Dinas Komunikasi dan Informatika
Kabupaten Natuna

BUKU 5

ARSITEKTUR KEAMANAN INFORMASI SPBE

Pekerjaan:
Penyusunan Dokumen Arsitektur dan Peta Rencana Sistem Pemerintah Berbasis Elektronik (SPBE)
Tahun 2022 - 2026

PENYUSUNAN DOKUMEN ARSITEKTUR DAN PETA RENCANA SPBE

BUKU 5 -
ARSITEKTUR KEAMANAN INFORMASI SPBE

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN NATUNA

TAHUN 2022

KATA PENGANTAR

Puji Syukur, atas perkenan Tuhan YME. Buku 5: Arsitektur Keamanan Informasi, telah selesai. Buku ini merupakan salah satu keluaran dari pekerjaan Pembuatan Dokumen Arsitektur dan Peta Rencana Sistem Pemerintahan Berbasis Elektronik (SPBE) di Pemerintah Kabupaten Natuna, Tahun 2022.

SPBE merupakan singkatan dari Sistem Pemerintahan Berbasis Elektronik yang merupakan suatu sistem tata kelola pemerintah yang memanfaatkan teknologi informasi secara menyeluruh dan terpadu dalam pelaksanaan administrasi pemerintahan dan penyelenggaraan pelayanan publik yang dilakukan pada suatu instansi pemerintahan.

Diharapkan dengan dilaksanakannya kegiatan ini akan didapatkan acuan berupa rumusan rencana strategis pembangunan dan pengembangan SPBE yang diantaranya mampu menjamin keselarasan antara pembangunan / pengembangan SPBE dengan Rencana Pembangunan Jangka Menengah Daerah (RPJMD) tahun 2021-2026 Kabupaten Natuna, menjamin ketersediaan dukungan SPBE dengan tugas pokok dan fungsi semua OPD pemerintah Kabupaten Natuna, serta memenuhi kesenjangan antara kondisi eksisting lingkungan sistem informasi saat ini dengan kondisi yang ingin dicapai di akhir tahun 2026.

Pada Buku selanjutnya yaitu Buku 6, akan di jelaskan Arsitektur Tata Kelola dan Manajemen SPBE dan Penyelenggara SPBE Pemerintah Kabupaten Natuna.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR ISTILAH (TERMINOLOGI)

Sebagaimana tertuang dalam Peraturan Presiden Nomor 95 tahun 2018, berikut ketentuan umum atau penjelasan dari beberapa istilah yang tertuang dalam dokumen ini:

1. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
2. Tata Kelola SPBE adalah kerangka kerja yang memastikan terlaksananya pengaturan, pengarahan, dan pengendalian dalam penerapan SPBE secara terpadu.
3. Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas.
4. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
5. Rencana Induk SPBE Nasional adalah dokumen perencanaan pembangunan SPBE secara nasional untuk jangka waktu 20 (dua puluh) tahun.
6. Arsitektur SPBE adalah kerangka dasar yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terintegrasi.
7. Arsitektur SPBE Nasional adalah Arsitektur SPBE yang diterapkan secara nasional.
8. Arsitektur SPBE Instansi Pusat adalah Arsitektur SPBE yang diterapkan di instansi pusat.
9. Arsitektur SPBE Pemerintah Daerah adalah Arsitektur SPBE yang diterapkan di pemerintah daerah.
10. Peta Rencana SPBE adalah dokumen yang mendeskripsikan arah dan langkah penyiapan dan pelaksanaan SPBE yang terintegrasi.
11. Peta Rencana SPBE Nasional adalah Peta Rencana SPBE yang diterapkan secara nasional.
12. Peta Rencana SPBE Instansi Pusat adalah Peta Rencana SPBE yang diterapkan di instansi pusat.
13. Peta Rencana SPBE Pemerintah Daerah adalah Peta Rencana SPBE yang diterapkan di pemerintah daerah.
14. Proses Bisnis adalah sekumpulan kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi instansi pusat dan pemerintah daerah masing-masing.

15. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
16. Infrastruktur SPBE Nasional adalah Infrastruktur SPBE yang terhubung dengan Infrastruktur SPBE instansi pusat dan pemerintah daerah dan digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah.
17. Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah adalah Infrastruktur SPBE yang diselenggarakan oleh instansi pusat dan pemerintah daerah masing-masing.
18. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
19. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
20. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
21. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
22. Aplikasi Umum adalah Aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh instansi pusat dan/atau pemerintah daerah.
23. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh instansi pusat atau pemerintah daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.
24. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
25. Audit Teknologi Informasi dan Komunikasi adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
26. Pengguna SPBE adalah instansi pusat, pemerintah daerah, pegawai Aparatur Sipil Negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan Layanan SPBE.

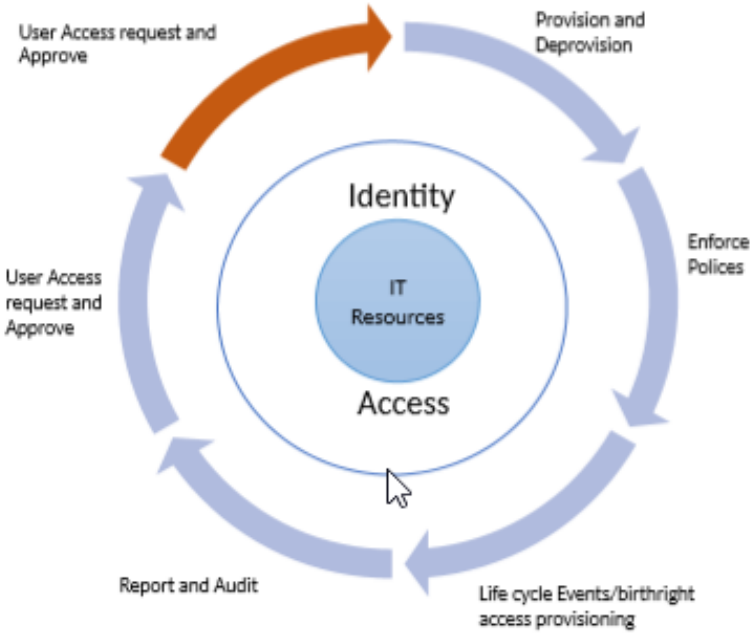
27. Instansi Pusat adalah kementerian, lembaga pemerintah nonkementerian, kesekretariatan lembaga negara, kesekretariatan lembaga nonstruktural, dan lembaga pemerintah lainnya.
28. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.

BAB I
KEAMANAN DATA DAN INFORMASI

1.1 STANDAR DAN KEBIJAKAN KEAMANAN DATA DAN INFORMASI

1.1.1. Identity and Access Management

Identity and Access Management mengacu pada proses Pengelolaan identitas pengguna dan Penggambaran hak akses *Internal* dan *Eksternal* selama masa jabatan dan tugas masing masing dari hari pertama hingga Hari terakhir atau dan Kontrak berakhir. Elemen mendasar dari Aspek keamanan ini adalah mengotomatiskan dan menyederhanakan proses yang terkait dengan pengguna yang masuk dan keluar, menetapkan dan mengelola hak akses, serta memantau dan melacak aktivitas akses.



Gambar 1. 1 Identity and Access

Berikut ini adalah beberapa *Key Point* yang harus ada di dalam Penerapan *Identity and Access Management*:

1. Akses ter Sentralisasi

   Single Sign On (SSO) menghilangkan kebutuhan pengguna untuk mengingat banyak Password untuk mengakses berbagai aplikasi / Modul Aplikasi. Pengguna dapat melihat akses pengguna untuk semua lingkungan sekaligus. Pengguna/Sumber Daya dapat melihat akses untuk apa yang mereka miliki dan dapat mengajukan permintaan untuk akses sistem baru.
2. Penurunan Biaya Manajemen Akun

Manfaat utama dari SSO adalah Operator Layanan SPBE dapat mengurangi biaya *Helpdesk* internal yang membantu pengguna terkunci dari akun aplikasi masing masing. SSO dapat memberikan akses kepada pengguna berdasarkan jam kerja dan tidak akan dapat mengakses sistem di luar jam kerja masing-masing.

3. Penerapan Kepatuhan

   Menjaga kontrol pencegahan dan pendeteksian di tempat untuk memastikan akses sesuai dengan kebijakan SPBE setiap saat.

4. Kemudahan Akses

   IAM/SSO memungkinkan pengguna untuk mengakses semua Sistem / Aplikasi / Modul Aplikasi dalam jaringan, di mana pun lokasi pengguna. Ini adalah salah satu persyaratan utama untuk Seluruh Penyedia layanan secara *Internet Based*, memberikan kemudahan akses ke Pengguna, mitra, dan *Auditor* dengan cara yang sama.

