IMPLEMENTASI DOUBLE DEEP PACKET INTRUSION DETECTION DAN PREVENTION SYSTEM (IDPS) INSPECTION DENGAN PERANGKAT FIREWALL NGFW DAN APPLICATION SECURITY MANAGER PADA CLOUD DATACENTER PT.XYZ

Anna Fitria

Universitas Gunadarma, anna_fitria@staff.gunadarma.ac.id

ABSTRAK

Pada era revolusi informasi yang berkembang dengan cepat, teknologi komputasi berbasis internet menjadi sangat dibutuhkan karena kemudahannya. Hal ini menyebabkan ketergantungan bisnis akan Teknologi Infomasi semakin tinggi dan hal ini sejalan dengan ancaman serangan siber yang semakin meningkat. PT. XYZ sebagai perusahaan di bidang jasa penyedia cloud datacenter yang dapat dikategorikan critical infrastructure. Critical infrastructure memiliki komponen yang didefinisikan sebagai sistem dan aset, baik virtual maupun physical. Komponen kritikal virtual yang berfungsi dalam menjaga keberlangsungan bisnis PT. XYZ adalah Sistem dan Teknologi Informasi, Sehingga diperlukan cyber resiliency yang dapat menjamin ketersediaan (availability) dan integritas (integrity) data dan layanan digital. Selain hal tersebut diatas, untuk menjaga ketersediaan layanan IT diperlukan juga pengadaan environment server yang berbasis virtualisasi pada Data Center (DC). Pengembangan dan peningkatan sistem ini sangat diperlukan mengingat pada saat ini belum tersedianya perangkat server yang berbasis virtualisasi cloud pada Data Center.

Kata kunci: Critical infrastucture, Cyber Resiliency, Cyber Security, virtualisasi cloud pada Data Center

PENDAHULUAN

Ancaman cyber dapat berpontensi merugikan PT. XZY secara finansial maupun non-finansial yang diharapkan menciptakan sistem infrastruktur yang kokoh dalam menjaga sumber data setiap konsumen perorangan maupun skala B2B (*Bussiness to Bussiness*). Disamping menjaga keamanan data untuk mencitapkan daya yang memiliki integritas (*integrity*), PT. XYZ juga harus dapat menyediakan pelayanan sistem maupun aplikasi yang dapat diakses secara 24 jam selama 365 hari dengan minimum downtime yang memenuhi SLA (*Service Level Aggrement*) dengan hal ini PT.XYZ mendukung yang dapat menjadi ketersediaan (*availability*) dengan memiliki konsep segmentasi HA (*High Availability*) Data Center.

Kebutuhan setiap manusia di era digitalisasi sangatlah tinggi dan menjadi tantangan bagi setiap bisnis yang mengandalkan interkoneksi publik agar menciptakan kepercayaan dalam mengunakan Solusi Sistem Informasi yang dapat diandalkan.

Bisnis digital dipaksa berlomba berinventasi akan sistem Teknologi Informasi yang terbaru untuk dapat melayani tingginya terhadap akses data digital mulai dari penggunaan perangkat keamanan jaringan seperti *Next Generation Firewall* dan *Application Security Manager.* Menurut Sanders (2011) Keamanan jaringan komputer *(computernetwork security)* sebuah inti saat membangun sebuah infrastruktur jaringan. Kebanyakan arsitektur jaringan menggunakan router dengan system *firewall* yang terintegrasi *(built-in integrated firewall)*, juga dukungan *software*

jaringan yang dapat kemudahan akses kontrol, data packet monitoring dan penggunaan protocol yang diatur secara ketat.

METODE PENELITIAN

Analisis Model dan Infrasturktur

Dalam memenuhi kerangka permasalah maka dilakukan analisis kebutuhan dan spesifikasi (*requirement analysis and requirement specification*) terhadap masalah yang sedang dalam pembahasan. Identifikasi kebutuhan maupun batasan yang menjadi kelemahan pada sistem terdahulu dalam mendeteksi maupun pencegahan penyerangan kepada sumber informasi yang berada didalam Data Center sehingga mengurangi nilai integritas dari sebuah sumber informasi, dalam tahap ini diharapkan memberikan solusi untuk mengurangi resiko-resiko bisnis.Tahapan Analisis ini melakukan untuk membentuk sistem yang diharapkan kokoh dengan melakukan inspeksi paket dua lapis (*double deep packet inspection)* terhadap seluruh lalulintas jaringan menuju sumber informasi.

Desain dan Perancangan Sistem

Perancangan sistem ini dilakukan berdasarkan hasil assesment terhadap sistem yang sedang berjalan dan melakukan identifikasi masalahnya. Sistem akan dilakukan peningkatan dari aspek menjaga keamanan data dengan itu diberikan penggambaran arsitektur perangkat-perangkat, data flow lalu lintas data maupun penggambaran UML secara sequence dari sistem yang akan dilakukan peningkatan.

Implementasi sistem dan Evaluasi Sistem

Setelah melakukan analisis dan desain rancangan sistem yang sesuai, maka dilakukan tahap implementasi. Tahap implementasi sistem merupakan sebuah tahap pembangunan sistem yang siap digunakan.

Pengujian Fungsional Sistem

Menurut Barak (2016) pengujian sistem fungsional terhadap serangan cyber apakah masih rentan dengan melihat respon sistem keamanan yang telah ditingkatkan dengan diberikan instruksi yang diberikan dan mengungkap setiap lalu lintas data apakah masih relevan atau masuk dalam instruksi yang membahayakan terhadap sumber informasi. Pengujian dengan menggunakan tool *hacker* untuk melukan eksplotasi terhadap database sumber informasi agar dapat masuk ke dalamnya tanpa otorisasi dan pula melakukan penyisipan instruksi penyisipan kode-kode XSS (Cross Site Scripting) dengan payload terbaru.

