



PREVINI

RUA ANTENOR DE MOURA RAUNHEITTI, 95, PREVINI, BAIRRO DA LUZ,
NOVA IGUAÇU, RJ.

CNPJ: 03.450.083/0001-09

www.previni.com.br

Fone: (21)2666-2200

1 OBJETIVO.....	3
2 DEFINIÇÕES	3
3 DISPOSIÇÕES GERAIS	6
4 PROCESSO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO PREVINI.....	10
5 MAPEAMENTO	23
6 ANEXO I – Instalação do ARCserve e Configuração de rotinas de backup.....	27
7 ANEXO II – Instalação do Pfsense e principais configurações do Firewall.....	43
8 ANEXO III – Demonstrativo dos RACKS.....	73

**PREVINI**

RUA ANTENOR DE MOURA RAUNHEITTI, 95, PREVINI, BAIRRO DA LUZ,
NOVA IGUAÇU, RJ.

CNPJ: 03.450.083/0001-09

www.previni.com.br

Fone: (21)2666-2200

PREFÁCIO**TÍTULO**

Manual de Normas e Procedimentos da Área de Tecnologia da Informação do PREVINI

UNIDADE GESTORA

Diretoria Administrativa e Financeira

REGULAMENTAÇÃO UTILIZADA

NBR ISO/IEC 17799:2005;

ABNT 21:204.01-010;

Lei 9.609/98 – Lei do Software.

1 OBJETIVO

Definir procedimentos para a política da segurança da informação. Esta Política define as Diretrizes, visando preservar a integridade, confidencialidade e disponibilidade das informações sob gestão do PREVINI.

2 DEFINIÇÕES

2.1 TERMOS E SIGLAS UTILIZADAS

2.1.1 Backup - Cópia de segurança de informações armazenada em meio magnético.

2.1.2 Caixa Postal / Correio Eletrônico - Espaço em disco, onde são armazenadas as mensagens de correio eletrônico.

2.1.3 Chave de Acesso/ Conta - Código de acesso atribuído a cada Usuário. A cada Chave de Acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos disponíveis.

2.1.4 Correio Eletrônico - Meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores.

2.1.5 Download - Baixar um arquivo ou documento de outro computador, através da Internet.

2.1.6 Internet - Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.

2.1.7 Intranet - Rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que

os funcionários possam acessar as informações internas da autarquia.

2.1.8 Órgão Público - Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

2.1.9 Servidores - Ativos de armazenamento das informações (Sistemas, Banco de Dados, serviços em geral etc.).

2.1.10 Site - Páginas contendo informações, imagens, fotos, vídeos, sons, etc., que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte à rede.

2.1.11 Software - Programa de Computador.

2.1.12 RPPS – Regime Próprio de Previdência Social.

2.1.13 Usuários – Servidores Públicos, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários.

2.1.14 Data center - Centro de processamento de dados. Trata-se de um local onde estão concentrados os sistemas computacionais.

2.1.15 ZABBIX - É um software que monitora vários parâmetros de rede de computadores e saúde e integridade de servidores.

2.1.16 Nobreak - Equipamento responsável por regular a voltagem e a pureza da energia que alcança os eletrônicos conectados a esse dispositivo. Ele também alimenta os aparelhos por meio de uma bateria, quando há queda ou variações bruscas de energia.

2.1.17 **Vírus** - É um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática

2.1.18 **LINK** - É uma palavra em inglês que significa elo, vínculo ou ligação. No âmbito da informática, a palavra link pode significar hiperligação, ou seja, uma palavra, texto ou imagem que quando é clicada pelo usuário, o encaminha para outra página na internet, que pode conter outros textos ou imagens.

2.1.19 **FIREWALL** - Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

2.1.20 **Help Desk** - Serviço de apoio a usuários para suporte e resolução de problemas técnicos.

2.1.21 **Clusters** - Consiste em computadores fracamente ou fortemente ligados que trabalham em conjunto, de modo que, em muitos aspectos, podem ser considerados como um único sistema.

2.1.22 **TI** – Tecnologia da informação.

2.1.23 **Storage** – Equipamento de alta disponibilidade que armazena dados de uma rede.

2.1.24 **Malwares** - Um código malicioso, programa malicioso, software nocivo, software mal-intencionado ou software malicioso, é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações.

2.1.25 **VPN** - Virtual Private Network. Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.

2.1.26 **USB** - É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

3 DISPOSIÇÕES GERAIS

3.1 A execução do processo para definir procedimentos de política de segurança da informação do PREVINI deve seguir os métodos descritos neste Manual Normativo.

3.2 A competência para a proposição de alterações no Manual de Normas e Procedimentos da área de Tecnologia da Informação do PREVINI é da Diretoria Administrativa e Financeira.

3.3 As informações de propriedade ou controladas pelo PREVINI devem ser utilizadas apenas para os propósitos determinados pela Diretoria executiva do órgão. Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações.

3.4 A identificação do usuário (senha) é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela.

3.5 Todos os usuários ao tomarem conhecimento de qualquer incidente de segurança da informação devem notificar o fato, imediatamente, a seu superior através de e-mail com cópia à Gerência da Divisão de Informática.

3.6 A segurança da informação é aqui caracterizada pela preservação da:

a) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

b) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) Disponibilidade, a Política de Segurança da Informação deve ser divulgada a todos os funcionários e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

3.7 Cabe a todos os funcionários (funcionários, estagiários e prestadores de serviços) cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo PREVINI; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente ao Instituto quando do descumprimento ou violação desta política.

3.8 Cabe às Diretorias, Gerências e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação.

3.9 As entradas ao Data Center têm acesso devidamente controlado. A entrada nesta área ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

3.10 Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

3.11 Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

3.12 Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

3.13 Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

3.14 Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades do PREVINI, só devem ser utilizadas em equipamentos com controles adequados.

3.15 Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado a área de Suporte Técnico – Infraestrutura TI, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente.

3.16 A Gerência da Divisão de Informática poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

3.17 Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

3.18 Somente os funcionários que estão devidamente autorizados a falar em nome do PREVINI para os meios de comunicação podem escrever em nome do Instituto em sites de Bate-papo (Chat Room), Redes Sociais (Facebook) ou Grupos de Discussão (fóruns, newsgroups). Em caso de dúvidas, procurar a Diretoria Executiva.

3.19 Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc.) nos drivers de rede, pois ocupam espaço comum limitado do departamento.

3.20 A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas ao Instituto.

3.21 O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdo impróprios e de relacionamentos.

3.22 É vedado qualquer tipo de download. Como também o upload de qualquer software licenciado ao PREVINI ou de dados de propriedade do instituto ou de seus segurados, sem expressa autorização do gerente responsável pelo software ou pelos dados.

3.23 É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico do PREVINI.

3.24 Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: bat,.exe,. src,, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

3.25 Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

3.26 O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

3.27 É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

3.28 Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

3.29 O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

4 PROCESSO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO PREVINI

4.1 GERÊNCIA DA DIVISÃO DE E INFORMÁTICA DA DIRETORIA ADMINISTRATIVA E FINANCEIRA

4.1.1 REDUNDÂNCIA

4.1.1.1 A redundância em TI é essencial para a alta disponibilidade de sistemas, redes e dados. Com a repetição de componentes críticos para o funcionamento de um serviço, a confiabilidade dele é aprimorada, pois caso aconteça uma falha que possa desabilitar o sistema primário, um sistema secundário assume a responsabilidade. O objetivo da redundância em TI é garantir a utilização ininterrupta de serviços e evitar a perda de dados. Isso é feito com fontes de energia alternativas, múltiplos locais de armazenamento de dados e outros dispositivos redundantes.

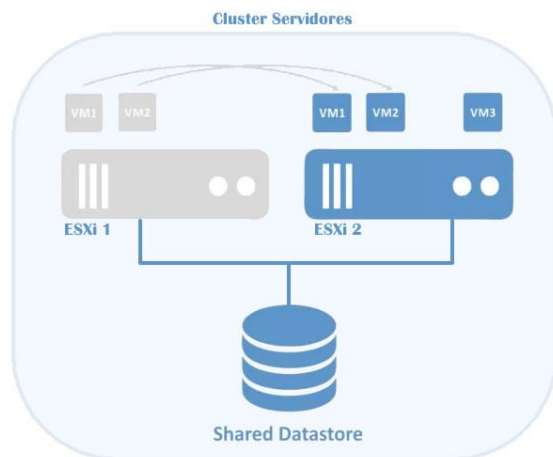
4.1.1.2 A Gerência da Divisão de Informática do PREVINI utiliza 2(dois) clusters, sendo um para redundância de servidores virtuais e outro para redundância de desktops virtuais.

4.1.1.3 Para gerenciar os Hosts, a Gerência da Divisão de Informática do PREVINI utiliza no seu data center uma ferramenta chamada VMware ESXi na versão 6.7, através dessa ferramenta pode ser gerenciado o Cluster de Servidores por exemplo que é composto por 2(dois) servidores físicos com o Sistema Operacional ESXi.

4.1.1.4 Exemplificando na imagem abaixo, quando um servidor físico (ESXi1) apresentar falhas, teoricamente os servidores virtuais (VM) gerenciado por esse servidor (ESXi1) também poderiam apresentar falhas, mas em se tratando de um cluster de servidores, podemos utilizar um serviço chamado de HA (High Availability) para fazer com que todas as VM (Virtual Machine) possam migrar automaticamente para o outro servidor (ESXi2) e fazendo com que os serviços disponibilizados não parem.

4.1.1.5 Na situação descrita no item 4.1.1.4 deste Manual Normativo, os 2(dois) servidores recebem o tráfego de forma igualmente distribuída. Porém, em momentos de falha em um deles, o dispositivo redireciona o seu tráfego para o servidor que continua funcionando. Dessa forma, a operação se mantém normal, permitindo que a inconsistência seja reparada sem custos para a organização.

4.1.1.6 Sendo assim, a redundância pode ser aplicada a diversos componentes de um sistema com o objetivo de garantir que sua disponibilidade seja mantida em momentos de problemas que levariam a pausa do funcionamento.

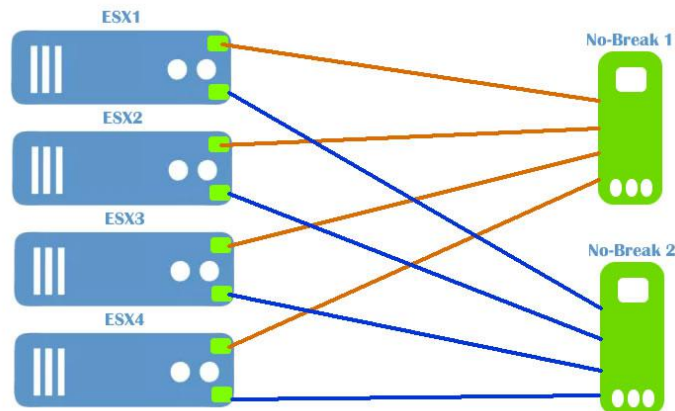


4.1.1.4 REDUNDÂNCIA EM FONTE DE ENERGIA

4.1.1.4.1 A redundância em fontes de energia consiste, na maior parte das vezes, em nobreaks e baterias que podem garantir a continuidade do trabalho em um local mesmo se houver indisponibilidade ou intermitência na rede elétrica.

4.1.1.4.2 É utilizado no PREVINI servidores físicos onde todos eles são providos de fontes de energia redundante, isso significa que caso uma fonte apresente problema, a outra fonte supri a necessidade para que o servidor não pare de funcionar, até que a fonte que apresentou falha seja trocada.

4.1.1.4.3 Utiliza-se também 2 (dois) nobreaks onde interligamos fonte de energia de cada servidor em nobreaks diferentes, conforme ilustrado no desenho abaixo. Assim pode ser garantido que além da redundância das fontes de energia, pode-se contar com a redundância de nobreaks.



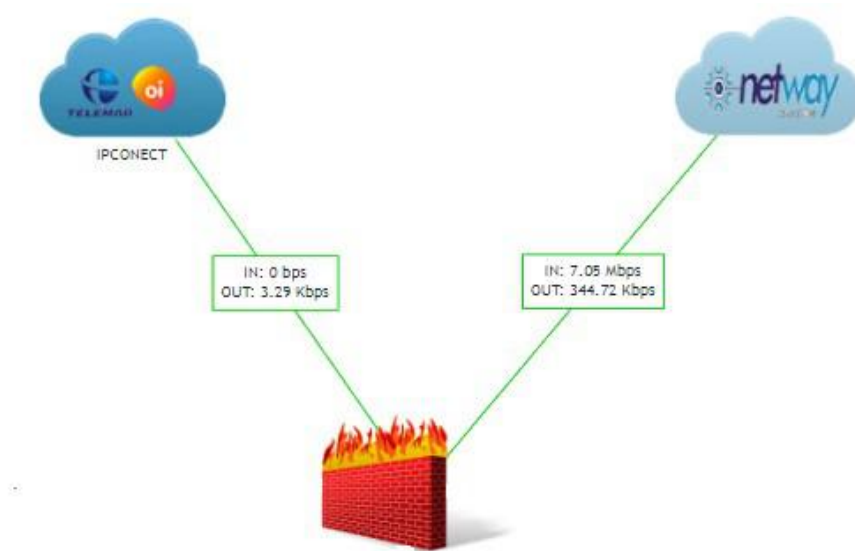
4.1.1.5 REDUNDÂNCIA EM REDES

4.1.1.5.1 A redundância de rede envolve a repetição de equipamentos modulares de fornecimento de rede e, pelo menos, duas conexões diferentes com a internet. A ideia é garantir a conexão mesmo no caso de falha de um componente ou serviço.

4.1.1.5.2 No caso do provedor de internet do PREVINI sofrer alguma falha, precisamos de uma opção alternativa para continuar operando, o que pode ser, por exemplo, uma conexão com outro provedor.

4.1.1.5.3 Em alguns casos, é interessante que essa conexão secundária ou terciária seja sem fio, para situações em que o problema é físico, como a queda de um poste na região em que passam todos os cabos de provedoras.

4.1.1.5.4 O PREVINI dispõe de 2(dois) links de internet redundantes, é de extrema importância que esses links sejam de operadoras diferentes. Utilizamos um link de fibra ótica (Oi Telemar) e um link via rádio frequência (NetWay Telecom). Sendo assim, quando uma operadora apresenta falha na comunicação, outro link entra em ação de forma automática como demonstrado na imagem abaixo.



Gateways				
Name	RTT	RTTsd	Loss	Status
WANGW	0.0ms	0.0ms	100%	Offline
WAN_NETWAYGW	4.0ms	3.4ms	0.0%	Online

4.1.1.6 REDUNDÂNCIA EM MEMÓRIA RAM

4.1.1.6.1 A redundância também pode ser usada na memória RAM dos dispositivos do PREVINI, garantindo que, quando um problema surge em um de seus componentes, os demais deem conta do recado.

4.1.1.6.2 Cabe esclarecer que a velocidade do dispositivo pode ser impactada, caso o total de memória disponível para as operações não seja alto, sobrecarregando as atividades.

4.1.1.6.3 Os colaboradores do PREVINI trabalham com sobra de memória para justamente poder receber serviços de outro servidor que apresentou falha de memória, algo que é muito comum em um ambiente virtualizado.

4.1.1.6.4 Importante ressaltar que todas as memórias dos servidores são ECC (Error Correction Check) o que garante ainda mais possíveis erros de memória.

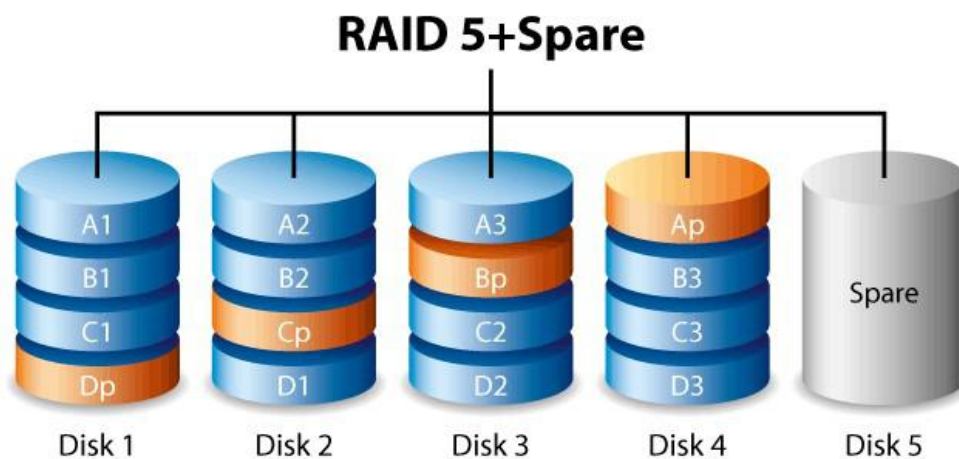
4.1.1.7 REDUNDÂNCIA EM DADOS

4.1.1.7.1 A redundância nos dados é feita com técnicas e equipamentos que vão garantir que eles sobrevivam a qualquer tipo de desastre e estejam sempre disponíveis.

4.1.1.7.2 O PREVINI utiliza em sua estrutura um equipamento chamado “Storage” que é uma expressão em inglês que remete a soluções de armazenamento, gerenciamento e proteção aos dados. O armazenamento de dados é uma responsabilidade de departamentos de TI, sendo um dos principais componentes do data center.

4.1.1.7.3 No PREVINI a storage funciona com RAID 5 de Hardware. RAID é um conjunto redundante de discos independentes que visa obter vantagens na utilização de subsistemas de dois ou mais discos, entre elas podemos citar aumento de desempenho, segurança, alta disponibilidade e tolerância a falhas. Existem diversos níveis RAID para as mais diversas finalidades.

4.1.1.7.4 No caso de qualquer um dos discos falhar, a controladora é capaz de calcular e recuperar em tempo real os dados contidos no disco defeituoso, permitindo assim que o sistema continue operando mesmo sem um dos discos.



4.1.1.7.5 O principal objetivo de um Storage é expandir a capacidade e performance de armazenamento sem que tenha um impacto direto na produção. Em outras palavras, seria permitir um armazenamento inteligente de dados.

4.1.1.8 REDUNDÂNCIA EM BACKUP

4.1.1.8.1 Importante que o PREVINI tenha uma política de backups consistente e, pelo menos, dois locais de armazenamento diferentes.

4.1.1.8.2 Uma boa política de backups é aquela que faz cópias de segurança dos dados em intervalos curtos que possam ser medidos em horas. Dessa forma, se algum tipo de falha afeta os sistemas principais de uma empresa, boa parte do trabalho ainda pode ser recuperada nos backups.

4.1.1.8.3 Como existe a possibilidade dos dados corrompidos ou malwares prejudicarem um backup, é muito recomendável que existam também cópias de datas um pouco mais antigas, que possam ser acessadas nesses casos.

4.1.1.8.4 Em relação aos locais de armazenamento, é extremamente recomendável que eles sejam distantes o bastante para garantir a segurança dos dados em catástrofes naturais: mesmo se a cidade em que um data center está instalado for devastada por uma inundação, os dados sobreviverão em outro local geograficamente afastado.

4.1.1.8.5 Outra técnica aqui é contar com, pelo menos, um backup armazenado na nuvem, o que garante disponibilidade e segurança de dados maior do que data centers físicos.

4.1.1.8.6 No PREVINI tomamos todo o cuidado com o Backup e aplicação de boas práticas conforme descrito no Anexo I.

4.1.2 SALA DE TÉCNICA

4.1.2.1 A sala de técnica (Data Center) está lotada na sala da Gerência da Divisão de Informática do PREVINI, foi pensada e construída com o piso elevado para melhor distribuição do cabeamento dos servidores físicos. A sala foi também pensada e construída no segundo andar para estar protegida de enchentes e por estar no meio do andar, ela distribui melhor os cabos. Houve também a preocupação com a distribuição elétrica, pois os nobreaks foram ligados em fases distintas para que na hipótese de queda de uma fase de energia, não haja a interrupção de algum serviço. Foi instalado na sala (2) dois equipamentos de ar condicionado para manter a temperatura entre 20 e 22°C e a redundância de equipamentos para garantir a temperatura adequada.

4.1.3 MONITORAMENTO ZABBIX

4.1.3.1 O Gerente da Divisão de informática deverá monitorar o sistema ZABBIX de forma recorrente para que possa identificar de forma antecipada as intercorrências e intervir de forma célere.

