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 necessitarem 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 continuadamente. 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.

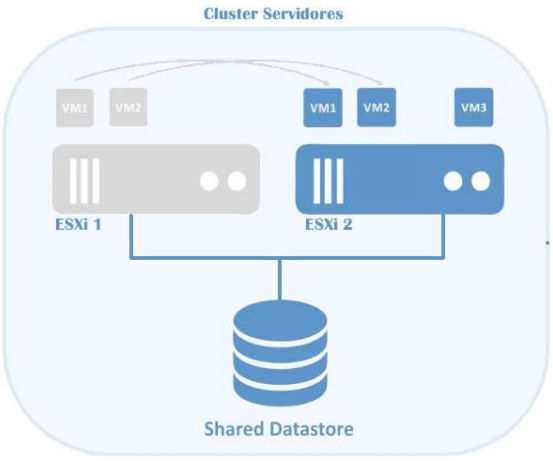
4.1.1.2 A Gerência da Divisão de Informática do PREVINI utiliza 2(dois) clusters, sendo um para redundância de servidores virtuais e outro para redundância de desktops virtuais.

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.

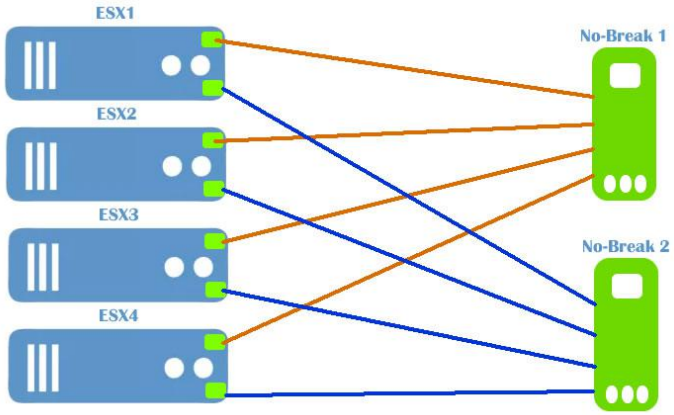


4.1.1.4 **REDUNDÂNCIA EM FONTE DE ENERGIA**

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.



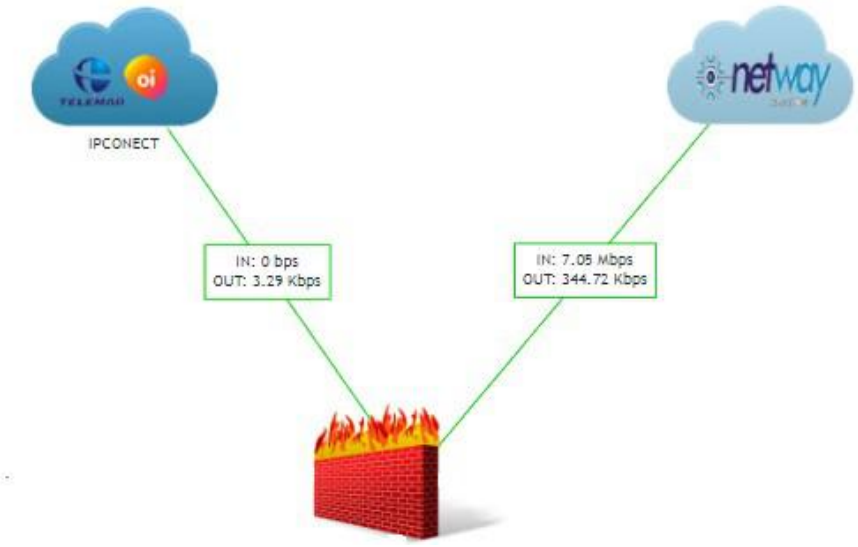
4.1.1.5 **REDUNDÂNCIA EM REDES**

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.

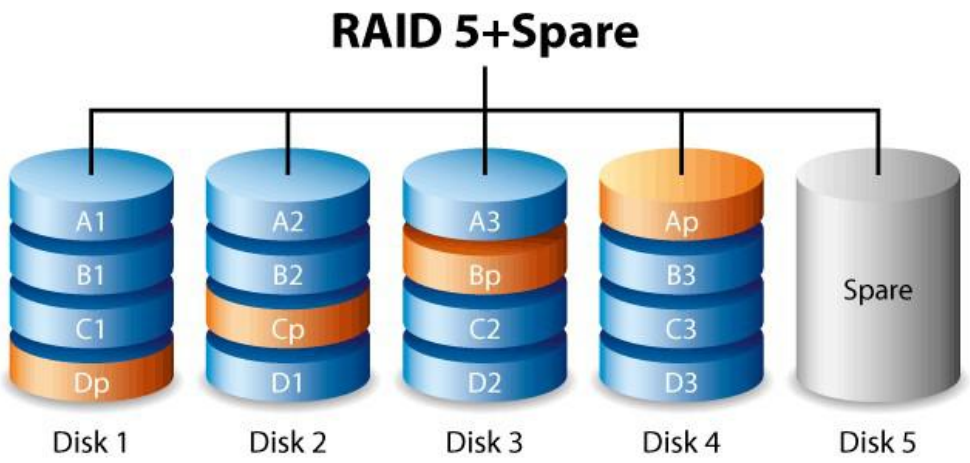
4.1.1.7 REDUNDÂNCIA EM DADOS

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 foi 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.

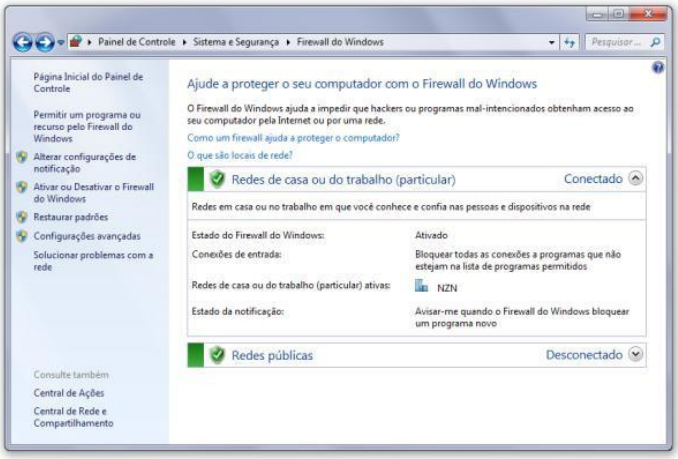
- Oi Telemar
- NetWay Telecom

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

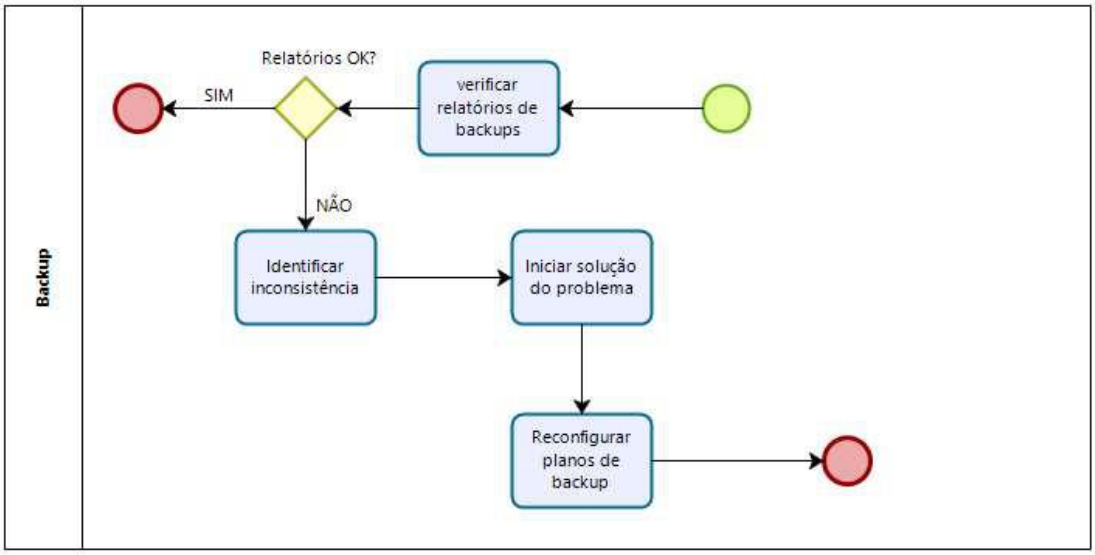
4.1.7.1 A Gerência da Divisão de Informática deverá, durante todo o expediente de trabalho, prestar suporte aos colaboradores do PREVINI. As demandas do help desk devem ser direcionadas para os ramais 2227 e 2228.

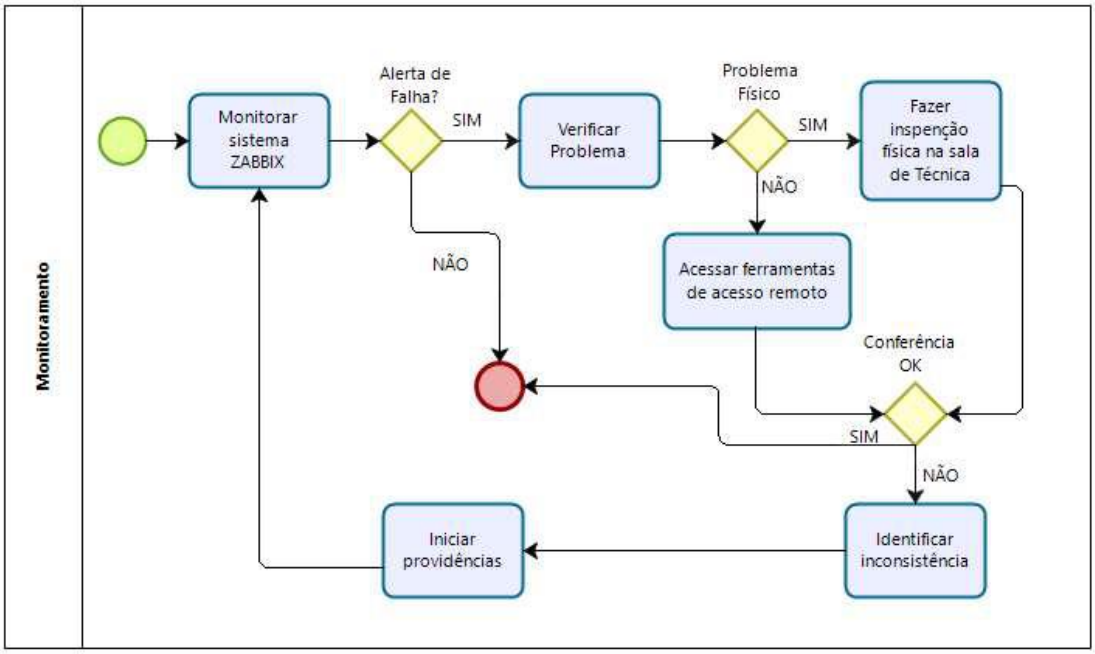
4.1.7.2 A Gerência da Divisão de Informática deverá ainda prestar suporte aos aposentados e pensionistas do Município de Nova Iguaçu quando da solicitação dos assuntos listados abaixo.

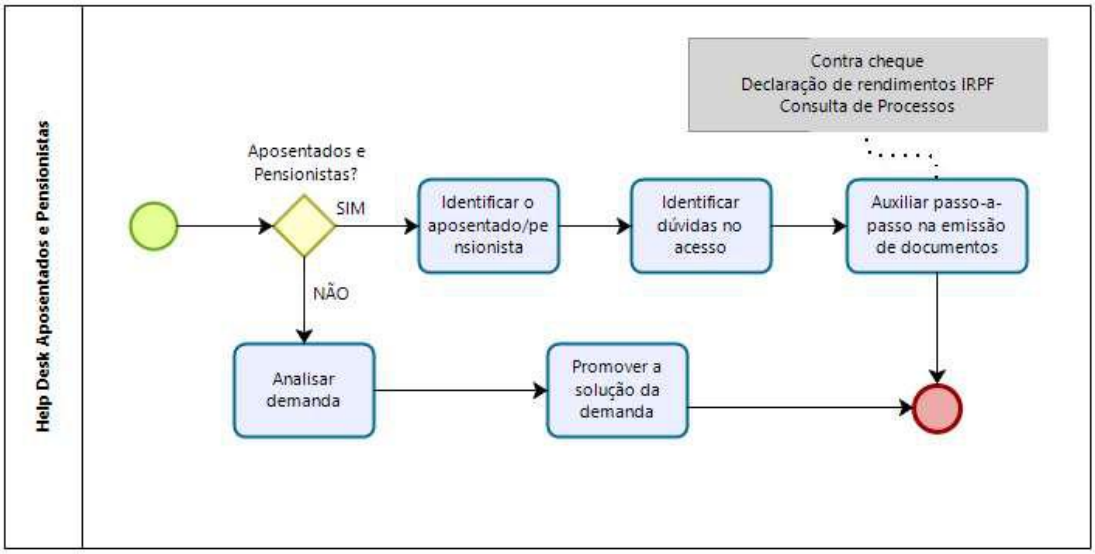
- Emissão de contracheque;
- Declaração de imposto de renda;
- Consulta processo online.

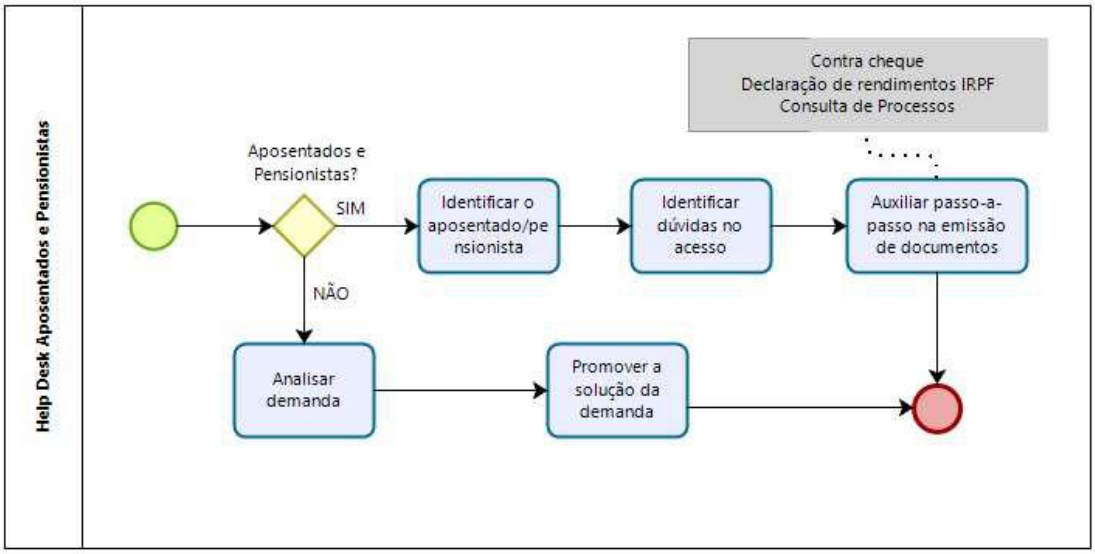
Os aposentados e pensionistas que precisarem dos serviços deverá ligar para o tele atendimento do PREVINI no telefone (21) 2666-2200 informando das dificuldades ou problemas para acessar os serviços, após entender a situação, a telefonista transfere a ligação para os ramais 2227 ou 2228.

