Implementasi *Zero Trust Architecture* ini akan di

implementasikan kedalam *cloud environment* dengan menggunakan *Microsoft Azure*, yang merupakan salah satu *Cloud Service Provider* yang marak digunakan. Penelitian ini ditujukan untuk memperjelas dan menyediakan kerangka implementasi *Zero Trust Architecture* menggunakan *Microsoft Azure* sebagai *Cloud Service Provider*.

## 3.2 Metode Penelitian

Dalam melakukan implementasi *Zero Trust Architecture* (ZTA) pada *cloud environment* dengan menggunakan *Microsoft Azure*, akan dibuat dua infrastruktur *cloud* yang berbeda. Hal ini dilakukan guna memberikan perspektif perbandingan pada implementasi yang dilakukan. Salah satu infrastruktur ini merupakan infrastruktur biasa tanpa implemetasi ZTA (*Project-Default*), sedangkan yang lainnya merupakan infrastruktur yang telah diimplementasi konsep ZTA (*Project-ZTA*).

Setelah kedua infrastruktur tersebut dibuat, maka akan dilakukan *testing* pada komponen yang ada guna mencerminkan funginya dalam memenuhi 7 prinsip *Zero Trust* yang telah di jelaskan pada bagian sebelumnya. Akan dilakukan juga perbandingan antara implementasi *Zero Trust Architecture* yang dibuat oleh *Microsoft* sendiri, dengan implementasi yang dilakukan pada penelitian ini. Perbandingan akan dilakukan melalui dua hal, yaitu komponen yang digunakan dan total harga dari masing- masing implementasi. Menurut panduan yang dipublikasi oleh *Microsoft* sendiri berikut merupakan komponen yang diperlukan dalam implementasi *Zero Trust Architecture* pada *Azure*[13]:

1. **Azure *Key Vault***

   Layanan untuk menyimpan dan mengelola *secrets*, *keys*, dan *certificates* secara aman. Membantu melindungi informasi sensitif seperti kredensial dan token dari akses yang tidak sah.

2. **Azure Bastion**

Layanan untuk mengakses mesin virtual (VM) secara aman melalui *browser* menggunakan RDP atau SSH tanpa perlu membuka IP publik. Ini mengurangi risiko serangan langsung ke VM dari internet.

3. ***Just-in-time Access***

   Fitur yang memberikan akses sementara dan terbatas waktu ke *resource* tertentu, seperti VM. Mengurangi permukaan serangan dengan hanya membuka akses saat dibutuhkan.

4. **Azure *Firewall***

   Layanan firewall jaringan berbasis cloud yang menyediakan kontrol lalu lintas masuk dan keluar berdasarkan aturan keamanan. Mendukung fitur seperti *filtering layer* 3–7 dan *logging* aktivitas jaringan.

5. **Azure *DdoS Protection***

   Layanan untuk melindungi aplikasi dan layanan dari serangan *Distributed Denial* of *Service* (DDoS). Mendeteksi dan merespons serangan secara otomatis untuk menjaga ketersediaan sistem.

6. **Azure AD**

   Layanan identitas berbasis cloud untuk manajemen autentikasi dan otorisasi pengguna. Mendukung fitur seperti *Single Sign-On* (SSO) dan *Multi-Factor Authentication* (MFA).

7. **Azure *Purview***

   Layanan tata kelola data (*data governance*) yang memungkinkan pemetaan, pelacakan, dan pengelolaan aset data di

seluruh lingkungan Azure dan non-Azure. Membantu organisasi memahami dan mengamankan data sensitif.

8. ***Application Gateway***

   *Load balancer* layer 7 yang mengelola lalu lintas HTTP/HTTPS dengan fitur seperti URL-based routing dan *Web Application Firewall* (WAF). Melindungi aplikasi *web* dari serangan umum seperti SQL *injection* dan XSS.

9. ***Virtual Network Gateway***

   Layanan yang digunakan untuk membangun koneksi VPN antara Azure dan lingkungan *on-premises*. Mendukung koneksi *site-to-site*, *point-to-site*, dan ExpressRoute.

10. **Azure *Monitor***

    Platform untuk mengumpulkan, menganalisis, dan merespons data telemetri dari aplikasi dan *resource* Azure. Membantu mengidentifikasi masalah performa dan memantau status sistem secara *real-time*.

11. **Azure *Advisor***

    Layanan rekomendasi berbasis AI yang memberikan saran untuk meningkatkan kinerja, keamanan, dan efisiensi biaya dari *resource* Azure. Menyediakan panduan berbasis praktik terbaik Microsoft.

Pengujian dilakukan pada masing-masing infrastruktur untuk mencerminkan sejauh mana penerapan prinsip *Zero Trust Architecture* dapat diterapkan dan memberikan dampak terhadap aspek keamanan. Setiap pengujian disesuaikan dengan tujuh prinsip dasar *Zero Trust Architecture* dari NIST yang telah dijelaskan sebelumnya, dengan skenario sebagai berikut:

1. ***Resources Includes All Data and Services***

   Pada prinsip ini, pengujian difokuskan pada penerapan *granular access control* terhadap seluruh sumber daya (*resources*) yang berada dalam satu *subscription*. Tidak ada akses yang diturunkan secara otomatis antar *resource* yang berbeda, sehingga setiap *resource* dilindungi secara individual dan hanya dapat diakses oleh entitas yang memiliki izin eksplisit.

2. ***Secure-line Communication***

   Seluruh komunikasi *inbound* maupun *outbound* dilakukan melalui *gateway* terproteksi seperti *Application Gateway* dan *VPN Gateway*. Tidak ada resource yang memiliki IP publik langsung, sehingga jalur komunikasi terenkripsi dan melewati lapisan validasi, guna mencegah akses langsung dari internet terbuka.

3. ***Time-limited Access***

   Akses ke salah satu resource diberikan kepada pengguna dengan batasan waktu tertentu melalui *time-based access policy*. Pengaturan ini memastikan bahwa akses yang diberikan bersifat sementara dan akan dicabut secara otomatis setelah melewati jangka waktu yang ditentukan.

4. ***Dynamic Access Policy***

   Untuk mencerminkan kebijakan akses yang dinamis, setiap pengguna diwajibkan untuk melakukan autentikasi dua faktor (*multi-factor authentication*/MFA) sebelum memperoleh akses ke *resource*. Hal ini memberikan lapisan keamanan tambahan dan meminimalkan risiko dari kredensial yang disalahgunakan.

5. ***Continuous System Monitoring***

Pengujian dilakukan dengan mengaktifkan fitur *resource health monitoring* pada setiap komponen infrastruktur. Dengan ini, status kesehatan sistem dapat dipantau secara berkala, memungkinkan deteksi dini terhadap potensi gangguan atau penyimpangan yang terjadi pada *resource*.

6. ***Evaluated Access***

   Evaluasi akses dilakukan sebelum pemberian hak akses baru. Setiap permintaan akses dievaluasi berdasarkan prinsip *least privilege*, sehingga hanya akses yang benar-benar dibutuhkan dan sesuai dengan tugas pengguna yang diberikan izin.

7. ***System Log Analysis***

   Aktivitas sistem dicatat secara menyeluruh melalui *activity logs* dan *diagnostic logs*. Selain itu, aturan peringatan (*alert rules*) diaktifkan untuk memberikan notifikasi otomatis kepada administrator saat terjadi aktivitas abnormal atau percobaan akses yang mencurigakan.

Sebelum melakukan implementasi ZTA, perlu dilakukan perancangan arsitektur sistem yang akan dibuat. Hal ini merupakan tahap yang penting karena dalam tahap perancangan arsitektur ini, harus juga dilakukan perhitungan *class inter-domain routing* (CIDR) terhadap *virtual network* yang akan dibuat. Perhitungan CIDR *range* ini mencangkup seluruh komponen dalam sistem yang memerlukan *range* IP-nya masing- masing. Komponen komponen yang berjalan dalam suatu *cloud environment* memerlukan bagian *range* dalam pembuatan dan penggunaannya, dengan masing- masing komponen membutuhkan *minimum range* yang bervariasi.

### 3.2.1 Perancangan Arsitektur *Cloud*

Dalam melakukan perancangan arsitektur *cloud* yang ada, kita perlu mengetahui komponen apa saja yang akan digunakan dalam infrastruktur ini. Dalam penelitian ini, penulis akan membuat infrastruktur sederhana yang dapat digunakan untuk melakukan *web hosting*. Setelah mengetahui tujuan penggunaan suatu infrastruktur, kita dapat mengetahui komponen yang perlu dikonfigurasi. Komponen- komponen utama yang akan digunakan adalah sebagai berikut:

1. ***Resource Groups***

   *Resource Group* merupakan kumpulan *service* dan *resource* yang digunakan dalam suatu infrastruktur *cloud* pada *Microsoft Azure*. Komponen ini merupakan komponen yang wajib dimiliki setiap infrastruktur yang ada karena akan menjadi basis pengelompokan komponen yang ada.

2. ***Azure Virtual Network***

   *Azure Virtual Network* merupakan komponen *private virtual network* yang memungkinkan komunikasi aman antar komponen yang ada didalamnya. Penggunaan komponen ini memastikan pemenuhan salah satu syarat dalam ZTA yang memerlukan *secure communication* dalam suatu infrastruktur.