5. Reviu Pengguna dan Pelaporan

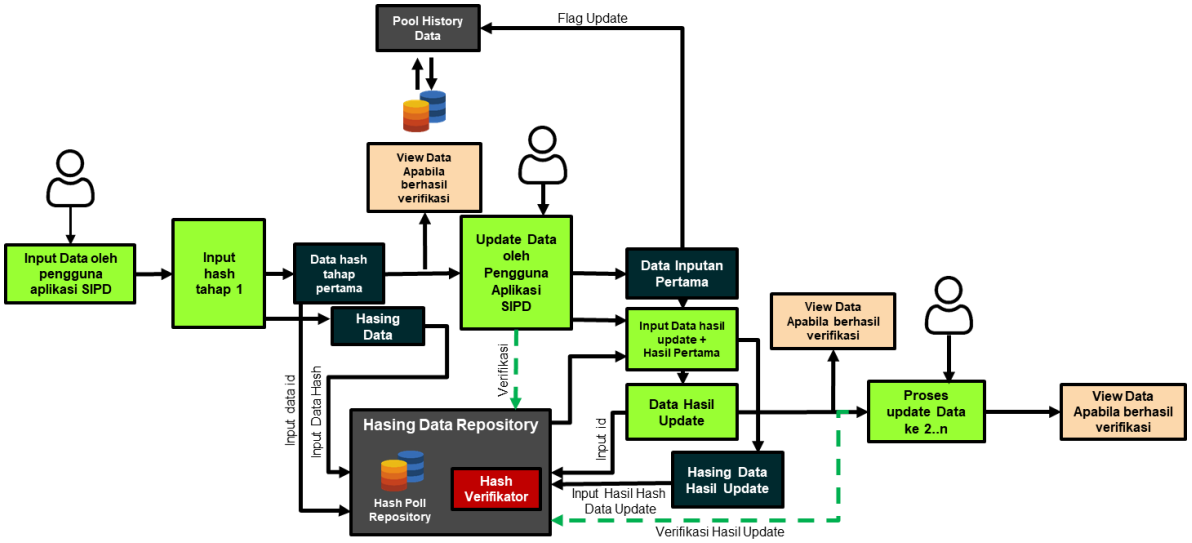
   Dengan *Tools* IAM, kami dapat melakukan Tinjauan Akses Pengguna sesuai dengan kebijakan kepatuhan SPBE dan mengakses sistem berdasarkan keputusan *Reviewer* | *Auditor*.

6. Siklus Hidup Akun / Identitas

   Setiap akun ataupun identitas di dalam SPBE seharusnya tidak berdiri sendiri dan mempunyai siklus hidup. Siklus hidup dimulai dari pembuatan akun, Distribusi Kredensial, Penggantian *password*, hingga penonaktifan akun harus dalam satu tarikan nafas (*life cycle*)

1.1.2. Data Flow Integrity Checker

Data Flow Integrity Checker adalah sebuah Metode yang bertujuan untuk memastikan Integritas Data terjaga dari satu tahapan bisnis proses ke tahapan bisnis proses berikutnya. Pada prinsipnya di dalam SPBE, Data mengalir menjadi satu tarikan nafas. Tujuan dari Desain ini adalah meastikan tidak adanya kesalahan pengolahan data di aplikasi maupun upaya alterisasi data secara tidak sah.



Gambar 1. 2 Arsitektur Konseptual Keamanan Informasi Kontrol Integritas Data

Pada setiap tahapan terjadi proses penginputan atau perubahan data. Pada setiap proses tersebut akan dilakukan juga pencatatan di sisi Database hash / Data hash *Repository*. Pencatatan tersebut berisi Nilai hash, nama table, *Primary Key* dan timestamp proses input atau perubahan data. Setiap data yang mengalir ke tahapan berikutnya maka data tersebut akan dicheck terlebih dahulu nilai hash nya secara langsung dan membandingkannya dengan nilai hash yang ada di hash *repository*. Jika nilai hash dari keduanya berbeda maka data tersebut tidak dapat digunakan atau dilanjutkan ke tahap berikutnya.

1.1.3. Data Encryption

Pemanfaatan Enkripsi data di Pemerintahan di seluruh Indonesia ditujukan kepada perlindungan pada saat proses Transmisi data berlangsung. Ada beberapa area yang harus diamankan dalam proses perlindungan Transmisi Data diantaranya :

1. Transmisi Pengiriman data pada media *Web HTTP*
   Menggunakan *Protokol* SSL pada semua transaksi pengiriman dan tampilan halaman HTTP, terutama pada saat berbagi pakai menggunakan API. Secara detail sudah dijelaskan di bagian *Secure Protocol*
2. Transmisi Pengiriman Data pada media *Email*
   Terdapat kerentanan di level User *Security*. Dimana setiap pengiriman *email* yang kadang digunakan untuk distribusi akun kredensial tidak terlindungi *End to End encryption*. Kami mengusulkan untuk diberlakukannya protocol pengiriman Email menggunakan *Pretty Good Privacy* (PGP).
3. Transmisi Pengiriman Data pada *File Sharing*

Menggunakan Protokol Enkripsi *Secure File Transfer Protocol* (SFTP) secara detail sudah dijelaskan di bagian *Secure File Sharing*.

1.1.4. Asset Management

Asset Management adalah metode pengelolaan asset Organisasi (baik yang *tangible*, maupun *intangible*) melalui proses yang sistematis untuk mempertahankan, memperbaharui, atau menggunakan aset dengan cara optimal agar tercapai prinsip efektif dan efisien.

Berikut ini adalah Rekomendasi Penerapan *Asset Management* :

- Standarisasi kategori Infrastruktur *Hardware*
- Standarisasi *Template* Dokumen pencatatan infrastruktur SPBE yang mencakup owner, Tahun pembuatan, tahun pencatatan, kondisi fisik, fungsi, dan Riwayat pemeliharaan.
- Portfolio Infrastruktur / Aset / *Hardware*
- Prosedur Pendataan / inventarisasi asset infrastruktur eksisting dan perbaruan secara berkala
- Rencana kebutuhan Infrastruktur secara menyeluruh mencakup semua proses bisnis dan kebutuhan teknis operasional Infrastruktur SPBE

1.1.5. Incident Response and Recovery

Berikut ini adalah uraian insident respon berdasarkan literasi dari badan sandi dan siber nasional :

Sebuah insiden dapat dideteksi dalam berbagai cara dan melalui berbagai sumber yang berbeda, tergantung pada sifat dan lokasi insiden tersebut. Beberapa insiden dapat dideteksi sendiri melalui *software* yang digunakan di dalam SPBE atau melalui anggota yang melakukan *monitoring anomaly traffic* (dapat di lihat pada *Information Security Event*

Assessment Procedure untuk mengetahui bagaimana *event* tersebut di *assessed*). Selain itu, insiden juga dapat dideteksi dan di notifikasi oleh pihak ketiga seperti *user*, vendor, atau lembaga penegakan hukum yang mengetahui adanya pelanggaran karena informasi yang telah dicuri dan digunakan untuk tujuan yang tidak semestinya. Jika terjadi penundaan saat insiden terjadi dengan waktu deteksi yang dilakukan, dapat dicegah dengan menggunakan pendekatan secara Proaktif. Hal ini dapat mencegah penundaan atau periode waktu yang berbeda. Salah satu faktor yang terpenting adalah prosedur tanggap insiden harus dimulai sesegera mungkin setelah terdeteksi sehingga tanggap insiden dapat dilakukan secara efektif.

1. Prosedur Tanggapan Sistem.

   Setelah dilakukan notifikasi insiden kepada Ketua Tim, Ketua Tim harus memutuskan apakah skala dan dampak aktual serta potensial dari insiden tersebut dapat dilanjutkan untuk proses aktivasi Prosedur Tanggap Insiden dan pembentukan Tim Tanggap Insiden/*Incident Response Team* (IRT). Ketua tim dapat memulai Prosedur Tanggap Insiden jika memenuhi salah satu dari :

   - Ada kerugian secara aktual atau potensial yang signifikan atas informasi rahasia, termasuk data pribadi
   - Ada gangguan secara aktual atau potensial yang signifikan terhadap proses bisnis
   - Ada risiko signifikan terhadap reputasi bisnis
   - Serta situasi lain yang dapat menyebabkan dampak signifikan bagi SPBE

   Jika terjadi ketidaksepakatan atau ketidakpastian tentang apakah akan mengaktifkan Prosedur Tanggap insiden atau tidak,perlu diketahui bahwa keputusan Ketua Tim bersifat final.

   Jika insiden tersebut memerlukan aktivasi prosedur Tanggap Insiden, Ketua Tim akan mulai dalam pembentukan IRT.

2. Pembentukan Tim Tangapan Insiden.

   Setelah keputusan dibuat untuk mengaktifkan prosedur tanggap insiden, Ketua Tim (atau wakil) akan memastikan bahwa semua *role* ataupun anggota telah di informasikan seluruh informasi terkait insiden yang terjadi serta berkumpul untuk melakukan berkoordinasi.

   Adapun pengecualian dilakukan pada Incident Liaison yang akan diminta untuk hadir di lokasi insiden (jika berbeda) untuk mulai mengumpulkan informasi dan diberikan kepada IRT untuk dilakukan penilaian insiden sehingga dapat ditentukan proses tanggap insiden yang tepat.

3. Prosedur Komunikasi

   Prosedur Komunikasi merupakan bagian penting dalam penanganan insiden. Komunikasi yang efektif harus dilaksanakan antara semua pihak yang terlibat dalam tanggap insiden. Sarana komunikasi utama selama insiden adalah tatap muka dan telepon, baik telepon kantor maupun seluler serta *email yang secure*.

