

IBM eNetwork Firewall for Windows NT

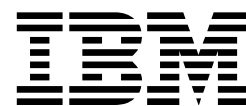


# Referência

*Versão 3 Release 2*



IBM eNetwork Firewall for Windows NT



# Referência

*Versão 3 Release 2*

**Nota:** Antes de utilizar estas informações e o produto que elas suportam, leia atentamente as informações gerais nos “Avisos” na página 155.

### **Primeira Edição (Março 1998)**

Esta edição aplica-se à versão 3 release 2 do IBM eNetwork Firewall para Windows NT (número de produto 5765-C16) e a todos os releases e modificações subseqüentes até indicações contrárias em novas edições.

O copyright de partes © 1993, 1994 pertence à NEC Systems Laboratory.

Contém software de segurança da RSA Data Security, Inc. Copyright © 1990, 1995 RSA Data Security, Inc. Todos os direitos reservados.

© Copyright International Business Machines Corporation 1994, 1998. Todos os direitos reservados.

# Índice

<b>Sobre Este Manual</b>	v
Conhecimentos de Pré-requisito	v
Recursos Neste Release	v
Socks Protocol Versão 5	vi
Administração Simples	vi
Robustecimento do NT	vi
Autenticação poderosa	vi
Utilitários de Relatório	vi
Alerta, Monitoração e Registro	vi
Várias Redes Isoladas	vi
Suporte a Idioma Nacional	vi
Fornecimento de Endereços de IP	vii
Como Chamar o Serviço IBM	vii
 <b>Capítulo 1. Utilização da Interface de Linha de Comandos do IBM Firewall</b>	 1
Servidor de Configuração	1
Serviços de Nome de Domínio	2
Filtros	3
Proxy HTTP	3
Interfaces	4
Arquivo Compactado de Log	5
Gerenciamento de Arquivo de Log	5
Monitor de Logs	7
Correio	10
Paginação	10
Usuários	14
 <b>Capítulo 2. Utilização dos Utilitários de Relatório</b>	 21
Utilização dos Utilitários de Relatório	21
Formato do Log do IBM Firewall	22
 <b>Capítulo 3. Kit de Desenvolvimento de Software Plug-in do SafeMail</b>	 43
Visão Geral do Processamento do SafeMail	43
Criação de um Plug-in do Gateway do SafeMail	43
 <b>Capítulo 4. Kit de Desenvolvimento de Software Plug-in do Compactador de Registro</b>	 45
Criação de um Plug-in do Compactador de Log	45
 <b>Capítulo 5. Fornecimento de Métodos Próprios de Autenticação</b>	 47
Autenticação Fornecida pelo Usuário	47
Utilização do Software Development Kit para Criar um Esquema de Autenticação Fornecido pelo Usuário	47
 <b>Capítulo 6. Utilização do Utilitário Make Key File (MKKF)</b>	 57
Criação de arquivo de chaves	57
 <b>Capítulo 7. Identificação de Problemas e Testes</b>	 65
Instalação e Configuração	65
Problemas de Roteamento	65

Problemas de DNS . . . . .	66
Cliente de Configuração . . . . .	68
Controle de Tráfego . . . . .	69
Servidores Proxy . . . . .	69
Serviços de Autenticação . . . . .	70
Dispositivos do Log . . . . .	70
Utilitários de Relatório . . . . .	70
 <b>Apêndice A. Mensagens</b> . . . . .	 73
Tag da Mensagem . . . . .	73
Mensagens . . . . .	73
 <b>Apêndice B. Robustecimento para a Configuração do Sistema Windows NT</b> . . . . .	 141
 <b>Apêndice C. Obtenção de Pedidos para Comentários (RFCs)</b> . . . . .	 143
 <b>Apêndice D. Formato do Arquivo de Configuração Socks5.conf do IBM eNetwork Firewall</b> . . . . .	 145
Especificação de Portas . . . . .	145
Especificação de Hosts . . . . .	145
Especificação dos Métodos de Autenticação . . . . .	146
Entradas de Autenticação . . . . .	147
Especificação de Comandos . . . . .	147
Carregamento de Módulos . . . . .	147
Roteamento de Entradas . . . . .	148
Entradas de Variáveis . . . . .	148
Entradas de Proxy . . . . .	149
Entradas do Controle de Acesso . . . . .	150
Filtros . . . . .	150
 <b>Bibliografia</b> . . . . .	 153
Informações em publicações IBM . . . . .	153
Informações em publicações industriais . . . . .	153
 <b>Avisos</b> . . . . .	 155
Marcas . . . . .	155
 <b>Glossário</b> . . . . .	 157
 <b>Índice Remissivo</b> . . . . .	 159

---

## Sobre Este Manual

Este manual pretende servir como referência para os administradores da rede ou de segurança do sistema que instalam, administram e utilizam o IBM eNetwork Firewall Versão 3.2 em uma máquina do Windows NT\*\*. Para utilizar programas cliente como Telnet ou FTP, consulte o guia do usuário para programas cliente TCP/IP.

---

## Conhecimentos de Pré-requisito

É importante que você tenha um profundo conhecimento de TCP/IP e de administração de rede antes de instalar e configurar o IBM eNetwork Firewall. Como serão feitos a configuração e os ajustes de um firewall que controla acesso tanto dentro quanto fora da rede, é preciso compreender como a rede funciona. De modo especial, é preciso entender os princípios em que se baseiam os endereços de IP, os nomes totalmente qualificados e as 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 obter mais detalhes.

---

## Recursos Neste Release

O IBM eNetwork Firewall for Windows NT oferece uma ampla gama de recursos e inclui as três arquiteturas do firewall:

1. Proxies da aplicação

- FTP
- HTTP, incluindo Gopher e WAIS
- Telnet
- SafeMail

HTTP, Telnet e FTP têm o recurso de autenticação.

2. Gateway de nível de circuito através do Socks Protocol Versão 5, um padrão Internet

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

Muitos serviços pré-definidos tornam a configuração rápida.

## **Socks Protocol Versão 5**

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

- Fácil disposição de métodos de autenticação e criptografia
- 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

## **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. E administradores diferentes podem ser atribuídos a diferentes níveis de autoridade para controlar, futuramente, o acesso ao firewall. Esta interface gráfica com o usuário, simples e 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**

É oferecido suporte a todos os mecanismos de autenticação mais conhecidos baseados em token, como o SecurID, SecureNet Key e outros.

## **Utilitários de Relatório**

Utilitários de relatório permitem que você execute uma consulta SQL junto ao registro do sistema depois que esta é exportada 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.

## **Várias Redes Isoladas**

Usando várias Placas de Interface de Rede (NICs) no firewall, você pode isolar várias 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. O número do atendimento é 0-800-784-262.

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



---

# Capítulo 1. Utilização da Interface de Linha de Comandos do IBM Firewall

Este capítulo trata dos comandos que podem ser usados em uma linha de comandos do IBM eNetwork Firewall.

As seguintes informações se aplicam aos comandos:

- Os comandos que aparecem neste manual usam a seguinte sintaxe:
  - sublinhado indica que os dados foram digitados pelo usuário.
  - [] indica que o parâmetro é opcional.
  - {} indica que o usuário tem opções de parâmetros.
  - | separa opções.
- Todos os parâmetros usam formato palavra-chave=valor.
- Se o parâmetro possuir vários valores, estes deverão ser colocados entre aspas duplas e delimitados por espaços em branco; exemplo:  
`secaddr="11.22.33.1 11.22.33.2"`
- Não inclua espaços dentro de nenhum parâmetro, a menos que seja dentro das aspas duplas.
- Se um ou mais parâmetros obrigatórios forem omitidos, o utilitário da linha de comandos os mostrará.
- Se for digitado um valor inválido para algum parâmetro, o utilitário da linha de comandos comunicará o erro.
- Alguns dos serviços do firewall atualizam dinamicamente seu comportamento quando ocorre alteração em seus arquivos de configuração. Alguns requerem um subcomando de atualização. É fornecido um subcomando update para estes serviços do firewall que requerem instrução.
- Somente administradores primários do firewall podem executar programas a partir da linha de comando.
- Devido à complexidade e às interdependências de arquivo, **não edite diretamente nenhum arquivo de configuração.**

---

## Servidor de Configuração

O comando `fwcfgsrv` relaciona ou altera as opções do servidor de configuração. Um administrador deve ter autoridade para administrar as funções de controle de tráfego para emissão deste comando.

Para relacionar as opções do servidor de configuração, emita o seguinte comando.

```
fwcfgsrv cmd=list
```

A saída do comando `fwcfgsrv` assemelha-se à seguinte:

```
localonly = yes/no
encryption = none/ssl
sslfile = filename if one is defined
```

Para alterar as opções do servidor de configuração, emita o seguinte comando.

```
fwcfgsrv cmd=change  
[localonly={yes|no}]  
[encryption={none|ssl}]  
[sslfile=]
```

As definições de parâmetro são:

**localonly** Indica se o firewall só pode ser administrado a partir de uma máquina local. Os valores válidos são sim ou não.

**encryption** Indica se o servidor de configuração espera que os dados que entram sejam criptografados sem ssl ou não. Os valores válidos são nenhum ou ssl.

**sslfile** Indica o nome do arquivo-chave ssl a ser usado para criptografia ssl. Consulte Capítulo 6, “Utilização do Utilitário Make Key File (MKKF)” na página 57.

---

## Serviços de Nome de Domínio

Os Serviços de Nome de Domínio (DNS) oferecem serviços completos de nome de domínio para hosts de dentro da rede protegida, fornecendo ao mesmo tempo informações mínimas para hosts de fora dela. São exigidos três servidores de nome de domínio para fazer isso:

- Um no firewall
- Um dentro da rede protegida
- Um fora da rede protegida

Consulte o *Guia do Usuário IBM eNetwork Firewall* para obter maiores informações.

### Nota:

1. x.x.x.x é um endereço de IP em seu formato decimal com pontos.
2. O valor dos parâmetros secaddr e remaddr pode ser um endereço de IP individual ou uma lista de endereços de IP. Se a lista de endereços de IP for especificada, seus espaços deverão ser delimitados e contidos dentro de aspas duplas.
3. Endereços duplicados são detectados e sinalizados como erro.
4. Quando o DNS é configurado pela primeira vez, o fwdns cmd=change cria o novo arquivo. O firewall vai sempre ter exatamente um registro de configuração do DNS. Os valores podem ficar vazios. O subcomando alterar é suficiente para alterar algum ou todos os valores do registro DNS.

O comando a seguir relaciona a configuração DNS atual.

```
fwdns cmd=list
```

Para mudar a entrada da configuração DNS e criar um arquivo novo:

```

fwdns cmd=change
      secdomain=SecureDomainName
      secaddr=x.x.x.x | "x.x.x.x x.x.x.x x.x.x.x"
      remaddr=x.x.x.x | "x.x.x.x x.x.x.x x.x.x.x"

```

As definições de parâmetro são:

**secdomain**=SecureDomainName nome de domínio da rede protegida interna

**secaddr**=SecureDNSAddr[,...] endereço de IP de seus servidores de nome de domínio protegido

**remaddr**=NonSecureDNSAddr[,...] Endereço de IP dos servidores de nome de domínio de fora da rede protegida que são protegidos pelo provedor de serviços de conexão da Internet.

---

## Filtros

Use o comando **fwfilter** para ativar e desativar as regras de filtro.

```

fwfilter cmd=update | verify | list | shutdown | startlog |
stoplog

```

As definições dos parâmetros são:

**fwfilter cmd=update** gera de novo a configuração e ativa o conjunto de regras.

**fwfilter cmd=verify** faz o "teste de geração" da configuração mas não ativa as alterações.

**fwfilter cmd=list** lista a configuração gerada mais recentemente

**fwfilter cmd=shutdown** desativa o mecanismo dos filtros

**fwfilter cmd=startlog** registra o tráfego selecionado no recurso log do firewall

**fwfilter cmd=stoplog** interrompe os registros de filtro do firewall

---

## Proxy HTTP

O proxy HTTP manipula eficientemente solicitações do navegador através do IBM Firewall eliminando a necessidade de um servidor de soquetes 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 comando **fwhttp** relaciona ou altera a configuração proxy HTTP.

Para relacionar a configuração proxy HTTP, use o seguinte comando.

```

fwhttp cmd=list

```

Para alterar a configuração proxy HTTP atual, use o seguinte comando.

```
fwhttp cmd=change
[port=]
[maxcontentlengthbuffer=]
[minactivethreads=]
[maxactivethreads=]
[idlethreadtimeout=]
[logging=]
[authenticate=]
[authentictetimeout=]
[maxpersistrequests=]
[persisttimeout=]
```

As definições de parâmetro são:

**port** A porta em que o serviço proxy atenderá.

**maxcontentlengthbuffer** O número máximo de um buffer para retornar documentos, com o objetivo de permitir a inclusão de um cabeçalho na extensão do conteúdo a ser retornado.

**minactivethreads** O número mínimo de cadeias trabalhadoras para começar na inicialização e que sejam mantidas ativadas durante a execução.

**maxactivethreads** O número máximo de cadeias trabalhadoras que podem estar em execução a qualquer momento.

**idlethreadtimeout** O período de tempo em que as cadeias inativas devem ser mantidas como disponíveis.

**logging** Indica se os registros são desejáveis para a atividade HTTP. Os valores são on (ligado) ou off (desligado).

**authenticate** O nível que os usuários possuem para autenticar. Os valores são all (tudo), none (nenhum) ou new (novo).

**authentictetimeout** O tempo de espera para uma solicitação do cliente após o estabelecimento de uma conexão persistente.

**maxpersistrequests** O número máximo de solicitações a serem recebidas numa conexão persistente.

**persisttimeout** Tempo para manter uma conexão persistente

---

## Interfaces

As interfaces protegidas conectam o host do IBM Firewall à rede de hosts em sua rede interna, a rede que deseja proteger. **É necessário ter, no mínimo, uma interface protegida para que o firewall funcione.** Interfaces não-protegidas conectam o IBM Firewall a uma ou mais redes externas ou à Internet. O IBM Firewall deverá possuir pelo menos uma interface não-protegida.

Este comando relaciona as interfaces da rede do firewall. Um administrador deve ter a autoridade de administrar as funções da interface para emitir este comando.

```
fwinterface cmd=list
[addr=x.x.x.x]
```

Consulte o capítulo sobre administração do *Guia do Usuário IBM eNetwork Firewall* para obter mais informações sobre autoridade do administrador.

As definições de parâmetro são:

**addr=x.x.x.x** Relaciona todas as interfaces da rede que foram configuradas para o firewall e identifica cada uma como sendo protegida ou não-protegida. Também poderia ser identificado um nome. Se o parâmetro opcional **addr** for especificado, só essa interface será relacionada. Se for fornecido um endereço IP decimal por pontos para **addr**, a lista conterá o endereço, o estado e o nome somente do endereço especificado, assumindo-se que ele tenha sido configurado para o firewall.

Este comando permite que você defina as interfaces da rede para o firewall. Um administrador deve ter a autoridade de administrar as funções da interface para emitir este comando.

```
fwinterface cmd=change
            addr=x.x.x.x
            [state={secure|nonsecure}]
            [name=]
```

As definições de parâmetro são:

**addr=x.x.x.x** Contém o endereço decimal por pontos da interface a ser alterada. Se esta interface não estiver definida para o firewall, será relatado um erro.

**state={secure|nonsecure}** Contém uma das duas palavras-chaves "secure" ou "nonsecure" que categorizam a rede anexa à interface especificada.

**name** É um nome significativo que identifica a interface ou a rede a que ele estiver ligado. Espaços podem ser incluídos, desde que entre aspas duplas, da maneira adequada.

Embora os parâmetros de estado e de nome sejam opcionais, é necessário que um deles seja especificado.

---

## Arquivo Compactado de Log

O seguinte comando chama o arquivo compactado do logfile para a manutenção de dispositivos do log que foram configurados para arquivamento.

```
fwlogmgmt -l ou fwlogmgmt -a
```

É útil colocar este comando em um Windows NT Scheduled Service. Consulte o *Guia do Usuário IBM eNetwork Firewall* para obter maiores informações.

---

## Gerenciamento de Arquivo de Log

O gerenciamento do arquivo de log define e gerencia os arquivos de log e os arquivos compactados. O comando **fwlog** inclui, modifica e elimina recursos de log.

Para incluir dispositivos de log, emita o seguinte comando.

```
fwlog cmd=add
      facility=Facility
      priority=Priority
      logfile=LogFileName
      [arcfile=ArchivePath]
      logtime=DaysToKeepInLog
      arctime=DaysToKeepInArchive
```

Valores válidos para **facility**:

- firewall (local4) - logs gerais do firewall, incluindo registros de filtro
- alert (local1) - status do daemon do monitor de logs e advertências de violação de limites usados para preencher a Exibição dos Alertas
- adminaudit (local0) - log de auditoria administrativo
- mail - logs de correspondência

Valores válidos para **priority**:

- debug
- info
- warning
- error
- crit

O parâmetro logfile indica para onde as entradas dos registros do firewall devem ser enviadas. O valor válido para logfile é um nome de arquivo completamente qualificado (unidade:Ödiretório) indicando o arquivo no qual as entradas de log devem ser gravadas.

**Nota:** Arquivos identificados para os dispositivos log de alerta ou log do firewall devem ser diferentes um dos outros e dos arquivos de todos os outros dispositivos de log, caso recursos do firewall venham a ser usados para processar estes arquivos.

**É importante que APENAS mensagens de log do firewall apareçam em entradas de arquivo de utilitários de relatório. Nenhum outro dispositivo deve ser direcionado para o mesmo arquivo que o log do firewall ou log de alerta.**

Os parâmetros arcfile, logtime e arctime são opcionais e válidos apenas quando o parâmetro logfile especificar um nome de arquivo. Todos os três parâmetros devem ser especificados se houver algum parâmetro especificado. Estes parâmetros controlam o arquivamento do log. Para que o arquivamento real ocorra, execute o comando fwlogmgmt periodicamente. Consulte “Arquivo Compactado de Log” na página 5.

Por padrão, o firewall utiliza estes parâmetros para indicar onde arquivar registros de log e com que frequência eles devem ocorrer. É necessário especificar estes três parâmetros para ativar a compactação.

O dispositivo de compactação pode ser substituído por meio da gravação de uma conexão de compactação do firewall. Consulte Capítulo 4, “Kit de Desenvolvimento de Software Plug-in do Compactador de Registro” na página 45.

O parâmetro **arcfile** deve conter um caminho completamente qualificado.

O parâmetro **logtime** indica o número mínimo de dias que uma entrada de registro do firewall permanecerá no logfile antes de ser transferida para o arquivo compactado.

O parâmetro **arctime** indica o número mínimo de dias que um registro de log do firewall permanecerá no arquivo compactado antes de ser eliminado.

Para alterar os recursos de log, emita o seguinte comando.

```
fwlog cmd=change
      index=Index
      [facility=Facility]
      [priority=Priority]
      [logfile=LogFileName]
      [arcfile=ArchiveFileName]
      [logtime=DaysToKeepInLog]
      [arctime=DaysToKeepInArchive]
```

Se alguma mudança, especialmente na instância inicial, deixar de criar um arquivo de configuração sintaticamente correto (exemplo: a definição do arquivo de log criado possui campos ausentes), será dada uma advertência e o firewall não registrará os dados.

Para realizar registros, mas não compactação, são necessários apenas os parâmetros **facility**, **priority** e **logfile**. Para desativar o compactador de log uma vez iniciado, limpe os parâmetros **archive**, **logtime** e **arctime**. Caso tenha programado um job de arquivamento, elimine-o.

Para relacionar os dados de configuração do arquivo de log atual, emita o seguinte comando.

```
fwlog cmd=list
```

Para eliminar a entrada de log do firewall especificada pelo número de índice devolvido para a entrada no comando fwlog cmd=list, emita o seguinte comando.

```
fwlog cmd=delete
      index=índice da entrada a ser eliminada
```

---

## Monitor de Logs

Use o comando do monitor de logs para informar ao monitor de logs quando e como acionar os alertas. Os alertas ocorrem quando os valores do limite especificados neste comando (ou o painel do cliente de configuração correspondente) são alcançados dentro de um intervalo de tempo especificado. Quando ocorre um alerta:

1. Um registro é gravado no recurso de alertas do firewall e no recurso de registro do firewall
2. Um comando especificado é executado
3. Um aviso é enviado a uma ou mais IDs de usuário
4. Uma mensagem é enviada a um dispositivo de paginação

As últimas três ações são controladas por configuração adequada de valores especificados aqui.

### Lista das Definições do Monitor de Logs

```
fwlogmon cmd=list
```

### **Especificação de IDs de Usuário para Receber Notificações de Correspondência quando algum Alerta Ocorrer**

Para especificar ids de usuário para receber notificações de correspondência quando algum alerta ocorrer (o aviso é enviado a cada id incluída):

```
fwlogmon cmd=add|delete
         type=id
         username=
         [comment=]
```

### **Especificação de um Comando a ser executado quando algum Alerta Ocorrer**

```
fwlogmon cmd=add|change
         type=command
         command=
         [comment=]
```

```
fwlogmon cmd=delete
         type=command
```

### **Especificação de um Limite em que um Alerta Deve ser Acionado Baseado no Número de Tentativas de Login Mal Sucedidas**

```
fwlogmon cmd=add
         type=single|multi|host
         count=
         time=
         pager=
         [comment=]
```

```
fwlogmon cmd=change
         type=single|multi|host
         [count=]
         [time=]
         [pager=]
         [comment=]
```

```
fwlogmon cmd=delete
         type=single|multi|host
```

### **Especificação de um Limite em que um Alerta Deve ser Acionado Baseado no Número de Ocorrências de uma ID de Mensagem do Firewall Específico**

```
fwlogmon cmd=add
         type=msg
         tag=
         count=
         time=
         pager=
         [comment=]
```

```
fwlogmon cmd=change
         type=msg
         tag=
         [count=]
         [time=]
         [pager=]
         [comment=]
```

```
fwlogmon cmd=delete
         type=msg
         tag=
```

As definições de parâmetro são:

- type** Identifica o tipo de característica de comando do monitor de log que está sendo incluída ou modificada.
- Valores permitidos são id, command, msg, single, multi e host.
- id** Emprega a id de usuário para enviar avisos.
- command** Especifica um comando a ser executado.
- msg** Emprega o monitoramento de uma mensagem de log específica.
- single** Emprega o monitoramento com base em ids de usuário individuais. Um contador é mantido para cada id que possui uma tentativa com falha. Se o contador de alguma id alcançar o valor limite especificado neste comando, um alerta é acionado.
- multi** Emprega o monitoramento com base em múltiplas ids de usuário. Se o total de todos os contadores, para todas as ids de usuário que tiveram tentativas com falhas, alcançar o valor limite especificado neste comando, um alerta será acionado.
- host** Emprega o monitoramento com base em nomes de sistemas centrais. Um contador é mantido para cada nome de host do qual ocorreu uma tentativa com falha. Se o contador de algum nome de host alcançar o valor limite especificado neste comando, um alerta é acionado.
- username** A id de correspondência de um administrador firewall ou outros usuários a serem avisados de qualquer alerta. As notificações de alerta serão remetidas com sucesso apenas se você tiver configurado adequadamente um servidor de correspondência secure-side.
- command** O nome do comando a ser executado quando ocorrer algum alerta. Ele deve ser o nome do caminho completo de um arquivo executável. Ele pode ser um arquivo .bat, que permite que vários comandos sejam executados de dentro desse arquivo, entretanto se o arquivo .bat fizer qualquer referência a outros arquivos, eles também deverão ser referências de nome de caminho completo.
- count** Define o limite para o número de falhas ou ocorrências de uma determinada mensagem de log em que um alerta será usado.

<b>time</b>	Define um intervalo de tempo em minutos. A conta deve ser alcançada dentro desse intervalo de tempo da primeira ocorrência, a fim de acionar um evento. As ocorrências mais antigas que esse intervalo, anteriores ao horário atual, são liberadas a partir da conta.
<b>pager</b>	Especifica se você usa uma página ou não, quando o limite associado aciona um alerta. A configuração de pager atual é usada para enviar a página.
<b>tag</b>	Uma tag da mensagem de log (com o prefixo de mensagem ICA) a ser monitorada. As mensagens do monitor de logs (tags ICA inferiores a 1000) não podem ser monitoradas.

---

## Correio

Use o comando `fwmail` para mapear domínios de correspondência públicos e protegidos.

```
fwmail cmd=list
fwmail cmd=add
    secdomain=
    mail=
    remdomain=

fwmail cmd=change
    secdomain=
    [mail=]
    [remdomain=]

fwmail cmd=delete
    secdomain=
```

As definições de parâmetro são:

**secdomain** O nome pelo qual o domínio da correspondência que estiver sendo descrito é conhecido pelos usuários no lado protegido do firewall.

**mail** Endereço de um servidor de correspondência.

**remdomain** O nome pelo qual o domínio da correspondência que estiver sendo descrito é conhecido pelos usuários no lado não-protetido do firewall.

---

## Paginação

Você pode ativar o suporte de Notificações do Pager para que o firewall procure o um administrador de sistema enviando uma mensagem ao beeper do administrador quando houverem alertas de intrusão no firewall. Para que isso funcione, você deve configurar o pager, o serviço da operadora e um modem usando os comandos `fwpggr`, `fwcarrier` e `fwmodem`.

## Configuração do Pager

O comando `fwpggr` configura os parâmetros do pager ativo, aquele que o Firewall sinalizará.

Para relacionar um pager, emita o seguinte comando.

```
fwpggr cmd=list
```

Para incluir um pager, emita o seguinte comando.

```
fwpggr cmd=add
      carrier=
      modem=
      pagerid=
      message=
```

Para modificar os parâmetros do pager, emita o seguinte comando.

```
fwpggr cmd=change
      [carrier=]
      [modem=]
      [pagerid=]
      [message=]
```

As definições de parâmetro são:

- carrier** Um nome do serviço de operadora, conforme definido no banco de dados de operadoras (através do comando `fwcarrier`).
- modem** Um nome do modem, conforme definido no banco de dados modems (através do comando `fwmodem`).
- pagerid** O nome ou número de identificação exclusivo, atribuído pela operadora para o dispositivo de paginação.
- message** A mensagem a ser enviada e exibida no dispositivo de paginação. Um número ou texto, dependendo do serviço que a operadora está fornecendo. Ele será truncado se exceder a menor definição do comprimento para a operadora ou 200 caracteres.

## Operadora

Use o comando `fwcarrier` para configurar parâmetros para qualquer serviço de paginação usado.

Para relacionar uma operadora, emita o seguinte comando.

```
fwcarrier cmd=list
      carrier=
```

Para incluir uma operadora, emita o seguinte comando.

```
fwcarrier cmd=add
    carrier=
    dial=
    method=
    [password=]
    length=
    baud=
    parity=
    databits=
    stopbits=
```

Para modificar os parâmetros da operadora, emita o seguinte comando.

```
fwcarrier cmd=change
    carrier=
    [dial=]
    [method=]
    [password]
    [length=]
    [baud]
    [parity=]
    [databits=]
    [stopbits=]
```

Para eliminar uma operadora, emita o seguinte comando.

```
fwcarrier cmd=delete
    carrier=
```

As definições de parâmetro são:

- carrier** O nome da operadora.
- dial** Deve especificar o número de telefone do modem da operadora para o serviço TAP que você contratou.
- method** O valor deve ser TAP.
- password** Esse é opcional a menos que seja necessário para o serviço da operadora.
- length** O tamanho máximo da mensagem permitido pelo serviço da operadora.
- baud** Especifica a velocidade de transmissão mais confiável suportado pelo serviço da operadora.
- parity** O tipo de teste de paridade suportado pelo serviço da operadora. Geralmente é uma paridade par do protocolo TAP.
- databits** O número de bits de dados suportados pelo serviço da operadora. Geralmente é 7 para o protocolo TAP.
- stopbits** O número de bits de parada suportados pelo serviço da operadora. Geralmente é 1 para o protocolo TAP.

## Configuração do Modem

Para configurar o suporte de notificação do pager, é necessário configurar o modem.

Utilize o comando modem para configurar um modem para enviar pedidos do pager para a operadora do pager.

Para relacionar um modem, emita o seguinte comando.

```
fwmodem cmd=list
modem=
```

Para incluir um modem, emite o seguinte comando.

```
fwmodem cmd=add
modem=
comport=
initstring=
outsideline=
```

Para modificar os parâmetros do modem, emite o seguinte comando.

```
fwmodem cmd=change
modem=
[comport=]
[initstring=]
[outsideline=]
```

Para eliminar um modem, emite o seguinte comando.

```
fwmodem cmd=delete
modem=
```

As definições de parâmetro são:

**modem** Um nome do modem.

**comport** A porta COM serial à qual o modem está conectado. O modem dessa porta COM não deve ser definido para o sistema Windows NT.

**initstring** A cadeia de inicialização para o modem. Os parâmetros da cadeia devem ser adequados a um comando do modem AT, mas o AT não deve ser incluído como parte da cadeia. Os parâmetros especificados devem ser coordenados com os requisitos de comunicação do modem da operadora.

**outsideline** O número de discagem para obter uma linha externa.

## Teste da Configuração do Pager

Para assegurar que você tenha configurado corretamente o pager ativo, use o seguinte comando.

```
pager
carrier=
modem=
pagerid=
message=
```

As definições dos parâmetros são idênticas às aquelas do comando `fwpggr`.

## Vários Pagers

Se você necessitar alterar regularmente o pager ativo, faça o seguinte:

- Certifique-se de ter definido todas as operadoras e modems necessários
- Use `fwpggr` ou o cliente de configuração para definir e salvar uma configuração do pager
- Copie o arquivo `R00TDIR\config\pager.cfg`, dando-lhe um nome que possa ser reconhecido
- Defina uma outra configuração do pager, copie e repita essa operação até ter cópias de todos os arquivos `pager.cfg` que precise
- Copie o arquivo de configuração que queira ativar novamente no `R00TDIR\config\pager.cfg`

Se estiver tentando manipular alterações de troca, configure um job programado usando o Windows NT no comando para repetir automaticamente o último bullet no início de cada troca.

---

## Usuários

Este comando inclui um novo usuário ou modifica um ou mais atributos de um usuário existente do firewall. Todos os parâmetros têm valores-padrão ou são desnecessários em certas circunstâncias. Para `cmd=add`, serão armazenados valores-padrão; para `cmd=change`, os valores existentes serão preservados.

```
fwuser cmd={add|change}
username=LoginName
[fullname="UsersRealName"]
[password={yes|no}]
[pwdvalue=Password]
[level={proxy|admin}]
[secftp=SecureFTPAuthentication]
[remftp=NonSecureFTPAuthentication]
[secauth=SecureTelnetAuthentication]
[remauth=NonSecureTelnetAuthentication]
[secadmin=SecureAdminAuthentication]
[remadmin=NonSecureAdminAuthentication]
[secsocks=SecureSocks]
[remsocks=NonSecureSocks]
[sechttp=SecureHTTP]
[key="SecureNet Key Code"]
[histexpire=HistoryExpiration]
[histsize=HistorySize]
[loginretries=LoginRetries]
[maxage=MaxAge]
[maxexpired=MaxExpiredAge]
[maxrepeats=MaxRepeatChars]
[minalpha=MinAlphaChars]
[mindiff=MinDifferentChars]
[minlen=MinLength]
[minother=MinNonAlphaChars]
[pwdwarntime=PasswordWarnTime]
[userchg={yes|no}]
[pwlocked={yes|no}]
[fg_all={yes|no}]
[fg_dns={yes|no}]
[fg_interfaces={yes|no}]
[fg_logmonitor={yes|no}]
[fg_logs={yes|no}]
[fg_mail={yes|no}]
[fg_netobjs1={yes|no}]
[fg_netobjs2={yes|no}]
[fg_pagers={yes|no}]
[fg_proxyserver={yes|no}]
[fg_user={yes|no}]
[fg_traffic={yes|no}]
```

## Parâmetros Fundamentais

**username** Nome de login do usuário.

**fullname** Nome completo do usuário ou alguma outra informação curta (de uma linha) pertinente ao usuário. Se forem incluídos espaços nesse valor, ele terá que ser colocado dentro de aspas duplas.

**level** O valor padrão é proxy, que indica que o usuário que está sendo criado é um usuário Socks ou proxy simples. Grupos de função de administração e autenticações de administração não se aplicam a usuários proxy.

**key** Chave usada para autenticar a placa Chave SecureNet do 'Digital Pathways' do usuário. Como este valor deve conter espaços, ele precisa ser colocado entre aspas duplas.

## Autenticações

A seguir estão as cadeias de autenticação e seus métodos de autenticação correspondentes. O uso das cadeias de autenticação para os diversos parâmetros do comando `fwuser` está sendo indicado abaixo.

- `permit`—permite tudo
- `deny`—nega tudo
- `password`—senha do firewall
- `NT`—senha de logon do NT
- `snk`—SNK
- `sdi`—SDI
- `user`—autenticações fornecidas pelo usuário
- `userauth2`—autenticações fornecidas pelo usuário
- `userauth3`—autenticações fornecidas pelo usuário

**secftp** Método de autenticação para logins FTP feitos a partir de uma interface protegida. Os valores válidos são `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` e `userauth3`. O padrão é negar (`deny`).

**remftp** Método de autenticação para logins FTP feitos a partir de uma interface não-protegida. Os valores válidos são `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` e `userauth3`. O padrão é negar (`deny`).

**secauth** Método de autenticação para logins telnet feitos a partir de uma interface protegida. Os valores válidos são `deny`, `permit`, `password`, `NT`, `snk`, `sdi` e `user`. O padrão é negar (`deny`).

**remauth** Método de autenticação para logins telnet feitos a partir de uma interface não-protegida. Os valores válidos são `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2`, `userauth3`. O padrão é negar (`deny`).

**secadmin** Método de autenticação para logins de Cliente de Configuração do Firewall feitos a partir de uma interface protegida. Os valores válidos são `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` e `userauth3`. O padrão é `deny` para usuários proxy e `NT` para administradores do Primary Firewall.

**remadmin** Método de autenticação para logins de Cliente de Configuração do Firewall a partir de uma interface não-protegida. Os valores válidos são `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2`, `userauth3`. O padrão é `deny` para usuários proxy e `NT` para usuários do Primary Firewall.

**secsocks** O método de autenticação Socks5 para conexões de cliente Socks provenientes do lado protegido do firewall. Os valores válidos são `deny`, `permit`, `password`, `NT`, `snk`, `sdi`, `user`, `userauth2` e `userauth3`.

Se o servidor Socks5 estiver configurado para métodos de autenticação estilo ID de Usuário/Senha ao invés de CRAM (Challenge Response Authentication Methods), o SNK não funcionará porque o protocolo ID de Usuário/Senha do Socks5 não pode exibir a exigência SNK.

O padrão é negar (`deny`).

**remsocks** O método de autenticação Socks5 para conexões de cliente Socks provenientes do lado não-protetido do firewall. Os valores válidos são deny, permit, password, NT, snk, sdi, user, userauth2 e userauth3.

Se o servidor Socks5 estiver configurado para métodos de autenticação estilo ID de Usuário/Senha ao invés de CRAM (Challenge Response Authentication Methods), o SNK não funcionará porque o protocolo ID de Usuário/Senha do Socks5 não pode exibir a exigência SNK.

O padrão é negar (deny).

**sechttp** Método de autenticação para pedidos HTTP feitos a partir de uma interface protegida. Os valores válidos são deny, permit, password, NT, sdi, user, userauth2 e userauth3.

SNK não é suportado pelo protocolo HTTP porque não há como exibir a exigência SNK ao usuário. SDI é suportado mas uma senha será solicitada ao usuário ao invés de um código de passagem SDI. O usuário deve fornecer seu código de passagem SDI.

**Nota:** fwdfuser não pode ter SNK ou a Senha do Firewall definida em nenhum de seus campos de método de autenticação.

### Parâmetros de Senha do Firewall

**password** Indica se o usuário será solicitado a fornecer senha. Por padrão, isso ocorrerá se for especificado algum método de autenticação que aceite senha.

**pwdvalue** Usado mais freqüentemente em programação de scripts, esse parâmetro permite que o valor de um parâmetro seja especificado na linha de comandos. Note que esse valor é digitado em texto claro e não é obscurecido por "bisbilhoteiros". Não há padrão.

**userchng** Determina como o sinalizador de alterações do administrador será definido no banco de dados do usuário. Um valor sim define o sinalizador de alterações do administrador que solicita ao usuário alterar sua senha na primeira vez em que iniciar sessão. O padrão é não. Este parâmetro só será válido se os parâmetros password=yes e pwdvalue=" forem fornecidos.

**pwlocked** Indica se a senha foi bloqueada. Ele será definido como sim quando o número máximo de logins falhos for ultrapassado ou quando a senha não tiver sido usada para o número de semanas especificado no tempo máximo antes do bloqueio.

**histexpire** Define o período de tempo (em semanas) durante o qual o usuário não pode reutilizar a senha. O valor é uma cadeia de números inteiros. Os valores válidos ficam entre 0 e 52. O valor 0 indica que não há limite a ser definido. O valor padrão é 0.

**histsize** Define o número de senhas antigas que o usuário não pode reutilizar. O valor é uma cadeia de números inteiros. Os valores válidos ficam entre 0 e 20. Válido apenas se histexpire=0. O valor padrão é 5.

**loginretries** Define o número de tentativas mal-sucedidas de login permitidas depois do último login bem sucedido antes de o sistema travar a conta. O valor é uma cadeia de números inteiros. Os valores válidos ficam entre 0 e 20. O valor padrão é 10. Um valor zero ou negativo indica que não há limite. Depois de bloqueada a conta do usuário, o usuário não

poderá iniciar sessão até que o administrador do sistema defina `pwlocked` para `no`.

**maxage** Define a duração máxima (em semanas) de uma senha. A senha deve ser trocada até essa data. O valor é uma cadeia de números inteiros. Os valores válidos ficam entre 0 e 52. O valor 0 indica que não há duração máxima. O padrão é 13.

**maxexpired** Define o tempo máximo (em semanas) além do valor de `maxage` que o usuário tem para mudar a senha vencida. Após esse tempo ser definido, só um usuário administrativo poderá trocá-lo. O valor é uma cadeia de números inteiros. Os valores válidos vão de -1 a 26. Se o atributo `maxexpired` for 0, a senha expirará quando o valor de `maxage` for atingido. Se o atributo for 0, o atributo `maxexpired` será ignorado. O padrão é 3.

**maxrepeats** Define o número máximo de vezes que um caractere pode ser repetido dentro da nova senha. Os valores válidos vão de 0 a 8, mas o valor 0 não tem significado. O valor 8 indica que não há número máximo. O padrão é 2.

**minalpha** Define o número mínimo de caracteres alfabéticos que a senha precisa ter. O valor é uma cadeia de números inteiros. Os valores válidos vão de 0 a 8. O valor 0 indica que não há número mínimo. O padrão é 4.

**mindiff** Define o número mínimo necessário de caracteres na nova senha que não estavam presentes na antiga. O valor é uma cadeia de números inteiros. Os valores válidos vão de 0 a 8. O valor 0 indica que não há número mínimo. O padrão é 3.

**minlen** Define o tamanho mínimo da senha. O valor é uma cadeia de números inteiros. Os valores válidos vão de 0 a 8. O valor 0 indica que não há número mínimo. O padrão é 8.

**minother** Define o número mínimo de caracteres não-alfanuméricos que a nova senha precisa ter. O valor é uma cadeia de números inteiros. Os valores válidos vão de 0 a 8. O valor 0 indica que não há número mínimo. O padrão é 1.

**pwdwarntime** Define o número de dias antes de o sistema emitir aviso indicando a necessidade de troca da senha. O valor é uma cadeia de números inteiros. Os valores válidos ficam entre 0 e 30. Um valor zero ou negativo indica que não vai ser emitida mensagem. O valor padrão é 5.

### Grupos Funcionais de Administração

**fg\_all** Digite sim se o administrador tiver permissão para administrar todos os aspectos do firewall. O padrão é não.

