# Gerenciamento de Conexões usando Firewall Automatizado a partir de Dados de Inteligência sobre Ameaças

Universidade Estadual do Ceará (UECE)
Laboratório de Redes de Computadores e Segurança (LARCES)

Marcus A. Costa
Yago M. Costa
Douglas A. Silva
Ariel L. Portela
Rafael L. Gomes

# Introdução

Larces
Laboratório de Redes de Computadores e Segurança

Universidade Estadual do Ceará

# Contexto

- A segurança da informação não é apenas uma necessidade, mas um pré-requisito para proteger dados sensíveis contra o crescente volume de ataques cibernéticos.
- Essa realidade exige soluções de segurança que sejam adaptáveis, resilientes e capazes de antecipar ameaças emergentes.
- O gerenciamento de conexão de rede se refere ao controle e supervisão do tráfego de rede entre dispositivos.
- **Foco**: Firewall Responsivo
    - Com base na análise de reputação e comportamento
    - Adapta-se dinamicamente para bloquear IPs de baixa reputação

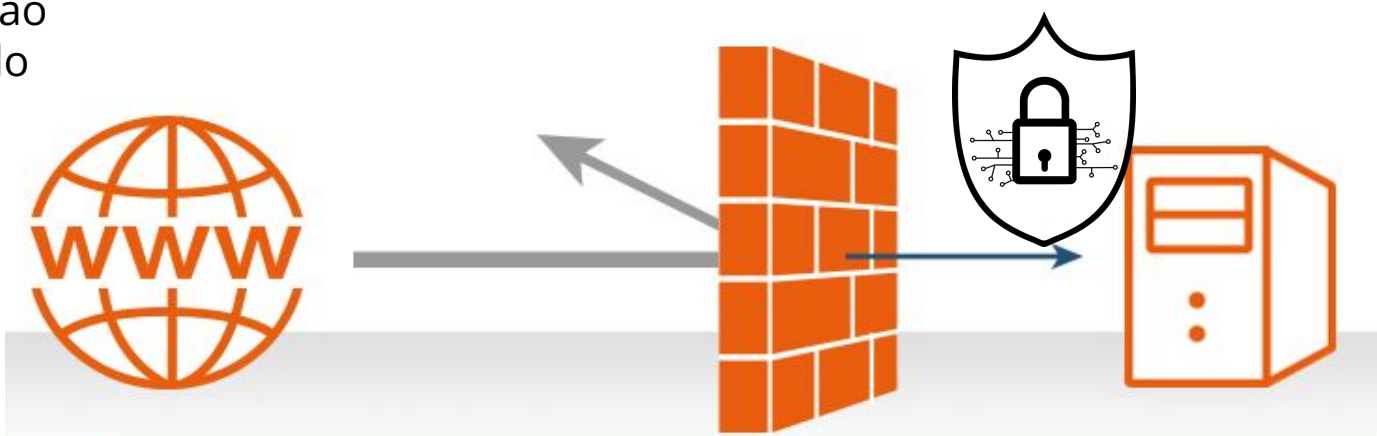
# Problema

- Principais questões:
  - Como definir a reputação de IP?
  - Como manter o equilíbrio entre segurança e desempenho na rede?
  - Como automatizar processos de segurança?

- **Abordagens**:
  - Inteligência sobre Ameaças.
  - Degradação de conexão.
  - Resposta automatizada.

# Proposta

- **FIBRA: Firewall Integrado com Blacklists e Reputação Automatizado**
  - Objetivo: combater ameaças de forma autônoma por meio de atualizações em tempo real de listas negras e técnicas de filtragem.
  - Organização: Vários módulos que aplicam tecnologias distintas e executam funcionalidades específicas.
    - Flexibilidade
    - Independência
    - Automação
    - Atualizado



