PROSIDING Seminar Nasional SISFOTEK ISSN 2597-3584 (Media Online)
Sistem Informasi dan Teknologi
website : www.seminar.iaii.or.id | email : seminar@iaii.or.id

Implementasi Pengamanan Terhadap Server Menggunakan Next Generation Firewall (NGFW)

Syahrul Ramadhan Nuriana[1*], Imam Sutanto[2], Nizirwan Anwar[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universita Esa Unggul
[1]syahrul1601@gmail.com, [2]imam.sutanto@esaunggul.ac.id, [3]nizirwan.anwar@esaunggul.ac.id

Abstract

The high use of information technology carries a significant risk of cyber attacks, making it important for organisations to secure their servers to prevent intrusion and data leaks. This research focuses on the development and implementation of a CheckPoint Next Generation Firewall (NGFW) configured to mitigate cyber attacks, especially those included in the OWASP Top 10, with a Network Development Life Cycle (NDLC) approach. The research results show that implementing NGFW effectively improves server security and protects against cyber attacks. These findings emphasize the importance of NGFWs in an organization's network security architecture, with the right configuration serving as a proactive mitigation tool against cyber threats.

Keywords: Cyberattack, firewall, NGFW, Owasp Top 10

Abstrak

Tingginya penggunaan teknologi informasi membawa risiko signifikan terhadap serangan siber, sehingga penting bagi organisasi untuk mengamankan servernya guna mencegah penyusupan dan kebocoran data. Penelitian ini berfokus pada pengembangan dan implementasi CheckPoint Next Generation Firewall (NGFW) yang dikonfigurasi untuk mitigasi serangan siber, terutama yang termasuk dalam OWASP Top 10, dengan pendekatan Network Development Life Cycle (NDLC). Hasil penelitian menunjukkan bahwa penerapan NGFW secara efektif meningkatkan keamanan server, memberikan perlindungan terhadap berbagai serangan siber. Temuan ini menegaskan pentingnya NGFW dalam arsitektur keamanan jaringan organisasi, dengan konfigurasi yang tepat mampu berfungsi sebagai alat mitigasi proaktif terhadap ancaman siber.

Kata kunci: Serangan siber, firewall, NGFW, Owasp Top 10

1. Pendahuluan

Dengan perkembangan internet dan juga teknologi informasi yang cepat juga merupakan kesempatan lain bagi beberapa oknum untuk menjalankan serangan yang merugikan pihak lain. Di era saat ini hampir semua pihak dapat mengirimkan dan juga menerima berbagai bentuk data berbentuk e-mail, audio, maupun video, hanya dengan satu kali klik. Begitupula seorang atau sekelompok pelaku kejahatan akan memanfaatkan kemudahan tersebut untuk menyerang kelemahan dalam teknologi. Seluruh serangan yang terjadi kerap kita kenal dengan istilah *cybercrime*.

Aktivitas kriminal yang dilakukan dengan menggunakan komputer sebagai alat atau menjadikannya target dari aktivitas itu sendiri dapat disebut dengan *cybercrime* [1]. Ketika masyarakat maupun pelaku bisnis telah melakukan kegiatan seluruhnya bergantung pada teknologi, sebagai seorang pengguna atau *user* pasti mengetahui bahwa privasi terhadap informasi mengenai diri kita tidak 100% aman dan hal inilah yang menyebabkan peningkatan terjadinya kasus *cybercrime* dari hari ke hari. Serangan siber (*cyber-attack*) pada umumnya terjadi dengan menyerang server dari suatu perusahaan atau organisasi dengan tujuan untuk mencuri data maupun informasi penting sehingga dapat membuat server down hingga tidak dapat diakses oleh organisasi.

Kasus mengenai *cybercrime* sendiri sudah banyak terjadi di Indonesia dan beberapa kasus tersebut juga menyerang server. Server merupakan sesuatu yang berada dalam jaringan, memiliki layanan khusus berupa penyimpanan data yang dimana layanan ditujukan khusus untuk client yang membutuhkan dalam menyediakan informasi bagi penggunannya. Selain itu, server memiliki peran penting didalam menyediakan akses cepat bagi yang mengirim atau menerima data atau informasi yang tersedia. Kejahatan siber dilakukan untuk menyerang server dan yang dicuri atau hendak diambil ialah data dari target yang sudah ditentukan.

Beberapa kasus kejahatan siber. Yang pertama yaitu kasus penyerangan dengan menggunakan metode SQL Injection pada website KPU di tahun 2004. Dimana *hacker* bernama Xnuxer (Dani Firmansyah) berhasil melakukan SQL Injection dan mengubah data seperti nama partai, misalnya, menjadi Partai Si Yoyo, Partai

Kolor Ijo, Partai Dibenerin Dulu Webnya, dan sebagainya. SQL Injection merupakan kerentanan yang memungkinkan penyerang untuk merubah kueri yang digunakan dalam database [2].

Kasus diatas menunjukkan betapa pentingnya suatu organisasi untuk mengamankan servernya sehingga dapat meminimalisir ataupun menghindari adanya penyusupan dan kebocoran data. Salah satunya adalah dengan menggunakan *firewall*. Namun, dengan perkembangan teknologi yang cepat *firewall* tradisional dinilai tidak mampu dalam melindungi jaringan dari ancaman *cyber-crime*. Maka dari itu munculah *Next Generation Firewall* atau NGFW.

Next Generation Firewall (NGFW) merupakan perkembangan dari *firewall* tradisional yang dapat memberikan perlindungan yang lebih baik terhadap ancaman keamanan jaringan. NGFW salah satu alat keamanan jaringan yang digunakan untuk memonitor kejadian di jaringan, menganalisis masalah kemanan jaringan, dan meningkatkan perlindungan keamanan jaringan dari ancaman. NGFW menggabungkan teknologi *firewall*, *intrusion prevention system* (IPS), *anti-mare* dan juga anti-bot dalam satu perangkat yang dapat memberikan perlindungan yang lebih baik terhadap ancaman keamanan jaringan.

CheckPoint NGFW (*Next Generation Firewall*) Software adalah keamanan yang bertugas untuk mendeteksi dan memblokir serangan siber dari dalam maupun luar jaringan. Berbeda dengan *firewall* tradisional, NGFW menginspeksi semua *traffic*, serangan, dan konten di berbagai platform, serta menganalisa metode kerja serangan siber. Sistem NGFW adalah gabungan dari *firewall* tradisional dengan fitur lain yaitu *Intrusion Prevention System* (IPS) dalam satu perangkat.

Sehingga tujuan akhir dari penelitian ini adalah meningkatkan pengamanan jaringan melalui penerapan Next Generation Firewall (NGFW) dengan menggunakan Sistem CheckPoint. Berdasarkan keterangan diatas, penulis tertarik mengambil topik penulisan dengan judul "Implementasi Pengamanan Terhadap Server Menggunakan NGFW (*Next Generation Firewall*)".

2. Metode Penelitian

2.1. Teknik Pengumpulan Data

Dalam penelitian ini diperlukan data-data yang berkaitan dengan permasalahannya. Oleh karena itu, penulis menggunakan teknik pengumpulan data kualitatif yaitu:

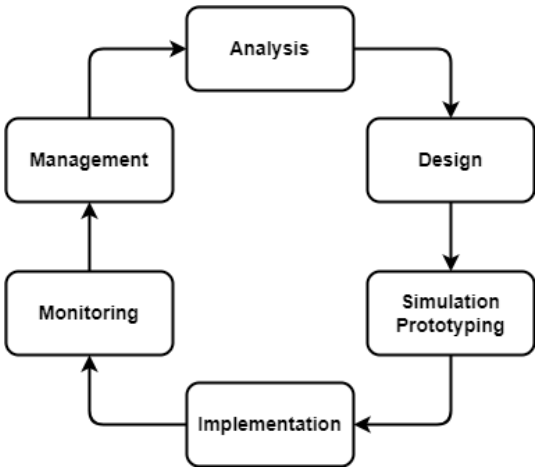
Studi Kepustakaan: Penulis memperoleh melalui studi kepustakaan (studi literatur) yaitu dengan mencari bahan dari internet, jurnal dan tesis yang sesuai dengan objek yang diteliti.

Observasi: Penulis akan melakukan perbandingan pada jaringan yang menggunakan *Next Generation Firewall* dan yang tidak. Dimana kedua jaringan tersebut akan diberikan perlakuan yang sama dengan melakukan serangan siber berupa SQL Injection, XSS, dan Brute Force Attack.

Wawancara: Penulis melakukan wawancara mengenai *Next Generation Firewall*. Wawancara ini diisi oleh para narasumber yang memiliki pekerjaan sebagai *implementation engineer*. Wawancara ini bertujuan untuk mendapatkan jawaban yang actual mengenai *Next Generation Firewall*.

2.2. Metode Perancangan Desain Topologi Dengan NGFW

Dalam penelitian ini penulis menggunakan model perancangan jaringan *Network Development Life Cycle* (NDLC). Metode tersebut terdari dari beberapa fase: *Analysis*, *Design*, *Simulation Prototyping*, *Implementation*, *Monitoring*, *Management*. Berikut adalah tahapan dari metode NDLC:



Gambar 1. Model Network Development Life Cycle (NDLC) [3].

Gambar 1 menjelaskan bahwa tiap metode NDLC memiliki tahapan yang saling terkait dengan tahapan-tahapan selanjutnya. Adapun penjelasan dari tahap diatas yaitu sebagai berikut:

Pada tahap *analysis*, penulis akan mengumpulkan informasi yang berkaitan dengan *firewall* dengan melakukan wawancara. Kemudian melakukan analisa dengan mengidentifikasi sistem yang tidak memiliki *firewall* dan mencoba mencari cara untuk mengembangkan sistem tersebut menjadi lebih baik.

Pada tahap *design*, penulis akan mengembangkan data yang sudah dikumpulkan pada tahap analysis untuk membuat perencanaan, desain sistem, dan topologi jaringan yang sesuai.

Penulis akan melakukan pengembangan jaringan yang akan membuat dalam bentuk simulasi dengan bantuan tools EVE-NG. Hal ini dimaksudkan untuk melihat kinerja dari keamanan jaringan, desain jaringan yang akan dibangun dan menjadi lingkungan testing

development sebelum akhirnya di implementasikan pada lingkungan production.

Penulis akan menerapakan semua yang direncanakan dan dirancang pada tahap-tahap sebelumnya.

Setelah melakukan implementasi, penulis akan memonitor dan memastikan bahwa jaringan dapat berjalan sesuai dengan yang diinginkan dan sudah direncanakan.

Dalam tahap *management*, penulis akan memberikan perhatian khusus pada jaringan dengan melakukan pembuatan kebijakan, pemeliharaan, dan pengelolaan agar jaringan yang telah dibangun dapat berjalan dengan baik, dapat berlangsung dengan waktu yang lama, dan memiliki unsur reliability.

Firewall merupakan suatu perangkat jaringan yang mana menerapkan kebijakan keamanan untuk lalul lintas jaringan. Istilah *firewall* sendiri berasal dari "*fire*" dan "*wall*" yang berarti dinding api, dimana dinding ini digunakan untuk mencegah penyebaran api. Selain itu *firewall* juga dapat membatasi paparan host pada lalu lintas jaringan yang berbahaya seperti jika ada organisasi yang hendak mengeksploitasi keamanan dalam aplikasi yang rentan dari jarak jauh, caranya adalah dengan mencegah packet tertentu yang masuk dalam jaringan yang dilindungi oleh *firewall* [4].

