Este manual do usuário oferece uma documentação para as principais configurações do **Winconnection 7**.

O **Winconnection 7** é um Gateway 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.

Veja a seguir os principais benefícios oferecidos pelo produto:

Os benefícios estão disponíveis de acordo com a versão adquirida.

Clique aqui e compare as versões do Winconnection.

Controle flexível do acesso à internet

Controlar o acesso de forma simples e eficiente é uma das principais características do **Winconnection 7**. Ao utilizá-lo, sua empresa tem a liberdade para determinar o tempo máximo diário de navegação conforme o perfil de cada colaborador ou grupo de colaboradores. O programa permite bloquear sites por conteúdo e URLs oferecendo flexibilidade para permitir ou bloquear acessos para fins pessoais, inclusive redes sociais.
Existem estudos que defendem a permissão, com certos limites, às redes sociais durante o expediente, em nosso blog você pode ler o artigo – "Acesso às redes sociais dentro das corporações: proibir ou liberar?".

Controle de Skype e MSN

Para restringir o uso do Skype e do MSN apenas às atividades profissionais, pode ser definida uma lista de contatos permitidos ou de contatos bloqueados. Essa filtragem seletiva garante os benefícios destas ferramentas de comunicação sem o problema do seu uso indiscriminado. Com o sistema é possível permitir, por exemplo, o uso do Skype e MSN somente entre os funcionários da empresa e parceiros ou fornecedores, ou mesmo bloquear totalmente o uso de instant messaging, quando for o caso.

Controle de Programas que acessam a internet

O **Winconnection 7** permite definir os programas autorizados ou proibidos de acessar à internet. Assim eventuais malwares não conseguem acessar a internet, tornando os seus riscos bem menores. Também evita a utilização de programas que estejam em desacordo com a política da empresa.

Bloqueio de Ultrasurf , Tor e outros sistemas de navegação anônima

Com o **Winconnection 7** em sua empresa os usuários da rede não conseguirão burlar as regras de acesso à internet, mesmo que usem programas de navegação anônima, tais como Ultrasurf ou Tor. Isso é possível graças a uma tecnologia exclusiva que integra o Firewall, o filtro de acesso à internet e o bloqueio de certificados inválidos. Através deste recurso você pode bloquear também Skype, MSN, sistemas de Torrent e outras aplicações TCP/IP.

Proteja-se dos hackers

O Firewall do **Winconnection 7** mantém a segurança da sua rede de computadores. O sistema é inteligente, configurando-se automaticamente à medida que os serviços são ativados e desativados. De acordo com os aspectos específicos de sua rede, é possível fazer ajustes e determinar o bloqueio a tipos de protocolo, o que confere grande flexibilidade à solução. Complementando o Firewall, o sistema de prevenção de intrusão (IPS) detecta tentativas de ataques, tais como port scan, quebra de senha por força bruta e injeção de código malicioso, bloqueando imediatamente o endereço IP de onde se origina o ataque.

Mais conectividade

A importância da internet no dia-a-dia das empresas muitas vezes exige a disponibilização de mais de uma conexão para o caso de falha em uma delas. Com o **Winconnection 7** você utiliza todas as conexões com balanceamento de carga entre as conexões disponíveis. Esta característica é diferente dos processos usuais de tolerância a falhas baseados em substituição de conexões com falhas por conexões em funcionamento ("hot-stand-by"). A principal vantagem é o aproveitamento maior de todos os recursos que estiverem funcionando, mantendo-os em atividade o máximo de tempo possível.

Controle de Banda – QoS

Permite controlar o uso das conexões limitando ou dando prioridade a determinados usuários ou serviços.

Segurança para acessos remotos e comunicação entre filiais

Os colaboradores da sua empresa, estejam onde estiverem, podem fazer conexões remotas com a rede interna através de uma conexão segura criptografada (VPN-SSL). Ao proporcionar mobilidade a seus funcionários este recurso contribui para o aumento da produtividade.
A solução de VPN do **Winconnection 7** permite ainda a interligação entre os diversos escritórios da empresa, utilizando os mesmos links de internet já existentes. Dessa forma é possível criar facilmente uma rede de comunicação privada e segura envolvendo as filiais (ou lojas) e a matriz.

Acesse seus e-mails de qualquer lugar

Com o serviço IMAP você tem acesso a todos os seus e-mails, inclusive os lidos, de qualquer lugar. Além disso, com o servidor de e-mail do **Winconnection 7** você pode gerenciar os e-mails de forma simples e segura, por intermédio de uma conexão SSL.
O acesso pode ser feito através do seu cliente de e-mail preferido (Outlook, Thunderbird e outros) ou através do Webmail com versões desktop ou mobile.

Relatórios de acesso à internet e monitoramento em tempo real

O **Winconnection 7** fornece relatórios completos do acesso à internet, seja por usuário, domínio ou tempo de navegação. Assim, você terá material para avaliar as politicas de acesso e gerenciá-la com base nos dados. Os relatórios podem ser exportados em formato PDF ou CSV.

Monitoramento com Alarmes

Permite o envio de mensagem de e-mail ou a execução de algum programa definido pelo administrador no caso de problemas nas conexões de internet, ataques de hackers,consumo de banda e problemas na fila de e-mail.

ÍNDICE

11.1 Programação e Extensibilidade
11.2 Configuração Anti-Spam – Função dos Perfis

1 Recursos

** Os recursos estão disponíveis de acordo com a versão adquirida.*

Clique aqui e compare as versões do Winconnection.

Sistema de Prevenção de Intrusão – IPS

- Detecta e bloqueia ataques de quebra de senha por tentativa e erro
- Detecta e bloqueia port scan (varredura de portas)
- Detecta e bloqueia injeção de código malicioso

Saiba Mais

Filtro Web

- Classificação automática dos sites
- Controle de internet
- Limite de navegação por tempo
- Bloqueio de Ultrasurf e Tor
- Bloqueio de certificados inválidos
- Filtro de URL (com whitelist e blacklist)
- Regras de acessos avançadas por grupo, usuário ou endereço IP
- Cache
- Tela de verificação de horas navegadas por usuário
- Proxy transparente
- Relatórios de acesso por usuário, domínios, horário de acesso e total/dia

Saiba Mais

E-mail

- Servidor IMAP
- Filtro de Mensagens
- Antispam
- Protocolos SMTP, POP e IMAP
- Controle de quota por usuário
- Opção de SSL para os protocolos acima
- Mapeador POP – acessa periodicamente caixas postais externas – num provedor, por exemplo – e as move para o servidor local
- Backup automático configurável
- Assinaturas automáticas
- Gerenciamento de listas
- Mensagens de ausência (férias) definidas por usuário
- Webmail mobile e para desktop
- API de programação em PHP para e-mails recebidos
- Relatórios de uso
- Rastreamento de mensagens
- Regras globais e por usuários para redirecionar, copiar, apagar e responder mensagens
- Múltiplos domínios com possibilidade de definir relays diferentes por domínio

Saiba Mais

Firewall

- Múltiplas conexões à internet com balanceamento de carga
- QoS – permite dar prioridade ou garantia de banda a usuários ou serviços
- Bloqueio por protocolo e porta
- Configuraçao automática (firewall inteligente)
- Nat direto e reverso
- Relatórios de utilização dos links
- Whitelist/Blacklist de programas que podem acessar a internet

Saiba Mais

Gerenciamento

- Administração via Web com painel de controle para o usuário
- Gerenciamento Centralizado de Filiais
- Relatórios integrados
- Integração com MS Active Directory
- Visualização de conexões ativas
- Possibilidade de vincular usuário a endereço IP ou MAC
- Tela de logoff
- Possibilidade de excluir alguns usuários dos logs (ex: diretoria)
- Auto update

- Monitoramento de falhas com alarmes por e-mail ou execução de algum programa pré-definido

Saiba Mais

VPN-SSL

- Topologia PC-Rede ou Rede-Rede
- Compatível com qualquer firewall
- Fácil instalação
- Acesso bidirecional
- Qualquer tipo de tráfego: acesso a servidores e impressoras remotas, desktops, câmeras,etc

Saiba Mais

Filtro de Skype e MSN

- Controle da lista de contatos
- Monitoramento de conversas em tempo real (só chat)
- Gravação do histórico de todas as mensagens enviadas e recebidas (só chat)
- Controle de envio e recebimento de arquivos entre os usuários (só para MSN)
- Pesquisa de mensagens por palavras contidas na conversa (só chat)
- Estatísticas de uso
- Suporte a banco de dados externos para logs e relatórios
- Relatórios com estatísticas de uso

Saiba Mais

Outros recursos

- Servidor Web com PHP
- Servidor FTP e FTPS
- DHCP
- DNS CACHE
- Winco Messenger
- DDNS client

Saiba Mais

2 Instalação

Requisitos:

Sistema Operacional Windows

- Windows XP Home Edition
- Windows XP Professional SP2
- Windows Server 2003 SP2
- Windows Server 2008
- Windows Vista Business
- Windows Vista Ultimate
- Windows 7
- Windows 8
- Windows Server 2012

Hardware

Requisitos Minímos sem o Servidor de E-mails do Winconnection:

- Processador x86 ou x64 de 1GHz
- 1 GB RAM Disponível para o Winconnection
- Espaço em disco: 120GB livres, disponíveis para o Winconnection.

Requisitos Minímos com o Servidor de E-mails do Winconnection:

- Processador x86 ou x64 de 1GHz
- 2 GB RAM Disponíveis para o Winconnection
- Espaço em disco: 120GB livres Disponíveis para o Winconnection.

2.1 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 7**:

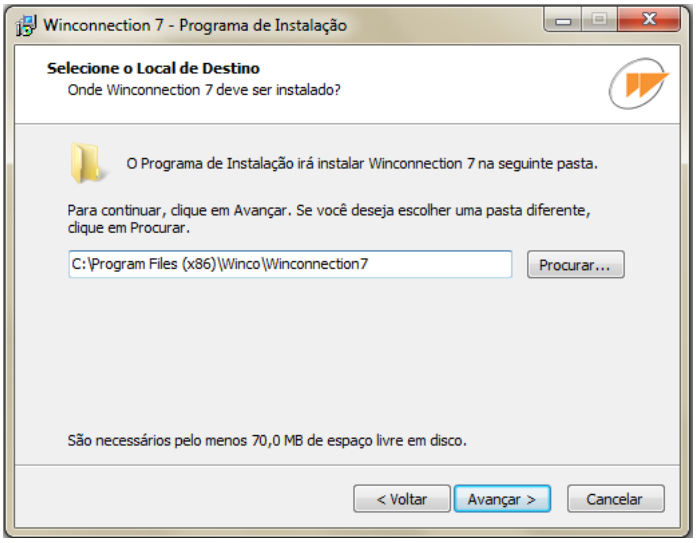
- O computador onde será instalado o **Winconnection 7** deve estar funcionando normalmente, conectado à internet e com todas as funções de navegação, recebimento de e-mail, etc., em perfeito estado.
- O computador onde será instalado o **Winconnection 7** deve ter no minímo 2 placas de rede no Servidor: uma para a Rede Interna (LAN) e outra para Rede Externa (internet).
- É necessário sempre fazer o login no servidor como Administrador do Windows ou do Active Directory.
- 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 da rede que irá fazer a instalação deve possuir uma ideia clara dos serviços que irá usar no **Winconnection 7** e por qual motivo quer usar o produto.
- O administrador da rede deve conhecer todos os logins dos e-mails que serão cadastrados.

2.2 Instalação

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 instalador irá ajudará a descompactar o arquivo e criar as pastas do **Winconnection 7**. 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 7*.



Após finalizar a instalação, o **Winconnection 7** 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 todas as etapas forem concluídas, o **Winconnection 7** será inicializado e estará pronto para ser usado.

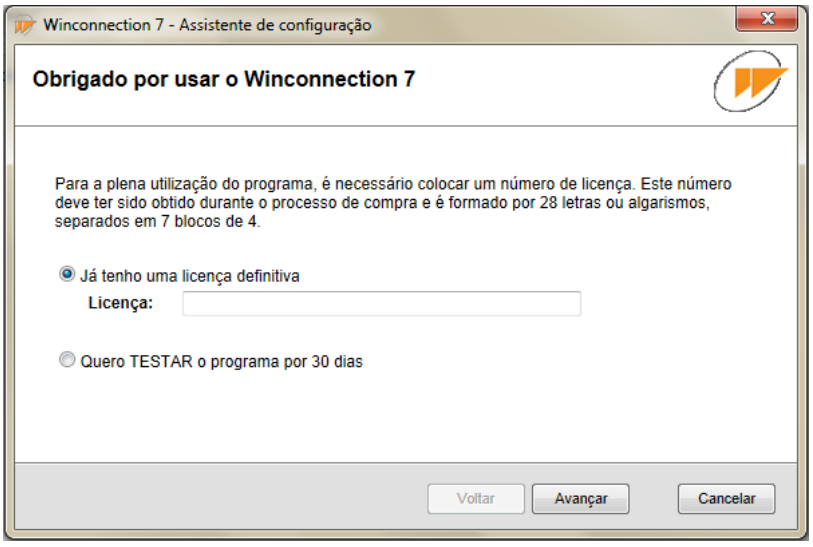
2.3 Assistente de Configuração

O *Assistente de Configuração* é iniciado logo após o término da instalação e realiza o processo de pré-configuração do **Winconnection 7**.

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

Licenciamento:

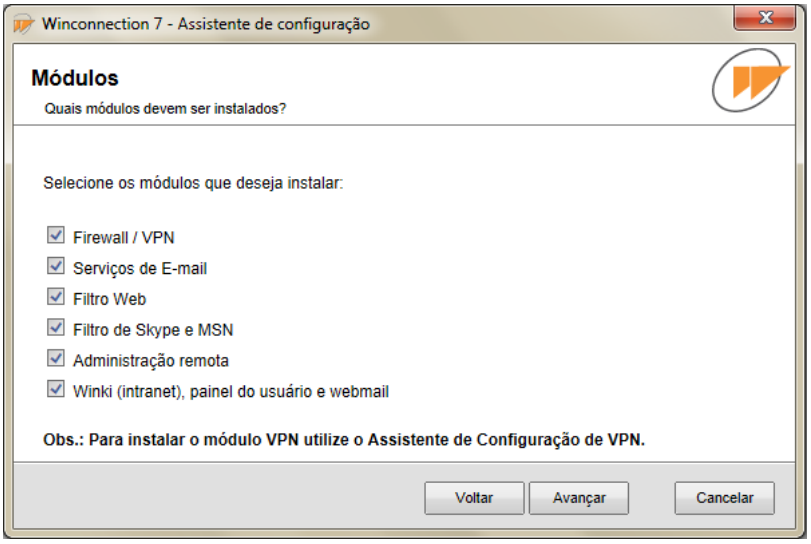
A primeira tela do assistente é a de licenciamento.



Digite o seu número de licença ou selecione a opção para testar o programa por 30 dias. Clique no botão *Avançar*.

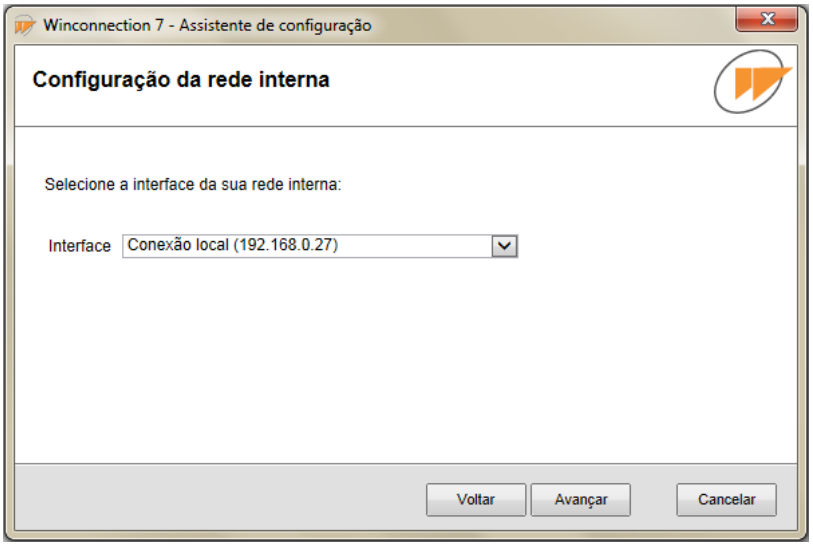
Módulos

Nesta etapa, selecione os módulos que devem ser instalados.



Configuração da rede interna

A configuração desta etapa garante o funcionamento correto do **Winconnection 7** e a proteção da rede contra acessos não autorizados.

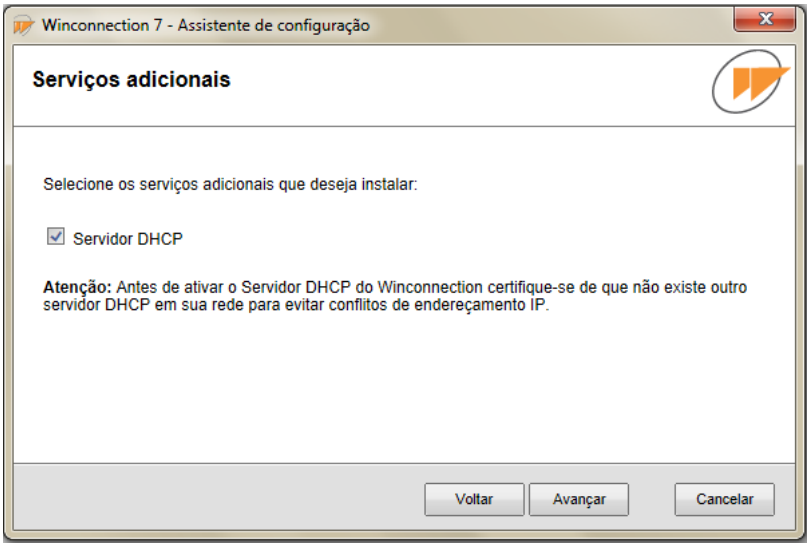


Informe a interface da sua rede interna e clique no botão *Avançar*.

Serviços Adicionais

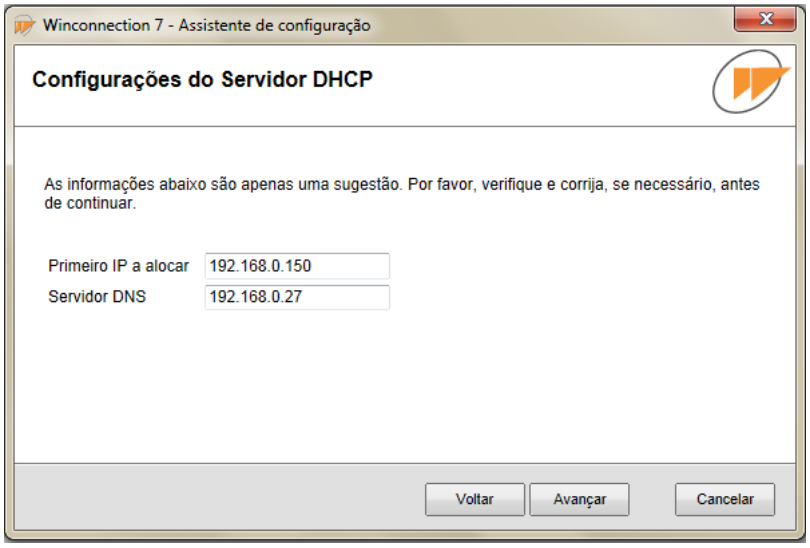
Caso deseja usar o Servidor DHCP do Winconnection, habilite essa opção e clique em *Avançar*.

Atenção: Antes de ativar este serviço, certifique-se de que não existe outro servidor DHCP em sua rede para evitar conflitos de endereçamento IP.



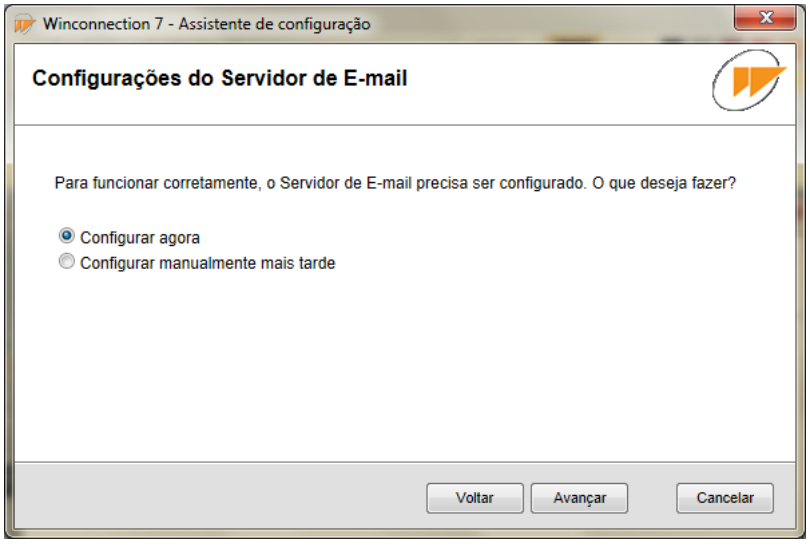
Configurações do Servidor DHCP:

Nesta etapa, informe o endereço IP que será alocado e o Servidor DNS.



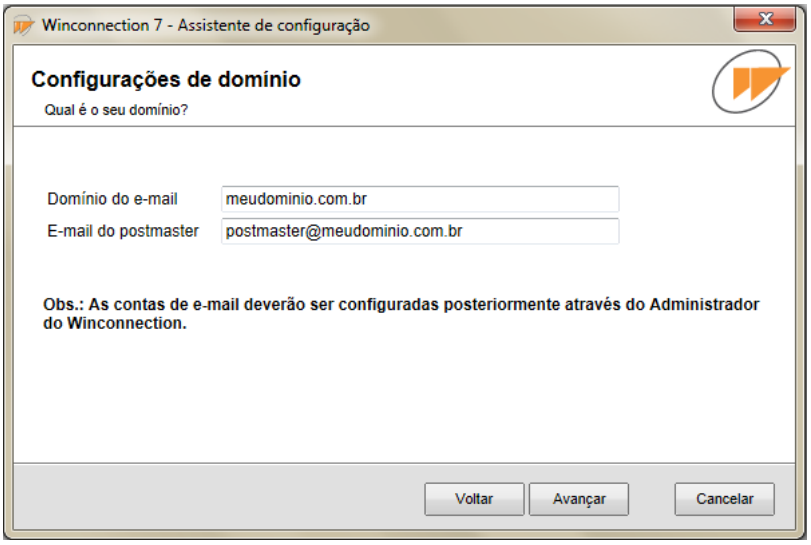
Configurações do Servidor de E-mail

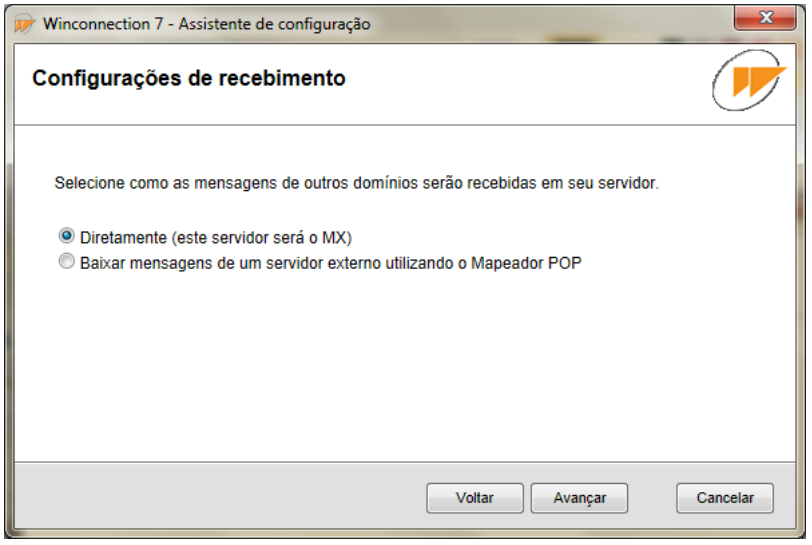
Para funcionar corretamente, o Servidor de E-mail precisa ser configurado. Nesta etapa, você pode definir se a configuração será feita agora ou se será feita manualmente mais tarde.

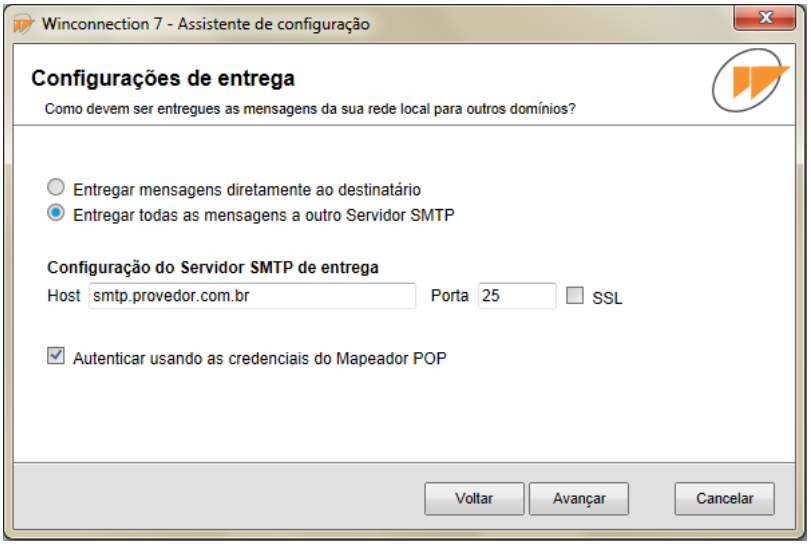


Se a opção *Configurar agora* for selecionada, as próximas etapas serão destinadas para a configuração do Servidor de E-mail.

Para descrições detalhadas destas configurações, consulte os tópicos dos serviços de e-mail deste manual (*Serviços -> E-mail*).

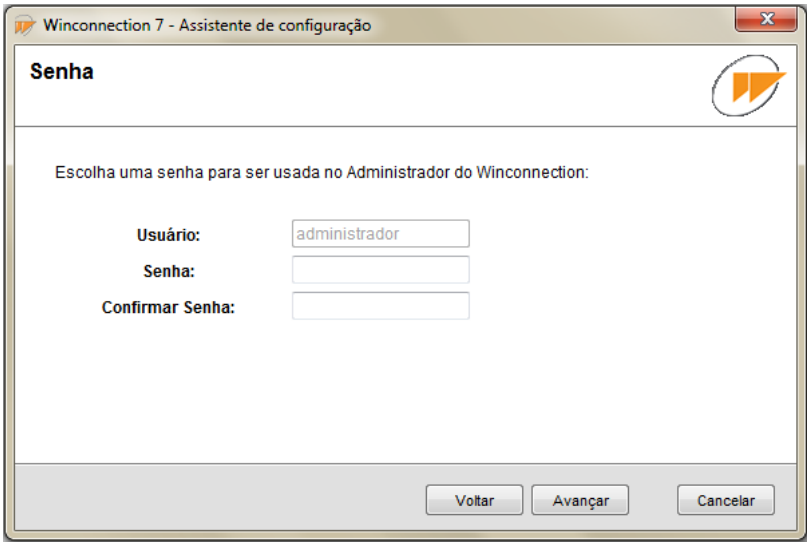






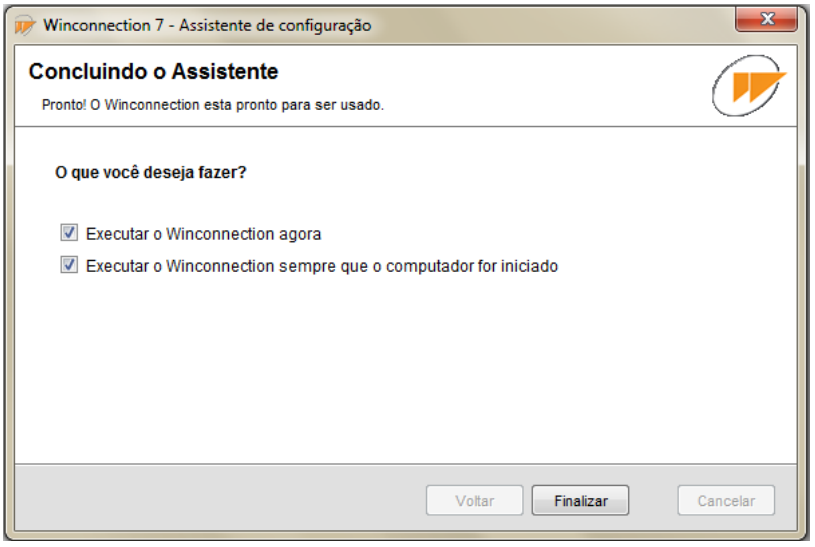
Senha:

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



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 7** e configurar as demais funcionalidades do produto. Todas elas estão descritas neste manual.

3 Administrador

O *Administrador* é o aplicativo que faz o gerenciamento do **Winconnection 7**.

Com o *Administrador Web* é possível gerenciar as configurações do **Winconnection 7** a partir de qualquer máquina.

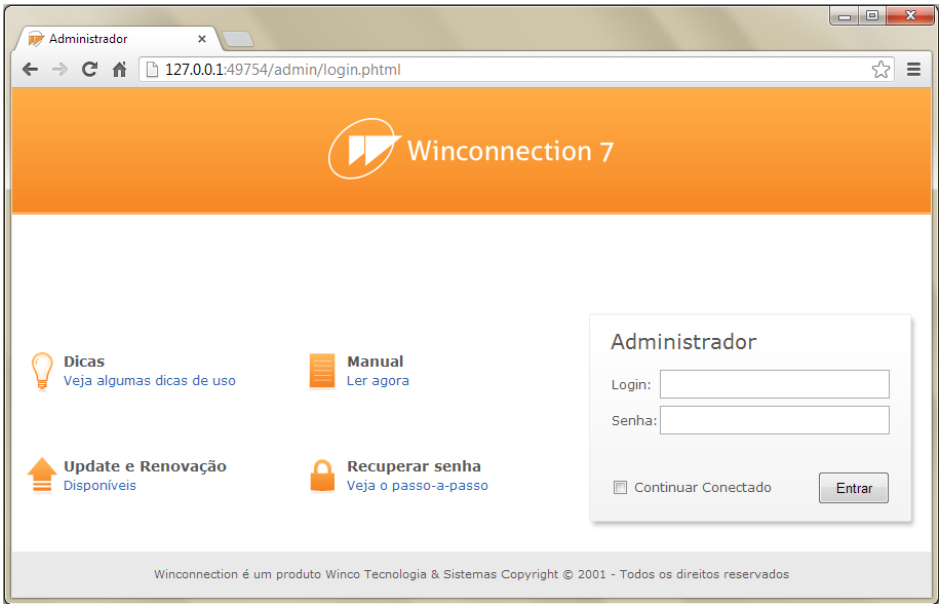
Existe três formas de acessar o administrador:

- Clicando duas vezes no ícone do Winconnection localizado na bandeja do sistema (próximo ao relógio do Windows);
- Clicando em Iniciar | Todos os Programas | Winco | Winconnection 7 | Administrador
- Se a administração remota estiver ativada, digitando o seguinte endereço: *http://ip_do_servidor/admin* a partir de qualquer estação da rede interna ou de redes autorizadas.

  Dica 1: Você pode abrir o Administrador do Winconnection em qualquer navegador copiando o link do browser que abre na máquina local para o outro browser. Porém, tenha em mente que a porta do serviço muda toda vez que o administrador se desconecta da máquina, o que muda o link a ser usado.

  Dica 2: Para acessar o Administrador do Winconnection a partir de um computador fora da sua rede, você deve antes autorizar a rede ou host externo a partir do próprio administrador, acessando o menu *Ferramentas -> Opções do administrador*. Mas é preciso ter cuidado! Recomendamos não utilizar senhas fracas e evitar este tipo de acesso caso o Servidor Web não tiver configurado para usar SSL.

Ao acessar o Administrador do **Winconnection 7** será exibida a seguinte tela de autenticação:

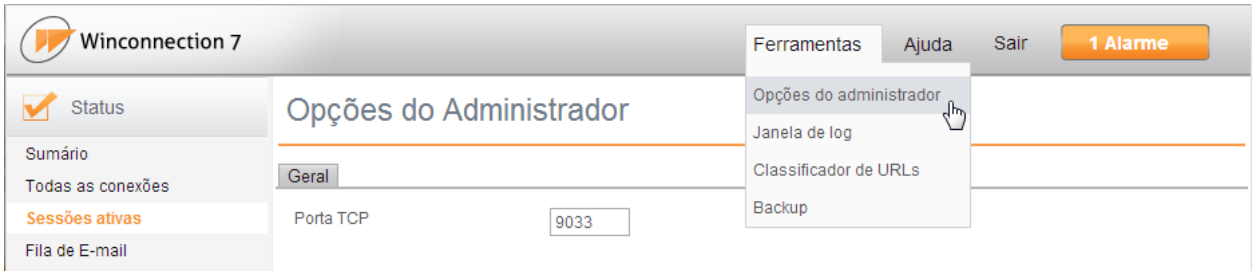


Para acessar o administrador, basta digitar o login e senha do administrador ou de algum usuário que pertença ao grupo Administradores.

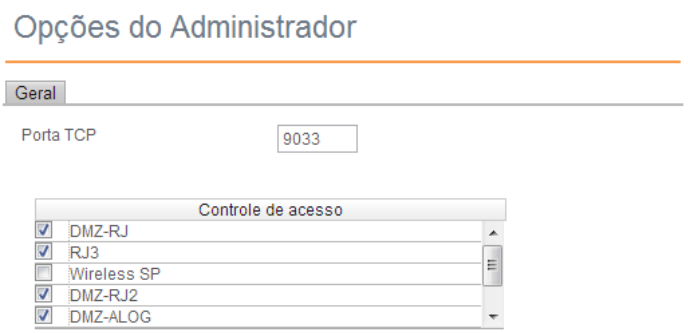
Para recuperar a senha do administrador, consulte este passo-a-passo.

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

Ferramentas:

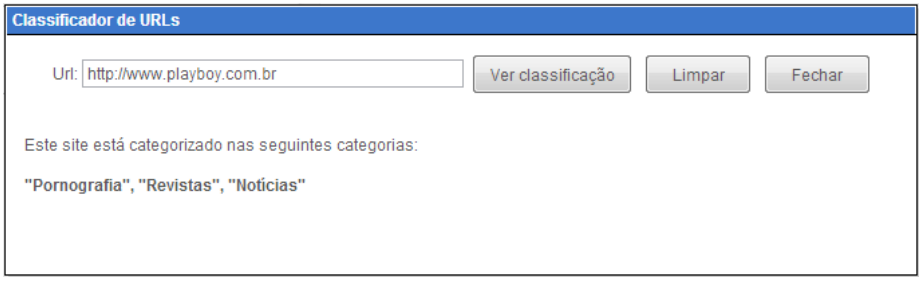


- *Opções do Administrador:* Permite definir a porta e as redes que terão acesso ao administrador do **Winconnection 7**.

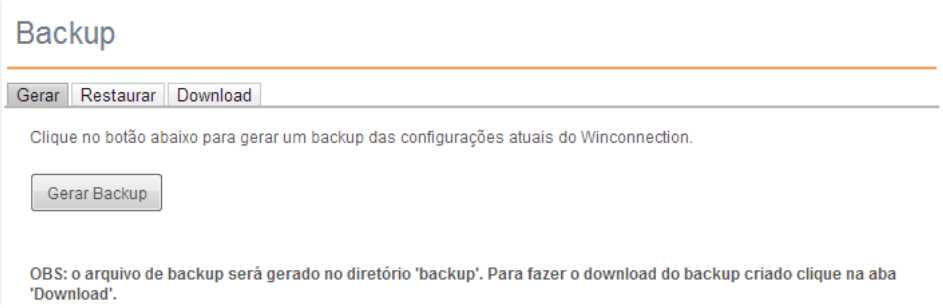


- *Janela de log:* Abre em uma nova guia as informações de todos os acessos ao servidor por serviço acessado.
- *Classificador de URL:* É um utilitário usado para saber a classificação de um site no *Netfilter*, auxiliando na criação das regras web.

  Por exemplo: O administrador da rede deseja bloquear o site da *Playboy* utilizando o *Filtro Automático de Conteúdo*, porém, ele não sabe a categoria que este site pertence. Ao digitar o site http://www.playboy.com.br, o classificador retornará a categoria do site.



- *Backup:* Aqui é possível realizar o backup e o restore das configurações do Winconnection 7.

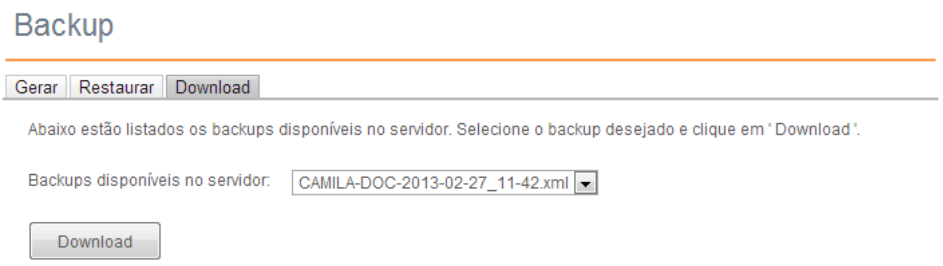


O backup será feito automaticamente nas seguintes situações:

- Todas as vezes que o Winconnection 7 for parado/reiniciado;
- Quando um novo serviço for adicionado (após abrir novamente o administrador);
- Todos os dias à meia-noite;
- Quando o botão “Gerar backup” for acionado;

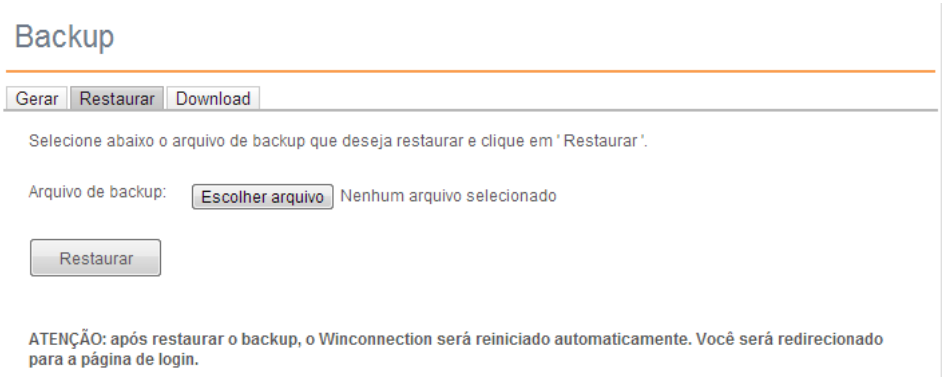
O arquivo de backup será salvo na seguinte pasta: C:\Arquivos de programas\Winco\Winconnection7\backup.

Para fazer o download do arquivo de backup, acesse a aba “Download”.

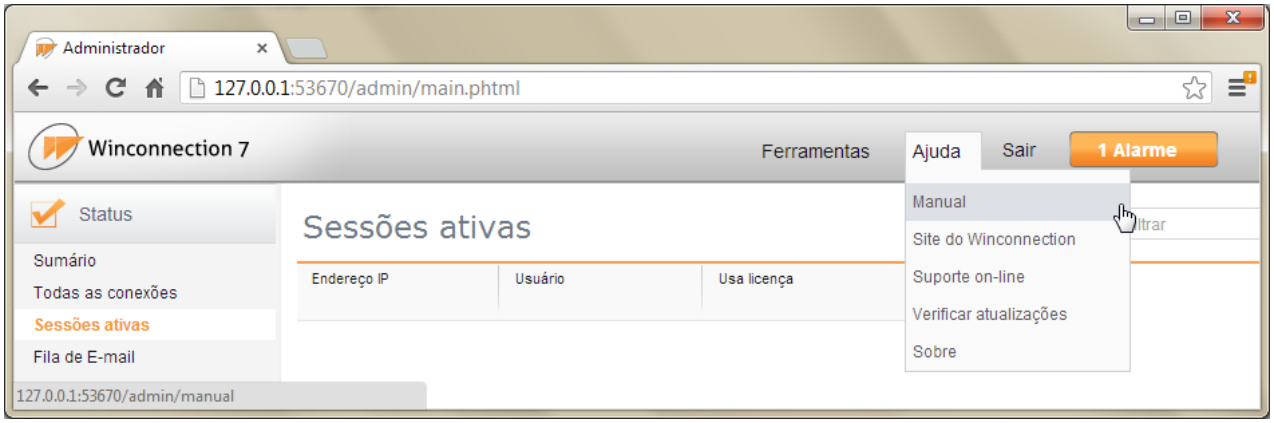


Para restaurar o backup, acesse a aba “Restaurar” -> Clique em “Escolher arquivo” -> Selecione o arquivo de backup e clique no botão “Restaurar”;

Atenção: Após restaurar o backup, o Winconnection será reiniciado automaticamente e você será redirecionado para a página de login.



Ajuda:



- *Manual:* Abre este manual do programa.
- *Site do* Winconnection: Abre o site do **Winconnection**.
- *Suporte* on-line: Abre a seção de suporte do site com as principais perguntas frequentes.
- *Verificar atualizações:* Verifica se novas atualizações do programa estão disponíveis.
- *Sobre:* Mostra informações sobre o software.

Sair: Desconecta o Administrador.

