**STANDAR TOOLS PENGAMANAN APLIKASI BERBASIS WEB**

**DI {{nama organisasi}}**

**{{logo organisasi}}**

|  |  |
| --- | --- |
| No Dokumen | : 0.1 (Draft) |
| Revisi | : 00 |
| Tanggal Terbit | : |

|  |  |  |
| --- | --- | --- |
| Disusun  oleh : | Diketetahui  oleh: | Disetujui / Disahkan  oleh : |
|  |  |  |
| **NN**  NN | **NN**  NN | **NN**  NN |

**Riwayat Dokumen**

|  |  |  |
| --- | --- | --- |
| **Versi** | **Tanggal** | **Perubahan** |
| 0.1 (Draft) | 28/02/2023 | Rilis draft awal dengan hanya menyalin sepenuhnya konten dari **PEDOMAN TATA KELOLA KEAMANAN APLIKASI BERBASIS WEB - BSSN** |
| … | … | … |
|  |  |  |

1. **TUJUAN**
   1. Memberikan petunjuk bagi instansi – instansi yang memiliki sistem web statis, web dinamis, web dinamis dengan aplikasi transaksi, serta web dinamis dengan aplikasi transaksi yang membutuhkan tingkat availibility tinggi, agar dalam mengadakan/menyediakan tools pengamanan web mengacu/memiliki Standar minimum.
   2. Untuk memastikan bahwa dalam pengadaan perangkat pengamanan tidak terlalu berlebihan (*overkill*) ataupun terlalu minim.
2. **RUANG LINGKUP**

Standar minimum untuk:

* 1. Intrusion Detection & Prevention System (IDPS)
  2. Web Application Firewall (Firewall Aplikasi Web)
  3. Security Information and Event Management (SIEM)
  4. Network Behavioral Analysis/NBA (Analisis Perilaku Jaringan)
  5. File Integrity Monitoring (Pemantauan Integritas File)
  6. IP Reputation Engine (Mesin Reputasi IP)
  7. Synchronization System (Sistem Sinkronisasi)
  8. Network Analytic System (Sistem Analitik Jaringan)

1. **ISTILAH DAN DEFINISI**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Zero Day Vulnerability | : | informasi kelemahan keamanan dari suatu aplikasi dimana  informasi ini belum diumumkan ke publik. |
| 2. | *Zero Day Attack* | : | serangan yang dilakukan penyerang sebelum informasi kelemahan keamanan dari aplikasi tersebut diumumkan ke  publik. |
| 3. | *Zero Day Protection* |  | kemampuan aplikasi menangkal *Zero Day Attack*/ kemampuan menangkal malware bahkan pada saat malware tersebut belum  diumumkan ke publik. |

|  |  |  |  |
| --- | --- | --- | --- |
| 4. | Korelasi |  | kemampuan untuk melakukan berbagai teknik korelasi untuk mengintegrasikan berbagai sumber, untuk mengubah data menjadi informasi yang bermanfaat. Korelasi biasanya merupakan fungsi dari bagian Manajemen Peristiwa Keamanan  dari solusi SIEM lengkap |
| 5. | Proxy | : | suatu sistem yang memungkinkan kita untuk bisa mengakses jaringan internet menggunakan IP yang berbeda dengan yang  diterima oleh perangkat. |
| 6. | Instansi | : | Kementerian/Lembaga, Instansi pusat atau daerah. |
| 7. | *Password* | : | Kata sandi yang digunakan bersamaan dengan *username* (*sign*  *on/sign in/log-on/log-in*) oleh pemilik yang sah sebelum melakukan koneksi/akses ke sistem komputer. |
| 8. | *Content Delivery Network* (CDN) | : | adalah kumpulan dari server global yang terletak di beberapa data center dan tersebar di berbagai negara. Jaringan ini berfungsi untuk mengirimkan konten dari server ke suatu Aplikasi Berbasis Web.  Yang dilakukan oleh CDN adalah meningkatkan kecepatan pengiriman data melalui jaringan server kepada visitor dari lokasi terdekat yang paling memungkinkan |

