BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, kebutuhan akan infrastruktur jaringan yang andal dan aman menjadi sangat penting, terutama bagi instansi pemerintah seperti Kantor Camat Basa Ampek Balai Tapan. Peningkatan layanan digital dan penggunaan teknologi informasi dalam administrasi pemerintahan telah membawa berbagai keuntungan, seperti kemudahan dalam pengelolaan data, akses informasi yang cepat, serta efisiensi operasional. Namun, perkembangan ini juga disertai dengan berbagai tantangan, salah satunya adalah ancaman keamanan jaringan (Sulistyo and Sartomo 2022).

jaringan yang terhubung ke Internet pada dasarnya tidak aman dan selalu dapat dimanfaatkan oleh peretas, baik jaringan LAN maupun nirkabel. ketika data dikirim, ia melakukan perjalanan melalui beberapa terminal untuk mencapai tujuannya, memberikan kesempatan kepada pengguna lain yang tidak bermoral untuk mencegat atau memodifikasi data. Dalam pengembangan desain ini, sistem keamanan jaringan yang terhubung ke Internet harus dirancang dan dipahami dengan baik sehingga sumber daya jaringan dapat dilindungi secara efektif dan serangan hacker diminimalkan (Nurnaningsih, Riskayani, and Anniar Husnang 2022).

Sebagai lembaga yang menangani data sensitif, Kantor Camat Basa Ampek Balai Tapan perlu memastikan keamanan informasi dan kelancaran operasional. Sistem jaringan yang tidak terlindungi dengan baik dapat membuka celah bagi berbagai ancaman, seperti serangan siber, akses tidak sah, dan pencurian data.

Insiden seperti ini tidak hanya mengancam kerahasiaan data, tetapi juga dapat mengganggu layanan publik yang disediakan oleh kantor Camat, sehingga berdampak pada tingkat kepercayaan masyarakat.

Permasalahan muncul ketika ada aktifitas-aktifitas yang mencurigakan atau bahkan aktifitas tersebut merupakan serangan namun tidak terdaftar pada rule atau aturan yang diinputkan sehingga hal itu sangat membahayakan sebuah jaringan komputer. Penelitian ini bertujuan untuk mengetahui kualitas keamanan jaringan pada kantor Camat Basa Ampek Balai Tapan. Kemampuan IDS dan IPS dalam mendeteksi seluruh aktivitas *port* scanning adalah karena IDS dan IPS ditempatkan pada komputer yang menjadi *gateway* dan sekaligus difungsikan sebagai *Firewall*. Penempatan IDS dan IPS pada server *gateway* ini akan melindungi data yang ada di server *gateway* dari serangan hacker.

Serangan atau gangguan biasa terjadi pada komputer yang terhubung ke jaringan adalah serangan DoS dan *port* scan. DoS serangan yang berasal dari satu perangkat, sedangkan *DDoS* serangan yang lebih dari satu perangkat. DoS dan *DDoS* sama-sama serangan *traffic Flooding* yang menggunakan paket data besar yang dapat membebani dan memblokir akses ke server. Serangan yang umumnya digunakan adalah *UDP Flooding*, *SYN Flooding*, dan *Ping of Death*. *Port* scan serangan yang dilakukan dengan cara memindai *port* jaringan target, menganalisa *port* jaringan target kemudian mencari celah pada *port* target yang terbuka. Maka dari itu keamanan jaringan sangat penting dalam sebuah sistem jaringan komputer untuk menghindari serangan dan melindungi jaringan komputer dari acaman jaringan luar maupun dalam(Awal 2023).

Salah satu pendekatan yang dapat dilakukan untuk mengatasi masalah tersebut adalah dengan mengembangkan infrastruktur jaringan yang kuat dan menerapkan sistem keamanan yang memadai. Penggunaan *Firewall* dan *Intrusion Detection System* (IDS) menjadi komponen kunci dalam menjaga keamanan jaringan. *Firewall* berfungsi sebagai penghalang awal yang memfilter lalu lintas jaringan dan mencegah akses yang tidak sah, sedangkan IDS berguna untuk mendeteksi aktivitas mencurigakan serta potensi serangan yang dapat terjadi dalam jaringan(Aryanti, Khairil, and Aspriyono 2023).