Next Generation Firewall atau NGFW mengacu pada solusi teknologi jaringan yang meningkatkan teknologi yang dimiliki oleh *firewall* tradisional dengan fitur tambahan yang terutama berfokus pada inspeksi *packet* mendalam. Dengan adanya dukungan pemeriksaan *packet* mendalam, NGFW mampu memberikan kemampuan keamanan lebih lanjut. Termasuk didalamnya *Intrusion Prevention System* (IPS), mengendalikan lalu lintas (*traffic*) jaringan berdasarkan aplikasi jaringan, dan meningkatkan visibilitas dan keamanan dengan dapat mendekripsi lalu lintas (*traffic*) TLS [5]. Berbeda dengan *firewall* tradisional, NGFW menginspeksi semua aplikasi, serangan, *traffic* dan konten di berbagai platform, serta menganalisa metode kerja serangan siber. NGFW menawarkan beberapa fitur dan keuntungan yang lebih banyak dibanding *firewall* tradisional yang sudah ada sebelumnya. NGFW melakukan perlindungan secara lebih baik dan cerdas. NGFW menambah fitur tambahan seperti inspeksi IPS, inspeksi SSH dan SSL, *application control*, web *filtering*, serta perlindungan terhadap malware.

CheckPoint adalah sebuah sistem kemanan besutan dari perusahaan Check-Point Software Technologies Ltd. CheckPoint *Firewall* merupakan *Next Generation Firewall* (NGFW), Teknologi NGFW adalah solusi keamanan mutakhir yang bertugas untuk mendeteksi dan memblokir serangan siber dari pihak ketiga. Sehingga, data yang perusahaan miliki tidak bisa diubah, dicuri atau dirusak dengan mudah.

2.3. Perbedaan Firewall Tradisional Dan NGFW

Seiring berkembangnya waktu *Firewall* telah berkembang dan salah satunya telah menjadi NGFW. Berikut merupakan tabel 1 yang menunjukkan perbedaan diantara *Firewall* dan NGFW [6].

Tabel 1. Perbedaan Firewall dan NGFW

Firewall	NGFW
Firewall tradisional menyediakan inspeksi "*stateful*" dari lalu lintas jaringan yang masuk dan keluar.	NGFW menyediakan inspeksi "*stateful*" dari lalu lintas jaringan yang masuk dan keluar bersamaan dengan fitur tambahan lainnya, seperti *antivirus*, IPS, *url filtering*, dan *application control*.
Firewall tradisional menyediakan kontrol dan visibilitas aplikasi secara parsial.	NGFW menyediakan kontrol dan visibilitas aplikasi secara menyeluruh.
Firewall tradisional bekerja pada layer 2 hingga layer 4.	NGFW bekerja pada layer 2 hingga layer 7. Sehingga memiliki jangkauan lebih luas.
Firewall tradisional tidak dapat mendeskripsi dan menginspeksi *traffic* SSL	NGFW dapat mendeskripsi dan menginspeksi *traffic* SSL.
Integrated Intrusion System dan *Intrusion Detection System* pada firewall tradisional di *deploy* secara terpisah.	*Integrated Intrusion System* dan *Intrusion Detection System* pada NGFW sudah terintegrasi.

Server merupakan program komputer atau perangkat yang menyediakan layanan kepada program komputer lain dan penggunanya, yang juga dikenal sebagai *client*. Dalam model pemrograman klien/server, program server menunggu dan memenuhi permintaan dari program klien, yang mungkin berjalan di komputer yang sama, atau komputer lain [7]. Berikut merupakan jenis-jenis server [7]:

Web Server merupakan program komputer yang melayani halaman atau berkas HTML yang diminta. Dimana didalam perihal ini, peramban web bertindak sebagai klien.

Application Server merupakan suatu program dalam komputer dalam jaringan terdistribusi yang menyediakan logika bisnis untuk program aplikasi.

Proxy Server merupakan suatu perangkat lunak atau software yang bertindak sebagai perantara antara perangkat titik akhir, seperti komputer, dan server lain dari mana pengguna atau klien meminta layanan.

Mail Server merupakan suatu aplikasi yang menerima email masuk dari local users atau dari orang-orang dalam domain yang sama dan juga pengirim jarak jauh dan meneruskan email keluar untuk pengiriman.

Virtual Server merupakan suatu program yang berjalan pada server bersama-sama yang kemudian dikonfigurasi sedemikian rupa sehingga tampak bagi setiap pengguna bahwa mereka memiliki kendali penuh atas server.

Blade Server adalah sasis server yang menampun beberapa papan sirkuit elektronik modular tipis, yang

dikenal sebagai bilah server. Dimana setiap bilah (blade) adalah server dengan haknya sendiri, sering kali didedikasikan untuk satu aplikasi.

File Server merupakan server komputer yang bertanggung jawab untuk penyimpanan pusat dan manajemen file data sehingga komputer lain pada jaringan yang sama dapat mengakses dengan mudah.

Policy Server merupakan komponen keaman dari jaringan berbasis kebijakan yang menyediakan layanan otorisasi dan memfasilitasi pelacakan dan kontrol file.

Database Server merupakan server yang bertanggung jawab untuk hosting satu atau lebih database. Dimana aplikasi klien melakukan kueri basis data yang mengambil data dari atau menulis data ke basis data yang dihosting di server.

Print Server merupakan server yang menyediakan pengguna dengan akses ke satu atau lebih printer yang terpasang di jaringan. Server pencetakan bertindak sebagai antrian untuk pekerjaan pencetakan yang diajukan pengguna.

Intrusion Prevention System (IPS) merupakan sistem yang mempunyai fungsi untuk mendeteksi dan melakukan blokir terhadap serangan pada jaringan komputer sehingga dengan adanya IPS dapat mencegah terjadinya pencurian data atau informasi, perusakan sistem, dan kejahatan cyber lainnya [8]. Maka dari itu, IPS kerap kali dimasukkan dalam bagian NGFW, dikarenakan dalam penggunaannya IPS bisa melakukan pemindaian volume lalu lintas yang tinggi tanpa membuat kinerja jaringan menjadi lambat. Dalam penggunaannya IPS memiliki beberapa teknik yang digunakan untuk mengidentifikasi ancaman diantaranya [9]:

Signature-based: IPS menggunakan database pola serangan yang diketahui untuk mengidentifikasi dan memblokir aktivitas jahat. Ketika lalu lintas jaringan cocok dengan "signature" yang telah diketahui, maka IPS akan mengambil tindakan untuk mencegah intrusi. Kendati demikian, metode ini memiliki kelemahan salah satunya adalah hanya dapat menghentikan serangan yang telah diidentifikasi sebelumnya dan tidak akan dapat mengenali serangan baru.

Anomaly-based: IPS memantau lalu lintas jaringan dan membuat dasar perilaku normal. Kemudian, IPS mengidentifikasi penyimpangan dari dasar tersebut dan menganggapnya sebagai ancaman potensial. Deteksi dengan anomaly-based ini dapat membantu mengidentifikasi serangan baru atau yang tidak diketahui dan tidak memiliki "signature" yang sudah ada sebelumnya. Beberapa IPS yang lebih baru dan lebih canggih menggunakan AI dan Teknologi Pembelajaran mesin (Machine Learning Technology) untuk mendukung pemantauan berbasis anomaly.

Policy-based: Metode ini kurang umum digunakan jika dibandingkan dengan 2 metode sebelumnya. Metode ini menggunakan kebijakan keamanan yang ditentukan oleh perusahaan dan memblokir aktivitas yang melanggar kebijakan tersebut. Dalam metode ini diperlukan administrator untuk mengatur dan mengkonfigurasi kebijakan keamanan.

Demilitarized Zone atau DMZ berangkat dari istilah yang merupakan zona penyangga yang dibuat antara Korea Utara dan Korea Selatan, pada dasarnya merujuk pada area dimana kegiatan militer dilarang oleh dua atau lebih negara. DMZ adalah sub-jaringan yang dibuat untuk menyediakan layanan eksternal organisasi kepada jaringan yang tidak dipercaya, seperti salah satunya internet. Dalam jaringan komputer, DMZ berperang penting dalam memberikan keamanan pada jaringan internal (LAN) dengan mencegah akses langsung melalui jaringan eksternal (WAN) [10]. Dengan menerapkan DMZ akan menambah layer dari keamanan jaringan sehingga penyerang tidak dapat mengakses dari pihak internal, selain itu DMZ juga dikenal sebagai "Perimeter Network" [11].

2.4. Bentuk-Bentuk Serangan Siber (*Cyber Attack*)

SQL Injection merupakan sebuah kerentanan yang terdapat pada *web*. Dimana kerentanan tersebut memungkinkan penyerang untuk merubah kueri yang digunakan dalam database [12]. SQL Injection memungkinkan penyerang untuk melihat data yang seharusnya tidak dapat diakses hingga memungkinkan penyerang untuk mendapatkan akses ke dalam server.

Cross-Site Scripting (XSS) merupakan sebuah serangan dengan melakukan injeksi *script* ke dalam suatu web [13]. Script tersebut dapat berupa html tag, javascript, dan lainnya. Dengan memanfaatkan kerentanan tersebut, penyerang dapat mengirimkan *script* berbahaya kepada pengguna lain dan pengguna lain tersebut tidak akan mengetahui bahwa ada *script* berbahaya yang berjalan di belakang layar dan mengambil data-data sensitif yang dimiliki.

Brute force attack merupakan sebuah serangan siber yang mencoba seluruh kombinasi *password* secara sistematis hingga menemukan *password* yang sesuai [14]. Penyerang dapat menggunakan alat otomatis yang dapat menghasilkan dan menguji sejumlah besar variasi *password* dengan cepat sehingga dapat membebani server.

OWASP Top 10 merupakan sebuah dokumen yang diperbarui secara berkala dan menjadi standar untuk developer dan web application security [15]. Dimana dokumen tersebut berisi data mengenai 10 kerentanan dalam *web application security* yang paling kritis. OWASP Top 10 seringkali menjadi acuan bagi perusahaan di seluruh dunia untuk meminimalkan dan / atau mengurangi risiko keamanan. Menggunakan OWASP Top 10 merupakan langkah pertama yang paling efektif untuk mengubah budaya pengembangan perangkat lunak dalam organisasi menjadi budaya yang menghasilkan kode yang lebih aman [16].

Berikut merupakan data OWASP Top 10 di tahun 2021:

Access Control merupakan kebijakan yang dibuat sedemikian rupa sehingga pengguna hanya bisa mengakses atau bertindak sesuai dengan izin yang diberikan [17]. Kerentanan atau kelemahan yang terjadi pada *access control* dapat menyebabkan *unauthorized information disclosure*, modifikasi data, penghapusan data, hingga melakukan tindakan yang hanya bisa dilakukan oleh pengguna lain.

Cryptographic failures disebabkan oleh kebocoran data sensitif seperti kata sandi, nomor kartu kredit, serta informasi pribadi [18]. Kebocoran data sensitif dapat disebabkan oleh penggunaan algoritma *cryptographic* yang lemah, serta *password* atau data sensitif yang disimpan secara *hard code*.