1. **REFERENSI**
   1. OWASP: Application Security Verification Standard 4.0
   2. Kebijakan Keamanan Informasi .
2. **STANDAR**
3. **Intrusion Detection & Prevention System (IDPS)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * IPS adalah suatu bentuk sistem keamanan jaringan yang berfungsi untuk mendeteksi dan mencegah ancaman yang teridentifikasi. * IPS memantau jaringan secara terus-menerus, mencari   kemungkinan insiden berbahaya dan menangkap informasinya. |

|  |  |  |
| --- | --- | --- |
|  |  | * IPS melaporkan peristiwa ini ke administrator sistem dan mengambil tindakan pencegahan, seperti menutup titik akses dan mengonfigurasi firewall untuk mencegah serangan di masa depan. * Solusi IPS juga dapat digunakan untuk mengidentifikasi masalah dengan kebijakan keamanan, menghalangi karyawan dan tamu jaringan melanggar aturan yang   terkandung dalam kebijakan ini. |
| PRASYARAT | : | * Next Generation Firewall System (Sistem Firewall Generasi Lanjut) * Unified Threat Management System (Sistem Manajemen Ancaman Terpadu) |
| KOLABORASI | : | * Next Generation Firewall System (Sistem Firewall Generasi Lanjut) * Unified Threat Management System (Sistem Manajemen Ancaman Terpadu) * 0-Day Protection System (Sistem Proteksi 0-Hari) * Network Analytics System (Sistem Analitik Jaringan) |
| METODA | : | * Signature-based (Berbasis-pratKita) * Anomaly-based (Berbasis-anomali) * Policy-based (Berbasis-kebijakan) |
| SYARAT UMUM | : | * Mampu mendeteksi dan mencegah ancaman berbasis- pratKita dengan berkolaborasi dengan sistem firewall generasi lanjut dan/atau sistem manajemen ancaman terpadu. * Mampu mendeteksi dan mencegah ancaman berbasis- anomali dengan berkolaborasi dengan sistem proteksi 0- hari dan/atau sistem analitik jaringan. * Dapat mendeteksi dan mencegah pelanggaran kebijakan jaringan dengan berkolaborasi dengan sistem firewall. |

|  |  |  |
| --- | --- | --- |
| CONTOH PRODUK | : | * OSSEC (Gratis) * Sagan (Gratis) * Open WIPS-NG (Gratis, hanya untuk Jaringan Nirkabel) * Fail2Ban (Gratis) * Bro NSM (Gratis)   Untuk IDPS berbayar, saat ini hampir semuanya telah terintegrasi dengan perangkat lainnya |

1. **Web Application Firewall (Firewall Aplikasi Web)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * WAF adalah sebuah sistem firewall yang dikhususkan   untuk menyaring, memantau, dan menghalangi trafik HTTP/S dari dan oleh aplikasi web. |
| PRASYARAT | : | * Next Generation Firewall System (Sistem Firewall Generasi Lanjut) * Unified Threat Management System (Sistem Manajemen Ancaman Terpadu) |
| KOLABORASI | : | * Next Generation Firewall System (Sistem Firewall Generasi Lanjut) * Unified Threat Management System (Sistem Manajemen Ancaman Terpadu) |
| METODA | : | * Signature-based (Berbasis-prasyarat) |
| SYARAT UMUM | : | * Mampu mendeteksi dan mencegah ancaman berbasis-pra prasyarat baik dengan kemampuan sendiri ataupun dengan berkolaborasi dengan sistem firewall generasi lanjut dan/atau sistem manajemen ancaman terpadu. * Mampu bertindak sebagai dekriptor akses berbasis SSL sebelum dienkripsi lagi ke server web. * Mampu mendeteksi dan mencegah 10 ancaman utama aplikasi web; yaitu: |

* Hidden Field Manipulation (Manipulasi field-tersembunyi)

Merupakan salah satu peretasan dengan cara mengubah input pada field-tersembunyi. Serangan ini terutama berfokus pada situs web e-niaga.