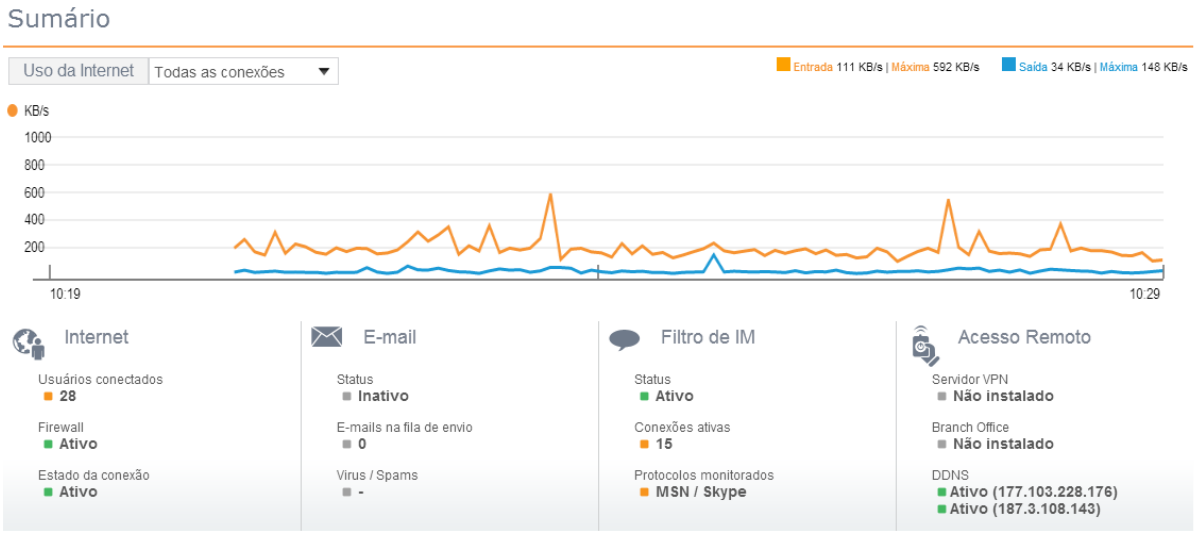
4 Status

4.1 Sumário

Sumário:

O menu Sumário exibe um resumo dos serviços e das atividades do Winconnection:

- **Uso da Internet:** Exibe um gráfico com o uso da internet (download e upload).
- **Internet:** Exibe a quantidade de usuários conectados, o status do firewall e o estado da conexão.
- **E-mail:** Exibe o status do e-mail, a quantidade de e-mail na fila de envio e a quantidade de vírus e spam detectados.
- **Filtro de MSN:** Exibe o status do Filtro de MSN, a quantidade de conexões ativas e os protocolos monitorados (MSN/Skype).
- **Acesso Remoto:** Informa se o Servidor VPN, o Branch Office e o DDNS estão instalados ou não.



4.2 Todas as Conexões

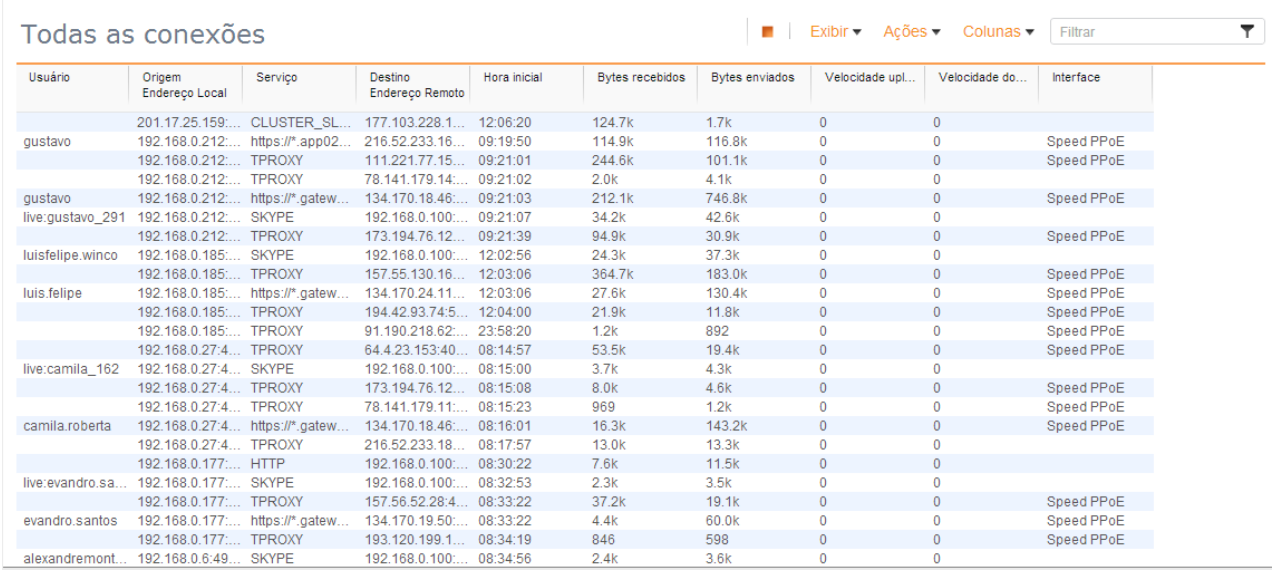
Todas as Conexões

Este menu exibe informações de todas as conexões (entrada e saída de dados).

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

Opções do menu superior:

- Exibir: Agrupa as conexões por usuário, origem, destino ou serviço.
- Ação: Permite excluir ou limitar a banda de uma conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.



Usuário	Origem Endereço Local	Serviço	Destino Endereço Remoto	Hora inicial	Bytes recebidos	Bytes enviados	Velocidade upl...	Velocidade do...	Interface
	201.17.25.159:...	CLUSTER_SL...	177.103.228.1...	12:06:20	124.7k	1.7k	0	0	
gustavo	192.168.0.212:...	https://*.app02...	216.52.233.16...	09:19:50	114.9k	116.8k	0	0	Speed PPoE
	192.168.0.212:...	TPROXY	111.221.77.15...	09:21:01	244.6k	101.1k	0	0	Speed PPoE
	192.168.0.212:...	TPROXY	78.141.179.14:...	09:21:02	2.0k	4.1k	0	0	
gustavo	192.168.0.212:...	https://*.gatew...	134.170.18.46:...	09:21:03	212.1k	746.8k	0	0	Speed PPoE
live:gustavo_291	192.168.0.212:...	SKYPE	192.168.0.100:...	09:21:07	34.2k	42.6k	0	0	
	192.168.0.212:...	TPROXY	173.194.76.12...	09:21:39	94.9k	30.9k	0	0	Speed PPoE
luisfelipe.winco	192.168.0.185:...	SKYPE	192.168.0.100:...	12:02:56	24.3k	37.3k	0	0	
	192.168.0.185:...	TPROXY	157.55.130.16...	12:03:06	364.7k	183.0k	0	0	Speed PPoE
luis.felipe	192.168.0.185:...	https://*.gatew...	134.170.24.11...	12:03:06	27.6k	130.4k	0	0	Speed PPoE
	192.168.0.185:...	TPROXY	194.42.93.74:5...	12:04:00	21.9k	11.8k	0	0	Speed PPoE
	192.168.0.185:...	TPROXY	91.190.218.62:...	23:58:20	1.2k	892	0	0	Speed PPoE
	192.168.0.27:4...	TPROXY	64.4.23.153:40...	08:14:57	53.5k	19.4k	0	0	Speed PPoE
live:camila_162	192.168.0.27:4...	SKYPE	192.168.0.100:...	08:15:00	3.7k	4.3k	0	0	
	192.168.0.27:4...	TPROXY	173.194.76.12...	08:15:08	8.0k	4.6k	0	0	Speed PPoE
	192.168.0.27:4...	TPROXY	78.141.179.11:...	08:15:23	969	1.2k	0	0	Speed PPoE
camila.roberta	192.168.0.27:4...	https://*.gatew...	134.170.18.46:...	08:16:01	16.3k	143.2k	0	0	Speed PPoE
	192.168.0.27:4...	TPROXY	216.52.233.18...	08:17:57	13.0k	13.3k	0	0	
	192.168.0.177:...	HTTP	192.168.0.100:...	08:30:22	7.6k	11.5k	0	0	
live:evandro.sa...	192.168.0.177:...	SKYPE	192.168.0.100:...	08:32:53	2.3k	3.5k	0	0	
	192.168.0.177:...	TPROXY	157.56.52.28:4...	08:33:22	37.2k	19.1k	0	0	Speed PPoE
evandro.santos	192.168.0.177:...	https://*.gatew...	134.170.19.50:...	08:33:22	4.4k	60.0k	0	0	Speed PPoE
	192.168.0.177:...	TPROXY	193.120.199.1...	08:34:19	846	598	0	0	Speed PPoE
alexandremont...	192.168.0.6:49...	SKYPE	192.168.0.100:...	08:34:56	2.4k	3.6k	0	0	

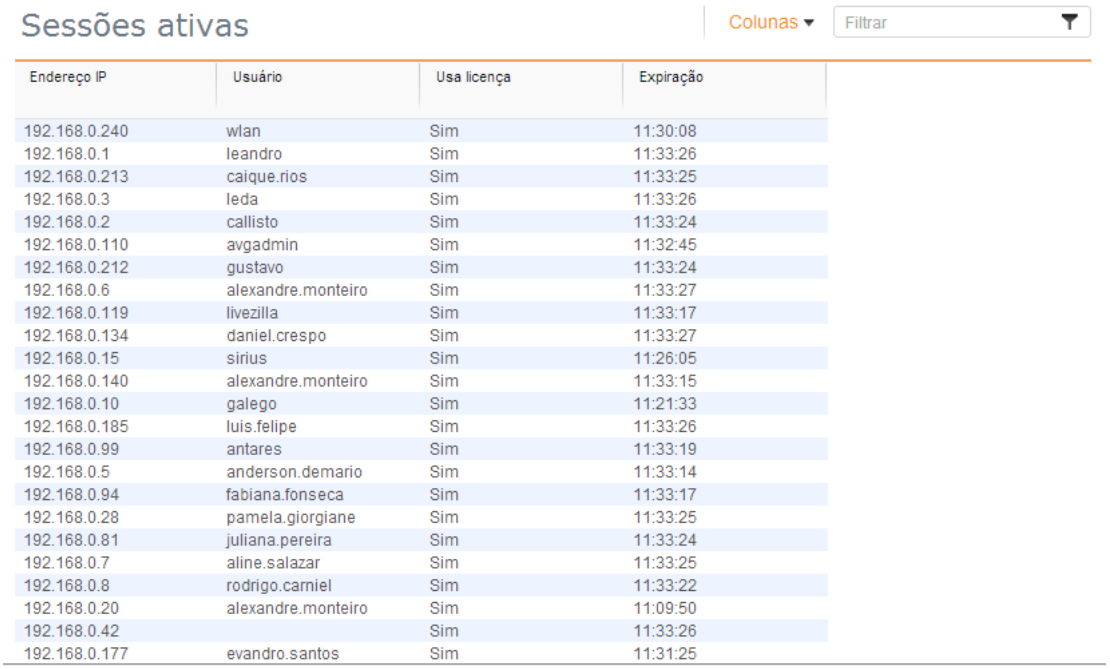
4.3 Sessões ativas

Sessões ativas

Exibe um resumo as sessões ativas.

As informações exibidas são: endereço IP, usuário, a licença utilizada e a expiração da sessão e o ID.

O menu Colunas disponibiliza as informações que poderão ser exibidas.



Endereço IP	Usuário	Usa licença	Expiração
192.168.0.240	wlan	Sim	11:30:08
192.168.0.1	leandro	Sim	11:33:26
192.168.0.213	caique.rios	Sim	11:33:25
192.168.0.3	leda	Sim	11:33:26
192.168.0.2	callisto	Sim	11:33:24
192.168.0.110	avgadmin	Sim	11:32:45
192.168.0.212	gustavo	Sim	11:33:24
192.168.0.6	alexandre.monteiro	Sim	11:33:27
192.168.0.119	livezilla	Sim	11:33:17
192.168.0.134	daniel.crespo	Sim	11:33:27
192.168.0.15	sirius	Sim	11:26:05
192.168.0.140	alexandre.monteiro	Sim	11:33:15
192.168.0.10	galego	Sim	11:21:33
192.168.0.185	luis.felipe	Sim	11:33:26
192.168.0.99	antares	Sim	11:33:19
192.168.0.5	anderson.demario	Sim	11:33:14
192.168.0.94	fabiana.fonseca	Sim	11:33:17
192.168.0.28	pamela.giorgiane	Sim	11:33:25
192.168.0.81	juliana.pereira	Sim	11:33:24
192.168.0.7	aline.salazar	Sim	11:33:25
192.168.0.8	rodrigo.carniel	Sim	11:33:22
192.168.0.20	alexandre.monteiro	Sim	11:09:50
192.168.0.42		Sim	11:33:26
192.168.0.177	evandro.santos	Sim	11:31:25

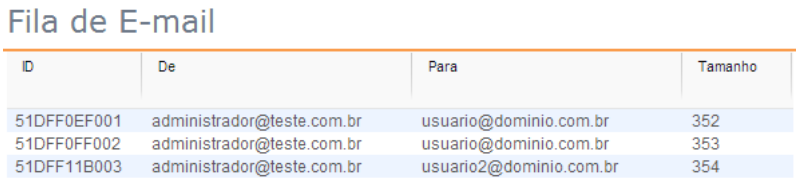
4.4 Fila de E-mail

Fila de E-mail

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

O menu *Filtro de E-mail* oferece as seguintes opções:

- Ações: Permite enviar todas as mensages, enviar ou excluir a mensagem selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.



4.5 Alarmes

Alarmes

Para consultar as configurações, basta clicar no menu Ver configuração.

Guia Geral

Nesta guia é possível definir as **situações** que os alarmes deverão ser emitidos:

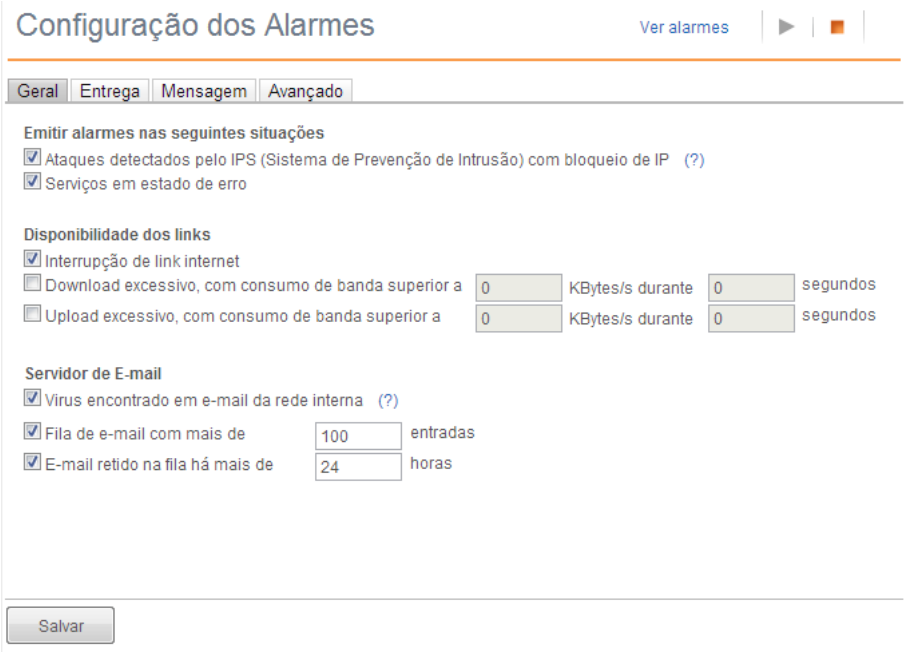
- **Ataques detectados pelo IPS (Sistema de Prevenção de Intrusão) com bloqueio de IP:** O IPS detecta ataques e bloqueia os endereços IP de origem conforme configurado em *Conectividade -> Firewall -> IDS/IPS*.
- **Serviços em estado de erro:** Se esta opção for habilitada, um alarme será emitido quando algum serviço estiver em estado de erro.

Alarmes para **Disponibilidade dos Links**:

- **Interrupção de link internet:** Informa quando houver alguma interrupção no link da internet.
- Nos campos **"Download excessivo"** e **"Upload excessivo"**, o administrador pode definir que um alarme seja enviado quando o consumo de banda de um download e/ou upload for considerado excessivo.

Alarmes para **Serviços de E-mail**:

- **Vírus encontrado em um e-mail da rede interna:** Se esta opção for habilitada, um alarme será emitido se um vírus for detectado originado da rede interna.
  Obs.: Esta opção será válida somente se o escaneamento de vírus estiver habilitado nas configurações do *Filtro de E-mail*.
- Habilitando as opções **"Fila de e-mail com mais de xx entradas:"** e **"E-mail retido na fila há mais de xx horas:"** o administrador da rede será informado quando houver algum problema com a entrega de e-mails.



Guia Entrega:

Nesta guia, o administrador da rede deve definir as configurações para o envio do alarme.

Envio de alarmes por e-mail:

Envio de alarmes por outros meios:

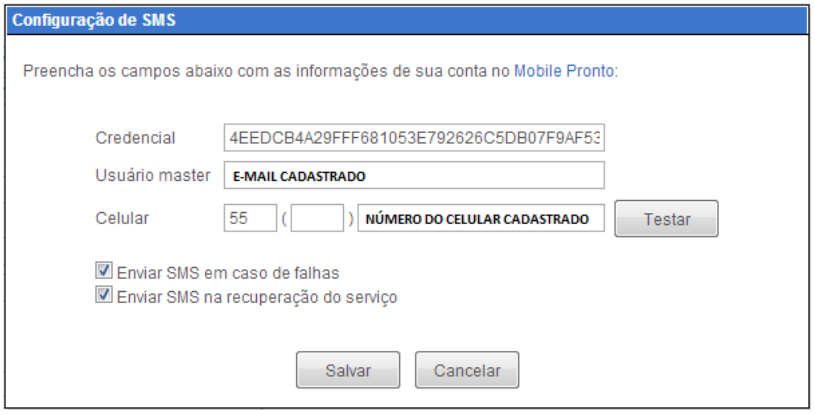
Além do envio por e-mail, também é possível enviar os alarmes por SMS ou por execução de comando:

- **Envio de SMS:** O serviço de envio de SMS é terceirizado, devendo ser contrato diretamente pelo cliente. O **Winconnection** integra o serviço de SMS da empresa Mobile Pronto.

  Para utilizar o serviço de envio de SMS utilizando o Mobile Pronto, siga os seguintes passos:

  - Acesse o site: https://www.mobilepronto.info/ e crie sua conta.
  - Após criar a conta, é necessário ativá-la seguindo as orientações do e-mail que será enviado para o endereço cadastrado.
  - Em seguida, será enviado um novo e-mail com os dados de acesso e com a credencial do projeto. Preencha a configuração de SMS de acordo com os dados fornecidos.

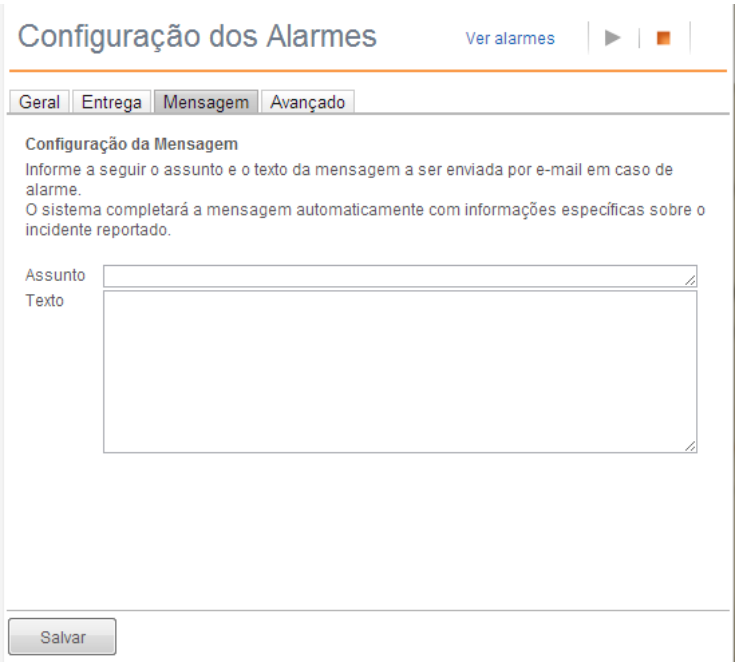
  Obs.: O serviço SMS é feito através da internet, portanto, ao menos um link precisa estar funcionando.



- **Execução de comando:** Neste campo, o administrador da rede deve definir o comando que será executado quando ocorrer um erro, o caminho de um script que será executado para corrigir o problema ou para avisar ao administrador.

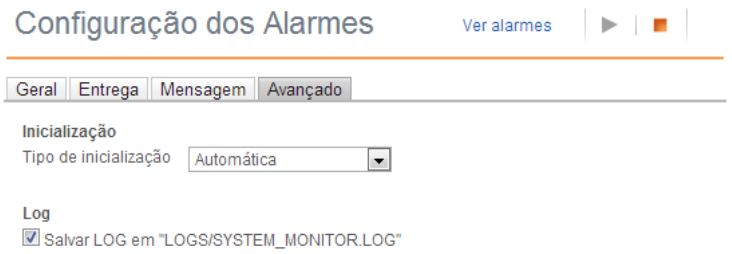
Guia Mensagem:

Nesta guia, o administrador da rede deve definir o assunto e a mensagem de alarme que será enviada por e-mail em caso de alarme. O sistema completará a mensagem automaticamente com informações específicas sobre o incidente reportado.



Guia Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: *Manual*, *Automática* e *Manter o último estado*.
- **Salvar LOG em LOGS/SYSTEM_MONITOR.LOG":** O arquivo em bloco de notas (SYSTEM_MONITOR.LOG) será criado no diretório *C:/Arquivos de programas/Winco/Winconnection 7/LOGS* e conterá todas as informações referentes a este serviço.



Para consultar os alarmes disparados, basta clicar no menu "Ver alarmes".

5 Relatórios

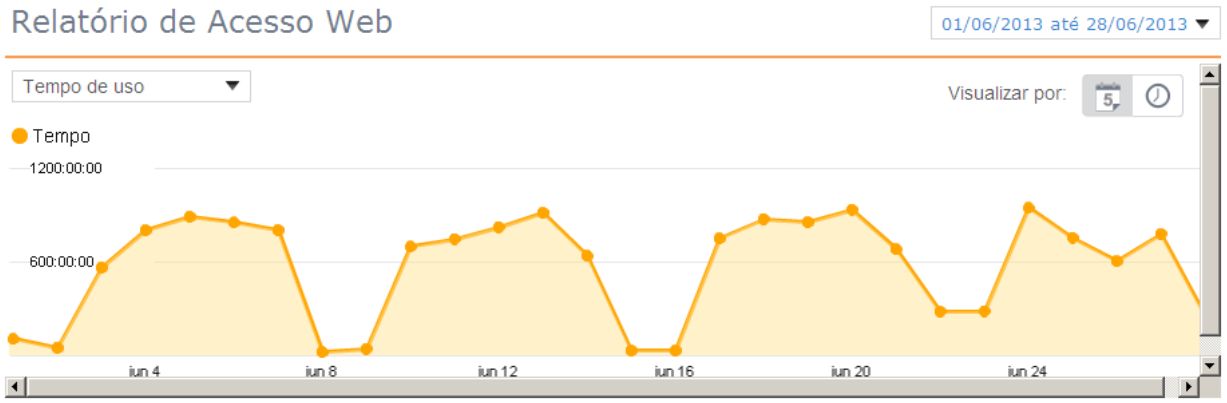
5.1 Acesso Web

O relatório de acesso 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.

A visualização do relatório pode ser filtrada por hora e por dia.

Relatórios gráficos podem ser gerados, baseandos nos seguintes dados:

- **Páginas acessadas**
- **URLs**
- **Tempo de Uso**
- **Transferência**



Outros relatórios podem ser gerados, baseando-se nos seguintes dados:

- **Relatórios por 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.
- **Relatórios por usuário:** Ao selecionar um usuário é possível verificar os domínios acessados por ele, com a possibilidade de detalhar os acessos aos domínios.
- **Domínio bloqueados**
- **Usuários bloqueados**

Relatório por domínio | Pesquisar | Filtrar por:

Páginas acessadas por: *Todos os Usuários*

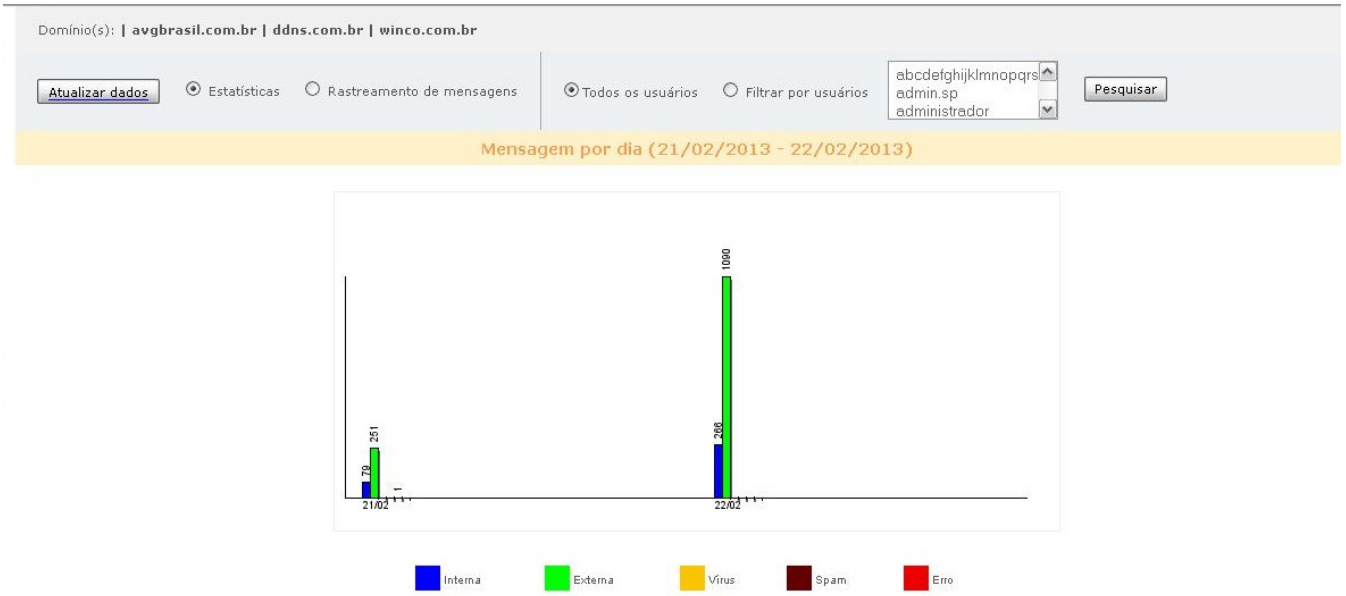
Domínios	Páginas	URL	Tamanho	Tempo de navegação
winco.com.br	1155734	1171853	3205.9M	901:30:00
globo.com	352667	472158	3030.0M	139:17:00
facebook.com	285170	286006	1065.6M	505:47:00
akamai.net	250226	250764	14.2M	272:48:00
alerta24h.com.br	178470	178470	3.0k	394:35:00
google.com	162674	170838	2100.6M	462:47:00
google-analytics.com	128815	135373	58.2M	321:09:00
avg.com	110016	122015	6859.1M	427:14:00
glbimg.com	104198	888723	3954.6M	115:36:00
doubleclick.net	94012	95198	193.0M	231:37:00
uol.com.br	93786	192750	1368.6M	56:43:00
realtime.co	89126	89244	31.1M	19:07:00
twitter.com	62618	66855	165.4M	146:08:00
youtube.com	60385	60866	22690.1M	83:12:00

5.2 E-mail

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.



Data	Interna	Externa	Vírus	Spam	Erro(s)
21/02/13	79 (3,42 Mb)	251 (8,70 Mb)	0	0	1
22/02/13	266 (15,12 Mb)	1090 (77,66 Mb)	0	0	0

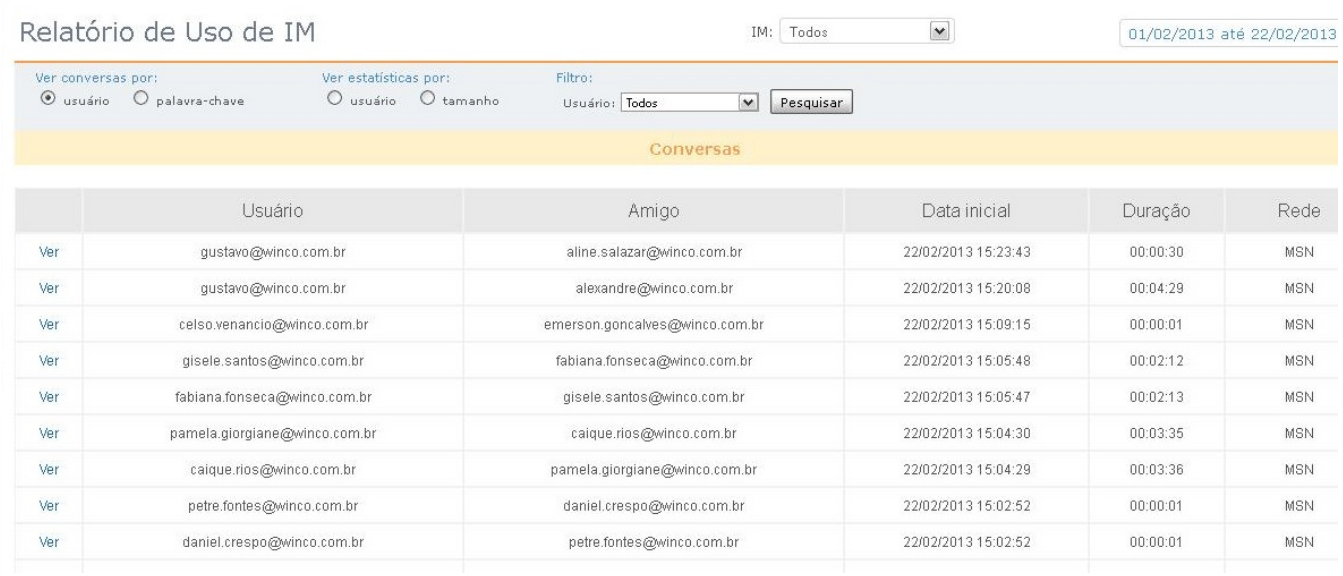
5.3 Skype e MSN

O **Winconnection 7** permite que relatórios gerenciais sejam gerados de maneira prática e organizada.

Os relatórios podem exibir vários resumos e estatísticas sobre como os programas de mensagens instantâneas estão sendo utilizados na empresa.

Com os relatórios gerenciais é possível:

- Filtrar a visualização das conversas por data, usuário ou palavra-chave.
- Filtrar a visualização das estatísticas por data, usuário e tamanho.



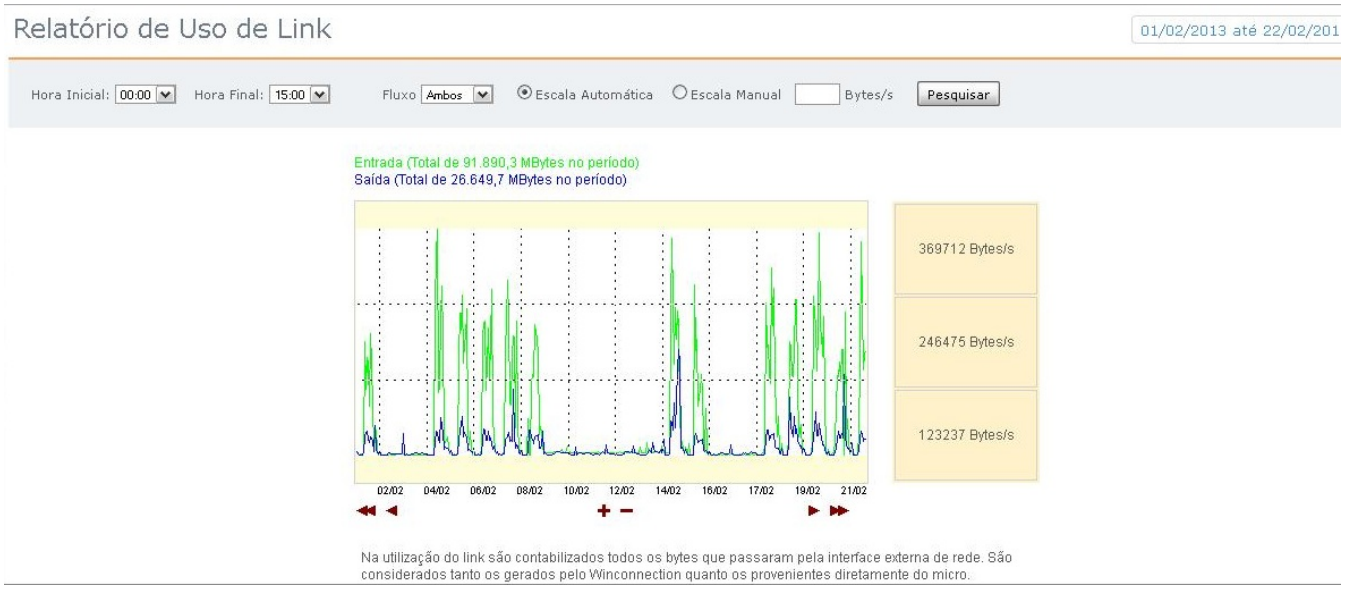
	Usuário	Amigo	Data inicial	Duração	Rede
Ver	gustavo@winco.com.br	aline.salazar@winco.com.br	22/02/2013 15:23:43	00:00:30	MSN
Ver	gustavo@winco.com.br	alexandre@winco.com.br	22/02/2013 15:20:08	00:04:29	MSN
Ver	celso.venancio@winco.com.br	emerson.goncalves@winco.com.br	22/02/2013 15:09:15	00:00:01	MSN
Ver	gisele.santos@winco.com.br	fabiana.fonseca@winco.com.br	22/02/2013 15:05:48	00:02:12	MSN
Ver	fabiana.fonseca@winco.com.br	gisele.santos@winco.com.br	22/02/2013 15:05:47	00:02:13	MSN
Ver	pamela.giorgiane@winco.com.br	caique.rios@winco.com.br	22/02/2013 15:04:30	00:03:35	MSN
Ver	caique.rios@winco.com.br	pamela.giorgiane@winco.com.br	22/02/2013 15:04:29	00:03:36	MSN
Ver	petre.fontes@winco.com.br	daniel.crespo@winco.com.br	22/02/2013 15:02:52	00:00:01	MSN
Ver	daniel.crespo@winco.com.br	petre.fontes@winco.com.br	22/02/2013 15:02:52	00:00:01	MSN

5.4 Uso do Link

A função do Relatório de Uso de Link é demonstrar como está o fluxo de dados destinados à internet dentro do Winconnection 7. 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.



6 Cadastros

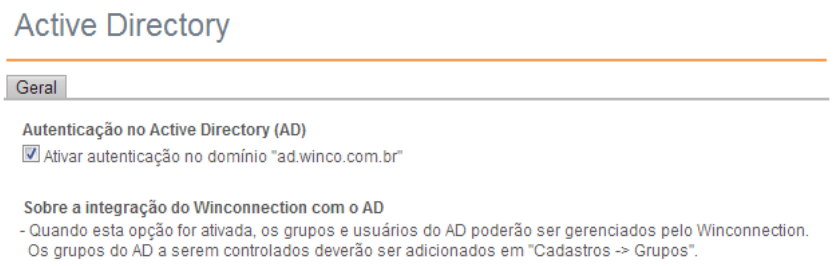
6.1 Active Directory

O **Winconnection 7** 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 7** 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.

No menu *Active Directory* é possível ativar autenticação de domínio que permite a integração do **Winconnection 7** com o *MS Active Directory (AD)*, ou seja, os grupos e usuários do AD poderão ser gerenciados pelo Winconnection.

Os grupos do AD a serem controlados deverão ser adicionados no menu *"Grupos"*.



Configuração do Winconnection usando AD:

Procedimentos:

1) A máquina onde o Winconnection está instalado deve fazer parte do domínio;

2) O DNS da placa da rede interna deve apontar para o AD;

3) A máquina deve ser configurada como confiável. Existem 2 maneiras para isso:

- 3.1) Opção 1: A máquina deve ser marcada como “trusted”(confiável) no AD; ou
- 3.2) Opção 2: Um login de usuário administrador do domínio deve ser colocado no Logon do serviço do Winconnection:
  - 3.2.1) Clique com o botão direito em Meu Computador -> Gerenciar -> Serviços -> Winconnection;
  - 3.2.2) Pare o Winconnection;
  - 3.2.3) Dê dois cliques no serviço do Winconnection, na aba ‘Logon’ marque a opção ‘Esta conta’ e procure pelo usuário administrador do AD. Digite a senha do usuário;
  - 3.2.4) Inicie o Winconnection;

Obs.: Caso a segunda opção seja escolhida, lembre-se que sempre que o administrador mudar a senha, ela também deverá ser alterada no Logon do serviço do Winconnection.

Problemas na sincronização Winconnection <-> AD:

Caso ocorra algum problema do tipo: usuário pertence a um grupo que não tem permissão de navegar em determinado site mas está navegando, siga os passos:

1) Abra o regedit;

2) Abra a chave HKEY_LOCAL_MACHINE -> SOFTWARE -> Winco _> ADCache -> USERS;

3) Selecione o usuário e verifique na chave AD_GROUPS os grupos a que ele pertence. Caso esteja incorreto, siga os seguintes procedimentos:

- 3.1) Renomeie a chave ADCache para ADCache.sav;
- 3.2) Pare e inicie o Winconnection. Verifique se a chave ADCache foi criada com as configurações de grupos corretas para os usuários.

6.1.1 Parâmetros Winconnection para Usuários do Domínio

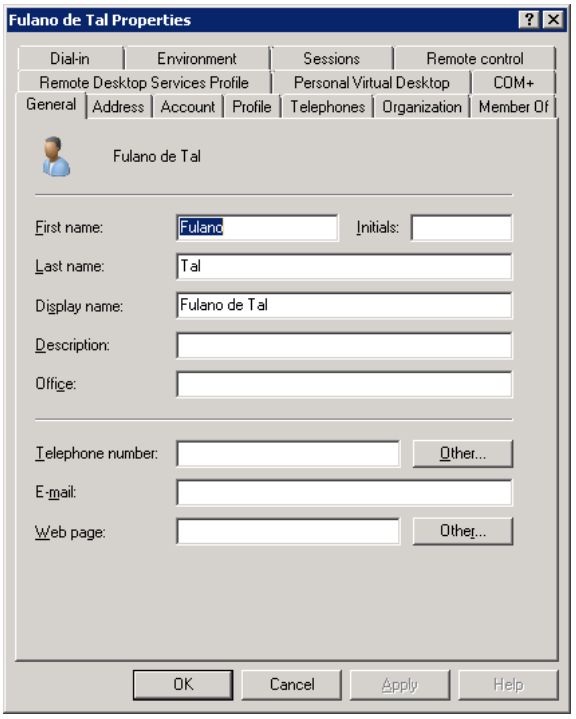
Algumas configurações de usuário do Winconnection podem ser estabelecidas diretamente no Active Directory do domínio, onde a máquina que hospeda o produto está instalada. Isto permite a administração centralizada de alguns parâmetros do usuário.

Os parâmetros de usuário que podem ser estabelecidos no Active Directory são os seguintes:

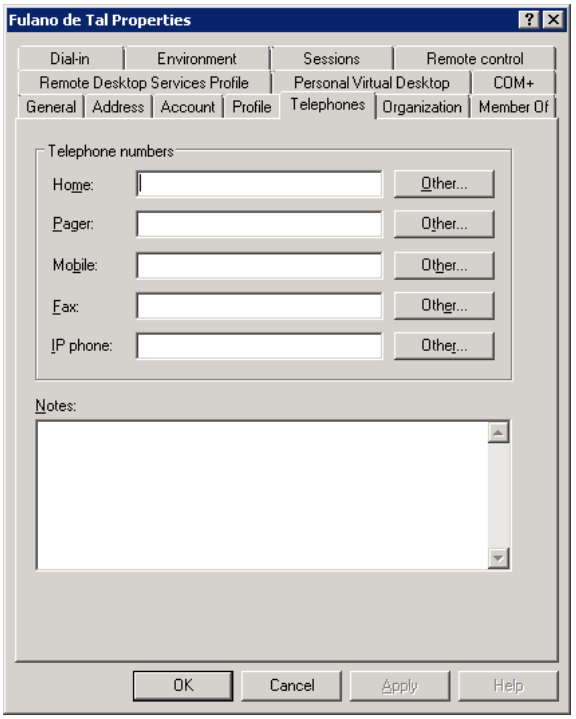
- **MAILHOST:** Servidor responsável pelo armazenamento de mensagens de e-mail do usuário. Em um ambiente onde haja diversos servidores de e-mail, este parâmetro especifica ao Filtro de E-mail,qual é o servidor específico do usuário. Isto permite ao filtro entregar as mensagens no servidor correto;
- **MSN:** Login ou identificação do usuário no MSN. Este parâmetro determina qual é o endereço, ou identificação, MSN do usuário;
- **SKYPE:** Login ou identificação do usuário no Skype. Este parâmetro determina qual é o endereço, ou identificação, Skype do usuário;

Como não há um campo específico no Active Directory para os parâmetros acima, os mesmos são armazenadas em um campo informacional do usuário que diz respeito aos telefones do mesmo, mais especificamente no campo das notas sobre os telefones.

Uma das maneiras de alterar as configurações de um usuário no Active Directory, é utilizar o utilitário "Usuários e Computadores do Active Directory" (Active Directory Users and Computers), presente no menu de sistema "Ferramentas Administrativas" (Administrative Tools). Uma vez dentro do utilitário, seleciona-se o usuário, localizado-o na árvore do domínio ao qual ele pertence. Clicando duas vezes no objeto representando o usuário, as configurações do mesmo são exibidas em uma janela.



