Conectividade Social

Manual de configurações do Conectividade Social Empregador

REROP/RJ

Versão 1.0

Rio de Janeiro – Outubro / 2004

REVISÕES

Versão	Data	Propósito
1.0	19/10/2004	Criação do documento

Índice

1 Condições para acesso

Para acessar o aplicativo, o Empregador deverá atender as seguintes condições:

- Ter acesso à Internet;

- Estar certificado no aplicativo Conectividade Social;

- Estar certificado com o tipo de identificação 01-CNPJ ou 02-CEI:

- Possuir o perfil de usuário igual a Cliente Empresa, Cliente DRT ou Cliente Sindicato.

2 Requisitos para conexão

- Internet Explorer 5.0 ou superior.

- Microsoft Java Virtual Machine ativada;

- Para conexão Internet através de PROXY consultar itens 4, 5 e 6 deste guia;

- Applet Java instalada;

- Certificado digital do empregador.

3 Pré-requisitos para a utilização da Applet Java Com Internet Explorer da versão 5.01 a 6.x.

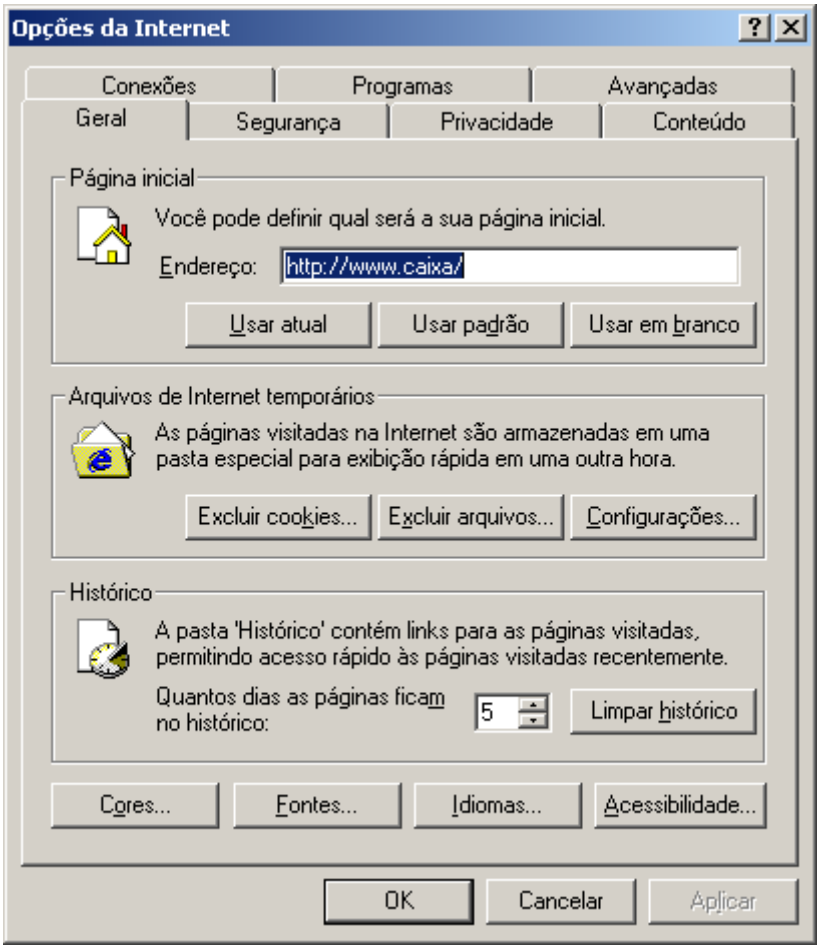
3.1 Cliente CNS Empresa

A ***Applet Java*** não pode ser executada ao mesmo tempo que o Aplicativo **CNS EMPRESA**, assim como não poderá ser utilizada de forma concorrente com qualquer outro aplicativo que utilize a porta TCP 80, tais como programas de "CHAT" (Messenger, ICQ), WEB Server entre outros.

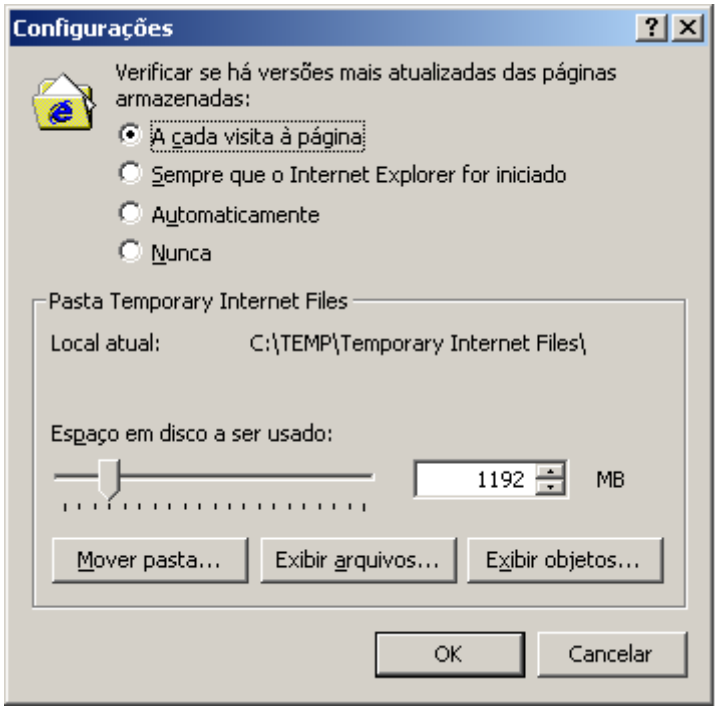
3.2 Limpeza dos arquivos pertinentes as versões anteriores da Applet Java

A versão da ***Applet Java*** compatível com o IE 6.x é diferente da anterior. Desta forma, é necessário desinstalar a antiga para que se possa utilizar a nova. Para exclusão da ***Applet*** siga os passos descritos abaixo :

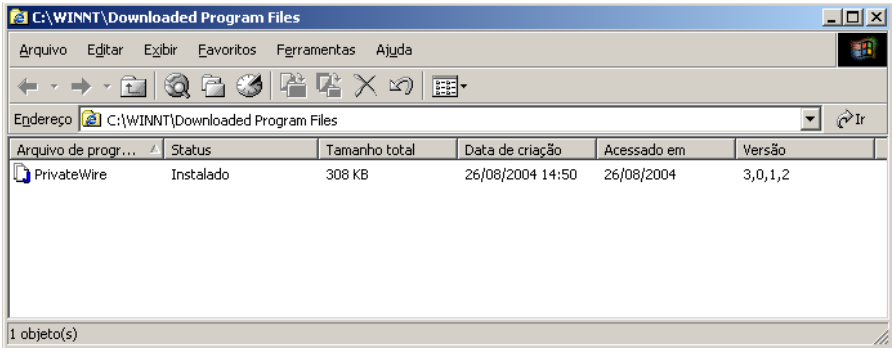
• No Internet Explorer, acessar a opção **FERRAMENTAS > OPÇÕES DA INTERNET**, e será apresentada a tela abaixo::



• Em seguida, selecionar a opção CONFIGURAÇÕES, onde será exibida a tela conforme figura abaixo:



• Para finalizar, será necessário clicar no botão EXIBIR OBJETOS onde será mostrada a tela com a lista dos itens instalados, incluindo a opção PRIVATEWIRE que representa a instalação da APPLET. Para desinstalar, será necessário selecionar o item PRIVATEWIRE e removê-lo.



3.3 Conexão Internet:

A conexão com a Internet pode ser direta ou através de utilização de proxies ou firewalls com ou em o uso de NAT. Por definição o proxy recebe a requisição de conexão HTTP do usuário, processam essa requisição e resgatam os dados do Host requisitado e repassam estes dados para o usuário. Esta solução não é adequada para ser utilizada com a conexão do Applet Java já que os dados que o proxy recebe são criptografados e são interpretados como dados corrompidos pelo proxy, é necessária uma conexão direta ao host sem que o proxy utilize mecanismos de controle e cache para a conexão.