4.1.3.2 Zabbix foi desenvolvido pela Zabbix SIA. Zabbix é uma solução open source de monitoração para empresas. Zabbix é um software que monitora vários parâmetros de rede de computadores e

saúde e integridade de servidores. Zabbix usa um mecanismo de notificação flexível que permite os usuários configurarem alerta de e-mail, SMS e Mensagens via Telegram baseado em praticamente qualquer evento. Isto permite uma rápida reação para problemas em servidores.

4.1.3.3 O Zabbix é gratuito e desenvolvido e distribuído de acordo com a GPL General Public License versão 2. Isso significa que seu código-fonte é distribuído gratuitamente e está disponível para o público em geral. O suporte comercial está disponível e é fornecido pela Zabbix Company.

Zabbix disponibiliza os itens abaixo:

- Autodescoberta de servidores e dispositivos de rede
- Monitoração distribuída com a administração centralizada via WEB
- Suporte para mecanismo de pooling e trapping
- Aplicação-servidor compatível com Linux, Solaris, HP-UX, AIX, BSD Livre, Open BSD, Mac OS X
- Aplicação cliente de alta performance compatível com Linux, Solaris, HP-UX, AIX, BSD Livre, Open BSD, OS X, Tru64/OSF1, NT4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista
- Monitoramento sem agente
- Autenticação segura de usuário
- Permissões flexíveis de usuário
- Interface baseada em web
- Notificação por e-mail flexível de eventos predefinidos
- Visualização em alto nível dos recursos monitorados a nível gerencial
- Auditoria

4.1.3.4 O PREVINI optou pela solução Zabbix pelos motivos apresentados abaixo:

- A solução Open Source
- Altamente eficiente para agentes baseado nas plataformas UNIX e WIN32
- Baixa curva de aprendizado
- Retorno do investimento elevado. Downtimes são muito caros.
- Baixo custo do licenciamento
- Configuração muito simples
- Sistema de monitoramento centralizado. Todas as informações (configuração, dados de desempenho) são armazenados em banco de dados relacional
- Árvore de serviço de alto nível
- Instalação fácil

- Suporte para SNMP (V1, V2). Os dois com trapping e polling
- Capacidades de visualização
- Desenvolvido com procedimento de limpeza

4.1.3.5 Roteiro para instalação do Zabbix, considerando que o Sistema operacional Debian 9(nove) já foi instalado:

1. Instalação do repositório Debian;
2. Instalação dos pacotes Zabbix (servidor e cliente) e suas dependências;
3. Configuração do banco de dados;
4. Configurar interface web;
5. Testar e validar a instalação acessado via navegador.

4.1.4 **BACKUP**

4.1.4.1 O Gerente da Divisão de Informática deverá, diariamente, verificar os relatórios de Backups do ARCserve.

4.1.5 **LINK**

4.1.5.1 O Gerente da área deverá verificar no ZABBIX se os links do PREVINI estão funcionando como esperado.

4.1.5.2 Em seguida, o Gerente da Divisão de Informática deverá ratificar as informações coletadas no item 4.4.1 deste Manual Normativo de forma manual. Ou seja, deverá inspecionar a sala de técnica.

4.1.5.3 No caso de algum dos LINKS estar com problema, o Gerente deverá entrar em contato com as operadoras para sanear o ocorrido.

- Oi Telemar
- NetWay Telecom

4.1.6 FIREWALL

4.1.6.1 Os firewalls são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede, mas também a confidencialidade deles.

4.1.6.2 Além do firewall presente em cada máquina, é bastante comum, empresas usarem computadores específicos que agem como um “guardião” de uma rede, filtrando todo o trânsito de dados entre os PCs locais e um ambiente mais hostil, como a internet. Usando essa segunda opção, é possível até aplicar regras exclusivas como: “Máquina X pode enviar arquivos por FTP à vontade, todas as outras estão limitadas apenas a downloads”.

4.1.6.3 Cabe ressaltar que, em ambos os casos, todas essas regras podem ser personalizadas à vontade, permitindo que o protocolo de segurança seja modificado de acordo com as suas necessidades. No Windows 7, você pode checar as configurações do firewall entrando em Painel de Controle > Sistema e Segurança > Firewall do Windows.



4.1.6.3 Atualmente no PREVINI utilizamos a ferramenta de firewall conhecida como Pfsense. O pfSense é open source, licenciado sob BSD license, baseado no sistema operacional FreeBSD e adaptado para assumir o papel de um firewall e/ou roteador de redes. Ele possui recursos que muitas vezes, só encontrada em firewalls comerciais caros, já que podemos realizar com o pfSense a imensa maioria das atividades que esperamos de sistemas com este título.

4.1.6.4 O projeto pfSense foi concebido em meados de setembro de 2004 por Chris Buechler e Scott Ullrich. Chris foi um colaborador assíduo de códigos por muito tempo do projeto m0n0wall. O m0n0wall tem basicamente as mesmas pretensões técnicas do pfSense, mas desde o seu surgimento até o fim de seu desenvolvimento, seu foco foi em appliances.

4.1.6.5 A desvantagem do m0n0wall foi de ser um sistema contido em si e voltado para dispositivos que pudessem rodá-lo diretamente da memória principal. Não é possível instalá-lo em um sistema de arquivos comum em um disco rígido, por exemplo. Daí muitas funções desejáveis para sistemas mais complexos (VPN, suporte a modems 3G, autenticação de usuários, proxy, IDS, etc.) não podem ser razoavelmente implementadas nele.

4.1.6.6 Diante de tal cenário, Chris Buechler e Scott Ullrich resolveram criar um projeto baseado em todas as funcionalidades existentes no m0n0wall, porém com melhorias na interface web de configuração e uma aproximação com as versões mais recentes do FreeBSD (sistema base). O sistema conquistou usuários por ser extremamente organizado e agregar uma série de funcionalidades com fácil acesso. O passo a passo para instalar o pfSense está descrito no Anexo II deste Manual Normativo.

4.1.7 ATENDIMENTO

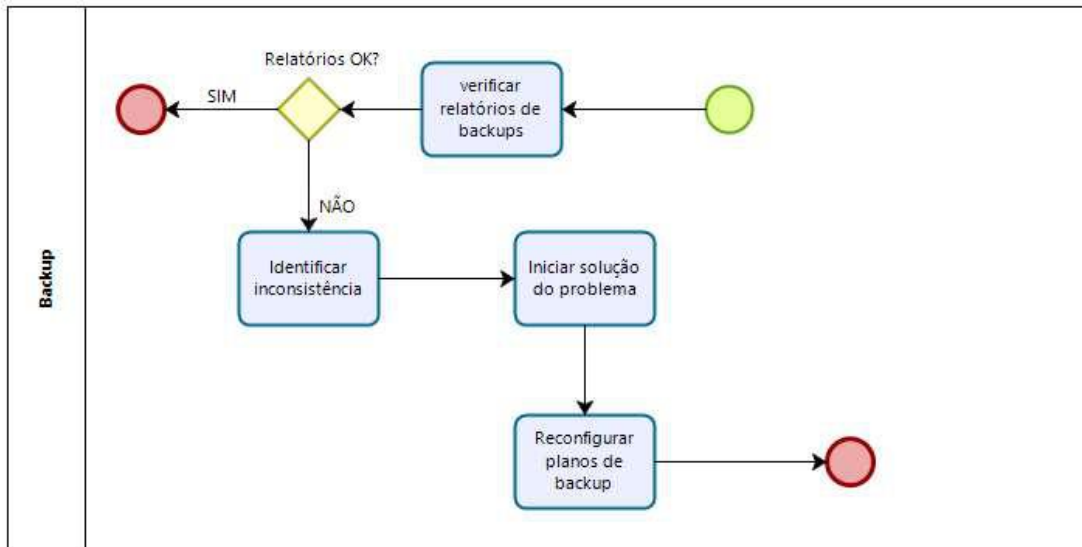
4.1.7.1 A Gerência da Divisão de Informática deverá, durante todo o expediente de trabalho, prestar suporte aos colaboradores do PREVINI. As demandas do help desk devem ser direcionadas para os ramais 2227 e 2228.

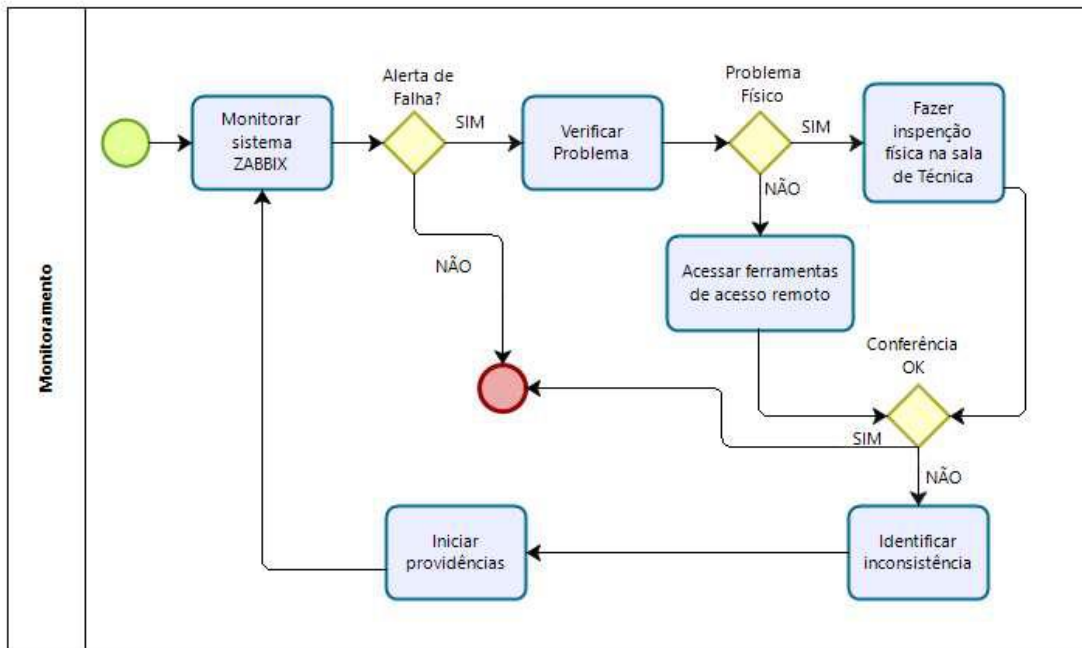
4.1.7.2 A Gerência da Divisão de Informática deverá ainda prestar suporte aos aposentados e pensionistas do Município de Nova Iguaçu quando da solicitação dos assuntos listados abaixo.

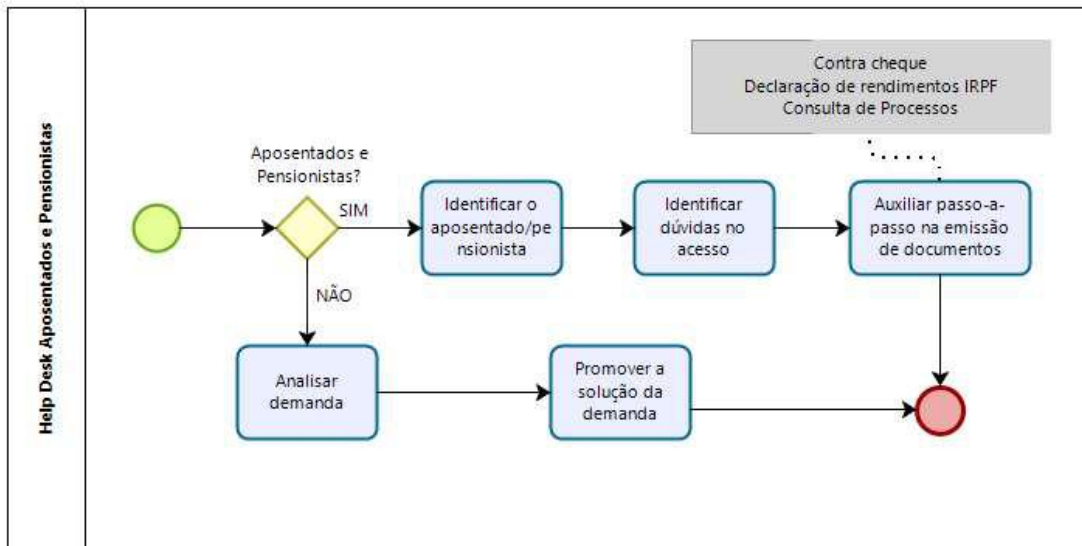
- Emissão de contracheque;
- Declaração de imposto de renda;
- Consulta processo online.

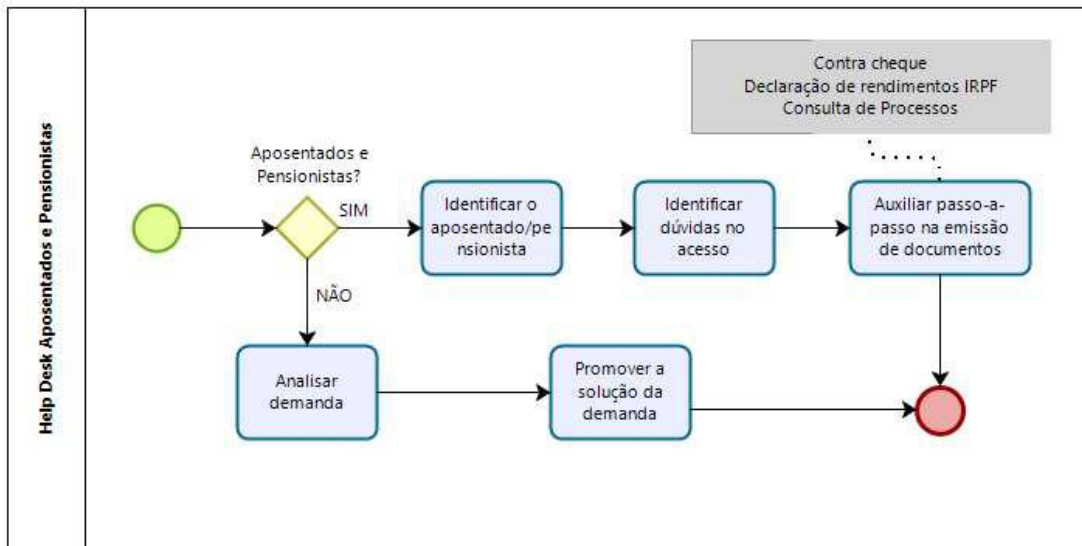
Os aposentados e pensionistas que precisarem dos serviços deverá ligar para o tele atendimento do PREVINI no telefone (21) 2666-2200 informando das dificuldades ou problemas para acessar os serviços, após entender a situação, a telefonista transfere a ligação para os ramais 2227 ou 2228.

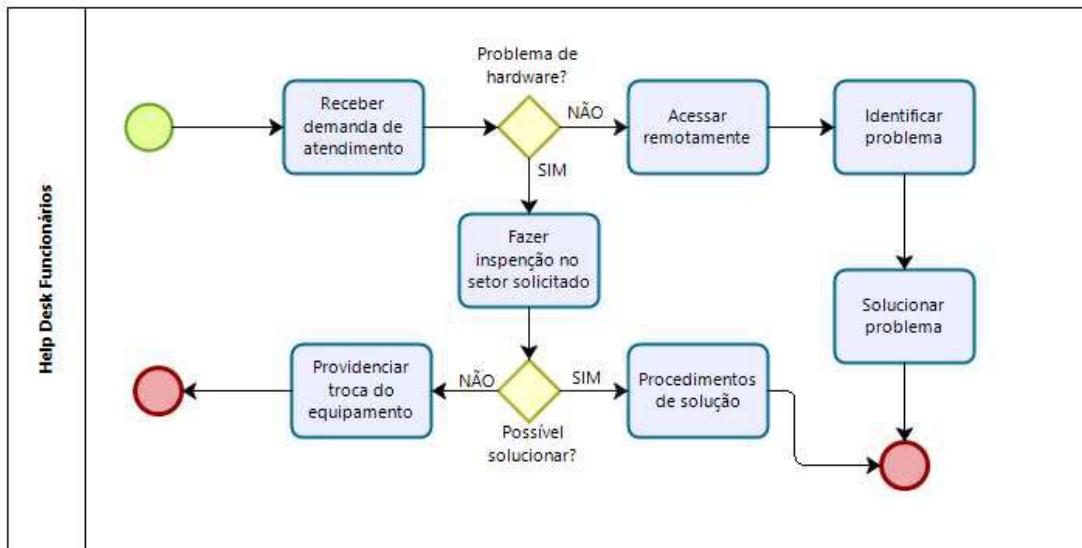
5 MAPEAMENTO











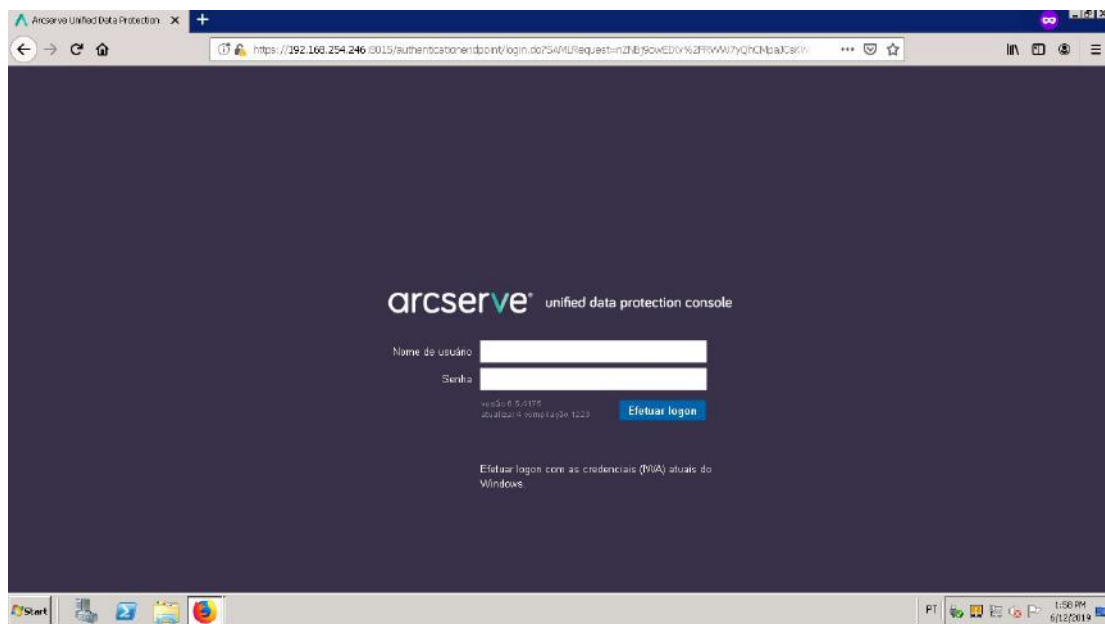
6 - Anexo I – Instalação do ARCserve

1 - A aplicação é totalmente licenciada e foi instalada por parceiros e foi homologada pelo setor de T.I. do PREVINI. Atualmente sendo executado em um servidor IBM System x3550 M3 (imagem abaixo) com 96 GB de memória RAM, 8 discos SAS em Raid 5 (redundância), 2 (duas) fontes de energia redundantes funcionando sobre a plataforma Microsoft Windows Server 2008 R2.

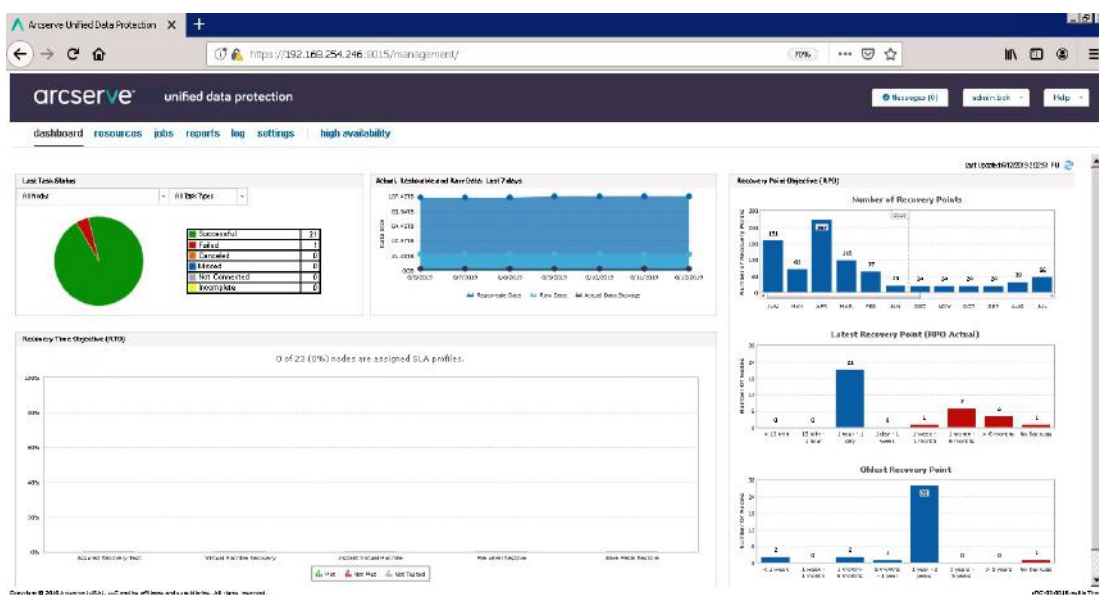


2 - A solução Arcserve UDP permite expandir com facilidade as topologias para continuidade dos negócios localmente ou por longas distâncias (e em vários locais), inclusive provedores de nuvem e de serviços. A instalação é feita com alguns cliques. A aplicação utiliza um recurso de duplicação (processo de analisar identificar e remover duplicidade nos dados, diminuindo assim a quantidade de informação a ser manipulada e armazenada).