3. ***Azure Virtual Machines***

   *Azure Virtual Machine* (VM) merupakan layanan *virtualization* yang dimiliki *Azure* dengan menempatkan *virtual machine* yang dibuat pada *cloud*. Penggunaan komponen VM ini akan menjadi tempat di *hosting*-nya *web page* dalam infrastruktur ini. Komponen ini juga memiliki IP *public* yang dapat digunakan untuk akses *via* internet.

4. ***Azure Disks***

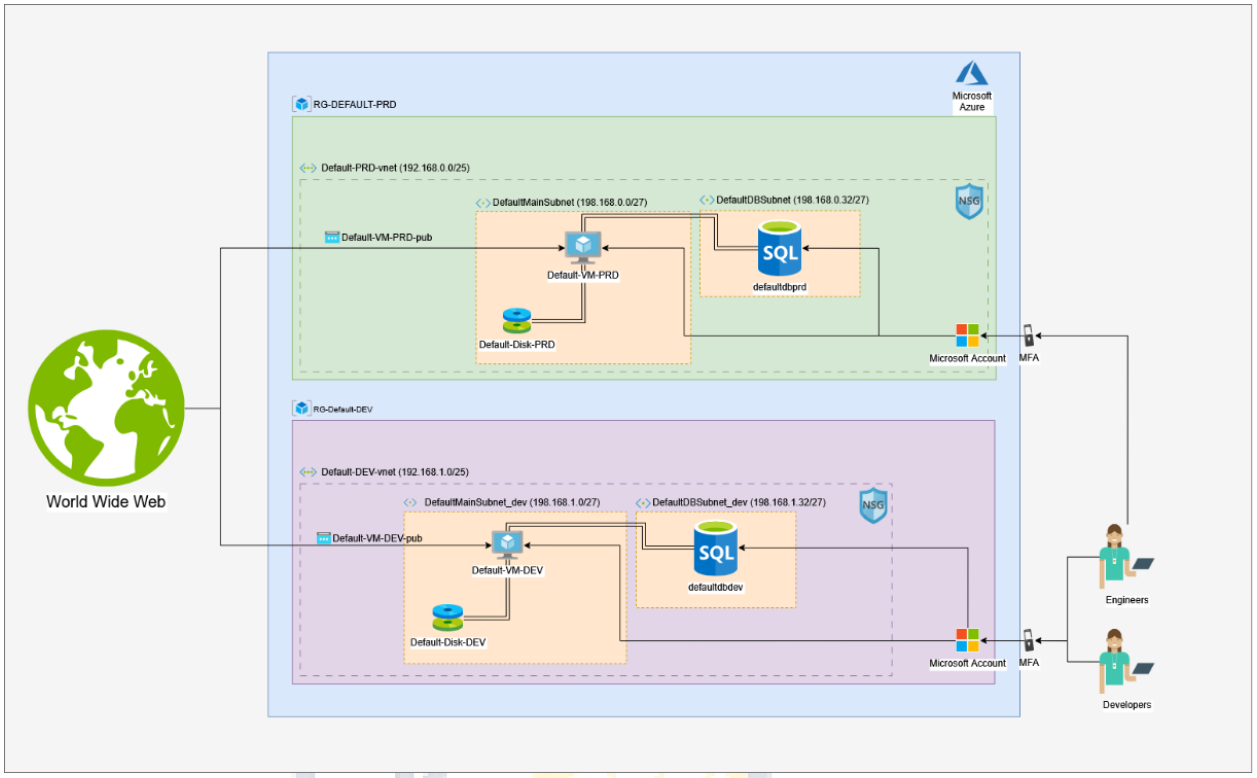
*Azure Disks* merupakan layanan manajemen penyimpanan berbetuk *disk* yang akan terhubung dengan VM yang telah dibuat. Komponen ini sendiri akan menyimpan seluruh data yang ada di dalam VM yang telah dibuat, hal ini termasuk OS hingga data- data individual yang ada di dalam VM tersebut.

5. ***Azure Databases***

   *Azure Databases* merupakan layanan basis data yang ditawarkan oleh *Azure*. Komponen ini akan digunakan sebagai *server* penyimpanan bagi *web page* yang di-*deploy* dalam *virtual machine* yang ada.

6. ***Microsoft Account***

   *Microsoft Account* merupakan salah satu komponen yang digunakan dalam infrastruktur ini sebagai gerbang akses standar yang digunakan dalam mengakses *Microsoft Azure*. Komponen ini dilengkapi juga dengan fitur *multi-factor authentication* (MFA) sebagai standar keamanan dalam akun *Microsoft* yang ada.




**Gambar 3.2: *Project-Default* (Tanpa Implementasi ZTA)**

Komponen- komponen yang ada diatas merupakan komponen utama, yang dimana akan digunakan di kedua infrastruktur yang ada. Dalam melakukan implementasi ZTA pada infrastruktur tersebut, kita perlu melakukan konfigurasi dan penambahan beberapa komponen lainnya. Komponen ini ditambahkan guna memenuhi prinsip yang ada dalam konsep *Zero Trust Architecture*, yaitu:

1. Semua komponen dalam sistem harus terlindungi (*secure component*)
2. Komunikasi antar komponen harus terjadi secara aman (*secure line communication*)
3. Akses yang diberikan harus disertakan dengan batasan waktu (*time limited access*)
4. Kebijakan sistem yang dinamis (*dynamic policy*)
5. Melakukan evaluasi terhadap akses dan kebijakan yang ada (*access and policy evaluation*)

6. Menggunakan informasi sistem yang ada guna meningkatkan postur keamanan (*system log analysis for security posture*)

Dengan adanya prinsip- prinsip tersebut, maka diperlukan komponen dan konfigurasi tambahan yang akan digunakan dalam infrastruktur implementasi ZTA, yang mencakup:

**1. *Resource Health Alerts* pada *Azure Vrtual Machines***

*Virtual Machine* dapat dilengkapi dengan fitur *resource health* yang dapat memberikan informasi terkait kondisi sistem yang ada selama VM tersebut berjalan. Fitur ini juga dapat menjadi garda depan apabila terjadi ketidaksesuaian dengan status penggunaan sistem yang ada, dan dapat memberikan peringatan kepada *engineer* sebelum terjadi isu yang lebih besar. Status yang dapat di-*monitor* oleh fitur ini mencakup penggunaan CPU, RAM, dan *Storage* pada VM; Juga tingkat *latency* yang ada antara VM dan komponen- komponen yang terkoneksi.

**2. *Azure Monitoring***

*Azure Monitor* merupakan komponen monitoring yang dimiliki oleh *Azure*. Komponen ini akan memenuhi persyaratan *monitoring* dan juga *system logging* guna meningkatkan postur keamanan dan investigasi *post-incident*.

**3. *Azure Application Gateway***

*Azure Application Gateway* merupakan komponen *load balancer* pada *application layer* (Layer 7) yang berfungsi untuk mengatur *ingress* dan *engress* kedalam suatu aplikasi web, yang dimana dalam infrastruktur ini merupakan *web page* yang di *host* di VM. Komponen ini juga memiliki fitur keamanan tambahan untuk memenuhi prinsip ZTA seperti, *web application firewall* (WAF), *url-based routing*, dan *SSL Termination*. Fitur keamanan tersebut akan membantu dalam mengamankan layanan *web* yang terkespos ke *public* (*public facing*).

4. ***Azure Web Application Firewall***

   *Azure Web Application Firewall* merupakan fitur keamanan dari *Azure Application Gateway* yang melindungi aplikasi web dari serangan umum seperti SQL injection, cross-site scripting, dan OWASP *Top* 10 *vulnerabilities*.

