Rede de sensores distribuídos do CAIS

Rildo Souza

28º GTS

cert.br

Agenda

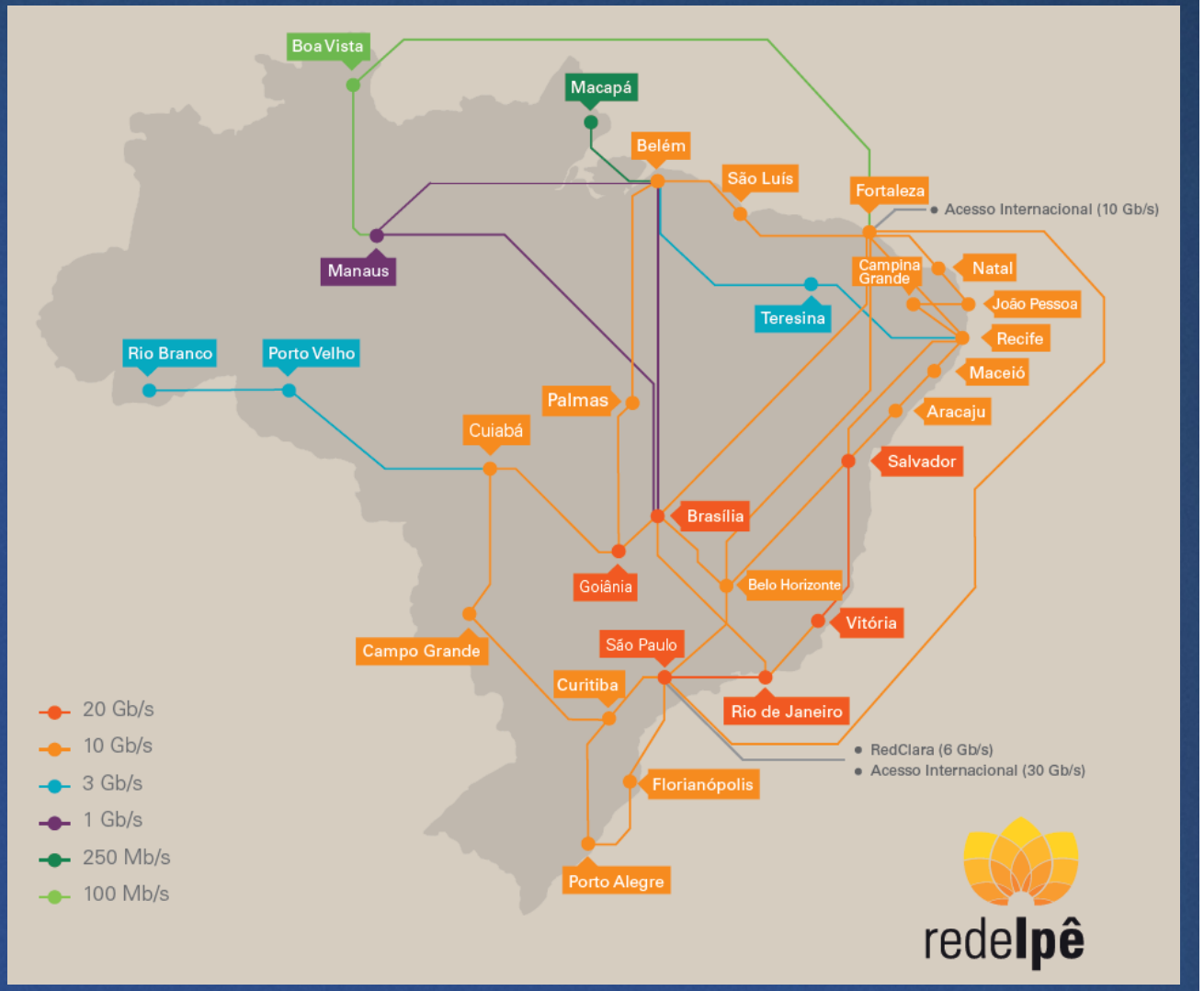
- [ ] Apresentação
- [x] O Projeto
- [ ] Principais números
- [ ] Eventos Detectados
- [ ] Encerramento

Apresentação

RNP

Rede Nacional de Ensino e Pesquisa (RNP), criada pelo MCTI em 1989, para construir uma infraestrutura de internet acadêmica.

Desde então, participa do desenvolvimento da internet no Brasil, com a introdução de novas tecnologias e a implantação da primeira rede óptica acadêmica da América Latina, em 2005, batizada de Ipê.



Apresentação

CSIRT de coordenação da rede acadêmica brasileira, a Rede Ipê, desde 1997.

Atua na detecção, resolução e prevenção de incidentes de segurança de rede, além de elaborar, promover e disseminar práticas de segurança na RNP e instituições a ela vinculadas.

