IBM eNetwork Firewall for Windows NT

Guia do usuário

Versão 3 Release 2.1.1

GC17-1348-01

IBM eNetwork Firewall for Windows NT

Guia do usuário

Versão 3 Release 2.1.1

GC17-1348-01

Nota: Antes de utilizar esta informação e o produto que suporta, certifique-se de ler a informação geral no Apêndice A, “Avisos” na página 125.

Segunda Edição (Junho 1998)

Esta edição aplica-se à Versão 3 Release 2.1.1 do IBM eNetwork Firewall para Windows NT (número de produto 5765-C16). Esta edição substitui a GC17-1348-00.

Índice

Sobre Este Manual

Este manual descreve como configurar e administrar o IBM eNetwork Firewall em um sistema Windows NT** para impedir comunicação indesejada ou não-autorizada dentro ou fora de sua rede protegida.

Este manual é destinado a administradores de proteção de sistemas ou de rede que instalam, administram e utilizam o IBM Firewall. Embora haja uma descrição de como acessar o firewall utilizando programas cliente, este não é um manual do usuário para programas cliente. Para utilizar programas cliente como telnet ou FTP, consulte o guia do usuário para seus programas cliente TCP/IP.

Utilize as Instruções de Instalação anexadas à caixa do CDROM para instalar o produto antes de utilizar este manual.

Depois de iniciar o cliente de configuração, as informações do auxílio online irão auxiliá-lo a preencher os campos do cliente de configuração e a deslocar-se de um quadro de diálogo para outro.

Conhecimento de Pré-requisito

É importante que se tenha um bom conhecimento a respeito de endereçamento TCP/IP, máscaras e administração de rede para se instalar e configurar o IBM Firewall. Como você irá instalar e configurar um firewall que controla o acesso dentro e fora da rede, é necessário primeiro entender como a rede opera. Especificamente, é necessário compreender os fundamentos dos endereços IP, nomes completamente qualificados e máscaras de sub-rede.

Um manual excelente sobre TCP/IP que abrange netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, roteamento e muito mais é o *TCP/IP Network Administration*. Consulte a *Bibliografia* para obter mais detalhes.

Um manual excelente para administradores UNIX, que também oferece uma excelente visão geral sobre TCP/IP e roteamento, hardware de rede, DNS e sendmail é o *UNIX System Administration Handbook.* Consulte a Bibliografia para maiores detalhes.

Recursos Neste Release

O IBM eNetwork Firewall for Windows NT oferece uma grande variedade de recursos e inclui todas as três arquiteturas do firewall.

1. Proxies de aplicação
   - FTP
   - HTTP, incluindo Gopher e WAIS
   - Telnet
   - SafeMail

   HTTP, Telnet e FTP possuem capacidade de autenticação.
2. Gateway de nível de circuito através do Socks Protocol Versão 5, um padrão da Internet

3. Filtragem—um conjunto de critérios amplo e robusto no qual o tráfego pode ser permitido ou negado. Os critérios incluem endereço, porta, protocolo, direção, adaptador (protegido/não-protegido) TCP/IP e mais.

   Muitos serviço pré-definidos tornam a configuração mais rápida.

Socks Protocol Versão 5

Além de sua simplicidade e flexibilidade, o Socks Protocol Versão 5 oferece estas vantagens:

- Fácil desenvolvimento de métodos de autenticação e codificação
- Associação UDP, que cria um circuito proxy virtual para atravessar circuitos proxy baseados em UDP.
- Socks V5 Watcher, que exibe informações de desempenho de soquetes em tempo real

Network Address Translation

Com o crescimento explosivo da Internet, o problema de esgotamento de endereços IP tornou-se significativo. Network Address Translation (NAT) apresenta uma solução ao problema de esgotamento de endereços IP com base na reutilização do endereço.

A vantagem do NAT é que ele permite, de modo transparente, que uma rede que utiliza endereços privados ou ilegais comunique-se com hosts na Internet, permitindo efetivamente que a rede privada tenha um grande espaço para endereço. Além disso, com o uso do NAT, endereços na rede privada ficam ocultos ao mundo externo fornecendo um nível extra de segurança.

Administração Simples

Através do uso de uma aplicação JAVA**, você pode administrar a partir de uma máquina remota, você pode facilmente fazer atualizações na configuração do firewall. Administradores diferentes podem ser atribuídos a diferentes níveis de autoridade para controlar, futuramente, o acesso ao firewall. Esta interface gráfica com o usuário (GUI) individual de fácil compreensão pode ser utilizada para administrar o Windows NT Firewall e o AIX Firewall.

Robustecimento do NT

Quando o firewall estiver instalado, protocolos diferentes dos de TCP/IP são desativados, serviços de sistema desnecessários são desativados, e logins locais de contas diferentes das do administrador são desativadas.

Autenticação poderosa

Suporte para todos os mecanismos de autenticação baseados em token, tais como SecurID, SecureNet Key e outros, é oferecido.

Utilitários de Relatório

Utilitários de relatório permitem que você execute uma consulta SQL junto ao registro de sistema uma vez que esse seja exportado para uma máquina de banco de dados.

Alerta, Monitoração e Registro

Os registros extensivos e detalhados incluem toda a atividade do firewall junto ao endereço TCP/IP, ids de usuário, TOD, nomes de arquivo, números de porta, e assim por diante. Um Monitor de Log encontra-se incluído para observar atividades suspeitas e alertar quando os limites forem ultrapassados.

Isolar Diversas Redes

Ao se utilizar diversas Placas de Interface de Rede (NICs) no firewall, você pode isolar diversas sub-redes.

Suporte a Idioma Nacional

O suporte a idioma nacional é oferecido para inglês, japonês, Coreano, francês, chinês simplificado, chinês tradicional, italiano, espanhol e português do Brasil.

Fornecimento de Endereços de IP

Ao configurar seu firewall, você será solicitado a fornecer endereços de IP. Será preciso digitar um endereço de IP completo, com pontos decimais, com todos os 4 octetos, no formato:

`nnn.nnn.nnn.nnn`

sendo que cada `nnn` é um conjunto de três números situados dentro do intervalo de 000–255.

Como Chamar o Serviço IBM

O Centro de Suporte IBM oferece assistência por telefone no diagnóstico e solução de problemas. Você pode ligar para o IBM Support Center a qualquer hora; sua chamada será retornada dentro das oito horas comerciais(Segunda–Sexta, 8:00 a.m.–5:00 p.m., horário comercial local). O número do atendimento é 1-800-237-5511.

Quem estiver fora do Brasil deve entrar em contato com o representante local da IBM ou com o fornecedor autorizado da IBM.

Capítulo 1. Introdução ao IBM Firewall

O IBM eNetwork Firewall é um programa de proteção de rede para AIX e Windows NT**. Na essência, um firewall é um bloqueio entre uma ou mais redes privadas internas protegidas e outras redes (não-protegidas) ou a Internet. O objetivo de um firewall é evitar a ocorrência de comunicação indesejada ou não-autorizada para dentro ou para fora da rede protegida. O firewall possui três funções:

- Reforçar seus regulamentos de segurança da Internet.
- Permitir que usuários em sua rede usem recursos autorizados da rede externa sem comprometer seus dados da rede e outros recursos.
- Manter usuários não autorizados fora de sua rede.

Conceitos do Firewall

A conectividade entre qualquer pessoa da Internet pode apresentar diversos riscos de segurança. É necessário proteger seus dados privados e também proteger o acesso às máquinas dentro de sua rede privada para evitar o uso externo abusivo. A primeira etapa para se alcançar esta proteção é limitar o número de pontos nos quais a rede privada está conectada à Internet. A configuração onde a rede privada está conectada à Internet apenas por um gateway fornece a você controle sobre qual tráfego será permitido dentro e fora da Internet. Este gateway é chamado de firewall.

Para compreender como um firewall funciona, conside ê co do co. Imagine um edifício no qual de ê eja restringir o acesso e ter controle das pessoas que entram. A sala de espera do edifício é o único ponto de entrada. Nesta sala, há algumas pessoas para recepcionar aqueles que entram no edifício, alguns seguranças para vigiá-cos, algumas câmeras de víde ê para registrar suas ações e alguns crachás para autenticar suas ide ê tificações.

Jdo funciona muito bem no controle da entrada de um edifício privado.
Mas se uma pessoa não-autorizada consegue ir além da sala de espera, não há como proteger o edifício das ações de ê ta pessoa. No entanto, se os movime ê tos de ê ta pessoa forem supervisionados, talvez seja possível de ê ectar qualquer comportame ê to suspeito.

Quando estiver de ê inindo sua estratégia do firewall, pode ê achar que é suficie ê te proibir tudo que apresenta risco para a empresa e permitir o resto. No entanto, de ê ido a no ê os métodos de ataque, é necessário antecipar como evitar ado ataques e, como no caso do edifício, é necessário monitorar os sinais que indicam que de algum modo suas de ê esas foram rompidas. Geralme ê te, os dano ê e custos para recuperação de um rompime ê to são muito maiores do que uma prevenção inicial.

Ferramentas IBM Firewall

O IBM Firewall é como uma caixa de ferramentas utilizadas para implementar diferentes arquiteturas do firewall. Depois de escolher a arquitetura e a estratégia de segurança, selecione as ferramentas IBM Firewall necessárias. O cliente de configuração do IBM Firewall fornece uma interface gráfica com o usuário amigável para administração. O IBM Firewall apresenta um registro amplo de todos os eventos significantes, como alterações na administração e tentativas de violação da segurança.

Como o IBM Firewall é, na verdade, um gateway IP, ele divide o mundo em duas ou mais redes: uma ou mais redes não-protegidas e uma ou mais redes protegidas. A rede não-protegida é, por exemplo, a Internet. As redes protegidas são, geralmente, suas redes IP da empresa. Algumas das ferramentas fornecidas pelo IBM Firewall são:

- Filtros expert
- Servidores Proxy
- Servidores socks
- Serviços específicos como serviço de nome de domínio (DNS) e SafeMail

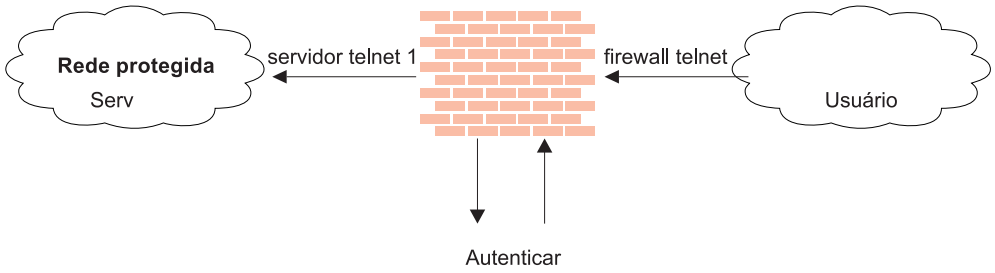
Filtros Expert

Filtros expert são ferramentas que inspecionam pacotes no nível de sessão baseado em múltiplos critérios tais como hora do dia, endereço IP e sub-rede. As regras do filtro trabalham com a função do gateway IP de tal modo que é necessário que a máquina tenha duas ou mais interfaces de rede, cada uma em uma rede ou sub-rede IP separada. Um conjunto de interfaces é declarado não-protegido e o outro conjunto é declarado seguro. O filtro atua entre os dois conjuntos de interfaces, como ilustrado na Figura 1.Figura 1. Firewall com Filtragem Expert

Rede p

Servidores Proxy

Ao contrário da filtragem, que só inspeciona pacotes que estão atravessando, os servidores proxy são aplicações executadas no firewall e realizam uma função TCP/IP específica em nome de um usuário da rede. O usuário contata o servidor proxy usando uma das aplicações TCP/IP (Telnet ou FTP). O servidor proxy faz contato com esse host remoto no nome do usuário, controlando assim o acesso enquanto oculta sua estrutura de rede dos usuários externos. A Figura 2 ilustra um servidor proxy Telnet interceptando um pedido de um usuário externo.Figura 2. Firewall com um



clara, o cliente de soquetes inicia uma sessão com o serviço soquetes do Windows NT no host do IBM Firewall, depois confirma que o endereço de origem e a ID de usuário tem permissão para estabelecer uma conexão progressiva com a rede não protegida e depois cria a segunda sessão. A Figura 3 ilustra um firewall com um servidor socks.

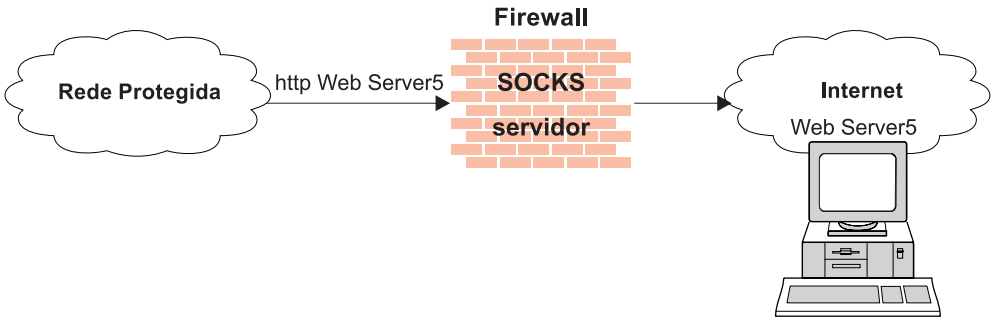


Figura 3. Firewall com um Servidor Socks

Clientes Socksified (clientes que estão cientes de Soquetes) estão disponíveis em muitas aplicações como Netscape Navigator** ou Microsoft** Internet Explorer ou através de software TCP/IP como o Aventail** AutoSocks**.

Objetivos do Servidor Socks

Para sessões de saída (de um cliente protegido para um servidor não protegido), o servidor de soquetes possui os mesmos objetivos de um servidor proxy, isto é interromper a sessão no firewall e fornecer uma porta protegida na qual usuários devem provar sua identidade para poderem passar. Ele possui a vantagem da simplicidade para o usuário, com pouco trabalho administrativo extra.

Serviço de Nome de Domínio

O acesso aos registros de nome de domínio para a rede protegida é uma grande assistência a intrusos, pois fornece a eles uma lista de sistemas centrais a serem atacados. Um servidor de serviço de nome de domínio subvertido também pode fornecer uma rota de acesso a um intruso. A partir da rede externa, o servidor de nome no firewall conhece somente a si mesmo e nunca fornece informações na rede IP interna. A partir da rede interna, este servidor de nome conhece a rede Internet e é muito útil para acessar qualquer máquina na Internet através do nome.

Objetivos do Servidor DNS

A execução do servidor DNS no firewall possui a dupla vantagem de impedir que solicitações de resolução de nome fluam pelo firewall e esconder sistemas centrais da rede protegida do mundo não-protegido.

SafeMail

Correspondência é um dos principais motivos que levam uma empresa a desejar acessar a Internet. O SafeMail é um gateway de correspondência da IBM projetado para ocultar nomes de domínio de sua rede interna. A função SafeMail não armazena correspondência no gateway ou roda sob a ID de usuário raiz. O nome de domínio público do gateway do firewall é substituído por nomes de domínio privado na correspondência distribuída, para que esta correspondência pareça estar vindo do endereço do firewall ao invés de vir do endereço do usuário.

O SafeMail suporta Simple Mail Transfer Protocol (SMTP) e Multipurpose Internet Mail Extensions (MIME).

Utilização do Auditor de Segurança de Rede

Auditor de Segurança de Rede - Network Security Auditor - varre sua rede a procura de falhas de segurança ou erros de configuração. O Auditor de Segurança de Rede varre seus servidores e firewalls para compor uma lista de problemas ou vulnerabilidades, tais como portas abertas e outras exposições e compila uma lista para que você possa executar as correções. O Auditor de Segurança de Rede pode ser utilizado como uma varredura periódica de hosts decisivos ou como uma ferramenta de agrupamento de informações em determinado momento. A administração do Auditor de Segurança de Rede é feita através de uma interface de linha de comando fácil de ser utilizada. Com o Auditor de Segurança de Rede, você mantém vigilância sobre o seu firewall.

Os recursos do Network Security Auditor são:

- Escaneamento das portas TCP e UDP
- Reconhecimento dos servidores em portas não padrão
- Relato de serviços perigosos, vulnerabilidades conhecidas, versões obsoletas do servidor e servidor ou serviços em violação de políticas personalizadas do site
- Geração de relatórios em HTML para fácil navegação

Capítulo 2. Planejamento

Antes de configurar o IBM Firewall, utilize a lista de verificação e as planilhas de planejamento para auxiliá-lo na configuração da rede.

Lista de Verificação de Planejamento

1. Defina seu objetivo. Você deseja:
   - Acessar a Internet (telnet, FTP anônimo, etc.)?
   - Dividir partes de sua rede interna?
   - Fornecer acesso *externo* para sua rede?
2. Avalie a topologia de sua rede no nível de sub-rede de IP.
   - Uma interface protegida e uma não-protegida seria uma configuração correta?
   - Seus endereços têm condições de suportar máscaras de sub-rede em regras?
3. Decidir como você usará DNS. Consulte Capítulo 6, “Manuseio do Serviço de Nome de Domínio” na página 31.
4. Decida como você usará safemail. Consulte Capítulo 7, “SafeMail” na página 39.
5. Se deseja utilizar socks, certifique-se de que clientes socksified, como o Netscape Navigator ou o navegador Microsoft, estão instalados. Para obter informações sobre a utilização de socks, consulte Capítulo 11, “Configuração do o Servidor de Socks” na página 69.
6. Que tipo de autenticação é necessário?
   - Se for utilizar o Security Dynamics** ACE/Server** para autenticar usuários, instale o código de cliente ACE/Server no host do firewall. Sugerimos a instalação do código de servidor ACE/Server em algum outro sistema central dentro da rede protegida.

     Para informações sobre a instalação e utilização de um Security Dynamics ACE/Server e da placa SecurID**, consulte as informações fornecidas pela Security Dynamics Technologies Inc.
   - Se a placa AssureNet Pathways** SecureNetKey** for utilizada, adquira placas independentemente do IBM Firewall.
   - Se utilizar seu próprio método de autenticação, consulte o capítulo Fornecimento de Seus Próprios Métodos de Autenticação no manual *IBM eNetwork Firewall Reference*.
   - Você deve configurar o código do cliente Windows, que implementa a capacidade de pesquisa em domínios Windows NT confiáveis para fins de autenticação, para que utilize TCP ao invés de NETBIOS. O NETBIOS será desativado. Os servidores do Windows NT confiáveis devem possuir nomes de host e endereços TCP/IP e conectividade TCP/IP entre eles e o firewall. O administrador firewall precisa criar conexões entre o firewall e os servidores NT confiáveis para permitir que o tráfego flua entre os dois.

     Configure esta conexão usando os seguintes serviços pré-definidos:

a. Autenticação do Controlador de Domínio - que permite o uso do Controlador de Domínio para autenticação de usuário

b. Transmissões de Serviços de Nome NetBT - que permitem NetBIOS nas transmissões de Serviços de Nome TCP/IP

E utilize os utilitários de configuração do NT para definir relações confiáveis.

7. Se for utilizar filtragem, comece com regras de filtro simples e torne-as altamente restritivas. Familiarize-se com as portas e protocolos utilizados por serviços que você necessita.
8. Escolha um método para compactar registros. A compactação de registros é um candidato ideal para um job programado no serviço do Programador Windows NT. Consulte Capítulo 15, “Gerenciamento de Arquivos de Log e Compactados” na página 107.

Planilha de Planejamento da Configuração da Rede

Preencha as seguintes informações como parte do planejamento para sua configuração do IBM Firewall.

Nome do sistema central do firewall _____

Interface(s) de rede protegida(s) (conectadas à rede interna protegida)

Endereço IP _____ Máscara Sub-rede _____

Endereço IP _____ Máscara Sub-rede _____

Endereço IP _____ Máscara Sub-rede _____

Endereço IP _____ Máscara Sub-rede _____

Interface(s) de rede não-protegida(s) (conectadas à rede não-protegida, não-confiável)

Endereço IP _____ Máscara Sub-rede _____
Endereço IP _____ Máscara Sub-rede _____
Endereço IP _____ Máscara Sub-rede _____
Endereço IP _____ Máscara Sub-rede _____

Nome do roteador _____

Endereço do roteador _____

Nome do Domínio Protegido _____

Endereço de IP do servidor de nome do domínio protegido (DNS) _____

Endereço IP do(s) servidor(es) de nome do domínio não-protegido(s) (DNS) _____

Servidor de Mail Seguro _____

Nome do Domínio Público _____

Endereço de IP do cliente de configuração _____

Endereço de IP do(s) cliente(s) remoto(s) _____

Diretório root do seu Windows NT Firewall_____
(Em toda documentação, fazemos referência a ele como ROOTDIR)

c:\winnt (Assume-se que o Windows NT está instalado neste diretório)

Capítulo 3. Configuração do Servidor e do Cliente de Configuração

Este capítulo descreve como configurar o servidor de configuração e o cliente de configuração, que é a interface gráfica com o usuário (GUI) para o IBM Firewall.

Configuração do Servidor de Configuração

O servidor de configuração é a interface do cliente de configuração do Firewall. O servidor de configuração processa pedidos do cliente de configuração. Ele é executado na máquina do Firewall e pode manipular pedidos de clientes de configuração que estão em máquinas locais ou remotas. Depois de configurado, considere-o parte da máquina do Firewall.

O número de porta do servidor de configuração é especificado no arquivo de serviços NT localizado no diretório onde você instalou o sistema operacional do Windows: `c:\winnt\system32\drivers\etc\services`. O número de porta é padronizado em 1014, mas ele pode ser alterado, para obter segurança extra, interrompendo o serviço do servidor de configuração, modificando o arquivo de serviços e reinicializando o serviço do servidor de configuração.

O servidor de configuração é inicialmente configurado para aceitar apenas pedidos de clientes de configuração na máquina local. Os pedidos iniciais não são codificados. Para alterar estas opções, utilize `fwcfgsrv cmd=change` a partir da linha de comando.

localonly= Indica se o Firewall só pode ser administrado a partir de uma máquina local.

- **localonly=yes** A configuração só pode ocorrer na máquina local; este é padrão.
- **localonly=no** A configuração pode ocorrer a partir de qualquer máquina.

encryption Indica se o servidor de configuração espera ou não que os dados de chegada sejam codificados através da camada de soquetes segura (ssl) ou não.

Se você alterar a opção de codificação ou o sslfile, você deve interromper e reinicializar o serviço do servidor de configuração.

- **encryption=none** Nenhuma codificação deve ocorrer; este é o padrão.
- **encryption=ssl** A codificação SSL irá ocorrer.

sslfile= Indica o nome do arquivo-chave SSL a ser utilizado com a codificação SSL; o padrão é `ROOTDIR\config\fwkey.kyr`. *ROOTDIR* é o diretório selecionado durante o processo de instalação como local de destino para o IBM Firewall. Para obter informações sobre como criar o arquivo-chave, consulte o manual *Referência ao IBM eNetwork Firewall.*

Se um cliente de configuração não puder conectar-se à máquina do Firewall, e se estiver em uma máquina diferente, utilize `fwcfgsrv cmd=list` para verificar se `localonly=no` está definido. Além disso, a linguagem utilizada pelo cliente e o servidor deve ser correspondente. Por último, certifique-se de que o serviço do servidor de configuração está operando observando o painel de serviços e verificando seu status. Para fazer isto, vá ao painel central, clique duas vezes o ícone Serviços e verifique o status de cada serviço. Caso não esteja operando, o serviço deve ser reinicializado.

Configuração do Cliente de Configuração (GUI)

Ao instalar o IBM Firewall, o cliente de configuração é automaticamente instalado. O cliente de configuração também pode ser instalado separadamente em qualquer máquina Windows NT sem o Firewall, o que possibilita a administração remota. Para iniciar o cliente de configuração, clique duas vezes o ícone do cliente de configuração no grupo do programa Firewall IBM. Quando o cliente de configuração é iniciado, você deve primeiro conectar-se ao Firewall usando uma conta de administrador Windows NT.

Somente administradores Windows NT e administradores firewall que possuem a autenticação de administração adequada podem utilizar o cliente de configuração para conectar-se ao Firewall.

Depois de instalado o Firewall, todos os administradores Windows NT são designados como administradores primários do firewall. Utilize o cliente de configuração para conectar-se ao servidor de configuração utilizando um administrador primário do firewall e defina os nomes de usuário de administrador do firewall adicionais, se necessário. Consulte Capítulo 12, “Administração de Usuários no Firewall” na página 75 para obter informações sobre como definir administradores do firewall utilizando o cliente de configuração.

Para definir o valor de timeout de logon para máquinas mais rápidas ou mais lentas, efetue a seguinte alteração clicando sobre o ícone do Cliente de Configuração do IBM Firewall, depois clique em **Propriedades**. Modifique as Propriedades utilizando o item **Atalho**. Altere o parâmetro `timeout` para *20*, onde 20 é o número de segundos a serem aguardados até que uma conexão ocorra. Máquinas mais rápidas devem ser definidas com 10 e as mais lentas devem aceitar o valor padrão.

Para aumentar o nível de informações de depuração no console do JAVA, execute `ibmfw.bat` no `ROOTDIR\cfgcli\gui` ao invés de utilizar o ícone do cliente de configuração. Observe, contudo, que ativando o console o registro pode diminuir o desempenho.

Logon no Cliente de Configuração

Para fazer o logon no cliente de configuração (na máquina local ou remota):

- O usuário deve ser um administrador do firewall.
- O administrador do firewall deve possuir um esquema de autenticação definido. Consulte “Métodos de Autenticação de Usuário” na página 81.
- O usuário deve possuir autorização para executar funções específicas de configuração

Ativação da Configuração Remota através do Cliente de Configuração

Para ativar a configuração remota através do cliente de configuração, certifique-se de que o administrador que vai fazer o logon possui os seguintes atributos definidos na máquina do Firewall:

- Se o administrador estiver no lado protegido da rede e utilizando uma interface protegida na máquina do Firewall, então ele deve ser definido com o método de autenticação apropriado para administração protegida. (Ele não pode ser definido para negar tudo). Isto também se aplica à conexão feita no Firewall local.
- Do mesmo modo, se o administrador estiver no lado não-protegido utilizando uma interface não-protegida na máquina do Firewall, então ele deve ser definido com o método de autenticação apropriado para administração não-protegida. (Ele não pode ser definido para negar tudo).

Todos os atributos de usuário podem ser definidos através do quadro de diálogo Modificar Usuário no cliente de configuração ou através do uso do comando `fwuser`. Todos os Administradores firewall terão todos os campos acima adequadamente definidos após a instalação do Firewall. Consulte o Capítulo 12, “Administração de Usuários no Firewall” na página 75 para maiores informações.

Exemplos de Saída de Registro para o Servidor de Configuração Remota

Segue abaixo o exemplo de uma saída de registro para o servidor de configuração remota:

```
Feb 03 13:52:15 1998 mr16n18: ICA9005i: Iniciando serv. de config. remota.

Feb 03 13:52:21 1998 mr16n18: ICA2024i: Adm. do usuário foi autenticado
com sucesso utilizando a autenticação NT a partir da rede protegida:127.0.0.
Feb 03 13:52:21 1998 mr16n18: ICA2169i: Adm. do usuário foi autenticado
com sucesso para o Serv.Adm.Remota util.NT a partir da rede protegida:127.0.0.1.
```

Capítulo 4. Utilização do Cliente de Configuração

Utilize o cliente de configuração, que é uma interface gráfica com o usuário, para configurar e administrar o IBM Firewall.

Quando o IBM Firewall é instalado pela primeira vez, ele é configurado inicialmente para só aceitar pedidos do cliente de configuração na máquina local. No entanto, o cliente de configuração pode ser instalado em outra máquina e a administração do Firewall pode ser feita remotamente. Veja informações a esse respeito no “Configuração do Servidor de Configuração” na página 11.

Para definir o cliente de configuração para iniciar na linguagem de seu ambiente específico, clique sobre o ícone do Cliente de Configuração do IBM Firewall, depois clique em **Propriedades**. Modifique as Propriedades utilizando o item **Atalho**. Por padrão, o local da máquina do host é usado. O IBM Firewall suporta estes ambientes:

- en_US - Inglês americano
- ja_JP - Japonês PC
- ko_KR - Coreano
- zh_CN - Chinês Simplificado EUC
- zh_TW - Chinês Tradicional (Big 5)
- fr_FR - Francês
- it_IT - Italiano
- pt_BR - Português do Brasil
- es_ES - Espanhol PC

Um mouse é necessário para se utilizar o cliente de configuração.

Um botão de **Auxílio** encontra-se próximo ao topo do painel principal do cliente de configuração. Clique em **Auxílio** para obter informações sobre qualquer função.

Efetuação do Logon no Cliente de Configuração

1. Para o Tipo de Logon, selecione Local se estiver na mesma máquina do firewall. Local é o padrão. Selecione Remoto para acessar remotamente outro Firewall. O logon remoto requer que a pessoa entre com um nome de host.
2. Caso tenha selecionado logon Remoto será preciso fornecer o nome do host ou endereço IP da máquina do firewall em que o logon vai ser feito.
3. Selecione SSL ou nenhum dependendo da criptografia que está sendo utilizada para o Firewall. Para o Cliente, o padrão para Local é Nenhum e o padrão para Remoto é SSL.
4. Digite um nome de usuário de um administrador do firewall ou administrador do Windows NT.
5. Forneça o número da porta na qual o servidor está interceptando. O padrão é 1014.

6. Para o Modo, selecione Host para configurar a máquina do firewall NT em que você está se conectando. Com a administração de host, o administrador pode atualizar localmente ou remotamente um Firewall por vez. Selecione Enterprise para a administração do Gerenciamento de Firewall de Enterprise (EFM) de firewalls AIX.
7. Depois do logon, mensagens de autenticação serão exibidas e talvez seja solicitado que você forneça uma senha caso esta seja a configuração do método de autenticação para o nome de usuário. Se você for solicitado a fornecer uma senha, digite sua senha no campo Resposta do Usuário e pressione Enter ou clique Submeter. Caso a senha esteja incorreta, será apresentada uma mensagem. Clique em Fechar e reinicie o processo de logon. Se uma senha não for solicitada, é provável que seu método de autenticação seja permitir tudo. Neste caso, o painel do cliente de configuração do IBM Firewall será exibido imediatamente.
8. Depois de ter sido autenticado com sucesso, você verá o painel principal de configuração.

Figura 4. Painel de Logon do Cliente de Configuração

A Árvore de Navegação

O cliente de configuração possui um auxiliar de navegação reduzível em estilo de árvore junto à lateral esquerda, conforme ilustrado em Figura 5 na página 17.

Se um nó ou função possui itens sob ele, um ícone de pasta de arquivos aparece à esquerda do nó. Para ver as subfunções você pode expandir a exibição dando um clique duplo sobre o ícone. Ao dar novamente um clique duplo sobre o ícone a exibição deste nó é reduzida voltando à exibição original.

