IBM SecureWay FirstSecure

Planejamento e Integração

Versão 2

IBM SecureWay FirstSecure

Planejamento e Integração

Versão 2

Nota

Antes de utilizar estas informações e o produto suportado por elas, leia as informações gerais incluídas no Apêndice A, “Avisos” na página 99.

Primeira Edição (Outubro de 1999)

Esta edição se aplica ao IBM SecureWay FirstSecure Versão 2 e a todos os releases e modificações subseqüentes até quando for indicado de outra forma em novas edições.

Índice

Figuras

Tabelas

Sobre este manual

O produto IBM SecureWay FirstSecure, também denominado FirstSecure, é uma estrutura ampla que ajuda sua empresa a:

- Garantir a segurança de todos os aspectos de acesso à Web e outras redes.
- Aumentar seus investimentos atuais de e-business. Ofertas modulares permitem que você adicione segurança de uma forma planejada.
- Reduzir o custo total de propriedade, conduzindo e-business seguro.

Este manual descreve o software FirstSecure, os produtos que formam o software FirstSecure, e fornece informações iniciais sobre o planejamento para a utilização destes produtos.

Os produtos descritos neste manual fazem pare de um release em estágios. Nem todos os produtos podem estar disponíveis ao mesmo tempo ou em todos os países. Entre em contato com um representante de marketing IBM para se informar sobre a disponibilidade de qualquer um destes produtos.

Figuras neste manual

As figuras neste manual são apenas para objetivo de planejamento. Cada figura ilustra apenas uma das várias disposições de servidores, clientes e aplicativos que podem ser apropriados para sua organização.

O formato das figuras mostradas depende do mecanismo de entrega do manual:

- A maioria das figuras na versão PDF (Portable Document Format) do manual são mais simples para economizar espaço em disco e para serem impressas mais rápido.
- As figuras em versões impressas são mais complexas e ocupam mais espaço de armazenamento e mais tempo para impressão.

As figuras em ambas as versões são funcionalmente equivalentes e possuem legendas e textos alternativos idênticos.

Quem deve ler este manual

Este manual é destinado para administradores de sistema que desejam planejar e integrar a segurança para sistemas baseados na Web. Você já deve conhecer sua rede e seus aplicativos de e-business.

Como este manual é organizado

Este manual contém as seguintes partes:

A Parte 1, “Visão geral do FirstSecure” na página 1 fornece uma visão geral do software FirstSecure, seus produtos componentes e as ofertas disponíveis.

A Parte 2, “Planejamento de uma rede de e-business segura” na página 15 descreve o planejamento para uma rede de e-business segura.

A Parte 3, “Considerações sobre instalação e integração” na página 53 descreve a instalação de requisitos e detalhes de integração dos produtos FirstSecure.

O Capítulo 16, “Documentação fornecida com o produto FirstSecure” na página 87 descreve toda a documentação disponível com o FirstSecure.

O “Glossário” na página 103 define termos relacionados a segurança utilizados neste manual.

O manual também inclui uma bibliografia descrevendo cada documentação do produto.

Ano 2000

A preparação do IBM SecureWay FirstSecure é descrita abaixo.

Produtos IBM no IBM SecureWay FirstSecure

Estes produtos estão preparados para o Ano 2000. Quando utilizado de acordo com a documentação associada, eles são capazes de processar, fornecer e/ou receber dados de data durante 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.

Produtos de outros fornecedores

Foi feita representação de outros à IBM como preparados para o Ano 2000. Entretanto, a IBM não faz representações ou dá garantias sobre a preparação para o Ano 2000 destes produtos. Entre em contato com o fabricante sobre questões em relação à preparação para o Ano 2000 destes produtos. Informações relacionadas a produtos e serviços não-IBM são "Republicações" sob o Information and Readiness Disclosure Act baseado em informações fornecidas pelas outras empresas sobre os produtos e serviços oferecidos por elas. Foi feita representação à IBM que os produtos são preparados para o Ano 2000. Entretanto, a IBM não faz representações ou dá garantias sobre a preparação para o Ano 2000 destes produtos. Entre em contato com os fabricantes sobre questões em relação à preparação para o Ano 2000 deste produto. A IBM não verificou independentemente o conteúdo destas

Republicações e não toma responsabilidade pela precisão da perfeição das informações contidas nestas Republicações.

Serviço e suporte

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

Convenções

Este manual utiliza as seguintes convenções tipográficas:

Negrito indica o nome de um item que você seleciona, o nome de um comando, o texto digitado pelo usuário ou um exemplo de texto.

`Monoespaçado` indica um exemplo (como um caminho ou nome de arquivo fictício) ou texto que é exibido na tela.

Informações da Web

Informações sobre atualizações recentes para o software FirstSecure estão disponíveis no endereço www.ibm.com/software/security na Internet nas seguintes localizações:

IBM SecureWay FirstSecure

www.ibm.com/software/security/firstsecure

As documentações estão disponíveis no endereço
www.ibm.com/software/security/firstsecure/library

IBM SecureWay Policy Director

www.ibm.com/software/security/policy

As documentações estão disponíveis no endereço
www.ibm.com/software/security/policy/library

IBM SecureWay Boundary Server

www.ibm.com/software/boundary

As documentações estão disponíveis no endereço
www.ibm.com/software/boundary/library

IBM SecureWay Trust Authority

www.ibm.com/software/security/trust

As documentações estão disponíveis no endereço
www.ibm.com/software/securitytrust/library

Um Redbook ITSO, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498–00 está disponível no endereço www.ibm.com/redbooks, na Internet.

Parte 1. Visão geral do FirstSecure

Esta parte é uma visão geral do FirstSecure e seus produtos componentes. Ela contém uma breve descrição de cada produto.

Esta parte também descreve o IBM Implementation Services.

Capítulo 1. O que é o FirstSecure?

O produto IBM SecureWay FirstSecure faz parte das soluções de segurança integradas IBM. O software FirstSecure é um conjunto amplo de blocos de construção que ajudam sua empresa a:

Estabelecer uma ambiente seguro de e-business.

Reduzir o custo total de propriedade de segurança, simplificando o planejamento de segurança.

Implementar critério de segurança mais facilmente.

Criar um ambiente de e-business mais funcional.

Os componentes do FirstSecure incluem proteção contra vírus, detecção de invasão, controle de acesso, controle do conteúdo do tráfego, criptografia, certificados digitais, tecnologia de firewall e conjuntos de ferramentas para desenvolvimento de aplicativos. Estas funções são fornecidas pela família de produtos de segurança IBM SecureWay, bem como através de ofertas de outros fornecedores, combinando os melhores componentes de vários fornecedores de segurança. Adicionalmente, estão disponíveis Implementation Services para componentes FirstSecure selecionados. Os blocos de construção FirstSecure são os seguintes:

SecureWay Policy Director

SecureWay Boundary Server

Intrusion Immunity

Public Key Infrastructure, fornecido pelo IBM SecureWay Trust Authority

IBM SecureWay Toolbox

Como o FirstSecure é um conjunto de produtos que podem ser instalados independentemente, você pode fazer uma mudança planejada para um ambiente seguro. Você pode começar em uma área, testar as melhorias e depois continuar buscando mais segurança. Isto reduz a complexidade e os custos e aumenta a velocidade de implementação de aplicativos e recursos da Web.

Porque o software FirstSecure é necessário?

Seus dados e recursos são vitais para seu e-business. Juntos, os produtos do software FirstSecure fornecem:

Autorização
Todos devem seguir as regras. A autorização permite que apenas usuários aprovados acessem seus sistemas, dados, aplicativos e redes.

Contabilidade
Você pode saber quem fez o quê e quando. A contabilidade permite que você determine quem realizou uma ação e quais ações ocorreram durante um intervalo de tempo especificado.

Garantia
Você ter a segurança de que o sistema mantém suas promessas de segurança. Esta proteção permite que você demonstre e valide que o nível de proteção de segurança anunciado é cumprido.

Disponibilidade
O sistema está ativo quando você precisa dele. Esta proteção o ajuda a manter seus sistemas, dados, redes e aplicativos disponíveis para utilização por seus funcionários, fornecedores, parceiros e clientes.

Administração
Você pode definir as regras. Esta proteção permite que você defina, mantenha, monitore e modifique informações de critérios.

Você pode implementar estas proteções baseado em critérios em nível de corporação para fornecer uma malha de proteção através do conjunto inteiro de redes, sistemas e aplicativos de sua empresa. A presença de um link vulnerável entre produtos nesta malha pode tornar inútil a infraestrutura restante.

Este manual liga cada um dos produtos do bloco de construção do SecureWay à lista de proteções fornecida.

Quais são os blocos de construção do software FirstSecure?

O software FirstSecure contém produtos componentes que você pode obter como um grupo de todos os produtos ou como produtos relacionados separados. Estes produtos, por sua vez, possuem um ou mais produtos componentes. Você pode começar com qualquer produto e construir uma solução de segurança completa.

Policy Director

O produto Policy Director é o foco central do planejamento de segurança. O produto Policy Director fornece autorização e gerenciamento de segurança de extremidade a extremidade para recursos da Web através de intranets e extranets geograficamente dispersadas. O produto Policy Director fornece autenticação, autorização, segurança de dados e gerenciamento de recursos. Utilize o produto Policy Director com aplicativos padrão baseados na Internet para criar intranets seguras e bem gerenciadas. O produto Policy Director inclui:

Serviços de Segurança

Console de Gerenciamento

Servidor de Gerenciamento

Gerenciados de Segurança (NetSEAL e WebSEAL)

Cliente NetSEAT

Directory Services Broker

Servidor de Autorização (suporte a aplicativo de terceiros)

O produto Policy Director é executado nos sistemas operacionais Windows NT, AIX e Solaris.

Para obter uma descrição mais completa do produto Policy Director consulte a seção Capítulo 5, “Planejamento do Policy Director em sua rede” na página 31.

SecureWay Boundary Server

Os produtos SecureWay Boundary Server fornecem segurança, administração e contabilidade para aplicativos de e-business baseados na Web. Limites seguros são necessários em todos os lugares — entre departamentos, como engenharia e recursos humanos, entre redes da matriz e escritórios remotos, entre a rede de sua empresa e a Internet, entre os aplicativos da Web de sua empresa e os clientes e entre a rede de sua empresa e parceiros de negócios. Segurança de limites apropriada requer controle tanto de quem pode acessar sua rede como de quais informações entram ou saem dela.

Esta seção descreve os blocos de construção do produto SecureWay Boundary Server. Para obter considerações sobre planejamento e integração consulte a seção Capítulo 12, “Requisitos e considerações sobre a instalação do componente SecureWay Boundary Server” na página 59.

IBM SecureWay Firewall

O produto IBM SecureWay Firewall, também denominado IBM Firewall, permite e-business seguro, através do controle de todas as comunicações para e da Internet. O produto IBM Firewall fornece as três funções críticas para firewalls — filtragem, proxy e gateway em nível de circuito — para fornecer a você um alto nível de segurança e flexibilidade.

ACE/Server

O produto ACE/Server, da Security Dynamic, inclui tokens SecurID (2 licenças para usuário e 2 tokens). O produto ACE/Server inclui um logon de administrador e uma conexão*VPN (virtual private network)* ao produto IBM SecureWay Firewall.

MIMEsweeper para IBM SecureWay Release 2

O produto MIMEsweeper, da Content Technology, inclui componentes para segurança na Internet. O produto MAILsweeper verifica e-mail para assegurar que nenhuma informação confidencial saia de seu e-business e que nenhum e-mail não permitido seja recebido.

O WEBsweeper evita que material da Web não desejado entre em sua empresa. Ele verifica e aceita dados apenas de applets Java, códigos executáveis ou sites da Web permitidos.

SurfinGate

O produto SurfinGate, da Finjan Software Ltd., é uma solução de segurança de código móvel para e-business. Como o código móvel atualmente sempre entra automáticas e rotineiramente na sua rede de e-business de fora de sua intranet, você precisa de mais proteção além de firewalls. O produto SurfinGate protege sua rede contra invasões de código Java, ActiveX, e JavaScript. Ele identifica ataques hostis potenciais, longe de recursos indispensáveis, antes de entrarem em sua rede. Ele mantém dados suspeitos em quarentena para que você possa fazer uma inspeção antes de aceitá-los.

Intrusion Immunity

O produto Intrusion Immunity fornece Garantia na forma de produtos de detecção e proteção da empresa. Para obter os requisitos do produto Intrusion Immunity consulte a seção Capítulo 13, “Requisitos e considerações sobre a instalação do Intrusion Immunity” na página 67. O produto Intrusion Immunity inclui o Tivoli Cross-Site for Security e o Norton AntiVirus.

Tivoli Cross-Site for Security

O produto Tivoli Cross-Site for Security fornece detecção de violação para sistemas que podem ser vulneráveis a invasão. Com o produto Tivoli Cross-Site for Security você pode:

- Instalar agentes Cross-Site for Security em sua rede para reportar incidentes suspeitos para o servidor de gerenciamento Cross-Site for Security.
- Exibir dados de violação em relatórios pré-definidos e personalizados.
- Detectar e registrar atividades não autorizadas ou suspeitas em tempo real.
- Ajustar os agentes de segurança para reduzir o número de alarmes falsos.

Norton AntiVirus

O Norton AntiVirus, um produto da Symantec Corporation, é um dos líderes mundiais na área de produtos de software antivírus. O produto Norton AntiVirus pode permanecer em execução em background constantemente, para ajudar a manter seus computadores protegidos contra vírus que podem estar contidos em anexos de mensagens de e-mail, controles ActiveX, applets Java, downloads da Internet, disquetes, CDs de software ou arquivos enviados através de uma rede. Com o produto Norton AntiVirus você pode deixar arquivos infectados em quarentena. Você pode configurar o Norton AntiVirus para informá-lo automaticamente sobre atualizações e vírus recém descobertos.

Public Key Infrastructure

O IBM FirstSecure suporta padrões PKI (Public Key Infrastructure) para criptografia e interoperabilidade fornecendo o IBM SecureWay Trust Authority.

O SecureWay Trust Authority é uma solução de segurança que suporta a emissão, renovação e revogação de certificados digitais. Estes certificados podem ser utilizados em um grande número de aplicativos de Internet, fornecendo um meio para autenticação de usuários e para assegurar comunicações confiáveis. O Trust Authority é baseado nas especificações *IETF (Internet Engineering Task Force) PKI (Public Key Infrastructure)* Working Group. Ele inclui:

- Suporte para servidores IBM AIX e Microsoft Windows NT
- Um RA (autoridade de registro)
- Um CA (autoridade de certificado)
- Interfaces de usuários para solicitação de certificados e administração de certificados emitidos
- Um *IBM SecureWay Directory* integrado
- Um subsistema de *auditoria*
- Suporte para o coprocessador criptográfico SecureWay 4758
- Suporte para *Smart Cards*

Esta infraestrutura suporta todo o ciclo de vida do certificado, incluindo inscrição e certificação inicial, atualização de par de chaves, renovação de certificado, publicação de lista de certificados e de revogação de certificados e revogação de certificado. Para obter mais informações consulte a seção Capítulo 14, “Requisitos e considerações sobre a instalação do produto Public Key Infrastructure” na página 75.

Toolbox

O FirstSecure Toolbox é um conjunto de ferramentas de segurança e relacionadas a segurança que podem fazer parte ou operar em paralelo com os componentes principais do FirstSecure. As ferramentas o ajudam a:

Integrar seus aplicativos com o FirstSecure.

Personalizar soluções e aplicativos utilizando o FirstSecure.

Criar aplicativos ISV e OEM que exploram FirstSecure.

As APIs dos conjuntos de ferramentas FirstSecure Toolbox suportam as seguintes funções de segurança:

Serviços de autorização

Serviços de certificado e gerenciamento

Serviços de diretório

Serviços de protocolo Secure Sockets Layer

Serviços de gerenciamento confiável e criptografia KeyWorks

— APIs IBM Key Recovery Service Provider 1.1.3.0 . O produto IBM Key Recovery Service Provider permite a recuperação de informações criptografadas.

— IBM Key Recovery Server 1.1.3.0. O produto IBM Key Recovery Server 1.1.3.0 é um aplicativo que, sob pedido autorizado, pode recuperar informações criptografadas quando as chaves não estão disponíveis, são perdidas ou danificadas.

Estes conjuntos de ferramentas fornecem interfaces padrão que os aplicativos podem utilizar para invocar serviços de segurança críticos e interfaces padrão que os provedores de segurança podem utilizar para conectar-se ao conjunto de ferramentas. As interfaces padrão são baseadas em CDSA (Common Data Security Architecture). Estes conjuntos de ferramentas estão disponíveis nos sistemas operacionais Windows NT, Solaris e AIX.

Implementation Services

O FirstSecure Implementation Services pode ajudar seu e-business a instalar e utilizar o FirstSecure rápida e eficientemente. Estes serviços, cobrados separadamente, são fornecidos pela IBM e são executados por uma equipe experiente de consultores. O FirstSecure Implementation Services inclui um FirstSecure Implementation Workshop e serviços de instalação QuickStart de nível de produto. A IBM também pode fornecer serviços de integração de sistema do FirstSecure que são personalizados para seu ambiente individual.

Entre em contato com um representante IBM para obter informações e opções de preço.

Capítulo 2. O que há de novo no Release 2

O Release 2 simplifica o planejamento e a instalação dos produtos IBM SecureWay FirstSecure. Os produtos individuais estão mais integrados, foram adicionados produtos e o gerenciamento e controle estão mais centralizados.