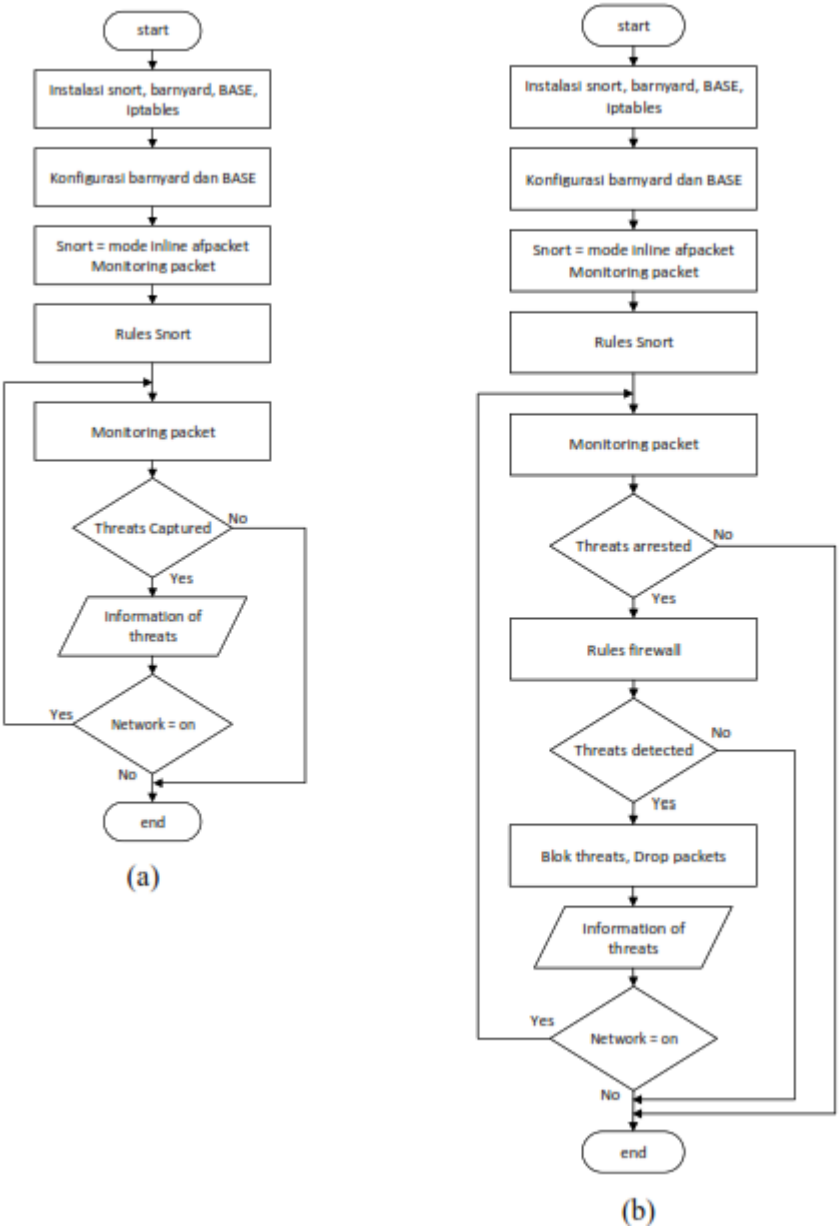
Evaluasi Sistem

Setelah proses pengujian fungsional sistem terhadap implementasi peningkatan dari sistem yang sebelumnya maka diadakan evaluasi pada sistm apakah mampu melakukan pendekteksi maupun pencegahan terhadap instruksi-instruksi yang mengancam seluruh aspek yaitu seperti integritas, kesiapan terhadap sumber informasi. Sistem juga memiliki konsep HA (*High Availibility*).

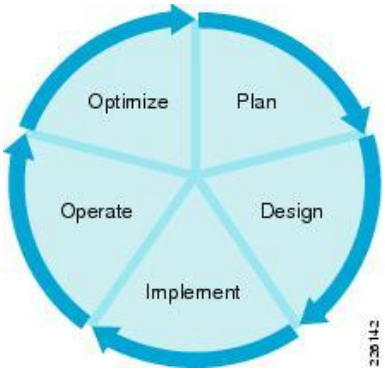
HASIL DAN PEMBAHASAN

Intrusion Detection and Prevention System

Intrusion Detection and Prevention System, atau disingkat dengan IDPS ini dapat dibagi dua, yaitu sistem yang menggunakan metode IDS dan IPS. Dapat dilihat pada flowchart dibawah.



Gambar 1 ***a) Flowchart IDS b) Flowchart IPS***



Gambar 2 ***Siklus SDLC***

Penggunaan IDS digunakan hanya untuk memantau trafik jaringan atau paket data bila terdapat intrusi, sedangkan IPS dapat digunakan untuk menghentikan atau *block threats* atau ancaman Baik IDS maupun juga IPS terdapat dua jenis deteksi ancaman yaitu host-based ataupun network-based. Menurut Bilal (2016) sistem di dalam IDPS ini memonitor lalu lintas jaringan baik yang terkoneksi lokal maupun online (internet) pada segmen jaringan atau perangkat jaringan tertentu, yang kemudian menganalisa mengenai protokol jaringan yang digunakan, untuk mengidentifikasi aktivitas yang mencurigakan. IDPS yang berbasiskan jaringan juga dapat memberikan layanan pengumpulan informasi dengan memanfaatkan database. Dalam hal ini IDPS dapat mengumpulkan informasi hasil dari monitoring host dan juga aktivitas lalu lintas trafik jaringan. Penggabungan dua metode IDS dan IPS dalam menganalisa dan mengindetifikasi aktivitas jaringan mencurigakan maka perangkat yang terpat digunakan adalah Firewall NGFW (Next Generation Firewall).

Firewall NGFW

Menurut TEC (2011). Next-generation firewall (NGFW) merupakan bagian dari suatu teknologi firewall generasi ketiga yang diimplementasikan dalam perangkat keras atau perangkat lunak. NGFW mampu mendeteksi dan memblokir serangan dengan memberlakukan kebijakan keamanan di tingkat aplikasi, port dan protocol. *Firewall* adalah suatu aturan-aturan yang mekanismenya bertujuan untuk melindungi hardware dan software. Perlindungan dapat dilakukan dengan menyaring, membatasi, atau bahkan

Perbedaan Next-generation firewall (NGFW) dengan Tradisional Firewall

Next-generation Firewall (NGFW) dan firewall tradisional mempunyai tujuan yang sama, yaitu melindungi jaringan dan aset data. Kesimpulan yang dinyatakan oleh Lammle (2013), Tujuan utama kedua tipe firewall ini melakukan penyaringan paket statis untuk memblokir paket di lalu lintas jaringan. Mereka juga memiliki kemampuan untuk menyediakan network, pentransalalian port dan inspeksi pake. Kedua firewall ini pula dapat mengatur koneksi VPN
Perbedaan yang mendasar antara firewall tradisional dan Next-generation Firewall (NGFW) yaitu, Next-generation Firewall (NGFW) memiliki fungsi inspeksi paket yang lebih mendalam yang melampaui pemeriksaan port dan protokol sederhana. Next-generation Firewall (NGFW) dapat memeriksa data yang dibawa dalam paket jaringan sedangkan firewall tradisional tidak memiliki kapabilitas ini

Menurut Warsinske (2019) perbedaan utama Next-generation Firewall (NGFW) menambahkan inspeksi tingkat aplikasi, pencegahan intrusi dan kemampuan untuk bertindak atas data yang disediakan oleh layanan intelijen ancaman (threat intelligence services). Selain itu menyimpulkan pernyataan dari Eko (2015) *Next-generation Firewall* (NGFW) memperluas fungsionalitas firewall tradisional dari NAT, PAT dan dukungan VPN untuk mengoperasikan keduanya dalam mode routed, pada bagian ini firewall berperilaku sebagai router dan mode transparan.

Pemodelan Solusi Infrastruktur

Critical infrastructure memiliki komponen yang didefinisikan sebagai sistem dan aset, baik *virtual* maupun *physical*. Komponen kritikal *virtual*

yang berfungsi dalam menjaga keberlangsungan bisnis PT. XYZ adalah Sistem dan Teknologi Informasi, sehingga diperlukan *cyber resiliency* yang dapat menjamin ketersediaan (*availability*) dan integritas (*integrity*) data dan layanan *digital*. Salah satu penunjang dalam meningkatkan data *availability* dan *integrity* terkait *cyber resiliency*.

