HARDENING SERVER

By : RADJA RIZQI RAMADHAN

Data Pendukung	
LinkedIn	https://id.linkedin.com/in/rajarizqi
Git Repo	https://github.com/dimasrizqi
Blog / Web	https://medium.com/radjarizqiramadhan
Youtube	https://www.youtube.com/user/dimasrizqi
Facebook	https://www.facebook.com/rajarramadhan01
Instagram	@dimasrizqi
Twitter	raja_rizqi
Telegram ID	@Dimasrizqi

Futami Food & Beverages

Website | Directions | Save

4.1 ★★★★☆ 35 Google reviews

Manufacturer in Tangkil, West Java

Address: JL. Telkom Pasir Muncang, RT 03/ RW 02, Pasir Muncang, Caringin, Pasir Muncang, Kec. Caringin, Bogor, Jawa Barat 16730

Hours: Open · Closes 5PM

A user suggested these hours

Mon-Sun 8AM–5PM

Phone: (0251) 220033

Feb 2019 - Now
PT. Futami Food & Bevereges - IT Support

Agt 2018 - Feb 2019
PT. Aplikanusa LINTASARTA - Project Engineer

Nov 2017 - Agt 2018
KOPERASI Simpan Pinjam Sejahtera Bersama - Network Engineer

Jul 2017 - Nov 2017
Kementrian Agama Jakarta - System Engineer

Jun 2016 - Jul 2017
PT Defender Nusa Semesta - Security Engineer

Mei 2015 - Jun 2016
PT. Futami Food & Bevereges - IT Support

Jun 2011 - Mei 2015
SMK WIKRAMA BOGOR - Maintenance & Repair

Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface. By removing superfluous programs, accounts functions, applications, ports, permissions, access, etc. attackers and malware have fewer opportunities to gain a foothold within your IT ecosystem.

Systems hardening demands a methodical approach to audit, identify, close, and control potential security vulnerabilities throughout your organization. There are several types of system hardening activities, including:

- Application hardening
- Operating system hardening
- Server hardening
- Database hardening
- Network hardening

Although the principles of system hardening are universal, specific tools and techniques do vary depending on the type of hardening you are carrying out. System hardening is needed throughout the lifecycle of technology, from initial installation, through configuration, maintenance, and support, to end-of-life decommissioning. Systems hardening is also a requirement of mandates such as PCI DSS and HIPAA.

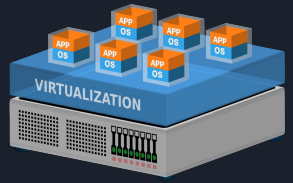
https://www.beyondtrust.com/resources/glossary/systems-hardening

Apa Itu Komputer Server?

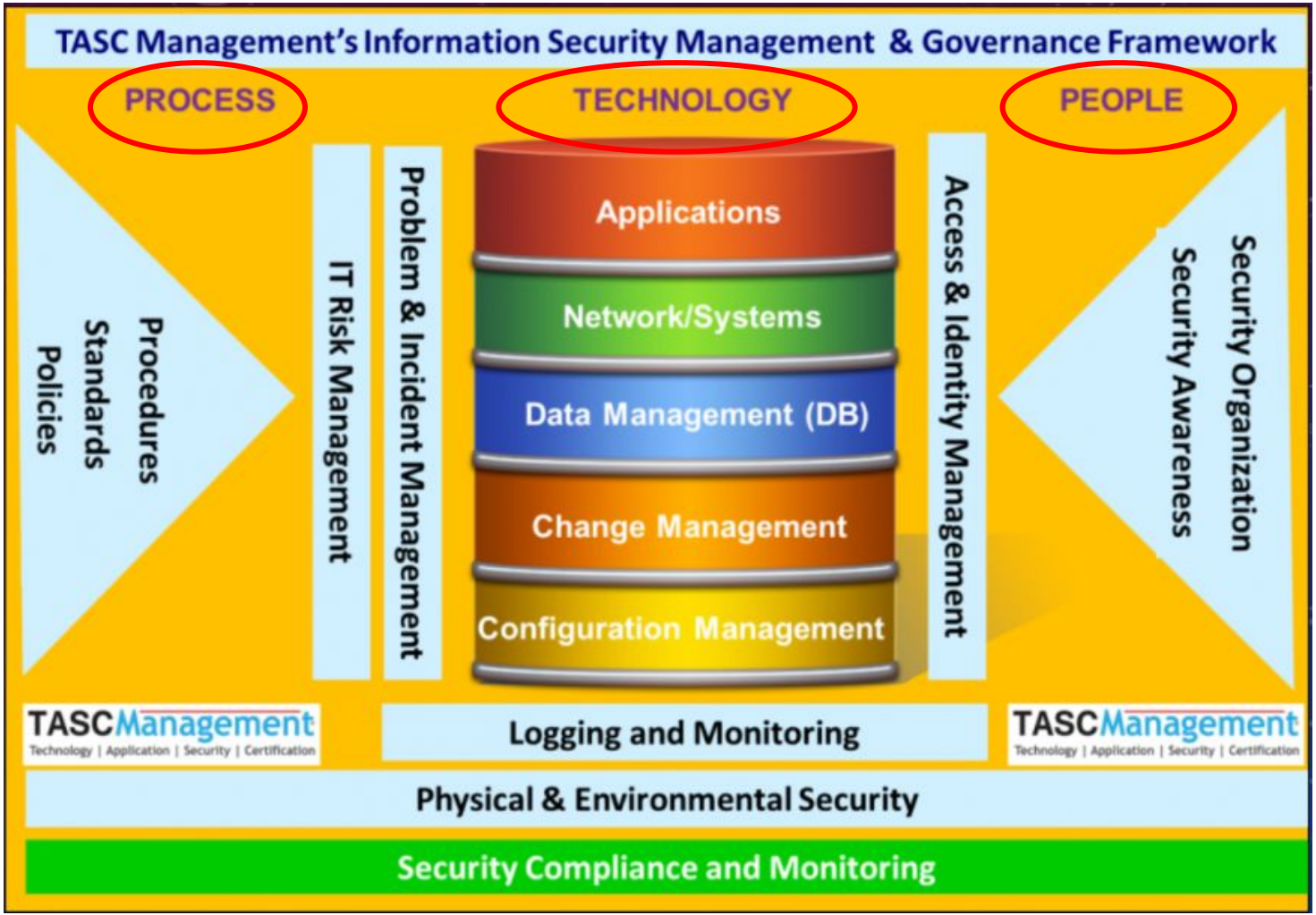
Di dalam suatu server atau jaringan terdapat dua jenis perangkat, yaitu komputer server dan komputer client. Nah, komputer server adalah perangkat yang digunakan untuk mengelola segala aktivitas yang terjadi di dalam jaringan tersebut.