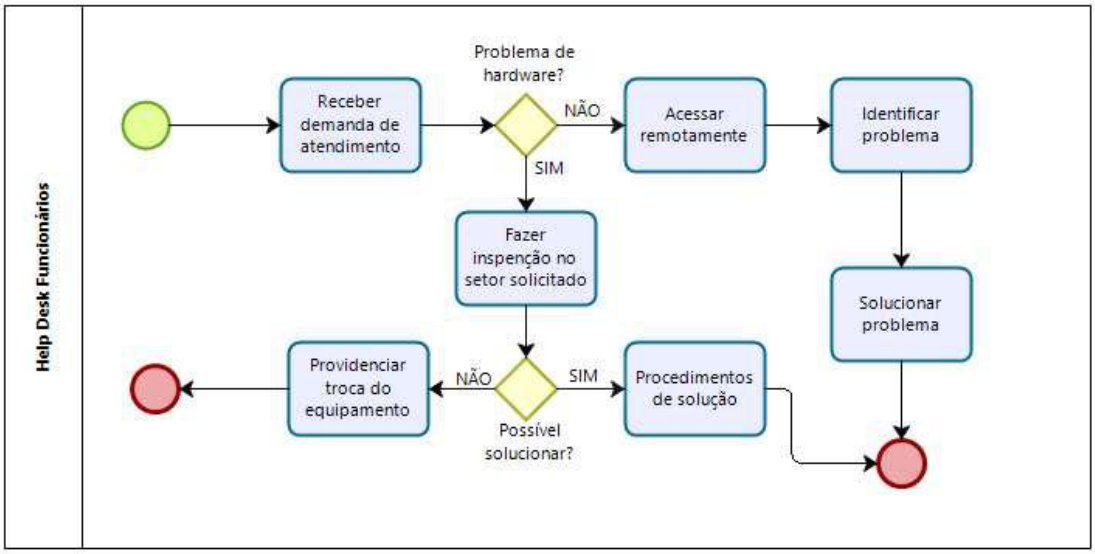
5 MAPEAMENTO




Monitoramento
Monitorar sistema ZABBIX
Alerta de Falha?
SIM
NÃO
Verificar Problema
Problema Físico
SIM
NÃO
Fazer inspenção física na sala de Técnica
Acessar ferramentas de acesso remoto
Conferência OK
SIM
NÃO
Identificar inconsistência
Iniciar providências


Help Desk Aposentados e Pensionistas
Contra cheque
Declaração de rendimentos IRPF
Consulta de Processos
Aposentados e Pensionistas?
SIM
NÃO
Identificar o aposentado/pensionista
Identificar dúvidas no acesso
Auxiliar passo-a-passo na emissão de documentos
Analisar demanda
Promover a solução da demanda


Help Desk Aposentados e Pensionistas
Contra cheque
Declaração de rendimentos IRPF
Consulta de Processos
Aposentados e Pensionistas?
SIM
NÃO
Identificar o aposentado/pensionista
Identificar dúvidas no acesso
Auxiliar passo-a-passo na emissão de documentos
Analisar demanda
Promover a solução da demanda

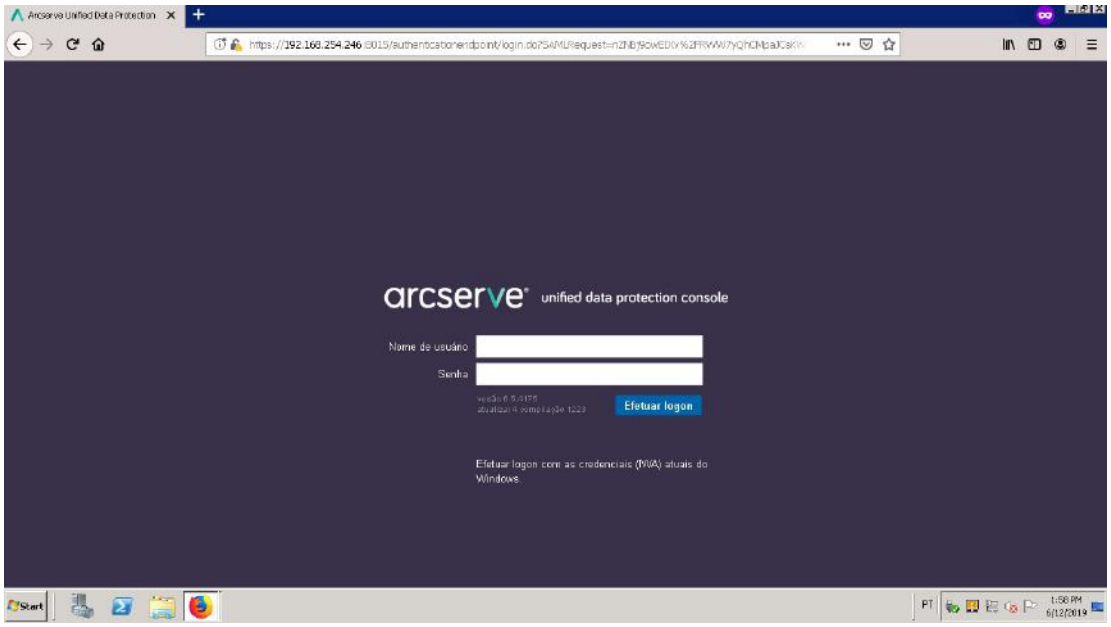

Help Desk Funcionários
Receber demanda de atendimento
Problema de hardware?
NÃO
SIM
Acessar remotamente
Identificar problema
Fazer inspenção no setor solicitado
Solucionar problema
Providenciar troca do equipamento
NÃO
SIM
Possível solucionar?
Procedimentos de solução

6 - Anexo I – Instalação do ARCserve

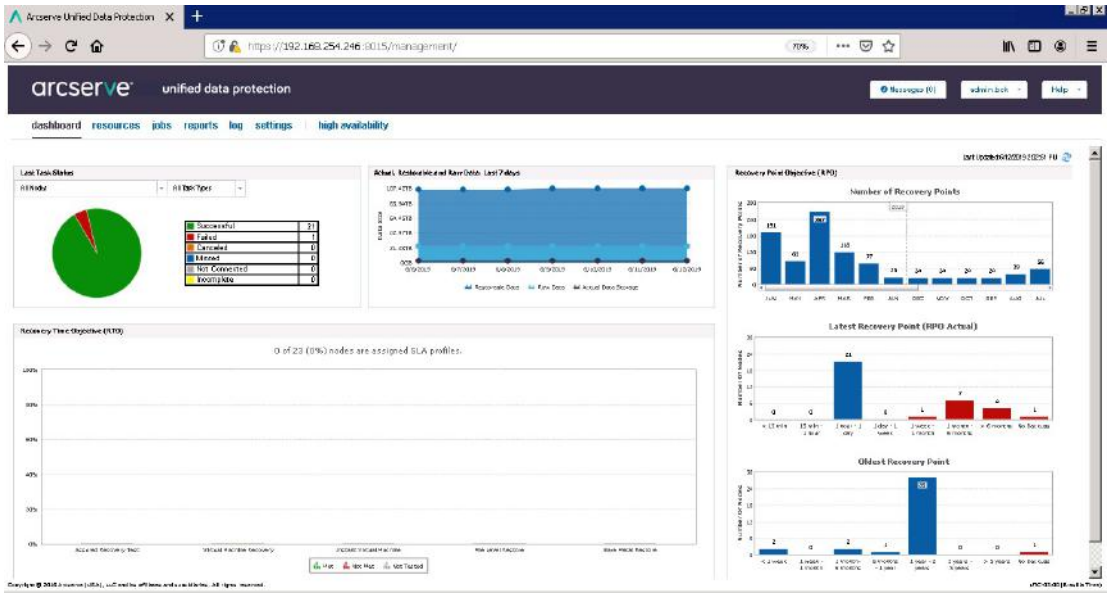
1 - A aplicação é totalmente licenciada e foi instalada por parceiros e foi homologada pelo setor de T.I. do PREVINI. Atualmente sendo executado em um servidor IBM System x3550 M3 (imagem abaixo) com 96 GB de memória RAM, 8 discos SAS em Raid 5 (redundância), 2 (duas) fontes de energia redundantes funcionando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

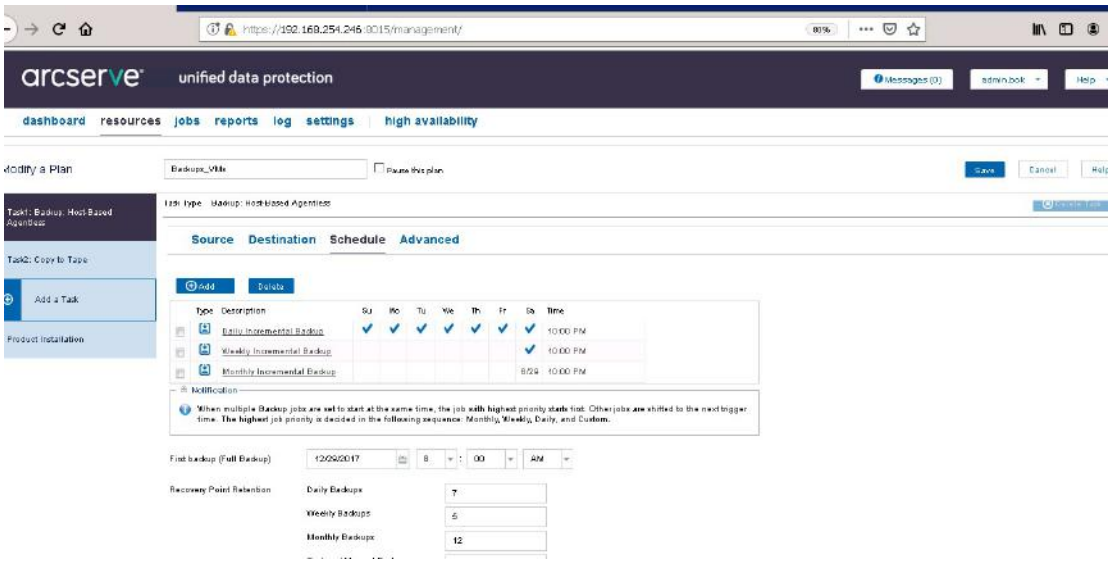


4 - Ao acessar a aplicação, podemos visualizar a tela que chamamos de “dashboard”, onde são mostrados diversos gráficos a respeito dos planos de backups. Nessa tela podemos verificar os status de backups (Successful, Failed, Canceled, Missed, Not Connected e Incomplete) o que facilita na tomada de decisões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

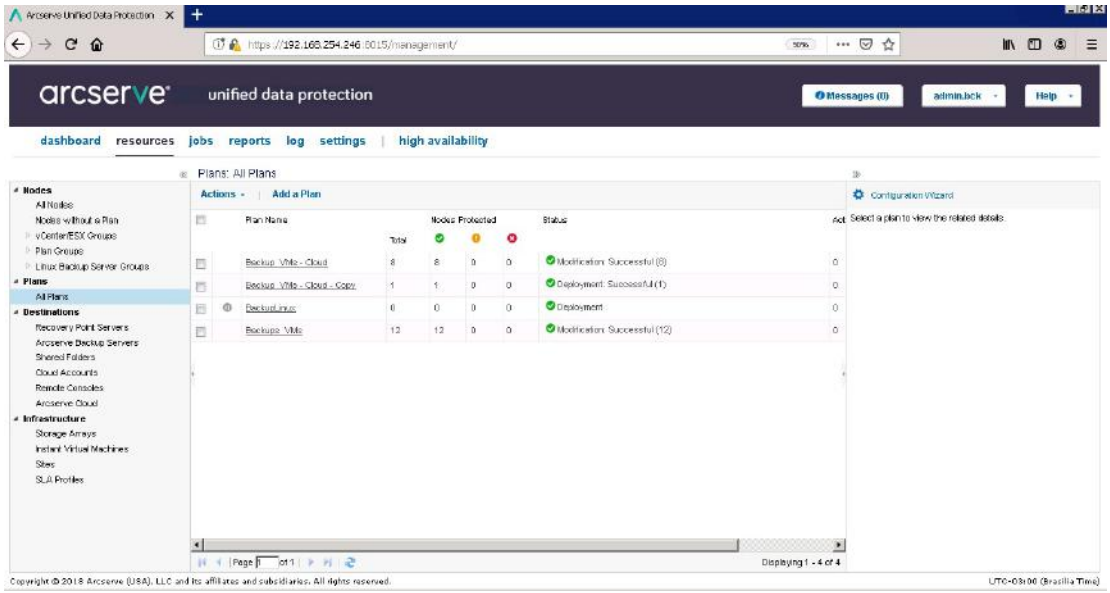


5 - Ao acessar a opção resources podemos visualizar diversas configurações e principalmente a área de planos de backups (all plans) criados e a possibilidade de criar mais planos, caso seja necessário.

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

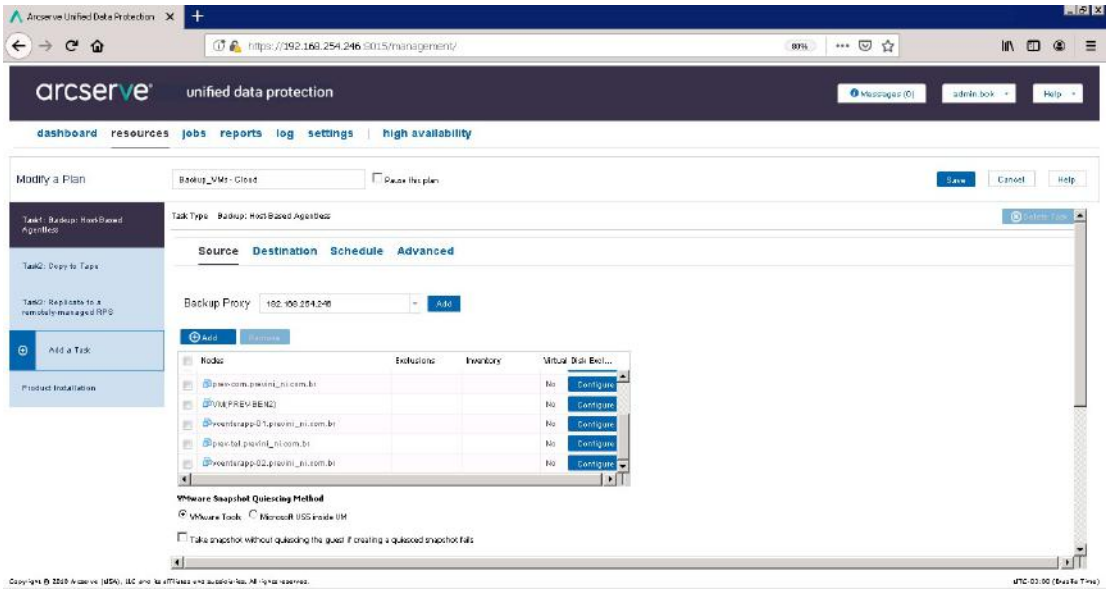


7 - Para a nossa estrutura atual utilizamos basicamente 2(dois) planos de backup (Backup VMs – Cloud e Backups VMs) conforme pode ser visto na tela abaixo:



- Backup VMs – Cloud: Esse plano foi criado para execução de backup de servidores mais importantes, são eles:

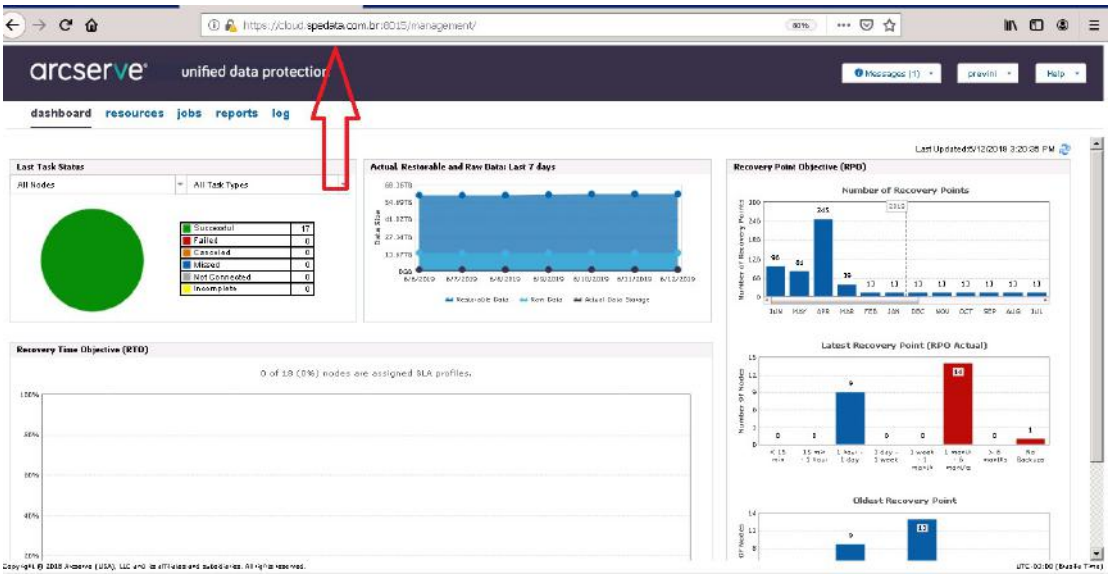
  - PREV-NET3 (Firewall)
  - PREV-SEC (Security Vmware)
  - PREV-CON (Connection Vmware)
  - PREV-COM (Compose Vmware)
  - PREV-BEN2 (Banco Postgres Softprevi)
  - PREV-BEM-APL (Servidor de Aplicação Softprevi)
  - PREV-SRV (Servidor de Arquivos ADDC)
  - PREV-TEL (Telefonia – Bilhetagem)
  - VcenterApp1 (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.