* Cookie Poisoning

Merupakan tindakan memanipulasi atau memalsukan cookie (sepotong kecil data yang dibuat dan disimpan di browser/peramban pengguna yang melacak informasi penting mengenai informasi sesi untuk situs tertentu) untuk tujuan melewati langkah-langkah pengamanan atau mengirim informasi palsu ke server.

* Parameter Tampering (Pengubahan Parameter)

Serupa dengan HFM, merupakan salah satu peretasan dengan cara mengubah input pada parameter-parameter web dalam URL, untuk mendapatkan akses otorisasi tanpa seijin pengguna.

* Buffer Overflow Attacks (Serangan Buffer Overflow)

Merupakan peretasan dengan menggunakan input-cacat untuk menyebabkan kondisi dimana ektra informasi tidak dapat ditampung pada buffer dan meng-overwrite ruang memori bersebelahan yang dapat mengakibatkan sistem- terhenti, bocornya informasi, teraksesnya kode tertentu, atau memasukkan kode pada aplikasi.

* Cross Site Scripting (XSS)

Serangan XSS adalah peretasan dengan injeksi, di mana skrip diinjeksikan ke situs web yang tepercaya. Serangan XSS terjadi ketika penyerang menggunakan aplikasi web untuk mengirim kode berbahaya, umumnya dalam bentuk skrip sisi peramban, ke pengguna-akhir yang berbeda.

* Backdoor or Debug options (Opsi debug)

Merupakan peretasan dengan memanfaatkan backdoor atau opsi debug tersedia yang dibuat secara sengaja oleh

|  |  |  |
| --- | --- | --- |
|  |  | developer/pemrogram untuk memeriksa aplikasi, sehingga peretas dapat mengakses informasi sensitif secara mudah.   * Stealth Commanding (Perintah Senyap)   Merupakan peretasan dengan memanfaatkan kelemahan inheren pada eksekusi perintah yang terdapat pada web server.   * Forced Browsing (Jelajah Paksa)   Jelajah paksa adalah serangan untuk mengakses sumber daya yang tidak dirujuk oleh aplikasi, tetapi masih dapat diakses. Peretasan manual ini biasanya menggunakan prediksi bila indeks direktori aplikasi berbasis pada generator angka atau nilai yang terprediksi.   * Third Party Misconfigurations (Miskonfigurasi Pihak Ketiga)   Merupakan kondisi yang sangat umum, dimana kontrol sekuriti untuk aplikasi web dan/atau server gagal diimplementasikan dengan baik atau salah diimplementasikan.   * Known Vulnerabilities (Kerentanan yang diketahui)   Merupakan kondisi dimana pembuatan dan/atau implementasi sebuah aplikasi web menggunakan kode yang secara umum diketahui memiliki celah keamanan, menggunakan kode yang diambil dari orang lain tanpa verifikasi terlebih dahulu, atau menggunakan kode yang  diambil dari sumber yang tingkat keamanannya rendah. |
| CONTOH PRODUK | : | * Imperva (Berbayar) * Akamai (Berbayar) * Radware (Berbayar) * Signal Sciences (Berbayar) * NAXSI (Gratis) * Nemesida (Gratis) |

1. **Security Information and Event Management (SIEM)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * SIEM adalah sebuah produk yang menyatukan beberapa fungsi pemantauan; terutama:   + Log Management (Manajemen Log)   + Security Information System (Sistem Informasi Keamanan)   + Security Event System (Sistem Peristiwa Keamanan) * Dalam praktiknya banyak produk mempromosikan terminologi mereka sendiri. * Produk-produk komersial memberikan kombinasi yang berbeda dari fungsi-fungsi ini dan tumpang tindih pada praktiknya. * SIEM dalam penggunaannya memerlukan kesatuan waktu agar tKita siaga yang tercipta dari korelasi informasi dan/atau peristiwa keamanan dapat menjadi sebuah tKita siaga yang tepat dan tidak terancukan oleh informasi dan/atau peristiwa keamanan yang tercipta baik sebelum   ataupun sesudahnya. |
| PRASYARAT | : | * Synchronization System (Sistem Sinkronisasi) |
| KOLABORASI | : | * Network Management System (Sistem Manajemen Jaringan) * Server and Application Monitoring System (Sistem Pemantauan Server dan Aplikasi) * Unifed Endpoint Management (Manajemen Endpoint Terpadu) * Performance Monitoring System (Sistem Pemantauan Performa) * Big Data Engine (Enjin Mahadata) * IT Service Management (Manajemen Servis TI) * File Integrity Monitoring (Pemantauan Integritas File) |