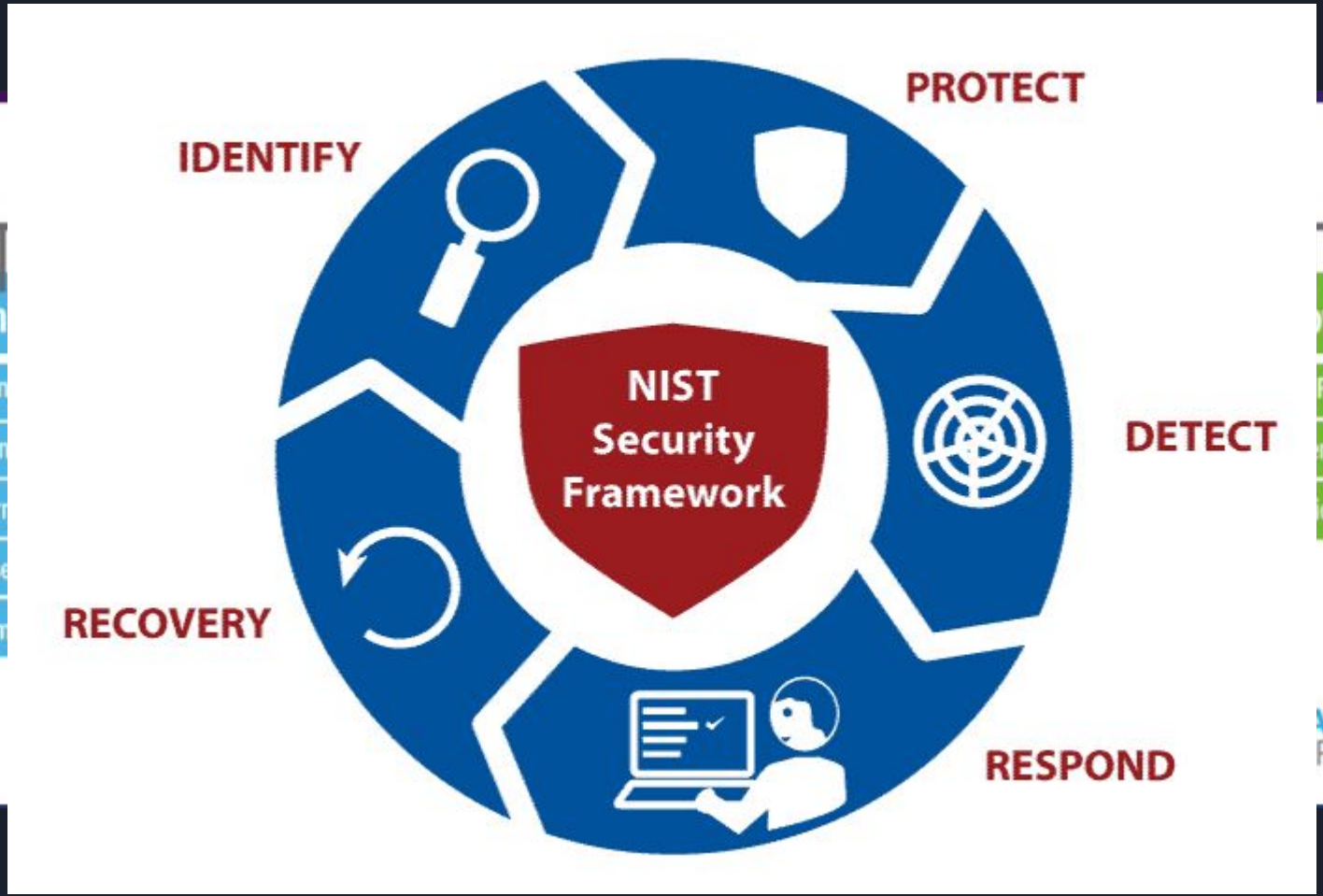
Oleh karena itu, komputer ini memiliki berbagai fungsi, termasuk:

- Menyediakan database atau file yang dapat digunakan bersama-sama oleh komputer client;
- Melayani permintaan komputer client untuk menggunakan database atau file tersebut;
- Mengatur lalu lintas transfer data atau file yang diminta komputer client;
- Menyimpan data atau file yang dikirim oleh komputer client;
- Mengatur hak akses data atau file dalam sebuah jaringan;
- Melindungi komputer client dari malware dengan anti malware atau firewall.