Policy Director

O produto Policy Director possui os seguintes aperfeiçoamentos:

- Suporte para o IBM SecureWay Directory para o armazenamento de informações de credenciais de usuários e de grupos.
- As últimas atualizações para a especificação de API de Autorização do Open Group.
- Habilidade para definir e editar credenciais de usuários de proxy IBM Firewall utilizando o Console de Gerenciamento do Policy Director.
- Um CAS (Credentials Acquisition Service) do Policy Director que fornece suporte para a utilização de serviços de autenticação externos.
- Suporte para autenticação baseada em certificado do lado do cliente utilizando o novo recurso Credentials Acquisition Service do Policy Director.
- A habilidade para escrever seu próprio serviço de aquisição de credenciais utilizando a interface IDL (Interface Definition Language) entre o WebSEAL e o CAS do Policy Director. O Policy Director também fornece a estrutura de servidor geral que suporta funções de servidor CAS do Policy Director, como inicialização, registro de servidor e identificação de sinal.
- A opção de utilização do mecanismo de túnel SSL (secure sockets layer) além do túnel GSS (generic security services).
- Utilização do console de Gerenciamento do Policy Director, ou a interface de linha de comandos, para gerenciar critérios de início de sessão e de senha.
- Utilização do Console de Gerenciamento do Policy Director, ou a interface de linha de comandos, para gerenciar usuários em sessão, grupos e recursos únicos (destino).
- Uma ferramenta de gerenciamento de senhas de destino de início de sessão único baseada na Web.
- Um processo de instalação integrado.

SecureWay Boundary Server

O produto SecureWay Boundary Server possui os seguintes aperfeiçoamentos:

Uma GUI (Graphical User Interface) de configuração unindo algumas funções do SecureWay Boundary Server e do Policy Director.

Uma nova TaskGuide de configuração unindo algumas funções do SecureWay Boundary Server e do Policy Director.

O que há de novo no produto IBM SecureWay Firewall para AIX e NT

O produto IBM SecureWay Firewall, também denominado IBM Firewall, possui os seguintes aperfeiçoamentos:

Aperfeiçoamentos de proxy de correio seguro

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 de mensagens (maneiras conhecidas de bloqueio de mensagens não desejadas), limites configuráveis do número de destinatários por mensagens de e-mail, limites configuráveis do tamanho máximo de uma mensagem.

Suporte anti-spoofing incluindo integração com mecanismos de autenticação fortes

Suporte para trap SNMP e suporte para o MADMAN MIB

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

Aperfeiçoamentos do protocolo Socks versão 5

O protocolo Socks versão 5 foi atualizado para incluir UNPW (autenticação de senha e nome de usuário), CRAM (autenticação de desafio/resposta) e plugins de autenticação.

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

Proxy HTTP

O produto IBM SecureWay Firewall fornece uma implementação de proxy HTTP com funções completas baseadas no produto WTE (IBM Web Traffic Express). O proxy HTTP identifica pedidos de navegador

eficientemente 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 e sem alterar seu ambiente de cliente para implementar o proxy HTTP.

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

O produto IBM SecureWay Firewall para AIX oferece numerosas extensões:

Suporte IPSec Aperfeiçoado

Suporte IPSec aperfeiçoado, incluindo 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.

Suporte para MP (Multiprocessador)

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

Aperfeiçoamento de Filtros

Melhor desempenho e mais flexibilidade com configuração. Você pode ajustar o desempenho de seu IBM SecureWay Firewall escolhendo onde localizar tipos diferentes de regras de filtro. Um indicador de freqüência fornece o número de vezes que uma conexão é utilizada.

Network Address Translation

Suporte para mapeamento de endereços de vários destinatários. Estes mapeamentos são de vários endereços particulares ou não registrados internos para um endereço legal registrado utilizando números de portas para criar mapeamentos únicos.

Assistente de configuração

Um assistente ajuda na configuração inicial do produto IBM Firewall. Este assistente de configuração permite que um usuário, que não possui muito conhecimento sobre o produto IBM Firewall, tenha uma configuração básica instalada e em uso rapidamente após a instalação.

Network Security Auditor

O NSA (Network Security Auditor) verifica se há furos ou erros de configuração em seus servidores de rede e no produto IBM Firewall. Ele está mais rápido e mais forte.

O que há de novo no MIMEsweeper para IBM SecureWay Release 2

Os aperfeiçoamento dos MAILsweeper incluem:

- Procura por palavras chave para bloquear correio ofensivo ou difamador e para evitar que dados valiosos saiam de sua empresa
- Bloqueio de recebimento de e-mail não desejado
- Bloqueio de envio ou recebimento de tipos específicos de arquivos por grupos ou indivíduos
- Bloqueio ou atraso de arquivos por tamanho para evitar contenção da rede

Os aperfeiçoamentos do WEBsweeper incluem:

- Bloqueio de acesso de funcionários a sites específicos que não sejam relacionados ao trabalho
- Ajuda na prevenção de invasões para extrair documentos através de HTML ou endereços de e-mail e informações do site através de cookies

O que há de novo no SurfinGate

O produto SurfinGate possui os seguintes aperfeiçoamentos:

- Inspeção de conteúdo JavaScript
- Monitoração de desempenho de missão crítica
- Maior gerenciamento de critérios
- Suporte para protocolos FTP (File Transfer Protocol) e HTTPS
- Integração de plugin com proxy HTTP firewall
- A habilidade para bloquear ou evitar download de arquivos executáveis específicos no computador de um usuário

Intrusion Immunity

Os produtos Intrusion Immunity agora incluem o Tivoli Cross-Site for Security.

O que há de novo no produto Tivoli Cross-Site for Security

O produto Tivoli Cross-Site for Security fornece detecção de violação. Ele permite que você monitore invasões de rede na integridade de seu e-business.

O que há de novo no produto Norton AntiVirus Solution Suite

O Norton AntiVirus Solution Suite, Release 3.0.4, inclui as seguintes versões atualizadas:

- Norton AntiVirus 5.02 para Windows 95/98 e Windows NT Workstation
- Norton AntiVirus 5.02 para Windows NT Server
- Norton AntiVirus para IBM Operating System/2 (OS/2) 5.02
- Norton AntiVirus OS/2 para Lotus Notes 2.0
- Norton AntiVirus para Lotus Notes 2.0
- Norton AntiVirus para Microsoft Exchange 1.5.2

Public Key Infrastructure

O componente Public Key Infrastructure agora inclui Trust Authority. O produto Trust Authority inclui:

- Um assistente de instalação para guiá-lo através de uma instalação simples no Windows NT.
- Uma configuração pré-definida para a placa criptográfica 4758. Você pode alterar estas informações.
- Um assistente de configuração que verifica a validade dos dados antes do programa de configuração de segundo plano começar.
- Mensagens e relatórios de erro.
- Documentação online, incluindo ajuda dependente de contexto para os Assistentes de Configuração, RA Desktop e aplicativo para cliente de entidade final.

IBM SecureWay Toolbox

O produto Toolbox possui os seguintes aperfeiçoamentos:

- Documentação e APIs do Policy Director
- APIs de serviço de diretório.
- APIs e documentação do PKIX (Public Key Infrastructure)

O IBM Key Recovery Server 1.1.3.0 agora é incluído no Toolbox. Ele está disponível apenas em inglês.

Parte 2. Planejamento de uma rede de e-business segura

A Parte 2 apresenta o planejamento para uma rede de e-business segura.

Os capítulos a seguir descrevem um tráfego de Internet típico e preocupações sobre segurança e depois apresentam como os produtos FirstSecure trabalham em sua rede de e-business.

Esta seção contém os seguintes capítulos:

Capítulo 3. Visão geral de uma rede de e-business

Sua rede de e-business é formada de recursos: dados e bancos de dados, usuários, clientes, fornecedores, programadores, hardware, informações sobre a empresa e assim por diante. Vamos verificar algumas destas áreas e ver onde a segurança é necessária.

A Internet é uma criação complexa. Os dados passam por ela de servidor a servidor e de usuário a usuário, em caminhos indefinidos que são alterados a cada transmissão.

Suas transmissões de dados comerciais através da Internet são misturadas com todos os outros tráfegos da Internet. Ao longo do caminho, dados vitais de sua empresa podem ter passado por qualquer servidor em qualquer lugar. E qualquer usuário da Internet pode ter tentado acessar seus recursos, seus funcionários e seus dados. Infelizmente, além do tráfego legítimo para educação, negócios e prazer, a Internet também carrega tráfego malicioso, tanto inocente como proposital. A Figura 1 na página 18 é uma visão geral da Internet com o tráfego passando através da Internet juntamente com o tráfego de todas as outras pessoas.

O FirstSecure o ajuda a separar e proteger suas transmissões de todos os outros tráfegos.

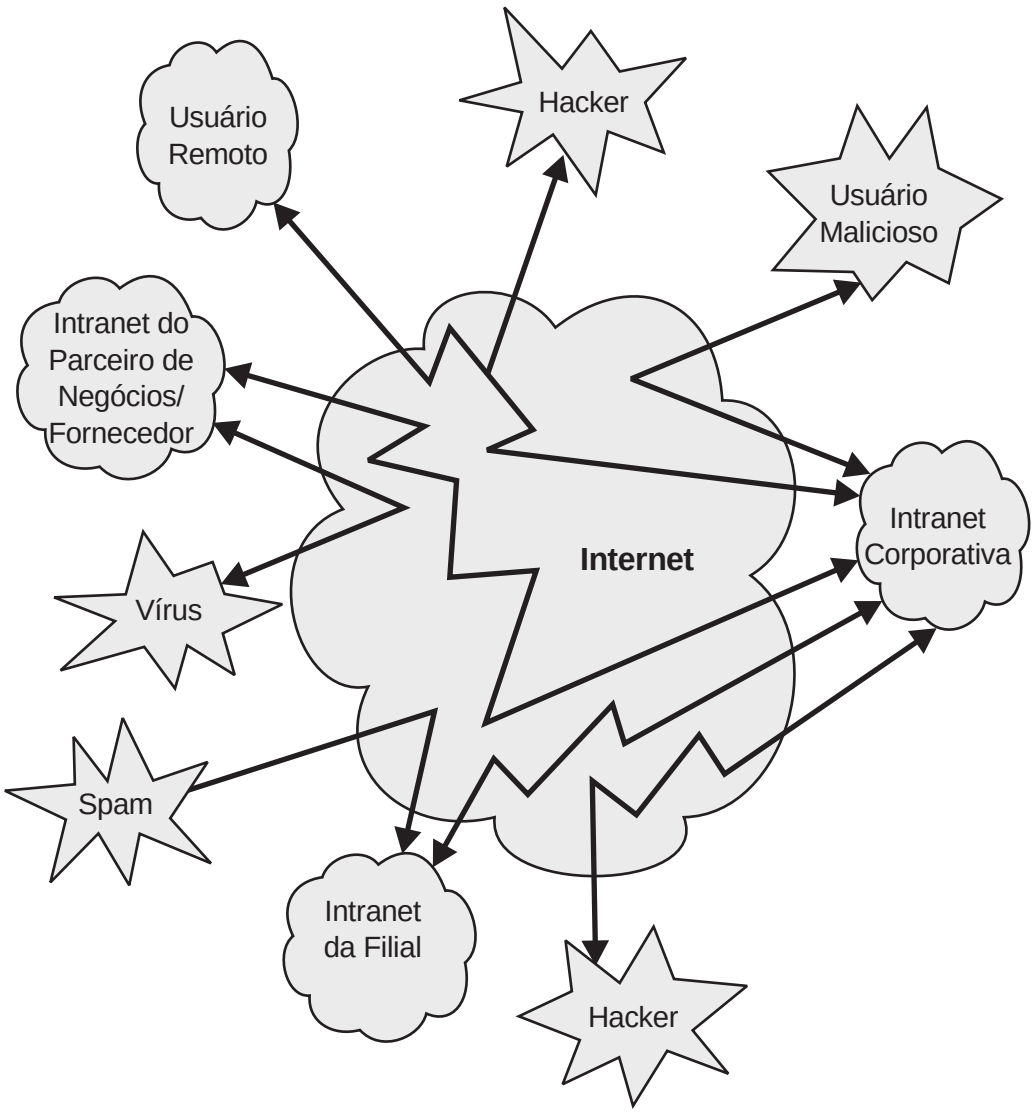


Figura 1. Visão geral da Internet ocupada com atividades não relacionadas

Você não deseja operar nesta exibição da Internet. Você deseja a exibição da Figura 2 na página 19, uma Internet protegida pelo FirstSecure.

A Internet ideal protegida pelo FirstSecure

A maioria do tráfego de e-business passa pela Internet. Mas você não deseja a exibição típica da Internet como uma coleção vasta de dados aleatórios

visíveis para praticamente qualquer pessoa que possua um computador pessoal. A Figura 2 na página 19 mostra a Internet que você deseja.

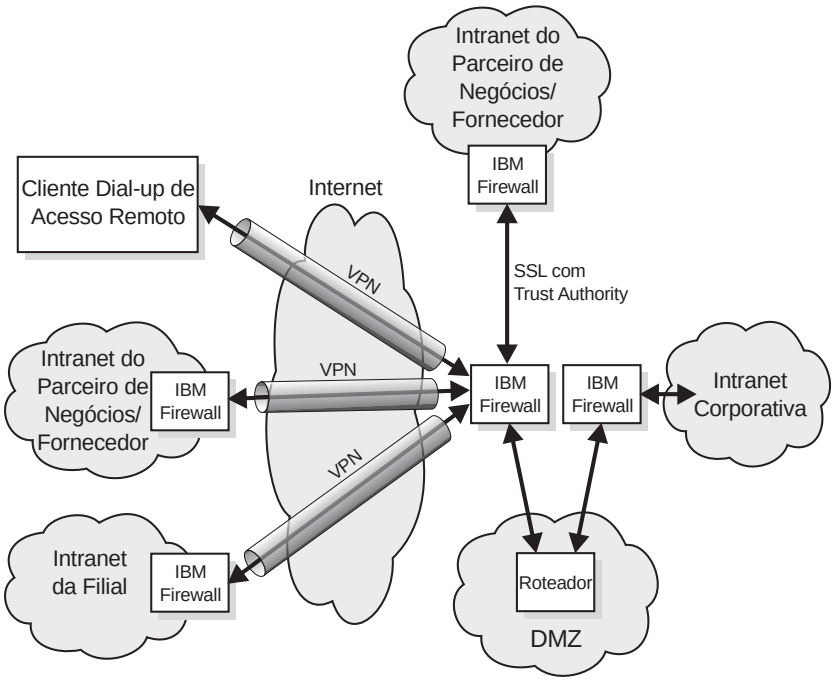


Figura 2. A Internet que você deseja

Embora existam muitas informações úteis disponíveis na Internet, existem também aplicativos, dados e acessos dos quais você deseja proteger sua empresa. Você deseja certificar-se de que

- Seus funcionários não fiquem distraídos das tarefas atribuídas a eles.
- Seus funcionários estejam protegidos contra e-mail inapropriado.
- Suas informações comerciais sensíveis permaneçam dentro de sua empresa.

A Rede Privada Virtual

Uma VPN (rede privada virtual) é o conceito de uma conexão privada, inacessível a outros, através da Internet. A Figura 3 na página 20 mostra uma VPN típica. A conexão é, para os usuários em cada extremidade, segura contra a invasão por usuários ou aplicativos indesejados. Os produtos FirstSecure, como o produto IBM SecureWay Firewall o ajudam a configurar e suportar VPNs.

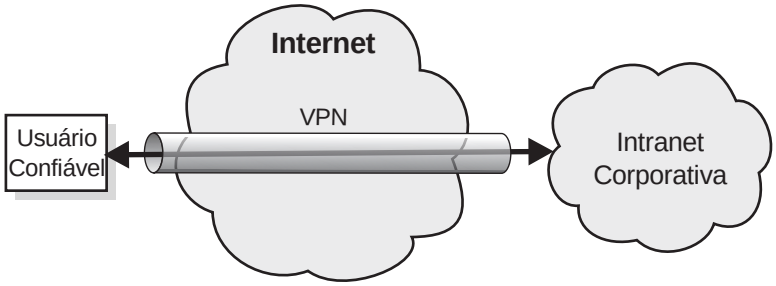


Figura 3. Uma rede privada virtual típica.

A demilitarized zone

A *DMZ (demilitarized zone)* é o corpo de recursos que você permite que usuários externos acessem. Você utiliza os produtos IBM Firewall, MIMEsweeper e outros produtos FirstSecure para assegurar que apenas usuários autorizados possam acessar a DMZ e que eles possam acessar apenas recursos específicos. O tráfego que entra e sai da DMZ deve ser monitorado para verificar se é apropriado.

O catálogo de sua empresa pode estar na DMZ para que qualquer possível cliente possa navegar por ele. Ou você pode possuir brochuras de informações que descrevem sua empresa. Os componentes do seu FirstSecure permitem que apenas usuários confiáveis acessem informações além da DMZ.

A Figura 4 na página 21 mostra uma DMZ típica.

