STUDI KASUS

Sistem Pakar Deteksi Kesalahan Konfigurasi Jaringan Data Center (VLAN & Switching) Menggunakan Metode Forward Chaining

Anggota Kelompok :

1. Rafhan Moch. S. A. (Ketua)
2. Fauzan Reza H.
3. Eldo Kelfiyansyah
4. Muhammad Rizma J.
5. Julianus G. S.
6. M. Fadlan Putra S. N.

Link Project Aplikasi :

https://github.com/RafhanArrasyid/2025/tree/main/studikasus_jaringan-data-center_logikainformatika

Link Jurnal Referensi :

https://teknosi.fti.unand.ac.id/index.php/teknosi/article/view/2310

Latar Belakang & Masalah

Data Center memiliki ribuan port switch dan server virtual.

- Permasalahan Utama:

- Fisik jaringan seringkali *redundant* (aman), namun masalah sering terjadi pada Logika Konfigurasi (Human Error).

- Gejala seringkali ambigu: "Lampu indikator menyala hijau (*Link Up*), tetapi data tidak mengalir."

- Teknisi menghabiskan waktu lama mengecek baris perintah (CLI) satu per satu.

- Solusi: Menggunakan metode *Forward Chaining* untuk mengonversi output teknis CLI menjadi diagnosa instan.

Masalah Yang Terjadi

- Kompleksitas Data Center: Data Center modern memiliki ribuan port switch dan server virtual yang saling terhubung.
- Human Error: Meskipun fisik jaringan seringkali sudah redundant (aman secara perangkat keras), kegagalan fatal sering terjadi pada lapisan Logika Konfigurasi akibat kesalahan manusia (Human Error).
- Gejala Ambigu: Masalah seringkali menipu, misalnya indikator lampu switch menyala hijau (Link Up) seolah normal, namun data tidak mengalir sama sekali.

Masalah Dan Penanganan

- Pengecekan Manual yang Lambat: Saat ini, teknisi harus menghabiskan waktu lama untuk mengecek baris perintah (Command Line Interface / CLI) satu per satu untuk mencari kesalahan.
- Inkonsistensi Diagnosa: Sering terjadi perbedaan diagnosa antara teknisi senior dan junior dalam menangani masalah yang sama, menyebabkan ketidakefisienan.
- Unsur Tebak-tebakan: Tanpa sistem yang baku, perbaikan konfigurasi seringkali didasarkan pada asumsi atau tebak-tebakan, bukan data yang akurat.

Pemilihan Metode

Mengapa Forward Chaining?

- Metode ini dipilih karena karakteristik masalah jaringan bersifat Data Driven (berbasis data/fakta di lapangan).
- Sangat cocok untuk kasus diagnosa di mana gejala-gejala awal (seperti lampu indikator, hasil ping, log error) sudah diketahui terlebih dahulu oleh user.
- Sistem dapat bergerak maju dari Fakta (Gejala) menuju Kesimpulan (Diagnosa Kerusakan).

Metode Forward Chaining

- Forward Chaining adalah metode penalaran yang bekerja secara "Maju", dimulai dari sekumpulan Fakta (data atau gejala yang terdeteksi) untuk bergerak menuju Kesimpulan (diagnosa akhir).

- Berbeda dengan Backward Chaining yang memulai dari hipotesa, metode ini sepenuhnya bergantung pada data yang dimasukkan oleh pengguna di awal.

Sistem Pakar

Sistem (System):

Merupakan kumpulan aturan logika (Rules Engine) yang disusun secara sistematis untuk memproses input gejala menjadi keputusan.

Pakar (Expert):

Pengetahuan dari Network Engineer yang diadopsi ke dalam program untuk mendeteksi pola kesalahan konfigurasi VLAN dan Switching.

Peran Sistem Pakar Dalam Jaringan

- Efisiensi Debugging: Menggantikan peran pengecekan manual yang memakan waktu berjam-jam menjadi diagnosa instan dalam hitungan menit.
- Panduan Cerdas: Bertindak sebagai asisten cerdas yang memandu teknisi dari gejala awal hingga memberikan perintah perbaikan (Solusi CLI) yang spesifik.
- Akurasi: Menghilangkan ambiguitas diagnosa dengan mencocokkan fakta lapangan (seperti status Interface UP/UP atau Ping RTO) dengan basis pengetahuan yang sudah valid.

Metodologi Dan Penerapan Forward Chaining

1. Analisis Masalah: Mengidentifikasi gejala umum pada Data Center (Misal: Native VLAN Mismatch, Missing VLAN).

2. Akuisisi Pengetahuan: Menyusun tabel gejala (kode GG) dan tabel diagnosa (kode PG) berdasarkan pengalaman engineer.

3. Perancangan Logika (Decision Tree): Membuat diagram pohon keputusan untuk memetakan alur pertanyaan "Ya/Tidak" dari gejala menuju solusi.

4. Implementasi Aturan (Rules): Menerapkan aturan IF-THEN (contoh: IF Err-Disabled AND Mac Table Kosong THEN Port Security Violation) .