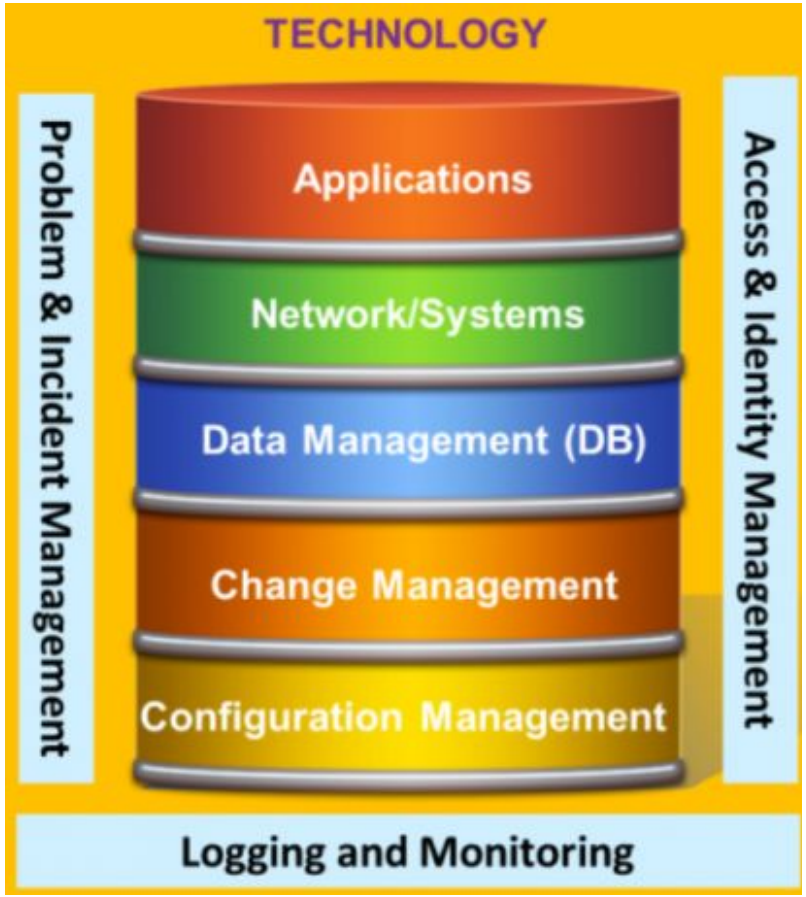


https://www.niagahoster.co.id/blog/komputer-server/


TASC Management's Information Security Management & Governance Framework
PROCESS
TECHNOLOGY
PEOPLE
Policies
Standards
Procedures
IT Risk Management
Problem & Incident Management
Applications
Network/Systems
Data Management (DB)
Change Management
Configuration Management
Access & Identity Management
Security Awareness
Security Organization
TASCManagement
Technology | Application | Security | Certification
Logging and Monitoring
TASCManagement
Technology | Application | Security | Certification
Physical & Environmental Security
Security Compliance and Monitoring


PROTECT
IDENTIFY
NIST
Security
Framework
DETECT
RECOVERY
RESPOND

All About Security



LINUX

1. Gunakan password yang tidak umum (simbol, angka, spasi)
2. SSH dengan private key
3. Disable root remote login
4. Atau tutup port port umum (ssh, database, file transfer, dns, proxy dll)
5. Hak akses user dalam menjalankan aplikasi
6. Monitoring & logging
7. Backup berbeda media (hardisk external, file server atau cloud)
8. Gunakan virtualisasi atau containerize
9. Pasang perangkat firewall pada jaringan

WINDOWS

1. Update windows & antivirus
2. Aktifkan firewall
3. Ganti atau disable port remote desktop
4. Matikan folder sharing jika tidak perlu
5. Disaran untuk tidak menginstall aplikasi bajakan
6. Jangan sembarangan download aplikasi yang tidak jelas
7. Tidak sering digunakan sebagai user
8. Backup berbeda media (hardisk external, file server atau cloud)
9. Gunakan virtualisasi atau containerize
10. Pasang perangkat firewall pada jaringan