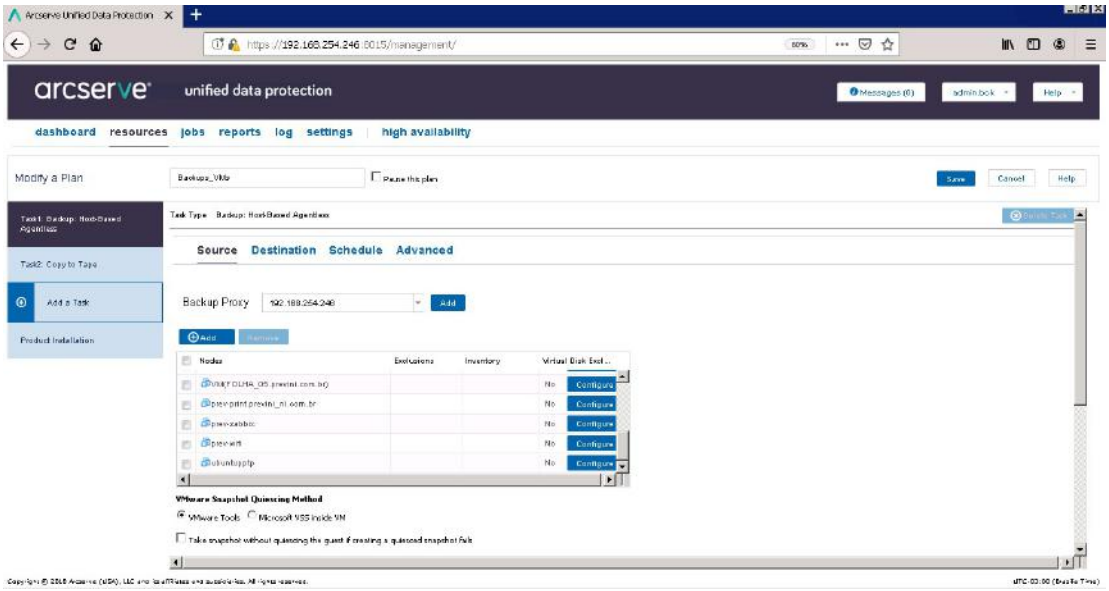
9 - Após a conclusão do backup nas fitas, automaticamente inicia-se um serviço de réplica em nuvem.

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.

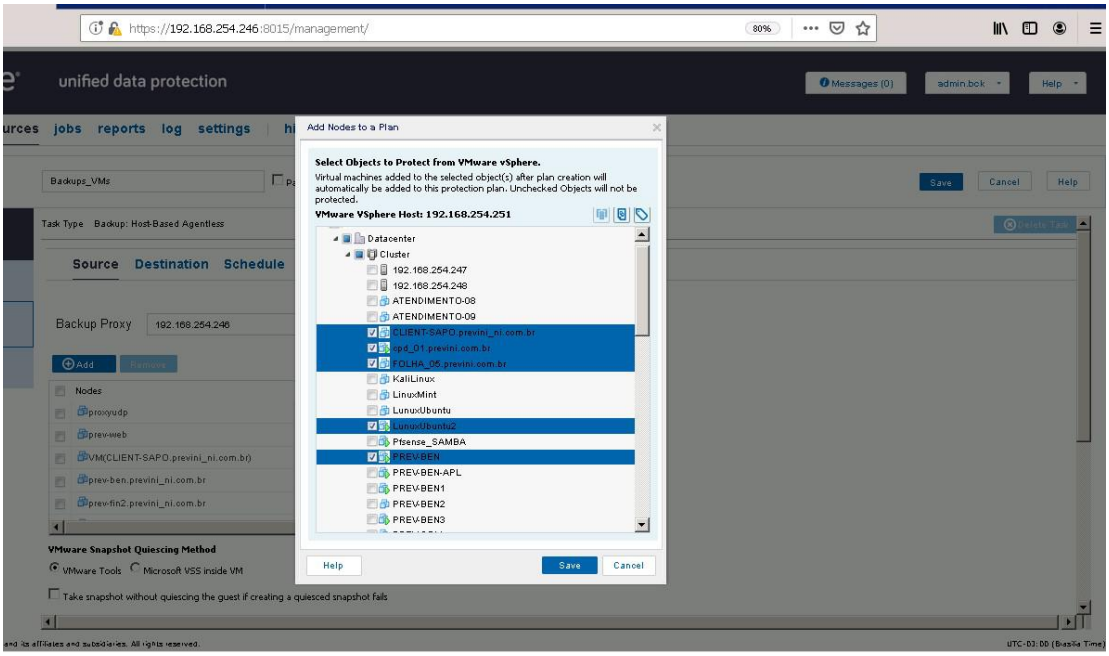


- Backup VMs: Esse plano foi criado para execução de backup de diversos servidores, são eles:

  - 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)

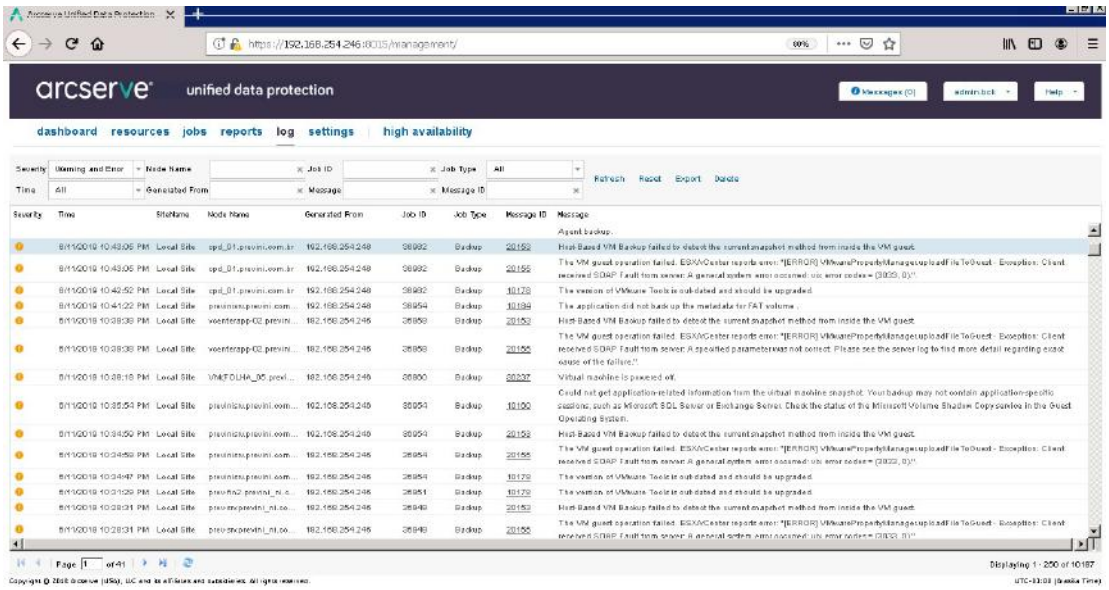

arcserve
unified data protection
dashboard
resources
jobs
reports
log
settings
high availability
Modify a Plan
Source
Destination
Schedule
Advanced
Backup Proxy
Add
Configure

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.

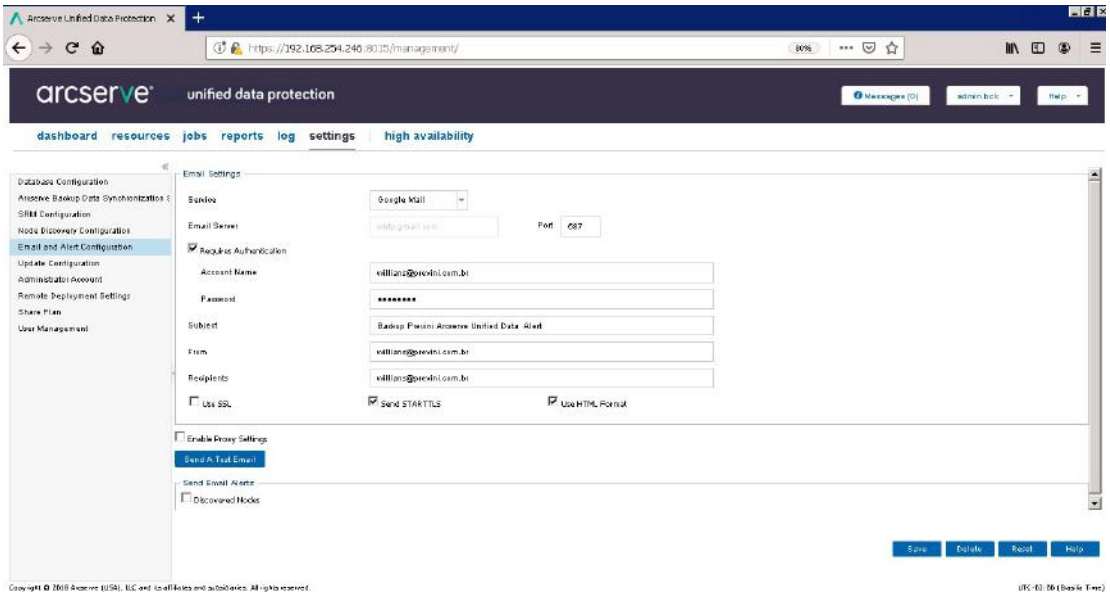


12 - São feitas réplicas de backups mensalmente também para um disco externo, onde esse disco fica armazenado fisicamente fora do prédio da instituição, assim garantindo também falhas contra desastres no prédio.

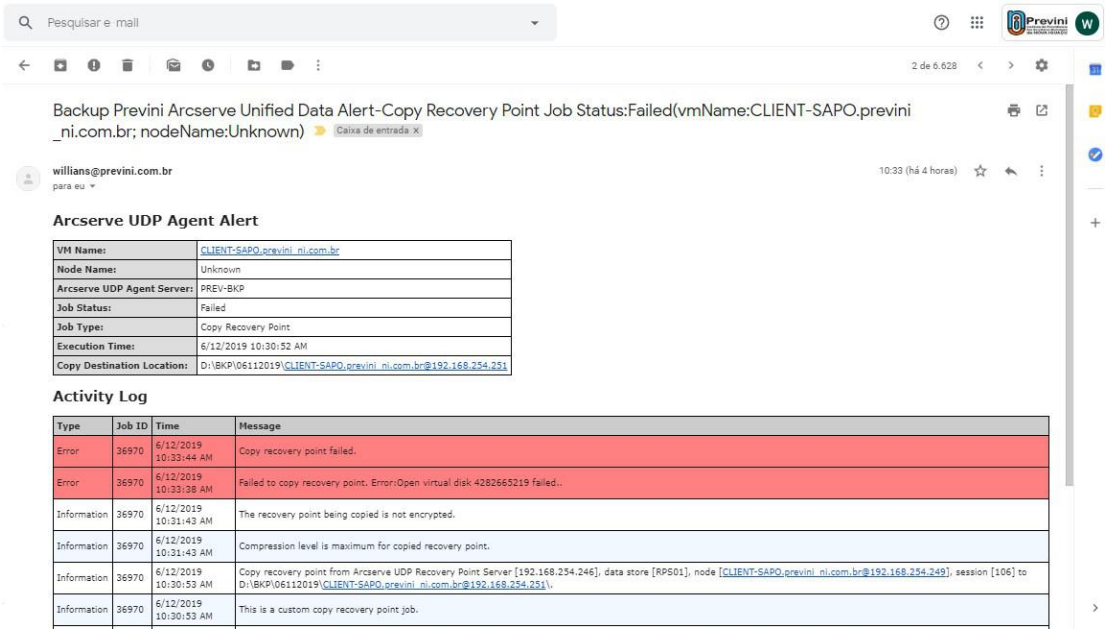
13 - Ao acessar a opção de Log, podemos verificar todos os procedimentos de backup e também podemos verificar alertas e erros, o que facilita na administração dos backups.



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:



Pesquisar e mail

2 de 6.628

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

willians@previni.com.br
para eu

10:33 (há 4 horas)

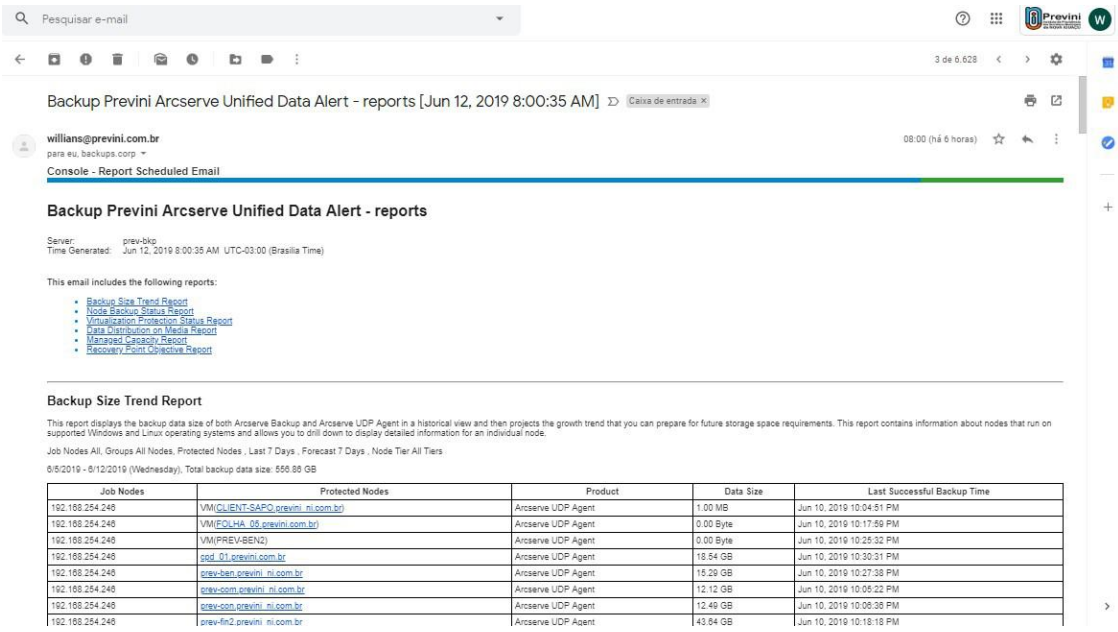
Arcserve UDP Agent Alert

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 10:33:38 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:



Pesquisar e-mail

Backup Previni Arcserve Unified Data Alert - reports [Jun 12, 2019 8:00:35 AM]

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

Console - Report Scheduled Email

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

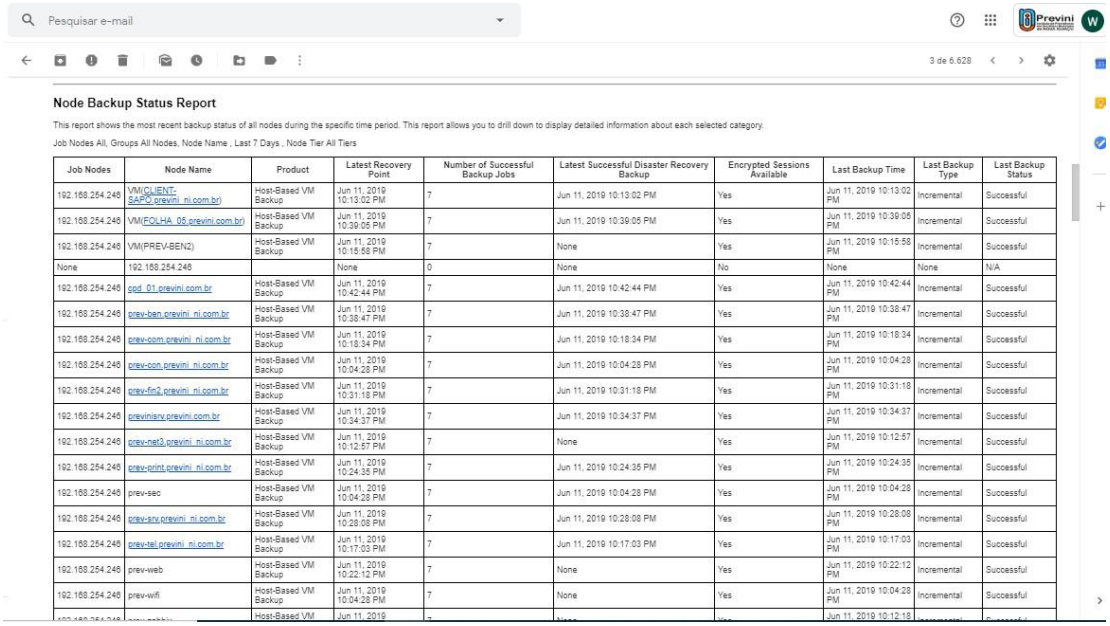
Backup Size Trend Report

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: 556.86 GB

Job Nodes	Protected Nodes	Product	Data Size	Last Successful Backup Time
192.168.254.246	VM(CLIENT-SAPO.previni_ni.com.br)	Arcserve UDP Agent	1.00 MB	Jun 10, 2019 10:04:51 PM
192.168.254.246	VM(FOLHA_05.previni.com.br)	Arcserve UDP Agent	0.00 Byte	Jun 10, 2019 10:17:59 PM
192.168.254.246	VM(PREV-BEN2)	Arcserve UDP Agent	0.00 Byte	Jun 10, 2019 10:25:32 PM
192.168.254.246	ged_01.previni.com.br	Arcserve UDP Agent	18.54 GB	Jun 10, 2019 10:30:31 PM
192.168.254.246	prev-ben.previni_ni.com.br	Arcserve UDP Agent	15.29 GB	Jun 10, 2019 10:27:38 PM
192.168.254.246	prev-com.previni_ni.com.br	Arcserve UDP Agent	12.12 GB	Jun 10, 2019 10:05:22 PM
192.168.254.246	prev-con.previni_ni.com.br	Arcserve UDP Agent	12.49 GB	Jun 10, 2019 10:06:36 PM
192.168.254.246	prev-fin2.previni_ni.com.br	Arcserve UDP Agent	43.64 GB	Jun 10, 2019 10:18:18 PM



Pesquisar e-mail

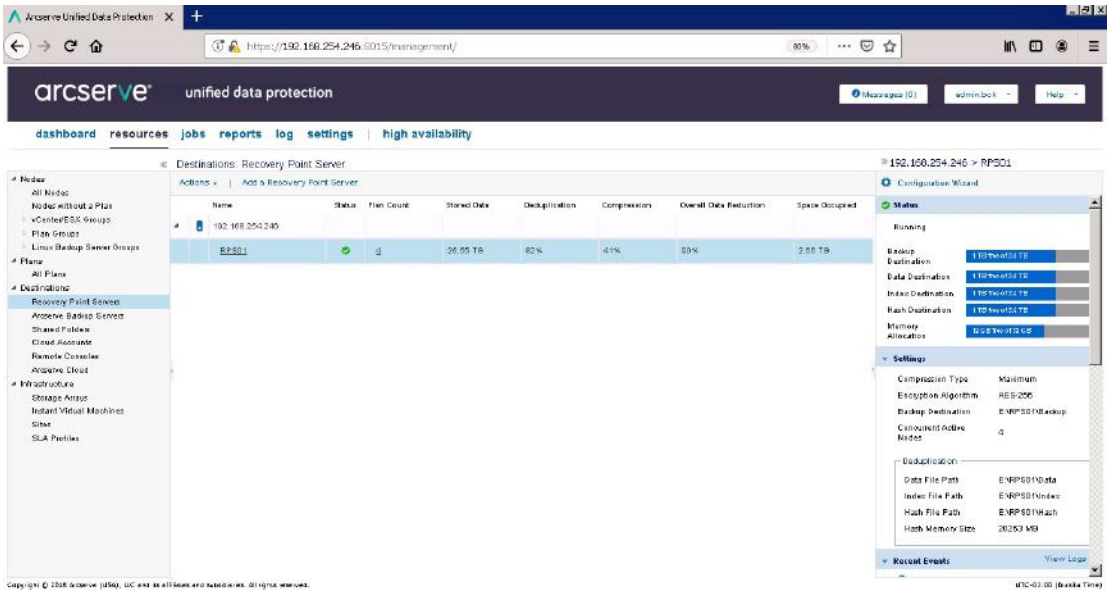
Node Backup Status Report

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.

