IBM SecureWay Boundary Server
para Windows NT e AIX

Instalação e Uso

Versão 2.0

IBM SecureWay Boundary Server
para Windows NT e AIX

Instalação e Uso

Versão 2.0

Nota

Antes de utilizar estas informações e o produto suportado por elas, leia as informações gerais no Apêndice B, “Avisos” na página 41.

Este edição se aplica à Versão 2, release 0, modificação 0 do produto IBM SecureWay Boundary Server e a todos os releases e modificações subseqüentes a menos que indicado de outra forma em novas edições.

Segunda Edição (Outubro de 1999)

Índice

Sobre este manual

Este manual descreve como planejar, instalar, configurar, utilizar e solucionar problemas do IBM SecureWay Boundary Server para Windows NT e AIX.

É importante que você possua conhecimento profundo sobre firewalls, redes privadas virtuais, segurança de conteúdo e administração de rede para instalar e configurar o SecureWay Boundary Server. Devido ao fato de você ter que instalar e configurar um firewall que controla o acesso de entrada e saída da rede, você deve antes compreender como a rede opera. Especialmente, você deve compreender as noções básicas de endereços IP, nomes completos e máscaras de sub-rede.

Quem deve ler este manual

Este manual é destinado a administradores de rede ou de segurança de sistema que instalam, administram e utilizam o IBM SecureWay Boundary Server.

Preparação para o ano 2000

Estes produtos estão preparados para o Ano 2000. Quando utilizado de acordo com a documentação associada, eles são capazes de processar, fornecer e receber dados de data entre os séculos vinte e vinte e um, desde que todos os produtos (por exemplo, hardware, software e firmware) utilizados com os produtos realizem troca correta de dados de data com eles.

Serviço e suporte

Entre em contato com a IBM para obter serviços e suporte para todos os produtos incluídos com o produto IBM SecureWay FirstSecure. Alguns destes produtos podem fazer referência a suporte não-IBM. Se você obtiver estes produtos como parte do produto FirstSecure, entre em contato com a IBM para obter serviços e suporte.

Como este manual é organizado

Este manual contém os seguintes capítulos:

O Capítulo 1, “Visão Geral do SecureWay Boundary Server” na página 1 fornece uma visão geral do produto SecureWay Boundary Server e seus componentes.

O Capítulo 2, “Apresentação do IBM SecureWay Boundary Server” na página 5 informa porque o produto SecureWay Boundary Server é necessário.

O Capítulo 5, “Instalação e Configuração do SecureWay Boundary Server” na página 21 descreve a instalação e configuração do produto SecureWay Boundary Server nos sistemas operacionais Windows NT e AIX.

O Capítulo 3, “Para Instalar o SecureWay Boundary Server” na página 11 fornece informações sobre como planejar para o produto SecureWay Boundary Server.

O Capítulo 4, “Requisitos para o IBM SBS (SecureWay Boundary Server)” na página 17 fornece informações sobre os requisitos mínimos para o produto SecureWay Boundary Server.

O Capítulo 6, “Documentação Relacionada” na página 35 informa onde encontrar outras documentações para o produto SecureWay Boundary Server e documentações para produtos relacionados.

Convenções

Este manual utiliza as seguintes convenções:

Convenção	Significado
negrito	Elementos de interface do usuário, como caixas de opções e comandos
monoespaçado	Padrões de sintaxe e de diretório que são relevantes para o produto SecureWay Boundary Server
->	Mostra uma série de seleções de um menu. Por exemplo: Selecione **Arquivo-> Executar** significa clicar em **Arquivo** e depois clicar em **Executar**

Informações da Web

Informações sobre atualizações recentes do produto SecureWay Boundary Server estão disponíveis no seguinte endereço da Web:

http://www.ibm.com/software/security/boundary/library

Informações sobre atualizações de outros produtos IBM SecureWay FirstSecure estão disponíveis no seguinte endereço da Web:

http://www.ibm.com/software/security/firstsecure/library

O que há de novo?

A Versão 2.0 do SecureWay Boundary Server contém vários recursos novos. Os novos recursos mais importantes estão listados aqui.

Integração com o produto SecureWay Policy Director

O produto SecureWay Policy Director pode gerenciar usuários de Proxy Firewall, se o Firewall estiver ativado para o produto SecureWay Boundary Server. Usuários de Proxy Firewall são definidos para os seguintes serviços de Firewall:

Telnet

FTP

HTTP

Socks

Os usuários e seus critérios associados são armazenados em um banco de dados LDAP (Lightweight Directory Access Protocol).

O produto SecureWay Directory fornece LDAP para manter as informações do diretório em uma localização central para armazenamento, atualizações, recuperação e troca. O produto SecureWay Policy Director gerencia os usuário proxy Firewall no banco de dados LDAP.

Eficiências de Roteamento

As eficiências de roteamento utilizam um plugin Finjan SurfinGate para tráfego de rede de circuito curto para filtragem de conteúdo.

Bloqueio de Invasão

Programas de linha de comando para criar regras DENY dinâmicas no Firewall. O bloqueio de invasão pode ser integrado em um script automatizado.

IBM SecureWay Firewall 4.1

O produto IBM SecureWay Firewall para Windows NT oferece:

Remote Access Service

O RAS (Remote Access Service) do Windows NT fornece conexões de rede através de mídia dial-up, ISDN ou X.25 utilizando PPP (Point-to-Point ProtocoL). NDISWAN é um driver de acesso à rede que é fornecido como parte do RAS e converte os dados PPP subjacentes para que fiquem semelhantes a dados de LAN Ethernet.

Aperfeiçoamentos do IBM SecureWay Firewall para AIX 4.1

O produto IBM SecureWay Firewall para AIX oferece:

Enhanced IPSec Support

O produto IBM SecureWay Firewall 4.1 inclui suporte IPSec avançado incluindo criptografia DES tripla, suporte para novos cabeçalhos. Ele também suporta capacidade de interoperação com vários servidores e roteadores IBM, bem como vários produtos VPN não-IBM que suportam novos cabeçalhos.

SMP (Symmetric Multi-Processor)

Os usuários do Firewall podem aproveitar os recursos de multiprocessador do RS/6000 para ajuste de escala e aperfeiçoamentos de desempenho.

Aperfeiçoamento de Filtros

Os filtros foram aperfeiçoados para fornecer melhor desempenho com configuração. Você pode ajustar o desempenho de seu Firewall escolhendo onde localizar tipos diferentes de regras de filtro. Além disso, o número de vezes que uma conexão utilizada é registrado.

Assistente de Configuração

Um assistente auxilia na configuração inicial do produto IBM SecureWay Firewall. Este assistente de configuração permite que novos usuários possuam uma configuração básica de Firewall rapidamente, após a instalação do produto IBM Firewall.

Network Security Auditor

O NSA (Network Security Auditor) verifica se há furos ou erros de configuração em seus servidores de rede e no Firewall. Ele foi aperfeiçoado para ser mais rápido e mais robusto.

National Language Support para Alemão

O serviço National Language Support para Alemão agora é oferecido, além do Português do Brasil, Português, Inglês, Francês, Italiano, Japonês, Coreano, Chinês simplificado, Espanhol e Chinês tradicional.

Network Address Translation O NAT (Network address translation) foi aperfeiçoado para suportar mapeamentos de endereços de vários remetentes. Estes mapeamentos são de vários endereços particulares ou não registrados internos para um endereço legal registrado utilizando números de porta para criar mapeamentos únicos.

Funções comuns suportadas pelo AIX e pelo Windows NT

Security Dynamics ACE/Server

A função Security Dynamics ACE/Server fornece dois fatores de autenticação. Este recurso foi aperfeiçoado e protege sua rede e seus recursos de dados contra invasões acidentais ou propositais potencialmente devastadoras.

Aperfeiçoamentos do Secure Mail Proxy

A função IBM Firewall Secure Mail Proxy foi aperfeiçoada para incluir as novas funções a seguir:

Algoritmo Anti-SPAM incluindo bloqueio de mensagens de SPAMers conhecidos (uma lista de exclusão), marcas de verificação para validade e capacidade de resposta das mensagens (maneiras conhecidas de bloqueio de mensagens não desejadas), limites configuráveis do número de destinatários de mensagens de e-mail, limites configuráveis do tamanho máximo de uma mensagem.

Suporte contra fraude incluindo integração com mecanismos de autenticação potentes

Suporte a trap SNMP e suporte ao MADMAN MIB

Rastreamento de mensagens incluindo a habilidade para rastrear mensagens diretamente entre firewall e Domino

Aperfeiçoamento do Protocolo Socks Versão 5

O protocolo Socks versão 5 foi atualizado para incluir UNPW (autenticação de senha de ID de usuário), CRAM (autenticação de desafio/resposta) e plug-ins de autenticação.

O registro em log foi aperfeiçoado para fornecer ao usuário maior controle sobre a classificação de mensagens registradas e na especificação de níveis de log.

Proxy HTTP

O produto IBM SecureWay Firewall fornece uma implementação proxy HTTP com funções completas baseadas no produto WTE (IBM Web Traffic Express). O proxy HTTP identifica eficientemente pedidos de navegador através do IBM Firewall, eliminando a necessidade de um servidor socks para navegação na Web. Os usuários podem acessar informações úteis na Internet, sem comprometer a segurança de suas redes internas. O navegador deve ser configurado para utilizar um proxy HTTP.

MIMEsweeper 2.0 para SecureWay

O produto MIMEsweeper possui três componentes principais: **MAILsweeper 4.1_2**, **WEBsweeper 3.2_5** e **WEBsweeper 1.0_2**. Alguns aperfeiçoamentos são:

MAILsweeper

O produto MAILsweeper 4.1_2 para SMTP é a atualização principal para o produto MIMEsweeper sinalizador da Content Technologies. Ele oferece os seguintes recursos novos:

Uma arquitetura de critério hierárquico de fácil utilização fornece a flexibilidade para aplicar critérios no nível organizacional apropriado diretamente para o usuário individual

Uma GUI (interface gráfica com o usuário) de padrão industrial simplifica a configuração do software, a criação de critérios e a administração

O novo recurso Split Delivery é uma função da implementação de critério hierárquico da versão 4. Para mensagens com destinatários múltiplos, os critérios são aplicados para cada destinatário. Destinatários autorizados recebem a mensagem e destinatários não autorizados são negados

O processamento de mensagens de encadeamento múltiplo melhora o rendimento e adiciona força, permitindo que o processamento da mensagem continue, utilizando encadeamentos restantes, caso ocorra um erro em um ou mais encadeamentos

Em conjunto com produtos anti-vírus de outros fornecedores, o MAILsweeper fornece detecção e limpeza de vírus em mensagens e anexos.

Análise de texto avançada utilizando as expressões NEAR, AND, NOT, e OR fornece grande flexibilidade na criação de cenários abrangentes e efetivos, baseados na sintaxe ou arquitetura de mensagens.