Injection merupakan sebuah serangan siber yang memungkinkan penyerang untuk memasukkan suatu *command* atau *code* ke dalam suatu situs yang nantinya akan dijalankan [19]. Dua jenis *injection* yang paling sering terjadi adalah *Cross Site Scripting (XSS)* dan *SQL Injection*.

Secure Design merupakan sebuah kebiasaan dan metodologi yang secara konstan mengevaluasi ancaman dan memastikan bahwa aplikasi, website, maupun jaringan yang dibuat telah dirancang dan diuji dengan kuat untuk menghadapi serangan yang dapat terjadi [20]. Oleh karena itu, *insecure design* merupakan kerentanan dimana kurangnya kontrol akan keamanan pada suatu aplikasi, website, maupun jaringan [21]. Dengan kurangnya *secure design* dapat memperbesar kemungkinan kebocoran data.

Security Misconfiguration merupakan kerentanan yang terjadi akibat dari kekeliruan atau kesalahan ketika melakukan konfigurasi [22]. Kekeliruan atau kesalahan tersebut akan membuat penyerang dapat mengakses secara tidak sah.

Vulnerable and Outdated Components merupakan komponen *software* yang sudah tidak lagi di-*support* oleh *developer*-nya, sehingga menyebabkan adanya kemungkinan celah keamanan atau kerentanan [23].

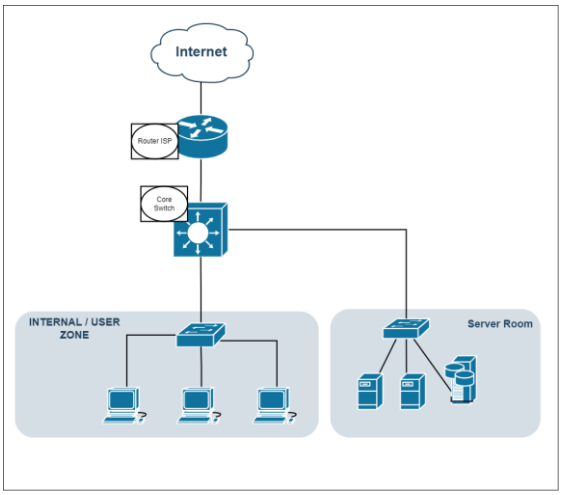
Identification and Authentication merupakan sebuah proses memvalidasi bahwa pengguna merupakan pengguna yang sebenarnya [24]. Validasi tersebut dapat dilakukan dengan berbagai cara, seperti memasukkan *password*, OTP (*One Time Password*) melalui SMS ataupun email, MFA (*Multi Factor Authentication*) melalui aplikasi autentikator, atau menggunakan biometrik.

Software and Data Integrity Failures berhubungan dengan kode dan infrastruktur yang tidak melindungi dari pelanggaran integritas [25]. Contohnya pada *auto update*, dimana *update* akan diunduh tanpa adanya verifikasi integritas terlebih dahulu. Hal tersebut memungkinkan penyerang untuk mengirim pembaruan yang mereka buat. Dimana pembaruan tersebut merupakan *malware*.

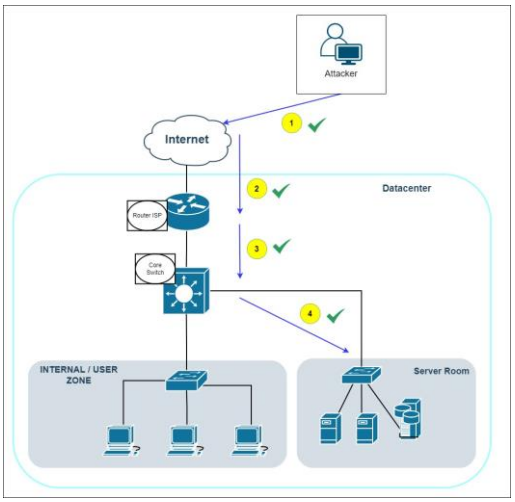
Security Logging and Monitoring Failures yang tidak memadai dapat berdampak pada visibilitas, peringatan insiden, kegagalan login, kegagalan sistem, dan pelanggaran [26].

Server-Side Request Forgery atau SSRF merupakan sebuah kerentanan yang memungkinkan penyerang untuk membaca atau memperbarui data internal [27]. Hal tersebut dapat terjadi setiap kali aplikasi web mengambil sumber daya jarak jauh tanpa memvalidasi URL yang diberikan pengguna [28].

Gambar 2 merupakan desain topologi yang berjalan saat ini dimana jaringan tersebut tidak memiliki Next Generation Firewall di antara router dan server. Sehingga tidak ada mekanisme yang diterapkan untuk melakukan filter atau menjaga traffic data yang mengarah ke server. Hal tersebut menyebabkan siapapun dapat melakukan akses ke server secara langsung tanpa adanya layer pertahanan atau perlindungan pertama.



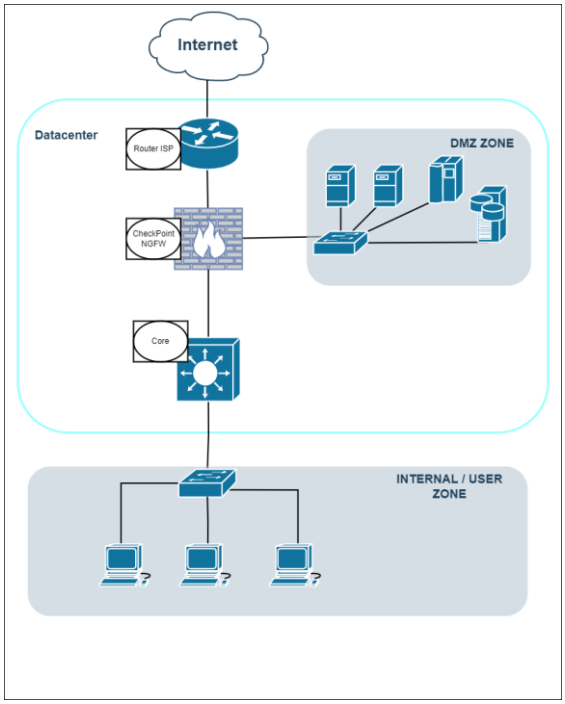
Gambar 2. Topologi Saat Ini Tanpa NGFW



Gambar 3. Serangan Terhadap Server dengan Topologi Tanpa NGFW

Gambar 3 merupakan gambaran kemungkinan darimana penyerang akan masuk dalam desain topologi tanpa *Next Generation Firewall*. Dalam gambar 3, penyerang akan masuk melalui internet (nomor 1). Kemudian penyerang akan melakukan serangan siber seperti *SQL Injection*, *XSS*, *maupun Brute Force Attack* terhadap server melalui Router ISP (nomor 2) dan Core Switch (nomor 3). Dikarenakan tidak adanya pertahanan antara internet (nomor 1) dan server (nomor 4). Maka penyerang dapat dengan mudah melakukan serangan siber terhadap server.

Gambar 4 merupakan desain topologi dimana jaringan tersebut memiliki *Next Generation Firewall* di antara router dan server yang terdapat pada *on premises*. Dengan adanya *Next Generation Firewall* diantara router dan server akan memisahkan jaringan *local private* dan *firewall* yang dapat melakukan *filtering* berdasarkan *IP Address* dan *Service Port* terhadap lalu lintas yang akan menuju ke area *DMZ Server*. Selain itu, *engine IPS* akan melakukan *inspection* terhadap lalu lintas yang tersaring oleh *engine Firewall* apakah *traffic* tersebut merupakan suatu serangan atau permintaan *request* yang *valid*. Tujuan dari semua itu adalah untuk mencegah kebocoran data yang tidak diinginkan dan *traffic* data yang mencurigakan memasuki jaringan, melindungi terhadap serangan siber dan lalu lintas berbahaya lainnya dengan memindai setiap packet data yang mencoba memasuki jaringan.



Gambar 4. Desain Topologi Dengan NGFW

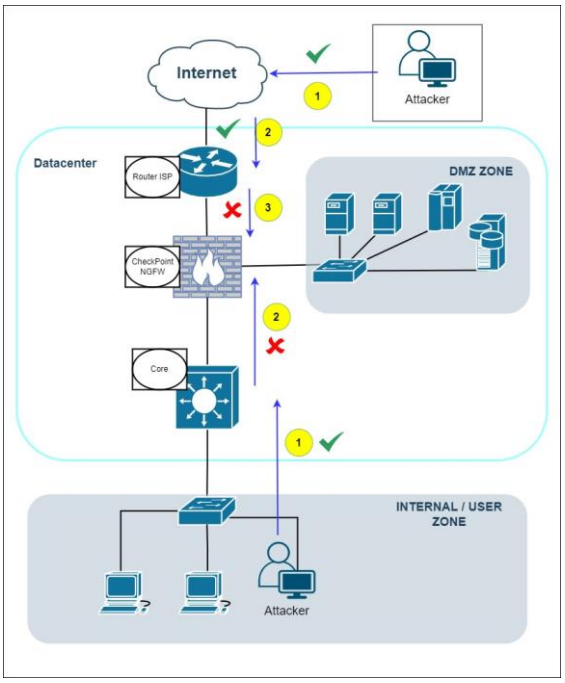
Dengan menggunakan topologi tersebut, berikut kelebihan yang akan didapatkan:

Server berada di belakang CheckPoint. Sehingga server akan jauh lebih aman apabila dibandingkan dengan desain sebelumnya. Dimana tidak terdapat NGFW yang menjadi tembok pertahanan pertama.

Server berada dalam DMZ. Dimana DMZ akan memberikan keamanan pada jaringan internal (LAN) dengan mencegah akses langsung melalui jaringan eksternal (WAN).

Server hanya dapat diakses melalui NGFW baik untuk *traffic* dari internet maupun internal. Hal tersebut merupakan tindakan preventif apabila terdapat serangan dari internal yang mengarah ke server.

Gambar 5 merupakan gambaran kemungkinan darimana penyerang akan masuk dalam desain topologi dengan menggunakan *Next Generation Firewall*.



Gambar 5. Serangan Dalam Desain Topologi Akses Server Melalui Next-Gen Firewall

Dalam Gambar 5, penyerang akan masuk melalui 2 cara, internet dan internal yang merupakan serangan dari dalam atau *internal attack* :

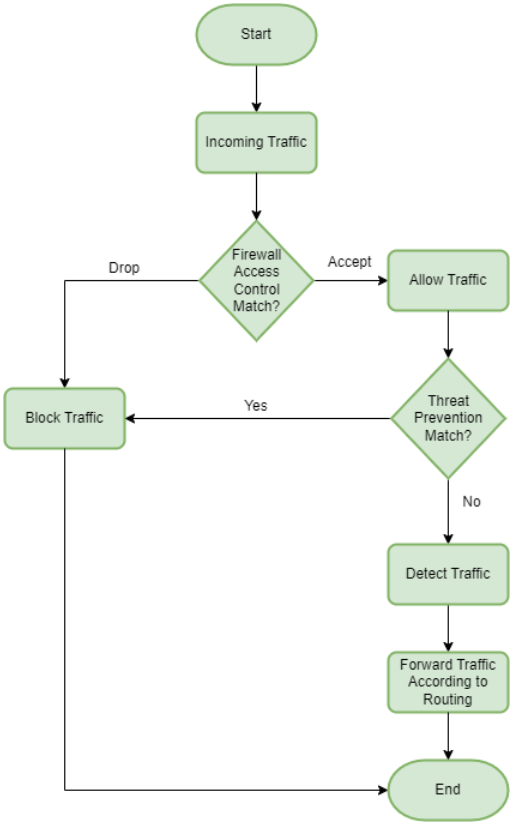
Untuk serangan melalui internet, penyerang akan melakukan serangan siber seperti *SQL Injection*, *XSS*, *maupun Brute Force Attack* terhadap server melalui Router ISP (nomor 2) dan NGFW (nomor 3). Ketika *packet* serangan tersebut sampai di NGFW, NGFW akan melakukan validasi terkait *packet* tersebut dan menemukan bahwa *packet* tersebut merupakan sebuah serangan siber, maka *packet* tersebut dilakukan *drop* oleh NGFW sehingga tidak dapat mencapai ke server.