4. *Incident Containtment, Eradication, Recovery and Notifications*

   Langkah pertama yang dilakukan oleh IRT adalah menghentikan insiden menjadi lebih buruk yang dikenal dengan proses *containment*. Sebagai contoh kasus virus memerlukan pemutusan jaringan yang terdampak; untuk serangan peretasan dapat menonaktifan port tertentu pada *firewall* atau bahkan memutuskan jaringan internal

dari Internet. Tindakan spesifik yang akan dilakukan akan tergantung pada keadaan insiden.

5. Rancangan Aktifitas *Post Insident*

   Ketua Tim akan memutuskan, berdasarkan informasi terbaru dari Penghubung Insiden dan anggota tim lainnya, titik di mana kegiatan *respons* harus dihentikan dan IRT dihentikan. Perhatikan bahwa pemulihan dan pelaksanaan rencana dapat berlanjut melampaui titik ini tetapi di bawah kendali manajemen yang kurang formal. Keputusan ini tergantung pada penilaian Ketua Tim tetapi harus didasarkan pada kriteria berikut:

   - Situasi telah sepenuhnya teratasi atau cukup stabil
   - Laju perubahan situasi telah melambat ke titik di mana beberapa keputusan diperlukan
   - *Respons* yang tepat sedang berjalan dengan baik dan rencana pemulihan sedang berjalan sesuai jadwal
   - Tingkat risiko terhadap bisnis telah berkurang ke titik yang dapat diterima
   - Tanggung jawab hukum dan peraturan langsung telah dipenuhi

     Jika pemulihan dari insiden sedang berlangsung, Ketua Tim harus menentukan tindakan selanjutnya yang akan diambil. Ini mungkin termasuk:
   - Rapat IRT yang lebih jarang, misalnya mingguan, tergantung pada keadaan
   - Memberitahu semua pihak yang terlibat bahwa IRT akan mundur
   - Memastikan bahwa semua dokumentasi insiden diamankan
   - Meminta semua staf yang tidak terlibat dalam pekerjaan lebih lanjut untuk kembali ke tugas normal.

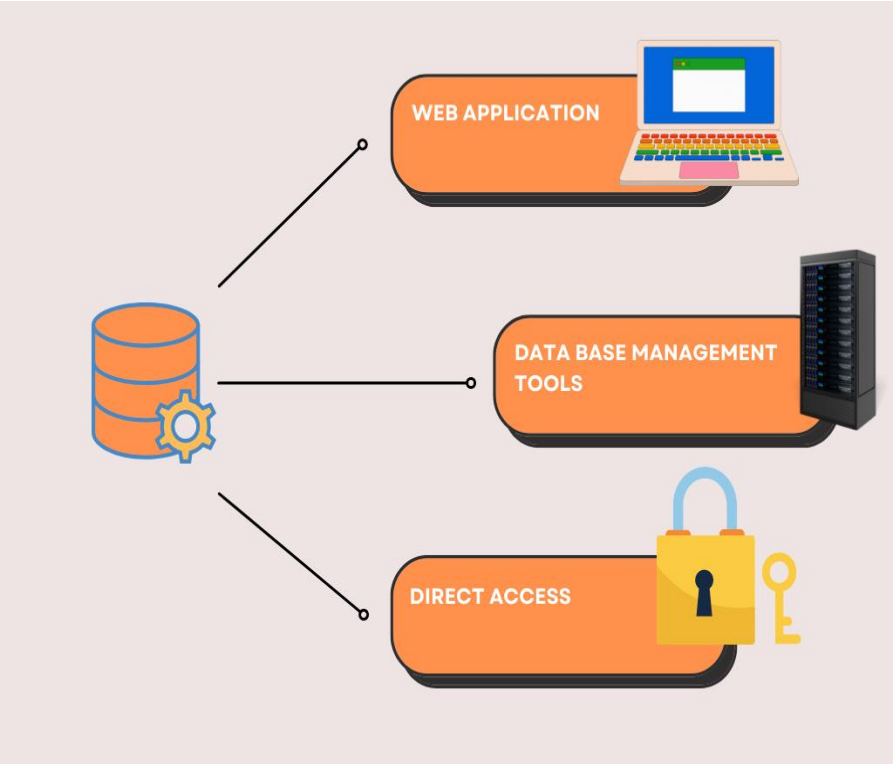
     Semua tindakan yang diambil sebagai bagian dari pengunduran diri harus dicatat.

Setelah IRT dibubarkan, Ketua Tim akan mengadakan *debrief* semua anggota idealnya dalam waktu 24 jam. Catatan insiden yang relevan akan diperiksa oleh IRT untuk memastikan bahwa catatan tersebut mencerminkan kejadian yang sebenarnya dan mewakili catatan insiden yang lengkap dan akurat. Setiap komentar atau umpan balik langsung dari tim akan dicatat. Tinjauan pasca-insiden yang lebih formal akan diadakan pada waktu yang akan diputuskan oleh manajemen puncak sesuai dengan besaran dan sifat insiden.

1.1.6. Audit Trail

Audit Trail adalah serangkaian catatan kejadian komputer, tentang sistem operasi, aplikasi, atau aktivitas pengguna. Sebuah sistem *computer* memiliki beberapa jejak audit, masing-masing ditujukan untuk jenis aktivitas tertentu. Auditing adalah *review* dan analisis manajemen, operasional, dan kontrol teknis. Auditor dapat memperoleh informasi berharga

tentang aktivitas pada sistem komputer dari jejak audit. Jalur audit meningkat kemampuan audit sistem *computer*. *Audit Trial* adalah aspek pengamanan keamanan informasi pada "*Integrity*". Dalam Ekosistem SPBE terdapat pada transaksi *database* yang perlu menjadi perhatian. Semua transaksi terjadi di dalam *Database*. Berikut ini adalah Usulan Arsitektur Sistem Audit Trail Sistem Informasi Berbasis Elektronik (SPBE).



Gambar 1. 3 Audit Trail System

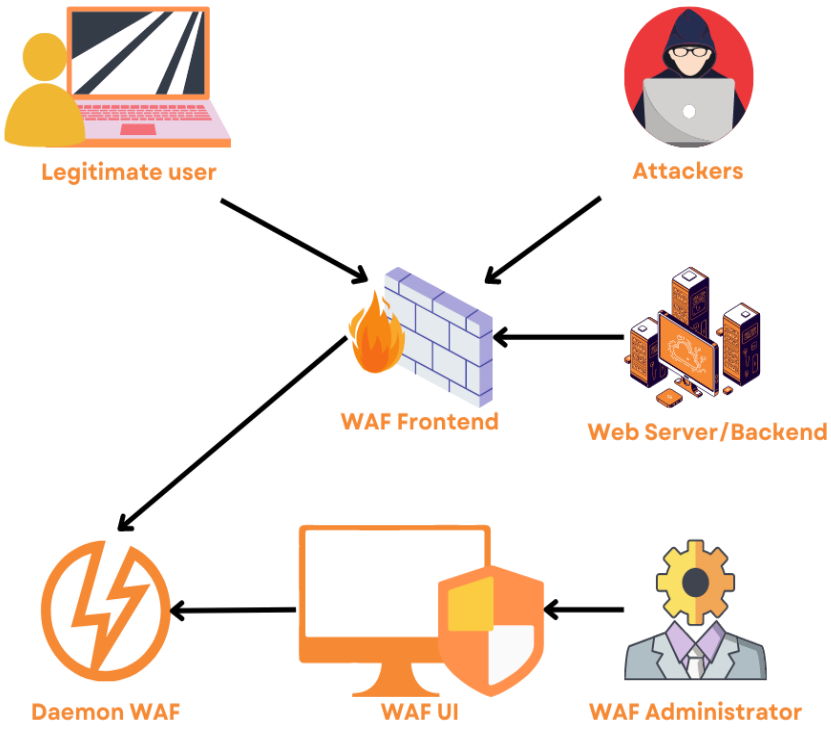
Audit Trail difocuskan pada Database sehingga semua transaksi dari dan ke Database Tercatat ke dalam Sistem. Sumber akses terdiri dari Web Application, *Database Management Tools* (DBMS) dan *Direct Access*. Tiga sumber tersebut adalah jalan masuk menuju ke dalam akses *Database*. *Web Application* adalah jalan masuk yang paling sah dan akan memberikan beberapa Informasi seperti *Web Session* Pengguna, Nama User ID Pengguna, dan Waktu Pada setiap Transaksi Pengguna. Sumber akses Database *Management Tools* akan menghasilkan *Log* berupa *Access Log Table*, Utilitas *Internal Table*. Sumber *Direct Access* Akan menghasilkan informasi berupa sesi Pengguna di lingkungan Sistem Operasi.