5. ***Azure Network Watchers***

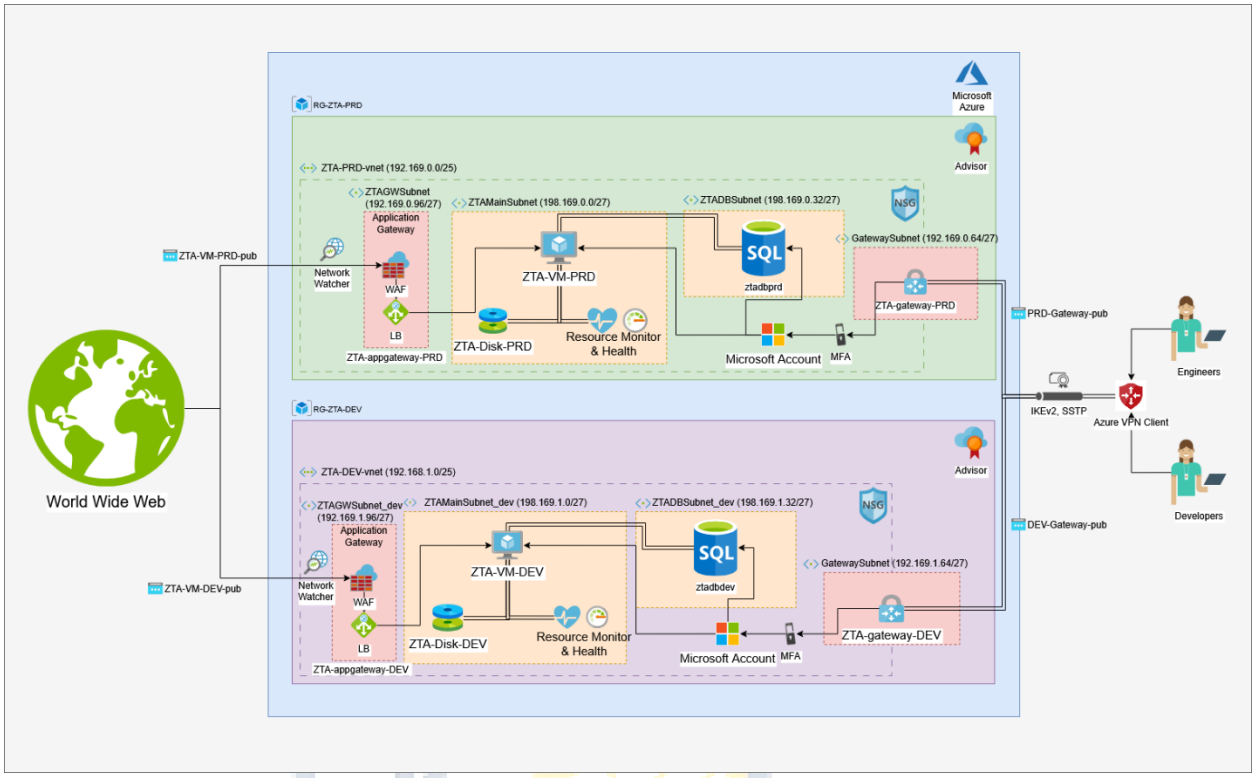
   *Azure NetWatch* merupakan komponen yang berfungsi sebagai alat pemantauan dan diagnostik jaringan yang dapat membantu dalam analisa dan visualisasi konektivitas pada suatu innfrastruktur. Komponen ini dapat memenuhi prinsip *secure line communication* dan *system log monitoring*.

6. ***Azure Advisor* pada *Microsoft Defender for Cloud***

   *Azure Advisor* merupakan komponen yang dapat menganalisa postur keamanan suatu infrastruktur *Azure* dengan berpondasikan 5 pillar, yaitu: *Cost, Reliability, Security, Performance,* dan *Operational Excellence*.

7. ***Azure Virtual Network Gateway***

   *Azure Virtual Network Gateway* merupakan komponen yang berfungsi untuk membuat koneksi VPN. Jenis koneksi VPN yang akan digunakan pada infrastruktur ini adalah koneksin VPN *point to site* yang menghubungkan antara perangkat personal dengan jaringan *Azure virtual network*.

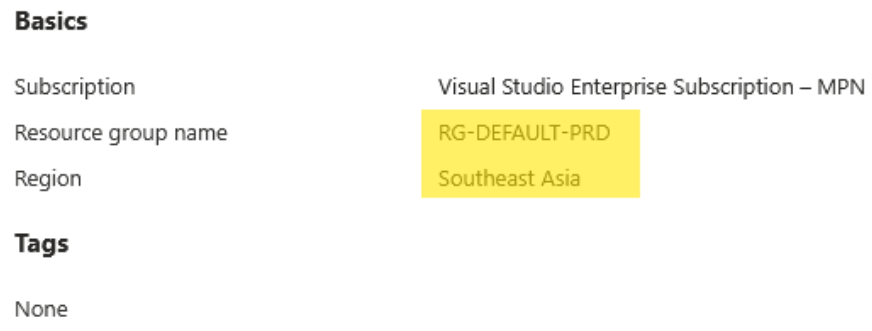



**Gambar 3.3: *Project-ZTA* (Setelah Implementasi ZTA)**

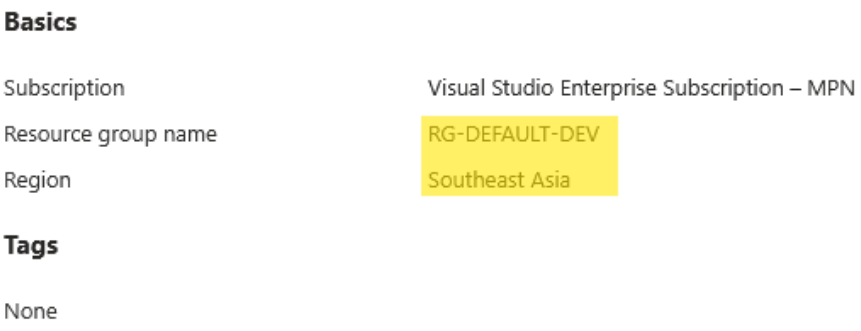
### 3.2.2 Pembuatan Infrastruktur *Project-Default*

Pada bagian ini, akan dijelaskan proses pembuatan infrastruktur *cloud* menggunakan *Microsoft Azure*. Bagian ini akan menjelaskan infrastruktur pertama, yaitu "Infrastruktur *Project-Default*" yang akan menjelaskan prosedur pembuatan infrastruktur *Project-Default* tanpa implementasi konsep ZTA. Seluruh prosedur akan dilakukan melalui *Azure Portal* yang diakses di *web browser*. Diagram arsitektur yang akan digunakan adalah diagram *Project-Default* pada Gambar 3.2.

Komponen pertama yang harus dibuat adalah 2 buah *resource group*, konfigurasi yang akan dilakukan hanya terdapat pada nama *resource group* (RG-DEFAULT-PRD & RG-DEFAULT-DEV) dan *region* dibuatnya komponen. Untuk seluruh komponen pada penelitian ini akan menggunakan Asia Tenggara (*Southeast Asia*) sebagai *region* yang dipilih.




**Gambar 3.4 Konfigurasi RG-DEFAULT-PRD**




**Gambar 3.5 Konfigurasi RG-DEFAULT-DEV**

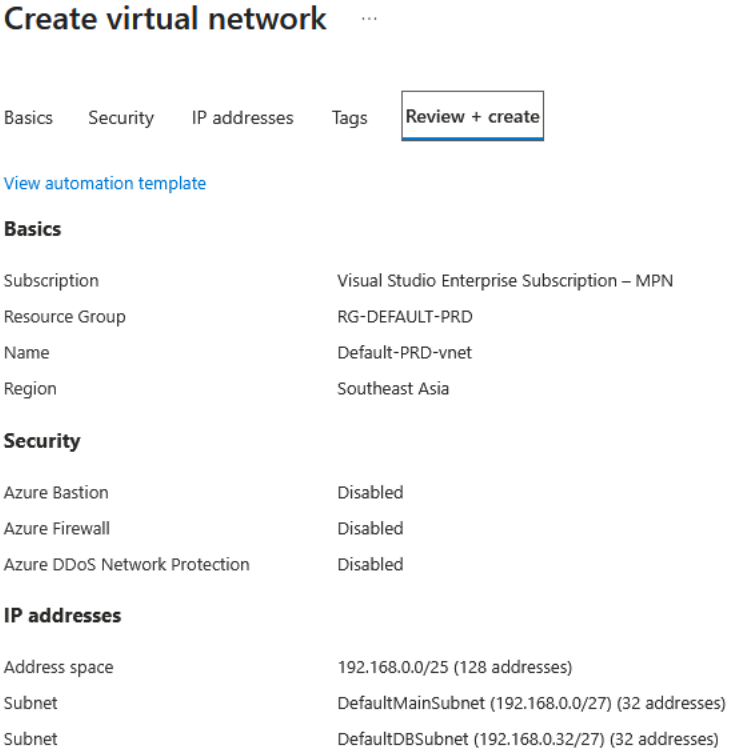
Setelah *resource group* yang diperlukan selesai dibuat, kita bisa melakukan pembuatan komponen- komponen lain dalam lingkup masing masing dari kedua *resource group* tersebut. Langkah selanjutnya adalah mengkonfigurasi *virtual network* berserta dengan *subnet* yang ada di dalamnya.

Infrastruktur ini memiliki 2 *virtual network* (Default-PRD-vnet & Default-DEV-vnet) dengan 2 *subnet* di masing- masing *virtual network* (*Main subnet* & *DB subnet*). Konfigurasi yang akan digunakan dalam membuat *virtual network* adalah sebagai berikut:

**RG-DEFAULT-PRD**

- Default-PRD-vnet:
  - *Resource Group*: RG-DEFAULT-PRD
  - *Name*: Default-PRD-vnet

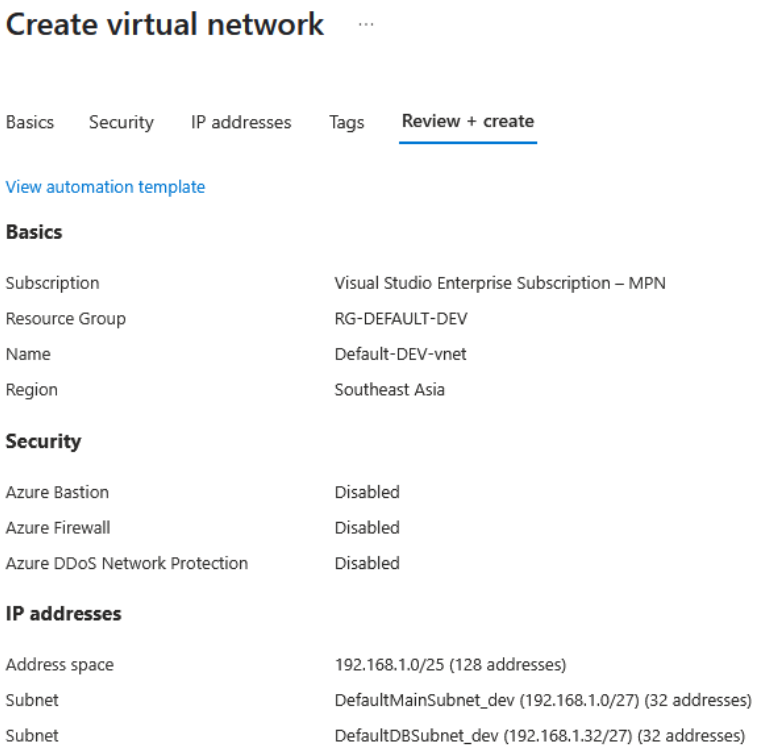
- *IP addresses*: 192.168.0.0/25
- *Subnet*:
  - DefaultMainSubnet (192.168.0.0/27)
  - DefaultDBSubnet (192.168.0.32/27)




