Digital Transformation Technology (Digitech) | e-ISSN : 2807-9000
Volume 3, **Number** 1, Maret 2023
https://doi.org/10.47709/digitech.v3i1.2766

Analisa Pengembangan Keamanan Menggunakan Stateful Inspection dan Metode Semi Deskriptif

Rhandy Elfandiar[1*], Tata Sutabri[2]
[1,2,]Universitas Bina Darma Palembang, Indonesia,
[1]dhedek.polskyti@gmail.com, [2]tata.sutabri@gmail.com

Histori Artikel:
Diajukan: 24 Agustus 2023
Disetujui: 25 Agustus 2023
Dipublikasi: 26 Agustus 2023

Kata Kunci:
Keamanan; Website; Stateful Inspection; Website; Semi Deskriptif

Abstrak
Serangan siber terhadap aplikasi web semakin berkembang dengan cepat, mengancam keamanan dan kerahasiaan data. Keamanan website telah menjadi isu yang semakin mendesak dalam era digital saat ini. Dengan semakin kompleksnya ancaman siber, perlindungan terhadap integritas dan kerahasiaan data pengguna serta kelancaran operasional website menjadi sangat penting. Solusi keamanan yang efektif diperlukan untuk menghadapi tantangan ini. Salah satu solusi yang menjanjikan adalah penggunaan stateful inspection, yang memungkinkan inspeksi mendalam terhadap lalu lintas jaringan dan pemantauan status koneksi. Kami akan membahas analisa mengenai stateful inspection sebagai upaya perlindungan terhadap ancaman keamanan pada jaringan tempat berjalannya website yamg pada penelitian ini kami mengambil objek pada Dinas Pemberdayaan Masyarakat dan Desa di Kabupaten Musi Banyuasin. serta dampak positif yang dihasilkan dalam meningkatkan keamanan dan ketersediaan layanan web. Penelitian ini bertujuan untuk menganalisa metode keamanan website menggunakan stateful inspection dengan pendekatan semi deskriptif, yang mengintegrasikan analisis teknis dan pendekatan konseptual untuk meningkatkan keamanan serta mendeteksi potensi ancaman.

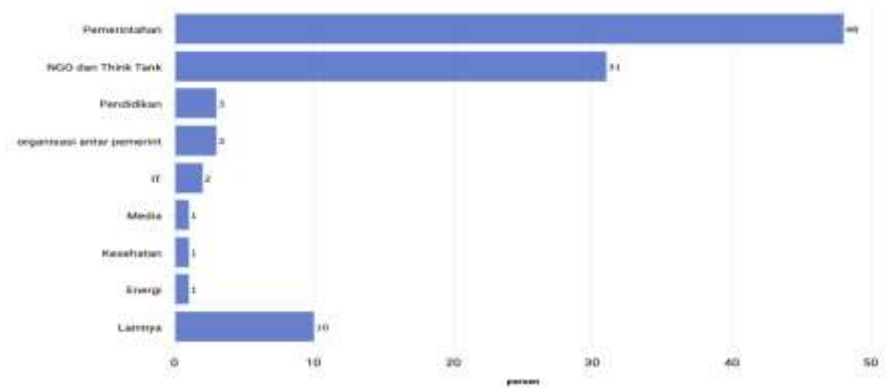
PENDAHULUAN

Berkembangnya penggunaan teknologi yang semakin meningkat beriringan dengan kemajuan informasi. Informasi dan berita yang dahulu kita dapatkan melalui media cetak, berpindah dan dtampilkan ke dalam teknologi. Informasi dan transaksi elektronik lainnya menjadi mudah, cepat dan terkini karena akses dibuka dan dilakukan pada media digital (Sutabri, 2012). Dengan perkembangan teknologi informasi saat ini, aplikasi website bagian utama dari kehidupan kita. Hal ini memberikan dampak positif bahwa perkembangan dan perubahan teknologi yang kian maju, membuat pada kemudahan terhadap kehidupan manusia (Pratama & Sutabri, 2023).

Digitalisasi teknologi maupun transaksi elektronik yang diolah secara digital membuat setiap aspek dan bidang organisasi maupun industri terpanggil untuk memanfaatkan segala aspek yang dapat memakai teknologi (Sutabri, 2012), termasuk instansi pemerintahan. Tetapi, selain mengggunakan teknologi sebagai media informasi, instansi pemerintahan juga perlu memperhatikan hal lain, terutama tentang keamanan informasi. Hal ini harus diperhatikan agar informasi yang dihasilkan dari teknologi yang ada tidak menjadi sumber masalah baru, misalnya informasi tersebut dicuri, lalu diolah sebagai ancaman yang diarahkan pada kepentingan tertentu yang merugikan.

