Aker Web Content Analyzer

Manual de Configuração

- Apêndice B - Copyrights e Disclaimers

Introdução

Este é o manual do usuário do Analisador de URLs Aker. Nos próximos capítulos você aprenderá como configurar esta poderosa ferramenta de controle de acesso. Esta introdução tem como objetivo descrever a organização deste manual e tentar tornar sua leitura o mais simples e agradável possível.

O que é o Analisador de URLs Aker ?

O Analisador de URLs Aker é uma poderosa ferramenta de controle de acesso a sites da Internet, quando trabalhando em conjunto com um firewall ou um servidor proxy compatível.

O produto consiste de uma imensa base de dados com URLs da Internet classificadas em uma ou mais categorias e com atualização automática e diária pela Aker Security Solutions. Dessa forma, é possível para um administrador configurar que categorias de sites determinados usuários podem acessar, sem se preocupar com o cadastro manual dos mesmos. Isso permite um aumento de produtividade por parte dos funcionários da empresa, que não mais perderão tempo acessando informações nada relevantes para seu trabalho, ao mesmo tempo que permite uma redução do tráfego no link com a Internet, diminuindo a necessidade de upgrades do mesmo e poupando dinheiro.

Como está disposto este manual.

Este manual está organizado em vários capítulos. Cada capítulo mostrará um aspecto da configuração do produto e todas as informações relevantes ao aspecto tratado.

Recomendamos que este manual seja lido pelo menos uma vez por inteiro, na ordem apresentada. Posteriormente, se for necessário, pode-se usá-lo como fonte de referência (para facilitar seu uso como referência, os capítulos estão divididos em tópicos, com acesso imediato pelo índice principal. Desta forma, pode-se achar facilmente a informação desejada).

Em vários locais deste manual, aparecerá o símbolo  seguido de uma frase escrita em letras vermelhas. Isto significa que a frase em questão é uma observação muito importante e deve ser totalmente entendida antes de se prosseguir com a leitura do capítulo.

Copyrights do Sistema

- Este produto utiliza o algoritmo MD5 retirado da RFC 1321. Copyright (c) 1991-2 RSA Data Security, Inc.

1-0 Instalando o Analisador de URLs Aker

Mostraremos aqui como instalar e remover o Analisador de URLs Aker.

1-1 Requisitos de Hardware e Software

O Analisador de URLs Aker executa sobre os sistemas operacionais Windows (NT 4.0, 2000 Server e 2003 Server), Linux (Red Hat 7.3, 8 e 9 e Conectiva 8 e 9) e FreeBSD (4.7 e 4.9) em plataformas Intel 32 ou compatíveis. Ele é compatível com o Firewall Aker em sua versão 4.0 ou superiores, MS Proxy Server e MS ISA Server, Checkpoint Firewall 1 e Squid Internet Object Cache. Com exceção do Firewall Aker, os demais produtos necessitam de um plugin para comunicarem-se com o Analisador de URLs.

Quanto ao hardware, para que o Analisador de URLs Aker execute de maneira satisfatória, é necessária a seguinte lista:

- Computador Pentium 233Mhz ou superior

Caso exista um grande número de clientes acessando o analisador de URLs, pode ser necessário uma máquina com maior capacidade de processamento.

- 64 Mbytes de memória RAM

O uso de 128Mbytes é altamente recomendado para todas as instalações.

- 50 Mbytes de espaço livre em disco
- Monitor
- Placa(s) de rede

É importante frisar que todos os dispositivos de hardware devem ser suportados pelo sitema operacional escolhido.

1-2 Instalando o Analisador de URLs

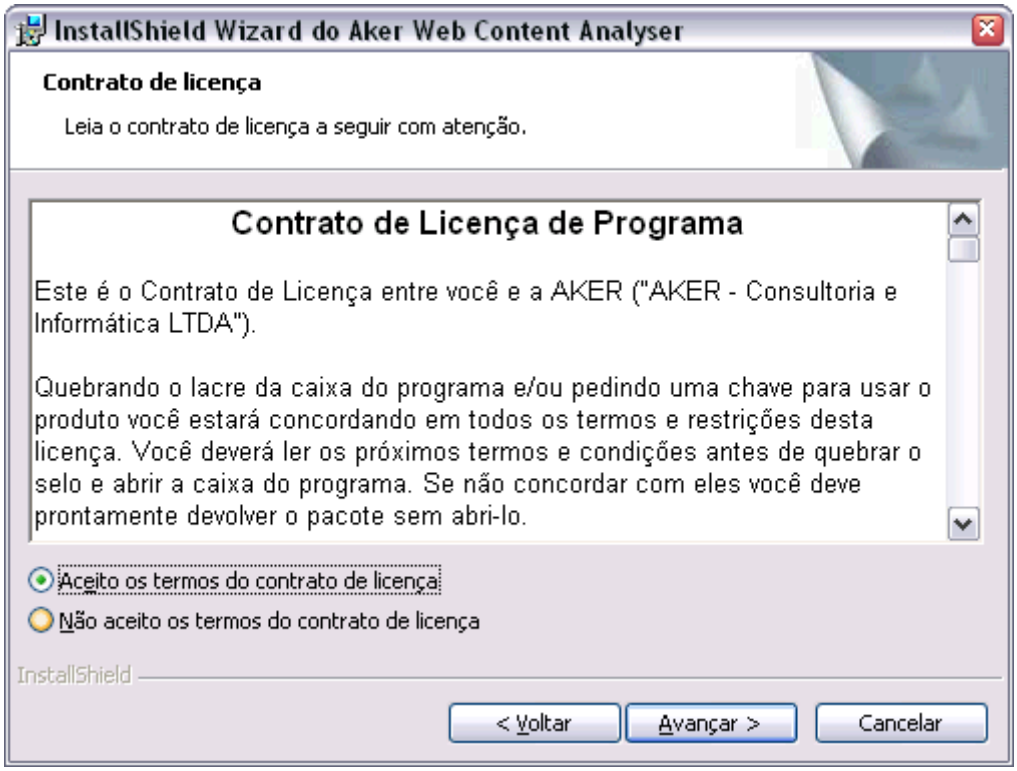
1-2-1 Instalando em servidores Windows

A instalação do Analisador de URLs Aker é bastante simples, sendo necessário executar os seguintes passos:

1. Clicar no menu **Iniciar**
2. Selecionar a opção **Executar**
3. Ao ser perguntado sobre qual programa executar, digitar a localização do arquivo de instalação `webcontentanalyzer_win_br_`*`versao`*`.exe`.

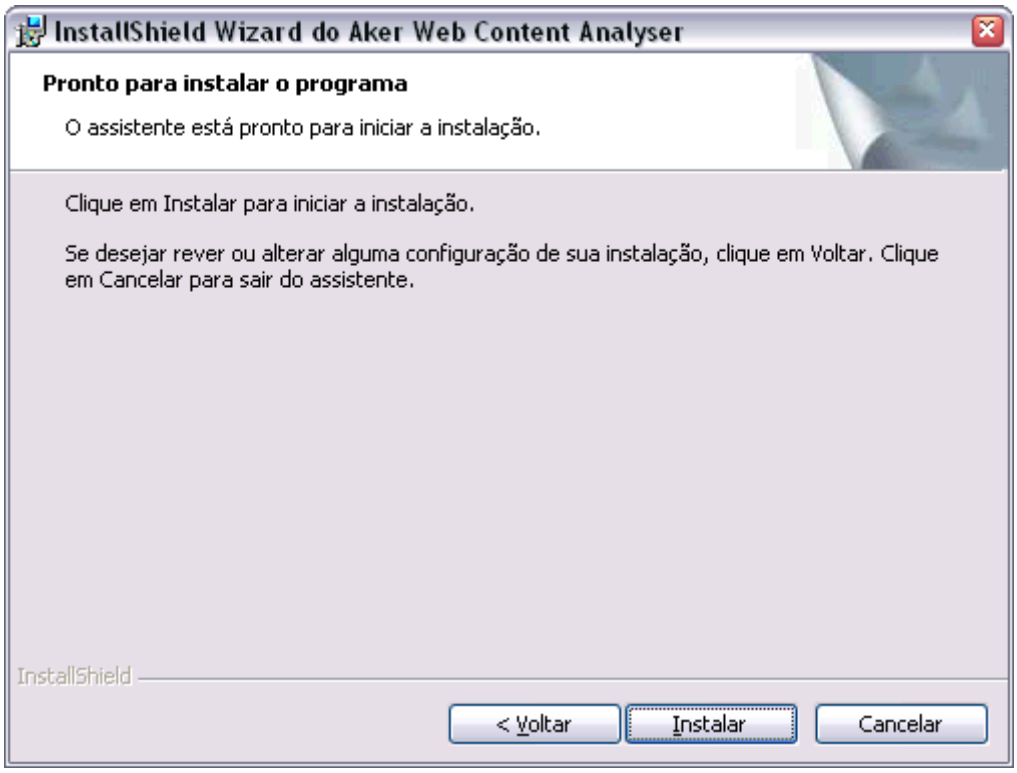
A janela abaixo irá aparecer, devendo-se clicar no botão de próximo:

Em seguida será mostrada a tela com o contrato de licença. Para proceder com a instalação selecione a opção **Aceito os termos do contrato de licença**. Caso você escolha a opção contrária, a instalação será cancelada.



Escolha o local onde deseja copiar os arquivos do analisador.

Pressione **Instalar** para finalizar a instalação:



1-2-2 Removendo de servidores Windows

A desinstalação do Analisador de URLs Aker é um processo simples, bastando se escolher a opção *Adicionar ou Remover Programas do painel de controle e escolher o produto pelo seu nome.*

1-2-3 Instalando em servidores Linux

O Analisador de URLs Aker para Linux vem em um pacote padrão RPM. Por isso, sua instalação deve ser feita ou com uma interface gráfica gerenciadora de pacotes da preferência do usuário, ou com o utilitário de linha de comando:

```
rpm -ivh <nome_do_pacote>.rpm
```

Pode ser necessária a instalação de pacotes adicionais, como o do QT. Eles podem ser obtidos no site da Aker (*www.aker.com.br*) ou no CD de instalação do produto.

1-2-4 Removendo de servidores Linux

O Analisador de URLs Aker para Linux vem em um pacote padrão RPM. Por isso, sua remoção deve ser feita ou com uma interface gráfica gerenciadora de pacotes da preferência do usuário, ou com o utilitário de linha de comando:

```
rpm -e <nome_do_pacote>
```

1-2-5 Instalando em servidores FreeBSD

O Analisador de URLs Aker para FreeBSD vem em um pacote padrão desse sistema operacional (*package*). Por isso, sua instalação deve ser feita ou com uma interface gráfica gerenciadora de pacotes da preferência do usuário, ou com o utilitário de linha de comando:

```
pkg_add <nome_do_pacote>.tgz
```

Pode ser necessária a instalação de pacotes adicionais, como o do QT. Eles podem ser obtidos no site da Aker (*www.aker.com.br*) ou no CD de instalação do produto.

1-2-6 Removendo de servidores FreeBSD

O Analisador de URLs Aker para FreeBSD vem em um pacote padrão desse sistema operacional (*package*). Por isso, sua remoção deve ser feita ou com uma interface gráfica gerenciadora de pacotes da preferência do usuário, ou com o utilitário de linha de comando:

```
pkg_delete <nome_do_pacote>
```

2-0 Configurando o Analisador de URLs Aker

Mostraremos aqui como configurar o Analisador de URLs Aker.

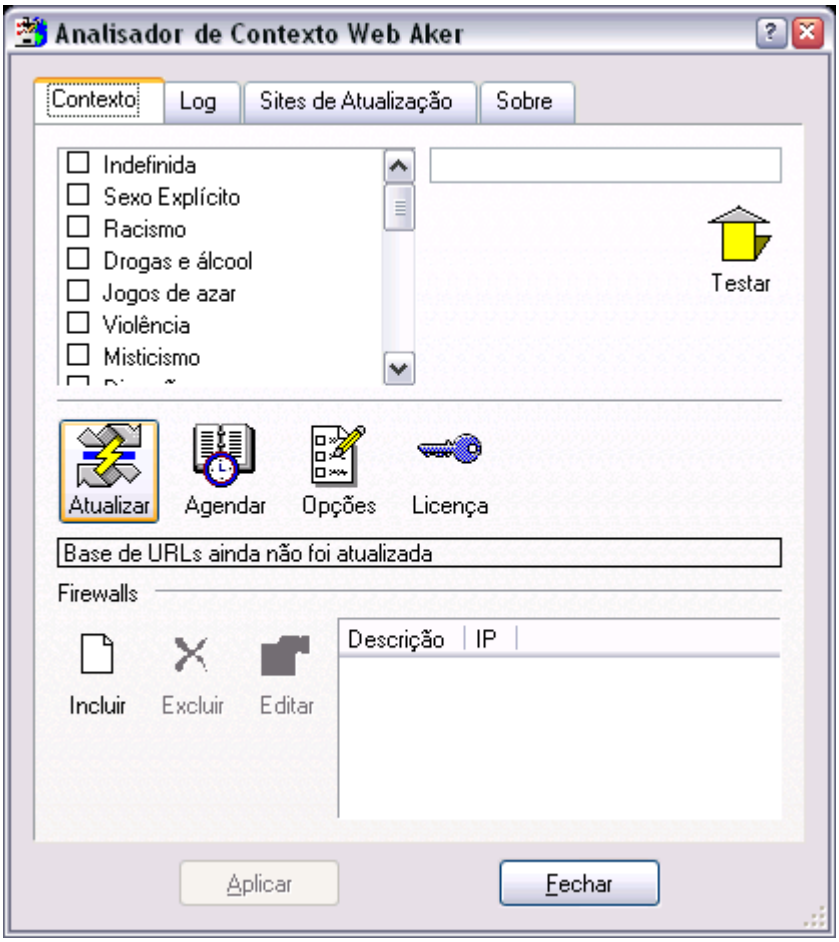
2-1 Configurações básicas

O Analisador de URLs Aker roda como um serviço do sistema operacional. Para configurá-lo é necessário iniciar a interface gráfica do produto.