3.4 Direitos do Usuário:

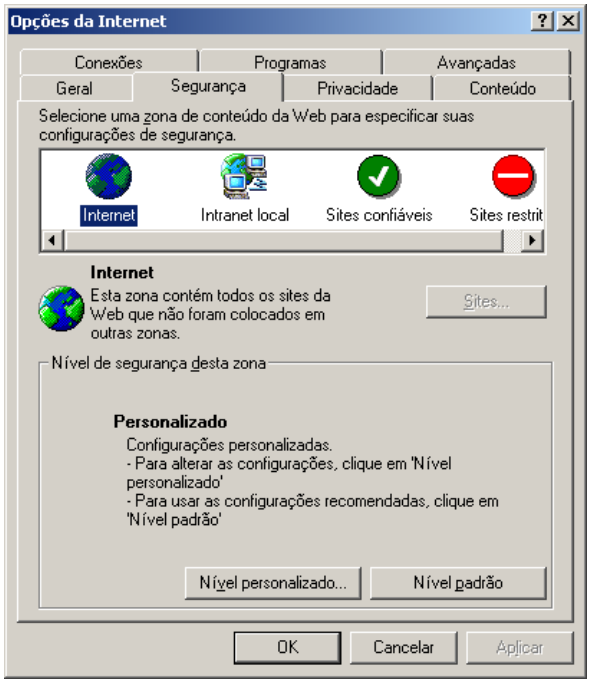
Usuário deve ter permissão de administrador ou equivalente no sistema operacional a ser instalada a ***Applet Java***.O Usuário deve ter este alto nível de permissão não só para instalar a ***Applet*** mas também para que possam ser efetuadas as configurações pertinentes ao Item.

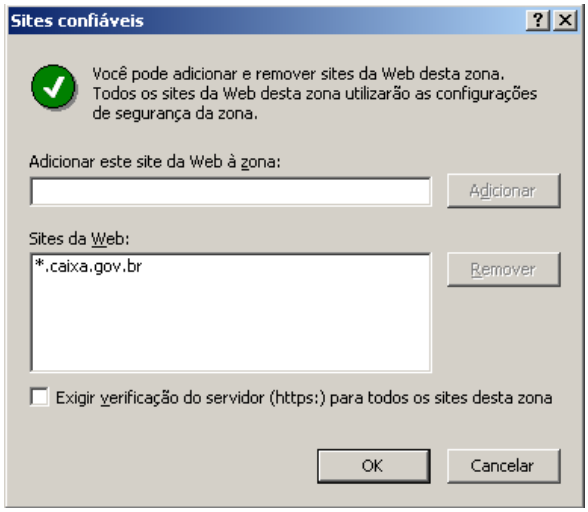
3.5 Navegador Internet:

Internet Explorer da versão 5.01 ou superior com a VM (Virtual Machine)
Para que o Internet Explorer 6.x funcione corretamente ele deverá ter sido instalado posteriormente a versão 5.01 ou 5.0 para que a VM (Virtual Machine) esteja funcionando corretamente.A Applet Java necessita ainda das configurações abaixo descritas:

4 Configurar o Internet Explorer

- Siga a opção **Ferramentas** do menu superior do seu Internet Explorer
- Selecione **Opções da Internet**
- Selecione a aba **Segurança**
- Selecione o ícone **Sites Confiáveis** e clique em **Sites**
- Em **<Adicionar este Site da WEB a Zona :>** Digite o texto : ***.caixa.gov.br**
- Desabilite a caixa de diálogo **Exigir verificação do Servidor (https) para todos os sites desta Zona** conforme a figura abaixo e tecle OK.

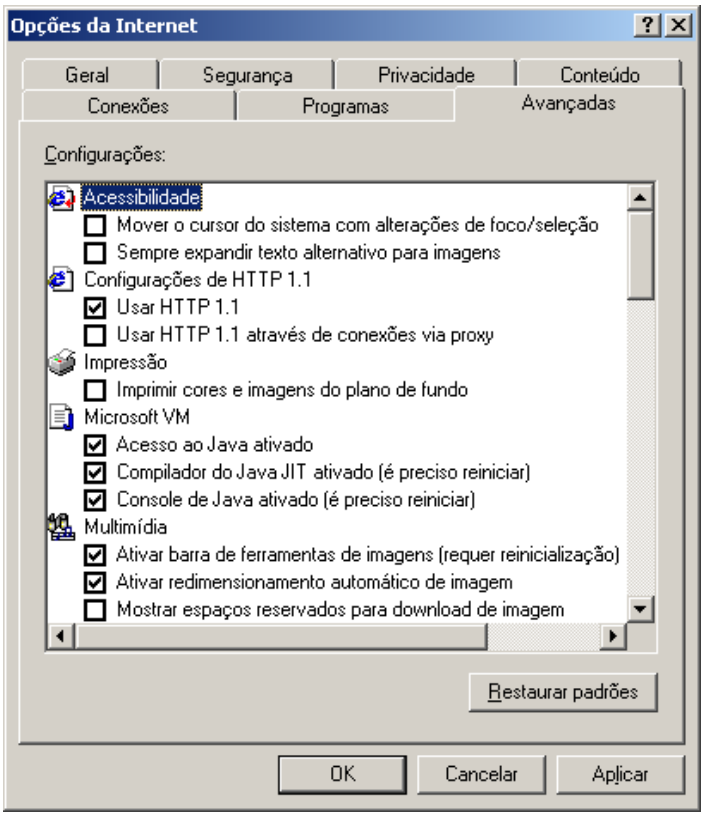




- Selecione o ícone **Sites confiáveis** e clique em **Nível Personalizado**
- Procure pelo grupo **Plug-ins e controles ActiveX** e pela opção **Inicializar e executar scripts de controles ActiveX não marcados como seguros.**

- Você será questionado se deseja realmente modificar as configurações de segurança para esta zona. Clique em **Sim.** Realizar o mesmo procedimento selecionado a opção INTRANET

- Selecione a aba **Avançadas**



- Procure pelo grupo **Microsoft VM** ou simplesmente **VM**
- Habilite todas as três opções
- Clique em **OK**
- Reinicie a máquina.

- Após a maquina ter sido reiniciada abra o Internet Explorer e digite no navegador a URL para acesso ao CS/E (www.cmt.caixa.gov.br) e tecle **Enter**
- Assim que você teclar **Enter,** caso a Applet não tenha sido instalada ou tenha sido desinstalada, a tela abaixo será exibida.

- **(Essa tela é um pedido de permissão para a instalação dinâmica da applet assinada na sua máquina)**

- Ela é necessária para a autenticação e criptografia da comunicação com o Conectividade Social Empregador.
- Clique no botão **Sim**

A fim de verificar se a Applet Java Conexão Segura está funcionando corretamente, basta digitar o caminho do seu certificado e clicar no botão “i”. Uma pequena janela com informações do seu certificado deve aparecer. Caso isto não ocorra, verifique os pré-requisitos acima.

O próximo passo é verificar o acesso ao CS/E. Se a estação de trabalho estiver utilizando uma conexão discada de acesso à Internet ou a estação esteja em uma rede a qual os endereços IPs sejam públicos, provavelmente não ocorrerá nenhum problema de acesso.

Ao clicar em Login, uma nova janela será aberta com a aplicação Conectividade Social Empregador. Mas se você estiver em uma máquina que esteja na Intranet, você pode ter problemas. Se a janela abrir, ótimo, mas se uma mensagem de erro (“Falha ao trocar mensagens com o Gateway”) aparecer, atente para os procedimentos abaixo.

5 Considerações para configuração do *Proxy*

A Applet precisa de uma conexão direta ao servidor. O proxy não pode utilizar sua configuração padrão para este aplicativo. Por definição o proxy recebe uma requisição HTTP do usuário, processa essa requisição, resgata o dado do servidor e repassa este dado para o usuário. Esta solução não é adequada para o uso da conexão com o Applet Java já que os dados que o proxy recebe do cliente são criptografados e serão interpretados como dados corrompidos sendo descartados em seguida. Para que isto não ocorra é necessária uma conexão direta, isto é, sem critica entre cliente e servidor, com o proxy realizando a única tarefa de repassar os pacotes entre as partes. Mecanismos de controle (filtro HTTP) e cache para esta conexão devem permanecer desativados. Existem alguns softwares de proxy que exigem a instalação de uma infra-estrutura para este tipo de configuração.

Configurações para Proxy/Firewall

Alguns proxies possuem funções de firewall, assim como alguns firewalls possuem um proxy embutido. Independente do produto utilizado, a conexão direta deve ser criada.

A porção proxy é responsável pelo repasse dos pacotes entre as partes, enquanto a porção firewall deve permitir o acesso do cliente ao ambiente Conectividade Social Empregador.