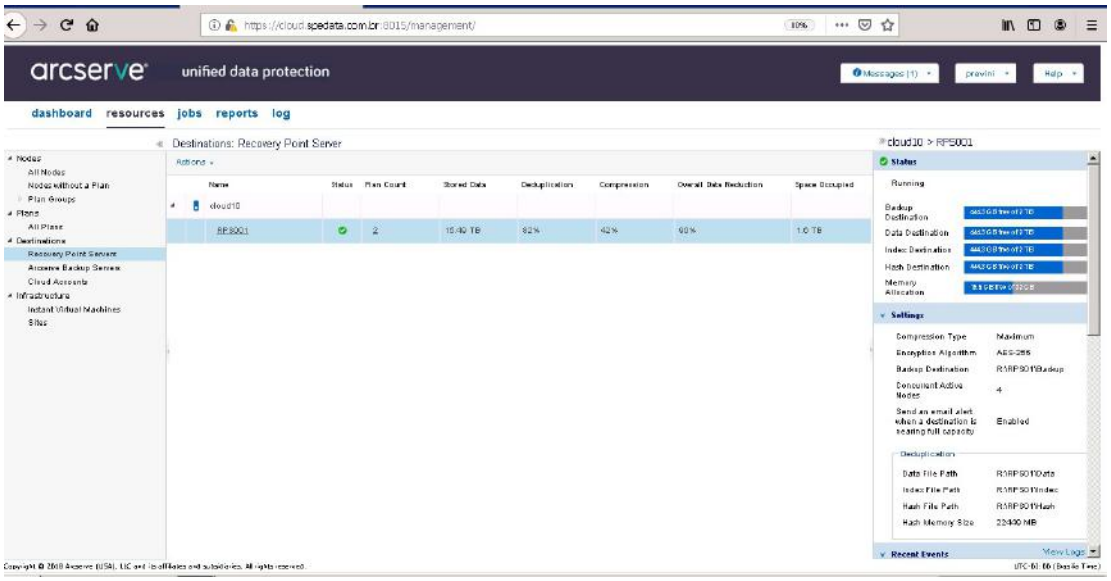
Job Nodes All, Groups All Nodes, Node Name , Last 7 Days , Node Tier All Tiers

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
192.168.254.246	VM(CLIENT-SAPO.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
192.168.254.246	VM(FOLHA_05.previni.com.br)	Host-Based VM Backup	Jun 11, 2019 10:39:05 PM	7	Jun 11, 2019 10:39:05 PM	Yes	Jun 11, 2019 10:39:05 PM	Incremental	Successful
192.168.254.246	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
192.168.254.246	ged_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
192.168.254.246	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
192.168.254.246	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
192.168.254.246	prev-con.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
192.168.254.246	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
192.168.254.246	previnisrv.previni.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
192.168.254.246	prev-net2.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
192.168.254.246	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
192.168.254.246	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
192.168.254.246	prev-srv.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
192.168.254.246	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
192.168.254.246	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
192.168.254.246	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

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:

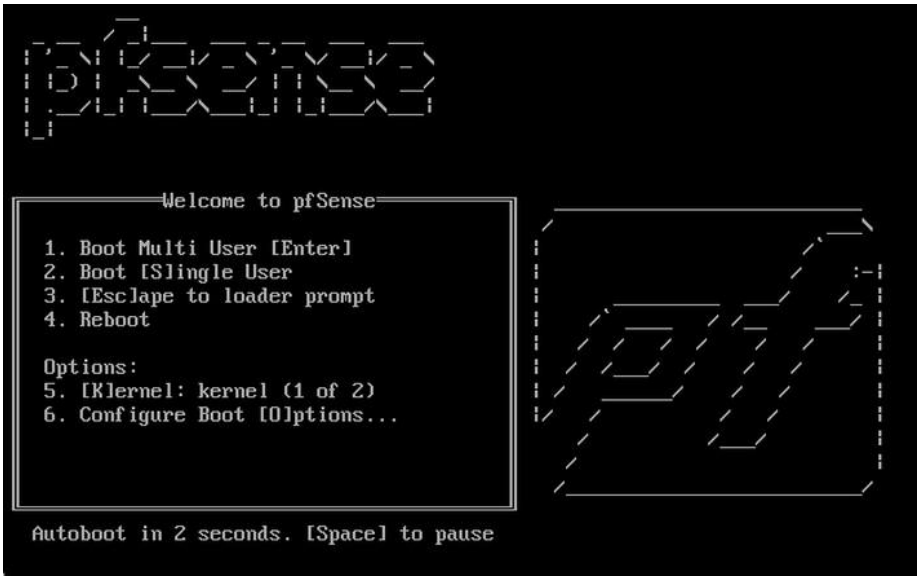


18 - Atualmente podemos verificar que o total de espaço utilizado em nosso RPS01 REMOTO (servidor de backup em nuvem) é de 1.6 TB conforme demonstrado em imagem abaixo:

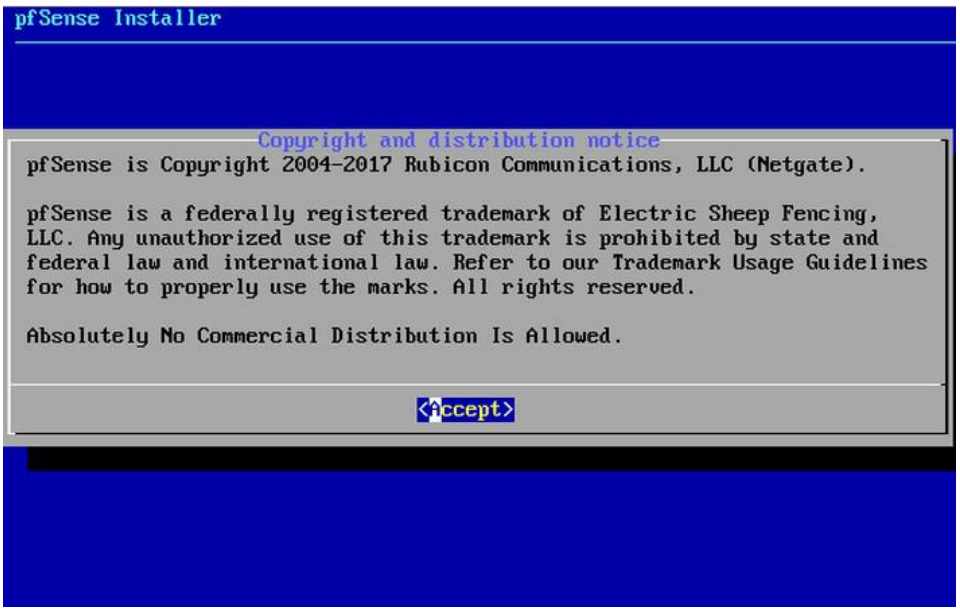


7 - Anexo II – Instalação do Pfsense

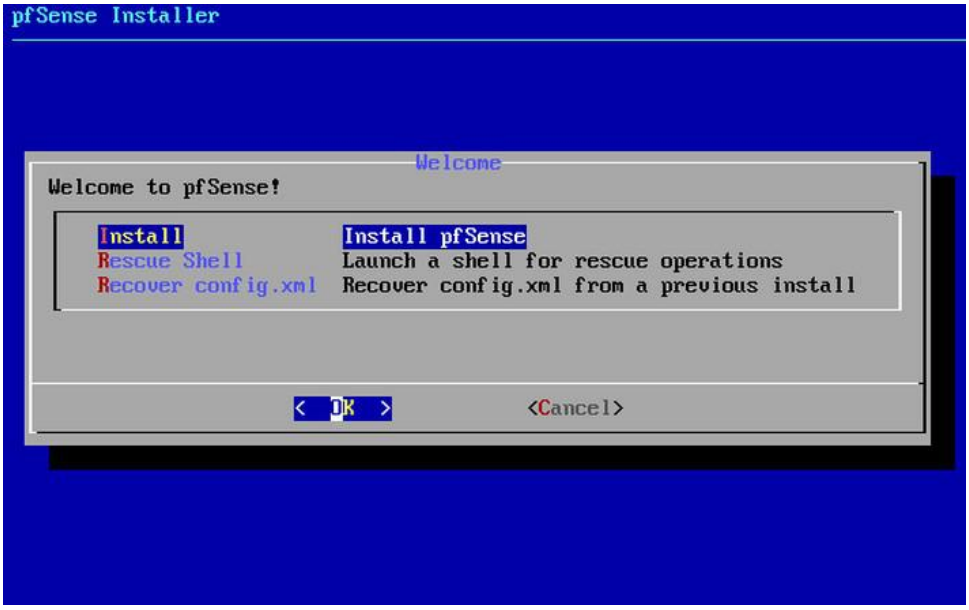
Após o boot, essa é a primeira tela, exibida por 5 segundos, clicar na tecla “Enter” ou deixa iniciar automaticamente.



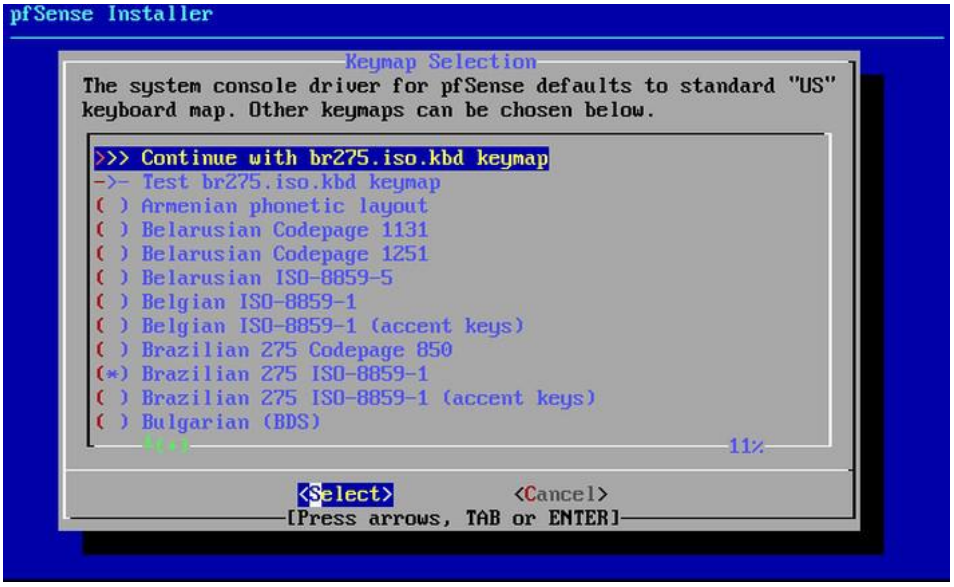
Termos de licenciamento de uso... Accept



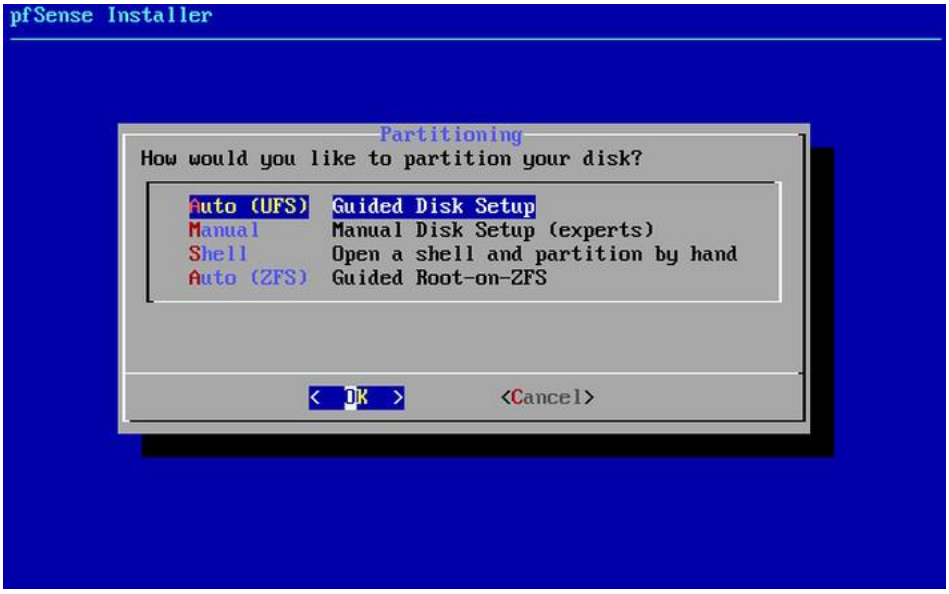
Install...



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

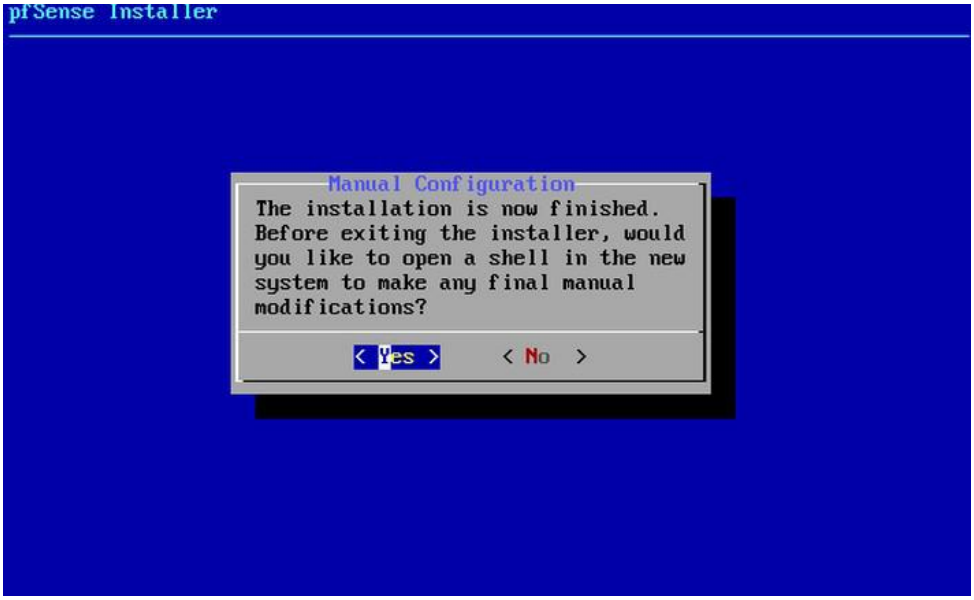


Utilizamos a opção AUTO (ZFS).