5. Pengujian Studi Kasus: Menguji sistem dengan skenario nyata, seperti migrasi server baru yang gagal koneksi.

Tabel Gejala

Kode	Nama Gejala (Fakta yang Terlihat/Terdeteksi)	Deskripsi Teknis
GG01	Interface Status: UP/UP (Connected)	Layer 1 (Fisik) dan Layer 2 (Protokol) aktif.
GG02	Interface Status: Err-Disabled	Port dimatikan paksa oleh sistem keamanan switch.
GG03	Interface Status: UP/DOWN	Masalah negosiasi protokol (misal: speed/duplex mismatch).
GG04	Ping status: RTO (Request Timed Out)	Tidak ada konektivitas IP ke gateway atau host lain.
GG05	Log Error: Native VLAN Mismatch	Muncul pesan error CDP/LLDP di konsol.
GG06	Status STP Port: BLK (Blocking/Discarding)	Port diblokir oleh Spanning Tree Protocol (indikator warna amber).
GG07	VLAN Database: ID Tidak Ditemukan	VLAN ID yang dikonfigurasi di port belum dibuat di database global.
GG08	Mac Address Table: Kosong	Switch tidak mempelajari alamat fisik perangkat.
GG09	Mode Port: Access (Seharusnya Trunk)	Link antar-switch salah mode.
GG10	VTP Domain Name: Berbeda	Switch client tidak bisa sinkronisasi VLAN database dari Server.

Tabel Diagnosa

Kode	Diagnosa Kerusakan	Solusi Perbaikan
PG01	**Port Security Violation**	Cek Sticky MAC Address asing atau reset interface (shutdown -> no shutdown).
PG02	**Native VLAN Mismatch**	Samakan konfigurasi switchport trunk native vlan <id> di kedua sisi trunk.
PG03	**Missing VLAN on Database**	Buat VLAN ID tersebut pada database switch (vlan <id>).
PG04	**VTP Domain Mismatch**	Samakan nama domain VTP pada semua switch di cluster tersebut.
PG05	**Spanning Tree Loop Protection**	Periksa redundant link tak terkelola atau aktifkan BPDU Filter jika perlu.
PG06	**Trunking Mode Failure**	Ubah mode interface menjadi Trunk (switchport mode trunk).

Aturan Keputusan (Rules Engine)

Rule 1: Deteksi Keamanan Port (Port Security)

- IF Port Status Err-Disabled (GG02)
- AND Mac Address Table Kosong (GG08)
- THEN Port Security Violation (PG01)

Rule 2: Deteksi Konflik Native VLAN

- IF Interface Status UP/UP (GG01)
- AND Ping Status RTO (GG04)
- AND Log Error Native VLAN Mismatch (GG05)
- THEN Native VLAN Mismatch (PG02)

