SISTEMAS DE INFORMAÇÃO

MURILO DE ARAUJO CHIANFA

NAMEDZEUS

UM SISTEMA DE IMPOSIÇÃO DE POLÍTICAS DE REDE BASEADO EM HOST

Apucarana
2023

MURILO DE ARAUJO CHIANFA

NAMEDZEUS

UM SISTEMA DE IMPOSIÇÃO DE POLÍTICAS DE REDE BASEADO EM HOST

Trabalho de conclusão de curso apresentado ao Curso de Bacharelado em Sistemas de Informação da Faculdade de Apucarana – FAP, como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Fabrício José Coelho.

Apucarana

2023

MURILO DE ARAUJO CHIANFA

NAMEDZEUS

UM SISTEMA DE DETECÇÃO DE INTRUSÃO BASEADO EM HOSTS

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Sistemas de Informação da Faculdade de Apucarana – FAP, como requisito parcial , com nota final igual a _____, conferida pela Banca Examinadora formada pelos professores:

COMISSÃO EXAMINADORA

Prof. Esp. Fabrício José Coelho
Faculdade de Apucarana

Prof. Me. Edmilson Domaredzki Verona
Faculdade de Apucarana

Prof. Esp. Guilherme H. S. Nakahata
Faculdade de Apucarana

Apucarana, 20 de Novembro de 2023.

Dedico este trabalho,

À minha família por sempre estar me incentivando a nunca desistir, para que assim eu conseguisse chegar até aqui.

À todos os amigos e colegas que estão diariamente em busca de conhecimento.

AGRADECIMENTOS

Sou grato à minha família por todo esforço investido em minha educação e pelo companheirismo de todas as horas.

Aos colegas de curso e professores, que juntos trilhamos mais uma etapa importante de nossas vidas.

A família Ganascim e a empresa Made4IT pela oportunidade de crescimento profissional.

A todos que direta ou indiretamente colaboraram para a realização deste trabalho.

“A chave do sucesso nos negócios é perceber para onde o mundo se dirige e chegar ali primeiro.”

Bill Gates

CHIANFA, Murilo de Araujo. **NAMEDZEUS – Um sistema de imposição de políticas de rede baseado em host**. 78p. Trabalho de Conclusão de Curso (Monografia). Graduação em Sistema de Informação da Faculdade de Apucarana. Apucarana-Pr. 2023.

RESUMO

Tendo em vista a grande complexidade no gerenciamento de regras e políticas de rede em firewalls para os diversos hosts, o software desenvolvido neste trabalho visa sanar essa dor, provendo um gerenciamento centralizado dessas regras em grupos e padrões, para que assim, sejam associadas aos servidores hospedando serviços de mesmo propósito de forma simples e rápida.

Palavras-chave: Firewall. Netfilter. Iptables.

CHIANFA, Murilo de Araujo. **NAMEDZEUS – A centralized host-based network policies enforcement system**. 78p. Course Completion Work (Monograph). Degree in Information System from the Faculty of Apucarana. Apucarana-Pr. 2023.

ABSTRACT

Considering the great complexity in managing network rules and policies on firewalls for various hosts, the software developed in this work aims to address this challenge by providing centralized management of these rules in groups and patterns. This allows them to be associated with servers hosting services of similar purposes in a simple and fast manner.

Palavras-chave: Firewall. Netfilter. Iptables.

LISTA DE FIGURAS

LISTA DE SIGLAS

2FA	Two Factor Authentication
CDN	Content Delivery Network
CIDR	Classless Inter-Domain Routing
CSV	Comma Separated Value
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
JPG	Joint Photografhics Experts Groups
NAT	Network Address Translation
OS	Operating System
OSI	Open Systems Interconnection
PDF	Portable Document Format
PNG	Portable Network Graphics
RBAC	Role Based Access Control
RFC	Request For Comments
RIR	Regional Internet Registry
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

SUMÁRIO

1 INTRODUÇÃO

O objetivo do sistema é proporcionar ao cliente uma segunda camada de segurança para seus servidores expostos ao público, tendo em vista gerenciar e visualizar as políticas de rede e regras de detecção de tráfego de rede malicioso, tudo em apenas um único lugar seguindo a ideologia de um IDS baseado em hosts.

1.1 Descrição do sistema

O sistema é acessível via web e poderá ser integrado com sistemas de automação de infraestrutura para agilizar a configuração no dia a dia.

Um de seus pontos fortes é a centralização dos logs gerados, de onde será possível gerar relatórios e controlar remotamente a grande quantidade de regras de detecção de uma só vez.

1.2 Principais características do sistema

Entre as principais características do NamedZeus, podemos citar:

- **Auditoria**: Possibilidade de realizar uma auditoria das alterações das políticas.
- **Monitoramento em tempo real**: Possibilidade de monitorar em tempo real os alertas.
- **Centralização das políticas de rede**: Possibilidade de pré cadastrar, agrupar e criar templates de regras.
- **Automações**: Possui automações para facilitar no uso do dia-a-dia.
- **Histórico**: Mantém um histórico dos logs do(s) servidor(es) por um longo período.

1.3 Equipamento necessários

O sistema é acessível via navegador web, foi testado em 2 principais disponíveis no mercado: Google Chrome e Mozilla Firefox, com as resoluções de tela 1920x1080 e 1366x768.

- Requisitos mínimos para o Google Chrome:
  https://support.google.com/chrome/a/answer/7100626?hl=en-US
  Link para download da última versão (Novembro, 2023):
  https://www.google.com/chrome/

- Requisitos mínimos para o Mozilla Firefox:
  https://www.mozilla.org/en-US/firefox/119.0.1/system-requirements/
  Download última versão (Novembro, 2023):
  https://www.mozilla.org/en-US/firefox/new/

1.4 Suporte técnico

Em caso de problemas ou dúvidas, o usuário deve primeiramente consultar este manual e averiguar se sua dúvida não é sanada pelo mesmo, caso o problema persista, o usuário deve contatar:

Desenvolvedor: Murilo de Araujo Chianfa.
Formulário: https://namedzeus.com/contact
Email: contact@namedzeus.com

2 ACESSANDO O SISTEMA

2.1 Entrando no sistema pela primeira vez

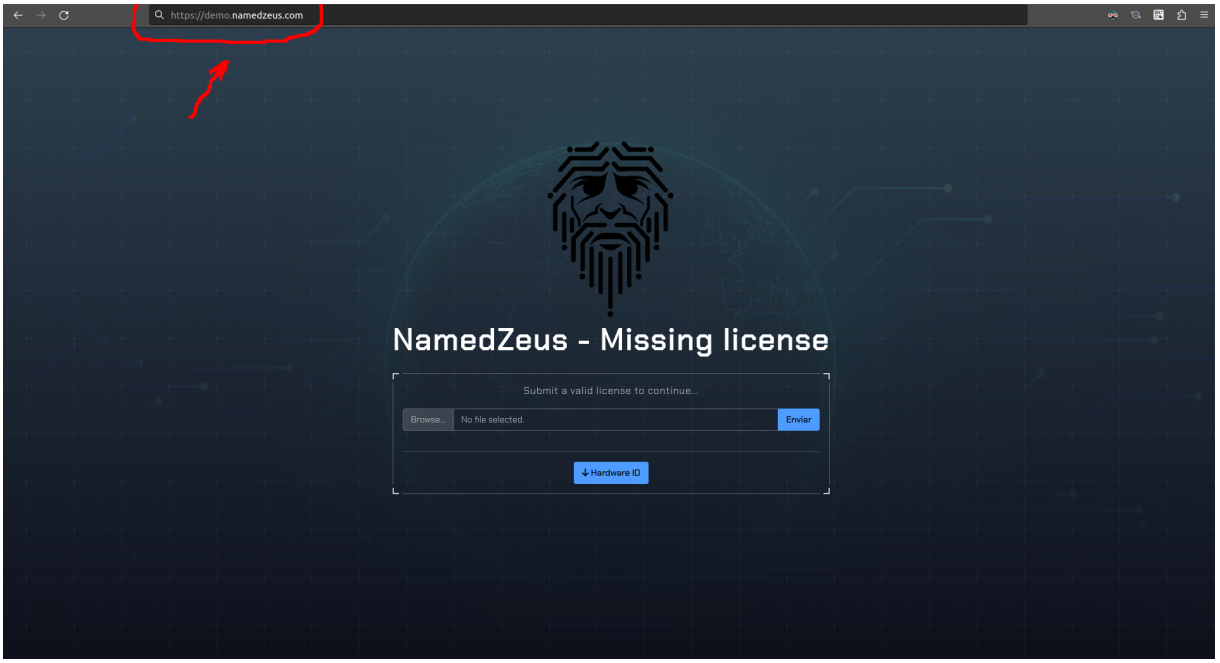
Ao instalar o sistema em seu próprio servidor, você pode acessá-lo através de um dos navegadores web homologados por nós (Google Chrome e Mozilla Firefox), na barra de endereços, utilize um dos endereços de IP da(s) interface(s) de rede de seu servidor ou registre um adicione um novo registro DNS redirecionado para o mesmo, para facilitar seu acesso.

Para este manual, vamos utilizar o ambiente de demonstração registrado em https://demo.namedzeus.com/ para confecção das figuras do manual.

Você pode entrar em nossa demonstração para visualizar você mesmo todas as funcionalidades disponíveis no sistema, as credenciais de acesso são:

- Usuário: demo@namedzeus.com
- Senha: demo@demo

Figura 1 – Acessando o sistema

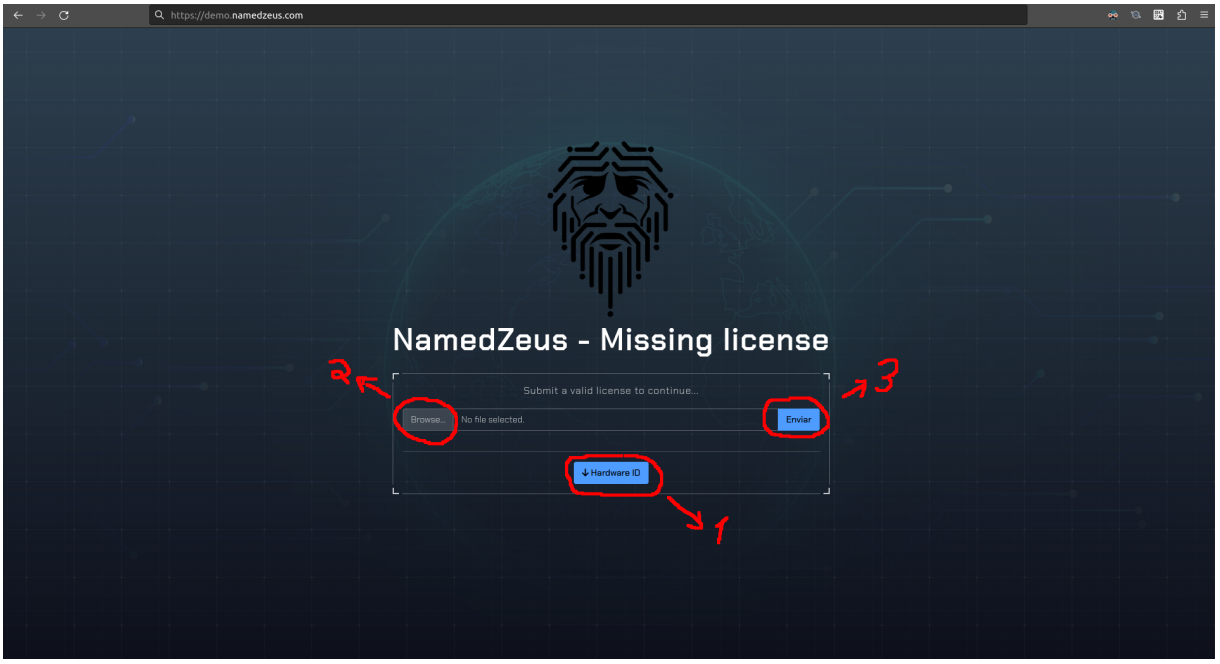


Fonte: Autoria própria, 2023.

2.2 Licenciando o sistema

Inicialmente, será necessário submeter uma licença válida para utilizar o sistema, para obter esta licença, você pode seguir os passos dispostos nesta página: https://namedzeus.com/pricing

Figura 2 - Licenciando o sistema

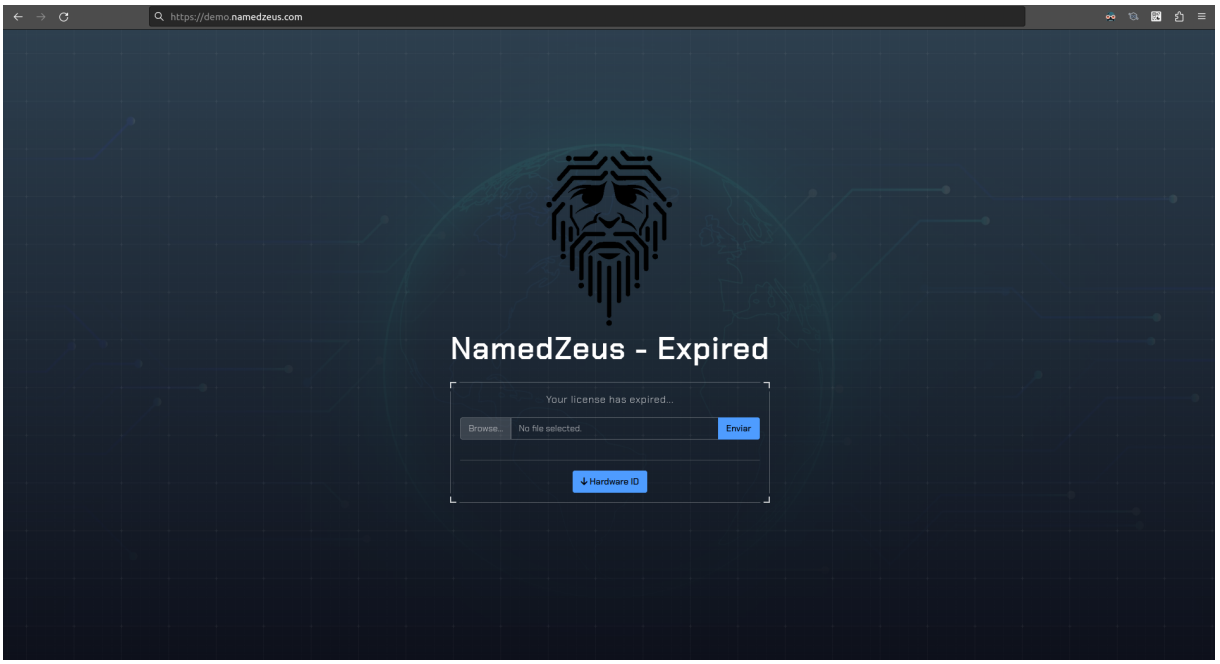


Fonte: Autoria própria, 2023.

- **1 –** Botão para realizar o download da identificação de hardware.
- **2 –** Botão para abrir a caixa de seleção para o arquivo de licença.
- **3 –** Botão para fazer o envio da nova licença.

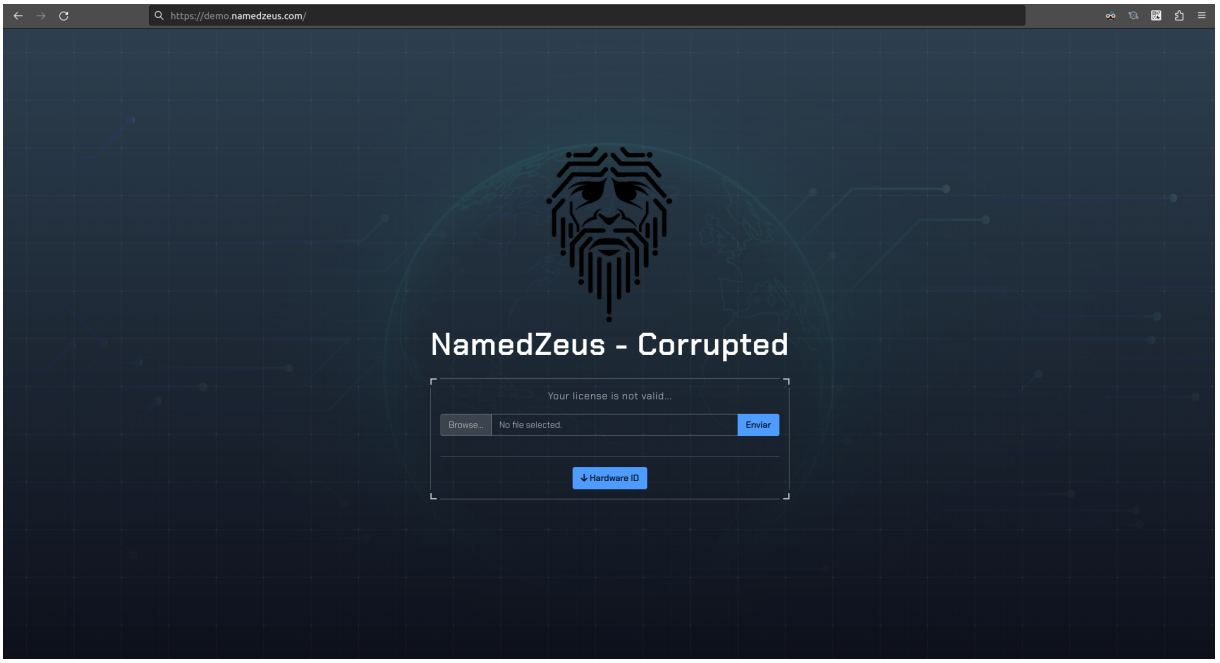
Alguns erros podem ocorrer após o upload da licença se ela não for válida, for corrompida, expirada ou não tenha permissão:

Figura 3 - Licença expirada



Fonte: Autoria própria, 2023.

Figura 4 - Licença corrompida

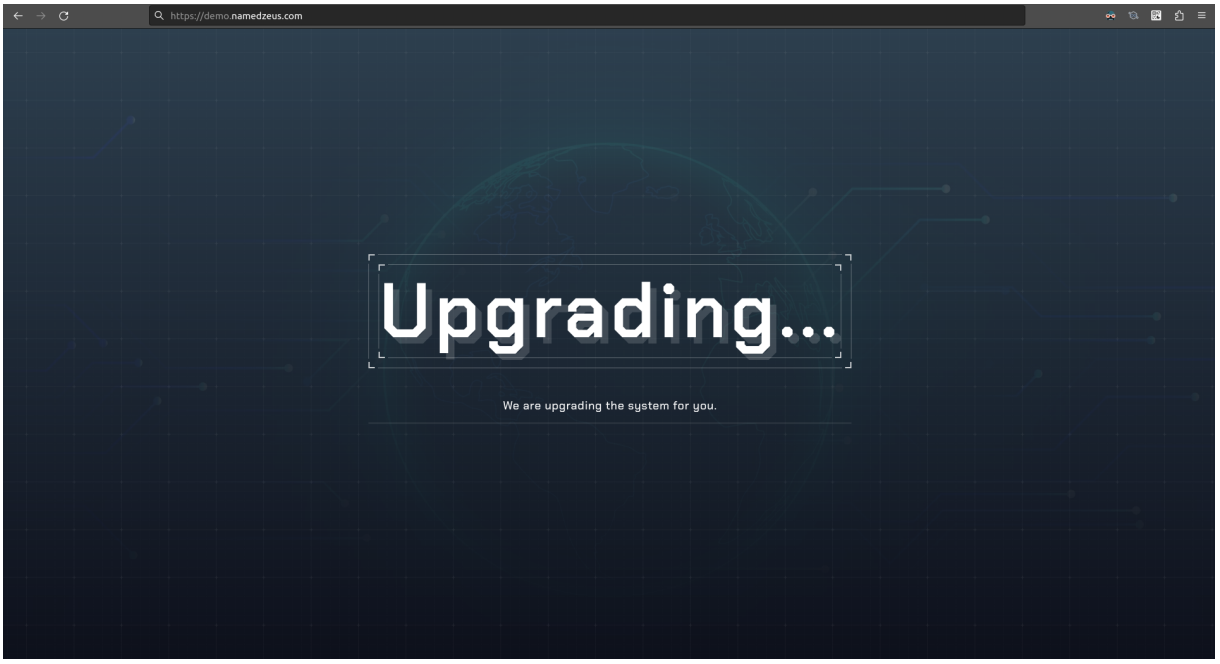


Fonte: Autoria própria, 2023.

2.3 Atualização do sistema

Após ter sucesso em submeter a nova licença, o sistema irá se auto atualizar para a última versão disponível, onde após o término, automaticamente você será redirecionado para página de login.

Figura 5 - Atualizando o sistema



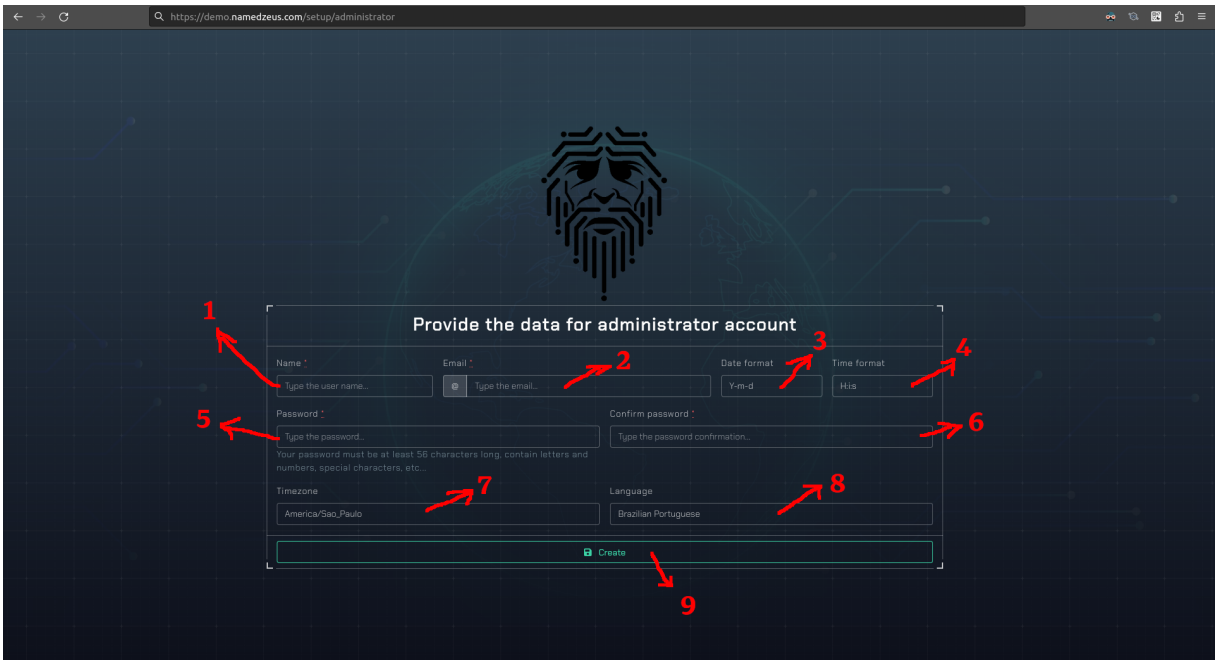
Fonte: Autoria própria, 2023.

Esta atualização pode demorar um pouco para terminar dependendo da velocidade e da qualidade de seus discos de armazenamento, nossos testes apontam cerca de 5 minutos utilizando um HDD e 30 segundos com um SSD.

2.4 Criação do super administrador

Para que seja possível acessar o sistema, é necessário criar o super administrador após ativar sua licença, caso seja uma renovação de licença, não será necessário realizar este passo.

Figura 6 - Cadastrando o super administrador



Fonte: Autoria própria, 2023.

