Imagine sua empresa **invisível para os hackers...**

...enquanto continua **visível para os seus clientes!**

NETSENSOR

Manual de Instruções

Versão 1.1

Sumário

NETSENSOR.....3
Acesso inicial à interface WEB.....4
Dashboard de Desempenho.....5
Dashboard de Geo Localização.....6
Log de Bloqueios.....7
Consulta e liberação de IPs bloqueados.....8
Log de Eventos.....9
Relatórios.....10
Log de Auditoria.....11
Configurações Gerais.....12
Topologia de Rede.....13
Sensores.....14
Grupos de Regras.....15
Sensores de Porta.....16
Sensores de Rede.....17
Origens Confiáveis.....18
Serviços Reais.....19
Links.....20
Usuários.....21
Serviços.....22
Backup.....23
Restauração de Backup.....24

NETSENSOR

Identificação e bloqueio de ataques cibernéticos.
"Imagine sua empresa invisível para hackers, enquanto continua visível para os seus clientes."

Criado para se tornar um aliado no combate mais efetivo a um grave problema que vem crescendo em uma escala assustadora, o de crimes cibernéticos, o NETSENSOR, principal produto da pilha de segurança, foi idealizado a partir de um sonho:

"Imagine sua empresa invisível para hackers, enquanto continua visível para os seus clientes."

Bom demais? Utopia? Impossível?

Após pouco mais de uma década o sonho se tornou realidade, um sistema capaz de observar de forma oculta o tráfego internet, identificar padrões presentes na grande maioria dos ataques, aprender quem é malicioso e deixar sua rede invisível para criminosos cibernéticos, enquanto continua operando normalmente para seus clientes e parceiros de negócio.

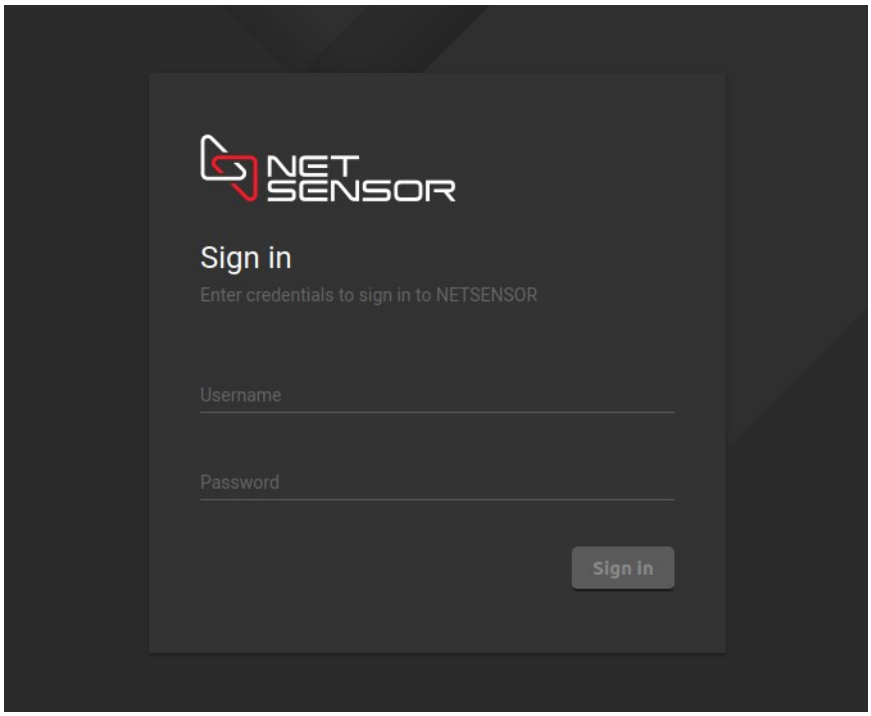
Utilizando conceitos de inteligência artificial (machine learning) esta solução, de forma proativa e sem intervenção humana, é capaz de observar de forma totalmente transparente o tráfego internet, identificar padrões presentes na grande maioria dos ataques cibernéticos e os bloquear já em suas fases iniciais, antes que eles sejam efetivados.

Através de dashboard, gráficos e mapa mundial, o NETSENSOR proporciona uma incrível experiência de visibilidade das tentativas de ataques detectadas e bloqueadas, com estatísticas de bloqueios, IPs, paises e continentes.

Acesso inicial à interface WEB

Através de um navegador WEB acesso a URL de acesso ao seu equipamento na sua estrutura de rede.
Exemplo: https://netsensor.minhaempresa.local

Você deverá chegar à tela de autenticação do NETSENSOR, onde deverá informa as credenciais de acesso ao sistema.



Dashboard de Desempenho

Após autenticar no NETSENSOR, você acessará o dashboard de desempenho, onde poderá acompanhar o desempenho das detecções de tráfegos maliciosos, dos sensores e de uso do equipamento.

No menu à esquerda, você terá acesso a todas as configurações e funcionalidades do NETSENSOR.

Na parte superior direita você terá:

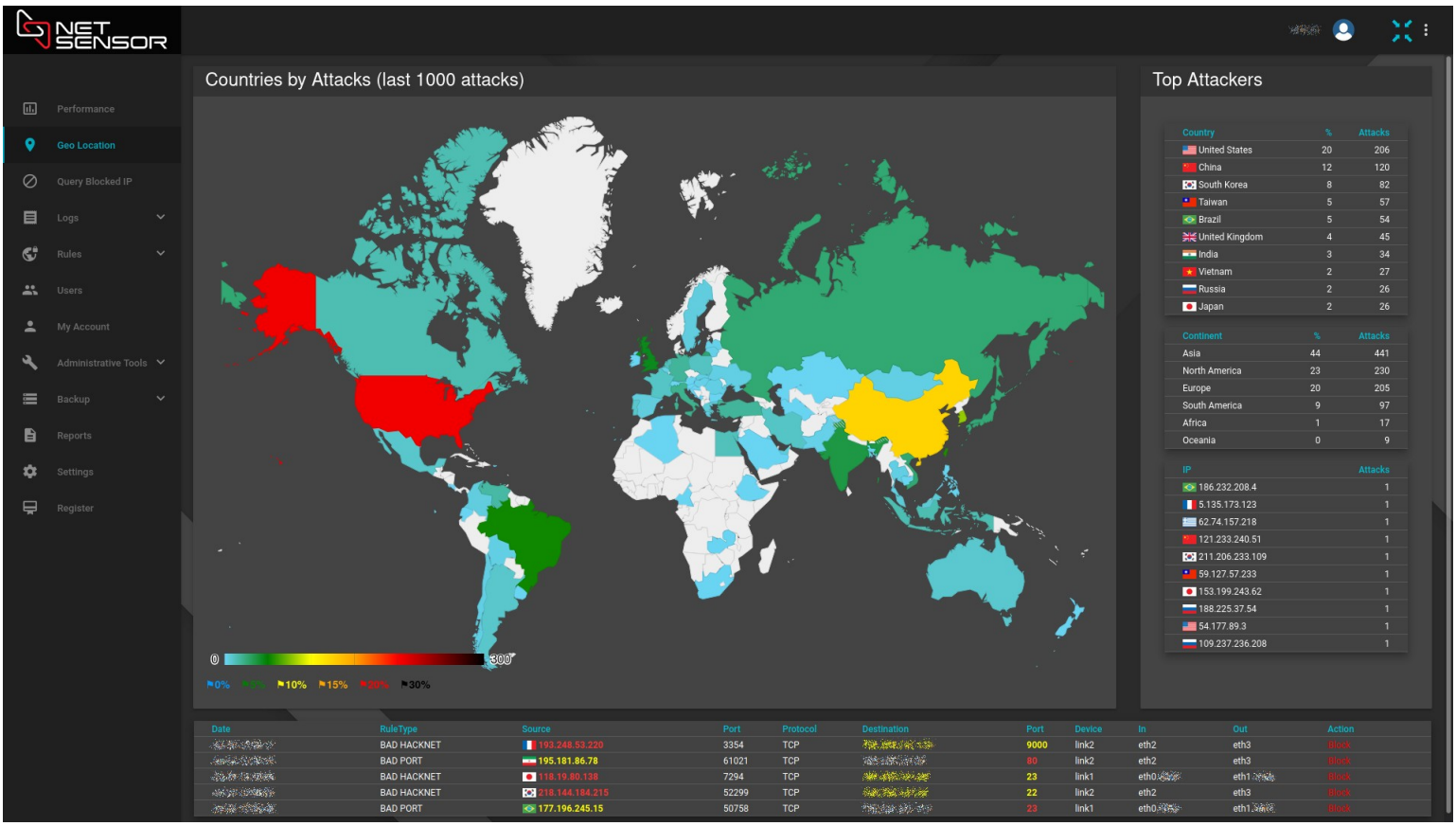
- Ícone para acesso rápido às configurações da conta e a opção de sair do sistema (log out);
- Ícone para entrar e sair do modo de tela cheia (full screen);
- Ícone com “três pontos” para acesso rápido as opções mais comumente usadas no NETSENSOR.

Dashboard de Geo Localização

Na opção “Geo Location” você acessará o dashboard de Geo Localização, onde poderá acompanhar um mapa de calor sinalizando os países que foram detectados gerando algum tráfego malicioso contra a sua rede.

No lado direito, você verá quem são os maiores atacantes contra a sua estrutura.

Já na parte inferior você verá, em tempo real, os tráfegos que estão sendo detectados como maliciosos, com informações da origem, do sensor que identificou o tráfego e do alvo que ele está tentou explorar.

