Implementação de políticas de segurança em pequenas e médias empresas

Raul Aparecido Franco Simionato

Inconfidentes
2013

Raul Aparecido Franco Simionato

Implementação de políticas de segurança em pequenas e médias empresas

Trabalho de Conclusão de curso apresentado como pré-requisito de conclusão do curso de Graduação Tecnológica em Redes de Computadores no Instituto Federal de Educação, Ciência e Tecnologia do sul de Minas Gerais – Campus Inconfidentes, para obtenção do título de tecnólogo em Redes de Computadores.

Orientador: Luiz Carlos Branquinho Caixeta Ferreira

Inconfidentes
2013

Raul Aparecido Franco Simionato

Implementação de políticas de segurança em pequenas e médias empresas

_____
Orientador: Prof. Luiz Carlos Branquinho Caixeta Ferreira
IFSULDEMINAS – Campus Inconfidentes

_____
Prof. André Luigi Amaral di Salvo
IFSULDEMINAS – Campus Inconfidentes

_____
Prof. Michelle Nery
IFSULDEMINAS – Campus Inconfidentes

Dedico este trabalho primeiramente a Deus.
Dedico também aos meus pais, Paulo e Nilcéia, e aos demais familiares, inclusive alguns que não estão mais presentes, que sempre me apoiaram em meus estudos e na busca por conhecimento.
Alem destes, dedico também aos meus amigos, que sempre me apoiaram e incentivaram a seguir em frente, mesmo em momentos difíceis.

AGRADECIMENTOS

Agradeço a todos os professores, que estiveram presentes durante a minha formação.
Em especial, agradeço o meu orientador, pela ajuda e incentivo no decorrer do trabalho.

"Se algum dia alguém lhe disser que seu trabalho não é o de um profissional, lembre-se: amadores construíram a Arca de Noé e profissionais, o Titanic." (Mestre Arièvlis)

RESUMO

Este trabalho de conclusão de curso tem como objetivo estudar as ferramentas necessárias para a aplicação de uma política de segurança da informação em empresas de pequeno e médio porte, utilizando uma empresa do ramo textil como estudo de caso. Para cumprir tal objetivo, foi feito um levantamento da estrutura, e a partir deste foi elaborado uma Política de Segurança. Com a política elaborada, e baseando-se nela, foram implementadas soluções para controlar o acesso e garantir que as informações da rede fiquem em segurança contra acessos indevidos, tanto oriundos da rede interna quanto da rede externa.

ABSTRACT

This course conclusion work aims to study the tools necessary to implement a policy of information security in small and medium, using a branch company of textile as a case study. To fulfill this goal, a survey was made of the structure, and from this was drawn a Security Policy. With the policy developed, and based on it, were implemented solutions to control access and ensure that the network information stay safe against unauthorized access, both originating from the internal network as the external network.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Devido ao grande aumento na informatização nos últimos anos, grande parte ou todas as informações de uma corporação são disponibilizadas na rede. No atual cenário, até as menores empresas possuem uma rede interna, onde se pode compartilhar recursos entre os funcionários, tais como internet, softwares gerenciais, entre outros.

Quando nos referimos a pequenas e medias empresas, é imprescindível a utilização de uma rede corporativa, para que os diversos setores possam compartilhar informações, facilitando a comunicação e o desenvolvimento das atividades diárias.

Porem, este compartilhamento gera um problema para as empresas: como manter estas informações sempre disponíveis, e proteger o acesso das mesmas do acesso indevido. Para o administrador de rede,esta não é uma tarefa fácil, já que envolve diversos fatores, tanto em softwares como hardwares, além do fator humano que inclui todos os que de alguma forma utilizam a estrutura de rede.

Para que se tenha um controle efetivo de toda a rede, dos serviços disponibilizados por ela e dos colaboradores que as utilizam, é necessário um grande empenho do setor de TI.

O objetivo deste trabalho é mostrar algumas diretrizes a serem seguidas para um bom controle. Nele serão vistas maneiras de se padronizar uma estrutura. A criação de uma política de segurança para se definir os detalhes e objetivos de controle. Além disso, serão mostradas a configuração do Active Directory no Windows Server 2008, utilizado para controlar quais usuários tem acesso a determinadas informações. A partir dele são controlados os acessos a rede corporativa, por meio de um domínio. Para finalizar, será mostrado a configuração de um firewall, com a finalidade de controlar o acesso a serviços potencialmente prejudiciais a rede interna.

O primeiro passo para o controle é conhecer toda a estrutura da empresa. Não há como definir políticas de segurança sem conhecer o que se quer defender. Nesta parte serão vistas algumas diretrizes para se mapear um estrutura, através do levantamento de todos os componentes, sejam eles de software, hardware ou componentes humanos. Um ponto que facilita o controle é a padronização da rede

interna. Quando se trabalha com uma estrutura padronizada, uma mesma solução de segurança pode ser aplicada em toda a estrutura.

Após ser feito o mapeamento e padronização da estrutura, é importante definir uma política de segurança. Nela serão descritos todos os detalhes que devem ser observados na configuração das ferramentas que farão a segurança. Detalhes como nível de acesso dos colaboradores, serviços disponíveis, entre outros.

Depois de concluídas estas etapas, inicia-se o processo de configuração das ferramentas. A primeira delas consiste em configurar um servidor de domínio, que será responsável por controlar o acesso dos usuários as informações disponíveis na rede corporativa.

Por ultimo, a instalação de um firewall para controlar o tráfego entre a rede interna e a rede externa. Não há como pensar eu uma empresa que não utilize serviços disponíveis na web ou disponibilize serviços para serem acessados remotamente. Por isso, é imprescindível que haja um controle deste tráfego, para que nenhuma informação possa ser acessada indevidamente, e para que conteúdos externos possam prejudicar a rede interna.

2 REFERENCIAL TEÓRICO

Abaixo serão mostrados alguns estudos que explicam a importância de se ter uma política de segurança, com ferramentas de controle dentro das redes corporativas.

2.1 Princípios da Segurança da Informação

Segundo Mauricio Rocha Lyra, “Segurança é um assunto muito discutido na atualidade, e tem várias vertentes.” Existem vários fatores em destaque que envolvem segurança da informação. Entre eles podemos destacar três, que podem ser definidos como os princípios da segurança, os quais são mostrados na Figura 1. São eles:

- Confidencialidade: capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo que impede que outros, não autorizados, as vejam.
- Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.
- Disponibilidade: a informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais.

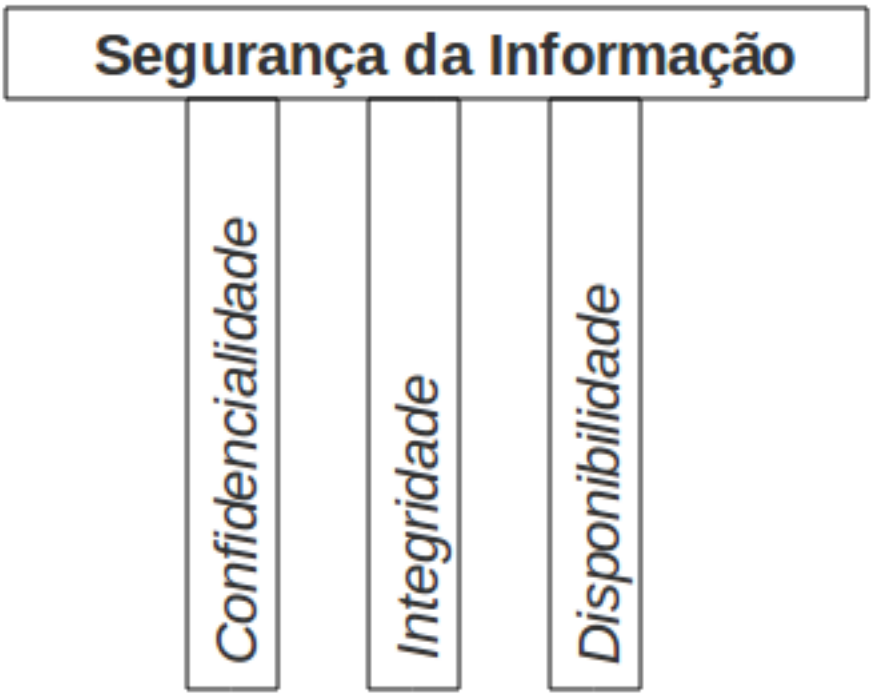

Figura 1 - Principios da segurança da informação

Alem destes três, podemos citar mais alguns fatores que servem como base para a segurança da informação:

- Autenticação: garantir que um usuário é quem alega ser.
- Não repúdio: capacidade de um sistema de provar que um usuário executou uma determinada ação.
- Legalidade: garantir que o sistema esteja aderente a legislação pertinente
- Privacidade: capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações (como no caso do voto eletrônico).
- Auditoria: capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.

Alem destes, há muitos outros fatores que podem ser considerados importantes para um bom sistema de segurança da informação, variando de acordo com a necessidade da empresa, do sistema, etc.

Para que a rede de uma empresa consiga atender a estes aspectos, as suas estrutura deve seguir determinados padrões, para facilitar a manutenção, auditoria e o controle da mesma.

2.2 Importância de uma política de segurança

Para o NIC.BR, “uma política de segurança é um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade).”

A política de segurança não apresenta os parâmetros que devem ser seguidos. Ela apenas apresenta as possibilidades aos usuários, para que estes conheçam as ferramentas que tem à disposição, passando assim a ser eles os responsáveis por manter os recursos em dia.

Outra função da política, quando determinado pela organização na qual ela é aplicada, consiste em informar quais as penalidades cabíveis no caso em que houver infrações as situações e procedimentos descritos.

Antes que a política de segurança seja escrita, é necessário definir a informação a ser protegida. Usualmente, isso é feito através de uma análise de riscos, que identifica:

- recursos protegidos pela política;
- ameaças às quais estes recursos estão sujeitos;
- vulnerabilidades que podem viabilizar a concretização destas ameaças, analisando-as individualmente.

Uma política de segurança deve cobrir os seguintes aspectos:

- aspectos preliminares:
    - abrangência e escopo de atuação da política;
    - definições fundamentais;
    - normas e regulamentos aos quais a política está subordinada;
    - quem tem autoridade para sancionar, implementar e fiscalizar o cumprimento da política;
    - meios de distribuição da política;
    - como e com que frequência a política é revisada.
- política de senhas:
    - requisitos para formação de senhas;
    - período de validade das senhas;

  - normas para proteção de senhas;
  - reuso de senhas;
  - senhas default.
- direitos e responsabilidades dos usuários, tais como:
  - utilização de contas de acesso;
  - utilização de softwares e informações, incluindo questões de instalação, licenciamento e copyright;
  - proteção e uso de informações (sensíveis ou não), como senhas, dados de configuração de sistemas
  - e dados confidenciais da organização;
  - uso aceitável de recursos como email, news e páginas Web;
  - direito `a privacidade, e condições nas quais esse direito pode ser violado pelo provedor dos recursos (a organização);
  - uso de antivírus.
- direitos e responsabilidades do provedor dos recursos, como:
  - backups;
  - diretrizes para configuração e instalação de sistemas e equipamentos de rede;
  - autoridade para conceder e revogar autorizações de acesso, conectar e desconectar sistemas e equipamentos
  - de rede, alocar e registrar endereços e nomes de sistemas e equipamentos;
  - monitoramento de sistemas e equipamentos de rede;
  - normas de segurança física.
- ações previstas em caso de violação da política:
  - diretrizes para tratamento e resposta de incidentes de segurança;
  - penalidades cabíveis.

3 METODOLOGIA

Este trabalho consiste em um estudo de caso, aplicando as ferramentas necessárias para se obter uma rede segura dentro de uma empresa de médio porte. É importante destacar este fato, pois apesar de haver uma base a ser seguida durante os estudos e as implementações, o que realmente será analisado, estudado e implementado depende das necessidades do ambiente em questão, no caso, a estrutura de uma empresa do ramo têxtil, com uma média de 150 funcionários diretos, que dependem de uma estrutura de rede segura e confiável para a realização de suas atividades de rotina, em diversos setores.

O motivo que levou a elaboração deste estudo foi a necessidade de se proteger as informações que ficam disponíveis na rede interna de acessos indesejados, tanto vindos da própria rede interna quanto da rede externa.

O primeiro passo foi fazer um levantamento da estrutura atual da empresa, verificando todos os pontos em questão, averiguando os possíveis pontos de fragilidade e as necessidades de adequação.

A partir daí, foi elaborada uma política de segurança, para que esta fosse a base para todas as implementações a serem realizadas. Neste documento, foram estabelecidas as regras básicas de conduta dos usuários e administradores de rede, bem como os padrões a serem seguidos dentro da estrutura.

Após isto, foram estudadas ferramentas necessárias para se fazer cumprir as diretrizes estabelecidas na política de segurança. Estas ferramentas incluem softwares (Firewall IPcop, Windows Server 2008), hardwares, além de treinamentos aos usuários, para divulgação e conscientização quanto a importância de se adotar e seguir a política.

Com as ferramentas selecionadas, o trabalho segue para a parte prática, onde as ferramentas são implementadas, fazendo com que as diretrizes estabelecidas sejam cumpridas, disponibilizando os recursos e protegendo os usuários.

4 DESENVOLVIMENTO

Este capitulo mostra o desenvolvimento dos trabalhos na estrutura da rede, desde o levantamento e documentação até as implementações práticas na estrutura.

4.1 Cenário anterior

Este trabalho foi desenvolvido em uma empresa do ramo têxtil, de médio porte. A empresa possui 150 funcionários diretos, além de alguns outros terceirizados. Produz e distribui cortinas de tecido para todo o Brasil.

Para organizar e controlar as informações, possui 45 estações ligadas em uma rede interna, conectadas à internet, para acesso as informações necessárias para o desenvolvimento das rotinas de todos os usuários. Além do acesso a informações disponíveis externamente, a empresa disponibiliza serviços no servidores internos que devem ser acessados externamente. Isso se faz necessário para que representantes, supervisores e vendedores possam acessar informações referentes à empresa mesmo estando fora da base de atuação.

A figura 2 mostra um esboço do cenário de rede da empresa. Nela podemos ver que os microcomputadores não possuem um padrão de configuração apropriado. A principio pode-se verificar que possuem configurações de rede divergentes, além de nomenclatura variada, dificultando a localização e atribuição de configurações aos mesmos. A empresa não possuía documentação da estrutura de rede, como nomes, configurações, usuários ou localização de maquinas. Não havia controle do acesso às pastas disponibilizadas no servidor e como a internet é disponibilizada na rede, qualquer usuário ou computador pode acessar a mesma.

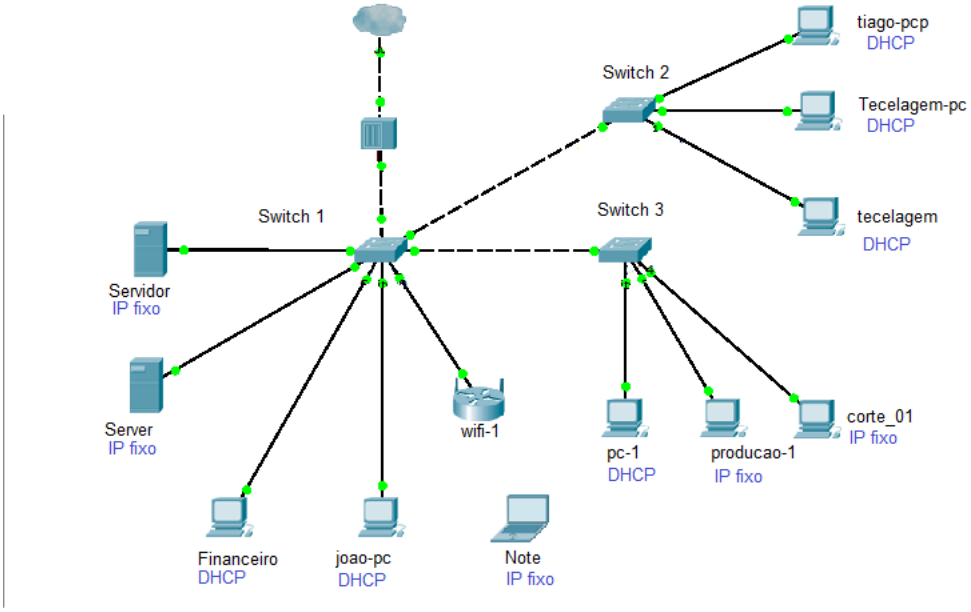

Figura 2 – Cenário anterior

4.2 Documentação

O primeiro passo para uma correta implementação de política de segurança consiste em conhecer a estrutura. Fazer um levantamento de toda a rede, padronizar e documentar a estrutura, para que seja mais fácil controlar, e no caso de falhas, localizar a origem do problema.

4.2.1 Segurança dentro das empresas

Até o momento foi feita uma abordagem geral sobre segurança da informação, mostrando os seus fundamentos. Conforme foi visto, diversas organizações trabalhando juntas definem padrões que fazem com que sistemas distintos possam

operar em conjunto. Esse fator é extremamente importante, pois permite que diversas soluções sejam aplicadas a um mesmo ambiente.

Agora, será feita uma abordagem sobre a padronização voltada para o ambiente empresarial. O foco deste trabalho é determinar maneiras de se aplicar uma política de segurança dentro de empresas de pequeno e médio porte.

4.2.2 Cenário empresarial

O primeiro passo consiste em se fazer um levantamento do cenário da empresa. Levantar os fatores críticos para a definição da política de segurança, as vulnerabilidades presentes, e o que deve ser feito para que se tenha uma estrutura padronizada.

Dentre estes fatores, podemos citar o fator humano, as vulnerabilidades dos softwares utilizados nas rotinas do dia-a-dia dos colaboradores, as vulnerabilidades físicas da estrutura da rede, entre outros.

4.2.2.1 Fator humano

Este é um fator importantíssimo de ser analisado para que a integridade das informações que circulam dentro da rede de uma empresa seja mantida. O sucesso ou o fracasso de um sistema de segurança está diretamente ligado aos usuários que o utilizam.

Segundo Zurco e Simon, sistemas dito seguros, particularmente, são conhecidos por sua pouca amigabilidade. Este é um fator interessante de ser analisado e levado em consideração no momento de se padronizar um software dentro de uma empresa.

Ter um software que ofereça um nível de segurança mais elevado é muito importante para que as informações manipuladas por ele mantenham-se confiáveis. Porém, quando para se obter um nível de segurança mais elevado, é necessário diminuir o rendimento diário do colaborador, esta solução perde a sua viabilidade.

Deve-se localizar um ponto de equilíbrio entre os fatores rendimento e

segurança, para que ambas as partes possam ser satisfeitas. Políticas e padrões de segurança da informação dentro de uma organização devem passar o mais despercebido possível pelos usuários, para que eles possam desenvolver suas tarefas da maneira mais natural possível, sendo que por trás de toda a estrutura, a segurança seja mantida.

4.2.2.2 Vulnerabilidades de softwares

Com o aumento da necessidade de que as informações sejam processadas e analisadas mais rapidamente, o uso de softwares cada vez mais detalhados e específicos aumentou exponencialmente dentro das empresas.

Desde tarefas simples como controlar a quantidade de peças produzidas até analises detalhadas que levam em consideração diversos fatores dentro da linha de produção, tornou-se indispensável a utilização de sistemas.

O aumento da utilização destes softwares causou um rápido crescimento no numero de soluções disponíveis no mercado, desde softwares simples para gestão de escritórios até soluções bastante complexas capazes de integrar os diversos módulos de uma empresa em um só sistema, soluções estas conhecidas como ERP (Enterprise Resource Planning – Planejamento de Recursos Empresariais).

Porem, esse aumento na utilização causou também um grande aumento na quantidade de softwares maliciosos. O gráfico apresentado na Figura 3 mostra um levantamento feito pelo CERT (Centro de estudos, Respostas e Tratamento de incidentes de segurança no Brasil) com a quantidade de spams reportados a entidade de 2003 a junho de 2012.

