

TerminET

Firewall Pessoal

Manual do Utilizador

Índice

| | | |
|----------|---|-----------|
| 1 | INTRODUÇÃO | 3 |
| 1.1 | ACERCA DO TERMiNET | 3 |
| 1.2 | FUNÇÕES CHAVE | 3 |
| 2 | COMO COMEÇAR | 3 |
| 2.1 | INSTALAR O TERMiNET | 3 |
| 2.2 | INICIAR A SESSÃO NO TERMiNET | 4 |
| 2.2.1 | <i>Windows 95/98</i> | 4 |
| 2.2.2 | <i>Windows NT/2000</i> | 4 |
| 2.3 | MODO ADMINISTRADOR | 4 |
| 2.4 | A INTERFACE TERMiNET | 5 |
| 3 | UTILIZADORES E GRUPOS. GERIR UTILIZADORES E GRUPOS | 7 |
| 3.1 | ADICIONAR UTILIZADORES | 7 |
| 3.2 | CRIAR GRUPOS | 8 |
| 4 | REGRAS DE TRÁFEGO | 8 |
| 4.1 | REGRAS STANDARD: | 8 |
| 4.2 | REGRAS AVANÇADAS: | 8 |
| 4.3 | CRIAR REGRAS: | 9 |
| 5 | LISTAS DA WEB | 11 |
| 5.1 | LISTAS NEGRAS | 11 |
| 5.2 | LISTAS BRANCAS | 11 |
| 5.3 | LISTAS GLOBAIS E LOCAIS | 11 |
| 6 | PROBLEMAS COM NETBIOS | 12 |

1 Introdução

1.1 Acerca do TermiNET

TermiNET é um Firewall Pessoal concebido para proteger o PC de ataques vindos do exterior quando o computador está ligado à Internet, navegando pela web ou acedendo a outros serviços da Internet. A instalação inicial do TermiNET pode ser efectuada de uma das seguintes maneiras:

1. **“Modo Fechado”**, por predefinição bloqueia todo o tráfego para e da máquina local. O administrador pode então abrir selectivamente o acesso - por exemplo, permitir apenas o acesso de FTP ou permitir o acesso de FTP, Telnet e Web. Para efeitos de controlo paternal o acesso pode ser limitado a um conjunto específico de páginas. . As páginas podem ser introduzidas directamente como regras específicas ou lidas a partir de uma “Lista Branca” de URLs.
2. **“Modo Aberto”**, não impõe nenhuma condição inicial de bloqueio. O administrador pode então fechar selectivamente o acesso específico por aplicação, porta e protocolo-por exemplo: bloquear Telnet e FTP, bloquear todas as comunicações que chegam na porta 25, bloquear o acesso a um conjunto específico de páginas da web. Também estas limitações podem ser introduzidas como regras específicas ou lidas de um URL “Lista Negra” ou sites aceitáveis
3. **“Modo Secreto”**, permite todo o tráfego de saída mas bloqueia todas as comunicações a entrar a menos que tenham sido iniciadas localmente. Neste modo a máquina pode ser utilizada para navegar pela Web, FTP etc. como normalmente, mas está protegida de ataques enquanto está ligada à Internet.

TermiNET é uma solução de segurança ideal para os utilizadores caseiros e de pequenas e médias empresas que desejam ligar-se com segurança à Internet mas não dispõem dos recursos para suportar uma grande infra-estrutura de segurança

1.2 Funções Chave

As funções chave do TermiNET incluem

- Regras Standard e Avançadas: Funcionalidade simples de caixas de verificação para **activar** ou **desactivar**.
- Funcionalidade Lista Negra/Lista Branca que fornece a capacidade de proibir o acesso a sites indesejados específicos ou para permitir o acesso apenas a sites conhecidos e aprovados.
- Controlo de acesso flexível permite que as regras sejam especificadas por Endereço IP, URL, Porta e / ou Protocolo
- As regras que se baseiam no tempo, podem ser configuradas para estar activas apenas em dias especificados.
- Uma interface do estilo “Windows Explorer”, fácil de utilizar, torna a configuração do TermiNET simples e intuitiva, mesmo para os utilizadores com limitados conhecimentos técnicos.

