Winconnection 6

Manual do usuário

WINCO

Sumário

1. Introdução

Este manual do usuário oferece uma documentação para as principais configurações do **Winconnection 6**.

O **Winconnection 6** é um *Gateway* para sistemas operacionais *Windows* desenvolvido no Brasil, que agrupa uma série de funções em um único produto para o gerenciamento seguro do tráfego dentro das redes existentes nas empresas.

Nosso produto é referência, no Brasil, para Servidores Proxy, Servidores de E-mail e Firewall, agregando funções de Mensagens Instantâneas, DDNS (DNS dinâmico), DHCP, Gerador de Relatórios e muito mais, além de várias ferramentas e possibilidades de configurações fundamentais em um produto de administração de redes.

1.1. Características do Winconnection 6?

Veja a seguir as principais características e funcionalidades do **Winconnection 6**:

- Produto com desenvolvimento 100% nacional.
- Suporte direto com o desenvolvedor.
- Agrega um grande número de funções em um único produto.
- Fácil instalação e configuração: o gerenciador pode ser executado de qualquer estação na rede local.
- Administrador Web.
- Estabilidade, segurança e administração simplificada.
- Integração com o MS Active Directory (AD).
- Bloqueio do Ultra-Surf.
- Compartilhamento de conexão.
- Registro de logs para todos os serviços.
- Atualização automática do programa (auto-update).
- Firewall integrado.
- Relatório de utilização do link.
- Controle de banda.

- Balanceamento e distribuição de uso de links.
- Inspetor de pacotes (bloqueio da conexão de acordo com o protocolo).
- Proxy Transparente (NAT).
- Servidor de E-mail contendo:
    - Filtro antivírus;
    - Filtro anti-spam;
    - Cota de e-mail;
    - Cópia de segurança de mensagens;
    - Lista de distribuição de e-mails;
    - Diversos filtros configuráveis e possibilidade de customização do produto via programação PHP;
    - Whitelist e Blacklist de Spam;
    - Relatórios de uso e rastreamento de mensagens;
    - Geração de avisos automáticos para os e-mails que chegarem conforme a configuração definida, podendo implementar mensagens de indisponibilidade e avisos de recebimento;
    - Aviso de férias com mensagem personalizada;
    - Autenticação em base própria ou na base de usuários do Windows;
    - Gerenciamento por grupo;
    - Suporte ao protocolo IMAP;
    - Controle de tamanho de mensagens;
    - Filtro de anexos;
    - Filtro Automático Anti-Spam – SpamCatcher;
- Servidor PROXY HTTP, HTTPS, FTP contendo:
    - Controle de acesso à internet por grupo de usuários;
    - Controle de acesso à internet por site/conjunto de site/horários;
    - Regras de acesso simplificadas;
    - Bloqueio de download de arquivos (extensão);
    - Plug in para Filtro Automático de Conteúdo;

  - Importação de lista de sites em formato texto;
  - Restrição de tempo de navegação;
  - Restrição de limite de transferência diária;
  - Relatório de navegação por usuário;
- Servidor Web contendo:
  - Suporte a PHP;
  - Criação de múltiplos "alias";
- Servidor de Mensagem Instantânea com transferência de arquivos (Winco Messenger).
- Cliente DDNS (DNS Dinâmico).
- Servidor DHCP.
- Serviço de VPN integrado.
- Serviço de replicação de regras globais de acesso à internet para todas as unidades da organização (matriz e filiais).

2. Instalação

2.1. Requisitos de Software

O **Winconnection 6** pode ser instalado nos seguintes sistemas operacionais:

- Windows 2000 Professional SP4
- Windows 2000 Server SP4
- Windows XP Home Edition
- Windows XP Professional SP2
- Windows Server 2003 SP2
- Windows Server 2008
- Windows Vista Business
- Windows Vista Ultimate
- Windows 7

Obs.: Para instalar o Winconnection 6 é necessário ter o Internet Explorer 6.0 ou superior.

2.2. Requisitos de Hardware

Equipamento Mínimo:

- Processador de 1GHz
- 512 MB de RAM
- HD de 120GB

Equipamento Recomendado:

- Processador de 2GHz ou superior
- 1GB de RAM
- HD de 120GB

Obs.: São necessárias **duas placas de rede**: Uma para rede interna e outra para rede externa.

2.3. Antes de Instalar

Este manual parte do princípio que o administrador tenha conhecimentos básicos de TCP/IP e conhecimento dos programas de acesso à Internet instalados na rede (chamados

de clientes).

Recomendamos verificar os itens abaixo antes de instalar o **Winconnection 6**:

- O computador onde será instalado o **Winconnection 6** deve estar funcionando normalmente, conectado à internet e com todas as funções de navegação, recebimento de e-mail, etc. em perfeito estado.

- Todos os clientes devem estar com o protocolo TCP/IP instalados e funcionando corretamente. O Administrador deve conhecer a topologia da rede interna, bem como o IP do servidor e dos clientes e a classe de rede utilizada.

- O Administrador que irá fazer a instalação deve possuir uma ideia clara dos serviços que irá usar no **Winconnection 6** e por qual motivo quer usar o produto.

- O Administrador deve conhecer todos os logins dos e-mails que serão cadastrados.

OBS: Recomendamos se logar no Windows como *Administrador* ou com algum usuário que tenha direitos administrativos. Isto se deve ao fato de que o programa se instala como um serviço do sistema operacional, que é iniciado automaticamente toda vez que o computador é ligado.

2.4. Instalando o Winconnection 6

Primeiramente faça o download da versão mais recente do programa disponível na seção de download do site do **Winconnection**.

Após concluir o download, execute o arquivo de instalação:

O *Assistente de Instalação* ajudará a descompactar o arquivo e criar as pastas do **Winconnection 6**. Escolha um disco rígido que tenha uma quantidade mínima de espaço em disco para abrigar com segurança a operação de sua intranet. O diretório sugerido é: *C:\Arquivos de programas\Winco\Winconnection 6.*

Após finalizar a instalação, o **Winconnection 6** inicia automaticamente o Assistente de Configuração. Siga os passos desse assistente, informando corretamente os dados (as etapas estão descritas detalhadamente no tópico Assistente de Configuração). Assim que as etapas do Assistente de Configuração forem concluídas, o **Winconnection 6** será

inicializado e pronto para ser usado.

3. Assistente de Configuração

O *Assistente de Configuração* é iniciado logo após o término da instalação e realiza o processo de pré-configuração do **Winconnection 6**.

Veja a seguir uma breve descrição das etapas disponíveis no *Assistente de Configuração*:

- **1ª Etapa – Licenciamento:**

  A primeira tela do assistente é a de licenciamento e exibe três opções:

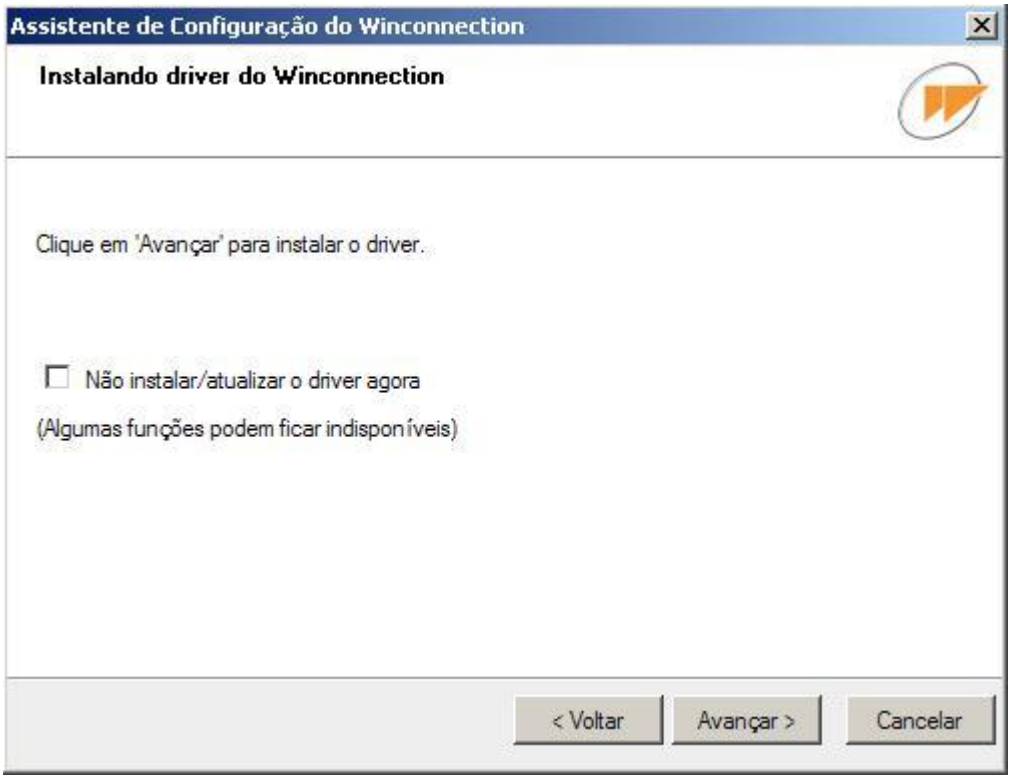
  - **Já tenho uma licença definitiva:** Para usuários que já possuem a licença do **Winconnection 6**.

  - **Quero TESTAR o programa por 30 dias:** Para usuários que querem testar o programa durante 30 dias (usuários ilimitados).

Selecione a opção desejada e clique no botão *Avançar*.

- **2ª Etapa – Instalação do driver**

Esta etapa irá instalar o driver do Winconnection necessário para o funcionamento correto do programa. Clique no botão *Avançar* para iniciar a instalação.



Obs.: Se a opção "Não instalar/atualizar o driver agora" for habilitada, algumas funções do **Winconnection 6** ficarão indisponíveis.

- **3ª Etapa – Migrando as configurações**

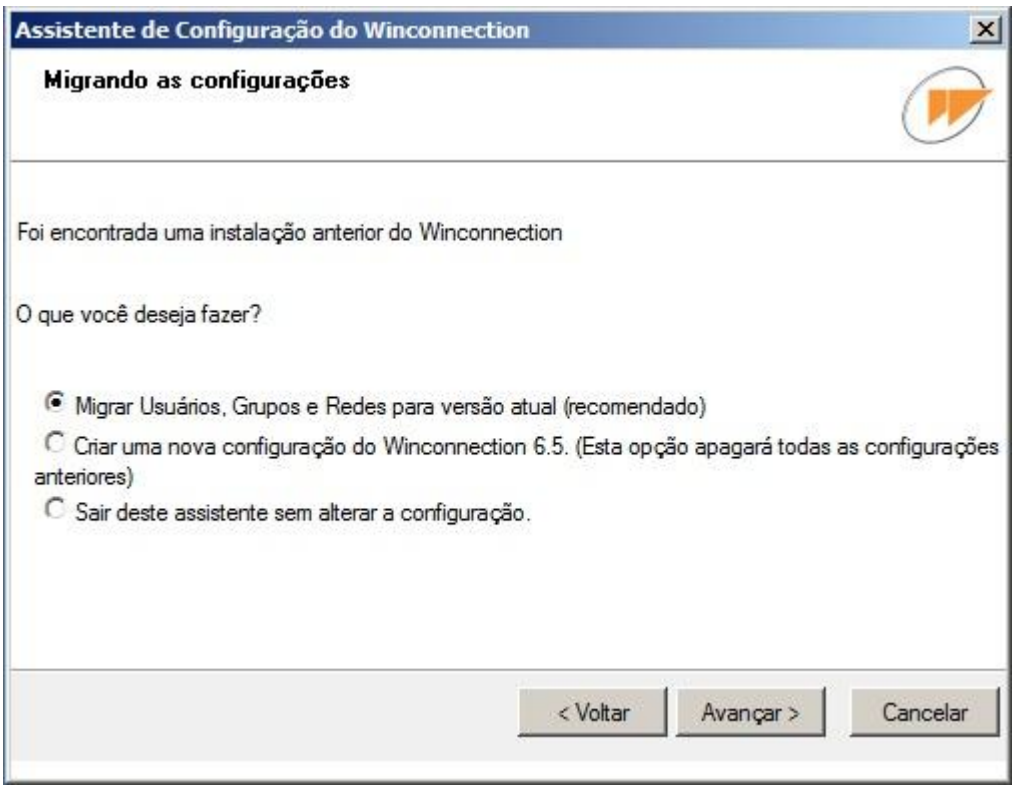
Se uma versão anterior do **Winconnection** for detectada, o *Assistente de Configuração* do **Winconnection 6** irá detectá-la automaticamente e oferecerá uma das três opções abaixo:

- **Migrar Usuários, Grupos e Redes para a versão atual (recomendado):** Os usuários, grupos e redes da versão atual serão importados para a versão que

está sendo instalada. Ao clicar no botão *Avançar,* o assistente direcionará para a *Etapa 6*.

- **Criar uma nova configuração do Winconnection 6:** Todas as configurações das versões anteriores serão apagadas. Ao clicar no botão *Avançar,* o assistente direcionará para a *Etapa 4*.

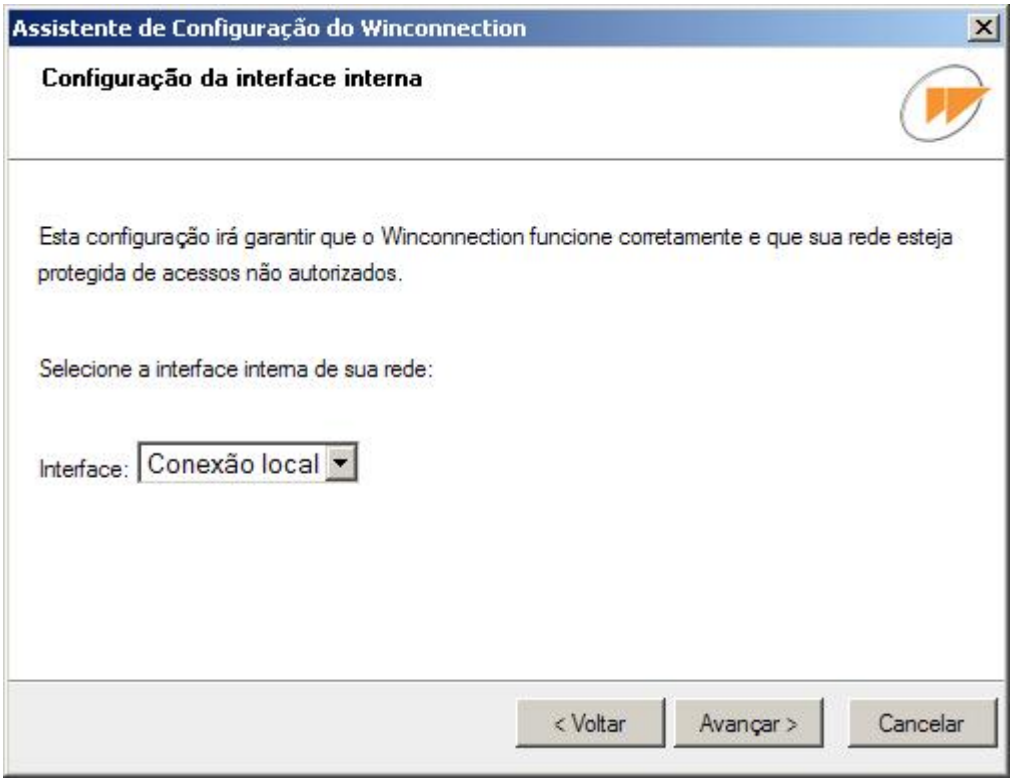
- **Sair deste assistente sem alterar a configuração:** A configuração da versão anterior será mantida. Ao clicar no botão *Avançar,* o assistente direcionará para a *Etapa 6*.



➢ 4ª Etapa – Configuração da Interface Interna

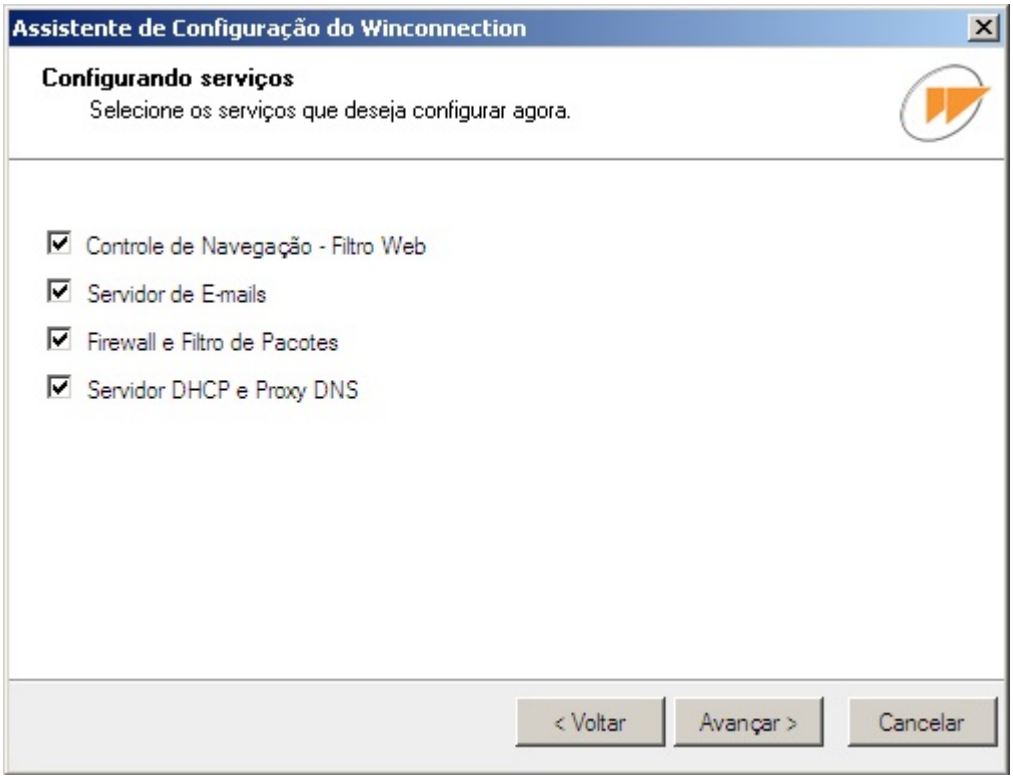
A configuração desta etapa garante o funcionamento correto do **Winconnection 6** e a proteção da rede contra acessos não autorizados.

Selecione a interface interna da rede e clique no botão *Avançar*.



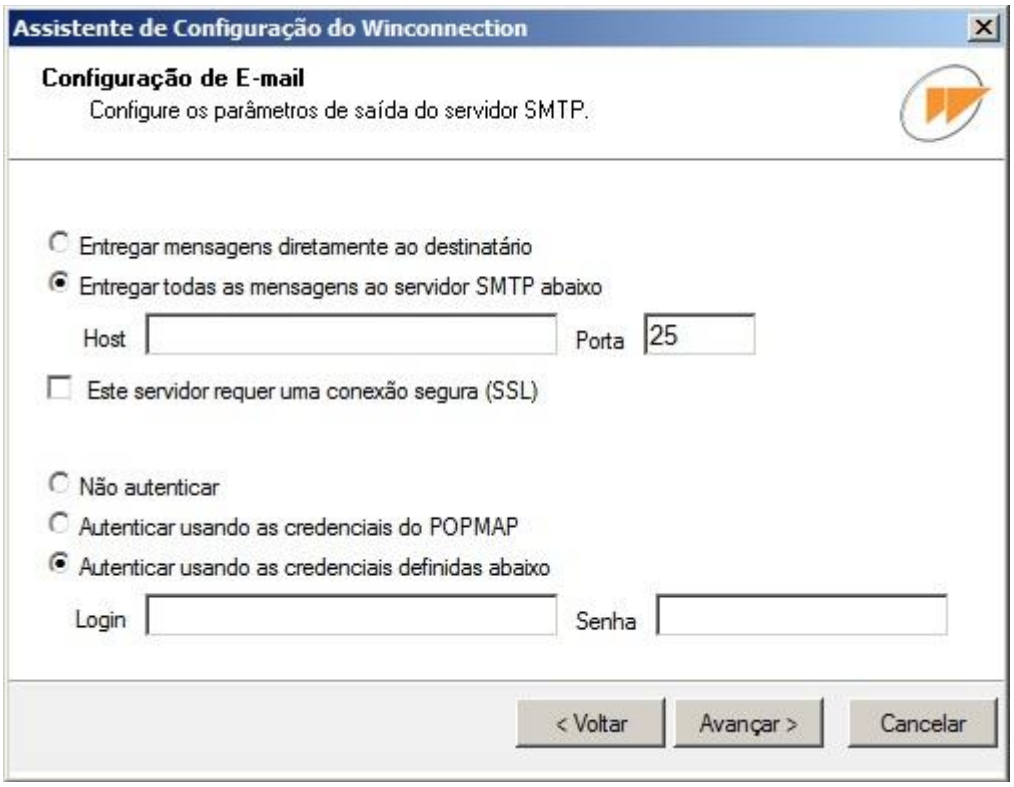
- **5ª Etapa – Configurando os Serviços**

Nesta etapa, o administrador da rede poderá selecionar os serviços que deverão ser instalados e configurados com o auxílio do *Assistente de Configuração*.



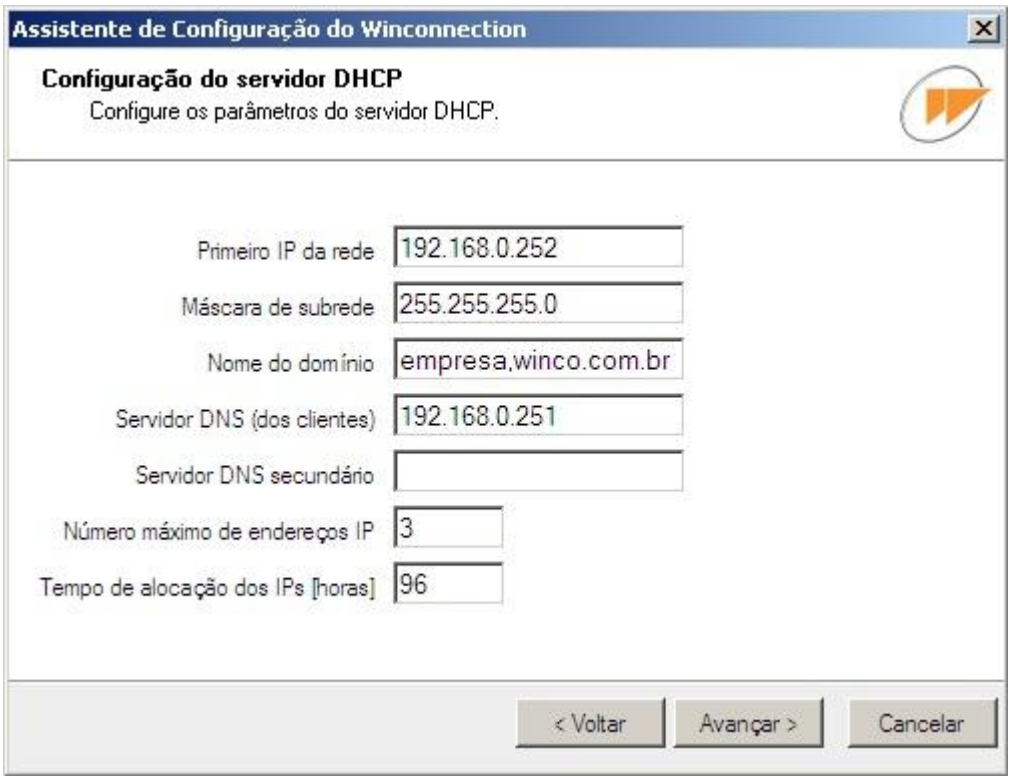
Configuração de E-mail:

Nesta tela, é possível configurar os parâmetros de saída que serão utilizados pelo *Servidor de E-mail* do **Winconnection 6**. Mais informações sobre essas configurações podem ser encontradas no capítulo Servidor SMTP (guia *Domínios -> Parâmetros de Saída*).



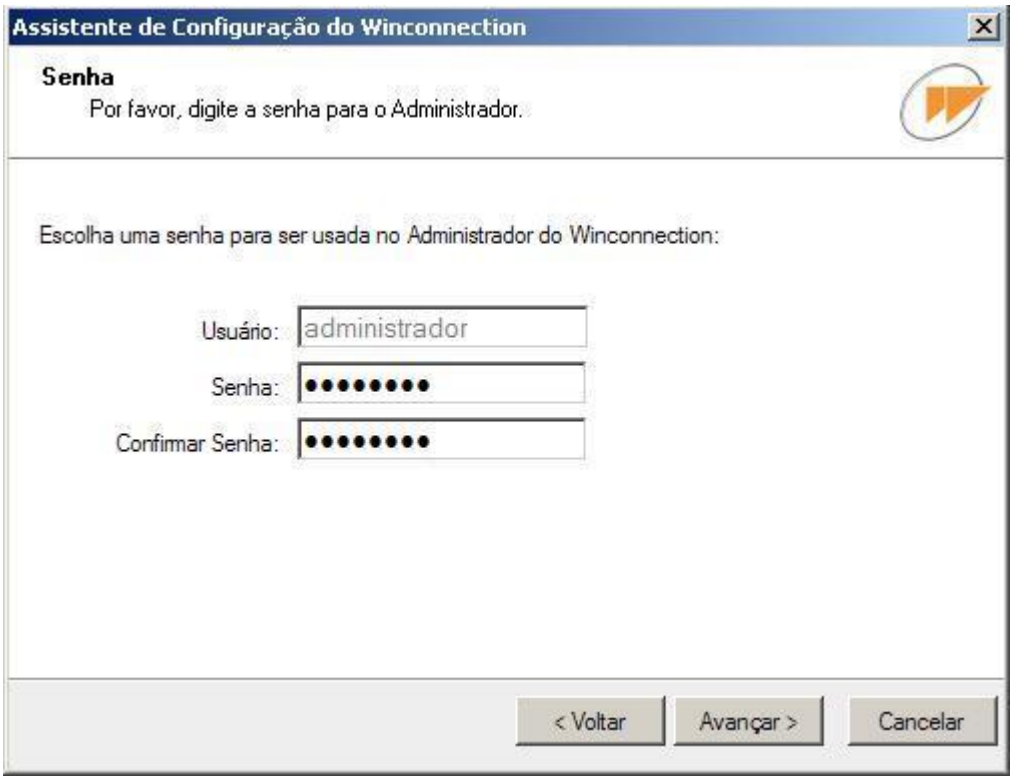
Configuração do Servidor DHCP:

Nesta tela, é possível configurar o *Servidor DHCP* do **Winconnection 6**. Para mais informações, consulte o capítulo DHCP.



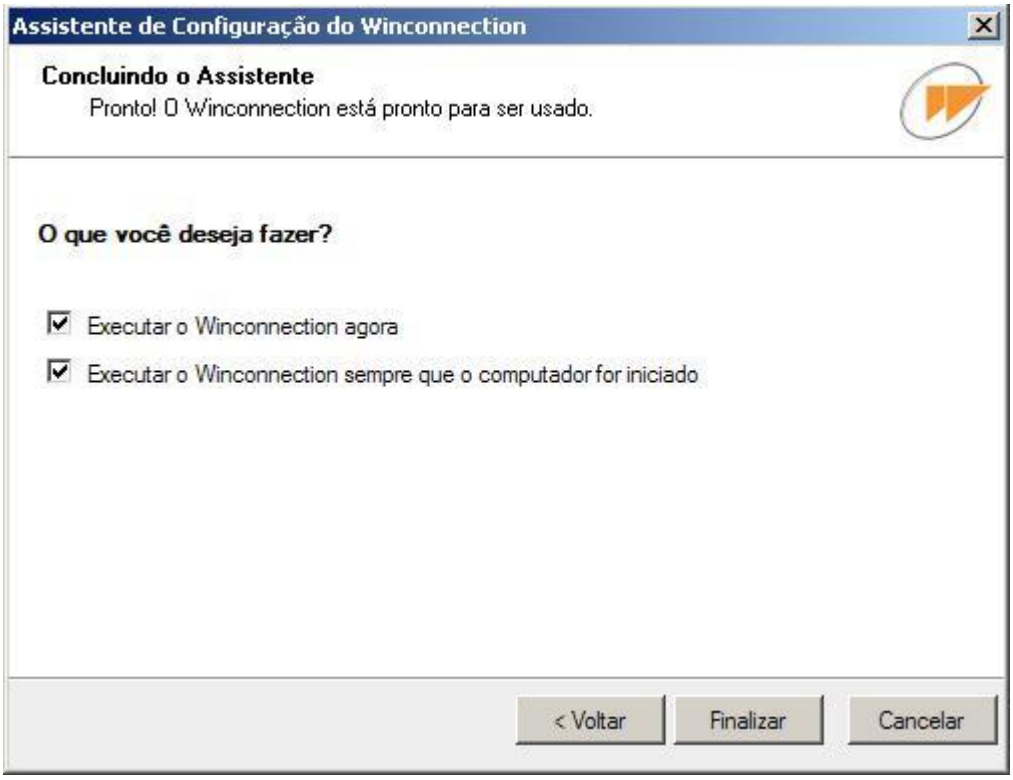
- **6ª Etapa: Definindo uma senha para o administrador:**

Digite uma senha que será usada para o acesso ao *Administrador*. Feito isso, clique em *Avançar*.



- **7ª Etapa: Concluindo o assistente:**

Esta é a última tela do *Assistente de Configuração*. Clique no botão *Concluir*.



Após concluir o *Assistente de Configuração*, é possível abrir o Administrador do **Winconnection 6** e configurar as demais funcionalidades do produto. Todas elas estão descritas neste manual.

4. Administrador do Winconnection 6

O *Administrador* é o aplicativo que faz o gerenciamento do **Winconnection 6**. A senha inicial do administrador é a escolhida durante a execução do *Assistente de Configuração* (consulte o capítulo Assistente de Configuração para obter mais informações).

Ao acessar o Administrador do **Winconnection 6** será exibida a seguinte tela de autenticação:

Veja a seguir uma breve descrição do menu principal disponível no *Administrador*:

Servidor:

- *Conectar:* Conecta o Administrador.
- *Desconectar* Desconecta o Administrador.
- *Auto-Update:* Executa o processo de verificação de atualização do **Winconnection**.
- *Sair*: Fecha o Administrador do **Winconnection**.

Exibir:

- *Barra de Ferramentas:* Exibe os botões de atalho do Servidor e dos Serviços.
- *Atualizar Gráfico:* Define o tempo (em segundos) para a atualização dos gráficos.
- *Exibir Árvore de Serviço:* Exibe no lado esquerdo da tela os serviços instalados.

Serviços:

- *Novo:* Inclui um novo serviço.

Ajuda:

- *Sobre:* Mostra informações sobre o software.

Botões de Atalho:

Desconecta o Administrador.

Exibe uma nova janela de registros de logs.

Seleciona o serviço inferior.

Seleciona o serviço superior.

Inicia o serviço selecionado.

Para o serviço selecionado.

Abre as configurações do serviço selecionado.

A janela de status mostra todos os acessos ao servidor por serviço acessado.

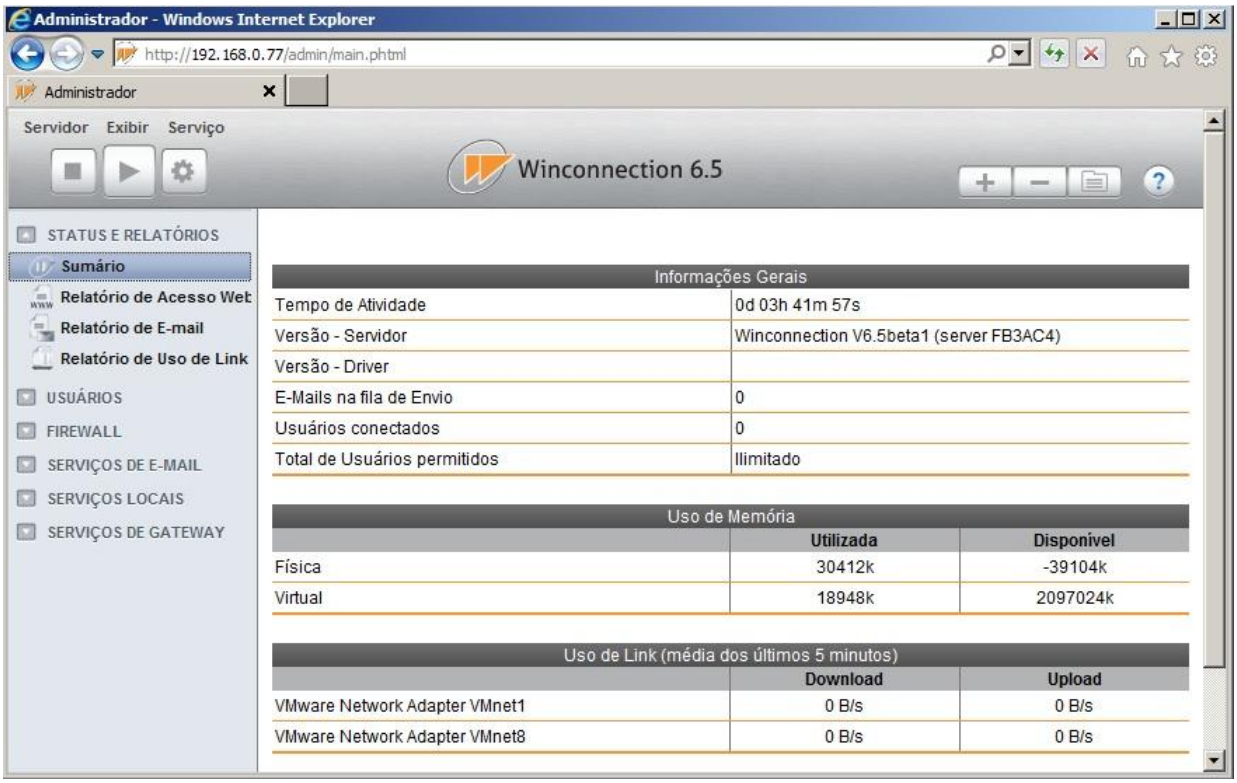
Por padrão, o Administrador é executado na máquina onde está instalado o programa. Contudo, também é possível acessá-lo em qualquer outra máquina utilizando o **Administrador Web**.

4.1. Administrador Web

Com o *Administrador Web* é possível gerenciar as configurações do **Winconnection 6** a partir de qualquer máquina.

Para acessá-lo, digite o seguinte endereço no navegador: http://ip_do_servidor/admin.

Digite o login e senha do administrador ou de algum usuário que pertença ao grupo Administradores.



Veja a seguir uma breve descrição do menu superior disponível no *Administrador Web*:

Servidor:

- *Logout:* Desconecta o *Administrador Web*.
- *Verificar Atualizações:* Executa o processo de verificação de atualização do **Winconnection 6**.

Exibir:

- *Janela de Log:* Abre em uma nova guia as informações de todos os acessos ao servidor por serviço acessado.

Serviços:

- *Iniciar:* Inclui um novo serviço.
- *Parar:* Para o serviço selecionado.
- *Configurar:* Configura o serviço selecionado.
- *Excluir*: Exclui o serviço selecionado.
- *Criar novo*: Cria um novo serviço.

Botões de Atalho:

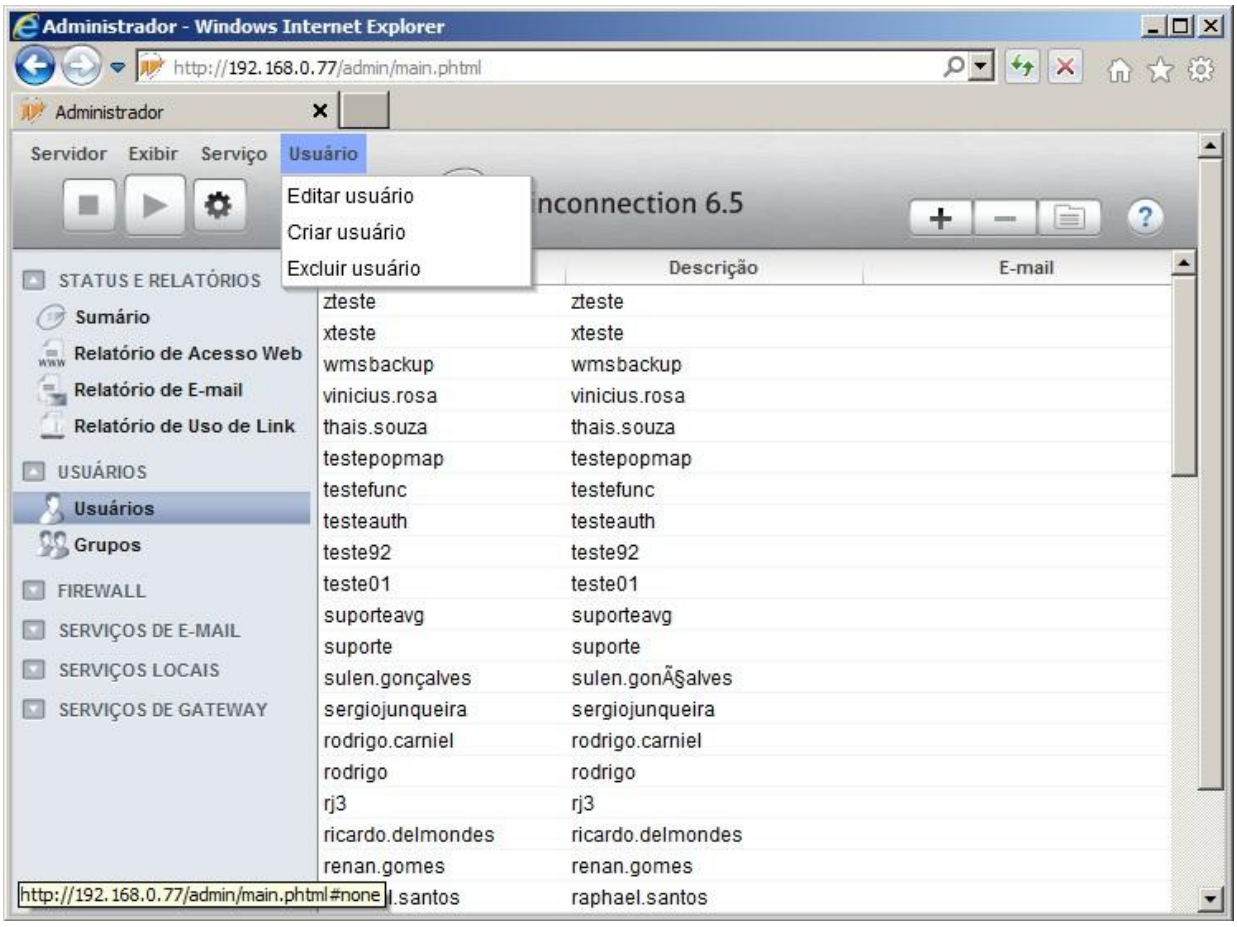
 Inicia o serviço selecionado.

 Para o serviço selecionado.

 Abre as configurações do serviço selecionado.

No menu superior do *Administrador Web*, no lado da opção *Serviço* é exibida a opção de configuração para o serviço que está atualmente selecionado.

Por exemplo: Ao selecionar a opção *Usuários* no menu do lado esquerdo, é exibido no menu superior a opção *Usuário* onde é possível Editar, Criar ou Excluir um usuário.



Todos os serviços disponíveis no *Administrador* e no *Administrador Web* estão descritos detalhadamente neste manual.

5. Gerenciamento de Usuários e Grupos

O **Winconnection 6** possui capacidades avançadas de controle de políticas de segurança, acesso, recebimento de e-mails etc., com base em usuários e grupos. Além disso, o **Winconnection 6** pode fazer uso da base de usuários de um *Active Directory da Microsoft (AD)*, criando um ambiente de segurança integrado e flexível.

Seu uso é recomendado, pois os grupos permitem ao produto simplificar políticas de segurança. Mesmo assim, sem usuários e grupos configurados, é possível estabelecer controles e políticas mínimas de acesso, perfeitamente capazes de manter pequenas topologias de redes protegidas.

Guia Configurações | Geral:

Nessa guia é possível bloquear um endereço IP sempre que ele atingir um número de tentativas consecutivas de autenticação sem sucesso.

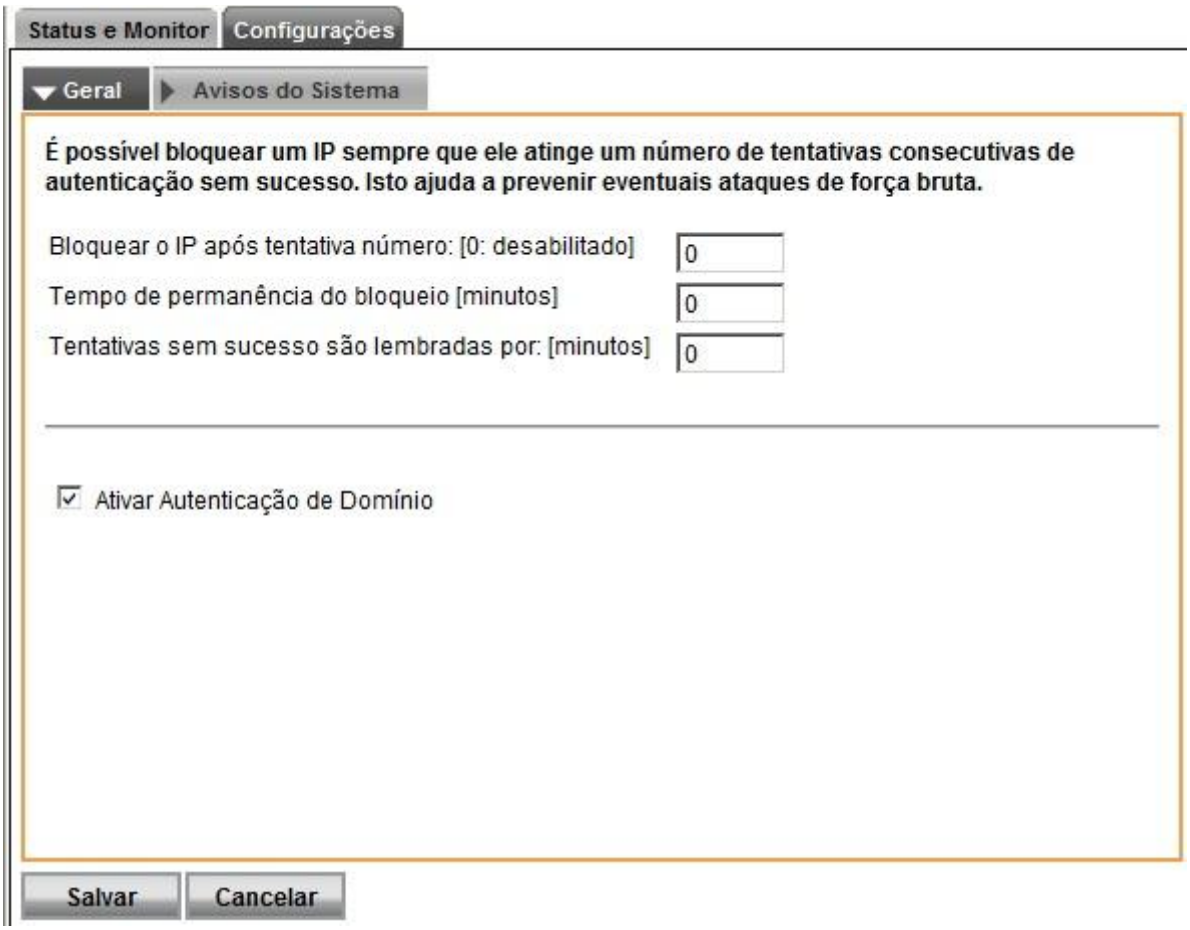
Esse tipo de configuração ajuda a prevenir eventuais ataques de força bruta.

- **Bloquear o IP após tentativa número [0 desabilitado]:** Neste campo, o administrador da rede deve informar o número de tentativas que poderão ser realizadas antes de efetuar o bloqueio.

- **Tempo de permanência do bloqueio [minutos]:** Deve-se informar por quanto tempo (em minutos) o bloqueio deve permanecer ativo.

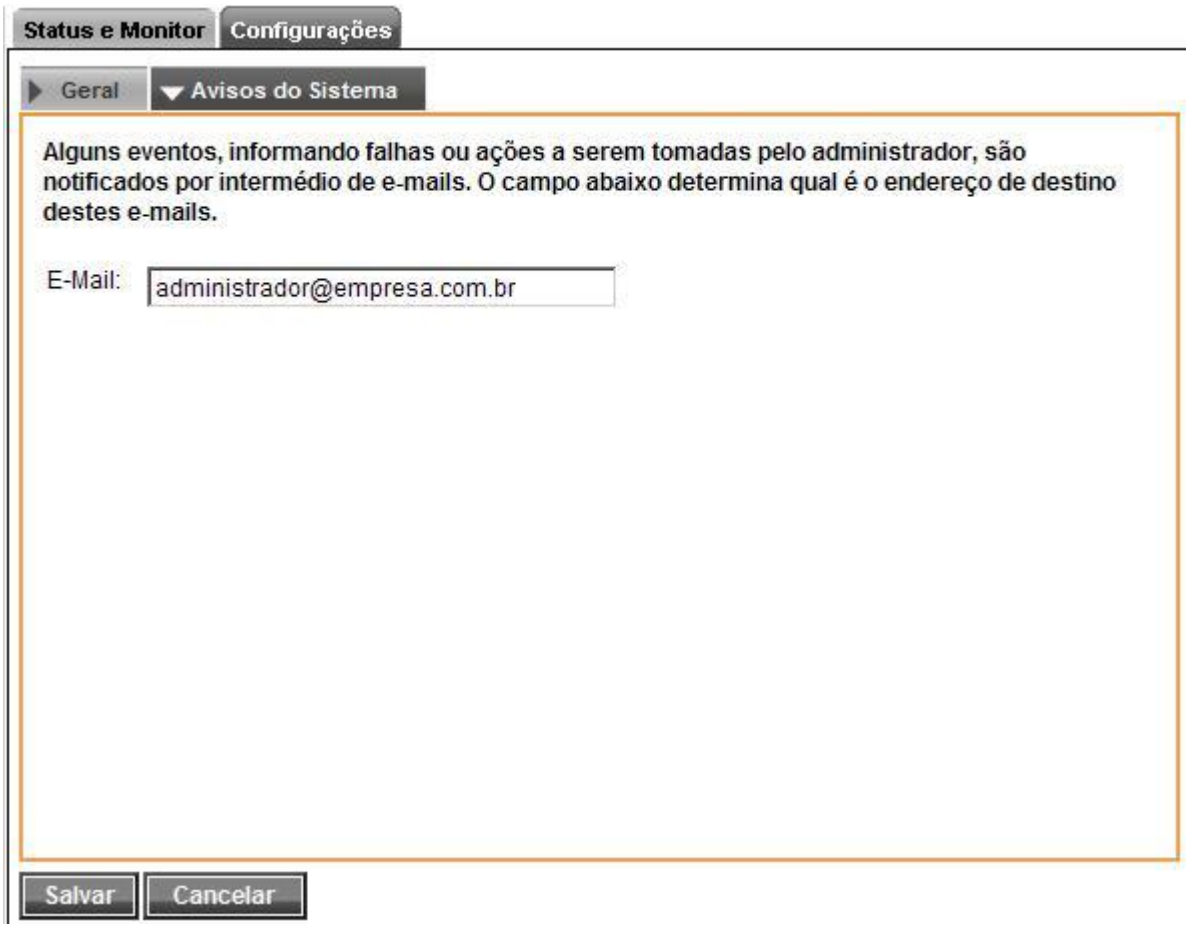
- **Tentativas sem sucesso são lembradas por [minutos]:** Neste campo, deve-se informar o intervalo máximo (em minutos) entre as tentativas de autenticação sem sucesso.

- **Ativar autenticação de Domínio:** Permite a integração do **Winconnection 6** com o **MS Active Directory (AD)**.



Guia Configurações | Aviso do Sistema:

Nesta guia de configuração é possível determinar um endereço de e-mail que receberá informações sobre falhas ou ações que deverão ser tomadas pelo administrador da rede.



Veja a seguir a descrição de cada serviço disponível no menu *Usuários*.

5.1. Usuários

Guia Status e Monitor:

Nessa guia de configuração são exibidas informações sobre os usuários que já foram cadastrados.

Os usuários listados em azul foram importados do *Active Directory (AD)* e não podem ser alterados no **Winconnection 6**.

Guia Novo | Geral:

Cadastrar um usuário no **Winconnection 6** é muito simples: Clique no menu *Usuários* → Selecione o item *Usuários*, clique com o botão direito na parte em branco da tela e clique em *Novo*. Insira as seguintes informações:

As seguintes informações estão disponíveis:

Informações básicas:

- **Login:** Nome do usuário. Este nome será o utilizado para receber e-mails ou se autenticar na internet, permitindo a navegação.

- **Descrição/Nome**: Uma breve descrição do usuário, exemplo: nome completo ou departamento.

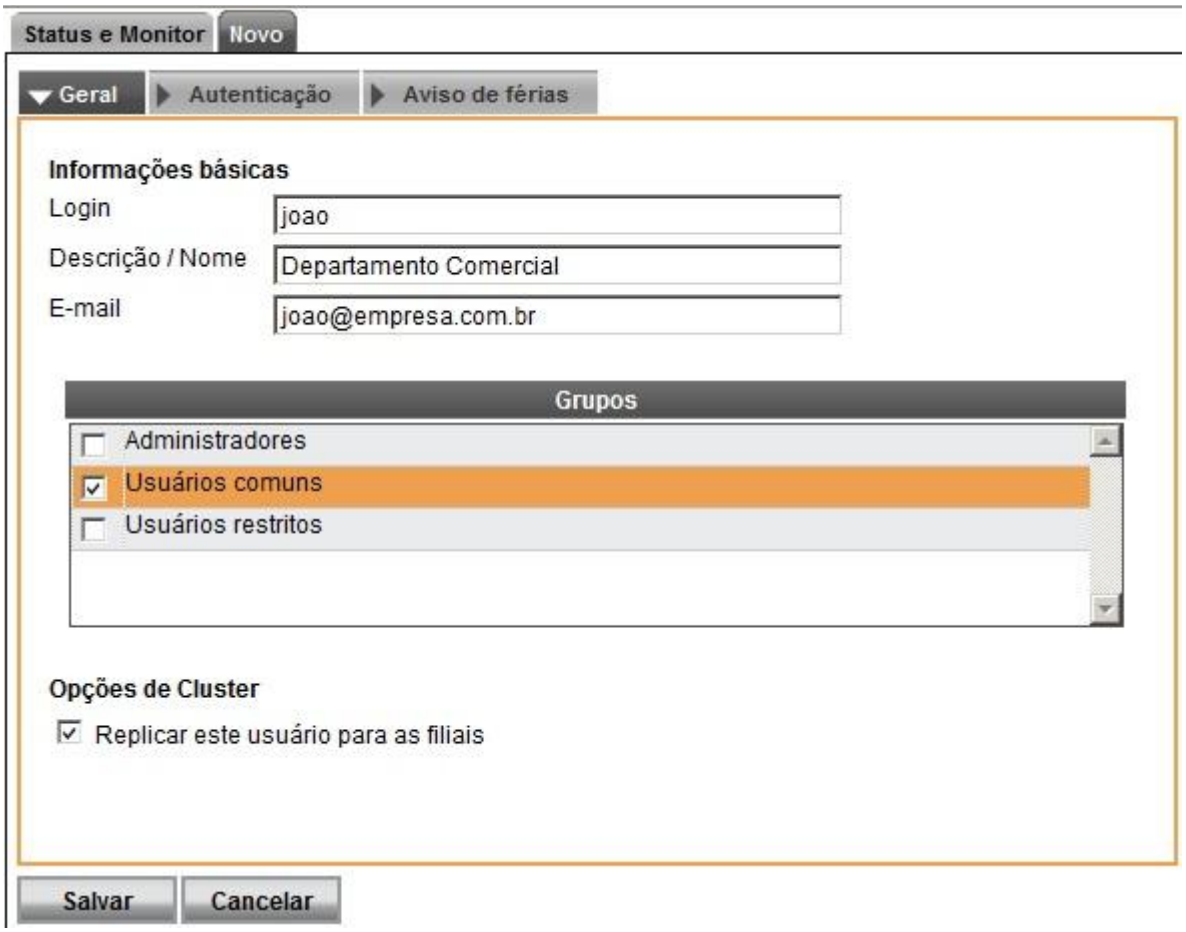
- **E-mail:** Neste campo é necessário digitar o e-mail do usuário.

Grupo:

Todo usuário tem que pertencer a um **Grupo**. Habilite nessa seção o Grupo a que o usuário pertencerá.

Opções de Cluster:

Esta opção deve ser habilitada se o administrador da rede desejar que o usuário seja replicado para as filiais (caso o serviço de replicação das regras globais de acesso à internet esteja sendo utilizado). Para mais informações sobre esse serviço, consulte o capítulo Cluster Master.



Guia Novo | Autenticação:

Critério de Autenticação:

Define como o usuário deverá se autenticar. As seguintes opções estão disponíveis:

Senha: Para o usuário se autenticar será necessário usar uma senha:

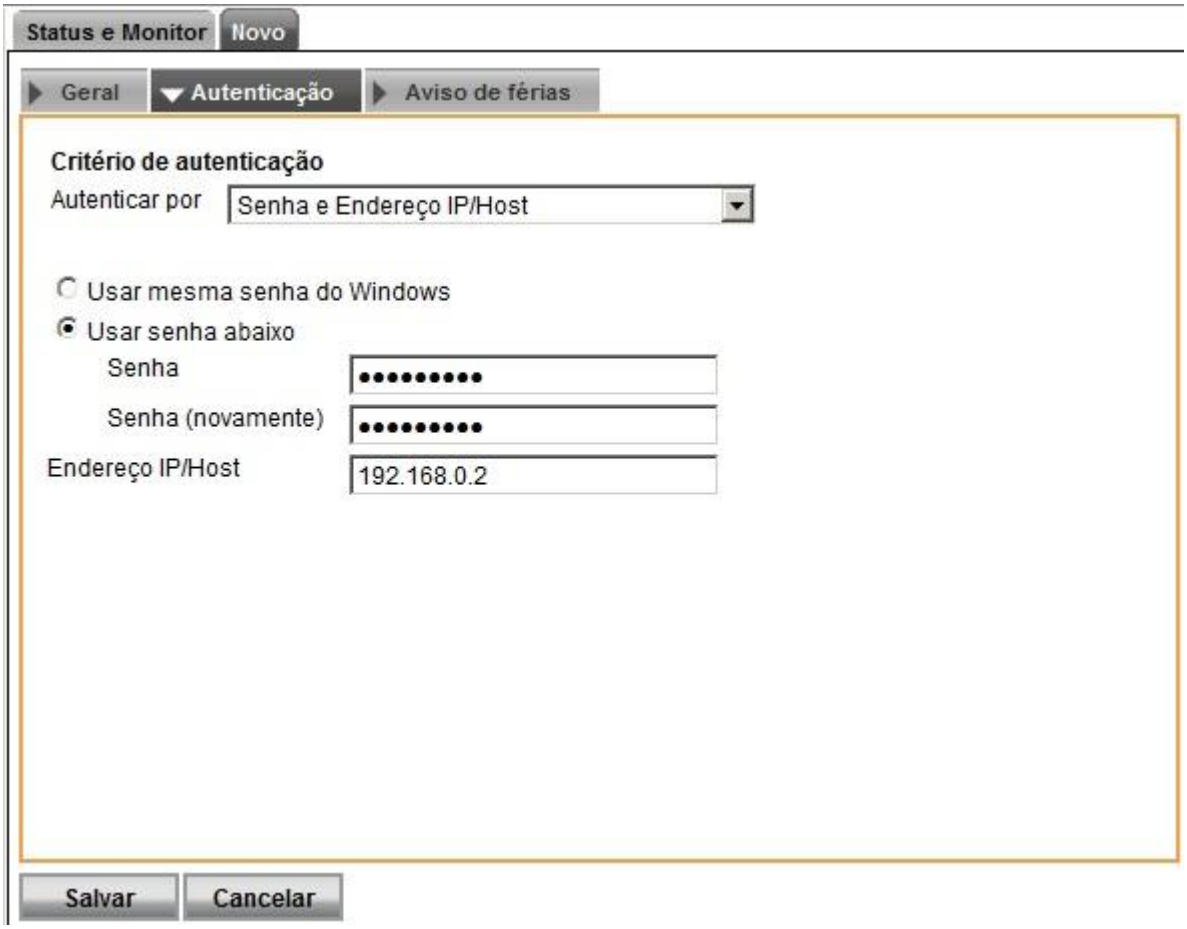
- **Usar a mesma senha do Windows**: Quando o **Winconnection 6** é instalado em um Windows 2000/2003 Server que seja o servidor de domínio ou membro deste domínio, o usuário pode usar a mesma senha de login do *Windows* para acessar seus e-mails ou permitir navegação na internet. Para tanto ative a opção "*Usar a mesma senha do Windows*".

- **Usar a senha abaixo**: O administrador da rede pode optar por usar a base de dados do próprio **Winconnection 6** para fazer a sua administração. Para tanto, basta usar a opção "*Usar a senha abaixo*" e inserir a senha do usuário.

Endereço IP/Host: Neste campo é necessário digitar o endereço IP da máquina do usuário. Esta opção serve para que o usuário não precise digitar o seu login e a sua senha para navegar (quando é exigida autenticação) e enviar e-mails. Ao receber uma conexão, o servidor procura na lista de usuários, o usuário que é o "dono" do IP indicado no campo "Endereço IP ou host" e a autenticação é feita automaticamente.

Endereço MAC: A autenticação será feita com base no endereço MAC do computador do usuário.

Combinações das opções citadas acima também poderão ser utilizadas para a autenticação do usuário, por exemplo: Senha e Endereço IP/Host, Senha e Endereço MAC, etc.



Guia Novo | Aviso de Férias:

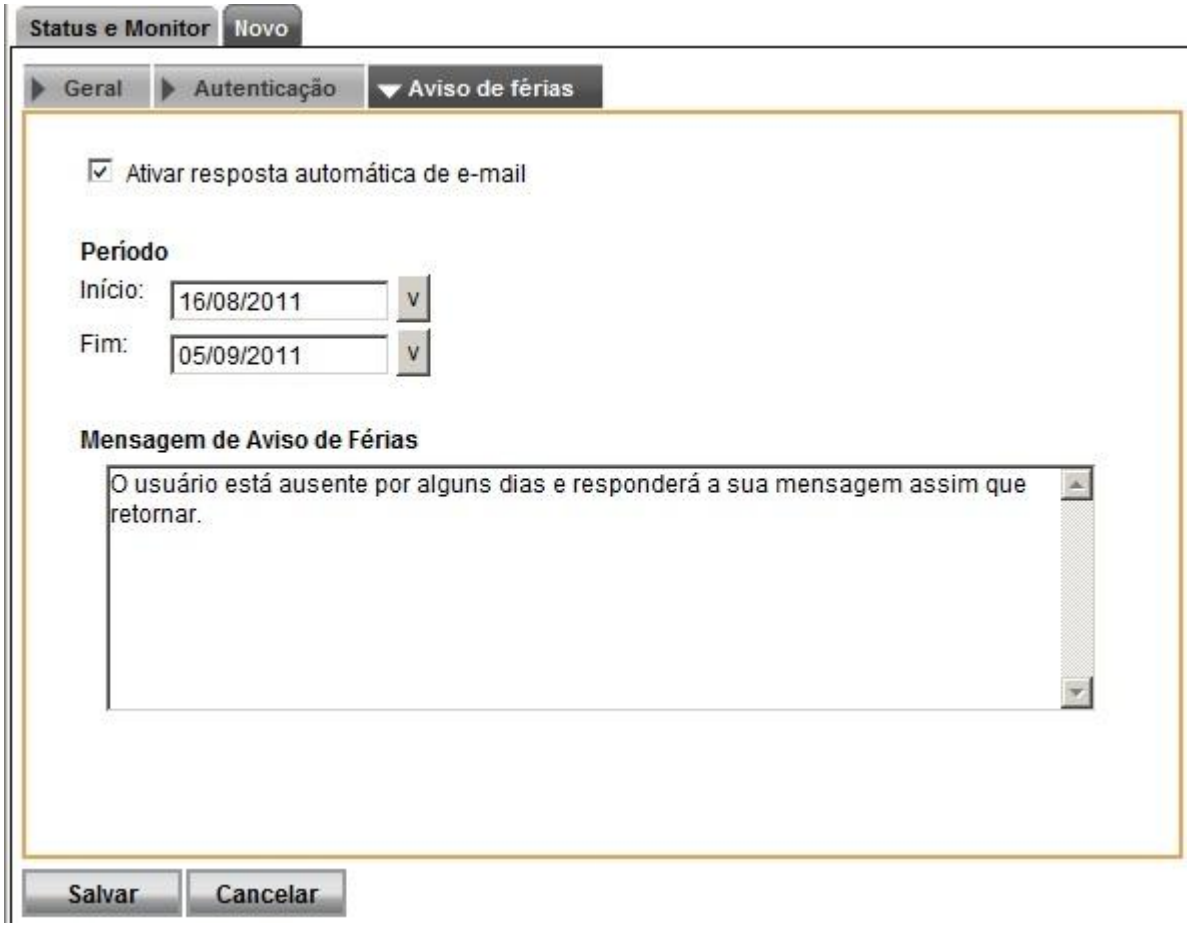
A guia *Aviso de Férias* permite que o administrador da rede configure um aviso para quando o usuário estiver de férias ou incapacitado de receber e-mails e não puder retornar

as mensagens para ele enviadas.

Para isso, basta habilitar a opção "*Ativar resposta automática de e-mail"*.

No campo *Período* é possível definir o intervalo de dias que a mensagem de resposta automática estará disponível.

No campo *Mensagem de Aviso de Férias* digite o texto que o remetente receberá ao mandar uma mensagem ao destinatário do **Winconnection 6**. Esse texto pode ser alterado a qualquer momento.



5.2. Grupos

Para facilitar a utilização do produto, a administração das políticas de segurança, acesso, regras etc., pode ser efetuada por grupos. Este mecanismo sugere ao administrador priorizar a distribuição dos privilégios e acessos aos grupos e não usuários, massificando as ações de controle. Seguindo esta regra, quando um usuário necessita de um determinado acesso ou privilégio, o administrador atribui o usuário como pertencente ao

grupo que detém este privilégio.

O ganho de produtividade com esta técnica advém do fato de que determinadas políticas de segurança nunca dependem da atribuição de um único privilégio, mas sim de um conjunto deles. Quando na aplicação da mesma política a diferentes usuários, a probabilidade de o administrador esquecer ou errar a atribuição de parte dos privilégios para um novo usuário é razoável. Ao passo que apenas atribuir o usuário a um determinado grupo é muito simples e *autodocumentada*. Não há nenhuma limitação na administração do produto por intermédio de privilégios aos usuários diretamente, a técnica de administração por grupos é apenas uma recomendação.

O **Winconnection 6** vem com 3 grupos básicos previamente cadastrados:

- **Administradores**: É o grupo que contém os usuários com maiores direitos dentro do **Winconnection 6**. Pelo sistema, estes usuários podem até logar. no Administrador do Winconnection, gerenciando assim direitos dos outros usuários. Recomenda-se que o acesso a este grupo seja restrito à equipe de TI.

- **Usuários Comuns**: São aqueles com direitos gerais sobre acesso aos sites. A real permissão do uso, por parte destes usuários, será dado pelo Administrador quando escolher quais grupos tem acesso à quais serviços.

- **Usuários Restritos**: São aqueles que terão restrições de acesso (por exemplo, em determinados sites). O administrador da rede deve cadastrar aqui quem não tem acesso ou tem um acesso limitado a determinadas partes na internet.

Note que não existem diferenças no sistema entre os grupos *Usuários Comuns* e *Usuários Restritos*. A política que o administrador da rede adotar de bloqueios e restrições será a que vale para a rede.

Guia Status e Monitor:

Nessa guia de configuração são exibidas informações sobre os grupos que já foram cadastrados.

Guia Novo | Geral:

Grupo:

Neste campo é necessário digitar o nome e a descrição do grupo.