# Proposta

Larces
Laboratório de Redes de Computadores e Segurança

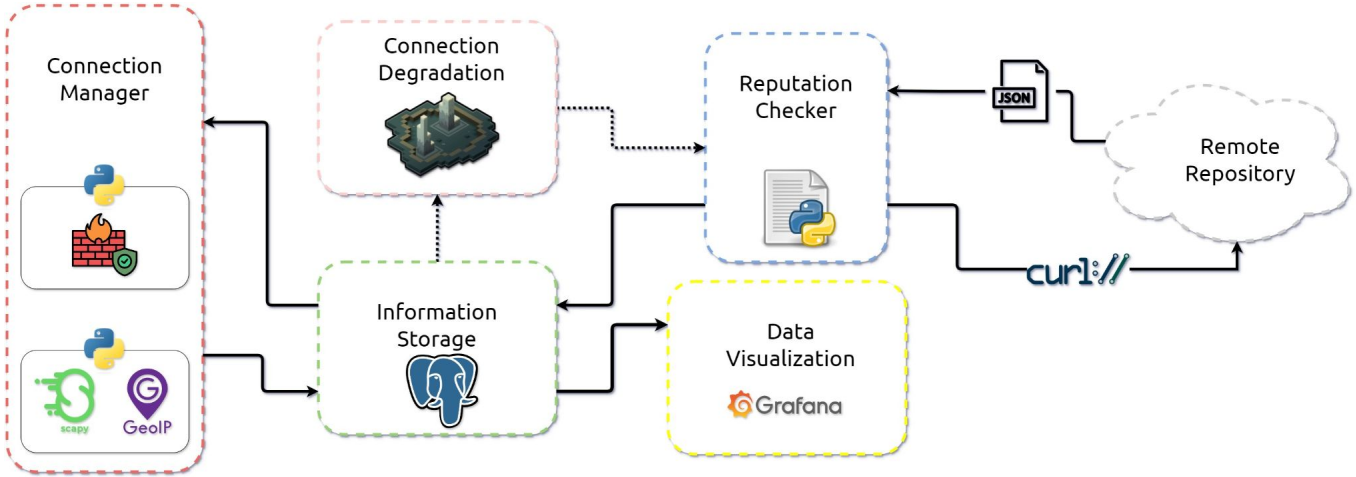
Universidade Estadual do Ceará

# Proposta: FIBRA

- A ideia do FIBRA é evoluir os firewalls tradicionais, incorporando:
  - Um mecanismo dinâmico para atualizar listas negras
  - Avaliação de reputação de IP, aprimorando a detecção de ameaças
  - Recursos de mitigação continuamente.
- Integração de lista negra dinâmica, banco de dados de ameaças e técnica de degradação.
- A FIBRA utiliza tecnologias contemporâneas:
  - Contêineres para implantação flexível de bancos de dados e ferramentas de visualização de dados.
  - APIs para comunicação.
  - Facilita o gerenciamento e a escalabilidade do sistema
  - Administradores de rede têm insights sobre o tráfego de rede
  - Identificação rápida de padrões suspeitos e decisões de segurança informadas.

