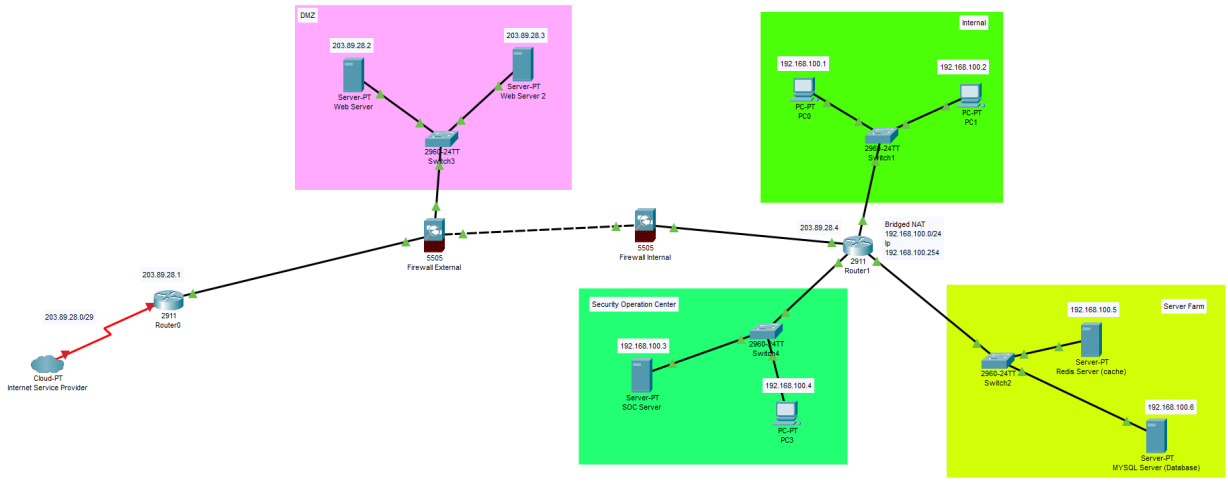
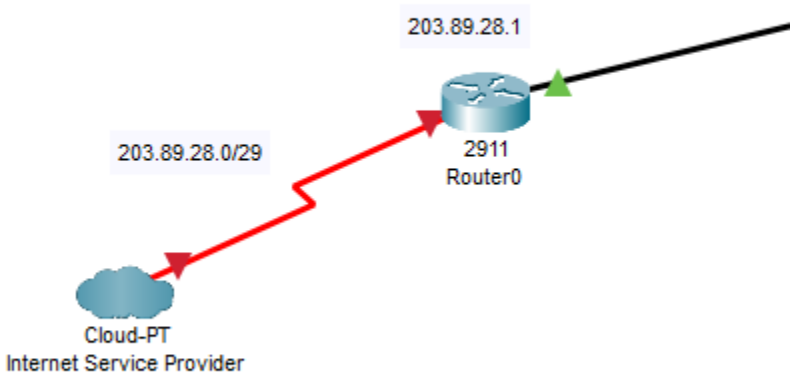
Secure Network Topology Design SMK Negeri 7 Semarang

Muhammad Zaky Adzkiya
Rafi Nur Ardiansyah

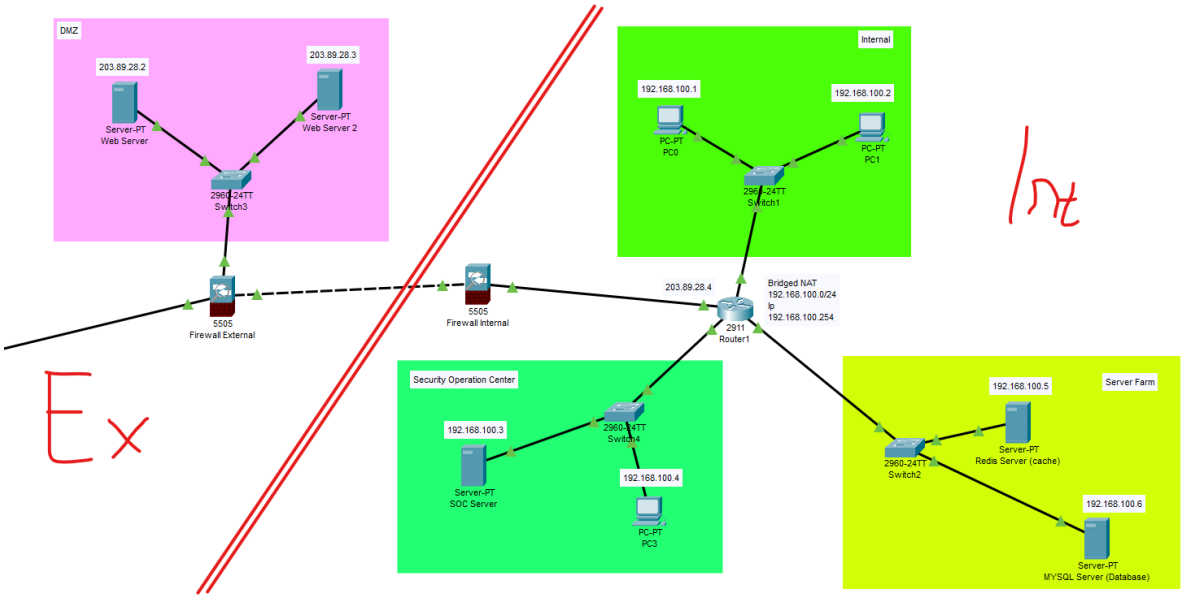


Topologi

Untuk Keseluruhan topologi jaringan dapat dilihat pada gambar diatas. Skenario penggunaan topologi tersebut adalah untuk Perusahaan Teknologi yang memiliki banyak aplikasi yang berjalan pada publik.

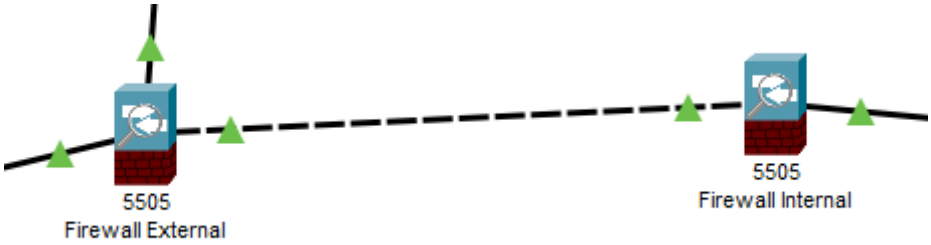


Pada gambar tersebut terlihat **Router 0**, router tersebut terdapat pada bagian terluar dan berhubungan langsung dengan ISP. Router tersebut berfungsi sebagai gateway untuk aplikasi yang berjalan di belakangnya.