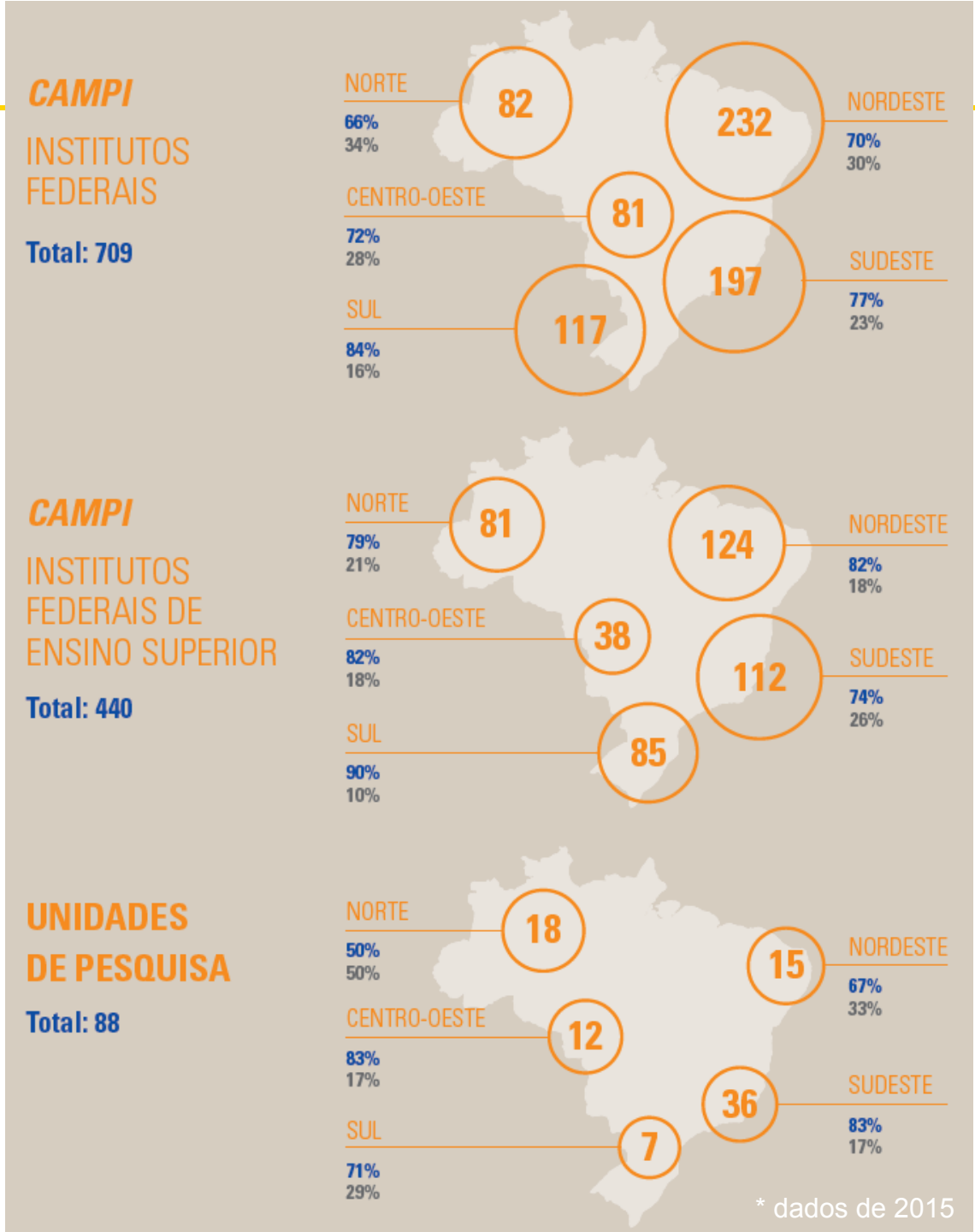
Projeto - Contexto

Rede Ipê, backbone da rede acadêmica.
Capacidade integrada de 345,45 Gb/s.

Interliga 1.237 *campi* de Organizações Usuárias (IFs, IFEs, Unidades de Pesquisa).

Ambiente altamente diversificado em redes, tecnologias e maturidade das equipes de segurança.

Dificuldades para uma detecção eficiente.

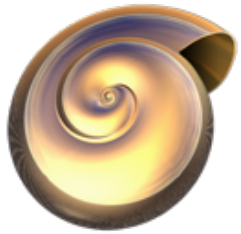



20%
2013
BUSINESS PLAN
MARKET
WWW

Projeto - Objetivo

Criar uma rede se sensores na rede acadêmica.

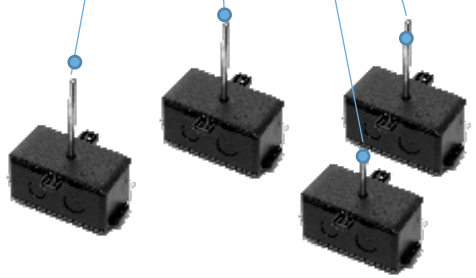
Projeto - O sistema



Projeto - O sistema

Master

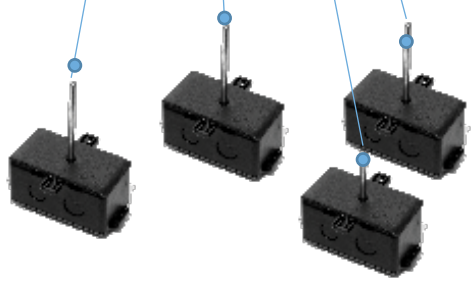
Sensor



Projeto - O sistema

Master

Sensor

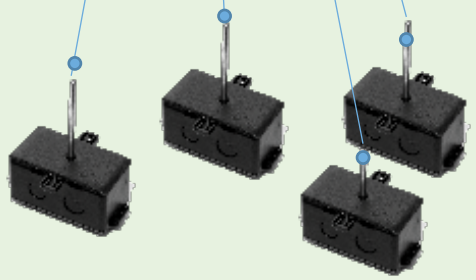


- Gerenciamento dos sensores e instituições
- Gerenciamento das atualizações
- Estatísticas do sistema geral e dos sensores
- Classificação das atividades maliciosas
- Administração geral do sistema

Projeto - O sistema

Master

Sensor



- Interface friendly user
- Plug and play
- Exige pouco conhecimento técnico
- Pouca manutenção e suporte
  - Envio das detecções por e-mail
  - Envio de dados estatísticos e de status
  - Solicitação de atualizações