Ferramentas de auditoria aperfeiçoadas que podem enviar dados para qualquer banco de dados compatível com DBC

Suporte ao servidor RBL (Real-Time Black List) que lista sites conhecidos por enviar e-mail inútil. O MAILsweeper pode recusar a aceitar conexões de todos os hosts presentes nesta lista

Segurança de conteúdo é mais fácil de ser gerenciada através de relatórios/gráficos/tabelas atrativos de tráfego de e-mail

Integração com diretórios LDAP

A função DSN (Delivery Service Notification) agora suporta SNMP e NT Alerter

WEBsweeper

Aperfeiçoamentos de desempenho adicionais melhoram a velocidade de processamento de dados.

Trabalha com Virus Scanners para tráfegos HTTP e FTP

WEBsweeper HTTPS

O produto WEBsweeper agora fornece suporte completo para aplicativos de e-commerce baseados na web através de uma nova solução de proxy HTTPS

SurfinGate 4.05

Os aperfeiçoamentos do produto SurfinGate incluem:

Inspeção de Conteúdo JavaScript

O produto SurfinGate 4.05 procura operações de JavaScript potencialmente problemáticas e pára JavaScripts que apresentem conflito com critérios de segurança corporativos O produto SurfinGate 4.05 permite que administradores definam e fortaleçam centralmente um critério para JavaScript, Java e ActiveX, com filtragem inteligente para VisualBasic Script e cookies.

Monitoramento de Desempenho Crítico para a Missão

O produto SurfinGate 4.05 inclui uma ferramenta automática que detecta comportamento anormal (como erros de tempo de execução) e reinicia o SurfinGate no caso de falha. Este é um recurso de segurança essencial para áreas de missão críticas.

Gerenciamento de Critério Ampliado

O produto SurfinGate insere perfis de applets não resolvidos no banco de dados para bloqueio automático. Os administradores podem editar a lista de applets/controles.

Suporte para Protocolo FTP e SSL

O produto SurfinGate 4.05 monitora canais de FTP (File Transfer Protocol) para código móvel, vigiando códigos que poderiam, de outro modo, entrar pela Internet. Além de FTP, o produto SurfinGate monitora tráfego HTTP para código móvel e passa tráfego HTTPS para dispositivos adicionais.

Interação de plugin com proxy HTTP firewall

O produto SurfinGate funcionará como um proxy em uma corrente proxy ou através de um plugin do Web Traffic Express no Firewall para Windows NT.

Capítulo 1. Visão Geral do SecureWay Boundary Server

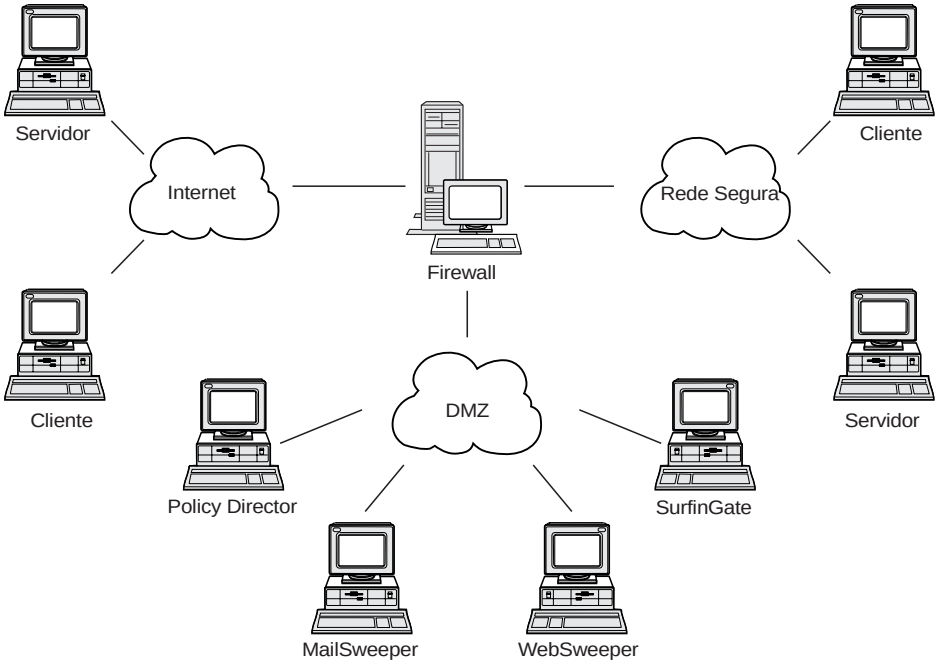

Figura 1. Um exemplo de uma configuração do IBM SecureWay Boundary Server

Este exemplo diagrama cinco estações de trabalho utilizando componentes dos produtos MAILsweeper, WEBsweeper, Policy Director e SurfinGate para monitorar e rotear tráfego da web e de correio entre clientes e servidores utilizando um Firewall. Para este exemplo, utilizaremos cinco estações de trabalho separadas fisicamente.

Exemplos Típicos de SecureWay Boundary Server

Recomendamos que você utilize as seguintes máquinas para uma configuração mínima:

Tabela 1. Requisitos de hardware para produtos do componente Boundary Server

Produto	**Máquina**
IBM Firewall	Windows NT ou AIX
MAILsweeper	Windows NT
WEBsweeper	Windows NT
SurfinGate	Windows NT

Se você deseja tirar toda a vantagem do produto SecureWay Boundary Server, o SecureWay Policy Director deve estar instalado em sua rede. Isto permite que usuários proxy Firewall sejam armazenados no SecureWay Directory (LDAP).

Exemplo HTTP (Firewall do Windows NT): Em um cenário típico, um pedido HTTP de conteúdo na Internet seria originado na máquina cliente. O pedido seguiria primeiro para o produto WEBsweeper. No caminho de transmissão, o WEBsweeper faria o proxy do pedido para o HTTP do Firewall.

No proxy HTTP do Firewall, o usuário seria autenticado. Se este for o primeiro pedido da sessão de navegação do cliente, um desafio de ID/Senha de Usuário será apresentado. O ID de Usuário seria utilizado para procurar o critério de segurança do cliente no banco de dados LDAP administrado pelo Policy Director. Dependendo do critério de autenticação HTTP para o cliente e do resultado da verificação da senha digitada, o pedido pode ser negado, ou permitido a continuar. A operação de autenticação pode requerer acessos adicionais ao banco de dados LDAP ou ao servidor Security Dynamics ACE. Em pedidos subseqüentes da mesma sessão de navegação, o navegador fornecerá o ID/Senha de Usuário automaticamente. O cliente não será desafiado, mas cada pedido ainda será autenticado através do mesmo processo utilizado para o primeiro pedido.

Se a autenticação for bem-sucedida será feito o proxy do pedido ao servidor solicitado na Internet.

Quando o conteúdo do servidor da Internet for recebido de volta no proxy HTTP do Firewall, ele será examinado pelo plugin SurfinGate. Informações de grupo do usuário, obtidas a partir do banco de dados LDAP, serão disponibilizadas para o plugin se basear em decisões de critério. Se o conteúdo não for de interesse para o SurfinGate, ele passa rapidamente pelo plugin, com sobrecarga de processamento mínima. Conteúdo incluindo JavaScript será filtrado no plugin. Conteúdo incluindo Java ou ActiveX será encaminhado para o servidor SurfinGate para filtragem e o conteúdo filtrado será devolvido para o proxy HTTP da Firewall. O conteúdo resultante do processamento do plugin SurfinGate será enviado de volta para o servidor WEBsweeper.

Quando o conteúdo voltar para o servidor WEBsweeper, ele será filtrado de acordo com os critérios do WEBsweeper e devolvido para o cliente.

Exemplo HTTP (Firewall do AIX): No AIX o fluxo de tráfego é essencialmente idêntico, exceto pelo fato de não haver plugin SurfinGate disponível para o Firewall do AIX. Portanto, o servidor SurfinGate deve ser definido como um proxy em uma cadeia proxy do cliente para o Firewall. O WEBsweeper deve ser configurado para encaminhar pedidos para o servidor SurfinGate ao invés de enviar diretamente para a proxy HTTP do Firewall. O servidor SurfinGate deve, então, ser configurado para encaminhar pedidos para o proxy HTTP do Firewall. Não haverá informações de grupo disponíveis no servidor SurfinGate, portanto, as decisões de critério podem ser baseadas apenas em endereço IP.

Exemplo de Correio: O MAILsweeper é configurado como um gateway de correio. O correio que chega no servidor MAILsweeper tem seu conteúdo filtrado antes de ser encaminhado para o próximo servidor de correio.

Cada servidor de correio seguro deve ser configurado para encaminhar pedidos de correio de cliente para o servidor MAILsweeper. O Firewall mail exchanger deve ser configurado para encaminhar correio recebido para o servidor MAILsweeper.

O MAILsweeper deve ser configurado para enviar correio endereçado para qualquer domínio externo ao Firewall mail exchanger. O MAILsweeper deve ser configurado para enviar correio endereçado para domínios internos ao servidor de correio seguro correto.

Capítulo 2. Apresentação do IBM SecureWay Boundary Server

Este capítulo apresenta uma visão geral do SecureWay Boundary Server e inclui as seguintes seções:

O que é o SecureWay Boundary Server?

O IBM SecureWay Boundary Server reúne, pela primeira vez, uma solução de segurança de limite completa. O produto SecureWay Boundary Server fornece proteção de firewall, VPN (virtual private networking) e segurança de conteúdo. O produto SecureWay Boundary Server reúne tecnologia da indústria de segurança em uma solução integrada com o apoio do suporte e serviços IBM. Esta solução inclui:

IBM SecureWay Firewall 4.1 (inclui Security Dynamic ACE/Server)

MIMEsweeper da Content Technologies

- MAILsweeper 4.1_2
- WEBsweeper 3.2_5
- WEBsweeper HTTPS proxy 1.0_2

SurfinGate 4.05 da Finjan

- SurfinGate Server
- SurfinConsole
- Banco de dados SurfinGate
- Integração SurfinGate Plugin for WTE para Windows NT 1.0

Porque o SecureWay Boundary Server é Necessário?

Limites seguros são necessários em todos os lugares – entre departamentos, como engenharia e recursos humanos, redes da matriz e escritórios remotos, a rede de sua empresa e a Internet, os aplicativos da Web de sua empresa e os clientes, a rede ou os aplicativos de sua empresa e parceiros comerciais. A segurança de limites não protege apenas sua rede, seus aplicativos e informações, mas também estende seu alcance. A segurança de limites apropriada requer controle tanto de quem pode acessar sua rede como de quais informações entram ou saem de sua rede.

Como o SecureWay Boundary Server se Ajusta ao FirstSecure?

O IBM SecureWay FirstSecure é um pacote de produtos integrados. Ele fornece uma estrutura ampla para ajudá-lo a proteger a todos os aspectos de acesso à rede através da Internet e de outras redes. Ele ajuda a aproveitar seus investimentos atuais com ofertas modulares e interoperáveis e a minimizar o custo total de propriedade realizando e-business seguro. Ele fornece proteção contra vírus, controle de acesso, controle de conteúdo de tráfego, criptografia, certificados digitais, firewall, kits de ferramenta e serviços de implementação.

O Boundary Server é um pacote de produtos que se ajusta ao FirstSecure. Ele cria um limite para a Internet que pode ser utilizado para bloquear vírus potencialmente perigosos (utilizando produtos de detecção de vírus suplementares), JavaScript, applets Java, controles ActiveX e até correio não desejado (SPAM). Com o produto Boundary Server, você controla exatamente o que pode entrar em sua rede pela Internet. Com o produto SecureWay Policy Director, você gerencia usuários de proxy Firewall e seus critérios de autenticação.