Configurações para Firewall

O cliente Applet Java utiliza a porta 80 para comunicar com a parte servidora da aplicação, mas ao contrário do que parece, o protocolo utilizado não é o HTTP.

Por este motivo, é necessário criar regra no firewall de modo a permitir que o cliente consiga conectar-se ao ambiente Conectividade Social Empregador (Rede IP 200.201.174.0 e Máscara de Rede 255.255.255.0).

Para que o cliente tenha acesso ao Site Conectividade Social da CAIXA, sua rede deverá suportar:

- Uso do serviço WinSock Proxy do Microsoft Proxy Server ou;
- Transparent Proxy, ou;
- Socks Proxy, ou;
- NAT — Network Address Translation.
- ISA SERVER - Internet Security and Acceleration.

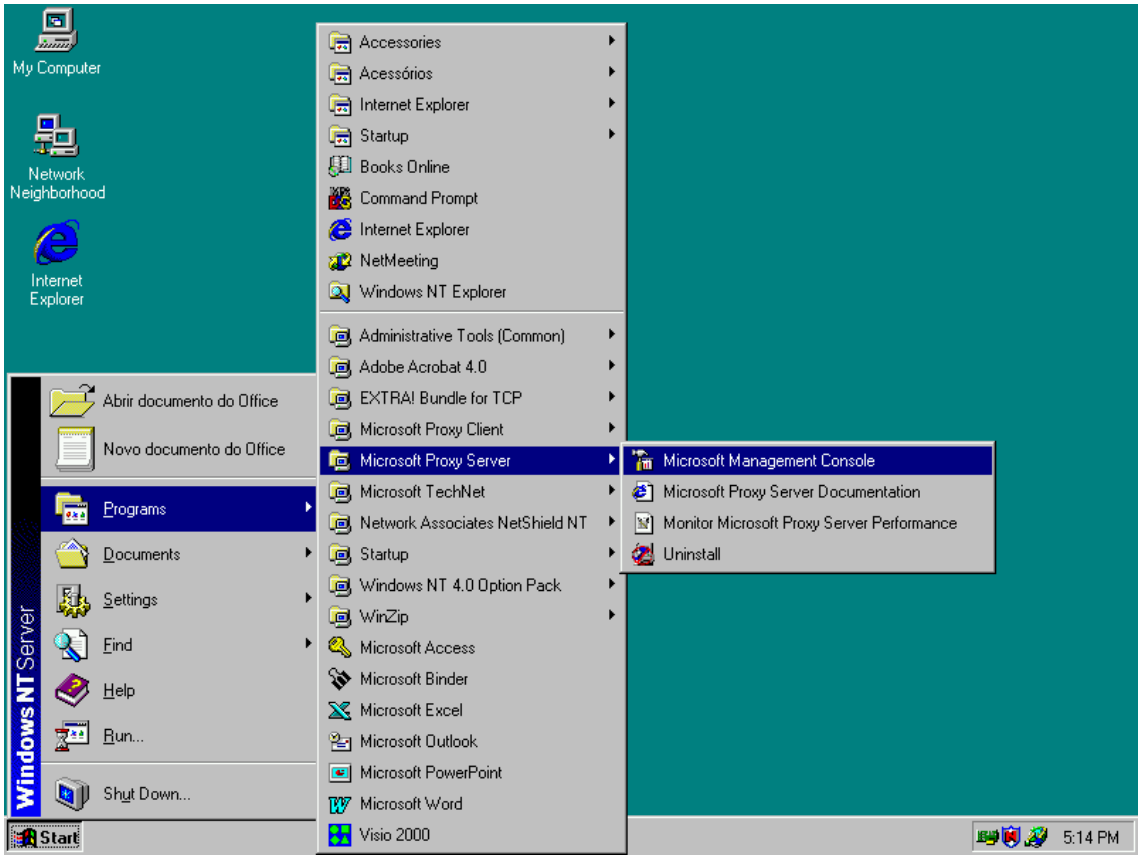
No acesso ao Site Conectividade Social da CAIXA, o módulo de segurança tem, dentre outras, a função de prover um nível de criptografia forte com chaves de sessão de 128 bits e chaves de autenticação de 1024 bits, em ambas direções. Esta criptografia faz a segurança dos dados no pacote TCP do CNS que transita entre o programa cliente e os servidores CNS. Assim sendo, o aplicativo do CNS não funciona caso sua rede local não suporte um serviço de *proxy* como descrito no parágrafo anterior. O que acontece é que, caso na rede dos clientes as estações possuam endereços IP privados, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, e o acesso à Internet seja feito apenas via web *cache proxy*, o usuário não poderá fazer acesso ao Site Conectividade Social Empregador da CAIXA pela característica de criptografia e segurança que ele implementa. No caso anterior o cliente apenas poderá utilizar a Internet para o acesso web (http/https). Para permitir que o cliente faça acesso ao Site Conectividade Social Empregador da CAIXA, sua rede deverá permitir o uso de um dos serviços descritos anteriormente, podendo ser configurada na modalidade NAT, ou seja, os endereços internos da rede continuam escondidos e inacessíveis da Internet.

6 Configuração do Microsoft Proxy Server

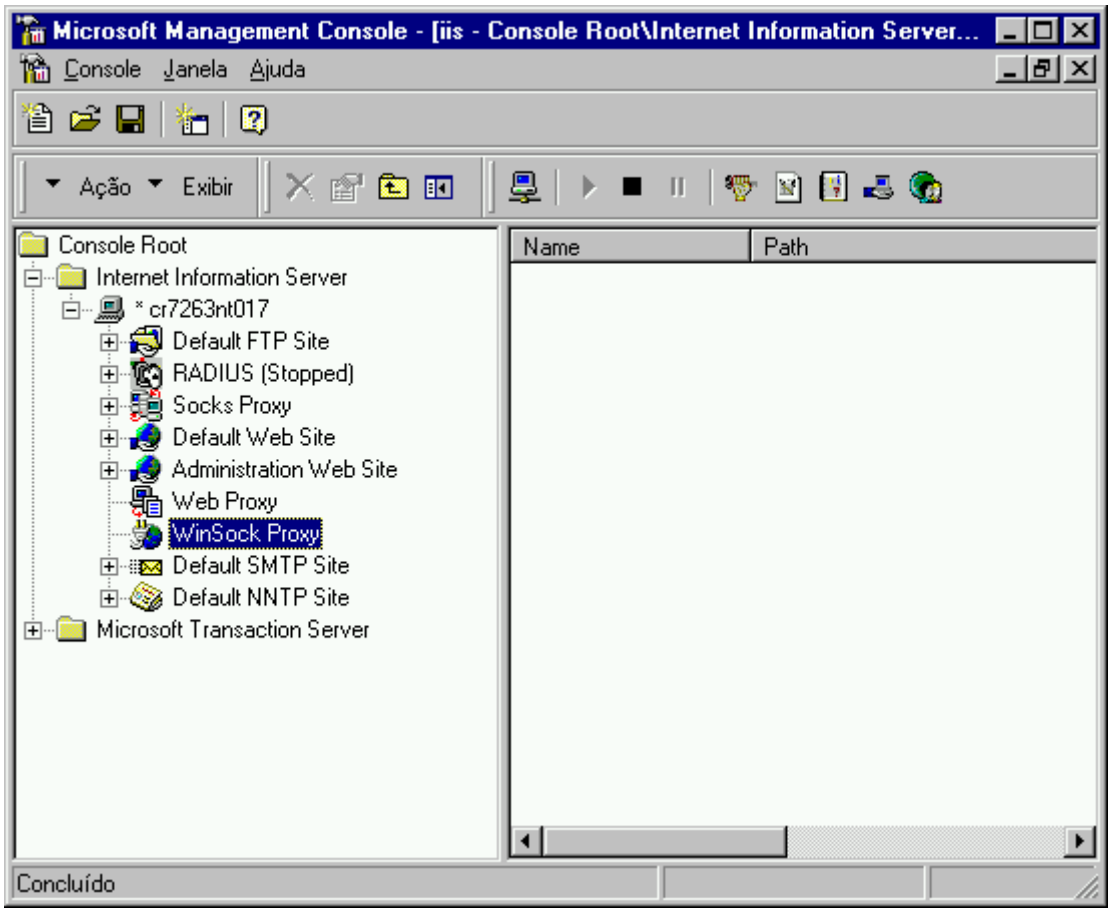
O Microsoft Proxy Server tem ambas funcionalidades de *proxy* em um único produto, ou seja, possui a função de *cache proxy*, a qual é configurada através do serviço Web Proxy e é responsável pelo armazenamento intermediário de páginas Web (http), ftp, e gopher, e também possui a função de *transparent proxy*, a qual é configurada através do serviço Winsock Proxy e é a de interesse aqui.

