



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.

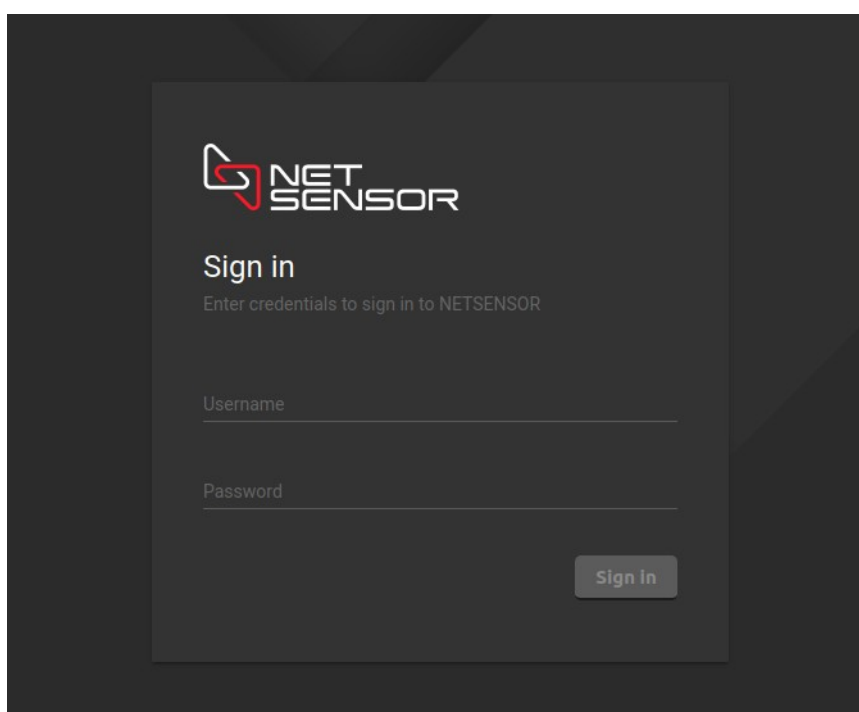
Utilizando conceitos de inteligência artificial (machine learning) esta solução, de forma proativa e sem intervenção humana, é capaz de observar de forma totalmente transparente o tráfego internet, identificar padrões presentes na grande maioria dos ataques cibernéticos e os bloquear já em suas fases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



The screenshot shows a dark-themed web interface for NET SENSOR. At the top left is the NET SENSOR logo. Below it, the text "Sign in" is displayed, followed by the instruction "Enter credentials to sign in to NETSENSOR". There are two input fields: "Username" and "Password". A "Sign in" button is located at the bottom right of the form area.

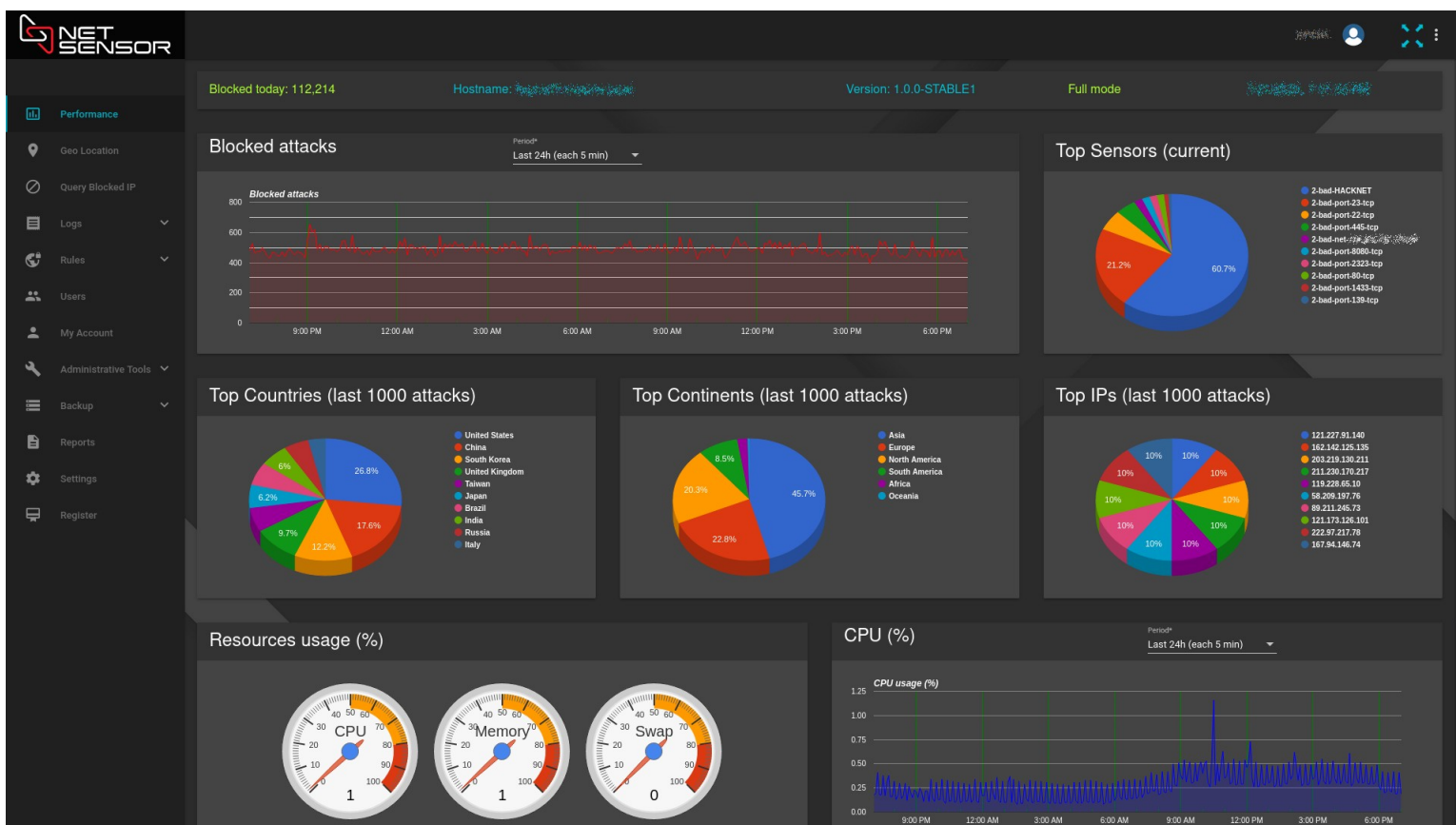
## Dashboard de Desempenho

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.

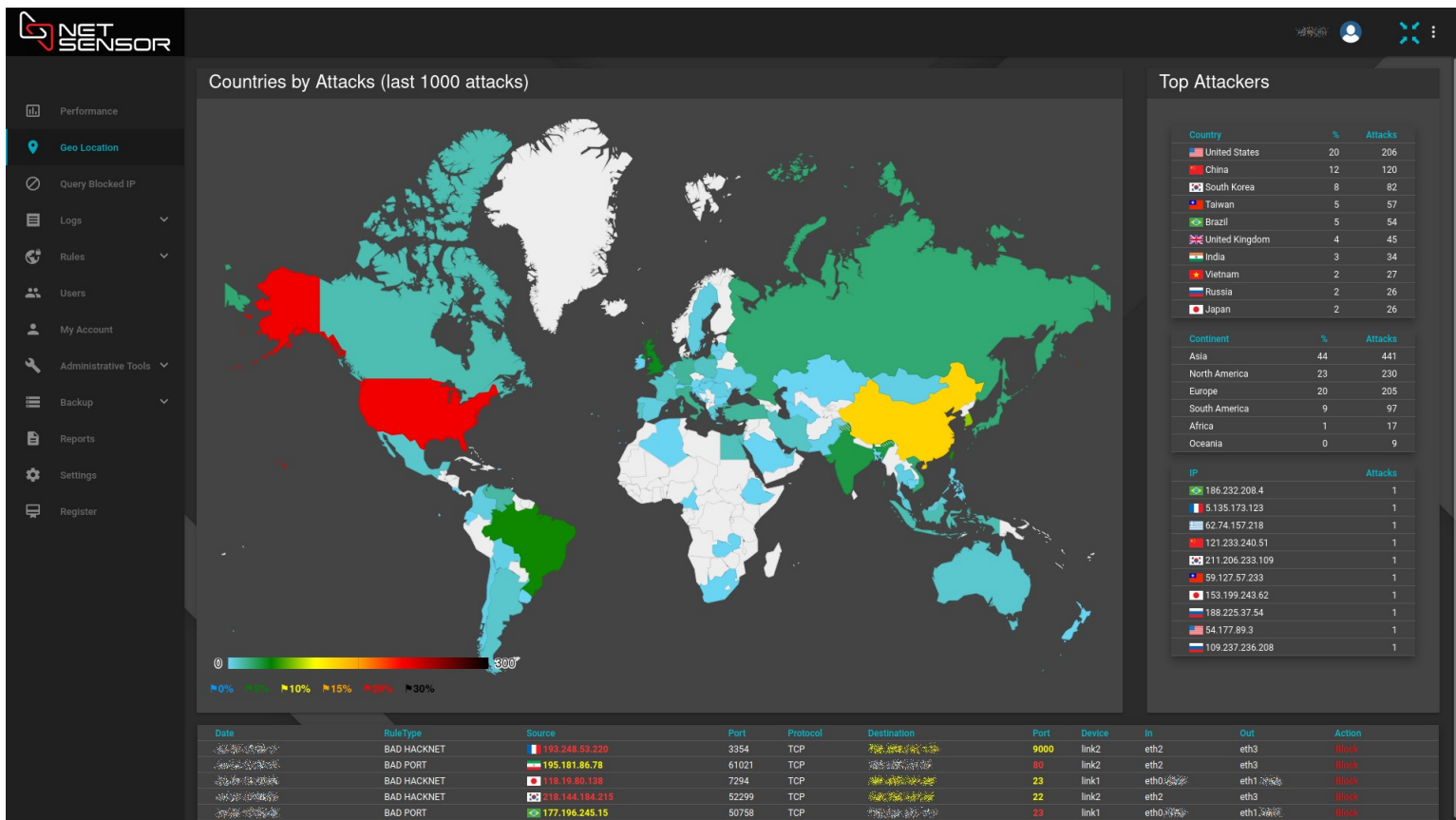


## Dashboard de Geo Localização

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 tentando explorar.