|  |  |  |
| --- | --- | --- |
| METODA | : | * Data Aggregation (Agregasi Data) * Correlation (Korelasi) * Alerting (TKita Siaga) |
| SYARAT UMUM | : | * SIEM minimal harus dapat memenuhi ketiga metoda utama SIEM. * Log/SNMP Perangkat yang teragregasi ke SIEM harus menggunakan timestamp (stempel waktu) yang tersinkronisasi. |
| CONTOH PRODUK | : | * Splunk (Berbayar) * LogRhythm (Berbayar) * Dell RSA (Berbayar) * Exabeam (Berbayar) * McAfee (Berbayar) * Securonix (Berbayar) * Snort (Gratis) * OSSEC (Gratis) * Elasticsearch (Gratis) |

1. **Network Behavioral Analysis/NBA (Analisis Perilaku Jaringan)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * NBA adalah cara untuk meningkatkan keamanan jaringan dengan memantau trafik dan mencatat tindakan atau penyimpangan yang tidak biasa dari operasi normal. * Solusi NBA memantau apa yang terjadi di dalam jaringan, mengumpulkan data dari banyak titik untuk mendukung analisis luring (offline). * Setelah menetapkan tolok ukur untuk trafik normal, program NBA secara pasif memantau aktivitas jaringan dan menKitai pola yang tidak diketahui, baru atau tidak biasa   yang mungkin mengindikasikan adanya ancaman. |

|  |  |  |
| --- | --- | --- |
|  |  | * NBA juga dapat memantau dan mencatat tren dalam penggunaan lebar-pita (bandwidth) dan protokol. * NBA sangat baik untuk menemukan malware baru dan eksploitasi 0-hari. |
| PRASYARAT | : | * Network Analytics System (Sistem Analitik Jaringan) |
| KOLABORASI | : | * 0-Day Protection System (Sistem Proteksi 0-Hari) * Network Analytics System (Sistem Analitik Jaringan) |
| METODA | : | * Data Aggregation (Agregasi Data) * Benchmarking (Penetapan Tolok Ukur) * Traffic Passive Monitoring (Pemantauan Pasif Trafik) * Flow and Route Analysis (Analisis Aliran dan Rute) |
| SYARAT UMUM | : | * Perangkat NBA minimal dapat memenuhi empat metoda utama di atas. * Perangkat NBA minimal dapat berfungsi sebagai   transparent bridging (jembatan transparan) dalam implementasinya. |
| CONTOH PRODUK | : | * NetScout (Berbayar) * Riverbed (Berbayar) * VIAVI (Berbayar) * Broadcom (Berbayar) * Colasoft (berbayar) * LiveAction (Berbayar) * SevOne (Berbayar) * FlowMatrix (Gratis) |