- **1 –** Campo para fornecer o nome do super administrador.
- **2 –** Campo para fornecer o email do super administrador.
- **3 –** Campo para escolher o formato de exibição das datas no sistema.
- **4 –** Campo para escolher o formato de exibição dos horários no sistema.
- **5 –** Campo para fornecer a senha do super administrador.
- **6 –** Campo para confirmar a senha do super administrador.
- **7 –** Campo para escolher o fuso-horário do super administrador.
- **8 –** Campo para escolher a linguagem de exibição do sistema para o super administrador e o padrão de criação para os próximos usuários.
- **9 –** Botão para fazer o cadastro do super administrador.

2.5 Login do sistema

Na tela de login do sistema, é possível entrar com um usuário já cadastrado no sistema, caso ainda não possua um usuário, a pessoa deverá pedir para o administrador do sistema convidá-lo, tendo em vista a alta criticidade e confidencialidade dos dados tratados dentro do sistema.

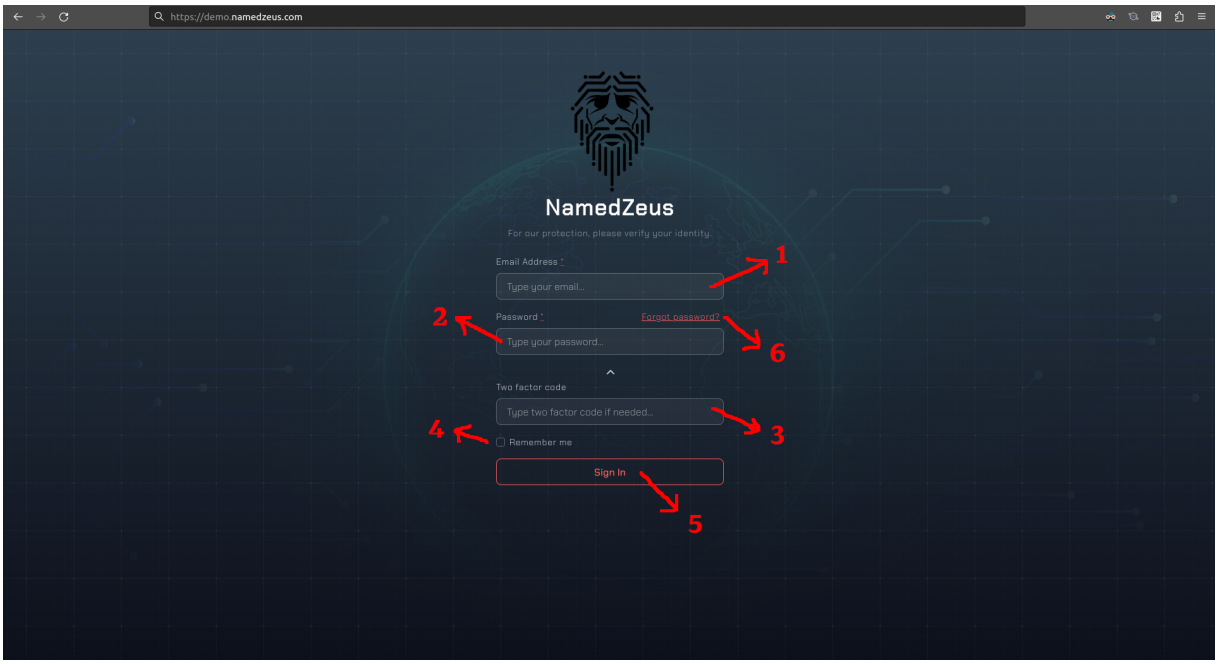
Caso necessário, o usuário deverá fornecer o código do segundo fator de autenticação para que ele possa se autenticar.

O usuário poderá marcar a caixa de “Remember me” caso queira que seu email seja salvo nos cookies para que o auto preenchimento do navegador possa agilizar a autenticação.

Outra opção disponível na tela de login será a de “Esqueci minha senha”, muito comum em sistemas WEB que possuem autenticação de usuário, ao solicitar o pedido de reset de senha, um link de reset da senha será enviado para o email fornecido caso ele exista na base de usuários do sistema.

Toda e qualquer ação no sistema depende dessa primeira identificação do usuário, quaisquer ações não serão permitidas sem o mesmo.

Figura 7 - Login do sistema



Fonte: Autoria própria, 2023.

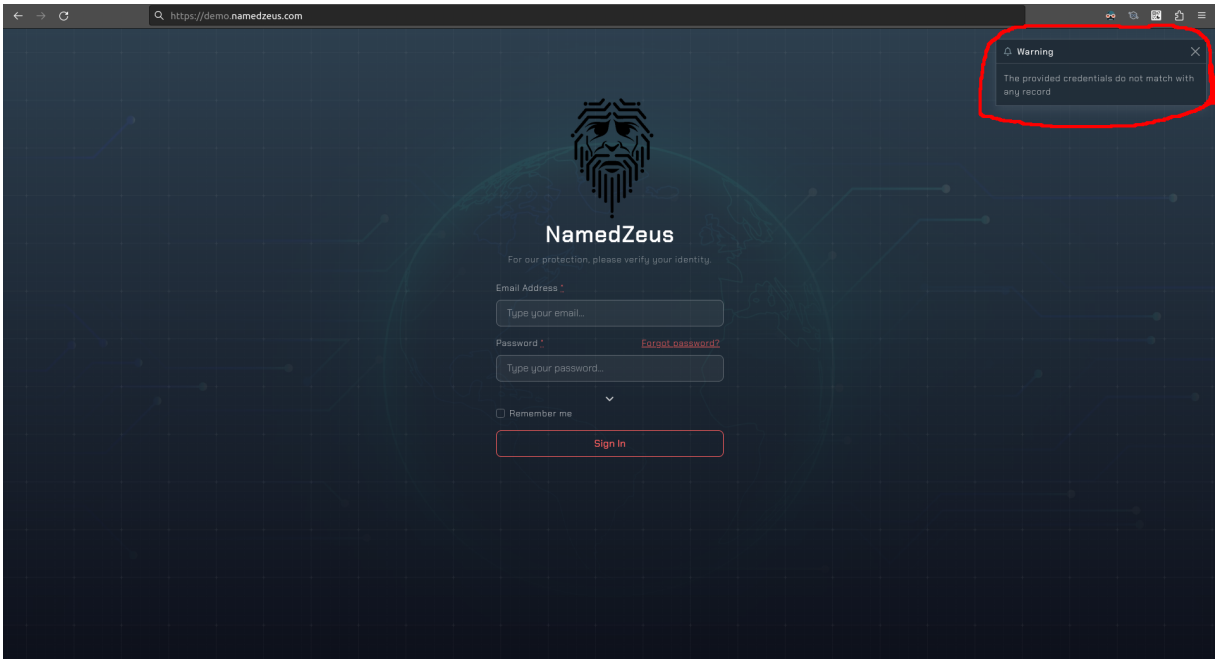
- **1 –** Campo para inserir o email de um usuário cadastrado no sistema.
- **2 –** Campo para inserir a senha de um usuário cadastrado no sistema.
- **3 –** Campo para confirmar o código do segundo fator de autenticação.
- **4 –** Botão para salvar um último email utilizado para entrar no sistema.
- **5 –** Botão para realizar o login no sistema.
- **6 –** Botão para recuperar a senha de um usuário por email.

3 ALERTAS COMUNS

3.1 Notificações de ações

Todos os alertas do sistema, aparecem em uma caixa no canto superior direito do sistema, tanto alertas de erros quanto avisos e informações.

Figura 8 - Notificações de ações



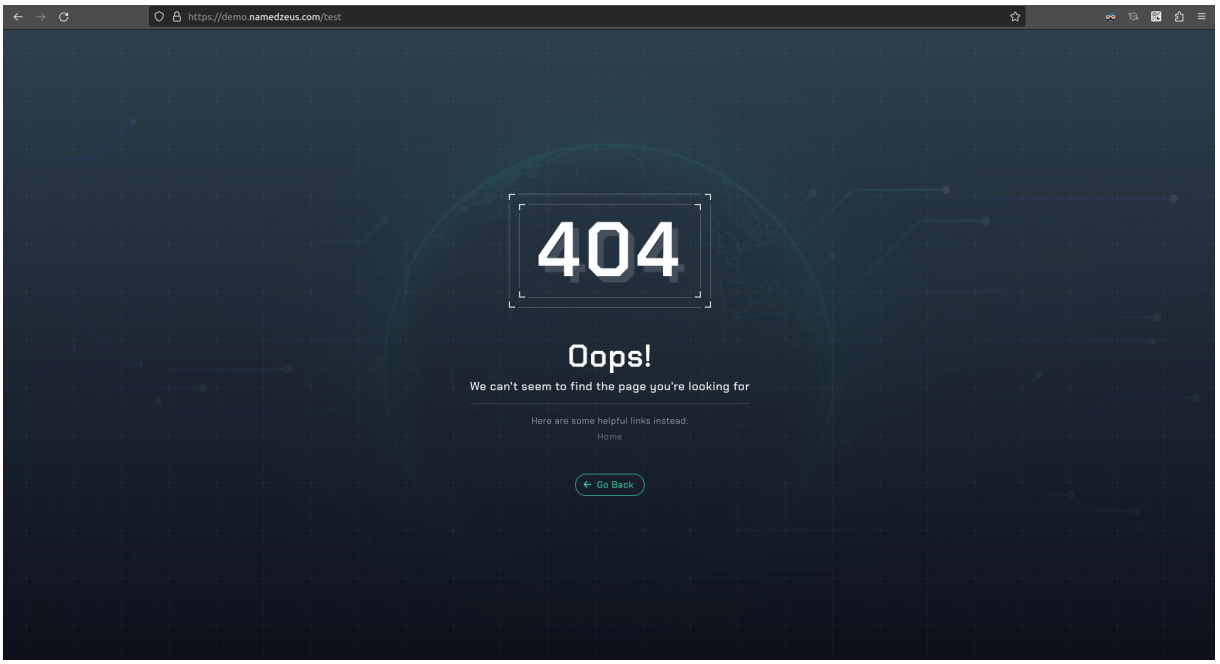
Fonte: Autoria própria, 2023.

3.2 Páginas de erros

Para alguns erros do sistema, uma página com o código HTTP de erro será exibida juntamente com uma mensagem descrevendo o erro para os usuários mais leigos.

3.2.1 Página não encontrada

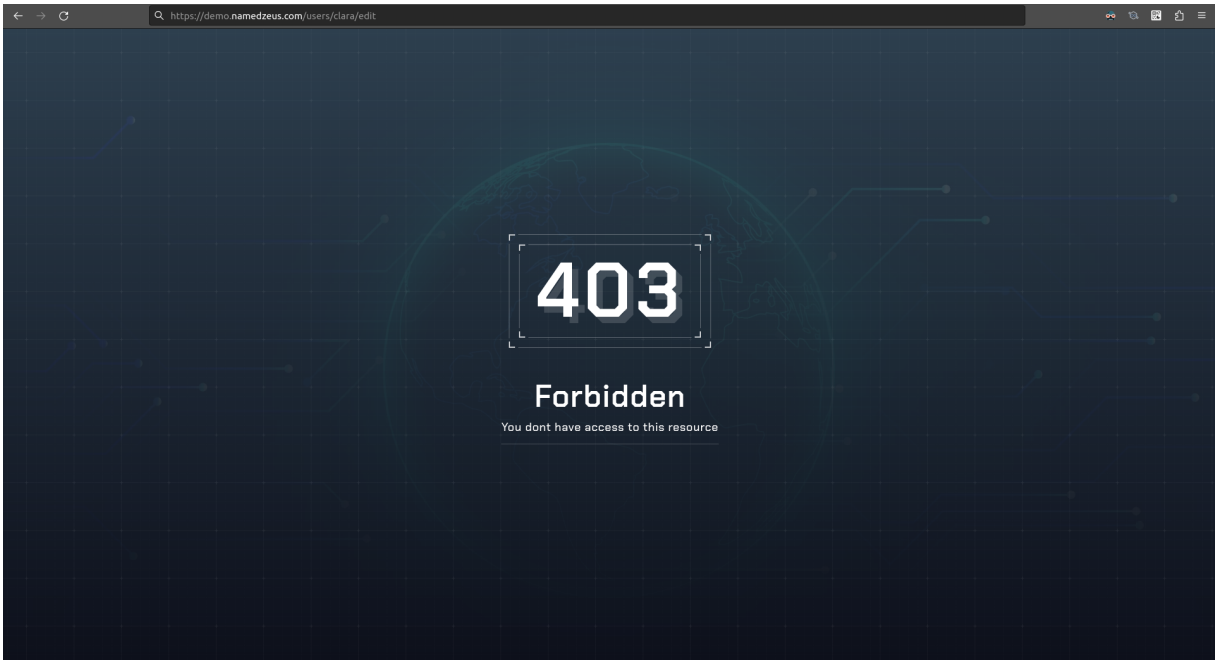
Figura 9 - Página não encontrada



Fonte: Autoria própria, 2023.

3.2.2 Ação não permitida

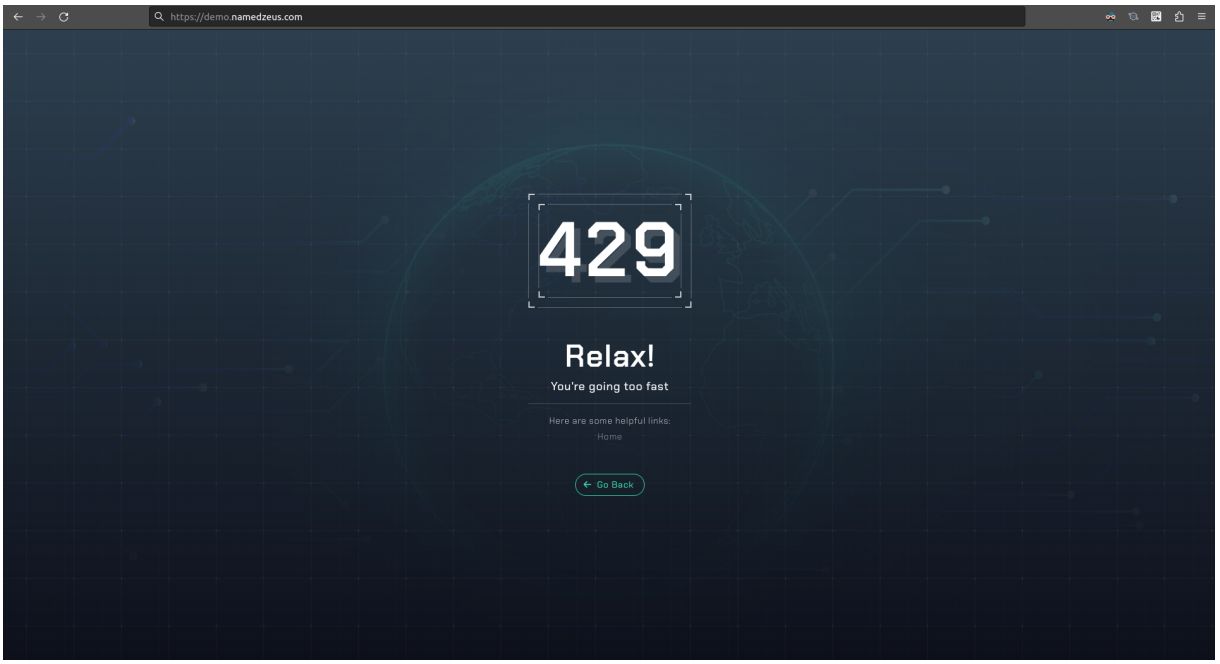
Figura 10 - Ação não permitida



Fonte: Autoria própria, 2023.

3.2.3 Limite de acesso

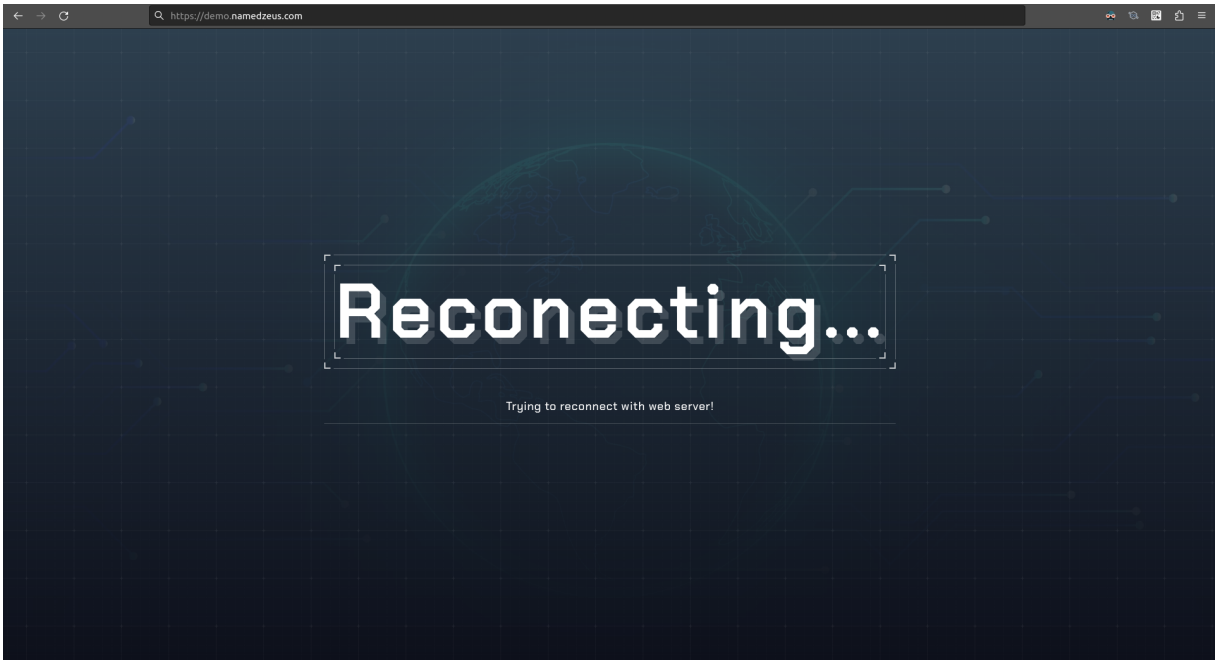
Figura 11 - Limite de requisições atingido



Fonte: Autoria própria, 2023.

3.2.4 Tentativas de reconexão

Figura 12 - Tentando reconexão

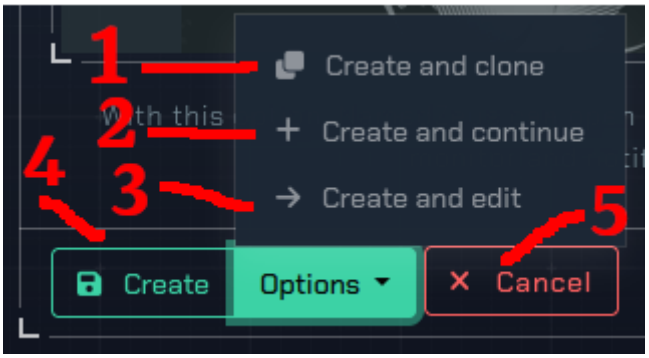


Fonte: Autoria própria, 2023.

4 PADRÕES DO SISTEMA

4.1 Botões de cadastro

Figura 13 - Botões de cadastro



Fonte: Autoria própria, 2023.

- **1 –** Botão para criar um registro e retornar para a página de criação com os mesmo dados preenchidos, para agilizar o cadastro em massa de registros.
- **2 –** Botão para criar um registro e retornar para a página de criação mas com os campos zerados.
- **3 –** Botão para criar um registro e ir direto para a página de edição.
- **4 –** Botão para criar um registro e retornar para a listagem.
- **5 –** Botão para cancelar a criação de um registro.

4.2 Informações do registro

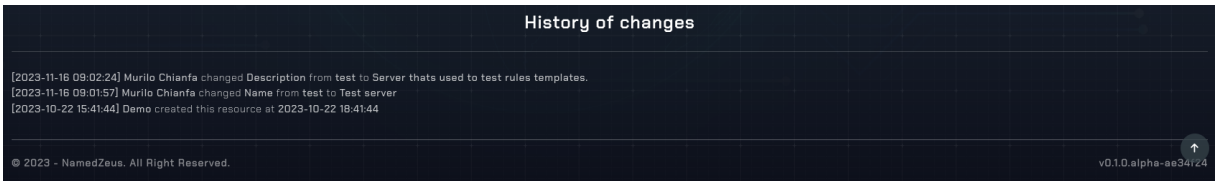
Cada registro no sistema, dispoẽ de informações de cadastro e de suas edições, a data de criação e qual usuário criou, assim como a data da última edição e por quem foi editado por último.

Figura 14 - Informações do registro

Fonte: Autoria própria, 2023.

Um histórico das alterações dos registros estará disponível na página de edição do mesmo, contendo a data da alteração, quem alterou e do que em qual campo, para o que.

Figura 15 - Histórico de alterações



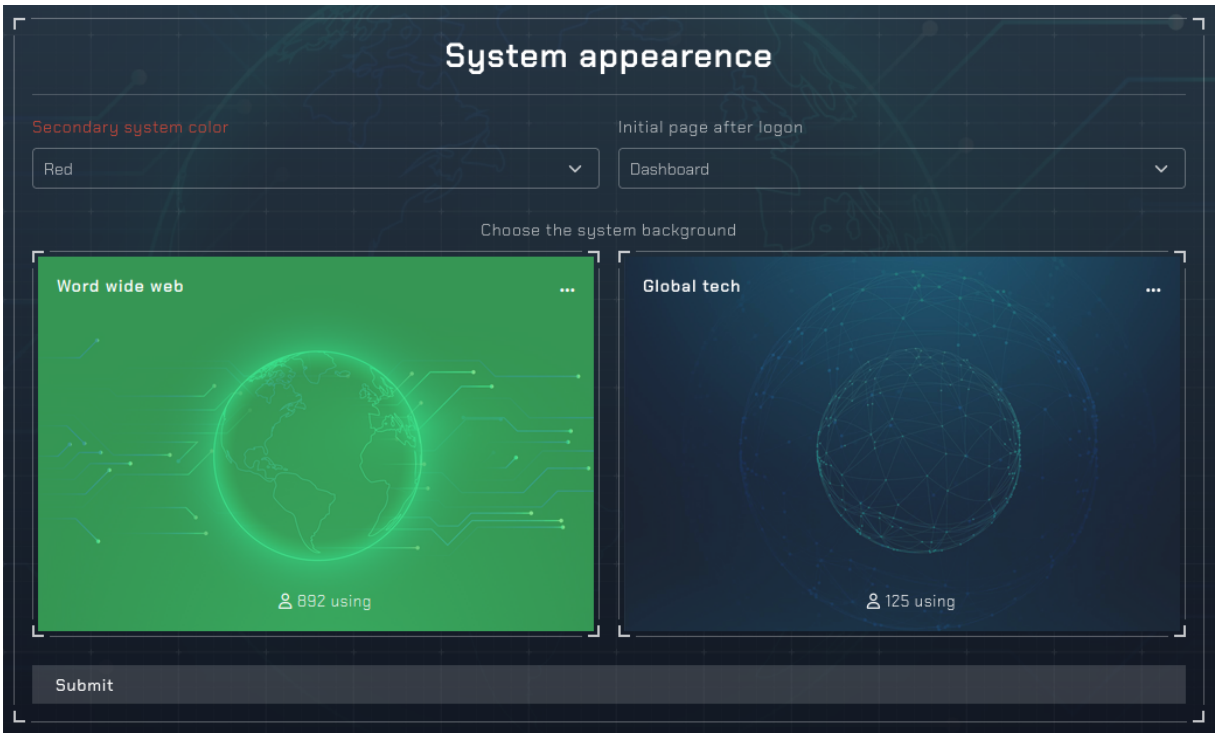
Fonte: Autoria própria, 2023.

4.3 Customização do sistema

O sistema por padrão inicia com a configuração abaixo de personalização, mas o mesmo pode ser alterado para de acordo com a preferência de cada usuário.

A coloração, a página inicial após realizar login e a imagem de fundo do sistema podem ser customizados na página de perfil do usuário.