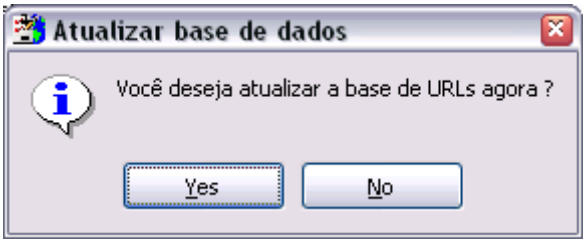
Para iniciar a interface gráfica deve-se executar os seguintes passos:

- **No Windows:** Clicar no menu **Iniciar**, selecionar o grupo **Firewall Aker**, dentro deste grupo o sub-grupo **Analisador de Contexto Web** e dentro deste último clicar na opção de mesmo nome.
- No Linux ou no FreeBSD, em um ambiente X Windows, digitar: `/usr/local/akerurl/akerurl_conf &`

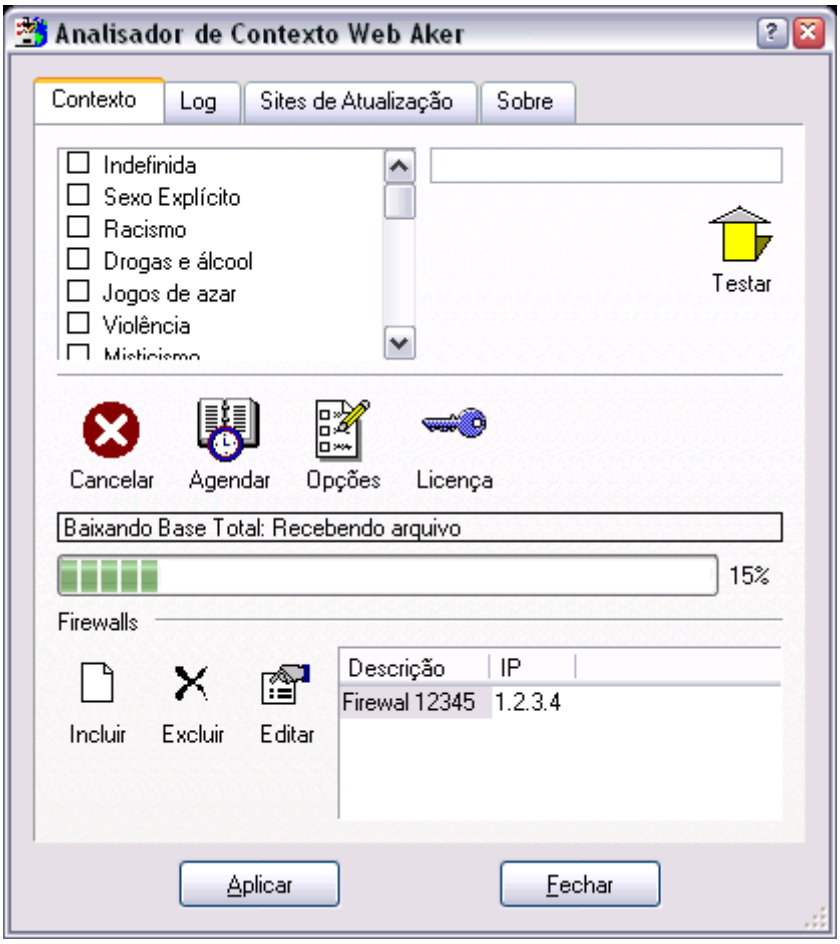
Será mostrada a seguinte janela:



A primeira ação a ser realizada pelo administrador deverá ser a atualização da base de URLs. Isso é necessário pois a base de dados que acompanha o produto com certeza estará desatualizada e muitas URLs novas não estarão listadas. Para se proceder com a atualização, deve-se clicar no botão **Atualizar**, localizado na barra de ferramentas. Será mostrada a seguinte caixa de diálogo:



Clique no botão **Sim** para continuar e repare que a opção ***Atualizar*** mudou para ***Cancelar***, permitindo que o usuário interrompa o processo de atualização a qualquer momento. O andamento da atualização é mostrado em uma barra de progresso, como visualizado na figura abaixo:



A primeira atualização da base poderá ser um pouco demorada, dependendo da velocidade de conexão com a Internet. As atualizações futuras serão bastante mais rápidas, já que serão transferidas apenas as diferenças da base.

O próximo passo para funcionamento do analisador será o cadastramento dos firewalls que irão acessá-lo. Para tal deve-se clicar no ícone ***Incluir*** da barra de tarefas do grupo ***Firewalls***

A seguinte janela será mostrada:

IP: É o endereço IP do firewall que irá acessar o analisador de URLs.

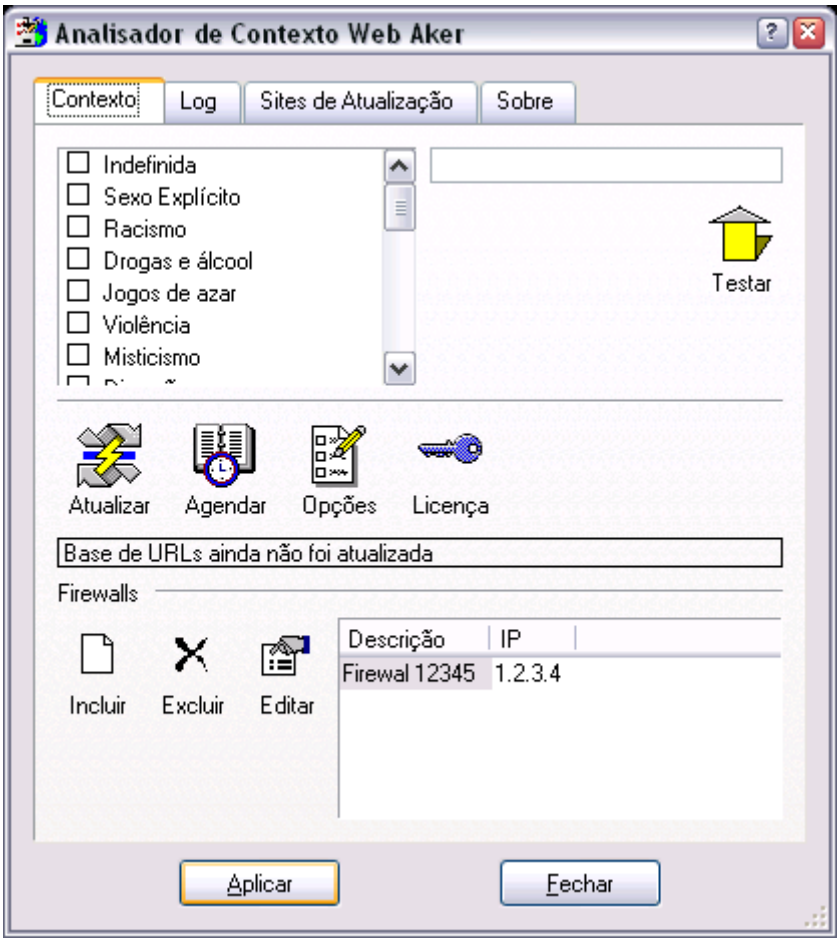
Descrição: É um campo livre, utilizado apenas para fins de documentação.

Senha: É a senha utilizada para gerar as chaves de autenticação e criptografia usadas na comunicação com o firewall. Esta senha deve ser igual à configurada no firewall.

Confirmação: Este campo é utilizado apenas para se verificar se a senha foi digitada corretamente. Deve-se digitá-la exatamente como no campo *Senha*.

Repare que a qualquer momento é possível se ***Editar*** ou ***Excluir*** os firewalls cadastrados, clicando-se no botão correspondente da barra de ferramentas.

Após serem feitas as alterações desejadas, é necessário se clicar no botão ***Aplicar***, para que as mesmas possam ter efeito.

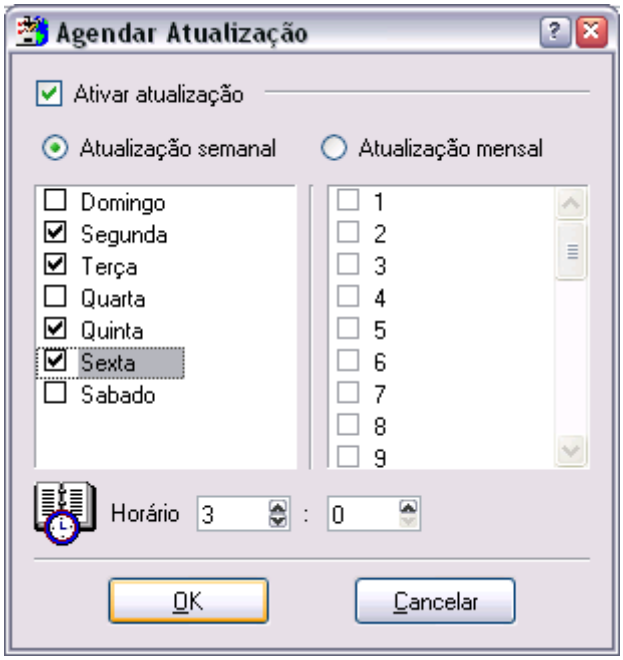


2-2 Configurações adicionais

Nessa seção serão mostradas as opções avançadas de configuração do Analisador de URLs Aker. São elas:

- **Agendar**

Clicando-se na opção ***Agendar***, localizada na barra de ferramentas, pode-se definir os dias e a hora em que as atualizações automáticas serão realizadas. Ao se clicar nessa opção, a seguinte janela será mostrada:

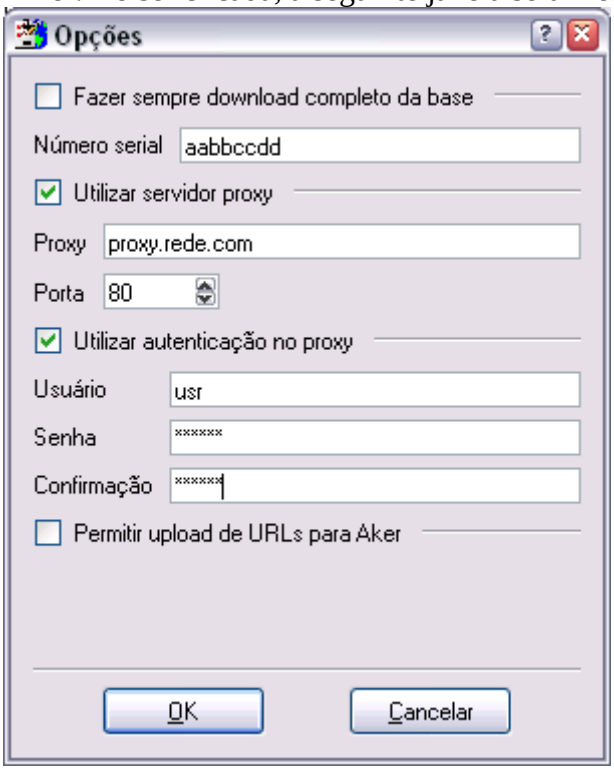


A opção **Ativar Atualização**, se estiver marcada, fará com que o analisador de URLs automaticamente baixe as atualizações da base de dados. Caso ela esteja desmarcada, as atualizações somente serão executadas manualmente.

As opções **Atualização semanal** e **Atualização mensal** permitem com que se defina os dias da semana ou do mês que as atualizações serão realizadas.

- **Opções**

Esta opção permite que se defina parâmetros adicionais ao funcionamento do Analisador de URLs Aker. Ao ser clicada, a seguinte janela será mostrada:



A opção **Fazer sempre download completo da base**, se estiver marcada, fará com que o analisador de URLs baixe sempre a base completa e não apenas as diferenças.

Essa opção deve ser utilizada apenas em caso de problemas, já que baixar a base completa provocará um aumento desnecessário de tráfego e tempo de download.

O campo **Número serial** permite que se veja e modifique o número serial do produto.

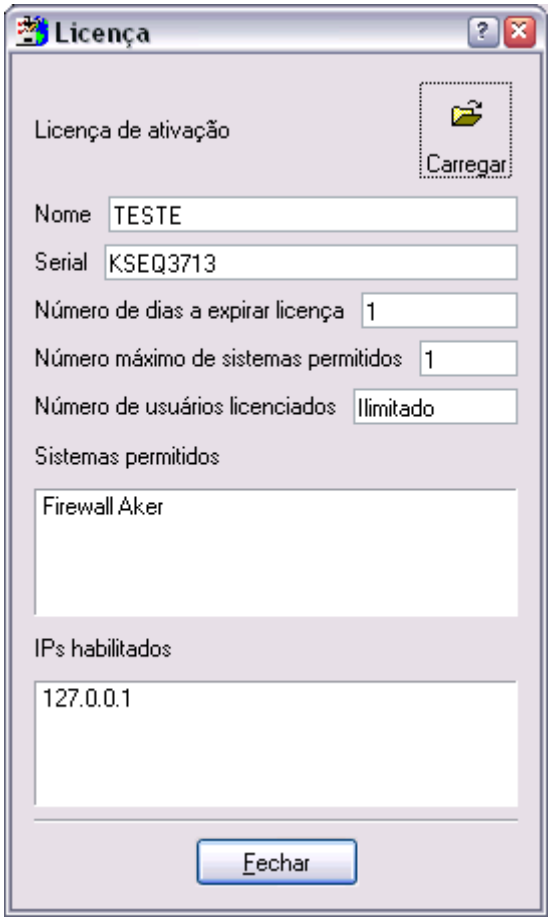
O número serial somente deve ser alterado se solicitado pelo suporte técnico da Aker Security Solutions, sob pena do produto não mais funcionar.