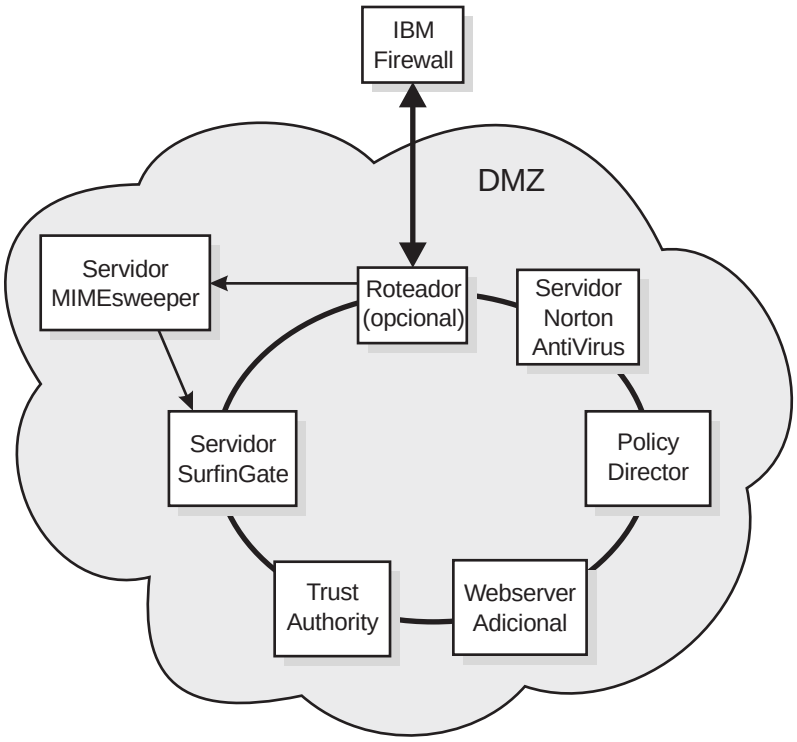


Figura 4. DMZ típica com recursos do sistema.

Conforme você desenvolve seus aplicativos seguros, você pode utilizar a DMZ como um teste de intranet antes de permitir acesso público a estes aplicativos.

Agora vamos considerar os tipos de informações para os quais você utiliza a Internet e a sua intranet.

Uma intranet corporativa típica

A intranet da sua corporação é o local para comunicação interna de sua empresa. Ela contém informações e recursos que não são compartilhados com a Internet. Seus funcionários compartilham dados, enviam e-mail uns para os outros, acessam recursos da corporação como bancos de dados, impressoras e scanners. A Figura 5 na página 22 mostra uma intranet corporativa típica.

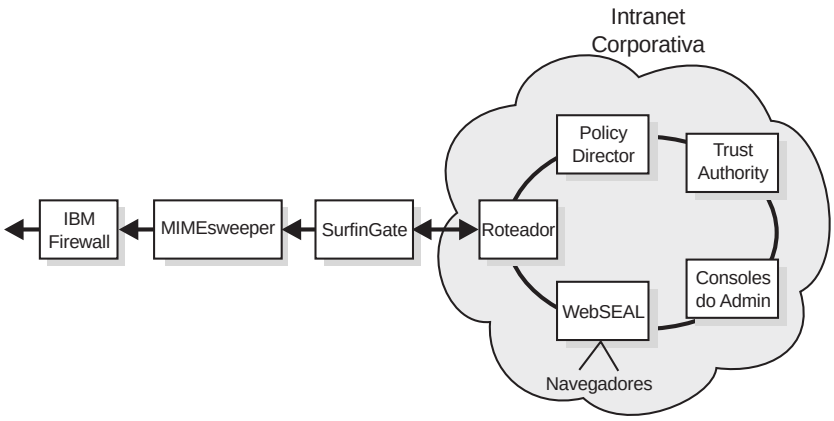


Figura 5. Visão geral de uma intranet corporativa típica

Você deve assegurar que as informações confidenciais de sua empresa permaneçam dentro de sua empresa e que apenas as pessoas autorizadas acessem estes dados. Entretanto, você possui alguns dados que deseja que os clientes utilizem e acessem. Por exemplo, você deseja que um depositante de seu banco possa verificar o saldo de sua conta, mas não deseja que o depositante acesse registros de funcionários. Seu produto IBM Firewall mantém as informações particulares privadas.

Os produtos IBM FirstSecure o ajudam a manter sua intranet segura. O Policy Director permite que você defina as regras de acesso. O IBM SecureWay Trust Authority certifica que os usuários sejam realmente quem alegam ser. O Tivoli Cross-Site for Security permite que você saiba se há tentativas não autorizadas de acessar os recursos de sua intranet.

Uma intranet típica de filial corporativa

Funcionários remotos em sua filial precisam de acesso aos mesmos dados e a outros recursos que seus funcionários locais. Mas, conexões telefônicas para enviar e receber informações são lentas e desprotegidas contra interferência maliciosa. Você deseja utilizar a Internet como medida de economia de custos e como um meio de adicionar proteção às suas transações. A Figura 6 na página 23 mostra uma filial típica se comunicando através da Internet com o escritório central.

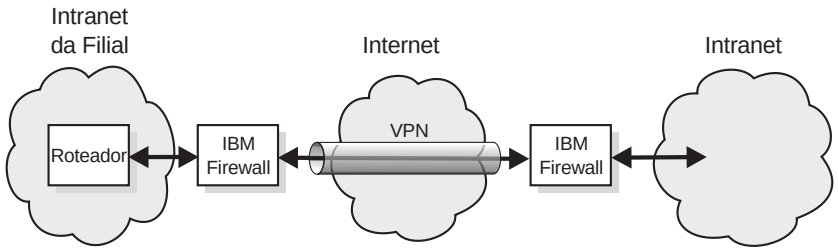


Figura 6. Filial conectada ao escritório central através de uma rede privada virtual

Você deseja que suas transmissões e dados estejam seguros como se estivessem em um local dentro de sua empresa. A *VPN (rede privada virtual)* é seu túnel através da Internet. Você utiliza a Internet como se fosse sua rede intranet privada.

Um funcionário de acesso remoto típico

Alguns funcionários podem, às vezes ou permanentemente, trabalhar remotamente em relação a seu escritório principal. Um funcionário pode acessar sua rede através da Internet com uma conexão dial-up ou alugada.

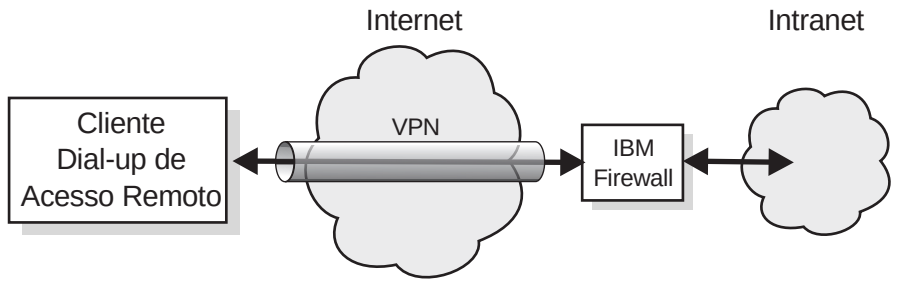


Figura 7. Cliente dial-up de acesso remoto conectado a um escritório principal através de uma rede privada virtual.

O produto IBM Firewall protege as transmissões deste funcionário.

Uma intranet de parceiro de negócios ou fornecedor típica

Seu negócio é mais eficiente quando seus parceiros de negócios e fornecedores podem acessar alguns de seu dados diretamente. Um fornecedor pode ser autorizado a verificar níveis de inventário e enviar novos estoques em níveis especificados. Outro parceiro de negócios pode ter acesso a registros específicos. Uma firma de contabilidade pode precisar de acesso a outros registros de imposto mas não aos registros do parceiro de negócios. A Figura 8 na página 24 e a Figura 9 na página 24 mostram um fornecedor ou

parceiro de negócios típicos. Você deseja que as transações comerciais atravessem a Internet como se estivessem passando por uma conexão privada.

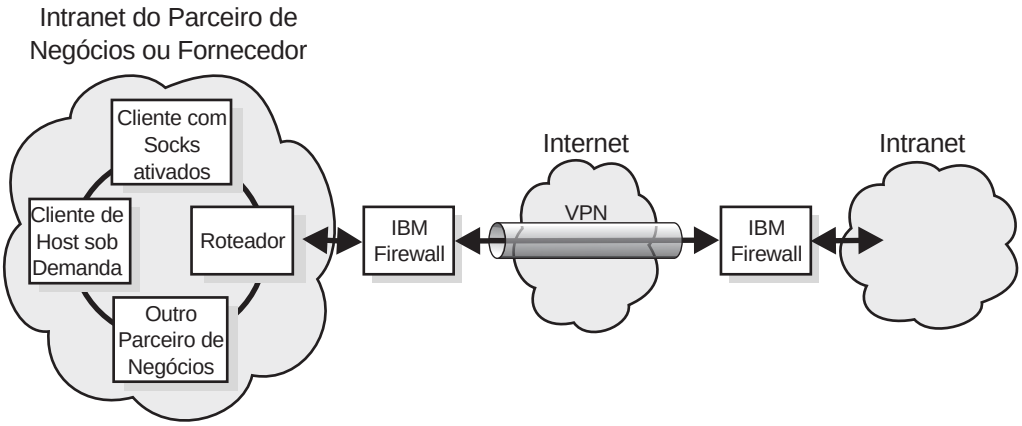


Figura 8. Intranet de parceiro de negócios ou fornecedor típica utilizando uma VPN (virtual private network)

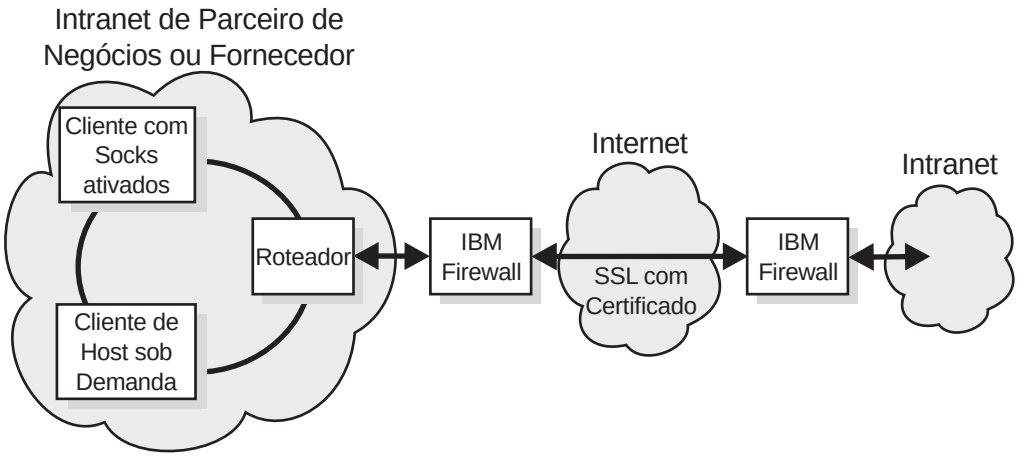


Figura 9. Intranet de parceiro de negócios ou fornecedor típica utilizando um protocolo de transmissão SSL (Secure Sockets Layer)

Este parceiro de negócios está utilizando SSL (Secure Sockets Layer) ao invés de utilizar uma VPN porque as transmissões são criptografadas de extremidade a extremidade. (O usuário também poderia utilizar uma VPN para ter uma camada adicional de segurança).

Estes usuários precisam ser protegidos uns dos outros, de interferência maliciosa e de invasores. Suas transmissões de dados precisam ser protegidas contra receptores remetentes não autorizados. Você também precisa assegurar que estes usuários acessem apenas os dados que você deseja que estejam

acessíveis. E você deseja assegurar que cada um destes usuários sejam os usuários que você espera.

Dados e bancos de dados

Os dados são um dos recursos mais valiosos para qualquer empresa. Alguns dados de e-business são projetados para estarem disponíveis para todos os usuários da Internet. Por exemplo, um distribuidor de hardware pode ter seu inventário e sua lista de preços disponíveis para compras online. Um revendedor de roupas pode ter um catálogo online ilustrado de estilos, cores e tamanhos para compras online.

Antes de conceder acesso aos dados, é necessário saber quem é o solicitador e porque os dados são desejados. Utilize o Trust Authority para emitir certificados para usuários confiáveis.

Outras áreas a serem protegidas

Este manual não discute contra-medidas para outras áreas de segurança. Você também precisa planejar para:

- Segurança do site, acesso, saída e divisão em compartimentos
- Segurança física de computadores laptop, computadores pessoais, estações de trabalho e outros tipos
- Verificações de segurança pessoal em background
- Renúncias legais de responsabilidade, contratos e afins
- Práticas operacionais como gerenciamento de chaves, controle de informações e conhecimentos e treinamento de segurança

O sistema operacional

A maioria dos sistemas operacionais são configurados para alta disponibilidade e para um rico conjunto de funções. Uma abordagem de segurança efetiva seria ter apenas as funções mínimas necessárias para realizar uma tarefa atribuída. Você deve considerar a remoção ou desativação de todos os recursos do sistema operacional que você não deseja que um invasor acesse.

Usuários típicos

A Internet possui vários tipos diferentes de usuários, alguns desejáveis, outros não. Um e-business deseja usuários que sejam clientes fazendo pesquisas e compras online. E e-business também deseja que parceiros de negócios possam acessar dados específicos para verificar inventários, tomar decisões de produção ou comentar sobre planos e atividades dentro da empresa. O

e-business também deseja que funcionários possam acessar os dados necessários para que realizem as tarefas atribuídas.

A Internet também possui usuários que um e-business não deseja: os hackers e spammers, os distribuidores de vírus, os usuários que desejam acessar seus dados confidenciais. Estes usuários podem até estar dentro de seu e-business.

Antes de conceder acesso a qualquer recurso, é necessário saber quem é o usuário que solicita, qual acesso o usuário deve ter aos dados e aplicativos e quais registros de acesso do usuário devem ser mantidos.

Aplicativos e criação de aplicativos

Os aplicativos podem ser projetados para incluir segurança. Você pode tirar vantagem da criptografia de dados a serem enviados, certificação de usuários que solicitam acesso, logs de auditorias de usuários e de transações.

As APIs do Toolbox permitem que você adicione segurança a seus aplicativos.

Segurança de hardware

Servidores e bancos de dados fazem parte de um sistema de segurança. Embora este manual não discuta sobre hardware, é necessário planejar a segurança física de servidores e de estações de trabalho utilizadas para gerenciamento de segurança.

Segurança de hardware do Trust Authority

Embora esta seção discuta especificamente componentes do Trust Authority, as considerações são aplicáveis a todos os componentes do FirstSecure.

Isolamento da área
: Instale o servidor em uma sala isolada dedicada à atividade de CA. Se for possível, a sala deve possuir paredes reforçadas, um única porta de madeira maciça ou de aço e um teto construído solidamente sem painéis de abertura. A sala também deve possuir um piso elevado para proteção contra descargas em caso de incêndio.

Manutenção da área
: A sala deve fornecer fonte de alimentação contínua aos computadores, acessórios de iluminação, detectores de movimento e sistemas de aquecimento e resfriamento. Você também deve verificar a ventilação da sala para assegurar que a temperatura seja suficiente para evitar aquecimento gerado pelo equipamento.

Controle de acesso da área
: Você pode fornecer acesso à área física de várias maneiras, por exemplo, utilizando crachás ou travas de portas controladas por teclado. Para evitar invasão maliciosa por um único indivíduo, você

deve instalar controles que requeiram a apresentação de credenciais apropriadas de pelo menos duas pessoas confiáveis.

Você também deve monitorar a sala para rastrear cada vez que a área de segurança é acessada e por quem. Para obter segurança máxima, instale detectores de movimento dentro e fora da porta.

Controle de comunicações

Não deve haver portas extras abertas no servidor Trust Authority. Você deve configurar o sistema para que atenda pedidos apenas nas portas explicitamente atribuídas a aplicativos Trust Authority ativos.

Siga os procedimentos e os requisitos de sua própria empresa para proteger o hardware utilizado em seu e-business.

Capítulo 4. Planejamento para FirstSecure na sua rede de e-business

Os capítulos a seguir nesta parte ligam os produtos incluídos no FirstSecure a seu e-business. Os capítulos se baseiam nas ilustrações da seção Capítulo 3, “Visão geral de uma rede de e-business” na página 17. Cada produto é descrito em algum detalhe. Para obter informações completas sobre um produto, consulte a documentação fornecida com o produto. Os cenários de implementação são apenas sugestões.

Em cada cenário de implementação, as mesmas etapas básicas são seguidas:

1. Faça com que todas as partes de sua rede utilizem uma referência de horário comum para que os logs de auditoria sejam mais simples e mais exatos.
2. Comece dentro de sua intranet para instalar e testar componentes.
3. Quando estiver confortável dentro da intranet, comece a criar aplicativos dentro de sua DMZ (demilitarized zone).
4. O tráfego entre sua intranet e a demilitarized zone deve passar através de um firewall.
5. Crie seus aplicativos de Internet externos e teste-os com dados de teste.
6. Instale um firewall para proteger o tráfego entre a Internet e sua DMZ.
7. Permita o acesso de usuários à sua rede.

Planejamento de um sistema FirstSecure completo

Aqui você encontra uma sugestão da ordem para a implementação dos produtos FirstSecure em sua rede. Ela está bastante simplificada. Para obter os requisitos de software e hardware detalhados de cada produto e as considerações de integração, consulte a Parte 3, “Considerações sobre instalação e integração” na página 53. Além disso, leia os requisitos de instalação e as instruções fornecidas com cada produto. Vários produtos também possuem informações atualizadas disponíveis na Internet. A seção “Informações da Web” na página xi lista os sites da Web que possuem informações sobre o FirstSecure. O Redbook, *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498 contém vários outros cenários detalhados.