Informasi yang menarik perhatian bahwa belakangan yang menjadi pembicaraan publik yaitu data instansi pemerintahan yang diretas lalu dibocorkan. Pelaku peretasan ini setidaknya mengungkap sembilan data milik Badan Usaha Milik Negara (BUMN), lembaga/kementerian, termasuk data para pejabat Indonesia. Lalu sejumlah data tersebut dijual. Menurut data Microsoft Digital Defense Report 2021, data pemerintahan Indonesia menjadi sasaran serangan peretasan. Microsoft menyebut, serangan ke sektor pemerintah sebagian besar difokuskan pada kementerian urusan luar negeri dan entitas pemerintah global lainnya yang terlibat dalam urusan luar negeri. Tercatat, sebanyak 48% serangan peretasan menyasar institusi pemerintahan (Mutia, 2022).

Serangan yang tertuju keamanan sistem teknologi informasi pada saat ini terjadi umumnya dilakukan oleh sekelompok orang yang ingin dan bertujuan untuk mencari, meperoleh, mengubah, dan bahkan membuang informasi tersebut hingga dijual pada pihak yang membutuhkan (Vidya, et al., 2020). Data Institusi yang Paling Rawan Terancam Serangan Hacker tersebut dapat dilihat pada Gambar 1.



Gambar 1. Data Institusi yang Paling Rawan Terancam Serangan Hacker
Sumber: (Mutia, 2022)

Hasil data survei yang dirilis National Cyber Security Index (NCSI) pada Maret 2022 yang dapat dilihat pada Gambar 2 dibawah ini, menampilkan indeks keamanan siber Indonesia ada di peringkat ke-6 se Asia Tenggara. Jika membandingkan Indonesia dengan negara-negara di Kawasan Asia Tenggara, indeks keamanan siber di Indonesia berada pada skor 38,96 poin. Posisi tertinggi ditempati oleh Malaysia dengan yang mencapai skor 79,22 poin. Dikuti oleh Singapura 71,43 poin, dan Thailand 69,94 poin. (Alifah, 2022). Berdasarkan data laporan yang diperoleh dari Badan Siber dan Sandi Negara (BSSN), ada lebih dari 1,6 miliar anomali trafik keamanan siber yang tercatat mulai dari Januari hingga Desember 2021. Angka tersebut meningkat mendekati sekitar empat kali lipat dari angka pada tahun 2020 yang ketika itu ancaman serangan siber di Indonesia berjumlah 495 juta (Naurah, 2022).

Gambar 2. Daftar Indeks Keamanan Siber Negara Asia Tenggara 2022

Sumber: (Alifah, 2022)

Stateful inspection merupakan bagian dari metode penyaringan di dalam *firewall* yang sering digunakan untuk menyaring paket data yang bekerja pada permintaan dan pengiriman pada jaringan internet sebagai solusi yang menjanjikan dengan kemampuan untuk melindungi topologi dan infrastruktur jaringan yang menjalankan aplikasi web (Vidya, et al., 2020). *Stateful* bertanggung jawab untuk melacak dan mengidentifikasi status lalu lintas jaringan berdasarkan perilaku dan aliran jaringan, untuk memantau dan mengamankan jaringan aplikasi web melibatkan tindakan untuk melindungi aplikasi dari berbagai serangan yang berpotensi merusak dan mengambil keuntungan dari celah keamanan dalam kode aplikasi untuk mencuri data pengguna atau merusak fungsionalitas dengan memeriksa konten lalu lintas dan memantau status koneksi dan lalu lintas data yang melewati *firewall* (Senthil, et al., 2022).

Dengan kata lain, proses yang dilakukan *stateful* akan berpengaruh terhadap kinerja sistem, karena akan melihat dan mengecek informasi dan status yang dimiliki dari paket tersebut, misalnya *IP Address* yang dituju, *port number* yang dituju, termasuk *connection state* (Mulia, et al., 2018). Hal ini tentu membuat sistem keamanan

pada sebuah jaringan memiliki kemanan yang semakin baik dan fleksibel dan mempunyai skala dalam menapis dan mencegah ancaman yang memiliki kompleksitas yang tinggi (Urbani, et al., 2019).

Dalam penerapannya, *stateful inspection* biasanya diterapkan pada tempat berlangsungnya topologi jaringan, yakni pada area perangkat keras dan perangkat lunak pada jaringan dan topologi dengan melalui *firewall*. Pengguna akan mendapati *firewall* yang mengikuti paket yang keluar yang meminta jenis paket yang masuk tertentu dan akan mengizinkan paket masuk untuk dilewati selama mereka merupakan respons yang akurat.