Estes spams são responsáveis pela disseminação de softwares maliciosos. Contando muitas vezes com a colaboração do usuário que nem sempre tem conhecimento dos meios utilizados pelos atacantes, estes malwares se instalam no computador, para os mais diversos objetivos.

Eles exploram as fragilidades dos sistemas operacionais e aplicativos instalados, para obter informações sobre o usuário ou a empresa.

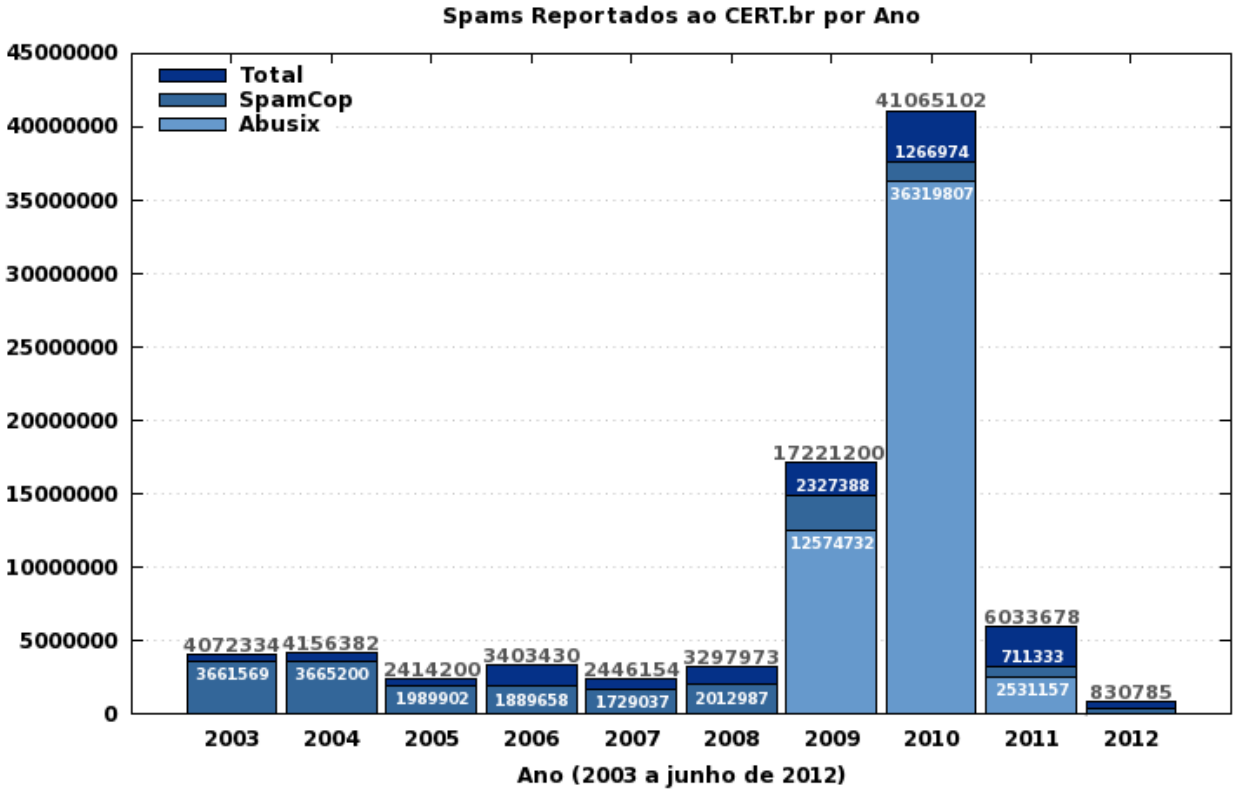

Figura 3 - Ataques de Spans reportados ao CERT
Fonte: (http://www.cert.br/stats/spam/).

4.2.2.3 Vulnerabilidades de hardware

Além dos fatores humano e de software, existe também as vulnerabilidades ligadas ao hardware ou a parte física da rede dentro de uma empresa.

Um grande problema que deve ser analisado refere-se a questão de redes wireless. Com o grande aumento mobilidade, seja ela com a utilização de notebooks, tablets ou celulares, é imprescindível a disponibilização de um sinal sem fio dentro de uma empresa.

Porem, esse fator gera um problema: como disponibilizar a mobilidade para os colaboradores sem que as demais pessoas que circulam na abrangência do sinal façam um mau uso do mesmo para fins que não sejam de interesse da organização.

Além de mau uso do sinal, ao entrar com um novo host dentro de uma organização, host este que não pertence a mesma e portanto pode não estar com as mesmas configurações e proteções dos demais, este pode se tornar uma porta de entrada na rede. Através desta porta, um atacante pode entrar na rede sem passar por qualquer mecanismo de defesa existente na entrada da rede.

4.2.3 Levantamento da estrutura

Acima foi explanado os principais pontos que geram vulnerabilidades dentro da rede de uma empresa.

Devido a grande quantidade de informações que circula nas redes e servidores das empresas, e sabendo que estas informações são um ativo de grande valor para a empresa, é extremamente necessário a proteção de toda estrutura.

Para isso, diversas soluções podem ser utilizadas, como firewalls, vlans, entre outros. Porém, o primeiro passo para que uma solução possa ser aplicada é conhecer todos os detalhes da estrutura.

É necessário fazer um levantamento de todas as partes da estrutura interna da empresa, para assim poder avaliar a situação da rede e verificar as vulnerabilidades. Este levantamento da rede deve analisar todos os componentes da estrutura, isso inclui todos os ativos, usuários, hosts fixos e hosts móveis, endereços de redes, entre outros.

Geralmente as empresas contam com uma estrutura básica que possui computadores distribuídos em diversos setores, que vão desde o administrativo até a produção, e executam as mais diversas tarefas. Outro detalhe que sempre estará presente são os servidores. Nestes, são rodados os serviços principais e é onde ficam as principais informações, portanto, deve ser dada uma atenção especial, pois eles geralmente serão os alvos de um ataque.

O primeiro passo para o levantamento da rede é relacionar todos os hosts. Identificar fisicamente a localização das maquinas, e quais funções são desenvolvidas nela. É necessário um relatório preciso, que relacione a localização do micro fisicamente, para que fique fácil localizá-lo posteriormente, as configurações de hardware (memória, HD, entre outros), qual (is) os usuários

utilizam, quais as funções que são desenvolvidas e quais aplicativos utilizados.

É importante detalhar isto, para que na hora de definir os padrões a serem seguidos, possa se saber exatamente as necessidades da empresa e de seus colaboradores. Também é necessário quando acontece algum incidente de segurança. Sabendo-se as configurações, é mais fácil prever onde pode ter ocorrido o incidente. Este levantamento é também uma ótima oportunidade para começar uma análise nas vulnerabilidades de rede. Documentar toda a rede também é essencial para que no futuro outras pessoas possam entender melhor a estrutura.

Os dados que serão levantados podem variar de acordo com o administrador de rede e da empresa. Na Tabela 1 temos um exemplo que pode ser feito com os dados básicos de levantamento da estrutura da rede.

Tabela 1 - Exemplo de tabela relacionando informações básicas da rede

Nome	Setor	Usuário	HD	Memória	SO	Aplicações
Server_01	Servidores	Administrador	2 TB	8 GB	Windows Server 2008	ERP, Active Directory, DHCP
Micro_01	Recursos Humanos	João	500 GB	2 GB	Windows 7	Sistema Ponto
Micro_02	TI	Pedro	1 TB	4 GB	Windows 7	-
Micro_03	Financeiro	Maria	320 GB	2 GB	Windows 7	Gerenciador Bancário

Fonte: Autoria própria.

Após se fazer um levantamento dos hosts da rede, deve-se levantar a outra parte da estrutura, composta por cabos, switches, roteadores sem fio, pontos de rede, hubs, entre outros.

A finalidade de se levantar esta parte da estrutura é verificar se em algum ponto é possível que um invasor encontre uma entrada para a rede interna. Com este levantamento também se pode determinar se a rede suporta uma possível necessidade de expansão.

Também neste caso é necessário relacionar os detalhes da estrutura, como por exemplo o caminho seguido pelos cabos (eletrodutos, eletrocalhas, caixas de passagens) desde a saída nos switches até o ponto de rede em cada estação. Assim, fica fácil identificar focos de problemas e possíveis locais de invasões.

Após se fazer todo o mapeamento físico da rede, relacionando todos os ativos e passivos da rede, e também todos os usuários, o ultimo passo para o mapeamento é relacionar os endereços lógicos.

Isto é necessário para que no momento da configuração de um firewall ou na divisão da rede em sub-redes se possa direcionar o tráfego e criar as regras corretas para cada usuário.

Da mesma maneira que os hosts e os equipamentos utilizados na rede, é necessário também relacionar e documentar todos os endereços IPs das redes, bem como os endereços mac das maquinas, relacionando uns aos outros, de maneira que as regras de segurança fiquem mais seguras ao se bloquear ou permitir tanto o mac quanto o IP.

4.2.4 Padronização no uso dos recursos computacionais

Após feita toda a documentação da estrutura da rede, deve-se realizar um trabalho de padronização em toda a estrutura de rede. O principal motivo da padronização é facilitar o conhecimento de todas as estruturas da rede, sabendo-se que todos os recursos e soluções aplicados a um ponto da rede pode ser aplicado aos outros pontos.

Esta padronização pode ser dividida em três partes principais: Software, hardware e Nomenclatura.

4.2.4.1 Padronização de Softwares

Como a cada dias novos softwares são lançados no mercado, os que já existem precisam sempre estar atualizados para que não percam em eficiência. Com a utilização dos mesmos softwares para determinadas tarefas em todas as estações da rede fica muito mais fácil controlar e atualizar.

Além disso, todas as ameaças de segurança deste software podem ser resolvidas de uma mesma maneira, não precisando aplicar uma solução para cada maquina.

Um outro ponto a ser observado se refere a utilização de antivírus. Com o aumento exponencial no numero de vírus e malwares, é necessário um bom e

atualizado software para combater. Para o cenário empresarial, temos antivírus pagos que controlam toda a estrutura de rede, e também soluções gratuitas, geralmente com menos funcionalidades, mas que ajudam a proteger.

Independente de se ter um antivírus empresarial pago ou uma versão gratuita, é imprescindível que ele esteja sempre atualizado, para que a sua proteção seja aplicada ao máximo.

4.2.4.2 Padronização de Hardware

Padronizar o hardware utilizado na estrutura também facilita no controle da rede. No caso de equipamentos de rede, como cabos, switchs, entre outros, a padronização garante um melhor rendimento da rede. De maneira geral, ter uma estrutura com os equipamentos padronizados facilita na manutenção, no controle e nas soluções a serem aplicadas.

4.2.4.3 Nomenclatura

Este também é um ponto que deve ser observado na hora de padronizar uma estrutura. O padrão a ser seguido para a nomenclatura pode variar de acordo com a empresa ou com o responsável pela padronização, mas independente disto, é necessário que haja um padrão para que, a partir do nome, seja possível identificar a estação e já se tenha em mãos as configurações da mesma.

4.3 POLITICA DE SEGURANÇA DA INFORMAÇÃO

Após ser feito o levantamento e a documentação da situação da rede da estrutura, bem como dos usuários e recursos disponibilizados, partimos para o próximo passo, que consiste em elaborar uma política de segurança.

A política de segurança consiste em um documento criado para proteger a organização das ameaças a segurança da informação, garantindo assim que sejam mantidos os princípios da segurança, conforme citado na sessão 2 deste trabalho.

4.3.1 Elaboração da política

A base para a elaboração da política de segurança consiste no estudo feito na sessão 4.1 deste trabalho, que descreve o cenário da empresa que será estudada, e do levantamento da estrutura e documentação da mesma.

A partir dos detalhes levantados, deve ser elaborado o documento. No caso em questão, foram avaliadas todas as vulnerabilidades da empresa, tanto em softwares como em hardwares.

Estas vulnerabilidades foram apresentadas à diretoria. Também foram apresentadas as ferramentas necessárias para que estas vulnerabilidades fossem resolvidas. A apresentação à diretoria é necessária, pois é esta que define quais os objetivos finais e quais as informações serão disponibilizadas para os colaboradores.

Junto com a diretoria, todas as ferramentas foram apresentadas, e quais os impactos que as modificações trariam para o dia a dia dos funcionários. Neste momento também foram apresentadas as necessidades de aquisição de recursos. No caso, a aquisição de um servidor com Windows Server 2008 e um servidor para Firewall, sendo este de distribuição gratuita.

4.3.2 Detalhes da política

Após a aprovação da diretoria, deve ser elaborado um documento, que será distribuído e assinado por todos os usuários, sendo então seguido como base para o

uso aceitável dos recursos computacionais.

Este documento descreve todos os detalhes que devem ser observados pelos usuários. Abaixo seguem alguns tópicos abordados na política de segurança, com uma breve explicação dos mesmos.

- Introdução: Breve descrição do conteúdo e do objetivo da política.
- Propósito: Mostrar quais os objetivos da política de segurança.
- Abrangência: Delinear a abrangência da política, ou seja, sobre quais recursos computacionais ela tem efeito.
- Direitos dos usuários: Relata todos os direitos dos usuários dentro da organização com relação ao uso e disponibilização de recursos computacionais.
- Deveres dos usuários: Mostra quais os deveres dos usuários para com os recursos disponibilizados, tais como cuidados a serem tomados, classificações das informações, entre outros.
- Proibições: Lista de proibições aos usuários da rede corporativa e dos recursos abrangidos pela política de segurança.
- Compromissos: Semelhante aos deveres do usuários, reforça as ações que são necessárias aos usuários. Esta sessão segue como base de procedimentos que devem ser tomados pelos usuários durante o desenvolver de suas atividades.
- Adição e remoção de recursos: Sessão que descreve o procedimento quando há necessidade de adição ou remoção de recursos computacionais, sendo que estes procedimentos não devem ser feitos pelos usuários e sim pelo administrador da rede.
- Administrador da rede: Descrição da função do administrador dentro da rede e da organização.
- Permissões e senhas: Sessão que descreve as permissões e senhas dos usuários, e quais os procedimentos a serem seguidos pelos usuários após receberem suas informações pessoais de acesso.
- Termo de uso: a ultima sessão da política de segurança consiste em um termo de uso a ser assinado pelos usuários após lidas e entendidas.

Vale ressaltar aqui que esta política consiste de um estudo de caso específico,

portanto, se analisada em outra empresa pode sofrer variações. Outra questão referente a sua elaboração está vinculada a posição da diretoria, que aprovou e resolveu adotar a política de maneira formal na empresa, além de ajudar na criação de suas clausulas.

4.3.3 Treinamento aos usuários

Já com a política de segurança já definida e elaborada, o ultimo passo consiste passar todas as definições aos usuários. Somente após os termos estarem passados a todos os usuários é que vai ser dado inicio à parte pratica, onde todas as definições serão implementadas, com as devidas ferramentas de controle.

O treinamento foi ministrado aos usuários, de maneira individual ou em grupo, dependendo da necessidade e disponibilidade da empresa. Ele foi passado com explicações sobre cada parte da política, esclarecendo as duvidas que surgiram e ao final, assinado o termo de uso.

A política deve sempre ficará a disposição dos usuários para consultas, e deve ser atualizada sempre que houver a necessidade por parte da empresa, sendo que as atualizações devem ser passadas a todos os usuários.

4.4 FERRAMENTAS PARA IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA

Abaixo serão descritas as ferramentas utilizadas para a implantação da política de segurança.

4.4.1 ACTIVE DIRECTORY

Segundo Marty Mathews, o AD (Active Directory) desempenha duas funções básicas dentro de um serviço de rede: Serviço de diretório contendo uma listagem hierárquica de todos os objetos da rede e serviço de autenticação e segurança que controla e provê acesso aos recursos da rede. Esses dois recursos são diferentes na natureza e no foco, porém são combinados para aumentar os recursos de usuários enquanto facilitam o trabalho da administração.

A estrutura do AD é organizada de maneira hierárquica. Os objetos são agrupados em Unidades Organizacionais (OU – organizational unit). Este agrupamento pode ser feito seguindo diversos critérios, dependendo da necessidade da organização em que está sendo aplicado.

Quando se instala o AD, algumas OUs já são instaladas por padrão, e outras podem ser criadas de acordo com a necessidade da organização. Por serem hierárquicas, outras OUs podem ser colocadas dentro das OUs principais, formando assim uma estrutura em que as configurações aplicadas na OU de primeiro nível se aplica a todas as outras que se encontram dentro da mesma.

4.4.1.1 Active Directory e domínios

AD e DNS (Domain Name System) compartilham a mesma central, chamada de domínio.

Um diretório DNS na verdade não armazena os objetos no seu banco de dados. Ao invés disso, DNS armazena domínios, a informação de acesso a cada domínio e

a informação de acesso aos objetos que estão dentro deste domínio.

4.4.1.2 Serviços de Active Directory

Apesar de conter praticamente as mesmas estruturas que os servidores DNS, o AD possui muito mais informações sobre cada objeto do seu banco de dados. Entre outras, ele inclui informações como:

Nome do usuário

Informações de contato, como endereço físico, números de telefone e endereço de e-mail

Contatos administrativos

Permissões de acesso

Propriedades

Atributos particulares de cada objeto

Instalar o AD em um servidor o transforma em um controlador de domínio, ou seja, um servidor que controla e guarda o banco de dados central de todos os usuários e grupos de domínio. Além disso, ele gerencia todas as funções relativas ao domínio, como autenticação de usuários, permissões de usuários, entre outros.

4.4.1.3 DHCP

O serviço de DHCP é o responsável por atribuir e gerenciar os endereços IP na rede. Quando você instala a função de DHCP, é necessária a criação de um escopo, que define quais os endereços que serão distribuídos entre os computadores.

Durante a criação do escopo, deve ser definido o endereço inicial e o endereço final que será distribuído na rede, alem da mascara de rede e os DNS que serão usados pelos computadores. A figura 4 mostra o diretório do DHCP, com suas pastas padrão.

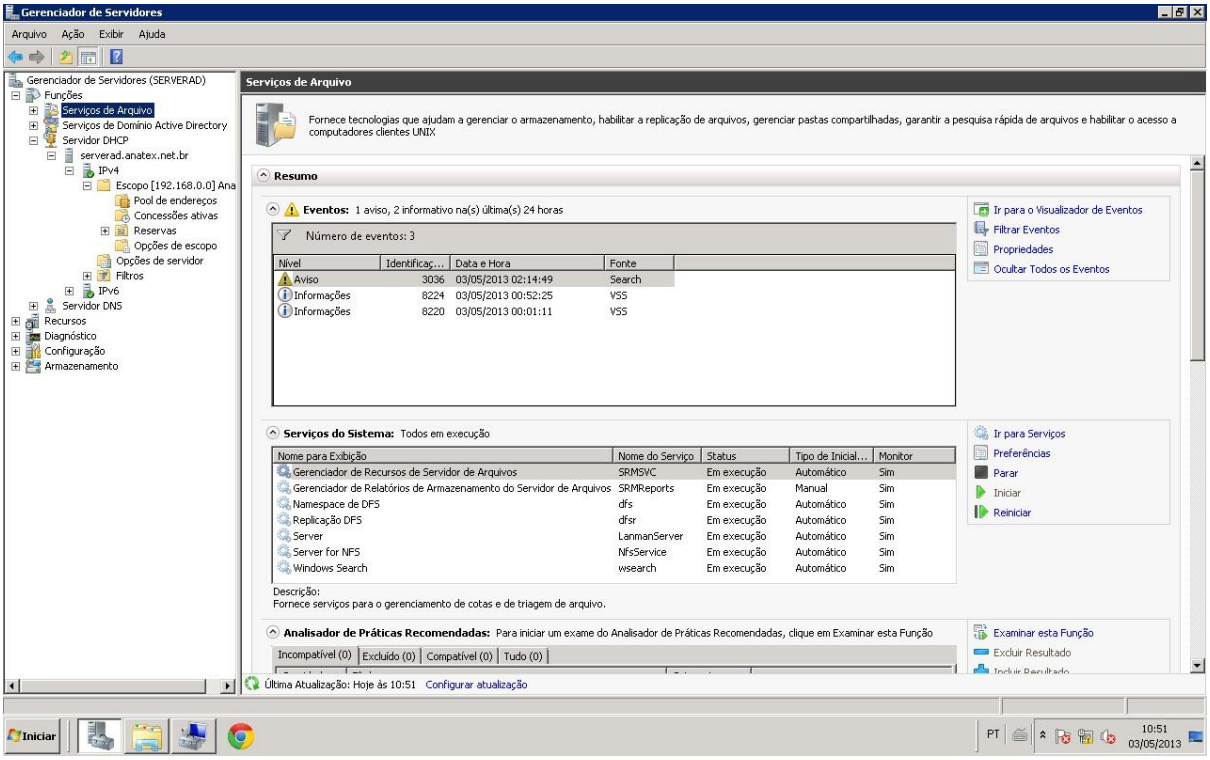

Figura 4 - Estrutura do DHCP

Cada diretório mostrado possui uma função especifica, conforme descrito abaixo:

- Pool de endereços: Endereços que serão atribuídos aos computadores da rede
- Concessões ativas: exibe todos os endereços atribuídos no momento, mostrando o endereço IP, o MAC e o nome da maquina.
- Reservas: Com esta função é possível reservar determinado IP para uma determinado cliente, através do seu endereço MAC.
- Opções do escopo: Possui os arquivos de configuração de DNS e Gateway que serão atribuídos automaticamente aos clientes.