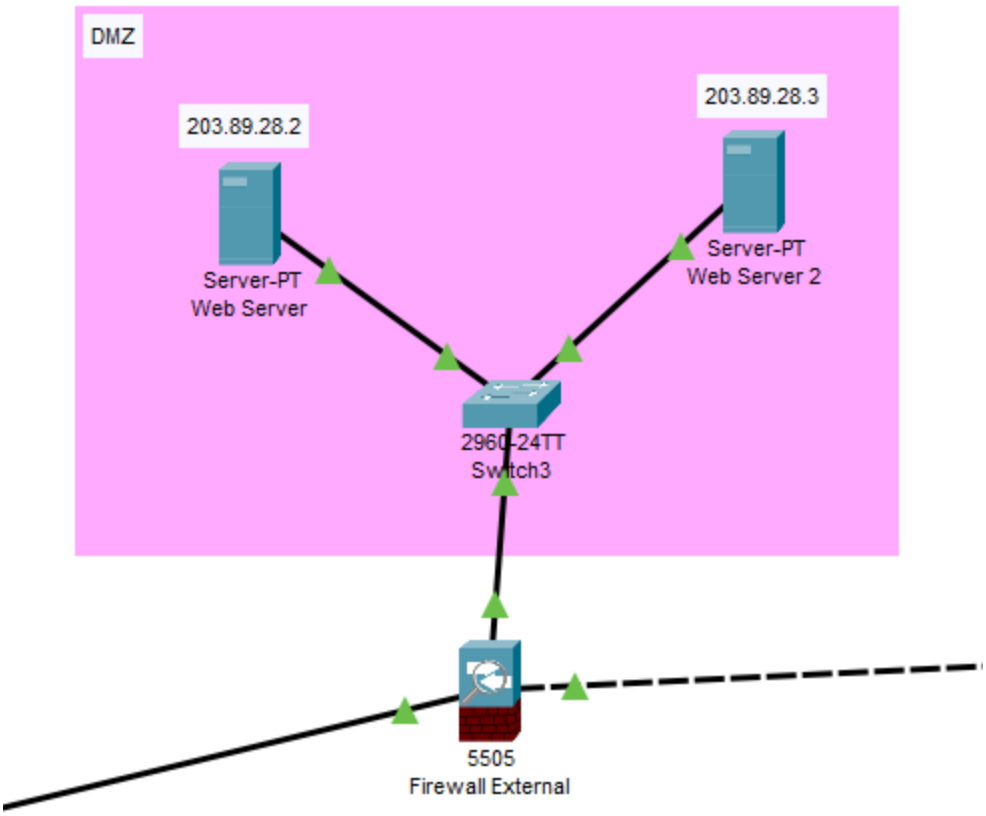


Selanjutnya adalah aplikasi yang ada di belakang router. Terlihat pada gambar, untuk aplikasi telah diklasifikasikan menjadi 2 kubu. Untuk yang berwarna hijau kekuningan menandakan bahwa aplikasi tersebut berjalan pada jaringan internal. Lalu untuk yang berwarna merah muda, aplikasi tersebut berada pada jaringan external.

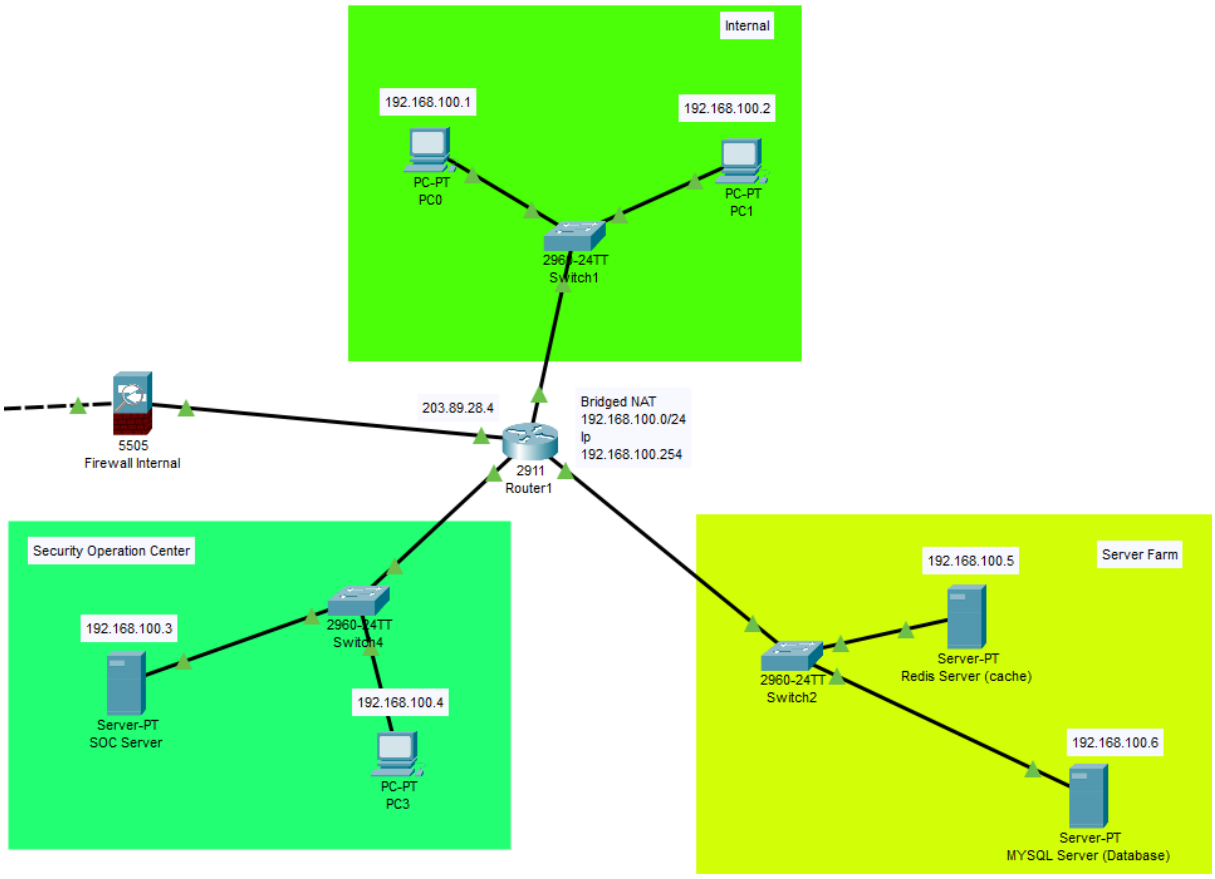
Alasan dibalik klasifikasi ini adalah, untuk aplikasi external adalah aplikasi yang bisa di akses oleh publik (dalam kasus ini web server). Karena bisa diakses oleh publik, maka aplikasi tersebut menjadi rentan karena bisa di serang. Lalu, jika penyerang berhasil ,maka sistem/aplikasi yang lain akan mudah terserang. Sedangkan aplikasi yang termasuk dalam aplikasi internal adalah aplikasi yang bersifat rahasia dan tidak untuk publik ,contoh: database.