BAB II
KEAMANAN INFRASTRUKTUR DAN APLIKASI

2.1 STANDAR DAN KEBIJAKAN JARINGAN DAN AKSES KOMUNIKASI

2.1.1. *Web Application Firewall* (WAF) SPBE

Arsitektur *Web Application Firewall* (WAF) akan menggambarkan Rencana *Deployment* yang harus dipenuhi. Berikut ini adalah gambaran umum penerapan minimum *Web Application Firewall* (WAF) pada aplikasi web yang berjalan :

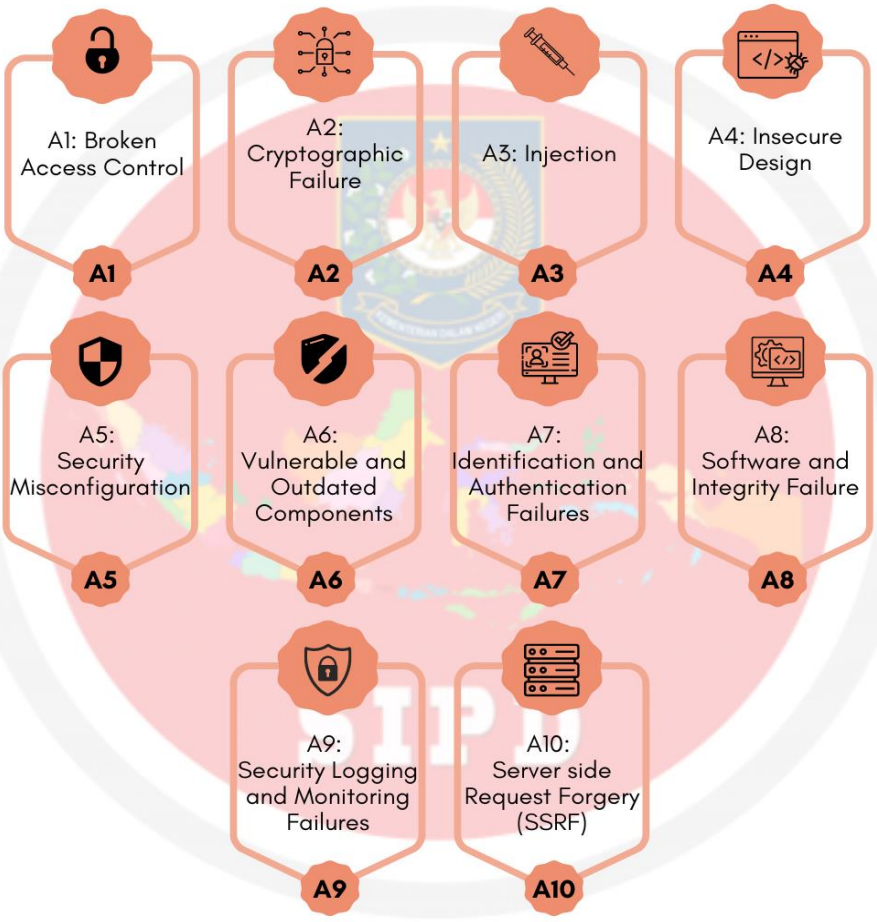


Gambar 2. 1 Web Application Firewall

Berikut ini adalah Fitur Minimum dari *Web Application Firewall* (WAF):

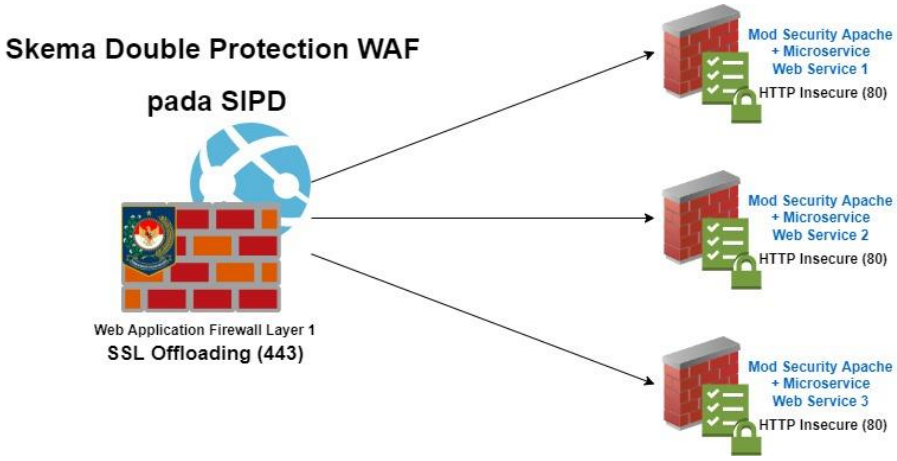
- *Transparent / Listening Mode / Detection Mode*
- *Protection Mode*
- *Custom Rule*
- *Whitelisting IP*
- *Blacklisting IP*
- *Delete / Modify Rule*
- *Update Signature*
- *Virtual Appliance / Software Defined*

Web Application Security harus memiliki fitur deteksi minimal "*Top 10 OWASP Attack*", pada tahun teraktual sebagai berikut:



Gambar 2. 2 Top 10 OWASP Attack

Berikut ini adalah rancangan *Double Web Application Firewal* (WAF) sebagai rancangan yang direkomendasikan:



Gambar 2. 3 Double Web Application Firewal

Berdasarkan gambar di atas kami menyarankan adanya dua lapis perlindungan pada *Web Application Firewall* (WAF). Pada satu lapisan *firewall* bisa saja serangan masih dapat ditembus hingga ke bagian *backend web server*. Serangan yang biasa digunakan untuk mengelabui atau melompati satu buah firewall disebut dengan "*Evading Firewall*". Pada konfigurasi atau deploymentnya nanti *Web Application Firewall* (WAF) di install di *firewall* terpusat yang melayani seluruh urusan WAF dan dikonfigurasi *SSL Offloading*. Sedangkan *backend Web Application Firewall* (WAF) yang menggunakan port http (*insecure*) tetap terlindungi oleh local *web application firewall* (WAF) dalam hal ini adalah *Modsecurity Apache* atau *Modsecurity Nginx*.

2.1.2. Security Hardening & Patch Management

Gambar 2. 4 Security Hardening and Patch Management System

Berdasarkan gambar di atas dapat dijelaskan bahwa *Security Hardening and Patch Management System* hampir serupa dengan *Vunlerability Assesment*. Perbedaannya terletak pada bagaimana upaya penerapan atau *hardening* atau *patching*, tidak hanya *focus* pada pencarian *bugs*, atau *vulnerability*.

Area Security Hardening pada aplikasi berbasis Web adalah sebagai berikut :

1. Sistem Operasi
2. *Firewall* di sisi Sistem Operasi
3. *Tools* dan *Software* Pendukung
4. *Software Development Kit* (SDK)
5. *Web Server*
6. *Application Server*

7. *Web Framework*
8. *Source Code*

2.1.3. Secure Development Life Cycle

Secure Software Development Life Cycle adalah Siklus Pengembangan Sistem Informasi yang dalam tahapannya disisipkan upaya pencegahan gangguan keamanan informasi atau *hardening Security*.

Gambar 2. 5 Secure Software Develoment Life Cycle

Berikut ini adalah High level Design pada Secure Software Development.

1. *Planning*

   Pengembang dan Ahli keamanan harus mempertimbangkan dan merencanakan bahaya tipikal yang akan menuntut perhatian selama pengembangan pada tahap perencanaan.
2. *Requirement and Analysis*

   Teknologi, *Framework*, dan bahasa yang akan digunakan ditentukan pada langkah kedua SDLC. Inilah saatnya untuk memikirkan kelemahan mana yang dapat membahayakan keamanan pada tools pengembangan yang dipilih, sehingga dapat dibuat keputusan keamanan terbaik selama proses desain dan pengembangan.
3. *Architecture and Design*

   Untuk menangani risiko yang telah dievaluasi dan dianalisis selama tahap sebelumnya, tim harus mengikuti prinsip arsitektur dan desain pada tahap ini.

mungkin kerentanan tidak akan memengaruhi perangkat lunak dalam tahap pengembangan jika kerentanan tersebut ditangani di awal tahap desain. Pemodelan ancaman dan analisis risiko arsitektur adalah dua proses yang akan membuat proses pengembangan lebih mudah dan aman.

4. *Development*

   Selama proses pengembangan, tim harus memastikan bahwa standar *Coding* yang aman diikuti. Pengembang harus memperhatikan setiap kerentanan keamanan dalam kode saat menyelesaikan tinjauan kode standar untuk memastikan proyek memiliki fitur dan fungsionalitas yang diinginkan

5. *Testing*

   Untuk meningkatkan keamanan aplikasi, langkah pengujian harus memasukkan pengujian keamanan menggunakan teknologi DevSecOps otomatis. Sangat penting untuk diingat bahwa metodologi DeSecvOps memerlukan pengujian berkelanjutan di seluruh SDLC. Pengujian awal dan sering adalah teknik yang paling efektif untuk memastikan bahwa barang dan SDLC Anda aman sejak awal. Ini berarti bahwa pengujian keamanan harus dimulai sejak awal proses pengembangan dan tidak boleh diakhiri dengan penerapan dan implementasi

6. *Maintenance*

   Meskipun tim sangat teliti selama pengujian, Bersiaplah untuk menangani kesalahan atau bahaya yang sebelumnya tidak diketahui, dan periksa kembali apakah konfigurasi dilakukan dengan benar.

Langkah-langkah keamanan harus diikuti selama pemeliharaan perangkat lunak, bahkan setelah penerapan dan implementasi. Produk harus diperbarui secara berkala untuk memastikan bahwa produk tersebut aman dari kerentanan baru dan kompatibel dengan alat baru apa pun yang diputuskan untuk digunakan.