4.4.1.3.1 Reservas de IP

Para que seja possível controlar os acessos a partir da rede, é necessário saber quais IPs são atribuídos a determinados clientes. Só assim será possível aplicar com precisão as regras do firewall. Quando se trabalha com DHCP, os computadores ficam com a opção de IP dinâmico, sendo que os IPs serão distribuídos a medida que os clientes façam requisições de endereço ao servidor.

Para garantir que um cliente sempre receba o mesmo IP, e para que o administrador sempre saiba qual IP foi atribuído, o serviço de DHCP disponibiliza a função de reservas, que seleciona um IP para um cliente.

Para criar uma reserva, basta clicar com o botão direito na pasta reserva do diretório DHCP, e selecionar “Nova reserva”. A Figura 5 mostra a caixa que será exibida. Nela basta preencher o Nome da reserva, o endereço IP que deverá ser atribuído, o endereço MAC e a descrição da reserva. Após isso, basta clicar em adicionar e toda vez que este cliente se conecte a rede, o IP será atribuído à ele.

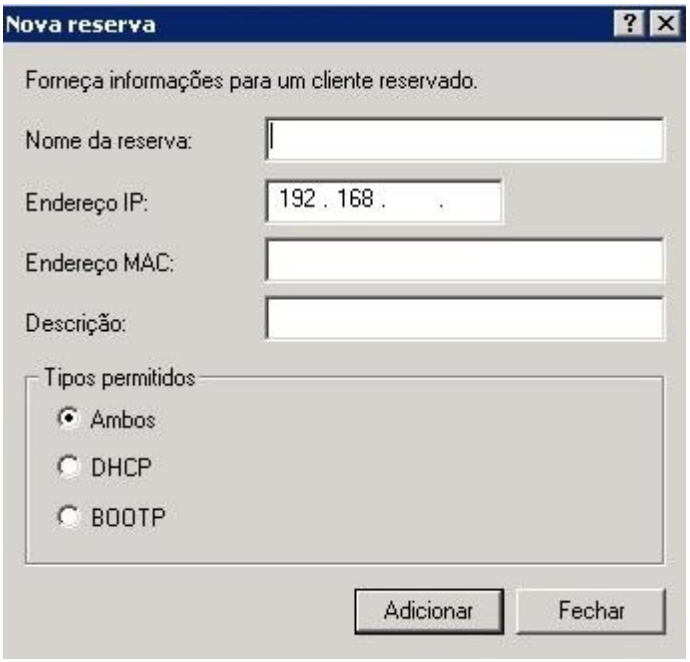

Figura 5 - Reserva de IP

4.4.1.4 Configuração do Active Directory

O próximo passo na configuração dos serviços para gerenciamento de segurança consiste em cadastrar os objetos do domínio, ou seja, os usuários, grupos e computadores. A Figura 6 mostra as unidades organizacionais dentro do Active directory:

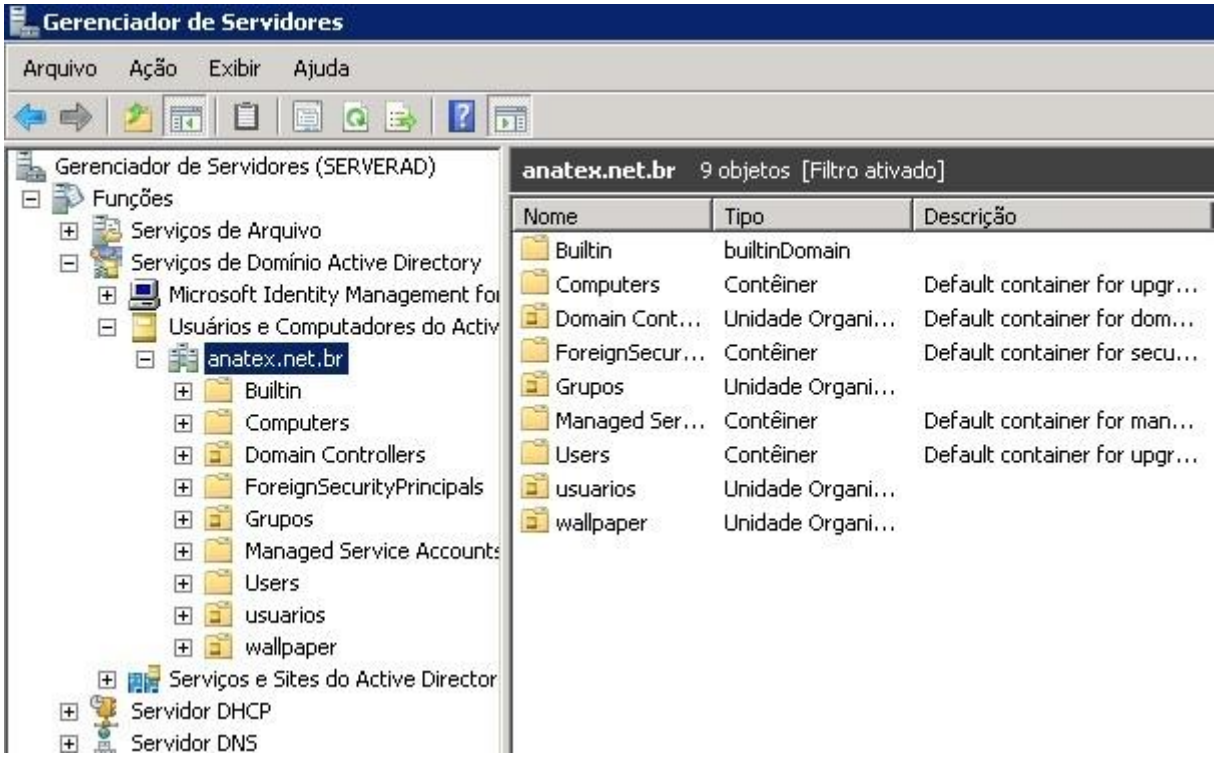

Figura 6 - Active Directory

Conforme já foi citado, algumas destas pastas são criadas por padrão ao instalar a ferramenta. Outras podem ser criadas dependendo da necessidade. No caso, as principais pastas (também chamadas de Unidades Organizacionais) e funções são comentadas abaixo:

- Computers: Onde serão cadastrados os computadores que farão parte do domínio
- Grupos: Pasta onde serão criados os grupos dos quais os usuários farão parte. Uma configuração aplicada a um grupo abrange todos os seus usuários. (Esta pasta não é criada por padrão).
- Users: Pasta com os usuários base do domínio, como controladores.
- Usuários: Pasta onde serão armazenados os usuários do domínio. (Esta pasta não é criada por padrão).

4.4.1.4.1 Cadastro de computadores

Todos os computadores devem ser cadastrados no domínio, para que caso haja necessidade de aplicação de uma politica por maquinas, estas estejam corretamente

cadastradas. Para cadastrar uma nova estação, basta clicar com o botão direito sobre a pasta onde ele será cadastrado, selecionar “Novo” e depois “Computador”, conforme mostra a Figura 7.

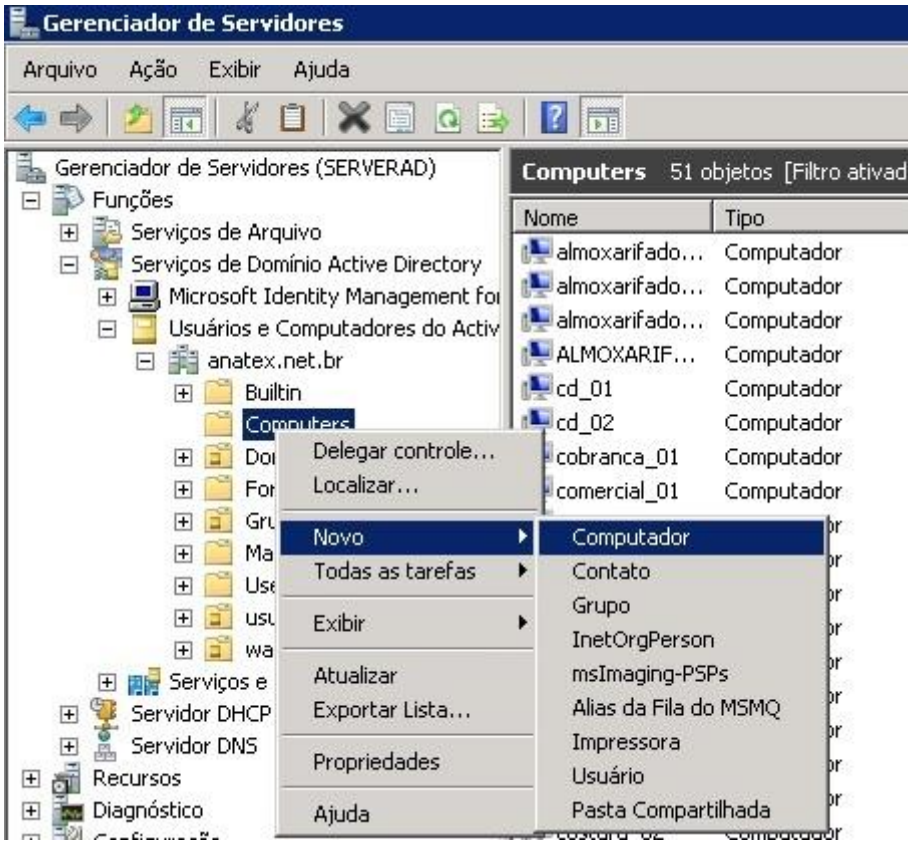

Figura 7 - Acesso ao cadastro de computadores

Na figura acima também podemos ver alguns computadores já cadastrados, que vão aparecer na parte direita da tela, a medida que são cadastrados.

A tela de cadastro de um computador é a mostrada na Figura 8. Nela, basta colocar o nome do computador e clicar em ok.

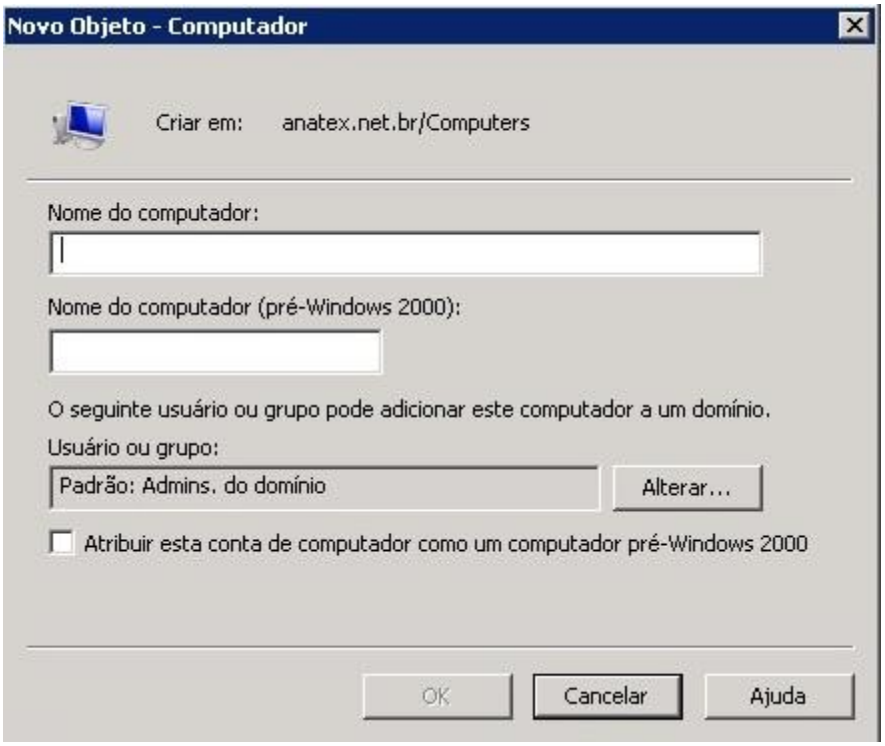

Figura 8 - Cadastro de computadores

4.4.1.4.2 Cadastro de grupos

O cadastro de grupo é bastante semelhante ao cadastro de computadores. A Figura 9 mostra como acessar ao controle para cadastro de um novo grupo. Ao lado direito da mesma figura podemos ver como são exibidos os grupos após o cadastro.

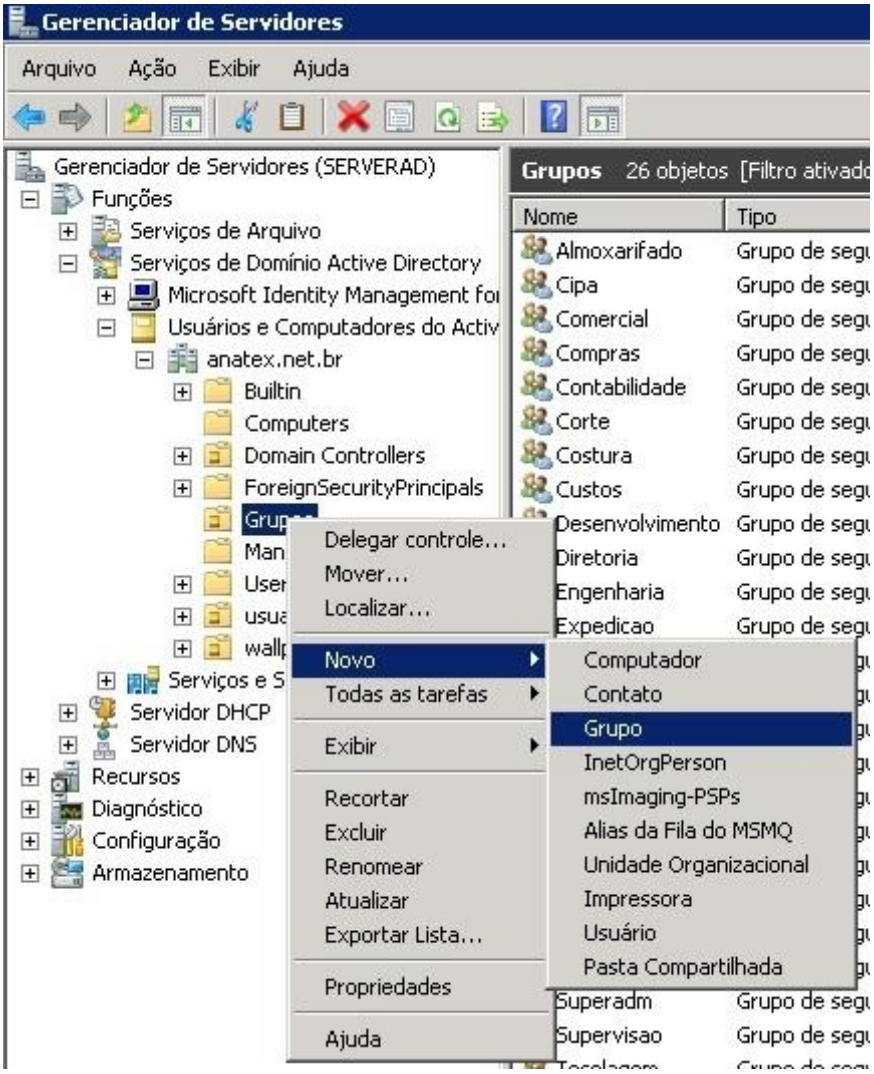

Figura 9 - Acesso ao cadastro de grupos

Ao clicar em grupo, a tela de cadastro de grupo é exibida, conforme mostra a Figura 10.

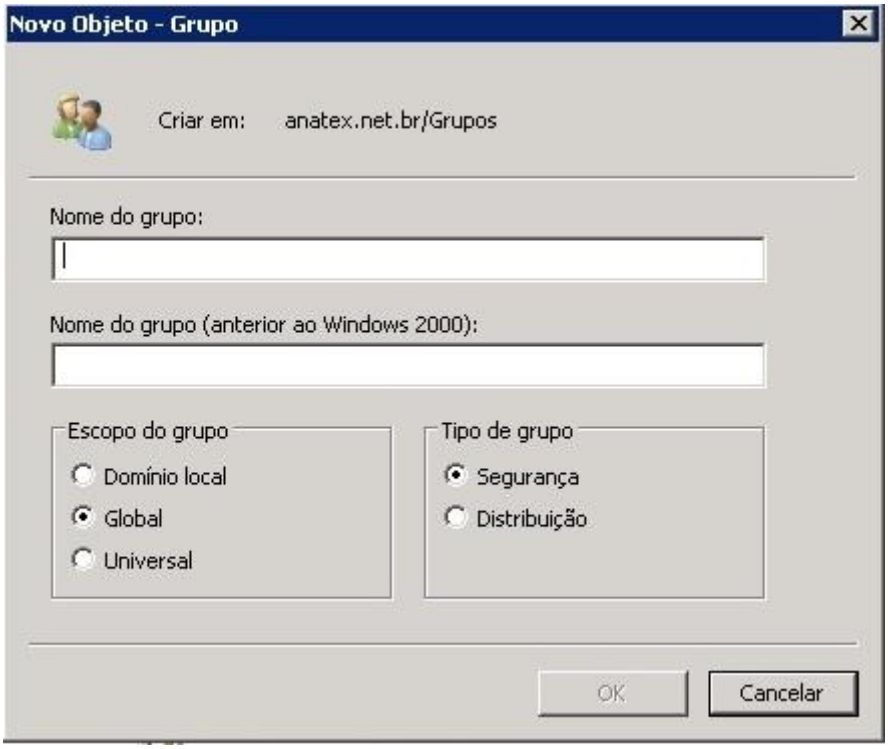

Figura 10 - Cadastro de grupos

Basta colocar o nome do grupo. As opções na parte de baixo da tela servem para informar o tipo de grupo a ser criado. Por padrão, usa-se o Escopo “Global e o tipo Segurança.

4.4.1.4.3 Cadastro de usuários

O cadastro dos usuários também é feito de maneira semelhante aos anteriores. A figura 11 mostra o acesso a este controle.