3 - A aplicação ARCSERVE funciona através de navegadores WEB pela da porta HTTPS (443). Para acessar a aplicação deve ser informa usuário e senha (imagem abaixo), garantindo assim segurança no acesso da aplicação.

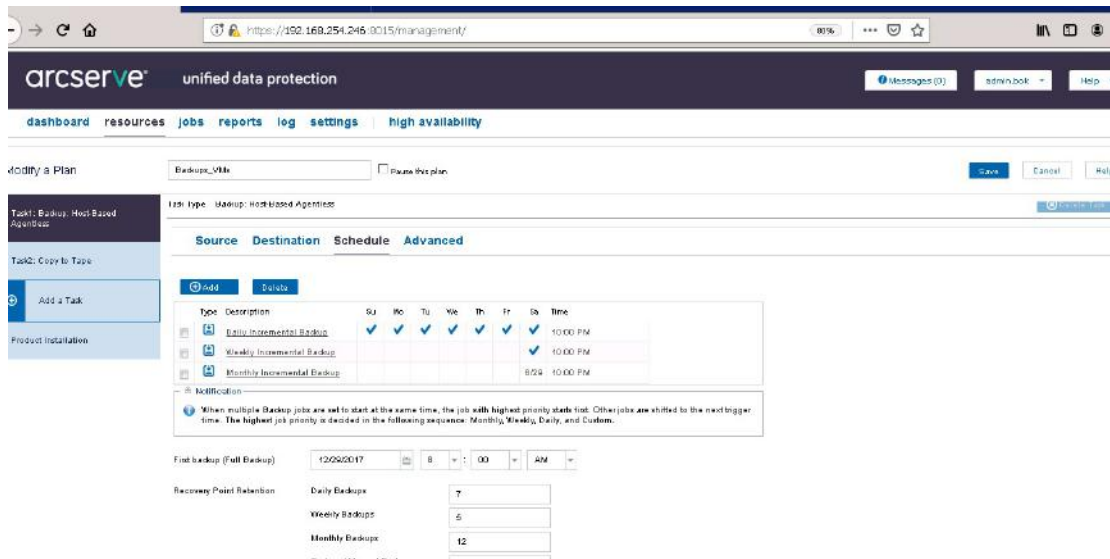


4 - Ao acessar a aplicação, podemos visualizar a tela que chamamos de “dashboard”, onde são mostrados diversos gráficos a respeito dos planos de backups. Nessa tela podemos verificar os status de backups (Successful, Failed, Canceled, Missed, Not Connected e Incomplete) o que facilita na tomada de decisões quando necessário.

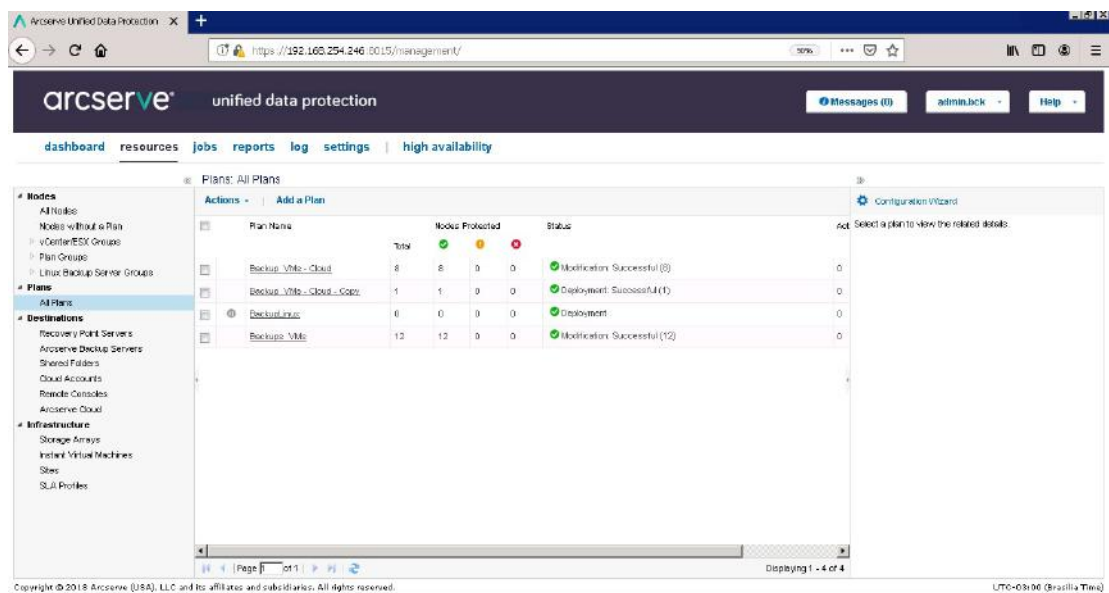


5 - Ao acessar a opção resources podemos visualizar diversas configurações e principalmente a área de planos de backups (all plans) criados e a possibilidade de criar mais planos, caso seja necessário.

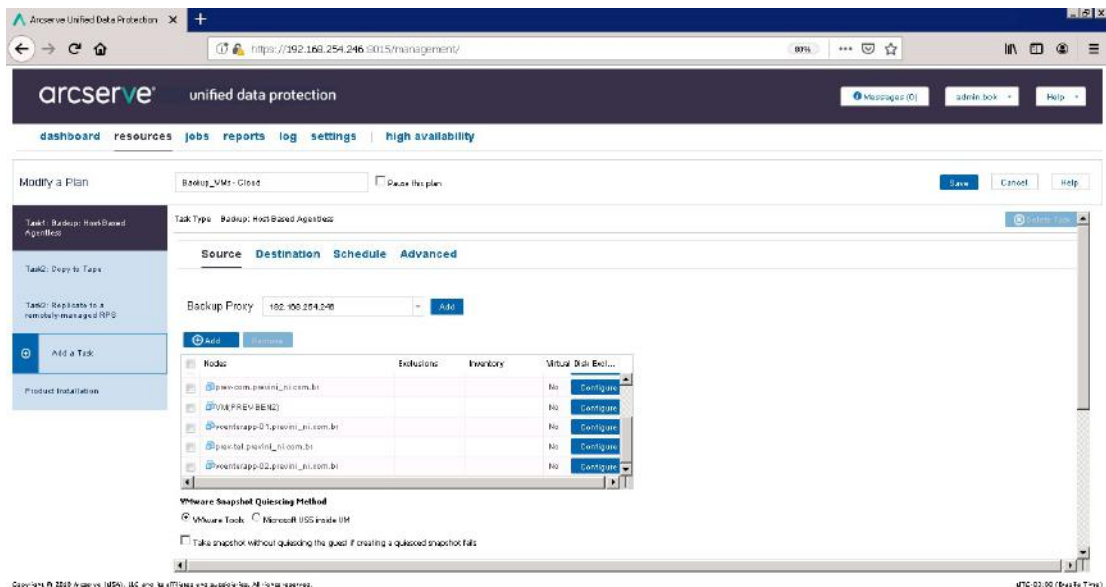
6 - Os backups são feitos de forma incremental diariamente e seu início sempre a partir das 22:00h.



7 - Para a nossa estrutura atual utilizamos basicamente 2(dois) planos de backup (Backup VMs – Cloud e Backups VMs) conforme pode ser visto na tela abaixo:



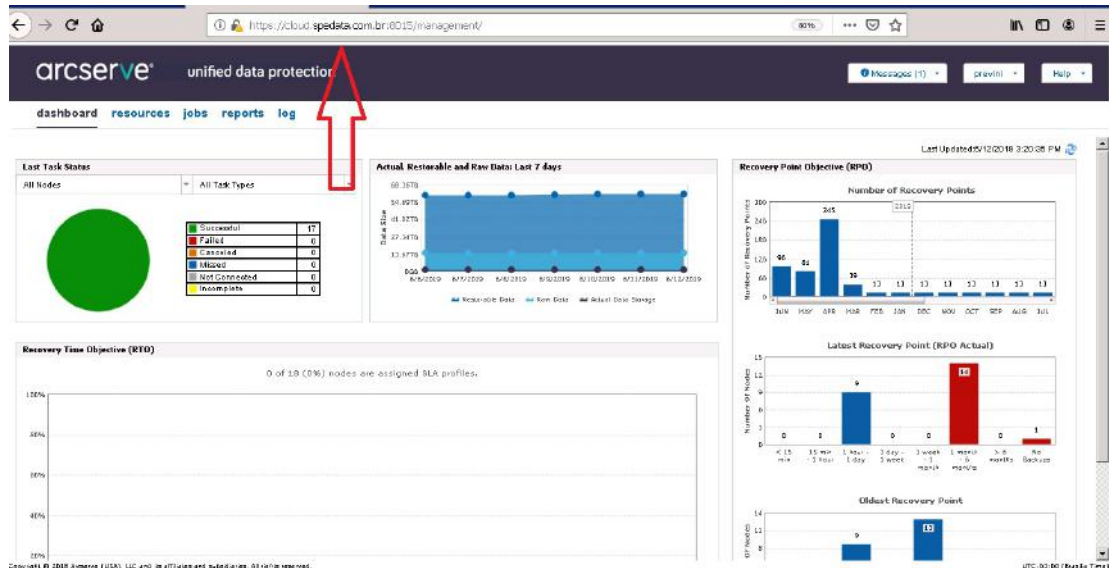
- Backup VMs – Cloud: Esse plano foi criado para execução de backup de servidores mais importantes, são eles:
 - PREV-NET3 (Firewall)
 - PREV-SEC (Security Vmware)
 - PREV-CON (Connection Vmware)
 - PREV-COM (Compose Vmware)
 - PREV-BEN2 (Banco Postgres Softprevi)
 - PREV-BEM-APL (Servidor de Aplicação Softprevi)
 - PREV-SRV (Servidor de Arquivos ADDC)
 - PREV-TEL (Telefonia – Bilhetagem)
 - VcenterApp1 (Vcenter Servidores Virtuais)
 - VcenterApp2 (Vcenter VDI)



8 - Após execução do backup em disco, são feitos de forma redundante os backups em fitas através de uma controladora IBM TS3100 Tape Library.

9 - Após a conclusão do backup nas fitas, automaticamente inicia-se um serviço de réplica em nuvem.

10 - Essa nuvem é disponibilizada através de contrato de serviço com a empresa SPE Data Informática (<https://cloud.spedata.com.br:8015/management/>), onde foram homologadas as devidas políticas de segurança de acesso tanto do lado de nossa instituição, quanto do lado da empresa contratada. Essa medida garante possíveis falhas contra desastre no prédio da instituição.



- Backup VMs: Esse plano foi criado para execução de backup de diversos servidores, são eles:
 - PROXYUDP (Restauração de BKP Linux)
 - PREV-WEB (Intranet)
 - PREV-BEN (Backup Imagens Softprevi)
 - PREV-FIN (Financeiro SIOP)
 - PREV-FIN2 (Financeiro Beta)
 - PREV-FIN3 (Financeiro Aplicação Modernização)
 - PREV-FIN4 (Financeiro Banco Modernização)
 - PREV-ZABBIX (Monitoramento)
 - PREV-WIFI (Gerenciador Wifi)
 - PREV-PPTP (VPN com a Prefeitura)



PREVINI

RUA ANTENOR DE MOURA RAUNHEITI, 95, PREVINI, BAIRRO DA LUZ,
NOVA IGUAÇU, RJ.

CNPJ: 03.450.083/0001-09

www.previni.com.br

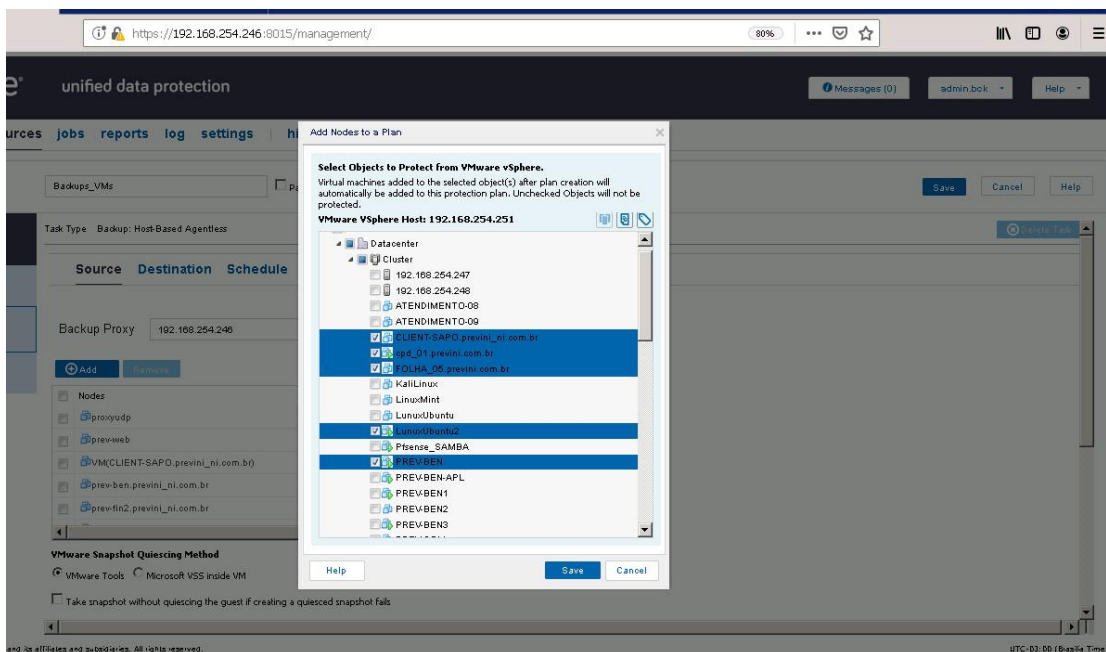
Fone: (21)2666-2200

The screenshot shows the Arcserve Unified Data Protection management console. The main content area is titled 'Modify a Plan' and shows a configuration for a backup plan named 'Backup_VMs'. The task type is 'Backup: HostBased Appliances'. The 'Source' tab is active, showing a table of backup proxies and a list of virtual disks.

Node	Exclusions	Inventory	Virtual Disk End...	
192.168.254.246			No	Configure
192.168.254.246			No	Configure
192.168.254.246			No	Configure
192.168.254.246			No	Configure
192.168.254.246			No	Configure

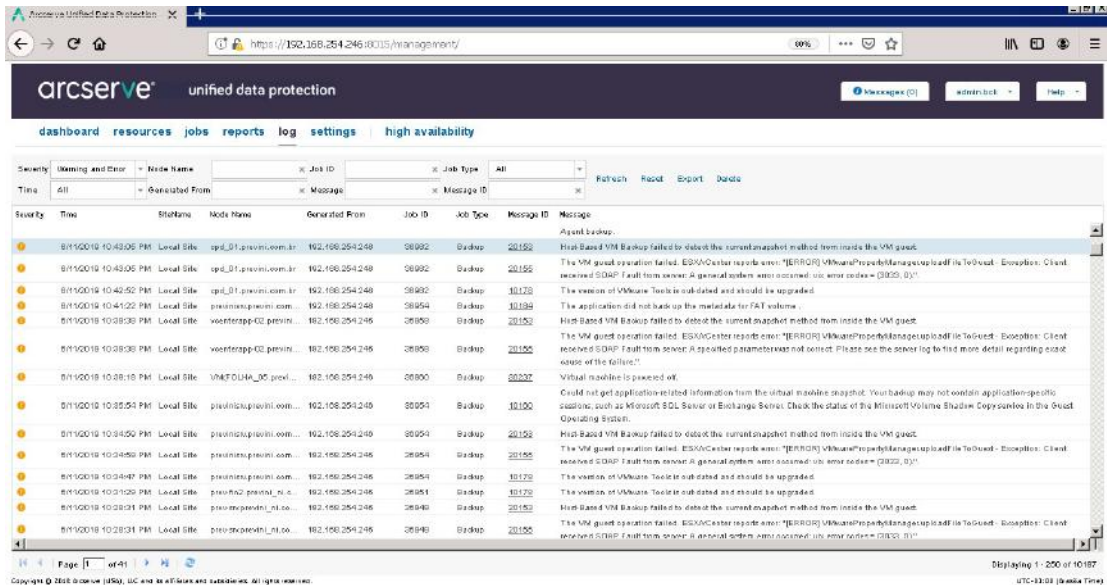
Below the table, the 'Virtual Machine Quiescing Method' is set to 'VMware Tools'. There is a checkbox for 'Take snapshot without quiescing the guest if creating a quiesced snapshot fails'.

11 - Caso seja necessária a modificação de um plano de backup existente e inclusão de um novo servidor no backup, basta clicar no plano com o botão direito do cursor (mouse) escolher a opção Modify na tela seguinte, clicar no botão Add e escolher a opção Add Nodes from a vCenter/ESX(i), na tela seguinte deverá ser informado o endereço e as credenciais do Vcenter, na tela seguinte, basta escolher o servidor que deseja incluir no plano de backup e clicar em Save.

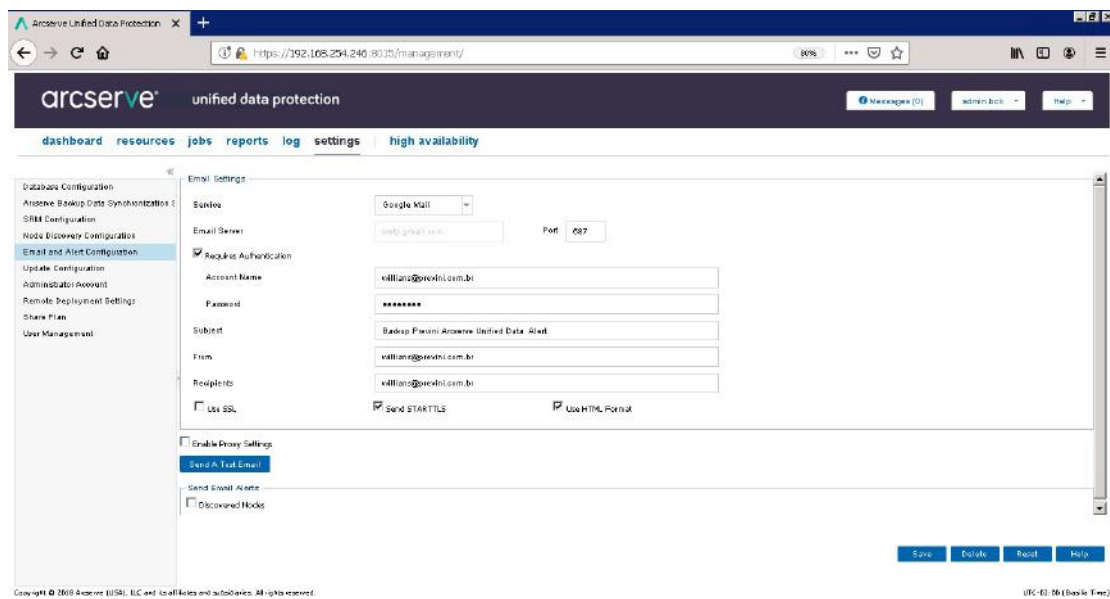


12 - São feitas réplicas de backups mensalmente também para um disco externo, onde esse disco fica armazenado fisicamente fora do prédio da instituição, assim garantindo também falhas contra desastres no prédio.