2.1.4. Vulnerability Management

Adalah proses mengidentifikasi, mengukur, dan memprioritaskan (atau memberi peringkat) kerentanan dalam suatu sistem informasi / Aplikasi. Dalam hal Penanganan dan Pengawasan Kerentanan PDNS menggunakan dua Prinsip yaitu:

1. *Periodic Vulnerability Assesment*

   Periodic Vulnerability Asessment adalah upaya *Vulnerability Assesment* terhadap Asset Sistem Informasi / Aplikasi yang dilakukan secara otomasis oleh *Engine*

Automated Vulnerability Management (AVM). *Automated Vulnerability Management* (AVM) adalah upaya pemindaian kerentanan terhadap aset sistem informasi / Aplikasi yang secara otomatis memindai target target asset dan memberikan report secara berkala. Hal ini sangat bermanfaat guna upaya proaktif pencegahan ganguan keamanan informasi secara dini. Kelemahannya adalah, *engine* ini hanya terbatas pada jumlah *Domain* atau dan *IP Address* Aplikasi web yang menjadi target, sedangkan terdapat ratusan hingga ribuan proyeksi aplikasi web yang berjalan

2. *Incidental Vulnerability Assesment*

   Incidental Vulnerability Assesment adalah upaya untuk menemukan celah kerentanan yang dilakukan di waktu tertentu.. *Best Practise* yang digunakan dalam *Vulnerability Assesment* tersebut adalah OWASP 4.0 sebagai berikut.

Gambar 2. 6 Vulnerability Assesment OWASP 4.0

Namun dalam hal mempersingkat waktu dan mempermudah jalannya *Vulnerability Assesment* disarankan menggunakan *Metode Blackbox Testing*. *Blackbox Testing* yang dilaksanakan memungkinkan adanya pengujian tanpa kredensial maupun informasi bantuan lainnya. Pertimbangan lain *Blackbox Testing* adalah Sistem / Aplikasi web akan diuji dengan pola serangan dan hak akses yang sama dengan cracker maupun *Black Hat*. Jadi *Blackbox Testing* dianggap mewakili atau memodelkan kondisi dan situasi di lingkungan *Production* yang sesungguhnya. Kondisi yang menjadi potensi kelemahan dari metode ini adalah terbatasnya jumlah personil *Vulnerability Assesment* dalam menjalankan proses pengujian kerentanan di setiap Aplikasi / Modul / Sub aplikasi / layanan sistem yang diperkirakan berjumlah banyak dan harus dilaksanakan masing masing minimal dua tahun sekali

2.1.5. Backup Recovery

Backup dan *Recovery* dalam desain ini adalah sebuah konsep *Disaster Recovery Center*. *Disaster Recovery Center* atau DRC adalah suatu tempat yang secara khusus ditujukan untuk

menempatkan sistem, aplikasi, hingga data-data cadangan SPBE ketika terjadi gangguan serius atau bencana yang menimpa satu atau berbagai unit kerja di SPBE. Pada prinsipnya Sistem sebesar SPBE sudah memiliki Sifat "*High Availability*", yang sudah mampu menjawab kemungkinan terjadinya "*Hardware Failure*", pada satu lokasi. Aset Data yang sangat berharga mengharuskan pengamanan data harus menjawab tantangan ancaman terhadap bencana atau *Total Failure* yang terjadi dalam satu lokasi. Untuk menanggulanginya maka dibuatlah konsep *Disaster Recovery Center*.

Ada berapa metode *Disaster Recovery Center* (DRC) yaitu :

1. *Cold Backup*

   Cold Backup atau yang lebih familiar disebut "*Offline Backup*", adalah metode *Backup* dan *Restore* sebuah data atau database yang dilakukan secara manual dan membutuhkan waktu proses yang sangat lama. Metode ini sangat tidak disarankan.
2. *Warm Backup*

   Warm Backup adalah sebuah Metode *Backup* yang *Active Passive Replication* yang memungkinkan adanya otomatisasi backup dari satu site ke site yang lainnya. Kekurangannya adalah proses *recovery*-nya masih membutuhkan proses manual walaupun dapat dilakukan dengan cepat.
3. *Hot Backup*

   Hot Backup atau *Active Replication* adalah metode replikasi yang paling sempurna namun membutuhkan *effort* yang sangat tinggi. *Hot Backup* nyaris tidak memiliki jeda waktu untuk perpindahan dari main site ke *backup site* karena keduanya *active* secara bersamaan. Ini merupakan metode paling ideal namun kurang realistis.

Dari ketiga metode *Backup* dan *Recovery* tersebut kami mengusulkan penggunaan *Warm Backup* atau *Active Passive Replication*. Kita sepakat bahwa hanya ada dua jenis data. Yaitu data berupa file dan data berupa database. Data berupa Database akan dilindungi dengan Repliaksi database yang node nya adalah server Database di Datacenter (*active*) dan *Server Database* di DRC (*Passive*). Sedangkan untuk perlindungan pada data berupa file maka dilakukan proses replikasi atau geo replication setiap terdapat perubahan data di *persistent storage*.

2.1.6. Penetration Testing

Metode Penetration Testing yang direkomendasikan adalah "Penetration Testing Life Cycle", sebagai berikut

1. Reporting

2. Pre Engagement Interactions
3. Reconnaissance or OSINT
4. Threat Modelling & Vulnerability Identification
5. Exploitation
6. Post-Exploitation, nalysis, & Recommendations

Penetration Testing adalah Upaya Pengujian keamanan yang menjadi kelanjutan dari Vulnerability Assesment (VA). Apabila diketemukan adanya kerentanan yang bersifat High atau Medium maka proses penetration testing dapat dilakukan.

2.1.7. Security Information and Event Management (SIEM)

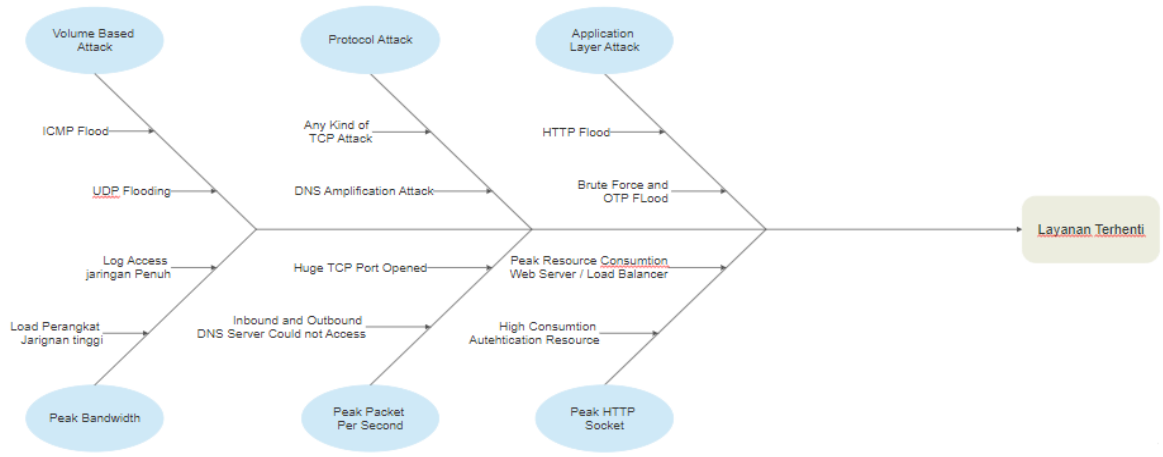
Perangkat lunak SIEM menggabungkan *Security Information Management* (SIM) dan *Security Event Management* (SEM) untuk menyediakan analisis *real-time* dari peringatan keamanan yang dihasilkan oleh aplikasi dan perangkat keras jaringan. Perangkat lunak SIEM mencocokkan peristiwa dengan aturan dan mesin analitik dan mengindeksnya untuk pencarian sub-detik guna mendeteksi dan menganalisis ancaman tingkat lanjut menggunakan intelijen yang dikumpulkan secara global. Ini memberi tim keamanan wawasan dan rekam jejak aktivitas dalam lingkungan TI mereka dengan menyediakan analisis data, korelasi peristiwa, agregasi, pelaporan, dan manajemen log. Adapun *Componenent and Capabilities* of SIEM, diantaranya :

1. *Log Collection*
2. *Log Analysis*
3. *Event Corelation*
4. *Log Forensics*
5. *IT Compliance*
6. *Application Log Monitoring*
7. *Object Access Auditing*
8. *Real-time Alerting*
9. *User Activity Monitoring*
10. *Dashboards*
11. *Reporting*
12. *File Integrity Monitoring*
13. *System and Device Log Monitoring*
14. *Log Retention*

2.1.8. Anti dDOS

DDoS adalah jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan. Umumnya serangan ini dilakukan menggunakan beberapa Server host penyerang sampai dengan Server target tidak bisa diakses. Menurut analisis kami penanganan DDOS tidak dapat diselesaikan oleh sumber daya internal seperti *Bandwidth, Firewall, Networking* dann *Web Server* Sendiri, Melainkan harus melibatkan penyedia Infrastruktur yang memiliki kemampuan penyediaan Kapasitas yang besar dalam Penanganan serangan *Distributed Denial of Service* (DDOS). Maka dari itu penanganan anti dDOS tidak hanya melibatkan alat pelindung atau anti dDOS namun juga melibatkan Pihak *eksternal* seperti ISP maupun CDN. ISP harus mau dan mampu melakukan pemblokiran akses pada sejumlah IP yang telah terindikasi melakukan serangan dDOS. Jika memungkinkan *Content Delivery Network* (CDN) bisa dimanfaatkan dalam penggunaan anti dDOS pada aplikasi / domain yang perlu diamankan.