1. Planeje os requisitos de segurança necessários.
2. Instale o Policy Director para atender a estes requisitos.
3. Crie e teste os aplicativos do servidor para clientes. Mantenha-os dentro da intranet corporativa, não os torne disponíveis na Internet ainda.

4. Instale o produto IBM Firewall que protege os aplicativos do servidor para clientes.
5. Adicione o produto SurfinGate à DMZ.
6. Em sua DMZ (demilitarized zone), adicione o MIMEsweeper e o Norton AntiVirus para proteger seus aplicativos quando eles forem disponibilizados na Internet. Quando torná-los disponíveis para tráfego externo, configure-os para apontar para seus servidores.
7. Instale o produto Tivoli Cross-Site for Security para obter imunidade e detecção de invasão.
8. Dentro de sua DMZ, adicione:

   Servidores da Web

   Servidores de catálogo da Web

   Servidores de inventário da Web

   Aplicativos clientes para clientes

   Aplicativos clientes seguros para clientes

   Um ou mais produtos Cross-Site for Security agent

   Teste todos seus aplicativos dentro do firewall antes de abri-los para tráfego. Utilize a ferramenta SecureWay Boundary Server's Network Security Auditor para testar as regras definidas.
9. Instale uma instância do produto IBM SecureWay Firewall para proteger o software dentro de sua DMZ. Sua configuração padrão deve ser “Sem tráfego” para que você possa testar a instalação antes de abri-la para o público.
10. Instale o Trust Authority e emita certificados para usuários confiáveis.
11. Abra seu aplicativo para a Internet depois de ter concluído todos os testes.
12. Execute o Network Security Auditor de fora do sistema para testar as regras antes de anunciar acesso ao público.
13. Verifique os logs de auditoria criados pelos programas componentes do FirstSecure para assegurar que não tenham ocorrido incidentes desfavoráveis.
14. Continue a verificar os logs de auditoria e adicione produtos Cross-Site for Security agent a medida que você adicionar aplicativos à sua rede.

Capítulo 5. Planejamento do Policy Director em sua rede

O software FirstSecure proporciona um ponto de controle consolidado, orientado por critérios, para ambientes heterogêneos da Web. Em ambientes onde os usuários acessam vários servidores da Web de programa emissor através de navegadores, o Policy Director fornece

Um início de sessão único para cada usuário da Web

Verificação de identificação

Verificação de autorização para usuários que solicitam acesso a páginas da Web protegidas

Com este suporte, você pode autorizar e proteger:

Trocas TCP/IP, como HTML, Telnet e POP3

Aplicativos de terceiros, como sistemas de banco de dados

Ferramentas de gerenciamento de rede

Aplicativos desenvolvidos internamente

Com o software FirstSecure, os usuários podem autenticar-se no componente Policy Director utilizando os seguintes mecanismos:

Autenticação básica via SSL (Secure Sockets Layer)

Início de sessão baseado em formulários através de SSL

SSL que utiliza certificados de clientes

Início de sessão Kerberos

Então, o software FirstSecure controla o acesso de usuários autenticados a objetos da Web individuais e pode limitar usuários não autorizados a um subconjunto destes recursos.

Implementação do Policy Director

O componente Policy Director gerencia o mapeamento entre usuários, grupos e recursos. Você usa o console de gerenciamento do Policy Director para:

Definir os usuários e grupos que utilizarão seus recursos.

Definir os objetos que precisam de proteção. Os objetos podem ser a Web, portas TCP, métodos e interfaces.

Definir como os usuários acessarão os recursos e quais serão as regras de proteção dos recursos, como ler, modificar, administrar, executar ou excluir.

A tabela a seguir descreve as configurações comuns do componente Policy Director. Determine a configuração apropriada para sua rede. Depois selecione os componentes durante a instalação.

Para obter mais detalhes consulte a seção *IBM SecureWay Policy Director Up and Running*.

Exemplo de Configuração	**Componentes Instalados**
Um servidor qu executa uma única ocorrência do servidor de Gerenciamento para o domínio seguro. Neste cenário, o servidor de Gerenciamento está localizado sozinho em seu sistema. O servidor de Gerenciamento mantém o banco de dados principal de autorização do domínio seguro, replica este banco de dados através do domínio seguro e mantém as informações de localização sobre outras máquinas de servidores Policy Director no domínio seguro.	Apenas servidor de Gerenciamento
Um servidor WebSEAL. Este cenário representa a solução para proteção de um espaço na Web. O WebSEAL suporta servidores de programa emissor, para alta disponibilidade e tolerância a falhas.	Gerenciador de Segurança com WebSEAL
Um servidor NetSEAL. Este cenário representa a solução para proteger uma VPN (Virtual Private Network) e fornece controle de acesso para serviços de rede legacy e de terceiros.	Gerenciador de Segurança com NetSEAL
Uma combinação dos servidores WebSEAL e NetSEAL.	Gerenciador de Segurança com WebSEAL e NetSEAL
Um servidor que fornece acesso ao Serviço de Autorização do Policy Director para aplicativos de terceiros.	Servidor de Autorização
Um servidor que fornece um ambiente de desenvolvimento para desenvolvedores que desejam criar aplicativos de terceiros que utilizam a API de autorização.	Servidor de Autorização e ADK
Um servidor que fornece os serviços combinados de todas as configurações acima.	Todos os componentes

O componente Policy Director é um sistema de segurança altamente distribuído que pode implementar seus componentes em várias configurações em uma ou mais máquinas. A seguir temos uma visão geral de implementação do componente Policy Director em sua rede. Instruções de

instalação completas são encontradas na seção *IBM SecureWay Policy Director Up and Running*.

1. Instale o servidor de segurança do Policy Director.

   Pelo menos um computador no domínio seguro deve conter o servidor de segurança do Policy Director para configurar um domínio seguro do Policy Director. Consulte os manuais de instalação e de administração e os recursos de suporte técnico de suas plataformas necessárias.

   Os servidores restantes podem funcionar apenas com instalações de cliente DCE (ou NetSEAT em sistemas Windows NT).
2. Instale o servidor LDAP (SecureWay Directory).
3. Instale o componente Policy Director.

   O servidor de segurança do componente Policy Director deve ser implementado primeiro (consulte a etapa 1).

   Todas as instalações de servidor Policy Director requerem o Policy Director Base.

   Se esta for a *primeira* ou *única* máquina no domínio seguro, você deve instalar o servidor de Gerenciamento.

   Se esta for uma máquina *adicional* em um domínio seguro com um servidor de Gerenciamento existente, não instale outro servidor de Gerenciamento. Deve haver apenas uma ocorrência do servidor de Gerenciamento em qualquer domínio seguro.

   WebSEAL, NetSEAL e componentes de servidor de autorização de terceiros são opcionais.

   O Gerenciador de Segurança combina com o WebSEAL para fornecer o componente de servidor HTTP do WebSEAL e controle de acesso refinado HTTP, e com o NetSEAL, para fornecer o componente de controle de acesso grosseiro TCP/IP do NetSEAL.
4. Instale o Console de Gerenciamento.

   O Console de Gerenciamento requer que você instale um cliente DCE (ou NetSEAT para Windows NT) no sistema operacional (consulte a etapa 1).
5. As dependências a seguir se aplicam aos aplicativos desenvolvidos com o ADK de Autorização:

   Você precisa do pacote do componente Policy Director.

   Instale IVAuthADK na máquina do aplicativo.

   O sistema operacional em que o aplicativo é executado deve possuir um cliente DCE ou NetSEAT para sistemas Windows NT.

   O domínio seguro que executa um aplicativo deve possuir um servidor de Autorização instalado em pelo menos um computador no domínio seguro. Um ambiente de desenvolvimento típico inclui o

servidor de Autorização no mesmo sistema operacional do ADK de Autorização.

Capítulo 6. Planejamento do SecureWay Boundary Server em sua rede

O software FirstSecure fornece segurança para aplicativos baseados na Web que tiram proveito de padrões de segurança existentes como SSL (Secure Sockets Layer), SOCKS e IPSec.

Se o seu ambiente operacional inclui conexões entre duas partes da rede com diferentes características asseguradas, o componente SecureWay Boundary Server do software FirstSecure pode ajudá-lo a endereçar os seguintes requisitos:

- Conexões protegidas com a Internet, minimizando a possibilidade de acesso não-autorizado à sua rede privada
- Infra-estruturas de extranet de larga escala para compartilhamento seletivo de dados com parceiros de negócios e fornecedores
- Utilização da Internet ou de outros segmentos de rede relativamente não assegurados, como uma rede privada virtual (VPN), com a manutenção da confidencialidade das mensagens conforme elas atravessam a infra-estrutura da rede não assegurada

O componente SecureWay Boundary Server do software FirstSecure utiliza tecnologias de filtragem de endereços de rede, filtragem de conteúdo, proxy e gateway em nível de circuito. Através da combinação destas tecnologias, o componente SecureWay Boundary Server ativa operações de e-business protegidas, seguras e orientadas por critérios, através do controle da comunicação entre redes com diferentes características asseguradas.

O produto SecureWay Boundary Server inclui:

- IBM SecureWay Firewall, inclusive ACE/Server
- MIMEsweeper para IBM SecureWay Release 2
- SurfinGate 4.05 para Windows NT
- Aperfeiçoamentos para gerenciamento de critério

Consulte a seção Figura 10 na página 36 para obter uma visão geral do fluxo de dados em uma instalação completa do SecureWay Boundary Server.

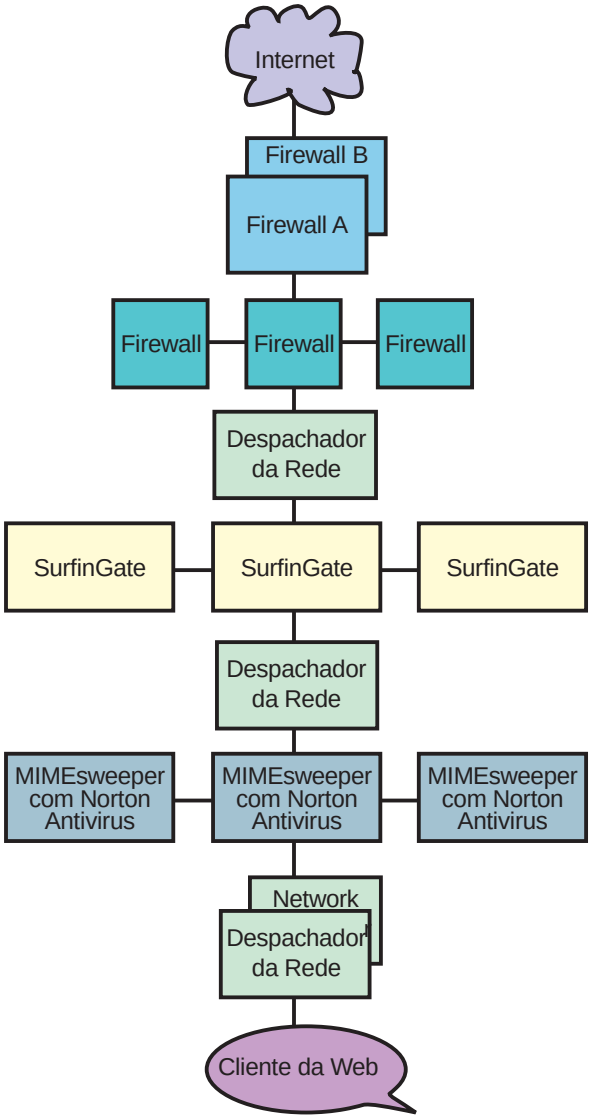


Figura 10. Visão geral de um fluxo de dados nos produtos SecureWay Boundary Server

Implementação do IBM SecureWay Firewall

O produto IBM SecureWay Firewall, também denominado IBM Firewall, controla comunicações recebidas e enviadas pela Internet. Esta tecnologia de firewall protege os próprios ativos da IBM.

Par obter considerações de instalação consulte a seção “Considerações do componente SecureWay Boundary Server” na página 62.

Entre as suas preocupações com a rede, estão:

- A necessidade de conexão com a Internet, porém impedindo o acesso não autorizado à sua rede, aos seus aplicativos e aos seus dados
- Abuso de seus ativos de rede por usuários internos
- Maneiras de planejar uma infra-estrutura de extranet de larga escala para parceiros de negócios e fornecedores, apesar do alto custo do gerenciamento de configuração
- O alto custo das linhas dedicadas que conectam as filiais
- Baixa produtividade nos negócios, causada por comunicações não eficazes, atrasadas ou mal-interpretadas com parceiros ou fornecedores
- O alto custo administrativo do gerenciamento de software em idiomas não nativos

O produto IBM Firewall resolve essas preocupações. Permitindo apenas o tráfego autorizado explicitamente no firewall, o produto IBM Firewall protege sua rede contra intrusos. Para proteção adicional, o software de verificação de vulnerabilidade fornecido com o IBM Firewall pode *fortalecer* o servidor em que o IBM Firewall está sendo executado, para garantir que hackers passem pelo firewall. Os endereços IP e a configuração da rede interna são ocultados da rede não assegurada. Todo o tráfego através do firewall é registrado em log e pode ser utilizado para gerar relatórios de atividades de usuários.

O produto IBM Firewall e seu aplicativo de configuração VPN permitem que você implemente e gerencie com economia infra-estruturas VPN de larga escala. Estudos de redes têm mostrado que clientes podem utilizar VPNs para realizar grandes economias sobre o custo de soluções de linhas dedicadas.

Com o produto IBM Firewall, você pode interconectar suas filiais utilizando a Internet, através da implementação de firewalls em cada filial e da utilização de um túnel baseado em IPSec.

O produto IBM Firewall é fornecido com o ACE/Server, um produto da Security Dynamics Technologies, Inc., que fornece serviços de autenticação fortes e centralizados para redes de empresas, de modo que apenas usuários autorizados possam acessar arquivos, aplicativos e comunicações da rede. Junto com o produto SecurID, patenteado pela Security Dynamics Technologies, Inc., o ACE/Server cria uma barreira contra acesso não autorizado. A autenticação se baseia em dois fatores: para serem autenticados, os usuários precisam *possuir* alguma coisa (um cartão de token SecurID) e *conhecer* alguma coisa (um PIN).

Implementação do produto MIMEsweeper

O MIMEsweeper é um produto da Content Technologies Ltd. que executa uma análise baseada em conteúdo de dados da Internet e da intranet para identificar ameaças ocultas e proteger os usuários da sua rede dessas ameaças.

Para obter considerações de instalação consulte a seção “Considerações do componente SecureWay Boundary Server” na página 62.

O MIMEsweeper contém dois módulos básicos, MAILsweeper e WEBsweeper, que protegem seus usuários de diferentes maneiras. À medida que os dados de correio (mail) e outros dados da Web entram, o MIMEsweeper e o MIMEsweeper verificam os endereços do remetente e do destinatário e desagrupam recursivamente os arquivos em suas partes componentes. Em seguida, o MAILsweeper e o WEBsweeper analisam estas partes para minimizar o risco da entrada de ameaças em sua rede privada.

O produto FirstSecure inclui o MAILsweeper 4.0 e o WEBsweeper 3.2_5. Cada um pode ser instalado, configurado e utilizado separadamente.

O produto MAILsweeper pode:

Trabalhar com os programas anti-vírus escolhidos, para verificar se os arquivos desagrupados não possuem vírus

Detectar e bloquear vírus em macros

Pesquisar palavras-chave para:

— Auxiliar na proteção contra linguagem ofensiva em e-mail

— Auxiliar na proteção contra a saída de dados valiosos da empresa

Bloquear a chegada de spam por e-mail, deixando a rede menos congestionada e minimizando a perda de produtividade dos funcionários

Impedir que indivíduos ou grupos enviem ou recebam determinados tipos de arquivos, como AVIs ou MPEGs

Bloquear ou atrasar a transmissão de arquivos com base no tamanho, até que a rede possa acomodar melhor o tráfego

O produto WEBsweeper pode:

Bloquear o acesso de funcionários a determinados sites, que provavelmente não estejam relacionados ao trabalho

Auxiliar na proteção contra perda inadvertida de documentos confidenciais ou sensitivos

Além disso, o MIMEsweeper contém uma API (application programming interface) que pode ser utilizada para integrar bloqueadores de URL de terceiros.

O produto MIMEsweeper pode ser um ativo de grande importância na proteção de sua empresa e de seus usuários contra ameaças de segurança provenientes da Internet.

Nota: Mesmo que a documentação do MIMEsweeper forneça informações para contato com a Content Technologies para assistência e suporte, se a sua cópia do produto MIMEsweeper para IBM SecureWay Release 2 foi obtida como parte da oferta SecureWay FirstSecure ou da oferta SecureWay Boundary Server, você deve entrar em contato com a IBM quando precisar de assistência e suporte.