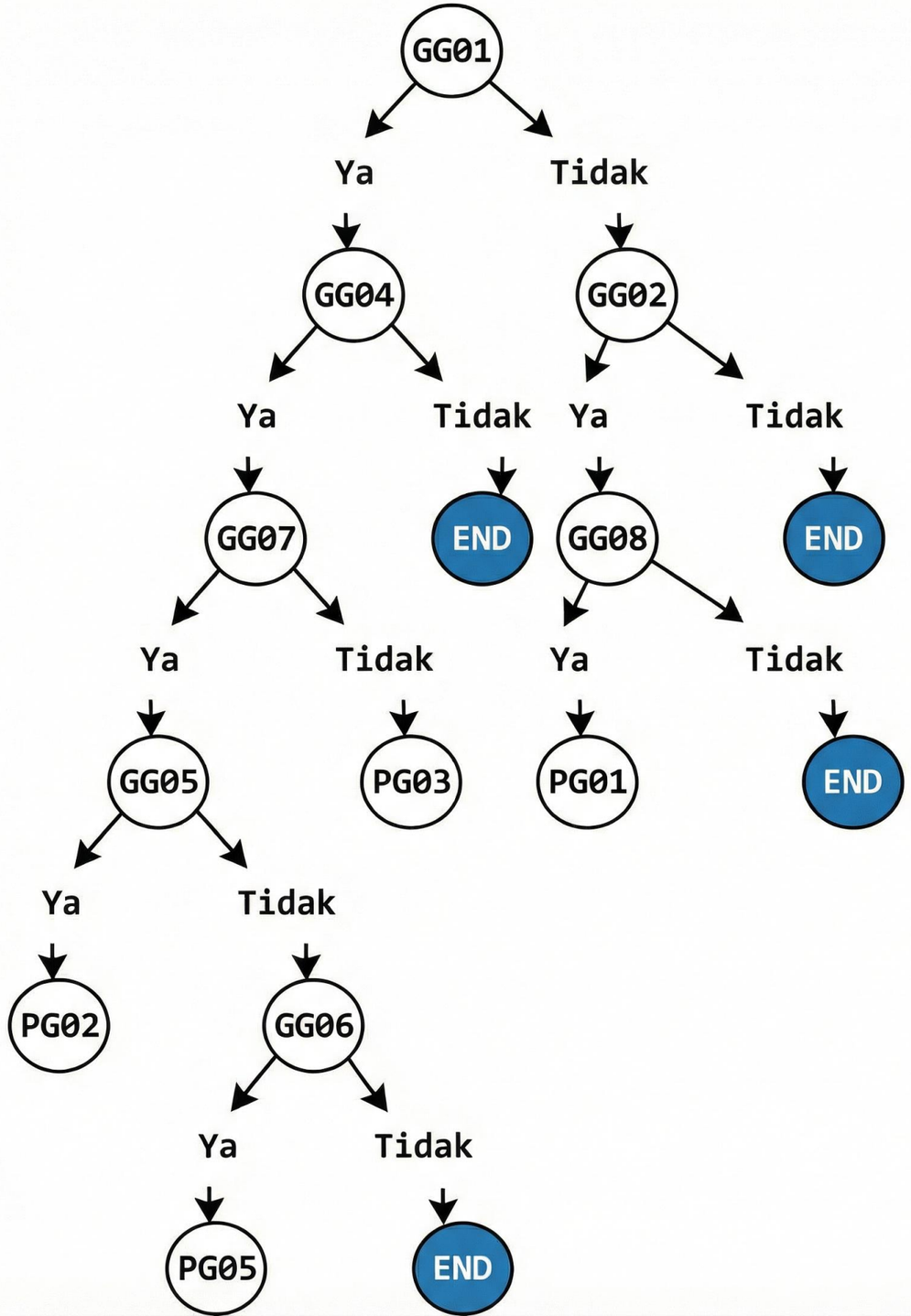
Rule 3: Deteksi VLAN Belum Dibuat

- IF Interface Status UP/UP (GG01)
- AND Ping Status RTO (GG04)
- AND VLAN Database ID Tidak Ditemukan (GG07)
- THEN Missing VLAN on Database (PG03)

Rule 4: Deteksi Loop / STP Blocking

- IF Interface Status UP/UP (GG01)
- AND Status STP Port BLK (GG06)
- THEN Spanning Tree Loop Protection (PG05)

Diagram Tree



KNOWLEDGEBASE/BASIS PENGETAHUAN 1

1. JIKA Interface Status menunjukkan UP/UP (Connected)
MAKA Tanya: Apakah status Ping ke gateway RTO (Request Timed Out)?
JIKA YA MAKA Lanjut pemeriksaan ke Database VLAN (Indikasi masalah Logic).

2. JIKA Status Ping RTO (Request Timed Out)
MAKA Tanya: Apakah VLAN ID port tersebut ada di Database VLAN?
JIKA TIDAK MAKA Diagnosa: Missing VLAN on Database (PG03).
(Solusi: Buat VLAN ID pada database switch)