**fg\_dns** Digite sim se o administrador tiver permissão para administrar os Serviços de Nome de Domínio. O padrão é não.

**fg\_interfaces** Digite sim se o administrador tiver permissão para definir interfaces do firewall. O padrão é não.

**fg\_logmonitor** Digite sim se o administrador tiver permissão para administrar limites do Monitor de Logs. O padrão é não.

**fg\_logs** Digite sim se o administrador tiver permissão para administrar Dispositivos de Log. O padrão é não.

- fg\_mail** Digite sim se esse administrador tiver permissão para administrar a gateway de correio do firewall. O padrão é não.
- fg\_netobjs1** Digite sim se o administrador tiver permissão para efetuar a administração básica de Objetos da Rede. O padrão é não.
- fg\_netobjs2** Digite sim se o administrador tiver permissão para efetuar a administração avançada de Objetos da Rede. O padrão é não.
- fg\_pagers** Digite sim se o administrador tiver permissão para administrar a Configuração do Pager. O padrão é não.
- fg\_proxyserver** Digite sim se esse administrador tiver permissão para configurar os daemons proxy do firewall. O padrão é não.
- fg\_traffic** Digite sim se o administrador tiver permissão para administrar o Controle de Tráfego. O padrão é não.
- fg\_user** Digite sim se o administrador tiver permissão para administrar usuários do firewall. O padrão é não.

Para listar todos os atributos de todos os usuários do firewall ou de um único usuário do firewall especificado:

```
fwuser cmd=list  
      [username=username]  
      [type={short|long}]
```

**type={short|long}** O padrão do tipo é longo (long) se for usado nome de usuário. Não sendo usado nome de usuário, o padrão é curto (short).

Para retirar um usuário do firewall:

```
fwuser cmd=delete  
      username=username
```



---

## Capítulo 2. Utilização dos Utilitários de Relatório

Este capítulo mostra como usar os utilitários de relatório do IBM Firewall. A finalidade básica dos utilitários de relatório é gerar arquivos tabulados de informações administrativas dos arquivos de log do firewall.

Os arquivos de texto tabulados podem ser gerados e importados para tabelas em sistema de banco de dados, como o DB2/6000 ou o DB2/2. O administrador pode então usar a Structured Query Language (SQL) para consultar dados e gerar relatórios. Os utilitários também permitem ao administrador criar um arquivo de texto legível com as mensagens do log do firewall.

Os utilitários de relatório se compõem dos seguintes programas e arquivos:

**fwlogtxt** Programa para gerar mensagens de texto completo a partir de um arquivo de log de firewall

**fwlogtbl** Programa para gerar arquivos de importação de banco de dados, em formato DEL (delimitado), a partir de log de firewall e de log de su.

Para usar o programa fwlogtbl e os arquivos DDL, DML e DEL, é preciso ter algum conhecimento a respeito de bancos de dados relacionais e dispor de um banco de dados relacional apropriado.

**fwschema.ddl** Arquivo de instruções de Data Definition Language (DDL) de SQL, próprio para definir as tabelas do banco de dados

**fwimport.dat** Arquivo de instruções de importação do DB2, próprio para importar os arquivos DEL para as tabelas do banco de dados

**fwqrysmpl.dml** Arquivo de instruções de Data Manipulation Language (DML) da SQL, próprio para gerar relatórios de exemplo

**fwlogcvrt** Programa para converter um formato de log do firewall Windows NT no formato de log do firewall AIX. Isto permite que as ferramentas de relatório de outros fornecedores funcionem como antes exceto pelo fato de que novas mensagens talvez não sejam reconhecidas.

Os arquivos DDL e DML são específicos para a família do DB2, mas podem ser modificados para serem usados com outros sistemas de gerenciamento de banco de dados. Arquivos de formato DEL podem ser prontamente importados (carregados) para o DB2/6000, para o DB2/2 e para outros sistemas de arquivos e de bancos de dados. Seu formato simples deve permitir conversão para outros formatos, se necessário.

---

### Utilização dos Utilitários de Relatório

Essas informações explicam como usar os recursos de relatório a partir da linha de comandos. Consulte o *Guia do Usuário IBM eNetwork Firewall* para obter informações sobre o uso dos recursos de relatório a partir do cliente de configuração.

Para exibir o arquivo de log de firewall a partir da linha de comandos, use o **utilitário fwlogtxt**. Consulte “Geração de Mensagens a partir do Arquivo de Log do Firewall” na página 23 para obter mais informações.

Para gerar relatórios com base em informações de log:

1. Instale o banco de dados relacional.
2. Crie um banco de dados vazio.
3. Crie tabelas de log do firewall vazias no banco de dados.
4. Para produzir os arquivos tabulados, execute o **fwlogtbl** da linha de comandos.
5. Importe os arquivos resultantes para preencher as tabelas do banco de dados com dados de log.
6. Produza relatórios executando instruções SQL ou programas SQL.

**Nota:** Os três primeiros passos precisam ser feitos de uma só vez, ao passo que os restantes são repetidos a cada vez que há novos dados de log disponíveis.

---

## Formato do Log do IBM Firewall

Cada entrada do arquivo de log do firewall possui o formato:

Date Time firewall\_name:year;pid:Amsg\_num; msg\_ID;var\_1;...;var\_n;

onde

- Os primeiros três campos, **date**, **time** e **firewall-name** são incluídos pelo recurso de registro do firewall.
- **year** são os quatro caracteres do ano.
- **pid** é a ID de cadeia à qual a entrada se aplica.
- **Amsg\_num** é um número seqüencial inteiro que os Utilitários de Relatório usa para acessar, no arquivo fw\_log.cat, o devido texto de mensagem convertido. O valor numérico msg\_num é imediatamente precedido de uma letra indicadora do nível de log (A). Essa letra indicadora distingue tanto a plataforma que originou o log, quanto as diferenças no formato do log.
- **msg\_ID** é o número externo da mensagem (como ICA0001e).
- **var\_1-n** representa os valores de variáveis de mensagem, sendo que **n** é o número de variáveis da definição da mensagem.

**Nota:** Não direcione outros registros para o mesmo arquivo que o log do firewall. Eles não vão se conformar ao formato exigido pelos utilitários de relatório e os resultados obtidos serão imprevisíveis.

Use o comando fwlogcvrt para converter do formato de log desse release do Windows NT para o de um log AIX. Você pode precisar fazer isso para usar outro fornecedor que informe quais ferramentas suportam os logs do Firewall para AIX. A conversão removerá o indicador do nível de log 'A' que antecede o msg\_num e colocará dois caracteres em branco ao lado dos dois pontos que estão entre o firewall\_name e o ano.

Os parâmetros incluem:

- input**      Entrada padrão redirecionada de um log do Windows NT Firewall.
- output**     Saída padrão, que pode ser redirecionada para um arquivo.

#### fwlogcvrt syntax

fwlogcvrt

Exemplo:

```
fwlogcvrt < fw980212.log >logcvrt.out
```

## Geração de Mensagens a partir do Arquivo de Log do Firewall

Use o comando **fwlogtxt** para gerar mensagens legíveis a partir de entradas de um arquivo de log de firewall.

Os parâmetros incluem:

**input**      Entrada padrão de um arquivo de log do firewall

**output**     Saída padrão

#### sintaxe do fwlogtxt

fwlogtxt

Exemplo:

```
fwlogtxt < fw980212.log >logtxt.out  
fwlogtxt < my.log | find "ICAO"
```

Não há parâmetros para o fwlogtxt; ele recebe informações da entrada padrão e coloca os resultados na saída padrão.

## Geração de Arquivos de Importação de Banco de Dados

Use o comando **fwlogtbl** para criar, gravar por cima ou anexar em arquivos tabulados a partir dos quais o usuário pode preencher as tabelas do banco de dados para gerar relatórios.

Os parâmetros incluem:

**input**      O arquivo de log do firewall.

**output**     Nomes de arquivo:

- a\_alert.tbl
- f\_rule.tbl
- f\_info.tbl
- f\_match.tbl
- f\_stat.tbl
- interfaces.tbl
- nat\_info.tbl
- p\_info.tbl
- p\_ftp.tbl
- p\_http.tbl
- p\_info.tbl
- p\_login.tbl
- p\_stat.tbl
- server\_info.tbl
- session.tbl

s\_ftp.tbl  
s\_info.tbl  
ssl\_info.tbl

#### sintaxe do fwlogtbl

```
fwlogtbl -w [-d OutDir] [-su] LogName  
          |  
          -a
```

Exemplo:

```
fwlogtbl -a -d :\reports fw961031.log
```

- w** Especifica que o arquivo de saída existente deve ser substituído. Se ele não existir, o fwlogtbl vai criá-lo.
- a** Especifica que o arquivo gerado deve ser anexado ao arquivo de saída existente. Se ele não existir, o fwlogtbl vai criá-lo.
- d** Identifica o diretório de saída.
- OutDir** Especifica o diretório em que todos os arquivos de saída devem ser armazenados. Se não houver diretório especificado, os arquivos de saída vão ser armazenados no diretório atual.
- su** Especifica que LogName é o nome de um arquivo de log de su do AIX. Assim, o Windows NT Firewall pode processar o firewall e os arquivos de log su de AIX Firewalls anteriores.

**LogName** Especifica um arquivo de log do firewall ou um arquivo de log AIX.

Os nomes dos arquivos de saída são pré-definidos mas podem ser copiados ou mudados depois de executar o fwlogtbl. Os arquivos de saída possuem formato de arquivo (DEL) ASCII delimitado, sem delimitadores para cadeias de caracteres e usam o ponto-e-vírgula (;) como delimitadores de coluna.

Para saber mais sobre mensagens, leia o Apêndice A, "Mensagens" na página 73.

## Utilização de Banco de Dados com os Utilitários de Relatório

Esta seção descreve arquivos fornecidos com o firewall para criar o banco de dados, para importar informações para o banco de dados e para consultar relatórios. Para quem tem o DB2, o comando db2 pode ser usado com esses arquivos. (Funções similares ao comando db2 podem existir em outros gerenciadores de banco de dados. Pode ser que os arquivos requeiram alterações para serem usados com tais funções.)

Para executar o comando db2, é preciso ter o DB2 instalado e uma 'instância' definida. Consulte a documentação de instalação do DB2. Inicialmente, é preciso usar o comando de criação de banco de dados do DB2 para criar um banco de dados vazio. (Sugerimos chamá-lo de 'fwlog'.) Para isso, digite na linha de comandos:

```
db2cmd
```

Depois, na janela de comandos DB2 resultante, digite:

```
db2 create database fwlog
```

Em seguida, você deve se conectar ao banco de dados fwlog:

```
db2 connect to fwlog
```

As opções -vf do comando db2 podem então ser usadas:

```
db2 -vf fwschema.ddl > schema.out  
db2 -vf fwimport.dat > import.out  
db2 -vf fwqrysmp.dml > report.out
```

Esses passos estão descritos mais detalhadamente nas seções a seguir. Em cada caso, o usuário pode verificar cuidadosamente a saída padrão (redirecionada para um arquivo em cada exemplo). Para importar, também é necessário verificar o arquivo .msg produzido por cada instrução de importação individual.

## Criação de Tabelas

O comando **db2 -vf fwschema.ddl > schema.out** cria todas as tabelas e índices necessários. Dê esse comando uma vez, de preferência depois de instalar o firewall. A ID de usuário atual, no momento em que este exemplo for executado, será a ID do criador das tabelas. Ela pode precisar ser usada como qualificador de tabela (como creatorid.tableName) em instruções SQL posteriores, a menos que elas sejam executadas sob a ID do criador. Assim, quando não se usa a ID do criador, o usuário precisa editar os arquivos fwimport.dat e fwqrysmp.dml para colocar a ID do criador na frente de cada nome de tabela.

O arquivo R00TDIR\sample\report\fwschema.ddl contém as instruções DDL para criar as tabelas do banco de dados necessárias à aceitação das gravações dos arquivos tabulados criados pelo **fwlogtbl**. *ROOTDIR* é o diretório selecionado durante o processo de instalação como local de destino para o IBM Firewall. É preciso examinar o schema.out para determinar se a operação foi bem sucedida. As instruções no arquivo fwschema.ddl podem ser usadas como estão ou podem ser modificadas para trabalhar com vários sistemas de banco de dados. (Os usuários não devem mudar os nomes das tabelas e das colunas.)

## Importação de Dados

O comando **db2 -vf fwimport.dat > import.out** carrega dados de todos os arquivos DEL nas tabelas criadas pelo comando **db2-vf fwschema.ddl**.

O arquivo R00TDIR\sample\report\fwimport.dat contém amostras de instruções referentes à importação dos dados dos arquivos \*.tbl para os bancos de dados DB2. Como foi mencionado antes em “Criação de Tabelas”, se o usuário das importações não for o criador das tabelas, a ID do criador precisará ser colocada na frente de cada nome de tabela.

Cada instrução de importação produz informações no padrão externo e informações adicionais num arquivo tblname.msg, sendo que tblname é específico para cada instrução de importação. O usuário deve verificar as duas formas de saída e determinar se a importação foi bem sucedida. Ao executar todas as instruções de importação desse arquivo com um programa como o DB2, o usuário deve direcionar o padrão externo para um arquivo e depois verificar esse arquivo e cada um dos arquivos .msg. Cada comando de importação produz um arquivo .msg separado. Além disso, o usuário deve repetir o comando **db2 -vf fwimport.dat > import.out** sempre que houver um novo log a ser refletido no banco de dados.

Ao importar arquivos de log grandes, você pode receber códigos de erro de SQL com descrições indicando a necessidade de mais memória ou espaço em disco. Por exemplo: a mensagem pode ser espaço de pilha insuficiente ou espaço de log de transação insuficiente. Esses erros requerem ajuste nas definições de parâmetros para o banco de dados ou para o banco de dados fwlog. Para saber mais informações, leia a documentação do DB2. Uma alternativa temporária para ajustar as definições de parâmetros do DB2 consiste em dividir logs grandes ou arquivos tabulados grandes em arquivos menores.

### **Execução de Consultas de Exemplo**

O comando **db2 -vf fwqrysmp.dml > report.out** executa as consultas de exemplo. O arquivo `R00TDIR:\sample\report\fwqrysmp.dml` contém amostras de instruções SQL que podem fornecer dados de relatório úteis, com base em alguns dos requisitos de consulta. Esses exemplos podem ser gerados para criar seus próprios relatórios. Como foi mencionado antes em “Criação de Tabelas” na página 25, se o usuário das importações não for o criador das tabelas, a ID do criador precisará ser colocada na frente de cada nome de tabela.

Quando as consultas são executadas pela linha de comandos, o DB2 aloca o espaço máximo que ele pode precisar para cada coluna de saída. O resultado pode ser um relatório difícil de ser lido. Pode-se obter resultados mais satisfatórios solicitando menos colunas em cada consulta ou embutindo as instruções de consulta num programa que permita um melhor controle da apresentação.

## **Interface de Usuário para Utilitários de Relatório**

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 ou o comando `fwlogtbl` pode ser usado para executar recursos de relatório no firewall. Em um não-firewall, use a linha de comandos.

## **As Tabelas SQL**

Esta seção define o layout das tabelas SQL.

Cada mensagem de log do firewall ou mensagem de log AIX su é mapeada para uma das seguintes tabelas SQL:

ADMIN\_ALERT  
FILTER\_INFO  
FILTER\_MATCH  
FILTER\_ACTIVE\_RULE  
FILTER\_STATUS  
INTERFACES  
NAT\_INFO  
PAGER\_INFO  
PROXY\_FTP  
PROXY\_HTTP  
PROXY\_INFO  
PROXY\_LOGIN  
PROXY\_STATUS  
SERVER\_INFO  
SESSION  
SOCKS\_FTP  
SOCKS\_INFO  
SSL\_INFO  
SU  
TUNNEL\_CONTEXT  
TUNNEL\_POLICY  
TUNNEL\_STATUS

**Os nomes de tabelas e das colunas não devem ser alterados.** No entanto, você pode aumentar a largura de uma coluna caso se sentir que alguns valores estão sendo truncados.

## Índices

Um registro de log representando um evento de firewall em particular deve aparecer apenas uma vez no banco de dados. Se um administrador importa o mesmo arquivo tabulado várias vezes ou se for importado outro arquivo tabulado, derivado do mesmo arquivo de log, o registro de log pode aparecer mais de uma vez.

Para evitar esse problema, o arquivo de exemplo de definições de banco de dados, `fwschema.dll`, define um índice único em cada tabela que usa esses três campos:

- Nome do arquivo de log que foi a origem do registro (`LOG_FILE`)
- Número da linha desse registro no arquivo de log (`LINE_NUM`)
- Número de repetição da linha, com base na mensagem do syslog 'última mensagem repetida n vezes' (`REPEAT_NUM`)

O índice evita carregar o mesmo número de linha a partir do mesmo arquivo nomeado mais de uma vez. Essa medida, aliada a um gerenciamento cuidadoso dos nomes dos arquivos de log, evita a duplicação dos eventos de log no banco de dados.

Acrescentar outros índices no banco de dados pode melhorar o desempenho da maioria das consultas comuns. Consulte a documentação do banco de dados para saber mais informações a esse respeito.

## Descrições de tabelas

Esta seção mapeia mensagens de log do firewall para tabelas e colunas e aponta para informações que você pode querer consultar para seus relatórios. Todas as mensagens mapeadas para uma tabela em particular estão listadas na nota do final da tabela. As mensagens que fornecem dados para colunas em particular são listadas na descrição dessas colunas. As tabelas contêm mensagens para o IBM Firewall for AIX, o IBM Firewall for NT e mensagens comuns a ambos os firewalls.

Para saber mais sobre mensagens de log do firewall, leia Apêndice A, "Mensagens" na página 73.

Na coluna Tipos de Dados, nas descrições a seguir, 'int' significa tipo de coluna SMALLINT para DB2; 'long int' significa tipo DB2 INTEGER. Os Tipos de Dados data-hora significam DB2 TIMESTAMP. Em data/hora, o valor dos microssegundos será sempre "000000".

Se uma descrição estiver indicada com *obrigatório*, um valor precisa ser especificado para que o registro possa ser digitado na tabela.

As três colunas que servem como índice único e uma coluna para o recebimento do indicador de nível do log são omitidas dessas descrições de tabela porque suas definições são idênticas e normalmente não há motivo para consultá-las.

*Tabela 1 (Página 1 de 2). ADMIN\_ALERT. Esta tabela contém mensagens relacionadas a alertas de intrusão feitos pelo arquivo a\_alert.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID de Usuário (ICA0001, ICA0002, ICA0003, ICA0004, ICA2001, ICA2002, ICA2003, ICA2026, ICA2043, ICA2068, ICA2167, ICA2168, ICA2170, ICA2173, ICA3001, ICA3012, ICA3018)
ACTION	char(7)	connect (ICA3012) ou bind (ICA3018)
NUM_COUNT	int	Número de falhas de autenticação (ICA0001, ICA0002, ICA0003); número de entradas de log para TAG_MSG_NUM (ICA0004); número de dias (ICA9000)
TAG_MSG_NUM	char (8)	Número da mensagem de tag (ICA0004)
SRC_IP	char(15)	Endereço IP fonte (ICA2001, ICA2028, ICA2079, ICA2167, ICA3012, ICA3018)
DST_IP	char(15)	Endereço IP de Destino (ICA2028, ICA2079, ICA3012, ICA3018)
AUTH_METHOD	char(20)	Método de Autenticação (ICA2002, ICA2167, ICA2170)

*Tabela 1 (Página 2 de 2). ADMIN\_ALERT. Esta tabela contém mensagens relacionadas a alertas de intrusão feitos pelo arquivo a\_alert.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
NETWORK	char(25)	Nome da rede (ICA2001, ICA2002, ICA2167)
HOST_NAME	char(100)	Nome do Host (ICA0003, ICA2002)
TIMEOUT_SEC	int	Segundos de time-out (ICA2026)
CONN_USERID	char(16)	Nome do usuário da conexão de soquetes (ICA3001)
APPLICATION	char(30)	Nome da aplicação como telnet, ftp, ... (ICA2167, ICA2168, ICA2170, ICA3012)
<b>Nota:</b> Mensagens Correlatas: ICA0001 ICA0002 ICA0003 ICA0004 ICA0005 ICA0006 ICA0007 ICA0008 ICA0009 ICA0010 ICA0011 ICA0012 ICA0013 ICA0014 ICA0015 ICA0016 ICA0017 ICA0018 ICA0019 ICA0020 ICA0021 ICA0022 ICA1010 ICA2001 ICA2002 ICA2003 ICA2020 ICA2026 ICA2028 ICA2037 ICA2040 ICA2042 ICA2043 ICA2079 ICA2167 ICA2168 ICA2170 ICA2173 ICA3001 ICA3012 ICA3018 ICA9000 ICA9001		

*Tabela 2. FILTER\_ACTIVE\_RULE. Esta tabela contém regras de FILTRO ativas do arquivo f\_rule.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
RULE_NUM	int	Número da Regra (obrigatório)
RULE	char(150)	Regra (obrigatório)
<b>Nota:</b> Mensagem Afim: ICA1037		

*Tabela 3 (Página 1 de 2). FILTER\_INFO. Esta tabela contém mensagens de erro ou mensagens informativas em geral relacionadas aos FILTROS do arquivo f\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
RULE_NUM	int	Número da regra de filtro (ICA1005)

Tabela 3 (Página 2 de 2). FILTER\_INFO. Esta tabela contém mensagens de erro ou mensagens informativas em geral relacionadas aos FILTROS do arquivo f\_info.tbl.

Coluna	Tipos de Dados	Descrição Resumida
ERROR_NUM	int	Número de Erro do Sistema -- número de erro AIX ou Último Erro Windows NT (ICA1007, ICA1008, ICA1009, ICA1011 ICA1013, ICA1015, ICA1021, ICA1023, ICA1024)  O texto correspondente a este número de erro pode ser obtido através da função _strerror. O texto para o Último Erro Windows NT está disponível através da função Format Message ou no Apêndice A do Win32 Programmer's Reference Volume 2.
LOAD_PATH	char(100)	Caminho de carregamento da extensão do kernel (ICA1011, ICA1012)
DVC_DRV	char(25)	Controlador de dispositivo (ICA1021)
TERM_SIG	char(25)	Sinal de término (ICA1260)
FILE_NAME	char(100)	Nome de Arquivo (ICA1024)
RC	int	Código de retorno interno do firewall (ICA1019)
<b>Nota:</b> Mensagens Relacionadas: ICA1001 ICA1002 ICA1003 ICA1005 ICA1007 ICA1008 ICA1009 ICA1011 ICA1012 ICA1013 ICA1014 ICA1015 ICA1016 ICA1017 ICA1019 ICA1021 ICA1022 ICA1023 ICA1024 ICA1200 ICA1260		

Tabela 4 (Página 1 de 2). FILTER\_MATCH. Esta tabela contém as regras de filtro compatíveis com o arquivo f\_match.tbl.

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
RULE_NUM	int	Número da Regra (obrigatório)
ACTION	char(6)	Tipo de regra: permitir, negar, etc.
DIRECTION	char (8)	Direção em que o pacote estava indo: de entrada ou de saída (obrigatório)
SRC_IP	char(15)	endereço de IP do emissor (obrigatório)
DST_IP	char(15)	Endereço de IP do destinatário (obrigatório)
PROTOCOL	char(7)	Protocolo de alto nível como UDP, IPIP, ICMP, TCP ou TCP/ACK (obrigatório)

Tabela 4 (Página 2 de 2). FILTER\_MATCH. Esta tabela contém as regras de filtro compatíveis com o arquivo f\_match.tbl.

Coluna	Tipos de Dados	Descrição Resumida
SRC_PORT	int	<ul style="list-style-type: none"> <li>Tipo de Pacote de IP de ICMP</li> <li>Número da porta do protocolo de recursos dos outros (obrigatório)</li> </ul>
DST_PORT	int	<ul style="list-style-type: none"> <li>Pacote de IP de ICMP</li> <li>Número da porta do protocolo de destino dos outros (obrigatório)</li> </ul>
ROTEAMENTO	char(5)	Afiliação de roteamento dos pacotes: rota ou local (obrigatório)
INTERFACE	char(10)	Tipo de interface: protegida ou não-protegida (obrigatório)
FRAGMENT	char (8)	Identifica se o pacote é fragmento ou não-fragmento (obrigatório)
TUNNEL_ID	int	ID do Túnel (obrigatório)
ENCRYPTION	char(7)	Algoritmo da criptografia: DES_CBC ou CDMF ou nenhum
BYTES	long int	Tamanho do pacote específico (obrigatório)
<b>Nota:</b> Mensagem Afim: ICA1036		

Tabela 5. FILTER\_STATUS. Esta tabela contém informações sobre mudanças de status dos filtros feitas pelo arquivo f\_stat.tbl file.

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
DAEMON	char(25)	Daemon de registro do filtro AIX (ICA1004) ou serviço de registro do filtro Windows NT.
VERSION	int	Número da Versão (ICA1004, ICA1033)
RELEASE	int	Número do release (ICA1004, ICA1033)
PACKET_LOGGING	char (8)	Status de registro do pacote ativado ou desativado (ICA1035)
<b>Nota:</b> Mensagens Relacionadas: ICA1004 ICA1032 ICA1033 ICA1034 ICA1035. Os detalhes da regra de filtro(ICA1032) podem ser obtidos pela tabela FILTER_ACTIVE_RULE.		

*Tabela 6. INTERFACES. Esta tabela contém as informações da mensagem de configuração (adaptador) do arquivo interface.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
IP	char(15)	Endereço IP para o adaptador (ICA9038, ICA9039, ICA9040)
OLD_MASK	char(15)	valor da máscara anterior (ICA9040)
NEW_MASK	char(15)	valor da máscara anterior (ICA9040)
<b>Nota:</b> Mensagens Correlatas: ICA9037, ICA9038, ICA9039, ICA9040, ICA9041		

*Tabela 7. NAT\_INFO. Esta tabela contém informações de mensagens da Conversão de Endereços da Rede feitas pelo arquivo nat\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
VERSION	int	Número da Versão NAT (ICA9033)
RELEASE	int	Número do Release do NAT (ICA9033)
IP	char(15)	Endereço IP (ICA9035, ICA9036)
<b>Nota:</b> Mensagens Relacionadas: ICA9032, ICA9033, ICA9034, ICA9035, ICA9036		

*Tabela 8 (Página 1 de 2). PAGER\_INFO. Esta tabela contém informações relacionadas ao recurso de paginação do Firewall, feitas pelo arquivo pgr\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID de usuário (ICA4036, ICA4174, ICA4175)

*Tabela 8 (Página 2 de 2). PAGER\_INFO. Esta tabela contém informações relacionadas ao recurso de paginação do Firewall, feitas pelo arquivo pgr\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
ERROR_NUM	int	Número de Erro do Sistema - número de erro AIX ou Último Erro do Windows NT (ICA4371)
PROGRAM	char(25)	Nome do Programa (ICA4000)
SIGNAL	int	Sinal de término (ICA4000)
ID	int	Identificador (ICA4036)
PRIORITY	int	Prioridade (ICA4036)
PERIOD	int	Período (ICA4036)
RETRY_COUNT	int	Número de novas tentativas (ICA4036, ICA4313, ICA4314, ICA4364, ICA4365)
FROM_ENTRY	char(15)	Nome da Função (ICA4036)
HOST_NAME	char(100)	Nome do Host (ICA4174, ICA4175)
MESSAGE_TEXT	char(250)	Texto da página (ICA4036, ICA4353 - 4360, ICA4368, ICA4372)
SERVICE	char(25)	Nome do Serviço (ICA4017)
SOCKET	int	Número do soquete (ICA4017)
FILENAME	char(100)	Nome de arquivo (ICA4154, ICA4351, ICA4352)
<b>Nota:</b> Mensagens Correlatas: ICA4000 ICA4001 ICA4007 ICA4017 ICA4036 ICA4154 ICA4168 ICA4174 ICA4175, ICA4300 - 4303, ICA4305 - 4315, ICA4351 - 4360, ICA4362 - 4372)		

*Tabela 9 (Página 1 de 2). PROXY\_FTP. Esta tabela contém informações da ação FTP de sessões FTP feitas pelo arquivo p\_ftp.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID do Usuário (obrigatório)
SRC_IP	char(15)	Endereço de IP do Usuário (obrigatório)
DST_IP	char(15)	Endereço de IP da máquina remota (obrigatório)
ACTION	char(5)	Ação de transferência do arquivo: put ou get (obrigatório)
FILE_NAME	char(100)	Nome de Arquivo
BYTES	long int	Quantidade de dados transferidos
SID	long int	ID de sessão única (obrigatório)

*Tabela 9 (Página 2 de 2). PROXY\_FTP. Esta tabela contém informações da ação FTP de sessões FTP feitas pelo arquivo p\_ftp.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
<b>Nota:</b> Mensagem Relacionada: ICA2075		

*Tabela 10. PROXY\_HTTP. Esta tabela contém informações de ação HTTP de sessões Proxy feitas pelo arquivo p\_http.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
STATUS	int	Status (obrigatório)
SRC_IP	char(15)	Endereço de IP do usuário (obrigatório)
REQUEST	char(250)	Conteúdo do pedido de HTTP (obrigatório)
BYTES	long int	Quantidade de dados transferidos.
<b>Nota:</b> Mensagem Relacionada: ICA2099		

*Tabela 11 (Página 1 de 3). PROXY\_INFO. Esta tabela contém mensagens de erro ou mensagens informativas em geral relacionadas ao PROXY feitas pelo do arquivo p\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID de Usuário (ICA2018, ICA2019, ICA2057, ICA2058, ICA2166, ICA2177, ICA2172)

Tabela 11 (Página 2 de 3). PROXY\_INFO. Esta tabela contém mensagens de erro ou mensagens informativas em geral relacionadas ao PROXY feitas pelo do arquivo p\_info.tbl.

Coluna	Tipos de Dados	Descrição Resumida
ERROR_NUM	int	Número de Erro do Sistema - número de erro AIX ou Último Erro Windows NT (ICA2005, ICA2006, ICA2009, ICA2029, ICA2035, ICA2038, ICA2039, ICA2052, ICA2054, ICA2055, ICA2056, ICA2057, ICA2058, ICA2059, ICA2063, ICA2064, ICA2065, ICA2066, ICA2067, ICA2068, ICA2069, ICA2069, ICA2070, ICA2071, ICA2074, ICA2110, ICA2111, ICA2113, ICA2114, ICA2115, ICA2118, ICA2119, ICA2121, ICA2122, ICA2123, ICA2124, ICA2200, ICA2201, ICA2202, ICA2203)  O texto de número de erro (Erros do Sistema AIX) pode ser obtido por meio da função _strerror. O texto para o Último Erro Windows NT está disponível através da função Format Message ou no Apêndice A do Win32 Programmer's Reference Volume 2.
OPTION_VAL	char(20)	Sinalizador de opção ou valor do parâmetro (ICA2014, ICA2015, ICA2049, ICA2050)
TIME	char(15)	Intervalo de hora inválido (ICA2044, ICA2202)
RC	int	Código de retorno do Firewall Interno (ICA2007, ICA2030, ICA2031, ICA2033, ICA2034, ICA2054, ICA2057, ICA2058, ICA2065, ICA2120 ICA2166, ICA2203)
INVOC_NAME	char(20)	Nome de chamada do soquete ou porta na hora que o erro de sistema ocorreu (ICA2055, ICA2056)
AUDIT_TYPE	char(7)	Tipo de audit. desconhecido (7 dígitos hexadecimais) (ICA2004)
HOST_NAME	char(100)	Nome do host (ICA2106, ICA2107, ICA2126)
FILE_NAME	char(100)	Nome do arquivo (ICA2029, ICA2030, ICA2072, ICA2183, ICA2204, ICA2205, ICA2206, ICA2207)
LINE_NUM	int	Número da linha (ICA2029, ICA2030)
PROTOCOL	char(25)	Nome de protocolo inválido (ICA2112, ICA2116)
CUSTOMIZED_ATTR	char(25)	Número de intervalo (ICA2105, ICA2106, ICA2125, ICA2166)
ODM_ERR_NUM	int	Número do erro do Gerenciador de Dados do Objeto (ICA2102, ICA2103, ICA2104, ICA2105, ICA2107, ICA2108, ICA2109, ICA2125)
APPLICATION (somente NT)	char(30)	Nome da aplicação (ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)
CALLER (somente NT)	char(25)	Chamando função (ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)

Tabela 11 (Página 3 de 3). PROXY\_INFO. Esta tabela contém mensagens de erro ou mensagens informativas em geral relacionadas ao PROXY feitas pelo do arquivo p\_info.tbl.

Coluna	Tipos de Dados	Descrição Resumida
FAILED_IN (somente NT)	char(25)	Falha na função (ICA2201, ICA2203)
<b>Nota:</b> Mensagens Correlatas: ICA2004 ICA2005 ICA2006 ICA2007 ICA2009 ICA2014 ICA2015 ICA2018 ICA2019 ICA2023 ICA2029 ICA2030 ICA2031 ICA2032 ICA2033 ICA2034 ICA2035 ICA2038 ICA2039 ICA2044 ICA2045 ICA2046 ICA2047 ICA2048 ICA2049 ICA2050 ICA2051 ICA2052 ICA2053 ICA2054 ICA2055 ICA2056 ICA2057 ICA2058 ICA2059 ICA2060 ICA2061 ICA2062 ICA2063 ICA2064 ICA2065 ICA2066 ICA2067 ICA2068 ICA2069 ICA2070 ICA2071 ICA2072 ICA2073 ICA2074 ICA2100 ICA2102 ICA2103 ICA2104 ICA2105 ICA2109 ICA2110 ICA2111 ICA2112 ICA2113 ICA2114 ICA2115 ICA2116 ICA2117 ICA2118 ICA2119 ICA2120 ICA2121 ICA2122 ICA2123 ICA2124 ICA2125 ICA2126 ICA2127 ICA2166 ICA2171 ICA2172 ICA2183 ICA2200 ICA2201 ICA2202 ICA2203 ICA2204 ICA2205 ICA2206 ICA2207		

Tabela 12. PROXY\_LOGIN. Esta tabela contém informações (relacionadas basicamente à autenticação) sobre logins PROXY bem sucedidos feitos pelo arquivo p\_login.tbl.

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID do Usuário (obrigatório)
APPLICATION	char(30)	Nome da aplicação - telnet, ftp, ... (obrigatório)
AUTH_METHOD	char(15)	Método de autenticação (obrigatório)
NETWORK	char(25)	Rede (protegida/não-protegida - pode ter também informações adicionais) (obrigatório)
HOST_NAME	char(100)	Nome do host (obrigatório)
<b>Nota:</b> Mensagens Correlatas: ICA2024 ICA2025 ICA2169		

Tabela 13 (Página 1 de 2). PROXY\_STATUS. Esta tabela contém informações sobre status do PROXY dadas pelo arquivo p\_stat.tbl.

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)

*Tabela 13 (Página 2 de 2). PROXY\_STATUS. Esta tabela contém informações sobre status do PROXY dadas pelo arquivo p\_stat.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
USERID	char(16)	ID do Usuário (ICA2008, ICA2016, ICA2021)
SRC_IP	char(15)	Endereço IP fonte (ICA2000, ICA2008, ICA2010, ICA2011, ICA2012, ICA2013, ICA2141, ICA2180)
DST_IP	char(15)	Endereço de IP de Destino (ICA2000, ICA2010, ICA2011, ICA2012, ICA2013)
REMOTE_HOST	char(100)	Nome do host remoto (da perspectiva da máquina de firewall) (ICA2021, ICA2022, ICA2027)
SID (somente NT)	int	Identificador de sessão (ICA2177, ICA2180, ICA2181 ICA2182)
SOCKET (somente NT)	char(25)	Nome do soquete (ICA2177)
RC (somente NT)	int	Código de retorno ou de motivo (ICA2181, ICA2182)
CMD (somente NT)	char(36)	Cartão SMTP (ICA2182)
<b>Nota:</b> Mensagens Correlatas: ICA2000 ICA2010 ICA2011 ICA2012 ICA2013 ICA2016 ICA2021 ICA2022 ICA2027 ICA2097 ICA2098 ICA2141 ICA2163 ICA2164 ICA2165 ICA2177 ICA2180 ICA2181 ICA2182		

*Tabela 14. SERVER\_INFO. Esta tabela contém informações sobre o status e as atividades do Servidor de Configuração, dadas pelo arquivo srv\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID do Usuário (ICA9003, ICA9004)
ERROR_NUM	int	Número do Erro do Sistema – número de erro AIX ou Último Erro Windows NT (ICA9008, ICA9009)  O texto de número de erro (Erros do Sistema AIX) pode ser obtido por meio da função strerror. O texto para o Último Erro Windows NT está disponível através da função Format Message ou no Apêndice A do Win32 Programmer's Reference Volume 2.
<b>Nota:</b> Mensagens Relacionadas: ICA9003 ICA9004 ICA9005 ICA9006 ICA9007 ICA9008 ICA9009 ICA9010 ICA9011 ICA9012 ICA9013 ICA9014 ICA9015		

*Tabela 15. SESSION. Esta tabela contém informações sobre iniciar/parar sessão SOCKS e PROXY dadas pelo arquivo session.tbl.*

Coluna	Tipos de Dados (tamanho)	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX AIX, ID da cadeia NT, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID do Usuário (obrigatório)
SERVICE_TYPE	char(10)	Tipo de serviço: soquetes ou proxy (obrigatório)
APPLICATION	char(30)	Nome da aplicação - telnet, ftp, .... (obrigatório)
SRC_IP	char(15)	Endereço de IP do usuário (obrigatório)
DST_IP	char(15)	Endereço de IP da máquina remota (obrigatório)
SESSION_EVENT	char(5)	<ul style="list-style-type: none"> <li>• início quando a sessão é estabelecida.</li> <li>• final quando a sessão é encerrada.</li> </ul> (obrigatório)
BYTES	long int	Quantidade de dados transferidos durante a sessão. Se a aplicação for telnet, ela será 0.
SID	long int	Identificador exclusivo da sessão, gerado pelo Firewall e baseado na hora de relógio.

**Nota:**

Mensagens Relacionadas:

- Início de Sessão Safemail: ICA2178
- Término da Sessão Safemail: ICA2179
- Início da Sessão de Socks: ICA3011
- Término da Sessão de Socks: ICA3015
- Início da Sessão Telnet Proxy: ICA2036 (Logs AIX) ICA2208, ICA2218 (Logs NT)
- Término da Sessão Telnet Proxy: ICA2077 (Logs AIX) ICA2209, ICA2219 (Logs NT)
- Início da Sessão FTP Proxy: ICA2041 (Logs AIX) ICA2208, ICA2218 (Logs NT)
- Término da Sessão FTP Proxy: ICA2076 (Logs AIX e NT)

Os detalhes das ações da sessão Socks FTP estão na tabela SOCKS\_FTP. Os detalhes das ações da sessão Proxy FTP estão na tabela PROXY\_FTP.