Implementação do produto SurfinGate

SurfinGate, um produto da Finjan Software Ltd., que inspeciona código móvel como o código JavaScript, applets Java e controles ActiveX, para proteger sua rede contra danos tais como modificação de dados, exclusão de informações e coleta ilícita de dados. O produto SurfinGate inspeciona códigos móveis em nível de gateway e identifica códigos que apresentam ameaça antes deles entrarem em sua rede. O código móvel pode ser bloqueado ou permitido seletivamente para determinados usuários ou departamentos, e o acesso ao código pode ser permitido ou negado à rede de sua empresa com base nas funções do código. Com o SurfinGate, os administradores podem ativar o código móvel e gerenciar, controlar e reforçar os critérios de segurança de toda a empresa referentes a ActiveX, Java, JavaScript, Visual Basic Script, Plugins e Cookies.

O SurfinGate inclui os seguintes componentes:

SurfinGate Server
SurfinConsole
Banco de dados SurfinGate
Plugin para integração WTE

O SurfinGate Server atua como um servidor proxy HTTP ou como um serviço para o firewall ou proxy. O SurfinGate Server pode ser posicionado depois do firewall corporativo e de outros proxies existentes e também atua como um servidor HTTP. Esta arquitetura permite que o tráfego de código móvel seja interrompido e inspecionado antes que os ataques ocorram.

Um administrador de rede utiliza o SurfinConsole para gerenciar e definir critérios de segurança corporativos centralizados para código móvel. O SurfinConsole pode controlar múltiplos SurfinGate Servers na rede e pode reforçar as regras para código móvel em toda a empresa por usuário ou por grupo ou através de listas personalizadas de código inaceitável/aceitável.

O banco de dados SurfinGate armazena detalhes de ASPs (Applet Security Profiles), incluindo informações sobre usuários e grupos e seus critérios de

segurança correspondentes. Como o SurfinGate inspeciona o conteúdo de todo o código móvel de modo dinâmico, o banco de dados não é requerido para segurança, mas ajuda a melhorar o desempenho em operações de larga escala.

Nota: Mesmo que a documentação do SurfinGate forneça informações para contato com a Finjan para assistência e suporte, se a sua cópia do produto SurfinGate para Windows NT foi obtida como parte da oferta SecureWay FirstSecure ou da oferta SecureWay Boundary Server, você deve entrar em contato com a IBM quando precisar de assistência e suporte.

Capítulo 7. Planejamento do Intrusion Immunity em sua rede

As tecnologias de segurança descritas até agora enfatizam a proteção contra ameaças de segurança. Um aspecto igualmente importante da segurança é a detecção de ameaças. Os produtos de imunidade contra violação do FirstSecure oferecem detecção de invasão e recursos anti-vírus, que permitem à sua empresa detectar as ameaças de segurança.

O software anti-vírus fornece proteção contra códigos maliciosos, incluindo cavalos de Tróia, worms, vírus de macro, controles ActiveX e applets Java trapaceiros. A proteção contra vírus é uma parte essencial de qualquer solução de segurança. Os produtos antivírus do FirstSecure resolvem estes requisitos chave de antivírus:

- Cobertura de um grande conjunto de clientes para ter uma abordagem abrangente e consistente das necessidades de antivírus de clientes estáticos e móveis.
- Serviço de subscrição para assinaturas de vírus. A atualização regular de assinaturas de vírus é crucial para manter proteção efetiva contra as últimas formas de código malicioso.
- Distribuição orientada por critérios das atualizações de antivírus dos servidores para os clientes para assegurar que seus critérios de antivírus tenham efeito.

Implementação do produto Tivoli Cross-Site for Security

O produto Tivoli Cross-Site for Security fornece detecção de violação baseada em rede para sistemas que podem ser vulneráveis a invasão. Você pode implementar os agentes Tivoli Cross-Site for Security em qualquer lugar em que seu domínio administrativo seja conectado com a Internet. O produto Tivoli Cross-Site for Security monitora redes para detectar ataques internos e externos. Ele apresenta os seguintes benefícios:

- Detecção de invasão em tempo real que alerta o administrador Cross-Site for Security sobre possíveis ataques.
- Critérios configuráveis que permitem que você defina diferentes critérios para agentes em sua DMZ e agentes em sua intranet
- Modificações online de critérios de agentes Security que permitem que você responda rapidamente a ambientes em modificação
- Integração com aplicativos do Tivoli's Enterprise para que você possa aumentar seu sistema de gerenciamento do Tivoli Enterprise

O Tivoli Cross-Site for Security pode:

- Detectar varreduras e vazamentos
- Monitorar tráfego IP
- Monitorar serviços de porta
- Detectar DNS, serviço de montagem e pedidos e respostas de sistema de arquivos da rede
- Detectar pedidos de serviços portmapper e dumps de respostas
- Detectar chamadas RStatd
- Detectar pedidos de nomes de mapas e nomes de arquivos específicos
- Detectar ataques com base em SMB em servidores de arquivos de PC
- Detectar protocolo de mensagem de controle de Internet

O produto Cross-Site for Security permite que você monitore o tráfego da rede e detecte tentativas de ataques e invasões. Ele monitora o tráfego tanto em sua DMZ que isola sua intranet da Internet e em sua rede interna.

Os tipos de invasões que o Cross-Site for Security pode detectar incluem:

- Detecção de assinatura ou modelo
- Detecção de vazamento
- Ataques com base na rede
- Ataques na rede do Windows
- Ataques de procedimentos remotos
- Exploração de serviços
- Tráfego de rede não autorizado
- Atividades suspeitas

O Cross-Site for Security protege sua rede utilizando o Cross-Site for Security agent e o servidor de gerenciamento Cross-Site for Security. Quando um agente detecta um ataque crítico, ele envia um evento criptografado para o servidor de gerenciamento Cross-Site for Security que, imediatamente, registra as informações e responde. Você pode configurar o servidor de gerenciamento Cross-Site for Security para enviar um alerta para o console, enviar um e-mail para um administrador ou avisar um administrador sob chamada.

Obtenção de um código de licença do Tivoli Cross-Site for Security

Para ativar seu produto Tivoli Cross-Site for Security, é necessário um código de licença personalizado.

Você pode receber o código de licença acessando o site do Tivoli Cross-Site na web e seguindo as etapas a seguir:

1. Localize o documento Passport Advantage Proof of Entitlement fornecido com seus produtos FirstSecure, inclusive o CD-ROM do Tivoli Cross-Site for Security e também o *Tivoli Cross-Site for Security Installation*.
2. Localize o número do pedido, um número de oito dígitos começando com 5, e seu número de cliente (site), um número de sete dígitos começando com 7, em seu Passport Advantage Proof of Entitlement. Estes números são utilizados para acessar o site do Tivoli Cross-Site na web pela primeira vez.
3. Inicie sessão no site do Tivoli Cross-Site na Web utilizando um navegador da web em um computador com acesso à Internet. A URL do site da web é `www.cross-site.com/support/licensing/`.
4. Digite seu número de pedido, seu número de cliente e informações para contato. Você também deve fornecer o nome do domínio do servidor em que planeja instalar o Tivoli Cross-Site for Security.
5. Siga as instruções adicionais na web.
6. Se você tiver problema ao acessar o site da web referente à chave de licença do Tivoli Cross-Site , entre em contato com o Representante IBM.

Produtos relacionados ao Tivoli Cross-Site

A família de produtos Tivoli Cross-Site inclui outros componentes que não fazem parte da família FirstSecure:

O Tivoli Cross-Site for Availability monitora e relata a qualidade de acesso de usuários finais a seu site na Web.

O Tivoli Cross-Site for Deployment estende o alcance de sua empresa, permitindo que você distribua e gerencie aplicativos e informações críticas através da Internet.

Embora estes produtos possam ser mencionados na documentação do Tivoli Cross-Site for Security, eles devem ser adquiridos separadamente.

Monitoração de tráfego com o Tivoli Cross-Site for Security

O Cross-Site for Security agent é um rastreador inteligente de rede. Ele monitora continuamente os pacotes na rede. O Cross-Site for Security agent filtra estes pacotes procurando várias assinaturas que representam atividade suspeita. Estas assinaturas podem indicar ataques na rede.

O Cross-Site for Security agent é executado como um *daemon* no sistema UNIX, e como um serviço do NT no sistema Windows NT. O Cross-Site for Security é configurado para iniciar automaticamente quando o sistema for iniciado. Ele permanece residente e é executado em background no sistema mesmo que não haja usuários com sessão iniciada.

Quando um possível ataque é detectado, o agente determina a gravidade e determina se o servidor de gerenciamento deve ser avisado imediatamente ou

se o alerta é registrado em um arquivo local. São feitos uploads periódicos dos registros para o servidor de gerenciamento.

O agente também entra em contato regularmente o servidor de gerenciamento Cross-Site for Security para informar que o agente está ligado e em execução. Este tipo de comunicação é denominada *pulsação*. Você pode configurar os intervalos de pulsação.

Quando o servidor de gerenciamento recebe uma pulsação do agente, o servidor de gerenciamento notifica o agente sobre qualquer informação de configuração atualizada, novas assinaturas e planejamentos de uploads. O agente automaticamente faz downloads e instala estas atualizações.

Tivoli Cross-Site for Security em sua rede

Você pode configurar o Cross-Site for Security para se ajustar às necessidades de sua empresa. As decisões principais são:

Onde instalar o servidor de gerenciamento Cross-Site for Security?

Quantos Cross-Site for Security agent são necessários?

Onde instalar os Cross-Site for Security agent?

Estas considerações, além do tamanho, topologia, tráfego e largura de banda da rede, são indispensáveis na determinação do número de servidores e agentes de gerenciamento. Para obter considerações de instalação para o Tivoli Cross-Site for Security consulte a seção “Requisitos de hardware e software do Intrusion Immunity” na página 67.

Nota: Embora a documentação do Tivoli Cross-Site for Security possa descrever assistência e suporte, se sua cópia do Tivoli Cross-Site for Security foi obtida como parte da oferta SecureWayFirstSecure, você deve entrar em contato com a IBM para obter assistência e suporte.

Implementação do Norton AntiVirus

O Norton AntiVirus, da Symantec Corporation é um dos líderes mundiais na área de produtos de software antivírus. O produto Norton AntiVirus pode:

Deixar arquivos infectados em quarentena

Proteger contra vírus e controles ActiveX e applets Java maliciosos

Proteger contra vírus que podem estar contidos em anexos de mensagens de e-mail, downloads da Internet, disquetes, CDs de software ou na rede

Você pode planejar o Norton AntiVirus para ser executado constantemente em background para ajudar a manter seu computador seguro. Os pesquisadores da Symantec sempre adicionam os vírus que o Norton AntiVirus pode detectar. Você pode utilizar o recurso LiveUpdate para obter

novas definições de antivírus da Symantec automaticamente, uma vez por semana.

O recurso de quarentena do Norton AntiVirus isola arquivos infectados ou suspeitos em uma localização segura de seu computador, separada de outros arquivos para evitar que o vírus se espalhe enquanto o arquivo é corrigido.

O assistente Scan and Deliver permite que você envie arquivos suspeitos à Symantec para avaliação. O centro de pesquisa SARC (Symantec AntiVirus Research Center) responde para ajudá-lo a corrigir o problema.

O scanner do Norton AntiVirus , *Bloodhound*, é executado em background para observar e classificar o comportamento de aplicativos que estejam potencialmente infectados por novos vírus. Se um aplicativo se comporta como um vírus e tenta infectar outros programas, o Bloodhound pode parar o programa, impedindo a infecção de outros arquivos até que você receba novas atualizações de vírus.

Os produtos Norton AntiVirus Solution Release 3.04 fornecidos no software FirstSecure são:

Soluções para Desktops:

— Norton AntiVirus 4.08 for DOS
— Norton AntiVirus 4.08 for Windows 3.51
— Norton AntiVirus 5.02 for Windows 95/98
— Norton AntiVirus 4.08 for Windows NT 3.51
— Norton AntiVirus 5.02 for Windows NT 4.0
— Norton AntiVirus 5.03 for Macintosh
— Norton AntiVirus 5.02 for OS/2

Soluções para Servidores:

— Norton AntiVirus 4.08 for Windows NT 3.51
— Norton AntiVirus 5.02 for Windows NT 4.0
— Norton AntiVirus 4.04 for NetWare
— Norton AntiVirus 2.0 for Lotus Notes and OS/2
— Norton AntiVirus 1.52 for Microsoft Exchange

Soluções para Gateways:

— Norton AntiVirus 1.02A for Internet E-mail Gateways for NT
— Norton AntiVirus 1.04 for Firewalls

Administração:

— Norton System Center 3.1
— Norton AntiVirus 5.03 for Macintosh Administrator
— Norton AntiVirus Plus 5.0 for Tivoli Enterprise
— Norton AntiVirus Plus 5.0 for Tivoli IT Director
— Outras Ferramentas Administrativas, incluindo o Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01

Para obter mais informações sobre o produto Norton AntiVirus consulte o arquivo contents.txt no diretório raiz do CD do Norton AntiVirus.

Nota: Mesmo que a documentação do Norton AntiVirus forneça informações para contato com a Symantec para assistência e suporte, se sua cópia do Norton AntiVirus Solution Release 3.04 foi obtida como parte da oferta SecureWay FirstSecure, você deve entrar em contato com a IBM para obter assistência e suporte.

Para obter as etapas de instalação detalhadas consulte a documentação fornecida com os produtos específicos e consulte os requisitos de hardware e software na seção Capítulo 13, “Requisitos e considerações sobre a instalação do Intrusion Immunity” na página 67.

Capítulo 8. Planejamento do Public Key Infrastructure em sua rede

O componente Trust Authority do Public Key Infrastructure fornece aplicativos de Internet com recursos para autenticar usuários e assegurar comunicações confiáveis. Criado sob padrões PKI (public key infrastructure) para criptografia e capacidade de interoperação, um sistema Trust Authority fornece a infra-estrutura necessária para emitir, publicar e administrar certificados digitais. Ele inclui:

Suporte para plataformas de servidores IBM AIX e Microsoft Windows NT

Um RA (Autoridade de Registro) que suporta as tarefas administrativas por trás do registro de usuários. Esta administração, que pode ser implementada através de processos automatizados ou dependentes de tomadas de decisão humanas, inclui os seguintes tipos de tarefas:

— Confirmação da identidade de um usuário

— Aprovação ou rejeição de pedido para obter, renovar ou revogar certificados

— Validação de que o usuário possui a chave privada associada à chave pública em um certificado

— Cumprimento das regras em um determinado processo de negócios ou perfil de certificado para emitir determinados tipos de certificados para tipos específicos de usuários

O RA também publica informações sobre certificados em um Diretório de chave pública integrado, o IBM SecureWay LDAP Directory.

Um CA (Autoridade de Certificado) confiável. O CA:

— Emite certificados digitais e gera pares de chaves digitais que permitem que os certificados sejam autenticados

— Suporta o ciclo de vida completo do certificado, da inscrição inicial até a renovação e a revogação do certificado

— O RA atualiza o Diretório imediatamente quando um certificado é revogado

— Pode utilizar hardware de criptografia como o IBM SecureWay 4758 PCI Cryptographic Coprocessor e Smart Cards, para estender sua habilidade para proteger chaves

Central de Credenciamento, uma interface de inscrição com base na Web que torna facilita a obtenção de certificados de navegadores, certificados de servidores e certificados para determinados dispositivos, como Smart

Cards. Os administradores também podem utilizar estes formulários de inscrição para pré-registrar usuários finais para um certificado PKIX.

O Trust Authority Client, uma interface independente do Windows que permite que usuários obtenham, renovem e revoguem certificados PKIX sem utilizar um navegador da Web.

O RA Desktop, uma interface administrativa com base na Web que permite que administradores humanos aprovem ou rejeitem pedidos para obter, renovar ou revogar certificados.

Um subsistema Audit que utiliza MACs (message authentication codes) para assegurar que eventos recebidos do RA e do CA do Trust Authority podem ser autenticados. Uma opção configurável permite que registros de auditoria também tenham sua integridade protegida quando são registrados.

Várias interfaces administrativas para configuração do sistema, alteração de senhas seguras, CAs de certificação cruzada, registros de auditoria de verificação de integridade e início e encerramento seguro de componentes do sistema.

Uma API (application programming interface) que permite que desenvolvedores de aplicativos escrevam aplicativos PKI padrão.

Suporte integrado de tempo de execução para o IBM DB2 Universal Database. Existem bancos de dados separados para o IBM SecureWay Directory e para os componentes do RA, CA e Audit.

Implementação do Trust Authority

Para obter informações de planejamento e instalação detalhadas, consulte a seção *IBM SecureWay Trust Authority Up and Running*. Este manual contém cenários e etapas para a instalação em servidores Windows NT e no AIX.

Capítulo 9. Planejamento do SecureWay Toolbox em sua empresa

Planeje a instalação do FirstSecure Toolbox em um ambiente de desenvolvimento, não em sua rede. Teste seus aplicativos dentro de seu ambiente de desenvolvimento antes de torná-los disponíveis para usuários externos.

Serviços de autorização

Os Serviços de autorização permitem que você monitore quem está autorizado a acessar seu site da Web. A autenticação é baseada em senhas ou chaves públicas. Estas medidas protegem a integridade e confidencialidade dos dados em seu site. Os Serviços de autorização criam ACLs (listas de controle de acesso) que definem quem pode acessar objetos em seu site e como estes objetos podem ser acessados. Os Serviços de autorização também permitem que você defina objetos protegidos e crie senhas para início de sessão único. Todas estas ferramentas de segurança são centralizadas para facilitar o gerenciamento dos critérios de segurança. Os Serviços de autorização são suportados pelas APIs de autorização do IBM SecureWay Policy Director.