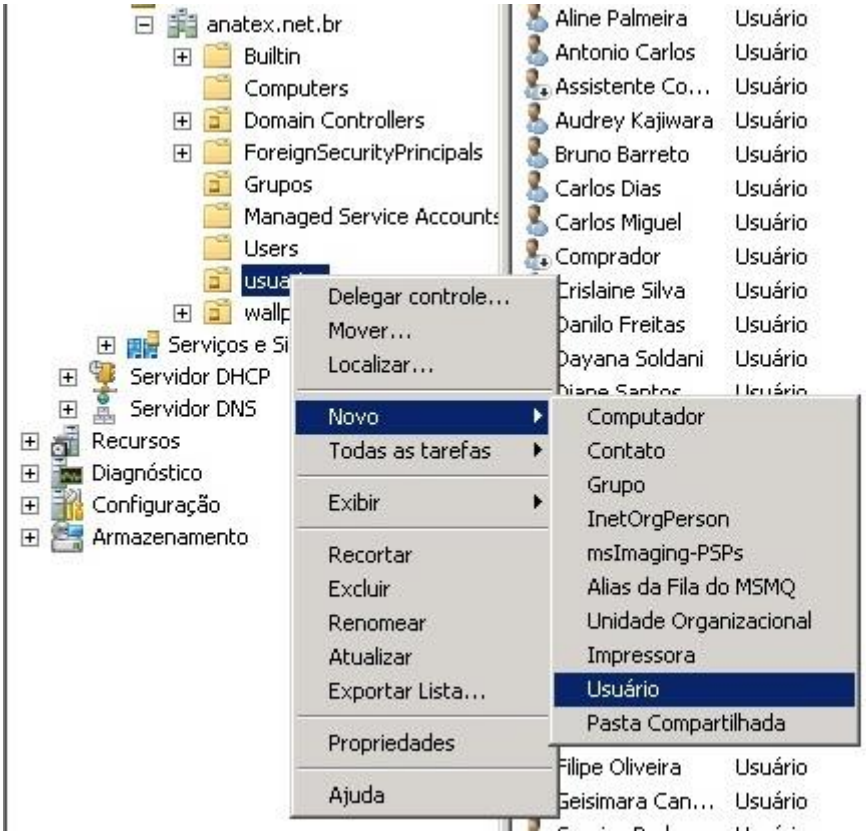

Figura 11 - Acesso ao cadastro de usuários

A figura 12 mostra a primeira tela de cadastro de usuários.

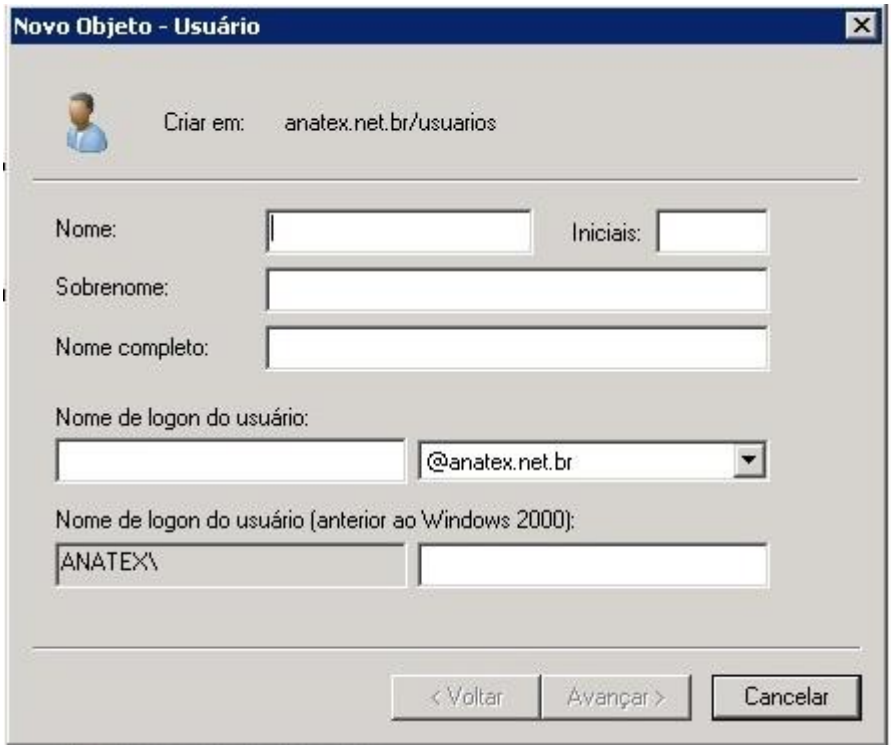

Figura 12 - Cadastro de usuários

Nela, basta preencher o Nome e o Sobrenome (a opção inicial é opcional) e depois o nome que será usado para logon. Vale lembrar que o nome de logon deve ser único para cada usuário na rede. Após isso , basta pressionar “avançar” para ir para a próxima tela de cadastro, mostrada na figura 13.

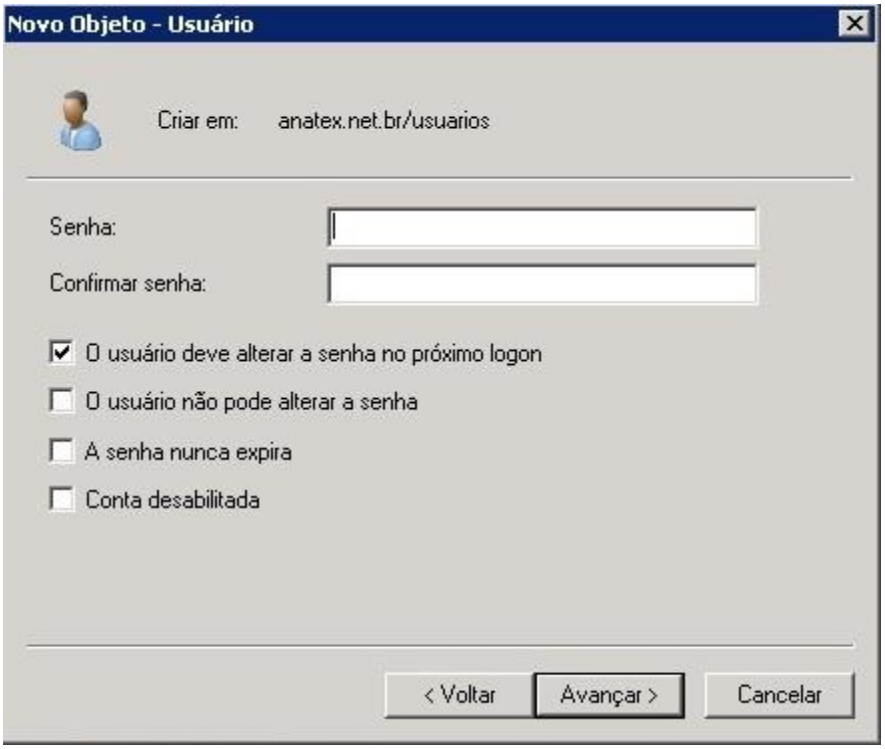

Figura 13 - Finalização do cadastro de usuário

4.4.1.5 Compartilhamento de pastas

O domínio também permite o compartilhamento de pastas no servidor, para que os usuários possam compartilhar informações apenas com as pessoas que necessitam da mesma. Assim é possível definir que pastas de um setor possam ser acessadas apenas por usuário daquele setor ou apenas para um usuário especifico.

As pastas que serão compartilhadas e como elas ficarão no servidor depende da necessidade de cada estrutura. Uma configuração bastante utilizada consiste em se

criar uma pasta para cada departamento e uma para cada usuário. A figura 14 mostra um pasta com várias pastas, uma para cada departamento.

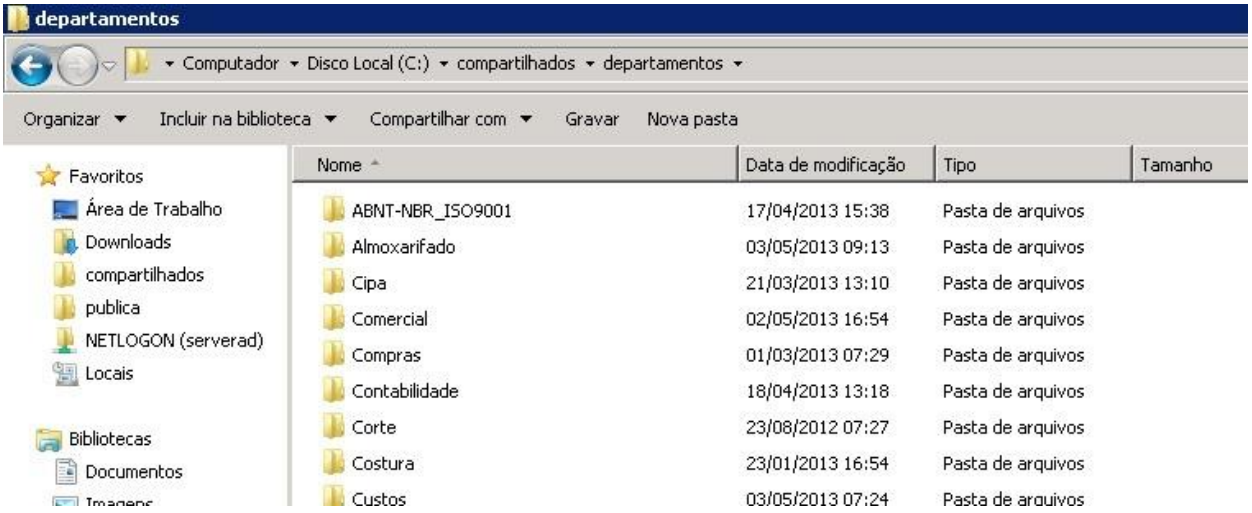

Figura 14 - Estrutura de pastas por setores

Após criar as pastas, deve-se configurá-las para que permitam apenas o acesso dos usuários que necessitam das informações que elas contenham. Pode-se definir que uma pasta seja acessada por todos os usuários, por apenas um ou por um grupo. A figura 15 mostra como configurar os acessos a cada pasta.

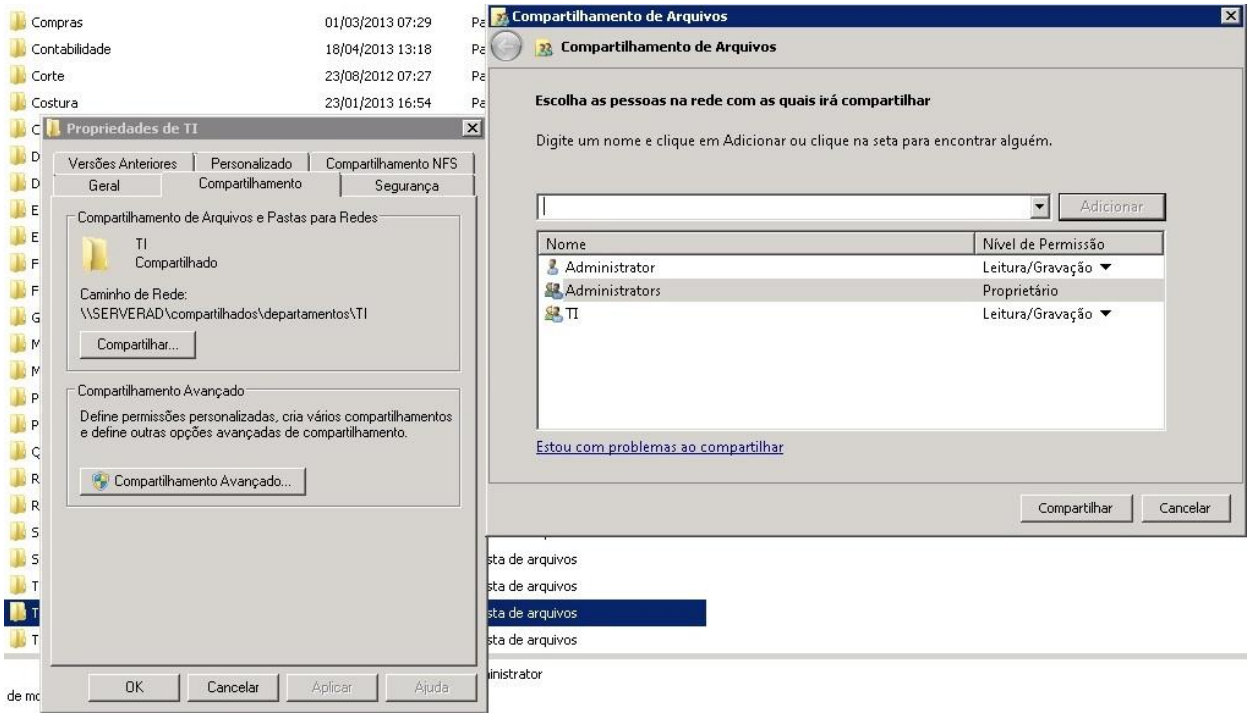

Figura 15 - Compartilhamento de pastas

Para acessar esta configuração, basta clicar com o botão direito sobre a pasta, e selecionar propriedades. Depois ir na guia Compartilhamento e clicar no botão compartilhar. Na tela exibida, basta selecionar o usuário ou grupo e informar se ele possui acesso de “Leitura/Gravação” ou “Somente leitura”.

Todas as configurações feitas em uma pasta se aplicam aos objetos e pastas que estiverem em seu interior. Caso seja necessário alterar a configuração de uma sub pasta cuja pasta principal já foi configurada, basta ir até a sub pasta e seguir o mesmo procedimento utilizado acima.

4.4.1.6 Finalização do Active Directory

Com as configurações aplicadas acima, já é possível ter um bom controle sobre a estrutura de rede. Os usuários e grupos gerenciam todos os colaboradores, e a partir deles é possível controlar os acessos, permitindo ou negando o acesso a determinadas pastas ou arquivos na rede. Nestes casos, é muito importante sempre manter os acessos e permissões atualizados, para que as informações estejam sempre disponíveis para os usuários.

Com a configuração de DHCP, reservando IP a todas as máquinas, você consegue controlar os endereços, para que na hora de configurar as permissões no firewall, seja possível aplicar as permissões corretas para cada estação ou usuário.

Existem diversas outras configurações que podem ser feitas com o uso de AD, que permitem diversos controles. Estas configurações não serão apresentadas neste trabalho, já que a finalidade do mesmo e permitir uma configuração básica e simples de proteção as informações disponibilizadas em rede.

4.4.2 FIREWALL

Segundo Morimotto, a função básica de um firewall em um servidor é bloquear o acesso a portas que não estão em uso, evitando assim a exposição de serviços vulneráveis, ou que não devem receber conexões por parte da internet.

Alem desta função, um firewall pode ser responsável por vários outros serviços, como roteamento do sinal de internet, controle de acesso e banda, entre outros, dependendo da configuração do mesmo.

Em resumo, o firewall trabalha como um fiscal, analisando todos os pacotes que chegam por suas interfaces e decidindo se podem ou não seguir para o seu destino. Ele pode analisar tanto o trafego que sai da rede interna para a externa quanto o tráfego que vem da internet com destino a rede interna.

No caso de implantação de um controle de acesso simples, como o caso em estudo, é necessário um firewall capaz de fazer redirecionar os serviços externos para os servidores internos através de redirecionamento de portas. Este firewall também deve controlar a saída de dados para internet, controlando o conteúdo acessado pelos usuários internos.

Para isso será utilizado o firewall IPcop, que será melhor explicado na próxima sessão, com detalhes de instalação, configuração e funcionamento. Para que ele controle efetivamente a rede da maneira necessária, ele será colocado na entrada do sinal externo, tornando-se a porta de entrada e saída da rede interna. A figura 16 ilustra a localização do firewall na rede, sendo esta a configuração padrão para aplicação de servidores firewall.

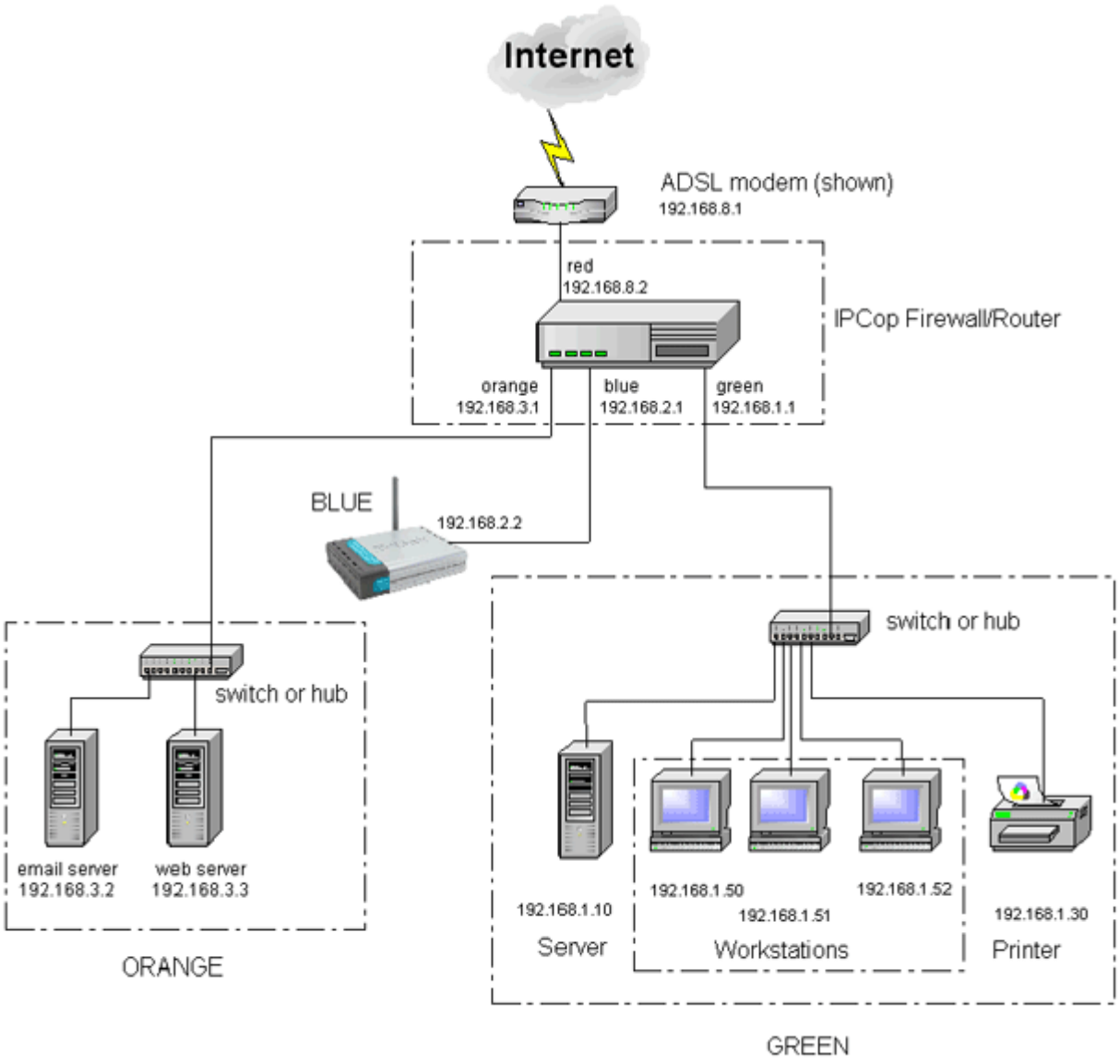

Figura 16 - Localização padrão de um Firewall em uma rede
Fonte: (http://www.manolo-lopez.com/wordpress/wp-content/uploads/2012/02/ipcop_form_web1.gif).

4.4.2.1 Ipcop Firewall

O Ipcop Firewall é uma distribuição do sistema operacional Linux, distribuído sob a licença GNU (general public license).

O Ipcop foi iniciado em outubro de 2001, através de um grupo de pessoas se desligou do projeto Smoothwall. Na época, havia uma proposta de que o Smoothwall seria cobrado. Este grupo, não concordando com a ideia, se desligaram do projeto.

Como eles possuíam os códigos fontes, eles os recodificaram e lançaram novamente sob o nome de IPCOP. Este mesmo grupo estipulou as seguintes metas:

- Fornecer uma distribuição de Firewall estável.
- Fornecer uma distribuição de Firewall seguro.
- Fornecer uma distribuição de firewall altamente configurável.
- Fornecer uma distribuição de Firewall que seja software livre.
- Fornecer uma distribuição de Firewall que seja fácil configuração.
- Fornecer suporte confiável.
- Fornecer um ambiente agradável para o usuário discutir e ter ajuda.
- Fornecer Upgrades/patches estáveis, assegurando fácil implementação.