Penelitian ini dilakakukan untuk mengkaji dan menganalisa kekuatan *stateful inspection* sebagai salah satu upaya pengembangan keamanan website yang berjalan pada jaringan di Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Musi Banyuasin. Hasil penelitian ini bertujuan untuk memberikan gambaran tentang analisa pengembangan *stateful inspection* dalam melindungi website pada instansi tersebut dengan menggunakan metode semi deskriptif. Hasil dari penelitian ini diharapkan dapat memberi tambahan pemahaman yang lebih terhadap *stateful inspection* dalam melindungi sebuah teknologi informasi berbasis website pada Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Musi Banyuasin.

STUDI LITERATUR

Jurnal penelitian lainnya yang terkait penggunaan *stateful inspection* pada penelitian ini adalah penelitian yang dilakukan Vidya, dkk (2015), dalam penlitian yang berjudul *Application Gateway* dan *Stateful Inspection Method* Pada Implementasi *Firewall* Untuk Optimasi Keamanan Jaringan Komputer menjelaskan bahwa penggunaan penggunaan *stateful* merupakan bagian penting untuk menyaring paket data baik permintaan ataupun pengiriman. Penelitian berikutnya yang dilakukan oleh Mulia, dkk (2016) yang beertopik Analisis dan Simulasi Perbandingan Kinerja *Stateless* dan *Stateful Firewall* Pada Arsitektur *Software-Defined Network* menjelaskan tentang bagaimana *stateful* lebih mengutamakan kecepatan, sehingga untuk sistem yang memprioritaskan hal tersebut, *stateful* lebih cocok digunakan. Selanjutnya penelitian yang dilakukan Urbani, dkk (2019), menerangkan dalam penelitiannya yang berjudul Pengembangan *Stateful Packet Inspection* dengan Metode NDPMon untuk *Duplicate Address Detection* diketahui bahwa salah satu program yang dapat diterapkan pada kontroler untuk mengatasi permasalahan kemanan pada *openFlow* yakni dengan menggunakan *stateful packet inspection.* Dengan itu, maka sistem berhasil mengatasi serangan *DDoS*.

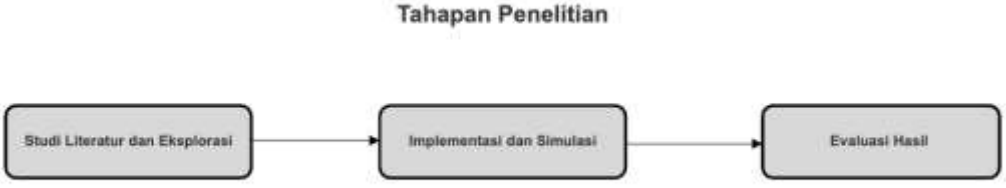
METODE

Pendekatan penelitian yang menggabungkan komponen deskriptif dengan menganalisis karakteristik teknis *stateful inspection* dan eksploratif yaitu dengan mengeksplorasi potensi penggunaan *stateful inspection* dalam konteks keamanan website. Pendekatan ini dipilih dalam penelitian karena pendekatan ini sesuai dengan apa yang menjadi arah penelitian.

Pertama, kami mengumpulkan data dengan studi literatur terlebih dahulu dan memastikan data yang diperoleh telah divalidasi sebelumnya untuk sebagai landasan kami menganalisis hal teknis dari penggunaan *stateful.* Lalu kami menggunakan lingkungan *virtual* untuk mensimulasikan implementasi *stateful inspection*. Kami menjalankan aplikasi *web* dengan potensi kerentanan.

Kemudian yang kedua, kami menerapkan *stateful inspection* sebagai perangkat lunak pada *server*. Dilakukan implementasi lalu lintas sebagai simulasi dari aktivitas pengguna. Peneliti memastikan konektivitas antara *server w*eb dan firewall pada lingkungan perangkat lunak *stateful inspection* yang dikonfigurasi meliputi alamat *IP, subnet*, dan parameter jaringan. Selanjutnya aturan keamanan pada firewall didefinisikan, termasuk izin dan pemblokiran lalu lintas berdasarkan alamat *IP, port*, protokol, dan status koneksi. Setelah itu dilakukan simulasi serangan berbasis aplikasi dan serangan siber yang dikumpulkan log aktivitas, koneksi, protokol, dicatat dan direkam untuk mendapatkan respons *firewall* terhadap masing-masing serangan.

Dan tahapan terakhir yang ketiga, dari hasil implementasi dan ujicoba, peneliti melakukan evaluasi untuk kemudian ditarik kesimpulan sebagai sebuah hasil dan rekomendasi yang akan menjadi hasil dari penelitian ini. Untuk lebih jelasnya lihat Gambar 3 berikut ini.