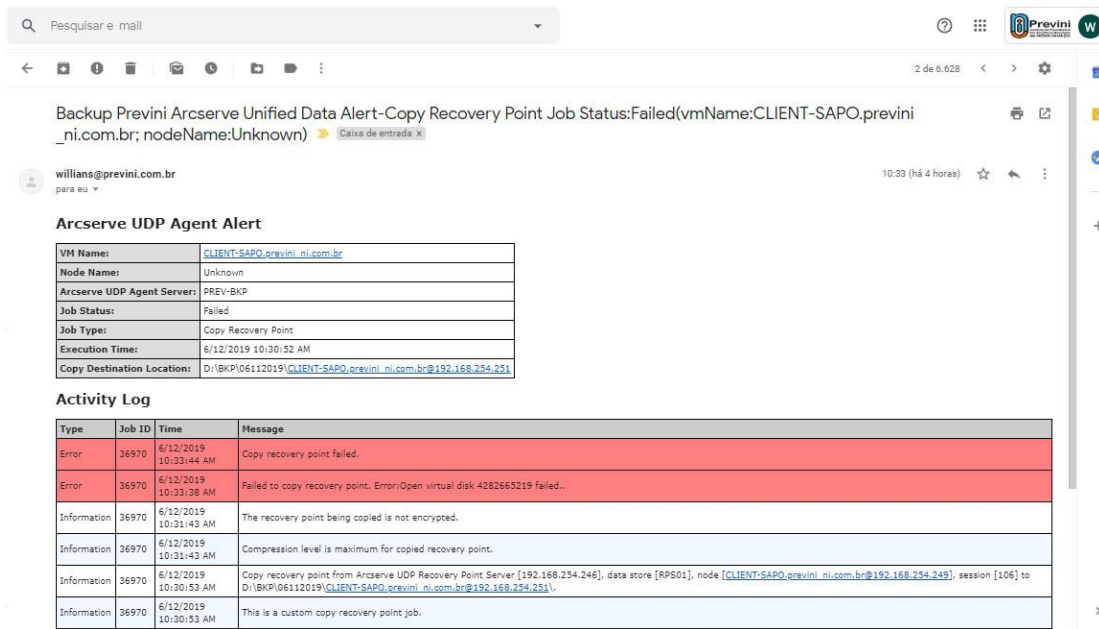
13 - Ao acessar a opção de Log, podemos verificar todos os procedimentos de backup e também podemos verificar alertas e erros, o que facilita na administração dos backups.



14 - Na opção Settings, podemos também configurar envio de alertas de erros e relatórios de conclusão de backup conforme imagens abaixo:



15 - Abaixo podemos visualizar como exemplo um alerta enviado por e-mail a respeito de um erro ao tentar executar um backup:



Backup Previni Arcserve Unified Data Alert-Copy Recovery Point Job Status:Failed(vmName:CLIENT-SAPO.previni_ni.com.br; nodeName:Unknown)

willians@previni.com.br
para eu

10:33 (há 4 horas)

Arcserve UDP Agent Alert

VM Name:	CLIENT-SAPO.previni_ni.com.br
Node Name:	Unknown
Arcserve UDP Agent Server:	PREV-BKP
Job Status:	Failed
Job Type:	Copy Recovery Point
Execution Time:	6/12/2019 10:30:52 AM
Copy Destination Location:	D:\BKP\06112019\CLIENT-SAPO.previni_ni.com.br@192.168.254.251

Activity Log

Type	Job ID	Time	Message
Error	36970	6/12/2019 10:33:44 AM	Copy recovery point failed.
Error	36970	6/12/2019 10:33:28 AM	Failed to copy recovery point. Error:Open virtual disk 4282665219 failed..
Information	36970	6/12/2019 10:31:43 AM	The recovery point being copied is not encrypted.
Information	36970	6/12/2019 10:31:43 AM	Compression level is maximum for copied recovery point.
Information	36970	6/12/2019 10:30:53 AM	Copy recovery point from Arcserve UDP Recovery Point Server [192.168.254.246], data store [RPS01], node [CLIENT-SAPO.previni_ni.com.br@192.168.254.249], session [106] to D:\BKP\06112019\CLIENT-SAPO.previni_ni.com.br@192.168.254.251).
Information	36970	6/12/2019 10:30:53 AM	This is a custom copy recovery point job.

16 - Abaixo podemos verificar um relatório de conclusão de backup recebido por e-mail:

Backup Previni Arcserve Unified Data Alert - reports [Jun 12, 2019 8:00:35 AM] > Caixa de entrada X

willians@previni.com.br
para eu, backups corp

Backup Previni Arcserve Unified Data Alert - reports

Server: prev-bkp
Time Generated: Jun 12, 2019 8:00:35 AM UTC-03:00 (Brasilia Time)

This email includes the following reports:

- Backup Size Trend Report
- Node Backup Status Report
- Virtualization Protection Status Report
- Data Distribution on Media Report
- Managed Capacity Report
- Recovery Point Objective Report

Backup Size Trend Report

This report displays the backup data size of both Arcserve Backup and Arcserve UDP Agent in a historical view and then projects the growth trend that you can prepare for future storage space requirements. This report contains information about nodes that run on supported Windows and Linux operating systems and allows you to drill down to display detailed information for an individual node.

Job Nodes All, Groups All Nodes, Protected Nodes - Last 7 Days , Forecast 7 Days , Node Tier All Tiers
6/5/2019 - 6/12/2019 (Wednesday), Total backup data size: 556.88 GB

Job Nodes	Protected Nodes	Product	Data Size	Last Successful Backup Time
192.168.254.248	VM(CLIEN-SAP0.previni.ni.com.br)	Arcserve UDP Agent	1.00 MB	Jun 10, 2019 10:04:51 PM
192.168.254.248	VM(FOLHA_06.previni.com.br)	Arcserve UDP Agent	0.00 Byte	Jun 10, 2019 10:17:58 PM
192.168.254.248	VM(PREV-BEN2)	Arcserve UDP Agent	0.00 Byte	Jun 10, 2019 10:25:32 PM
192.168.254.248	pod_01.previni.com.br	Arcserve UDP Agent	18.54 GB	Jun 10, 2019 10:30:31 PM
192.168.254.248	prev-ben.previni.ni.com.br	Arcserve UDP Agent	18.29 GB	Jun 10, 2019 10:27:38 PM
192.168.254.248	prev-com.previni.ni.com.br	Arcserve UDP Agent	12.12 GB	Jun 10, 2019 10:05:22 PM
192.168.254.248	prev-com.previni.ni.com.br	Arcserve UDP Agent	12.49 GB	Jun 10, 2019 10:05:38 PM
192.168.254.248	prev-fin2.previni.ni.com.br	Arcserve UDP Agent	43.84 GB	Jun 10, 2019 10:18:19 PM

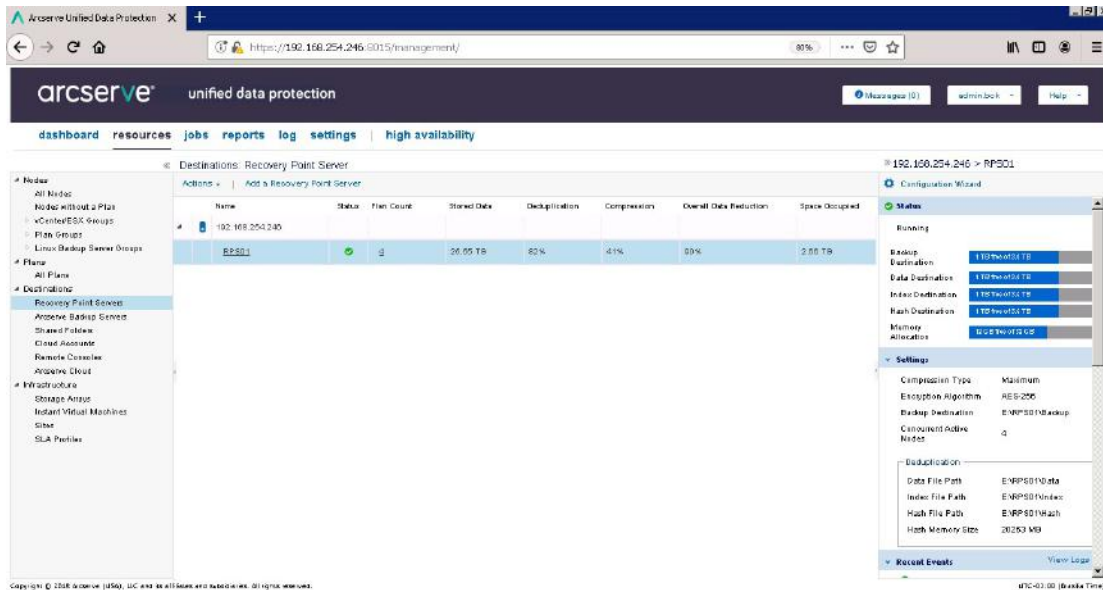
Node Backup Status Report

This report shows the most recent backup status of all nodes during the specific time period. This report allows you to drill down to display detailed information about each selected category.

Job Nodes All, Groups All Nodes, Node Name - Last 7 Days , Node Tier All Tiers

Job Nodes	Node Name	Product	Latest Recovery Point	Number of Successful Backup Jobs	Latest Successful Disaster Recovery Backup	Encrypted Sessions Available	Last Backup Time	Last Backup Type	Last Backup Status
192.168.254.248	VM(CLIEN-SAP0.previni.ni.com.br)	Host-Based VM Backup	Jun 11, 2019 10:13:02 PM	7	Jun 11, 2019 10:13:02 PM	Yes	Jun 11, 2019 10:13:02 PM	Incremental	Successful
192.168.254.248	VM(FOLHA_06.previni.com.br)	Host-Based VM Backup	Jun 11, 2019 10:30:05 PM	7	Jun 11, 2019 10:30:05 PM	Yes	Jun 11, 2019 10:30:05 PM	Incremental	Successful
192.168.254.248	VM(PREV-BEN2)	Host-Based VM Backup	Jun 11, 2019 10:15:58 PM	7	None	Yes	Jun 11, 2019 10:15:58 PM	Incremental	Successful
None	192.168.254.248		None	0	None	No	None	None	N/A
192.168.254.248	pod_01.previni.com.br	Host-Based VM Backup	Jun 11, 2019 10:42:44 PM	7	Jun 11, 2019 10:42:44 PM	Yes	Jun 11, 2019 10:42:44 PM	Incremental	Successful
192.168.254.248	prev-ben.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:38:47 PM	7	Jun 11, 2019 10:38:47 PM	Yes	Jun 11, 2019 10:38:47 PM	Incremental	Successful
192.168.254.248	prev-com.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:18:34 PM	7	Jun 11, 2019 10:18:34 PM	Yes	Jun 11, 2019 10:18:34 PM	Incremental	Successful
192.168.254.248	prev-com.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:04:28 PM	7	Jun 11, 2019 10:04:28 PM	Yes	Jun 11, 2019 10:04:28 PM	Incremental	Successful
192.168.254.248	prev-fin2.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:31:18 PM	7	Jun 11, 2019 10:31:18 PM	Yes	Jun 11, 2019 10:31:18 PM	Incremental	Successful
192.168.254.248	prev-fin2.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:34:37 PM	7	Jun 11, 2019 10:34:37 PM	Yes	Jun 11, 2019 10:34:37 PM	Incremental	Successful
192.168.254.248	prev-fin3.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:12:57 PM	7	None	Yes	Jun 11, 2019 10:12:57 PM	Incremental	Successful
192.168.254.248	prev-print.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:24:35 PM	7	Jun 11, 2019 10:24:35 PM	Yes	Jun 11, 2019 10:24:35 PM	Incremental	Successful
192.168.254.248	prev-sec	Host-Based VM Backup	Jun 11, 2019 10:04:28 PM	7	Jun 11, 2019 10:04:28 PM	Yes	Jun 11, 2019 10:04:28 PM	Incremental	Successful
192.168.254.248	prev-sec.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:28:08 PM	7	Jun 11, 2019 10:28:08 PM	Yes	Jun 11, 2019 10:28:08 PM	Incremental	Successful
192.168.254.248	prev-tel.previni.ni.com.br	Host-Based VM Backup	Jun 11, 2019 10:17:03 PM	7	Jun 11, 2019 10:17:03 PM	Yes	Jun 11, 2019 10:17:03 PM	Incremental	Successful
192.168.254.248	prev-web	Host-Based VM Backup	Jun 11, 2019 10:22:12 PM	7	None	Yes	Jun 11, 2019 10:22:12 PM	Incremental	Successful
192.168.254.248	prev-wifi	Host-Based VM Backup	Jun 11, 2019 10:04:28 PM	7	None	Yes	Jun 11, 2019 10:04:28 PM	Incremental	Successful
192.168.254.248	prev-wifi	Host-Based VM Backup	Jun 11, 2019 10:12:18 PM	7	None	Yes	Jun 11, 2019 10:12:18 PM	Incremental	Successful

17 - Atualmente podemos verificar que o total de espaço utilizado em nosso RPS01 LOCAL (servidor de backup no instituto) é de 2.66 TB conforme demonstrado em imagem abaixo:

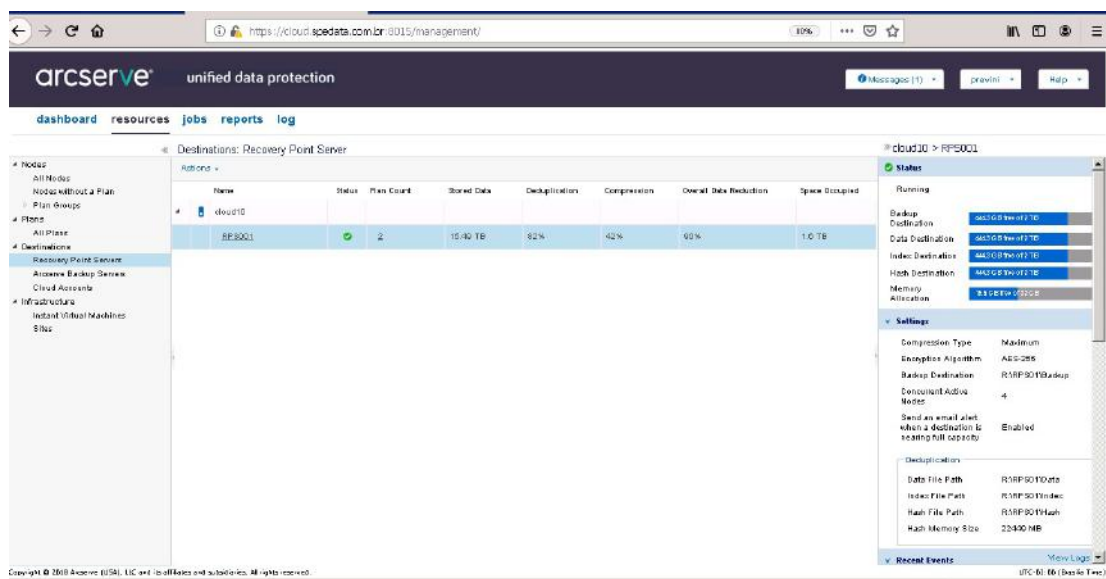


The screenshot shows the Arcserve Unified Data Protection management interface. The main content area displays a table titled "Destinations: Recovery Point Server" with the following data:

Name	Status	Item Count	Stored Data	Deduplication	Compression	Overall Data Reduction	Space Occupied
RPS01	Running	1	26.65 TB	80%	41%	59%	2.66 TB

On the right side, the "Configuration Wizard" for the selected RPS01 server is visible, showing various settings such as Backup, Data Destination, Index Destination, Hash Destination, Multiplex Allocation, Compression Type (Maximum), Encryption Algorithm (AES-256), Backup Destination (ENPFS01Backup), Concurrent Active Nodes (1), and Deduplication settings (Data File Path, Index File Path, Hash File Path, Hash Memory Size).

18 - Atualmente podemos verificar que o total de espaço utilizado em nosso RPS01 REMOTO (servidor de backup em nuvem) é de 1.6 TB conforme demonstrado em imagem abaixo:



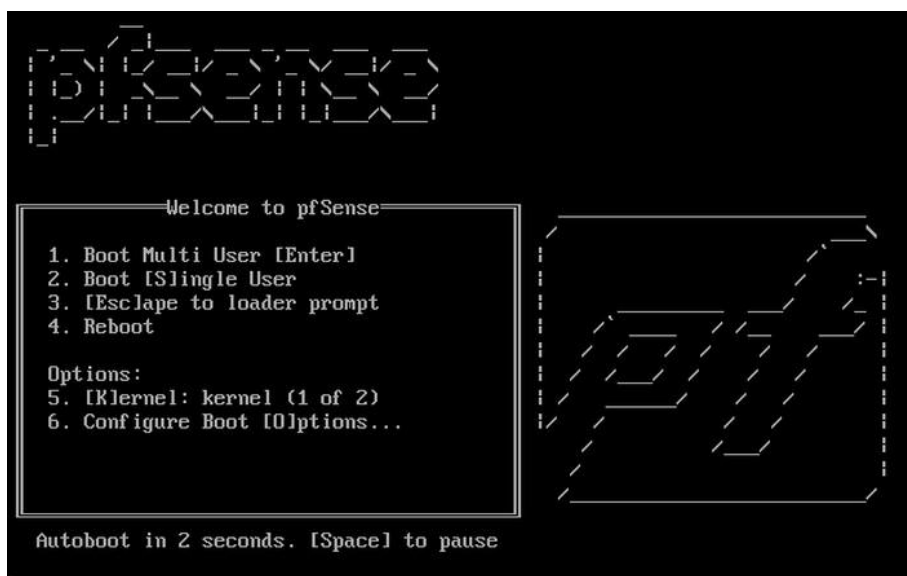
The screenshot shows the Arcserve management console. The main view displays a table of backup jobs under 'Destinations: Recovery Point Server'. The table has columns for Name, Status, Plan Count, Stored Data, Deduplication, Compression, Overall Data Reduction, and Space Occupied. One job named 'cloud10' is listed with a status of 'Running' and 'Space Occupied' of 1.0 TB.

Name	Status	Plan Count	Stored Data	Deduplication	Compression	Overall Data Reduction	Space Occupied
cloud10	Running	2	1540 TB	82%	42%	60%	1.0 TB

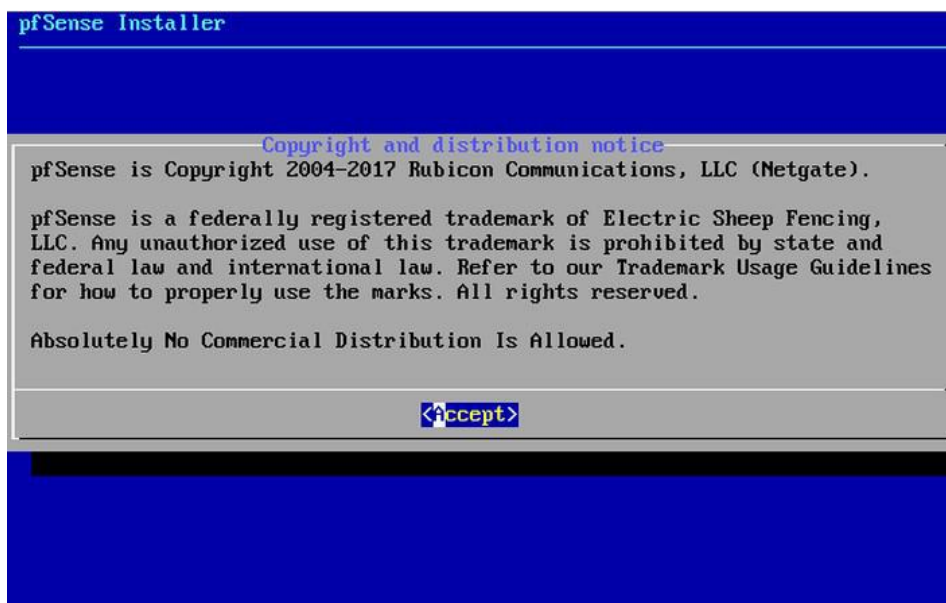
The right-hand pane shows the 'States' for the selected job, including Backup Destination, Data Destination, Index Destination, Hash Destination, and Memory Allocation. Below this, the 'Settings' section shows configuration details such as Compression Type (Maximum), Encryption Algorithm (AES-256), Backup Destination (R/RP50/Backup), and Deduplication settings (Data File Path, Index File Path, Hash File Path, Hash Memory Size).