Quais são os Componentes do SecureWay Boundary Server?

Os três componentes do produto SecureWay Boundary Server são IBM Firewall, MIMEsweeper e SurfinGate. O produto SecureWay Boundary Server fornece integração com o produto IBM SecureWay Policy Director.

Visão Geral do IBM SecureWay Boundary Server

O IBM SecureWay Boundary Server fornece a grandes organizações proteção, controle de acesso e segurança de conteúdo necessários para que e-business seja aproveitado, abrindo com segurança sua empresa a clientes, fornecedores e parceiros. Os recursos incluem:

Proteção de Firewall para sua rede

VPN (Virtual Private Networking) para estender o alcance de sua rede

Scanner de conteúdo para correio e tráfego da web para proteger os dados, a imagem, a confiabilidade e produtividade de sua empresa

O produto SecureWay Boundary Server reúne o melhor da tecnologia da indústria em uma solução integrada com o apoio do suporte e serviços IBM. Ele está disponível para os sistemas operacionais AIX e Windows NT.

Função do SecureWay Boundary Server

O SecureWay Boundary Server aplica filtragem de pacote, proxies e tecnologia de servidor Socks e segurança de conteúdo para ocultar e proteger sua rede e seu sistema. Estas tecnologias permitem que administradores definam explicitamente quais dados possuem permissão para passar para dentro e para fora de sua rede. Isto ajuda a evitar tentativas de "ataques de negação de serviço" e hackers de penetrar na rede e limita responsabilidades legais. O produto SecureWay Boundary Server oferece uma solução VPN para permitir que você substitua servidores remotos e bancos de modem com uma solução baseada na Internet.

Quando implementado com o Policy Director, o produto SecureWay Boundary Server oferece autenticação de usuários utilizando um esquema central baseado em critérios. O software anti-vírus pode ser utilizado com o SecureWay Boundary Server para fornecer proteção contra vírus para seu site.

Visão Geral do IBM SecureWay Policy Director

O produto Policy Director é uma solução de gerenciamento de segurança e autorização independente que fornece segurança de extremidade a extremidade para recursos através de intranets e extranets geograficamente dispersadas. Uma extranet é uma VPN (virtual private network) que utiliza controle de acesso e recursos de segurança para restringir a assinantes selecionados a utilização de uma ou mais Intranets conectadas à Internet. O produto Policy Director fornece autenticação, autorização, segurança de dados e gerenciamento de recursos e serviços. O produto Policy Director é utilizado em conjunto com aplicativos padrão baseados na Internet para criar intranets e extranets seguras e bem gerenciadas.

Função do IBM SecureWay Policy Director

Quando utilizado com o SecureWay Boundary Server, o produto IBM SecureWay Policy Director fornece armazenamento de critérios de usuário proxy e informações de autenticação.

Visão Geral do IBM SecureWay Firewall

O IBM SecureWay Firewall é um programa de segurança de rede. Um firewall é um bloqueio entre uma ou mais redes privadas internas seguras e outras redes ou a Internet. Um firewall evita comunicações não desejadas ou não autorizadas para dentro ou para fora da rede segura.

Função do IBM SecureWay Firewall

O produto IBM SecureWay Firewall restringe o acesso entre uma rede protegida, a Internet e outros conjuntos de redes. Ele também faz o seguinte:

Restringe as pessoas que entram em um ponto controlado cuidadosamente

Evita que invasores se aproximem de outras defesas

Restringe as pessoas que saem de um ponto controlado cuidadosamente

Firewalls internos segregam informações internas sensíveis de funcionários não autorizados

Restringe qual tráfego pode entrar e sair da rede

Visão Geral do produto MIMEsweeper

O produto MIMEsweeper fornece Segurança de Conteúdo, analisando os dados que passam pelo Firewall através de correio eletrônico ou da world wide web. A Segurança de Conteúdo permite que as organizações gerenciem efetivamente questões da empresa relacionadas ao uso de e-mail e da world wide web. Estas questões podem ser divididas em integridade de rede e integridade da empresa.

A filtragem para integridade da rede pode:

Identificar e remover vírus em e-mail recebido e enviado

Filtrar tipos de arquivos não desejados

Gerenciar arquivos de tamanho excessivo

Proteger redes de congestionamento ou perda de serviço de ataques por correio-bomba

A filtragem para integridade da empresa pode:

Evitar transgressão de confidencialidade e perda de segredos comerciais

Limitar exposição a responsabilidade legal

Reduzir perda por utilização imprópria de serviços de e-mail e da world wide web por funcionários

Proteger contra perda de serviço de rede através de utilização imprópria e ataques hostis

Ameaças à integridade da rede podem corromper ou apagar dados, interromper o fluxo de e-mail e destruir hardware do sistema, fatos que podem resultar em tempo de inatividade da rede, perda de produtividade e custos altos de limpeza e recuperação.

Ameaças a integridade de negócios, entretanto, podem ser ainda mais destrutivas, resultando em enormes custos legais, perda de propriedade intelectual e danos à reputação e credibilidade da empresa. Questões de integridade da empresa podem causar uma paralisação em suas operações comerciais.

O MIMEsweeper é o produto líder da indústria para proteger organizações de questões de integridade de rede e comerciais impostos pela utilização de e-mail e da Internet da organização.

Funções do MIMEsweeper

O produto MIMEsweeper pode:

Adicionar restrições legais à transmissão de e-mail

Proteger documentos e dados confidenciais

Autorizar e controlar usuários baseados em e-mail e na web

Isolar ou bloquear material ofensivo

Bloquear e-mail não desejado

Rastrear anexos e downloads para verificar conteúdo apropriado

Parar vírus e códigos maliciosos

Bloquear páginas da web e sites não apropriados

Reportar, registrar e arquivar

Visão Geral do SurfinGate

O produto SurfinGate 4.05 é uma ferramenta de segurança de código móvel para qualquer empresa que utilize a Internet, extranet ou intranet para transações comerciais. Através de inspeção de conteúdo de código móvel, incluindo JavaScript, o produto SurfinGate ajuda a proteger redes de computadores contra danos hostis ou não intencionais incluindo espionagem industrial, modificação de dados e exclusão de informações. O processo de inspeção de conteúdo do SurfinGate verifica o conteúdo de códigos móveis de Java, JavaScript e ActiveX no nível de gateway, longe de recursos críticos e atribui um ID e um ASP (applet security profile) único ao código, notando qualquer transgressão de segurança possível. O SurfinGate identifica códigos potencialmente problemáticos antes que ele possa entrar na rede.

O SurfinGate 4.05 inclui quatro componentes:

- SurfinGate Server
- SurfinConsole
- Banco de dados SurfinGate
- Integração SurfinGate Plugin for WTE para Windows NT

O SurfinGate Server age como um servidor proxy HTTP. O SurfinGate pode ser posicionado como parte de uma cadeia proxy juntamente com o proxy HTTP do Firewall e do proxy WEBsweeper. Para Windows NT, ele pode ser alternativamente utilizado como um plugin para o proxy HTTP do Firewall. Quando utilizado como um plugin, o produto SurfinGate obterá um grupo de informações para o usuário proxy que fizer o pedido. Os critérios de filtragem SurfinGate podem ser baseados nestas informações de grupo. Esta arquitetura permite que o tráfego de códigos móveis seja parado e inspecionado antes da invasão ocorrer. Este componente fornece proteção de acordo com o critério de segurança da corporação.

O SurfinConsole é uma interface amigável para gerenciamento e definição de um critério de segurança da corporação central para código móvel. O SurfinConsole pode controlar vários SurfinGate Servers na rede e reforçar regras de código móvel em toda a organização, de acordo com o usuário, o grupo ou através de listas ou códigos não aceitáveis e aceitáveis.

O banco de dados SurfinGate armazena detalhes de ASPs (applet security profiles), incluindo informações relativas a usuários e grupos e seus critérios de segurança correspondentes. O banco de dados pode utilizar um mecanismo de banco de dados de acesso interno ou um banco de dados Oracle existente. Como o SurfinGate inspeciona o conteúdo de todos os códigos móveis no caminho, o banco de dados não é necessário para segurança, mas ajuda a melhorar o desempenho de operações de larga escala.

Funções do SurfinGate

O SurfinGate fornece:

- Inspeção de conteúdo em nível de Gateway para applets Java, controles ActiveX e JavaScript

Monitoração em tempo real, inspeção dinâmica

Reforço de critérios de segurança para códigos móveis baseados na web

Inspeção de "códigos móveis" (por exemplo, apllets Java, controles ActiveX, JavaScript, scripts Visual Basic, plug-ins, cookies)

O produto SurfinGate pode funcionar como um proxy em uma cadeia proxy ou através de um plugin WTE no Firewall para Windows NT.

Capítulo 3. Para Instalar o SecureWay Boundary Server

Este capítulo descreve como preparar-se para instalar o SecureWay Boundary Server utilizando o assistente e inclui as seguintes seções:

Como se Preparar?

Esta seção descreve como preparar os componentes do SecureWay Boundary Server.

Integração com o Produto SecureWay Policy Director

Para obter a configuração básica do IBM SecureWay Policy Director no Windows NT ou AIX , proceda da seguinte maneira:

1. Verifique se seu sistema operacional está configurado corretamente para suportar o Policy Director.
2. Determine quais componentes do servidor se ajustam melhor a seus requisitos de implementação e em quais máquinas instalar estes componentes.
3. Instale e configure uma infra-estrutura DCE, se existir uma.
4. Instale e configure o SecureWay Directory (LDAP).
5. Configure o CAS (Certificate Authorization Service) se você pretende fazer autenticação de certificado de cliente.
6. Instale o cliente NetSEAT.
7. Instale os componentes do servidor Policy Director.
8. Instale a Console de Gerenciamento.

Para obter mais informações sobre o Policy Director consulte a publicação *Instalação e Uso do Policy Director 3.0*.

SecureWay Firewall

Para obter a configuração básica do IBM Firewall no Windows NT ou AIX , proceda da seguinte maneira:

1. Assegure-se de possuir os pré-requisitos listados em "Requisitos de Hardware do SecureWay Boundary Server" na página 17.
2. Planeje a instalação de seu IBM Firewall. Decida antes quais funções do firewall você deseja utilizar o como deseja utilizá-las.
3. Informe ao Firewall quais de suas interfaces estão conectadas a redes seguras. Você deve possuir uma interface segura e uma interface não segura para que seu firewall funcione apropriadamente. A partir da árvore de navegação do cliente de configuração, abra a pasta Administração do Sistema e clique em **Interfaces** para

exibir uma lista de interfaces de rede de sua firewall. Para alterar o status de segurança de uma interface, selecione uma interface e clique em **Alterar**.

Nota: Se você for conectar-se à Internet, entre em contato com seu ISP (Provedor de Serviços da Internet) para obter um endereço IP registrado para a interface não segura do Firewall.