Figura 16 - Histórico de alterações



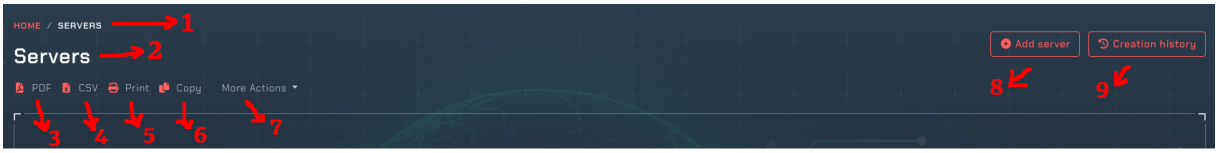
Fonte: Autoria própria, 2023.

4.4 Listagem de registros

4.4.1 Opções das listagens

Todas as listas de registros possuem algumas opções por padrão.

Figura 17 - Opções das listagens



Fonte: Autoria própria, 2023.

- **1 –** Informações do caminho atual no sistema.
- **3 –** Botão para criar um relatório em PDF dos registros.
- **4 –** Botão para criar um relatório em CSV dos registros.
- **5 –** Botão para criar um relatório dos registros adaptado para impressão.
- **6 –** Botão para copiar os registros da tabela para a área de transferência.
- **7 –** Botão com outras opções, geralmente para realizar tarefas em massa.
- **8 –** Botão para ir para a página de adição de registros.
- **9 –** Botão para visualizar o histórico dos registros cadastrados anteriormente.

4.4.2 Relatório de registros em PDF

Figura 18 - PDF de usuários

Users

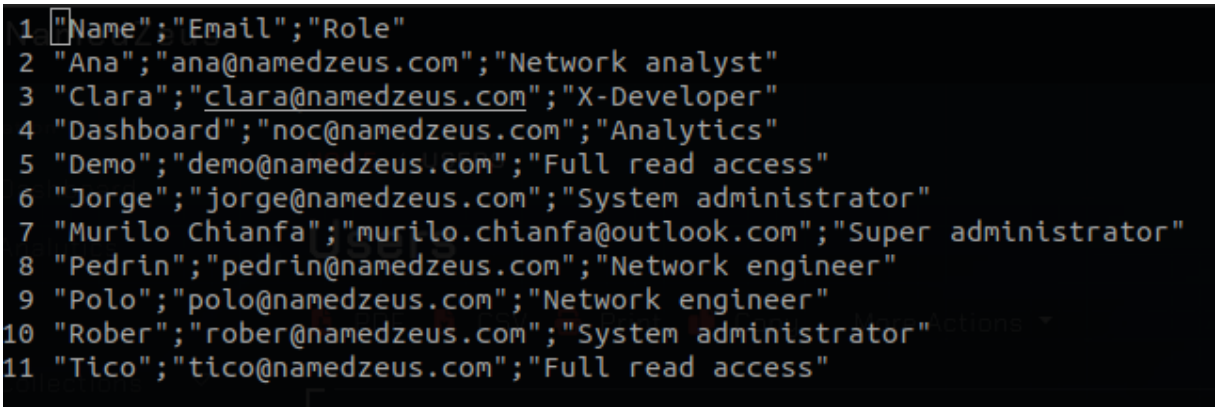
Name	Email	Role
Ana	ana@namedzeus.com	Network analyst
Clara	clara@namedzeus.com	X-Developer
Dashboard	noc@namedzeus.com	Analytics
Demo	demo@namedzeus.com	Full read access
Jorge	jorge@namedzeus.com	System administrator
Murilo Chianfa	murilo.chianfa@outlook.com	Super administrator
Pedrin	pedrin@namedzeus.com	Network engineer
Polo	polo@namedzeus.com	Network engineer
Rober	rober@namedzeus.com	System administrator
Tico	tico@namedzeus.com	Full read access

Fonte: Autoria própria, 2023.

4.4.3 Relatório de registros em CSV

Exemplo de um relatório em **CSV** do registro de usuários:

Figura 19 - CSV de usuários



```
"Name";"Email";"Role"
"Ana";"ana@namedzeus.com";"Network analyst"
"Clara";"clara@namedzeus.com";"X-Developer"
"Dashboard";"noc@namedzeus.com";"Analytics"
"Demo";"demo@namedzeus.com";"Full read access"
"Jorge";"jorge@namedzeus.com";"System administrator"
"Murilo Chianfa";"murilo.chianfa@outlook.com";"Super administrator"
"Pedrin";"pedrin@namedzeus.com";"Network engineer"
"Polo";"polo@namedzeus.com";"Network engineer"
"Rober";"rober@namedzeus.com";"System administrator"
"Tico";"tico@namedzeus.com";"Full read access"
```

Fonte: Autoria própria, 2023.

4.4.4 Relatório de registros impresso

Exemplo de um relatório impresso do registro de usuários:

Figura 20 - Impressão de usuários

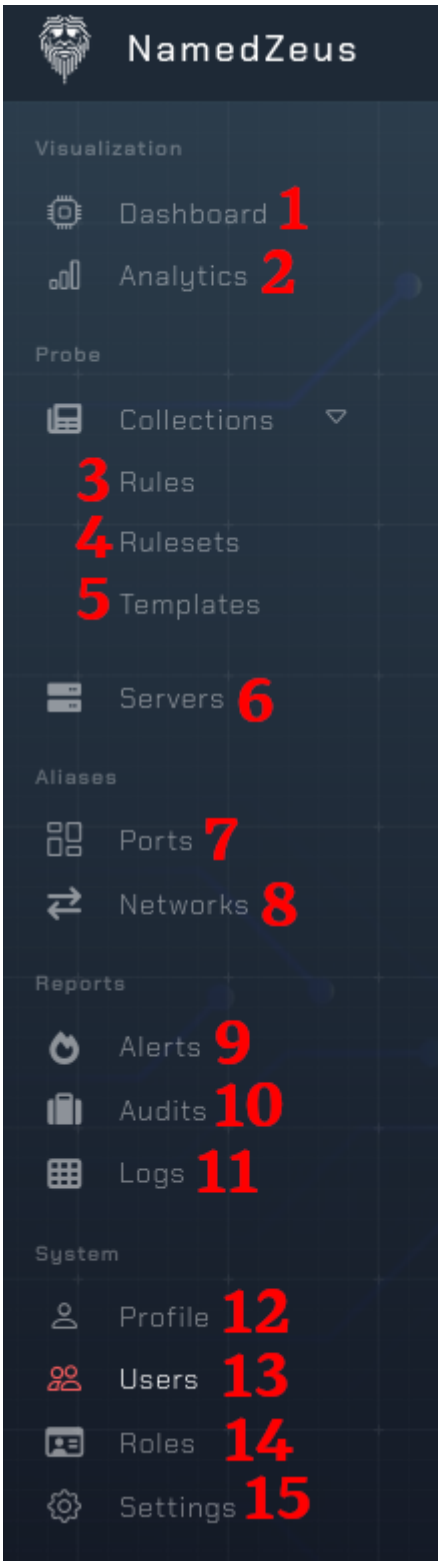
Users

Name	Email	Role
Ana	ana@namedzeus.com	Network analyst
Clara	clara@namedzeus.com	X-Developer
Dashboard	noc@namedzeus.com	Analytics
Demo	demo@namedzeus.com	Full read access
Jorge	jorge@namedzeus.com	System administrator
Murilo Chianfa	murilo.chianfa@outlook.com	Super administrator
Pedrin	pedrin@namedzeus.com	Network engineer
Polo	polo@namedzeus.com	Network engineer
Rober	rober@namedzeus.com	System administrator
Tico	tico@namedzeus.com	Full read access

Fonte: Autoria própria, 2023.

5 MENUS DO SISTEMA

Figura 21 - Menus do sistema

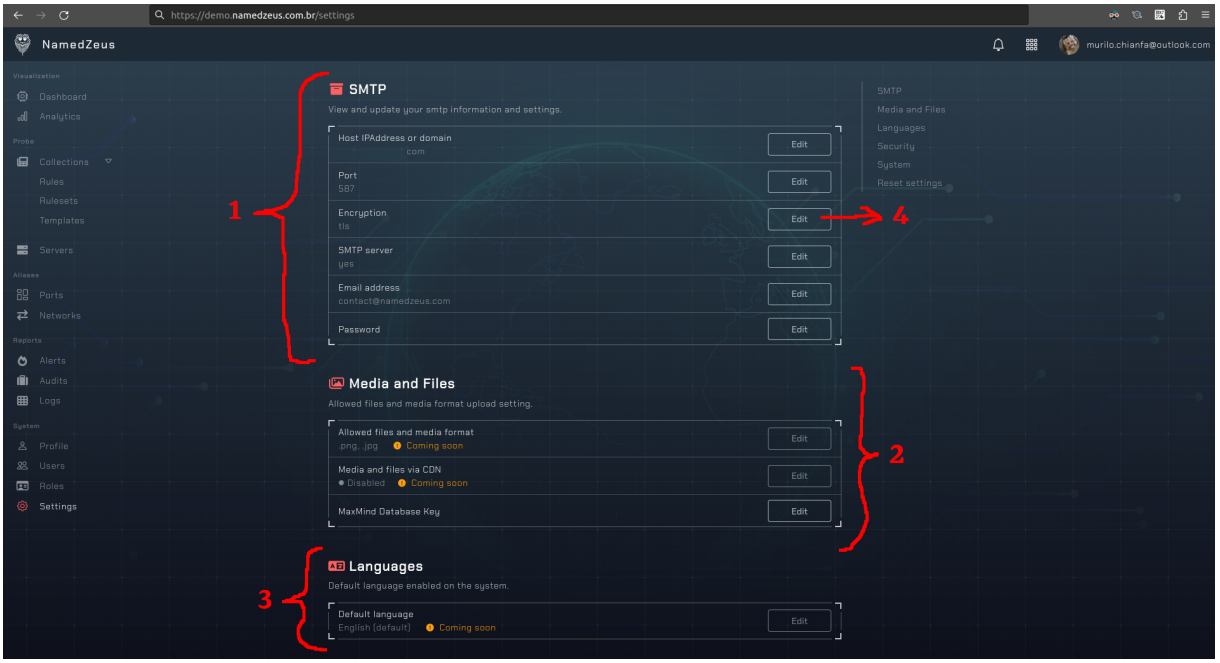


Fonte: Autoria própria, 2023.

- **1 –** Dashboard principal do sistema.
- **2 –** Dashboard de análises das informações.
- **3 –** Menu de gerência de regras e políticas de rede.
- **4 –** Menu de gerência dos conjuntos de regras.
- **5 –** Menu dos templates de regras e conjuntos de regras.
- **6 –** Menu de gerência dos servidores.
- **7 –** Menu de gerência dos apelidos de portas e grupos de portas.
- **8 –** Menu de gerência dos apelidos de redes e grupos de redes.
- **9 –** Menu de relatórios de alertas do sistema.
- **10 –** Menu de auditoria das ações do sistema.
- **11 –** Menu de visualização dos logs do sistema.
- **12 –** Página do perfil da conta de um usuário.
- **13 –** Menu de gerência dos usuários do sistema.
- **14 –** Menu de gerência dos perfis de acesso ao sistema.
- **15 –** Página de configurações do sistema.

5.1 Configurações

Figura 22 - Menu de configurações



Fonte: Autoria própria, 2023.

- **1 –** Configurações de SMTP do sistema.
- **2 –** Configurações de mídia do sistema.
- **3 –** Configurações de linguagem padrão do sistema.
- **4 –** Botão para editar uma única configuração.

Nesta tela, o administrador do sistema pode gerenciar as configurações gerais do sistema, como SMTP para envio de email, controle de mídia e linguagens disponíveis para seus usuários.

Na configuração de SMTP, o administrador, deverá fornecer os dados do servidor de SMTP de sua hospedagem de email, no meu caso utilizo a hostinger para isso, assim fornecendo seu endereço, porta e protocolo de conexão, também é necessário fornecer uma conta de usuário para validar a autenticidade dos dados cadastrais.

Para as mídias, terá a opção de escolher o formato de mídia em que os usuários poderão realizar o upload de seus avatares, por padrão, as mais comuns já serão liberadas, PNG e JPG. É altamente recomendado deixar somente estas duas.

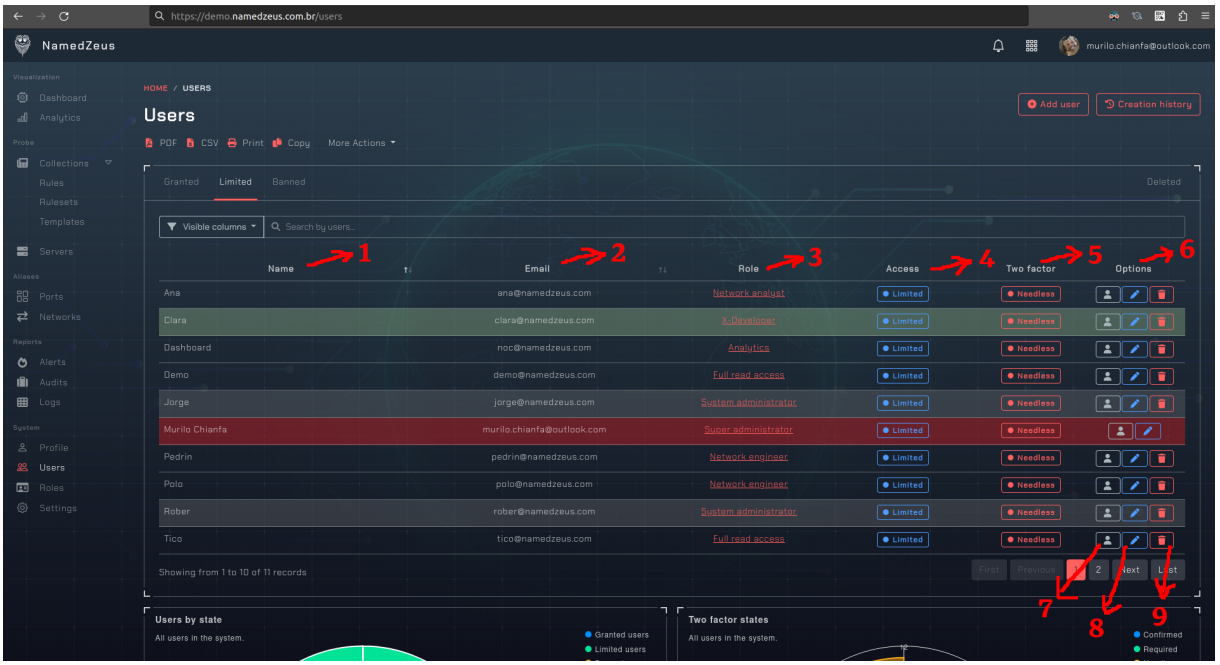
Será possível escolher desabilitar o uso de CDNs para a entrega do conteúdo estático do sistema, assim possibilitando seu uso de forma offline (sem comunicação com a internet), os usuário poderão acessar o sistema sem nenhum problema pela intranet, sem necessidade de se comunicar com qualquer endereço no exterior.

Quanto às linguagens do sistema, a princípio, será possível somente escolher o inglês, para que futuramente o sistema tenha suporte à múltiplas linguagens, assim podendo ser vendido em diversos países, tendo em vista que será um sistema autônomo digital online para a world wide web.

5.2 Listagem de usuários

Aqui também podemos adicionar novos usuários, editar os existentes ou até mesmo excluí-los ou bani-los.

Figura 23 - Menu de usuários



Fonte: Autoria própria, 2023.

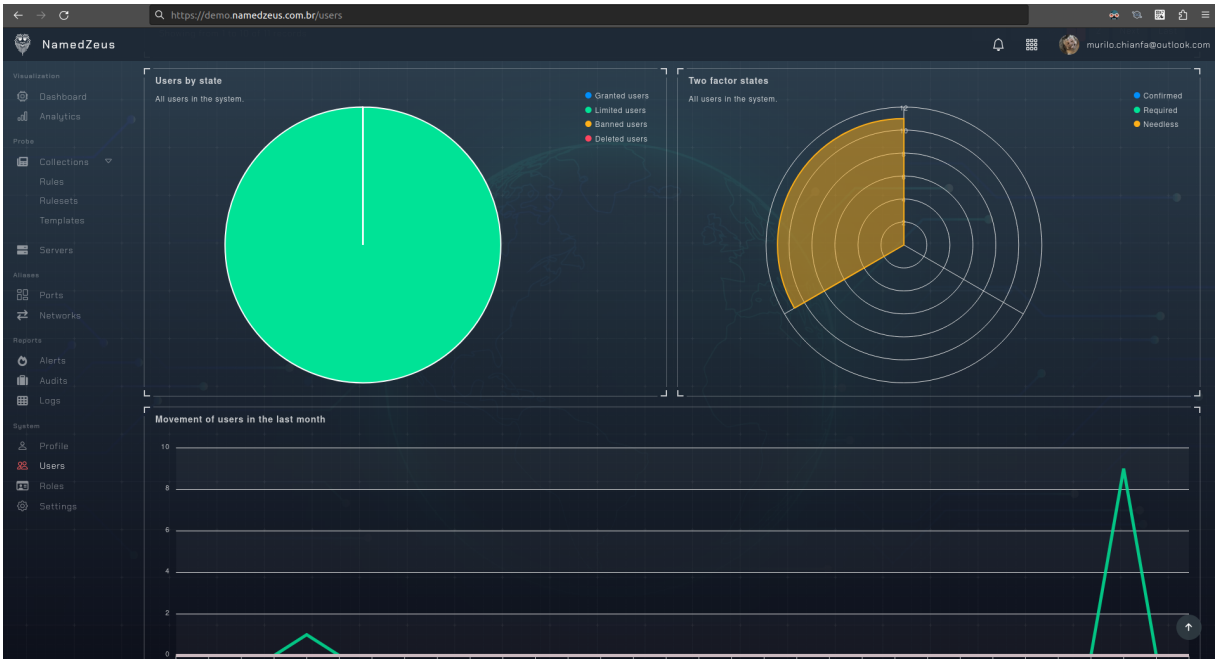
- **1 –** Campo de nome da listagem de usuários.
- **2 –** Campo de email na listagem de usuários.
- **3 –** Campo de função do usuário no sistema.
- **4 –** Campo de nível de acesso ao acesso do usuário.
- **5 –** Campo para ver se o usuário tem o segundo fator de autenticação habilitado e configurado corretamente.
- **6 –** Campo de opções para realizar em um usuário específico.
- **7 –** Botão para visualizar o perfil de um usuário.
- **8 –** Botão para editar um usuário.
- **9 –** Botão para banir um usuário do sistema.

Nessa tela é possível visualizar todos os usuários cadastrados no sistema, eles podem ser divididos em 4 categorias:

- **Granted**: Usuários que confirmaram o email e estão com o segundo fator de autenticação configurado em sua conta.
- **Limited**: Usuários que ainda não confirmaram sua conta ou ainda não ativaram o segundo fator de autenticação, assim, tendo acesso limitado aos recursos do sistema.
- **Banned**: Usuários cujo tempo hábil configurado para sua conta expirou ou tiveram seu acesso removido pelo administrador do sistema.
- Deleted: Usuários que faziam parte do sistema, agora sem acesso mas não excluídos do sistema para podermos manter os logs de auditoria.

Os gráficos na parte inferior da listagem, ajuda na visualização do estado atual dos usuários do sistema, ajuda particularmente quando o sistema possui muitos usuários simultâneos.

Figura 24 - Gráfico de usuários



Fonte: Autoria própria, 2023.

5.3 Adição de usuários

Figura 25 - Adição de usuários

Fonte: Autoria própria, 2023.

- **1 –** Campo de nome do usuário.
- **2 –** Campo de email do usuários.
- **3 –** Campo de seleção do formato de exibição das datas no sistema.
- **4 –** Campo de seleção do formato de exibição dos horários no sistema.
- **5 –** Campo de senha do usuário.
- **6 –** Campo de confirmação de senha do usuário.
- **7 –** Campo de descrição do perfil do usuário.
- **8 –** Campo para escolher o perfil de acesso do usuário no sistema.
- **9 –** Campo de seleção para o fuso-horário do usuário.
- **10 –** Campo de seleção de linguagem do sistema.
- **11 –** Opção para pedir que o usuário confirme o email no primeiro acesso.
- **12 –** Opção para pedir que o usuário troque a senha no primeiro acesso.
- **13 –** Opção para pedir que o usuário configure o 2FA no primeiro acesso.
- **14 –** Opção para alertar o usuário de tentativas de acesso incorretas.
- **15 –** Opção para alertar o administrador do sistema quando o usuário entrar.
- **16 –** Opção para selecionar o período em que o usuário será ativo.

Nessa tela, é possível adicionar novos usuários ao sistema, a senha deve ser muito segura, com algumas regras de criação, como por exemplo, conter no mínimo 56 caracteres entre letras maiúsculas e minúsculas, números e símbolos dentro da norma UTF-8.

A parte de edição do usuário é praticamente idêntica.

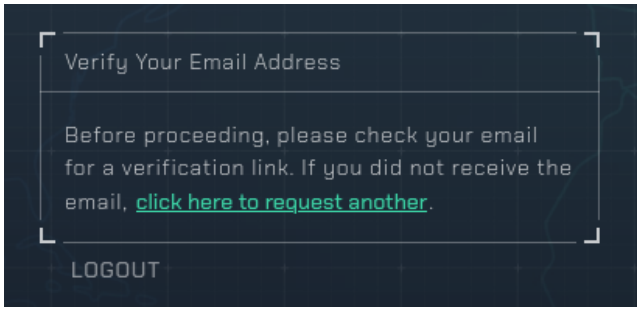
O cargo deste novo usuário também pode ser escolhido, bem como algumas outras opções para a conta, como o formato da data e hora, a linguagem e o timezone padrão e algumas opções para a validação da conta, como solicitar que o usuário confirme o email antes de realizar o primeiro acesso, trocar a senha ao realizar o primeiro acesso ou obrigá-lo a configurar um segundo fator de autenticação.

5.4 Email de confirmação

Na primeira vez que o usuário entrar no sistema, caso seja necessário, ele precisará confirmar seu endereço de email.

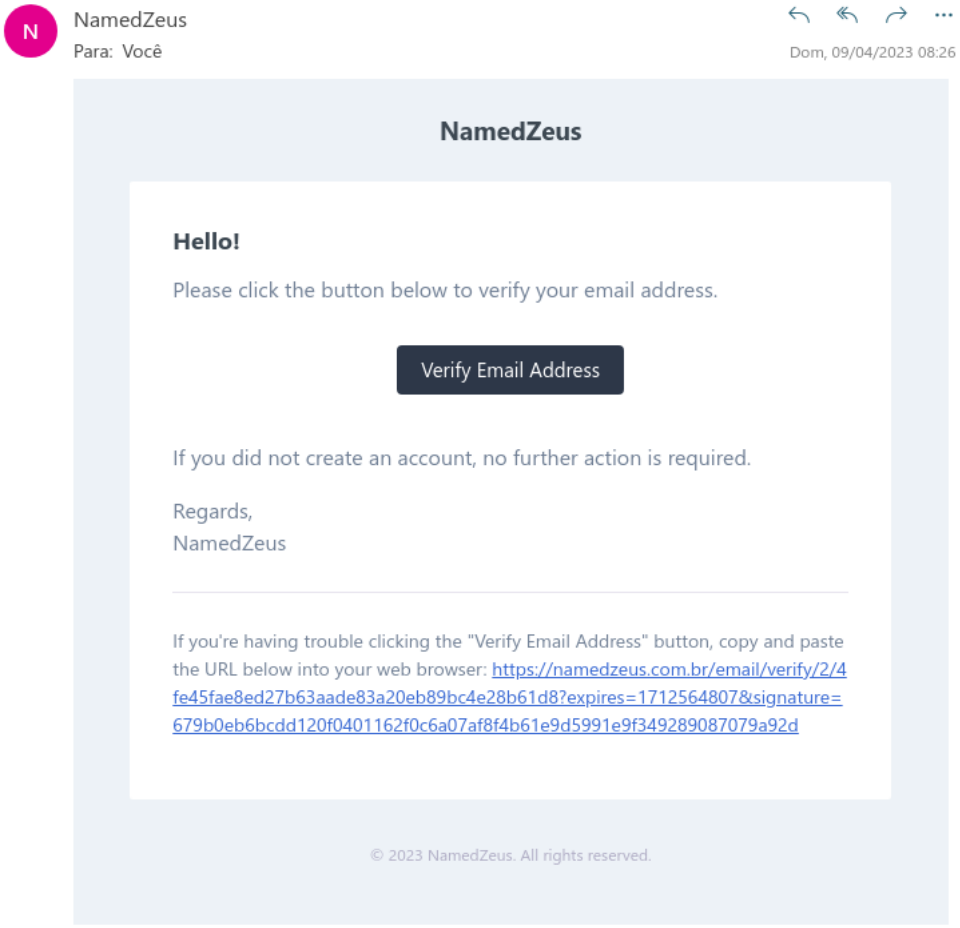
Um email que será enviado ao destinatário, ao clicar no botão ou no link, o usuário será redirecionado de volta para o sistema para trocar sua senha no primeiro acesso, assim como ao solicitar o reset de senha na tela de login.