KNOWLEDGEBASE/BASIS PENGETAHUAN 2

3. JIKA VLAN ID sudah ada di Database namun Ping tetap RTO
MAKA Tanya: Apakah muncul Log Error "Native VLAN Mismatch"?
JIKA YA MAKA Diagnosa: Native VLAN Mismatch (PG02). *(Solusi: Samakan konfigurasi native vlan di kedua sisi trunk)*

4. JIKA Interface Status menunjukkan 'Err-Disabled'
MAKA Tanya: Apakah Mac Address Table kosong?
JIKA YA MAKA Diagnosa: Port Security Violation (PG01). *(Solusi: Reset interface atau cek sticky MAC address asing)*

Simulasi Studi Kasus

Skenario: Migrasi Server Baru

Seorang *Network Engineer* baru saja memindahkan Server Database ke Rack B. Kabel sudah terpasang rapi, lampu indikator switch menyala hijau, tetapi server tidak bisa di-ping dari luar.

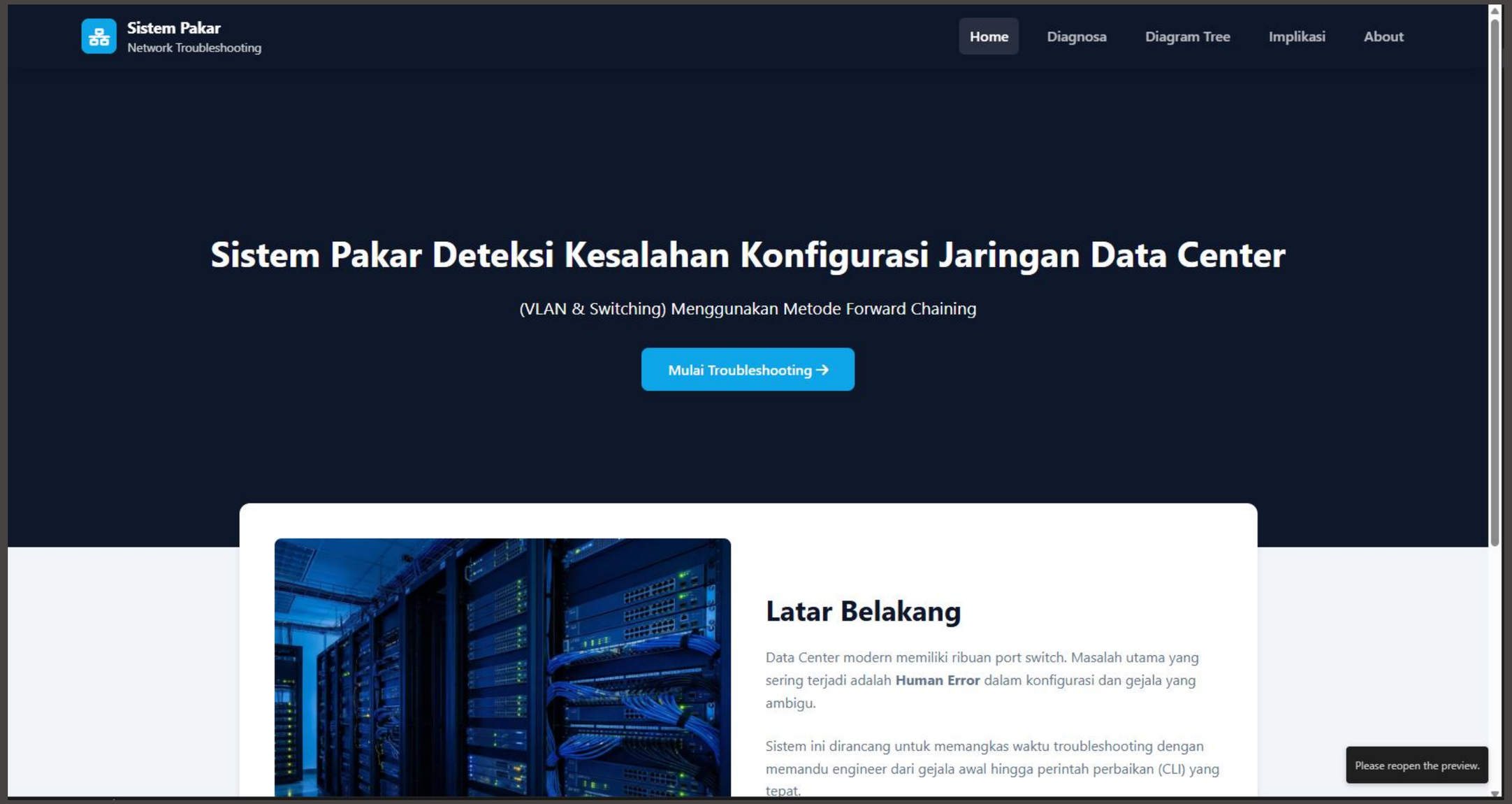
Langkah Diagnosa Sistem (Forward Chaining):