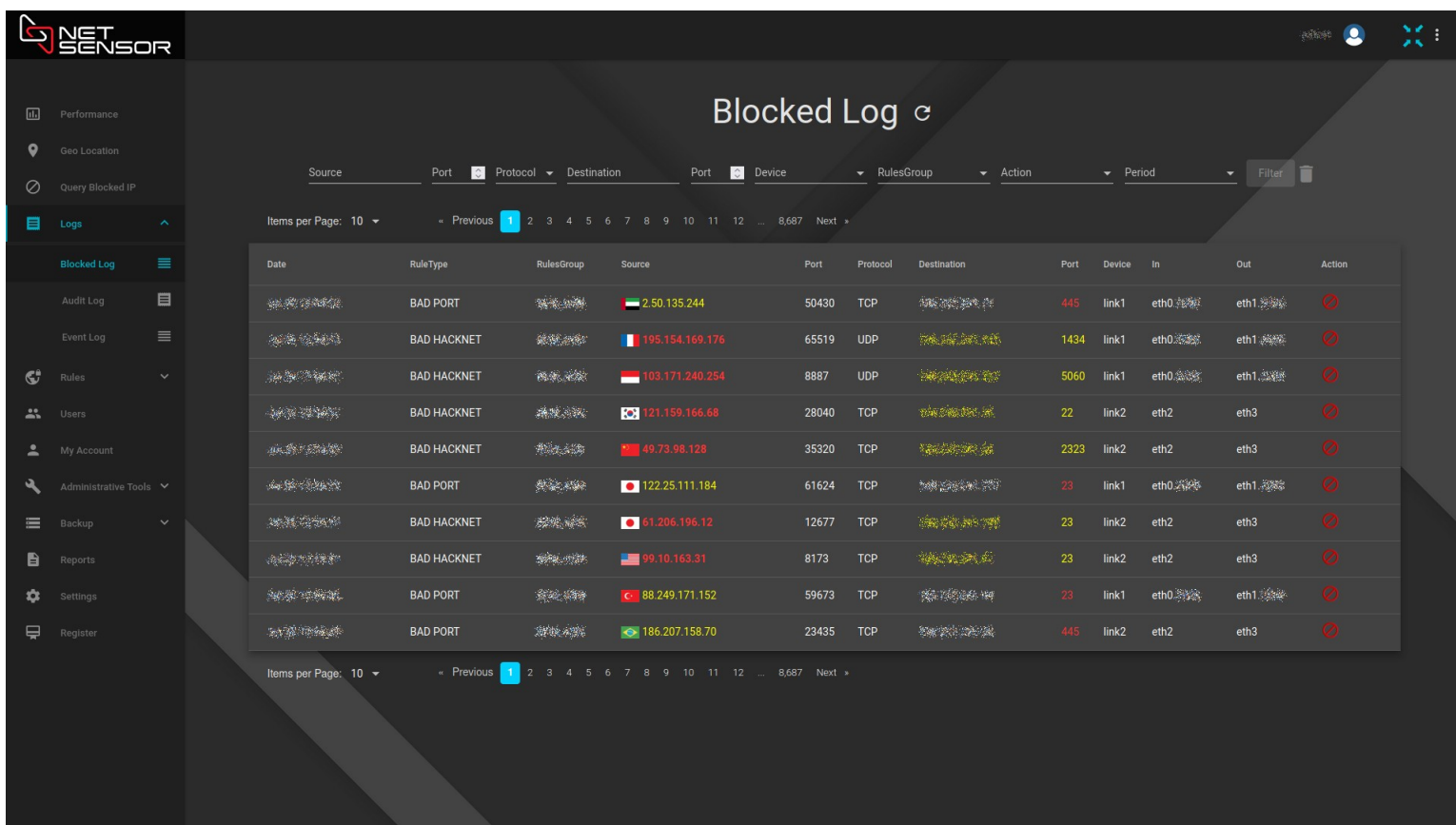


## Log de Bloqueios

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.



Date	RuleType	RulesGroup	Source	Port	Protocol	Destination	Port	Device	In	Out	Action
	BAD PORT		2.50.135.244	50430	TCP		445	link1	eth0	eth1	
	BAD HACKNET		195.154.169.176	65519	UDP		1434	link1	eth0	eth1	
	BAD HACKNET		103.171.240.254	8887	UDP		5060	link1	eth0	eth1	
	BAD HACKNET		121.159.166.68	28040	TCP		22	link2	eth2	eth3	
	BAD HACKNET		49.73.98.128	35320	TCP		2323	link2	eth2	eth3	
	BAD PORT		122.25.111.184	61624	TCP		23	link1	eth0	eth1	
	BAD HACKNET		61.206.196.12	12677	TCP		23	link2	eth2	eth3	
	BAD HACKNET		99.10.163.31	8173	TCP		23	link2	eth2	eth3	
	BAD PORT		88.249.171.152	59673	TCP		23	link1	eth0	eth1	
	BAD PORT		186.207.158.70	23435	TCP		445	link2	eth2	eth3	

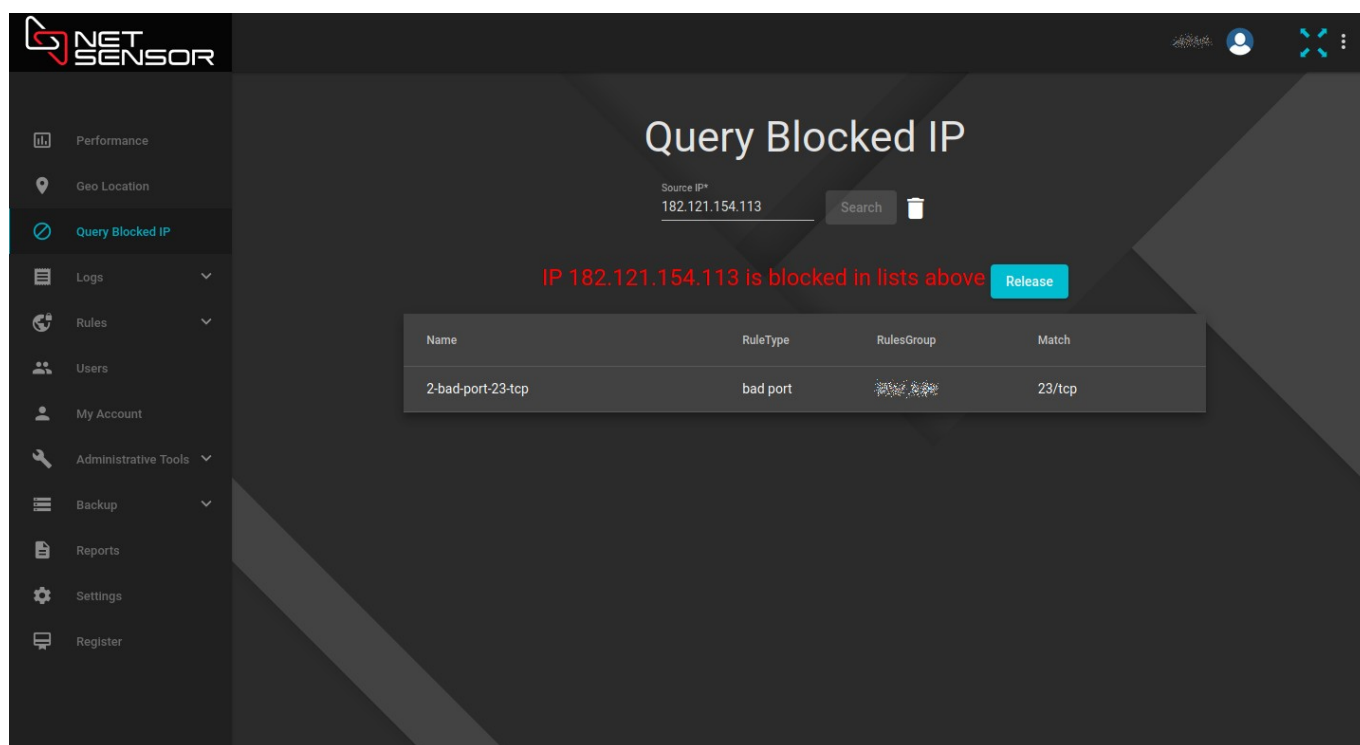
## Consulta e liberação de IPs bloqueados

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”.*



The screenshot shows the NET SENSOR web interface. The main heading is "Query Blocked IP". Below it, there is a search bar with "Source IP\*" and the value "182.121.154.113". A "Search" button and a trash icon are also present. Below the search bar, a message states "IP 182.121.154.113 is blocked in lists above" with a "Release" button. A table below shows the search results:

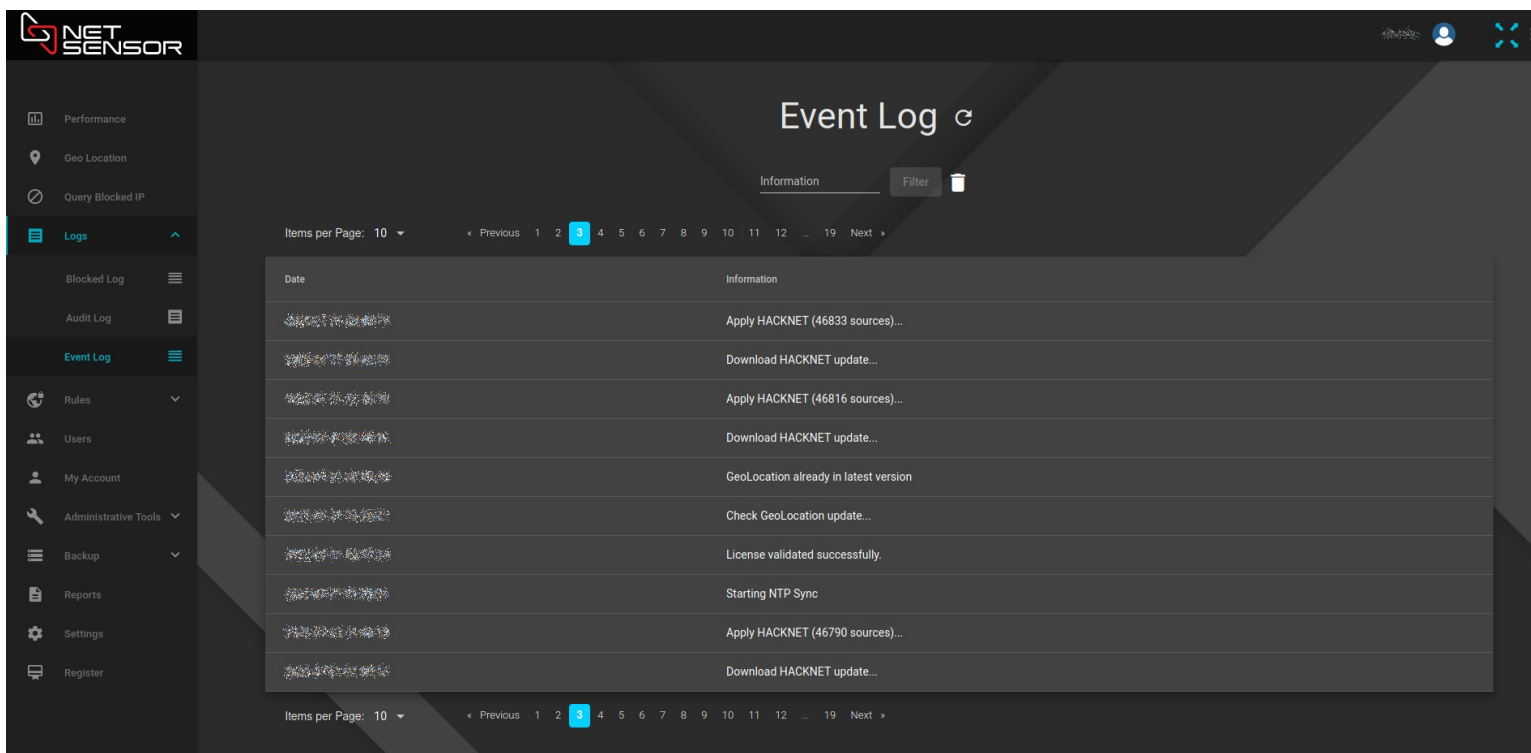
Name	RuleType	RulesGroup	Match
2-bad-port-23-tcp	bad port		23/tcp



## 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.



The screenshot shows the NET SENSOR web interface. On the left is a navigation sidebar with the following menu items: Performance, Geo Location, Query Blocked IP, Logs (highlighted), Blocked Log, Audit Log, Event Log (highlighted), Rules, Users, My Account, Administrative Tools, Backup, Reports, Settings, and Register. The main content area is titled "Event Log" and includes a search bar with "Information" entered and a "Filter" button. Below the search bar is a pagination control showing "Items per Page: 10" and a list of page numbers from 1 to 19, with page 3 selected. The event log table has two columns: "Date" and "Information". The table contains the following entries:

Date	Information
2023-07-20 10:00:00	Apply HACKNET (46833 sources)...
2023-07-20 10:00:00	Download HACKNET update...
2023-07-20 10:00:00	Apply HACKNET (46816 sources)...
2023-07-20 10:00:00	Download HACKNET update...
2023-07-20 10:00:00	GeoLocation already in latest version
2023-07-20 10:00:00	Check GeoLocation update...
2023-07-20 10:00:00	License validated successfully.
2023-07-20 10:00:00	Starting NTP Sync
2023-07-20 10:00:00	Apply HACKNET (46790 sources)...
2023-07-20 10:00:00	Download HACKNET update...

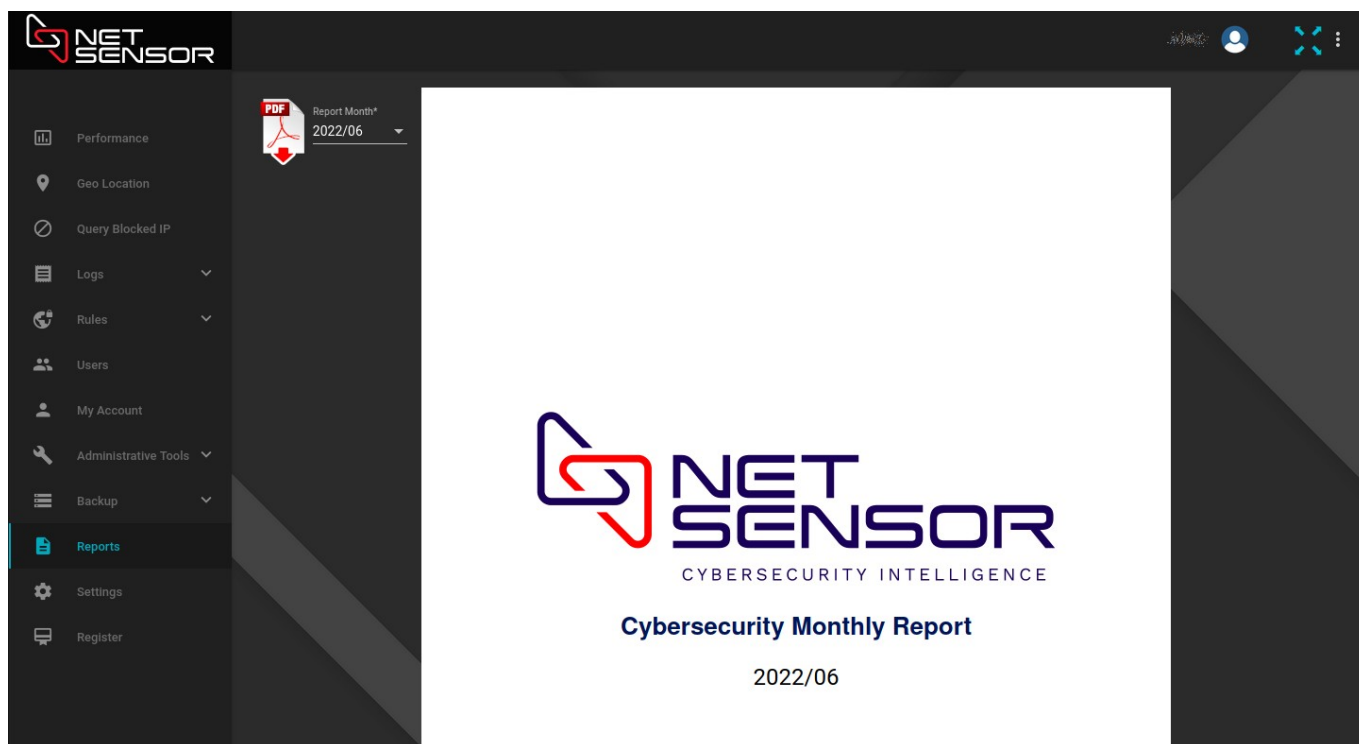
At the bottom of the table, there is another pagination control showing "Items per Page: 10" and a list of page numbers from 1 to 19, with page 3 selected.

## 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 formato “.pdf”.

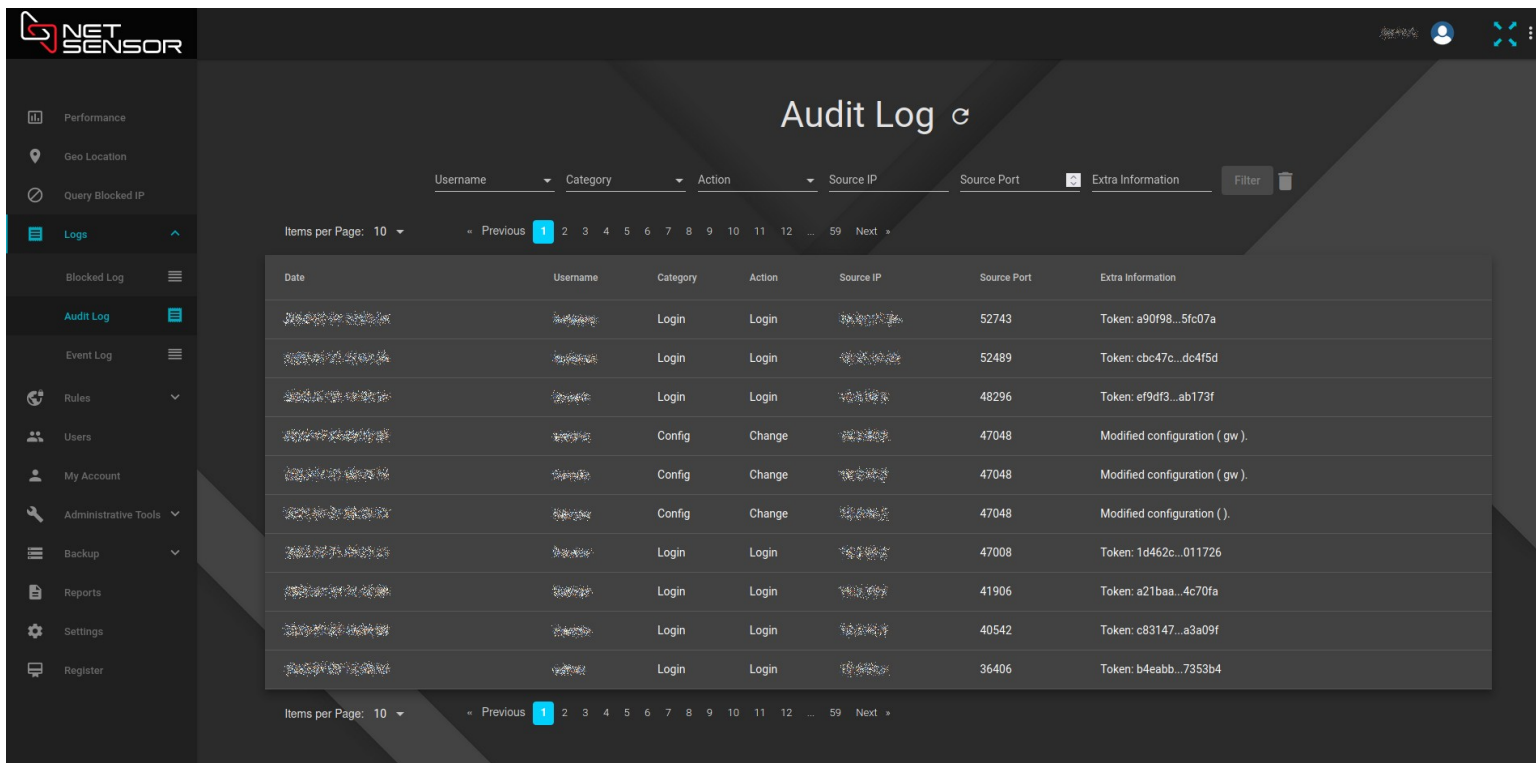
Na opção “Report Month”, ao lado do ícone do “PDF”, pode-se selecionar os relatórios de meses anteriores.