7 - Anexo II – Instalação do Pfsense

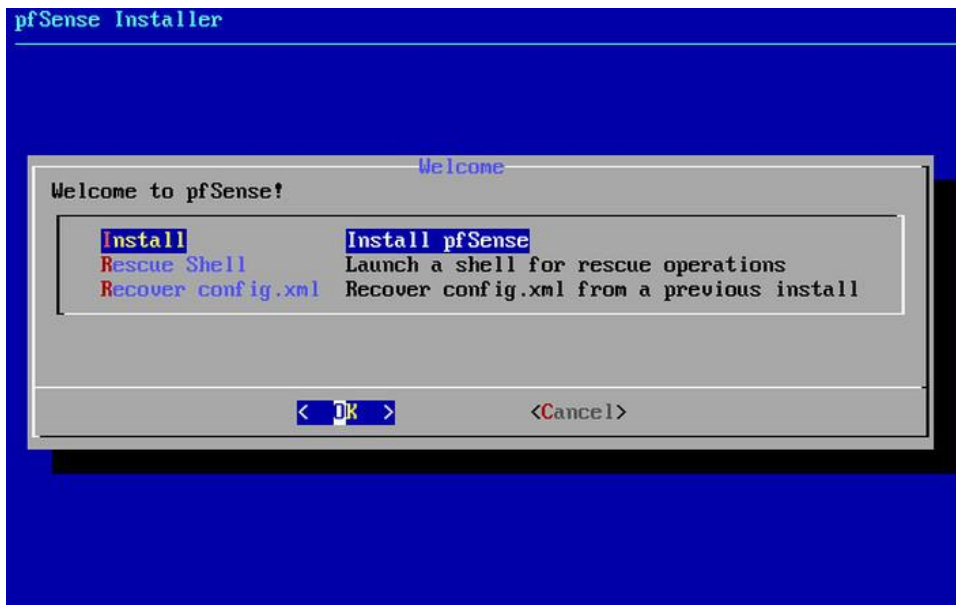
Após o boot, essa é a primeira tela, exibida por 5 segundos, clicar na tecla “Enter” ou deixa iniciar automaticamente.



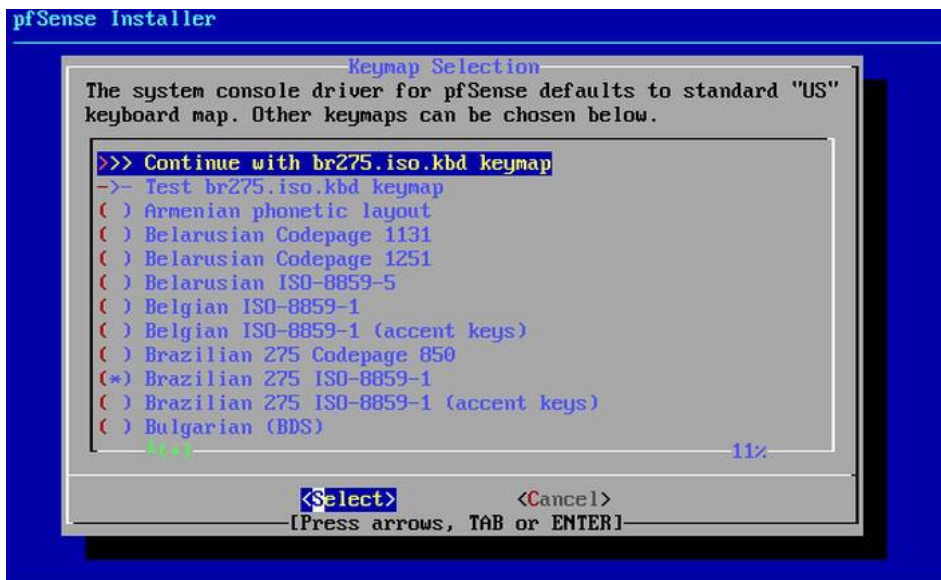
Termos de licenciamento de uso... Accept



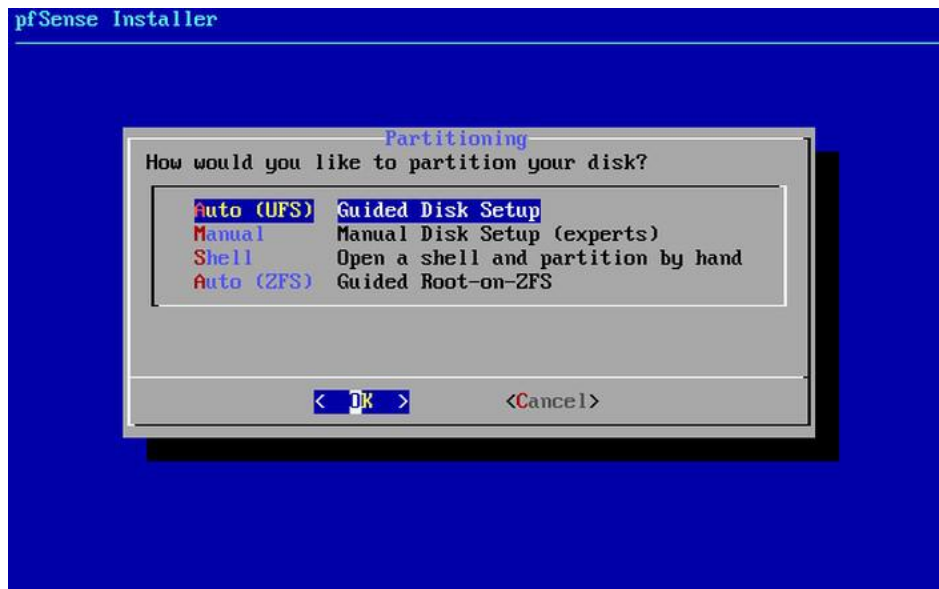
Install...



Escolha o teclado e "S" ou navegue até o Select com o Tab.



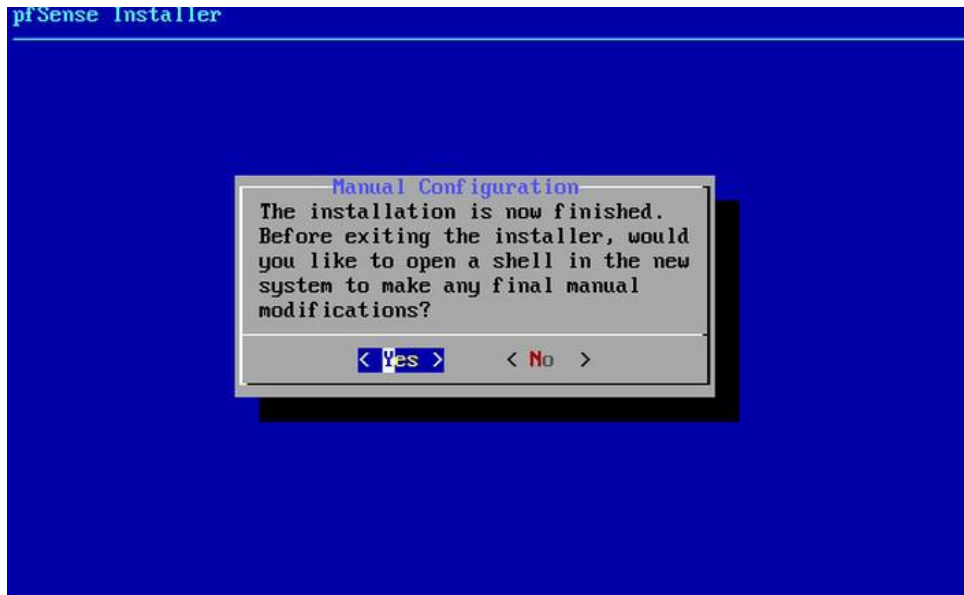
Utilizamos a opção AUTO (ZFS).



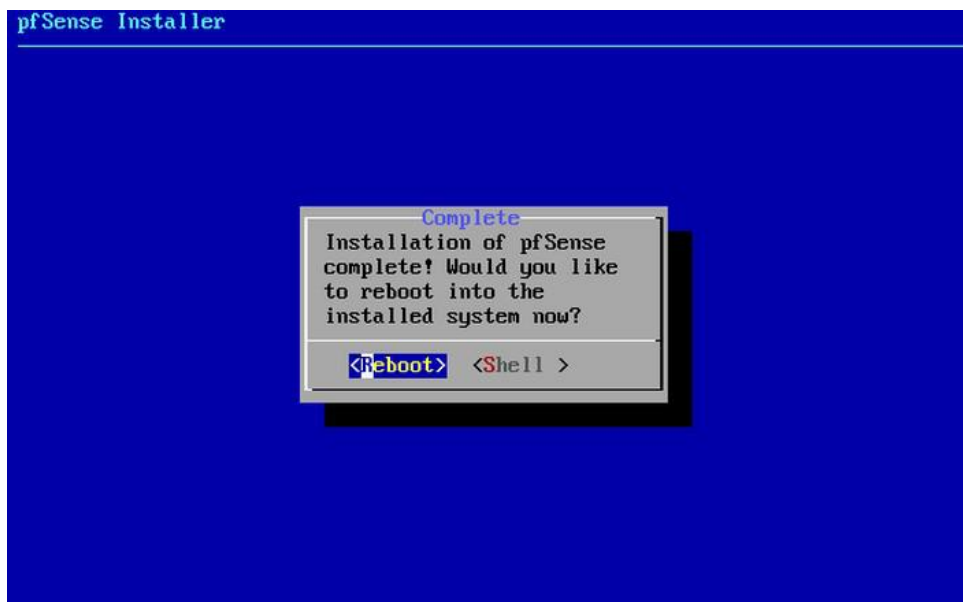
E aguarde a cópia dos arquivos e a instalação.



Caso seja necessária alguma configuração adicional via shell (prompt) selecione Y, no PREVINI inicialmente escolhemos a opção N.



Será necessário reiniciar o sistema.



Instalação concluída! Agora vamos começar as configurações. Ao reiniciar, ele vai procurar pelas placas de rede e é imprescindível que o sistema as encontre, dando tudo certo, ele vai te mostrar as interfaces válidas e te perguntar se quer criar uma VLAN, no caso não é necessário, pois as Vlans são gerenciadas pelo switch cisco, então N.

```
Valid interfaces are:
hn0      00:15:5d:0a:3a:16 (down) Hyper-U Network Interface
hn1      00:15:5d:0a:3a:17 (down) Hyper-U Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y/n]?
```

É possível ver que ele dê um nome qualquer para as duas interfaces de rede e mostrou o status de ambas (down, pq estão desconectadas). Após decidir sobre a VLAN, você deve dizer quem vai ser a sua Wan e Lan.

```
Should VLANs be set up now [y/n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a): hn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn1 a or nothing if finished): hn1

The interfaces will be assigned as follows:

WAN  -> hn0
LAN  -> hn1

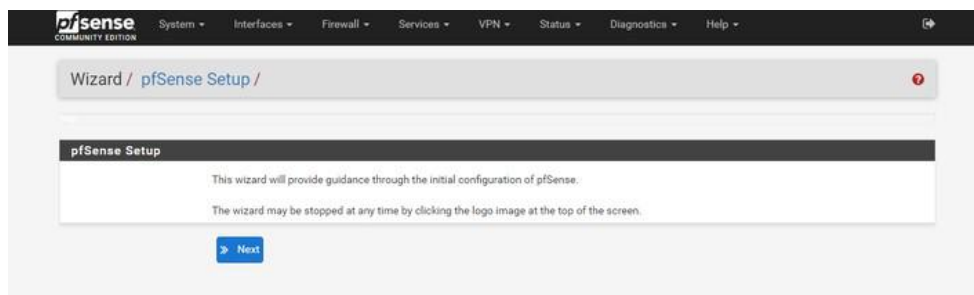
Do you want to proceed [y/n]? y
```

Confirmado, as interfaces vão tentar pegar IP ou será necessário configurar IP manualmente e agora você tem a tela de boas-vindas do pfSense.

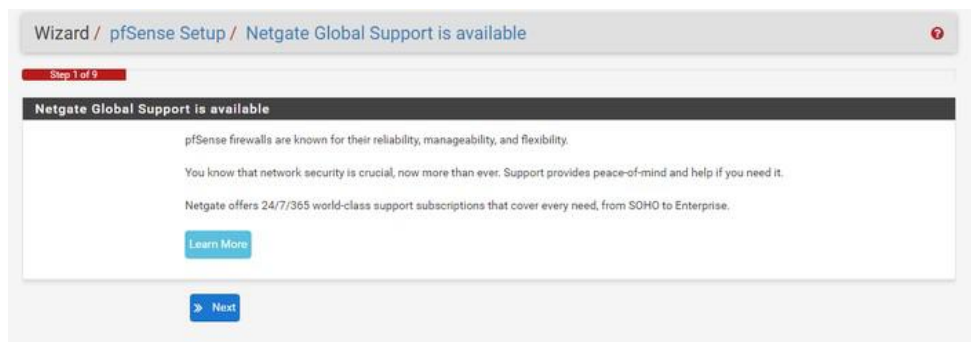
Para acessar a interface web, basta entrar com o ip da Lan no navegador de um computador que esteja nessa rede. O acesso é protegido por usuário e senha.



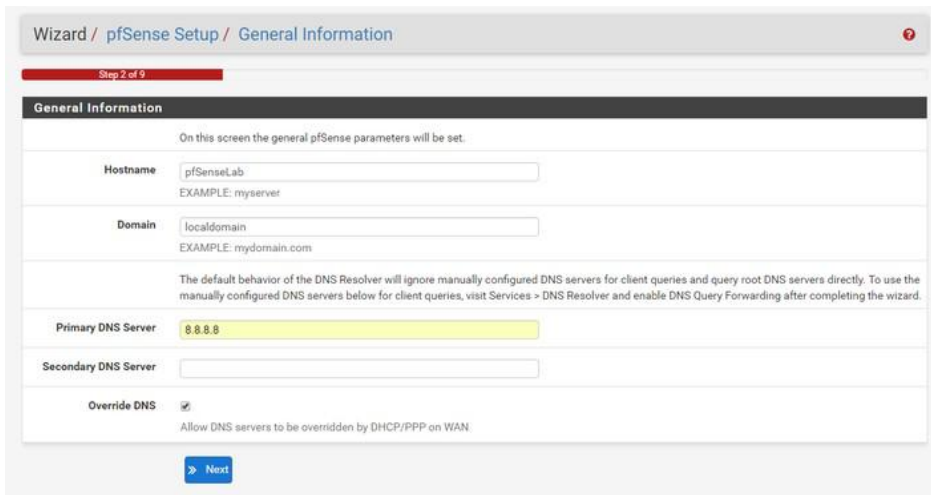
Ao acessar pela primeira vez, temos um assistente para as primeiras configurações.



O passo 1 é sobre o suporte que é oferecido, você pode ler mais sobre isso ou clicar em Next.



Passo 2: você pode configurar um nome, um domínio e DNS .



Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSenseLab
EXAMPLE: myserver

Domain: localdomain
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

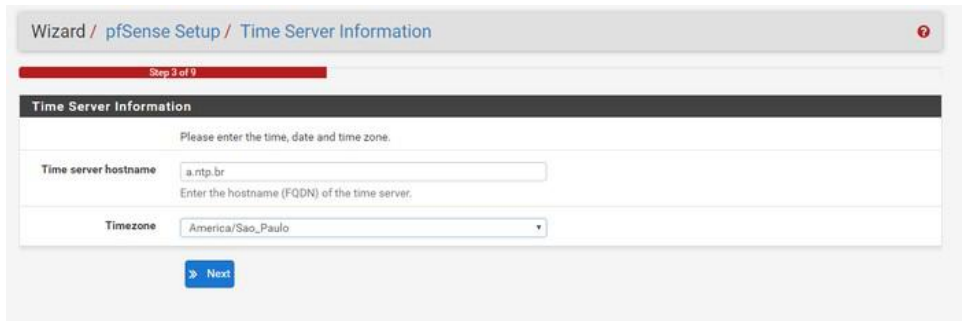
Primary DNS Server: 8.8.8.8

Secondary DNS Server:

Override DNS:
Allow DNS servers to be overridden by DHCP/PPP on WAN.

Next

Passo 3: ele já vem configurado com um servidor de tempo, mas vamos utilizar o *a.ntp.br*, a timezone America/São_Paulo.



Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

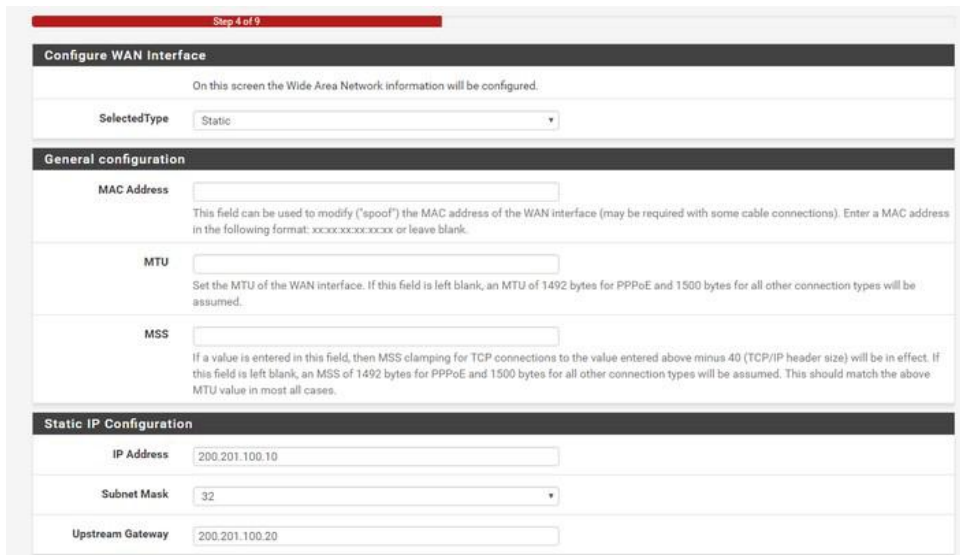
Please enter the time, date and time zone.

Time server hostname: a.ntp.br
Enter the hostname (FQDN) of the time server.

Timezone: America/Sao_Paulo

Next

Passo 4: configurar a Wan, no PREVINI são configuradas 2 Wan (Oi Telemar e Netway)



Step 4 of 9

Configure WAN interface

On this screen the Wide Area Network information will be configured.

SelectedType: Static

General configuration

MAC Address: [text input]
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU: [text input]
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS: [text input]
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address: 200.201.100.10

Subnet Mask: 32

Upstream Gateway: 200.201.100.20

Passo 5: Configurar a Lan. A configuração de IP da LAN

Passo 6: redefinir a senha do administrador.



Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

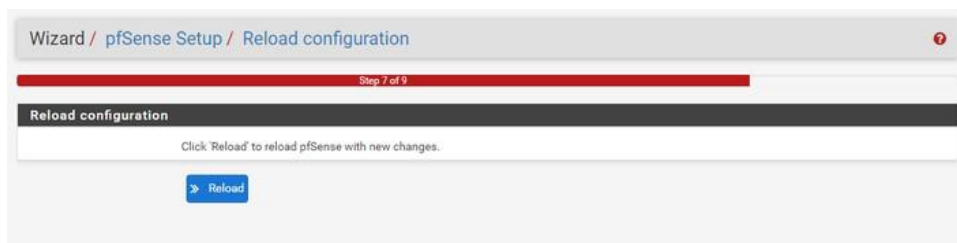
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: [password input]

Admin Password AGAIN: [password input]

Next

Clique em Reload.



Wizard / pfSense Setup / Reload configuration

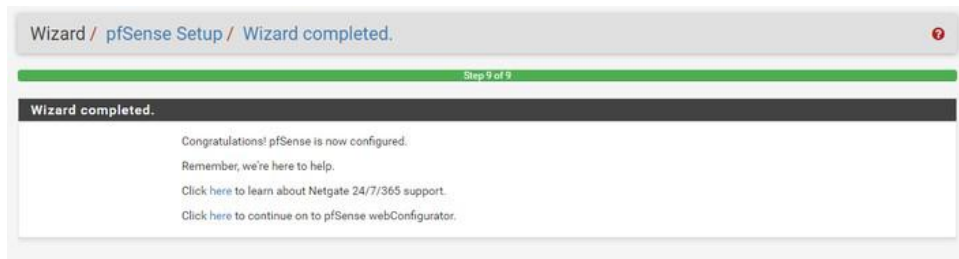
Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

Reload

Clique para continuar no pfSense WebConfigurator.



Pronto, aí está o Dashboard do pfsense (essa tela já está com todos os serviços configurados que são configurados após a instalação).