1. Sistem Cek Fakta 1: Bagaimana status Interface?
   - *Input User:* UP/UP (GG01).
2. Sistem Cek Fakta 2: Bagaimana hasil Ping?
   - *Input User:* RTO / Gagal (GG04).
3. Sistem Cek Fakta 3: (Sistem menelusuri kemungkinan Rule 2 & Rule 3). Cek Log Error, apakah ada pesan "Mismatch"?
   - *Input User:* Tidak ada (GG05 False). -> *Rule 2 Gugur.*
4. Sistem Cek Fakta 4: Cek Database VLAN, apakah VLAN ID port tersebut ada di database?
   - *Input User:* Tidak ada / Not Found (GG07).
5. KESIMPULAN:
   - Cocok dengan Rule 3.
   - Diagnosa: Missing VLAN on Database (PG03).
   - Solusi: Jalankan perintah vlan <id> lalu name <nama_vlan> pada global config.

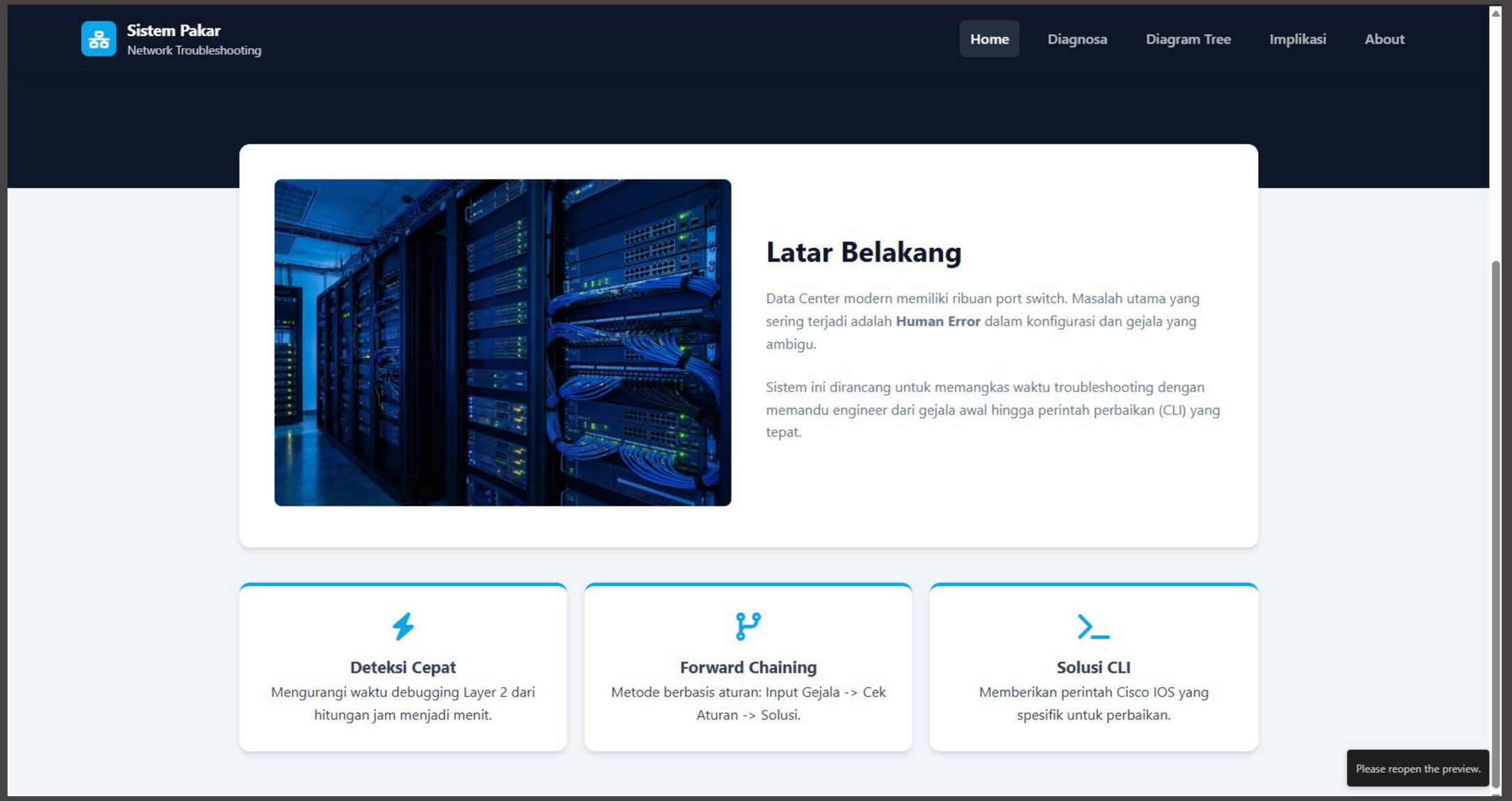
Manfaat Penerapan

1. Efisiensi Debugging: Mengurangi waktu *troubleshooting* layer 2 yang biasanya memakan waktu berjam-jam menjadi hitungan menit.
2. Standarisasi Konfigurasi: Mencegah teknisi senior dan junior melakukan diagnosa yang berbeda untuk masalah yang sama.
3. Akurasi Tinggi: Menghilangkan unsur tebak-tebakan dalam perbaikan konfigurasi switch.