Topologi ini memiliki 2 firewall, kita sebut saja firewall internal dan eksternal. Alasan di balik penggunaan 2 firewall adalah untuk menambahkan keamanan extra. Fungsi kedua firewall ini juga berbeda. Firewall external berfungsi untuk melindungi DMZ Karena DMZ terletak di luar firewall serta untuk memberikan keamanan tambahan untuk aplikasi internal. Sedangkan fungsi firewall internal adalah untuk mengamankan aplikasi internal yang ada di belakangnya.

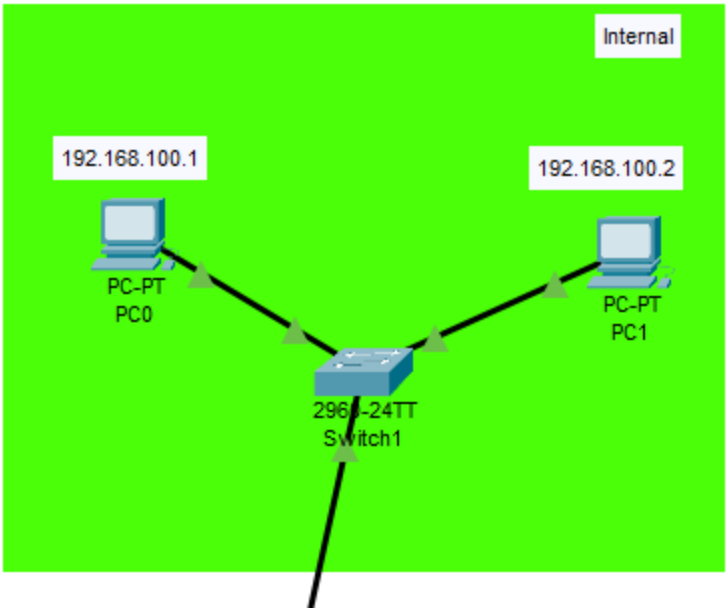


Bagian external topologi ini hanya diisi oleh DMZ. DMZ merupakan singkatan dari **Demilitarized Zone** yang berfungsi untuk mencegah terjadinya serangan pada aplikasi internal yang bersifat rahasia. DMZ ini terletak di luar firewall internal. Pada DMZ ini terdapat 2 web Server yang sudah terkonfigurasi dengan load balancer.

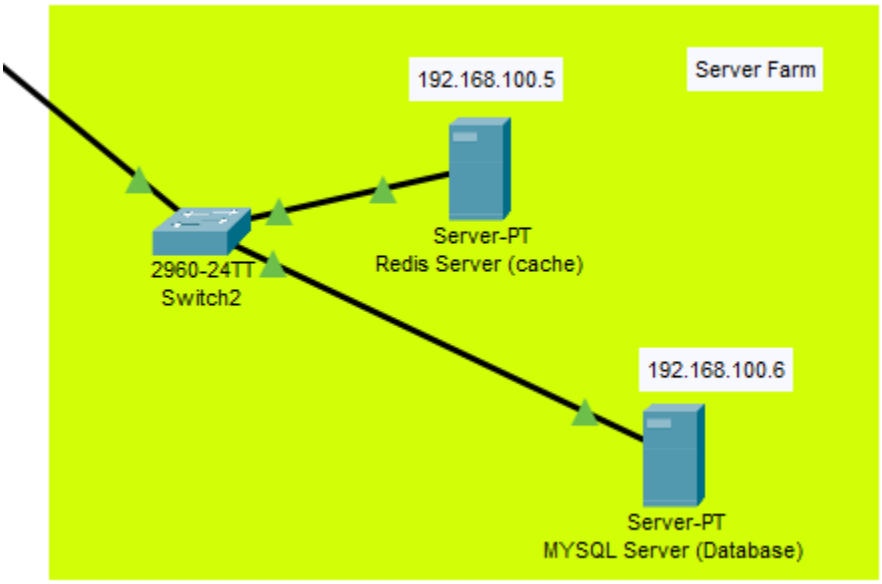


Pada bagian internal dalam topologi ini terdapat router yang mentranslasikan ip menjadi ip lokal atau biasa kita sebut sebagai NAT. Seluruh port yang tersambung pada tiap switch tiap zona sudah ter bridge sehingga antar zona bisa berkomunikasi.

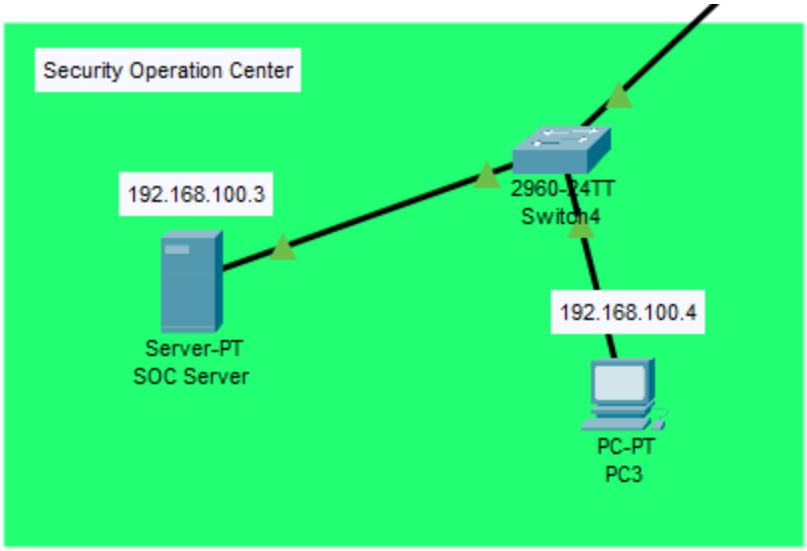
Topologi bagian internal dibagi menjadi 3 zona untuk memudahkan dalam membaca topologi serta untuk mengatur konfigurasi ACL.



Di zona ini adalah tempat dimana system administrator bekerja. Hanya terdapat PC dengan konfigurasi ip static disini.



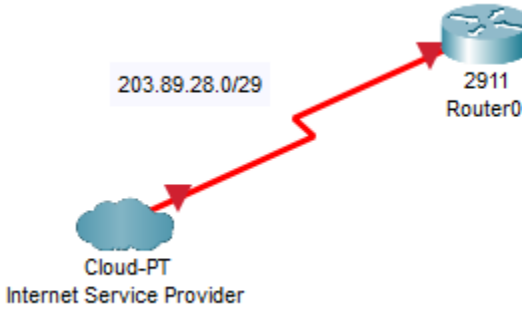
Selanjutnya di zona Server Farm terdapat 2 buah server yaitu MYSQL Server sebagai database dan Redis Server.