**Gambar 3.6 Konfigurasi Default-PRD-vnet**

**RG-DEFAULT-DEV**

- Default-DEV-net:
  - *Resource Group*: RG-DEFAULT-DEV
  - *Name*: Default-DEV-vnet
  - *IP addresses*: 192.168.1.0/25
  - *Subnet*:
    - DefaultMainSubnet (192.168.1.0/27)
    - DefaultDBSubnet (192.168.1.32/27)




**Gambar 3.7 Konfigurasi Default-DEV-vnet**

Setelah membuat *virtual network,* akan dibuat *virtual machine* menggunakan vnet yang ada. Infrastruktur ini memiliki 2 buah VM (Default-VM-PRD & Default-VM-DEV) dan masing- masing 1 *disk* yang ada didalamnya (Default-Disk-PRD & Default-Disk-DEV). Dalam penelitian ini kita akan menggunakan konfigurasi sebagai berikut:

- ***DEFAULT-VM-PRD***
  - **Basic**
    - *Resource group*: RG-DEFAULT-PRD
    - *Name*: Default-VM-PRD
    - *Availability options*: *No infrastructure redundancy required*
    - *Security type*: *Standard*
    - *Machine Type*: *Standard*_B1 ls (1 vCPU, 0.5 GiB *memory*)
    - *Image*: *Ubuntu Server* 24.04 LTS- x64 *Gen*2

- *Authenticaiton Type*: SSH *public key*
- *Username*: *Default-admin*
- *Key pair name*: *Default-key*
- *Inbound ports*: SSH (22)

- **Disk**
  - OS *Disk size*: *Image default* (30 GiB)
  - *OS Disk type*: *Standard* HDD (*locally-redundant storage*)
- **Networking**
  - *Virtual Network*: Default-PRD-vnet
  - *Subnet*: DefaultMainSubnet (192.168.0.0/27)
  - *Public IP*: Default-VM-PRD-pub
- **Management**
  - *Auto-shutdown*: Disabled
- **Monitoring**
  - *Boot Diagnostics*: Disabled

**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-DEFAULT-PRD |
| Virtual machine name | Default-VM-PRD |
| Region | Southeast Asia |
| Availability options | No infrastructure redundancy required |
| Zone options | Self-selected zone |
| Security type | Standard |
| Image | Ubuntu Server 24.04 LTS - Gen2 |
| VM architecture | x64 |
| Size | Standard B1ls (1 vcpu, 0.5 GiB memory) |
| Enable Hibernation | No |
| Authentication type | SSH public key |
| Username | Default-admin |
| SSH Key format | RSA |
| Key pair name | Default-key |
| Public inbound ports | SSH |
| Azure Spot | No |

**Disks**

| | |
|---|---|
| OS disk size | Image default |
| OS disk type | Standard HDD LRS |
| Use managed disks | Yes |
| Delete OS disk with VM | Enabled |
| Ephemeral OS disk | No |

**Networking**

| | |
|---|---|
| Virtual network | Default-PRD-vnet |
| Subnet | DefaultMainSubnet (192.168.0.0/27) |
| Public IP | (new) Default-VM-PRD-pub |
| Accelerated networking | Off |
| Place this virtual machine behind an existing load balancing solution? | No |
| Delete public IP and NIC when VM is deleted | Disabled |

**Management**

| | |
|---|---|
| Microsoft Defender for Cloud | Standard |
| System assigned managed identity | Off |
| Login with Microsoft Entra ID | Off |
| Auto-shutdown | Off |
| Backup | Disabled |
| Enable periodic assessment | Off |
| Enable hotpatch | Off |
| Patch orchestration options | Image Default |

**Monitoring**

| | |
|---|---|
| Alerts | Off |
| Boot diagnostics | Off |
| Enable OS guest diagnostics | Off |
| Enable application health monitoring | Off |

**Advanced**

| | |
|---|---|
| Extensions | None |
| VM applications | None |
| Cloud init | No |
| User data | No |
| Disk controller type | SCSI |
| Proximity placement group | None |
| Capacity reservation group | None |

**Gambar 3.8 Konfigurasi Default-VM-PRD**

- ***DEFAULT-VM-DEV***
  - **Basic**
    - *Resource group*: RG-DEFAULT-DEV
    - *Name*: Default-VM-DEV
    - *Availability options*: *No infrastructure redundancy required*
    - *Security type*: *Standard*
    - *Machine Type*: *Standard*_B1 ls (1 vCPU, 0.5 GiB *memory*)
    - *Image*: *Ubuntu Server* 24.04 LTS- x64 *Gen*2
    - *Authenticaiton Type*: SSH *public key*
    - *Username*: *Default-admin-dev*
    - *Key pair name*: *Default-key-dev*
    - *Inbound ports*: SSH (22)
  - **Disk**
    - OS *Disk size*: *Image default* (30 GiB)
    - *OS Disk type*: *Standard* HDD (*locally-redundant storage*)
  - **Networking**
    - *Virtual Network*: Default-DEV-vnet
    - *Subnet*: DefaultMainSubnet_dev (192.168.0.0/27)
    - *Public IP*: Default-VM-DEV-pub
  - **Management**
    - *Auto-shutdown*: Disabled
  - **Monitoring**
    - *Boot Diagnostics*: Disabled

**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-DEFAULT-DEV |
| Virtual machine name | Default-VM-DEV |
| Region | Southeast Asia |
| Availability options | No infrastructure redundancy required |
| Zone options | Self-selected zone |
| Security type | Standard |
| Image | Ubuntu Server 24.04 LTS - Gen2 |
| VM architecture | x64 |
| Size | Standard B1ls (1 vcpu, 0.5 GiB memory) |
| Enable Hibernation | No |
| Authentication type | SSH public key |
| Username | Default-admin-dev |
| SSH Key format | RSA |
| Key pair name | Default-key-dev |
| Public inbound ports | SSH |
| Azure Spot | No |

**Disks**

| | |
|---|---|
| OS disk size | Image default |
| OS disk type | Standard HDD LRS |
| Use managed disks | Yes |
| Delete OS disk with VM | Enabled |
| Ephemeral OS disk | No |

**Networking**

| | |
|---|---|
| Virtual network | Default-DEV-vnet |
| Subnet | DefaultMainSubnet_dev (192.168.1.0/27) |
| Public IP | (new) Default-VM-DEV-pub |
| Accelerated networking | Off |
| Place this virtual machine behind an existing load balancing solution? | No |
| Delete public IP and NIC when VM is deleted | Disabled |

**Management**

| | |
|---|---|
| Microsoft Defender for Cloud | Standard |
| System assigned managed identity | Off |
| Login with Microsoft Entra ID | Off |
| Auto-shutdown | Off |
| Backup | Disabled |
| Enable periodic assessment | Off |
| Enable hotpatch | Off |
| Patch orchestration options | Image Default |

**Monitoring**

| | |
|---|---|
| Alerts | Off |
| Boot diagnostics | Off |
| Enable OS guest diagnostics | Off |
| Enable application health monitoring | Off |

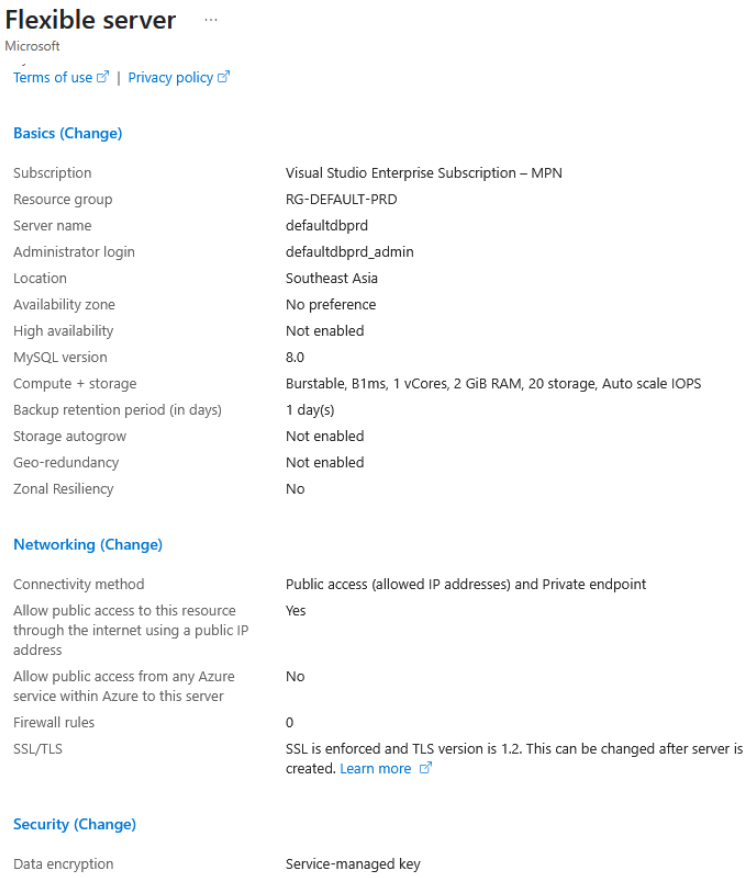
**Advanced**

| | |
|---|---|
| Extensions | None |
| VM applications | None |
| Cloud init | No |
| User data | No |
| Disk controller type | SCSI |
| Proximity placement group | None |
| Capacity reservation group | None |