1. **File Integrity Monitoring (Pemantauan Integritas File)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * FIM merupakan sebuah sistem yang memantau integritas dari sebuah file pada server secara berkala dan terus menerus. * Bila terjadi perubahan pada file yang dipantau, FIM akan memberikan tKita-siaga dan memberikan opsi apakah file tersebut akan dikembalikan sesuai dengan duplikat file yang ada pada FIM atau diotorisasikan untuk diubah dan FIM akan memperbarui duplikat yang ada pada FIM. * FIM dalam bahasa umum biasa disebut dengan Web Deface Monitoring |
| PRASYARAT | : | - |
| KOLABORASI | : | * Storage System (Sistem Penyimpanan) |
| METODA | : | * On premises Agent-based (Di tempat Berbasis-agen) * On premise Agentless (Di tempat Tanpa-agen) * Cloud -based Agent-based (Berbasis-awan Berbasis-agen) * Cloud -based Agentless (Berbasis-awan Tanpa-agen) |
| SYARAT UMUM | : | * Baik sistem on premise atau cloud-based harus mampu mendeteksi perubahan file secara berkala sesuai dengan waktu yang ditetapkan oleh pengguna. * Untuk sistem berbasis-agen, harus menggunakan sumber   daya yang minimal (< 5%) agar tidak mengganggu fungsi utama server. |
| CONTOH PRODUK | : | * ELock (Berbayar) * TrustWave (Berbayar) * Qualys (Berbayar) * Tripwire (Berbayar) * OSSEC (Gratis) |

1. **IP Reputation Engine (Mesin Reputasi IP)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * IP RE adalah sebuah sistem yang berbasiskan kepercayaan melalui reputasi sebagai sarana mengidentifikasi kemungkinan ancaman keamanan siber. * IP RE dapat dibentuk oleh para pengguna dengan saling menilai dalam komunitas daring (online) untuk membangun kepercayaan melalui reputasi. * Atau IP RE dapat dilakukan oleh sebuah institusi yang   kemudian akan membagikannya kepada pengguna melalui perangkat. |
| PRASYARAT | : | - |
| KOLABORASI | : | * Next Generation Firewall System (Sistem Firewall Generasi Lanjut) * Unified Threat Management System (Sistem Manajemen Ancaman Terpadu) * Global Reputation Source (Sumber Reputasi Global) * Big Data Engine (Enjin Magadata) |
| METODA | : | * Active (Aktif) * Passive (Pasive) |
| SYARAT UMUM | : | * Pada metoda aktif, IP RE minimal harus dapat melakukan pengecekan dan korelasi kepada institusi yang terkait. * Pada metoda pasif, IP RE minimal harus dapat menerima   informasi dari sumber kepercayaan reputasi yang terkait. |
| CONTOH PRODUK | : | * Secucloud (Berbayar) * Akamai (Berbayar) * DenyAll (Berbayar) * Cisco (Berbayar) * McAfee (Berbayar) * DNSBL (Gratis) * Spamhaus (Gratis) |

1. **Synchronization System (Sistem Sinkronisasi)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * SS merupakan sebuah sistem sinkronisasi stempel-waktu yang detil dan tepat. * SS memungkinkan perangkat-perangkat dan/atau sistem- sistem yang terhubung dapat memiliki satu sinkronisasi waktu sehingga memungkinkan sebuah peristiwa terdeteksi secara tepat saat terjadinya. * Dengan ketepatan sinkronisasi waktu, sebuah peristiwa keamanan dapat terinci kronologinya, pengambilan keputusan juga dapat menjadi lebih tepat, serta memperkecil terjadinya putus jaringan untuk perangkat-   perangkat yang sensitif terhadap waktu. |
| PRASYARAT | : | - |
| KOLABORASI | : | * Global Positioning System (Sistem Penentuan Posisi Global) * Master Timing System (Sistem Master Pengaturan Waktu) * Network Time Protocol Server (Server Protokol Waktu Jaringan) |
| METODA | : | * Master Timing (Master Pengaturan Waktu) * Grandmaster Timing (Grandmaster Pengaturan Waktu) |
| SYARAT UMUM | : | * MT harus dapat menerima signal waktu secara langsung (Stratum-1) pada 1 (satu) Global Navigation Satellite System (GNSS/Sistem Satelit Navigasi Global) utama yaitu A-GPS, Galileo, BeiDou, dan GLONASS. * GMT harus dapat menerima signal waktu secara langsung (Stratum-1) pada lebih dari 1 (satu) Global Navigation Satellite System (GNSS/Sistem Satelit Navigasi Global) utama yaitu A-GPS, Galileo, BeiDou, dan GLONASS. * GMT harus memiliki opsi penambahan atomic clock (jam   atom) untuk cadangan penghitungan waktu bilamana terputus secara total dari GNSS. |

|  |  |  |
| --- | --- | --- |
|  |  | * MT dan/atau GMT harus dapat berfungsi sebagai NTP   Server. |
| CONTOH PRODUK | : | * Bodet MT (Berbayar) * Fibrolan GMT (Berbayar) * Orolia MT (Berbayar) |