FIREWALL GATHNER

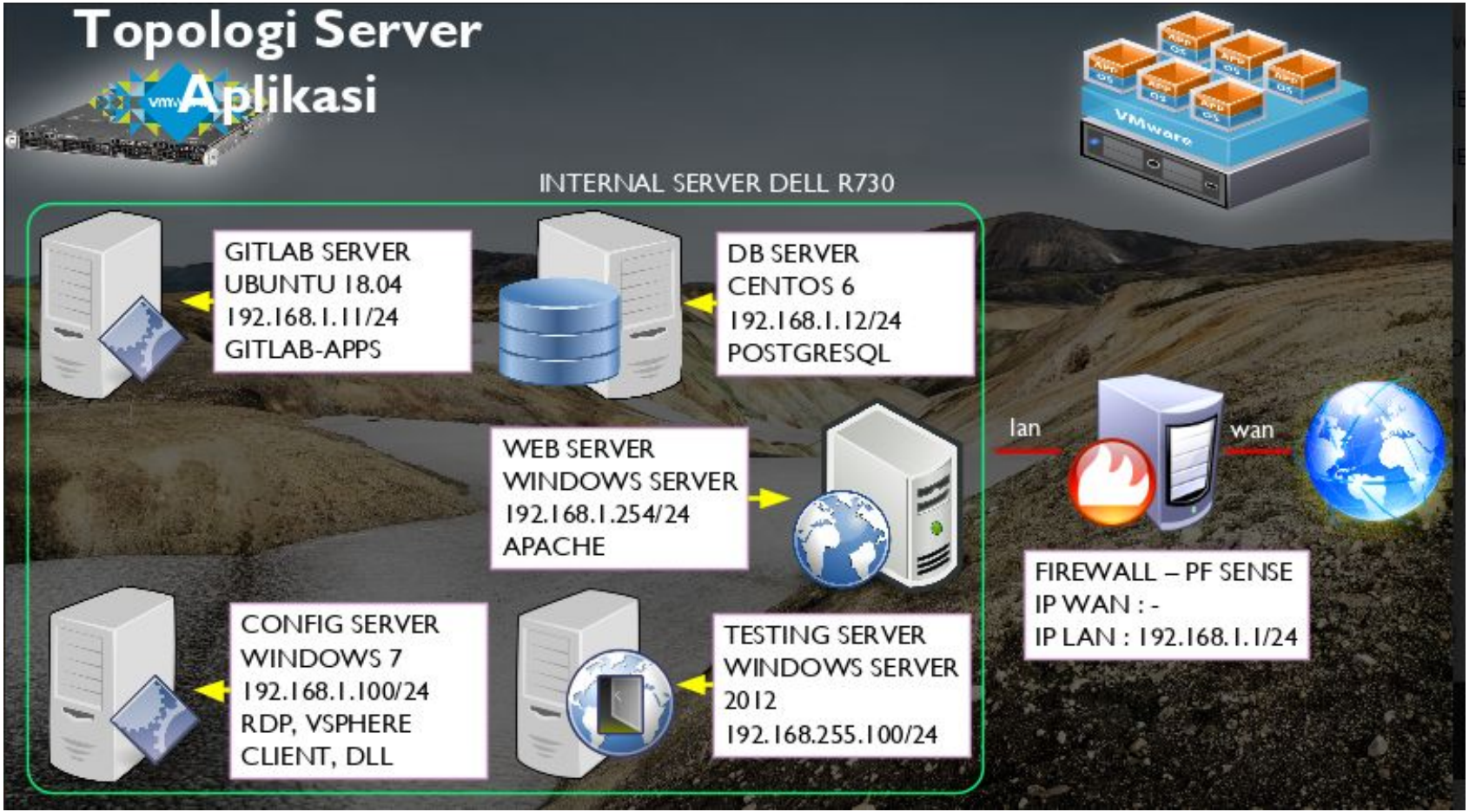
Figure 1. Magic Quadrant for Network Firewalls