Proxy Web: Caso seja necessário utilizar um proxy web para fazer download da base de dados e suas atualizações, é possível se especificar o nome e senha de acesso que o Analisador de URLs Aker informará para o proxy.

A opção **Permitir uload de URLs para a Aker** ativa a transmissão para a Aker Security Solutions das URLs que não obtiveram classificação. Se ativada, as URLs sem categoria utlizadas por seus usuários serão enviadas de forma cifrada para nossa equipe de classificação após que se removam os componentes privados como valores de variáveis CGI. Suas URLs serão tratadas de forma anônima pela equipe da Aker, de modo a garantir sua privacidade. O objectivo dessa operação é classificar primeiro as URLs efetivamente utilizadas por nossos usuários.

- **Licença**

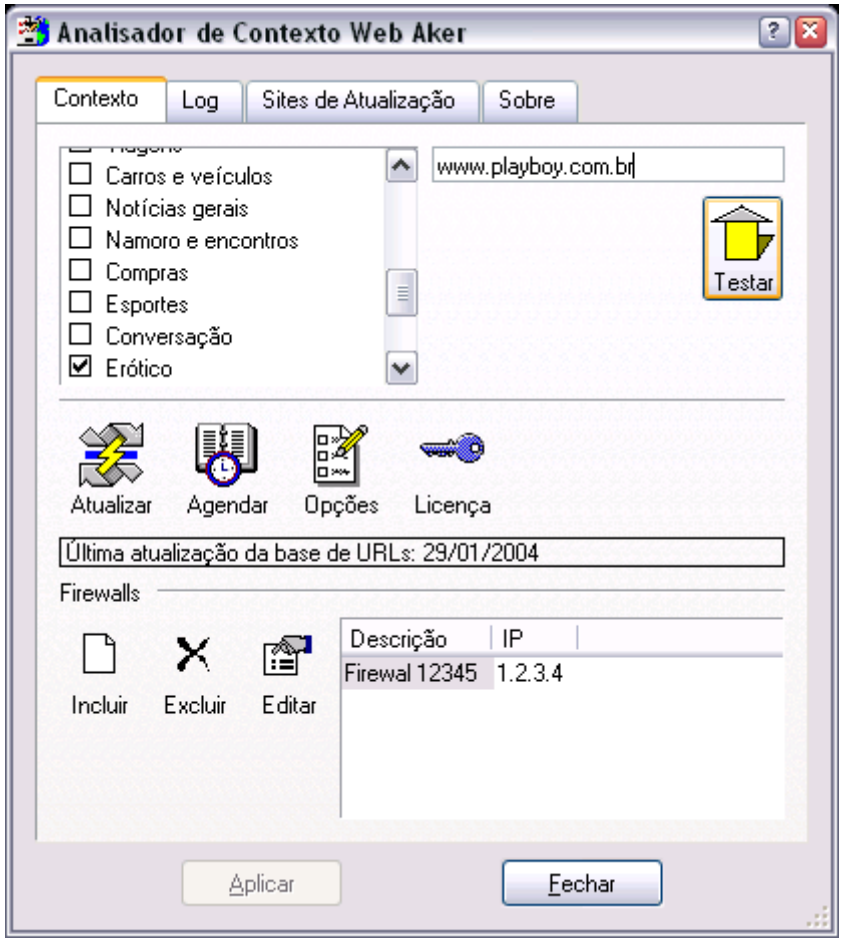
Essa opção permite que se veja os dados da licença atual e se carregue uma nova. Ao ser clicado, a seguinte janela será mostrada:



Para se carregar uma nova licença, deve-se clicar no botão **Carregar**, localizado na parte superior da janela. Será mostrada então uma nova janela onde se pode especificar o nome do arquivo com a licença.

- **Teste de URLs**

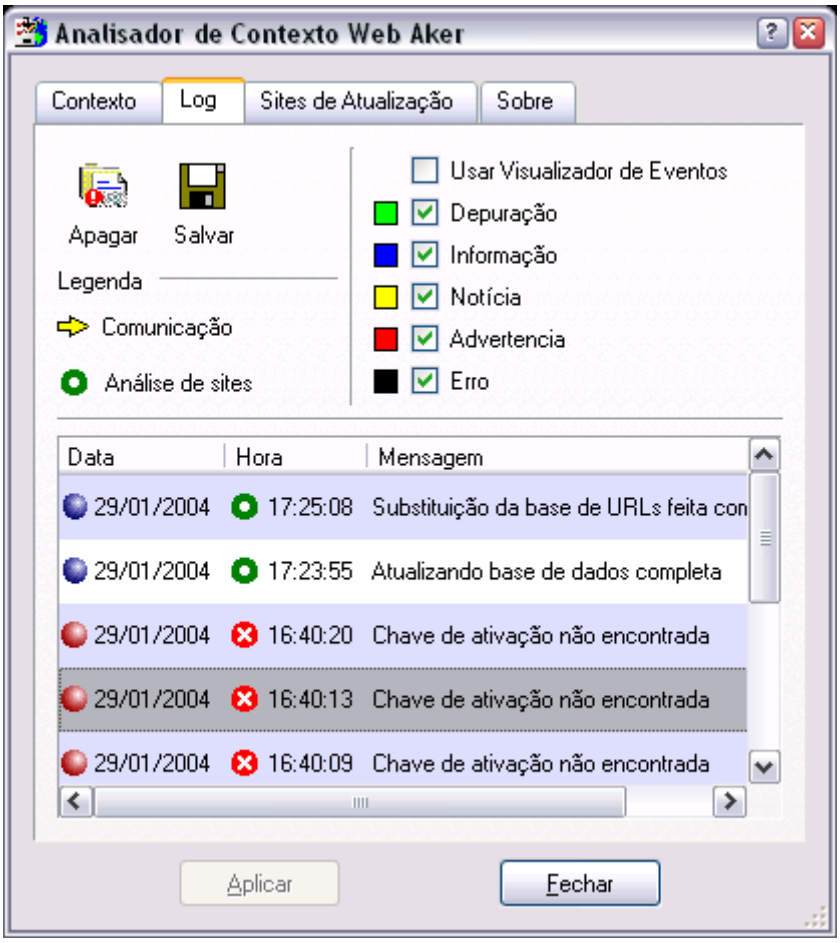
A qualquer momento o administrador poderá checar a classificação de uma URL, bastando para isso entrar o endereço desejado no campo de teste, localizado na parte superior direita da janela, e clicar o botão ***Testar***. Caso o site tenha classificação, a mesma aparecerá no campo ao lado. Caso não possua, todos os campos de categorias serão mostrados em branco.



2-3 Outras opções

Em adição à pasta principal, onde são configurados todos os aspectos do funcionamento do Analisador de URLs Aker, existem mais três outras pastas onde é possível se obter mais informações sobre o produto e seu funcionamento. São elas:

Log



Nesta pasta é possível se verificar todo o funcionamento do Analisador de URLs Aker. Ela consiste de uma lista com várias mensagens, cada uma mostrada em linhas de cores alternadas, de forma a facilitar sua identificação. À direita de cada mensagem é mostrado um quadrado colorido com sua importância.

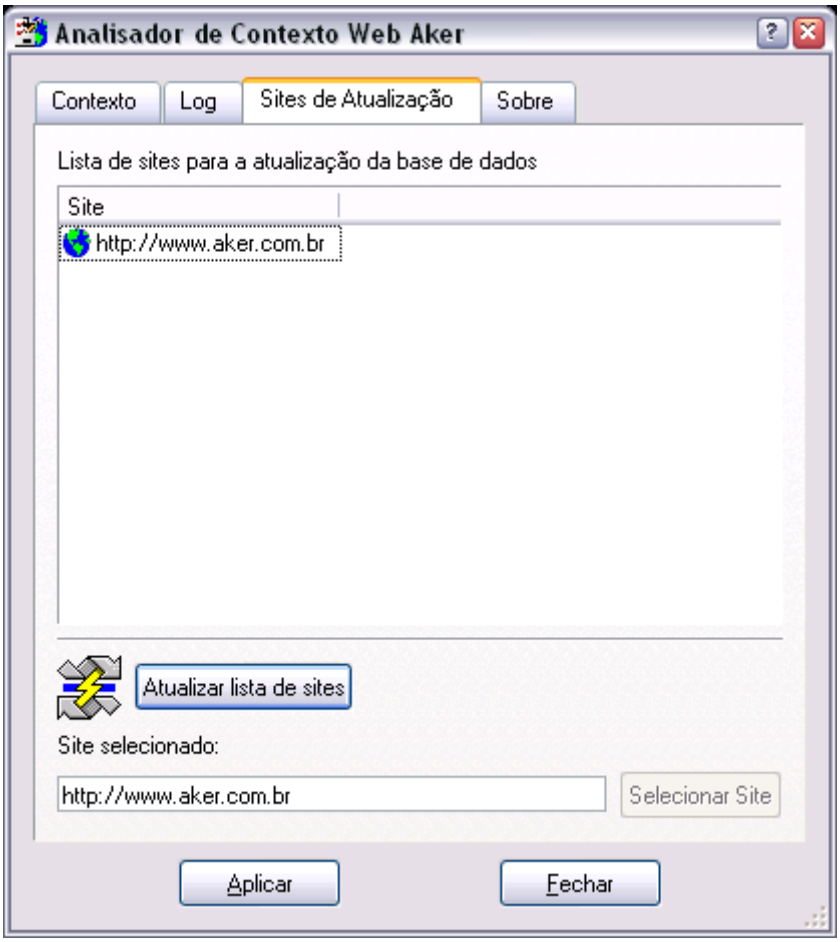
O botão **Apagar**, localizado na barra de ferramentas permite com que se apague todas as entradas existentes no log.

O botão **Salvar**, localizado na barra de ferramentas permite com que se salve o log em um arquivo formato texto. Ao ser clicado, será mostrada uma janela para que se especifique o nome do arquivo que será salvo.

A opção **Usar visualizador de eventos**, se estiver marcada fará com que todas as mensagens de log sejam enviadas para o Visualizador de eventos do Windows

A descrição de todas as mensagens do log do Analidador de URLs Aker se encontra no Apêndice A.

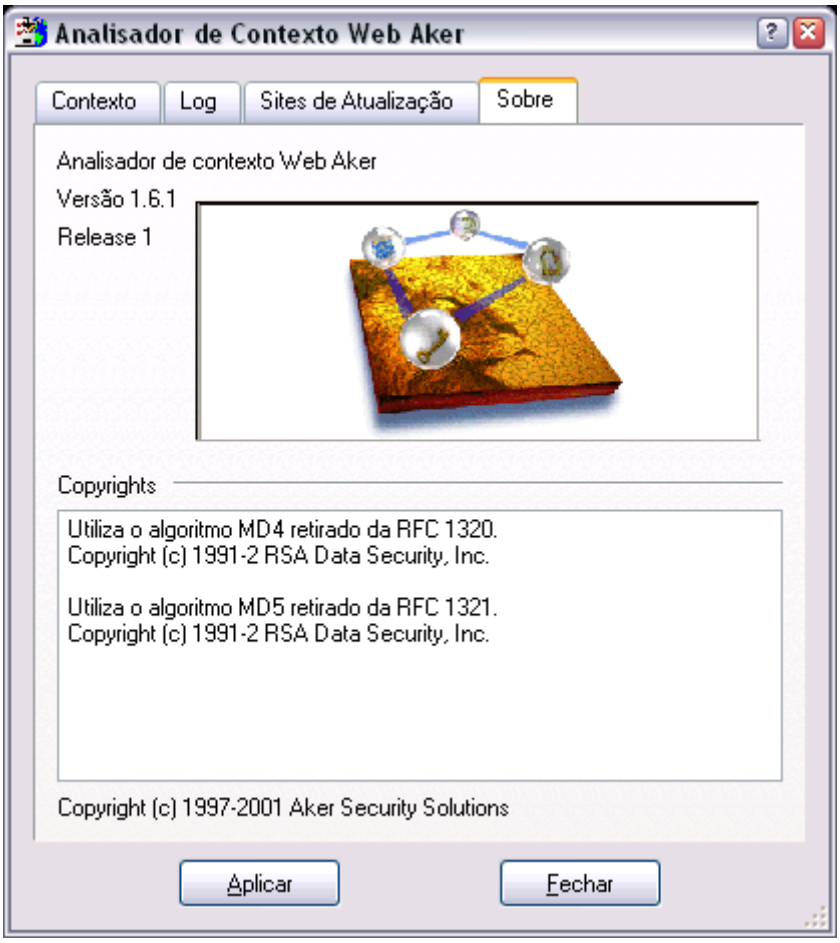
Sites de Atualização



Visando minimizar o tráfego nos servidores da Aker Security Solutions, a base de endereços poderá ser distribuída para outros parceiros da Aker. A medida que estes sites forem sendo ativados a ***Lista de sites para atualização da base de dados*** será disponibilizada automaticamente para o usuário que, desta forma, poderá escolher a que tiver menor tempo de latência, bastando para isso selecionar o site desejado e clicar no botão ***Selecionar Site.***

A qualquer momento poderá ser feita uma atualização forçada da lista, pressionando o botão **Atualizar lista de sites**.

Sobre



Esta é uma pasta meramente informativa e serve para que se obtenha algumas informações do Analisador de URLs. Dentre as informações úteis se encontram sua versão e release.