A seguir será exemplificada a configuração do serviço Winsock Proxy do Microsoft Proxy Server versão 2.0, instalado em um servidor Windows NT 4.0 US International, com o Option Pack igualmente instalado, para acessar o Site Conectividade Social Empregador da CAIXA, o qual se utiliza a porta TCP / 80.

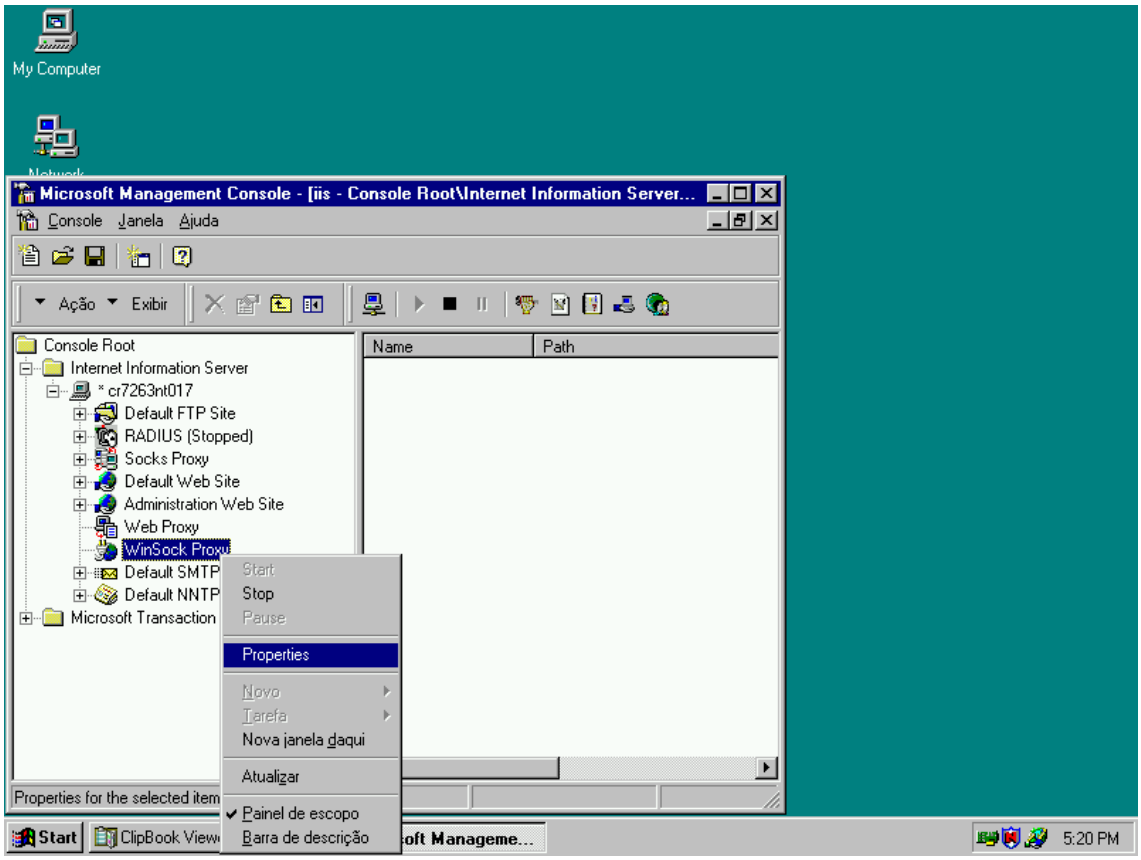
1. Inicialize a console de gerenciamento do Microsoft Proxy Server conforme a tela seguinte.



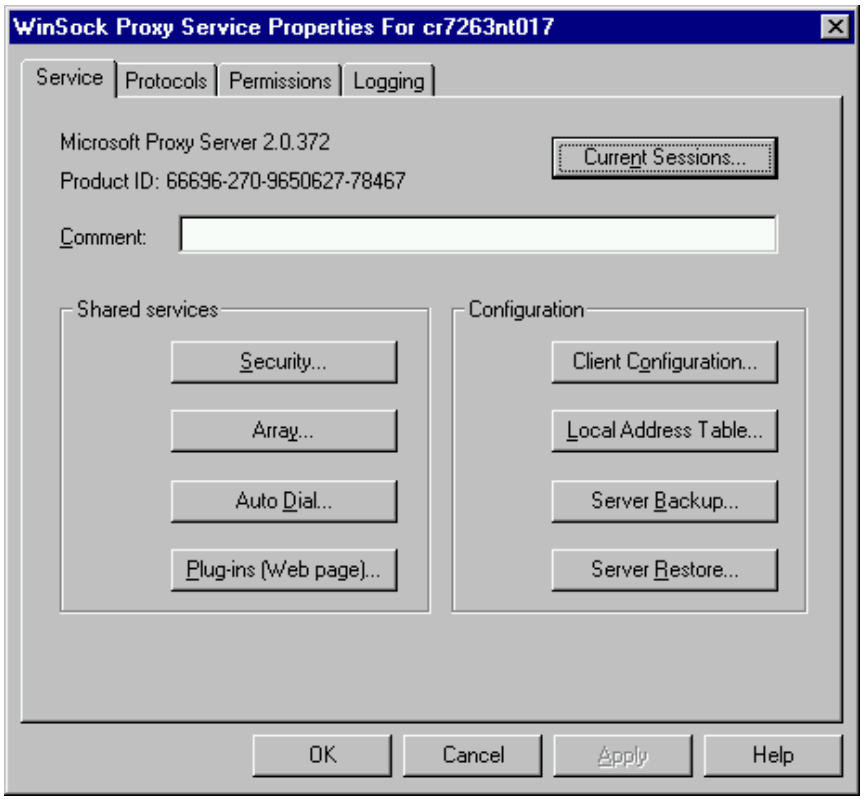
2. A seguinte janela então surgirá.



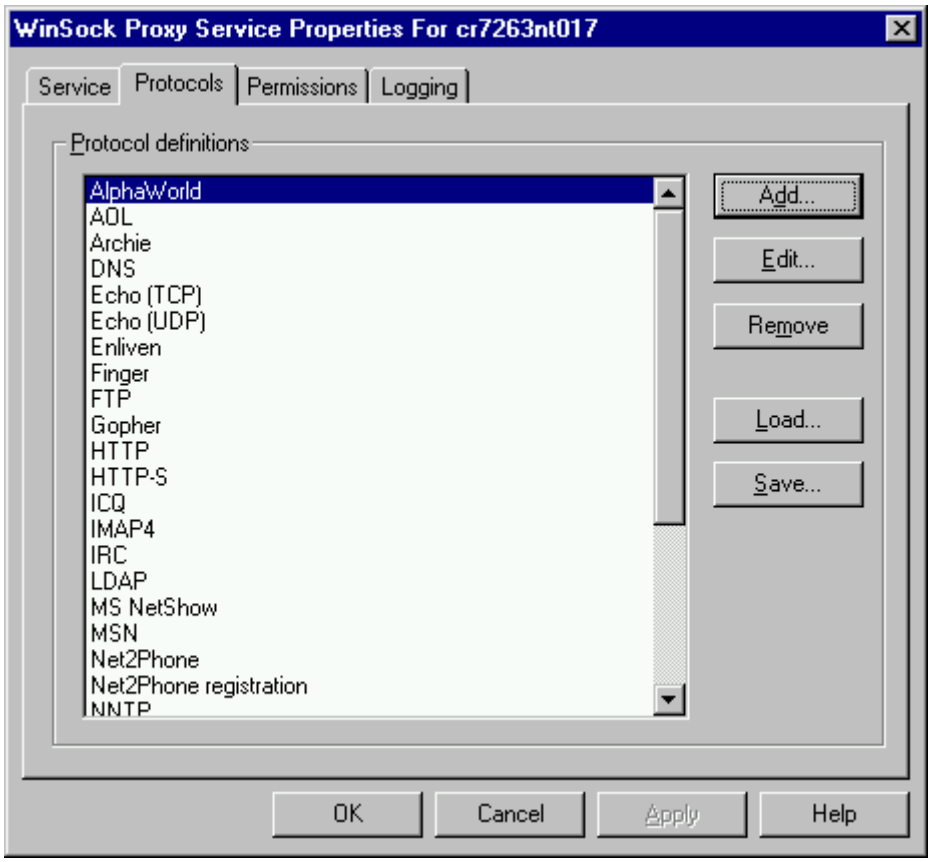
3. Inicialize a configuração do serviço Winsock Proxy conforme a tela seguinte.