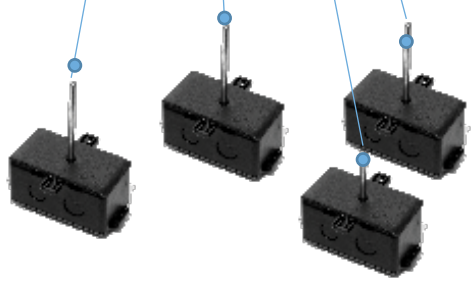
Projeto - O sistema

Master

Conexão

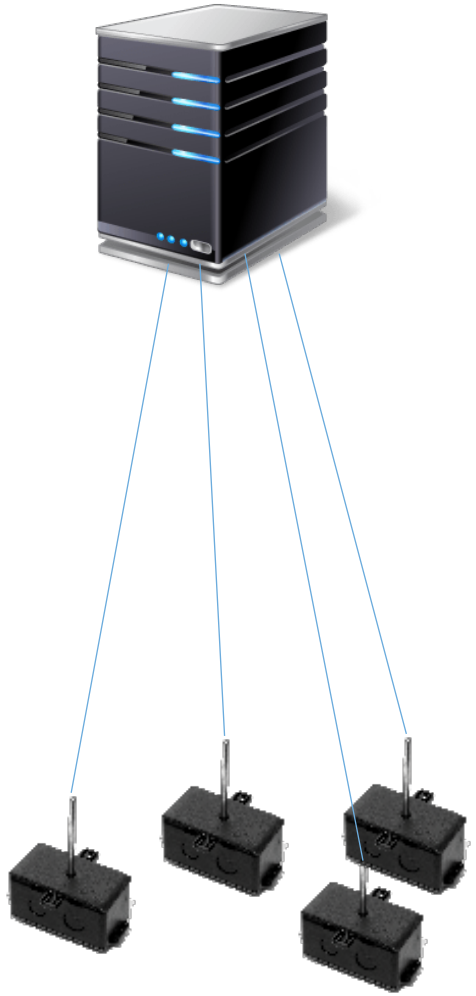
- HTTPS
- Autenticação

Sensor



Projeto - O sistema

Master

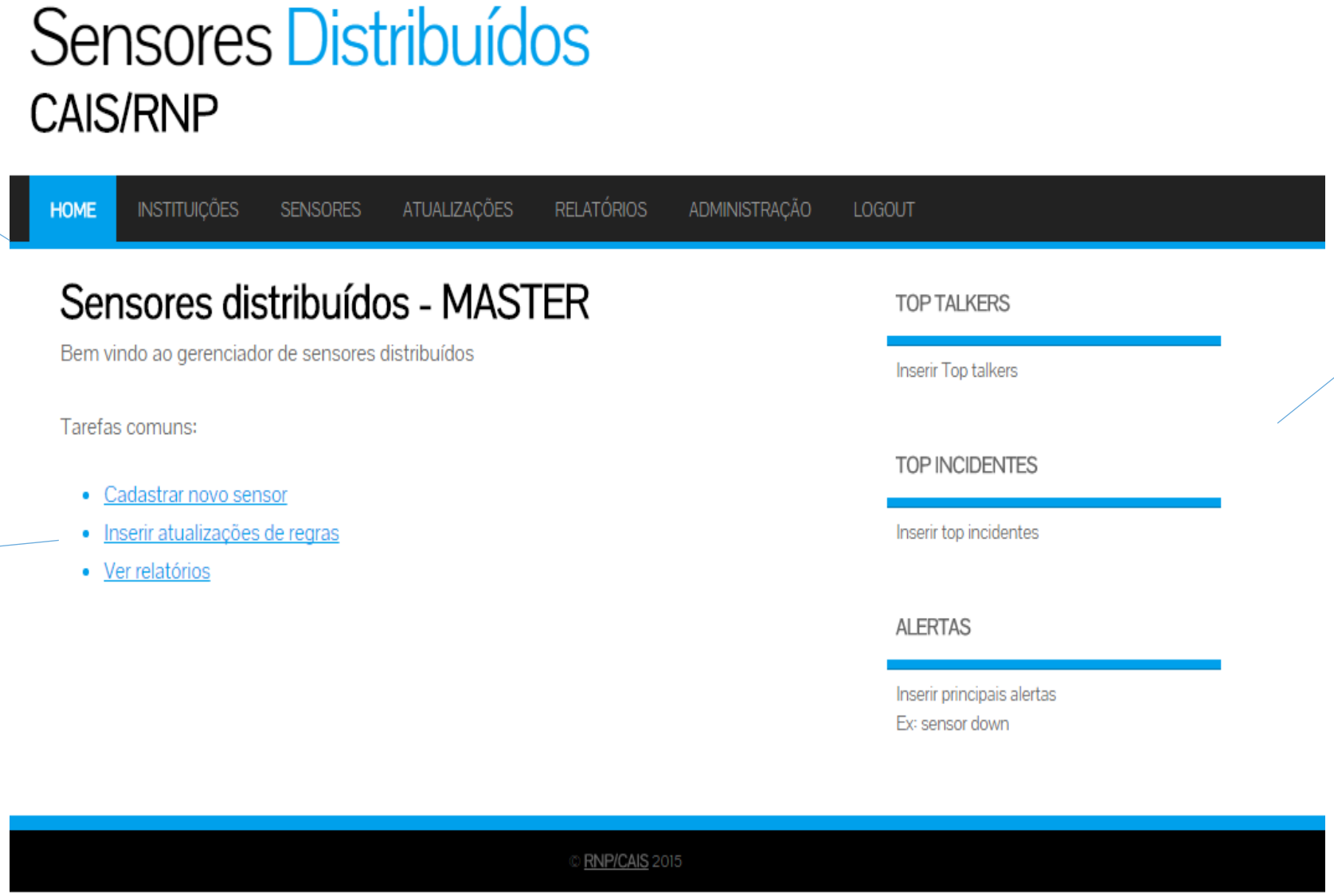


Sensor

Tipos de atualizações

Tipo	Origem	Finalidade
Regras gerais	Emerging Threats	Prover as regras gerais.
Regras customizadas	CAIS	Prover regras específicas, sob demanda.
Exceções de regras	CAIS	Desativar regras, sem a necessidade de gerar nova release.
Blacklist URLs	CAIS / APWG / Catálogo de Fraudes, etc.	Identificar acessos a URLs maliciosas
Blacklist de IPs	CAIS / Shadow Server, etc.	Identificar acessos a IPs maliciosos, como C&C.
Redes	CAIS	Cada cliente possui sua própria rede, portanto a HOME_NET de cada um deve ser única, para maior assertividade.
Atualizações de Sistema	CAIS	Novas versões do sensor, correções e features.

ScreenShots do Master



Menu principal

Tarefas de acesso rápido

Dashboard com informações rápidas

ScreenShots do Master

Sensores Distribuídos
CAIS/RNP

HOME | INSTITUIÇÕES | SENSORES | ATUALIZAÇÕES | RELATÓRIOS | ADMINISTRAÇÃO | LOGOUT

Gerenciamento de updates

- Testar
- Atualizações de Regras
- Exceções de Regras
- Atualizações de URLs
- Atualizações de IPs de botnet
- Atualizações de Sistema

Inserir atualizações de regras:

As regras inseridas aqui serão disponibilizadas para download das engines.
Os arquivos devem ser inseridos no formato .tar.gz.