IDS adalah sebuah sistem yang dapat secara otomatis memonitor kejadian pada jaringan komputer dan dapat menganalisa masalah keamanan jaringan. IDS mampu mendeteksi penyusup dan memberikan respons secara *real-time*. Terdapat dua teknik yang digunakan dalam IDS yaitu, NIDS (Network Based *Intrusion Detection System*) dan HIDS (*Host Based Intrusion Detection System*). IDS merupakan salah satu opsi untuk meningkatkan keamanan jaringan dalam sebuah network baik intranet maupun internet. IDS (*Intrusion Detection System*) juga berfungsi sebagai sistem yang memantau lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan dan mengeluarkan peringatan saat aktivitas tersebut terdeteksi. IDS akan memberikan peringatan jika terjadi serangan dan memungkinkan pemblokiran alamat IP agar tidak dapat mengakses kembali server yang diserang. Log adalah kumpulan informasi atau data peristiwa seperti timestamp, alamat IP sumber, alamat IP tujuan, dan lainnya, yang dapat digunakan untuk membantu proses investigasi serangan siber dengan menganalisis data log tersebut (Eben, Mukramin, and Abduh 2024).

Firewall adalah sebuah sistem atau perangkat yang berperan sebagai garis pertahanan pertama dalam perlindungan sistem. Keamanan jaringan adalah suatu sistem yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data di dalam jaringan komputer. Dalam konteks ini, integritas merujuk pada keutuhan data, kerahasiaan berkaitan dengan privasi informasi, dan ketersediaan mengacu pada ketersediaan layanan dan sumber daya jaringan. Dengan meningkatnya serangan terhadap jaringan, penggunaan teknologi keamanan telah menjadi suatu keharusan.Keamanan jaringan tidak hanya melibatkan perangkat keras (hardware) dan perangkat lunak (software), tetapi juga melibatkan praktik-praktik keamanan yang efektif (Cahyawati et al. 2023).

Penenlitian yang dilakukan oleh Abdul Khaliq dan Sri pada tahun 2022 dengan judul Pemanfaatan Kerangka Kerja Investigasi Forensik Jaringan Untuk Identifikasi Serangan Jaringan Menggunakan Sistem Deteksi Intrusi (IDS), penelitian ini menunjukkan IDS adalah sistem deteksi dini jika terjadi serangan jaringan komputer. IDS akan memperingatkan administrator jaringan komputer jika terjadi serangan jaringan komputer. IDS juga mencatat semua upaya dan aktivitas yang bertujuan mengganggu jaringan komputer dan serangan jaringan komputer lainnya. Tujuan dari penelitian ini adalah untuk mengimplementasikan IDS pada sistem jaringan dan menganalisis log IDS untuk menentukan jenis dan jenis serangan jaringan komputer. Log pada IDS akan dianalisis secara mendalam untuk digunakan sebagai upaya meningkatkan keamanan jaringan komputer. Metode penelitian yang akan digunakan adalah penelitian terapan. Penelitian dilakukan dengan menggunakan *Network Forensic Investigation Framework* yang diusulkan oleh Pilli, Joshi dan Niyogi. Tahapan Kerangka Kerja Investigasi Forensik Jaringan

digunakan untuk melakukan simulasi jaringan, analisis dan investigasi untuk menentukan jenis serangan jaringan komputer. Hasil penelitian menunjukkan bahwa *Network Forensic Investigation Framework* memfasilitasi proses investigasi ketika terjadi serangan jaringan. Kerangka kerja investigasi forensik jaringan secara efektif digunakan ketika jaringan komputer memiliki aplikasi dukungan keamanan jaringan seperti IDS atau lainnya. IDS efektif dalam mendeteksi aktivitas pemindaian jaringan dan serangan DOS. IDS memberikan peringatan kepada administrator karena ada aktivitas yang melanggar aturan di IDS (Khaliq and Novida Sari 2022).