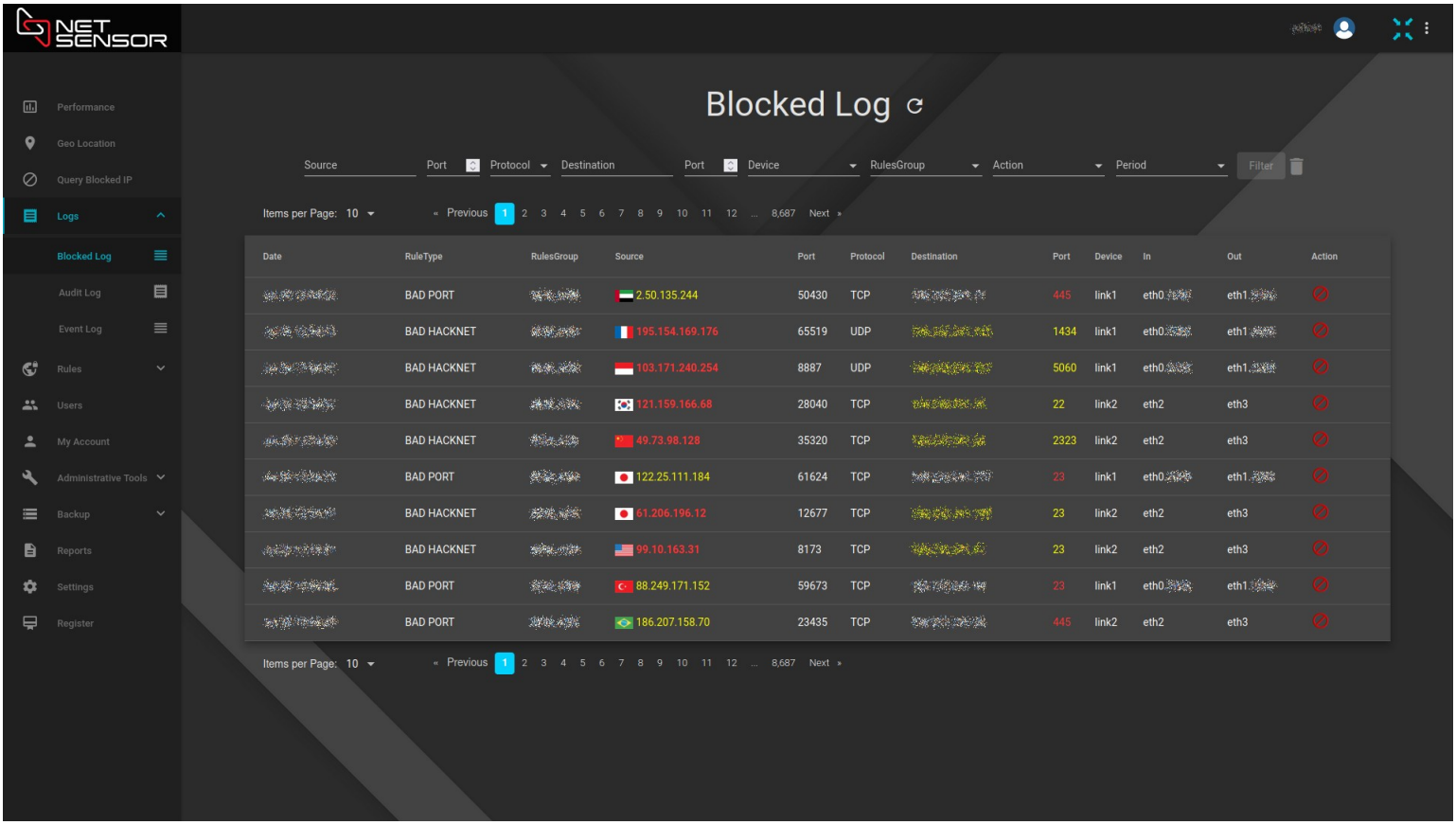


Log de Bloqueios

Abrindo o menu “Logs” e selecionando a opção “Blocked Log”, você poderá ver todos tráfegos identificados como maliciosos pelo NETSENSOR, com informações da origem, do sensor que identificou o tráfego e do alvo que ele tentou explorar.

Na parte superior você tem diversas opções de filtro, para facilitar na busca de registros mais específicos.

Os registros são referentes aos bloqueios ocorridos no dia atual. Na opção de filtro “Period” pode-se selecionar a pesquisa no histórico dos 7 dias anteriores.



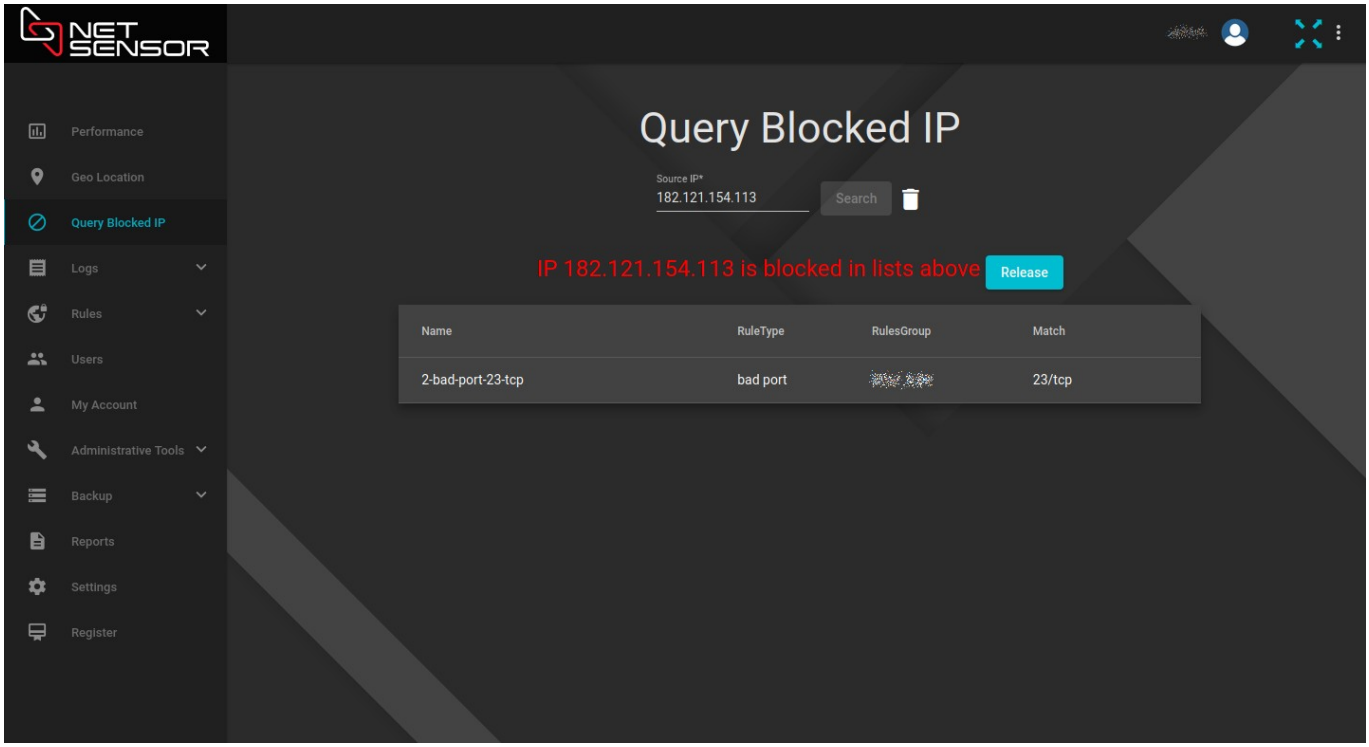
Consulta e liberação de IPs bloqueados

Na opção “Query Blocked IP” você poderá consultar se um IP encontra-se atualmente bloqueado, ver em qual lista ele foi adicionado, e identificar qual sensor disparou a detecção.

Haverá também um botão de “Release”, o qual permite a remoção do IP da(s) lista(s) de bloqueio(s).

** A remoção do atual bloqueio não impede que o IP seja bloqueado novamente, caso dispare algum sensor.*

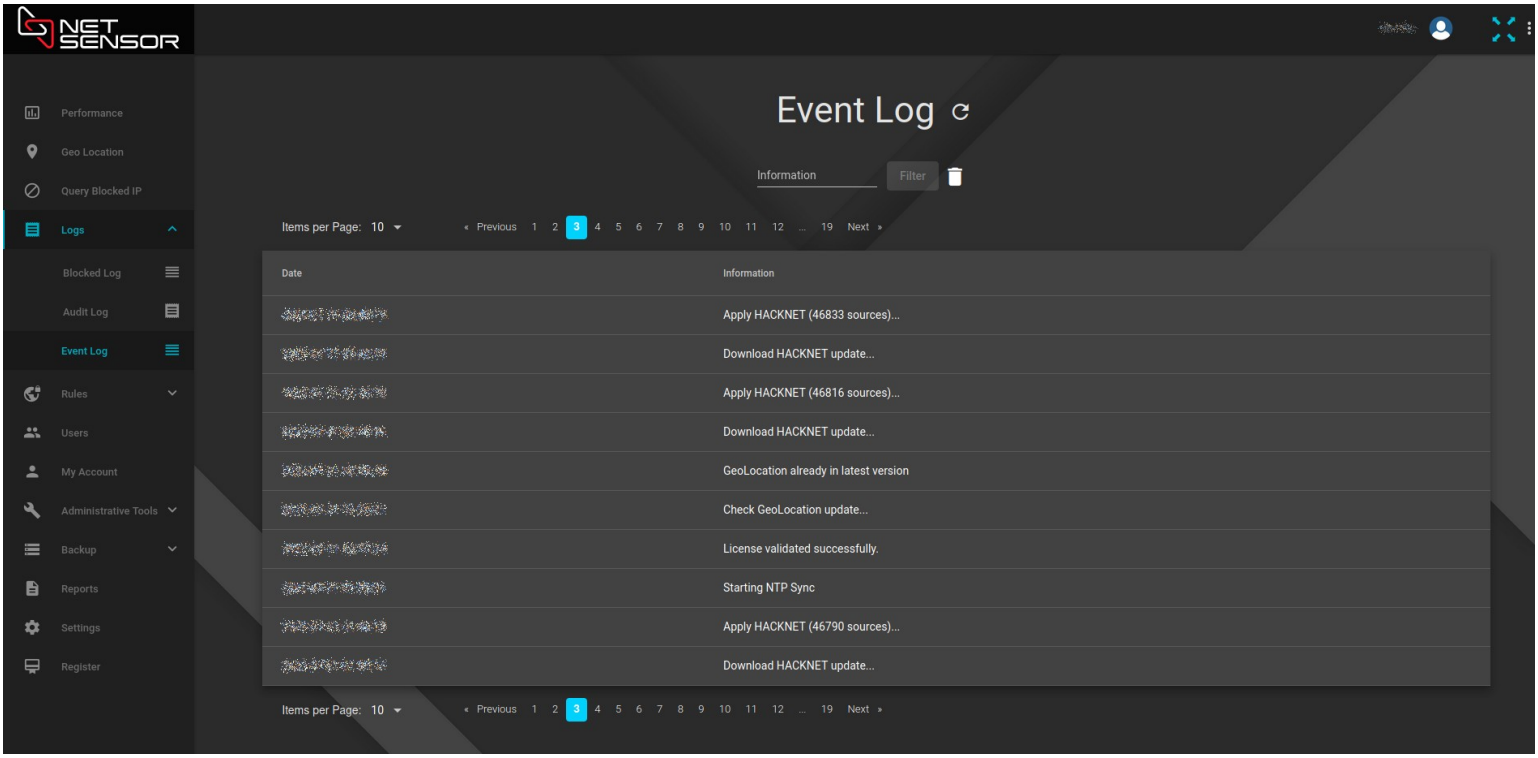
** Para evitar que um IP confiável seja bloqueado, consultar a seção de configuração: “Definição de Origens Confiáveis”.*