*Tabela 16 (Página 1 de 2). SOCKS\_FTP. Esta tabela contém informações de ações SOCKS FTP de sessões FTP dadas pelo arquivo s\_ftp.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)

*Tabela 16 (Página 2 de 2). SOCKS\_FTP. Esta tabela contém informações de ações SOCKS FTP de sessões FTP dadas pelo arquivo s\_ftp.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID do Usuário (obrigatório)
SRC_IP	char(15)	Endereço de IP do Usuário (obrigatório)
DST_IP	char(15)	Endereço de IP da máquina remota (obrigatório)
DATA_BIND	char(5)	<ul style="list-style-type: none"> <li>'iniciar' quando a ligação de dados é estabelecida.(ICA3010)</li> <li>'parar' quando a ligação de dados é encerrada.(ICA3014)</li> </ul> (obrigatório)
BYTES	long int	Quantidade de dados transferidos.
<b>Nota:</b> Mensagens Correlatas: ICA3010 ICA3014		

*Tabela 17 (Página 1 de 2). SOCKS\_INFO. Esta tabela contém mensagens de erro ou com informações gerais relativas ao Socks do arquivo s\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
USERID	char(16)	ID de Usuário (ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
ACTION	char(7)	connect (ICA3044, ICA3049) ou bind (ICA3046, ICA3047)
ERROR_NUM	int	Número de Erro do Sistema - número de erro AIX (ICA3013, ICA3019, ICA3031, ICA3032, ICA3040, ICA3044, ICA3101, ICA3102, ICA3103, ICA3104, ICA3106, ICA3107, ICA3108, ICA3122, ICA3124, ICA3125, ICA3126, ICA3128)
SRC_HOST	char(25)	Nome do host de origem (ICA3019, ICA3035)
DST_HOST	char(25)	Nome do host de destino (ICA3016, ICA3045)
SRC_IP	char(15)	Endereço Fonte (ICA3042, ICA3043, ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)

*Tabela 17 (Página 2 de 2). SOCKS\_INFO. Esta tabela contém mensagens de erro ou com informações gerais relativas ao Socks do arquivo s\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DST_IP	char(15)	Endereço de Destino (ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
LINE_NUM	int	Número da Linha (ICA3022, ICA3023, ICA3024, ICA3025, ICA3026, ICA3109, ICA3110, ICA3111, ICA3112, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120); ou Número de de linhas (ICA3113)
EXEC_STATUS	int	Status da execução (ICA3027)
CMD	char(36)	Comando, como login (ICA3027, ICA3039, ICA3042, ICA3044, ICA3048) nota: para ICA3042, o comando está em formato hexadecimal
FILE_NAME	char(100)	Nome de Arquivo (ICA3030, ICA3032, ICA3105, ICA3109, ICA3110, ICA3111, ICA3112, ICA3113, ICA3114, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120)
APPLICATION	char(30)	Nome da aplicação - telnet, ftp... . (ICA3044, ICA3045, ICA3049)
VERSION	char(10)	Número da versão dos soquetes em hex (ICA3043)
<b>Nota:</b> Mensagens Relacionadas: ICA3013 ICA3016 ICA3017 ICA3019 ICA3022 ICA3023 ICA3024 ICA3025 ICA3026 ICA3027 ICA3030 ICA3031 ICA3032 ICA3033 ICA3035 ICA3039 ICA3040 ICA3041 ICA3042 ICA3043 ICA3044 ICA3045 ICA3046 ICA3047 ICA3048 ICA3049 ICA3052 ICA3101 ICA3102 ICA3103 ICA3104 ICA3105 ICA3106 ICA3107 ICA3108 ICA3109 ICA3110 ICA3111 ICA3112 ICA3113 ICA3114 ICA3115 ICA3116 ICA3117 ICA3118 ICA3119 ICA3120 ICA3121 ICA3122 ICA3123 ICA3124 ICA3125 ICA3126 ICA3127 ICA3128		

*Tabela 18. SSL\_INFO. Esta tabela contém informações sobre o status e atividades do SSL fornecidas pelo arquivo ssl\_info.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
Client_IP	char(15)	Endereço de IP do cliente
<b>Nota:</b> Mensagens Relacionadas: ICA5015 ICA5022 ICA5023 ICA5028 ICA5029 ICA5036 ICA5039 ICA5060 ICA5063 ICA5082 ICA5120		

*Tabela 19. SU. Esta tabela contém detalhes sobre atividades SU do arquivo su.tbl se você estiver carregando um log su do AIX.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)  Como o AIX não registra o ano no arquivo de log do su, a porção do ano da coluna DATE_TIME é definida ou para o ano corrente ou para o ano anterior, com base das definições de mês/dia (se mês/dia for posterior ao mês/dia atual, o sistema assume que se trata do ano anterior).
FROM_USERID	char(16)	ID do Usuário (obrigatório)
TO_USERID	char(16)	ID do Usuário (obrigatório)
LOGIN_STATUS	char(7)	Status da tentativa de login: sucesso ou insucesso (obrigatório)

*Tabela 20. TUNNEL\_CONTEXT. Esta tabela contém as especificações de contexto do TÚNEL ativo, feitas pelo arquivo t\_cntxt.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
TUNNEL_ID	long int	ID do Túnel (obrigatório)
SRC_IP	char(15)	Endereço de IP da Origem (obrigatório)
DST_IP	char(15)	Endereço de IP do Destino (obrigatório)
ENCRYPTION	char(7)	Algoritmo da criptografia  DES_CBC ou CDMF

**Nota:** Mensagem Relacionada: ICA1043

*Tabela 21 (Página 1 de 2). TUNNEL\_POLICY. Esta tabela contém instruções do regulamento do TÚNEL dadas pelo arquivo t\_policy.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)

*Tabela 21 (Página 2 de 2). TUNNEL\_POLICY. Esta tabela contém instruções do regulamento do TÚNEL dadas pelo arquivo t\_policy.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
POLICY	char(60)	Instrução do regulamento lida no arquivo fwpolicy (obrigatório)
<b>Nota:</b> Mensagem Correlata: ICA1040		

*Tabela 22. TUNNEL\_STATUS. Esta tabela contém informações sobre alterações de status de TÚNEIS dadas pelo arquivo t\_stat.tbl.*

Coluna	Tipos de Dados	Descrição Resumida
DATE_TIME	date_time	Data e hora para a ação (obrigatório)
FIREWALL	char(100)	Nome qualificado completo da máquina firewall (obrigatório)
PID	int	ID do Processo AIX, ID da cadeia NT (obrigatório)
MSG_NUM	int	Número de mensagem (obrigatório)
SESSION_SCKT	long int	Porta do soquete da sessão (para ICA1038)
MASTER_SCKT	long int	Porta do soquete principal (para ICA1038)
TUNNEL_ID	long int	ID do Túnel eliminado (para ICA1041)
<b>Nota:</b> Mensagens Correlatas: ICA1038 ICA1039 ICA1041 ICA1042 <ul style="list-style-type: none"> <li>Os detalhes do regulamento definido(ICA1039) podem ser obtidos pela tabela TUNNEL_POLICY.</li> <li>Os detalhes do contexto de túnel definido(ICA1042) podem ser obtidos pela tabela TUNNEL_CONTEXT.</li> </ul>		

---

## Capítulo 3. Kit de Desenvolvimento de Software Plug-in do SafeMail

A principal finalidade do gateway do IBM Firewall SafeMail é encaminhar correspondências entre as redes protegida e não-protégida enquanto oculta os nomes dos hosts na rede protegida.

O gateway do SafeMail não apresenta nenhuma capacidade de filtragem de conteúdo por si próprio. No entanto, você pode gravar um Projetor de Conteúdo do SafeMail e instalá-lo no Firewall como um plug-in do gateway do SafeMail. O plug-in do gateway do SafeMail possui a habilidade para visualizar a mensagem de e-mail inteira e projetar o e-mail de acordo com os critérios estabelecidos por você. O plug-in do gateway do SafeMail pode pedir ao gateway do SafeMail para abortar a transferência de uma mensagem ou permitir que a mensagem flua pelo gateway.

---

### Visão Geral do Processamento do SafeMail

Quando um cliente SMTP conecta-se ao gateway do SafeMail, o gateway do SafeMail conecta-se ao servidor SMTP de destino e transmite a mensagem de e-mail uma linha por vez, do cliente ao servidor de destino, a medida que recebe as linhas de e-mail do cliente. O gateway do SafeMail irá reescrever algumas linhas de cabeçalho do e-mail conforme necessário para ocultar os nomes dos hosts da rede protegida.

Se um plug-in projetor de conteúdo estiver instalado, o gateway do SafeMail irá chamar o projetor de conteúdo com cada linha da mensagem de e-mail a medida que passa pelo gateway. O gateway do SafeMail também transmite informações sobre a origem e o destino da mensagem de e-mail e outras informações para que o projetor de conteúdo possa correlacionar as diversas chamadas entre si. Isto é útil em casos nos quais a mensagem inteira precisa ser analisada antes que o projetor de conteúdo possa tomar uma decisão sobre permitir ou não que a mensagem flua pelo Firewall.

Se o gateway do SafeMail tiver que reescrever algum dos cabeçalhos para ocultar os nomes dos hosts na rede protegida, o plug-in do projetor de conteúdo será chamado antes do cabeçalho ser reescrito.

---

### Criação de um Plug-in do Gateway do SafeMail

Para criar e instalar um plug-in do gateway do SafeMail, é necessário:

- Gravar o código fonte para a DLL do plug-in
- Gerar a DLL
- Instalar a DLL no Firewall

ROOTDIR\samples\safemail contém código amostra para um plug-in do projetor de conteúdo, os arquivos de cabeçalho necessários e arquivos de exemplo para o IBM Visual Age and Microsoft Visual C++. *ROOTDIR* é o diretório selecionado durante o processo de instalação como local de destino para o IBM Firewall.

## Gravação do Código Fonte

O plug-in do projetor de conteúdo deve implementar uma função denominada `UsrCheck`, que possui o seguinte protótipo:

```
int _Export UsrCheck(pCheckData Data);
```

Este é o ponto de entrada que o gateway do SafeMail chama quando ele possui uma linha de uma mensagem de e-mail pronta para o projetor de conteúdo verificar. Esta função é responsável pelo exame da linha da mensagem de e-mail e por retornar 0 se ele desejar que a mensagem de e-mail continue a fluir pelo gateway do SafeMail ou diferente de zero se desejar que o SafeMail aborte o processamento da mensagem.

Veja o código amostra no `usrcheck.c` in `R00TDIR\samples\safemail` para obter uma descrição completa da interface entre o gateway do SafeMail e o projetor de conteúdo.

O parâmetro `pCheckData` na função de Verificação é uma estrutura C documentada no `usrcheck.h` in `R00TDIR\samples\safemail`. Esta estrutura contém informações importantes sobre a mensagem de e-mail sendo processada, como os endereços de origem e destino dos servidores SMTP e os tipos de redes (protegida ou não-protegida) para o envio e recepção de servidores SMTP. Esta estrutura também contém um correlator de conversação, que irá permitir que o projetor de conteúdo correlacione diversas chamadas com a mesma mensagem de e-mail.

## Geração da DLL

Depois de ter gravado o código fonte para o plug-in do projetor de conteúdo, você deve compilar e conectar-se a uma DLL. A DLL deve ser chamada de `smusr.dll`. E o ponto de entrada `UsrCheck` deve ser exportado a partir da DLL. Veja os `make files` amostra no `R00TDIR\samples\safemail` para obter exemplos de compilações e conexões apropriadas necessárias para gerar a DLL corretamente. `Makefiles` amostras são fornecidos para o IBM VisualAge C++ e para o Microsoft Visual C.

## Instalando a DLL

Depois de gerar com sucesso a `smusr.dll`, você deve instalá-la no Firewall. Copie a `smusr.dll` para o diretório `\bin` do Firewall. Depois, utilize o Gerenciador de Controle de Serviços a partir do Painel de Controle do Windows NT para interromper e reinicializar o servidor do IBM Firewall SafeMail para que o plug-in seja carregado.

O IBM Firewall envia a `smusr.dll` de amostra no diretório `\bin` do Firewall. Renomeie esta DLL antes de copiar sua `smusr.dll` para este diretório para que possa restaurá-la caso remova seu plug-in futuramente.

Os nomes do compilador variam de instância para instância neste capítulo e nos dois próximos capítulos. Todos os três capítulos referem-se aos mesmos dois compiladores.

---

## Capítulo 4. Kit de Desenvolvimento de Software Plug-in do Compactador de Registro

O daemon de registro do IBM Firewall grava informações de log nos arquivos especificados com o quadro de diálogo **Recursos de Log** do cliente de configuração. Depois, você utiliza o comando `fwlogmgmt` para compactar periodicamente registros de log antigos. Geralmente, você executa o comando `fwlogmgmt` a partir do Windows NT Scheduler. Por padrão, o comando `fwlogmgmt` compacta registros de log antigos em um diretório e os comprime utilizando o comando de compactação do Windows NT. No entanto, você pode gravar um plug-in do Compactador de Log para substituir o comportamento do arquivo compactado padrão.

---

### Criação de um Plug-in do Compactador de Log

Para criar um plug-in do Compactador de Log você deve:

1. Gravar o código fonte para a DLL do plug-in
2. Gerar a DLL
3. Instalar a DLL no Firewall

O diretório `R00TDIR\sample\logarch` contém código amostra para um plug-in do compactador de log que duplica o comportamento padrão do Firewall e arquivos de amostra para o IBM Visual Age for C++. *R00TDIR* é o diretório selecionado durante o processo de instalação como local de destino para o IBM Firewall.

### Gravação do Código Fonte

O plug-in do Compactador de Log deve implementar um conjunto de funções que o Firewall utiliza para realizar uma função de compactação. Os protótipos para estas funções estão definidos no `fwarch.h` no diretório `R00TDIR\sample\logarch`.

Estas funções implementam funções de compactação básicas como incluir, extrair, renovar e listar a partir de um arquivo compactado.

Veja o código amostra no `fwarch.c` no diretório `R00TDIR\sample\logarch` para obter mais detalhes sobre estas funções.

### Geração da DLL

Depois de ter gravado o código fonte para o plug-in do Compactador de Log, você deve compilar e conectar este a uma DLL. A DLL deve ser chamada de `fwarch.dll`. Todas as funções listadas no `fwarch.h` devem ser exportadas a partir da DLL.

Um arquivo de amostra para o IBM VisualAge for C++ gerar o código amostra na DLL adequada é fornecido no diretório `R00TDIR\sample\logarch`.

## Instalação da DLL

Depois de gerar com sucesso a fwarch.dll, instale-a Firewall. Copie a fwarch.dll para o diretório ROOTDIR\bin.

A fwarch.dll padrão do Firewall também está localizada neste diretório. Faça uma cópia de segurança ou renomeie esta DLL antes de copiar sua DLL de substituição para o diretório.

Além disso, certifique-se de que o comando fwlogmgmt não está sendo executado no momento e de que o daemon do log do IBM Firewall não está em execução durante a substituição da DLL padrão. Utilize o Gerenciador de Controle de Serviços para parar o daemon do log do IBM Firewall e reinicie-o depois de ter substituído a DLL.

---

## Capítulo 5. Fornecimento de Métodos Próprios de Autenticação

Este capítulo apresenta informações sobre como o usuário pode fornecer seus próprios métodos de autenticação.

---

### Autenticação Fornecida pelo Usuário

Fornecemos uma amostra de autenticação do usuário que encontra-se no diretório `ROOT_DIR\bin\authsdk`. Os arquivos incluídos são:

- `authschm.h` - arquivos de definição de interface
- `authus.cpp` - arquivo fonte para esquema amostra
- `gwauth4.lib` - biblioteca do Firewall
- `msvc++.mak` - arquivo de amostra do Microsoft Visual C
- `schmname.h` - arquivos de definição de interface
- `vac++.mak` - arquivo de amostra do IBM Visual Age

Utilize os seguintes comandos para compilar a amostra de autenticação do usuário para o Visual Age da IBM:

- `nmake -f vac++.mak` - gera a DLL
- `nmake -f vac++.mak install` - gera e instala a DLL
- `nmake -f vac++.mak clean` - limpa o diretório local

Utilize os seguintes comandos para compilar a amostra de autenticação do usuário para o Visual C da Microsoft:

- `nmake -f msvc++.mak` - gera a DLL
- `nmake -f msvc++.mak install` - gera e instala a DLL
- `nmake -f msvc++.mak clean` - limpa o diretório local

---

### Utilização do Software Development Kit para Criar um Esquema de Autenticação Fornecido pelo Usuário

O IBM Firewall fornece uma interface de conexão para permitir a integração de produtos de segurança de autenticação de terceiros. Ele faz isto criando um `.dll` de esquema de autenticação que conecta-se à interface do esquema de autenticação do Firewall.

### Visão Geral do Processo de Autenticação do Firewall

Os seguintes serviços do firewall devem autenticar usuários antes de permitir que eles acessem os serviços do firewall:

- Servidor de Configuração do IBM Firewall
- Daemon FTP Proxy do IBM Firewall
- Daemon HTTP Proxy do IBM Firewall

- Daemon Telnet do IBM Firewall
- Servidor Socks do IBM Firewall

O Firewall fornece os seguintes esquemas de autenticação:

**Negar Tudo** O acesso ao serviço é sempre negado ao usuário.

**Permitir Tudo** Ao usuário é permitido o acesso sem exigências.

**Senha Firewall** Exige-se uma senha do usuário que está definida no banco de dados do Usuário do Firewall.

**Senha Logon NT** É exigida do usuário uma Senha de Logon do Windows NT.

**SecureNetKey** O usuário é autenticado com a Chave AssureNet Pathways SecureNet.

**Cartão SecurID** O usuário é autenticado com o cartão de segurança Security Dynamics SecurID.

O esquema de autenticação utilizado pode ser definido por usuário ou por serviço. Por exemplo, o Firewall pode ser configurado de modo que quando o usuário *John*, tenta iniciar sessão no servidor de configuração do IBM Firewall sua Senha de Logon do Windows NT é exigida. Mas quando o *John* deseja utilizar o Proxy Telnet do IBM Firewall, ele é autenticado utilizando seu Cartão SecurID. Entretanto, quando a usuária, *Mary*, tenta iniciar sessão no Servidor de Configuração do IBM Firewall, sua Senha do Firewall é exigida. Consulte o capítulo de administração do *Guia do Usuário IBM eNetwork Firewall* para obter mais informações sobre os esquemas de autenticação fornecidos pelo Firewall e como defini-los para cada usuário.

Além dos esquemas de autenticação fornecidos pelo IBM Firewall, você pode instalar até três esquemas de autenticação fornecidos pelo usuário. Você pode gravar estes esquemas para que interajam com sua infra-estrutura de segurança existente ou pode obtê-los de outros fornecedores de segurança para integrá-los com o Firewall.

Cada esquema de autenticação no Firewall, incluindo os esquemas de autenticação fornecidos pelo usuário, é representado por uma DLL que implementa a API do esquema de autenticação. Esta API define como o esquema de autenticação se registra com o Firewall e como o Firewall transmite pedidos de autenticação para ele.

## Criação de um Esquema de Autenticação Fornecido pelo Usuário

A criação de um esquema de autenticação fornecido pelo usuário consiste em:

- Gravar o código fonte para implementar a API do esquema de autenticação.
- Compilar e ligar o código fonte a uma DLL
- Instalar a DLL no Firewall

Os arquivos de cabeçalho e arquivos de biblioteca fonte-C necessários para criar um esquema de autenticação fornecido pelo usuário, assim como um código amostra e arquivos de amostra para o Microsoft Visual C++ e IBM Visual Age for C++, podem ser encontrados no R00TDIR\bin\authsdk.

## Gravação do Código Fonte

Todos os esquemas de autenticação devem fazer duas coisas:

1. Registrarem-se com o Firewall
2. Implementar AuthSchmFn

**Registrar com o Firewall:** Antes de serem iniciados os serviços do Firewall, o Firewall tenta carregar cada DLL que ele encontra no subdiretório \bin\authschm. A medida que cada DLL é carregada, sua rotina de inicialização deve chamar uma função no Firewall denominada registerAuthSchm para se registrar com o Firewall.

O protótipo da função registerAuthSchm está definido no arquivo de cabeçalho authschm.h. Ele obtém um único parâmetro que é indicador para uma estrutura AuthSchmInfo, que também está definido no authschm.h. A estrutura AuthSchmInfo associa um nome de esquema de autenticação ao endereço do AuthSchmFn apropriado que o Firewall deve chamar para passar os pedidos de autenticação para o esquema de autenticação.

Os esquemas de autenticação fornecidos pelo usuário devem utilizar um dos seguintes três nomes:

1. user
2. userauth2
3. userauth3

Há nomes simbólicos definidos para estes nomes no arquivo de cabeçalho schmname.h. Os esquemas de autenticação fornecidos pelo usuário devem ser projetados para permitir que o usuário final especifique quais destes três nomes são utilizados, para que diversos esquemas de autenticação fornecidos pelo usuário possam ser instalados sem que tenha que se preocupar com dois esquemas diferentes solicitando o mesmo nome.

Depois que a rotina de inicialização da DLL tiver chamado com sucesso AuthSchm de registro e retornado ao chamador, a DLL deverá estar preparada para processar pedidos de autenticação. Por este motivo, talvez seja necessário efetuar qualquer inicialização específica para esquema também na rotina de inicialização da DLL.

**Implementar AuthSchmFn:** Cada DLL do esquema de autenticação deve implementar uma função chamada AuthSchmFn utilizando o protótipo definido no authschm.h. A função AuthSchmFn possui um parâmetro, um indicador para uma estrutura AuthReq. A estrutura AuthReq é uma estrutura C simples que contém todas as informações pertencentes ao pedido de autenticação atual. AuthReq está definida no authschm.h. A estrutura AuthReq contém o nome do usuário sendo autenticado, o componente/serviço do Firewall que está solicitando a autenticação e outras informações sobre o pedido. Para obter uma lista completa e uma explicação sobre as informações na estrutura AuthReq, veja os comentários sobre isto no authschmh.

Além do nome de usuário e componente do firewall, há três parâmetros na estrutura AuthReq que são particularmente importantes na implementação de um esquema de autenticação:

- gwaput** Este é o endereço da rotina de retorno de chamada fornecida pelo Firewall, que o esquema de autenticação pode usar sempre que for necessário enviar uma mensagem ao usuário. Por exemplo, se o esquema de autenticação precisasse emitir uma mensagem de indicação ao usuário, ele chamaria o ponto de entrada fornecido no parâmetro gwaput para fazê-lo. A função de retorno de chamada gwaput é transformada em protótipo pela AuthSchmPut typedef no authschm.h. Veja os comentários em AuthSchmPut typedef para obter uma lista completa dos parâmetros que a AuthSchmFn deve transmitir nesta chamada.
- gwaget** Este é o endereço de uma rotina de retorno de chamada fornecida pelo Firewall, o qual o esquema de autenticação pode utilizar sempre que precisar recuperar uma resposta do usuário final sendo autenticado. Por exemplo, se o esquema de autenticação precisasse obter uma senha do usuário, ele chamaria o ponto de entrada fornecido no parâmetro gwaget para fazê-lo. A função de retorno de chamada gwaget é transformada em protótipo pela AuthSchmGet typedef no authschm.h. Veja os comentários em AuthSchmGet typedef para obter uma lista completa de parâmetros que a AuthSchmFn deve transmitir nesta chamada. Um parâmetro que é particularmente importante é o parâmetro echo. A AuthSchmFn pode utilizar este parâmetro para indicar se a resposta do usuário deve ser devolvida ou não para ele.
- opaque\_data** O campo opaque\_data é utilizado pelo Firewall para co-relacionar chamadas à AuthSchmFn com chamadas às suas rotinas de retorno de chamada. Ao chamar as rotinas gwaget ou gwaput, a AuthSchmFn deve transmitir o mesmo valor de opaque\_data que foi transmitido a ela na estrutura AuthReq.

Observe que os esquemas de autenticação devem ter condições de interagir com todos os componentes do Firewall. Alguns dos componentes do Firewall podem suportar diversos diálogos de exigência/resposta com o usuário final. Estes componentes são chamados de componentes interativos do Firewall. Alguns componentes do Firewall, devido a natureza de seus protocolos, só podem suportar uma única exigência/resposta. Estes são chamados de componentes do Firewall não-interativos.

O esquema de autenticação fornecido pelo usuário deverá poder modificar seu comportamento com base no componente do Firewall que está efetuando sua chamada, conforme indicado pelo campo do componente da estrutura AuthReq. Os valores válidos para o campo do componente estão definidos no authschm.h. Os valores válidos atuais para o campo do componente são:

<i>Tabela 23. Valores Válidos para o Campo do Componente</i>		
<b>Símbolo do Componente do AuthSchm.h</b>	<b>Componente do Firewall</b>	<b>Interativo/Não-interativo</b>
AUTHSCHM_UNKNOWN	Componente do Firewall novo ou não-reconhecido	Suponha que é interativo
AUTHSCHM_REMADMIN	Servidor de Configuração	interativo
AUTHSCHM_FTP	Proxy FTP	não-interativo
AUTHSCHM_TELNET	Proxy Telnet	interativo
AUTHSCHM_HTTP	Proxy HTTP	interativo
AUTHSCHM_SOCKS_PWD	Servidor Socks utilizando autenticação de senha	não-interativo
AUTHSCHM_SOCKS_CRAM	Servidor Socks utilizando autenticação CRAM	interativo
AUTHSCHM_REMIPSEC	Servidor IPSEC do Cliente Remoto (Atualmente não disponível no Windows NT)	interativo

Quando a AuthSchmFn concluir seu processamento, ela deve retornar ao chamador com um dos códigos de retorno GWA definidos no authschm.h. Este código de retorno é utilizado para indicar se o usuário foi autenticado com sucesso e se houve ou não um erro durante o processamento:

<i>Tabela 24. Códigos de Retorno GWA</i>	
<b>Código de Retorno</b>	<b>Significado</b>
GWA_OK	Nenhum erro durante o processamento e o usuário foi autenticado com sucesso
GWA_DENY	Nenhum erro durante o processamento, mas houve falha na autenticação do usuário
GWA_IOFAILURE	Um erro ocorreu ao tentar enviar prompts ao usuário ou ao tentar obter uma resposta do usuário. Geralmente, ele é devolvido quando há erros nas rotinas de retorno de chamada.
GWA_BUFFERTOOSMALL	A função AuthSchmFn não pôde recuperar uma resposta do usuário porque ela não pôde alocar um buffer grande o suficiente para receber a resposta.
GWA_NOAUTHFN	Erro - Irrelevante para esquemas de autenticação
GWA_FNNOTREG	Erro - Irrelevante para esquemas de autenticação
GWA_RSVNAME	Erro- O pedido de autenticação continha um nome que está reservado e não pode ser usado para este esquema de autenticação
GWA_BADNETTYPE	Erro - Irrelevante para esquemas de autenticação
GWA_BADAPP	Erro - Irrelevante para esquemas de autenticação
GWA_BADADDR	Erro - Endereço fornecido no pedido de autenticação era inválido
GWA_MEMSHORTAGE	Erro - Pedido de autenticação não pôde ser processado porque não foi possível alocar memória
GWA_USERDBFAIL	Erro - Não foi possível consultar um banco de dados necessário
GWA_REGFAILED	Erro - Irrelevante para esquemas de autenticação
GWA_AUTHERROR	Erro - Condição de erro específica do esquema de autenticação
GWA_INTERNAL	Erro - Condição de erro diversa no esquema de autenticação

Quando a AuthSchmFn retorna ao Firewall, se o código de retorno for GWA\_OK, o usuário é considerado autenticado e a ele é concedido acesso ao serviço solicitado. GWA\_DENY não é tratado como uma condição de erro, mas ao usuário é negado o acesso ao serviço solicitado. Todos os outros códigos de retorno são condições de erro e ao usuário é negado acesso ao serviço solicitado.

**Compilar e Ligar ao Código Fonte:** Ao compilar e ligar o código fonte a uma DLL, você deve ligar a DLL ao gwauth4.dll utilizando o gwauth4.lib fornecido no diretório \bin\authsdk para decifrar os nomes de ponto de entrada definidos no authschm.h. Além disso, é importante que a AuthSchmFn não seja exportada da DLL. Arquivos de amostra para o IBM VisualAge for C++ e Microsoft Visual C++ são fornecidos no diretório \bin\authsdk.

**Instalação da DLL:** Depois que a DLL tiver sido gerada com sucesso, copie para o diretório R00TDIR\bin\authschm e reinicialize a máquina do Firewall. A reinicialização é necessária para que o Firewall tente carregar a DLL e registrar os esquemas de autenticação da DLL.

**Agregar Tudo:** Figura 1 na página 54 mostra como os esquemas de autenticação são carregados e como a função chave faz a chamada durante o processamento de pedido de autenticação.

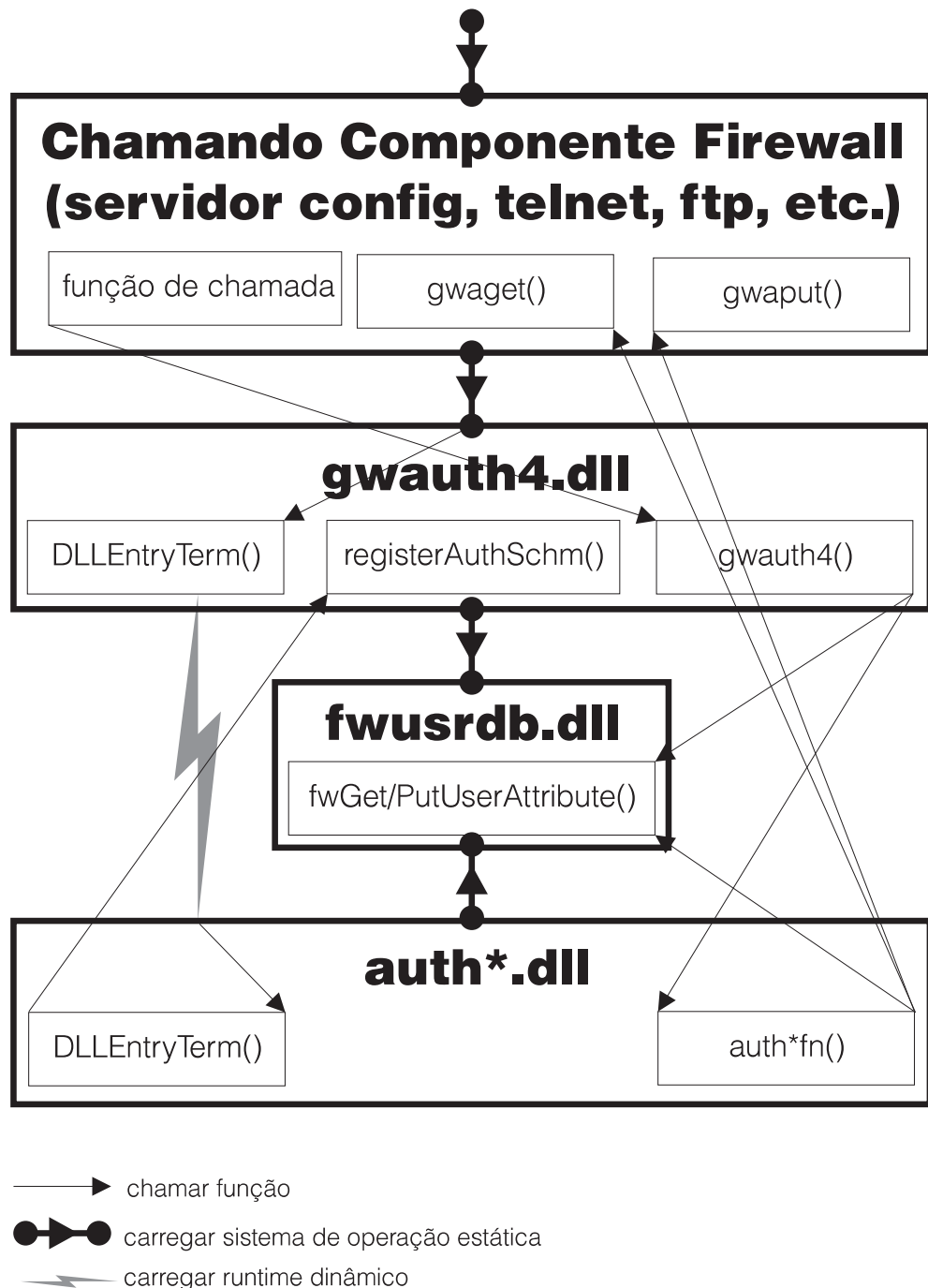


Figura 1. Inicialização e Registro DLL

Componentes do Firewall que precisam utilizar os serviços de autenticação conectam-se a uma DLL do Firewall denominada gwauth4. Quando a dll gwauth4 é carregada, sua rotina DLLEntryTerm é chamada e irá tentar efetuar um carregamento em execução de todas as DLLs no R00TDIR\bin\authschm. Se houver falha de carregamento de uma DLL do esquema de autenticação, ela não será considerada como um erro para o carregamento da dll gwauth4. A dll gwauth4 coloca em série estas tentativas de carregamento.

Quando a rotina DLLEntryTerm de esquemas de autenticação é executada, ela é responsável pelo registro dos esquemas de autenticação com gwauth4.dll. Isto é

feito através da invocação de `registerAuthSchm`. A `dll authschm` precisa chamar `registerAuthSchm` uma vez para cada esquema de autenticação que a DLL suporta. A estrutura `AuthSchmInfo` que é transmitida na função `registerAuthSchm` associa o nome do esquema de autenticação, conforme armazenado no banco de dados do usuário, ao ponto de entrada da função `AuthSchmFn`. A função de registro irá fazer cópias da estrutura transmitida para ela, para que a `dll authschm` possa reutilizar ou modificar esta estrutura conforme necessário. A DLL do esquema de Autenticação também é responsável pela liberação da estrutura `AuthSchmInfo`.

A função `registerAuthSchm` é responsável pela geração de uma lista conectada que representa todos os esquemas de autenticação registrados. A rotina `DLLEntryTerm` da `gwauth4` irá inicializar a lista âncora como `NULL`. Assim, quando as DLLs `authschm` chamam a função `registerAuthSchm` ele fará o seguinte:

1. Examinar a lista de esquemas de autenticação em busca de uma entrada que possui nome igual ao nome transmitido. Caso exista um, remova-o da lista e elimine qualquer memória associada a ele.
2. Crie uma estrutura `AuthSchmEntry` com base na estrutura `AuthSchmInfo` e acrescente-a na lista de esquemas de autenticação.
3. Devolva ao chamador uma indicação de que o registro obteve sucesso (`GWA_OK`) ou falhou (`GWA_REGFAILED`).

Depois que a `DLLEntryTerm` do `gwauth4` tiver feito um carregamento em tempo de execução em cada uma das `dlls authschm` e que as DLLs `authschm` tiverem registrado seus esquemas de autenticação, a rotina `DLLEntryTerm` do `gwauth4` irá retornar ao chamador. Neste ponto, outros componentes podem começar a solicitar serviços de autenticação chamando a função `gwauth4`.

Quando a `gwauth4.dll` é descarregada, a rotina `DLLEntryTerm` será chamada novamente para o término do processamento. Quando chamada para o término, esta rotina irá eliminar todos os itens `AuthSchmEntry` na `AuthSchmList` e suas memórias associadas. Isto é feito para que os esquemas de autenticação não tenham que cancelar os seus registros do Firewall.

**Processamento do Pedido de Autenticação:** Quando um serviço do Firewall precisa autenticar um usuário, ele chama funções na `gwauth4.dll`. O `gwauth4` pega informações deste componente de chamada e consulta o banco de dados do usuário Firewall para determinar o nome de qual esquema de autenticação irá utilizar para processar o pedido.

Depois que o `gwauth4` tiver determinado o nome do esquema de autenticação, ele examina sua lista de esquemas de autenticação registrados em busca de um esquema com o mesmo nome. Se ele encontrar um esquema registrado com o mesmo nome, ele cria uma estrutura `AuthReq` para representar o pedido atual e chama o ponto de entrada na DLL do esquema de autenticação associada ao nome.

A função `AuthSchmFn` chamada pelo `gwauth4` processa o pedido e chama os retornos de chamada `gwaget` e `gwput` conforme necessário para interagir com o usuário final. Ao concluir seu processamento, ela retorna o controle para `gwauth4` com um código de retorno apropriado.

O gwauth4 grava os registros de log apropriados para documentar o pedido de autenticação e depois retorna ao componente do firewall que originou o pedido, propagando o código de retorno que é recebido da DLL do esquema de Autenticação.

---

## Capítulo 6. Utilização do Utilitário Make Key File (MKKF)

Uma conexão de rede SSL protegida exige que:

- O servidor de configuração esteja configurado para SSL
- Ter sido criada uma chave para comunicação protegida
- Você tenha sido designado como root de confiança no servidor
- A senha do arquivo de senha esteja escondida

Utilize o MKKF para criar a chave de servidor inicial, o arquivo de anel de chave e o pedido de certificado. O MKKF também é usado para receber o certificado inicial num anel de chave e esconder a senha do arquivo de chave.

---

### Criação de arquivo de chaves

Você deve iniciar sessão utilizando uma conta de administrador Windows NT ao executar este utilitário.

1. Passe para o diretório ROOTDIR\config e inicie o utilitário de chaves digitando:

```
c:\program files\IBM\Firewall\config > mkkf
```

```
MKKF Key Manager  
Copyright IBM Corp. 1996  
Todos os Direitos Reservados
```

2. Criar um novo arquivo de chaves.

```
Menu do Anel de Chave  
Anel de Chave Selecionado no Momento: (nenhum)
```

```
N - Criar Novo Arquivo de Chaves  
O - Abrir Arquivo de Chaves  
X - Sair
```

Digite um comando: **n**

Digite 'n' como foi mostrado acima para criar um novo arquivo de chaves.

O sistema pedirá um nome para o arquivo de chaves. Pode ser usado qualquer nome, mas que termine com .kyr. Por padrão, o firewall procura um arquivo de nome fwkey.kyr.

Dê o nome do arquivo de anel de chave ou pressione ENTER para aceitar o padrão **fwkey.kyr**

O MKKF vai criar um novo arquivo de chaves e exibir o menu do anel de chave. Note que o arquivo de chaves vai ser listado como o anel de chave selecionado no momento.

3. Crie uma nova chave e um pedido de certificado.

Menu do Anel de Chave  
Anel de Chave Selecionado no Momento: (fwkey.kyr)

N - Criar Novo Arquivo de Chaves  
O - Abrir Arquivo de Chaves  
S - Salvar Arquivo de Anel de Chave  
A - Salvar Anel de Chave como Outro Arquivo  
P - Definir Senha para Arquivo de Anel de Chave  
C - Criar Arquivo Escondido para Arquivo de Anel de Senha  
R - Receber Certificado no Arquivo em Anel de Chave  
W - Trabalhar com Chaves e Certificados  
  
X - Sair

Digite um comando: **w**

Digite 'w', como foi mostrado acima, para ir para o menu Chave.

Menu Chave  
Anel de Chave Selecionado no Momento: (fwkey.kyr)  
Entrada de Chave Selecionada: (nenhuma)

L - Listar/Selecionar uma chave para trabalhar  
C - Criar Nova Chave e Pedido de Certificado  
I - Importar chave de arquivo de chaves blindado  
X - Sair deste menu

Digite um comando: **c**

Digite 'c' como foi mostrado acima para criar uma nova chave.

Antes de armazenar a chave no arquivo de chaves, este precisa ser protegido por senha. O MKKF vai solicitar essa senha. Ela não aparece quando é digitada. O MKKF também vai perguntar se a senha deve ter validade. Digite 'n' como mostrado abaixo:

Digite a senha para o arquivo de chaves:

senha

Digite a senha de novo para verificação:

senha

A senha deve ter validade?

Digite Y para sim ou N para não:

**n**

Senha definida.

Tecle ENTER para continuar

O MKKF vai solicitar o tipo de chave a ser criada.

Escolha Menu Tipo de Certificado S - PEM Formato de  
Solicitação de Certificado (Mensagem Privada Aprimorada)  
P - Formato de Solicitação de Certificado PKCS10  
C - Cancelar

Digite um comando: **s**

Digite 's', como acima mostrado, para criar um Formato de Solicitação de Certificado PEM. O MKKF vai gerar um certificado vazio:

## Menu Compor Certificado de Servidor Protegido

### Informações Atuais do Certificado

Nome da Chave: (nenhuma)  
Tamanho da Chave: 0  
Nome do Servidor: (nenhum)  
Organização: (nenhuma)  
Unidade da Organização: (nenhuma)  
Cidade/Localidade: (nenhuma)  
Estado/Província: (nenhum)  
Código Postal: (nenhum)  
País: (nenhum)

M - Modificar os Campos do Certificado

R - Pronto para Criar Chave e Pedido de Certificado

C - Cancelar

Digite um comando: **m**

Digite 'm' para modificar o certificado vazio. O sistema pedirá informações sobre o novo certificado:

- Digite um nome. Pode ser qualquer cadeia, que só será usada pelo utilitário MKKF:

Digite um nome para ser usado na entrada da chave:

### **Chave do Firewall**

- Digite o tamanho da chave. O IBM Firewall só envia a versão exportável do MKKF. O tamanho máximo de chave é 1024.