## 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.



The screenshot shows the NET SENSOR web interface. The left sidebar contains a navigation menu with items: Performance, Geo Location, Query Blocked IP, Logs (selected), Blocked Log, Audit Log (selected), Event Log, Rules, Users, My Account, Administrative Tools, Backup, Reports, Settings, and Register. The main content area is titled "Audit Log" and features a table of audit records. Above the table are filter options for Username, Category, Action, Source IP, Source Port, and Extra Information, along with a Filter button. Below the table are pagination controls showing "Items per Page: 10" and a page number "1" selected.

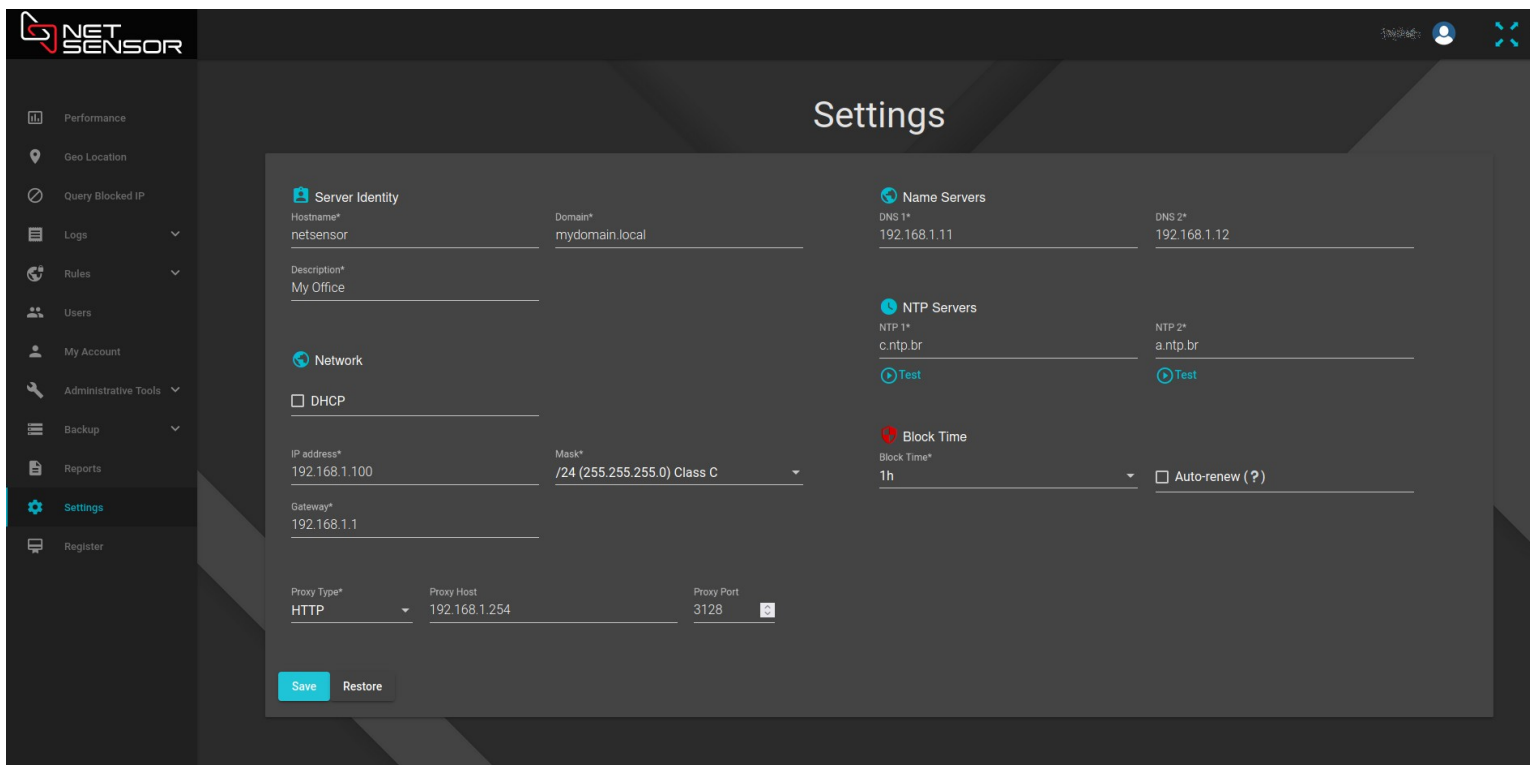
Date	Username	Category	Action	Source IP	Source Port	Extra Information
2023-10-27 10:10:10	admin	Login	Login	192.168.1.1	52743	Token: a90f98...5fc07a
2023-10-27 10:10:10	admin	Login	Login	192.168.1.1	52489	Token: cbc47c...dc4f5d
2023-10-27 10:10:10	admin	Login	Login	192.168.1.1	48296	Token: ef9df3...ab173f
2023-10-27 10:10:10	admin	Config	Change	192.168.1.1	47048	Modified configuration ( gw ).
2023-10-27 10:10:10	admin	Config	Change	192.168.1.1	47048	Modified configuration ( gw ).
2023-10-27 10:10:10	admin	Config	Change	192.168.1.1	47048	Modified configuration ( ).
2023-10-27 10:10:10	admin	Login	Login	192.168.1.1	47008	Token: 1d462c...011726
2023-10-27 10:10:10	admin	Login	Login	192.168.1.1	41906	Token: a21baa...4c70fa
2023-10-27 10:10:10	admin	Login	Login	192.168.1.1	40542	Token: c83147...a3a09f
2023-10-27 10:10:10	admin	Login	Login	192.168.1.1	36406	Token: b4eaab...7353b4

## 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>.



The screenshot displays the 'Settings' page of the NET SENSOR web interface. The left sidebar contains navigation options: Performance, Geo Location, Query Blocked IP, Logs, Rules, Users, My Account, Administrative Tools, Backup, Reports, Settings (highlighted), and Registrar. The main content area is titled 'Settings' and is divided into several sections:

- Server Identity:** Hostname\* (netsensor), Domain\* (mydomain.local), Description\* (My Office).
- Network:** DHCP (unchecked), IP address\* (192.168.1.100), Mask\* (/24 (255.255.255.0) Class C), Gateway\* (192.168.1.1).
- Name Servers:** DNS 1\* (192.168.1.11), DNS 2\* (192.168.1.12).
- NTP Servers:** NTP 1\* (c.ntp.br), NTP 2\* (a.ntp.br), with 'Test' buttons for each.
- Block Time:** Block Time\* (1h), Auto-renew (?) (unchecked).
- Proxy:** Proxy Type\* (HTTP), Proxy Host (192.168.1.254), Proxy Port (3128).

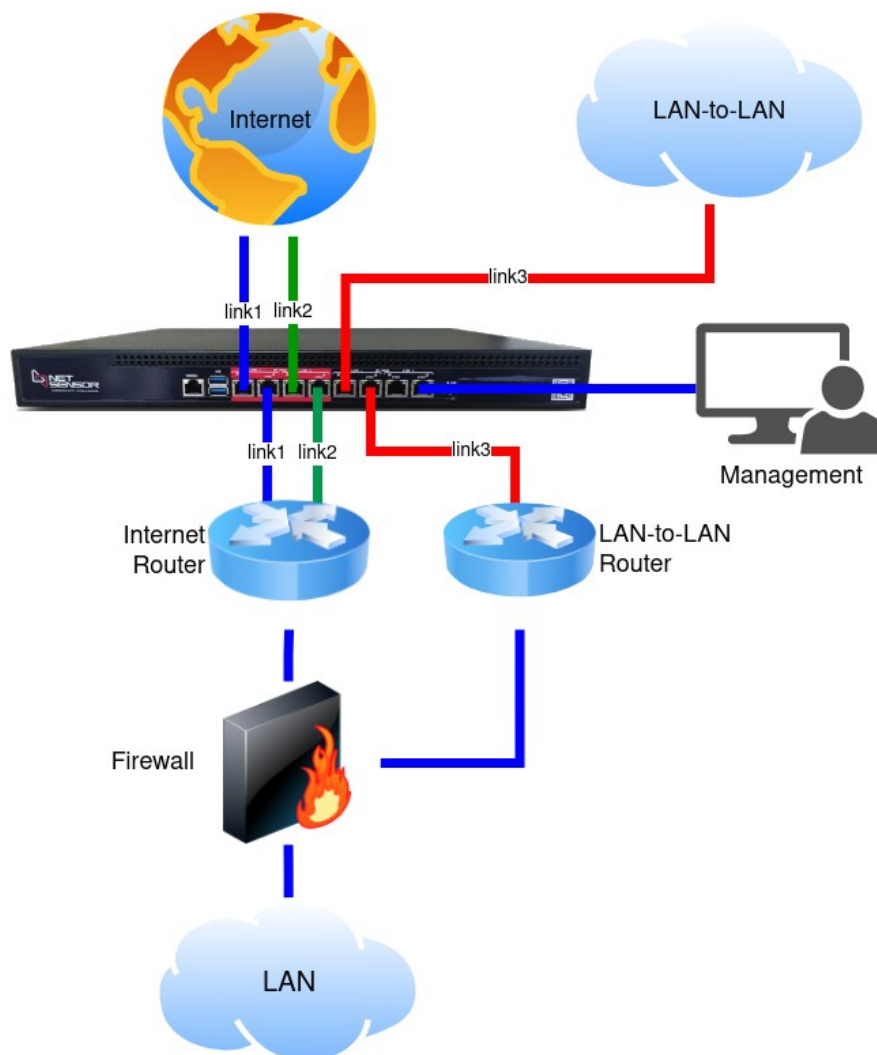
At the bottom of the settings panel are 'Save' and 'Restore' buttons.