Nesta janela existe uma aba "Telefones" (Telephones), onde um campo "Notas" (Notes) está disponível. Neste campo pode-se colocar as configurações Winconnection do usuário.

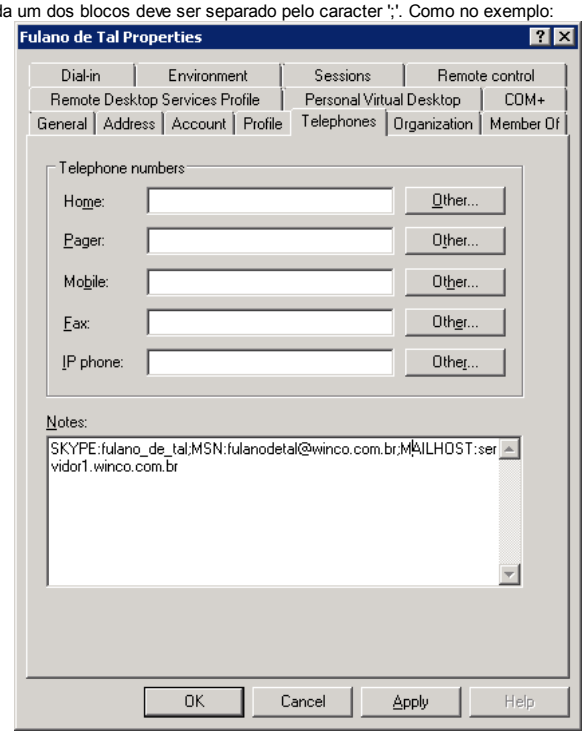


As configurações Winconnection do usuário devem ser dispostas da seguinte maneira: [NOME DO PARÂMETRO]:[VALOR DO PARÂMETRO]. Veja o exemplo:

- SKYPE:fulano_de_tal
- MSN:fulanodetal@winco.com.br

- MAILHOST:servidor1.winco.com.br

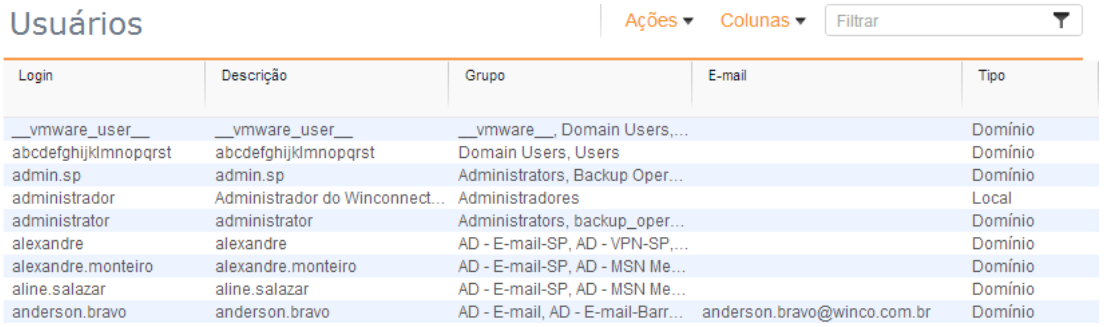
Se forem necessárias mais de um parâmetro, cada um dos blocos deve ser separado pelo caracter ';'. Como no exemplo:



6.2 Usuários

O menu *Usuários* oferece as seguintes opções:

- Ações: Permite criar, editar ou excluir um usuário.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

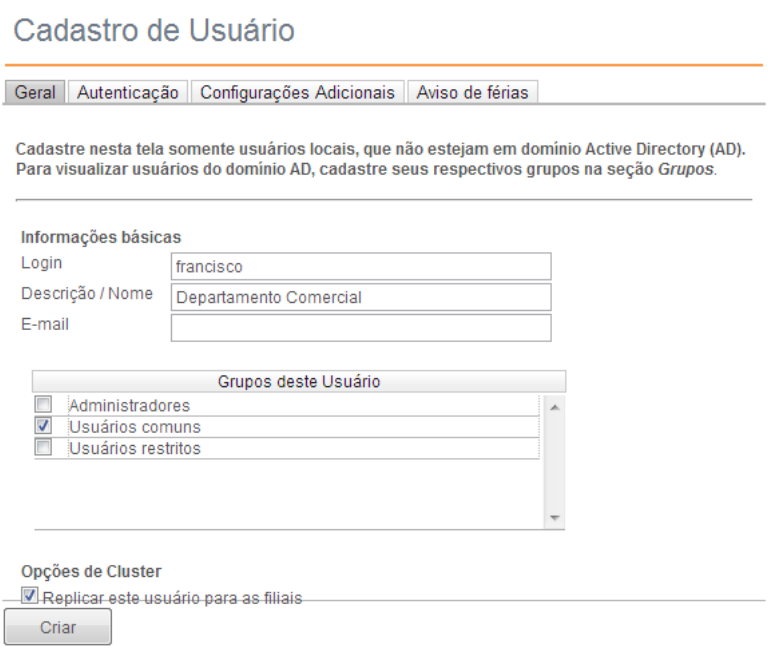


O administrador da rede, deve cadastrar somente os usuários locais, que não estejam em domínio Active Directory (AD).
Para visualizar usuários do domínio AD, é necessário cadastrar seus respectivos grupos na menu *"Grupos"*.

Ao cadastrar um novo usuário, as seguintes informações estão disponíveis:

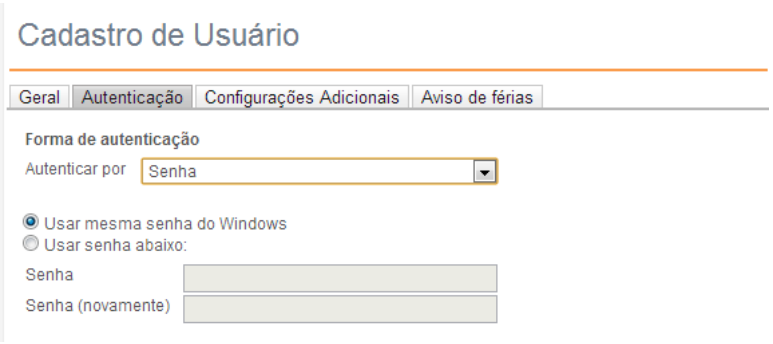
Guia Geral:

- **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 tópico *Cluster Master*.



Guia Autenticação:

- **Forma de Autenticação:** Define como o usuário deverá se autenticar. As seguintes opções estão disponíveis (é possível usar somente uma ou então, uma combinação destas opções):
- **Senha:** Para o usuário se autenticar será necessário usar uma senha:
    - Usar a mesma senha do Windows: Quando o Winconnection 7 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 7 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.

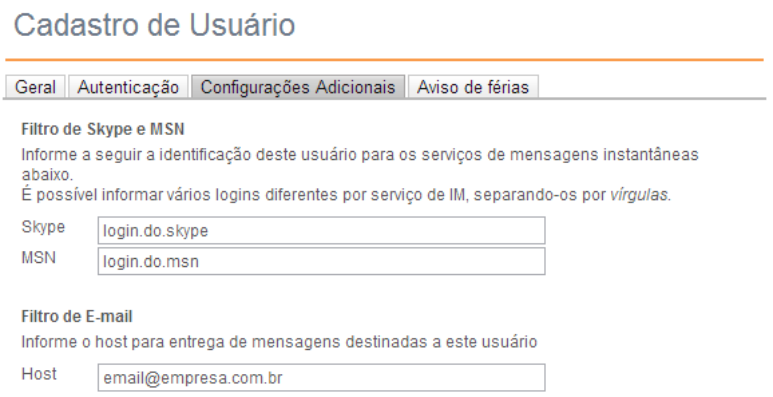


Guia Configurações Adicionais:

- **Filtro de Skype e MSN:** Informe neste campo, a identificação deste usuário que está sendo criado/editado para os serviços de mensagens instantâneas (Skype e/ou MSN).

  Obs.: É possível informar vários logins diferentes por serviço de mensagens instantâneas, separando-os por vírgulas.

- **Filtro de E-mail:**
  - **Host:** Digite nesse campo, o endereço de e-mail que servirá como host para entregar mensagem para esse usuário.



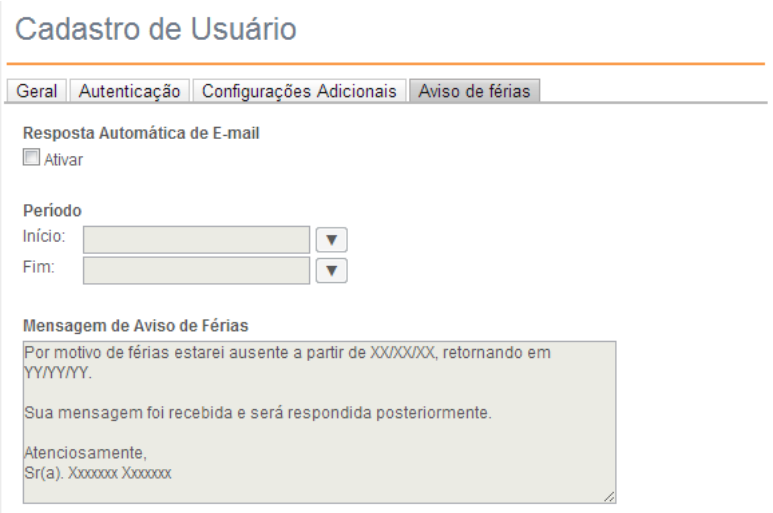
Guia Aviso de Férias:

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**.

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 7**. Esse texto pode ser alterado a qualquer momento.



6.3 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. 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 7** vem com 3 grupos básicos previamente cadastrados:

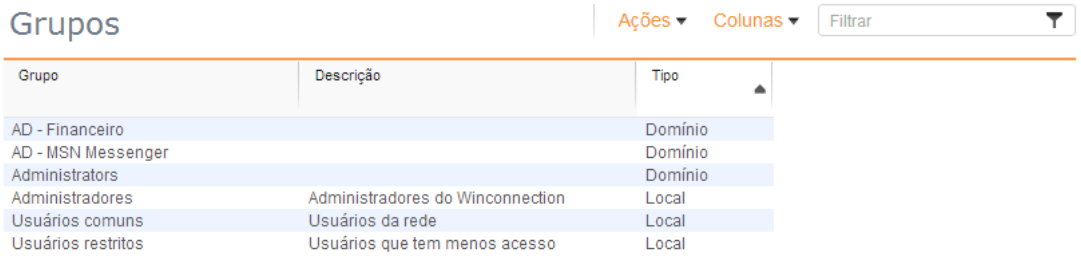
- **Administradores:** É o grupo que contém os usuários com maiores direitos dentro do Winconnection 7. Pelo sistema, estes usuários podem até logar. no *Administrador do Winconnection*, gerenciando assim direitos dos outros usuários. Recomenda-se que o acesso a este grupo seja restrito à equipe de TI.
- **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.

Ao clicar no menu *Grupos*, são exibidas informações sobre os grupos que já foram cadastrados.

O menu *Grupos* oferece as seguintes opções:

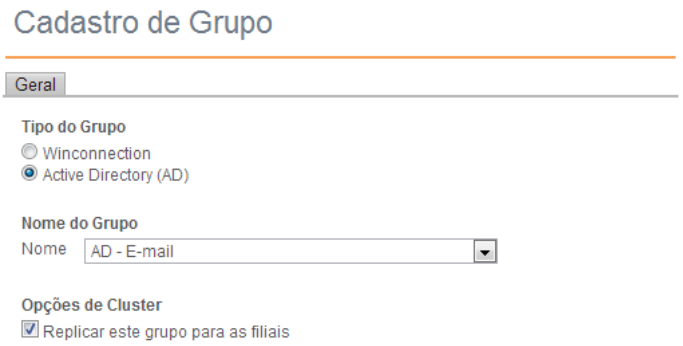
- Ações: Permite criar, editar ou excluir um grupo de usuários.
- Colunas: Disponibiliza as informações que poderão ser exibidas.



Ao criar ou editar um grupo, as seguintes opções são exibidas:

- **Tipo de Grupo:**
  - **Winconnection:** Neste campo é necessário digitar o nome e a descrição do grupo.
  - **Active Directory (AD):** O administrador da rede poderá selecionar um grupo de usuários do *Active Directory* (AD).

    Obs.: É necessário ativar a autenticação de domínio (menu Active Directory).
- **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 tópico *Cluster Master*.



6.4 Redes Lógicas

O **Winconnection 7** tem um conceito bastante abrangente de *Redes e Acessos* permitidos aos serviços.

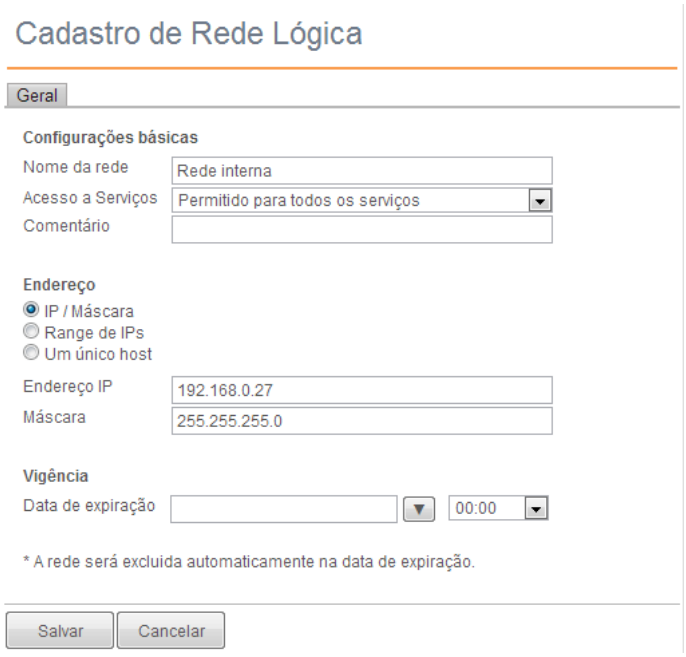
A instalação padrão tem um algoritmo que calcula e permite que o acesso dos computadores da rede interna, seja configurado por cada serviço pré-instalado formando uma *Regra de Acesso.*

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.

O menu R*edes Lógicas* oferece as seguintes opções:

- Ações: Permite criar, editar ou excluir uma rede lógica.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Veja um exemplo da regra geral e básica do **Winconnection 7** na imagem abaixo:



Ao criar ou editar uma rede lógica, as seguintes opções são exibidas:

Configurações básicas:

- **Nome da Rede:** Neste campo, é necessário definir o nome da rede que está sendo criada.
- **Nível de Acesso:** Indica ao **Winconnection 7** 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 7.
    - **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 7** 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 7** 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.

Vigência:

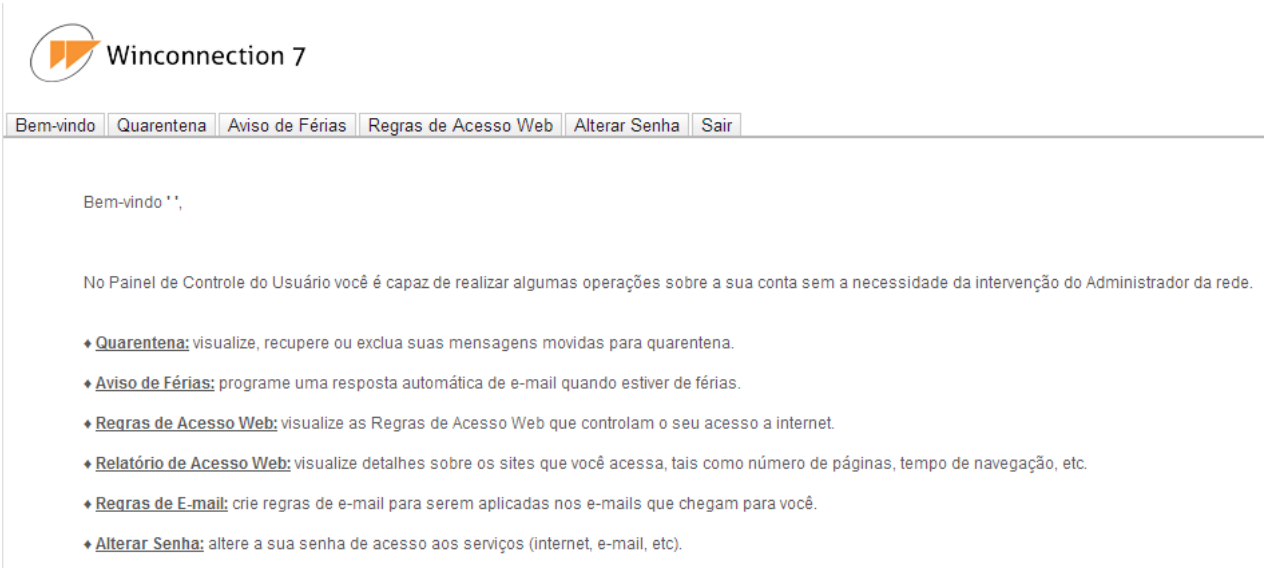
- **Data de expiração:** Permite que o administrador da rede defina uma data e hora para a expiração da rede que está sendo criada/editada. A rede será excluída automaticamente quanto o tempo de uso definido expirar.

6.5 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, Alterar Senha*.

Para acessá-lo, o administrador da rede deve liberar o alias do *Painel de Controle de Usuário*, clicando no botão *Aliases administrativos* do serviço *Servidor WWW*.

Algumas opções ficam ativas somente se o serviço associado a elas estiver em execução. Em caso de dúvidas entre em contato com o administrador da rede.



- **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 7**, 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*.

- **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.

- **Regras de Acesso a Web:** Nesta guia, o usué possível visualizar as regras de acesso que o usuário fez uso até o momento do acesso desta guia.

- **Relatório de Acesso a Web:** Nesta guia, o usuário poderá visualizar o seu relatório de acesso a Web.

- **Regras de E-mail:** Nesta guia, o usuário poderá criar suas próprias regras de email.

  Para isto, o administrador do sistema deve habilitar o usuário na configuração do *Filtro de E-mail (Filtro de E-mail->Regras por Usuário)*. O administrador do sistema terá acesso as regras criadas pelos usuários em *Filtro de E-mail->Regras por Usuário->{usuário}-> Editar*, e poderá editar e/ou excluir as regras criadas pelos usuários, além de poder criar novas regras. Os usuários também terão acesso as regras criadas pelo administrador, especificamente para eles, e também poderão editar ou excluí-las.

  Observação: Se o administrador quiser que uma regra não possa ser visualizada/editada/excluída pelo usuário, ele deverá criar uma *Regra Avançada*.

- **Alterar Senha:** Esta guia permite que o usuário altere a sua senha de autenticação.

7 Conectividade

7.1 Firewall

O Firewall do **Winconnection 7** 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.

O **Winconnection 7** controla automaticamente a abertura de portas do Firewall conforme a necessidade, baseado nas configurações realizadas nos menus de *"Conectividade"* e de *"Serviços"*.

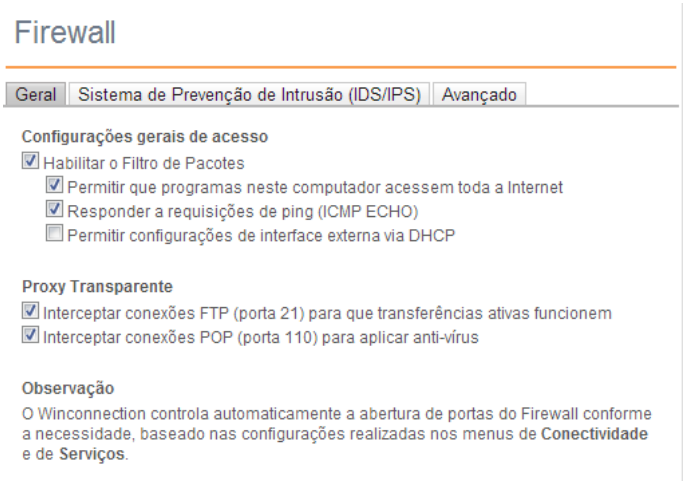
Guia Geral

Configurações gerais de acesso:

- **Habilitar Filtro de Pacotes:** Habilitando esta opção, o filtro de pacotes do Winconnection 7 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.

Proxy Transparente:

- **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 Sistema de Prevenção de Intrusão (IPS)

O IPS do **Winconnection 7** oferece 3 tipos de proteção. Estes tipos foram selecionados por proporcionarem um grande aumento da segurança, mantendo um número bem baixo de falsos positivos. Em resumo, é eficaz sem incomodar o administrador da rede com informações sobre possíveis invasões, que na verdade são acessos comuns feitos por usuários legítimos. Os tipos de proteção do IPS são:

Port Scan

Detecção de "varredura de portas": um procedimento bastante comum entre hackers é fazer uma varredura para descobrir quais serviços estão disponíveis para serem atacados no computador "alvo". Esta técnica, chamada de "port scan", é detectada e o potencial hacker é bloqueado automaticamente antes que possa descobrir ou atacar os serviços.

- **Bloquear o IP (somente com Filtro de Pacotes habilitado):** Neste campo, o administrador da rede deve informar o número de tentativas que poderão ser realizadas antes de efetuar o bloqueio e por quanto tempo (em minutos) o bloqueio deve permanecer ativo.

Injeção de Código Malicioso

Detecção de "injeção de código malicioso": códigos maliciosos são sequencias de dados enviadas para um serviço internet (por exemplo, IMAP ou SMTP) como se fossem credenciais de acesso, mas que na verdade são trechos de programas maliciosos que serão executados no computador remoto devido a falhas de segurança dos sistemas. Mesmo que tal ataque não seja bem sucedido, o fato de alguém tentar injetar sequencias de programação em uma conexão é motivo suficiente para bloquear a rede antes que o hacker encontre uma outra forma de invadir o sistema. Assim, quando a tentativa de injeção de código malicioso ocorre, o potencial intruso é imediatamente bloqueado.

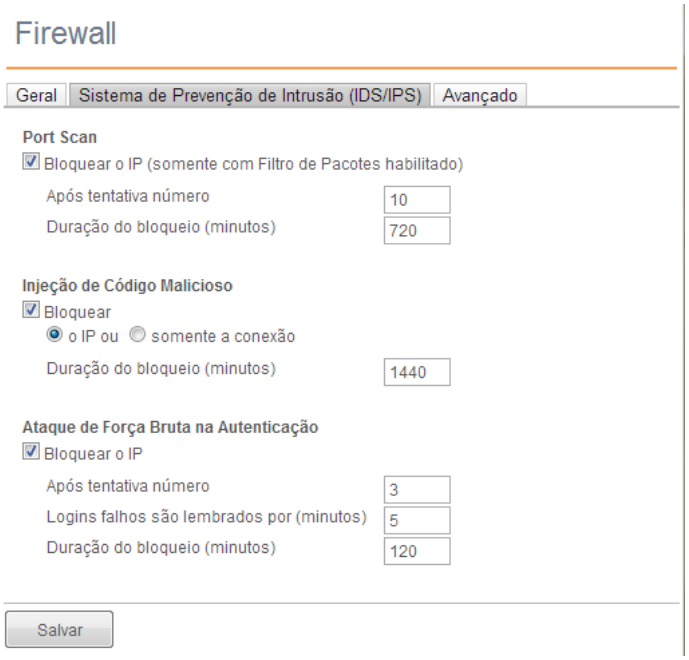
- **Bloquear:** Neste campo, é possível determinar se o bloqueio será feito para o endereço IP ou somente para a conexão. Também é possível informar por quanto tempo (em minutos) o bloqueio deve permanecer ativo.

Ataque de Força Bruta na Autenticação:

Detecção de ataques por "força bruta": ataques de força bruta são invasões feitas através de tentativa e erro até encontrar uma conta de usuário que tenha senha fraca, ou fácil de ser descoberta. Estes ataques normalmente utilizam dicionários de nomes de usuários e senhas comuns e tentam literalmente milhares de combinações até achar uma que funcione no computador a ser atacado. Este ataque é o mais comum em contas de e-mail e FTP e causa danos porque o hacker assume o e-mail ou a identidade de um usuário da rede local e com isso ganha acesso indevido. No **Winconnection 7**, se um número grande de tentativas de conexão for detectado, o endereço IP será bloqueado para todo e qualquer acesso, mesmo em outros serviços/portas por um determinado tempo (configurável).

- **Bloquear o IP:**
    - **Após tentativa número:** Neste campo, o administrador da rede deve informar o número de tentativas que poderão ser realizadas antes de efetuar o bloqueio.
    - **Logins falhos são lembradas por [minutos]:** Neste campo, deve-se informar o intervalo máximo (em minutos) entre as tentativas de autenticação sem sucesso.

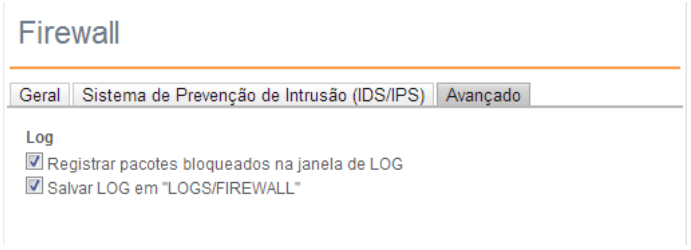
- **Duração do bloqueio [minutos]:** Deve-se informar por quanto tempo (em minutos) o bloqueio deve permanecer ativo.



Com estas proteções ativas, a rede fica melhor protegida, sem gerar informações difíceis de avaliar e que necessitam de uma resposta do administrador. Mas ainda assim, o administrador pode, caso tenha interesse, receber alertas via e-mail ou SMS (configurável no menu *"Alarmes"*).

Guia Avançado

- **Registrar pacotes bloqueados na janela de LOG:** Todos os pacotes bloqueados serão exibidos na janela de log do administrador do **Winconnection 7**.
- **Salvar log em "LOGS/FIREWALL":** O arquivo em bloco de notas (FIREWALL.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 7\LOGS* e conterá todas as informações referente ao serviço Firewall.



7.2 Interfaces

O menu *Interface* oferece as seguintes opções:

- Ações: Permite editar a interface selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Ao editar uma interface as seguintes opções estarão disponíveis:

Guia Geral

Informações da Interface:

- **Gerenciar pelo Winconnection**: Habilite esta opção se você deseja gerenciar pelo **Winconnection** a conexão selecionada.
- **Tipo:** O **Winconnection 7** 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 *Controle de Banda*, quando os filtros estão ativados.
- **Especificar um endereço IP:** Neste campo, o administrador da rede deve definir o endereço IP da conexão selecionada.
- **Compartilhar conexão com a internet através dessa interface:** Se esta opção estiver habilitada, o **Winconnection 7** irá compartilhar as conexões de internet através desta interface.

Balanceamento de Carga e Controle de Banda:

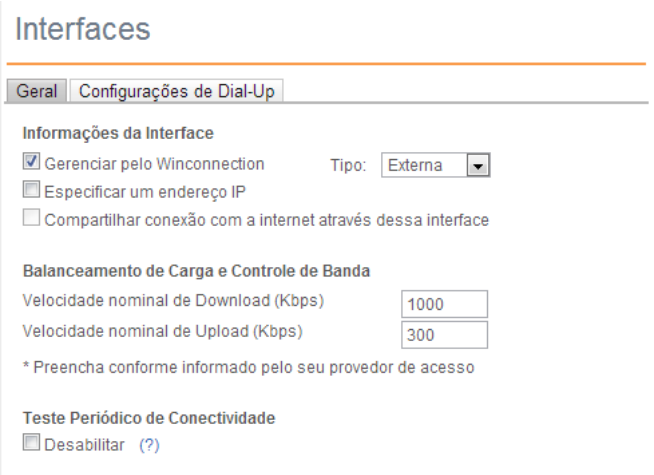
Neste campo, o administrador da rede poderá definir o balanceamento de carga e controle de banda para a interface de rede selecionada. Os campos **"Velocidade nominal de Download (Kbps)"** e **"Velocidade nominal de Upload (Kbps)"** devem ser preenchidos de acordo com as informações disponibilizadas pelo seu provedor de acesso.

Teste Periódico de Conectividade:

O **Winconnection** está constantemente realizando testes nas interfaces classificadas como "externas". Se os testes indicarem uma interface como falha, ela é automaticamente retirada do balanceamento de links. Basicamente dois testes são realizados, testes locais e remotos. Os testes locais dizem respeito ao alinhamento do link, a presença de um IP, conexões dial-up ativas e etc. O teste remoto é realizado através de uma requisição de DNS a um servidor externo. O único teste que pode ser desabilitado é o teste externo.

Em determinadas situações, o teste pode resultar em falso-positivo e acusar que existe uma falha na interface erroneamente.

Nessas situações, é possível desabilitar a execução dos testes. Porém, fazendo isso você não será alertado sobre eventuais problemas que a interface venha a apresentar.

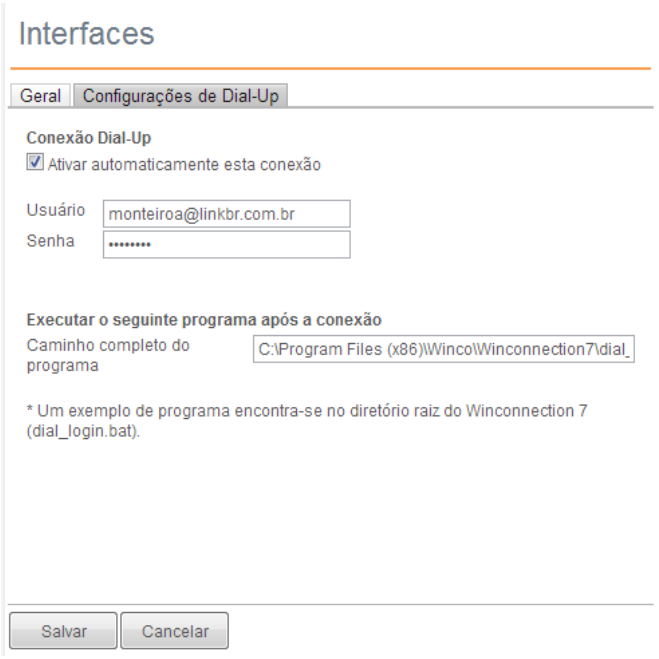


Guia Configurações de Dial-Up:

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:


Interfaces
Geral
Configurações de Dial-Up
Conexão Dial-Up
Ativar automaticamente esta conexão
Usuário
monteiroa@linkbr.com.br
Senha
Executar o seguinte programa após a conexão
Caminho completo do programa
C:\Program Files (x86)\Winco\Winconnection7\dial_
* Um exemplo de programa encontra-se no diretório raiz do Winconnection 7 (dial_login.bat).
Salvar
Cancelar

7.3 Balanceamento de Links

O **Winconnection 7** suporta múltiplos links externos. Suportando múltiplos links externos, é possível explorar arquiteturas tolerantes a falhas ou balanceadas.

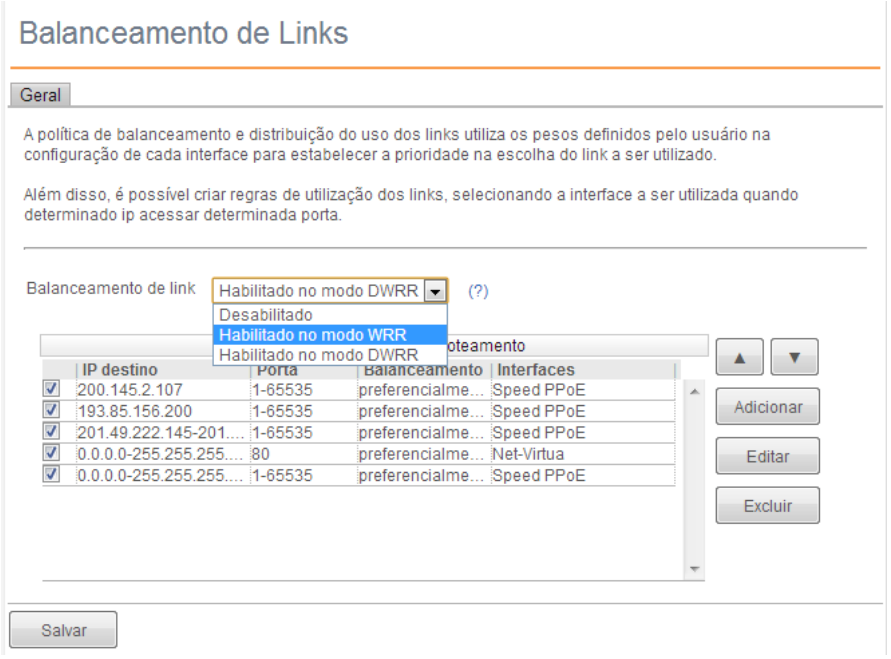
Mesmo que bem facilitada pelo Winconnection, a manuteção de múltiplos links requer alguns cuidados especiais que colaboram na composição e manutenção de um ambiente de rede saudável.

As informações contidas neste manual trarão ao administrador de rede um conjunto valioso de informações que o ajudará no projeto e manutenção de uma rede com múltiplos links de saída.

Como Funciona

A ativação do balanceamento começa com o administrador selecionando quais dos links são externos (responsáveis pela conexão com a internet) na seção *Interfaces*. Após a classificação dos links, o balanceamento de links pode ser ativado.

Uma vez ativado, todas as conexões que necessitarem de uma conexão externa serão avaliadas e um link externo será designado para efetuar a conexão.



O Winconnection disponibiliza dois modos de balanceamento:

- **Modo WRR:** Neste caso, basta especificar uma prioridade diferente para cada interface. Interfaces com prioridades maiores serão mais utilizadas que as de menos prioridade. Neste esquema, não é necessário especificar corretamente a velocidade de cada link. A classificação do link é realizada na noção e bom censo do administrador em especificar a prioridade do link.
- **Modo DWRR:** Neste tipo de balanceamento, um ajuste dinâmico é realizado sobre as prioridades atribuídas as interfaces. Neste caso, além da prioridade de cada link o administrador necessita especificar sua velocidade correta.

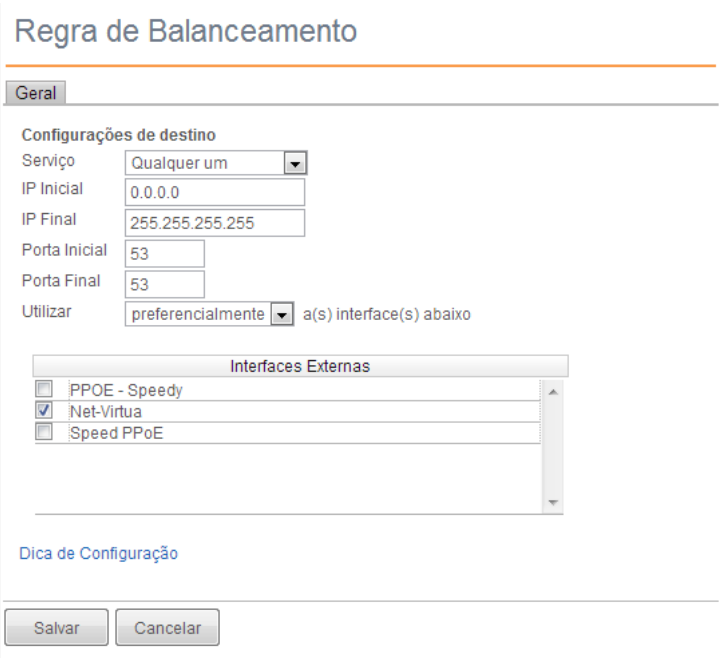
  O Winconnection irá monitorar a banda utilizada do link e ajustará a prioridade do link na intenção de distribuir melhor a carga sobre os links.

Regras de Balanceamento

Uma tabela, conhecida como tabela de regras de balanceamento, pode ser definida pelo administrador. Esta tabela estabelece o processo de escolha do link a ser utilizado, permitindo que links específicos sejam destinados a serviços específicos. Quando a tabela não está definida, todos os links classificados como externos são utilizados no processo de escolha de link.

Uma regra de balanceamento relaciona um range de serviços (range de portas) e um range de IPs de destino a um conjunto de links.

Veja o exemplo abaixo:



Esta regra faz com que todas as conexões destinadas a porta 53 para qualquer IP destino, sejam encaminhadas pela Interface "Net-Virtua".

Se mais de um link for selecionado na regra, o tráfico gerado por esta regra seria balanceados entre os links selecionados.

Detecção de Falhas

Nas regras de balanceamento pode-se especificar como o balanceamento irá se comportar diante de uma falha em um ou mais links. Se os links selecinados na regra forem escolhidos como "preferencialmente", o link selecionado será um da lista apresentada na regra, excluindo-se os links classificados como falhos. Diante de falhas concorrentes a todos os links da regra, qualquer um outro link "externo" disponível no sistema será selecionado. Se, por outro lado, a regra estabelecer que "apenas" os links especificados na mesma deverão ser utilizados, na ocorrência de falhas em todos os links da lista, a conexão não será realizada.

Boas práticas para redes com múltiplas conexões à internet

- **Se possível, tenha conexões com velocidades parecidas:**

  Para utilizar várias conexões ao mesmo tempo, é muito importante que as velocidades de acesso sejam semelhantes. Se não forem, sempre que o usuário pegar a conexão mais lenta, vai achar que a internet está “ruim”, porque estará pior do que era quando ele pegou a conexão rápida.

  Além da velocidade, um fator muito importante, mas bastante desconhecido, é a “latência”. Ela mede o tempo necessário para que um único byte saia do seu computador e chegue num servidor remoto. Embora a latência esteja relacionada à velocidade da conexão, algumas tecnologias possuem uma latência muito elevada para velocidades relativamente altas, como as redes 3G e as conexões via satélite.

  Portanto, se for para usar simultaneamente duas ou mais conexões, procure não misturar banda larga terrestre (ADSL, cabo, IP direto, rádio) com tecnologias 3G e satélite, porque o resultado não é bom. Se não houver dois provedores de links terrestres na sua região, é melhor operar no modo “backup”, ou “fail-over”. Neste modo, a conexão pior só é usada quando a principal está ruim.

- **Defina os serviços de e-mail com uma conexão preferencial:**

  Servidores de e-mail são bastante sensíveis ao endereço de origem das conexões por causa de problemas como SPAM e autenticação. Se você configurar os serviços de e-mail para utilizar cada vez uma conexão diferente, podem ocorrer erros de entrega de mensagens que não são fáceis de reproduzir, e isto irá dificultar o diagnóstico. Além disso, normalmente o tráfego de e-mail não é muito relevante perto do total e sendo assim não há vantagens em distribuí-lo por várias conexões.

- **Problemas gerados pelo acesso a partir de vários endereços IP:**

  Ao utilizar múltiplas conexões internet simultaneamente, a rede é percebida pelos servidores internet como se fossem várias redes desconectadas. Isto ocorre porque cada conexão internet tem o seu próprio IP, e este comportamento pode gerar problemas. O Winconnection está preparado para lidar com estas questões automaticamente:

  - *Acesso ao servidor DNS do provedor:*

    Este é um servidor disponibilizado pelo seu provedor de acesso para que sua conexão funcione, traduzindo em endereços IP os nomes dos sites acessados. No momento em que se estabelece uma conexão com a internet, o endereço IP do servidor DNS é passado do seu provedor para o seu roteador ou gateway. Cada servidor DNS só responde às requisições feitas através da conexão do próprio provedor. Porém, como o Windows não entende esta restrição, ele irá tentar acessar o servidor DNS de um provedor através da conexão do outro provedor e isso causa problemas.

  - *Sessões dos usuários:*

    Este é um problema muito comum em sistemas de internet banking. Quando um usuário faz o login no site do banco, o endereço IP usado para acessar o banco é registrado na sessão do usuário. Se este endereço IP mudar, o banco muitas vezes considera que a sessão foi encerrada e joga o usuário para a tela de login novamente. Para que este tipo de site funcione, é necessário manter uma tabela que enumera as sessões abertas pelo usuário nos sites remotos, e utilizar sempre a mesma conexão que estiver associada à sessão do usuário.

Dicas de Configuração:

Criando regra para qualquer destino da internet:

- IP Inicial: 0.0.0.0
- IP Final: 255.255.255.255

Criando regra para todas as portas:

- Porta Inicial: 1
- Porta Final: 65535

7.4 NAT Reverso (DMZ)

O Firewall do **Winconnection 7** vem configurado de forma a proteger a interface de rede externa contra ataques em todas as portas.

Para liberar uma porta no firewall, basta criar uma regra de entrada. Além disso, é possível criar regras de redirecionamento (porta mapeada).

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.

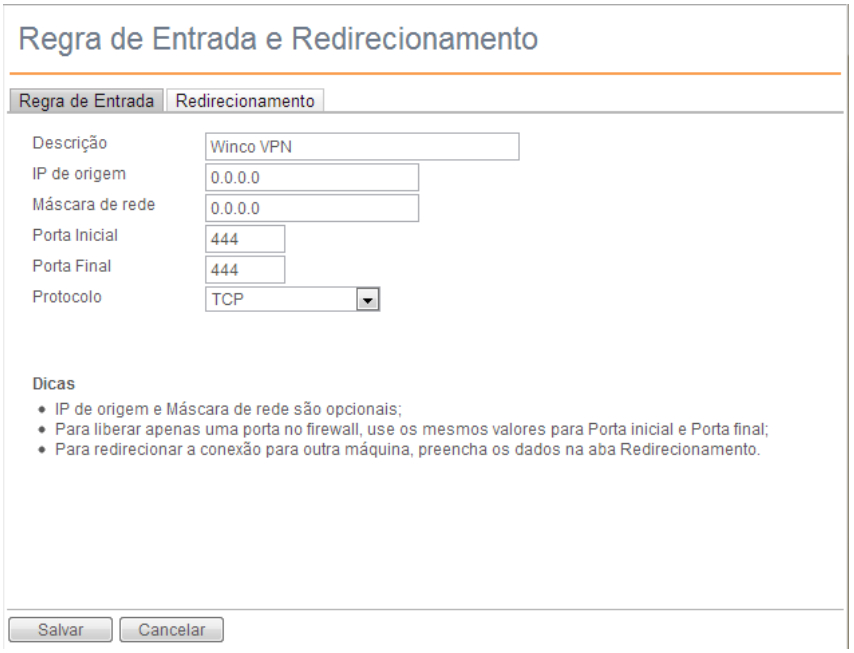
Ao adicionar/editar uma regra, as seguintes opções estão disponíveis:

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 7**.