2 Como Começar

2.1 Instalar o TermiNET

Insira o CD do TermiNET na unidade de CDs do PC. O Programa de Instalação deverá ser executado automaticamente, mas se Autorun (Execução Automática) tiver sido desactivado faça clique em “Iniciar” -> “Executar” e digite “D:\setup” onde D: é a letra da unidade de CDs. Siga as instruções no ecrã para instalar o produto. Durante a instalação é possível especificar a localização da instalação e escolher um dos três modos de segurança predefinidos, Aberto, Fechado ou Secreto descritos acima

Quando a rotina de instalação estiver concluída, o PC **tem de** ser reiniciado para a instalação ficar completa.

2.2 Iniciar a Sessão no TerMiNET

2.2.1 Windows 95/98

Aquando do início do sistema, o TerMiNET inicia-se com um conjunto de regras predefinido, determinado pelo Administrador. Se tiverem sido criados múltiplos perfis de utilizador TerMiNET, existem duas maneiras de iniciar a sessão como um dos utilizadores definidos, fazendo duplo clique no ícone TerMiNET no grupo do sistema ou, em alternativa, fazendo clique com o botão direito do rato no ícone TerMiNET e seleccionando "Iniciar Sessão". Seja qual for o processo escolhido, será apresentado ao utilizador um ecrã de início de sessão que lhe solicita a indicação da ID do utilizador e da palavra-passe. A introdução da ID do Utilizador e da Palavra-passe, irá activar o perfil de permissão de acesso do utilizador especificado.

2.2.2 Windows NT/2000

Os utilizadores iniciam automaticamente a sessão no TerMiNET com base no perfil de Início de Sessão do NT.

2.3 Modo Administrador

O modo Administrador permite especificar o perfil de permissão de acesso predefinido do utilizador, criar novos perfis de utilizador e definir regras avançadas para utilizadores específicos.

A entrada no modo Administrador é efectuada fazendo clique com o botão direito do rato no ícone do sistema TerMiNET e seleccionando "Modo Administrador". Ser-lhe-á pedida a palavra-passe do Administrador. Uma vez introduzida a palavra-passe aparece o ecrã Configuração do TerMiNET, onde é permitido efectuar as funções administrativas.

Para sair do modo Administrador, basta fechar o ecrã de configuração utilizando a opção do menu "Ficheiro" -> "Sair do Administrador".

2.4 A Interface TermiNET

A Interface TermiNET (Figura 1) só está acessível se for utilizada a palavra-passe do Administrador. É simples utilizar uma ferramenta gráfica para definir os perfis de permissão de acesso para uma máquina.