Penenlitian yang dilakukan oleh Awal dkk pada tahun 2023 dengan judul Implementasi *Intrusion Detection Prevention System* Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunkan *Snort* Dan *IPTables* Berbasis Linux, penelitian ini menunjukkan bahwa Perkembangan jaringan komputer terus berlanjut, dalam skalabilitas, jumlah node, dan teknologi. Komputer yang terhubung ke jaringan berpotensi mengalami gangguan atau serangan. Maka dari itu keamanan jaringan sangat penting dalam sebuah sistem jaringan komputer untuk menghindari serangan dan melindungi jaringan komputer. *Intrusion Detection System* (IDS) dengan *Snort* yang diimplementasikan pada sistem operasi linux dapat melakukan pemantauan serangan DoS (*Denial of Service*) dan *Port* Scanning. *Snort* mode IDS akan memberi alert secara *real-time* sesuai dengan *rules Snort* yang diatur dalam local.*rules* . *IPTables* sebagai tools IPS akan menghentikan serangan/gangguan tersebut dengan *rules IPTables* yang diterapkan. Dalam penelitian ini dilakukan pengujian sistem *Snort* IDS, *IPTables* dan pengujian kualitas layanan server. Hasil pengujian *Snort* IDS dapat memberikan *alert* bahwa

adanya serangan secara *real-time*. Hasil pengujian IPS dapat mengatasi serangan/gangguan yang masuk dengan memblokir alamat *IP intruder*. Pengujian kualitas layanan server setelah diterapkan IDPS nilai index yang diperoleh adalah 3,75 yang sebelumnya kualitas layanan server memiliki nilai index 2. Yang artinya IDPS mampu mengatasi serangan/gangguan yang masuk ke jaringan (Awal 2023).

Penenlitian yang dilakukan oleh Cahya dkk pada tahun 2023 dengan judul Implementasi *Firewall* Pada Mikrotik Untuk Keamanan Jaringan, penelitian ini menunjukkan bahwa perkembangan teknologi informasi sangat pesat. jaringan komputer sudah menjadi bagian penting dalam kehidupan sehari-hari. Meskipun perkembangan ini membawa banyak kemudahan dan manfaat, namun juga membawa tantangan baru terutama dalam hal keamanan jaringan. Keamanan jaringan sangat penting karena informasi sensitif dan data pribadi terus melewati infrastruktur jaringan. Keamanan jaringan merupakan suatu metode yang mengharuskan organisasi untuk mengantisipasi potensi ancaman. Sistem Operasi bernama Mikrotik *Router*OS adalah sebuah perangkat lunak yang bisa digunakan pada komputer agar komputer bisa menjadi sebuah *router* jaringan yang hebat dalam hal fitur yang dibuat untuk ip network dan jaringan nirkabel, serta sangat pas bila digunakan oleh ISP dan provider *HOTSPOT*. *Firewall* adalah teknologi keamanan siber yang digunakan untuk meningkatkan keamanan komputer yang terhubung ke jaringan, seperti Jaringan Area Lokal (LAN) atau Internet. Setelah mengimplementasikan *Firewall* hasil yang diperoleh adalah *Website* yang ditentukan, hasilnya implementasi *Firewall* dalam memblok *Website* berhasil diterapkan dan terbukti berhasil (Cahya et al. 2023).