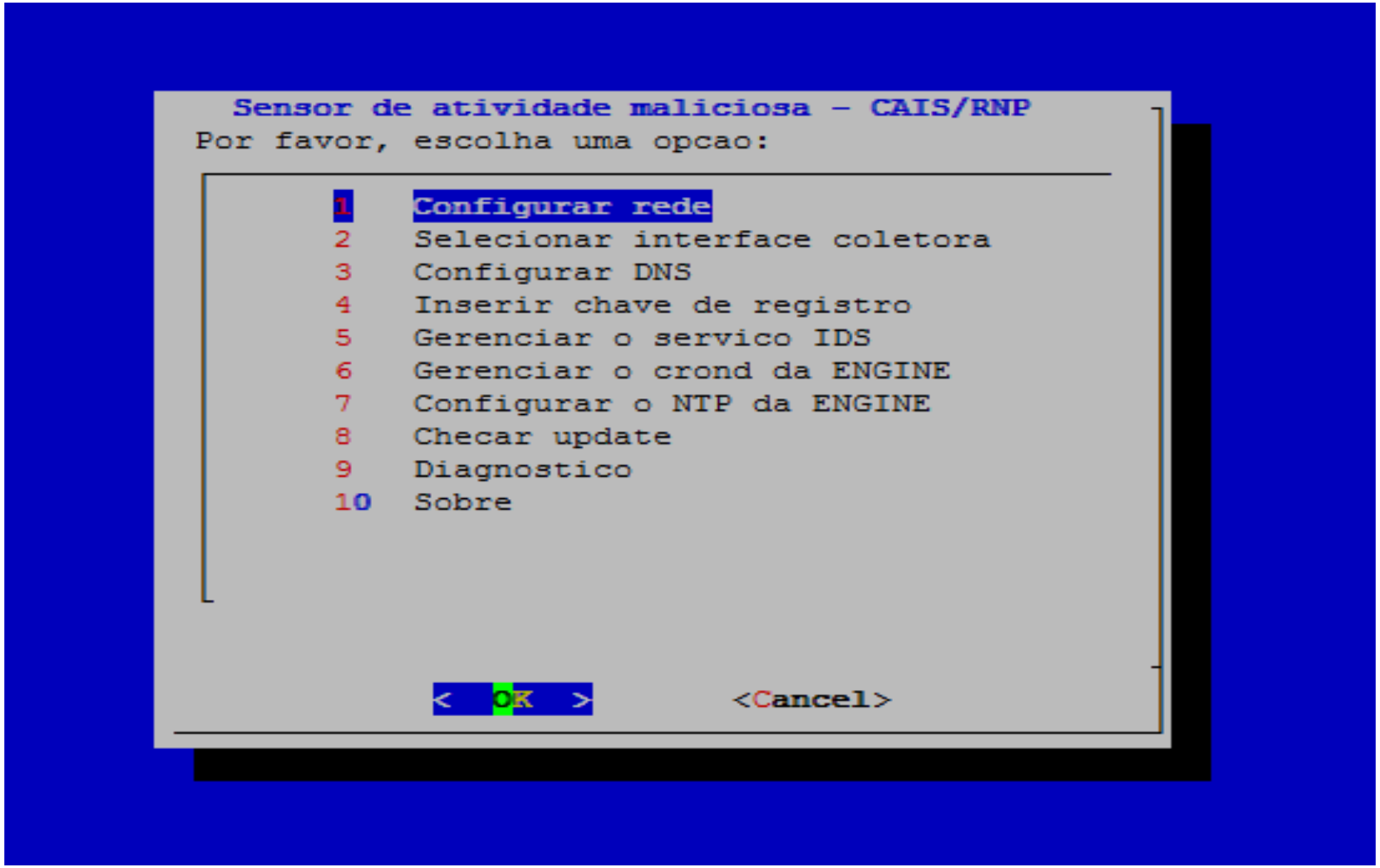
Regras [Escolher arquivo] Nenhum arquivo selecionado

Comentários a respeito dessa atualização

[Enviar arquivo]

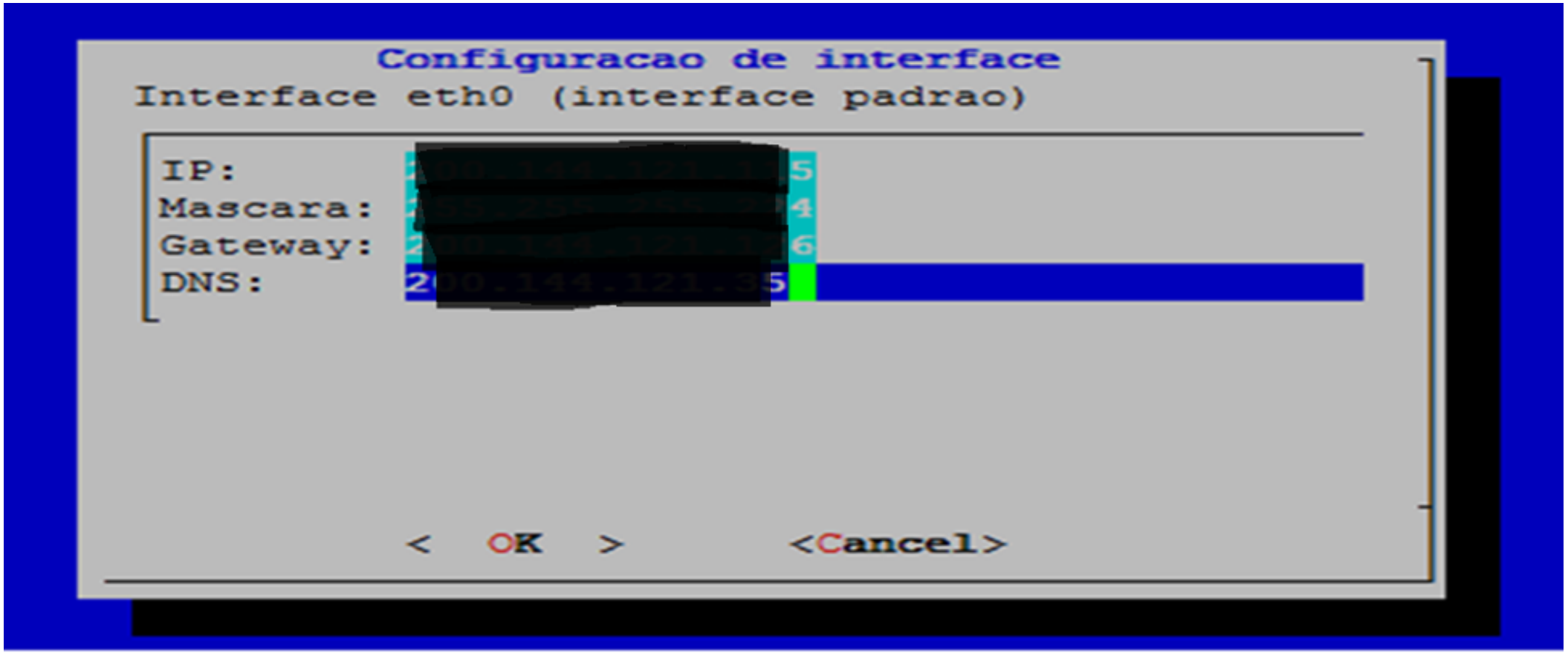
Versões anteriores						
Versão	Data	Tamanho	Tipo	Arquivo	Exceções do arquivo	Comentários a respeito da atualização
5	2016-10-05 14:24:43	1.83 MB	application/gzip	emerging.rules.tar.gz	#2200003,#2200007,#2...	Última versão da ET
4	2016-09-08 14:10:48	1.83 MB	application/gzip	emerging.rules.tar.gz	#2200003,#2200007,#2...	Última versão da ET
3	2016-02-04 17:02:07	1.75 MB	application/gzip	emerging.rules.tar.gz	#2200003,#2200007,#2...	Ultima versão da ET.
2	2015-10-05 10:39:10	1.7 MB	application/gzip	emerging.rules_v2.tar.gz	#2200003,#2200007,#2...	
1	2015-09-30 11:47:19	1.69 MB	application/gzip	emerging.rules.tar.gz	#2200003,#2200007,#2...	Primeira versão das regras.