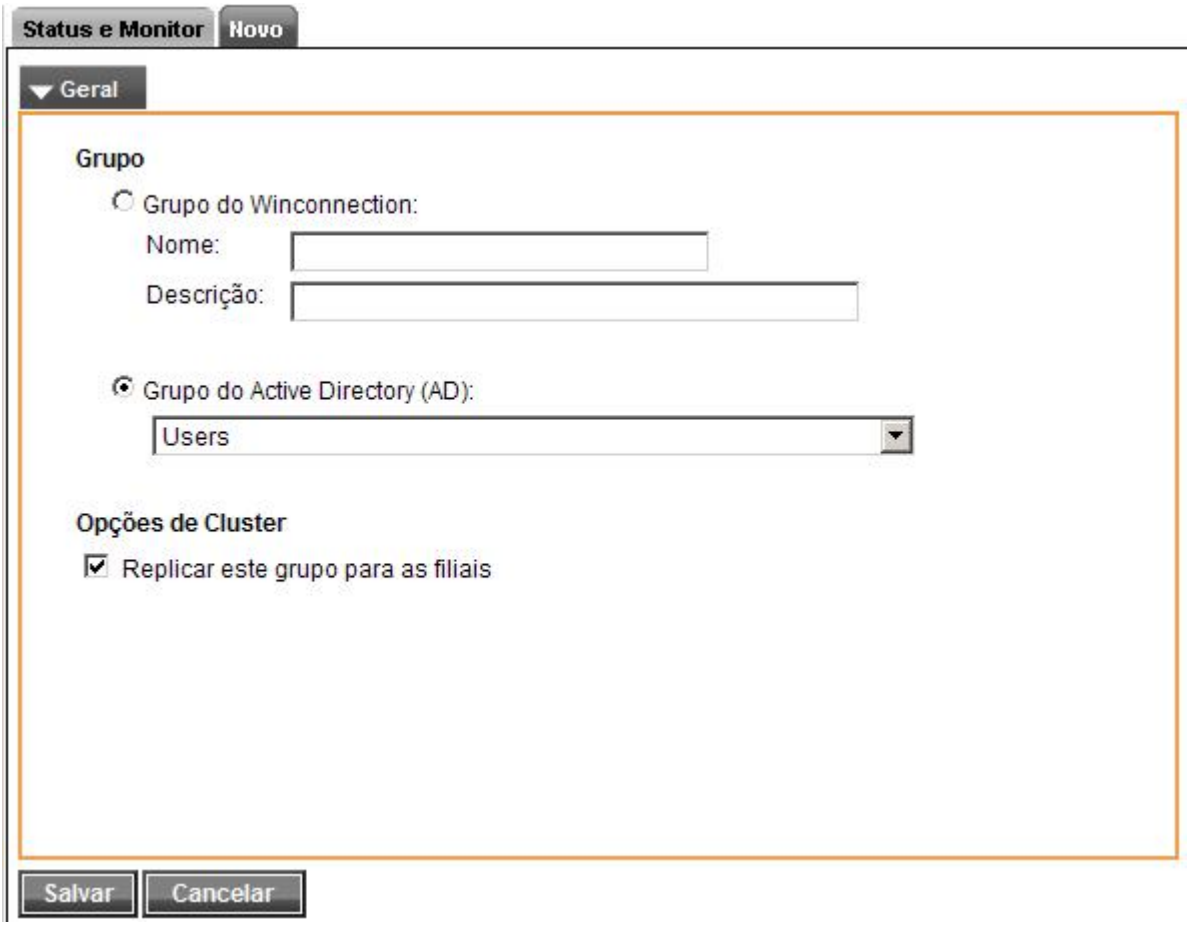
Grupo do Active Directory (AD):

O administrador da rede poderá selecionar um grupo de usuários do *Active Directory* (AD).

Obs.: É necessário habilitar a opção *"Ativar Autenticação de Domínio",* disponível no menu *Usuários → Configurações.* Para mais informações, consulte o capítulo Usuários.

Opções de Cluster:

Essa opção deve ser habilitada se o administrador da rede desejar que esse grupo de usuários seja replicado para as filiais (caso o serviço de replicação das regras globais de acesso à internet esteja sendo utilizado). Para mais informações sobre esse serviço, consulte o capítulo Cluster Master.



5.3. Painel do Usuário

O *Painel do Usuário* permite que aos usuários da rede tenham acesso as seguintes configurações: *Quarentena*, *Aviso de Férias*, *Regras de Acesso à Web*, *Relatório de Acesso a Web*.

Além disso, ao acessar o *Painel de Usuário* é exibida a opção para o usuário efetuar o log off.

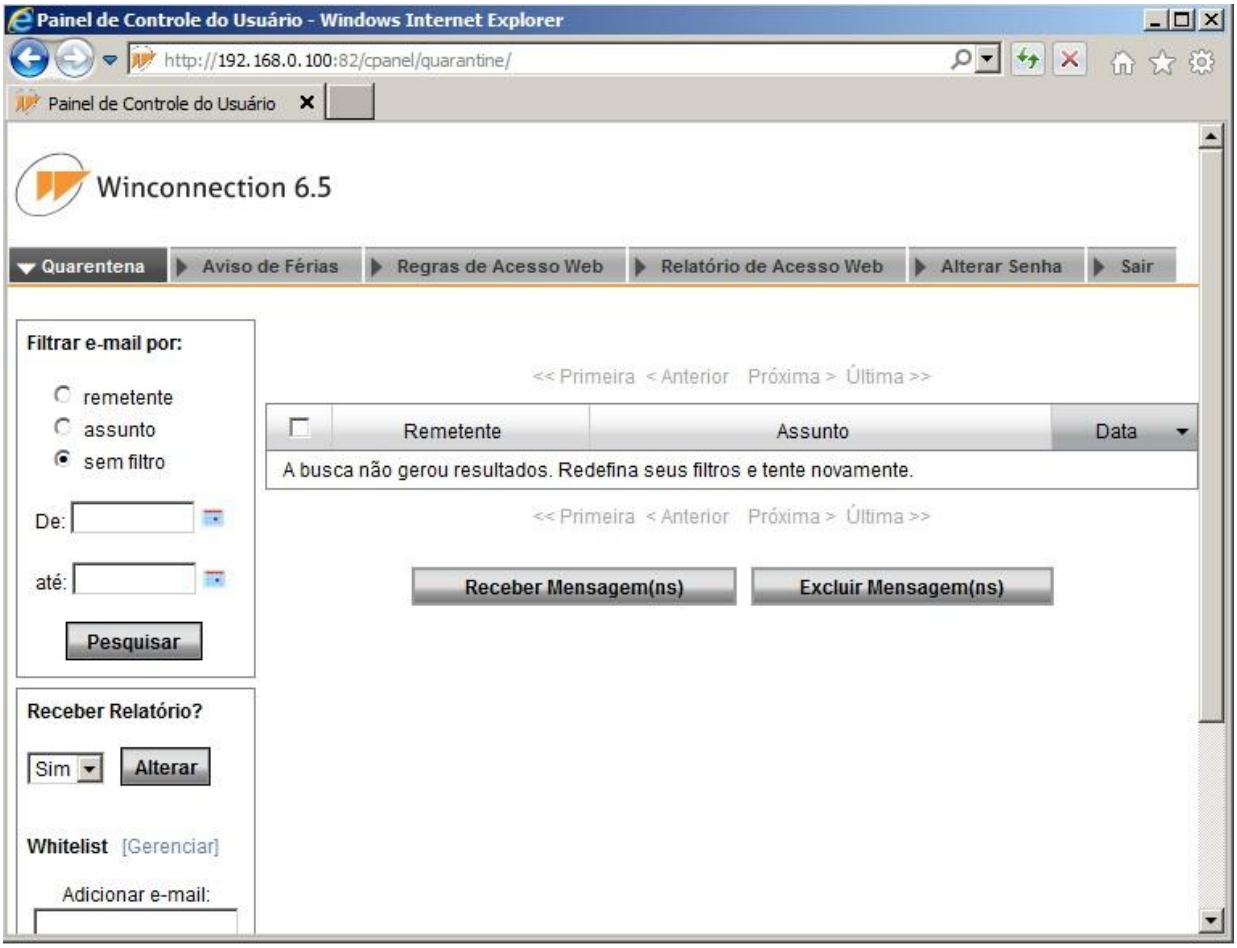
Para acessá-lo, basta digitar o seguinte endereço no navegador: http://ip_do_servidor/cpanel.

Por padrão, o acesso é feito na porta 80, mas pode ser alterada no serviço *Web*.

Guia Quarentena:

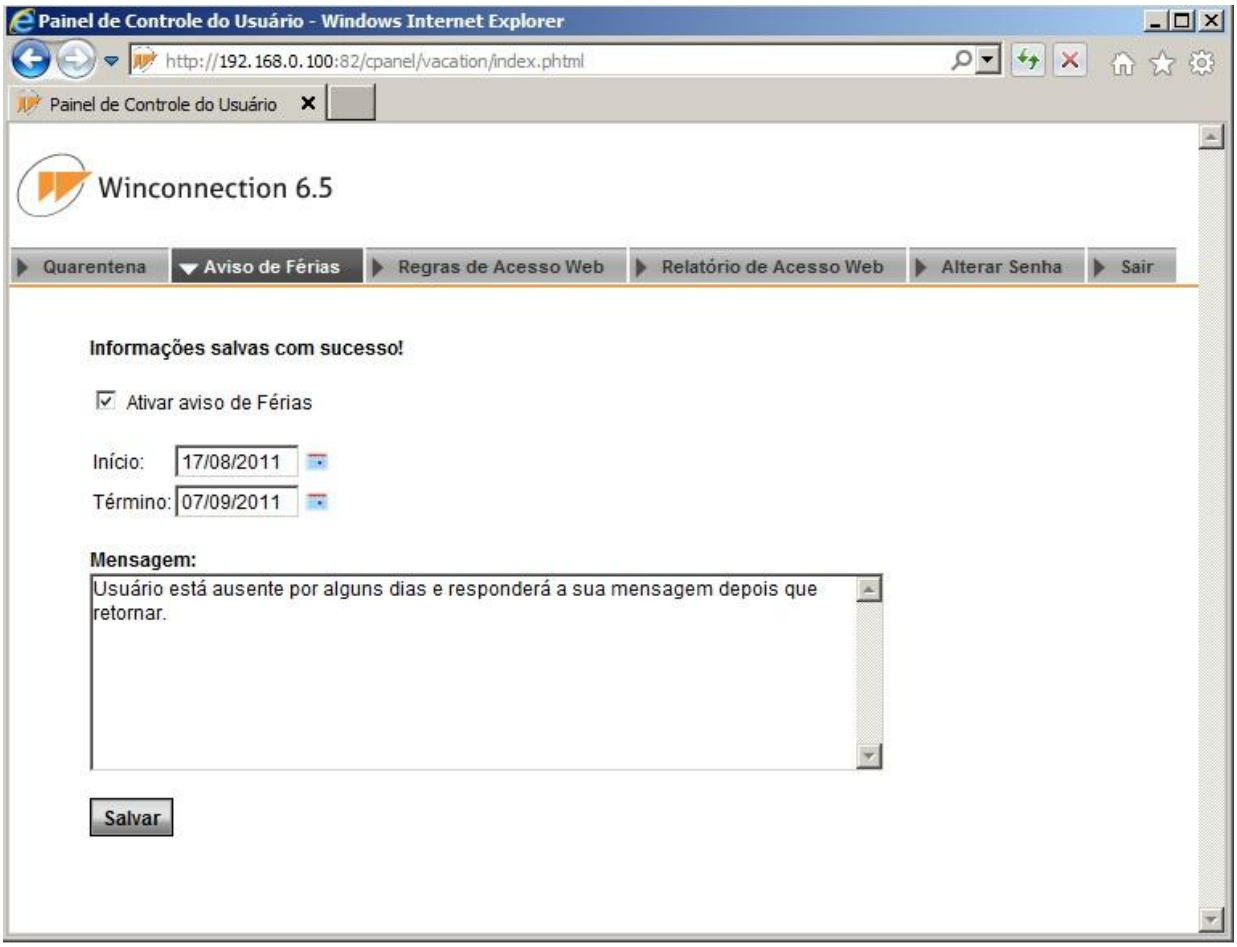
Conforme a configuração do administrador da rede, uma mensagem poderá ser enviada para a quarentena por meio de uma ou mais regras.

No **Winconnection 6**, a fila de quarentena de cada usuário pode ser gerenciada pelo próprio, que pode apagar, liberar mensagens da quarentena ou ainda, adicionar um endereço de e-mail em sua *Whitelist*. O administrador do sistema pode acessar a fila de quarentena de todos os usuários, mas não pode manipular os endereços de *Whitelist*.



Guia Aviso de Férias:

Nesta guia, o usuário poderá definir o período que o aviso ficará ativo e criar a sua própria mensagem de aviso de férias.



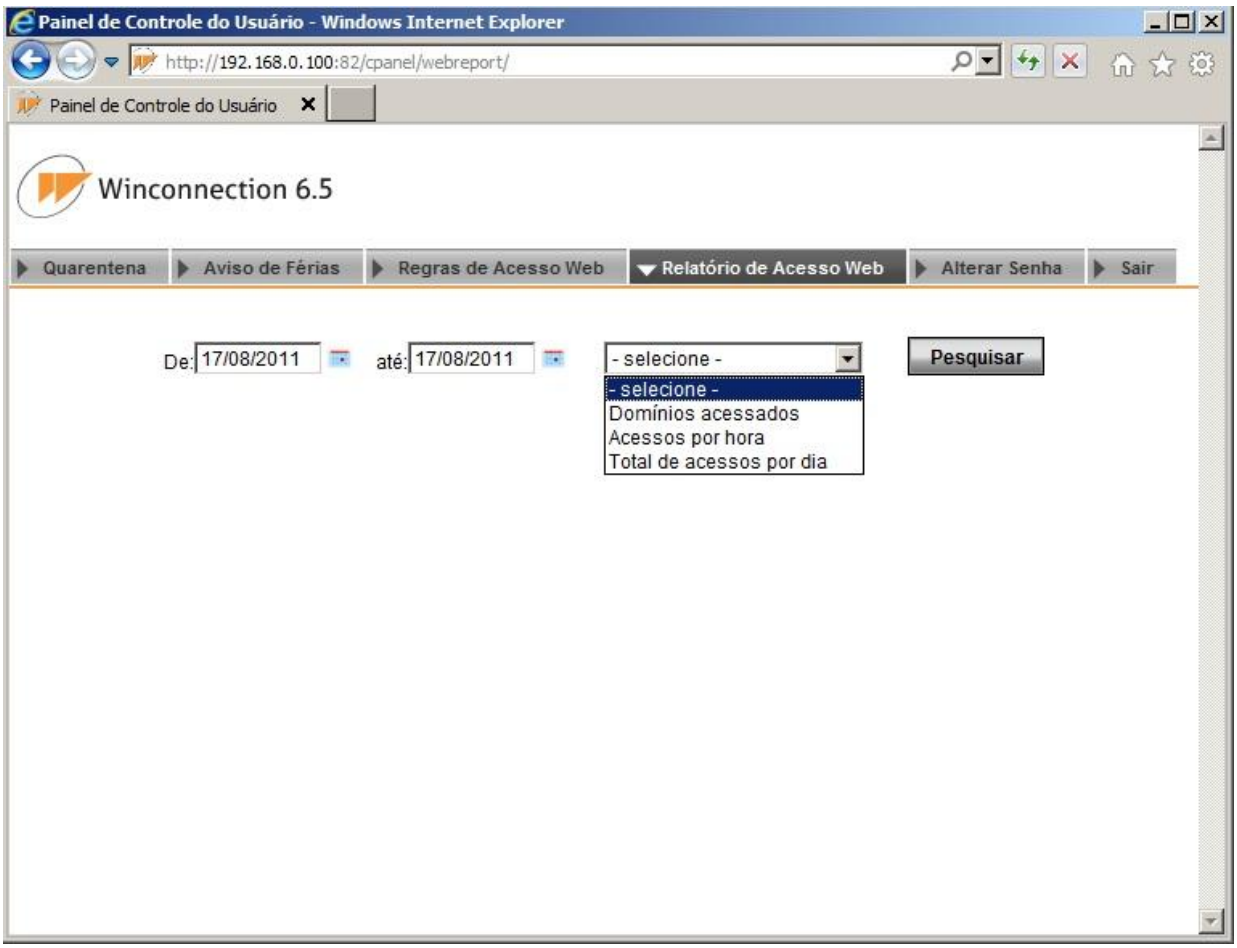
Guia Regras de Acesso a Web:

Nesta guia, é possível visualizar as regras de acesso que o usuário fez uso até o momento do acesso desta guia.

Regra	URLs	Tempo de navegação		Transferência de bytes	
		Permitido	Utilizado	Permitido	Utilizado
#2	*wintrade* *bastter* *tesouro.direto* finance.google.com	Ilimitado	8 min	Ilimitado	555 KB

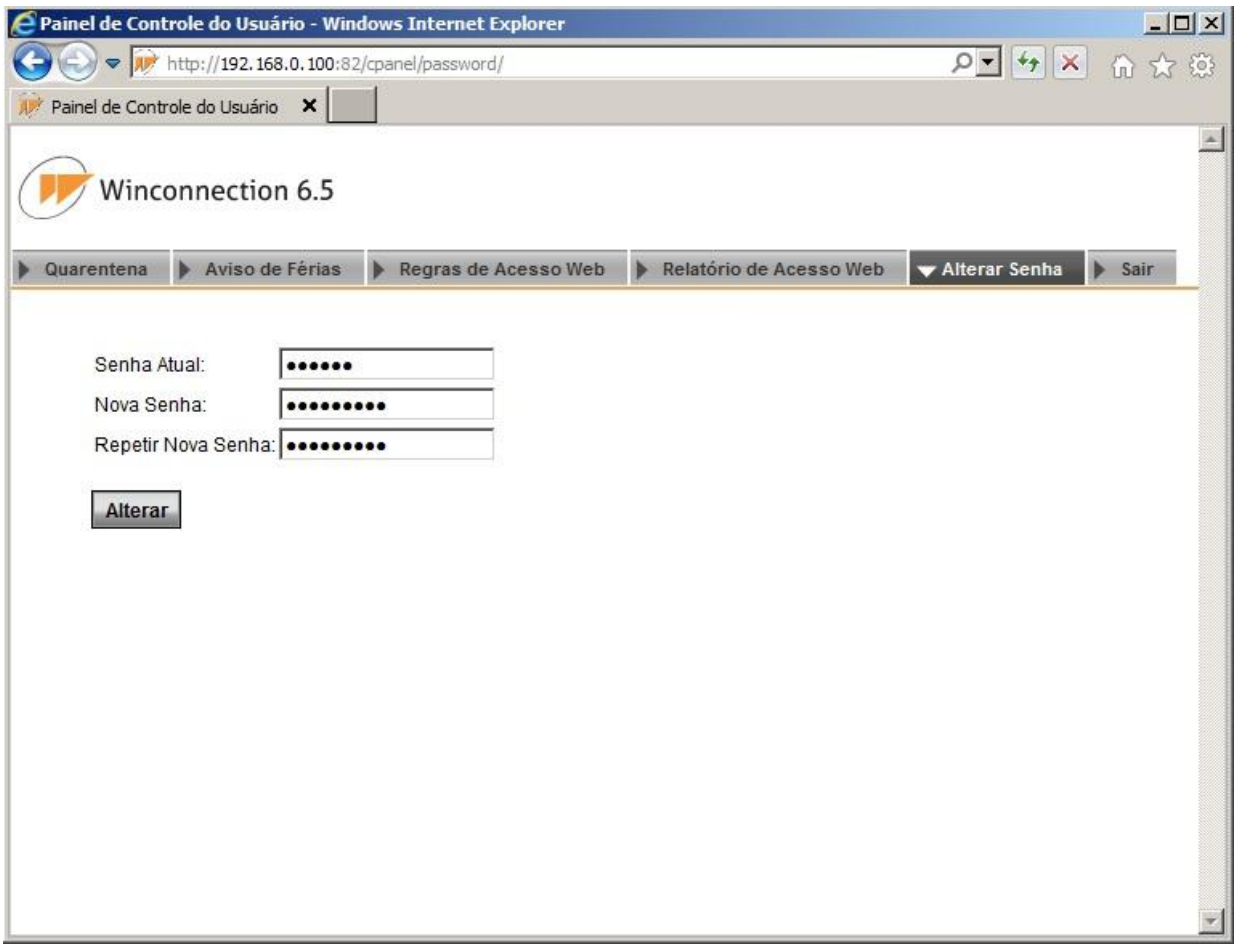
Guia Relatório de Acesso a Web:

Nesta guia, o usuário poderá visualizar o seu relatório de acesso a Web.



Guia Alterar Senha:

Esta guia permite que o usuário altere a sua senha de autenticação.



6. Firewall

O Firewall do **Winconnection 6** permite deixar o computador seguro contra ataques de hackers.

Por padrão o produto vem configurado de forma a proteger todas as interfaces classificadas como externas, filtrando pacotes de origem externa, bloqueando todas as portas. Quando outros serviços são habilitados dentro do produto, as respectivas portas externas, necessárias ao funcionamento dos serviços, são automaticamente liberadas.

Para uma segurança maior, é recomendada a manutenção do sistema operacional sempre atualizado, aplicando-se com frequência os pacotes de atualização de segurança.

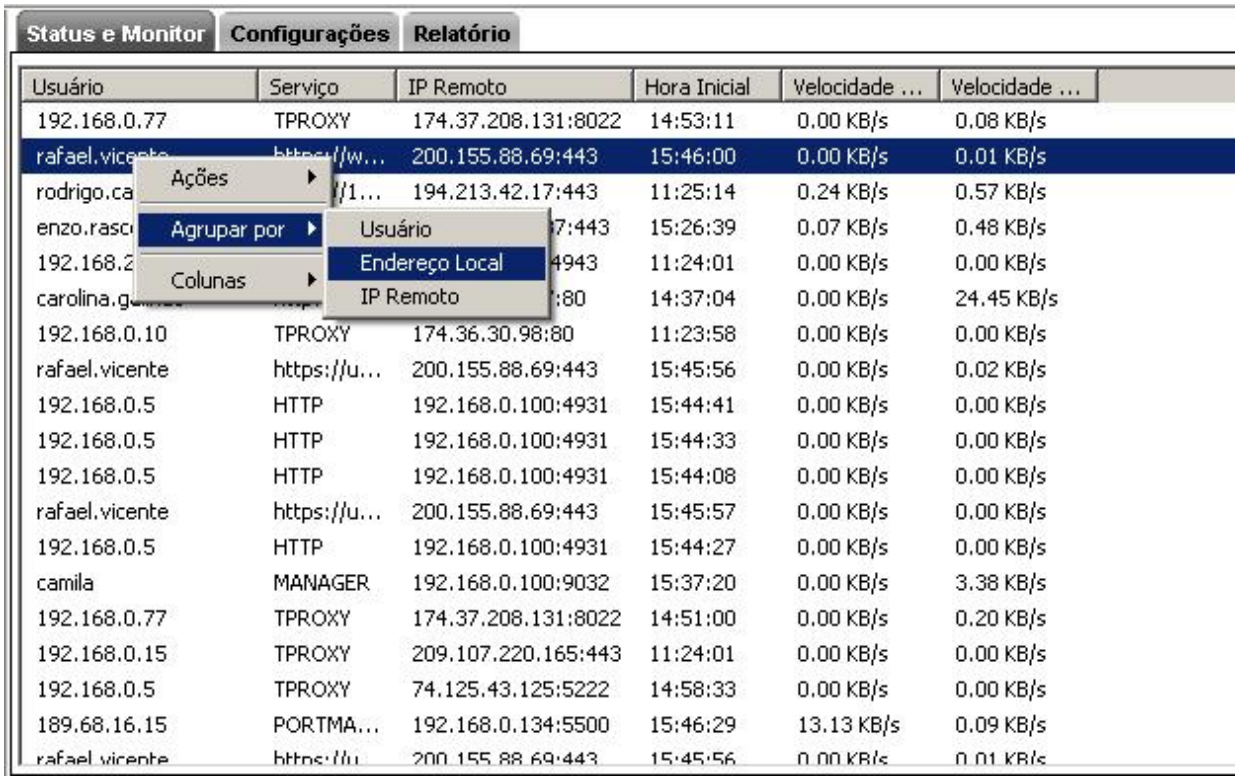
Guia Status e Monitor:

Essa guia exibe informações de conexões de entrada e saída de dados.

As seguintes informações sobre as conexões poderão ser exibidas: *Usuário, Serviço, IP Remoto, Hora Inicial, Velocidade de Upload, Velocidade de Download, ID, Endereço Local, Protocolo, Bytes Recebidos* e *Bytes Enviados*.

Clicando com o botão direito do mouse sobre uma conexão, o **Winconnection 6** disponibiliza das seguintes opções:

- **Ação:** Fecha a conexão selecionada.
- **Agrupar por:** Agrupa as conexões por *Usuário,* por *Endereço Local* ou por *IP Remoto*.
- **Colunas:** Mostra as opções de colunas que poderão ser exibidas.



Guia Configurações | Geral:

- **Habilitar Filtro de Pacotes:** Habilitando esta opção, o filtro de pacotes do Winconnection 6 será ativado.

- **Permitir que os programas deste computador acessem toda a internet:** Caso esta opção não seja habilitada, o acesso a programas na internet neste computador será bloqueado, porém, isso impedirá até o software antivírus seja atualizado.

- **Responder a requisições de PING (ICMP ECHO):** Habilita o computador protegido a responder (quando solicitado) aos pings externos.

- **Permitir configuração de interface externa via DHCP:** Esta opção deve ser habilitada quando uma das conexões com a internet fazer uso de IP Dinâmico.

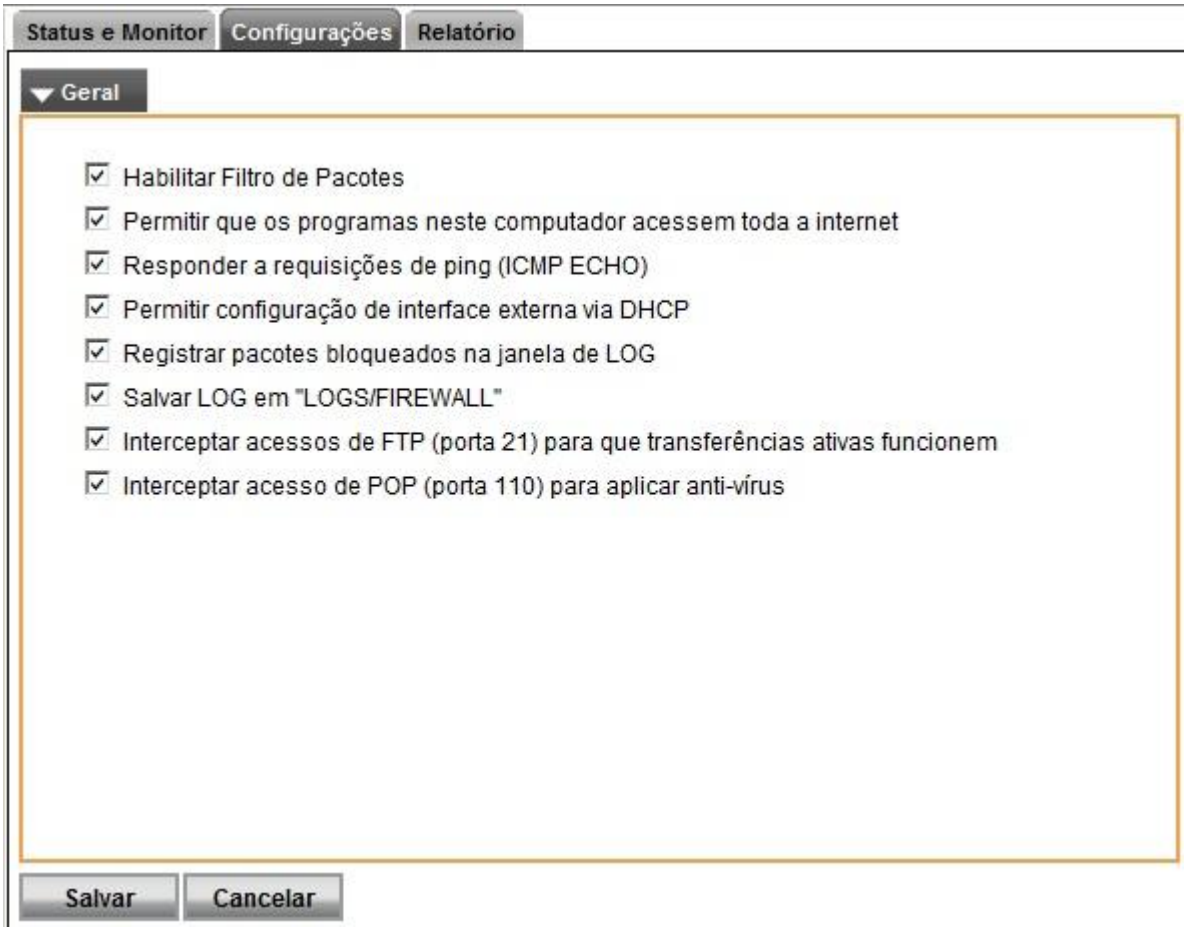
- **Registrar pacotes bloqueados na janela de LOG:** Todos os pacotes bloqueados serão exibidos na janela de log do administrador do **Winconnection 6**.

- **Salvar log em "LOGS/FIREWALL":** O arquivo em bloco de notas (FIREWALL.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referente ao

serviço Firewall.

- **Interceptar acessos de FTP (porta 21) para que as transferências ativas funcionem:** É necessário ativar esta opção para que todos os acessos a Servidores FTP possam ter um acesso transparente, ou seja, configura-se o cliente FTP como se estivesse conectado diretamente à internet.

- **Interceptar acesso de POP (porta 110) para aplicar anti-virus:** É necessário ativar esta opção para que as regras criadas no Filtro de E-mail (guia Anti-Virus) sejam aplicadas corretamente.

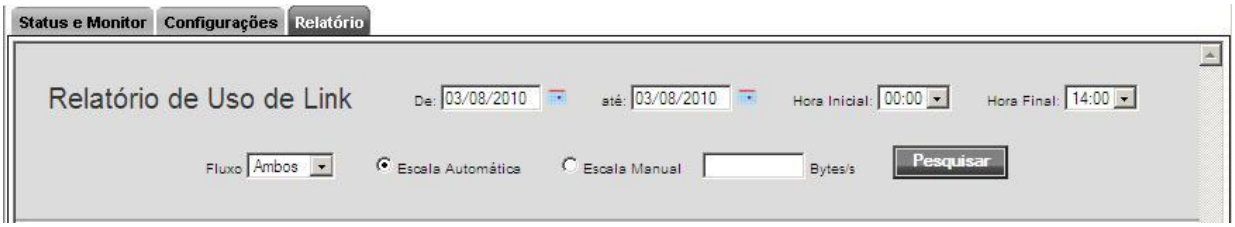


Guia Relatório:

A função do *Relatório de Uso de Link* é demonstrar como está o fluxo de dados destinados à internet dentro do **Winconnection 6**. Este relatório é particularmente útil quando o administrador da rede precisa analisar eventuais sobrecargas nos links da internet e onde exatamente o existe a sobrecarga do link.

Para análises de datas e horários específicos, o módulo de consulta permite escolher horários/quantidade de dias de acordo com a necessidade do administrador.

A escala do gráfico pode ser alterada pelo usuário, caso a escala automática não seja adequada.



Obs.: Também é possível acessar o relatório *Uso de Link* através do navegador, acessando o endereço: *http://ip_do_servidor/relatorio*. Após se logar no Gerador de Relatórios, selecione a opção *Relatórios → Uso de Link.*

6.1. Interfaces

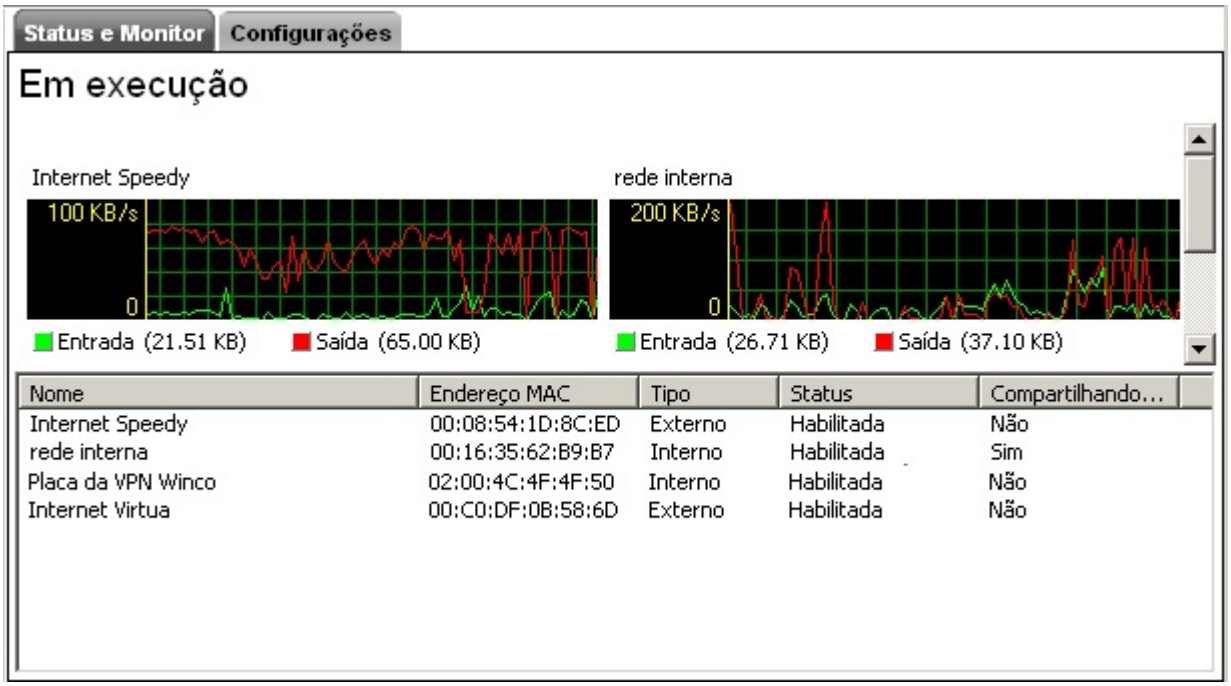
O **Winconnection 6** classifica as interfaces de rede em dois grupos: *Internas* e *Externas*. A partir desta classificação, são adotados dois comportamentos distintos.

As *Interfaces Internas* não são protegidas por filtros de pacotes e são destinadas a disponibilizar serviços aos usuários da Rede Interna. As *Interfaces Externas* são usadas para conexão com a Internet. Nelas são ativados filtros de pacotes quando o *Firewall* está ligado e participam do esquema de *Balanceamento de Carga* e *Controle de Banda*, quando os filtros estão ativados.

As seções abaixo mostram as configurações aplicáveis às interfaces de rede.

Guia Status e Monitor:

Esta guia de configuração permite configurar as interfaces de rede disponíveis no computador.



Clicando com o botão direito do mouse sobre uma interface e em seguida, clicando em *Propriedades*, o **Winconnection 6** disponibiliza as seguintes informações:

Guia Propriedades | Geral:

Resumo da Rede: Exibe um resumo de informações (Nome, Mac, Tipo de mídia, Status) da interface de rede selecionada.

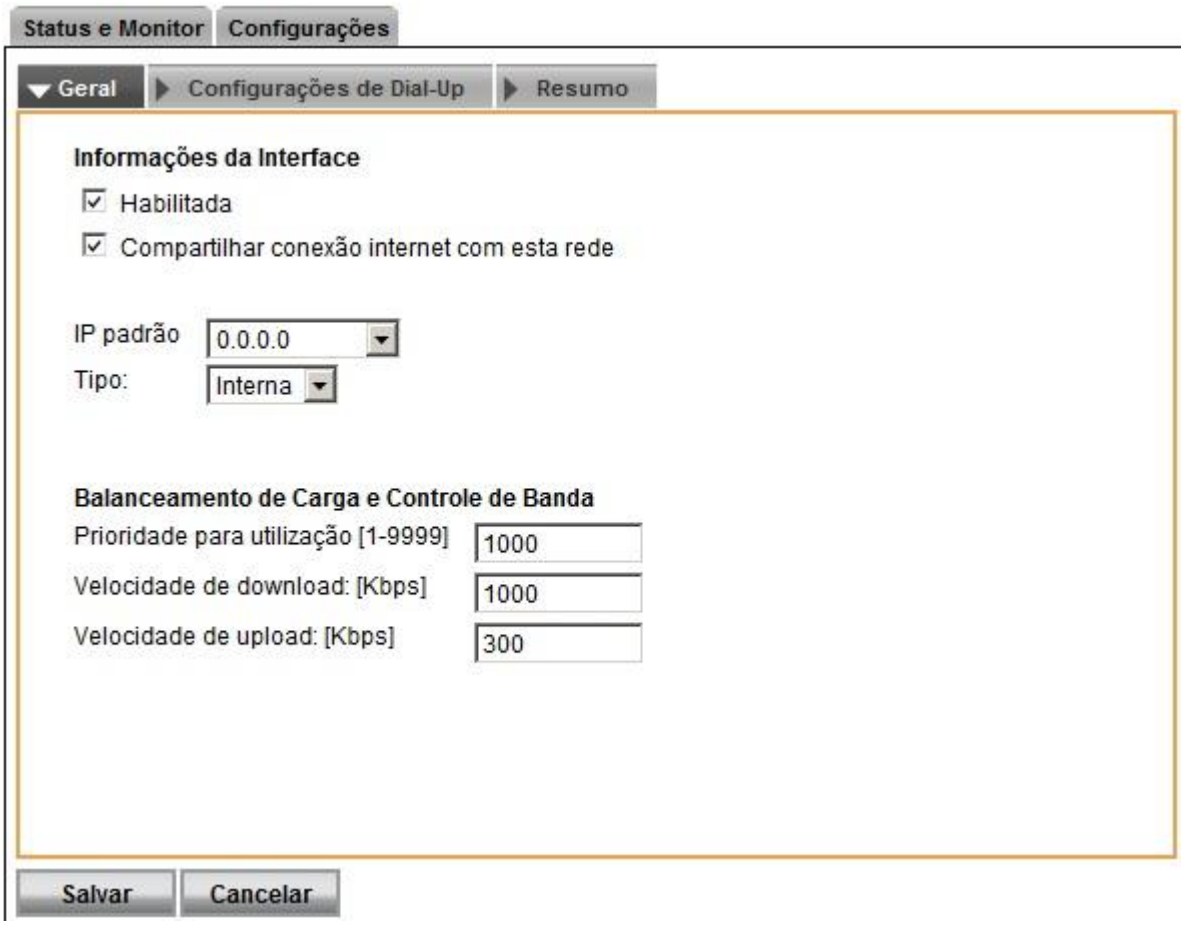
Informações da Interface:

- **Habilitada**: Habilita a utilização da interface de rede selecionada.

- **Compartilhar conexão internet com esta rede:** Se esta opção estiver habilitada, o **Winconnection 6** irá compartilhar as conexões de internet através desta interface. Esta configuração deve ser apenas atribuída às interfaces classificadas como internas.

- **Tipo:** Define o tipo da interface de rede (interna ou externa).

Balanceamento de Carga e Controle de Banda:
Neste campo, o administrador da rede poderá definir o balanceamento de carga e controle de banda para a interface de rede selecionada. As seguintes opções de configurações estão disponíveis: *Prioridade para utilização*, *Velocidade de download* e *Velocidade de upload*.



<u>Guia Propriedades | Configurações de Dial-Up:</u>

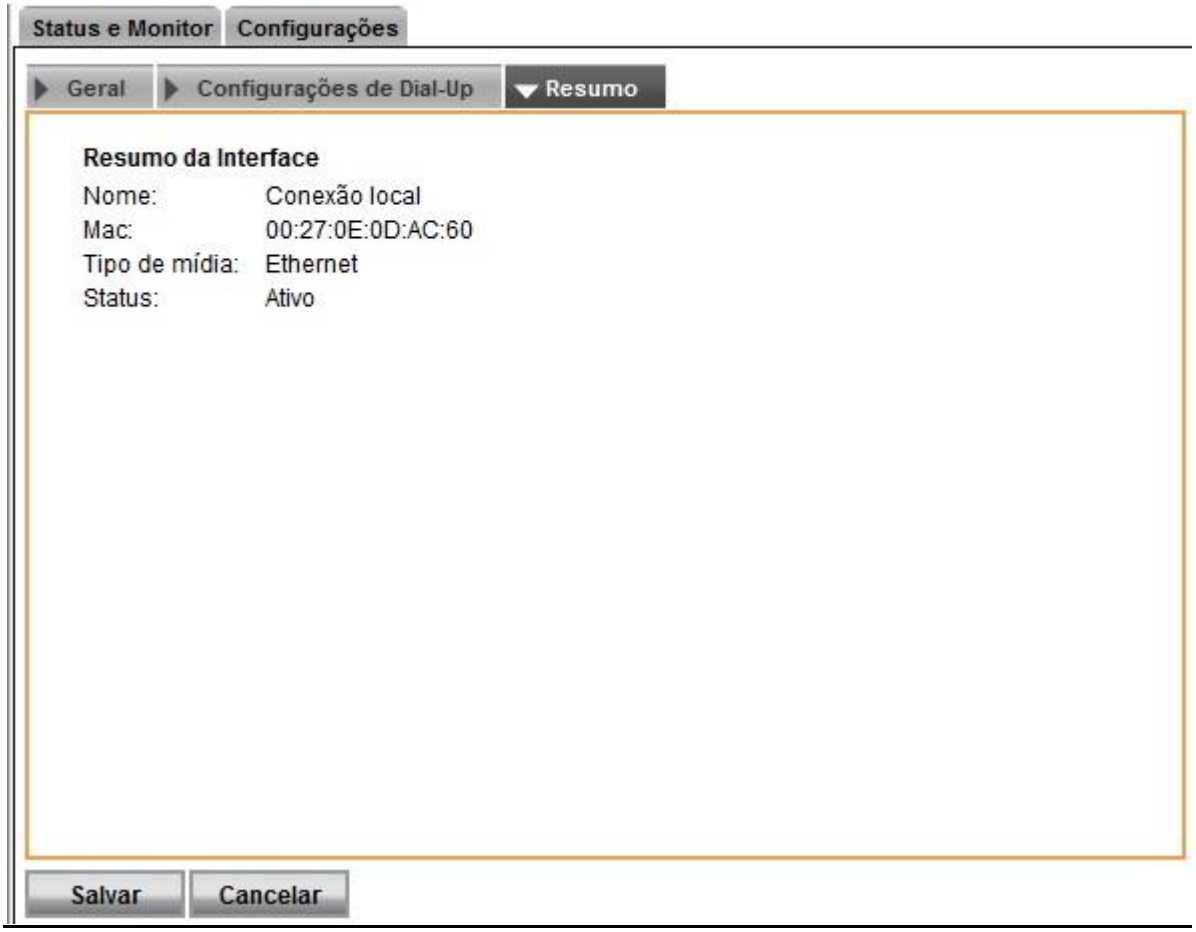
O gerenciador de conexões de internet conecta automaticamente o computador na interface de rede selecionada se a opção *Usar a Dial-Up* estiver habilitada.

Este recurso é útil quando a conexão da rede é feita via modem ou via protocolo *PPPoE*, em que é necessário discar uma conexão para se ter o acesso.

São solicitados *Nome do Usuário* e *Senha* para o gerenciamento, conforme figura abaixo:

Guia Propriedades | Resumo:

Exibe um resumo da interface.



Guia Configurações:

Esta guia de configuração exibe informações sobre as interfaces e permite configurar as interfaces de saída e o comportamento do balanceamento de link.

Esta opção permite ao **Winconnection 6** gerenciar duas ou mais conexões de internet. Com o balanceamento ativado, a todo o momento uma das interfaces externas é escolhida para realizar uma dada conexão demandada. A escolha é baseada nos parâmetros operacionais escolhidos para o balanceamento, descritos adiante. Além disso, o **Winconnection 6** faz uma análise de cada link externo, para avaliar se ele está em funcionamento ou não. Caso seja detectada alguma falha de comunicação, a respectiva interface é classificada como inativa ou falha. Nesta condição ela não mais participa do processo de escolha de interfaces descrito anteriormente. Isto traz ao produto características de tolerância a falha no que tange a quedas de links, uma vez que a máquina será mantida sempre conectada à Internet através dos demais links que restaram em funcionamento.

Esta característica é diferente dos processos usuais de tolerância a falhas baseadas em substituição de links falhos por links em funcionamento ("hot-stand-by"). A principal vantagem é o aproveitamento maior de todos os recursos (links) que estiverem funcionan-

do, mantendo-os em atividade o máximo de tempo possível.

Embora alguns usuários percebam que algumas conexões caiam no exato momento da falha de um determinado link, este processo por muitas vezes traz uma boa sensação de continuidade operacional.

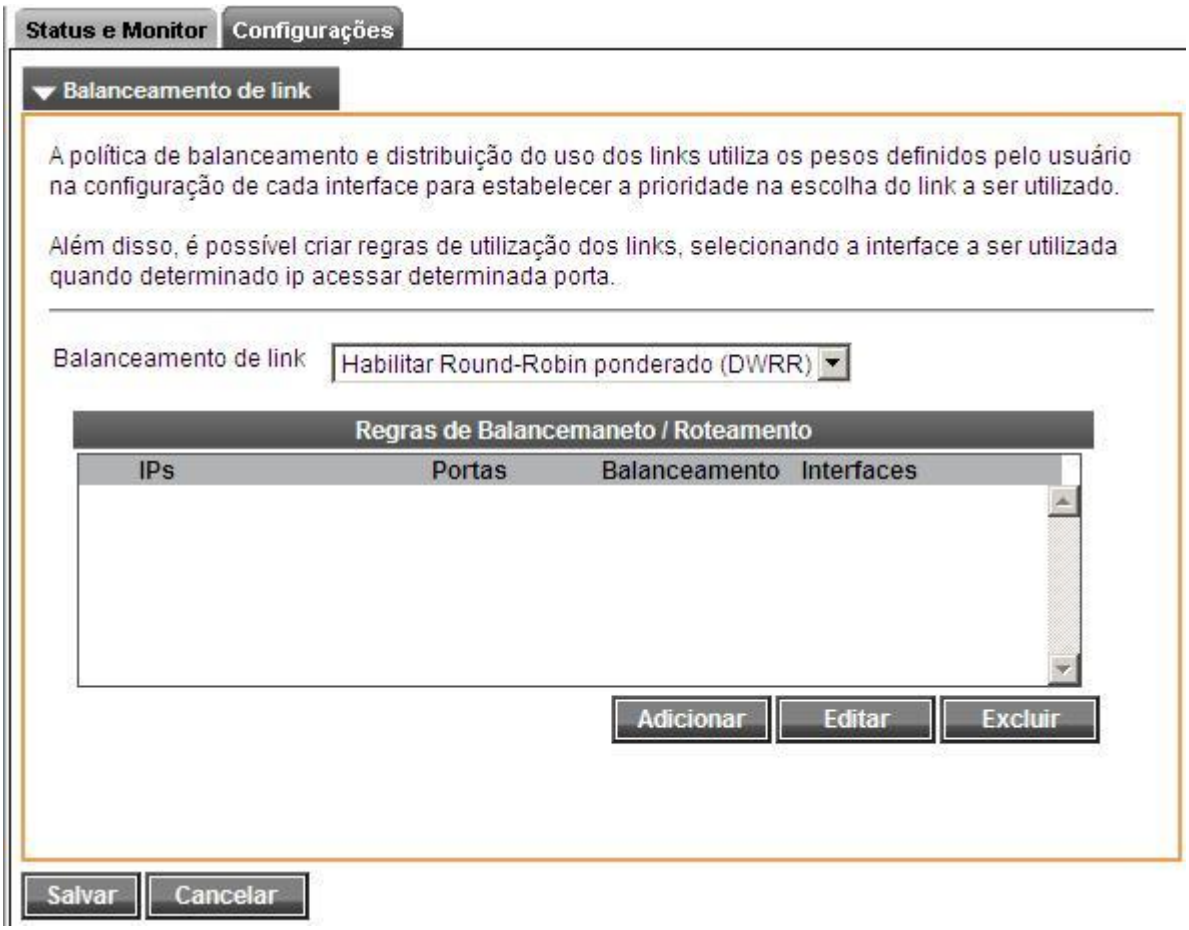
A política de balanceamento e distribuição do uso dos links utiliza os pesos definidos pelo administrador da rede na configuração de cada interface para estabelecer a prioridade na escolha do link a ser utilizado.

Balanceamento de Link:

- **Desabilitado:** Desabilita o balanceamento do link.

- **Habilitar Balanceamento de Link (WRR):** A política de balanceamento e distribuição de uso dos links utiliza o modelo "*Round Robin Ponderado por Pesos* (*WRR Weighted Round Robin)"*. Esta modalidade utiliza os pesos definidos pelo usuário, na configuração de cada interface, para estabelecer a prioridade na escolha dos links.

- **Habilitar Round-Robin ponderado (DWRR):** Como a política simples apenas baseada nos pesos pode ser insuficiente para uma justa partilha de uso dos links, uma política mais dinâmica pode ser estabelecida. Ela é conhecida como "*Round Robin Ponderado por Pesos com Pesos Dinamicamente Ajustados* (*DWRR Dynamic Weighted Round Robin*)". Ela se baseia no ajuste dos pesos estabelecidos pelo administrador da rede através de medições da capacidade ociosa dos links, ou seja, quanto mais utilizado um link, menor sua capacidade ociosa, portanto, o peso fornecido pelo administrador é diminuído e a partilha dos links é feita sobre os pesos "efetivos" assim calculados. Para que funcione corretamente, é necessário que a caracterização dos links quanto a peso e velocidade seja feita com cuidado.



É possível definir regras de utilização dos links, selecionando a interface a ser utilizada quando determinado endereço IP acessar determinada porta.

Veja um exemplo de regra na imagem abaixo:

Note que é possível atribuir mais de uma interface para uma regra de balanceamento. Quando assim configurado, toda vez que a regra for aplicada, um dos links é escolhido, com a vantagem de que os mesmos continuam sendo balanceados, mas apenas entre aqueles contidos na regra.

Além disso, pode-se escolher se a regra usa "apenas" ou "preferencialmente" os links listados. Na primeira forma, se todos os links da lista estiveram inativos, ou falhos, a conexão não poderá acontecer, gerando um erro de acesso. Ao passo que quando a regra usa "preferencialmente" a lista de links, na mesma situação de falha de todos os links da lista, qualquer link associado a uma interface classificada como externa será selecionado.

As regras de balanceamento permitem a escolha de links próprios para determinadas aplicações. Por exemplo, se os links forem de igual tamanho, mas um deles possuir uma latência maior pode-se determinar através das regras de balanceamento, que todos os pacotes de VOIP direcionados a um determinado servidor sigam pelo link de menor latência.

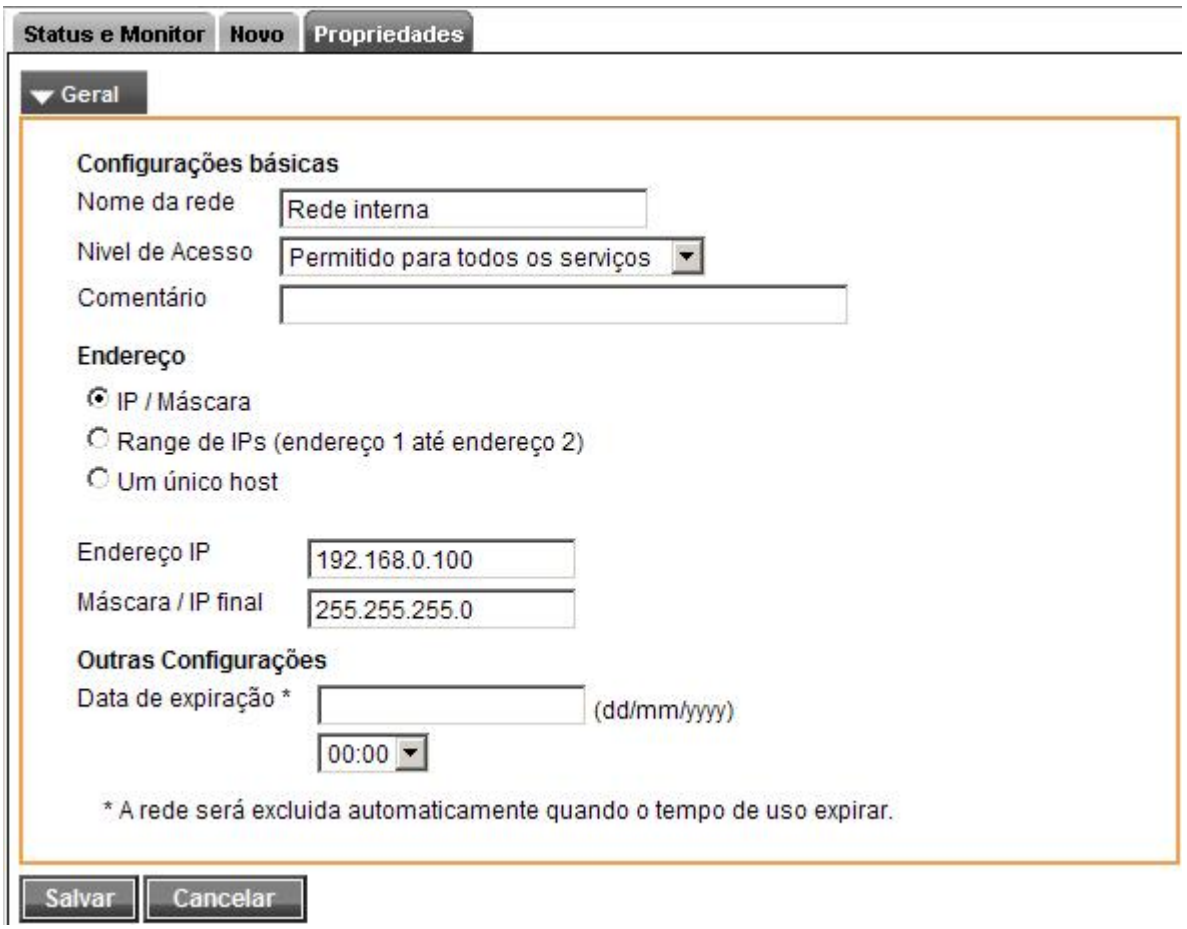
6.2. Redes Lógicas

O **Winconnection 6** tem um conceito bastante abrangente de **Redes e Acessos** permitidos aos serviços.

A instalação padrão tem um algoritmo que calcula e permite que o acesso dos computadores da Rede Interna, seja configurado por cada serviço pré-instalado formando uma *Regra de Acesso.*

Por sua vez, todos os serviços têm acesso garantido à *Regra de Acesso* criada para a Rede Interna. Isto permite uma instalação simples e segura que pode ser melhorada de acordo com a necessidade do Administrador.

A guia *Status e Monitor* exibe informações das redes lógicas que já foram criadas. Veja um exemplo da regra geral e básica do **Winconnection 6** na imagem abaixo:



Configurações básicas:

- **Nome da Rede:** Neste campo, é necessário definir o nome da rede que está sendo criada.

- **Nível de Acesso:** Indica ao **Winconnection 6** como os serviços internos se comportarão perante à *Regra de Acesso.* As seguintes opções estão disponíveis:

    - **Bloqueado para todos os serviços:** Bloqueia os serviços para o *Endereço de Rede*, seja ele o *Endereço IP / Faixas de IPs / Um único host.* Ou seja, os *Endereços de Rede* selecionados para a *Regra de Acesso* não terão acesso aos serviços do Winconnection 6.

    - **Configurado para cada serviço**: Cada serviço é habilitado pelo Administrador da rede como pertencente a esta *Regra de Acesso.* Isto permite filtrar os serviços de acordo com a real utilização do mesmo.

    - **Permitido para todos os serviços**: Com esta opção ativa, automaticamente todos os serviços funcionarão com o **Winconnection 6** sem maiores configurações. Em uma instalação padrão, esta é a opção que fica ativa, além de ser uma das que mais deve ser usada pelos administradores da rede.

- **Comentário:** Neste campo, é possível adicionar um comentário para a rede que está sendo criada/editada.

- **Endereço de Rede:**

  A opção **Endereço de Rede** indica ao **Winconnection 6** quais redes são permitidas nesta *Regra de Acesso*.

    - **IP /Máscara**: Este tipo de endereço de rede é o padrão de instalação do produto. Permite ao administrador da rede inserir o IP do Servidor Winconnection. A configuração mais comum é deixar o IP do Servidor / Máscara de sub-rede. Contudo, é possível alterar para qualquer máscara que melhor atenda à rede de modo a limitar os IPs de acesso.

    - **Faixas de IPs (endereço1 até endereço 2)**: Permite ao administrador da rede limitar somente uma faixa da rede, configurável pelo IP inicial até o IP final. É bastante útil quando se quer limitar algum ou todos os serviços para uma determinada faixa de rede.

- **Um único host**: Permite ao Administrador inserir o IP do único usuário que terá acesso ao servidor. Uma aplicação interessante é criar uma *Regra de Acesso*, por exemplo, onde somente determinado IP terá acesso ao serviço. Mas isto tem que ser configurado no Nível de acesso ao servidor (veja adiante).

- **Outras Configurações:**

  - **Data de expiração:** Permite que o administrador da rede defina uma data e hora para a expiração da rede que está sendo criada/editada. A rede será excluída automaticamente quanto o tempo de uso definido expirar.

6.3. Entrada

Guia Status e Monitor:

Essa guia exibe informações de conexões de entrada e saída de dados.

As seguintes informações sobre as conexões poderão ser exibidas: *Usuário, Serviço, IP Remoto, Hora Inicial, Velocidade de Upload, Velocidade de Download, ID, Endereço Local, Protocolo, Bytes Recebidos* e *Bytes Enviados*.

Clicando com o botão direito do mouse sobre uma conexão, o **Winconnection 6** disponibiliza as seguintes opções:

- **Ação:** Fecha a conexão selecionada.

- **Agrupar por:** Agrupa as conexões por *Usuário,* por *Endereço Local* ou por *IP Remoto*.

- **Colunas:** Mostra as opções de colunas que poderão ser exibidas.

Guia Configurações | Geral:

Esta guia exibe uma listagem de todas as regras de entradas criadas no Firewall e todas as regras de redirecionamentos de portas (portas mapeadas) criadas.

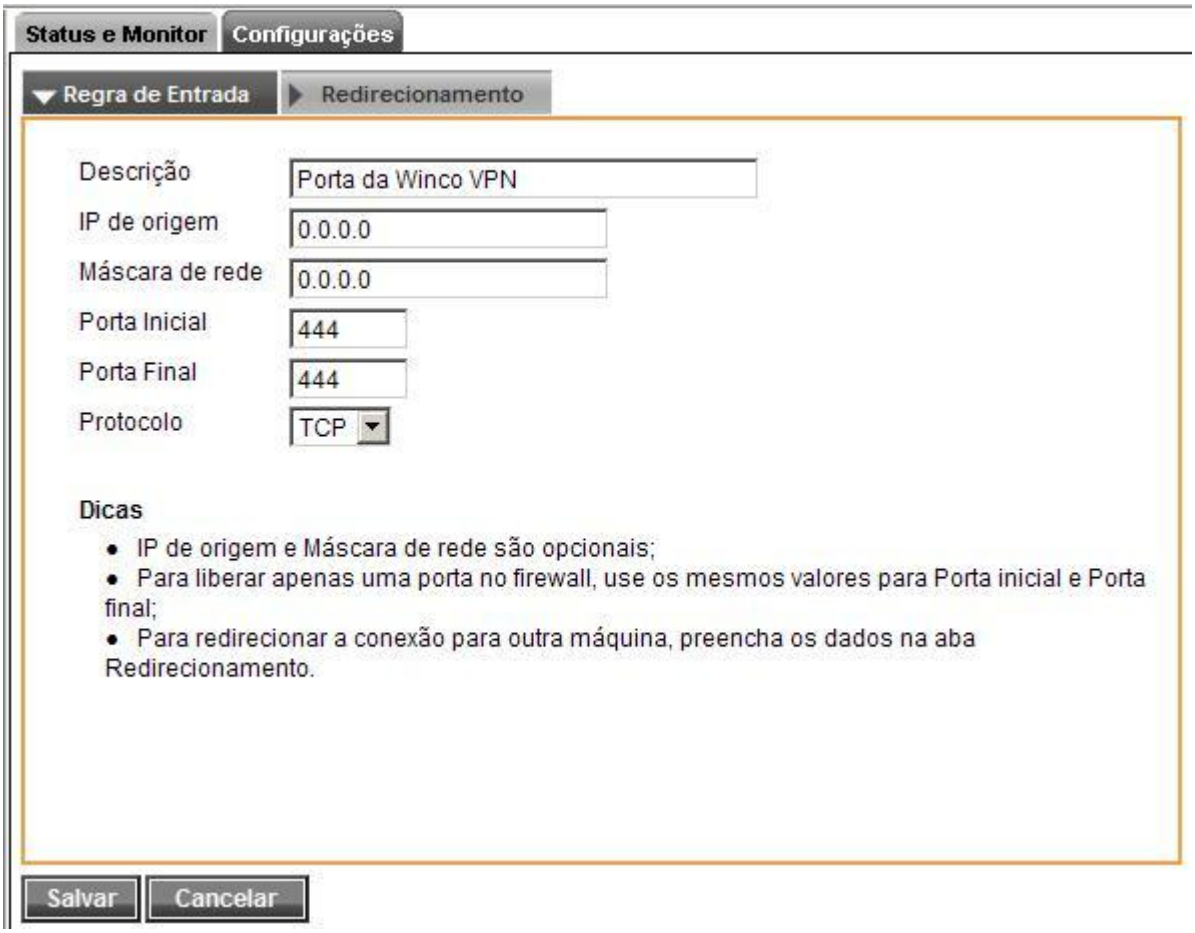
É possível *Adicionar*, *Editar* e *Excluir* as regras. Para isso, basta usar os respectivos botões.

Ao adicionar/editar uma regra, as seguintes opções estão disponíveis:

Guia Regra de Entrada: Exibe as opções para a criação/edição de uma regra de entrada:

- **Descrição:** Neste campo, é possível adicionar um nome para a regra.
- **IP de origem:** O administrador da rede deve informar nesse campo, o IP da conexão de entrada.
- **Máscara de Entrada:** É a máscara de rede do IP informado no campo *IP de Entrada*.
- **Porta Inicial:** É a porta inicial da conexão.
- **Porta Final:** É a porta final da conexão.
- **Protocolo:** Neste campo, é necessário informar o protocolo que será usado pela regra (TCP, UDP).

Veja um exemplo de configuração na tela a seguir. No exemplo, a *Porta TCP 444* (utilizada pela *VPN*) está sendo liberada no firewall do **Winconnection 6**.



Guia Redirecionamento: Esta guia é utilizada para possibilitar o acesso a serviços que não sejam padronizados, desde que se saiba o computador e porta a qual se deseja ter acesso.

Com este serviço instalado, sempre que um cliente conectar na *Porta (TCP/UDP)* do *PIPE* (mapeamento) do **Winconnection 6**, a conexão será redirecionada ao computador remoto especificado.

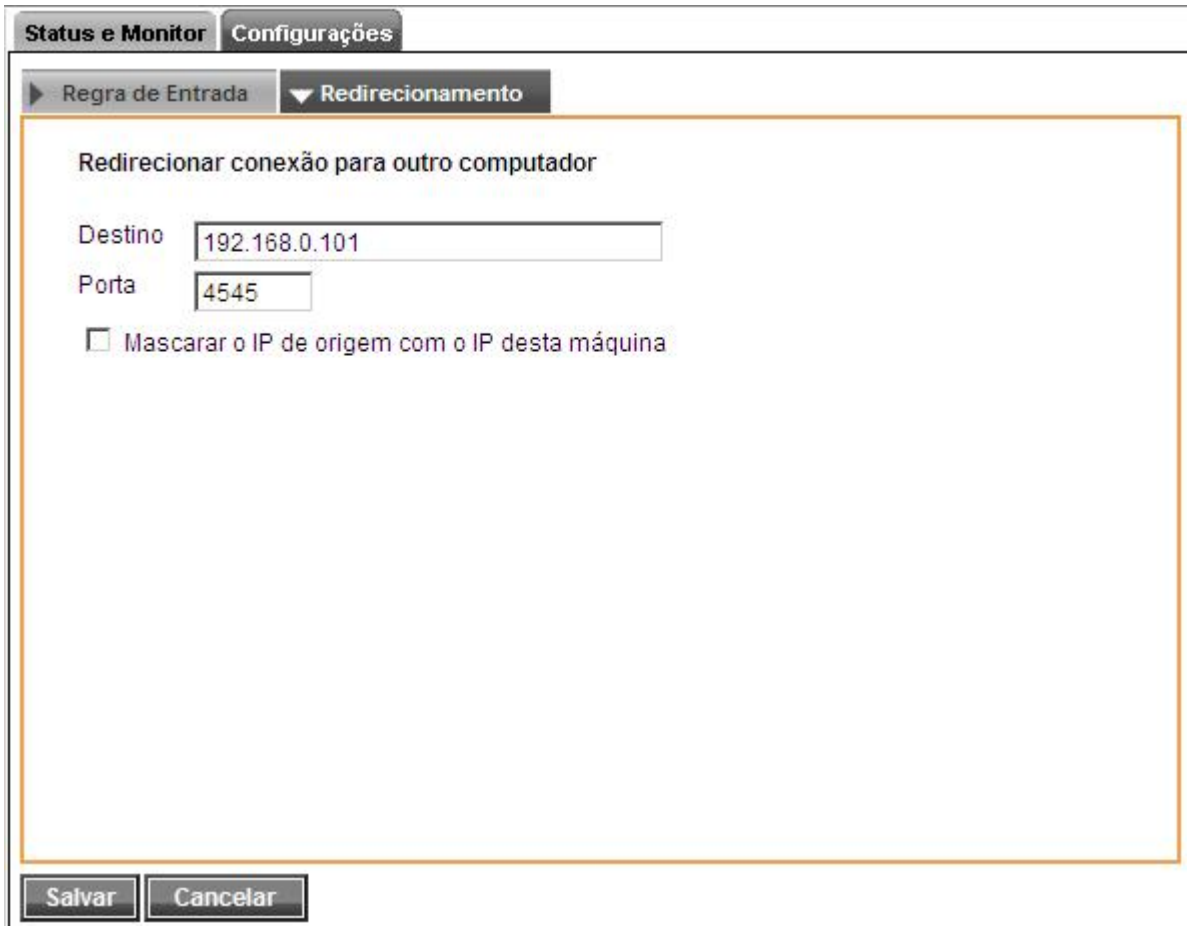
- **Destino:** Deve ser informado o IP do computador que receberá a conexão.