Log de Eventos

Abrindo o menu “Logs” e selecionando a opção “Event Log”, você poderá ver os registros dos eventos ocorridos no NETSENSOR, como sincronização de hora, validação de licenças, atualização das informações de Geo Localização e base de conhecimento da HACKNET.

Na parte superior você tem a opção de filtrar por alguma ocorrência específicas.

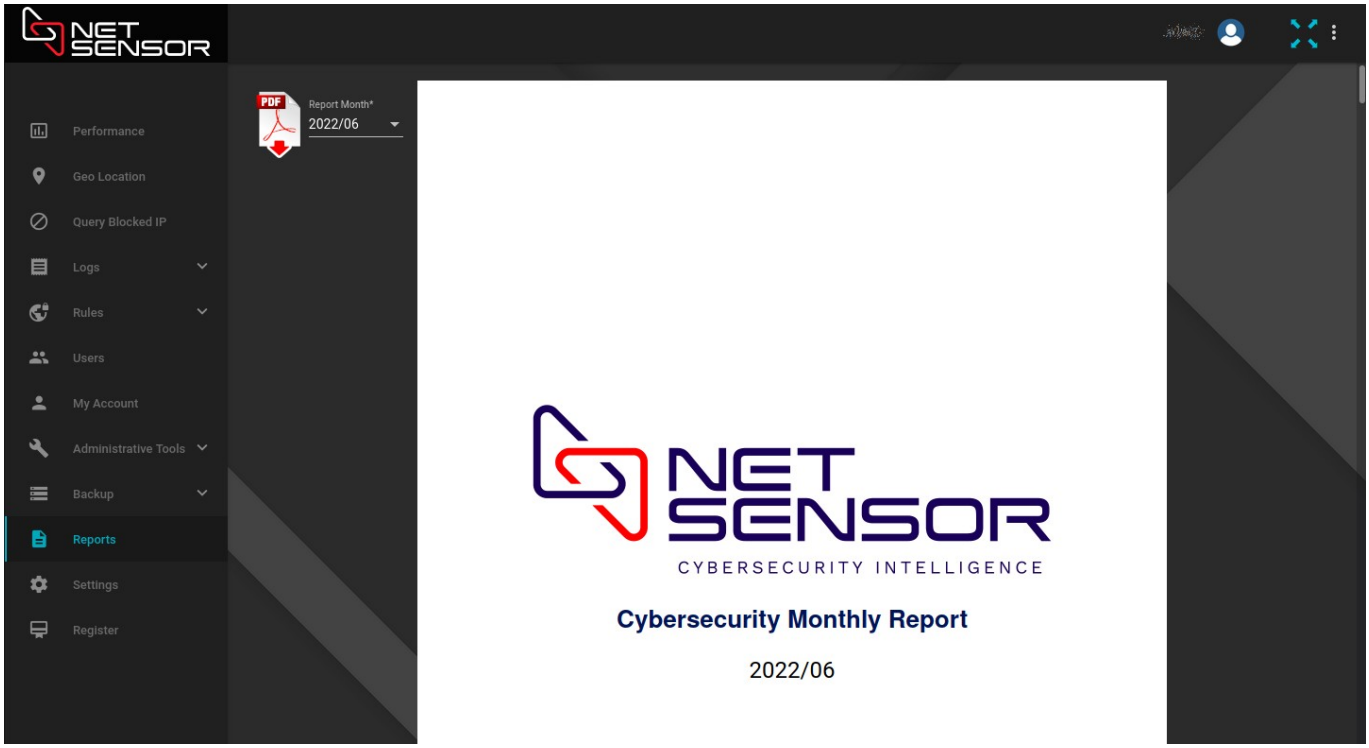


Relatórios

Na opção “Reports” você poderá ver e analisar os relatórios mensais que o NETSENSOR gera com os dados consolidados e estatísticas dos ataques identificados e bloqueados durante cada mês.

Clicando no ícone do “PDF” será feito o download do relatório em formado “.pdf”.

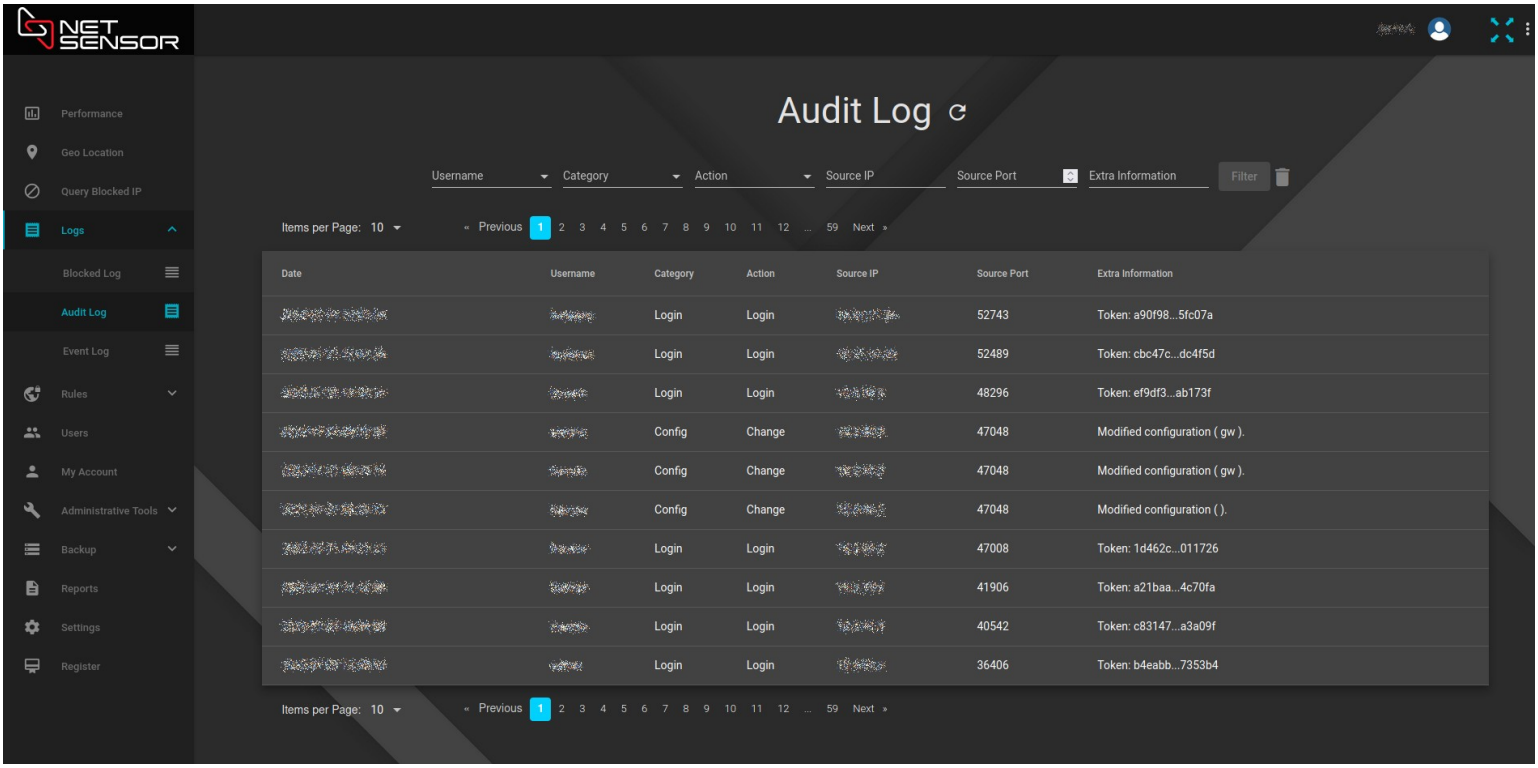
Na opção “Report Month”, ao lado do ícone do “PDF”, pode-se selecionar os relatórios de meses anteriores.