Untuk serangan melalui internal, penyerang akan melakukan serangan siber seperti *SQL Injection*, *XSS*, maupun *Brute Force Attack* terhadap server melalui Core Switch (nomor 2) dan NGFW (nomor 3). Ketika *packet* serangan tersebut sampai di NGFW, NGFW akan melakukan validasi terkait *packet* tersebut dan

menemukan bahwa packet tersebut merupakan sebuah serangan siber, maka *packet* tersebut dilakukan *drop* oleh NGFW sehingga tidak dapat mencapai ke server.

3. Hasil dan Pembahasan

Gambar 6 merupakan alur *traffic* dalam *Next Generation Firewall*. Dimana untuk setiap *traffic* yang masuk, akan dilakukan pengecekan dengan menggunakan *rule*. Apabila traffic tersebut masuk ke dalam *rule drop*, maka *traffic* dilakukan *drop*. Apabila *traffic* masuk ke dalam *rule accept*, maka *traffic* akan diteruskan dan dicek melalui *threat prevention* yang telah dibuat. Apabila *traffic* tersebut match dengan *threat prevention*, maka *traffic* dilakukan *block*. Sedangkan apabila *traffic* tidak *match* dengan *threat prevention*, maka *traffic* akan diteruskan berdasarkan *routing table* yang ada.



Gambar 6. Serangan Dalam Desain Topologi Akses Server Melalui Next-Gen Firewall

Untuk menjalankan emulator EVE-NG dengan berbagai node, Tabel 2 merupakan spesifikasi yang digunakan:

Tabel 2.Tabel Spesifikasi Emulator EVE-NG

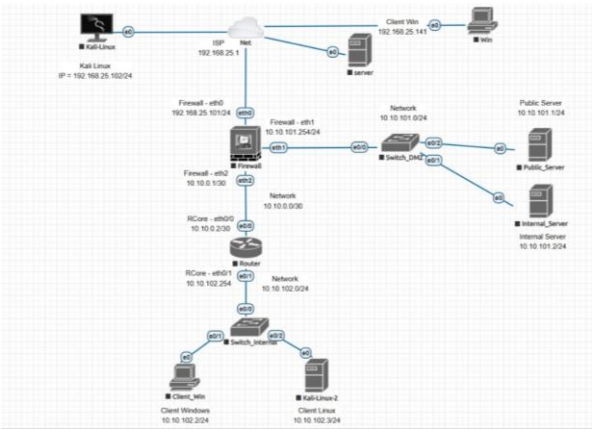
Perangkat	Spesifikasi
CPU	Intel Core i5 (2.50 Ghz)
Core	4
RAM	12 GB
Disk	150 GB

Resource tersebut digunakan untuk setiap node yang dijalankan. Tabel 3 adalah spesifikasi untuk setiap node yang digunakan:

Tabel 3.Tabel Spesifikasi Seluruh Node yang Dijalankan

Nama	CPU	RAM	Ethernet
CheckPoint Firewall	2	4 GB	4
Kali Linux	2	2 GB	1
Switch_DMZ	1024 KB (NVRAM)	1 GB	4
Public_Server	1	1 GB	1
Internal_Server	1	1 GB	1
Router	1024 KB (NVRAM)	1 GB	4
Switch_Internal	1024 KB (NVRAM)	1 GB	4
Client_Win	2	2 GB	1
Kali-Linux-2	2	2 GB	1

Pembagian IP Address dalam penelitian ini dilakukan untuk mengatur alokasi alamat IP pada setiap node atau perangkat yang terhubung. Tabel 4 adalah pembagian IP Address yang digunakan dalam implementasi jaringan.



Gambar 7. Pemetaan IP Address

Tabel 4.Tabel Pembagian IP Address

Nama Node	Port	IP Address	Gateway	Terhubung Ke	Port	Deskripsi
CheckPoint Firewall	eth0	192.168.25.101/24	192.168.25.1	ISP	eth0	Untuk Ke Ouside / Internet
CheckPoint Firewall	eth1	10.10.101.254/24	N/A	Switch DMZ	e0/0	Ke DMZ Server
CheckPoint Firewall	eth2	10.10.0.1/30	N/A	Router	e0/0	Untuk Ke Inside
Public Server	e0	10.10.101.1/24	10.10.101.254	Switch DMZ	e0/2	Server ke Gateway
Internal Server	e0	10.10.101.2/24	10.10.101.254	Switch DMZ	e0/1	Server ke Gateway
Router	e0/0	10.10.0.2/30	10.10.0.1	CheckPoint Firewall	eth2	Router ke Outisde
Router	e0/1	10.10.102.254	N/A	Switch Internal	e0/0	Router ke Inside
Client Win	e0	10.10.102.2/24	10.10.102.254	Switch Internal	e0/1	Client ke Gateway
Kali Linux 2	e0	10.10.102.3/24	10.10.102.254	Switch Internal	e0/2	Client ke Gateway

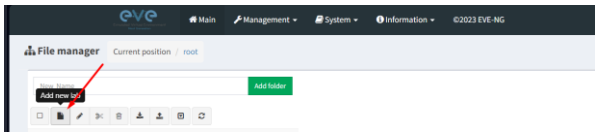
Gambar 7 adalah topologi jaringan yang menunjukkan pemetaan IP Address pada setiap node atau perangkat yang digunakan:

Berikut adalah langkah-langkah untuk membuat proyek baru pada emulator EVE-NG:

Login ke emulator EVE-NG melalui browser dengan mengakses 192.168.25.25 pada kolom url, seperti Gambar 8.

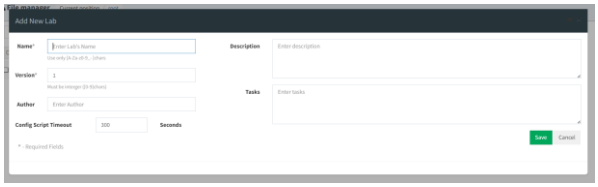
Gambar 8. Tampilan Halaman Login EVE-NG

Masukkan default credential **admin**:**eve.** Buat proyek baru dengan melakukan klik pada *add new lab* seperti Gambar 9.



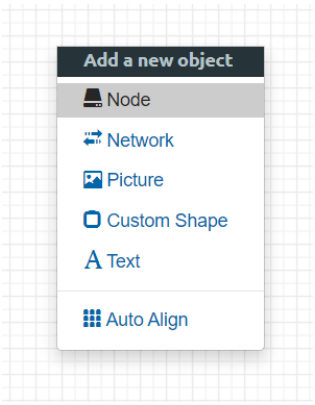
Gambar 9. Pilih Menu Add New Lab

Berikan nama pada proyek baru dan klik *save*, seperti Gambar 10.



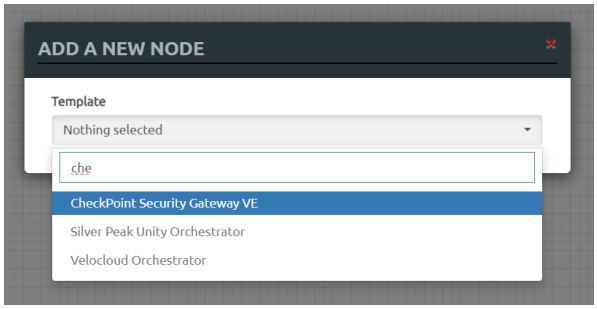
Gambar 10. Membuat Nama Proyek

Menambahkan node pada proyek dengan cara klik kanan lalu pilih node, seperti Gambar 11.



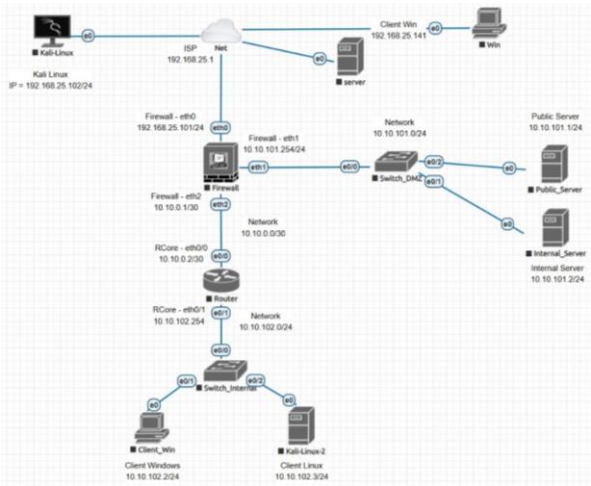
Gambar 11. Menambahkan Node

Pilih template untuk setiap node dan lakukan konfigurasi sesuai dengan Tabel 4, seperti Gambar 12.



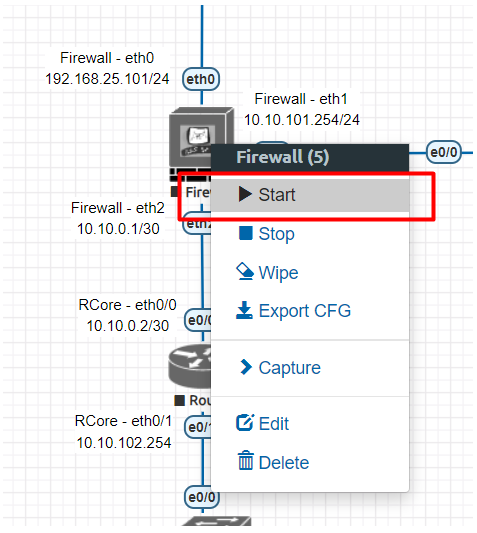
Gambar 12. Memilih Template Node

Hubungkan seluruh node mengikuti topologi pada Gambar 13.



Gambar 13. Pemetaan IP Address

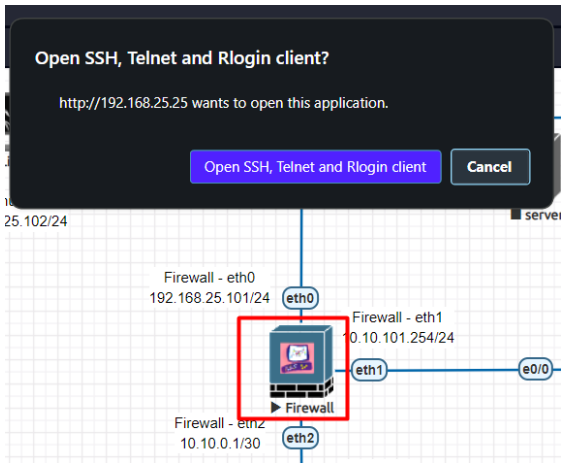
Hidupkan setiap node dengan cara klik kanan pada node, kemudian pilih start, seperti Gambar 14.