- **Porta:** Deve ser informada a porta que receberá a conexão. A porta padrão utilizada é 0, e deve ser alterada para os programas acessarem a porta correta.

- **Mascarar IP de origem com o IP dessa máquina:** Habilitando essa opção, o IP de origem será mascarado com o IP da máquina que receberá a

conexão.

Veja um exemplo de configuração na imagem a seguir. A conexão recebida na Porta TCP 444 (Regra VPN criada no exemplo mencionado anteriormente) será redirecionada para o computador com endereço IP 192.168.0.101 na Porta 4545.



6.4. Saída

Guia Configurações | Regras de Saída:

Controle de Acesso:

O **Controle de Acesso** é uma função típica dos serviços **Proxy Transparente**.

Este controle possibilita ao administrador da rede permitir ou proibir as estações da rede acessar ou não a um determinado programa.

Por padrão, o **Winconnection 6** permite que todas as estações tenham acesso a

todos os programas. Como o serviço **Proxy Transparente** deixa a estação como "conectada diretamente à internet", o administrador da rede pode impedir que determinadas estações acessem determinados programas ou serviços.

É possível criar uma Rede de Acesso para determinar quais usuários farão parte do bloqueio da regra criada no Controle de Acesso.

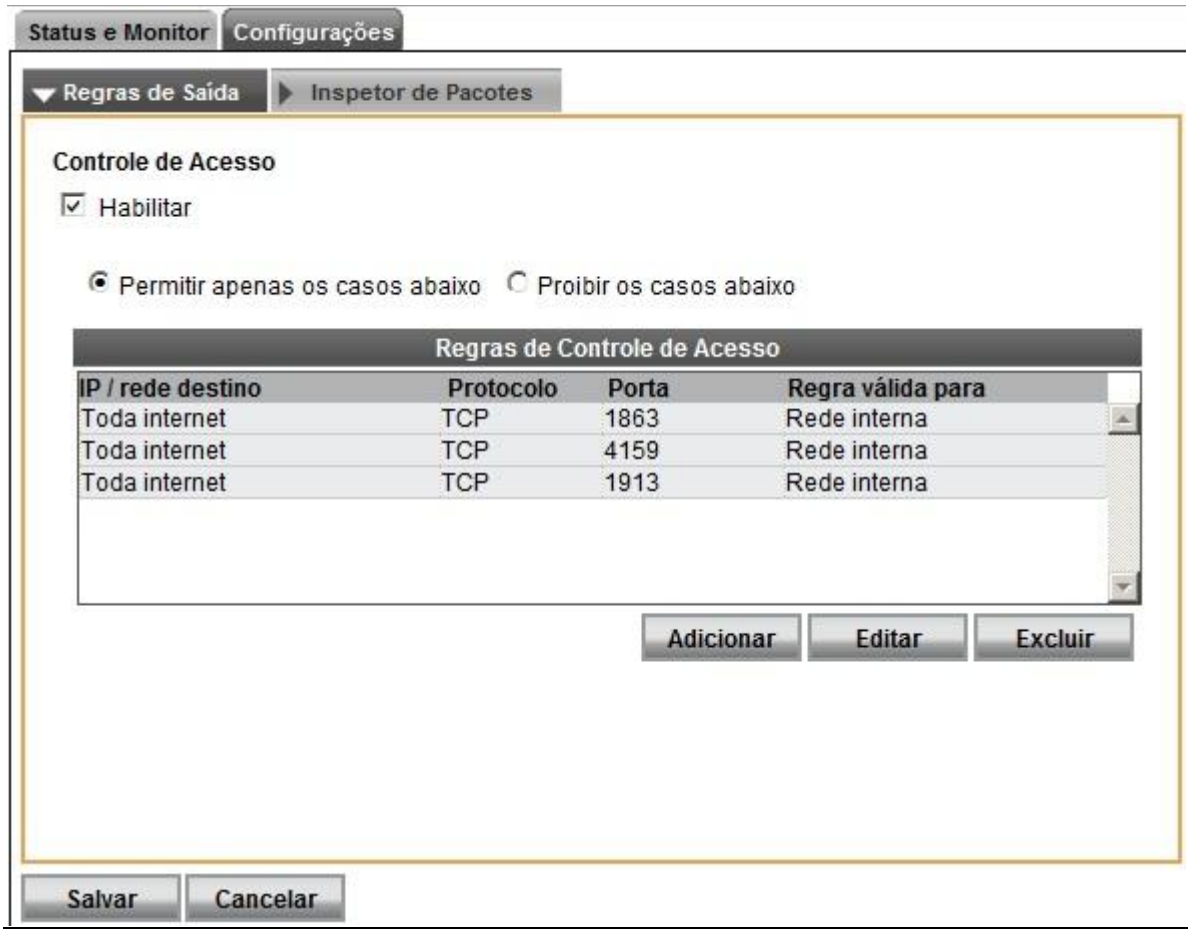
Um exemplo clássico é proibir a utilização de ICQ, MSN Messenger, Kazaa e outros aplicativos na rede que usam os serviços **Proxy Transparente**, através de regras no Controle de Acesso.

- **Permitir apenas os casos abaixo:** Quando o administrador cria a regra, pode permitir o acesso ao serviço somente para os casos digitados no campo logo abaixo.

  Esta opção pode ser utilizada quando o administrador não quer que os usuários fiquem conectados diretamente à internet, via **Proxy Transparente** e/ou **Socks 5**. Porém, existe aplicativo específico na estação que exige um dos serviços acima para funcionar corretamente. Neste caso, ele permite um usuário, uma faixa de usuários ou uma faixa de portas para acesso externo do aplicativo que deseja usar.

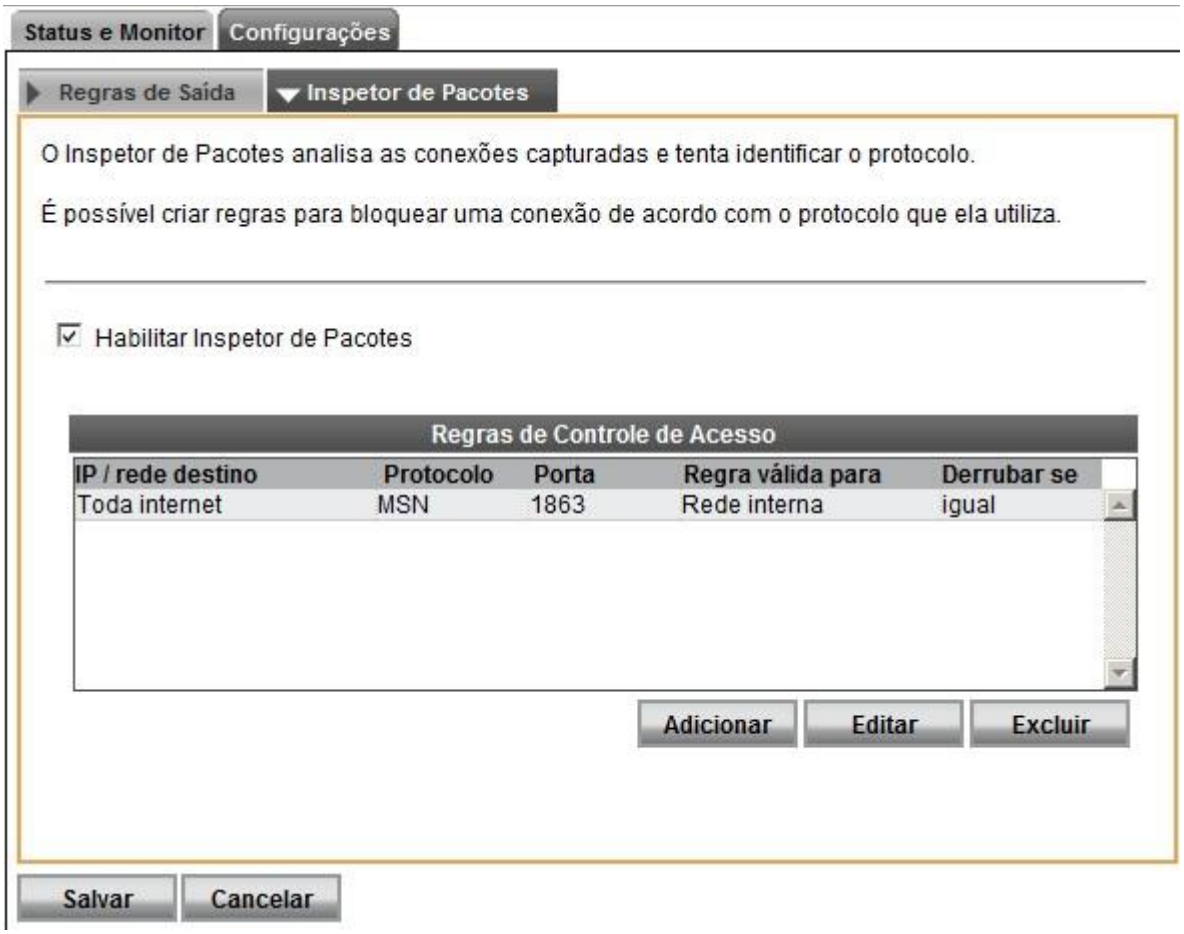
- **Proibir os casos abaixo:** Quando o administrador cria a regra, pode criar uma lista negra de acessos ao serviço, com base em computadores ou serviços. É a regra mais usada.

  Esta opção pode ser usada quando o administrador não quer permitir que determinados usuários ou uma faixa de usuários ou até uma porta acesse a rede externa. Um exemplo de utilização é o bloqueio ao MSN, ICQ, Kazaa, etc.



A configuração do **Proxy Transparente** nas estações está descrita no tópico Configuração do Proxy Transparente nas estações.

Guia Configurações | Inspeção de Pacotes:



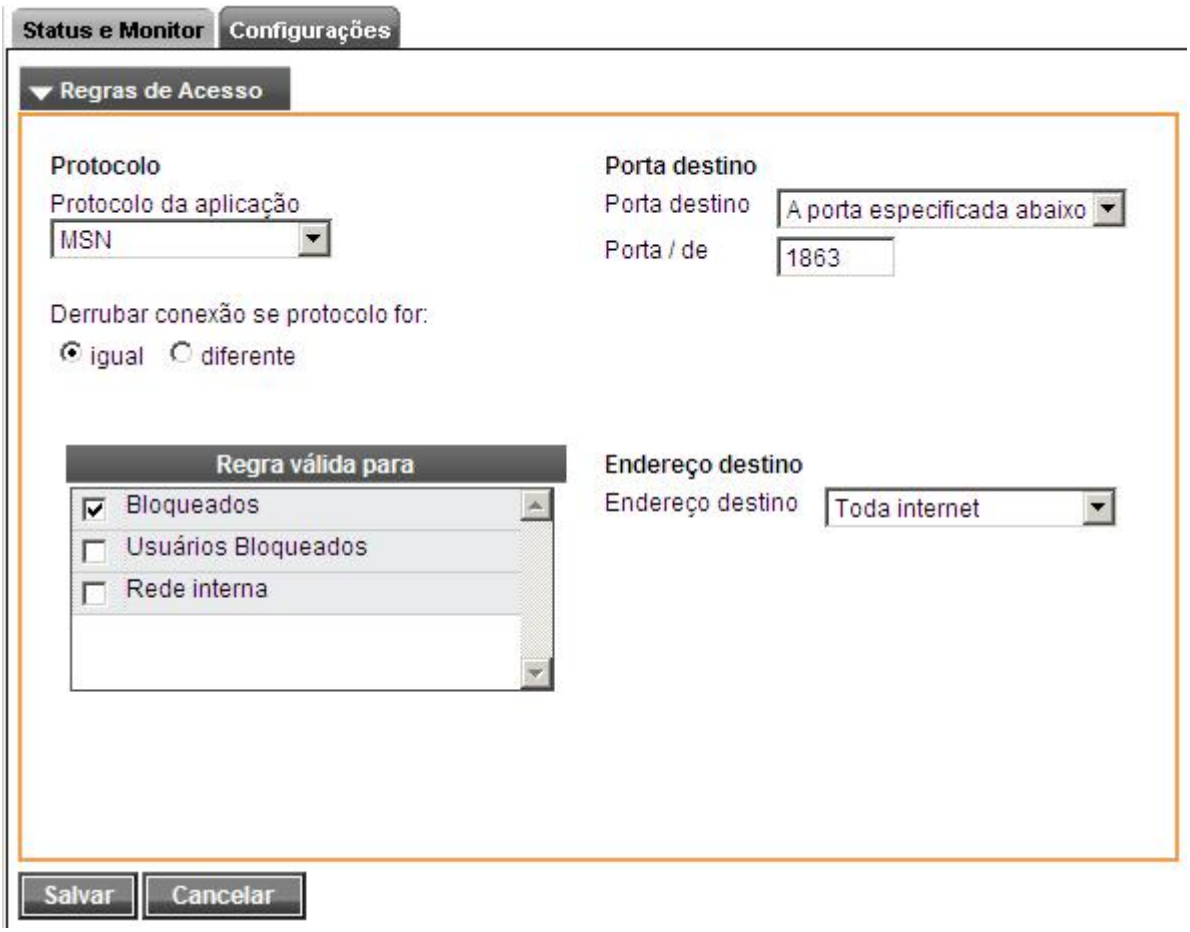
Nesta guia é possível habilitar a *Inspeção de Pacotes*. Com base nas regras criadas, o *Inspetor de Pacotes* pode derrubar conexões dependendo do seu protocolo.

É possível criar uma Rede de Acesso para determinar quais usuários farão parte da Inspeção de Pacotes.

Para criar uma regra, basta clicar no botão *Adicionar*.

É possível derrubar a conexão se o protocolo for igual ao mencionado na regra (habilitando a opção *"Bloquear se o protocolo for igual"*) ou se o protocolo for diferente da regra (habilitando a opção *"Bloquear se o protocolo for diferente"*).

Veja um exemplo de configuração de uma regra de inspeção de pacotes na imagem a seguir:



6.5. Controle de Banda

O serviço **Controle de Banda** do **Winconnection 6**, permite que o administrador da rede crie regras para controlar a utilização da banda.

As regras podem ser criadas para reservar parte da banda internet para os serviços do **Winconnection 6**, como Servidor de E-mail, Navegação e outros serviços.

Guia Configurações | Regra Padrão:

O **Controle de Banda** irá dividir a banda nominal de cada interface de rede em fatias. O tamanho de cada fatia é determinado por uma das regras de controle de banda definidos na guia *Regra Padrão*.

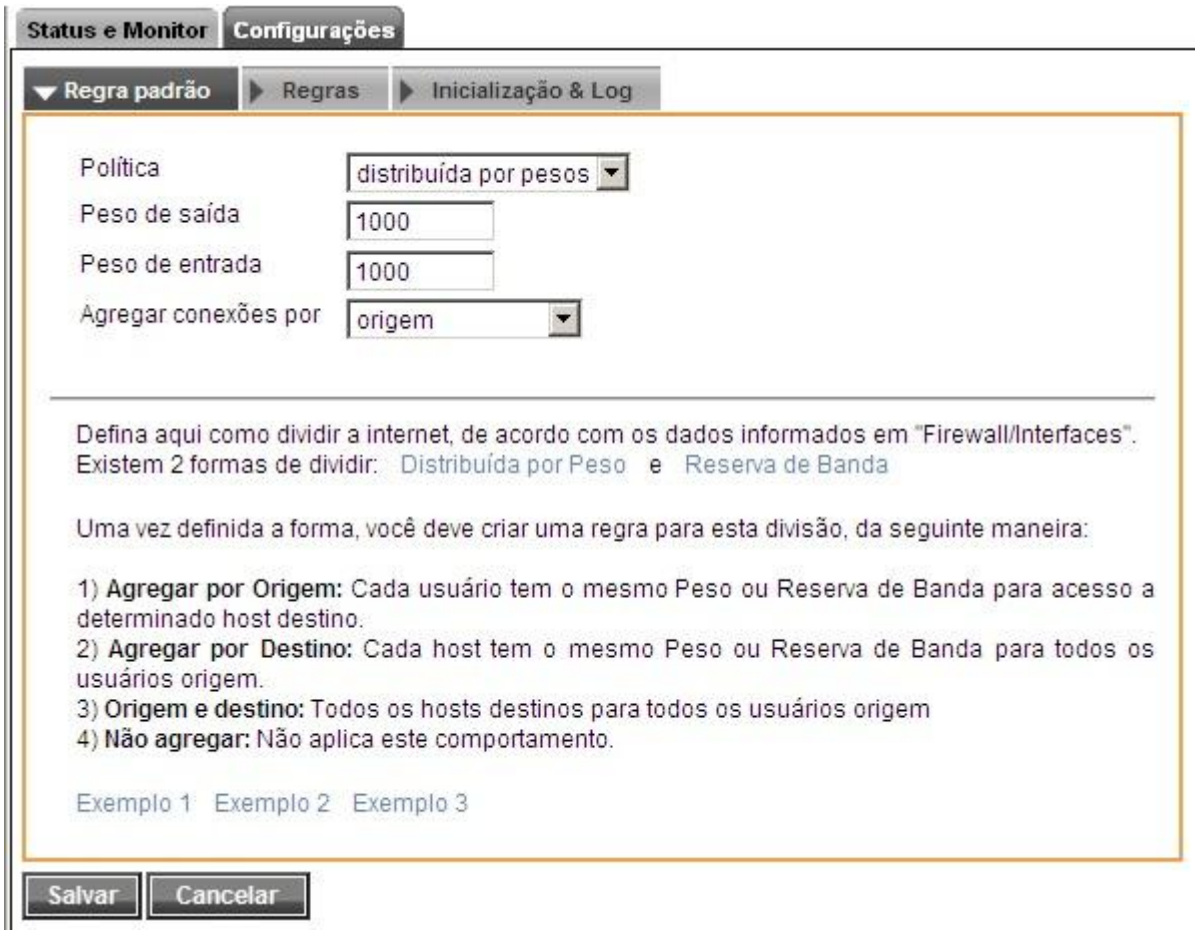
A primeira regra que possuir *Origem* e *Destino* compatíveis com a conexão que está sendo analisada será a escolhida. Caso nenhuma regra seja encontrada, a *Regra Padrão* será aplicada.

As fatias podem agregar mais de uma conexão. Ou seja, mais de uma conexão pode contribuir para o consumo da banda destinada a uma fatia. As regras de controle de banda determinam o tipo de agregação a ser aplicada às conexões. Uma regra pode ser responsável pela produção de mais de uma fatia.

A *Banda Nominal* de cada interface é definida em "Firewall / Interfaces".

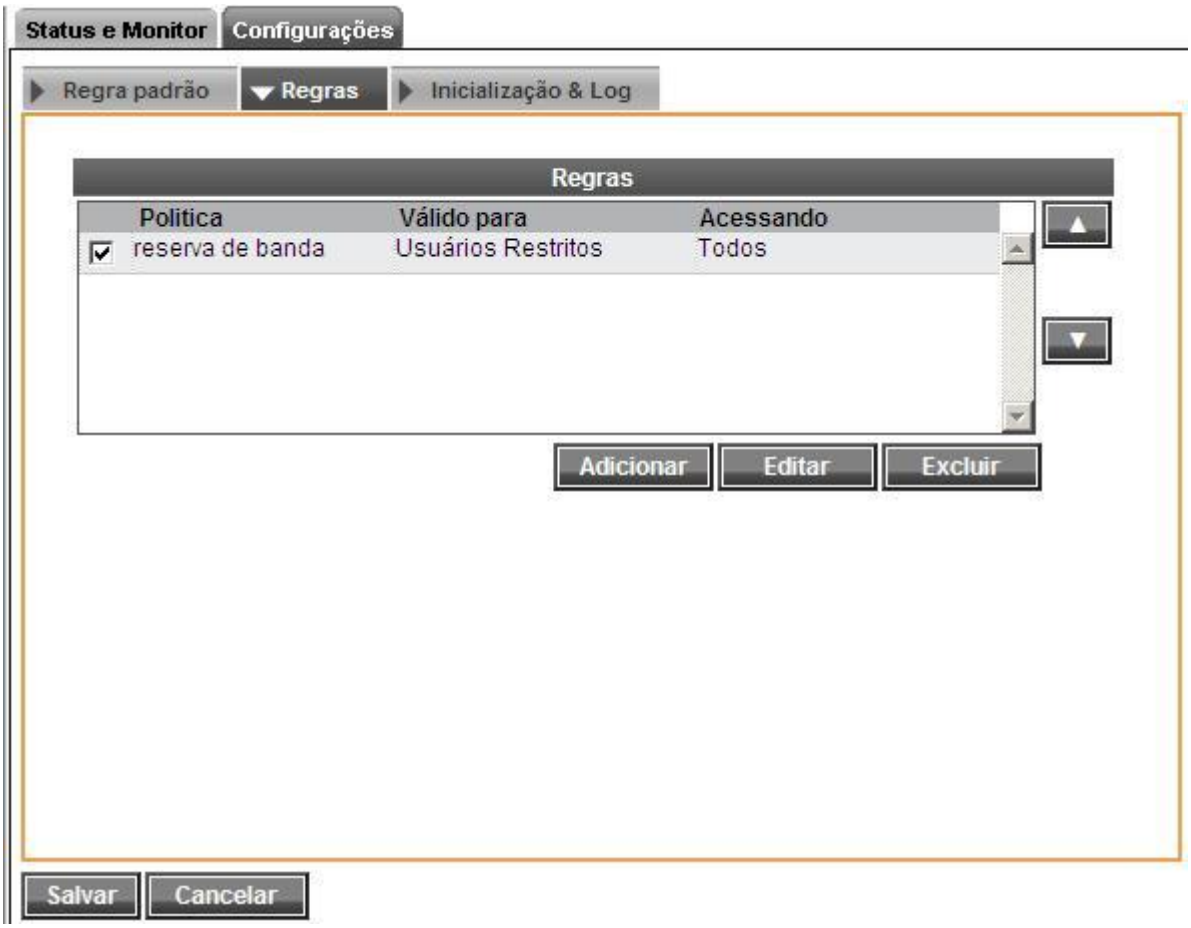
As fatias correspondentes às políticas do tipo "reserva de banda" são alocadas primeiro e subtraídas da *Banda Nominal*. Toda banda restante é distribuída proporcionalmente segundo os pesos especificados nas regras do tipo "distribuída por peso".

- **Política:** Neste campo é necessário o tipo da política da regra: reserva de banda ou distribuída por pesos.
- **Peso de Saída:** Neste campo é informada a banda que será reservada para saída (upload).
- **Peso de Entrada:** Neste campo é informada a banda que será reservada para saída (download).
- **Agregar conexões por:** É necessário informar se a conexão será agregada à origem, destino, origem e destino ou se a conexão não será agregada.



Guia Configurações | Regras:

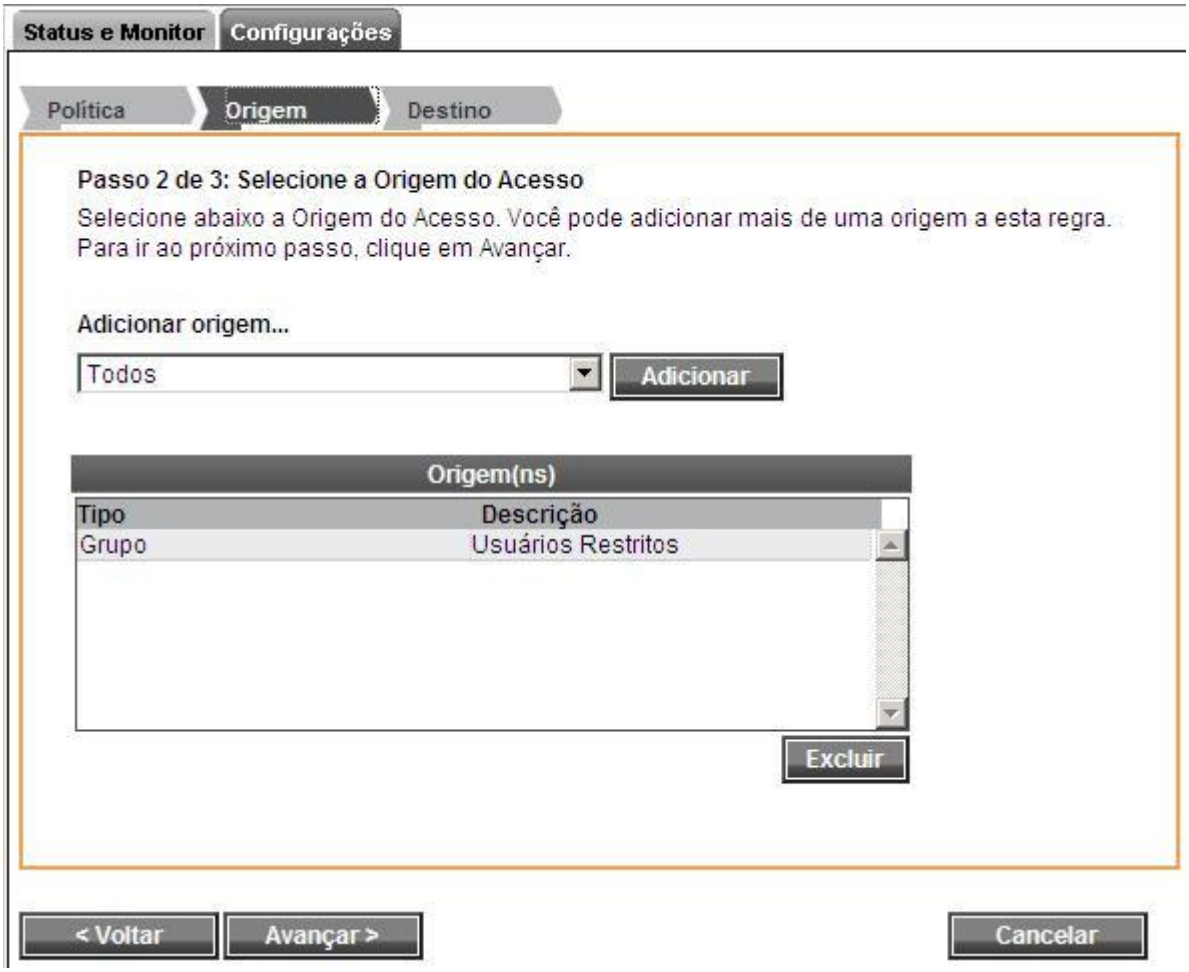
Nesta guia de configuração é possível criar, editar e excluir regras para o controle de banda.



As regras são criadas ou editadas em 3 passos:

- **Passo 1 – Política:** Neste passo, é necessário definir a política da regra (como explicado anteriormente).

- **Passo 2 – Origem:** Neste passo, deve ser informada a origem de acesso para a qual a regra será aplicada: *Todos*, *Usuário (somente para serviço HTTP)*, *Grupo ou IP*.



- **Passo 3 – Destino:** Neste passo de configuração, o administrador da rede deve informar o destino de acesso para a qual a regra será aplicada: *Todos* ou *IP*.

Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/BANDWIDTH_CONTROL.LOG":** O arquivo em bloco de notas (BANDWIDTH_CONTROL.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.

6.6. Porta TCP Mapeada

O serviço **Porta TCP Mapeada** é utilizado para possibilitar o acesso a serviços que não sejam padronizados ou de aplicações TCP dentro da sua rede, desde que se saiba o computador e porta a qual se deseja ter acesso.

Com este serviço instalado, sempre que um cliente conectar na porta do *PIPE* do **Winconnection 6** a conexão será redirecionada ao computador remoto na porta especificada como "*destino do PIPE*".

Guia Configurações | Geral:

- **Host ou IP de destino:** Neste campo o administrador da rede, deve digitar o endereço o IP da estação da rede interna que receberá a conexão.

- **Porta destino**: É a porta utilizada pelo aplicativo cuja conexão está sendo redirecionada. A porta padrão utilizada é 0, e DEVE ser alterada para os programas acessarem a porta correta.

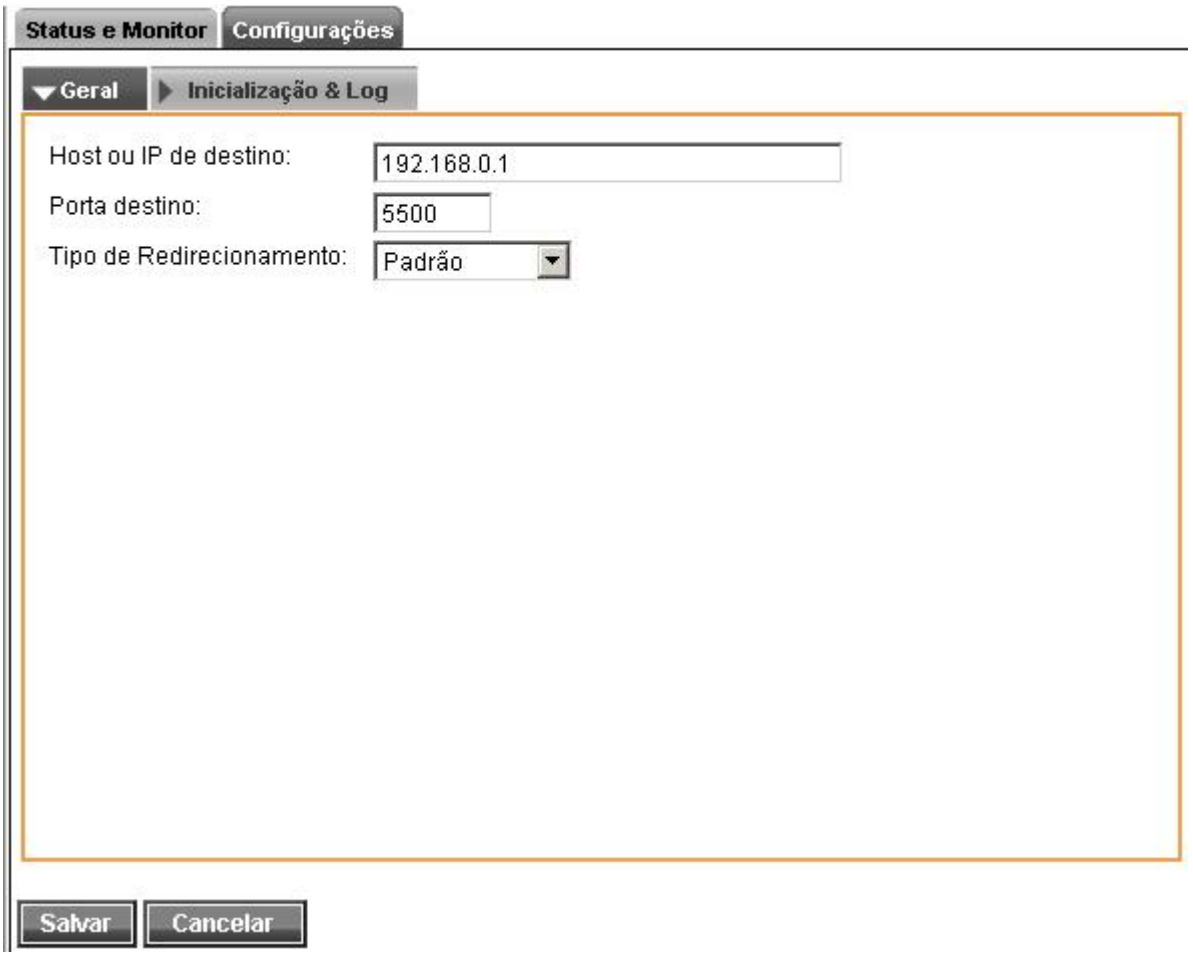
- **Tipo de direcionamento:** A opção **Tipo de Redirecionamento** possui quatro escolhas:

    - **Padrão:** Selecione essa opção para os casos que não se enquadram nas opções citadas abaixo.

    - **NAT Reverso:** Esta opção é útil quando o cliente usa *NAT reverso*, ou seja, quando existe uma requisição de dentro da rede interna para a rede externa (Internet).

    - **Conexão FTP*:*** Selecione essa opção se existir uma requisição de FTP da rede externa para rede interna, e que a rede interna precise retornar a requisição feita pela rede externa (Internet).

    - **VPN PPTP:** Selecione esta opção se existir uma requisição de VPN PPTP.



Guia Configurações | Inicialização & Log:

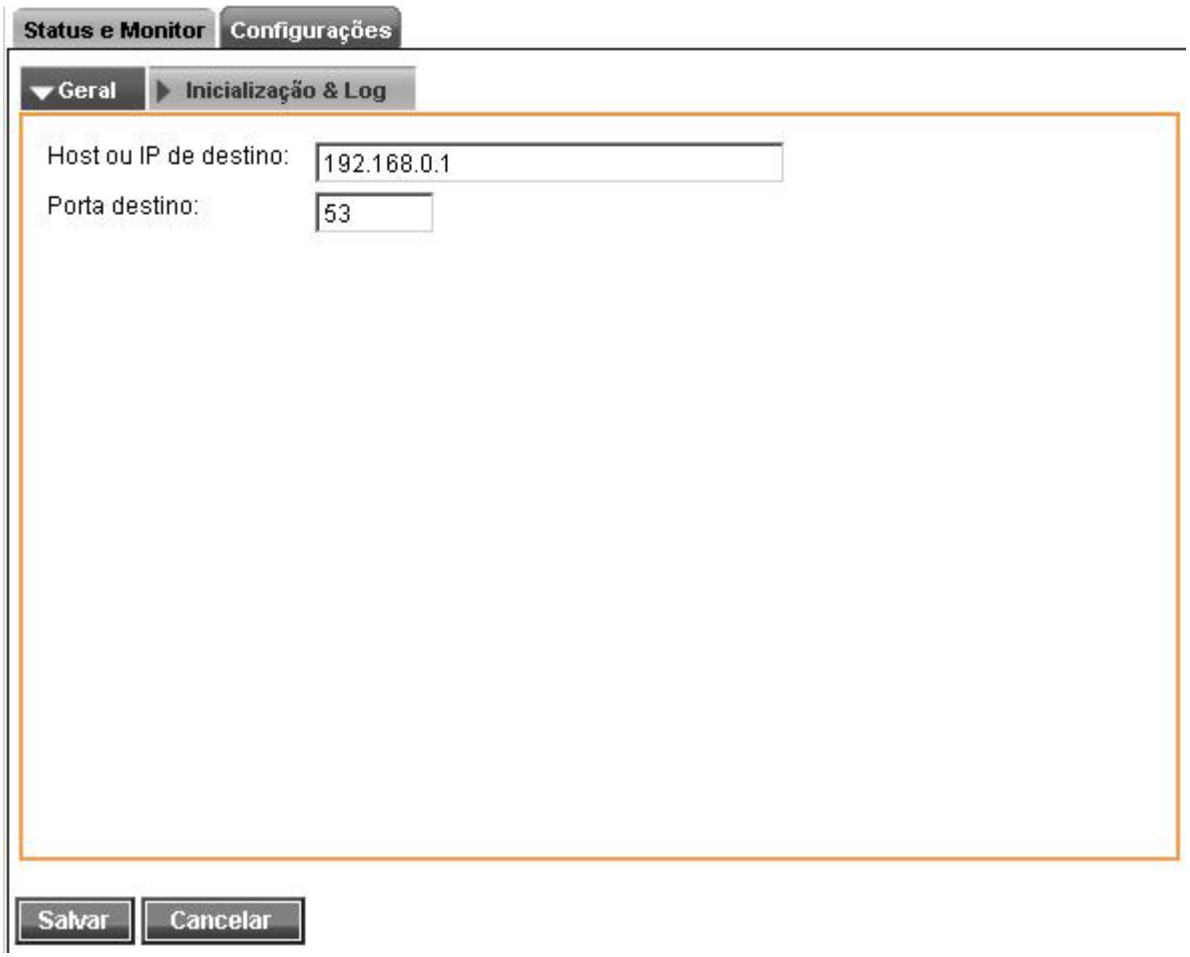
- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.
- **Salvar LOG em "LOGS/PORTMAP_TCP.LOG":** *O arquivo em bloco de notas (PORTMAP_TCP.LOG)* será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.
- **Porta TCP**: É a porta externa que responderá às requisições.
- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.

6.7. Porta UDP Mapeada

Assim como a Porta TCP Mapeada, o serviço Porta UDP Mapeada é utilizado para possibilitar o acesso a serviços que não sejam padronizados ou de aplicações UDP (como por exemplo o DNS) desde que se saiba o computador e porta a qual se deseja ter acesso.

Guia Configurações | Geral:

- **Host ou IP de destino:** Neste campo o administrador da rede, deve digitar o endereço o IP da estação da rede interna que receberá a conexão.
- **Porta destino**: É a porta utilizada pelo aplicativo cuja conexão está sendo redirecionada. A porta padrão utilizada é 0, e DEVE ser alterada para os programas acessarem a porta correta.



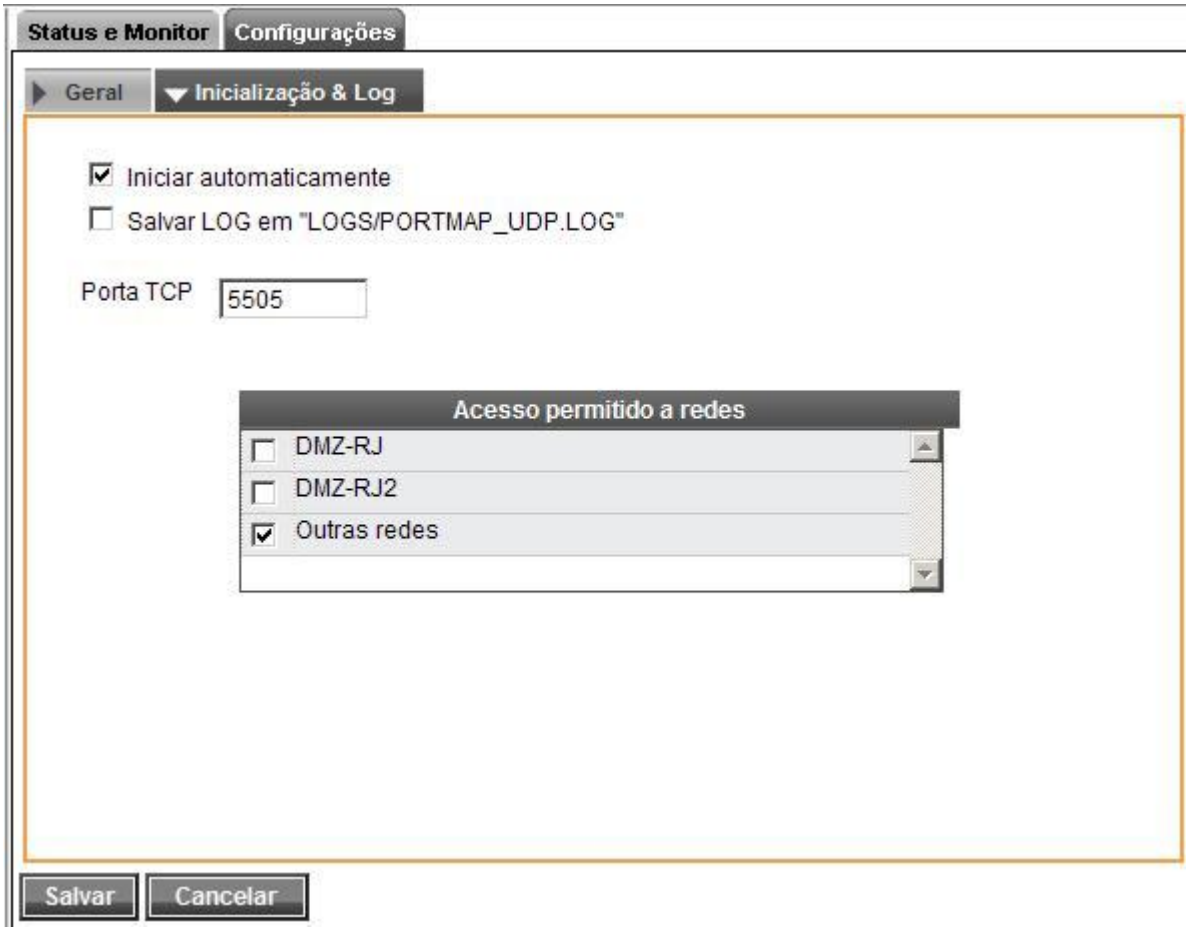
Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/PORTMAP_UDP.LOG":** *O arquivo em bloco de notas (PORTMAP_UDP.LOG)* será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.

- **Porta TCP**: É a porta externa que responderá às requisições.

- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.



7. Serviços de E-mail

Guia Status e Monitor:

Essa guia exibe informações de conexões de entrada e saída de dados.

As seguintes informações sobre as conexões poderão ser exibidas: *Usuário, Serviço, IP Remoto, Hora Inicial, Velocidade de Upload, Velocidade de Download, ID, Endereço Local, Protocolo, Bytes Recebidos* e *Bytes Enviados*.

Clicando com o botão direito do mouse sobre uma conexão, o **Winconnection 6** disponibiliza as seguintes opções:

- **Agrupar por:** Agrupa as conexões por *Usuário,* por *Endereço Local* ou por *IP Remoto*.
- **Colunas:** Exibe as opções de colunas que poderão ser exibidas.

Guia Configurações | Geral:

Quarentena:

Manter mensagens na quarentena por [dias]: Neste campo deve ser informado o tempo máximo, em dias, que uma mensagem deverá permanecer na quarentena. Após esse período, as mensagens serão excluídas automaticamente.

Interface PHP onDispach:

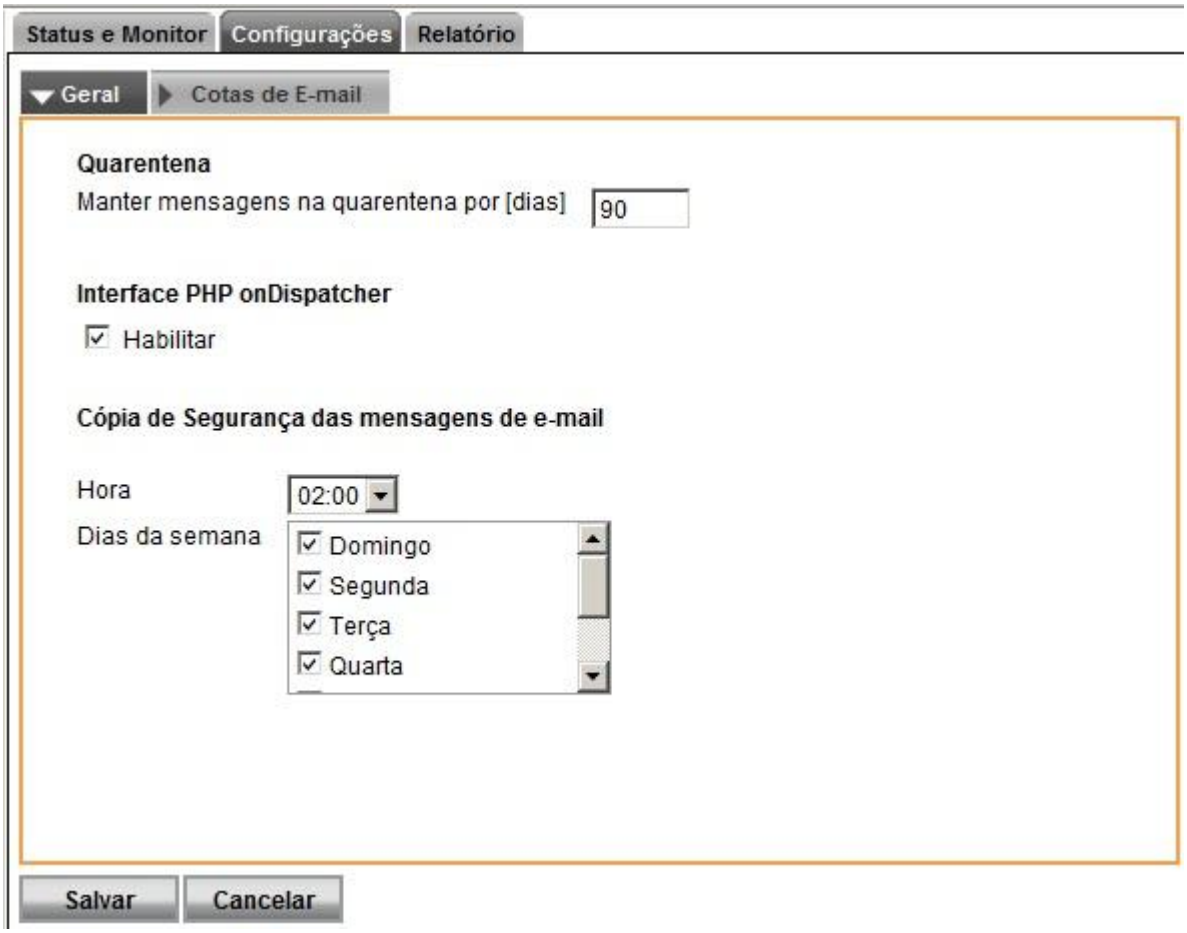
Habilita a função **Interface onDispach** *que* permite estender a funcionalidade do programa com uma simples API (*Application Programming Interface*) para a linguagem PHP. Mais informações podem ser obtidas no capítulo XII.1. Programação e Extensibilidade.

Cópia de Segurança das mensagens de e-mail:

O armazenamento das mensagens do **Winconnection 6** é dividido em 2 partes: banco de dados (índices das mensagens) e as mensagens de e-mail propriamente ditas.

Neste campo, o administrador da rede pode definir à hora e os dias da semana em que cópias de segurança dos índices das mensagens de e-mail serão efetuadas (caso o índice seja corrompido, este backup ajudará na sua restauração).

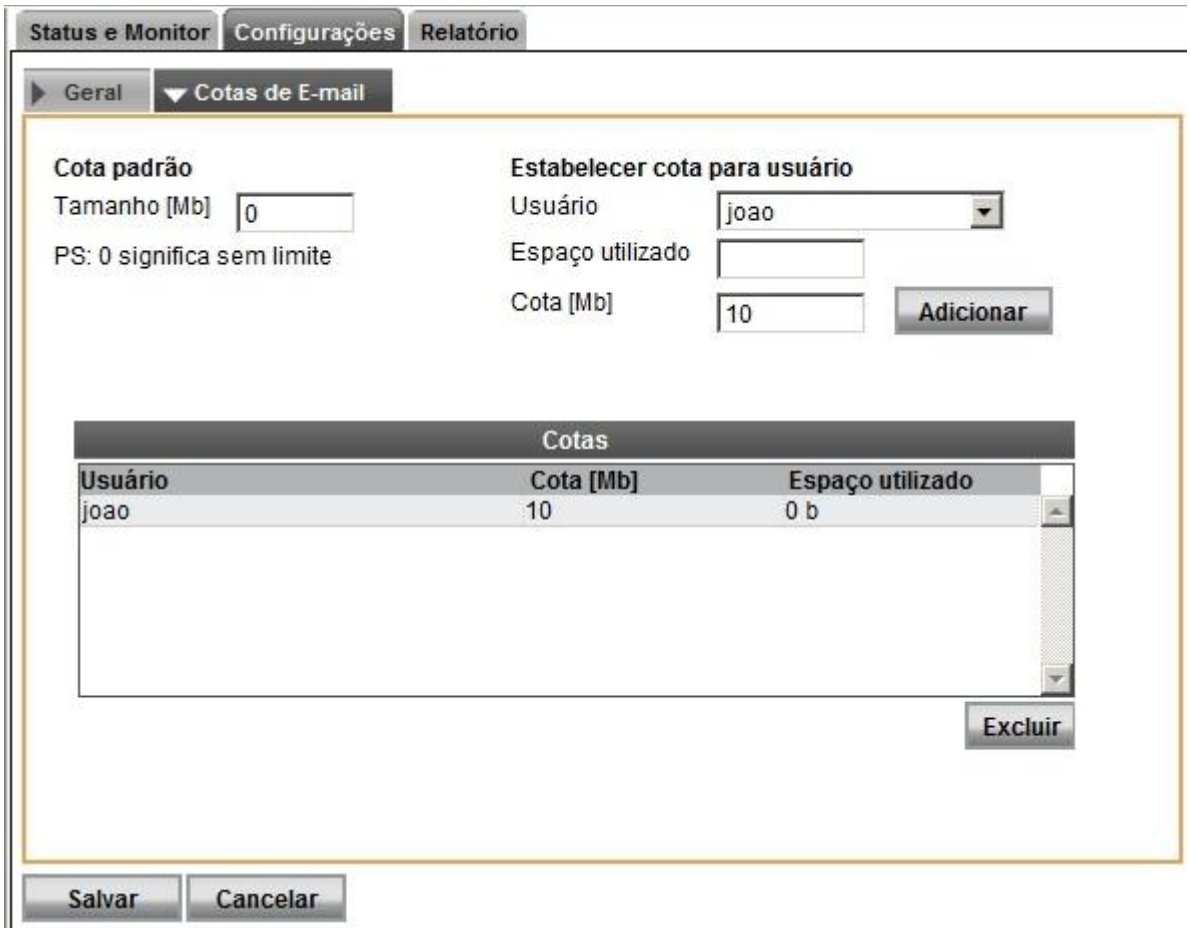
Importante! Recomendamos que o backup do diretório *C:\Arquivos de programas\Winco\Winconnection 6\mbox* seja efetuado com frequência.



Guia Configurações | Cotas de E-mail:

Nesta guia de configuração é possível especificar cotas de e-mail para cada usuário. Ou seja, é possível definir limites de armazenamento de mensagens (em MB).

Se o usuário não possuir uma cota especificada, significa que ele não tem limite de armazenamento.



Guia Relatório:

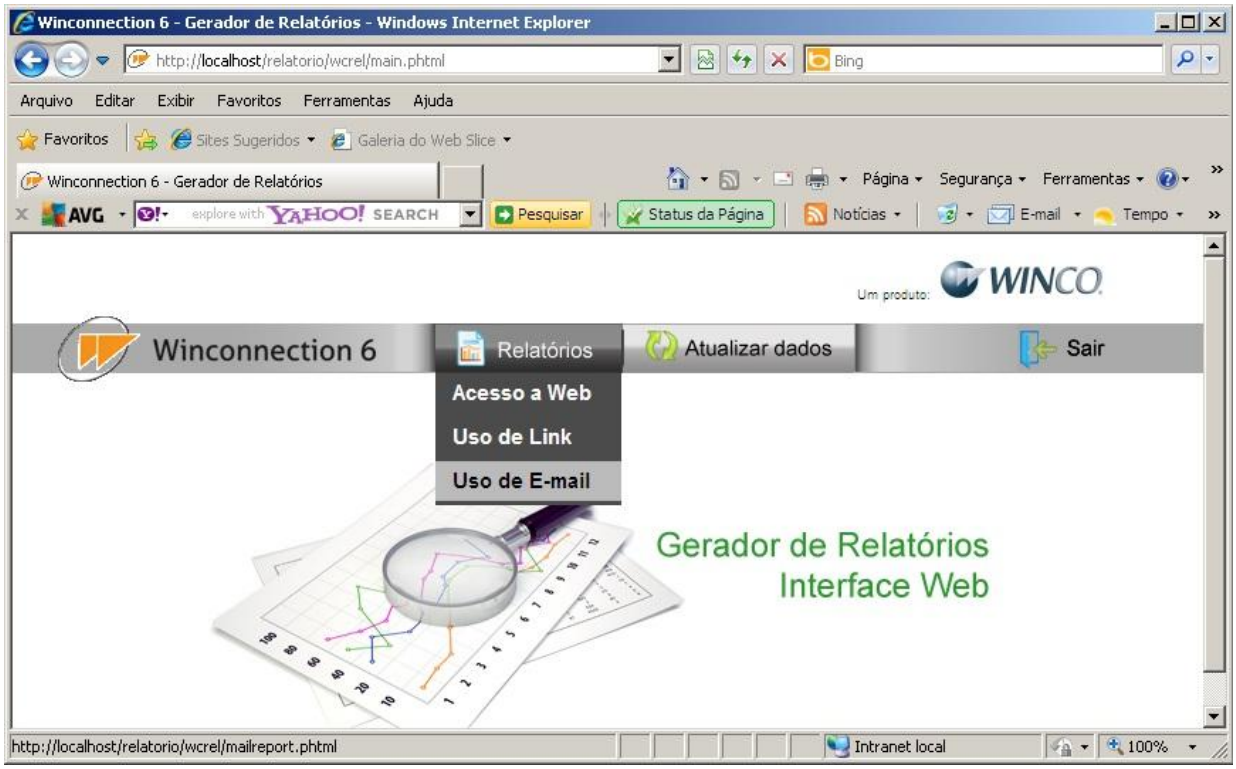
O **Relatório de E-mail** exibe informações sobre o processo de envio e recebimento de e-mails dentro da rede, bem como efetuar um rastreamento das mensagens enviadas para determinados usuários.

O administrador da rede pode escolher duas formas de relatórios:

- **Estatísticas**: Mostra um gráfico com as informações de tráfego de e-mails internos e externos. Após a emissão da estatística, é possível consultar usuário por usuário para se saber o fluxo de e-mail que este usuário está gerando para a rede, bem como tamanho, vírus recebidos/enviados, etc.

- **Rastreamento de Mensagens**: Mostra a opção de rastreamento de mensagens de determinado e-mail para outro e-mail ou com base no ID da mensagem. Esse tipo de relatório é particularmente útil quando se precisa de um relatório detalhado de quem está enviando e-mail para outras pessoas na rede.

Obs.: Também é possível acessar o relatório *Uso de E-mail* através do navegador, acessando o endereço: *http://ip_do_servidor/relatorio*. Após se logar no Gerador de Relatórios, selecione a opção *Relatórios → Uso de E-mail*.



Veja a seguir a descrição de cada serviço disponível no menu *Serviços de E-mail*.

7.1. Fila de Mensagens

Esta guia exibe a fila de mensagens que estão na espera para serem enviadas.

É possível visualizar o ID, o remetente, o destinatário e o tamanho das mensagens que estão na fila.

Além disso, é possível forçar o envio de uma mensagem ou de todas as mensagens, clicando com o botão direito em uma mensagem *Ação → Enviar agora* (ou *Enviar todas as mensagens*).

7.2. Listas

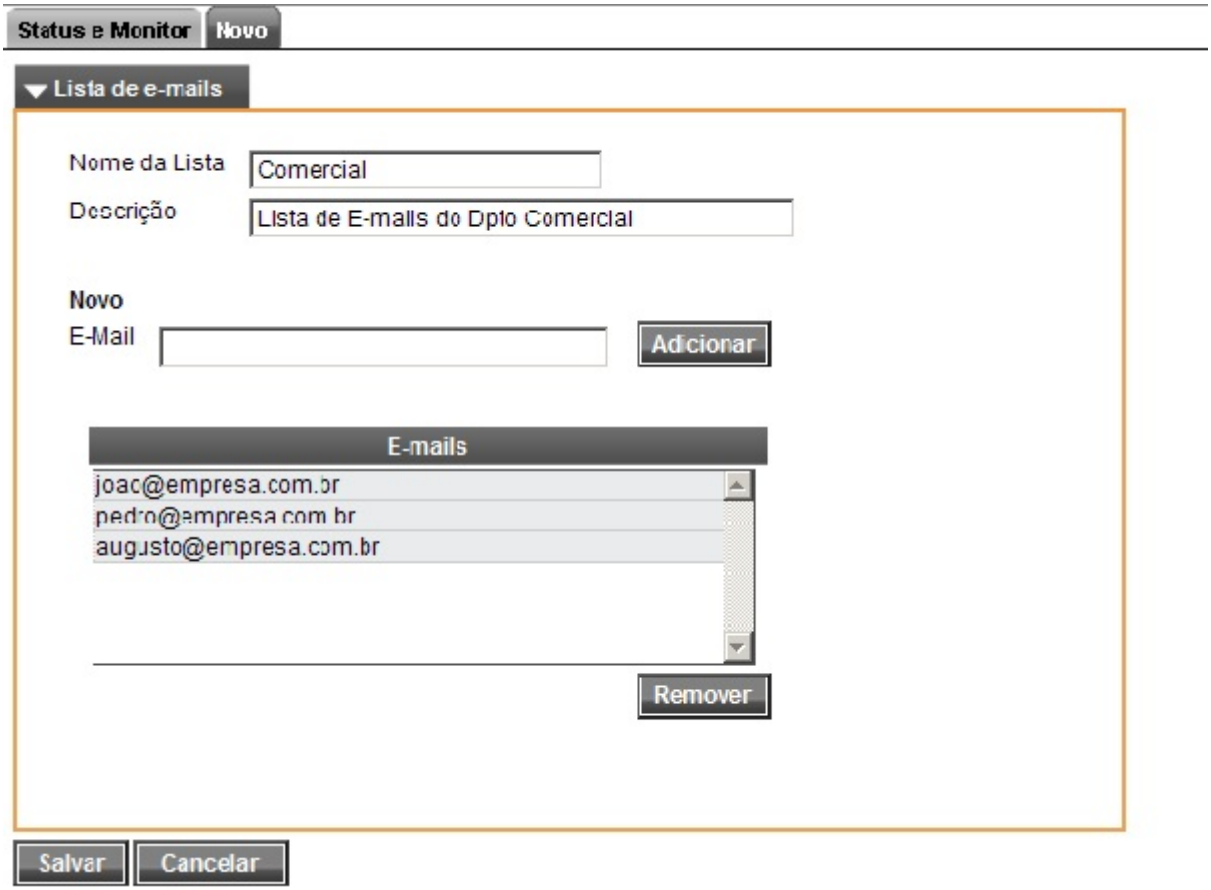
O serviço **Listas** permite a criação de listas de distribuição de e-mail.

Uma **Lista de Distribuição de e-mail** distribui um determinado e-mail para várias pessoas na rede interna, ou seja, o mesmo e-mail é recebido por vários usuários.

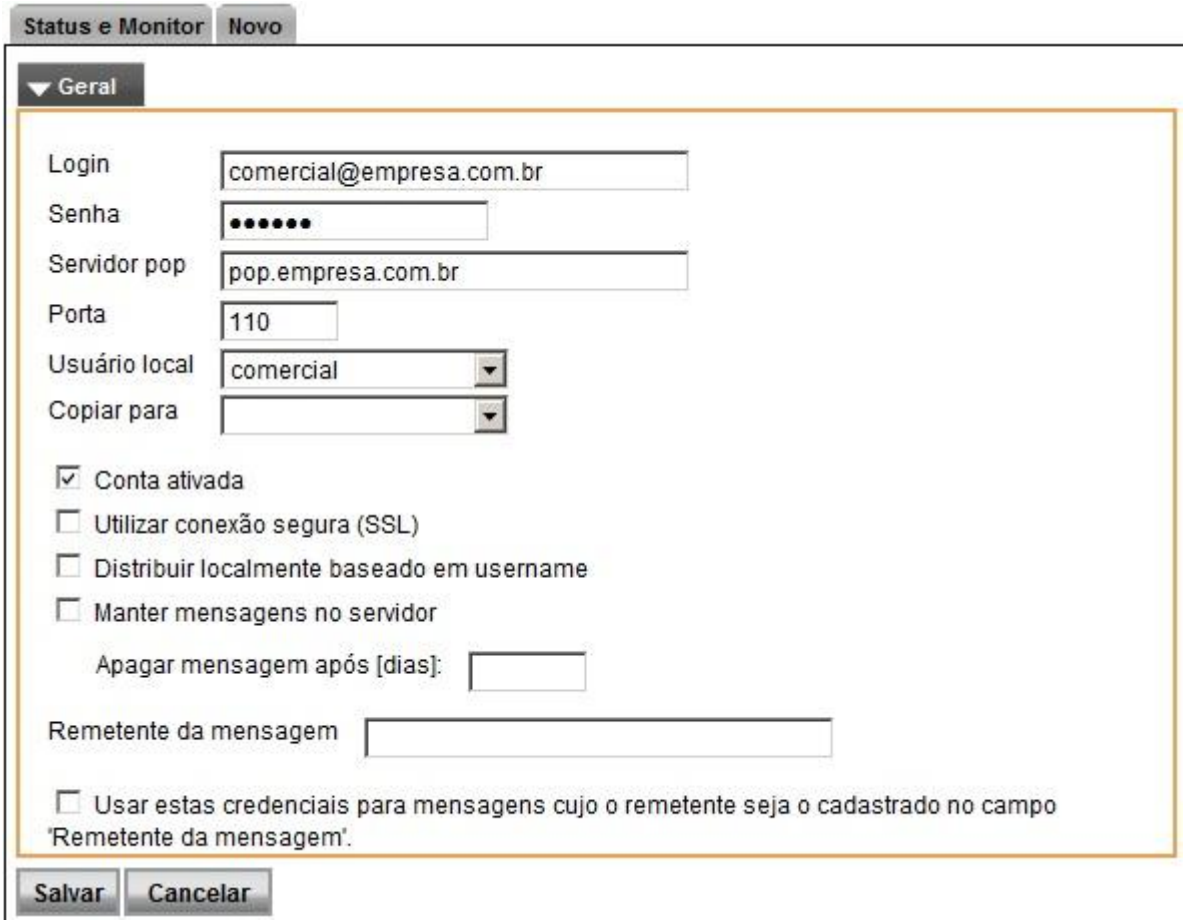
Exemplo:

Suponhamos que exista o e-mail comercial@empresa.com.br e este e-mail deve ser recebido por **João, Pedro** e **Augusto**. O procedimento é o seguinte:

- No serviço **Listas**, clique na Guia *Novo*.
- **Nome da Lista:** Digite o nome da lista de distribuição de e-mail. O nome normalmente é curto, sem espaços e acentos. Caracteres especiais também não podem ser usados.
- **Descrição:** Descreva aqui a utilidade para o qual a lista foi criada.
- **Novo:** Digite o e-mail do usuário que fará parte dessa lista de distribuição (por exemplo: joao@empresa.com.br) **Adicionar**. Com todos os usuários adicionados, clique no botão **Salvar**.



- No serviço **Mapeador POP3**, clique no botão **Novo**. Preencha os campos de acordo com o e-mail (no nosso exemplo comercial@empresa.com.br) e no campo **"Usuário local"**, selecione a lista (no nosso exemplo comercial).



7.3. Filtro de E-mail

O serviço **Filtro de E-mail** disponibiliza uma série de configurações que poderão ser utilizadas nos e-mails.

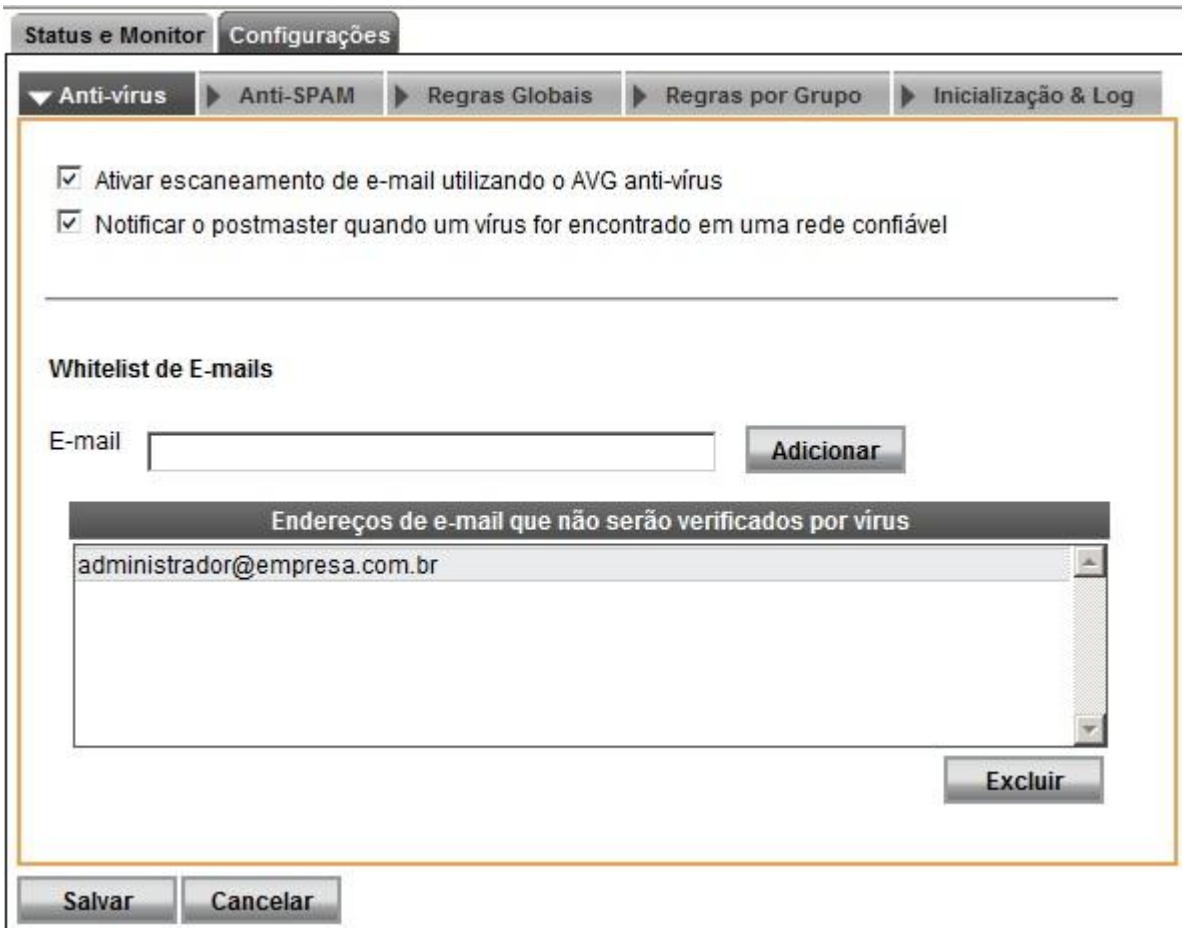
Guia Configurações | Antivírus:

Esta guia possui as seguintes configurações:

- **Ativar escaneamento de e-mail utilizando o AVG anti-vírus:** O **Winconnection 6** é compatível com o antivírus **AVG**. Habilitando esta opção, se o programa *AVG Anti-Vírus* estiver instalado no computador, as mensagens passarão a ser verificadas.