## 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.

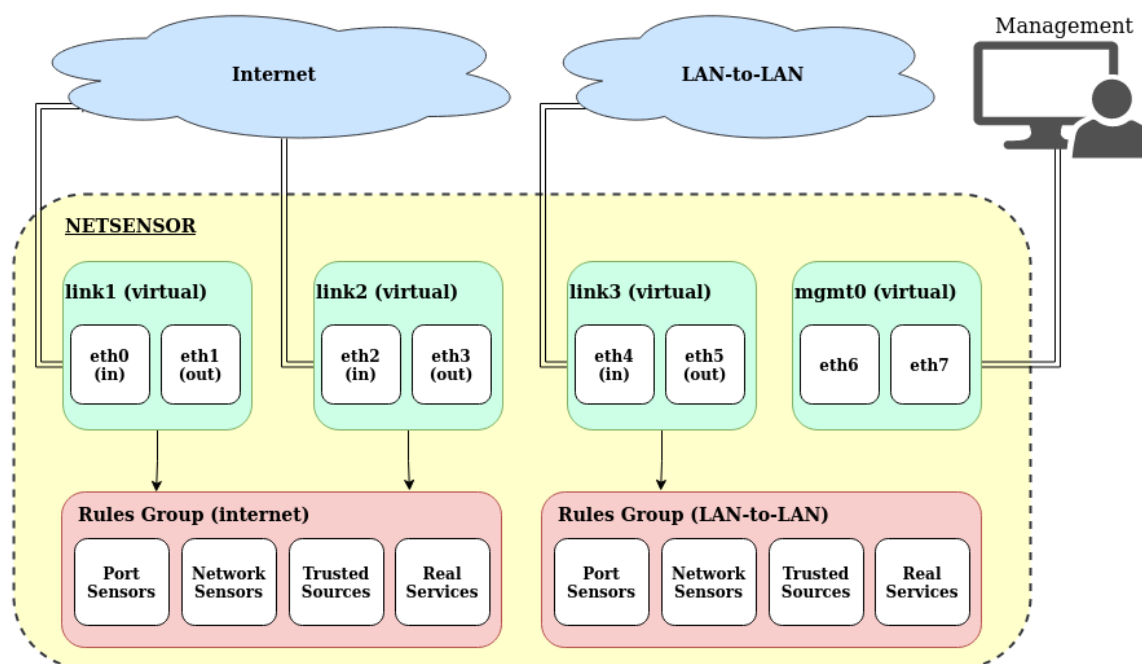
Os sensores são criados dentro de grupos de regras chamados “Rules Groups”, que facilitam e flexibilizam as configurações.

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”.



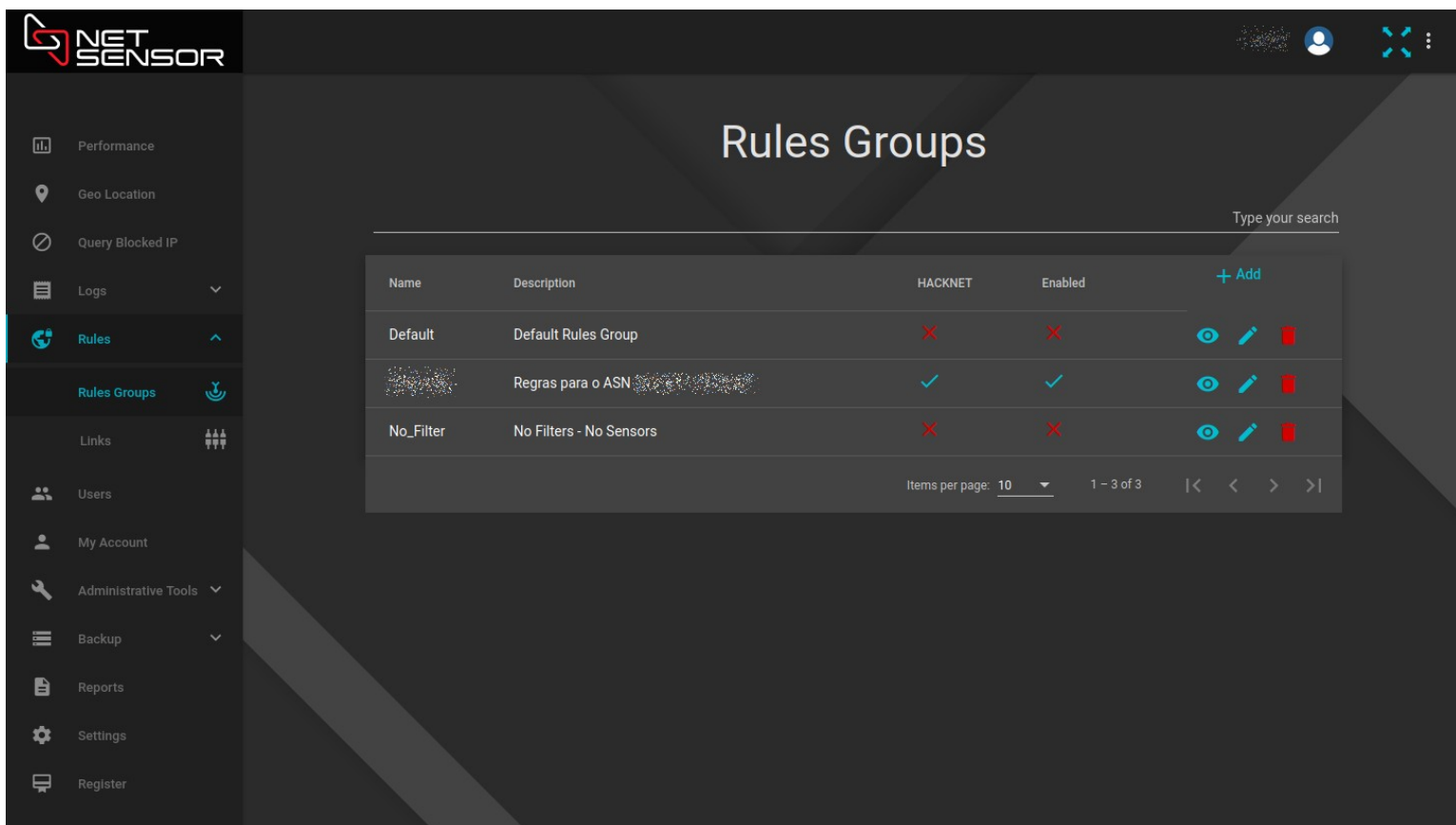
## Grupos de Regras

Abrindo o menu “Rules” e selecionando a 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”.



The screenshot shows the 'Rules Groups' page in the NET SENSOR interface. The page title is 'Rules Groups'. Below the title is a search bar with the placeholder text 'Type your search'. A table displays the following data:

Name	Description	HACKNET	Enabled	+ Add
Default	Default Rules Group	×	×	  
Regras para o ASN	Regras para o ASN	✓	✓	  
No_Filter	No Filters - No Sensors	×	×	  

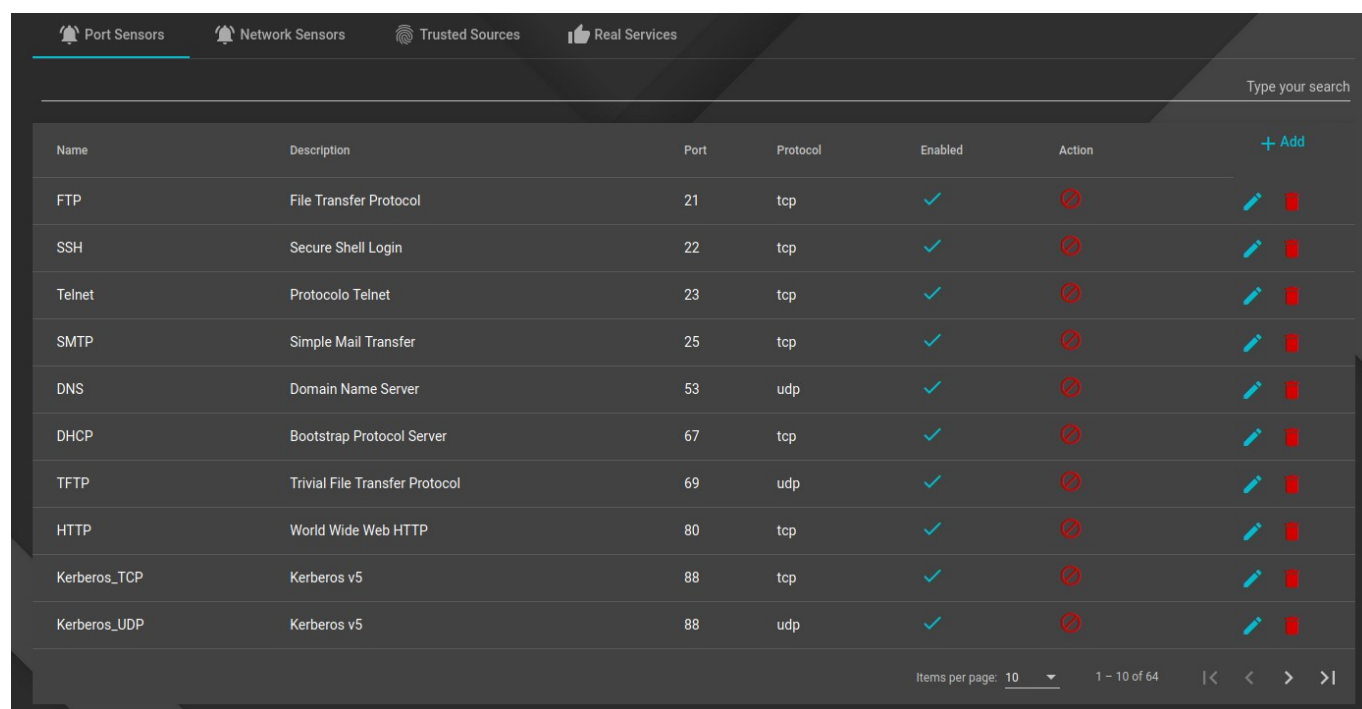
At the bottom of the table, there is a pagination control showing 'Items per page: 10' and '1 - 3 of 3'.





