Qualquer função em que der um clique será considerada selecionada e destacada. Você pode expandir ou reduzir os nós sem efetuar nenhuma alteração na exibição da janela à direita. Quando a árvore expandida excede o espaço vertical disponível, uma barra de deslocamento aparece à direita da árvore de navegação.

Uma barra de deslocamento horizontal aparece se algum dos nomes de função não couber na árvore de navegação.

Figura 5. Árvore de Navegação do Cliente de Configuração

Recursos Gerais do Painel Principal

Acima de **Exibição dos Alertas** serão vistos os três botões a seguir, conforme ilustrado em Figura 5.

Auxílio Um botão de **Auxílio** encontra-se próximo ao topo do painel principal do cliente de configuração. Clique em **Auxílio** para ver o que fazer para instalar e utilizar o IBM Firewall.

Guia do Usuário Um botão **Guia do Usuário** encontra-se próximo ao topo do painel principal do cliente de configuração. Clique em **Guia do Usuário** para ver esta publicação em cópia eletrônica.

Referência Um botão de **Referência** encontra-se próximo ao topo do painel principal do cliente de configuração. Clique em **Referência** para ver esta publicação em cópia eletrônica.

Outros botões que podem ser encontrados no painel principal são:

Último Um botão **Último** encontra-se na parte inferior do painel principal do cliente de configuração. Clique em **Último** para ver os alertas mais recentes.

Logoff/LogOn Um botão **Logoff/LogOn** encontra-se no canto direito superior do cliente de configuração. É um botão de reconexão. A seqüência de logon pode ser reiniciada para que seja feita a conexão com outro Firewall ou para ser feito o logon como outro administrador.

Para desconectar-se, clique logoff e depois clique Cancelar no painel de logon e na aplicação.

Visualizador de Registro

Um botão **Visualizador do Log** encontra-se no canto direito inferior do cliente de configuração. Ele permite que os logs do firewall sejam percorridos.

Anterior

Um botão **Anterior** encontra-se na parte inferior do painel principal do cliente de configuração. Clique em **Anterior** para ver alertas anteriores.

A Exibição de Alertas

Você pode visualizar registros de alertas gerados pelo monitor de log do sistema na seção inferior direita da janela principal do cliente de configuração, conforme ilustrado na Figura 6.

Os registros de alerta exibidos são obtidos do arquivo identificado pelo primeiro recurso de `log de alerta` definido no `ROOTDIR\config\syslog.conf`. Se nenhum recurso `log de alerta` estiver definido você verá uma exibição em branco. Consulte “Inclusão de Recursos de Log” na página 108 para obter auxílio para uma definição de um recurso `log de alerta`.

O painel exibe o nome do arquivo de alertas e os números das linhas atualmente exibidas a partir daquele arquivo. Você pode clicar **Último** para observar os alertas mais recentes. Clicando **Anterior** permite que você veja os alertas anteriores.

Cada linha exibida mostra a data e a hora do alerta, o nome do sistema central do firewal em que o alerta ocorreu, o código de mensagem do alerta e o texto da mensagem de alerta. O código é uma indicação do tipo de alerta.

Figura 6. Exibição dos Alertas

O Visualizador do Log

Clicando **Visualizador de Log** para trazer uma janela visualizador de registro, conforme ilustrado em Figura 7. O visualizador do log permite visualizar registros do log do Firewall. Você pode especificar um arquivo de log e uma contagem de registro (padrão é 25).

O log padrão é o arquivo identificado pelo primeiro recurso `log firewall` definido no `ROOTDIR\config\syslog.conf`. Você pode selecionar um arquivo de log de destino diferente a partir do menu suspenso do campo do nome de arquivo ou pode digitar o nome de um arquivo a ser visualizado.

Para solicitar uma linha de início específica, clique **Iniciar na Linha:,** após digitar o número de linha no campo próximo a ela. Para solicitar as últimas linhas, clique **Rodapé**, que leva para o rodapé do arquivo. **Próximo** avança você para o próximo conjunto de linhas no arquivo. **Anterior** leva você ao conjunto anterior de linhas. **Topo** leva você ao topo do arquivo. Marcando **Sim**, você pode opcionalmente expandir logs do firewall para texto legível.

Consulte “Criação, Colocação e Compactação do Arquivo de Log Utilizando o Cliente de Configuração” na página 107 e Capítulo 14, “Monitoramento dos Registros do Firewall” na página 97 para maiores informações sobre arquivos de log, recursos, monitoração e alertas.

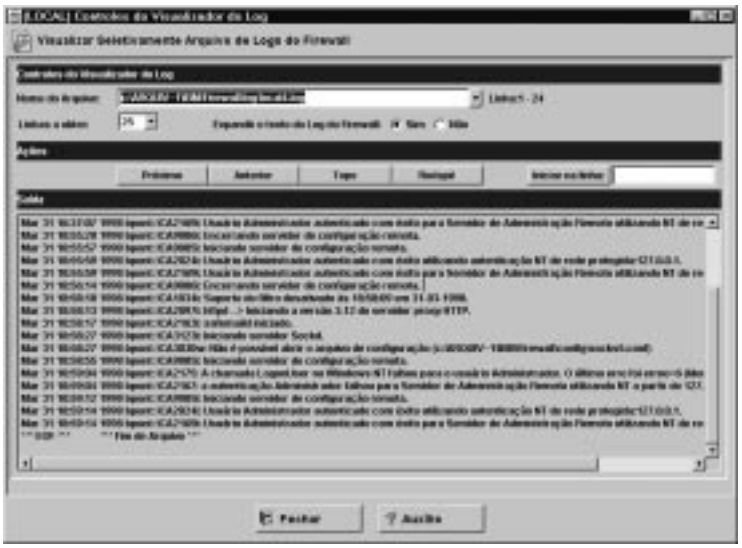


Figura 7. Visualizador do Log

Outros Recursos

Um campo **Pesquisar** encontra-se próximo ao canto esquerdo superior de alguns painéis. Você pode fornecer uma cadeia de pesquisa e clicar em **Encontrar**.

Outros botões que você observará em muitas das caixas de diálogo do cliente de configuração são:

Aplicar Clique em **Aplicar** para preencher o campo no painel anterior com a seleção atual ou para salvar alterações efetuadas em um painel. O botão **Aplicar** não faz com que a janela desapareça.

Rodapé Clique em **Rodapé** para ir para a base de um painel.

Cancelar Clique sobre **Cancelar** para fechar a janela sem salvar qualquer alteração.

Fechar Clique sobre **Fechar** para eliminar a janela de sua tela.

Copiar O botão **Copiar** ajuda a economizar tempo na inclusão de novos itens na lista. Após a seleção de um item na lista, clique em **Copiar** para criar um item que é semelhante ao item selecionado. Ao clicar em **Copiar** para criar um item que é semelhante ao item selecionado, abrirá um novo item que irá copiar valores de campo do item selecionado na lista. Você estará então habilitado a modificar os conteúdos dos campos conforme necessário para o novo item.

Eliminar Clique sobre **Eliminar** para eliminar um item selecionado da lista.

Mover para Baixo Selecione um item na lista e clique em **Mover para Baixo** para que a posição relativa do item desça na lista. Cada clique fará o item descer uma posição.

Mover para Cima Selecione um item na lista e clique em **Mover para Cima** para elevar a posição relativa do item na lista. Cada clique causará a movimentação do item para cima em uma posição.

OK Clique sobre **OK** para salvar as alterações e fechar a janela.

Abrir Após selecionar um item na lista, clique em **Abrir** para ver ou modificar este item. Para acrescentar um novo item, clique em **NOVO** item na lista e clique em **Abrir**.

Atualizar Clique em **Atualizar** para acessar novamente os dados do firewall e exibi-los novamente no painel.

Remover Clique em **Remover** para excluir um item selecionado da lista. Esta ação só removerá o item da lista. Esta ação não terá nenhum efeito em outros lugares onde este item estiver definido.

Selecionar Clique em **Selecionar** para acessar uma lista de itens candidatos válidos para esta função.

Topo Clique em **Topo** para ir para o topo de um painel.

Campos Comuns

Campos comuns que você verificará em muitas caixas de diálogo de cliente de configuração são:

Saída A medida que o comando que você iniciou progride, informações de progresso serão exibidas aqui.

Nome	Fornece um nome para este item. Este nome de item deve ser exclusivo para esta função em particular no firewall. O nome NÃO deve conter um símbolo de canalização (|), aspas simples (ou apóstrofo) ('), ou aspas duplas(") pois estes caracteres são utilizados como SMIT e delimitadores de arquivo. O uso destes caracteres poderá resultar em dados não-confiáveis.
Descrição	Este campo é opcional e é fornecido caso você queira fornecer um comentário ou uma informação adicional sobre este item.

Recursos Exclusivos

Há diversos recursos exclusivos do cliente de configuração dos quais deve estar ciente.

Para cliente de configuração do Windows 95 ou do Windows NT, o cliente de configuração parece melhor com resolução mínima de 1024 pixels x 768 pixels.

Se você mantiver pressionado o botão esquerdo do mouse para continuar em um controle de rotação e, acidentalmente, arrastar o mouse sem liberar o botão do mouse, o controle de rotação continua. Para pará-lo, clique em uma das setas de direção do controle de rotação com o botão esquerdo do mouse.

Se você conectar-se ao Firewall duas ou mais vezes em sucessão rápida utilizando SSL, a conexão será recusada. Saia e reinicie o cliente de configuração.

Capítulo 5. Guia Inicial do IBM Firewall

Este capítulo descreve as etapas básicas de configuração necessárias para se obter a configuração do IBM Firewall. Ele explica como definir uma interface protegida, como determinar sua norma de segurança e como definir objetos da rede.

Etapas Básicas de Configuração

Para obter uma configuração básica do IBM Firewall:

1. Planeje sua configuração do IBM Firewall. Decida as funções do firewall que deseja utilizar e como deseja utilizá-las o quanto antes. Estas seções são de grande utilidade:

   - Capítulo 1, “Introdução ao IBM Firewall” na página 1
   - Capítulo 2, “Planejamento” na página 7
   - “Considerações de Planejamento” na página 53

2. Informe ao Firewall quais de suas interfaces estão conectadas a redes protegidas. Você necessita ter uma interface protegida e uma não-protegida para que o firewall possa funcionar corretamente. Na árvore de navegação do cliente de configuração, abra a pasta Administração do Sistema e clique em **Interfaces** para ver uma lista de interfaces de rede no firewall. Para alterar o status de segurança de uma interface, selecione uma interface e clique em **Alterar**. Consulte “Designação de Sua Interface de Rede” na página 24 para maiores informações.

   Se você vai conectar-se à Internet, entre em contato com o seu ISP para obter um endereço IP registrado para a interface não-protegida do Firewall.

3. Configure as normas gerais de segurança acessando o diálogo **Normas de Segurança** na pasta Administração do Sistema. Para obter configurações típicas do Firewall:

   - Permitir consultas DNS
   - Negar mensagem de difusão para interfaces não-protegidas
   - Negar Socks para adaptadores não-protegidos

   Consulte “Utilização do Cliente de Configuração para Definir um Regulamento de Segurança” na página 25 para maiores informações.

4. Configure seu serviço de nome de domínio e o serviço de correspondência. Acesse estas funções a partir da pasta de Administração do Sistema na árvore de navegação do cliente de configuração. Primeiro leia Capítulo 6, “Manuseio do Serviço de Nome de Domínio” na página 31.

5. Defina elementos-chave da(s) rede(s) para o firewall utilizando a função **Objetos da Rede** na árvore de navegação do cliente de configuração. A função Objetos da Rede controla o tráfego através do Firewall. Defina os seguintes elementos-chave como objetos da rede:

   - Interface Protegida do Firewall
   - Interface Não Protegida do Firewall
   - Rede Protegida
   - Cada sub-rede em sua rede protegida

- Um objeto de rede do host para seus servidores de SDI e seus servidores de domínio NT, se apropriado

Consulte o “Objetos de Rede” na página 27 para maiores informações.

6. Ativar serviços do Firewall. São os métodos pelos quais os usuários de rede protegida podem acessar a rede não-protegida (como socks ou proxy). Os serviços que serão implementados vão depender de decisões tomadas no

protegida, utilize as regras do filtro expert para negar ou permitir acesso entre as diversas sub-redes na mesma interface com base no endereço IP ou uma máscara de endereço.

Para designar interfaces protegidas e não-protegidas, utilize a pasta Administração do Sistema na árvore de navegação do cliente de configuração. Todas as interfaces (adaptadores) conhecidas serão exibidas e identificadas como protegidas ou não-protegidas.

Para poder executar a filtragem específica de interface, é necessário fornecer um nome para cada interface.

Para identificar uma interface de rede como protegida ou não-protegida:

1. Selecione uma interface e clique em **Alterar**.
2. Quando necessário, repita.
3. Clique em **Fechar**.

Para identificar a interface como protegida ou não-protegida e para fornecer um nome significativo para esta interface, clique em **Abrir**. Este nome será usado pelos filtros para especificar filtragem de interface.

Utilização do Cliente de Configuração para Definir um Regulamento de Segurança

Uma das primeiras coisas a se considerar ao configurar o IBM Firewall é o regulamento geral de segurança para sua instalação.

O IBM Firewall apresenta um quadro de diálogo para auxiliá-lo na configuração do seu regulamento de segurança, conforme ilustrando na Figura 8 na página 26.

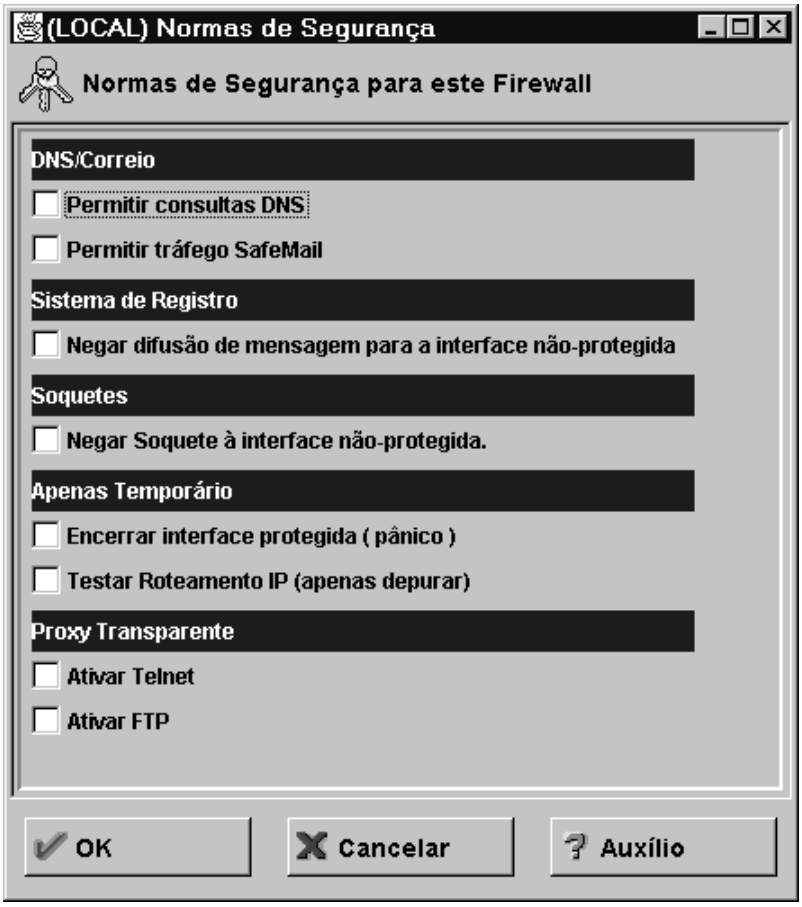


Figura 8. Norma de Segurança

Clique em Auxílio para aprender mais sobre o painel de regulamento de segurança.

O Regulamento de Segurança consiste numa maneira rápida e fácil para administradores estabelecerem regulamentos coletivos para o firewall. A maioria dos quadros de opções exibidos na janela de normas de segurança oferecem um modo rápido de seleção de certos Serviços Pré-definidos que se aplicarão a todo o tráfego de rede recebido pelo Firewall. As exceções são as opções do Proxy Transparente, que servem simplesmente para ativar ou desativar o Telnet e o FTP Transparente.

Quando você selecionar uma norma de segurança, o Firewall cria as regras do filtro, as quais você então necessita ativar. O Firewall ativa os serviços selecionados nesta janela e torna-os globalmente disponíveis.

Observe que sempre que selecionar um quadro de opção pertencente a um Serviço Pré-definido e clicar em **OK**, é necessário ativar estas alterações através da janela Ativação da Conexão. Não é necessário ativar as seleções do Proxy Transparente, pois estas não pertencem aos Serviços Pré-definidos. Consulte “Serviços Pré-definidos” na página 63 para obter uma lista de serviços pré-definidos.

A seguinte lista de quadros de opções é apresentada e a partir dela você pode selecionar atributos que refletem o regulamento de segurança para o seu site. Os

atributos selecionados aplicam-se a todos os endereços em ambos lados do IBM Firewall.

- Selecione **Permitir consultas DNS** para permitir pedidos de resolução e respostas do Serviço de Nomes de Domínio.
- Selecione **SafeMail** para permitir o fluxo do tráfego de correspondência no Firewall.
- Selecione **Negar difusão de mensagem para a interface não-protegida** para impedir que difusões de mensagens sejam recebidas pela porta não-protegida. Se a interface não-protegida do firewall estiver conectada à Internet, esse serviço pode contribuir para reduzir a quantidade de registros no Firewall.
- Selecione **Negar Soquetes à interface não-protegida** para impedir que tráfego de soquetes entre no Firewall a partir da rede não protegida.
- Selecione **Encerrar a interface protegida (pânico)** para impedir qualquer tráfego para e a partir do Firewall nas interfaces protegidas. Somente utilizado em casos de emergência.
- Selecione **Testar Roteamento IP (apenas depurar)** para permitir todo tráfego para e a partir do Firewall em qualquer interface. Observe que se o valor deste quadro de opção for alterado, é necessário salvá-lo clicando em **OK** e ativá-lo através da janela Ativação da Conexão. **O uso deste Serviço pode expor o Firewall, comprometendo sua segurança. Utilize-o com muito cuidado.**
- Selecione **Ativar Telnet** para permitir Telnets Proxy Transparentes.
- Selecione **Ativar FTP** para permitir FTPs Proxy Transparentes.

Objetos de Rede

Objetos de rede são representações de componentes que já existem em sua rede como hosts, redes, roteadores, redes privadas virtuais ou usuários. Objetos de rede designam endereços de origem e destino dos serviços quando as conexões são criadas.

Objetos podem ser identificados pelo nome, representação de ícone, tipo e descrição. Há diversos tipos de objetos de rede, porém Host e Firewall são os mais comuns. O objeto de rede padrão enviado com o IBM Firewall é "O Mundo". Este é um objeto global que abrange todos os endereços de IP possíveis. Depois de preencher as planilhas de configuração da rede (consulte “Planilha de Planejamento da Configuração da Rede” na página 8), você está pronto para criar objetos.

Você pode criar objetos individuais ou de grupo. Todos os objetos de rede são definidos por um endereço IP e uma máscara de endereço (máscara da sub-rede) para que seja possível um objeto representar uma faixa de endereços de rede.

Utilização do Cliente de Configuração para Definir Objetos de Rede

Para definir um único objeto de rede, selecione **Objetos de Rede** a partir da árvore de navegação do cliente de configuração. O quadro de diálogo Objetos de Rede aparece. Dê um clique duplo em **NOVO**. O quadro de diálogo **Incluir um Objeto de Rede** é exibido, como mostrado em Figura 9 na página 28.

Figura 9. Incluir Objeto de Rede

1. Forneça o tipo do objeto. Clique sobre a seta **Tipo do Objeto** para ver os tipos de objeto que você pode criar. Por questões de desempenho, é melhor criar objetos de tipo de rede ao invés de objetos de tipo de host. Os tipos de objeto que você pode criar são:
   - Host - um nó em particular da rede com uma máscara de 255.255.255.255.
   - Rede - uma série coletiva de endereços de rede, caracterizada por uma faixa de endereço e uma máscara de sub-rede específica.
   - Firewall - uma única máquina com um firewall instalado com uma máscara de 255.255.255.255. Somente um objeto de rede do firewall pode ser o destino de um túnel IBM ou manual.
   - Roteador - um host que encaminha o tráfego entre duas ou mais redes com uma máscara de 255.255.255.255.
   - Interface - um adaptador de rede em uma máquina com um máscara de 255.255.255.255. Não precisa ser adaptador do Firewall.
2. Preencha o nome do objeto.
3. Preencha a descrição. Este campo é opcional.
4. Forneça um endereço de IP com ponto decimal para este objeto.
5. Forneça um máscara de sub-rede que especifique os bits no endereço para comparar ao endereço do pacote IP.
6. Clique em **OK**.

Grupos de Objeto de Rede

Um grupo representa um conjunto de objetos de rede. Os grupos são utilizados como uma conveniência na configuração de conexões e podem eliminar o trabalho repetitivo. Um exemplo seria agrupar alguns endereços, individualmente representados por objetos de rede, em um grupo de objetos de rede para representar um departamento. Este departamento pode ser utilizado como o endereço de origem ou destino de uma conexão.

Para definir um grupo de objetos de rede, selecione Objetos de Rede a partir da árvore de navegação do cliente de configuração. O quadro de diálogo **Objetos de Rede** é exibido. Dê um clique duplo em **NOVO GRUPO**. O quadro de diálogo **Definir Objeto de Rede** é exibido.

1. Forneça o nome do grupo.
2. Forneça uma descrição. Este campo é opcional.
3. Clique em **Selecionar** para selecionar objetos para o grupo.
4. Clique em **OK**.

Dica: É recomendável incluir séries de endereços contíguos em um único objeto de rede sempre que possível. Isto melhora o desempenho do processamento da regra de conexão. O seguinte exemplo ilustrará isto.

```
DEPARTAMENTO DE CONTABILIDADE
   Kevin's machine  191.1.10.1
   Susan's machine  191.1.10.3
   Helen's machine  191.1.10.5
   Peter's machine  191.1.10.7
   Bob's machine    191.1.10.9
```

Para criar um objeto de rede para este departamento de contabilidade, você forneceria as informações do endereço IP para este grupo da seguinte forma: 191.1.10.0 com uma Máscara de Sub-rede de: 255.255.255.0. Este objeto de rede, departamento de contabilidade, pode ser utilizado como a origem ou destino de uma conexão.

Realização de uma Cópia de Segurança da Configuração do Firewall

O Firewall armazena todos os seus arquivos de configuração no `ROOTDIR\config`. Caso deseje efetuar a cópia de segurança da sua configuração do firewall sem incluir todos os arquivos do Firewall, faça uma cópia de segurança do conteúdo inteiro do diretório `ROOTDIR\config`.

Caso deseje restaurar uma configuração do Firewall que possui cópia de segurança, elimine todos os arquivos existentes no diretório `ROOTDIR\config` e depois restaure as versões com a cópia de segurança dos arquivos. Será necessário regenerar e ativar as regras de filtro para que a configuração restaurada entre em vigor.

Os arquivos principais da configuração do firewall estão relacionados abaixo. É possível que o diretório `\config` do seu Firewall não contenha todos os arquivos relacionados aqui. Observe que embora a maioria dos arquivos de configuração do firewall sejam arquivos de texto simples que podem ser visualizados com um editor de texto, **a edição manual destes arquivos não é suportada**.

- carriers.cfg - Definições da operadora do pager
- cfgfilt.output
- explode.cfg
- filters.active - Indica se a filtragem está ativa
- fwadpt.cfg - Definições para interfaces de rede
- fwconfig.map - Contém nomes de arquivo de configuração
- fwconns.cfg - Definições de conexões do filtro

- fwfilters.cfg - Filtros atualmente ativos
- fwhttp.cfg - Configuração proxy HTTP
- fwmail.conf - Configuração do SafMail
- fwobjects.cfg - Definições de objetos de rede
- fwpolicy.cfg - Opções de Normas de Segurança
- fwrules.cfg - Definições do gabarito de regras do filtro
- fwservices.cfg - Definições de serviços
- fwsocks.cfg - Regras Socks 5 do cliente de configuração
- fwtdefn.conf - Definições de alerta
- fwtpproxy.cfg - Definições do proxy transparente
- fwusrdb.cfg - Banco de dados do Usuário Firewall
- logmgmt.cfg - Definições do arquivo compactado
- modems.cfg - Definições do modem
- pager.cfg - Definições do pager
- rcsfile.cfg - Parâmetros do Serviço de Configuração
- Socks5.conf - arquivo de configuração do Socks 5 gerado
- Socks5.header.cfg - Porções fornecidas pelo usuário do Socks5.conf gerado
- syslog.conf - Definições do recurso do log

Firewall, esse pedido seria encaminhado a um domínio DNS não protegido e, mais uma vez, nenhuma informação sensível seria divulgada.

Configuração do DNS Utilizando o Cliente de Configuração

Para configurar o DNS, selecione Administração do Sistema a partir da árvore de navegação do cliente de configuração. Dê um clique duplo sobre o ícone da pasta de arquivo para expandir a exibição. Selecione **Serviços de Nome de Domínio**. O IBM Firewall exibe a atual configuração DNS, que pode ser modificada.

Figura 11. Serviço de Nome de Domínio

Nota: Ao incluir o DNS, o firewall salva e renomeia qualquer arquivo de configuração existente do serviço de nome de domínio.

1. O campo **Nome de Domínio Protegido** identifica o nome de domínio que o Firewall vai anexar a todos os nomes não qualificados de host.
2. O campo **Servidor de Nome de Domínio Protegido** refere-se ao servidor que resolve nomes e endereços IP do host protegido a partir da Internet pelo IBM Firewall. Pode-se digitar endereços IP decimais com pontos, separados por espaços.
3. O campo **Servidor de Nome de Domínio Não-Protegido** refere-se ao(s) servidor(es) fornecido(s) pelo provedor de serviços para resolver informações sobre rede não protegida. Pode-se digitar endereços IP decimais com pontos, separados por espaços.

Nota: Quando um servidor de nome é inicializado, ele envia uma consulta para obter a lista dos nomes de servidor raiz. Quase todas as implementações conservam essa lista na memória. A implementação da Microsoft, porém, grava a lista no arquivo de configuração. Com isso, o comportamento do servidor de nome não é modificado, mas os valores exibidos no campo **Servidor de Nome Não-Protegido** sofrem alteração. Não há, porém, motivo para preocupação.

Configuração do Servidor de Nomes Protegidos

O servidor de nomes protegido tem que ser configurado de modo a enviar as consultas não resolvidas no Firewall. Quem tem a implementação BIND padrão deve incluir uma instrução *forwarders* e uma instrução *cache* no arquivo de *boot* do servidor de nomes protegido:

```
forwarders      aaa.bbb.ccc.ddd
cache           .               named.cache
```

Crie o arquivo de cache, *named.cache*, para apontar para o Firewall:

```
. 99999999 IN NS firewall.private.com
firewall.private.com   99999999 IN A aaa.bbb.ccc.ddd
```

sendo que *private.com* é o nome de domínio usado a partir do lado protegido e *aaa.bbb.ccc.ddd* são os endereços de IP do Firewall.

Além disso, pode ser interessante colocar o nome do host do firewall nos bancos de dados DNS. Dessa forma os usuários podem acessar o servidor de Soquetes, o proxy HTTP, o proxy Telnet e o proxy FTP do Firewall usando o nome do host em vez de usar seus endereços de IP. Para isso são necessários dois passos a mais, como descreve o *Capítulo 4* do *DNS e BIND*. Veja mais detalhes sobre esse manual na *Bibliografia*.