Source: Gartner (September 2019)

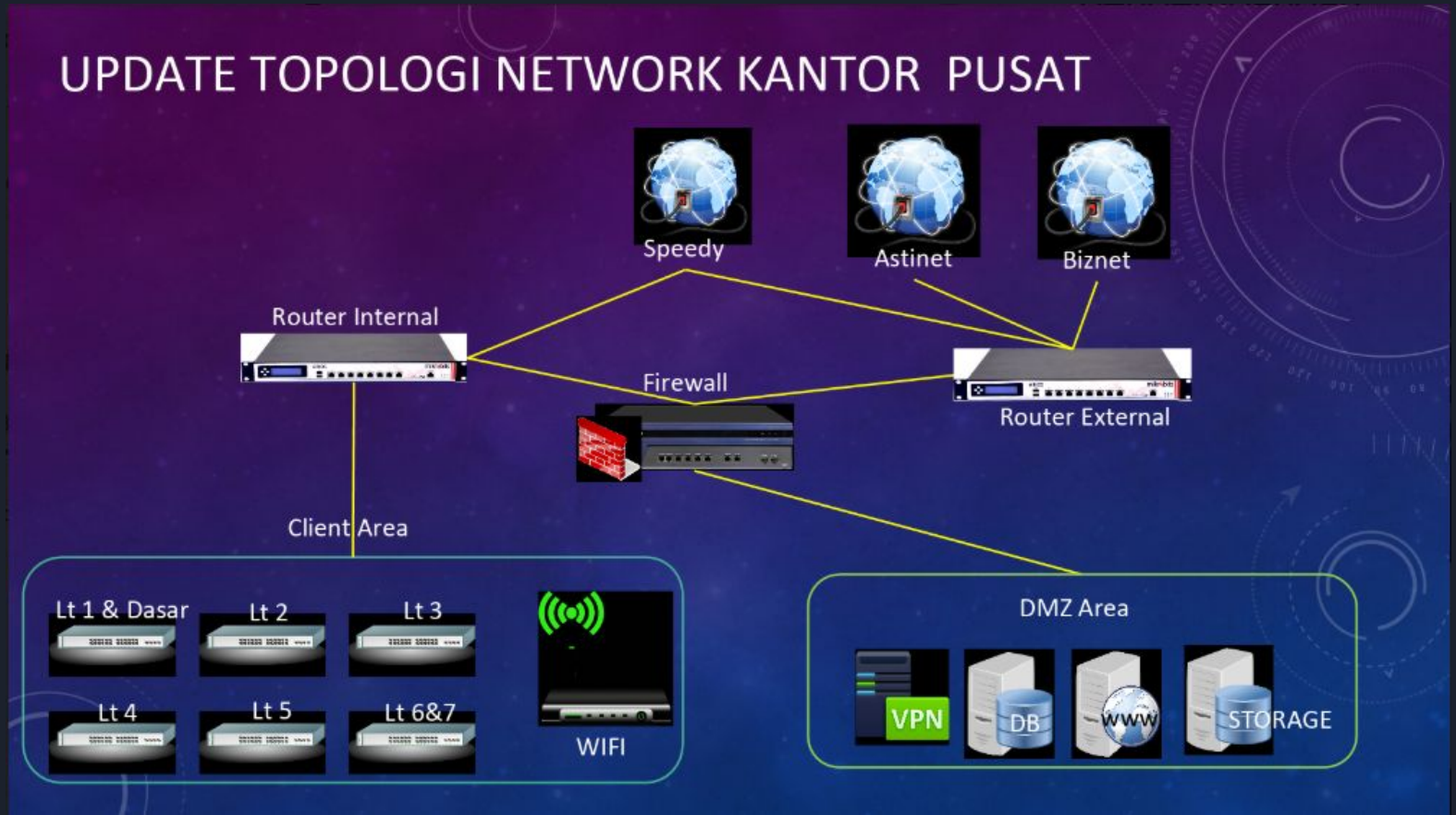
Figure 1. Magic Quadrant for Web Application Firewalls