ScreenShots da Engine(Sensor)



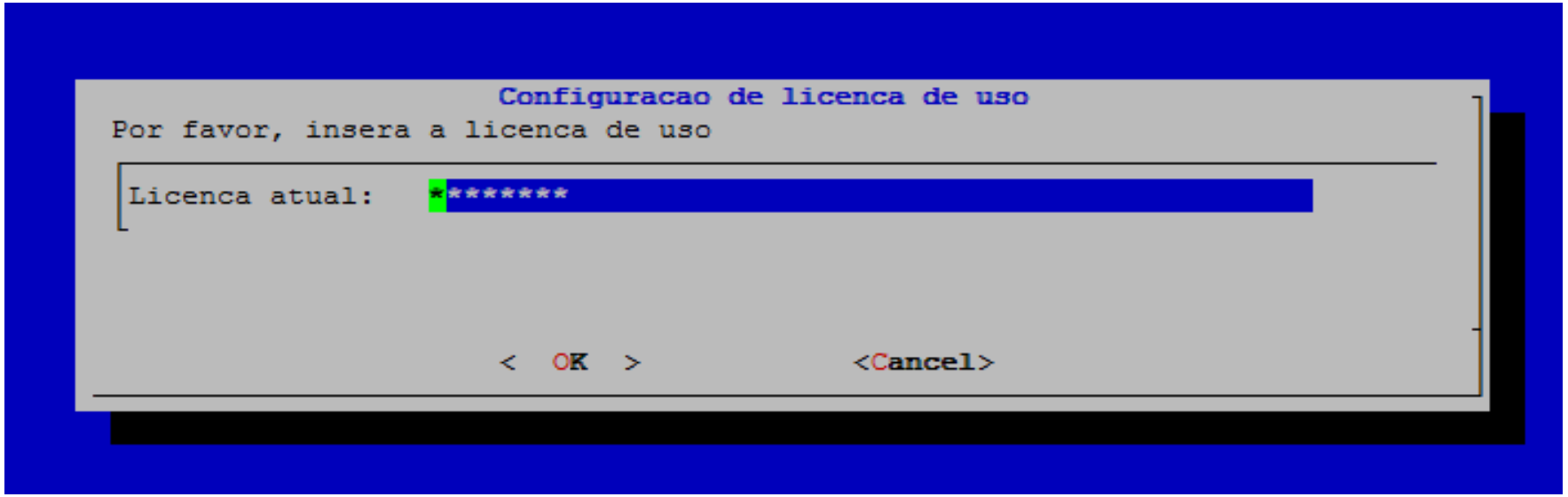
Menu principal

ScreenShots da Engine(Sensor)