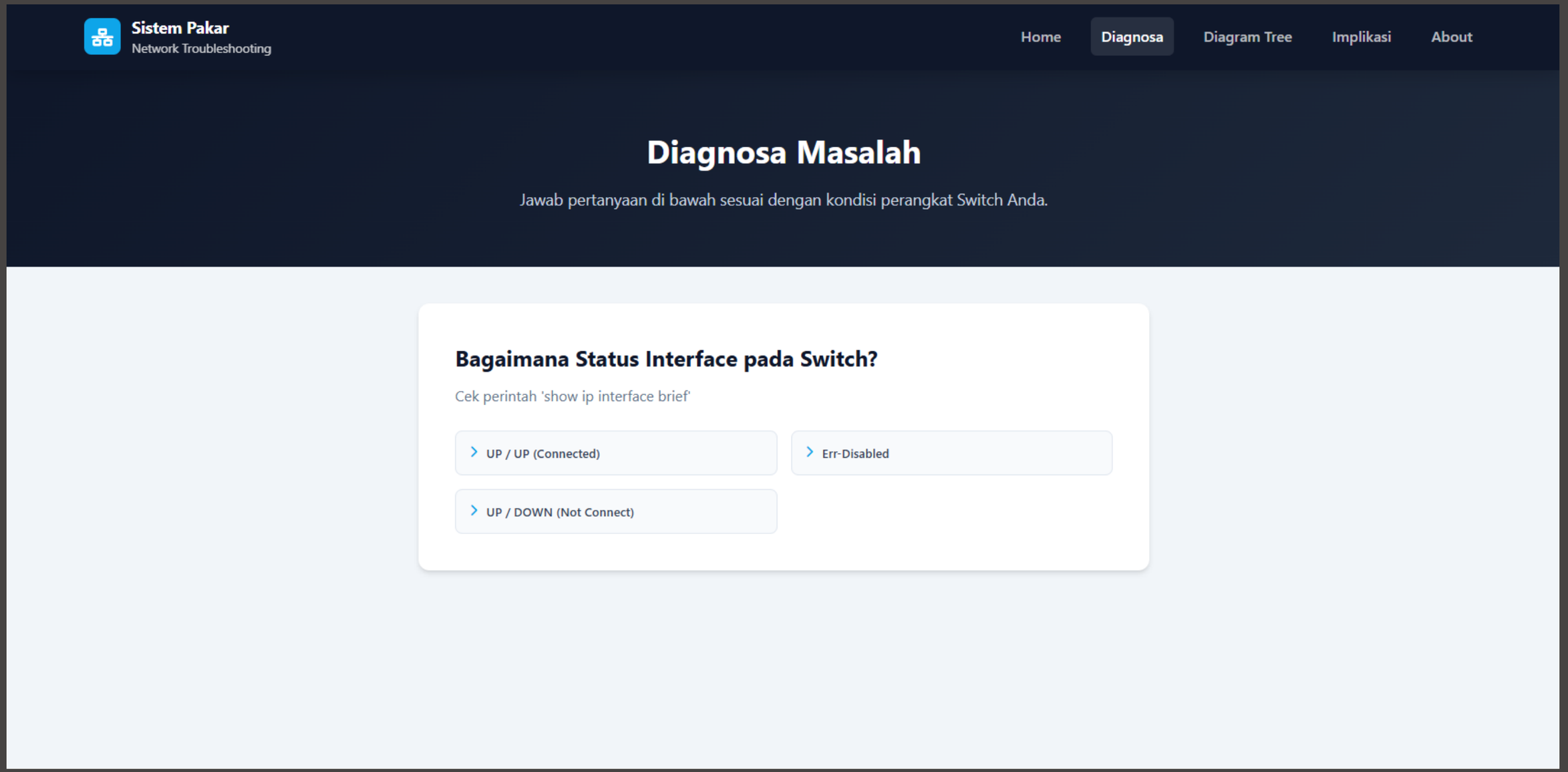
Halaman Home Aplikasi ‘1



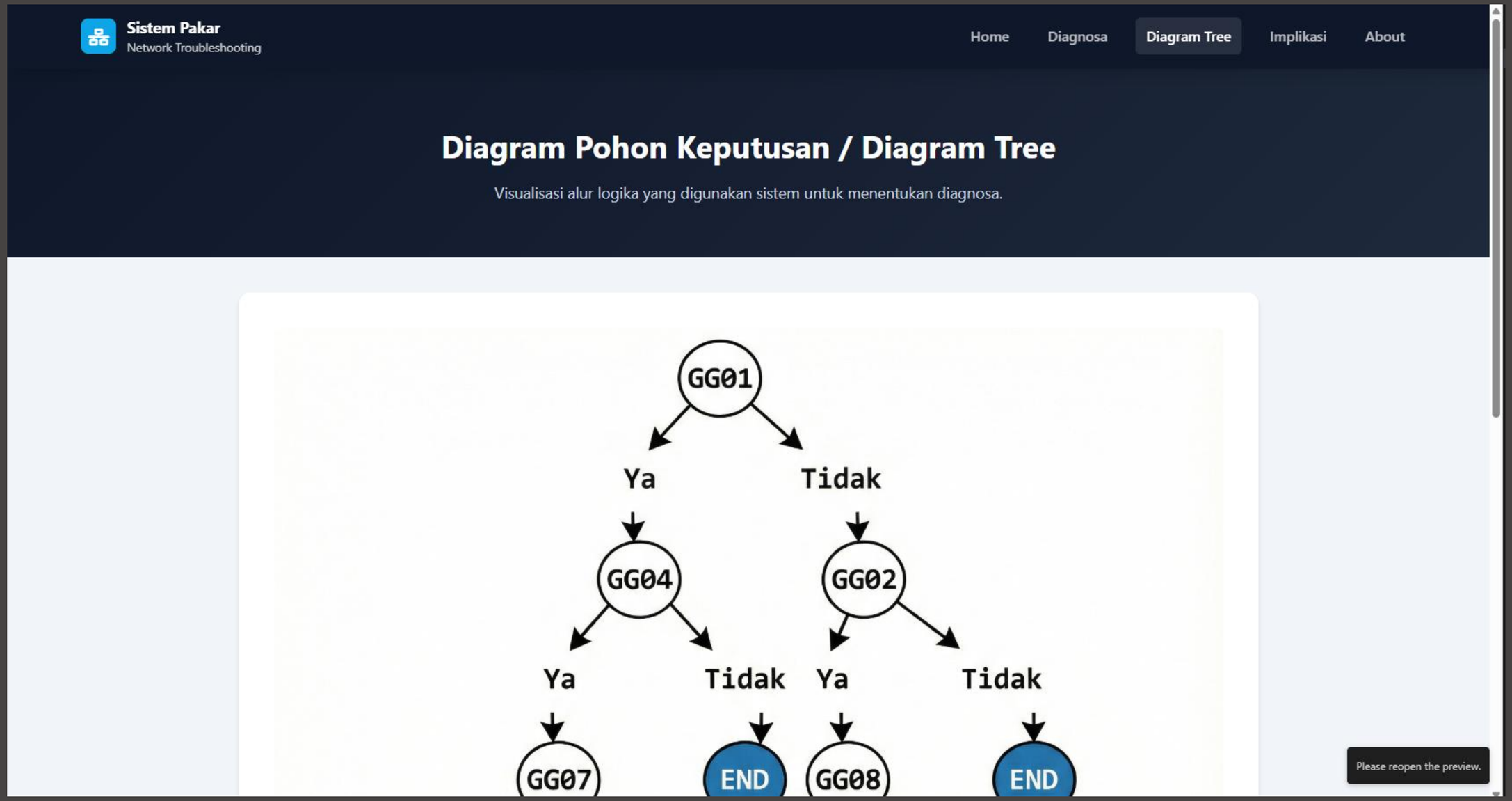
Halaman Home Aplikasi ‘2