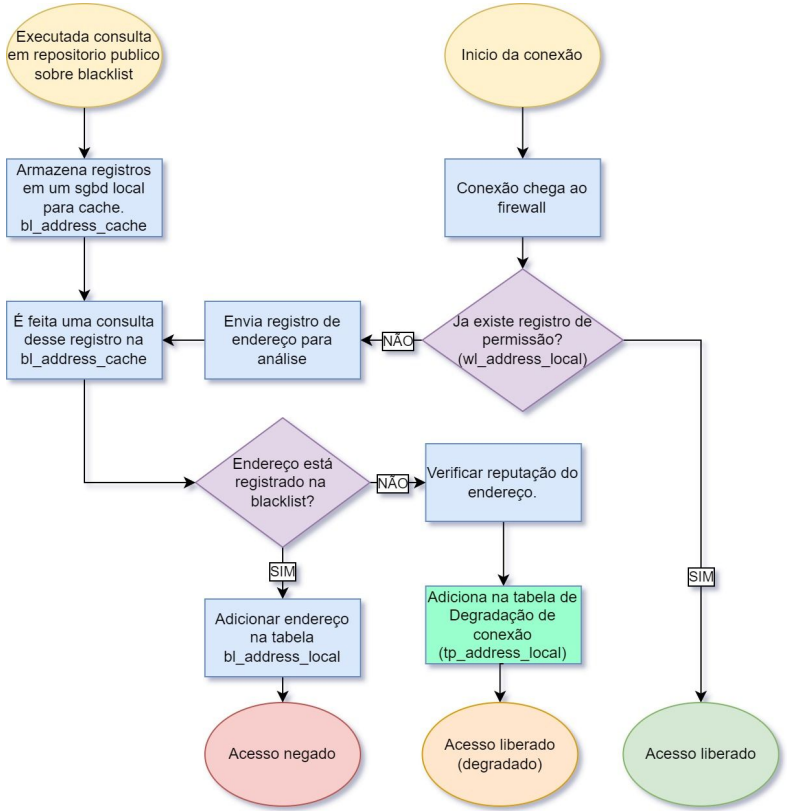
# Estrutura do FIBRA

- Vários módulos foram desenvolvidos:
  - Gerenciador de Conexões: monitora e analisa o tráfego de rede em tempo real.
  - Armazenamento de Dados: registra e armazena informações sobre os eventos.
  - Checagem de Reputação: consulta as tentativas de conexão capturadas.
  - Degradação de Conexão: configuração de regras para responder a IPs maliciosos.
  - Visualização de Dados: GUI para leitura e visualização de dados coletados.



# Fluxo de Execução no FIBRA

- O Reputação baixa a lista negra para armazenamento local.
- Os registros de conexão do tipo SYN conectam as conexões TCP, concatenam com a lista de geolocalização e as armazenam.
- A degradação compara os dados armazenados pela Connection com a lista negra local da Reputation
  - se for novo, ele recebe a pontuação de confidencialidade e sua conexão é limitada (suspeita).
  - Se o IP estiver na lista negra, ele será adicionado à tabela de bloqueio (malicioso).



# Definição de Reputação no FIBRA

- O módulo Reputation obtém as informações da plataforma AbuseIPDB, que são importadas no formato JSON.
  - countryCode: nacionalidade do endereço;
  - abuseConfidenceScore: reputação reportada
  - lastReportedAt: hora do relatório de informações
- **Suspeito** se tiver um abuseConfidenceScore positivo nos últimos 7 dias.
- **Malicioso** se tiver abuseConfidenceScore de 100.


```
{"meta": {"generatedAt": "2024-03-29T19:44:48+00:00"},
  "data": [
    { "ipAddress": "43.134.29.37",
      "countryCode": "SG",
      "abuseConfidenceScore": 100,
      "lastReportedAt": "2024-03-29T19:17:01+00:00"},
    { "ipAddress": "162.216.149.64",
      "countryCode": "US",
      "abuseConfidenceScore": 100,
      "lastReportedAt": "2024-03-29T19:17:00+00:00"},
    {"ipAddress": "198.235.24.200",
      "countryCode": "US",
      "abuseConfidenceScore": 100,
      "lastReportedAt": "2024-03-29T19:16:59+00:00"},
    {"ipAddress": "124.223.219.9",
      "countryCode": "CN",
      "abuseConfidenceScore": 100,
      "lastReportedAt": "2024-03-29T18:39:30+00:00"}
  ]}
```