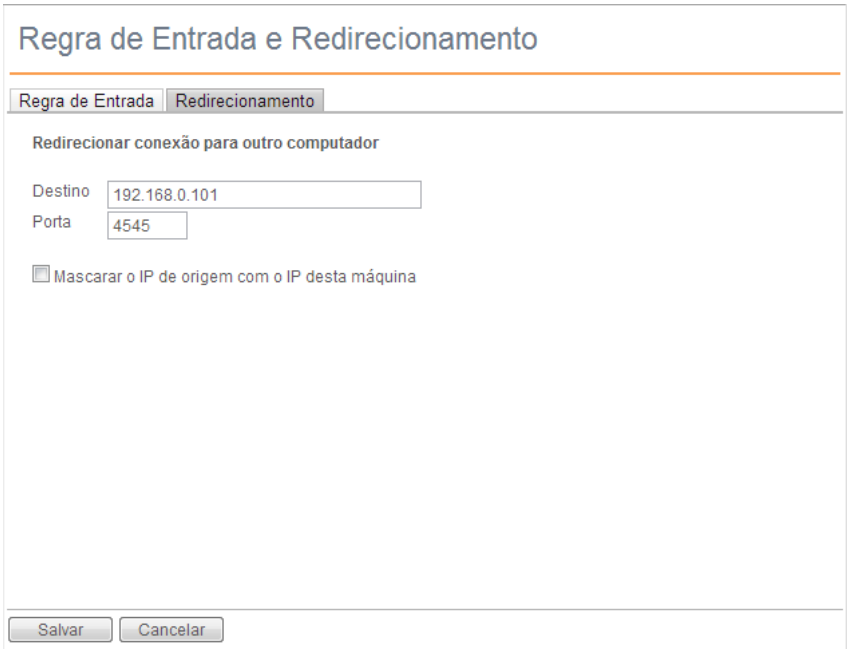
Guia Redirecionamento:

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 7, 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.


Regra de Entrada e Redirecionamento
Regra de Entrada
Redirecionamento
Redirecionar conexão para outro computador
Destino
192.168.0.101
Porta
4545
Mascarar o IP de origem com o IP desta máquina
Salvar
Cancelar

7.5 NAT de Saída

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Guia 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.

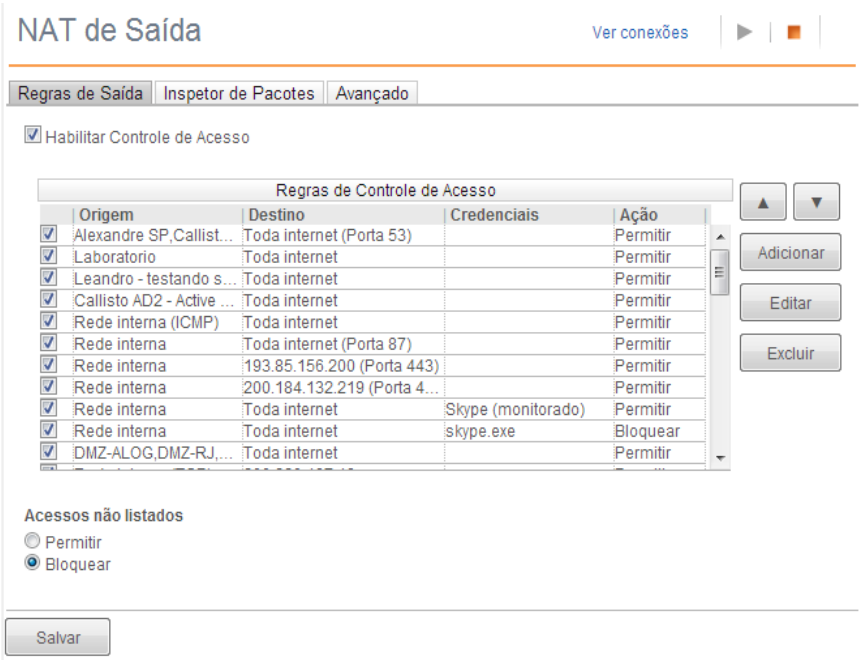
Por padrão, o **Winconnection 7** permite que todas as estações tenham acesso a todos os programas. Como o serviço Proxy Transparente deixa a estação como "conectada diretamente à internet", o administrador da rede pode impedir que determinadas estações acessem determinados programas ou serviços.

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.

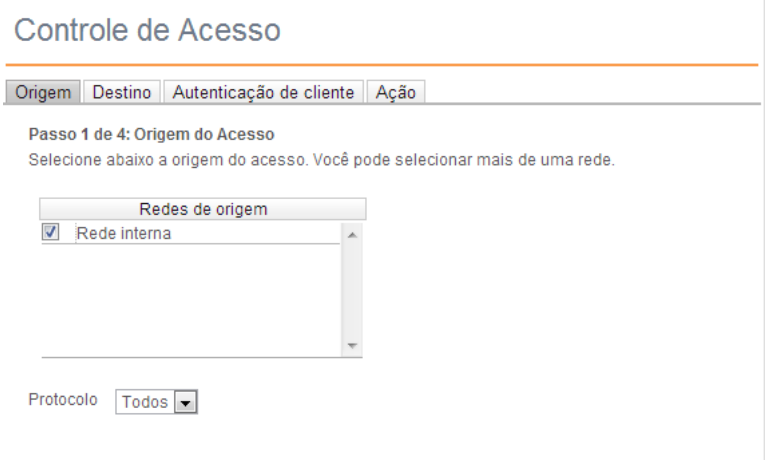
- **Permitir apenas os casos abaixo:** Quando o administrador cria a regra, pode permitir o acesso ao serviço somente para os casos digitados no campo logo abaixo. Esta opção pode ser utilizada quando o administrador não quer que os usuários fiquem conectados diretamente à internet, via Proxy Transparente e/ouSocks 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*.

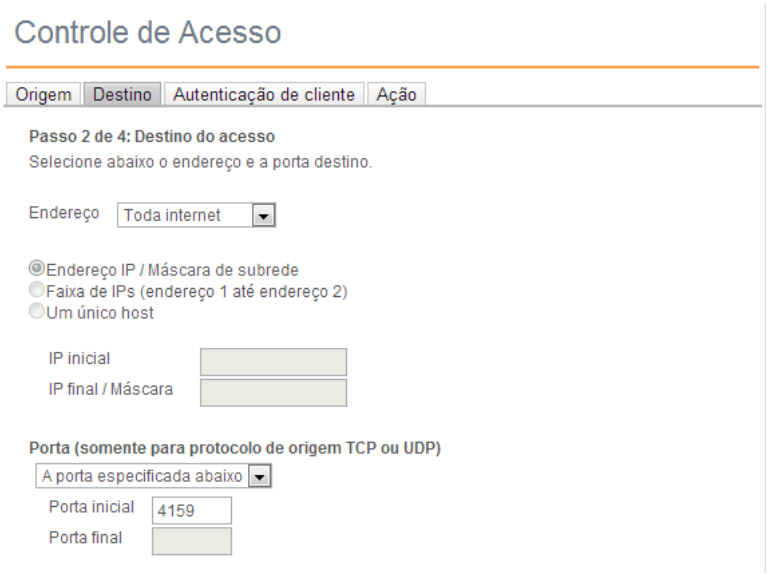


Ao adicionar ou editar uma regra de controle de acesso, será aberto um assistente com dois passos de configuração:

- **Passo1 - Origem:**
  - **Origem do Acesso:** Nesse campo, é necessário definir uma ou mais redes que será a origem do acesso. É possível definir mais do que uma rede.
  - **Protocolo:** Defina qual o protocolo será utilizado nesta regra. Se o protocolo escolhido for *Todos*, a porta de destino escolhida não será levada em consideração.



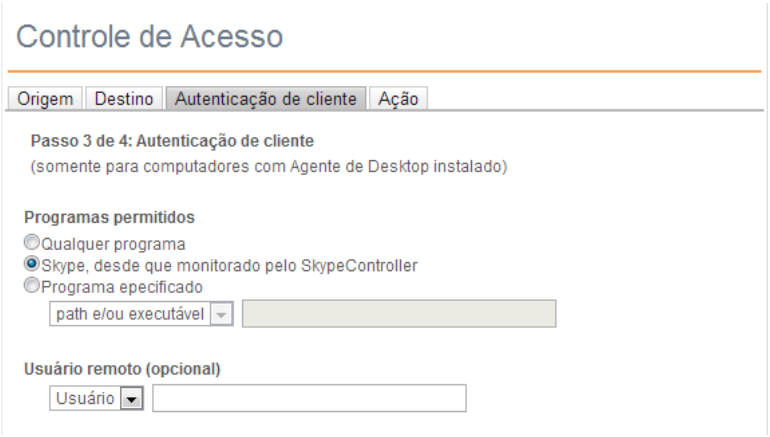
- **Passo 2 - Destino do acesso:**
  - **Endereço:** Neste campo, é necessário definir o endereço do destino.
  - **Porta (somente para protocolo de origem TCP ou UDP):** Neste campo, é necessário definir a porta do destino.



- **Passo 3 - Autenticação de cliente:**

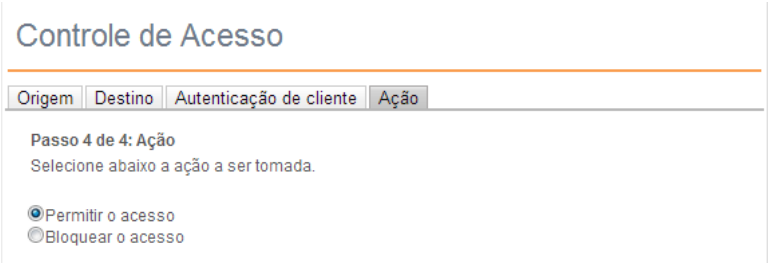
  Esse passo é destinado somente para os computadores com o Agente de Desktop instalado.

  - **Programas permitidos:**
    - **Qualquer programa:** Permite a conexão de qualquer programa.
    - **Skype, desde que monitorado pelo SkypeController:** Ao habilitar esta opção, será permitido o uso do Skype somente de maneira monitorada. Somente as estações que tiverem o *Skype Controller* instalado conseguirá acessar o Skype.
    - **Programa especificado:** permitir que um programa se conecte na internet cadastrando uma descrição (exemplo: "Firefox") ou um caminho (exemplo: C:\Program Files (x86)\Mozilla Firefox\firefox.exe).
  - **Usuário Remoto:** Permitir o acesso somente para um determinado usuário.



- **Passo 4: Ação:**

  Neste passo, o administrador da rede deve definir se o acesso da regra que está sendo criado será permitido ou bloqueado.



Guia Inspetor de Pacotes:

Para garantir maior segurança, os pacotes que trafegam para a internet podem ser analisados e o protocolo identificado. Assim o controle dos pacotes de dados é feito não só por portas de origem e destino mas pelo protocolo efetivamente utilizado. Com isso, o Winconnection evita que o usuário tente burlar as regras de saída usando, por exemplo, o protocolo HTTP em porta diferente da porta padrão.

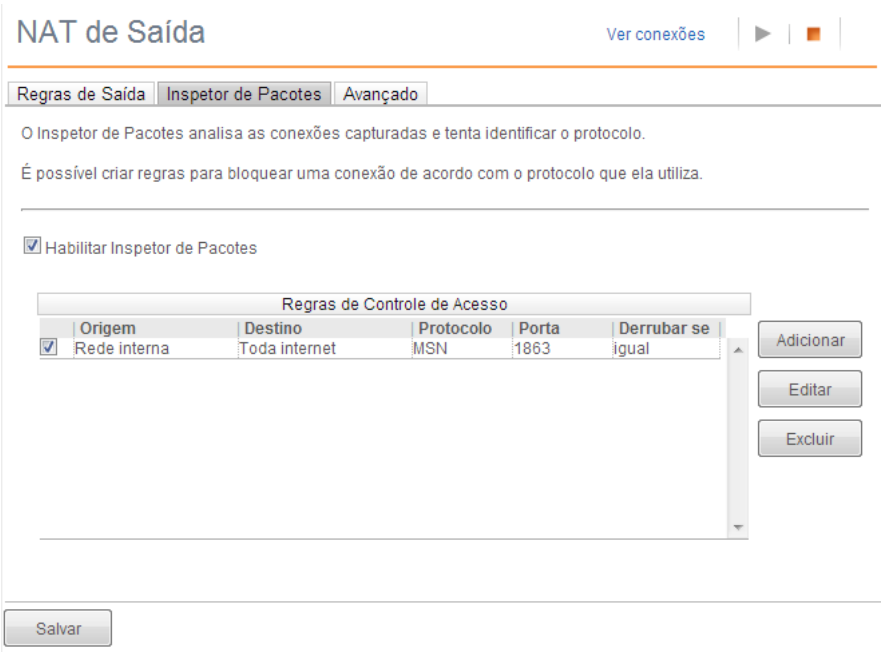
Nesta guia é possível habilitar a "Inspeção de Pacotes". Com base nas regras criadas, o Inspetor de Pacotes pode derrubar conexões dependendo do seu protocolo.

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:



Guia Avançado:

- **Máscara de rede do compartilhamento:** aqui o administrador pode definir a máscara de rede do compartilhamento da internet.
- **Salvar LOG em "LOGS/TPROXY.LOG":** O arquivo em bloco de notas *(TPROXY_TCP.LOG)* será criado no diretório *C:/Arquivos de programas/Winco/Winconnection 7/LOGS* e conterá todas as informações referentes a este serviço.

7.6 Controle de Banda

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Aliado ao balanceamento de carga, o Winconnection oferece controle de banda, garantindo a qualidade de serviço (QoS). Esta é obtida com reserva banda ou definição de diferentes níveis de prioridade a serviços ou usuários.

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.

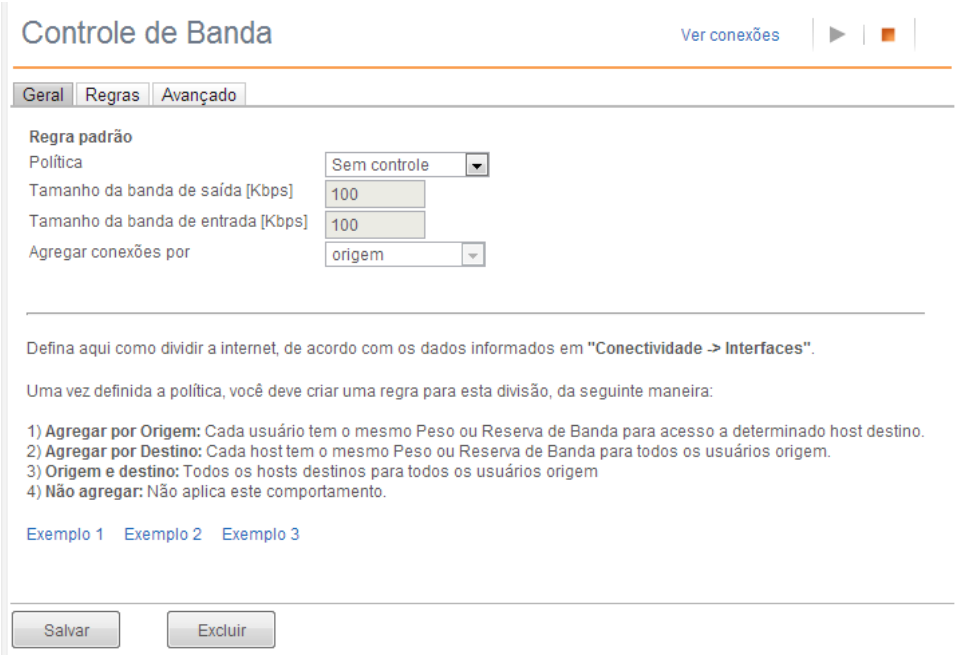
A *Banda Nominal* de cada interface é definida em *"Firewall / Interfaces"*.

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"*.

As regras podem ser criadas para reservar parte da banda internet para os serviços do **Winconnection 7**, como Servidor de E-mail, Navegação e outros serviços.

Guia Geral:

- **Política:** Neste campo é necessário o tipo da política da regra:
    - **Reserva de banda:** Em todas as políticas, é possível estabelecer uma prioridade as conexões. Quando associadas a prioridades diferentes, todas conexões de uma dada conexão serão avaliadas e ativadas, enquanto as demais com prioridades inferiores serão pausadas. Por esta razão, o uso de prioridades elevadas destina-se a processos prioritários que não tenham tendência a monopolizar os links.
    - **Limitado:** Nesta políticas as conexões são limitadas ao valor determinado na regra.
    - **Sem controle:** Esta política determina que as conexões classificadas como tal não devam alvo de quaisquer controle de banda. Como não é possível implementar a reserva de banda, sem que outras conexões afetradas, as conexões "sem controle" funcionarão livres a menos que uma ou mais conexões "reservadas" estejam em curso.
- **Tamanho da banda de saída[kbps]:** Neste campo é informada a banda que será reservada para saída (upload).
- **Tamanho da banda de entrada[kbps]:** 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.

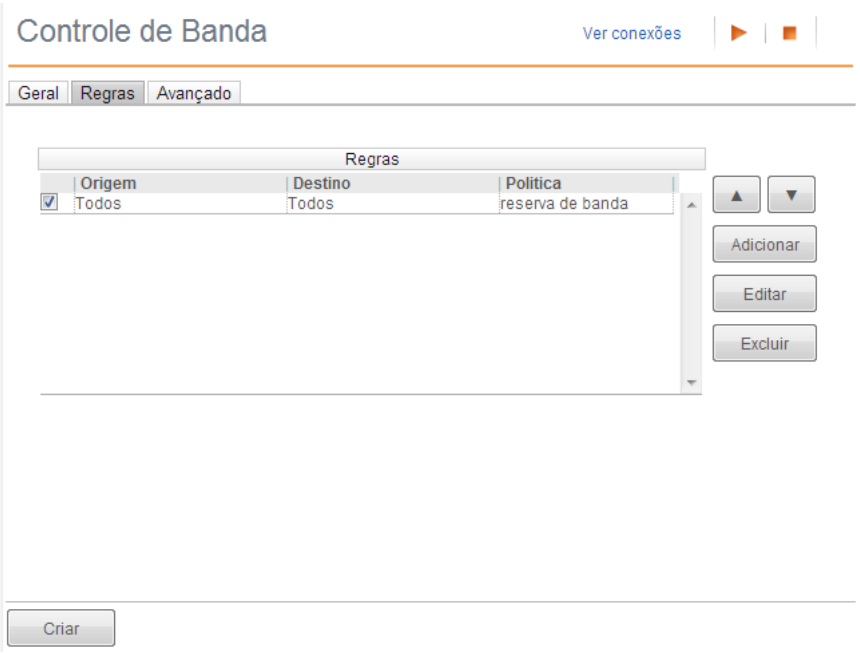


Guia Regras:

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

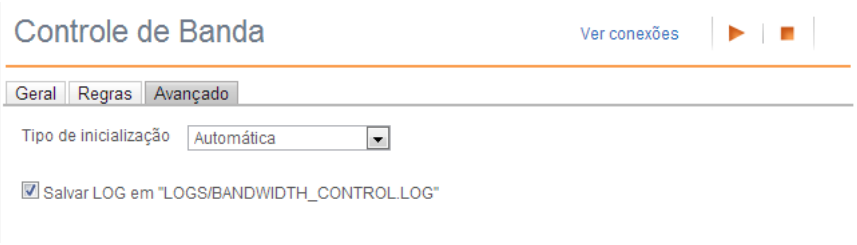
As regras são criadas ou editadas em 3 passos:

- **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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **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 7/LOGS* e conterá todas as informações referentes a este serviço.



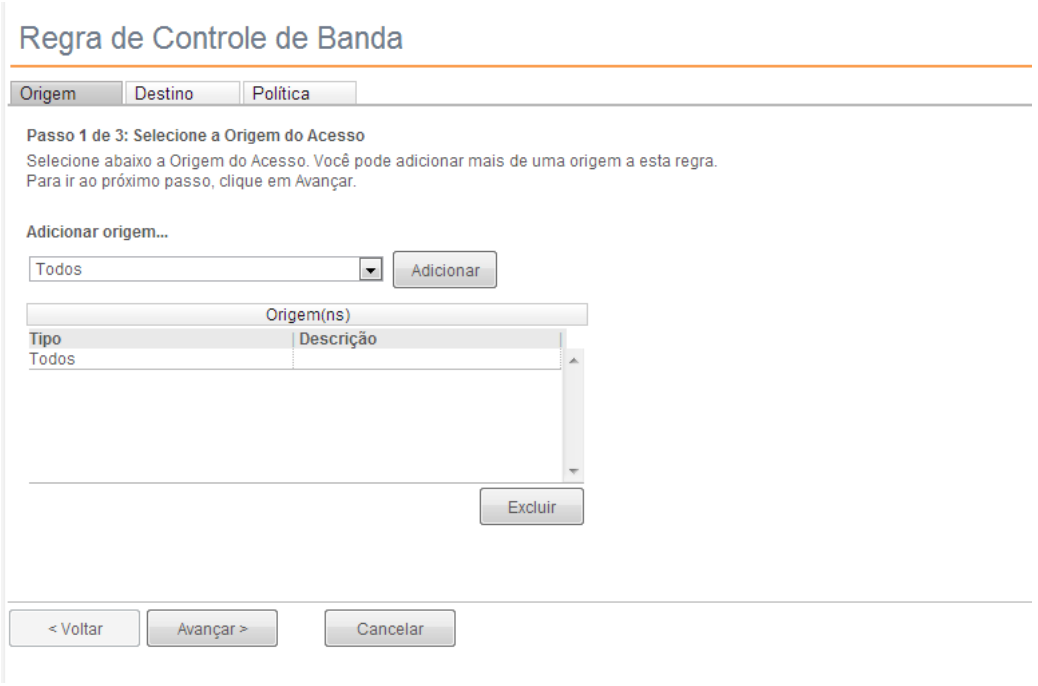
7.6.1 Exemplos de Utilização

Exemplo 1: Agregando a Origem

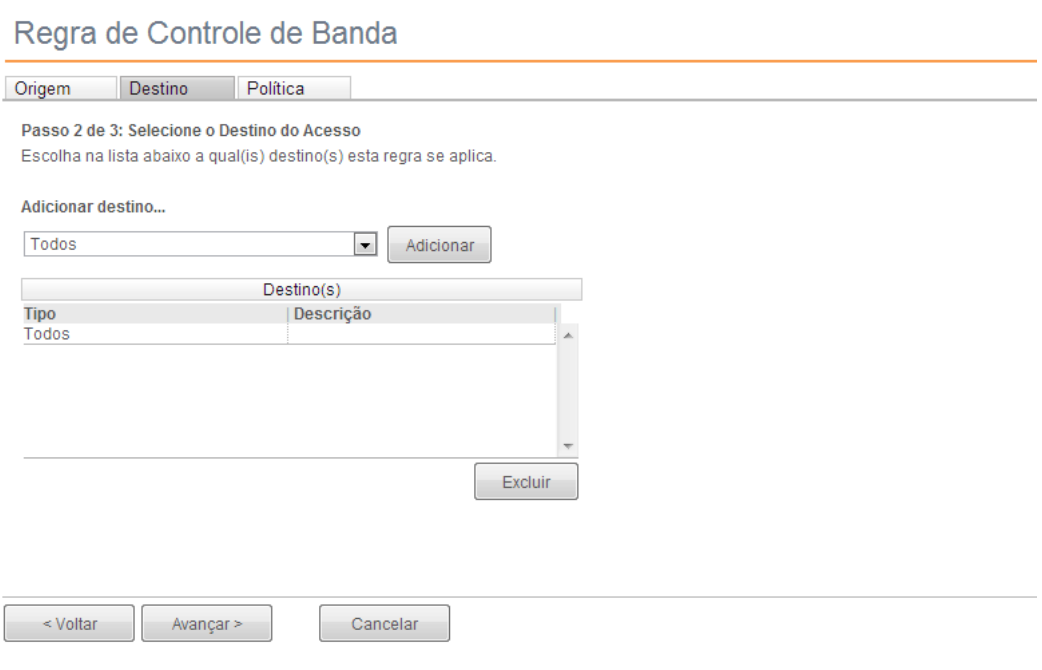
Queremos uma reserva de banda para 3 IPs internos, de 200K, para os destinos 10.10.10.10 e 10.10.10.20.

As formas e regras ficam assim:

Regra 121:
Origem: Todos



Destino: Todos



Agregador: Origem

Banda Reservada: 200 kbps

Fatia 1:

Origem: 192.168.0.10,
Destino: {10.10.10.10, 10.10.10.20},
Banda: 200 kbps

Fatia 2:
Origem: 192.168.0.20,
Destino: 10.10.10.10,
Banda: 200 kbps

Fatia 3:
Origem: 192.168.0.30,
Destino: 10.10.10.10,
Banda: 200 kbps

Exemplo 2: Agregando o Destino

Queremos dar somente 200Kb para um destino, e 200k para outro, dividindo para 3 IPs internos.

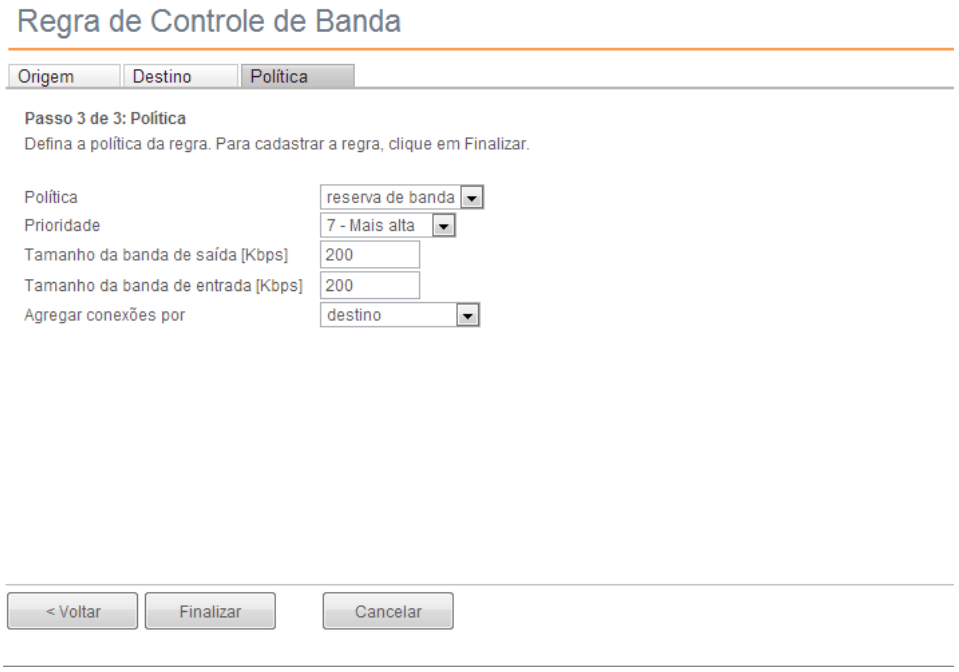
As formas e regras ficam assim:

Regra 334:
Origem: Todos

Destino: Todos

Agregador: Destino

Banda Reservada: 200 kbps



Fatia 1:
Origem: {192.168.0.10, 192.168.0.20, 192.168.0.30},
Destino: 10.10.10.10;
Banda: 200 kbps

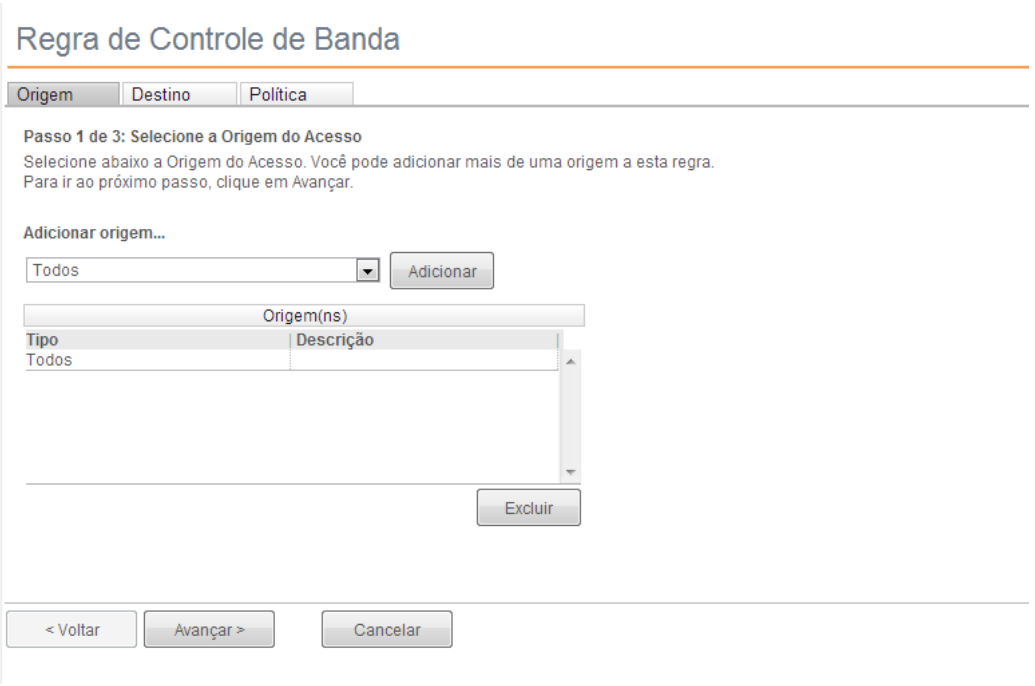
Fatia 2:
Origem: 192.168.0.10,
Destino: 10.10.10.20;
Banda: 200 kbps

Exemplo 3 - Agreagando a Origem e Destino

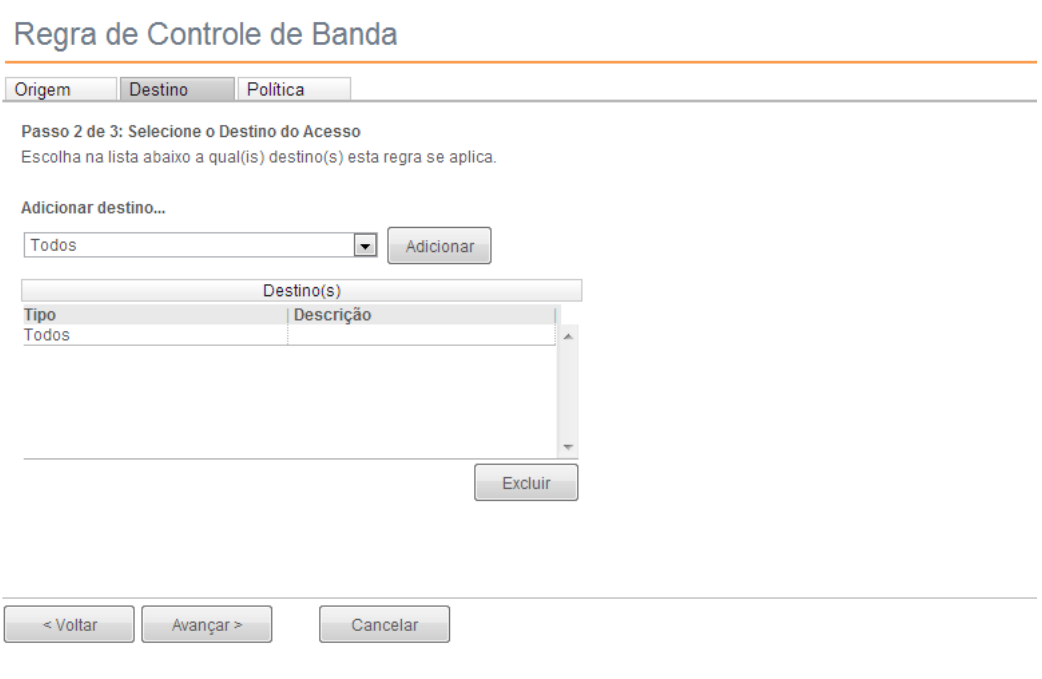
Queremos dar 200Kb para 2 destinos, dividindo para 3 IPs internos.

As formas e regras ficam assim:

Regra 223:
Origem: Todos

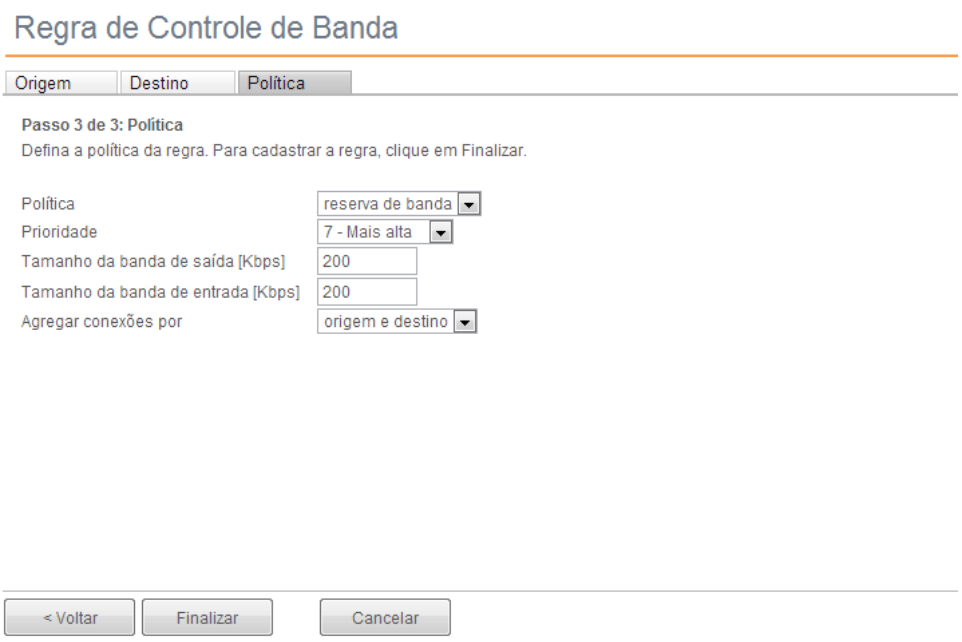


Destino: Todos



Agregador: Origem e Destino

Banda Reservada: 200 kbps



Fatia 1:
Origem: {192.168.0.10, 192.168.0.20, 192.168.0.30},
Destino: {10.10.10.10, 10.10.10.20};
Banda: 200 kbps

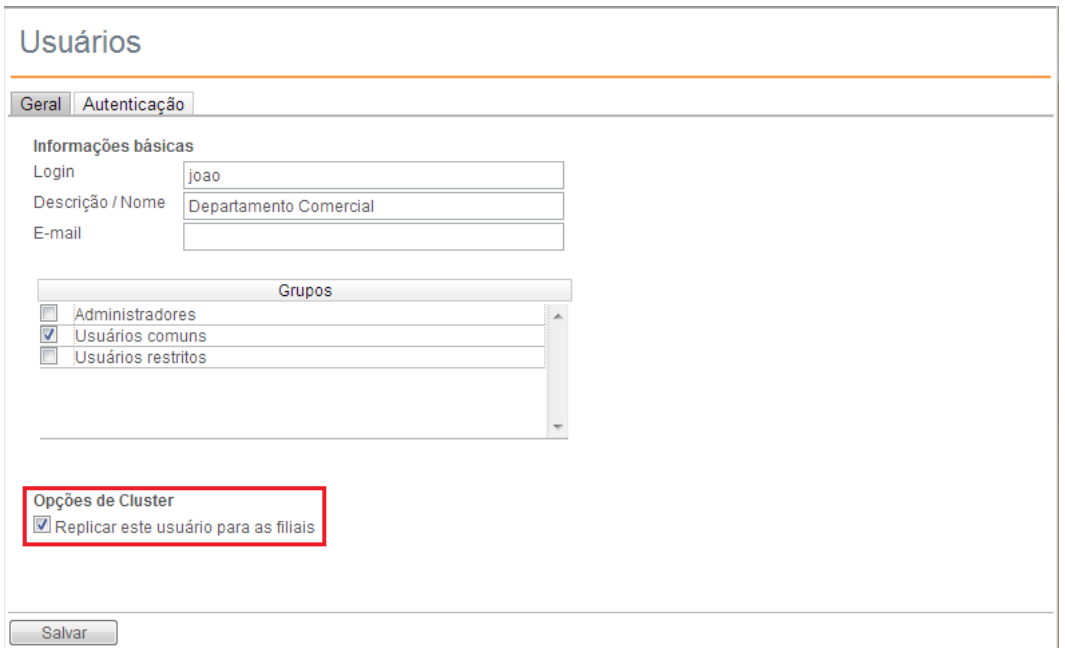
7.7 Cluster Master

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.

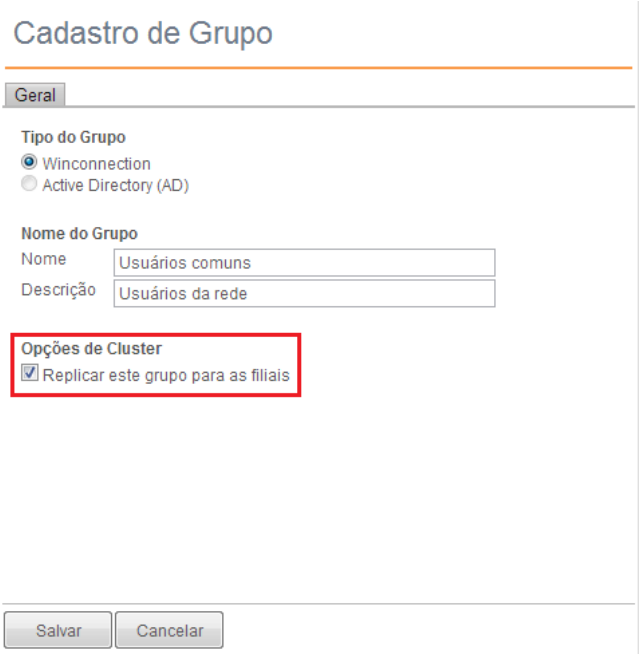
Para consultar as conexões ativas, basta clicar no menu Ver conexões.

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.



- **Grupos** – desde que a opção *"Replicar este grupo para as filiais"* esteja habilitada no cadastro do usuário.



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

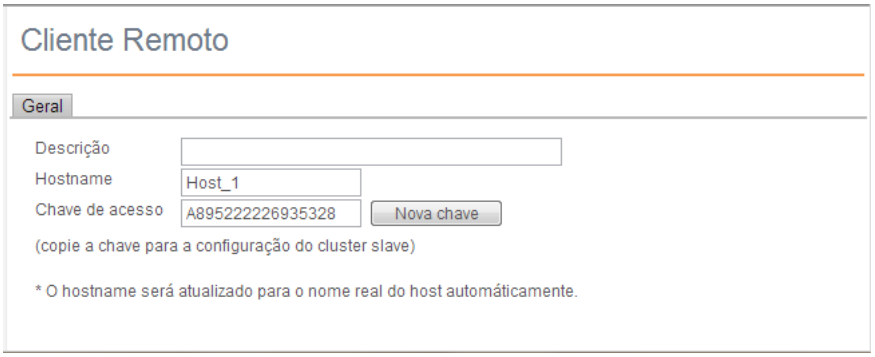
Guia Geral:

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:

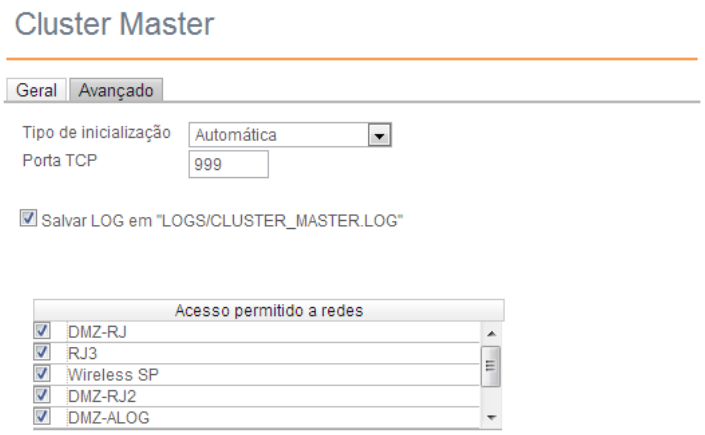
Informações do Winconnection Slave:

- **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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta TCP:** A porta padrão para este serviço é 999, mas pode ser alterada nesse campo.
- **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 7/LOGS* e conterá todas as informações referentes a este serviço.
- **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.



7.8 Cluster Slave

O serviço Cluster Slave deve ser instalado no **Winconnection 7** da filial que irá receber automaticamente as configurações realizadas no Winconnection da matriz.

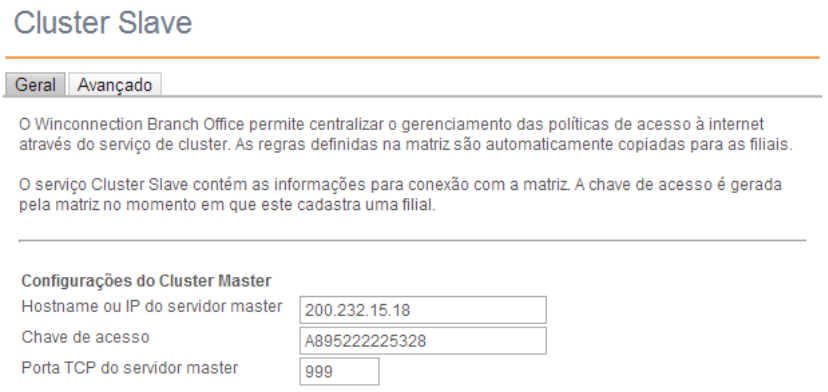
Obs.: A instalação desse serviço depende de uma licença especial, pois o serviço de replicação de configuração é um módulo adicional e deve ser adquirido separadamente.