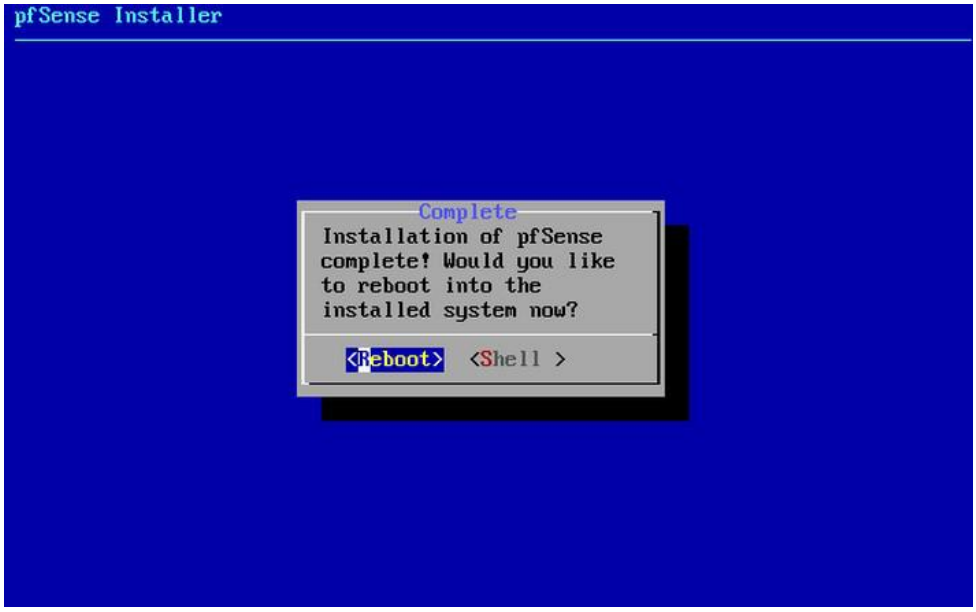


E aguarde a cópia dos arquivos e a instalação.

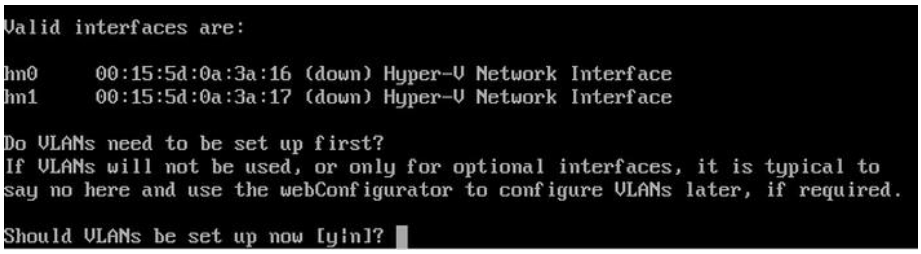
Caso seja necessária alguma configuração adicional via shell (prompt) selecione Y, no PREVINI inicialmente escolhemos a opção N.



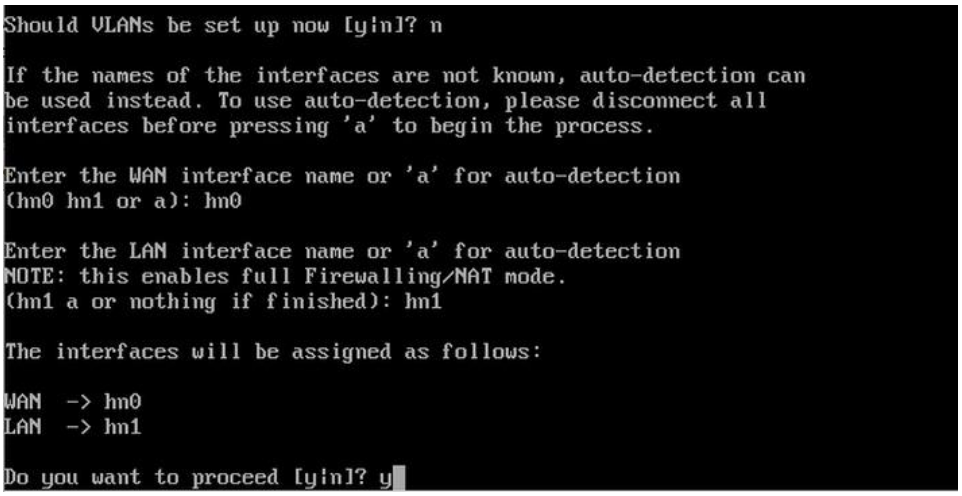
Será necessário reiniciar o sistema.



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.



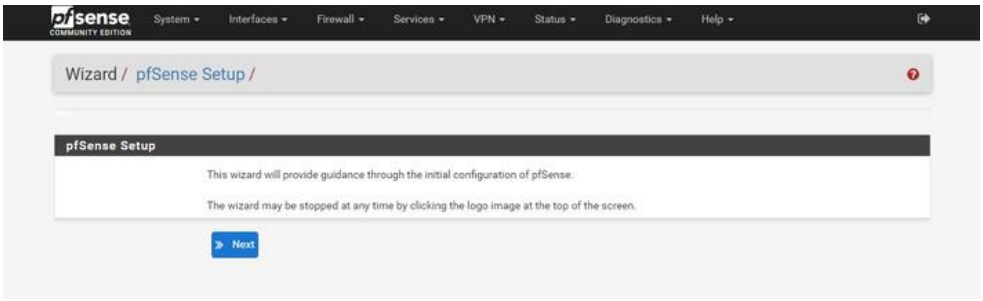
É possível ver que ele dê um nome qualquer para as duas interfaces de rede e mostrou o status de ambas (down, pq estão desconectadas). Após decidir sobre a VLan, você deve dizer quem vai ser a sua Wan e Lan.



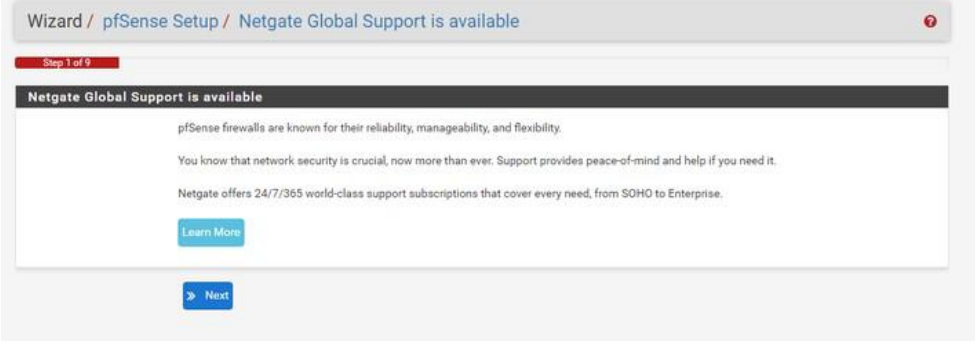
Confirmado, as interfaces vão tentar pegar IP ou será necessário configurar IP manualmente e agora você tem a tela de boas-vindas do pfSense.

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.

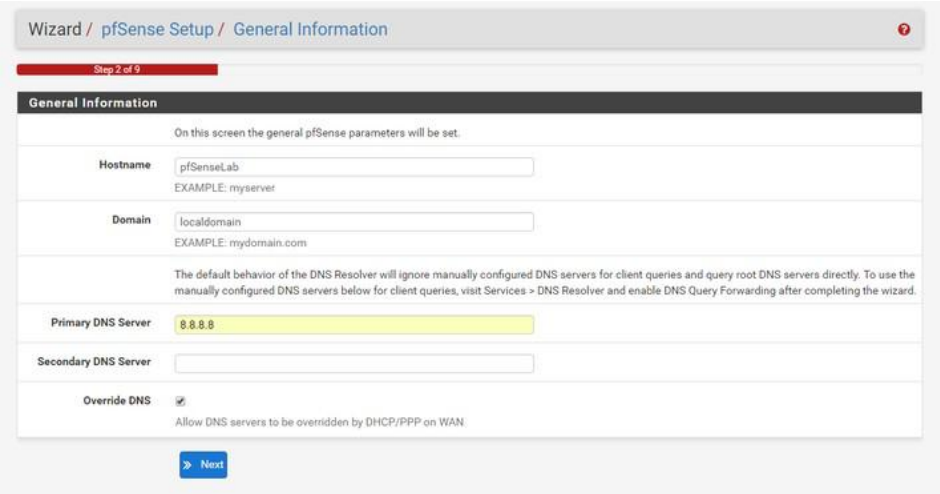
Ao acessar pela primeira vez, temos um assistente para as primeiras configurações.



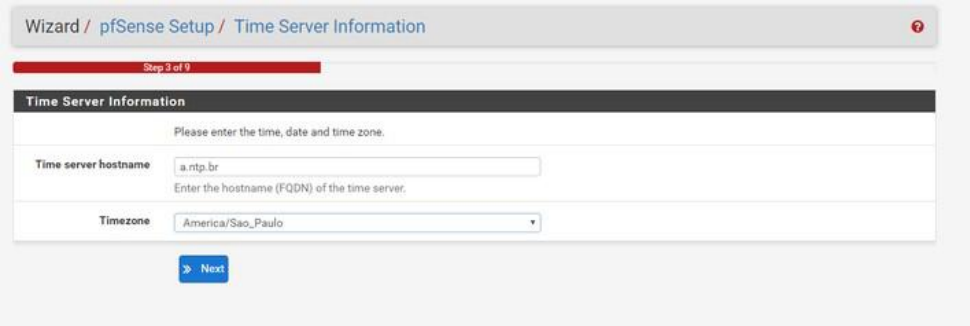
O passo 1 é sobre o suporte que é oferecido, você pode ler mais sobre isso ou clicar em Next.



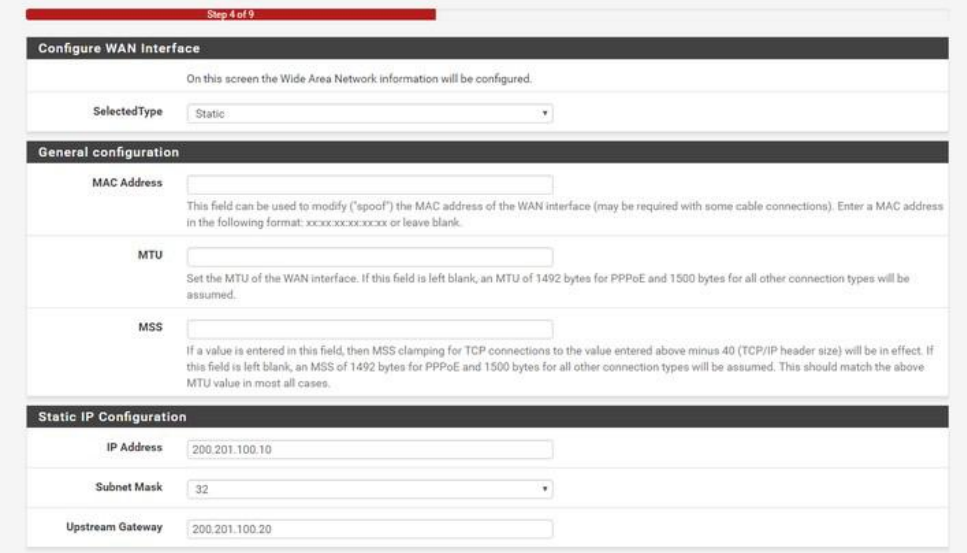
Passo 2: você pode configurar um nome, um domínio e DNS .



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



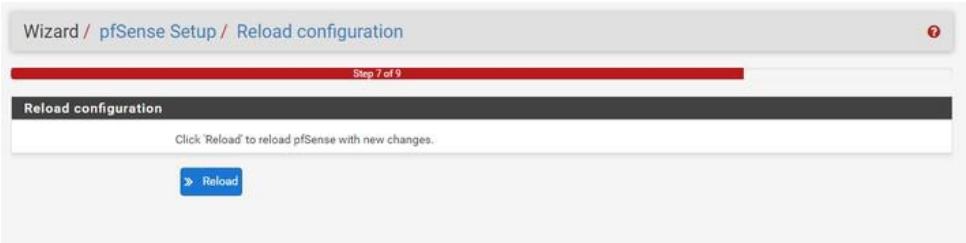
Passo 4: configurar a Wan, no PREVINI são configuradas 2 Wan (Oi Telemar e Netway)



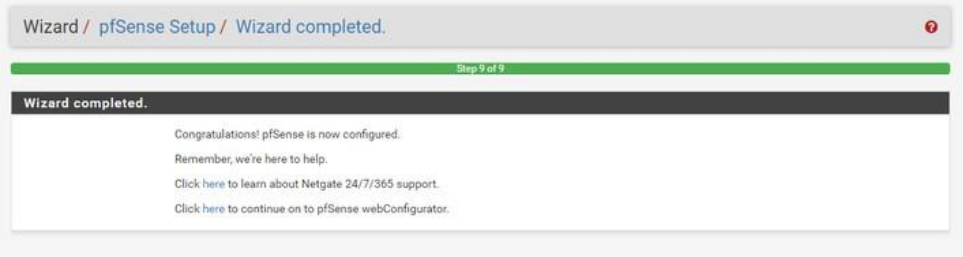
Passo 5: Configurar a Lan. A configuração de IP da LAN

Passo 6: redefinir a senha do administrador.

Clique em Reload.



Clique para continuar no pfSense WebConfigurator.



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

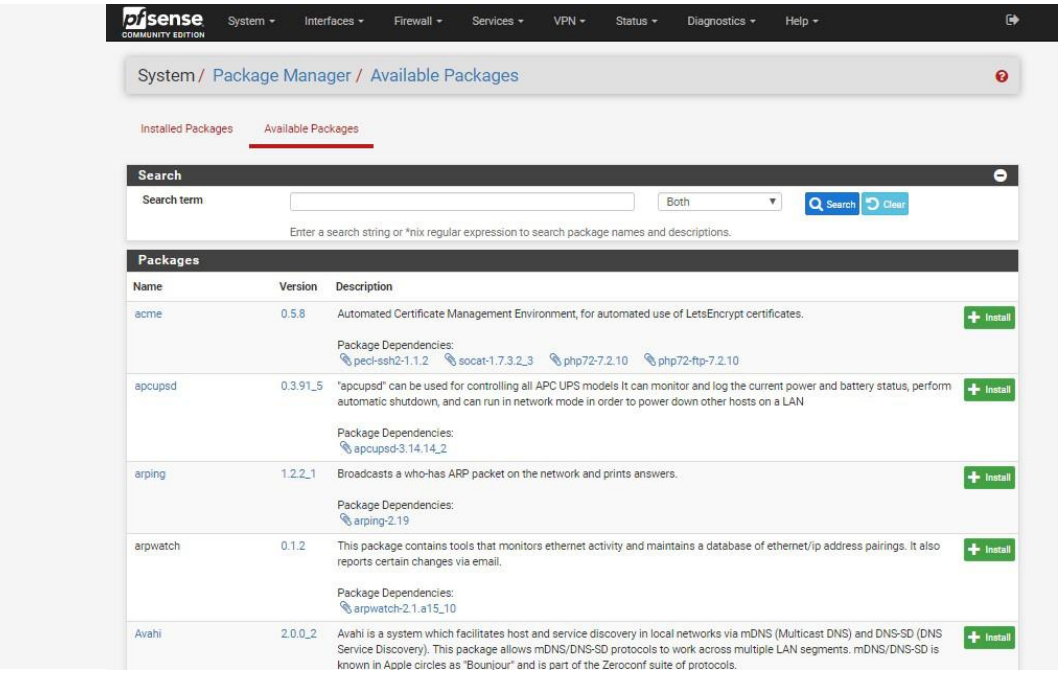
Pacotes Instalados

Os pacotes instalados são:

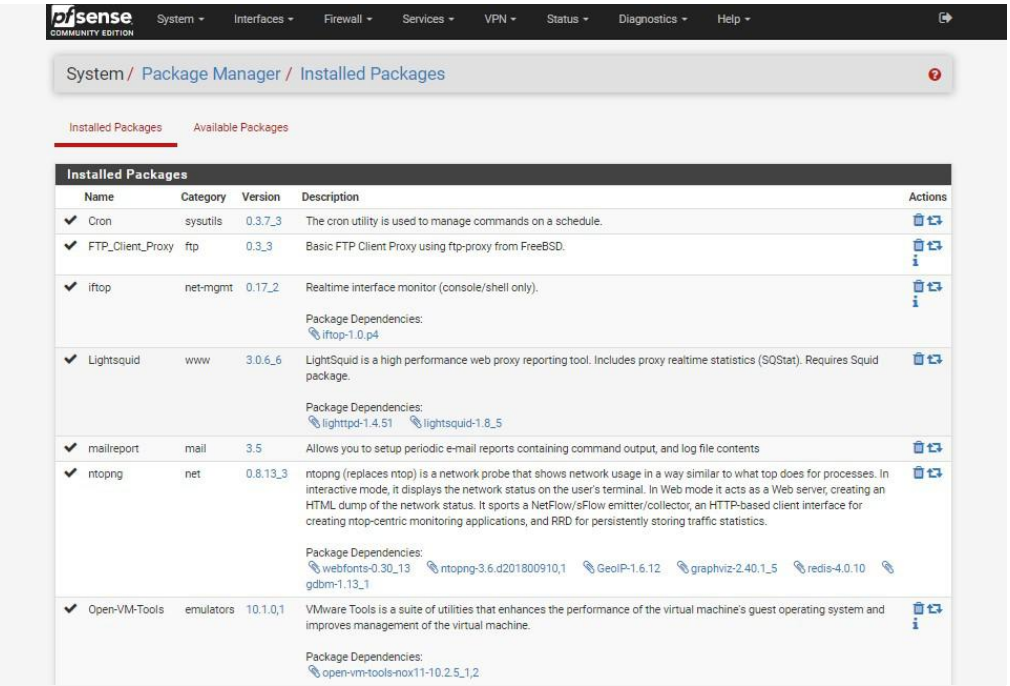
- Cron
  Utilitário usado para gerenciar comandos agendados
- FTP_Client_Proxy
  Cliente de Acesso a FTP
- Iftop
  Console monitor
- Lightsquid
  Gerador de Relatórios de acessos do squid
- Mailreport
  Permite o envio de alertas por e-mail
- Ntopng
  Ferramenta de relatórios de gerencias
- Open-VM-Tools
  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.