1: 508  
2: 512  
3: 768  
4: 896  
5: 1024

Digite o número correspondente ao tamanho de chave desejado:

**2**

- Digite o nome de host TCP/IP completamente qualificado para o firewall (Por exemplo, jupiter.raleigh.ibm.com):

Digite o nome de  
domínio totalmente qualificado do  
TCP/IP ou pressione  
Enter para deixar o campo em branco

**jupiter.raleigh.ibm.com**

- Digite o nome de uma empresa para associar ao certificado. (Exemplo: o nome da empresa):

Digite o Nome da Empresa para o certificado  
ou pressione  
ENTER para deixar o campo em branco.

**AAA Inc.**

- Digite o nome da unidade organizacional. (Exemplo: o nome de um departamento):

Digite o Nome da Unidade Organizacional para o certificado  
ou pressione  
ENTER para deixar o campo em branco.

#### **Produtos de Segurança da Rede**

- Digite a cidade em que o certificado vai ser usado:

Digite a  
Localidade/Nome da Cidade para o certificado  
ou pressione  
ENTER para deixar o campo em branco.

**RTP**

- Digite um estado ou província.

**Nota:** Devido às especificações dos certificados, este campo precisa ter no mínimo três caracteres, de modo que abreviações de estado de duas letras não são válidas.

Digite o Nome do  
Estado/Província para o certificado  
ou pressione  
ENTER para deixar o campo em branco.  
O Estado/Província precisa ter no mínimo três caracteres.

**N.C.**

- Digite o código postal a ser associado ao certificado. (É a mesma coisa que CEP):

Digite o Código Postal do certificado  
ou pressione  
ENTER para deixar o campo em branco.

**27709**

- Forneça um código de país com duas letras:  
 Digite o Código de  
 País do certificado  
 ou pressione  
 ENTER para deixar o campo em branco.  
 Ele precisa ter exatamente dois caracteres.

US

Depois de o MKKF ter coletado todas as informações, o certificado será mostrado:

Menu Compor Certificado de Servidor Protegido

Informações Atuais do Certificado

Nome da Chave: Chave do Firewall

Tamanho da chave: 512

Nome do Servidor: jupiter.raleigh.ibm.com

Empresa: AAA Inc.

Unidade Organizacional: Produtos de Segurança de Rede

Cidade/Localidade: RTP

Estado/Província N.C.

Código Postal: 27709

País: US

M - Modificar os Campos do Certificado

R - Pronto para Criar Chave e Pedido de Certificado

C - Cancelar

Digite um comando: **r**

Se houver erros nas informações, digite 'm' para fazer as correções. Se as informações estiverem certas, digite 'r' para criar uma nova chave e o arquivo de chaves associado a ela.

O MKKF vai pedir um arquivo para armazenar o certificado. Pode ser usado qualquer nome de arquivo, mas uma boa convenção a seguir é usar o mesmo nome de base do arquivo de chaves e acrescentar .cert como extensão:

Informe o arquivo que vai armazenar o pedido de certificado em:

**fwkey.cert**

Criando Chave Privada...

A chave privada foi criada.

Criando um pedido de certificado...

O pedido de certificado foi criado

Acrescentado uma nova chave no arquivo de chaves.

A nova chave e o pedido de certificado foram criados.

Tecla ENTER para continuar

#### 4. Faça da chave recém-criada o padrão.

Depois de terem sido criados a chave e o certificado, o menu chave será mostrado. A chave recém-criada vai ser listada como Entrada de Chave Seleccionada:

Menu Chave

Anel de Chave Selecionado no Momento: (fwkey.kyr)

Entrada de Chave Selecionada: Chave do Firewall

L - Listar/Selecionar uma Chave para Trabalhar  
S - Exibir Informações sobre a Chave Selecionada  
D - Eliminar Chave Selecionada  
C - Criar Nova Chave e Pedido de Certificado  
I - Importar Chave de Arquivo de Chaves Blindado  
E - Exportar Chave Selecionada Para Arquivo de Chaves Blindado  
F - Fazer da Chave Selecionada a Chave Padrão para esse Anel de Chave  
U - Desmarcar Status de Root de Confiança da Chave Selecionada  
R - Criar Pedido de Certificado para Chave Selecionada  
X - Sair Deste Menu

Digite um comando: **f**

Faça da chave recém-criada a chave padrão do arquivo de chaves. Digite 'f' como foi mostrado no exemplo anterior. Um prompt pedirá que a ação seja confirmada:

Menu Chave

Chave selecionada no momento: Chave do Firewall

Esta chave deve passar a ser o padrão?

Digite Y para sim ou N para não:

**y**

A chave se tornou o padrão.

Tecle ENTER para continuar

Depois de marcada a chave como padrão, o Menu Chave é mostrado:

Menu Chave

Anel de Chave Selecionado no Momento: (fwkey.kyr)

Entrada de Chave Selecionada: Chave do Firewall

L - Listar/Selecionar uma Chave para Trabalhar  
S - Exibir Informações sobre a Chave Selecionada  
D - Eliminar Chave Selecionada  
C - Criar Nova Chave e Pedido de Certificado  
I - Importar Chave de Arquivo de Chaves Blindado  
E - Exportar Chave Selecionada Para Arquivo de Chaves Blindado  
F - Fazer da Chave Selecionada a Chave Padrão para esse Anel de Chave  
U - Desmarcar Status de Root de Confiança da Chave Selecionada  
R - Criar Pedido de Certificado para Chave Selecionada  
X - Sair Deste Menu

Digite um comando: **x**

Saia do menu Chave digitando 'x'.

##### 5. Receber o certificado no arquivo de anel de chave.

O menu Anel de Chave vai ser mostrado:

Menu do Anel de Chave  
Anel de Chave Selecionado no Momento: (fwkey.kyr)

N - Criar Novo Arquivo de Chaves  
O - Abrir Arquivo de Chaves  
S - Salvar Arquivo de Anel de Chave  
A - Salvar Anel de Chave como Outro Arquivo  
P - Definir Senha para Arquivo de Anel de Chave  
C - Criar Arquivo Escondido para Arquivo de Anel de Senha  
R - Receber Certificado no Arquivo em Anel de Chave  
W - Trabalhar com Chaves e Certificados

X - Sair

Digite um comando: **r**

**Nota:** Como o firewall não usa SSL para fins de autenticação, o certificado não precisa ser assinado por autoridade de certificado.

Digite o nome do arquivo ou pressione ENTER  
para Cert.txt.

**fwkey.cert**

Trata-se de um certificado auto-assinado. Deseja acrescentá-lo ao arquivo de chaves?

Digite Y para sim ou N para não:

**y**

Certificado acrescentado ao anel de chave.

Tecla ENTER para continuar

#### 6. Crie um arquivo escondido para o arquivo de chaves.

Depois do certificado ser acrescentado ao anel de chave, o Menu Anel de Chave é mostrado:

Menu do Anel de Chave  
Anel de Chave Selecionado no Momento: (fwkey.kyr)

N - Criar Novo Arquivo de Chaves  
O - Abrir Arquivo de Chaves  
S - Salvar Arquivo de Anel de Chave  
A - Salvar Anel de Chave como Outro Arquivo  
P - Definir Senha para Arquivo de Anel de Chave  
C - Criar Arquivo Escondido para Arquivo de Anel de Senha  
R - Receber Certificado no Arquivo em Anel de Chave  
W - Trabalhar com Chaves e Certificados

X - Sair

Digite um comando: **c**

É preciso criar um arquivo escondido para o arquivo de chaves. Digite 'c' como foi mostrado no exemplo anterior. O MKKF vai usar o mesmo nome de base do arquivo de chaves, com extensão .sth:

Arquivo de senhas escondido salvo como fwkey.sth  
Tecla ENTER para continuar

Depois de criado o arquivo escondido, o Menu do Anel de Chave é mostrado:

Menu do Anel de Chave

Anel de Chave Selecionado no Momento: (fwkey.kyr)

N - Criar Novo Arquivo de Chaves  
O - Abrir Arquivo de Chaves  
S - Salvar Arquivo de Anel de Chave  
A - Salvar Anel de Chave como Outro Arquivo  
P - Definir Senha para Arquivo de Anel de Chave  
C - Criar Arquivo Escondido para Arquivo de Anel de Senha  
R - Receber Certificado no Arquivo em Anel de Chave  
W - Trabalhar com Chaves e Certificados

X - Sair

Digite um comando: **x**

Seu arquivo de chaves está agora pronto para ser usado. Digite 'x' como foi mostrado acima para sair do MKKF e digite 'y' para salvar as alterações feitas ao arquivo de chaves:

O arquivo de anel de chave foi alterado. Deseja salvá-lo?

Digite Y para sim ou N para não:

**y**

Anel de chave salvo como fwkey.kyr

Tecle ENTER para continuar

#

#### 7. Atualizando o arquivo de configuração.

Depois de criar o arquivo de chaves, é preciso especificar o nome dele no arquivo de parâmetros do servidor de configuração utilizando o comando `fwcfgsrv`.

Se estiver utilizando criptografia SSL para o servidor de configuração, também será preciso definir a opção `encryption=ssl` utilizando o comando `fwcfgsrv`.

Depois de utilizar o comando `fwcfgsrv`, pare e reinicie o serviço do servidor.

---

## Capítulo 7. Identificação de Problemas e Testes

Este capítulo mostra como identificar alguns problemas comumente encontrados quando se configura e ajusta um IBM Firewall.

Se estiverem surgindo problemas, crie primeiro um log do firewall, com prioridade para a depuração, a fim de aumentar a quantidade de informações enviadas aos registros. Para saber mais a esse respeito, leia “Gerenciamento de Arquivo de Log” na página 5.

---

### Instalação e Configuração

#### O suporte do filtro não funciona

**Explicação do Problema** Você recebe estas mensagens de erro.

Falha na verificação de suporte do filtro.

Falha na chamada da criação do soquete.

Há um arquivo ou diretório no nome de caminho que não existe.

Esse problema ocorre quando não se faz a reinicialização do firewall após a instalação.

**Ação Recomendada** Reinicialize o firewall e tente fazer o procedimento de novo.

---

### Problemas de Roteamento

O IBM Firewall possui um recurso no quadro de diálogo **Normas de Segurança** intitulado *Testar Roteamento IP*, que pode ser de grande utilidade na depuração de problemas de roteamento. Ative essa opção, a Configuração da conexão e o Registro das Regras de Conexão. Depois examine o log do firewall para ver informações detalhadas sobre o fluxo de todos os pacotes pelo firewall.

Faça os testes usando primeiro endereços de IP e depois nomes de host. Se o tráfego correr adequadamente com endereços mas não com nomes, procure mais informações em “Problemas de DNS” na página 66.

#### Impossível fazer o ping de hosts a partir do firewall

**Explicação do Problema** A interface da rede não está devidamente configurada.

**Ação Recomendada** Veja a documentação do sistema operacional.

**Explicação do Problema** A conexão com a rede não-protetida não está devidamente configurada.

**Ação Recomendada** Entre em contato com o Provedor de Serviços de Internet para pedir assistência.

**Explicação do Problema** Se a rede protegida estiver isolada atrás de um roteador, o firewall precisará ter uma rota estática para esse roteador. Use o `netstat -rn` para verificar o roteamento estático:

`netstat -rn`

A saída deve ser esta para a Família de Protocolo 2:

Gateway	de Destino	Sinalizadores	....
default	nrr.nrr.nrr.nrr	UG	
nnn.nnn.nnn	nnn.nnn.nnn.nnn	U	
sss.sss.sss	sss.sss.sss.sss	U	
ss1.ss1.ss1	srr.srr.srr.srr	UG	
127	127.0.0.1	U	

Figura 2. Saída de exemplo de netstat -rn.

**nrr.nrr.nrr.nrr** representa o roteador para a internet e é a rota padrão.

A rota padrão é uma rota estática (Flag=UG).

**nnn.nnn.nnn** representa seu domínio não-protetido. Trata-se de uma rota de interface (Flag=U).

**nnn.nnn.nnn.nnn** representa sua interface não-protetida.

**sss.sss.sss** representa seu domínio protegido. Trata-se de uma rota de interface (Flag=U).

**sss.sss.sss.sss** representa sua interface protegida.

**ss1.ss1.ss1** representa um subdomínio do lado protegido da rede e

srr.srr.srr.srr representa o roteador para esse subdomínio. Trata-se de uma rota estática (Flag=UG).

**127.0.0.1** é o ponto de retorno ou host local. Trata-se de uma rota de interface (Flag=U).

Você deve ter uma rota de interface para cada interface e a rota padrão deve apontar para o roteador no lado não-protetido do firewall.

**Ação Recomendada** Inclua uma rota estática no roteador. Entre em contato com o administrador do roteador. Utilize o comando route add.

**Explicação do Problema** A máscara de sub-rede da interface protegida ou do host com o qual se está tentando fazer contato pode estar incorreta.

**Ação Recomendada** Utilize os utilitários de configuração do cliente para corrigir as definições da máscara.

## Não é possível fazer o ping de hosts não-protetidos a partir de hosts protegidos (ou vice-versa)

**Explicação do Problema** Cada roteador adjacente ao firewall deve conter uma rota estática especificando o firewall como o gateway para redes de destino além do firewall.

**Ação Recomendada** Entre em contato com o administrador.

**Explicação do Problema** Se sua rede protegida usar endereços que não estejam registrados e que não sejam roteáveis na rede não-protetida - entre os quais endereços privados como os especificados no RFC 1597 - os pacotes não vão ser roteados de volta para o emissor.

**Ação Recomendada** Use cliente com endereço registrado.

## Problemas de DNS

O DNS do firewall DNS resolve nomes consultando o servidor de nomes protegidos. O servidor de nomes protegidos resolve todos os nomes da rede protegida. Ele encaminha pedidos de nomes não-protetidos para o servidor de nomes do firewall. Este consulta o servidor de nomes não-protetidos para resolver o pedido.

Problemas DNS podem afetar outras áreas da operação do firewall. Seria bom verificar o DNS mesmo que o problema não esteja evidentemente relacionado ao DNS.

Eis alguns exemplos que mostram o método passo-a-passo, usando o utilitário `nslookup` para isolar o problema. Nestes exemplos, vamos usar os seguintes valores:

**www.ibm.com** representa um nome de host arbitrário na rede não-protegida

**nns.nns.nns.nns** representa o endereço de um servidor de nomes não-protegidos

**sns.sns.sns.sns** representa o endereço do servidor de nomes protegidos

**host.secure.company.com** representa o nome de um host arbitrário dentro da rede protegida

**127.0.0.1** representa o endereço de ponto de retorno no firewall.

Estes valores podem ser obtidos no quadro de diálogo **Serviços de Nome de Domínio** no Cliente de Configuração. Eles serão necessários para se trabalhar com os exercícios.

**Nota:** O comando `nslookup` requer o ponto adicional depois do nome de host para impedir que o `nslookup` anexe o nome do domínio protegido.

## O DNS ainda não foi configurado

**Explicação do Problema** Você não configurou os recursos DNS do firewall.

**Ação Recomendada** Complete o quadro de diálogo **Serviços de Nome de Domínio**.

## Falha de Consultas DNS ou Tempo Expirado

**Explicação do Problema** O controle de tráfego do Firewall não está permitindo o fluxo dos pacotes de DNS.

**Ação Recomendada** Vá para o quadro de diálogo **Normas de Segurança**, ative o quadro de opção *Permitir consultas DNS* e reative o controle de tráfego.

## Falha do nslookup **www.ibm.com. nns.nns.nns.nns**

**Explicação do Problema** O servidor de nome não-protegido não está usando o endereço indicado ou não está devidamente configurado.

**Ação Recomendada** Entre em contato com o provedor de serviços do DNS para saber um endereço de servidor de nome válido.

## Falha do nslookup **www.ibm.com. 127.0.0.1**

**Explicação do Problema** O serviço DNS da Microsoft talvez não esteja operando. Vá até o gerenciador de controle de serviço para determinar se ele está operando.

**Ação Recomendada** Utilize o gerenciador de controle de serviço para iniciar o DNS.

## **nslookup host.secure.company.com. sns.sns.sns.sns falhou**

**Explicação do Problema** O servidor de nome protegido caiu.

**Ação Recomendada** Reinicie o servidor de nomes.

## **nslookup www.ibm.com. sns.sns.sns.sns falhou**

**Explicação do Problema** O servidor de nomes protegidos não está devidamente configurado para interagir com o IBM Firewall.

**Ação Recomendada** Consulte o *Guia do Usuário IBM eNetwork Firewall* para requisitos de configuração.

---

## **Cliente de Configuração**

### **O servidor não responde**

**Explicação do Problema** O cliente de configuração e o servidor de configuração estão utilizando linguagens diferentes.

**Ação Recomendada** No painel no log do cliente de configuração, selecione a linguagem na qual o firewall foi instalado.

**Explicação do Problema** Pode ser que a criptografia do SSL não esteja devidamente configurada.

**Ação Recomendada** Veja se o SSL está selecionado no painel de logon do cliente. Pare e reinicie o servidor de configuração do firewall utilizando o gerenciador de controle de serviço.

**Explicação do Problema** O servidor de configuração do firewall pode estar desativado.

**Ação Recomendada** Certifique-se de que o servidor de configuração do firewall está operando.

**Explicação do Problema** O servidor de configuração do firewall pode estar monitorando uma porta não-padrão.

**Ação Recomendada** Examine o c:\winnt\system32\drivers\etc\services e certifique-se de que ele contém a linha ibmfwrcc 1014/tcp. Para usar o servidor em outra porta, edite a linha ibmfwrcc 1014/tcp correspondentemente e não deixe de especificar a nova porta no painel de logon do cliente. Pare e reinicie o servidor de configuração utilizando o gerenciador de controle de serviço.

**Explicação do Problema** O controle de tráfego do firewall pode não estar permitindo comunicações para e do Servidor de Configuração. Isso só afeta os Clientes de Configuração executados em host remoto.

**Ação Recomendada** Codifique uma conexão entre a máquina que executa o Cliente de Configuração e o firewall. O Cliente de Configuração deve ser a fonte da conexão e o firewall o destino. Gere de novo e ative as alterações. Consulte o *Guia do Usuário IBM eNetwork Firewall* para obter maiores informações.

**Explicação do Problema** O Servidor de Configuração pode não estar configurado de modo a permitir logins de host remoto.

**Ação Recomendada** Utilize o comando `fwcfgsrv` para verificar se o parâmetro `localonly` está definido como `no`.

## Não é possível efetuar o logon no Servidor de Configuração

**Explicação do Problema** Cada nome de usuário autenticado no firewall é configurado para usar qualquer um dos vários métodos de autenticação. Negar tudo é usado para proibir o uso de um determinado serviço para aquele usuário.

**Ação Recomendada** Examine nos campos Administração Protegida e Administração Não-Protegida os nomes de usuário que estão sendo usados. Estes campos são válidos apenas para Administradores, não para usuários do firewall.

---

## Controle de Tráfego

### As mudanças feitas nas Conexões não passam a ter efeito

**Explicação do Problema** As mudanças feitas a qualquer componente do Controle de Tráfego não passam a ter efeito até que sejam ativadas. Isto inclui o quadro de diálogo **Normas de Segurança** sob Administração do Sistema.

**Ação Recomendada** Utilize o quadro de diálogo **Ativação da Conexão** para gerar novamente e ativar sua configuração.

---

## Servidores Proxy

### Os dados não são transmitidos

**Explicação do Problema** Os serviços de proxy do firewall não são iniciados até que a máquina seja reiniciada após a instalação.

**Ação Recomendada** Reinicialize a máquina.

**Explicação do Problema** O Controle de Tráfego do firewall deve ser configurado para permitir que pacotes fluam para e do processo proxy, e não diretamente através do firewall.

**Ação Recomendada** Configure cada metade da conexão proxy da maneira descrita no *Guia do Usuário IBM eNetwork Firewall*.

Use os serviços pré-definidos sempre que possível, especialmente com tráfego FTP.

### Não é possível conectar-se ao host desejado

**Explicação do Problema** Se os dados fluem de e para o proxy mas o host não é contactado, pode ser que o cliente não esteja resolvendo adequadamente os nomes de host.

**Ação Recomendada** Veja se *Permitir consultas DNS* está ativado no quadro de diálogo **Normas de Segurança** e se sua configuração da conexão foi ativada. Para ter mais informações, leia o "Problemas de DNS" na página 66.

**Explicação do Problema** Cada nome de usuário sendo autenticado no firewall por qualquer um dos serviços do firewall pode ser configurado para utilizar um dos diversos métodos de autenticação. Negar tudo é utilizado para proibir o uso de um determinado proxy para aquele usuário.

**Ação Recomendada** Examine as definições da autenticação da conta do usuário no quadro de diálogo **Usuários** no Cliente de Configuração.

---

## Serviços de Autenticação

### Uma conta de administrador Windows NT não pode ser autenticada

**Explicação do Problema** Os atributos do firewall para uma conta de administrador Windows NT são armazenados no banco de dados do usuário firewall sob fwdadm.

**Ação Recomendada** Verifique se fwdadm possui o método de autenticação correto definido para o serviço que você está tentando usar.

### O usuário proxy do Firewall não pode ser autenticado

**Explicação do Problema** Se o usuário proxy do firewall não estiver definido no banco de dados de usuário do firewall, o nome fwdfuser é utilizado para definir os atributos do usuário.

**Ação Recomendada** Verifique se o método de autenticação fwdfuser's está definido corretamente para o serviço que o usuário está tentando acessar.

---

## Dispositivos do Log

### Alterações do dispositivo de log não tem efeito no servidor

**Explicação do Problema** Ao eliminar ou alterar um dispositivo do log, ela parece funcionar na GUI, mas não no servidor.

**Ação Recomendada** Reinicialize o sistema.

---

## Utilitários de Relatório

### Ocorreu um erro durante o acesso ao arquivo:

**Explicação do Problema** O erro acima pode ser visto depois de se usar algum destes comandos:

```
db2 -vf fwschema.dll > schema.out
db2 -vf fwimport.dat > import.out
db2 -vf fwqrysmpl.dll > sample.out
```

**Ação Recomendada** Forneça os nomes de arquivo completamente qualificados para o arquivo

## Ocorrem erros durante a importação de dados para o banco de dados.

**Explicação do Problema** O arquivo import.out resultante de um comando `db2 -vf fwimport.dat>import.out` possui mensagens que indicam que uma das importações falhou ou foi apenas parcialmente bem sucedida.

**Ação Recomendada** Verifique o arquivo .msg correspondente à instrução de importação na qual o problema foi mencionado. Ele fornecerá mais detalhes sobre o problema. Procure o(s) registro(s) relacionado(s) no arquivo .tbl correspondente para ver os dados de entrada e determinar o que há de errado com ele. Por exemplo, é muito extenso para sua coluna de destino no banco de dados? Os tipos de dados são apropriados para o tipo da coluna de destino? Se os dados de entrada não parecerem corretos, talvez seja necessário localizar o registro do arquivo de log original para certificar-se de que o `fwlogtbl` gerou o registro de arquivo .tbl corretamente.

Caso não consiga resolver o problema, salve o arquivo import.out, o arquivo .msg, o arquivo .tbl associado e o arquivo de log original antes de entrar em contato com o Serviço IBM.



---

## Apêndice A. Mensagens

Este apêndice contém mensagens para o IBM Firewall for AIX, para o IBM Firewall for NT e mensagens comuns aos dois. Ele também fornece as seguintes informações sobre as mensagens do IBM Firewall :

- Como as mensagens são formatadas
- Os níveis de gravidade das mensagens
- As mensagens e suas explicações

Caso tenha lido a mensagem e sua explicação, mas precisa de mais informações, consulte o Capítulo 7, “Identificação de Problemas e Testes” na página 65.

---

### Tag da Mensagem

<b>ICA</b>	Os 3 primeiros bytes fixos.
<b>xxxx</b>	Entre o número 0000 – 9999.
<b>a</b>	Indicador de severidade. As mensagens são classificadas por nível de severidade. <ul style="list-style-type: none"> <li>• i – informativo</li> <li>• w – atenção</li> <li>• e – erro</li> <li>• s – severo</li> </ul>

Os números entre 0000 – 9999 são depois classificados de acordo com as seguintes categorias:

- 0000 – 0999 Alarme de Intrusão
- 1000 – 1999 Filtros
- 2000 – 2999 Proxy
- 3000 – 3999 Socks
- 4000 – 4999 Pager
- 5000 – 8999 Disponível
- 9000 – 9999 Geral/Outros

---

### Mensagens

---

**ICA0001    ALERTA - *número* falhas de autenticação.**

**Explicação:** As condições-limite das falhas de autenticação foram satisfeitas.

---

**ICA0002    ALERTA - *número* falhas de autenticação relativas ao nome do usuário do usuário.**

**Explicação:** As condições-limite para a detecção de uma mensagem de log específica foram satisfeitas.

---

**ICA0003    ALERTA - *número falhas de autenticação a partir do endereço de IP do host.***

**Explicação:** As condições-limite das falhas de autenticação dadas a partir de qualquer host específico foram satisfeitas.

---

**ICA0004    ALERTA - Tag *id da mensagem com número entradas de log.***

**Explicação:** As condições-limite para a detecção de uma mensagem de log específica foram satisfeitas.

---

**ICA0005    Monitor de logs - sem memória.**

**Explicação:** O processo ficou sem memória.

---

**ICA0006    Monitor de logs - falha no acesso do arquivo de serviços: *número do erro***

**Explicação:** Não foi encontrada entrada para fwlogmond no /etc/services.

---

**ICA0007    Monitor de logs - a criação do soquete falhou: *número do erro***

**Explicação:** O soquete não pôde ser aberto - veja a mensagem do erro.

---

**ICA0008    Monitor de Logs - o bind() falhou: *número do erro***

**Explicação:** O soquete não pôde ser ligado - veja a mensagem do erro.

---

**ICA0009    O arquivo de definição dos limites não pôde ser aberto: *número do erro***

**Explicação:** Problema no acesso ao arquivo de definição de limites - veja a mensagem do erro.

---

**ICA0010    Monitor de Logs - erro fatal de leitura: *número do erro***

**Explicação:** Problema na leitura a partir do soquete - veja a mensagem do erro.

---

**ICA0011    O status do arquivo de definição de limites não foi obtido: *número do erro***

**Explicação:** Problema no acesso ao arquivo de definição de limites - veja a mensagem do erro.

---

**ICA0012    O daemon do monitor de logs está sendo encerrado.**

**Explicação:** O daemon está sofrendo término anormal ou recebeu sinal de encerramento. As mensagens de log dadas antes devem dar detalhes.

---

**ICA0013    O monitor de logs captou sinal de encerramento.**

**Explicação:** O daemon recebeu sinal de encerramento e vai ser fechado.

---

**ICA0014    Iniciando o daemon do monitor de logs.**

**Explicação:** O daemon foi iniciado.

---

**ICA0015    Não foi possível criar daemon para o monitor de logs: *número do erro***

**Explicação:** A criação do daemon falhou - veja a mensagem do erro.

---

**ICA0016    O arquivo de ids do processo não pôde ser aberto - pode ser que o daemon já esteja ativo.**

**Explicação:** O daemon não conseguiu abrir o arquivo de ids do processo.

---

---

**ICA0017** A id do processo (*id do processo*) não pôde ser gravada no *arquivo*.

**Explicação:** O daemon não conseguiu gravar a id do processo no arquivo.

---

**ICA0018** Monitor de Logs - vazio para leitura.

**Explicação:** Recebido pacote sem dados - descartado.

---

**ICA0019** Monitor de Logs - leitura incompleta. Código descartado.

**Explicação:** Recebido pacote sem dados suficientes - descartado.

---

**ICA0020** Monitor de Logs - tag de ICA mal formatada.

**Explicação:** Recebido pacote com dados mal formatados - descartados.

---

**ICA0021** Monitor de Logs - dados de autenticação mal formatados.

**Explicação:** Recebido pacote com dados mal formatados - descartados.

---

**ICA0022** Sintaxe inválida no arquivo de definição de limites (*entrada inválida*).

**Explicação:** A entrada indicada no arquivo de limites está sintaticamente incorreta.

---

**ICA0023** Impossível abrir o arquivo *fwmail.conf*.

**Explicação:** falha ao abrir o arquivo *fwmail.conf* ou o arquivo está vazio

---

**ICA0024** Impossível Conectar-se ao Servidor SMTP.

**Explicação:** O servidor SMTP está ocupado ou está recusando a conexão

---

**ICA0025** O Email da Mensagem de Alerta falhou.

**Explicação:** Não foi possível enviar pelo email uma mensagem de alerta do monitor de log para o endereço especificado.

---

**ICA0051** Dias para manter no arquivo de log, *nome do arquivo de log*, deve ser um valor curto de números inteiros sem sinais.

**Explicação:** Dias para manter no arquivo de log deve ser um número inteiro válido.

---

**ICA0052** Dias para manter nos arquivos compactados, *nome do arquivo de log*, deve ser um valor curto de números inteiros sem sinais.

**Explicação:** Dias para manter nos arquivos compactados deve ser um número inteiro válido.

---

**ICA0053** Não é permitido várias entradas para o arquivo de log, *nome de arquivo de log*, no *logmgmt.cfg*.

**Explicação:** Não é permitido várias entradas para um arquivo de log no *logmgmt.cfg*.

---

**ICA0054** Impossível abrir arquivo *\$ Variables* .:

**Explicação:** Impossível abrir arquivo *logmgmt.cfg*.

---

**ICA0055** Não há nenhuma entrada válida no arquivo *logmgmt.cfg*.

**Explicação:** Não há nenhuma entrada válida no arquivo *logmgmt.cfg*.

---

---

**ICA0056 A mensagem de log,"\$ Variables :", é inválida**

**Explicação:** A mensagem de log é inválida

---

---

**ICA1001 Impossível criar arquivo com a nossa id de processo**

**Explicação:** O daemon do sistema de registros do filtro encontrou erro quando gravava o arquivo fwlogd.pid.

**Resposta do Usuário:** Verifique o sistema de arquivos onde reside o diretório /etc/security. É possível que exista condição de falta de espaço.

---

---

**ICA1002 A comunicação com o programa cfgfilt não é possível**

**Explicação:** Devido ao fato de o arquivo fwlogd.pid não ter sido criado, a comunicação entre o daemon fwlogd e o aplicativo cfgfilt (necessário para o controle do filtro) não é possível.

**Resposta do Usuário:** Verifique o sistema de arquivos onde reside o diretório /etc/security. É possível que exista condição de falta de espaço.

---

---

**ICA1003 Prosseguindo com a inicialização do daemon do sistema de registros.**

**Explicação:** O daemon do fwlogd vai continuar a fazer o processamento de inicialização.

---

---

**ICA1004 O daemon de registros do filtro *fwlogd* (nível *versão.release*) inicializado as *horário em data***

**Explicação:** O daemon do sistema de registros do pacote de IP foi iniciado. Quando/se os registros do pacote estiverem ativos, o daemon fwlogd registrará as gravações necessárias no syslog, local4, arquivo.

---

---

**ICA1005 Os registros da(s) mensagem(ns) do pacote *sem regra do filtro* foram suspensos devido a estouro do buffer**

**Explicação:** O buffer de registros do filtro do daemon fwlogd estourou. Há um pacote da regra de filtro especificada que não pode ser registrado.

**Resposta do Usuário:** Verifique o registro. O firewall pode estar sob um ataque de negação de serviço ou pode ser que você esteja registrando mensagens desnecessárias. Mensagens de difusão, por exemplo, devem ter regra de negação com controle de registros definido para não (I=n) para evitar lotação do registro.

---

---

**ICA1006 Erro de fwlogd fatal - *falha na função: mensagem de erro***

**Explicação:** O servidor fwlogd falhou na função indicada, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie fwlogd.

---

---

**ICA1007 Não é possível bifurcar o processo filho: *número do erro***

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

**Resposta do Usuário:** Com base no erro apresentado, adote as medidas corretivas apropriadas.

---

---

**ICA1008 Retorno de erro da rotina *setpgrp*: *número do erro***

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

---

---

**ICA1009 Não é possível bifurcar o segundo processo filho: *número do erro***

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

---

**ICA1010 Esse daemon deve ser executado com autorização do root.**

**Explicação:** O daemon dos registros do filtro devem ser iniciados sob a autoridade do root.

**Resposta do Usuário:** Reinicie com autorização root.

---

**ICA1011 A chamada sysconfig para consultar extensão kernel *caminho carregado* falhou: *número do erro***

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

---

**ICA1012 A extensão do núcleo AIX *netinet* não foi carregada -- impossível continuar**

**Explicação:** O controlador de dispositivo **netinet** não contém suporte de filtro.

**Resposta do Usuário:** Instale o código do Firewall. Potencialmente, o código foi instalado mas a *reinicialização* não foi executada.

---

**ICA1013 A chamada de criação do soquete falhou: *número do erro***

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

---

**ICA1014 O controlador de dispositivo netinet do AIX não está no nível exigido**

**Explicação:** O controlador de dispositivo netinet e o daemon fwlogd não são do mesmo nível.

**Resposta do Usuário:** Resolva o conflito, é possível que seja necessário reinicializar depois de instalar o novo nível do Firewall.

---

**ICA1015 Erro na chamada ioctl() (SIOCGFWLOG): *número do erro***

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

---

**ICA1016 Impossível acessar a fila de log diferida atual**

**Explicação:** Informações adicionais associadas à mensagem do registro imediatamente anterior.

---

**ICA1017 Retorno de erro da chamada SIOCGFWLOG ioctl()**

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

---

**ICA1018 Erro fwlogd fatal - *falha na função: mensagem de erro do sistema***

**Explicação:** O servidor fwlogd falhou na função indicada, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie fwlogd.

---

**ICA1019 Saída de erro inesperada com *código de retorno interno fw***

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

---

**ICA1020 Erro fwlogd fatal - falha na função: código de retorno = 0x***código de retorno da função*

**Explicação:** O servidor fwlogd falhou na função indicada, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie fwlogd.

---

**ICA1021 Erro ao abrir /dev/ipsd\_poiif: número do erro**

**Explicação:** O controlador de dispositivo indicado não foi instalado.

**Resposta do Usuário:** Se o código do Firewall tiver sido instalado, verifique no arquivo /tmp/rc/net.out a presença de possíveis mensagens de erro.

---

**ICA1022 A verificação do suporte do filtro falhou.**

**Explicação:** Devido a um erro gravado antes dessa mensagem, não é possível verificar o suporte ao filtro.

---

**ICA1023 Erro na chamada ioctl() (SIOCGFWLVL): número do erro**

**Explicação:** Durante a inicialização do daemon dos registros do filtro, foi encontrado o erro do sistema indicado.

**Resposta do Usuário:** Execute uma das ações seguintes:

- Para AIX: :p.Verifique se o nível correto do controlador de dispositivo netinet do Firewall foi instalado e se a máquina foi reinicializada desde a instalação.
  - Para OS/390: :p.Verifique se foi instalado o nível correto do TCP/IP e se ele foi iniciado com a instrução de configuração **IPCONFIG FIREWALL**.
- 

**ICA1024 Erro ao gravar no arquivo /etc/security/fwlogd.pid: número do erro**

**Explicação:** Devido ao número do erro de sistema indicado, fwlogd não conseguiu gravar o arquivo especificado.

**Resposta do Usuário:** Corrija o problema indicado e reinicie o daemon dos registros do filtro.

---

**ICA1032 Regras do filtro atualizadas as *horário do dia data***

**Explicação:** As regras de filtragem do pacote de IP foram atualizadas.

---

**ICA1033 Suporte do filtro (nível *versão.release*) inicializado as *horário do dia data***

**Explicação:** O suporte do filtro do Firewall foi inicializado.

---

**ICA1034 Suporte do filtro desativado as *horário do dia data***

**Explicação:** Os filtros do pacote IP agora estão usando as regras de filtro padrão em vez das regras definidas no arquivo /etc/security/filters.cfg.

---

**ICA1035 Status dos registros do pacote definido para *ativado/desativado* as *horário do dia data***

**Explicação:** O status do registro do pacote foi alterado. A mensagem indica o estado atual com o registro de data e horário.

---

---

**ICA1036** *Número:sem regra R: direção do tipo de regra: interface s:end. src d: end. dst p: protocolo tag: porta scr/tipo icmp tag: porta dst/código icmp r:roteada/local a: seguro/não seguro f:sim/não T:id de túnel e:C/D/n l:comprimento do pacote*

**Explicação:** Registro de log indicando pacote de IP processado e sua correspondente regra de filtro. Para esse registro ser gravado, a regra de filtro correspondente deve ter o controle do registro definido para *sim*. Se o pacote de IP compatível com a regra for um fragmento, a informação ports/icmp type/code aparece para o pacote do cabeçalho mais é mostrada como zero para outros pacotes que não sejam o de cabeçalho.

---

**ICA1037** *número:regra sem ação end. src máscara src end. dst máscara dst protocolo valor lógico op valor op lógico tipo de interface direção roteamento= controle de log f=controle de fragmentação= ID do túnel enc\_alg auth\_alg*

**Explicação:** Quando as regras de filtro são atualizadas, as regras ativadas são gravadas no registro. Essa mensagem de registro descreve uma das regras ativadas.

---

**ICA1038** **O mecanismo da Chave de Sessão foi iniciado, usando a porta do soquete da sessão:***número da porta e a porta de soquete principal número da porta*

**Explicação:** O túnel de criptografia foi iniciado usando números de porta UDP especificados, como define o /etc/services.

---

**ICA1039** **Regulamento sendo (re)definido como:**

**Explicação:** Cache do regulamento sendo (re)definido usando o arquivo /etc/security/fwpolicy. As linhas a seguir mostram o novo cache do regulamento.

---

**ICA1040** **Instrução do regulamento do >:** *origem do túnel, endereço do túnel, ID do túnel, sinalizador de criptografia/sinalizador autenticado*

**Explicação:** Linha registrada foi lida a partir do arquivo /etc/security/fwpolicy.

---

**ICA1041** **Especificação de contexto eliminada para o túnel:***ID do túnel*

**Explicação:** O contexto do túnel, para o ID listada, não é mais operacional.

---

**ICA1042** **Está(ão) definida(s) a(s) seguinte(s) especificação(ões) de contexto do túnel:**

**Explicação:** As especificações de contexto do túnel estão sendo definidas, como mostram os seguintes registros de log.

---

**ICA1043** **>tunnel\_ID:***número, src\_addr: endereço de IP, end. dst: endereço de IP, criptografia: algoritmo*

**Explicação:** Atributos específicos das listas de mensagem do contexto de túnel ativado.

---

**ICA1044** **Aviso do Contador do Host: IP(Endereço de IP) acima do limite**

**Explicação:** Há muitos hosts protegidos; tente conectar-se com a máquina do firewall

**Ação do Sistema:** passar conexões

---

**ICA1045** **Estouro de limite do TCP:** *Endereço de IP(Porta)->Endereço de IP(Porta) rejeitados*

**Explicação:** Há sessões de TCP em demasia passando pela máquina de firewall

**Ação do Sistema:** rejeitar conexões

---

**ICA1046 Estouro de limite do UDP:** *Endereço de IP(Porta)->Endereço de IP(Porta)* rejeitados.

**Explicação:** Há sessões de UDP em demasia passando pela máquina de firewall

**Ação do Sistema:** rejeitar conexões

---

**ICA1047 Aviso de Período de Tolerância :** *sessões de TCP em demasia* *Endereço de IP( Porta)->Endereço de IP( Porta)* passaram

**Explicação:** Há sessões de TCP em demasia passando pela máquina de firewall

**Ação do Sistema:** passar conexões

---

**ICA1048 Advertência do Período de Tolerância :** *sessões de UDP demais,Endereço IP(%2\$d)->Endereço IP(%4\$d)* passado

**Explicação:** Há sessões de UDP em demasia passando pela máquina de firewall

---

**ICA1049 Pacote ipsec inválido:** *s:Endereço IP d:Endereço IP protocolo:Protocolo spi:Índice de Segurança do Parâmetro*

**Explicação:** O pacote ipsec não pode ser decapsulado pelo firewall receptor.

**Resposta do Usuário:** Certifique-se de que a definição do túnel foi exportada corretamente e ativado em cada firewall.