- **Notificar o postmaster quando um vírus for encontrado em uma rede confiável**: Se essa opção estiver habilitada, o administrador será informado quando um vírus for enviado de dentro de sua rede interna.

- **Whitelist de E-mails:** Nesta caixa de diálogo é possível adicionar, modificar e remover endereços de e-mail que não serão verificados pelo antivírus. Esta configuração é útil quando existe a necessidade de ter uma caixa postal dentro de sua rede que tenha a necessidade de receber vírus.



Guia Configurações | Anti-Spam:

A guia de configuração *Anti-Spam* possui as seguintes funções:

- **Ativar o SpamCatcher da Mailshell:** Ativa o plugin anti-spam desenvolvido pela empresa **Mailshell**. Este plugin pontua as mensagens recebidas de acordo com uma série de regras que são baixadas de um servidor dessa empresa.
    - **Licença:** Uma licença especial é necessária para ativar a opção **SpamCatcher da Mailshell**.

- **Perfil**: O administrador da rede poderá escolher, dentre os perfis listados, qual o melhor se adapta às necessidades de sua empresa. Cada perfil tem interferência direta no uso e funcionamento do Spamcatcher.

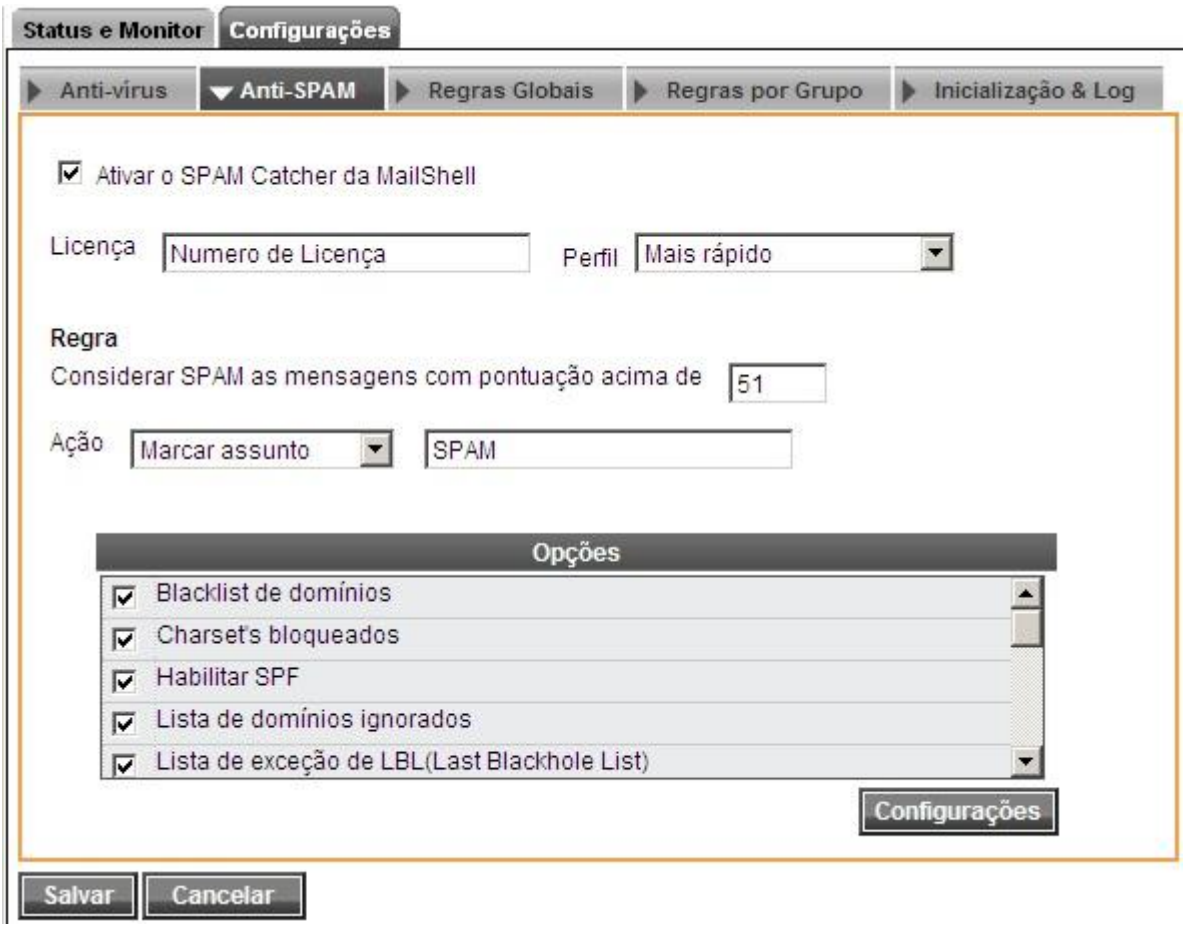
Regra:

- **Considerar SPAM as mensagens com pontuação acima de:** Como já foi citado anteriormente, o **SpamCatcher** analisa a mensagem recebida e gera uma pontuação para ela. Esta pontuação é a probabilidade de a mensagem ser um *SPAM*. Quanto maior a pontuação, maior a probabilidade. Nesta opção, o administrador da rede deve informar ao sistema qual é a pontuação para que uma mensagem seja considerada *SPAM*.

- **Ação:** O administrador da rede pode definir como as mensagens consideradas *SPAM* pelas regras criadas devem ser tratadas: *Aceitar mensagem, Marcar assunto com, Deletar a mensagem, Copiar para, Mover para*.

Opções:

De acordo com o perfil escolhido, o administrador poderá personalizar algumas configurações do **SpamCatcher**, como por exemplo: *Domain Whitelist*, que é uma lista de domínios considerados "confiáveis" fazendo com que o Spamcatcher assuma que a mensagem recebida tenha uma pontuação baixa. Consulte o tópico Configuração Anti-Spam - Funções dos Perfis para mais informações. Para editar estas opções, basta selecioná-las e clicar no botão *Configurações*.



Guia Configurações | Regras Globais:

Esta guia do **Winconnection 6** dispõe sobre métodos de filtragem de e-mails como tamanho de mensagens, exclusões de anexos e regras para filtragem de mensagens consideradas *SPAM*.

Tamanho máximo de mensagens: Utilize estes campos para o controle do tamanho de mensagens enviadas para fora ou roteadas internamente.

- **Mensagens internas:** Este valor é para mensagens enviadas ou recebidas de domínios considerados internos. O valor é em kilobytes e o padrão do sistema é 0, que significa tamanho ilimitado.

- **Mensagens externas:** este valor é para mensagens enviadas ou recebidas de domínios que não são considerados como interno. O valor é em kilobytes e o padrão do sistema é 0, que significa tamanho ilimitado.

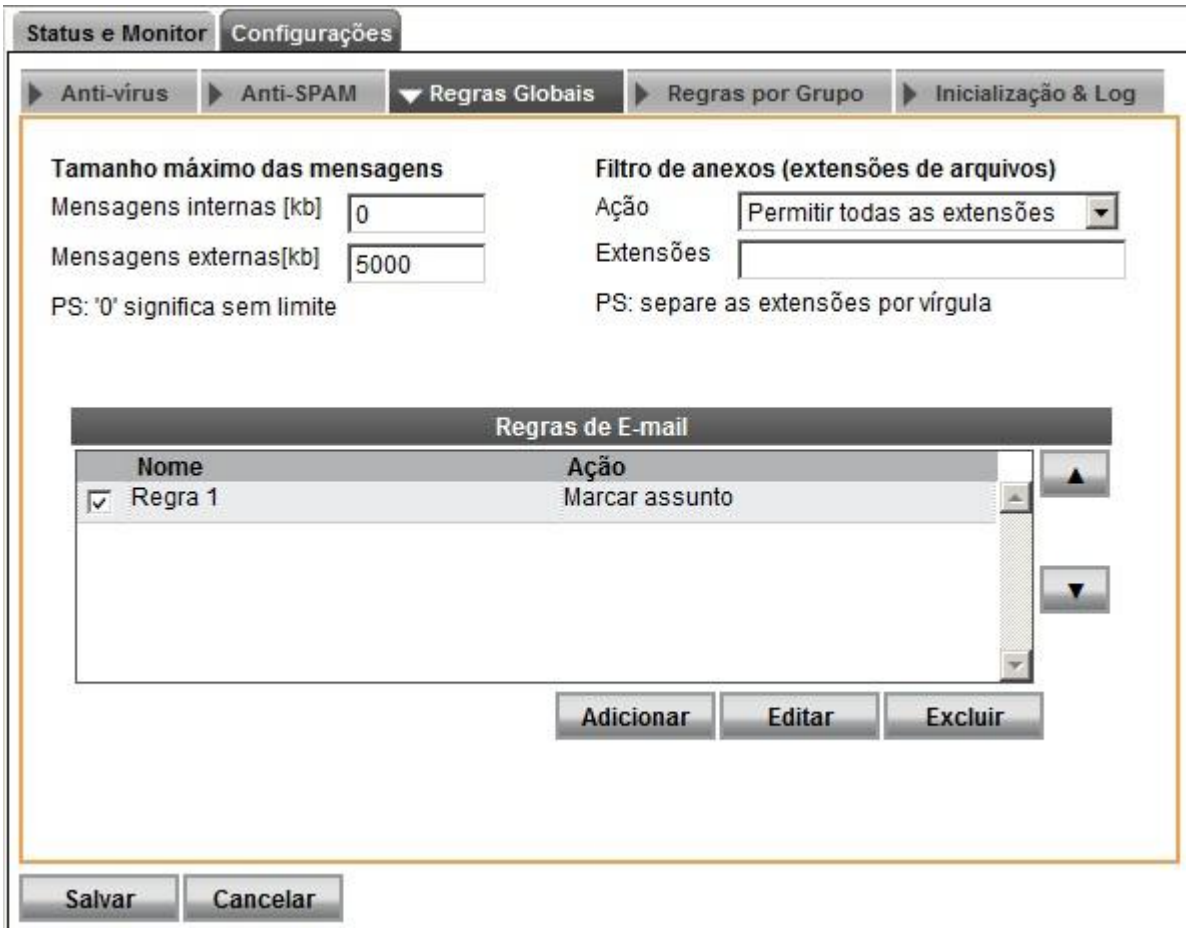
Filtro de Anexos (extensões de arquivos):

- **Ação:** Indica se as extensões serão bloqueadas ou se somente as extensões mencionadas no campo acima serão permitidas.

- **Extensões:** Esta opção proíbe que seja enviado e/ou recebidos e-mails com determinados tipos de anexos. É possível bloquear arquivos com qualquer extensão evitando assim queda de produtividade e o aumento na segurança na rede. Digite as extensões separadas por vírgula, por exemplo: exe, scr, pif.

Regras de E-mail:

O administrador da rede pode criar regras de roteamento das mensagens com base em informações como *De, Para, Cc, Data, Assunto, Prioridade, Endereço Original, Endereço Final, E-mail de, IP do Remetente, Tamanho (bytes).*



Guia Configurações | Regras por Grupo:

Esta guia do Winconnection 6 permite a criação de regras de filtro de mensagens ba-

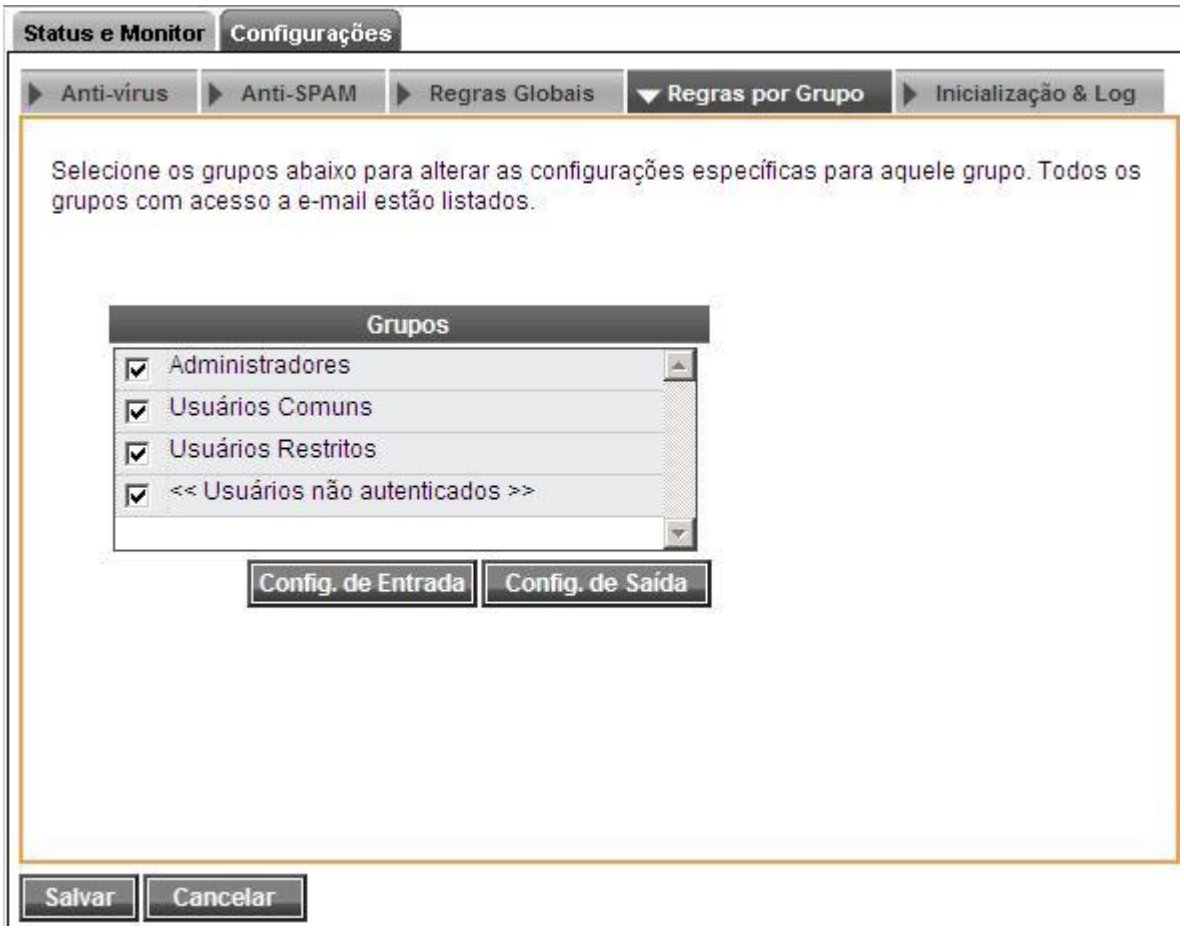
seadas em *Grupos de Usuários*.

As regras por grupo estão divididas em duas categorias: *Configurações de Entrada* e *Configurações de Saída*.

Nas *configurações de entrada* devem ser criadas as regras que serão processadas todas as vezes que uma mensagem for recebida pelo Winconnection 6 e tenha como destinatário um usuário local.

Nas *configurações de saída* devem ser criadas as regras que serão processadas todas as vezes que uma mensagem for recebida pelo Winconnection 6 e tenha como destinatário um usuário que não seja considerado interno.

É importante frisar que, caso uma mensagem seja enviada de um usuário interno para outro usuário interno, apenas a regra de entrada será processada.



Para criar a regra baseada no grupo de usuários, selecione o grupo e clique no botão *Configurações de Entrada* ou *Configurações de Saída*.

Configurações de Entrada:

Anti-Spam:

- **Pontuação**: Pontuação mínima para que a mensagem seja considerada SPAM no grupo em questão.
- **Ação:** O administrador pode definir como as mensagens consideradas SPAM pelas regras criadas devem ser tratadas: *Aceitar mensagem, Marcar assunto com, Deletar a mensagem, Copiar para, Mover para*.

Regras:

O administrador da rede pode criar regras de roteamento das mensagens com base em informações como *De, Para, Cc, Data, Assunto, Prioridade, Endereço Original, Endereço Final, E-mail de, IP do Remetente, Tamanho (bytes).*O administrador da rede pode criar regras de roteamento das mensagens com base em informações como *De, Para, Cc, Data, Assunto, Prioridade, Endereço Original, Endereço Final, E-mail de, IP do Remetente, Tamanho (bytes).*

Tamanho máximo de mensagens:

Utilize estes campos para o controle do tamanho de mensagens de domínios externos.

Filtros de anexos (extensões de arquivos):

Ação: Indica se as extensões serão bloqueadas ou se somente as extensões mencionadas no campo acima serão permitidas.

Extensões: Neste campo, o administrador pode informar quais extensões de arquivos do anexo serão bloqueadas para as mensagens de saída. As extensões deverão ser separadas por vírgula, por exemplo: exe, scr, pif.

Configurações de Saída:

Tamanho máximo da mensagem:

Neste campo deverá ser informado o tamanho máximo das mensagens que estão sendo enviadas. Lembrando que caso a mensagem seja enviada para um domínio local, somente as Configurações de Entrada terão efeito sobre ela.

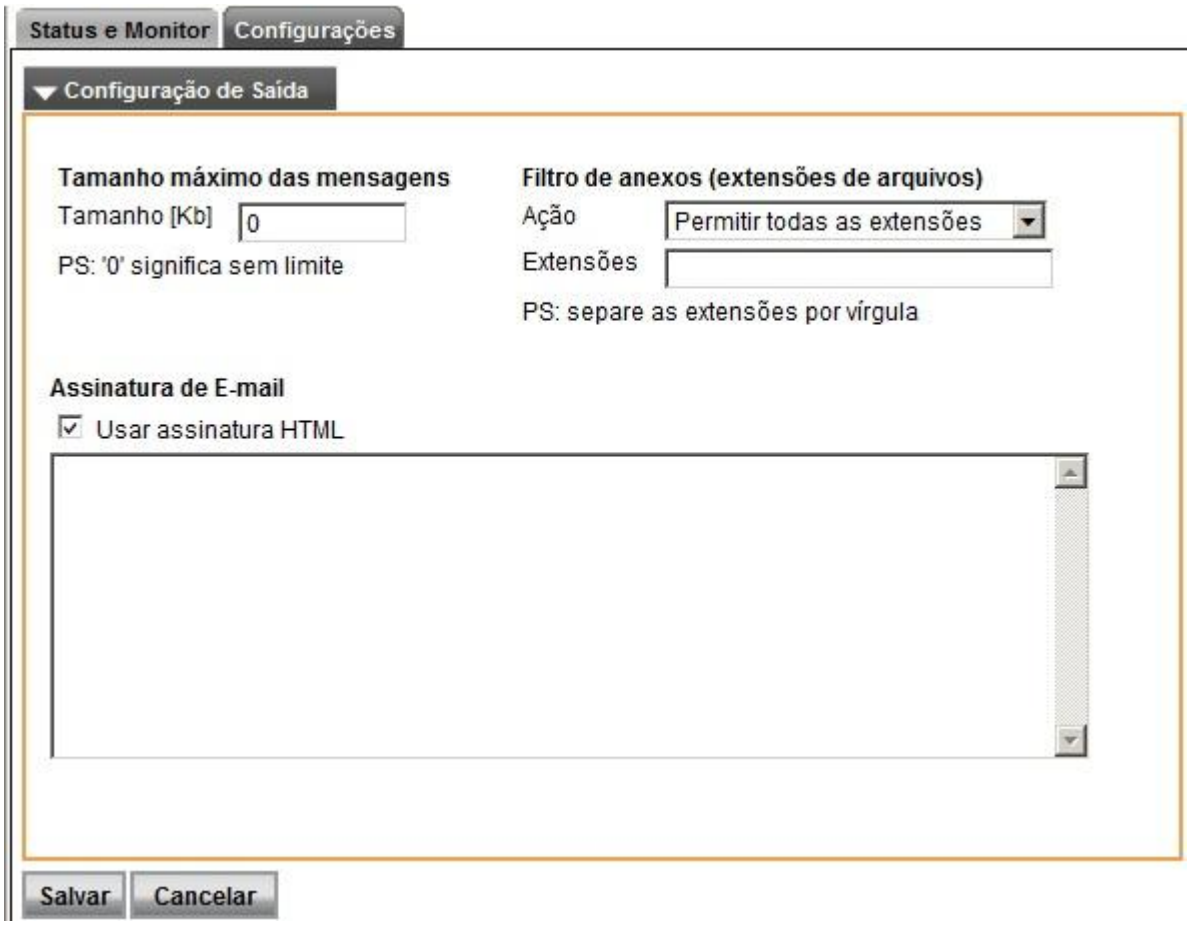
Filtro de anexos (extensões de arquivos):

Ação: Indica se as extensões serão bloqueadas ou se somente as extensões mencionadas no campo acima serão permitidas.

Extensões: Neste campo, o administrador pode informar quais extensões de arquivos do anexo serão bloqueadas para as mensagens de saída. As extensões deverão ser separadas por vírgula, por exemplo: exe, scr, pif.

Assinatura:

Neste campo, é possível adicionar uma assinatura HTML. Para isso, basta habilitar a opção "Usar Assinatura HTML" e digitar no campo abaixo a assinatura desejada.



Guia Configurações | Inicialização & Log:

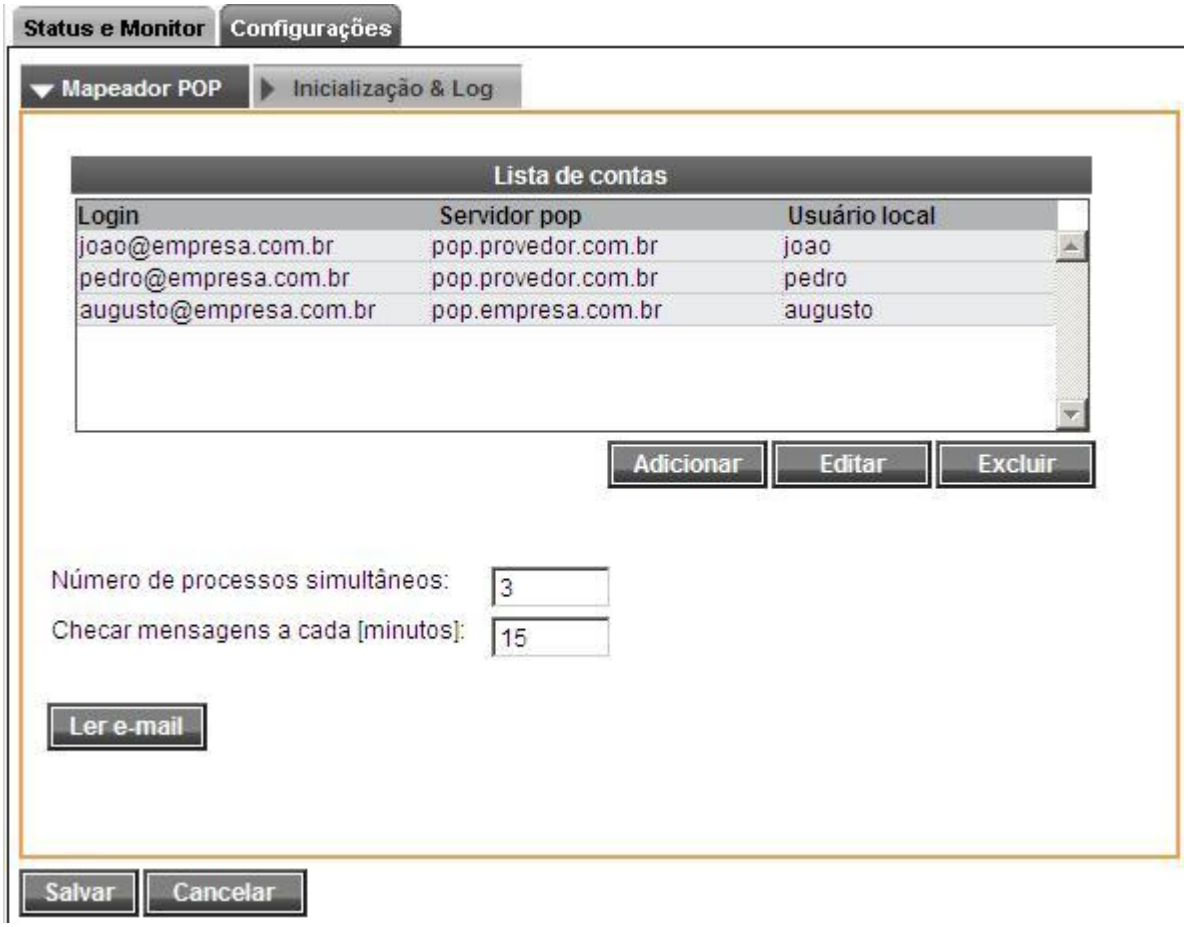
- **Iniciar automaticamente:** Habilite essa opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/MAIL_DISPATCHER.LOG":** O arquivo em bloco de notas (MAIL_DISPATCHER.LOG) será criado no diretório C:\Arquivos de programas\Winco\Winconnection 6\LOGS e conterá todas as informações referentes a este serviço.

7.4. Mapeador POP

Este serviço é utilizado para tratar do recebimento de mensagens periodicamente. O **Mapeador POP** acessa as caixas postais e recebe os e-mails, armazenando nos Usuários Locais, permitindo com isto que este serviço receba e armazene localmente as mensagens enviadas para os servidores externos.

Este serviço não tem porta local, visto que é um serviço do sistema.



Guia Configurações | Mapeador POP:

- **Lista de Contas**: Armazena as caixas postais externas. Utilize os botões Adicionar, Editar e Excluir para manipular as informações sobre estas caixas postais.

- **Número de processos simultâneos**: Define quantas caixas postais serão lidas simultaneamente. Aumente este número se o tempo de coleta de e-mail for muito longo. Note, porém, que o aumento deste número diminui a disponibilidade da conexão para usuários que desejam navegar e degrada o desempenho do servidor. O recomendado é usar até 5 processos simultâneos.

- **Checar mensagens a cada [minutos]**: Define o período entre conexões para envio de e-mail. Se sua conexão for direta com a internet (ADSL, Satélite, LP dados) digite nesse campo 1 minuto. Se for discada, deixe em 30 minutos ou ajuste de acordo com as necessidades de sua empresa.

Ao adicionar ou editar uma conta no **Mapeador POP**, as seguintes opções estarão disponíveis.

Geral:

- **Login:** Digite aqui o login do usuário no provedor onde a caixa postal se encontra. Para ter certeza qual é o login, verifique no cliente de e-mail (outlook, eudora, etc.) do usuário qual a conta que ele usa.

- **Senha:** Digite aqui a senha de acesso à caixa postal do provedor, a mesma usada no cliente de e-mail (outlook, eudora, etc.) do usuário. Caso não saiba a senha, entre em contato com o seu provedor.

- **Servidor POP:** Digite aqui o nome do Servidor POP3 do provedor onde a caixa postal se encontra. Normalmente é "pop.provedor.com.br", mas pode ser "mail.provedor.com.br" ou somente "provedor.com.br".

- **Usuário local:** Digite aqui o nome do usuário (cadastrado previamente, consulte o capítulo Usuários para mais informações), lista ou ainda outra caixa postal remota que deve receber a mensagem.

- **Cópia para:** Caso seja necessário enviar cópias da mensagem para mais um usuário, utilize este campo. Caso seja necessário enviar cópias para mais de um usuário, utilize uma lista.

- **Conta ativada:** Indica se a conta está recebendo ou não via *Mapeador POP*. Se esta opção estiver desmarcada, o **Winconnection 6** não recolhe os e-mails.

- **SSL:** Caso o servidor POP de seu provedor exija conexão segura (SSL), habilite a opção "Utilizar conexão segura (SSL)". Caso você tenha um e-mail do **Gmail**, altere a porta do POP para **995.**

- **Distribuir localmente baseado em username:** Somente selecione esta opção quando for utilizar coleta de mensagens para o domínio ("*Domain POP Collection*"). Neste caso, os nomes dos usuários locais serão procurados nos cabeçalhos da mensagem recebida nos campos "To:" e "Cc:". Caso o usuário exista, a mensagem será redirecionada para este. Caso contrário, esta é entregue ao usuário padrão, definido no campo "Usuário Local".

  Atenção: Esta opção é útil quando o contrato com o provedor de acesso provê "alias de e-mail" ao invés de caixa postal, mas se ativada indevidamente causará duplicidade das mensagens enviadas/recebidas na caixa postal interna do usuário!

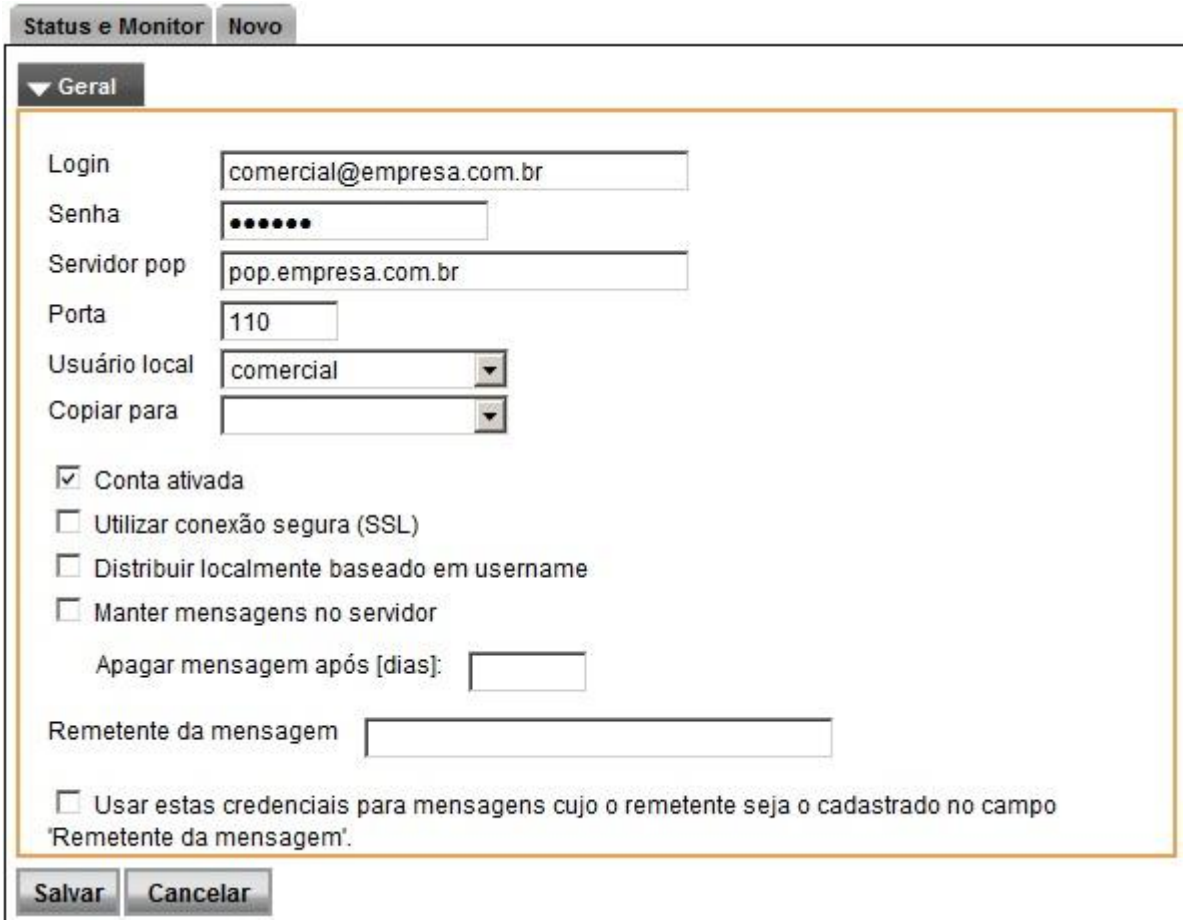
- **Manter mensagens no servidor:** Mantêm uma cópia da mensagem no servidor. Este processo é usado quando o usuário deseja receber os e-mails no escritório, mas consultar em casa também.

- **Apagar mensagem após [dias]:** Indica quanto tempo as mensagens devem ficar no provedor antes de serem apagadas.

- **Usar credenciais ao enviar e-mail cujo remetente seja igual a:** Esta opção é destinada em que o *Relay Remoto* (SMTP remoto usado para enviar as mensagens) obriga que a autenticação seja feita pelo usuário que está enviando a mensagem.

  Por exemplo: Os e-mails enviados por claudio@provedor.com.br só podem ser enviados se o usuário claudio se autenticar.

  Neste caso, é necessário habilitar a opção *"Usar estas credenciais ao enviar e-mail cujo remetente seja"* e digitar o e-mail do remetente.



Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/POPMAP.LOG":** O arquivo em bloco de notas (POPMAP.LOG) será criado no diretório C:\Arquivos de programas\Winco\Winconnection 6\LOGS e conterá todas as informações referentes a este serviço.

7.5. Servidor POP3

O **Servidor POP3** é necessário quando o **Winconnection 6** é utilizado como **Servidor de E-mail**, sendo utilizado um programa cliente de e-mail (Eudora, Outlook, etc.) para receber as mensagens nas estações dos usuários.

Guia Configurações | Geral:

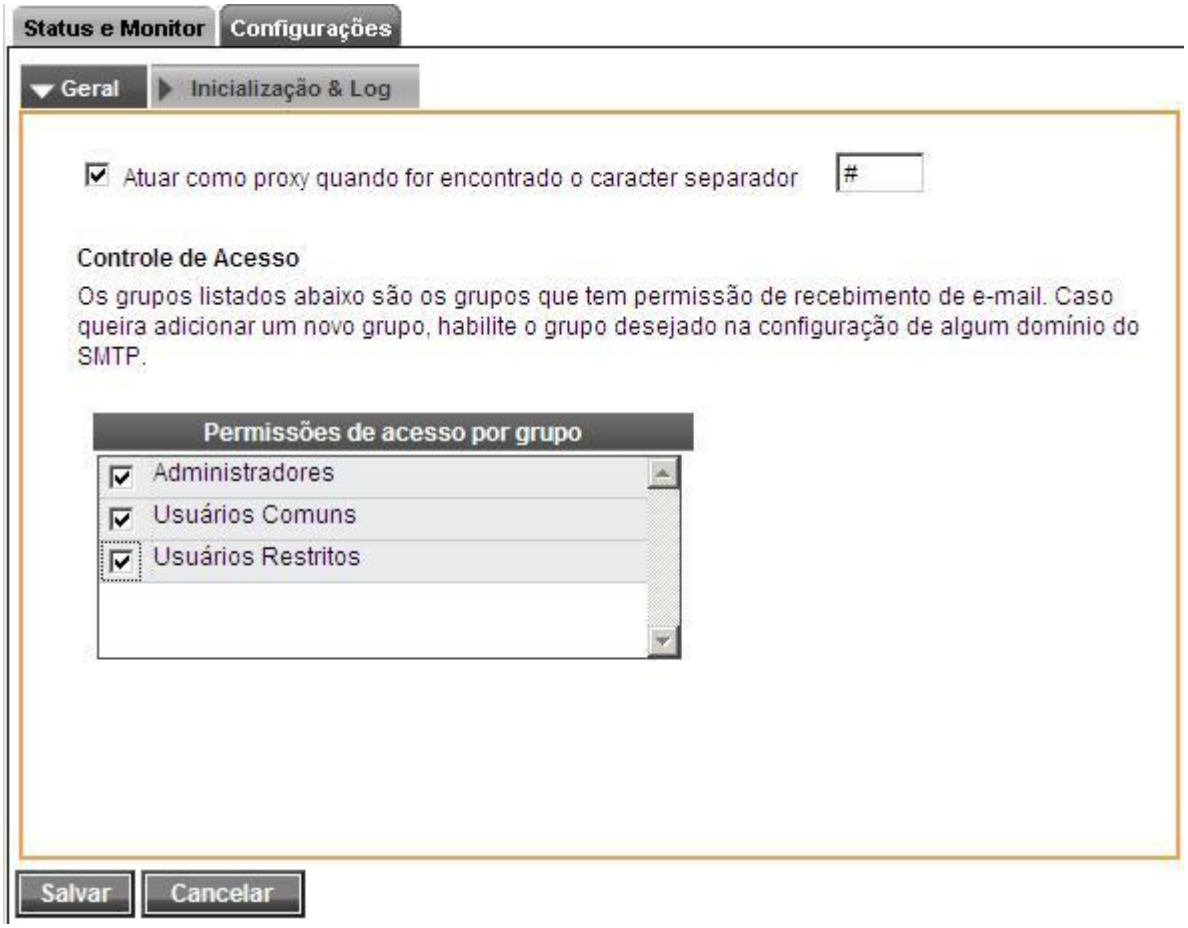
- **Atuar como proxy quando for encontrado o caractere separador**: O Servidor POP3 também funciona como *Proxy POP3*, para possibilitar o acesso às caixas postais de outros servidores de e-mail. Basta haver uma configuração com caractere separador para ele aceitar a conexão como proxy.

  Esta configuração define o símbolo que será utilizado para separar o login do usuário do nome do Servidor POP. Se o caractere for '**#**', o nome utilizado para ler as mensagens será login#pop.provedor.com.br.

- **Controle de Acesso**

  Os grupos listados e habilitados nesta seção são os grupos que têm permissão de recebimento de e-mail. Para que os grupos fiquem visíveis nesta seção, é necessário primeiramente habilitar o grupo desejado na configuração de algum do Servidor SMTP.

  - **Permissão de Acesso por Grupo**: Habilita a utilização do serviço por Grupo de Usuários. Portanto, o Grupo de Usuários que não estiver habilitado nesta opção não terá direito de receber e-mails no *Servidor POP3*.



Guia Configurações | Inicialização & Log:

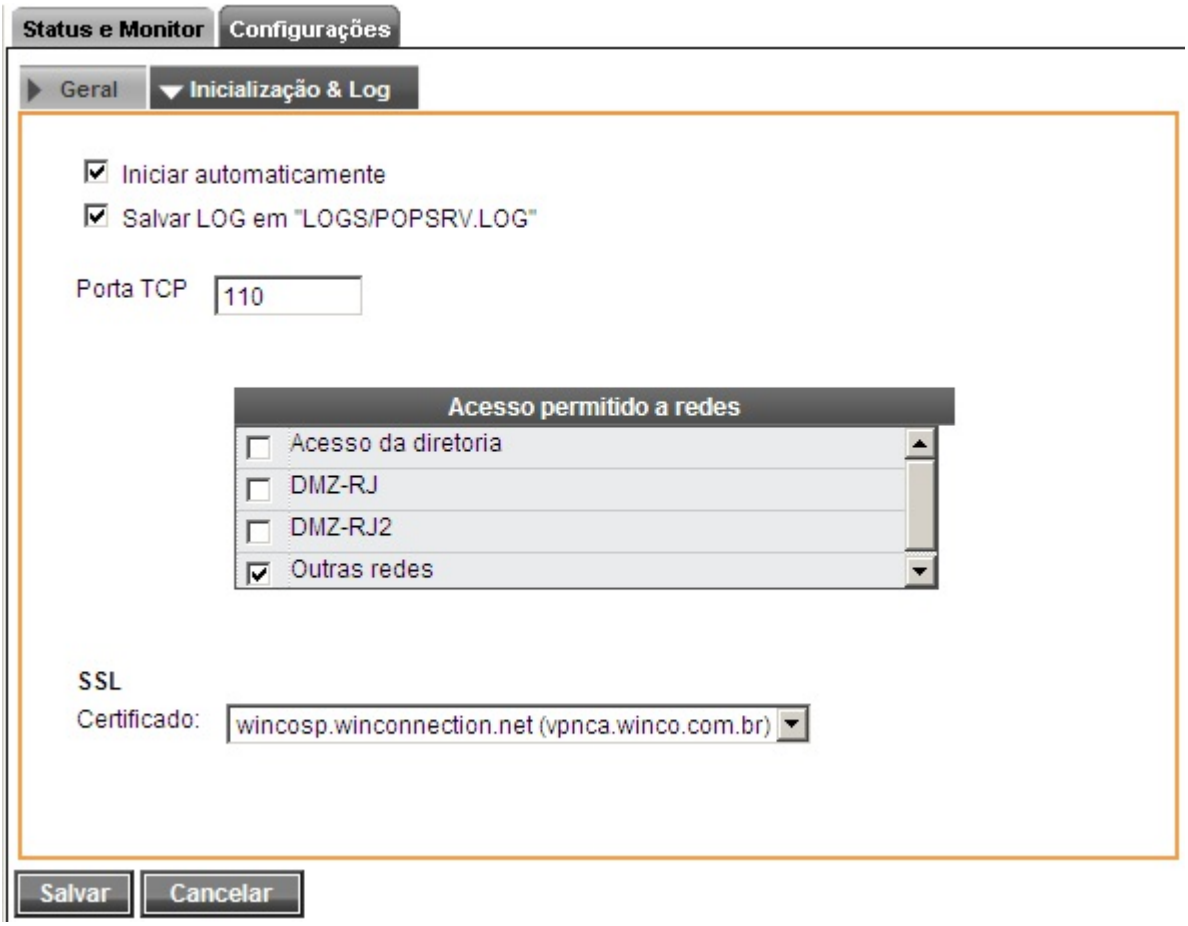
- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o Winconnection 6.

- **Salvar LOG em "LOGS/POPSRV.LOG":** O arquivo em bloco de notas (POPSRV.LOG) será criado no diretório C:\Arquivos de programas\Winco\Winconnection 6\LOGS e conterá todas as informações referentes a este serviço.

- **Porta TCP:** A porta padrão para este serviço é **110**, mas pode ser alterada nesse campo.

- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.

- **SSL:** Esta opção ativa a utilização da criptografia SSL (*Secure Sockets Layer*). Um SSL faz com que o serviço **Servidor POP 3** se torne um serviço seguro (desde que o campo **Porta TCP** seja alterado para a porta **995**). O administrador da rede deverá selecionar qual *Certificado SSL* será utilizado.



7.6. Servidor IMAP

O **Winconnection 6** oferece suporte ao protocolo **IMAP**.

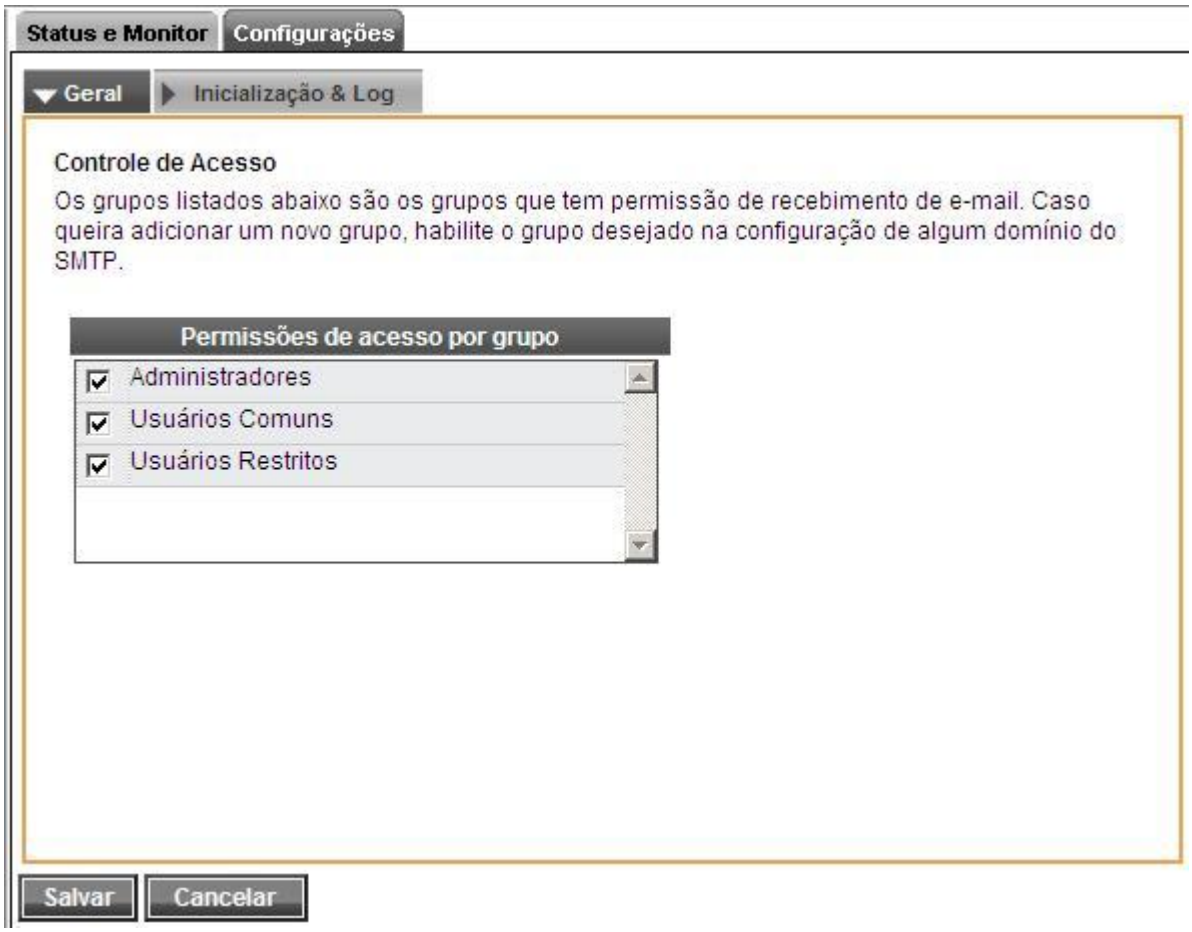
O serviço **Servidor IMAP** é necessário quando o provedor de e-mail utiliza o protocolo *IMAP* e o **Winconnection 6** está sendo utilizado como **Servidor de E-mail**, sendo usado um programa cliente de e-mail (Eudora, Outlook, etc.) para receber as mensagens nas estações dos usuários.

Guia Configurações | Geral:

Controle de Acesso

Os grupos listados e habilitados nesta seção são os grupos que têm permissão de recebimento de e-mail. Para que os grupos fiquem visíveis nessa seção, é necessário primeiramente habilitar o grupo desejado na configuração de algum do Servidor SMTP.

Permissão de Acesso por Grupo: Habilita a utilização do serviço por Grupo de Usuários. Portanto, o Grupo de Usuários que não estiver habilitado nesta opção não terá direito de receber e-mails no *Servidor IMAP*.



Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/IMAP.LOG":** O arquivo em bloco de notas (IMAP.LOG) será criado no diretório C:\Arquivos de programas\Winco\Winconnection 6\LOGS e conterá todas as informações referentes a este serviço.

- **Porta TCP:** A porta padrão para este serviço é **143**, mas pode ser alterada nesse campo.

- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.

- **SSL:** Esta opção ativa a utilização da criptografia SSL (*Secure Sockets Layer*). Um SSL faz com que o serviço **Servidor IMAP** se torne um serviço seguro (desde que o campo **Porta TCP** seja alterado para a porta 993). O administrador da rede deverá selecionar qual *Certificado SSL* será utilizado.

7.7. Servidor SMTP

Guia Configurações | Servidor SMTP:

A guia **Servidor SMTP** deve ser configurada sempre que o servidor de correio interno do **Winconnection 6** for utilizado. Através do **Servidor SMTP**, o programa cliente de e-mail envia mensagens a todos os destinatários, sejam eles locais (na mesma rede) ou externos (endereços de internet externos).

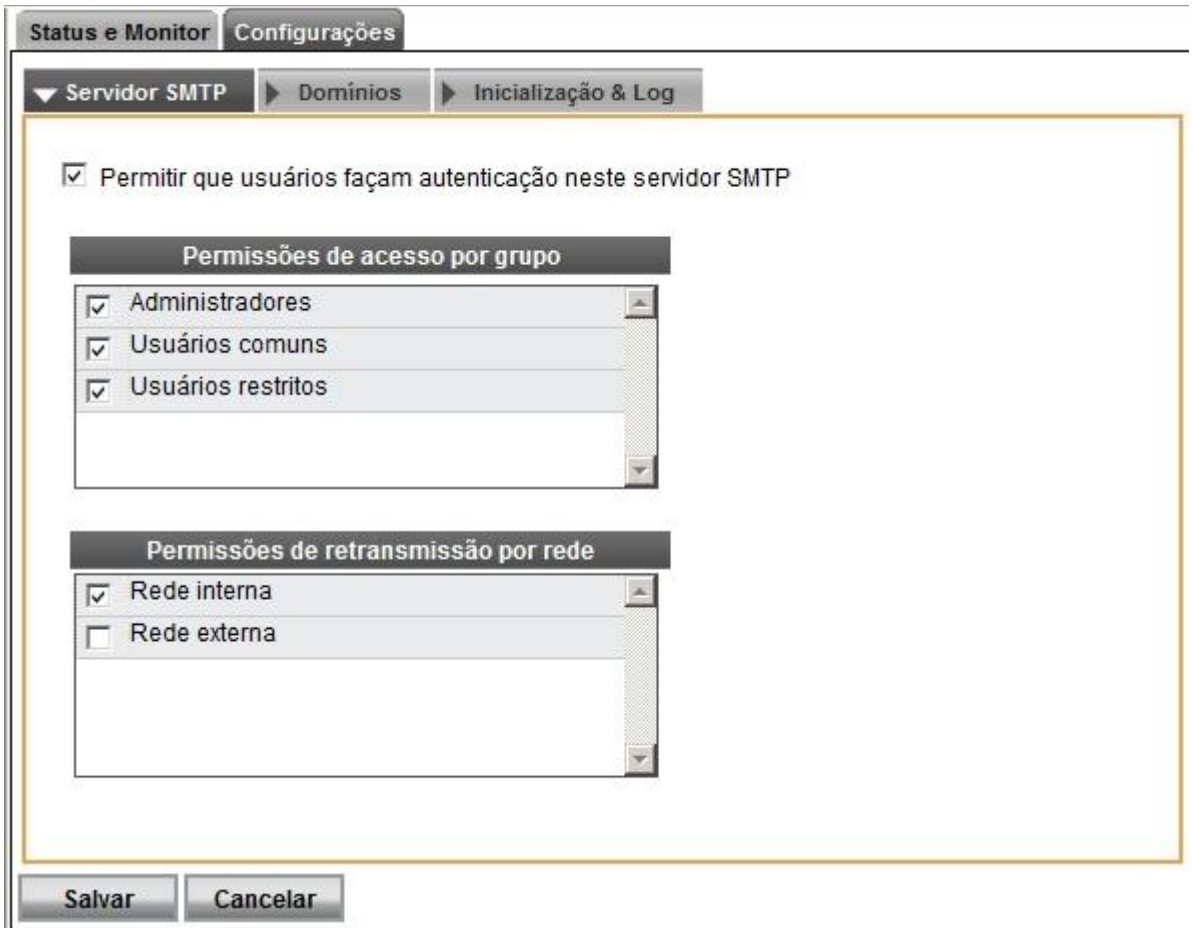
Sempre que o **Winconnection 6** recebe uma mensagem para enviar via **Servidor SMTP**, imediatamente distribui a mensagem a todos os destinatários internos. Se houver algum destinatário externo, de acordo com o tratamento na guia Domínios, a mensagem é encaminhada para a fila de mensagens.

- **Permitir que os usuários façam autenticação neste Servidor SMTP:** Habilita o pedido de Autenticação de SMTP neste servidor. Isto permite que o administrador da rede possa definir se o **Servidor SMTP** aceitará a definição de grupos de usuários que possam entregar no **Servidor SMTP**. Se esta opção estiver **desabilitada**, a configuração *Permissões de acesso por grupo* não funcionará.

- **Permissões de acesso por grupo:** O **Servidor SMTP** pode entregar as mensagens mediante autenticação dos usuários no servidor. Esta opção indica quais grupos de usuários terão direito a se autenticar no **Servidor SMTP** para a entrega de mensagem.

  Quando um usuário não está na *rede permitida* para retransmissão, ele pode entregar mesmo assim, porém o grupo dele deve estar ativo nesta opção. Veja em Usuários como incluir um usuário em um grupo.

- **Permissões de retransmissão por rede:** O controle mais simples do **Servidor SMTP** é a permissão de envio via a(s) rede(s) que ele faz "relay". O administrador pode indicar neste campo quais redes ele deseja fazer a entrega sem precisar que o usuário faça a autenticação de SMTP para o envio.



Guia Configurações | Domínios:

Esta guia do **Servidor SMTP** disponibiliza funções que permitem redirecionar os e-mails enviados para serem roteados internamente, enviados para contas externas ou fazerem parte de outros domínios.

O campo **Lista de Domínios** exibe a lista de domínios hospedados neste computador.

Para configurar o SMTP de saída é necessário editar a opção **"<Outros Domínios>"**. Além disso, é possível *Incluir*, *Alterar* ou *Excluir* os domínios locais.

Ao editar a opção **<Outros Domínios>**, o sistema abrirá uma tela de diálogo com as seguintes opções de configuração:

Parâmetros de Saída:

- **Entregar mensagens diretamente ao destinatário:** Ativando-se esta opção, o **Winconnection 6** passa a entregar as mensagens diretamente para o SMTP de destino do e-mail.

Neste caso o controle passa a ser totalmente do administrador, contudo se o

IP de conexão estiver em uma *BlackList* (listas que recusam e-mails de determinados IPs) os e-mails poderão não chegar a determinados destinos.

Conexões ADSL residenciais (speedy home, velox, etc.) e muitas conexões via Cable modem estão com problemas de bloqueio no endereçamento IP. As listas Anti-Spam estão bloqueando indiscriminadamente todos os IPs destas redes.

Acesse: http://www.ordb.org/faq/ para mais informações sobre Listas Anti-Spam (ou Black List).

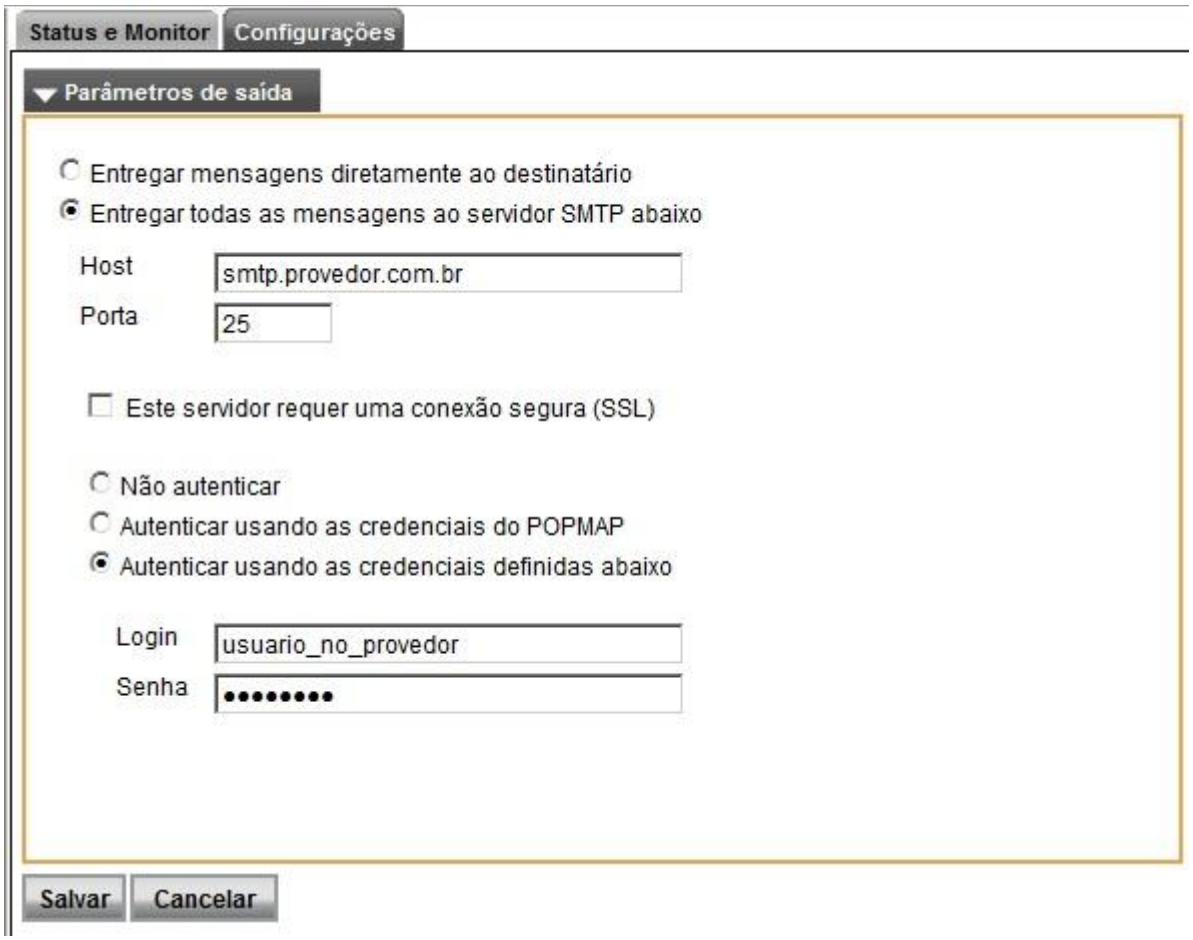
- **Entregar todas as mensagens ao servidor SMTP abaixo:** Habilitando esta opção, é possível definir um SMTP que será responsável pela entrega das mensagens. O SMTP e a porta utilizada devem ser definidos nos campos *Host* e *Porta*.

- **Este servidor requer uma conexão segura (SSL):** Se o SMTP do provedor exigir uma conexão de segurança (SSL) esta opção deve ser habilitada.

- **Não autenticar:** Esta opção permite que não seja feita a autenticação.

- **Autenticar-se usando as credenciais do POPMAP:** Se o provedor exige que a autenticação seja feita pelo usuário que está enviando a mensagem, habilite esta opção. Feito isso, cadastre as informações no serviço Mapeador POP.

- **Autenticar-se usando as credenciais definidas abaixo:** Se o provedor exige autenticação, mas não exige que a autenticação seja feita pelo usuário que está enviando a mensagem, habilite esta opção. No campo *Login* e *Senha* digite o login e a senha de acordo com o seu provedor.



Ao adicionar um novo domínio as seguintes opções estarão disponíveis:

Guia Geral:

Informações básicas:

- **Nome do Domínio:** Este campo é automaticamente associado com * e não é possível editá-lo.

- **Aliases (sep. Vírgulas):** Neste campo, o administrador da rede deve digitar o alias do domínio, por exemplo:

  Domínio: provedor.com.br
  Alias: servidor.provedor.com.br

- **Endereço do "postmaster":** E-mail da pessoa responsável por receber as mensagens que não foram entregues corretamente ou para comunicação de algum problema com o serviço.

Validação dos e-mails:

Comparar parte do usuário do e-mail com o nome de usuário: Se esta opção for habilitada, a validação será feita pela informação dada antes do '@' com o campo de login. Por exemplo:

Login: joao
Domínio: provedor.com.br
E-mail sendo enviado para: joao@provedor.com.br

Neste exemplo, o e-mail será válido, pois existe o usuário joao e o domínio provedor.com.br está cadastrado como domínio local.

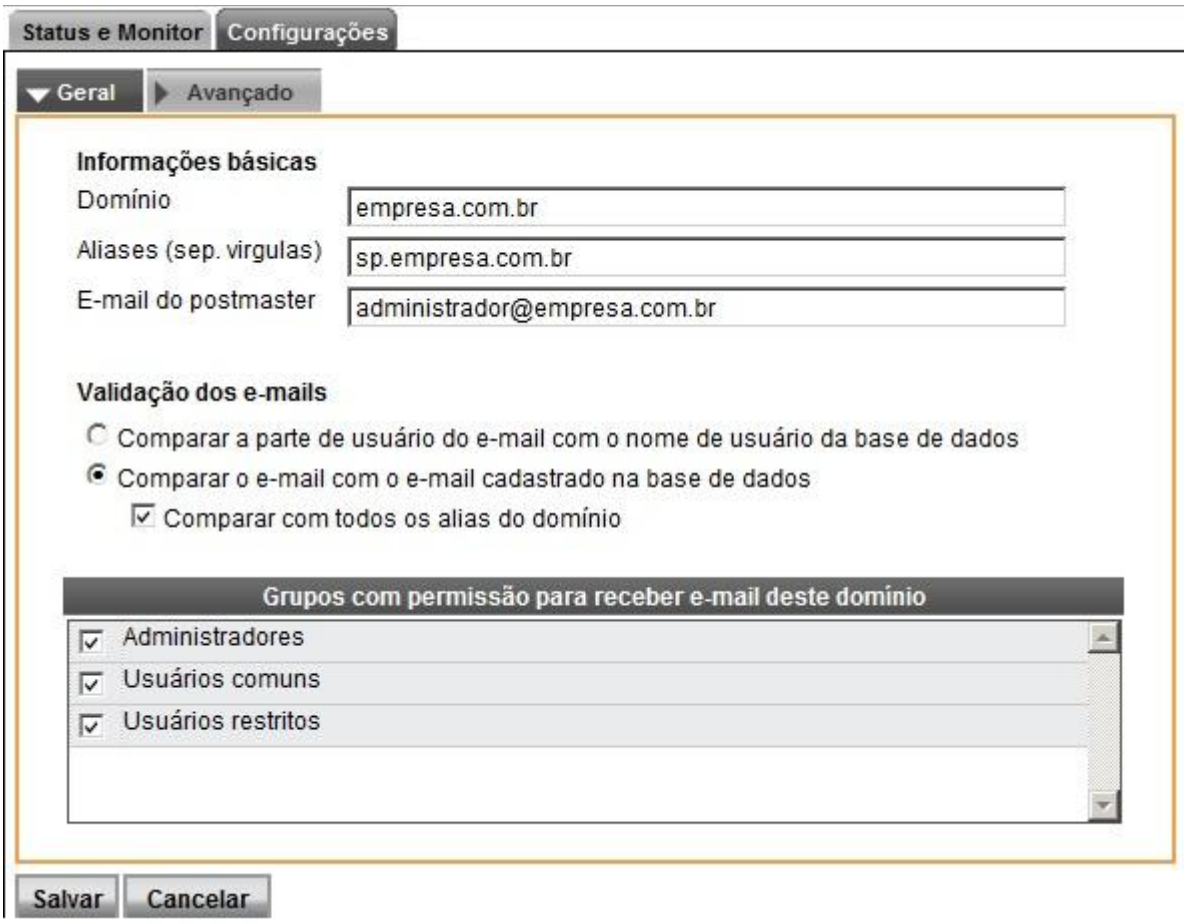
Comparar o campo e-mail com o da base de usuários: Se esta opção for habilitada, a validação será feita pelo campo e-mail na base de usuários do **Winconnection 6**.

- **Comparar com todos os alias do domínio:** Se esta opção for habilitada, além do campo de e-mail será feita uma validação com os alias do domínio. Por exemplo:

  E-mail cadastrado: joao@provedor.com.br. Se chegar um e-mail para joao@servidor.provedor.com.br e servidor.provedor.com.br estiver cadastrado como alias, então o destinatário será considerado válido.

Grupos com permissão para receber e-mails deste domínio:

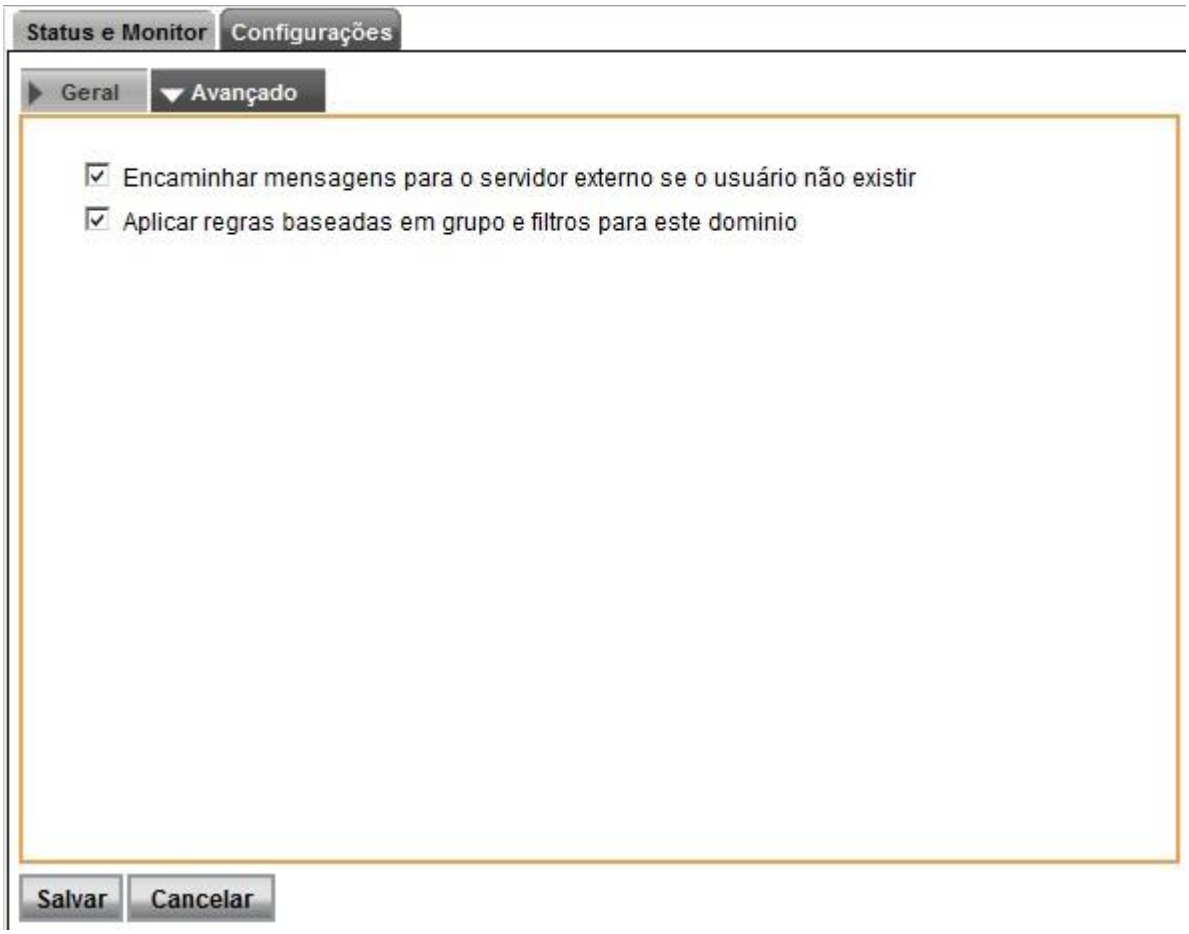
Nesse campo é necessário informar o(s) grupo(s) de usuários que serão verificados, quando o **Winconnection 6** receber uma mensagem.