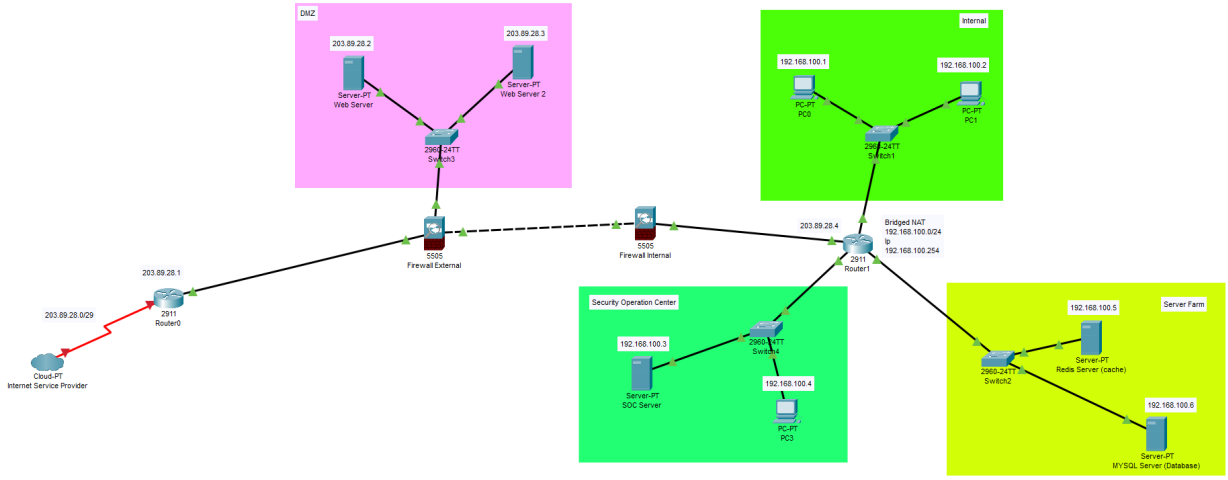
Pada Security Operation Center terdapat server maupun pc yang mencatat seluruh aktivitas pada jaringan. Sehingga memudahkan security analyst jika terjadi penyerangan pada ekosistem.

IP Addressing

Topologi ini menggunakan IP Public static dengan range **203.89.28.0/29**. Dengan range ini, maka terdapat 6 ip public yang bisa digunakan yaitu 203.89.28.1 - 203.89.28.6.



IP yang public digunakan pada topologi ini adalah sebagai berikut



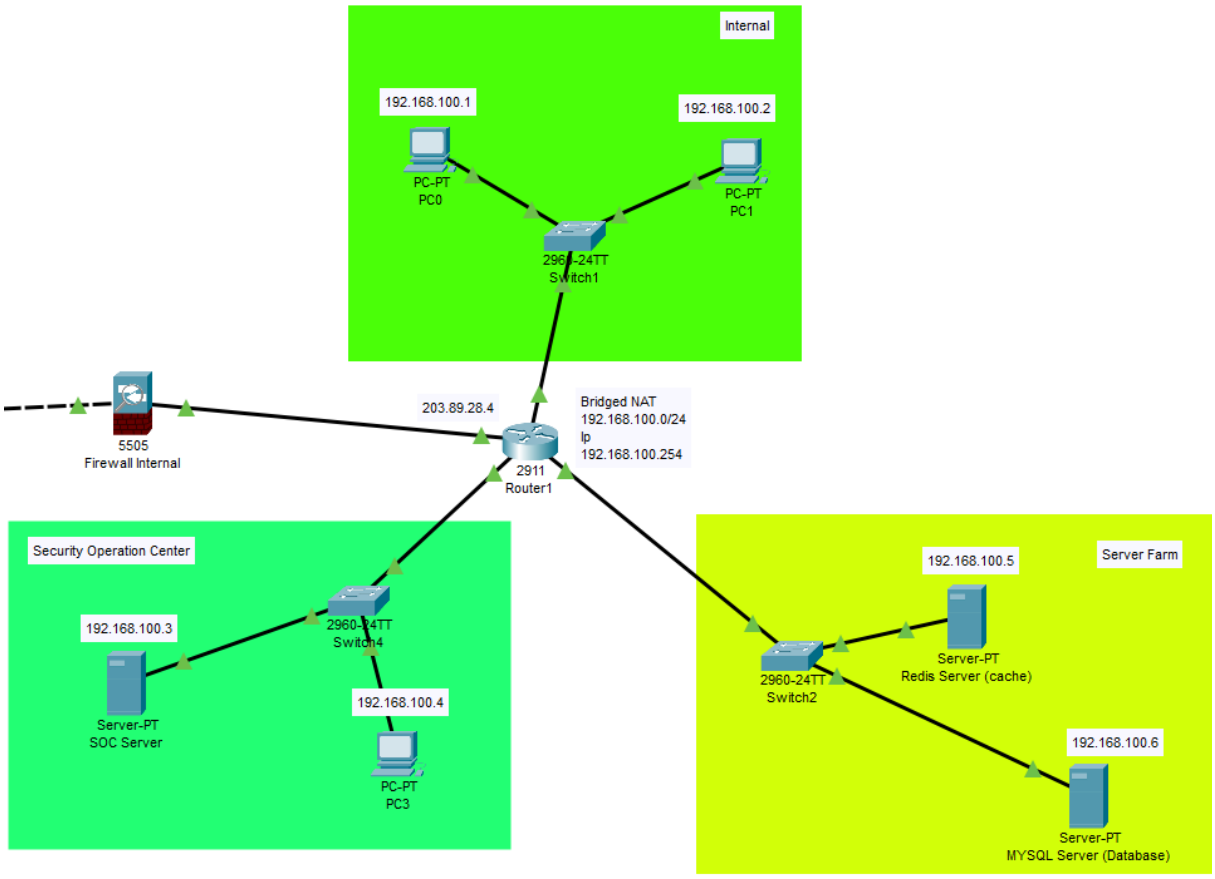
203.89.28.1 sebagai Router 0
203.89.28.2 sebagai Web Server
203.89.28.3 sebagai Web Server 2
203.89.28.4 sebagai Router 1

IP 203.89.28.1 adalah sebagai gateway yang sudah saya jelaskan tadi, sedangkan IP 203.89.28.2 dan 203.89.28.3 adalah sebagai web server. Load balancer di sana berfungsi untuk mengantisipasi request yang berlebih pada server, sehingga performa web akan jauh lebih baik. Untuk IP 203.89.28.4 digunakan sebagai IP Router 1.