Serviços de autoridade de certificado

Serviços de autoridade de certificado são suportados pelo X.509 Public Key Infrastructure for Multiplatforms e pelo IBM KeyWorks Toolkit.

Os serviços de autoridade de certificado permitem que você assegure a segurança através do gerenciamento de certificados digitais. Estes serviços incluem APIs para o ciclo de vida completo destes certificados: emissão, renovação e revogação. Eles também publicam listas de revogações de certificados. As APIs utilizam criptografia de chave pública e tecnologia de smart card como um meio de autenticar os usuários de certificados.

O X.509 Public Key Infrastructure for Multiplatforms, também denominado PKIX, é fornecido através das APIs PKIX. Estas APIs permitem a criação, gerenciamento, armazenamento, distribuição e revogação de certificados através dos componentes EE (entidade final), CA (autoridade de certificado) e RA (autoridade de registro). As APIs são ativados para fazer interface com o IBM SecureWay Trust Authority, e são baseadas no IBMKeyWorks.

Para obter informações sobre o APIs do PKIX, consulte a seção *IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and*

Reference. Para obter mais informações sobre o IBM KeyWorks, consulte o Capítulo 16, “Documentação fornecida com o produto FirstSecure” na página 87 uma lista de documentações fornecidas com o Toolbox.

Serviços de diretório

Os serviços de diretório são suportados pelo IBM SecureWay Directory Client.

Os serviços de diretório utilizam Lightweight Directory Access Protocol (LDAP) para organizar, controlar e acessar diretórios. Estes serviços são baseados em um modelo cliente/servidor que fornece acesso de cliente para um servidor LDAP. Os serviços de diretório fornecem meios para manter as informações do diretório em uma localização central para armazenamento, atualizações, recuperação e troca. Os Serviços de Diretório utilizam SSL (Secure Sockets Layer) para criptografar informações.

Para obter informações sobre serviços de diretório, consulte o Capítulo 16, “Documentação fornecida com o produto FirstSecure” na página 87 para obter uma lista completa das documentações do IBM SecureWay Directory Client fornecida com o Toolbox.

Serviços de criptografia e gerenciamento confiável KeyWorks

Os serviços de criptografia e gerenciamento confiável são suportados pelo IBM KeyWorks Toolkit, que também é denominado KeyWorks.

Os serviços de criptografia e gerenciamento confiável KeyWorks criptografam e decriptografam informações para controlar quem tem permissão de acesso às informações. Estes serviços criam e verificam assinaturas digitais para autenticar as identidades de indivíduos e computadores em redes. Um sistema de recuperação de chave que permite a recuperação de informações criptografadas, sem distribuição da chave, é incorporado no IBM Key Recovery Service Provider.

O KeyWorks é um conjunto de ferramentas de criptografia e serviços confiáveis. Ele consiste em um conjunto de serviços de segurança em camadas e interfaces de programação associadas que fornecem um conjunto integrado de informações e recursos de segurança de comunicações. Cada camada é formada sobre os serviços mais fundamentais da camada imediatamente inferior. Estas camadas começam com componentes fundamentais, como algoritmo criptográfico, números aleatórios e informações de identificação únicas nas camadas inferiores aumentam para certificados digitais, gerenciamento de chave e mecanismos de recuperação.

O KeyWorks é ativado para NLS (National Language Support), o que significa que o produto não depende de nenhum idioma, script, cultura ou conjunto de caracteres codificados.

Para obter mais informações sobre as APIs KeyWorks, consulte o Capítulo 16, “Documentação fornecida com o produto FirstSecure” na página 87 para obter uma lista de documentações do KeyWorks fornecida com a Toolbox.

Serviços de protocolo Secure Sockets Layer

Os serviços de protocolo Secure Sockets Layer são suportados pelo Toolkit IBM SSL (Secure Sockets Layer).

Os serviços de protocolo SSL permitem que você decida quem possui acesso a seus dados. Estes serviços criptografam dados utilizando chaves privadas e públicas para vários objetivos, inclusive autenticação de usuários, prevenção de acesso por clientes não autorizados e prevenção de adulteração de dados. Você controla para quem são emitidos certificados, para que possa controlar a quem confia o acesso a seus dados. A tecnologia SSL é incorporada em várias outras APIs para criptografia de dados e criação de senhas.

Parte 3. Considerações sobre instalação e integração

Esta seção descreve como os componentes se ajustam uns aos outros. Ela lista os requisitos de hardware e software para cada produto e quaisquer aplicativos necessários ou produtos de banco de dados.

Capítulo 10. Planejamento para instalação do FirstSecure

Antes de instalar os produtos componentes do software FirstSecure, leia as próximas seções, para assegurar que o hardware e o software necessários estão disponíveis. Informações sobre as atualizações mais recentes do software FirstSecure estão disponíveis no endereço www.ibm.com/software/security/firstsecure . Verifique o site da Web para obter as últimas atualizações antes de começar a instalação dos produtos.

As instruções passo a passo detalhadas para instalação e configuração dos produtos componentes do FirstSecure são fornecidas na documentação de cada um dos produtos componentes.

Requisitos gerais do sistema

Esta seção descreve os requisitos gerais do sistema para os produtos FirstSecure. Para obter os requisitos específicos de hardware e software para cada um dos produtos componentes, consulte o produto componente específico.

Para instalar os componentes do FirstSecure, você precisa de hardware que possa executar a versão Server de um destes sistemas operacionais:

Microsoft Windows NT Versão 4 com service pack 5.

AIX Versão 4.3.1 ou superior.

Sun Solaris Versão 2.6 ou superior.

Nota: No sistema Solaris, o Toolbox requer Sun Solaris Versão 2.6 com o Pacote de Correção de Maio de 1999.

Cada um dos produtos componentes do FirstSecure pode ser executado em pelo menos um dos sistemas operacionais listados acima. Cada seção de um produto componente mostra as plataformas de sistemas operacionais suportadas e outro software de pré-requisito para cada produto componente. Dentre estes sistemas operacionais, você precisará de servidores, consoles de gerenciamento e sistemas clientes. As seções a seguir fornecem uma visão geral destes requisitos.

Requisitos de sistema operacional para servidores e clientes

Consulte a seção Tabela 1 na página 56 para obter os requisitos de sistema operacional para os produtos SecureWay.

Tabela 1. Requisitos de sistema operacional para servidores e clientes

Sistema Operacional	Nível Mínimo do Servidor	Nível Mínimo do Cliente
Windows NT	Versão 4.0, Service Pack 5	Versão 4.0, Service Pack 5
IBM AIX	Versão 4.3.1	Versão 4.3.1
Sun Solaris	Versão 2.6	Versão 2.6
Windows 95	N/A	Todas as versões suportadas
Windows 98	N/A	Todas as versões suportadas
Windows 3.1 (apenas Norton AntiVirus)	N/A	Todas as versões suportadas
IBM OS/2 (apenas Norton AntiVirus)	N/A	Versão 4.0, Pacote de Correção 6 ou superior

Detalhes e requisitos do produto componente

As próximas seções mostram os requisitos de hardware e software dos produtos componentes do FirstSecure. Os capítulos a seguir descrevem os blocos de construção em detalhes e informam requisitos de hardware e software para cada um. Os capítulos também fornecem uma visão geral da instalação e configuração de cada produto, inclusive uma discussão sobre integração com outros componentes.

Capítulo 11, “Requisitos e considerações sobre a instalação do Policy Director” na página 57

Capítulo 12, “Requisitos e considerações sobre a instalação do componente SecureWay Boundary Server” na página 59

Capítulo 13, “Requisitos e considerações sobre a instalação do Intrusion Immunity” na página 67

Capítulo 14, “Requisitos e considerações sobre a instalação do produto Public Key Infrastructure” na página 75

Capítulo 15, “Requisitos e considerações sobre a instalação do produto Toolbox” na página 81

Capítulo 11. Requisitos e considerações sobre a instalação do Policy Director

Este capítulo lista os requisitos de hardware e software do componente Policy Director. Ele também fornece considerações de instalação sobre integração com outros produtos FirstSecure.

Requisitos de hardware e software do Policy Director

A Tabela 2 lista os requisitos de hardware do Policy Director.

Tabela 2. Requisitos de hardware do produto Policy Director

Plataforma	Espaço em Disco Mínimo	Memória Mínima
Servidor Windows NT: Intel ou compatível com Intel 80486 de 133 MHZ ou superior	16 MB	64 MB
Servidor AIX: hardware que execute AIX 4.3.1	16 MB	64 MB
Servidor Solaris: hardware que execute Solaris 2.6	16 MB	64 MB

Os requisitos de software do Policy Director são:

Servidores Policy Director

Servidor Windows NT Versão 4.0, Service Pack 5
AIX Versão 4.3.1
Sun Solaris, Versão 2.6

Clientes NetSEAT

Servidor Windows NTVersão 4.0, Service Pack 5
Windows 95
Windows 98

Console de Gerenciamento

Estação de trabalho Windows NT
Windows NT Server Client
AIX Versão 4.3.1 Client
Sun Solaris, Versão 2.6 Client

O Policy Director requer outros componentes de software que são incluídos no pacote. Siga as instruções na seção *IBM SecureWay Policy Director Up and Running* para instalar o software necessário para a implementação do seu Policy Director.

Considerações sobre a instalação do Policy Director

O endereço www.ibm.com/software/security/policy lista todas as atualizações aos pré-requisitos de software atuais do produtoPolicy Director.

Integração dos produtos Policy Director e Trust Authority

O IBM SecureWay Trust Authority fornece autenticação, assegurando que cada usuário é quem afirma ser. O Trust Authority emite certificados para usuários baseado em informações contidas no IBM SecureWay Directory, algumas vezes denominado Lightweight Directory Access Protocol ou LDAP.

O Policy Director, por sua vez, utiliza estes certificados e fornece autorização, assegurando que cada usuário tenha acesso apenas aos recursos permitidos. O Policy Director armazena suas informações no mesmo IBM SecureWay Directory.

Seu e-business pode possuir uma identificação de usuário única com todas as permissões do Policy Director, e todas as informações do Trust Authority. Você também armazena informações sobre SecureWay Boundary Server no IBM SecureWay Directory, o Policy Director pode gerenciá-las para você também.

Capítulo 12. Requisitos e considerações sobre a instalação do componente SecureWay Boundary Server

Este capítulo lista os requisitos de hardware e software para o componente SecureWay Boundary Server. Ele também fornece considerações de instalação sobre integração com outros produtos SecureWay Boundary Server.

Requisitos de hardware e software do produto SecureWay Boundary Server

Os requisitos de hardware dos produtos componentes SecureWay Boundary Server estão localizados na Tabela 3 e na Tabela 4 na página 60.

Tabela 3 (Página 1 de 2). Requisitos de hardware dos produtos componentes do SecureWay Boundary Server

Componente SecureWay Boundary Server	**Tipo de Máquina**	**Espaço em Disco**	**Memória**	**Outros**
IBM SecureWay Firewall[1]	NT: Pentium 133 MHz ou superior AIX: máquina RS/6000 que suporte AIX 4.3.2	NT: 24 MB[2] AIX: 307 MB	NT: 64 MB AIX: 64 MB	2 placas de interface de rede
ACE/Server	NT: Pentium de 166 MHz ou superior (apenas processador único) AIX: Máquina que suporte AIX 4.2	Software do servidor principal: 50 MB Servidor de backup: 22 MB Banco de dados de usuários inicial: 4 MB Instalação: 240 MB	Mínimo: 32 MB	Os requisitos de armazenamento real são baseados no número de usuários

Tabela 3 (Página 2 de 2). Requisitos de hardware dos produtos componentes do SecureWay Boundary Server

Componente SecureWay Boundary Server	**Tipo de Máquina**	**Espaço em Disco**	**Memória**	**Outros**
SurfinGate				
Server	Pentium de 233 MHz ou superior	20 MB	Mínimo: 128 MB Recomendado: 256 MB	
Console	Pentium 233 MHz ou superior	15 MB	Mínimo: 32 MB Recomendado: 64 MB	
MIMEsweeper para IBM SecureWay Release 2				
MAILsweeper	Pentium de 200 MHz ou superior	1 GB	64 MB	1 placa de interface de rede
WEBsweeper	Pentium de 400 MHz ou superior	1 GB	128 MB + 1 MB para cada conexão da Web concorrente	1 placa de interface de rede

Notas:

1. Veja mais detalhes na documentação incluída com o produto IBM Firewall.
2. 13 MB de espaço em disco também são necessários para o navegador Netscape.

Tabela 4 (Página 1 de 2). Requisitos de software dos produtos componentes do SecureWay Boundary Server

Componente SecureWay Boundary Server	**Plataformas Microsoft Windows**		**AIX**	**Solaris**
	Cliente	**Servidor**	**Servidor**	**Servidor**
IBM SecureWay Firewall	Windows 95, cliente IPSec	Servidor Windows NT Versão 4.0, Service Pack 5[1]	AIX 4.3.2	Não Disponível
ACE/Server	Windows NT Workstation 4.0, Service Pack 2 ou superior	Windows NT Server Versão 4.0, Service Pack 5 ou superior	AIX 4.2	Solaris 2.5.1
SurfinGate 4.05				

Tabela 4 (Página 2 de 2). Requisitos de software dos produtos componentes do SecureWay Boundary Server

Componente SecureWay Boundary Server	**Plataformas Microsoft Windows**		**AIX**	**Solaris**
	Cliente	**Servidor**	**Servidor**	**Servidor**
Server	Não Disponível	Windows NT 4.0[2]	Não Disponível	Não Disponível
Console	Windows NT 4.0 ou superior [2] Windows 95, Windows 98	Não Disponível	Não Disponível	Não Disponível
MIMEsweeper para IBM SecureWay Release 2				
MAILsweeper	Não Disponível	Windows NT 4.0[3]	Não Disponível	Não Disponível
WEBsweeper	Windows NT Workstation 4.0, Service Pack 3 ou superior	Windows NT 4.0[4]	Não Disponível	Não Disponível

Notas:

1. Verifique a documentação fornecida com o produto IBM Firewall para Windows NT para obter as correções necessárias.
2. Além disso:
   O cliente de rede do Windows para Microsoft Windows é requerido.
   Windows NT Workstation não é suportado.
3. Além disso:
   NT 3.5.1 e Windows NT Workstation não são suportados.
   Um destes ambientes é requerido:
   — Microsoft Exchange
   — SMTP
   — cc:Mail
   — Groupwise
   — Lotus Notes
4. Consulte as recomendações para o produto MIMEsweeper na seção “Considerações sobre o MIMEsweeper” na página 65.

Considerações do componente SecureWay Boundary Server

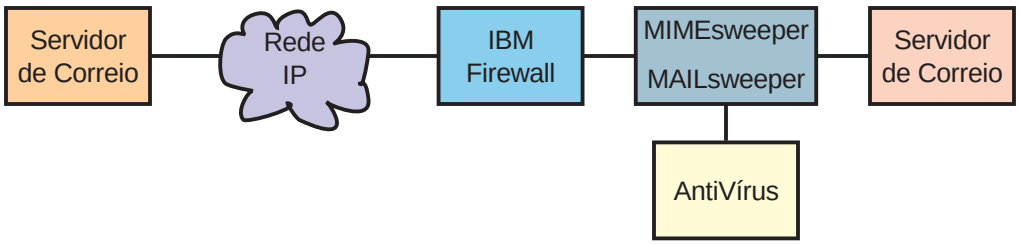
As próximas seções descrevem as considerações sobre instalação e configuração dos componentes do produto SecureWay Boundary Server.

Considerações sobre o IBM Firewall

As considerações sobre o IBM Firewall envolvem principalmente onde ele é instalado no fluxo de tráfego em relação a outros produtos SecureWay Boundary Server.

Configurações de amostra

Configurações de amostra do IBM Firewall e MAILsweeper: Ao instalar os produtos IBM Firewall e MIMEsweeper, você pode utilizar a configuração descrita nesta seção.



O MAILsweeper é parte do MIMEsweeper que verifica o conteúdo de mensagens de correio. O MAILsweeper possui uma função para ativar verificações de antivírus.

O MAILsweeper está posicionado entre o IBM Firewall e os servidores SMTP protegidos.

O IBM Firewall aponta para o MAILsweeper como o host de correio para distribuição de correio.

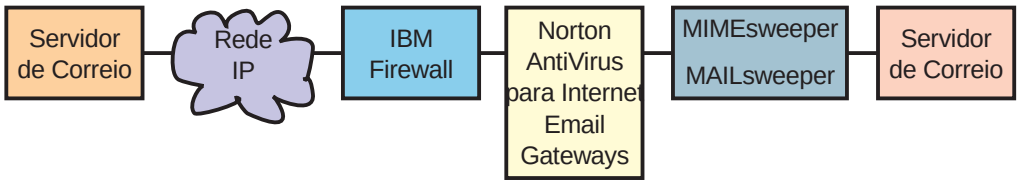
— O produto IBM Firewall requer que regras de correio predefinidas sejam configuradas para permitir o fluxo de tráfego do correio.

Os servidores SMTP também devem apontar para o MAILsweeper como o host para distribuição de correio.

O MAILsweeper verifica o conteúdo das mensagens de correio enviadas que fluem nas duas direções.