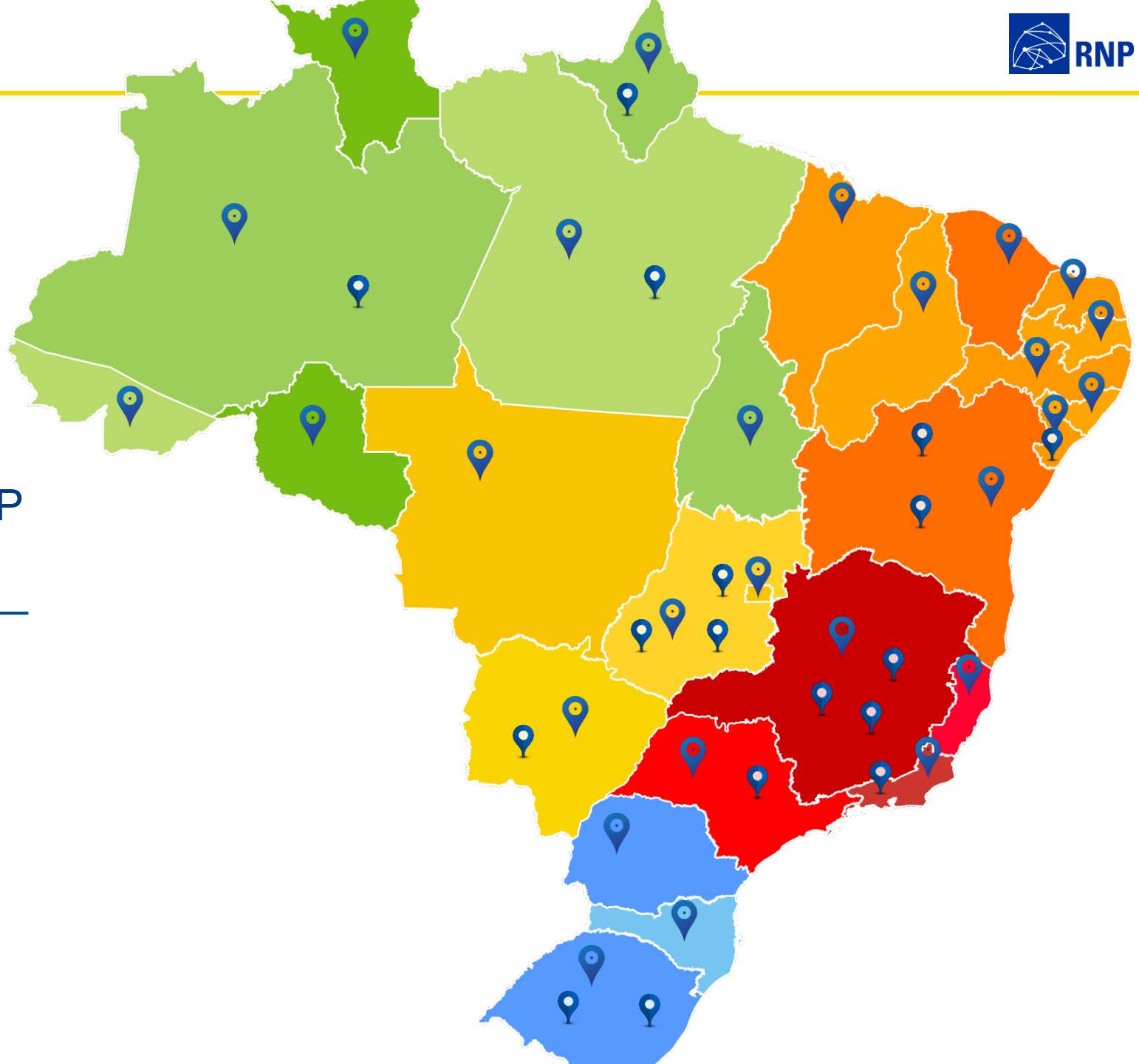
Configuração de interface

ScreenShots da Engine(Sensor)



Inserção de licença

Projeto - Implantação

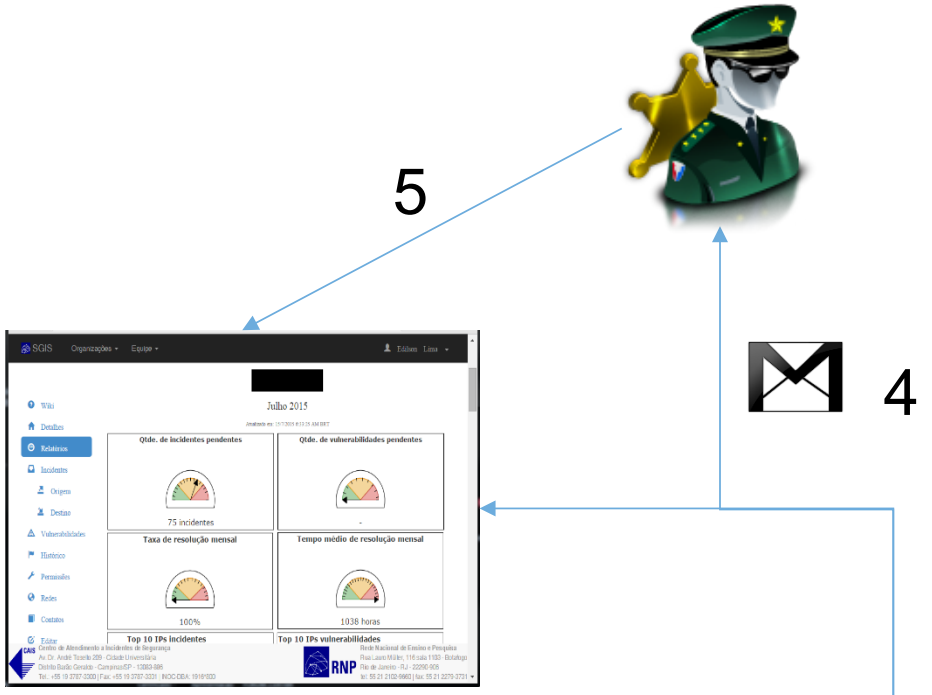


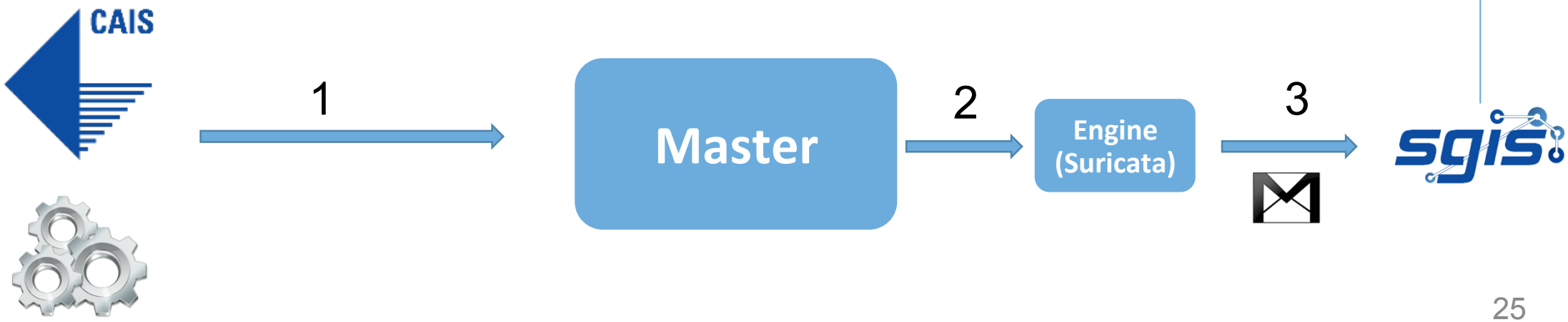
- ✓ 27 Pontos de Presença da RNP
- ✓ 17 Organizações Usuárias