Primeiro acrescente um registro A no arquivo de banco de dados do domínio:

```
firewall.private.com     IN A aaa.bbb.ccc.ddd
```

Depois coloque um registro PTR no arquivo de consulta invertida:

```
ddd.ccc.bbb.aaa.in-addr.arpa.   IN PTR  firewall.private.com.
```

Não sendo usado o DNS para a rede protegida, o firewall deverá continuar sendo capaz de resolver suas próprias informações. Configure o firewall da forma descrita para o caso normal, mas coloque a interface protegida do firewall no campo **Servidor de Nome Protegido**. Acrescente então a seguinte linha ao `c:\winnt\system32\dns\boot`.

```
primary ccc.bbb.aaa.in-addr.arpa c:\winnt\system32\dns\fwnamed.rev
```

Crie então o *fwnamed.rev* de modo a ficar parecido com:

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9        ; Serial
                          86400    ; Atualizar após 1 dia
                          300      ; Repetir após 5 minutos
                          654000   ; Expirar após 1 semana
                          3600  )  ; TTL mínimo de 1 dia
ccc.bbb.aaa.in-addr.arpa.          IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.   IN PTR  firewall.private.com.
```

Configurando os Clientes Protegidos

Os clientes da rede protegida precisam ser configurados para enviar suas consultas ao servidor de nomes protegido, não ao Firewall. Isso é importante porque garante que nenhuma informação do lado protegido fica armazenada na memória cache do Firewall. E também poupa carga de trabalho sobre o Firewall,

uma vez que ele não vai envolver-se, a menos que uma consulta envolva o encaminhamento de consulta do lado protegido para o lado não protegido.

Não sendo usado o DNS para a rede protegida, os clientes terão que apontar para o Firewall como seu servidor de nomes.

Publicação de Serviços para o Público

Muitas empresas desejam publicar serviços em particular para o público da Internet. Muitas vezes, esses serviços incluem e-mail e servidores de Web, embora possa ser usado qualquer tipo de servidor TCP/IP. A fim de garantir a oferta de tais serviços, é preciso não apenas colocar o servidor na rede em que ele vai poder ser alcançado, como será preciso listar o servidor com o DNS público, para que os usuários possam obter a informação certa.

Isso pode ser feito de duas maneiras. Ou o provedor de serviços vai fornecer a lista dos servidores como parte do domínio deles (e assim dos servidores de nome deles) ou você fornece seu próprio servidor de nomes e o registra na Internet. É muito mais fácil que o ISP (Provedor de Serviços da Internet) forneça esse serviço para você. Se for essa a opção escolhida, será preciso fornecê-los com os nomes de host e endereços de IP que deverão aparecer na lista. Se, por exemplo, você opera seu servidor de web público como *www.public.com*, cujo endereço IP é *50.100.150.200*, é preciso pedir ao ISP que liste *www.public.com at 50.100.150.200*.

Além disso, para receber e-mail, é preciso pedir ao ISP que liste seu firewall como *permutador de correspondência* de seu domínio de e-mail público. O ISP precisa saber qual é o nome do host *(gateway.public.com)* seu endereço IP *(50.100.150.201)*, além do nome de domínio pelo qual a correspondência será recebida *(public.com)*.

Se seu ISP não estiver disposto a fornecer-lhe esses serviços, você mesmo terá que fazê-lo. Aqui, de novo, há duas opções a mais. Pode-se colocar um servidor de DNS no DMZ ou usar o próprio firewall como servidor de nomes. Usar o firewall não implica riscos de segurança adicionais, porque os arquivos do banco de dados a serem colocados lá não contêm nenhuma informação sobre sua rede protegida. A única informação que vai ser armazenada vai pertencer aos serviços públicos que forem escolhidos para serem oferecidos.

Os detalhes sobre a configuração de um servidor DNS podem ser encontrados no Capítulo 4 do *DNS e BIND*, que consta da *Bibliografia*. A leitura desse capítulo é altamente recomendada, assim como a dos capítulos anteriores a ele, se necessário. Configurar um servidor de DNS não é tarefa trivial e em geral é melhor deixá-la a cargo de especialistas no assunto. Quem conhece algum deve pensar seriamente em pedir auxílio a ele.

Consulte “Exemplos de Configurações” na página 35 para maiores informações.

Instalação do DNS Server da Microsoft

Para instalar o DNS Server da Microsoft, vá para o painel de controle, clique em **Rede**, clique no **item Serviços**, clique em **Incluir** e selecione **Microsoft DNS Server**. Você precisará do CDROM de instalação.

Diagnóstico de Problemas do DNS

A *Referência ao IBM eNetwork Firewall* possui um capítulo sobre diagnóstico de problemas no Firewall. Nele há uma seção específica que trata de problemas do DNS. Lá se encontram sugestões sobre o uso do comando *nslookup* para identificar o segmento do sistema do DNS que está apresentando problemas.

Exemplos de Configurações

Esta seção ilustra alguns exemplos de configuração nas quais um firewall pode ser distribuído. A maioria dos exemplos está focalizada na configuração necessária para operação DNS. É pouco provável que um destes exemplos ilustre sua rede, então analise cuidadosamente cada exemplo para aplicar os conceitos adequados para sua instalação em particular.

Exemplo 1: Servidor DNS em um DMZ na Interface Não Protegida

O primeiro exemplo ilustra os arquivos necessários para operar o servidor de nome em um DMZ que se encontra dentro da rede não protegida, conforme mostrado na Figura 12.

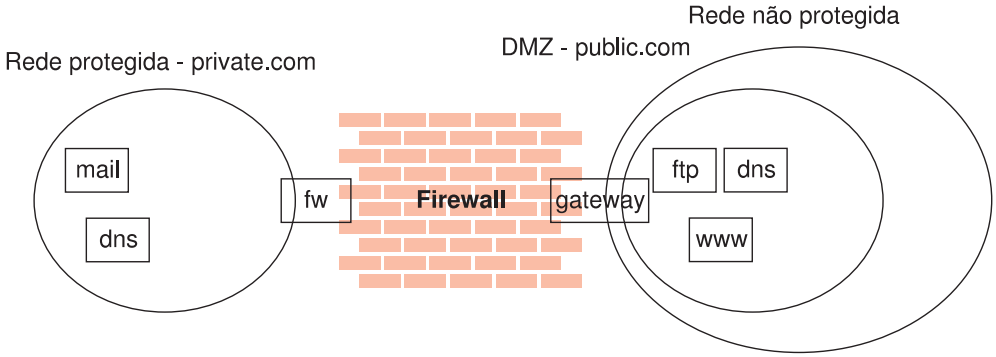


Figura 12. Servidor de nome no DMZ Dentro da Rede Não Protegida

Esta figura ilustra uma rede privada, *private.com*, por trás de um IBM Firewall cuja interface protegida é chamada de *fw.private.com* e cuja interface não protegida é chamada de *gateway.public.com*. O DMZ da empresa é anexado à interface não protegida e contém um servidor de nome *dns.public.com*, um servidor FTP *ftp.public.com* e um servidor web *www.public.com*. Os arquivos no *dns.public.com* para implementar este panorama são os seguintes:

db.public

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; número serial
                 10800       ; atualizar após 3 horas
                  3600        ; tentar novamente após 1 hora
                 604800      ; expirar após 1 semana
                 86400  )    ; TTL mínimo de 1 dia
;
; Servidores de nome
;
public.com           IN NS  dns.public.com.
;
; Hosts no DMZ
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; Entradas relacionadas ao Mail
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

db.50.100.150

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; número serial
                 10800       ; atualizar após 3 horas
                 3600        ; tentar novamente após 1 semana
                 604800      ; expirar após 1 semana
                 86400  )    ; TTL mínimo de 1 dia
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

db.127.0.0

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; número serial
                 10800       ; atualizar após 3 horas
                 3600        ; tentar novamente após 1 semana
                 604800      ; expirar após 1 semana
                 86400  )    ; TTL mínimo de 1 dia
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

db.cache

A melhor opção para este arquivo é efetuar o FTP na lista atual de servidor de nome raiz a partir de *ftp://ftp.rs.internic.net/domain/named.root*.

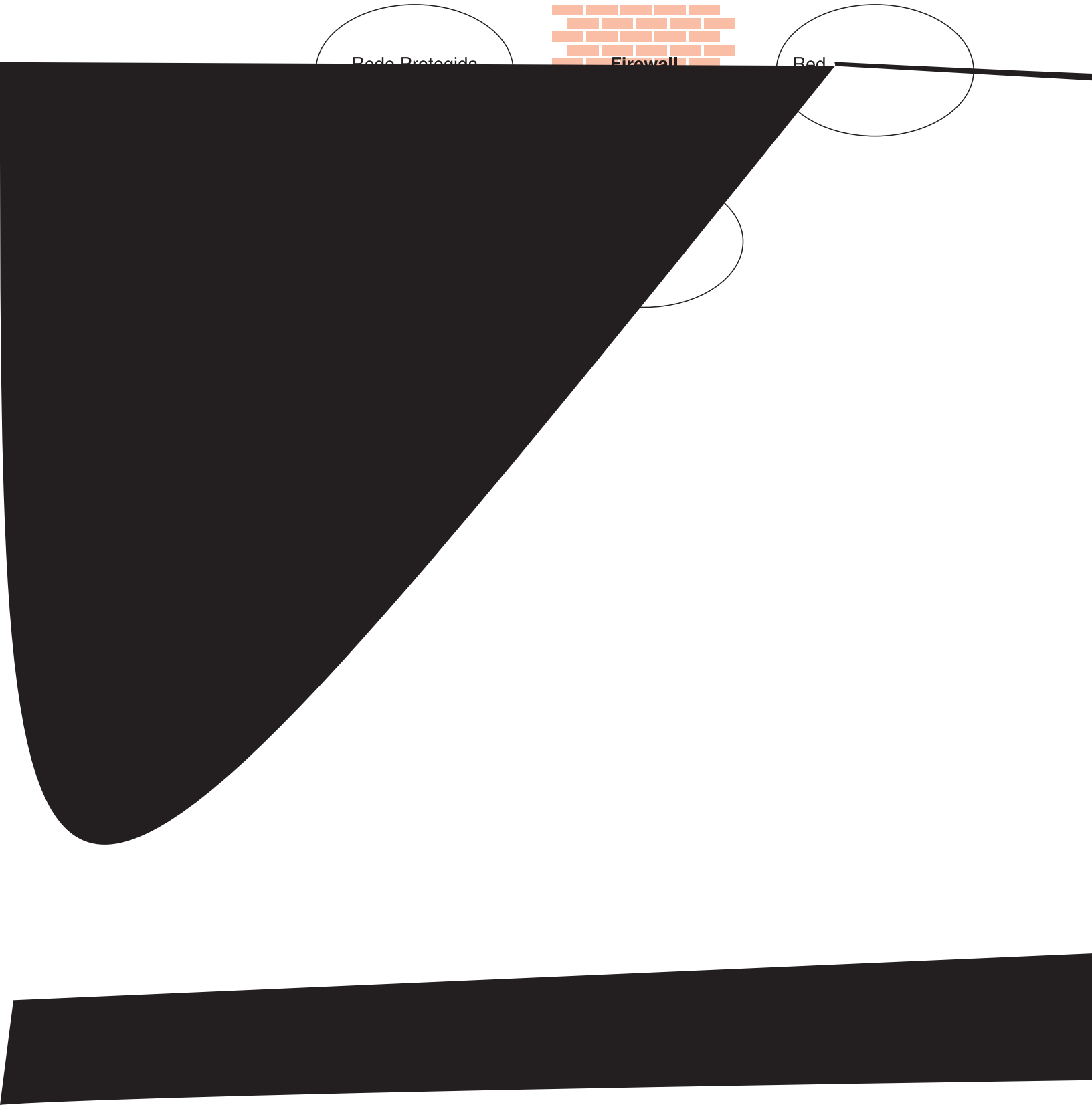
boot

```
primary public.com                  db.public
primary 150.100.50.in-addr.arpa     db.50.100.150
primary 0.0.127.in-addr.arpa        db.127.0.0
cache   .                           db.cache
```

Para definir o filtro de tráfego para que permita o tráfego DNS adequado, ative *Permitir Consultas DNS* no painel **Norma de Segurança**.

Exemplo 2: DNS em um DMZ dentro de uma Interface Dedicada

No segundo exemplo, o DNS para o DMZ ainda está em um servidor de nome dedicado, mas desta vez o DMZ está anexado a uma interface distinta ao invés da mesma interface da rede não protegida.



Para ativar a transferência de zona, acrescente as seguintes linhas no arquivo *boot* do Firewall no `c:\winnt\system32\dns`:

```
secondary public.com     50.100.150.202 db.public
secondary 150.100.50.in-addr.arpa  50.100.150.202 db.50.100.150
```

Depois vá até o Gerenciador de Controle de Serviço, pare e reinicie o serviço do Servidor DNS.

Exemplo 3: Utilização do Firewall como Servidor de Nome Protegido

Para utilizar o Firewall como o servidor de nome protegido, coloque os arquivos de banco de dados que normalmente residiriam no servidor protegido, no Firewall. Assim, seus clientes podem indicar o Firewall como o servidor DNS. Os riscos associados a esta abordagem são que o servidor DNS não pode diferenciar um pedido do lado protegido de um pedido do lado não protegido. Desta forma, ele fornecerá estas informações do lado protegido a qualquer cliente que solicitar; você não poderá mais ocultar suas informações DNS.

Para implementar esta abordagem, comece configurando o recurso DNS do Firewall utilizando o cliente de configuração. Para o campo *Nome de Domínio Protegido*, forneça o nome de domínio que será utilizado em sua rede protegida. Para o *Servidor de nome Protegido*, liste a interface protegida do Firewall. Para o *Servidor de nome Não Protegido*, liste o servidor de nome fornecido pelo seu ISP, como habitualmente. Depois, você deve criar um arquivo de consulta reversa no Firewall para suplementar esta configuração.

Crie o arquivo `c:\winnt\system32\dns\fwnamed.rev` para que se pareça com o seguinte exemplo.

Para este exemplo, a interface protegida do Firewall é chamada de *fw.private.com* e seu endereço IP é *10.100.100.1*.

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                  1           ; número serial
                  10800       ; atualizar após 3 horas
                  3600        ; tentar novamente após 1 semana
                  604800      ; expirar após 1 semana
                  86400  )    ; TTL mínimo de 1 dia
1.100.100.10.in-addr.arpa.        IN NS fw.private.com.
1.100.100.10.in-addr.arpa.        IN A  fw.private.com.
```

Em seguida, acrescente a seguinte linha no `c:\winnt\system32\dns\boot`:

```
primary 100.100.10.in-addr.arpa     fwnamed.rev
```

Neste panorama, seus clientes devem estar configurados para indicar o Firewall (10.100.100.1) como servidor DNS. Seu Firewall irá comparecer com a resolução de informações externas, mas não haverá resolução de informações do lado protegido. Isto significa que qualquer cliente do lado protegido, que desejar conectar-se ao servidor de configuração ou qualquer um dos servidores proxy no Firewall, deve referir-se ao Firewall pelo endereço IP, não pelo nome do host.

Capítulo 7. SafeMail

O gateway do IBM Firewall SafeMail é um gateway para tráfego SMTP. Ele transmite mensagens do(s) mailserver(s) protegido(s) para o lado não-protegido, ocultando, ao passar, nomes de domínio sensíveis. Ele transmite mensagens do lado não-protegido para o domínio de correspondência protegido e isola a rede protegida contra ataques.

Embora não faça exibição na tela do conteúdo, o SafeMail oferece uma saída de usuário pela qual a exibição na tela pode ser efetuada. Para saber mais detalhes, consulte o “Saída de Usuário do SafeMail” na página 41.

O SafeMail transmite mensagens em tempo real do emissor para o receptor. Assim são evitados os riscos e a complexidade envolvidos na manutenção de uma fila de mensagens no Firewall. Para isso são necessários certos requisitos de configuração nos domínios de correspondência adjacentes. Em alguns casos, tais requisitos não serão praticáveis para uma instalação em particular. Em situações assim, qualquer um dentre os diversos servidores SMTP pode ser adquirido separadamente e instalado no lugar do SafeMail. Quem optar por instalar um servidor SMTP completo deverá configurá-lo tendo a segurança em mente. Consulte “Utilização de um Servidor SMTP no lugar do SafeMail” na página 42 para maiores informações.

Configuração do SafeMail Utilizando o Cliente de Configuração

Para configurar o SafeMail, selecione Administração do Sistema a partir da árvore de navegação do cliente de configuração. Dê um clique duplo sobre o ícone da pasta de arquivo para expandir a exibição. Selecione **SafeMail**. O IBM Firewall exibe a lista dos servidores e domínios de correspondência configurados. É preciso configurar uma entrada para cada domínio de correspondência do lado privado que está sendo configurado.

1. Para incluir um domínio, selecione **NOVO** e clique em **Abrir**. Aparece a caixa de diálogo **Incluir Servidor de Correspondência**.
2. O campo **Nome do Domínio Protegido** contém o nome pelo qual o domínio de correspondência descrito é conhecido pelos usuários no lado protegido do firewall.
3. O campo **Nome do Servidor de Correspondência Protegido** contém o nome do host ou o endereço IP com pontos decimais do servidor de correspondência ao qual a entrada se aplica. Este servidor deverá ser uma das redes protegidas. Só é possível listar um mailserver para um determinado domínio.
4. O campo **Nome do Domínio Público** contém o nome através do qual o domínio de correspondência descrito é conhecido pelos usuários no lado não protegido do firewall. Este nome será substituído no lugar do nome de domínio protegido, para ocultar a topografia da rede protegida.
5. Clique em **OK**.

Alteração de Entrada de Configuração de Correspondência

Para alterar uma entrada de configuração de correspondência, selecione-a na lista e clique em **Abrir**. Aparece a caixa de diálogo **Alterar Configuração do Servidor de Correspondência**.

O campo **Nome do Domínio Protegido** está desativado, mas os outros campos podem ser modificados, como está descrito em “Configuração do SafeMail Utilizando o Cliente de Configuração” na página 39.

Notas:

1. Caso tenha configurado anteriormente o SafeMail protegido e especificar aqui um servidor de correspondência protegido, este servidor de correspondência substituirá o que foi configurado anteriormente.
2. Se o SafeMail *não* tiver sido configurado antes e for especificado um servidor de correspondência protegido aqui, ele será acrescentado à configuração.

Eliminação de Entrada de Configuração de Correspondência

Para eliminar uma entrada de configuração do SafeMail, selecione-a na lista e clique em **Eliminar**. Um aviso de eliminação será exibido. Clique em **OK** para eliminar ou **Cancelar**, caso mude de idéia.

Configuração dos Servidores Protegidos

É preciso configurar os servidores de correspondência protegidos de modo que eles mostrem o Firewall como gateway de domínios desconhecidos. Assim a correspondência destinada à rede não protegida é encaminhada ao Firewall. Além disso, cada servidor deve ser configurado de modo a aceitar mensagens endereçadas tanto ao seu nome de domínio público como ao seu nome de domínio privado. Quando o Firewall encaminha uma nota da rede não protegida, todos os receptores são listados com seus nomes de domínio do lado público.

Quem tem mais de um domínio de correspondência distinto individual dentro de sua rede protegida deve também configurar cada servidor para que a correspondência destinada a outro domínio do lado protegido seja encaminhada diretamente ao esse servidor, não ao Firewall. Isso retira do Firewall carga de trabalho desnecessária e permite que seu mecanismo de distribuição em tempo real funcione da maneira correta.

Configuração do Domínio Público

A única configuração necessária na rede não protegida é que o Firewall seja listado como permutador de correspondência da rede. Peça a seu provedor de serviços que inclua as informações necessárias para isso em seus servidores de DNS. Veja no Capítulo 6, “Manuseio do Serviço de Nome de Domínio” na página 31 as especificações adicionais relativas aos mecanismos aí envolvidos.

O objetivo é listar o Firewall como *permutador de correspondência* para cada nome de domínio público para o qual se quer aceitar correspondência. Quem usa, por exemplo, o nome de domínio *private.com* dentro de sua rede protegida e *public.com* fora dela deve denominar o firewall como *gateway.public.com*. Em casos assim, peça a seu fornecedor que liste o nome de host e os endereços IP

do Firewall como host (que normalmente será listado com registros "A" e "PTR"). Depois, para aceitar correspondência endereçada a *userÃpublic.com*, peça ao provedor para incluir um registro MX no domínio *public.com*, que lista *gateway.public.com* como permutador de correspondência desse domínio. Para receber também correspondência endereçada a *userÃsomethingelse.com*, liste um registro MX a mais apontando também para o Firewall.

Saída de Usuário do SafeMail

O SafeMail oferece uma saída de usuário pela qual a instalação pode adaptá-lo para rejeitar tráfego potencialmente prejudicial. Consulte o *IBM eNetwork Firewall Reference* para obter uma descrição detalhada do Kit de Desenvolvedores de Software fornecido para esta finalidade.

Esse recurso permite criar uma função, a *UsrCheck()*, que é chamada toda vez que o SafeMail recebe pacote do emissor. A função recebe numa estrutura que contém vários campos relacionados ao estado do sistema. Tal estrutura possui uma ID de sessão única, os endereços IP dos servidores emissores e receptores, indicadores para comandos recebidos antes e um buffer de texto simples contendo o pacote que está sendo analisado.

Alguns dos tipos de verificação que podem ser implementados nessa função são:

- listas de hosts *proibidos*
- varredura de seqüências de caracteres não permitidas, como linguagem não-apropriada ou nomes de código de projeto
- exame de cadeias entre aspas embutidas
- restrições quanto ao tamanho da mensagem

Se desejado, a saída de usuário também pode ser usada para implementar uma interface para produto de exibição na tela do conteúdo de outros fabricantes.

Se a função de saída de usuário decidir que uma mensagem não deve ser processada, a função retornará um código de motivo ao SafeMail. O SafeMail vai imediatamente rejeitar a conexão com o servidor SMTP emissor. Ao mesmo tempo, será gravada uma mensagem no log do firewall que inclui o código de motivo retornado pela saída de usuário.

Ao gravar saída de usuário, tenha em mente que essa função é chamada para cada pacote recebido. Tome cuidado para escrevê-la da maneira mais efetiva possível, para evitar causar impacto negativo sobre o desempenho do sistema. Lembre-se também de que essa função vai rodar em ambiente multi-tarefa e que, conseqüentemente, deve ser escrita de maneira que seja compatível com a presença de tarefas. A saída de usuário pode ser escrita com qualquer compilador que suporte operação multi-tarefa e pode usar a convenção de ligação *_cdecl*. São fornecidos arquivos de amostra para o IBM Visual Age C++ e para o Microsoft Visual C++.

Utilização de um Servidor SMTP no lugar do SafeMail

Desativação do SafeMail

Para desativar o SafeMail a fim de evitar conflitos com outro produto de servidor SMTP, desative o funcionamento do SafeMail em **Gerenciador de Controle dos Serviços**. No menu **Iniciar** do Windows, selecione **Definições, Painel de Controle, Serviços**. Desloque a tela para selecionar *Servidor de SafeMaid do IBM Firewall*. Clique em **Inicialização**. No campo **Tipo de Inicialização**, selecione **Desativado**. Clique em **OK**.

Configuração de um Servidor SMTP

É preciso considerar diversos aspectos ao instalar um servidor SMTP completo no lugar do SafeMail. Esta seção explica os recursos de segurança do SafeMail, na tentativa de permitir a configuração do servidor SMTP de modo a desempenhar funções similares. Certos produtos de servidor SMTP podem não conseguir desempenhar algumas dessas tarefas e portanto estude as opções disponíveis e suas necessidades cuidadosamente antes de adquirir o produto.

Há certos ataques que tentam estourar ou danificar a fila de correspondências. Embora não haja servidor inteiramente ampliado capaz de operar sem fila de correspondência, os riscos associados a ela são reduzidos quando um volume de disco é dedicado exclusivamente a essa tarefa. As chances de que a fila estourada cause impacto sobre outras operações do firewall são reduzidas.

Também é importante que o servidor de correspondência oculte informações sobre a rede protegida. De acordo com as regras do SMTP, todo servidor que encaminha uma peça de correspondência deve inserir uma linha de cabeçalho *Recebido:*. Ela vai pode ser usada por atacantes para mapear sua rede protegida. O SafeMail retira todos esses cabeçalhos ao processar a nota; configure o servidor SMTP para fazer o mesmo. O SafeMail também reescreve todos os nomes de host do lado privado para o nome de domínio público. Com isso são removidas ainda mais informações que poderiam ser usadas para mapear a rede.

Saída do Sistema de Logs para o SafeMail

Eis a seguir um exemplo de saída do sistema de logs para o SafeMail.

```
Fev 03 13:46:11 1998 mr16n18: ICA2163i: safemaild iniciado.

Fev 03 13:41:14 1998 mr16n18: ICA2177i: Conexão do SafeMail 0xd71e7a19
recebida de RACK3BD.
Fev 03 13:41:21 1998 mr16n18: ICA2179i: SafeMail encaminhou 215575
bytes para a conexão 0xd71e6118 de 9.67.144.52 para 9.67.131.250.
Fev 03 13:41:21 1998 mr16n18: ICA2178i: Sessão do SafeMail 0xd71e7a19
estabelecida de 9.67.144.52 para 9.67.131.250.
Fev 03 13:41:23 1998 mr16n18: ICA2177i: Conexão do SafeMail 0xd71e831a
recebida de RACK3BD.
Fev 03 13:41:36 1998 mr16n18: ICA2177i: Conexão do SafeMail 0xd71e901b
recebida de RACK3BD.
Fev 03 13:41:56 1998 mr16n18: ICA2179i: SafeMail encaminhou 215567
bytes para a conexão 0xd71e7a19 de 9.67.144.52 para 9.67.131.250.
Fev 03 13:41:56 1998 mr16n18: ICA2178i: Sessão do SafeMail 0xd71e831a
estabelecida de 9.67.144.52 para 9.67.131.250.
Fev 03 13:41:56 1998 mr16n18: ICA2178i: Sessão do SafeMail 0xd71e901b
estabelecida de 9.67.144.52 para 9.67.131.250.
Fev 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail encaminhou 346
bytes para a conexão 0xd71e901b de 9.67.144.52 para 9.67.131.250.
Fev 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail encaminhou 358
bytes para a conexão 0xd71e831a de 9.67.144.52 para 9.67.131.250.
```

As mensagens de log indicam o seguinte:

- ICA2177 - indica o início de uma nova conexão.
- ICA2179 - indica um término bem sucedido.
- ICA2178 - indica que o contato foi estabelecido com o servidor SMTP de recepção.
- ICA2181 - indica que o SafeMail rejeitou a sessão. Consulte o *IBM eNetwork Firewall Reference* para obter os códigos de motivo.
- ICA2180 - indica o final da sessão.
- ICA2182 - indica que a saída de usuário decidiu que a sessão deve ser rejeitada.

Capítulo 8. Controle do Tráfego Através do Firewall

Este capítulo informa como utilizar o cliente de configuração para controlar tráfego de rede através do Firewall. Usando filtros expert, o firewall filtra pacotes no nível de sessão baseado em critérios múltiplos tais como hora do dia, endereço IP e sub-rede. O filtro age entre as interfaces de rede protegida e não protegida. Eles não têm impacto sobre as tabelas de roteamento do firewall.

Por padrão, o Firewall não permite qualquer tráfego entre a rede protegida e não protegida. Você deve criar conexões para permitir que tipos específicos de tráfego fluam entre as redes protegida e não protegida.

Utilização do Cliente de Configuração para Criar Conexões

Os componentes do cliente de configuração ilustrados na Figura 14 na página 46 são utilizados para criar objetos de rede, gabaritos de regra, serviços e conexões.

Conexões Associe objetos de rede a serviços e/ou gabaritos de soquetes para definir os tipos de comunicação permitidos entre as extremidades. Cada conexão define um tipo específico de tráfego IP a ser permitido ou negado entre um objeto de rede de origem e destino.

Serviços São criados de um ou mais gabaritos. Define o tipo de tráfego IP que é permitido ou negado entre um objeto de origem e de destino. Por exemplo, você poderia construir um serviço para permitir Telnet e negar Ping. (Um dos serviços FTP consiste em oito gabaritos de regras). O IBM Firewall vem com um conjunto de serviços padrão. Estes serviços pré-carregados padrão não podem ser eliminados, mas alguns campos podem ser modificados. No entanto, se estes serviços pré-definidos não satisfizerem suas necessidades, você pode acrescentar serviços utilizando os gabaritos de regras para criar novas regras. Consulte “Definição de Serviços” na página 65 para maiores informações.

Gabaritos de Regra Fornecem instruções ao Firewall para permitir ou negar pacotes IP com base em seus vários atributos.

Gabaritos de Soquetes
Fornecem instruções ao daemon de soquetes do firewall para permitir ou negar pacotes IP com base em seus vários atributos.

Objetos de Rede Representam os diversos componentes de rede, tais como sistemas centrais, usuários e sub-redes, que interagem com o Firewall. Eles são definidos por um endereço IP e uma máscara de endereço, então é possível que um objeto represente uma faixa inteira de endereços de rede. Objetos de rede podem ser agrupados.

Grupos de Objeto de Rede
Representam um ou mais objetos de rede. Eles são utilizados como aparelhos úteis na configuração de conexões e podem eliminar o trabalho repetitivo. Um exemplo seria

agrupar vários endereços em um grupo de objetos de rede para representar um departamento. Este grupo de objetos de rede pode ser usado como a origem ou destino de uma conexão.

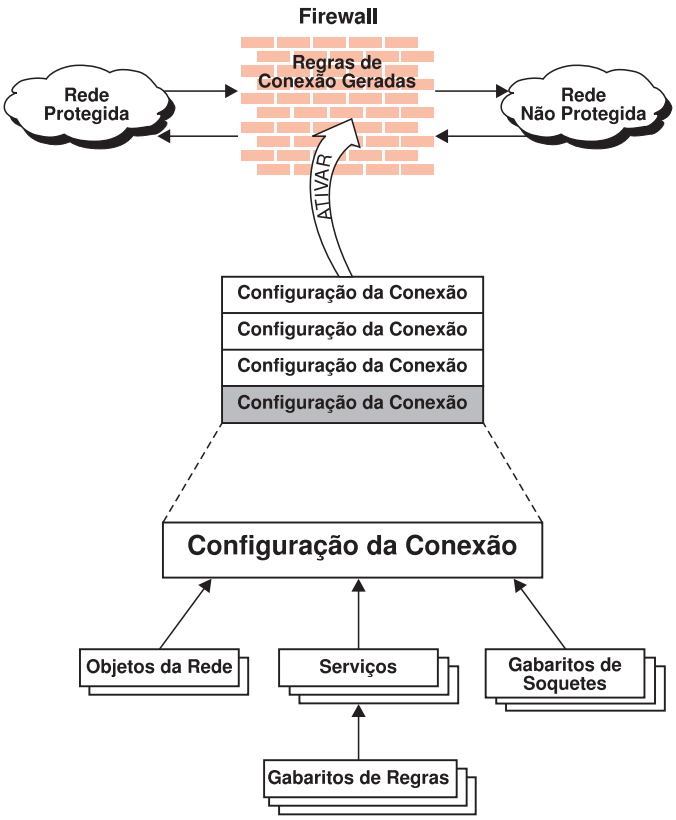


Figura 14. Criação de Conexões

Criação de Conexões Utilizando os Serviços Pré-definidos

A fim de permitir ou negar tipos específicos de comunicações entre dois objetos de rede nomeados, ou grupos de objeto de rede que servem como extremidades, você necessita criar uma conexão.

Depois de definir seus objetos de rede, você criará conexões. Selecione um objeto de rede ou grupo para ser a origem e outro objeto de rede ou grupo para ser o destino do fluxo de tráfego pelo Firewall.

Para criar uma conexão, selecione Controle de Tráfego a partir da árvore de navegação do cliente de configuração e dê um clique duplo sobre o ícone da pasta do arquivo para expandir a exibição. Selecione **Configuração da Conexão**. O quadro de diálogo **Lista de Conexões** é exibido. Selecione **NOVO** e clique em **Abrir**. O quadro de diálogo **Incluir Conexão** é exibido, como mostrado em Figura 15 na página 47.

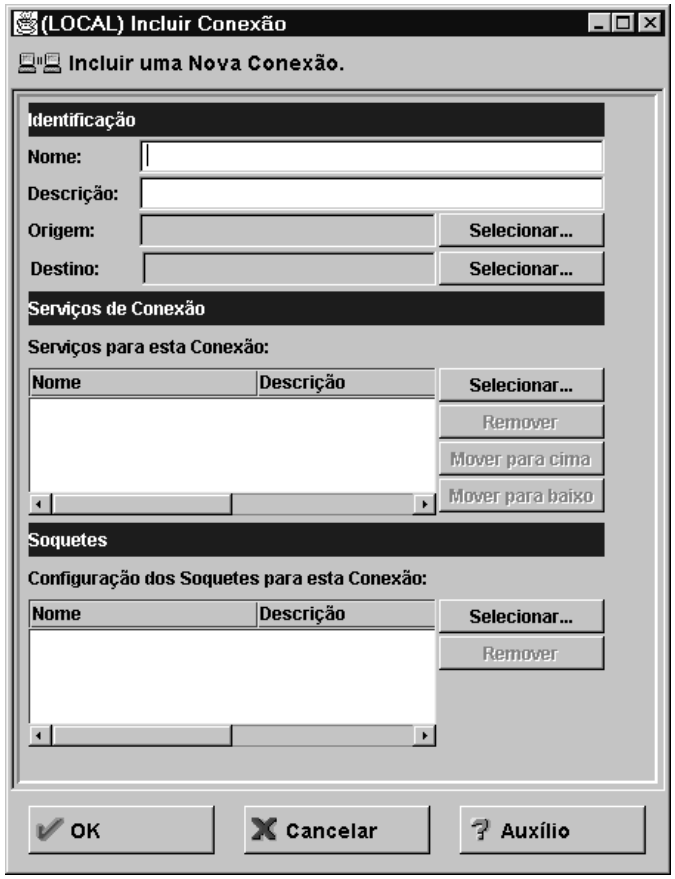


Figura 15. Incluir uma Conexão

1. Preencha com um nome para a conexão.
2. Forneça uma descrição da conexão.
3. Para o campo origem, clique em **Selecionar** e escolha um objeto de rede da lista de diálogos **Objeto de Rede**.
4. Para o campo de destino, clique em **Selecionar** e escolha um objeto de rede da lista de diálogos **Objetos de Rede**.
5. Para escolher os serviços para esta conexão, clique em **Selecionar** e escolha o tipo de tráfego que deseja controlar entre as extremidades.
6. Escolha um ou mais serviços da lista para incluir o serviço na Conexão.
7. Você pode reorganizar a lista selecionando um serviço e clicando em **Mover para cima** ou **Mover para baixo**. Consulte “Organização de Conexões” na página 48.
8. Você pode remover um serviço selecionando-o e clicando em **Remover**.
9. Utilize **Configuração dos Soquetes para esta Conexão**. Siga as etapas de 5–7 para efetuar conexões dos Soquetes.
10. Depois que tudo estiver definido, clique em **OK**.
11. Ative todas as suas conexões. Consulte “Ativação de Conexão” na página 48.