Anti dDOS harus mampu memeberikan perlindungan terhadap jenis serangan berikut ini berdasarkan hasil analisis berikut ini.



Gambar 2. 7 Analisis Anti dDOS SPBE

Berikut ini adalah uraian dari gambar di atas

Gambar 2. 8 Uraian hasil Analisis Anti dDos

Jenis Serangan	Serangan	Deskripsi Serangan	Dampak
Volume Based Attack	ICMP *Flooding*	adalah serangan dimana penyerang membanjiri korban dengan paket "*echo request*" (ping) ICMP secepat mungkin tanpa menunggu balasan	Log Akses Jaringan dipenuhi informasi serangan DOS

Jenis Serangan	Serangan	Deskripsi Serangan	Dampak
	UDP *Flooding*	adalah jenis serangan yang memanfaatkan protokol UDP dengan mengurangi sambungan (*connectionless*) untuk menyerang target	Beban akses perangkat jaringan menjadi tinggi *Bandwidth* tinggi
Protocol Attack	DNS Amplification	Serangan DNS Amplification merupakan serangan yang memanfaatkan Open DNS Server dimana attacker akan memanipulasi Query (permintaan) normal menjadi permintaan palsu,serangan ini akan membanjiri permintaan palsu (*False Query*) dalam jumlah yang sangat banyak dengan tempo yang sangat cepat	Port TCP/IP dalam satu IP *address* dipenuhi open Port DNS
Application Layer Attack	HTTP *Flood*	Adalah salah satu jenis serangan yang secara spesifik menjadikan http atau https sebagai target. Sebetulnya http *flood* masuk ke dalam kategori *volume based attack* namun menurut Analisa kami di dalam kasus ini http flood yang terjadi menjadi bagian tersendiri	Web Server tidak mampu lagi melayani *legitimate Traffci* karena sumber daya sibuk melayani permintaan *flooding*
	Brute Force	Adalah upaya menghentikan layanan dengan cara memberikan permintaan service login secara terus menerus dari berbagai sumber IP.	Layanan Otentikasi di dalam aplikasi tidak dapat lagi melayani proses otentikasi dengan baik

BAB III
KEAMANAN JARINGAN INTRA PEMERINTAH

3.1 STANDAR DAN KEBIJAKAN JARINGAN INTRA PEMERINTAH

3.1.1 Secure Protocol

Protokol keamanan pada dasarnya adalah protokol komunikasi - urutan tindakan yang disepakati yang dilakukan oleh dua atau lebih entitas yang berkomunikasi untuk mencapai beberapa tujuan yang diinginkan bersama - yang menggunakan teknik kriptografi, memungkinkan entitas yang berkomunikasi untuk mencapai tujuan keamanan. Sebuah protokol tertentu, bagaimanapun, dapat memungkinkan pihak yang berkomunikasi untuk menetapkan satu atau lebih tujuan tersebut. Beberapa tujuan keamanan umum termasuk otentikasi (data dan entitas), kerahasiaan dan integritas. Dalam hal *focus* terhadap Desain dari Keamanan yang diusulkan, kami menentukan bahwa *Web Application* menjadi *focus* utama mengingat *web application* menjadi sumber kerentanan paling tinggi.

Berikut ini adalah Rekomendasi *Secure* Protokol pada Aplikasi berbasis Web:

1. *Remote Akses* dan *File Sharing*

   Remote Akses dan *File Sharing* yang dimaksudkan adalah sebuah Protokol Keamanan yang digunakan pada saat melakukan *remote akses* atau dan unggah maupun unduh file dari dan ke server. ada dua mekanisme untuk *Remote Akses* dan *File Sharing* diantaranya:

   a) *Bastion Host*

      Bastion Host adalah sebuah *Mekanisme* Penerapan *Firewall* atau dan DMZ yang memungkinkan hanya ada satu *Host* yang dapat menerima koneksi *remote akses* atau *file sharing* dari *Internet*. *Host* yang diberikan akses tadi berada di dalam satu *autonomous system* (AS) yang sama dengan target server atau *storage* yang akan di remote atau di akses.

   b) *Virtual Private Network* (VPN) / *Tunneling Protocol*

      Sebuah cara aman untuk mengakses *local area network* yang berada pada jangkauan tertentu, dengan menggunakan *internet* atau jaringan umum lainnya untuk melakukan transmisi data paket.

2. *Transport Layer Security*

   Protokol Keamanan pada *Transport Layer* dalam *focus* pada aplikasi adalah TLS / SSL. *Transport Layer Security* (TLS) adalah protokol enkripsi yang digunakan untuk transmisi data di *Internet*. Protokol ini menjelaskan standar umum yang dapat

diimplementasikan di lingkungan tertentu. Dalam pnerapannya di dalam aplikasi web maka TLS diwujudkan dalam Bentuk *Http Over* SSL. jadi semua aplikasi web baik yang kritikal maupun yang tidak, harus menerapkan *protocol* SSL HTTP ini untuk dua tujuan.

a) Pencegahan *Man In the Midle Attack* (MITM)

   Dengan Menggunakan *HTTP Over* SSL maka dapat dipastikan bahwa paket yang berjalan di atasnya sepenuhnya *encrypted* dan tidak dapat dilihat atau dirubah datanya pada saat proses Transmisi. Hanya *Web Browser* maupun *Endpoint* yang dituju saja yang dapat membuka atau melihat data yang dikirimkan.

b) Pencegahan Penipuan Web

   SSL Memiliki Level "*Trusted*", bagi pemilik Domain dan Server nya. Semakin tinggi levelnya maka semakin "*trusted*", webnya. Ada beberapa jenis verifikasi di antaranya adalah *Domain Verification* (DV), *Organization Verification* (OV), dan *Enterprised Verfication* (EV).

3. CSRF *Token*

   Cross-Site Request Forgery atau CSRF adalah salah satu teknik *hacking* yang dilakukan dengan cara mengeksekusi perintah yang seharusnya tidak diizinkan, tetapi output yang dihasilkan sesuai dengan yang seharusnya. Contoh serangan jenis ini: mencoba untuk login lewat media selain *web browser*, seperti menggunakan CURL, menembak langsung endpoint login. Masih banyak contoh lainnya yang lebih ekstrim. Csrf token sendiri merupakan sebuah *random string* yang di-generate setiap kali halaman form muncul. Biasanya di tiap *POST request*, token tersebut disisipkan sebagai *header*, atau form data, atau *query string*.

   Dengan adanya CSRF Token, Hanya Form HTML atau *Client Site* tertentu yang dapat mengirimkan *request POST* ke dalam *Server Backend*. Ini sangat diharuskan untuk diterapkan disemua Form Post aplikasi Web

4. *Algoritma Hashing*

   Algoritma hash merupakan fungsi yang dapat digunakan untuk memetakan data dari yang bersifat acak menjadi data ukuran tetap. Nilai hash, kode hash, dan jumlah hash akan dikembalikan selama fungsi hashing berlangsung. Hash algoritma yang disarankan adalah Algoritma Hash yang dibuat secara kombinasi antara satu Hash algoritma dengan hash algoritma yang lain.

3.1.2 IPS / IDS

Intrusion Prevention System (IPS) adalah sebuah aplikasi yang bekerja untuk monitoring traffic jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan pencegahan dini

terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya. Ada beberapa jenis IPS yaitu: *Host-based Intrusion Prevention System* dan *Network Intrusion Prevention System*.

a) *Host-based Intrusion Prevention System*

Host Based IPS (HIPS) bekerja dengan memaksa sekelompok perangkat lunak fundamental untuk berkovensi secara konstan. Hal ini disebut dengan *Application Binary Interface* (ABI). Hampir tidak mungkin untuk membajak sebuah aplikasi tanpa memodifikasi *Application Binary Interface*, karena konvensi ini bersifat universal di antara aplikasi-aplikasi yang dimodifikasi. HIPS merupakan sebuah system pecegahan yang terdiri dari banyak layer, menggunakan packet filtering, inspeksi status dan metode pencegahan intrusi yang bersifat real-time untuk menjaga host berada di bawah keadaan dari efisiensi performansi yang layak.