1. Siklus dimulai dengan perencanaan, yang harus mencakup penilaian ancaman dan risiko yang bertujuan mengidentifikasi aset dan postur keamanan saat ini. Perencanaan juga harus mencakup *gap* analisis untuk mengungkap kekuatan dan kelemahan arsitektur saat ini.
2. Setelah perencanaan awal, siklus dilanjutkan dengan desain dan pemilihan platform, kemampuan, dan praktik terbaik yang diperlukan untuk menutup *gap* dan memenuhi persyaratan dimasa depan. Ini menghasilkan desain yang terperinci untuk memenuhi persyaratan bisnis dan teknis.
3. Implementasinya mengikuti desain. Ini termasuk penyebaran dan penyediaan platform dan kemampuan. Penempatan biasanya dilakukan dalam fase terpisah, yang membutuhkan urutan rencana.
4. Setelah implementasi di tempat baru perlu dipelihara dan dioperasikan. Ini termasuk manajemen dan pemantauan infrastruktur serta intelijen keamanan untuk mitigasi ancaman.
5. Terakhir, karena persyaratan bisnis dan keamanan terus berubah, penilaian berkala perlu dilakukan untuk mengidentifikasi dan mengatasi kemungkinan *gap* Informasi yang diperoleh dari operasi sehari-hari dan dari penilaian *adhoc* dapat digunakan untuk tujuan ini.

Kelemahan Sistem yang berjalan

Berikut penjelasan mengenai kelemahan terhadap sistem yang berjalan yang dijabarkan dalam beberapa point yaitu sisi keamanan, ketersediaan hingga high availability (Tabel 1).

Peningkatan sistem

Berdasarkan poin-point kelemahan sistem saat ini, maka salah satu cara untuk meningkatkan kapasitas jaringan PT.XYZ (Tabel 2).

Desain sistem

Dalam perencanaan implementasi jaringan PT.XYZ, berdasarkan dari *best practice* desain network yang umum digunakan oleh perusahaan adalah dengan system hirarki dan modular. Model desain jaringan hierarki memecah jaringan menjadi beberapa jaringan yang lebih kecil dan lebih mudah dikelola. Setiap level atau tingkatan dalam hierarki difokuskan pada serangkaian peran tertentu. Pendekatan desain ini menawarkan fleksibilitas tinggi kepada perancang jaringan untuk mengoptimalkan dan memilih perangkat keras, perangkat lunak, dan fitur jaringan yang tepat untuk melakukan peran spesifik untuk level jaringan yang berbeda.Berikut ini adalah gambar topologi High Level Design yang akan diimplementasikan di Jaringan Data Center PT. XYZ (gambar 3).

Matriks *High Level* Perangkat Datacenter PT. XYZ

Berikut adalah penjelasan kodifikasi matriks untuk *High Level Design* perangkat-perangkat datacenter PT. XYZ berdasarkan fungsi sesuai dengan Hierarki standarisasi yang telah ditentukan (Tabel 3).

Tabel 1.
Kelemahan sistem Datacenter PT. XYZ

No	Pain Point	Keterangan
1	Perangkat Security	Perangkat sekuriti saat ini hanya Firewall Layer 4, dimana secara kapasitas juga kecil karena merupakan seri kecil dari Cisco ASA series dimana sebagai sistem firewall tradisional dengan statefull.
2	Perangkat Load Balancer	Belum ada perangkat Load balancer F5 LTM dan F5 GTM
3	Sistem Backup	Tidak adanya perangkat sebagai backup sistem.

Tabel 2.
Solution untuk Improvement

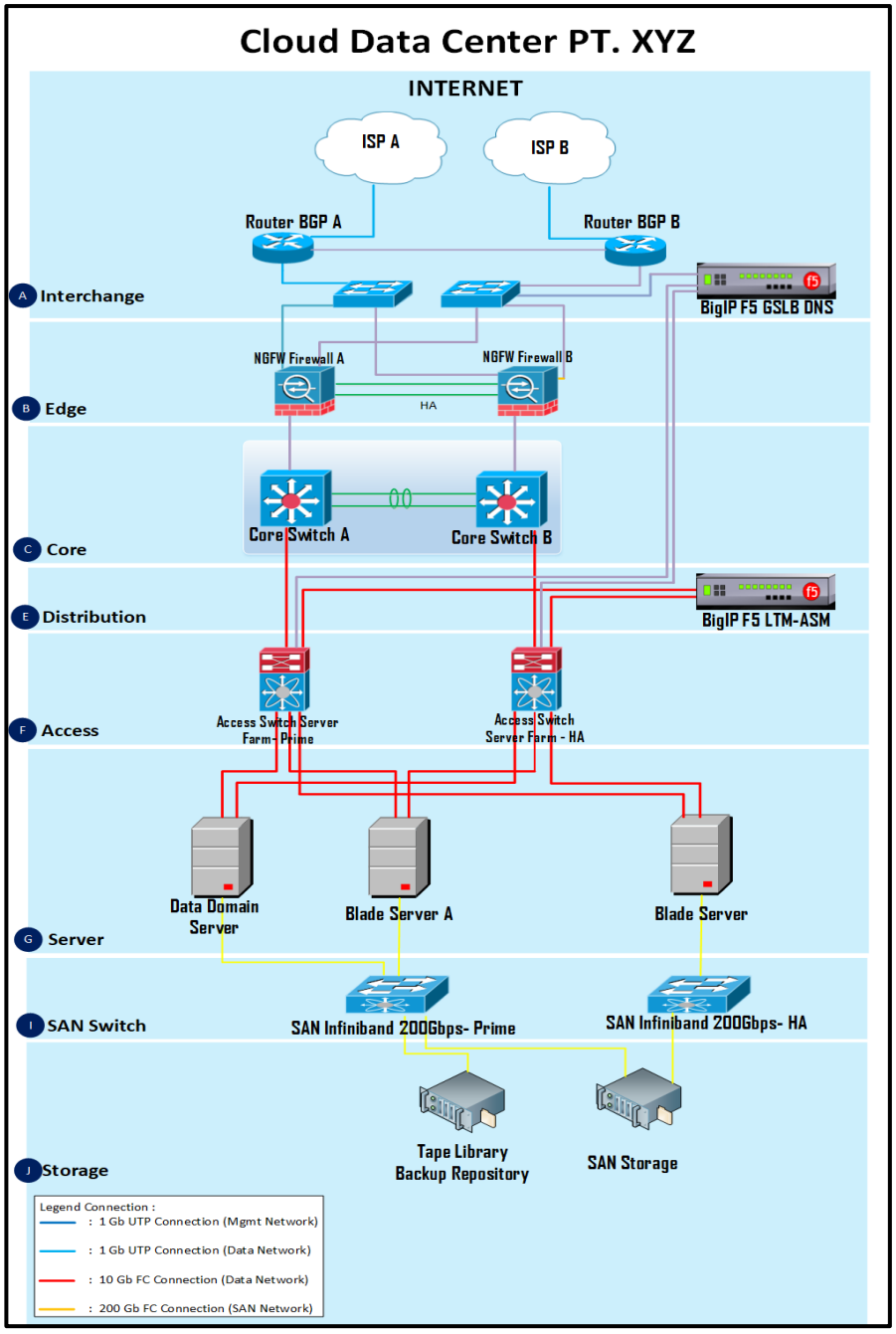
No	Improvement	Keterangan
1	Perangkat Security Layer 7	Palo Alto NGFW dengan fitur Threat Prevention
2	Perangkat Load Balancer & GTM	F5 LTM dan GTM, SSL Offload
3	Sistem Backup	Ada dua system backup, yaitu dengan : Veeam Backup – untuk proses backup Virtual Machne, berguna untuk menyimpan backup retensi 7 hari. Data Domain – pengamanan informasi dengan backup harian, mingguan dan bulanan.
4	Perangkat Security WAF	Penambahan Perangkat Big-IP F5 ASM dengan fitur mengamakan sistem lebih spesifik berdasarkan teknologi yang digunakan.