Organização de Conexões

A maioria do usuários do IBM Firewall possuem menos de 1000 regras. Quanto mais regras se tem, maior o impacto sobre o desempenho.

Quando é recebido um pacote em uma interface de rede, entrando ou saindo do host do firewall, regras são aplicadas começando pelo topo das regras de conexão geradas. Quando as informações do pacote correspondem exatamente às informações em uma regra, a ação (permitir ou negar) é desempenhada. Se o arquivo inteiro for pesquisado sem que se encontre um correspondente, o pedido é negado.

Dica: Coloque as conexões mais específicas mais próximas do topo e as menos específicas mais próximas da base. Por exemplo, você poderá ter um Departamento ABC, com um endereço de (1.1.10.X) e um máquina que é utilizada como servidor dentro do Departamento ABC, com um endereço de (1.1.10.7). Se deseja excluir a máquina 1.1.10.7 porque é um servidor que não deverá ser utilizado para o tráfego telnet, coloque a conexão `Negar telnet para servidor do Dept ABC` antes das conexões `Permitir telnet para Dept ABC`. Se a ordem das conexões for invertida, a conexão para negar nunca será encontrada.

Ativação de Conexão

Nota: Antes de ativar suas conexões, certifique-se de que sua interface protegida está definida.

Selecione **Ativação da Conexão** a partir da árvore de navegação do cliente de configuração para efetuar um dos seguintes procedimentos:

Regenerar Regras de Conexão e Ativar O Firewall cria as regras de conexão geradas a partir da configuração de conexão e ativa aquele conjunto de regras.

Desativar Regras de Conexão O Firewall agora está protegido pelas regras padrão.

Listar Regras de Conexão Atuais Exibe o conjunto de regras de conexão mais recentemente criado. Se você desativou regras anteriormente, elas não estão sendo usadas.

Validar Geração de Regras As regras que você criou são válidas ou inválidas.

Ativar o Sistema de Registro O Firewall registra o tráfego selecionado para o recurso do `sistema de registro do firewall`.

Desativar o Sistema de Registro Interrompe o sistema de registro do Firewall.

O quadro de diálogo **Ativação da Conexão** é exibido, como mostrado na Figura 16 na página 49.

Figura 16. Ativação da Conexão

Depois de efetuar uma seleção, clique em **Executar**.

Exemplo de Saída de Registro ao Gerar Novamente e Ativar Regras de Conexão

Segue abaixo o exemplo de uma saída de registro quando ele é gerado novamente e as regras da conexão são ativadas.

```
Feb 03 13:46:53 1998 mr16n18: ICA9037i: Interfaces do Firewall sendo atualizadas
automaticamente na Terça Fev  3 13:46:53 1998.

Feb 03 13:46:55 1998 mr16n18: ICA1032i: Regras do filtro atualizadas às
13:46:55 em Fev-03-1998

Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp gt  1023 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 gt  1023 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:4 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp     gt  1023 eq 25 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:5 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp/ack eq  25 gt 1023 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:6 permit 9.67.144.49 255.255.255.240
9.67.130.154 255.255.248.0 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:7 permit 9.67.130.154 255.255.248.
0 9.67.144.49 255.255.255.240 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:8 permit 9.67.144.49 255.255.255.240
9.67.131.250 255.255.255.255 tcp     gt  1023 eq  21 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:9 permit 9.67.131.250 255.255.255.255
9.67.144.49 255.255.255.240 tcp/ack eq  21 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:10 permit 9.67.131.250 255.255.255.
255 9.67.144.49 255.255.255.240 tcp     eq  20 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:11 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp/ack gt  1023 eq  20 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:12 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp     gt  1023 gt  1023 secure local inbound
l=n f=y t=0 e=none a=none
.
.
.
Feb 03 13:46:58 1998 mr16n18: ICA1037i: #:100 deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
all any 0 any 0 both both both l=y f=y t=0 e=none a=none
```

Determinação dos Estados das Regras

As regras do IBM Firewall podem se encontrar em um destes estados:

1. A configuração não está ativa.

   Você ainda não utilizou o cliente de configuração para ativar a configuração ou você desativou a configuração. Este é o estado da configuração assim que você instalar o IBM Firewall pela primeira vez e reinicializar seu sistema ou desativar regras de filtragem. Filtros padrões estão no lugar para proteger sua rede de intrusos assim que você instalar o Firewall.

   Acesso ao Firewall:

   - A configuração de filtro padrão permite todo o tráfego de entrada local e permite todo tráfego de saída.

2. A configuração está ativa mas possui erros.

Capítulo 9. Exemplos de Serviços

Este capítulo descreve como configurar o Firewall para que ele execute algumas tarefas comuns. As tarefas relacionadas são apenas exemplos, mas depois de compreender estas, você deverá conseguir configurar o seu firewall para utilização de qualquer serviço fornecido.

Considerações de Planejamento

O controle de tráfego do Firewall é organizado de acordo com as conexões que definem os tipos de comunicação que são permitidos ou proibidos entre duas extremidades. Sendo assim, é crucial planejar sua conexões sob o aspecto destas extremidades.

Como descrito NO Capítulo 8, “Controle do Tráfego Através do Firewall” na página 45, extremidades são representadas no Firewall por objetos de rede. Caso ainda não o tenha feito, você deve preencher a planilha de planejamento da rede no Capítulo 2, “Planejamento” na página 7 e criar os objetos de rede necessários para representar sua rede.

Os exemplos neste capítulo utilizam os seguintes objetos de rede:

Interface Protegida A interface protegida do Firewall.

Interface Não-Protegida
A interface não protegida do Firewall.

Rede Protegida
A série de endereços que podem ser acessados através da interface protegida do Firewall. Isto poderia ser um grupo de objetos de rede que poderia conter diversos domínios distintos, cada um dos quais é representado por seu próprio objeto de rede.

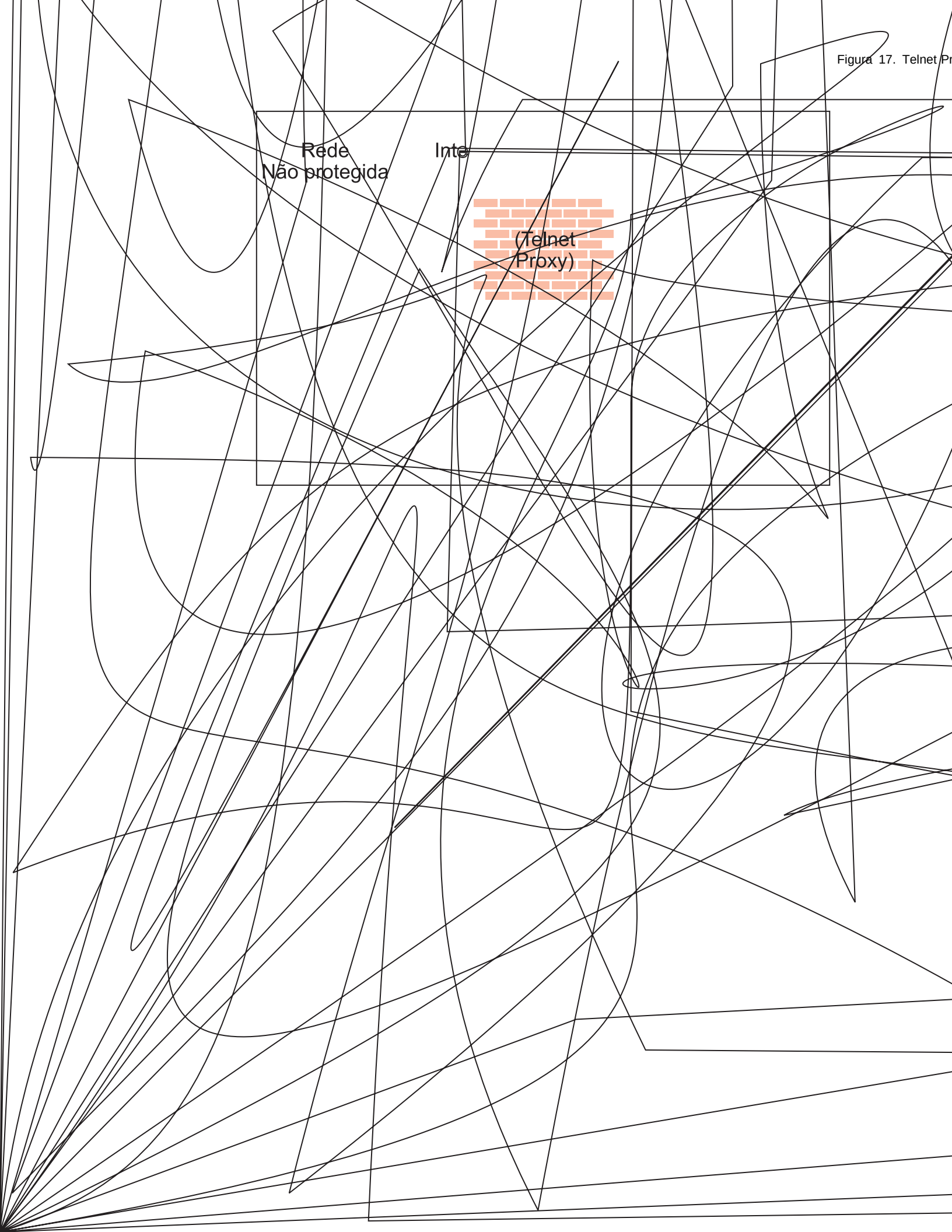
O Mundo A rede não protegida.

Cada tipo de comunicação desejado deve ser visto sob o aspecto da comunicação entre extremidades envolvidas. Neste estágio, considere se o seu firewall estará agindo como proxy com estas comunicações ou se o Firewall irá direcionar estas comunicações.

Se o firewall agir como um proxy, então o firewall irá realizar o trabalho necessário em nome do usuário protegido e os sistemas centrais nunca saberão que o sistema central protegido existe. Se o firewall direcionar o tráfego, então o host protegido e o host não protegido se comunicarão diretamente um com o outro.

Se você for utilizar o Firewall como um proxy, então as extremidades de sua comunicação irão incluir o firewall, conforme ilustrado na Figura 17 na página 54.

Figura 17. Telnet Pr



Tabe	*ado*	
Obje	**Objeto de Destino**	**Serviços Necessários**
Rede	O Mundo	Saída direta Telnet

Esta co , conforme observado anteriormente, expor os endereços de seus cli los à medida que se conectam a hosts não protegidos.

Exemplo de Proxy HT

A maioria ções deseja que pelo menos alguns de seus clientes protegido urfar na Web. O IBM Firewall oferece um serviço direto de saída HT ido para possibilitar o HTTP direcionado, que funciona exatamen xemplo do Telnet filtrado. Além disso, o Firewall fornece um proxy HT

O protocol diferente do Telnet no que se refere a poder encapsular outros pro esmo para o surf simples, a maioria dos usuários irá precisar não apena mas também de serviços FTP. Para oferecer a amplitude total da fun , Gopher e WAIS também devem ser permitidos, embora estes sejan s com bem menos freqüência.

Ainda assim que quando estes protocolos adicionais são utilizados, eles são empaco HTTP entre o cliente e o proxy. Sendo assim, a comunicação seria semelh diagrama na Figura 18.Figura 18. Proxy HTTPComo temos dois pares de e

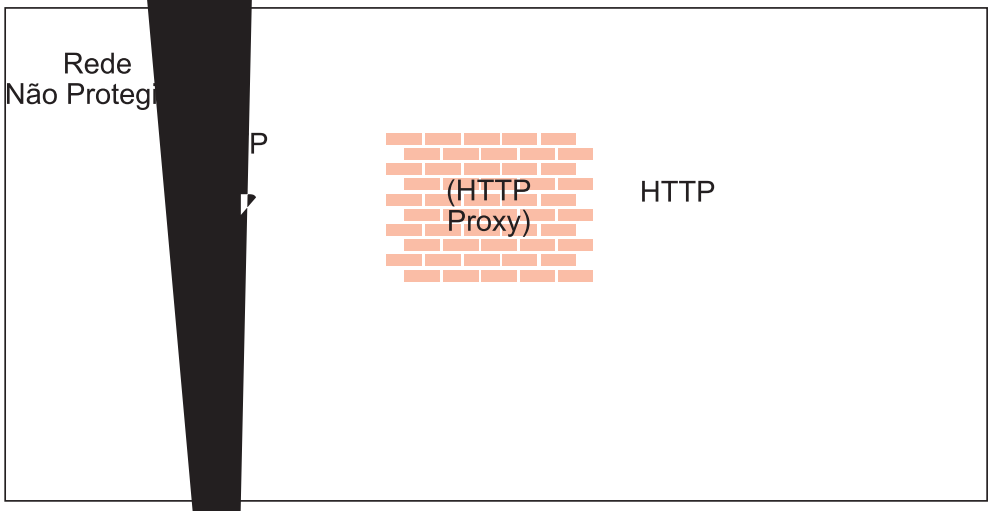


Tabela 3. Proxy HTTP		
Objeto Fonte	**Objeto de Destino**	**Serviços Necessários**
Rede Protegida	Interface Protegida	Proxy HTTP de saída 1/2
Interface Não-Protegida	O Mundo	Selecione a partir de... • HTTP proxy de saída 2/2 • FTP proxy de saída 2/2 • Gopher proxy de saída 2/2 • WAIS proxy de saída 2/2 • HTTPS proxy de saída 2/2

Para maiores informações sobre o Proxy HTTP, consulte Capítulo 13, “Configuração de Servidores Proxy” na página 89.

Exemplo de Socks

Os Soquetes apresenta um desafio semelhante àquele do proxy HTTP no qual o daemon dos soquetes manipula diferentes protocolos e os encapsula em um único fluxo de dados entre o Firewall e o cliente. Os Soquetes são mais flexíveis que o proxy HTTP porque ele pode conciliar qualquer protocolo orientado por TCP ou UDP e porque o Firewall pode ser configurado independentemente dos filtros para futuramente controlar comunicações.

Devido a esta flexibilidade adicionada, a configuração de socks requer uma terceira conexão além daquelas demonstradas com o proxy HTTP. As duas conexões básicas irão permitir que os pacotes fluam para o Firewall e a partir dele; a terceira conexão é necessária para dizer ao daemon dos soquetes para efetuar o proxy nas solicitações assim que receber os pacotes.

Tabela 4. Socks		
Objeto Fonte	**Objeto de Destino**	**Serviços Necessários**
Rede Protegida	Interface Protegida	Socks 1/2
Interface Não-Protegida	O Mundo	Selecione a partir de... • HTTP proxy de saída 2/2 • FTP proxy de saída 2/2 • Telnet proxy de saída 2/2 (Qualquer segunda metade do serviço do proxy para o qual deseja fornecer suporte)
Rede Protegida	O Mundo	Na janela Configuração do Socks, selecione a partir de... • permitir HTTP socksified • permitir FTP socksified • permitir Telnet sockisfied

Certamente, os clientes dentro de sua rede protegida devem ser socksified e devem ser configurados para utilizar o seu firewall como o servidor de socks deles.

Para maiores informações sobre Socks, consulte Capítulo 11, “Configuração do o Servidor de Socks” na página 69.

Dicas para o DNS

Muita pouca comunicação ocorrerá de modo eficiente se a resolução DNS não for fornecida. Consulte Capítulo 6, “Manuseio do Serviço de Nome de Domínio” na página 31 para obter detalhes sobre a configuração DNS. Não se esqueça de ativar "Permitir Consultas DNS" em seus Regulamentos de Segurança.

Dicas para Clientes Socks Não-Protegidos

O painel Regulamentos de Segurança contém um quadro de opção para **Negar Soquetes para interface não protegida**. Este serviço irá rejeitar qualquer pacote endereçado ao daemon do socks de qualquer interface não-protegida e tornará o seu firewall muito mais seguro.

Caso deseje que clientes entrem em sua rede a partir da rede não protegida, você *não deve* ativar este quadro de opção.

Capítulo 10. Personalização do Controle de Tráfego

Este capítulo auxilia na definição de regras e serviços do filtro. Serviços são uma coleção de regras ou um conjunto de instruções destinadas a permitir ou negar um determinado tipo de tráfego pelo Firewall - por exemplo uma sessão de telnet. Pode-se acrescentar serviços a ele por meio dos gabaritos de regras para criar novas regras. É possível também excluir serviços. Serviços de Soquetes aplicam-se a conexões com soquetes.

O IBM Firewall vem pré-carregado com um conjunto-padrão de serviços. Você pode adaptar qualquer serviço pré-definido de acordo com suas necessidades particulares ou criar novos serviços.

Utilização do Cliente de Configuração para Criar Gabaritos de Regras

Utilize este procedimento para incluir uma nova regra na lista de gabaritos de regras disponíveis.

1. A partir da árvore de navegação do cliente de configuração, selecione Controle de Tráfego e dê um clique duplo sobre o ícone da pasta de arquivos. Selecione **Gabaritos da Conexão** e depois **Regras**.
2. Na caixa de diálogo **Lista das Regras**, de um clique duplo em **NOVO**.

   O IBM Firewall exibe uma caixa de diálogo **Incluir Regra de IP**, como mostra o Figura 19, para que a regra possa ser definida.

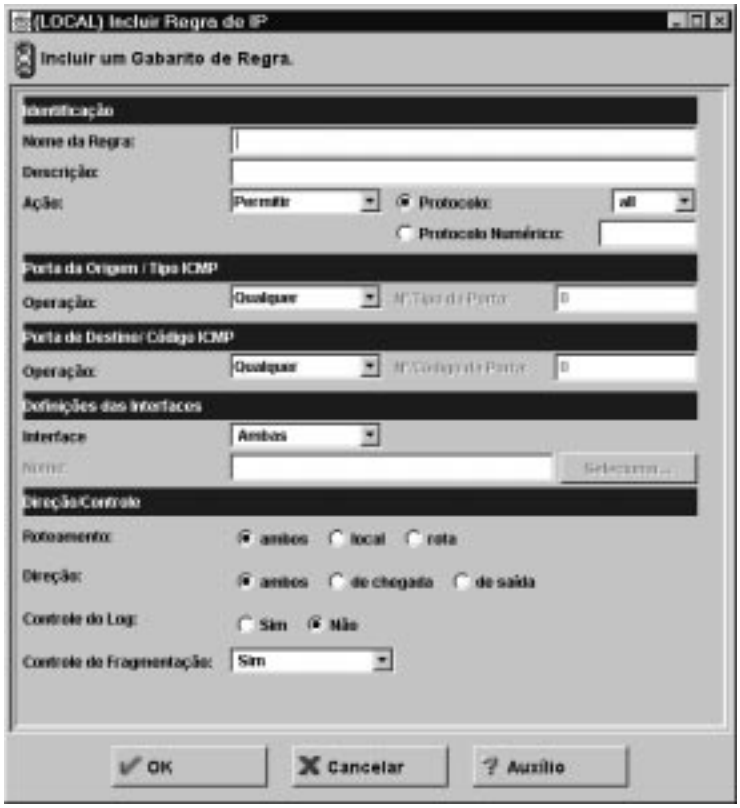


Figura 19. Incluir Regra de IP

3. Forneça um Nome de Regra.
4. Forneça a Descrição da Regra. Este campo é opcional.
5. Clique na seta de ação e escolha permitir ou negar acesso ao Firewall.
6. Clique na seta de protocolo e, na lista, selecione:

   Todos Qualquer protocolo será correspondente a esta regra.

   tcp O protocolo do pacote deve ser o TCP (Transmission Control Protocol) para corresponder a esta regra.

   tcp/ack O protocolo do pacote deve ser TCP com aviso de recebimento para corresponder a esta regra.

   udp O protocolo do pacote deve ser UDP (User Datagram Protocol) para corresponder a esta regra.

   icmp O protocolo do pacote deve ser o ICMP (internet control message protocolo) para corresponder a esta regra.

   ospf O protocolo do pacote deve ser ospf (open shortest path first) para corresponder a esta regra. Quando ele é especificado como protocolo, a operação e o valor da porta de origem são usados para o valor do tipo de registro do ospf. A filtragem também pode ser feita no tipo ospf. Um valor de tipo **qualquer** pode ser especificado e os campos da porta de destino devem ser especificados como **qualquer 0**. Tudo mais será ignorado.

   ipip O protocolo do pacote deve ser IPIP (IP-in-IP) para corresponder a esta regra. Quando IPIP é especificado, os campos da porta devem ser especificados como **qualquer 0**.

   esp O protocolo do pacote deve ser o protocolo de segurança de encapsulação, usado pela rede privada virtual para enviar pacotes de IP encapsulados, para corresponder a esta regra.

   ah O protocolo de cabeçalho de autenticação é o protocolo de pacote utilizado pela rede privada virtual para enviar pacotes de IP que possuem um sinal de autenticação associado.
7. O protocolo numérico permite que você especifique um protocolo através da utilização de seu valor decimal (de acordo com o RFC-1700). Os valores válidos estão no intervalo de 1 a 252. Observe que os campos da porta dessa regra devem ser especificados como 0 (denotando qualquer porta) ao utilizar esta opção. Veja o RFC-1700 para obter uma lista de todos os protocolos. Ou você pode acessar o Internet Assigned Numbers Authority (IANA) diretamente com um navegador.
8. Os operandos da operação e do número da porta são usados juntos. As operações de origem e lógicas denunciam uma relação entre o número da porta (destino ou origem) correspondente ao pacote e os operandos Porta nº de origem e Porta nº de destino. Se, por exemplo, a porta de destino do pacote é 20 e a operação de destino e a Porta nº de destino são “ge 15”, o pacote está de acordo com as regras. (20 é maior ou igual a 15).

   Quando se usa operação de origem ou de destino de valor **qualquer**, o filtro não observa o número da porta; qualquer porta serve. Neste caso, o número da porta não pode ser alterado.

Para o protocolo ICMP, ao invés de especificar uma porta de origem, especifique um tipo ICMP e no lugar de uma porta de destino, especifique um código ICMP. O operador lógico especificado é aplicado ao tipo ou código e, como no caso das portas, o operador qualquer significa que qualquer valor de tipo e/ou código está de acordo com a regra. Neste caso, o número da porta não pode ser alterado.

Os valores de operação são:

- Qualquer
- Igual a
- Diferente de
- Menor que
- Maior que
- Menor ou igual a
- Maior ou igual a

Eis algumas das portas mais importantes a serem protegidas. Os valores para os números de porta devem estar no intervalo de 1 a 65535:

Porta	**Use**
20	Dado FTP
21	Controle FTP
23	Telnet
25	Correio
53	Servidor do Nome de Domínio
70	Gopher
80	HTTP
111	RPC
161	SNMP
1080	socks

Eis alguns tipos e códigos ICMP:

Digite	**Código e Descrição**
0	0 - Resposta de ping
8	0 - Solicitação de ping
3	1 - Sistema central inacessível
3	3 - Porta inacessível
5	1 - Redirecionar para host

9. Clique na seta **Interface** para selecionar o tipo de interface (adaptador).

ambos	Para pacotes que vêm ou vão tanto pela interface protegida quanto pela não protegida
protegida	Para pacotes que vêm ou vão pela interface protegida
não-protegida	Para pacotes que vêm ou vão pela interface não-protegida
específica	Use com o campo de nome de interface quando selecionar uma interface, caso você tenha atribuído um nome à interface.

10. Se escolher o tipo de interface específica, o nome da interface específica irá aparecer no campo Nome.
11. Clique sobre o roteamento desejado:

    ambos Aplica-se a todos os tráfegos.

    local Implica que o pacote é local para o host do firewall. Isto significa que:

    - Pacotes locais de chegada são pacotes recebidos pela interface e destinados a este host do firewall; eles não serão encaminhados a outro host. Seu destino é local.
    - Pacotes de saída são transmitidos a partir da interface, mas são originários do host do firewall. Sua origem é local.

    rota Implica que o pacote é encaminhado pelo host do firewall. Isto significa que:

    - Pacotes de chegada locais são os recebidos pela interface e têm como destino algum outro host; eles não vão permanecer no Firewall. Seu destino é remoto.
    - Pacotes de saída são transmitidos a partir da interface, mas são originários de algum outro host. Sua origem é remota.
12. Selecione a direção desejada:

    ambos Para pacotes que saem do ou em direção à interface selecionada.

    chegada Para pacotes que chegam à interface selecionada vindos da rede

    partida Para pacotes que saem da interface selecionada em direção à rede
13. Quando se escolhe Sim no campo Controle de Log, todo pacote que obedece à regra é registrado no `log do firewall` com nível de prioridade `Erro`. Se este parâmetro não estiver especificado, o padrão é não.
14. Clique na seta **Controle do Fragmentação** para escolher o controle de fragmento desejado. Para que as informações do pacote IP correspondam a uma especificação de controle de fragmentação da regra, o controle é interpretado da seguinte maneira:

    Sim A regra irá corresponder a cabeçalhos de fragmentos, fragmentos e não-fragmentos. Para fragmentos, as informações de porta serão ignoradas e assume-se que são correspondentes.

    Apenas Somente fragmentos e cabeçalhos de fragmentos podem corresponder. Para cabeçalhos de fragmento, as informações da porta devem corresponder. Para fragmentos, as informações de porta serão ignoradas.

    Não Somente não-fragmentos podem corresponder. Cabeçalhos de fragmento e fragmentos são excluídos por este parâmetro.

    Cabeçalhos Somente não-fragmentos e cabeçalhos de fragmentos podem corresponder. Fragmentos são excluídos por este parâmetro.

    Se este parâmetro não estiver especificado, o padrão para as regras "permitir" e "negar" é Sim.

    Nota: Independente da definição deste controle, fragmentos IP com um deslocamento de um (1) serão descartados. Esta ação elimina um

ataque conhecido de se utilizar fragmentos do pacote para sobrepor sinalizadores do cabeçalho TCP.

Para que um cabeçalho do pacote corresponda a uma regra IP definida, as informações do pacote devem corresponder a todos os parâmetros especificados na regra codificada. Para fragmentos do pacote, todos os parâmetros exceto informações da porta são utilizados para determinar uma correspondência.

Se os fragmentos não tiverem sido permitidos por alguma regra anterior - que tinha Sim ou Apenas codificado - os fragmentos do pacote vão ser negados pela regra final que é sempre anexada ao final do arquivo de regras.

Alteração de Entrada da Configuração de Regra de IP

Para modificar uma regra de IP que você criou:

1. Dê um clique duplo numa regra que já existia na **Lista das Regras**. Aparece a caixa de diálogo **Modificar Regra do IP**.
2. Modifique os devidos campos, como descreve o Capítulo 10, “Personalização do Controle de Tráfego” na página 59, e clique em **OK** para aplicar as alterações.

Eliminação de Entrada de Configuração da Regra

Para excluir uma regra selecione uma regra da **Lista das Regras** e clique em **Excluir**.

Serviços Pré-definidos

O IBM Firewall vem pré-carregado com um conjunto-padrão de serviços. Serviços são uma coleção de regras ou um conjunto de instruções destinadas a permitir ou negar um determinado tipo de tráfego pelo Firewall - por exemplo uma sessão de telnet. Pode-se acrescentar serviços a ele por meio dos gabaritos de regras para criar novas regras.

Os serviços padrão pré-carregados são:

Tudo não-protegido Negar todo tráfego por interface não-protegida

Permitir tudo Permitir todo tráfego (apenas para fins de depuração)

Permitir tudo, em uma direção Permitir todo tráfego (apenas para fins de depuração)

Tudo protegido Negar todo tráfego na interface protegida (no caso de violação de segurança)

Encerrar tudo Negar todos os pacotes (encerrar ou depurar)

Anti Fraude Negar pacotes não protegidos de chegada com endereço de origem protegido

Transmissões Negar mensagens de transmissão para interface não protegida

Cliente Config não-protegido Permitir uso de cliente de configuração a partir de rede não protegida

Cliente Config protegido Permitir uso de cliente de configuração a partir de rede protegida

CU-SeeMe Vídeo CU-SeeMe nas portas padrão 7649 e 7648

Consultas DNS (SECURITY POLICY) Permitir consultas DNS

Transferências DNS Permitir transferências de zona DNS (para servidor de nome secundário)

Autenticação de Controlador de Domínio Permite usar o Controlador de Domínio para autenticação de usuário

Proxy FTP de chegada 1/2 Permitir FTP de chegada proveniente de rede não protegida para o Firewall

Proxy FTP de chegada 2/2 Permitir FTP de chegada do Firewall para rede protegida

Proxy FTP de saída 1/2 Permitir FTP de saída da rede protegida para o Firewall

Proxy FTP de saída 2/2 Permitir FTP de saída do Firewall para rede não protegida

Gopher proxy de chegada 2/2 Permitir gopher do Firewall para rede protegida

Proxy Gopher de saída 2/2 Permitir gopher do Firewall para rede não protegida

HTTP negar não-protegido Negar HTTP para interfaces não protegidas

HTTP direto de saída Permitir HTTP da rede protegida diretamente para rede não protegida

HTTP proxy de chegada 2/2 Permitir HTTP do Firewall para rede protegida

Proxy HTTP de saída 1/2 Permitir uso de porta de rede protegida para o Firewall

Proxy HTTP de saída 2/2 Permitir HTTP do Firewall para rede não protegida

HTTPS direto de saída Permitir HTTPS (SSL) de rede protegida para rede não protegida

Proxy HTTPS de saída 2/2 Permitir HTTPS (túnel SSL) do Firewall para rede não protegida

IDENTD Permitir identificação de usuário como protocolos Socks

Correio (SECURITY POLICY) Permitir Tráfego de correspondência pelo Firewall

Transmissões de Serviços de Nome NetBT Permite NetBIOS em transmissões de Serviços de Nome TCP/IP

Ping Permitir rede protegida de saída Ping para qualquer lugar

Autenticação SDI Permitir conexão ao servidor SecurID ACE na rede protegida

Socks 1/2 Permitir uso de soquetes de rede protegida para o Firewall

Socks negar não-protegido Negar soquetes de adaptadores não protegidos

Soquete de chegada 1/2 Permitir uso de soquetes de rede não protegida para o firewall

Telnet direto de saída Permitir conexão Telnet de rede protegida para rede não protegida

Proxy Telnet de chegada 1/2 Permitir Telnet de chegada da rede não protegida para o Firewall

Proxy Telnet de chegada 2/2 Permitir Telnet de chegada do Firewall para a rede protegida

Proxy Telnet de saída 1/2 Permitir Telnet de saída da rede protegida para o Firewall

Proxy Telnet de saída 2/2 Permitir Telnet de saída do Firewall para rede não protegida

VDOLIVE Direto de Chegada Permite que cliente não protegido use servidor protegido

Note que os usuários precisam configurar propriedades de tocador individual para usar apenas UDP porta 7001.