Log de Auditoria

Abrindo o menu “Logs” e selecionando a opção “Audit Log”, você poderá ver os registros de auditoria, contendo os acessos ao sistema, mudanças de configurações, manipulações de serviços e liberações de origens que estavam bloqueadas.

Na parte superior você tem diversas opções de filtro, para facilitar na busca de registros mais específicos.

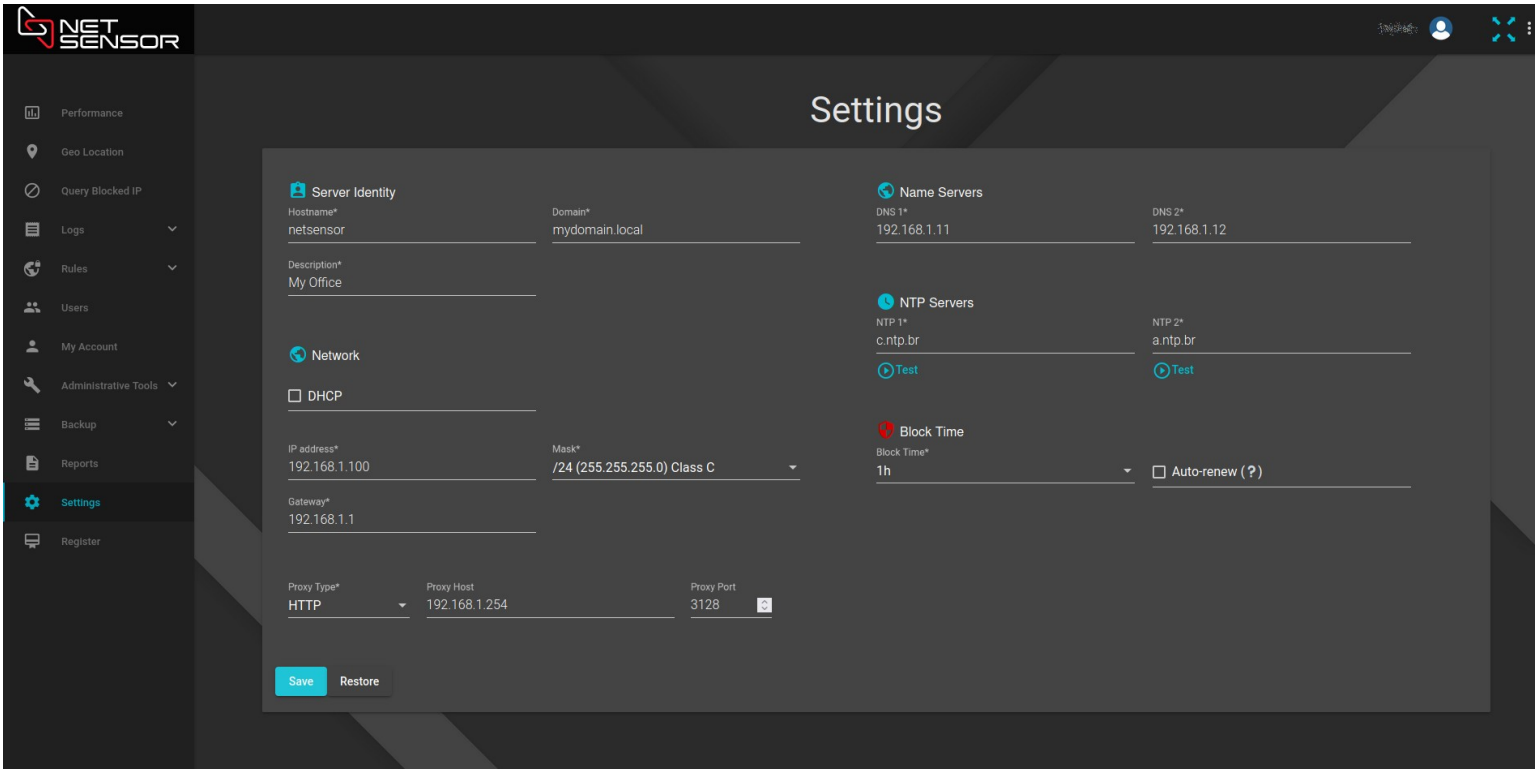


Configurações Gerais

Na opção “Settings” você tem acesso às configurações gerais do equipamento, referentes à sua identificação, configurações de rede e configurações do tempo de bloqueado.

- Server Identity: Configurações de identificação do equipamento;
- Network: Configurações de rede do equipamento e uso de proxy para acesso à internet;
- Name Servers: Servidores DNS para resolução de nomes. Podem ser internos ou na internet;
- NTP Servers: Servidores NTP para sincronismo de hora. Podem ser internos ou na internet;
- Block Time: Por quanto tempo será bloqueada uma origem que gere tráfego identificado como malicioso;
- Auto-renew: Renova o “Block Time” sempre que for visto tráfego proveniente de uma origem que encontra-se bloqueada. Com isso, uma origem que tenha deferindo tráfego considerado malicioso só terá seu bloqueio removido após ficar o tempo configurado no “Block Time” sem gerar nenhum tráfego.

** O NETSENSOR precisa de comunicação internet apenas para acessar a Cloud da sua plataforma, no endereço https://cloud.netsensor.com.br.*

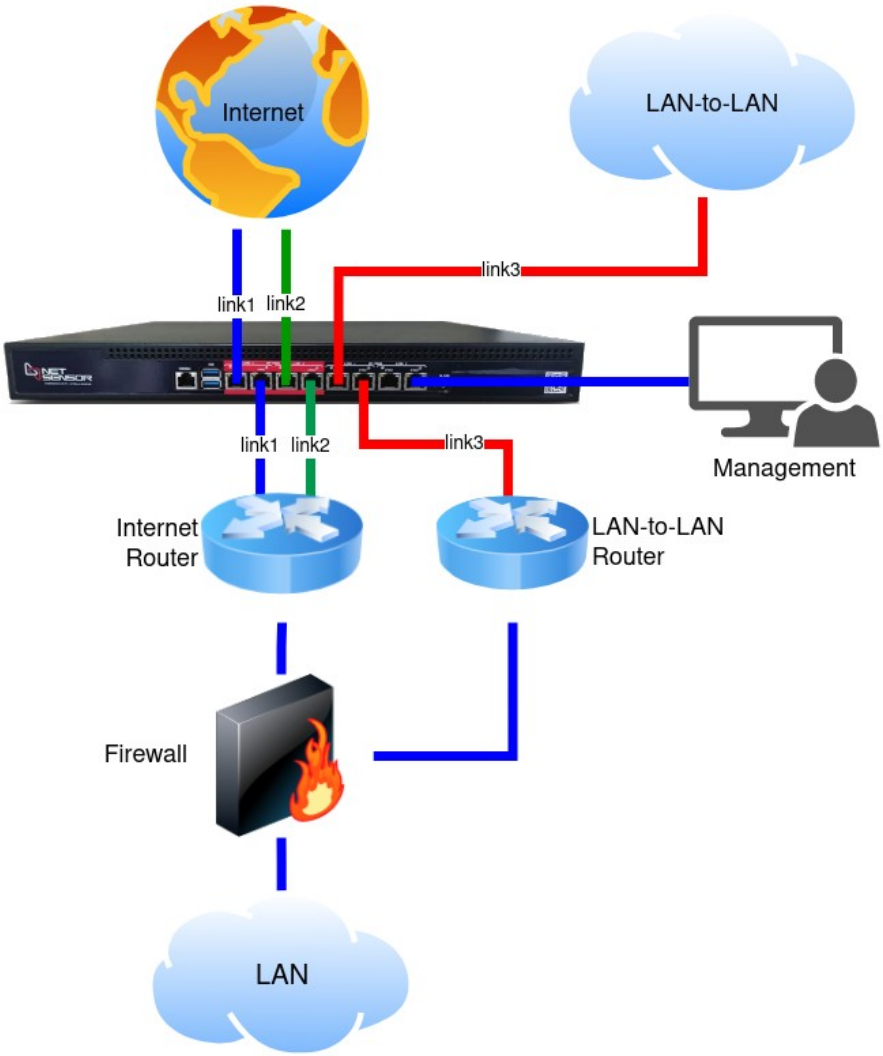


Topologia de Rede

Abaixo temos o exemplo de uma topologia envolvendo as seguintes conexões:

- link1 - Link internet da operadora A
- link2 - Link internet da operadora B
- link3 - Link LAN-to-LAN com um parceiro de negócios

O NETSENSOR foi colocado à frente de todos os equipamentos da estrutura, inclusive dos roteadores que recebem os links das operadoras. Dessa forma, o NETSENSOR consegue dar uma camada de proteção até mesmo aos equipamentos de borda da estrutura, que geralmente são mais expostos.



Sensores

O funcionamento do NETSENSOR é baseado na definição de sensores, usados como premissas para o aprendizado de origens que gerem tráfegos considerados maliciosos.

Qualquer tráfego que não deveria existir na rede, seja para porta de serviço ou para IPs/redes não usadas, pode ser usado como um sensor que identifique uma anomalia que possa oferecer risco à estrutura.