Gambar 14. Menghidupkan Node

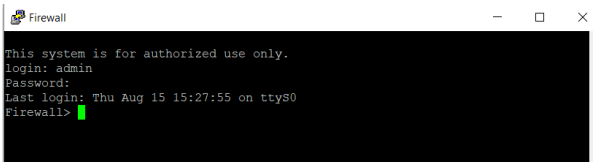
Untuk melakukan konfigurasi terhadap CheckPoint NGFW dalam penanganan atau mitigasi terhadap OWASP Top 10, berikut merupakan langkah-langkah yang dapat dilakukan:

Masuk ke command line pada CheckPoint Firewall. Akses SSH dengan cara doble klik node CheckPoint pada emulator EVE-NG, seperti Gambar 15.



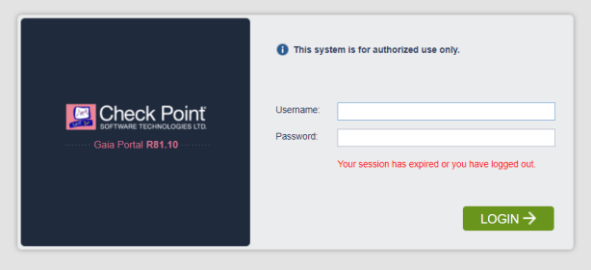
Gambar 15. Mengakses SSH

Login menggunakan *default credential* **admin**:**admin.** Seperti Gambar 16.



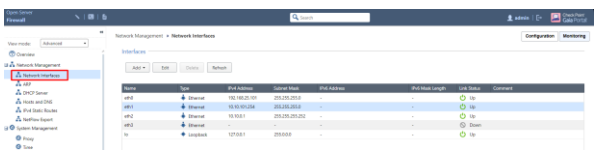
Gambar 16. Login dengan *Default Credential*

Setting IP Address menggunakan *command* berikut: set interface eth0 ipv4-address 192.168.25.101 mask-length 24; Kemudian masuk ke webui CheckPoint dengan menggunakan web browser ke alamat https://192.168.25.101, seperti Gambar 17.



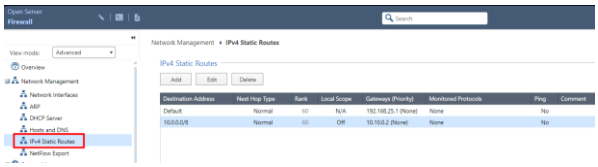
Gambar 17. Login Pada Webui CheckPoint

Setting IP Address untuk setiap interface: Masuk ke *menu Network Management > Network Interface; Double click* pada *interface;* Ceklist pada *Enable;* Masukan IPv4; Klik Ok. seperti Gambar 18.



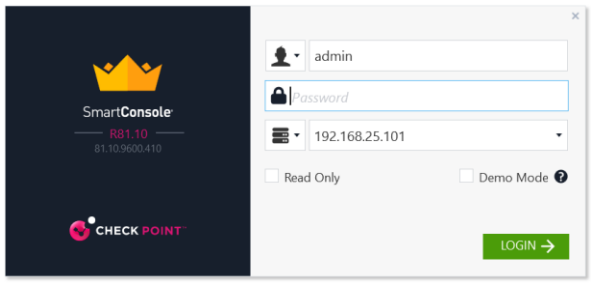
Gambar 18. Login Pada Webui CheckPoint

Konfigurasi Routing, pada menu Network Management > IPv4 Static Routes; Klik *Add* seperti Gambar 19.



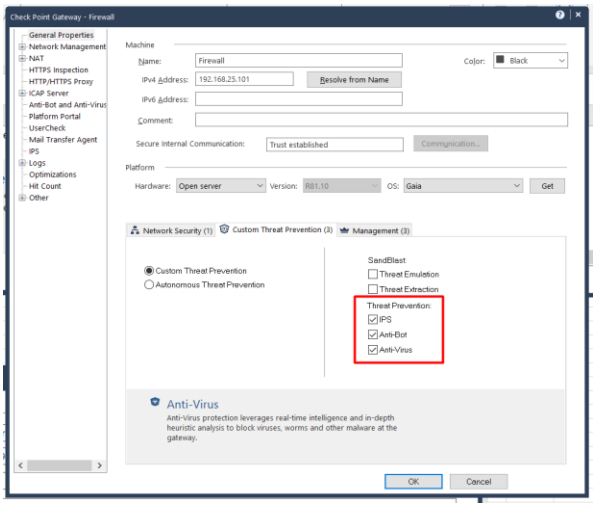
Gambar 19. Login Pada Webui CheckPoint

Login ke Checkpoint NGFW dengan SmartConsole R81.10 seperti Gambar 20.



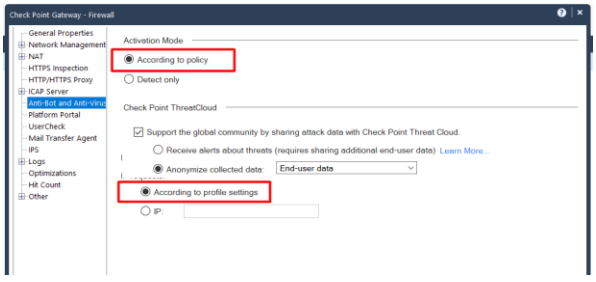
Gambar 20. Halaman Login pada CheckPoint NGFW

Double click pada *object Firewall*; Pilih *Gateway Properties > Network Security*; *Select* pada *Firewall*; Pilih *Custom Threat Prevention*; Select pada *Threat Prevention: IPS, Anti-bot & Anti-Virus* seperti Gambar 21.



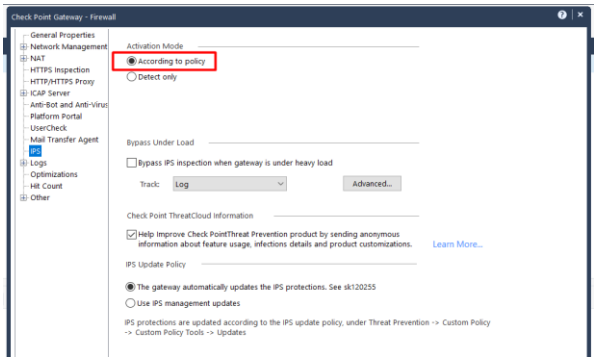
Gambar 21. *Custom Threat Prevention*

Masuk ke menu "*Anti-Bot and Anti-Virus*" lalu *select* "*According to Policy*" dan "*According to Policy*". seperti Gambar 22.



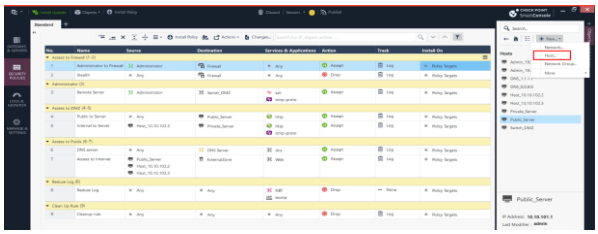
Gambar 22. Menu *Anti-Bot* and *Anti-Virus*

Masuk ke menu IPS dan Select "*According to Policy*" seperti Gambar 23.



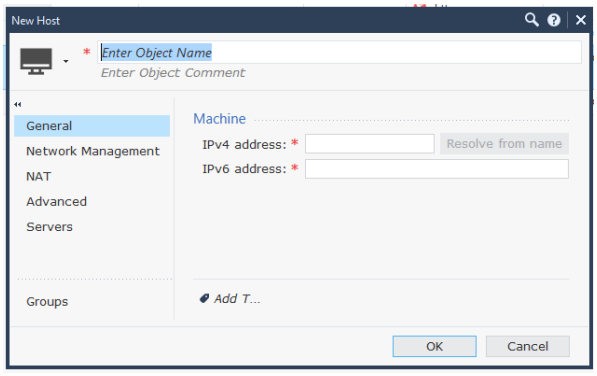
Gambar 23. Menu IPS

Klik OK; *Create Host Object* dan NAT. Pilih *Object* > *Host* > *New Host* seperti Gambar 24.



Gambar 24. *Add New Host*

Masukkan ***Object Name*** dan ***IPv4 Address*** seperti Gambar 25.

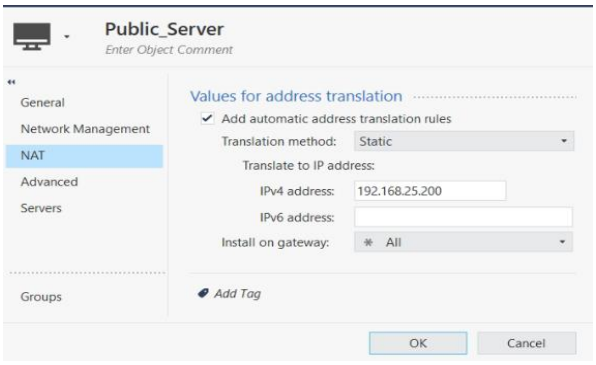


Gambar 25. *Input Object Name* dan IPv4 *Address*

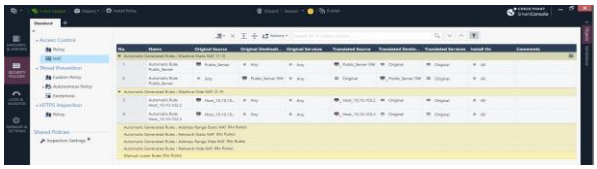
Klik tab NAT > ***Check Add automatic address translation rules***. Tentukan *method* sebagai ***static*** dan isi IPv4 address yang akan menjadi NAT IP seperti Gambar 26.

Klik **OK**. *Policy* NAT akan secara otomatis terbentuk seperti Gambar 27.

Konfigurasi Policy Pada Access Control Firewall: Access control policy merupakan komponen yang sangat penting untuk di perhatikan karena disana traffic data ditentukan dapat lewat atau di-block oleh firewall. Access Control Policy di perlukan konfigurasi dengan kontrol akses yang aman dan kinerja jaringan yang dioptimalkan.



Gambar 26. DMZ_NAT *Configuration*



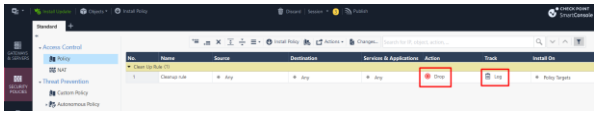
Gambar 27. Hasil *Policy* NAT

Buat *Policy Rule* sebagai aturan pembersih yang bertujuan menutup semua lalu lintas data yang tidak sesuai. Masuk ke *Security Policies* > *Access Control* > *Policy*. Buat *Policy Rule* dan bagian baru dengan nama *Clean Up Rule* seperti pada Tabel 5.

Tabel 5. Policy Rule

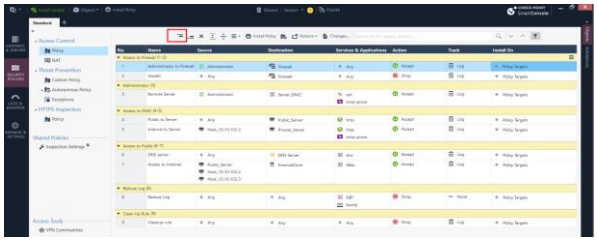
Name	Source	Destination	Service	Action	Track
Cleanup Rule	Any	Any	Any	Drop	Log

Name adalah Nama dari aturan, *Source* merupakan dari mana sumber lalu lintas, *Destinatio* merupakan tujuan dari lalu lintas, *Service* adalah *port* yang akan di akses dari *source*, *Action* adalah Tindakan yang harus dilakukan, *Track* berfungsi sebagai tindakan apakah *firewall* harus mencatat *log* lalu lintas ke dalam penyimpanan, *Any* adalah value yang mengartikan sebagai semua atau apapun seperti Gambar 28.