1. **Network Analytic System (Sistem Analitik Jaringan)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * NAS merupakan sebuah sistem berbasis packet analyzer (penganalisisan paket) yang digunakan sebagai pengumpul data jaringan menjadi sebuah mahadata untuk mengetahui performa jaringan, memprediksi tren trafik jaringan, dan/atau memantau reliabilitas jaringan yang ada. * Hasil dari NAS dapat diolah lebih lanjut untuk NBA, dan   saat ini banyak perangkat NAS juga dapat langsung berfungsi sebagai perangkat NBA. |
| PRASYARAT | : | - |
| KOLABORASI | : | * Intrusion Prevention System (Sistem Pencegahan Intrusi) * 0-Day Protection System (Sistem Proteksi 0-Hari) |
| METODA | : | * Manual * Otomatis |
| SYARAT UMUM | : | * NAS yang terhubung dengan NBA dan IPS atau berfungsi   gKita sebagai NBA dan IPS harus dapat memutuskan dan/atau membelokkan alur jaringan pada kejadian DDoS. |
| CONTOH PRODUK | : | * Radware (Berbayar) * Netscout (Berbayar) * Cisco (Berbayar) * Riverbed (Berbayar) * Akamai (Berbayar) |

1. **Secure Proxy (Proksi Aman)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * SP merupakan sebuah cara mengalihkan jalur koneksi-logik dari langsung menjadi melewati SP terlebih dahulu. * SP akan menyaring koneksi ke domain sebenarnya dan   meneruskan koneksi yang telah tersaring ke domain sebenarnya. |
| PRASYARAT | : | - |
| KOLABORASI | : | Security Information and Event Management (Manajemen Informasi dan Peristiwa Keamanan) |
| METODA | : | * On premises (Di tempat) * Cloud -based (Berbasis-awan) |
| SYARAT UMUM | : | Baik sistem on premise atau cloud-based harus mampu  mendeteksi gangguan dan ancaman sebelum meneruskan ke koneksi sebenarnya. |
| CONTOH PRODUK | : | * BitGlass (Berbayar) * Symantec (Berbayar) * Microsoft (Berbayar) * Netskope (Berbayar) * McAfee (Berbayar) * CipherCloud (Berbayar) |

1. **Deception System (Sistem Pengecoh)**

|  |  |  |
| --- | --- | --- |
| PENJELASAN | : | * DS merupakan pengembangan dari Honeypot System (Sistem Pot-Madu) yaitu sebuah sistem yang tidak hanya membuat sebuah Pot-Madu untuk mengecoh peretas melainkan membuat keseluruhan sistem palsu baik perangkat keras server, perangkat keras jaringan, perangkat keras pengguna, serta perangkat lunaknya. * DS juga kan membuat keseluruhan kredensial yang nantinya   akan digunakan untuk membangun labirin-sistem dimana sistem asli akan tersembunyi. |