4.4.2.2 Instalação Firewall

O Ipcop suporta até 4 interfaces de rede diferentes, cada uma com uma finalidade, e classifica cada uma delas com uma cor:

- Green – Rede Interna
- Red – Rede externa ou internet
- Orange – DMZ
- Blue – Conexão Access point

O Ipcop pode ser instalado de diversas formas. No caso, será usado a mídia gravada em CD-rom. O arquivo de instalação pode ser encontrado no endereço http://www.ipcop.org/download.php.

4.4.2.3 Configuração do Ipcop Firewall

Abaixo temos um passo a passo configuração de um firewall ipcop:

Após concluir a instalação e conectar-se via web ao firewall, é apresentada a tela mostrada na figura 17.

Figura 17 - Tela inicial do Ipcop

Nela podemos ver a página inicial do Ipcop. Para se conectar basta clicar em conectar deve-se usar o usuário admin e a senha cadastrada durante a instalação.

Conforme foi mostrado anteriormente, o ipcop já é um firewall nativo, e por isso já possui algumas funcionalidade básicas. Porem, para um melhor aproveitamento e atendendo as necessidades do projeto, foram instalados dois addonns.

As funcionalidades e recursos são exibidos divididos em abas na parte superior da janela. Ao todo, temos 7 categorias principais: Sistema, Situação, Rede, Serviços, Firewall, VPNs, Logs. Abaixo temos uma explicação mais detalhada de cada menu.

4.4.2.3.1 Menu Sistema

Composto pelas seguintes opções mostradas na figura 18.

Figura 18 - Menu Sistema

- A opção 1 é somente a pagina inicial do Ipcop.
- A opção 2 é onde se pode verificar se há atualizações para o sistema. Quando você instala o sistema, na tela inicial é apresentada uma mensagem dizendo que o sistema necessita de atualização, conforme mostra a figura 6. Neste caso basta acessar este menu e fazer as atualizações.
- A opção 3 é usada para alterar a senha do administrador.
- A opção 4 é usada para habilitar o acesso SSH. (citar que já foi visto na instalação).
- A opção 5 permite a alteração do idioma usado na interface web. No nosso caso usaremos a opção “Brasileiro”.
- A opção 6 permite a realização de cópias de backup.
- A opção 7 permite configurar o desligamento ou reinicialização automática do firewall.
- A opção 8 apresenta as pessoas que fazem parte do grupo ipcop, responsáveis por mante-lo ativo.

4.4.2.3.2 Menu Situação

No menu situação temos um resumo da situação do firewall, conforme mostrado na figura 19.

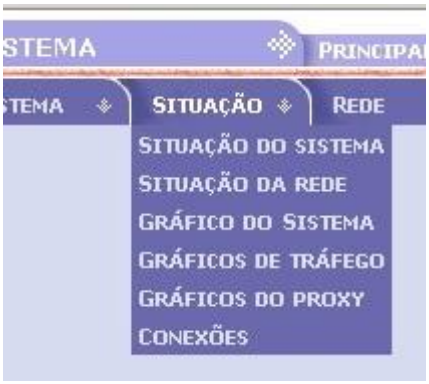

Figura 19 - Menu Situação

- A opção 1 exibe os serviços instalados no sistema e quais estão parados ou ativos.
- A opção 2 apresenta as interfaces de rede do sistema, com os endereços ip, mac e tabela de roteamento.
- A opção 3 apresenta de maneira gráfica a utilização da memória, HD, CPU e Swap. O padrão mostra as ultimas 24 horas de utilização, mas clicando em cima de uma das opções, são exibidos os gráficos desta para o dia, mês e ano.
- A opção 4 exibe a situação do trafego nas interfaces, com as mesmas opções de data do menu anterior.
- A opção 5 exibe um gráfico com as resoluções do servidor de proxy.
- A opção 6 exibe as conexões entre o sistema e a rede externa e interna.

4.4.2.3.3 Menu Rede

O menu Rede possui quatro opções: Discagem, Enviar, Modem, Apelidos. Esta opção deve ser configurada quando se usa internet via modem.

4.4.2.3.4 Menu Serviços

Neste menu se encontram as principais configurações a serem feitas no firewall. A figura 20 mostra este menu com as suas opções, que serão explicadas em detalhes logo abaixo.

Figura 20 - Menu Serviços

4.4.2.3.4.1 Proxy Avançado

Esta opção está disponível porque o addon advproxy foi instalo. Este servidor Proxy funciona da seguinte maneira. Quando um usuário da rede interna faz uma requisição de navegação no browser, esta solicitação é encaminhada ao servidor Proxy. Ele navega até o endereço, armazena o cachê e repassa as informações para os usuário. Esta informação fica armazenada por determinado tempo no Proxy, e se outro usuário procurar a mesma informação, ela é repassada sem a necessidade de uma nova busca na internet. Com isso, há uma grande diminuição no trafego entre a rede interna e externa.

A configuração do Proxy avançado possui as seguintes etapas.

Configurações comuns: A opção “Habilitação ligada Green” diz que a rede conectada a interface Green pode navegar através do firewall. A porta Proxy vem habilitada por default na 800. A opção “Transparência ligada Green” deve ser habilitada para não haja necessidade de configurar o Proxy manualmente nos computadores conectados. Em hostname visível, coloca- se o nome do servidor Proxy que será exibido. Na opção “E-mail do administrador de cachê” configura- se o email da pessoa que administra o servidor. Em “Linguagem das mensagens de erro” e “Desingn das mensagens de erro”, seleciona-se a linguagem e o modelo das

mensagens a serem exibidas aos usuários em caso de erros. A Figura 21 mostra estas configurações.

Figura 21 - Web proxy avançado

As opções da sessão Proxy principal deve ser configurada caso haja um Proxy alem deste na rede. Caso não tenha, deve-se deixar esta opção em branco, conforme mostra a Figura 22.

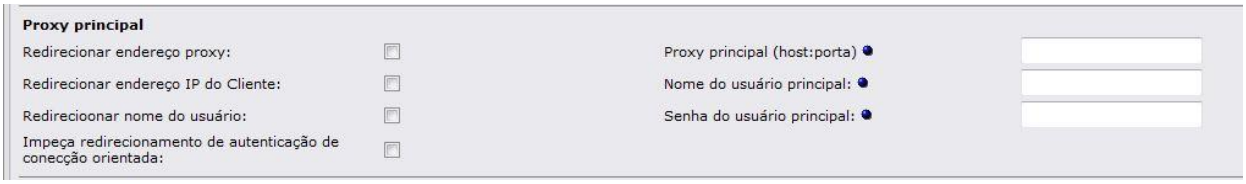

Figura 22 - Proxy principal

Nas configurações de log, deve-se habilitar as 3 opções, para que o sistema gere logs da navegação com a internet. A Figura 23 mostra estas opções.

Figura 23 - Log

Conforme citado anteriormente, o Proxy funciona armazendo paginas em cachê e as repassando aos usuários. Nesta sessão são configuradas as principais opções do gerenciamento do cachê. Abaixo temos as opções com as devidas explicações da sua funcionalidade:

Tamanho da memória em (NB): Define a quantidade de memória RAM que o servidor usa para fazer cachê de objetos. Ele não deve exceder 50% da memória RAM instalada.

Tamanho do cachê em (MB): É o espaço do disco que será usado para fazer cachê. Ele não deve exceder 20% do total da unidade.

Tamanho mínimo do objeto em (KB): è o tamanho mínimo dos objetos armazenados em cachê. O valor padrão é zero, que significa que não existe tamanho mínimo definido.

Tamanho Maximo do objeto em (KB): è o tamanho Maximo dos objetos que serão armazenados em cachê. O valor padrão é 4096 KB.

Não faça cachê desses domínios (um por linha): Especificar domínios para que o servidor não faça cachê.

Substituição de regra de memória: especifica qual regra será usada na substituição de objetos armazenados na memória. O valor padrão é LRU.

Substituição de regra de cachê: especifica a regra usada na substituição de objetos armazenados em cachê. O padrão desta função também é LRU.

A Figura 24 mostra as opções descritas acima.

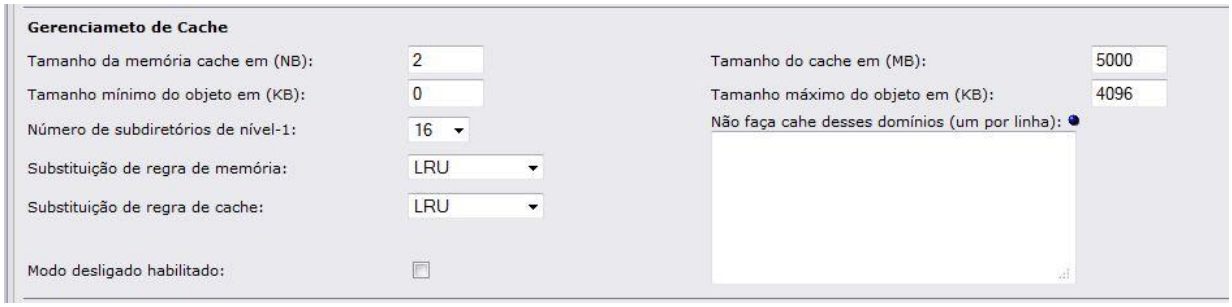

Figura 24 - Gerenciamento de cache

A sessão de portas de destino enumera as portas padrões permitidas, conforme mostra a Figura 25:

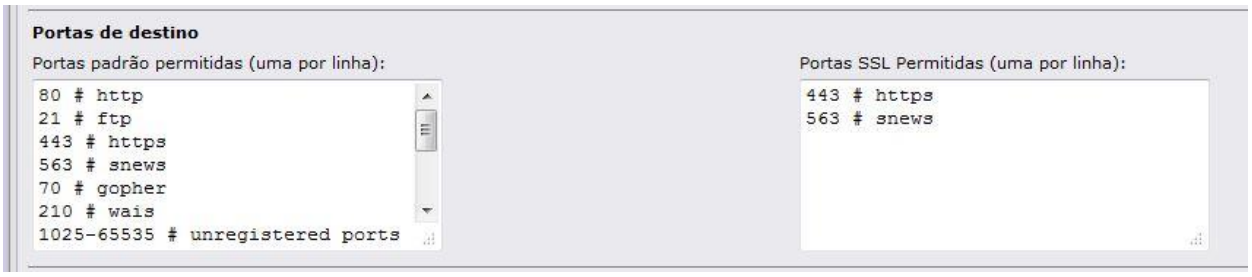

Figura 25 - Portas de destino

A sessão de controle de acesso baseado na rede permite configurar o acesso dos usuários da rede interna ao servidor Proxy.

Em subnets permitidas deve-se citar as redes com permissão para navegar através do Proxy. Nela deve-se configurar a sub rede conectada a interface Green.

Em endereços IP sem restrição e endereços MAC sem restrição deve-se inserir os computadores que não terão restrição no acesso ao Proxy. O ideal é colocar o MAC e o IP para maior segurança, mas elas funcionam de maneira independente. Em endereços IP banidos e Endereços MAC banidos insere-se os ips banidos de navegar pelo Proxy.

A Figura 26 mostra estas opções.

Figura 26 - Controle de acesso baseado na rede

Na sessão de restrição de tempo, define-se quais dias e horário o acesso ao firewall e permitido.

Em limites de transferência define-se qual o tamanho maximo de arquivo que pode ser feito download e upload. Já em Limitação para download é especificado a velocidade de download e upload e o tipo de arquivo que pode ser baixado.

A Figura 27 mostra estas configurações.

Figura 27 - Restrições de tempo

A sessão Filtro tipo MIME, mostrada na Figura 28, serve para bloquear o acesso a determinados tipos de arquivo. Para utilizar esta função, basta clicar em habilitado e depois citar qual o tipo se deseja bloquear (exemplo: para bloquear arquivos com a extensão PDF, digita-se .pdf).

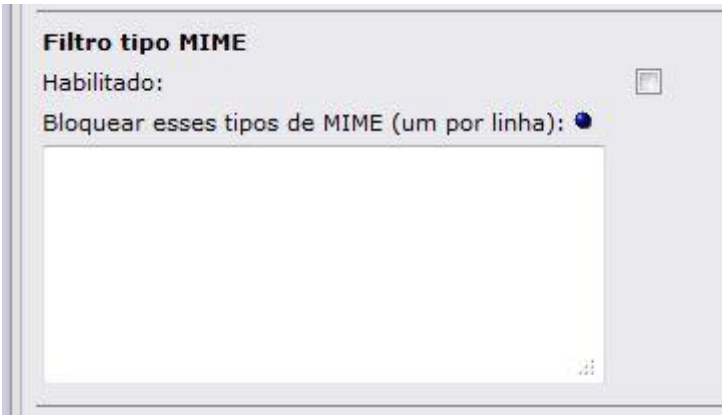

Figura 28 - Filtro tipo MIME

A sessão privacidade tem por finalidade manter o usuário anônimo quando navegar pela internet. Como mostrado na Figura 29, ela possui dois campos. O primeiro (falso Useragent para sistes externos) serve para alterar o cabeçalho usado na navegação. Por exemplo, se colocarmos a string de identificação do navegador Mozilla Firefox, independente do navegador utilizado, os sites externos sempre interpretarão como uma navegação com origem no Mozilla. Já o segundo campo serve para manter o usuário anônimo. Basta inserir uma URL falsa (exemplo: “Http://xxxxxxxxxxxxxxxxxx” para que, quando for navegar, esta URL seja enviada para o site de destino e não a URL de origem. Com esta duas opções o usuário da rede interna consegue se manter anônimo enquanto navega pela internet.

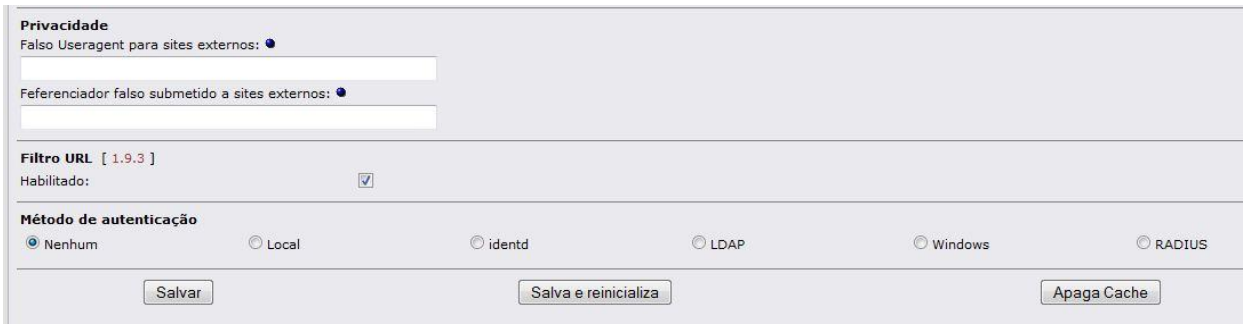

Figura 29 - Privacidade

A Figura 38 também mostra mais duas opções. A opção Filtro URL estará disponível quando o addon ipcop-urlfilter estiver instalado. Basta deixá-la habilitada para que se possa utilizar o urlfilter. A opção “Método de configuração” não deve ser configurada, já que estamos trabalhando com proxy transparente.

Na Figura 30 vemos a ultima parte da configuração do Proxy. Ela serve para bloquear determinados navegadores de passar através do firewall. Basta habilitar e marcar quais navegadores serão permitidos.

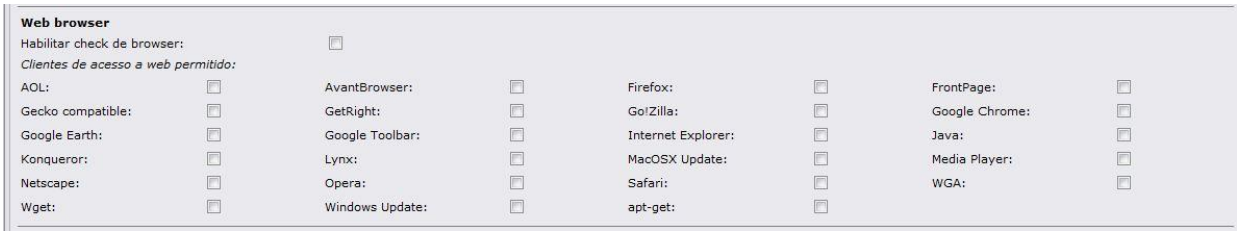

Figura 30 - Web browser

4.4.2.3.4.2 URL filter

O filtro URL ficará disponível após a instalação do addon ipcop-urlfilter. A função dele é limitar e controlar o acesso à internet. Através dele é possível bloquear domínios, palavras chave, URLs e arquivos indesejáveis. Também é possível determinar quais hots podem ou não acessar determinados destinos.

A configuração do urlfilter também é feita por etapas, conforme mostrado abaixo.

A figura 31 mostra a sessão “bloquear categorias”. Serve para bloquear categorias completas. Para bloquear basta marcar a opção. Quando o addon é instalado, algumas categorias já vem instaladas, mas é possível instalar novas categorias que estão disponíveis na internet ou criar categorias personalizadas, conforme será mostrado na sessão “manutenção de filtro URL”.

Figura 31 - Bloquear categorias

A figura 32 mostra a opção “Blacklist personalizada”. Nela temos dois campos. O primeiro permite bloquear domínios completos. Para bloquear o acesso ao site Uol basta digitar neste campo o domínio uol.com.br . Já a opção URLs bloqueadas serve para bloquear URLs especificas de um domínio, como por exemplo, esporte.uol.com.br. Em ambos os campos deve-se digitar um domínio ou URL por linha.

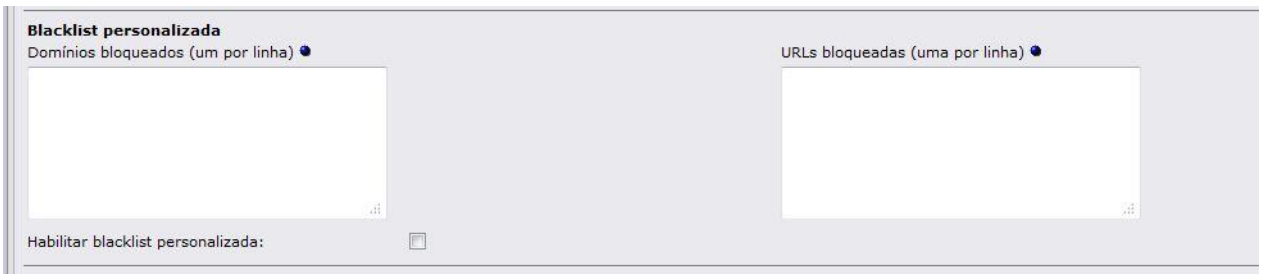

Figura 32 - Blacklist personalizada

A opção whitelist personalizada mostrada na figura 33 possui a função contraria a mostrada acima. Nela é possível determinar domínios e URLs permitidas para

navegação. Da mesma maneira que na sessão Blacklist, basta digitar o domínio ou a URL permitida, sempre sendo um por linha.

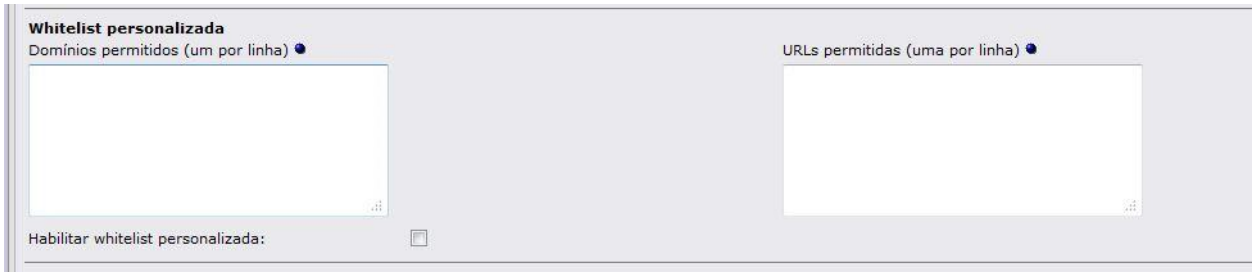

Figura 33 - Whitelist personalizada

Há ainda uma opção para criar uma lista personalizada de expressões, conforme mostrada na figura 34. Está opção permite o bloqueio de palavras chave. Por exemplo, se digitarmos a palavra filme nesta opção, todos os sites que possuem esta expressão serão bloqueados automaticamente, assim como as pesquisas contendo esta palavra em sites de busca.

