

Manual de Usuário – Sistema de Captura, Análise e Plotagem de Pacotes de Rede

Este manual descreve o funcionamento básico do sistema desenvolvido para captura de tráfego HTTP/TCP, processamento por modelo C++, análise de anomalias e geração de gráficos estatísticos por meio do módulo Python.

1. Iniciando a Captura

Para iniciar o processo completo (captura, geração de JSONs e execução do modelo), acesse o endpoint:

`/start`

O sistema iniciará automaticamente:

- o treinamento do modelo,
 - a captura dos pacotes,
 - a classificação das anomalias,
 - e a atualização dos dados internos.
-

2. Intervalo Recomendado

Recomenda-se configurar **um intervalo mínimo de 30 segundos** entre as execuções.

Esse intervalo garante tempo suficiente para:

- captura de pacotes,
- processamento dos valores,
- execução do modelo C++,

- atualização do JSON final que será utilizado pelo plotter Python.
-



3. Selecionando o IP da Rede

Antes de iniciar a captura, selecione o IP correto da interface de rede no endpoint:

/ip

Escolha o IP correspondente à interface na qual o servidor está sendo executado.

O sistema só capturará pacotes pertencentes a esta interface.



4. Treinamento do Modelo

Após configurado o IP e o intervalo, o modelo C++ será **automaticamente treinado** na primeira execução.

Esse treinamento inicial é necessário para que o sistema aprenda o comportamento esperado da rede e possa detectar anomalias nas próximas execuções.



5. Início da Captura

Com o sistema configurado e o treinamento finalizado, a captura dos pacotes TCP começa automaticamente.

O sistema irá:

- coletar pacotes,
- salvar no banco de dados,
- gerar JSONs de entrada,
- executar o modelo,
- atualizar as flags de anomalia,
- e gerar o JSON consolidado para os gráficos.



6. Aguarde para Gerar os Gráficos

Após iniciar a captura, **aguarde alguns segundos antes de plotar os gráficos.**

Durante esse tempo estão acontecendo:

- atualização das flags detectadas pelo modelo,
- escrita do JSON consolidado,
- preparação dos dados para plotagem.

Se tentar gerar o gráfico imediatamente, os dados podem não estar atualizados.



7. Visualizando os Gráficos

Para visualizar os gráficos referentes ao **último intervalo executado**, acesse:

`/plot`

O sistema irá:

1. chamar o módulo Python,
 2. processar os dados atualizados,
 3. gerar os gráficos solicitados,
 4. e retorná-los na resposta da requisição.
-



8. Configurando os Intervalos

Para ajustar os intervalos de execução, acesse:

`/configure`

Nessa rota você poderá definir:

- **intervalo de execução** (tempo entre capturas),
- **intervalo de contexto** (tempo adicional para aguardar processamento interno).

Importante:

- Os valores **não podem ser negativos**.
- Os valores **não podem ser quebrados (devem ser inteiros)**.