Tabel 3.
Matriks HLD Perangkat Datacenter

Level	Device Label	Device	Function
Interchange	A	Router BGP	Routing To WAN DC
		Switch Provider	Traffic spliter From/To Untrust, Branch, WAN DC
		GTM	DNS External & Internal
		Router ColloWAN 1	Routing To Branch
		Router ColloWAN 2	Routing To Branch
Edge	B	Firewall	Firewall & Gateway Server Packet Filtering & Packet Inspector Routing To Untrust

Tabel Lanjutan 3

Core	C	Switch VDC CORE	Central Routing & Switching
Management	D	Switch Management	Management Access
Distribution		LTM & ASM	Load Balancer Firewall Apps
Access	F	Switch Access	Server Farm Access Switch
Server	G	Server	Server, SAN Storage, Backup Repository & proxy
SAN Switch	I	SAN Switch	Storage Access
Storage	J	SAN Storage	Data Storage

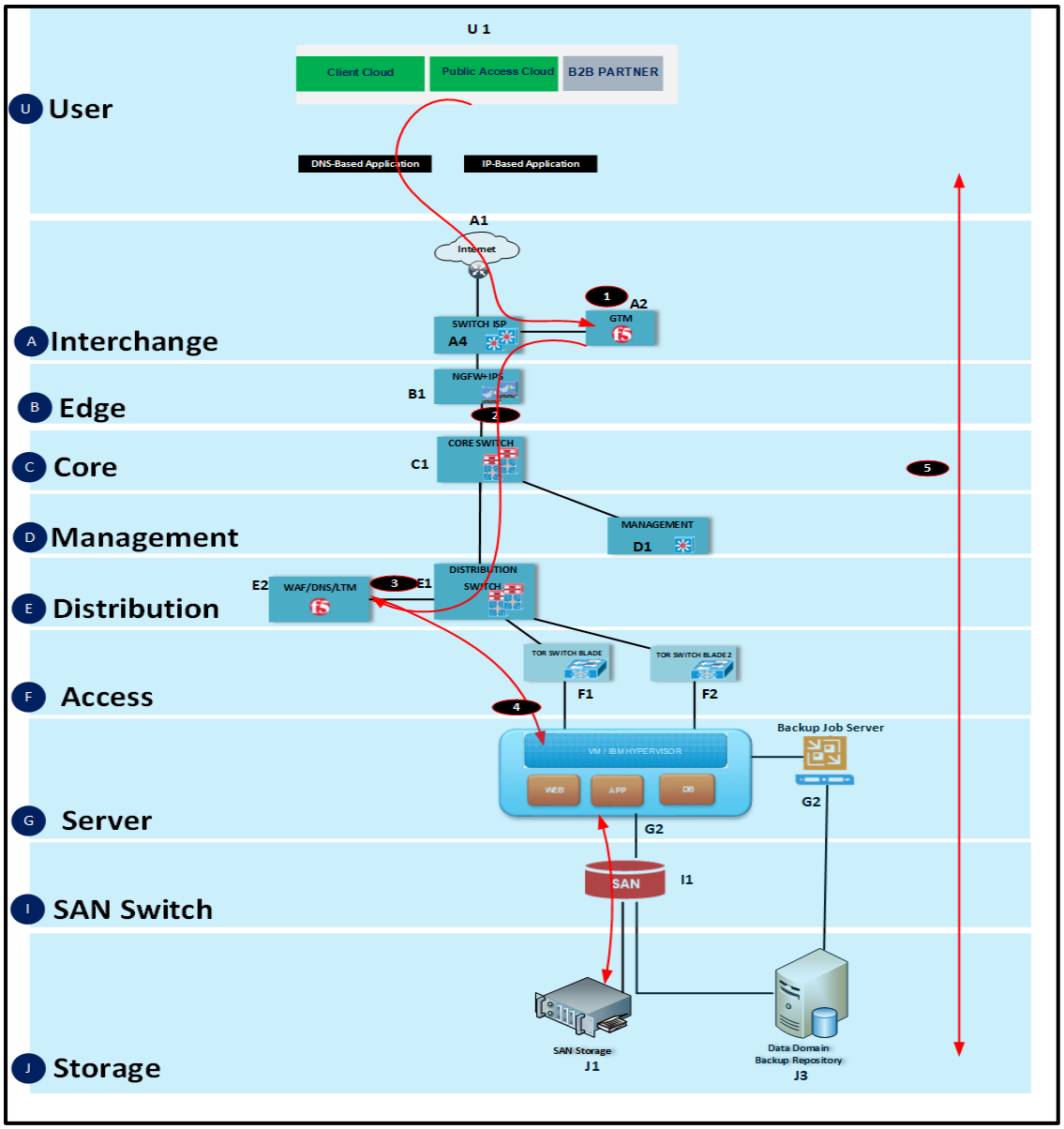


Gambar 3 *High Level Design* Infrastruktur Datacenter PT. XYZ

Fungsional Diagram Design

Fungsional Diagram pada *system engineering* adalah blok diagram yang menjelaskan fungsi masing-masing blok dan korelasi diantara bagian pada sistem tersebut. Pada infrastruktur jaringan yang mengadopsi system hirarki dan modular, blok diagram bisa diasumsikan sebagai modul dari infrastruktur jaringan. Berikut adalah blok diagram dari Infrastruktur Jaringan Datacenter PT. XYZ.

Infrastruktur yang dibangun pada intinya adalah sarana yang dibuat untuk menghubungkan client ke application. Infrastruktur ini dibuat sedemikian rupa agar dapat diandalkan baik dari segi ketersediaan layanan, maupun kehandalan dari menangkis serangan-serangan dari internet (cyber attack). Berikut matriks Fungsional Diagram berdasarkan gambar diatas.Kemudian saat ini layanan-layanan yang ada yang sudah berbasis *DNS-based* dan adapula yang masih menggunakan *IP-Based*.



Gambar 4 ***Data Flow Traffic DNS Based Application***

Traffic Data Flow DNS Based

Blok diagram data flow berdasarkan traffic DNS, berikut adalah flow dari source/client sampai destination/application ke host yang berada di Server Datacenter (Gambar 4).

Berdasarkan Blok gambar diagram di atas, berikut adalah *flow* dari *source/client* sampai *destination/application*. Proses dari sampainya *request* dari *client/source* menuju ke *destination/application*, pada dasarnya berdasarkan *routing protocol*, bisa *routing static* ataupun *routing dynamic* OSPF. Dari gambar diatas tentang *data flow traffic DNS Based application*, berikut adalah prosesnya (Tabel 4).

Data Flow Traffic IP Based Application

Blok diagram *data flow* berdasarkan *traffic IP Address*, berikut adalah flow dari *source/client* sampai *destination/application* ke *host* yang berada di *Server* Datacenter (Gambar 5).

Sequence Diagram* Jaringan dengan *domain

Berdasarkan *High Level Design* Perangkat Jaringan *Data Center* memiliki penjelasan *sequence diagram* Jaringan menggunakan *domain* adalah sebagai berikut (Gambar 6).