Mekanisme kerjanya yaitu dengan mencegah kode-kode berbahaya yang memasuki host agar tidak dieksekusi tanpa perlu untuk mengecek threat signature. Program agent HIPS diinstall secara langsung di sistem yang diproteksi untuk dimonitor aktifitas sistem internalnya. HIPS di binding dengan kernel sistem operasi dan services sistem operasi. Sehingga HIPS bisa memantau dan menghadang system call yang dicurigai dalam rangka mencegah terjadinya intrusi terhadap host. HIPS juga bisa memantau aliran data dan aktivitas pada aplikasi tertentu. Sebagai contoh HIPS untuk mencegah *intrusion* pada webserver misalnya. Dari sisi security mungkin solusi HIPS bisa mencegah datangnya ancaman terhadap host. Tetapi dari sisi *performance*, harus diperhatikan apakah HIPS memberikan dampak negatif terhadap *performance host*. Karena menginstall dan binding HIPS pada sistem operasi mengakibatkan penggunaan *resource* komputer *host* menjadi semakin besar.

b) *Network Intrusion Prevention System*

Network Based IPS (NIPS), yang juga disebut sebagai "*In-line proactive protection*", menahan semua trafik jaringan dan menginspeksi kelakuan dan kode yang mencurigakan. Karena menggunakan *in-line* model, performansi tinggi merupakan sebuah elemen krusial dari perangkat IPS untuk mencegah terjadinya *bottleneck* pada jaringan. Oleh karena itu, NIPS biasanya didesain menggunakan tiga komponen untuk mengakselerasi performansi *bandwidth*, yaitu: *Network Chips* (*Network processor*), FPGA *Chips* dan ASIC *Chips*

Network Based IPS (NIPS) biasanya dibangun dengan tujuan tertentu, sama halnya dengan *switch* dan *router.* Beberapa teknologi sudah diterapkan pada NIPS, seperti

signature matching, analisa *protocol* dan kelainan pada *protocol*, identifikasi dari pola trafik, dan sebagainya. NIPS dibuat untuk menganalisa, mendeteksi, dan melaporkan seluruh arus data dan disetting dengan konfigurasi kebijakan keamanan NIPS, sehingga segala serangan yang datang dapat langsung terdeteksi. Kebijakan keamanan NIPS sendiri terdiri dari:

1. *Content based Intrusion Prevention System*, yang bertugas mengawasi isi dari paket-paket yang berlalu lalang dan mencari urutan yang unik dari paket-paket tersebut, berisi virus *worm*, trojan horse,dll.
2. *Rate based Intrusion Prevention System*, bertugas mencegah dengan cara memonitor melalui arus lalu lintas jaringan dan dibandingkan dengan data *statistic* yang tersimpan dalam *database*.

Apabila RBIPS mengenali paket-paket yang tidak jelas, maka langsung mengkarantina paket tersebut. Dari dua jenis IPS tersebut kami menyarankan untuk menggunakan NIPS yang *Opensource*. Berikut ini adalah Rekomendasi Penerapan Konfigurasi IPS / IDS sesuai Perban BSSN No 4 tahun 2021:

- Penerapan *Konfigurasi Sentralisasi* Log IDS / IPS (*Log Management*)
- Penerapan *Signature* / Standar keamanan IDS / IPS
- Penerapan Konfigurasi *Backup Log* IDS / IPS
- Penerapan Kontrol Pembuatan Laporan Pengawasan *Intrusion* yang terdeteksi IDS maupun IPS

3.1.3 *Firewall*

Firewall jaringan adalah perangkat keamanan yang digunakan untuk menghentikan atau mengurangi akses tidak sah ke *Private Network* yang terhubung ke *Internet*, terutama intranet. Satu-satunya lalu lintas yang diizinkan di jaringan ditentukan melalui kebijakan firewall – lalu lintas lain yang mencoba mengakses jaringan diblokir. *Firewall* jaringan berada di garis depan jaringan, bertindak sebagai penghubung komunikasi antara perangkat internal dan eksternal. Kami menyarankan untuk Menggunakan metode *Whitelisting Inbound firewall* pada *Circuit Level Firewall* | *Network Firewall dan Blacklisting inbound firewall* pada *Application Level Firewall*.

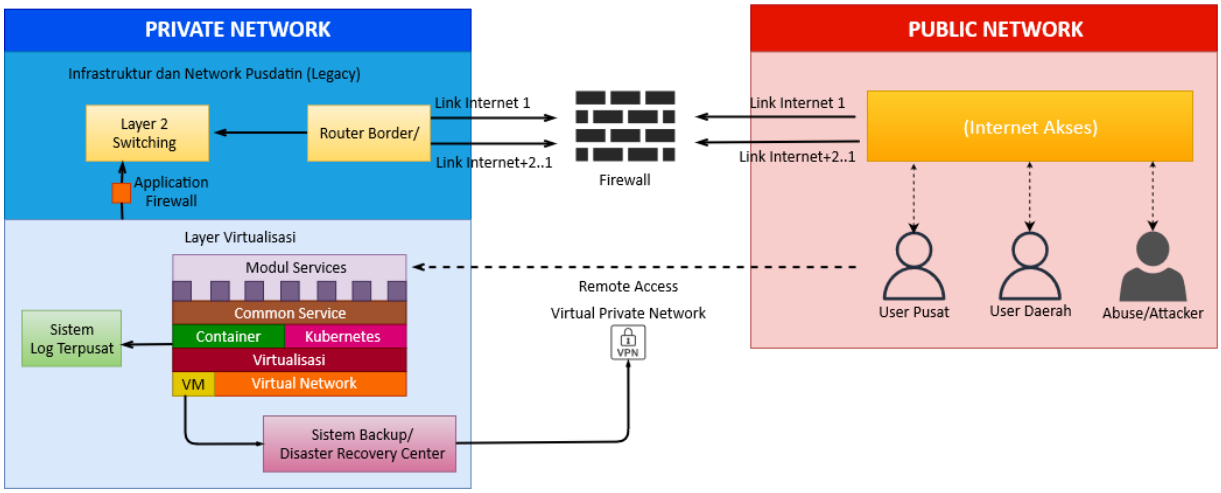
Berikut ini adalah Rekomendasi Penerapan Konfigurasi *Firewall* sesuai Perban BSSN No 4 tahun 2021:

- Penerapan *Application* Level Gateway (WAF, IDS, IPS). WAF sudah dijelaskan di bagian "*Web Application Firewall*", sedangkan IDS dan IPS akan dijelaskan di pembahasan berikutnya.
- Penerapan WAF dan Layer 7 Firewall. WAF sudah dijelaskan di bagian "*Web Application Firewall*"
- Penerapan *Inspection Packet filtering* (*Whitelisting*). Penutupan *Traffic* selain dari akses yang diizinkan.
- Penerapan *Circuit Level Firewall (Layer 3)* (*Whitelisting*).
- Penerapan *Backup* log dan *versioning firmware* Perangkat perimeter *Security*
- Penerapan Kontrol Pembuatan Laporan Pengawasan akses tidak sah yang terdeteksi *firewall*
- Penerapan Pembatasan *Incomming Traffic* (*Input* setiap Node) dikonfigurasi secara *Whitlisting*
- Penerapan Pembatasan *Incomming Traffic* (*Forward*) dikonfigurasi secara Blacklisting
- Penerapan Pembatasan *Outgoing Traffic* (*Input*, *forward*, *Output*) dikonfigurasi *allow all*.

3.1.4 Virtual Private Network (VPN)

VPN adalah Sebuah cara aman untuk mengakses *local area network* yang berada pada jangkauan tertentu, dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data. Berikut ini adalah Rencana Rekomendasi Penerapan *Virtual Private Network* berdasarkan Perban BSSN No 4 Tahun 2021.

- *Protocol* VPN yang digunakan adalah *Open* VPN
- VPN Server dibawah kendali *Router* VPN Jaringan Internal
- Autentikasi Menggunakan *Metode Key* file dan *Passphrase* (*Password*)
- Rencana Konfigurasi dan Dokumentasi *Repositori file Private Key* (.ovpn) dan Passphrase dalam penyimpanan tertentu
- Rencana Dokumentasi *Access Controll* Pengguna VPN *Client*
- Standarisasi Distribusi file .ovpn dari Operator VPN ke *User*



Gambar 3. 1 Arsitektur Konseptual Keamanan Informasi SPBE di Level Akses

Gambar di atas menjelaskan bahwa semua akses yang dilakukan developer maupun Admin pusat maupun tim pengelola layanan hanya dapat mengakses sistem melalui *Remote Akses* VPN. Hal ini disebabkan karena tujuan akses mereka adalah *asset* kritikal sistem.

3.1.5 Network Time Management

Network Time Management merupakan sebuah pengelolaan waktu di dalam seluruh perangkat yang terkoneksi ke jaringan. Tujuannya adalah untuk memastikan bahwa waktu yang berjalan di setiap *server*, *storage, controller, switch* dan perangkat lainnya memiliki tingkat akurasi waktu yang tinggi dan seragam. Waktu ini menjadi penting dalam penjaminan kualitas integrasi data dan informasi di dalamnya. *Network time Management* diwujudkan melalui *Network Time Protocol* yang disarankan Badan siber dan Sandi Nasional (BSSN) sebagai berikut :

1. Alamat server ntp.bsn.go.id
2. *Pool Server* merupakan mesin atau server yang dengan sukarela menjadikan dirinya sebagai NTP Server untuk publik. Umumnya, *pool* ini terkoneksi dengan NTP Server stratum 2, sehingga waktunya pun cukup akurat, tapi tak cukup akurat untuk mendekati hingga ke *milisecond*
3. NTP Server BSN merupakan stratum 1 (yang langsung terkoneksi dengan stratum 0), maka waktu yang didapat dari server tersebut sangat akurat hingga ke *millisecond*.