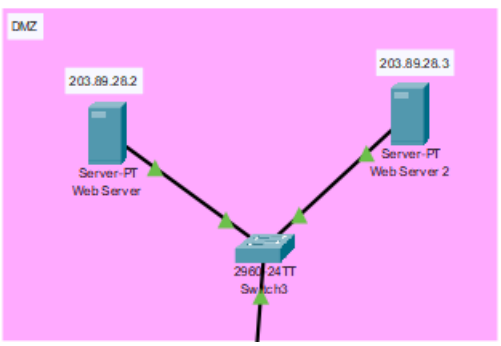
Pada Router 1, IP ditranslasikan menjadi IP lokal dan di bridge sehingga semua zona bisa saling interaksi. Untuk interaksi para host tidak bisa seenaknya mengakses ip lain karena telah diatur oleh ACL pada router. Seluruh IP pada Topologi, telah diatur secara statik sehingga memudahkan untuk konfigurasi akses.

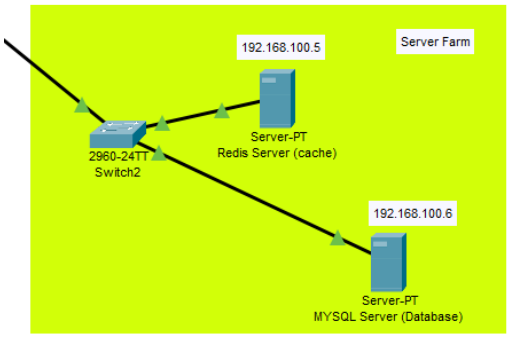
Access Control List

ACL (Access Control List) adalah metode menyeleksi traffic terhadap packet data yang akan dikirimkan pada alamat yang dituju. Secara sederhana ACL dapat diilustrasikan sebagai gerbang keamanan, dan bagi packet yang memiliki kriteria yang sesuai pada dengan aturan yang ditetapkan, maka packet tersebut diizinkan. Namun untuk packet yang tidak memenuhi kriteria, maka packet tersebut akan ditolak. ACL dapat berisi IP Address, MAC Address, subnet, dan port yang diperbolehkan ataupun ditolak untuk melewati jaringan

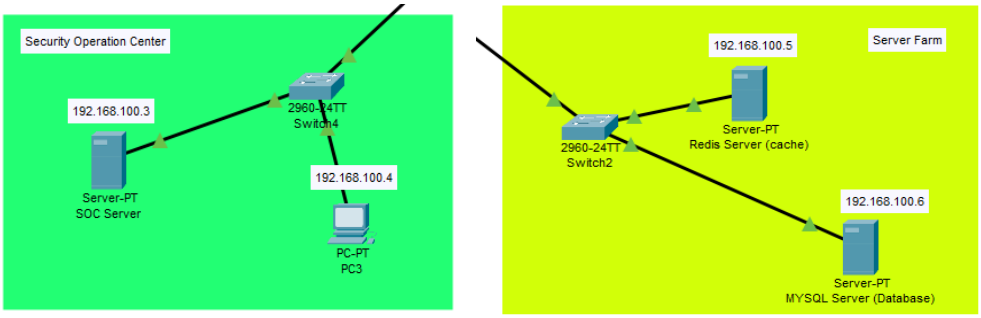


Untuk ACL rule pada topology kali ini, area DMZ, INTERNAL, dan SOC dapat mengakses area SERVER FARM. Namun area SERVER FARM tidak dapat diakses secara public karena akan berdampak pada kerentanan server-server yang ada pada SERVER FARM. Sebagai contoh, database server yang terdapat pada area SERVER FARM tidak boleh diberikan akses dari luar karena jika dapat diakses dari luar, maka Attacker akan mendapatkan akses database itu sendiri dan berakibat sebagai kebocoran data. Setelahnya akan mendapatkan akses pada jaringan internal lain





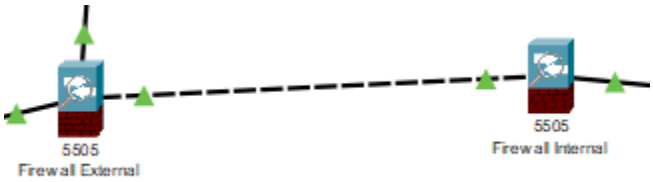
Skenarionya yaitu area DMZ akan diizinkan untuk mengakses area SERVER FARM oleh ACL menggunakan network internal. Untuk memantau pada SERVER FARM bisa menggunakan area INTERNAL yang juga diizinkan mengakses oleh ACL.



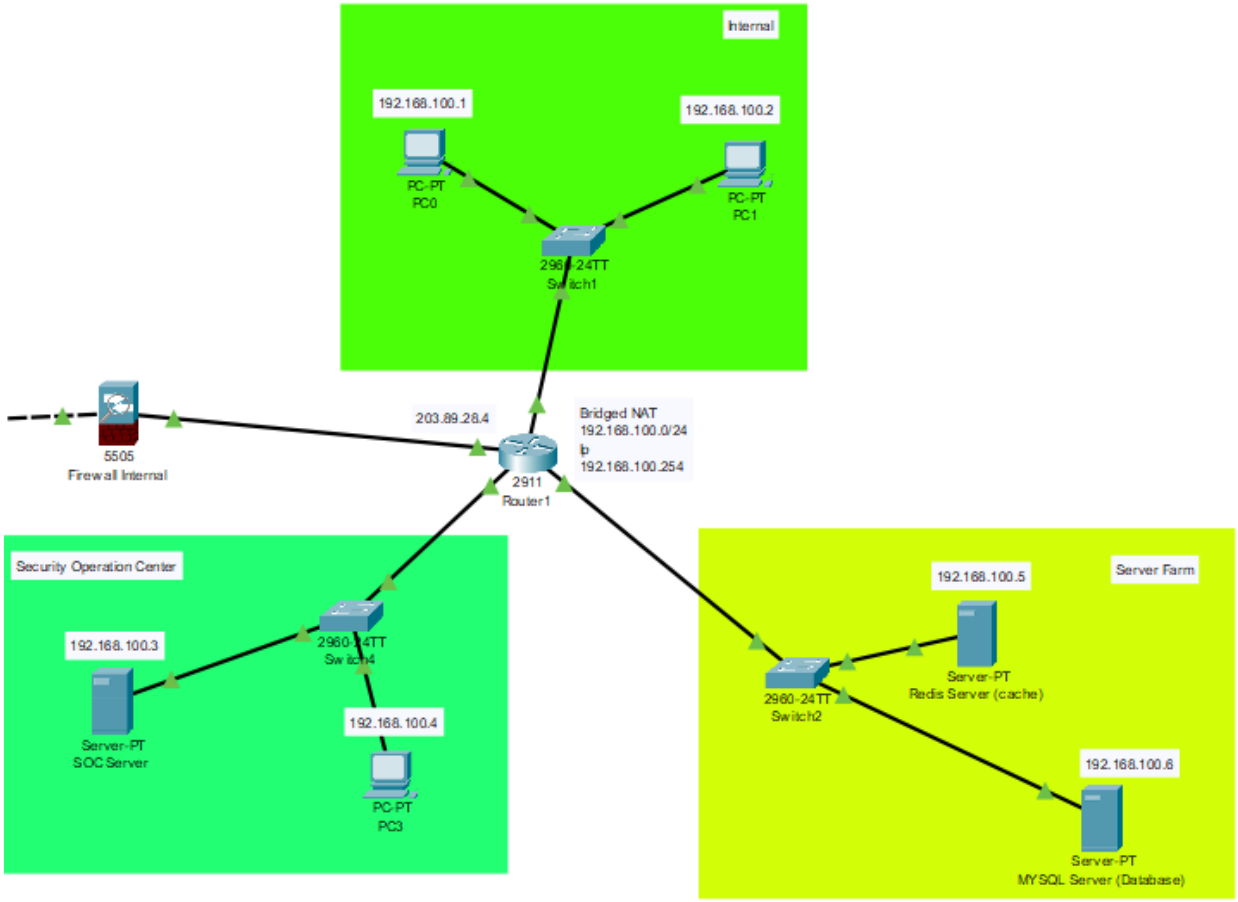
Pada area SOC juga dapat melakukan pemantauan pada catatan log agar bisa membantu menemukan aksi jika sebelumnya mengalami kebocoran data