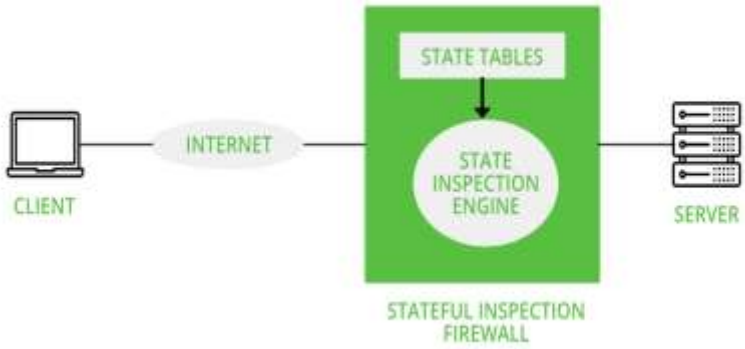


Gambar 3. Tahapan Penelitian

HASIL

Stateful inspection akan bekerja dengan cara mendeteksi paket komunikasi dalam periode waktu dan memeriksa paket masuk dan keluar. *Firewall* pada *stateful inspection* memantau semua sesi dan memverifikasi semua paket, meskipun metode yang digunakannya dapat bervariasi bergantung pada teknologi firewall dan oleh karena itu protokol komunikasi yang digunakan. Misalnya, ketika protokolnya adalah TCP, *firewall* menangkap keadaan paket dan informasi konteks dan membandingkannya dengan data sesi yang ada. Jika entri yang identik sudah ada, paket tersebut diizinkan untuk melewati *firewall*. Jika kecocokan tidak ditemukan, maka paket harus menjalani pemeriksaan kebijakan tertentu (hk4hritikjaiswal, 2022).

Pada saat itu, jika paket memenuhi persyaratan kebijakan, *firewall* menganggap bahwa itu untuk koneksi pengganti dan menyimpan data sesi dalam tabel yang sesuai. Ini kemudian mengizinkan paket untuk lewat. Jika paket tidak sesuai dengan ketentuan kebijakan, paket akan ditolak. Lebih jelas, dapat dilihat Gamabr 3 mengenai alur kerja dari *stateful inspection. Firewall* sebagai komponen sentral dalam keamanan jaringan, firewall berfungsi untuk mengendalikan lalu lintas antara jaringan internal dan eksternal (hk4hritikjaiswal, 2022).



Gambar 3. Alur Kerja *Stasteful Inspection*

Sumber: (hk4hritikjaiswal, 2022)

Keunggulan dari implementasi *stateful inspection* dalam konteks keamanan aplikasi web meliputi:

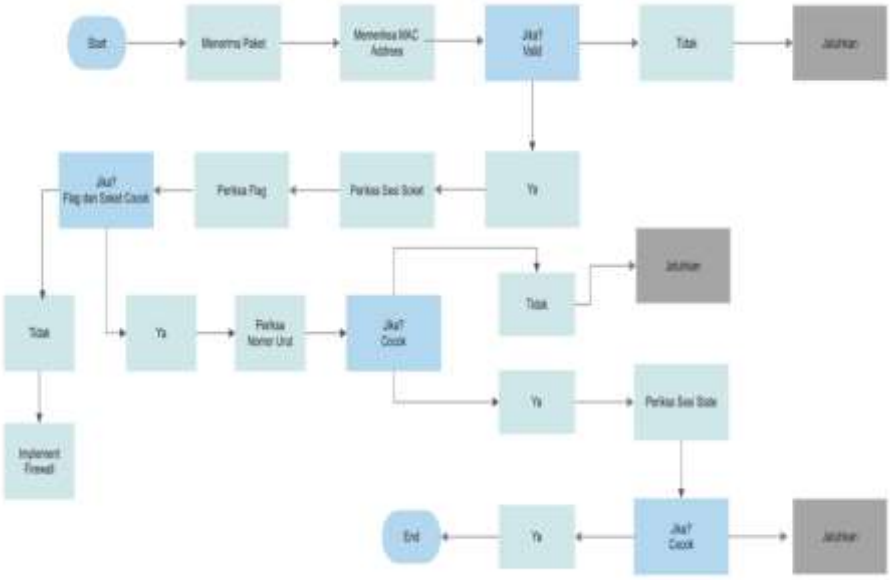
1. Deteksi dini serangan berbasis koneksi yang dilakukan oleh *stateful inspection* untuk memantau status koneksi secara cermat dan dapat mendeteksi upaya serangan berbasis koneksi yang mencurigakan, dan tidak perlu membuka *port* yang banyak untuk komunikasi.
2. Perlindungan terhadap serangan berbasis aplikasi yang dilakukan *stateful inspection* dapat menganalisis konten lalu lintas dan mencegah serangan berbasis aplikasi.
3. Pengelolaan lalu lintas oleh *stateful inspection* dengan pembuatan tabel status koneksi, lalu *stateful inspection* mampu mengelola lalu lintas masuk dan keluar, mengurangi risiko DDoS, dan mempertahankan kinerja aplikasi.
4. Respons cepat dari *stateful inspection* yang melakukan respons otomatis terhadap serangan berpotensi mengurangi dampak serangan dan mencegah penyalahgunaan lebih lanjut.
5. Memiliki kekuatan dalam mencatat atau menyimpan aspek-aspek penting yang ada pada koneksi jaringan.