Figura 34 - Lista personalizada de expressões

A opção “Bloqueamento por extensão de arquivo” mostrado na figura 35 serve para bloquear determinados tipos de arquivos. Basta selecionar a opção correspondente para o bloqueio. Já a opção redirecionar arquivo local permite redirecionar os downloads para a rede local, diminuindo o trafego da rede.

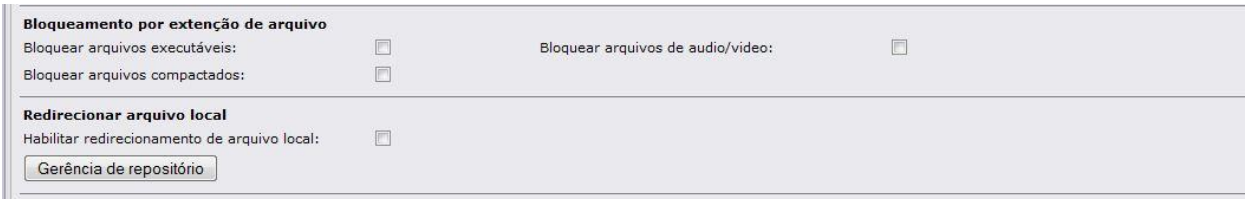

Figura 35 - Bloqueamento por extensões de arquivo

A opção “Controle de acesso a rede” mostrada na figura 36 possibilita definir IPs para serem bloqueados ou liberados no acesso a internet. Em “Endereços IP não filtrados” define-se quais IPs não serão considerados nas regras do URL filtro.

Independente da regra aplicada, os IPs indicados aqui terão a navegação liberada. Já em “Endereços IPs descartados” define-se quais IPs não terão nenhum acesso a internet, independente das regras aplicadas.

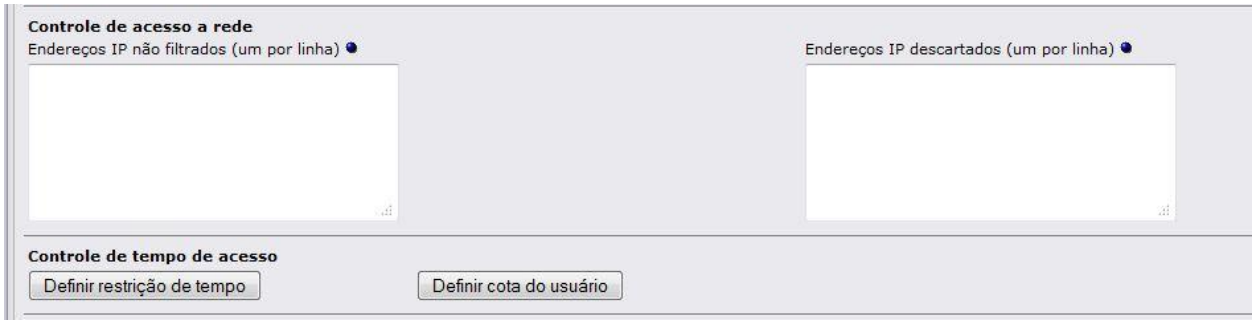

Figura 36 - Controle de acesso à rede

O botão “definir restrição de tempo” permite um controle mais especifico sobre as regras do filtro. Através dele se tem acesso a tela mostrada na figura 37. Nela pode-se criar regras especificas para bloquear ou liberar determinados hots ao acesso a categorias diversas, sendo que também é possível definir um horário especifico para esse bloqueio ou acesso.

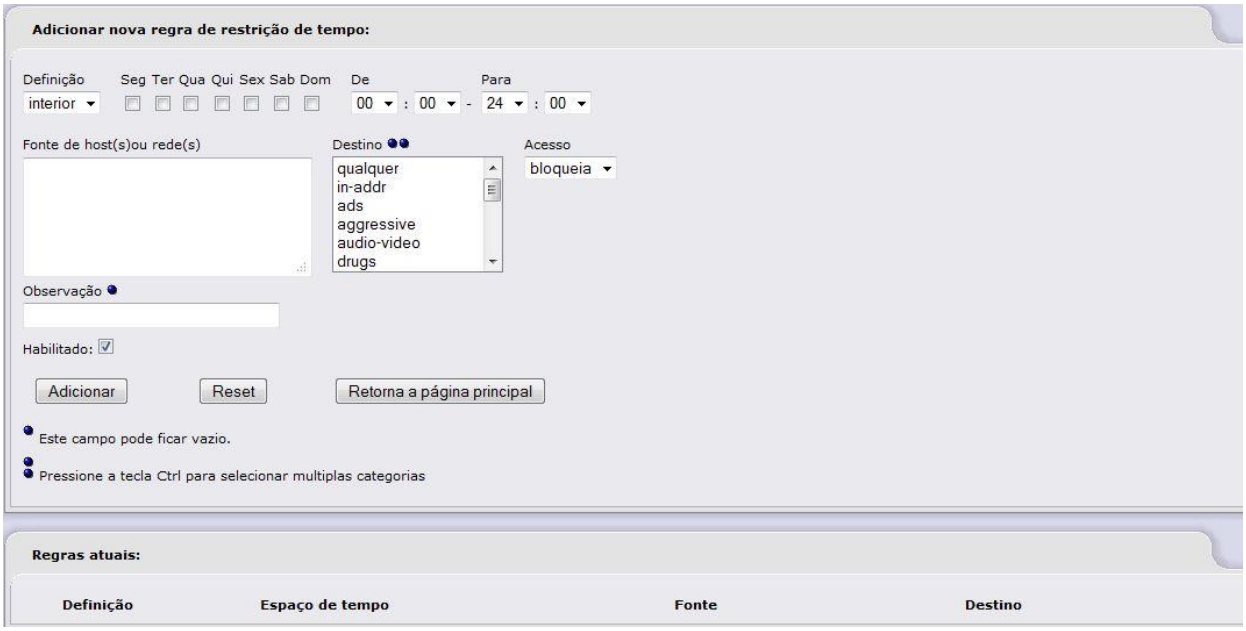

Figura 37- Restrição de tempo

Na parte de baixo desta tela tem-se as regras existentes, sendo possível habilitar, desabilitar, editar ou excluir qualquer uma delas.

A figura 38 mostra como cadastrar cotas de uso por usuário, definindo um limite

de tempo para o uso da internet por IP.

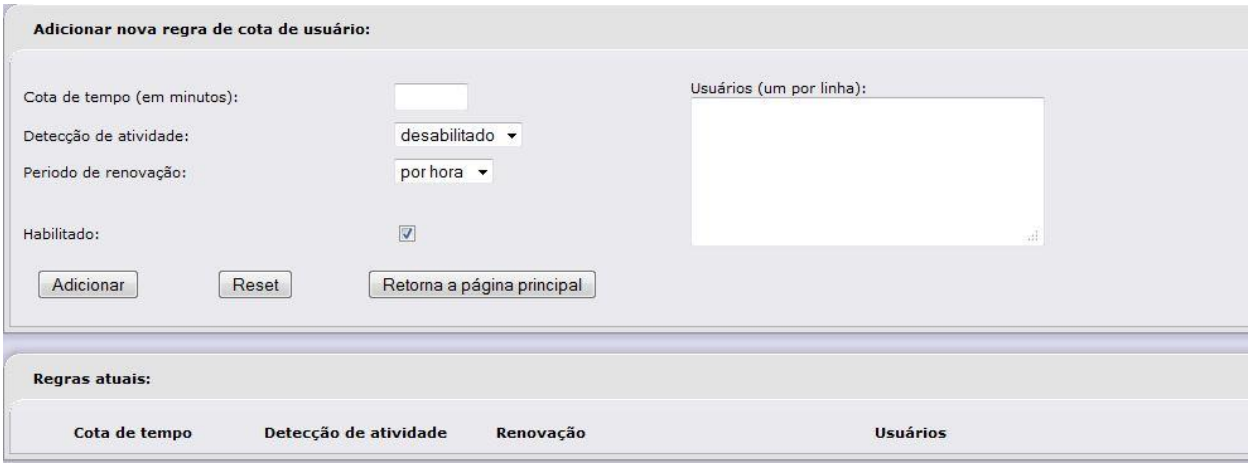

Figura 38 - Cota de usuário

A próxima sessão, mostrada na figura 39, denominada “configurações de páginas bloqueadas” é onde se configuram as mensagens que irão aparecer para os usuários quando estes tentarem acessar uma página bloqueada por qualquer regra.

Figura 39 - Configuração de página bloqueada

Ela possui as seguintes opções:

- Mostrar categoria de página bloqueada: exibe na mensagem a categoria da pagina que foi bloqueada. Pode ser o nome de uma blacklist ou uma categoria personalizada.
- Mostrar URL da página bloqueada: Exibe a URL que foi bloqueada.
- Mostrar IP da página bloqueada: mostra o IP do usuário que tentou acessar a página bloqueada (testar esta configuração para ver se é o IP da página ou do usuário).
- Use DNS error para bloquear URLs: Quando habilitada, em vez de mostar a mensagem padrão de bloqueio exibe uma mensagem de página não encontrada.
- Habilitar Imagem de Background: Se habilitada, exibe uma imagem como

plano de fundo da página de bloqueio. Para selecionar a imagem, basta pressionar o botão “selecionar imagem” e depois fazer o upload da mesma.

- Redirecionar para este URL: Redireciona as páginas bloqueadas para uma determinada URL.
- Linhas de Mensagem 1,2 e 3: Aqui devem ser digitadas as mensagens que serão exibidas na página de bloqueio.

A figura 40 mostra uma página padrão de bloqueio, com mensagem e imagem habilitadas.

Figura 40 - Página bloqueada

A sessão “configurações avançadas”, mostrada na figura 41, finaliza as regras de ativação do filtro URL.

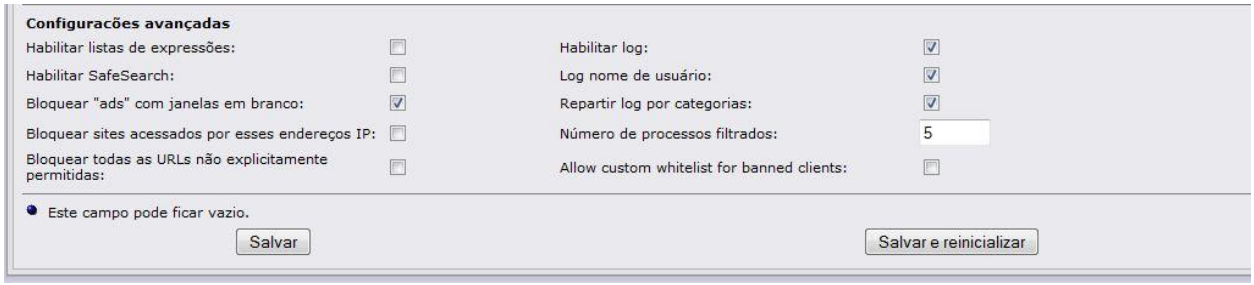

Figura 41 - Configurações avançadas

Ela possui as seguintes opções:

- Habilitar lista de expressões: Habilita o uso das listas de expressões

bloqueadas.

- Habilitar SafeSearch: verificação de palavras-chave, frases, etc.
- Bloquear “ads” com janelas em branco: bloqueia anúncios e banners indesejados.
- Bloquear sites acessados por endereços IPs: Bloqueia os sites que forem acessados pelo endereço IP. Nestes casos, o site estará liberado caso seja acessado pela URL.
- Bloquear todas as URLs não explicitamente permitidas: Caso habilitada, apenas as URLs que estiverem na Whitelist personalizada poderão ser acessadas.
- Habilitar Log: Habilita a geração de logs do filtro URL.
- Log nome do usuário: grava junto ao log o nome do usuário.
- Repartir Log por categorias.
- Numero de processos filtrados: Quantidade de processos filtrados que estão ativos.
- Allow custon whitelist for banned clients: Quando um cliente é bloqueado, todas as solicitações são negadas. Ao habilitar esta opção, as URLs que estiverem na whitelis serão permitidas a esses usuários.

Alem destas opções, a figura 41 mostra os botões “Salvar” e “salvar e reinicializar” que servem para salvar as configurações e salvar e reiniciar o serviço, respectivamente. É necessário reiniciar o serviço para que as configurações sejam ativadas.

As próximas telas se referem a manutenção das Blacklist.

A figura 42 mostra estas opções. As quais será explicadas a seguir:

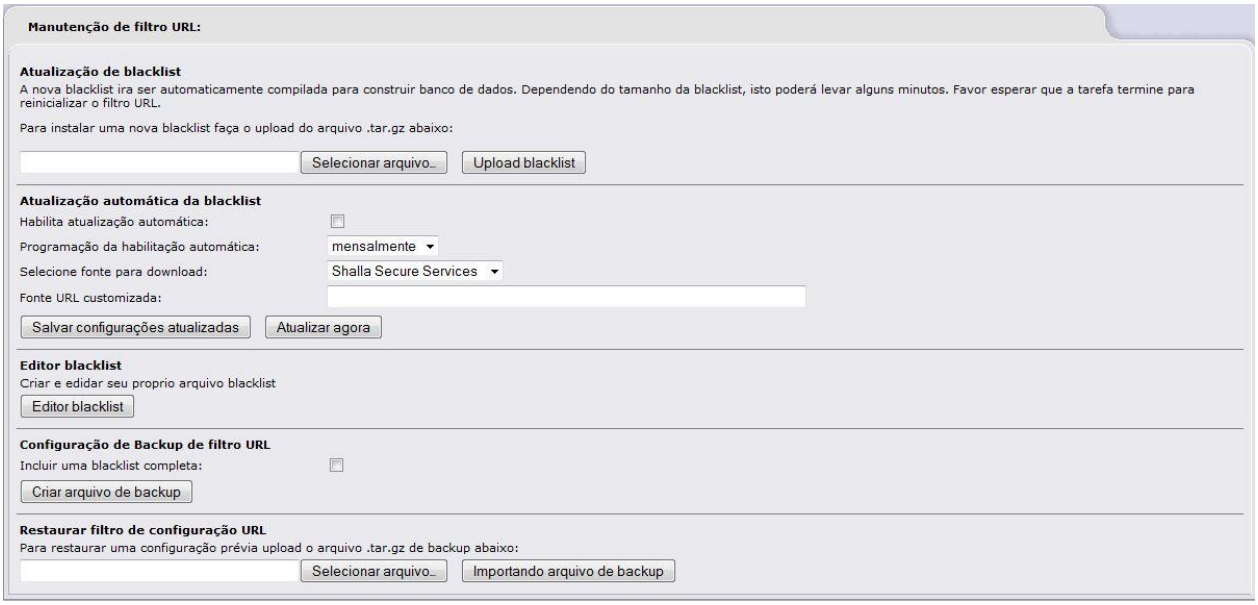

Figura 42- Manutenção de filtro URL

A opção atualização de blacklist serve para instalar blacklists prontas. Esta blacklist estão disponíveis em diversos sites de segurança. Para que seja feita uma atualização automática destas basta selecionar as opções da próxima sessão e salvar.

O botão “Editor blacklist” da acesso a tela mostrada nas figuras 43 e 44. Esta tela tem a função de criar ou modificar as blacklist instaladas.

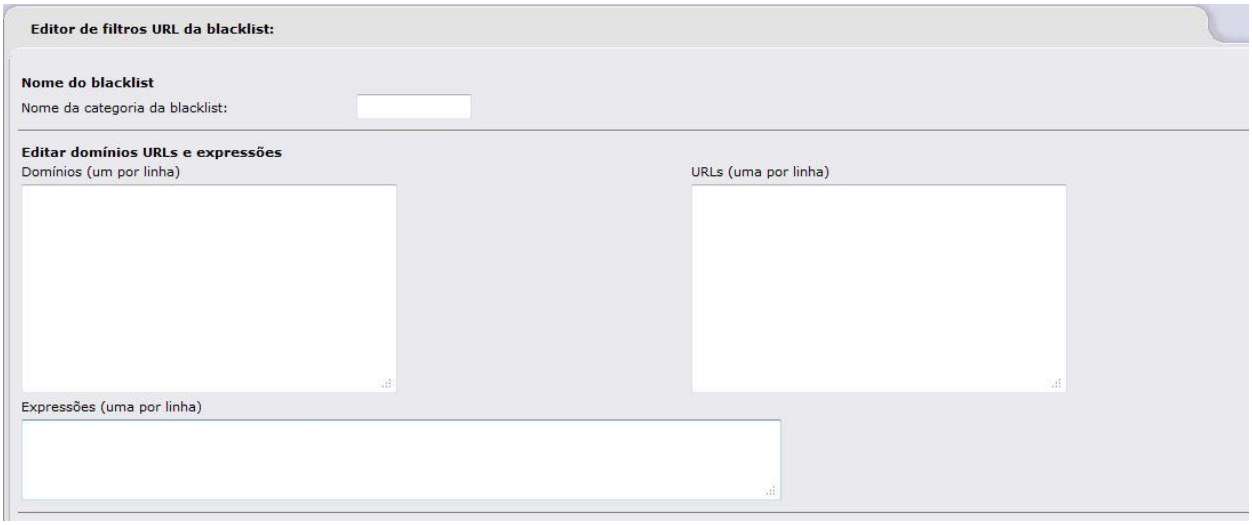

Figura 43 - Editor de blacklist - 1

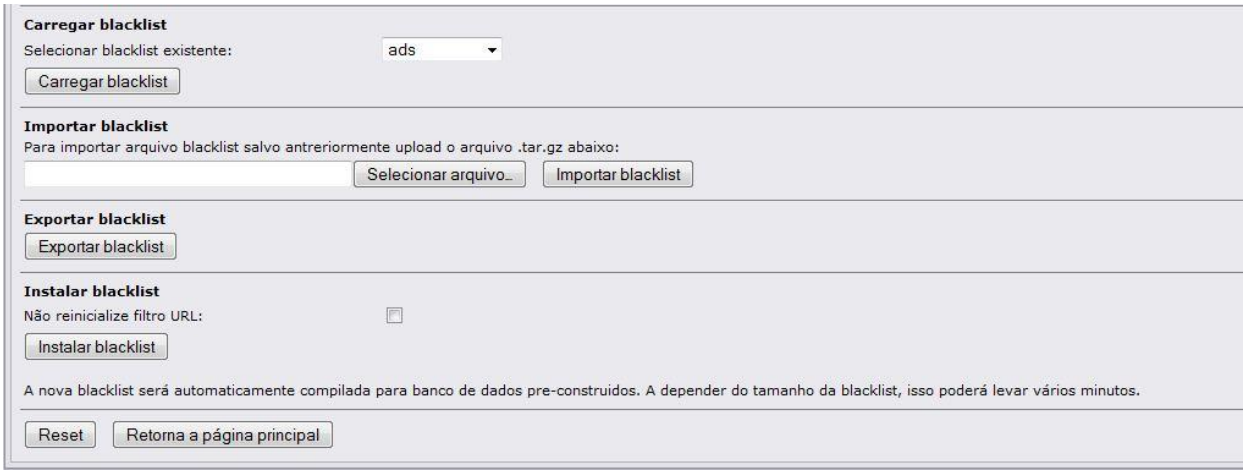

Figura 44 - Editor de blacklist - 2

Para modificar uma blacklist basta carregá-la através do botão “Carregar blacklist” e alterá-la. Após feitas as modificações, basta clicar no botãoo “instalar blacklist” para que ela seja aplicada ao filtro URL.

Para criar uma nova blacklist basta digitar um nome para a mesma, configurar os domínios, URLs e expressões e depois clicar no botão “instalar blacklist”.