Penenlitian yang dilakukan oleh Andi dkk pada tahun 2023 dengan judul Penerapan Sistem Keamanan Ids Pada Jaringan Nirkabel (*HOTSPOT*) penelitian ini menunjukkan bahwa Infrastruktur Jaringan Nirkabel memiliki satu masalah besar, terutama yang membuka akses untuk umum, seperti *HOTSPOT* adalah masalah keamanannya, dimana banyak terjadi penyerangan oleh satu atau beberapa orang penyerang (*attacker*) baik pada server penyedia *HOTSPOT* atau pengguna. Dengan demikian dibutuhkan suatu taktik atau teknik pengamanan guna menanggulangi masalah tersebut. Subyek penelitian ini adalah penerapan sistem keamanan jaringan nirkabel *HOTSPOT*. Metode yang digunakan dalam penelitian ini adalah Studi Pustaka (*Library Research*) dan observasi yaitu melakukan pengamatan secara lagsung terhadap jaringan hospot di Cafe Atrium. Analisis dilakukan untuk mendapatkan hasil serta data yang bisa dijadikan sebagai acuan guna menerapkan suatu sistem keamanan jaringan *HOTSPOT* berbasis *honeypot* dan *Snort* . Sistem hasil implementasi diuji dengan dua metode yaitu *Alpha Test* dan *Beta test*. Hasil penelitian ini adalah kombinasi antara *Honeypot* dan IDS dengan *Honeyd* dan *Snort* ini memberikan sebuah sistem keamanan berlapis dengan menipu dan mendeteksi serangan yang ditujukan ke jaringan *HOTSPOT* (Andi Muhammad Nur Hidayat 2023).

Penenlitian yang dilakukan oleh Adzimi dkk pada tahun 2024 dengan judul Implementasi Konfigurasi *Firewall* dan Sistem Deteksi Intrusi menggunakan *Debian* penelitian ini menunjukkan bahwa mengimplementasikan konfigurasi *Firewall* dan sistem deteksi intrusi (IDS) menggunakan *Debian*, guna meningkatkan keamanan jaringan secara keseluruhan. Dalam era digital yang menghadirkan berbagai ancaman siber seperti *malware*, *phishing*, dan serangan

DDoS, keamanan siber menjadi krusial. *Debian* dipilih karena stabilitas dan keamanannya, serta ketersediaan alat *open-source* seperti *IPTables* untuk *Firewall* dan *Snort* untuk IDS. Metodologi penelitian mencakup studi literatur, eksperimental, dan konfigurasi *Firewall* yang disesuaikan dengan kebutuhan spesifik jaringan, serta implementasi Wazuh sebagai IDS. Pengujian dilakukan melalui simulasi serangan untuk mengevaluasi efektivitas konfigurasi. Hasilnya menunjukkan peningkatan signifikan dalam kemampuan deteksi dan respons terhadap ancaman siber. *Firewall* berhasil memblokir akses tidak sah dan mencatat aktivitas mencurigakan, sementara Wazuh IDS mendeteksi serangan *brute force* dan *malware*, serta memberikan respons otomatis terhadap ancaman. Integrasi *Firewall* dan IDS menghasilkan pendekatan keamanan berlapis, memungkinkan pertahanan proaktif dan *real-time*. Implementasi ini menunjukkan bahwa kombinasi teknologi keamanan, pelatihan berkelanjutan, dan kebijakan yang kuat dapat memberikan perlindungan komprehensif terhadap ancaman siber (Adzimi et al. 2024).

Penenlitian yang dilakukan oleh Pitrianti dkk pada tahun 2023 dengan judul Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan *Intrusion Detection System* (IDS) Berbasis *Snort* . Penelitian ini menjelaskan tentang Kantor Sistem Administrasi Satu Atap atau yang lebih dikenal dengan Samsat Empat di Kabupaten Lawang merupakan sebuah instansi pemerintah yang menyelenggarakanpajak jalan raya yang transparan dan transparan kepada masyarakat. Permasalahandi kantor samsat kabupaten empat lawang adalah server samsat tidak terlindungi dari serangan pihak - pihak yang tidak bertanggung jawab yang dapat menyebabkankerusakan samsat di kabupaten empat lawang, baik itu

kehilangan data atau kemudiandata rusak. Berdasarkan hal tersebut diperlukan suatu sistem untuk mendeteksi serangan pada server Samsat Kabupaten Empat Lawang untuk mencegah serangandari pihak yang tidak bertanggung jawab dan mengamankan server Samsat dengan IDS (*Intrusion Detection System*) dengan *Snort* untuk mendeteksi serang(Pitriyanti, Khairani Daulay, and Agus Syamsul Arifin 2023).