Guia Avançado:

Encaminhar mensagens para servidor externo se o usuário não existir: Habilitando esta opção, ao se mandar uma mensagem para um usuário não existente no domínio local, ela será encaminhada para a entrega em outro SMTP.

Aplicar regras baseadas em grupos para este domínio: Ativando essa opção, as regras e filtros baseados por grupo serão processados sempre que um e-mail for enviado ou recebido para o domínio que está sendo criado/editado.



Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/SMTPSRV.LOG":** O arquivo em bloco de notas (SMTPS-RV.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.

- **Porta TCP:** É a porta de entrega externa do *Servidor SMTP* do **Winconnection 6**, por padrão **25**. Nesta opção se coloca a porta onde está o *Servidor SMTP* que fará a entrega dos e-mails que é usada quando o *Servidor SMTP* externo está em uma porta não padrão.

- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.

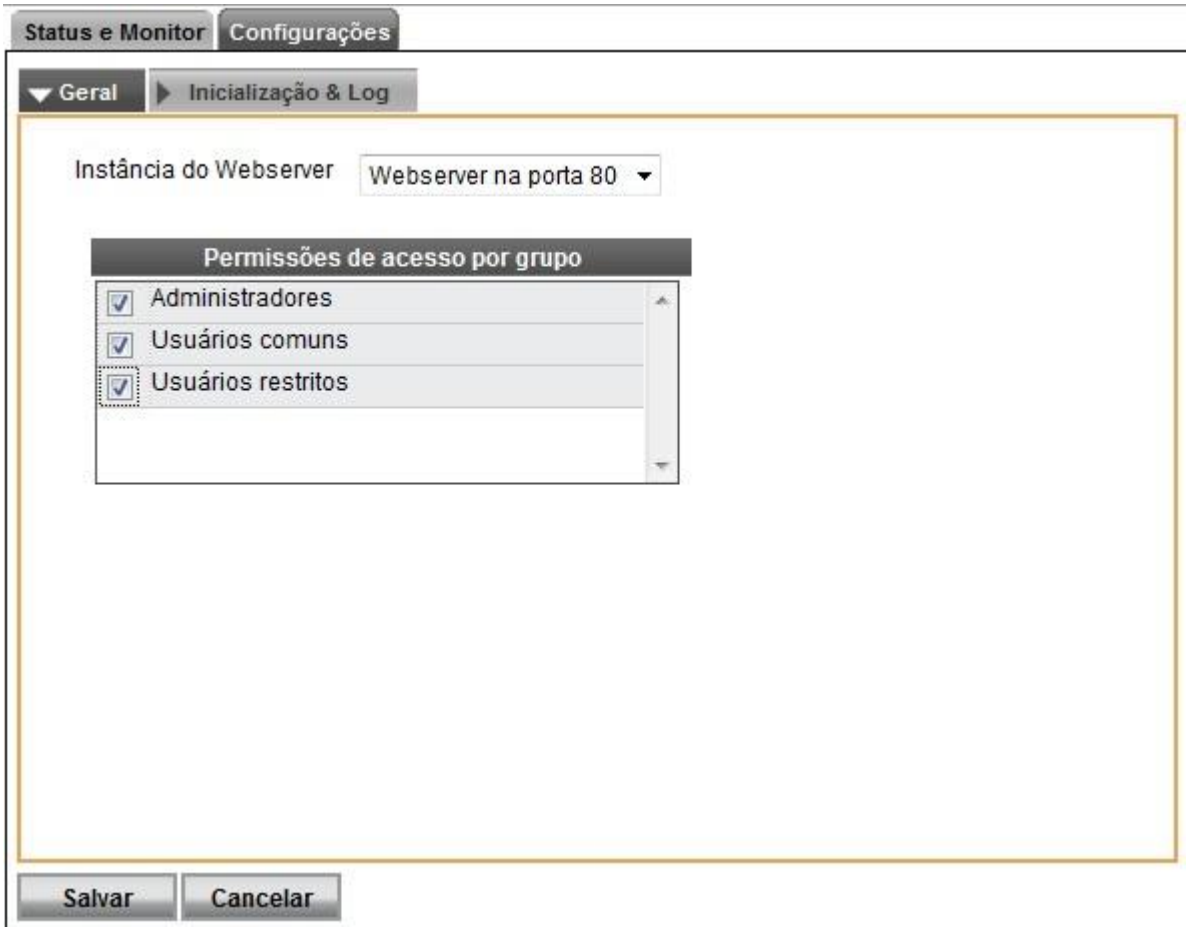
- **SSL:** Esta opção ativa a utilização da criptografia SSL (*Secure Sockets Layer)*. Um

SSL faz com que o serviço **Servidor SMTP** se torne um serviço seguro (desde que o campo **Porta TCP** seja alterado para a porta **465**). O administrador da rede deverá selecionar qual *Certificado SSL* será utilizado.

7.8. Webmail

O serviço **Webmail** permite que os usuários, dentro da empresa ou em trânsito, tenham acesso às suas caixas postais, lendo e enviando e-mails internos ou externos. Este serviço é integrado ao serviço *Web* e por padrão acessado na porta 80.

É possível definir quais grupos de usuários terão acesso ao *Webmail*.



O **Webmail Mobile** também permite que os e-mails sejam acessados pelo celular.

Para acessar o Webmail fora da rede, é necessário digitar o seguinte endereço no navegador: http://ip_externo_do_servidor/mwebmail.

Observação: Se o IP do seu provedor for dinâmico, você poderá utilizar o Cliente DDNS.

8. Serviços Locais

Veja a seguir a descrição de cada serviço disponível no menu *Serviços Locais*.

8.1. Cliente DDNS

Quando um usuário contrata uma conexão de internet, seja ela discada ou banda larga, a maioria dos provedores disponibiliza um IP Real para usuário.

Um IP Real é um IP que é visível por qualquer outro computador na internet, ao contrário do IP Inválido. Esse segundo tipo de IP é usado em redes corporativas e não pode ser acessado pelos computadores de fora da rede corporativa.

Os IPs Reais (no Brasil) costumam ter o prefixo 200.XXX, e os IPs Inválidos (no mundo todo) têm os prefixos 10., 192.168. e 172.16 até 172.31.

Para colocar um serviço qualquer na internet, um requerimento básico é que o computador com o serviço tenha um IP Real, de forma que os computadores da Internet possam vê-lo. Quem tem IP Inválido não consegue colocar serviços na internet (pelo menos não sem tem que usar técnicas mais complicadas). Portanto, em tese, todos os usuários com IP Real poderiam registrar domínios, servidores de email e outros serviços usando qualquer provedor de internet.

Porém, o problema que ocorre é que o IP que os provedores disponibilizam aos seus usuários, apesar de ser Real, não é Fixo, ou seja o IP muda a cada reconexão do usuário ou a cada período pré-determinado de horas (*por exemplo:* o IP é 200.1.2.3.4 e de repente muda para 200.222.111.5). Dessa forma, é impossível fornecer serviços usando estes IPs, já que a cada vez que o IP muda, o serviço precisa que ser reconfigurado.

Para resolver este problema foi criado o **DDNS**, que significa **Dynamic Domain Name System**. O conceito é bem antigo, mas a implementação da Winco é extremamente simples de usar. O **DDNS** cria um nome fixo, que passa a representar o IP do usuário, mesmo que este IP mude. Portanto, um usuário registra o nome 'empresa.winconnection.net' e passa a poder usar este nome sempre que quiser se referir ao computador que fornece o serviço.

Este programa utiliza o sistema de nomes de domínio da internet para associar um nome ao computador que o usuário tem conectado na internet.

O **Cliente DDNS** permite que o servidor **Winconnection 6** seja o responsável por monitorar as mudanças de IP que o provedor força e enviar a informação do novo IP para um servidor centralizado que atualiza imediatamente o nome 'empresa.winconnection.net' para se referir ao novo IP.

Em termos práticos, para ativar o serviço, tudo que o usuário tem que fazer é realizar o download do programa **Cliente DDNS** que oferece o registro do domínio. A instalação é feita em apenas 2 passos.

As aplicações práticas são voltadas para o segmento dos usuários domésticos e empresas que necessitam prover serviços externos:

1. Estabelecimento de VPNs.
2. Acesso remoto ao próprio computador.
3. Utilização do computador como Servidor Web, Webmail, Servidores de Email, Servidores de Arquivos, etc.
4. Servidor de jogos.

A lógica é a seguinte:

1) O sistema de subdomínio consiste em associar um nome ao domínio *winconnection.net* ou *ddns.com.br*. Então, este nome passa a ser subdomínio do domínio. Por exemplo: *minhaempresa.winconnection.net* ou m*inhaempresa.ddns.com.br*.

2) Quando for digitada a URL *minhaempresa.winconnection.net* (ou *minhaempresa.ddns.com.br*), o **Servidor DNS** responsável transforma o nome *winconnection.net* (ou o *ddns.com.br*). para seu endereço IP, identificando a máquina que possui esse domínio.

3) Ao localizar o *winconnection.net* (ou o *ddns.com.br*), o **Servidor DNS** avisa que está sendo solicitado o nome *minhaempresa.winconnection.net* (ou *minhaempresa.ddns.com.br*).

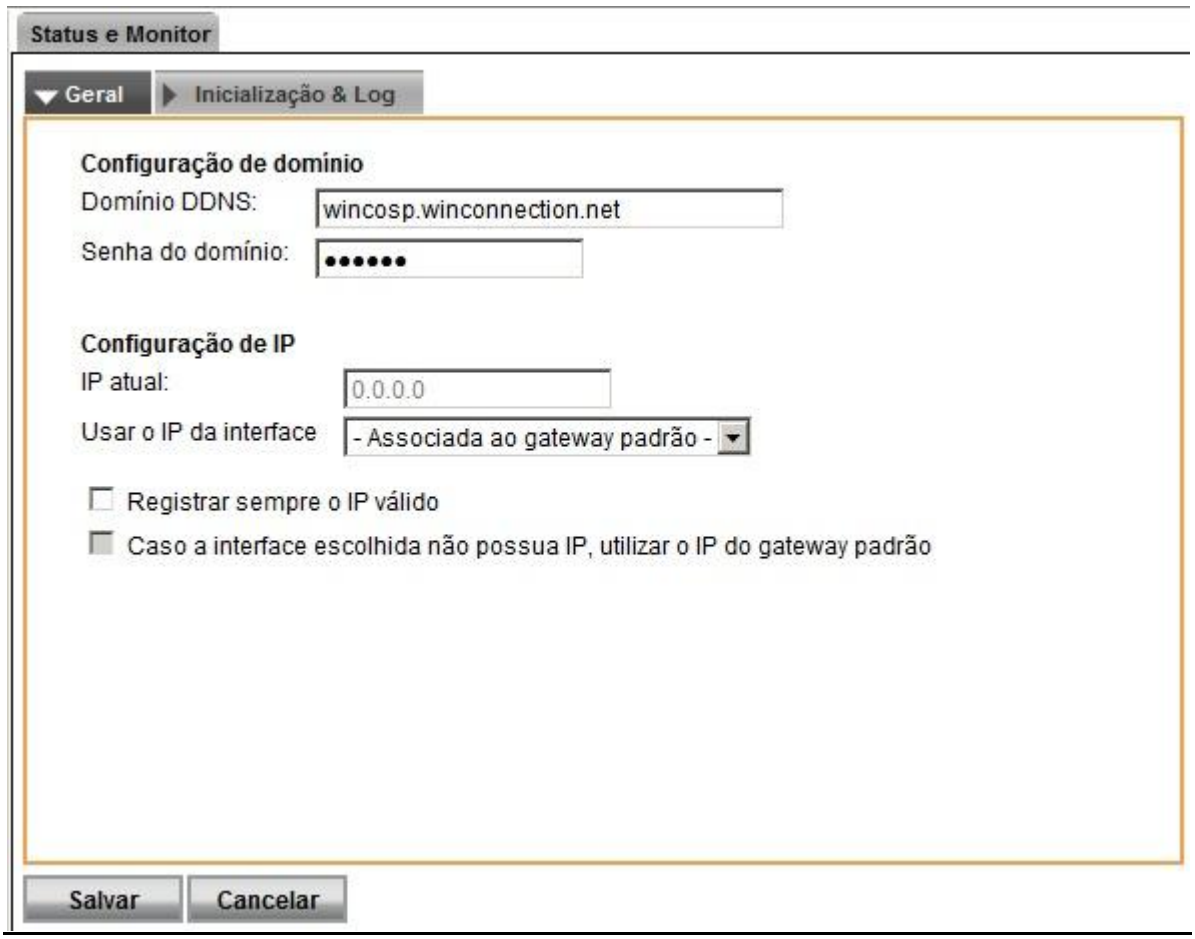
4) O Servidor da Winco responderá que *minhaempresa.winconnection.net* (ou *minhaempresa.ddns.com.br*), está associado ao IP xxx.xxx.xxx.xxx, de acordo com as informações do último acesso do **Agente DDNS**, que fica instalado na máquina onde está a conexão de internet do cliente.

O pacote de instalação do **Cliente DDNS** está disponível na seção de download do nosso site.

Após baixar o programa, execute o arquivo e siga o Assistente de Instalação para iniciar a iniciar a instalação e configuração do programa.

Guia Configurações | Geral:

- **Domínio DDNS:** Neste campo, o administrador da rede deve digitar o domínio cadastrado no sistema **DDNS**.
- **Senha do domínio:** Senha cadastrada no sistema **DDNS**.
- **IP atual:** Exibe o endereço IP atual da conexão.
- **Usar o IP da interface:** Neste campo, é necessário informar o IP de qual interface de rede será utilizado.
- **Registrar sempre o IP válido:** Habilitando esta opção, será feito o registro do endereço de IP válido.



Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/DDNS.LOG":** O arquivo em bloco de notas (DDNS.LOG) será criado no diretório C:\Arquivos de programas\Winco\Winconnection 6\LOGS e conterá todas as informações referentes a este serviço.

8.2. Web

O serviço **Web** do **Winconnection 6** permite a hospedagem de sites diretamente no servidor de rede. A página inicial (index.html) será uma página do **Winconnection 6** que poderá ser alterada. A localização da página está no Diretório Base para serviço dos sites (document root).

Veja a seguir as principais características do serviço **Web**:

- Funciona com o protocolo HTTP/1.0;
- Possibilita incluir arquivos na lista de 'Tipos MIME' independentemente da lista do Windows;
- Suporta apenas um DocumentRoot, e sem alias. Pode disparar SCRIPTS que sejam compatíveis com CGI 1.1, como PHP, PERL e .EXE;
- Suporta atalhos de Diretórios;

O serviço **Web** também serve páginas externas. Para isso, basta apenas que o acesso externo seja permitido. Uma regra no firewall é automaticamente criada no **Winconnection 6** permitindo o acesso à porta 80, quando o administrador da rede desejar que as páginas sejam acessadas externamente.

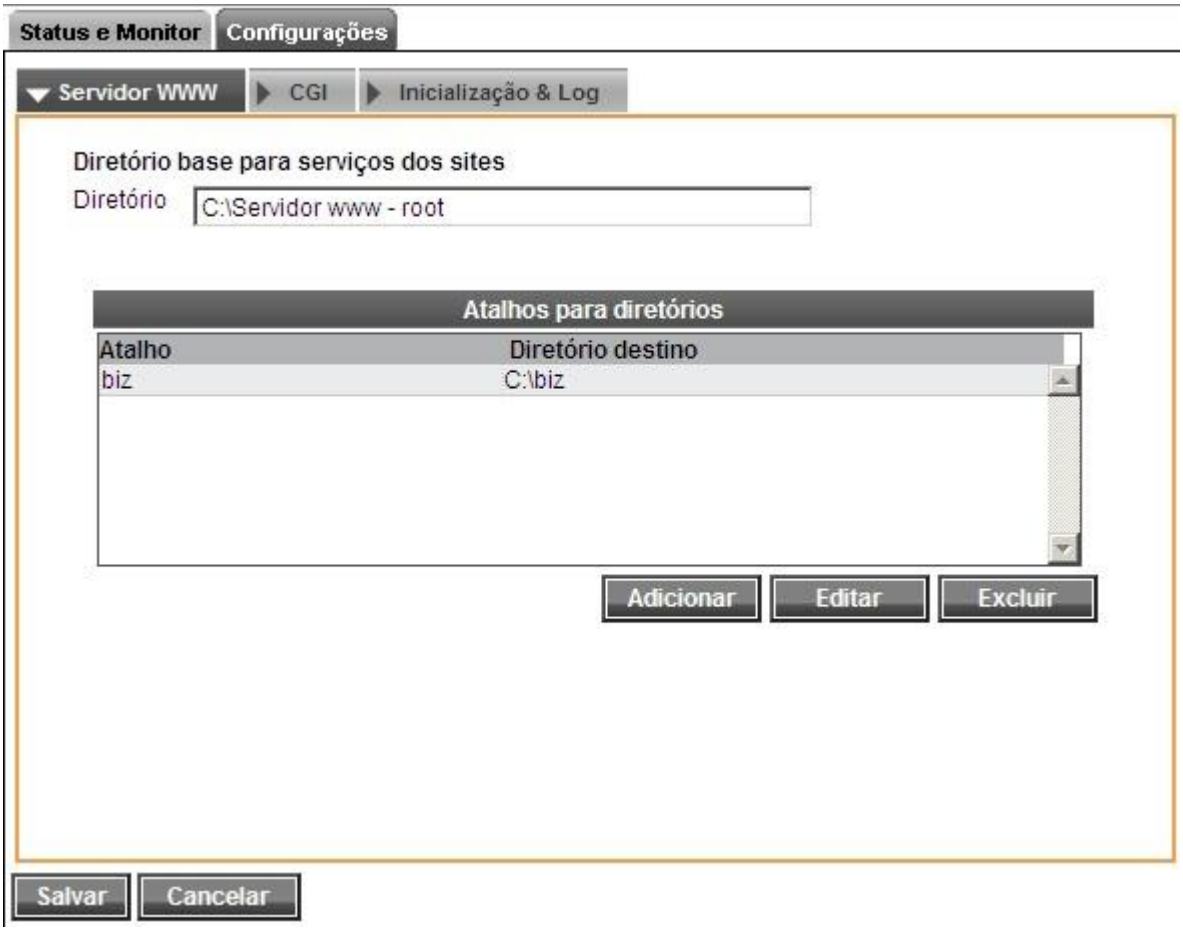
Guia Configurações | Servidor WWW:

- **Diretório base para serviço dos sites:** Diretório onde se encontra as páginas Web. Ao configurar este diretório, o **Winconnection 6** passa a disponibilizar as informações contidas nele como um site na internet.

- **Atalhos para diretórios:** Permite a inclusão de um determinado diretório na máquina, fazendo com que este diretório vire um alias.

Por exemplo: C:\meus documentos\comercial\propostas atalho = proposta

Quando se digitar http://servidor/proposta o **Winconnection 6** listará os arquivos daquele diretório. Esta solução é extremamente útil para compartilhar informações para os colaboradores, via WEB.



Guia Configurações | CGI:

- **Extensões de servidor:** Permite incluir as extensões associadas às aplicações CGI. Toda vez que tiver determinada extensão listada, vai executar determinado CGI.

Por exemplo: Extensão = .PHP execute c:\php\php.exe

Guia Configurações | Inicialização & Log:

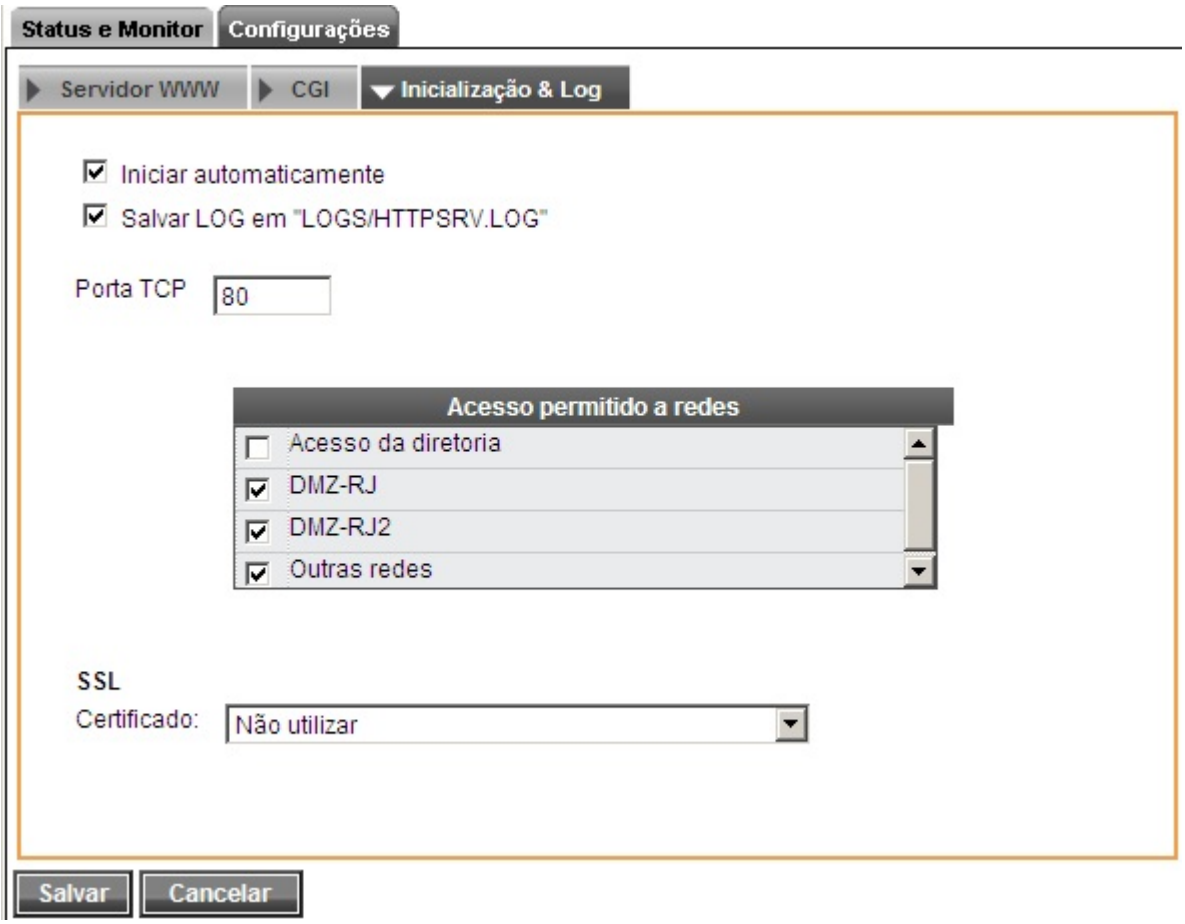
- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/HTTPSRV.LOG":** O arquivo em bloco de notas (HTTPSRV.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.

- **Porta TCP:** A porta padrão para este serviço é **80**, mas pode ser alterada nesse campo.

- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.

- **SSL:** Esta opção ativa a utilização da criptografia SSL (*Secure Sockets Layer*). Um SSL faz com que o serviço **Web** se torne um serviço seguro (desde que o campo **Porta TCP** seja alterado para a porta **443**). O administrador da rede deverá selecionar qual *Certificado SSL* será utilizado.

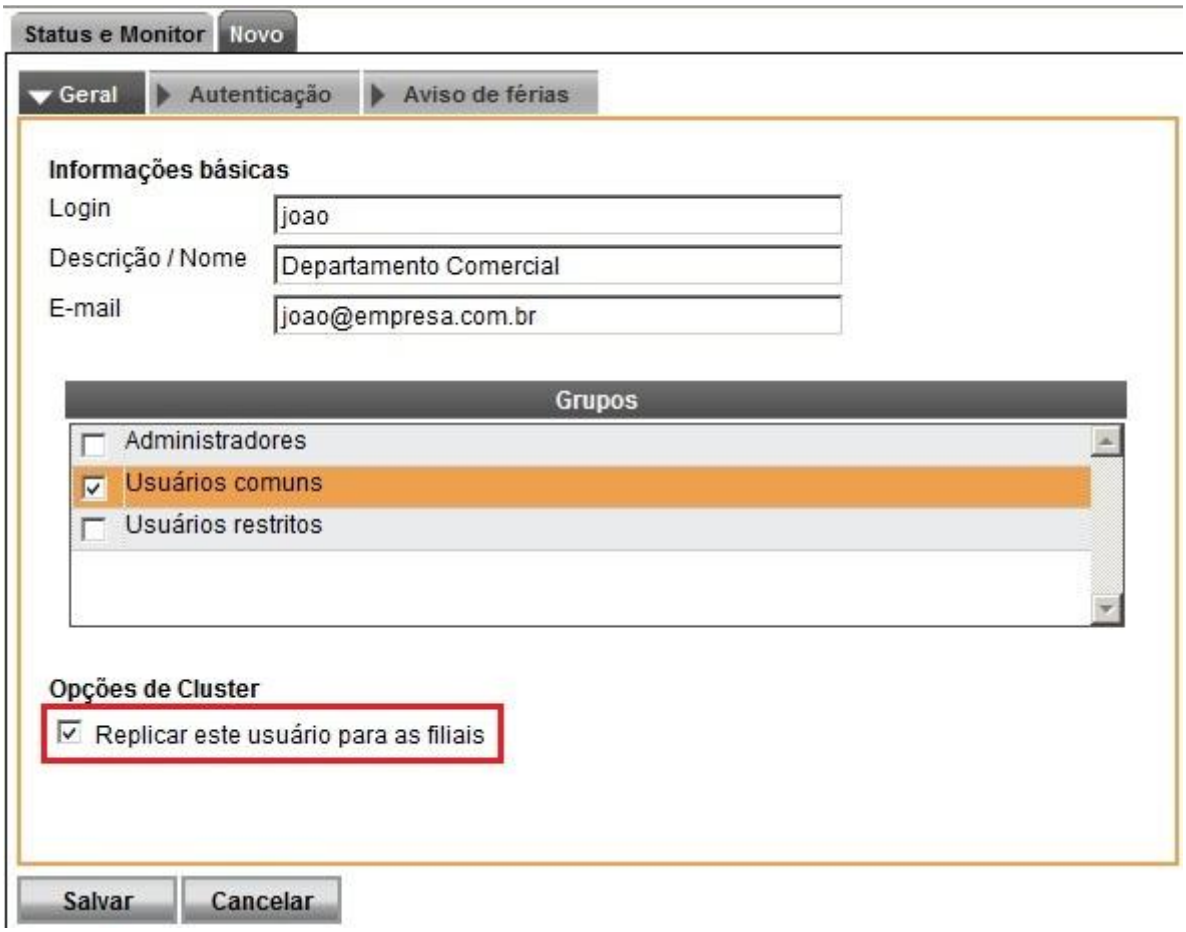


8.3. Cluster Master

O módulo **Winconnection Branch Office** permite centralizar o gerenciamento das políticas de acesso à internet através do serviço de cluster. As regras definidas na matriz são automaticamente copiadas para as filiais.

As seguintes configurações do Winconnection poderão ser exportadas automaticamente:

- **Usuários** – desde que a opção *"Replicar este usuário para as filiais"* esteja habilitada no cadastro do usuário, conforme exibido na imagem a seguir:



- **Grupos** – desde que a opção *"Replicar este grupo para as filiais"* esteja habilitada no cadastro do usuário, conforme exibido na imagem a seguir:

- **Configurações de acesso à internet** – por exemplo, lista de sites de bloqueio, configurações de permissão de acesso, etc.

Guia Configurações | Geral:

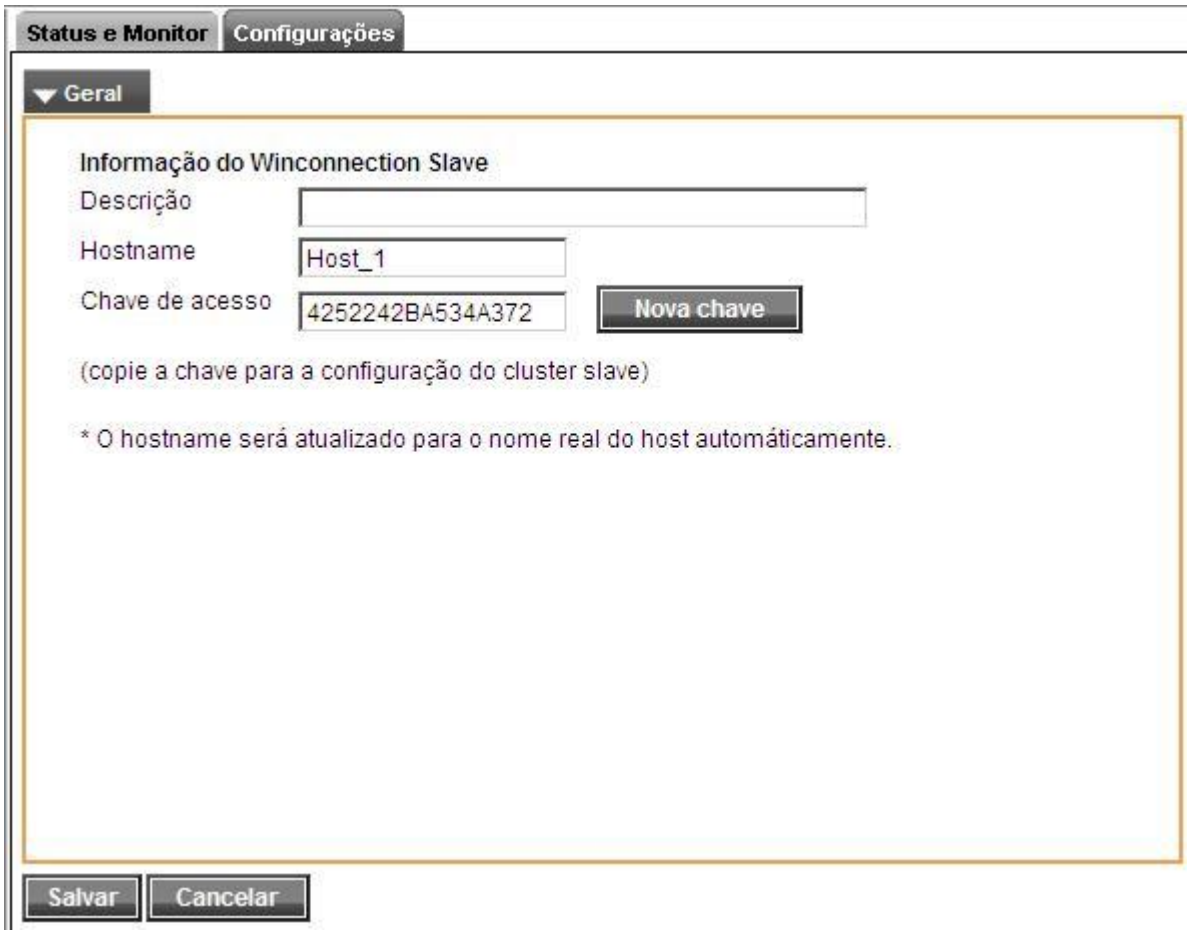
O serviço **Cluster Master** é responsável pelo cadastro das filiais. Para adicionar uma nova filial, é necessário apenas gerar uma chave de acesso, que deve ser cadastrada no serviço de **Cluster Slave** da filial.

Ao adicionar ou editar uma chave de acesso, as seguintes opções estarão disponíveis:

Informações do Winconnection Slave:

- **Descrição:** Informe a descrição da Filial, por exemplo: *Filial SP*.
- **Hostname:** O hostname será atualizado para o nome real do host automaticamente.

- **Chave de acesso:** Esta chave será usada no Winconnection da Filial (serviço *Cluster Slave* da Filial SP). Por medida de segurança, essa chave poderá ser alterada a qualquer momento. Para isso, basta clicar no botão "*Nova Chave"*.



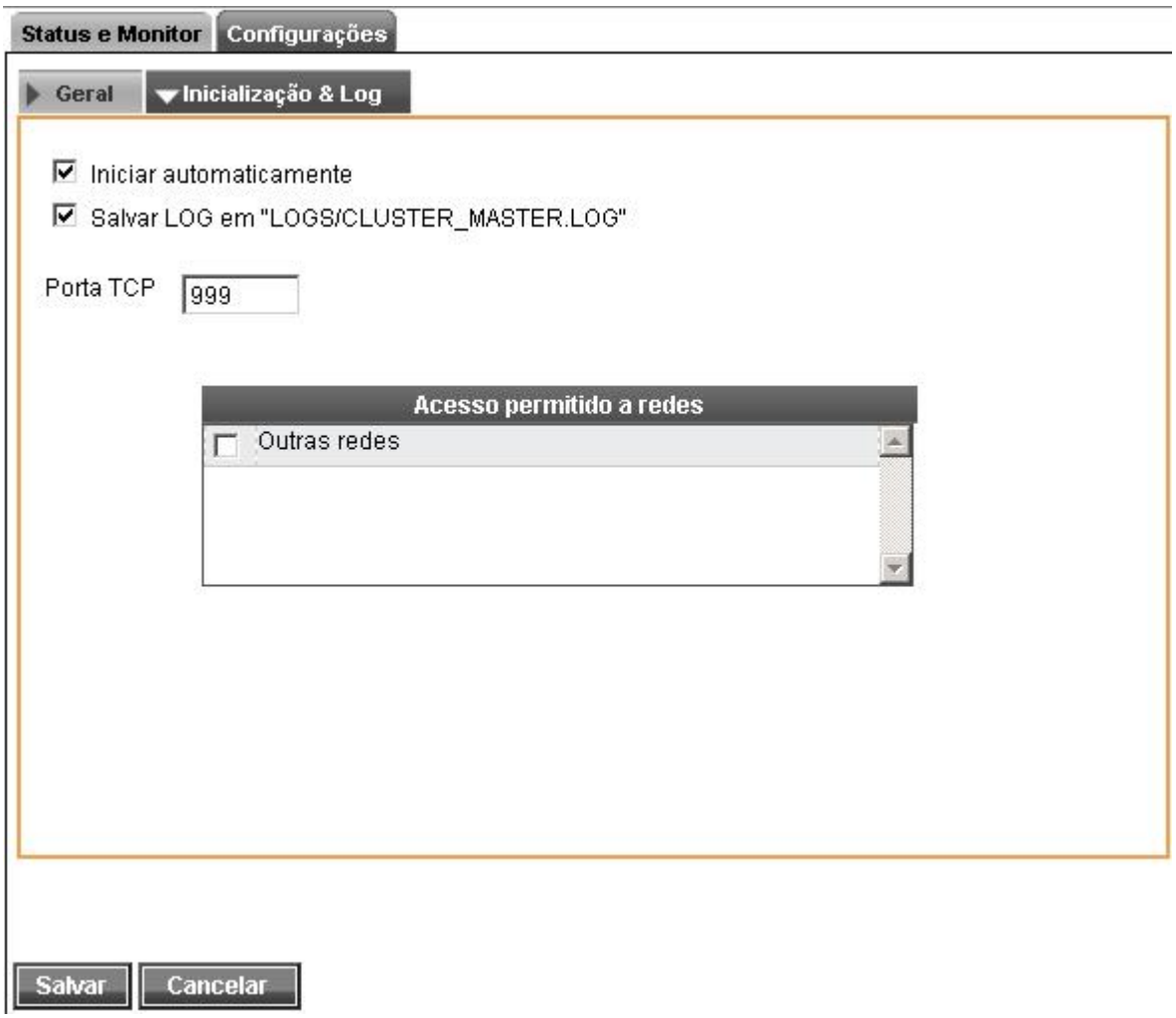
Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/CLUSTER_MASTER.LOG":** O arquivo em bloco de notas (CLUSTER_MASTER.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.

- **Porta TCP:** A porta padrão para este serviço é **999**, mas pode ser alterada nesse campo.

- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.



8.4. Cluster Slave

O serviço **Cluster Slave** deve ser instalado no **Winconnection 6** da **filial** que irá receber automaticamente as configurações realizadas no Winconnection da matriz.

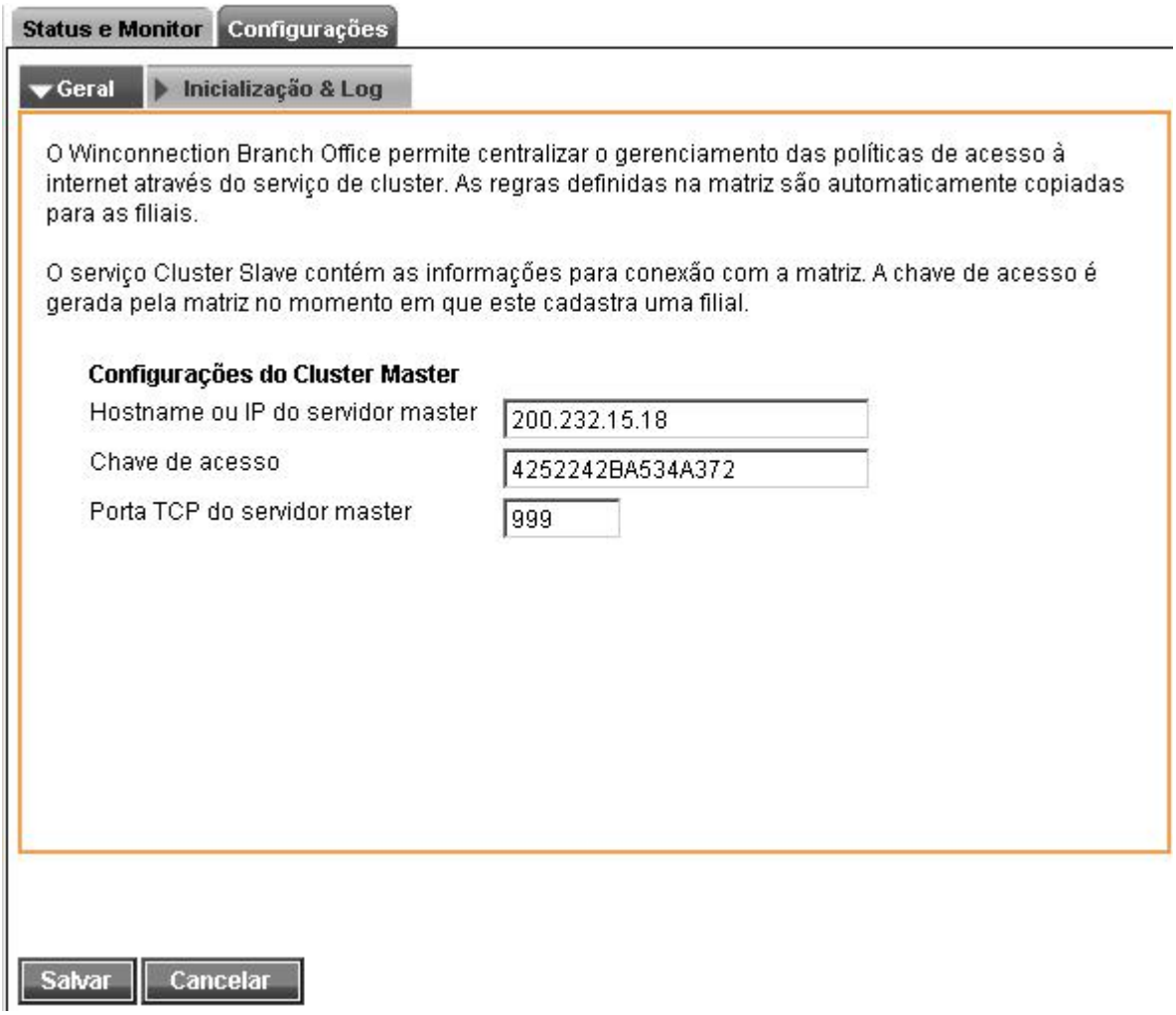
Obs.: A instalação desse serviço depende de uma licença especial, pois o serviço de replicação de configuração é um módulo adicional e deve ser adquirido separadamente.

Configurações do Cluster Master:

- **Hostname ou IP do servidor master:** Nesse campo, é necessário informar o hostname ou endereço IP da máquina onde está instalado o Winconnection na Matriz (por exemplo: 200.232.15.18).

- **Chave de Acesso:** Nesse campo, o administrador da rede deverá informar a chave exibida no serviço **Cluster Master** do **Winconnection 6** que está instalado na Matriz (por exemplo: 4252242BA534A372).

- **Porta TCP do servidor master:** A porta por padrão é a 999. Não é necessário alterar essa porta (ao menos que você a tenha alterado no serviço **Cluster Master** do Winconnection da Matriz).



Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/CLUSTER_SLAVE.LOG":** O arquivo em bloco de notas (CLUSTER_SLAVE.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.

8.5. Servidor VPN

O **Sistema de VPN** do **Winconnection 6** oferece segurança em relação aos seguintes aspectos da comunicação:

- **Privacidade:** Uma criptografia forte garante que ninguém poderá enxergar as informações que passam pela VPN, trafegando entre sua casa e o escritório ou entre duas filiais da sua empresa.

- **Autenticidade:** Certificados Digitais e o uso de senha dão certeza em relação a quem está do outro lado da conexão.

- **Integridade:** Dados não podem ser inseridos ou retirados por alguém de fora, e nem as informações podem ser alteradas.

Além de prover toda esta segurança, o uso da tecnologia SSL para transmissão das informações garante a facilidade de conexão entre as redes, visto que todos os provedores e roteadores lidam bem com este tipo de tecnologia, que está rapidamente se tornando a mais utilizada para conexões VPN.

O **Sistema de VPN** do **Winconnection 6** funciona usando tunelamento SSL. Isto significa que os dados são criptografados e enviados através de uma conexão (ou "túnel") SSL. SSL é o mesmo sistema, com base em certificados digitais, usado nas conexões seguras com os bancos.

Apesar de utilizar uma conexão SSL, qualquer tipo de dado pode trafegar na VPN. Acesso remoto a discos e impressoras, servidores de e-mail e intranets são alguns dos exemplos de aplicações que podem ser usadas.

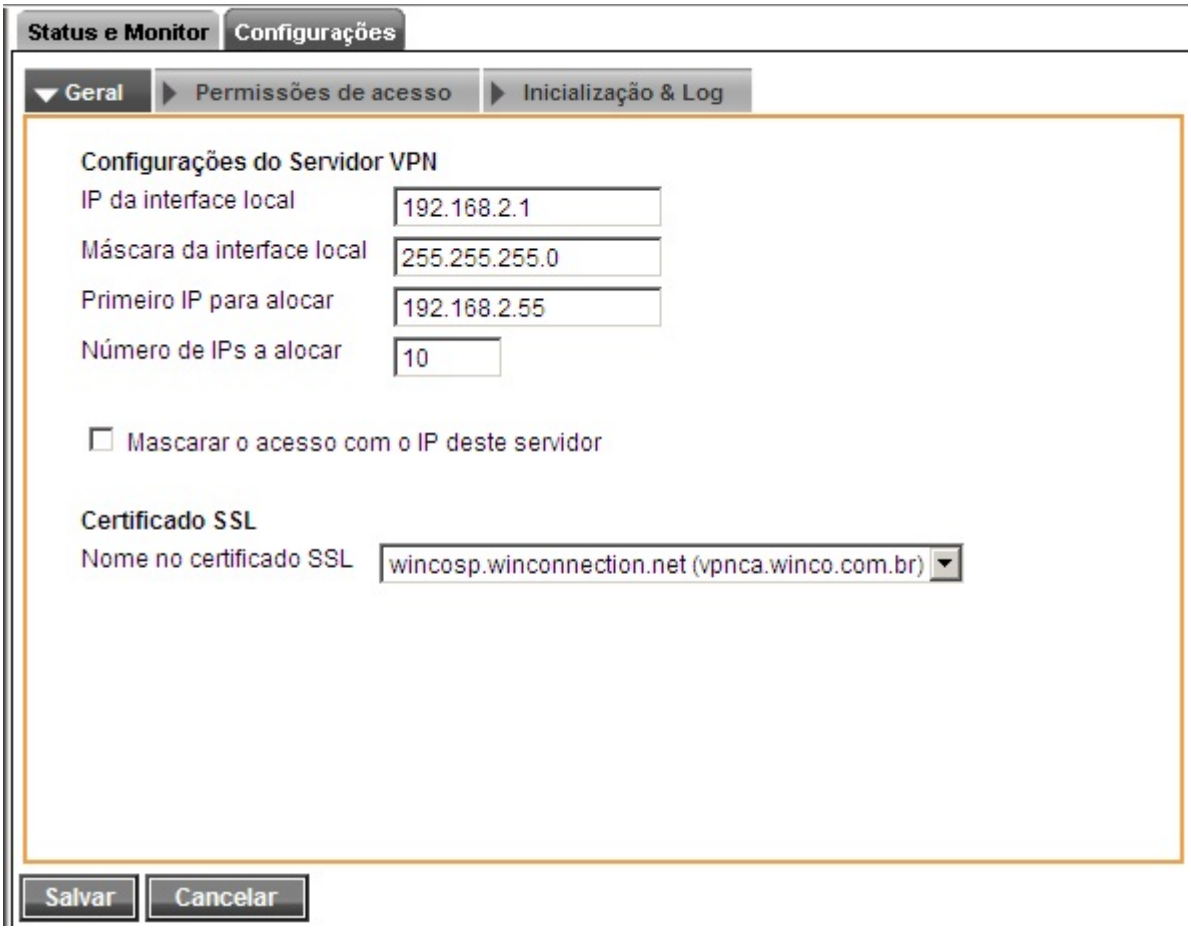
O acesso é bidirecional e, portanto, uma vez conectado à VPN, o computador remoto pode enviar e receber dados pela rede normalmente como se estivesse fisicamente ligado à rede onde está o Servidor VPN. Portanto não há qualquer restrição para que os computadores da rede do escritório central acessem dados localizados no computador remoto.

Obs.: A instalação deste serviço depende de uma licença especial, pois o serviço de VPN é um módulo adicional e deve ser adquirido separadamente.

Guia Configurações | Geral:

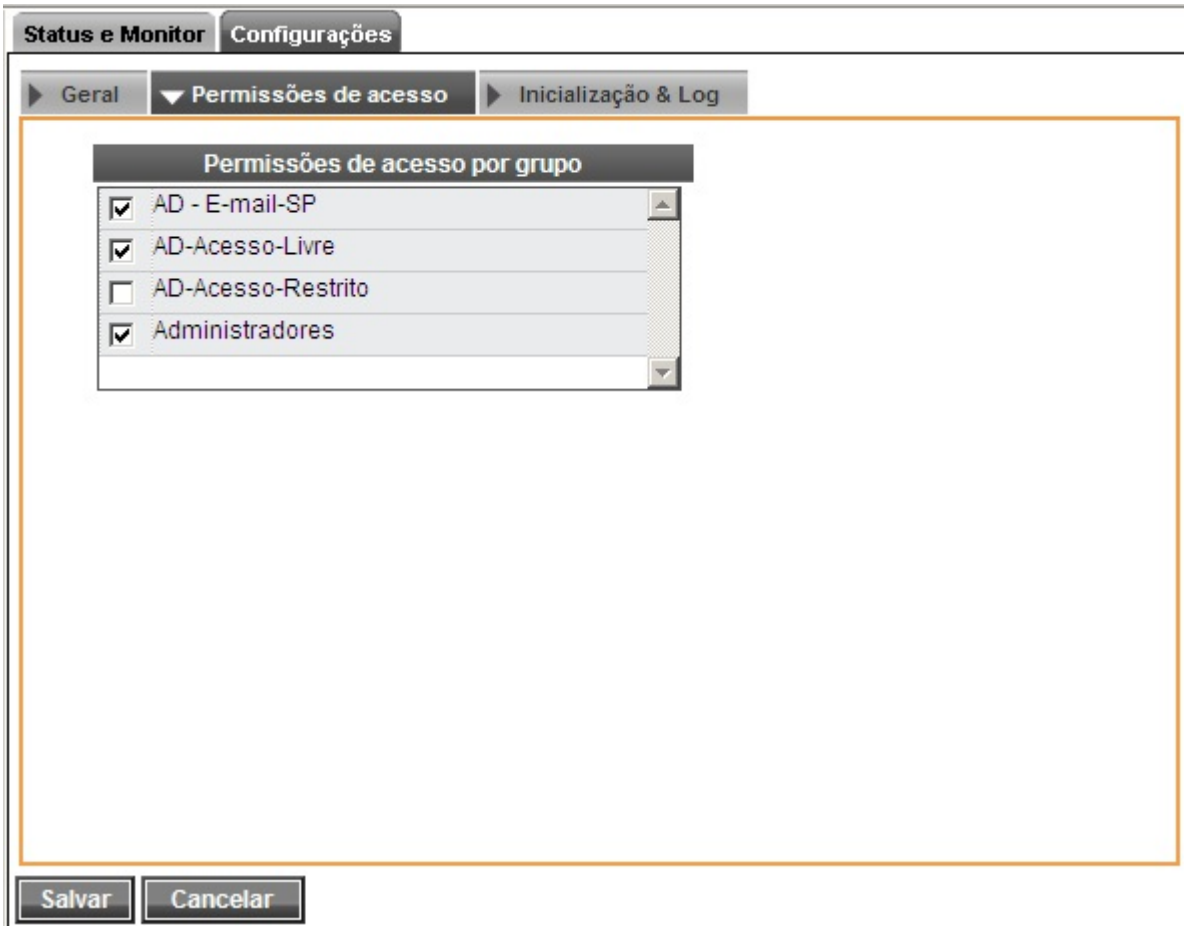
Configurações do Servidor VPN:

- **IP da interface local:** Neste campo, o administrador da rede deve digitar o endereço IP da interface local.
- **Máscara da interface local:** Neste campo, o administrador da rede deve digitar a máscara da interface local.
- **Primeiro IP para alocar:** É necessário separar uma faixa de endereços IPs pertencentes a sua própria rede para os clientes remotos. O primeiro endereço IP dessa alocação deve ser incluído nesse campo.
- **Número de IPs a alocar:** Neste campo, o administrador da rede deve definir o número de endereços IPs que serão alocados.
- **Mascarar o acesso com o IP desse servidor:** Habilitando esta opção, o acesso será mascarado com o endereço IP do servidor.
- **Certificado SSL:**
- **Nome no certificado SSL:** O **Certificado SSL** é utilizado para garantir a legitimidade do serviço de VPN disponibilizado neste computador. Evitando, por exemplo, que hackers usando sistemas de spoofing de IP possam se passar pelo servidor e roubar os dados protegidos. Para tanto, é possível usar certificados existentes no computador.



Guia Configurações | Permissões de acesso:

Nesta guia de configuração é possível indicar os grupos de usuários que terão acesso a este serviço.



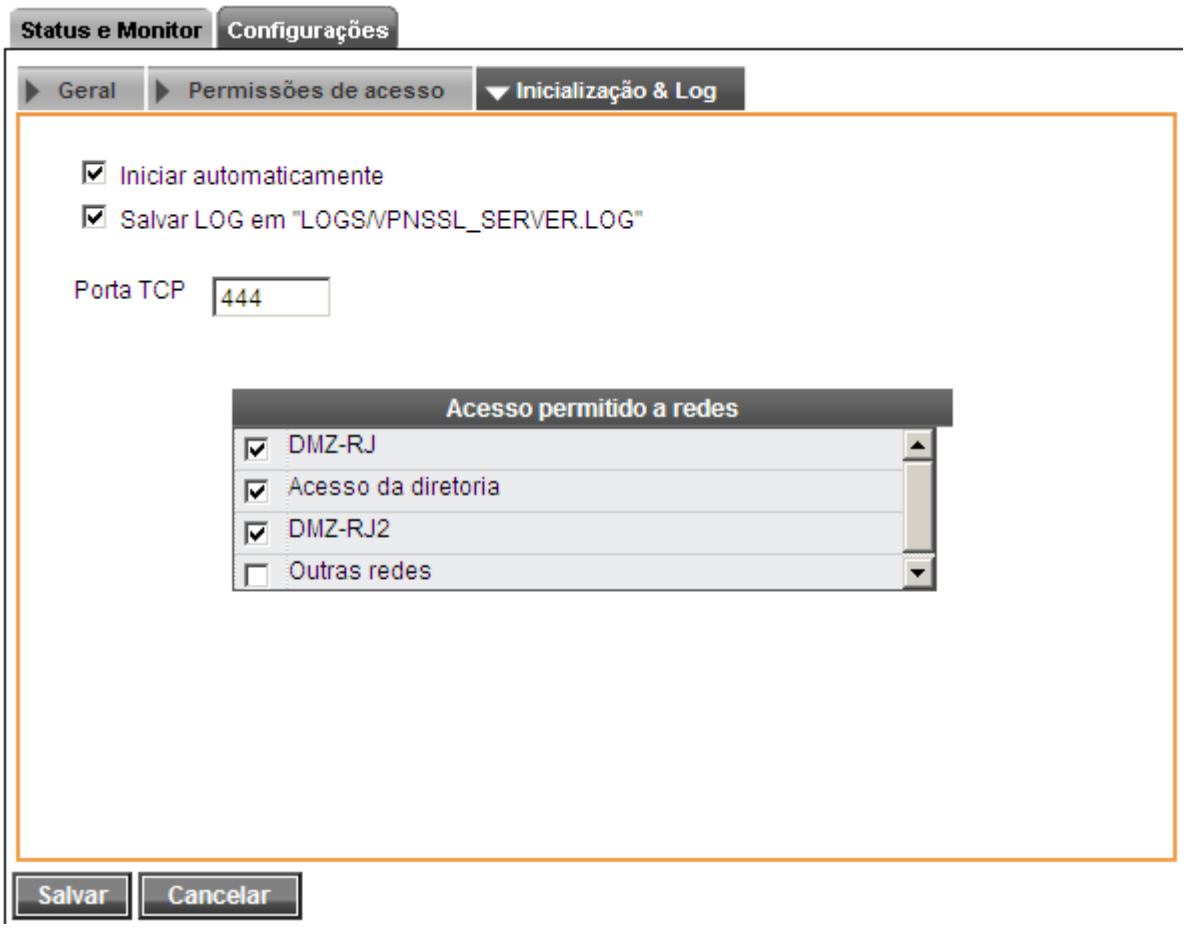
Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/VPNSSL_SERVER.LOG":** O arquivo em bloco de notas (VPNSSL_SERVER.LOG) será criado no diretório C:\Arquivos de programas\Winco\Winconnection 6\LOGS e conterá todas as informações referentes a este serviço.

- **Porta:** Neste campo é definido a porta de acesso para o Servidor VPN. A porta padrão é a 444, mas pode ser alterada.

- **Acesso permitido a redes:** Indica as redes que têm acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.



8.6. Cliente VPN

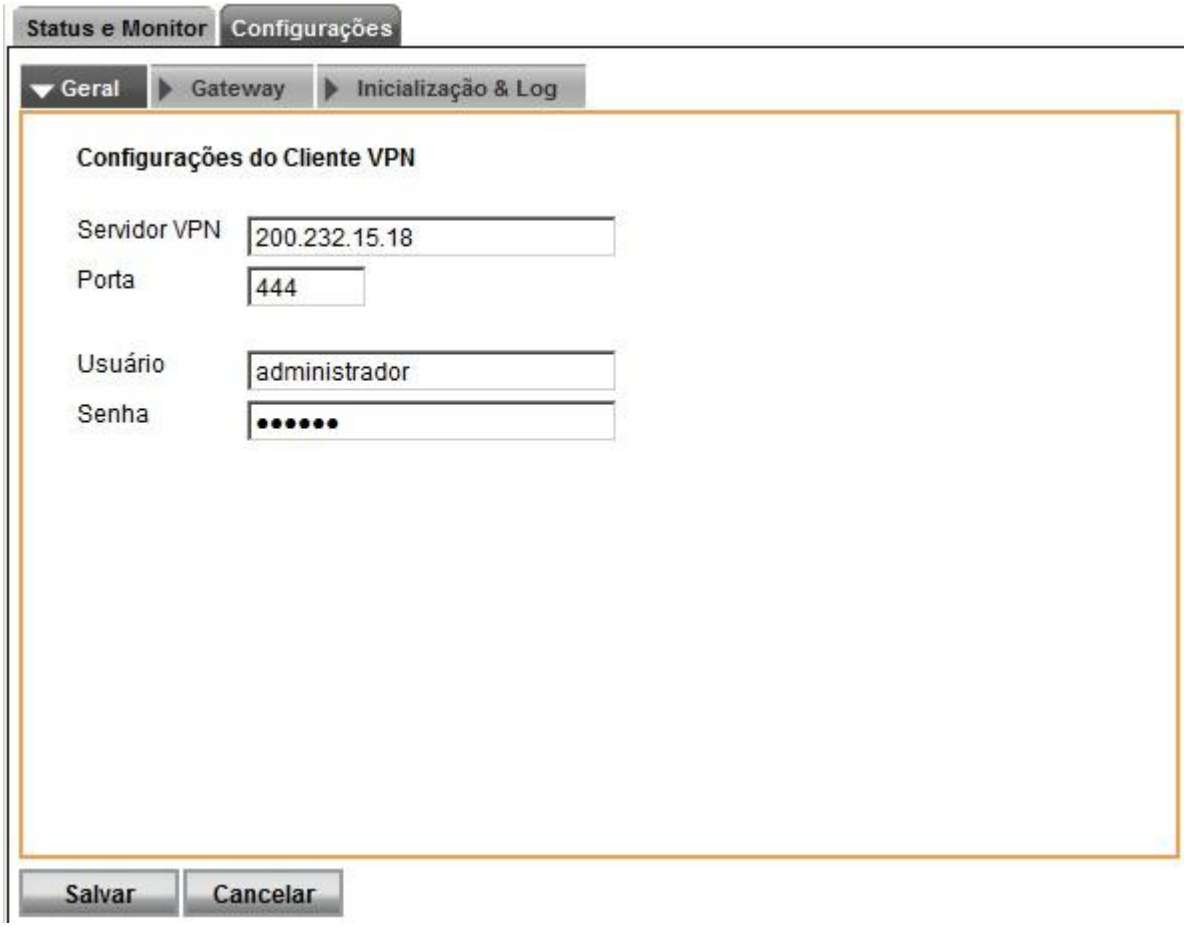
O serviço **Cliente VPN** deve ser instalado no **Winconnection 6** do computador que irá acessar o **Servidor VPN**.

Guia Configurações | Geral:

Configurações do Cliente VPN:

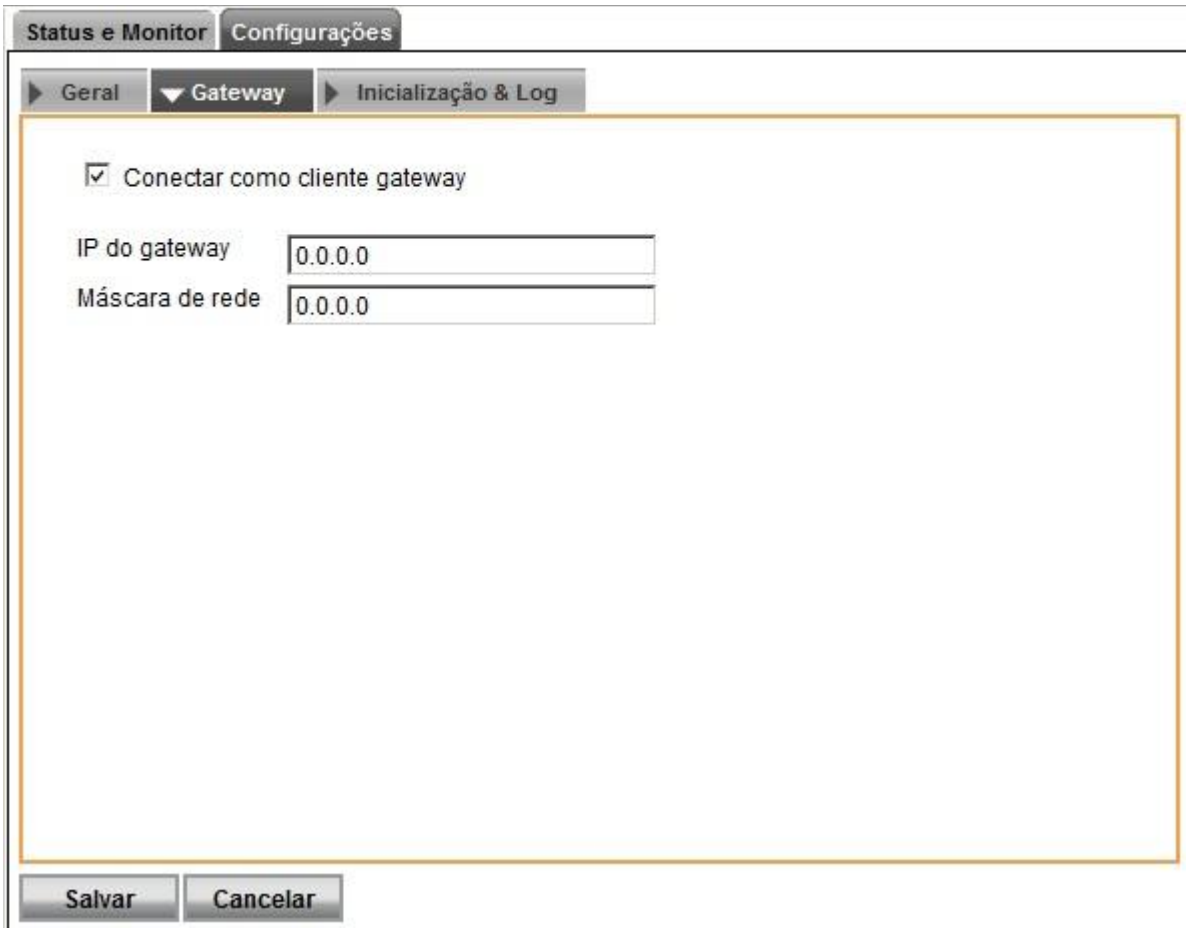
- **Servidor de VPN:** Neste campo é necessário digitar o hostname ou o endereço IP do servidor de VPN.
- **Porta:** Neste campo, é necessário definir a porta de acesso do Servidor VPN (normalmente 444).
- **Usuário:** Neste campo, o administrador da rede deve digitar o usuário que tenha acesso ao servidor de VPN.

- **Senha:** Neste campo, o administrador da rede deve digitar a senha do usuário definido no campo acima.



Guia Gateway:

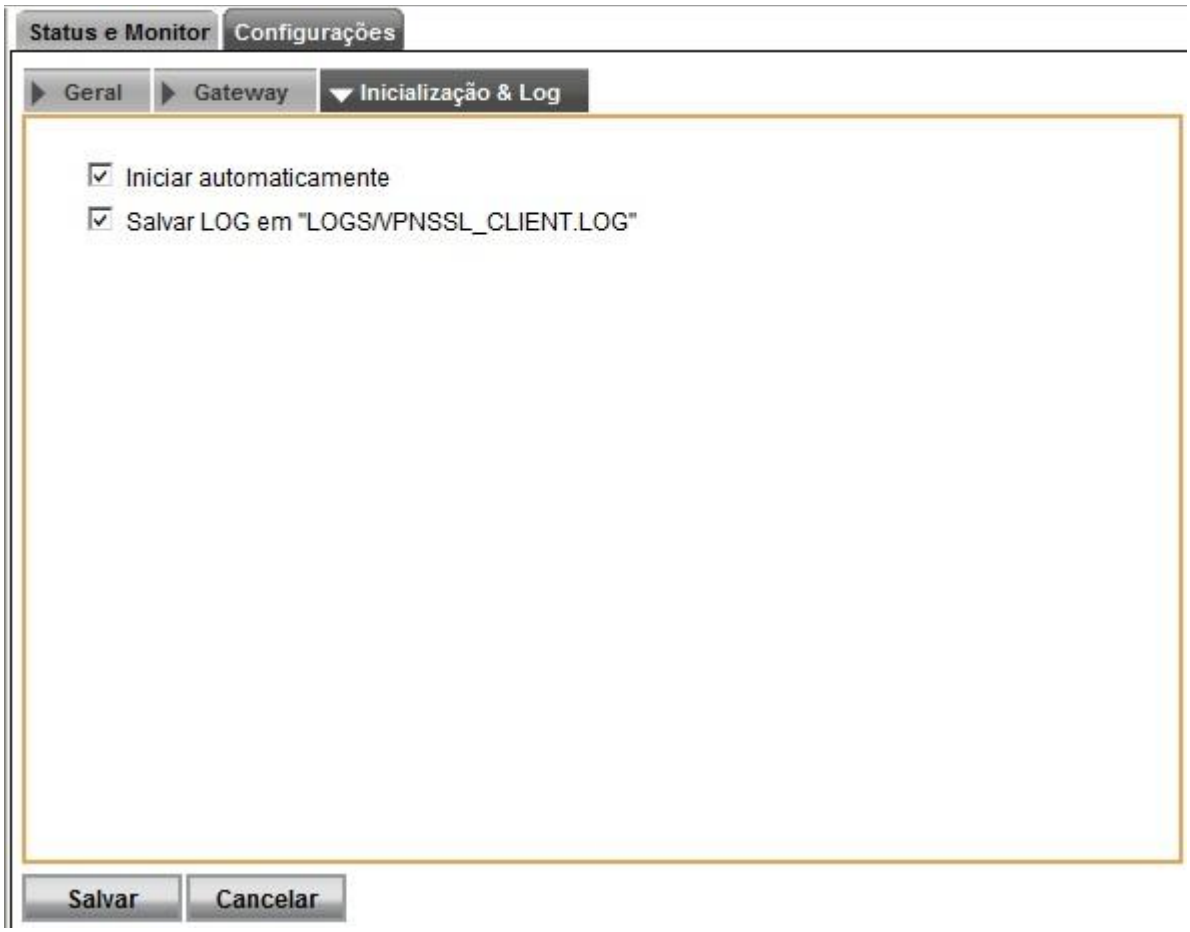
Conectar como cliente gateway: Habilite esta opção caso a conexão seja feita como gateway. O endereço IP e a mascara do Gateway deverão ser informados.



Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/VPNSSL_CLIENT.LOG":** O arquivo em bloco de notas (VPNSSL_CLIENT.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.



8.7. Winco Messenger

O **Winco Messenger** é um serviço do **Winconnection 6** para aplicação de mensagem instantânea em uma rede interna ou externa.

No **Winconnection 6** é executado o servidor do **Winco Messenger**, e nas estações é necessário instalar um cliente para que seja possível a troca de mensagens pelo sistema.

O arquivo de instalação do **Winco Messenger** está disponível na seção de download do site do **Winconnection**.

Guia Configurações | Geral:

Na seção *"Permissões de acesso por grupo"*, o administrador da rede deve habilitar os *Grupos de Usuários* que terão acesso ao serviço de mensagem.

Veja a seguir as principais características o **Winco Messenger**:

- Controle de permissão de uso.
- Transferência de arquivos.
- Busca de contatos automática, com base na lista de usuários.
- Salva a lista de contatos no servidor.
- Histórico de mensagens enviadas e recebidas.
- Pode servir tanto a rede interna como a externa (internet).
- Alerta sonoro.
- Envio de *Broadcast* (mensagem para todos).
- Aviso de usuário *Away* (com descanso de tela).
- Novo Lay-out.

Guia Configurações | Inicialização & Log:

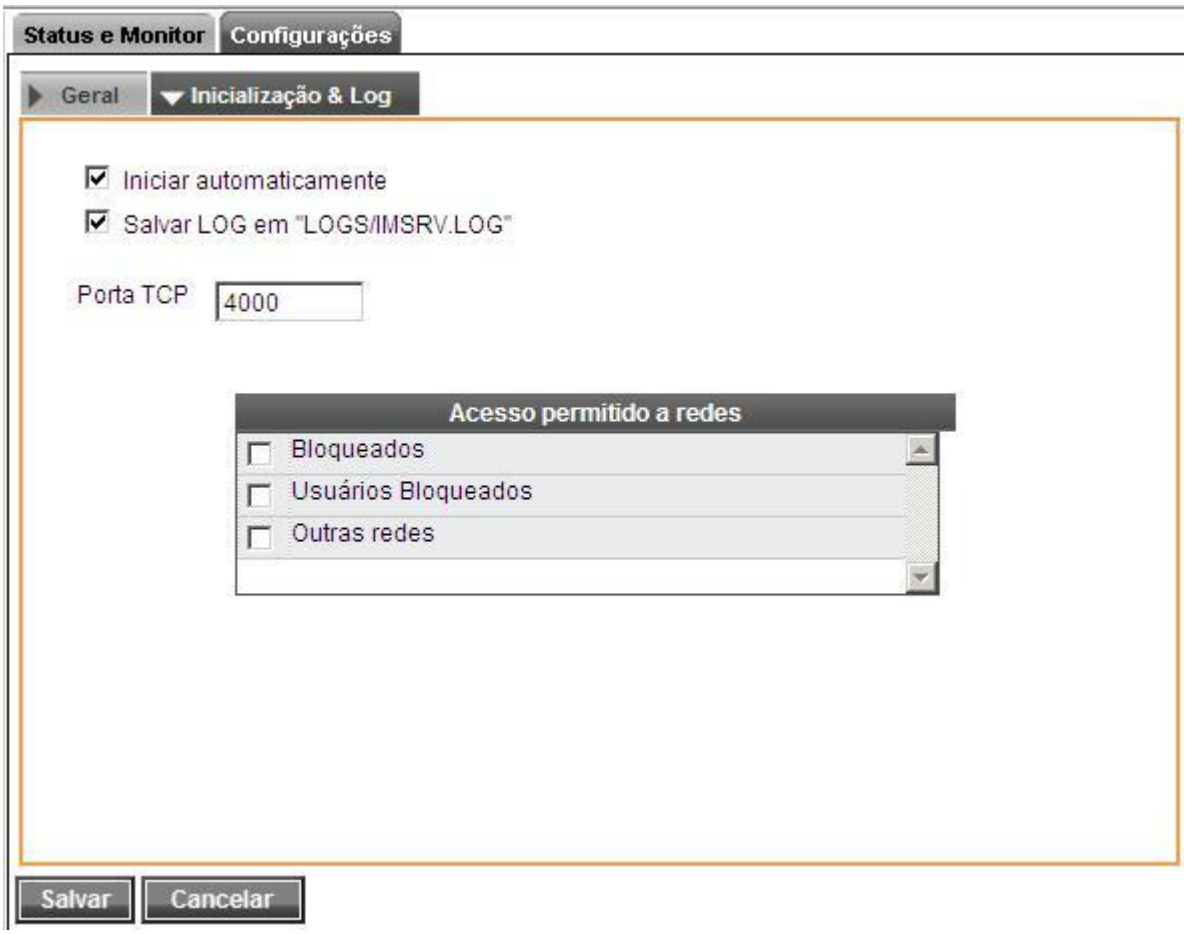
- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/IMSRV.LOG":** O arquivo em bloco de notas (IMSRV.LOG) será criado no diretório C:\Arquivos de progra-

mas\Winco\Winconnection 6\LOGS e conterá todas as informações referentes a este serviço.

- **Porta TCP:** A porta padrão para este serviço é **4000**, e não pode ser alterada, pois o cliente sempre fará o acesso nessa porta.

- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.



9. Serviços de Gateway

Veja a seguir a descrição de cada serviço disponível no menu *Serviços de Gateway*.

9.1. DNS

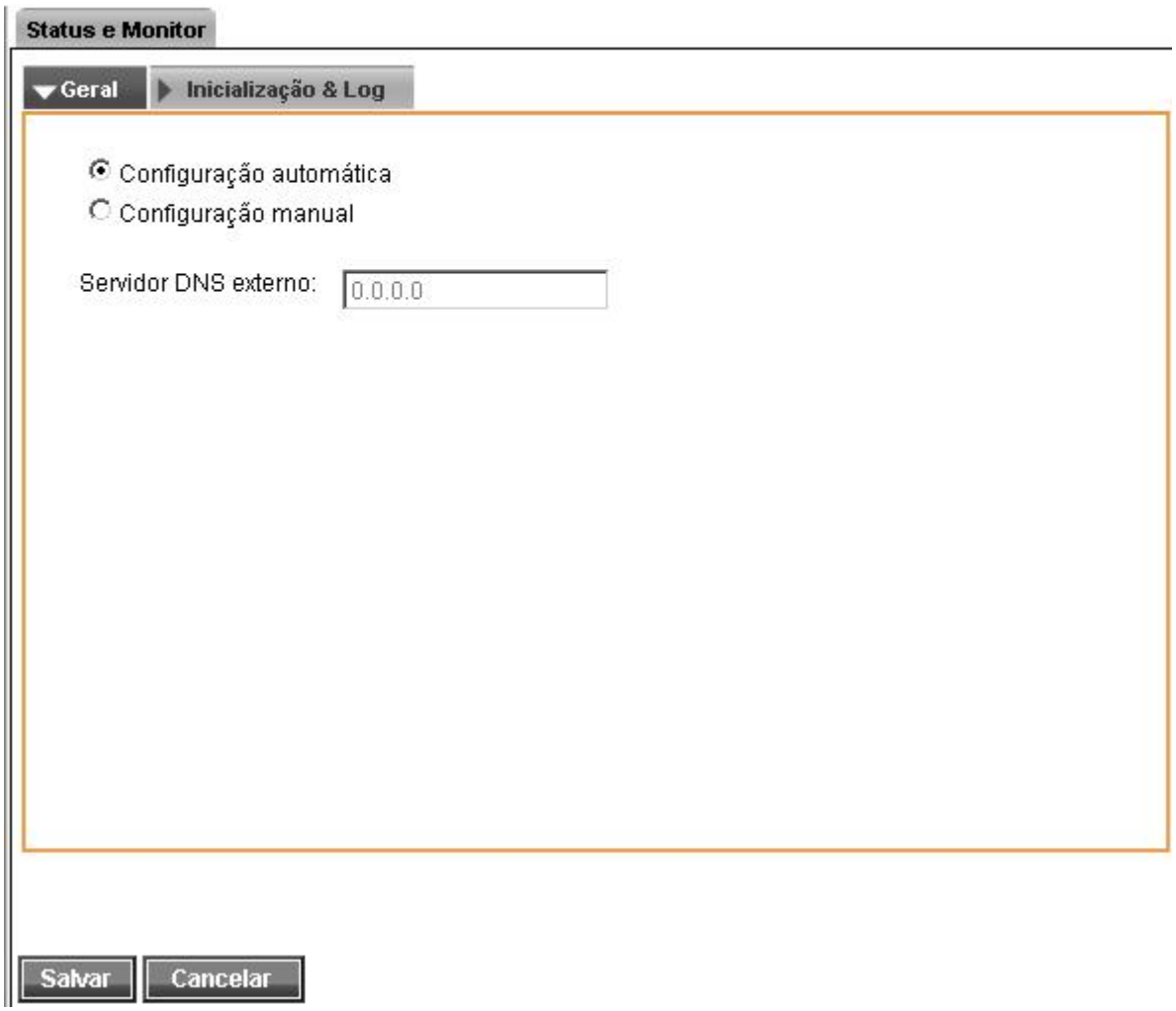
Permite que as estações resolvam o Domínio dos Servidores da Internet localmente.

Guia Configurações | Geral:

- **Configuração Automática:** Habilita o **Winconnection 6** a usar a mesma configuração de *DNS Externo* da placa de rede do servidor, permitindo assim a navegação. Esta é a opção indicada e deve ser usada sempre que possível.

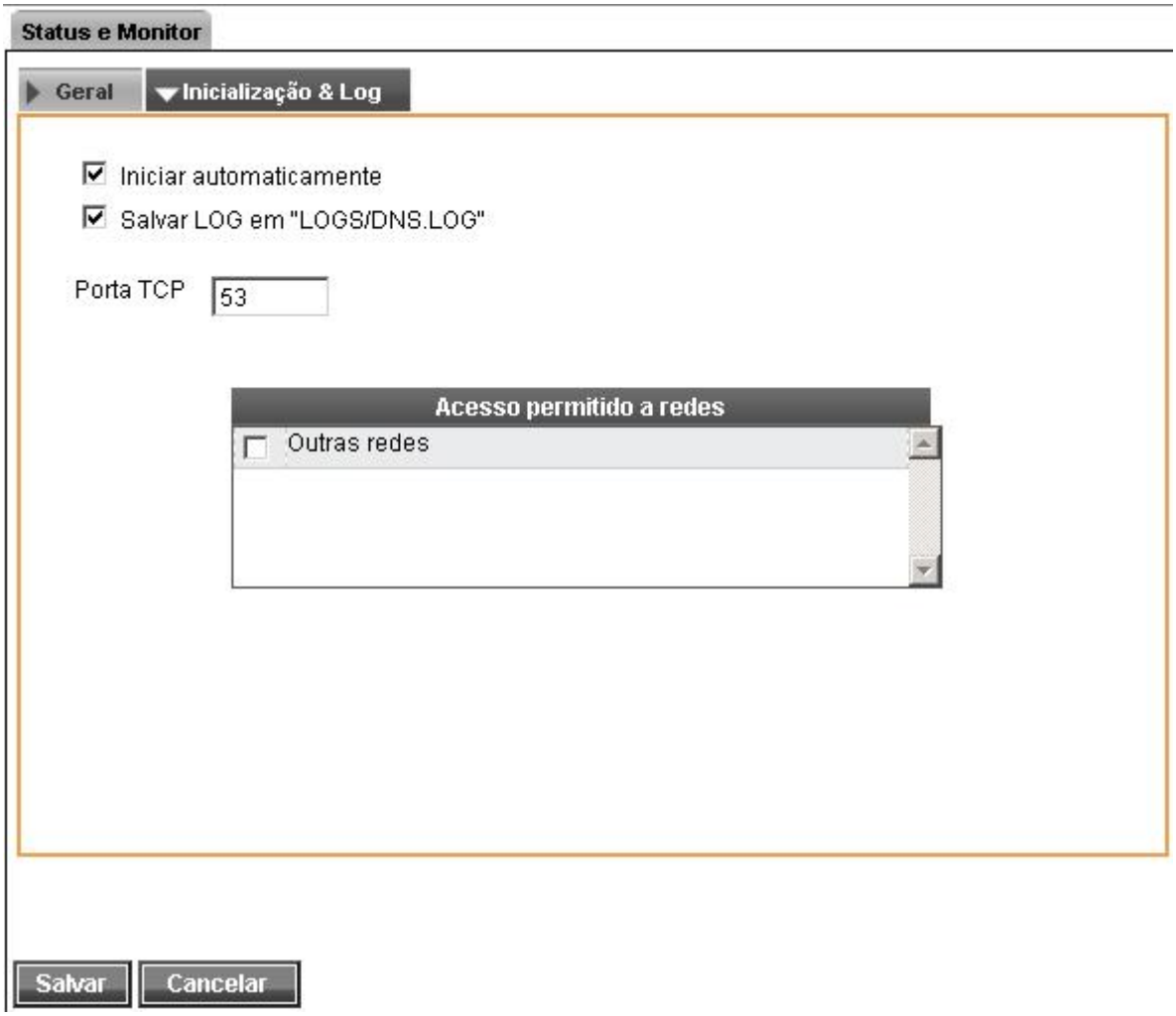
- **Configuração Manual:** O administrador da rede pode escolher qual *Servidor DNS Externo* usar. No caso do *Servidor DNS automático* não estiver resolvendo domínios, é possível utilizar o *DNS* alternativo neste campo.

- **Servidor DNS Externo:** É o serviço que resolve os domínios para esta conexão. Entre em contato com o seu provedor para descobrir qual o *IP do Servidor DNS* que eles oferecem.



Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.
- **Salvar LOG em "LOGS/DNS.LOG":** *O arquivo em bloco de notas (DNS.LOG)* será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.
- **Porta TCP:** Normalmente a porta padrão é **53** e não deve ser alterada.
- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Sempre que ativada uma rede externa, o acesso no firewall é liberado automaticamente.



9.2. DHCP

O *Dynamic Host Configuration Protocol* (Protocolo de configuração dinâmica de servidor) define uma forma para atribuir automaticamente endereços IP para computadores na rede. Os endereços IP são gerenciados por um Servidor DHCP. Se um computador Windows estiver configurado para "Obter endereços IP automaticamente", ele irá obter automaticamente um endereço IP fornecido por um Servidor DHCP.

A lógica é a seguinte:

Quando um computador é configurado para "*Obter um Endereço IP automaticamente*", o Protocolo TCP/IP faz um BroadCast para a rede requisitando por algum **Servidor DHCP** na Porta 67.

- Caso seja detectado um **Servidor DHCP**, o computador informa seu endereço físico da placa de rede (conhecido como *Endereço MAC* - este endereço é único

no mundo todo), então o **Servidor DHCP** consulta em sua base de dados para verificar se alguma máquina com esse *Endereço MAC* já requisitou algum endereço IP. Se sim, o **Servidor DHCP** informa o mesmo IP que foi atribuído anteriormente para essa máquina (caso a validade não tenha expirado).

- Caso essa máquina não tenha requisitado o IP, o **Servidor DHCP** do **Winconnection 6** informa um IP para aquele MAC e armazena no seu Banco de Dados interno.

- O formato do endereço MAC é: 02-00-4C-4F-4E-50 e o arquivo que armazena essas informações no **Winconnection** é o macsinf.mac. Para refazer todos os IPS da Rede no **Servidor DHCP**, basta excluir o arquivo macsinf.mac e na próxima inicialização, todas as máquinas irão obter novos IPS.

O **Servidor DHCP** reduz os gastos com manutenção, através do fornecimento automático de IPs nas configurações de rede para as máquinas clientes.

A utilização do **Servidor DHCP** é indicada principalmente para redes internas que possui uma constante movimentação de Notebooks no acesso a rede, pois evitaria o trabalho de configurar o TCP/IP do Notebook toda vez que o mesmo conectar-se na rede.

O **DHCP** também é indicado para redes internas que tenham mais de 20 estações conectadas ao servidor **Winconnection 6**, pois a configuração torna-se rápida e prática.

Redes que possuem Sub-Redes com faixas de IP diferentes, o uso do DHCP também seria fundamental, tanto para o desempenho da rede interna como para a utilização do **Winconnection 6**.

Guia Configurações | Geral:

Interface da Rede Interna:

Neste campo, deve-se habilitar o IP/Máscara de Rede do computador onde está instalado o **Winconnection 6**.

DHCP:

- **Primeiro IP da Rede:** O **Servidor DHCP** inicia a faixa de IP da rede no número que for digitado neste campo. É possível usar, por exemplo, o 192.168.0.2 como primeiro IP da rede.

- **Máscara de Sub Rede:** Neste campo, é necessário informar a mascara de sub rede da rede.

- **Gateway default:** Neste campo, o administrador da rede pode informar o *Gateway* padrão da rede.

- **Nome do Domínio:** Neste campo, é possível digitar o nome do domínio da rede.

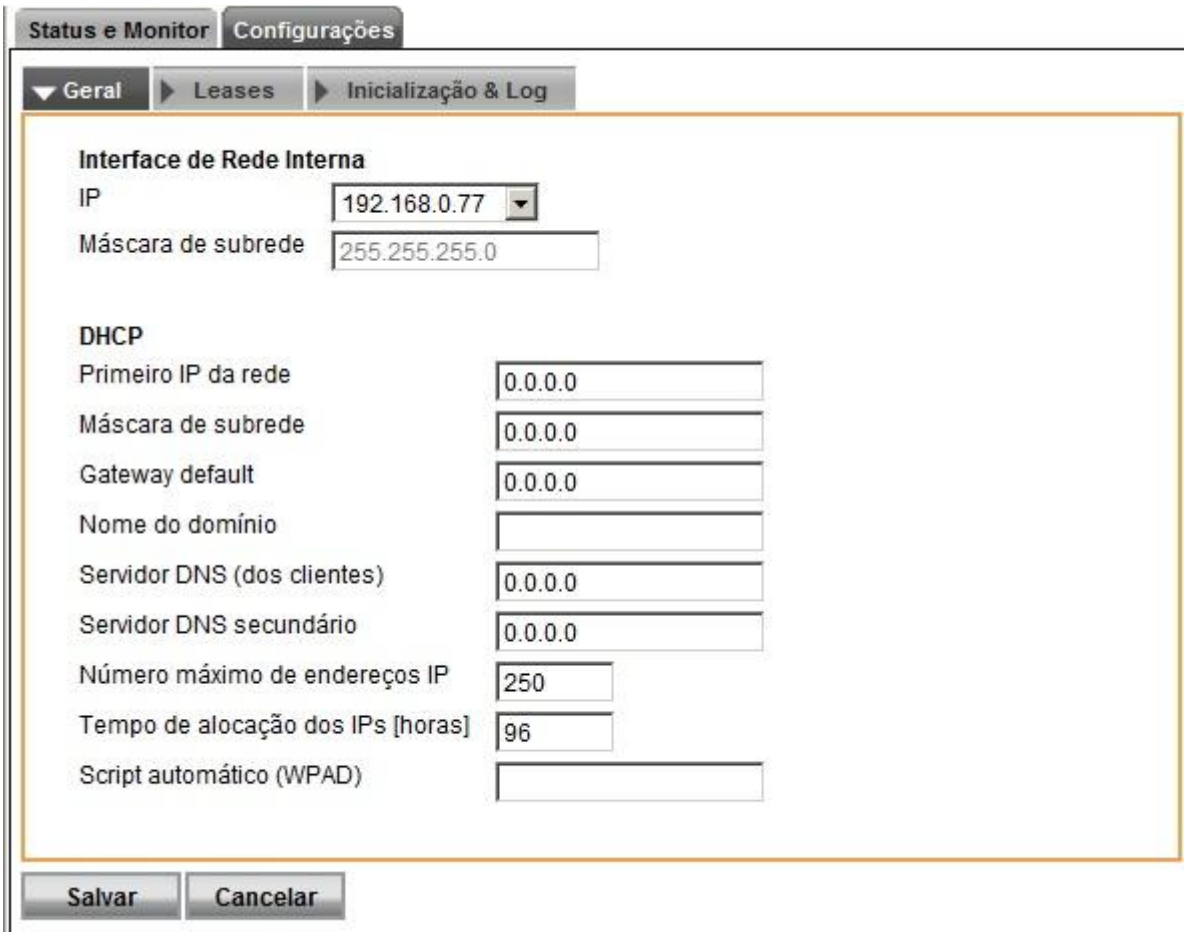
- **Servidor DNS (dos clientes):** É a máquina que será servidora DNS da rede. Caso seja o próprio **Winconnection 6**, digite o IP da máquina onde está instalado o programa neste campo. Nesse caso, o serviço DNS deve estar instalado DNS (Serviços → Novo → DNS).

- **Servidor DNS secundário:** É a máquina que será servidora DNS secundária da rede.

- **Número máximo de endereços IPs:** É a quantidade de máquinas que o **Winconnection 6** irá gerenciar. Por padrão, está configurado o valor 250.

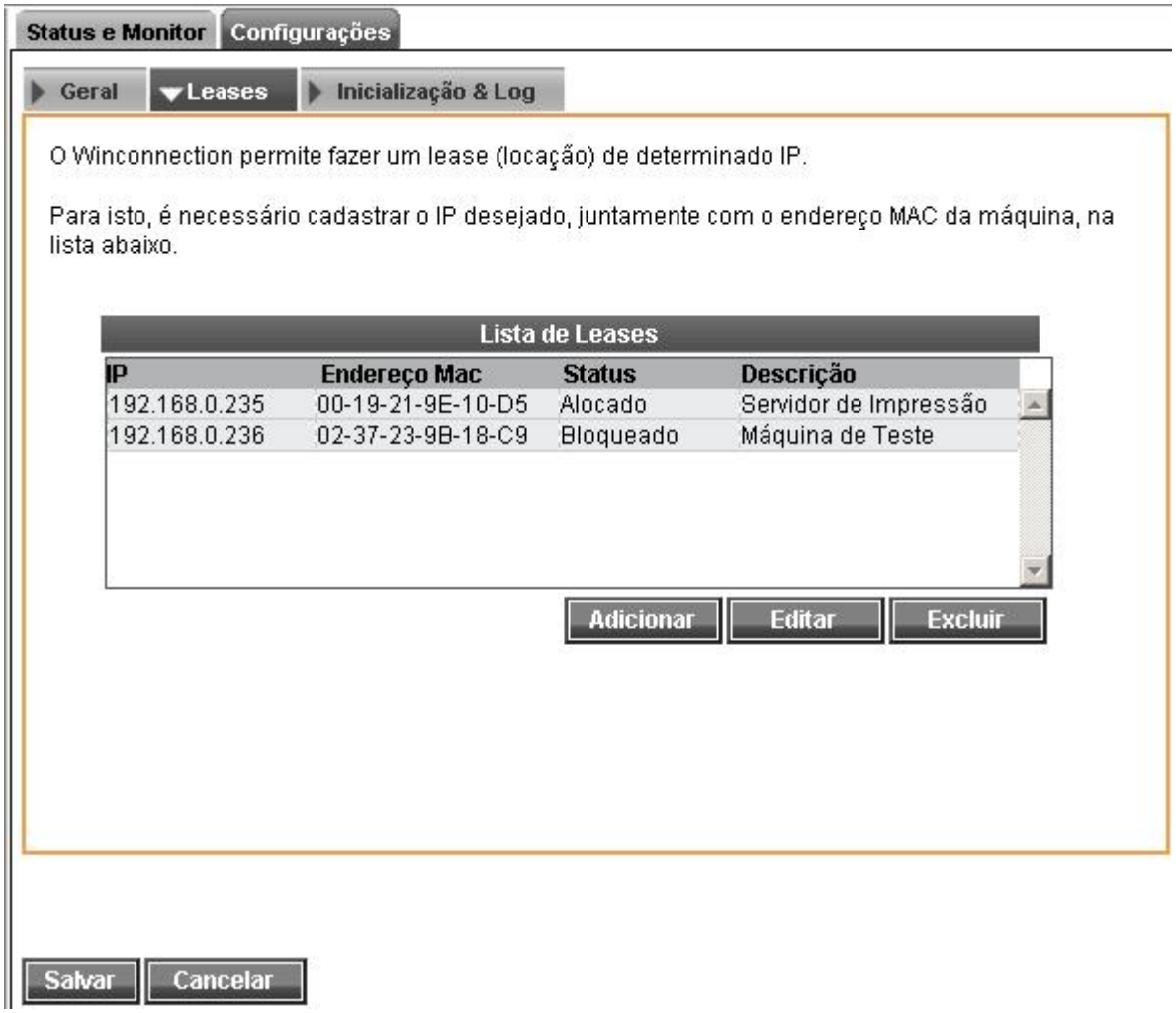
- **Tempo de alocação dos Ips [horas]:** Nesse campo, o administrador da rede define o tempo (em horas) que os endereços IPs serão alocados. Por padrão, está configurado o valor 96.

- **Script Automático (WPAD):** Neste campo, é possível adicionar um IP automático de configuração para o *DHCP*.



Guia Configurações | Leases:

Lease significa a locação de um determinado IP. Esta guia exibe a lista de *leases* que contém os IPs que foram locados no servidor.



É possível *Adicionar*. *Editar* e *Excluir* a lista de *leases* usando os respectivos botões:

DHCP Lease:

- **Status:** Neste campo, deve-se definir o status do IP.
- **Descrição:** É possível uma descrição para o *lease*.
- **Endereço Mac:** O administrador da rede, deverá informar nesse campo, o endereço IP da máquina que receberá esse IP.
- **IP:** Endereço IP que será alocado, bloqueado ou liberado.

Parâmetros Opcionais:

- **Máscara de Sub Rede:** Neste campo, é necessário informar a máscara de sub rede da rede.

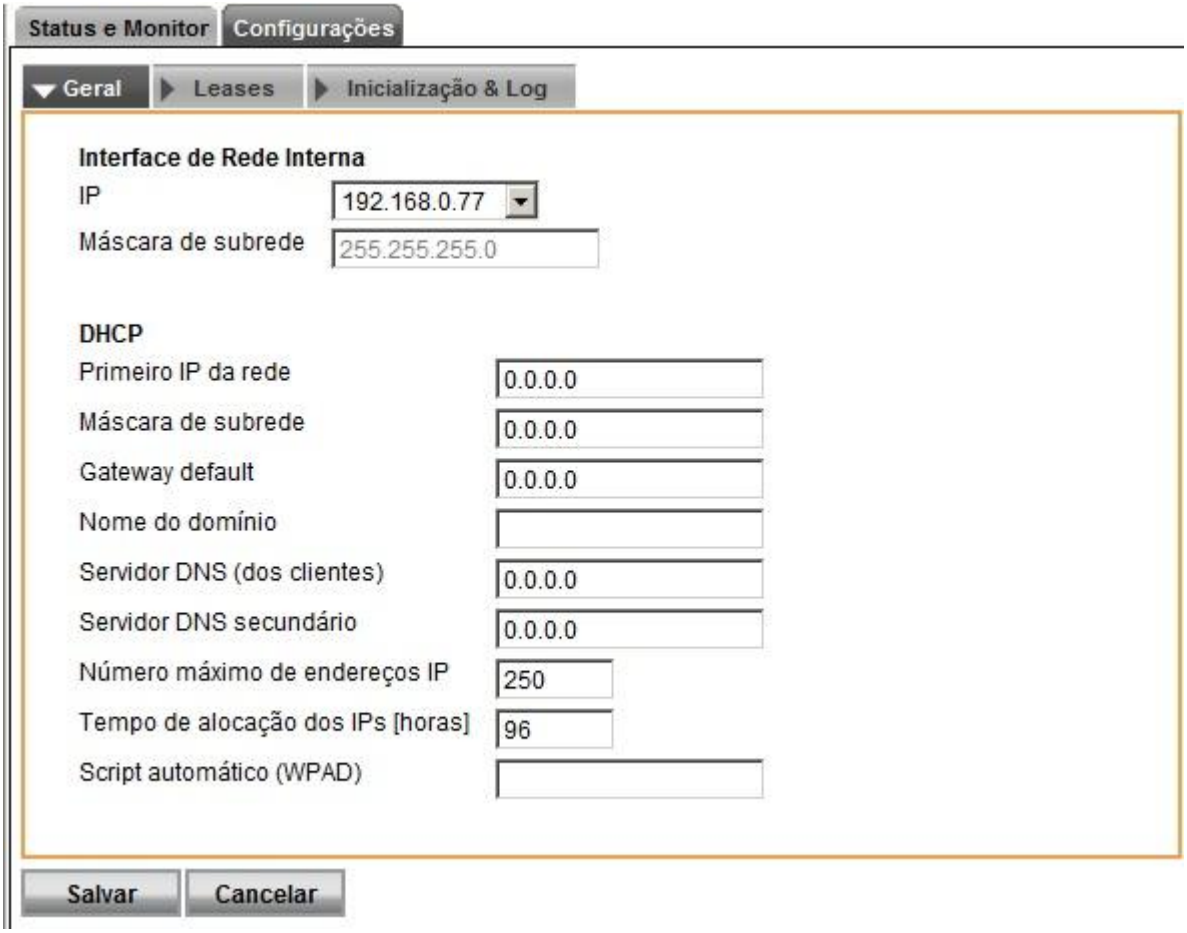
- **Gateway default:** Neste campo, o administrador da rede pode informar o *Gateway* padrão da rede.

- **DNS:** É a máquina que será servidora DNS da rede. Caso seja o próprio **Winconnection 6**, digite o IP da máquina onde está instalado o programa neste campo. Neste caso, o serviço DNS deve estar instalado DNS (Serviços → Novo → DNS). Acesse o tópico IX. DNS para mais informações.

- **DNS Secundário:** É a máquina que será servidora secundária de DNS da rede.

- **Nome do Domínio:** Neste campo, é possível digitar o nome do domínio da rede.

- **Script Automático (WPAD):** Neste campo, é possível adicionar um IP automático de configuração para o *DHCP*.



Guia Configurações | Inicialização & Log:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/DHCP.LOG":** *O arquivo em bloco de notas (DHCP.LOG)* será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.

9.4. Socks 5

O serviço **Socks 5** é um protocolo padrão de Gateway para conexões tipo Socks 5 na Internet, utilizado por alguns programas como o ICQ e alguns clientes FTP.

Com este protocolo é possível receber uma conexão vindo de fora desde que haja um programa na rede interna esperando a conexão. Outra utilização do serviço **Socks 5** é quando uma troca de pacotes UDP é necessária.

Guia Configurações | Geral:

Gateway:

Interceptar acessos de FTP (porta 21) para que transferências ativas funcionem: É necessário ativar esta opção para que todos os acessos a Servidores FTP possam ter um acesso transparente, ou seja, configura-se o cliente FTP como se estivesse conectado diretamente à internet.

Interceptar acesso de POP (porta 110) para aplicar anti-vírus: É necessário ativar esta opção para que as regras criadas no Filtro de E-mail (guia Anti-Virus) sejam aplicadas corretamente.

Controle de Acesso:

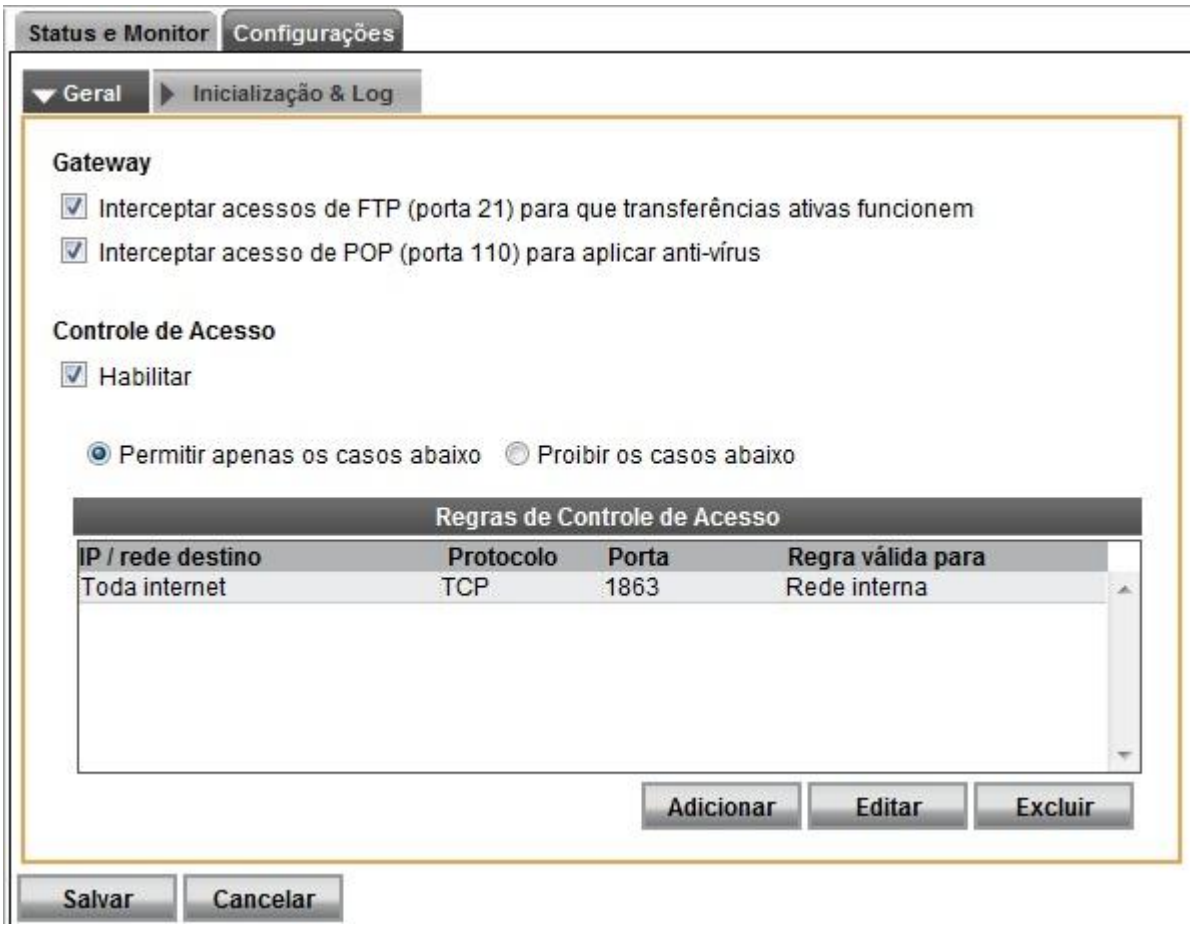
O Controle de Acesso possibilita ao administrador da rede permitir ou proibir as estações da rede acessar ou não a um determinado programa.

Permitir apenas os casos abaixo: Quando o administrador cria a regra, pode permitir o acesso ao serviço somente para os casos digitados no campo logo abaixo.

Esta opção pode ser utilizada quando o administrador não quer que os usuários fiquem conectados diretamente à internet, via Proxy Transparente e/ou Socks 5. Porém, existe aplicativo específico na estação que exige um dos serviços acima para funcionar corretamente. Neste caso, ele permite um usuário, uma faixa de usuários ou uma faixa de portas para acesso externo do aplicativo que deseja usar.

Proibir os casos abaixo: Quando o administrador cria a regra, pode criar uma lista negra de acessos ao serviço, com base em computadores ou serviços. É a regra mais usada.

Esta opção pode ser usada quando o administrador não quer permitir que determinados usuários ou uma faixa de usuários ou até uma porta acesse a rede externa. Um exemplo de utilização é o bloqueio ao MSN, ICQ, Kazaa, etc.



9.3. Filtro Web

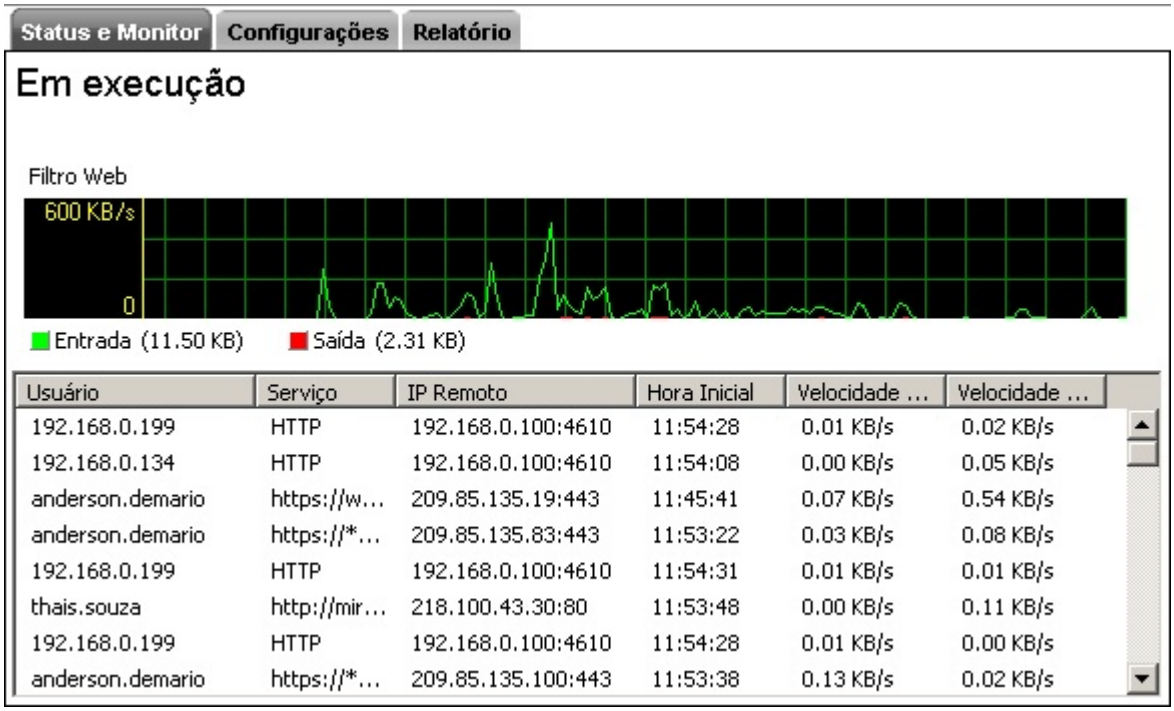
O serviço **Filtro Web** é utilizado pelos programas de navegação (Netscape, Internet Explorer, Opera, etc.) para navegar na internet. O **Winconnection 6** implementa os protocolos *HTTP*, *FTP* e *HTTPS* (seguro) para permitir o acesso a qualquer site externo, inclusive os sites seguros (compra, bancos, etc.).

Guia Status e Monitor:

Esta guia exibe informações sobre a navegação dos usuários. As seguintes informações são exibidas: *Usuário, Serviço, IP Remoto, Hora Inicial, Velocidade de Upload, Velocidade de Download, ID, Endereço Local, Protocolo, Bytes Recebidos e Bytes Enviados*.

Clicando com o botão direito do mouse sobre uma conexão, o **Winconnection 6** disponibiliza as seguintes opções:

- **Ação:** Fecha a conexão selecionada.
- **Agrupar por:** Agrupa as conexões por Usuário, por Endereço Local ou por IP Remoto.
- **Colunas:** Mostra as opções de colunas que poderão ser exibidas.



9.3.1. Guia Configurações | Geral:

Acesso à navegação:

- **Exigir autenticação**: Obriga aos usuários a digitarem o login e senha antes de começarem a navegar, permitindo que o administrador da rede saiba qual usuário está navegando e em qual site.

- **Pedir senha sempre que o usuário abrir o browser:** Exige que a toda abertura de uma nova janela do *Browser* (*Navegador*), o usuário forneça seu login e senha. Essa opção incrementa a segurança nas estações.

- **Permitir acesso somente se o usuário estiver utilizando proxy no browser:** Se esta opção for habilitada, a navegação só será permitida se as informações do Proxy estiverem configuradas no navegador.

- **Capturar conexões transparentes:** Habilitando esta opção, todas as conexões transparentes serão capturadas.

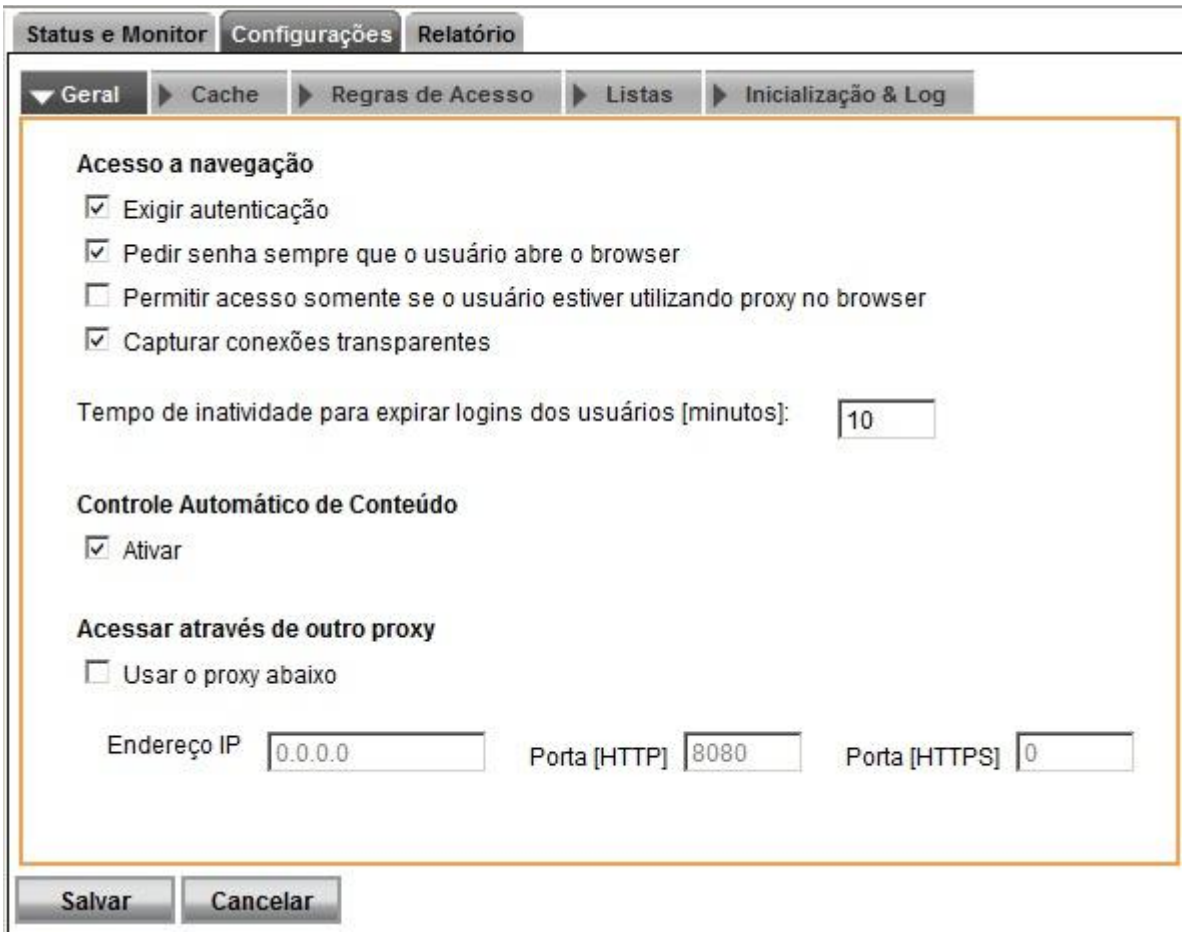
- **Tempo de inatividade para expirar logins dos usuários [minutos]:** Neste campo, é possível informar quantos minutos a estação deverá ficar sem navegar para o **Winconnection 6** pedir novamente a autenticação do usuário. Recomendamos 10 minutos.

Controle automático de conteúdo:

Ativando esta opção é possível realizar bloqueio por categorias de sites, tais como: Pornô, Vídeo, Música, etc.

Acessar através de outro proxy:

- **Usar o Proxy abaixo:** Quando existe um outro Servidor Proxy na rede, e se deseja cascatear o mesmo através do **Winconnection 6** essa opção deve ser ativada, informando o IP e as portas utilizadas no outro Servidor Proxy.

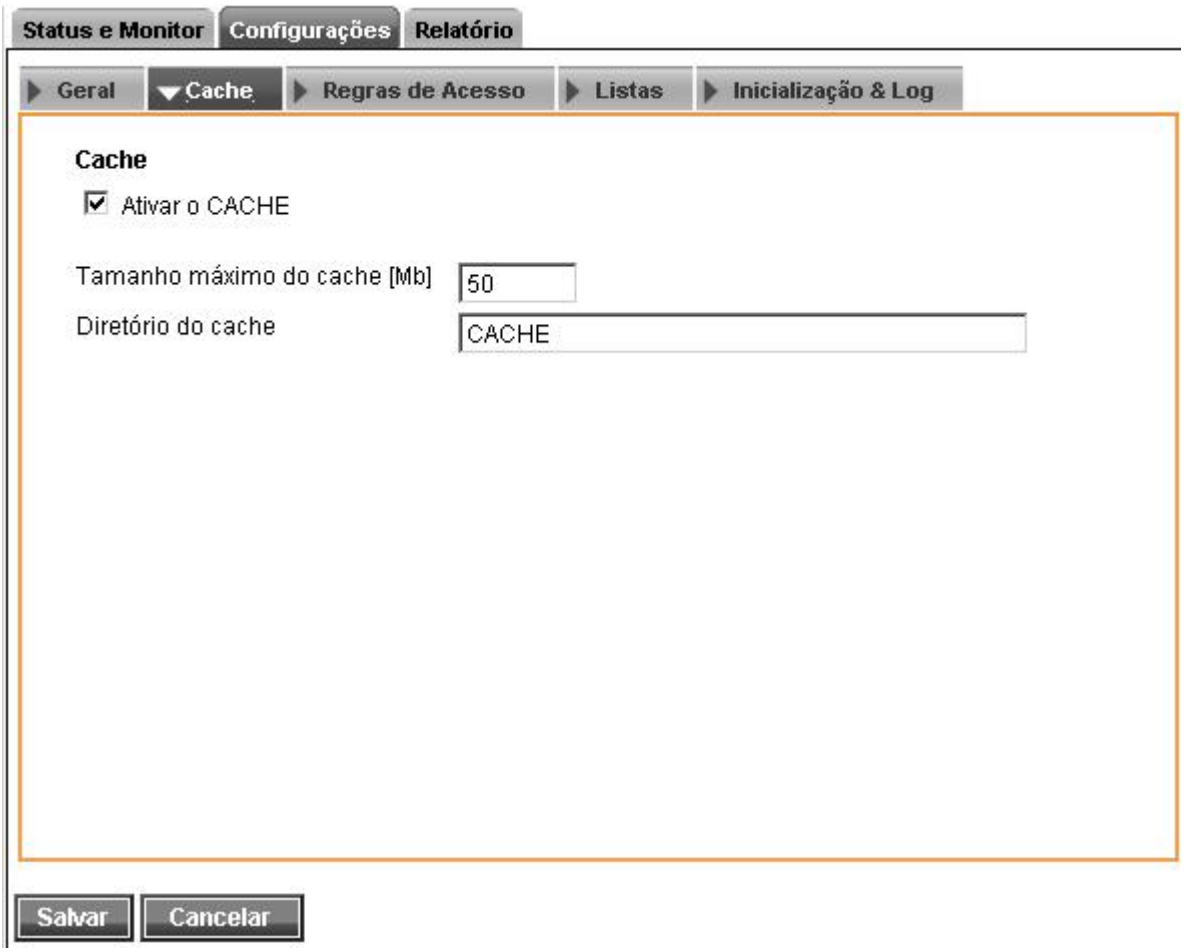


9.3.2. Guia Configurações | Cache

O **Cache** é o local no disco rígido onde se armazenam temporariamente os arquivos transferidos, quando se carrega uma página Web. Ao se retornar para a mesma página, o navegador pode buscá-la no *cache* em vez de ir até o servidor original novamente, poupando tempo e reduzindo o tráfego na Internet.

Cache:

- **Ativar cache**: Ativa a utilização do serviço de cache.
- **Tamanho máximo do cache [Mb]**: Neste campo, o administrador da rede pode definir o tamanho do cache.
- **Diretório do cache**: Neste campo é definido o diretório do cache.

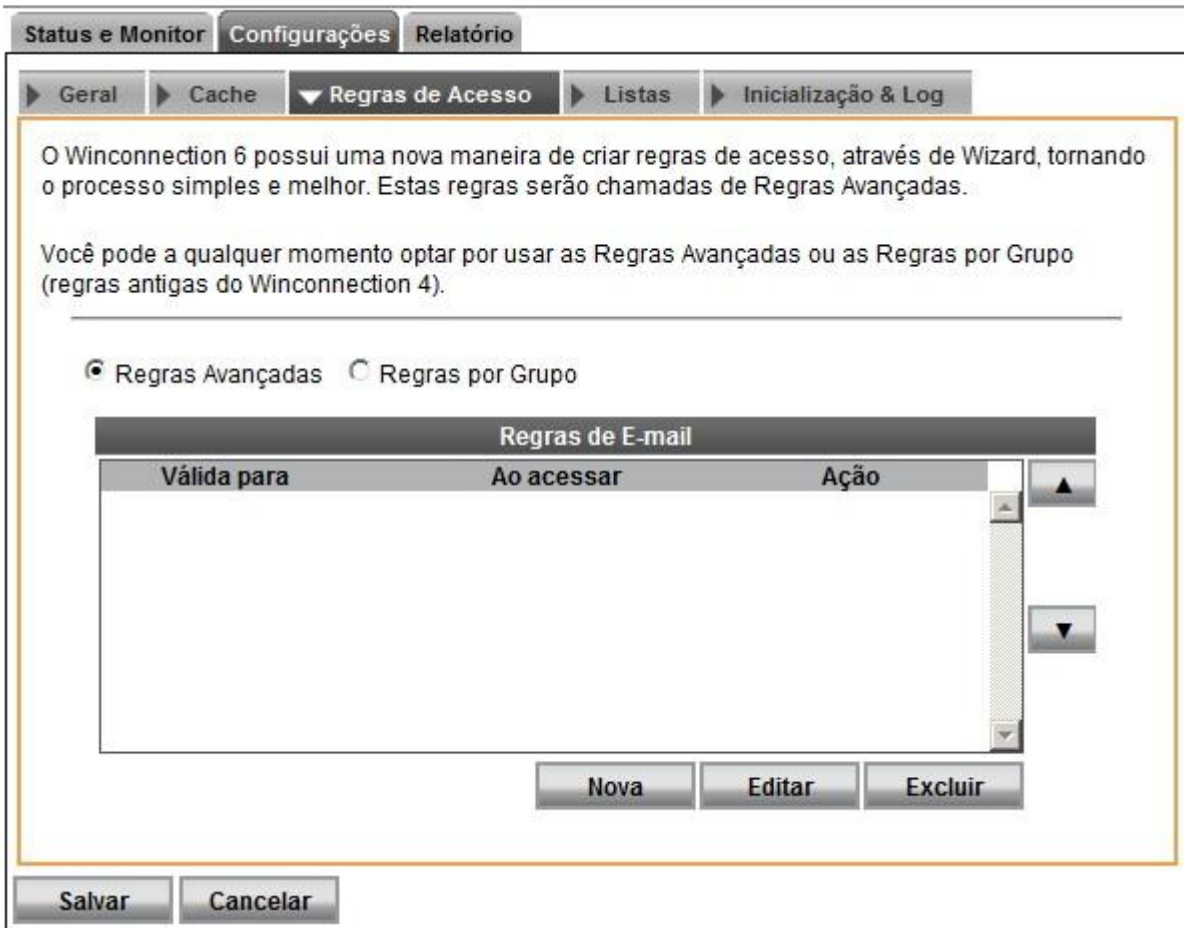


9.3.3. Guia Configurações | Regras de Acesso:

As regras de acesso para o controle de conteúdo do **Winconnection 6** são separadas por *Regras Avançadas* e *Regras por Grupo*.

- **Regras Avançadas:** As regras avançadas de acesso são criadas através de um Assistente, tornando esse processo simples e melhor.

- **Regras por Grupo:** Habilitando essa opção, é possível criar regras de acesso baseadas em grupos de usuários.



a) Regras Avançadas:

As regras avançadas são criadas através de um assistente que contêm 4 passos:

Passo 1 - Origem de Acesso:

Neste passo de configuração é necessário informar os usuários, grupos e/ou endereços IPs que serão afetados pela regra que está sendo criada/editada.

Passo 2 - Destino:

Neste passo, o administrador da rede deverá informar para quais destinos a regra de acesso que está sendo criada/editada se aplicará.

- **Todos:** Todos os sites farão parte da regra de acesso.

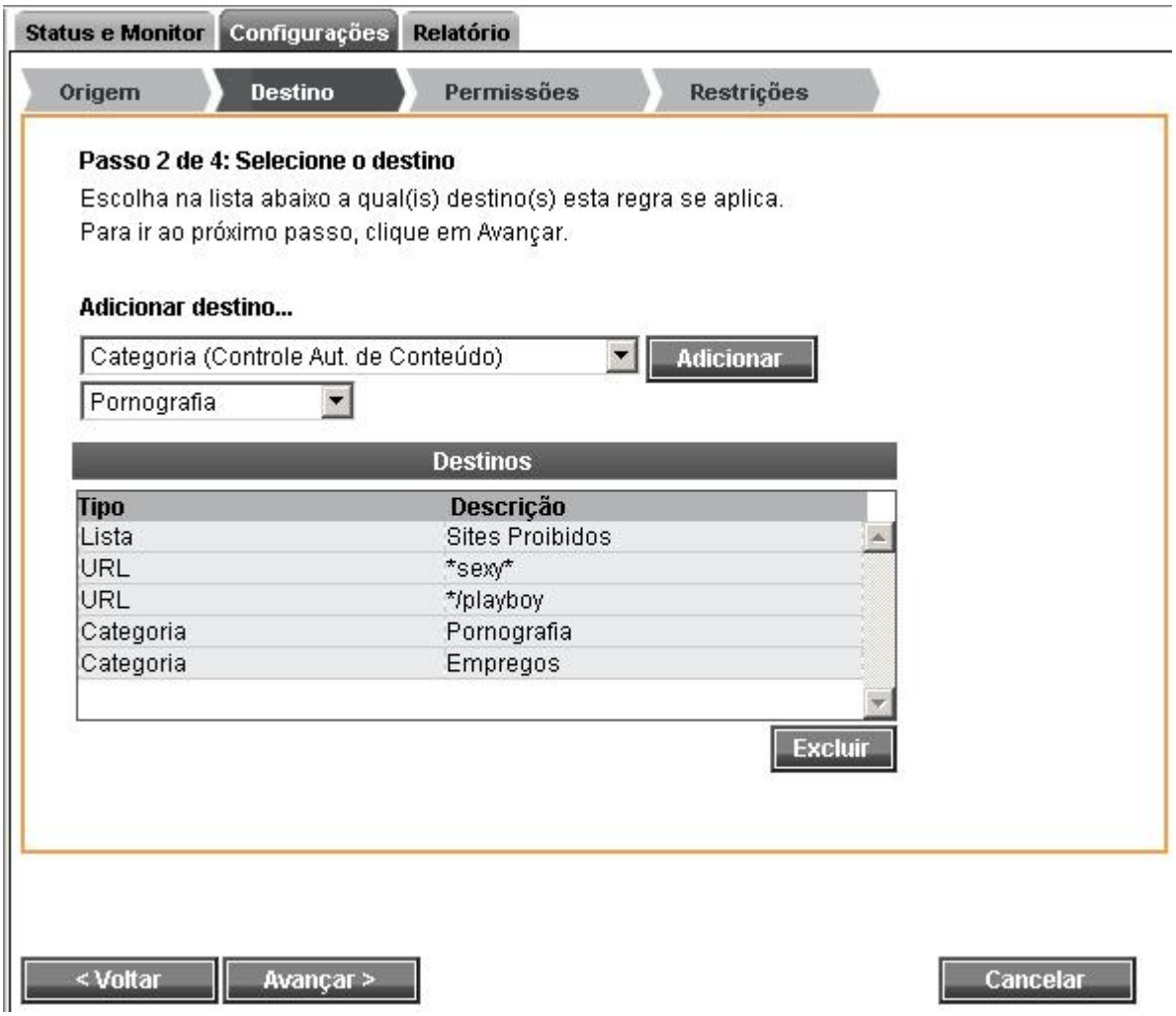
- **URL (pode ter "wildcards",* e ?):** O site deve ser informado no campo *URl* e o botão A*dicionar* deverá ser pressionado. Dicas de configurações de bloqueio por site estão disponíveis no Bloqueio por sites – Dicas de Configuração.

- **Lista de sites/URLS:** O cadastro de *Lista de Sites* permite com que o administrador da rede crie várias listas de sites, diferenciando as mesmas por tipo e depois importe estas listas para os diferentes regras de acesso, de acordo com a sua necessidade. A lista de site/URLS deve ser criada na guia

Configurações | *Lista de Sites*. Consulte o tópico Guia Configurações | Lista de Sites para mais informações.

- **Categoria (Controle Aut. Conteúdo):** Esta opção utiliza o módulo de controle automático de conteúdo para todos os sites que não estão na lista de sites proibidos/permitidos.

- **Sites acessados por IP:** bloqueia a acesso pelo Endereço IP (sites sem *hostname*).



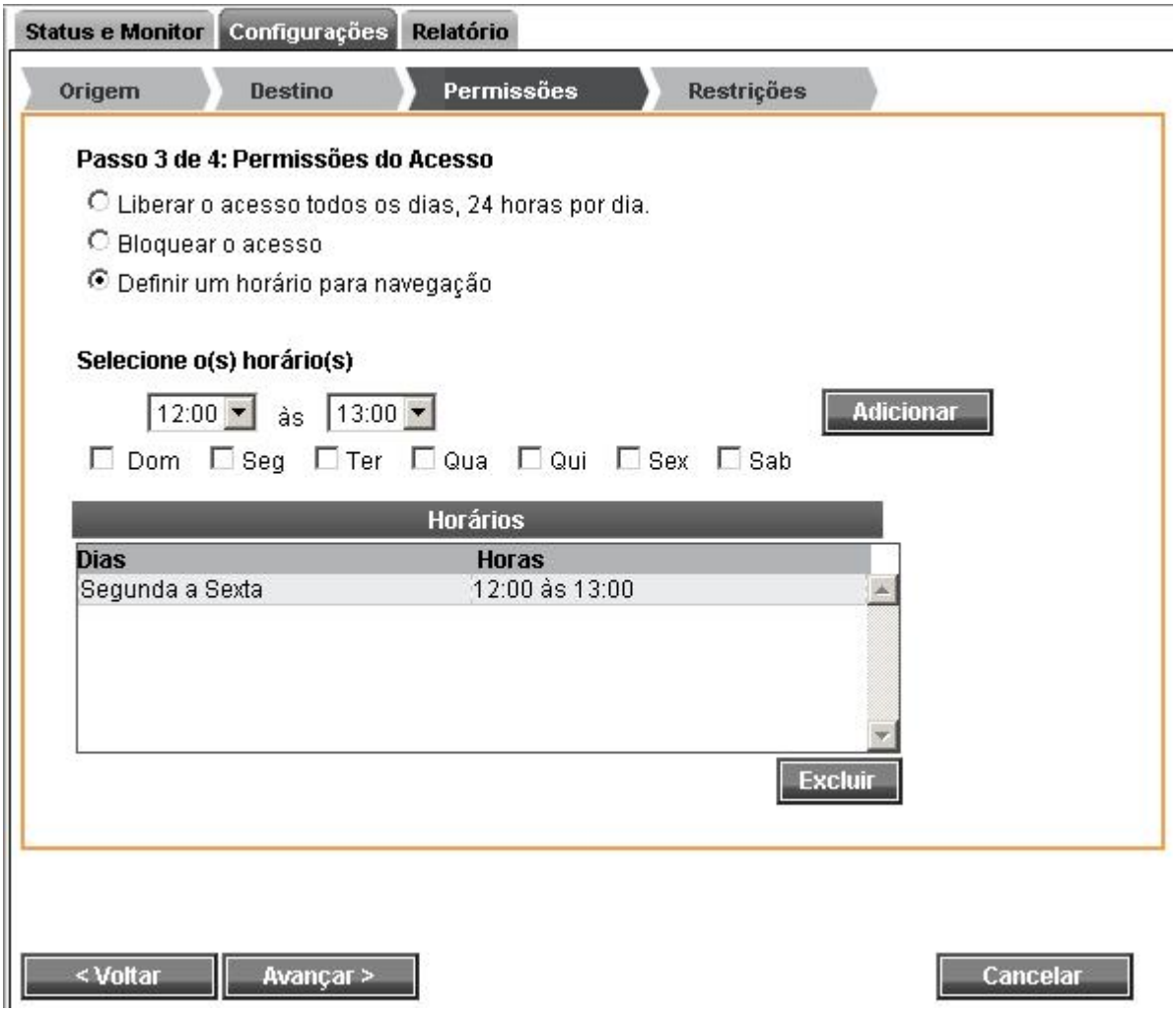
Passo 3 – Permissões:

Neste passo é possível definir o controle do acesso por horário. As seguintes opções estão disponíveis:

- **Liberar o acesso todos os dias, 24 horas por dia:** Habilitando esta opção, nenhum controle por horário é realizado.

- **Bloquear o acesso:** Habilitando esta opção, o bloqueio é feito independente do horário.

- **Definir um horário para navegação:** Neste campo, o administrador da rede deverá informar o período de tempo quando o acesso for permitido.



Passo 4 – Restrições:

Neste passo é possível definir quais restrições serão aplicadas na regra que está sendo criada.

Protocolos permitidos:

São os protocolos válidos para a regra de acesso. Habilite os protocolos que serão permitidos na regra.

Restrições:

- **Tempo de navegação [minutos]:** Neste campo, é possível restringir o tempo que o usuário ficará online. Essa configuração deve ser feita em minutos.

- **Limite de transferência diária [kb]:** O administrador da rede poderá definir neste campo um limite de transferência diária que será aplicado na regra que está sendo criada/editada.

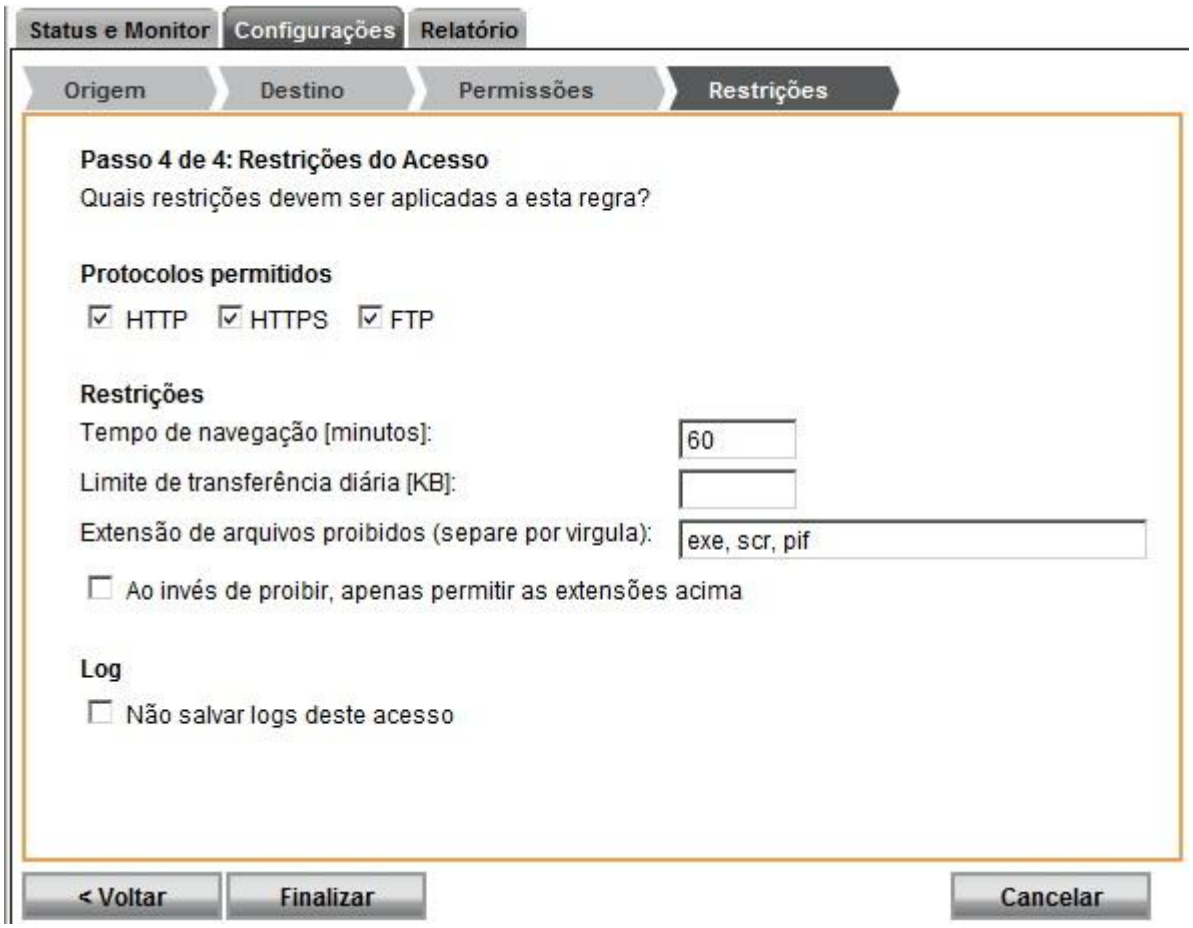
- **Extensões de arquivos proibidos (separe por vírgula):** O **Winconnection 6** permite proibir o download por extensão de arquivos nos protocolos HTTP e FTP.