4.4.2.3.4.3 Servidor DHCP

O servidor de DHCP serve para fornecer endereços IPs à rede interna. Como no nosso caso o servidor com Windows Server 2008 possui a função de servidor DHCP, deixaremos esta função desabilitada.

4.4.2.3.4.4 DNS dinâmico

A função do DNS dinâmico é fornecer aos servidores de DNS qual o IP utilizado para acessar o Ipcop. Como no caso, o Ipcop está na entrada da rede interna, porém sem o IP real configurado em sua interface red, não será utilizada nenhuma opção desta sessão.

4.4.2.3.4.5 Editar host

A função “adicionar um host" serve para nomear os hosts da rede interna. Basta colocar o IP, Nome, Dominio e clicar no botão “Adicionar”. A figura 45 mostra esta opção.

Figura 45 - Adicionar um host

4.4.2.3.4.6 Servidor de horas

O servidor de horário serve para sincronizar todos os hosts da re interna através do firewall. As opções são mostradas na figura 46. A partir desta tela é possível selecionar onde será sincronizada a hora, e depois basta habilitar a opção “Fornecer hora para a rede local” e selecionar a maneira que será feita a atualização, sendo que ela pode ser automática ou manual.

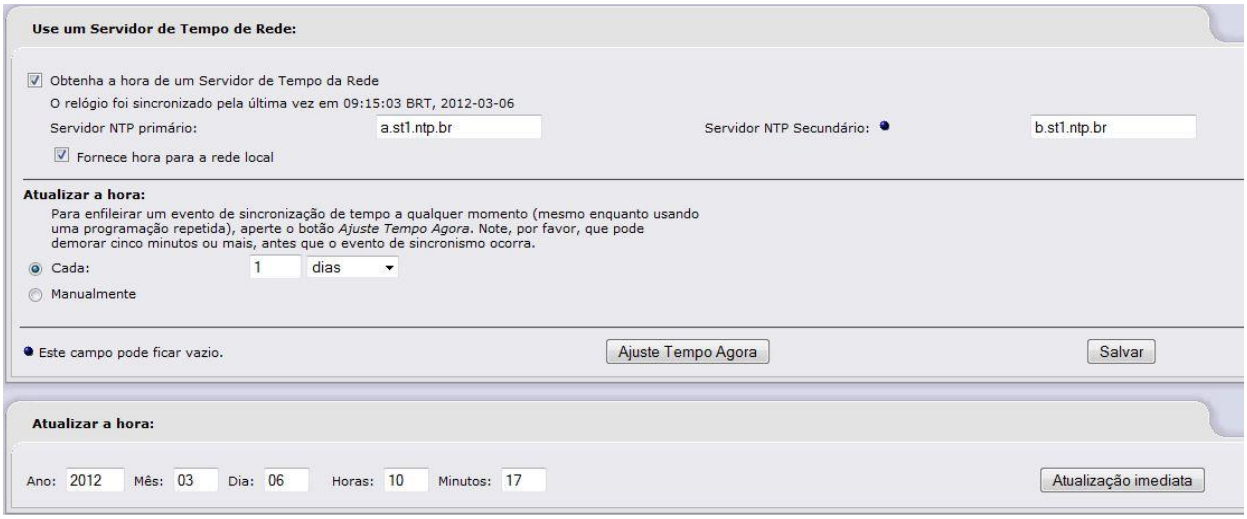

Figura 46 - Servidor de horário

4.4.2.3.4.7 Controle de tráfego

A próxima opção dentro do menu serviços é a opção de Controle de tráfego, mostrada na figura 47. A partir dela é possível limitar a velocidade de download e upload. Além disso pode-se determinar prioridades para determinados serviços. Para isso basta selecionar a prioridade, digitar a porta e o protocolo usado e clicar em adicionar.

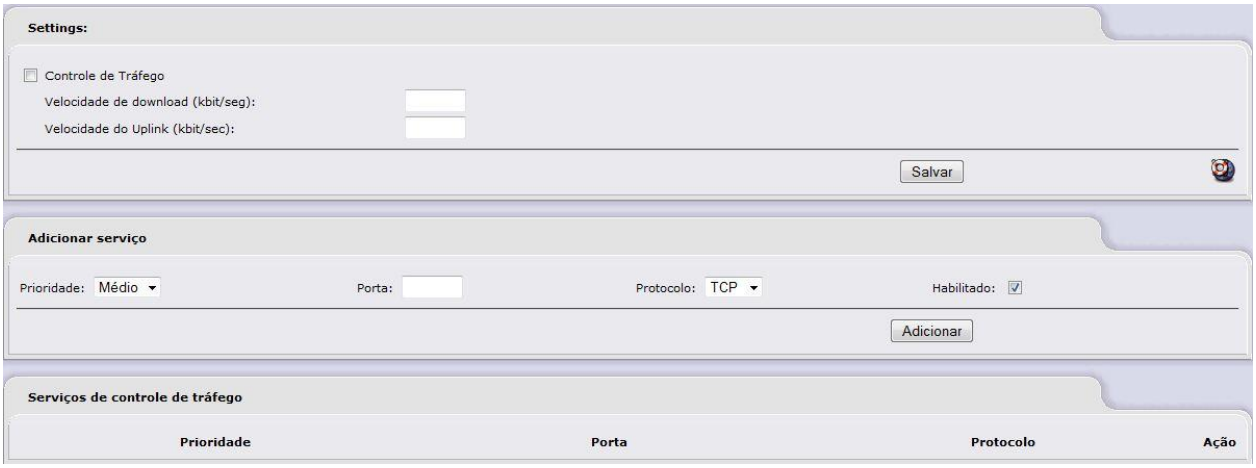

Figura 47 - Controle de tráfego

4.4.2.3.4.8 Detecção de intrusão

O ultimo serviço a ser configurado refere-se ao de “detecção de intrusão”. O Ipcop utiliza o Snort para fazer a análise dos pacotes recebidos pelo firewall e verificar se eles possuem códigos que podem ser maliciosos para a rede. Para utilizar esta opção deve-se fazer o cadastro no site www.snort.org e depois copiar o código gerado e cadastrar o snort, conforme mostra a figura 48.

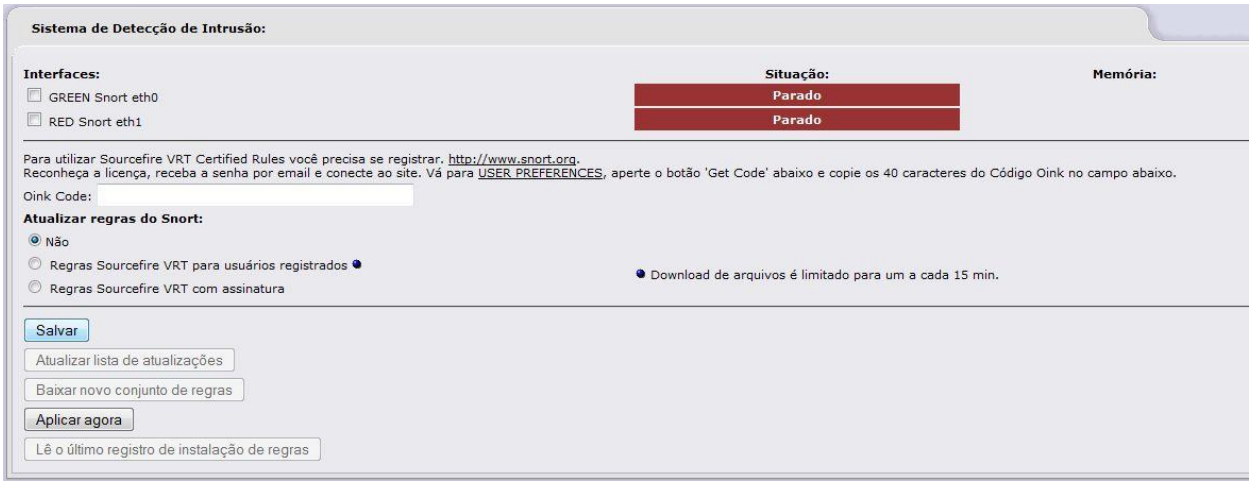

Figura 48 - Controle de intrusão

4.4.2.3.5 Menu firewall

O próximo menu , mostrado na figura 49, refere-se as configurações de firewall. A partir deste menu é possível fazer configurações de redirecionamento de portas, acessos externos e regras de iptables. Algumas destas opções só estarão disponíveis com a instalação de determinados addons.

Figura 49 - Menu Firewall

4.4.2.3.5.1 Forwarding de porta

A primeira opção é “Forwarding de Porta”. A sua função é criar os redirecionamentos de porta para que seja possível que serviços da rede interna possam ser acessados de fora. Sem esta configuração é impossível que usuários de fora da sua rede consigam acessar serviços disponíveis nos servidores internos. Para configurar, deve-se indicar a porta de origem, o IP do servidor no qual o serviço está disponível e a porta de destino. Depois é só marcar a opção habilitado e clicar em adicionar. Na parte de baixo da tela são mostrados as regras configuradas. O processo deve ser feito duas vezes, uma para o protocolo TCP e outra para o UDP. A figura 50 mostra a tela para estas configurações.

Figura 50 - Adicionar regra

4.4.2.3.5.2 Acesso externo

A próxima opção, denominada acesso externo, é um complemento da opção “forwarding de porta”. Ela faz a liberação da entrada do serviço para a rede interna. A figura 51 mostra as opções desta configuração. Após se configurar o redirecionamento das portas, deve-se liberar o acesso a este serviço a partir da rede externa. Para isto basta informar a porta de destino, habilitar a opção e clicar em adicionar. Da mesma maneira que na opção anterior, o processo deve ser repetido para os protocolos TCP e UDP.

Figura 51 - Acesso externo

4.4.2.3.5.3 Opções de Firewall

A tela de opções do firewall mostrada na figura 52 serve para bloquear as respostas ao comando ping nas interfaces red e Green do firewall. Basta selecionar a opção desejada e salvar.

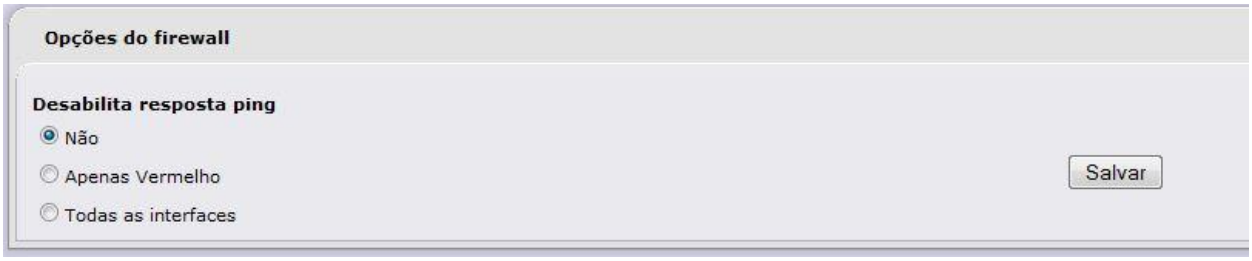

Figura 52 - Opções de Firewall

4.4.2.3.6 Menu Logs

Após configurar todas as opções do IPcop, devemos configurar os logs. A partir deles é possível verificar o que acontece e controlar o tráfego entre as interfaces.

A figura 53 mostra a tela de configuração dos logs. A primeira opção define a ordem na qual os logs serão exibidas, sendo que pode ser em ordem cronológica ou em ordem cronológica inversa. Além disso pode-se selecionar quantas linhas devem

ser exibidas na página. A segunda opção definem por quantos dias o firewall deve armazenar os dados de log e qual o nível a ser exibido. A terceira opção define o envio dos logs a um servidor remoto.

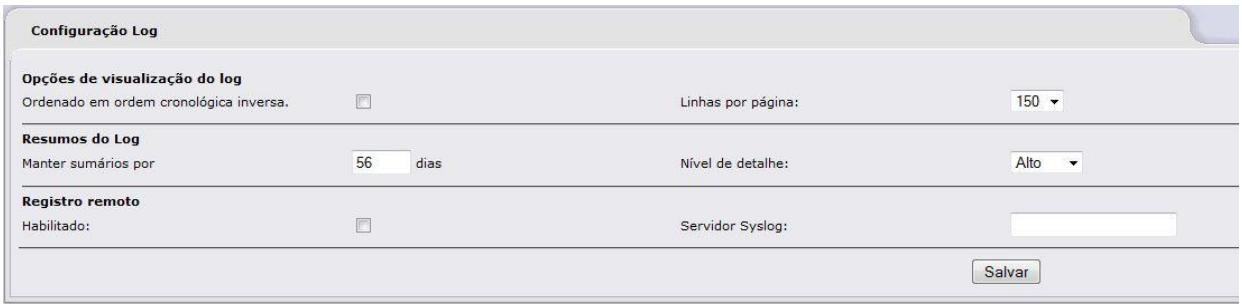

Figura 53 - Configurações de Log

A opção resumo de log mostra um resumo dos logs armazenados, conforme mostra a figura 54.

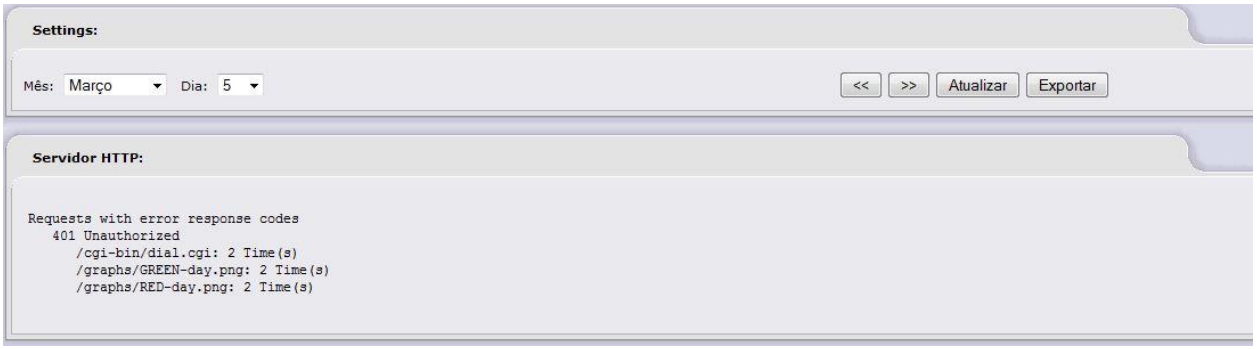

Figura 54 - Resumo do Log

A tela de logs de Proxy mostra o endereço interno da maquina e o website que ela acessou. A figura 55 mostra como são exibidos os logs de Proxy.

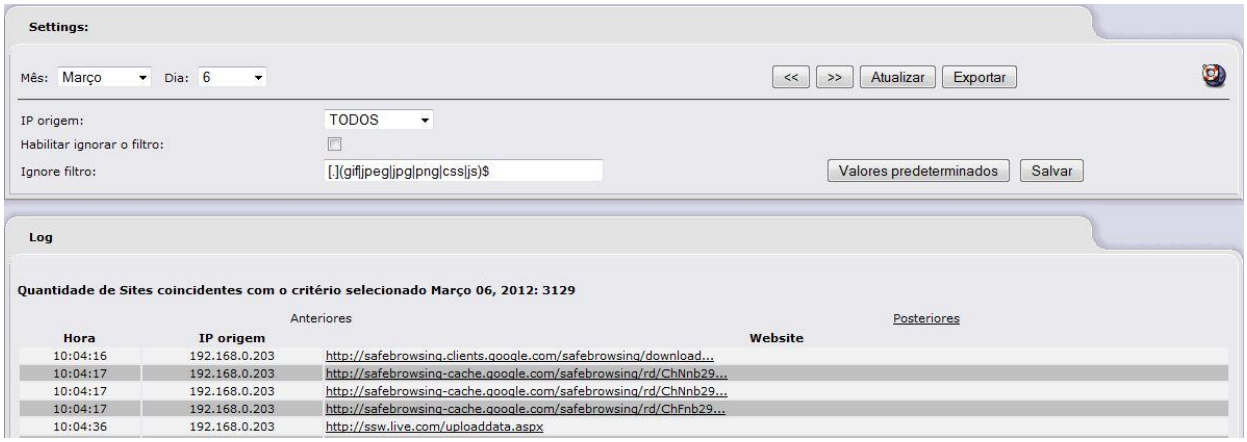

Figura 55 - Log de proxy

A figura 56 mostra a tela de logs do firewall. Ela detalha todo o trafego que passa pelo firewall. Conforme pode ser visto, ela mostra a hora, a política adotada, a interface, o protocolo, o Ip de origem, a porta de origem, o MAC de origem, o IP de destino e a porta de destino.

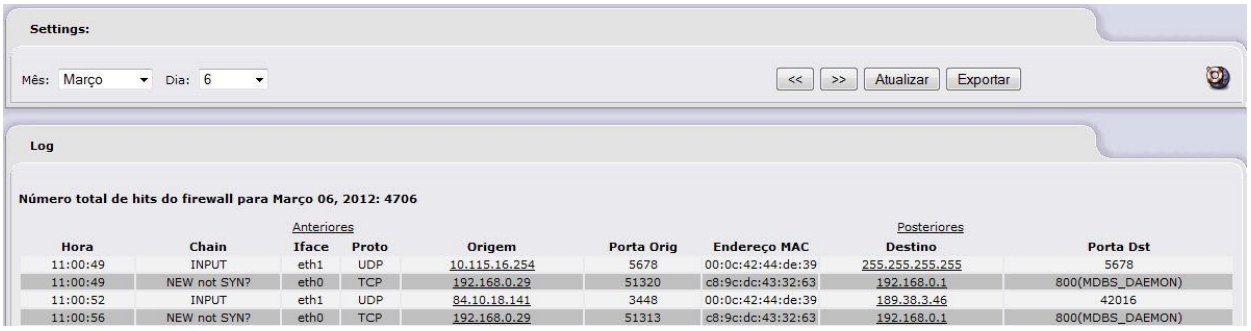

Figura 56 - Log de firewall

A sessão Log do filtro URL mostra os sites barrados pelo filtro URL. Ela mostra a hora que o usuário tentou acessar, a categoria que bloqueou o acesso, o IP da maquina e o endereço URL do site. A figura 57 mostra como estes logs são exibidos.

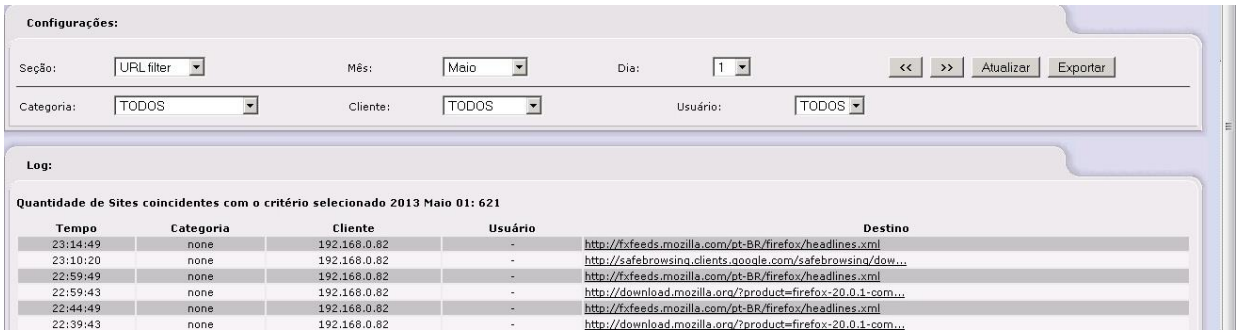

Figura 57 - Log de filtro URL

A figura 46 mostra os logs do sistema, como erros, alterações nos serviços e funcionalidades.

4.5 CENÁRIO ATUAL

Após aplicadas todas as configurações, a estrutura da rede foi documentada para possibilitar o controle e localização das maquinas e usuários. Todas as funcionalidades disponíveis foram mapeadas.