---

**ICA1200 Encerrando o daemon dos registros devido aos erros acima**

**Explicação:** Devido aos erros registrados antes desta mensagem, o daemon fwlogd está sendo encerrado.

**Ação do Sistema:** Os registros do filtro de IP não serão ativados.

**Resposta do Usuário:** Corrija os erros indicados e reinicie fwlogd.

---

**ICA1260 O daemon dos registros do filtro está sendo encerrado as** *horário do dia data* **devido ao recebimento de sinal de término**

**Explicação:** O daemon do fwlogd recebeu o sinal de término indicado e está sendo interrompido.

---

**ICA1305 \ "desconhecido"**

**Explicação:** Ao formatar um pacote de IP para syslog, foi encontrado um registro com especificação de protocolo desconhecida. Os protocolos IP, ICMP, TCP, UDP e IPSP são os protocolos reconhecidos. Note que IPSP é a designação da IBM para os pacotes criptografados passados por túnel.

---

**ICA1400 Erro fwtimernat fatal - falha na função:** *mensagem de erro do sistema*

**Explicação:** O servidor fwtimernat falhou na função indicada, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie fwtimernat.

---

**ICA1401 Erro fwtimernat fatal - falha na função:** *código de retorno = 0xcódigo de retorno da função*

**Explicação:** O servidor fwtimernat falhou na função indicada, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie fwtimernat.

---

---

**ICA1402 Erro fwtimernat fatal - falha na função: mensagem de erro**

**Explicação:** O servidor fwtimernat falhou na função indicada, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie fwtimernat.

---

**ICA2000 Nova sessão FTP para endereço de IP a partir do endereço de IP (local não-protegido).**

**Explicação:** Iniciando uma sessão ftp nova de um site não-protegido.

---

**ICA2001 Autenticação falha para nome de usuário (desconhecido) proveniente de ftp de rede: endereço IP.**

**Explicação:** Um usuário, sem uma conta, tentou usar ftp proxy a partir da rede.

**Resposta do Usuário:** Fale com o administrador do firewall para configurar uma conta de proxy.

---

**ICA2002 A autenticação falhou para o usuário nome com método de autenticação a partir da rede: nome do host.**

**Explicação:** O firewall não consegue autenticar o nome de usuário indicado usando o método de autenticação especificado.

**Resposta do Usuário:** Entre em contato com o administrador do Firewall.

---

**ICA2003 Não há shells configuradas para o nome do usuário.**

**Explicação:** O usuário identificado tentou um login proxy, mas não há login shell definido.

**Resposta do Usuário:** Fale com o administrador do Firewall para corrigir o perfil de login do usuário.

---

**ICA2004 Recebido evento de auditoria desconhecido do 0xvalor hex.**

**Explicação:** Foi recebido um pedido de auditoria desconhecido por parte do módulo tcpip\_audit.c.

---

**ICA2005 Erro na gravação para cliente: número do erro.**

**Explicação:** Impossível comunicar-se com o cliente, consulte a mensagem do sistema registrada.

---

**ICA2006 ptelnetd: auditproc: número do erro.**

**Explicação:** Retornado erro indicado pelo processo de auditoria do telnet. Corrupção de dados em potencial dos arquivos do sistema.

---

**ICA2007 ptelnetd: estado de pânico=valor.**

**Explicação:** Detectado um erro desconhecido. Corrupção de dados em potencial dos arquivos do sistema.

---

**ICA2008 Usuário não-firewall nome do :endereço de IP no telnet.**

**Explicação:** Um usuário sem conta firewall tentou usar o proxy telnet.

**Ação do Sistema:** Usado Assumir Autenticação Genérica.

---

---

**ICA2009** */bin/login: número do erro.*

**Explicação:** Erro fatal durante login do sistema. Veja a mensagem de erro de sistema indicada.

---

**ICA2010** **Conecte-se ao endereço de IP a partir do endereço de IP (não-protegido).**

**Explicação:** Conexão bem sucedida entre os endereços de IP indicados através da interface não-protegida.

---

**ICA2011** **Conecte-se ao endereço de IP a partir do endereço de IP (protegido).**

**Explicação:** Conexão bem sucedida entre os endereços de IP indicados através da interface protegida.

---

**ICA2012** **Nova sessão FTP para endereço de IP a partir do endereço de IP (local protegido).**

**Explicação:** Iniciando uma nova sessão ftp.

---

**ICA2013** **Nova sessão Telnet para endereço de IP a partir do endereço de IP.**

**Explicação:** Estabelecida nova sessão de telnet.

---

**ICA2014** **Opção valor não suportada.**

**Explicação:** O sinalizador indicado não é suportado; veja a mensagem anterior.

---

**ICA2015** **Opção -valor não suportada.**

**Explicação:** O sinalizador indicado não é suportado; veja a mensagem anterior.

---

**ICA2016** **ID de usuário remoto \"nome\".**

**Explicação:** solicitação de conexão ftp para usuário indicado.

---

**ICA2017** **Depurar - na linha.**

**ICA2018** **Chave SNK não encontrada para nome do usuário.**

**Explicação:** Valor de SecureNetKey não encontrado para ID de usuário indicada.

**Resposta do Usuário:** Indague ao administrador do Firewall sobre possível problema de configuração de login.

---

**ICA2019** **A chave SNK não está adequadamente pronta para o nome do usuário.**

**Explicação:** Valor de SecureNetKey não legível como dígitos octais para a ID de usuário indicada.

**Resposta do Usuário:** Indague ao administrador do Firewall sobre possível problema de configuração de login.

---

**ICA2020** **/usr/bin/fwuserau ou /usr/bin/fwuserpt não existe.**

**Explicação:** A autenticação pelo método fornecido pelo usuário foi abortada.

**Ação do Sistema:** A autenticação foi abortada.

**Resposta do Usuário:** Veja se /usr/bin/fwuserau e /usr/bin/fwuserpt existem e se o proprietário é o root. Se o executável não existir, o usuário deve criar um executável, usando um compilador compatível com o sistema operacional do firewall e nomeá-lo como /usr/bin/fwuserau ou como /usr/bin/fwuserpt.

---

**ICA2021** Tentando fazer conexão com o host remoto *nome* com id de usuário *nome*.

**Explicação:** Tentando estabelecer uma nova conexão ftp.

---

**ICA2022** Tentando fazer conexão com o host remoto *nome*.

**Explicação:** Tentando estabelecer uma nova conexão ftp.

---

**ICA2023** Uso: `ptelnetd {-n,, {-s,,.`

**Explicação:** Sinalizador desconhecido especificado ao iniciar o daemon do ptelnet.

**Resposta do Usuário:** Use apenas sinalizadores -n e/ou -s.

---

**ICA2024** Usuário *nome* autenticado com sucesso usando a autenticação *método da rede: nome do host*.

**Explicação:** O FW autenticou o nome de usuário indicado usando o método de autenticação especificado.

---

**ICA2025** Usuário *nome* logado usando autenticação *método da rede: nome do host*.

**Explicação:** usuário ftp com sessão iniciada.

---

**ICA2026** O *nome do usuário* venceu depois de *n segundos* do *horário atual*.

**Explicação:** A tentativa de conexão teve seu tempo esgotado para o usuário especificado. Problema de roteamento da rede em potencial ou o host remoto não está disponível.

---

**ICA2027** Conexão a partir do *host remoto* as *horário*.

**Explicação:** Conexão ftp da rede estabelecida com o Firewall.

---

**ICA2028** Tentativa de conexão FTP com *endereço de IP* a partir de *endereço de IP* recusada. Esta máquina não suporta FTP de local não-seguro.

**Explicação:** Geralmente, indica uma tentativa de estabelecer uma conexão ftp com o Firewall através da interface não-protetida.

**Ação do Sistema:** Rejeitar a conexão.

---

**ICA2029** Erro de sistema com número do erro = - na *linha* *linha*.

**Explicação:** A chamada do sistema encontra um problema durante a execução da chamada do sistema.

**Ação do Sistema:** Execução do sistema paralisada

**Resposta do Usuário:** acesse o log, descubra o significado do número do erro e tente resolver o problema. Se não conseguir, entre em contato com a IBM.

---

**ICA2030** Chamada de função com código de retorno = - na *linha* *linha*.

**Explicação:** A chamada da função encontrou um problema.

**Ação do Sistema:** Erro retornado

**Resposta do Usuário:** Chame o log, descubra o significado do código de retorno e tente resolver o problema. Se não conseguir, entre em contato com a IBM.

---

---

**ICA2031 Chamada de função sdi creadcfg() rc = -.**

**Explicação:** A chamada da função encontrou um problema.

**Ação do Sistema:** Erro retornado

**Resposta do Usuário:** consulte a referência sdi para saber a explicação.

---

**ICA2032 Conexão perdida.**

**Explicação:** Conexão ftp perdida.

**Resposta do Usuário:** Reestabelecer sessão.

---

**ICA2033 Chamada de função sdi sd\_init rc = -.**

**Explicação:** A chamada da função encontrou um problema.

**Ação do Sistema:** Erro retornado

**Resposta do Usuário:** consulte a referência sdi para saber a explicação.

---

**ICA2034 Chamada de função sdi sd\_check rc = -.**

**Explicação:** A chamada da função encontrou um problema.

**Ação do Sistema:** Erro retornado

**Resposta do Usuário:** consulte a referência sdi para saber a explicação.

---

**ICA2035 setsockopt(): número do erro.**

**Explicação:** Erro de sistema na chamada setsocketopt.

---

**ICA2036 Sessão de Telnet *id da sessão iniciada para usuário id de usuário (end. de IP de origem:end. de IP de destino).***

**Explicação:** Mensagem gerada no início de cada sessão de Telnet. A sessão começa quando a id do usuário, o ip de origem e o ip de destino são conhecidos para o firewall. A id da sessão é um identificador único, gerado pelo firewall.

---

**ICA2037 O usuário fwdfuser ou fwdpuser tentou efetuar login, mas não tem permissão.**

**Explicação:** fwdfuser e fwdpuser são usuários reservados e não devem ser usados.

**Ação do Sistema:** Login recusado.

**Resposta do Usuário:** O administrador deve investigar quem está usando essa id de usuário.

---

**ICA2038 tloop: o peer foi interrompido: número do erro.**

**Explicação:** Ocorreu erro ao limpar o buffer de saída da rede. Parece que o processo do peer morreu.

---

**ICA2039 tloop: leitura: número do erro.**

**Explicação:** Ocorreu erro ao limpar o buffer de saída da rede.

---

---

**ICA2040 Autenticação definida para senha, nenhum ou snk não é permitida para ID de usuário fwdfuser.**

**Explicação:** fwdfuser é uma ID de usuário reservada e não deve usar senha ou nenhum - n - como método de autenticação.

**Ação do Sistema:** Login recusado.

**Resposta do Usuário:** O administrador deve mudar o método de autenticação para a ID de usuário fwdfuser.

---

**ICA2041 Sessão FTP *id da sessão iniciada para id de usuário ( end. IP de origem: end. IP de destino).***

**Explicação:** Mensagem gerada no início de cada sessão de FTP. A sessão começa quando a id do usuário, o ip de origem e o ip de destino são conhecidos para o firewall. A id da sessão é um identificador único, gerado pelo firewall.

---

**ICA2042 req\_rsp\_code está definido incorretamente para FW\_AUTH\_REQ.**

**Explicação:** fw\_tn\_authenticate não tem permissão para definir req\_rsp\_code para FW\_AUTH\_REQ.

**Ação do Sistema:** Abortar a autenticação.

**Resposta do Usuário:** Mude o fw\_tn\_authenticate, faça a biblioteca fwuser.o de novo e coloque-a no Firewall.

---

**ICA2043 Não foi possível obter senha para *nome do usuário.***

**Explicação:** O tipo de autenticação para esse usuário é 'senha' e não foi encontrada nenhuma senha.

**Resposta do Usuário:** Entre em contato com o administrador do Firewall.

---

**ICA2044 Horário incorreto (*valor*) especificado para -t.**

**Explicação:** O valor do horário mostrado contém caracteres fora do intervalo numérico de 0..9 ou excede o valor máximo permitido.

---

**ICA2045 Opção -T não suportada no firewall.**

**Explicação:** Opção indicada não suportada.

---

**ICA2046 Opção -k não suportada no firewall.**

**Explicação:** Opção indicada não suportada.

---

**ICA2047 Opção -s não suportada no firewall.**

**Explicação:** Opção indicada não suportada.

---

**ICA2048 Opção -u não suportada no firewall.**

**Explicação:** Opção indicada não suportada.

---

**ICA2049 Sinalizador desconhecido -*valor* ignorado.**

**Explicação:** O sinalizador indicado foi especificado, mas não é reconhecido.

---

**ICA2050 Parâmetro desconhecido *valor*.**

**Explicação:** O valor indicado, especificado como opção, não é reconhecido.

---

**ICA2051 Erro de conversão adapt\_addr no endereço.**

**Explicação:** O endereço de IP mostrado não é válido.

**Resposta do Usuário:** Corrupção possível do arquivo /etc/security/fwsecadpt.cfg. Remova o arquivo, reconfigure a(s) interface(s) protegida(s) e reinicialize os filtros.

---

**ICA2052 afopen não conseguiu abrir /etc/security/login.cfg: número do erro.**

**Explicação:** Impossível autenticar usuário, erro aberto no arquivo indicado.

---

**ICA2053 O arquivo de interfaces protegidas não pôde ser aberto.**

**Explicação:** Não foi configurada interface protegida.

**Resposta do Usuário:** Se uma interface protegida tiver de ser definida, use os painéis Comandos/smit do Firewall para definir a(s) interface(s) protegida.

---

**ICA2054 enduserdb rc=valor, número do erro.**

**Explicação:** Recebido código de erro do sistema indicado tentando recuperar as informações do perfil de início de sessão do usuário.

**Resposta do Usuário:** Consulte o administrador do Firewall para verificar sua conta de login.

---

**ICA2055 getpeername() (nome de invocação): número do erro.**

**Explicação:** Erro do sistema quando o ftp daemon tentou obter o nome do soquete.

---

**ICA2056 getsockname() (nome de invocação): número do erro.**

**Explicação:** Erro do sistema quando ftp daemon tentou obter o nome da porta.

---

**ICA2057 shell não-protégida getuser rc=valor para ID de usuário, número do erro.**

**Explicação:** Recebido código de erro do sistema indicado tentando recuperar o nome da shell para conexão do lado não-protégido do Firewall.

**Resposta do Usuário:** Fale com o administrador do Firewall para definir uma shell para o perfil de login do usuário.

---

**ICA2058 shell protegida getuser rc=valor para ID de usuário, número do erro.**

**Explicação:** Recebido código de erro do sistema indicado tentando recuperar o nome da shell para conexão do lado protegido do Firewall.

**Resposta do Usuário:** Fale com o administrador do Firewall para que ele defina um shell para o seu perfil de início de sessão de usuário.

---

**ICA2059 ioctl(): número do erro**

**Explicação:** Erro de sistema na chamada ioctl() para SIOCSPGRP.

---

**ICA2060 ptelnetd: o ftok de memória compartilhada falhou.**

**Explicação:** Não foi possível alocar segmento de memória compartilhada.

**Resposta do Usuário:** Contate o administrador do Firewall, problema de memória aparente.

---

**ICA2061    ptelnetd: o shmat de memória compartilhada falhou.**

**Explicação:** Não foi possível alocar segmento de memória compartilhada.

**Resposta do Usuário:** Contate o administrador do Firewall, problema de memória aparente.

---

**ICA2062    ptelnetd: o shmget de memória compartilhada falhou.**

**Explicação:** Não foi possível alocar segmento de memória compartilhada.

**Resposta do Usuário:** Contate o administrador do Firewall, problema de memória aparente.

---

**ICA2063    setsockopt() (SO\_DEBUG): número do erro.**

**Explicação:** A mensagem de erro indicada foi retornada na chamada de sistema 'setsockopt'.

---

**ICA2064    setsockopt() (SO\_KEEPALIVE): número do erro.**

**Explicação:** A mensagem de erro indicada foi retornada na chamada de sistema 'setsockopt'.

---

**ICA2065    setuser rc=valor, número do erro.**

**Explicação:** Recebido código de retorno ruim para uma chamada de sistema pela razão indicada.

---

**ICA2066    signal(): número do erro.**

**Explicação:** Erro do sistema quando o ftp daemon tentou estabelecer o manipulador de sinais.

---

**ICA2067    Erro de inicialização pftpd fatal - bind(): número do erro**

**Explicação:** A inicialização do servidor pftpd falhou, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie o pftpd. A causa mais provável para este erro é outro ftp daemon já ter atendido na porta ftp padrão (21).

---

**ICA2068    Erro de inicialização pftpd fatal - listen(): número do erro**

**Explicação:** A inicialização do servidor pftpd falhou, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie o pftpd.

---

**ICA2069    Erro pftpd fatal - main accept(): número do erro**

**Explicação:** A rotina principal do servidor pftpd falhou, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie o pftpd.

---

**ICA2070    Erro de inicialização pftpd - socket(): número do erro**

**Explicação:** A inicialização do servidor pftpd falhou, o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie o pftpd.

---

---

**ICA2071 Conexão recusada, número máximo de conexões foi atingido.**

**Explicação:** O servidor pftpd não pode criar outra sessão FTP porque o número máximo de sessões já existe.

**Ação do Sistema:** A conexão é recusada.

**Resposta do Usuário:** Aguarde até que conexões existentes sejam encerradas e depois tente fazer o pedido novamente.

---

**ICA2072 O arquivo de configuração ftp (*nome do arquivo*) não está disponível.**

**Explicação:** O ftp daemon tentou abrir o arquivo de configuração ftp especificado mas ele não existe ou não pode ser aberto.

**Ação do Sistema:** O processamento do ftp daemon usa a configuração padrão

**Resposta do Usuário:** Nenhum, a não ser o arquivo deve existir, caso em que ele deve ser criado ou transferido para o local especificado na mensagem.

---

**ICA2073 Impossível obter armazenamento para a tabela de linguagem ftp.**

**Explicação:** O armazenamento requerido para representar uma instrução REPLYLANGUAGE no arquivo de configuração ftp não pôde ser obtido.

**Ação do Sistema:** O processamento continua.

**Resposta do Usuário:** Aumente o tamanho da região ou reduza as entradas no arquivo de configuração.

---

**ICA2074 Processamento completo para instrução ftp config: *instrução de configuração***

**Explicação:** ftp processou a instrução de configuração indicada.

**Ação do Sistema:** O processamento continua.

**Resposta do Usuário:** Nenhuma

---

**ICA2075 FTP correspondente à *id de usuário (endereço de IP de origem: endereço de IP de destino)*, operação *nome do arquivo*, número de bytes **bytes**. **sid:** *id da sessão*.**

**Explicação:** Mensagem gerada para cada transferência de arquivo em sessões de FTP abertas. O sid é um identificador único e exclusivo, gerado pelo firewall no início da sessão.

---

**ICA2076 A sessão FTP *id da sessão* terminou para a *id de usuário ( endereço IP de origem: endereço IP de destino)*, duração **segundos**, número de bytes **bytes**.**

**Explicação:** Mensagem gerada no fim de cada sessão do daemon FTP. O sid é um identificador único e exclusivo, gerado pelo firewall no início da sessão.

---

**ICA2077 A sessão de Telnet *id da sessão* terminou para *id do usuário (endereço IP de origem: endereço IP de destino)*, número de bytes **bytes**.**

**Explicação:** Mensagem gerada no final de cada sessão de Telnet. O sid é um identificador único e exclusivo, gerado pelo firewall no início da sessão.

---

**ICA2078 Usuário de proxy desconectado *usuário* - inativo por *tempo* minutos.**

**Explicação:** A sessão do usuário excedeu o tempo máximo permitido de inatividade.

---

**ICA2079    Atenção - Tentativa de conexão não autorizada para *endereço de IP* a partir de *endereço de IP*.**

**Explicação:** Em geral indica tentativa de estabelecer conexão com o Firewall através de interface não-protegida.

**Ação do Sistema:** Rejeitar a conexão.

---

**ICA2080    Erro de sintaxe (*motivo*) próximo à coluna *coluna* na linha do arquivo de configuração *linha: instrução de configuração***

**Explicação:** A instrução de configuração ftp na linha dada apresenta erro. O motivo do erro e a localização em que ele foi detectado são fornecidos.

**Ação do Sistema:** A instrução é ignorada.

**Resposta do Usuário:** Corrija a instrução no arquivo de configuração ftp.

---

**ICA2081    Nenhum catálogo de mensagens dado pelas instruções de configuração ftp é utilizável.**

**Explicação:** Tentativas de abrir os catálogos de mensagens dados pelas instruções de configuração ftp REPLYLANGUAGE falharam. Não pode ser usado nenhum catálogo de mensagens do cliente.

**Ação do Sistema:** O catálogo de mensagens do cliente foi forçado a assumir o idioma inglês no diretório C.

**Resposta do Usuário:** Certifique-se de que há arquivos de catálogo em cada um dos diretórios associados aos diretórios de linguagem nas instruções REPLYLANGUAGE de configuração ftp. Verifique também se a variável de ambiente NLSPATH está definida corretamente para permitir a substituição tanto do subdiretório, a partir da variável de ambiente LANG (%L), quanto do nome do catálogo (%N).

---

**ICA2082    Impossível definir a variável ambiental LANG para *subdiretório*, motivo: *motivo***

**Explicação:** Um erro do sistema (dado pelo motivo) ocorreu quando o ftp daemon estava tentando alterar a definição da variável ambiental LANG para o subdiretório especificado.

**Ação do Sistema:** O processamento continua. A recuperação pode gerar outras mensagens.

**Resposta do Usuário:** Use o motivo dado para determinar se se trata de erro do sistema ou de erro de programação.

---

**ICA2083    Impossível abrir o catálogo de mensagens do cliente ftp no diretório: *subdiretório*, motivo: *motivo***

**Explicação:** O ftp daemon não pôde abrir o catálogo de mensagens no subdiretório dado. A razão dada é o número do erro retornado pelo catopen().

**Ação do Sistema:** O processamento continua. A recuperação pode gerar outras mensagens.

**Resposta do Usuário:** Procure certificar-se de que há catálogo no diretório associado ao diretório de idioma fornecido. Verifique se a variável de ambiente NLSPATH está definida corretamente para permitir a substituição tanto do subdiretório (%L) quanto do nome do catálogo (%N).

---

**ICA2084 Forçando catálogo de mensagens do cliente ftp para Inglês via subdiretório de C.**

**Explicação:** Devido a erros anteriormente relacionados, o ftp daemon forçou o catálogo de mensagens do cliente para o idioma Inglês usando o subdiretório de C.

**Ação do Sistema:** Se o idioma puder ser forçado para o catálogo de mensagens C, o processamento continuará. Se não puder, o programa sairá.

**Resposta do Usuário:** Corrija o erro a partir da mensagem anterior. Se o programa também existia, crie o catálogo de mensagens no subdiretório C e defina corretamente a variável de ambiente NLSPATH.

---

**ICA2085 A Sessão de Telnet terminou para a pid *id do processo (endereço de IP de origem)*.**

**Explicação:** Mensagem gerada no final de cada sessão de Telnet.

---

**ICA2086 Arquivo de usuário mal configurado; usuário *usuário sem chave (chave)*.**

**Explicação:** O ftpd encontrou o usuário solicitado no arquivo de usuários, mas não pôde encontrar a chave - arquivo de usuário mal configurado.

**Resposta do Usuário:** Use os comandos do Firewall/painéis smit para corrigir o problema.

---

**ICA2087 O ftpd não pôde encontrar o usuário especificado *usuário no arquivo config*.**

**Explicação:** O nome de usuário especificado não foi configurado ou então o arquivo user.cfg está danificado.

**Resposta do Usuário:** Use os comandos do Firewall/painéis smit para corrigir o problema.

---

**ICA2088 O ftpd não pôde abrir o arquivo de configuração do usuário.**

**Explicação:** O ftpd fez uma chamada a fopen que falhou por não poder abrir o arquivo de config do usuário.

**Resposta do Usuário:** Confira se o arquivo de config. do usuário (user.cfg, por padrão) está disponível; use os comandos/painéis smit do Firewall

---

**ICA2089 O tipo de autorização do arquivo do usuário (*Tipo de autorização*) não correspondeu a nenhuma entrada na tabela (struct tab2 authtab{,,).**

**Explicação:** O tipo de autorização do usuário especificado (retornado pelo user.cfg) não corresponde a nenhum tipo suportado (como negar,nenhum,sdi,senha,etc.)

**Resposta do Usuário:** Verifique a integridade ou a configuração do arquivo de user.cfg; use os comandos/painéis smit do Firewall para corrigir o problema.

---

**ICA2090 A autenticação falhou para o usuário '*nome do usuário*' a partir do *ip do cliente* porque KEY=DENY no arquivo user.cfg.**

**Explicação:** A autenticação falhou devido a especificações do arquivo user.cfg definidas pelo administrador do Firewall.

**Resposta do Usuário:** Entre em contato com o administrador do Firewall.

---

**ICA2091    Usuário '*nome do usuário*' não permitido ao ftp para a porta não-protégida (*firewall ip*).**

**Explicação:** Usuário tentou o ftp no servidor do firewall via uma porta não-protégida (nsp) - todos os usuários nsp devem ter suas chaves 'fwnsftp' configuradas corretamente para um tipo de autorização válido (no arquivo user.cfg).

**Resposta do Usuário:** Verifique a integridade ou a configuração do arquivo de user.cfg; use os comandos/painéis smit do Firewall para corrigir o problema.

---

**ICA2092    Erro Interno: o nt\_gwauth() falhou.**

**Explicação:** nt\_gwauth() normalmente retorna um dos três valores (AUTHENTICATED, NOT\_AUTHENTICATED ou DENY) neste caso nt\_gwauth retornou algum inteiro inválido.

---

**ICA2093    Usuário '%1\$s' não permitido ao ftp para a porta protegida (%2\$s).**

**Explicação:** Usuário tentou o ftp no servidor do firewall via uma porta protegida (sp) - todos os usuários devem ter a chave 'fwsftp' deles configurada corretamente para um tipo de autorização válido (no arquivo user.cfg).

**Resposta do Usuário:** Verifique a integridade ou a configuração do arquivo de user.cfg; use os comandos/painéis smit do Firewall para corrigir o problema.

---

**ICA2094    O Login Falhou: formato esperado: "SENHA <senha>" depois: "USUÁRIO <nome do usuário>"; recebido cmd. inválido.**

**Explicação:** A autenticação falhou porque o cliente ftp não enviou o formato esperado (PASS 'senha' por RFC959)

**Resposta do Usuário:** Digite "usuário <nome do usuário>"; digite a senha correta. Entre em contato com o administrador do Firewall.

---

**ICA2095    O Login Falhou: (via método *método de autenticação*) falhou a autenticação do usuário '*nome do usuário*' a partir do *ip do cliente* (local do cliente).**

**Explicação:** A autenticação falhou devido a uma entrada inválida (pelo cliente para o tipo de autenticação especificado) - como senha, chave snk, etc inválidos fornecidos pelo usuário.

**Resposta do Usuário:** Entre em contato com o administrador do Firewall.

---

**ICA2096    Autenticado: (via método *método de autenticação*) autenticação bem sucedida do usuário '*nome do usuário*' a partir do *ip do cliente* (local do cliente) .**

**Explicação:** A autenticação foi feita

---

**ICA2097    httpd --> Iniciando a versão do servidor de proxy HTTP *Versão Proxy HTTP*.**

**Explicação:** Proxy HTTP para acesso à WWW sendo iniciado.

---

**ICA2098    httpd --> Encerrando o servidor de proxy HTTP.**

**Explicação:** O proxy HTTP para acesso à WWW está sendo encerrado.

---

---

**ICA2099**    **httpd --> Status: <Código de Status HTTP> do cliente < endereço de IP>, que solicitou <Ö" pedido GET HTTPÖ"> para <número de bytes>.**

**Explicação:** Status do pedido HTTP do cliente por arquivo através do proxy. Para obter maiores informações sobre o valor do código de "Status", consulte os documentos HTTP 1.0(RFC 1945) ou HTTP 1.1(RFC 2068) (ou RFCs cedidos) disponíveis em vários sites na internet, incluindo ds.internic.net.

---

**ICA2100**    **Endereço de soquete igual a zero.**

**Explicação:** Foi encontrado endereço de destino inválido no pedido local.

---

**ICA2101**    **Erro de família no endereço de soquete: tipo de família sin.**

**Explicação:** Foi encontrado um tipo de família com endereço inválido no pedido local.

---

**ICA2102**    **Erro na inicialização do odm: número do erro odm.**

**Explicação:** Ocorreu um erro odm\_initialize() para ODM (Gerenciador de Dados do Objeto).

---

**ICA2103**    **Erro na definição do caminho padrão do odm: número do erro odm.**

**Explicação:** Ocorreu um erro odm\_set\_path() para o ODM (Gerenciador de Dados do Objeto). classe do objeto, OCSvhost.

---

**ICA2104**    **Erro ao travar o banco de dados odm: número do erro odm.**

**Explicação:** Ocorreu um erro odm\_lock() para o ODM (Gerenciador de Dados do Objeto).

---

**ICA2105**    **Erro na abertura do objeto odm Atributos Customizados: número do erro odm.**

**Explicação:** Ocorreu um erro odm\_open\_class() para o ODM (Gerenciador de Dados do Objeto).

---

**ICA2106**    **Erro ao pesquisar objeto odm host virtual OCS: número do erro odm.**

**Explicação:** Ocorreu um erro odm\_get\_first() para o ODM (Gerenciador de Dados do Objeto). classe do objeto, OCSvhost.

---

**ICA2107**    **Erro no fechamento do objeto host virtual OCS: número do erro odm.**

**Explicação:** Ocorreu um erro odm\_close\_class() para o ODM (Gerenciador de Dados do Objeto). classe do objeto, OCSvhost.

---

**ICA2108**    **Erro ao destravar banco de dados odm: número do erro odm.**

**Explicação:** Ocorreu um erro odm\_unlock() para o ODM (Gerenciador de Dados do Objeto).

---

**ICA2109**    **Erro no fechamento do odm: número do erro odm.**

**Explicação:** Ocorreu um erro odm\_open\_terminate() para o ODM (Gerenciador de Dados do Objeto).

---

**ICA2110**    **Erro ao chamar o servidor pelo nome: número do erro.**

**Explicação:** Ocorreu um erro de getservbyname(). O serviço do Monitor de Login do host, lm, não está devidamente especificado no arquivo /etc/services.

---

---

**ICA2111 erro de byname():** *número do erro.*

**Explicação:** Ocorreu um erro de gethostbyname(). O nome da máquina do host não está devidamente especificado no /etc/hosts.

---

**ICA2112 Nome de protocolo inválido:** *nome de protocolo.*

**Explicação:** O nome de protocolo especificado na classe de objeto ODM, OCSvhost, não é suportado.

---

**ICA2113 Erro na abertura do soquete para LM:** *número do erro.*

**Explicação:** Ocorreu um erro no socket() para a máquina de host em que reside o Monitor de Logins.

---

**ICA2114 Erro na ligação do endereço local:** *número do erro.*

**Explicação:** Erro de bind() ao usar o endereço local para esse nó OCS.

---

**ICA2115 Erro na conexão do soquete com o LM:** *número do erro.*

**Explicação:** Ocorreu um erro connect() com a máquina do host em que o Monitor de Login reside.

---

**ICA2116 Erro de tipo de protocolo:** *tipo de protocolo.*

**Explicação:** O tipo de protocolo terminal virtual usado para fazer a comunicação com o Monitor de Login do host é inválido.

---

**ICA2117 Erro de malloc na mensagem LM.**

**Explicação:** Ocorreu um erro de malloc() quando o espaço era alocado dinamicamente para a mensagem do Monitor de Login de comprimento variável.

---

**ICA2118 Erro na transmissão de msg para LM:** *número do erro.*

**Explicação:** Ocorreu um erro de send() quando era enviado ao Monitor de Logins um pedido de abertura do dispositivo de host correto.

---

**ICA2119 Erro ao receber msg do LM:** *número do erro.*

**Explicação:** Ocorreu um erro de recv() quando o Monitor de Login retornou aviso de recebimento.

---

**ICA2120 Erro de status a partir do LM:** *status.*

**Explicação:** O aviso de recebimento dado pelo Monitor de Logins (LM) indica que o dispositivo do host NÃO havia sido bem aberto.

---

**ICA2121 Erro na abertura do dispositivo de administração do OCS:** *número do erro.*

**Explicação:** O dispositivo de administração do OCS não foi bem aberto.

---

**ICA2122 Falha na conversão do endereço de IP para TBM ID:** *número do erro.*

**Explicação:** Ocorreu erro ioctl() OCS\_GET\_TBMD. O comando ioctl OCS\_GET\_TBMD falhou no dispositivo de administração do OCS.

---

---

**ICA2123 Erro na conexão do TBM determinado pelo rlogin: número do erro.**

**Explicação:** Ocorreu erro ioctl() OCS\_IS\_TBM\_CONNECTED. O comando ioctl OCS\_IS\_TBM\_CONNECTED falhou no dispositivo de administração do OCS.

---

**ICA2124 Não há host conectado: número do erro.**

**Explicação:** Não há nós de host conectados a esse nó de OCS a partir da lista de nós de host possíveis.

---

**ICA2125 Erro na obtenção da lista para ODM (Gerenciador de Dados do Objeto):**  
*Atributo Customizado: número do erro odm.*

**Explicação:** Ocorreu erro de odm\_get\_list() para a classe de objeto ODM, CuAt(Customized Attribute).

---

**ICA2126 Não há nome de nó de host OCS associado a: nó do host para conexão.**

**Explicação:** A entrada CuAt(Customized Attribute) foi encontrada mas não foram encontradas correspondências nó do host/nó de ocs.

---

**ICA2127 Erro de malloc na matriz do Host.**

**Explicação:** Ocorreu um erro de malloc() quando o espaço era alocado dinamicamente para a matriz de nomes de host possíveis.

---

**ICA2128 O usuário (desconhecido) a partir do ip do cliente (local do cliente) tentou um comando 'comando inválido' antes da autenticação.**

**Explicação:** Um usuário tentou realizar ações antes de digitar nome e senha para autenticação - antes de fazer qualquer processamento o usuário precisa primeiro ser autenticado.

**Resposta do Usuário:** Faça o login com USUÁRIO e SENHA

---

**ICA2129 gethostbyname (nome de chamamento): número do erro**

**Explicação:** Erro do sistema quando ftpd tentou obter informações do host correspondentes ao nome do host.

---

**ICA2130 O usuário (nome do usuário) a partir do ip do cliente (local do cliente) tentou dar um comando 'comando inválido' .**

**Explicação:** O usuário especificado tentou dar um comando inválido.

**Resposta do Usuário:** Só os comandos USER, QUOTE SITE e QUIT são permitidos enquanto o "destino do local da citação" não for especificado.

---

**ICA2131 A autenticação falhou para o usuário "nome do usuário" a partir do ip do cliente devido a um erro no arquivo user.cfg.**

**Explicação:** A autenticação falhou devido a especificações do arquivo user.cfg definidas pelo administrador do Firewall (veja registros anteriores).

**Resposta do Usuário:** Entre em contato com o administrador do Firewall.

---

**ICA2132 O usuário 'usuário' a partir do ip do cliente (local do cliente) tentou dar um comando 'comando inválido' .**

**Explicação:** O usuário tentou usar um comando inválido. Os únicos comandos válidos nesse ponto são SITE,USER e QUIT.

---

**ICA2133 Erro: a chamada de função falhou na instância:linha, WSAGetLastError**

**Explicação:** Mensagem de erro geral; verifique os registros

---

**ICA2134 Aviso: ftpd: connect() (in instância) não conseguiu alcançar IP, WSAGetLastError.**

**Explicação:** Connect() não conseguiu encontrar o endereço solicitado; verifique o resultado de WSAGetLastError.

**Resposta do Usuário:** confira o endereço - pode haver erro de DNS ou de rede

---

**ICA2135 Transferência de dados concluída: Recebeu %1\$d bytes (do IP de origem); enviados bytes bytes (para IP de destino).**

**Explicação:** Essas informações refletem uma transferência de dados durante uma sessão ftp em particular. Õ No entanto, observe que a transferência de dados pode não ser concluída com sucesso Õ (verifique o log quanto a um rcv falho ou envie chamada).

---

**ICA2136 Erro: CreateThread() falhou na instância: número do erro.**

**Explicação:** ftpd não pôde criar uma cadeia

---

**ICA2137 Conexão de dados estabelecida; servidor: ip de origem cliente: ip de destino.**

**Explicação:** Conexão de dados bem sucedida.

---

**ICA2138 Memória insuficiente: pftpd: malloc(%1\$d) retornou NULL na função instância.**

**Explicação:** Não foi possível alocar memória suficiente - malloc retornou NULL.

---

**ICA2139 LogonUser() falhou: motivo.**

**Explicação:** O LogonUser da API (SAM) do Windows NT (para autenticação de senha) falhou devido ao(s) motivo(s) especificado(s).

**Resposta do Usuário:** Entre em contato com o administrador do Firewall.

---

**ICA2140 httpd --> Autenticação HTTP Proxy resultado para usuário <usuário>, no <ip de usuário>, via rede ... RC:<motivo>.**

**Explicação:** O HTTP Proxy tentou autenticação do usuário. O seu sucesso ou a sua falha é relatada aqui para o motivo especificado.

**Resposta do Usuário:** Entre em contato com o administrador do Firewall.

---

**ICA2141 A sessão de FTP com endereço de IP a partir de endereço de IP é encerrada.**

**Explicação:** A sessão ftp para o firewall é encerrada, independentemente do site citado para o destino.

---

**ICA2142 fw\_tn\_authenticate autenticou id do usuário com sucesso.**

**ICA2143 a autenticação fw\_tn\_authenticate de id do usuário falhou.**

**Explicação:** fw\_tn\_authenticate não pode autenticar a ID de usuário especificada.

**Ação do Sistema:** Login recusado.

**Resposta do Usuário:** Se fw\_tn\_authenticate tiver algum recurso de sistema de registro, o administrador n deve examinar o arquivo de log para determinar a causa.

---

**ICA2144 fw\_tn\_authenticate não retornou com sucesso.**

**Explicação:** O valor retornado por fw\_tn\_authenticate não é zero. A função n\_fw\_tn\_authenticate pode estar faltando.

**Ação do Sistema:** Login recusado.

**Resposta do Usuário:** Examine fw\_tn\_authenticate com cuidado para ver se ele chega a retornar n - valor diferente de zero - e corrija-o se isso ocorrer. Nesse caso, faça a biblioteca fwuser.o de novo e coloque-a no Firewall.

---

**ICA2145 O sistema retornou código de retorno rc no arquivo nome do arquivo na linha número da linha.**

**Explicação:** Falha em chamada do sistema. A biblioteca fwuser.o pode estar ausente.

**Ação do Sistema:** A autenticação foi abortada.

**Resposta do Usuário:** Confirme se /usr/lib/fwuser.o está presente. Se estiver, entre em contato com a IBM.

---

**ICA2146 A fwuser.o fornecida pela IBM não foi substituída.**

**Explicação:** A fwuser.o fornecida pela IBM está sendo usada porque ela não foi substituída por sua própria fwuser.o.

**Ação do Sistema:** A autenticação foi abortada.

**Resposta do Usuário:** Escreva e compile sua própria autenticação caso tenha definido algum usuário para usar a autenticação Fornecida pelo Usuário. A fwuser.o fornecida pela IBM nega acesso a todos os usuários não-AIX e não-Firewall.