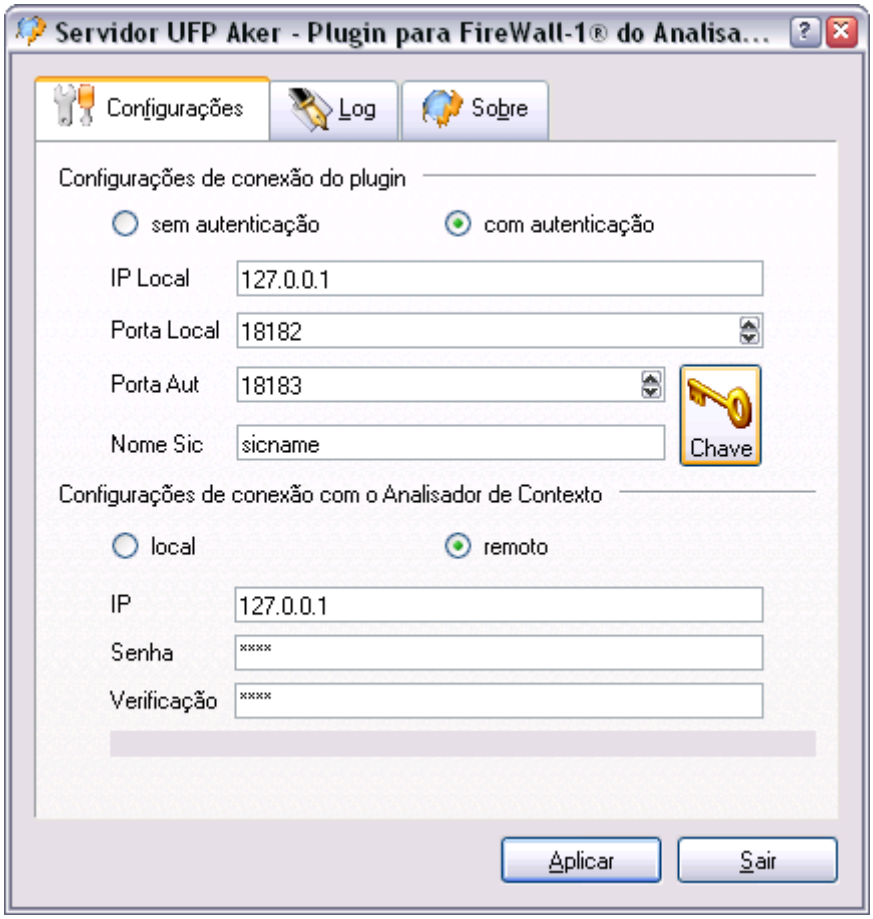
3-0 Utilizando o plugin para Firewall - 1

Mostraremos aqui como configurar o Plugin para Firewall 1

3-1 Introdução

O Plugin para Firewall - 1 é um programa que faz a função de intermediário entre o Checkpoint Firewall - 1 e o Analisador de URLs Aker. Para tanto, ele precisa saber como se conectar tanto em um quanto em outro

3-2 Configurações



A tela acima permite configurar tanto como se conectar ao Firewall-1 quanto como se conectar ao Analisador de URLs.

- Conectando-se ao Firewall-1:

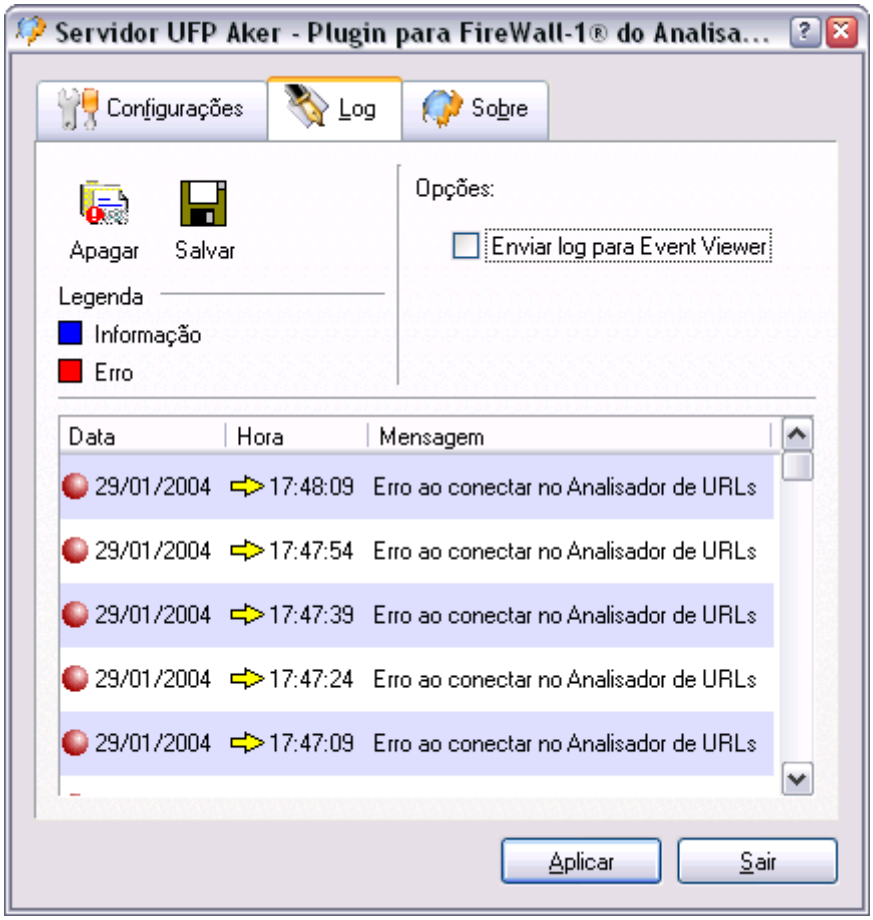
  O tráfego de dados entre o analisador e o firewall-1 pode ser desprotegido (**sem autenticação**) ou protegido por autenticação digital e criptografia (**com autenticação**)
  Devem ser configurados o endereço **IP local**, a **Porta Local** onde o serviço deve

esperar conexões do Firewall-1/
Caso se esteja usando autenticação, deverão ser configuradas as opções de autenticação como o segredo compartilhado entre o Firewall - 1 e o Analisador de URLs clicando-se no botão **Chave**. Além disso, a **Porta Aut** (usada para conexões de criptografia) e o **Nome Sic** devem ser configurados com os mesmos valores tanto no Firewall - 1 quanto no plugin.

- Conectando-se ao Aker Web Content Analyzer

Existem duas opções de conexão: **local** (apenas para sistemas Linux), onde o plugin estabelece uma conexão com o Analisador de Contexto usando um método rápido chamado *local socket* e **remoto** (via TCP/IP). Essa segunda opção funciona sempre e depende de um segredo compartilhado a ser configurado tanto no Analisadro quanto no plugin. A comunicação é sempre cifrada e autenticada.

3-3 Log



Nessa janela, o sistema mostra os eventos relevantes ocorridos, dando as opções de **Salvar** (em um arquivo texto) e de usar o sistema de log padrão do sistema operacional (**Event Viewer**, no Windows ou **Syslog** no Linux)

4-0 Utilizando o plugin para Squid

Mostraremos aqui como configurar o Aker Web Control para Squid

4-1 Introdução

O Aker Web Control para Squid é um produto que possibilita ao Squid aceitar ou rejeitar acessos de acordo com o nível de acesso de cada usuário e a categoria da página desejada.
O Squid irá iniciar diversas instâncias do mesmo, de acordo com seu arquivo de configurações, e repassará cada URL a ele requisitada

4-2 Configurações do Squid

Quatro diretivas da configuração do Squid são especialmente importantes para o Plugin do analisador de URls:

- `cache_effective_user` - Define qual o usuário efetivo do sistema será usado pelos processos Squid. Esse usuário deve ser desprivilegiado e deve ser o mesmo a ser configurado no campo correspondente do plugin
- `cache_effective_group` - Define qual o grupo efetivo do sistema será usado pelos processos Squid. Esse grupo deve ser desprivilegiado e deve ser o mesmo a ser configurado no campo correspondente do plugin
- `redirect_program` - Define o programa a ser usado pelo Squid para filtrar as URLs. Deve ser o proprio plugin:

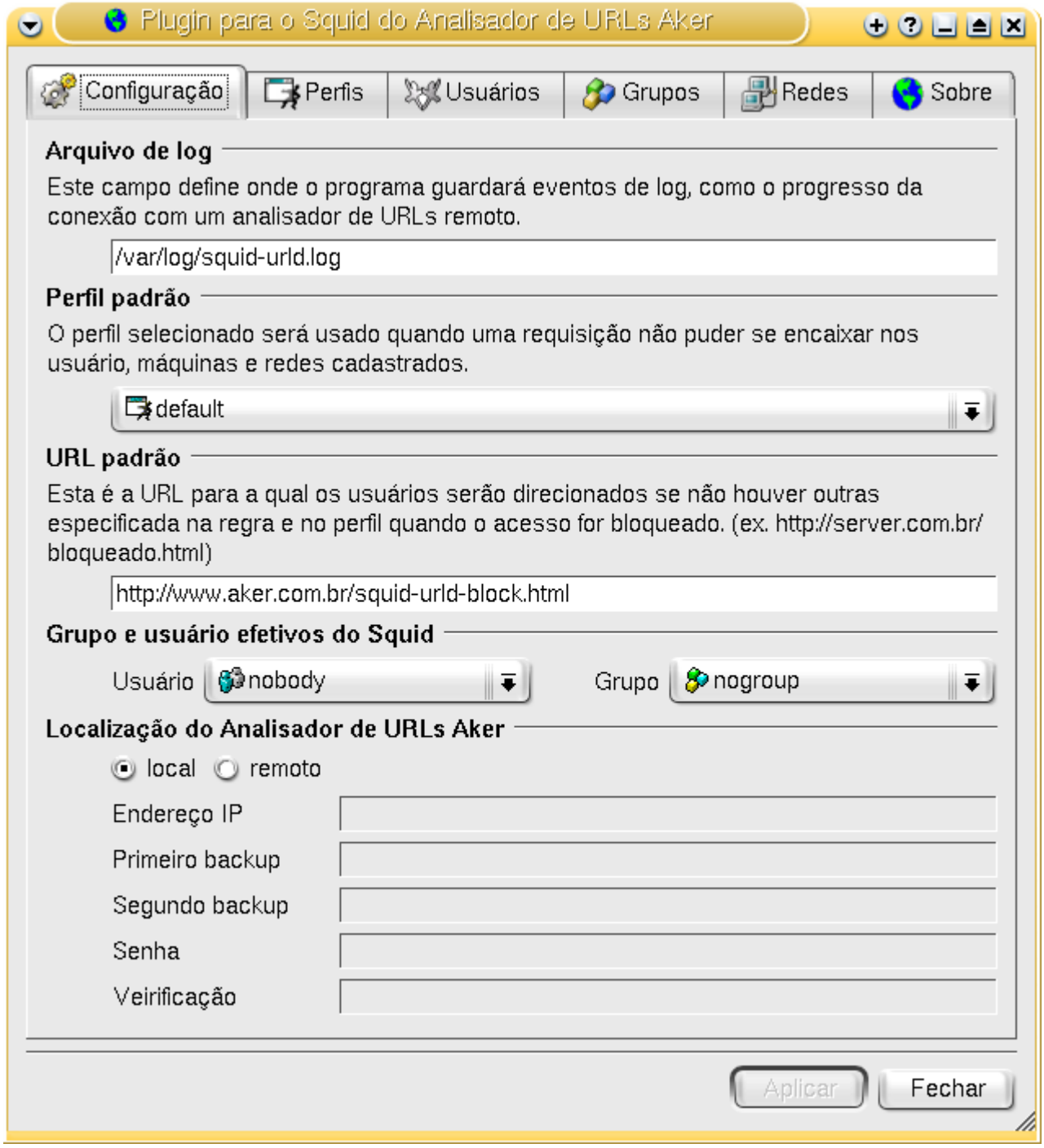
  ```
  /usr/local/squid-urld/squid-urld
  ```

- `redirect_children` - Define quantas cópias do plugin serão instanciadas pelo Squid. O número de processos é a quantidade de requisições pendentes que pode haver em um determinado instante. Recomenda-se utilizar um número nunca inferior a 5 e sempre aumentá-lo gradualmente, para evitar a sobrecarga do sistema operacional.
- `auth_param basic program` - Define o programa a ser usado pelo Squid para autenticar os usuários. Deve ser o seguinte programa:

  ```
  /usr/local/squid-urld/squid_auth /etc/passwd
  ```

- `auth_param basic children` - Define quantas cópias do programa acima serão instanciadas pelo Squid. O número de processos é a quantidade de requisições pendentes que pode haver em um determinado instante. Recomenda-se utilizar um número nunca inferior a 5 e sempre aumentá-lo gradualmente, para evitar a sobrecarga do sistema operacional.