Dalam menggali lebih dalam mengenai dampak penggunaan *stateful inspection*, kita perlu mempertimbangkan skenario implementasi yang lebih spesifik. Misalnya, dalam lingkup pemerintahan Dinas Pemberdayaan Masyarakat dan Desa Kab. Musi Banyuasisn, penggunaan *stateful inspection* dapat berkontribusi pada pemeliharaan reputasi instansi dengan mencegah serangan yang dapat mengakibatkan pelanggaran data pengguna atau kebocoran informasi penting yang berkaitan dengan masayarakt dan desa. Hal ini juga dapat membantu menjaga kualitas layanan dan ketersediaan website, menghindari *downtime* yang merugikan.

Dalam hal regulasi keamanan data, *stateful inspection* juga dapat menjadi komponen penting dalam memastikan kepatuhan dengan standar terhadap data perlindungan data umum dan undang-undang yang berkatian dengan akuntabilitas institusi. *Stateful inspection* memungkinkan deteksi dan mitigasi terhadap ancaman yang dapat melanggar kebijakan privasi dan keamanan data yang ditetapkan oleh undang-undang tersebut. Dimulai dengan menyiapkan alat-alat yang diperlukan yang terdiri atas perangkat keras dan perangkat lunak serta instalasi yang sudah ada dan berjalan pada lingkup instansi, diantaranya:

- Perangkat Keras
  Perangkat keras yang dipakai mencakup komputer dan perangkat jaringan yang mencakup sebagai administrator dan client dengan spesifikasi Intel Core i3, dengan RAM 4GB, dengan Realtek *onboard* dan PCI Express serta alat pendukung jaringan seperti *switch* dan *router* serta kabel UTP.
- Perangkat Lunak
  Perangkat lunak yang dipakai yakni perangkat lunak dengan berbasis Linux, dan Windows 7 sebagai sistem informasi, *browser* Google Chrome, WinSCP, XAMPP, nmap yang diletakkan pada komputer *server* dan *client.*

Selanjutnya kami menyusun algoritma yang akan digunakan sebagai langkah-langkah yang akan dilakukan oleh *Statefull Inspection Firewall* dalam memproses dan menindaklanjuti aktivitas penerimaan atau pengiriman paket di dalam sebuah simulasi yang akan dilakukan. Di bawah ini pada Gambar 4, akan kami berikan alur proses langkah-langkah yang proses dan tidak lanjut dari aktivitas penerimaan dan pengiriman paket dalam insoeksi *stateful*.



Gambar 4. Alur Inspeksi *Stateful*

Pada gambar tersebut menggambarkan bagaimana kerja *firewall* yang memeriksa, lalu memproses, dan akan mengambil tindakan berdasarkan informasi yang terdapat dalam setiap paket penerimaan yang melewati *firewall*. Pada dasarnya, penyusunan ini setiap langkahnya dirancang untuk memastikan bahwa lalu lintas yang masuk sesuai dengan kebijakan keamanan yang ditetapkan. Langkah-langkah tersebut dimulai dengan melakukan proses dengan masukan yang diberikan seperti berikut ini:

1. ST *(Session Table),*
2. SNC *(Sequence Number Check),*
3. RT *(Firewall Rule Table),*
4. SS *(Session State)*

Session table digunakan sebagai tabel yang berisi informasi tentang sesi-sesi aktif dalam jaringan, seperti alamat socket, status sesi, dan atribut terkait lainnya. *Sequence number check* merupakan nomor urut atau *sequence number* yang digunakan untuk memeriksa integritas data dalam paket. Sedangkan *firewall rule table* ini akan berisi aturan keamanan untuk mengizinkan atau menolak lalu lintas berdasarkan kriteria tertentu. Dan *session state* digunakan sebagai status sesi yang mengindikasikan apakah sesi dalam keadaan aktif atau tidak.

```
1. START
2. Receive Packet;
3. Perform Network Sanity Check (mac = phdr.find(mac));
4. If (mac == 0:0:0:0) then:
   - Drop the packet;
5. Else:
6. Examine socket in Session Table (socket = ST.find(socket));
7. Examine flag in Session Table (flag = ST.find(flag));
8. If (pkt == socket && flag) then:
   - pkt.send(SNC);
9. Else:
10. Apply Firewall Filtering Policy (rule = RT.match(rule));
11. If (rule.match() == allow) then:
    - pkt.send(ST);
12. Else:
    - Drop the packet;
13. Endif
14. Endif
15. Examine Sequence Number (SNC = phdr.find(SNC));
16. If (pkt == SNC) then:
    - pkt.send(SS);
17. Else:
    - Drop the packet;
18. Endif
19. Examine Session State (SS = ST.find(active));
20. If (pkt == SS) then:
    - pkt.send(Cp);
21. Else:
    - Drop the packet;
22. Endif
23. Endif
24. END
```