4. Configure seu critério de segurança geral acessando o diálogo **Security Policy** na pasta Administração do Sistema. Para obter configurações típicas de Firewall:

   Permita consultas de DNS

   Negue mensagens de difusão a interfaces não seguras

   Negue Socks para placas não seguras

5. Configure seu serviço de nome de domínio e serviço de correio. Comunicação eficiente não ocorrerá se você não fornecer resolução DNS. Acesse estas funções da pasta Administração do Sistema na árvore de navegação de cliente de configuração.

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

   Interface Segura do Firewall
   Interface Não Segura do Firewall
   Rede Segura
   Cada sub-rede em sua rede segura
   Um objeto de rede de host para seus servidores Security Dynamics e para seus servidores de domínio Windows NT, se apropriado

7. Ative serviços no Firewall. Estes são métodos (como socks ou proxy) pelos quais usuários na rede segura podem acessar a rede não segura. Quais serviços são implementados depende das decisões feitas no estágio de planejamento. A implementação de um serviço geralmente requer a configuração de algumas configurações de conexão para permitir determinados tipos de tráfego. Por exemplo, se você deseja permitir que seus usuários seguros naveguem na Web ou na Internet utilizando Proxy HTTP, você não precisa apenas configurar o daemon Proxy HTTP no Firewall, mas também precisa configurar conexões para permitir tráfego HTTP. Se você for configurar o Policy Director, consulte a seção “Integração com o Produto SecureWay Policy Director” na página 11.

8. **Apenas Windows NT:** Como o processo de endurecimento desativa o NETBIOS, se você desejar utilizar as senhas de domínio do Windows NT para autenticação, você deve configurar o código de cliente do Windows que implementa a habilidade para procurar domínios do Windows NT confiáveis para objetivos de autenticação. Os servidores do Windows NT confiáveis devem possuir nomes e endereços de host TCP/IP e possuir conectividade entre eles e o Firewall. O administrador de firewall deve criar conexões entre o Firewall e os servidores confiáveis do Windows NT para permitir o fluxo de tráfego entre os dois.

9. Se você for utilizar tradução de endereço de rede, primeiro entre em contato com seu ISP para obter um endereço de Internet registrado para utilizar com tradução de endereço de muitos para um. Este endereço é além do endereço solicitado na etapa 3 na página 11. Em seguida, vá para o painel *Adicionar Configuração NAT* para adicionar endereços de Internet registrados no campo *Endereço IP de Vários Remetentes*.

A realização destas etapas deve ajudá-lo a concluir a configuração e execução do firewall básico. O IBM Firewall fornece outras funções, como logs do sistema para ajudá-lo a assegurar a segurança de sua rede.

Se o Firewall encerrar de maneira normal ou anormal, seus dados de configuração não são afetados porque são salvos no disco rígido e reativados automaticamente na reinicialização. Entretanto, certas mensagens de log da firewall ocorrerão indicando que algumas conexões ativas foram interrompidas, por exemplo, uma sessão de FTP ativa.

SecureWay Boundary Server

Você pode utilizar o assistente do SecureWay Boundary Server para configurar o Firewall para utilizar o IBM SecureWay Policy Director para administração de usuários para integração com o Policy Director. Opcionalmente, este assistente configura o Proxy HTTP do Firewall para passar informações de autenticação para o plugin SurfinGate (apenas Windows NT).

As informações necessárias para configurar o IBM SecureWay Boundary Server para Firewall são:

O nome do host e do domínio do servidor IBM SecureWay Directory que o Firewall irá utilizar.

O número da porta em que o servidor IBM SecureWay Directory está atendendo. A porta padrão é 389.

A senha do SecurityMaster para o servidor IBM SecureWay Directory.

O nome de domínio a ser utilizado para distinguir os usuários proxy para este Firewall. Todos os firewalls que utilizam este nome irão administrar o mesmo conjunto de usuários. Normalmente, você deve utilizar o nome de host completo da máquina do Firewall.

O nome do administrador do Firewall utilizado para acessar usuários proxy armazenados no SecureWay Directory. Este nome receberá acesso para modificar todos os usuários proxy criados no SecureWay Policy Director. Você deve utilizar o nome do host completo da máquina do Firewall.

O Nome Distinto que o IBM SecureWay Directory utiliza como uma raiz para iniciar a procura de usuários Firewall no banco de dados. Este deve ser o sufixo criado no SecureWay Directory para armazenar usuários Policy Director.

Uma senha para o ID do administrador do Firewall a ser utilizada na conexão com o servidor IBM SecureWay Directory.

Será necessário criar uma conexão para permitir fluxo de tráfego entre o Firewall e o servidor SecureWay Directory.

Assegure-se de possuir os pré-requisitos listados em “Requisitos de Hardware do SecureWay Boundary Server” na página 17.

SurfinGate

Para preparar-se para utilizar o SurfinGate, você deve possuir o Windows NT Service Pack 5 instalado. Assegure-se de possuir os pré-requisitos listados em “Requisitos de Hardware do SecureWay Boundary Server” na página 17.

Para utilizar o SurfinGate, proceda da seguinte maneira:

Se estiver utilizando banco de dados Oracle, ele deve estar configurado.

Se estiver utilizando o Windows NT Firewall, você deve decidir entre utilizar o modo de plugin ou de proxy.

Para ativar o plugin SurfinGate no WTE, instale o plugin SurfinGate na máquina Firewall e execute o assistente SecureWay Boundary Server.

Você deve criar uma conexão para permitir o fluxo de tráfego do plugin SurfinGate para o servidor SurfinGate.

MIMEsweeper

Para se preparar para utilizar o MIMEsweeper, você deve entender como sua rede irá funcionar. Assegure-se de possuir os pré-requisitos listados em “Requisitos de Hardware do SecureWay Boundary Server” na página 17.

MAILsweeper

Se você configurar o MIMEsweeper, o MAILsweeper e o WEBsweeper devem estar em máquinas separadas.

Realize as tarefas a seguir antes de configurar o MAILsweeper:

Determine os domínios de correio que você utiliza internamente. O MAILsweeper e o Firewall mail exchanger devem estar configurados para aceitar correio de cada um destes domínios de correio.

Determine quais servidores de correio seguro suportam cada um de seus domínios. O MAILsweeper deve ser configurado para encaminhar correio endereçado a todos os seus domínios de correio para o servidor de correio seguro correto.

Determine o endereço do servidor MAILsweeper. Cada servidor de correio seguro deve ser configurado para encaminhar correio recebido de clientes internos para o servidor MAILsweeper.

Determine o endereço do Firewall. O MAILsweeper deve ser configurado para encaminhar correio endereçado para domínios externos ao Firewall mail exchanger.

WEBsweeper

Realize as tarefas a seguir antes de configurar o WEBsweeper:

Determine o endereço do servidor WEBsweeper. Isto será necessário para cada um dos Web browsers de clientes em sua rede. Os navegadores devem estar configurados para utilizar o servidor WEBsweeper como seus proxies para HTTP, FTP e HTTPS.

Determine o endereço da interface segura de seu Firewall. O WEBsweeper deve ser configurado para encaminhar pedidos de proxy para o proxy HTTP residente no Firewall.

Se você não desejar que clientes sejam capazes de desviar a filtragem de conteúdo da web, é necessário configurar uma conexão com o Firewall para limitar o acesso proxy aos servidores WEBsweeper e/ou SurfinGate.

Capítulo 4. Requisitos para o IBM SBS (SecureWay Boundary Server)

Este capítulo fornece os requisitos mínimos do SecureWay Boundary Server.

Requisitos de Hardware do SecureWay Boundary Server

Os requisitos de hardware dos produtos do componente Boundary Server são mostrados na tabela a seguir.

Tabela 2. Requisitos de hardware dos produtos do componente Boundary Server

Componente do Boundary Server	Tipo de Máquina	Espaço em Disco	Memória	Outro
Policy Director	N/A	64 MB	16 MB	N/A
IBM Firewall	Windows NT: 266 MHz ou superior AIX: máquina RS/6000 que suporte 4.3.2	Windows NT: 200 MB AIX: 200 MB	Windows NT: 64 MB AIX: 128 MB	2 NICs (network interface cards)
ACE/Server	Windows NT: 166 MHz ou superior (apenas para processadores únicos) AIX: Máquina que suporte AIX 4.2	Software de servidor principal: 50 MB Servidor de backup: 22 MB Banco de dados de usuários inicial: 4MB Instalação: 240 MB	Mínima: 32 MB	Os requisitos de armazenamento reais são baseados no número de usuários
MAILsweeper	Windows NT: processador de 400 MHz ou superior	1 GB	128 MB	N/A
WEBsweeper	Windows NT: processador de 450 MHz ou superior	1 GB	128 MB	N/A
Requisitos do sistema WEBsweeper para Ambiente de Volume Alto	Windows NT: processador de 450 MHz ou superior	3 GB	512 MB	N/A
Servidor SurfinGate 4.05	Windows NT: processador de 233 MHz ou superior	20 MB	256 MB	N/A
Console SurfinGate 4.05	Windows NT: processador de 233 MHz ou superior	15 MB	64 MB	N/A

Nota: Para obter mais detalhes consulte a publicação IBM Secureway Firewall for AIX or Windows NT Version Setup and Installation for Multiple Languages. 138 MB de Espaço em Disco também são necessários para o Navegador Netscape.

Requisitos de Software para SecureWay Boundary Server

Os requisitos de software para os produtos do componente Boundary Server são mostrados na tabela a seguir.

Tabela 3. Requisitos mínimos de software para produtos do componente Boundary Server

Produto	Windows	AIX	Outro
Servidores Policy Director	Windows NT versão 4.0 com Service Pack 5	4.3.1	N/A
IBM Firewall	Windows NT versão 4.0 com Service Pack 5	4.3.2	N/A
SecureWay Boundary Server	IBM SecureWay Firewall 4.1	IBM SecureWay Firewall 4.1	N/A
MAILsweeper	Windows NT versão 4.0 com Service Pack 5; Internet Explorer 4.01 ou superior; Microsoft Management Console 1.1; unidade NTFS; Windows Messaging	N/A	Ferramentas Anti-Vírus que você deseja utilizar
WEBsweeper	Windows NT versão 4.0 com Service Pack 5	N/A	Ferramentas Anti-Vírus que você deseja utilizar
SurfinGate Server	Windows NT versão 4.0 com Service Pack 5	N/A	N/A
Console SurfinGate 4.05	Windows NT versão 4.0 com Service Pack 5 ou Windows 95	N/A	N/A

Capítulo 5. Instalação e Configuração do SecureWay Boundary Server

Este capítulo descreve como configurar e instalar o SecureWay Boundary Server no Windows NT e no AIX.

Instalação dos Componentes do SecureWay Boundary Server

Esta seção ajuda a instalar o IBM SecureWay Firewall, o SurfinGate e o MIMEsweeper para Windows NT e AIX.

Instalação do SecureWay Firewall

Para obter mais informações sobre uma configuração básica para o produto IBM SecureWay Firewall para Windows NT e AIX consulte a seção "Como se Preparar?" na página 11. Ela explica como definir uma interface segura, como determinar seu critério de segurança e como definir objetos de rede. Para obter mais informações sobre a instalação do SecureWay Firewall, consulte o *IBM SecureWay Firewall Installation Guide for AIX* e o *IBM SecureWay Firewall Installation Guide for Windows NT*.