4-3 Configurações do plugin



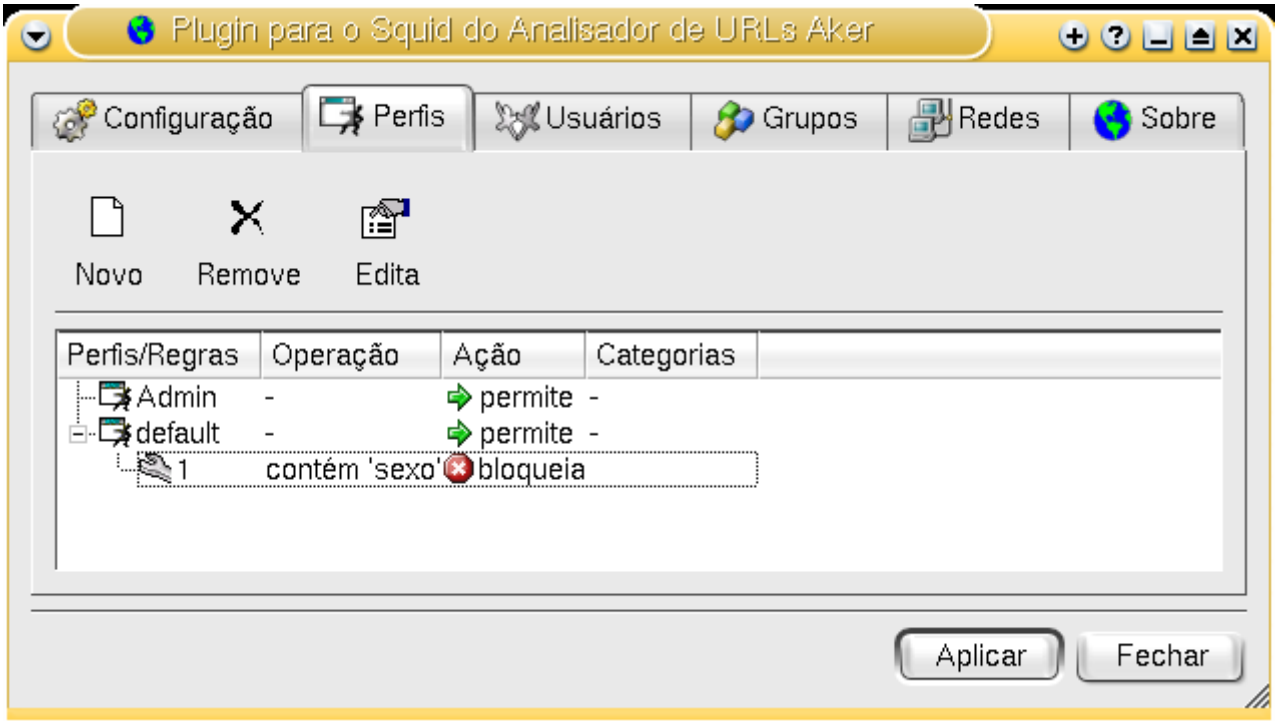
- **Arquivo de log**: Nesse campo, você deve definir um local onde o plugin possa guardar seus registros de fatos relevantes ocorridos, tais como possíveis erros de conexão com o analisador de URLs. Lembre-se que o usuário/grupo efetivo do Squid deve ser capaz de criar um arquivo nesse local, ou então o arquivo deve ser pré-criado e com direitos de gravação para esse par.
- **Perfil padrão**: Se uma requisição não se encaixar em nenhum perfil específico (veja seções de *Usuários*, *Grupos* e *Redes*), então ela utilizará o perfil aqui definido

- **URL padrão**: O plugin para Squid, ao perceber que uma URL deve ser bloqueada, redireciona o usuário para uma página informativa a ser definida. A URL de redireção aponta para essa página e ainda pode passar informações específicas para a mesma, através da substituição de seqüências especiais de caracteres:

Seqüência especial	Substituída por
%%	Caractere '%'
%u	URL que foi bloqueada
%s	Usuário que tentou um acesso indevido
%i	Endereço IP que originou a requisição bloqueada
%m	Método HTTP utilizado (GET, PUT, ...)
%d	Servidor web (FQDN) para o qual se destinava o acesso bloqueado

- **Grupo e usuário efetivos do Squid**: Devem conter os mesmos valores dos campos `cache_effective_user` e `cache_effective_group` no arquivo de configuração do Squid.
- **Localização do Analisador de URLs Aker**: Diz como o plugin deve comunicar-se com o Analisador de URLs Aker:
    - Via socket **local**: Essa opção apenas funcionará se o plugin for executado no mesmo computador que o Analisador
    - Via socket **remoto** (via TCP/IP): Essa opção fará o plugin abrir uma conexão TCP cifrada e autenticada para o Analisador, que pode estar hospedado em um computador remoto

4-4 Definição de regras e perfis de acesso



Um perfil de acesso é composto de um conjunto de regras ordenadas e de uma ação padrão. Os perfis possuem uma organização hierárquica, ou seja, um perfil criado em um nível inferior possuirá as regras do perfil de nível superior ao qual está subordinado. É importante ressaltar que as regras poderão ser modificadas somente no perfil onde foram criadas.

As regras contém duas partes:

1. Parte de busca: que define uma operação de um pequeno texto. A operação define como o texto será procurado dentro da URL.
2. Parte de ação: Existem quatro ações:
    - **Permite**: Permite o acesso que se enquadrar nessa regra
    - **Bloqueia**: Não permite o acesso que se enquadrar nessa regra, redirecionando ou para a URL especificada, ou para a padão
    - **Bloqueia as categorias**: Não permite o acesso às páginas que se enquadrarem nas categorias especificadas
    - **Permite as categorias**: Permite o acesso apenas às páginas que se enquadrarem nas categorias especificadas, rejeitando-o às demais.

Dentro do perfil, ainda existe uma URL de redireção padrão para suas regras que não a especificarem. Desse modo, a URL de redireção efetiva será:

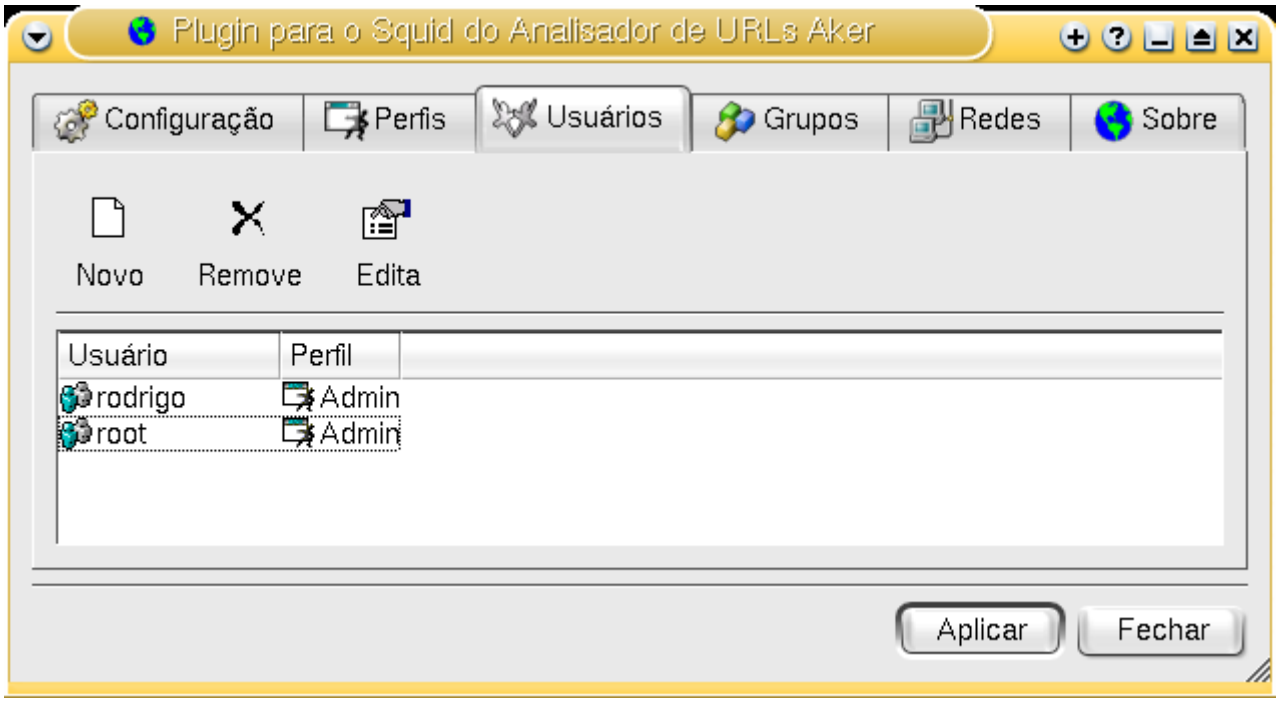
1. A da regra, se houver
2. A do perfil, estando a da regra em branco
3. A padrão, estando ambas as da regra e do perfil em branco

4-5 Escolha do perfil

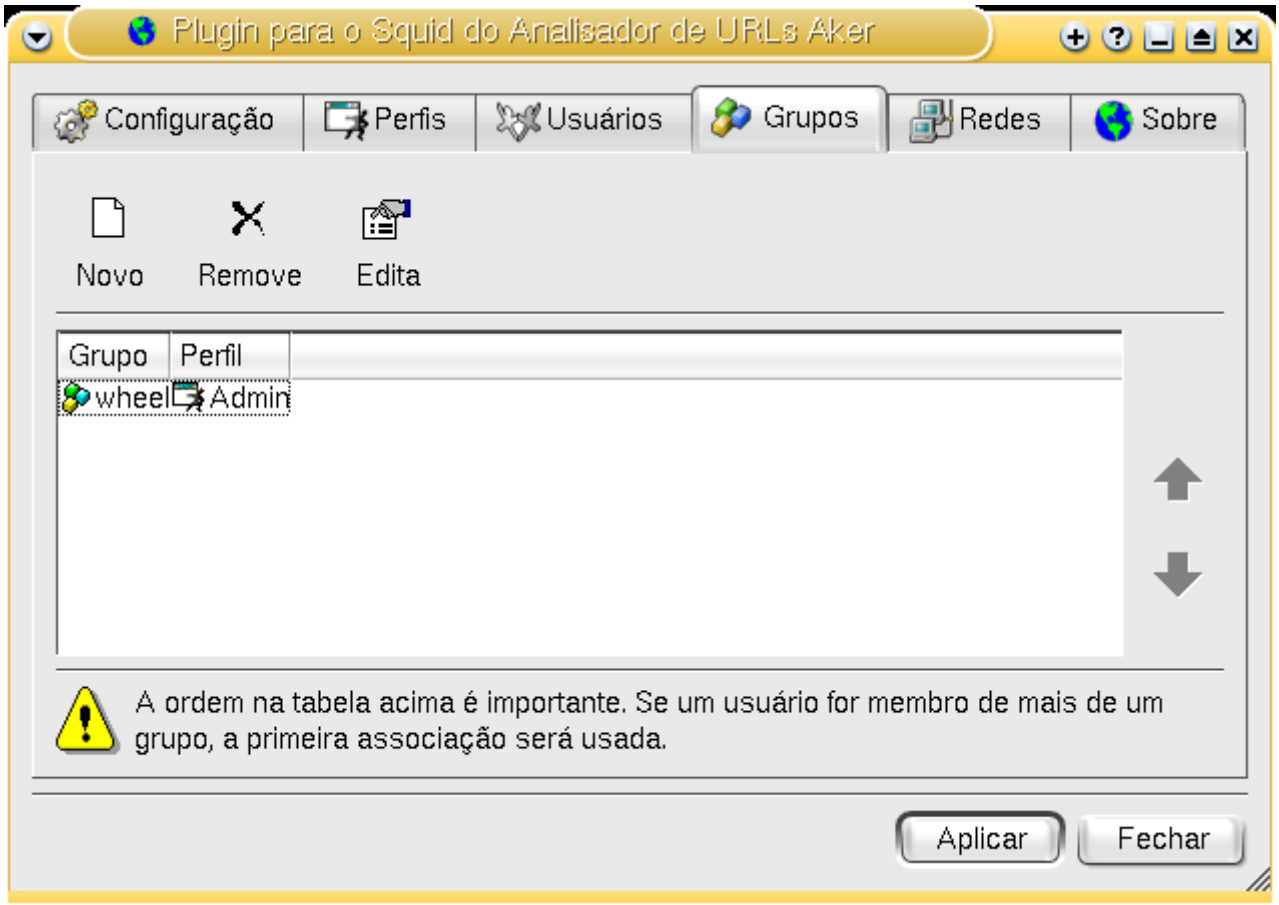
Definidos os perfis de acesso, é preciso configurar o plugin para que ele possa associar cada um dos usuário aos mesmos. Para tanto, existem três características do mesmo que podem ser pesquisadas, na seguinte ordem:

1. **Nome do usuário**
2. **Grupo do sistema operacional a que pertence o usuário**
3. **Endereço IP do computador que o usuário está utilizando**

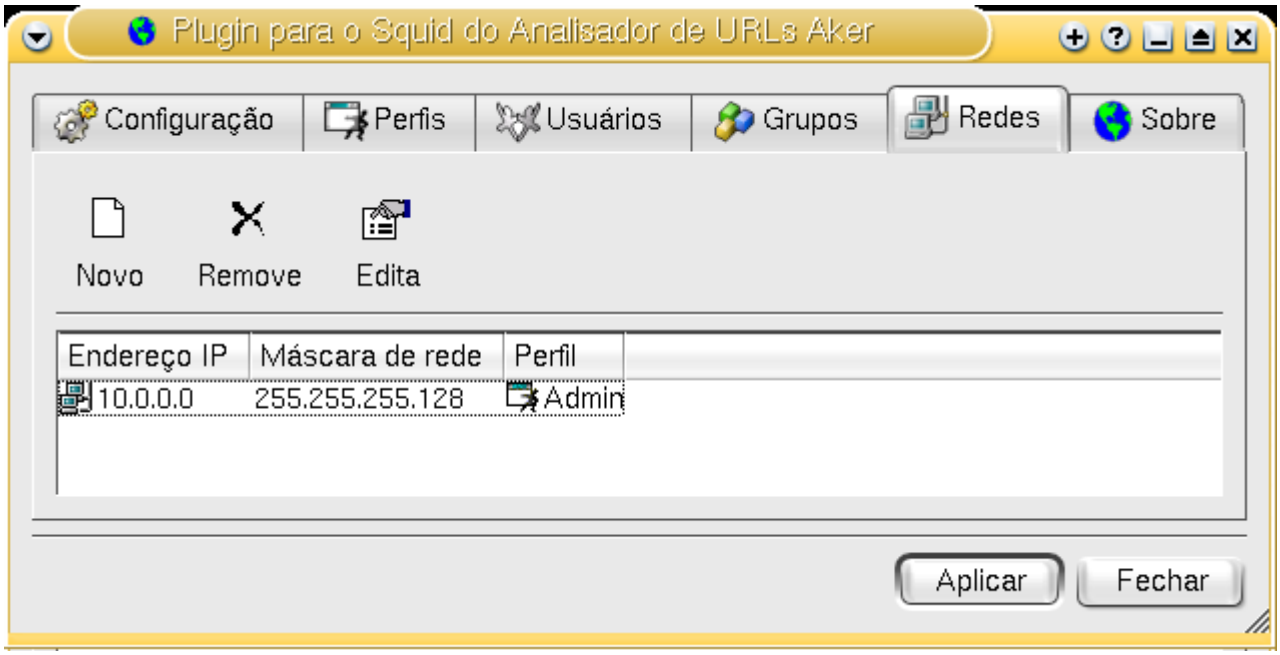
As telas a seguir permitem especificar esses três tipos de regra:



Quando você for editar ou incluir um usuário nessa lista, atentar ao fato que podem ser escolhidos usuários do sistema ou digitados os nomes dos mesmos dentro do mesmo *combo-box*. O nome do usuário que o Squid vai informar ao plugin depende do programa externo de autenticação utilizado no Squid.