Figura 26 - Confirmação de email



Fonte: Autoria própria, 2023.

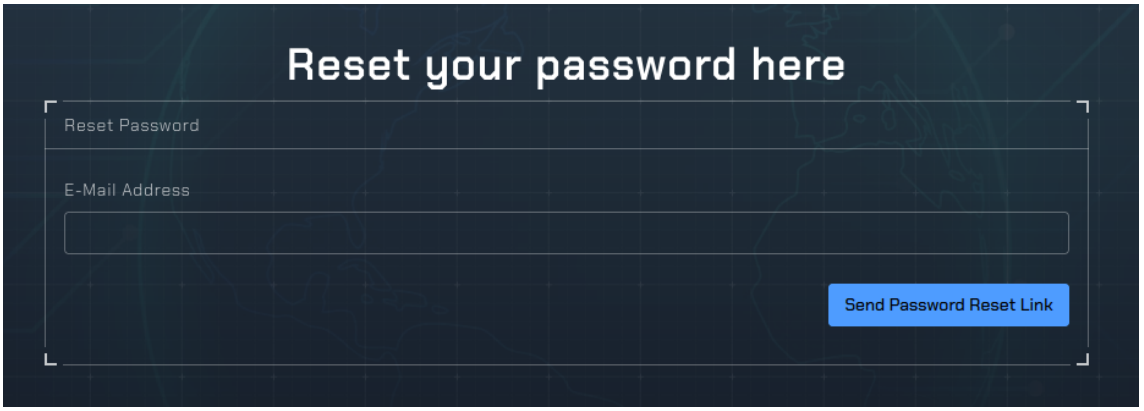
Figura 27 - Email de confirmação



Fonte: Autoria própria, 2023.

Um pedido de alteração de senha pode ser realizado clicando no link de esqueci minha senha localizado na tela de login do sistema.

Figura 28 - Pedido de troca de senha

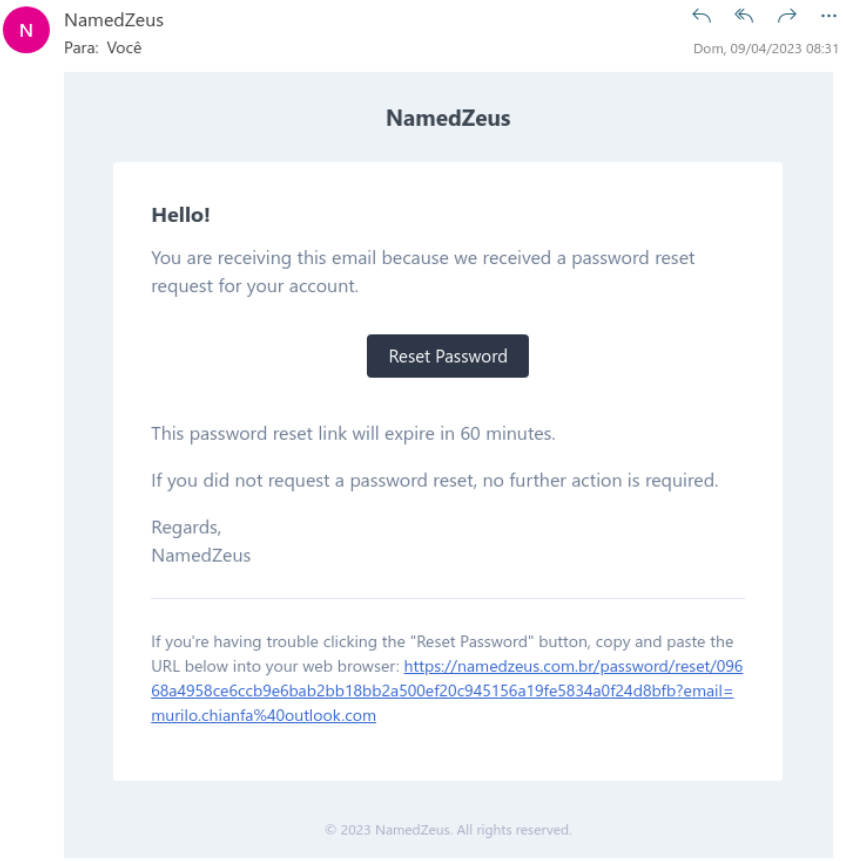


Fonte: Autoria própria, 2023.

5.5 Email de reset de senha

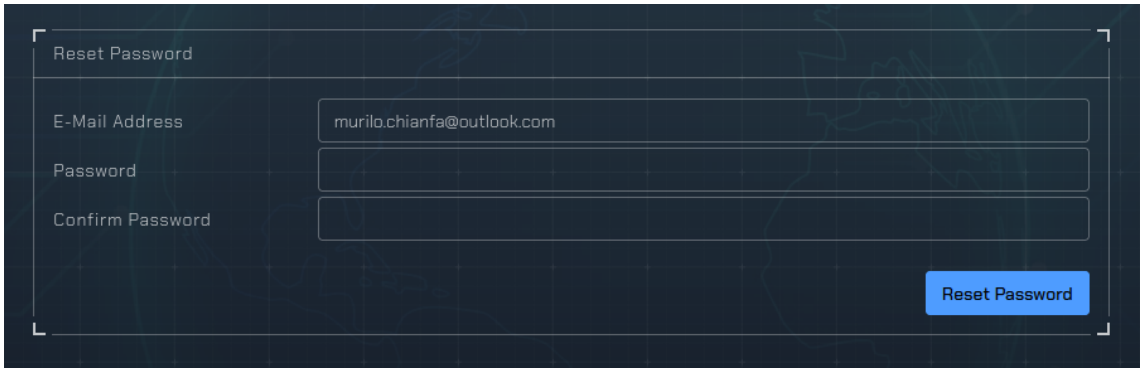
Este será o email que será enviado ao destinatário, ao clicar no botão ou no link, o usuário será redirecionado de volta para o sistema para trocar sua senha no primeiro acesso.

Figura 29 - Email de reset de senha



Fonte: Autoria própria, 2023.

Figura 30 Troca de senha



Fonte: Autoria própria, 2023.

5.6 Vínculo 2FA à nova conta

Depois de efetuar o reset de senha, será necessário vincular um segundo fator de autenticação a conta, o google autenticador pode ser utilizado para isso.

Figura 31 - Adição do 2FA

Fonte: Autoria própria, 2023.

5.7 Listagem de cargos

Figura 32 - Listagem de cargos

Fonte: Autoria própria, 2023.

Nessa tela será possível visualizar a lista de todos os cargos baseado em RBAC disponíveis no sistema, com informações de nome do cargo, quantos usuários utilizam o cargo e quantas permissões ele possui.

Caso o usuário tenha permissão, também temos aqui a opção de adicionar mais cargos, editar um cargo já existente ou até mesmo excluir um cargo, o que acarretaria na exclusão ou migração do cargo de todos os usuários que se utilizam do mesmo.

Figura 33 - PDF de cargos

Roles

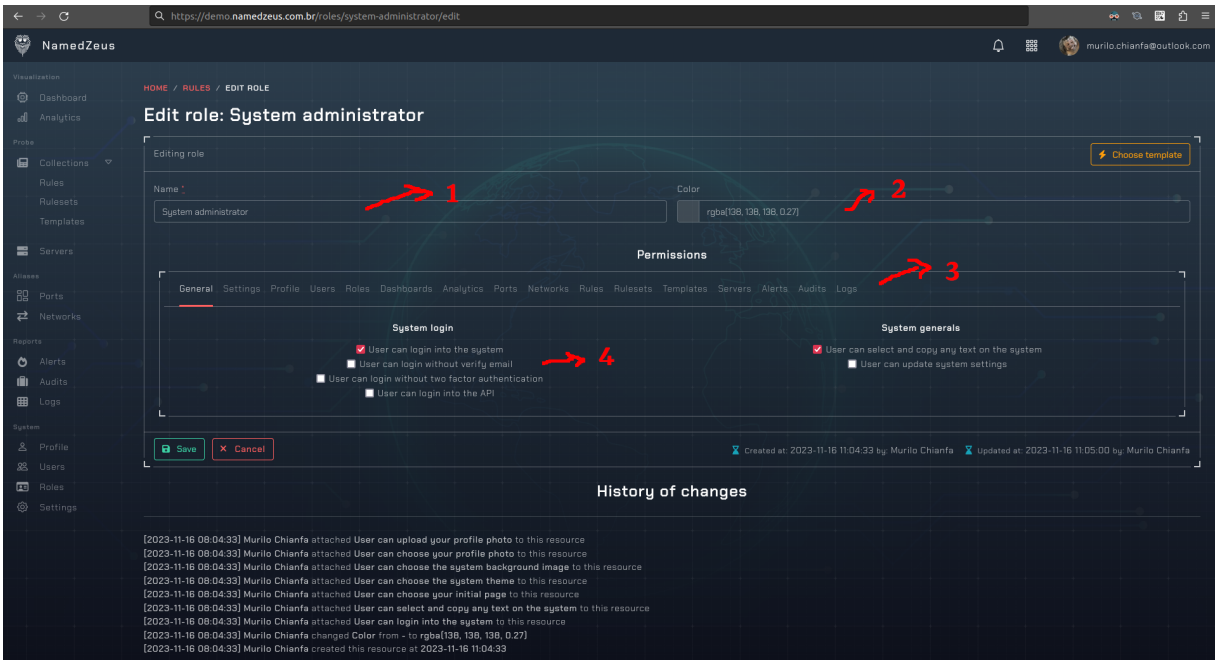
Name	Users	Permissions
Read only	1	1
Super administrator	1	33

Fonte: Autoria própria, 2023.

5.8 Edição de cargos

Aqui temos uma série de permissões divididas por grupos de ações para serem vinculadas aos cargos, o usuário que fizer parte do cargo, herdará todas as suas permissões.

Figura 34 - Edição de cargos



Fonte: Autoria própria, 2023.

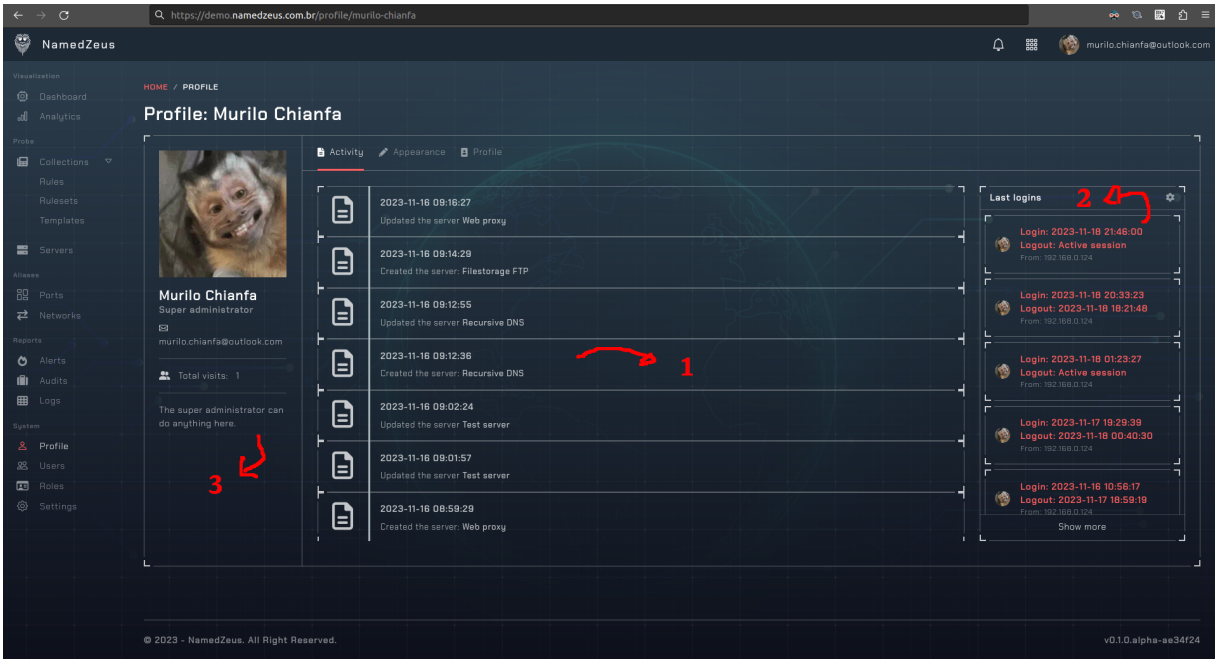
- **1 –** Campo de nome do cargo.
- **2 –** Campo para escolher uma cor para o cargo.
- **3 –** Tipos de permissões disponíveis para o cargo.
- **4 –** Botões de escolha das permissões do cargo.

O cargo de super administrador com todas as permissões e o cargo de read only com permissões restritas, já serão criados por padrão pelo bootstrap do sistema na instalação, porém alguns templates de permissões serão disponibilizados para ajudar na escolha e entendimento de uso do mesmo.

5.9 Perfil do usuário

Para poder acessar essa página, o usuário precisa ter a permissão de visualização, as informações de atividade de logins possuem permissões separadas, para o caso de segregação de interfaces.

Figura 35 - Perfil do usuário

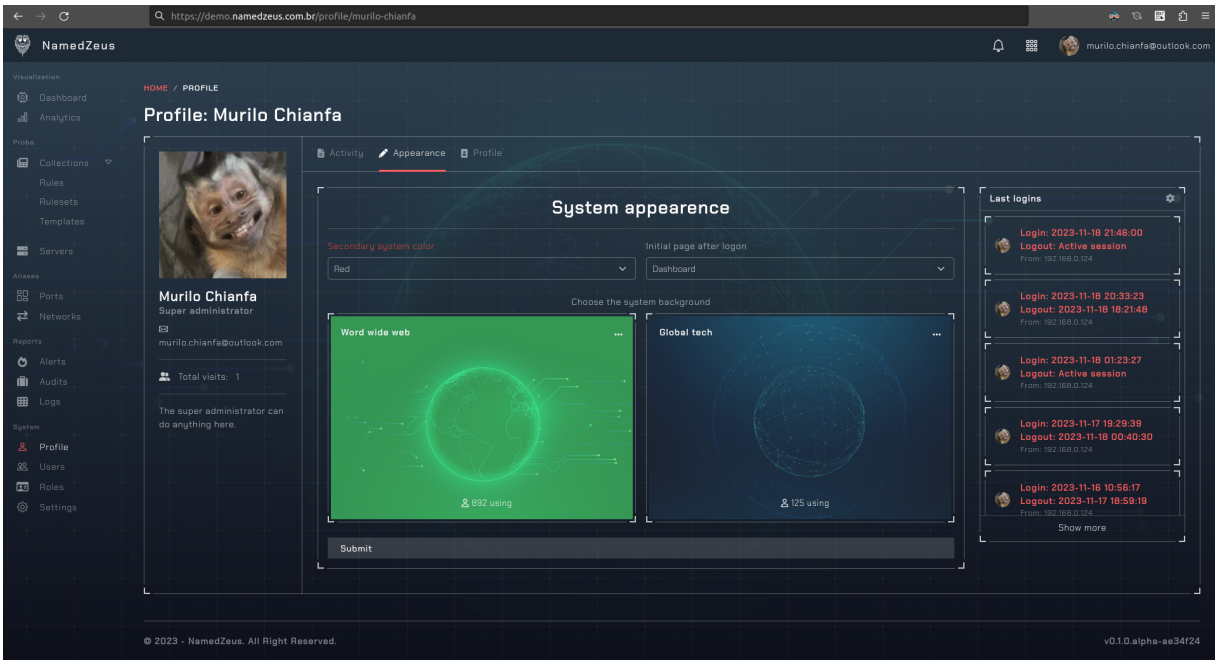


Fonte: Autoria própria, 2023.

- **1 –** Dentro do perfil de cada usuário, podemos ver seus registros de atividade no sistema, todas as suas ações serão registradas para manter possível auditoria futura.
- **2 –** Registros de logins e logouts também serão monitorados, horário de entrada, horário de saída e endereço de IP utilizado na hora do login também serão mantidos.
- **3 –** Algumas outras informações pertinentes ao usuário serão mostradas ao lado esquerdo, abaixo de sua foto de perfil, como o cargo em que pertence, seu nome, endereço de email, total de visitas e uma breve descrição.

5.10 Preferências do usuário

Figura 36 - Preferências do usuário



Fonte: Autoria própria, 2023.

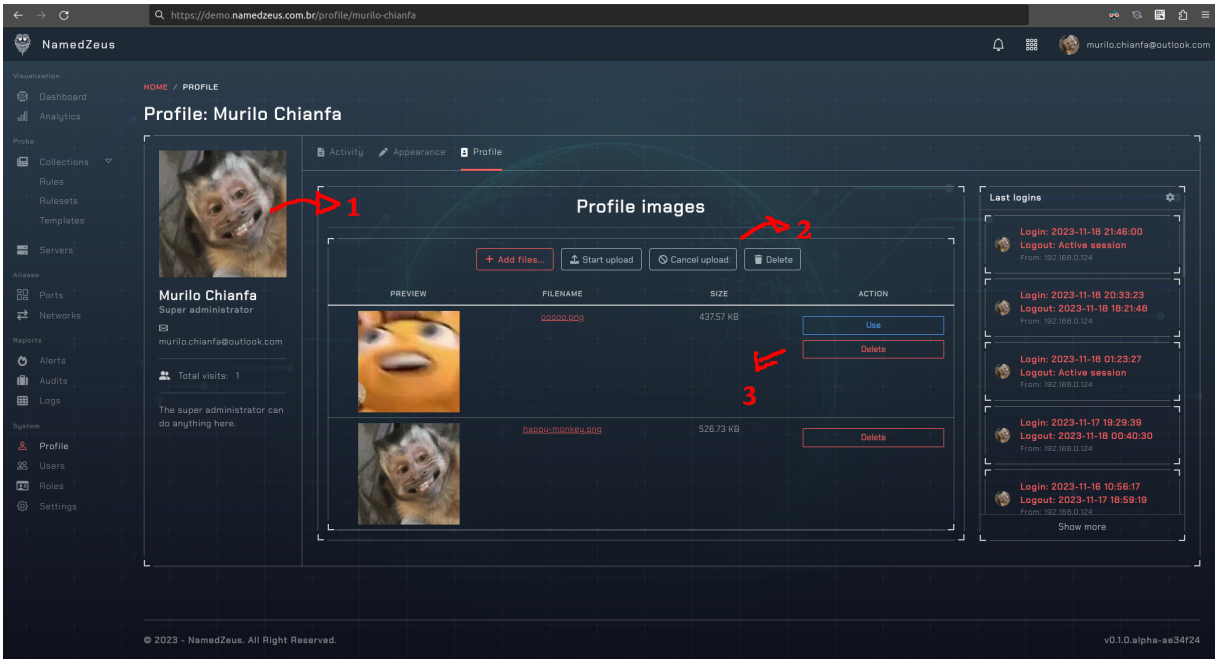
Na segunda aba do perfil do usuário, é possível alterar algumas preferências relacionadas à aparência do sistema. Assim como mencionado na descrição da dashboard geral, o usuário poderá escolher sua página de início após realizar login, a cor de exibição do tema e a imagem fundo do sistema.

Nem todas as páginas do sistema são possíveis para escolha de página inicial, apenas algumas pré-cadastradas, já para as cores tema do sistema, estarão disponíveis:

- Vermelho
- Rosa
- Amarelo
- Azul
- Verde
- Laranja

5.11 Envio de imagem do usuário

Figura 37 - Avatar do usuário



Fonte: Autoria própria, 2023.

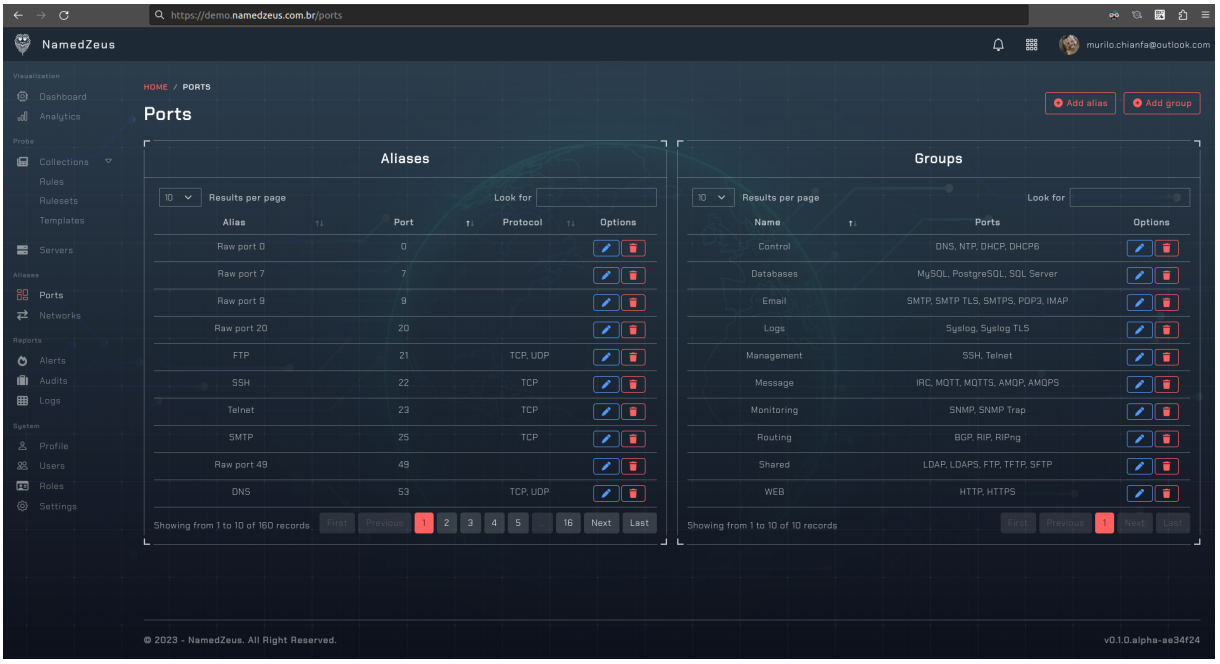
- **1 –** Pré visualização da imagem atual do usuário.
- **2 –** Botões para adição e remoção de novas imagens.
- **3 –** Botões para gerenciar as imagens existentes.

Será possível realizar o upload de imagens para a foto de perfil do usuário, um usuário só poderá escolher seus próprios avatares. Caso seja realizado o upload de mais de uma, uma lista dos arquivos recentes será mantida para o caso de o usuário querer voltar à antiga imagem, porém terá a opção de excluir caso necessário.

A lista de formatos permitidos para o upload será configurável na página de configurações de sistema pelo super administrador, por padrão será possível o upload de PNG e JPG.