Configuração de amostra dos produtos IBM Firewall, Norton AntiVirus for Internet Email Gateways e MIMEsweeper: Se estiver instalando os produtos IBM Firewall, Norton AntiVirus for Internet Email Gateways e MIMEsweeper, você pode utilizar a configuração descrita nesta seção. Este cenário combina os produtos IBM Firewall, Norton AntiVirus for Internet Email Gateways e

MAILsweeper em uma cadeia para verificar vírus e conteúdo de dados de correio, conforme ilustrado no diagrama apresentado a seguir.

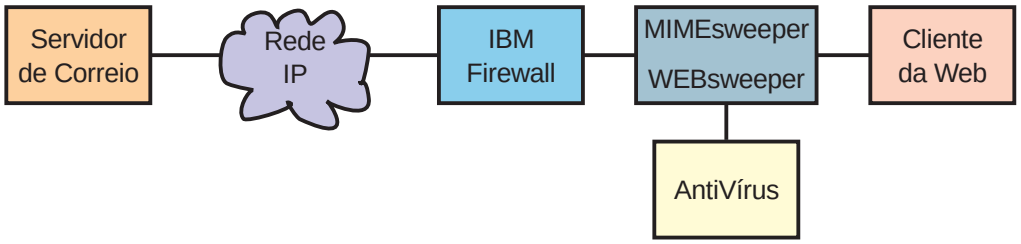


O firewall aponta para o Norton AntiVirus for Internet Email Gateways como seu servidor de correio protegido. Regras de firewall corretas devem ser definidas para permitir este tráfego específico.

O Norton AntiVirus for Internet Email Gateways indica o MAILsweeper como seu distribuidor de correio protegido e indica o firewall para distribuição de correio de destino.

O MAILsweeper recebe e verifica o correio enviado para ele. Em seguida, ele distribui o correio para o servidor correto, dependendo de suas tabelas de roteamento ou de consultas de registro MX. Se o MAILsweeper e o Norton AntiVirus for Internet Email Gateways estiverem na mesma máquina, você deve alterar a porta de recepção para o MAILsweeper para evitar conflito com o Norton AntiVirus for Internet Email Gateways.

Configurações de amostra do IBM Firewall e WEBsweeper: Se estiver instalando os produtos IBM Firewall e MIMEsweeper, você pode utilizar a configuração descrita nesta seção.



O WEBsweeper é parte do MIMEsweeper, que verifica o tráfego da Web. O WEBsweeper possui uma função para ativar as verificações de antivírus.

O WEBsweeper funciona como um proxy intermediário. Os clientes apontam para o WEBsweeper como seu proxy. Em seguida, o WEBsweeper é definido para distribuir tráfego para o proxy do firewall.

Regras devem ser configuradas no firewall para permitir o tráfego de proxy.

Os pedidos de proxy podem ser provenientes apenas da rede protegida atrás do firewall.

O WEBsweeper não lida com HTTPS. Para utilizar HTTPS, você deve desviar do WEBsweeper, para evitar problemas com o firewall e com a garantia de verificação de todo o tráfego da Web. Você deve apontar diretamente para o proxy do firewall. O tráfego da Web ainda está protegido, mas não é verificado pelo WEBsweeper.

Configurações de amostra do IBM Firewall e SurfinGate: Se estiver instalando os produtos IBM Firewall e SurfinGate, você pode utilizar a configuração descrita nesta seção.

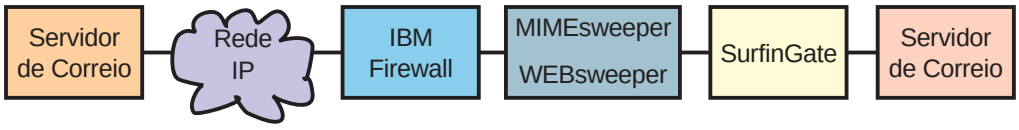
O SurfinGate verifica a presença de controles ActiveX e outros itens no tráfego da Web.

O SurfinGate atua como um proxy Web intermediário. Os clientes apontam para o SurfinGate como seu proxy para HTTP, FTP e HTTPS. Em seguida, o SurfinGate envia o pedido para o proxy do produto IBM Firewall.

Regras devem ser configuradas no firewall para permitir o tráfego de proxy.

Os pedidos de proxy podem ser provenientes apenas da rede protegida atrás do firewall.

Configuração de amostra dos produtos IBM Firewall, MIMEsweeper e SurfinGate: Se estiver instalando os produtos IBM Firewall, MIMEsweeper e SurfinGate, você pode utilizar a configuração descrita nesta seção.



O SurfinGate verifica a presença de controles ActiveX e outros itens no tráfego da Web. Este produto utiliza verificações diferentes do componente WEBsweeper do MIMEsweeper.

Os produtos SurfinGate e WEBsweeper atuam como proxies intermediários da Web. Os clientes apontam para o SurfinGate como seu proxy para HTTP e FTP. Em seguida, o SurfinGate envia o pedido para o WEBsweeper. Em seguida, o WEBsweeper envia o pedido para o proxy do IBM Firewall.

Regras devem ser configuradas no firewall para permitir o tráfego de proxy. Estas regras estão definidas na publicação *IBM eNetwork Firewall Version 3.3 for Windows NT User's Guide.*

Os pedidos de proxy podem ser provenientes apenas da rede protegida atrás do firewall.

O WEBsweeper não lida com HTTPS. Ao utilizar HTTPS, para evitar problemas com o firewall e para assegurar que todo o tráfego da Web seja verificado, você precisa desviar do WEBsweeper. Você deve apontar diretamente para o proxy do firewall. O tráfego da Web ainda está protegido, mas não é verificado pelo WEBsweeper.

Considerações sobre o MIMEsweeper

O sistema a seguir é um sistema WEBsweeper típico:

Um Pentium de 400 MHz ou superior

1 GB de espaço em disco e 128 MB RAM

Windows NT Server ou Workstation Versão 4.0 Server Service Pack 3 ou superior

Protocolo TCP/IP, incluindo um nome de host e de domínio

Ferramentas antivírus

A seguir descrevemos um ambiente WEBsweeper típico de volume alto de até 500 usuários concorrentes:

Um Intel Pentium II dual, de 450 MHz ou superior

3 GB de espaço em disco e 256 MB RAM

Windows NT Server ou Workstation Versão 4.0 Server Service Pack 3 ou superior

Protocolo TCP/IP, incluindo um nome de host e de domínio

Ferramentas antivírus

Se seu ambiente suporta mais de 500 usuários concorrentes, é recomendada a utilização dos servidores múltiplos WEBsweeper

Capítulo 13. Requisitos e considerações sobre a instalação do Intrusion Immunity

Este capítulo lista os requisitos de hardware e software dos componentes Intrusion Immunity, Tivoli Cross-Site for Security e Norton AntiVirus.

Requisitos de hardware e software do Intrusion Immunity

A seção apresentada a seguir descreve a documentação de instalação e configuração dos produtos do componente Intrusion Immunity.

Os requisitos de hardware e software do produto Tivoli Cross-Site for Security são mostrados nas Tabela 5, Tabela 6 na página 68 e Tabela 7 na página 68. Os requisitos de hardware e software dos produtos componentes do Norton AntiVirus são mostrados na Tabela 8 na página 69 e na Tabela 9 na página 69.

Tabela 5. Requisitos de hardware e software dos servidores Tivoli Cross-Site for Security

Requisitos de servidor	
Sistema Operacional	AIX 4.3.2 Windows NT Versão 4.0, Service Pack 5 Solaris 2.5.1 ou 2.6
Java	JDK 1.1.6 revisão 04 ou superior
Servidor da Web	Netscape Enterprise Server 3.51
Banco de Dados	IBM DB2 Release 5.2 Oracle 7.3.4 (ou 8.0.4 recomendado) Microsoft SQL Server
Espaço em disco	Windows NT 290 MB AIX 180 MB Solaris 180 MB
Memória	256 MB
Espaço de Troca	300 MB (400 MB recomendado)

Notas:

1. Netscape Enterprise Server 3.51 e 3.6 não são suportados.
2. Veja os requisitos de Correção para Solaris na documentação de instalação do produto Tivoli Cross-Site for Security.

Tabela 6. Requisitos de hardware e software do console de gerenciamento do Tivoli Cross-Site for Security

Requisitos do console de gerenciamento	
Sistemas operacionais	Windows 95 Windows 98 Windows NT Versão 4.0, Service Pack 5 (máquina 166 MHz ou superior recomendada) Solaris 2.5.1 ou 2.6 executando em Sun SPARC
Espaço em disco	25 MB para todas as plataformas
Memória	Windows NT 40 MB AIX 64 MB Solaris 40 MB

Tabela 7. Requisitos de hardware e software dos agentes do Tivoli Cross-Site for Security

Requisitos de agente	
Sistemas operacionais	Windows NT Versão 4.0, Service Pack 5 ou superior AIX 4.3.2 Solaris 2.5.1 ou 2.6 executando em Sun SPARC
Java	JDK 1.1.6 revisão 04 ou superior em Solaris (necessário apenas para UNIX)
Espaço em disco	15 MB no Windows NT 10 MB no AIX 10 MB no Solaris
Memória	32 MB no Windows NT 32 MB no AIX 20 MB no Solaris

Notas:

1. Netscape Enterprise Server 3.51 e 3.6 não são suportados.
2. Veja os requisitos de Correção para Solaris na documentação de instalação do produto Tivoli Cross-Site for Security.

A Tabela 8 na página 69 lista os requisitos de hardware do produto Norton AntiVirus.

Tabela 8. Requisitos de hardware do produto Norton AntiVirus.

Componente Intrusion Immunity	Tipo de Máquina	Espaço em Disco	Memória	Outros
Norton AntiVirus	CPU Intel	24 MB	Mínimo: 16 MB Recomendado: 32 MB	Unidade de CD-ROM
Norton AntiVirus para Gateways de E-mail da Internet	Pentium 133 ou superior	6 MB	32 MB	Unidade de CD-ROM 500 MB - 5 GB para operação eficiente de correio

Tabela 9. Requisitos de software do produto Norton AntiVirus

Componente Intrusion Immunity	Plataformas Microsoft Windows		OS/2
	Cliente	Servidor	Cliente
Norton AntiVirus[1]	Windows NT 4.0 Windows 95, Windows 98	Windows NT 4.0	OS/2 2.11 ou superior

Notas:

1. Além disso, uma conexão de Internet TCP/IP é necessária para o produto Norton AntiVirus for Internet Email Gateways.

O produto Norton AntiVirus não está disponível para AIX e Solaris.

Considerações sobre a instalação do produto Tivoli Cross-Site for Security

As ilustrações a seguir mostram posicionamentos típicos de agentes Cross-Site for Security e servidor de gerenciamento Cross-Site for Security em uma rede de e-business.

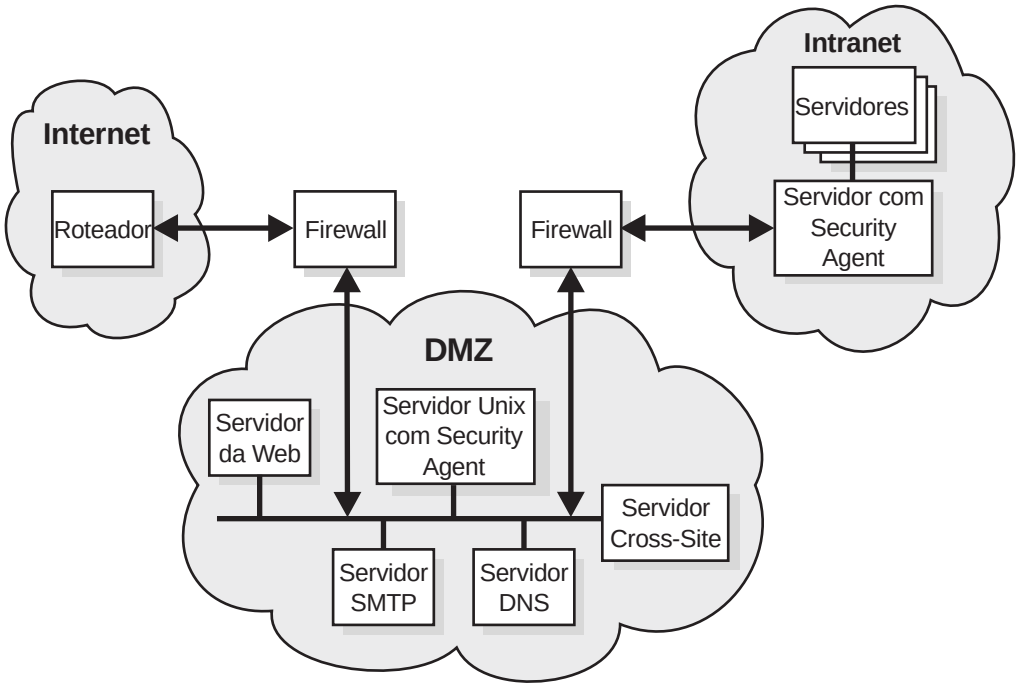


Figura 11. Instalação do servidor de gerenciamento Cross-Site for Security na DMZ

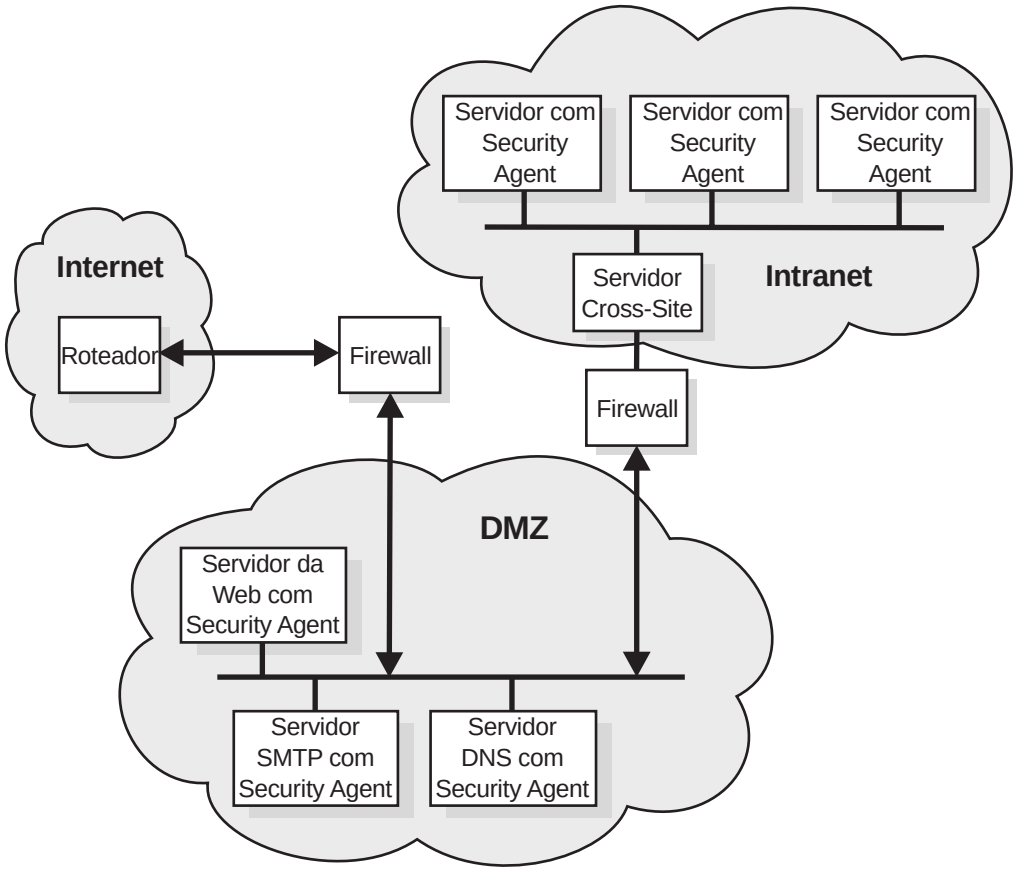


Figura 12. Instalação do servidor de gerenciamento Cross-Site for Security em sua intranet

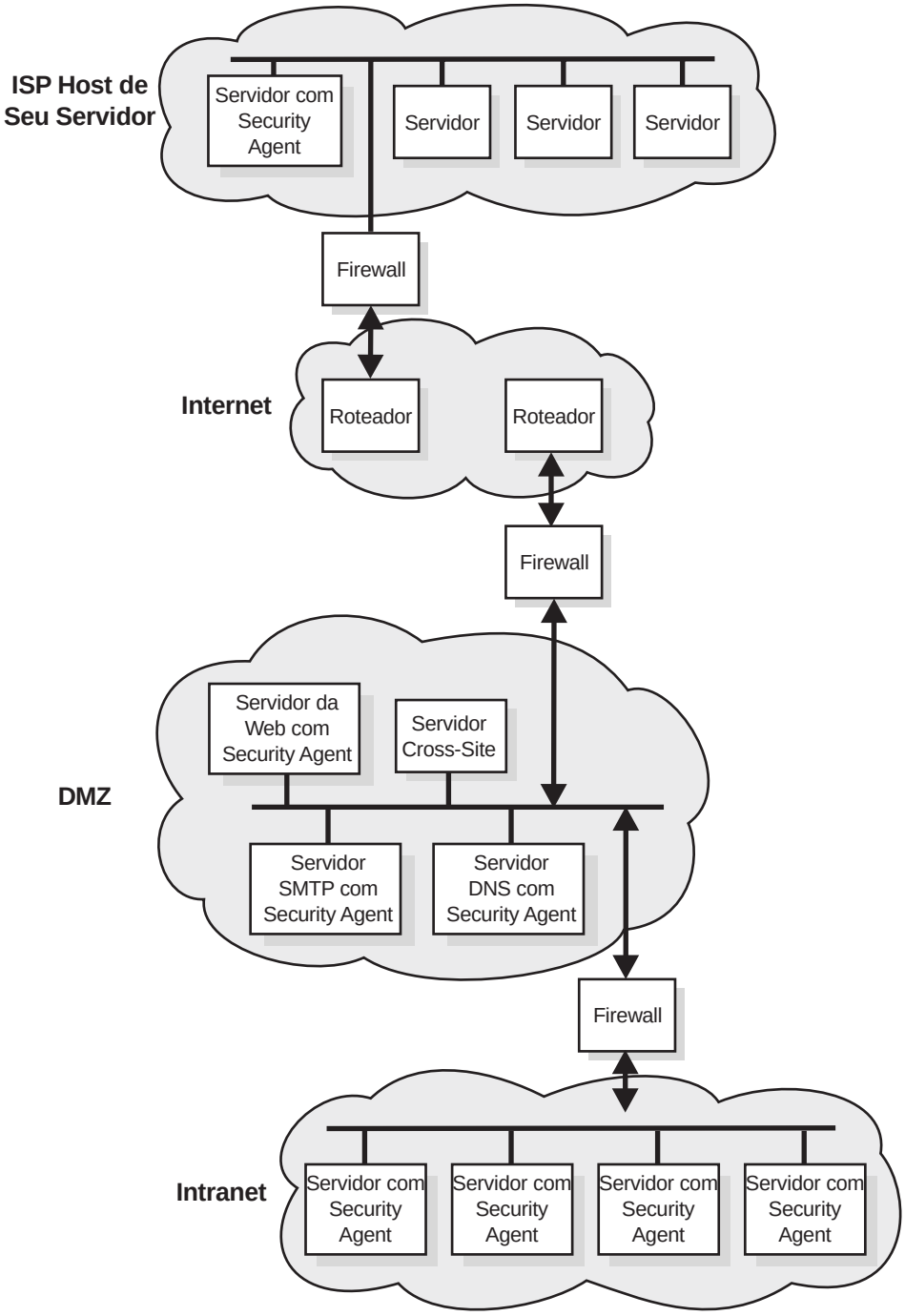


Figura 13. Instalação do servidor de gerenciamento Cross-Site for Security na DMZ suportando um servidor conectado à Internet

Considerações sobre a instalação do produto Norton AntiVirus

Informações sobre a instalação do Norton AntiVirus se encontram no arquivo contents.txt, localizado no diretório raiz do CD do produto.