Dari gambar di atas tentang *sequence traffic DNS Based application*, berikut adalah proses nya:

1. Pada tahap pertama ini *Source/Client*, akses aplikasi berdasarkan nama (misal xyz.com)
2. Kemudian F5 DNS sebagai *authoritave* DNS akan memberitahukan *IP address* dari aplikasi.
3. Setelah *source/client* mendapatkan *IP address* maka proses selanjutnya adalah untuk menuju *destination*, maka *client* akan mencari jalur untuk menuju tujuan dengan melihat *routing table* dari WAN / CPE.
4. Jalur koneksi yang datang melewati perangkat *Switch provider* yang bertugas pemisahan koneksi WAN / CPE yang akan diteruskan ke *firewall PAN*.
5. Pada *Hop* yang akan dilalui terdapat perangkat *security NGFW Firewall* (Palo Alto 3060), perangkat ini akan mengecek *rule filtering* nya, dan akan mengecek konten isi dari *request* sampai *layer* 7.
6. Koneksi yang masuk masuk akan dilakukan *routing internal* melalui perangkat *edge*.
7. *Transfer routing internal* akan diolah kembali oleh *Core* untuk diteruskan menuju *hop distribution* terdekat.
8. Pada *layer* distribusi sebelum ditransfer ke arah *access*, *traffic application* akan dilakukan penyaringan kembali oleh F5 ASM berdasarkan *policy* teknologi yang digunakan pada *server* aplikasi.
9. Apabila aplikasi tersebut menggunakan *Load Balancer*/F5 LTM, maka IP yang akan di akses adalah IP dari *Load Balancer*nya, berikut proses yang terjadi pada tahap ini *Client* mengakses *Virtual* IP dari Aplikasi, yaitu IP dari *Load balancer* nya.
10. Setelah melalui F5 LTM, proses selanjutnya adalah meneruskan *traffic* dari *client* ke *real* IP dari *server* nya melalui distribution.
11. *Packet* datang menuju titik terdekat *server*. Setelah *request* diterima oleh *server* maka di *reply* kembali hingga *user*.
12. *Reply* paket akan langsung ditransfer *routing* hingga PAN untuk dilakukan *filtering* kembali sebelum menuju *client*.
13. *Firewall* akan mengembalikan *reply* untuk dipisahkan apakah akan dikirim melaui WAN / CPE oleh perangkat *Switch provider*.

14. *Transfer reply* akan sampai ke *client* akan ditransmisikan oleh *router* CPE / WAN.
15. Semua proses tahapan ini, dari *source/client* sampai ke aplikasi akan selesai dengan baik, apabila *routing* dari *source* ke *destination* nya benar.

Sequence Diagram Jaringan dengan IP pada jalur Replikasi

Berdasarkan *High Level Design* Perangkat Jaringan *Data Center* memiliki penjelasan *sequence diagram* Jaringan menggunakan IP adalah sebagai berikut (Gambar 7).

Dari gambar di atas tentang *sequence traffic IP Based application*, berikut adalah proses nya:

1. Pada tahap pertama ini *Source/Client* mengakses menggunakan *IP Address*
2. Setelah *source/client* mendapatkan *IP address* maka proses selanjutnya adalah untuk menuju *destination*, maka *client* akan mencari jalur untuk menuju tujuan dengan melihat *routing table* dari WAN / CPE.
3. Jalur koneksi yang datang melewati perangkat *Switch provider* yang bertugas pemisahan koneksi WAN / CPE yang akan diteruskan ke *firewall* PAN.
4. Pada *Hop* yang akan dilalui terdapat perangkat *security* NGFW *Firewall* (*Palo Alto* 3060), perangkat ini akan mengecek rule *filtering* nya, dan akan mengecek konten isi dari *request* sampai *layer* 7.
5. Koneksi yang masuk masuk akan dilakukan *routing internal* melalui perangkat *edge*.
6. *Transfer routing internal* akan diolah kembali oleh *Core* untuk diteruskan menuju *hop distribution* terdekat.
7. Pada *layer* distribusi akan ditransfer ke arah *access*.
8. *Packet* datang menuju titik terdekat *server*. Setelah *request* diterima oleh *server* maka di *reply* kembali hingga *user*.
9. *Reply* paket akan langsung ditransfer *routing* hingga PAN untuk dilakukan *filtering* kembali sebelum menuju *client*.
10. *Firewall* akan mengembalikan *reply* untuk dipisahkan apakah akan dikirim melaui WAN / CPE oleh perangkat *Switch provider*.
11. *Transfer reply* akan sampai ke *client* akan ditransmisikan oleh *router* CPE / WAN.
12. Semua proses tahapan ini, dari *source/client* sampai ke aplikasi akan selesai dengan baik, apabila *routing* dari *source* ke *destination* nya benar.

Uji Coba Sistem

Tujuan dari tes ini adalah untuk memastikan apakah Vulnerability Protection Palo Alto Networks PA-3060 dapat berfungsi dengan baik

Aktivitas :

- Enable Fitur Vulnerability Protection Palo Alto Networks PA-3060
- Menghubungkan Palo Alto Networks PA-3060 ke jaringan
- Buat satu server tes berisi form login untuk target attack
- Tes serangan menggunakan SQL injection dan XSS
- Memeriksa monitor log dari Palo Alto Networks PA-3060

Hasil yang diharapkan :

- SQL injection attack terblokir akan mendapat perlakuan block (drop atau reset) dari Palo Alto Networks PA-3060
- XSS attack terblokir akan mendapat perlakuan block (drop atau reset) dari Palo Alto Networks PA-3060