5.12 Listagem de portas

Figura 38 - Listagem de portas



Fonte: Autoria própria, 2023.

Aqui na listagem de portas, podemos perceber que tem duas listas:

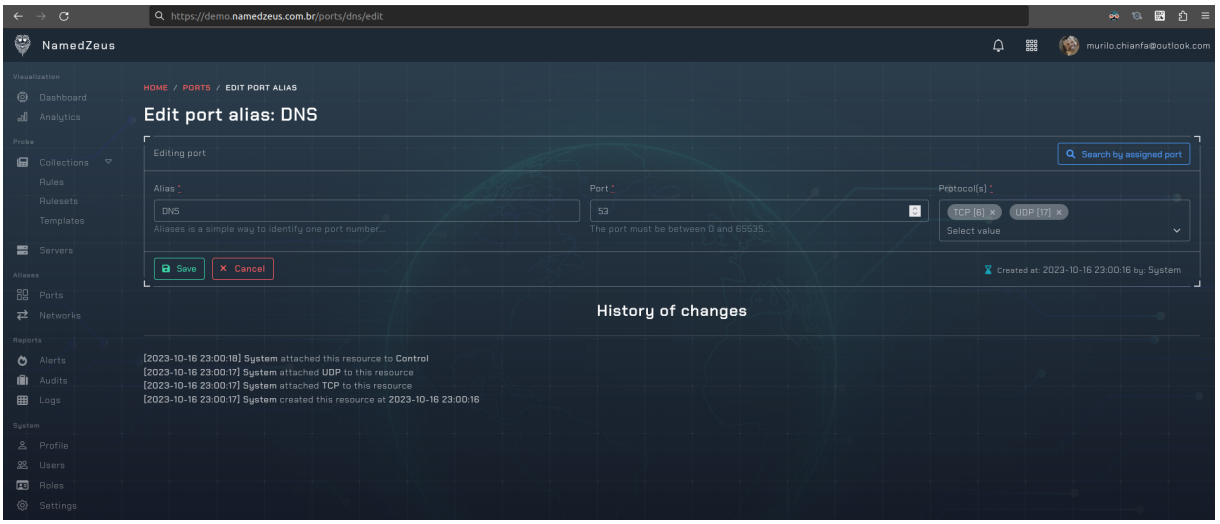
- Aliases
- Groups

Aliases aqui, se refere ao simples nome dado às portas de entrada e saída de camada 4 no modelo OSI, o usuário poderá dar o alias que quiser as portas, mas é recomendável seguir para portas que possuem uma atribuição já registrada pela IANA, seguir sua tabela de atribuições entre portas e serviços.

Por padrão no sistema já estão cadastradas as portas e grupo de portas mais comuns utilizadas nos sistemas hoje em dia, grupos estes como de portas para acesso WEB: HTTP (80) e HTTPS (443), muito utilizadas nas regras de detecção de intrusão.

5.13 Edição de portas

Figura 39 - Edição de portas



Fonte: Autoria própria, 2023.

Para a edição de um alias de porta, serão necessários o alias, o número da porta e os protocolos de camada 4 do modelo OSI (como TCP e UDP) em que será monitorado o tráfego.

Um botão de ajuda estará disponível para ajudar na descoberta de atribuições feitas pela IANA caso seja conveniente.

Todas as modificações, alterações, inclusões e adições de aliases de portas, serão auditáveis, como podemos ver na parte inferior em “History of changes”.

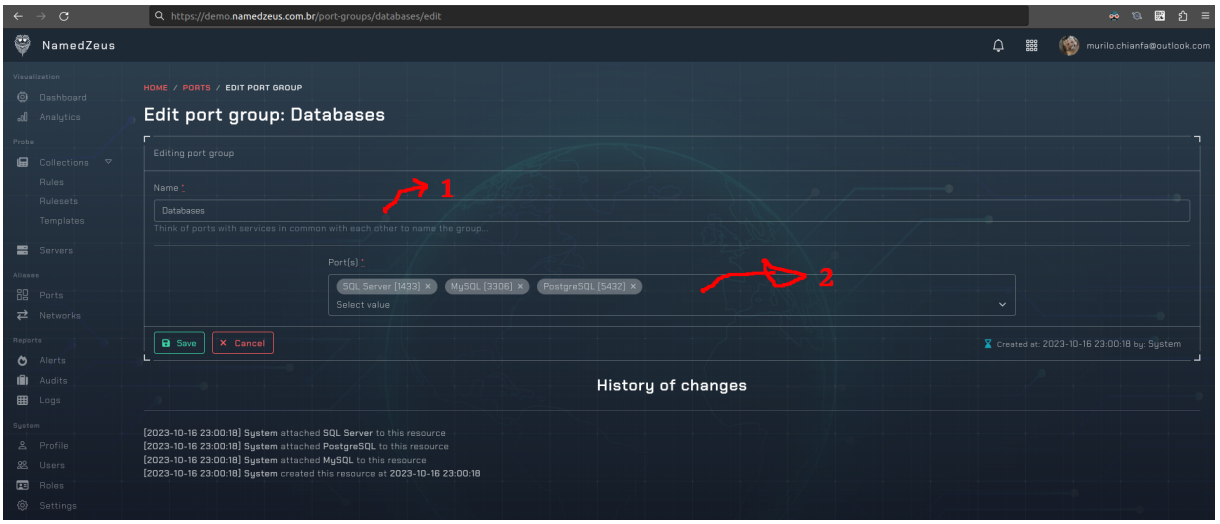
Figura 40 - Serviços para porta 80

Service Name	Port Number	Transport Protocol	Description	Assignee	Contact	Registration Date	Modification Date	Reference
http	80	tcp	World Wide Web HTTP	[IESG]	[IETF Chair]		2021-10-01	[RFC9110]
http	80	udp	World Wide Web HTTP	[IESG]	[IETF Chair]		2021-10-01	[RFC9110]
www	80	tcp	World Wide Web HTTP	[IESG]	[IETF Chair]		2021-10-01	[RFC9110]
www	80	udp	World Wide Web HTTP	[IESG]	[IETF Chair]		2021-10-01	[RFC9110]
www-http	80	tcp	World Wide Web HTTP	[Tim Berners-Lee]	[Tim Berners-Lee]			

Fonte: IANA - assignments to port 80, 2023.

5.14 Edição do grupo de portas

Figura 41 - Edição de grupo portas



Fonte: Autoria própria, 2023.

- **1 –** Campo de nome do grupo de portas.
- **2 –** Opção para atribuir as portas a um grupo de portas.

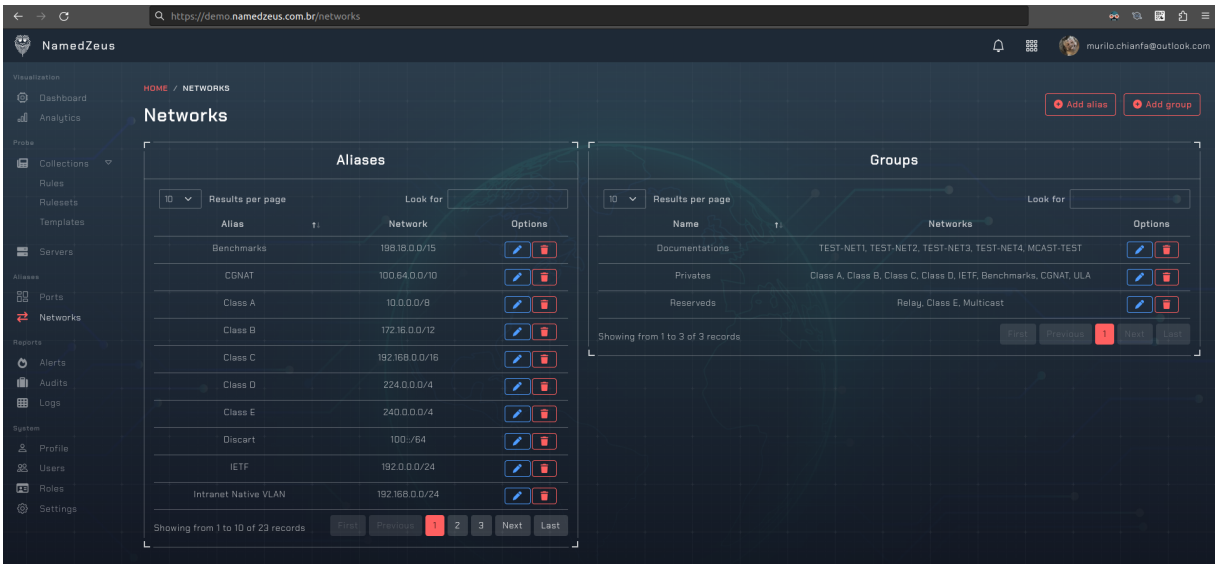
Já nos grupos de portas, podemos vincular as portas criadas anteriormente, criando assim, um agrupamento para facilitar no gerenciamento e identificação dos serviços por trás.

Por padrão alguns grupos já serão criados, grupos como portas padrões para serviços como WEB, Email, Management e monitoramento.

Todas as modificações, alterações, inclusões e adições de grupo de portas, serão auditáveis, como podemos ver na parte inferior em “History of changes”.

5.15 Listagem de networks

Figura 42 - Listagem de networks



Fonte: Autoria própria, 2023.

Aqui na listagem de networks, podemos perceber que tem duas listas:

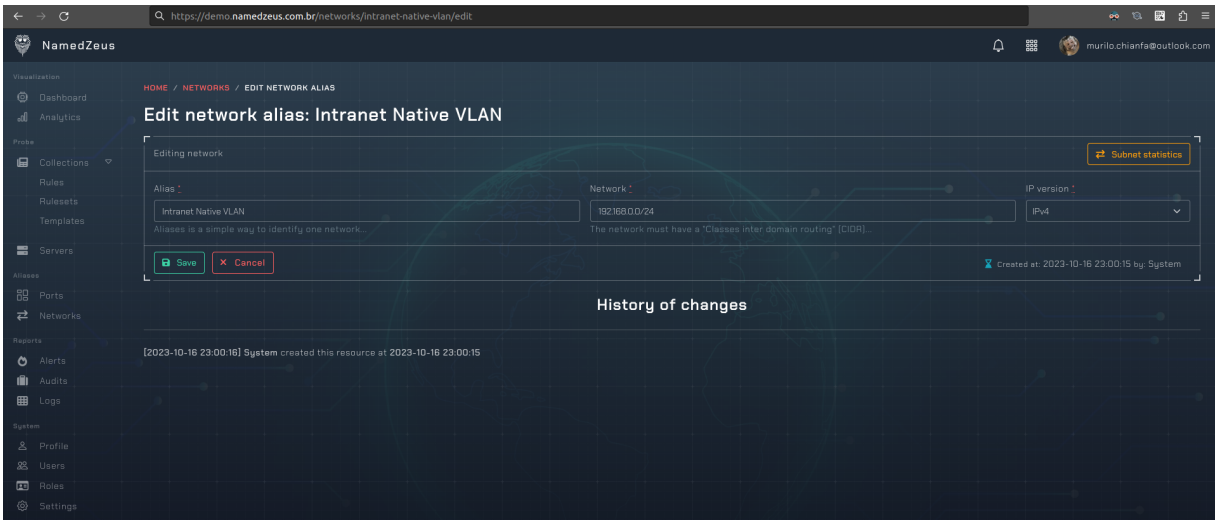
- Aliases
- Groups

Aliases aqui, se refere ao simples nome dado às subnets de entrada e saída de camada 3 no modelo OSI, o usuário poderá dar o alias que quiser as networks, mas é recomendável seguir algumas RFCs estabelecidas que possuem uma atribuição já registrada pela IANA, seguir sua tabela de atribuições é muito importante.

Por padrão no sistema já estão cadastradas as networks e grupo de networks mais comuns utilizadas nos sistemas hoje em dia, grupos estes como de networks para acesso privado, somente local: Class A (10.0.0.0/8), Class B (172.16.0.0/12), etc. muito utilizadas nas regras de detecção de intrusão.

5.16 Edição de networks

Figura 43 - Edição de networks



Fonte: Autoria própria, 2023.

Para a edição de um alias de network, serão necessários o alias, a subnet da rede e a versão do que será monitorado o tráfego. Um botão de estatísticas estará disponível para ajudar no cálculo de sub rede caso seja conveniente.

Todas as modificações, alterações, inclusões e adições de networks, serão auditáveis, como podemos ver na parte inferior em “History of changes”.

A sub rede deverá ser identificada na notação de CIDR:

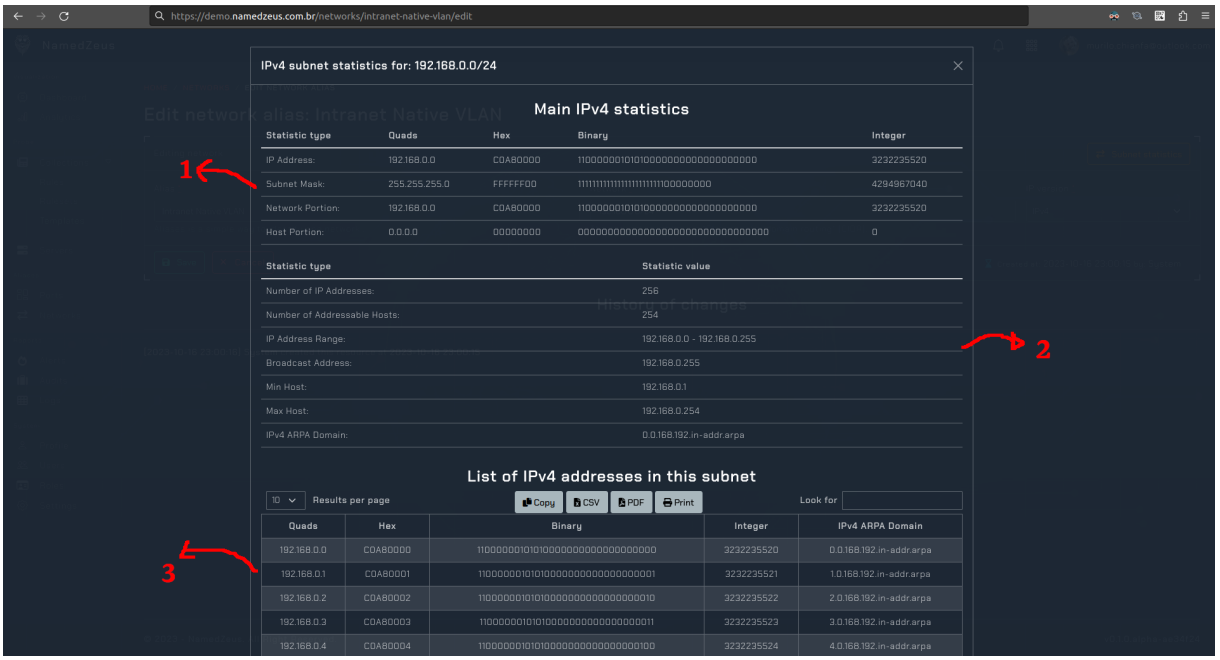
Figura 44 - Exemplo de sub redes

Subnet Mask	CIDR	Host
255.255.255.0	/24	256
255.255.255.128	/25	128
255.255.255.192	/26	64
255.255.255.224	/27	32
255.255.255.240	/28	16
255.255.255.248	/29	8
255.255.255.252	/30	4

Fonte: IANA, subnet masks, 2023.

5.17 Detalhes de network

Figura 45 - Estatísticas de sub rede



Fonte: Autoria própria, 2023.

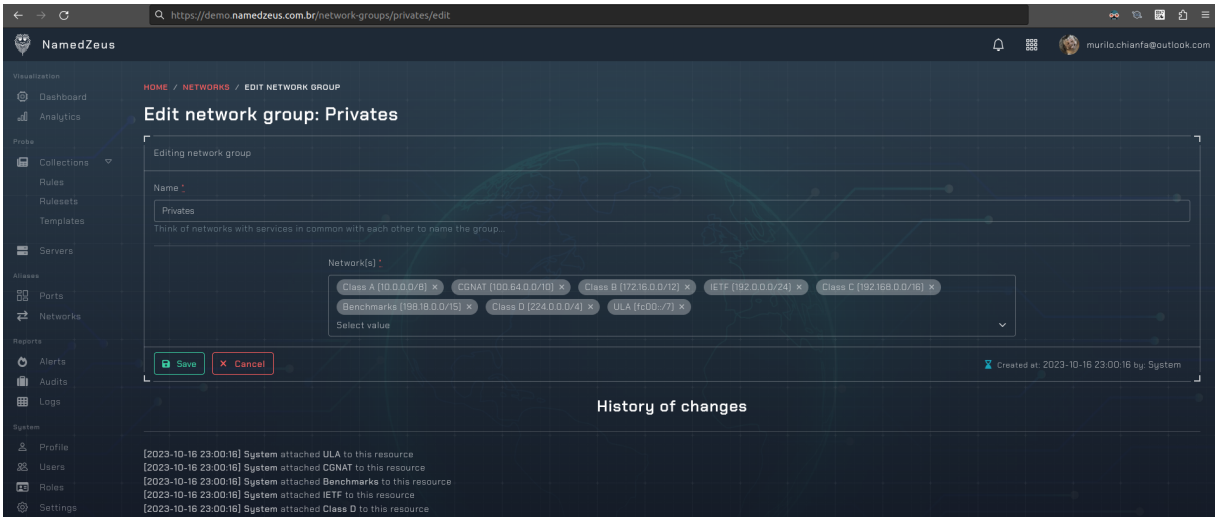
- **1 –** Campos de descrição da sub rede.
- **2 –** Cálculos da sub rede e seus limites.
- **3 –** Listagem de todos os IPs da sub rede.

Caso o usuário clique no botão de estatísticas para IPv4, um modal com todas as informações pertinentes a network digitada no campo de network será mostrado.

Todos os tipos de dados serão calculados, do binário ao inteiro, as informações mais relevantes que agilizarão no dia a dia, seria do número de IPs endereçáveis da rede, endereço de host e rede e a listagem de todos os endereços da sub rede.

5.18 Edição do grupo de networks

Figura 46 - Edição de grupo de networks



Fonte: Autoria própria, 2023.

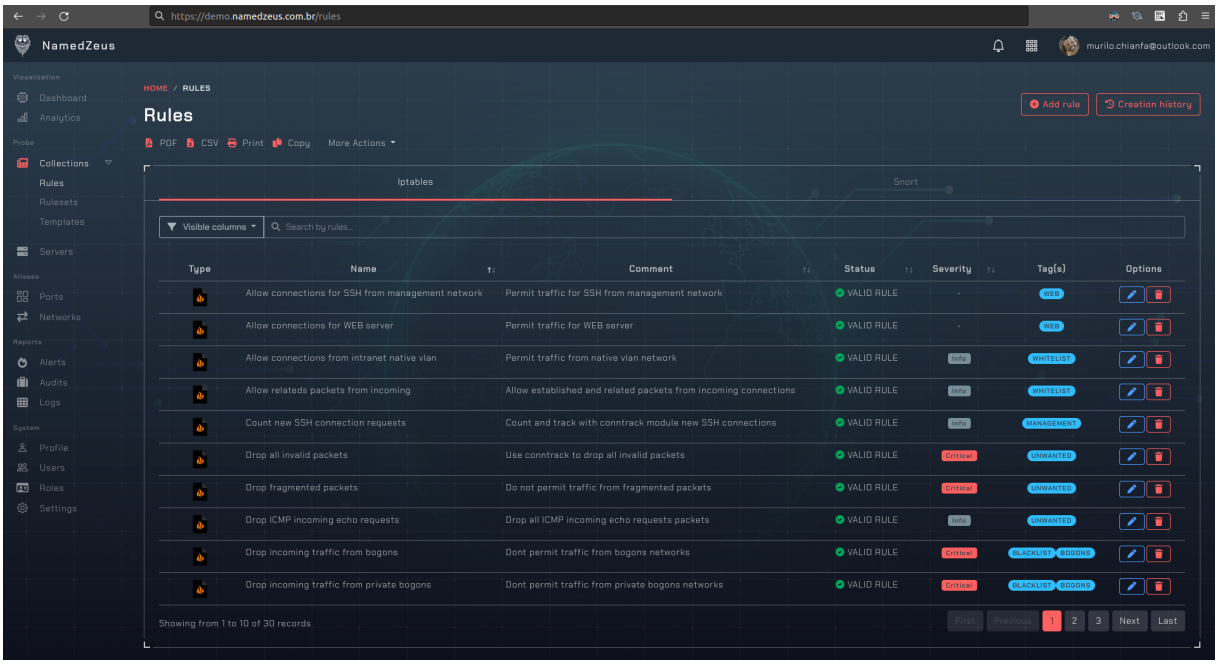
Já nos grupos de networks, podemos vincular as networks criadas anteriormente, criando assim, um agrupamento para facilitar no gerenciamento e identificação dos serviços por trás.

Por padrão alguns grupos já serão criados, grupos como portas padrões para serviços como endereços privados de rede, endereços utilizados para documentação, identificação de bogons (não delegados pela RIR) e endereços locais.

Todas as modificações, alterações, inclusões e adições de grupo de networks, serão auditáveis, como podemos ver na parte inferior em “History of changes”.

5.19 Listagem de regras

Figura 47 - Listagem de regras



Fonte: Autoria própria, 2023.

Aqui na listagem de regras, estarão dispostas as regras de detecção de intrusão, assim como algumas opções para controle de fluxo e filtragem de pacotes.

Para as regras de filtragem de pacotes e controle de fluxo, será utilizado o formato como disposto pela ferramenta IPTABLES. Um diagrama do fluxo dos pacotes de rede pode ser visto no **ANEXO A - Fluxo de pacotes no módulo de kernel NETFILTER**.

Já as regras de detecção de intrusão, será utilizado o formato das regras do SNORT, onde o sistema irá identificar o template usado e irá converter para o padrão IPTABLES via FWSNORT, onde os logs serão monitorados pelo PSAD.

Um relatório das regras disponíveis poderá ser extraído em PDF ou CSV, assim como estarão disponíveis botões para adição de novas regras e edição e deleção das regras existentes.

5.20 Edição de regras

Nessa tela é possível dar um nome e um comentário a regra, assim como escolher seu protocolo de camada 4 do modelo OSI, tags para facilitar o manuseio, restrições de portas e networks (podendo escolher os grupos também) e severidade.

Quaisquer alterações em questão da restrição dos grupos de networks e/ou portas e protocolos, a regra seja recalculada pelo sistema e aplicada em todos os servidores que a utilizam tudo de forma automática, facilitando e agilizando o dia a dia do analista de rede.

Figura 48 - Edição de regras

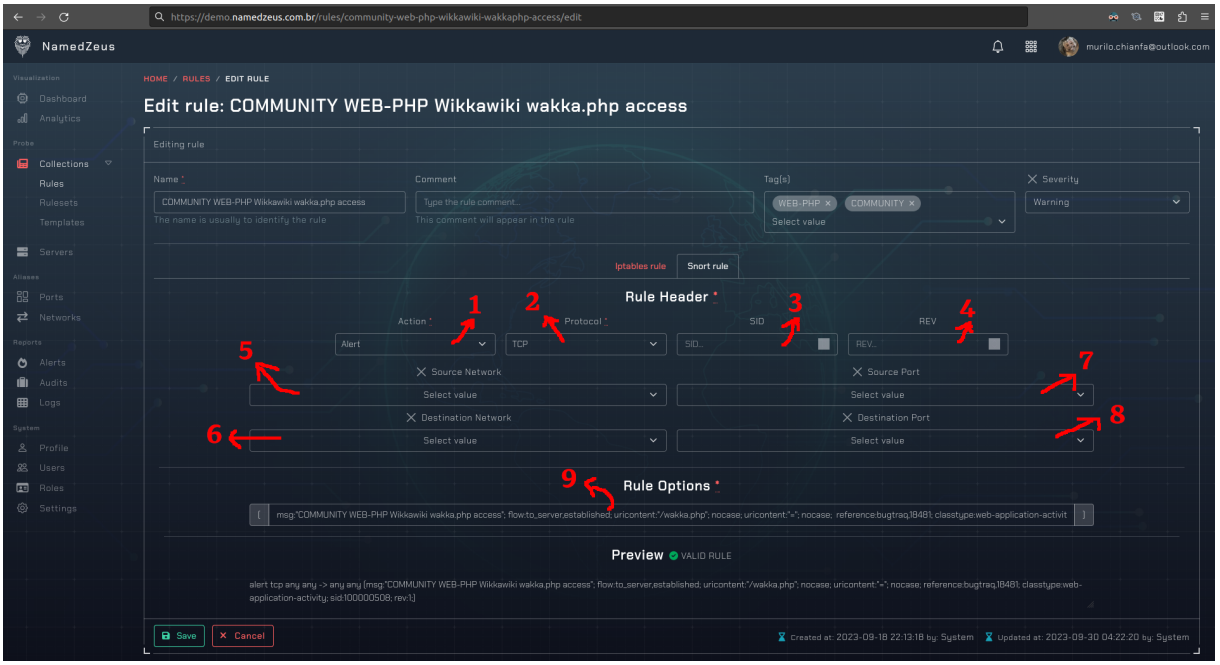
Fonte: Autoria própria, 2023.