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Guia Geral:

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 7** 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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **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 7/LOGS* e conterá todas as informações referentes a este serviço.

7.9 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 7** a conexão será redirecionada ao computador remoto na porta especificada como "*destino do PIPE*".

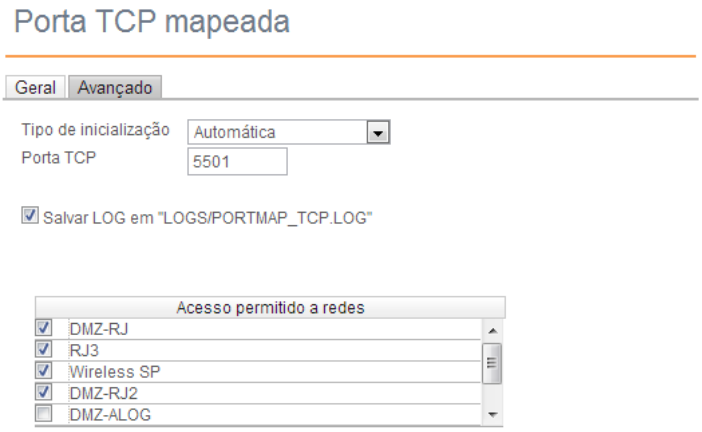
Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Guia 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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta TCP:** É a porta externa que responderá às requisições.
- **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 7/LOGS* e conterá todas as informações referentes a este serviço.
- **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.



7.10 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.

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Guia 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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta TCP:** É a porta externa que responderá às requisições.
- **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 7/LOGS* e conterá todas as informações referentes a este serviço.
- **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.

7.11 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 7 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.

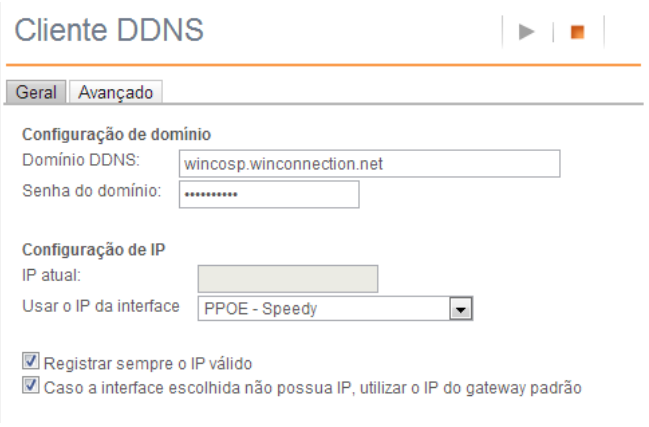
O pacote de instalação do **Cliente DDNS** está disponível na seção de download do nosso site.

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

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

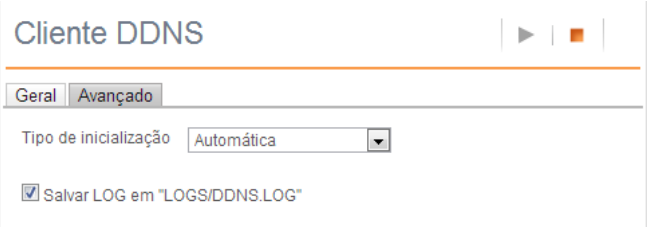
Guia Geral:

- **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.
- **Caso a interface escolhida não possua IP, utilizar o IP do gateway padrão:** Esta opção deve ser habilitada para o IP do gateway padrão ser utilizado se a interface escolhida não possuir IP válido.



Guia Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Salvar LOG em "LOGS/DDNS.LOG":** O arquivo em bloco de notas (DDNS.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 7\LOGS* e conterá todas as informações referentes a este serviço.


Cliente DDNS
Geral
Avançado
Tipo de inicialização
Automática
Salvar LOG em "LOGS/DDNS.LOG"

7.12 Servidor VPN-SSL

O Sistema de VPN do **Winconnection 7** 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 7** 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.

Para configurar a VPN, execute o Assistente de Configuração da VPN disponível no menu Iniciar | Todos os Programas | Winco | Winconnection 7.

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Configurações | Geral:

Configurações do Servidor VPN:

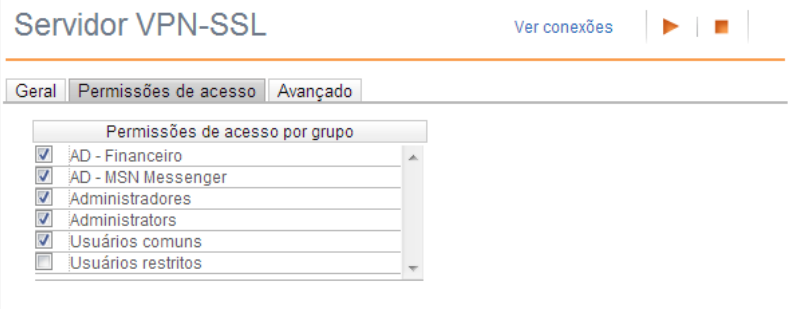
- **IP da interface local:** Neste campo, o administrador da rede deve digitar o endereço IP da interface local.
- **Máscara da interface local:** Neste campo, o administrador da rede deve digitar a máscara da interface local.
- **Primeiro IP para alocar:** É necessário separar uma faixa de endereços 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 Permissões de acesso:

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



Guia Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.

- **Porta:** Neste campo é definido a porta de acesso para o Servidor VPN. A porta padrão é a 444, mas pode ser alterada.
- **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 7/LOGS e conterá todas as informações referentes a este serviço.
- **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.

7.13 Cliente VPN-SSL

O serviço *Cliente VPN* deve ser instalado no **Winconnection 7** do computador que irá acessar o *Servidor VPN*.

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Guia Geral:

Configurações do Cliente VPN:

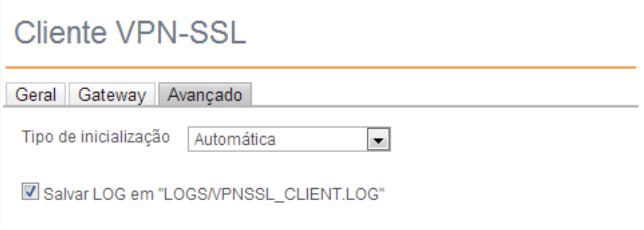
- **Servidor de VPN:** Neste campo é necessário digitar o hostname ou o endereço IP do servidor de VPN.
- **Porta:** Neste campo, é necessário definir a porta de acesso do Servidor VPN (normalmente 444).
- **Usuário:** Neste campo, o administrador da rede deve digitar o usuário que tenha acesso ao servidor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

Guia Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **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 7/LOGS* e conterá todas as informações referentes a este serviço.



7.14 Servidor SOCKS 5

O **Servidor Socks 5** é um protocolo padrão de Gateway para conexões tipo Socks 5 na internet que permite receber uma conexão vindo de fora desde que haja um programa na rede interna esperando a conexão.

Atenção: Esse serviço é obrigatório quando se instala o *Filtro de Skype e MSN* em um computador que não seja o Gateway de internet da rede. Para mais informações, consulte o tópico *Filtro de Skype e MSN*.

Guia 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 é uma função típica do serviço Socks 5. Este controle concede ao administrador direitos de permitir ou proibir as estações da rede acessarem ou não a um determinado serviço.

- **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.

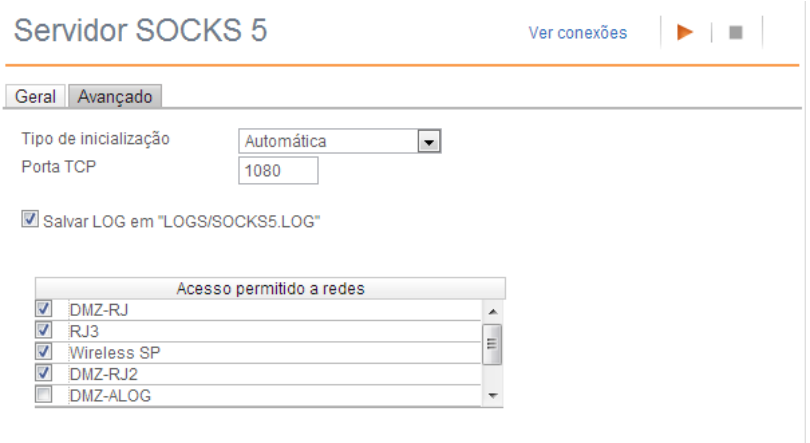
  Esta opção pode ser utilizada quando o administrador não quer que os usuários fiquem conectados diretamente à internet, via Proxy Transparente e/ou Socks 5. Porém, existe aplicativo específico na estação que exige um dos serviços acima para funcionar corretamente. Neste caso, ele permite um usuário,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

Guia Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta:** Neste campo é definido a porta de acesso para o Servidor VPN. A porta padrão é a 1080.
- **Salvar LOG em "LOGS/SOCKS5.LOG":** O arquivo em bloco de notas (SOCKS5.LOG) será criado no diretório C:/Arquivos de programas/Winco/Winconnection 7/LOGS e conterá todas as informações referentes a este serviço.
- **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 Serviços

8.1 Filtros

8.1.1 E-mail

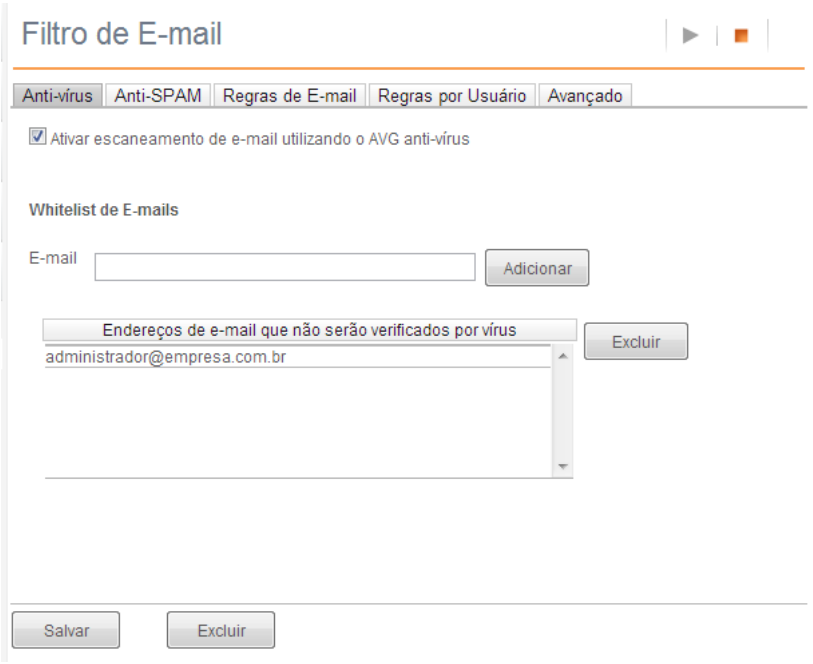
O serviço *Filtro de E-mail* disponibiliza uma série de configurações que poderão ser utilizadas nos e-mails.

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Guia Antivírus:

Esta guia possui as seguintes configurações:

- **Ativar escaneamento de e-mail utilizando o AVG anti-vírus:** O **Winconnection 7** 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.
- **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 Anti-SPAM:

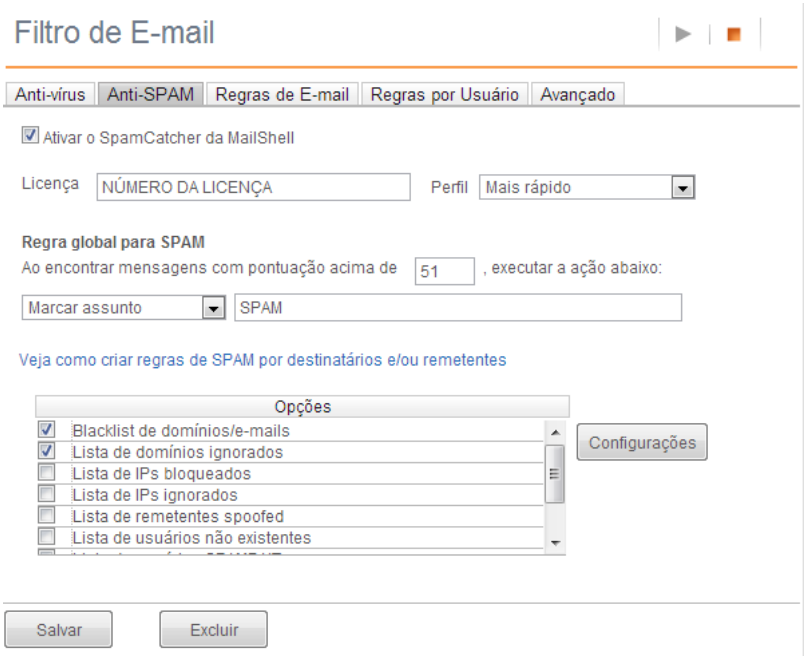
A guia de configuração *Anti-Spam* possui as seguintes funções:

- **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 global para SPAM:**
  - **Ao encontrar mensagens com pontuação acima de [ ], executar a ação abaixo:** 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, caso ele queria aplicar a mesma regra para todas as mensagens. As ações possíveis são: *Marcar assunto, Mover para Quarentena*, *Deletar a mensagem*, *Copiar para*, *Mover para*.

    Para criar regras de SPAM diferenciadas por destinatário, siga os procedimentos de acordo com o modelo de regras utilizado na sua instalação (selecionável na aba *Regras de E-mail*).

    1) Usando regras avançadas e por usuário: Utilize o campo *"Pontuação do Anti-Spam"*, na aba *[Mais filtros]* na hora que estiver criando a regra de e-mail;

    2) Usando regras globais e por grupo: Utilize o campo próprio para isso nas regras de entrada dos grupos.
- **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 Regras de E-mail:

O processamento dos emails recebidos pelo servidor SMTP e pelo POPMAP do **Winconnection 7** passa pelas seguintes etapas:

- **Filtro Antivírus.**
- **Anti-Spam.**
- **Expansão de listas:** Caso algum destinatário da mensagem seja uma lista de distribuição, esta é expandida de forma a serem conhecidos os destinatários finais da mensagem (sejam estes usuários locais ou remotos).
- **Regras de e-mail**: Neste momento, é executado o filtro de regras avançadas, que é avaliado uma vez para cada destinatário final da mensagem. Cada destinatário recebe sua cópia da mensagem da forma que o filtro permitir.

  As regras avançadas de e-mail são criadas seguindo o assistente de configuração que possui 5 passos:

  - **Passo 1 - Geral:** Digite um nome ou uma descrição para a regra.
  - **Passo 2 - Remetente:** É possível adicionar mais de um remetente a esta regra.
  - **Passo 3 - Destinatário:** É possível adicionar mais de um destinatário a esta regra.
  - **Passo 4 - Mais filtros:** Nesta etapa é possível definir se filtros de cabeçalhos (header) serão adicionados na regra.
  - **Passo 5 - Ação:** Defina qual ação deve ser tomada (o*bservação:* Para ação "*Mover mensagem para a pasta IMAP do usuário"* a pasta deve existir, caso contrário a mensagem será entregue na caixa de entrada do usuário).
    - **Continuar processamento de regras:** No **Winconnection 7** é possível continuar o processamento das regras mesmo quando uma regra for aplicada. Essa opção é configurada dentro de cada regra. Regras com ações como a de excluir mensagem ou mover para quarentena não permitem continuar o processamento, pois retiram a mensagem da fila.

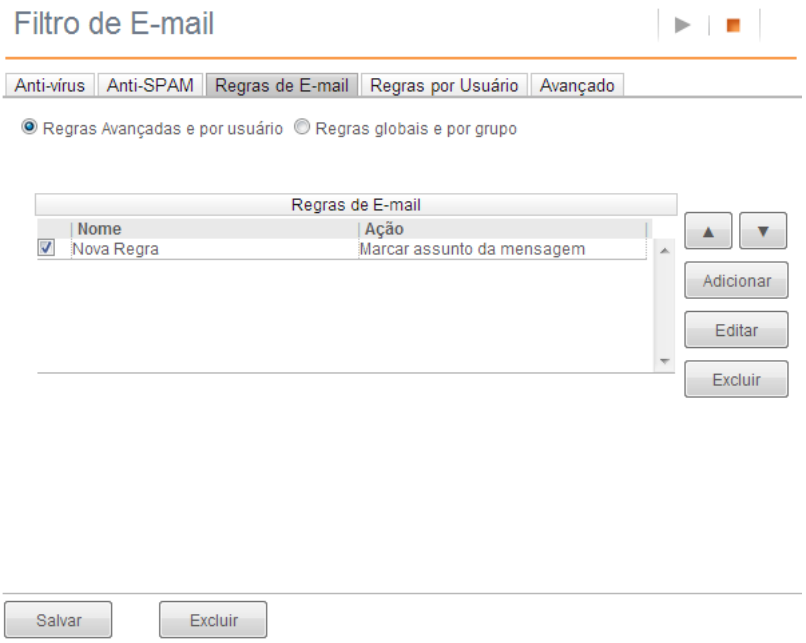
  Algumas dicas importantes sobre as regras avançadas:

  1 - Quando a mensagem é enviada para uma lista que é direcionada ao usuário final, o parâmetro *E-mail* da aba [Destinatário] irá conter o e-mail ORIGINAL da lista. Portanto, para todas as mensagens para o usuário, utilize o campo *Usuário* e para filtrar apenas mensagens recebidas através da lista, utilize o campo *E-mail*.

  2 - Para filtrar todas as mensagens enviadas para fora da empresa, selecione na aba [Remetente] a opção *Rementente interno* e na aba destinatário a opção *Destinatário externo*. Da mesma forma, para selecionar todas as mensagens recebidas de fora da empresa, selecione na aba [Rementente] a opção *Remetente externo* e na aba [Destinatário] a opção *Destinatário interno*.

  3 - Quando uma mensagem é copiada ou movida para um novo destinatário, ela é resubmetida na fila de mensagens DEPOIS do filtro anti-spam. Portanto, a expansão das listas de distribuição é feita e em seguida, as regras de e-mail são aplicadas novamente para o novo destinatário. É como se a mensagem tivesse sido encaminhada de fora, tirando o fato que o remetente original é PRESERVADO.

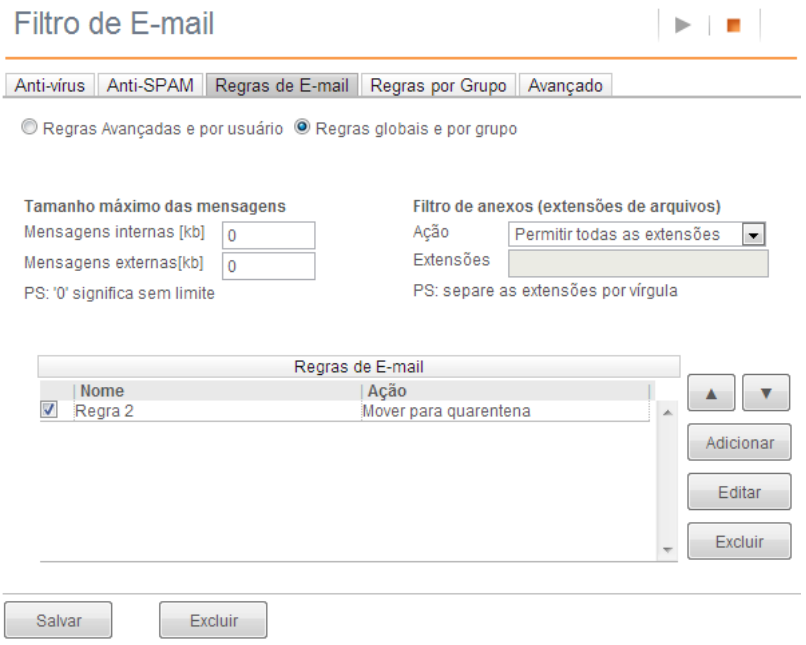
  4 - Regras por usuário: O administrador pode criar regras para serem aplicadas a um único usuário para cada mensagem que ele receber. Estas regras do usuário também podem ser editadas pelo próprio usuário no seu painel de controle e a presença desta aba no administrador tem o intuito de permitir que o administrador dê um suporte melhor aos seus usuários. Não existe regra por usuário para mensagens enviadas por ele.



- **Regras globais e por grupo:** É possível criar regras de acordo com cada grupo de usuários.

  Ao selecionar esta opção, o **Winconnection 7** 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.



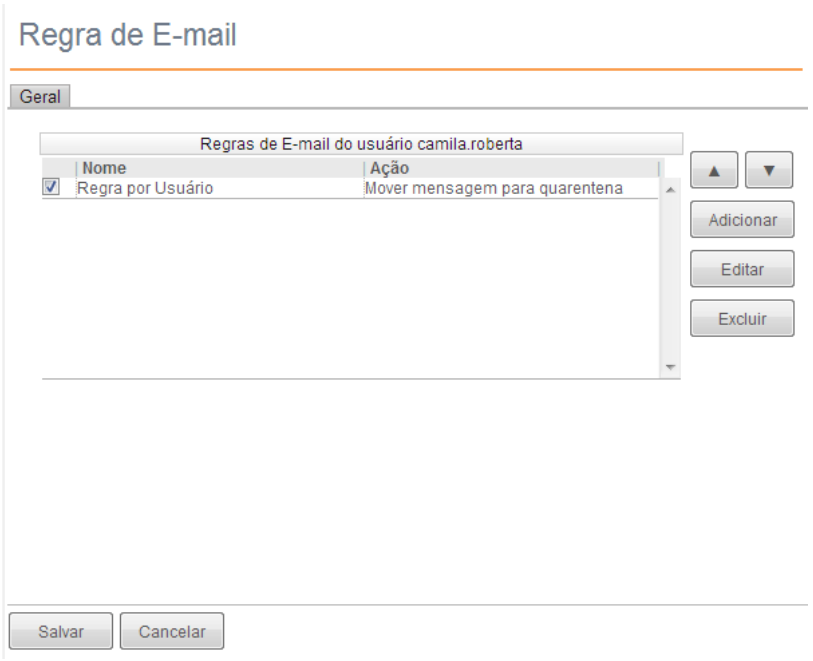
Guia Regras por Usuário/Grupo:

As regras dos usuários ou grupos são executadas por último. Sendo assim, uma *Regra Avançada* pode anular uma *Regra do Usuário/Grupo*.

As **Regras por Usuário/Grupo** são criadas seguindo o Assistente de Configuração que possui 3 passos:

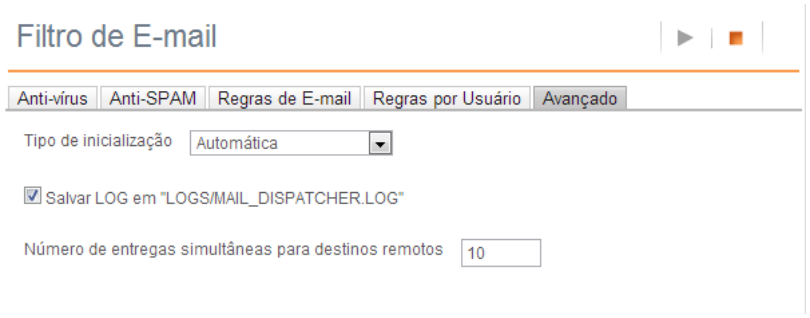
- **Passo 1 - Geral:** Digite um nome ou uma descrição para a regra.
- **Passo 2 - Filtros:** Defina nesta etapa quais quais outros critérios devem ser atendidos.
- **Passo 3 - Ação:** Defina qual ação deve ser tomada (*observação:* Para ação "*Mover mensagem para a pasta IMAP do usuário"* a pasta deve existir, caso contrário a mensagem será entregue na caixa de entrada do usuário).
  - **Continuar processamento de regras:** No **Winconnection 7** é possível continuar o processamento das regras mesmo quando uma regra for aplicada. Essa opção é configurada dentro de cada regra. Regras com ações como a de excluir mensagem ou mover para quarentena não permitem continuar o processamento,

pois retiram a mensagem da fila.



Guia Avançado:

- **Tipo de Inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **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 7/LOGS e conterá todas as informações referentes a este serviço.
- **Número de entregas simultâneas para destinos remotos:** Quando a quantidade de mensagens para destinos remotos (fora da rede local) é muito grande, é importante aumentar o número de entregas simultâneas. Com isto, o uso da conexão é otimizado, em detrimento dos usuários que desejam navegar enquanto as mensagens são transmitidas.



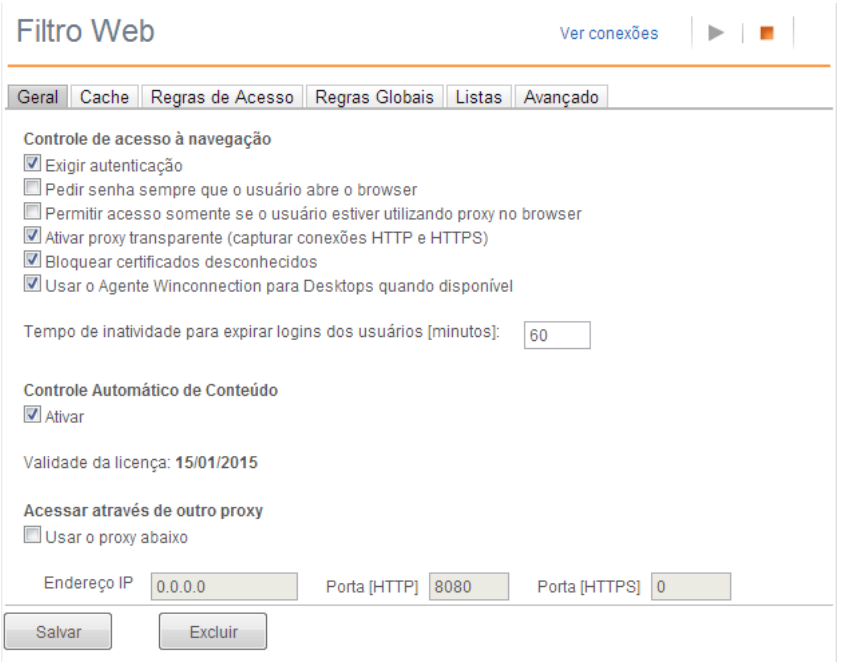
8.1.2 Web (8080)

O serviço *Filtro Web* é utilizado pelos programas de navegação (Netscape, Internet Explorer, Opera, etc.) para navegar na internet. O Winconnection 7 implementa os protocolos *HTTP*, *FTP* e *HTTPS* (seguro) para permitir o acesso a qualquer site externo, inclusive os sites seguros (compra, bancos, etc.).

Para consultar as conexões ativas, basta clicar no menu Ver conexões.

Guia 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.
  - **Ativa Proxy Transparente (capturar conexões HTTP e HTTPS):** Habilitando esta opção, todas as conexões transparentes serão capturadas.
  - **Bloquear certificados desconhecidos:** Habilitando esta opção, todos os certificados desconhecidos serão bloqueados.
  - **Usar o Agente Winconnection para Desktops quando diponível:** Esta opção deve ser habilitada quando o Agente Winconnection estiver instalado nas estações.
- **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 7** 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 7** essa opção deve ser ativada, informando o IP e as portas utilizadas no outro *Servidor Proxy*.



Guia 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:

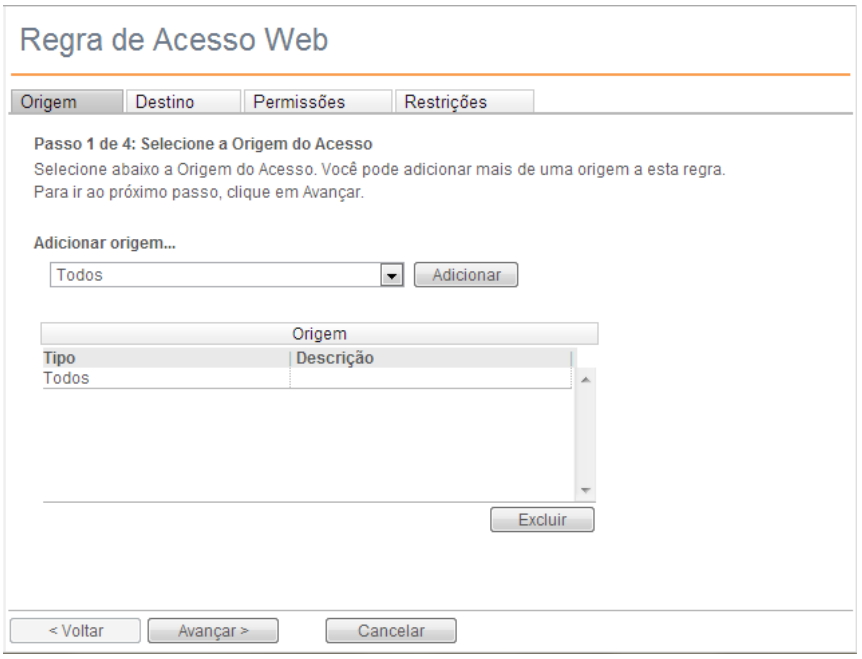
- **Ativar CACHE:** Ativa a utilização do serviço de cache.
- **Tamanho máximo do cache [Mb]:** Neste campo, o administrador da rede pode definir o tamanho do cache.
- **Diretório do cache:** Neste campo é definido o diretório do cache.

Guia Regras de Acesso:

As regras de acesso para o controle de conteúdo do **Winconnection 7** são criadas através de um Assistente que contém 4 etapas, tornando esse processo simples e eficaz.

Passo 1 - Origem de Acesso:

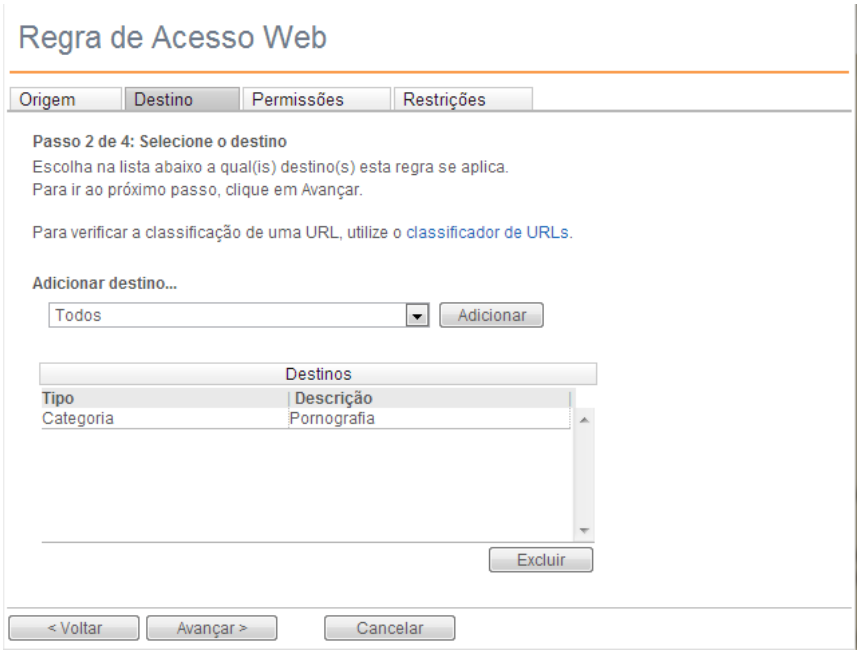
Neste passo de configuração é necessário informar os usuários, grupos e/ou endereços IPs que serão afetados pela regra que está sendo criada/editada.



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.

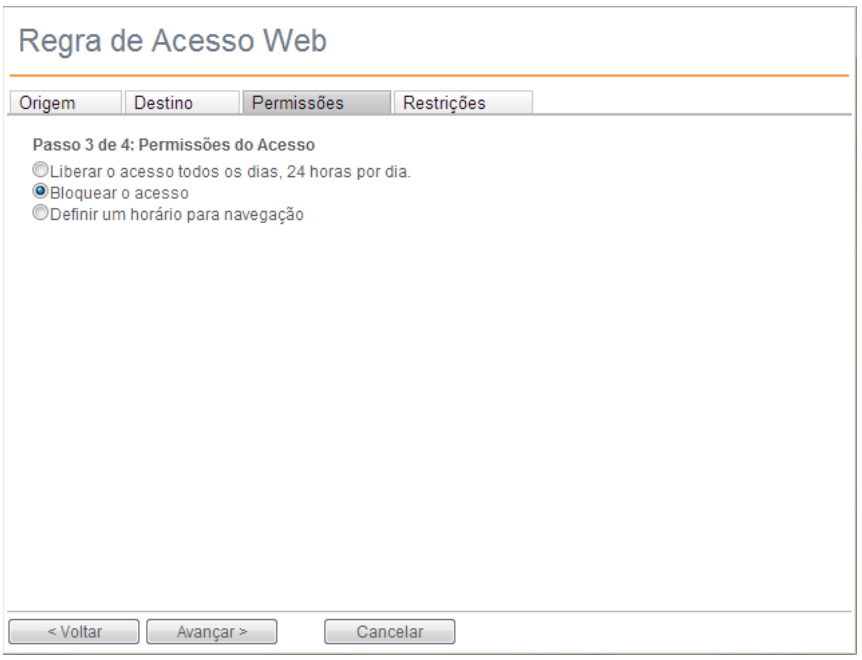
- **Todos:** Todos os sites farão parte da regra de acesso.
- **URL (pode ter "wildcards",* e ?):** O site deve ser informado no campo *URl* e o botão A*dicionar* deverá ser pressionado. Dicas de configurações de bloqueio por site estão disponíveis no tópico *Bloqueio por sites – Dicas de Configuração*.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

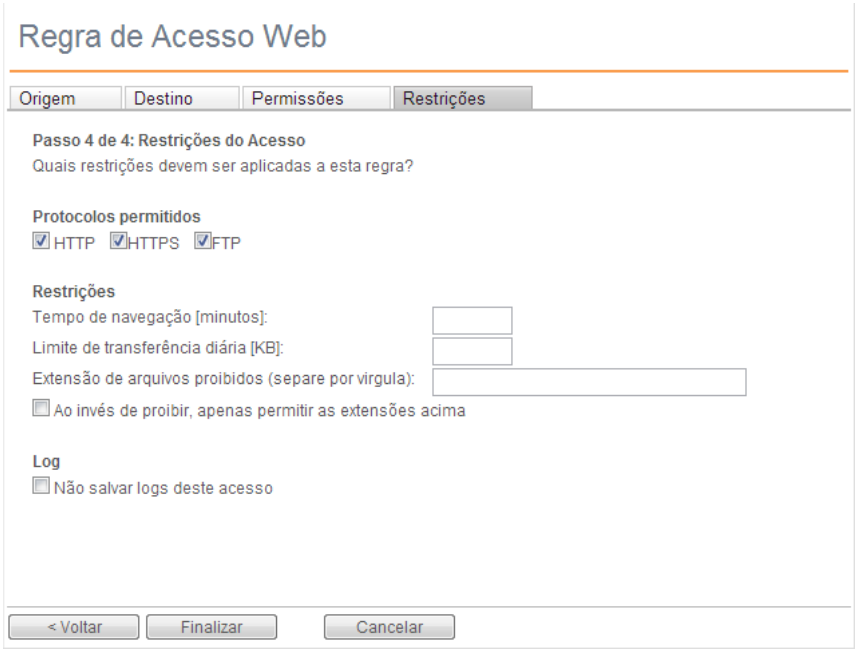
- **Liberar o acesso todos os dias, 24 horas por dia:** Habilitando esta opção, nenhum controle por horário é realizado.
- **Bloquear o acesso:** Habilitando esta opção, o bloqueio é feito independente do horário.
- **Definir um horário para navegação:** Neste campo, o administrador da rede deverá informar 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.

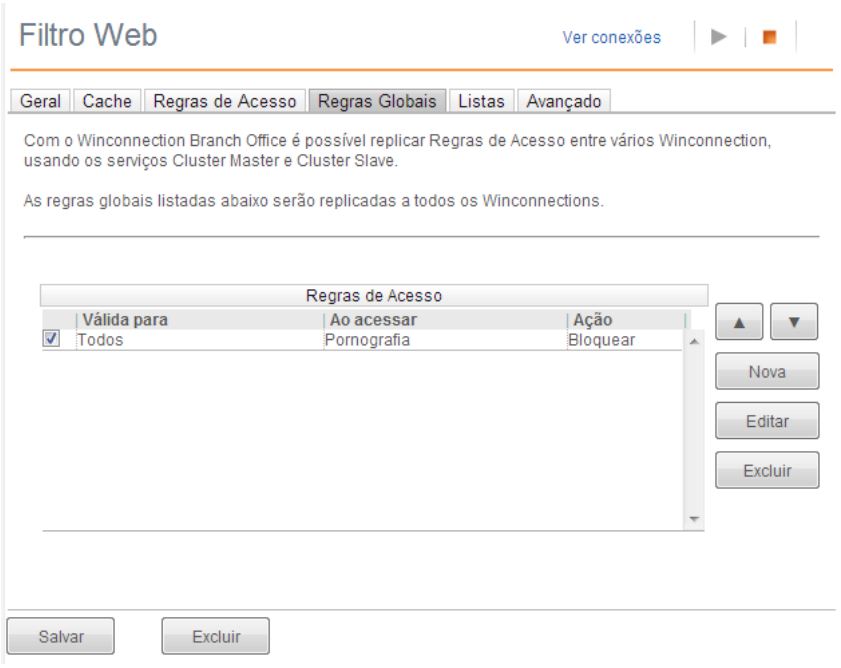
- **Protocolos permitidos:** São os protocolos válidos para a regra de acesso. Habilite os protocolos que serão permitidos na regra.
- **Restrições:**
  - **Tempo de navegação [minutos]:** Neste campo, é possível restringir o tempo que o usuário ficará online. Essa configuração deve ser feita em minutos.
  - **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 7** 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*. Se esta opção for habilitada, o acesso também não será mostrado nos *Relatórios de Acesso a Web*.



Guia Regras Globais:

Com o **Winconnection Branch Office** é possível replicar Regras de Acesso entre vários Winconnection, usando os serviços *Cluster Master* e *Cluster Slave*.

As regras globais listadas nesta guia de configuração replicadas a todos os Winconnection.



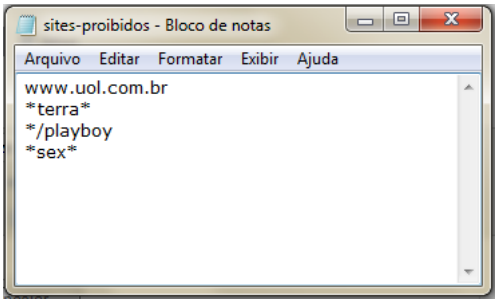
Guia Listas:

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.

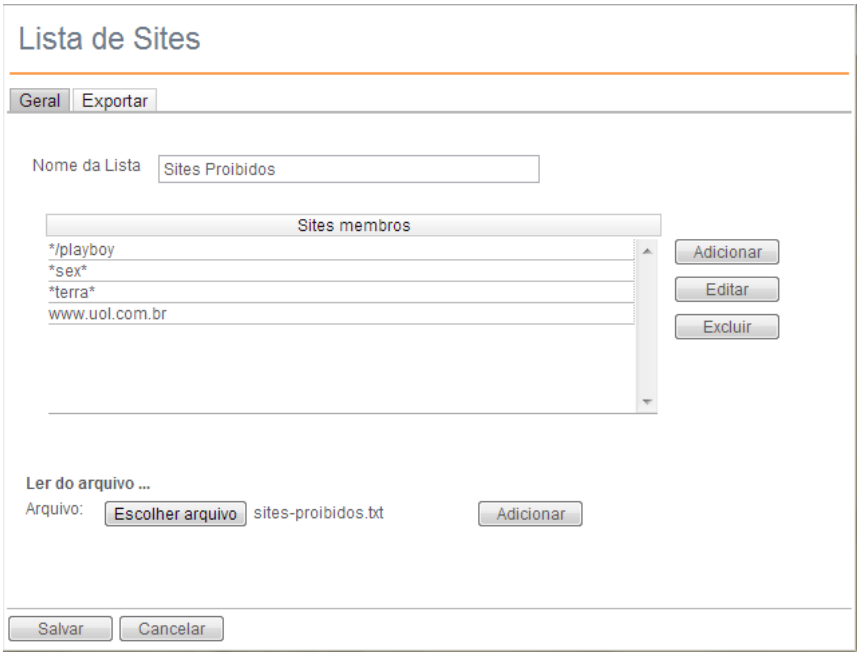
Na existência de outra fonte de sites de uso proibido na empresa, o administrador da rede pode importar uma lista completa de sites de um arquivo texto colocando um site por linha.

Por exemplo:

Arquivo "Sites_Proibidos.txt":

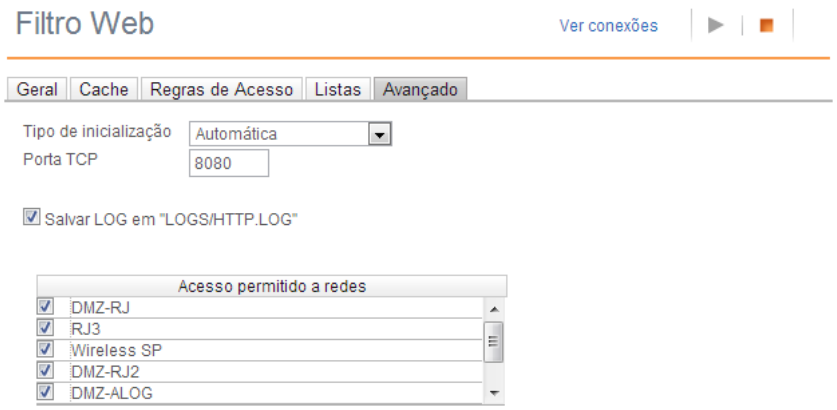


Para importar o arquivo, clique no botão "*Escolher arquivo*", e então clique no botão *"Adicionar"*.