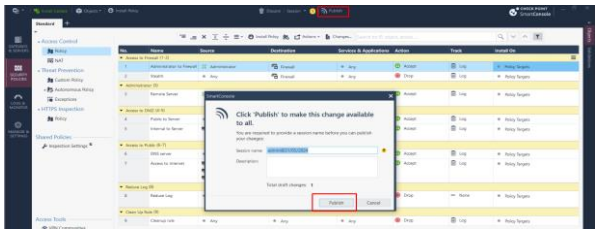
Gambar 28. Hasil *Policy Rule*

Buat section title dan aturan lainnya untuk mengizinkan traffic dengan memposisikan diatas aturan Cleanup Rule seperti Gambar 29.



Gambar 29. Section Title

Tekan *publish* pada *pop up* yang muncul seperti Gambar 30.

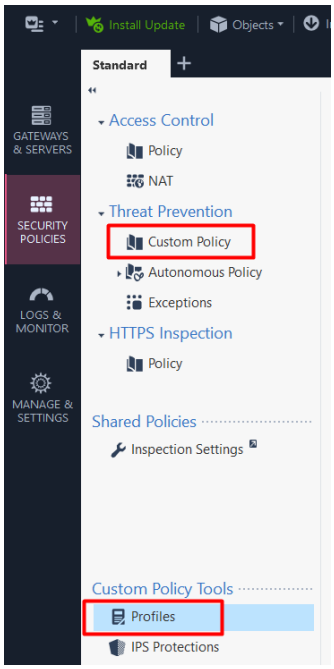


Gambar 30. Tekan Publish pada Pop Up

3.4. Konfigurasi Policy Pada Threat Prevention

Policy threat prevention merupakan elemen krusial dalam menjaga keamanan jaringan dari berbagai ancaman dan serangan siber. Dengan konfigurasi yang tepat, *policy threat prevention* mampu mendeteksi dan memitigasi ancaman sebelum mereka dapat merusak sistem. Penting untuk memastikan bahwa konfigurasi ini tidak hanya melindungi dari serangan, tetapi juga menjaga kinerja jaringan tetap optimal.

Masuk ke Security Policies > Threat Prevention > Custom Policy > Profiles seperti Gambar 31.



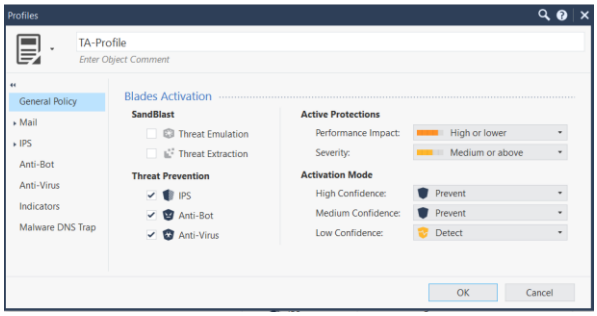
Gambar 31. Menu *Custom Policy Profiles*

Membuat *profile* baru untuk konfigurasi *Threat Prevention* dengan cara: klik * (New). Masukan nama *profile* dan centang pada bagian T*hreat Prevention*: *IPS, Anti-Bot* dan *Anti-Virus*. Pada *Genernal Policy* > *Active Protections & Activation Mode* seperti Gambar 32.

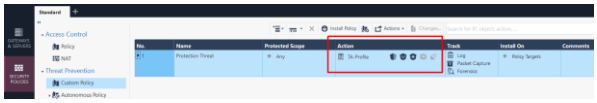
Klik OK. Masuk ke Security Policies > Threat Prevention > Custom Policy. Tambahkan Rule menggunakan Profile TA-Profile seperti Gambar 33.

Install Policy untuk memasang semua konfigurasi seperti Gambar 34.

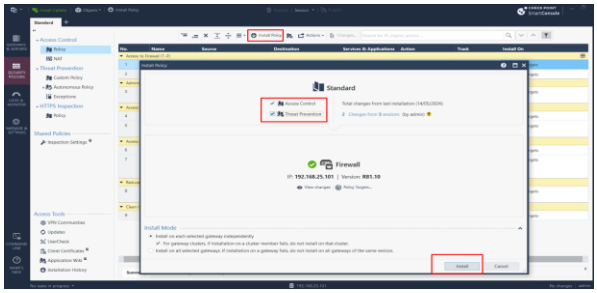
Pengujian Terhadap Serangan Siber: Untuk melihat bahwa topologi dengan menggunakan Next Generation Firewall dapat lebih baik dalam melakukan pencegahan serangan siber, penulis melakukan perbandingan dengan melakukan simulasi serangan siber terhadap topologi tanpa Next Generation Firewall dengan topologi dengan menggunakan Next Generation Firewall. Serangan siber dilakukan dengan metode SQL Injection, XSS (Cross Site Scripting), serta Brute Force.



Gambar 32. Hasil Profile



Gambar 33. Menambahkan Rule pada Profile TA-Profile



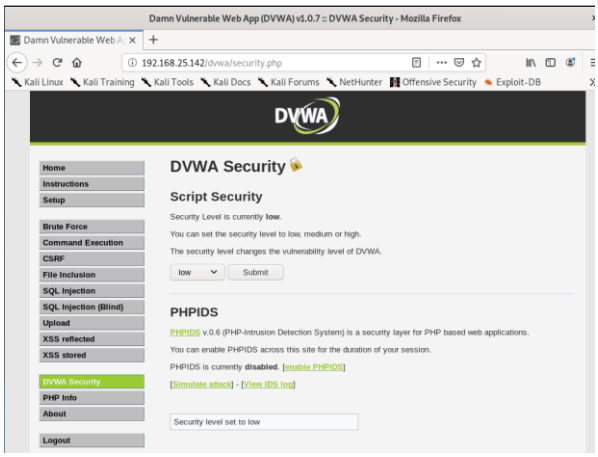
Gambar 34. Install Policy

Pengujian Topologi Tanpa Next Generation Firewall Terhadap Serangan Siber: Simulasi serangan siber yang dilakukan terhadap topologi tanpa Next Generation Firewall dilakukan secara manual untuk SQL Injection dan XSS (Cross Site Scripting), sedangkan untuk Brute Force akan dilakukan dengan menggunakan tools Hydra.

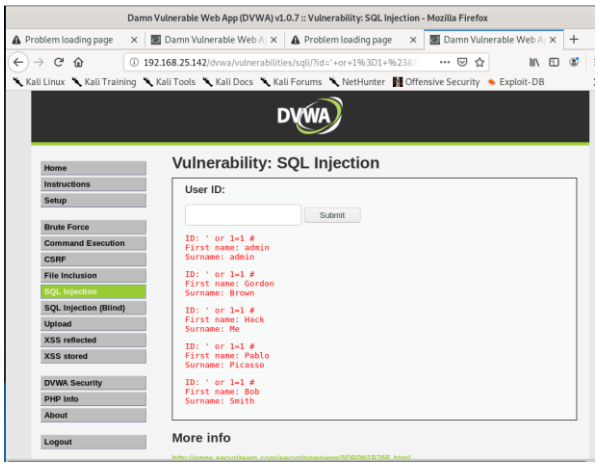
Pada web aplikasi target, DVWA (Damn Vulnerable Web Application), telah diatur dengan konfigurasi *security low* atau paling rendah seperti Gambar 35. Hal tersebut ditujukan agar pengamanan yang digunakan hanya berdasarkan pada topologi itu sendiri, yang berarti tidak ada pengamanan sama sekali.

SQL Injection: Untuk melakukan simulasi serangan siber dengan SQL Injection, penulis mencoba menggunakan ' or 1=1 # sebagai input pada User Id seperti Gambar 36.

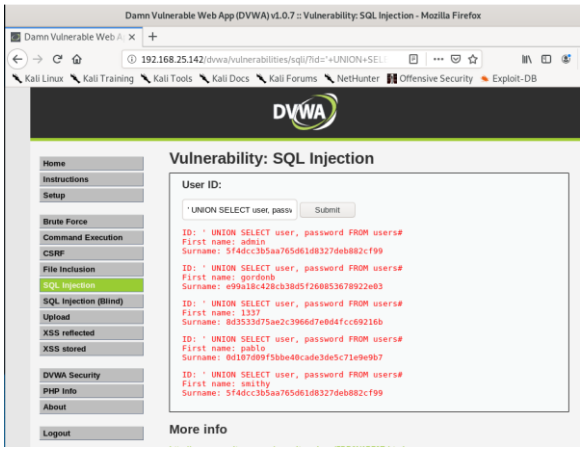
Pada Gambar 37 terlihat bahwa input tersebut membuat penyerang dapat melihat seluruh data dalam *table*. Selain itu penulis juga mencoba menggunakan `' UNION SELECT user, password FROM users#` sebagai *input*.



Gambar 35. Konfigurasi Security DVWA Pada Topologi Tanpa *Next Generation Firewall*



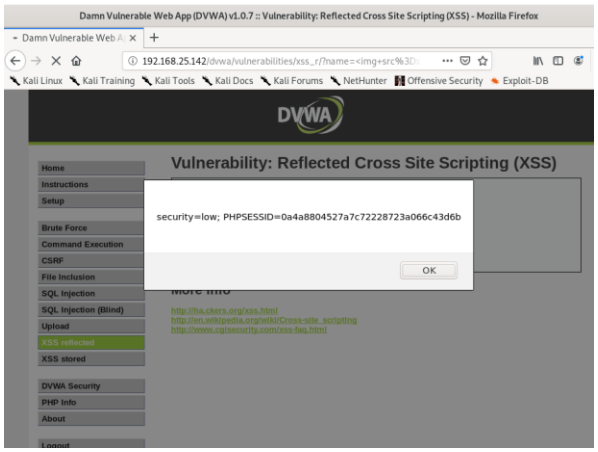
Gambar 36. ' or 1=1 # Sebagai Input Pada Topologi Tanpa Next Generation Firewall



Gambar 37. ' UNION SELECT user, password FROM users# Sebagai Input Pada Topologi Tanpa Next Generation Firewall

Pada Gambar 37 terlihat bahwa *input* tersebut dapat membuat penyerang dapat melihat *username* dan juga *password* yang ditampilkan dalam *surname*. Hal tersebut menunjukkan bahwa web aplikasi memiliki kerentanan terhadap serangan siber SQL Injection.

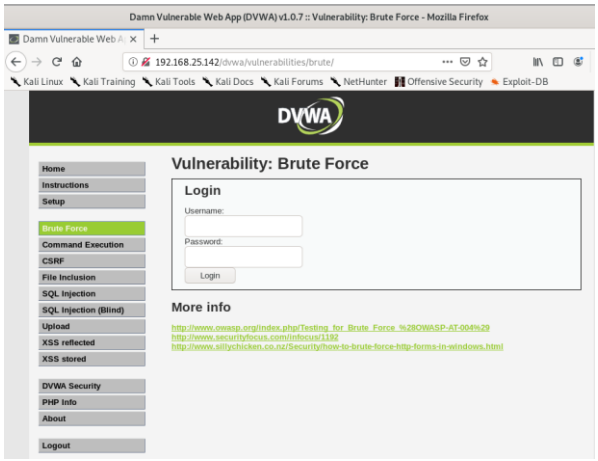
Untuk melakukan simulasi serangan siber dengan XSS (Cross Site Scripting), penulis mencoba menggunakan `<img src=x onerror="alert(document.cookie)">` sebagai *input*. *Input* tersebut akan membuat web aplikasi menampilkan *alert* dengan nilai *cookie* pengguna.