Em acordo com a diretoria e gerencia, foi elaborada a politica de segurança, e a

partir dela, a estrutura foi reconfigurada.

A figura 58 mostra um esboço do cenário atual da empresa, ressaltando a questão de padronização da nomenclatura e das configurações de rede, além de uma melhor descrição dos serviços do servidor.

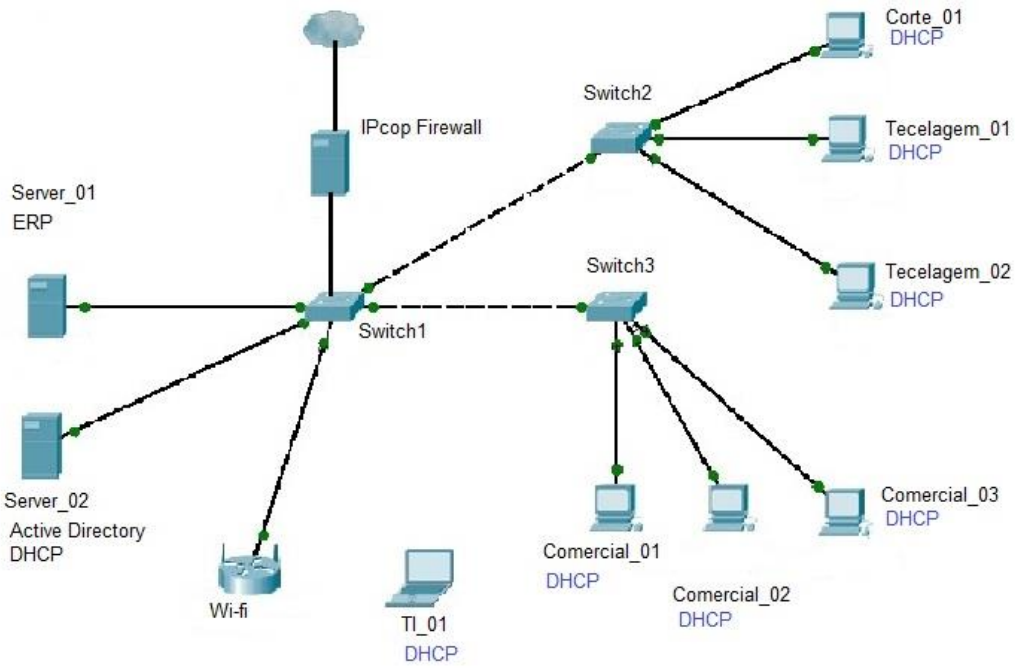

Figura 58 – Cenário Atual

5 CONCLUSÃO

Ao finalizar este trabalho, podemos concluir que com o constante aumento da informatização, cada vez mais os sistemas e redes devem estar seguros contra ataques. Diversas soluções foram e estão sendo desenvolvidas para aumentar a segurança das redes, porem, também o numero de ameaças cresce na mesma velocidade.

Para uma completa segurança de um sistema, é necessário que várias ferramentas e técnicas sejam empregadas em conjunto, cada uma voltada para a defesa de um tipo de ameaça.

Dentro do cenário empresarial estudado, foram implementadas ferramentas para controlar o acesso dos usuários à informações disponibilizadas na rede, sendo que cada usuário apenas acessa o que é necessário às suas tarefas. Também foi implementada uma ferramenta que controla o acesso dos usuários à rede externa, evitando assim conteúdos proibidos, prejudiciais ou simplesmente não necessários a realização das atividades. Com isso, diminui-se o tráfego da rede, e minimiza-se o risco de ataques vindos de fora, com o objetivo de extrair informações.

Estas ferramentas foram implementadas a partir de uma política de segurança, elaborada pela diretoria da empresa em conjunto com o administrador de rede, baseada nas necessidades da empresa e nas vulnerabilidades encontradas durante o levantamento da estrutura.

Além de empregar todas as ferramentas necessárias a proteção da rede e dos sistemas, é necessário ao administrador conhecer todos os detalhes da estrutura. Saber quais os serviços são usados pelos usuários, quais os pontos fortes da rede e quais as vulnerabilidades.

Além disso é importante manter o padrão entre os softwares utilizados, para que não se corra o risco de abrir portas desnecessárias a realização dos serviços.

Para finalizar, é importante citar que a segurança da informação não depende somente do administrador da rede ou da segurança dos softwares e equipamentos utilizados, mas também dos usuários que utilizam todos os serviços disponíveis. Portanto apenas com a colaboração de todas as esferas dentro do cenário industrial é possível estabelecer uma estrutura informatizada e com um bom nível de segurança.

6 REFERÊNCIAS

BARBOSA, A. N. **Um sistema para análise ativa de comportamento de Firewall**. 2006. 121f. Dissertação (Mestrado em Curso de Engenharia) - Escola Politécnica da Universidade de São Paulo, São Paulo, 2006.

COMITE GESTOR DE INTERNET NO BRASIL **Cartilha de segurança para Internet**. Versão 3.1. ed. São Paulo: Cert.br, 2006. 117p.

FONSECA, C. R. **Segurança de Redes com uso de um aplicativo firewall nativo do Linux**. 2006. 64f. Monografia (Bacharelado em Ciência da Computação) - Centro Universitário Barão de Mauá, Ribeirão Preto, 2006.

HOLME, D.; RUEST, D.; RUEST, N. **Kit de treinamento MCTS - Exame 70-640: Configuração do Windows Server 2008 Active Directory**. Reimpressão 2010. ed. Porto Alegre: Bookman, 2009. 992p.

JUNIOR, V. F. R. **Estudo e Implementação de Firewall em ambientes corporativos**. 2010. 98f. Monografia (Especialização em Segurança da Informação) - Faculdade de Tecnologia de João Pessoa - Fatec, João Pessoa, 2010.

LYRA, M. R. **Segurança e auditoria em Sistemas de Informações**. Rio de Janeiro: Ciência Moderna Ltda, 2008. 253p.

MATTHEWS, M. **Windows Server 2008: O guia do iniciante**. Rio de Janeiro: Ciência Moderna Ltda, 2008. 740p.

MENDES, D. **Redes de Computadores - Teoria e Prática**. São Paulo: Novatec, 2007. 384p.

MORIMOTO, C. E. **Redes: Guia prático**. 2ª reimpressão. ed. Porto Alegre: Sul editores, 2010. 555p.

MORIMOTO, C. E. **Servidores Linux: guia prático**. 2ª reimpressão. ed. Porto Alegre: Sul editores, 2010. 735p.

NETO, J. J. S. **PFADMIN - uma ferramenta web para gerencia de firewall utilizando o packt filter do openbsd**. 2008. 113f. Monografia (Bacharelado em Ciência da Computação) - Universidade Federal do Pará, Belém, 2008.

NIC.BR **Práticas de segurança para administradores de rede Internet**. Versão 1.2. ed. São Paulo: NIC.BR, 2003. 46p.

RODRIGUES, M. A. **Implementação de Firewall em micros e pequenas empresas**. 2007. 107f. Monografia (Bacharelado em Tecnologia em Redes de Computadores) - Centro Universitário de Maringá, Maringá, 2007.

SILVA, A. L. **Sistema de administração e controle de usuários de um dominio em servidores Microsoft**. 2004. 54f. Monografia (Bacharelado em Sistema de Informação) - Universidade para o Desenvolvimento do Alto Vale do Itajaí, Rio do Sul, 2004.

SILVA, A. M.; UCHOA, J. Q. **Uma implementação de alta disponibilidade em Firewall Linux**. Bazar: Softwares e Conhecimentos Livres, São Paulo, n.1, p.1-12, 2005.

SPANCESKI, F. R. **Politica de Segurança da Informação**. 2004. 102f. Monografia (Bacharelado em Sistema de informação) - Instituto Superior Tupy, Joinville, 2004.

Centro de estudos, respostas e tratamentos de incidentes de segurança no Brasil. Disponível em: <http://www.cert.br/stats/span/> Acesso em: 1 mai. 2013

Hierarquia das entidades de padronização para Internet. Disponível em: <http://www.novateceditora.com.br/livros/redescom/capitulo9788575221273.pdf> Acesso em: 9 jan. 2013

Posicionamento de um firewall. Disponível em: <http://www.manolo-lopez.com/wordpress/wp-content/uploads/2012/02/ipcop_form_web1.gif> Acesso em: 17 out. 2012

7. APÊNDICE I – POLÍTICA DE SEGURANÇA

2012

Política de Utilização de Recursos Tecnológicos

Raul Aparecido Franco Simionato

Anatex Indústria e Comércio Ltda.

19/07/2012

Conteúdo

1. INTRODUÇÃO

A intenção do Departamento de TI com a publicação da Política de Utilização de Recursos Tecnológicos não é impor restrições contrárias à cultura de abertura e confiança da Anatex Ind. e Com. Ltda, mas proteger a Empresa, os funcionários e parceiros, de ações ilegais ou danosas praticadas por qualquer indivíduo, de forma proposital ou inadvertidamente.

Sistemas relacionados à Internet, Intranet, os equipamentos de computação, software, sistemas operacionais, dispositivos de armazenamento, contas de rede que permitem acesso ao correio eletrônico, consultas WWW e FTP a partir de IP's (endereços de protocolo da internet) e o sistema de telefonia - são propriedades da Anatex Ind. e Com. Ltda., devendo ser utilizados com o exclusivo propósito de servir aos interesses da Empresa e de seus clientes, no desempenho de suas atividades empresariais.

A segurança efetiva é um trabalho de equipe envolvendo a participação e colaboração de todos os funcionários e afiliados de nossa Empresa que manipulam informações e/ou sistemas de informação. É de responsabilidade de cada usuário conhecer esta política e conduzir suas atividades de acordo com a mesma.

2. PROPÓSITO

O propósito desta política é delinear a utilização aceitável dos equipamentos de informática e telefonia da Anatex Ind. e Com. Ltda, e com isso garantir a disponibilidade, a integridade e a confidencialidade das informações necessárias ao funcionamento da empresa.

Estas regras foram definidas para proteger os funcionários e a Empresa. A utilização inapropriada dos equipamentos e sistemas relacionados no item anterior torna-os vulneráveis a atuação de hackers, contaminação por "vírus" e danificação, gerando comprometimento dos sistemas e serviços da rede, além de problemas legais.

3. ABRANGÊNCIA

Esta política se aplica aos funcionários, prestadores de serviços, consultores, auditores, fiscais, temporários e demais colaboradores que estejam a serviço da Anatex Ind. e Com. Ltda., incluindo toda a mão-de-obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas; e abrange todos os sistemas e equipamentos de propriedade da empresa, bem como aqueles de propriedade de terceiros que lhe sejam confiados a qualquer título, ou cedidos pela mesma a terceiros.

4. DIREITOS DOS USUÁRIOS

Os usuários de recursos computacionais da Anatex Ind. e Com. Ltda., possuem os seguintes direitos:

- Fazer uso legal dos recursos computacionais colocados à sua disposição, respeitando as normas de utilização estabelecidas pela Empresa;
- Ter conta de acesso à rede corporativa, respeitando as normas de utilização estabelecidas pela Empresa;
- Ter conta de correio eletrônico com a extensão do domínio da Empresa, desde que seja necessário ao desenvolvimento de suas atividades.
- Acessar a Internet para o desenvolvimento de suas atividades, respeitando as políticas da Empresa;
- Acessar as informações que forem franqueadas, relativas às áreas de armazenamento privado e compartilhado, respeitando as normas de utilização e confidencialidade estabelecidas pela Empresa;
- Solicitar suporte técnico sempre que verificado o mau funcionamento dos equipamentos ou do sistema de rede corporativa;
- Fazer uso do telefone da Empresa para tratar de assuntos relacionados ao trabalho.

5. DEVERES DOS USUÁRIOS

Os usuários de recursos computacionais da Anatex Ind. e Com. Ltda., possuem as seguintes obrigações:

- Responder pelo uso exclusivo de sua conta pessoal de acesso à rede corporativa;
- Identificar, classificar e enquadrar as informações da rede corporativa relacionadas às atividades por si desempenhadas;
- Zelar por toda e qualquer informação armazenada na rede corporativa contra alteração, destruição, divulgação, cópia e acessos não autorizados;
- Guardar sigilo das informações confidenciais, mantendo-as em caráter restrito;
- Manter, em caráter confidencial e intransferível, a senha de acesso aos recursos computacionais e de informação da organização, informando-a formalmente ao Administrador da Rede;

- Informar imediatamente à Gerência sobre quaisquer falhas ou desvios das regras estabelecidas neste documento, bem como sobre a ocorrência de qualquer violação às mesmas, praticadas em atividades relacionadas ao trabalho, dentro ou fora das dependências da Empresa;

- Responder cível e criminalmente pelos danos causados em decorrência da não observância das regras de proteção da informação e dos recursos computacionais da rede corporativa;

- Fazer uso dos recursos computacionais para trabalhos de interesse exclusivo da organização;

- Zelar e manter em segurança todos os equipamentos disponibilizados para o desenvolvimento de suas atividades;

6. PROIBIÇÕES

É proibido aos usuários de recursos computacionais:

- Acessar, copiar ou armazenar programas de computador ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais (copyright), bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, racista ou que faça apologia ao crime;

- Utilizar os recursos computacionais ou quaisquer outros de propriedade da Empresa, colocados à disposição do colaborador em razão do exercício de sua função, para constranger, assediar, prejudicar ou ameaçar a mesma ou terceiros, sejam eles indivíduos ou organizações;

- Passar-se por outra pessoa ou esconder, por qualquer meio, a própria identidade quando utilizar os recursos computacionais ou quaisquer outros de propriedade da Empresa, colocados à disposição do colaborador em razão do exercício de sua função;

- Alterar os sistemas padronizados, sem autorização;

- Divulgar quaisquer informações confidenciais para concorrentes e/ou qualquer pessoa não ligada às atividades da Empresa;

- Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes à Empresa;

- Violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, entre outros mecanismos de segurança e restrição de acesso;

- Utilizar acesso discado através de modem, ou qualquer outra forma de conexão não autorizada, quando conectado às redes instaladas nas dependências da Empresa;

- Acessar e-mail pessoal, sites de relacionamento ou redes sociais;
- Fazer uso do telefone da Empresa para assuntos pessoais;
- Fazer uso do e-mail corporativo para assuntos pessoais;
- Fazer uso da internet para assuntos que não estejam relacionados à sua função na Empresa, tais como pesquisas, entretenimento, entre outros;
- Utilizar quaisquer recursos ou equipamentos da Empresa para fins diversos, senão daqueles necessários ao desempenho da função contratada;
- Criar blogs e comunidades na Internet, ou qualquer ambiente virtual semelhante, utilizando-se, sem autorização expressa, da logomarca da Empresa;
- Fazer uso do telefone celular particular dentro das dependências da Empresa.

7. COMPROMISSOS

Os usuários dos recursos computacionais comprometem-se a:

- Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores;
- Não utilizar recursos computacionais corporativos para desenvolver, fomentar ou promover ações que incentivem o racismo ou qualquer tipo de discriminação que viole quaisquer outros direitos constitucionais do cidadão;
- Não fazer uso da rede para molestar, ameaçar ou ofender seus usuários ou terceiros, por quaisquer meios, sejam textos, imagens, vídeos ou correios eletrônicos;
- Não fazer uso da rede para circulação de propaganda política;
- Não tomar atitude ou ação que possa, direta ou indiretamente, indisponibilizar recursos da rede corporativa;
- 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 indisponibilização de serviços;
- Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da Empresa;

- Não utilizar nenhum programa de bate-papo, mensagem instantânea ou sites de relacionamento tais como Skype, MSN,Google Talk, Orkut, Facebook, Twitter entre outros; exceto para fins de trabalho e com autorização da diretoria.

- Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha “robusta”;

- Responsabilizar-se perante a Empresa e terceiros por quaisquer prejuízos advindos da violação dos compromissos, deveres e proibições estabelecidas nesse documento;

- Utilizar-se, de forma ética e em conformidade com as normas de conduta e segurança estabelecidas pela Empresa, de todos os recursos, equipamentos e informações que lhe sejam confiados em razão do desempenho de sua atividade profissional.

8. ADIÇÃO E REMOÇÃO DE RECURSOS

Não é permitido aos usuários de recursos computacionais da organização a adição e remoção de quaisquer recursos, sejam eles microcomputadores, caixas de som, impressoras, pen drives, mp3 players ou outros equipamentos e dispositivos, exceto nos casos em que a utilização destes é necessária para a realização das atividades diárias, nestes casos com prévia autorização do setor de TI. Também não é permitida a instalação ou alteração de qualquer tipo de software, seja ele pago ou livre.

Quando houver a necessidade de adição ou remoção destes recursos (software ou hardware), deverá ser feita uma solicitação formal ao administrador da rede, que avaliará o pedido e passará para aprovação. Sendo aprovada, a instalação destes recursos deverá ser feita pelo setor de TI.

9. ADMINISTRADOR DA REDE

O uso das senhas e informações dos usuários, pelo Administrador da Rede, deverá ser realizado com fins operacionais e preventivos, cabendo ao Administrador manter a confidencialidade das informações adquiridas, sob pena de punição;

O controle de senhas e níveis de acesso dos usuários e todos os recursos computacionais devem ser feitos pelo Administrador da Rede, e reportado formalmente para a Alta Direção da Empresa com as devidas atualizações.

10. PERMISSÕES E SENHAS

Todo usuário que necessite acessar a rede corporativa deverá possuir um login e senha fornecidos pelo setor de TI. Esta senha será pessoal e intransferível, sendo de responsabilidade do usuário mantê-la em sigilo e segurança.

As permissões de acesso que serão atribuídas aos usuários deverão ser informadas pelo seu superior direto, cabendo a este informar formalmente o setor de

TI sobre modificações nas mesmas.

No caso de alteração de cargo, mudança de setor ou demais alterações na situação do funcionário, é de responsabilidade de seu superior a comunicação ao setor de TI, para que sejam feitas as devidas alterações nas configurações de permissão e acesso.

No caso de contratação de um novo funcionário, caberá ao setor de Recursos Humanos, junto ao responsável pelo setor contratante, informar ao setor de TI sobre a necessidade de uso dos recursos tecnológicos, para que possa ser efetuado o cadastro e liberação de uso.

Quando houver um desligamento, caberá ao setor de Recursos Humanos informar ao setor de TI para quem deverá ser feito o direcionamento dos recursos do funcionário desligado, tais como aparelhos eletrônicos, caixas de e-mail e permissões de acesso a rede.

POLÍTICA DE UTILIZAÇÃO DE RECURSOS TECNOLÓGICOS DA EMPRESA ANATEX IND. E COM. LTDA.

O colaborador abaixo nominado declara, para os fins de Direito, livre de qualquer impedimento, que por serem de propriedade da empresa, todos os equipamentos, sistemas, acessos à rede corporativa e e-mails corporativos, bem como os terminais de telefonia fixa ou móvel, somente poderão ser utilizados para o desempenho das funções profissionais, e nos seus limites, conforme a legislação pertinente e normas internas, no interesse da Anatex Ind. e Com. Ltda..

Assim sendo, o colaborador abaixo nominado reconhece a legitimidade da Anatex Ind. e Com. Ltda., para monitorar suas atividades laborativas com a finalidade de manutenção da ordem e segurança pessoal de seus colaboradores, bem como da integridade da rede corporativa (informática e telefonia) e dos equipamentos e sistemas de sua propriedade, além do necessário sigilo das informações.

Pelos mesmos motivos, o colaborador abaixo nominado declara ter recebido, lido e concordado com todas as normas estabelecidas neste documento, autorizando, por este ato, a empresa, a monitorar qualquer atividade computacional e de telefonia, tais como e-mail, acessos a rede interna e à internet, entre outros, realizadas da empresa.

Eu, _____ , declaro estar ciente dos termos das políticas de segurança relacionadas neste documento e autorizo o monitoramento de minhas atividades computacionais e de telefonia pela Anatex Ind. e Com. Ltda., estando ciente dos meus direitos, obrigações e deveres para com esta empresa.

_____ , ____ de _____ de _____.