Menggunakan fitur authorization seperti administrator dan user. Untuk setiap user dilarang untuk memasuki SERVER FARM karena tidak memiliki perizinan khusus. Hanya administrator yang boleh memasuki dan memonitor pada SERVER FARM

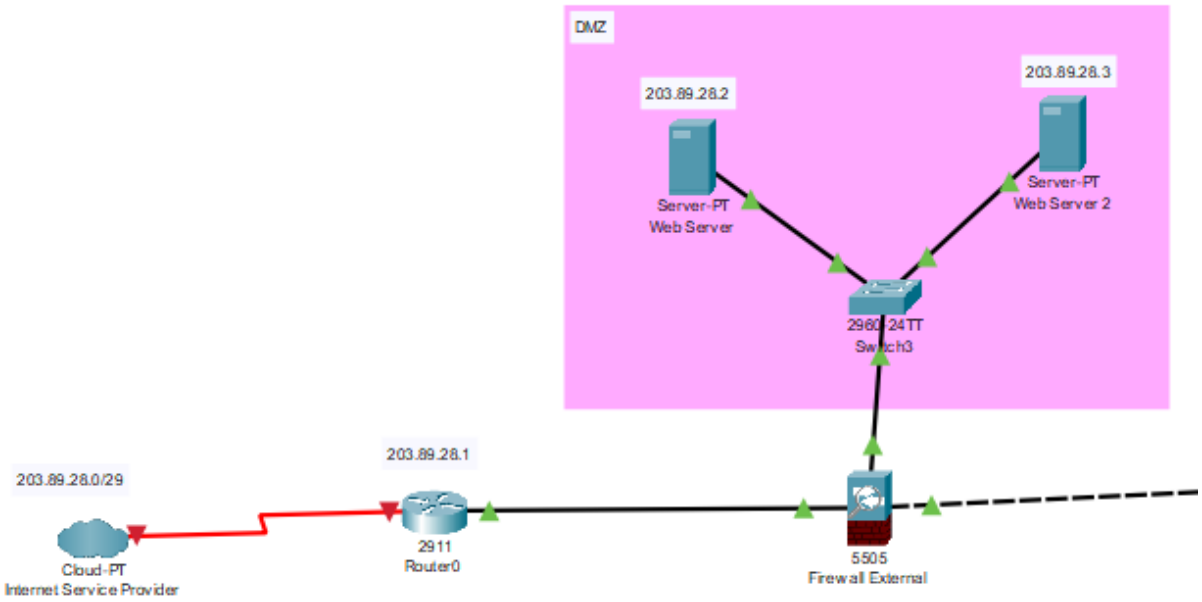
Network Policy Configuration



Pemasangan firewall pada internal network dapat mengatur lalu lintas dari network. Pada area DMZ dikonfigurasikan firewall external sebagai jembatan antara jaringan luar dengan area DMZ karena jika tanpa firewall maka, packet-packet yang masuk tidak dapat di filter sempurna yang menyebabkan server terbanjiri traffic yang disebabkan oleh jaringan luar. Jika terpasang firewall kita dapat memantau, memberi izin, dan memblokir lalu lintas tertentu berdasarkan konfigurasi yang kita inginkan.



Pada firewall internal berfungsi untuk menyortir keluar masuknya traffic internal pada area SOC, INTERNAL, dan SERVER FARM. Area DMZ jika ingin berhubungan dengan salah satu dari ketiga area tersebut harus melalui firewall internal. Jika tanpa diberikan firewall internal, maka lalu lintas network akan kacau karena tidak diberlakukanya penyeleksian sesuai aturan yang dikonfigurasikan.



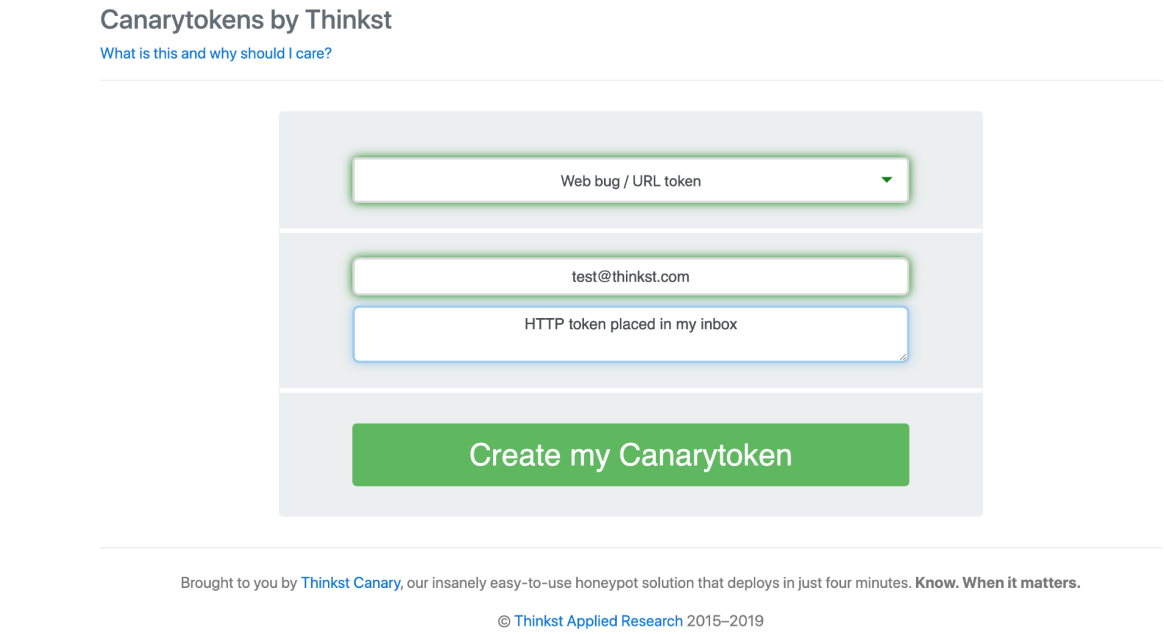
Untuk firewall external kita bisa lakukan penyortiran untuk ip yang boleh dan tidak boleh masuk pada area tertentu. Sebagai contoh, jaringan luar yang diduga melakukan ddos dapat dicegah dengan cara blacklist pada ip tertentu atau pun dengan whitelist ip yang mungkin dapat dipercaya. Dengan memanfaatkan firewall tersebut pada topology jaringan kita, dapat meminimalisir adanya serangan dari hacker karena ip yang mencurigakan akan langsung di drop oleh firewall.