## 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 considerada como um tráfego malicioso.

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



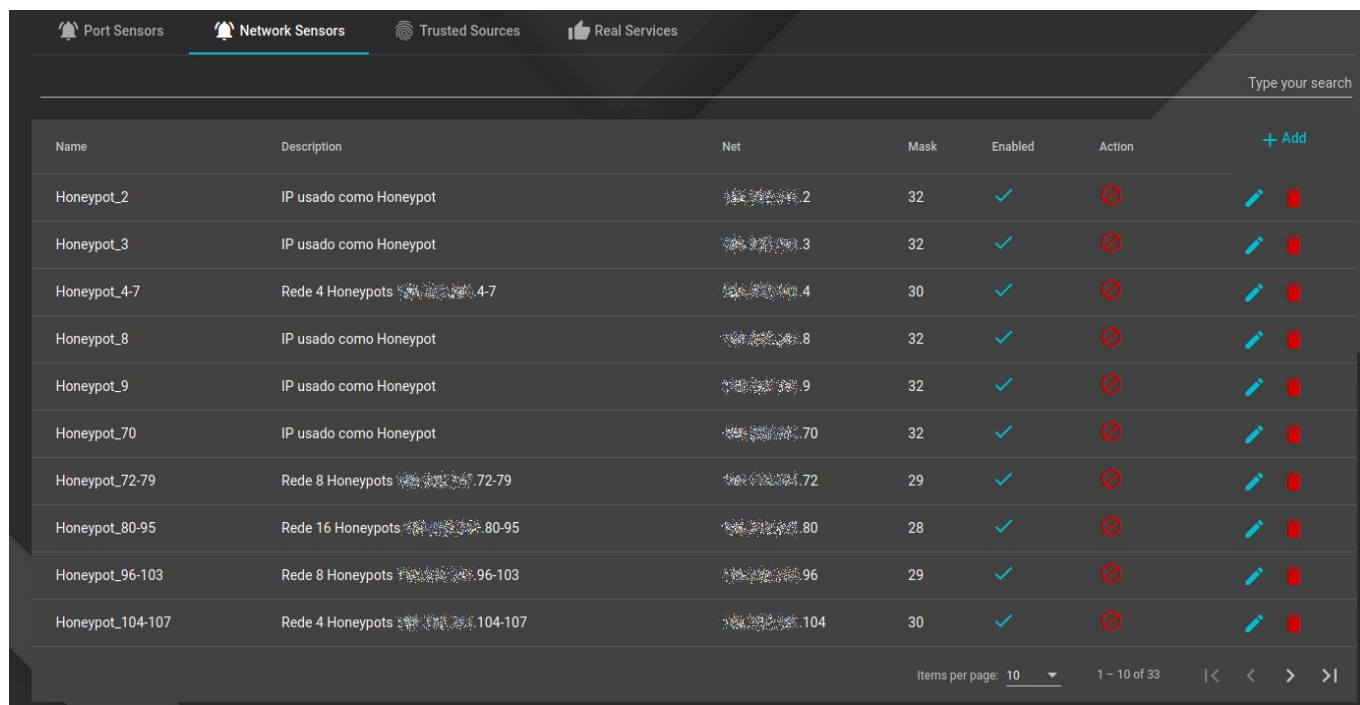
Name	Description	Port	Protocol	Enabled	Action	+ Add
FTP	File Transfer Protocol	21	tcp	✓	⊗	 
SSH	Secure Shell Login	22	tcp	✓	⊗	 
Telnet	Protocolo Telnet	23	tcp	✓	⊗	 
SMTP	Simple Mail Transfer	25	tcp	✓	⊗	 
DNS	Domain Name Server	53	udp	✓	⊗	 
DHCP	Bootstrap Protocol Server	67	tcp	✓	⊗	 
TFTP	Trivial File Transfer Protocol	69	udp	✓	⊗	 
HTTP	World Wide Web HTTP	80	tcp	✓	⊗	 
Kerberos_TCP	Kerberos v5	88	tcp	✓	⊗	 
Kerberos_UDP	Kerberos v5	88	udp	✓	⊗	 























## 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 considerada como um tráfego malicioso.

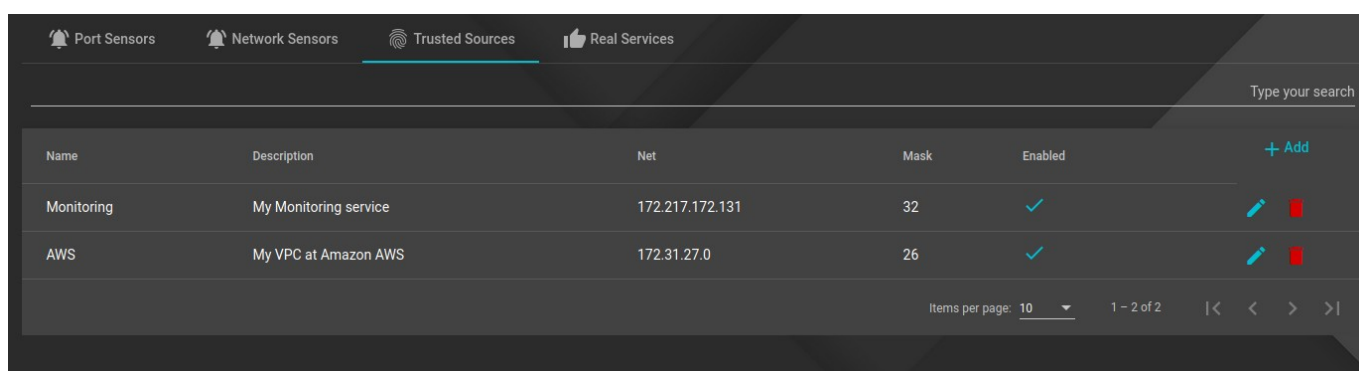






Name	Description	Net	Mask	Enabled	Action	+ Add
Honeypot_2	IP usado como Honeypot	192.168.1.2	32	✓	⊘	 
Honeypot_3	IP usado como Honeypot	192.168.1.3	32	✓	⊘	 
Honeypot_4-7	Rede 4 Honeypots	192.168.1.4-7	30	✓	⊘	 
Honeypot_8	IP usado como Honeypot	192.168.1.8	32	✓	⊘	 
Honeypot_9	IP usado como Honeypot	192.168.1.9	32	✓	⊘	 
Honeypot_70	IP usado como Honeypot	192.168.1.70	32	✓	⊘	 
Honeypot_72-79	Rede 8 Honeypots	192.168.1.72-79	29	✓	⊘	 
Honeypot_80-95	Rede 16 Honeypots	192.168.1.80-95	28	✓	⊘	 
Honeypot_96-103	Rede 8 Honeypots	192.168.1.96-103	29	✓	⊘	 
Honeypot_104-107	Rede 4 Honeypots	192.168.1.104-107	30	✓	⊘	 

Items per page: 10 1 - 10 of 33

## 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.



Name	Description	Net	Mask	Enabled	+ Add
Monitoring	My Monitoring service	172.217.172.131	32	✓	 
AWS	My VPC at Amazon AWS	172.31.27.0	26	✓	 

Items per page: 10 1 - 2 of 2 |< < > >|

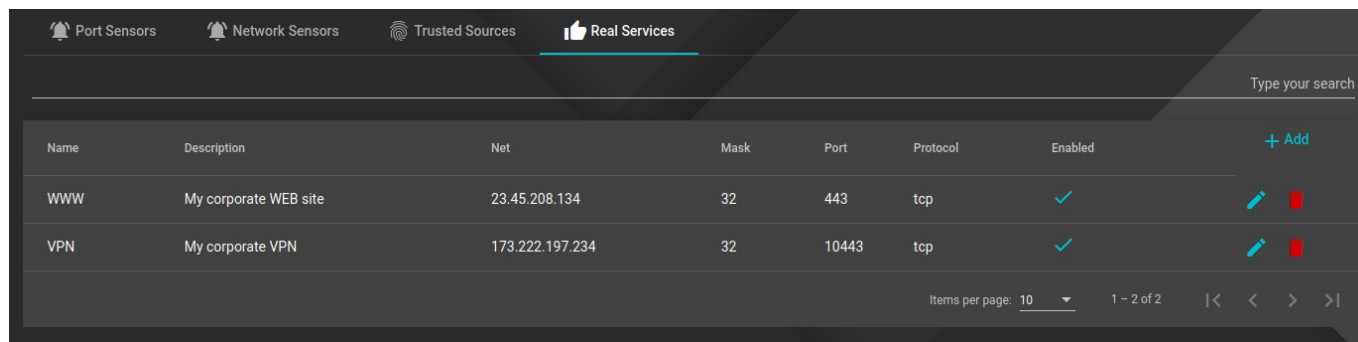
## Serviços Reais

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”.



The screenshot shows the 'Real Services' configuration page. At the top, there are navigation tabs: 'Port Sensors', 'Network Sensors', 'Trusted Sources', and 'Real Services' (which is selected). Below the tabs is a search bar labeled 'Type your search'. The main content is a table with the following columns: Name, Description, Net, Mask, Port, Protocol, Enabled, and a column with edit and delete icons. There is also a '+ Add' button in the top right of the table area. At the bottom right, there are pagination controls: 'Items per page: 10', '1 - 2 of 2', and navigation arrows.