VDOLIVE Direto de Saída Permitir cliente protegido para servidor não protegido

Proxy WAIS de chegada 2/2 Permitir WAIS (z39.50) do Firewall para a rede protegida

Proxy WAIS de saída 2/2 Permitir WAIS (z39.50) do Firewall para a rede não protegida

Definição de Serviços

Depois de definir regras, é preciso inclui-las em serviços. Selecione Controle de Tráfego a partir da árvore de navegação do cliente de configuração e dê um clique duplo em Gabaritos da Conexão, depois selecione Serviços. A caixa de diálogo Lista de Serviços aparece. Dê um clique duplo em NOVO para obter a caixa de diálogo Incluir um Serviço, conforme ilustrado na Figura 20 na página 66.

Figura 20. Incluir Serviço

Utilização do Cliente de Configuração para Criar Serviços

1. Forneça o nome do serviço.
2. Forneça uma descrição.
3. O campo **Sobrepor o Controle de Log** consiste num meio de substituir a definição de controle do log nos gabaritos da regra que foram selecionados para esse serviço. Por exemplo, se você incluir um conjunto de gabaritos de regra que normalmente tem o conjunto de controle definido como não, você pode substituir esta definição por sim, para fins deste serviço. A definição de sobreposição terá efeito em todas as regras neste serviço. No campo **Sobrepor o Controle de Log**, digite uma das seguintes opções:
   - sem substituição - a substituição é desativada e ficam valendo as definições das próprias regras.
   - sim - grava um registro de log quando alguma regra neste serviço encontra correspondente
   - não - não grava um registro de log quando alguma regra neste serviço encontra correspondente

   Quando um registro de log é gravado para uma regra de filtro, os valores mostrados nele são os verdadeiros, fornecidos pelo pacote IP. Registrar regras de filtro casadas pode fornecer informações sobre o conteúdo dos pacotes de IP vistos pelo Firewall - por exemplo o protocolo e os números de porta verdadeiros.

4. O campo **Sobrepor o Controle de Fragmentação** consiste num meio de substituir a definição de Controle da Fragmentação nos gabaritos da regra selecionadas para esse serviço. Por exemplo, se você incluir um conjunto de gabaritos de regra que normalmente tem o conjunto de Controle de Frag. definido como não, você pode substituir esta definição por sim, para fins deste serviço. A definição de sobreposição terá efeito em todas as regras neste serviço. No campo Substituir Controle de Frag., forneça um dos seguintes:
   - sem substituição - a substituição é desativada e ficam valendo as definições das próprias regras.
   - sim - para casar com qualquer pacote de IP, como não-fragmentos, cabeçalhos de fragmento e fragmentos sem cabeçalho
   - não - para casar apenas com pacotes de não-fragmento e não casar com cabeçalhos de fragmento nem cabeçalhos sem fragmento
   - somente - para casar somente cabeçalhos de fragmento e fragmentos sem cabeçalho, não casar não-fragmentos
   - cabeçalhos - para casar somente não-fragmentos e cabeçalhos de fragmento, não casar fragmentos sem cabeçalho
5. Os controles de tempo permitem que você associe um intervalo de tempo para cada serviço. Assim, este serviço só será válido em um período de tempo especificado. Se não houver especificação de tempo para um serviço, este serviço será válido o tempo todo.

   Controlar por Hora do Dia Selecione se prefere que esse serviço fique ativado ou desativado de acordo com os horários de início e fim durante o dia. Use o formato de 24 horas. Se o campo não ficar ativado, os campos Hora do Dia ficarão valendo 24 horas por dia.

   Controle pelos Dias Selecione se prefere que o serviço fique ativado ou desativado de acordo com uma programação baseada em dias da semana ou em datas do calendário. Observe que a ativação ou não ativação do serviço depende do valor do campo Ação de Controle do Horário.

   Ação do Controle do Horário Escolha **Ativar Serviço Durante Horários Especificados** se quiser que o serviço fique ativado durante os horários especificados. O serviço será desativado durante todos os horários que não foram especificados.

   Escolha **Desativar Serviço Durante Horários Especificados** se quiser que o serviço fique desativado durante os horários especificados. O serviço ficará ativado durante os horários que não são os especificados.
6. Clique em **Selecionar** para escolher as regras que compõem o serviço.
7. Utilize o comutador Fluxo para determinar como os valores de Origem e Destino da Conexão devem ser atribuídos aos filtros à medida que são gravados no arquivo Básico de Regras.

```
---> Esquerda para direita indica que a Origem e Destino da
     Conexão serão gravados diretamente na regra da mesma maneira
     que foram gravados no arquivo Básico de Regras.

<--- Direita para esquerda indica que a Origem e o Destino da
     Conexão serão invertidos quando forem gravados no arquivo
     Básico de Regras.
```

8. Quando um pacote é recebido, o IBM Firewall compara as informações do pacote com as regras do arquivo de configuração das regras começando pelo topo do arquivo. Ele interrompe a comparação quando a primeira correspondência exata é encontrada e executa a ação contida na regra.

   Depois de acrescentar uma série de regras no serviço, a ordem em que elas estão pode ser alterada. Selecione uma regra na lista **Objetos do Serviço** e clique nos botões **Mover para cima** ou **Mover para baixo** para reposicionar a regra. Ou então exclua a regra clicando em **Remover**. O cliente de configuração exibe uma lista atualizada das regras. Clique em **OK** para salvar as alterações.

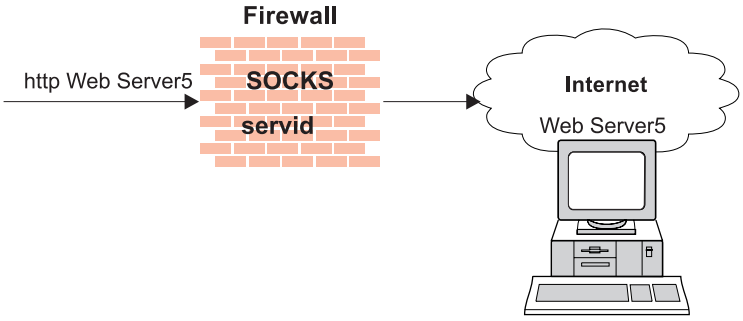
Capítulo 11. Configuração do o Servidor de Socks

Soquetes é um padrão da Internet para gateways no nível do circuito. Use o servidor de Soquetes para a conversão de endereço se a aplicação usar TCP, tal como navegadores Web, aplicações FTP ou Telnet. Os Soquetes podem ajudar no acesso à Internet, enquanto ocultam os endereços IP internos.

Para pedidos de saída, de um cliente protegido a um servidor não protegido, o servidor de Soquetes possui os mesmos objetivos de um servidor proxy: interromper a sessão no Firewall e fornecer uma porta segura na qual os usuários possam acessar a rede externa e não protegida enquanto protegem o endereçamento e a estrutura da rede interna. O servidor de Soquetes possui a vantagem de não ser difícil para o usuário, que precisa apenas de um pouco mais de trabalho administrativo.

O servidor de Soquetes pode interceptar todos os pedidos TCP de saída que passariam entre a rede e a Internet. O servidor Socks fornece uma interface do programa de aplicação remoto para que as funções executadas pelos programas cliente em domínios protegidos sejam canalizadas através dos servidores protegidos nas estações de trabalho firewall, ocultando o endereço de IP do cliente. O acesso é controlado pelos filtros que estão associados às regras de Soquete.

O servidor de Soquetes é semelhante ao servidor proxy. Mas enquanto o servidor proxy realmente realiza a função TCP/IP no Firewall, o servidor de Soquetes apenas identifica o usuário e encaminha novamente a função através do Firewall. A função TCP/IP real é realizada na estação de trabalho cliente, não no firewall. Isso salva o processamento no Firewall. Os usuários da rede protegida podem usar os muitos produtos TCP/IP que suportam o soquete padrão. A Figura 21 ilustra o servidor de Soquetes interceptando um pedido HTTP de um cliente dentro da rede protegida.Figura 21. O servidor SocksO servidor de Soquetes efetivamente oculta seus



O daemon do Soquete opera como um Serviço Windows NT iniciando automaticamente quando o sistema é iniciado. Além disso, um Observador é fornecido para permitir o monitoramento do servidor. Você pode iniciar o Observador manualmente.

O IBM Firewall oferece um caminho de migração regular em forma de três perfis de autenticação, para que os consumidores possam continuar a utilizar os clientes Socks Protocol Versão 4 à medida que introduzem os clientes Socks Protocol Versão 5.

1. O perfil mais permissivo não permite a autenticação de saída e permite que qualquer usuário, utilizando um cliente Socks Protocol Versão 4 ou Socks Protocol Versão 5 conecte-se. Neste panorama conexões de chegada são negadas.
2. O perfil de migração permite que usuários do Socks Protocol Versão 4 passem sem autenticação, porém requer que usuários do Socks Protocol Versão 5 estejam autenticados. Conexões de chegada do Socks Protocol Versão 4 são negadas e conexões de chegada do Socks Protocol Versão 5 precisam ser autenticadas. Este é o perfil padrão.
3. O perfil mais seguro requer que todos os usuários utilizem os clientes Socks Protocol Versão 5 e forneçam autenticações válidas.

Quando o Firewall é instalado, o servidor Soquete é ativado, mas não há regras no arquivo de configuração do Soquete. Para que clientes de socks utilizem o servidor de Socks, é necessário configurar o socks utilizando o cliente de configuração. Consulte “Exemplo de Socks” na página 56 para obter um exemplo de como configurar um serviço de Soquetes.

Protocolos Suportados pelo Servidor Socks Protocol Versão 5

O servidor do Socks Protocol Versão 5 suporta os seguintes protocolos TCP e UDP e muitos outros:

- Archie
- Finger
- FTP
- Gopher
- HTTP
- Proxy HTTP
- News
- SNMP
- Telnet
- TFTP
- RealAudio
- RealPlayer
- Whois
- X-Windows

Além disso, a maioria do clientes de e-mail são aceitos. A aceitação destes protocolos depende de sua implementação em si.

Configuração do Servidor de Soquetes Utilizando o Cliente de Configuração

Os Gabaritos de Soquetes são regras que controlam a segurança por meio do servidor de Soquetes. Os gabaritos de soquetes permitem personalizar, acrescentar, copiar ou eliminar gabaritos de soquetes existentes. Estes gabaritos, por sua vez, podem ser usados em definições de conexões no Firewall do mesmo modo que gabaritos de regras são utilizados.

Inclusão de Nova Regra de Soquetes

Para incluir uma regra no arquivo de configuração de soquetes utilizando um gabarito de soquetes fornecido pelo cliente de configuração, selecione Controle de Tráfego a partir da árvore de navegação do cliente de configuração. Dê um clique duplo sobre o ícone da pasta de arquivo para expandir a exibição. Selecione Gabaritos da Conexão. Dê um clique duplo sobre o ícone da pasta de arquivo para expandir a exibição. Selecione **Soquetes**. O quadro de diálogo **Soquetes** é exibido.

1. Dê um clique duplo em **NOVO** para incluir um novo gabarito de Soquetes.

   O quadro de diálogo **Incluir uma Regra de Soquetes** é exibido, como mostrado em Figura 22.

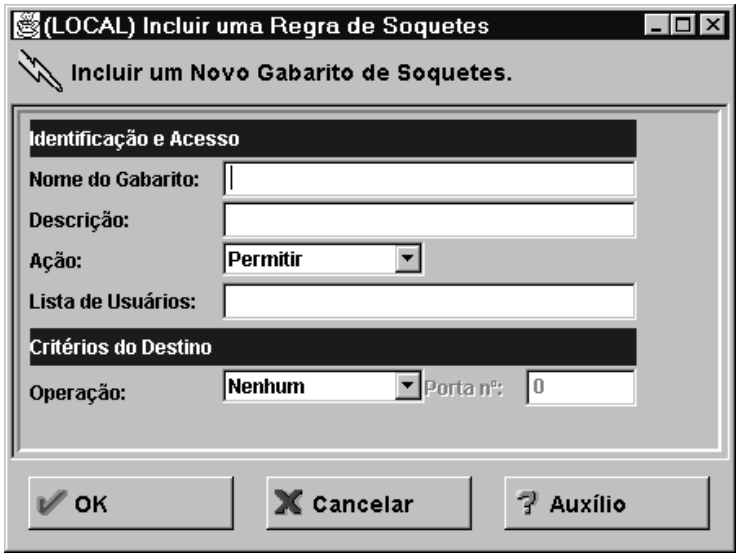


Figura 22. Incluir uma Regra de Soquetes

2. No campo **Nome do Gabarito**, forneça o nome da entrada de soquetes. Esse nome deve ser exclusivo e não deve conter símbolo de canalização (|), aspas simples (ou apóstrofo) nem aspas duplas ("), pois esses caracteres são usados como delimitadores de arquivo. Se eles forem empregados, os dados não ficarão confiáveis.
3. Forneça uma descrição.
4. Clique a seta Ação e escolha entre permitir ou negar acesso a partir de uma origem ou de um destino.

Quando um datagrama chega ao servidor de Soquetes, ele compara as especificações do datagrama com cada regra no arquivo de configuração começando pela primeira regra até encontrar a que coincide exatamente. Aí então a pesquisa é interrompida e ele executa uma ação relevante (permite ou

Utilize este quadro de diálogo **Incluir Regra de Soquetes** para permitir ou negar o acesso do firewall a hosts da rede com base no endereço IP.

Modificação de uma Regra de Socks

1. Dê um clique duplo em uma entrada no quadro de diálogo **Soquetes**.

   O quadro de diálogo **Modificar Regra de Soquetes** é exibido.

2. Modifique os campos apropriados conforme descrito em “Inclusão de Nova Regra de Soquetes” na página 71, e clique em **OK**.

Eliminação de uma Regra de Socks

Selecione uma entrada do quadro de diálogo **Soquetes** e clique em **Eliminar**. Você será perguntado se realmente deseja eliminar esta regra de socks. Clique em **OK** para eliminar a regra.

Ativação de Regras da Conexão

Assim como com as regras do filtro, é necessário ativar as regras do socks. Clique em **Ativação da Conexão** na árvore de navegação do cliente de configuração, selecione **Regenerar Regras de Conexão e Ativar**, depois clique em **Executar**.

O Firewall copia as regras do arquivo de configuração dos soquetes para as regras do firewall e ativa as regras. Quando as regras estiverem ativadas, as novas regras são registradas no arquivo de log do firewall.

Exemplo de Saída de Registro para Soquete

Segue abaixo um exemplo de uma saída de registro para Soquete.

```
Feb 03 13:46:20 1998 mr16n18: ICA3123i: Servidor Sockd iniciando
Feb 03 13:47:31 1998 mr16n18: ICA3010i: Início da sessão
Feb 03 13:47:31 1998 mr16n18: ICA3011i: Início da sessão
Feb 03 13:49:15 1998 mr16n18: ICA3007i: Número excessivo de tarefas
Feb 03 13:58:31 1998 mr16n18: ICA3015i: Término da sessão
```

Considerações ao Cliente para Utilização do Servidor de Socks

A maioria dos navegadores Web são socksified e você pode obter pilhas socksified para maioria das plataformas. Clientes Socksified para outras aplicações TCP/IP estão disponíveis a partir de diversas fontes. Para obter um cliente específico que o soquete executa, consulte a documentação do cliente. Para obter informações adicionais, consulte:

http://www.raleigh.ibm.com/sng/sng-socks.html
http://www.socks.nec.com

Encadeamento do Servidor de Soquetes

O encadeamento do Servidor de Soquetes é um recurso através do qual um servidor de Soquetes pode residir atrás de outro e ainda assim permitir acesso à rede que se encontra além do servidor de Soquetes na extremidade mais distante. (Pode-se considerar isso como socksifyng um servidor de soquetes). Este é um panorama de intranet muito útil.

Para configurar um encadeamento de servidor de soquetes com o servidor de Soquetes, edite o arquivo `socks5.header.cfg`. Este arquivo reside no subdiretório `config` do Firewall. Acrescente o seguinte:

- Uma diretiva *no proxy* - para indicar as sub-redes as quais o Firewall possui acesso direto
- Uma diretiva *socks4* - para indicar as sub-redes que são acessíveis através de um servidor SOCKS Protocol Versão 4
- Uma diretiva *socks5* - para indicar as sub-redes que são acessíveis através de um servidor Socks Protocol Versão 5

Por exemplo, considere a seguinte rede. O departamento de Pesquisa possui uma pequena rede privada, *q.private.com*, por trás do próprio firewall. A sub-rede do departamento de Pesquisa é 10.007.007.0/255.255.255.0. A rede privada da empresa, *private.com*, contém a rede 10.0.0.0/255.0.0.0 inteira. O servidor SOCKS Protocol Versão 4 da empresa, *socks.private.com*, fornece acesso à Internet.

No servidor Soquetes da Pesquisa *socks.q.private.com*, acrescente as duas linhas a seguir no `socks5.header.cfg`.

```
no proxy 10.0.0.0/255.0.0.0 - - -
socks4      0/0   - socks.private.com 1080
```

Por último, acrescente uma conexão de Controle de Tráfego para permitir a comunicação do *socks.q.private.com* com o *socks.private.com*. É possível que isto já tenha sido feito por um Serviço mais geral. Acrescente uma Conexão cuja fonte é a interface não protegida do Firewall *q.private.com* Firewall, cujo destino é *socks.private.com*, e acrescente o serviço *Encadeamento de Soquetes Proxy*. Depois reative suas regras de Controle de Tráfego.

Capítulo 12. Administração de Usuários no Firewall

Este capítulo descreve como realizar tarefas administrativas diárias com o IBM Firewall, incluindo:

- Inclusão de usuários no IBM Firewall para que possam acessar hosts fora da rede protegida
- Alteração dos atributos dos usuários que acessam o firewall
- Exclusão de usuários que não precisam mais de acesso fora da rede

Não edite os arquivos de configuração diretamente; caso o faça, os atributos do usuário do IBM Firewall não serão configurados corretamente. Faça toda a administração do IBM Firewall utilizando os diálogos do cliente de configuração ou a linha de comandos.

Inclusão de um Usuário no IBM Firewall

O IBM Firewall define três tipos de usuários e armazena informações sobre os mesmos em dois diferentes bancos de dados de usuário.

Tipos de Usuários

O IBM Firewall divide os usuários em três categorias:

Usuários Proxy Use os serviços do firewall - como o proxy HTTP - para acessar sites Web na Internet de dentro de uma rede empresarial. Os usuários proxy conseguem usar serviços através do firewall mas não têm acesso à máquina do firewall e não conseguem efetuar logins locais na máquina do Firewall.

Administradores Firewall Podem usar os serviços proxy do Firewall mas também podem configurar o Firewall por meio do cliente de configuração e efetuar o login no Firewall a partir de um host remoto. Assim como os usuários proxy, administradores do firewall não podem efetuar logins locais na máquina do Firewall.

Os administradores firewall podem criar e modificar definições para usuários proxy, mas não podem criar ou modificar as definições de outros administradores firewall.

Administradores Firewall Primários Possuem as mesmas capacidades dos administradores firewall. Podem também efetuar logins locais na máquina do Firewall. Os administradores firewall primários podem criar e modificar definições para outros administradores firewall.

Tipos de Bancos de Dados

Há dois tipos de bancos de dados de usuário.

Banco de Dados do Usuário do Firewall Contém atributos relacionados ao firewall para cada usuário e administrador proxy. Inclui atributos tais como a senha e regras de senha de firewall do usuário e cujos métodos devem ser utilizados para autenticar o usuário para cada serviço.

Se o usuário proxy não estiver definido no banco de dados de usuário firewall e o usuário tentar utilizar serviços proxy do firewall, o registro de

usuário padrão, `fwdfusr` será utilizado para definir atributos e esquemas de autenticação utilizados para validar o usuário.

Administradores primários do firewall não podem ser definidos no banco de dados de usuário firewall. Use o registro de administrador do firewall padrão, `fwdfadm`, para fornecer atributos aos administradores.

Como os usuários proxy, se os administradores firewall também são definidos no banco de dados do usuário do Windows NT, suas senhas de início de sessão NT serão usadas quando o usuário solicitar serviços que devem ser autenticados usando senhas de início de sessão do NT.

Banco de dados de Usuário de Windows NT Contém as senhas de início de sessão NT para usuários. Em geral, os usuários proxy não precisam ser definidos no banco de dados de usuário NT a menos que sejam autenticados utilizando suas senhas de logon NT.

Se outros métodos de autenticação serão usados para autenticar usuários proxy, eles não têm de ser definidos no banco de dados do Usuário do Windows NT.

Administradores primários do firewall é sinônimo de usuários do Windows NT que são membros do grupo de administradores NT e devem ser definidos no banco de dados do usuário do Windows NT.

Utilização do Cliente de Configuração para Incluir um Usuário

A inclusão de um usuário no IBM Firewall concede a ele acesso à rede externa.

1. A partir da árvore de navegação do cliente de configuração, selecione Usuários. Aparece a caixa de diálogo **Administração de Usuário**.
2. Selecione **Novo** na caixa de diálogo **Administração de Usuário** e clique em **Abrir**. Aparece a caixa de diálogo **Incluir Usuário**, como mostra o Figura 23 na página 77.

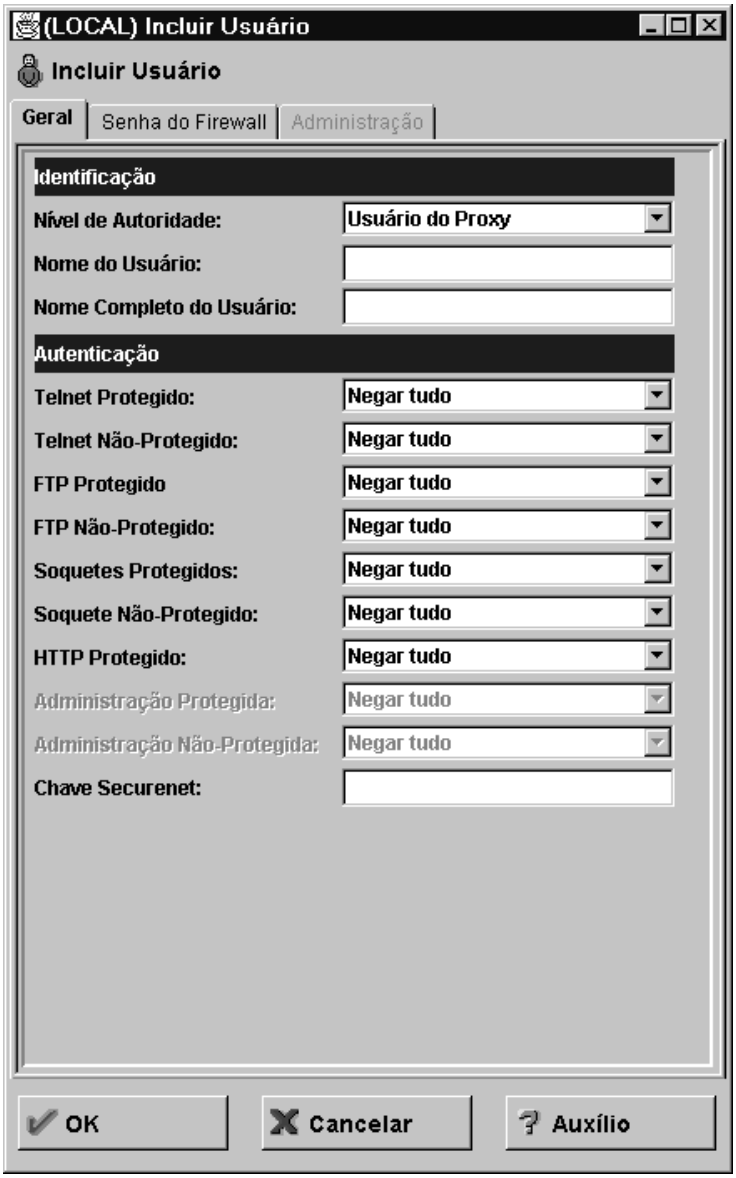


Figura 23. Incluir Usuário

3. Forneça estas informações:

   Nível de Autoridade

   Especifica o nível de autoridade para este usuário. Clique na seta **Nível de Autoridade** para selecionar o tipo de usuário.

   Usuário de Soquetes/Proxy

   O usuário que está sendo definido é tanto para acesso a servidor de Soquetes quanto para acesso proxy. O usuário não possui autoridade de administração. Este é o padrão.

Administrador Firewall

Possui todos os atributos de um usuário, mas o administrador também pode efetuar login no Firewall e efetuar tarefas administrativas. Um administrador possui atributos adicionais que definem quais funções administrativas ele tem permissão para realizar. Um administrador firewall pode criar usuários firewall mas não pode criar outros administradores firewall. Os administradores firewall não podem efetuar o login localmente na máquina do Firewall. Eles devem acessar o servidor de configuração a partir de uma máquina remota.

Administrador Firewall Primário

O administrador primário de firewall pode efetuar login localmente na máquina do Firewall. Ele possui acesso total a todas as funções administrativas. Ele também pode criar outros administradores firewall exceto administradores firewall primários.

Para definir o administrador primário de firewall, cria-se um usuário no banco de dados NT e transforma-se esse usuário em membro do grupo de administradores NT. Modifique o registro `fwdfadm` para que defina os atributos para o administrador firewall primário.

Nome de Usuário Especifica o nome para este usuário. Este é o nome de usuário com o qual este usuário irá conectar-se na telnet ou servidor FTP no IBM Firewall. Não é necessariamente o nome de usuário TCP/IP do usuário ou o nome do host, porém eles podem ser iguais.

Os nomes de usuários podem ser compostos de 1 a 20 caracteres, incluindo:

a até z
A até Z
0 até 9
_ (o sublinha)

Nome de usuários não são sensíveis a maiúsculas e minúsculas.

O Firewall vem com dois usuários pré-instalados:

a. Usuário padrão ou `fwdfuser`. Se um usuário não estiver definido no banco de dados firewall, o `fwdfuser` é utilizado para determinar os atributos firewall do usuário, como os métodos de autenticação a serem utilizado ao se autenticar o usuário.

   Na instalação, quando o `fwdfuser` é criado, todos os métodos de autenticação são definidos para negar tudo. A permissão para o `fwdfuser` controla como o firewall processa nomes de usuários não definidos.

   O administrador pode ver o `fwdfuser` ou alterar o método de autenticação atribuído utilizando o cliente de configuração ou a linha de comando. No entanto, o `fwdfuser` não pode ser excluído e deve sempre existir no firewall. Além disso, a senha do firewall e SNK não são tipos de autenticação válidos para `fwdfuser`. Para maiores informações, consulte o manual *IBM eNetwork Firewall Referência*

b. O Administrador Firewall Primário Padrão, `fwdfadm`, define os atributos de firewall para todos os administradores primários de firewall. Como os administradores firewall primários não possuem seus próprios registros de usuário no banco de dados firewall, este registro é utilizado para definir os métodos de autenticação utilizados para autenticar administradores firewall primários.

   Na instalação, todos os métodos de autenticação do `fwdfadm` são definidos para *negar tudo*, a não ser quanto aos métodos de autenticação de administração não protegidos, que são definidos para senha de logon NT. Os administradores firewall primários podem ver e modificar este registro, mas ele não pode ser eliminado. Além disso, a senha do firewall e SNK não são tipos de autenticação válidos para `fwdfadm`.

Nome Completo do Usuário
Especifica uma descrição do usuário.

Os seguintes campos referem-se a métodos de autenticação. Clique nas setas para selecionar pela lista de métodos de autenticação. Elas estão explicadas em “Métodos de Autenticação de Usuário” na página 81.

Telnet Protegida Indica se a identidade deste usuário, ao iniciar sessão a partir da rede protegida, deve ser autenticada de alguma maneira.

Telnet Não-Protegida
Indica se a identidade deste usuário, ao iniciar sessão a partir da rede não protegida, deve ser autenticada de alguma maneira.

FTP Protegido Especifica em que nível de autenticação que o usuário precisa usar o FTP para acessar o Firewall a partir da rede protegida.

FTP Não-protegido Especifica em que nível de autenticação o usuário precisa usar o FTP para acessar o Firewall a partir da rede não protegida.

Soquete Protegido Especifica o método de autenticação do Socks V5 para conexões de cliente de Soquetes originárias do lado protegido do firewall. Clique na seta para selecionar pela lista de opções. Elas estão explicadas em “Métodos de Autenticação de Usuário” na página 81.

Soquete Não-Protegido
Especifica o método de autenticação do Socks V5 para conexões de cliente de Soquetes originárias do lado não-protegido do firewall. Clique na seta para selecionar pela lista de opções. Elas estão explicadas em “Métodos de Autenticação de Usuário” na página 81.

HTTP Protegido Especifica um tipo de ID de usuário/senha de autenticação em solicitações proxy HTTP de saída. Clique na seta para selecionar pela lista de opções. Elas estão explicadas em “Métodos de Autenticação de Usuário” na página 81.

O navegador solicita a ID de usuário e a senha, então se você estiver usando SDI, preencha um código de entrada no prompt da senha.

O método fornecido pelo usuário tem que reconhecer que Soquetes/senha não podem suportar diálogos interativos e apresentar comportamento compatível com eles.

Administração Protegida
Especifica o método de autenticação utilizado para iniciar sessão a partir do cliente de configuração através de uma interface protegida. Lembre-se que ao iniciar sessão localmente (ao escolher local no painel de logon) está sempre em um ambiente protegido, então este é o método de autenticação que seria utilizado.

Administração Não-protegida
Especifica o método de autenticação utilizado para iniciar sessão a partir do cliente de configuração através de uma interface não protegida.

Chave SecureNet Especifica a seqüência de caracteres a ser fornecida por usuário remoto que possui cartão da Chave AssureNet Pathways SecureNet. Forneça o código chave com o qual você também irá instruir o cartão chave. Consulte as informações da Chave SecureNet para obter instruções sobre a seleção e instalação de um código chave.

Notas:

a. Este campo não é utilizado para o cartão SecurID.

b. É necessário criar uma chave aleatória exclusiva para cada usuário.

c. Ao instalar a chave no cartão da chave SecureNet, utilize o procedimento de instalação AssureNet Pathways e selecione **Modo 5**.

Consulte “Métodos de Autenticação” na página 85 para maiores informações.

Métodos de Autenticação de Usuário

As escolhas para autenticação de usuário são:

Negar Tudo O acesso é negado ao usuário.

Permitir Tudo Não é necessária autenticação.