---

**ICA2147 fwtnet: o usuário id de usuário iniciou sessão de telnet transparente a partir de end. IP de origem (local protegido) para end. IP de destino.**

**Explicação:** Mensagem gerada no início de cada sessão de proxy transparente (fwtnet). A sessão começa quando a id do usuário, o ip de origem e o ip de destino são todos conhecidos para o firewall. Só é permitida sessão iniciada a partir de local protegido.

**Ação do Sistema:** permita o telnet transparente.

---

**ICA2148 Atenção -- Foi feita uma tentativa de conexão não autorizada para o usuário id do usuário de end. IP de origem (local não-protegido) para end. IP de destino, que não é permitida.**

**Explicação:** Em geral indica tentativa de estabelecer conexão com o Firewall através de interface não-protegida.

**Ação do Sistema:** Rejeitar a conexão.

**Resposta do Usuário:** É preciso fazer o telnet a partir de local protegido usando proxy transparente.

---

**ICA2149 fwtnet: ocorreu um LOGIN\_ADAPTER\_ERROR no início da sessão de telnet transparente de end. IP de origem para end. IP de destino.**

**Explicação:** Ocorreu um LOGIN\_ADAPTER\_ERROR ao chamar q\_check\_secure(0).

**Ação do Sistema:** Rejeitar a conexão.

**Resposta do Usuário:** verifique o adaptador protegido.

---

**ICA2150 Erro pftpd - falha na função: código de retorno = 0xcódigo de retorno da função**

**Explicação:** O servidor pftpd detectou um erro na função indicada. O daemon é encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie o pftpd.

---

**ICA2151 Início de sessão recusado.**

**Explicação:** Esta mensagem deve ser exibida para o usuário que tenta efetuar login mas não obtém permissão.

---

**ICA2152 fwlogin: a gravação em dispositivo falhou.**

**Explicação:** Não é possível gravar no dispositivo.

---

**ICA2153 fwlogin: a leitura de dispositivo falhou.**

**Explicação:** Não é possível ler no dispositivo.

---

**ICA2154 erro em nome da porta com motivo.**

**Explicação:** Este Firewall encontrou um problema.

---

**ICA2155 Erro pftpd - falha na função: mensagem de erro do sistema**

**Explicação:** O servidor pftpd detectou um erro na função indicada. O daemon é encerrado.

**Resposta do Usuário:** Corrija o problema do sistema indicado e reinicie o pftpd.

---

**ICA2156 Atenção -- O usuário *id de usuário* que tentou usar ftp transparente do lado NONSECURE *end. IP de origem* para *end. IP de destino*, não tinha permissão.**

**Explicação:** Em geral indica tentativa de estabelecer conexão com o Firewall através de interface não-protegida.

**Ação do Sistema:** Rejeitar a conexão.

**Resposta do Usuário:** É preciso fazer o ftp a partir do lado protegido usando proxy transparente.

---

**ICA2157 O usuário *id do usuário de end. IP de origem* não tem permissão para usar proxy transparente para *end. IP de destino*.**

**Explicação:** Em geral indica tentativa de estabelecer conexão com o Firewall enquanto o proxy transparente não está configurado.

**Ação do Sistema:** Rejeitar a conexão.

**Resposta do Usuário:** deixe fwtp proxy ftp = on (ligado)

---

**ICA2158 Opção *valor* foi indevidamente especificado.**

**Explicação:** O sinalizador indicado foi especificado incorretamente.

---

**ICA2159 Valor de timeout não especificado para a opção -t.**

**Explicação:** É preciso fornecer um valor de timeout para a opção -t.

---

---

**ICA2160 A senha mudou para o usuário** *ID do usuário da rede :nome do host.*

**Explicação:** Um usuário do FTP mudou com sucesso sua senha no banco de dados de senhas.

**Ação do Sistema:** Nenhuma

**Resposta do Usuário:** Nenhuma

---

**ICA2161 O usuário** *ID do usuário* **tentou efetuar login usando senha vencida a partir da rede** *:nome do host.*

**Explicação:** Um usuário do FTP tentou estabelecer conexão com o Firewall usando senha vencida.

**Ação do Sistema:** A validação de login do FTP falha e o usuário é retornado para a shell de comandos do FTP.

**Resposta do Usuário:** O usuário deve tentar fazer a validação de novo por meio do comando FTP USER ou restabelecendo a conexão FTP e passando a cadeia da senha sob a forma "old\_password/new\_password/new\_password".

---

**ICA2162 Falha da mudança da senha para o usuário** *ID do usuário a partir da rede :nome do host.*

**Explicação:** Um usuário FTP tentou mudar sua senha e a rotina de validação da senha falhou. As razões possíveis para a falha incluem: - Senha "antiga" incorreta foi especificada, - Apenas uma ocorrência de senha "nova" foi especificada, - Duas ocorrências de senha "nova" não correspondem, ou - Delimitador usado para separar senhas não foi "/".

**Ação do Sistema:** A validação da senha FTP falha e o usuário é retornado para a shell do comando FTP.

**Resposta do Usuário:** Tente revalidar com o servidor FTP, verificando as senhas que estão sendo inseridas corretamente. Se o problema persistir, contate o representante de serviços.

---

**ICA2163 safemaidl iniciado.**

**Explicação:** Iniciando safemaidl.

---

**ICA2164 safemaidl encerrado.**

**Explicação:** encerrando safemaidl.

---

**ICA2165 Sessão de telnet interrompida.**

**Explicação:** A sessão de telnet está sendo encerrada, mas não consegue recuperar do canal as informações da sessão. A sessão foi provavelmente interrompida durante a inicialização pelo cliente, o que impediu que ela fosse totalmente inicializada.

---

**ICA2166 Não pôde recuperar o atributo** *atributo para usuário id de usuário. Código de retorno = código de retorno.*

**Explicação:** O serviço de autenticação não pôde recuperar o atributo especificado do banco de dados do usuário para o usuário especificado. Ação do Sistema : Falha na autenticação do usuário.

**Resposta do Usuário:** Contate o administrador do sistema para corrigir a gravação do banco de dados do usuário.

---

**ICA2167** A autenticação da *id de usuário* falhou para *serviço* usando o *esquema de autenticação do endereço de cliente no tipo de rede*

**Explicação:** O usuário especificado falhou em ser autenticado para o serviço especificado com a utilização do método de autenticação especificado. O usuário estava solicitando o serviço a partir do endereço e tipo de rede indicados. Ação do Sistema : Falha na autenticação do usuário.

**Resposta do Usuário:** Contate o administrador do sistema.

---

**ICA2168** A autenticação da *id do usuário* falhou para *serviço* devido à *insuficiência de memória*.

**Explicação:** A ID de usuário não pôde ser autenticada para o serviço porque houve uma falha de alocação de memória durante o processo de autenticação. Ação do Sistema : Falha na autenticação do usuário.

**Resposta do Usuário:** Contate o administrador do sistema.

---

**ICA2169** Usuário *nome* autenticado com sucesso para *serviço* usando *método da rede:nome do host*.

**Explicação:** O FW autenticou o nome de usuário indicado para o serviço solicitado usando o esquema de autenticação especificado.

---

**ICA2170** A autenticação da *id de usuário* falhou para *serviço*. O *método de autenticação não está registrado junto ao Firewall*.

**Explicação:** A ID de usuário não pôde ser autenticada para serviço. O método de autenticação solicitado não está registrado junto ao Firewall. Ação do Sistema : Falha na autenticação do usuário.

**Resposta do Usuário:** Contate o administrador do sistema.

---

**ICA2171** A conta *nome do usuário* foi bloqueada devido a uma *senha vencida*.

**Explicação:** A senha venceu e não foi alterada. Esta conta foi bloqueada.

**Ação do Sistema:** A conta está bloqueada e as autenticações da senha do Firewall falharão. UserRes

---

**ICA2172** A conta *nome do usuário* está bloqueada.

**Explicação:** Esta conta foi bloqueada.

**Ação do Sistema:** A conta está bloqueada. As autenticações de senha do Firewall falharão.

**Resposta do Usuário:** Fale com o administrador do Firewall para desbloquear a conta.

---

**ICA2173** Usuário tentou iniciar sessão usando nome de usuário *id de usuário reservado*.

**Explicação:** A ID fornecida pelo usuário está reservada ao uso pelo firewall.

**Ação do Sistema:** Login recusado.

**Resposta do Usuário:** O administrador deve investigar quem está usando este nome de usuário.

---

**ICA2174**    **A autenticação da *id de usuário* falhou para *serviço usando o esquema de autenticação de endereço de cliente em tipo de rede* devido a um erro de processamento interno.**

**Explicação:** O usuário especificado falhou em ser autenticado para o serviço especificado com a utilização do método de autenticação especificado. O usuário estava solicitando o serviço a partir do endereço e tipo de rede indicados. A solicitação de autenticação falhou devido a um erro interno de processamento. Ação do Sistema : Falha na autenticação do usuário.

**Resposta do Usuário:** Contate o administrador do sistema.

---

**ICA2175**    **A chamada Windows NT LogonUser falhou para usuário *nome de usuário*. O último erro foi *último erro*.**

**Explicação:** O nome de usuário especificado falhou em ser autenticado pela chamada Windows NT LogonUser API. O Windows NT relatou o último erro depois que o LogonUser falhou. Ação do Sistema : Falha na autenticação do usuário.

**Resposta do Usuário:** Contate o administrador do sistema.

---

**ICA2176**    **Esquema de autenticação *esquema de autenticação desconhecido* foi definido para *nome de usuário utilizando componente da rede*.**

**Explicação:** O esquema de autenticação especificado foi definido para o usuário especificado quando o componente do firewall especificado estava sendo usado a partir da rede especificada, mas o esquema de autenticação não está registrado atualmente junto ao firewall. Ação do Sistema : Falha na solicitação de autenticação do usuário.

**Resposta do Usuário:** Contate o administrador do sistema.

---

**ICA2177**    **Conexão SafeMail *0xID da sessão recebida do nome do par do soquete*.**

**Explicação:** SafeMail recebeu uma conexão inbound do *Nome do par relacionado*. O número de ID da conexão indicada foi *Atribuído* para rastreamento. (Depurar nível)

**Ação do Sistema:** Uma cadeia foi despachada para manipular esta *Conexão*.

---

**ICA2178**    **A sessão do SafeMail *0xID de sessão* foi estabelecida do endereço IP do remetente para o endereço IP do destinatário.**

**Explicação:** O SafeMail estabeleceu contato com o servidor de correspondência do destinatário *Se* está pronto para transferir a correspondência. (Nível info)

**Ação do Sistema:** A transferência de dados está para começar.

---

**ICA2179**    **O SafeMail avançou *tamanho da mensagem bytes* para a conexão *0xID da sessão do endereço do servidor que envia para o endereço do servidor que recebe*.**

**Explicação:** O SafeMail avançou uma mensagem com sucesso entre os *Dois* servidores de correspondência relacionados. Esta sessão foi anteriormente identificada em *Uma* mensagem ICA2166. Esta mensagem continha o número de bytes *indicado*. (Nível info)

---

**ICA2180**    **O SafeMail encerrou a sessão *0xID da Sessão do endereço do remetente*.**

**Explicação:** O SafeMail recusou transferir a correspondência que está sendo enviada na *Sessão* indicada. (Nível info)

**Ação do Sistema:** A sessão foi encerrada.

**Resposta do Usuário:** Aumente o nível de prioridade dos registros para obter *Informações de diagnóstico* mais detalhadas.

---

**ICA2181 O SafeMail encerrou a sessão 0xID da Sessão para o código de razão código de razão.**

**Explicação:** O processador principal do SafeMail encerrou a sessão indicada porque foi detectada uma condição de erro primário. Os códigos de razão incluem: 001 - impossível localizar o servidor de correspondência do destinatário 002 - remetente tentou rotear a correspondência entre dois servidores não-protegidos 003 - servidor de correspondência do destinatário rejeitou a conexão, pode estar inativo 004 - servidor de correspondência do destinatário recusou-se a aceitar a correspondência 005 - uma ou mais conexões expiraram; o servidor de correspondência do remetente ou o do destinatário pode estar inativo 006 - recv() retornou 0 bytes; o servidor de correspondência do remetente ou do destinatário pode estar inativo 007 - recv() retornou negativo; o servidor de correspondência do remetente ou do destinatário pode estar inativo 008 - muitos comandos de erro foram recebidos 009 - select() retorna negativo; o servidor de correspondência do destinatário ou do remetente pode estar inativo 00Esta mensagem esta registrada no nível de Depuração.

**Ação do Sistema:** A conexão foi encerrada.

---

**ICA2182 O SafeMail rejeitou a sessão 0xID de Sessão devido a um comando comando SMTP inválido, código de motivo código de motivo.**

**Explicação:** A sub-rotina de validação de comandos do SafeMail detectou um comando válido ou perigoso. Esses códigos de motivo variam para cada comando SMTP. Consulte a página da web de Suporte ao IBM Firewall quanto aos valores atuais. (Depurar nível)

**Ação do Sistema:** A conexão foi encerrada.

**Resposta do Usuário:** Corrija o cliente que está enviando a correspondência garantindo a segurança e a validade das informações que estiverem sendo enviadas.

---

**ICA2183 httpd --> arquivo de Configuração HTTP Proxy (nome de arquivo) não está disponível.**

**Explicação:** O daemon HTTP proxy tentou abrir o arquivo de configuração especificado mas ele não existe ou não pôde ser aberto.

**Ação do Sistema:** HTTP Proxy não inicia

**Resposta do Usuário:** Configure o proxy via o GUI ou o comando fwhttp e reinicie o proxy.

---

**ICA2184 Erro signal() com sinal Número de sinal. Saída de safemaid.**

**Explicação:** Erro do sistema quando o safemaid daemon tentou estabelecer um manipulador de sinais.

---

**ICA2185 Não é possível abrir soquete. saída de safemaid**

**Explicação:** Falha durante a abertura do soquete.

---

**ICA2186 Não é possível ligar o soquete na porta. saída de safemaid**

**Explicação:** Falha ao ligar o soquete na porta.

---

**ICA2187 Impossível aceitar nova conexão. Nova tentativa do safemaid.**

**Explicação:** Falha ao aceitar a nova conexão.

---

**ICA2188 Horário incorreto (valor) especificado para -l.**

**Explicação:** O valor do horário mostrado contém caracteres fora do intervalo numérico de 0..9 ou excede o valor máximo permitido.

---

**ICA2189** Valor de timeout não especificado para a opção -l.

**Explicação:** É preciso fornecer um valor de timeout para a opção -l.

---

**ICA2200** (serviço:função) erro de inicialização do WinSocket : WSAGetLastError

**Explicação:** Ocorreu erro durante a inicialização do WinSocket.

**Resposta do Usuário:** Corrija o problema do sistema indicado por WSAGetLastError e reinicie o serviço indicado (Primeiro Parâmetro).

---

**ICA2201** (serviço:chamando função) função falha falha na linha número da linha : WSAGetLastError

**Explicação:** O componente da rede especificado falhou

**Resposta do Usuário:** Corrija o problema do sistema indicado por WSAGetLastError e reinicie o serviço indicado (Primeiro Parâmetro).

---

**ICA2202** (serviço:chamando função) timeout tempo vencido após WSAGetLastError segundos :

**Explicação:** A função indicada teve o seu tempo de espera vencido depois de permanecer inativa pelo tempo especificado.

**Resposta do Usuário:** Reconectado ao serviço indicado e respondido antes do timeout indicado

---

**ICA2203** (serviço:chamando função) Erro de memória; função falha retornou valor de retorno na linha número da linha: WSAGetLastError

**Explicação:** Ocorreu erro de memória, normalmente estouro de memória; verifique WSAGetLastError

**Resposta do Usuário:** Libere espaço em disco - consulte o Administrador do Sistema

---

**ICA2204** (serviço:chamando função) Erro de nome de arquivo: acesso negado ou falha na criação.

**Explicação:** O serviço indicado encontrou um erro ao tentar acessar ou criar o arquivo especificado ou o arquivo associado ao parâmetro de arquivo.

**Resposta do Usuário:** Certifique-se de que o nome de arquivo indicado exista e de que possua as permissões corretas.

---

**ICA2205** (serviço:chamando função) O arquivo nome de arquivo é necessário mas não pôde ser encontrado.

**Explicação:** O arquivo especificado não existe. A causa mais provável da falha é que a configuração padrão do Firewall tenha sido apagada. Restaure o arquivo a partir de uma cópia de segurança atual.

**Resposta do Usuário:** Verifique a existência do arquivo de configuração. O programa de configuração espera que este arquivo exista. Se uma versão da cópia de segurança não estiver disponível, contate o representante de serviços.

---

**ICA2206** (serviço:chamando função) O arquivo de configuração nome de arquivo está corrompido.

**Explicação:** O arquivo de configuração indicado não se encontra num formato utilizável. O conteúdo tornou-se corrompido. A causa mais provável da corrupção é que o arquivo tenha sido editado manualmente e nele tenha sido incluído dados inválidos.

**Resposta do Usuário:** O arquivo de configuração precisará ser recriado corretamente. Primeiro dê um cat no arquivo (ou faça uma cópia visível dele) e depois apague o arquivo

original. Reconfigure o arquivo usando o comando de configuração do firewall, e tomando como referência o arquivo original.

---

**ICA2207** (serviço: chamando função) **O arquivo de configuração nome de arquivo está vazio.**

**Explicação:** O arquivo de configuração indicado não foi encontrado ou o arquivo foi encontrado mas estava vazio. A causa mais provável para o arquivo não estar sendo encontrado é que a configuração para o serviço indicado não tenha sido executada.

**Resposta do Usuário:** Verifique o estado do arquivo de configuração. Se o arquivo existir, o comando de configuração espera que este arquivo contenha dados. Consulte o manual para obter mais informações.

---

**ICA2208** serviço **A sessão id de sessão foi iniciada para id de usuário a partir de um adaptador não-protégido (endereço IP de origem: endereço IP de destino).**

**Explicação:** A mensagem gerada no começo de cada sessão indicada.

---

**ICA2209** serviço **A sessão id da sessão foi encerrada para id de usuário a partir de um adaptador não-protégido (endereço IP de origem: endereço IP de destino); bytes total de bytes.**

**Explicação:** Mensagem gerada no fim de cada sessão indicada. Total de Bytes indica o número de bytes transferidos durante a sessão. Os serviços (i.e., ptnetd) que não suportam o Total de Bytes indicarão zero.

---

**ICA2210** (serviço) **O usuário id de usuário tentou iniciar sessão usando uma senha vencida a partir de endereço IP de origem (não-protégido).**

**Explicação:** O usuário indicado tentou estabelecer uma conexão com o Firewall usando a senha vencida indicada a partir do IP de origem indicado num adaptador não-protégido.

**Resposta do Usuário:** A senha dada venceu devido à definição de regras para senha. Contate o admin do sistema.

---

**ICA2211** (serviço) **O usuário id de usuário tentou iniciar sessão usando senha vencida a partir do endereço IP de origem (protégido).**

**Explicação:** O usuário indicado tentou estabelecer uma conexão com o Firewall usando a senha vencida indicada a partir do IP de origem indicado num adaptador protégido.

**Resposta do Usuário:** A senha dada venceu devido à definição de regras para senha. Contate o admin do sistema.

---

**ICA2212** (serviço) **O usuário nome foi autenticado com sucesso do endereço IP de origem (protégido).**

**Explicação:** O FW autenticou o nome de usuário indicado a partir do IP de origem indicado num adaptador protégido.

---

**ICA2213** (serviço) **O usuário nome foi autenticado com sucesso a partir de endereço IP de origem (não-protégido).**

**Explicação:** O FW autenticou o nome de usuário indicado a partir do IP de origem indicado num adaptador não-protégido.

---

**ICA2214** (serviço) O usuário *nome* falhou na autenticação a partir de *endereço IP de origem* (não-protégido).

**Explicação:** O FW falhou na autenticação para o nome de usuário indicado a partir do IP de origem indicado num adaptador não-protégido.

**Resposta do Usuário:** A causa mais provável foi a digitação incorreta do nome de usuário ou da senha. Nomes de usuário e senhas consideram maiúsculas e minúsculas (verificar Caps Lock).

---

**ICA2215** (serviço) O usuário *nome* falhou na autenticação a partir de *endereço IP de origem* (protégido).

**Explicação:** O FW falhou na autenticação para o nome de usuário indicado a partir do IP de origem indicado num adaptador protégido.

**Resposta do Usuário:** A causa mais provável foi a digitação incorreta do nome de usuário ou da senha. Nomes de usuário e senhas consideram maiúsculas e minúsculas (verificar Caps Lock).

---

**ICA2216** (serviço) O usuário *nome* a partir de *endereço IP de origem* (não-protégido) não forneceu senhas correspondentes (para verificação).

**Explicação:** Uma alteração de senha foi solicitada ou exigida e o usuário indicado a partir do IP de origem indicado num adaptador não-protégido forneceu senhas que não eram correspondentes. Os dados de autenticação do usuário não foram alterados.

**Resposta do Usuário:** A alteração de senhas requer a digitação da senha duas vezes, a segunda vez para verificação. A causa mais provável foi a digitação incorreta de uma senha de verificação.

---

**ICA2217** (serviço) O usuário *nome* a partir de *endereço IP de origem* (protégido) não forneceu senhas (de verificação) correspondentes.

**Explicação:** Uma alteração de senha foi solicitada ou exigida e o usuário indicado a partir do IP de origem indicado num adaptador protégido forneceu senhas que não eram correspondentes. Os dados de autenticação do usuário não foram alterados.

**Resposta do Usuário:** A alteração de senhas requer a digitação da senha duas vezes, a segunda vez para verificação. A causa mais provável foi a digitação incorreta de uma senha de verificação.

---

**ICA2218** serviço A sessão *id de sessão* iniciada para *id de usuário* a partir de um adaptador protégido (*end. IP de origem: end. IP de destino*).

**Explicação:** A mensagem gerada no começo de cada sessão indicada.

---

**ICA2219** serviço A sessão *id de sessão* foi encerrada para *id de usuário* a partir de um adaptador protégido (*end. IP de origem: end. IP de destino*); bytes *Total de Bytes*.

**Explicação:** Mensagem gerada no fim de cada sessão indicada. Total de Bytes indica o número de bytes transferidos durante a sessão. Os serviços (i.e., ptnetd) que não suportam o Total de Bytes indicarão zero.

---

**ICA2220** (serviço) O usuário *id de usuário* iniciou uma sessão de proxy transparente a partir de *end. IP de origem* (lado protégido) para *end. IP de destino*.

**Explicação:** Mensagem gerada no início de cada sessão de proxy transparente. Uma sessão começa quando a *id de usuário*, o *ip de origem* e o *ip de destino* são todos conhecidos do firewall. Só é permitida sessão iniciada a partir de local protégido.

**Ação do Sistema:** permite o proxy transparente.

---

**ICA2221** (serviço) **Advertência: O IP (Ender IP de controle) no ponto final da Linha de controle não era igual ao IP (Ender IP de dados) no ponto final da Linha de dados.**

**Explicação:** Para a segurança proposta (i.e., anti-sequestro), certifique-se de que o Endereço IP do ponto a que o soquete de Conexão de Controle está conectado é o mesmo que o IP do ponto a que o soquete de Conexão de Dados está conectado. Eles podem ser diferentes se estiver sendo usado o Net Dispatcher ou se o destino tiver usado vários adaptadores

**Ação do Sistema:** Verifique se o Servidor FTP de Destino está usando vários adaptadores ou se o Net Dispatcher está sendo usado. Certifique-se de que os filtros permitem apenas endereços IP válidos através da porta 20 e da porta 21.

---

**ICA2222** (serviço) **Advertência! Violação do protocolo. Recebido comando compatível com não-RFC cadeia inválida; Esperado cadeia de protocolo.**

**Explicação:** O serviço indicado recebeu uma cadeia inesperada e não compatível com o RFC associado; possível hacker.

**Ação do Sistema:** Use um Cliente compatível com o RFC para o serviço indicado

---

**ICA3001** **\*Alerta\*: o usuário real é o nome de usuário ident, e não o nome de usuário da conexão de soquetes**

**Explicação:** Possível tentativa de quebra de segurança, nome de usuário não autenticado.

---

**ICA3006** *número bytes do cliente, número bytes do servidor*

**Explicação:** Mensagem indicando o número de bytes transferidos entre o daemon sockd e seus respectivos hosts cliente e servidor.

---

**ICA3007** **Uma conexão foi recusada devido ao excedente na contagem máxima de conexões.**

**Explicação:** O servidor de soquetes está configurado para aceitar somente um determinado número máximo de sessões cliente. Esta mensagem é gerada quando o limite já tiver sido alcançado e chegam pedidos adicionais de conexão.

**Ação do Sistema:** A conexão recém tentada está fechada.

**Resposta do Usuário:** O número máximo de conexões simultâneas é determinado pelo parâmetro SOCKS5\_MAXCHILD no socks5.conf. Aumente esta definição e atualize o servidor. Consulte a referência do IBM Firewall para obter detalhes. start unused

---

**ICA3010** **conectado -- Bind do usuário(usuário real)\$end. src para end. dst ( porta de destino)**

**Explicação:** Conexão estabelecida.

---

**ICA3011** **conectado -- Conexão entre usuário(usuário real)\$end. src e end. dst ( aplicação)**

**Explicação:** Conexão do soquete com o mundo externo bem sucedida.

---

**ICA3012** **recusado -- Conexão de user(real\_user)\$src\_addr com dst\_addr (aplicação)**

**Explicação:** O host remoto recusou a conexão.

---

**ICA3013** **select() número do erro**

**Explicação:** Erro de sistema.

---

**ICA3014 encerrado -- Bind de *user*(usuário real)\$end. src para end. dst (porta de destino).(conta bytes de cliente, conta bytes de servidor)**

**Explicação:** Conexão encerrada.

---

**ICA3015 encerrada -- Conexão de *usuário*(usuário real)\$end. src para end. dst ( host de destino).(número bytes do cliente, número bytes do servidor)**

**Explicação:** Conexão com o servidor encerrada.

---

**ICA3016 \*\*\*Impossível encontrar interface adequada para comunicar-se com o *host de destino***

**Explicação:** O arquivo /etc/sockd.route não contém informações de roteamento para o host de destino especificado.

---

**ICA3017 O comando da shell não pode ser executada para o *pid processo sockd***

**Explicação:** O daemon sockd não consegue executar o comando /bin/sh.

**Resposta do Usuário:** Verifique se a shell de /bin/sh está disponível no sistema.

---

**ICA3018 recusada -- Bind de *usuário*(usuário real)\$end. src para end. dst**

**Explicação:** O host remoto recusou a conexão.

---

**ICA3019 Erro no GetDst() a partir do *host nome de soquete src: número do erro***

**Explicação:** Erro na resolução do endereço de destino para a conexão solicitada.

---

**ICA3022 Inválido != campo na linha *número da linha***

**Explicação:** Entrada inválida encontrada no arquivo /etc/sockd.conf.

---

**ICA3023 Comparação inválida na linha *número da linha***

**Explicação:** Entrada inválida encontrada no arquivo /etc/sockd.conf.

---

**ICA3024 Entrada inválida na linha *número da linha***

**Explicação:** Entrada inválida encontrada no arquivo /etc/sockd.route.

---

**ICA3025 Permissão inválida/negar campo na linha *número da linha***

**Explicação:** Entrada inválida encontrada no arquivo /etc/sockd.conf.

---

**ICA3026 Número de porta inválido na linha *número da linha***

**Explicação:** Entrada inválida encontrada no arquivo /etc/sockd.conf.

---

**ICA3027 O Comando da Shell Falhou (*status de execução*) para *Ö"cmdÖ"***

**Explicação:** O comando da shell exibido falhou.

**Resposta do Usuário:** Verifique se o processador da shell está disponível no sistema.

---

**ICA3030 O arquivo de config não pode ser aberto (*/etc/sockd.conf*)**

**Explicação:** O pedido de abertura contra o arquivo indicado falhou.

---

---

**ICA3031** O arquivo de roteamento não pôde ser aberto (*/etc/sockd.route*): número do erro

**Explicação:** O pedido de abertura contra o arquivo indicado falhou.

**Resposta do Usuário:** Entre em contato com o administrador do Firewall. Foi fornecido um arquivo padrão durante a instalação do Firewall.

---

**ICA3032** O arquivo de usuários não pôde ser aberto (*nome do arquivo de usuários*): número do erro

**Explicação:** O nome de arquivo especificado para a \*=lista de usuários em regra de permissão não foi encontrado.

---

**ICA3033** Resultado inesperado de Validate()

**Explicação:** Verificação de Identd do nome de usuário foi especificada, Identd respondeu com resultado inesperado.

---

**ICA3035** Não é possível fazer a conexão com identd no *host do cliente*

**Explicação:** Verificação de Identd do nome de usuário foi especificada, Identd não responde.

---

**ICA3039** Erro -- o comando da shell *Ö"cmdÖ"* não contém caracteres alfanuméricos.

**Explicação:** Comando de shell inválido, consulte mensagem de log.

---

**ICA3040** Erro -- *shell\_cmd fork()* número do erro

**Explicação:** Sockd daemon incapaz de alternar para o processo filho via 'fork()'

---

**ICA3041** Erro -- o endereço do cliente não foi obtido.

**Explicação:** Retorno de erro da chamada 'getpeername()'.  
**Resposta do Usuário:** Verifique o roteamento e a configuração do DNS.

---

**ICA3042** Erro -- comando indefinido (*0xcomando hex recebido*) do *host endereço do cliente*

**Explicação:** Recebido comando inválido da aplicação cliente.

**Resposta do Usuário:** Possível problema de configuração do cliente, ou desacordo entre o cliente e o nível de suporte do Firewall.

---

**ICA3043** Erro -- versão errada (*0xn da versão hex*) do *endereço de cliente do host*.

**Explicação:** O Firewall suporta soquetes versão 4.2.

**Resposta do Usuário:** Possível problema de configuração do cliente, ou desacordo entre o cliente e o nível de suporte do Firewall.

---

**ICA3044** Falha -- Conexão entre *usuário(usuário real)send. src e end. dst ( aplicação)*.  
**Código de erro:** comando causando falha número do erro.

**Explicação:** O pedido de conexão falhou.

---

**ICA3045** Falhou -- Bind de *usuário(usuário real)send. src para end. dst*. Erro: conectado ao host errado *nome dst (porta dst (aplicação))*.

**Explicação:** O pedido de bind falhou.

---

---

**ICA3046 Falhou -- Bind de usuário(usuário real)§end. src para end. dst. Código de erro: comando causando falha número do erro.**

**Explicação:** O pedido de bind falhou.

---

**ICA3047 Tempo esgotado -- Bind de usuário(usuário real)§end. srcend. dst**

**Explicação:** O tempo da conexão se esgotou.

---

**ICA3048 Comando de shell muito longo: comando...**

**Explicação:** O comando a ser executado, do arquivo /etc/sockd.conf, é grande demais.

---

**ICA3049 Tempo esgotado -- Conexão entre usuário(usuário real)§ end. src e end. dst ( aplicação)**

**Explicação:** O tempo da conexão se esgotou.

---

**ICA3050 regra de filtro do sockd.conf correspondente**

**Explicação:** Regra de filtro do arquivo /etc/sockd.conf que correspondeu à conexão do soquete.

---

**ICA3051 O sockd\_route() do AIX não conseguiu encontrar interface para endereço remoto.**

**Explicação:** Não foi possível encontrar as informações de roteamento da interface.

---

**ICA3052 Erro na definição da id de usuário para "ninguém".**

**Explicação:** Não foi possível definir a id de usuário do processo sockd filho para "ninguém".

---

**ICA3053 Erro em popen(script de rota do AIX): mensagem de erro de sistema**

**Explicação:** Falha na execução do script para procurar as informações de roteamento.

---

**ICA3054 Falha fatal de alocação de memória no sockd\_route() do AIX.**

**Explicação:** Falha de alocação de memória tentando coletar informações de roteamento.

---

**ICA3055 Erro fatal quando sockd\_route() do AIX analisava primeiro espaço em: linha de entrada**

**Explicação:** Erro na análise das informações de roteamento do sistema.

---

**ICA3056 Erro fatal quando sockd\_route() do AIX analisava segundo espaço em: linha de entrada**

**Explicação:** Erro na análise das informações de roteamento do sistema.

---

**ICA3057 Erro fatal quando sockd\_route() do AIX lia saída do script de roteamento: mensagem de erro do sistema**

**Explicação:** Erro na leitura da saída do script.

---

**ICA3058 Erro em popen(script do adaptador do AIX): mensagem de erro do sistema**

**Explicação:** Falha na execução do script para procurar as informações da interface.

---

---

**ICA3101 Erro do sockd no envio de dados - select():** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) Erro durante o envio de dados.

---

**ICA3102 Erro do sockd no envio de dados - write():** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) Erro durante o envio de dados.

---

**ICA3103 Erro do sockd no recebimento de dados - select():** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) Erro durante o recebimento de dados.

---

**ICA3104 Erro do sockd no recebimento de dados - read():** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) Erro durante o recebimento de dados.

---

**ICA3105 Não foi possível criar o arquivo de id de processo** *nome do arquivo.*

**Explicação:** (SOCKS422) A criação/gravação no arquivo de id de processo falhou.

---

**ICA3106 Sockd falhou ao bifurcar filho:** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) A tentativa de bifurcar filho para manipular pedido de SOCKS falhou.

---

**ICA3107 A opção de definir soquete de chegada SO\_LINGER falhou:** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) não crítico

---

**ICA3108 A opção de definir soquete de chegada SO\_LINGER falhou:** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) não crítico

---

**ICA3109 Entrada inválida na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3110 Campo de interface ilegal na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3111 IP de destino ilegal na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3112 Máscara de destino ilegal na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3113 Analisadas** *número de linhas no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

---

**ICA3114 Não foram encontradas linhas válidas no arquivo** *nome do arquivo.*

**Explicação:** (SOCKS422) Arquivo de configuração vazio ou sintaxe incorreta.

**Resposta do Usuário:** Corrija o arquivo de configuração indicado.

---

**ICA3115 Campo 'permitir/negar' inválido na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3116 Campo inválido '?=' na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3117 IP de origem ilegal na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3118 Máscara de origem ilegal na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3119 Comparação inválida na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3120 Número de porta inválido na linha** *número da linha no arquivo nome do arquivo.*

**Explicação:** (SOCKS422) Sintaxe incorreta da entrada de configuração.

---

**ICA3121 Recebido SIGUSR1 - configuração dos soquetes de descarga.**

**Explicação:** (SOCKS422) Sinal para descarregar configuração ativa no arquivo de log depois desta mensagem.

---

**ICA3122 O sockd não conseguiu bifurcar o daemon:** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) A bifurcação para inicializar daemon do sockd falhou.

**Resposta do Usuário:** Corrija o problema de sistema indicado e reinicie o sockd.

---

**ICA3123 Servidor do sockd sendo iniciado.**

**Explicação:** (SOCKS422) O sockd foi iniciado com sucesso e está aguardando conexões.

---

**ICA3124 Erro fatal de inicialização do sockd - bind():** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) A inicialização do servidor do sockd falhou, daemon encerrado.

**Resposta do Usuário:** Corrija o problema de sistema indicado e reinicie o sockd.

---

**ICA3125 Erro fatal de inicialização do sockd - listen():** *mensagem de erro do sistema*

**Explicação:** (SOCKS422) A inicialização do servidor do sockd falhou, daemon encerrado.

**Resposta do Usuário:** Corrija o problema de sistema indicado e reinicie o sockd.

---

---

**ICA3126 Erro fatal do sockd - main accept(): mensagem de erro do sistema**

**Explicação:** (SOCKS422) A rotina principal do servidor de sockd falhou, daemon encerrado.

**Resposta do Usuário:** Corrija o problema de sistema indicado e reinicie o sockd.

---

**ICA3127 O servidor do sockd recebeu sinal de encerramento.**

**Explicação:** root ou ninguém matou o processo, daemon encerrado.

**Resposta do Usuário:** Reinicie o sockd se o administrador assim o desejar (digite "sockd").

---

**ICA3128 Erro fatal de inicialização do sockd - socket(): mensagem de erro do sistema**

**Explicação:** A inicialização do servidor do sockd falhou; o daemon foi encerrado.

**Resposta do Usuário:** Corrija o problema de sistema indicado e reinicie o sockd.

---

**ICA3129 Erro fatal de inicialização do sockd - função que falhou: mensagem de erro do sistema**

**Explicação:** A inicialização do servidor do sockd falhou na função indicada, daemon encerrado.

**Resposta do Usuário:** Corrija o problema de sistema indicado e reinicie o sockd.

---

**ICA3130 Erro do sockd - função falhou: mensagem de erro do sistema**

**Explicação:** O servidor do sockd detectou um erro na função indicada. O daemon continua, mas as conexões podem ser recusadas ou encerradas.

**Resposta do Usuário:** Se o problema persistir, pare o sockd, corrija o problema de sistema indicado e reinicie o sockd.

---

**ICA3131 Erro na leitura do nome do arquivo. Dados colocados na cache anteriormente serão utilizados.**

**Explicação:** O arquivo não pôde ser lido ou continha dados incorretos. Alguma mensagem anterior deve descrever o problema. O sockd vai continuar a operar com dados de cache da versão anterior do arquivo.