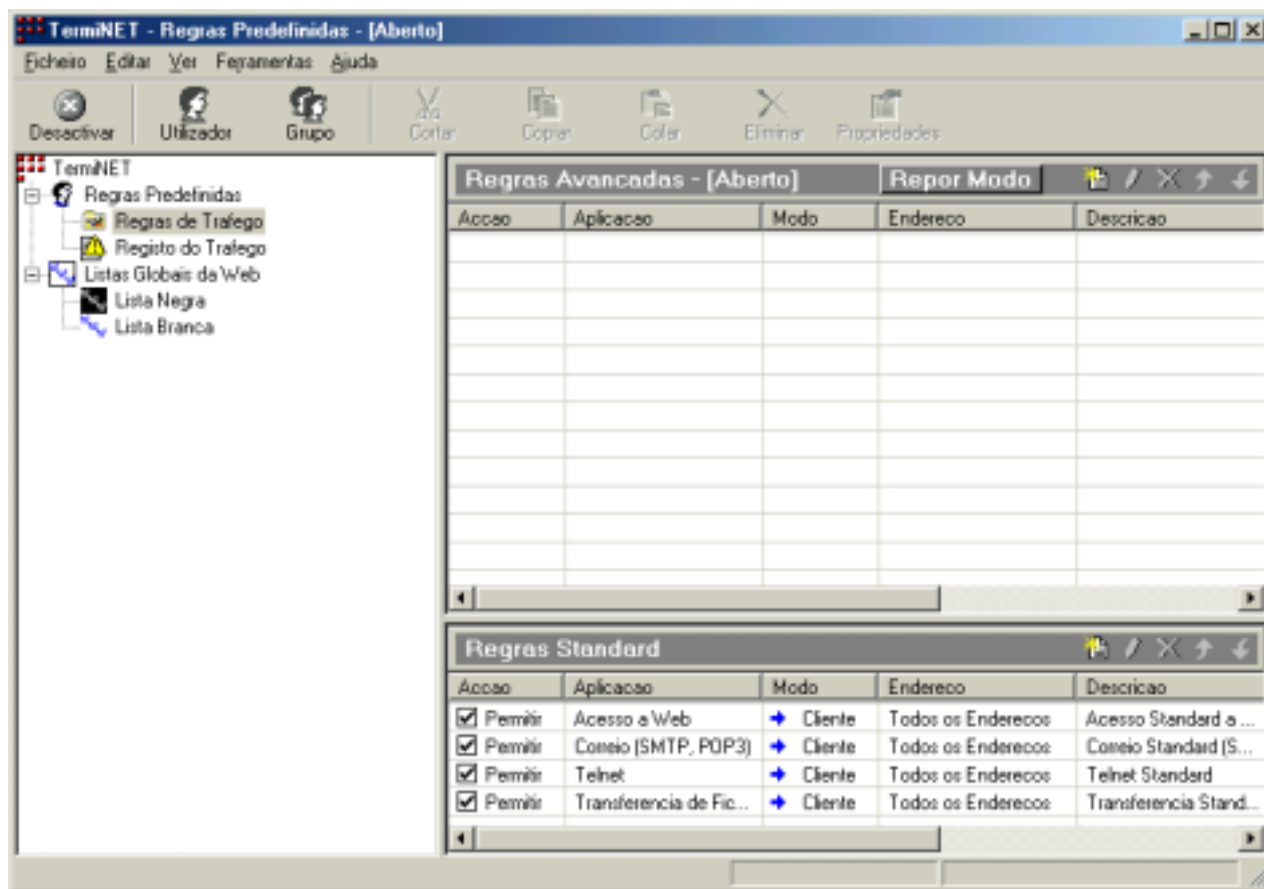


Figura 1

A interface está dividida em três secções; a secção do lado esquerdo apresenta uma vista em árvore do sistema de segurança definido. A secção inferior direita apresenta as "Regras Standard" que são predefinidas pelo sistema. A secção superior direita apresenta as regras avançadas que possam ter sido criadas. Seleccionando um utilizador na janela do lado esquerdo faz com que a janela do lado direito apresente o estado das regras avançadas e standard desse utilizador.

Os menus Ficheiro, Editar e Ver permitem que a interface seja personalizada de acordo com as preferências dos Administradores. O menu “Ferramentas” -> “Opções” permite a definição de propriedades aplicáveis a todo o sistema.