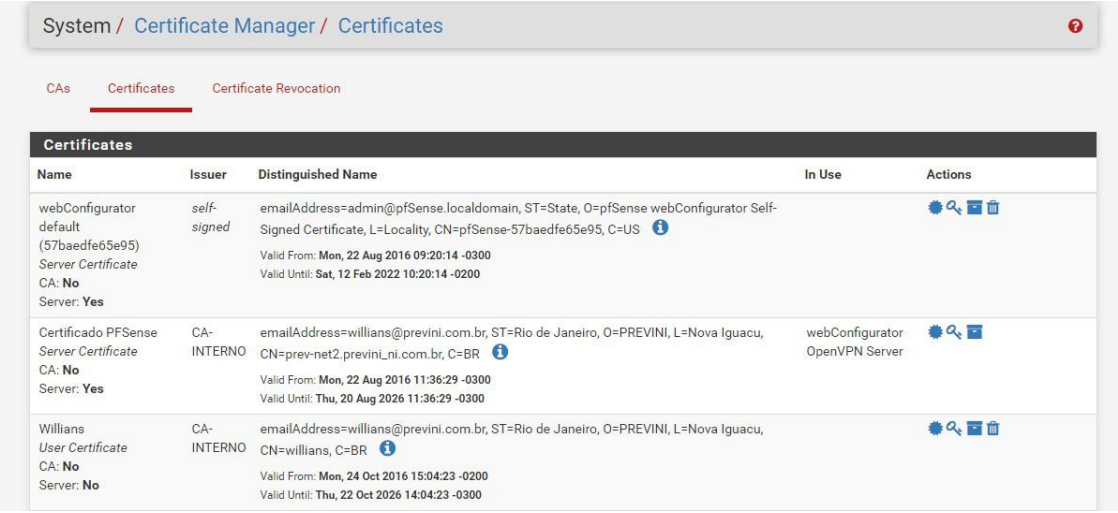


Para remover um pacote já instalado, basta clicar no ícone de Lixeira.



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.



Routing

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

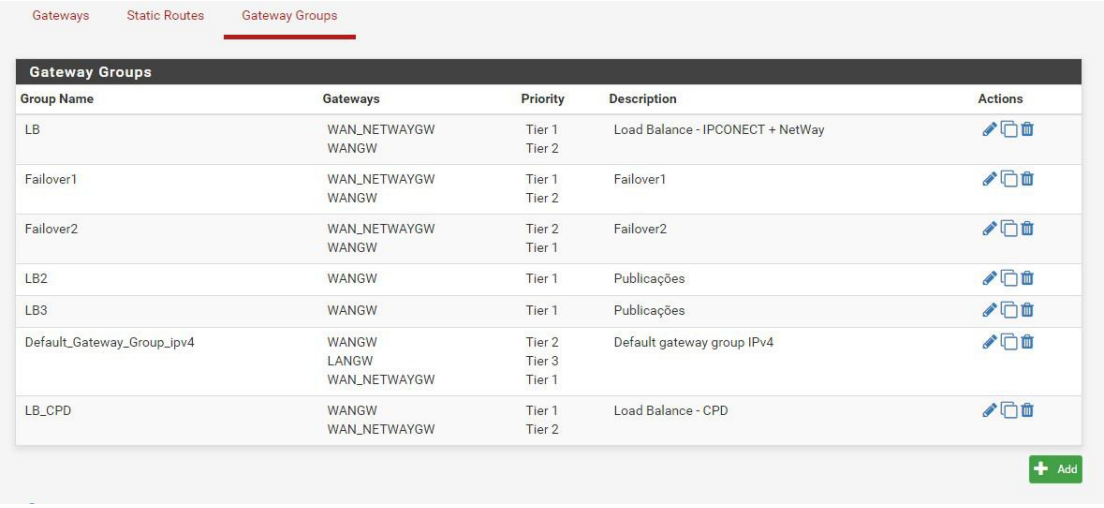
Gateway:
WANGW → Rota de Internet (Link de internet da operadora Oi – Telemar)
WAN_NETWAY → Rota de Internet (Link de internet da operadora – Netway)
LAN_GW → Responsável pela rota da rede interna.

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:
Incluímos 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.



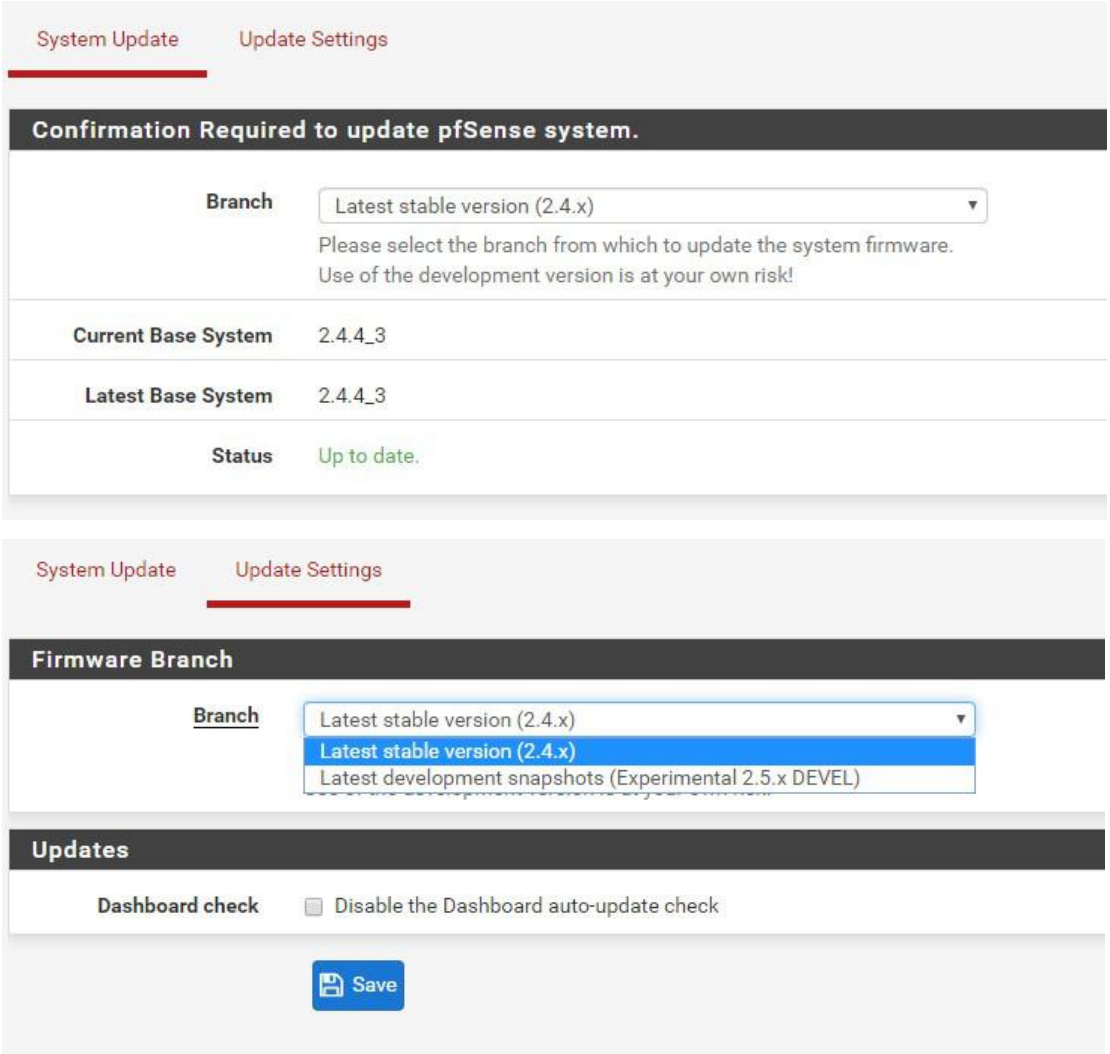
Opção onde determinar o default gateway

Update

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

A opção utilizada pelo PREVINI é a *Latest stable vercion*. 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.

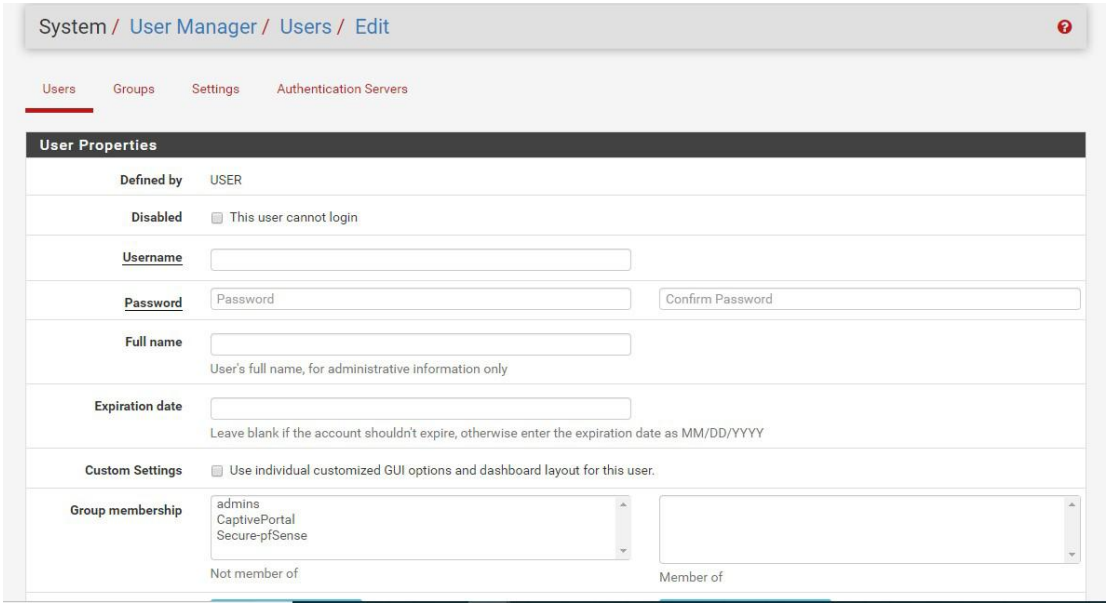
É sempre importante antes de atualizar, verificar quais os itens foram atualizados e quais foram as melhorias na versão. Em muitos casos algumas atualizações precipitadas acabam trazendo problemas no funcionamento de diversos serviços.



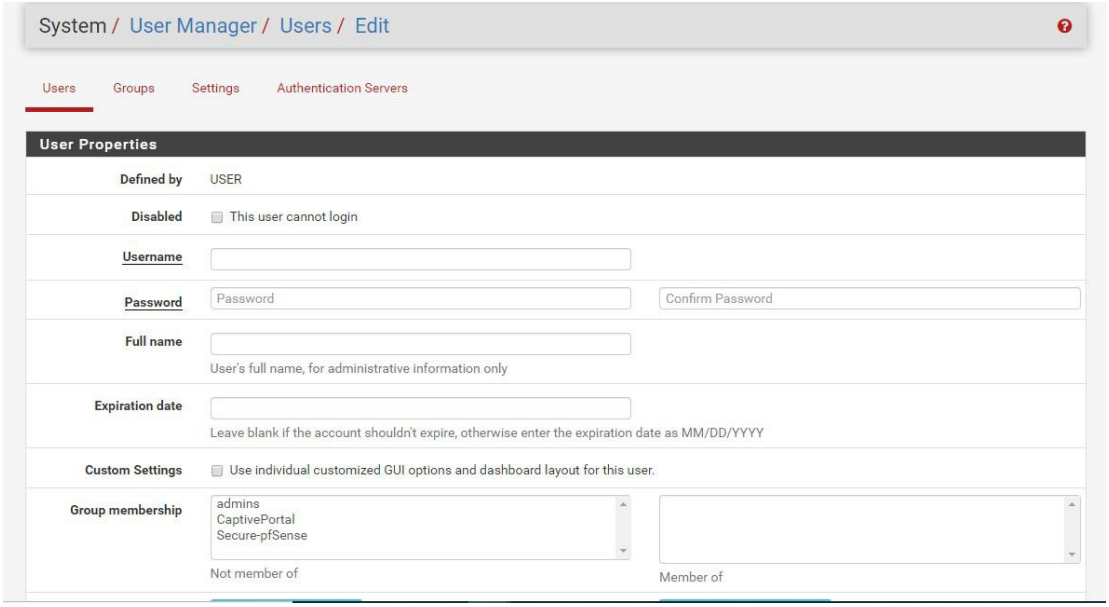
User Manager

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*.



Tela abaixo para criação de grupos



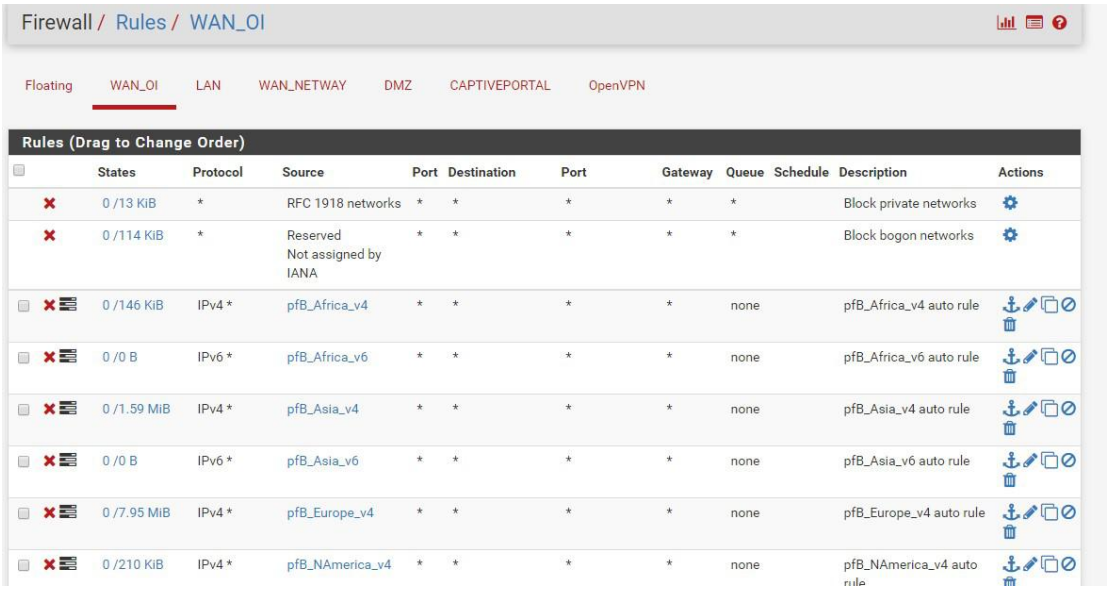
Interfaces

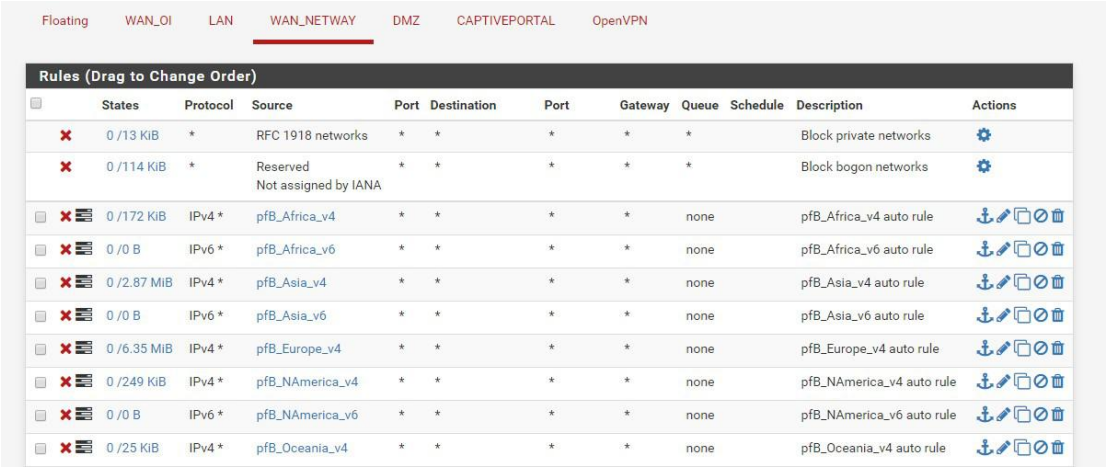
Atualmente utilizamos 5 interfaces de rede.

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.