Source: Gartner (September 2019)

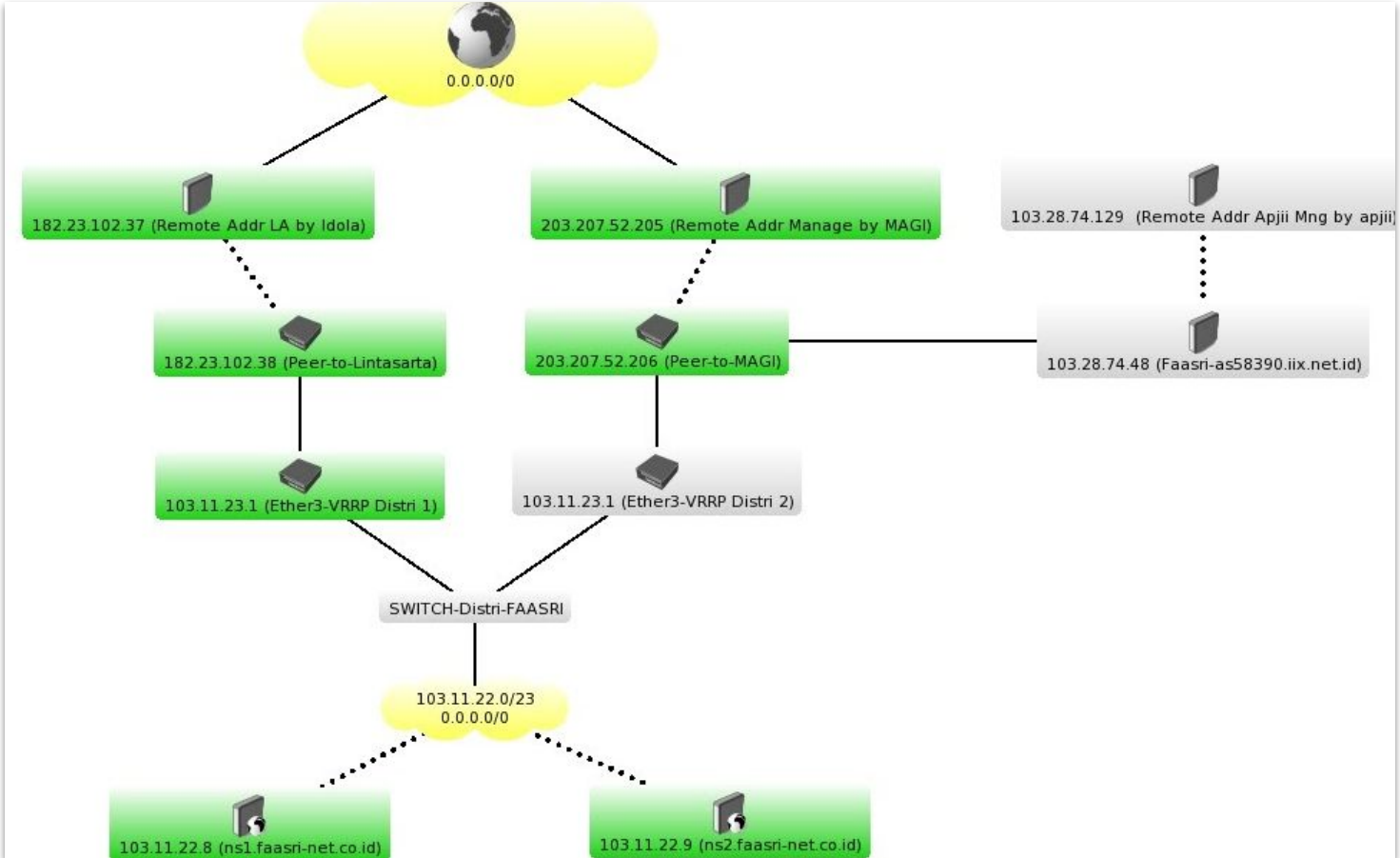
Layout Jaringan - RSMM



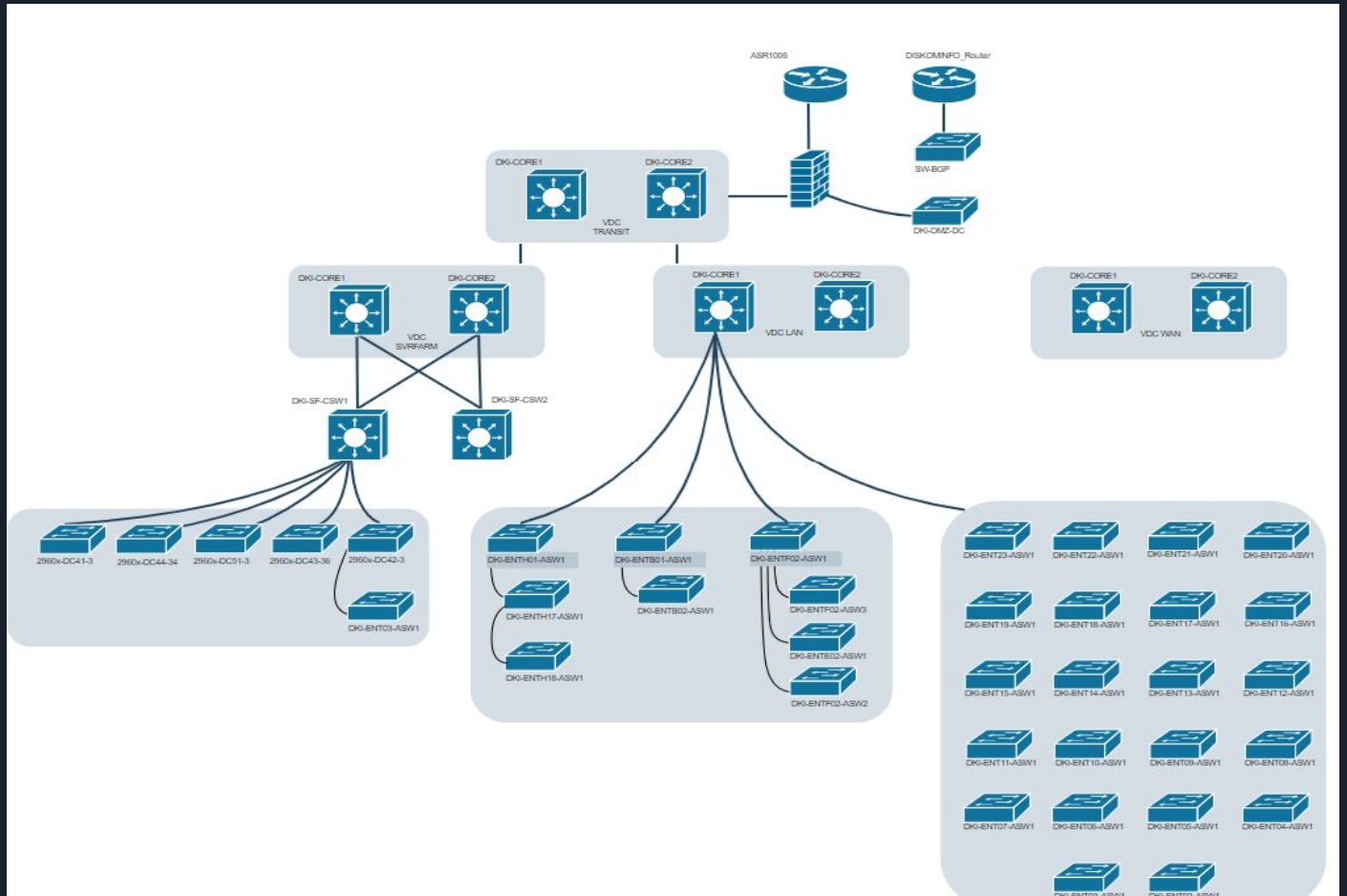
Layout jaringan - Koperasi Sejahtera Bersama