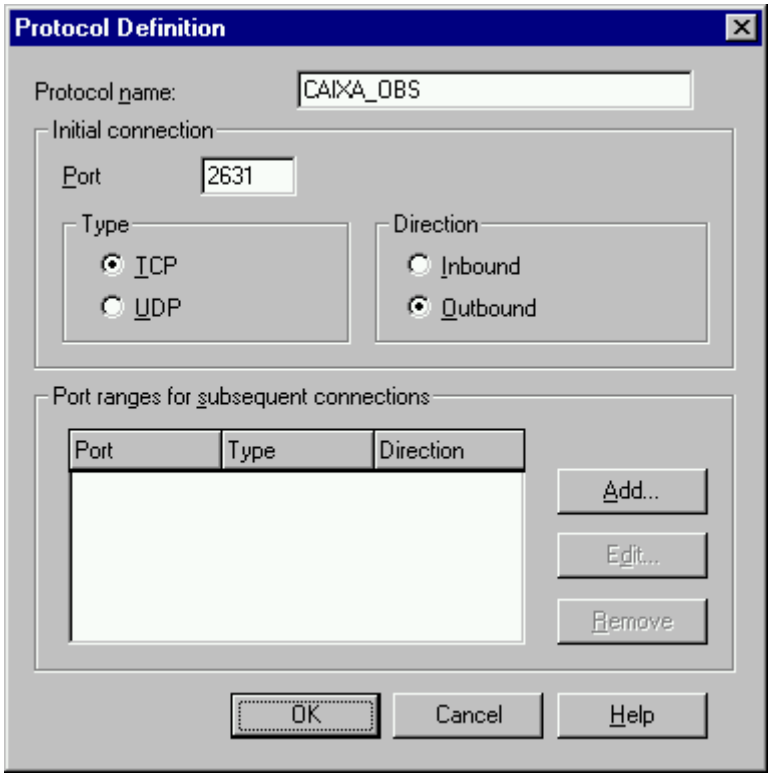
4. A seguinte janela então surgirá.



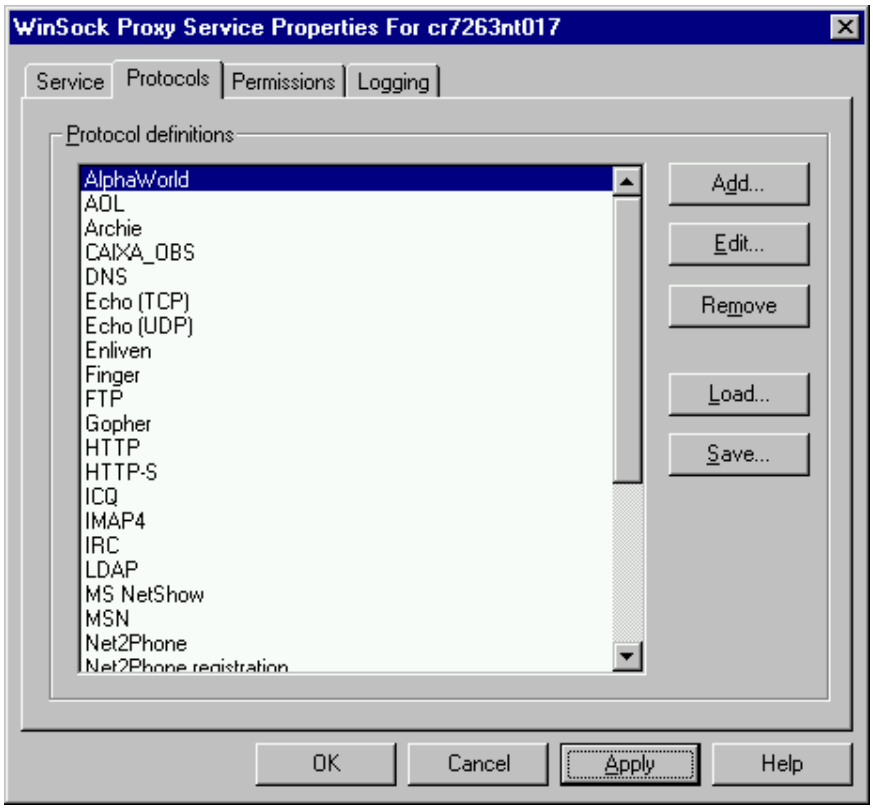
5. Selecione o *tab Protocols*. A seguinte janela então surgirá.



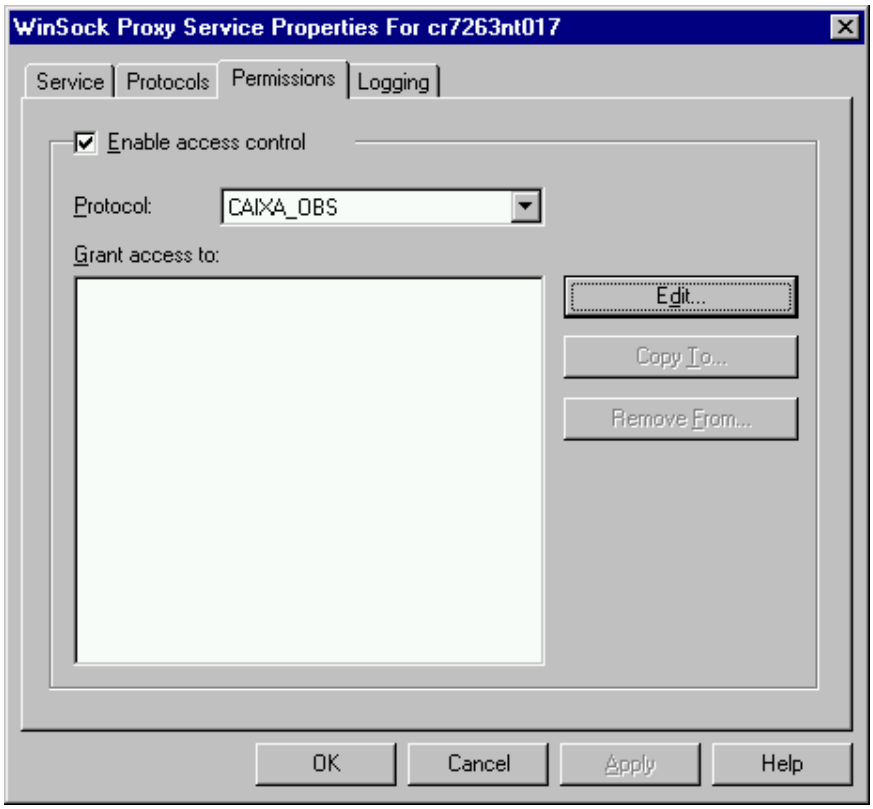
6. Pressione o botão *Add*. A seguinte janela então surgirá, porém com os campos vazios. Preencha-os conforme mostrado. E então pressione o botão *OK*.



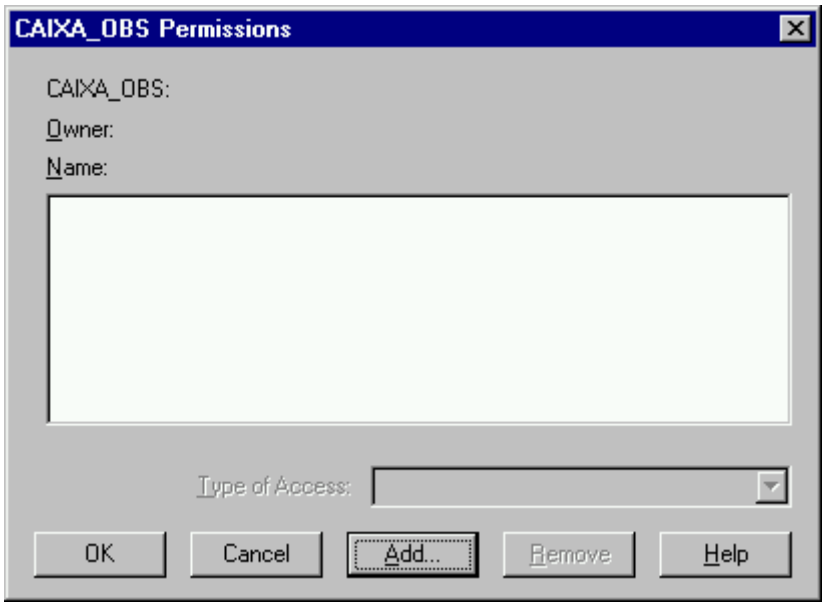
7. A seguinte tela então surgirá. Pressione o botão *Apply*.