Security Tools Implementation

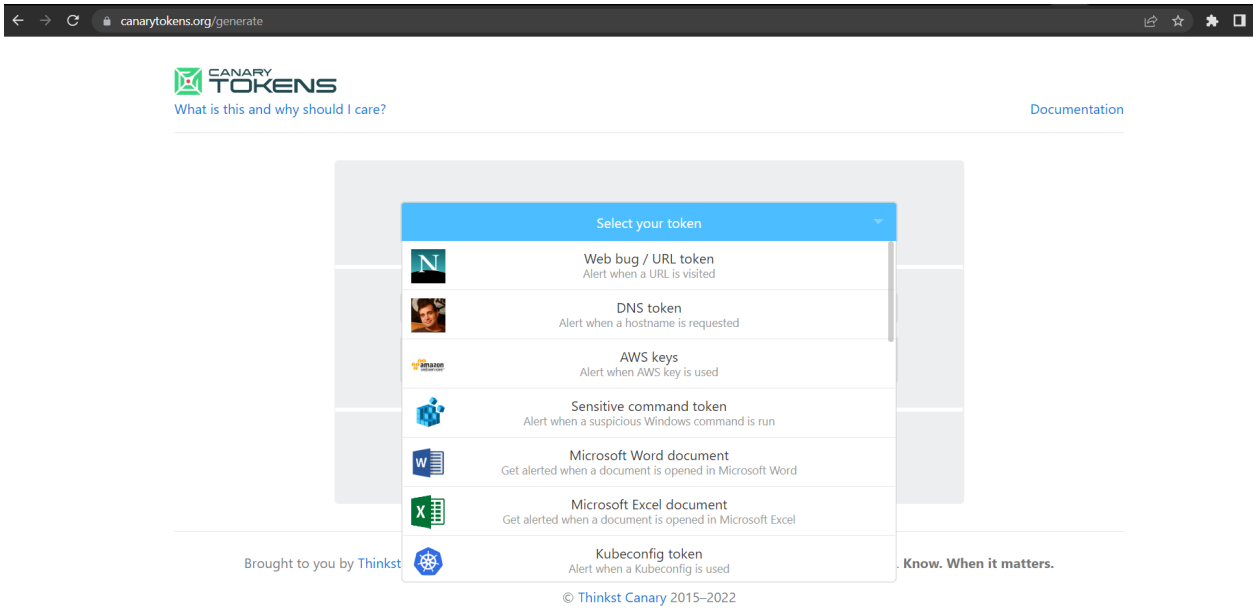
Security Tools akan di pasang pada area SOC untuk mencegah, memantau, dan mendeteksi kegiatan mencurigakan pada semua server yang berdampak buruk pada sisi internal network.

- Canary Token

CANARY TOKENS



Kita dapat menggunakan service canary token untuk mendapatkan email jika terjadi kegiatan anomali / mencurigakan dari sisi server kita. Sebagai contoh, server kita sedang disusupi oleh hacker. Hacker tersebut ingin mengakses database kita yang berisi ingformasi penting dari vendor,customer dll. Ketika hacker tersebut mengetik perintah yang dapat mentrigger canary token, maka seketika muncul pesan di email kita jika terdapat penyusup pada database. Canary tokens dapat digunakan pada banyak service, seperti database, DNS, AWS Key, Kubeconfig token, file executable dll.



Canary token bisa kita tempatkan pada area SERVER FARM dan DMZ karena dari DMZ lah koneksi dari luar berasal, untuk mencegah adanya penyusupan pada web server kita

- Splunk

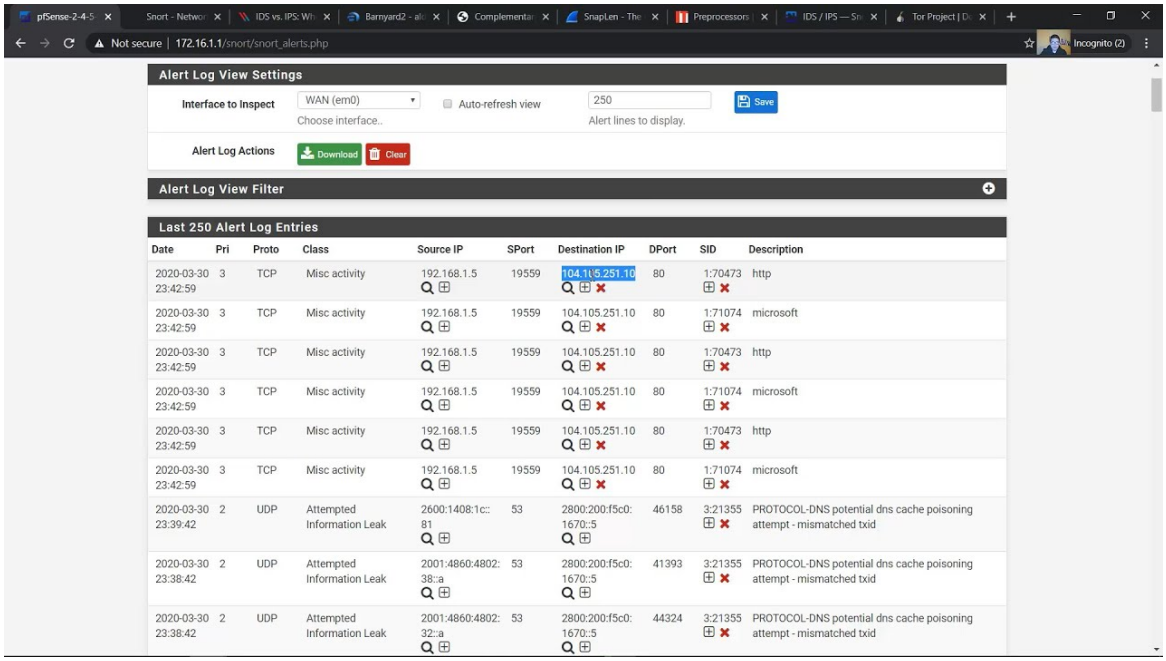
Aplikasi ini sebagai software keamanan untuk memantau network traffic. Splunk digunakan untuk melakukan analisis jaringan secara real-time dan menyimpan history untuk data ancaman. Splunk mudah digunakan karena tersedia berbagai alat bantu untuk mencari data, report, dan alert dengan dipadukan oleh graphic real time.