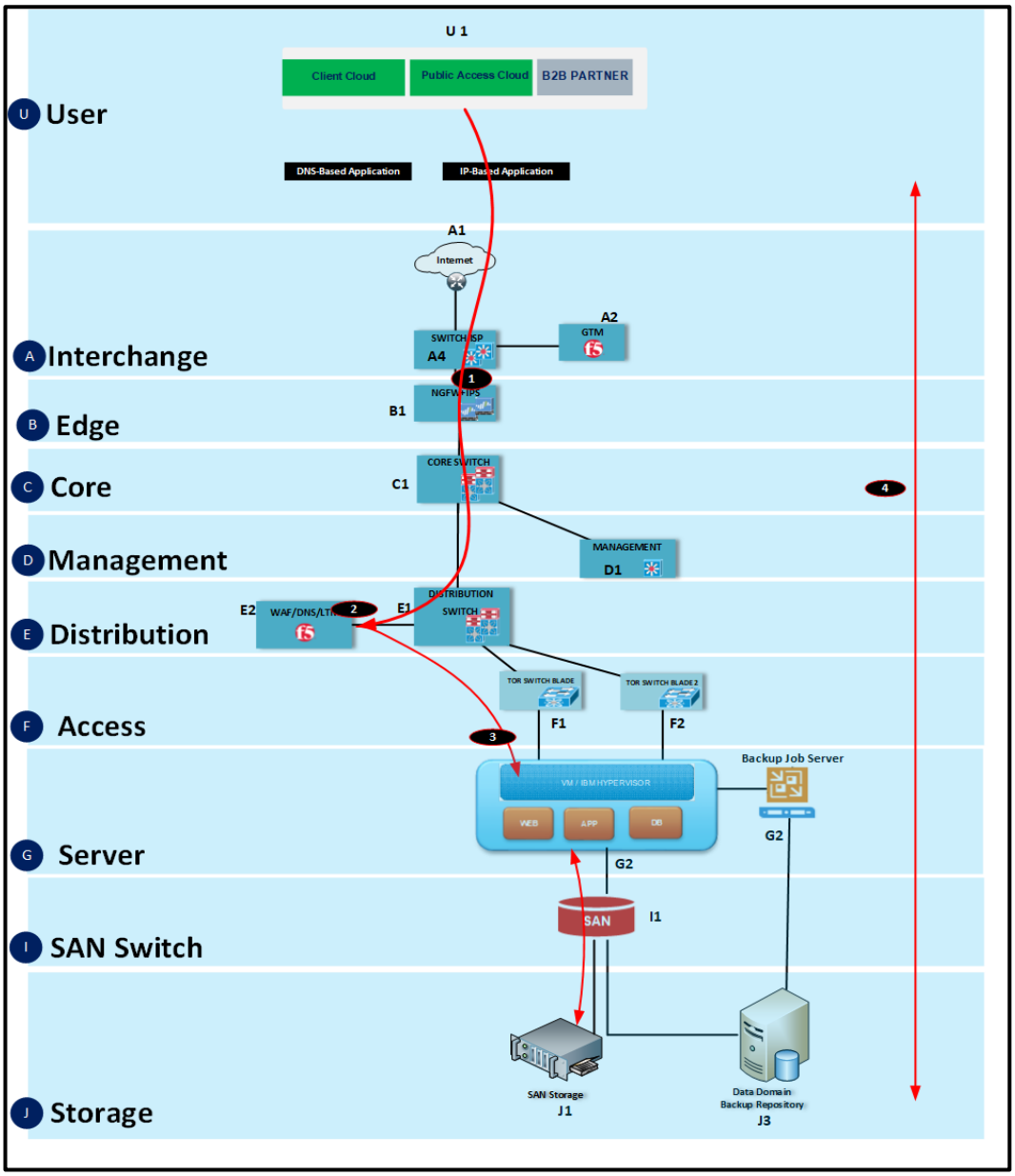
Pembuatan web server untuk dilakukan testing penetration test.

Tabel 4.
Matriks traffic flow Datacenter DNS Based

Proses	Entitas		*Description*
	Incoming Packet		
	Label	Indentitas	
1	*U*	U1	Akses oleh B2B, Client Cloud, Public Access Cloud melalui API aplikasi yang dapat diakses jaringan *public* melalui DNS *name* , contoh xyz.com
	A	A1	*Router* jaringan publik
		A4	Sebagai pemecah trafik yang masuk dari jaringan publik atau *private* yang akan diteruskan sesuai pembagiannya
		A2	sebagai *authoritave query* DNS akan memberitahukan *IP address* dari aplikasi
2	*First Inspeksi & Routing Packet*		
	Label	Indentitas	
	B	*B1*	perangkat *security NGFW Firewall*, perangkat ini akan mengecek *rule filtering*nya, dan akan mengecek *packet* isi dari *request* sampai *layer* 7, *Packet* yang sudah aman akan diteruskan oleh *Router* penghubung antara jaringan luar dengan jaringan Dalam *Data Center*
	C	*C1*	*Packet* akan diterima pada pusat *Routing table*
3	*Second Inspeksi & Distibution Packet*		
	Label	Indentitas	
	E	E2	- Menerima *packet* yang di*broadcast* dari pusat *switching* dengan Segmentasi IP *Virtual Server Loadbalancer* - *IP Virtual Server* dari aplikasi ini dilindungi oleh fitur WAF dari perangkat BigIP-F5 sesuai dengan *policy* yang ditetapkan
4	Receiving Packet		
	Label	Identititas	
	E	E1	Menerima *broadcast traffic* dari F5 LTM IP untuk *real* IP *server* nya yang ditransimisikan untuk diakses
	F	F1	Sebagai switch *Top Of Rack Engine Cloud Virtualization*, bekerja pada *segment Layer* 2 *(broadcast)*
	G	G2	Server tujuan sesuai dengan IP DNS *name* yang diakses oleh *client*
	I	I1	Sebagai penghubung komunikasi data antara *server* dengan *Storage*
	J	J1	Media penyimpanan yang berisi *database* yang hanya diakses di luar komunikasi *Network* (jaringan)

Lanjutan Tabel 4

Answering Request		
Label	**Identititas**	
G	G2	*Server* akan memberikan konten sesuai dengan permintaan dari *client* kepada BigIP F5 untuk dilakukan pembungkusan konten
E	E2	Konten secara UI maupun isi dibungkus sesuai dengan *IP Virtual Server*
B	B1	perangkat *security NGFW Firewall*, perangkat ini akan mengecek kedua kali untuk *rule filtering* keluarnya data dari sergment server *farm* ke *client*.
A	A5	sebagai *authoritave query* DNS akan konten dari aplikasi xyz.com yang sudah dikirim dari server menuju *client.*



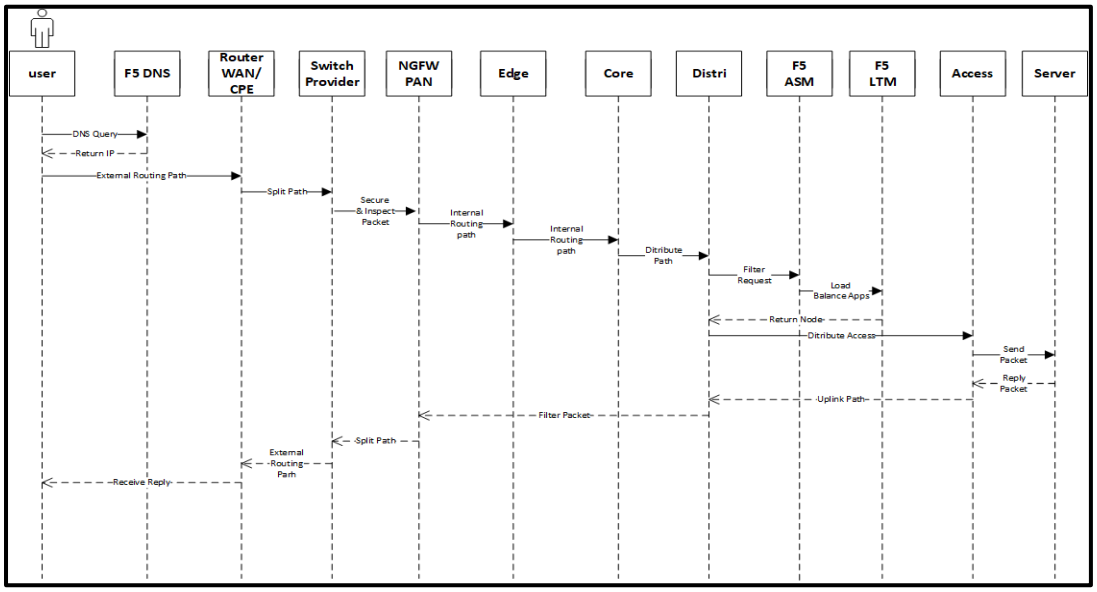
Gambar 5 ***Data Flow Traffic IP Based Application***