    - **Ao invés de proibir, apenas permitir as extensões acima:** Habilitando esta opção somente o download dos arquivos mencionados no campo acima será permitido.

Logs:

Se o administrador optar por não salvar os logs desta regra, basta selecionar a opção *Não salvar logs desse acesso*.

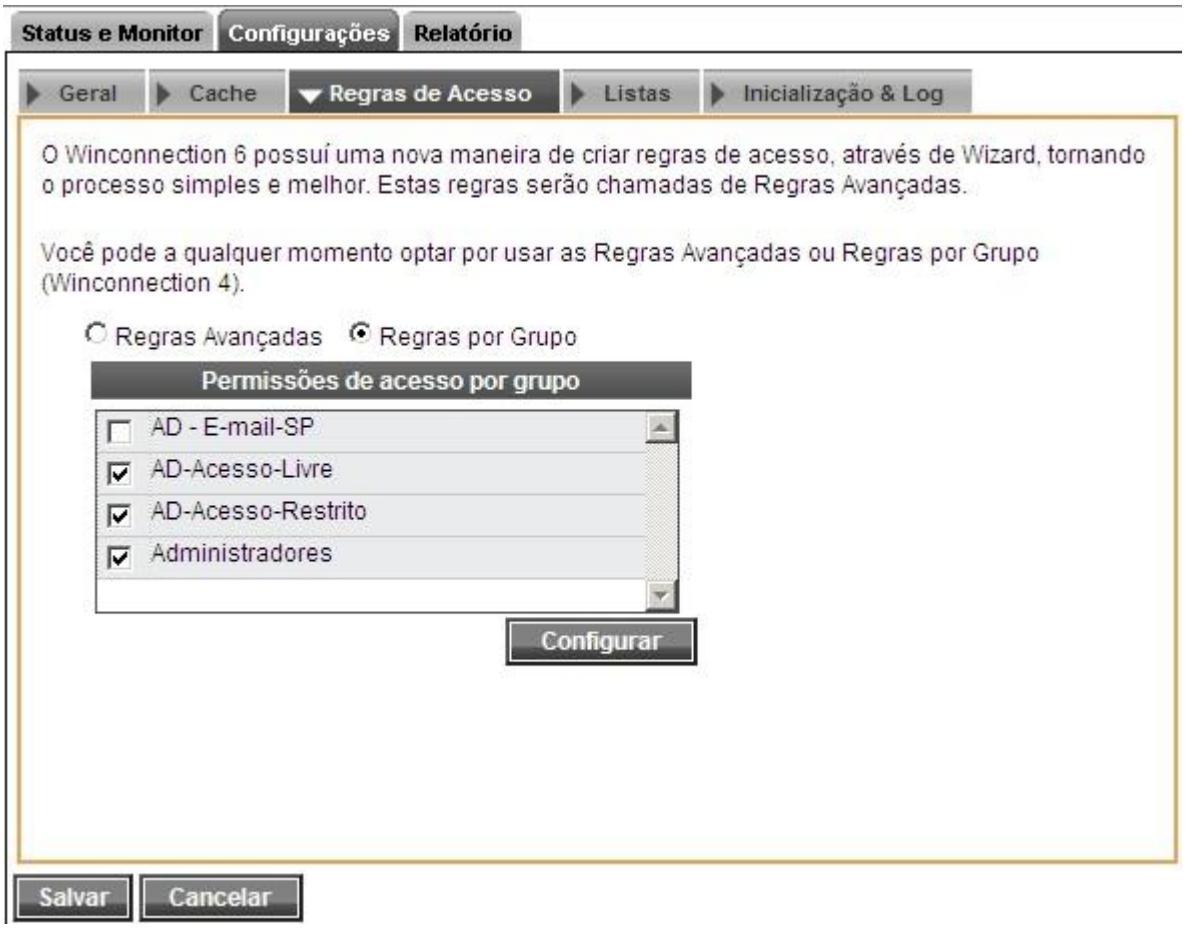
Observação: Se esta opção for habilitada, o acesso também não será mostrado nos *Relatórios de Acesso a Web*.



b) Regras por grupos

Habilitando a opção **Regras por grupos** é possível definir as regras de acesso à navegação baseadas em grupos de usuários.

Na seção *Permissões de acesso por grupo*, o administrador da rede deverá habilitar os grupos de usuários que terão acesso à navegação através do serviço **Filtro Web**.



Para configurar as regras por grupo, é necessário selecionar o grupo e em seguida clicar no botão *Configurar*.

Regras de Acesso:

- **Ativar o controle de conteúdo**: Ativa o controle de conteúdo com base nas regras que serão criadas.

- **Proibir acesso aos sites abaixo**: Proíbe acesso aos Sites ou Lista de Sites que o administrador da rede irá cadastrar no campo abaixo. O administrador deve também definir as regras adicionais, como protocolo que é válido (http, https e ftp), horário de proibição e tratamento da extensão de arquivos que podem ser baixados.

- **Permitir acesso aos sites abaixo**: Permite acesso aos Sites ou Lista de Sites que o administrador da rede irá cadastrar no campo abaixo.

Dicas de configurações de bloqueio por site estão disponíveis em Bloqueio por sites – Dicas de Configuração.

Também é possível cadastrar *Lista de Sites*, diferenciando-as por tipo e depois importar estas listas para as diferentes regras de acesso. A lista de site/URLS deve ser criada na Guia *Configurações → Lista de Sites*. Consulte o tópico IX.5.4. Guia Configurações | Lista de Sites para mais informações.

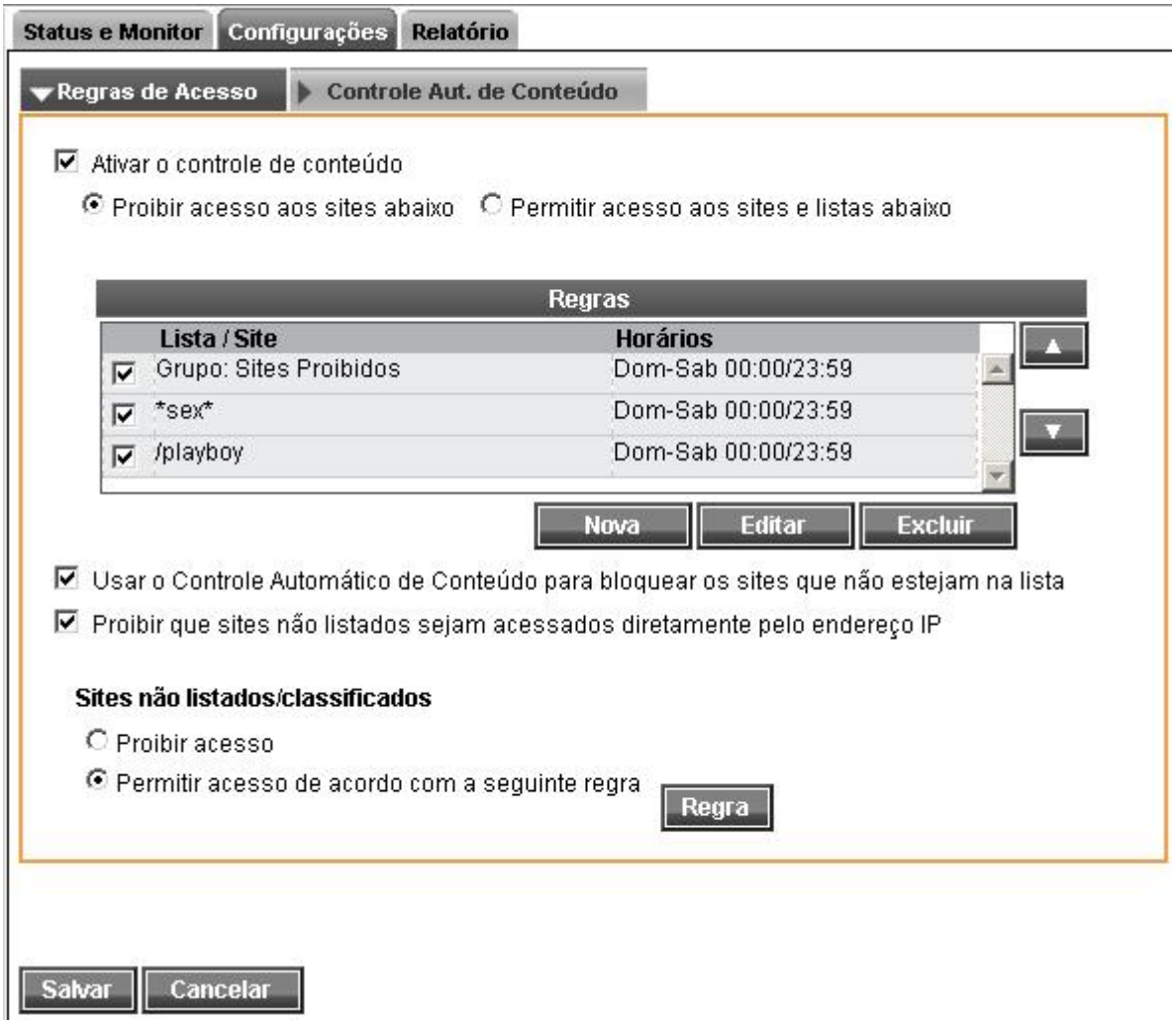
- **Usar o Controle de Conteúdo Automático para classificar os sites que não estejam na lista:** Utiliza o módulo adiciona *Filtro Automático de Conteúdo Web* para todos os sites que não estão na lista de sites proibidos/permitidos.

- **Proibir que sites não listados sejam acessados diretamente pelo endereço IP:** Bloqueia o acesso pelo Endereço IP dos sites não listados na Lista de Sites.

- **Sites não listados acima**: São as regras definidas para os sites não cadastrados no campo acima. O Administrador da rede pode utilizar as seguintes regras:

- **Proibir acesso**: Todo e qualquer site que não esteja na lista acima de permissão ou de proibição, será proibido.

- **Permitir acesso de acordo com a seguinte regra**: Todo e qualquer site não listado nas regras acima terão o tratamento geral dado por esta opção.

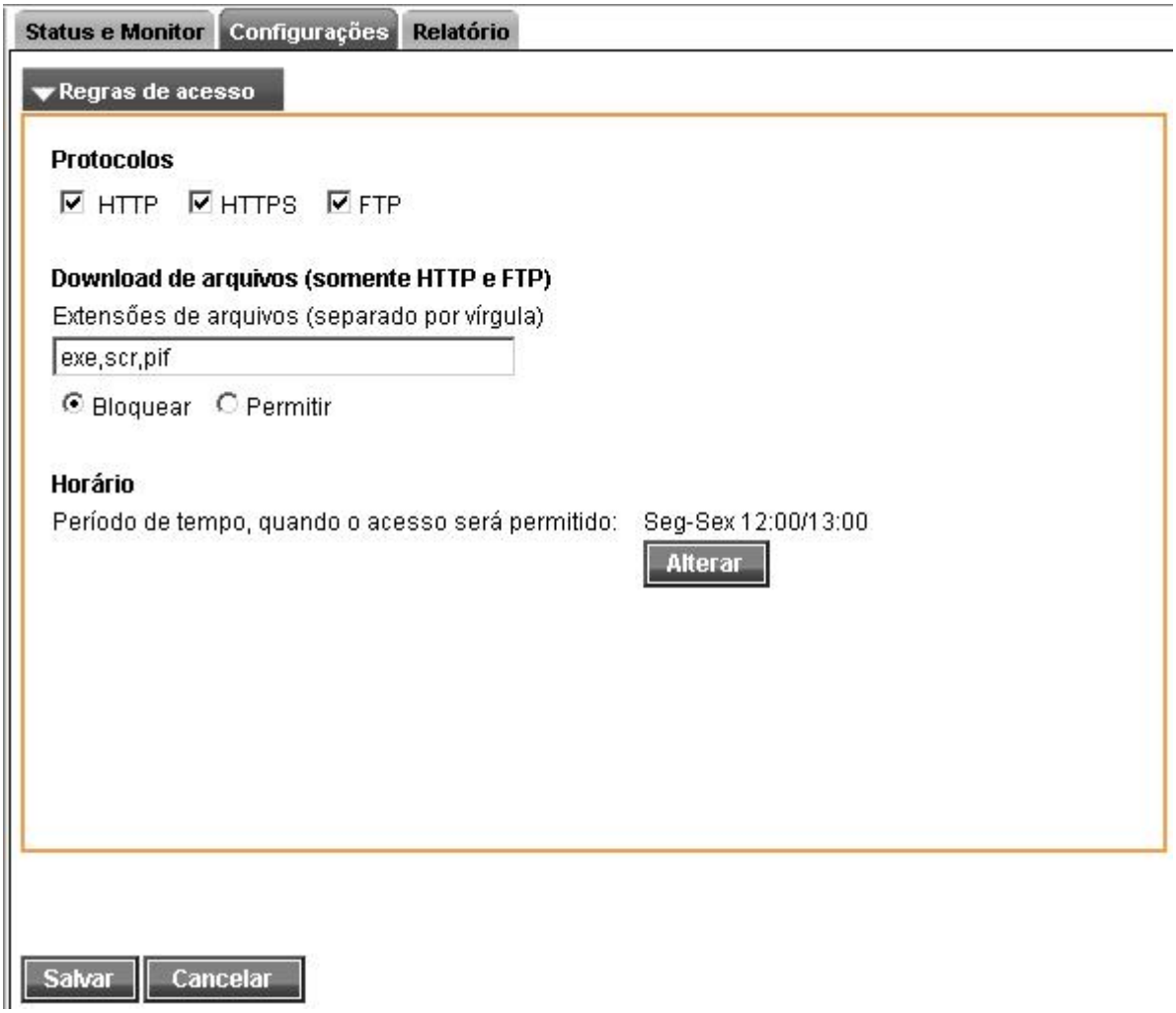


- **Regra**: O administrador deve também definir as regras adicionais, como protocolo que é válido (http, https e ftp), horário quando o acesso será permitido e proibição e tratamento da extensão de arquivos que podem ser baixados:

    - **Protocolos:** São os protocolos válidos para a regra de acesso.

    - **Downloads de arquivos:** O **Winconnection 6** possibilita proibir ou permitir o download por extensão de arquivos nos protocolos HTTP e FTP.

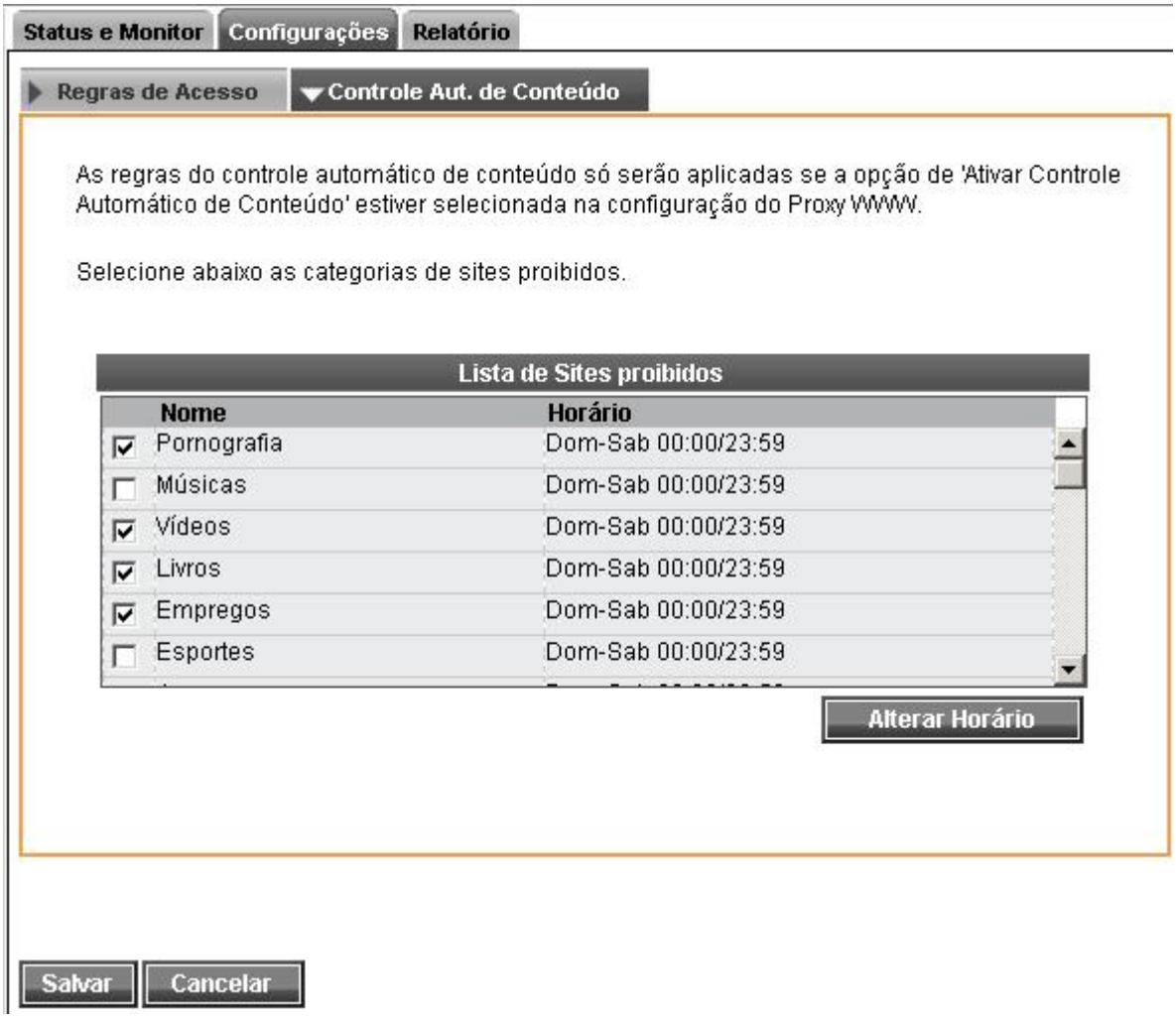
    - **Horário:** Neste campo, o administrador da rede deverá informar o período de tempo quando o acesso for permitido. Para alterar esta configuração, basta clicar no botão *Alterar*.



Controle Automático de Conteúdo:

Nessa guia de configuração, o administrador da rede deve selecionar as categorias de sites que serão bloqueados.

O bloqueio é realizado por horário. O botão *Alterar Horário* deve ser utilizado para alterar os horários de bloqueio.



9.3.4. Guia Configurações | Lista de Sites

O cadastro de **Lista de Sites** permite com que o administrador da rede crie várias listas de sites, diferenciando-as por tipo e depois importe estas listas para os diferentes tipos de regras de acesso que poderão ser criadas, de acordo com a sua necessidade. Para isso, clique no botão *"Nova"* → *"Uma única URL"* e adicione os sites que serão proibidos.

Na existência de outra fonte de sites de uso proibido na empresa, o administrador da rede pode importar uma lista completa de sites de um arquivo texto colocando um site por linha. Por exemplo:

Arquivo "Sites_Proibidos.txt":

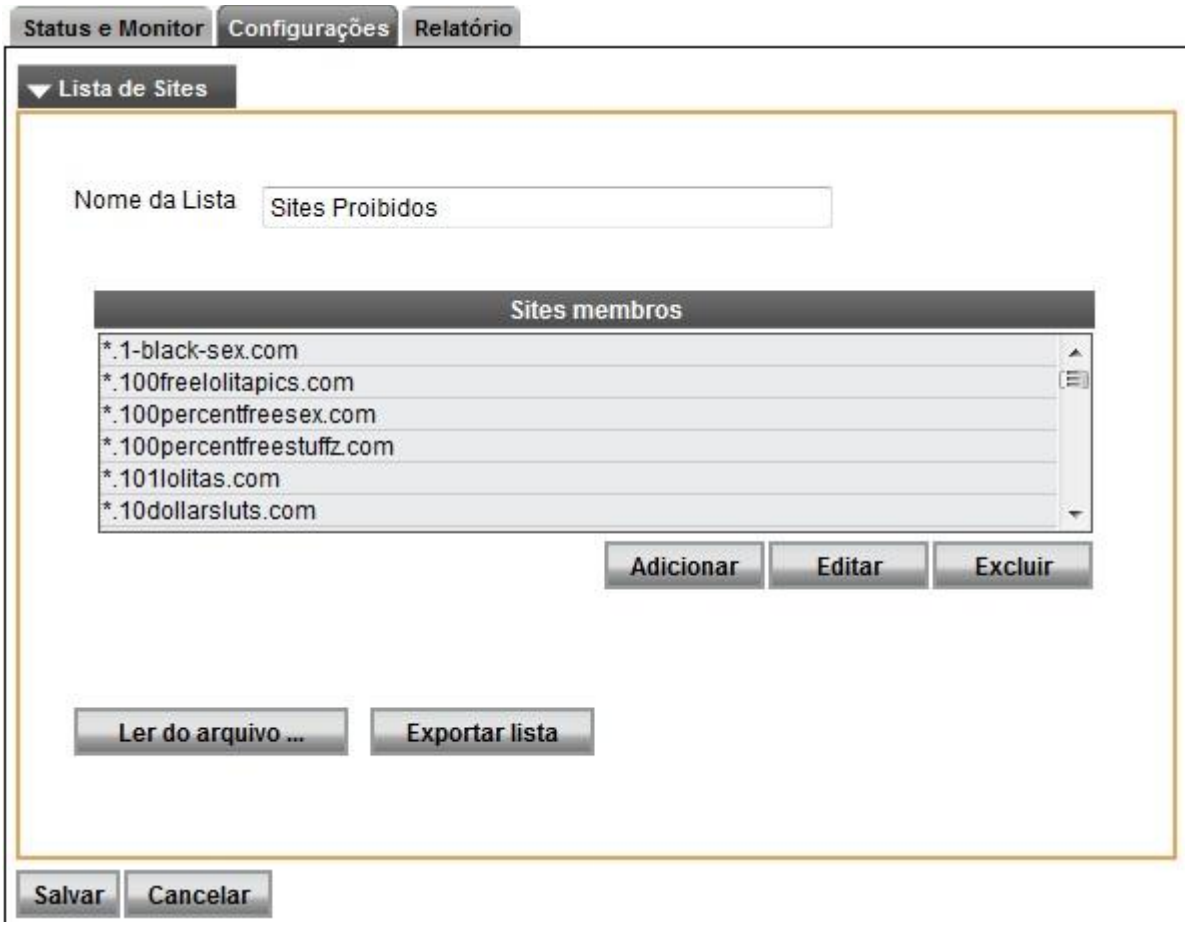
www.uol.com.br

terra

*/playboy

sex

Para importar o arquivo, selecione a opção "*URLs de um arquivo*", clique no botão "*Procurar",* indique o arquivo .txt e clique no botão "*Salvar*".



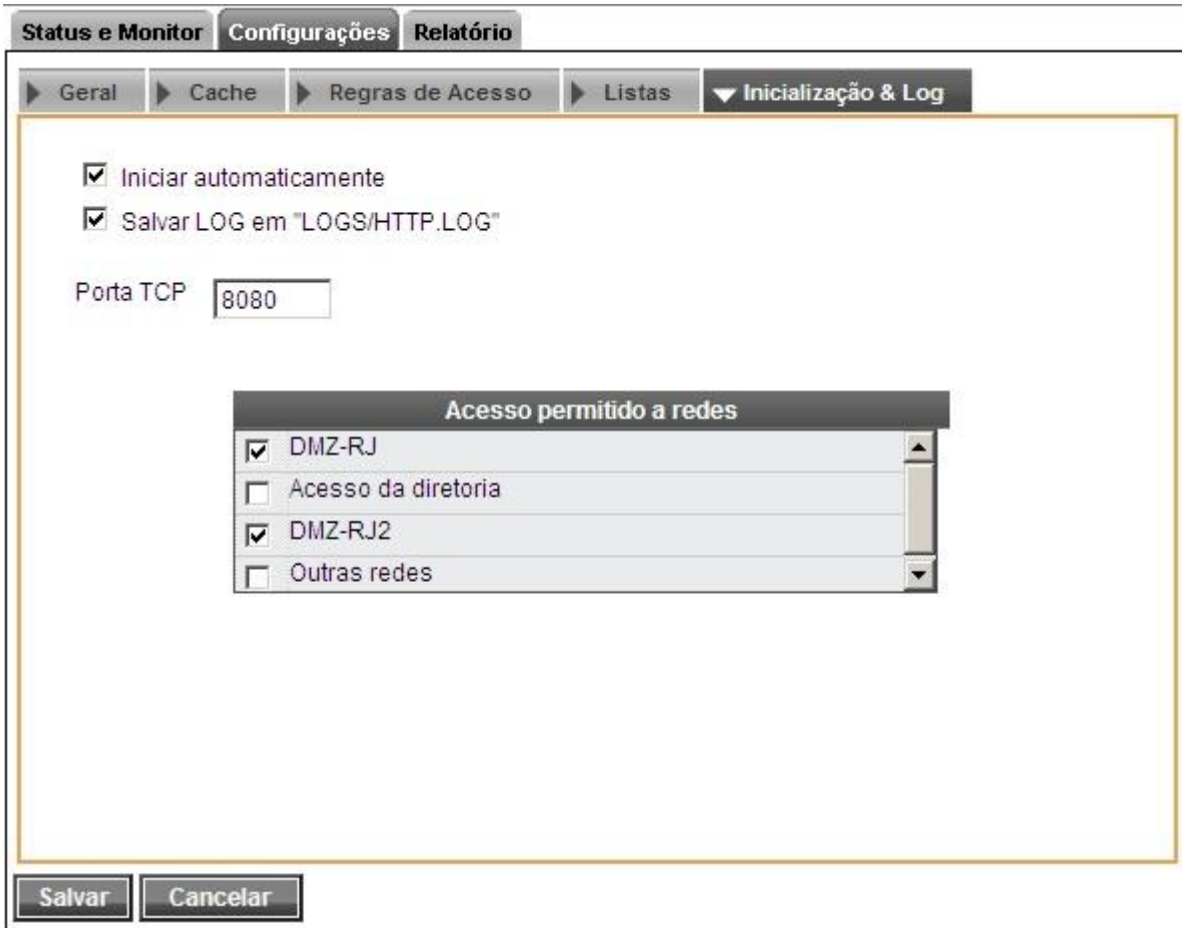
9.3.5. Guia Inicialização & Log

- **Iniciar automaticamente:** Habilite essa opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 6**.

- **Salvar LOG em "LOGS/HTTP.LOG":** *O arquivo em bloco de notas (HTTP.LOG)* será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 6\LOGS* e conterá todas as informações referentes a este serviço.

- **Porta TCP:** Normalmente a porta padrão é **8080** e não deve ser alterada.

- **Acesso permitido a redes:** Indica a rede que tem acesso ao serviço. Não é aconselhável habilitar o acesso a clientes externos (Outras Redes), pois isto permitiria uma invasão a rede interna.



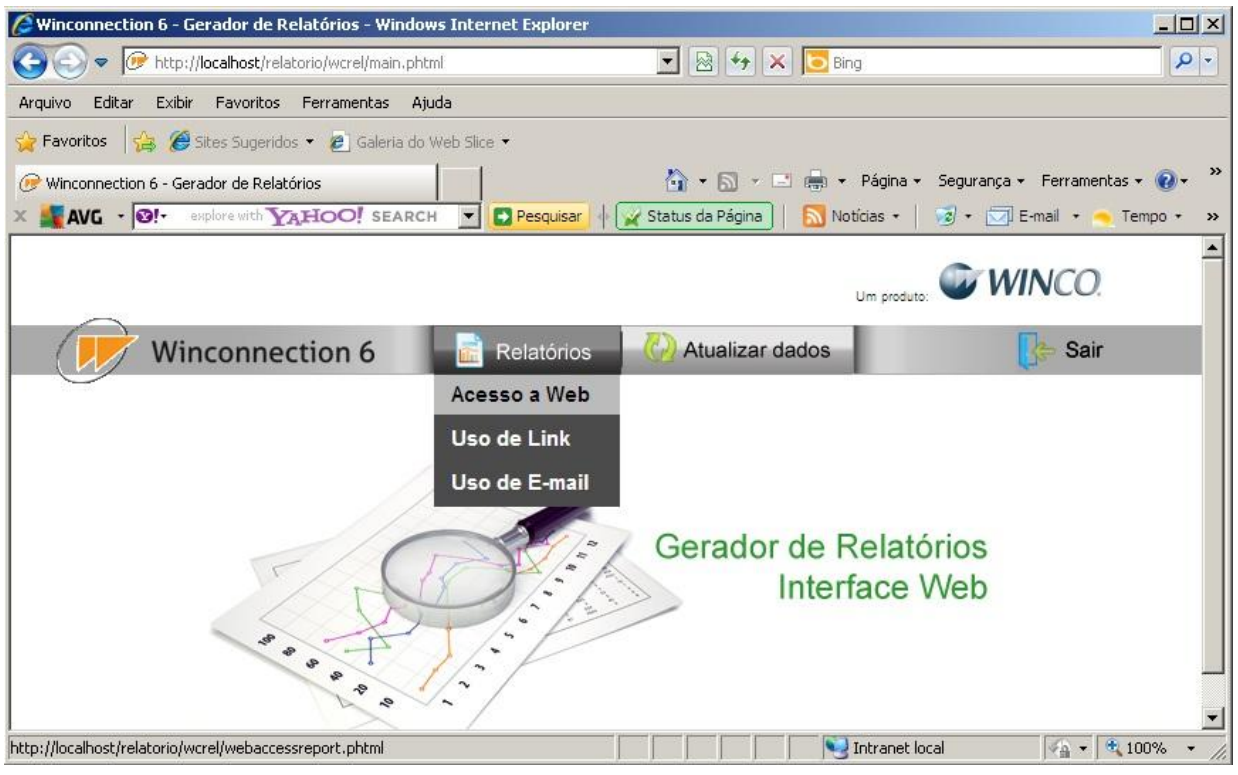
9.3.6. Guia Relatórios

O **Relatório Web** permite que o administrador de rede possa verificar todos os sites acessados na internet e desta maneira imprimir relatórios de acordo com a totalização mais adequada. Esta é a forma indicada de consulta ao histórico de navegação da empresa, por usuário ou IP da máquina.

O relatório pode ser gerado, baseando-se nos seguintes dados:

- **Usuário:** Ao selecionar um usuário é possível verificar os domínios acessados por ele, com a possibilidade de detalhar os acessos aos domínios.
- **Domínio:** Exibe um ranking de domínios mais acessados, com possibilidade de detalhar o acesso ao domínio ou exibir os usuários que fizeram acesso ao domínio em questão.
- **Hora de acesso**
- **Total de acessos/dia**

Obs.: Também é possível acessar o *Relatório Web* através do navegador, digitando o endereço: *http://ip_do_servidor/relatorio*. Após se logar no Gerador de Relatórios, selecione a opção *Relatórios → Acesso a Web*.



9.3.7. Bloqueio por sites – Dicas de Configuração

Ao adicionar um site em uma regra de acesso à navegação do **Winconnection 6**, o administrador da rede pode escolher um domínio específico como www.website.com ou um conjunto de sites através do uso de coringas (wildcards). Como no DOS, os coringas são os caracteres interrogação (?) e asterisco (*).

Observação importante: Não utilize o protocolo quando for adicionar ou alterar um site proibido ou permitido. O protocolo é a parte "http://" ou "ftp://" da URL.

Defina um site através dos seguintes exemplos:

www.meusite.com => Controla o acesso ao site "www.meusite.com"

www.???site.com => Controla o acesso aos sites "www.meusite.com",

www.teusite.com, e outros que tenham outros caracteres nas posições das interrogações.

*meusite.com.br => Controla o acesso aos sites terminados com "meusite.com.br".

www.meusite* => Controla o acesso aos sites iniciados por "www.meusite".

sex => Controla o acesso aos sites que contenham o termo "sex", exemplos: www.sex.com , www.sexo.com.br , www.sextosentido.com.br, www.sextavado.com.

*/playboy => Controla o acesso aos sites que contenha os subdiretórios */playboy, por exemplo: www.uol.com.br/playboy, www.abril.com.br/playboy

10. Topologias e Casos de Uso

10.1. Configuração do Proxy Transparente nas estações

O **Proxy Transparente** é compatível, nas estações, com qualquer sistema operacional. Para ativar o uso do **Proxy Transparente** nas estações de trabalho, faça o seguinte:

Windows NT/2000/XP/2003:

- Clique em *Iniciar -> Configurações -> Conexões de Rede* -> Clique em *Conexão de Rede -> Propriedades - TCP/IP -> Propriedades.*
- No Campo *Gateway* digite o **IP do servidor Winconnection 6** (*por exemplo*: 192.168.0.1).
- No Campo *Servidor DNS Preferencial* digite o **IP do servidor Winconnection 6** (*por exemplo*: 192.168.0.1).

Windows 95/98/ME:

- Clique em *Iniciar -> Configurações -> Painel de Controle -> Rede → TCP/IP -> Propriedades*.
- Na Guia *Gateway* digite o **IP do servidor Winconnection 6** (por exemplo: 192.168.0.1).
- Na Guia *Servidor DNS Preferencial* digite o ou I**IP do servidor Winconnection 6** (por exemplo: 192.168.0.1).

É necessário reiniciar o computador para finalizar as configurações.

Linux:

- Edite o arquivo /etc/sysconf/network e altere o valor de *Gateway* para o **IP do servidor Winconnection 6**, por exemplo: GATEWAY="192.168.0.1"
- Edite o arquivo /etc/resolv.conf e altere o valor de *nameserver* para o **IP do servidor Winconnection 6**, por exemplo: nameserver 192.168.0.1
- Reinicie o /etc/rc5.d/S restart

Este serviço deixa a estação como que "conectada diretamente à internet". Acesse o tópico Saída para aprender como **bloquear/permitir** aos usuários determinadas funções, limitando assim o uso da internet na empresa.

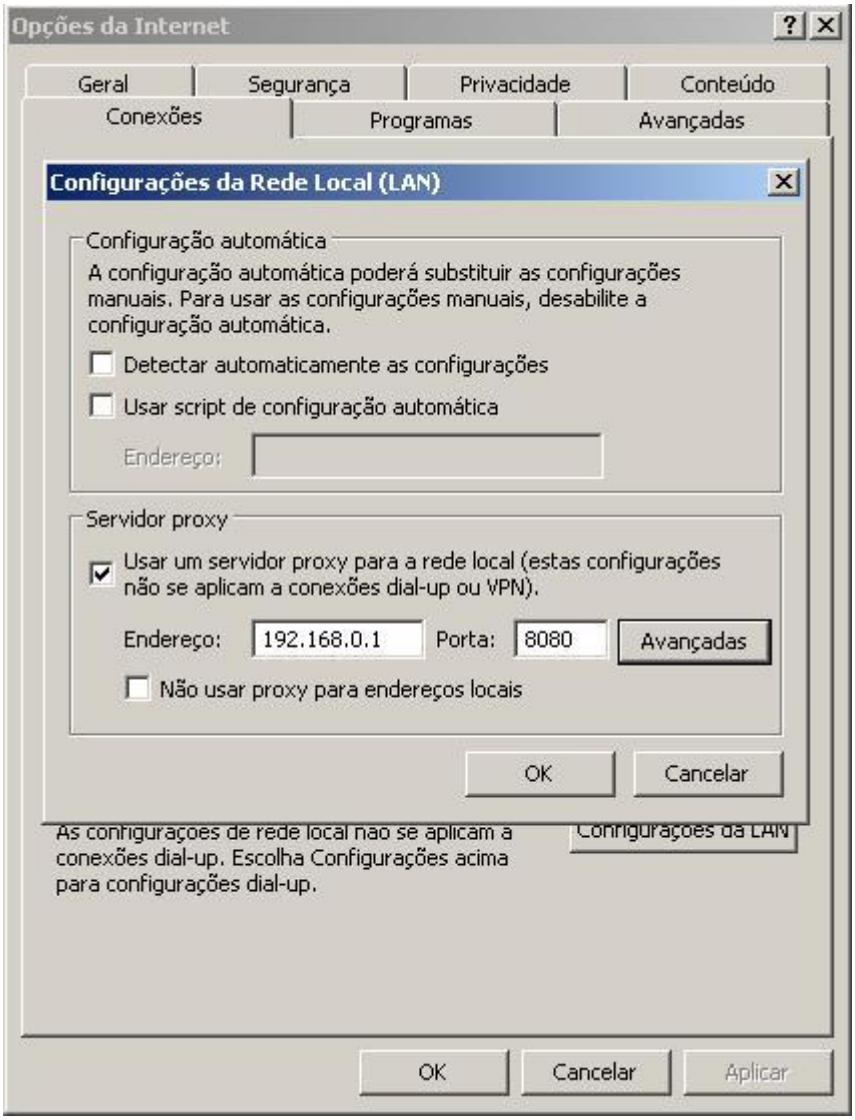
10.2. Configuração da navegação

10.2.1. Configuração da navegação através do Proxy WWW

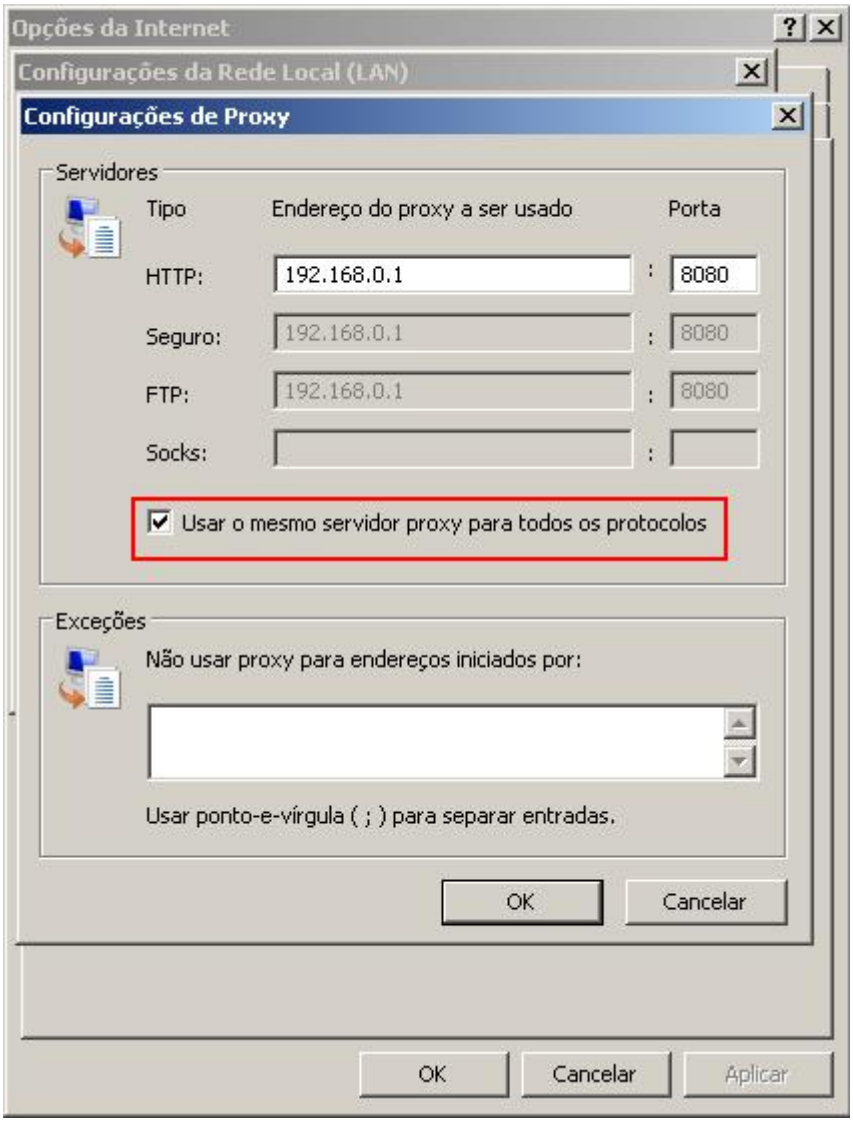
Após a instalação do **Winconnection 6**, o serviço **Filtro Web** é adicionado automaticamente na porta 8080 no menu de serviço Servidos de Gateway.

Para configurar a navegação nas estações, faça o seguinte:

- Abra Internet Explorer, clique no menu superior Ferramentas –> Opções da Internet. Clique na guia *Conexões* e clique em *Configuração da LAN*. Habilite a opção "**Usar um servidor Proxy para a rede local**", no campo Endereço, digite o IP do servidor Winconnection (por exemplo: 192.168.0.1) e no campo Porta, digite: 8080.



- Clique no botão *Avançadas* e selecione a opção "**Usar o mesmo proxy para todos os protocolos**". Clique no botão OK em todas as telas.



O **Winconnection 6** passará todas as conexões HTTP 1.0 e 1.1, HTTPS e WebFTP. É possível controlar o conteúdo de navegação bloqueando ou permitindo sites através de regras de acesso à navegação. Consulte o tópico Filtro Web para mais informações.

10.2.2. Configurando a navegação através do Proxy Transparente

Para configurar a navegação através do **Proxy Transparente**, realize a configuração no **Winconnection 6** citada no tópico Saída e configure as estações conforme descrito no tópico Configuração do Proxy Transparente nas estações.

10.3. Configurando o Servidor de E-mails no Winconnection 6

Existem três maneiras de configurar os e-mails usando o **Winconnection 6**:

- **Servidor de E-mails**
- **Direto do Provedor**
- **Usando o Winconnection 6 diretamente como MX.**

Todas atendem qualquer tipo de cliente. Porém a mais indicada e que é um diferencial em relação aos seus concorrentes é o Servidor de E-mails. Esta configuração permite controlar tamanho de e-mails, domínios internos, verificação de vírus em mensagens, monitoramento de mensagens enviadas/recebidas, filtro anti-spam, etc.

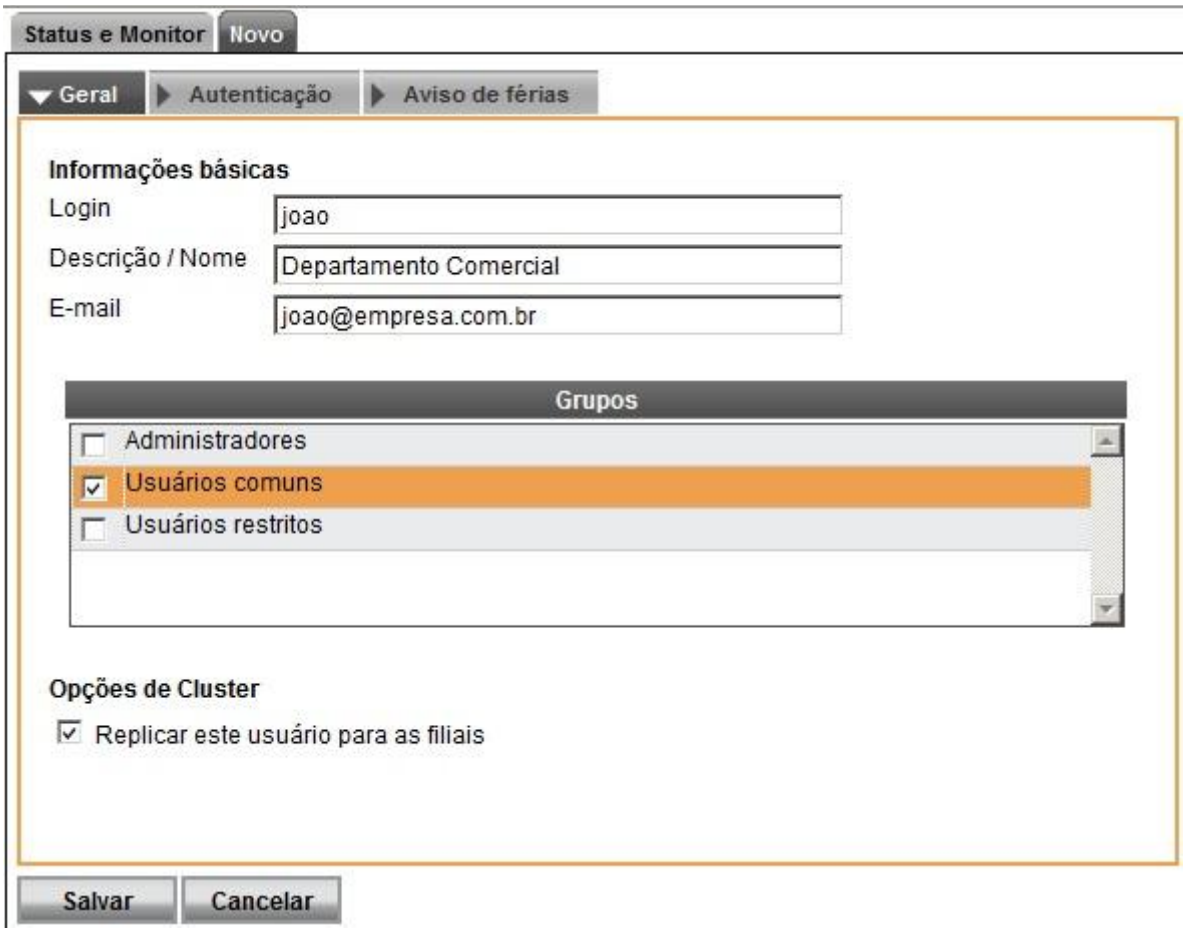
Para configurar o servidor de e-mail do **Winconnection 6**, faça o seguinte:

1º) Passo – Configurando o Administrador:

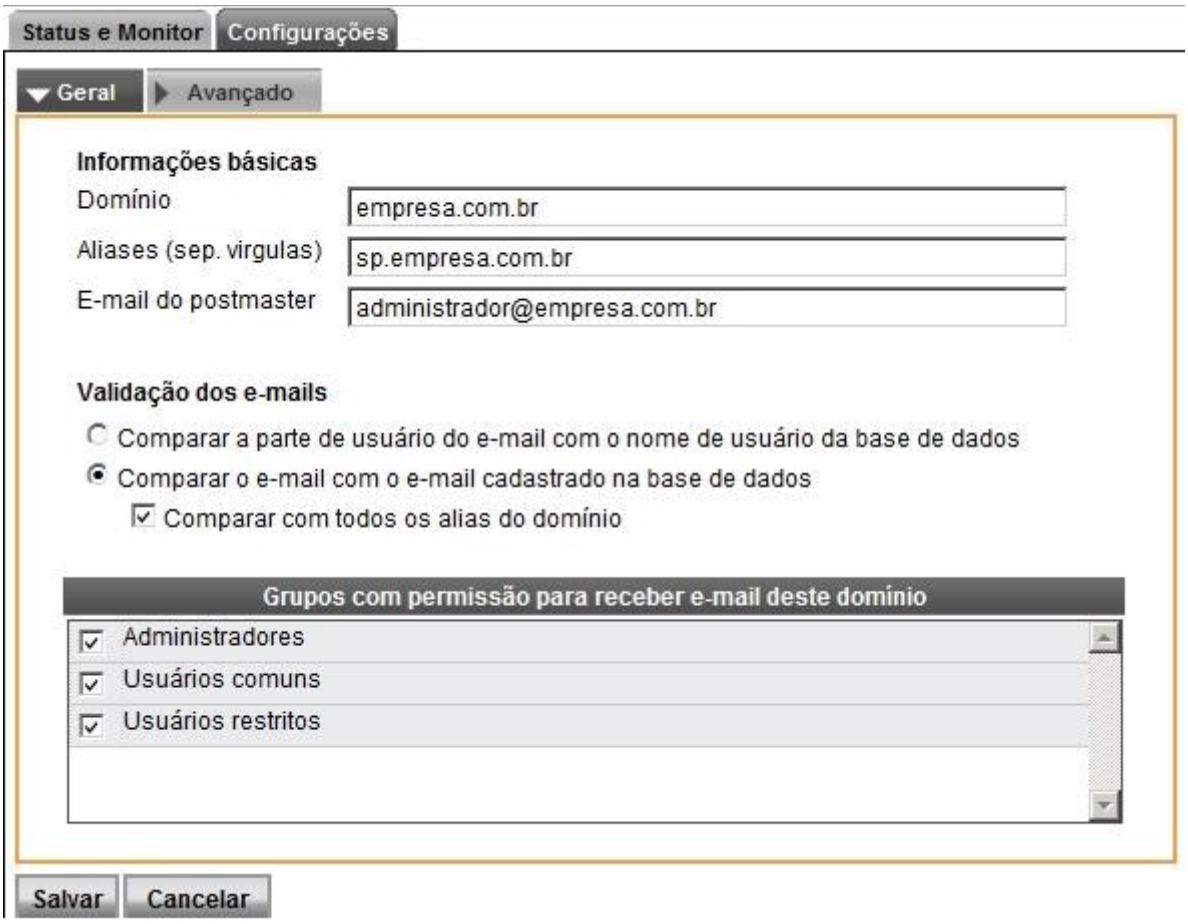
a) Crie todos os usuários que farão parte do Servidor de E-mail do **Winconnection 6** conforme descrito no capítulo Usuários.

b) No administrador do **Winconnection 6**, clique em *Serviços de E-mail* e verifique se os seguintes serviços estão instalados no Administrador do Winconnection 6:

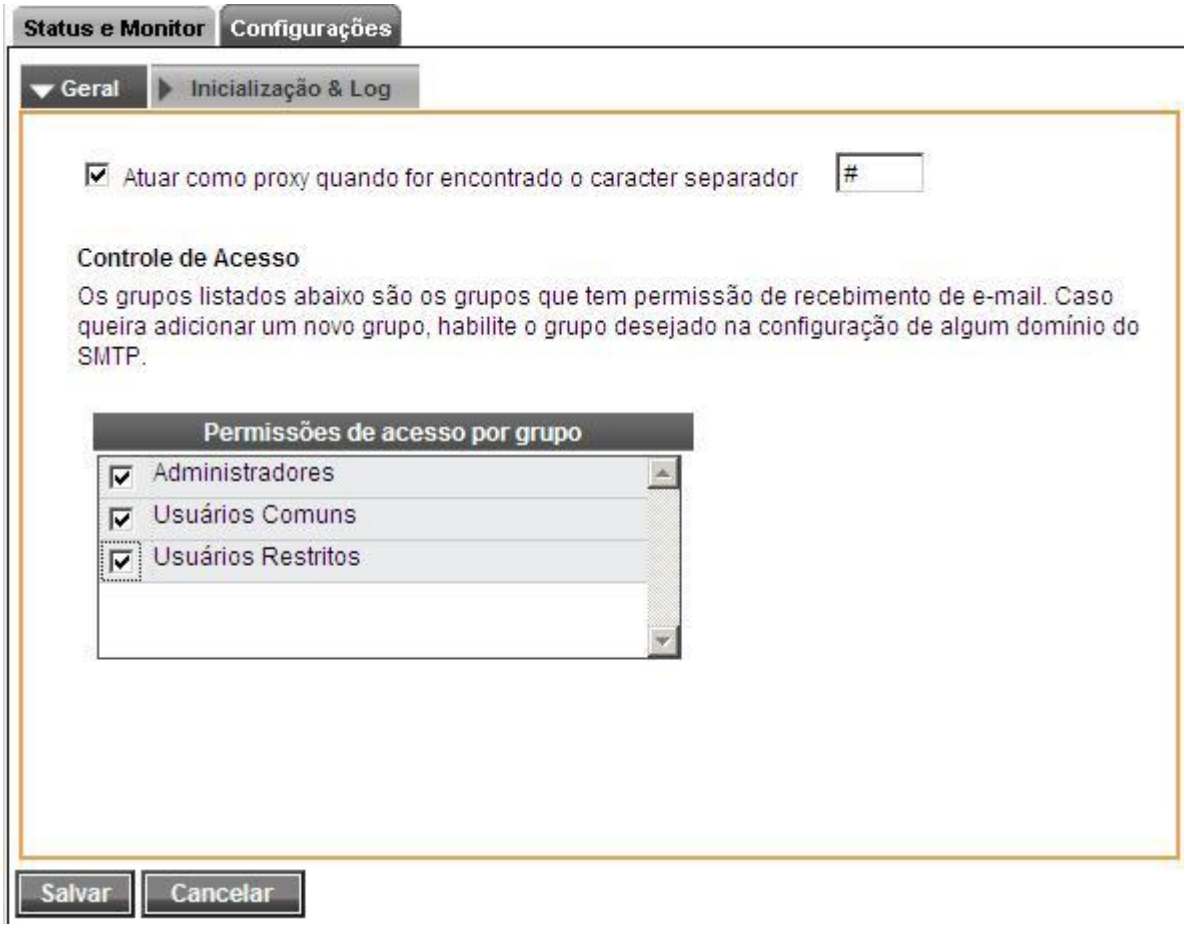
Obs.: Se esses serviços não estiverem instalados, será necessário instalá-los clicando no meu superior *Serviços* | *Novo*.



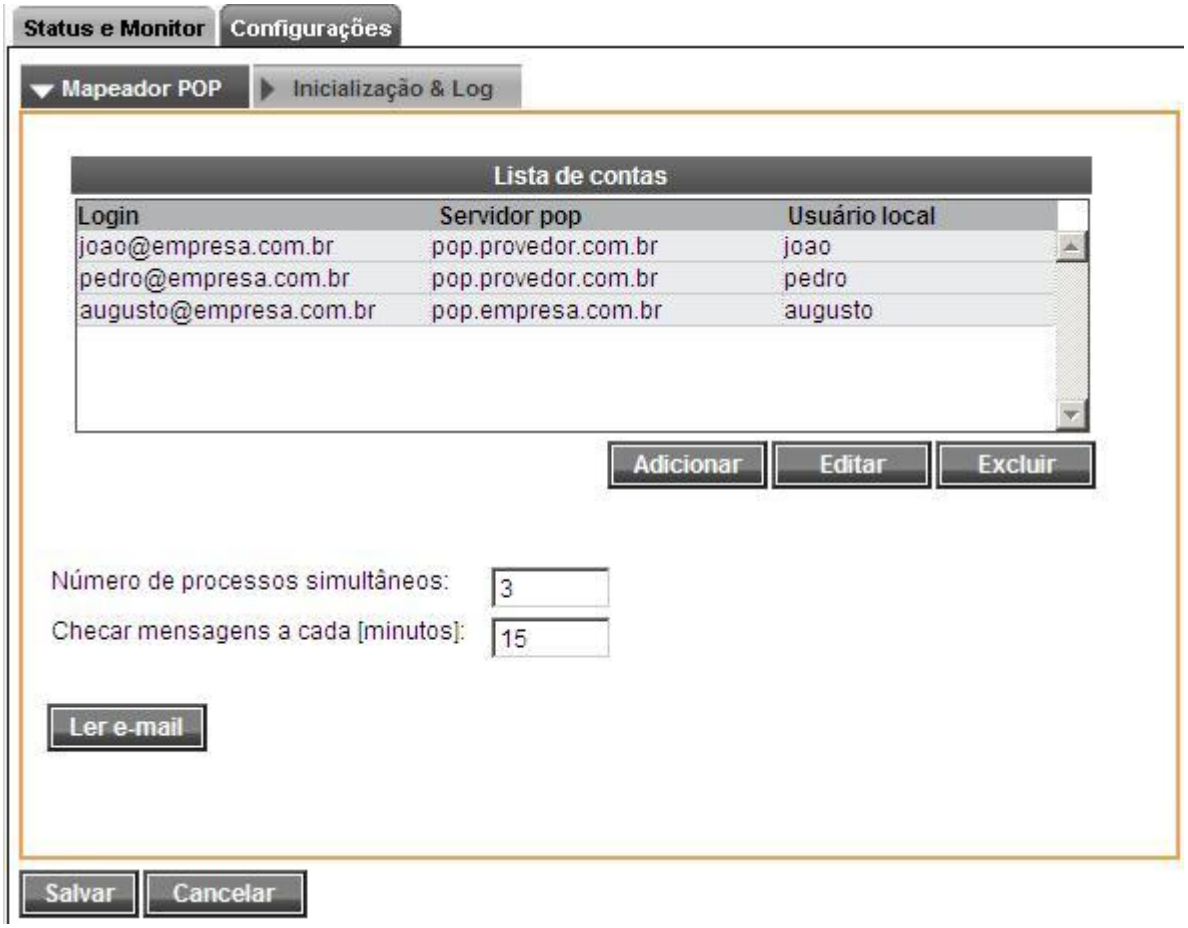
c) No lado esquerdo da tela, selecione o serviço **Servidor SMTP** e clique na guia "Configurações". Configure esse serviço seguindo as instruções descritas no capítulo Servidor SMTP.



d) No lado esquerdo da tela, selecione o serviço **Servidor POP3**, clique na guia "Configurações" e habilite os grupos de usuários que terão acesso a esse serviço. Para mais informações, consulte o capítulo Servidor POP3.



e) No lado esquerdo da tela, selecione o serviço Mapeador POP e cadastre as contas de e-mail que farão parte do Servidor de E-mail do **Winconnection 6**.



2º) Passo – Configurando as Estações:

a) Entre na tela de configuração de contas do Cliente de E-mail da estação. Usaremos como exemplo o Outlook Express:

- Clique no menu superior Ferramentas -> Contas -> Selecione a conta e clique em Propriedades -> Clique na guia Servidores.

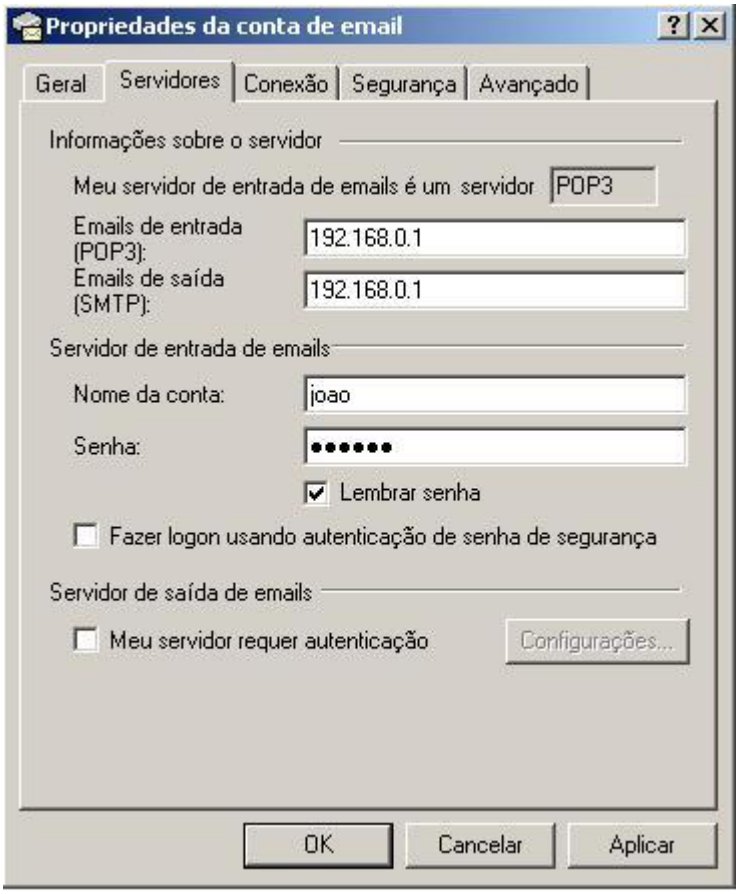
b) No campo *Servidor POP3*, digite o IP do servidor **Winconnection 6**. (No nosso exemplo: 192.168.0.1).

c) No campo *Servidor SMTP*, digite o IP do servidor **Winconnection 6**. (No nosso exemplo: 192.168.0.1).

d) No campo *Usuário*, coloque o nome do usuário cadastrado na *Lista de Usuários* do **Winconnection 6**. No nosso exemplo: **joao**.

e) No campo *Senha*, coloque a senha para o usuário que você criou no **Winconnection 6**.

Obs.: Note que neste campo, estamos usando a senha do usuário interno (criado no **Winconnection 6**) e não, a senha no provedor.



Após clicar no botão OK, a estação já estará pronta para enviar e receber e-mails através do Servidor de E-mail do **Winconnection 6**.

10.4. Configurando o Winco Messenger

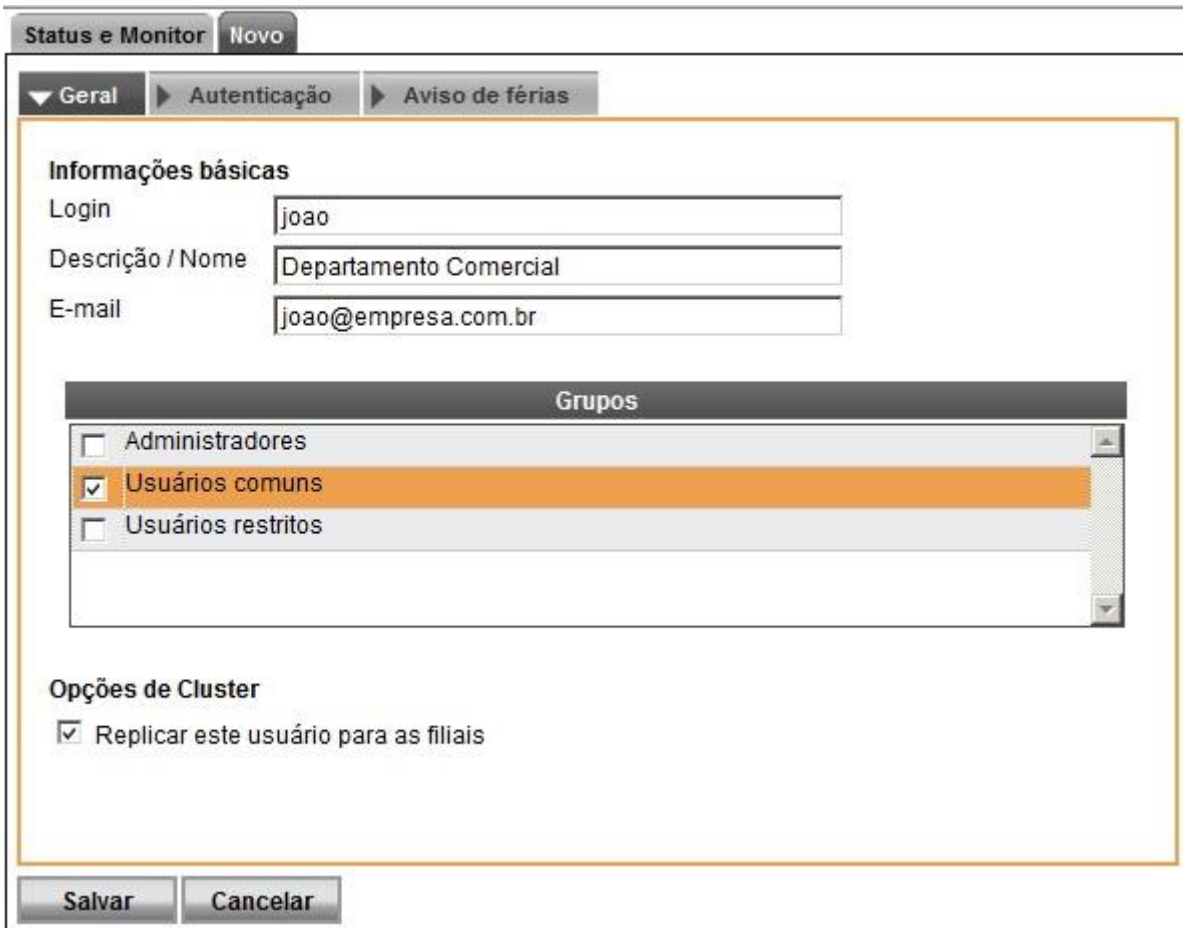
O **Winco Messenger** é integrado na base de usuários do **Winconnection 6**, e pode ser usado para troca de mensagens entre os colaboradores internos ou externos à rede da empresa. O produto possui funções de transferência de arquivos, aviso sonoro e gravação de históricos de conversas efetuadas na estação onde foi instalado.

Este módulo é **gratuito** para todos os usuários que adquiram as licenças do **Winconnection 6**, e pode ser instalado sem a necessidade de uma licença adicional.