44 Sensores Instalados

Integração com o SGIS

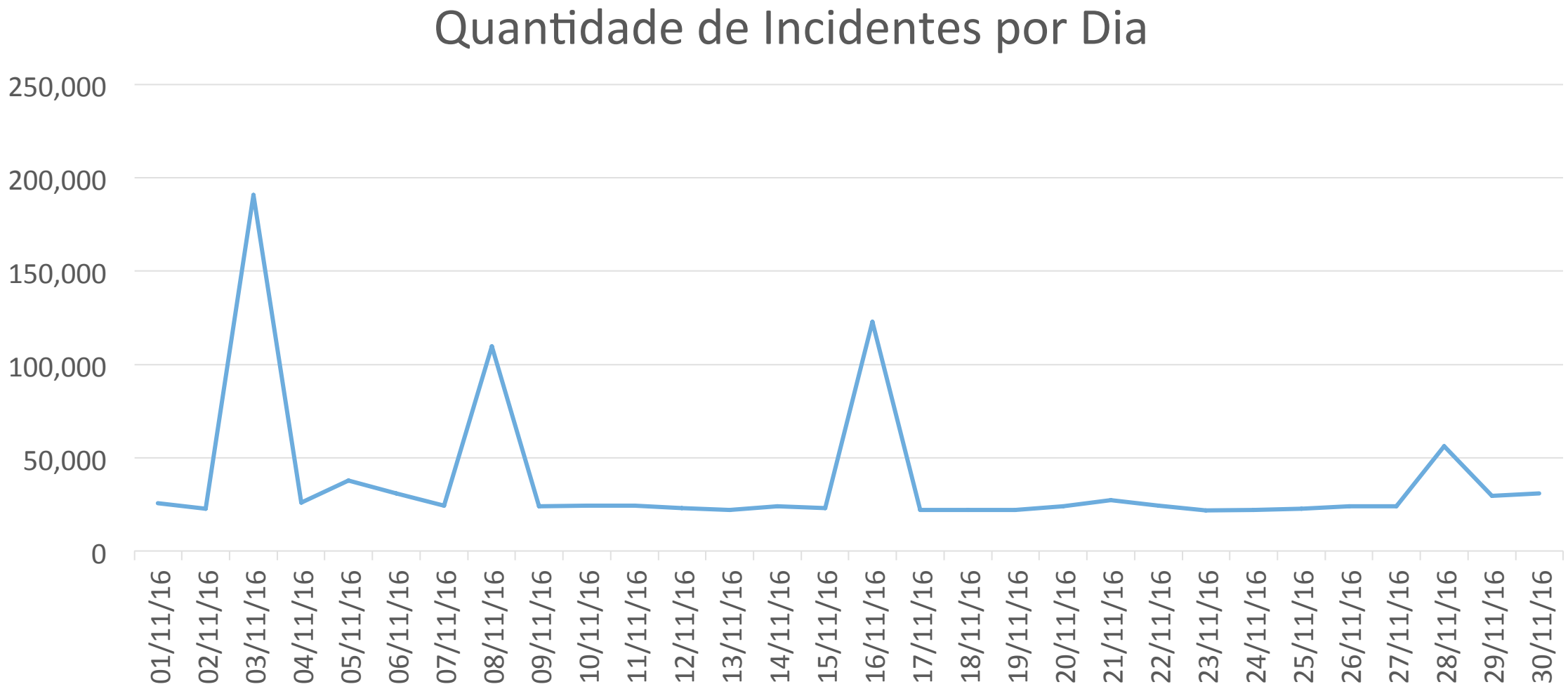
Passo	Ação
1	CAIS alimenta o Master com informações processadas
2	Master envia update para Engine
3	Engine detecta eventos e notifica SGIS
4	SGIS notifica usuário
5	Usuário acessa interface do SGIS