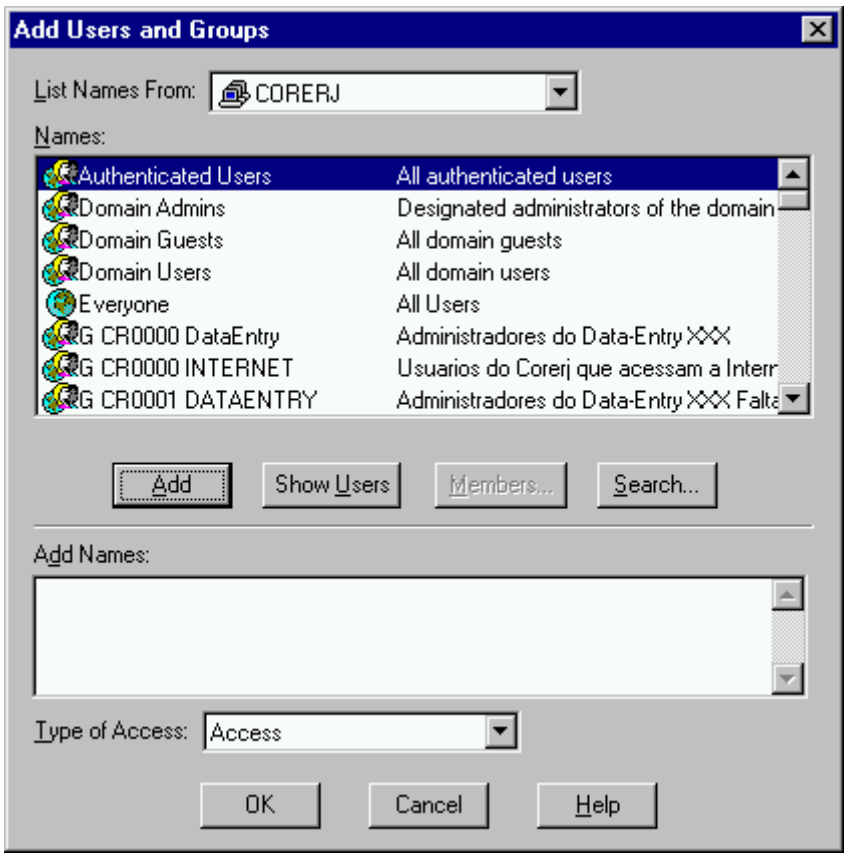
8. Selecione o *tab Permissions*. Utilize a caixa *Protocol* para selecionar o protocolo CAIXA_OBS (CAIXA_OBS ou CAIXA ??? ou talvez CAIXA_CSE ...) criado nos passos anteriores. A seguinte janela então surgirá.



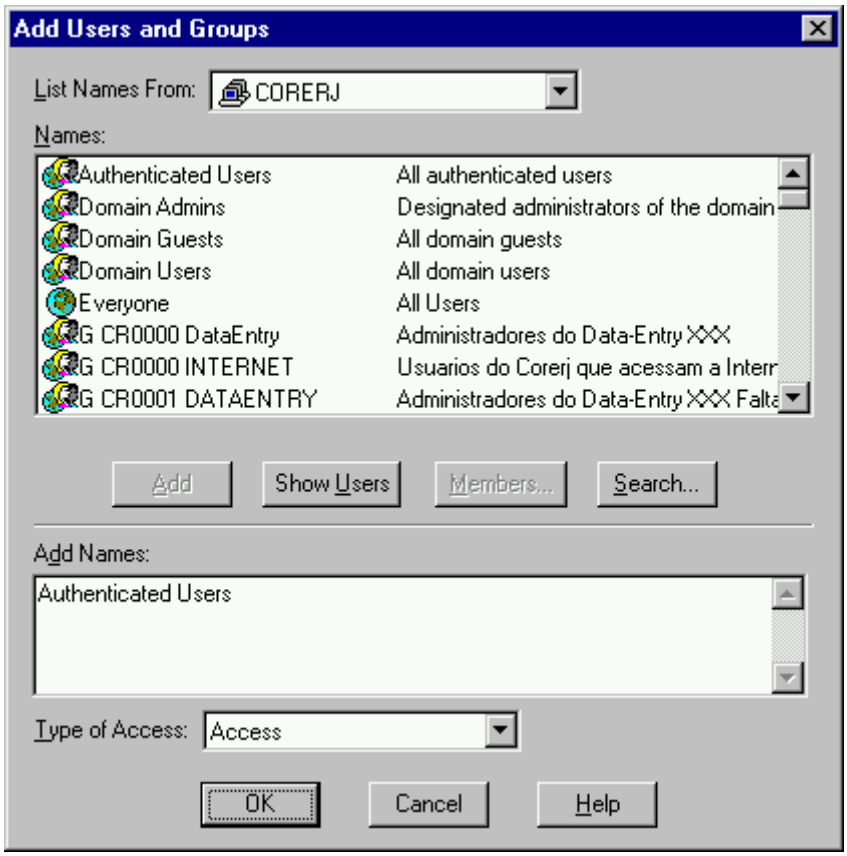
9. Pressione o botão *Edit*. A seguinte janela então surgirá.



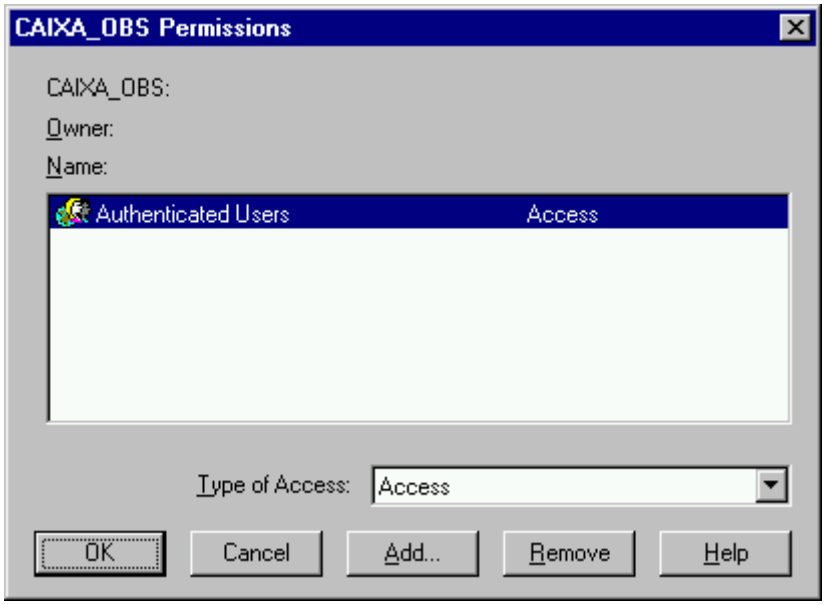
10. Pressione o botão *Add*. A seguinte janela então surgirá. Selecione o grupo de usuários desejado, aqui *AuthenticatedUsers*, ou um usuário específico pressionando o botão *ShowUsers* para mostrá-los. Então pressione o botão *Add*.