Senha Logon NT A senha logon NT é menos segura que a senha firewall. No entanto, se os usuários já estiverem definidos em domínio NT, a senha de logon NT poderá ser usada para que o usuário não precise ter diversas senhas.

Quem optar por este método de autenticação terá sua ID de usuário e sua senha validadas contra o banco de dados de usuário local do Windows NT. Se o Firewall estiver configurado para depender de outros servidores do Windows NT, esses servidores dependentes serão pesquisados em busca de definições de usuário.

Antes que relações de dependência possam ser configuradas entre o Firewall do Windows NT e servidores do Windows NT dependentes, uma conexão deve ser configurada para permitir o tráfego de comunicação TCP/IP entre as duas máquinas.

Configure esta conexão usando os seguintes serviços pré-definidos:

1. Autenticação do Controlador de Domínio - que permite o uso do Controlador de Domínio para autenticação de usuário
2. Transmissões de Serviços de Nome NetBT - que permitem NetBIOS nas transmissões de Serviços de Nome TCP/IP

Use os utilitário de configuração do Windows NT para definir as relações de dependência.

Chave SecureNet A autenticação é feita utilizando uma chave AssureNet Pathways SecureNet.

No campo Chave SecureNet, forneça o código chave com o qual também irá instruir o cartão da Chave SecureNet.

Notas:

1. É necessário criar uma chave aleatória exclusiva para cada usuário.
2. A chave aleatória deve estar no intervalo de 1–377 para cada 8 valores octal
3. Ao instalar a chave no cartão da chave SecureNet, utilize o procedimento de instalação AssureNet Pathways e selecione **Modo 5**.

Consulte “Métodos de Autenticação” na página 85 para maiores informações.

Cartão SecurID A autenticação é feita utilizando um cartão de segurança Security Dynamics SecurID ou cartão pinpad. *Não* use o campo Chave SecureNet. O PIN deve ser definido antes de utilizar este método de autenticação com o IBM Firewall.

Para FTP, o novo modo PIN SDI e o próximo modo de sinal não são aceitos.

Consulte “Métodos de Autenticação” na página 85 para maiores informações.

Autenticação Fornecida pelo Usuário 1, 2 e 3
A autenticação é fornecida pelo usuário. Podem ser instalados até três métodos de autenticação fornecida pelo usuário no Firewall. Para saber como criar e compilar uma subrotina para autenticação fornecida pelo usuário, consulte a *Referência ao IBM eNetwork Firewall*.

Senha Firewall O usuário deve ser solicitado a fornecer, e deve fornecer, uma senha válida. Quando este painel está completo, o IBM Firewall solicita a especificação de uma senha para este novo usuário.

A senha de firewall permite a definição de senhas e de regras de senha mais seguras do que a senha de logon no Windows NT, sendo ela portanto a opção recomendada para senhas.

Solicitar Alteração do Usuário Clique em Sim ou Não para indicar se o usuário será solicitado a alterar sua senha a próxima vez que for autenticado.

Bloquear Senha Clique em Sim ou Não para indicar se a senha está bloqueada. Este é definido com Sim quando o número máximo de logins falhos é ultrapassado ou quando a senha não tiver sido utilizada durante o número de semanas especificado em Tempo Máximo Antes do Bloqueio.

O administrador pode definir este campo com sim para impedir que um usuário utilize autenticação de senha.

Notas:

1. As senhas são sensíveis a maiúsculas e minúsculas. O usuário terá que digitá-la exatamente com o mesmo tipo de letra com que ela foi definida. Se houver estações de trabalho que só utilizam letra maiúscula, digite as senhas desses usuários em letra maiúscula.
2. O sistema operacional permite definir regras para senhas. Essas regras para senhas se aplicam quando o usuário altera sua senha mas não quando o administrador faz alterações de senha. As regras para senhas são:

   Dias a Advertir Antes de Expirar (dias) Número de dias antes de uma senha expirar e período dentro do qual o firewall dará ao usuário a opção de alterar sua senha.

   Máximo de Semanas Antes de Expirar Número de semanas antes que o usuário seja solicitado a alterar a senha.

   Máximo de Semanas Antes de Bloquear Número de semanas dentro do qual a senha não é utilizada antes de ser bloqueada.

   Máximo de Tentativas de Login Permitido Número máximo de tentativas de login falhas antes da senha ser bloqueada.

   Senhas Antes da Reutilização Número de senhas armazenadas na lista do histórico de senhas. A senha não pode ser substituída por qualquer senha que esteja atualmente na lista do histórico. Este parâmetro só é válido se Semanas Antes da Reutilização de Senha for igual a zero.

   Semanas Antes da Reutilização de Senha Número de semanas que as senhas são mantidas no lista do histórico de senhas. A senha não pode ser substituída por qualquer senha que esteja atualmente na lista do histórico.

   Tamanho Mínimo Número mínimo de caracteres em uma senha.

   Mínimo de Caracteres Alfabéticos Número mínimo de caracteres alfabéticos em uma senha.

   Mínimo de Outros Caracteres Número mínimo de caracteres não-alfabéticos em uma senha.

   Máximo de Caracteres Repetidos Número máximo de vezes que um caractere pode ser repetido em uma senha.

   Mínimo de Caracteres Diferentes Número mínimo de caracteres diferentes na senha.

Clique no item **Senha do Firewall** para personalizar esses valores para cada usuário, como mostra o Figura 24 na página 84.

Figura 24. Item de Senha do Firewall

Alteração do Acesso de um Usuário

Depois do usuário ser incluído no Firewall, seus atributos de segurança poderão ser alterados pela caixa de diálogo **Modificar Usuário**.

1. Selecione o usuário a ser alterado na caixa de diálogo **Usuários** e clique em **Abrir**.
2. Quando a caixa de diálogo **Modificar Usuário** aparecer, mude os campos apropriados. Consulte “Inclusão de um Usuário no IBM Firewall” na página 75 para obter uma lista de atributos de usuário que podem ser alterados.
3. Feitas as alterações, clique em **OK**.

Eliminação de Usuário do IBM Firewall

Nota: Não elimine os usuários `fwdfuser` ou `fwdfadm`.

Para eliminar um usuário, clique em **Eliminar** no painel **Lista de Usuários**.

Nível de Autoridade do Administrador por Função

Só o *administrador de firewall primário* pode criar e modificar administradores e determinar sobre que funções de firewall eles terão autoridade. Por exemplo, você pode limitar um determinado administrador a só ter autorização para executar funções de Usuários e do Monitor de Logs.

Na caixa de diálogo **Incluir Usuário**, selecione Administrador de Firewall para o campo **Nível de Autoridade**. Leia “Inclusão de um Usuário no IBM Firewall” na página 75 para saber como completar a caixa de diálogo **Incluir Usuário**.

Depois selecione o item **Administrador** no alto da caixa de diálogo **Incluir Usuário**. Selecione as funções que o administrador está autorizado a usar.

Métodos de Autenticação

A seguir, estão vários métodos de autenticação do usuário.

Negar Tudo

O IBM Firewall proíbe o acesso ao servidor.

Permitir Tudo

Nenhuma autenticação é necessária. O servidor não tenta autenticar você; mas continua com um prompt de comando para que você possa acessar um host estrangeiro.

Senha Firewall

O servidor solicita sua senha firewall (que não será exibida) antes de permitir que você continue.

```
Senha:
```

Digite a sua senha firewall. Esta é a mesma senha com a qual seu nome de usuário foi incluído no Firewall.

Autenticação do Cartão SecurID

Utilize este método se possuir um cartão SecurID e a sua rede utiliza o Security Dynamics ACE/Server.

O servidor proxy pede o PASSCODE (que não será exibido) antes de deixar você prosseguir.

```
Digite o PASSCODE:
```

Agora, digite seu código SecurID PIN de 4 dígitos seguido por uma vírgula e depois o código do seu cartão SecurID. Por exemplo, para conectar-se como

usuário NEWUSER com um PIN de 1234, quando o seu cartão SecurID mostra o código 179091, você digitaria:

```
login: NEWUSER
Digite PASSCODE: 1234,179091
```

Se os usuários usam inicialmente o FTP, a autenticação do cartão SecurID vai falhar porque o FTP não tem a opção de permitir mudança de senha. Os usuários precisam usar o telnet na primeira vez que tentam fazer uma autenticação com o cartão SecurID pelo qual vão criar um PIN. Depois eles podem usar esse PIN para fazer autenticações posteriores, como FTP, HTTP e assim por diante.

Se o cartão SecurID estiver no novo modo PIN, você deve definir o PIN antes de utilizar este método de autenticação com o IBM Firewall.

Autenticação da Chave SecureNet

Quem tem cartão da Chave Assurenet Pathways SecureNet deve usar esse método. Ao inicializar o cartão SNK, utilize o seguinte:

- Formato de exibição (hexadecimal)
- Capacidade de ERASE (ligado ou desligado)
- Capacidade de challenge de dígito único (desligado)

O servidor proxy solicitará uma resposta fornecida pelo seu cartão da Chave SecureNet Key, antes de permitir que você continue.

```
   Utilize
SNK para challenge
   ######## para o usuário user_id
   Ed:
```

O desafio ######ÕÕ é um número com 8 dígitos que é fornecido no cartão da chave SecureNet.

1. Ao receber esta solicitação, ative seu cartão da chave SecureNet e forneça seu código PIN. O código PIN foi fornecido a você junto com o cartão.
2. Forneça o desafio do modo como fornecido pelo servidor.

   Por exemplo: você conecta-se ao servidor; o servidor solicita:

   ```
      Utilize
   SNK para challenge
         78987648 para o usuário NEWUSER
      Ed:
   ```

   Forneça o valor 78987648 no cartão da Chave SecureNet. O cartão exibe a resposta, que você fornece ao servidor proxy.
3. Forneça esta resposta ao servidor.

   Se o cartão da Chave SecureNet exibiu 8AE222A9 em resposta ao seu challenge, então forneça 8AE222A9 ao servidor:

   ```
      logon: NEWUSER
         Utilize SNK para challenge 78987648 para o usuário NEWUSER
      Ed:8AE222A9
   ```

O nome do SecurNetKey (SNK) foi trocado para Defender Handheld Token** (DHT) pelas tecnologias AXENT**.

Senha Logon NT

Quem optar por este método de autenticação terá sua ID de usuário e sua senha validadas contra o banco de dados de usuário local do Windows NT. Se o Firewall estiver configurado para depender de outros servidores do Windows NT, esses servidores dependentes serão pesquisados em busca de definições de usuário.

Autenticação Fornecida pelo Usuário 1, 2 e 3

Pode-se usar a Autenticação Fornecida pelo Usuário para FTP e telnet. Consulte o *IBM eNetwork Firewall Referência* para obter maiores informações.

Capítulo 13. Configuração de Servidores Proxy

Este capítulo contém informações gerais sobre como configurar e utilizar os servidores proxy a partir de estações de trabalho dentro e fora da rede protegida.

Proxy HTTP

O proxy HTTP manipula eficientemente solicitações do navegador através do IBM Firewall eliminando a necessidade de um servidor socks para navegar na Web. Os usuários podem acessar informações úteis na Internet, sem comprometer a segurança da rede interna e sem alterar o ambiente do cliente para implementar o proxy HTTP.

O proxy HTTP não é um servidor. O usuário final não pode carregar arquivos do proxy ou colocar arquivos no proxy. Além disso, ele não é um proxy de cache. Nada é armazenado no firewall em nome de uma solicitação HTTP.

Sessões Persistentes

As conexões persistentes permitem que um cliente e um servidor sinalizem o fechamento de uma conexão TCP. Esta sinalização utiliza um campo de cabeçalho de conexão.

O proxy do IBM Firewall suporta conexões persistentes entre um cliente e o proxy. A condição *pedidos máximos persistentes* e a condição *timeout de conexão persistente* controlam por quanto tempo a conexão irá existir. Se uma destas condições aumentar, a conexão do soquete entre o proxy e o cliente fechará. Se a condição *pedidos máximos persistentes* e a condição *timeout de conexão persistente* não forem satisfeitas, a conexão permanecerá aberta e é responsabilidade do cliente determinar quando um pedido está concluído.

Se determinado incorretamente, isto poderá resultar em um display indicando tráfego na conexão quando não há nenhum. Um exemplo disto seria quando o ícone animado de um navegador fica operando continuamente embora a página toda já tenha sido carregada. Clique em **Parar** para interromper a animação. Consulte “Máximo de Solicitações Persistentes” na página 92 e “Timeout para Conexão Persistente” na página 92 para obter informações sobre estes parâmetros.

Configuração do Proxy HTTP Utilizando o Cliente de Configuração

Para configurar o Proxy HTTP, faça o seguinte:

1. É necessário permitir consultas DNS para que o Proxy HTTP possa funcionar adequadamente. Um jeito fácil de fazer isto é clicar em Regulamento de Segurança de dentro da pasta Administração do Sistema na árvore de navegação do cliente de configuração e clicar em Permitir Consultas DNS.
2. Ative filtros
3. Inclua uma conexão. Consulte “Exemplo de Proxy HTTP” na página 55 para obter um exemplo de como configurar uma conexão no lado não-protegido da sua rede.

4. Para configurar o Proxy HTTP, selecione HTTP da árvore de navegação do cliente de configuração. O IBM Firewall exibe o quadro de diálogo **Proxy HTTP**, como mostrado na Figura 25 na página 90.

Figura 25. HTTP

5. Para encerrar o proxy, selecione `meu computador/painel de controle/serviços`. Escolha o IBM Firewall HTTP Proxy e clique em *Parar*.

   O executável phttpd é um serviço do sistema que é iniciado automaticamente quando o sistema é iniciado.

Configure os parâmetros no quadro de diálogo **Proxy HTTP**. Se algum parâmetro for alterado, o serviço do Firewall HTTP irá parar e iniciar novamente. Os usuários do proxy ativo terão seus pedidos encerrados até que o proxy seja reiniciado (em alguns segundos).

Número da Porta do Proxy

Utilize este parâmetro para especificar o número de porta que o proxy deve interceptar para solicitações. Se você alterar o número de porta, será necessário configurar os filtros para permitir ou não o fluxo através das portas. Números de porta menores que 1024 são reservados para aplicações TCP/IP. Portas comuns utilizadas para servidores Web proxy são 8080 e 8088.

As regras do filtro padrão são definidas para vetar o tráfego não-protegido de chegada na porta 8080, mas permitir o tráfego protegido na mesma porta. O proxy só irá rejeitar requisitos de proxy não-protegidos. O padrão é `8080`. Se você alterar isto, o número de porta também deverá ser alterado nos Serviços que estão definidos para esta configuração. Se qualquer uma das definições for alterada, será necessário reiniciar o processo phttpd.

Tamanho do Buffer de Conteúdo

Utilize este parâmetro para definir o tamanho do buffer para dados dinâmicos gerados por um servidor. Os dados dinâmicos são saídas dos programas CGI, inclusões do lado do servidor e programas API. São dados que não vêm de um proxy.

Especifique o valor em kilobytes (K). O padrão é `50K`.

Tamanho do Conjutos de Tarefas

Use este parâmetro para definir o número fixo de tarefas que você deseja ter ativados de uma vez. O proxy suspende novas solicitações até que outra solicitação termine e que cadeias tornem-se disponíveis. Geralmente, quanto maior a potência de uma máquina, maior o valor que deve ser utilizado para este parâmetro. Se a máquina começar a gastar muito tempo em tarefas suplementares, como swap de memória, tente reduzir este valor. Especifique um número inteiro como 60, por exemplo. O padrão é `200`.

Nível dos Usuários

Este parâmetro informa ao proxy o nível de usuários a ser autenticado. Especifique o valor como todos, novo ou nenhum. O padrão é nenhum. Os valores são:

Todos Todos os navegadores receberão a resposta de autenticação do proxy para indicar que o navegador deve solicitar ao usuário uma ID de usuário e senha. Se o navegador não aceita a resposta de autenticação do proxy, será exibida uma página de erro indicando isto. Se o navegador a aceita, o prompt de ID de usuário e senha será exibido.

novo É utilizado como um auxílio à migração. Ele só enviará de volta uma resposta de autenticação do proxy 407, para pedir ao navegador que emita um prompt de id de usuário/senha, a um navegador cliente que se auto-identifica como um navegador HTTP/1.1. Você pode definir uma chave no Internet Explorer 4.0 para que ele transmita pedidos com o identificador HTTP/1.1. O Netscape e outros se auto-identificam como pedidos HTTP/1.0.

nenhum Não verifica pedidos do navegador. Não solicita nenhuma id de usuário/senha.

Timeout

Este parâmetro informa ao proxy quanto tempo deve aguardar por um pedido do cliente antes de solicitar que o usuário se autentique novamente. Um usuário é autenticado a partir do endereço IP e ID de usuário específico fornecido na hora da autenticação original para este período de tempo inativo. Especifique o tempo em minutos. O padrão é 60.

Enquanto o usuário estiver navegando ativamente, esta janela de tempo não irá expirar.

Máximo de Solicitações Persistentes

Este parâmetro indica o número máximo de pedidos que um proxy pode receber em uma conexão persistente HTTP/1.1. Esta é uma ferramenta de desempenho que tem impacto direto sobre o timeout de autenticação. Enquanto estiver em uma sessão persistente, nenhum teste da autenticação de um usuário será feito até que a sessão persistente termine. Especifique o valor como um número inteiro, por exemplo 25. O padrão é 5.

Timeout para Conexão Persistente

Este parâmetro indica o tempo em segundos para manter uma conexão persistente HTTP/1.1 com um navegador cliente assim que um navegador compatível com HTTP/1.1 inicia uma sessão com o proxy. Esta é uma ferramenta de desempenho que tem impacto direto sobre o timeout de autenticação. Enquanto estiver em uma sessão persistente, nenhum teste da autenticação de um usuário será feito até que a sessão persistente termine. Especifique o tempo em segundos. O padrão é 60.

Gerenciamento do Sistema de Registros do HTTP

Este parâmetro pede ao proxy para registrar solicitações de inicialização/encerramento e todas as solicitações do proxy no registro do firewall. Ele utiliza o nível de registro LOG_NOTICE. Ative-o caso deseje monitorar a atividade de solicitação do HTTP. Os eventos são registrados ao recurso `registro do firewall`.

Configuração do Navegador

O navegador cliente deve ser configurado para conectar-se à porta na qual o proxy HTTP está recebendo.

Se estiver utilizando HTTPS, indique o proxy HTTP no IBM Firewall também para o proxy de segurança.

Se deseja representar seu navegador Internet Explorer como um navegador HTTP/1.1 para o proxy, faça o seguinte:

- Abra o menu suspenso *Exibir*.
- Selecione *Opções de Internet*.
- Selecione o *Avançar Item*.
- Desloque-se até as definições do HTTP 1.1 e as ative.

Conexões SSL

A criação de túneis SSL para a Conexão Protegida HTTP a outros servidores é aceita. Neste caso, o IBM Firewall age como um gateway. O túnel vai do cliente, pelo firewall, até o servidor. Utilize a porta padrão 443 para Conexão Protegida HTTP conforme ilustrado no seguinte exemplo:

```
https://www.ibm.com:443
```

Além disso, utilize o serviço pré-definido `HTTPS proxy out 2/2`.

Se estiver utilizando HTTPS, indique o proxy HTTP no IBM Firewall também para o proxy de segurança.

Para maiores informações, consulte “Exemplo de Proxy HTTP” na página 55.

Métodos Aceitos

O proxy HTTP aceita os seguintes métodos, que são maneiras diferentes de se consultar a Internet:

- FTP
- Gopher
- HTTP
- HTTPS
- WAIS

Exemplo de Saída de Registro para Proxy HTTP

Segue abaixo um exemplo da saída de log para pedidos get autenticados do Proxy HTTP.

```
Mar 06 14:04:50 1998 fire3: ICA2140i: httpd -->
Autenticação Proxy HTTP NÃO OBTEVE SUCESSO
para usuário <Desconhecido>, no 9.67.140.162, pela rede protegida ... RC:30.
Mar 06 14:04:50 1998 fire3: ICA2099i: httpd --> Status: 407 do cliente
9.67.140.162, que solicitou "GET http://9.67.128.69/ HTTP/1.1" para 0 bytes.
Mar 06 14:05:05 1998 fire3: ICA2024i: Usuário fred autenticado com sucesso
utilizando a autenticação NT a partir da rede protegida:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2169i: Usuário fred autenticado com sucesso
para o Servidor HTTP utilizando NT a partir da rede protegida:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> Autenticação do Proxy HTTP
OBTEVE SUCESSO para o usuário, no 9.67.140.162, pela rede prot. ...RC:1.
Mar 06 14:05:05 1998 fire3: ICA2099i: httpd --> Status: 200 do cliente
9.67.140.162, que solicitou "GET http://9.67.128.69/HTTP/1.1"
para 2693 bytes.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> Autenticação do Proxy HTTP
OBTEVE SUCESSO para o usuário, no 9.67.140.162, pela rede prot....RC:1.
Mar 06 14:05:06 1998 fire3: ICA2099i: httpd --> Status: 200 do cliente
9.67.140.162, que solicitou "GET http://9.67.128.69/Admin/lgsplash.gif
HTTP/1.1" para 211 bytes.
Mar 06 14:05:10 1998 fire3: ICA2140i: httpd --> Autenticação Proxy HTTP
OBTEVE SUCESSO para o usuário, no 9.67.140.162, pela rede prot. ...RC:1.
Mar 06 14:05:10 1998 fire3: ICA2099i: httpd --> Status: 200 do cliente
9.67.140.162, que solicitou "GET http://9.67.128.69/Admin/lgmast.gif
HTTP/1.1" para 211 bytes.
```

A atividade de log é explicada da seguinte forma:

- ICA2099i - mostra um código de retorno de 407 e significa que houve falha de autenticação para o pedido get.

  O navegador, então, solicita ao usuário alguma autenticação. O navegador pede uma id de usuário e senha.

- ICA2140i - a autenticação obteve sucesso para o usuário fred.

A autenticação ocorre em cada pedido get para cada elemento na página Web.

FTP

1. Utilize o proxy FTP para acessar o host do firewall. (Utilizaremos `ftp_gw.domain.net.com` como nome do host para o firewall).

   ```
   ftp ftp_gw.domain.net.com
   ```

   O servidor proxy irá solicitar seu nome de usuário:

   ```
   início de sessão:
   ```

2. Forneça seu nome de usuário autorizado a utilizar o Firewall:

   ```
   login: jane_doe
   ```

O servidor valida sua identidade dependendo do esquema de autenticação selecionado quando seu nome de usuário foi incluído no Firewall (consulte “Inclusão de um Usuário no IBM Firewall” na página 75). Consulte “Métodos de Autenticação” na página 85 para obter informações sobre como usuários são autenticados por servidores proxy.

Após a sua autenticação, o servidor proxy exibe um prompt de comando FTP.

```
ftp>
```

Utilize os comandos `quote` e `site` do FTP para conectar-se ao host estrangeiro:

```
ftp> quote site forhost.network.outside.com
```

O host estrangeiro irá solicitar um nome de usuário e senha para você conectar-se. Este é provavelmente um nome de usuário e senha diferentes daqueles utilizados para FTP no Firewall.

O padrão do valor de timeout para login é 60 segundos e para o proxy inativo é 7200 segundos. Para alterar os valores de timeout padrões, consulte “Substituição de Valores de Timeout em Proxies FTP e Telnet” na página 96.

FTP Transparente

Você pode fazer um ftp de maneira transparente através do Firewall. Os proxies transparentes não requerem autenticação do firewall, sendo assim usuários de proxies transparentes não precisam ser definidos como usuários de proxy do firewall. Os proxies transparentes só são permitidos a partir do lado protegido do firewall indo para o lado não-protegido do firewall. Para que o proxy transparente funcione, é necessário selecioná-lo no painel do cliente de configuração Regulamento de Segurança.

1. Utilize ftp para acessar o host do firewall. (Utilizaremos `ftp_gw.domain.net.com` como nome do host para o firewall.)

   ```
   ftp ftp_gw.domain.net.com
   ```

2. O servidor proxy irá solicitar seu nome de usuário:

   ```
   USUÁRIO:
   ```

3. Forneça seu nome de usuário na rede não-protegida:

   ```
   USUÁRIO: usernameÃremote_site_host_name
   ```

4. Então, o host de destino irá solicitar sua senha do `nome de usuário` fornecido na etapa anterior.

```
password:
```

5. Digite a sua senha.

O padrão do valor de timeout para login é 60 segundos e para o proxy inativo é 7200 segundos (duas horas). Para alterar os valores de timeout padrões, consulte “Substituição de Valores de Timeout em Proxies FTP e Telnet” na página 96.

Telnet

Utilize o proxy telnet para conectar-se ao servidor proxy do firewall. Você pode utilizar o nome do host ou endereço da Internet. E então, depois que suas credenciais forem autenticadas, você utiliza o comando telnet no Firewall para conectar-se ao host pretendido. Por exemplo, vamos utilizar telnet de dentro da rede protegida, através do Firewall, com o nome de host de `telnet_gw`, para acessar seu destino definitivo, `forhost.network.outside.com`.

1. Para iniciar o processo, utilize o telnet para acessar o host do firewall. (Utilizaremos telnet_gw.domain.net.com como o nome do host para o Firewall.)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. O servidor proxy irá solicitar seu nome de usuário:

   ```
   início de sessão:
   ```

3. Forneça seu nome de usuário autorizado a utilizar o Firewall:

   ```
   login: jane_doe
   ```

O servidor valida sua identidade dependendo do esquema de autenticação selecionado quando seu nome de usuário foi incluído no Firewall (consulte “Inclusão de um Usuário no IBM Firewall” na página 75). Consulte “Métodos de Autenticação” na página 85 para obter informações sobre como usuários são autenticados por servidores proxy.

Você irá utilizar a shell oneact. Com o daemon de telnet do proxy do IBM Firewall, todas as comunicações passam através do firewall.

Se estiver utilizando a shell oneact, depois de você ser autenticado, o servidor proxy exibe:

```
ENTER DESIRED HOST:
```

Digite

```
telnet forhost.network.outside.com
```

O host estrangeiro solicita seu nome de usuário e senha, do modo como é conhecido naquele host. Estes podem ser diferentes do nome de usuário e senha utilizados no servidor proxy do firewall.

O padrão do valor de timeout para login é 60 segundos e para o proxy inativo é 7200 segundos. Para alterar os valores de timeout padrões, consulte “Substituição de Valores de Timeout em Proxies FTP e Telnet” na página 96.

Telnet Transparente

Você pode fazer um telnet de maneira transparente através do Firewall. Proxies transparentes não requerem autenticação firewall, o que elimina a necessidade de definir os proxies transparentes como usuários proxy firewall. Os proxies transparentes só são permitidos a partir do lado protegido do Firewall indo para o lado não protegido do Firewall. Para que o proxy transparente funcione, é necessário selecioná-lo no painel do cliente de configuração Regulamento de Segurança.

1. Utilize telnet para acessar o host do firewall. (Utilizaremos `ftp_gw.domain.net.com` como nome do nosso host.)

   ```
   telnet telnet_gw.domain.net.com
   ```

2. O servidor proxy irá solicitar seu nome de usuário:

   ```
   Login:
   ```

3. Forneça seu nome de usuário na rede não-protegida:

   ```
   LoginÃremote_host
   ```

O host estrangeiro solicita seu nome de usuário e senha, do modo como é conhecido naquele host. Estes podem ser diferentes do nome de usuário e senha utilizados no servidor proxy do firewall.

O padrão do valor de timeout para login é 60 segundos e para o proxy inativo é 7200 segundos. Para alterar os valores de timeout padrões, consulte “Substituição de Valores de Timeout em Proxies FTP e Telnet”.

Substituição de Valores de Timeout em Proxies FTP e Telnet

O FTP e o Telnet possuem valores de timeout para esperas de início de sessão e inatividade. Por padrão, deverá haver atividade na sessão por pelo menos uma vez a cada 60 segundos durante a autenticação de início de sessão e do usuário. Este é conhecido como o loginTimeout.

Depois de concluído com sucesso o início de sessão, deverá haver atividade na sessão por pelos menos uma vez a cada 7200 segundos ou a sessão será desconectada.

Você pode substituir estes padrões criando um arquivo `fwTimeout.cfg` no diretório `ROOTDIR\config` especificando novos valores de timeout em segundos. O arquivo `fwTimeout.cfg` deverá ter o seguinte formato.

```
telnet
proxyTimeout=7200
loginTimeout=60

ftp
proxyTimeout=7200
loginTimeout=60
```

Capítulo 14. Monitoramento dos Registros do Firewall

Este capítulo explica como monitorar os registros dos alertas em tempo real. Um alerta será gerado quando um limite configurado for violado.

O IBM Firewall monitora as mensagens enviadas ao log do firewall para situações de crise em potencial, com base em limites definidos pelo usuário. No evento de uma violação de limite, Firewall envia um alerta, do modo especificado pelo administrador do firewall.

Definições de Limites

Limites consistem em parâmetros de contagem e tempo — se uma contagem (número de eventos específicos) for ultrapassada no período especificado (minutos), o limite terá sido violado e uma mensagem de alerta será gerada. O monitor de registros reconhece quatro tipos de limites:

1. Falhas totais de autenticação
2. Falhas de autenticação em relação a uma ID de usuário em particular
3. Falhas de autenticação originárias de um host em particular
4. Ocorrências de códigos de mensagens no registro

Todos os limites podem ser configurados utilizando o cliente de configuração ou a interface de linha de comando. Qualquer alteração nas definições de limite é automaticamente selecionada pelo IBM Firewall.

Mensagens de Alerta

Quando um limite é atingido, o IBM Firewall gera uma mensagem de alerta. A entrega da mensagem de alerta pode ter um dos seguintes quatro formatos:

1. Entrada em um arquivo de registros:
   - Através do recurso `log de alerta` configurável através do cliente de configuração ou a linha de comando.
   - No `log do firewall`
2. Envie uma mensagem de e-mail para uma lista de usuários
3. Pager, conforme configurado. Consulte “Suporte de Notificações do Pager” na página 99.
4. Execução de um comando definido pelo usuário, com a mensagem de alerta como primeiro parâmetro

A mensagem de alerta contém informações relevantes a violação de limite em particular. Por exemplo:

```
ICA0001e: ALERTA – 20 falhas de autenticação.
ICA0002e: ALERTA – 10 falhas de autenticação para usuário raiz.
ICA0003e: ALERTA – 15 falhas de autenticação do host 56.67.78.89
ICA0004e: ALERTA – Código ICA1234e com 3 entradas de registro.
```

Mensagens de alerta e outras mensagens originárias do Monitor de Logs não são monitoradas.

Configuração do Monitor de Registros Utilizando o Cliente de Configuração

Esta seção descreve como utilizar o cliente de configuração para configurar o monitor de registros em tempo real. Selecione Logs do Sistema a partir da árvore de navegação do cliente de configuração. Dê um clique duplo sobre o ícone da pasta de arquivo para expandir a exibição. Clique em **Limiares do Monitor de Logs**.