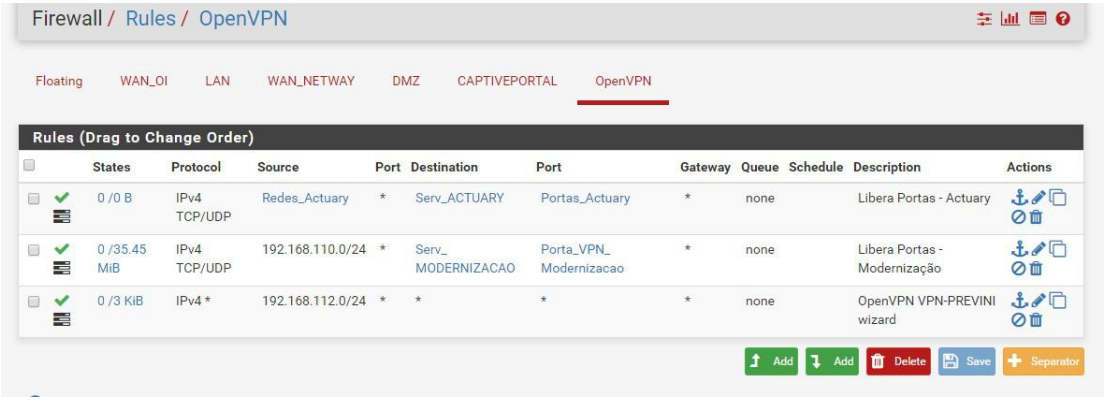




Na interface **OpenVPN** configuramos o que cada usuário poderá acessar em nossa rede local. Por padrão os usuários que precisam de acesso VPN são fornecedores de software e o pessoal de TI do próprio PREVINI.

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.



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

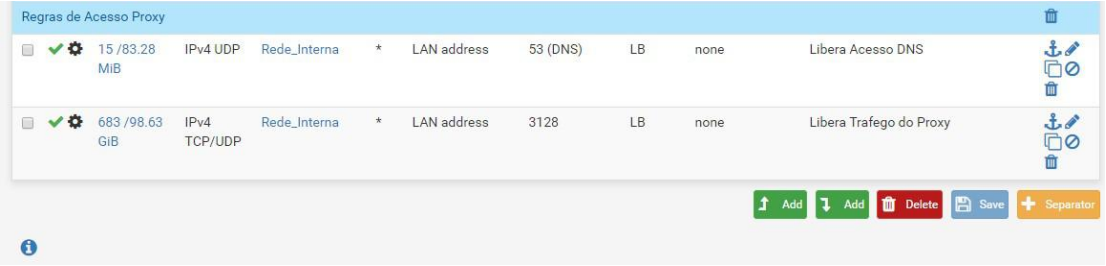
A vantagem é que se um desses servidores sofrer algum tipo de ataque na internet, eles estão protegidos dos demais servidores, evitando assim que um vírus possa alastrar.
Permitimos somente o estritamente necessário para que o acesso aos serviços possa ser efetivado.

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

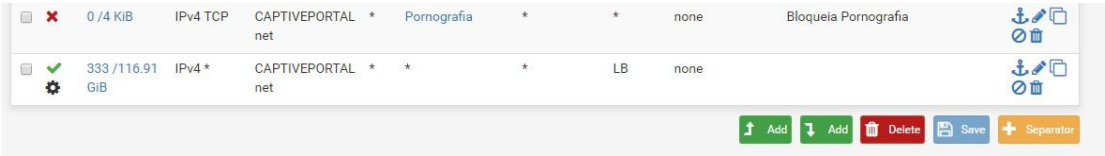
Por padrão utilizamos diversos serviços/pacotes para restringir o acesso à internet, o que visa à segurança da rede interna para que não seja permitido que usuários acessem sites inapropriados.

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 **shallalist.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)



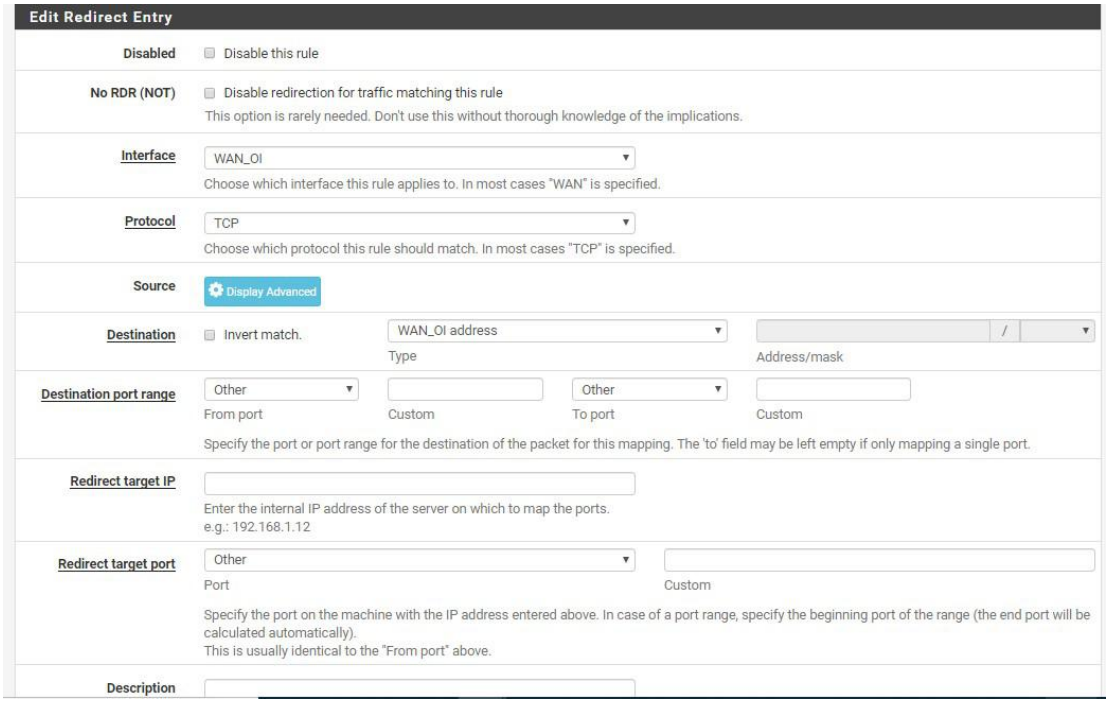
Na interface **CAPTIVEPORTAL** configuramos as regras de acesso ao WiFi do PREVINI. Nessa interface não utilizamos o proxy como saída para internet, utilizamos apenas o firewall permitindo alguns acessos internamente e efetuando bloqueios a sites inapropriados apelidado pela categoria *Pornografia*,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



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



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.

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

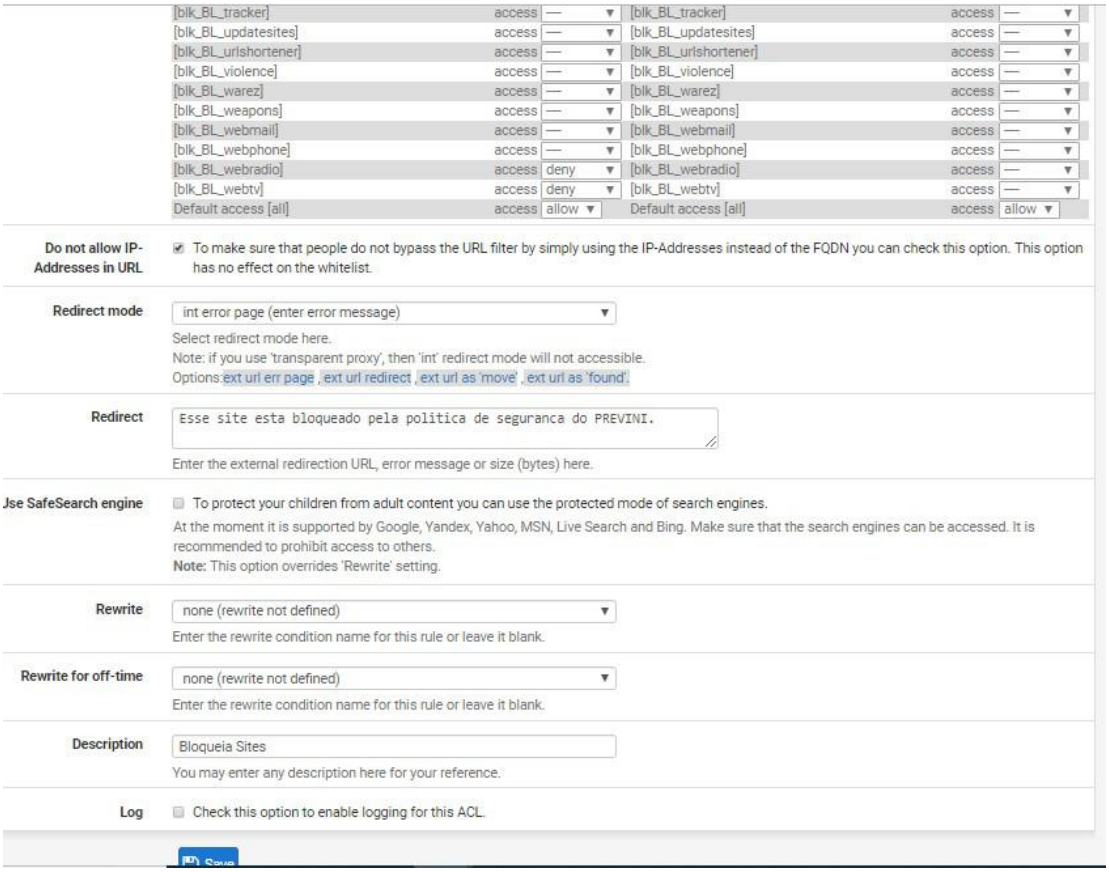
[blk_BL_webradio]
[blk_BL_webtv]
[blk_BL_spyware]
[blk_BL_socialnet]
[blk_BL_sex_lingerie]
[blk_BL_porn]
[blk_BL_radiotv]
[blk_BL_movies]
[blk_BL_hobby_games-misc]
[blk_BL_hobby_games-online]
[blk_BL_hacking]
[blk_BL_aggressive]
Lista_Whatsapp [Whatsapp]
Diversos sites bloqueados [Bloqueios-Geral]
Relação de Proxy's [Proxys]
Videos [Sites_Videos]
Relação de Radios Online [Radios]

Target Rules List

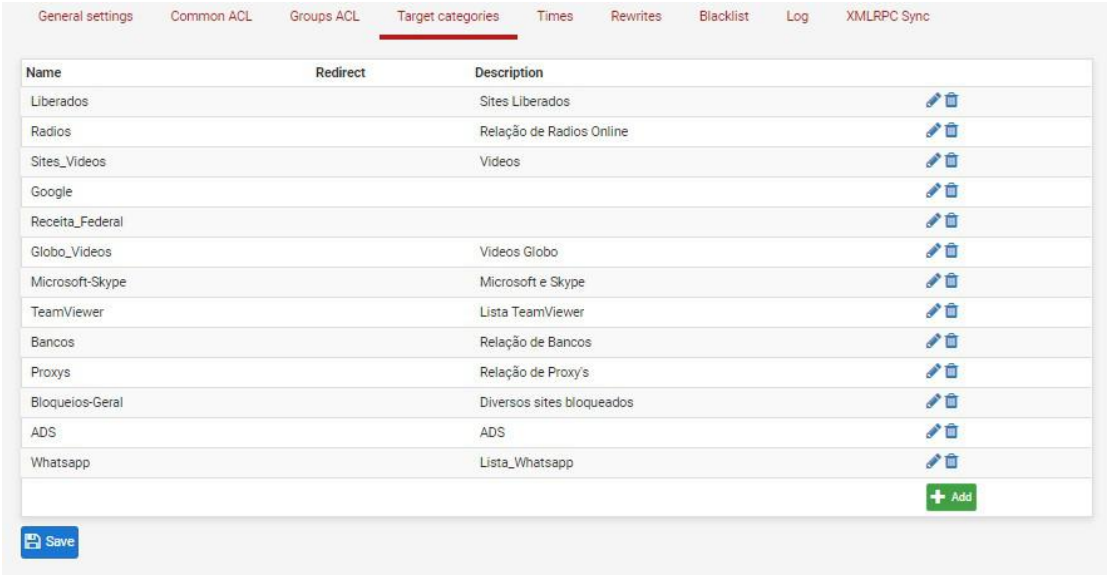
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

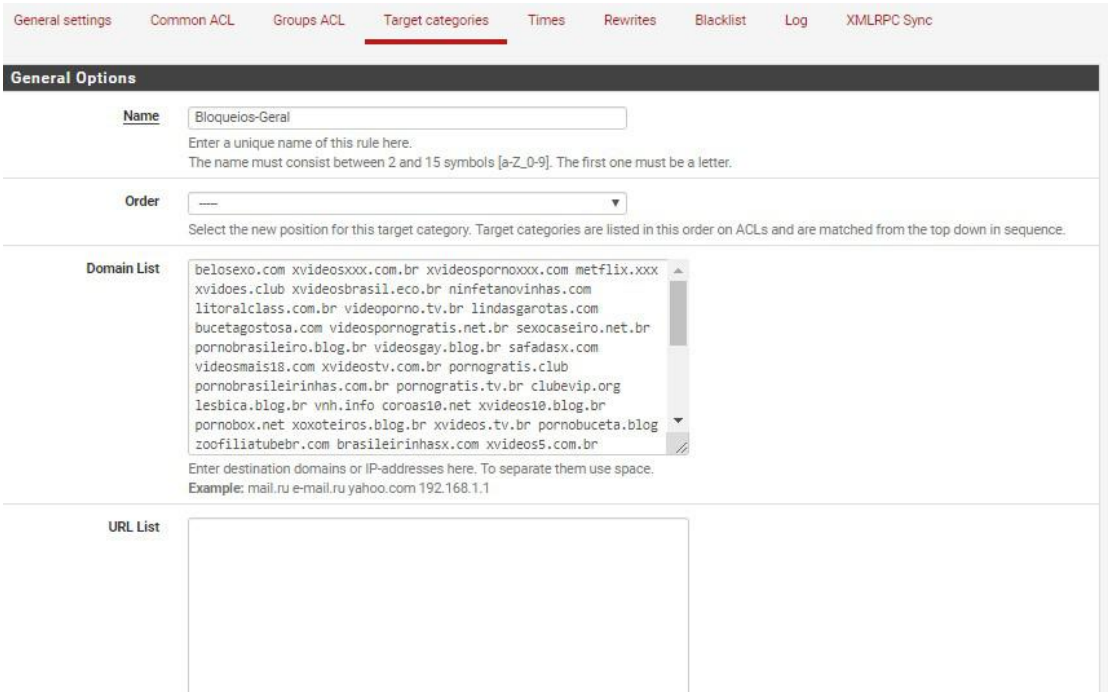
Target Categories		Target Categories for off-time (If 'Time' not defined, this is column will be ignored.)	
Sites Liberados [Liberados]	access —	Sites Liberados [Liberados]	access —
Relação de Radios Online [Radios]	access deny	Relação de Radios Online [Radios]	access —
Videos [Sites_Videos]	access deny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

[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_porn]	access	deny	[blk_BL_porn]	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	—

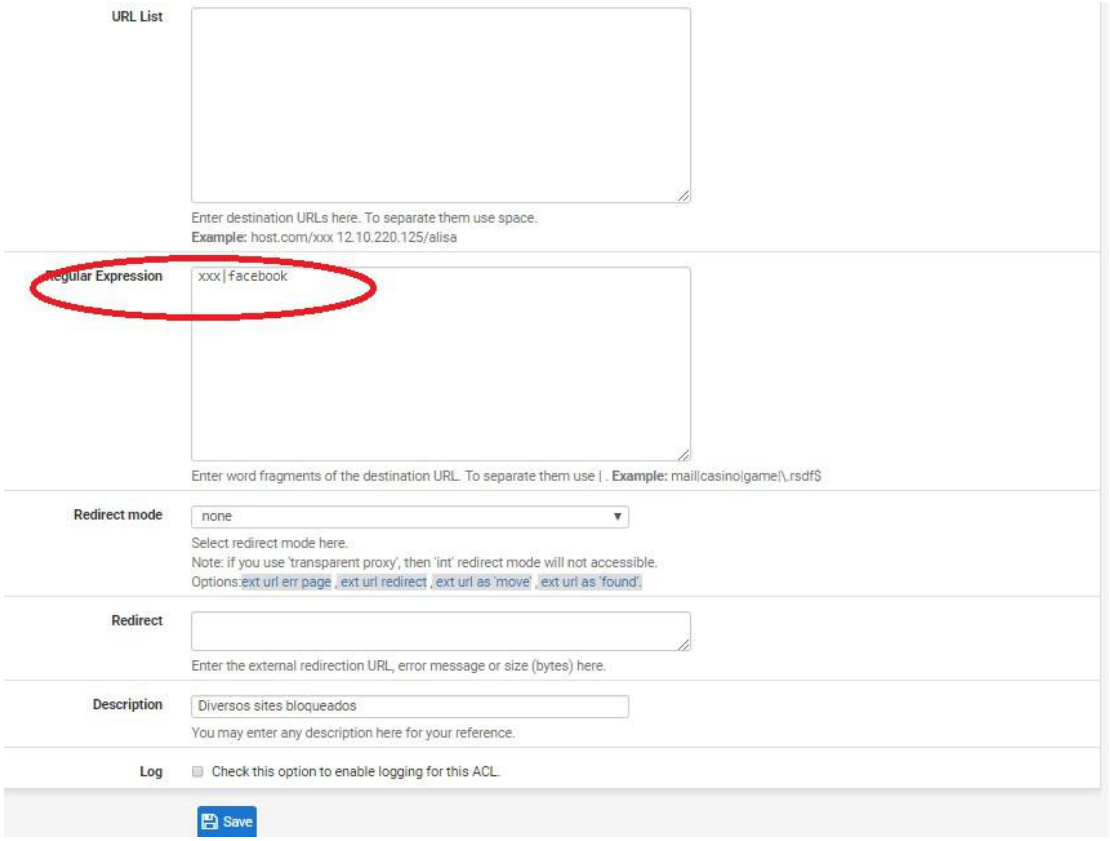

[blk_BL_tracker] access — [blk_BL_tracker] access —
[blk_BL_updatesites] access — [blk_BL_updatesites] access —
[blk_BL_urlshortener] access — [blk_BL_urlshortener] access —
[blk_BL_violence] access — [blk_BL_violence] access —
[blk_BL_warez] access — [blk_BL_warez] access —
[blk_BL_weapons] access — [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
int error page (enter error message)
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
Esse site esta bloqueado pela politica de seguranca do PREVINI.
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
none (rewrite not defined)
Enter the rewrite condition name for this rule or leave it blank.
Rewrite for off-time
none (rewrite not defined)
Enter the rewrite condition name for this rule or leave it blank.
Description
Bloqueia Sites
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:



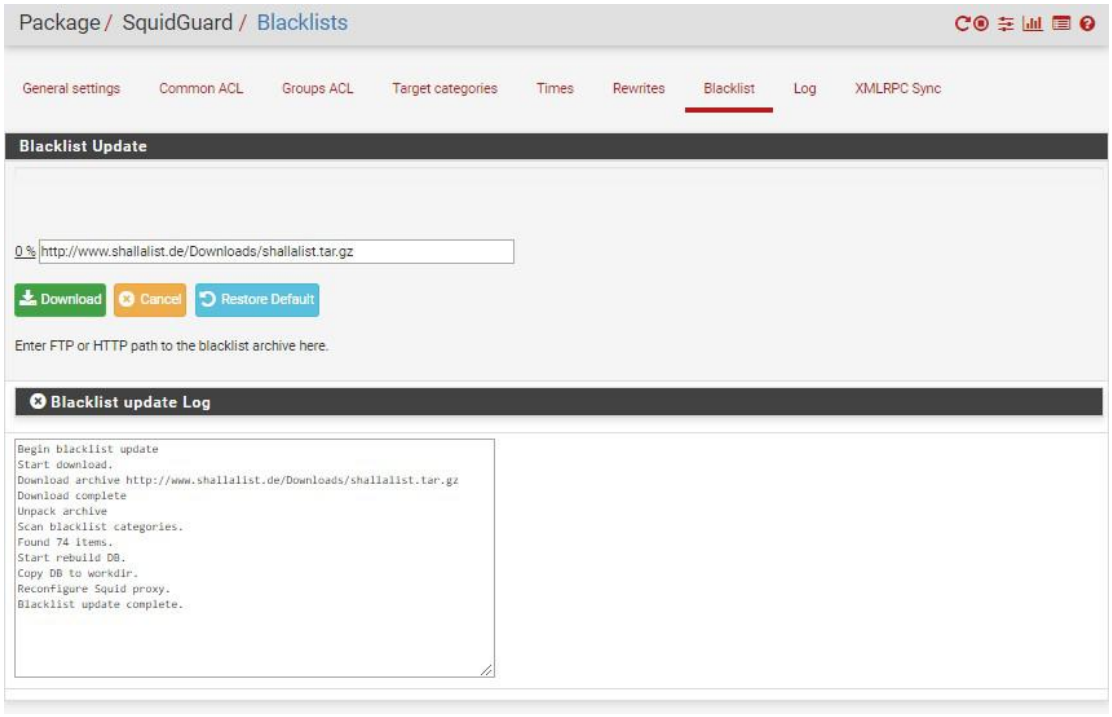


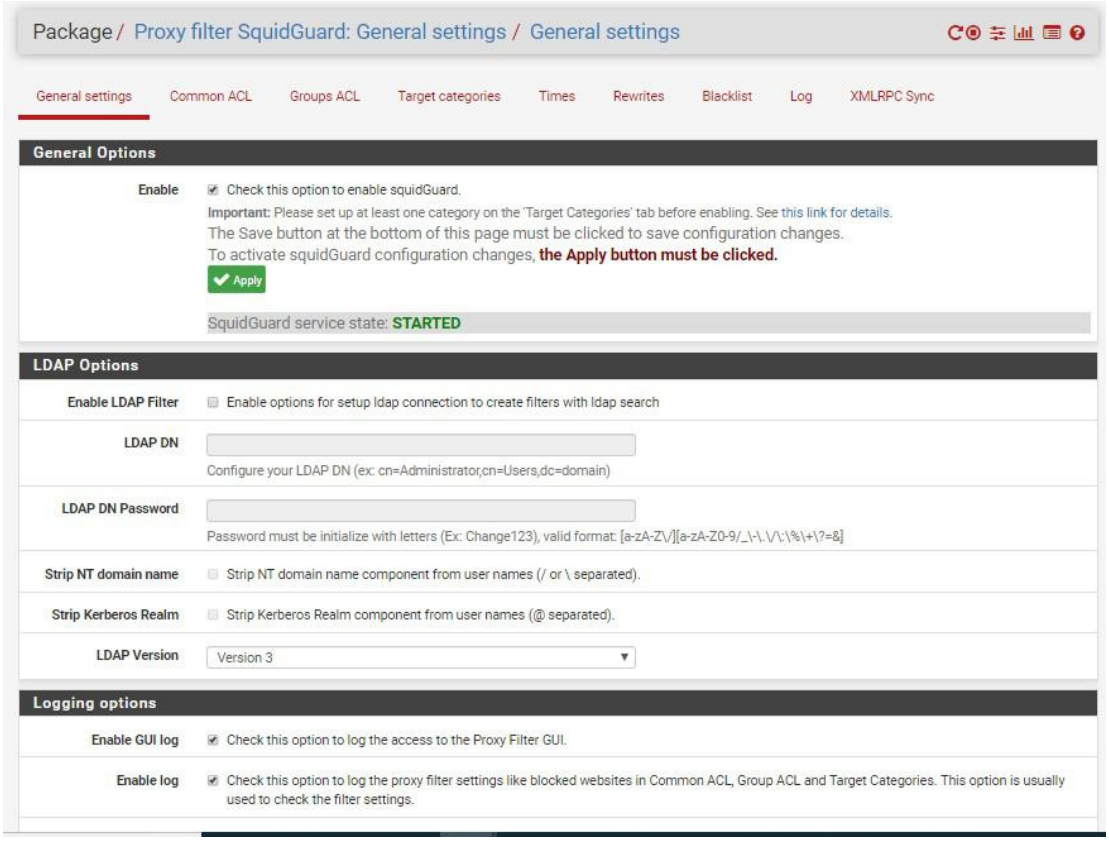
Bloqueios são feitos por expressões regulares também:

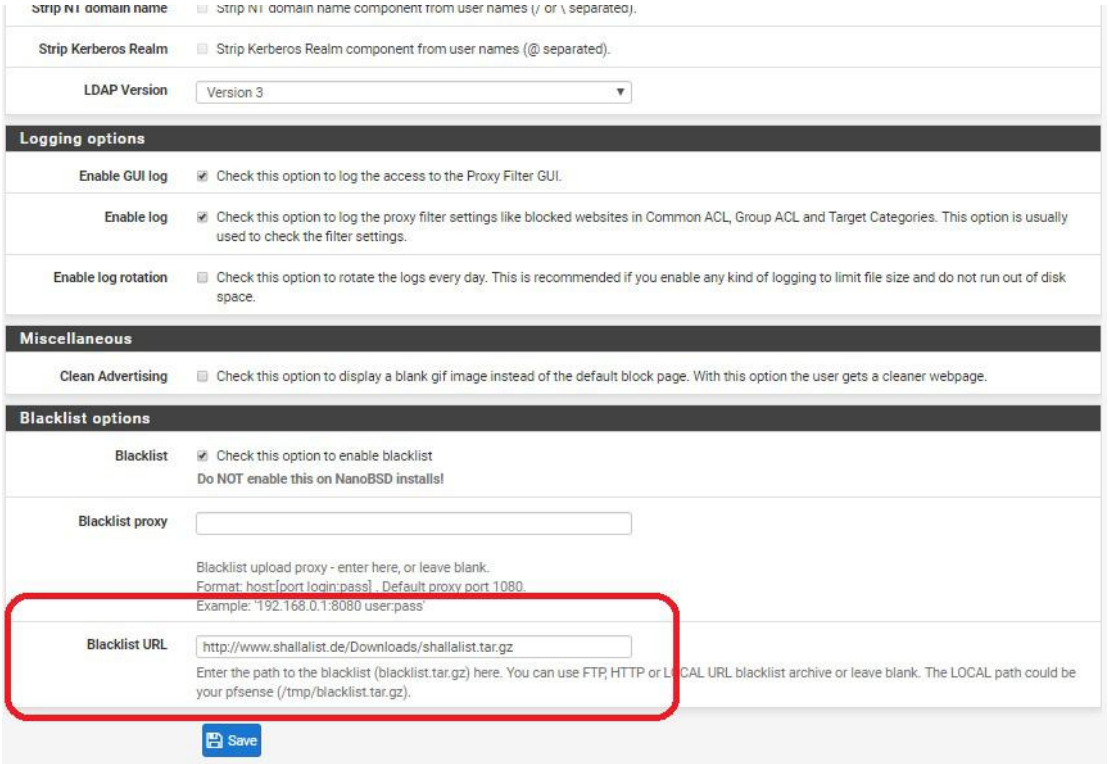


Configuração da Blacklist

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




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.
Apply
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
Version 3
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.



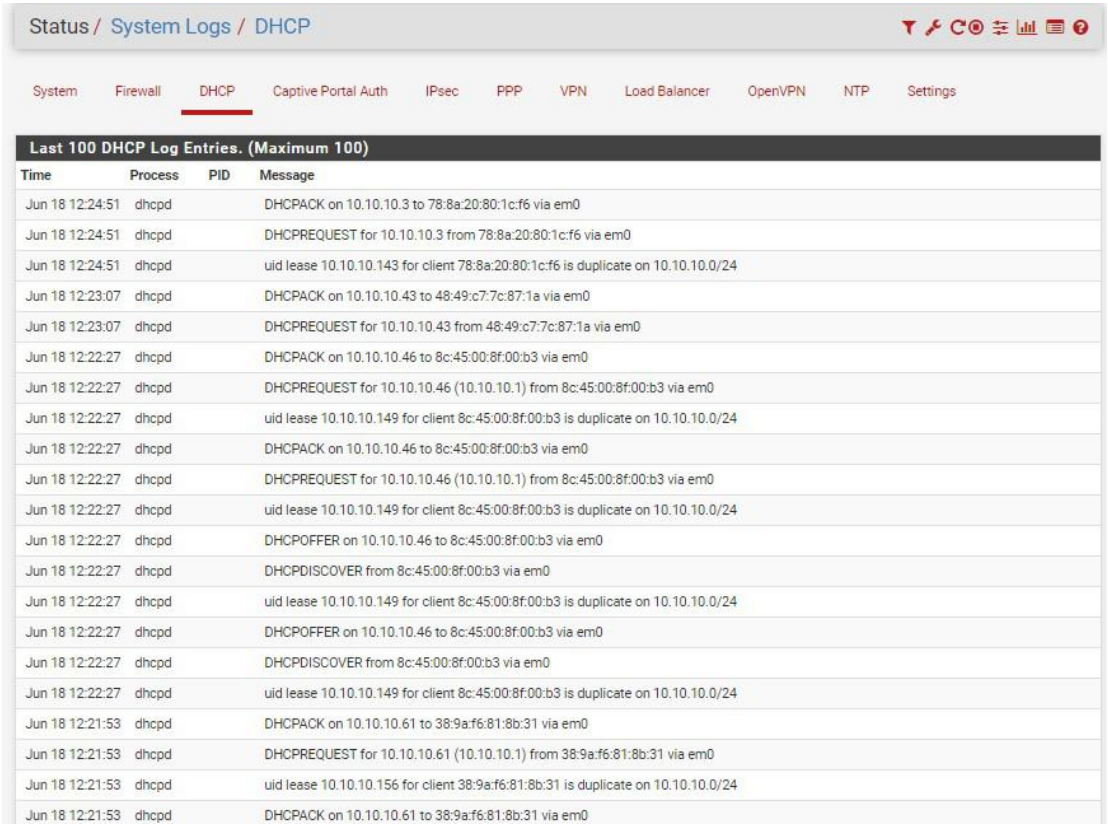
Log/Firewall

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.

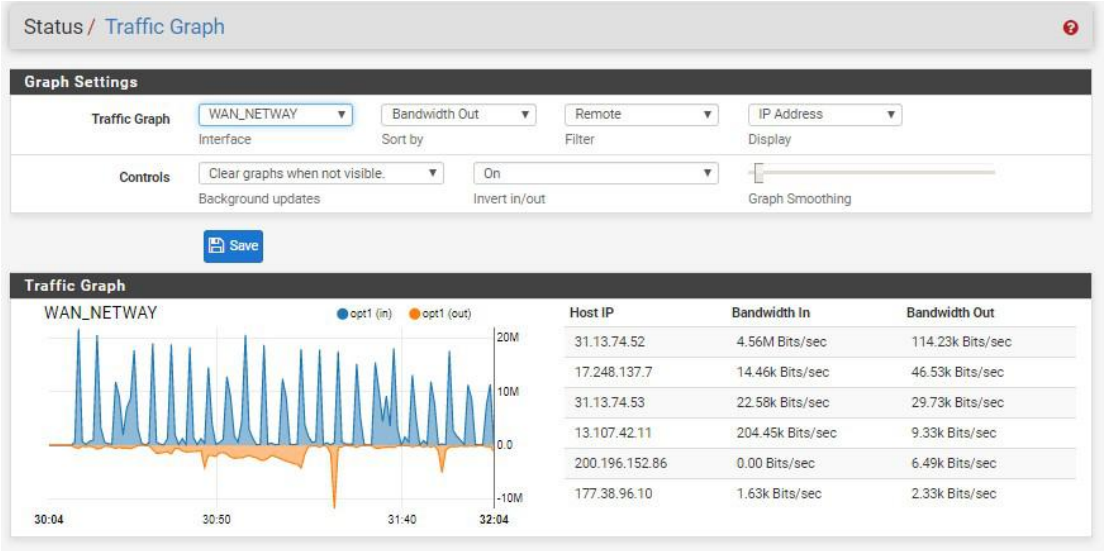


Log/OpenVPN

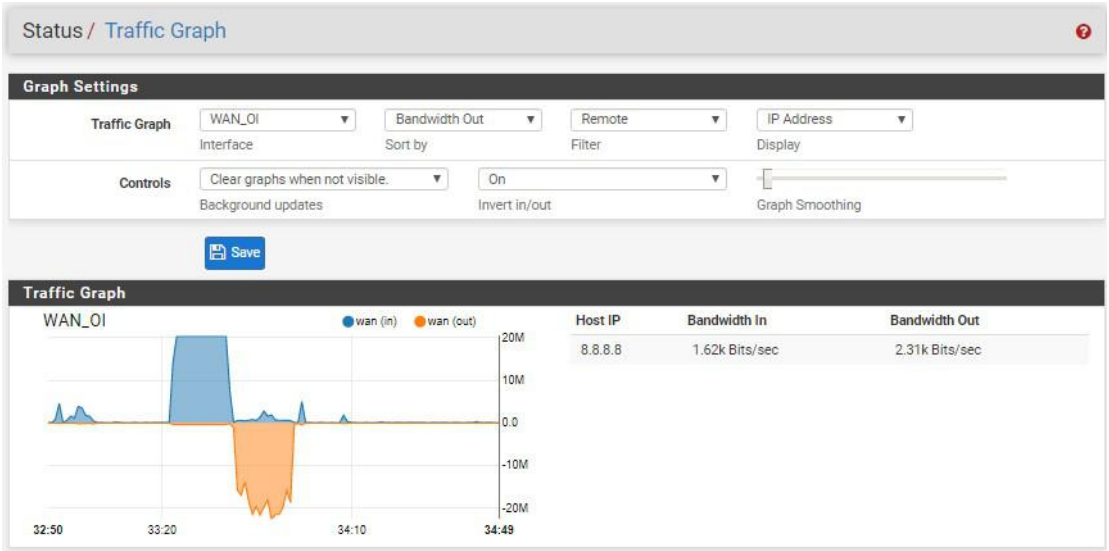
Podemos identificar e acompanhar todos os acessos efetuados pela VPN.

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