Name	Description	Net	Mask	Port	Protocol	Enabled	
WWW	My corporate WEB site	23.45.208.134	32	443	tcp	✓	 
VPN	My corporate VPN	173.222.197.234	32	10443	tcp	✓	 

## Links

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

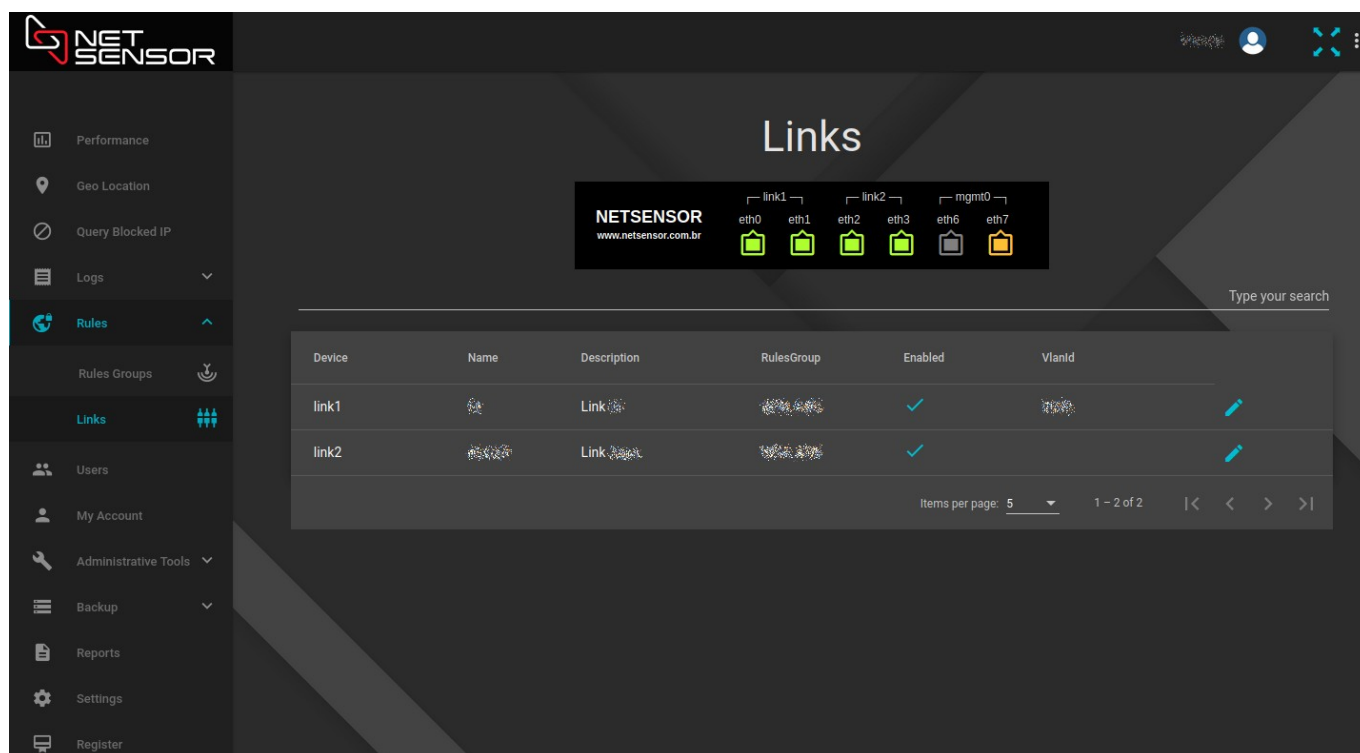
As interfaces de rede são agrupadas aos pares. Cada par forma uma interface lógica que recebe a nomenclatura “linkX”, onde “X” é um número de identificação crescente que inicia em “1”, representando a primeira interface do tipo “link”.

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.



The screenshot shows the NET SENSOR web interface. The left sidebar contains navigation options: Performance, Geo Location, Query Blocked IP, Logs, Rules, Rules Groups, Links (selected), Users, My Account, Administrative Tools, Backup, Reports, Settings, and Register. The main content area is titled 'Links' and features a diagram of a device with network interfaces: link1, link2, and mgmt0. Below the diagram is a table listing the configured links.

Device	Name	Description	RulesGroup	Enabled	VlanId
	link1	Link		✓	
	link2	Link		✓	

At the bottom of the table, there is a pagination control showing 'Items per page: 5' and '1 - 2 of 2'.

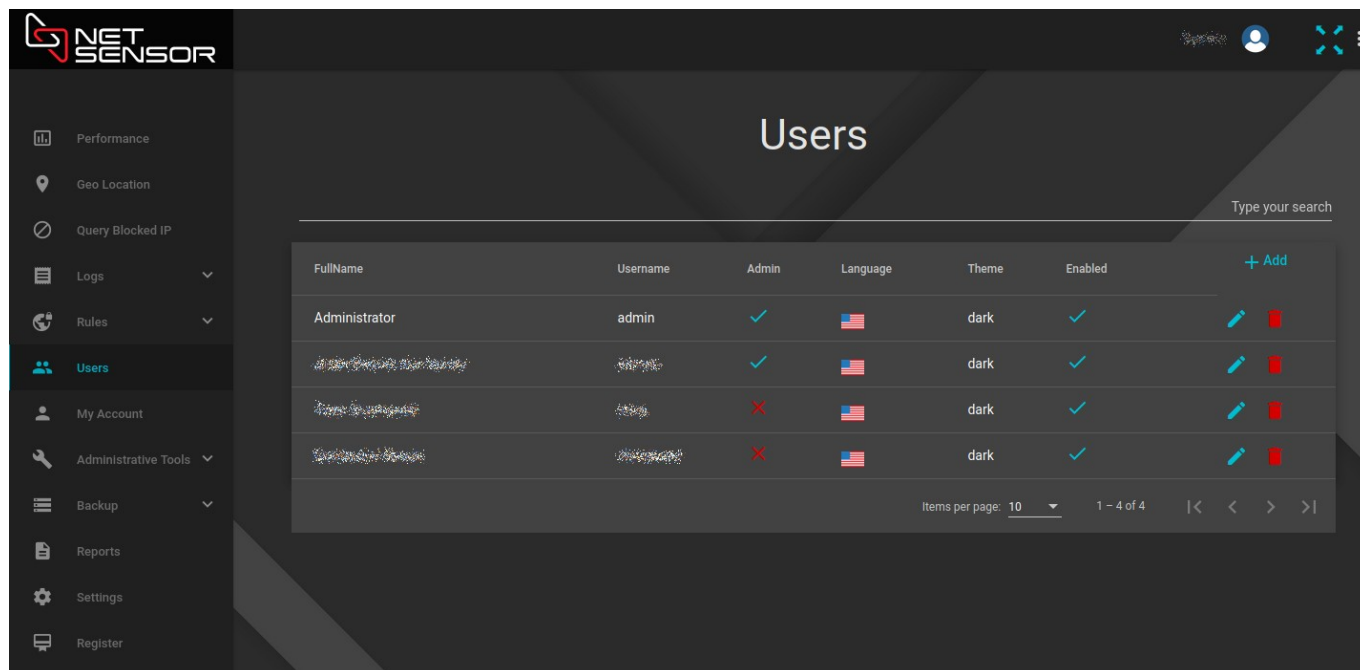
## Usuários









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.*



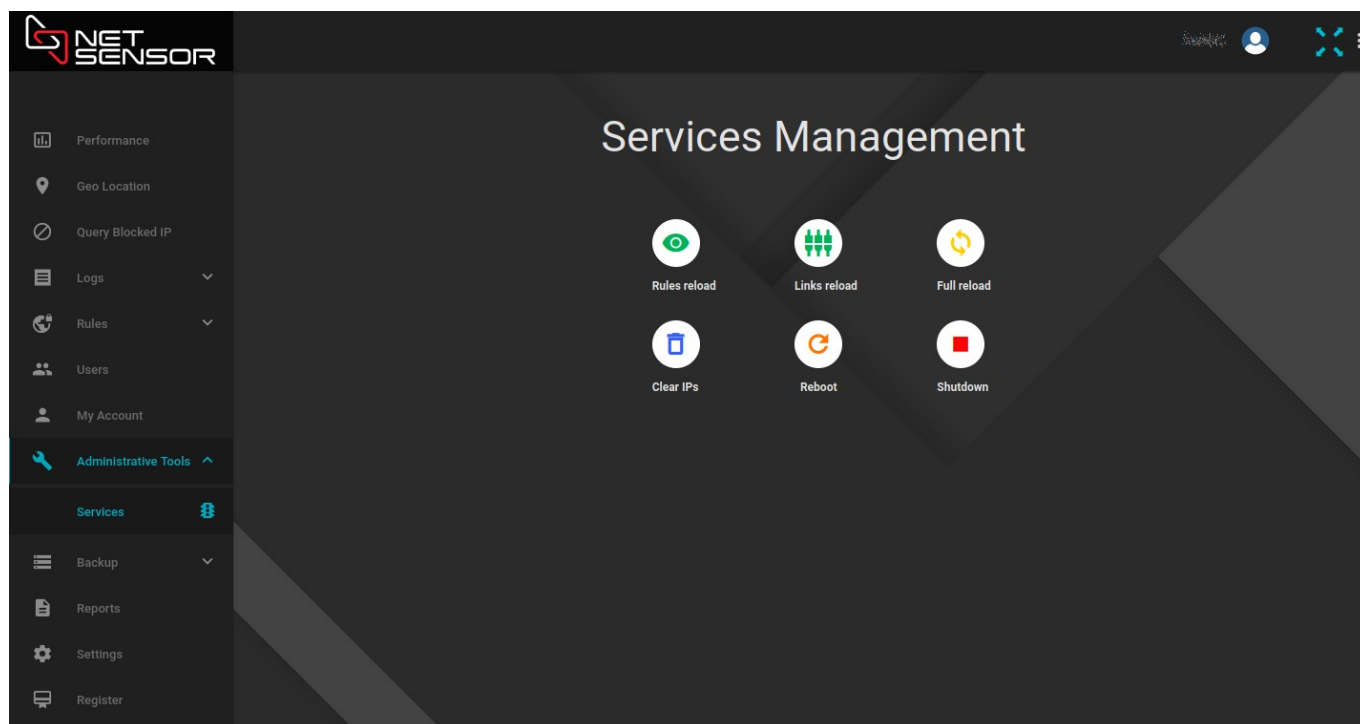
FullName	Username	Admin	Language	Theme	Enabled	
Administrator	admin	✓	🇺🇸	dark	✓	 
[blurred]	[blurred]	✓	🇺🇸	dark	✓	 
[blurred]	[blurred]	✗	🇺🇸	dark	✓	 
[blurred]	[blurred]	✗	🇺🇸	dark	✓	 