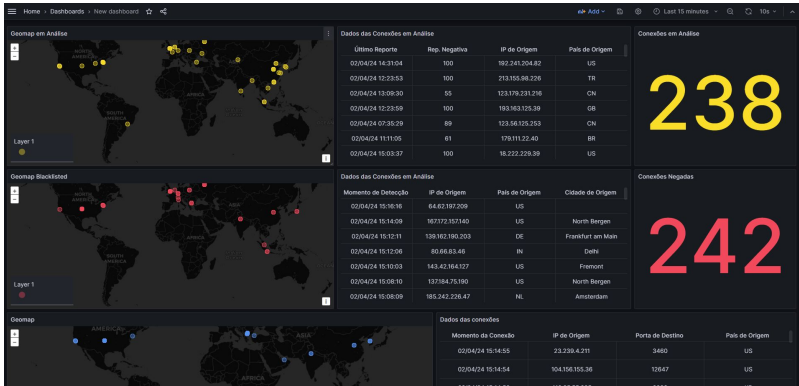
# Experimentos

Larces
Laboratório de Redes de Computadores e Segurança

Universidade Estadual do Ceará

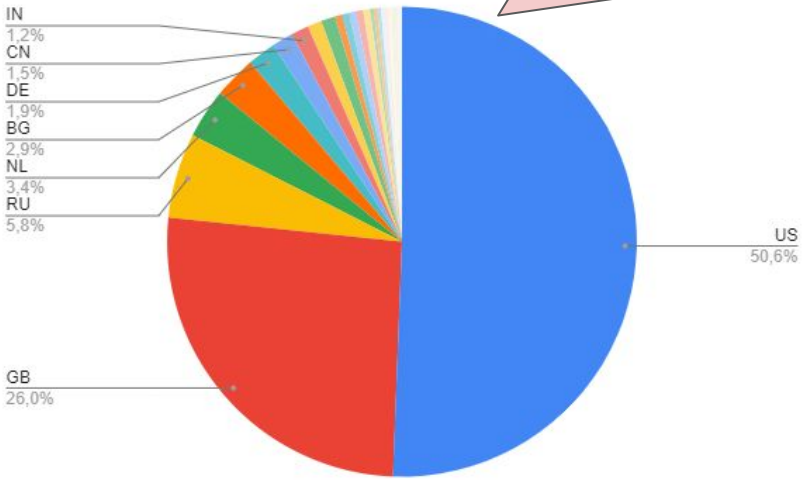
# Experimentos

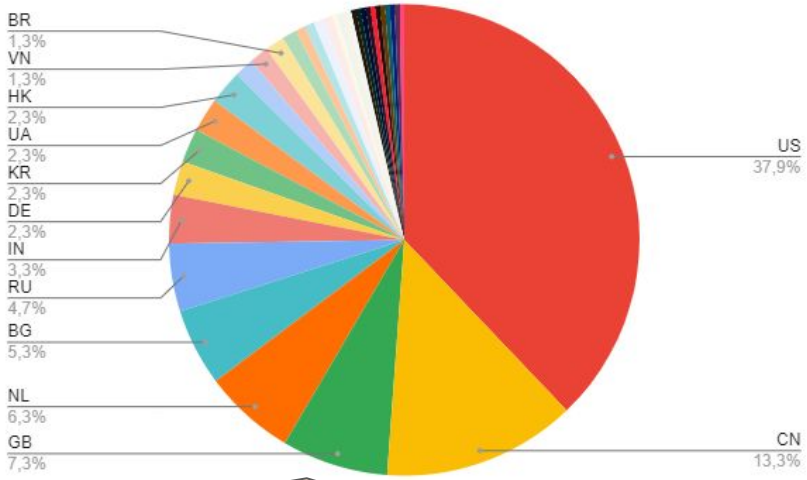
- Para o desenvolvimento e operação do FIBRA, foram utilizadas as ferramentas:
  - Python: subprocess, psycopg2, scapy, requests, re, datetime, geoip2.database e ipaddress.
  - Geoipupdate: geração de um banco de dados local com informações de geolocalização de endereço IP.
  - Docker: conteinerização de serviços não conectados diretamente à conexão.
  - Grafana: permite a visualização desses dados em painéis intuitivos.
- Inicialmente, os testes foram conduzidos em ambiente local. Posteriormente, foram migrados para a nuvem (AWS).



# Resultados

Registros de conexões que foram identificadas como maliciosas e correspondem a endereços IP nas listas negras




conexões não reconhecidas, mas suspeitas o suficiente para serem degradadas

# Conclusão

Larces
Laboratório de Redes de Computadores e Segurança

Universidade Estadual do Ceará

# Conclusão e Trabalho Futuro

- Apresentamos uma solução de segurança chamada FIBRA, desenvolvida para gerenciar conexões em infraestruturas de rede usando dados de Threat Intelligence.
  - Combata ameaças de forma autônoma por meio de atualizações em tempo real de listas negras
  - escalabilidade e visão abrangente do tráfego de rede e ameaças identificadas.
- Trabalho futuro: Evoluir a solução para integrar novos recursos
  - Use IA de forma automatizada no fluxo de execução
  - Expanda os indicadores de ameaça
  - Melhore os experimentos em outros ambientes e métricas de desempenho.

# Obrigado !


**Contato:**

larces@uece.br
larces.uece.br