**Gambar 3.9 Konfigurasi Default-VM-DEV**

Setelah membuat *virtual machine,* akan dibuat *Azure database* pada vnet yang ada. Infrastruktur ini memiliki 2 buah DB (defaultdbprd & defaultdbdev). Dalam penelitian ini kita akan menggunakan konfigurasi sebagai berikut:

- ***defaultdbprd***
  - **Basics**
    - *Resource Group*: RG-DEFAULT-PRD
    - *Server name*: defaultdbprd
    - *Workload type*: *For development and hobby projects*
    - *Store autogrow*: *Disabled*
    - *Backup retention:* 1 *day*
    - *Authentication method*: MySQL *authentication only*
    - *Administrator login*: defaultdbprd_admin
    - *Administrator password*: root123!



**Flexible server** ...

Microsoft

Terms of use | Privacy policy

**Basics (Change)**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-DEFAULT-PRD |
| Server name | defaultdbprd |
| Administrator login | defaultdbprd_admin |
| Location | Southeast Asia |
| Availability zone | No preference |
| High availability | Not enabled |
| MySQL version | 8.0 |
| Compute + storage | Burstable, B1ms, 1 vCores, 2 GiB RAM, 20 storage, Auto scale IOPS |
| Backup retention period (in days) | 1 day(s) |
| Storage autogrow | Not enabled |
| Geo-redundancy | Not enabled |
| Zonal Resiliency | No |

**Networking (Change)**

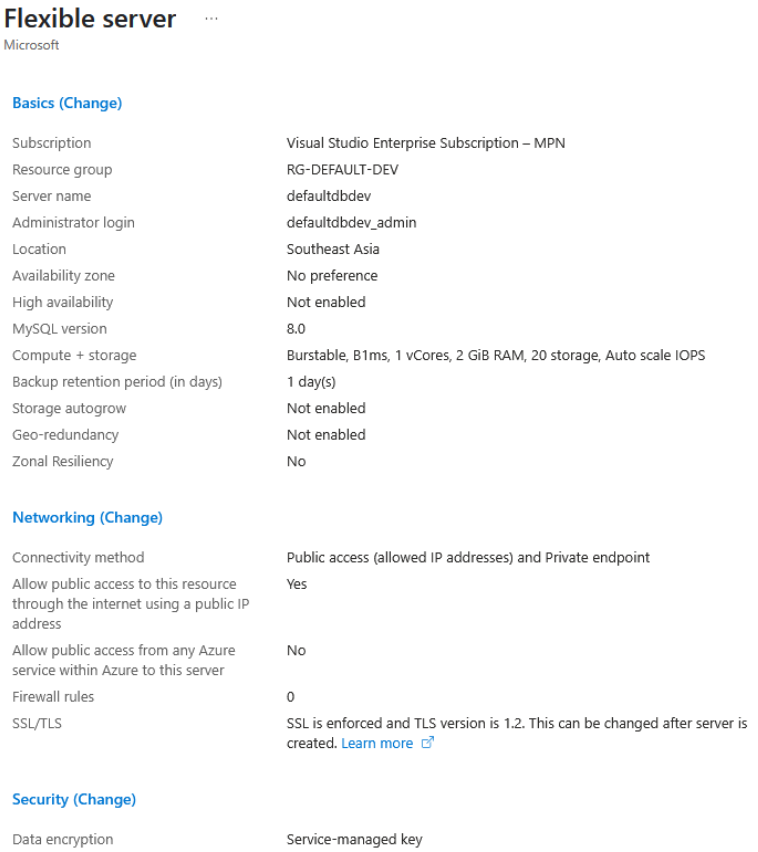
| | |
|---|---|
| Connectivity method | Public access (allowed IP addresses) and Private endpoint |
| Allow public access to this resource through the internet using a public IP address | Yes |
| Allow public access from any Azure service within Azure to this server | No |
| Firewall rules | 0 |
| SSL/TLS | SSL is enforced and TLS version is 1.2. This can be changed after server is created. Learn more |

**Security (Change)**

| | |
|---|---|
| Data encryption | Service-managed key |

**Gambar 3.10 Konfigurasi DB defaultdbprd**

- ***defaultdbdev***
  - **Basic**
    - *Resource Group*: RG-DEFAULT-DEV
    - *Server name*: defaultdbdev
    - *Workload type*: *For development and hobby projects*
    - *Store autogrow*: *Disabled*
    - *Backup retention:* 1 *day*
    - *Authentication method*: MySQL *authentication only*
    - *Administrator login*: defaultdbdev_admin
    - *Administrator password*: root123!



**Flexible server** ···
Microsoft

**Basics (Change)**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-DEFAULT-DEV |
| Server name | defaultdbdev |
| Administrator login | defaultdbdev_admin |
| Location | Southeast Asia |
| Availability zone | No preference |
| High availability | Not enabled |
| MySQL version | 8.0 |
| Compute + storage | Burstable, B1ms, 1 vCores, 2 GiB RAM, 20 storage, Auto scale IOPS |
| Backup retention period (in days) | 1 day(s) |
| Storage autogrow | Not enabled |
| Geo-redundancy | Not enabled |
| Zonal Resiliency | No |

**Networking (Change)**

| | |
|---|---|
| Connectivity method | Public access (allowed IP addresses) and Private endpoint |
| Allow public access to this resource through the internet using a public IP address | Yes |
| Allow public access from any Azure service within Azure to this server | No |
| Firewall rules | 0 |
| SSL/TLS | SSL is enforced and TLS version is 1.2. This can be changed after server is created. Learn more |

**Security (Change)**

| | |
|---|---|
| Data encryption | Service-managed key |

**Gambar 3.11 Konfigurasi DB defaultdbdev**

Pada tahap ini, seluruh komponen/ *resource* yang sudah didesain pada diagram rancangan arsitektur *project-default* sudah dibuat dan siap digunakan. Dalam infrastruktur ini, *developer* dapat melakukan upload *source code* pada VM yang tersedia dan melakukan *hosting* dengan menggunakan *runtime* yang diinginkan. *Database engineer* dapat mengkonfigurasi lebih lanjut pada laman basis data di *Azure portal*, sedangkan *Cloud engineer* dapat mengakses *resource* yang dibuat melalui *Azure portal* dengan menggunakan akun *Microsoft* yang sudah terdaftar dalam *subscription* ini.

### 3.2.3 Pembuatan Infrastruktur *Project-ZTA*

Pada bagian ini, akan dijelaskan proses pembuatan infrastruktur *cloud* menggunakan *Microsoft Azure*. Bagian ini akan menjelaskan infrastruktur pertama, yaitu "Infrastruktur *Project-ZTA*" yang akan menjelaskan prosedur pembuatan infrastruktur *Project-ZTA* dan implementasi konsep ZTA pada arsitektur *cloud*. Seluruh prosedur akan dilakukan melalui *Azure Portal* yang diakses di *web browser*. Diagram arsitektur yang akan digunakan adalah diagram *Project-ZTA* pada Gambar 3.3.

Sama dengan prosedur yang dilakukan sebelumnya, hal pertama yang perlu dibuat adalah 2 buah *resource group* yang ada pada arsitektur *Project-ZTA*. Kedua *resource group* ini akan dibuat di *region* asia tenggara (*Southeast Asia*).

**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group name | RG-ZTA-PRD |
| Region | Southeast Asia |

**Gambar 3.12 Konfigurasi RG-ZTA-PRD**

**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group name | RG-ZTA-DEV |
| Region | Southeast Asia |

**Gambar 3.13 Konfigurasi RG-ZTA-DEV**

Setelah *resource group* terbuat, selanjutnya akan dibuat *virtual network* yang digunakan untuk keperluan *private network* pada lingkungan *cloud*. *Virtual network* ini akan dikonfigurasi dengan *subnet* yang ada pada desain arsitektur *Project-ZTA*.

Pada konfigurasi *virtual network* ini, *virtual network encryption* tidak perlu diaktifkan karena hanya ada satu buah *virtual machine* pada

arsitektur ini. Fitur ini dapat melakukan enkripsi anta koneksi *virtual machine* yang ada dalam suatu *network*. Fitur *Azure Firewall* dan *Azure DdoS* Protection juga tidak akan di aktivasi, melainkan akan dikompensasi melalui komponen *web application firewall* yang berada pada *application gateway*. Sedangkan *Azure Basiton* yang merupakan salah satu cara untuk mengammankan koneksi RDP/SSH ke dalam *virtual machine* dapat dikompensasi dengan pembukaan/penutupan akses *port* SSH hanya pada saat diperlukan.