**Resposta do Usuário:** Corrija o erro no arquivo indicado.

---

**ICA3132 Sinalizador desconhecido -valor.**

**Explicação:** O sinalizador indicado não é reconhecido; daemon encerrado.

**Resposta do Usuário:** Corrija a sintaxe e reinicie o sockd.

---

**ICA3133 Parâmetro desconhecido valor.**

**Explicação:** O parâmetro indicado não é reconhecido; daemon encerrado.

**Resposta do Usuário:** Corrija a sintaxe e reinicie o sockd.

---

**ICA3134 Opções conflitantes opção1 e opção2.**

**Explicação:** As opções indicadas não podem ser especificadas juntas; daemon encerrado.

**Resposta do Usuário:** Corrija a sintaxe e reinicie o sockd.

---

---

**ICA3135 Erro do sockd error - falha de função: código de retorno = 0xcódigo de retorno da função**

**Explicação:** O servidor do sockd detectou um erro na função indicada. O daemon é encerrado.

**Resposta do Usuário:** Corrija o problema de sistema indicado e reinicie o sockd.

---

**ICA3700 Erro de inicialização do WinSocket : %1\$d**

**Explicação:** Ocorreu erro durante a inicialização do WinSocket.

**Resposta do Usuário:** Corrija o problema de sistema indicado e reinicie o sockd.

---

**ICA4000 programa - Advertência: Recebido sinal *sinal*, encerrando ...**

**Explicação:** Encerramento devido a recebimento de sinal.

---

**ICA4001 PARE o programa como PID *Id do processo***

**Explicação:** Imprime o final da conclusão do daemon. Mensagem informativa.

---

**ICA4002 ID temporária**

**Explicação:** Mensagem informativa.

---

**ICA4003 Problema com processo filho *Id do processo*.**

**Explicação:** Não foi possível criar processo filho.

---

**ICA4004 Erro Fatal. Cancelando fwpagerd no sinal *sinal*.**

**Explicação:** Manipulador do sinal.

---

**ICA4005 Não há daemon fwpagerd em execução, programa não encontrado.**

**Explicação:** Não pôde enviar uma página porque o daemon não estava ativo.

---

**ICA4006 Nenhum fwpagerd daemon está sendo executado com a id do processo *Id do processo*.**

**Explicação:** Não foi possível encontrar a ID de processo do daemon.

---

**ICA4007 INICIE o programa como PID *ID do processo***

**Explicação:** Imprima informações de início. Mensagem informativa.

---

**ICA4008 Não foi possível definir sigignore para SIGPIPE.**

**Explicação:** Falha durante a configuração para ignorar sinal de canal danificado.

---

**ICA4009 Não foi possível definir sigset para SIGCHILD.**

**Explicação:** Falha na configuração para captar sinal filho morrendo.

---

**ICA4010 Não é possível definir processo de encerramento.**

**Explicação:** Falha durante a definição do sinal para captar processo de encerramento.

---

**ICA4011 Não é possível abrir soquete.**

**Explicação:** Falha durante a abertura do soquete.

---

---

**ICA4012 Não é possível definir sigset para SIGTERM.**

**Explicação:** Falha durante a configuração para captar os sinais SIGTERM & SIGINT.

---

**ICA4013 Não é possível definir opção de reutilização de soquete.**

**Explicação:** Falha ao definir opção de reutilização de soquete.

---

**ICA4014 Não é possível definir opção de retardo do soquete.**

**Explicação:** Falha durante a definição da opção de retardo do soquete.

---

**ICA4015 Não é possível ligar o soquete na porta.**

**Explicação:** Falha ao ligar o soquete na porta.

---

**ICA4016 Não é possível definir ouvir no soquete.**

**Explicação:** Falha durante a configuração ouvir no soquete.

---

**ICA4017 Serviço Nome do serviço usando soquete TCP soquete.**

**Explicação:** Mensagem informativa.

---

**ICA4018 Falha na chamada da função select().**

**Explicação:** Falha interna de chamada de função.

---

**ICA4019 Erro grave de new\_work().**

**Explicação:** Erro interno grave da rotina new\_work.

---

**ICA4020 Erro(programa): Não foi possível gravar no soquete de fluxo: soquete**

**Explicação:** Possível erro do sistema.

**Resposta do Usuário:** Verifique a utilização do soquete.

---

**ICA4021 Problema no recebimento da resposta.**

**Explicação:** Problema no recebimento da resposta do modem.

**Resposta do Usuário:** Verifique as conexões do modem e a cadeia de inicialização.

---

**ICA4022 Pedido bem sucedido.**

**Explicação:** Mensagem informativa.

---

**ICA4023 O pedido falhou.**

**Explicação:** O pedido para enviar página falhou.

---

**ICA4024 Erro(programa): Prioridade fora do intervalo (prioridade mín. - prioridade máx.).**

**Explicação:** Intervalo de prioridade incorreto.

**Resposta do Usuário:** Corrija o intervalo de prioridade. Os valores válidos vão de -1 a 5.

---

---

**ICA4025 Erro(programa): O endereço precisa estar na forma de ID\$operadora quando a opção -n é usada.**

**Explicação:** Sintaxe de utilização de comando incorreta.

**Resposta do Usuário:** Corrija a sintaxe de utilização de comando.

---

**ICA4026 Erro(programa): Host desconhecido *nome do host***

**Explicação:** Não foi possível resolver o nome do host.

**Resposta do Usuário:** Verifique o nome do host.

---

**ICA4027 Erro(programa): Não foi possível abrir o soquete de fluxo : *número do erro***

**Explicação:** Não foi possível criar um novo soquete.

---

**ICA4028 Erro(programa): Não foi possível definir as opções do soquete : *número do erro***

**Explicação:** Não foi possível definir a opção de retardo do soquete.

---

**ICA4029 Erro(programa): Não foi possível fazer a conexão com o host : *número do erro.***

**Explicação:** Não foi possível fazer a conexão com o host.

**Resposta do Usuário:** Verifique a configuração da porta serial e a existência de arquivo controlador de dispositivo.

---

**ICA4030 Erro(programa): Não foi possível gravar no soquete de fluxo : *número do erro.***

**Explicação:** Não foi possível gravar no soquete de fluxo.

---

**ICA4031 Problema no recebimento da resposta. Condição da mensagem desconhecida.**

**Explicação:** Problema no recebimento da resposta do modem.

---

**ICA4032 Mensagem enviada com sucesso para a fila.**

**Explicação:** Mensagem informativa. A mensagem foi enviada para a fila.

---

**ICA4033 A mensagem falhou. Nenhuma mensagem enviada.**

**Explicação:** Não foi possível enviar a mensagem para a fila do pager.

---

**ICA4034 *data* Falhou (ID *ID* Pri *prioridade* Secs *período* Tentativas *número de tentativas*) {da Entrada,, Nome: mensagem.**

**Explicação:** Exibe esta mensagem quando a página é enviada sem sucesso.

---

**ICA4035 Não é possível enfileirar de novo a mensagem *mesg do programa* para a *pessoa*.**

**Explicação:** Não foi possível enviar para a fila de paginação.

---

---

**ICA4036 BEM-SUCEDIDA (ID ID Pri prioridade Secs período Tentativas número de tentativas) {da Entrada,, Nome: mensagem.**

**Explicação:** Exibe esta mensagem quando a página é enviada com sucesso. Mensagem informativa.

---

**ICA4037 DESCARREGADA para arquivo de descarga (ID ID Pri prioridade Secs período Tentativas número de tentativas) {da Entrada,, Nome: mensagem.**

**Explicação:** As páginas não enviadas imediatamente são descarregadas num arquivo para nova tentativa mais tarde.

---

**ICA4038 Não é possível gravar no arquivo de descarga arquivo de descarga.**

**Explicação:** O arquivo de descarga não aceita gravação.

**Resposta do Usuário:** Verifique as permissões de sistema do arquivo.

---

**ICA4039 IpcKey: 0xIpcKey**

**Explicação:** Mensagem informativa.

---

**ICA4040 O tempo para fazer novas tentativas Tempo para tentativa minutos foi excedido.**

**Explicação:** Falha na inicialização do modem após os minutos especificados.

**Resposta do Usuário:** Verifique a cadeia de inicialização.

---

**ICA4041 Encontrada mensagem alfanumérica para pager numérico.**

**Explicação:** Pagers numéricos não podem conter dados alfanuméricos.

**Resposta do Usuário:** Corrija usando o menu smitty/SMIT.

---

**ICA4042 A pessoa não consegue receber mensagens.**

**Explicação:** O pager provavelmente não está ativado.

**Resposta do Usuário:** Verifique se o pager está ativado.

---

**ICA4043 A operadora operadora não existe.**

**Explicação:** A operadora especificada não existe.

**Resposta do Usuário:** Corrija usando o menu smitty/SMIT.

---

**ICA4044 A operadora operadora não possui número de telefone DTMF.**

**Explicação:** A operadora especificada não possui número de telefone DTMF.

**Resposta do Usuário:** Corrija usando o menu smitty/SMIT.

---

**ICA4045 O número do pager Número do pager é grande demais para o máximo da operadora de Tamanho da operadora.**

**Explicação:** O número do pager é grande demais para o máximo da operadora.

**Resposta do Usuário:** Use outro número de pager, que seja menor do que o máximo da operadora.

---

**ICA4046 O número do pager** *Número do pager é grande demais para o tamanho padrão de tamanho padrão da operadora.*

**Explicação:** Essa mensagem ocorre quando o tamanho padrão é muito pequeno.

**Resposta do Usuário:** Corrija usando o menu smitty/SMIT. Aumente o tamanho padrão.

---

**ICA4047 Problema na linha** *número da linha do arquivo de modem Nome do caminho do arq do modem.*

**Explicação:** O arquivo de definição do modem contém caractere inválido.

**Resposta do Usuário:** Corrija usando o menu smitty/SMIT.

---

**ICA4048 O modem não pode ser aberto no dispositivo** */dev/Nome do dispositivo.*

**Explicação:** O modem não pôde ser aberto no dispositivo especificado.

**Resposta do Usuário:** Verifique ou reconfigure a porta serial. Verifique o dispositivo.

---

**ICA4049 Abertura do modem no** */dev/Nome do dispositivo.*

**Explicação:** Mensagem informativa. O modem foi devidamente detectado na porta serial.

---

**ICA4050 Não é possível definir as características do modem.**

**Explicação:** Falha na tentativa de definição das características do modem.

**Resposta do Usuário:** Verifique a cadeia de inicialização do modem.

---

**ICA4051 O modem não pôde ser inicializado após** *número inicial de tentativas tentativas.*

**Explicação:** O modem não foi inicializado.

**Resposta do Usuário:** Verifique a cadeia de inicialização e a configuração da porta serial.

---

**ICA4052 Não é possível discar o número do pager** *Número do pager*

**Explicação:** O número do pager não pode ser discado.

**Resposta do Usuário:** Verifique a validade do número do pager.

---

**ICA4053 O modem não pode ser desligado.**

**Explicação:** O modem não pode ser desligado.

**Resposta do Usuário:** Verifique a cadeia de inicialização do modem e o comando de desligar utilizado.

---

**ICA4054 Não é possível discar a mensagem** *mensagem*

**Explicação:** Não é possível discar mensagens.

---

**ICA4055 Problema na linha** *número da linha no arquivo de modem nome do arquivo.*

**Explicação:** Arquivo de definição de modem inválido.

**Resposta do Usuário:** Corrija usando o menu smitty/SMIT.

---

**ICA4056 Não é possível discar o número de DTMF da operadora** *(DTMFnumb).*

**Explicação:** O número de DTMF pode ter mudado ou está incorreto para essa operadora.

**Resposta do Usuário:** Corrija usando o menu smitty/SMIT.

---

---

**ICA4057 Não é possível transmitir o bloco.**

**Explicação:** Falha durante a tentativa de transmitir o bloco.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4058 Não há resposta para o bloco transmitido.**

**Explicação:** Não foi possível obter resposta da operadora depois de transmitir o bloco.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4059 Não é possível receber resposta para entrega de mensagem.**

**Explicação:** Não foi possível obter resposta da operadora depois da entrega da mensagem.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4060 Não foi possível transmitir a id do pager.**

**Explicação:** Não foi possível transmitir a id do pager.

**Resposta do Usuário:** Verifique os parâmetros de número e da operadora usando o menu smitty/SMIT.

---

**ICA4061 Não é possível transmitir final <CR> de pedido de modo automático.**

**Explicação:** Não é possível transmitir final <CR> de pedido de modo automático.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4062 Não é possível transmitir o pedido de modo automático.**

**Explicação:** Não é possível transmitir sinal de pedido de modo automático.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4063 Falha no recebimento do aviso de siga em frente da operadora *operadora* após *número de tentativas* tentativas.**

**Explicação:** A operadora deve estar ocupada.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT e tente mais tarde.

---

**ICA4064 Erro de comunicação durante o prompt com a operadora *operadora*.**

**Explicação:** Erro de comunicação pode ocorrer por diversas razões. Tente de novo mais tarde.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT e tente mais tarde.

---

**ICA4065 Não é possível receber resposta para login.**

**Explicação:** O modem não consegue receber resposta para login.

**Resposta do Usuário:** Confira a cadeia de inicialização do modem e os parâmetros da operadora.

---

---

**ICA4066 A operadora *operadora* não respondeu à tentativa de logon.**

**Explicação:** A operadora não respondeu à tentativa de logon.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT e tente mais tarde.

---

**ICA4067 A operadora *operadora* disse *receber cadeia de dados*.**

**Explicação:** A operadora transmitiu de volta alguma mensagem de erro ou mensagem de ocupado.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT e tente mais tarde.

---

**ICA4068 A operadora *operadora* forçou uma desconexão durante o logon.**

**Explicação:** A operadora forçou uma desconexão durante o logon.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4069 Descarga de mensagens para a operadora *operadora* causada por *Tentativas máximas de conexão* tentativas em loop.**

**Explicação:** Se a operadora está ocupada, o programa descarrega as páginas e tenta de novo mais tarde.

---

**ICA4070 Desistência de descarregar mensagens para a operadora *operadora* causada por *Tentativas Máximas* tentativas de conexão de sessão.**

**Explicação:** A operadora não pode ser contactada após um determinado número de tentativas.

**Resposta do Usuário:** Verifique os parâmetros da operadora e tente novamente mais tarde.

---

**ICA4071 Erro(*programa*): Não é possível alocar memória para nova tentativa da operadora: *número do erro*.**

**Explicação:** Possível erro de sistema ou de alocação de memória.

---

**ICA4072 Erro(*programa*): Não é possível colocar na lista de tentativas da operadora: *número do erro*.**

**Explicação:** É possível que a operadora não exista.

**Resposta do Usuário:** Verifique a validade da operadora e tente novamente.

---

**ICA4073 A conexão de dados com a operadora *operadora* no *número do telefone* falhou após *Contagem de tentativas* tentativas.**

**Explicação:** A conexão de dados falhou.

**Resposta do Usuário:** Verifique as conexões de modem e os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4074 O prompt de ID da operadora *operadora* não foi recebido após *número de tentativas* tentativas.**

**Explicação:** A operadora não respondeu com prompt de ID ou de aviso de recebimento.

**Resposta do Usuário:** Confira se a operadora está usando o Protocolo TeleAlfanumérico.

---

**ICA4075 Erro de comunicação durante o logon com a operadora** *operadora*.

**Explicação:** Erro de comunicação pode ocorrer por diversas razões.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4076 O número máximo de tentativas de logon para a operadora** *operadora* **foi excedido.**

**Explicação:** A operadora deixou de responder dentro do número especificado de tentativas.

**Resposta do Usuário:** Verifique os parâmetros da operadora e tente novamente mais tarde.

---

**ICA4077 Não foi recebida a mensagem de vá em frente enviada pela operadora** *operadora*.

**Explicação:** A operadora não respondeu com prompt de vá em frente.

**Resposta do Usuário:** Verifique os parâmetros da operadora e tente novamente mais tarde.

---

**ICA4078 Os blocos não podem ser criados.**

**Explicação:** A operadora não pôde criar blocos para transmissão.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4079 A operadora** *operadora* **não respondeu à entrega das mensagens.**

**Explicação:** A operadora teve dificuldade para entregar a mensagem.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4080 A operadora** *operadora* **forçou a desconexão durante a entrega da mensagem.**

**Explicação:** A operadora forçou a desconexão durante a entrega da mensagem.

**Resposta do Usuário:** Confira os parâmetros da operadora e a cadeia de inicialização.

---

**ICA4081 A operadora** *operadora* **rejeitou mensagem ou ID do Pager.**

**Explicação:** A operadora rejeitou a mensagem do pager ou a id do pager.

**Resposta do Usuário:** Confira a validade da id do pager, a ativação do pager e os parâmetros da operadora.

---

**ICA4082 Erro de comunicação durante a entrega da mensagem à operadora** *operadora*.

**Explicação:** Erro de comunicação pode ocorrer por diversas razões.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4083 Falha no recebimento da confirmação da operadora** *operadora* **após tentativas maximas tentativas.**

**Explicação:** Essa mensagem ocorre quando a operadora está ocupada ou não consegue estabelecer conexão.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT e tente de novo depois de alguns minutos.

---

---

**ICA4084** Não é possível transmitir <EOT>.

**Explicação:** O modem não consegue transmitir <EOT>.

**Resposta do Usuário:** Confira as conexões do modem e a cadeia de inicialização.

---

**ICA4085** Não há recebimento de resposta para <EOT>.

**Explicação:** O modem não pode receber resposta para <EOT>.

**Resposta do Usuário:** Confira as conexões do modem e a cadeia de inicialização.

---

**ICA4086** A operadora *operadora* não respondeu a <EOT>.

**Explicação:** A operadora não responde a dados transmitidos.

**Resposta do Usuário:** Confira a validade da operadora e as conexões do modem.

---

**ICA4087** A operadora *operadora* respondeu com erro inaceitável de dados por causa do conteúdo.

**Explicação:** A operadora não responde a dados transmitidos.

**Resposta do Usuário:** Verifique os parâmetros da operadora usando o menu smitty/SMIT.

---

**ICA4088** O arquivo de padrões *nome do caminho padrão* não pode ser aberto.

**Explicação:** Pode ser que o arquivo de padrões do modem não exista ou possua permissões incorretas.

**Resposta do Usuário:** Verifique a existência de permissões no arquivo.

---

**ICA4089** Arquivo de padrões incompleto *nome de caminho padrão*.

**Explicação:** Há dados faltando no arquivo de padrões do modem.

**Resposta do Usuário:** Corrija usando o menu smitty/SMIT.

---

**ICA4090** Número de linha externa inválida no arquivo de padrões *nome de caminho padrão na linha número da linha*.

**Explicação:** O arquivo de banco de dados da operadora possui número de linha externa inválido.

**Resposta do Usuário:** Limpe o arquivo de banco de dados da operadora.

---

**ICA4091** Valor inválido de velocidade de transmissão no arquivo de padrões *Arquivo padrão na linha número da linha*.

**Explicação:** O arquivo de banco de dados da operadora possui velocidade de transmissão inválida.

**Resposta do Usuário:** Limpe o arquivo de banco de dados da operadora.

---

**ICA4092** Valor inválido de bit de dados no arquivo padrões *Arquivo padrão na linha número de linha*.

**Explicação:** O arquivo de banco de dados da operadora possui valor inválido de bit de dados.

**Resposta do Usuário:** Limpe o arquivo de banco de dados da operadora.

---

---

**ICA4093** Valor de paridade inválido no arquivo de padrões *dArquivo padrão na linha número de linha.*

**Explicação:** O arquivo de banco de dados possui valor de paridade inválido.

**Resposta do Usuário:** Limpe o arquivo de banco de dados da operadora.

---

**ICA4094** Valor inválido de bit de parada no arquivo de padrões *Arquivo padrão na linha Número de linha.*

**Explicação:** O arquivo de banco de dados da operadora possui valor de bit de parada inválido.

**Resposta do Usuário:** Limpe o arquivo de banco de dados da operadora.

---

**ICA4095** Tag não reconhecida *tag id no arquivo de padrões Arquivo padrão na linha número da linha.*

**Explicação:** O arquivo de banco de dados da operadora possui tag inválida.

**Resposta do Usuário:** Limpe o arquivo de banco de dados da operadora.

---

**ICA4096** Número incorreto de parâmetros.

**Explicação:** Mensagem informativa.

---

**ICA4097** Erro(*programa*): Não é possível criar lista da operadora. Problemas na memória.

**Explicação:** Possível problema de sistema ou de memória.

---

**ICA4098** Erro(*programa*): Erros na paginação do arquivo da operadora *Arquivo da operadora.*

**Explicação:** O arquivo de banco de dados da operadora possui alguns dados inválidos.

**Resposta do Usuário:** Verifique se não há tags inválidas no arquivo de banco de dados da operadora.

---

**ICA4099** Erro(*programa*): Não é possível criar token IPC *número do erro.*

**ICA4100** Erro(*programa*): Não é possível criar lista de tentativas. Possíveis problemas de memória.

**Explicação:** Possível erro de sistema ou problemas de memória.

---

**ICA4101** Erro(*operadora*): Não é possível criar fila, *page\_q\_err: pageQErr.*

**ICA4102** Erro(*programa*): Não é possível captar SIGTERM/SIGINT: *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4103** Erro(*programa*): Não é possível definir as características do modem para a operadora *operadora.*

**Explicação:** Não foi possível configurar o modem.

**Resposta do Usuário:** Confira a configuração da porta serial e a cadeia de inicialização.

---

**ICA4104** Está faltando a tag *tag para a operadora operadora.*

**Explicação:** Estão faltando informações do modem. A tag pode ser a velocidade de transmissão, a linha de fora, etc..

**Resposta do Usuário:** Veja se não há caracteres inválidos do arquivo de configuração do modem.

---

**ICA4105** A operadora *operadora* precisa ter no mínimo um número de telefone listado.

**Explicação:** A operadora precisa conter o número de telefone.

**Resposta do Usuário:** Inclua o número de telefone usando o menu smitty/SMIT.

---

**ICA4106** O arquivo *Arquivo do Nome da operadora* não pode ser aberto.

**Explicação:** O banco de dados da operadora deve existir.

**Resposta do Usuário:** Se já não estiver presente, crie um usando o menu smitty/SMIT.

---

**ICA4107** Linha *número da linha* muito grande.

**Explicação:** A linha do arquivo de banco de dados da operadora é muito grande.

**Resposta do Usuário:** Verifique se o arquivo de banco de dados da operadora não contém linha inválida.

---

**ICA4108** Tag desconhecida na linha *número da linha*.

**Explicação:** Há uma tag desconhecida no arquivo de banco de dados da operadora.

**Resposta do Usuário:** Verifique se não há tag inválidas no arquivo de banco de dados da operadora.

---

**ICA4109** Seqüência inválida na linha *número da linha*.

**Explicação:** Há uma seqüência inválida no arquivo de banco de dados da operadora.

**Resposta do Usuário:** Verifique se não há seqüência inválida no arquivo de banco de dados da operadora.

---

**ICA4110** A operadora *operadora* não é válida e está sendo pulada.

**Explicação:** A operadora não pode ser usada para fins de paginação.

**Resposta do Usuário:** Verifique a validade da operadora.

---

**ICA4111** Não é possível colocar operadora na lista.

**Explicação:** A operadora não pode ser colocada na lista.

**Resposta do Usuário:** Confira a validade da operadora e os números de telefone.

---

**ICA4112** O nome da operadora está faltando ou é grande demais na linha *número da linha*.

**Explicação:** O nome da operadora está faltando.

**Resposta do Usuário:** Inclua a operadora usando o menu smitty/SMIT.

---

**ICA4113** Não é possível alocar nova operadora de paginação: *operadora*.

**Explicação:** A operadora não pode ser alocada na lista.

**Resposta do Usuário:** Confira a validade da operadora e os números de telefone.

---

**ICA4114** O valor da linha *número da linha* é grande demais.

**Explicação:** Encontrada linha grande demais no arquivo de banco de dados da operadora.

**Resposta do Usuário:** Retire a linha grande do arquivo de banco de dados da operadora.

---

---

**ICA4115** Tag repetida *tag* na linha *número da linha* ignorada.

**Explicação:** Encontrada tag repetida.

**Resposta do Usuário:** Retire a tag repetida do arquivo de banco de dados da operadora.

---

**ICA4116** O valor da linha *número da linha* não existe.

**Explicação:** Encontrado campo em branco.

**Resposta do Usuário:** Use smitty/SMIT para incluir um valor no campo em branco.

---

**ICA4117** O valor deve ser S, Sim, N ou Não na linha *número da linha*.

**Explicação:** Este campo requer S, Sim, N ou Não.

**Resposta do Usuário:** Use smitty/SMIT para incluir ou alterar dados válidos.

---

**ICA4118** O valor precisa ser maior que 0 na linha *número da linha*.

**Explicação:** Este campo deve ser positivo

**Resposta do Usuário:** Altere o valor usando smitty/SMIT para um valor positivo.

---

**ICA4119** Valor inválido na linha *número da linha*.

**Explicação:** Encontrado valor inválido na linha especificada.

**Resposta do Usuário:** Altere o valor usando o menu smitty/SMIT.

---

**ICA4120** A operadora *nome* é inválida e está sendo pulada.

**Explicação:** Encontrada uma operadora inválida.

**Resposta do Usuário:** Inclua um operadora válido usando o menu smitty/SMIT.

---

**ICA4121** Não é possível colocar operadora na lista.

**Explicação:** Não é possível incluir operadora na lista de paginação.

**Resposta do Usuário:** Confira a validade da operadora.

---

**ICA4122** Tag repetida *tag* na linha *número da linha* ignorada.

**Explicação:** Encontrada tag repetida em bloco da operadora.

**Resposta do Usuário:** Limpe o bloco da operadora que contém valores repetidos.

---

**ICA4123** Erro(*programa*): Não foi possível obter token IPC: *Número do erro*

**Explicação:** O programa não conseguiu obter token IPC.

---

**ICA4124** Erro(*programa*): Erro *pageqErr* durante a leitura da fila.

**Explicação:** O programa não conseguiu ler a fila.

---

**ICA4125** *número* Entradas na fila.

**Explicação:** Mensagem informativa.

---

**ICA4126** Mensagem com ID *id* apagada.

**Explicação:** Mensagem informativa.

---

---

**ICA4127** A ID *id* não está na fila.

**Explicação:** Mensagem informativa.

---

**ICA4128** Erro(*programa*): Erro *pageqErr* durante a tentativa de eliminar a ID *id*.

**Explicação:** Tentou eliminar uma ID da fila.

---

**ICA4129** A chave é: *entryKey* conteúdo é § *ptr*: *ptr*.

**Explicação:** Apenas mensagem informativa.

---

**ICA4130** Características do Modem:

**Explicação:** Informação de inicialização do modem.

---

**ICA4131** Nome: *Nome do modem*

**Explicação:** Informação de inicialização do modem.

---

**ICA4132** Init: *Cadeia inicial*

**Explicação:** Informação de inicialização do modem.

---

**ICA4133** Modo de comando: *comando*

**Explicação:** Informação de inicialização do modem.

---

**ICA4134** Terminador do comando: *0xterminador*

**Explicação:** Informação de inicialização do modem.

---

**ICA4135** Discagem: *discagem*

**Explicação:** Informação de inicialização do modem.

---

**ICA4136** Pausa de Discagem: *pausa*

**Explicação:** Informação de inicialização do modem.

---

**ICA4137** Discagem #: *diallb*

**Explicação:** Informação de inicialização do modem.

---

**ICA4138** Discagem \*: *dialstar*

**Explicação:** Informação de inicialização do modem.

---

**ICA4139** Desligar: *desligar*

**Explicação:** Informação de inicialização do modem.

---

**ICA4140** Resposta de comando válida: *resposta de comando válida*

**Explicação:** Informação de inicialização do modem.

---

**ICA4141** Conexão válida: *Conexão válida*

**Explicação:** Informação de inicialização do modem.

---

---

**ICA4142**    **Eco:** *eco*

**Explicação:** Informação de inicialização do modem.

---

**ICA4143**    **Registro de depuração do modem:** **PUTS(*id*) txd->** *Cadeia externa*

**Explicação:** Informações do sinal de transmissão do modem.

---

**ICA4144**    **Registro de depuração do modem:** **PUTC(*id*) txd->** *Cadeia externa*

**Explicação:** Informações do sinal de transmissão do modem.

---

**ICA4145**    **Registro de depuração do modem:** **GET rxd-> %1\$s**

**Explicação:** Informações do sinal de transmissão do modem.

---

**ICA4146**    **Registro de depuração do modem:** **INPUT(%1\$s**

**Explicação:** Informações do sinal de transmissão do modem.

---

**ICA4147**    **Registro de depuração do modem:** **) rxd->**

**Explicação:** Informações do sinal de transmissão do modem.

---

**ICA4148**    **Registro de depuração do modem:** **WAITFOR(%1\$s**

**Explicação:** Informações do sinal de transmissão do modem.

---

**ICA4149**    **Não foi possível desbloquear sinal filho.**

**Explicação:** Desbloqueia o sinal SIGCHLD.

---

**ICA4150**    **Não foi possível bloquear o sinal filho.**

**Explicação:** Bloqueia o sinal SIGCHLD.

---

**ICA4151**    **O arquivo de partida aquecida** *nome do caminho do arquivo não existe.*

**Explicação:** Mensagem informativa.

---

**ICA4152**    **Não é possível abrir o arquivo de partida aquecida** *nome do caminho do arquivo*

**Explicação:** Mensagem informativa.

---

**ICA4153**    **Linha grande demais no arquivo de partida aquecida** *nome do caminho do arquivo.*

**Explicação:** O arquivo de partida aquecida contém caracteres inválidos.

---

**ICA4154**    **O arquivo de partida aquecida** *nome do caminho do arquivo possui dados que não estão sendo usados.*

**Explicação:** Mensagem informativa.

---

**ICA4155**    **O arquivo de partida aquecida** *nome do caminho do arquivo está vazio.*

**Explicação:** Mensagem informativa.

---

---

**ICA4156** A linha *número da linha do arquivo de partida aquecida* nome do caminho do arquivo possui um endereço ruim endereço, ignorado.

**Explicação:** O arquivo de partida aquecida possui caracteres inválidos. Mensagem informativa.

---

**ICA4157** A linha *número da linha do arquivo de partida aquecida* nome do caminho do arquivo tem formato ruim; ignorado.

**Explicação:** O arquivo de partida aquecida possui caracteres inválidos. Mensagem informativa.

---

**ICA4158** A linha *número da linha do arquivo de partida aquecida* nome do caminho do arquivo não tem mensagem; ignorado.

**Explicação:** O arquivo de partida aquecida não tem mensagens. Mensagem informativa.

---

**ICA4159** Erro no enfileiramento da linha *número da linha do arquivo de partida aquecida* nome do caminho do arquivo, ignorado.

**Explicação:** O arquivo de partida aquecida possui caracteres inválidos. Mensagem informativa.

---

**ICA4160** A partida aquecida completa de *número mensagens do arquivo* nome do caminho do arquivo.

**Explicação:** Mensagem informativa.

---

**ICA4161** Erro(programa): Muitos erros filho consecutivos.

**Explicação:** Muitos erros filho numa linha. Isso ocorre se a operadora ou o arquivo de definição do modem possui caracteres inválidos.

**Resposta do Usuário:** Verifique o arquivo do banco de dados do operadora e arquivo de definição do modem usando o menu smitty/SMIT.

---

**ICA4162** Filho não consegue executar programa : *número do erro*.

**Explicação:** Possível erro do sistema.

---

**ICA4163** Erro(*número do erro*): Filho não consegue bifurcar filho : *nome do programa*.

**Explicação:** Possível erro do sistema.

---

**ICA4164** Não foi possível criar lista de operadoras de paginação.

**Explicação:** Erro interno de programa.

---

**ICA4165** Erros na paginação do arquivo da operadora *Arquivo da operadora*

**Explicação:** O banco de dados da operadora contém dados inválidos.

**Resposta do Usuário:** Verifique o arquivo do banco de dados do operadora usando o menu smitty/SMIT.

---

**ICA4166** Mensagem informativa. A chave do IPC é: *0xChave lpc*.

**Explicação:** Mensagem informativa.

---

**ICA4167** Não foi possível criar fila, *page\_q\_err: erro de página Q*.

**Explicação:** Falha ao tentar criar fila.

---

**ICA4168** Criado arquivo de Partida Aquecida de Paginação as *horário*

**Explicação:** Mensagem informativa.

---

**ICA4169** *prioridade* -p *prioridade* número de pager a partir de objfrom mensagem

**Explicação:** Mensagem informativa.

---

**ICA4170** *prioridade* -p *prioridade* Pager alfanumérico\$operadora de de mensagem

**Explicação:** Mensagem informativa.

---

**ICA4171** *prioridade* -p *prioridade* -n Pager numérico\$operadora de de mensagem

**Explicação:** Mensagem informativa.

---

**ICA4172** Final do arquivo de partida aquecida do pager.

**Explicação:** Mensagem informativa. Indica o final da mensagem.

---

**ICA4173** Não é possível gravar no arquivo de partida aquecida *arquivo de cadeia aquecida*.

**Explicação:** Pode ser que o arquivo de partida aquecida não exista.

---

**ICA4174** *horário* STATUS-REQUEST do usuário\$host

**Explicação:** Exibe as informações do pedido de status.

---

**ICA4175** *horário* SUMMARY-REQUEST do usuário\$host.

**Explicação:** Exibe as informações de pedido de sumário.

---

**ICA4176** *número* entradas na fila.

**Explicação:** Conta o número de entradas da fila do pager.

---

**ICA4177** Entrada mais antiga: ID *id* recebida as *horário*.

**Explicação:** Exibe a entrada mais antiga da fila.

---

**ICA4178** Reacoplamento da memória após falha de expansão.

**Explicação:** Possível erro do sistema.

---

**ICA4179** Reacoplamento de memória após falha de alinhamento da expansão.

**Explicação:** Possível erro do sistema.

---

**ICA4180** Não foi possível descer sinal PAGE\_Q em page\_q\_print() : *número do erro*.

**Explicação:** Possível erro do sistema.

---

**ICA4181** Não foi possível subir sinal PAGE\_Q em page\_q\_print() : *número do erro*.

**Explicação:** Possível erro do sistema.

---

**ICA4182** link *Ligação de cabeçalho* -> ID da mensagem: *id*.

**Explicação:** Mensagem informativa.

---

<b>ICA4183</b>	<b>Prioridade:</b> <i>prioridade</i> .
<b>Explicação:</b>	Mensagem informativa.
<b>ICA4184</b>	<b>Pessoa:</b> <i>nome</i> .
<b>Explicação:</b>	Mensagem informativa.
<b>ICA4185</b>	<b>Operadora:</b> <i>operadora</i> .
<b>Explicação:</b>	Mensagem informativa.
<b>ICA4186</b>	<b>Mensagem:</b> <i>mensagem</i> .
<b>Explicação:</b>	Mensagem informativa.
<b>ICA4187</b>	<b>Não foi possível obter RAM compartilhada :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4188</b>	<b>Não foi possível obter RAM compartilhada acoplada :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4189</b>	<b>Não foi possível obter sinal PAGE_Q.</b>
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4190</b>	<b>Não foi possível inicializar sinal PAGE_Q em page_q_create() :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4191</b>	<b>Não foi possível definir sinal PAGE_Q em page_q_create() :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4192</b>	<b>Não foi possível descer sinal PAGE_Q em page_q_empty() :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4193</b>	<b>Não foi possível subir sinal PAGE_Q em page_q_empty() :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4194</b>	<b>Não foi possível descer sinal PAGE_Q em page_q_enq(<i>nome</i>,<i>mensagem</i>) :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4195</b>	<b>Não foi possível subir sinal PAGE_Q em page_q_enq() :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.
<b>ICA4196</b>	<b>page_q_enq():</b> ID( <i>id</i> ) Pri( <i>prioridade</i> ) Pessoa( <i>nome</i> ) Mesg( <i>mensagem</i> ).
<b>Explicação:</b>	Mensagem informativa.
<b>ICA4197</b>	<b>Não foi possível descer sinal PAGE_Q em page_q_head() :</b> <i>número do erro</i> .
<b>Explicação:</b>	Possível erro do sistema.

---

**ICA4198** Não foi possível subir sinal PAGE\_Q em `page_q_head()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4199** Não foi possível descer sinal PAGE\_Q em `page_q_first()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4200** Não foi possível subir sinal PAGE\_Q em `page_q_first()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4201** Não foi possível descer sinal PAGE\_Q em `page_q_next()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4202** Não foi possível subir sinal PAGE\_Q em `page_q_next()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4203** Não foi possível descer sinal PAGE\_Q em `page_q_tail()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4204** Não foi possível subir sinal PAGE\_Q em `page_q_tail()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4205** Não foi possível descer sinal PAGE\_Q em `page_q_del()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4206** Não foi possível subir sinal PAGE\_Q em `page_q_del()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4207** `page_q_del(ID)`.

**Explicação:** Informação de depuração.

---

**ICA4208** Não foi possível descer sinal PAGE\_Q em `page_q_deq()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4209** Não foi possível subir sinal PAGE\_Q em `page_q_deq()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4210** `page_q_del()`: ID(*id*) Pri(*prioridade*) Pessoa( *nome*) Mesg(*mensagem*).

**Explicação:** Mensagem informativa.

---

**ICA4211** Não foi possível descer sinal PAGE\_Q em `page_q_walk()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

**ICA4212** Não foi possível subir sinal PAGE\_Q em `page_q_walk()` : *número do erro.*

**Explicação:** Possível erro do sistema.

---

---

**ICA4213 PAGE\_Q cheio.**

**Explicação:** A fila de paginação está cheia.

**Resposta do Usuário:** Aguarde um tempo para enviar a página.

---

**ICA4300 Desligando.**

**Explicação:** Desligando a chamada.

---

**ICA4301 Inicializando o modem ..**

**Explicação:** Inicializando o modem com a cadeia de inic.

---

**ICA4302 Discando .....**

**Explicação:** Discando o número do telefone.

---

**ICA4303 Esperando a conexão.**

**Explicação:** Esperando pela conexão do modem

---

**ICA4304 CONECTADO *velocidade***

**Explicação:** Conectando com velocidade de transmissão de 'velocidade'

---

**ICA4305 CONECTADO!!!!!!**

**Explicação:** Conectado ao provedor de serviços de pager

---

**ICA4306 Solicitando prompt para Modo Automático.**

**Explicação:** Solicitando prompt para modo automático. Esperando pela "ID="

---

**ICA4307 Prompt OK.....**

**Explicação:** Recebida "ID=" de volta do provedor.

---

**ICA4308 Enviando Pedido de Modo Automático.**

**Explicação:** Enviando ID e SST para o provedor de serviços de pager

---

**ICA4309 Enviar Pedido de Modo Automático .....OK!**

**Explicação:** P de volta. Indicação de comunicação bem sucedida

---

**ICA4310 Enviando mensagem**

**Explicação:** Enviando bloco de mensagens por

---

**ICA4311 Esperando pelo resultado**

**Explicação:** Esperando pela confirmação

---

**ICA4312 Ack recebido. Página bem-sucedida****ICA4313 Nak recebido, Reenviar bloco. Tentar *Tentativas Nak***

**Explicação:** Nak recebido. O provedor de pager está pedindo para enviar de novo

---

**ICA4314 Erro de transação. Reenviar bloco. Tentar *Tentativas de Reenvio***

**Explicação:** Erro de transação. Enviando o bloco de novo.

---

---

**ICA4315**    **Conexão da operadora terminada.**

**Explicação:** O provedor de pager terminou a conversação. Chame o provedor para o problema

---

**ICA4350**    **fwpage operadora="..." "modem="..." "ID="..." "msg="..." "**

**Explicação:** Utilização de fwpage. Confira os parâmetros e tente de novo

---

**ICA4351**    ***Este arquivo não existe***

**Explicação:** Veja se arquivo está sob o diretório certo. Carriers.cfg, modems.cfg, e pager.cfg precisam ser criados antes de usar esse código.

---

**ICA4352**    ***Que arquivo danificado***

**Explicação:** O arquivo foi modificado pelo usuário e não está no formato do bloco. Todos os atributos devem ser introduzidos pela GUI.

---

**ICA4353**    ***O que muito grande; reduza-o e tente de novo***

**Explicação:** 'O que' muito grande. Reduza-o e tente de novo.

---

**ICA4354**    ***O que está errado.***

**Explicação:** Se a taxa de bauds estiver errada, as opções válidas são: 600, 1200, 2400, 4800, 9600, 14400. Se o bit de dados por byte estiver errado, as opções válidas são: 7, 8. Se os bits de parada estiverem errados, as opções válidas são: 1,2. Se o prefixo de linha fora estiver errado, as entradas devem ser apenas números. Se o método de paginação estiver errado, só o TAP será suportado nesta versão. Se houver erro de ID do pager, verifique se ele é formado apenas por números. Se a paridade estiver errada, as opções válidas são: O(odd - ímpar), E(even - par), N(none - nenhum), S(space - espaço), M(mark - marca). Se a porta COM estiver errada, as opções válidas são: COM1, COM2 .... A porta COM deve ser menor que 10 nesta versão. Se o caractere da mensagem estiver errado, examine-a para ver se ela contém caracteres especiais.

---

**ICA4355**    **Erro na definição de parâmetros em *onde*.**

**Explicação:** Não foi possível definir parâmetros em 'onde'. Confira os parâmetros e tente de novo.

---

**ICA4356**    **quando *Quando*, erro de leitura da porta COM.**

**Explicação:** Erro de leitura da porta COM. Defina o eco do modem e tente de novo.

---

**ICA4357**    **quando *Onde*, erro de gravação na porta COM.**

**Explicação:** Erro de gravação na porta COM.

---

**ICA4358**    **Defina *que* erro**

**Explicação:** Defina 'Que' erro. Examine o arquivo de log e identifique o erro.

---

**ICA4359**    **Número máximo de tentativas excedido em *Onde*. Abortar programa**

**Explicação:** Tente abrir a porta 60 vezes em 60 minutos. Tudo falhou. Se este for o caso, verifique a conexão do hardware. Tente enviar mensagem do pager 10 vezes em 10 minutos. Tudo falhou. Se este for o caso, o provedor de página deve estar inativo.