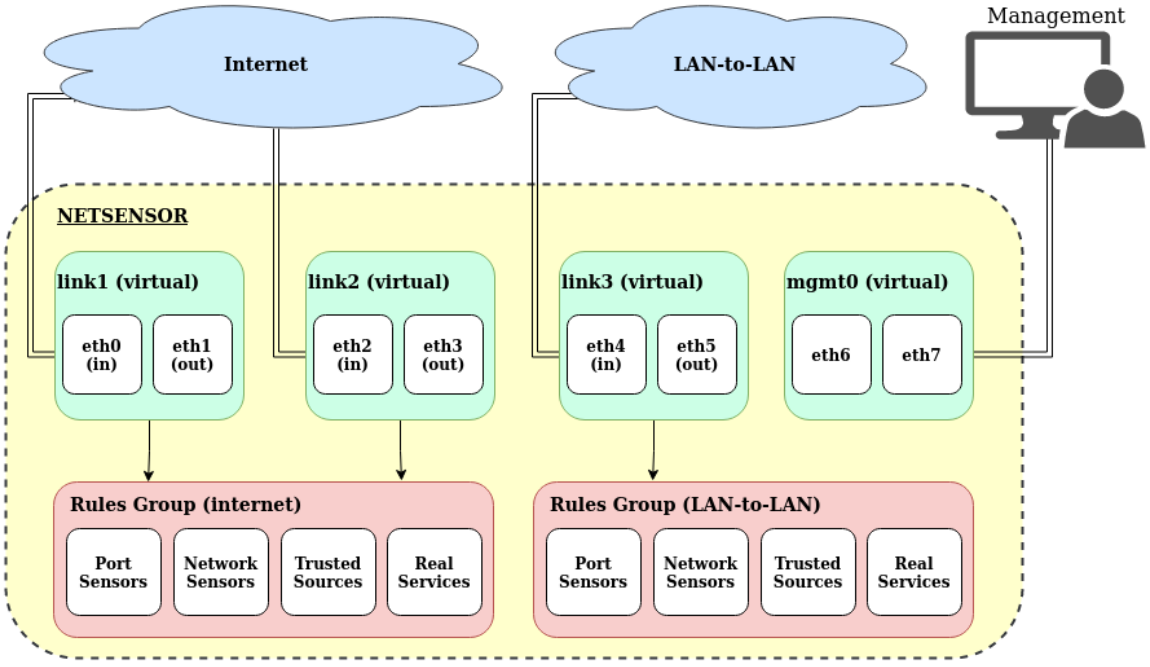
Os sensores são criados dentro de grupos de regras chamados “Rules Groups”, que facilitam e flexibilizam as configurações.

Cada “link” é associado a um “Rules Group”, o qual fará a análise do tráfego de rede.

Os tráfegos que chegarem na porta “In” de cada interface “link” do equipamento serão monitorados pelos sensores definidos no “Rules Group” usado para proteger aquele “link”.

As ações possíveis para um sensor podem ser:

- Block: A origem do tráfego considerado malicioso será bloqueada pelo tempo configurado na seção “Settings” do equipamento.
- Simulate: Irá registrar o evento considerado malicioso mas não irá bloquear a origem. É útil nos casos onde não se tem certeza se o serviço existe na rede e não se sabe o impacto que a ação de “Block” poderia causar no ambiente. Depois de aprender com os casos registrados, pode-se tomar uma decisão mais precisa sobre remover o sensor ou modificá-lo para a ação “Block”.



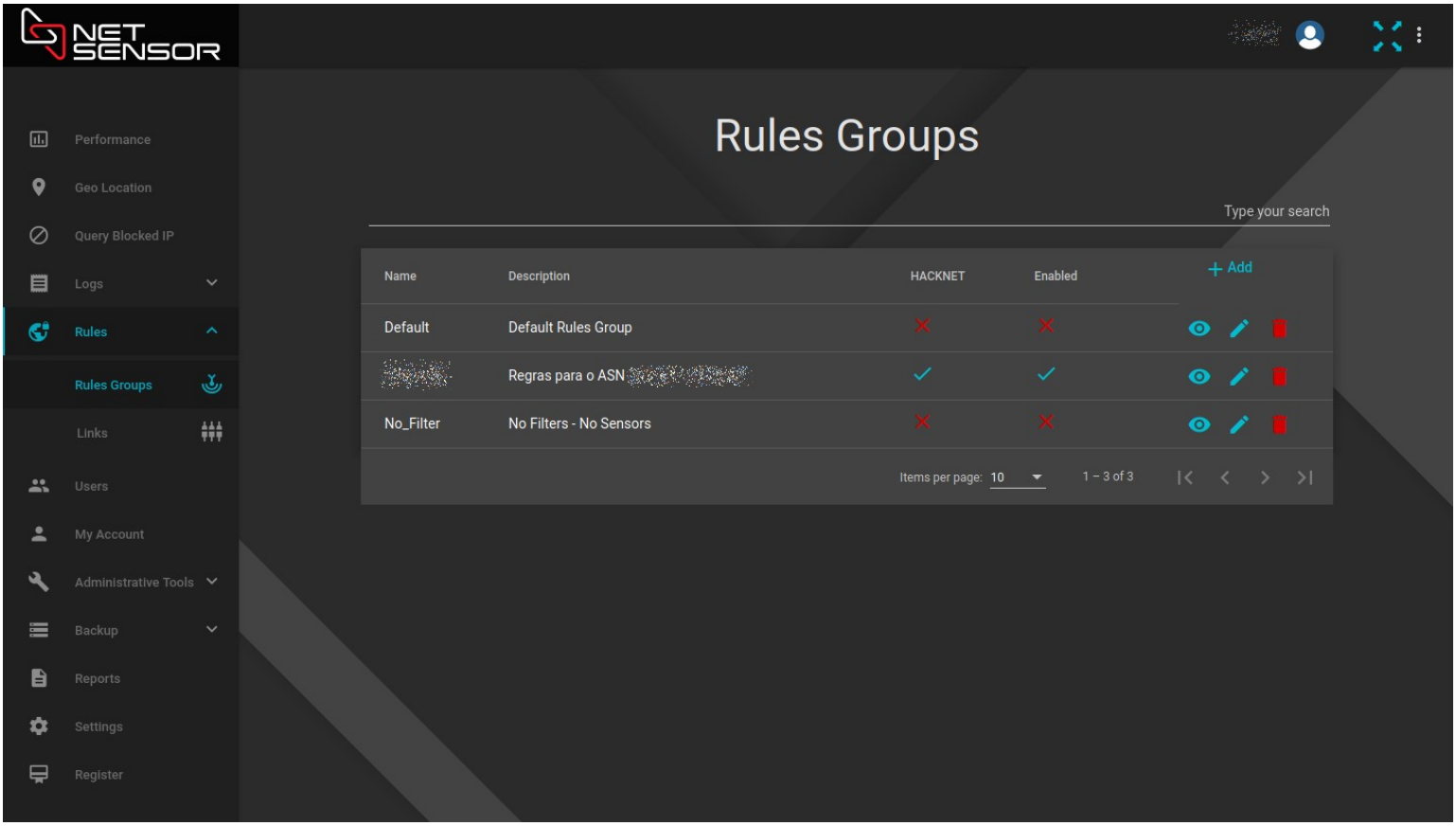
Grupos de Regras

Abrindo o menu “Rules” e selecionando à opção “Rules Groups”, você terá acesso a todos os grupos de regras existentes no equipamento.

Os grupos de regras são usados para definir sensores que possibilitem a identificação de tráfegos não legítimos e que podem ser considerados como maliciosos.

O NETSENSOR já vem com um grupo chamado “Default”, que trás uma série de sensores de exemplo.

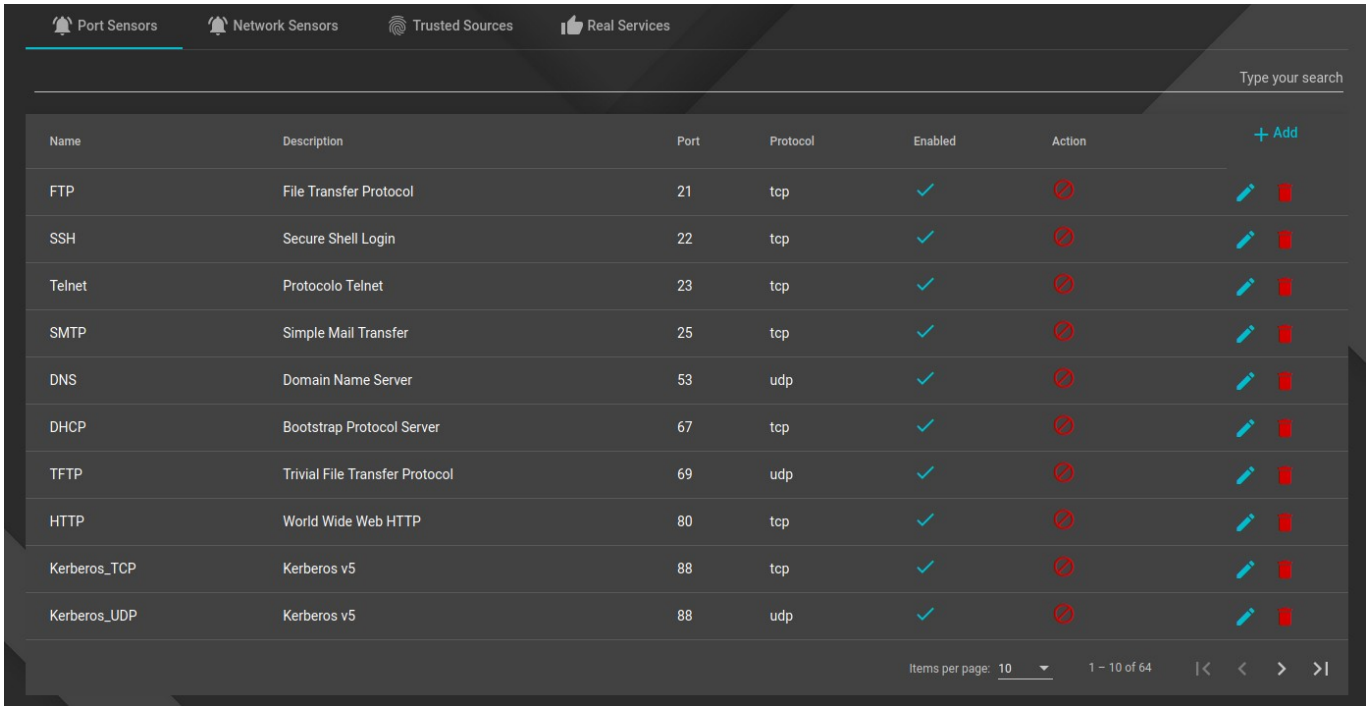
Para ver os sensores existentes em um grupo, basta clicar na respectiva linha ou no ícone do “olho”.