- **1 –** Campo de nome da regra.
- **2 –** Campo comentário da regra.
- **3 –** Campo de seleção das tags da regra.
- **4 –** Campo de seleção da severidade da regra.
- **5 –** Campo de seleção de portas ou grupo de portas da regra.
- **6 –** Campos de seleção da direção da porta na regra.
- **7 –** Campo para marcar a porta como volátil.
- **8 –** Campos de seleção da direção de network da regra.
- **9 –** Campo de seleção da network ou grupo de networks da regra.

- **10 –** Campo de seleção do protocolo da regra.
- **11 –** Campo de seleção da tabela alvo da regra.
- **12 –** Campo de seleção da corrente da regra.
- **13 –** Opção para marcar a regra como pulo para uma coleção de regras.
- **14 –** Campo para selecionar a ação de caso na regra.
- **15 –** Campo para selecionar o tipo de log da regra.
- **16 –** Opção para ignorar o pulo da regra.
- **17 –** Campo para inserir manualmente mais opções do que a disponível.
- **18 –** Texto com o preview da regra montada em tempo real.

A outra opção de criação de regras, é a regra do tipo “Snort”, um exemplo do template de regras do estilo snort pode ser vista no **ANEXO C - Anatomia de regras baseadas em SNORT**.

Figura 49 - Edição de regras snort



Fonte: Autoria própria, 2023.

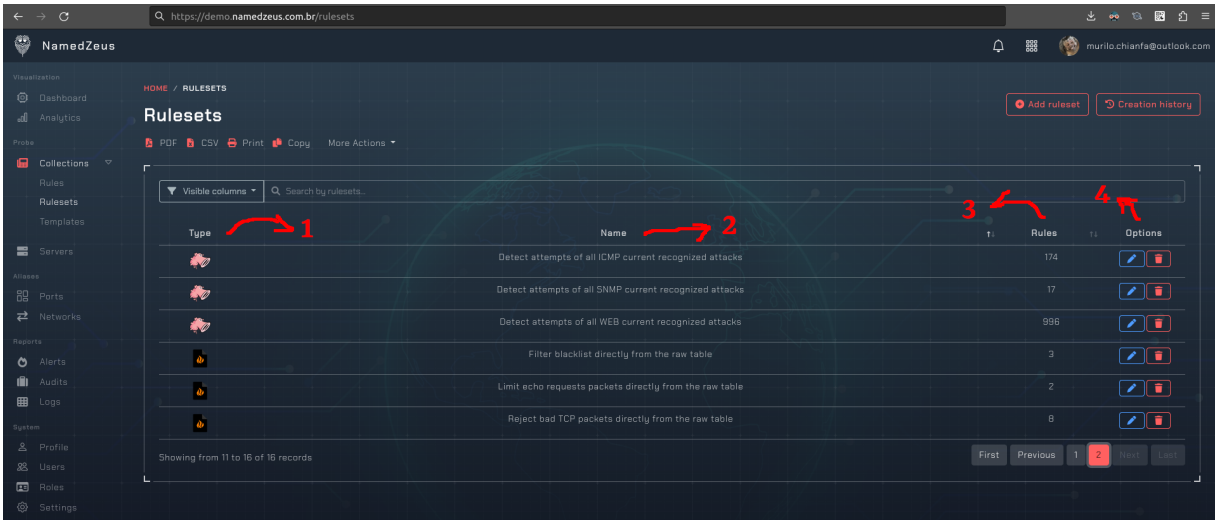
- **1 –** Campo de ação da regra.
- **2 –** Campo de seleção do protocolo de detecção da regra.
- **3 –** Número de identificação único da regra.
- **4 –** Número de revisão da regra.

- **5 –** Rede ou grupo de redes de origem para detecção da regra.
- **6 –** Rede ou grupo de redes de destino para detecção da regra.
- **7 –** Porta ou grupo de portas de origem para detecção da regra.
- **8 –** Porta ou grupo de portas de destino para detecção da regra.
- **9 –** Campo para inserir manualmente mais opções do que a disponível.

5.21 Listagem de conjunto de regras

Nesta página de listagem de coleções de regras, você pode gerenciar um conjunto de regras tanto de iptables quanto snort.

Figura 50 - Listagem de conjunto de regras

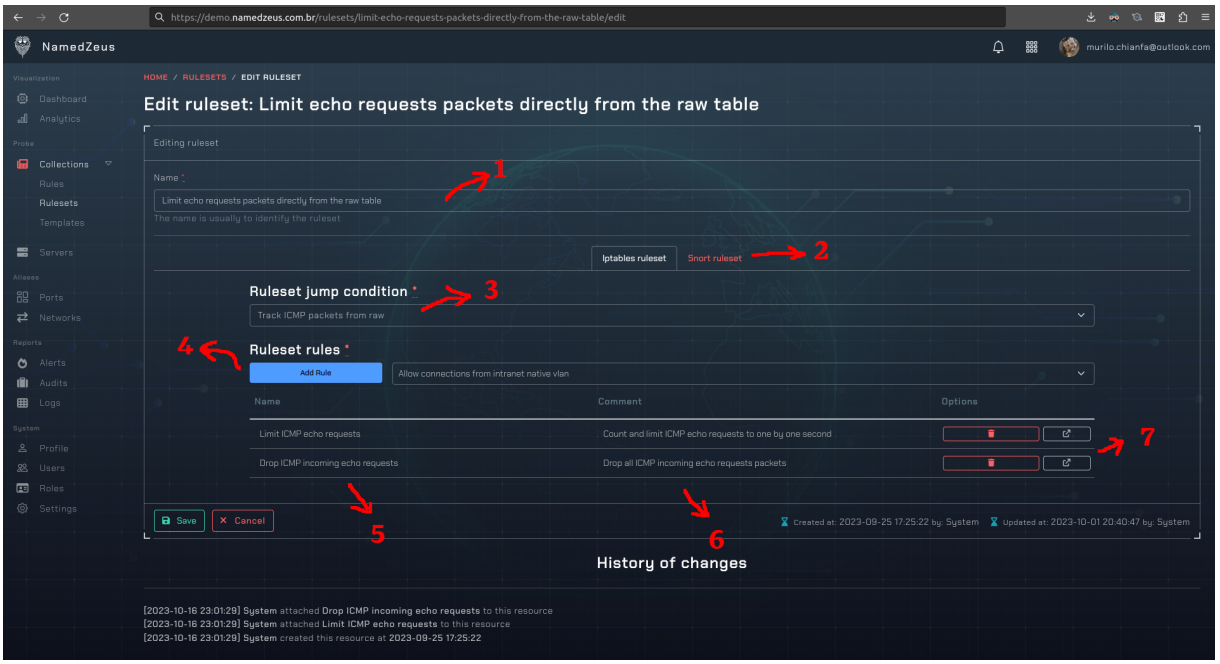


Fonte: Autoria própria, 2023.

- **1 –** Coluna para mostrar o tipo de coleção de regras.
- **2 –** Coluna de nome das coleções de regras.
- **3 –** Coluna de quantidade de regras na coleções de regras.
- **4 –** Coluna de opções da coleção de regras.

5.22 Edição de conjunto de regras

Figura 51 - Edição de conjunto de regras



Fonte: Autoria própria, 2023.

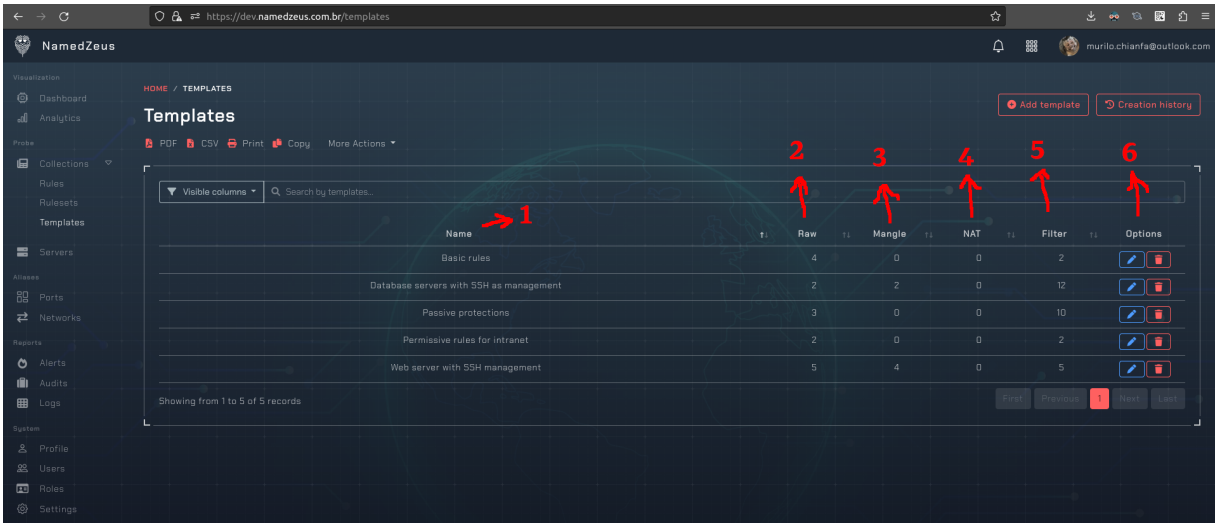
- **1 –** Campo de nome da coleção de regras.
- **2 –** Opções para selecionar qual tipo de regras vamos ter nessa coleção.
- **3 –** Campo de seleção da regra de pulo para ser iniciada na coleção.
- **4 –** Botão e campo de seleção da nova regra para a coleção.
- **5 –** Coluna de nome das regras adicionadas na coleção.
- **6 –** Coluna de descrição das regras adicionadas na coleção.
- **7 –** Opções das regras já adicionadas na coleção, aqui você excluir a regra da coleção e ir para a página da regra para visualizá-la melhor.

Uma opção disponível, é poder reordenar as regras adicionadas na coleção de maneira muito fácil, basta segurar e arrastar a regra para a ordem que você deseja, e soltar, lembrando que os pacotes seguem a ordem do conjunto de regras, sendo assim, muito importante você ordená-la corretamente.

5.23 Listagem de templates

Nesta página de listagem de templates, é possível visualizar quais templates tem quantas regras adicionadas, lembrando que quanto mais regras, mais pesado fica o processamento dos pacotes nos servidores em que estes templates estão aplicados.

Figura 52 - Listagem de templates



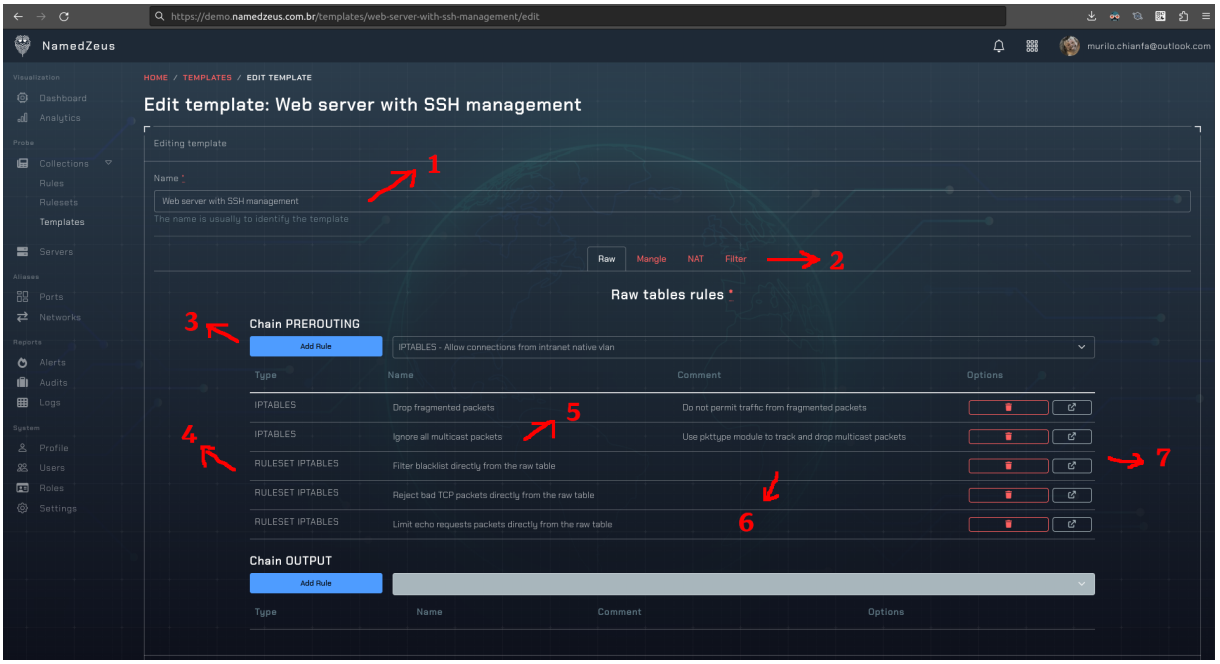
Fonte: Autoria própria, 2023.

- **1 –** Coluna do nome do template.
- **2 –** Coluna que mostra a quantidade de regras na tabela “Raw”.
- **3 –** Coluna que mostra a quantidade de regras na tabela “Mangle”.
- **4 –** Coluna que mostra a quantidade de regras na tabela “NAT”.
- **5 –** Coluna que mostra a quantidade de regras na tabela “Filter”.
- **6 –** Coluna de opções do template.

5.24 Edição de templates

Nesta tela de templates, só é possível utilizar regras e conjuntos de regras do tipo “Snort”, na tabela “Filter”, em qualquer uma das correntes que a tabela “Filter” tiver.

Figura 53 - Edição de templates

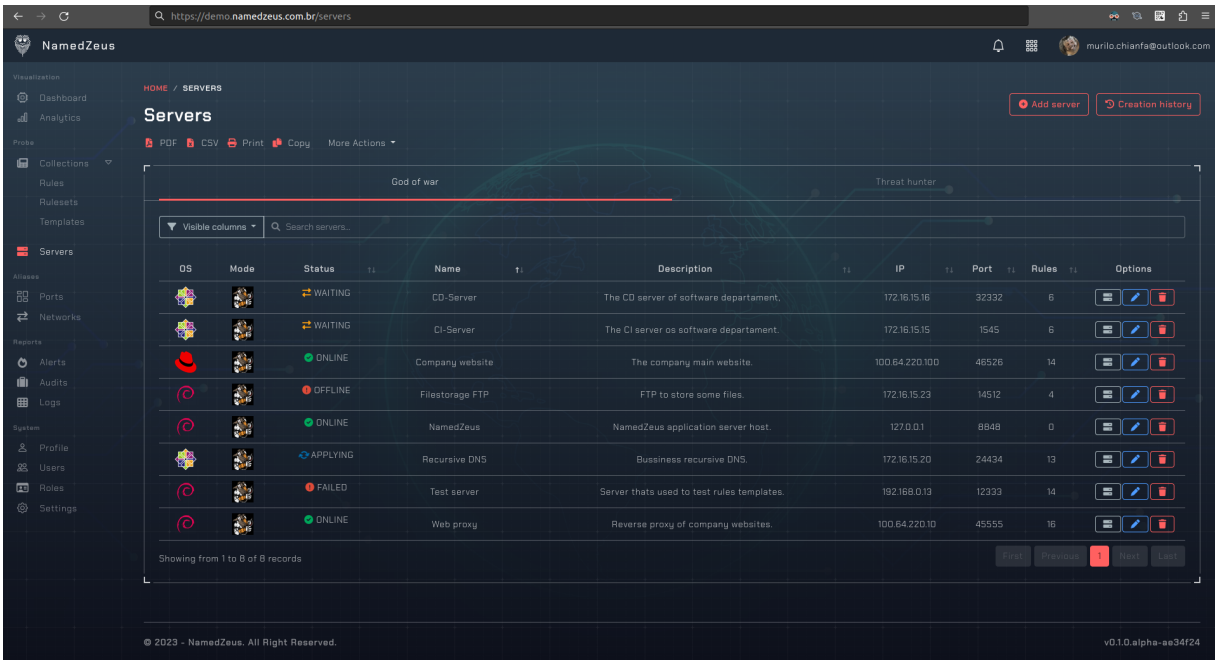


Fonte: Autoria própria, 2023.

- **1 –** Campo de nome do template.
- **2 –** Opções de seleção da tabela alvo atual das regras e conjunto de regras.
- **3 –** Botão e campo de seleção de novas regras ou conjunto de regras.
- **4 –** Coluna de tipo de regra ou conjunto de regras.
- **5 –** Coluna de nome da regra ou do conjunto de regras.
- **6 –** Coluna de comentário da regra ou do conjunto de regras.
- **7 –** Opções das regras ou conjunto de regras já adicionadas na chain da tabela alvo atual, aqui você pode excluir a regra ou o conjunto de regras da coleção ou ir para a página da regra ou do conjunto de regras para visualizá-la melhor.

5.25 Listagem de servidores

Figura 54 - Listagem de servidores



Fonte: Autoria própria, 2023.

Aqui na listagem de servidores, vamos poder visualizar todos os servidores monitorados e controlados pela aplicação, as informações de OS, modo de operação, status do NamedZeus Agent, IP/porta e quantidade de regras aplicadas ao servidor serão exibidos na tabela. A listagem será dividida entre os modos de operação: “Deus da guerra” e “Caçados de ameaças”.

O primeiro modo será recomendável caso haja uma comunicação direto entre o servidor e a aplicação, para que assim possam estabelecer uma conexão ponto a ponto para a troca de informações. Já o segundo modo de operação, será necessário caso não seja possível estabelecer essa comunicação direta (casos como de NAT no meio, muito comum em virtualizações e conteinerização).

Caso seja utilizado o modo de operação “Deus da guerra”, o NamedZeus Agent poderá atuar também como um IPS para receber regras de bloqueio dinamicamente, as diferenças entre um IDS e IPS podem ser vistas no **ANEXO B - Diferenças entre um IDS e IPS**.

5.26 Edição de servidores

Nesta página de edição de um servidor, você pode configurar o modo de operação do agent, as portas e redes particulares deste servidor e forçar a aplicação das regras e a instalação no servidor.

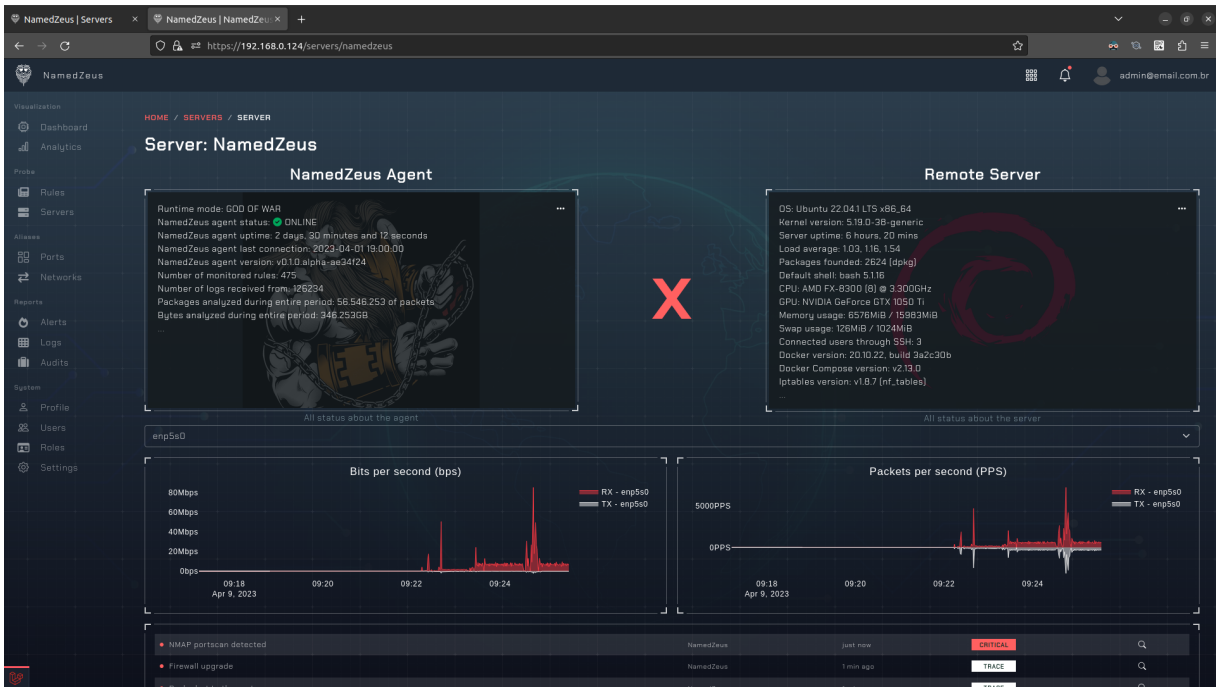
Figura 55 - Edição de servidores

Fonte: Autoria própria, 2023.

- **1 –** Campo de identificação único do servidor.
- **2 –** Campo de nome do servidor.
- **3 –** Campo de IP do servidor.
- **4 –** Campo de porta do agent instalado no servidor.
- **5 –** Campo de tipo de sistema operacional do servidor.
- **6 –** Campo de escolha do template que será utilizado neste servidor.
- **7 –** Campos de listagem das portas voláteis contidas no template, onde o servidor precisa dizer qual é o seu padrão.
- **8 –** Campos das networks voláteis.
- **9 –** Campo de escolha do modo de operação do servidor.
- **10 –** Botão contendo as instruções de instalação do agent no servidor alvo.
- **11 –** Botão para aplicar as regras e políticas no servidor.

5.27 Visualização de servidores

Figura 56 - Visualização de um servidor



Fonte: Autoria própria, 2023.

Após adicionado e configurado o cadastro do servidor e o NamedZeus Agent, uma página de diagnóstico será disponibilizada para podemos visualizar algumas informações do servidor.