Gambar 38. Menampilkan Cookie Pada Topologi Tanpa Next Generation Firewall

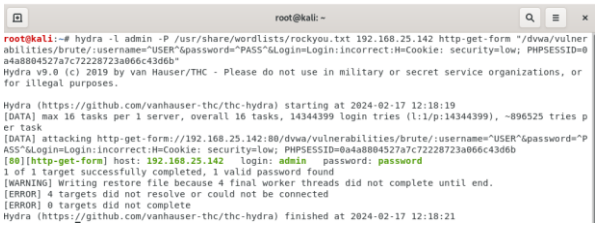
Pada Gambar 38 terlihat bahwa web aplikasi menampilkan *alert* dengan nilai *cookie* pengguna. Hal tersebut menunjukkan bahwa web aplikasi memiliki kerentanan terhadap serangan siber XSS (Cross Site Scripting).

Untuk melakukan simulasi serangan siber dengan Brute Force, penulis mencoba menggunakan *tools* hydra dengan *wordlist* rockyou yang menyimpan berbagai kemungkinan *credential* yang digunakan.



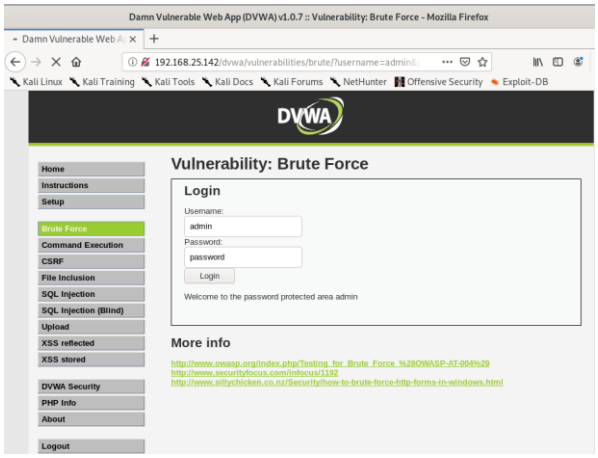
Gambar 39. Tampilan Awal Web Aplikasi Untuk Brute Force Pada Topologi Tanpa Next Generation Firewall

Pada Gambar 39 terlihat tampilan awal web aplikasi untuk simulasi serangan siber *brute force*. Tampilan tersebut memungkinkan pengguna untuk memasukkan *username* dan *password* untuk *login*. Apabila *username* dan *password* sesuai dengan salah satu pengguna yang telah disimpan datanya, maka akan pengguna akan berhasil *login*.



Gambar 40. Menggunakan Tools Hydra Pada Topologi Tanpa Next Generation Firewall

Pada Gambar 40, penulis menggunakan *tools* Hydra, dengan menggunakan *wordlist* rockyou, *cookie* dan akan berhenti apabila web aplikasi tidak memberikan *string* "*incorrect*". Dari menggunakan *tools* tersebut, penulis berhasil mendapatkan credential *user* admin dengan *password* "password".

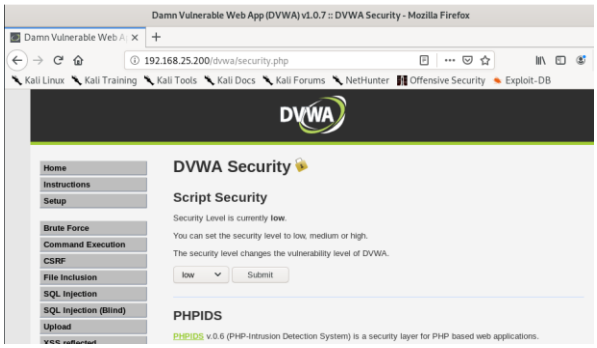


Gambar 41. Hasil Login dengan Menggunakan Credential yang Ditemukan Pada Topologi Tanpa Next Generation Firewall

Ketika penulis mencoba login pada Gambar 41 dengan menggunakan *credential* yang didapatkan dengan *tools* Hydra, web aplikasi memberikan nilai "*Welcome to the password protected area admin*" yang berarti *credential* yang ditemukan merupakan *credential* yang *valid*. Hal tersebut menunjukkan bahwa web aplikasi memiliki kerentanan terhadap serangan siber Brute Force.

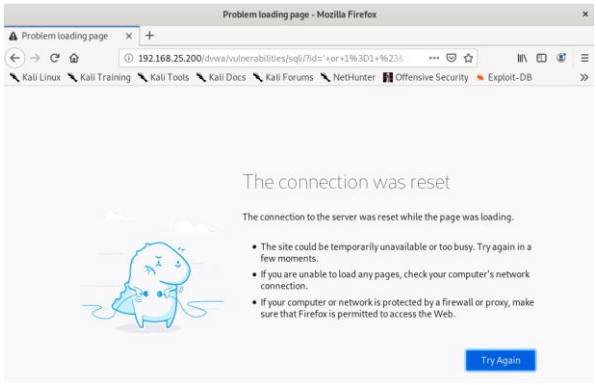
Pengujian Topologi Dengan Menggunakan Next Generation Firewall Terhadap Serangan Siber: Simulasi serangan siber yang dilakukan terhadap topologi dengan menggunakan *Next Generation Firewall* dilakukan secara manual untuk SQL Injection dan XSS (Cross Site Scripting), sedangkan untuk Brute Force akan dilakukan dengan menggunakan *tools* Hydra.

Pada web aplikasi target, DVWA (Damn Vulnerable Web Application), telah diatur dengan konfigurasi *security low* atau paling rendah. Hal tersebut ditujukan agar pengamanan terhadap web aplikasi hanya mengandalkan *Next Generation Firewall* yang telah terimplementasi pada topologi dengan posisi NGFW yang tepat seperti Gambar 42.

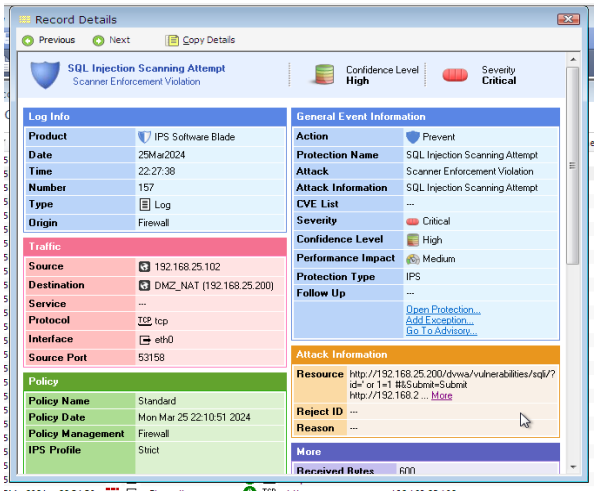


Gambar 42. Konfigurasi Security DVWA Pada Topologi dengan Menggunakan Next Generation Firewall

Untuk melakukan simulasi serangan siber dengan SQL Injection, penulis mencoba menggunakan `' or 1=1 #` sebagai input pada User Id seperti yang telah dilakukan pada topologi tanpa *Next Generation Firewall* seperti Gambar 43.

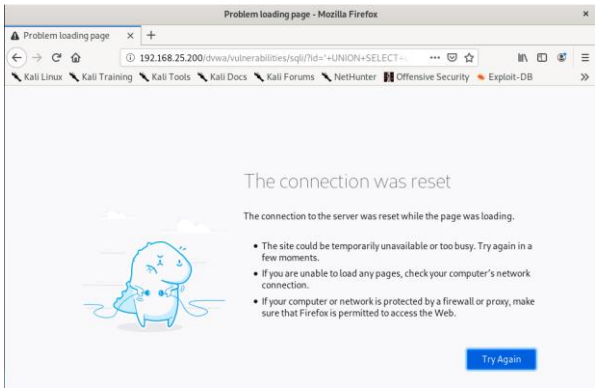


Gambar 43. ' or 1=1 # Sebagai Input Pada Topologi dengan Menggunakan Next Generation Firewall

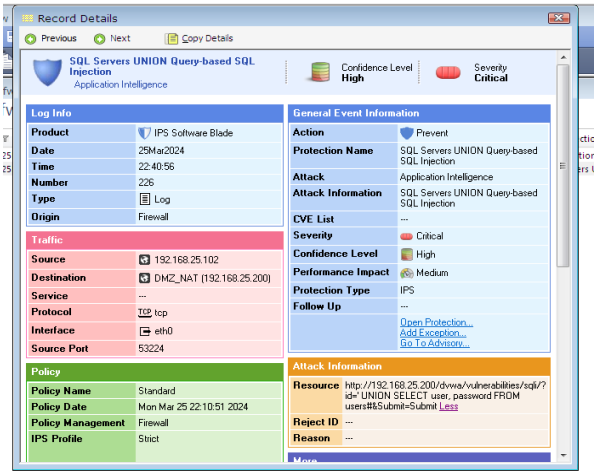


Gambar 44. Log Blocking pada NGFW dengan Input ' or 1=1 #

Pada Gambar 43 terlihat bahwa *input* tersebut membuat web aplikasi melakukan *drop* terhadap *traffic* yang mengarah ke tampilan SQL Injection. Kondisi *traffic* yang di-*drop* dikonfirmasi pada Gambar 44. Hal tersebut membuat penulis tidak dapat mengakses tampilan SQL Injection yang seharusnya menampilkan seluruh data dalam *table*.



Gambar 45. ' UNION SELECT user, password FROM users# Sebagai Input Pada Topologi dengan Menggunakan Next Generation Firewall

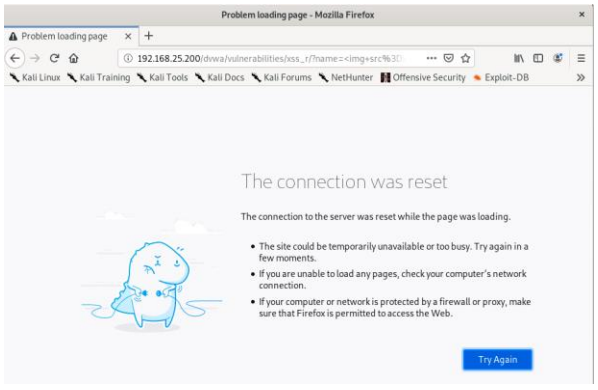


Gambar 46. Log Blocking pada NGFW dengan Input ' UNION SELECT user, password FROM users#

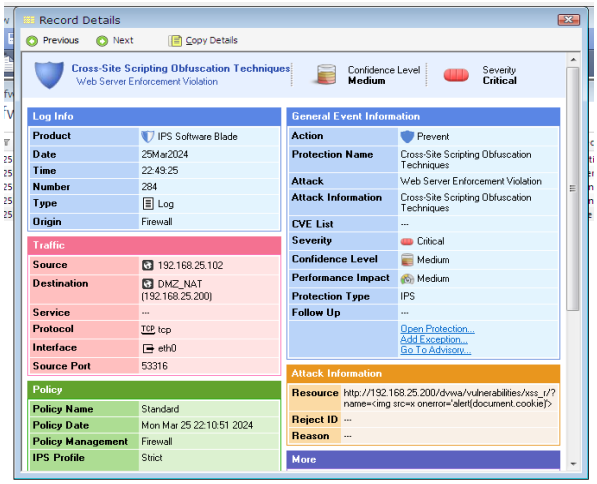
Begitupula sama halnya ketika penulis menggunakan `' UNION SELECT user, password FROM users#` sebagai input. Ketika input tersebut digunakan pada topologi tanpa *Next Generation Firewall*, maka web aplikasi akan memberikan *username* dan juga *password*-nya. Namun ketika digunakan pada topologi dengan menggunakan *Next Generation Firewall* seperti pada Gambar 45, web aplikasi melakukan *drop* terhadap *traffic* yang mengarah ke tampilan SQL Injection. Kondisi *traffic* yang di-*drop* dikonfirmasi pada Gambar 46. Hal tersebut membuat web aplikasi tidak menampilkan hasil yang seharusnya didapatkan melalui SQL Injection.