Tabel 5.
Matriks traffic flow Data center IP Based

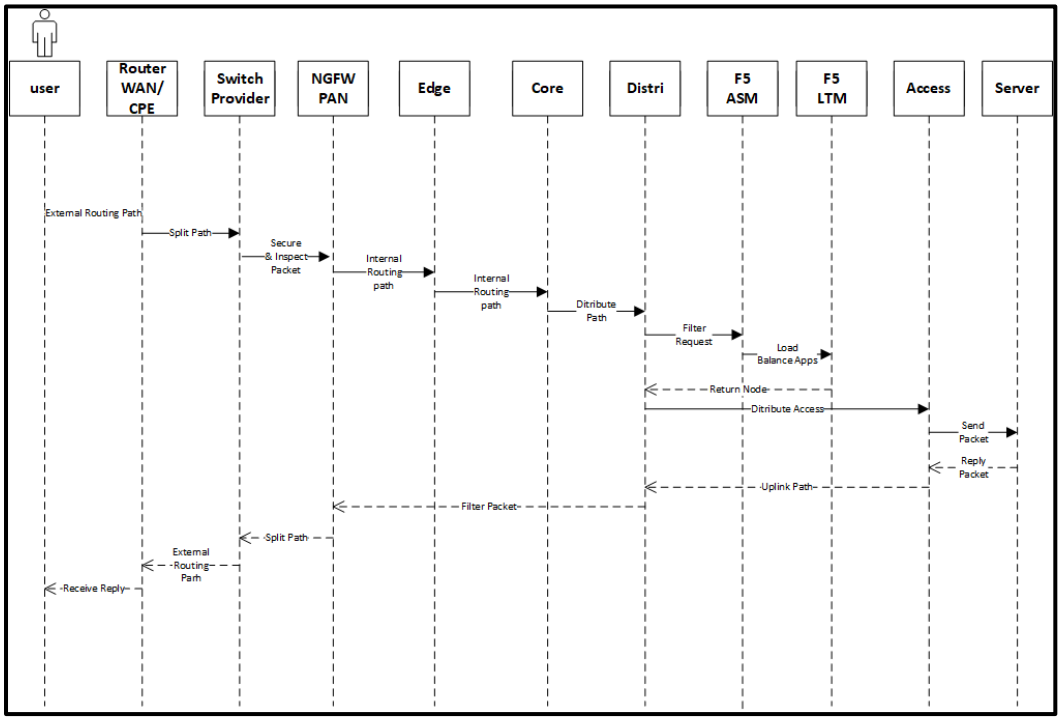
Proses	Entitas		*Description*
	Incoming Packet		
	Label	Indentitas	
1	*U*	U1	Akses oleh B2B, Client Cloud, Public Access Cloud melalui API aplikasi yang dapat diakses jaringan *public* melalui IP *based*.
	A	A1	*Router* jaringan publik
		A4	Sebagai pemecah trafik yang masuk dari jaringan publik atau *private* yang akan diteruskan sesuai pembagiannya
2	*First Inspeksi & Routing Packet*		
	Label	Indentitas	
	B	*B1*	perangkat *security NGFW Firewall*, perangkat ini akan mengecek *rule filtering* nya, dan akan mengecek *packet* isi dari *request* sampai *layer* 7, *Packet* yang sudah aman akan diteruskan oleh *Router* penghubung antara jaringan luar dengan jaringan Dalam *Data Center*
	C	*C1*	*Packet* akan diterima pada pusat *Routing table*
	E	*E1*	Meneruskan paket ke Pusat *Switch* layer 2 yang akan mendistribusikan sesuai VLAN
3	*Second Inspeksi & Distibution Packet*		
	Label	Indentitas	
	E	E2	- Menerima *packet* yang di*broadcast* dari pusat *switching* dengan Segmentasi IP *Virtual Server Loadbalancer* - *IP Virtual Server* dari aplikasi ini dilindungi oleh fitur WAF dari perangkat BigIP-F5 sesuai dengan policy yang ditetapkan
4	*Receiving Packet*		
	Label	Identititas	
	E	E1	Menerima *broadcast traffic* dari F5 LTM IP untuk *real* IP *server* nya yang ditransimisikan untuk diakses
	F	F1	Sebagai switch *Top Of Rack Engine Cloud Virtualization*, bekerja pada *segment Layer* 2 *(broadcast)*
	G	G2	*Server* tujuan sesuai dengan IP DNS *name* yang diakses oleh *client*
	I	I1	Sebagai penghubung komunikasi data antara *server* dengan s*torage*
	J	J1	Media penyimpanan yang berisi database yang hanya diakses diluar komunikasi *Network* (jaringan)

Lanjutan Tabel 5

	Answering Request		
	Label	Identititas	
5	G	G2	*Server* akan memberikan konten sesuai dengan permintaan dari *client* kepada BigIP F5 untuk dilakukan pembungkusan konten
	E	E2	Konten secara UI maupun isi dibungkus sesuai dengan *IP Virtual Server*
	B	B1	perangkat *security NGFW Firewall*, perangkat ini akan mengecek kedua kali untuk *rule filtering* keluarnya data dari sergment *server* farm ke *client*.