Gambar 5. Langkah-langkah Inspeksi *Stateful*

Penjelasan dari langkah-langkah pada Gambar 5 mengenai langkah-langkah inspeksi *stateful* diatas, yakni diawali dengan memulai algoritma. Dilanjutkan dengan *firewall* menerima paket yang datang dari lalu lintas jaringan yang masuk. Langkah berikutnya melibatkan mencari alamat MAC atau *Media Access Control* dalam header paket (phdr) menggunakan *perform network sanity check* (mac = phdr.find(mac)). Ini adalah langkah awal untuk memeriksa integritas paket. Jika alamat MAC yang ditemukan adalah "0:0:0:0", maka paket dijatuhkan (dropped). Ini menunjukkan bahwa alamat MAC tidak valid atau mencurigakan (If (mac == 0:0:0:0) then: Drop the packet;) dan Else, jika alamat MAC dalam paket adalah alamat yang valid, Kemudian akan melanjutkan ke langkah berikutnya.

Pada tahap ini Examine socket in Session Table (socket = ST.find(socket)), firewall mencari alamat soket yang sesuai dengan paket dalam *session table*. Ini untuk memeriksa apakah sesi yang terkait dengan paket ini ada dalam tabel. Examine flag in Session Table (flag = ST.find(flag)) pada firewall juga mencari status sesi (flag) terkait dengan sesi yang mungkin ada dalam tabel. If (pkt == socket && flag) then: pkt.send(SNC): Jika alamat socket dalam paket cocok dengan yang ada dalam Session Table dan status sesi cocok dengan flag yang diharapkan, langkah ini akan mengirimkan paket untuk diperiksa nomor urut *sequence number check*, dan Else, Jika alamat socket dalam paket tidak cocok dengan yang ada dalam Session Table atau status sesi tidak cocok dengan flag yang diharapkan, langkah ini akan dijalankan.

Kemudian di langkah ini *apply firewall filtering policy* (rule = RT.match(rule)), *firewall* akan mencocokkan paket dengan aturan keamanan yang ada dalam firewall rule table. Jika hasil pencocokan aturan menunjukkan bahwa paket harus diperbolehkan (allow), langkah ini mengirimkan paket ke *session table* If (rule.match() == allow) then: pkt.send(ST):. Dan jika Else, maka dilakukan Drop the packet, jika hasil pencocokan aturan menunjukkan bahwa paket harus ditolak (deny), langkah ini menghapuskan (drop) paket karena melanggar kebijakan keamanan.

Endif, Endif, Di langkah ini, firewall mencari nomor urut (Sequence Number) dalam paket yang masuk *examine sequence number* (SNC = phdr.find(SNC)). Jika nomor urut dalam paket cocok dengan yang diharapkan, langkah ini mengirimkan paket ke *session state* untuk dilakukan pemeriksaan status sesi. If (pkt == SNC) then: pkt.send(SS): dan akan Else: Drop the packet: Jika nomor urut dalam paket tidak cocok dengan yang diharapkan, langkah ini menghapuskan (drop) paket karena nomor urut yang tidak valid atau mencurigakan.

Langkah selanjutnya, Endif *examine session state* (SS = ST.find(active)), *firewall* akan mencari status sesi terkait dengan alamat soket di dalam paket. Jika status sesi dalam paket cocok dengan yang diharapkan, langkah ini mengirimkan paket ke langkah yang akan dilakukan sesuai dengan status sesi. If (pkt == SS) then: pkt.send(Cp):. Dan jika status sesi dalam paket tidak cocok dengan yang diharapkan, langkah ini menghapuskan (drop) paket karena status sesi yang tidak valid atau mencurigakan. Else: Drop the packet: Endif Endif, hingga END untuk menutup langkah.

PEMBAHASAN

Setelah menggambarkan alur kerja dari penelitian ini, selanjutnya yang dilakukan pada penulisan penelitian yang kami lakukan yakni:

- Analisis dan Prototipe

  Pada tahap analisis ini kami membagi kedalam beberapa bagian lagi, diantaranya identifikasi terhadap permasalahan, lalu memahami permasalahan dan memahami bentuk jalan menyelesaikan permasalahan tersebut, berikutnya analisis kebutuhan hasil analisis yang akan diterapkan di perangkat keras juga perangkat lunak yang ada.