Para configurar o Winco Messenger, siga os seguintes passos:

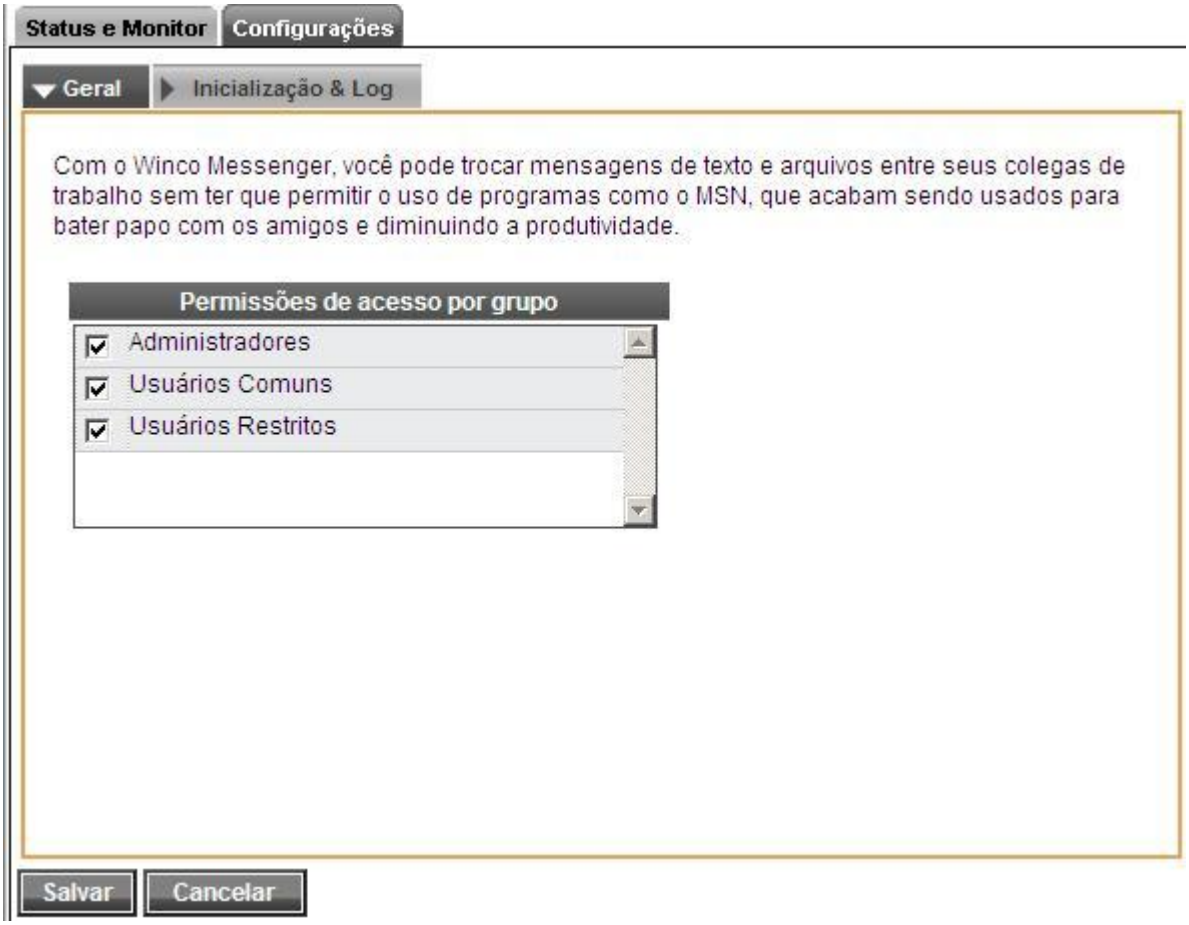
1º Passo: Configurando o Administrador.

a) Se os usuários ainda não foram cadastrados no administrador, você deverá cadastrá-los no menu **Usuários**", conforme descrito no capítulo V.1. Usuários.



b) Clique no menu superior *Serviços* -> *Novo* e selecione o serviço **Winco Messenger**.

c) Selecione os grupos que poderão usar o **Winco Messenger**.



2º Passo: Configurando as Estações.

a) Logando-se no Winco Messenger:

- Clique duas vezes no ícone do **Winco Messenger** exibido próximo ao relógio de Windows. Irá aparecer uma tela solicitando "*Servidor*", "*Login*" e "*Senha*".

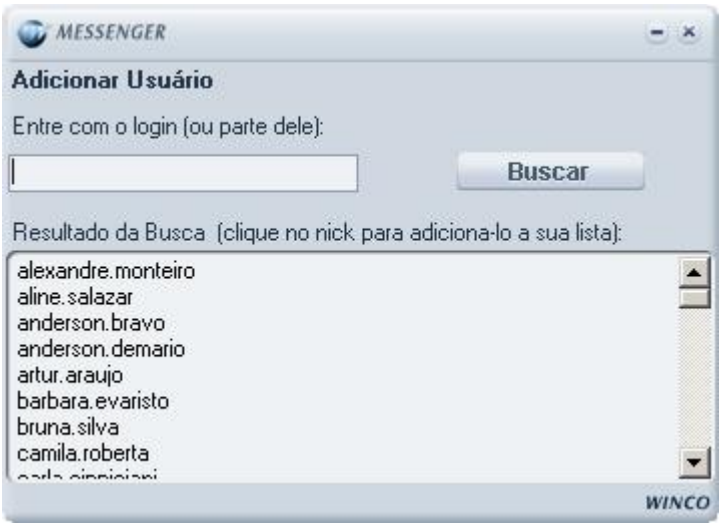
- No campo "**Servidor**", digite o IP do Servidor onde foi instalado o **Winconnection 6** (por exemplo: 192.168.0.1).

- No campo "**Login**", coloque o nome do usuário que está cadastrado na lista de usuários do **Winconnection 6**.

- No campo "**Senha**", coloque a senha do usuário que está cadastrada no **Winconnection 6**.

b) Adicionar usuários:

Para adicionar os usuários no **Winco Messenger**, basta clicar em "**Contatos**", e em seguida, clicar em "**Buscar**".



10.5. Bloqueando o Ultrasurf

O *Utrasurf* é um software criado pela *Ultrareach Internet Corporation* com o objetivo inicial de ajudar usuários da internet na China a burlar a censura e garantir a sua privacidade. Outros 42 países, segundo a *Freedom House*, também promovem alguma forma de censura na internet e o *Ultrasurf* tem sido uma valiosa ferramenta para os que tentam escapar da censura e repressão em seus países. Por conta disso, conta com o suporte de uma extensa rede de voluntários em favor da causa da liberdade.

No entanto, o *Ultrasurf* também está sendo usado para burlar as políticas de uso e segurança de redes corporativas. Com o auxílio deste programa, os usuários das redes das empresas conseguem acessar pornografia e outros itens não relacionados ao trabalho, sem deixar rastros. As empresas costumam criar regras de uso da internet para evitar dispersão no trabalho, acesso a sites impróprios para o ambiente de trabalho e diminuir os riscos de segurança.

Felizmente, o *Ultrasurf* e outros programas do gênero podem ser bloqueados usando o **Winconnection 6**. Basta configurar o **Winconnection 6** utilizando técnicas de *hardening* para bloquear o *Ultrasurf* e ainda tornar a sua rede mais segura.

Programas como *Ultrasurf*, utilizam portas altas para fazer a conexão e como não são portas fixas, é necessário criar regras para liberar apenas as portas mais utilizadas na rede.

Para isso, siga os seguintes procedimentos:

- No *Administrador* **Winconnection 6**, clique em *Filtro Web*;

- Habilite a opção "*Capturar conexões transparentes*" (caso contrário, o acesso à web não funcionará).

  Veja um exemplo na imagem abaixo:

- Clique em *Salvar*.

Em seguida, é necessário criar regras de acesso para habilitar as portas que são efetivamente usadas.

ATENÇÃO: Não configure essas mesmas regras para as portas **80**, **8080** e **443**, pois as mesmas são freqüentemente utilizadas por programas como o *Ultrasurf* para fazer as conexões.

Estas regras devem ser criadas da seguinte forma:

- No *Administrador* **Winconnection 6**, clique em *Firewall -> Saída -> Configurações*;

- Selecione as opções *Habilitar Controle de Acesso* e *Permitir apenas os casos abaixo*;

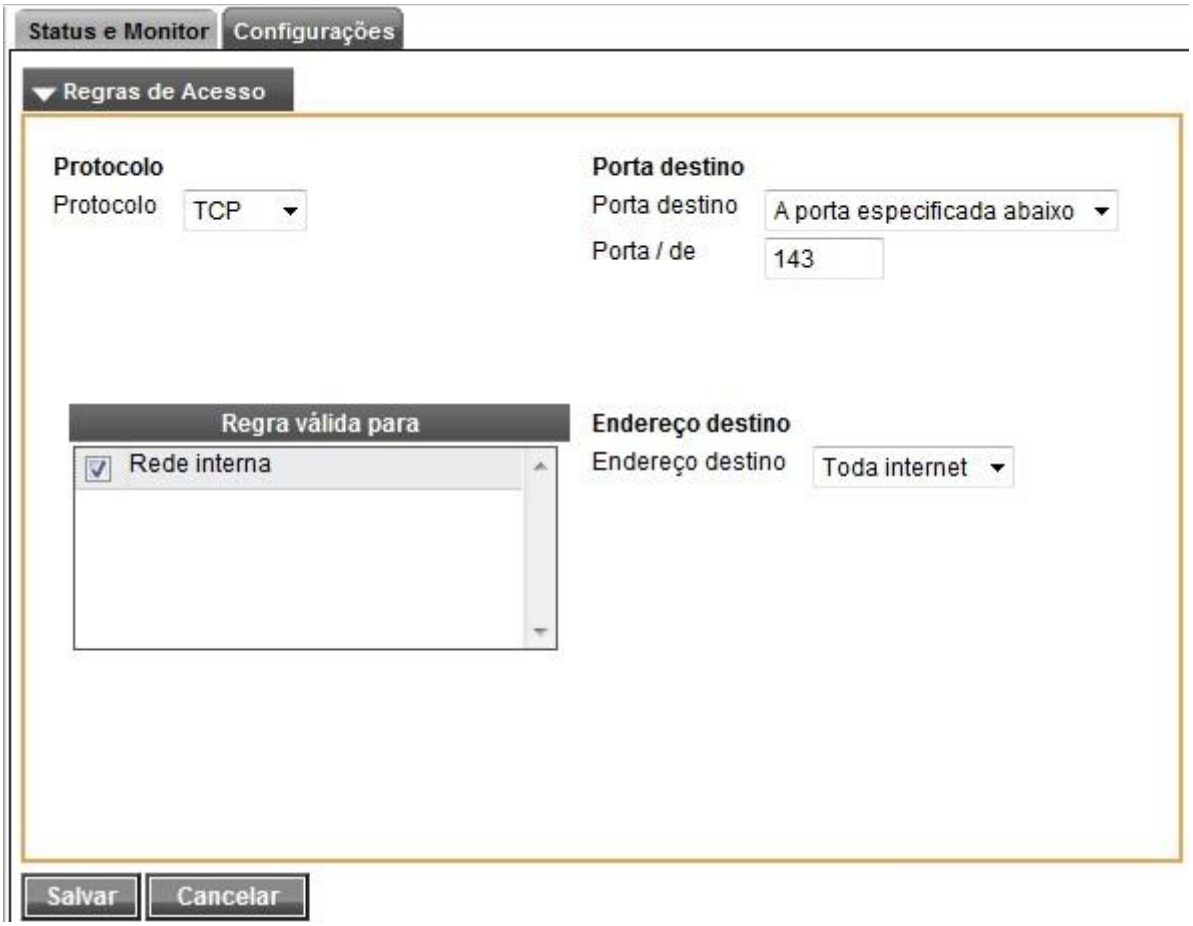
- Clique em *Adicionar* e configure as regras de acordo com a necessidade da sua rede.

A seguir, mostraremos alguns exemplos para liberar o acesso de algumas portas:

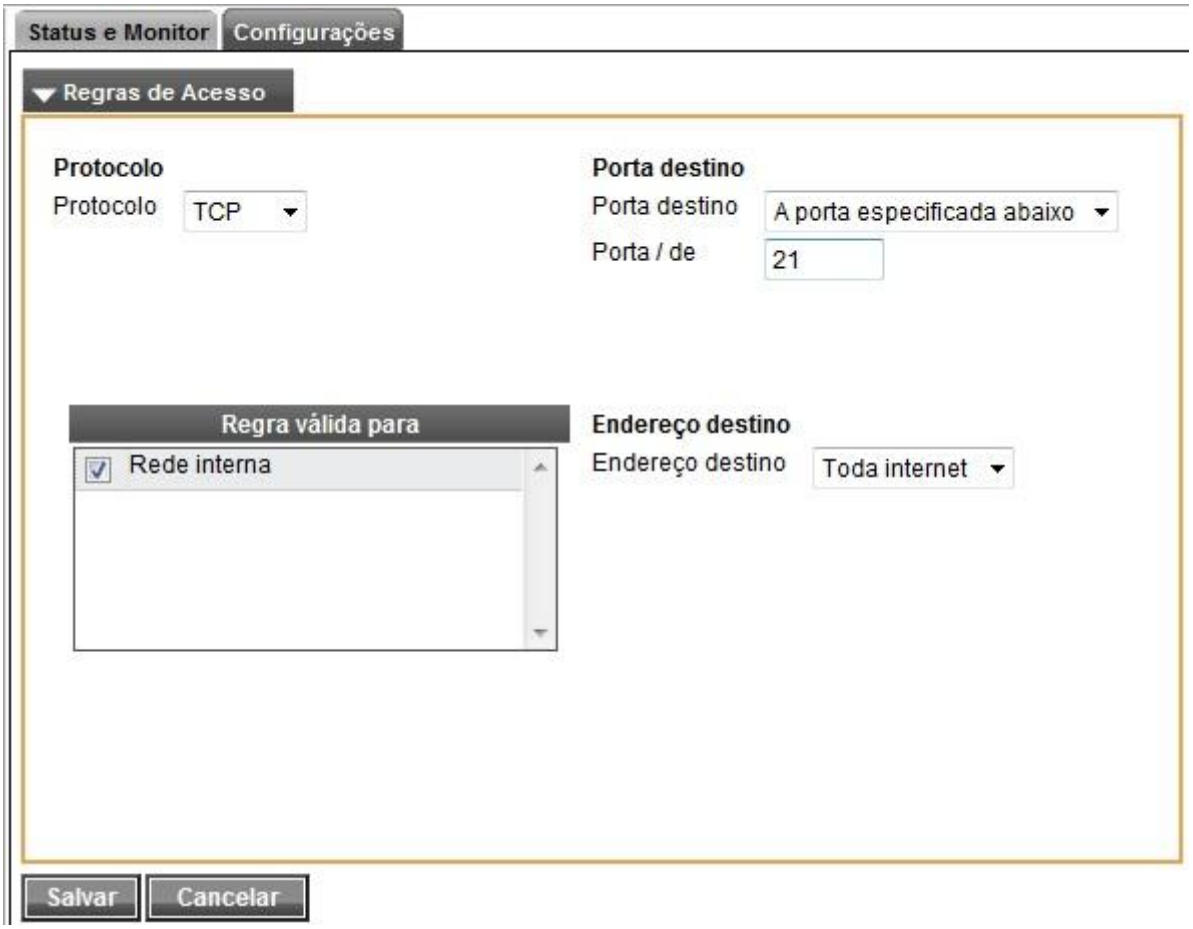
Regra para SMTP (porta TCP 25):

Regra para POP (porta TCP 110):

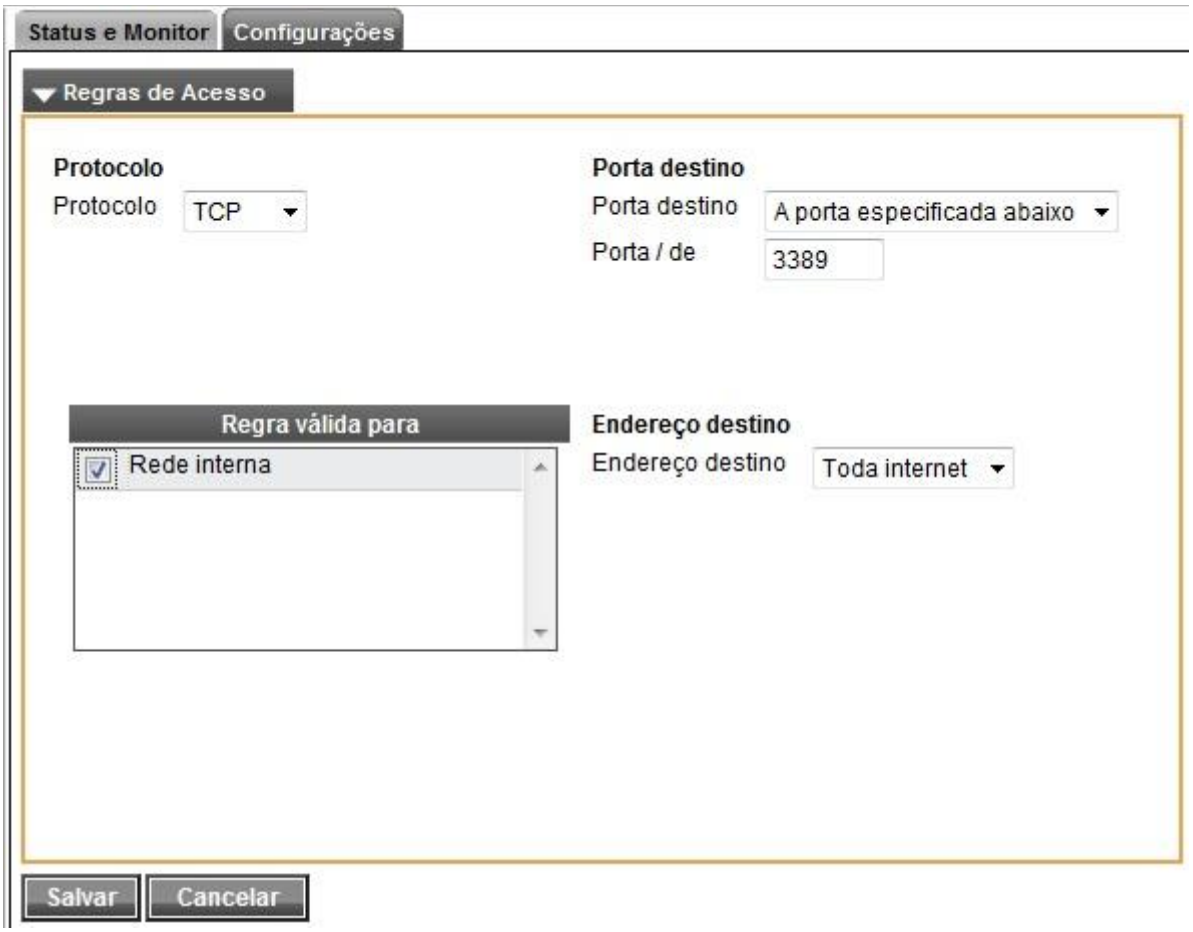
Regra para IMAP (porta TCP 143):



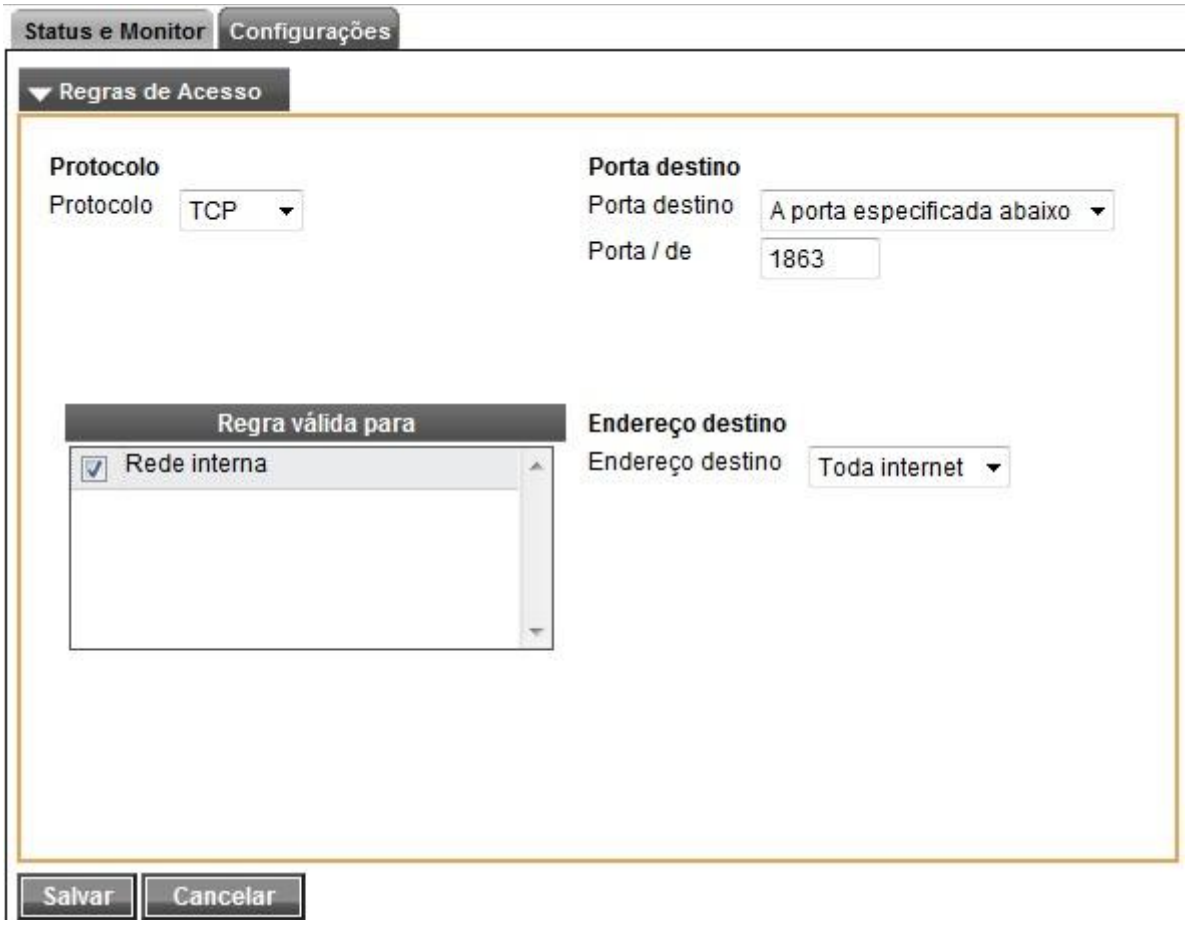
Regra para FTP (porta TCP 21):



Regra para Terminal Server (porta TCP 3389):



Regra para MSN (porta TCP 1863):



11. Winconnection Web Filter para Linux

Neste capítulo do manual, vamos descrever as principais configurações do **Winconnection Web Filter para Linux**.

11.1. Características do Winconnection Web Filter para Linux

Veja a seguir as principais características e funcionalidades do **Winconnection Web Filter para Linux**:

- Fácil instalação e configuração: o gerenciamento é feito através de um Administrador Web.
- Estabilidade, segurança e administração simplificada.
- Integração com o MS Active Directory (AD).
- Bloqueio do Ultra-Surf.
- Compartilhamento de conexão.
- Registro de logs para todos os serviços.
- Atualização automática do programa (auto-update).
- Relatório de utilização do link.
- Controle de banda.
- Inspetor de pacotes (bloqueio da conexão de acordo com o protocolo).
- Servidor PROXY HTTP, HTTPS contendo:
    - Controle de acesso à internet por grupo de usuários;
    - Controle de acesso à internet por site/conjunto de site/horários;
    - Regras de acesso simplificadas;
    - Bloqueio de download de arquivos (extensão);
    - Plug in para Filtro Automático de Conteúdo;
    - Importação de lista de sites em formato texto;
    - Restrição de tempo de navegação;
    - Restrição de limite de transferência diária;
    - Relatório de navegação por usuário;
- Servidor Web contendo:

- Suporte a PHP;
- Criação de múltiplos "alias";

- Servidor de Mensagem Instantânea com transferência de arquivos (Winco Messenger).
- Cliente DDNS (DNS Dinâmico).
- Servidor DHCP
- Porta TCP Mapeada

11.2. Instalação

11.2.1. Requisitos de Software

O **Winconnection Web Filter para Linux** pode ser instalado nos seguintes sistemas operacionais:

- Centos / Ubutun / Red-Hat / Debian / Fedora / Suse
- Plataformas I386/ I586 / I64
- Kernel superior a versão 2.4

Obs.: Para instalar o **Winconnection Web Filter para Linux** é necessário ter acesso a Internet e protocolo HTTPS para validar a licença no momento da instalação.

11.2.2. Requisitos de Hardware

Equipamento Mínimo:

- Processador de 1GHz
- 512 MB de RAM
- HD de 120GB

Equipamento Recomendado:

- Processador de 2GHz ou superior
- 1GB de RAM
- HD de 120GB

Obs.: São necessárias **duas placas de rede**: Uma para rede interna e outra para rede externa.

11.2.3. Antes de Instalar

Este manual parte do princípio que o administrador tenha conhecimentos básicos de TCP/IP e conhecimento dos programas de acesso à Internet instalados na rede (chamados de clientes).

Recomendamos verificar os itens abaixo antes de instalar o **Winconnection Web Filter para Linux**:

- O computador onde será instalado o **Winconnection Web Filter para Linux** deve estar funcionando normalmente, conectado à internet e com todas as funções de navegação em perfeito estado.

- Todos os clientes devem estar com o protocolo TCP/IP instalados e funcionando corretamente. O Administrador deve conhecer a topologia da rede interna, bem como o IP do servidor e dos clientes e a classe de rede utilizada.

- O Administrador que irá fazer a instalação deve possuir uma ideia clara dos serviços que irá usar no **Winconnection Web Filter para Linux** e por qual motivo quer usar o produto.

- Recomendamos se logar no Linux como *Administrador (root)*. Isto se deve ao fato de que o programa se instala como um serviço do sistema operacional, que é iniciado automaticamente toda vez que o computador é ligado.

- Modos de Serviço de Verificações de Daemons (como o **SeLinux**) devem estar desabilitados ou a liberação do Serviço do Winconnection deve ser realizada.

11.2.4. Instalando o Winconnection Web Filter para Linux

Primeiramente, faça o download da versão mais recente do programa disponível na seção de download do site do **Winconnection**.

Após concluir o download, execute o arquivo de instalação:
./nome do arquivo de instalação do Winconnection

Por Exemplo:
./Winconnection65-linux.sh

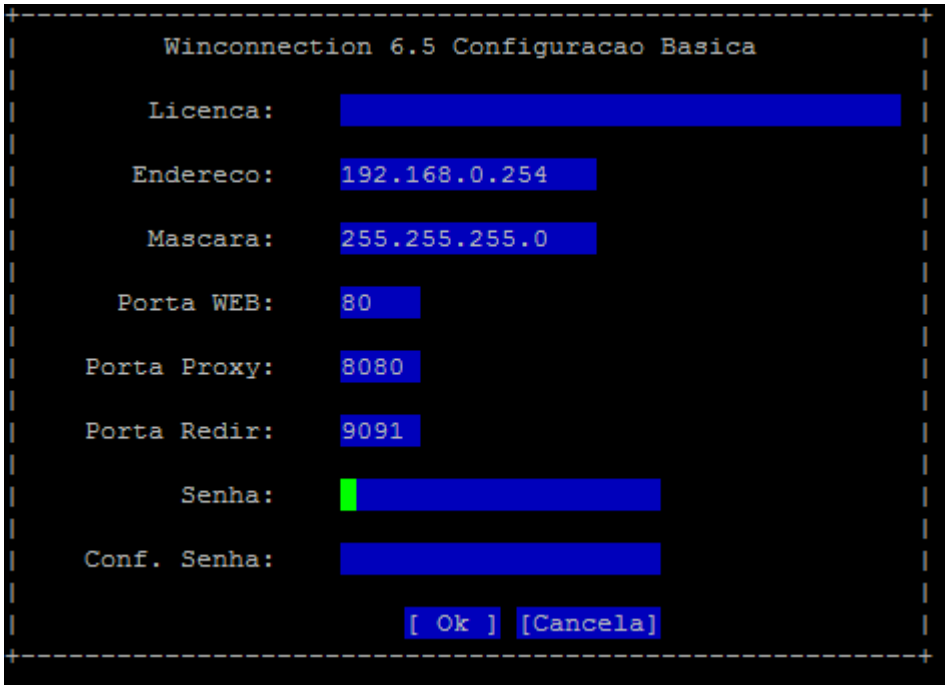
O *Assistente de Instalação* ajudará a instalar e criar as pastas e arquivos do **Winconnection Web Filter para Linux**. O diretório padrão é *opt**wc65*\.

Após finalizar a instalação, o **Winconnection Web Filter para Linux** inicia automaticamente o Assistente de Configuração. Siga os passos desse assistente, informando corretamente os dados (as etapas estão descritas detalhadamente no próximo tópico - 11.3.5. Assistente de Configuração). Assim que as etapas do Assistente de Configuração forem concluídas, o **Winconnection Web Filter para Linux** será inicializado e pronto para ser usado.

11.3.5. Assistente de Configuração

O *Assistente de Configuração* é iniciado logo após o término da instalação e realiza o processo de pré-configuração do **Winconnection Web Filter para Linux**.

Veja a seguir uma breve descrição das etapas disponíveis no *Assistente de Configuração*:



- **Licença:**
  O primeiro campo do assistente é o de licenciamento. Inseria a licença que foi enviada para o e-mail cadastrado no momento da aquisição do produto.

- **Endereço:**
  No segundo campo, é necessário informar o endereço IP da rede interna.

- **Máscara:**
  Neste campo, é necessário informar a máscara da rede interna.

- **Porta Web**

  Informe a Porta Web que será utilizada para o acesso do Administrador Web do Winconnection.

  Obs.: Verifique se não está sendo utilizado o *Serviço Apache* ou qualquer *Serviço Web* do Linux (O Winconnection possui seu próprio serviço Web não necessitando a instalação de serviço Web aparte, por exemplo, *Apache*, *Tomcat*, etc.).

- **Porta Proxy:**

  Informe em qual porta irá funcionar o serviço de Proxy. Por padrão, o programa **Winconnection** funciona na porta 8080, mas esta porta pode ser alterada.

- **Porta Redir.:**

  Neste campo, é necessário informar a porta do redirecionamento de requisições do Winconnection (este serviço é o *Proxy Transparente* na versão **Winconnection** para Windows).

- **Senha:**

  O sétimo campo é a criação de senha para o acesso do usuário "administrador" do Winconnection.

- **Confir. Senha:**

  Confirme a senha digitada no campo anterior.

  Por fim, confirme todas as informações pressionando *[OK]*.

Após concluir o *Assistente de Configuração*, é possível abrir o Administrador Web do **Winconnection Web Filter para Linux** via navegador (Internet Explorer/ Firefox/ Chrome) e realizar outras configurações e as demais funcionalidades do produto que estão descritas neste manual.

Para acessá-lo, digite o seguinte endereço no navegador:
http://ip_do_servidor/admin

Digite o login e a senha do administrador ou de algum usuário que pertença ao grupo *"Administradores"*.

Mais informações sobre o Administrador Web podem ser encontradas no Capítulo 4 deste manual.

11.3. Integrando o Winconnection Web Filter para Linux

Para que o **Winconnection Web Filter para Linux** funcione de maneira integrada com as políticas de segurança previamente estabelecidas pelo administrador do sistema, certos cuidados e procedimentos devem ser adotados. Adiante apresentamos o conjunto de procedimentos e informações que possibilitarão a integração bem sucedida, complementando as políticas de segurança estabelecidas.

11.3.1. Arquiteturas Básicas

O **Winconnection Web Filter para Linux** permite o uso de várias arquiteturas de rede. Embora, não esgotemos todas as possibilidades de arquitetura que existam, as apresentadas aqui fornecem blocos de construção para muitas delas.

a) Filtro com Acesso Exclusivo a Rede Interna ("Single Hosted Bastion Host")

Esta arquitetura é caracterizada pelo fato da máquina onde o Filtro de Conteúdo é instalado, possuir apenas uma única interface de rede, posicionada dentro da rede interna protegida por um firewall.

Nesse caso, é importante que o firewall bloqueie os pacotes HTTP e HTTPS (portas 80 e 443 respectivamente) que não vierem do **Winconnection** para garantir o cumprimento das políticas estabelecidas.

b) Filtro posicionado no "Firewall" de Borda ("Dual Hosted Bastion Host")

O Filtro de Conteúdo é instalado no próprio "firewall", possuindo pelo menos duas interfaces de rede, uma ligada a rede interna e a outra ligada a Internet. Neste caso, o acesso a Internet pode ser implementado via uma ou mais interfaces e provedores.

11.3.2. Regras de "Firewall"

Mesmo instalado na mesma máquina do "firewall", o Filtro de Conteúdo não realiza qualquer alteração nas regras de "firewall" estabelecidas pelo administrador. Desta forma, a implementação das regras que permitam o acesso a Internet pelo filtro, bem como do acesso ao filtro pelos usuários, é de total responsabilidade do administrador.

Três tipos de regras necessitam ser determinadas:

1. Regra de acesso ao filtro pelos usuários;
2. Regra de acesso à interface administrativa;
3. Regra de saída à internet realizada pelo filtro.

Quando o acesso ao filtro pelos usuários é realizado diretamente na rede interna, é muito comum que a regra de acesso seja bastante ampla, permitindo que a administração seja realizada por todas as máquinas da rede interna.

Veja os exemplos de regras para a rede interna:

Rede interna liberada a todos:

```
iptables -A INPUT -i eth0 -j ACCEPT
```

Porta de "proxy" (8080, no exemplo) liberada a parte da rede, e porta de administração WEB (80) liberada a apenas para máquina de IP "192.168.0.17":

```
iptables -A INPUT -i eth0 -p tcp --dport 8080 -s 192.168.0.128/25
```

```
iptables -A INPUT -i eth0 -p tcp --dport 80 -s 192.168.0.17
```

Agora alguns exemplos de regra de saída:

Interface de saída totalmente liberada:

```
iptables -A OUTPUT -o ppp0 -j ACCEPT
```

Saída liberada apenas para os protocolos HTTP e HTTPS, apenas para conexões iniciadas localmente:

```
iptables -A OUTPUT -o ppp0 -p tcp --destination-port 80 -m state --state NEW -
j ACCEPT

iptables -A OUTPUT -o ppp0 -p tcp --destination-port 443 -m state --state NEW
-j ACCEPT
```

Convém observar que o Filtro de Conteúdo não atribui nenhuma porta ao "endpoint local", utilizado na saída. Desta forma, uma vez que a escolha do "enpoint local" é feita de forma aleatória pelo kernel do Linux, para uma conexão efetuada pelo filtro, não é possível estabelecer uma regra de saída baseada na porta de origem.

11.3.3. Translação de Endereços Internos (NAT)

Quando o filtro é posicionado dentro da rede interna, sem acesso direto a rede externa (configurado como "Single Hosted Bastion Host") o "firewall" deve ser configurado de modo a permitir que os pacotes originados pelo filtro sejam adequadamente enviados aos servidores de conteúdo. Como na maioria destas configurações, associa-se a máquina onde o filtro é instalado, endereços privados (RFC-1918), a configuração do "firewall" deverá prover uma regra de NAT que realize a translação dos endereços internos em endereços públicos.

Uma configuração comum é fazer com que somente o filtro possa realizar acessos externos, impedido as demais máquinas o acesso WEB direto. Neste caso, pode-se optar por restringir o acesso das demais máquinas da rede a máquinas externas, via regras de "firewall", ou ainda criar uma regra de translação de Ips (NAT), somente associada a máquina de filtro de conteúdo.

Quando instalado no "firewall" de borda, a configuração da regra de NAT também se faz necessária. A maioria dos frameworks ou assistentes de configuração de "firewall" já providencia a criação da regra de NAT necessária.

11.3.4. Redirecionamento de Pacotes

A configuração do Filtro de Conteúdo como "proxy" transparente depende de uma regra de NAT que transfira o fluxo de rede para o **Winconnection Web Filter para Linux**. Neste caso, uma regra de "iptables" deve redirecionar todos os pacotes WEB a porta de redireção especificada durante a instalação do produto ("Porta de Redir").

Configurado como "proxy" transparente, os usuários terão duas formas de acessar as paginas WEB na Internet, configurando o endereço do "proxy" diretamente no navegador, ou via "proxy" transparente.

É necessário que o **Winconnection Web Filter para Linux** esteja no caminho entre o navegador e a Internet. A maneira mais simples de fazer isto é instalando o Winconnection na mesma máquina onde do "firewall" e que o mesmo seja o roteador padrão da rede interna.

A regra abaixo é um exemplo de regra de redirecionamento de porta para a configuração de "proxy" transparente, para o Winconnection posicionado no gateway padrão de IP 192.168.0.1:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port
9091 --destination ! 192.168.0.1
```

Na regra acima, os pacotes direcionados a porta 80 (http) são direcionados a porta 9091 (porta de redirecionamento padrão do Winconnection). É bastante interessante, notarmos o uso da expressão:

```
--destination ! 192.168.0.1
```

Esta cláusula impede que os pacotes envolvidos na administração do Winconnection sejam direcionados ao "proxy". Se a porta do servidor WEB do Winconnection, usado na administração local, escolhida for diferente de 80, esta cláusula poderá ser omitida.

É perfeitamente possível a configuração de um "proxy transparente", sem que o Winconnection seja instalado no gateway padrão. Neste caso, é necessária o uso de uma configuração mais complicada, empregando regras de "iproute2" e regras "iptables" para marcação de pacotes (-t mangle -j MARK). Basicamente, todos os pacotes WEB são marcados, para que, durante a fase de roteamento, sejam conduzidos a máquina onde o Winconnection foi instalado. Como esta configuração é um tanto incomum e altamente dependente da topologia de rede utilizada, ela não será descrita aqui.

11.3.5. Rotas Múltiplas e "IPROUTE2"

Uma das características principais do **Winconnection Web Filter para Linux** é a habilidade de fazer o balanceamento de carga quando diversos "links" de saída estão disponíveis.

Parte do trabalho de balanceamento é realizado por um conjunto de configurações de "iproute2" criado automaticamente pelo Winconnection. Como esta configuração pode vir a colidir com outras, determinadas pelo administrador de rede, apresentamos aqui um pequeno "guia de convivência" entre o administrador e o Winconnection.

É parte do trabalho do Winconnection descobrir o conjunto de rotas padrão disponível. As rotas são extraídas de diversos lugares, como arquivos de estado de "daemons" e arquivos de configuração de sistema.

Para cada interface que possui rota padrão, uma tabela de roteamento dedicada a esta interface é criada. Para fins de consistência, o id de cada tabela é armazenado no arquivo de configuração posicionado em:

```
/opt/wc65/etc/iproute2/rt_tables
```

O formato deste arquivo é exatamente igual ao utilizado pelo sistema operacional e usado pelos comandos do "iproute2" que é mantido no diretório:

```
/etc/iproute2/rt_tables
```

Esta coincidência não é feita de forma leviana, mas sim para que o administrador possa copiar as definições de um arquivo no outro. Desta forma, a manipulação das tabelas pode ser compartilhada. O Winconnection faz sempre atualização dos ids das tabelas em seu próprio arquivo. Uma vez criados, os ids nunca são alterados. Mesmo que uma interface seja apagada, o seu id é preservado no arquivo de configuração. Veja o exemplo abaixo:

```
[root@wc65-linux ~]# cat /opt/wc65/etc/iproute2/rt_tables

52 rtdev_eth1

53 rtdev_ppp0

54 rtdev_eth2:1
```

Cada tabela de roteamento é preenchida com as rotas necessárias ao funcionamento do balanceador de links. O administrador pode fazer atualizações em qualquer uma das tabelas criadas pelo Winconnection. A menos que as definições de rota criadas pelo administrador colidam, nenhuma rota que não tenha sido criada pelo Winconnection é apagada por ele.

É importante saber que algumas tarefas do sistema operacional podem apagar rotas da tabela. Neste caso, o Winconnection reporá as rotas necessárias, mas não as criadas pelo administrador. É recomendado que as rotas criadas pelo administrador sejam guardadas em arquivos de configuração do sistema operacional. Infelizmente, não há um consenso entre as diversas distribuições Linux, quanto ao posicionamento destas configurações.

O exemplo abaixo mostra a tabela de roteamento construída para a interface "ppp0":

```
[root@wc65-linux ~]# ip route list table rtdev_ppp0

188.16.246.240 dev ppp0 src 188.16.246.240

default via 188.16.246.240 dev ppp0
```

Além das rotas, o Winconnection cria as regras de roteamento (*rules*) que orientam o roteamento de pacotes. As regras estabelecem um tipo de roteamento baseado no IP de origem do pacote. O exemplo abaixo mostra uma tabela alterada pelo Winconnection:

```
[root@wc65-linux ~]# ip rule list

0: from all lookup 255

32764: from 188.16.246.240 lookup rtdev_ppp0

32765: from 188.1.208.60 lookup rtdev_eth1

32766: from all lookup main

32767: from all lookup default
```

Os dois comandos acima só sãos possíveis se as definições do arquivo "/opt/wc65/etc/iproute2/rt_tables" forem copiadas para o arquivo "/etc/iproute2/rt_tables".

Do contrário, os ids digitados deverão estar na sua forma numérica.

11.4. Alguns Comandos Operacionais do Winconnection Web Filter para Linux

Todos os comandos do **Winconnection Web Filter para Linux** encontram-se em:

```
[root@wc65-linux ~]#cd /opt/wc65/bin
```

```
bash          ls       php          redhat.sh  wc65_ctl.bin  xml_restore
iptables      pear     php-cgi      sh         wc65d         xml_restore.bin
linsetup      peardev  php-config   smtpmail   wclog
linsetup.bin  pecl     phpize       wc65_ctl   wcrel
```

11.4.1. Iniciar / Parar / Restart Serviço do Winconnection Web Filter para Linux

```
[root@wc65-linux ~]# service wc65 start

[root@wc65-linux ~]# service wc65 stop

[root@wc65-linux ~]# service wc65 restart
```

11.4.2. Configurando o Winconnection para iniciar automaticamente após um boot

```
[root@wc65-linux ~]# chkconfig wc65 on
```

11.4.3. Restaurar Backup

O comando *"xml_restore"* tem como objetivo realizar a restauração das configurações realizadas anteriormente no **Winconnection Web Filter para Linux**.

O backup será feito automaticamente nas seguintes situações:

- Todas as vezes que o Winconnection Web Filter para Linux for parado/reiniciado, (service wc65 start/stop/restart);
- Todos os dias à meia-noite;

O arquivo de backup será salvo na pasta /opt/wc65/backup.

Para restaurar o backup, execute o procedimento abaixo:

- Pare o Winconnection:

```
[root@wc65-linux bin]# service wc65 stop
```

- Restaure o Backup:

```
[root@wc65-linux bin]#./xml_restore /opt/wc65/backup/wc65-2011-12-23_02-16.xml
```

- Inicie o Winconnection:

```
[root@wc65-linux bin]# service wc65 start
```

11.4.4. Licença

O comando "linsetup" e "wc65_ctl" tem como objetivo adicionar, remover, substituir e visualizar a licença utilizada pelo **Winconnection Web Filter para Linux**.

Acesso ao Assistente de Configuração do **Winconnection Web Filter para Linux**:

```
 [root@wc65-linux bin]# ./linsetup dialog
```

Os comandos utilizando "wc65_ctl" servem para adicionar, remover, substituir e visualizar:

```
[root@wc65-linux bin]# ./wc65_ctl

Options:

- wc65_ctl add_license license -> Adicionar Licença

- wc65_ctl del_license license -> Remover Licença

- wc65_ctl list_license [-l] [-u] [-v]-> Visualizar o produto e a licença

- wc65_ctl change_license oldLicense newLicense -> Alterar a licença
```

12. Glossário

Veja a seguir os principais termos técnicos utilizados nesse manual.

Cache - Local no disco rígido onde se armazenam temporariamente os arquivos transferidos, quando se carrega uma página Web. Ao se retornar para a mesma página, o navegador pode buscá-la no cache, em vez de ir até o servidor original novamente, poupando tempo e reduzindo o tráfego na Internet

---

DHCP - O *Dynamic Host Configuration Protocol* é um protocolo de organização e simplificação da administração de endereços IP de máquinas locais. Em muitos casos um Servidor DNS está embutido no Servidor DHCP para maior simplificação. Ao especificar o endereço IP de um dispositivo de rede em particular, normalmente o dispositivo ligado à Internet, o DHCP usará os valores do DNS associado com aquele dispositivo.

DNS - O *Domain Name System* é um método de nomeação para o endereçamento IP. Por exemplo, www.winco.com.br é um nome de domínio e tem um endereço IP associado. Um Servidor DNS faz a correspondência dos nomes de domínio com um endereço IP. Nós usamos o sistema de nome de domínio (DNS) porque é mais fácil lembrar um nome de domínio do que uma sequência de números.

Endereço IP - O endereço IP é um número único de 32 bits, que identifica o computador em uma rede IP. Um único endereço IP é atribuído a cada computador na Internet. Cada pacote de passagem pela Internet contém a informação, de qual endereço foi enviado (endereço IP de origem) e para qual endereço ele deve ser remetido (endereço IP de destino).

Firewall - Sistema de segurança cujo principal objetivo é filtrar o acesso a uma rede. As empresas utilizam o firewall para proteger suas redes internas conectadas à Internet contra a entrada de usuários não autorizados.

IMAP (Internet Message Access Protocol) - É um protocolo de gerenciamento de e-mail superior em recursos ao POP3 (protocolo que a maioria dos provedores oferece aos seus assinantes). Esse protocolo permite que os clientes de e-mail tenham acesso a e-mails armazenados em um servidor sem ter que baixar e apagá-los (ao contrário do

protocolo *POP3*). Os e-mails sempre ficam no servidor. Isto é protocolo é muito útil quando várias pessoas precisam ter acesso à mesma conta de e-mail.

Interface Externa (Pública) - Uma interface externa ou pública é uma placa de rede que está fisicamente conectada a uma rede pública, como a Internet. A interface externa é configurada com um endereço de IP público.

Interface Interna (Privada) - Uma interface interna ou privada é uma placa de rede que está fisicamente conectada a uma rede interna. A maioria das redes internas estão configuradas com um intervalo de endereços IP de rede privado.

LAN (Rede Local) - Uma rede local (*Local Area Network*) é um grupo de computadores interconectados com a habilidade de compartilhar recursos.

Máscara de rede - A máscara de rede é usada para agrupar endereços IP. Há um grupo de endereços atribuídos a cada segmento de rede. Por exemplo, a máscara 255.255.255.0 agrupa um conjunto de 254 endereços IP. Se tivermos, por exemplo, uma sub-rede 192.168.0.xxx com máscara 255.255.255.0, os endereços que poderemos atribuir aos computadores na sub-rede serão de 192.198.0.1 até 192.168.0.254.

NAT - Com o NAT - *Network Address Translator* - você pode conectar-se à Internet por meio de um único endereço IP e os computadores dentro da rede usarão a Internet como se estivessem conectados a ele diretamente (certas limitações se aplicam).

A conexão de uma rede inteira com o uso de um único endereço IP é possível uma vez que o módulo do NAT reescreve o endereço de origem nos pacotes enviados, dos computadores na rede local, com o endereço do computador no qual o WinRoute está sendo executado.

O NAT diferencia-se significativamente de vários servidores proxy e gateways de nível de aplicação pois esses, em princípio, nunca estariam aptos a suportar tantos protocolos como o NAT.

POP3 (Post Office Protocol) - Protocolo usado por programas de correio eletrônico para o recebimento de correspondência.

Proxy (Servidor) - O proxy serve como um intermediário entre os PCs de uma rede e a Internet. Um servidor proxy pode ser usado com basicamente três objetivos: 1- Compartilhar a conexão com a Internet quando existe apenas um IP disponível (o proxy é o único realmente conectado à Web, os outros PCs acessam através dele). 2- Melhorar o desempenho do acesso através de um cache de páginas; o proxy armazena as páginas e arquivos mais acessados, quando alguém solicitar uma das páginas já armazenadas do cache, esta será automaticamente transmitida, sem necessidade de baixá-la novamente. 3- Bloquear acesso a determinadas páginas (pornográficas, etc.), como tipo passa pelo proxy é fácil implantar uma lista de endereços ou palavras que devem ser bloqueadas, para evitar por exemplo que os funcionários percam tempo em sites pornográficos em horário de trabalho.

Hoje em dia os servidores proxy são extremamente comuns, mesmo em redes domésticas, não é necessário um PC dedicado a esta função, basta instalar um dos vários programas de servidor proxy disponíveis no PC com a conexão à Internet.

Round-Robin: Algoritmo de escalonamento usado em projetos de sistemas operacionais multitarefa.

SMTP (Simple Mail Transfer Protocol) - É o protocolo utilizado para enviar mensagens de correio eletrônico.

SSL (Secure Socket Layer) - É um padrão de segurança utilizado para criar uma conexão criptografada entre o navegador do usuário e a internet. É usado principalmente para o envio de dados sigilosos, como informações de cartão de crédito ou senhas. Certificados de servidor web são necessários para criar uma conexão SSL segura.

VPN (Virtual Private Network) - A VPN envolve múltiplas redes locais com a habilidade de compartilhar recursos através da Internet ao criar um túnel direto que faz a criptografia e a descodificação em ambas as extremidades.

---

13. Apêndices

13.1. Programação e Extensibilidade

O **Winconnection 6** possui uma inovadora ferramenta que permite estender a funcionalidade do programa com uma simples API (*Application Programming Interface*) para a linguagem PHP.

A API é composta por uma função de *call back* chamada **onDispatch** e um *toolset*. O script *onDispatch* é chamado antes de se aplicarem as regras de roteamento.

13.1.1. Interface onDispatch

Ao fazer a entrega de uma mensagem (*onDispatch*), o **Winconection 6** executará o script PHP, e só então passará para a execução dos filtros originais do programa (filtros globais e por grupo).

A **Interface onDispatch** possibilita:

- Alterar parte ou inteiramente a lista de destinatários de uma mensagem.
- Incluir ou alterar *headers* da mensagem.
- Apagar a mensagem da fila.
- Alterar a pontuação do detector de SPAM.
- Fazer com que uma mensagem não passe pelos filtros do programa.
- Criar e-mails.

Para utilizar a interface *onDispatch*, basta criar a função *onDispatch*() no arquivo '**on_mail_message.php**', que deverá ser criado no diretório *C:\Arquivos de programas\Winco\Winconnection6\Scritps.*

O usuário pode habilitar a interface onDispatch em *Serviços de E-mail → Guia Configurações* e marcando a opção '*Habilitar PHP Interface*'.

13.1.2. Toolkit do Winconnection 6

Para que seja possível utilizar a *Interface onDispatch*, o **Winconnection 6** possui um *toolset* de funções que devem ser utilizadas pelo usuário na criação dos scripts.

Antes de analisarmos o *toolset* de funções do **Winconnection 6**, vamos primeiramente analisar a sintaxe da função *OnDispatch*:

- A função principal é a **function onDispatch($id)**, onde o **$id** é o id da mensagem que é passado para a função automaticamente pelo programa.

```
function OnDispatch($id) {
}
```

- O usuário pode declarar todas as funcionalidades que desejar dentro da função principal, ou pode declarar novas funções e chamá-las dentro da função principal:

```
function OnDispatch($id) {
    $rc = wc_ms_addrecipient($id, "usuario@dominio.com.br");
    $rc = wc_ms_setspamscore($id, 100);
    return 0;
}
```

Ou:

```
function addRecipiente($id) {
    $rc = wc_ms_addrecipient($id, "usuario@dominio.com.br");
    return $rc;
}
function changeSpamScore($id) {
    $rc = wc_ms_setspamscore($id, 100);
    return $rc;
}
function OnDispatch($id) {
    $rc = addRecipiente($id);
    if($rc != 0)
        wc_ms_log($id, 2, "Erro adicionando recipiente");
    $rc = changeSpamScore($id);
    if($rc != 0)
        wc_ms_log($id, 2, "Erro alterando spam score");
    return 0;
}
```

Analisaremos agora o *"toolset"* de funções:

a) Mail Utility

- **wc_ms_getmessagefile($id)** – obtém o nome do arquivo da mensagem.
- **wc_ms_discard($id) –** descarta a mensagem.

- **wc_ms_log($id, $severity, $message) –** grava mensagem no log.

$severity: **0** – informação (mensagem azul no log);

1 – aviso (mensagem dourada no log);

2 – erro (mensagem vermelha no log);

- **wc_ms_skipstdrouting($id) –** aponta a mensagem para não passar pelos filtros do programa.

b) SPAM Score

- **wc_ms_getspamscore($id)** – obtém o spam score da mensagem.
- **wc_ms_setspamscore($id, $score) –** modifica o *spam score* da mensagem.

c) Gerenciamento de Recipientes

- **wc_ms_getnumrecipients($id)** – obtém o número de recipientes da mensagem.
- **wc_ms_getorgrecipient($id, $i) –** obtém o recipiente original da mensagem.
- **wc_ms_getrecipient($id, $i) –** obtém um recipiente específico da mensagem.
- **wc_ms_deleteallrecipients($id) –** deleta todos os recipientes da mensagem.
- **wc_ms_addrecipient($id, $recipient) -** adiciona recipiente à mensagem.

d) Gerenciamento de Header:

- **wc_ms_getheader($id, $headerKey)** – obtém determinado header.

  Por exemplo: wc_ms_getheader($id, "subject");

- **wc_ms_setheader($id, $headerKey, $headerValue) –** altera determinado header

  Por exemplo: wc_ms_setheader($id, "subject", "SPAM");

- **wc_ms_addheader($id, $headerKey, $headerValue) –** adiciona determinado header

Por exemplo: wc_ms_addheader($id, "from", "usuario@dominio.com.br");

e) Criação de E-mail:

- **wc_ms_CreateMessage($from)** – inicia criação de e-mail cujo remetente é $from. Retorna um $id que deverá ser usado nas funções abaixo.
- **wc_ms_AddLineToMessage($id, $line) –** adiciona linha ao e-mail que está sendo criado.

  Por exemplo: "Subject: Teste"
- **wc_ms_AddRecipientToMessage($id, $recipient) –** adiciona recipiente ao e-mail que está sendo criado.
- **wc_ms_SubmitMessage($id) –** envia o e-mail que foi criado.
- **wc_ms_DiscardMessage($id) –** descarta o e-mail que foi criado

13.1. 3. Exemplo de programa

Para exemplificar a criação de um script PHP para ser utilizado na **interface onDispatch,** elaboramos um exemplo cuja função é descartar a mensagem se o spam score for maior que 80 e gravar uma mensagem no log do programa.

Segue o exemplo a seguir:

```
<?
function OnDispatch($id)
{
    $score = wc_ms_getspamscore($id); // obtém spam score da mensagem
    if ($score > 80) {
        wc_ms_log($id, 1, "Descartando a mensagem"); // grava mensagem no log
        $rc = wc_ms_discard($id); // descarta a mensagem
    }
    return 0;
}
?>
```

A função acima é um exemplo muito simples da utilização do *'toolset'* de funções do **Winconnection 6**.

13.2. Configuração Anti-Spam – Função dos Perfis

Na configuração *Anti-Spam* do **Winconection 6**, o administrador poderá escolher o perfil que melhor se adaptar às necessidades de sua empresa.

Cada perfil tem interferência direta no uso e funcionamento do **SpamCatcher** e de acordo com o perfil escolhido, o administrador poderá personalizar algumas configurações.

Veja na tabela abaixo as opções de configurações disponíveis:

Nome da Opção	Descrição	Observação
Blacklist de domínios	Esta opção permite especificar os domínios que devem ser sempre bloqueados.	
Charset bloqueados	Bloqueio de conteúdos que contenham um determinado conjunto de caracteres internacionais. Assim, pode-se eliminar e-mails que contenham mensagens codificadas em chinês ou em russo.	Uma lista de conjuntos de caracteres internacionais pode ser encontrada em: http://www.w3.org/International/
Habilitar SPF	Esta opção permite habilitar a verificação SPF.	SPF (Sender Policy Framework) é um sistema que evita que outros domínios enviem emails não autorizados em nome de um domínio. O SPF verifica no cabeçalho se o SMTP utilizado para enviar a mensagem, está autorizado na relação de IP's que respondem pelo domínio do remetente. Também informa se o domínio autoriza ou não que outros IP's fora desta relação enviem emails em seu nome.
Lista Blackhole Skip	Lista de IPs que não serão avaliados pelas LBLs (last blackhole lists).	
Lista de domínios ignorados	Esta opção permite especificar corpo de domínios e IPs que devem sempre ser excluídos das verificações DNSBL e MSBL e devem ser ignorados.	
Lista de IPs bloqueados	Esta opção permite especificar os IPs que devem ser bloqueados.	
Lista de IPs ignorados	Esta opção permite especificar IPs que devem ser ignorados na verificação RBL.	

Lista de Língua de Origem	Esta opção permite que você defina quais línguas são preferidas nas suas mensagens de e-mail.	As línguas devem ser especificadas com duas letras (ISO 639).
Lista de remetentes spoofed	Consiste em uma lista contendo e-mails, servidores (faixa de IPs) e pontuação. Assim, um e-mail cujo remetente esteja cadastrado na lista e tenha sido emitido pelo servidor listado, terá sua pontuação crescida do valor também especificado na lista. Isto pode ajudar a eliminar mensagens cujos remetentes de e-mails sejam usuários que tenham sido inescrupulosamente capturados por spamners. Um ataque muito comum, é o envio de e-mails por spammers utilizando-se de remetentes que realmente existem, ou sejam conhecidos, pela infraestrutura alvo. Sabendo-se que alguns remetentes fazem uso de determinados servidores fixos, esta lista pode ajudar na detecção de mensagens maliciosas utilizando-se destes remetentes.	
Lista de usuários SPAMBAIT	Lista de destinatários inválidos ("BAIT" -> isca em inglês) que são usados para identificar SPAMs. Estes usuários não devem existir ou sequer terem sido cadastrados um dia, de modo que a existência de uma mensagem para eles determine que a mesma seja pontuada como SPAM.	Os endereços devem ser especificados exatamente como são. *Wildcard* (coringas) não são suportados.
Países bloqueados	Permite realizar o bloqueio de e-mails por país. Por exemplo, se você deseja bloquear os endereços de e-mail do campo "De" que terminam com .ru, você pode utilizar essa lista de bloqueio.	Os países devem ser especificados com duas letras (ISO 3166).
Países de origem	Esta opção permite especificar uma lista de países que são considerados como países de "origem". As mensagens encaminhadas através de um país que não está nesta lista serão pontuadas mais agressivamente. Se esta opção estiver vazia, então nenhuma penalidade ocorrerá.	Os países devem ser especificados com duas letras (ISO 3166).
Regras Customizadas	Esta opção permite definir uma lista de regras customatizadas (e.x. Spam, phishing ou palavras/frases).	Consulte Regras Customatizadas para mais informações.

Servidor Livefeed	São os servidores da Mailshell responsáveis pela pontuação de IPs e domínios. O seu funcionamento tem como base a mesma tecnologia usada em servidores DNS para resolução de nomes.	
Usuários não existentes	Endereços inexistentes não devem ser publicados ou apresentados em lugar algum. Portanto, não e-mail legítimo será enviado para esses endereços.	Os endereços devem ser especificados exatamente como são. *Wildcard* (coringas) não são suportados.
Whitelist de domínios	Esta opção permite especificar os domínios que devem ser sempre aprovados.	
Whitelist de IPs	Esta opção permite especificar os endereços IPs que devem ser sempre aprovados.	

Os seguintes perfis estão disponíveis na configuração da guia *Anti-Spam* do **Winconection 6**:

- **Mais Rápido:** Este perfil disponibiliza uma avaliação mais rápida, priorizando a velocidade de entrega do e-mail.

  Para esse perfil, as seguintes configurações estão disponíveis: *Usuários não existentes, Whitelist de IPs, Whitelist de domínios, Charset´s bloqueados, Blacklist de domínios, Lista de IPs bloqueados, Países de origem, Países bloqueados, Regras customatizadas, Lista de domínios ignorados, Lista de IPs ignorados, Lista Blackhole Skip, Lista de usuários SPAMBAIT.*

- **Menos CPU:** Este perfil disponibiliza um menor consumo de CPU.

  Para esse perfil, as seguintes configurações estão disponíveis: *Whitelist de IPs*, *Whitelist de domínios, Charset´s bloqueados, Blacklist de domínios, Países bloqueados, Regras customatizadas, Países de Origem, Lista de domínios ignorados, Lista de IPs ignorados, Lista Blackhole Skip, Lista de Usuários não existentes, Língua de origem, Lista de remetentes spoofed, Lista de usuários SPAMBAIT.*

- **Menos espaço em Disco:** Este perfil disponibiliza um menor consumo de disco.

Para este perfil, as seguintes configurações estão disponíveis: *Habilitar SPF, Servidor Livefeed, Whitelist de IPs, Whitelist de domínios, Charset´s bloqueados, Blacklist de domínios, Países bloqueados, Lista de IPs bloqueados, Países de origem, Língua de origem, Lista de domínios ignorados, Lista de IPs ignorados, Lista Blackhole Skip, Lista de remetentes spoodfed, Lista de usuários não existentes, Lista de usuários SPAMBAIT.*

- **Menos Memória:** Este perfil disponibiliza um menor consumo de memória.

  Para este perfil, as seguintes configurações *estão disponíveis: Habilitar SPF, Livefeed Server.*

- **Menos uso de Rede:** Este perfil disponibiliza um menor consumo de banda de rede.

  Para este perfil, as seguintes configurações estão disponíveis: *Whitelist de domínios, Whitelist de IPs, Charset´s bloqueados, Países bloqueados, Blacklist de domínios, Lista de IPs bloqueados, Regras customizadas, Países de origem, Lista de línguas de origem, Lista de domínios ignorados, Lista de IPs ignorados, Lista de usuários não existentes, Lista de usuários SPAMBAIT, Lista Blackhole Skip, Lista de usuários spoofed, Habilitar SPF.*

- **Mais acurado:** Este perfil disponibiliza menores probabilidades de falsos positivos e negativos.

  Para etse perfil, as seguintes configurações estão disponíveis: *Whitelist de domínios, Whitelist de IPs, Charset´s bloqueados, Países bloqueados, Blacklist de domínios, Lista de IPs bloqueados, Regras customizadas, Países de origem, Lista de línguas de origem, Lista de domínios ignorados, Lista de IPs ignorados, Lista Blackhole Skip, Lista de usuários não existentes, Lista de usuários SPAMBAIT, Lista de usuários spoofed, Habilitar SPF.*

- **Mais Seguro:** Este é o perfil mais conservador e seguro, reduzindo a probabilidade de falsos negativos.

  Para este perfil, as seguintes configurações *estão disponíveis: Habilitar SPF, Habilitar Whitelist.*

- **Servidor:** Este perfil é indicado para servidores de e-mail e *Mail Gateways*.

  Para este perfil, as seguintes configurações estão disponíveis*: Whitelist de domínios, Whitelist de IPs, Charset´s bloqueados, Países bloqueados, Blacklist*

de domínios, Lista de IPs bloqueados, Regras customizadas, Países de origem, Lista de línguas de origem, Lista de domínios ignorados, Lista de IPs ignorados, Lista Blackhole Skip, Lista de usuários SPAMBAIT, Lista de usuários spoofed, Habilitar SPF.

13.2. Regras Customatizadas

Para utilizar a opção **Regras Customatizadas**, é necessário criar um ou mais arquivos de regras customatizadas no diretório de configuração: *C:\Arquivos de programas\Winco\Winconnection6\spamconf*.

As regras customatizadas se aplicam ao campo *Assunto*, *Corpo* e *Anexos.*

A lista de regras customatizadas é especificada em uma lista com os nomes dos arquivos separados por vírgula. Por exemplo:

custom_rules_list=filename1, filename2

Outro exemplo:

custom_rules_list=spam_phrases.csv,phish_phrases.csv

Os arquivos de regras customatizadas contêm frases no seguinte formato em linhas separadas*:*

phrase,type,confidence,caseSensitivity

- ***phrase*** → pode ser qualquer texto, exceto vírgulas. Qualquer vírgula na frase deve ser excluída*.*
- ***type*** → pode ser *SPAM, PHISH,* ou *BOUNCE.* Se qualquer outro além destes forem especificados, o *TYPE* é automaticamente assumido como *SPAM.* Este campo é *case insensitive.*
- ***Confidence*** → pode ser de *1* até *100. Se o type é SPAM,* então 100 indica com uma maior convicção de spamminess*.* Se o *type* é *PHISH,* então 100 indica uma maior convicção de phishiness*.* Se o *type* é *BOUNCE,* então 100 indica uma maior convicção que a frase está relacionada a um bounces.

- ***CaseSensitivity*** → valor *1* significa que a frase será em *case sensitive; 0* significa que a frase será em *case insensitive.*

Por exemplo:

spamming is fun,SPAM,100,0
phishing is Phun, PHISH,90,1
return to sender,BOUNCE,80,0

A primeira linha significa que todas as variações de "spamming is fun" são consideradas SPAM com convicção de 100. A frase não está em case sensitive.

A segunda linha significa que todas as variações de "phishing is phun" são consideradas como PHISH com convicação de 90. A frase está em case sensitive.

A terceira linha significa que todas as variações de "return to sender" são consideradas como BOUNCE com convicção de 80. A frase não está em case sensitive.

www.winco.com.br