Essas informações estão divididas entre:

- Informações pertinentes ao NamedZeus Agent
- Informações pertinentes ao servidor

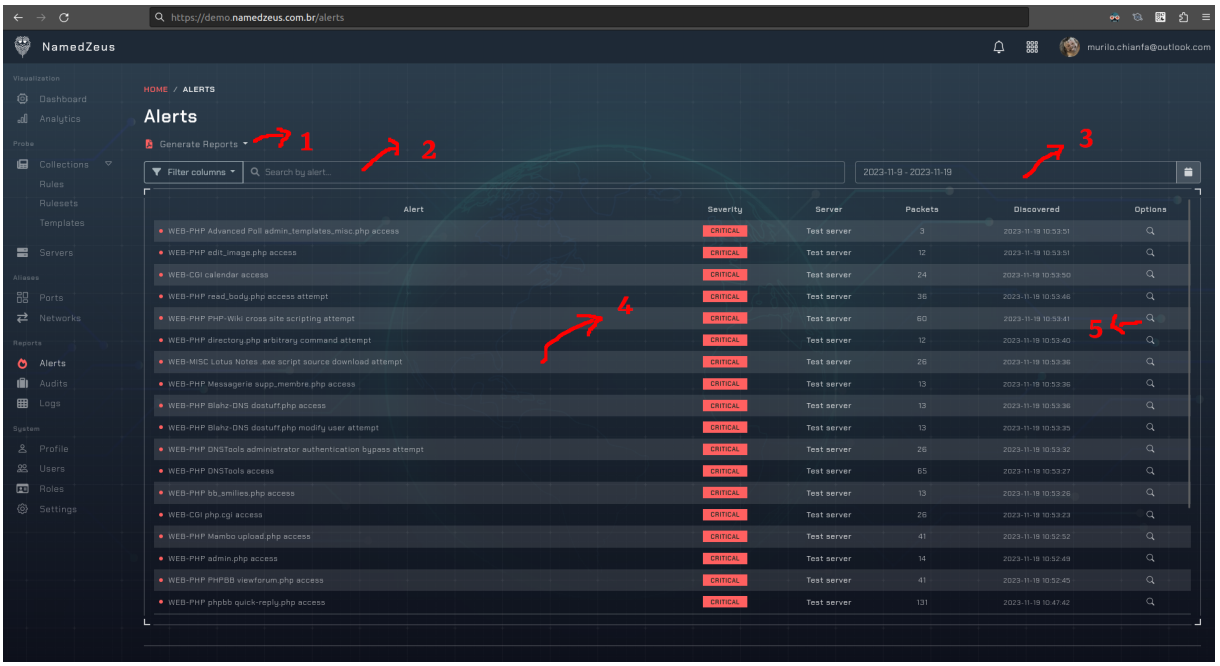
Um gráfico do tráfego em tempo real das interfaces do servidor também será disponibilizado para a validação do funcionamento do NamedZeus Agent.

Uma lista dos últimos alertas disparados detectados pelo NamedZeus Agent também estará disponível para visualização na parte inferior da página.

5.28 Relatório de alertas

Cada alerta poderá ser expandido para um detalhamento muito maior caso seja necessário uma investigação mais a fundo sobre o mesmo, assim como a visualização agregada do tipo de alerta por severidade ou regra.

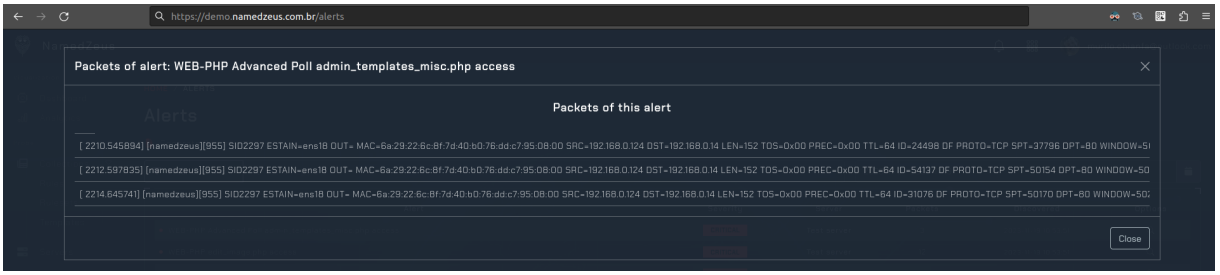
Figura 57 - Relatório de alertas em tela



Fonte: Autoria própria, 2023.

- **1 –** Botão com opções para gerar relatórios dos alertas.
- **2 –** Campo para pesquisa por palavras chaves no histórico.
- **3 –** Botão com opções para gerar relatórios dos alertas.
- **4 –** Listagem do histórico dos alertas.
- **5 –** Botão para visualizar os pacotes de um alerta em específico.

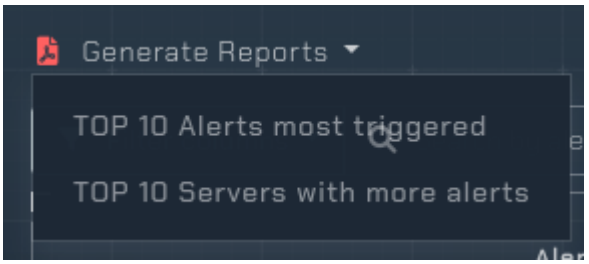
Figura 58 - Pacotes maliciosos de um alerta



Fonte: Autoria própria, 2023.

Para uma melhor tomada de decisão, é possível gerar alguns relatórios em PDF, ajudando assim a escolher a melhor opção na hora de tomar uma decisão estratégica.

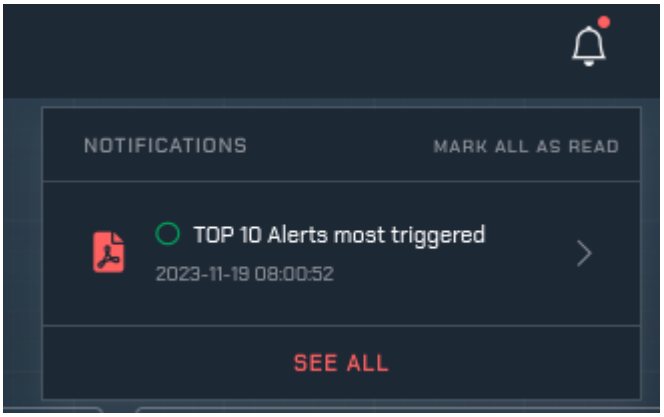
Figura 59 - Relatórios de alertas disponíveis



Fonte: Autoria própria, 2023.

Após clicar para gerar um alerta, o mesmo será gerado e quando estiver pronto, poderá ser acessível na aba de notificações.

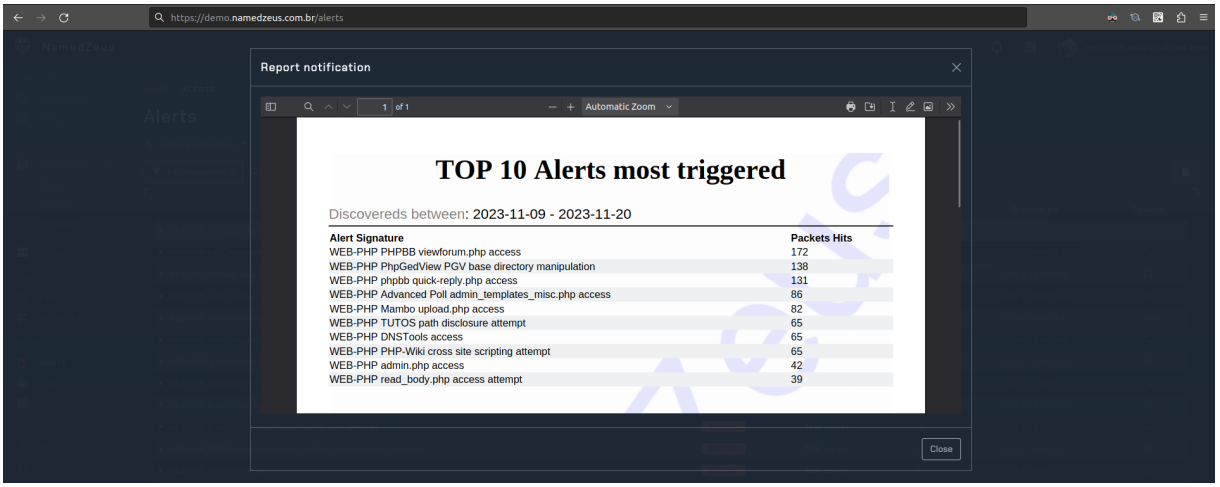
Figura 60 - Abertura de um relatório



Fonte: Autoria própria, 2023.

5.28.1 Relatório de alertas mais acionados

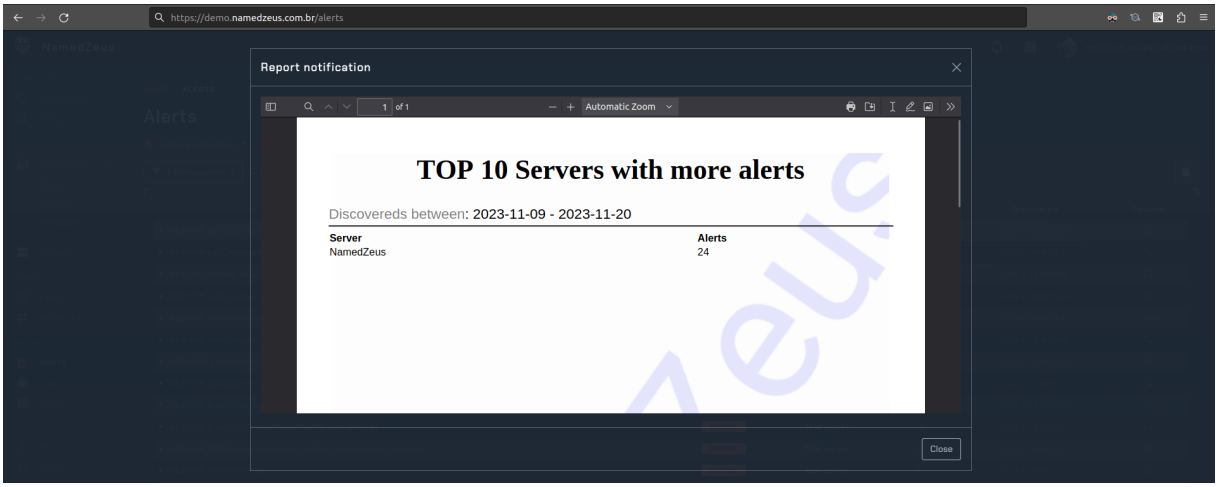
Figura 61 - Relatório de alertas mais acionados



Fonte: Autoria própria, 2023.

5.28.2 Relatório de servidores com mais alertas

Figura 62 - Relatório de servidores com mais alertas



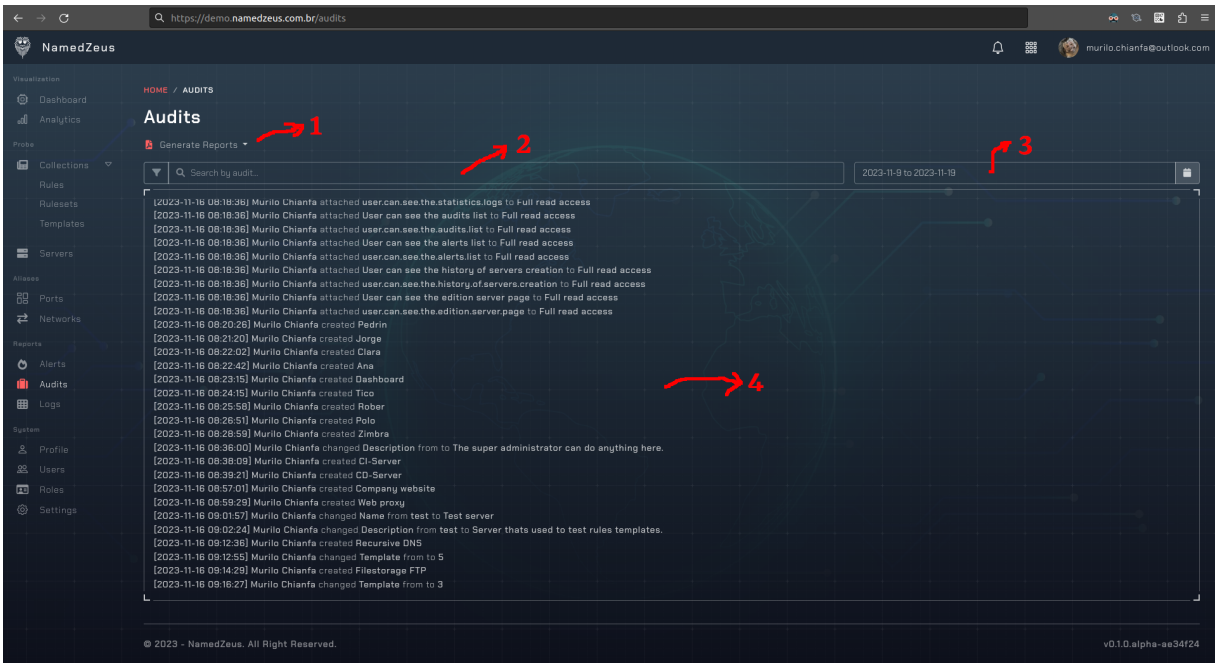
Fonte: Autoria própria, 2023.

5.29 Relatório de auditoria

Nessa tela de relatório de auditoria, podemos visualizar todas as ações executadas no sistema por que usuário sobre que recurso e em que horário ele

aconteceu, para que possamos realizar uma auditoria completa no sistema caso necessário.

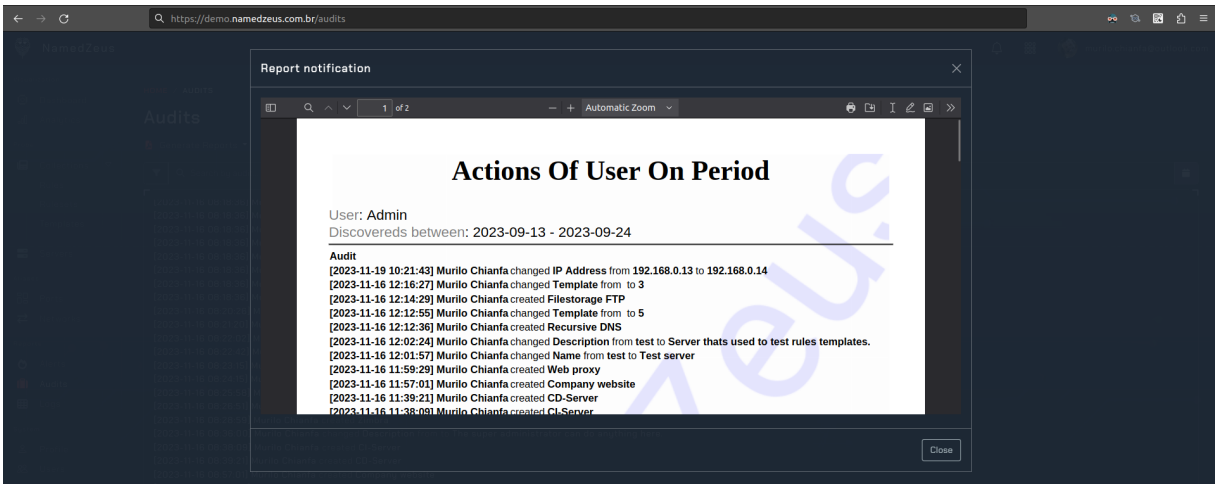
Figura 63 - Auditoria do sistema



Fonte: Autoria própria, 2023.

- **1 –** Botão com opções para gerar relatórios de auditoria.
- **2 –** Campo para pesquisa por palavras chaves no histórico.
- **3 –** Campo para seleção da data de filtro da auditoria.
- **4 –** Listagem do histórico de ações dos usuários no sistema.

Figura 64 - Relatório de auditoria por usuário



Fonte: Autoria própria, 2023.

5.30 Dashboard geral

Aqui podemos ver o status geral de nossos servidores monitorados, como o número de alertas gerados por hora, quantidade de pacotes e banda considerados maliciosos pelas regras configuradas e até mesmo um overview dos IPs que originaram os ataques a nossa infraestrutura caso sejam públicos.

Podemos reparar também que no cabeçalho do sistema, temos acesso a nossa conta e as notificações do sistema para nosso usuário, assim como no menu lateral, onde temos os links de navegação do sistema.

Figura 65 - Dashboard geral

Fonte: Autoria própria, 2023.

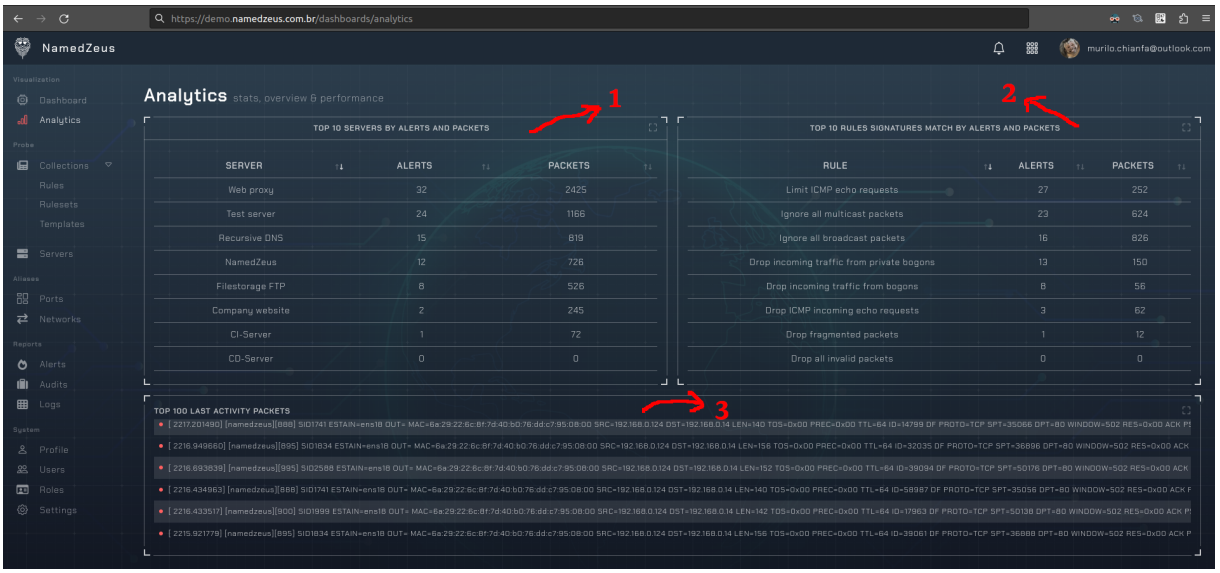
- **1 –** Valores de pacotes maliciosos trafegados nos servidores registrados.
- **2 –** Valores de tráfego malicioso nos servidores registrados.
- **3 –** Quantidade de IPs únicos descobertos em ataques.
- **4 –** Número de regras atingidas do total de monitoradas.
- **5 –** Gráfico do total de alertas registrados por hora nas últimas 24 horas.
- **6 –** Gráfico de geo localização dos IPs de origem dos ataques.
- **7 –** Listagem dos últimos alertas registrados pelo sistema.

5.31 Dashboard de análises

Aqui podemos ver o status geral de nossos servidores monitorados, como o número de alertas gerados por hora, quantidade de pacotes e banda considerados maliciosos pelas regras configuradas e até mesmo um overview dos IPs que originaram os ataques a nossa infraestrutura caso sejam públicos.

Podemos reparar também que no cabeçalho do sistema, temos acesso a nossa conta e as notificações do sistema para nosso usuário, assim como no menu lateral, onde temos os links de navegação do sistema.

Figura 66 - Dashboard de análises



Fonte: Autoria própria, 2023.

- **1 –** Listagem dos servidores com mais alertas registrados.
- **2 –** Listagem das regras monitoradas com mais alertas registrados.
- **3 –** Últimos 100 pacotes maliciosos recebidos pelos servidores monitorados.

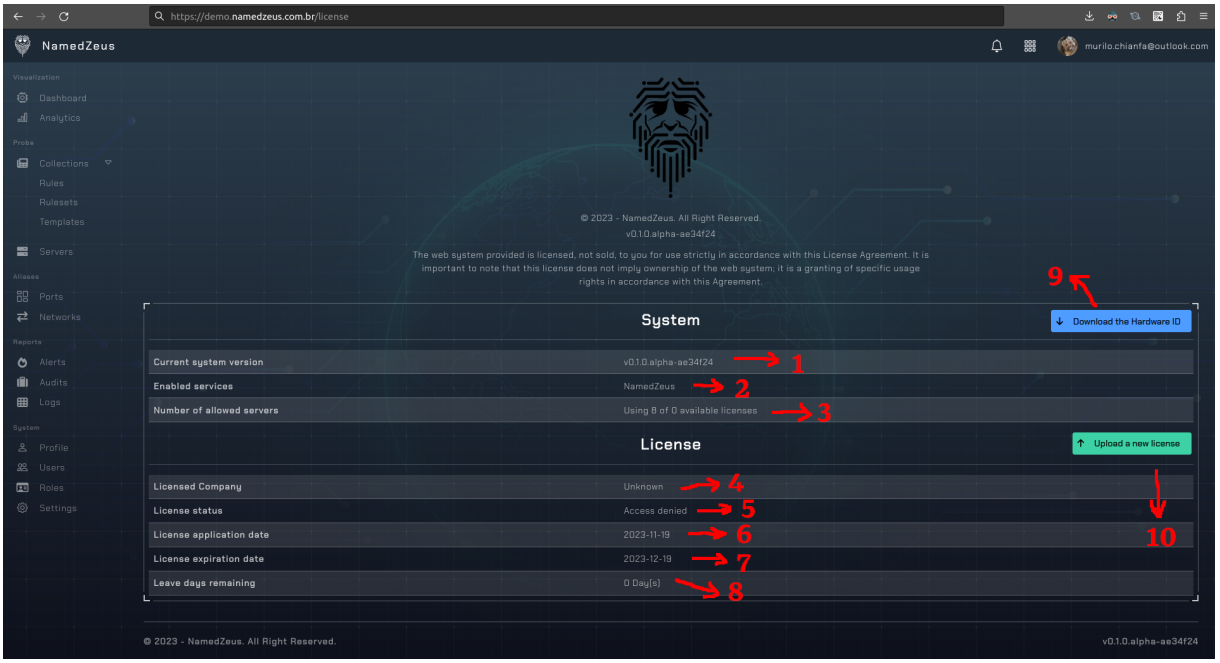
Todos os dados desta tela são baseados em todo o tempo de atividade do sistema, você pode dar zoom em cada uma das informações para poder vê-las por completo se necessário.

5.32 Licenciamento do sistema

Nesta tela de licenciamento, você pode visualizar todas as atualizações referentes à licença atual ativa no sistema, e algumas outras informações como versão do sistema e para quem a licença atual foi acordada.

Caso seja necessário, você pode enviar uma nova licença por aqui clicando no botão de upload de nova licença.

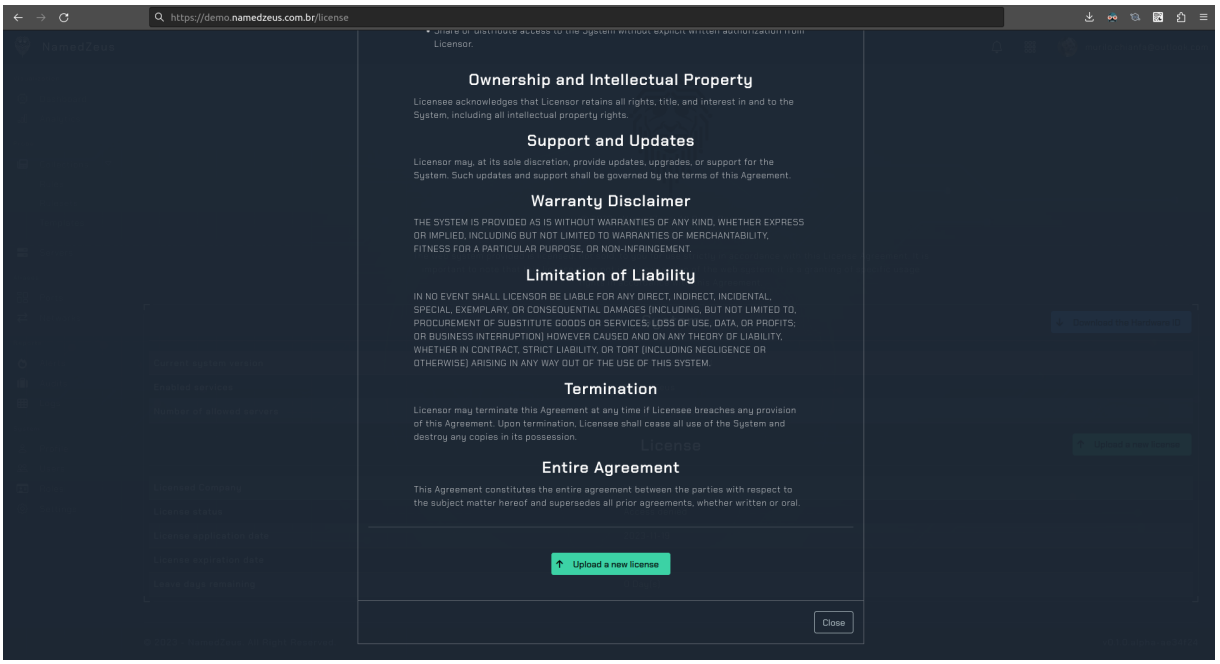
Figura 67 - Licença do sistema



Fonte: Autoria própria, 2023.