Untuk melakukan simulasi serangan siber dengan XSS (Cross Site Scripting), penulis mencoba menggunakan `<img src=x onerror="alert(document.cookie)">` sebagai *input* seperti yang digunakan pada topologi tanpa *Next Generation Firewall*.

Pada Gambar 47 terlihat bahwa *input* tersebut membuat web aplikasi melakukan *drop* terhadap *traffic* yang mengarah ke tampilan XSS. Kondisi *traffic* yang di-*drop* dikonfirmasi pada gambar 48. Hal tersebut membuat penulis tidak mendapatkan hasil *alert* yang seharusnya muncul seperti pada topologi tanpa *Next Generation Firewall*.



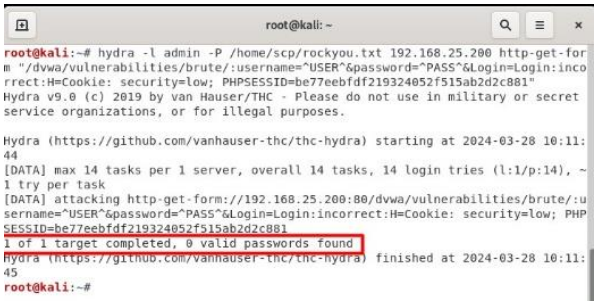
Gambar 47. <img src=x onerror="alert(document.cookie)"> Sebagai Input Pada Topologi dengan Menggunakan Next Generation Firewall



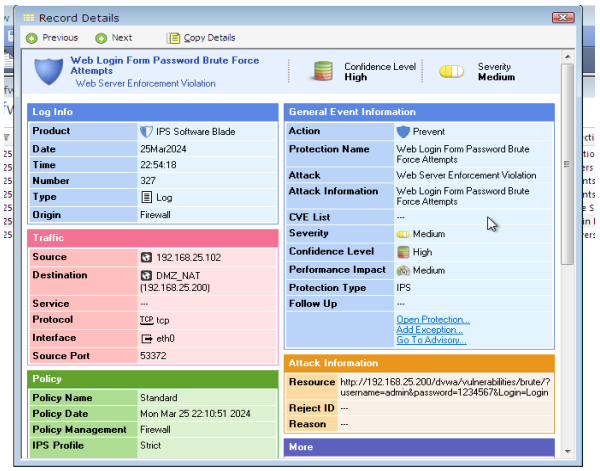
Gambar 48. Log Blocking pada NGFW dengan Input <img src=x onerror="alert(document.cookie)">

Untuk melakukan simulasi serangan siber dengan Brute Force, penulis mencoba menggunakan *tools* hydra dengan *wordlist* rockyou yang menyimpan berbagai kemungkinan *credential* yang digunakan.

Pada Gambar 49 terlihat bahwa *tools* Hydra terus berjalan hingga akhir *wordlist* rockyou dan tidak menemukan hasilnya. Hal tersebut terjadi karena NGFW melakukan *drop* terhadap seluruh traffic yang dideteksi merupakan *brute force*. Kondisi *traffic* yang di-*drop* dikonfirmasi pada Gambar 50.



Gambar 49. Menggunakan Tools Hydra Pada Topologi dengan Menggunakan Next Generation Firewall



Gambar 50. Log Blocking pada NGFW ketika Brute Force

Evaluasi Perbandingan Hasil Serangan Siber Antara Topologi Tanpa Next Generation Firewall dengan Topologi dengan Menggunakan Next Generation Firewall: Berdasarkan simulasi serangan siber terhadap topologi tanpa *Next Generation Firewall* dan topologi dengan menggunakan *Next Generation Firewall*. Dimana kedua topologi tersebut memiliki *security level* pada tingkatan *low*. Tabel 6 merupakan perbandingan serangan siber terhadap topologi tanpa *Next Generation Firewall* dan topologi dengan menggunakan *Next Generation Firewall*:

Tabel 5. Perbandingan Serangan Siber Terhadap Topologi Jaringan

No	Serangan Siber	Tanpa Next Generation Firewall	Next Generation Firewall
1.	SQL Injection dengan input ' or 1=1 #	✕	✓
2.	SQL Injection dengan input ' UNION SELECT user, password FROM users#	✕	✓
3.	XSS (Cross Site Scripting) dengan input <img src=x onerror= "alert(document.cookie)">	✕	✓
4.	Brute Force	✕	✓

Hasil dari simulasi serangan siber tersebut menunjukkan bahwa Next Generation Firewall yang dirancang dengan baik dapat membantu mencegah serangan siber yang mungkin terjadi. Dimana dengan adanya Next Generation Firewall lebih efektif untuk mencegah serangan siber sebesar 100% terhadap pengujian yang telah dilakukan.

4. Kesimpulan

Berdasarkan proses perancangan, pembuatan, pengujian, dan evaluasi yang telah dilakukan pada topologi tanpa *Next Generation Firewall* dan dengan menggunakan *Next Generation Firewall*. Topologi jaringan untuk *Next Generation Firewall* (*NGFW*) telah berhasil dirancang dengan menggunakan CheckPoint *Next Generation Firewall*. Topologi dengan menggunakan *Next Generation Firewall* dapat berjalan dengan efektif sesuai dengan rancangan untuk melakukan pencegahan terhadap serangan siber. Hal ini didasari oleh hasil evaluasi perbandingan hasil antara pengujian topologi tanpa *Next Generation Firewall* terhadap serangan siber dengan pengujian topologi dengan menggunakan *Next Generation Firewall*. Topologi dengan menggunakan *Next Generation Firewall* dapat berjalan dengan baik sesuai dengan rancangan untuk membatasi akses *traffic* data dan memblokir serangan siber. Hal ini didasari oleh hasil pengujian topologi dengan menggunakan *Next Generation Firewall*.

Daftar Rujukan

[1] R. S. Deora and D. Chudasama, "Brief Study of Cybercrime on an Internet," Journal of Communication Engineering & Systems, vol. 11, no. 1, 2021.a
[2] "What is OWASP? What is the OWASP Top 10?," Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/security/threats/owasp-top-10/. [Accessed 20 Juni 2023].
[3] "NDLC (Network Development Life Cycle)," Cerita Hosting, 2021. [Online]. Available: https://ceritahosting.com/2021/08/04/ndlc-network-development-life-cycle/.
[4] N. Provos, Encyclopedia of Cryptography and Security, Boston: Springer, 2005.
[5] J. Heino, A. Hakkala and S. Virtanen, "Study of Methods for Endpoint Aware Inspection in A Next-Generation Firewall," Cybersecurity, vol. 5, 27 Juli 2022.
[6] "PHINTRACO GROUP," 27 Juli 2021. [Online]. Available: https://phintraco.com/perbedaan-next-generation-firewall-dan-firewall-tradisional/. [Accessed 20 Juni 2023].
[7] B. Posey, "WhatIs.com," [Online]. Available: https://www.techtarget.com/whatis/definition/server. [Accessed May 2023].
[8] R. Suwanto, I. Ruslianto and M. Diponegoro, "Implemetasi Intrusion Prevention System (IPS) Menggunakan SNORT dan IPTABLE Pada Monitoring Jaringan Lokal Berbasis Website," Jurnal Komputer dan Aplikasi, vol. 7, pp. 97-107, 2019.
[9] "VMWARE," [Online]. Available: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html. [Accessed 05 June 2023].
[10] M. Patel, "Demilitarized Zone: An Exceptional Layer of Network Security to Mitigate DDoS Attack," Electronic Theses and Dissertations, 2020.
[11] S. Shrimali, "DeMilitarized Zone: Network Architecture for Information Security," International Journal of Computer Applications, vol. 174, no. 5, 2017.
[12] "SQL injection," PortSwigger, [Online]. Available: https://portswigger.net/web-security/sql-injection.
[13] "Cross Site Scripting (XSS)," OWASP, [Online]. Available: https://owasp.org/www-community/attacks/xss/.
[14] "FORTINET," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/brute-force-attack. [Accessed 5 6 2023].
[15] "What is OWASP? What is the OWASP Top 10?," Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/security/threats/owasp-top-10/.
[16] "OWASP Top Ten," The OWASP® Foundation, [Online]. Available: https://owasp.org/www-project-top-ten/.
[17] "A01:2021 – Broken Access Control," The OWASP® Foundation, [Online]. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/.
[18] "OWASP Top Ten: Cryptographic Failures," PentestPeople, [Online]. Available: https://www.pentestpeople.com/blog-posts/owasp-top-ten-cryptographic-failures.

[19] "OWASP Top 10: Injection," Sypnopsys, [Online]. Available: https://www.synopsys.com/blogs/software-security/owasp-top-10-injection.html.
[20] "A04:2021 – Insecure Design," The OWASP® Foundation, [Online]. Available: https://owasp.org/Top10/A04_2021-Insecure_Design/.
[21] "OWASP Top 10 – #4 Insecure Design," Foresite CyberSecurity, [Online]. Available: https://foresite.com/blog/owasp-top-10-insecure-design/.
[22] "Security Misconfiguration: Impact, Examples and Prevention," Balbix, [Online]. Available: https://www.balbix.com/insights/security-misconfiguration-impact-examples-and-prevention/.
[23] "Vulnerable and outdated components," Synk, [Online]. Available: https://learn.snyk.io/lesson/vulnerable-and-outdated-components/.
[24] "OWASP Top Ten – #7 Identification and Authentication Failures," Foresite, [Online]. Available: https://foresite.com/blog/owasp-top-ten-7-identification-and-authentication-failures/.
[25] "A08:2021 – Software and Data Integrity Failures," The OWASP® Foundation, [Online]. Available: https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/.
[26] "OWASP Top Ten: #9 Security Logging and Monitoring Failures," Foresite, [Online]. Available: https://foresite.com/blog/owasp-top-ten-9-security-logging-and-monitoring-failures/.
[27] "OWASP Top 10 – #10 Server-Side Request Forgery," Foresite, [Online]. Available: https://foresite.com/blog/owasp-top-10-10-server-side-request-forgery/.
[28] "A10:2021 – Server-Side Request Forgery (SSRF)," The OWASP® Foundation, [Online]. Available: https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/.