Instalação do SecureWay Directory

Se você estiver utilizando o recurso LDAP do SecureWay Boundary Server, você deve instalar o SecureWay Directory, consulte a publicação *Instalação e Uso do IBM SecureWay Policy Director 3.0*.

O servidor SecureWay Directory deve estar localizado na parte segura do Firewall, ou dentro da DMZ (Demilitarized Zone) segura do Firewall.

Instalação do SecureWay Policy Director

Se estiver utilizando o recurso LDAP do SecureWay Boundary Server, você deve instalar o SecureWay Policy Director (consulte a publicação *Instalação e Uso do IBM SecureWay Policy Director 3.0*).

Instalação do SecureWay Boundary Server

Para instalar o SecureWay Boundary Server no Windows NT, proceda da seguinte maneira:

Instale o SecureWay Firewall para Windows NT

A partir do CD do SecureWay Boundary Server, execute o arquivo setup.exe

Escolha seu idioma e clique em **OK**

O InstallShield perguntará onde você deseja instalar o SecureWay Boundary Server. O diretório padrão do Windows NT é C:\Arquivos de Programas\IBM\SBS

Reinicialize

Para instalar o SecureWay Boundary Server no AIX, proceda da seguinte maneira:

Instale o SecureWay Firewall para AIX

Insira o CD e instale utilizando o comando SMITTY

Selecione Instalação e Manutenção de Software

Selecione Instalar e Atualizar Software

Selecione Instalar e Atualizar a partir do Último Software Disponível

Quando for solicitado o dispositivo de ENTRADA, liste as seleções e escolha a Unidade de CD-ROM

Liste as seleções do SOFTWARE a ser instalado e escolha sbs.

Pressione **Enter** para instalar o software

Reinicialize

Instalação do SurfinGate

O SurfinGate possui dois componentes: Servidor SurfinGate e Console SurfinGate. Para instalar os dois componentes do SurfinGate, consulte o manual de Instalação localizado em `\docs\install.pdf` no CD do SurfinGate.

Plugin SurfinGate

Para instalar o plugin do SurfinGate no IBM SecureWay Firewall para Windows NT, consulte o manual de Instalação localizado no diretório `\docs` do CD do SurfinGate.

Instalação do MIMEsweeper

O MIMEsweeper possui três componentes: MAILsweeper, WEBsweeper e WEBsweeper HTTPS.

O MAILsweeper 4.1 deve ser instalado em uma partição NTFS.

Instalação do MAILsweeper

Para instalar o MAILsweeper, consulte o *Getting Started Guide* localizado em `\install\MSW4_ _2\docs\qsg.pdf` no CD MIMEsweeper.

NÃO instale o MAILsweeper na mesma máquina do proxy WEBsweeper HTTP.

NÃO instale o MAILsweeper na mesma máquina do proxy WEBsweeper HTTPS.

Se você instalar o `MAPI32.dll` a partir do CD do Windows NT e depois instalar o Microsoft Management Console 1.1 a partir do CD do MIMEsweeper, a versão correta do `MAPI32.dll` será substituída por uma versão inferior instalada com o Microsoft Management Console. Depois de instalar o Microsoft Management Console, certifique-se de instalar o `MAPI32.dll`versão 4.0 ou posterior. O `dll` é normalmente encontrado no componente Windows Messaging.

Instalação do WEBsweeper

Para instalar o WEBsweeper, consulte o *Administrator's Guide* localizado em `\install\WSW3_2_5\docs\manual.pdf` no CD do MIMEsweeper.

NÃO instale o WEBsweeper na mesma máquina do MAILsweeper.

Instalação do WEBsweeper HTTPS

Para instalar o WEBsweeper HTTPS, consulte o arquivo *Readme* localizado em `\install\WSWHTTPS1_ _2\readme.txt` no CD do MIMEsweeper.

NÃO instale o proxy WEBsweeper HTTPS na mesma máquina do MAILsweeper.

Configuração dos Componentes do SecureWay Boundary Server

Configuração do SecureWay Firewall

Para obter uma configuração básica do IBM Firewall:

1. Planeje a instalação de seu IBM Firewall. Decida antes quais funções do Firewall você deseja utilizar o como deseja utilizá-las.
2. Informe ao Firewall quais de suas interfaces estão conectadas à redes seguras. Você deve possuir uma interface segura e uma interface não segura para que seu firewall funcione apropriadamente. A partir da árvore de navegação do cliente de configuração, abra a pasta Administração do Sistema e clique em **Interfaces** para exibir uma lista de interfaces de rede de seu firewall. Para alterar o status de segurança de uma interface, selecione uma interface e clique em **Alterar**.
3. Configure seu critério de segurança geral acessando o diálogo **Critério de Segurança** na pasta Administração do Sistema. Para obter configurações típicas do Firewall:

   Permita consultas de DNS

   Negue mensagens de difusão a interfaces não seguras

   Negue Socks para placas não seguras
4. Configure seu serviço de nome de domínio e serviço de correio. Comunicação eficiente não ocorrerá se você não fornecer resolução DNS. Acesse estas funções da pasta Administração do Sistema na árvore de navegação do cliente de configuração.
5. Defina elementos chave de sua rede para o Firewall utilizando a função **Objetos de Rede** na árvore de navegação do cliente de configuração. A função Objetos de Rede controla tráfego através do Firewall. Defina os seguintes elementos chave como objetos de rede:

   Interface Segura do Firewall
   Interface Não Segura do Firewall
   Rede Segura
   Cada sub-rede em sua rede segura

Um objeto de rede de host para seus servidores Security Dynamics e para seus servidores de domínio do Windows NT, se apropriado

6. Ative serviços no Firewall. Estes são métodos pelos quais usuários na rede segura podem acessar a rede não segura (como socks ou proxy). Quais serviços são implementados depende das decisões feitas no estágio de planejamento. A implementação de um serviço geralmente requer a configuração de algumas configurações de conexão para permitir determinados tipos de tráfego. Por exemplo, se você deseja permitir que seus usuários seguros naveguem na web ou na Internet utilizando Proxy HTTP, você não precisa apenas configurar o daemon Proxy HTTP na Firewall, mas também configurar conexões para permitir tráfego HTTP.
7. Configure usuários de Firewall. Se você solicitar autenticação para funções como acesso à Web de transmissão ou para administradores do Firewall, é necessário definir estes usuários no Firewall. Se você estiver utilizando um SecureWay Policy Director para armazenar usuários no LDAP, não crie usuários proxy desta vez. Utilize o console do Policy Director para criar os usuários proxy do Firewall durante a configuração do Policy Director.

Estas etapas devem ajudá-lo a obter uma configuração básica do Firewall ativa e em execução. O IBM Firewall fornece outras funções, como logs do sistema para ajudá-lo a assegurar a segurança de sua rede.

Se o Firewall encerrar de maneira normal ou anormal, seus dados de configuração não devem ser afetados porque são salvos no disco rígido e serão reativados automaticamente na reinicialização. Entretanto, determinadas mensagens de log do firewall podem ocorrer indicando que algumas conexões ativas foram interrompidas, por exemplo, uma sessão de FTP ativa.

Configuração do SecureWay Firewall para Integração do Policy Director

O Firewall deve ser configurado para utilizar o IBM SecureWay Policy Director com o Assistente do SecureWay Boundary Server para aproveitar a integração com o Policy Director. Se o IBM SecureWay Policy Director não for utilizado, usuários proxy serão definidos apenas pela GUI (Graphical User Interface) do Firewall. Tais usuários não podem ser gerenciados pelo SecureWay Policy Director.

Uma conexão terá que ser criada para permitir a comunicação entre o SecureWay Firewall e o SecureWay Directory. O SecureWay Directory deve estar no lado seguro do Firewall, na DMZ segura ou na rede segura.

Para obter mais informações sobre como configurar conexões, consulte o *IBM SecureWay Firewall User's Guide for Windows NT* e o *IBM SecureWay Firewall User's Guide for AIX*. Seguem informações para configurar a conexão.

Para o pedido, estes são os itens que você deverá configurar para a regra de transmissão:

A origem será o endereço da placa segura do Firewall.

O destino será o endereço do SecureWay Directory.

A porta de origem será maior que 1023

A porta de destino será igual a 389.

A interface será segura.

O roteamento será local.

A direção será de transmissão.

Para a resposta, estes são os itens que você deverá configurar para a regra de recepção:

A origem será o endereço do SecureWay Directory.

O destino será o endereço da placa segura do Firewall.

A porta de origem será igual a 389

A porta de destino será maior que 1023

A interface será segura.

O roteamento será local.

A direção será de recepção.

Um exemplo da conexão é mostrado abaixo:

```
# Service : ldap
# Description :

permit 9.67.13 .153 255.255.255.255 9.67.141.85
255.255.255.255 tcp gt 1 23 eq 389 secure both
outbound l=y f=y t=  e=none a=none

permit 9.67.141.85 255.255.255.255 9.67.13 .153
255.255.255.255 tcp/ack eq 389 gt 1 23 secure local
inbound l=y f=y t=  e=none a=none
```

Execute o assistente de configuração do servidor SecureWay Boundary. Selecione a opção para ativar o firewall para trabalhar com o Policy Director. Para obter mais informações, consulte a seção “Configuração do SecureWay Boundary Server para Integração do Policy Director” na página 28.

Configuração do SecureWay Firewall para Utilizar o SurfinGate Plugin (apenas Windows NT)

Uma conexão deverá criada para permitir a comunicação entre o SecureWay Firewall e o servidor SurfinGate. O servidor SurfinGate deve estar no lado seguro do Firewall.

Para obter mais informações sobre como configurar conexões, consulte o *IBM SecureWay Firewall User's Guide for Windows NT*. Seguem informações para configurar a conexão.

Para o pedido, estes são os itens que você deverá configurar para a regra de transmissão:

A origem será o endereço da placa segura do Firewall.

O destino será o endereço do servidor SurfinGate.

A porta de origem será maior que 1023.

A porta de destino será igual a 3141.

A interface será segura.

O roteamento será local.

A direção será de transmissão.

Para o pedido, estes são os itens que você terá que configurar para a regra de recepção:

A origem será o endereço do servidor SurfinGate.

O destino será o endereço da placa segura da Firewall.

A porta de origem será igual a 3141.

A porta de destino será maior que 1023.

A interface será segura.

O roteamento será local.

A direção será de recepção.

Um exemplo de tal conexão é mostrado abaixo:

```
# Service : SurfinGate Plugin Communication
# Description:

permit 9.67.143.113 255.255.255.255 9.67.143.115 255.255.255.255 tcp gt 1 23 eq 3141
secure local outbound l=y f=y
permit 9.67.143.115 255.255.255.255 9.67.143.113 255.255.255.255 tcp eq 3141 gt 1 23
secure local inbound  l=y f=y

Nota: As conexões devem estar na mesma linha.
```

Você também deverá configurar o servidor SurfinGate para permitir os dados que serão varridos. No SurfinConsole, (a interface de administração do SurfinGate) você deve verificar a opção **Modo de Plugin** sob a guia Geral. Você também deve digitar o endereço e o número de porta da proxy HTTP do Firewall no campo Próximo Proxy da guia Proxy.