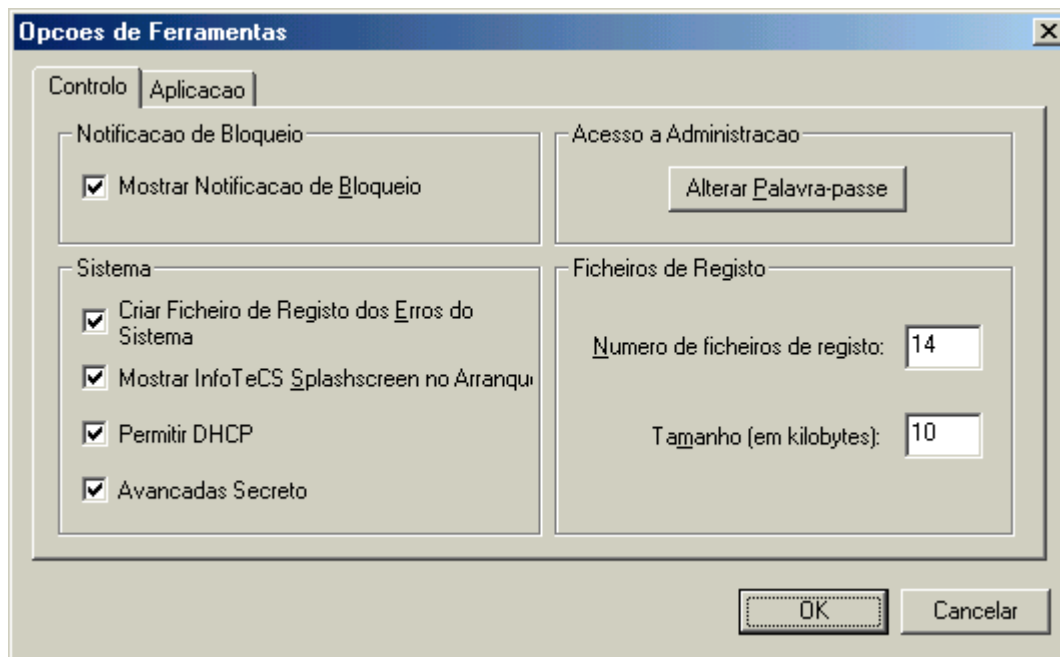


Figura 2

O separador Controlo (Figura 2) dá acesso às seguintes opções.

- | | |
|--|---|
| Mostrar Notificação de Bloqueio: | Se for seleccionada, o Registo do Tráfego mostra tanto o tráfego bloqueado como o permitido. Se esta opção não estiver seleccionada só será registado o tráfego permitido. |
| Criar Ficheiro de Registo dos Erros do Sistema: | Se for seleccionada os erros do sistema serão gravados no ficheiro \Programas\Infotecs\Terminet\Data\errorlog.txt |
| Mostrar Infotecs Splashscreen no Arranque: | Deixe não seleccionada para impedir que o Infotecs Splashscreen apareça quando o TerMiNET é iniciado. |
| Mudar Palavra-passe: | Permite que a palavra-passe de Administração seja alterada. |
| Número de ficheiros de registo: | Define o número de ficheiros de registo do tráfego que serão gravados. Uma vez atingido o número de ficheiros de registo especificado e de o último ficheiro ter chegado ao seu tamanho máximo, o primeiro ficheiro começará a ser substituído. |
| Tamanho (em kilobytes): | Define o tamanho em kilobytes até ao qual os ficheiros de registo do tráfego podem crescer. Uma vez atingido este tamanho, o ficheiro será guardado e o registo começa a ser feito noutra ficheiro. |

O separador Aplicação (Figura 3) permite a criação de novas aplicações standard.