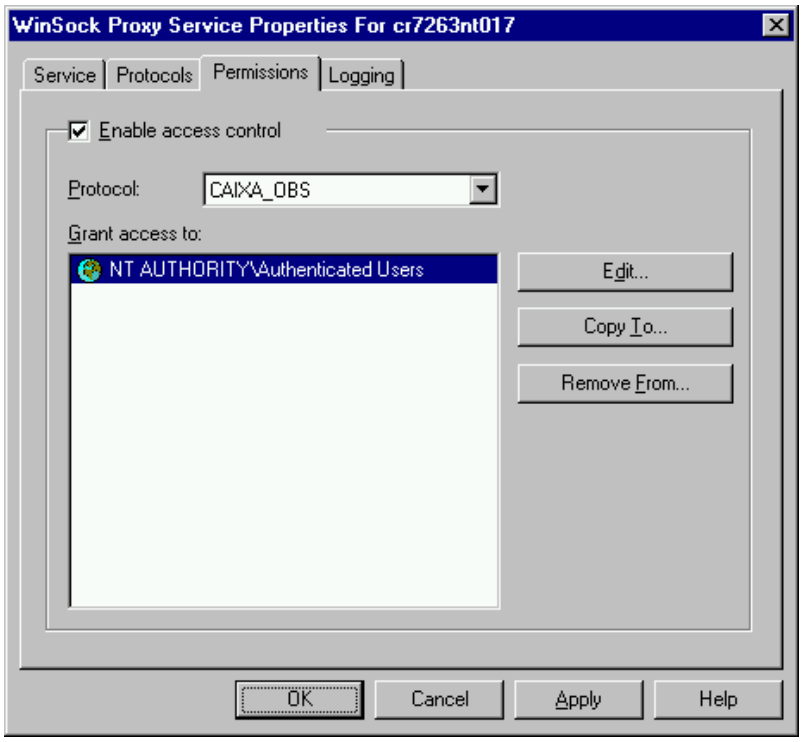
11. A seguinte janela então surgirá com o grupo, ou usuário, selecionado. Pressione o botão *OK*.



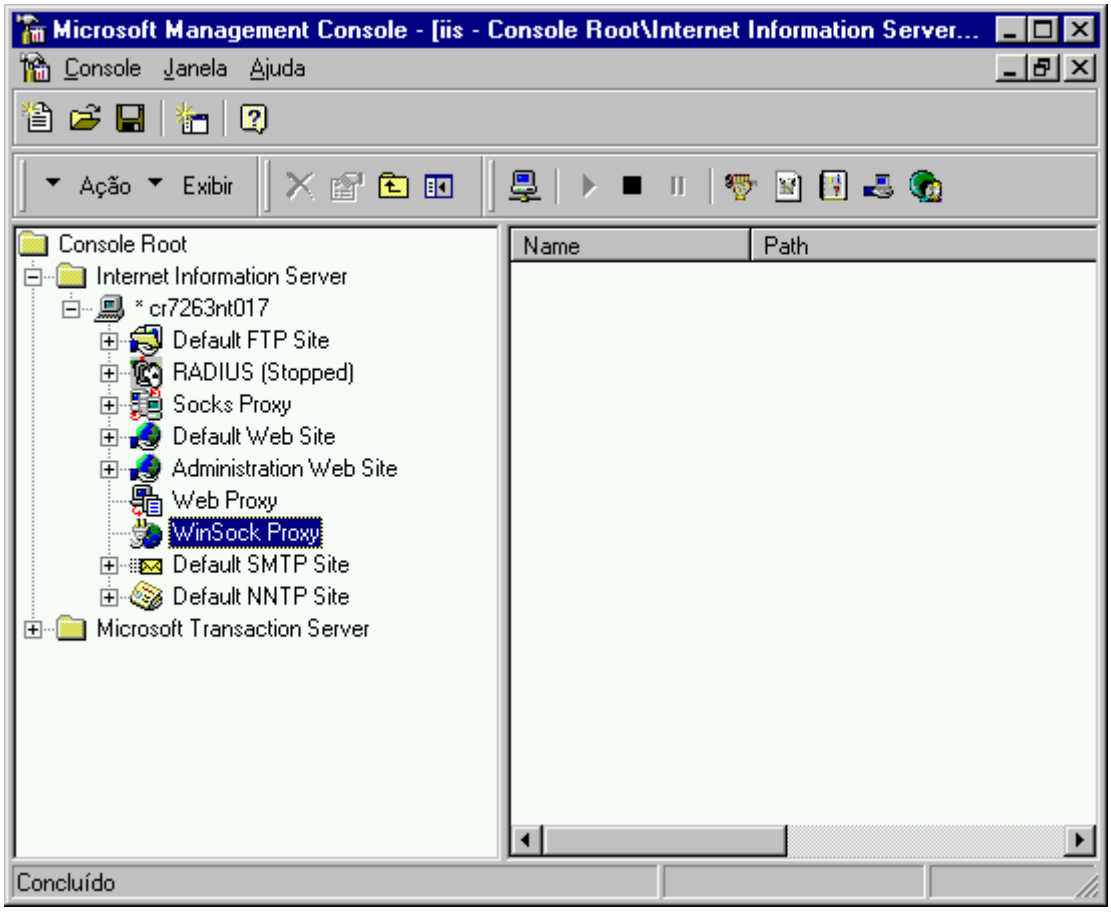
12. A seguinte janela então surgirá exibindo o grupo, ou usuário, autorizado. Pressione o botão *OK*.



13. A seguinte janela então surgirá exibindo o grupo, ou usuário, autorizado. Pressione o botão *OK*.



14. A janela da console de gerenciamento do Microsoft Proxy Server novamente surgirá. Feche-a, pois as configurações necessárias já estão realizadas.



As configurações não precisam ser exatamente iguais as descritas acima, a qual é um exemplo, pois, caso existam diretórios a mais, o Site Conectividade Social Empregador da CAIXA funciona sem problemas, mas caso falte algum diretório pode não funcionar.

A partir deste momento, o Microsoft Proxy Server está apto a funcionar para acesso ao Site Conectividade Social Empregador da CAIXA, bastando que cada cliente da rede interna, utilizando o ambiente Microsoft Windows, seja ele 3.x, 9x, NT, 2000, ou ME, instale o Microsoft Proxy Client, disponível num compartilhamento *default* de seu servidor *proxy*, por exemplo "\\SRVPROXY\mspclnt\SetUp.exe".

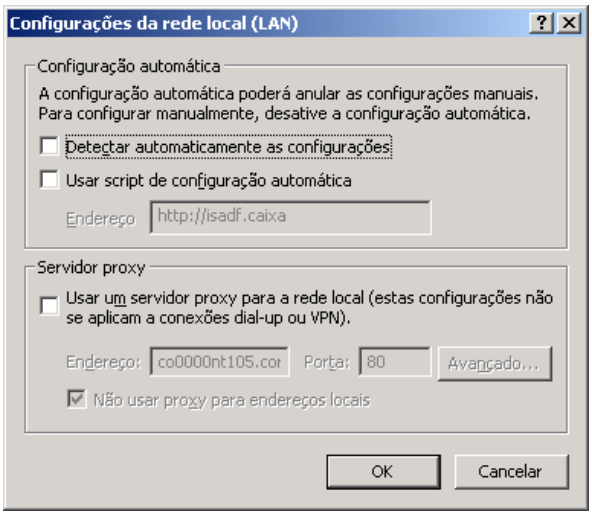
7 Configuração do Microsoft ISA Server.

7.1 Instalação do Firewall Client (Cliente ISA)

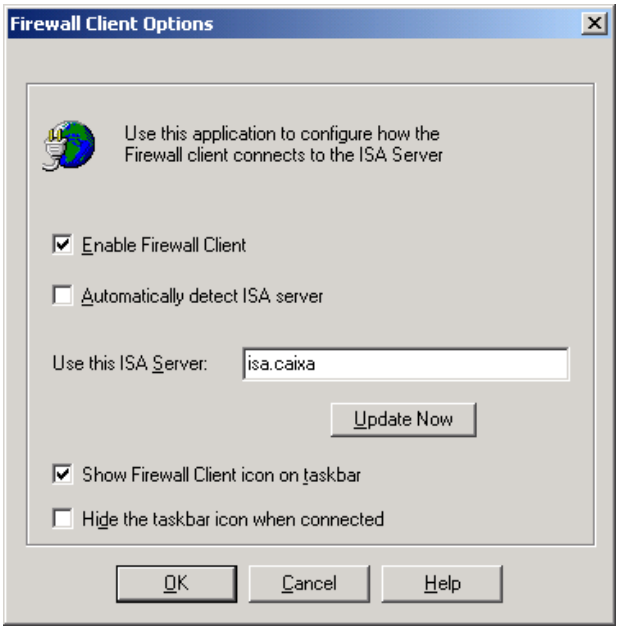
Se faz necessária apenas configuração no Internet Explorer, a saber:

- Abra o Internet Explorer.
- Clique em **Ferramentas**, clique em **Opções da Internet**. Clique na aba **Conexões** e **Configurações de LAN...**

- Na janela **Configurações da rede local (LAN)** desmarque todas as opções, segundo a figura a seguir. Esta configuração deverá ser utilizada 'apenas' para acesso ao Conectividade Social, estando 'fora do padrão' para quaisquer outros acessos.