Configuração do SecureWay Firewall para Utilizar o MAILsweeper

O Mail Exchanger definido no SecureWay Firewall deve apontar para a máquina MAILsweeper ao invés do servidor de correio seguro real. O próprio MAILsweeper entregará o correio aos servidores de correio seguros.

Configuração do SecureWay Policy Director

Certifique-se de o SecureWay Directory foi instalado. Você deve saber o endereço da máquina onde o SecureWay Directory está instalado, a porta em que ele está atendendo, o ID do administrador no servidor SecureWay Directory e a senha do administrador.

Instale o cliente LDAP do SecureWay Directory na mesma máquina do SecureWay Policy Director. (O cliente pode já estar instalado, se você estiver utilizando a mesma máquina para seu SecureWay Directory e para seu SecureWay Policy Director.)

Você deve modificar o esquema LDAP do SecureWay Directory para suportar eProxyUsers do Policy Director. As adições de esquema são armazenadas em dois arquivos fornecidos pelo Policy Director. Você precisará dos arquivos `secschema.def` e `puschema.def` localizados no diretório `/schema` do CD do Policy Director.

Para modificar o esquema LDAP no servidor SecureWay Directory, execute os seguintes comandos na máquina do Policy Director:

```
ldapmodify -h <LDAPHOST> -p <LDAPPORT>  -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f secschema.def

ldapmodify -h <LDAPHOST> -p <LDAPPORT> -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f puschema.def
```

Em que:

`<LDAPHOST>` é o nome do servidor SecureWay Directory

`<LDAPPORT>` é a porta em que o servidor está atendendo

`<LDAPADMINUSER>` é o id do administrador

`<LDAPADMINPWD>` é a senha do administrador

Quando tiver modificado o esquema LDAP para suportar usuários proxy, é necessário ativar a manipulação de usuário proxy para a Console do Policy Director. Para fazer isto, você deve retirar o comentário da linha Proxyusers TaskView no arquivo `console.properties` localizado no diretório `\Arquivos de Programas\IBM\IVConsole`.

Configuração do SecureWay Directory

Você deve definir um sufixo para o SecureWay Directory que será utilizado como a raiz em que os usuários do Policy Director serão armazenados. Para adicionar um sufixo para o LDAP, consulte a publicação *IBM SecureWay Directory Administrator's Guide*. Por exemplo, um sufixo típico deve ser:

```
o=yourcompany,c=yourcountry
```

Depois de adicionar o sufixo para armazenamento de usuários do Policy Director, você deve definir sua ACL (Access Control List) corretamente. Você deve fornecer todos os direitos de acesso ao novo sufixo para o grupo de segurança do Policy Director. O DN (Distinguished Name) do grupo de segurança do Policy Director é:

```
cn=securitygroup,secauthority=default
```

Configuração do SecureWay Boundary Server para Integração do Policy Director

Você pode configurar o servidor SecureWay Boundary utilizando o assistente. Este assistente ajuda nas etapas necessárias para configurar o Firewall para funcionar com outros produtos no Boundary Server e no Policy Director. Os painéis seguintes fazem perguntas sobre seu servidor LDAP. Quando você tiver preenchido todas as informações necessárias, o assistente irá configurar o Firewall para utilizar o mesmo banco de dados LDAP que o Policy Director está utilizando para critérios de usuário e de grupo. Este assistente também pode configurar ou desconfigurar o Proxy HTTP do Firewall para passar informações de autenticação para o plugin SurfinGate (apenas Windows NT Firewall).

Para configurar o IBM SecureWay Boundary Server, execute o assistente do SecureWay Boundary Server. No AIX, execute o comando **sbswizard**, no Windows NT, selecione **Iniciar->Programas->SecureWay Boundary Server**. Isto exibe o assistente do SBS.

1. Selecione a opção para **Configurar o Firewall para compartilhar um banco de dados LDAP com Policy Director**".
2. Responda às perguntas apresentadas utilizando as informações contidas em "SecureWay Boundary Server" na página 13.

Configuração do SecureWay Boundary Server para Ativar o Plugin SurfinGate (apenas Windows NT)

Selecione **Iniciar->Programas->SecureWay Boundary Server**. Isto exibe o assistente do SBS.

1. Selecione a opção para **Configurar o Proxy HTTP do Firewall para passar informações de autenticação para o plugin SurfinGate**.
2. Conclua o diálogo.

Configuração do SurfinGate

No Windows NT, há duas maneiras de configurar o SurfinGate:

Como um proxy encadeado

Como um plugin para o proxy HTTP do Firewall

No AIX, há uma maneira de configurar o SurfinGate:

Como um proxy encadeado

Configuração do SurfinGate como um Proxy Encadeado

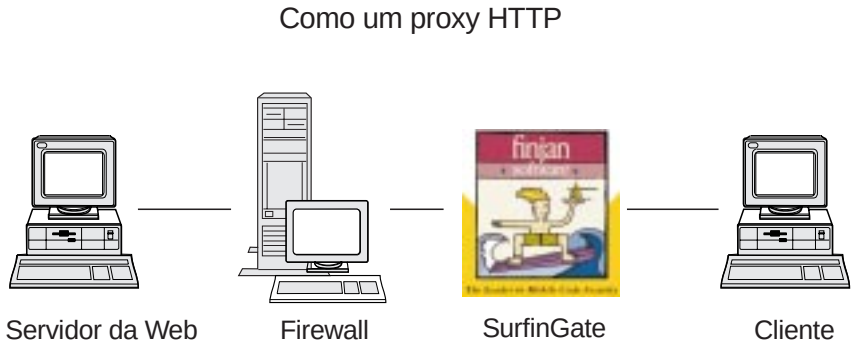

Figura 2. Configurações do SurfinGate

Os navegadores da web do cliente devem ser configurados para utilizar o SurfinGate como o proxy para HTTP, FTP e HTTPS. Assegure-se de especificar o número da porta em que o SurfinGate está atendendo (o padrão é 8080).

No SurfinConsole (a interface de administração do SurfinGate) você deverá marcar a opção **Modo Proxy** sob a guia Geral. Você também deve digitar o endereço e o número da porta do proxy HTTP do Firewall no campo Próxima Proxy da guia Proxy. Alternativamente, se você tiver proxies adicionais definidos, você pode apontar para eles como o próximo proxy.

Configuração do SurfinGate como um Plugin para o Proxy HTTP do Firewall

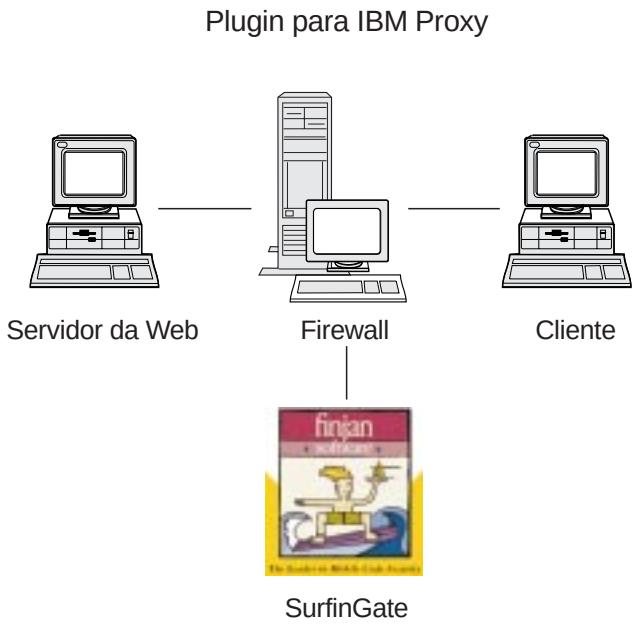

Figura 3. Configurações do SurfinGate

Os navegadores da web do cliente devem ser configurados para utilizar o proxy HTTP do Firewall como o proxy para HTTP, FTP e HTTPS. Especifique o número da porta em que o proxy HTTP do Firewall está atendendo (padrão é 8080).

No SurfinConsole (a interface de administração do SurfinGate), você deverá marcar a opção **Modo de Plugin** sob a guia Geral. Você também deve digitar o endereço e o número da porta do proxy HTTP do Firewall no campo Próximo Proxy da guia Proxy.

Nota: Esta funcionalidade está disponível apenas no SecureWay Firewall para Windows NT.

Configuração do MIMEsweeper

Configuração do MAILsweeper

Figura 4. Configurações do MAILsweeper

Se você possuir um ambiente simples, o MAILsweeper deve ser configurado pelas perguntas feitas durante a instalação. Para realizar configuração adicional, proceda da seguinte maneira: **Iniciar->Programas->MAILsweeper for SMTP->MAILsweeper for SMTP Console.** Para obter mais informações consulte a publicação *MAILsweeper Getting Started Guide*.

Configuração do WEBsweeper

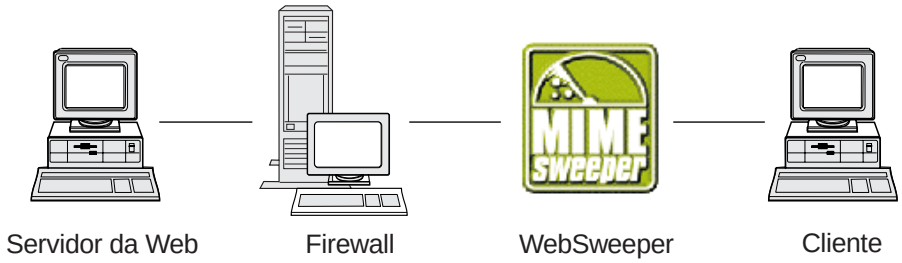

Figura 5. Configurações do WEBsweeper

Para configurar, vá para o Painel de Controle e selecione o applet WEBsweeper. Para obter mais informações consulte a publicação *WEBsweeper Administrator's Guide* localizada no CD do MIMEsweeper.

Configuração do WEBsweeper HTTPS

Para configurar, vá para o Painel de Controle e selecione o applet WEBsweeper HTTPS. Para obter mais informações consulte a publicação *WEBsweeper Administrator's Guide*

Bloqueio de Invasão

Utilize a linha de comandos para criar filtros que podem bloquear endereços IP específicos. Os endereços a serem bloqueados podem ser determinados dinamicamente como um resultado de inspeção de conteúdo. Os comandos são:

fwadd_deny

fwdelete_dynamic

fwadd_deny Se o programa for invocado sem parâmetros, ele exibirá um prompt solicitando o formato dos parâmetros requeridos.

Os parâmetros são:

Filter ID **Para Windows NT Firewall, o seguinte se aplica:** Um ID pode ser atribuído a filtros para organizar sua manutenção. Os IDs são atribuídos em ordem crescente começando com 1 e, se o ID fornecido for maior que o próximo número de ID disponível, o ID atribuído será o próximo número de ID disponível, não o número de ID fornecido pelo programa. Por exemplo, se algumas regras existirem com o ID 1 e você

tentar criar um conjunto de regras de filtro com o ID 3, o ID 2 será atribuído. Várias regras podem ser atribuídas para o mesmo número de ID. Quando regras são excluídas utilizando-se o programa delete_dynamic, elas são referenciadas pelo ID e, portanto, quando for criar regras por ID, planeje exclui-las como um grupo caso compartilhem o mesmo ID.