Meskipun demikian, penerapan *Firewall* dan IDS di lingkungan kantor Camat menghadapi tantangan tersendiri, seperti keterbatasan anggaran, kurangnya sumber daya manusia yang terlatih, serta infrastruktur yang belum memadai. Oleh karena itu, diperlukan pengembangan yang terencana dan sistematis agar dapat mengimplementasikan solusi keamanan jaringan secara efektif dan efisien.

Berdasarkan latar belakang di atas, penelitian ini bertujuan untuk melakukan pengembangan infrastruktur jaringan dan meningkatkan sistem keamanan di Kantor Camat Basa Ampek Balai Tapan dengan memanfaatkan *Firewall* dan *Intrusion Detection System* (IDS). Diharapkan, hasil penelitian ini dapat membantu kantor Camat dalam mengelola jaringan yang lebih aman, sehingga mendukung kelancaran layanan kepada masyarakat.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas dapat disimpulkan permasalahan yang akan dibahas pada laporan ini sebagai berikut :

1. Bagaimana pengembangan Infrastruktur keamanan jaringan *Firewall* dan *Intrusion Detection System* (IDS) dapat mengoptimalkan keamanan jaringan di Kantor Camat Basa Ampek Balai Tapan?

2. Bagaimana efektivitas pengembangan *Intrusion Detection System* (IDS) dapat membantu mendeteksi dan meningkatkan keamanan serta kinerja jaringan di Kantor Camat?
3. Bagaimana pengembangan infrastruktur jaringan dapat memberikan dampak yang baik untuk kemanan jaringan pada akses layanan publik ?
4. Bagaimana hasil pengembangan sistem keamanan jaringan yang diterapkan dapat bermanfaat untuk pegawai kantor camat?

1.3 Hipotesa

Hipotesa merupakan dugaan sementara dimana nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Berdasarkan permasalahan yang ada dapat dikemukakan beberapa hipotesa sebagai berikut :

1. Di harapkan pengembangan Infrastruktur keamanan jaringan *Firewall* dan Intrusion Detection System (IDS) yang optimal dan efektif mencegah akses tidak sah dan serangan siber yang berpotensi merusak jaringan di Kantor Camat Basa Ampek Balai Tapan.
2. Di harapkan pengembangan *Firewall* dan *Intrusion Detection System* (IDS) mampu mendeteksi aktivitas mencurigakan secara *real-time*, sehingga mengurangi risiko serangan siber dan meningkatkan kinerja operasional jaringan di kantor Camat.
3. Di harapkan pengembangan infrastruktur jaringan memberikan dampak baik pada akses layanan publik di Kantor Camat Basa Ampek Balai Tapan.
4. Di harapkan hasil pengembangan sistem keamanan dapat di terapkan dapat barmanfaat sehingga berguna bagi pegawai Kantor Camat.

1.4 Batasan Masalah

Penelitian ini dibatasi pada :

1. pengembangan infrastruktur jaringan internal di Kantor Camat Basa Ampek Balai Tapan.
2. fokus pada penerapan *Firewall* dan *Intrusion Detection System* (IDS) untuk meningkatkan keamanan terhadap ancaman siber umum, tanpa mencakup teknologi keamanan lain serta jaringan eksternal, dan evaluasi dilakukan melalui uji coba di lingkungan kantor Camat.
3. Implementasi hanya menggunakan perangkat keras dan perangkat lunak yang tersedia atau terjangkau oleh Kantor Camat, seperti *router*, *switch*, *Firewall* berbasis perangkat lunak, dan IDS berbasis *open-source*.