- **1 –** Versão atual do sistema.
- **3 –** Número de licenças sendo utilizadas, baseado no número de servidores cadastrados no sistema.
- **4 –** Nome da empresa que comprou e ativou a licença atual.
- **5 –** Estado de liberação de uso da licença atual.
- **6 –** Data de ativação da licença atual.
- **7 –** Data de expiração da licença atual.
- **8 –** Dias restantes da licença atual.
- **9 –** Botão para realizar o download da identificação de hardware.
- **10 –** Botão para abrir a opção de upload de nova licença.

Figura 68 - Enviar nova licença

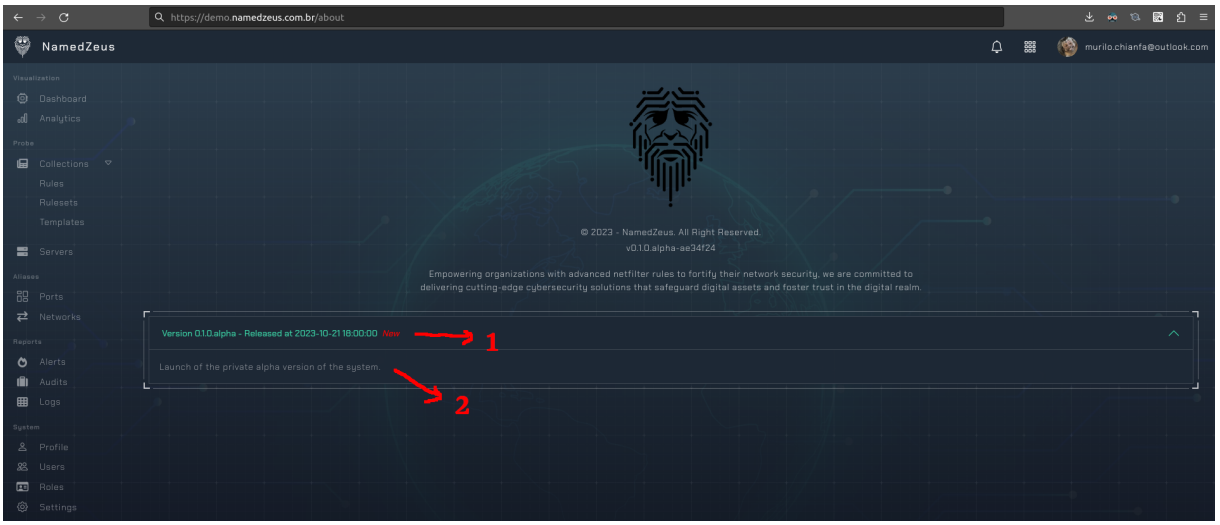


Fonte: Autoria própria, 2023.

5.33 Sobre o sistema

Nesta tela de sobre o sistema, você pode visualizar todas as atualizações do sistema.

Figura 69 - Sobre o sistema



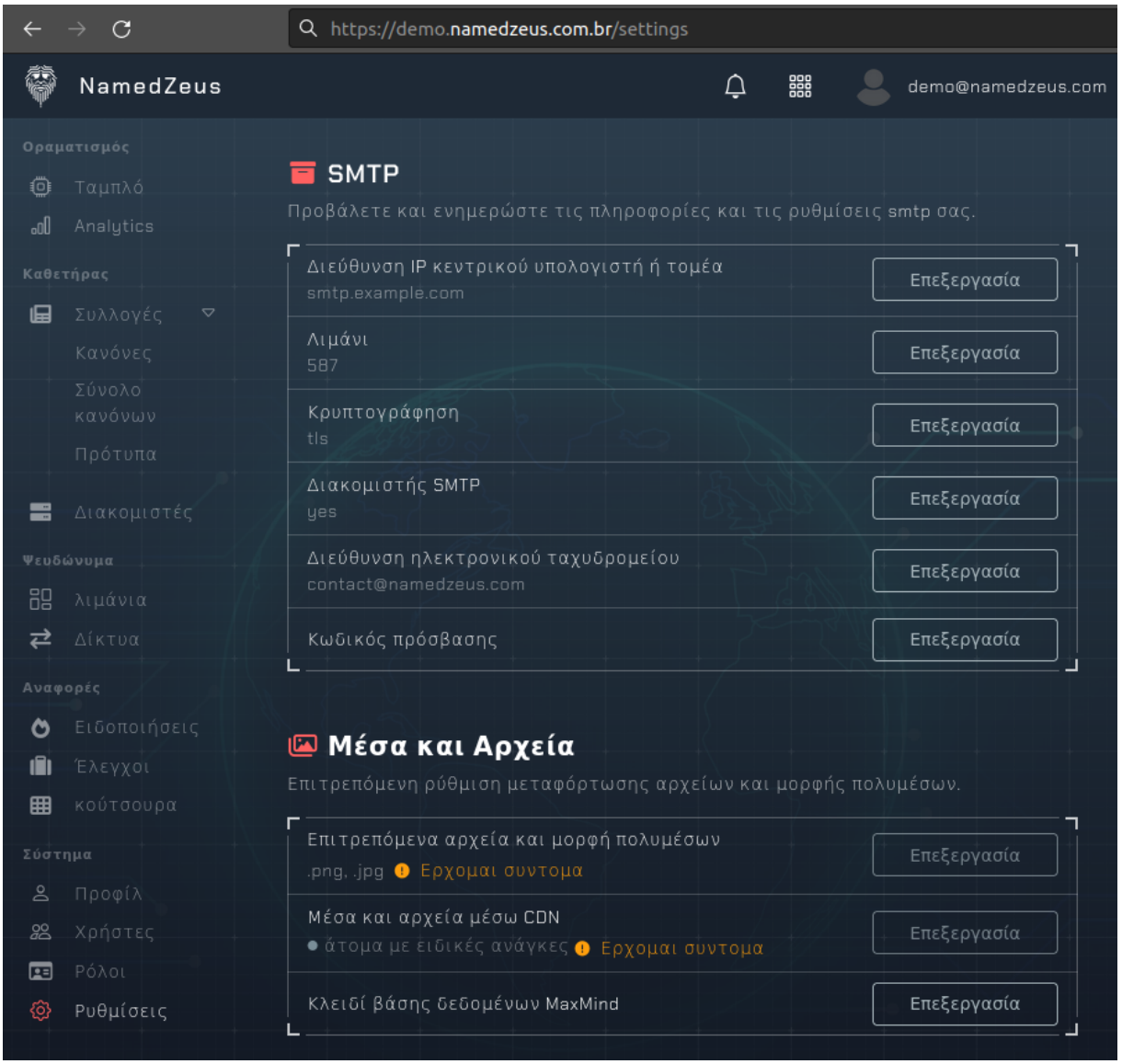
Fonte: Autoria própria, 2023.

- **1 –** Título e data de lançamento da nova atualização.
- **2 –** Atualizações detalhadas da nova atualização.

5.34 Outras linguagens

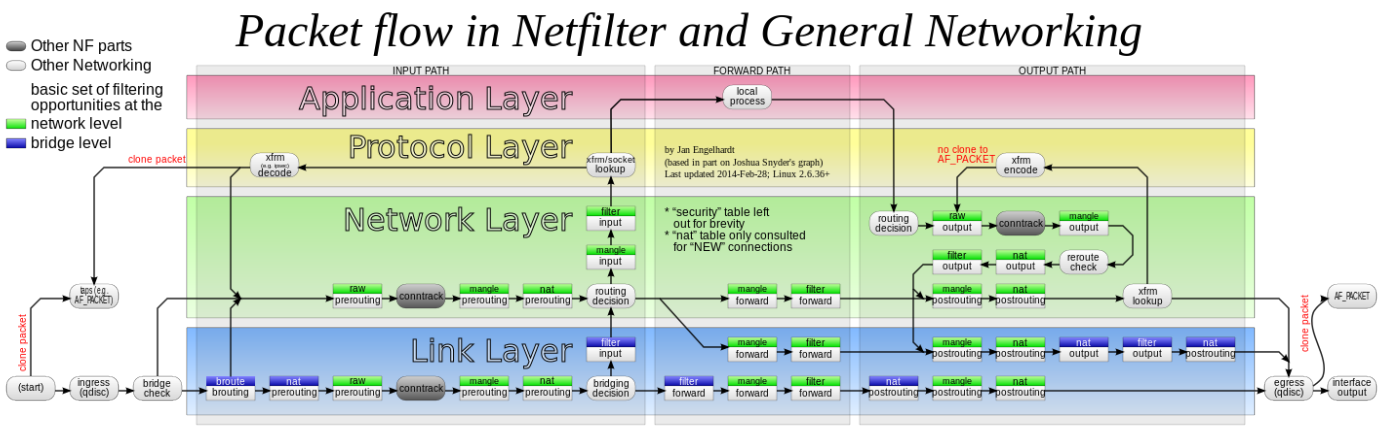
Atualmente estão disponíveis 68 línguas de exibição do sistema, porém ainda sem a revisão de nativos de cada uma. Aqui podemos ver um exemplo do sistema em grego:

Figura 70 - Sistema em grego



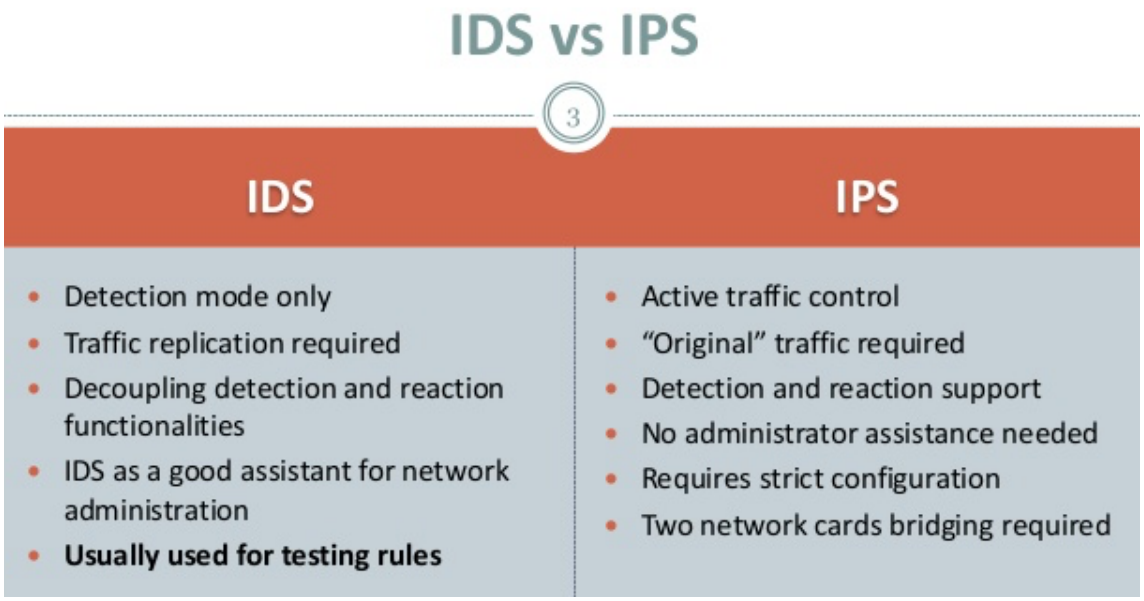
Fonte: Autoria própria, 2023.

ANEXO A - Fluxo de pacotes no módulo de kernel NETFILTER



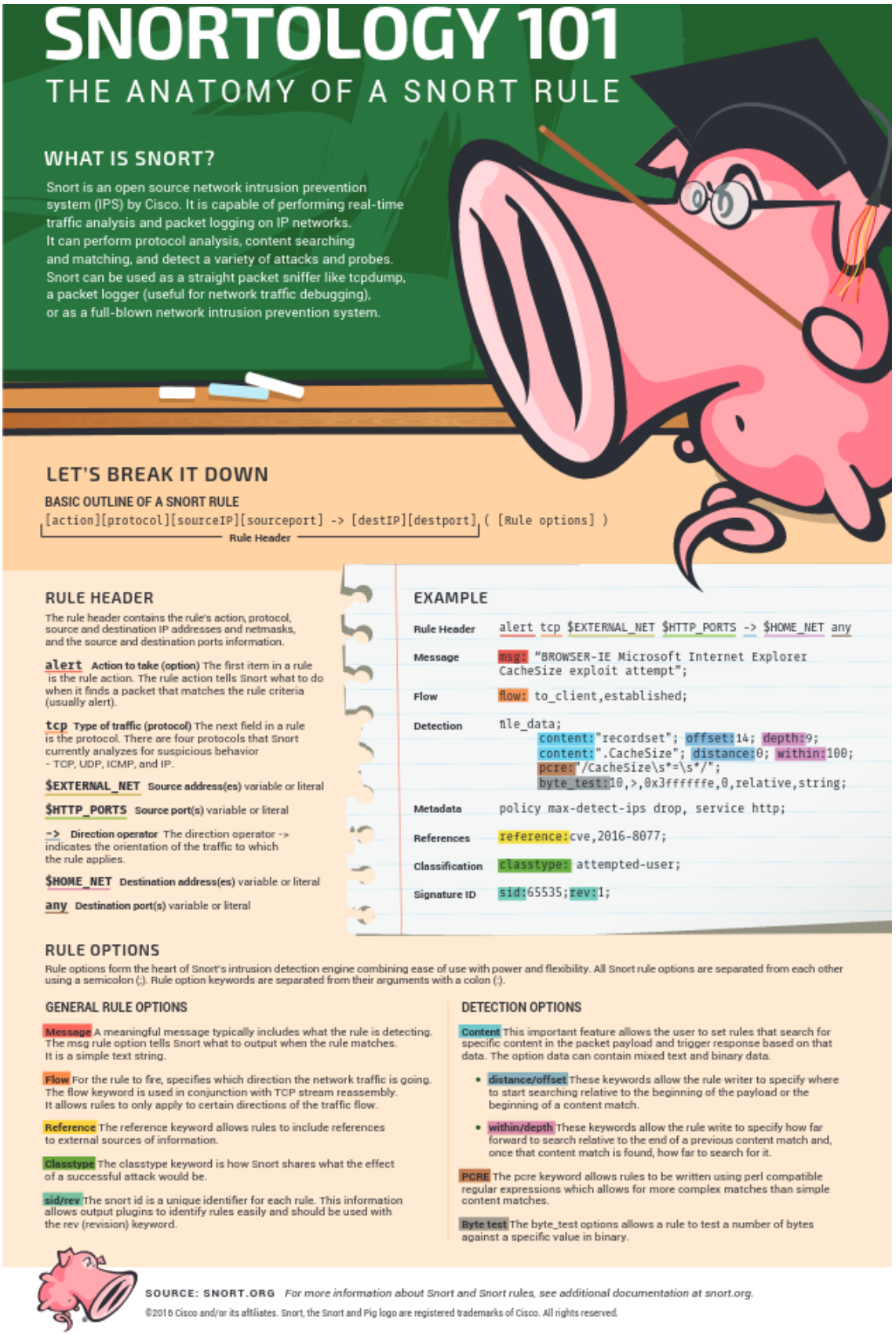
Fonte: Jan Engelhard, 2014.

ANEXO B - Diferenças entre um IDS e IPS



Fonte: SY110 - Introduction to Cyber Security, 2023.

ANEXO C - Anatomia de regras baseadas em SNORT



APÊNDICE A - RESUMO EXPANDIDO: NAMEDZEUS – UM SISTEMA DE IMPOSIÇÃO DE POLÍTICAS DE REDE BASEADO EM HOST

NAMEDZEUS – UM SISTEMA DE IMPOSIÇÃO DE POLÍTICAS DE REDE BASEADO EM HOST

CHIANFA, Murilo de Araújo[1]; COELHO, Fabrício José[2];

Palavras-chave: Firewall. Netfilter. Iptables.

INTRODUÇÃO

O ambiente corporativo é um ambiente que integra diversos sistemas de diferentes organizações, sendo a rede a tecnologia utilizada para realizar a integração que permite todas as conexões entre seus elementos. A confiabilidade, integridade e disponibilidade da rede são essenciais para o próprio negócio da organização.

Os seguintes fatores justificam a preocupação com a segurança contínua: a natureza dos ataques, novas vulnerabilidades das tecnologias emergentes, a criação de novas formas de ataques, o aumento da conectividade, a complexidade da defesa, o aumento dos crimes digitais e os grandes prejuízos ocasionados pela falta de segurança. (NAKAMURA; GEUS, 2003, p.10).

Uma organização pode se proteger utilizando diferentes técnicas e mecanismos, um deles é o que vamos abordar aqui, o firewall de redes. Firewall é um ponto entre duas ou mais redes, por onde todo o tráfego transita por sua estrutura, permitindo assim um controle e auditoria de maneira eficaz.

---

[1] Murilo de Araujo Chianfa. Acadêmico do Curso de Bacharelado em Sistemas de Informação da faculdade de Apucarana – FAP. Apucarana – Pr. 2023.

[2] Fabrício José Coelho. Docente/Orientador do Curso de Bacharelado em Sistema de Informação da Faculdade de Apucarana – FAP. Apucarana – PR. 2023.

Porém de acordo com as recomendações do Instituto Nacional de Padrões e Tecnologia (NIST, 2009, p.20, tradução nossa), os firewalls como gateway da rede por si só, não são capazes de reconhecer todas as instâncias e formas de ataques, permitindo que alguns ataques penetrem e alcancem os hosts internos, e os ataques enviados de um host interno para outro podem nem passar pelo firewall principal, sendo necessário a adição de outros firewalls pelo caminho, como por exemplo os firewalls baseados em host para os servidores de aplicação, fornecendo assim uma camada adicional de segurança contra os ataques pela rede.

Para João Eriberto (2013, p.353): “Com a defesa em profundidade, não dependeremos de somente um mecanismo de segurança. Teremos, em vez disso, vários mecanismos que se ligam uns aos outros e a falha de um desses mecanismos não compromete todo o conjunto.”

OBJETIVO

Tendo em vista a grande complexidade no gerenciamento das regras e políticas do firewall para os diversos hosts, o software desenvolvido visa sanar esta dor agrupando essas regras em grupos para serem de forma centralizada, associadas aos servidores hospedando serviços de mesmo propósito.

> A complexidade das regras de filtragem cresce cada vez mais na medida em que serviços e aplicações são adicionados no ambiente corporativo. Dessa forma, o gerenciamento centralizado se torna um fator importante para que erros na criação e implementação de regras sejam minimizados (ESQUIVEL, 2006, p.29).

O sistema terá um conjunto de regras já pré cadastradas para que o administrador de redes possa ter um norte na configuração e customização das políticas e regras a serem aplicadas aos seus servidores.

Contando ainda com a possibilidade de realizar uma auditoria nas mudanças aplicadas aos servidores, para que seja possível rastrear quaisquer alterações.

MÉTODO

Inicialmente foi realizada uma pesquisa literária sobre o assunto para o embasamento teórico dos requisitos funcionais. Em conjunto a isso, a construção dos diagramas foi iniciada, tanto o diagrama de casos de uso, quanto o diagrama de modelo de entidade e relacionamento para o banco de dados.

Após o término do levantamento de requisitos e da criação dos diagramas foi dado início à construção do projeto. Para dar início, foi escolhido utilizar um template pronto para a interface gráfica, para facilitar e agilizar o desenvolvimento do software.

DESENVOLVIMENTO

Para o desenvolvimento do software em questão, foi dedicada uma atenção primordial aos aspectos relacionados à segurança. Compreendendo a importância crítica de garantir sua integridade e proteção, uma abordagem meticulosa na concepção e elaboração do sistema foi necessária, com práticas de codificação segura, a fim de prevenir potenciais vulnerabilidades, atualizações regulares ao longo do desenvolvimento e mecanismos de proteção nas funcionalidades mais importantes.

A linguagem de programação escolhida para a construção do software foi PHP com o framework Laravel, já para o banco de dados, foi utilizado MariaDB, Apache2 para o servidor WEB, Nginx como proxy reverso, RabbitMQ para enfileiramento dos alertas, Rsyslog como coletor dos pacotes maliciosos, Redis2 para cache em memória primária, Docker para o empacotamento da aplicação e C++ com o framework Drogon para a criação da probe.

Todas as tecnologias utilizadas estão em sua última versão estável disponível, garantindo assim uma maior estabilidade e performance para o sistema.

CONCLUSÕES

Atualmente o sistema está com seu MVP (Minimum viable product) pronto e agora passa pela fase final de testes antes de seu lançamento oficial, com uma arquitetura sólida e funcionalidades inovadoras, o mesmo se destaca como uma solução abrangente e eficaz para o que se propõe.

Outro destaque notável é a capacidade de integrar-se perfeitamente em diferentes distribuições linux, evidenciando sua versatilidade e adaptabilidade. Com uma interface intuitiva e ferramentas de gerenciamento simplificadas proporcionam uma experiência de usuário otimizada, reduzindo o tempo de aprendizado e aumentando a eficiência operacional.

Após o término dos testes finais, o próximo passo será lançar o software ao público para assim validar sua eficácia, o software desenvolvido será comercializado por meio de um modelo de licenciamento flexível, que por sua vez, se adapta às necessidades e ao porte de diferentes organizações.

A transparência e a flexibilidade do modelo de venda, irão assegurar que o software atenderá às expectativas e requisitos individuais de cada cliente, promovendo assim uma parceria duradoura e confiável.

Fonte: Autoria própria, 2023.

REFERÊNCIAS

NAKAMURA, GEUS. **Segurança de Redes em Ambientes Cooperativos**. 2ª. ed., São Paulo, Futura, 2003.

NIST - National Institute of Standards and Technology. **Recommendations of the National Institute of Standards and Technology**. 1ª. ed., Gaithersburg, 2009.

MOTA, João E. **Análise de Tráfego em Redes TCP/IP: Utilize tcpdump na análise de tráfegos em qualquer sistema operacional**. 1ª ed., Novatec Editora, 2013.

ESQUIVEL, C.J. **Gerenciamento de regras de Firewall IPTABLES em ambiente Linux**. 2006.

GHEORGHE, Lucian. **Designing and Implementing Linux Firewalls and QoS Using Netfilter, Iproute2, NAT and L7-filter: Learn how to Secure Your System and Implement QoS Using Real-world Scenarios for Networks of All Sizes**. 1ª ed., PacktPub., 2006.

PURDY, Gregor N. **Linux Iptables Pocket Reference**. 1ª ed., O'Reilly Media, 2004.

RASH, Michael. **Linux Firewalls: Attack Detection and Response**. 1ª ed., No Starch Press, 2007.

RICE, Liz. **Container Security: Fundamental Technology Concepts that Protect Containerized Applications**. 1ª ed., O'Reilly Media, Incorporated, 2020.

LISKA, Allan. **Segurança de DNS: Defendendo o Sistema de Nomes de Domínio**. 1ª ed., Novatec Editora, 2016.

BINNIE, Chris. **Segurança em servidores Linux: Ataque e Defesa**. 1ª ed., Novatec Editora, 2017.

URUBATAN, Neto**. Dominando Linux Firewall Iptables**. 1ª ed., Ciência Moderna, 2020.