Quando a regra tiver sido incluída, o número de ID utilizado é exibido.

Filter ID **Para AIX Firewall, o seguinte se aplica:** O ID pode ser atribuído por número. Por exemplo, se você disser que o id de filtro é o ID 12, então ID=12 será atribuído a ele. Não pode haver filtros atribuídos com o mesmo número de ID no AIX. Cada filtro terá seu próprio ID único.

Source IP address O endereço IP a ser utilizado para a origem dos pacotes deve ser digitado em notação pontuada, por exemplo 255.255.255.255.

Source IP Mask Este campo é utilizado em conjunto com o endereço IP de origem e é digitado em notação pontuada. Por exemplo, se o endereço IP de origem digitado for 10.5.8.0 e a máscara IP de origem for 255.255.255.0, então todos os pacotes de 10.5.8.1 a 10.5.8.255 corresponderão.

Destination IP address O endereço IP a ser utilizado para o destino dos pacotes deve ser digitado em notação pontuada, por exemplo 255.255.255.255.

Destination IP Mask Este campo é utilizado em conjunto com o endereço IP de destino e é digitado em notação pontuada. Por exemplo, se o endereço IP de destino digitado for 10.5.8.0 e a máscara IP de destino for 255.255.255.0, então todos os pacotes de 10.5.8.1 a 10.5.8.255 corresponderão.

Adapter A especificação de placa é:

S para placas designadas como seguras

N para placas designadas como não seguras

B para todas as placas (seguras e não seguras)

Pacotes originados de placa(s) que atendem ao tipo especificado corresponderão à regra.

Scope O escopo de pacote transversal à firewall é especificado com este parâmetro, que pode ser um dos seguintes valores:

L para pacotes locais

R para pacotes roteados

B para pacotes locais e roteados

Direction Especifica a recepção ou transmissão de tráfego, ou ambas as direções.

I para tráfego de recepção

O para tráfego de transmissão

B para tráfego de recepção e de transmissão

Logging Especifique S para ligar o registro em log ou N para desligar o registro em log da atividade de filtro dinâmico.

fwdelete_dynamic Se este programa for invocado sem parâmetros, todos os filtros dinâmicos definidos atualmente são listados.

```
>>>>  Dynamic Rule Id         =  1
 >>>>>>>>  Jump               =
 >>>>>>>>  Filter Action       =  Deny
 >>>>>>>>  Source Address      =  9.192.8.7
 >>>>>>>>  Source Mask         =  255.255.255.
 >>>>>>>>  Destination Address  =  9.192.24 .1
 >>>>>>>>  Destination Mask     =  255.255.255.
 >>>>>>>>  Protocol           =  Any
 >>>>>>>>  Source Port         =  Any
 >>>>>>>>  Destination Port    =  Any
 >>>>>>>>  Adapter            =  Both (Secure and NonSecure)
 >>>>>>>>  Scope              =  Both (Routed and Local)
 >>>>>>>>  Direction          =  Both (Inbound and Outbound)
 >>>>>>>>  Tunnel Id          =
 >>>>>>>>  Logging Enabled     =  Unavailable
 >>>>>>>>  Fragments Allowed   =  No
```

Nota: O comando `fwdelete_dynamic` deve ser utilizado para verificar antes se as regras a serem excluídas possuem o ID esperado.

Quando o programa é invocado com um ID de filtro válido, a regra dinâmica é excluída e o número de regras excluídas é exibido no formato x Rules encontrado com id: x.

AVISO: Se você tentar adicionar um filtro duplicado, ele avisará que um filtro já existe. Se você tentar adicionar um filtro sem um Filter ID, você receberá um aviso de erro.

O bloqueio de violação do AIX pode ser substituído se houverem regras no conjunto de regras de nível superior. Se o bloqueio de violação for utilizado, a maioria das regras deve estar no conjunto de regras de nível inferior. Regras dinâmicas são adicionadas no meio destes dois conjuntos de regras. Se houver uma regra no nível superior permitindo tráfego, não é possível desligar o tráfego com regras dinâmicas.

Teste de sua Configuração

Depois de ter feito toda a configuração dos capítulos anteriores, a configuração deve ser testada. Para testar a configuração do SecureWay Boundary Server, faça o seguinte:

1. Configure um usuário de Proxy Firewall utilizando o Policy Director. Defina o usuário para utilizar senha de Firewall para telnet segura e defina a senha do usuário.
2. Execute o assistente do SecureWay Boundary Server para estabelecer o link entre o Firewall e o LDAP (Directory).
3. A partir do cliente seguro, inicie uma sessão de telnet proxy.
4. Digite a configuração do usuário no Policy Director.
5. Será solicitada uma senha.
6. Agora você está autenticado.

Capítulo 6. Documentação Relacionada

Você pode utilizar a documentação listada neste capítulo para encontrar mais informações sobre o IBM SecureWay Boundary Server Versão 2.0 e os produtos relacionados.

IBM SecureWay FirstSecure

O manual a seguir *IBM SecureWay FirstSecure Planning and Integration, Versão 2.0* contém informações sobre o produto FirstSecure. Este manual descreve o FirstSecure e os produtos que formam o FirstSecure e o ajuda a iniciar o planejamento para utilizar todos os produtos do IBM SecureWay.

IBM SecureWay Firewall

Os documentos a seguir contêm informações sobre o IBM SecureWay Firewall para Windows NT e estão disponíveis em formato PDF e HTM localizados no diretório `x:\books\pt_BR` do CD do IBM SecureWay Firewall:

IBM SecureWay Firewall para Windows NT - Guia de Instalação

IBM SecureWay Firewall para Windows NT - Guia do Usuário

IBM SecureWay Firewall para Windows NT - Referência

Guarding the Gates Using the IBM eNetwork Firewall for Windows NT 3.3 (um redbook)

Os documentos a seguir contêm informações sobre o IBM SecureWay Firewall para AIX e estão disponíveis no formato PDF e HTM localizados no diretório `books/pt_BR` do CD do IBM SecureWay Firewall:

IBM SecureWay Firewall para AIX - Guia de Instalação

IBM SecureWay Firewall para AIX - Guia do Usuário

IBM SecureWay Firewall para AIX - Referência

A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions (um redbook)

MIMEsweeper

MAILsweeper

Os documentos a seguir contêm informações sobre o MAILsweeper e estão disponíveis em formato PDF e HTM em \install no CD do MIMEsweeper:

A publicação *Getting Started Guide* está localizada em \install\MSW4_0_2\Doc\qsg.pdf

O Readme está localizado em \install\MSW4_0_2\README.htm

WEBsweeper

Os documentos a seguir contêm informações sobre o WEBsweeper e estão disponíveis em formato PDF e HTM em \install no CD do MIMEsweeper:

A publicação *WEBsweeper Administrator's Guide* está localizada em \install\WSW3_2_5\Doc\manual.pdf

A publicação Release Note está localizada em \install\WSW3_2_5\Doc\RELNOTES.htm

Proxy HTTPS do WEBsweeper

Os documentos a seguir contêm informações sobre o proxy HTTPS do WEBsweeper e estão disponíveis no formato TXT em \install do CD MIMEsweeper:

O Readme está localizado em \install\WSWHTTPS1_0_2\readme.txt

---

SurfinGate

Os documentos a seguir contêm informações sobre o SurfinGate e estão disponíveis no formato PDF em \docs no CD do SurfinGate:

A publicação *SurfinGate Installation Guide* está localizada em \Docs\install.pdf

A publicação *SurfinGate User's Manual* está localizada em \Docs\manual.pdf

A Release Note está localizada em \Docs\SFG 405 RelNotes.pdf

Informações sobre o plugin SurfinGate estão localizadas no diretório \docs.

Apêndice A. Detecção de Problemas

Este capítulo o ajuda a detectar e resolver problemas associados ao SecureWay Boundary Server.

Solução de Problemas Comuns do IBM SecureWay Firewall

Problemas de Roteamento

O IBM Firewall fornece um recurso na caixa de diálogo **Critério de Segurança** denominado *Testar Roteamento IP*, que pode ser útil para depurar problemas de roteamento. Ative esta caixa de opções, ative sua configuração de Conexão e ative a opção Registro de Regras de Conexão. Em seguida, examine seu `log do firewall` para exibir informações detalhadas sobre todos os pacotes que fluem através de seu firewall.

Execute estas etapas primeiro utilizando endereços IP e depois utilizando nomes de hosts.

Não é Possível Executar Ping de Hosts a Partir do Firewall

Explicação do problema Sua interface de rede não está configurada apropriadamente.

Ação recomendada Consulte a documentação de seu sistema operacional.

Explicação do problema Sua conexão à rede não segura não está configurada apropriadamente.

Ação recomendada Entre em contato com o Provedor de Serviços da Internet para obter assistência.

Explicação do problema Sua rede segura está isolada atrás de um roteador, seu firewall deve possuir uma rota estática para este roteador. Utilize o comando `netstat -rn` para verificar o roteamento estático:

```
netstat -rn
```

A saída deve ser a seguinte, para Protocolo Família 2:

```
Destination  Gateway         Flags    ....
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. . .1       U
```

Figura 6. Exemplo de saída do comando netstat -rn.

nrr.nrr.nrr.nrr representa seu roteador para a internet e é o roteador padrão. O roteador padrão é uma rota estática (Flag=UG).

nnn.nnn.nnn representa seu domínio não seguro. Esta é uma rota de interface (Flag=U).
nnn.nnn.nnn.nnn representa sua interface não segura.
sss.sss.sss representa seu domínio seguro. Esta é uma rota de interface (Flag=U).
sss.sss.sss.sss representa sua interface segura.
ss1.ss1.ss1 representa um sub-domínio no lado seguro da rede e srr.srr.srr.srr representa o roteador para este sub-domínio. Esta é uma rota estática (Flag=UG).
127.0.0.1 é o circuito fechado ou o host local. Esta é uma rota de interface (Flag=U).

Você deve possuir uma rota de interface para cada interface e sua rota padrão deve apontar para o roteador no lado não seguro do firewall.

Ação recomendada Adicione uma rota estática a seu roteador. Entre em contato com o administrador do roteador. Utilize o comando `route add`.

Explicação do problema A máscara de sub-rede em sua interface segura ou que o host está tentando contatar pode estar incorreta.

Ação recomendada Utilize os utilitários de configuração de cliente para corrigir as definições de máscara.

Não é Possível Executar Ping para Hosts não Seguros a Partir de Hosts Seguros (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 do roteador.

Explicação do problema Se sua rede segura utilizar endereços que não são registrados e roteáveis na rede não segura, incluindo endereços privados como os especificados em RFC 1597, os pacotes não serão roteados de volta para o remetente.

Ação recomendada Apenas para Windows NT: Utilize um cliente com um endereço registrado. O recurso NAT do firewall pode ser utilizado para tráfego TCP e UDP, mas o NAT não traduzirá endereços em pacotes ICMP como ping.

Ação recomendada Apenas para AIX: Utilize um cliente com um endereço registrado.

Falhas de DNS

Nota: DNS é apenas para Windows NT.

Explicação do problema Você recebeu mensagens de erro de DNS porque configurou o Microsoft DNS Service com o Microsoft DNS Service Manager.