Guia Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta TCP:** Normalmente a porta padrão é 8080 e não deve ser alterada.
- **Salvar LOG em "LOGS/HTTP.LOG":** *O arquivo em bloco de notas (HTTP.LOG)* será criado no diretório *C:/Arquivos de programas/Winco/Winconnection 7/LOGS* e conterá todas as informações referentes a este serviço.
- **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.



Bloqueio por sites - Dicas de Configuração:

Ao adicionar um site em uma regra de acesso à navegação do **Winconnection 7**, 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.

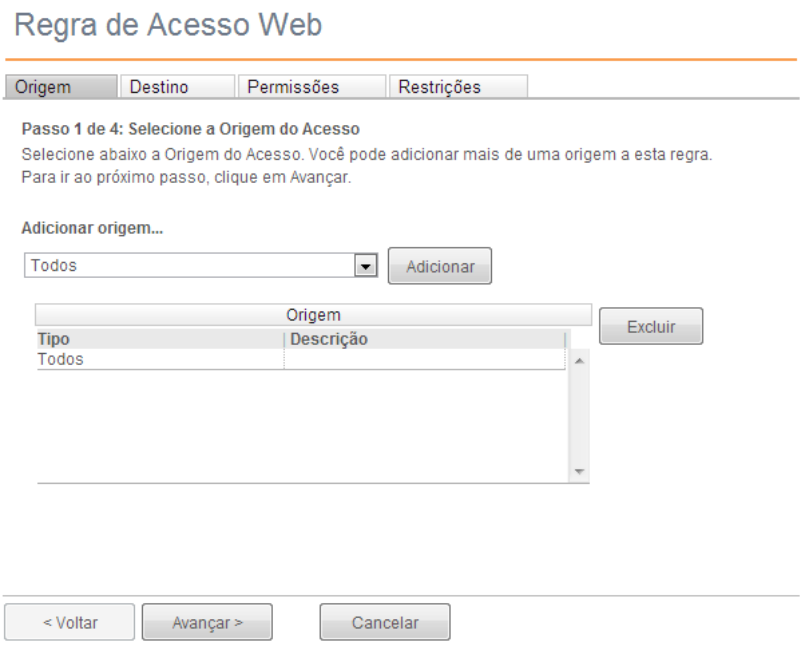
***/playboy:** Controla o acesso aos sites que contenha os subdiretórios */playboy, por exemplo: www.uol.com.br/playboy, www.abril.com.br/playboy

8.1.2.1 Exemplo de Configuração

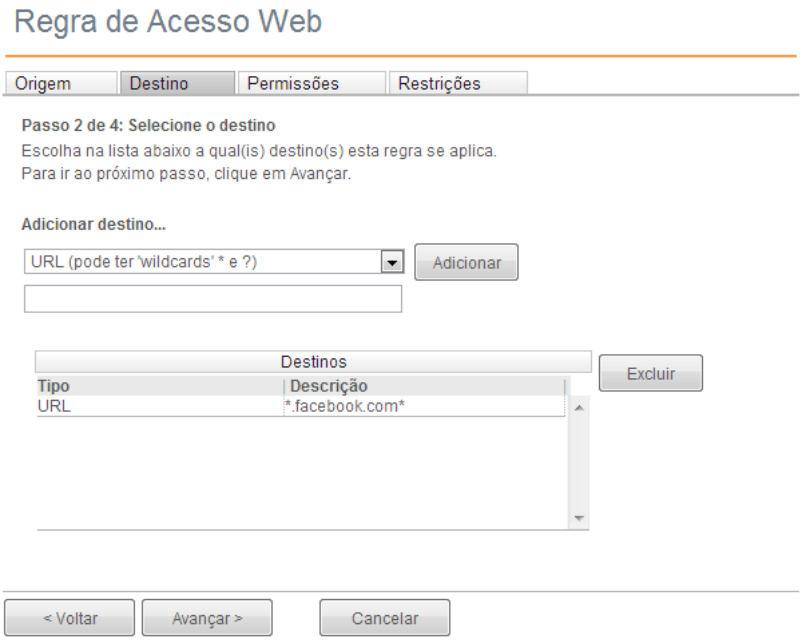
Exemplo de Configuração - Como bloquear o Facebook:

a) Para bloquear o Facebook totalmente, na seção "Filtro" -> "Web" -> Regras Avançadas crie uma regra de acesso da seguinte forma:

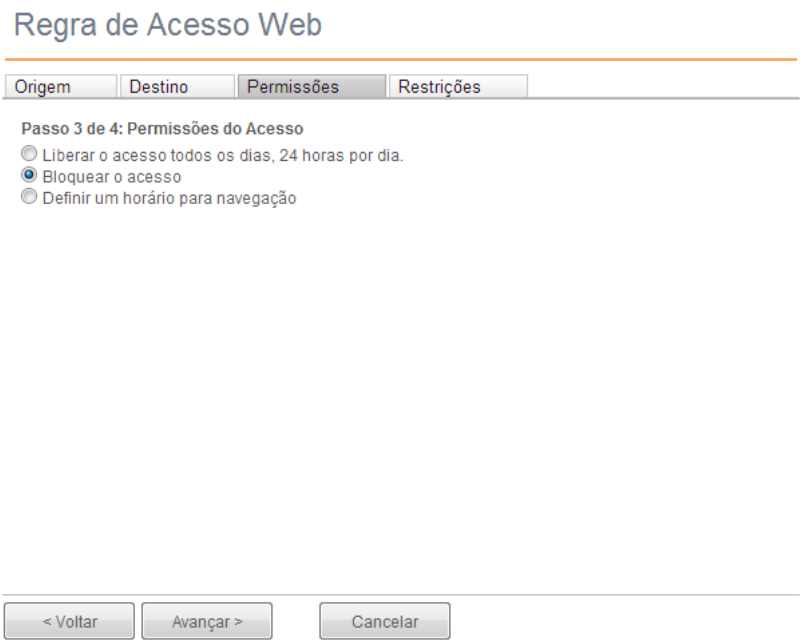
- Origem: Selecione Todos ou os usuários ou grupos de usuários que deseja bloquear.



- Destino: Cadastre a URL *.facebook.com*



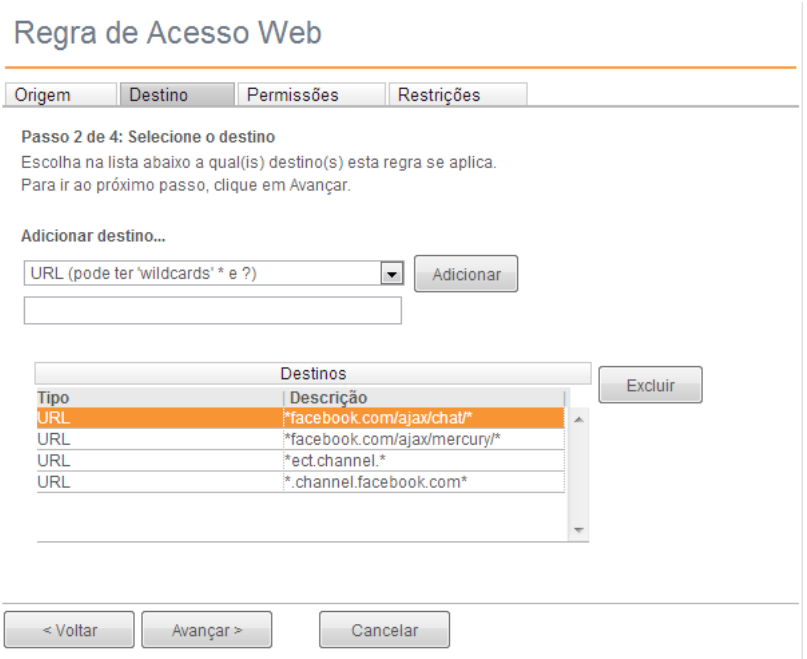
- Permissões: Marcar a opção “Bloquear o acesso”.



- Clique no botão "Avançar" e em seguida, clique em "Finalizar.

b) Para bloquear apenas o chat do Facebook, crie uma regra de acesso semelhante à do exemplo anterior mas no destino você cadastra as seguintes URLs:

- *facebook.com/ajax/chat/*
- *facebook.com/ajax/mercury/*
- *ect.channel.*
- *.channel.facebook.com*



8.1.3 Skype e MSN

O uso do Skype e MSN para comunicação interna na empresa e também no contato com parceiros, fornecedores e clientes agiliza a comunicação e pode aumentar a produtividade da empresa. Estas ferramentas estão cada vez mais sendo usadas para suporte a produtos, call centers e contatos comerciais.

No entanto, também é uma grande fonte de dispersão permitindo conversas com familiares, amigos, namoradas, etc. Com esse recurso é possível fazer um filtro seletivo onde se define quais contatos são permitidos e quais são bloqueados, garantindo o uso do Skype e MSN para as atividades profissionais.

Filtro de Skype e MSN

O nosso filtro de Skype e MSN permite a definição dos contatos permitidos para cada usuário ou grupo de usuários. Dessa forma, eles podem ser usados para contatos profissionais, tanto dentro como fora da empresa, sem a interrupção por pessoas alheias ao trabalho.

Assim não é necessário bloquear o Skype ou MSN totalmente, o que impediria também os benefícios dessa comunicação rápida e simples.

Monitoramento do Skype e MSN

Além de garantir a aplicação da política de uso definida pela empresa, o filtro permite o monitoramento e auditoria da comunicação por essas ferramentas.
As conversas podem ser gravadas em banco de dados para posterior consulta ou geração de relatórios.

Além de gerar estatísticas de uso, é possível ver as conversas através de busca por data, usuário ou palavra-chave. E as conversas também podem ser monitoradas em tempo real.

O log das conversas pode ser habilitado ou desabilitado por usuários ou grupos de usuários.

Ao clicar no menu Ver conexões, as seguintes opções são oferecidas:

- Ações: Permite monitorar a conversa selecionada e excluir a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

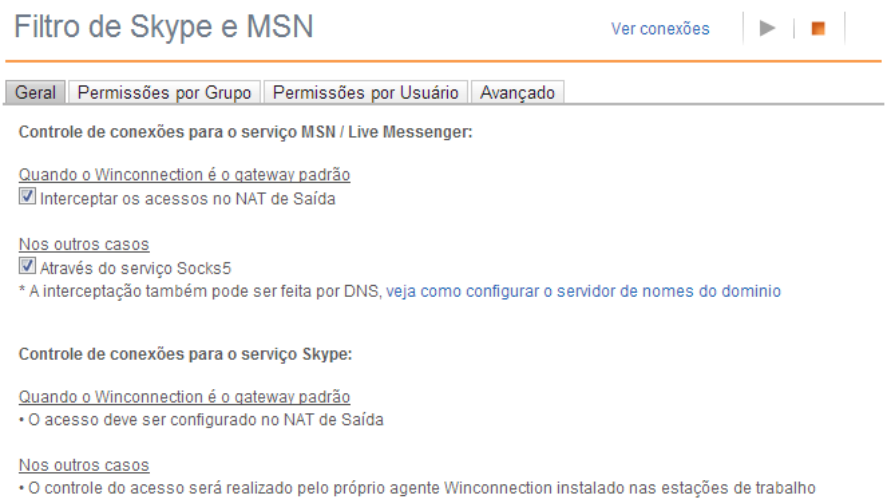
Guia Geral:

Controle de conexões para o serviço MSN / Live Messenger:

- Quando o Winconnection é o gateway padrão:
  - Interceptar os acessos no NAT de Saída: Essa opção deve ser habilitada quando o Winconnection é o gateway padrão da rede. Neste caso, o acesso deve ser configurado na seção *NAT de Saída*.
- Nos outros casos:
  - Através do serviço Socks5: Quando o Winconnection não for o gateway padrão da rede, essa opção deve ser habilitada. Neste caso,o controle do acesso será realizado pelo próprio agente Winconnection instalado nas estações de trabalho. O serviço Servidor *SOCKS 5* deve estar ser instalado.

    A interceptação também pode ser feita por DNS, da seguinte forma:

    Crie uma zona de forward lookup com o nome **messenger.hotmail.com**, e crie nesta zona um registro A, deixando o nome do host vazio e colocando o IP do servidor Winconnection no registro criado.



Guia Permissões de Acesso:

Nesta guia de configuração é possível definir a configurações do Filtro de Skype e MSN por grupos de usuários.

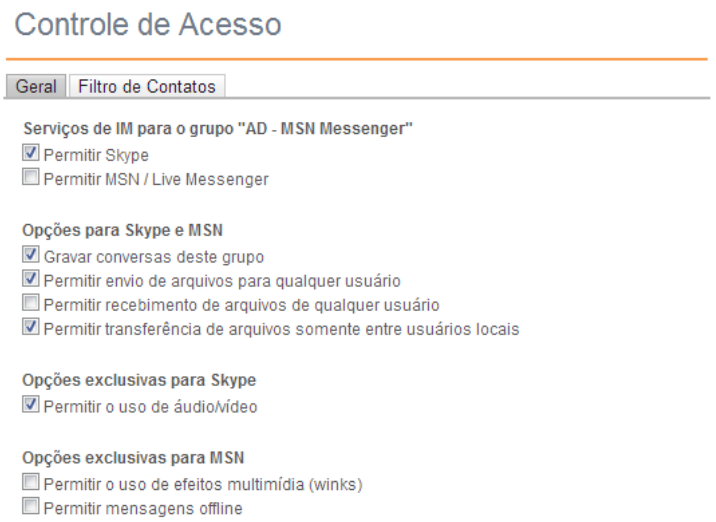
Habilite os grupos de usuários que poderão acessar serviços de IM (Skype e MSN).
Em seguida, configure o controle de acesso para cada um dos grupos selecionados.

Atenção: Para grupos pertencentes ao domínio do AD é preciso cadastrar os logins conforme descrito neste link.

Ao clicar no botão *Configurar*, as seguintes opções serão exibidas:

Guia Geral:

- **Serviços de IM para o grupo:**
  - Permitir Skype
  - Permitir MSN
- **Opções para Skype e MSN:**
  - Gravar conversas deste grupo
  - Permitir envio de arquivos para qualquer usuário
  - Permitir recebimento de arquivos de qualquer usuário
  - Permitir transferência de arquivos somente entre usuários locais
- **Opções exclusivas para Skype:**
  - Permitir o uso de áudio/vídeo
- **Opções exclusivas para MSN:**
  - Permitir o uso de efeitos multimídia (winks)
  - Permitir mensagens offline



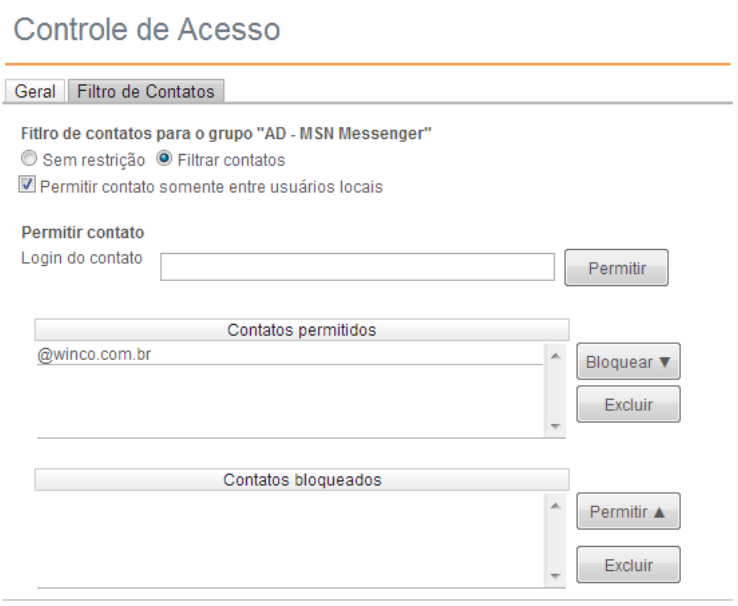
Guia Filtro de Contatos:

Nesta guia de configuração, é possível permitir ou bloquear determinado contato.

As seguintes opções estão disponíveis:

- **Sem restrição**
- **Filtrar contatos**
  - Permitir contato entre usuários locais
  - Permitir transferência de arquivos entre usuários locais
- **Permitir contato**
  - Contatos permitidos

- Contatos bloqueados



Guia Permissões por Usuário:

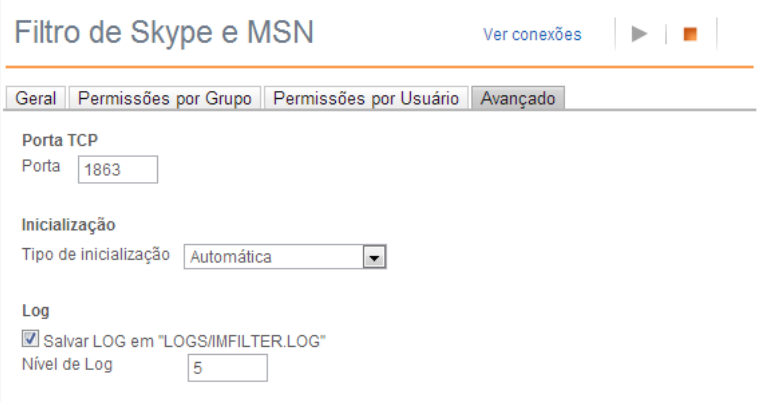
Nesta guia, o administrador da rede poderá cadastrar os usuários de Skype e MSN que poderão acessar estes serviços.

Em seguida, deverá configurar as permissões de acesso para cada um destes usuários.

Atenção: As *Permissões por Usuário* tem precedência sobre as *Permissões por Grupo*.

Guia Avançado:

- **Porta TCP:** Porta utilizada pelo serviço Filtro de Skype e MSN.
- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Salvar LOG em "LOGS/IMFILTER.LOG":** *O arquivo em bloco de notas (LOGS/IMFILTER.LOG)* será criado no diretório *C:/Arquivos de programas/Winco/Winconnection 7/LOGS* e conterá todas as informações referentes a este serviço.



8.1.3.1 Dicas de Configuração

Como bloquear totalmente o Skype

Como o Skype busca vários caminhos alternativos para se conectar, para bloquear os Skype é preciso permitir no *NAT de Saída* apenas as conexões que efetivamente serão utilizados e deixar o resto bloqueado.

Essa configuração, a mais recomendada sempre, é a mais segura independente da necessidade de bloquear o Skype.

Para fazer essa configuração, é preciso:

1) Fazer um levantamento de todos os tipos de acesso que são necessários. Veja abaixo uma lista dos acessos frequentemente usados:

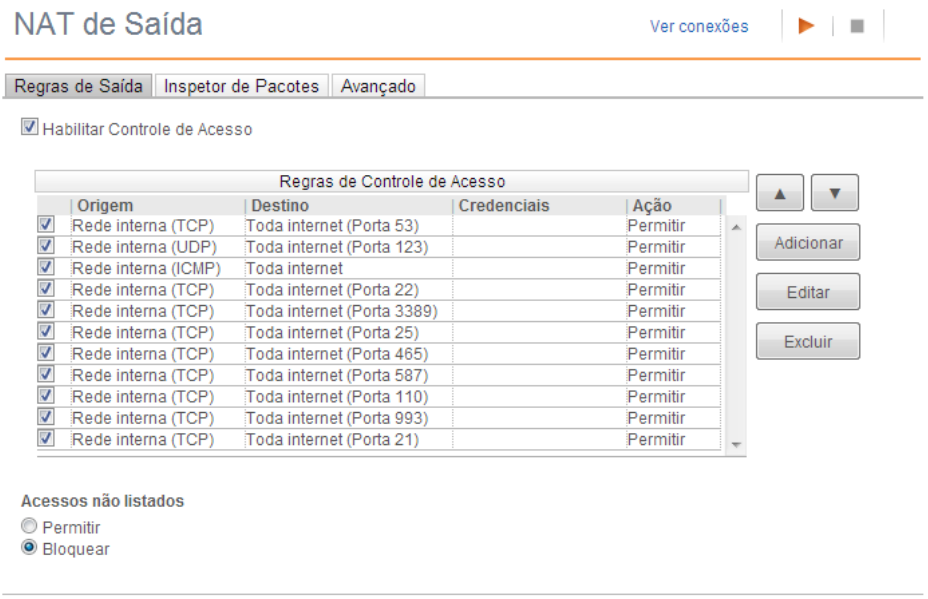
- DNS – Usado para converter nomes em endereços IP: protocolo UDP porta 53
- NTP (Network Time Protocol) – Usado para acertar os relógios dos computadores: UDP porta 123
- ICMP – protocolo de controle da Internet: protocolo ICMP
- SSH – Conexão segura com servidores Linux: protocolo TCP porta 22
- RDP (Remote Desktop Protocol) – usado para conectar com Terminais Remetos (Terminal Server) – protocolo TCP porta 3389
- SMTP – Protocolo de envio de e-mail: TCP portas 25, 465 e 587
- POP – Protocolo de recebimento de e-mail: TCP portas 110 e 995
- IMAP – Protocolo de recebimento de e-mail: TCP portas 143 e 993
- FTP e SFTP – protocolo de transferência de arquivos: TCP porta 21
- VNC – protocolo de terminal remoto – UDP e TCP porta 5900
- Receita Net – para entrega de declarações da Receita Federal – TCP porta 3456

2) Selecione no menu lateral esquerdo, abaixo de Conectividade, a opção “NAT de Saída”.

3) Abra a guia “Regras de Saída” e:

- Marcar a opção “Habilitar Controle de Acesso”;
- Adicionar uma regra para cada um dos acessos definidos no passo 1 com a opção “Permitir o acesso” marcado na aba “Ação”;
- Marcar a opção “Bloquear” em “Acessos não Listados”;

Veja um exemplo na imagem abaixo:



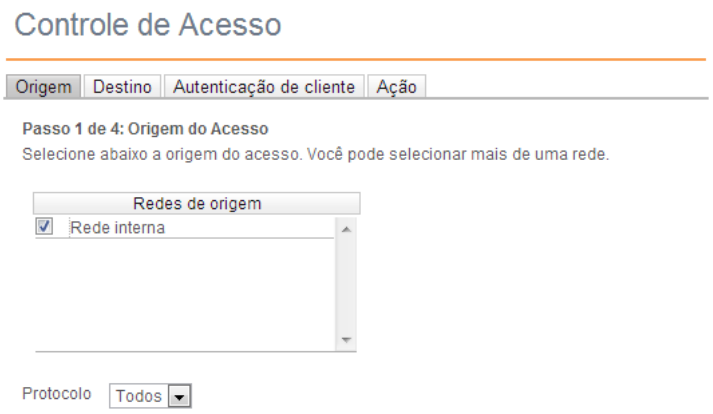
Como controlar e monitorar o uso do Skype:

Para utilizar o Skype de forma controlada na sua rede, ou seja, definindo contatos permitidos e registrando as conversas é necessário:

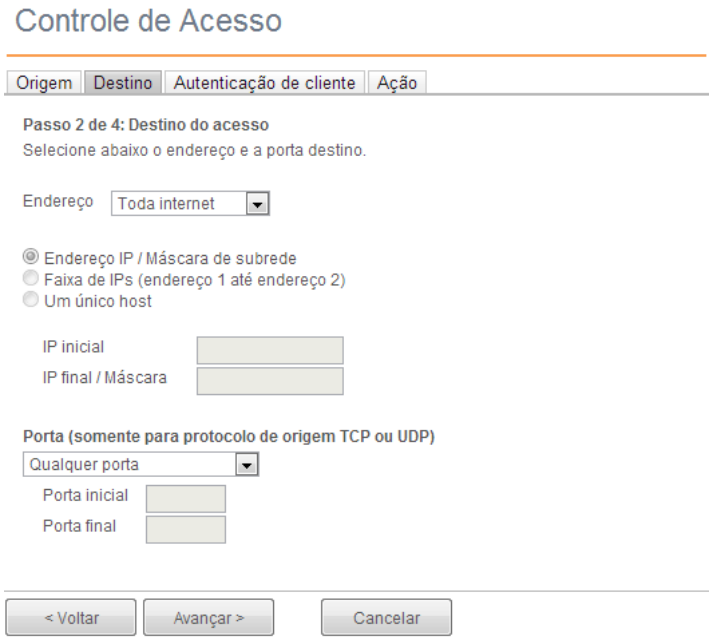
1) Bloquear o Skype conforme a dica acima.

2) Criar uma regra de acesso no *NAT de Saída* da seguinte forma:

- Origem: Selecione a rede para a qual deseja permiter o acesso controlado do Skype. Normalmente é a Rede Interna.

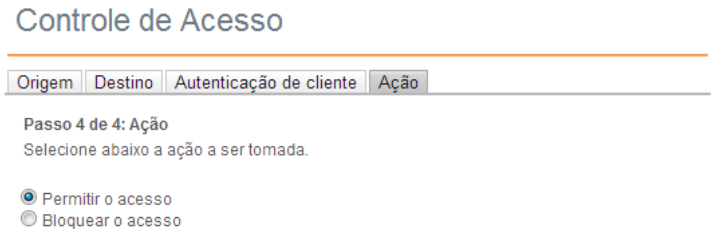


- Destino: em endereço colocar selecionar “Toda a internet”.



- Autenticação do Cliente: marcar “Skype, desde que monitorado pelo Skype Controller”.

- Ação: Selecionar “Permitir o acesso”



3) Instalar o programa Agente Winconnection em todas as estações que irão ter acesso ao Skype.

8.2 E-mail

8.2.1 Servidor de E-mail

O Winconnection oferece um servidor de e-mail simples e completo, com as funcionalidades necessárias para um servidor corporativo.

O servidor de e-mail pode ser configurado com o servidor SMTP primário de um domínio ou pode ser o destino final das mensagens recebidas em um servidor SMTP na nuvem, como de um provedor por exemplo.

Protocolos

Além dos protocolos SMTP e POP, o Winconnection suporta o protocolo IMAP que, ao manter os e-mails organizados em pastas no servidor, permite acesso a todas as mensagens a partir de qualquer computador. Ideal quando se acessa o e-mail do escritório, do notebook e do celular.

Outro recurso exclusivo é o Mapeador POP que permite que as mensagens hospedadas em um servidor POP sejam trazidas automaticamente para o servidor de e-mail local do Winconnection. Isso é feito associando uma conta de e-mail externa a um usuário local.

Além do recurso de IMAP, usuários de smartphones podem acessar o Mobile Webmail cuja interface é otimizada para esses dispositivos.

E-mails internos mais rápidos com o acesso local

Ao armazenar os e-mails na própria empresa, o acesso é feito localmente com rapidez. Os e-mails internos da empresa nem precisam passar pela internet, trazendo agilidade e economia de banda.

Filtro de Mensagens

O poderoso filtro de mensagens permite uma série de ações baseadas nos campos do cabeçalho e envelope de e-mail como remente, destinatário e assunto, além de IP de origem, tamanho da mensagem e outros. As ações podem ser redirecionar ou copiar para outro e-mail, apagar a mensagem, ou responder automaticamente. Essas regras podem ser globais ou por usuário.

Podem ser criados filtros personalizados em PHP para realizar ações mais específicas de acordo com as suas necessidades.
O recurso de copiar para outro e-mail aliado aos relatórios permite que sejam feitas, se necessárias, auditoria dos e-mails enviados ou recebidos.

Possibilidade de criar contas de e-mail somente para uso interno

Com o filtro descrito acima, é possível definir que algumas contas só podem usar o e-mail internamente, ou seja, para comunicação interna. E-mails vindos de fora ou enviados para fora são bloqueados.

Antispam

A exclusão de SPAM além de economizar tempo valioso dos usuários evita que mensagens legítimas se percam no meio de centenas de SPAMs.

O plugin opcional de Filtro Antispam permite a detecção de SPAMS que podem ser marcados, encaminhados à quarentena ou apagados.

Contém com uma série de recursos que podem ser configurados pelo administrador. Dentre eles destacamos:

- Black e whitelist de domínios e IPS
- SPF
- Reputação do remetente que usa um banco de dados em tempo real

Um e-mail pode ser enviado diariamente com um resumo dos e-mails colocados na quarentena. Com isso, de uma forma rápida, o usuário pode verificar se houve um falso positivo, ou seja, uma mensagem marcada indevidamente como SPAM.
A qualquer momento, o usuário pode gerenciar a sua quarentena, liberando e-mails e definindo sua própria whitelist.

Relatórios

Os relatórios mostram estatísticas de uso globais ou por usuário. Dentre as informações apresentadas temos: número de mensagens internet e externas, mensagens com vírus, spams e além mensagens com erro.
Também permite o rastreamento de mensagens.

Gerenciamento

Para evitar o esgotamento de espaço em disco, podem ser definidas cotas de utilização por usuário.
O administrador pode configurar cópias de segurança (backups) definindo dias da semana e horários que o backup deve ser realizado automaticamente.
Assinaturas automáticas podem ser anexadas ao final das mensagens enviadas.
E por fim, listas de distribuição são criadas facilmente permitindo a criação de aliases, como por exemplo, financeiro, diretoria, etc que serão encaminhadas às pessoas na lista.

Segurança

O e-mail do Winconnection apresenta vários recursos relativos à segurança. Começando pela utilização do SSL, que é utilizado para transações seguras na internet como acesso a bancos e lojas virtuais, com os protocolos suportados.
Permite ainda a verificação de vírus mensagens, caso o AVG esteja instalado no servidor de e-mail. Outro recurso é o bloqueio de anexos baseados em extensões evitando assim o download de arquivos potencialmente perigosos como, por exemplo, executáveis.

Mensagens de reposta automática (aviso de férias)

Respostas automáticas podem ser configuradas por cada usuário. Essas respostas são muito utilizadas para avisar que o destinatário está de férias.
Além de definir o texto, o usuário pode definir as datas de início e fim do envio da resposta automática.

8.2.2 Armazenamento

Guia 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 tópico *Apêndice - Programação e Extensibilidade*.

- **Cópia de Segurança das mensagens de e-mail:** O armazenamento das mensagens do Winconnection 7 é dividido em 2 partes: banco de dados (índices das mensagens) e as mensagens de e-mail propriamente ditas.

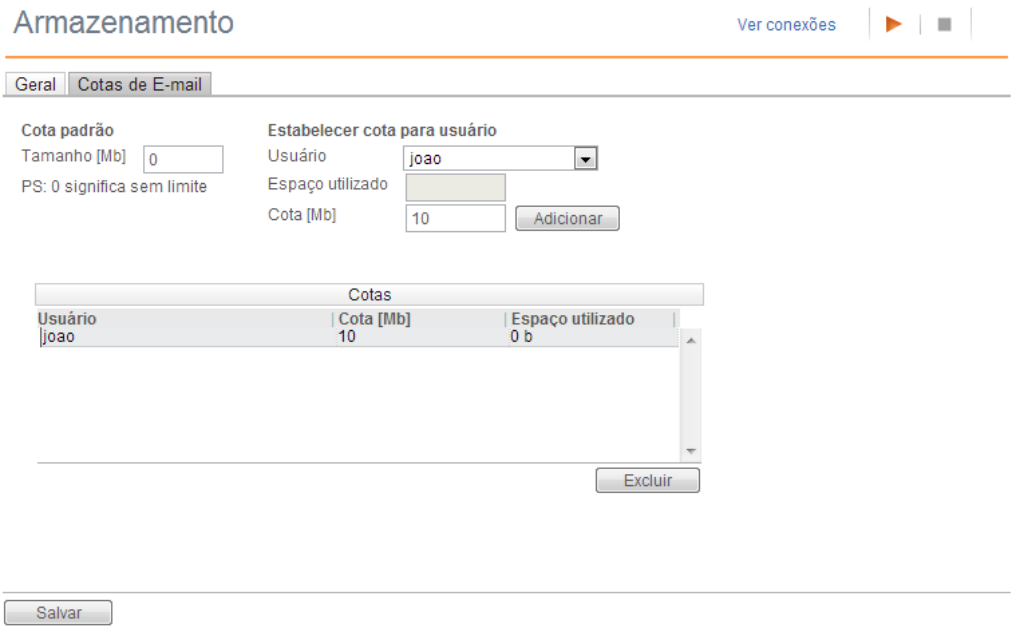
  Neste campo, o administrador da rede pode definir à hora e os dias da semana em que cópias de segurança dos índices das mensagens de e-mail serão efetuadas (caso o índice seja corrompido, este backup ajudará na sua restauração).

Importante! Recomendamos que o backup do diretório *C:/Arquivos de programas/Winco\Winconnection 7/mbox* seja efetuado com frequência.

Guia 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.



8.2.3 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.

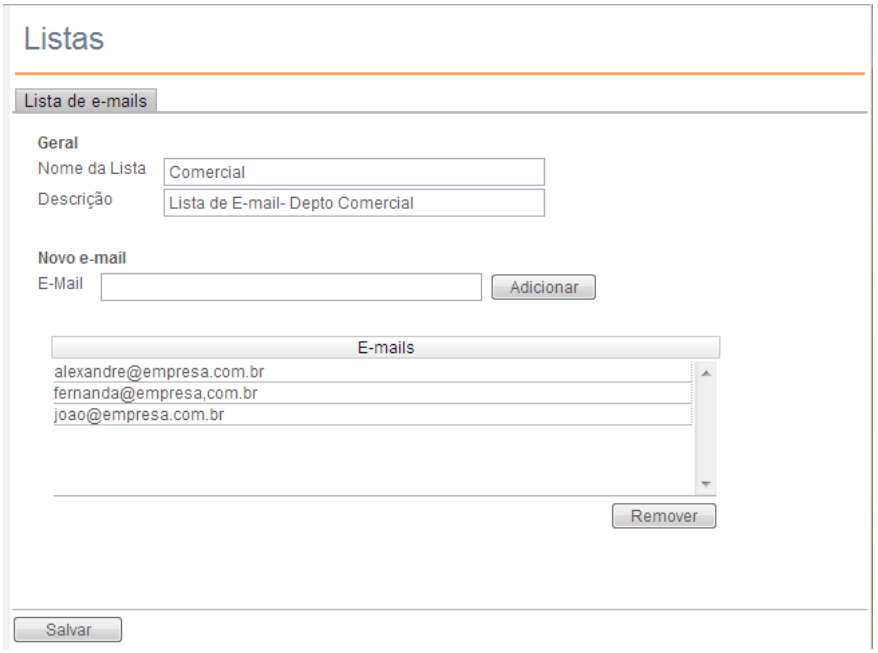
O menu *Usuários* oferece as seguintes opções:

- Ações: Permite criar, editar ou excluir uma lista.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

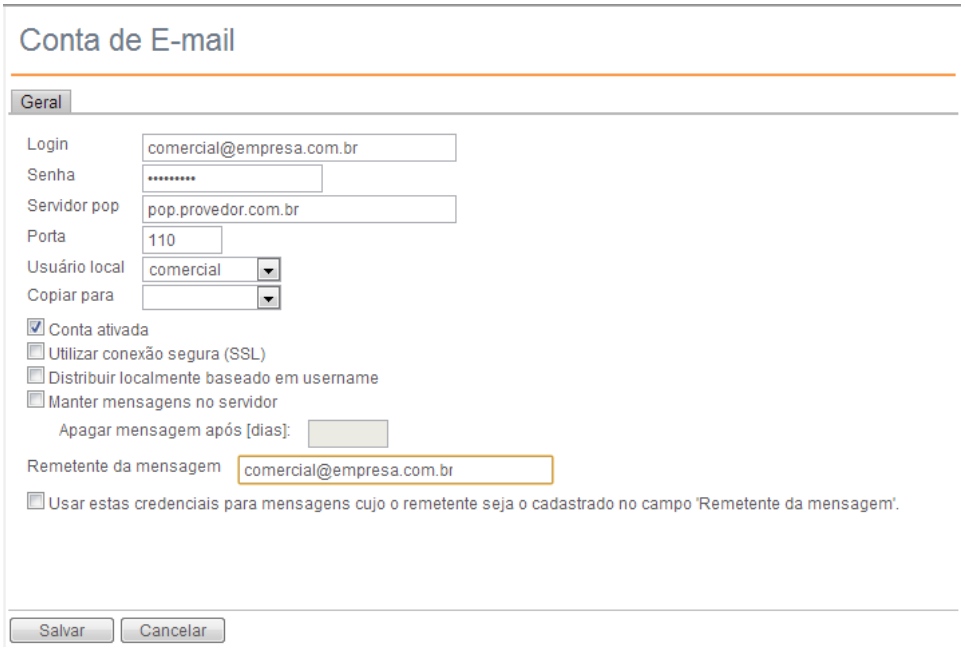
Exemplo:

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

- Se os usuários ainda não foram cadastrados, cadastre-os no menu *Cadastro*.
- Clique em *Ações* | *Criar uma lista*.
- **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.
- **E-mail:** 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).



8.2.4 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.

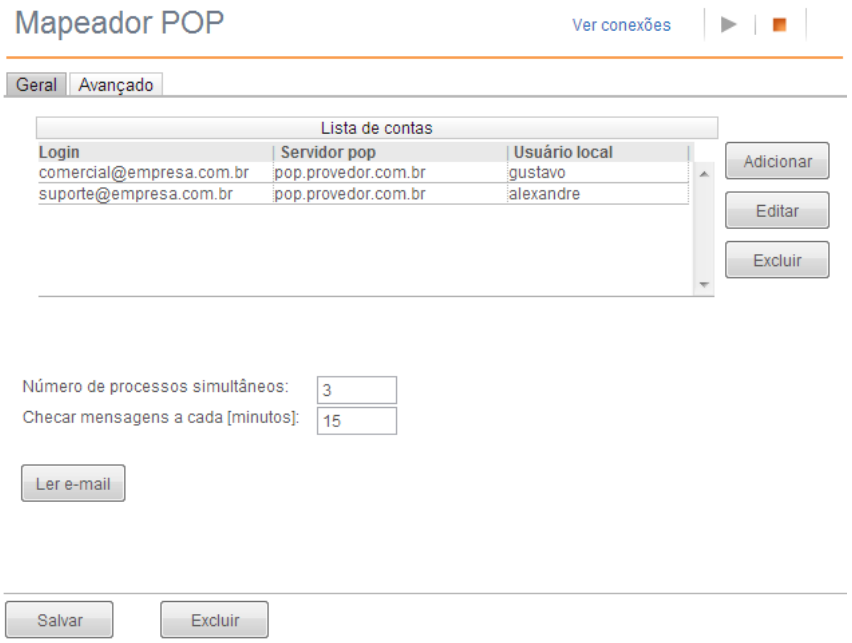
Ao utilizar o Mapeador POP, o **Winconnection 7** irá buscar os e-mails dos usuários em um Servidor POP e processará o conteúdo dos e-mails aplicando as regras de filtragem (definidas no Filtro de E-mail). Este processo é similar ao *Fetchmail* do *Linux* ou o *POP Connector* do *MS Exchange Server*, permitindo que o produto aja como um cliente POP que é configurado com as senhas de cada caixa postal envolvida no processo.
Esta configuração é muito útil na implementação de ambientes redundantes, além de constituir uma ferramenta interessante na migração de ambientes, principalmente naqueles onde a convivência do sistema legado é necessária durante algum tempo.

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Guia 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.

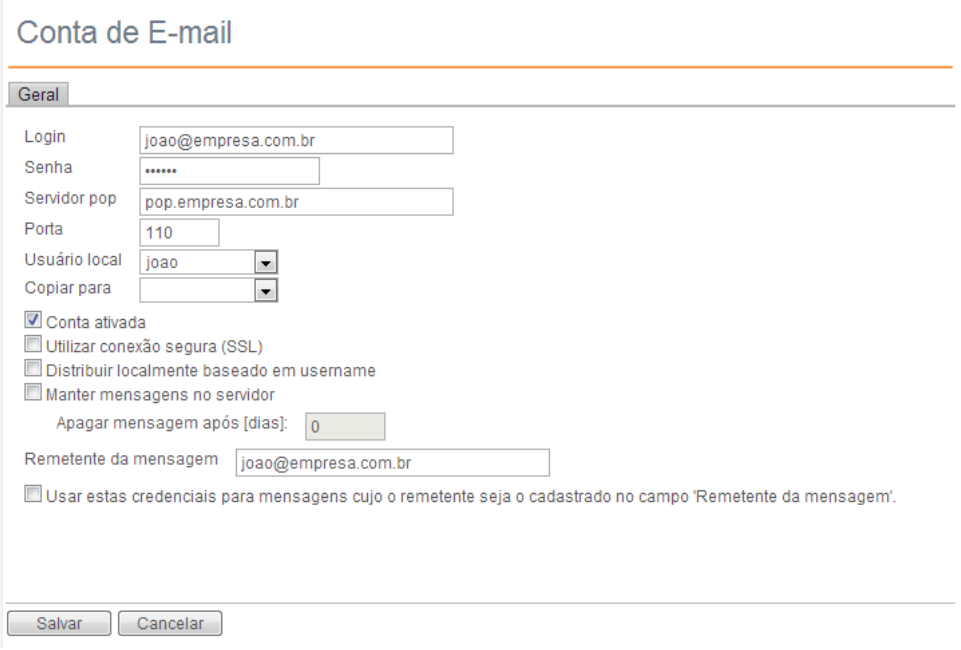
- **Login:** Digite aqui o login do usuário *no provedor* onde a caixa postal se encontra. Para ter certeza qual é o login, verifique no cliente de e-mail (outlook, eudora, etc.) do usuário qual a conta que ele usa.
- **Senha:** Digite aqui a senha de acesso à caixa postal *do provedor*, a mesma usada 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 tópico *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 7 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.