Berikut merupakan konfigurasi yang dilakukan pada *virtual network* yang ada:

**RG-ZTA-PRD**

- ZTA-PRD-vnet:
  - *Resource Group*: RG-ZTA-PRD
  - *Name*: ZTA-PRD-vnet
  - *IP addresses*: 192.169.0.0/25
  - *Subnet*:
    - ZTAMainSubnet (192.169.0.0/27)
    - ZTADBSubnet (192.169.0.32/27)
    - GatewaySubnet (192.169.0.64/27)
    - ZTAGWSubnet (192.169.0.96/27)

| Name ↑ | IPv4 |
|---|---|
| ZTAMainSubnet | 192.169.0.0/27 |
| GatewaySubnet | 192.169.0.64/27 |
| ZTADBSubnet | 192.169.0.32/27 |
| ZTAAGWSubnet | 192.169.0.96/27 |

**Gambar 3.14 Konfigurasi ZTA-PRD-vnet**

**RG-ZTA-DEV**

- ZTA-DEV-vnet:
    - *Resource Group*: RG-ZTA-DEV
    - *Name*: ZTA-DEV-vnet
    - *IP addresses*: 192.169.1.0/25
    - *Subnet*:
        - ZTAMainSubnet_dev (192.169.1.0/27)
        - ZTADBSubnet_dev (192.169.1.32/27)
        - GatewaySubnet (192.169.1.64/27)
        - ZTAGWSubnet_dev(192.169.1.96/27)

| Name ↑ | IPv4 |
|---|---|
| ZTAMainSubnet_dev | 192.169.1.0/27 |
| GatewaySubnet | 192.169.1.64/27 |
| ZTADBSubnet_dev | 192.169.1.32/27 |
| ZTAAGWSubnet_dev | 192.169.1.96/27 |

**Gambar 3.15 Konfigurasi ZTA-DEV-vnet**

Pada *virtual network* ini, terdapat tambahan 2 buah *subnet* di masing- masing *virtual network* yang disebut dengan *GatewaySubnet*, *subnet* ini akan dipergunakan untuk keperluan akses seluruh *resource* yang ada pada *virtual network* tersebut walaupun hanya mempunyai *private* IP. Sedangkan *ZTAGWSubnet* akan digunakan sebagai jaringan untuk *Application Gateway*.

*Resource* selanjutnya yang akan dikonfigurasi adalah *virtual machine* dan *database* yang merupakan komponen utama dalam arsitektur ini. Berikut merupakan konfigurasi yang digunakan:

- ***ZTA-VM-PRD***
    - **Basic**
        - *Resource group*: RG-ZTA-PRD
        - *Name*: ZTA-VM-PRD

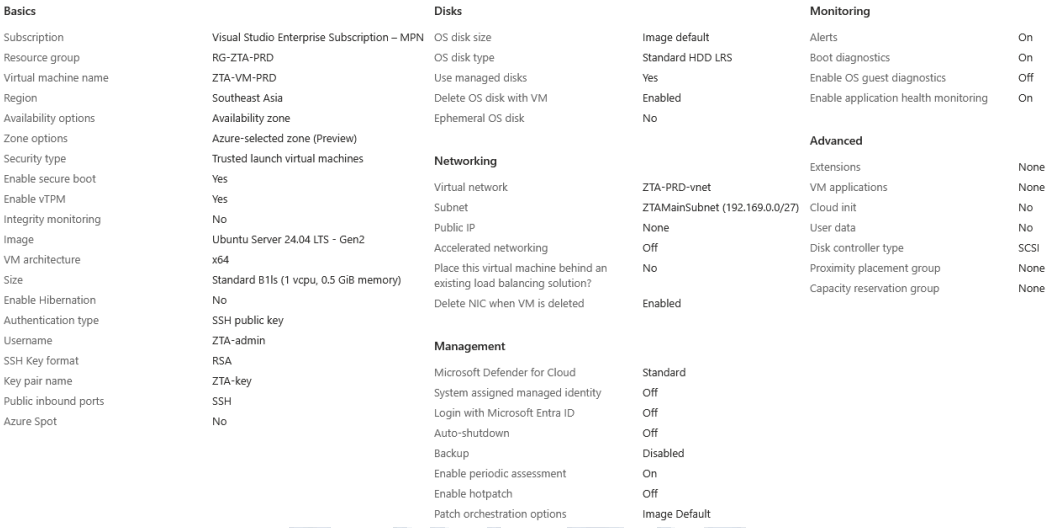
- *Availability options*: *Availability Zone (Azure Selected)*
- *Security type*: *Standard*
- *Machine Type*: *Standard*_B1 ls (1 vCPU, 0.5 GiB *memory*)
- *Image*: *Ubuntu Server* 24.04 LTS- x64 *Gen*2
- *Authenticaiton Type*: SSH *public key*
- *Username*: *ZTA-admin*
- *Key pair name*: *ZTA-key*
- *Inbound ports*: SSH (22)

- **Disk**
  - *OS Disk size: Image default (30 GiB)*
  - *OS Disk type: Standard HDD (locally-redundant storage)*
  - *Encryption at Host: Enabled*

- **Networking**
  - *Virtual Network: ZTA-PRD-vnet*
  - *Subnet: ZTAMainSubnet (192.169.0.0/27)*
  - *Public IP: -*

- **Management**
  - *Auto-shutdown: Disabled*
  - *Enable Periodic Assessment: Enabled*

- **Monitoring**
  - *Boot Diagnostics: Enabled with managed storage account*
  - *Alert rules: Enabled, Default config*
  - *Health monitoring: Enabled*



**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-ZTA-PRD |
| Virtual machine name | ZTA-VM-PRD |
| Region | Southeast Asia |
| Availability options | Availability zone |
| Zone options | Azure-selected zone (Preview) |
| Security type | Trusted launch virtual machines |
| Enable secure boot | Yes |
| Enable vTPM | Yes |
| Integrity monitoring | No |
| Image | Ubuntu Server 24.04 LTS - Gen2 |
| VM architecture | x64 |
| Size | Standard B1ls (1 vcpu, 0.5 GiB memory) |
| Enable Hibernation | No |
| Authentication type | SSH public key |
| Username | ZTA-admin |
| SSH Key format | RSA |
| Key pair name | ZTA-key |
| Public inbound ports | SSH |
| Azure Spot | No |

**Disks**

| | |
|---|---|
| OS disk size | Image default |
| OS disk type | Standard HDD LRS |
| Use managed disks | Yes |
| Delete OS disk with VM | Enabled |
| Ephemeral OS disk | No |

**Networking**

| | |
|---|---|
| Virtual network | ZTA-PRD-vnet |
| Subnet | ZTAMainSubnet (192.169.0.0/27) |
| Public IP | None |
| Accelerated networking | Off |
| Place this virtual machine behind an existing load balancing solution? | No |
| Delete NIC when VM is deleted | Enabled |

**Management**

| | |
|---|---|
| Microsoft Defender for Cloud | Standard |
| System assigned managed identity | Off |
| Login with Microsoft Entra ID | Off |
| Auto-shutdown | Off |
| Backup | Disabled |
| Enable periodic assessment | On |
| Enable hotpatch | Off |
| Patch orchestration options | Image Default |

**Monitoring**

| | |
|---|---|
| Alerts | On |
| Boot diagnostics | On |
| Enable OS guest diagnostics | Off |
| Enable application health monitoring | On |

**Advanced**

| | |
|---|---|
| Extensions | None |
| VM applications | None |
| Cloud init | No |
| User data | No |
| Disk controller type | SCSI |
| Proximity placement group | None |
| Capacity reservation group | None |

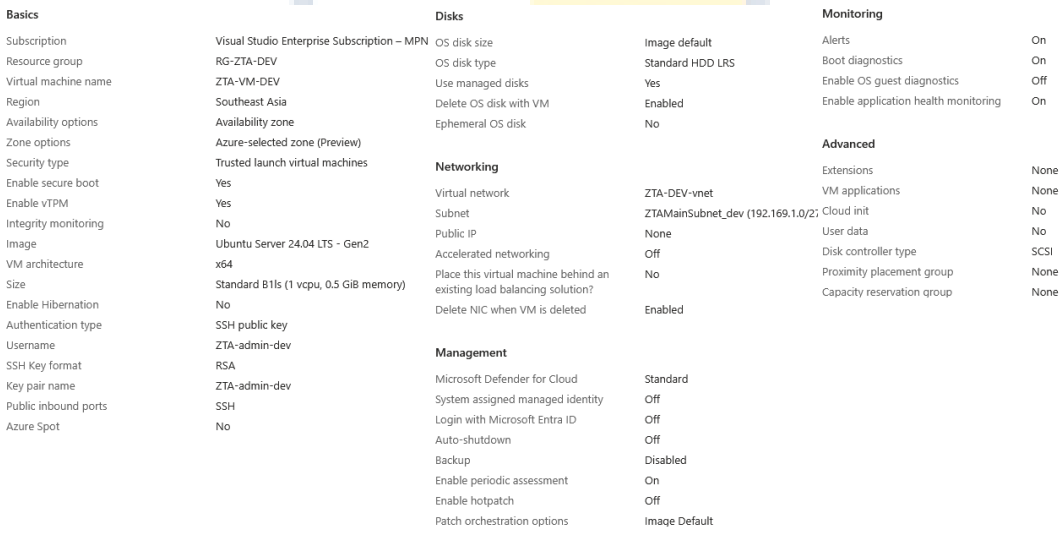
**Gambar 3.16 Konfigurasi ZTA-VM-PRD**

- ***ZTA-VM-DEV***
  - **Basic**
    - *Resource group*: RG-ZTA-DEV
    - *Name*: ZTA-VM-DEV
    - *Availability options*: *No Infrastructure Redundancy*
    - *Security type*: *Standard*
    - *Machine Type*: *Standard*_B1 ls (1 vCPU, 0.5 GiB *memory*)
    - *Image*: *Ubuntu Server* 24.04 LTS- x64 *Gen*2
    - *Authenticaiton Type*: SSH *public key*
    - *Username*: *ZTA-admin-dev*
    - *Key pair name*: *ZTA-key-dev*
    - *Inbound ports*: SSH (22)
  - **Disk**
    - OS *Disk size*: *Image default* (30 GiB)
    - *OS Disk type*: *Standard* HDD (*locally-redundant storage*)
    - *Encryption at Host: Enabled*