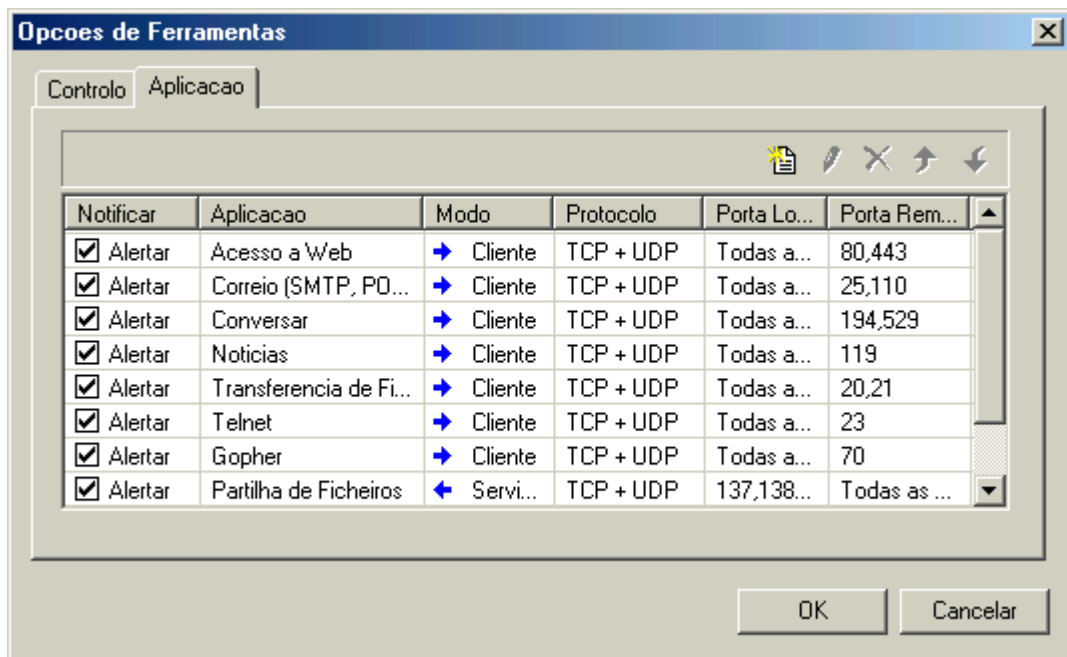


Figura 3

Faça clique no botão Adicionar Aplicação  para abrir a caixa de diálogo Personalizar Aplicação (Figura 4).

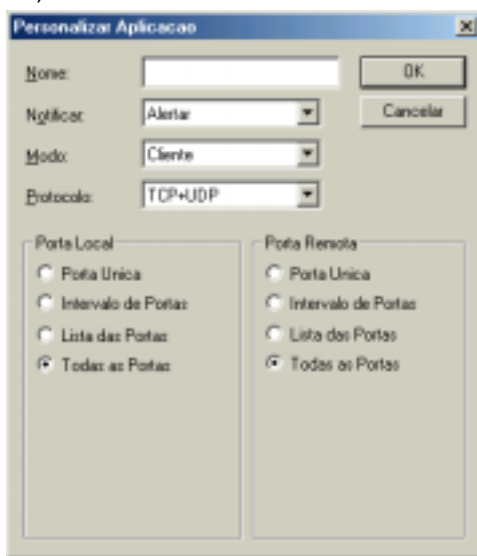


Figura 4

Esta janela permite definir as seguintes opções.

- **Nome:** Especifica o Nome da aplicação personalizada.
- **Protocolo:** Selecciona da lista pendente o protocolo desejado para a aplicação.
- **Notificar:** Selecciona da lista pendente Alertar ou Ignorar. Se for seleccionada a opção Alertar, irá aparecer uma notificação quando o tráfego deste tipo estiver bloqueado.
- **Direcção:** Selecciona da lista pendente Para Dentro ou Para Fora.
- **Porta Remota:** Especifica a definição da porta aplicável à máquina remota para esta aplicação.
- **Porta Local:** Especifica a definição da porta aplicável à máquina local para esta aplicação.

3 Utilizadores e Grupos. Gerir Utilizadores e Grupos

3.1 Adicionar Utilizadores

Para adicionar um perfil de utilizador, faça clique com o botão direito do rato no nível mais alto da vista em árvore do TermiNET e seleccione "Adicionar Utilizador" do menu de atalhos, ou faça clique no botão Utilizador da barra de ferramentas. Abre-se a caixa Propriedades do Utilizador (Figura 5)