Do mesmo modo que na lista de associações para usuários, você pode digitar nomes de grupos arbitrários. Diferentemente dos usuários, os grupos não são informados pelo Squid ao plugin, de forma que esse vai procurar sempre dentro da lista de grupos do sistema operacional onde ele está sendo executado.



Não conseguindo escolher um perfil por uma associação de usuário ou de grupo, o plugin vai examinar o endereço IP do cliente para obter um perfil de acesso.

5-0 Utilizando o plugin para ISA Server

Mostraremos aqui como configurar o Aker Web Control para ISA Server

5-1 Introdução

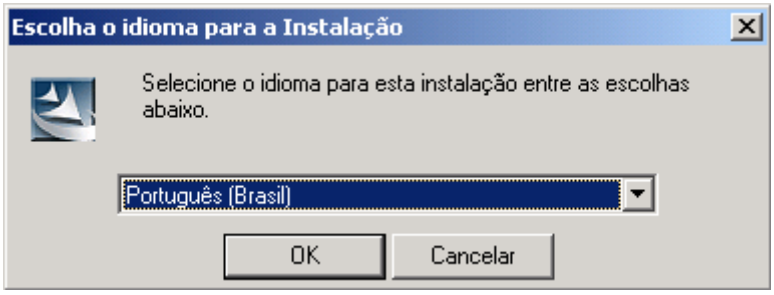
O Aker Web Control para ISA Server é um produto que possibilita ao ISA Server aceitar ou rejeitar acessos de acordo com o nível de acesso de cada usuário e a categoria da página desejada.

5-2 Instalando o plugin

A instalação do Aker Web Control para ISA Server é bastante simples, sendo necessário executar os seguintes passos:

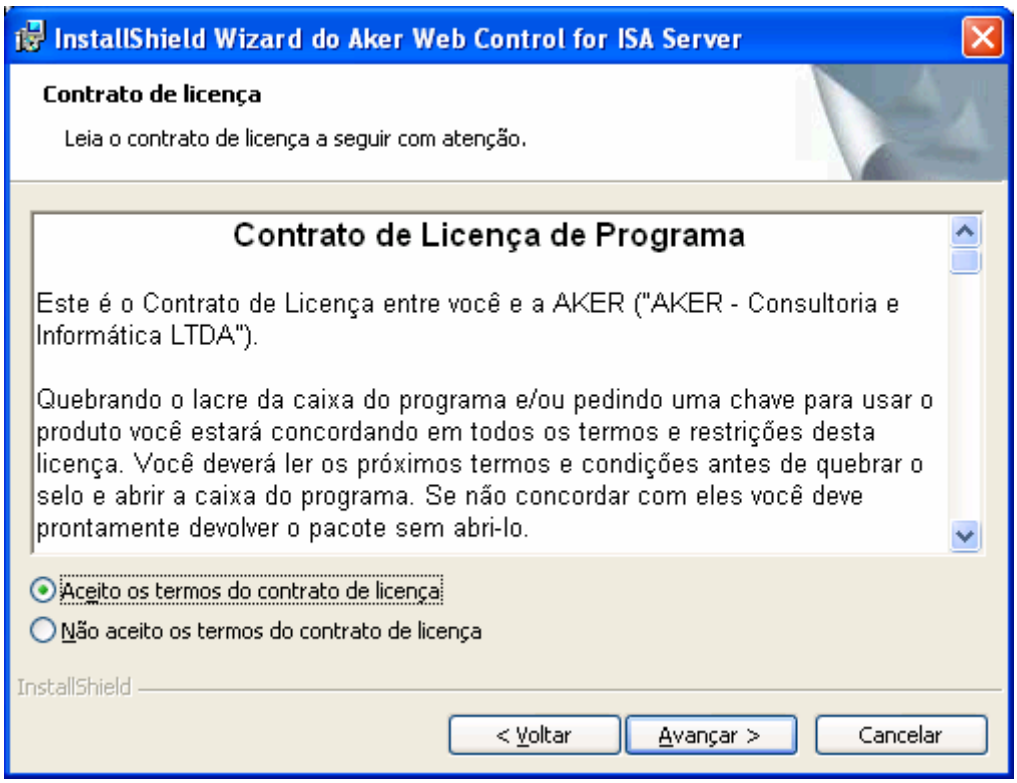
1. Clicar no menu **Iniciar**
2. Selecionar a opção **Executar**
3. Ao ser perguntado sobre qual programa executar, digitar a localização do arquivo de instalação `aker_web_control_isa.exe`.

A janela abaixo irá aparecer, devendo-se escolher o idioma desejado e clicar no botão OK:

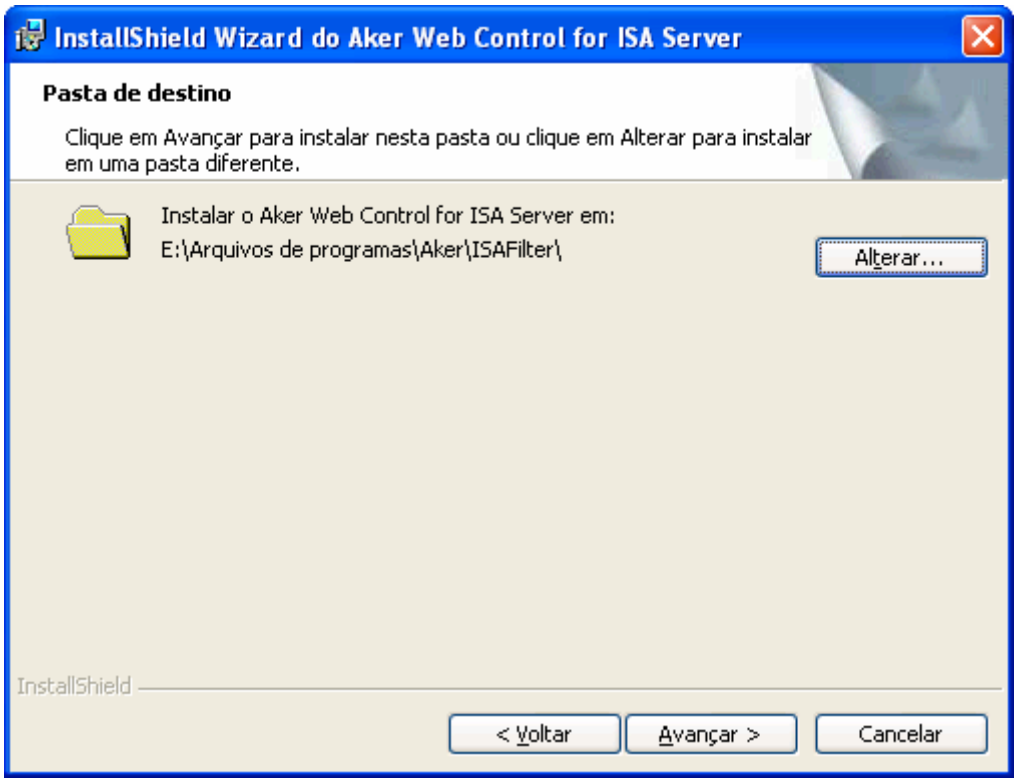


Será exibida a janela seguinte, devendo-se pressionar o botão de **Avançar**:

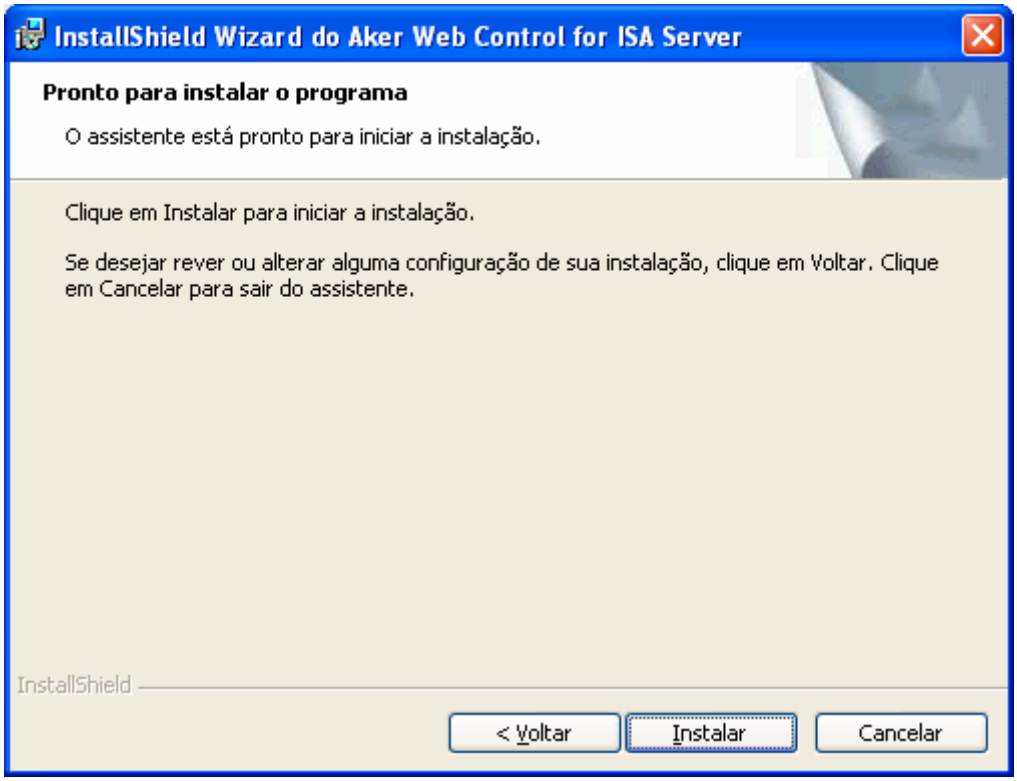
Em seguida será mostrada a tela com o contrato de licença. Para proceder com a instalação selecione a opção **Aceito os termos do contrato de licença**. Caso você escolha a opção contrária, a instalação será cancelada.



Escolha o local onde deseja copiar os arquivos do plugin.



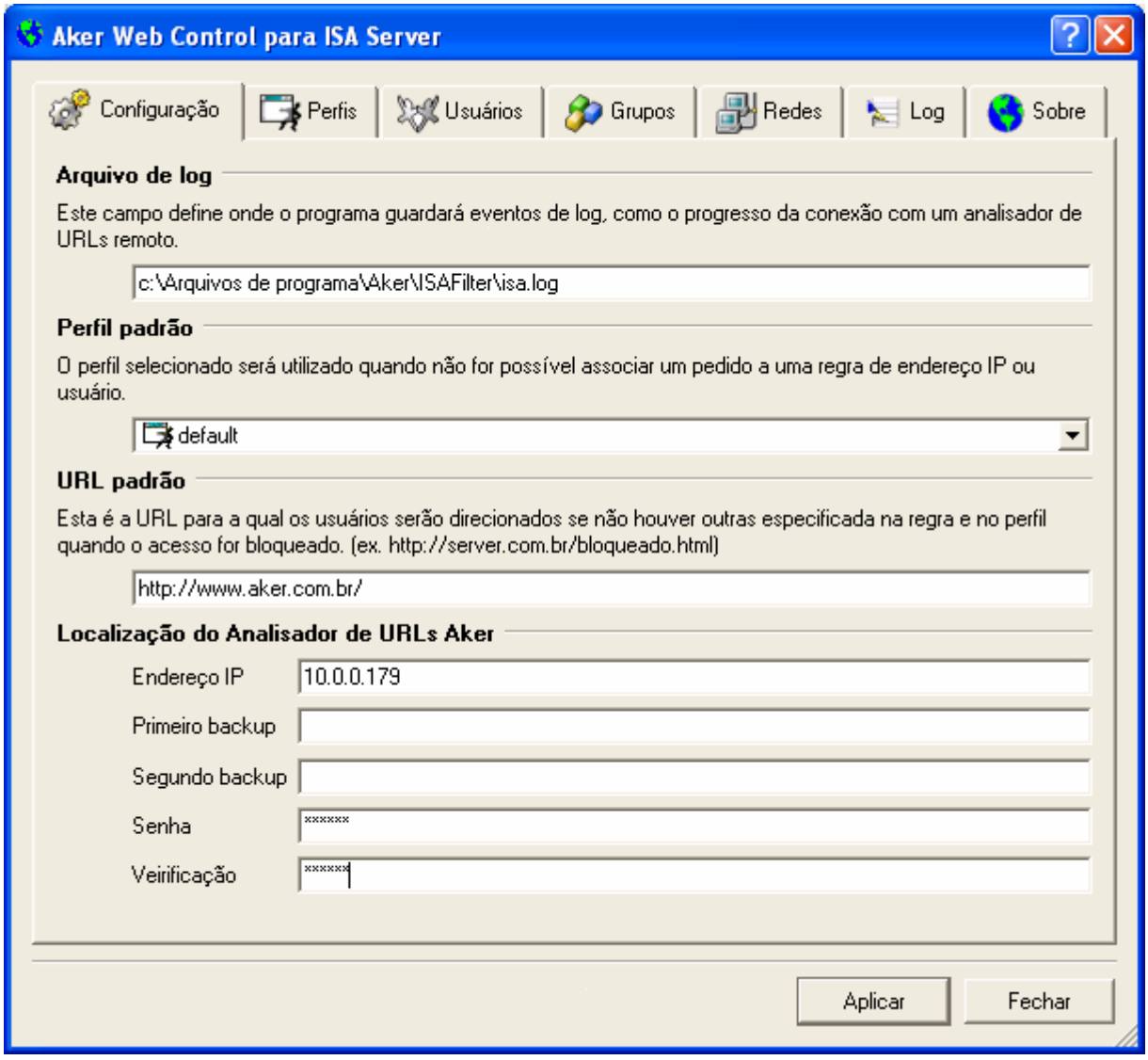
Pressione **Instalar** para finalizar a instalação:



5-3 Configuração do ISA Server

Depois de instalado o plugin, pode-se ativar ou desativar o filtro através do aplicativo **ISA Management** na opção **Servers and Arrays->[nome_do_servidor]->Extensions->Web Filters**.