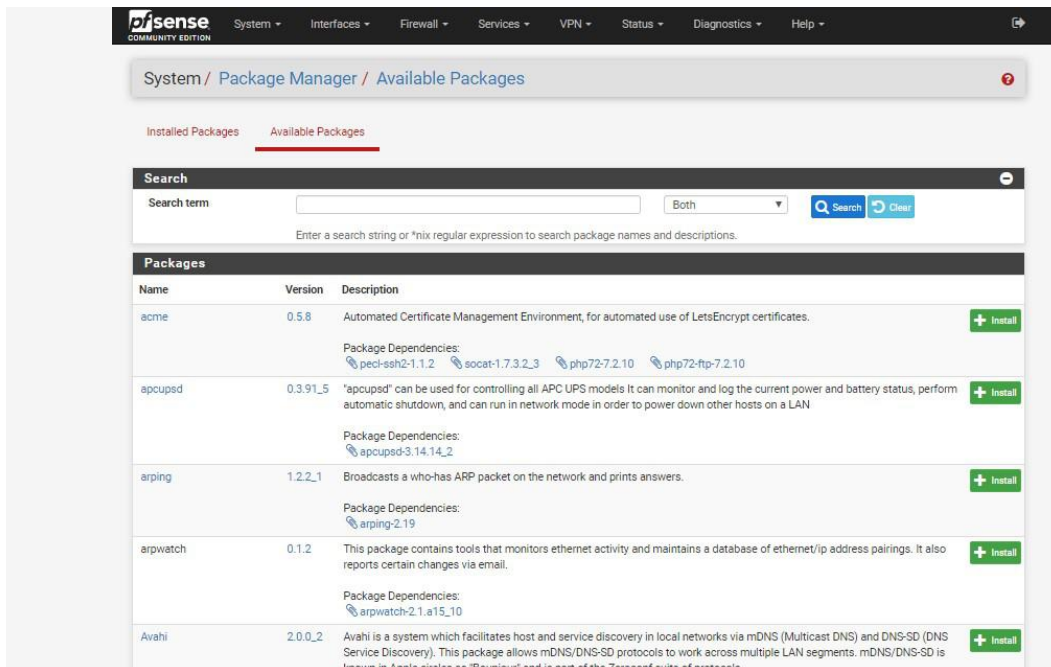
Pacotes Instalados

Os pacotes instalados são:

- Cron
Utilitário usado para gerenciar comandos agendados
- FTP_Client_Proxy
Cliente de Acesso a FTP
- Iftop
Console monitor
- Lightsquid
Gerador de Relatórios de acessos do squid
- Mailreport
Permite o envio de alertas por e-mail
- Ntopng
Ferramenta de relatórios de gerencias
- Open-VM-Tools
Ferramenta de performance de Maquinas Virtuais
- openvpn-client-export
Ferramenta de exportação de usuários de acesso a VPN
- pfBlockerNG
Ferramenta responsável por bloqueios através de Geo Localização
- squid
Ferramenta responsável por gerenciar os acessos HTTP/HTTPS através de Proxy

- squidGuard
Ferramenta que funciona juntamente com o Squid para filtro de proxy URL
- zabbix-agent
Serviço de Agente responsável por permitir envio de coleta de informações ao servidor de monitoramento (Zabbix).

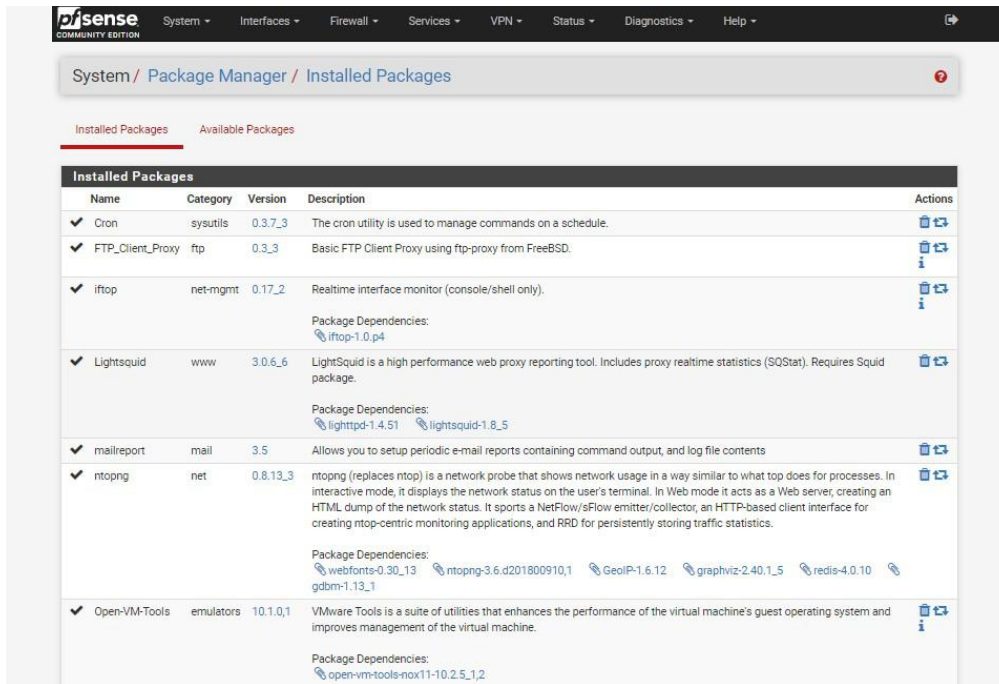
Caso seja necessário instalar algum outro pacote ou serviço, basta clicar na opção Available Packages e clicar no botão +Install.



The screenshot shows the pfSense web interface, specifically the Package Manager section. The breadcrumb trail is "System / Package Manager / Available Packages". There are two tabs: "Installed Packages" and "Available Packages", with the latter being active. A search bar is present with a search term field, a dropdown menu set to "Both", and "Search" and "Clear" buttons. Below the search bar is a table of available packages. Each row includes the package name, version, description, and a green "+ Install" button. Package dependencies are listed below each package description.

Name	Version	Description	Install
acme	0.5.8	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.	+ Install
Package Dependencies: pecl-ssh2-1.1.2 socat-1.7.3.2_3 php72-7.2.10 php72-ftp-7.2.10			
apcupsd	0.3.91_5	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN	+ Install
Package Dependencies: apcupsd-3.14.14_2			
arping	1.2.2_1	Broadcasts a who-has ARP packet on the network and prints answers.	+ Install
Package Dependencies: arping-2.19			
arpwatch	0.1.2	This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email.	+ Install
Package Dependencies: arpwatch-2.1.a15_10			
Avahi	2.0.0_2	Avahi is a system which facilitates host and service discovery in local networks via mDNS (Multicast DNS) and DNS-SD (DNS Service Discovery). This package allows mDNS/DNS-SD protocols to work across multiple LAN segments. mDNS/DNS-SD is known in Apple circles as "Bonjour" and is part of the Zeroconf suite of protocols.	+ Install

Para remover um pacote já instalado, basta clicar no ícone de Lixeira.



Certificate Manager

No PfSense trabalhamos com um gerenciador de certificados, ele gerencia o certificado de acesso HTTPS do próprio PfSense, gerencia os certificados de acesso dos clientes de acesso a Internet através de interceptação SSL e gerencia os certificados de cada usuário de acesso a VPN.

System / Certificate Manager / Certificates

CA's **Certificates** Certificate Revocation

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (57baedfe65e95) Server Certificate CA: No Server: Yes	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-57baedfe65e95, C=US ⓘ Valid From: Mon, 22 Aug 2016 09:20:14 -0300 Valid Until: Sat, 12 Feb 2022 10:20:14 -0200		⚙️ 🔍 🗑️
Certificado PFSense Server Certificate CA: No Server: Yes	CA-INTERNO	emailAddress=willians@previni.com.br, ST=Rio de Janeiro, O=PREVINI, L=Nova Iguacu, CN=prev-net2.previni_ni.com.br, C=BR ⓘ Valid From: Mon, 22 Aug 2016 11:36:29 -0300 Valid Until: Thu, 20 Aug 2026 11:36:29 -0300	webConfigurator OpenVPN Server	⚙️ 🔍 🗑️
Willians User Certificate CA: No Server: No	CA-INTERNO	emailAddress=willians@previni.com.br, ST=Rio de Janeiro, O=PREVINI, L=Nova Iguacu, CN=willians, C=BR ⓘ Valid From: Mon, 24 Oct 2016 15:04:23 -0200 Valid Until: Thu, 22 Oct 2026 14:04:23 -0300		⚙️ 🔍 🗑️

Routing

Na opção de roteamento do pfsense, trabalhamos com gateways, static routes e gateway groups. Foram configurados para o cenário do PREVINI o seguinte:

Gateway:

WANGW → Rota de Internet (Link de internet da operadora Oi – Telemar)

WAN_NETWAY → Rota de Internet (Link de internet da operadora – Netway)

LAN_GW → Responsável pela rota da rede interna.

Utilizamos os endereços de DNS do Google e DNS da Netway para monitorar se o Link esta ativo.

Para adicionar um novo Gateway, basta clicar em Add, preencher os seguintes campos (Destination network, Gateway e Description) e clicar em Salvar.

Static

Routes:

Incluimos as redes de Estações e a rede de Gerência para que o pfsense possa acessar e receber acesso das redes.

Gateway

Groups:

Aqui onde configuramos a redundância e prioridades dos links de internet. Na queda de um link, automaticamente o outro assume e permite conexão com a internet.

Gateways Static Routes Gateway Groups

Gateway Groups				
Group Name	Gateways	Priority	Description	Actions
LB	WAN_NETWAYGW WANGW	Tier 1 Tier 2	Load Balance - IPCONNECT + NetWay	
Failover1	WAN_NETWAYGW WANGW	Tier 1 Tier 2	Failover1	
Failover2	WAN_NETWAYGW WANGW	Tier 2 Tier 1	Failover2	
LB2	WANGW	Tier 1	Publicações	
LB3	WANGW	Tier 1	Publicações	
Default_Gateway_Group_ipv4	WANGW LANGW WAN_NETWAYGW	Tier 2 Tier 3 Tier 1	Default gateway group IPv4	
LB_CPD	WANGW WAN_NETWAYGW	Tier 1 Tier 2	Load Balance - CPD	

Add

Opção onde determinar o default gateway

Default gateway	
Default gateway IPv4	LB (Load Balance - IPCONNECT + NetWay)
	Select the gateway or gatewaygroup to use as the default gateway.
Default gateway IPv6	Automatic
	Select the gateway or gatewaygroup to use as the default gateway.

Save

Update

Sempre importante acompanhar as atualizações do pfsense que são disponibilizados pela comunidade.

A opção utilizada pelo PREVINI é a *Latest stable version*. Significa que ele sempre vai mostrar apenas as versões estáveis do sistema. A atualização não é feita de forma automática, aguardando a confirmação do administrador se deseja efetuar tais atualizações.

É sempre importante antes de atualizar, verificar quais os itens foram atualizados e quais foram as melhorias na versão. Em muitos casos algumas atualizações precipitadas acabam trazendo problemas no funcionamento de diversos serviços.

System Update Update Settings

Confirmation Required to update pfSense system.

Branch Latest stable version (2.4.x) ▼
Please select the branch from which to update the system firmware.
Use of the development version is at your own risk!

Current Base System 2.4.4_3

Latest Base System 2.4.4_3

Status Up to date.


System Update Update Settings

Firmware Branch

Branch Latest stable version (2.4.x) ▼
Latest stable version (2.4.x)
Latest development snapshots (Experimental 2.5.x DEVEL)

Updates

Dashboard check Disable the Dashboard auto-update check

 Save

User Manager

Área responsável pelo gerenciamento de usuários acesso a administração do pfsense e VPN. Nessa tela podemos criar usuários e grupos de usuários e definir permissões.

Para criar um novo usuário, basta clicar em *Add* e preencher os campos que são intuitivos, após necessário informar o grupo que esse usuário participa e clicar em *Save*.

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by: USER

Disabled: This user cannot login

Username:

Password: Confirm Password:

Full name:
User's full name, for administrative information only

Expiration date:
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Group membership:

- admins
- CaptivePortal
- Secure-pfSense

 Not member of: Member of:

Tela abaixo para criação de grupos

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by: USER

Disabled: This user cannot login

Username:

Password: Confirm Password:

Full name:
User's full name, for administrative information only

Expiration date:
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Group membership:

- admins
- CaptivePortal
- Secure-pfSense

 Not member of: Member of:

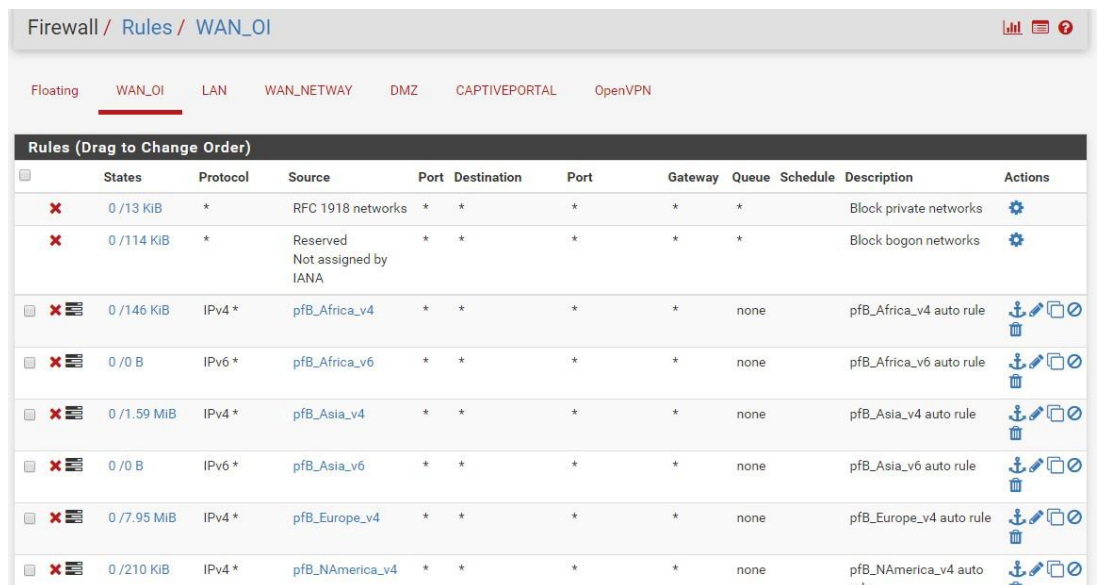
Interfaces

Atualmente utilizamos 5 interfaces de rede.

Regras/Rules

As regras de firewall são definidas por interfaces de rede, ou seja, cada interface de rede deverá ter suas próprias regras.

Nas interfaces de **WAN_OI** e **WAN_NETWAY** determinamos através do pacote BfBlocker diversos bloqueios de GeoLocalização, isso significa que o Bfblocker categoriza listas de IP's/Endereços por continente. Em nosso caso estão listados diversas listas de endereços por continentes bloqueados, sendo assim, qualquer endereço que conste em alguma lista dessas, não conseguira acessar nossos servidores e serão bloqueados de imediatos.

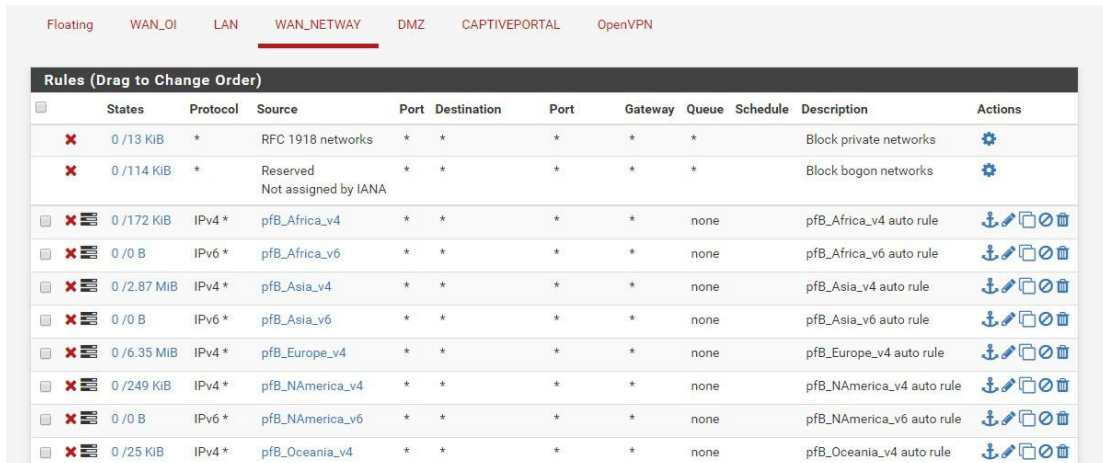


Firewall / Rules / WAN_OI

Floating **WAN_OI** LAN WAN_NETWAY DMZ CAPTIVEPORTAL OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 13 KiB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
0 / 114 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
0 / 146 KiB	IPv4 *	pfb_Africa_v4	*	*	*	*	none		pfb_Africa_v4 auto rule	
0 / 0 B	IPv6 *	pfb_Africa_v6	*	*	*	*	none		pfb_Africa_v6 auto rule	
0 / 1.59 MiB	IPv4 *	pfb_Asia_v4	*	*	*	*	none		pfb_Asia_v4 auto rule	
0 / 0 B	IPv6 *	pfb_Asia_v6	*	*	*	*	none		pfb_Asia_v6 auto rule	
0 / 7.95 MiB	IPv4 *	pfb_Europe_v4	*	*	*	*	none		pfb_Europe_v4 auto rule	
0 / 210 KiB	IPv4 *	pfb_NAmerica_v4	*	*	*	*	none		pfb_NAmerica_v4 auto rule	



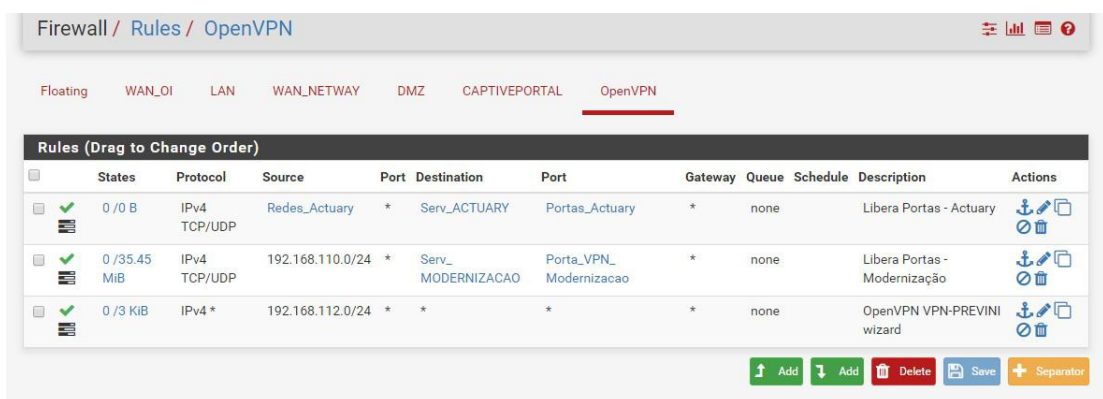
Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0 /13 KIB	*	RFC 1918 networks	*	*	*	*	*	Block private networks	⚙️
✗	0 /114 KIB	*	Reserved Not assigned by IANA	*	*	*	*	*	Block bogon networks	⚙️
☑️	✗	0 /172 KIB	IPv4 *	pfB_Africa_v4	*	*	*	none	pfB_Africa_v4 auto rule	🔗 ⚙️ 🗑️
☑️	✗	0 /0 B	IPv6 *	pfB_Africa_v6	*	*	*	none	pfB_Africa_v6 auto rule	🔗 ⚙️ 🗑️
☑️	✗	0 /2.87 MIB	IPv4 *	pfB_Asia_v4	*	*	*	none	pfB_Asia_v4 auto rule	🔗 ⚙️ 🗑️
☑️	✗	0 /0 B	IPv6 *	pfB_Asia_v6	*	*	*	none	pfB_Asia_v6 auto rule	🔗 ⚙️ 🗑️
☑️	✗	0 /6.35 MIB	IPv4 *	pfB_Europe_v4	*	*	*	none	pfB_Europe_v4 auto rule	🔗 ⚙️ 🗑️
☑️	✗	0 /249 KIB	IPv4 *	pfB_NAmerica_v4	*	*	*	none	pfB_NAmerica_v4 auto rule	🔗 ⚙️ 🗑️
☑️	✗	0 /0 B	IPv6 *	pfB_NAmerica_v6	*	*	*	none	pfB_NAmerica_v6 auto rule	🔗 ⚙️ 🗑️
☑️	✗	0 /25 KIB	IPv4 *	pfB_Oceania_v4	*	*	*	none	pfB_Oceania_v4 auto rule	🔗 ⚙️ 🗑️

Na interface **OpenVPN** configuramos o que cada usuário poderá acessar em nossa rede local. Por padrão os usuários que precisam de acesso VPN são fornecedores de software e o pessoal de TI do próprio PREVINI.