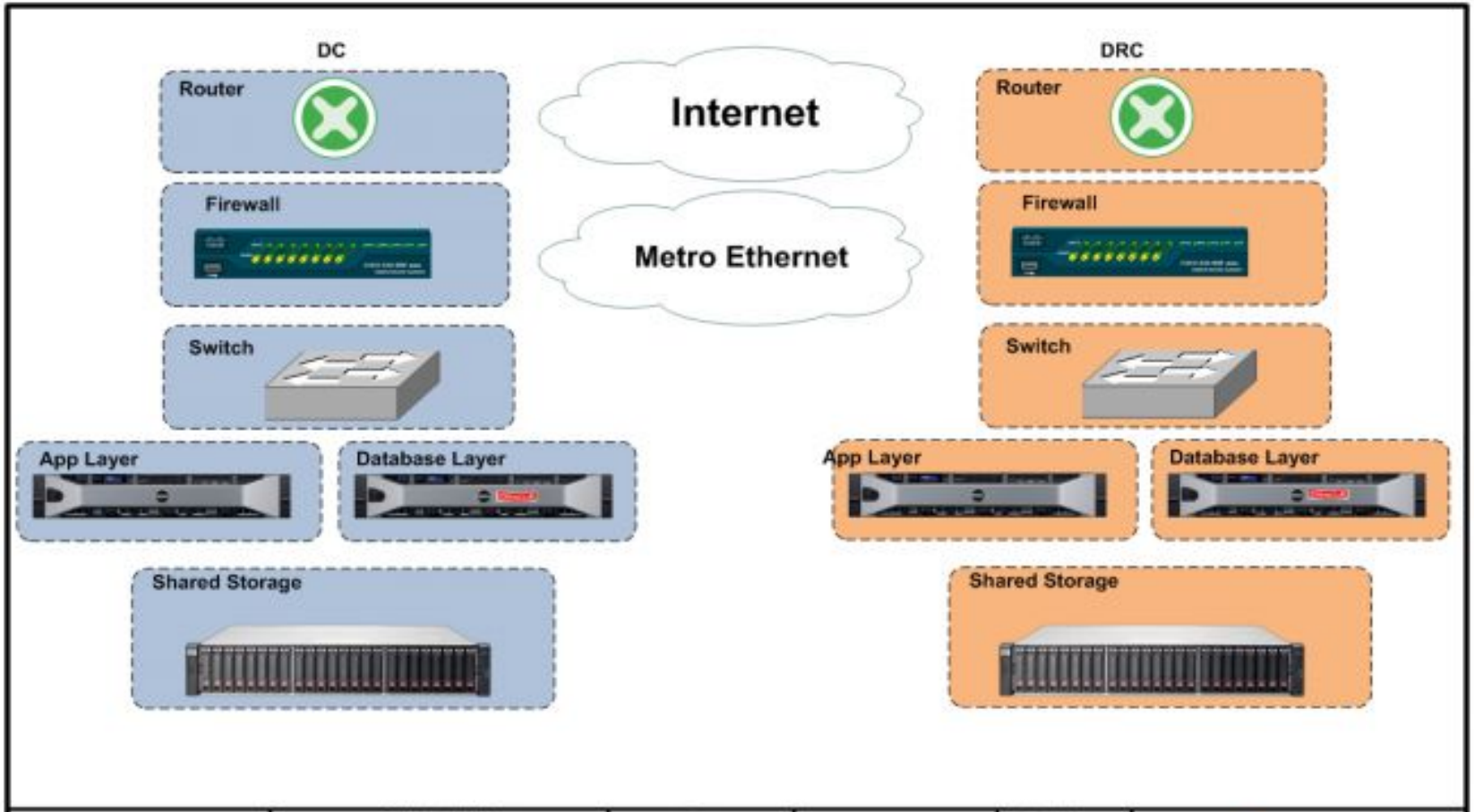
Layout Jaringan - PT Faasri



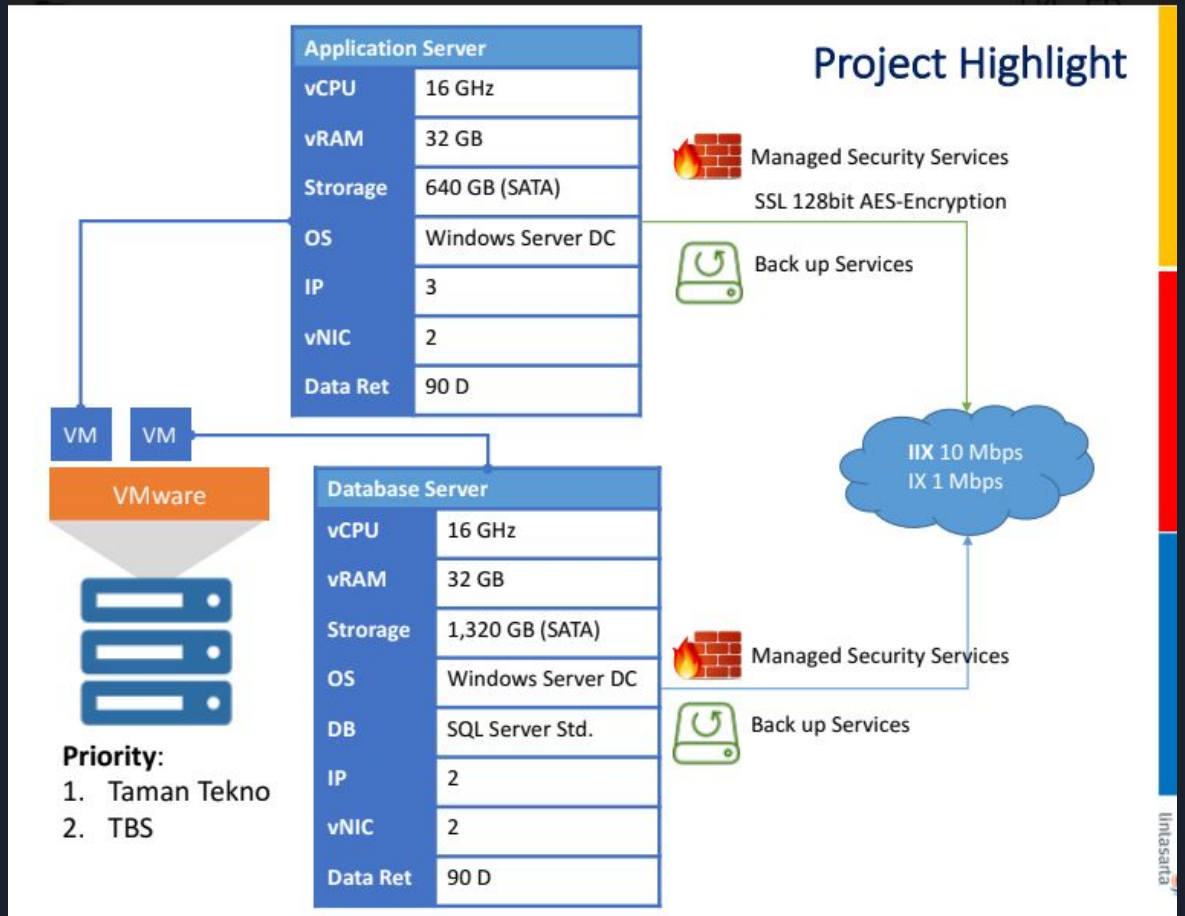
Layout jaringan - PEMPROV DKI



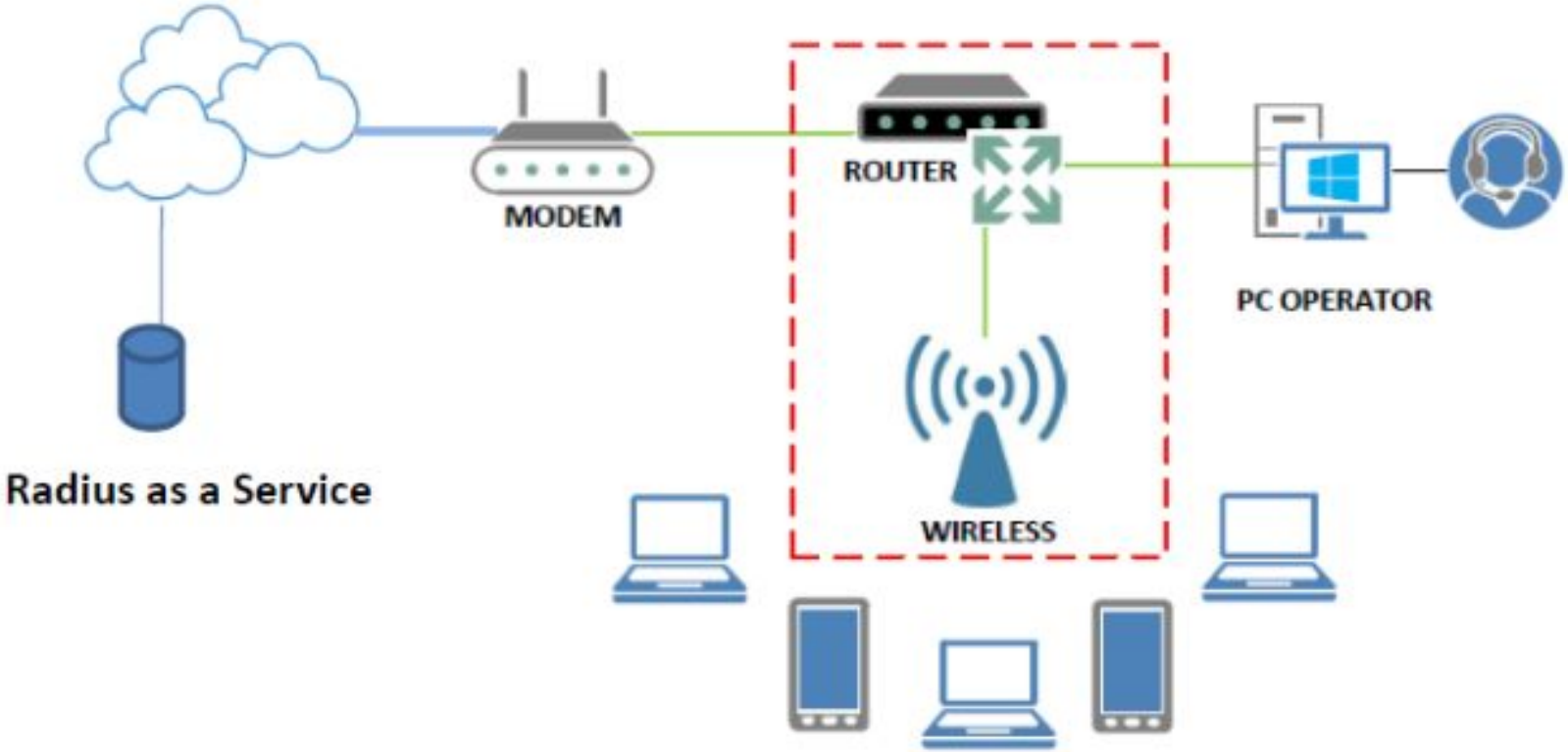
Layout Jaringan - PT CRIF



Layout jaringan - PT VALE



Layout Jaringan - Balaikota DKI



Layout jaringan - PT FUTAMI

Learn & Growth | Internal Process | Costumer | Financial

Update IT - Internet

Pabrik Futami Food and Beverages

Head Office PT. Djarum

Intranet WAN connection Metro E dari Telkom & Icon +

Link Referensi

1. Tahun Pertama Menjadi Seorang System Administrator - Ryan Rizky Diantoro
2. How I made $31500 by submitting a bug to Facebook
3. Privilege Escalation by Changing HTTP Response (Admin Access)
4. https://medium.com/bugbountywriteup
5. https://medium.com/@danangtriatmaja
6. https://portswigger.net/web-security
7. Kuliah Online Onno W. Purbo
8. Trend Micro Security Day
9. Cyber Security Unpas
10. Cyber Security Unpas
11. Defenxor
12. Automate your Security Operations Center (SOC) with Ansible
13. Nolsatu.id
14. http://s.id/rhcadwebinar
15. https://fadhilthomas.github.io/portfolio/
16. https://github.com/tokopedia/Bug-Bounty

Terimakasih