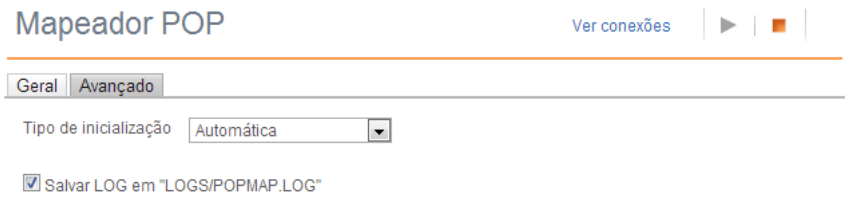
  Por exemplo: Os e-mails enviados por joao@empresa.com.br só podem ser enviados se o usuário joao se autenticar.

  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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Salvar LOG em "LOGS/POPMAP.LOG":** O arquivo em bloco de notas (POPMAP.LOG) será criado no diretório C:/Arquivos de programas/Winco/Winconnection 7\LOGS e conterá todas as informações referentes a este serviço.



8.2.5 Servidor POP (110)

O *Servidor POP* é necessário quando o **Winconnection 7** é utilizado como Servidor de E-mail, sendo utilizado um programa cliente de e-mail para receber as mensagens nas estações dos usuários.

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Guia Geral:

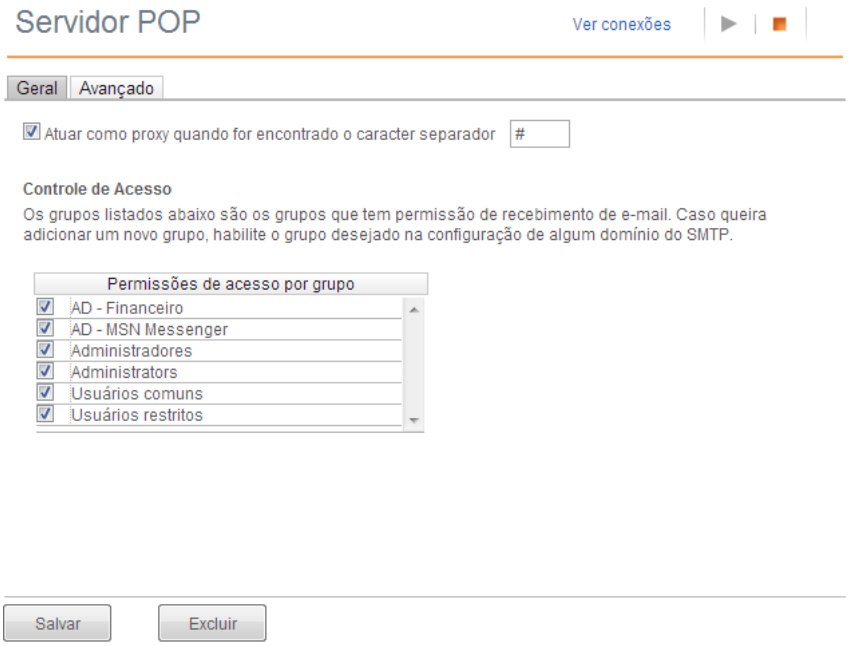
- **Atuar como proxy quando for encontrado o caractere separador:** O Servidor POP3 também funciona como *Proxy POP3*, para possibilitar o acesso às caixas postais de outros servidores de e-mail. Basta haver uma configuração com caractere separador para ele aceitar a conexão como proxy.

  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 do domínio no serviço *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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta TCP:** A porta padrão para este serviço é 110, mas pode ser alterada nesse campo.
- **Salvar LOG em "LOGS/POPSRV.LOG":** O arquivo em bloco de notas (POPSRV.LOG) será criado no diretório C:/Arquivos de programas/Winco/Winconnection 7/LOGS e conterá todas as informações referentes a este serviço.
- **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.

Servidor POP

Geral | Avançado

Tipo de inicialização: Automática

Porta TCP: 110

☑ Salvar LOG em "LOGS/POPSRV.LOG"

Nível de Log: 1

Acesso permitido a redes
☑ DMZ-RJ
☑ RJ3
☑ Wireless SP
☑ DMZ-RJ2
☑ DMZ-ALOG

SSL

Certificado: wincosp.winconnection.net (vpnca.winco.com.br)

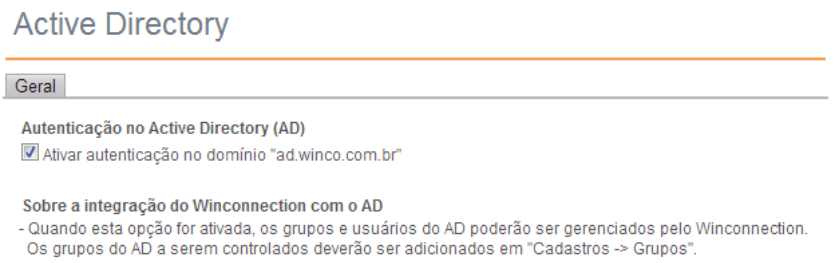
Criar

8.2.5.1 Configurando o Servidor de E-mail com Servidor POP

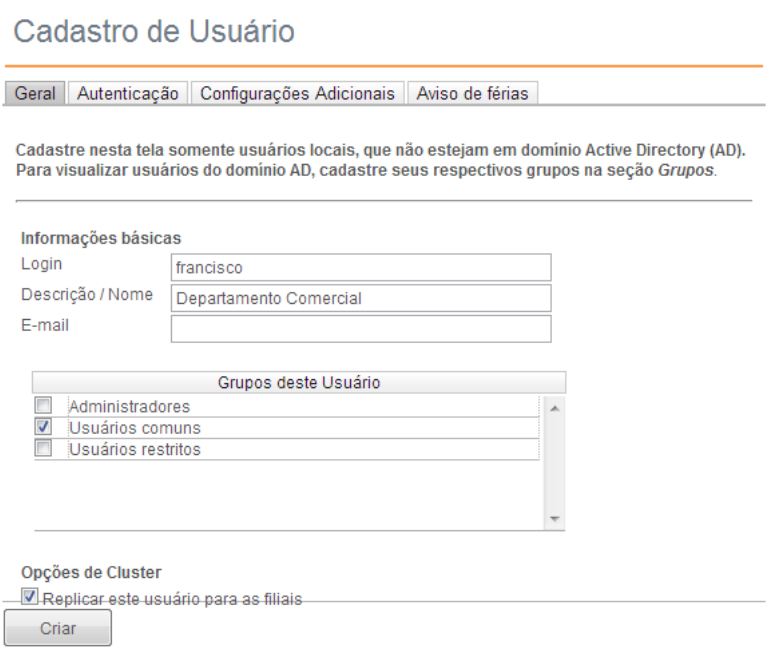
Para configurar o servidor de e-mail do Winconnection 7 com Servidor POP, faça o seguinte:

1º) Passo – Cadastrando os Usuários:

- Se a base de usuários que farão parte do Servidor de E-mail estão cadastrados no AD, habilite a opção "Ativar autenticação no domínio" disponível em Casdatro -> Active Directory.



- Se AD não estiver configurado na rede, é necessário cadastrar os usuários na seção Cadastro -> Usuários.



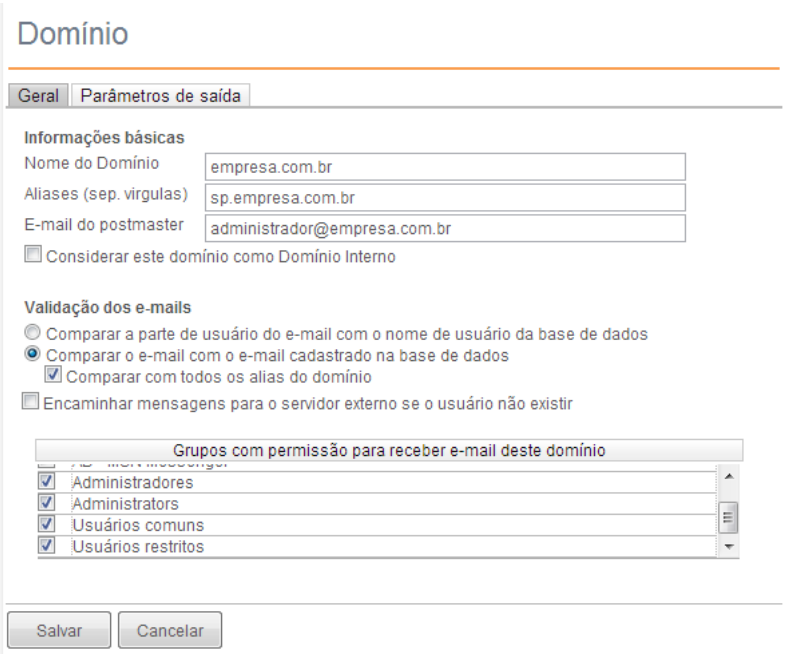
2º) Cadastrando os Serviços:

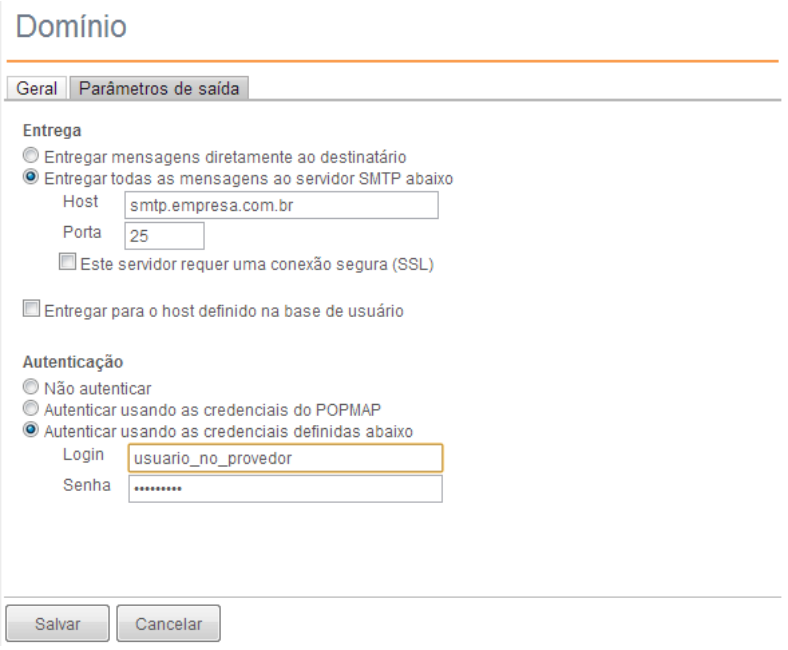
- Clique em Serviços | E-mail e verifique se os seguintes serviços estão instalados:

Obs.: Se esses serviços não estiverem instalados, será necessário instalá-los clicando no sinal **+** do meu Serviços.

3º) Configurando o Servidor SMTP:

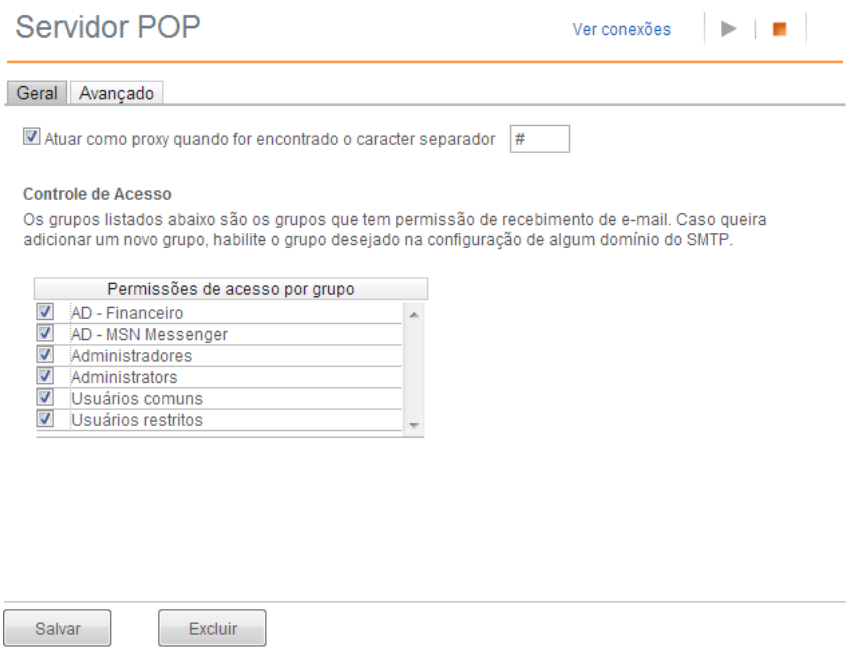
- No lado esquerdo da tela, selecione o serviço Servidor SMTP. Configure esse serviço conforme descrito no menu Serviços -> E-mail | Servidor SMTP. **Obs.:** Na guia da Domínios, é necessário adicionar um novo domínio conforme as configurações do domínio da sua empresa.





4º) Configurando o Servidor POP:

- No lado esquerdo da tela, selecione o serviço Servidor IMAP e habilite os grupos de usuários que terão acesso a esse serviço.



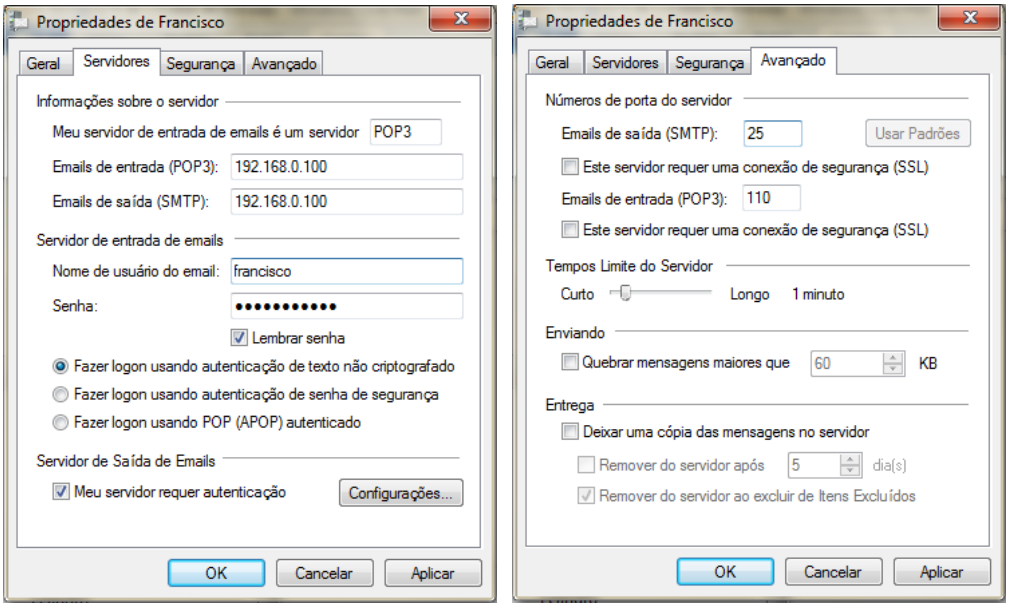
5º) Configurando o Mapeador POP:

- 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.

6º) Configurando as Estações:

- Entre na tela de configuração de contas do Cliente de E-mail da estação. Usaremos como exemplo o Windows Live Mail:
    - Selecione a conta -> Clique no menu superior Contas -> Clique em Propriedades -> Clique na guia Servidores.
    - No campo Servidor POP3, digite o IP do servidor Winconnection 7. (No nosso exemplo: 192.168.0.100).
    - No campo Servidor SMTP, digite o IP do servidor Winconnection 7. (No nosso exemplo: 192.168.0.100).
    - No campo Usuário, coloque o nome do usuário cadastrado na Lista de Usuários do Winconnection 7. No nosso exemplo: francisco.
    - No campo Senha, coloque a senha para o usuário no AD ou a que você criou no Winconnection 7.

Obs.: Note que neste campo, estamos usando a senha do usuário interno (do AD ou criado no Winconnection 7) 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 7**.

Para informações sobre o Filtro de E-mail, consulte o tópico Serviços | Filtro | Filtro de E-mail.

8.2.6 Servidor IMAP (143)

O **Winconnection 7** oferece suporte ao protocolo **IMAP**.

O serviço *Servidor IMAP* é necessário quando o provedor de e-mail utiliza o protocolo *IMAP* e o **Winconnection 7** 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.

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

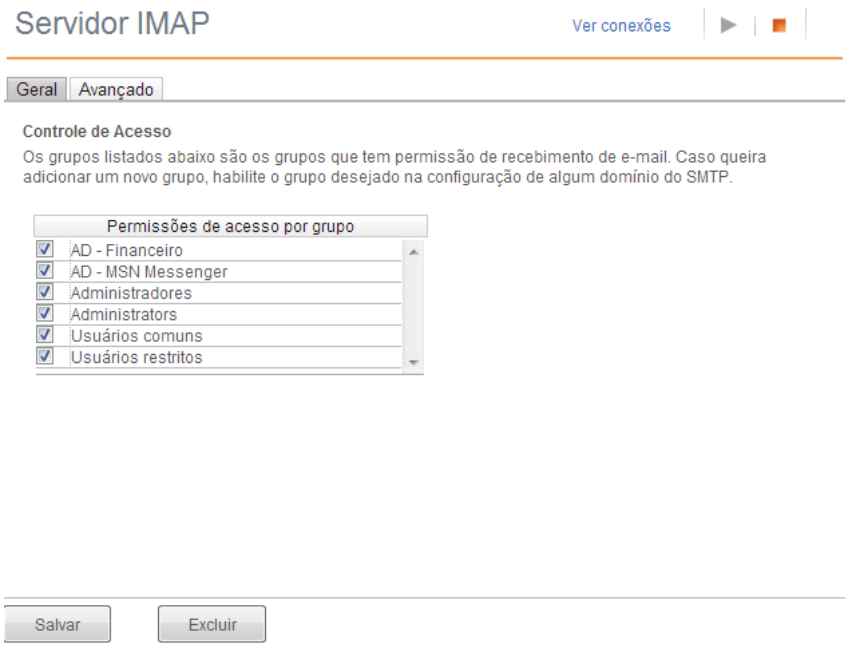
- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Guia 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 do domínio no serviço *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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta TCP:** A porta padrão para este serviço é 143, mas pode ser alterada nesse campo.
- **Salvar LOG em "LOGS/IMAP.LOG":** O arquivo em bloco de notas (IMAP.LOG) será criado no diretório C:\Arquivos de programas\Winco\Winconnection 7\LOGS e conterá todas as informações referentes a este serviço.
- **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.

Servidor IMAP

Geral | Avançado

Tipo de inicialização: Automática

Porta TCP: 143

☑ Salvar LOG em "LOGS/IMAP.LOG"

Nível de Log: 1

Acesso permitido a redes
☑ DMZ-RJ
☑ RJ3
☑ Wireless SP
☑ DMZ-RJ2
☑ DMZ-ALOG

SSL

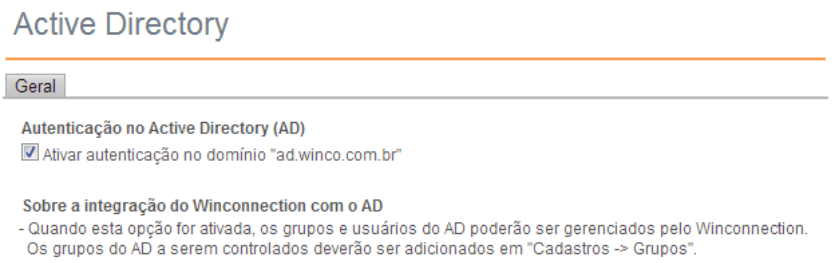
Certificado: wincosp.winconnection.net (vpnca.winco.com.br)

8.2.6.1 Configurando o Servidor de E-mail com IMAP

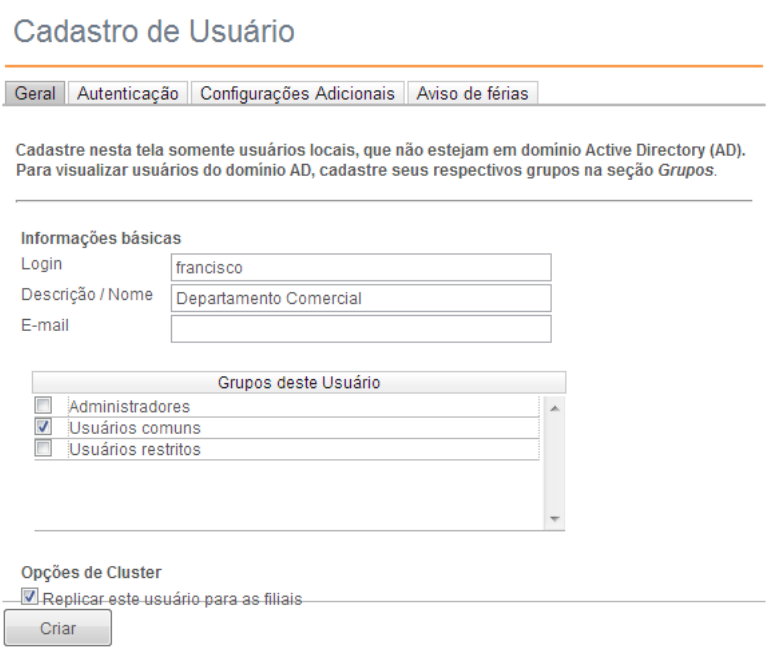
Para configurar o servidor de e-mail do Winconnection 7 com IMAP, faça o seguinte:

1º) Passo – Cadastrando os Usuários:

- Se a base de usuários que farão parte do Servidor de E-mail estão cadastrados no AD, habilite a opção "Ativar autenticação no domínio" disponível em Casdatro -> Active Directory.



- Se AD não estiver configurado na rede, é necessário cadastrar os usuários na seção Cadastro -> Usuários.



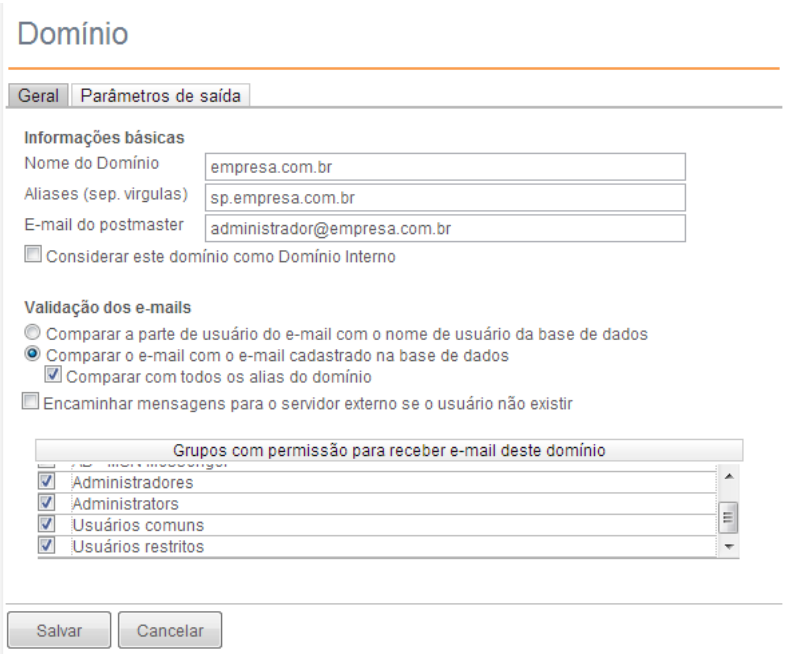
2º) Cadastrando os Serviços:

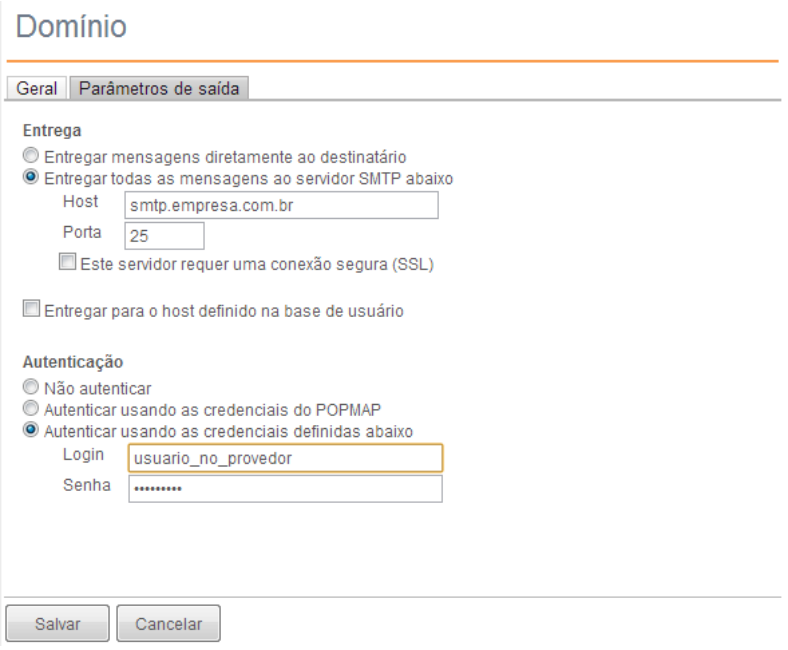
- Clique em Serviços | E-mail e verifique se os seguintes serviços estão instalados:

Obs.: Se esses serviços não estiverem instalados, será necessário instalá-los clicando no sinal + do meu Serviços.

3º) Configurando o Servidor SMTP:

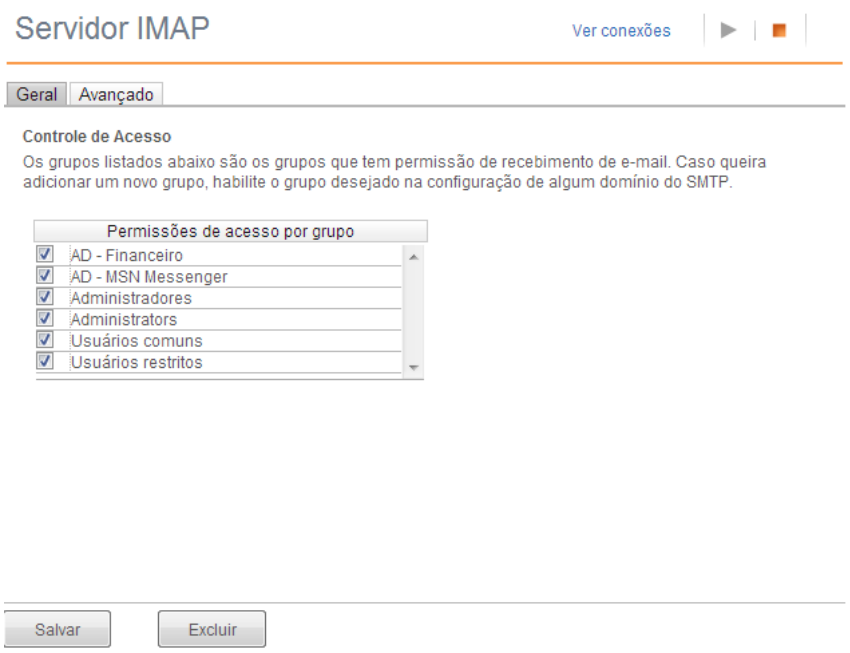
- No lado esquerdo da tela, selecione o serviço Servidor SMTP. Configure esse serviço conforme descrito no menu Serviços -> E-mail | Servidor SMTP. **Obs.:** Na guia da Domínios, é necessário adicionar um novo domínio conforme as configurações do domínio da sua empresa.





4º) Configurando o IMAP:

- No lado esquerdo da tela, selecione o serviço Servidor IMAP e habilite os grupos de usuários que terão acesso a esse serviço.



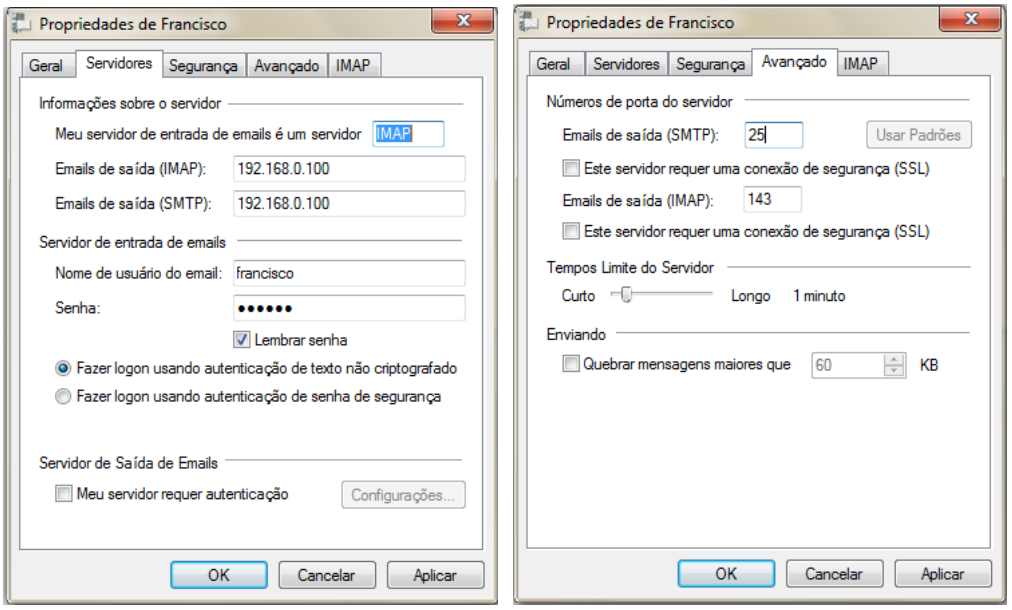
5º) Configurando o Mapeador POP:

- 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.

6º) Configurando as Estações:

- Entre na tela de configuração de contas do Cliente de E-mail da estação. Usaremos como exemplo o Windows Live Mail:
    - Selecione a conta -> Clique no menu superior Contas -> Clique em Propriedades -> Clique na guia Servidores.
    - No campo Servidor POP3, digite o IP do servidor Winconnection 7. (No nosso exemplo: 192.168.0.100).
    - No campo Servidor SMTP, digite o IP do servidor Winconnection 7. (No nosso exemplo: 192.168.0.100).
    - No campo Usuário, coloque o nome do usuário cadastrado na Lista de Usuários do Winconnection 7. No nosso exemplo: francisco.
    - No campo Senha, coloque a senha para o usuário no AD ou a que você criou no Winconnection 7.

      Obs.: Note que neste campo, estamos usando a senha do usuário interno (do AD ou criado no Winconnection 7) 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 7**.

Para informações sobre o Filtro de E-mail, consulte o tópico Serviços | Filtro | Filtro de E-mail.

8.2.7 Servidor SMTP

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

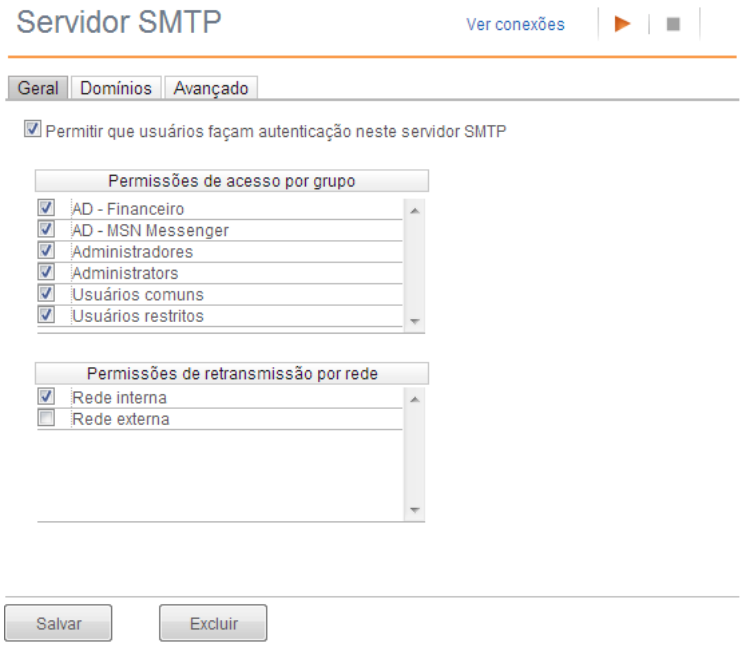
Guia Servidor SMTP:

A guia Servidor SMTP deve ser configurada sempre que o servidor de correio interno do **Winconnection 7** 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 7** 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 no tópico *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 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:

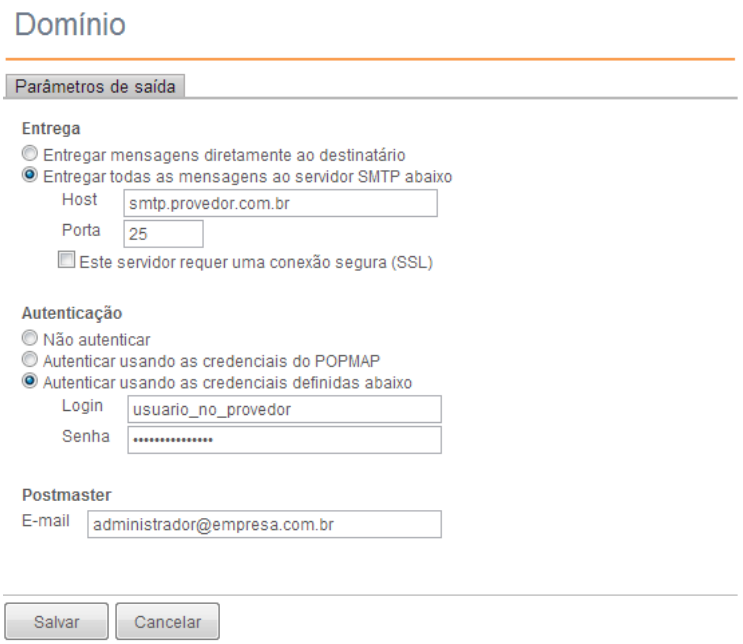
- **Entrega**
  - **Entregar mensagens diretamente ao destinatário:** Ativando-se esta opção, o Winconnection 7 passa a entregar as mensagens diretamente para o SMTP de destino do e-mail.

    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.
- **Autenticação**
  - **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.

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



Ao adicionar um novo domínio, além das opções de Parâmetros de Saída descritas acima, 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
  - **E-mail 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.
  - **Considerar este domínio como Domínio Interno:** Se esta opção for habilitada, este domínio será considerado como o domínio interno.
- **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:

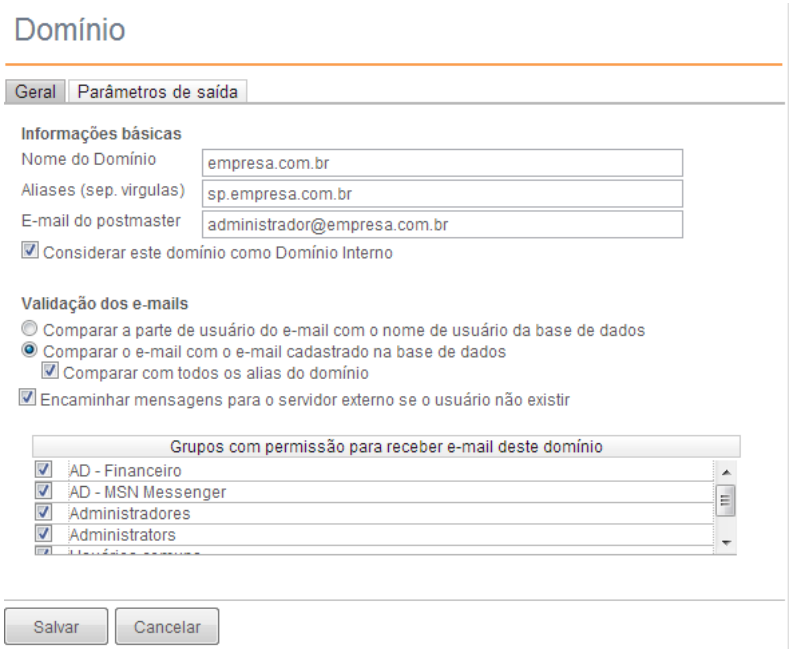
    Login: joao

    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 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 7**.
    - **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.
  - **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.
- **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 7** receber uma mensagem.

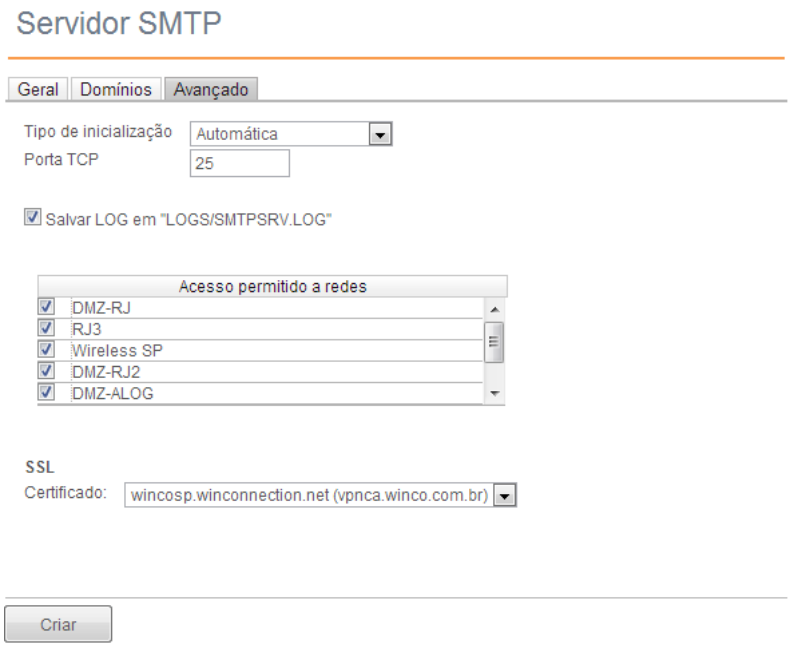


Guia Parâmetros de Saída:

Essa guia deve ser configurada conforme as instruções mencionada acima.

Guia Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta TCP:** É a porta de entrega externa do *Servidor SMTP* do Winconnection 7, 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.
- **Salvar LOG em "LOGS/SMTPSRV.LOG":** O arquivo em bloco de notas (SMTPSRV.LOG) será criado no diretório *C:\Arquivos de programas\Winco\Winconnection 7\LOGS* e conterá todas as informações referentes a este serviço.
- **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.



8.2.8 Webmail (Mobile)

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

O serviço *Webmail (Mobile)* permite que os usuários, dentro da empresa ou em trânsito, tenham acesso às suas caixas postais, lendo e enviando e-mails internos ou externos.

Guia Geral:

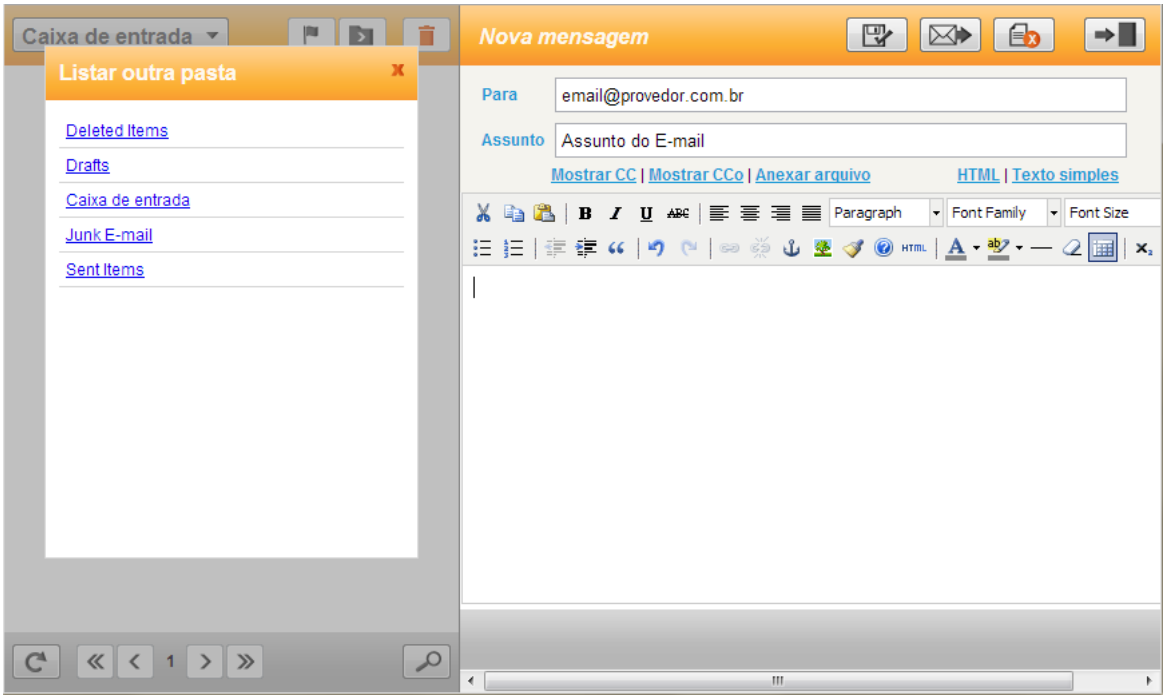
Este serviço é integrado ao serviço *Web* e por padrão acessado na porta 80.

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.

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



Guia Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Salvar LOG em "LOGS/WEBMAIL.LOG":** O arquivo em bloco de notas (WEBMAIL.LOG) será criado no diretório C:/Arquivos de programas/Winco/Winconnection 7/LOGS e conterá todas as informações referentes a este serviço.