Nos casos dos terceirizados (fornecedor) eles têm permissão de acesso aos servidores em que estão funcionando suas aplicações e banco de dados, não sendo permitido nenhum acesso diferente disso, esse acesso fica restrito também ao número de porta de acesso.

Assim temos VPN's diferentes e regras diferentes quando se trata de fornecedores distintos.



Firewall / Rules / OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☑️	0 /0 B	IPv4	Redes_Actuary	*	Serv_ACTUARY	Portas_Actuary	*	none	Libera Portas - Actuary	🔗 ⚙️ 🗑️
☑️	0 /35.45 MIB	IPv4	192.168.110.0/24	*	Serv_MODERNIZACAO	Porta_VPN_Modernizacao	*	none	Libera Portas - Modernização	🔗 ⚙️ 🗑️
☑️	0 /3 KiB	IPv4 *	192.168.112.0/24	*	*	*	*	none	OpenVPN VPN-PREVINI wizard	🔗 ⚙️ 🗑️

↑ Add ↓ Add 🗑️ Delete 💾 Save ➕ Separator

Na interface **DMZ** configuramos regras específicas para proteger os servidores que disponibilizam serviços publicados na Internet.

A vantagem é que se um desses servidores sofrer algum tipo de ataque na internet, eles estão protegidos dos demais servidores, evitando assim que um vírus possa alastrar.

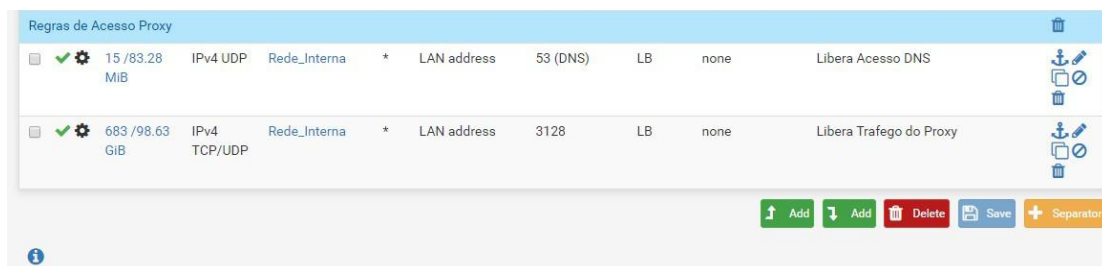
Permitimos somente o estritamente necessário para que o acesso aos serviços possa ser efetivado.

Na interface **LAN** configuramos os acessos de dentro da nossa rede interna para outras redes ou WANs.

Por padrão utilizamos diversos serviços/pacotes para restringir o acesso à internet, o que visa à segurança da rede interna para que não seja permitido que usuários acessem sites inapropriados.

A nossa política de Bloqueio de internet funciona atualmente com o *Squid* e *SquidGuard* que utilizam listas categorizadas de sites inapropriados (blacklist) para acesso, essas listas são atualizadas por uma grande comunidade na internet. A lista utilizada está sob a responsabilidade da **shallaist.de**.

O acesso de usuários de rede para internet é feito através de proxy na porta 3128 (squid). Podemos verificar que na regra de firewall apontamos as saídas de DNS (porta 53) e Proxy (porta 3128) na saída do gateway **LB** (Load Balance de internet)



Regras de Acesso Proxy													
<input type="checkbox"/>	<input checked="" type="checkbox"/>		15 /83.28 MIB	IPv4 UDP	Rede_Interna	*	LAN address	53 (DNS)	LB	none	Libera Acesso DNS		
<input type="checkbox"/>	<input checked="" type="checkbox"/>		683 /98.63 GIB	IPv4 TCP/UDP	Rede_Interna	*	LAN address	3128	LB	none	Libera Trafego do Proxy		

↑ Add ↓ Add Delete Save + Separator

Na interface **CAPTIVEPORTAL** configuramos as regras de acesso ao WiFi do PREVINI. Nessa interface não utilizamos o proxy como saída para internet, utilizamos apenas o firewall permitindo alguns acessos internamente e efetuando bloqueios a sites inapropriados apelidado pela categoria *Pornografia*, como por exemplo: pornografia, pedofilia, violência e etc.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 4 KIB	IPv4 TCP	CAPTIVEPORTAL net	*	Pornografia	*	*	none	Bloqueia Pornografia		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	333 / 116.91 GIB	IPv4 *	CAPTIVEPORTAL net	*	*	*	LB	none			

NAT/Port Forward

Local onde publicamos todos os serviços de internet do PREVINI, normalmente os serviços funcionam via acesso WEB e são publicados na porta 80 (HTTP) para que servidores Ativos, Aposentados e Pensionistas possam usufruir dos serviços.

Tela para criar uma nova publicação

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination Invert match.
Type
Address/mask

Destination port range
From port To port
Specify the port or port range for the destination of the packet for this mapping. The "to" field may be left empty if only mapping a single port.

Redirect target IP
Enter the internal IP address of the server on which to map the ports.
 e.g.: 192.168.1.12

Redirect target port
Port
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
 This is usually identical to the "From port" above.

Description

Squid/SquidGuard

O Squid é um servidor proxy que suporta HTTP, HTTPS, FTP e outros. Ele reduz a utilização da conexão e melhora os tempos de resposta fazendo cache de requisições frequentes de páginas web numa rede de computadores.



PREVINI

RUA ANTENOR DE MOURA RAUNHEITTI, 95, PREVINI, BAIRRO DA LUZ,
NOVA IGUAÇU, RJ.

CNPJ: 03.450.083/0001-09

www.previni.com.br

Fone: (21)2666-2200

As categorias de restrição/bloqueio de acessos estão listadas abaixo:

[blk_BL_webradio]

[blk_BL_webtv]

[blk_BL_spyware]

[blk_BL_socialnet]

[blk_BL_sex_lingerie]

[blk_BL_porn]

[blk_BL_radiotv]

[blk_BL_movies]

[blk_BL_hobby_games-misc]

[blk_BL_hobby_games-online]

[blk_BL_hacking]

[blk_BL_aggressive]

Lista_Whatsapp [Whatsapp]

Diversos sites bloqueados [Bloqueios-Geral]

Relação de Proxy's [Proxys]

Videos [Sites_Videos]

Relação de Radios Online [Radios]

Target Rules List + -			
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.			
Target Categories		Target Categories for off-time	
If 'Time' not defined, this is column will be ignored.			
Sites Liberados [Liberados]	access	—	Sites Liberados [Liberados]
Relação de Radios Online [Radios]	access	deny	Relação de Radios Online [Radios]
Videos [Sites_Videos]	access	deny	Videos [Sites_Videos]
[Google]	access	—	[Google]
[Receita_Federal]	access	—	[Receita_Federal]
Videos Globo [Globo_Videos]	access	whitelist	Videos Globo [Globo_Videos]
Microsoft e Skype [Microsoft-Skype]	access	allow	Microsoft e Skype [Microsoft-Skype]
Lista TeamViewer [TeamViewer]	access	allow	Lista TeamViewer [TeamViewer]
Relação de Bancos [Bancos]	access	allow	Relação de Bancos [Bancos]
Relação de Proxy's [Proxys]	access	deny	Relação de Proxy's [Proxys]
Diversos sites bloqueados [Bloqueios-Geral]	access	deny	Diversos sites bloqueados [Bloqueios-Geral]
ADS [ADS]	access	—	ADS [ADS]
Lista_Whatsapp [Whatsapp]	access	deny	Lista_Whatsapp [Whatsapp]
[blk_BL_adv]	access	—	[blk_BL_adv]
[blk_BL_aggressive]	access	deny	[blk_BL_aggressive]
[blk_BL_alcohol]	access	—	[blk_BL_alcohol]
[blk_BL_anonvpn]	access	—	[blk_BL_anonvpn]
[blk_BL_automobile_bikes]	access	—	[blk_BL_automobile_bikes]
[blk_BL_automobile_boats]	access	—	[blk_BL_automobile_boats]
[blk_BL_automobile_cars]	access	—	[blk_BL_automobile_cars]
[blk_BL_automobile_planes]	access	—	[blk_BL_automobile_planes]
[blk_BL_chat]	access	—	[blk_BL_chat]
[blk_BL_costtraps]	access	—	[blk_BL_costtraps]
[blk_BL_dating]	access	—	[blk_BL_dating]
[blk_BL_downloads]	access	—	[blk_BL_downloads]
[blk_BL_drugs]	access	—	[blk_BL_drugs]
[blk_BL_dynamic]	access	—	[blk_BL_dynamic]
[blk_BL_education_schools]	access	—	[blk_BL_education_schools]
[blk_BL_finance_banking]	access	—	[blk_BL_finance_banking]
[blk_BL_finance_insurance]	access	—	[blk_BL_finance_insurance]
[blk_BL_finance_moneylending]	access	—	[blk_BL_finance_moneylending]
[blk_BL_finance_other]	access	—	[blk_BL_finance_other]
[blk_BL_finance_realestate]	access	—	[blk_BL_finance_realestate]
[blk_BL_finance_trading]	access	—	[blk_BL_finance_trading]
[blk_BL_fortunetelling]	access	—	[blk_BL_fortunetelling]
[blk_BL_forum]	access	—	[blk_BL_forum]
[blk_BL_gamble]	access	—	[blk_BL_gamble]



PREVINI

RUA ANTENOR DE MOURA RAUNHEITTI, 95, PREVINI, BAIRRO DA LUZ,
NOVA IGUAÇU, RJ.

CNPJ: 03.450.083/0001-09

Fone: (21)2666-2200

www.previni.com.br

[blk_BL_government]	access	---	[blk_BL_government]	access	---
[blk_BL_hacking]	access	deny	[blk_BL_hacking]	access	---
[blk_BL_hobby_cooking]	access	---	[blk_BL_hobby_cooking]	access	---
[blk_BL_hobby_games-misc]	access	deny	[blk_BL_hobby_games-misc]	access	---
[blk_BL_hobby_games-online]	access	deny	[blk_BL_hobby_games-online]	access	---
[blk_BL_hobby_gardening]	access	---	[blk_BL_hobby_gardening]	access	---
[blk_BL_hobby_pets]	access	---	[blk_BL_hobby_pets]	access	---
[blk_BL_homestyle]	access	---	[blk_BL_homestyle]	access	---
[blk_BL_hospitals]	access	---	[blk_BL_hospitals]	access	---
[blk_BL_imagehosting]	access	---	[blk_BL_imagehosting]	access	---
[blk_BL_isp]	access	---	[blk_BL_isp]	access	---
[blk_BL_jobsearch]	access	---	[blk_BL_jobsearch]	access	---
[blk_BL_library]	access	---	[blk_BL_library]	access	---
[blk_BL_military]	access	---	[blk_BL_military]	access	---
[blk_BL_models]	access	---	[blk_BL_models]	access	---
[blk_BL_movies]	access	deny	[blk_BL_movies]	access	---
[blk_BL_music]	access	---	[blk_BL_music]	access	---
[blk_BL_news]	access	---	[blk_BL_news]	access	---
[blk_BL_podcasts]	access	---	[blk_BL_podcasts]	access	---
[blk_BL_politics]	access	---	[blk_BL_politics]	access	---
[blk_BL_pom]	access	deny	[blk_BL_pom]	access	---
[blk_BL_radiotv]	access	deny	[blk_BL_radiotv]	access	---
[blk_BL_recreation_humor]	access	---	[blk_BL_recreation_humor]	access	---
[blk_BL_recreation_martialarts]	access	---	[blk_BL_recreation_martialarts]	access	---
[blk_BL_recreation_restaurants]	access	---	[blk_BL_recreation_restaurants]	access	---
[blk_BL_recreation_sports]	access	---	[blk_BL_recreation_sports]	access	---
[blk_BL_recreation_travel]	access	---	[blk_BL_recreation_travel]	access	---
[blk_BL_recreation_wellness]	access	---	[blk_BL_recreation_wellness]	access	---
[blk_BL_redirector]	access	---	[blk_BL_redirector]	access	---
[blk_BL_religion]	access	---	[blk_BL_religion]	access	---
[blk_BL_remotecontrol]	access	---	[blk_BL_remotecontrol]	access	---
[blk_BL_ringtones]	access	---	[blk_BL_ringtones]	access	---
[blk_BL_science_astronomy]	access	---	[blk_BL_science_astronomy]	access	---
[blk_BL_science_chemistry]	access	---	[blk_BL_science_chemistry]	access	---
[blk_BL_searchengines]	access	---	[blk_BL_searchengines]	access	---
[blk_BL_sex_education]	access	---	[blk_BL_sex_education]	access	---
[blk_BL_sex_lingerie]	access	deny	[blk_BL_sex_lingerie]	access	---
[blk_BL_shopping]	access	---	[blk_BL_shopping]	access	---
[blk_BL_socialnet]	access	deny	[blk_BL_socialnet]	access	---
[blk_BL_spyware]	access	deny	[blk_BL_spyware]	access	---
[blk_BL_tracker]	access	---	[blk_BL_tracker]	access	---
[blk_BL_updatesites]	access	---	[blk_BL_updatesites]	access	---
[blk_BL_urlshortener]	access	---	[blk_BL_urlshortener]	access	---



PREVINI

RUA ANTENOR DE MOURA RAUNHEITTI, 95, PREVINI, BAIRRO DA LUZ,
NOVA IGUAÇU, RJ.

CNPJ: 03.450.083/0001-09

Fone: (21)2666-2200

www.previsi.com.br

[blk_BL_tracker]	access	---	[blk_BL_tracker]	access	---
[blk_BL_updatesites]	access	---	[blk_BL_updatesites]	access	---
[blk_BL_urlshortener]	access	---	[blk_BL_urlshortener]	access	---
[blk_BL_violence]	access	---	[blk_BL_violence]	access	---
[blk_BL_warez]	access	---	[blk_BL_warez]	access	---
[blk_BL_weapons]	access	---	[blk_BL_weapons]	access	---
[blk_BL_webmail]	access	---	[blk_BL_webmail]	access	---
[blk_BL_webphone]	access	---	[blk_BL_webphone]	access	---
[blk_BL_webradio]	access	deny	[blk_BL_webradio]	access	---
[blk_BL_webtv]	access	deny	[blk_BL_webtv]	access	---
Default access [all]	access	allow	Default access [all]	access	allow

Do not allow IP-Addresses in URL To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

Redirect mode
 Select redirect mode here.
 Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible.
 Options: [ext url err page](#), [ext url redirect](#), [ext url as 'move'](#), [ext url as 'found'](#).

Redirect
 Enter the external redirection URL, error message or size (bytes) here.

Use SafeSearch engine To protect your children from adult content you can use the protected mode of search engines.
 At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search and Bing. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.
 Note: This option overrides 'Rewrite' setting.

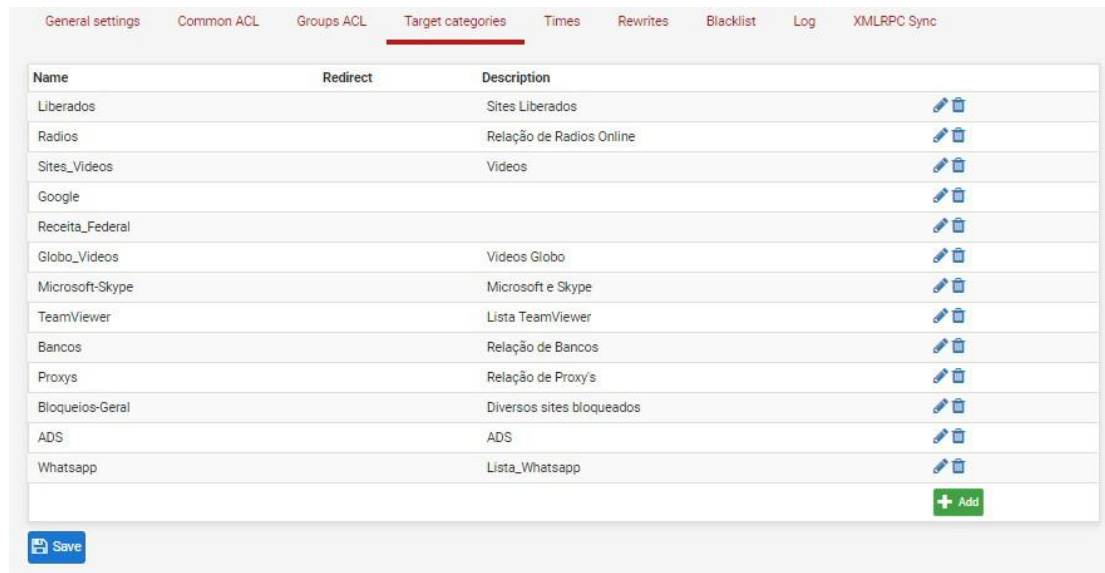
Rewrite
 Enter the rewrite condition name for this rule or leave it blank.

Rewrite for off-time
 Enter the rewrite condition name for this rule or leave it blank.

Description
 You may enter any description here for your reference.

Log Check this option to enable logging for this ACL.

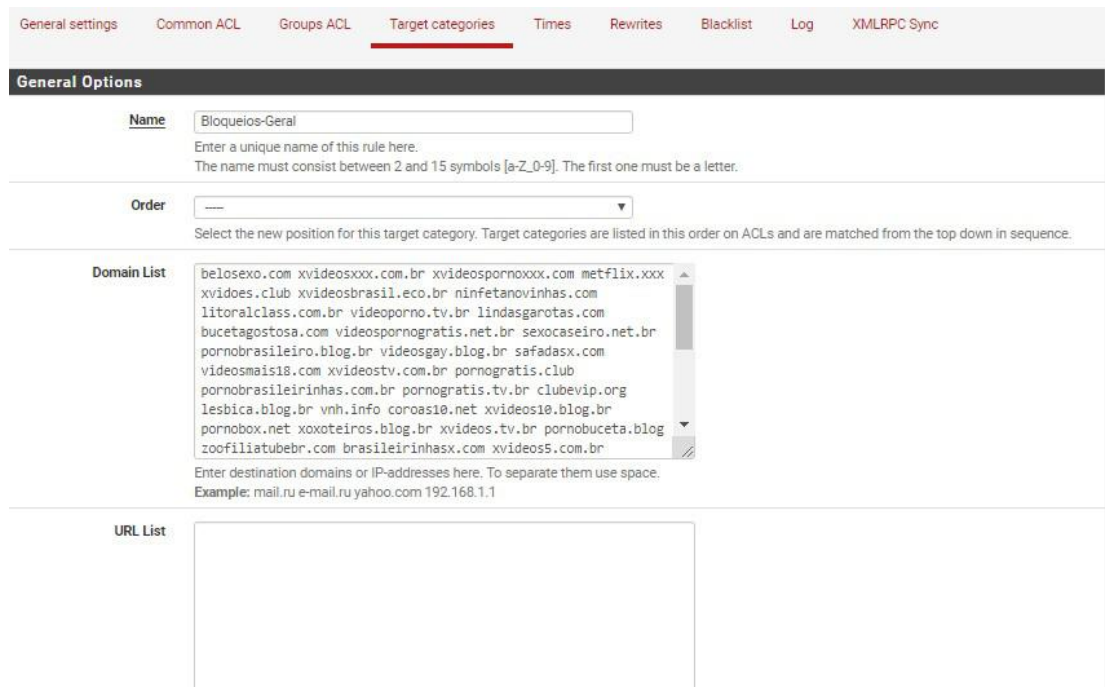
Podemos criar categorias próprias e de forma manual conforme tela abaixo:



The screenshot shows the 'Target categories' management interface. At the top, there are navigation tabs: General settings, Common ACL, Groups ACL, Target categories (selected), Times, Rewrites, Blacklist, Log, and XMLRPC Sync. Below the tabs is a table with the following columns: Name, Redirect, and Description. The table contains the following entries:

Name	Redirect	Description
Liberados		Sites Liberados
Rádios		Relação de Rádios Online
Sites_Videos		Videos
Google		
Receita_Federal		
Globo_Videos		Videos Globo
Microsoft-Skype		Microsoft e Skype
TeamViewer		Lista TeamViewer
Bancos		Relação de Bancos
Proxys		Relação de Proxy's
Bloqueios-Geral		Diversos sites bloqueados
ADS		ADS
Whatsapp		Lista_Whatsapp

At the bottom of the table, there is a '+ Add' button and a 'Save' button.