1.5 Tujuan Penelitian

Dalam melaksanakan penelitian ini tujuan yang ingin dicapai diantaranya adalah:

1. Mengembangkan infrastruktur jaringan saat ini di Kantor Camat Basa Ampek Balai Tapan yang optimal dan efektif serta mengidentifikasi kelemahan dan potensi perbaikannya.
2. Menerapkan *Firewall* dan *Intrusion Detection System* (IDS) sebagai bagian dari sistem keamanan yang mampu melindungi jaringan kantor Camat dari serangan siber dan akses tidak sah.
3. Mengembangkan desain infrastruktur jaringan yang lebih baik dengan menerapkan teknologi *Firewall* dan *Intrusion Detection System* (IDS) untuk meningkatkan keamanan jaringan.

4. Menganalisis pemanfaatan hasil penerapan sistem keamanan jaringan setelah pengembangan, guna memastikan peningkatan keamanan dan kinerja sistem keamanan jaringan sehingga berguna bagi pegawai kantor camat.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini yaitu :

1. Menambah pengetahuan dan referensi ilmiah mengenai penerapan *Firewall* dan *Intrusion Detection System* (IDS) dalam pengembangan infrastruktur keamanan jaringan.
2. Memberikan kontribusi terhadap literatur akademis terkait strategi pengembangan jaringan yang aman dan efisien pada lingkungan pemerintahan.
3. Membantu Kantor Camat Basa Ampek Balai Tapan dalam meningkatkan keamanan jaringan, sehingga dapat mengurangi risiko serangan siber dan akses tidak sah.
4. Meningkatkan efisiensi pelayanan publik melalui sistem jaringan yang lebih aman dan andal, mendukung implementasi layanan e-government di lingkungan kantor Camat.
5. Menyediakan panduan dan rekomendasi bagi instansi pemerintahan lainnya yang ingin mengembangkan infrastruktur jaringan dan sistem keamanan berbasis *Firewall* serta IDS.

1.7 Gambaran Umum Objek Penelitian

1.7.1 Sekilas Tentang Kantor Camat Basa Ampek Balai

Kecamatan Basa Ampek Balai Tapan merupakan salah satu kecamatan di Kabupaten Pesisir Selatan, Provinsi Sumatera Barat. Kecamatan ini memiliki karakteristik geografis yang beragam, dengan wilayah yang meliputi area dataran rendah hingga pegunungan. Kecamatan ini dikenal dengan nama "Basa Ampek Balai," yang berasal dari budaya lokal Minangkabau, merujuk pada sistem pemerintahan adat yang melibatkan empat pemangku adat atau balai utama.

Sebelah utara Kecamatan Basa Ampek Balai Tapan berbatasan dengan Kecamatan Pancung Soal, sebelah selatan dengan Kecamatan Ranah Ampek Hulu Tapan, sebelah timur dengan Kecamatan Ranah Ampek Hulu Tapan dan sebelah barat dengan Kecamatan Lunang.

Kantor camat Basa Ampek Balai Tapan yang beralamatkan Nagari Tanjung Pondok Jl. Padang - Muko-Muko, Tapan, Kec. Basa Ampek Balai Tapan, Kabupaten Pesisir Selatan, Sumatera Barat. Bapak Syamwil, S.STP.,MM. yang merupakan camat Basa Ampek Balai Tapan.

Basa Ampek Balai Tapan adalah sebuah kecamatan yang terletak di bagian selatan Kabupaten Pesisir Selatan Provinsi Sumatera Barat, Indonesia. Secara administratif wilayahnya adalah sebagian wilayah Tapan yang sebagiannya lagi masuk wilayah Kecamatan Ranah Ampek Hulu Tapan. Kota Tapan berada di jalan

lintas barat Sumatera dan persimpangan yang menghubungkan tiga provinsi, yaitu Sumatera Barat, Jambi dan Bengkulu. *(sumber : Camat Tapan, 2024)*