Na caixa de diálogo **Administração do Limite do Monitor de Logs** é possível incluir, alterar ou eliminar definições de limites.

Inclusão de Monitor de Log

Para incluir uma definição de limite, selecione **NOVO** na caixa de diálogo **Administração do Limite do Monitor de Logs** e clique em **Abrir**. Aparece a caixa de diálogo **Incluir Monitor de Log**. Preencha os seguintes campos:

1. Clique na seta **Tipo de classe** para escolher pela lista de tipos de classe. Os tipos de classe são:
   - Notificação de Correspondência
   - Comando executar
   - Limite de Falha de Autenticação Por Usuário
   - Limites de Falha da Autenticação Total
   - Limite de Falha de Autenticação Por Host
   - Limite da Mensagem
2. Se tiver selecionado o tipo de classe: Notificação de Correspondência, forneça um endereço de e-mail. Diversas classes de notificação de correspondência podem ser definidas.

   Todas as mensagens de violação de limite são enviadas ao endereço de e-mail especificado.
3. Se tiver selecionado o tipo de classe: Comando Executar, preencha um nome de arquivo do comando.

   O monitor de registros irá executar este comando com a mensagem de alerta como sendo seu primeiro parâmetro. Somente uma classe do comando executar pode ser definida.
4. Se tiver selecionado o tipo de classe: Limite da Mensagem, preencha um código de mensagem, um código padrão das mensagens de registro do IBM Firewall que deseja que seja monitorado.
5. Se tiver selecionado uma das classes de limite, preencha o campo de contagem de limite.

   A contagem de limite é o número máximo de eventos com falhas permitido dentro de um período especificado.
6. Se tiver selecionado uma das classes de limite, preencha o campo período de limite.

   O período de limite é o número de minutos começando com a primeira ocorrência de um evento.

7. Se tiver selecionado uma das classes de limite, clique em Sim ou Não para indicar se deseja que a notificação do pager esteja ativa.
8. A colocação de um comentário é opcional.
9. Clique em **OK**.

Alteração de Definição de Limite

Para mudar uma definição de limite, selecione o item a ser modificado na caixa de diálogo **Administração do Limite do Monitor de Logs** e clique em **Abrir**. Aparece a caixa de diálogo **Alterar Monitor de Logs**.

1. Forneça as alterações que deseja para os campos contagem de limite e período de limite.

   A contagem de limite é o número máximo de mensagens de autenticação falhas a serem detectadas dentro de um período de tempo especificado. O período de limite é o número de minutos começando com a primeira ocorrência de um mensagem.

2. Clique em **OK**.

Eliminação de Definição de Limite

Para eliminar uma definição de limite, selecione o item a ser eliminado na caixa de diálogo **Limiares do Monitor de Logs** e clique em **Eliminar**. Você será solicitado a confirmar a eliminação. Clique em **Sim** para confirmar. Observe que eliminar não significa eliminar do arquivo de registros. Significa eliminar a definição.

Suporte de Notificações do Pager

O Firewall pode chamar o administrador do sistema, enviando mensagem ao pager do administrador quando houver alertas de intrusão no Firewall. Para configurar o suporte de notificação do pager, é necessário configurar os seguintes três componentes de pager.

1. Personalização de Comando - Este componente deve ser criado e modificado através do cliente de configuração. Este define os padrões para o comando do pager, o qual é usado pelo monitor de log e pode ser usado a partir da linha de comando. Este componente possuirá uma entrada exclusiva que define o ambiente do pager. Consulte “Personalização de Comando” na página 101 para maiores informações sobre a definição e personalização deste componente.
2. Administração da Operadora - É necessário definir uma operadora adequada antes de conectar seu modem. Este componente contém uma lista de três operadoras padrões utilizadas nos EUA. Se a operadora que está utilizando não é nenhuma destas, inclua-a neste componente. Consulte “Administração da Operadora” na página 102 para maiores informações.

   Valide os números de telefone existentes para as operadoras obtendo estes números de suas operadoras. Ao comunicar-se com as operadoras, não deixe de pedir o número de telefone do modem da operadora, junto com outras definições que são válidas para o serviço em particular que foi adquirido.
3. Administração do Modem - Antes de conectar o seu modem, é necessário que você crie definições de modem adequadas. Estas definições irão conter todas as informações do modem relevantes que o suporte de notificação do pager irá

utilizar. Este componente contém uma lista de modems a partir da qual pode fazer sua escolha. Essa lista pode sofrer acréscimos, mas alguns modems podem não ser compatíveis com o suporte da operadora. Consulte “Administração do Modem” na página 103 para obter informações sobre a manutenção de definições do modem.

Nota: O IBM Firewall suporta o protocolo de comunicação TAP (Tele-AlphaNumeric Protocol) para suporte de notificação do pager.

Quais Operadoras e Modems são Suportados

O arquivo de banco de dados das operadoras contém uma lista de operadoras e parâmetros de transmissão relacionados. Você pode incluir outras operadoras. Alguns dos parâmetros além do nome da operadora e número de telefone do modem são:

- O comprimento de mensagem máximo para um pager alfanumérico e o máximo de dígitos para um pager numérico
- O comprimento dos bits da velocidade de transmissão, paridade, dados e bits de parada

Antes de utilizar uma determinada operadora, certifique-se de que a operadora utiliza o protocolo TAP.

O código do pager vêm com definições padrões do modem. Estas são:

- IBM MOD 448 14400 bps
- IBM 5853 2400 bps
- IBM 7852 28800 bps
- IBM 7855 2400 bps
- Compatível com Generic Hayes
- US Robotics Courier 9600 bps
- Zoom V.34

Configuração do Suporte de Notificação do Pager

A Configuração do Pager é usada para configurar o arquivo de personalização de comando e para manter operadoras e modems. Se estiver utilizando um pager, você deve utilizar Configuração do Pager para personalizar o ambiente do pager antes de utilizar o Monitor de Registro.

Antes de iniciar, você necessita obter os números corretos do fone de modem, ID do pager e parâmetros do modem de sua operadora.

Para configurar o suporte de notificação do pager, selecione Administração do Sistema a partir da árvore de navegação do cliente de configuração. Dê um clique duplo sobre o ícone da pasta de arquivo para expandir a exibição. Selecione **Logs do Sistema**. Dê um clique duplo sobre o ícone da pasta de arquivo para expandir a exibição. Selecione **Configuração do Pager**.

Personalização de Comando

Quando se seleciona **Configuração do Pager**, pode-se selecionar uma operadora e um modem para utilizar e gravar mensagens do pager.

Definições da Personalização de Comando

Quando se seleciona **Configuração do Pager** na árvore de navegação, obtém-se uma caixa de diálogo **Configuração do Pager** com Definições da Personalização de Comandos semelhantes às da caixa de diálogo mostrada na Figura 26.

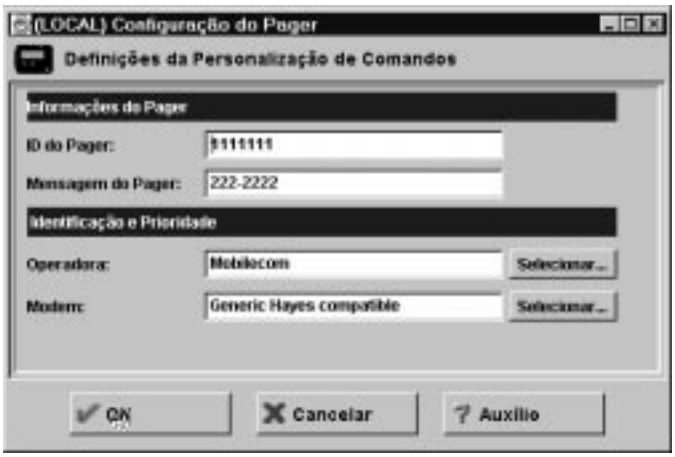


Figura 26. Configuração do Pager

Digite ou selecione valores nos campos de entrada a serem incluídos.

1. Forneça a ID do pager. Geralmente, trata-se de um número PIN exclusivo atribuído ao seu pager por sua empresa operadora.
2. Forneça a mensagem do pager. Esta é uma cadeia contendo a mensagem padrão que o usuário deseja enviar. No caso de pager numéricos, ela só pode ser um número. Para pagers alfanuméricos, pode ser uma mensagem de texto. Não ultrapasse o tamanho máximo de mensagem especificado na configuração de sua operadora ou sua mensagem poderá ficar truncada. Não utilize dois pontos (:). Caso utilize, ele será substituído por um espaço em branco.
3. Se não houver nome de operadora, clique em **Selecionar** para definir uma. Aparecerá a caixa de diálogo **Administração da Operadora do Pager**. Leia “Administração da Operadora” na página 102 para saber como preencher o painel.
4. Se não houver nome de modem, clique em **Selecionar** para defini-lo. Aparecerá a caixa de diálogo **Administração do Modem do Pager**. Leia “Administração do Modem” na página 103 para saber como preencher o painel.
5. Clique em **OK**.

Alteração da Personalização do Comando

Quando se selecionar Configuração do Pager na árvore de navegação aparece a caixa de diálogo **Configuração do Pager** com Definições da Personalização de Comandos.

1. Digite ou selecione valores nos campos de entrada para modificar os valores dos campos de entrada de personalização existentes.

2. Clique em **OK**.

Eliminação da Personalização do Comando

1. Para eliminar uma entrada da caixa de diálogo **Administração da Operadora do Pager** ou da caixa de diálogo **Administração do Modem do Pager**, selecione o item na lista e dê um clique duplo em **Eliminar**.

   Você será solicitado a confirmar a eliminação.

2. Clique em **Sim** para confirmar a eliminação ou em **Não** para voltar à caixa de diálogo **Configuração do Pager**.

Se não existir nenhuma entrada de personalização, o suporte de notificação do pager não terá condições de enviar uma mensagem via pager.

Administração da Operadora

Na caixa de diálogo **Configuração do Pager**, passe para o campo do nome da operadora e clique em **Selecionar**. Aparece uma caixa de diálogo **Administração da Operadora do Pager** semelhante à mostrada no Figura 27.

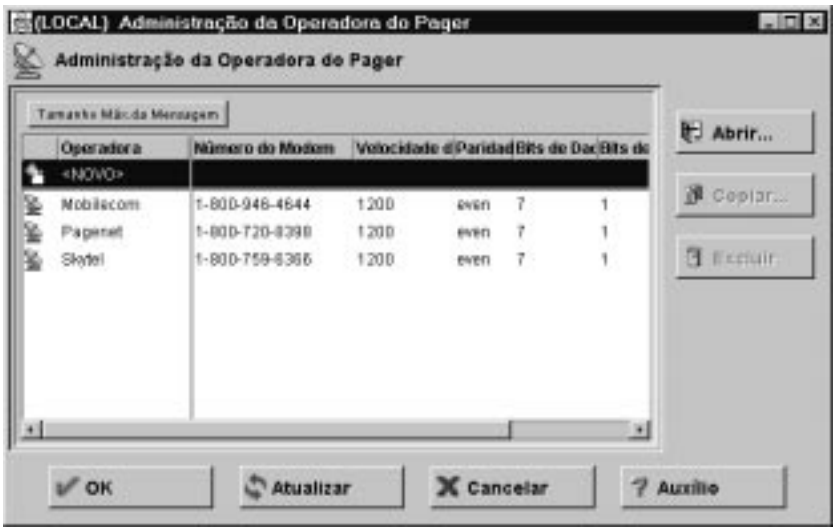


Figura 27. Administração da Operadora do Pager

Inclusão de uma Operadora

Para incluir uma nova operadora, selecione **NOVO** na caixa de diálogo **Administração da Operadora do Pager** e clique em **Abrir**. Digite ou selecione valores nos campos de entrada apropriados:

1. Forneça o nome do operador. Pode ser qualquer coisa contanto que seja exclusivo e forneça informações suficientes para que seja possível reconhecer de que operadora se trata.
2. Forneça o número de telefone da operadora, que é o número de telefone para um modem na empresa da operadora, em oposição ao paging de voz e outro número de serviço. Deve ser o número de modem correto para a região ou extensão nacional e para um pager numérico ou alfa, conforme o solicitado pelo dispositivo de paging e o serviço contratado por você.
3. Digite o TAP para o método de paging; o único valor permitido.

4. Forneça a senha se a operadora permitir ou solicitar uma.
5. Forneça o comprimento de mensagem máximo para um pager alfanumérico e o máximo de dígitos para um pager numérico
6. Forneça a Velocidade de Transmissão. Clique na seta e escolha um valor da lista.
7. Clique em **Par**, **Ímpar** ou **Nenhum** para o campo de paridade.
8. Escolha os bits de dados padrão; clique em **7** ou **8**.
9. Escolha dos bits de parada padrão: clique em **1** ou **2**.
10. Clique em **OK**.

Alteração de Operadora

1. Selecione a operadora a ser alterada na caixa de diálogo **Administração da Operadora do Pager** e clique em **Abrir**.
2. Consulte “Inclusão de uma Operadora” na página 102 para obter uma explicação dos campos que podem ser alterados. O nome da operadora em si não pode ser alterado. Este campo será desativado.
3. Faça as alterações desejadas.
4. Clique em **OK**.

Eliminação de Operadora

1. Selecione a operadora a ser eliminada na caixa de diálogo **Administração da Operadora do Pager** e clique em **Excluir**.
2. Você será solicitado a confirmar a eliminação. Clique em **Sim** para confirmar.

   Nota: O banco de dados da operadora deve sempre conter, ao menos, uma operadora. Se nenhuma operadora estiver definida, o suporte de notificação do pager irá falhar.

Administração do Modem

Seu manual do modem conterá todas as informações relevantes sobre como inicializá-lo. Você poderá necessitar coordenar definições do modem com sua operadora. Em geral, somente modems compatíveis ao Hayes, que utilizam os comandos de modem padrão são suportados.

Na caixa de diálogo **Configuração do Pager**, passe para o campo do nome do modem e clique em **Selecionar**. Aparece uma **Administração do Modem do Pager** similar àquela mostrada em Figura 28 na página 104.

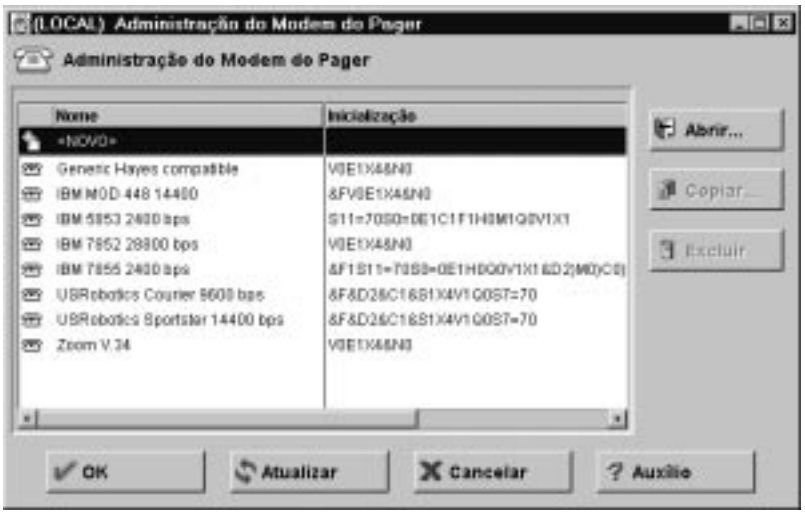


Figura 28. Administração do Modem do Pager

Você pode incluir ou eliminar vários modems usando esta caixa de diálogo.

Inclusão de um Modem

Para incluir um novo arquivo de definição de modem, selecione **NOVO** na caixa de diálogo **Administração do Modem do Pager** e clique em **Abrir**. Na caixa de diálogo **Incluir Modem**, digite ou selecione valores nos campos de entrada.

1. Forneça o nome do modem. Pode ser qualquer coisa contanto que seja exclusivo em relação a outras definições e forneça informações suficientes para que seja possível reconhecer de que modem se trata.
2. Forneça o número da Porta COM, que define a Porta COM, em série, à qual o modem está anexado. Forneça um número menor que 10. Embora o modem deva ser configurado no hardware para esta porta, ele não deve ser definido para Windows NT, pois nesse caso o acesso às funções por essa porta será negado. Se o modem não estiver de acordo com as definições do hardware, o código do pager irá ficar tentando por um longo período e eventualmente falhará.
3. Forneça a cadeia de inicialização, que deve definir o modem como um modem de dados com um eco no X level4 e uma velocidade de transmissão fixa definida pelo site local. Não inclua o comando AT. A função do pager irá colocá-lo no início da cadeia de inicialização.
4. Forneça o prefixo de linha externo. Este é o número que você disca para chamadas fora da empresa.
5. Clique em **OK**.

Alteração do Modem

1. Selecione um nome de modem na caixa de diálogo **Administração do Modem do Pager** e clique em **Abrir** para mudar o arquivo de definição de modem.

   Na caixa de diálogo **Alterar Modem** aparecerá a lista dos campos da definição do modem que podem ser alterados. Consulte “Inclusão de um Modem” para obter explicações sobre estes campos.
2. Clique em **OK**.

Eliminação de Modem

1. Selecione um nome de modem na caixa de diálogo **Administração do Modem do Pager** e clique em **Eliminar** para apagar o arquivo de definição de modem.
2. Você será solicitado a confirmar a eliminação. Clique em **Sim** para confirmar.

Registro da Notificação do Pager

O processo de notificação do pager utiliza o utilitário de registro do firewall para gravar registros de saída. Todas as mensagens e erros do pager são gravados no recurso geral syslog do Firewall Para maiores informações sobre como configurar e utilizar os arquivos de registro do firewall, consulte Capítulo 15, “Gerenciamento de Arquivos de Log e Compactados” na página 107.

Teste da Configuração do Pager

Para verificar a configuração do pager, use o comando `pager`. Consulte o manual *IBM eNetwork Firewall Referência* para obter detalhes. É altamente recomendado que se utilize o comando do pager sempre que a configuração for definida ou alterada para certificar-se de que os dispositivos do sistema, modem, operadora e pager estão comunicando-se uns com os outros adequadamente e de que envios e recepções podem ser realmente efetuados.

Executar Comandos

Pode-se especificar um programa que seja chamado toda vez que um limite de alerta é alcançado. Para isso:

1. Clique em **Administração do Monitor de Logs** e depois dê um clique duplo em **NOVO**.

   Aparece a caixa de diálogo **Incluir Monitor de Log**.

2. Na caixa suspensa **Tipo de Classe**, selecione **Executar Comando**. O campo **Nome de Arquivo do Comando** do painel é ativado.

3. No campo **Nome de Arquivo do Comando**, digite o nome de caminho completo do programa a ser chamado quando o limite de alerta é atingido.

   O diretório de trabalho para os comandos executados pelo monitor de log é `\winnt\system32`. Como a shell de comando é lançada a partir de um processo do sistema, somente variáveis de ambiente do sistema são definidas. Variáveis de ambiente do usuário não são definidas. Geralmente, o programa lançado deve utilizar nomes de arquivo inteiramente qualificados ao invés de confiar nas variáveis de caminho.

   O Firewall vai passar a mensagem de Alerta completa como primeiro parâmetro do programa:

   ```
   Total de Alertas de Falha de Autenticação: ICA0001e
   Alertas de Falha de Autenticação por Usuário: ICA0002e
   Alertas de Falha de Autenticação por Host: ICA0003e
   Alertas de Limite da Mensagem: ICA0004e
   ```

Consulte o *Referência ao IBM eNetwork Firewall* para ver a descrição completa das mensagens.

Capítulo 15. Gerenciamento de Arquivos de Log e Compactados

Este capítulo descreve como utilizar os dispositivos de log no cliente de configuração. A medida que usuários tentam acessar hosts através de vários servidores do IBM Firewall, o IBM Firewall grava entradas no arquivo de logs mantido pelo `serviço de registro do IBM Firewall`.

O IBM Firewall pode gerar volumes grandes de informações de registro dependendo de como o firewall estiver configurado. Entradas de log podem vir de uma variedade de lugares como soquetes e filtros expert. Além do mais, os arquivos de log podem ser gravados numa grande variedade de níveis de gravidade - como *depuração, informação* ou *erro*. Este capítulo também explica como utilizar os recursos de gerenciamento de log e do gerenciamento dos arquivos compactados para gerenciar o tamanho do seus arquivos de log e compactados.

Criação, Colocação e Compactação do Arquivo de Log Utilizando o Cliente de Configuração

O cliente de configuração pode ser utilizado para gerenciamento de registro e gerenciamento de fichário. Supõe-se que o seu disco tenha espaço em disco disponível suficiente para conter todas as informações de registro. O Firewall gera depuração de rotina e informação de erros no recurso `log do firewall`. Somente o administrador de firewall primário possui acesso ao recurso `log do firewall`. Mensagens de alerta vão para o registro de alerta . Informações administrativas de log de auditoria vão para o log de auditoria .

Para que os utilitários de relatório funcionem corretamente, é importante que somente mensagens do log do firewall apareçam em seus arquivos de entrada. Nenhum outro recurso deve ser direcionado para o mesmo arquivo que o `log do firewall` para definir o log de firewall de acordo.

Se você deseja ver alertas no painel de cliente de configuração central, você tem de direcionar seus alertas para um arquivo designado como um recurso `log de alerta`. Nada mais deve ser designado para este arquivo.

Os seguintes níveis de prioridade se somam à *depuração* que captura a maioria das informações. O *crítico* captura apenas os eventos mais graves do firewall.

- Depuração
- Informação
- Advertência
- Erro
- Crítico

Sugerimos começar pelo nível *informação* até os procedimentos do firewall ficarem estáveis. Depois passe para *aviso* ou *erro* para reduzir a atividade de registro e o tamanho do log do sistema.

Os níveis de prioridade não correspondem precisamente ao sufixo de tag de mensagem *(i,e,w,s..)*. Talvez seja necessário testar para determinar como *encerrar* algumas mensagens.

Inclusão de Recursos de Log

A partir da árvore de navegação do cliente de configuração, dê um clique duplo no ícone da pasta do arquivo Administração do Sistema para expandir a exibição. Dê um clique duplo no ícone da pasta do arquivo Logs do Sistema para expandir a exibição. Selecione Dispositivos de Log. Aparece a caixa de diálogo **Recursos de Log** mostrando o conjunto de recursos de log que se encontram ativados.

1. Selecione **NOVO** na caixa de diálogo **Recursos de Log** e clique em **Abrir** para acrescentar uma entrada de syslog às que já estão ativadas.

   Aparece a caixa de diálogo **Incluir Recursos de Log**, como mostra o Figura 29.

Figura 29. Incluir Recursos de Log

2. Clique na seta **Tipo** para selecionar o tipo. O tipo é Nome do Arquivo.
3. O Dispositivo de Log determina o tipo e a origem das informações que são registradas. Clique na seta **Recurso** para selecionar um dos seguintes recursos de log:
   - Log do Firewall - logs gerais do firewall, incluindo registro de filtragem
   - Log de Alerta - status do daemon do monitor de log e avisos de violação de limites usados para preencher a Exibição de Alertas
   - Log cronológico
4. Clique na seta **Prioridade** para escolher a prioridade. As prioridades de registro são listadas em ordem crescente de gravidade. A prioridade selecionada será o nível mínimo a ser registrado.
5. Preencha o nome de arquivo do log. O nome de arquivo do log deve ter um caminho absoluto (começando com a unidade e uma barra invertida \) e o caminho do nome de arquivo tem que existir.

6. O Gerenciamento do Arquivo Compactado só pode ser usado com recurso de log do tipo do *nome do arquivo*. Quando ativado, o tamanho do arquivo de logs pode ser periodicamente reduzido. Ativar o gerenciamento do arquivo compactado significa que são definidos parâmetros dos quais depende o comando `fwlogmgmt`. Consulte “Compactação de Logs”. Você pode ativar ou desativar parâmetros de gerenciamento de arquivos compactados.
7. Selecione o número de dias inteiros que devem transcorrer até o(s) registro(s) de um log ativo serem compactados. O valor deve ser maior ou igual a zero. A compactação de registros vai ocorrer quando o comando `fwlogmgmt -l` encontrar registros de log ativos que atendem aos requisitos dos critérios. O gerenciamento de log não inclui a data do dia ao calcular o número de dias que os registros são mantidos.
8. Forneça um nome de arquivo de arquivo compactado e um caminho completo. O IBM Firewall fornece uma função de fichário padrão, que utiliza um diretório. No entanto, você pode utilizar funções de compactação plug-in, se desejar.
9. Selecione o número de dias inteiros que devem transcorrer até o arquivo de logs arquivado ser eliminado do arquivo compactado. O valor deve ser maior ou igual a zero. A depuração vai ocorrer quando o comando `fwlogmgmt -a` encontrar arquivo(s) compactado(s) que atendem aos requisitos dos critérios. O gerenciamento de log não inclui an data do dia ao calcular o número de dias que o arquivo acumulado é mantido.
10. Clique em **OK**.

Alteração de Recursos de Log

1. Selecione na caixa de diálogo **Recursos de Log** a entrada a ser modificada e clique em **Abrir**.

   Aparece a caixa de diálogo **Alterar Recursos de Log**.
2. Altere os campos desejados. Consulte “Inclusão de Recursos de Log” na página 108 para obter uma explicação dos campos.
3. Clique em **OK**.

Eliminação de Recursos de Log

1. Selecione na caixa de diálogo **Recursos de Log** uma entrada dentre as que estão ativadas e clique em **Excluir**.

   Aparece o painel **Excluir Advertência**.
2. Clique em **OK** para continuar fazendo a eliminação. Clique em **Cancelar** se mudar de idéia. Isto não elimina o arquivo de registro em si.

Compactação de Logs

O processo de compactação:

- Remove de log ativo registros que atendem aos requisitos
- Coloca-os num arquivo separado
- Compacta o arquivo resultante
- Coloca o novo arquivo num diretório de arquivos compactados

Para iniciar um programa de gerenciamento de arquivos para arquivar registros de log acumulados, você tem duas opções:

1. Execute o comando `fwlogmgmt -l` pela linha de comandos de tempos em tempos ou
2. Configure o comando `fwlogmgmt -l` como um Serviço Programado NT.

A depuração dos arquivos de log consiste em eliminar do diretório de arquivos compactados os arquivos que atendem aos requisitos.

Para eliminar os arquivos compactados você possui duas opções:

1. Executar o comando `fwlogmgmt -a` pela linha de comandos de tempos em tempos ou
2. Configurar o comando `fwlogmgmt -a` como um Serviço Programado NT.

Os registros e arquivos que atendem aos requisitos são determinados pelos valores especificados nas definições dos recursos de log descritas no “Inclusão de Recursos de Log” na página 108.

O meio mais eficiente ou conveniente de se executar este processo de gerenciamento de log seria configurando-o como um Serviço Programado NT. Inicie-o utilizando o objeto Serviços no painel de controle.

Por exemplo, se desejar configurar o processo de compactação do gerenciamento de log de tal modo que seja executado todos os dias às 3:00 AM, digite

```
at 3:00 /every:M,T,W,Th,F,S,Su fwlogmgmt -l
```

Plug-in DLL

Consulte o *IBM eNetwork Firewall Reference* para obter informações sobre a DLL plug-in do fichário de log que pode ser utilizada para substituir a DLL padrão do Firewall.

Saídas de Gerenciamento de Registros

O recurso de gerenciamento de registro efetua algumas verificações de integridade preliminares antes de continuar qualquer atividade de gerenciamento do registro. Se algum problema for encontrado, os diagnósticos são enviados ao firewall quando se executa o comando `fwlogmgmt` a partir da linha de comando.

Os recursos de log Mail ou admin audit (local0) estão sujeitos a regras de arquivo diferentes das de outros recursos. Todos os recursos de log requerem que a compactação de registros esteja ativado para que sejam compactados. No entanto, os registros de log do firewall (local4) e alerta (local1) só são compactados se suas datas excederem critérios especificados na definição dos recursos na hora que o processo de compactação é executado; ao passo que o arquivo de log *inteiro* de correspondência ou auditoria será compactado a cada vez. Além disso, as informações no log de correspondência são consideradas como sendo para fins de depuração e, geralmente, há pouco valor em sua compactação. Outras informações de correspondência, geralmente mais úteis, são registradas no log do firewall (local4).

Utilitários de Relatório

As funções do utilitário de relatório podem ser utilizadas para auxiliar na geração de relatórios dos arquivos de log atuais ou compactados. Os utilitários de relatório geram arquivos tabulares de informações administrativas que são organizadas e formatadas de modo a facilitar o mapeamento para tabelas de bancos de dados relacionais. Estas tabelas ajudam o administrador do firewall analisar:

- Uso geral do Firewall
- Erros no processo do firewall
- As tentativas de acesso não-autorizado à rede protegida

Usando os utilitários e o log do firewall, o administrador pode criar um arquivo de texto comum com as mensagens. Além disso, os arquivos tabulados podem ser gerados e importados para tabelas em um sistema de banco de dados relacional, como a família de produtos DB2. O administrador pode então usar a Structured Query Language (SQL) para consultar dados e gerar relatórios.

Os Utilitários de Relatório são instalados como parte da instalação do Firewall. Eles também podem ser instalados separadamente e executados num host não-firewall. O cliente de configuração pode ser usado para executá-los em um firewall. Em máquina não-firewall, use a linha de comandos.

Para que os utilitários de relatório funcionem corretamente, é importante que somente mensagens de `log do firewall` apareçam em seus arquivos de entrada. Nenhum outro recurso deve ser direcionado para o mesmo arquivo que o `log do firewall`, então, leve isto em consideração para definir o registro do firewall.

Não tente usar utilitários de relatório em arquivos de log anteriores ao IBM Firewall for AIX V3R1. No entanto, você pode utilizar utilitários de relatório para processar arquivos de log a partir do IBM Firewall for AIX V3R1 ou posterior. Você também pode utilizá-los para processar o AIX su log. Veja na *Referência ao IBM eNetwork Firewall* informações mais detalhadas sobre utilitários de relatório .

Execução de Utilitários de Relatório Utilizando o Cliente de Configuração

A partir da árvore de navegação do cliente de configuração, dê um clique duplo no ícone da pasta do arquivo Administração do Sistema para expandir a exibição. Dê um clique duplo no ícone da pasta do arquivo Logs do Sistema para expandir a exibição. Selecione **Utilitários de Relatório**. Aparece a caixa de diálogo **Utilitários de Relatório**, como mostra o Figura 30 na página 112.