Items per page: 10 | 1 - 4 of 4 | < >

## 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.

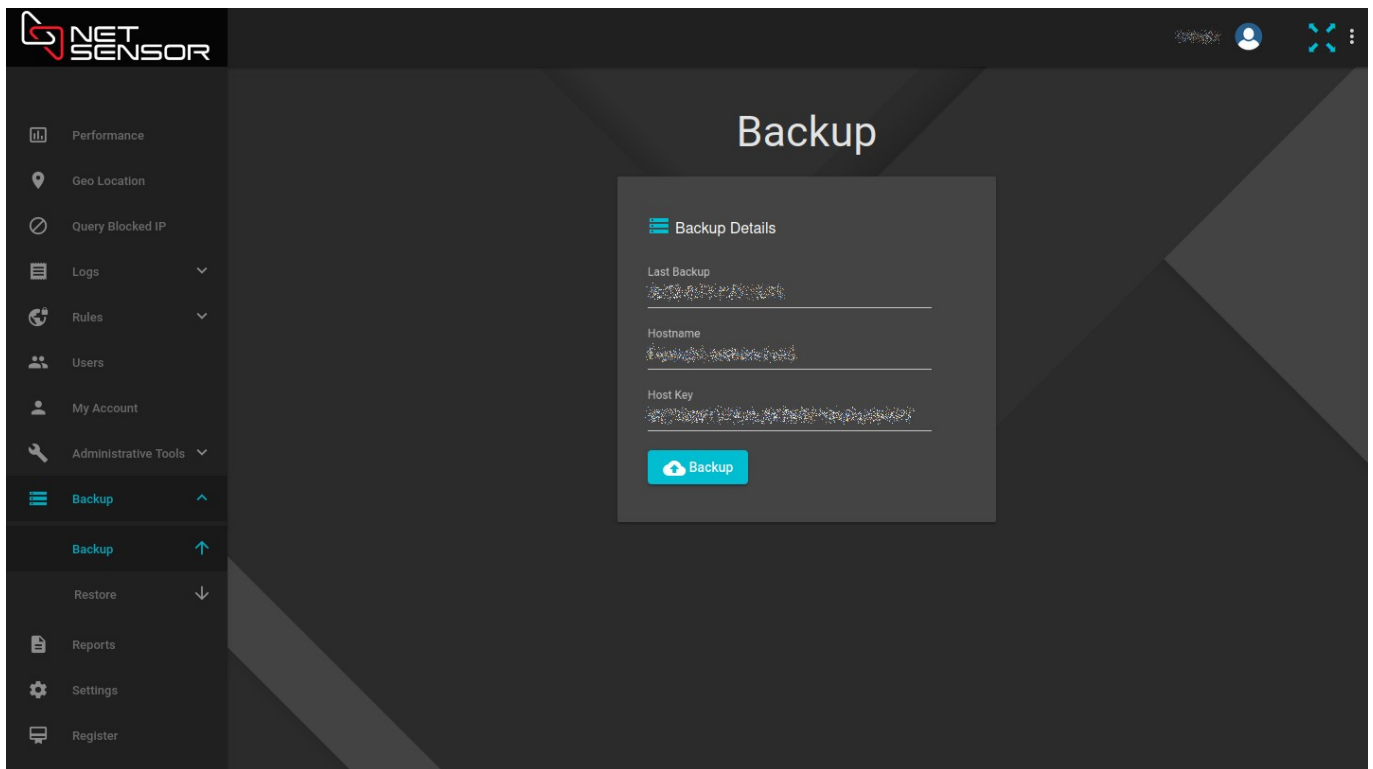


## Backup

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.

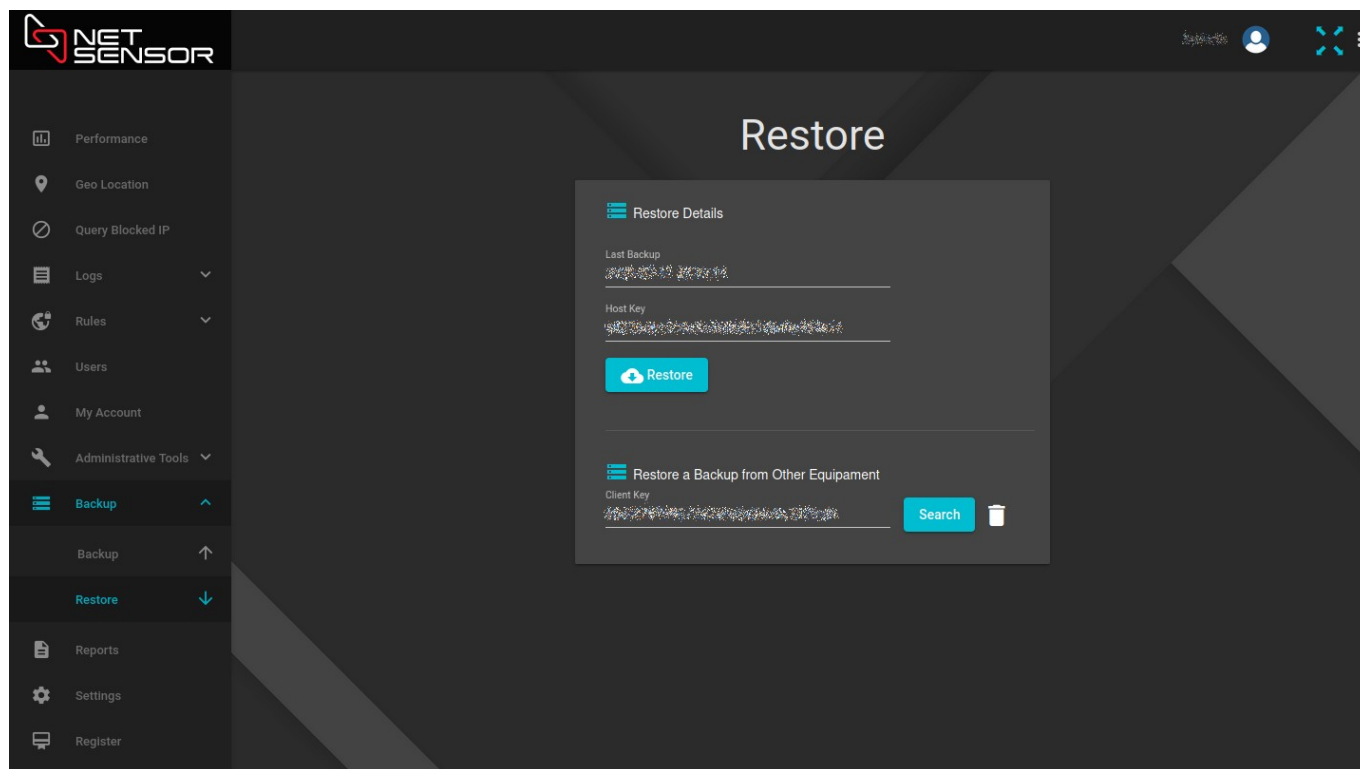


## Restauração de Backup

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.

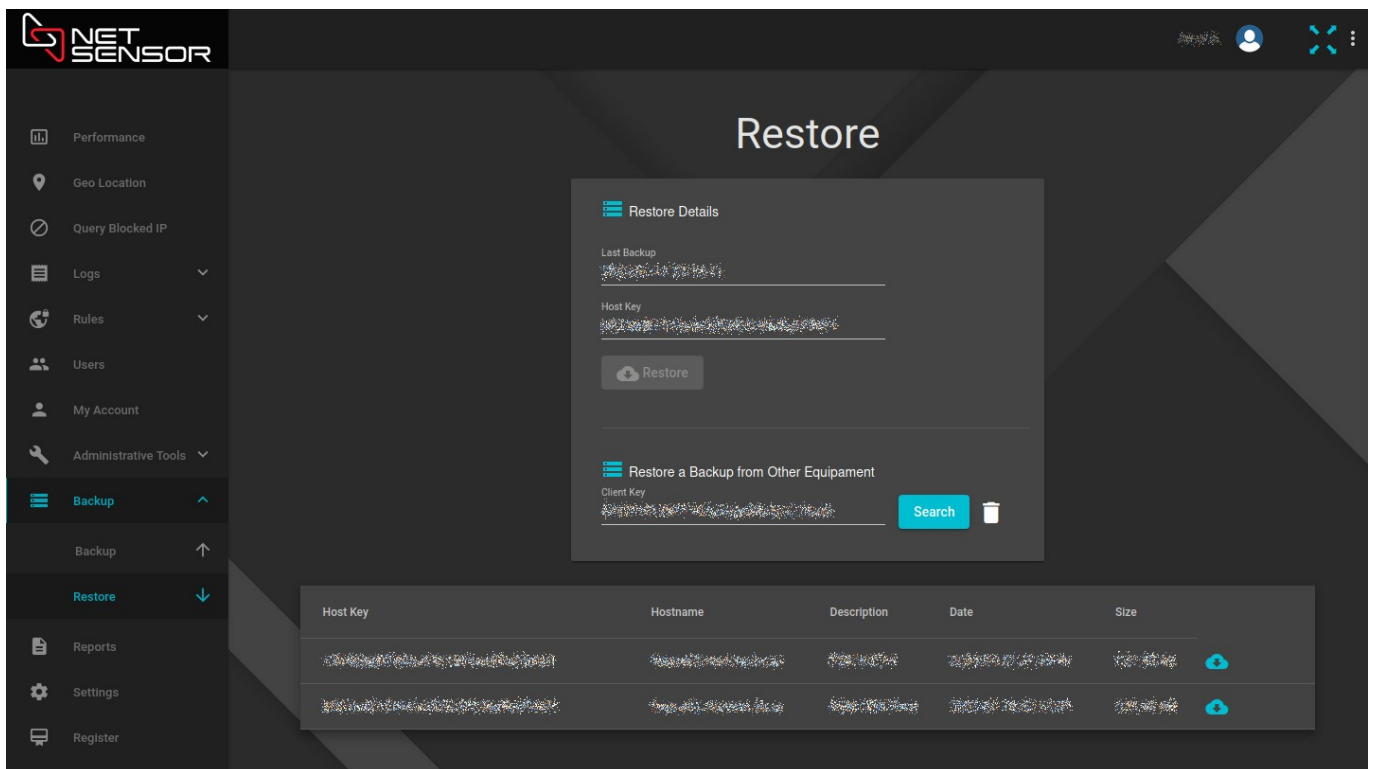
A busca por backups de outros equipamentos é feita usando a chave de identificação do cliente, a qual dá acesso aos backups de todos os equipamentos que ele possui.

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.



**Restore**

**Restore Details**


Last Backup  
[Redacted]

Host Key  
[Redacted]

Restore

**Restore a Backup from Other Equipment**

Client Key  
[Redacted] Search [Trash Icon]

Host Key	Hostname	Description	Date	Size
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted] 
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted] 