- **Networking**
  - *Virtual Network: ZTA-PRD-vnet*
  - *Subnet: ZTAMainSubnet (192.169.0.0/27)*
  - *Public IP: -*

- **Management**
  - *Auto-shutdown: Disabled*
  - *Enable Periodic Assessment: Disabled*

- **Monitoring**
  - *Boot Diagnostics: Enabled with managed storage account*
  - *Alert rules: Enabled, Default config*
  - *Health monitoring: Enabled*



**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-ZTA-DEV |
| Virtual machine name | ZTA-VM-DEV |
| Region | Southeast Asia |
| Availability options | Availability zone |
| Zone options | Azure-selected zone (Preview) |
| Security type | Trusted launch virtual machines |
| Enable secure boot | Yes |
| Enable vTPM | Yes |
| Integrity monitoring | No |
| Image | Ubuntu Server 24.04 LTS - Gen2 |
| VM architecture | x64 |
| Size | Standard B1ls (1 vcpu, 0.5 GiB memory) |
| Enable Hibernation | No |
| Authentication type | SSH public key |
| Username | ZTA-admin-dev |
| SSH Key format | RSA |
| Key pair name | ZTA-admin-dev |
| Public inbound ports | SSH |
| Azure Spot | No |

**Disks**

| | |
|---|---|
| OS disk size | Image default |
| OS disk type | Standard HDD LRS |
| Use managed disks | Yes |
| Delete OS disk with VM | Enabled |
| Ephemeral OS disk | No |

**Networking**

| | |
|---|---|
| Virtual network | ZTA-DEV-vnet |
| Subnet | ZTAMainSubnet_dev (192.169.1.0/2 |
| Public IP | None |
| Accelerated networking | Off |
| Place this virtual machine behind an existing load balancing solution? | No |
| Delete NIC when VM is deleted | Enabled |

**Management**

| | |
|---|---|
| Microsoft Defender for Cloud | Standard |
| System assigned managed identity | Off |
| Login with Microsoft Entra ID | Off |
| Auto-shutdown | Off |
| Backup | Disabled |
| Enable periodic assessment | On |
| Enable hotpatch | Off |
| Patch orchestration options | Image Default |

**Monitoring**

| | |
|---|---|
| Alerts | On |
| Boot diagnostics | On |
| Enable OS guest diagnostics | Off |
| Enable application health monitoring | On |

**Advanced**

| | |
|---|---|
| Extensions | None |
| VM applications | None |
| Cloud init | No |
| User data | No |
| Disk controller type | SCSI |
| Proximity placement group | None |
| Capacity reservation group | None |

**Gambar 3.17 Konfigurasi ZTA-VM-DEV**

Pada konfigurasi VM di *Project-ZTA*, dapat diketahui ada beberapa fitur yang diaktifkan. Hal ini guna memenuhi prinsip- prinsip dalam konsep ZTA, yaitu selalu dilakukannya pemantauan (*monitoring*) yang dimana dapat dalam VM, dapat dipenuhi dengan menggunakan *resource health*

*monitoring* dan *alerting*. Lalu juga ada prinsip dimana diperlukannya pengamanan dalam setiap komponen yang ada, hal ini dapat dipenuhi dengan menggunakan fitur *encryption at host* pada *disk* yang ada dalam VM tersebut. Fitur *boot diagnostics* juga diaktifkan untuk memastikan VM berjalan dengan versi atau *patch* paling baru. *Zone redundancy* juga digunakan

- ***ztadbprd***
  - **Basics**
    - *Resource Group*: RG-ZTA-PRD
    - *Server name*: *ztadbprd*
    - *Workload type*: *For development and hobby projects*
    - *Store autogrow*: *Disabled*
    - *Backup retention:* 7 *day*
    - *Authentication method*: MySQL *authentication only*
    - *Administrator login*: ztadbprd_admin
    - *Administrator password*: root123!
  - **Networking**
    - *Connectivity Method: Private Access*
    - *Virtual Network*: *ZTA-PRD-vnet*
    - *Subnet*: ZTA-PRD-vnet/ZTADBSubnet
    - *Private DNS Zone*: (New), Default

**Basics (Change)**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-ZTA-PRD |
| Server name | ztadbprd |
| Administrator login | ztadbprd_admin |
| Location | Southeast Asia |
| Availability zone | No preference |
| High availability | Not enabled |
| MySQL version | 8.0 |
| Compute + storage | Burstable, B1ms, 1 vCores, 2 GiB RAM, 20 storage, Auto scale IOPS |
| Backup retention period (in days) | 7 day(s) |
| Storage autogrow | Not enabled |
| Geo-redundancy | Not enabled |
| Zonal Resiliency | No |

**Networking (Change)**

| | |
|---|---|
| Connectivity method | Private access (VNet Integration) |
| Virtual network subscription | Visual Studio Enterprise Subscription – MPN |
| Virtual network resource group | RG-ZTA-PRD |
| Virtual network | ZTA-PRD-vnet |
| Delegated subnet | ZTADBSubnet |
| Private DNS zone subscription | Visual Studio Enterprise Subscription – MPN |
| Private DNS zone resource group | RG-ZTA-PRD |
| Private DNS zone | (New) ztadbprd.private.mysql.database.azure.com |

**Security (Change)**

| | |
|---|---|
| Data encryption | Service-managed key |

**Gambar 3.18 Konfigurasi *ztadbprd***

- ***ztadbdev***
  - **Basics**
    - *Resource Group*: RG-ZTA-DEV
    - *Server name*: *ztadbdev*
    - *Workload type*: *For development and hobby projects*
    - *Store autogrow*: *Disabled*
    - *Backup retention: 7 day*
    - *Authentication method*: MySQL *authentication only*

- *Administrator login*: ztadbdev_admin
- *Administrator password*: root123!

- **Networking**
  - *Connectivity Method: Private Access*
  - *Virtual Network*: *ZTA-DEV-vnet*
  - *Subnet*: ZTA-DEV-vnet/ZTADBSubnet_dev
  - *Private DNS Zone*: (New), Default

**Basics (Change)**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-ZTA-DEV |
| Server name | ztadbdev |
| Administrator login | ztadbdev_admin |
| Location | Southeast Asia |
| Availability zone | No preference |
| High availability | Not enabled |
| MySQL version | 8.0 |
| Compute + storage | Burstable, B1ms, 1 vCores, 2 GiB RAM, 20 storage, Auto scale IOPS |
| Backup retention period (in days) | 7 day(s) |
| Storage autogrow | Not enabled |
| Geo-redundancy | Not enabled |
| Zonal Resiliency | No |

**Networking (Change)**

| | |
|---|---|
| Connectivity method | Private access (VNet Integration) |
| Virtual network subscription | Visual Studio Enterprise Subscription – MPN |
| Virtual network resource group | RG-ZTA-DEV |
| Virtual network | ZTA-DEV-vnet |
| Delegated subnet | ZTADBSubnet_dev |
| Private DNS zone subscription | Visual Studio Enterprise Subscription – MPN |
| Private DNS zone resource group | rg-zta-prd |
| Private DNS zone | ztadbprd.private.mysql.database.azure.com |

**Security (Change)**

| | |
|---|---|
| Data encryption | Service-managed key |

**Gambar 3.19 Konfigurasi *ztadbdev***

Setelah terbuatnya komponen utama yang ada pada *Project_ZTA*, selanjutnya akan dilanjutkan dengan konfigurasi 2 buah komponen tambahan pada kedua *resource group* yang ada, yaitu *application gateway* dan *virtual network gateway*. Berikut merupakan konfigurasi yang akan digunakan untuk *application gateway* yang ada:

- ***ZTA-appgateway-PRD***
  - **Basics**
    - *Resource Group*: RG-ZTA-PRD
    - *Name*: ZTA-appgateway-PRD
    - *Virtual Network:* ZTA-PRD-vnet
    - *Subnet:* ZTAGWSubnet *(192.169.0.96/27)*
  - **Frontends**
    - *Public* IP*:* ZTA-VM-PRD-pub