Splunk kita pasang pada area SOC karena dapat dengan mudah memantau semua traffic network semisal terjadi kegiata yang mencurigakan

- Snort

Snort adalah Open source network security yang digunakan untuk memindai network dan mencegah adanya intrusion pada network kita. Pada topology kali ini kita bisa menggunakan snort untuk menganalisa network traffic yang

menemukan tanda-tanda dari percobaan intrusion oleh penyerang. Aplikasi ini dapat memberikan peringatan kepada user saat penyerang melakukan intrusion dan mencegah dengan cara mem-block traffic mencurigakan tersebut secara bersamaan.



Alert Log View Settings

Interface to Inspect: WAN (em0) — Choose interface..

☐ Auto-refresh view

250 — Alert lines to display.

Alert Log Actions

Alert Log View Filter

Last 250 Alert Log Entries

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2020-03-30 23:42:59	3	TCP	Misc activity	192.168.1.5	19559	104.105.251.10	80	1:70473	http
2020-03-30 23:42:59	3	TCP	Misc activity	192.168.1.5	19559	104.105.251.10	80	1:71074	microsoft
2020-03-30 23:42:59	3	TCP	Misc activity	192.168.1.5	19559	104.105.251.10	80	1:70473	http
2020-03-30 23:42:59	3	TCP	Misc activity	192.168.1.5	19559	104.105.251.10	80	1:71074	microsoft
2020-03-30 23:42:59	3	TCP	Misc activity	192.168.1.5	19559	104.105.251.10	80	1:70473	http
2020-03-30 23:42:59	3	TCP	Misc activity	192.168.1.5	19559	104.105.251.10	80	1:71074	microsoft
2020-03-30 23:39:42	2	UDP	Attempted Information Leak	2600:1408:1c::81	53	2800:200:f5c0:1670::5	46158	3:21355	PROTOCOL-DNS potential dns cache poisoning attempt - mismatched txid
2020-03-30 23:38:42	2	UDP	Attempted Information Leak	2001:4860:4802:38::a	53	2800:200:f5c0:1670::5	41393	3:21355	PROTOCOL-DNS potential dns cache poisoning attempt - mismatched txid
2020-03-30 23:38:42	2	UDP	Attempted Information Leak	2001:4860:4802:32::a	53	2800:200:f5c0:1670::5	44324	3:21355	PROTOCOL-DNS potential dns cache poisoning attempt - mismatched txid

- Nagios

Sama halnya seperti Splunk, nagios adalah tools yang digunakan untuk memonitoring network secara real-time. Nagios dapat memonitoring berbagai protocol seperti ICMP,POP3,SMTP,HTTP secara menyuluruh.

Nagios dapat kita pasang pada bagian area SOC ataupun INTERNAL karena kita dapat secara real-time memonitoring network internal.

Hardening

Untuk seluruh server pada topologi ini telah dilakukan hardening pada sisi Platform, Maupun Credential

Platform Hardening meliputi:

Update Kernel dan Kernel Module Signing

Dengan cara membuat (mengcompile) dan dan sign kernel sendiri maka akan jauh lebih aman karena tidak sembarang module bisa terinsert pada kernel. Berikut adalah genkey yang saya buat untuk sign kernel click here . Setelah membuat genkey, bisa langsung di generate key nya menggunakan openssl di linux.

Kernel Module Loading Enforcement

Ini digunakan untuk membatasi agar tidak ada modul baru yang masuk

SSH Attack Surface Reductions

Konfigurasi berikut ini berfungsi untuk mereduksi serangan dari ssh

PermitRootLogin no
ClientAliveInterval 900
PasswordAuthentication no

AppArmor

App armor digunakan untuk membatasi aplikasi untuk bertindak seenaknya pada server. Aplikasi ini bersifat mandatory sehingga root user pun harus patuh kepada apparmor. Untuk instalasi bisa menggunakan **apt install apparmor apparmor-utils.**

Configure Iptables to Enforce Local Firewall Rules

Untuk IPtable agar lebih aman maka semua port akan di tutup kecuali port pada service yang berjalan. Konfigurasi ip table akan disesuaikan dengan service yang berjalan pada server. Berikut adalah contoh konfigurasi IPtables

```
# drop all port
Iptables -P INPUT DROP
Iptables -P FORWARD DROP
Iptables -P OUTPUT DROP

# allow ssh
Iptables -I INPUT -p tcp -dport 22 -s 0.0.0.0/0 -i enp0s3 -j ACCEPT
Iptables -I OUTPUT -p tcp -dport 22 -s 0.0.0.0/0 -i enp0s3 -j ACCEPT

# allow to download package from apt
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp --dport 53 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Disable Unnecessary Services

Selain untuk meringankan beban server, kita juga lebih tau apa saja yang berjalan pada server serta untuk memastikan bahwa service pada server berjalan sesuai yang diharapkan.

Credential Hardening

Root Account Hardening

Pasang password yang sukar untuk akun root, dengan menggunakan Minimal panjang 8 karakter, penggunaan simbol, serta huruf besar.

Identify and Protect Privileged Accounts

check yang punya uid 0
cat /etc/passwd | awk -F: '($3 == 0) { print $1 }'

```
root@server:/home/ubuntu# cat /etc/passwd | awk -F: '($3 == 0) { print $1 }'
root
penjahat
root@server:/home/ubuntu#
```

check yang punya akses sudo
cat /etc/group | awk -F: '($1 == "sudo")'

Strong Password Enforcement

# install libpam
sudo apt install libpam-cracklib

Konfigurasi pada **/etc/pam.d/common-password**
• retry=3 : Prompts user at most 1 time before returning with error.
• minlen=8 : The minimum acceptable size for the new password.
• ucredit=-1 : The password must contain at least 1 uppercase characters.
• dcredit=-1 : The new password must contain at least 1 digits.
• ocredit=-1 : The new password must contain at least 1 symbols.

pam_cracklib.so retry=3 minlen=8 ucredit=-1 dcredit=-1 ocredit=-1

```
# here are the per-package modules (the "Primary" block)
password        requisite                       pam_cracklib.so retry=3 minlen=8 ucredit=-1 dcredit=-1 ocredit=-1
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass sha512
# here's the fallback if no module succeeds
```

Auditing and Visibility

System Auditing Configurations

Administrator harus mereview konfigurasi linux yang tersedia pada linux auditing system (AuditD) dan memastikan bahwa suatu insiden tercatat untuk di review dan dianalisa.

Linux Auditing System (Auditd)
apt install auditd