Webmail (mobile)

Geral | Avançado

Tipo de inicialização: Automática

☑ Salvar LOG em "LOGS/WEBMAIL.LOG"

8.3 Locais

8.3.1 Cache de DNS

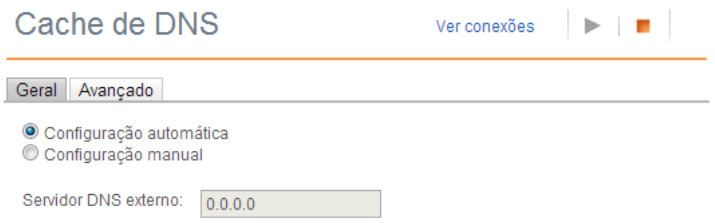
Permite que as estações resolvam o *Domínio dos Servidores da Internet* localmente.

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

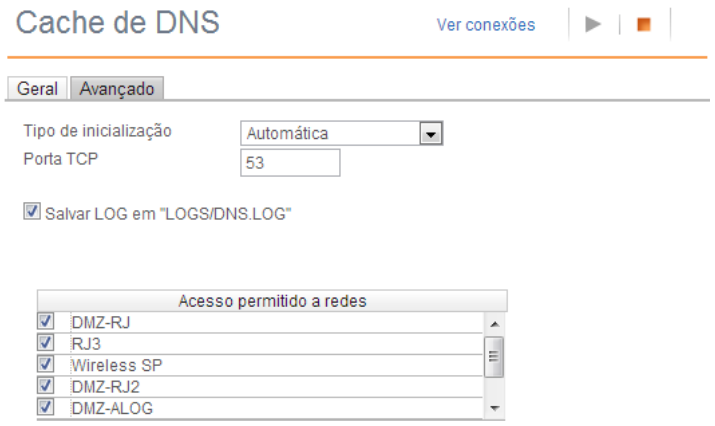
Guia Geral:

- **Configuração Automática:** Habilita o **Winconnection 7** 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 Avançado:

- **Tipo de inicialização:** Define o tipo de inicialização deste serviço. As opções disponíveis são: Manual, Automática e Manter o último estado.
- **Porta TCP:** Normalmente a porta padrão é 53 e não deve ser alterada.
- **Salvar LOG em "LOGS/DNS.LOG":** *O arquivo em bloco de notas (DNS.LOG)* será criado no diretório *C:/Arquivos de programas/Winco/Winconnection 7/LOGS* e conterá todas as informações referentes a este serviço.
- **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.



8.3.2 Servidor WWW

O serviço Servidor WWW do **Winconnection 7** permite a hospedagem de sites diretamente no servidor de rede. A página inicial (index.html) será uma página do Winconnection 7 que poderá ser alterada. A localização da página está no *Diretório Base* para serviço dos sites (document root).

Veja a seguir as principais características deste serviço:

- 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;

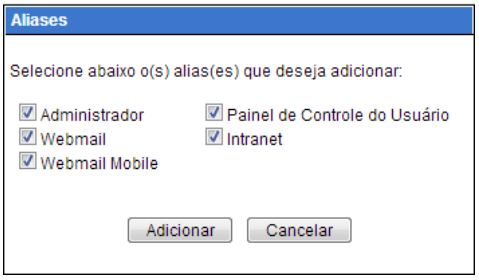
O serviço Servidor WWW também serve páginas externas. Para isso, basta apenas que o acesso externo seja permitido. Uma regra no firewall é automaticamente criada no **Winconnection 7** permitindo o acesso à porta 80, quando o administrador da rede desejar que as páginas sejam acessadas externamente.

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Guia Servidor WWW:

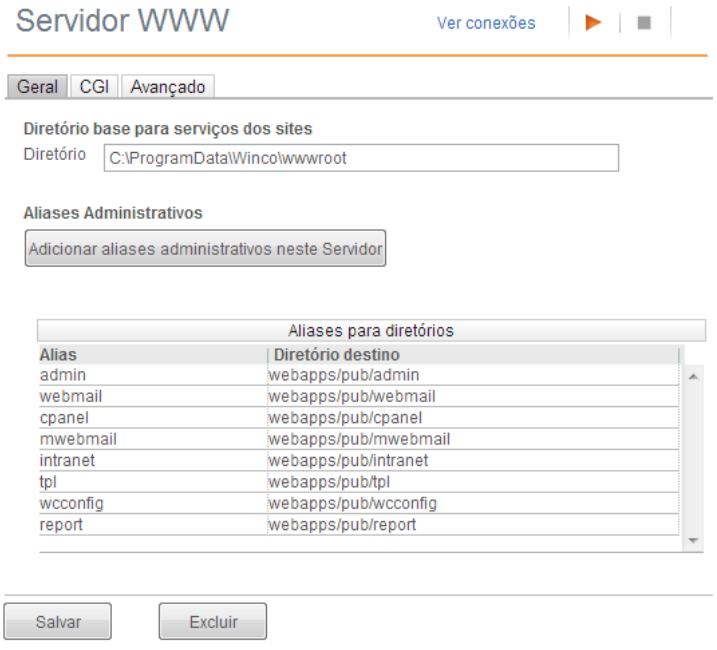
- **Diretório base para serviço dos sites:** Diretório onde se encontra as páginas Web. Ao configurar este diretório, o **Winconnection 7** passa a disponibilizar as informações contidas nele como um site na internet.
- **Aliases administrativos:** Adiciona os aliases administrativos do programa: Administrador, Webmail, Webmail (Mobile), Painel de Controle do Usuário e Intranet.



- **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

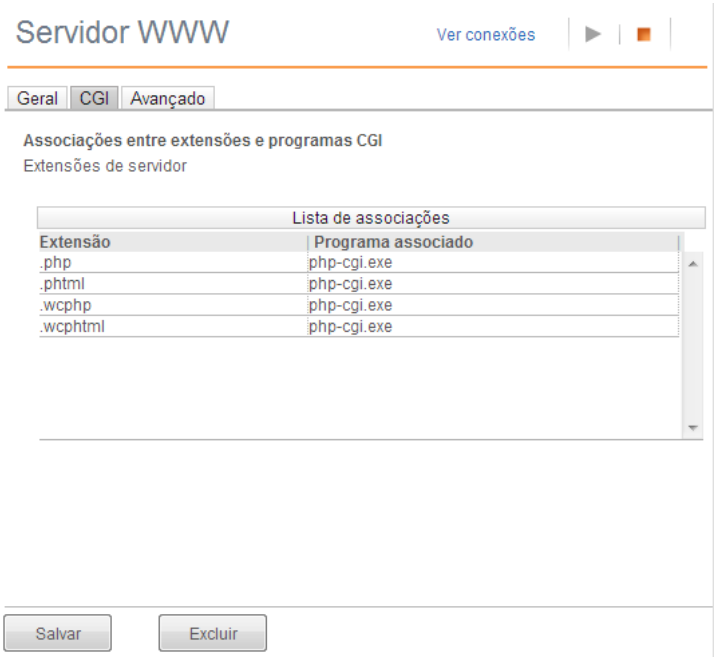
  Quando se digitar *http://servidor/proposta* o **Winconnection 7** listará os arquivos daquele diretório. Esta solução é extremamente útil para compartilhar informações para os colaboradores, via WEB.



Guia CGI:

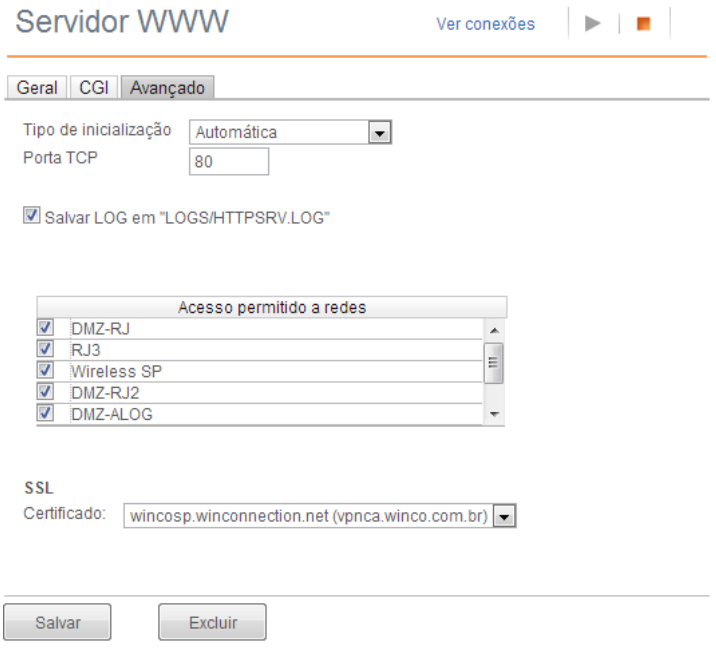
- **Extensões de servidor:** Permite incluir as extensões associadas às aplicações CGI. Toda vez que tiver determinada extensão listada, vai executar determinado CGI.

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



Guia Avançado:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 7**.
- **Porta TCP:** A porta padrão para este serviço é 80, mas pode ser alterada nesse campo.
- **Salvar LOG em "LOGS/HTTPSRV.LOG":** O arquivo em bloco de notas (HTTPSRV.LOG) será criado no diretório *C:/Arquivos de programas/Winco/Winconnection 7/LOGS* e conterá todas as informações referentes a este serviço.
- **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.



8.3.3 Servidor FTP

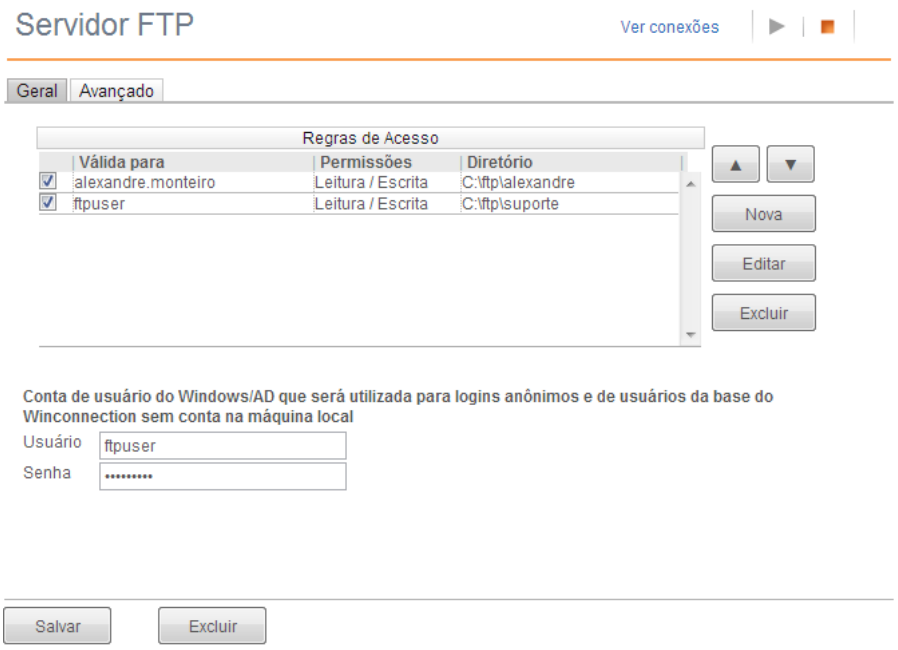
Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Guia Geral

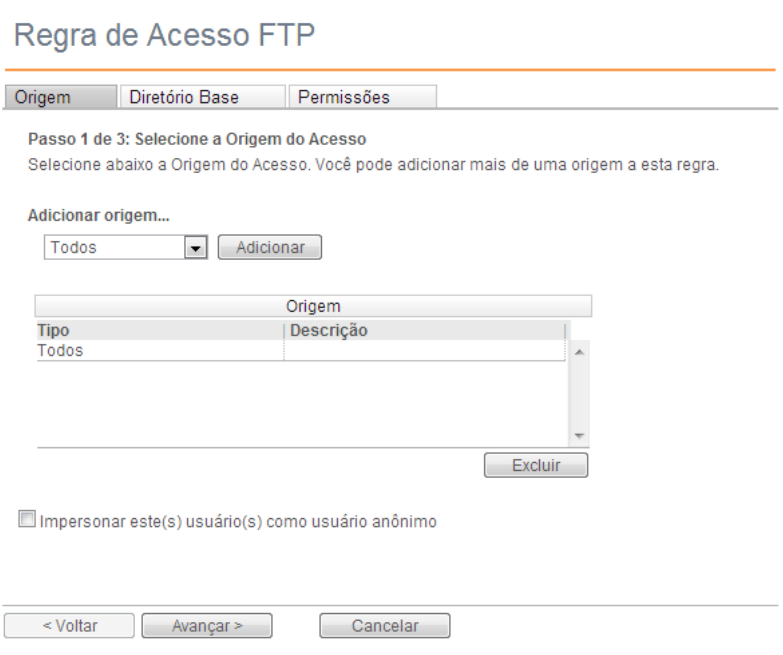
Nesta guia, é possível definir novas regras de acesso para o serviço Servidor FTP.

Também é necessário, definir a conta de usuário do Windows/AD que será utilizada para logins anônimos e de usuários da base do Winconnection sem conta na máquina local.

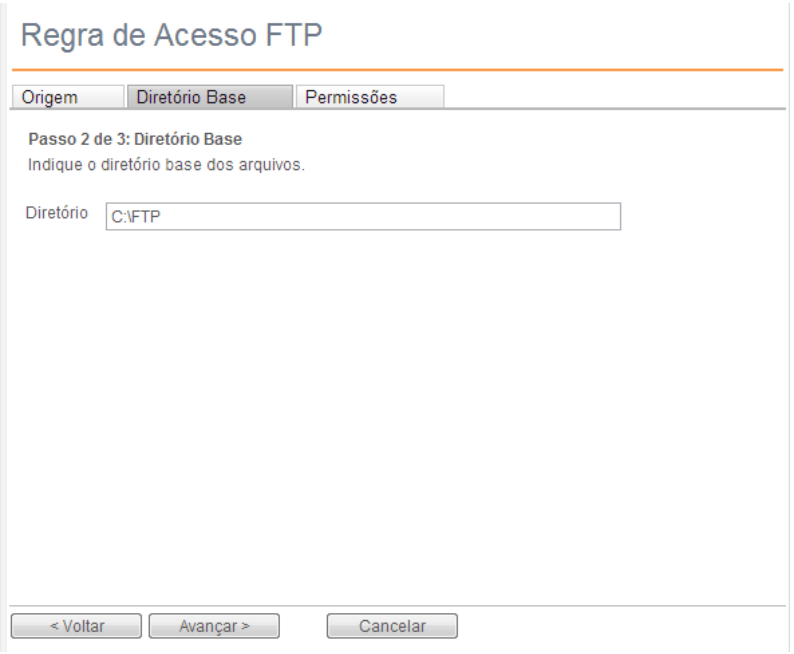


Ao adicionar ou editar uma nova regra de acesso, é exibido um *Assistente de Configuração* com 3 etapas:

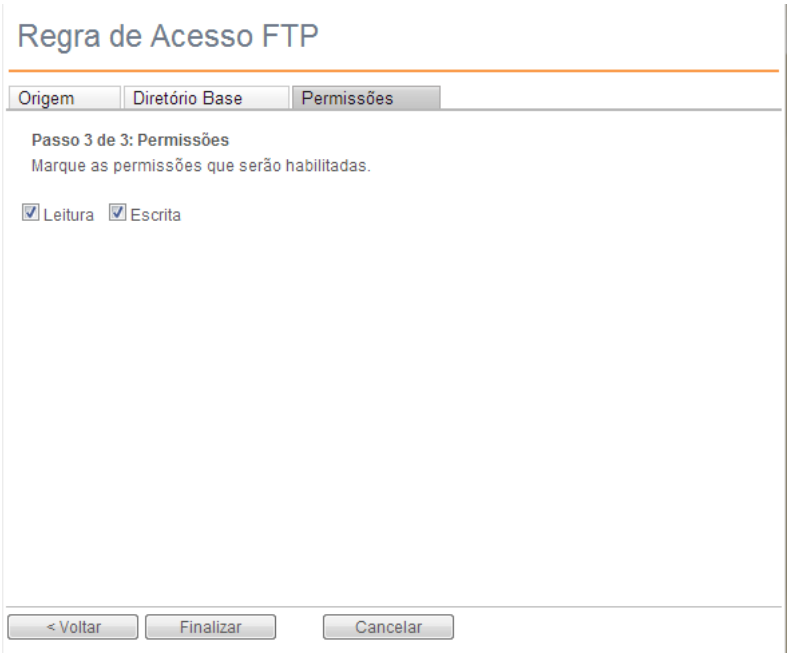
- **Passo 1 - Origem:** Selecione a origem do acesso: *Todos*, *Usuário*, *Grupo*, *Usuário anônimo*. É possível adicionar mais de uma origem para a regra.



- **Passo 2 - Diretório Base:** Neste campo, indique o diretório base dos arquivos.

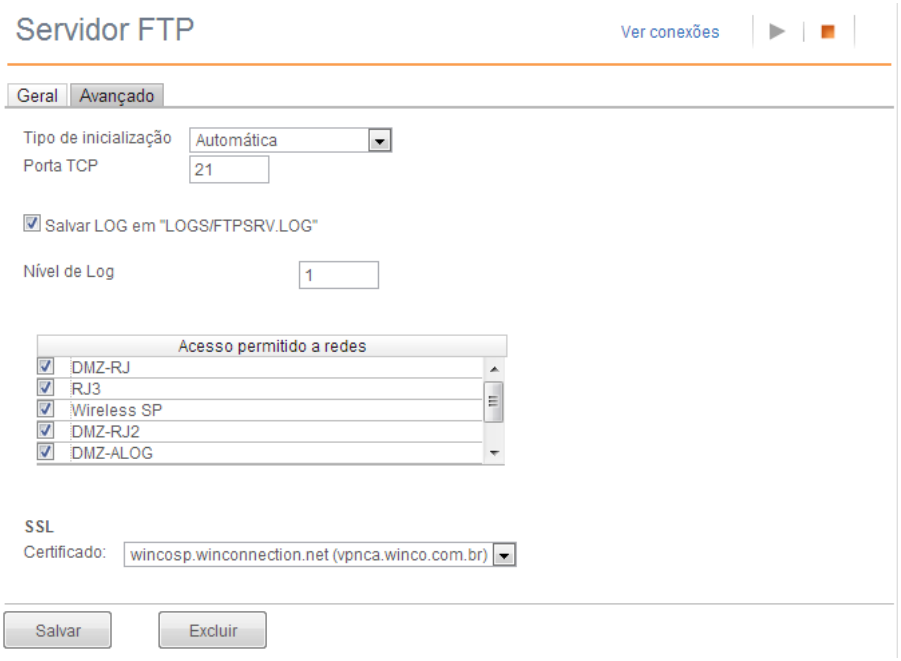


- **Passo 3 - Permissões:** Marque as permissões que serão habilitadas: Leitura e/ou Escrita.



Guia Avançado:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 7**.
- **Salvar LOG em "LOGS/FTPSRV.LOG":** O arquivo em bloco de notas (LOGS/FTPSRV.LOG) será criado no diretório C:/Arquivos de programas/Winco/Winconnection 7/LOGS e conterá todas as informações referentes a este serviço.
- **Porta:** Neste campo é definido a porta de acesso para o Servidor FTP. A porta padrão é a 21, 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.
- **SSL:** Esta opção ativa a utilização da criptografia SSL (Secure Sockets Layer). Um SSL faz com que o serviço Servidor FTP se torne um serviço seguro. O administrador da rede deverá selecionar qual Certificado SSL será utilizado.


Servidor FTP
Ver conexões
Geral
Avançado
Tipo de inicialização
Automática
Porta TCP
21
Salvar LOG em "LOGS/FTPSRV.LOG"
Nível de Log
1
Acesso permitido a redes
DMZ-RJ
RJ3
Wireless SP
DMZ-RJ2
DMZ-ALOG
SSL
Certificado:
wincosp.winconnection.net (vpnca.winco.com.br)
Salvar
Excluir

8.3.4 Servidor 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 7** 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 7** 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 7**, pois a configuração torna-se rápida e prática.

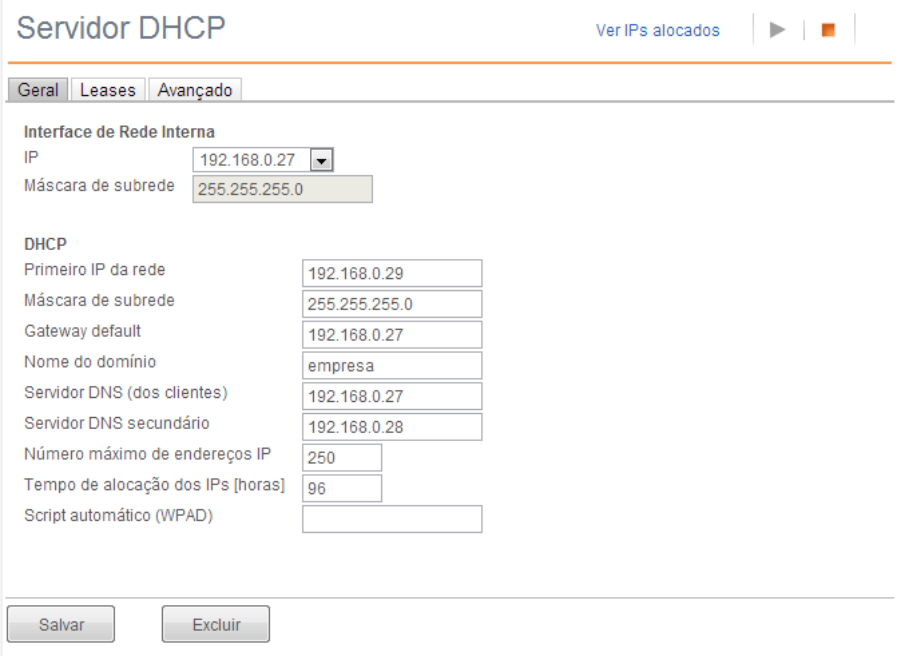
Redes que possuem Sub-Redes com faixas de IP diferentes, o uso do DHCP também seria fundamental, tanto para o desempenho da rede interna como para a utilização do **Winconnection 7**.

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

- Ações: Permite excluir o lease selecionado.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Guia Geral:

- **Interface da Rede Interna:** Neste campo, deve-se habilitar o IP/Máscara de Rede do computador onde está instalado o Winconnection 7.
- **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 7, 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 7** 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*.

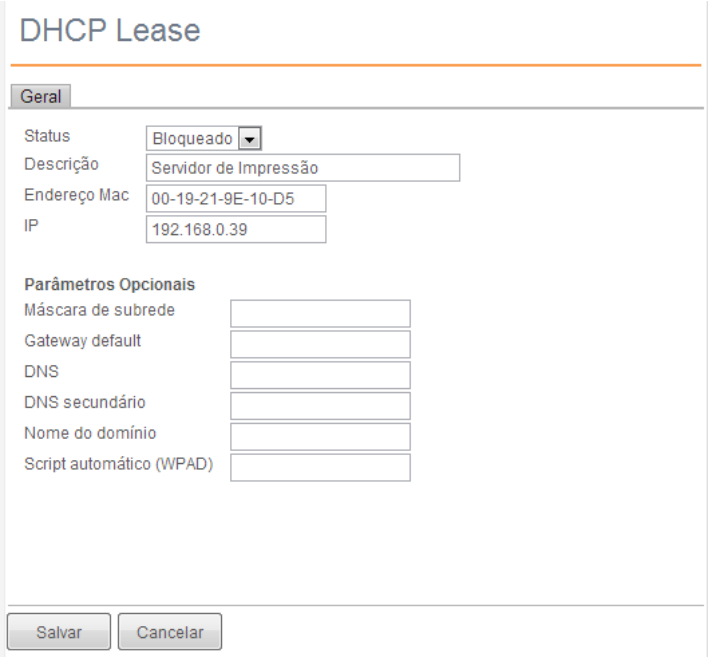


Guia Leases:

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

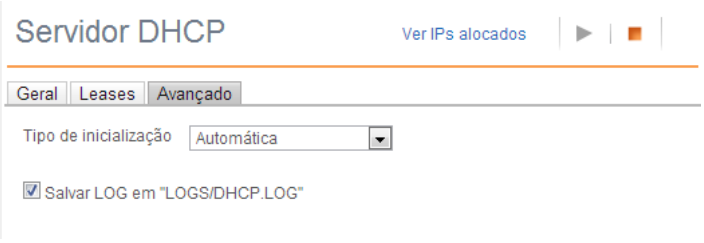
É possível *Adicionar*. *Editar* e *Excluir* a lista de *leases* usando os respectivos botões:

- **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 7**, 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 *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 Avançado:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 7**.
- **Salvar LOG em "LOGS/DHCP.LOG":** *O arquivo em bloco de notas (DHCP.LOG)* será criado no diretório *C:/Arquivos de programas/Winco/Winconnection 7/LOGS* e conterá todas as informações referentes a este serviço.



8.3.5 Winco Messenger

O Winco Messenger é um serviço do **Winconnection 7** para aplicação de mensagem instantânea em uma rede interna ou externa.

No **Winconnection 7** 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.

Ao clicar no menu Ver conexões, as seguintes opções serão oferecidas:

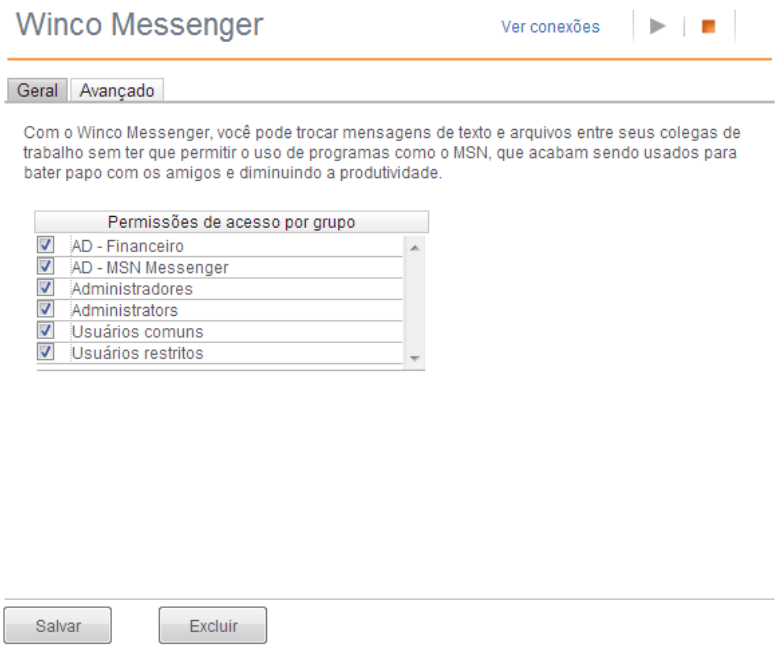
- Ações: Permite excluir ou limitar a banda para a conexão selecionada.
- Colunas: Disponibiliza as informações que poderão ser exibidas.

Guia 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 Avançado:

- **Iniciar automaticamente:** Habilite esta opção para que esse serviço seja iniciado automaticamente junto com o **Winconnection 7**.
- **Porta TCP:** A porta padrão para este serviço é 4000, e não pode ser alterada, pois o cliente sempre fará o acesso nessa porta.
- **Salvar LOG em "LOGS/IMSRV.LOG":** O arquivo em bloco de notas (IMSRV.LOG) será criado no diretório C:/Arquivos de programas/Winco/Winconnection 7/LOGS e conterá todas as informações referentes a este serviço.
- **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.

Winco Messenger

Geral | Avançado

Tipo de inicialização: Automática

Porta TCP: 4000

☑ Salvar LOG em "LOGS/IMSRV.LOG"

Acesso permitido a redes
☑ DMZ-RJ
☑ RJ3
☐ Wireless SP
☐ DMZ-RJ2
☐ DMZ-ALOG

9 Tutoriais

9.1 Proxy Transparente

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 7 (*por exemplo*: 192.168.0.1).
- No Campo *Servidor DNS Preferencial* digite o IP do servidor Winconnection 7 (*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 7 (por exemplo: 192.168.0.1).
- Na Guia *Servidor DNS Preferencial* digite o ou IIP do servidor Winconnection 7 (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 7, por exemplo: GATEWAY="192.168.0.1"
- Edite o arquivo /etc/resolv.conf e altere o valor de *nameserve*r para o IP do servidor Winconnection 7, 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.

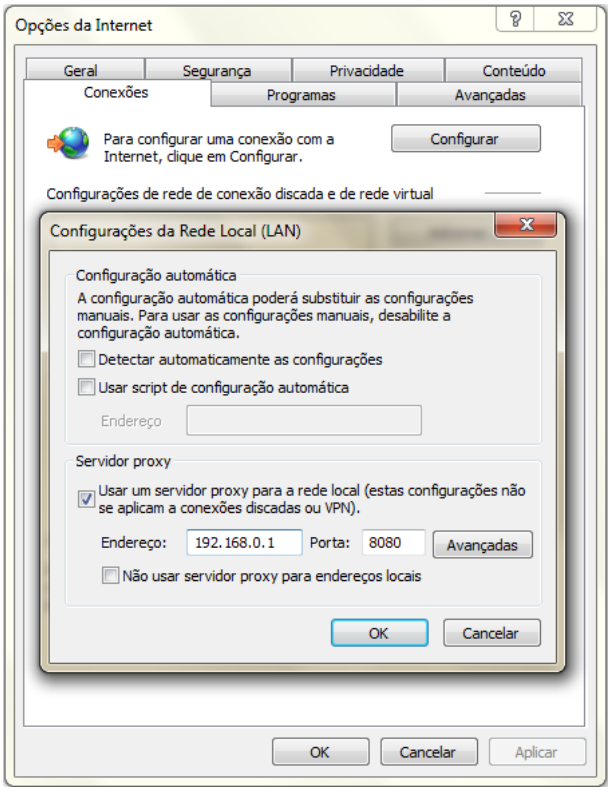
9.2 Navegação

Configuração da navegação através do Filtro Web

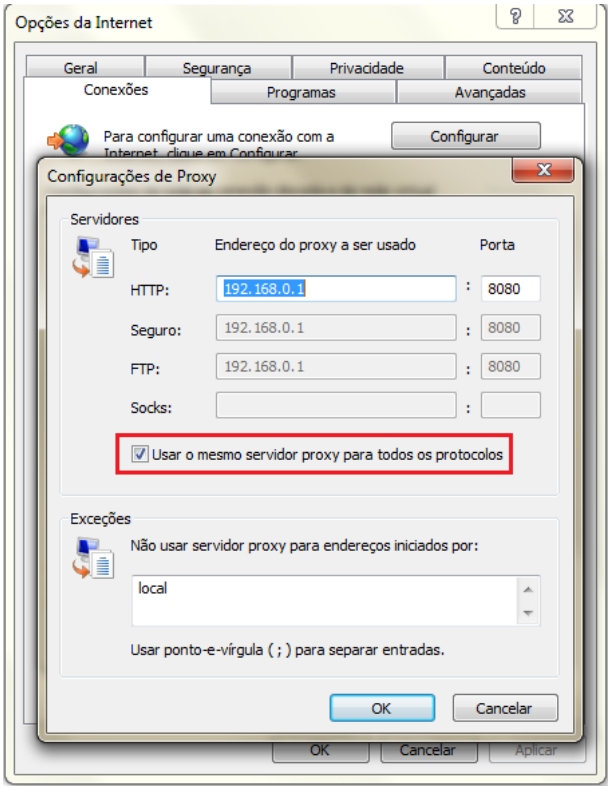
Após a instalação do **Winconnection 7**, o serviço Filtro Web é adicionado automaticamente na porta 8080 no menu de serviço Servidos de Gateway.

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 7** 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.

Configurando a navegação através do Proxy Transparente

Para configurar a navegação através do **Proxy Transparente**, realize a configuração no **Winconnection 7** citada no tópico *Saída* e configure as estações conforme descrito no tópico *Tutoriais -> Proxy Transparente.*

9.3 Winco Messenger

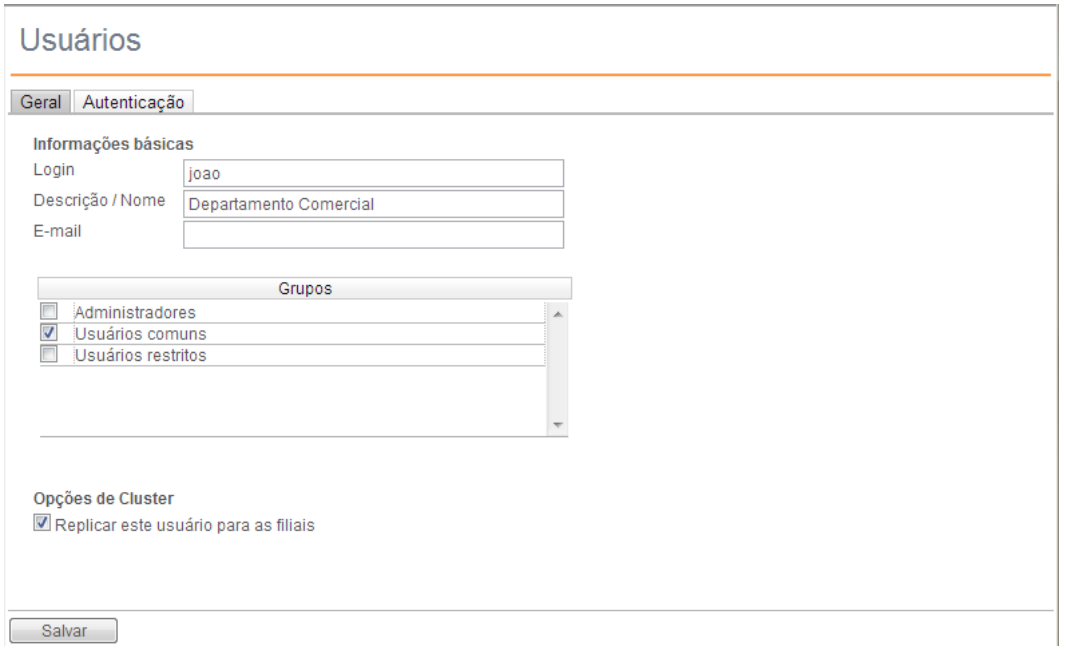
O **Winco Messenger** é integrado na base de usuários do **Winconnection 7**, e pode ser usado para troca de mensagens entre os colaboradores internos ou externos à rede da empresa. O produto possui funções de transferência de arquivos, aviso sonoro e gravação de históricos de conversas efetuadas na estação onde foi instalado.

Este módulo é gratuito para todos os usuários que adquiram as licenças do **Winconnection 7**, 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 tópico *Usuários*.



b) Clique no sinal **+** menu superior Serviços;

c) Selecione o serviço Winco Messenger e clique em "Adicionar Serviço";

d) 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 7** (por exemplo: 192.168.0.1).
- No campo "**Login**", coloque o nome do usuário que está cadastrado na lista de usuários do **Winconnection 7**.
- No campo "**Senha**", coloque a senha do usuário que está cadastrada no **Winconnection 7**.

b) Adicionar usuários:

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


MESSENGER
Adicionar Usuário
Entre com o login (ou parte dele):
Buscar
Resultado da Busca (clique no nick para adiciona-lo a sua lista):
alexandre.monteiro
aline.salazar
anderson.bravo
anderson.demario
artur.araujo
barbara.evaristo
bruna.silva
camila.roberta
WINCO

9.4 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.

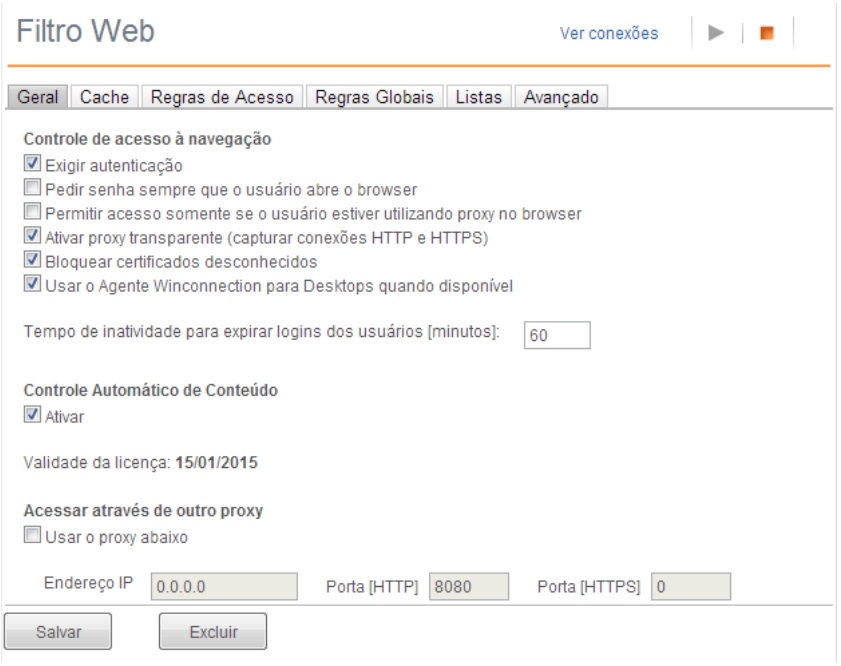
Felizmente, o *Ultrasurf* e outros programas do gênero podem ser bloqueados usando o **Winconnection 7**. Basta configurar o **Winconnection 7** utilizando técnicas de *hardening* para bloquear o *Ultrasurf* e ainda tornar a sua rede mais segura.

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 7**, clique em Serviços | Filtros | Filtro Web;
- Habilite a opção "*Ativar proxy transparent (capturar conexões HTTP e HTTPS)*" (caso contrário, o acesso à web não funcionará).

Veja um exemplo na imagem abaixo:



- Clique em *Salvar*.

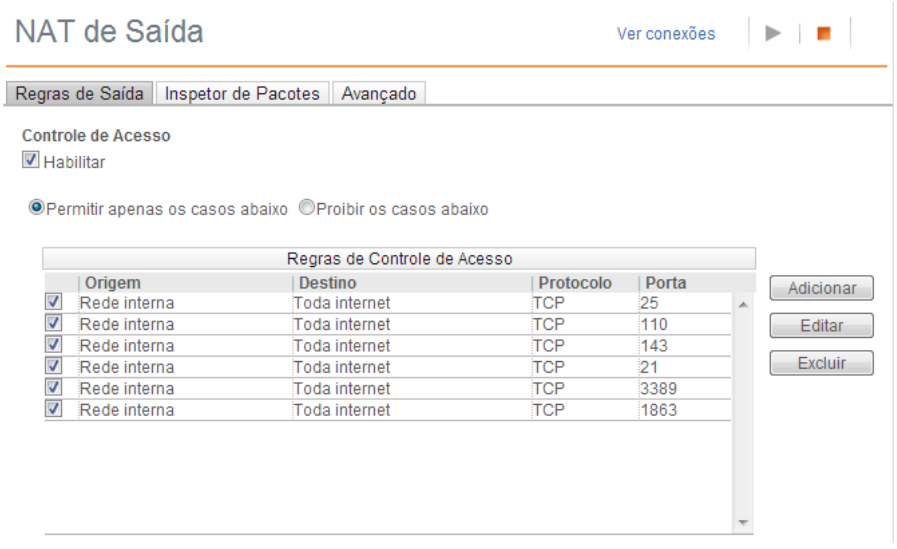
Em seguida, é necessário criar regras de acesso para habilitar as portas que são efetivamente usadas.

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 7**, clique em *Conectividade -> Nat de Saída*;
- Habilite as opções "*Habilitar*" e "*Permitir apenas os casos abaixo*";
- Clique em "*Adicionar*" e configure as regras de acordo com a necessidade da sua rede.

Veja alguns exemplos na imagem abaixo:



Segue uma lista de acessos que frequentemente usados:

- DNS – Usado para converter nomes em endereços IP: protocolo UDP porta 53
- NTP (Network Time Protocol) – Usado para acertar os relógios dos computadores: UDP porta 123
- ICMP – protocolo de controle da Internet: protocolo ICMP
- SSH – Conexão segura com servidores Linux: protocolo TCP porta 22
- RDP (Remote Desktop Protocol) – usado para conectar com Terminais Remetos (Terminal Server) – protocolo TCP porta 3389
- SMTP – Protocolo de envio de e-mail: TCP portas 25, 465 e 587
- POP – Protocolo de recebimento de e-mail: TCP portas 110 e 995
- IMAP – Protocolo de recebimento de e-mail: TCP portas 143 e 993
- FTP e SFTP – protocolo de transferência de arquivos: TCP porta 21
- VNC – protocolo de terminal remoto – UDP e TCP porta 5900
- Receita Net – para entrega de declarações da Receita Federal – TCP porta 3456

10 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.

11 Apêndices

11.1 Programação e Extensibilidade

O **Winconnection 7** 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.

Interface onDispatch

Ao fazer a entrega de uma mensagem (*onDispatch*), o **Winconection 7** 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\Winconnection7\Scritps.*

O usuário pode habilitar a interface onDispatch em *Serviços de E-mail → Armazenamento de Filas de Mensagens* e marcando a opção "*Habilitar PHP onDispatch"*.

Toolkit do Winconnection 7

Para que seja possível utilizar a *Interface onDispatch*, o **Winconnection 7** possui um *toolset* de funções que devem ser utilizadas pelo usuário na criação dos scripts.

Antes de analisarmos o *toolset* de funções do **Winconnection 7**, 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

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 7**.

11.2 Configuração Anti-Spam – Função dos Perfis

Na configuração *Anti-Spam* do **Winconection 7**, 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 o tópico *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	Endereços inexistentes não devem ser publicados ou apresentados em lugar algum. Portanto, não e-mail legítimo será enviado para	Os endereços devem ser especificados exatamente como

existentes	esses endereços.	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 7**:

- **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.*

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/Winconnection7/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.