Figura 30. Utilitários de Relatórios

1. Para o compactador padrão fornecido com o Firewall IBM, o nome de caminho do arquivo de logs é o diretório que contém arquivos de log comprimidos. No campo do nome do arquivo compactado de logs, digite o nome do diretório especificado no campo do diretório compactado da caixa de diálogo **Recursos de Log**. Forneça o nome do caminho absoluto do diretório compactado. Para poder ver um arquivo de log que não foi acumulado, deixe este campo em branco.
2. Selecione **Tipo de Relatório**. Para produzir o texto expandido das mensagens de log, selecione **Log em Texto**. Para criar arquivos tabulares para uso do DB2, selecione **Log em Tabela**. Se os arquivos resultantes forem importados para o DB2, será possível efetuar consultas SQL nos dados do log. Consulte a *Referência ao IBM eNetwork Firewall* para saber mais informações a esse respeito.
3. O nome de arquivo do logs é o de um dos arquivos de log arquivados compactados ou de outro `log do firewall` válido ou o nome de um arquivo de logs su do AIX. Se tiver sido feita uma entrada no campo do diretório compactado de logs, clique na seta **Nome de arquivo Compactado de Logs** para escolher um log para trabalhar. Se não for informado um compactado de logs no passo 1, o nome do arquivo de logs informado aqui terá que ser o nome de um arquivo de logs de firewall não comprimido e válido ou de um arquivo de logs su do AIX. É preciso especificar um caminho completo.
4. Selecione **tipo de log**, **firewall** ou **su AIX**.
5. Digite o **Caminho e Nome de Arquivo do Texto de Saída**.
6. Selecione **Sim** para anexar os resultados do pedido de registro de tabela aos arquivos tabulares que já existiam ou **Não** para substituir os arquivos já existentes.
7. Esse campo permite selecionar certos tipos de mensagem para serem colocadas no arquivo de texto de saída. O conteúdo desse campo é tratado como parâmetro que é colocado num comando padrão `Encontrar` do Windows

NT. Quando se digita, por exemplo, "ICA0" no campo (é preciso colocar as aspas), é como se estivesse sendo executado o seguinte comando:

```
fwlogtxt < my.log | find "ICA0"
```

Eis algumas entradas de exemplo que podem ser colocadas nesse campo e seus resultados:

```
FILTRO                          RESULTADO
"ICA0"          Mostra as mensagens de alteração do limite do monitor de logs
"ICA3"          Mostra mensagens relacionados aos soquetes (#ICA3000 - 3999)
"ICA2010"       Mostra apenas ocorrências da mensagem ICA2010
/V "ICA3"       Mostra todas as mensagens menos as de soquetes
/C "ICA001"     Conta o número de mensagens ICA0001
```

8. Clicar em **OK** produz o(s) arquivos(s) solicitados no diretório de saída especificado na máquina de firewall.
9. A área Resultados dos Utilitários de Relatório mostra todas as mensagens de erro dadas pelo utilitário de relatório executado. Para exibir o texto de logs resultante de um tipo de relatório Log do Texto, clique em **Visualizador de Registro** no painel de configuração principal do Firewall e digite o nome completo do arquivo da saída. Os arquivos .tbl resultantes de um tipo de relatório Log da Tabela podem ser carregados em um banco de dados como descreve o *IBM eNetwork Firewall Reference.*

host 193.5.8.2 pode iniciar uma conexão TCP com o host 10.1.1.1 (utilizando o endereço global 195.9.5.2) somente se uma entrada estática existir na tabela de conversão do NAT, que mapeia o 195.9.5.2 ao 10.1.1.1.

Todos os pacotes gerados por aplicações TCP/UDP podem ser convertidos. As dificuldades surgem se os dados da aplicação contidos no pacote IP possuírem um endereço IP. Uma aplicação especialmente problemática para conversão de endereço é a FTP. A conexão de controle FTP emite comandos "PORT" ou respostas "PASV" que contém na mensagem um endereço IP codificados em ascii. Neste caso, o NAT deve modificar não apenas os endereços no cabeçalho IP, mas também o endereço ascii e o número de porta no payload.

Com o release de um APAR que está para vir, as opções de conversão de vários-para-um do NAT e de conversão MAP irão permitir que pacotes ICMP de chegada e saída sejam convertidos. Pacotes de resposta ICMP de chegada (ping, timestamp, máscara de endereço) e todos os pacotes de erro (destino inatingível, extinção da fonte, redirecionamentos, tempo excedido e mensagens incorretas do pacote) só serão convertidos se houver uma entrada de tabela de conversão existente com a exceção de redirecionamentos. Os redirecionamentos do ICMP irão passar pelo NAT sem estar convertidos. A permissão ou não dos redirecionamentos do ICMP dependem das suas regras do filtro.

Pacotes ICMP de consulta/resposta de saída (solicitação/resposta de ping, solicitação/resposta de timestamp, resposta de solicitação de máscara de endereço) são suportados através da conversão do endereço protegido do pacote e identificador de consulta ICMP de modo que os pacotes ICMP de hosts protegidos diferentes possam compartilhar um único endereço registrado.

Os administradores devem tomar cuidado ao permitir que determinados pacotes ICMP, especialmente máscara/resposta de endereço e redirecionamentos, fluam pelas redes protegidas e não-protegidas. Para obter informações sobre os riscos de segurança ao permitir tráfego ICMP através do Firewall, consulte o seguinte redbook, relacionado na bibliografia: *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*.

Implementação do IBM eNetwork Firewall NAT

A implementação do IBM Firewall NAT suporta a conversão básica de endereço conforme descrita anteriormente com os seguintes caveats:

- Aplicações TCP/UDP (exceto por FTP como descrito anteriormente) que contém informações de endereço IP no payload só terão os campos de cabeçalho do pacote convertidos, como descrito acima. Isto implica que as aplicações UDP como DNS ou SNMP não terão informações de endereço contidas no payload convertido.
- Os comandos FTP PORT são completamente convertidos. No entanto, o endereço embutido em um pacote de resposta PASV não é convertido.
- Mensagens de solicitação/resposta e de codificação ICMP são convertidas. Isto permite, por exemplo, que pings de saída operem corretamente assim como a descoberta MTU de caminho TCP.
- O NAT não detecta uma desconexão TCP mas ao invés disso recai sobre um timestamp inativo configurável antes de remover uma entrada de tabela de

conversão dinâmica e inserir o endereço IP registrado de volta no pool de endereços disponíveis.

Exemplo de Interação Entre NAT, Filtros e Túneis

Figura 32 apresenta um exemplo de interação entre NAT, filtros e túneis.

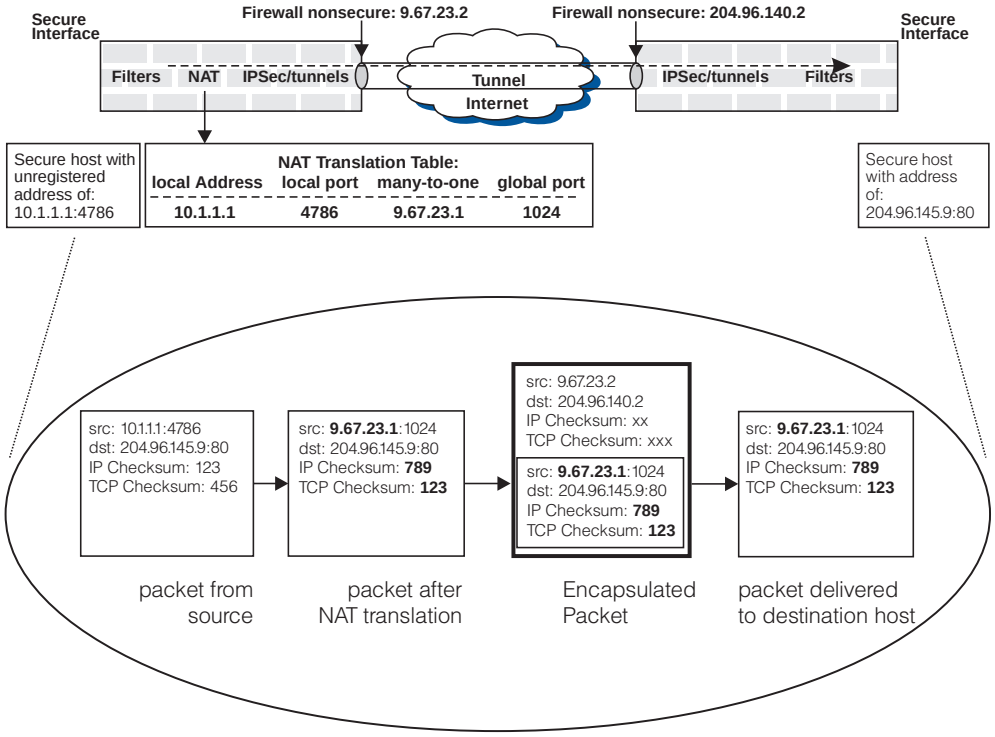


Figura 32. Exemplo de Interação entre NAT, Filtros e Túneis

Suponha que um túnel ESP IPSec seja estabelecido manualmente entre os firewalls 9.67.23.2 e 204.96.140.2. O NAT está ativo somente no firewall 9.67.23.2 porque esta rede protegida utiliza endereços privados. A rede protegida na outra extremidade do túnel não está utilizando NAT. Além de ilustrar a conversão básica do NAT (os campos em negrito no segundo pacote a partir da esquerda ilustram os campos no pacote que são modificados durante a conversão de endereço de saída), a Figura 32 também mostra que o pacote convertido do host é encapsulado em um pacote IP que *não* está convertido.

Em geral, a filtragem é aplicada em pacotes de saída antes do NAT e em pacotes de chegada após a conversão do NAT. Sendo assim, as regras do filtro são baseadas em endereços não convertidos. Quando NAT e túneis estão envolvidos, as regras de filtro no firewall que tem o NAT ativo também são baseadas em endereços não convertidos. Na outra extremidade do túnel (supondo que o NAT não está ativo neste firewall), as regras do filtro para pacotes de entrada são baseadas em endereços convertidos de origem e destino (para os casos de chegada e saída respectivamente). Se o NAT estiver ativo em ambas extremidades do túnel, a discussão acima aplica-se em ambas direções.

Utilizando o cenário ilustrado na Figura 32 como exemplo, e supondo que o objetivo é permitir que o host protegido 10.1.1.1 comunique-se com o host

protegido 204.96.145.9 através de um túnel, o firewall anexado ao 10.1.1.1 deverá possuir uma regra de filtro permitindo que 10.1.1.1 comunique-se com 204.96.145.9 através de um túnel. No outro firewall conectado ao host de destino, uma regra de filtro é necessária para permitir a comunicação entre 9.67.23.1 e 204.96.145.9 através do túnel.

Mais Sobre NAT

Use NAT se deseja permitir:

- Acesso direto a uma máquina atrás de um firewall para um site não-protegido enquanto protege o endereço daquela máquina segura.
- Um número de máquinas sem endereços registrados para compartilhar um endereço registrado para que elas possam alcançar sites na Internet.
- Outras localizações não-protegidas acessam um servidor atrás de um firewall.

Obtenha os endereços registrados para NAT a partir de seu ISP. Todos os endereços usados para NAT não podem ser usados para qualquer outro propósito.

Há quatro opções para NAT:

Vários-para-Um Envolve a conversão de um endereço protegido e número de porta do pacote de tal modo que vários (até 65536) endereços internos podem compartilhar um endereço IP registrado. Este único endereço IP registrado compartilhado vai ocultar endereços locais, mas além disso, você precisa de outro endereço de Internet registrado, para o endereço não-protegido do Firewall. A configuração do NAT irá identificar o endereço de Internet registrado que é utilizado para a conversão de porta utilizando uma entrada de vários-para-um.

Translate Utilizado para criar uma lista de endereços protegidos que serão convertidos.

Exclude Utilizado para criar uma lista de endereços protegidos que não serão convertidos.

Map Utilizado para reservar um endereço registrado específico para um endereço protegido específico.

Configuração da Conversão de Endereço de Rede Utilizando o Cliente de Configuração

1. A partir da árvore de navegação do cliente de configuração, dê um clique duplo no ícone da pasta de arquivos Conversão de Endereço para expandir a exibição. Dê um clique duplo sobre o ícone da pasta de arquivo NAT para expandir a exibição.
2. Selecione **Configuração do NAT** para configurar o módulo de Conversão de Endereço de Rede.

   A **Lista de Conversão de Endereço de Rede** é exibida, como ilustrado na Figura 33 na página 119.

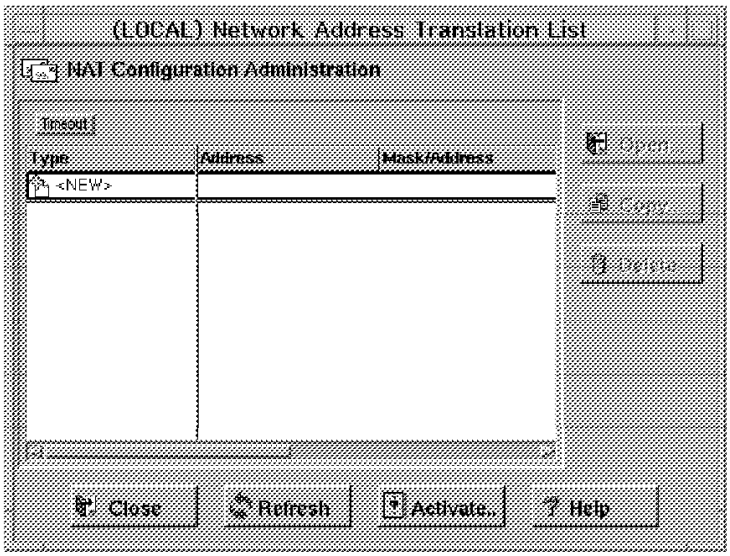


Figura 33. Lista de Conversões de Endereços da Rede

3. Entradas de Conversão de Endereço de Rede - Network Address Translation - contidas no arquivo de configuração de NAT são exibidas neste quadro de diálogo. Você também pode incluir, alterar ou excluir entradas NAT.

Inclusão de Entrada NAT

1. Selecione **Novo** a partir da **Lista de Conversão de Endereço de Rede** e clique em **Abrir** para incluir novas entradas no arquivo de configuração NAT.

   O quadro de diálogo **Incluir NAT** é exibido, como ilustrado na Figura 34.

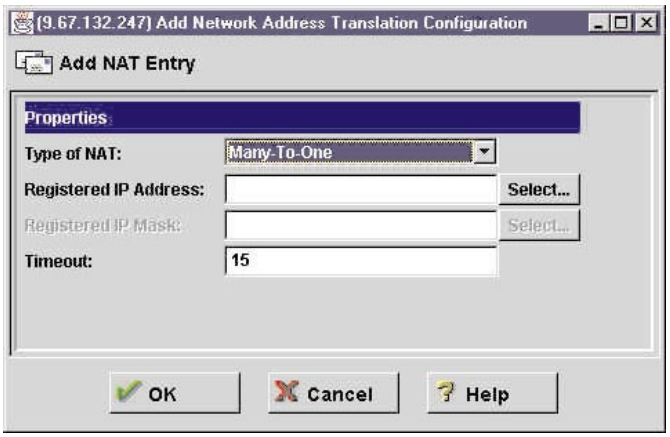


Figura 34. Incluir Configuração NAT

2. A partir do quadro de diálogo **Incluir NAT**, clique na seta no campo Tipo de NAT e selecione a partir do seguinte:
   - Endereço de Rede Registrado de Vários-para-Um: Inclui os endereços IP especificados para o endereço IP reservado. Os parâmetros são endereço IP reservado e tempo de espera associados à tabela de conversão.
   - Converter Endereço de Rede Protegido: Especifica um intervalo de endereços IP protegidos que solicitam a conversão de endereço de rede.

- Excluir Endereço de Rede Protegido: Especifica um intervalo de endereços IP protegidos que devem ser excluídos da conversão de endereço de rede.
- Mapear Endereço de Rede Protegido: Define uma conversão estática de endereço IP de protegido para registrado.

Endereço de Rede Registrado de Vários-para-Um

Uma entrada de endereço registro de vários-para-um converte o endereço protegido e número de porta do pacote de tal modo que vários (até 65536) endereços internos podem compartilhar um endereço IP registrado. Conseqüentemente, você pode ocultar vários endereços locais com um endereço IP registrado. (Você vai precisar de um endereço de Internet registrado adicional para o endereço não-protegido do firewall).

Quando um host protegido envia pacotes a uma rede não-protegida, um endereço IP registrado é alocado. Este endereço de IP registrado exclusivo é utilizado para transportar uma estrutura IP entre o IBM Firewall e as máquinas fora da rede protegida.

Se você selecionou Vários-para-Um na tela Incluir NAT, forneça os seguintes valores:

Endereço IP Registrado Obtenha isto do seu ISP. Este será um endereço IP com pontos decimais por trás do qual todos os endereços protegidos vão estar escondidos.

Escolha um objeto de rede clicando em **Selecionar** para obter o quadro de diálogo **Selecionar Objeto da Rede**. Selecione um objeto da rede e clique em **OK**. O objeto de rede é incluído no campo Objeto da Rede no quadro de diálogo **Incluir Configuração NAT**. Ou, digite um valor diretamente no campo se não tiver criado anteriormente um objeto de rede.

Valor do Tempo de Espera

Forneça o número de minutos que uma conversão de endereço pode permanecer inativa antes que o NAT possa liberar o endereço de IP registrado. Este Valor de tempo de espera aplica-se somente à conversão de endereço que utiliza um endereço IP registrado dentro do intervalo de endereços IP especificados por esta entrada.

O padrão é 15 minutos. O intervalo de valores é de 5 a 45.

Converter Endereço de Rede Protegido

Uma entrada converter endereço IP protegido define um conjunto de endereços de rede protegidos que requer que o NAT execute a conversão do endereço IP. Por padrão, o NAT executa a conversão de endereços em todos os endereços de IP protegidos da entrada converter conjunto de endereços de IP protegidos.

Se tiver selecionado Converter na tela Incluir NAT, forneça os seguintes valores:

Endereço IP Protegido Especifique um endereço de IP com ponto decimal que identifique um intervalo de endereços de IP protegidos que requerem a conversão de endereço de rede.

Escolha um objeto de rede clicando em **Selecionar** para obter o quadro de diálogo **Selecionar Objeto da Rede**. Selecione um objeto da rede e clique em **OK**. O objeto de rede é incluído no campo Objeto de Rede no quadro de diálogo **Incluir Configuração NAT**. Ou, digite um valor diretamente no campo se não tiver criado anteriormente um objeto de rede.

Máscara do Endereço IP Protegido
Especifique uma máscara, como uma máscara de sub-rede que possa especificar os bits no endereço de IP protegido utilizados para identificar um intervalo de endereços de IP. Os bits dessas máscaras definidos como 0 indicam que posições de bit que possuem 0 ou 1 são incluídos no intervalo de endereços de IP. Assim, especificar 255.255.255.255 na máscara indica que apenas um endereço de IP protegido é incluído nesta entrada de conversão, ao passo que uma máscara de 255.255.255.0 indica que endereços de IP classe C requerem conversão de endereço.

Excluir Endereço de Rede Protegido

Uma entrada excluir endereço IP protegido define um conjunto de endereços de rede protegidos que não requer que o NAT execute a conversão do endereço IP. Por padrão, o NAT executa a conversão de endereços em todos os endereços IP protegidos da entrada converter conjunto de endereços IP protegidos.

Se tiver selecionado Excluir na tela de diálogo **Incluir NAT**, forneça os seguintes valores:

Endereço IP Protegido Especifique um endereço IP com ponto decimal que identifique um intervalo de endereços IP protegidos que devem ser excluídos da conversão de endereço de rede.

Escolha um objeto de rede clicando em **Selecionar** para obter o quadro de diálogo **Selecionar Objeto da Rede**. Selecione um objeto da rede e clique em **OK**. O objeto de rede é incluído no campo Objeto de Rede no quadro de diálogo **Incluir Configuração NAT**. Ou, digite um valor diretamente no campo se não tiver criado anteriormente um objeto de rede.

Máscara do Endereço IP Protegido
Especifique uma máscara, como uma máscara de sub-rede que especifique os bits no endereço IP protegido utilizados para identificar um intervalo de endereços IP. Os bits dessas máscaras definidos como 0 indicam que posições de bit que possuem 0 ou 1 são incluídos no intervalo de endereços de IP. Assim, especificar 255.255.255.255 na máscara indica que apenas um endereço IP protegido está especificado nesta entrada,

ao passo que uma máscara de 255.255.255.0 indica que endereços IP classe C são excluídos da conversão de endereços.

Mapear Endereço De Rede Protegido

Uma entrada mapear endereço IP protegido define um mapeamento de um-para-um a partir de um endereço IP protegido para um endereço IP registrado. Tal mapeamento permite que clientes de aplicações externas, como clientes FTP ou telnet, configurem sessões TCP com máquinas servidoras que residem na rede protegida. Os endereços IP registrados nas entradas mapear endereço IP protegido podem sobrepor o espaço destes especificado pelas entradas reservar endereços IP registrados.

Se tiver selecionado Mapa do quadro de diálogo **Incluir Configuração NAT**, forneça os seguintes valores:

Endereço IP Protegido Um endereço IP com ponto decimal que deve ser convertido em um endereço IP registrado especificado.

Escolha um objeto de rede clicando em **Selecionar** para obter o quadro de diálogo **Selecionar Objeto da Rede**. Selecione um objeto da rede e clique em **OK**. O objeto de rede é incluído no campo Objeto de Rede no quadro de diálogo **Incluir Configuração NAT**. Ou, digite um valor diretamente no campo se não tiver criado anteriormente um objeto de rede.

Campo Endereço IP Registrado

Um endereço IP com ponto decimal em que um endereço IP protegido especificado deve ser convertido.

Você pode escolher um objeto de rede clicando em **Selecionar** para obter o quadro de diálogo **Selecionar Objeto de Rede**. Selecione um objeto da rede e clique em **OK**. O objeto de rede é incluído no campo Objeto de Rede no quadro de diálogo **Incluir Configuração NAT**.

Alteração de Entrada NAT

Selecione uma entrada NAT existente a partir do quadro de diálogo **Configuração NAT** e clique em **Abrir** para alterar entradas da Conversão de Rede no arquivo de configuração NAT.

Eliminação de Entrada NAT

1. Selecione uma entrada NAT existente a partir do quadro de diálogo **Configuração NAT** e clique em **Eliminar** para remover uma entrada de Conversão de Rede do arquivo de configuração NAT.

   Um quadro de diálogo de confirmação aparece.

2. Selecione Sim ou Não.

Ativação NAT

1. A partir da árvore de navegação do cliente de configuração, dê um clique duplo no ícone da pasta de arquivos Conversão de Endereço para expandir a exibição. Dê um clique duplo sobre o ícone da pasta de arquivo NAT para expandir a exibição.
2. Selecione **Ativação NAT** e um quadro de diálogo semelhante ao mostrado em Figura 35 é exibido.

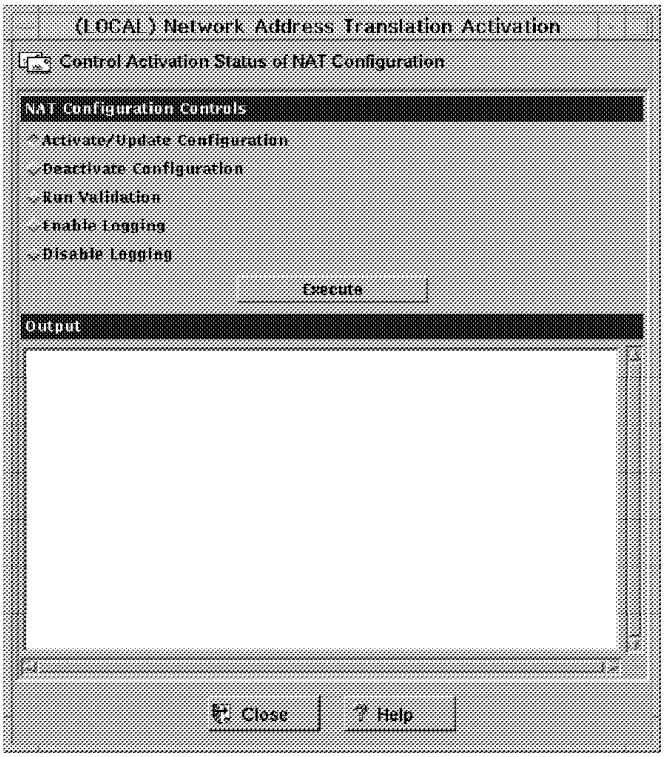


Figura 35. Ativação NAT

3. Você pode selecionar um dos seguintes e depois clicar em **Executar**:
   - Validar entradas da conversão do endereço de rede contidas em um arquivo de configuração NAT especificado.
   - Ativar/Atualizar a configuração para exibir entradas de Conversão de Endereço de Rede atualmente utilizadas pelo módulo NAT.
   - Desativar NAT para desativar a conversão de endereço da rede.
   - Ativar Registro para ativar o registro de conversão de endereço de rede.
   - Desativar Registro para desativar o registro de conversão de endereço da rede.

Registro

O NAT irá registrar uma variedade de condições de erro desde que o registro do NAT e o registro do filtro estejam ativados. O registro do NAT é ativado através do painel **Ativação do NAT** ou através do uso do comando **fwnat**. O registro do filtro é ativado através do painel **Recurso de Registro** ou através do uso do comando **fwlog**.

As seguintes atividades serão registradas no recurso de registro do firewall:

- Atualizações nas tabelas do NAT a partir do Administrador (por exemplo, entradas estáticas ou do MAP)
- Atualizações dinâmicas na tabela de conversão do NAT
- Mensagens de erro
- Tentativas falhas de conversão que resultam no descarte do pacote
- Cada vez que o NAT é ativado e desativado

Criação de Regras de Filtragem para NAT

Após você completar a configuração de NAT, você deve criar as regras de filtragem para as conexões que irão usar NAT. Reveja Capítulo 8, “Controle do Tráfego Através do Firewall” na página 45 e use os serviços pré-definidos para as conexões diretas. Exemplos de serviços pré-definidos para conexões diretas são:

- Saída direta HTTP
- Saída direta Telnet

Consulte “Criação de Conexões Utilizando os Serviços Pré-definidos” na página 46 para maiores informações.

Se você desejar que um serviço venha diretamente em sua rede, você terá que criar um. Consulte “Utilização do Cliente de Configuração para Criar Serviços” na página 66 para informações sobre como fazer isso.

Apêndice A. Avisos

As referências encontradas nesta publicação a produtos, programas e serviços da IBM não devem ser interpretados como indício de que a IBM pretenda colocá-los à disposição em todos os países em que opera. Nenhuma dessas referências pretende afirmar ou deixar implícito que só podem ser usados programas, produtos ou serviços da IBM. Estando subordinado aos direitos de propriedade intelectual da IBM ou a quaisquer outros direitos legais de proteção válidos equivalentes, todo produto, programa ou serviço funcionalmente equivalente pode ser usado no lugar do produto, programa ou serviço da IBM. A avaliação e a verificação da operação conjunta com outros produtos, exceto com aqueles explicitamente designados pela IBM, são responsabilidade do usuário.

A IBM pode ter patentes ou pedidos pendentes de patente que abordam o assunto tratado neste documento. O fornecimento deste documento não dá a quem o recebe nenhum tipo de licença em relação a tais patentes. Pedidos de licença podem ser enviados por escrito para:

Gerente de Relações Industriais e Comerciais da IBM Brasil
Av. Pasteur, 138 / 146
Botafogo
22290-240 Rio de Janeiro RJ
BRASIL.

Os portadores de licença para o uso deste programa que desejem obter informações a fim de possibilitar: (i) a troca de informações entre programas criados independentemente e outros programas (inclusive este) e (ii) o uso mútuo dessas informações, devem entrar em contato com:

Av. Pasteur, 138 / 146
Botafogo
22290-240 Rio de Janeiro RJ
Rio de Janeiro RJ
BRASIL.

Estas informações poderão estar disponíveis mediante termos e condições adequados, que incluem, em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo material licenciado disponível para ele são fornecidos pela IBM sob os termos do IBM Customer Agreement (Acordo de Cliente IBM).

Este documento não se destina a fins de produção e é fornecido como se encontra, sem nenhuma garantia de nenhum tipo, sendo que todas as garantias ficam doravante negadas, inclusive as relativas a comercialização e adequação a finalidades particulares.

Este produto inclui software desenvolvido pela Universidade da Califórnia, de Berkeley e seus contribuintes.

Marcas

Os seguintes termos são marcas da IBM corporation nos Estados Unidos ou em outros países ou em ambos:

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

Os logotipos da Microsoft, Windows, Windows NT e Windows 95 são marcas ou marcas de serviço da Microsoft Corporation.

Java e HotJava são marcas da Sun Microsystems, Inc.

Outros nomes de empresas, produtos e serviços que estejam indicados por dois asteriscos (**) podem ser marcas de terceiros.

Bibliografia

Para informações adicionais sobre segurança na Internet, visite a home page IBM eNetwork Firewall em **http://www.software.ibm.com/enetwork/firewall**.

Informações em publicações IBM

Estão relacionadas aqui outras fontes de informações IBM relacionadas a firewalls, segurança na Internet e tópicos gerais de segurança.

Tópico: Firewall

Os seguintes documentos estão disponíveis no IBM Firewall CD-ROM e na home page do IBM eNetwork Firewall.

- *IBM eNetwork Firewall User's Guide*, GC31-8658
- *IBM eNetwork Firewall Reference*, SC31-8659
- *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*, SG24-5209

Tópicos: Internet e World Wide Web

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

Tópico: Segurança Geral

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

Informações em publicações industriais

Estas publicações industriais referem-se a TCP/IP e UNIX:

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail*. O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration*. O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook*. Prentice Hall. (ISBN: 0-13-151051-7

Estas publicações industriais referem-se a firewalls e segurança na Internet:

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)

- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

Glossário

É possível acessar o glossário de Software IBM em:
http://www.networking.ibm.com/nsg/nsgmain.htm.

Índice Remissivo

I

L

M

N

O

P

R

S

T

U

V

Comentários do Leitor

IBM eNetwork Firewall for Windows NT
Guia do usuário
Versão 3 Release 2.1.1

Publicação Nº GC17-1348-01

Neste formulário, faça-nos saber sua opinião sobre este manual. Utilize-o se encontrar algum erro, ou se quiser externar qualquer opinião a respeito (tal como organização, assunto, aparência ...) ou fazer sugestões para melhorá-lo.

Para pedir publicações extras, fazer perguntas ou tecer comentários sobre as funções de produtos ou sistemas da IBM, fale com o seu representante IBM.

Quando você envia seus comentários, concede direitos, não exclusivos, à IBM para usá-los ou distribuí-los da maneira que achar conveniente, sem que isso implique em qualquer compromisso ou obrigação para com você.

Não se esqueça de preencher seu nome e seu endereço abaixo, se desejar resposta.

Nome

Endereço

Companhia ou Empresa

Telefone

Comentários do Leitor
GC17-1348-01

Corte ou dobre ao longo da linha

Dobre e cole com fita **Não grampeie** Dobre e cole com fita

COLE SELO POSTAL AQUI

Centro Industrial IBM Brasil
Centro de Traduções
Caixa Postal 71
13001-970 Campinas, SP
BRASIL

Dobre e cole com fita **Não grampeie** Dobre e cole com fita

Corte ou dobre ao longo da linha

GC17-1348-01

Impresso na Dinamarca.

GC17-1348-01