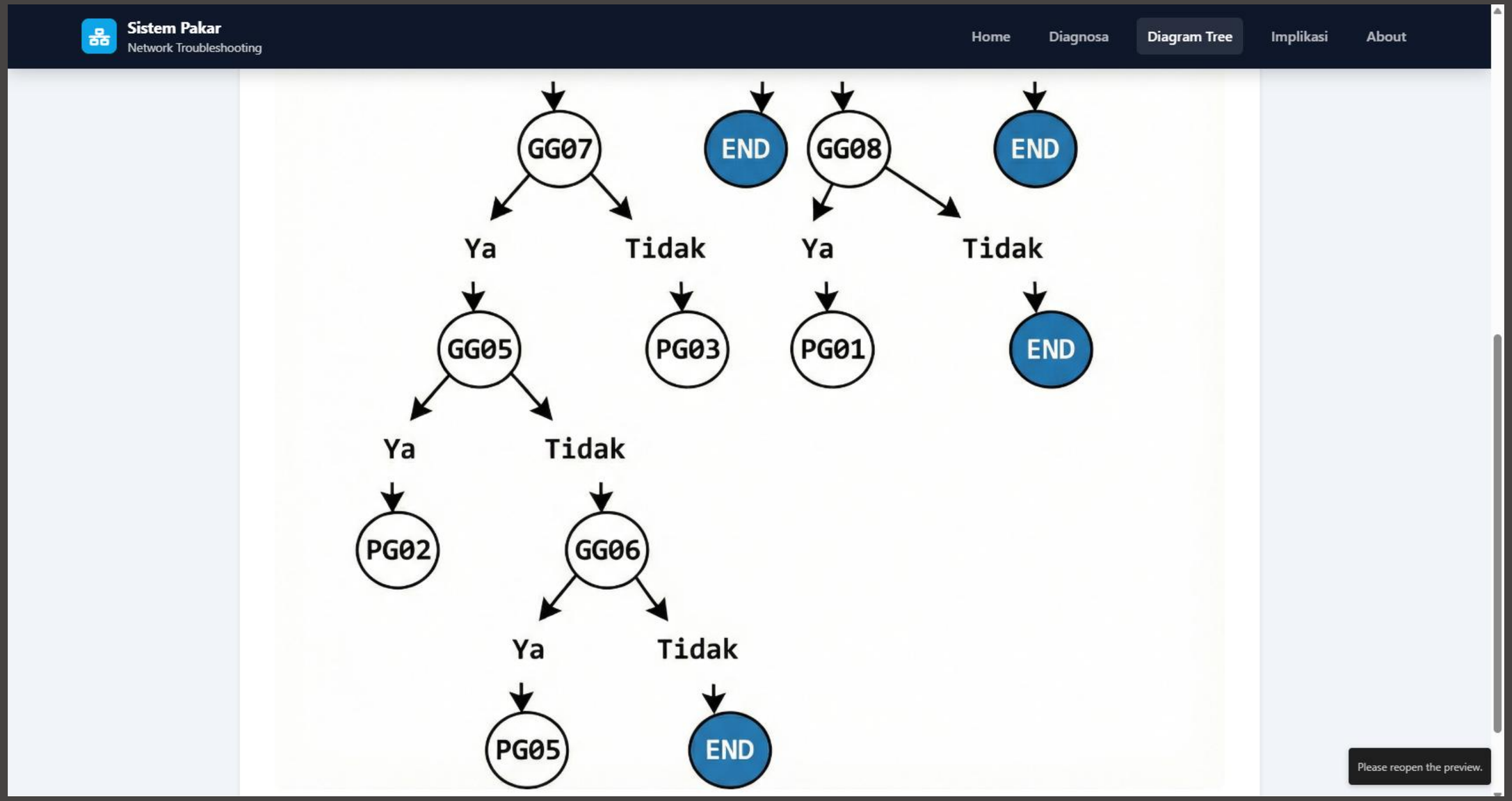
Halaman Diagnosa



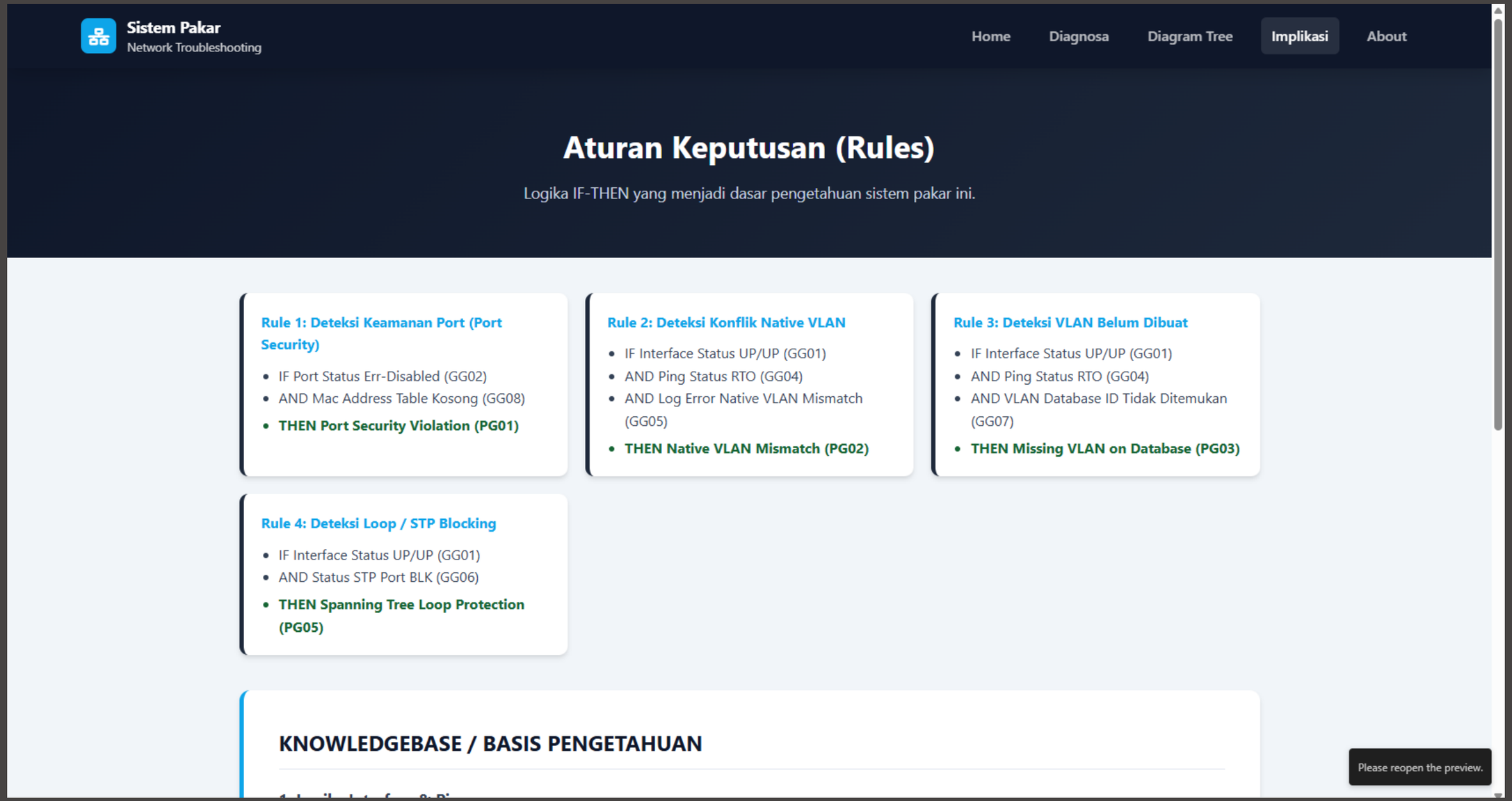
Halaman Diagram Tree ‘1