Ação recomendada Consulte as instruções de Instalação novamente e

1. Remova o Microsoft DNS, excluindo todo o diretório: `\winnt\system32\DNS`

2. Reinstale o Microsoft DNS
3. Reinicialize
4. Reinstale o DNS hotfix
5. Reinicialize

Solução de Problemas Comuns – MIMEsweeper

WEBsweeper e MAILsweeper Parecem não Funcionar na Mesma Máquina

Explicação do problema Problemas durante a tentativa de executar o MAILsweeper e o WEBsweeper na mesma máquina.

Ação recomendada Instale o MAILsweeper em uma máquina e o WEBsweeper em uma máquina separada.

Desempenho Lento do WEBsweeper

Explicação do problema Atrasos insatisfatórios durante o download de conteúdo da web quando o WEBsweeper é utilizado.

Ação recomendada

1. Desative o registro em log utilizando o applet do WEBsweeper do Painel de Controle.
2. Instale o WEBsweeper no hardware mais rápido que você puder.

Problemas com o Licenciamento do WEBsweeper

Explicação do problema Ao instalar o WEBsweeper 3.2_5 em uma máquina que possui uma versão anterior do WEBsweeper instalada pode haver um conflito de código de licenciamento. Quando o WEBsweeper for iniciado, se ocorrer uma mensagem de erro interno do Windows: 2140, verifique o log do aplicativo no visualizador de eventos. A mensagem do WEBsweeper é: "Erro de PAKMSG: O nome do usuário conflita com seção de licença definida anteriormente."

Ação recomendada Remova o código de licença do registro do Windows. Carregue o regedit e pesquise no caminho \\HKEY_LOCAL_MACHINE\SOFTWARE\Content Technologies\MIMEsweeper\License. Se for encontrado mais de um código lá, exclua o que não estiver identificado como "IBM MIMEsweeper System". Reinicialize.

O WEBsweeper tem Problemas para Fazer Download de Arquivos Grandes

Explicação do problema O WEBsweeper pode ficar sem memória virtual para armazenar arquivos durante a filtragem.

Ação recomendada Aumente a quantidade de memória física no servidor WEBsweeper.

Solução de Problemas Comuns — SurfinGate

O SurfinConsole Pára de Responder Quando o Microsoft Internet Explorer Está Aberto

Explicação do problema O aplicativo SurfinConsole apresenta comportamento estranho ou pára de responder quando o Internet Explorer está aberto. Estes dois aplicativos possuem um conflito e não podem ser executados ao mesmo tempo.

Ação recomendada Não carregue o Internet Explorer e o SurfinConsole ao mesmo tempo.

Desempenho Lento do Plugin SurfinGate

Explicação do problema Downloads de códigos móveis através da web são muito lentos utilizando-se o Plugin SurfinGate.

Ação recomendada Assegure que o campo Próximo Proxy esteja definido para SecureWay Firewall HTTP proxy na seção Proxy do SurfinConsole.

Apêndice B. Avisos

Referências nesta publicação a produtos, programas ou serviços IBM não significam que a IBM pretenda disponibilizá-los em todos os países onde opera. Qualquer referência a um produto, programa ou serviço IBM, não significa que apenas o produto, programa ou serviço IBM possa ser utilizado. Sujeito à propriedade intelectual da IBM ou outros direitos protegidos legalmente, qualquer produto, programa ou serviço funcionalmente equivalente pode ser utilizado em substituição ao produto, programa ou serviço IBM. A avaliação e verificação da operação em conjunto com outros produtos, exceto aqueles expressamente designados pela IBM, são de inteira responsabilidade do usuário.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Consultas sobre licenças devem ser enviadas, por escrito, para:

Gerência de Relações Comerciais e Industriais
Av. Pasteur 138-146 - Botafogo
Rio de Janeiro - RJ
CEP: 22.290-240

O programa não está licenciado segundo os termos do Contrato do Cliente IBM (ICA - IBM Customer Agreement). Está licenciado segundo os termos do Contrato de Licença do Programa Internacional IBM (IPLA - IBM International Program License Agreement).

Este documento não deve ser utilizado em nível de produção e é fornecido "no estado" sem garantia de espécie alguma; a IBM se exime de todas as garantias, incluindo as garantias de comercialização e adequação a um fim específico.

Este produto inclui software do computador criado e disponibilizado pelo CERN. Esta declaração deve ser mencionada por completo em todo produto que contiver o software de computador CERN aqui incluído ou em outras partes.

Marcas

Os termos a seguir são marcas da IBM Corporation nos Estados Unidos e/ou em outros países.

AIX

IBM

Microsoft e Windows NT são marcas ou marcas registradas da Microsoft Corporation.

**SurfinGate é marca da Finjan Software, Ltd.

**MIMEsweeper, **MAILsweeper e **WEBsweeper são marcas da Content Technologies, Ltd.

Outros nomes de empresas, produtos e serviços, que podem estar denotados por asteriscos duplos (**), podem ser marcas ou marcas de serviços de terceiros.

Glossário

A

assistente. Um diálogo de um aplicativo que utiliza instruções passo a passo para guiar um usuário através de uma tarefa específica.

C

cliente. Um sistema ou processo de computador que solicita um serviço de outro sistema ou processo de computador que é geralmente denominado servidor. Vários clientes podem compartilhar acesso a um servidor comum.

D

DMZ. Demilitarized Zone. Um dispositivo que evita que usuários externos obtenham acesso direto a um servidor que possui dados da empresa.

E

endereço de servidor. O código único atribuído à cada computador que fornece serviços compartilhados a outros computadores através de uma rede; por exemplo, um servidor de arquivo, um servidor de impressora ou um servidor de correio. Um endereço IP padrão é um campo de endereço de 32 bits. O endereço do servidor pode ser o endereço IP pontuado ou o nome do host.

Endereço IP. Endereço de Internet Protocol. O endereço único de 32 bits que especifica a localização real de cada dispositivo ou estação de trabalho em uma rede. Ele também é conhecido como um endereço de Internet.

F

Firewall. Uma unidade funcional que protege e controla a conexão de uma rede a outras redes. O firewall evita que tráfego de comunicação não desejada ou não autorizada entre na rede protegida e permite que apenas tráfego de comunicação selecionada para deixar a rede protegida.

FTP (File Transfer Protocol). Um protocolo de aplicativo utilizado para transferência de arquivos para e a partir de computadores de rede. O FTP requer um ID de usuário e às vezes uma senha para permitir acesso a arquivos em um sistema de host remoto.

G

gateway. Uma unidade funcional que interconecta duas redes de computadores com arquiteturas diferentes.

I

ICMP. Internet Control Message Protocol. O protocolo utilizado para identificar mensagens de erro e de controle na camada IP (Internet Protocol). Relatórios de problemas e destino de datagramas incorretos são devolvidos para a origem de datagrama original.

interface de circuito fechado. Uma interface que desvia funções de comunicação desnecessárias quando as informações são endereçadas a uma entidade dentro do mesmo sistema.

Internet. A coleção mundial de redes interconectadas que utilizam o conjunto de protocolos da Internet e permite acesso público.

intranet. Uma rede segura, particular que integra padrões da Internet e de aplicativos (como Web browsers) com uma infra-estrutura de rede de computadores existente de uma organização.

IP. Internet Protocol. Um protocolo sem conexão que roteia dados através de uma rede ou redes interconectadas. O IP age como um intermediário entre as camadas de protocolo superior e a camada física.

IPSEC. Internet Protocol Security. Um padrão em desenvolvimento para segurança na rede ou na camada de processamento de pacote da comunicação de rede.

N

NAT. Network Address Translation. Em um firewall, a conversão de endereços IP seguros para endereços registrados externos. Isto permite comunicação com redes externas mas mascara os endereços IP que são utilizados dentro do firewall.

P

padrão. Um valor, atributo ou opção que é assumida quando nenhuma outra é especificada explicitamente.

PICS. Platform for Internet Content Selection. Clientes ativados para PICS permitem que os usuários determinem quais serviços de taxa querem utilizar e, para cada serviço de taxa, quais taxas são aceitáveis e quais são inaceitáveis.

ping. Um comando que envia pedidos de eco de ICMP (Internet Control Message Protocol) a um host, gateway ou roteador com a expectativa de receber uma resposta.

porta. Um número que identifica um dispositivo de comunicação abstrato. Servidores da Web utilizam a porta 80 por padrão.

protocolo. O conjunto de regras que governam a operação de unidades funcionais de um sistema de comunicação se ocorrer comunicação. Os protocolos podem determinar detalhes de baixo nível de interfaces de máquina para máquina, como a ordem em que os bits de um byte são enviados; eles também podem determinar trocas de alto nível entre programas aplicativos, como transferência de arquivo.

S

serviço. Uma função fornecida por um ou mais nós; por exemplo, HTTP, FTP, Telnet.

servidor. Um computador que fornece serviços compartilhados para outros computadores através de uma rede; por exemplo, um servidor de arquivo, um servidor de impressora ou um servidor de correio.

shell. O software que aceita e processa linhas de comando de uma estação de trabalho de usuário. O shell Korn é um dos vários shells UNIX disponíveis.

SMTP. Simple Mail Transfer Protocol. No conjunto de protocolos Internet, um protocolo de aplicativo para transferência de correio entre usuários no ambiente da Internet. O SMTP especifica as seqüências de troca de correio e o formato da mensagem. Ele assume que o TCP (Transmission Control Protocol) é o protocolo subjacente.

T

TCP. Transmission Control Protocol. Um protocolo de comunicações utilizado na Internet. O TCP fornece troca confiável de informações de host para host. Ele utiliza IP como o protocolo subjacente.

TCP/IP. Protocolo de Controle de Transmissão/Protocolo de Internet. Um conjunto de protocolos designados para permitir comunicação entre redes, independente das tecnologias de comunicação utilizadas em cada rede.

Telnet. Protocolo de emulação de terminal, um protocolo de aplicativo TCP/IP para serviço de conexão remota. O Telnet permite que um usuário em um local da instalação obtenha acesso a um host remoto como se a estação de trabalho do usuário estivesse conectada diretamente ao host remoto.

tempo limite. O intervalo de tempo alocado para que uma operação ocorra.

U

UDP. User Datagram Protocol. No conjunto de protocolos da Internet, um protocolo que fornece serviço de datagrama não confiável, sem conexão. Ele permite que um programa aplicativo em uma máquina ou em um processo envie um datagrama a um programa aplicativo em outra máquina ou processo. O UDP utiliza o protocolo IP (Internet Protocol) para enviar datagramas.

V

VPN. Virtual Private Network (VPN). Uma rede formada de um ou mais túneis IP seguros conectando duas ou mais redes.

W

Web. A rede de servidores HTTP que contêm programas e arquivos, vários deles documentos de hipertexto que contém links para outros documentos em servidores HTTP. Também denominada World Wide Web.

WTE. Web Traffic Express (WTE). Um servidor proxy de cache que pode ajudar a aumentar o tempo de resposta do usuário final através de esquemas de cache altamente eficientes. Filtros PICS flexíveis ajudam os administradores de rede a controlar acesso a informações baseadas na Web em uma localização central.

Número da Peça: CT6RZBP

Impresso no Brasil

CT6RZBP