Sensores de Porta

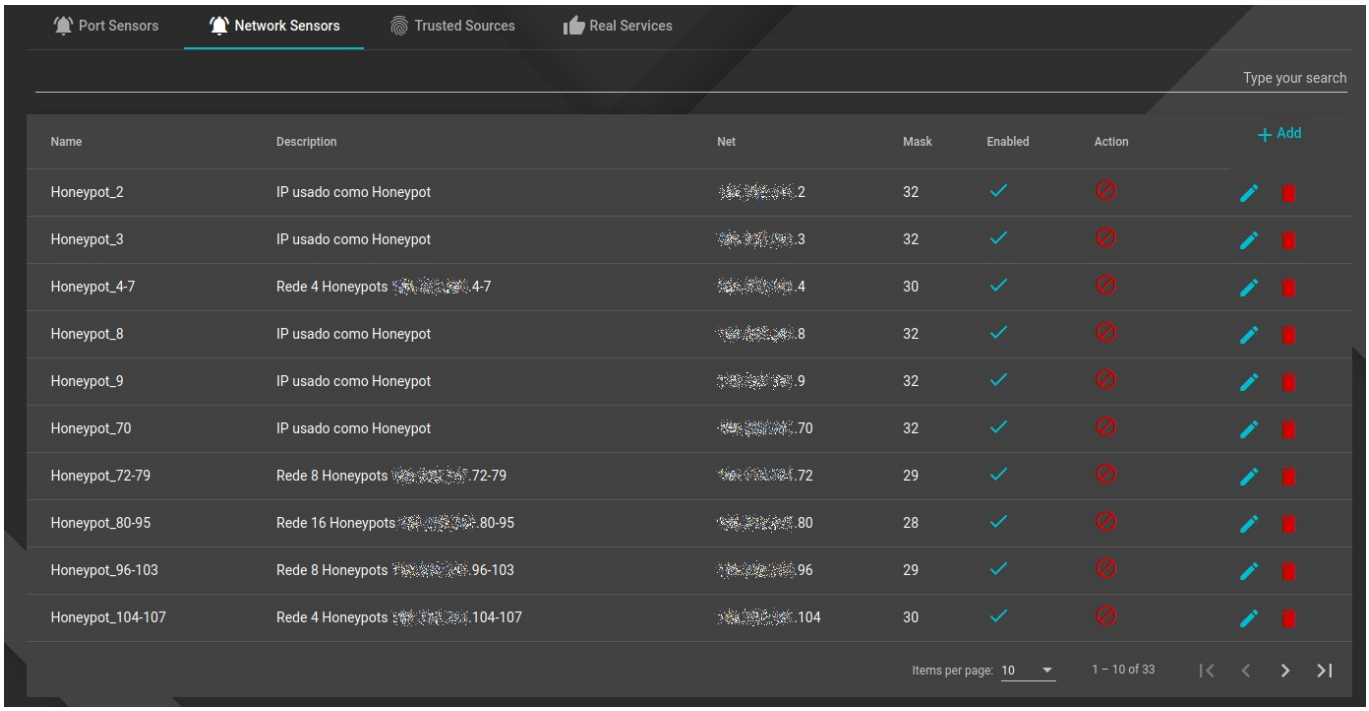
Abrindo um “Rules Group” se tem acesso à configuração dos sensores de porta. Eles são usados para monitorar tráfegos destinados a portas de serviços que não deveriam chegar na sua rede.
Qualquer tráfego destinado a esses sensores indica uma anomalia que pode ser considera como um tráfego malicioso.

O NETSENSOR já vem com um grupo chamado “Default”, que trás uma série de sensores de exemplo.



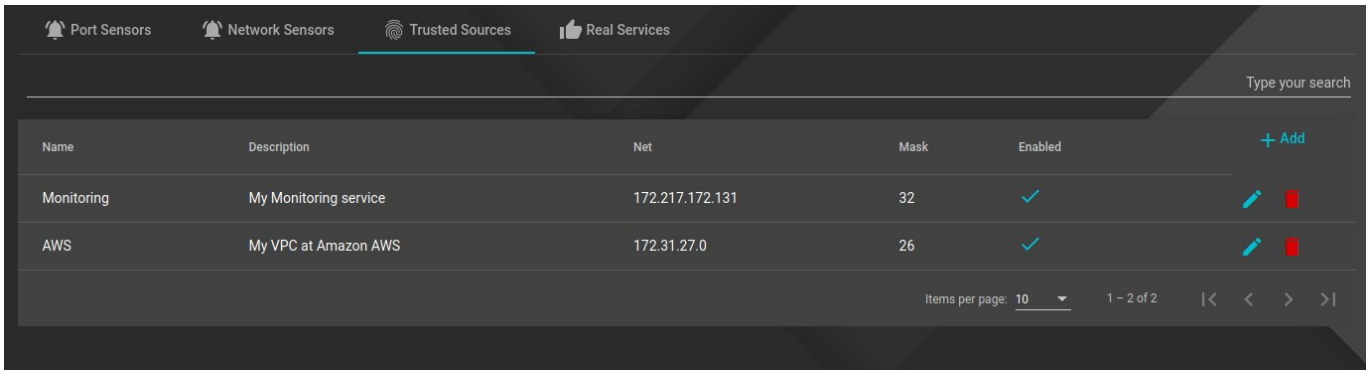
Sensores de Rede

Abrindo um “Rules Group” se tem acesso à configuração dos sensores de rede. Eles são usados para monitorar tráfegos destinados a IPs ou redes que não estejam em uso, para os quais não deveria chegar nenhuma requisição.
Qualquer tráfego destinado a esses sensores indica uma anomalia que pode ser considera como um tráfego malicioso.



Origens Confiáveis

Abrindo um “Rules Group” se tem acesso à configuração de origens confiáveis. Elas são usadas para definir endereços de origem que você conhece, confia plenamente e não quer que ela seja bloqueada em hipótese alguma, independentemente de qualquer tráfego que ela venha a gerar e qualquer sensor que ela poderia vir a disparar.

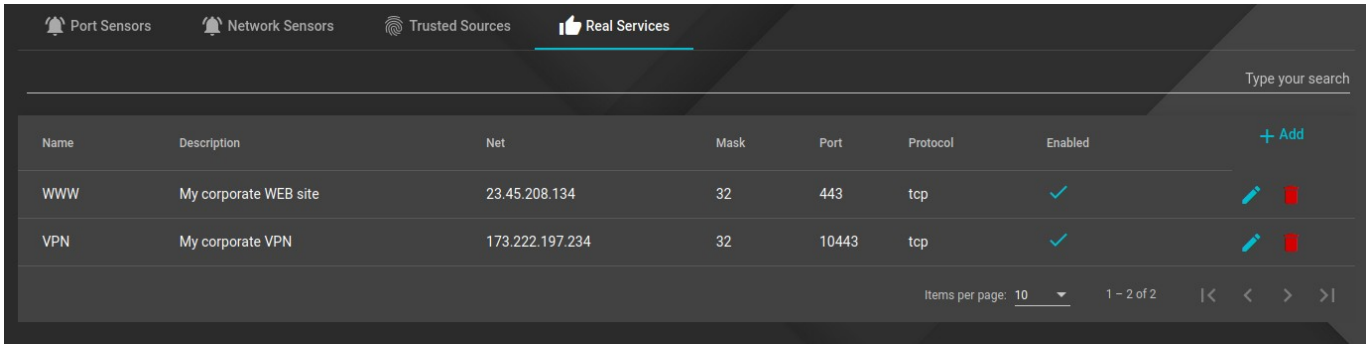


Serviços Reais

Abrindo um “Rules Group” se tem acesso à configuração de serviços reais. Eles são usados para definir serviços legítimos em sua estrutura, mas que conflitem com algum sensor de porta ou de rede que se deseje usar.

Caso você queira usar um sensor conhecido pela sua eficiência na detecção de tráfegos maliciosos como, por exemplo, Telnet, FTP, SSH ou RDP, mas você tem esse serviço em um único ponto da sua estrutura, a opção de “Serviços Reais” pode ser usada para tratar isso.
Nesse caso, você configura normalmente o sensor desejado e, então, especifica o serviço legítimo que deve ser tratado como uma exceção e não deve disparar o sensor.

A mesma configuração pode ser usada para especificar uma exceção em um IP ou rede que se queira usar como “Sensor de Rede”.