|  |  |  |
| --- | --- | --- |
|  |  | * Bila peretas berhasil menembus pertahanan utama sistem keamanan (dalam hal ini UTM/NGFW yang kerap digunakan), DS akan menjadikan sistem palsu sebagai target empuk yang mudah diretas, kemudian DS akan menyuplai peretas dengan berbagai macam data, file, dan akses ke perangkat palsu lainnya untuk memperlambat proses peretasan hingga pihak   terkait dapat mengisolasi peretasan. |
| PRASYARAT | : | - |
| KOLABORASI | : | Security Information and Event Management (Manajemen Informasi dan Peristiwa Keamanan) |
| METODA | : | * Appliance based with agent and Software based for Cloud   (Berbasis perangkat disertai agen dan perangkat lunak untuk Sistem-awan) |
| SYARAT UMUM | : | * Perangkat utama DS harus mampu membuat keseluruhan sistem palsu untuk mengecoh peretas baik dari eksternal ataupun internal. * Agen DS harus mampu membuat keseluruhan kredensial palsu untuk masing-masing perangkat server dan perangkat pengguna untuk mengecoh peretas. * Perangkat lunak DS harus mampu bertindak sebagai redundan untuk Server berbasis sistem-awan. |
| CONTOH PRODUK | : | * Attivo (Berbayar) * Acalvio (Berbayar) * TrapX (Berbayar) * Illusive (Berbayar) * Fidelis (Berbayar) |

1. **STANDAR DESAIN NETWORK & PERANGKAT KEAMANAN (TOPOLOGI SPINE – LEAF)**
   1. **Kantor Pusat**

**Gambar 3.8 Standar Desain Network & Perangkat Keamanan Kantor Pusat**

Diagram

Description automatically generated

* 1. **Kantor Wilayah/Cabang/Regional**

**Gambar 3.9 Standar Desain Network & Perangkat Keamanan Kantor Wilayah/Cabang**

Diagram

Description automatically generated

## Gambaran Umum:

1. Topologi Spine and Leaf adalah topologi jaringan pusat data (Data Center) dua lapis yang berguna untuk pusat data (Data Center) yang mengalami lebih banyak lalu lintas jaringan timur-barat (horizontal antar server; contohnya server aplikasi, server web, server transaksi, dll) daripada lalu lintas utara-selatan (vertikal dari server ke luar datacenter; contohnya mainframe, koneksi klien-server, thin-client, terminal server, dll).
2. Topologi terdiri dari switch-leaf (yang terhubung dengan server dan penyimpanan/storage) dan switch- spine (terhubung dengan leaf-switch).
3. Switch-leaf terhubung secara mesh ke switch-spine, membentuk lapis-akses yang memberikan titik koneksi jaringan untuk server.

## Karakteristik

1. Memiliki dua lapis switch yaitu:
   * Switch-Spine sebagai core
   * Switch-Leaf sebagai:
     + Switch Akses ke server dan penyimpanan/storage
     + Pembatas (Border Switch) ke jaringan lainnya di luar jarigan pusat data (datacenter)
2. Tidak terdapat koneksi antar Switch-Spine.
3. Menggunakan Protokol-Routing untuk meningkatkan penggunaan lebar-pita (bandwidth) secara penuh untuk koneksi utara-selatan (vertikal dari switch-leaf ke switch-spine).
4. Tidak menggunakan STP (*Spanning Tree Protocol*) untuk menghindari looping melainkan menggunakan protokol-routing seperti OSPF (*Open Shortest Path First*) atau BGP (*Border Gateway Protocol*)
5. Seluruh rute dikonfigurasi aktif serta menggunakan ECMP (*Equal-Cost Multipathing*)

## Keuntungan

1. Stabilitas
   * Penambahan switch dan/atau perawatan/maintenance switch tidak memerlukan downtime.
   * Kerusakan baik switch-spine ataupun switch-leaf tidak menghasilkan downtime.
   * Tidak memerlukan jeda waktu untuk penentuan koneksi karena tidak menggunakan STP melainkan protocol-routing .
2. Skalabilitas
   * Penambahan kapasitas dapat dilakukan dengan mudah yaitu dengan menambahkan Switch-Spine dan/atau Switch-Leaf.
3. Pengurangan latensi
   * Hanya menggunakan dua lapis switch dibandingkan dengan topologi terdahulu yang menggunakan tiga lapis switch.
4. Pengurangan biaya
   * Topologi Spine and Leaf tidak selalu memerlukan switch yang sangat besar ataupun padat densitas portnya, sehingga mengurangi biaya pembelian dan biaya penggunaan listrik tiap bulannya.