Gambar 1. 1 Kantor Camat Basa Ampek Balai Tapan

1.7.2 Visi, Misi, Dan Tujuan Kecamatan Basa Ampek Balai Tapan

1. **Visi**

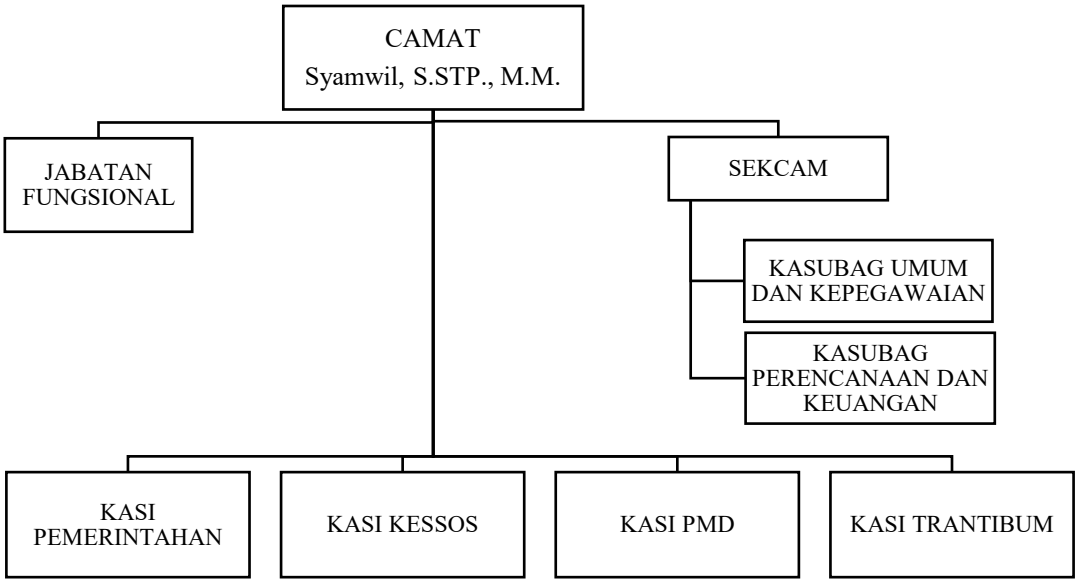
   Terwujudnya Masyarakat Kabupaten Pesisir Selatan Yang Mandiri, Unggul, Agamais Dan Sejahtera

2. **Misi**

   1) Mengupayakan reformasi secara sungguh-sungguh untuk menuju aparatur yang bersih dan responsive guna mewujudkan pelayanan prima dalampemenuhan hak-hak dasar rakyat seperti; kependudukan (akta kelahiran, KTP dan KK), kesehatan dan pendidikan;
   2) Akan menjalankan amanah masyarakat dengan mengedepankan keterbukaan (transparansi) dalam berbagai bidang, termasuk mengenai besaran anggaran yang ada dalam APBD kabupaten pesisir selatan, anggaran masuk dan keluar serta pemasukan-pemasukan bagi keuangan daerah dari luar APBD, yang selama ini belum banyak diketahui masyarakat banyak;

3) Memfokuskan pada pembangunan nyata pada perekonomian masyarakat dengan lebih memberi perhatian kepada sektorpenyumbang PDRB Terbesar, yaitu pertanian dan perkebunan, perikanan dan kelautan, pariwisata, perdaganag dan jasa serta industri pengolahan;
4) Mewujudkan kehidupan umat beragama yang rukun, toleransi dan penuh kesejukan serta memelihara, mengembangkan budaya dan kearifan lokal;
5) Pembangunan pertanian dan perkebunan, perikanan dan kelautan serta berkelanjutan dengan memberikan nilai tambah untuk kesejahteraan petani dan nelayan;
6) Mengurangi tingkat kejahatan, kriminalitas, dan peredaran obat-obatan terlarang**.**

1.7.3 Struktur Organisasi Kantor Camat Basa Ampek Balai Tapan



Gambar 1. 34 Struktur Organisasi kantor Camat Basa Ampek Balai