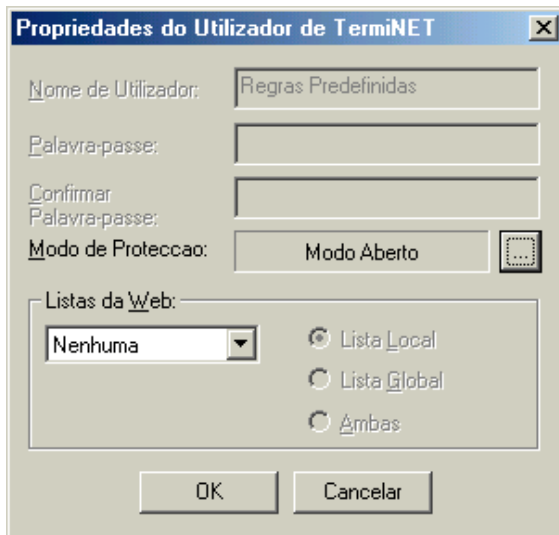


Figura 5

Estão disponíveis os seguintes campos:

- **Nome do Utilizador:** Utilizado para introduzir o Nome do Utilizador.
- **Palavra-passe:** Introduza a palavra-passe do utilizador.
- **Confirmar Palavra-passe:** Introduza novamente a palavra-passe para confirmação.
- **Modo de Protecção:** Seleccione o Modo de Segurança predefinido para este utilizador.
- **Listas URL:** Determina se este utilizador vai utilizar as Listas Brancas ou Negras de URLs e se serão utilizadas listas globais, locais ou ambas.

3.2 Criar Grupos

Os Grupos podem ser utilizados para organizar listas de utilizadores dentro da vista em árvore do TermiNET. Crie um novo grupo fazendo clique com o botão direito do rato no nível mais alto da árvore, seleccionado “Adicionar Grupo” do menu de atalho e digitando o nome desejado para o Grupo. Os utilizadores podem a seguir ser colocados nos grupos fazendo clique no nome do utilizador e arrastando-o para o grupo desejado. Pode ser criado um utilizador num grupo existente fazendo clique com o botão direito do rato no grupo da vista em árvore e seleccionando “Adicionar Utilizador” no menu de atalho

4 Regras de Tráfego

Existem dois tipos de regras de tráfego que podem ser definidas no TermiNet.

4.1 Regras Standard:

Aplicam-se a todos os Endereços IP e podem ser utilizadas para permitir ou proibir de forma global o acesso a serviços específicos. Existem quatro regras standard predefinidas pelo sistema, Web Access, Mail, FTP e Telnet. Podem ser adicionadas regras adicionais seleccionando um utilizador na vista em árvore, fazendo clique com o botão direito do rato no painel Regras Standard e seleccionando “Adicionar Regra” no menu de atalho para abrir a caixa de diálogo Adicionar Regra (Figura 6).

4.2 Regras Avançadas:

Aplicam-se a Endereços IP ou URLs específicos e são utilizadas para permitir ou proibir selectivamente o acesso a sites e serviços. As regras são adicionadas seleccionando o utilizador ao qual a regra se vai aplicar, fazendo clique com o botão direito do rato na janela Regras Avançadas e seleccionando “Adicionar Regra” no menu de atalho para abrir a caixa de diálogo Adicionar Regra (Figura 6).

Quando o TermiNET está instalado no modo Secreto só podem ser configuradas Regras Avançadas.

4.3 Criar Regras:

A caixa de diálogo Adicionar Regra (Figura 6) é utilizada para criar e definir novas regras.