  Selain itu, kami juga mengganti topologi yang ada sebelumnya dengan skema menjadi seperti berikut ini:

  Dimulai, ketika pengguna yang mencoba mengakses website Anda melalui sumber lalu lintas eksternal, yakni internet. Lalu *firewall stateful inspection* akan berfungsi sebagai filter pertama yang mencegah lalu lintas yang tidak diinginkan atau berbahaya masuk ke jaringan internal. *stateful inspection* juga memantau dan menganalisis status koneksi secara cermat pada *server* web yang menjalankan portal *website* Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Musi Banyuasin.

  Kemudian di dalam jaringan ini juga berjalan dimana didalam jaringan tersebut perangkat seperti komputer *client* dan server internal juga berada. Berikutnya yang juga penting adalah zona antara jaringan internal dan eksternal yang digunakan untuk menempatkan *server* yang dapat diakses oleh pengguna eksternal, seperti *server web*, dengan menggunakan *demilitary zone*, dimana *demilitary zone* memiliki lapisan keamanan tambahan.

  Selanjutnya terkait dengan *database server* yang menyimpan data yang diperlukan oleh *website*, seperti basis data dan lain sebagainya juga dilakukan pembatasan akses. Kami mencoba melakukan *intrusion detection* yang akan memantau lalu lintas jaringan dan mencari tanda-tanda serangan yang tidak diinginkan. Kemudian selain melakukan pembatasan, kami juga mencoba perangkat *load balancer*. Ini adalah perangkat yang mendistribusikan lalu lintas masuk secara merata ke beberapa server web untuk meningkatkan kinerja dan ketersediaan. Dan hal penting lainnya yaitu *monitoring* untuk melacak aktivitas jaringan dan *firewall* untuk mendeteksi ancaman potensial. Serta *log analysis*: yang digunakan untuk menganalisis *log* pada aktivitas untuk mendapatkan informasi tentang keamanan, kondisi, dan efisiensi jaringan.

- Simulasi dan Implementasi

  Kami mensimulasikan jenis serangan yang ingin dicegah, seperti *injection*, atau serangan lainnya dengan diintegrasikan ke dalam infrastruktur jaringan. Menentukan zona keamanan dan aturan untuk lalu lintas masuk dan keluar dan aturan yang mendefinisikan jenis lalu lintas yang diizinkan dan yang diblokir untuk melindungi aplikasi web, misalnya pemblokiran potensi serangan berbasis aplikasi, misalnya: mengizinkan lalu lintas pada *port* 80 dan *port* 443 dengan menggunakan perintah:

$$\boldsymbol{sudo\ iptables\ -A\ INPUT\ -p\ tcp\ --dport\ 80\ -j\ ACCEPT}$$
$$\boldsymbol{sudo\ iptables\ -A\ INPUT\ -p\ tcp\ --dport\ 443\ -j\ ACCEPT}$$

  Kami menerapkan juga perizinan pada lalu lintas dengan *port* tertentu misalnya dengan perintah:

$$\boldsymbol{sudo\ iptables\ -A\ INPUT\ -p\ tcp\ --dport\ 22\ -s\ <IP\_Address>\ -j\ ACCEPT}$$

  yang mengizinkan hanya *port* 22.

  Perlu juga kami mengaktifkan fitur deteksi serangan dan mengatur parameter deteksi sesuai kebutuhan. Bahkan membatasi jumlah koneksi dengan perintah:

$$\boldsymbol{sudo\ iptables\ -A\ INPUT\ -p\ tcp\ --syn\ --dport\ 80\ -m\ connlimit\ --connlimit\ -above\ 20\ -j\ DROP}$$

Kami memastikan konektivitas antara *server* dan *firewall* pada lingkungan perangkat lunak yang dikonfigurasi dalam parameter jaringan. Kemudian aturan keamanan pada *firewall* didefinisikan, termasuk izin dan pemblokiran lalu lintas. Dalam hal ini, *stateful inspection firewall* membangun tabel status koneksi yang mencatat informasi penting tentang setiap koneksi yang aktif, termasuk *port*, alamat IP, dan status koneksi.