Links

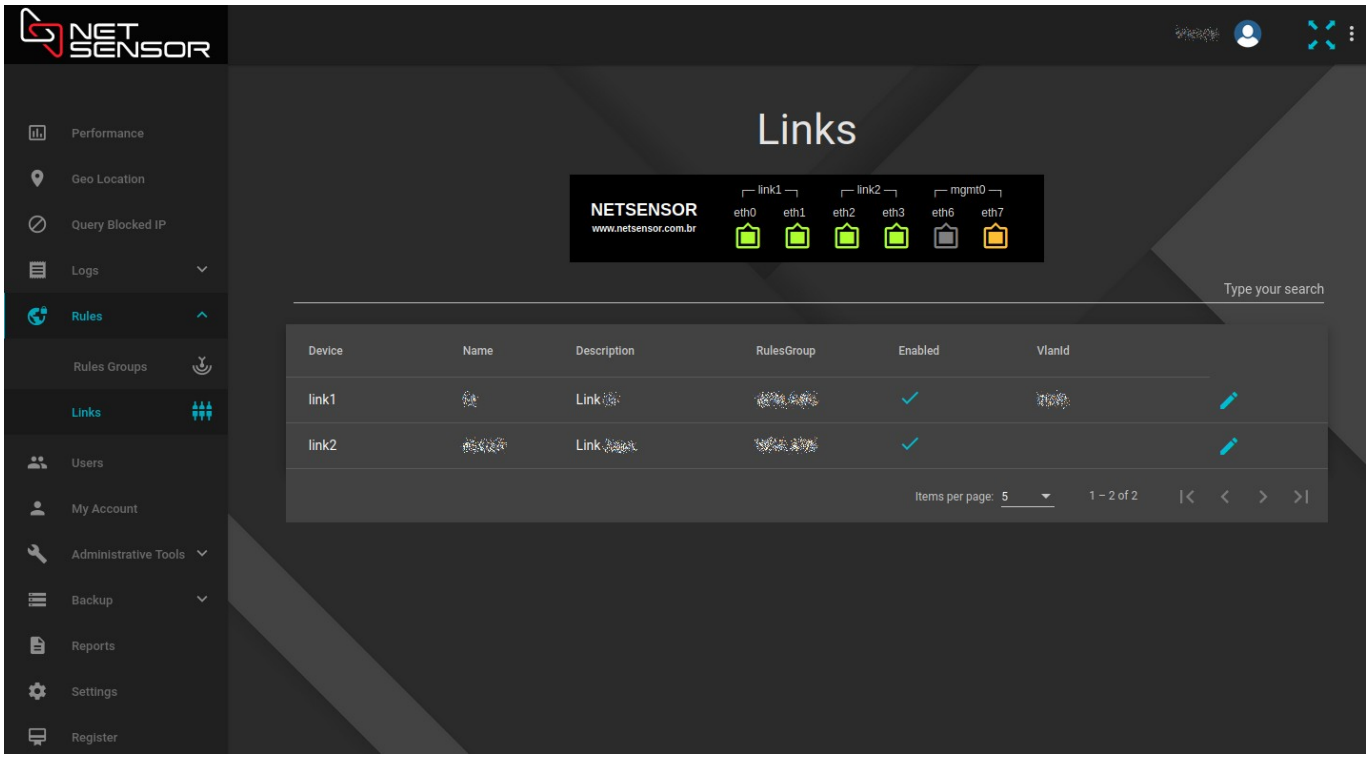
Na opção “Links” temos acesso a todas as interfaces de rede ativas no equipamento.

As interfaces de rede são agrupadas aos pares. Cada par forma uma interface lógica que recebe a nomenclatura “linkX”, onde “X” é um número de identificação crescente que inicia em “1”, representando a primeira interface do tipo “link”.

Cada interface “link” é usada para receber um link de comunicação na sua primeira interface física (In), analisar o tráfego, e encaminhar os pacotes, através da segunda interface física (Out), para o equipamento que já estava recebendo aquele link.

As interfaces “link” são totalmente independentes e, cada uma delas, pode ser protegida por um grupo de regras diferente, com sensores específicos que façam sentido para aquele link de dados.

As duas últimas interfaces físicas do equipamento formam uma interface lógica chamada “mgmt0”, usada para gerenciamento e comunicação do equipamento.
A “mgmt0” é a única interface com endereçamento de rede e a única forma possível de acesso ao equipamento. Por esse motivo, o acesso a essa interface deve ser restrito e é altamente recomendado que não seja visível na internet ou qualquer outra rede de acesso público.



Usuários

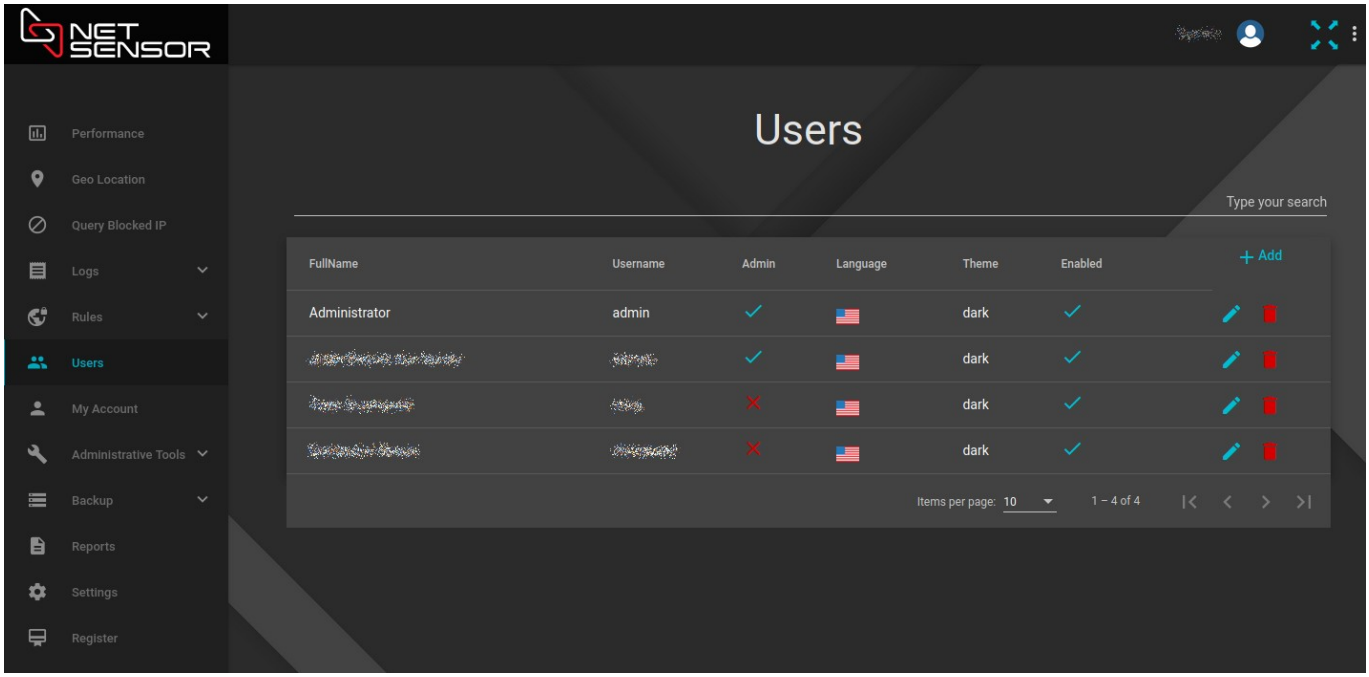
Na opção “Users” temos acesso a todos os usuários do sistema.

Os usuários podem ter privilégios de administrador ou apenas de operador do sistema:

- Administrador: Tem acesso total ao equipamento, pode modificar qualquer configuração, gerenciar usuários, sensores, interfaces de rede, manipular os serviços, fazer e restaurar backup.

- Operador: Tem acesso somente para visualizar os dashboards, consultar o log de bloqueios, log de eventos, relatórios mensais, gerenciar seu próprio usuário e remover um IP da lista de bloqueio.

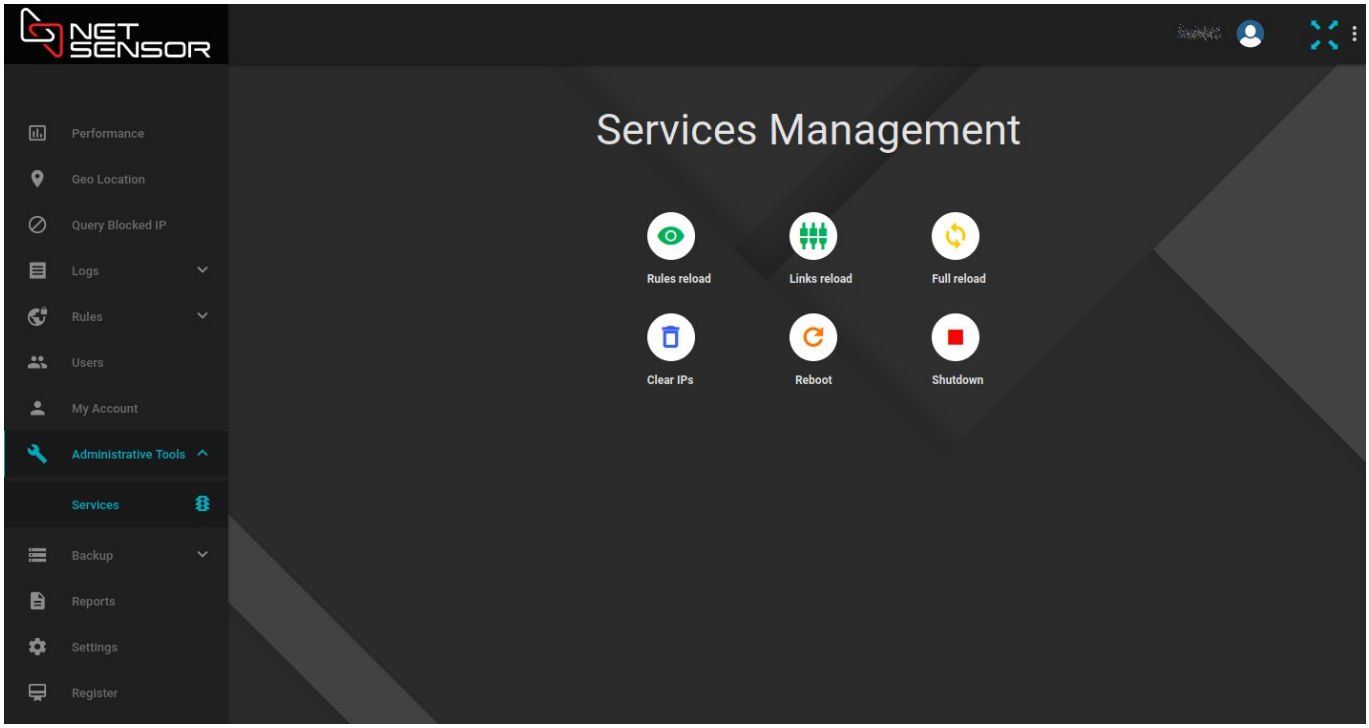
** A remoção de um IP da lista de bloqueio apenas remove o bloqueio momentâneo daquela origem. Qualquer sensor que venha a ser disparado irá causar seu bloqueio novamente.*



Serviços

Abrindo o menu “Administrative Tools” e selecionando a opção “Services”, você poderá manipular os serviços do sistema. As opções disponíveis são:

- **Rules Reload**: Atualiza as regras e sensores do sistema, aplicando todas as modificações que tenham sido realizadas;
- **Links Reload**: Atualiza as configurações dos links, incluindo o grupo de regras usado para proteger cada um deles;
- **Full Reload**: Atualiza as regras, sensores, configurações dos links, configurações de rede, sincronismo de hora, validação de licenças, atualização da base de conhecimento da HACKNET e de Geo Localização;
- **Clear IPS**: Remove todos os IPs que encontram-se bloqueados;
- **Reboot**: Reinicia o equipamento;
- **Shutdown**: Desliga o equipamento. Dependendo do modelo do equipamento ele pode ser ligado automaticamente após o shutdown.