**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-ZTA-PRD |
| Name | ZTA-appgateway-PRD |
| Region | Southeast Asia |
| Tier | Basic |
| Instance count | 2 |
| Availability zone | Zones 1, 2, 3 |
| HTTP2 | Enabled |
| Virtual network | ZTA-PRD-vnet |
| Subnet | ZTAAGWSubnet (192.169.0.96/27) |

**Frontends**

| | |
|---|---|
| Public IPv4 address name | ZTA-VM-PRD-pub |
| SKU | Standard |
| Assignment | Static |
| Availability zone | ZoneRedundant |

**Gambar 3.20 Konfigurasi *ZTA-appgateway-PRD***

- ***ZTA-appgateway-DEV***
  - **Basics**
    - *Resource Group*: RG-ZTA-DEV

- *Name*: ZTA-appgateway-DEV
- *Virtual Network:* ZTA-DEV-vnet
- *Subnet:* ZTAGWSubnet-dev *(192.169.1.96/27)*

- **Frontends**
  - *Public* IP*:* ZTA-VM-DEV-pub

**Basics**

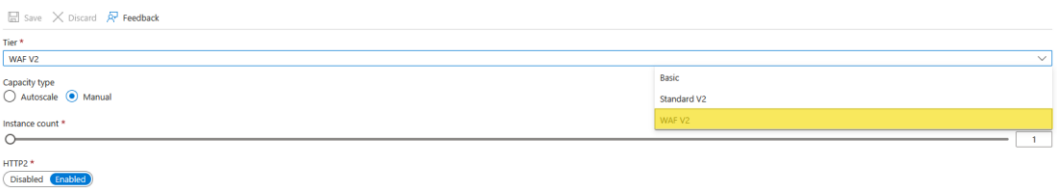
| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-ZTA-DEV |
| Name | ZTA-appgateway-DEV |
| Region | Southeast Asia |
| Tier | Basic |
| Instance count | 2 |
| Availability zone | Zones 1, 2, 3 |
| HTTP2 | Enabled |
| Virtual network | ZTA-DEV-vnet |
| Subnet | ZTAAGWSubnet_dev (192.169.1.96/27) |

**Frontends**

| | |
|---|---|
| Public IPv4 address name | ZTA-VM-DEV-pub |
| SKU | Standard |
| Assignment | Static |
| Availability zone | ZoneRedundant |

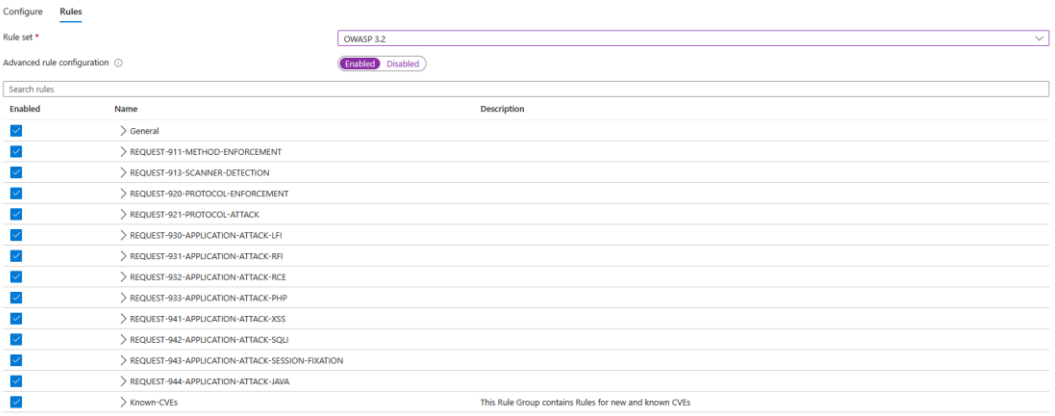
**Gambar 3.21 Konfigurasi *ZTA-appgateway-DEV***

Setelah *Application Gateway* sudah selesai dibuat, selanjutnya kita perlu merubah beberapa konfigurasi yang ada pada masing masing *application gateway*. Hal yang akan diubah adalah *tier* yang digunakan dari *Basic* menjadi WAF v2. Hal ini dilakukan untuk mengaktifkan protokol keamanan *web application firewall* yang ada pada *application gateway* yang telah dibuat.



**Gambar 3.22 Mengubah *Gateway Tier* pada *Application Gateway***

Dengan mengaktifkan *tier* WAF v2, *application gateway* akan mempunyai *firewall* yang bekerja dengan mengikuti salah satu protokol standar keaman dalam *web application*. Protokol yang akan digunakan pada penelitian ini adalah OWASP 3.2, protokol ini juga dapat dikonfigurasi lebih lanjut sesuai dengan kebijakan yang ada dengan mengaktifkan *advanced rule configuration*.




**Gambar 3.23 Mengaktifkan WAF *Rules*.**

Setelah semua konfigurasi yang harus dilakukan pada *application gateway* telah terpenuhi, akan dibuat satu komponen terakhir yang menjadi gerbang belakang bagi *developer* dan *engineer* dalam mengakses komponen yang ada di dalam lingkup *Project_ZTA*. Komponen ini adalah *Azure Virtual Network Gateway* yang akan dikonfigurasi menjadi *gateway* bagi koneksi VPN yang akan dibuat. Aplikasi VPN yang akan digunakan adalah *Azure VPN Client* yang merupakan salah satu dari beberapa VPN *client* yang dapat digunakan selaras dengan *gateway* ini. Berikut merupakan konfigurasi yang harus dilakukan pada *virtual network gateway*:

- ***ZTA-gateway-PRD***
    - **Basic**
        - *Resource Group*: RG-ZTA-PRD
        - *Name*: ZTA-gateway-PRD

- SKU: VpnGw1
- *Generation*: 1
- *Virtual Network*: ZTA-PRD-vnet
- *Subnet*: GatewaySubnet (192.169.0.64/27)
- *Gateway type*: VPN
- *Public* IP: PRD-Gateway-pub

**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-ZTA-PRD |
| Name | ZTA-gateway-PRD |
| Region | Southeast Asia |
| SKU | VpnGw1 |
| Generation | Generation1 |
| Virtual network | ZTA-PRD-vnet |
| Subnet | GatewaySubnet (192.169.0.64/27) |
| Gateway type | Vpn |
| VPN type | RouteBased |
| Enable active-active mode | Disabled |
| Configure BGP | Disabled |
| Public IP address | PRD-Gateway-pub |

**Gambar 3.24 Konfigurasi *ZTA-gateway-PRD***

- ***ZTA-gateway-DEV***
  - **Basic**
    - *Resource Group*: RG-ZTA-DEV
    - *Name*: ZTA-gateway-DEV
    - SKU: VpnGw1
    - *Generation*: 1
    - *Virtual Network*: ZTA-DEV-vnet
    - *Subnet*: GatewaySubnet (192.169.1.64/27)
    - *Gateway type*: VPN
    - *Public* IP: DEV-Gateway-pub

**Basics**

| | |
|---|---|
| Subscription | Visual Studio Enterprise Subscription – MPN |
| Resource group | RG-ZTA-DEV |
| Name | ZTA-gateway-DEV |
| Region | Southeast Asia |
| SKU | VpnGw1 |
| Generation | Generation1 |
| Virtual network | ZTA-DEV-vnet |
| Subnet | GatewaySubnet (192.169.1.64/27) |
| Gateway type | Vpn |
| VPN type | RouteBased |
| Enable active-active mode | Disabled |
| Configure BGP | Disabled |
| Public IP address | DEV-Gateway-pub |

**Gambar 3.25 Konfigurasi *ZTA-gateway-DEV***

Setelah konfigurasi *virtual network gateway* selesai, selanjutnya akan dilakukan konfigurasi koneksi P2S dari *local device* ke *Azure VPN Gateway* yang telah dibuat. Hal ini dapat dilakukan dengan mengaktifkan dan melakukan konfigurasi VPN pada masing- masing *gateway*. Koneksi yang ada akan berbasis *self-signed certificate*, dimana *certificate* akan dibuat melalui *local device* yang akan terkoneksi dengan VPN *gateway* tersebut.

## 3.3 Instrumen Penelitian

Dalam penelitian ini, penulis akan menggunakan *Microsoft Azure* sebagai instrumen penelitiannya. Dalam penelitian ini, *Microsoft Azure* akan digunakan sebagai *cloud service provider* yang dimana akan menjadi tempat diimplementasikannya konsep *Zero Trust Architecture*. Penulis memilih *Microsoft Azure* sebagai instrumen penelitian karena *cloud provider* tersebut merupakan salah satu yang paling marak digunakan. Hal ini menjadi pertimbangan penulis agar hasil yang diberikan dapat bermanfaat bagi banyak penggunanya serta dapat memberikan ide dalam melakukan pengembangan keamanan di dalam *cloud*.

### 3.4 Objek Penelitian

Hal yang menjadi objek penelitian adalah konsep keamanan *Zero Trust Architecture* yang merupakan salah satu pengembangan kerangka kerja keamanan dalam dunia komputer. Konsep ZTA ini menjadi objek fokus dalam penelitian ini karena akan diimplementasikan kedalam *cloud environment*. Proses implementasi tersebut akan dilakukan di dalam *cloud environment Microsoft Azure* yang merupakan salah satu dari *cloud service provider* yang sangat marak digunakan.