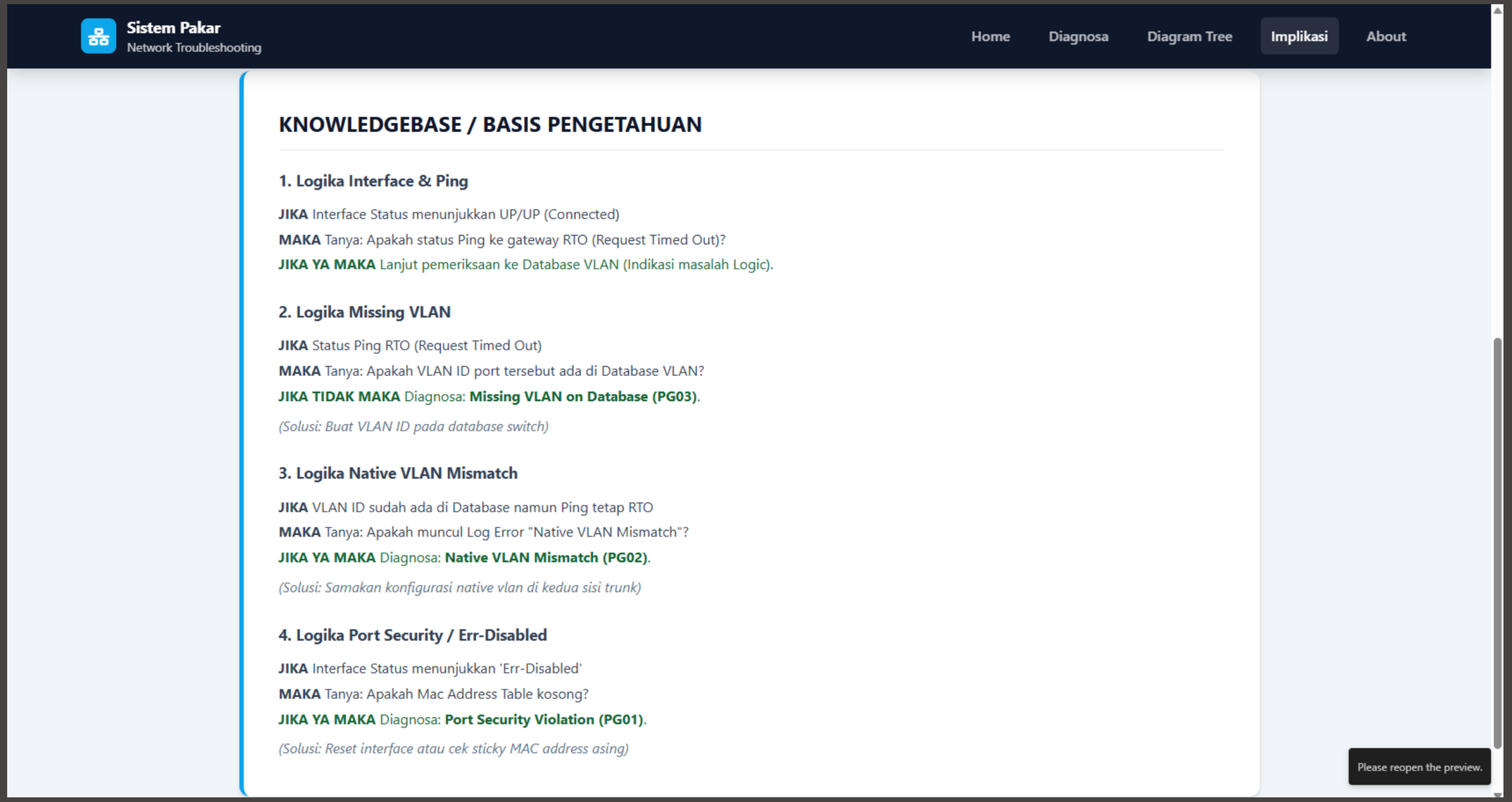
Halaman Diagram Tree ‘2



Halaman Implikasi ‘1



Halaman Implikasi ‘2



Halaman About