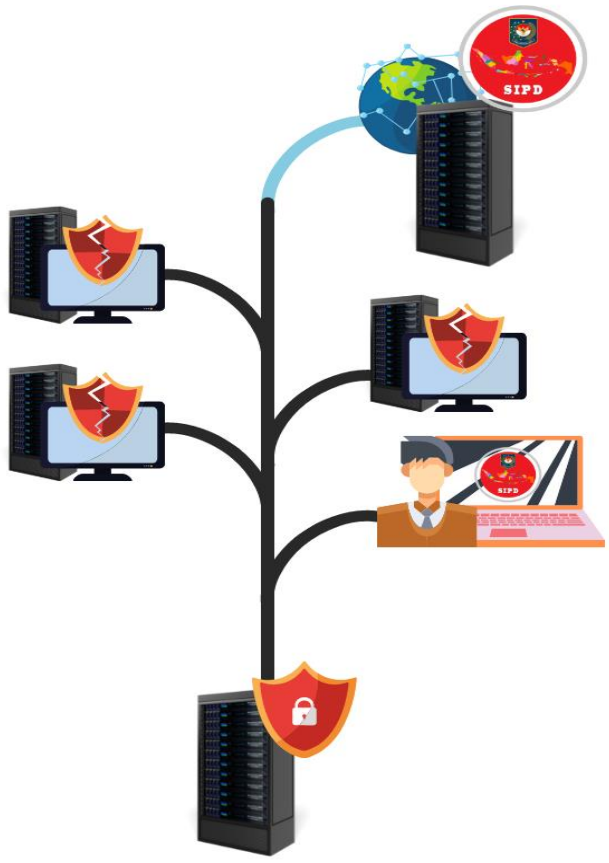
3.1.6 Multi Factor Authentication

Multi Factor Authentication atau minimal disebut dengan *Two Factor Authentication* adalah metode keamanan yang membutuhkan dua jenis autentikasi yang dilakukan pengguna. Pada

metode ini minimal menggunakan login via email sebagai token kedua autentikasi pengguna. Secara lebih detail dijelaskan di bagian aplikasi masing masing modul otentikasi atau login.

3.1.7 Anti Malware / Anti Virus

Anti malware / *Anti virus* harus digunakan aktif di semua perangkat yang memiliki Sistem Operasi baik windows maupun *Linux*. Rekomendasi Penggunaan *Antivirus* / *Anti Malware* Terpusat.



Gambar 3. 2 Anti Malware / Antri Virus

3.1.8 Physical Security

Phisical Security merupakan aspek keamanan yang harus dipenuhi guna menjaga *asset* fisik dari gangguan keamanan informasi maupun gangguan ketersediaan. Kami mengusulkan *desain physical security* dalam bentuk syarat prosedur keamanan fisik sebagai berikut:

1. Menyediakan Tempat/Lokasi Gedung Pusat Data yang Stragetegis sesuai dengan Standar Nasional Indonesia

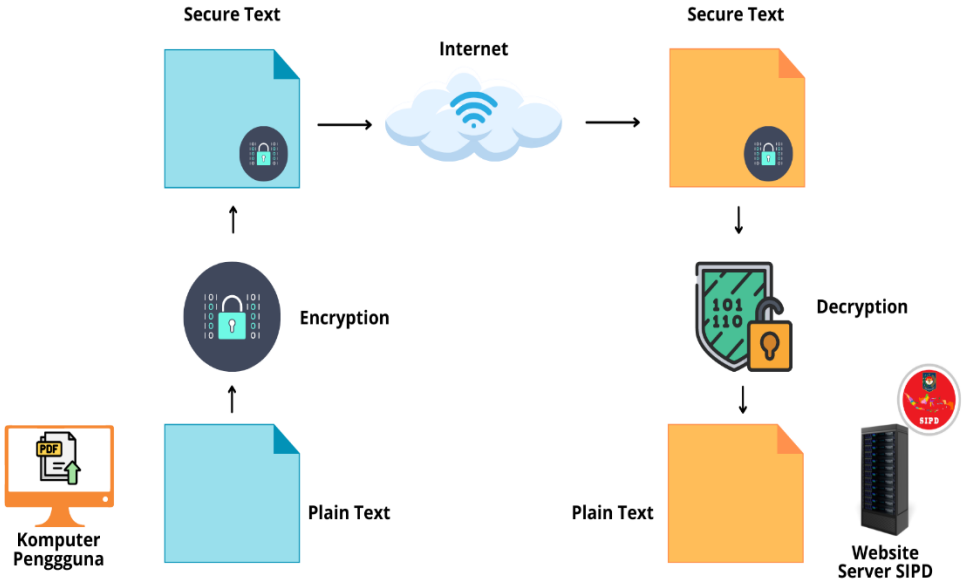
2. Menyediakan Tempat/Lokasi Gedung Pusat Data yang Tahan Gempa sesuai dengan Standar Nasional Indonesia
3. Menyediakan Tempat/Lokasi Gedung Pusat Data yang Tahan Beban sesuai dengan Standar Nasional Indonesia
4. Spesifikasi material gedung yang menunjukkan ketahanan material gedung pusat data sesuai dengan kriteria SNI.
5. Memiliki Sistem Monitoring yang menunjukkan fitur monitoring dimiliki oleh gedung pusat data sesuai dengan kriteria SNI
6. Sistem Kelistrikan / Skema catu daya listrik yang menunjukkan spesifikasi distribusi jaringan sistem kelistrikan dari catu daya sesuai dengan kriteria SNI. Skema kesinambungan listrik yang menunjukkan distribusi jaringan sistem kelistrikan berkesinambungan dengan catu daya cadangan seperti genset dan *Uninterruptible Power Supply* (UPS) dengan pemisahan panel–panel distribusi listrik untuk area pusat data hingga perangkat yang berada didalam gedung pusat data sesuai dengan kriteria SNI. Skema konstruksi panel listrik yang menunjukkan kontruksi panel listrik, khususnya untuk panel induk sesuai dengan kriteria SNI. Skema jalur kabel listrik yang menunjukkan skema pemisahan jalur kabel bermuatan listrik yang tercatat dalam dokumentasi dan diagram sesuai dengan kriteria SNI. Skema jalur kabel listrik yang memuat lokasi pembumian yang menunjukkan bahwa Pusat data memiliki pembumian bagi perangkat teknologi informasi, panel elektrikal, perangkat dari bahan metal dan pembumian penangkal petir sesuai dengan kriteria SNI. Hasil perhitungan PUE yang menunjukkan perhitungan efisiensi pemakaian listrik pada pusat data (*Power Usage Effectiveness*) terhadap keseluruhan beban daya maksimum pusat data. Penyediaan bahan bakar yang menunjukkan jumlah dan kapasitas tanki bahan bakar penyuplai genset untuk melayani operasi pusat data sesuai dengan kriteria SNI
7. Sistem Pengelolaan Keamanan yang menunjukkan fitur keamanan dimiliki oleh gedung pusat data sesuai dengan kriteria SNI
8. Prosedur keamanan fisik ruang peralatan yang menunjukan kendali akses untuk memasuki berbagai ruang pusat data dengan mempergunakan berbagai moda
9. Prosedur keamanan fisik perimeter yang menunjukan pembatasan fisik antara berbagai ruangan di pusat data.
10. prosedur manajemen keamanan merupakan kerangka kerja dalam pengelolaan keamanan pada area pusat data yang meliputi keamanan fisikal dan keamanan logikal, akses data dan informasi yang mengacu kepada standar yang ditentukan.

BAB IV
KEAMANAN SISTEM PENGHUBUNG LAYANAN PEMERINTAH

4.1 STANDAR DAN KEBIJAKAN SISTEM PENGHUBUNG LAYANAN

4.1.1 Secure File Sharing

Secure File Sharing adalah sebuah Desain Keamanan informasi yang memastikan proses Transaksi pengiriman file tidak terjadi alterisasi atau *Man in the midle attack* atau *Packet Sniffing*. Dalam hal Realisasi dari *Secure File Sharing* ini kami merancang *Secure File Transfer Protocol* (SFTP) sebagai Protokol utama *Secure file sharing*.



Gambar 4. 1 Secure File Transfer Protocol pada SPBE

4.1.2 Digital Signature

Digital signature adalah jenis tanda tangan elektronik khusus yang dibuat menggunakan aplikasi eSign khusus. Tanda tangan digital ini menggunakan kriptografi untuk melindungi dokumen dan juga menyematkan detail seperti alamat *email*, kapan dan di mana Penandatanganan dokumen apa pun, dan perangkat apa yang digunakan untuk melakukannya. TTE menciptakan sidik jari digital yang membuat dokumen itu unik dan jejak kertas yang dapat diverifikasi secara independen

Semua dokumen yang dikeluarkan oleh SPBE tidak lagi ditandatangani secara manual melainkan melalui Tanda tangan digital. Nantinya SPBE akan terintegrasi dengan aplikasi E-Sign Kemendagri

4.1.3 Privilege Access Management

Privilege Access Management merupakan kelanjutan dari *Identity* and *Access Management*. Di dalam aplikasi maupun sistem informasi, harus ada satu modul khusus yang berfungsi untuk memberikan hak akses pada setiap Pengguna yang sudah disediakan di IAM.