---

**ICA4360** **Caractere desconhecido no número de telefone da Operadora:**  
*\*pCarrierPhoneNum*

**Explicação:** encontrado um caractere não-reconhecido no número do telefone da operadora. Confira o número e tente de novo.

---

**ICA4361** **Aviso!!! A velocidade do modem do provedor de pager normalmente deve ser menor que 2400.**

**Explicação:** Não se trata apenas de um aviso. A velocidade do modem do provedor de paginação costuma ser definida para menos de 2400.

---

**ICA4362** **Não foi possível inicializar o modem**

**Explicação:** Mude a cadeia de inicialização do modem e tente de novo.

---

**ICA4363** **O modem retornou erro.**

**Explicação:** Erro de comunicação do modem

---

**ICA4364** *número de tentativas* **tentativas de abrir a porta de Com. Tente novamente em 1 minuto**

**Explicação:** Erro de abertura da porta de com. É provável que outro programa a esteja utilizando. Nova tentativa automática em 1 minuto.

---

**ICA4365** **O envio da página falhou após *número de tentativas* tentativas. Tente novamente em 1 minuto**

**Explicação:** O envio da página falhou. Examine o arquivo de log para descobrir o motivo exato.

---

**ICA4366** **Mensagem grande demais; truncada**

**Explicação:** Apenas um aviso. O tamanho da mensagem é grande demais. Ela foi truncada para caber no espaço.

---

**ICA4367** **Redefina o Comprimento de mensagem máxima para o valor interno definido:***comprimento-msg*

**Explicação:** Redefina o tamanho máximo da mensagem para o valor padrão, porque o usuário o definiu para valor maior do que o definido internamente, que é 80.

---

**ICA4368** **Ação: Onde erro**

**Explicação:** Se há erro de abertura da porta COM, confira a configuração e tente de novo. Se há erro de fechamento do indicador de COM, trata-se de problema do sistema. Se há erro de depuração de COM, trata-se de problema do sistema. Se há erro de envio de comando de discagem, trata-se de problema com o comando de discagem. Verifique se ele é um modem compatível com Haye. Se há erro de solicitação de envio de ID, verifique se o provedor de pager suporta o protocolo TAP. Se há erro de envio do prompt automático, verifique se o serviço de pager está funcionando corretamente. Se há erro de envio de mensagem, examine o arquivo de log para localizar a causa da falha. Se há erro de prompt, não é possível obter prompt de volta do provedor de pager.

---

**ICA4369** **Erros de transação em demasia. Abortando ....**

**Explicação:** Erros de transação em demasia, aborte essa tentativa.

---

**ICA4370** Recebidos Naks demais; o programa está sendo abortado .....

**Explicação:** Recebidos Naks demais do provedor de pager; aborte esta tentativa.

---

**ICA4371** Porta Com sz na porta COM com a função Nome da função retornou Número do Erro

**Explicação:** Verifique os parâmetros e tente de novo.

---

**ICA4372** Mensagem de erro de retorno do modem ..... Mensagem de Retorno

**Explicação:** As mensagens são Não conectado, Chamando, mas não conectado, Sem operadora, Sem tom de discagem, Ocupado, Sem resposta.

---

**ICA4373** (nome de função) Código de resposta desconhecido a partir do modem ou operadora: caractere1, caractere2.

**Explicação:** Esta mensagem relata uma resposta do modem ou da operadora, que o recurso de paginação do Firewall não reconhece. caractere1 e caractere2 são os códigos ascii (hex) para os 2 primeiros caracteres na resposta.

**Resposta do Usuário:** Use estas informações ao consultar as instruções de modem ou a operadora para determinar o significado da resposta desconhecida.

---

**ICA5005** Inicialização de SKIT falhou. O código de retorno é: código de retorno

**Explicação:** Falha de inicialização do soquete seguro, código de retorno do SKIT é exibido.

---

**ICA5014** Servidor de Túnel de Cliente Remoto atendendo porta número da porta de servidor

**Explicação:** O número de porta configurado para sslrctd é exibido.

---

**ICA5015** Conexão aceita de chp0.chp1.chp2.chp3

**Explicação:** O endereço IP do cliente é exibido.

---

**ICA5017** Não é possível obter soquete seguro. A função skit\_secure\_soc\_init retcode é:retcode da função

**Explicação:** Não é possível obter soquete seguro porque o skit\_secure\_soc\_init() falhou.

---

**ICA5018** As especificações de cifra de servidor controlado usadas são especificações1 especificações2 especificações3

**Explicação:** Especificações de cifra são exibidas.

---

**ICA5019** Impossível obter conjunto Free Homenet IP.

**Explicação:** Problema de filtros dinâmicos.

---

**ICA5020** Impossível abrir arquivo de config de cliente remoto.

**Explicação:** O arquivo /etc/security/rcsfile.cfg não está disponível.

**Resposta do Usuário:** Verifique a presença do arquivo e seu conteúdo.

---

---

**ICA5021 Não é possível encontrar a palavra-chave 'palavra-chave'.**

**Explicação:** O arquivo /etc/security/rcsfile.cfg não possui esta palavra-chave.

**Resposta do Usuário:** Verifique e corrija o /etc/security/rcsfile.cfg.

---

**ICA5024 Erro da função skit\_secure\_soc\_write() em nome da rotina.**

**Explicação:** Falha do skit\_secure\_soc\_write() nesta rotina.

---

**ICA5025 Erro da função skit\_secure\_soc\_write() em ACKClient().**

**Explicação:** skit\_secure\_soc\_write() falhou na rotina ACKClient().

---

**ICA5026 Código de retorno inválido recebido do Cliente na nome da rotina.**

**Explicação:** Código de erro inesperado recebido do cliente nesta rotina.

---

**ICA5027 Código de retorno recebido para solicitação errada do Cliente em nome da rotina.**

**Explicação:** O código de retorno na mensagem de código de retorno é inesperado nesta rotina.

---

**ICA5028 Pedido de Login Inválido.**

**Explicação:** Formato da mensagem do pedido de login é inválido.

---

**ICA5030 ID de Cliente Remoto Desconhecida : ID do cliente remoto**

**Explicação:** Esta ID de usuário é desconhecida para a máquina do firewall.

**Resposta do Usuário:** Corrija informações do usuário para este cliente remoto.

---

**ICA5031 Erro da função skit\_secure\_soc\_write em RCTLoginPhase.**

**Explicação:** Falha do skit\_secure\_soc\_write() para fase de login.

---

**ICA5035 Solicitação de Saída de Sessão Inválida.**

**Explicação:** Formato da mensagem do pedido de logout é inválido.

---

**ICA5067 Pacote inválido recebido.**

**Explicação:** Formato do pacote recebido é inválido.

---

**ICA5078 Acessar solicitação não reconhecida em SvrReqHandler()**

**Explicação:** Recebida solicitação não-reconhecida e esta será ignorada.

---

**ICA5082 Túnel para o cliente ID do cliente remoto foi desconectado.**

**Explicação:** Túnel para o cliente remoto com esta ID foi desconectado.

---

**ICA5086 ID: id de usuário não definido.**

**Explicação:** Esta ID de usuário não existe na máquina do firewall.

---

**ICA5087 Autenticação falhou para 'id de usuário'.**

**Explicação:** Falha de autenticação para esta ID de usuário.

---

---

**ICA5089** A função `rcFilterClear()` falhou. O código de retorno é *código de retorno*.

**Explicação:** Falha de `rcFilterClear()` com este código de retorno.

**Resposta do Usuário:** Verifique a presença do cliente LAN IPSEC. Estes produtos não podem coexistir.

---

**ICA5090** A função `rcFilterInit()` falhou. O código de retorno é *código de retorno*

**Explicação:** Falha de `rcFilterInit()` com este código de retorno.

---

**ICA5091** A função `TunnelUp()` não pode processar o arquivo executável *linha de comando*.

**Explicação:** Falha da chamada `system()` na linha de comando exibida.

---

**ICA5092** Impossível obter senha do conjunto de chaves a partir da chamada de função `recoverstash`.

**Explicação:** Não é possível recuperar senha keyring do arquivo `stash`.

---

**ICA8001** SYSLOG/udp: serviço desconhecido

**ICA8002** Falha da função *nome de função - número do erro, número do erro 2 = 0x**número do erro 2*

**Explicação:** O processo é encerrado porque o `syslogd` não pôde executar a função especificada. A informação número do erro é anexada à mensagem de erro.

**Resposta do Usuário:** Entre em contato com o programador do sistema. Programador do Sistema :Utilize a informação número do erro para determinar a causa da falha.

---

**ICA8003** ICA8003 ICA8003;

**ICA8004** Erro detectado no soquete `AF_INET`, `Ö` `slogd` não monitorará mais o soquete

**ICA8005** ICA8005 ICA8005;

**ICA8006** Nome de prioridade desconhecido `Ö`"*prioridade*`Ö`"

**Explicação:** Um nome de prioridade encontrado no arquivo de configuração é inválido. :nota.Como este erro ocorreu antes do `syslogd` processar o arquivo de configuração do `syslog`, esta mensagem só aparece no console do operador.

**Resposta do Usuário:** Entre em contato com o programador do sistema. Programador do Sistema :Verifique o arquivo de configuração.

---

**ICA8007** Nome de recurso desconhecido `Ö`"*recurso*`Ö`"

**Explicação:** Um nome de recurso encontrado no arquivo de configuração é inválido. :nota.Como este erro ocorreu antes do `syslogd` processar o arquivo de configuração do `syslog`, esta mensagem só aparece no console do operador.

**Resposta do Usuário:** Entre em contato com o programador do sistema. Programador do Sistema :Verifique o arquivo de configuração.

---

**ICA8008** `Öb`Mensagem do SYSLOG§*nome de host em %2\$.24s...*

**Explicação:** O arquivo de configuração do daemon do `syslog` continha uma entrada para enviar mensagens do `syslog` a todos os usuários conectados. Esta mensagem será enviada a todos os usuários que estão atualmente conectados ao sistema no qual o daemon do `syslog` está executando.

**Resposta do Usuário:** Nenhum Programador do Sistema :Nenhum

---

---

**ICA8009    SYSLOGD saindo no sinal *sinal***

**Explicação:** O daemon do syslog recebeu um sinal que fez com que o daemon do syslog saísse.

**Resposta do Usuário:** Nenhum Programador do Sistema :Nenhum

---

**ICA8010    SYSLOGD reiniciou**

**ICA8011    ICA8011 ICA8011;**

**ICA8012    SYSLOGD não consegue registrar no SMF - *texto de erro***

**Explicação:** Um erro ocorreu durante a gravação de um registro no SMF. A informação de texto do erro é anexada à mensagem de erro.

**Resposta do Usuário:** Entre em contato com o programador do sistema. Programador do Sistema :Utilize a informação de texto do erro para determinar a causa da falha de gravação no SMF.

---

**ICA8013    Falha ao atualizar status do processo, código de retorno = 0x*código de retorno***

**Explicação:** Ocorreu um erro durante a tentativa de atualização do status do processo syslogd para o processo kernel do Firewall. O código de retorno resume o erro específico que foi retornado da chamada de atualização de status do processo.

**Resposta do Usuário:** Entre em contato com o programador do sistema. Programador do Sistema :Entre em contato com o representante de serviços.

---

**ICA8014    Opção desconhecida (*-opção de inicialização*) especificada na chamada SYSLOGD**

**Explicação:** Ocorreu um erro durante a tentativa de inicialização do processo do daemon syslogd. A opção especificada não é aceita na chamada do syslogd.

**Resposta do Usuário:** Verifique as opções de inicialização e reinicie o daemon do syslogd. Programador do Sistema :Se o problema continuar, entre em contato com o representante de serviços.

---

**ICA8015    Entrada inválida do arquivo de configuração (*dados de configuração*)**

**Explicação:** Ocorreu um erro durante a tentativa de análise de uma entrada de configuração do arquivo de configuração SYSLOG.

**Resposta do Usuário:** Verifique as entradas do arquivo de configuração e reinicie o daemon do syslogd. Programador do Sistema :Se o problema continuar, entre em contato com o representante de serviços.

---

**ICA8016    Falha de nome de função para nome de arquivo - *número do erro***

**Explicação:** Ocorreu um erro durante a tentativa de execução da função especificada para o dispositivo especificado. A informação de número do erro é anexada à mensagem de erro.

**Resposta do Usuário:** Verifique se o dispositivo especificado existe e tente novamente o pedido. Se o problema continuar, entre em contato com o programador do sistema. Programador do Sistema :Se o problema continuar, entre em contato com o representante de serviços.

---

**ICA9000    A avaliação do IBM Firewall expira em *número de dias*.**

**Explicação:** Este software está identificado como cópia de avaliação e vai desativar a si mesmo conforme indicado.

---

**ICA9001    Aviso de Verificador da Integridade do Sistema de Arquivos**  
               - *texto de descrição do aviso*

**Explicação:** fwfschk achou uma discrepância no sistema de arquivos - ameaça em potencial

---

**ICA9002    última mensagem repetida %1\$d vezes**

**Explicação:** Mensagem gerada pelo syslogd do AIX quando uma mensagem idêntica é iniciada sem nenhuma mensagem interveniente. A mensagem é mantida aqui para que o Monitor de Logs possa detectar a condição. Ela precisa estar no idioma em que a verdadeira mensagem syslogd esteja sendo escrita.

---

**ICA9003    A autenticação do usuário *nome* no servidor de configuração falhou.**

**Explicação:** O servidor de configuração do FW não consegue autenticar o usuário indicado.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9004    O usuário *nome* foi autenticado com sucesso no servidor de configuração.**

**Explicação:** O servidor de configuração do FW autenticou o usuário indicado.

---

**ICA9005    Iniciando o servidor de configuração remoto.**

**Explicação:** O servidor de configuração remoto foi iniciado.

---

**ICA9006    Encerrando o servidor de configuração remoto.**

**Explicação:** O servidor de configuração está sendo encerrado.

---

**ICA9007    O servidor de configuração remoto não consegue abrir o catálogo de mensagens.**

**Explicação:** Podem estar faltando um ou mais catálogos de mensagem usados pelo servidor de configuração remoto.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9008    O servidor de configuração remoto falhou em getpeername(): erro *número* do erro.**

**Explicação:** O servidor de configuração não consegue obter informações sobre o cliente.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9009    O servidor de configuração remoto falhou em getsockname(): erro *número* do erro.**

**Explicação:** O servidor de configuração não consegue obter informações sobre si mesmo.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9010    O servidor de configuração remoto não conseguiu obter informações do adaptador.**

**Explicação:** O servidor de configuração remoto não conseguiu obter informações do adaptador.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9011 O servidor de configuração não está habilitado para configuração remota.**

**Explicação:** O servidor de configuração possui definição local=sim em seu arquivo de configuração e o cliente está em máquina remota.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9012 O servidor de configuração remoto não consegue ler o pedido de logon.**

**Explicação:** O servidor de configuração não consegue ler o pedido de logon do cliente.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9013 O servidor de configuração remota recebeu pedido de logon incorreto.**

**Explicação:** O pedido de logon continha informações incorretas.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9014 O servidor de configuração remota não consegue criar canal.**

**Explicação:** O servidor de configuração não consegue criar canal para autenticação.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9015 O servidor de configuração remota não consegue criar processo.**

**Explicação:** O servidor de configuração não consegue criar processo para autenticação.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9016 Iniciando o daemon EFM.**

**Explicação:** O daemon EFM foi iniciado no firewall gerenciado.

---

**ICA9017 Encerrando o daemon EFM; rc = valor.**

**Explicação:** O daemon EFM está sendo encerrado com o código de retorno especificado.

---

**ICA9018 O daemon EFM não conseguiu abrir o catálogo de mensagens.**

**Explicação:** Podem estar faltando um ou mais catálogos de mensagem usados pelo daemon EFM.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9020 Não foi possível mudar a ID de usuário em execução.**

**Explicação:** Não foi possível fazer a chamada do sistema mudar a ID de usuário em execução.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9021 Este firewall não suporta modo *logon*.**

**Explicação:** Este firewall não suporta este modo em particular.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9022 O usuário não está autorizado a efetuar logon no firewall no *modo logon*.**

**Explicação:** Este nome de usuário não está autorizado a efetuar logon usando esse modo em particular.

**Resposta do Usuário:** Consulte o administrador do FW.

---

---

**ICA9023 Não foi possível carregar a DLL do EFM.**

**Explicação:** Falha no carregamento da dll do efm.

**Resposta do Usuário:** Consulte o administrador do FW.

---

**ICA9024 Solicitação de transferência iniciada por usuário para máquina do firewall.**

**Explicação:** O operação de transferência foi iniciada.

---

**ICA9025 O pedido de transferência terminou com código de retorno código de retorno.**

**Explicação:** A operação de transferência foi concluída.

---

**ICA9026 Solicitação de transferência recebida de usuário em máquina do firewall as horário.**

**Explicação:** A operação de transferência iniciou no horário especificado.

---

**ICA9027 O arquivo nome do arquivo na função função foi acrescentado ao pedido de transferência.**

**Explicação:** O arquivo especificado vai ser transferido.

---

**ICA9028 Solicitação de ativação iniciada por usuário em máquina do firewall.**

**Explicação:** O operação de ativação foi iniciada.

---

**ICA9029 A solicitação de ativação terminou com código de retorno código de retorno.**

**Explicação:** A operação de ativação foi concluída.

---

**ICA9030 Solicitação de ativação recebida de usuário em máquina do firewall as horário.**

**Explicação:** A operação de ativação iniciou no horário especificado.

---

**ICA9031 A ativação da função função foi encerrada com código de retorno código de retorno.**

**Explicação:** A ativação da função especificada foi concluída.

---

**ICA9032 Configuração do NAT atualizada as horário de data.**

**Explicação:** A configuração NAT foi atualizada.

---

**ICA9033 Suporte do NAT (nível versão.release) inicializado as horário de data.**

**Explicação:** O suporte NAT do Firewall foi inicializado.

---

**ICA9034 Suporte NAT desativado as horário de data.**

**Explicação:** NAT agora está desativado.

---

**ICA9035 O NAT não consegue alocar Endereço Registrado para Endereço Protegido Endereço de IP Protegido.**

**Explicação:** Endereço Registrado não foi convertido porque não há endereços disponíveis no conjunto de endereços de IP registrados.

---

**ICA9036 NAT liberou Endereço Registrado** *Endereço de IP Registrado para conjunto de endereços.*

**Explicação:** Endereço Registrado liberado para conjunto de endereços de IP registrados.

---

**ICA9037 Interfaces do firewall sendo atualizadas automaticamente em** *horário e data.*

**Explicação:** O programa de inicialização do Firewall chamou **UpdateInterfaces()** para acionar a atualização automática do arquivo de interfaces do Firewall, fwadpt.cfg.

**Ação do Sistema:** nenhum

**Resposta do Usuário:** nenhum

---

**ICA9038 O endereço da interface foi removido das configurações do Firewall.**

**Explicação:** O endereço de ponto decimal relacionado tinha sido relacionado no arquivo de config do Firewall fwadpt.cfg, mas não foi reconhecido pela pilha TCP e, assim, foi removido do arquivo config.

**Ação do Sistema:** nenhum

**Resposta do Usuário:** nenhum

---

**ICA9039 O endereço de interface foi incluído na configuração do Firewall.**

**Explicação:** O endereço de ponto decimal relacionado foi encontrado pela pilha TCP mas não tinha sido encontrado no arquivo de config do Firewall fwadpt.cfg e, assim, foi incluído no arquivo de config.

**Ação do Sistema:** nenhum

**Resposta do Usuário:** nenhum

---

**ICA9040 A máscara de endereço da interface foi atualizada de** *máscara velha para máscara nova.*

**Explicação:** A máscara no arquivo fwadpt.cfg não correspondeu ao que foi encontrado instalado no hardware. O campo de máscara correto foi atualizado no arquivo fwadpt.cfg.

**Ação do Sistema:** nenhum

**Resposta do Usuário:** nenhum

---

**ICA9041 Nenhuma interface foi encontrada nesta máquina.**

**Explicação:** Nenhuma interface de adaptador foi encontrada nesta máquina.

**Ação do Sistema:** nenhum

**Resposta do Usuário:** nenhum

---

## **Apêndice B. Robustecimento para a Configuração do Sistema Windows NT**

O robustecimento é um processo que maximiza a segurança e a eficiência por meio da desativação dos daemons desnecessários e das IDs de usuário não autorizadas. O robustecimento faz parte da instalação do software IBM Firewall e edita os recursos do sistema que podem comprometer a segurança.

Os serviços desnecessários à configuração do IBM Firewall e que se constituírem em uma ameaça em potencial para a segurança, são desativados. Todos os protocolos que não sejam TCP/IP são eliminados.



---

## Apêndice C. Obtenção de Pedidos para Comentários (RFCs)

Pedidos para comentários (RFCs) são documentos que apresentam novos protocolos e estabelecem padrões para a sequência de protocolos da Internet. Cópias de todos os RFCs estão disponíveis a partir do Network Information Center (NIC), tanto individualmente quanto em regime de assinatura. O endereço para obtenção desses documentos é:

Centro de Atendimento IBM  
Av. Pasteur, 138/146 - Botafogo  
22290-240  
Rio de Janeiro RJ  
Brasil

Os RFCs podem ser acessados na URL:

**<http://www.cis.ohio-state.edu/hypertext/information/rfc.html>**.

Para obter cópias online, solicite ao NIC (Network Information Center) usando o FTP para conectar-se a `ds.internic.net`. Os arquivos podem ser transferidos por meio do seguinte formato:

RFC:RFCnnnn.TXT  
RFC:RFCnnnn.PS

Onde:

nnnn      É o número RFC  
TXT        É o formato do texto  
PS        É o formato PostScript

O formato do índice RFC é:

RFC:RFC-INDEX.TXT

**Nota:** Muitos RFCs só estão disponíveis em formato de texto. Ao solicitar um arquivo PostScript, olhe antes o Índice do RFC para ter certeza de ele está disponível nesse formato. Também é possível solicitar cópias online dos RFCs pelo correio eletrônico, através do servidor de correio automatizado do NIC, enviando uma mensagem para `mailserv@ds.internic.net`. Inclua um dos seguintes comandos no corpo da nota:

SEND RFCnnnn.TXT  
ou  
SEND RFCnnnn.PS

Onde:

nnnn      É o número RFC  
TXT        É o formato do texto  
PS        É o formato PostScript

Eis um exemplo: para pedir o formato de texto do RFC 812, é preciso especificar no corpo da nota:

SEND RFC812.TXT

Para pedir uma cópia online do índice do RFC, inclua o seguinte comando no corpo da nota:

```
SEND RFC-INDEX.TXT
```

---

## Apêndice D. Formato do Arquivo de Configuração Socks5.conf do IBM eNetwork Firewall

O arquivo de configuração **socks5.conf** está localizado, por padrão, no diretório de instalação do IBM Firewall. Se você quiser, pode editar esse arquivo usando um editor de texto.

O arquivo de configuração **socks5.conf** é lido na primeira vez que o servidor é chamado. (Para atualizar sem interromper, digite `socks5.config`). Esse arquivo contém todas as informações que o IBM Firewall precisa para determinar qual interface usar para alcançar um dado endereço, se se deve conectar diretamente um dado endereço ou usar um outro servidor proxy e quais exigências precisam ser cumpridas para que seja realizada uma conexão proxy.

As seções a seguir aparecem no arquivo de configuração:

- Aliases
- Variáveis
- Módulos
- Autenticação
- Roteamento
- Proxies
- Controle de Acesso

Nas seções Autenticação, Roteamento, Proxies e Controle de Acesso, as linhas são lidas em ordem até ser encontrada uma correspondência para essa seção: a ordem das linhas é muito importante. Para que as linhas coincidam, todas as entradas da linha devem coincidir.

---

### Especificação de Portas

As portas podem ser especificadas usando um nome, número ou intervalo. Os intervalos começam com um `[` ou `(` e terminam com um `)` ou um `]` dependendo do fato do intervalo ser ou não inclusivo. Dentro dos delimitadores do intervalo devem estar dois especificadores de porta (nomes ou números), separados por uma vírgula. O método de especificação das portas é indicado como o *padrão da porta*.

---

### Especificação de Hosts

As máscaras de rede e os endereços do host são sempre necessários à especificação dos sistemas centrais que se aplicam a uma determinada regra. Esse método de especificação dos sistemas centrais é indicado como o padrão do host. Há vários modos de especificar o par host/máscara:

Parâmetro	Descrição
hostIP/ mask	Um endereço do host "ANDed" com a máscara deve ser igual ao IP do host "ANDed" com a máscara. Isso é geralmente usado para mascarar a porção de host do endereço com a porção de sub-rede ou rede.
-	Nada coincide. Todos os sistemas centrais são permitidos.
n1	Equivalente a n1.0.0.0/255.0.0.0.
n1.n2	Equivalente a n1.n2.0.0/255.255.0.0.
n1.n2.n3	Equivalente a n1.n2.n3.0/255.255.255.0.
.domain.name	O nome do host deve terminar com a cadeia .domain.name.
a.host.name	O nome de host deve corresponder exatamente ao a.host.name.

Há também suporte à sintaxe do padrão do host, conforme está descrito abaixo. Entretanto, o método mais recente é recomendado e mais fácil de ler.

Parâmetro	Descrição
hostIP/a	Nada coincide (o mesmo que "-"). Todos os sistemas centrais são permitidos.
hostIP/n	Rede coincide. Aplica máscara do host e das porções de sub-rede do endereço, deixando apenas a porção da rede. A máscara usada para fazer isso depende da classe do endereço de IP do host.
hostIP/s	Sub-rede coincide. Aplica máscara na porção de host do endereço, deixando apenas a porção da rede e sub-rede. A máscara usada para fazer isso depende da classe do endereço de IP do host.
hostIP/h	Host coincide. Equivalente ao IP do host.

## Especificação dos Métodos de Autenticação

Os métodos de autenticação enviados são *ibmcram* e *ibmpwd*. Outros podem ser acrescentados.

Os métodos de autenticação podem ser especificados como uma lista de métodos separada por uma vírgula. Para que uma linha coincida com outra, o método de autenticação escolhido tem de ser representado por um dos métodos da lista. Essa sintaxe é indicada como um padrão de autent. O método de autenticação NULO está definido a princípio. Outros métodos podem ser incluídos por meio do carregamento do(s) módulo(s) apropriado(s). Um "-" indica que qualquer método de autenticação, inclusive NULO, é aceitável.

---

## Entradas de Autenticação

As entradas de autenticação indicam o(s) tipo(s) de autenticação que podem ser usados. O formato é:

```
auth/ban source-address source-port
auth-methods
```

Parâmetro	Descrição
auth/ban	Se as entradas de autenticação estão autorizadas (auth) ou não (ban).
source-address	Um padrão de host válido.
source-port	Um padrão de porta válido.
auth-methods	Um padrão de autenticação válido.

A palavra-chave "ban" indica que a autenticação não deve ser nem tentada com esse host e não possui uso válido para o servidor especificado.

Se nenhuma linha auth/ban for especificada, o padrão será: qualquer método de autenticação é aceitável. Se as permissões da conexão forem definidas para *deny* (o padrão), a conexão não seria rejeitada até depois da autenticação ter sido aplicada. No protocolo SOCKS5, a autenticação coloca-se antes da autorização. Você deve decidir, com base somente no host, como esse sistema autenticará.

---

## Especificação de Comandos

Os comandos podem também ser especificados como uma lista delimitada por vírgula. Essa sintaxe é indicada como um padrão do comando. Os comandos definidos são: connect, bind, udp, ping e traceroute. Outros comandos podem ser incluídos via módulos. Um "-" (travessão) indica que qualquer comando é aceitável.

---

## Carregamento de Módulos

Os módulos permitem uma expansão personalizada para a funcionalidade do servidor por meio da inclusão de novos métodos de autenticação, comandos, verificações de autenticações e filtros de conteúdo. O formato é: *module stub filename options*

Parâmetro	Descrição
module	O identificador do módulo a carregar.
stub	Um prefixo de nome dependente do módulo para o acesso aos nomes de função.
filename	O nome de arquivo do módulo a carregar.
options	Informações de configuração específicas do módulo, caso haja alguma.

Os módulos podem definir campos usados em qualquer lugar, então é melhor colocar linhas de módulo primeiro. Por exemplo, os módulos de autenticação definem nomes do método de autenticação usados em linhas de auth e permit.

---

## Roteamento de Entradas

Em máquinas com várias interfaces de rede (conseqüentemente, endereços de IP), é desejável ter certeza de que certas interfaces de rede são usadas em conjunto com certos endereços. Isso evita o "IP spoofing" (máquinas externas à rede que aparentam ser máquinas internas à rede), por meio da certificação de que as máquinas internas usam a interface da rede interna e as máquinas externas usam a interface da rede externa. Ele também é usado pelo servidor SOCKS na determinação da interface de rede para ser ligada quando aceitar uma solicitação de BIND ou quando emitir uma solicitação de SENDTO. Caso nenhuma entrada coincida, o INADDR\_ANY é usado para ligar e uma conexão pode ser recebida em qualquer interface. Os sistemas centrais de home única não precisam ter entradas de roteamento: elas são necessárias apenas nas máquinas com mais de uma interface de rede. O formato é: **route** *dest-address dest-port interface-address*

Parâmetro	Descrição
route	Palavra-chave para indicar as entradas de roteamento.
dest-address	Um padrão de host válido.
dest-port	Um padrão de porta válido.
interface-address	O endereço de IP de uma placa de interface de rede, ou o nome da interface de rede (por exemplo: elnk31).

---

## Entradas de Variáveis

A quantidade e os tipos de mensagens informativas e de registro podem ser controlados por certas variáveis e sinalizadores no arquivo de configuração. O formato é: **set** *variable value*

Parâmetro	Descrição
set	Palavra-chave para definição das entradas da variável de ambiente para uso local.
variable	Uma variável de ambiente válida. Consulte "Variáveis de Ambiente" abaixo para obter uma listagem das variáveis disponíveis.
value	O valor a atribuir.

## Variáveis de Ambiente

Variável de Ambiente	Descrição
SOCKS5_BINDPORT [port]	Configura o IBM Firewall para usar a porta especificada, em lugar do padrão de porta 1080.
SOCKS5_RECVFROMANYONE	Se o suporte UDP estiver ativado, ela permite que os clientes UDP recebam mensagens de remetentes desconhecidos.
SOCKS5_USECLIENTSPORT	Configura o IBM Firewall apenas para proxy se ele puder ligar-se à mesma porta que o cliente usa para enviar mensagens. Isso é necessário para tornar as conexões UDP proxy, quando o servidor estiver deslocando dados ao cliente (enviando mensagens ao cliente antes do cliente enviar mensagens ao servidor). Um exemplo desse uso seria RealAudio.
SOCKS5_MAXCHILD	O número máximo de cadeias simultâneas.
SOCKS5_NOVERSEMAP	Desativa o mapeamento de endereços de IP aos nomes do host. Se os aliases estiverem atribuídos no arquivo de configuração, isso aumentaria o desempenho as custas de informações do registro.
SOCKS5_NOSERVICENAME	Desativa o mapeamento dos números de porta para nomes de serviço. Se os aliases estiverem atribuídos no arquivo de configuração, isso aumentaria o desempenho as custas de informações do registro.
SOCKS5_NOIDENT	Desativa solicitações IDENT, mesmo se compiladas. Isso é útil quando você possui uma ligação lenta com os clientes e eles não estão usando IDENTD. Isso reduzirá os períodos de timeout.
SOCKS5_DEMAND_IDENT	Configura a autenticação NULO para que falhe, se não houver nenhuma resposta IDENT dos clientes. Isso é útil para assegurar que um nome de usuário esteja sempre associado a uma solicitação de conexão.

## Entradas de Proxy

As entradas de proxy descrevem os endereços de servidores proxy SOCKS. Essas linhas informam ao servidor como contactar um determinado host. Se nenhuma linha corresponder a um host, o host será contactado diretamente. O formato é: *proxy-type dest-addr dest-port proxy-addr proxy-port*

Parâmetro	Descrição
proxy_type	O tipo de servidor proxy. As entradas válidas são: <ul style="list-style-type: none"> <li>• soquetes5</li> <li>• soquetes4</li> <li>• sem proxy</li> </ul>
dest-address	Um padrão de host válido.
dest-port	Um padrão de porta válido.
proxy-address	O endereço de IP ou o nome do servidor proxy.
proxy-port	A porta do servidor proxy em que o daemon SOCKS está aceitando as conexões.

## Entradas do Controle de Acesso

A seção do controle de acesso determina se uma solicitação para estabelecer uma conexão foi permitida ou negada. Há dois tipos de linhas, linhas de permissão e linhas de negação. Todas as entradas da linha devem coincidir para que toda a linha coincida. O formato é:

```
permit auth cmd src-host dest-host src-port dest-port [userlist]
deny auth cmd src-host dest-host src-port dest-port [userlist]
```

Parâmetro	Descrição
auth	Uma lista de métodos de autenticação, especificada por uma entrada de autenticação e padrão de autenticação válido.
cmd	Um padrão de comando válido que especifica os comando que estão em correspondência com essa linha.
scr-host	Um padrão de host válido para o host de origem.
dest-host	Um padrão de host válido para o host de destino.
scr-port	Um padrão de porta válido para a porta do host de origem.
dest-port	Um padrão de porta válido para a porta do host de destino.
userlist	Um padrão de usuário válido.

## Filtros

A filtragem através de um módulo carregado é realizada pelo filtro directivo. O formato é:

```
filter name auth cmd src-host dest-host src-port dest-port [userlist]
```

<b>Parâmetro</b>	<b>Descrição</b>
name	O identificador do módulo de filtro.
auth	Uma lista de métodos de autenticação, especificada por uma entrada de autenticação e padrão de autenticação válido.
cmd	Um padrão de comando válido que especifica os comando que estão em correspondência com essa linha.
scr-host	Um padrão de host válido para o host de origem.
dest-host	Um padrão de host válido para o host de destino.
scr-port	Um padrão de porta válido para a porta do host de origem.
dest-port	Um padrão de porta válido para a porta do host de destino.
userlist	Um padrão de usuário válido.



---

## Bibliografia

Para obter informações adicionais sobre segurança na Internet, visite a home page do IBM 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.

- *Guia do Usuário IBM eNetwork Firewall*, GC17-1348-00
- *IBM eNetwork Firewall Referência*, SC17-1349-00

### 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 pertencem ao sendmail, 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 com 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, William 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)

---

## Avisos

As referências contidas nesta publicação a produtos, programas ou serviços da IBM não significam que a IBM pretenda comercializá-los em todos os países onde opera. Qualquer referência a um produto, programa ou serviço IBM não significa que apenas os produtos, programas ou serviços IBM possam ser utilizados. Sujeito aos direitos de propriedade intelectual válidos IBM ou outros direitos protegidos legalmente, qualquer produto, programa ou serviço funcionalmente equivalente poderá ser usado em vez de produtos, programas ou serviços IBM. A avaliação e a verificação da operação em conjunto com outros produtos, exceto aqueles expressamente designados pela IBM, são de responsabilidade do usuário.

A IBM pode ter patentes ou solicitações de patentes relativas a assuntos tratados neste documento. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença podem ser enviados, por escrito, ao:

Gerente de Relações Industriais e Comerciais da  
IBM  
Av. Pasteur, 138 / 146  
22290-240  
Botafogo 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:

Centro de Atendimento IBM:  
Av. Pasteur, 138/146  
22290-240 Botafogo  
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).

Esta publicação não foi planejada para uso de produção e é fornecida como está, sem garantia de qualquer tipo. Todas as garantias são por este documento negadas, inclusive garantias de comercialização e capacidade para um determinado objetivo.

Este produto inclui o software desenvolvido pela Universidade da Califórnia, Berkeley e seus colaboradores.

---

## Marcas

Os seguintes termos são marcas da IBM Corporation nos Estados Unidos e/ou em outros países:

- 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.

UNIX é uma marca nos Estados Unidos e outros países licenciada exclusivamente pela X/Open Company Limited.

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.



---

## Glossário

É possível acessar o glossário de Software IBM em:  
<http://www.networking.ibm.com/nsg/nsgmain.htm>.



---

# Índice Remissivo

## Caracteres Especiais

(MKKF), Utilização do Utilitário Make Key File 57  
(RFCs), Pedidos para comentários 143

### A

a\_alert.tbl 23  
acordo de licenciamento 155  
ADMIN\_ALERT 27  
arquivo de chaves, Criando um 57  
Autenticação Fornecida pelo Usuário 47  
Autenticação, Fornecida Pelo Usuário 47

### B

bibliografia 153

### C

Centro de Suporte IBM vii  
Centro de Suporte, IBM vii  
Consultas de Exemplo 26  
Consultas, Exemplo 26  
Controle de Tráfego 69  
Criação do Arquivo de Chaves 57

### D

DB2 24  
DB2/6000 ou DB2/2 21  
Dispositivos do Log 70

### E

endereços de IP, como fornecer vii

### F

f\_info.tbl 23  
f\_match.tbl 23  
f\_rule.tbl 23  
f\_stat.tbl 23  
FILTER\_ACTIVE\_RULE 27  
FILTER\_INFO 27  
FILTER\_MATCH 27  
FILTER\_STATUS 27  
Filtros 3  
fornecer endereços de IP, como vii  
fwfilter 3  
fwimport.dat 21  
fwinterface 4

fwlog 5  
fwlogcvrt 21  
fwlogmon 8  
fwlogtbl 21, 22  
fwlogtxt 21  
fwmail 10  
fwqrysmp.dml 21  
fwschema.ddl 21, 25  
fwuser 15

### G

Geração de Mensagens 23  
Gerenciamento de Arquivo de Log 5  
Gerenciamento de Arquivo, Log 5  
Gerenciamento, Arquivo de Log 5  
Grupos Funcionais de Administração 18  
Grupos, Administração Funcionais 18

### I

Identificação de Problemas e Testes 65  
Interface de Linha de Comando 1  
Interfaces 4, 27  
interfaces.tbl 23

### L

log do firewall 21  
log, firewall 21

### M

métodos de autenticação 47  
métodos, autenticação 47  
mensagens 73  
Mensagens, Geração 23  
Monitor de Log 7

### N

NAT\_INFO 27  
nat\_info.tbl 23

### O

O proxy HTTP 3

### P

p\_ftp.tbl 23  
p\_http.tbl 23

- p\_info.tbl 23
- p\_login.tbl 23
- p\_stat.tbl 23
- PAGER\_INFO 27
- Página Web 153
- Parâmetros Fundamentais 15
- Parâmetros, Fundamentais 15
- Pedidos para comentários (RFCs) 143
- Problemas de DNS 66
- PROXY\_FTP 27
- PROXY\_HTTP 27
- PROXY\_INFO 27
- PROXY\_LOGIN 27
- PROXY\_STATUS 27
- proxy, HTTP 3

## R

- referências 153
- robustecimento 141

## S

- s\_ftp.tbl 24
- s\_info.tbl 24
- SERVER\_INFO 27
- server\_info.tbl 23
- Serviços de Nome de Domínio 2
- Serviços de Nome, Domínio 2
- Serviços, Nome de Domínio 2
- Servidor de Configuração 1
- Servidores Proxy 69
- SESSION 27
- session.tbl 23
- SOCKS\_FTP 27
- SOCKS\_INFO 27
- SSL\_INFO 27
- ssl\_info.tbl 24
- SU 27

## T

- Tabelas SQL 26
- Tabelas, SQL 26
- TUNNEL\_CONTEXT 27
- TUNNEL\_POLICY 27
- TUNNEL\_STATUS 27

## U

- um arquivo de chaves, Criação 57
- URLs 153
- utilitários de relatório 21, 70
- utilitários, relatório 21
- Utilização do Utilitário Make Key File (MKKF) 57
- Utilização dos Utilitários de Relatório 21

---

# Comentários do Leitor

**IBM eNetwork Firewall for Windows NT**

**Referência**

**Versão 3 Release 2**

**Publicação Nº SC17-1349-00**

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



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





Impresso na Dinamarca.

SC17-1349-00