KESIMPULAN

Dalam penelitian ini telah dilakukan analisa dan mengsimulasikan teknik dan metode *stateful inspection*. Hasil dari penelitian ini menunjukkan bahwa penerapan metode *stateful inspection* pada instansi Dinas

Pemberdayaan Masyarakt dan Desa Kabupaten Musi Banyuasin dengan menggunakan *stateful inspection* pada jaringan tempat berjalannya sistem berbasis web dapat memberikan tambahan keamanan untuk menjaga situs web dari serangan siber. *Stateful inspection* merupakan jenis firewall yang di mana setiap paket data dianalisis dalam konteks status koneksi. Metode dalam di mana status dari setiap koneksi dipantau dan dianalisis, memungkinkan *firewall* untuk membuat keputusan yang lebih cerdas tentang apa yang harus diizinkan dan apa yang harus ditolak. Dalam pandangan yang lebih luas, kami memberikan rekomendasi bahwa pengembangan keamanan website dengan menggunakan *stateful inspection* dan metode semi deskriptif cukup memberikan hasil yang relevan dalam melindungi website dari ancaman siber yang semakin canggih. Kinerja *stateful inspection* dalam mendeteksi dan merespons serangan pada lalu listas yang ada, memiliki dampak relevan dalam mencegah keamanan. Namun, kami juga mengakui bahwa upaya keamanan website bersifat berkelanjutan dalam menghadapi tantangan serangan siber yang terus berkembang di dunia digital. Pentingnya untuk terus menganalisa dan mengembangkan solusi untuk mengatasi serangan siber yang bersifat semakin rumit. Sebagai catatan, implementasi *stateful inspection* juga dapat membawa tantangan tertentu. Pengaturan aturan yang tidak tepat atau ketidakkonsistenan dalam konfigurasi firewall dapat mengakibatkan pemblokiran lalu lintas yang sah atau, sebaliknya, membiarkan lalu lintas berbahaya masuk.

REFERENSI

Alifah, N. N. (6 November, 2022). *Keamanan Siber Negara Asia Tenggara 2022, Indonesia Peringkat Berapa?* Retrieved from goodstats.id: https://goodstats.id/article/keamanan-siber-negara-asia-tenggara-2022-indonesia-peringkat-berapa-3RLgv

hk4hritikjaiswal. (10 February, 2022). *What is Stateful Inspection*. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/what-is-stateful-inspection/

Mutia, A. (12 September, 2022). *Pemerintah dan NGO Jadi Institusi Paling Rawan Ancaman Hacker*. Retrieved from Databoks: https://databoks.katadata.co.id/datapublish/2022/09/12/pemerintah-dan-ngo-jadi-institusi-paling-rawan-ancaman-hacker

Naurah, N. (23 June, 2022). *Membandingkan Indeks Keamanan Siber Indonesia dengan Negara ASEAN*. Retrieved from goodstats.id: https://goodstats.id/article/indeks-keamanan-siber-indonesia-jauh-lebih-buruk-dari-malaysia-ini-grafiknya-GQkGl

Pratama, Y., & Sutabri, T (2023). Service Operation ITIL V3 Pada Analisis dan Evaluasi Layanan Teknologi Informasi. *Nuansa Informatika*, 17(1), 169-178. DOI: https://doi.org/10.25134/fkom%20uniku.v17i1.7233

Senthil, P., Kavin, B. P., Srividhya, S. R., Ramachandran, V., Kavitha, C., Lai, W.C. (2022). Performance Evaluation of Stateful Firewall-Enabled SDN with Flow-Based Scheduling for Distributed Controllers. *Journals Electronics*. 11(19), 3000; https://doi.org/10.3390/electronics11193000

Sutabri, T. (2012). *Konsep Sistem Informasi.* Yogyakarta: Andi.

Sutabri, T. (2012). *Analisis Sistem Informasi.* Yogyakarta: Andi.

Vidya, V., Surono., & Setiarso, G (2020). Application Gateway dan Statefull Inspection Method Pada Implementasi Firewall Untuk Optimasi Keamanan Jaringan Komputer. *Jurnal Pengembangan Rekayasa dan Teknologi*, 16(2), 87-97. http://dx.doi.org/10.26623/jprt.v16i2.2624

Mulia, R., Suwastika, N. A., & Nugroho, M. A. (2018). Analisis Dan Simulasi Perbandingan Kinerja Stateless Dan Stateful Firewall Pada Arsitektur Software-Defined Network. *e-Proceeding of Engineering : Vol.5, No.2* (p. 3556). Bandung: Universitas Telkom. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/6740

Urbani, S., Yahya, W., & Pramukantoro, E. S. (2019). Pengembangan Stateful Packet Inspection dengan Metode NDPMon untuk Duplicate Address Detection. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 3(2), 1411–1420. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/4387

Andarini, R.Y., Hendradi, P., & Nugroho, S. (2023). Meningkatkan Keamanan Terhadap SQL Injection Studi Kasus Sistem Kepegawaian BNN. *Indonesian Journal of Business Intelegence*. 6(1). 34-42. http://dx.doi.org/10.21927/ijubi.v6i1.3161

Safitri, E.M., Larasati, A.S., & Hari, S.R (2022). Analisis Keamanan Sistem Informasi E-Banking di Era Industri 4.0: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi dan Robotika*. 2(1). 12-16. https://doi.org/10.33005/jifti.v2i1.25