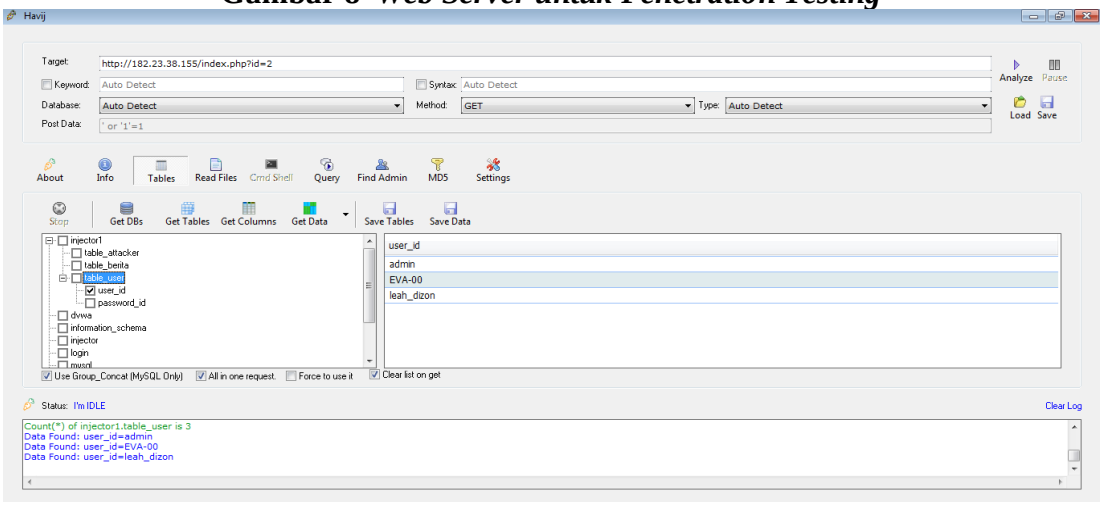


Gambar 6 *Sequence Diagram* Jaringan dengan *domain* Datacenter

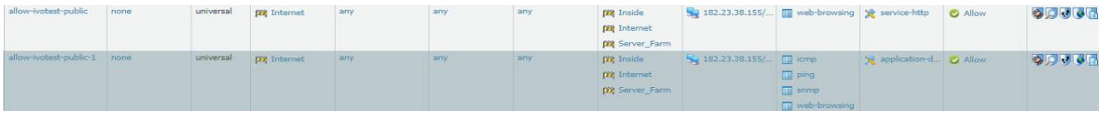


Gambar 7 *Sequence Diagram* Jaringan dengan *IP Address* Datacenter

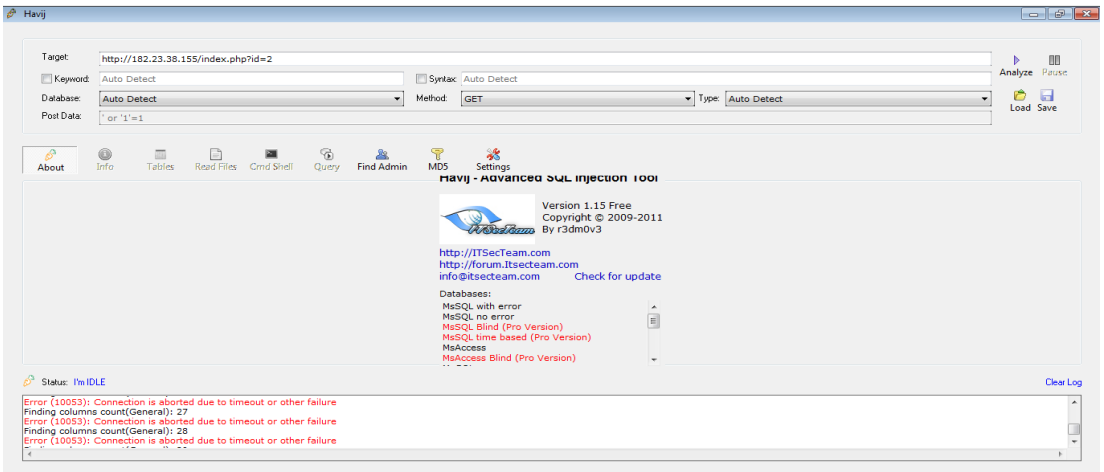
Gambar 8 ***Web Server untuk Penetration Testing***



Gambar 9 ***SQL Injection Penetration Testing***

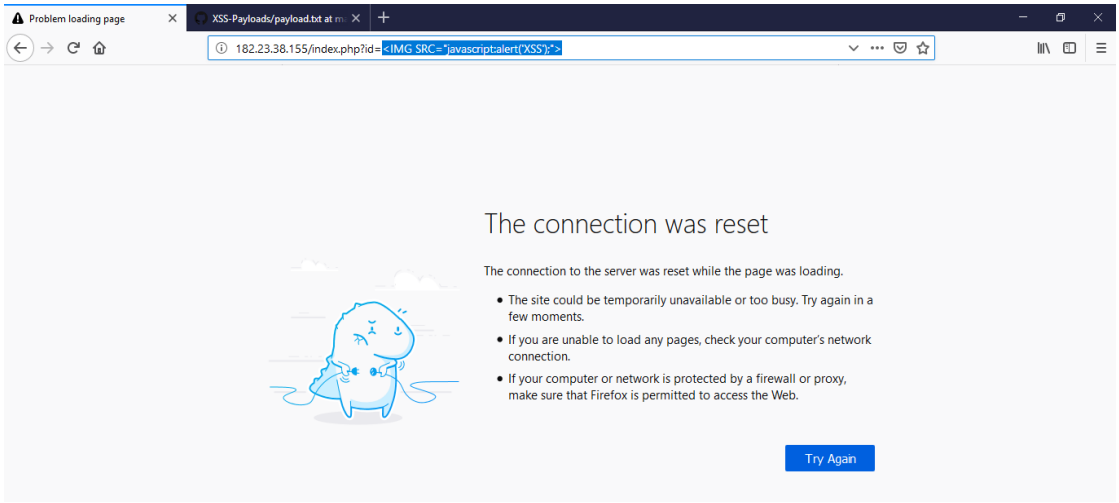


Gambar 10 ***NGFW Rule***



Gambar 11 ***SQL Injection Penetration Testing setelah ada NGFW***

Gambar 12 ***SQL Injection Penetration Testing terblock terlihat pada monitor***



Gambar 13 ***XSS Attack tidak berefek pada system***

Gambar 14 ***XSS Attack Testing terblock terlihat pada monitor***

Melakukan penetration test untuk proses SQL Injection (Gambar 9). SQL injection dilakukan bahwa firewall sebelumnya masih dapat diserang untuk mengeksploitasi sistem database web server yang berada di cloud (Gambar 10). Dilakukan testing kembali untuk melakukan SQL Injection saat sudah menggunakan NGFW dan rule dalam keadaan aktif (Gambar 11). Setelah dilakukan penetration test kembali bahwa SQL Injection tidak bisa dilakukan kembali dikarena adanya rule menghalau penyerangan terhadap sistem cloud (Gambar 12). Setelah itu melakukan perangan dengan menggunakan teknik Cross site Scripting atau dikenal dengan XSS attack dengan scipt (Gambar 13). Serangan XSS Attack tidak mengefek pada sistem yang berjalan karena NGFW telah melakukan blocking pada serangan (Gambar 14).

KESIMPULAN DAN SARAN

Dengan menggunakan firewall NGFW dengan Web Application Firewall (WAF) saat ini masih mampu melakukan pengamanan terhadap sumber informasi pada Cloud PT. XYZ sehingga mengurangi komponen kritikal *virtual* yang berfungsi dalam menjaga keberlangsungan bisnis PT. XYZ adalah Sistem dan Teknologi Informasi, sehingga diperlukan *cyber resiliency* yang dapat menjamin ketersediaan (*availability*) dan integritas (*integrity*) data dan layanan *digital*. Salah satu penunjang dalam meningkatkan data *availability* dan *integrity* terkait *cyber resiliency*.

Penulis menyadari bahwa keamanan data selalu memiliki peningkatan dari hari ke hari, sehingga penggunaan perangkat keamanan berskala enterprise harus selalu mengikuti perkembangan dari sistem yang sedang kita gunakan dengan cara melakukan pembaharuan pada sistem keamanan untuk menutup celah-celah vulnerability pada sistem keamanaan terdahulu tidak lupa pula melakukan perpanjangan lisensi perangkat keamanan agar sistem keamanan tetap memberikan pengamanan pada sumber data.

DAFTAR PUSTAKA

Sanders, Chris. (2011).Practical Packet Analysis, 2nd Edition., San Francisco: No Starch Press

Barak, Lior. (2016). "Implementing a prototype for the Deep Packet Inspection as a Service Framework." M.Sc. Efi Arazi School of Computer Science,

Bilal Maqbool Beigh, Prof.M.A.Peer,.(2012). Intrusion Detection and Prevention System: Classification and Quick Review, ARPN Journal of Science and Technology, Vol. 2, No. 7, August 2012, ISSN: 2225-7217

TEC.(2011). "White Paper on Deep Packet Inspection." Internet: http://tec.gov.in/pdf/Studypaper/White%20paper%20on%20DPI.pdf, 20 November, 2011

Lammle,Todd.(2013)." CCNA Data Center - Introducing Cisco Data Center Networking Study Guide".Newyork: Sybex Inc.

Warsinske,John.(2019)." CISSP Certified Information System Security Professional" .Newyork: Sybex Inc.

Eko Nugroho, Faizal.(2015). "Analisis Perbandingan Perfomansi Deep Packet Inspection Firewall Antara L7-Filter dan n-DPI," e-Proceeding of Engineering., vol. 2 no. 1 pp.1469 April 2015.