The screenshot shows the 'General Options' form for creating a new target category. At the top, there are navigation tabs: General settings, Common ACL, Groups ACL, Target categories (selected), Times, Rewrites, Blacklist, Log, and XMLRPC Sync. Below the tabs is a section titled 'General Options' with the following fields:

- Name:** Bloqueios-Geral. Below the input field, there is a note: "Enter a unique name of this rule here. The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter."
- Order:** A dropdown menu with a downward arrow. Below it, there is a note: "Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence."
- Domain List:** A text area containing a list of domains:


```
belosexo.com xvideosxxx.com.br xvideospornoxxx.com metflix.xxx
xvideos.club xvideosbrasil.eco.br ninfetanovinhas.com
litoralclass.com.br videoporno.tv.br lindasgarotas.com
bucetagostosa.com videospornogratis.net.br sexocaseiro.net.br
pornobrasileiro.blog.br videosgay.blog.br safadasx.com
videosmais18.com xvideostv.com.br pornogratis.club
pornobrasileirinhas.com.br pornogratis.tv.br clubevip.org
lesbica.blog.br vnh.info coroa10.net xvideos10.blog.br
pornobox.net xoxoteiros.blog.br xvideos.tv.br pornobuceta.blog
zoofiliatubebr.com brasileirinhasx.com xvideos5.com.br
```

 Below the text area, there is a note: "Enter destination domains or IP-addresses here. To separate them use space. Example: mail.ru e-mail.ru yahoo.com 192.168.1.1"
- URL List:** An empty text area.

Bloqueios são feitos por expressões regulares também:

URL List

Enter destination URLs here. To separate them use space.
Example: host.com/xxx 12.10.220.125/alisa

Regular Expression

`xxx|facebook`

Enter word fragments of the destination URL. To separate them use |. Example: mail(casino|game)\.rdsf\$

Redirect mode

none

Select redirect mode here.
Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible.
Options: [ext url err page](#), [ext url redirect](#), [ext url as 'move'](#), [ext url as 'found'](#).

Redirect

Enter the external redirection URL, error message or size (bytes) here.


Description

Diversos sites bloqueados

You may enter any description here for your reference.

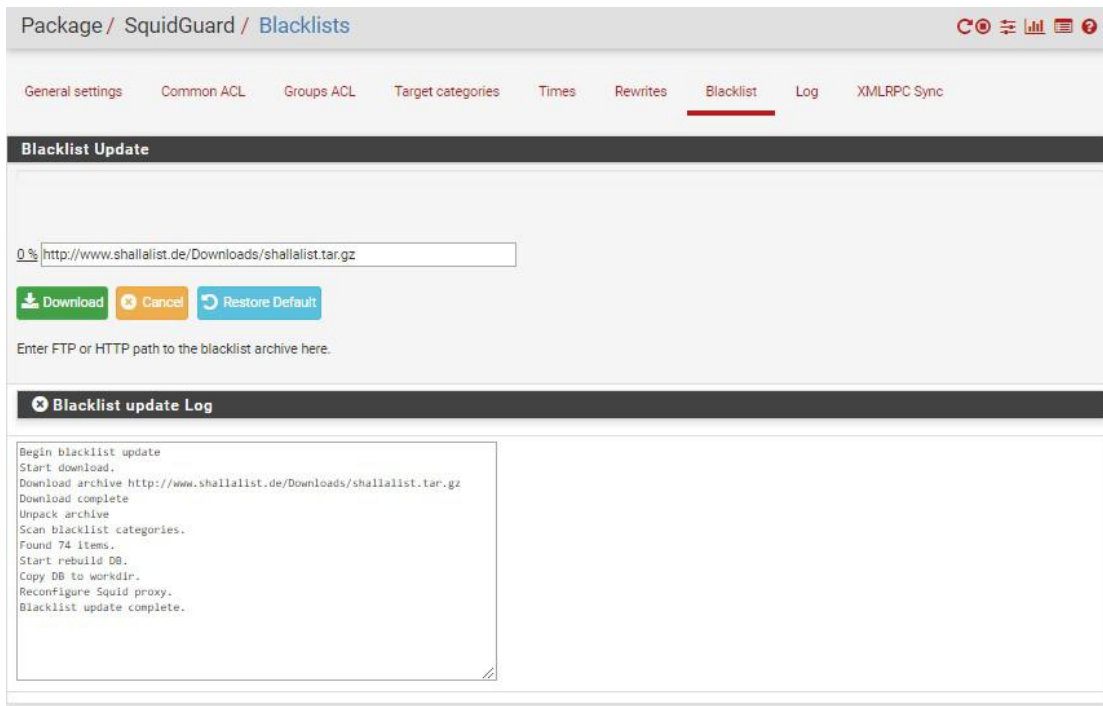
Log

Check this option to enable logging for this ACL.



Configuração da Blacklist

Essa tela onde configuramos o endereço da blacklist que será utilizada e atualizada.



The screenshot shows the SquidGuard web interface for configuring Blacklists. The breadcrumb path is "Package / SquidGuard / Blacklists". The "Blacklist" tab is selected in the navigation menu. The "Blacklist Update" section contains a text input field with the URL "http://www.shallalist.de/Downloads/shallalist.tar.gz". Below the input are three buttons: "Download", "Cancel", and "Restore Default". A note below the buttons says "Enter FTP or HTTP path to the blacklist archive here." The "Blacklist update Log" section shows a log of the update process:

```
Begin blacklist update
Start download.
Download archive http://www.shallalist.de/Downloads/shallalist.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 74 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.
```

Package / Proxy filter SquidGuard: General settings / General settings

General settings | Common ACL | Groups ACL | Target categories | Times | Rewrites | Blacklist | Log | XMLRPC Sync

General Options

Enable Check this option to enable squidGuard.
 Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details.
 The Save button at the bottom of this page must be clicked to save configuration changes.
 To activate squidGuard configuration changes, **the Apply button must be clicked.**

SquidGuard service state: **STARTED**

LDAP Options

Enable LDAP Filter Enable options for setup ldap connection to create filters with ldap search

LDAP DN
 Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)

LDAP DN Password
 Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z][a-zA-Z0-9/_\.\|\;\|\+\?=&]

Strip NT domain name Strip NT domain name component from user names (/ or \ separated).

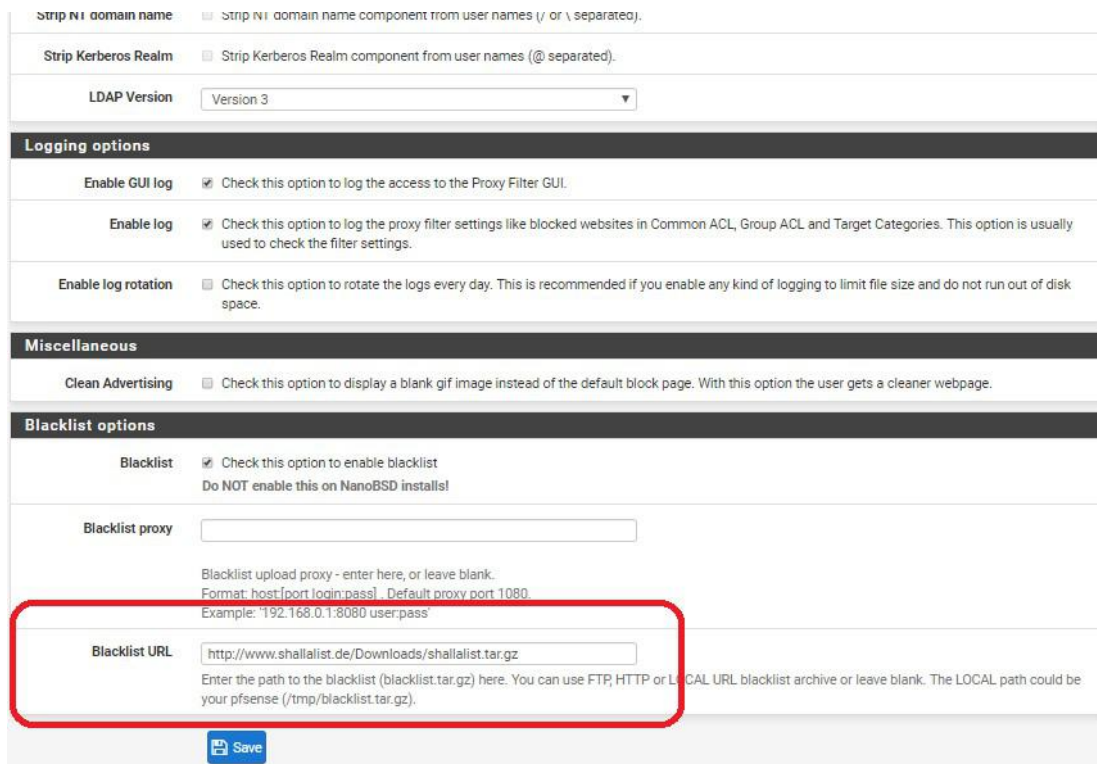
Strip Kerberos Realm Strip Kerberos Realm component from user names (@ separated).

LDAP Version

Logging options

Enable GUI log Check this option to log the access to the Proxy Filter GUI.

Enable log Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.



The screenshot shows a configuration interface for Proxy Filter. It includes sections for 'Logging options', 'Miscellaneous', and 'Blacklist options'. The 'Blacklist URL' field is highlighted with a red box and contains the value 'http://www.shallalist.de/Downloads/shallalist.tar.gz'. Below this field is a 'Save' button.

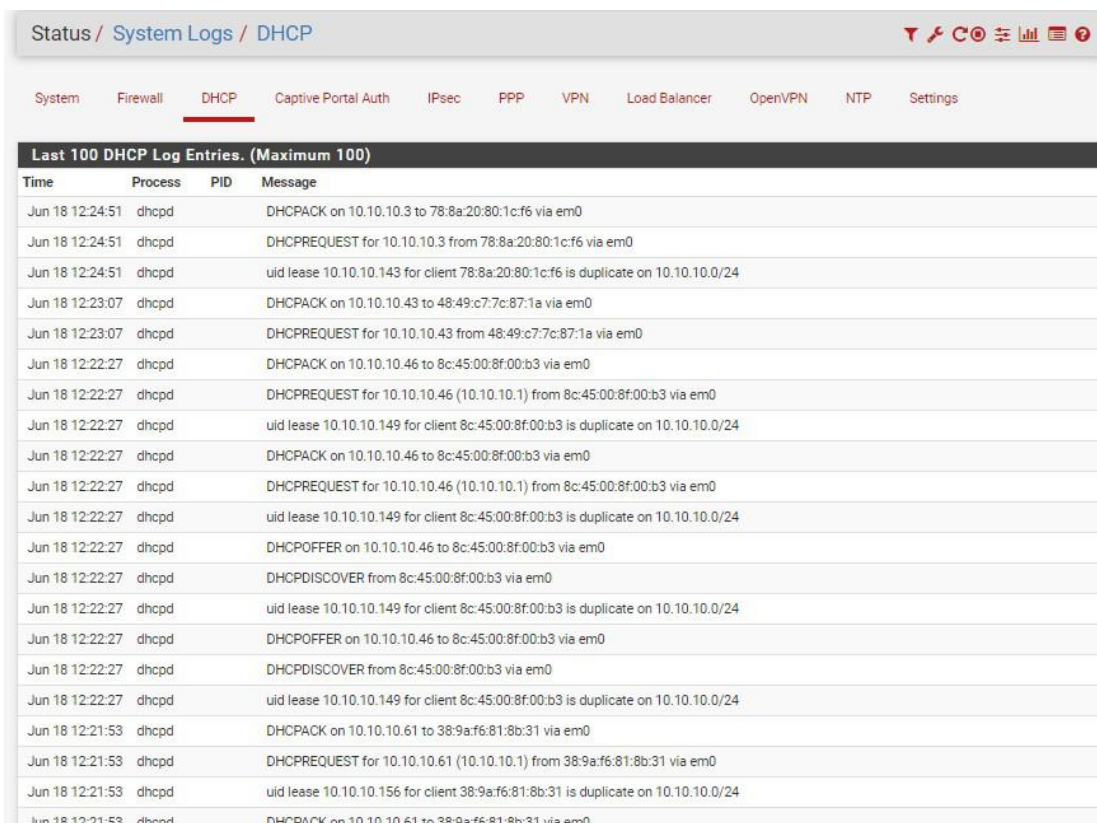
Log/Firewall

Podemos verificar em tempo real todos os bloqueios efetuados pelo firewall, de dentro pra fora, quanto de fora para dentro.

Podemos identificar a Interface (interface) utilizada, o endereço de origem (source) e o endereço de destino (Destination), bem como o protocolo (Protocol). Com essas informações de LOG, o administrador pode tomar diversas medidas para restringir ainda mais um acesso, ou permitir um acesso que está restrito.

Log/DHCP

Podemos verificar as distribuições de IP para a rede Wifi do servidor DHCP exclusivo de acesso WiFi.



The screenshot shows the Mikrotik WinBox interface for DHCP logs. The breadcrumb navigation is 'Status / System Logs / DHCP'. Below the navigation menu, there is a table titled 'Last 100 DHCP Log Entries. (Maximum 100)'. The table has four columns: Time, Process, PID, and Message. The logs show a sequence of DHCP transactions including requests, offers, leases, and acknowledgments for various IP addresses on the em0 interface.

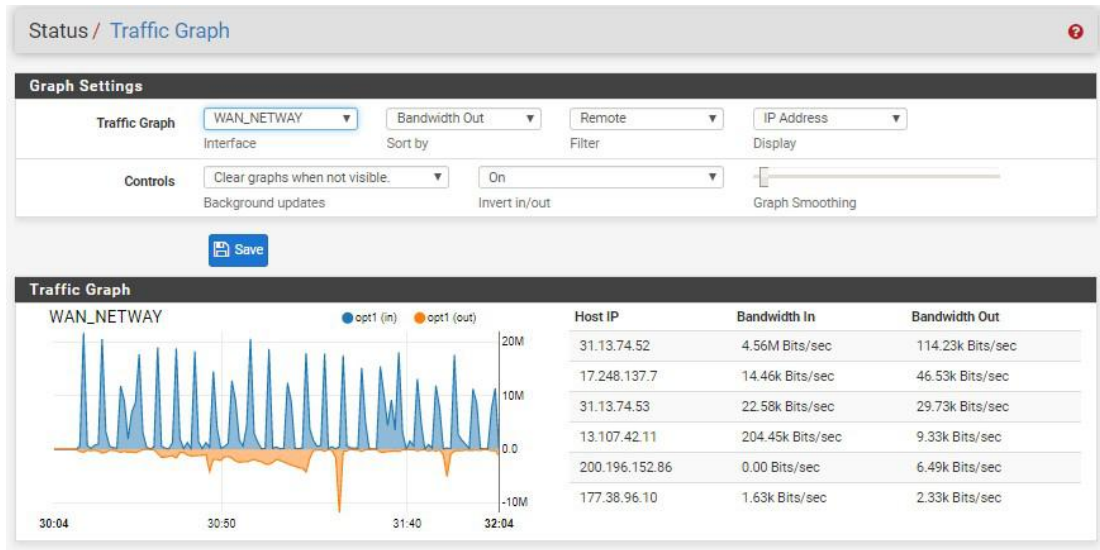
Time	Process	PID	Message
Jun 18 12:24:51	dhcpcd		DHCPACK on 10.10.10.3 to 78:8a:20:80:1c:f6 via em0
Jun 18 12:24:51	dhcpcd		DHCPREQUEST for 10.10.10.3 from 78:8a:20:80:1c:f6 via em0
Jun 18 12:24:51	dhcpcd		uid lease 10.10.10.143 for client 78:8a:20:80:1c:f6 is duplicate on 10.10.10.0/24
Jun 18 12:23:07	dhcpcd		DHCPACK on 10.10.10.43 to 48:49:c7:7c:87:1a via em0
Jun 18 12:23:07	dhcpcd		DHCPREQUEST for 10.10.10.43 from 48:49:c7:7c:87:1a via em0
Jun 18 12:22:27	dhcpcd		DHCPACK on 10.10.10.46 to 8c:45:00:8f:00:b3 via em0
Jun 18 12:22:27	dhcpcd		DHCPREQUEST for 10.10.10.46 (10.10.10.1) from 8c:45:00:8f:00:b3 via em0
Jun 18 12:22:27	dhcpcd		uid lease 10.10.10.149 for client 8c:45:00:8f:00:b3 is duplicate on 10.10.10.0/24
Jun 18 12:22:27	dhcpcd		DHCPACK on 10.10.10.46 to 8c:45:00:8f:00:b3 via em0
Jun 18 12:22:27	dhcpcd		DHCPREQUEST for 10.10.10.46 (10.10.10.1) from 8c:45:00:8f:00:b3 via em0
Jun 18 12:22:27	dhcpcd		uid lease 10.10.10.149 for client 8c:45:00:8f:00:b3 is duplicate on 10.10.10.0/24
Jun 18 12:22:27	dhcpcd		DHCPOFFER on 10.10.10.46 to 8c:45:00:8f:00:b3 via em0
Jun 18 12:22:27	dhcpcd		DHCPDISCOVER from 8c:45:00:8f:00:b3 via em0
Jun 18 12:22:27	dhcpcd		uid lease 10.10.10.149 for client 8c:45:00:8f:00:b3 is duplicate on 10.10.10.0/24
Jun 18 12:22:27	dhcpcd		DHCPOFFER on 10.10.10.46 to 8c:45:00:8f:00:b3 via em0
Jun 18 12:22:27	dhcpcd		DHCPDISCOVER from 8c:45:00:8f:00:b3 via em0
Jun 18 12:22:27	dhcpcd		uid lease 10.10.10.149 for client 8c:45:00:8f:00:b3 is duplicate on 10.10.10.0/24
Jun 18 12:21:53	dhcpcd		DHCPACK on 10.10.10.61 to 38:9a:f6:81:8b:31 via em0
Jun 18 12:21:53	dhcpcd		DHCPREQUEST for 10.10.10.61 (10.10.10.1) from 38:9a:f6:81:8b:31 via em0
Jun 18 12:21:53	dhcpcd		uid lease 10.10.10.156 for client 38:9a:f6:81:8b:31 is duplicate on 10.10.10.0/24
Jun 18 12:21:53	dhcpcd		DHCPACK on 10.10.10.61 to 38:9a:f6:81:8b:31 via em0

Log/OpenVPN

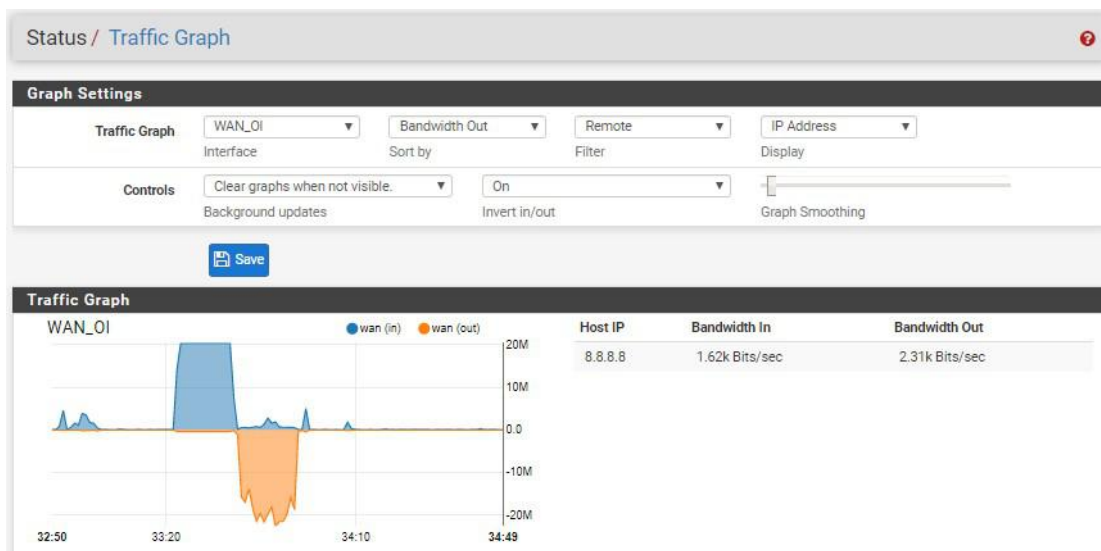
Podemos identificar e acompanhar todos os acessos efetuados pela VPN.

Status/Traffic Graph

Podemos acompanhar em tempo real o gráfico de acesso pelo link de Internet NETWAY



Podemos acompanhar em tempo real o gráfico de acesso pelo link de Internet OI – Telemar



8 - Anexo III – Demonstrativo dos RACKS