Principais números

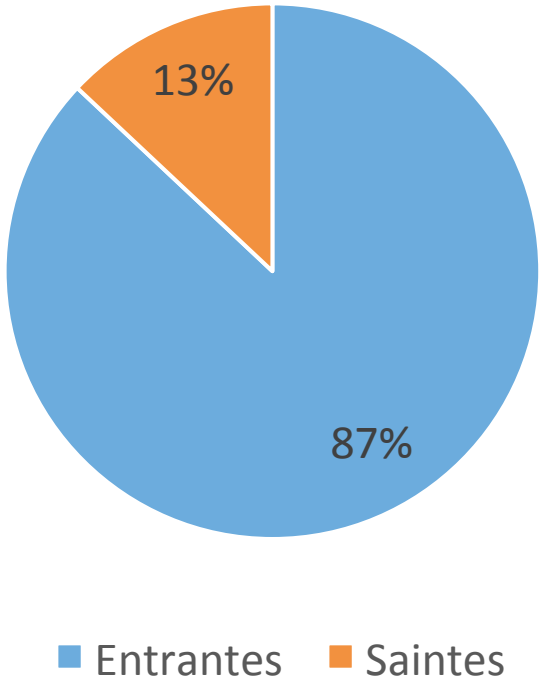
Principais números



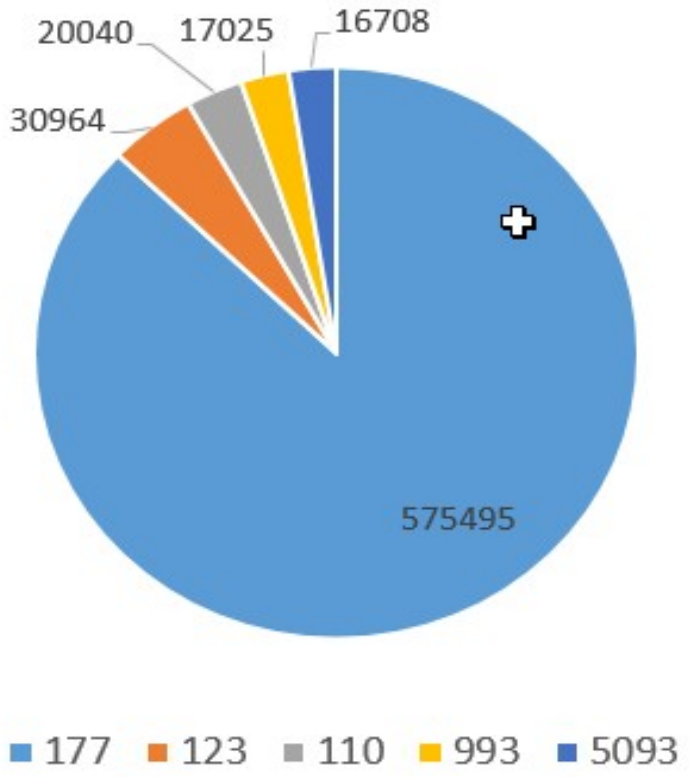
Média: 37.580

Principais números

Fluxo da atividade maliciosa

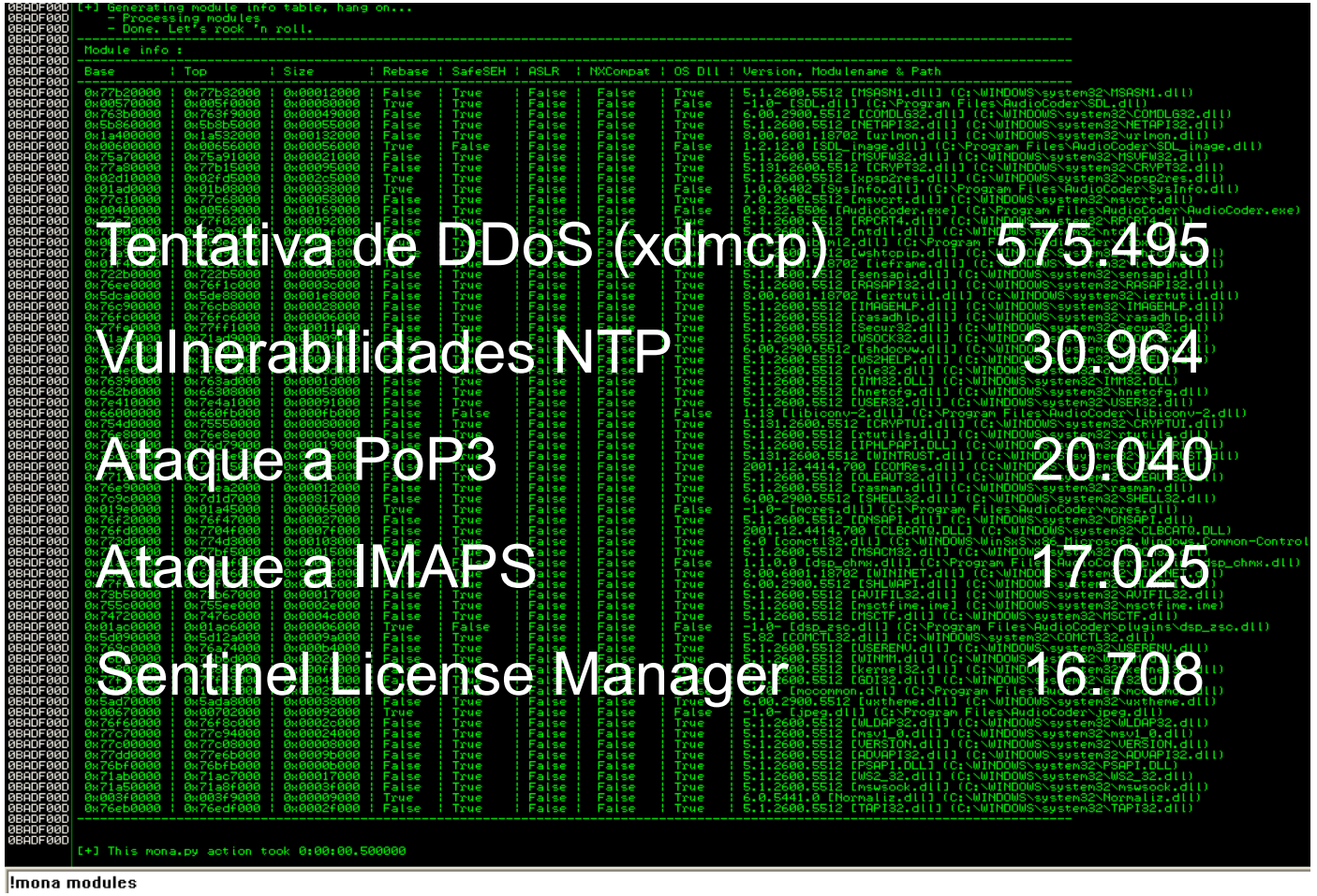


Portas utilizadas



Principais números

Principais atividades maliciosas detectadas



Tentativa de DDoS (xdmcp) 575.495

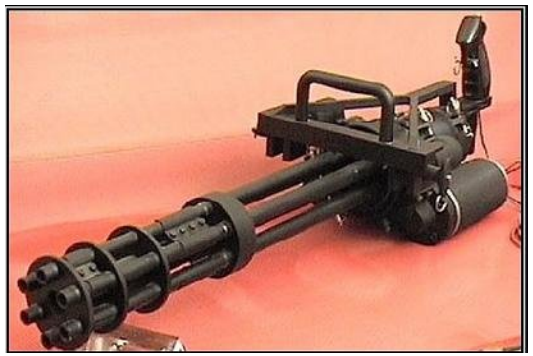
Vulnerabilidades NTP 30.964

Ataque a PoP3 20.040

Ataque a IMAPS 17.025

Sentinel License Manager 16.708

Eventos detectados



Eventos detectados

Mais de 10 botnets diferentes detectadas

nicaze.net	Zeus	XcodeGhost
PCRat/Gh0st	Kelihos	Bladabindi/njrat
Beacon	Feodo	Palevo
	DealPly	

Próximos passos

- Otimizar os relatórios
- Fazer a integração com outras fontes(Blacklist URL,Ips e outros)
- Integrar com PhotoDNA (sistema anti-pornografia infantil)
- Aumentar o número de sensores nas instituições de ensino

Dúvidas

Encerramento

Muito obrigado,

Rildo Souza
rildo.Souza@rnp.br