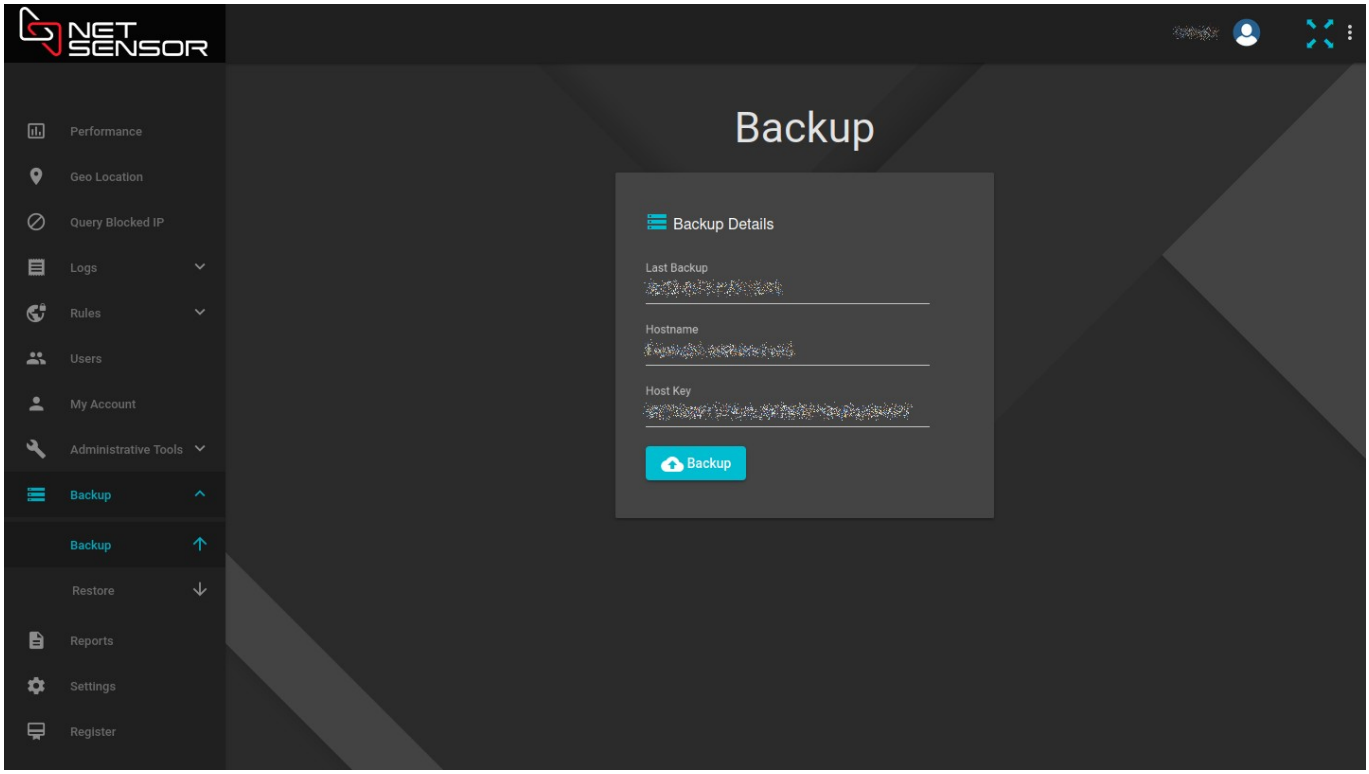


Backup

Abrindo o menu “Backup” e selecionando a opção “Backup”, você poderá ver quando foi realizado o último procedimento de backup do equipamento e poderá realizar um novo backup, com as configurações atuais, clicando no botão “Backup” e confirmando a ação.

O backup sempre é associado à chave de identificação do equipamento físico (Host Key).

Para maior segurança e facilidade dos processos de backup e restore, o conteúdo dos backups são armazenados na Cloud da NETSENSOR, protegidos por criptografia.

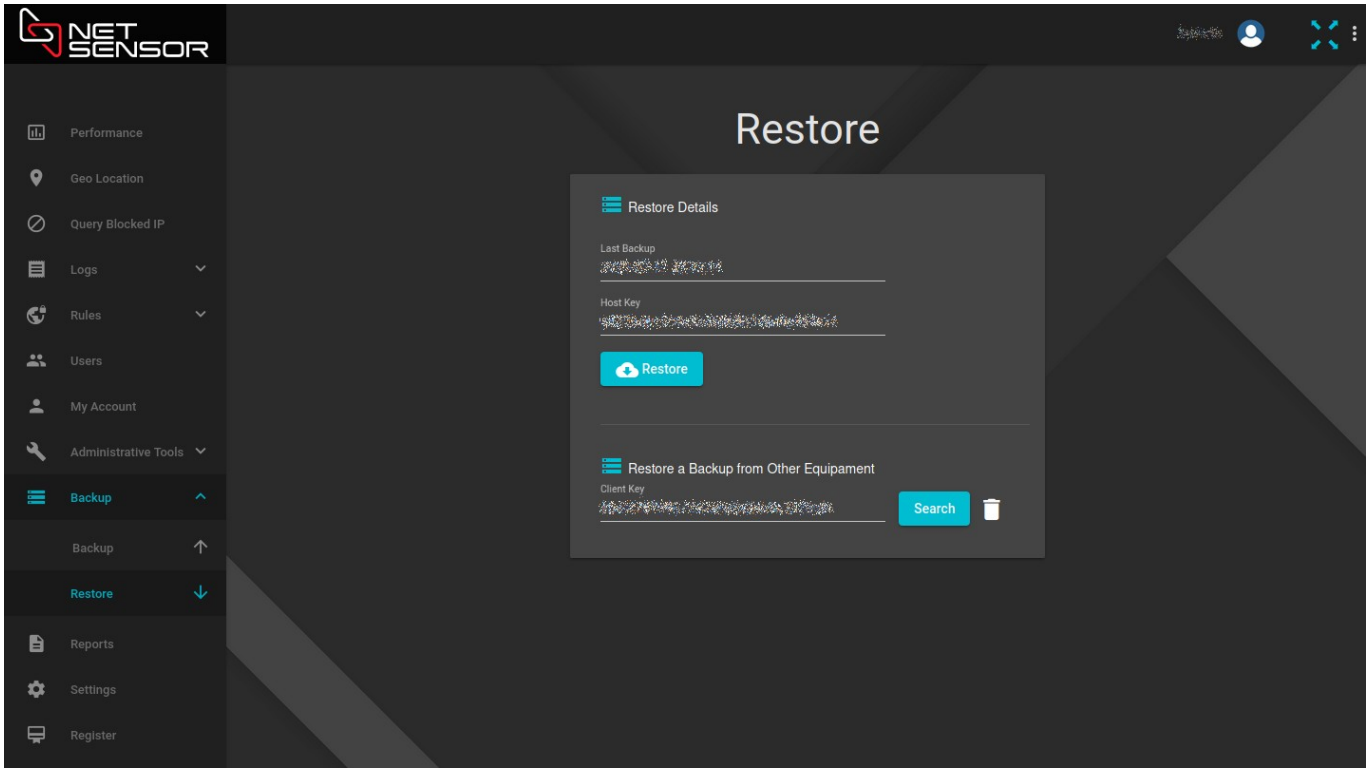


Restauração de Backup

Abrindo o menu “Backup” e selecionando a opção “Restore”, você poderá ver quando foi realizado o último procedimento de backup do equipamento e poderá restaurar esse backup clicando no botão “Restore” e confirmando a ação.

O backup sempre é associado à chave de identificação do equipamento físico (Host Key).

Para maior segurança e facilidade dos processos de backup e restore, o conteúdo dos backups são armazenados na Cloud da NETSENSOR, protegidos por criptografia.



Logo abaixo do botão “Restore” existe uma segunda sessão, destinada à restauração de backups de outros equipamentos físicos. Essa opção é útil, principalmente, quando se substitui um equipamento e se deseja restaurar o backup das configurações do equipamento anterior.

A busca por backups de outros equipamentos é feita usando a chave de identificação do cliente, a qual dá acesso aos backups de todos os equipamentos que ele possui.

Se o equipamento já estiver vinculado a uma chave de cliente nas configurações de licença, o campo da chave será preenchido automaticamente. Caso contrário, basta inserir a chave do cliente.
Clique no botão “Search”, para pesquisar os backups disponíveis para restauração.

Após realizar a pesquisa na Cloud da NETSENSOR, serão mostrados todos os backups de equipamentos do cliente que estão disponíveis para restauração.

Para restaurar um dos backups disponíveis, basta clicar no ícone da “nuvem” referente ao equipamento que se deseja restaurar o backup e confirmar a ação.