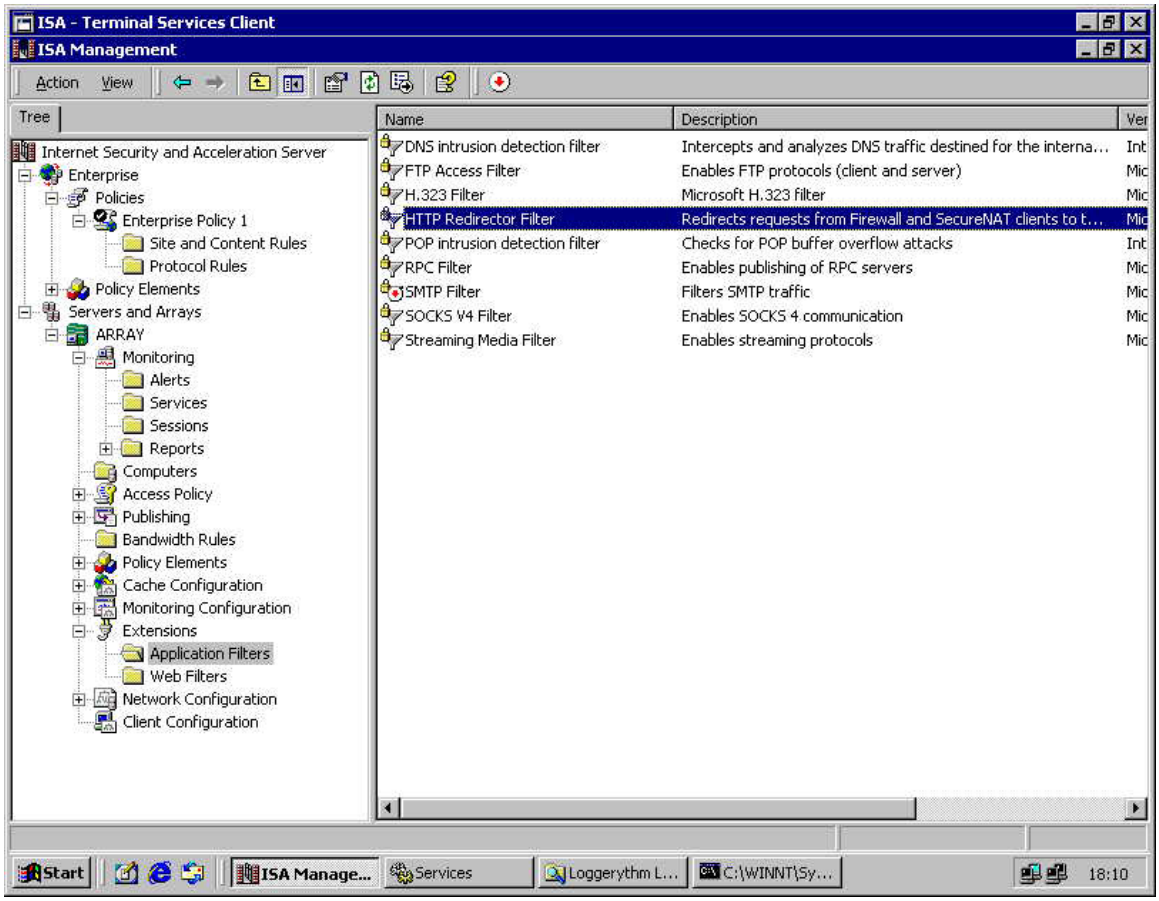
- Clique Ok, e Ok novamente. Feche todas as janelas do I.E e reabra-o.
- Quanto ao Firewall Client, não é necessário fazer nenhuma configuração adicional. Apenas para certificação, ele deverá estar configurado como a figura abaixo. **Não** deverá ser marcada a caixa 'Automatically detect ISA server'.



7.2. Instalação do ISA Server SP1 Enterprise Edition

Filtro Redirecionador

Para que o ISA Server não bloqueie os aplicativos, é preciso alterar as configurações padrão do ISA Server. Abra o gerenciador do ISA, abra Server and Arrays, selecione o Array, abra Extensions e em seguida clique em “Application Filters”.



O Filtro de Aplicação HTTP Redirector deve estar:
- **desabilitado**

Esse filtro redireciona os pedidos do serviço Firewall para o serviço Web Proxy, eliminando a autenticação, o que faz com que o aplicativo tente passar como anônimo.
Configurando conforma a figura acima, as credenciais do usuário são passadas para o serviço Firewall que então autentica o usuário a passar para o Site requisitado.

Regras de Site and Content

Para que os usuários não tenham acesso à sites proibidos, deve-se atentar para a forma como o ISA Server bloqueia os sites.

Para acesso via **Web Proxy Service**, o ISA bloqueia os endereços utilizando o nome que o usuário digita para acesso ao site. Ex: www.playboy.com

Entretanto, quando se utiliza o **Firewall Service** para acesso à Internet, o servidor ISA trata o endereço www.playboy.com de uma maneira diferente. Ele pega o IP do site e faz um **lookup** do mesmo, o que resulta no seguinte endereço: free-chi.playboy.com

Desta forma, para que o site **playboy** seja bloqueado, é necessário incluir uma regra de site e conteúdo que bloqueie o seguinte endereço: *.playboy.com

8 Configuração do sistema operacional GNU-Linux

Existem vários tipos de *proxies* e a nomenclatura pode variar, conforme o sistema operacional ou os pacotes utilizados. No caso do sistema operacional GNU-Linux, será abordado a funcionalidade IP Masquerading do *kernel*. Fazendo uma comparação com o produto Microsoft Proxy Server, seria similar ao serviço Socks Proxy. Um dos componentes do Módulo de Segurança utilizado para acessar o CNS da CAIXA é o Private Wire. Sua finalidade é criptografar a comunicação entre o computador do cliente e o servidor. Como a comunicação entre cliente e servidor é criptografada, os *proxies* do tipo *cache*, que se baseiam no conteúdo dessa comunicação para funcionar, não são capazes de fazer a intermediação entre cliente e servidor. Já os *proxies* do tipo *socks*, ou *transparent*, funcionam porque eles não manipulam o conteúdo da comunicação, mas apenas os endereços IP e números das portas, e esses dados não são criptografados pelo Private Wire.

O objetivo deste documento é prover, ao administrador de um sistema GNU-Linux já instalado, as informações necessárias para que ele possa implementar e configurar, inclusive na mesma máquina que já executa o *cache proxy*, a funcionalidade de *socks proxy*. Note-se que é possível implementar esta funcionalidade e manter, ou mesmo aumentar, o nível de segurança existente numa configuração onde se tem somente o *cache proxy* operando.
Estas instruções foram preparadas e baseadas num servidor GNU-Linux com o *kernel* 2.0.*.

8.1 SISTEMA GNU-LINUX CONFIGURADO PARA SER SIMILAR A UM *SOCKS PROXY*

Para obter a funcionalidade similar a de um *socks proxy* no sistema GNU-Linux, é necessário um *kernel* compilado com a opção "CONFIG_IP_MASQUERADE" habilitada. Esta opção faz com que o *kernel* possa operar como se fosse um NAT — Network Address Translator —, embora um NAT normalmente opere com vários IPs do lado de fora, ao passo que o sistema GNU-Linux aqui configurado vai operar apenas com uma faixa de IP — a do CNS— Se você nunca compilou um kernel, procure ajuda especializada.
Agora que o seu novo kernel está rodando, execute o seguinte comando para habilitar o NAT para o CNS:

ipfwadm -F -i accept -m -P tcp -S 10.0.0.0/8 1024:65535 -D 200.201.174.0/24) 80

A regra acima é para o caso da rede local ser 10.0.0.0 com máscara de rede 255.0.0.0, e ela só será aplicada no caso de conexões originadas a partir de algum cliente na rede local e destinadas ao intervalo de endereços IP de, 200.201.174.0 até 200.201.174.255), com protocolo tcp e porta 80. Isto é suficiente para acessar os servidores do CNS da CAIXA.

8.2 A COMBINAÇÃO DE UM CACHE PROXY E DE UM SOCKS PROXY

O Apache Web Server com *cacheproxy, ou o Squid,* pode estar rodando na mesma máquina que implementa o NAT e, eventualmente, o *firewall*. No entanto, é necessário analisar o conjunto de regras definido com o "ipfwadm" no sentido de evitar que outras regras mais restritivas sejam tratadas antes da regra descrita acima, que habilita a funcionalidade NAT para os servidores da CAIXA.