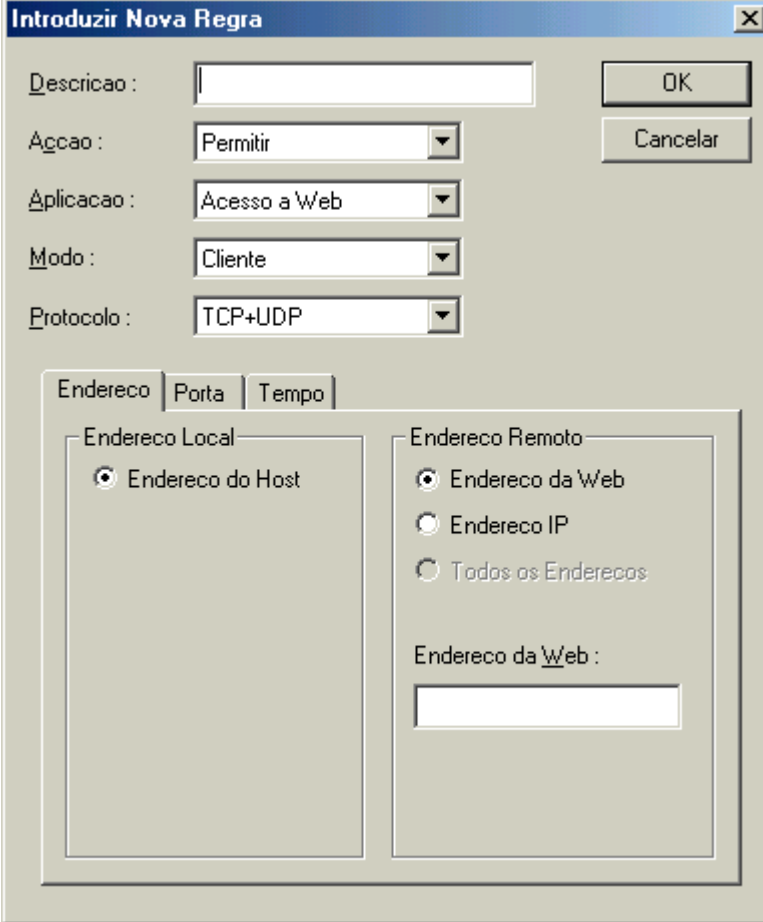


Figura 6

Estão disponíveis os seguintes campos:

- **Descrição:** Digite uma descrição para a regra que está a ser criada
- **Ação:** Decida se a regra irá Permitir ou Bloquear o tráfego definido.
- **Aplicação:** Seleccione da lista predefinida de aplicações ou digite um novo nome para a aplicação a que esta regra se aplica.
- **Modo:** Especifique se a máquina local vai ser um computador cliente ou servidor para esta regra. Se especificar cliente, isso significa que a regra se vai aplicar ao tráfego que sai, se especificar servidor, isso significa que a regra se vai aplicar ao tráfego que entra.

Os separadores Endereço (Figura 7), Porta (Figura 8) e Tempo (Figura 9) são utilizados para especificar as funções avançadas da regra.

Endereço:

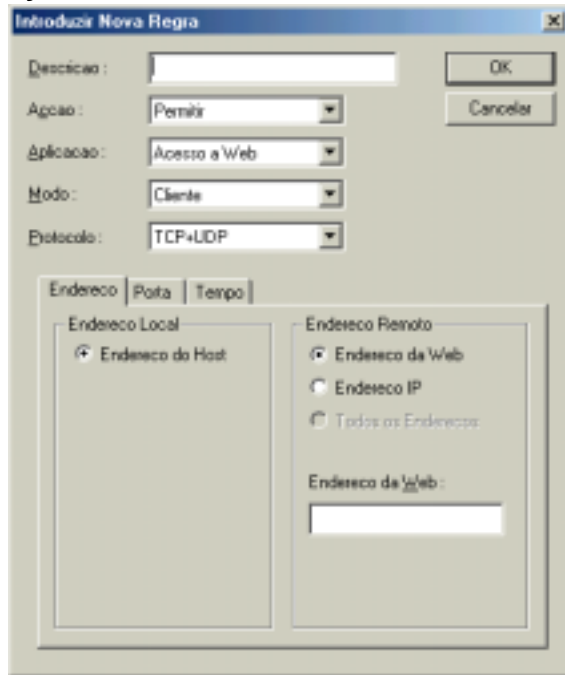


Figura 7

Para as regras standard a única opção disponível neste separador é “Todos os Endereços”.