5-4 Configurações do plugin

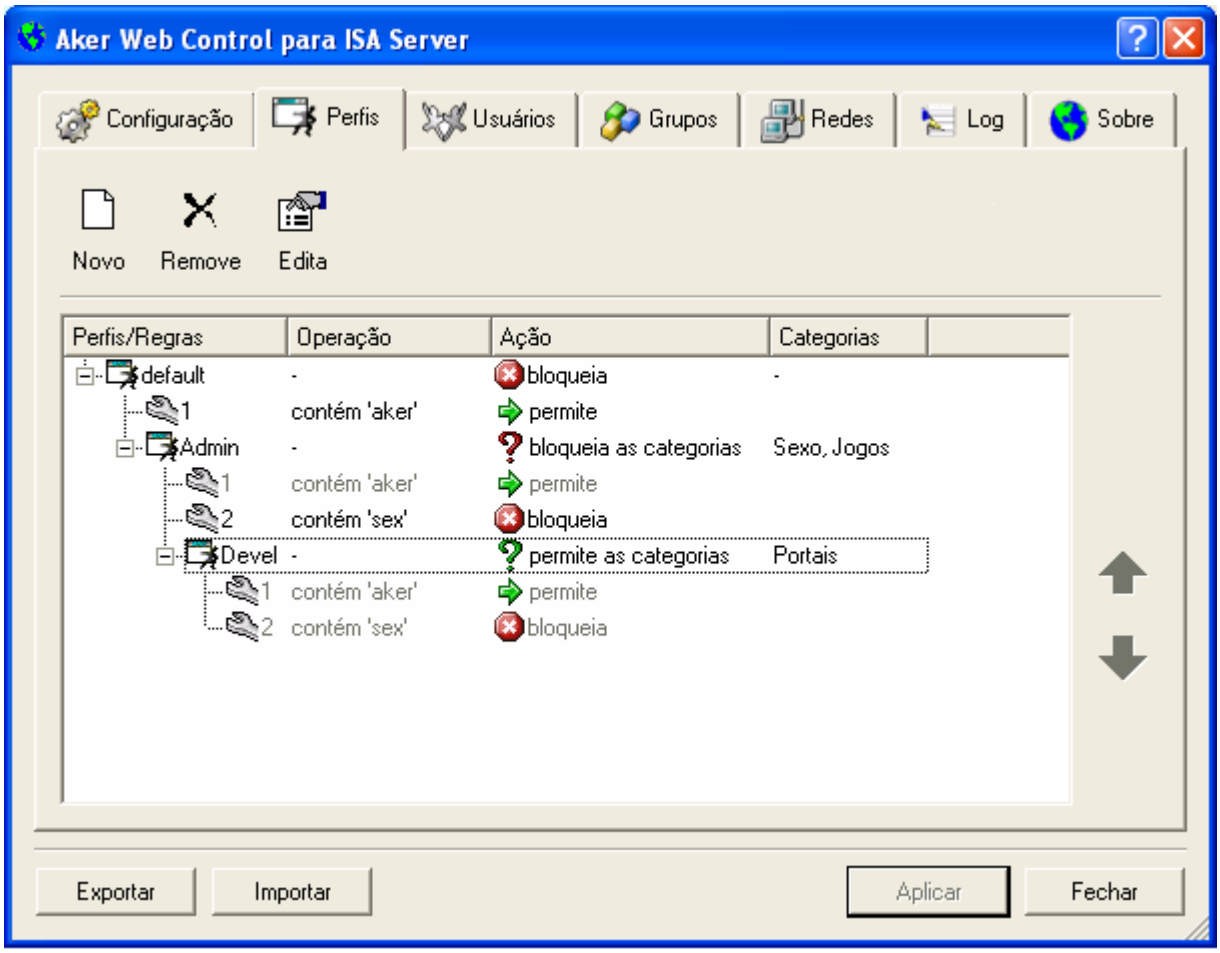


- **Arquivo de log**: Nesse campo, você deve definir um local onde o plugin possa guardar seus registros de fatos relevantes ocorridos, tais como possíveis erros de conexão com o analisador de URLs.
- **Perfil padrão**: Se uma requisição não se encaixar em nenhum perfil específico (veja seções de *Usuários*, *Grupos* e *Redes*), então ela utilizará o perfil aqui definido
- **URL padrão**: O plugin para ISA Server, ao perceber que uma URL deve ser bloqueada, redireciona o usuário para uma página informativa a ser definida. A URL de redireção aponta para essa página e ainda pode passar informações

específicas para a mesma, através da substituição de seqüências especiais de caracteres:

Seqüência especial	Substituída por
%%	Caractere '%'
%u	URL que foi bloqueada
%s	Usuário que tentou um acesso indevido
%i	Endereço IP que originou a requisição bloqueada
%d	Servidor web (FQDN) para o qual se destinava o acesso bloqueado

5-5 Definição de regras e perfis de acesso



Um perfil de acesso é composto de um conjunto de regras ordenadas e de uma ação padrão. Os perfis possuem uma organização hierárquica, ou seja, um perfil criado em um nível inferior possuirá as regras do perfil de nível superior ao qual está subordinado. É importante ressaltar que as regras poderão ser modificadas somente no perfil onde foram criadas.

As regras contém duas partes:

1. Parte de busca: que define uma operação de um pequeno texto. A operação define como o texto será procurado dentro da URL.
2. Parte de ação: Existem quatro ações:

- **Permite**: Permite o acesso que se enquadrar nessa regra
- **Bloqueia**: Não permite o acesso que se enquadrar nessa regra, redirecionando ou para a URL especificada, ou para a padrão
- **Bloqueia as categorias**: Não permite o acesso às páginas que se enquadrarem nas categorias especificadas
- **Permite as categorias**: Permite o acesso apenas às páginas que se enquadrarem nas categorias especificadas, rejeitando-o às demais.

Dentro do perfil, ainda existe uma URL de redireção padrão para suas regras que não a especificarem. Desse modo, a URL de redireção efetiva será:

1. A da regra, se houver
2. A do perfil, estando a da regra em branco
3. A padrão, estando ambas as da regra e do perfil em branco

No campo URL pode-se especificar uma redireção para arquivo local utilizando-se uma URL da forma "file://caminho_completo_do_arquivo". Em caso de um arquivo HTML todas as figuras carregadas por este deverão ser colocadas no diretório "<install_dir>\images\" e carregadas no código como demonstrado no exemplo a seguir.

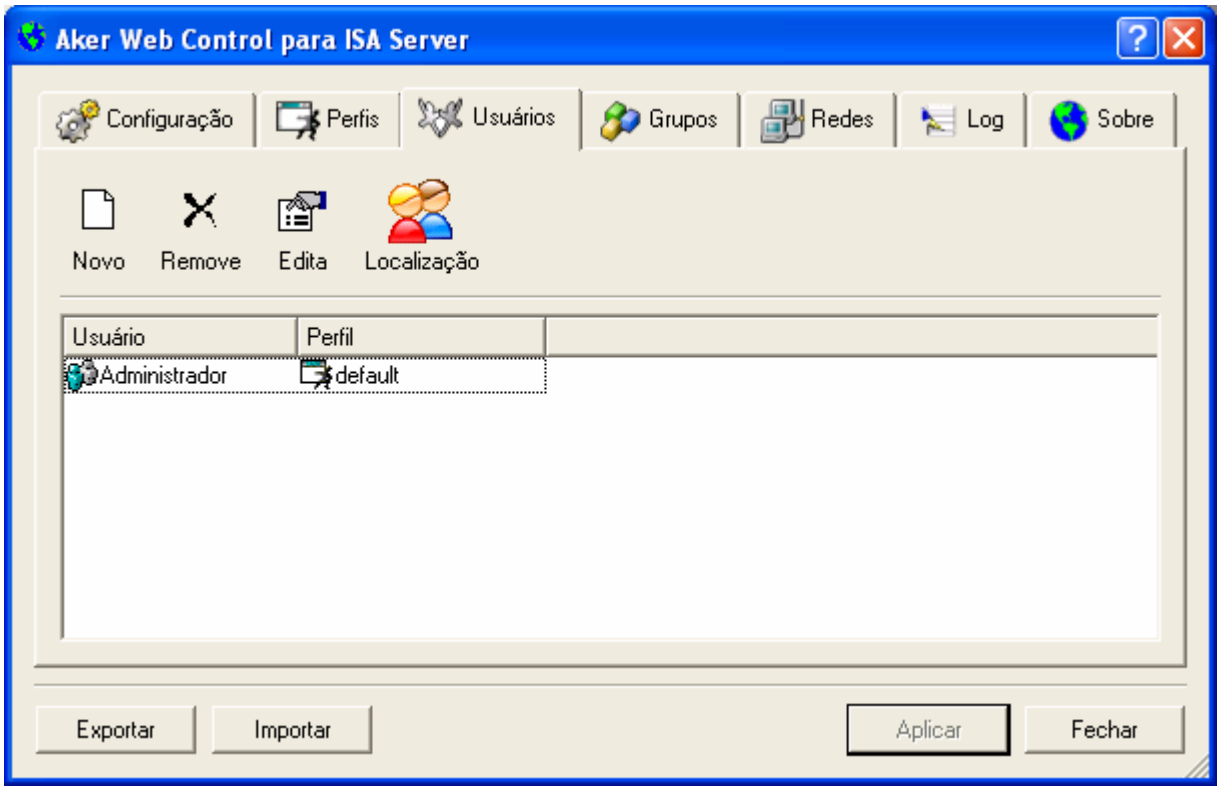
IMG SRC = "http://10.10.10.10/exemplo.gif" (no caso de um servidor acessível pelo IP 10.10.10.10)

5-6 Escolha do perfil

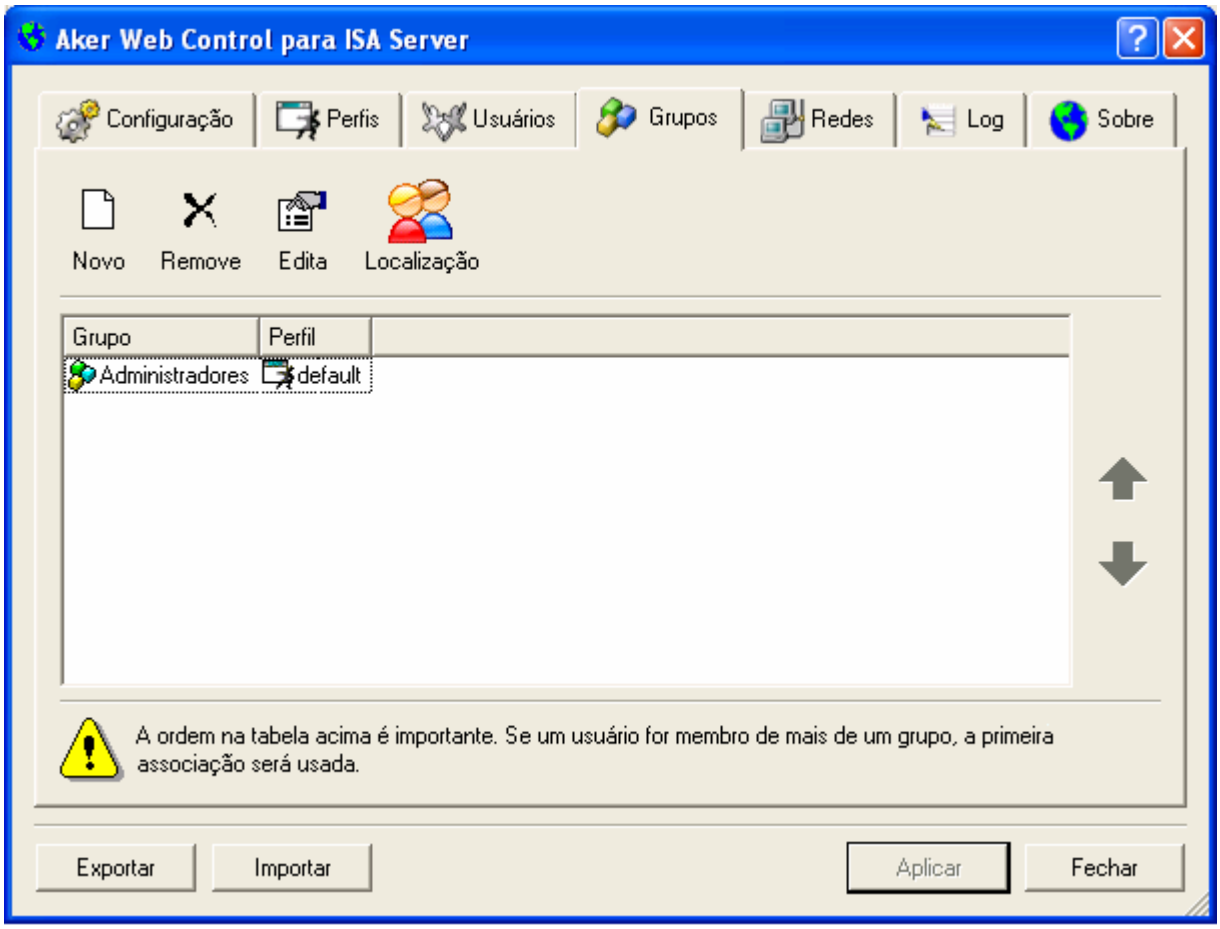
Definidos os perfis de acesso, é preciso configurar o plugin para que ele possa associar cada um dos usuário aos mesmos. Para tanto, existem três características do mesmo que podem ser pesquisadas, na seguinte ordem:

1. **Nome do usuário**
2. **Grupo a que pertence o usuário**
3. **Endereço IP do computador que o usuário está utilizando**

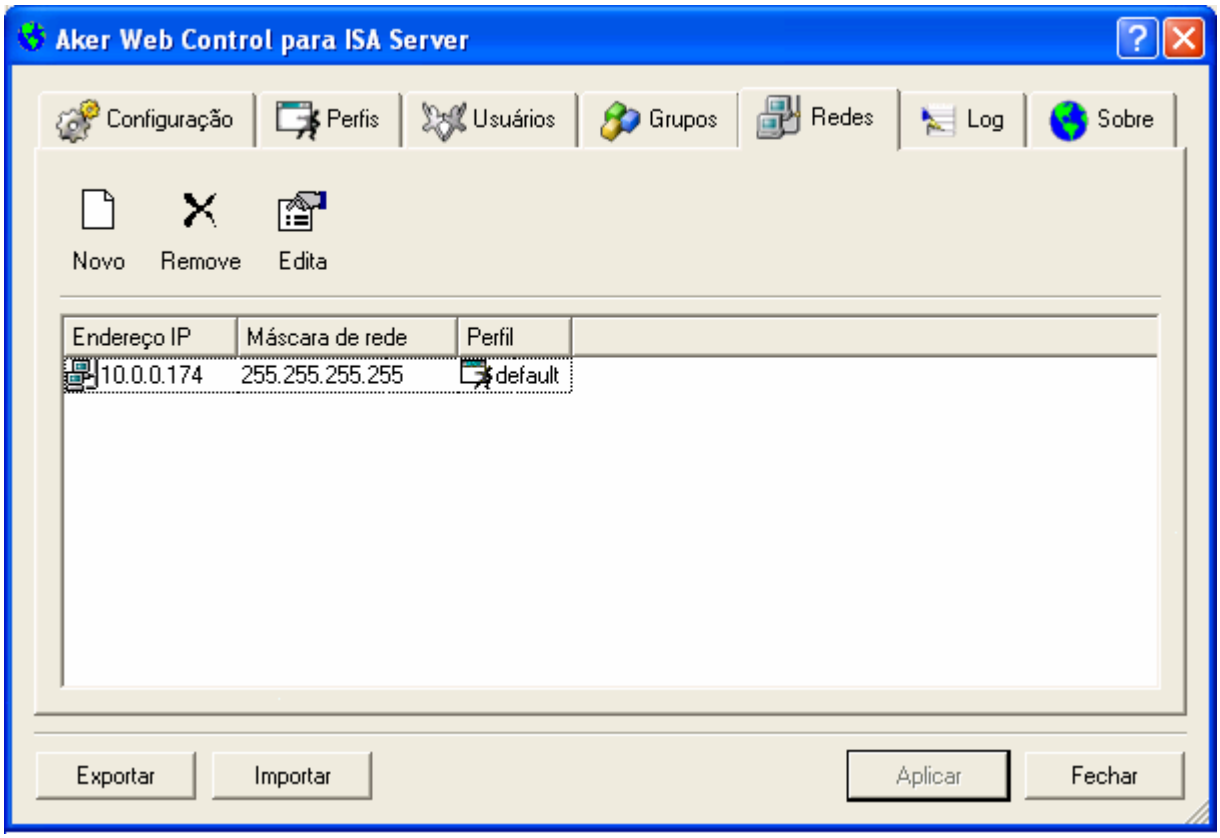
As telas a seguir permitem especificar esses três tipos de regra:



Quando você for editar ou incluir um usuário nessa lista, atentar ao fato que podem ser escolhidos usuários do sistema, obtidos a partir de um agente de autenticação ou digitados os nomes dos mesmos dentro do mesmo *combo-box*. O nome do usuário que o ISA Server vai informar ao plugin depende da autenticação de usuários feita pelo pr&oacuteprio servidor.



Do mesmo modo que na lista de associações para usuários, você pode digitar nomes de grupos arbitrários. Diferentemente dos usuários, os grupos não são informados pelo ISA Server ao plugin, de forma que esse vai procurar dentro da lista de grupos do sistema operacional onde ele está sendo executado ou a partir de um agente remoto.



Não conseguindo escolher um perfil por uma associação de usuário ou de grupo, o plugin vai examinar o endereço IP do cliente para obter um perfil de acesso.

Apêndice A - Mensagens do Log

Abaixo estão mostradas todas as mensagens que podem aparecer no log do Analisador de URLs Aker. Sempre que ocorrerem, elas estarão seguidas de um registro que contém informações adicionais sobre o evento.

- **Erro ao criar socket**

Esta mensagem indica que o analisador não conseguiu criar o socket na pilha TCP/IP necessário para seu funcionamento. Verifique se o protocolo TCP/IP está instalado e funcioando.

- **Erro no bind**

  Esta mensagem indica que o analisador de URLs não conseguiu associar seu socket com a porta necessária para sua comunicação com os firewalls. Verifique se existe algum outro programa utilizando a mesma porta do analisador.

- **Erro no accept**

Erro interno do protocolo Winsocks. Verifique se a pilha TCP/IP esta corretamente instalada e funcionando.

- **Erro ao receber dados**

Essa mensagem indica que ocorreram problemas durante a recepção dos dados enviados pelo firewall. Verifique a conexão física (cabos, placas de rede, hubs, etc) entre as duas máquinas.

- **Firewall fechou a conexão**

A conexão com o firewall foi fechada inesperadamente. Isso pode ocorrer devido a reinicializações no firewall feitas pelos administradores.

- **Autenticação da comunicação com o Firewall**

O analisador conseguiu autenticar corretamente um firewall que estabeleceu uma conexão. O número IP do firewall em questão será mostrado no painel de log.

- **Tentativa de conexão de Firewall não cadastrado**

O analisador recebeu uma tentativa de conexão de um firewall não cadastrado e, devido a isso, a recusou. Para aceitar conexões de um firewall, é necessário que se cadadastre o mesmo na janela ***Contexto*** > ***Firewalls***

- **Erro no select**

Erro interno do protocolo Winsocks. Verifique se a pilha TCP/IP esta corretamente instalada e funcionando.

- **Erro ao enviar dados**

Essa mensagem indica que ocorreram problemas durante o envio de dados para o firewall. Verifique a conexão física (cabos, placas de rede, hubs, etc) entre as duas máquinas.

- **Restabelecendo conexão com Firewall**

  Esta mensagem indica que um dos firewalls cadastrados está reestabelecendo uma conexão com o analisador de URLs.

- **Conexão com Firewall estabelecida com sucesso**

Esta mensagem indica que todo o processo de estabelecimento.

- **Finalizando conexões com Firewalls**

Esta mensagem indicar que as conexões foram encerradas com os firewalls que utilizavam o analisador de URLs.

- **Erro na autenticação com proxy http**

O analisador de URLs não conseguiu utilizar o proxy da rede do usuário para atualizar a base de dados de URLs. Verifique no botão Opções se a senha e nome de usuários estão corretos

- **Site sem categoria definida**

O site não está cadastrado na base de dados do Analisador de URLs Aker.

- **Site com categoria não definida**

A base de dados de URLs está corrompida. Entre em contato com o suporte técnico da Aker Security Solutions para notificação do problema.

- **Site de sexo**

A URL está classificada como tendo conteúdo de sexo.

- **Site contendo frases de baixo calão**

A URL está classificada como tendo conteúdo de frases de baixo calão.

- **Sites de drogas ou álcool**

A URL está classificada como tendo conteúdo de drogas ou álcool.

- **Site de jogos de azar**

A URL está classificada como tendo conteúdo de jogos de azar.

- **Site de violência**

A URL está classificada como tendo conteúdo de violência.

- **Site de astrologia ou misticismo**

A URL está classificada como tendo conteúdo de astrologia ou misticismo.

- **Site de diversão**

A URL está classificada como tendo conteúdo de diversão.

- **Site de jogos eletrônicos**

A URL está classificada como tendo conteúdo de jogos eletrônicos.

- **Site de hobbies**

A URL está classificada como tendo conteúdo de hobbies.

- **Site financeiro ou de investimentos**

A URL está classificada como tendo conteúdo financeiro ou de investimento.

- **Site de procura de empregos**

A URL está classificada como tendo conteúdo de procura de empregos.

- **Site de viagens**

A URL está classificada como tendo conteúdo de viagens ou turismo.

- **Site de veículos ou motores**

A URL está classificada como tendo conteúdo de veículos ou motores.

- **Site de notícias**

A URL está classificada como tendo conteúdo de notícias.

- **Site de encontros e namoros**

A URL está classificada como tendo conteúdo de encontros e namoros.

- **Site de compras**

A URL está classificada como tendo conteúdo de compras.

- **Site de esportes**

A URL está classificada como tendo conteúdo de esportes.

- **Site de bate-papo**

A URL está classificada como tendo conteúdo de bate-papo.

- **Site erótico ou de nudez**

A URL está classificada como tendo conteúdo erótico ou de nudez.

- **Site portal da internet**

A URL está classificada como sendo um portal da internet.

- **Site de hackers**

A URL está classificada como tendo conteúdo de assuntos de hackers.

- **Site de crimes ou de terrorismo**

A URL está classificada como tendo conteúdo de crimes ou de terrorismo.

- **Site de música ou MP3**

A URL está classificada como tendo conteúdo de música ou MP3.

- **Site de WebMail**

A URL está classificada como sendo um WebMail.

- **Erro ao abrir arquivo de atualização de URLs**

Esta mensagem indica que a base de dados foi transferida, contudo o arquivo poderá estar corrompido. Tente baixar novamente a base de dados.

- **Arquivo de atualização de URLs inválido**

O analisador conseguiu transferir a base de dados, contudo a mesma está em formato incompatível. Tente baixar novamente a atualização da base de dados. Se o problema persistir contate o suporte técnico.

- **Erro na leitura de arquivo de atualização de URLs**

O arquivo de atualização poderá estar danificado. Tente baixar novamente a atualização.

- **Erro na escrita de arquivo de atualização de URLs**

O analisador de contexto não está conseguindo gravar o arquivo de base de dados. Verifique se existe espaço suficiente no disco rígido para efetuar a gravação.

- **URLs atualizadas com sucesso**

A base de dados de URLs foi atualizada com sucesso. A mensagem complementar indica o número de URLs que foram inseridas, modificadas ou excluídas desde a última atualização.

- **Erro ao criar arquivo de atualização de URLs**

O analisador de URLs não está conseguindo gravar o arquivo de base de dados. Verifique se existe espaço disponível no disco rígido e que as permissões de gravação do diretório estão corretas.

- **URL inválida**

A URL foi digitada erradamente. Ela deve estar no formato http://www.nomedosite.dominio.sufixo

- **Erro durante o download de arquivo de atualização**

Durante a transferência da base dados houve erro de comunicação com o servidor da Aker Security Solutions. Verifique se os sites de atualização estão corretos.

- **Substituição da base de URLs falhou**

A troca do arquivo com a base dados antiga por uma nova não obteve sucesso. Tente baixar novamente a atualização ou a base de dados completa.

- **Substituição da base de URLs feita com sucesso**

A troca do arquivo com a base dados antiga por uma nova foi realizada com sucesso.

- **Base de dados corrompida**

A base de dados local encontra-se corrompida. Faça o download da base completa e se o problema persistir entre em contato com o suporte técnico da Aker Security Solutions.

- **Atualizando base de dados diária**

A atualização da base de dados de URLs está em andamento.

- **Arquivo ainda não disponível para download**

A base de dados de URLs do dia que se está tentanto baixar ainda não foi colocada no site para distribuição. Tente nova conexão mais tarde.

- **Chave de ativação não encontrada**

A chave de ativação não se encontra no diretório especificado. Execute novamente os procedimentos de carga da mesma.

- **Chave de ativação expirou**

A chave de ativação chegou ao fim do seu tempo de uso. Contacte a Aker Security Solutions para uma renovação.

- **Chave de ativação irá expirar dentro de alguns dias**

A chave de ativação está com seu tempo de uso próximo do fim. A quantidade de dias restantes é mostrada no log. Contacte a Aker Security Solutions para uma renovação.

- **Autenticação com proxy falhou**

O proxy da rede poderá estar fora do ar. Verifique o problema e tente nova conexão.

- **Firewall já está conectado**

Um mesmo firewall está tentando nova conexão com o analisador de contexto. Isso pode ocorrer no caso de quedas desse firewall.

Em circustâncias normais, o analisador de URLs detecta uma nova conexão e encerra a antiga. No caso de problemas, entretanto, é suficiente se fechar o serviço e iniciá-lo novamente.

Apêndice B - Copyrights e Disclaimers

Neste apêndice estão listados os *disclaimers* dos códigos fontes de terceiros utilizadas no Analisador de URLs Aker. Estes *disclaimers* se aplicam apenas às partes explicitamente citadas e não ao Analisador de URLs Aker como um todo. Eles estão citados aqui devido a exigências das entidades desenvolvedoras:

Algoritmo MD4

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD4 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD4 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Algoritmo MD5

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.