Para as Regras Avançadas pode ser especificado o site a que a regra se aplica, quer pelo URL ou pelo Endereço IP.

Se o botão de rádio URL for seleccionado pode introduzir um URL no campo Endereço.

Se o botão Endereço IP for seleccionado, o campo Endereço passa a ser um campo de introdução de Endereço IP.

Porta:



Figura 8

O separador Porta (Figura 8) é utilizado para especificar a porta ou o intervalo de portas a que a regra se aplica. As definições da porta devem ser configuradas tanto para a máquina local como remota. Estão disponíveis as seguintes opções:

- **Porta Única:** Permite a especificação de um único número de porta para a regra
- **Intervalo de Portas:** Permite a especificação de um intervalo de portas para a regra.
- **Lista of Portas:** Permite que uma lista de portas seja especificada para a regra.
- **Todas as Portas:** A regra é aplicável a todas as portas.

Tempo:



O separador Tempo permite que a regra seja activada apenas em dias específicos.

Figura 9

5 Listas da Web

As listas da Web podem ser utilizadas para permitir ou bloquear o acesso a sites específicos. As listas de URLs podem ser Listas Negras ou Listas Brancas. As Listas Negras e Brancas são mutuamente exclusivas, isto é, os utilizadores configurados para utilizar uma Lista Negra não podem ser configurados para utilizar uma Lista Branca e vice versa.

5.1 Listas Negras

As Listas Negras são utilizadas para bloquear o acesso a sites que uma regra possa permitir. Por exemplo, uma regra standard pode estar configurada para permitir o acesso a toda a web, mas um determinado site, por exemplo, www.nãopermitido.com consta de uma Lista Negra. Nestas circunstâncias, o utilizador poderá navegar para todos os sites da web excepto o www.nãopermitido.com.

5.2 Listas Brancas

As Listas Brancas são utilizadas para permitir o acesso a sites que uma regra possa bloquear. Por exemplo uma regra standard pode bloquear o acesso a toda a web mas um site específico, por exemplo www.disney.com consta de uma Lista Branca e assim o utilizador não poderá navegar para outros sites da web para além do www.disney.com.

5.3 Listas Globais e Locais

Existem dois tipos de Listas Negras e Brancas: Locais e Globais. Uma lista Global é criada pelo Administrador e pode ser aplicada a todos os utilizadores; as entradas da lista global serão aplicadas a todos os utilizadores para os quais o Administrador especificou utilizar a lista Global de URLs. Uma lista local é criada apenas para um utilizador específico; as entradas nesta lista só se aplicam ao utilizador para o qual a lista foi criada.

6 Problemas com NetBIOS

Em determinadas circunstâncias poderá ter problemas no acesso a hosts que utilizam NetBIOS sobre TCP/IP quando no modo Secreto. O problema ocorre quando a sua máquina utiliza emissões para determinar o Endereço IP de um host da rede. No Modo Secreto o TermiNET bloqueia as mensagens de resposta dos hosts impedindo o estabelecimento de comunicações.

Nestas circunstâncias é necessário fazer uma entrada no ficheiro "HOSTS" relacionando os Endereços IP dos hosts relevantes com os seus nomes NetBIOS. "HOSTS" é um simples ficheiro de texto geralmente localizado no directório C:\windows do Win'98 ou c:\system32\drivers\etc do Win NT e pode ser editado utilizando qualquer processador de texto. Um ficheiro de amostra chamado hosts.sam nesse directório fornece detalhes sobre a estrutura de ficheiros. Um ficheiro host típico terá o seguinte aspecto.

```
192.168.25.2 myserver.myorg.com
192.168.56.10 nt_server_1
```

Se desejar adicionar um host chamado nt_server_2 com Endereço IP 192.168.35.23 edite o ficheiro como a seguir se indica.

```
192.168.25.2 myserver.myorg.com
192.168.55.10 nt_server_1.192.168.35.23 nt_server_2
```

Este problema não existe se a sua rede tiver um servidor WINS configurado.