Capítulo 14. Requisitos e considerações sobre a instalação do produto Public Key Infrastructure

As empresas hoje em dia precisam de infra-estrutura de chave pública para aplicativos seguros de e-business e o produtos FirstSecure Trust Authority fornece dois níveis de funções que implementam uma infra-estrutura de chave pública:

Gerenciamento do ciclo de vida completo de certificados digitais, fornecendo:

— A capacidade de solicitar, renovar e revogar certificados

— Um RA (autoridade de registro) para aprovar pedidos de certificados

— Um CA (autoridade de certificado) para criar certificados digitais e listas de revogações

As capacidades de registro avançadas para permitir que as empresas registrem suas entidades e-business confiáveis online. O aplicativo de registro foi criado com base nos seguintes princípios:

— Os certificados que estão sendo emitidos e gerenciados devem dignos da segurança requerida por aplicativos sensitivos de e-business, e o RA (autoridade de registro) deve ser criado de modo a atender os mesmos altos requisitos de confiança e segurança.

— O aplicativo deve fornecer a flexibilidade para suportar uma variedade de critérios de registro, incluindo aprovações manuais ou automatizadas, autenticações flexíveis internas ou externas ao site, e a opção de isolar critérios de registro em domínios confiáveis separados.

O modelo confiável ajuda a garantir a capacidade de acesso, confidencialidade, integridade e a autoria de suas transações comerciais. Através de criptografia digital, certificação e assinatura, o Trust Authority permite que você conduza e-business seguro através da Internet, de uma intranet ou de uma rede privada virtual. Para obter segurança estendida de sua chave de assinatura, o CA (autoridade de certificado) é projetado para trabalhar com hardware de criptografia.

Requisitos de hardware e software do produto Trust Authority server

Os requisitos de software de servidor do componente Trust Authority estão listados na Tabela 10 na página 76.

Tabela 10. Requisitos de software de servidor e hardware opcional do componente Public Key Infrastructure Trust Authority

Produto	**Notas**
Um dos seguintes sistemas operacionais: IBM AIX/6000 (AIX), versão 4.3.2 Microsoft Windows NT, versão 4.0 com Service Pack 5	Requerido. Você deve instalar todos os programas do servidor Trust Authority na mesma plataforma. Você não pode misturar máquinas AIX e Windows NT na mesma configuração de sistema.
IBM SecureWay Directory Versão 3.1.1	Requerido; integrado com o código do Trust Authority. Durante a instalação do Trust Authority, você pode instalar o software Directory na mesma máquina em que o Trust Authority foi instalado ou pode instalá-lo em uma máquina remota.
IBM WebSphere Application Server Version 2.02, Standard Edition. Inclui IBM HTTP Server Versão 1.3.3 e o Sun Java Development Kit (JDK) 1.1.7.	Requerido; fornecido no pacote de mídia do Trust Authority. Antes de instalar o Trust Authority, você deve instalar o software de servidor da Web na mesma máquina em que planeja instalar o Trust Authority e o software de servidor do Trust Authority.
IBM DB2 Universal Database Enterprise Edition Version 5.2 com pacote de manutenção 9.	!Necessário; fornecido no pacote de mídia Trust Authority. Uma única ocorrência de banco de dados existe para cada componente de servidor. Antes de instalar o Trust Authority, você deve instalar o DB2 em cada máquina que você planeja utilizar como um servidor Trust Authority.
IBM SecureWay 4758 PCI Cryptographic Coprocessor, Model 001 IBM SecureWay 4758 CCA Support Program, versão 1.3.0.0 com pacote de manutenção 1.3.0.1	*Opcional* e disponível apenas para sistemas AIX; você deve solicitar este produto através de canais de pedido IBM normais. Antes de instalar o Trust Authority, você deve instalar o hardware 4758 e o programa de suporte no servidor em que planeja instalar o CA Trust Authority. A placa criptográfica 4758 requer um barramento PCI no RS/6000.

A Tabela 11 na página 77 e a Tabela 12 na página 78 listam os requisitos de hardware do Trust Authority.

Na Tabela 11 na página 77 e na Tabela 12 na página 78:

Um ambiente de produção pequeno emite centenas de certificados por dia.

Um ambiente de produção médio emite milhares de certificados por dia.

Um ambiente de produção grande emite muitos milhares de certificados por dia. Ele também pode ser um sistema que fornece serviços de CA de terceiros para outras organizações.

Se você planeja executar o Trust Authority sob o sistema Windows NT, a IBM recomenda que você instale-o em um IBM Netfinity Server. A tabela a seguir fornece recomendações de tamanho de sistema baseados no número de certificados que você espera emitir através de um CA do Trust Authority.

Tabela 11. Exemplo de configuração de máquina Windows NT

Tipo de Máquina	**Processadores**	**Espaço em Disco**	**Memória**
Ambiente de Produção Pequeno			
Netfinity 3000	1 (450 MHz, Pentium II)	2 unidades (9.1 GB)	256 MB
Netfinity 5000	2 (450 MHz, Pentium II)	2 unidades (9.1 GB)	512 MB
Ambiente de Produção Médio			
Netfinity 3000	1 (500 MHz, Pentium III)	4 unidades (18.2 GB)	768 MB
Netfinity 5000	2 (500 MHz, Pentium III)	4 unidades (9.1 GB)	1 GB
Ambiente de Produção Grande			
Netfinity 5500	2 (450 MHz, Pentium III)	4 unidades (9.1 GB alta velocidade)	1 GB
Netfinity 5500	4 (500 MHz, Pentium III Xeon com 1024K de Cache L2)	4 unidades (9.1 GB alta velocidade)	1 GB
Netfinity 7000	2 (500 MHz, Pentium III com 512K de Cache L2)	4 unidades (9.1 GB alta velocidade)	1 GB
Netfinity 7000	4 (500 MHz, Pentium III Xeon com 1024K de Cache L2)	4 unidades (18.2 GB)	2 GB

Se você planeja executar o Trust Authority sob AIX, você deve instalá-lo em uma máquina IBM RISC System/6000 . A tabela a seguir fornece

recomendações de tamanho de sistema baseado no número de certificados que você espera emitir através de um CA do Trust Authority.

Tabela 12. Exemplo de configuração de hardware de máquina AIX

Tipo de Máquina	Processadores	Espaço em Disco	Memória
Ambiente de Produção Pequeno			
F40	2 (233 MHz)	2 unidades (9.1 GB, Ultra 2 Fast Wide)	512 MB
Ambiente de Produção Médio			
F40	2 (233 MHz)	3 unidades (9.1 GB, Ultra 2 Fast Wide)	1 GB
Ambiente de Produção Grande			
F50	4 (332 MHz)	5 unidades (uma 9.1 GB Ultra 2 Fast Wide mais quatro 9.1 GB SSA)	2 GB
H50	4 (332 MHz)	5 unidades (uma 9.1 GB Ultra 2 Fast Wide mais quatro 9.1 GB SSA)	2 GB
R50	6 (200 MHz)	2 unidades (9.1 GB Ultra 2 Fast Wide)	1 GB
R50	8 (200 MHz)	5 unidades (uma 9.1 GB Ultra 2 Fast Wide mais uma 7133 SSA Rack com quatro 9.1 GB SSA)	2 GB

Requisitos de hardware e software do cliente Trust Authority

A IBM recomenda a seguinte configuração de estação de trabalho para utilização com os formulários de inscrição de navegador e para execução do aplicativo Trust Authority Client.

A configuração de máquina física a seguir:

— Processador de 166 MHz Intel 486 com memória de 32 MB, no mínimo (Processador de 200 MHz Intel Pentium com pelo menos 64 MB de memória é preferível)

— Placas de gráfico

— Placa de vídeo VGA, ou melhor

— Mouse ou dispositivo de indicação compatível com mouse

Um dos seguintes sistemas operacionais:

— Microsoft Windows 95

— Microsoft Windows 98

— Microsoft Windows NT, versão 4.0

Um dos seguintes navegadores da Web:

— Netscape Navigator ou Netscape Communicator, versão 3.0 ou posterior

— Microsoft Internet Explorer, versão 4.0 ou posterior, com Java ativado.

Interação do IBM KeyWorks Toolkit com o IBM SecureWay Trust Authority

Não instale o produto IBM KeyWorks Toolkit no mesmo servidor do IBM SecureWay Trust Authority.

Capítulo 15. Requisitos e considerações sobre a instalação do produto Toolbox

O FirstSecure Toolbox é um conjunto de APIs para ajudá-lo a desenvolver aplicativos seguros em seu e-business.

Serviços de autorização

Serviços de certificado e gerenciamento

Serviços de diretório

Serviços de protocolo Secure Sockets Layer

Serviços de gerenciamento confiável e criptografia KeyWorks

— APIs IBM Key Recovery Service Provider 1.1.3.0 . O produto IBM Key Recovery Service Provider permite a recuperação de informações criptografadas.

— IBM Key Recovery Server 1.1.3.0. O produto IBM Key Recovery Server 1.1.3.0 é um aplicativo que, sob pedido de autorização, pode recuperar informações criptografadas quando as chaves não estiverem disponíveis, estiverem perdidas ou danificadas.

Estes conjuntos de ferramentas fornecem interfaces padrão que os aplicativos podem utilizar para invocar serviços de segurança indispensáveis bem como interfaces padrão que provedores de segurança podem utilizar para conectar-se ao conjunto de ferramentas. As interfaces padrão são baseadas em CDSA (Common Data Security Architecture). Estes conjuntos de ferramentas estão disponíveis nos sistemas operacionais Windows NT, Solaris e AIX.

Requisitos de hardware e software do produto Toolbox

Os requisitos de hardware do produto Toolbox são mostrados na Tabela 13.

Tabela 13. Requisitos de hardware do produto Toolbox

Plataforma	Espaço em disco	Memória
Versão 4.0, Service Pack 5	2 a 4 GB	64 MB
AIX 4.3.2	9.1 GB	1 GB
Sun Solaris, Versão 2.6 com Pacote de Correção de Maio de 1999	4.2 GB	128 MB

Tabela 14. Requisitos de hardware dos produtos componentes do Toolbox

Conjunto de Ferramentas	**Tipo de Máquina**	**Espaço em Disco**	**Memória**
IBM KeyWorks Toolkit	Hardware que suporte produtos em execução nestes sistemas: Windows NT Versão 4.0, Service Pack 5 ou superior Windows 95 AIX 4.2 ou superior Sun Solaris	50 MB	32 MB
IBM Key Recovery Service Provider	Hardware que suporte produtos em execução nestes sistemas: Windows NT Versão 4.0, Service Pack 5 ou superior Windows 95 AIX 4.2 ou superior Sun Solaris	50 MB	32 MB

Os requisitos de software dos produtos do componente Toolbox são mostrados na tabela a seguir.

Tabela 15. Requisitos de software dos produtos componentes do Toolbox

Componentes do produto Toolbox	**Plataformas Microsoft Windows**		**AIX**	**Solaris**
	Cliente	**Servidor**	**Servidor**	**Servidor**
IBM KeyWorks Toolkit	Windows NT Versão 4.0, Service Pack 5 ou superior Windows 95	Windows NT Versão 4.0, Service Pack 5 ou superior Windows 95	AIX 4.2 ou superior [1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT Versão 4.0, Service Pack 5 ou superior[2] Windows 95	Windows NT Versão 4.0, Service Pack 5 ou superior	AIX 4.2 ou superior	Sun Solaris

Notas:

1. O cliente AIX também é suportado.
2. Além disso, o produto IBM KeyWorks Toolkit é necessário.

IBM KeyWorks Toolkit 1.1

O produto IBM KeyWorks Toolkit 1.1 fornece aos desenvolvedores de aplicativos um meio aberto, expansível e padrão para acessar funções criptográficas e outras funções de segurança em diferentes ambientes operacionais.

O IBM KeyWorks Toolkit fornece interfaces padrão (APIs) que os aplicativos podem utilizar para invocar serviços críticos de criptografia, confiabilidade e segurança, bem como interfaces padrão que os módulos adicionais de Provedores de Serviços podem utilizar para estabelecer interface com o kit de ferramentas. Estas interfaces padrão são baseadas em CDSA (Common Data Security Architecture), um padrão da organização The Open Group que foi desenvolvido inicialmente pela Intel Corporation e expandido pela IBM no componente KeyWorks Toolkit. Quando você utiliza interfaces padrão:

Sua empresa pode escolher a implementação de criptografia e confiabilidade que seja mais adequada para suas necessidades, sem alterar os aplicativos que utilizam os serviços de segurança.

A produtividade de seu aplicativo e dos programadores middleware é melhorada.

O produto IBM KeyWorks Toolkit fornece uma camada de isolamento entre aplicativos e middleware como uma classe e as funções criptográficas e Provedores de Serviços. O kit de ferramentas contém uma estrutura e módulos de plugin de Provedores de Serviços.

Para aplicativos, a estrutura fornece a API CSSM (Common Security Services Manager), rica em funcionalidade, do padrão CDSA da Intel Corporation. A IBM expandiu a API CSSM, adicionando funções de recuperação de chave. Quando você utiliza o produto IBM KeyWorks Toolkit, seu aplicativo pode:

- Criptografar e decriptografar informações
- Verificar assinaturas digitais com vários objetivos
- Recuperar certificados e listas de revogação de certificados dos diretórios
- Criar campos de recuperação de chave para recuperação de chave e backup criptográfico
- Decidir se um certificado pode ser confiado, com base nos critérios estabelecidos por projetistas e programadores de sistemas, seguindo as instruções de usuários

Normalmente, uma empresa ou um distribuidor OEM integra os produtos IBM KeyWorks Toolkit e IBM Key Recovery Service Provider Toolkit aos aplicativos e middleware, de modo a permitir a utilização de APIs CSSM na estrutura CSSM Framework. O produto desta integração é um conjunto de aplicativos de tempo de execução e middleware para servidores e clientes distribuídos no ambiente ou ambientes operacionais. Os outros elementos do FirstSecure irão, com o tempo, depender do IBM KeyWorks Toolkit para todos os serviços criptográficos e operações de critérios confiáveis.

Integradores que utilizam o IBM KeyWorks Toolkit devem ter em sua equipe técnica engenheiros e programadores com experiência razoavelmente vasta em design criptográfico e programação, bem como middleware e estruturas, ou que tenham acesso a integradores subcontratados ou distribuidores OEM com essa experiência.

Para provedores de serviços, a estrutura fornece a interface SPI (Service Provider Interface), o padrão CDSA da organização Open Group. A IBM melhorou a interface SPI, adicionando funções de recuperação de chave.

O produto SDK (IBM KeyWorks Toolkit) inclui módulos plugin de provedores de serviços, que suportam padrões abertos e certificados de chave pública proprietários. Estes módulos incluem PKCS#11, funções criptográficas BSAFE da RSA Data Security, certificados X.509V3, critérios confiáveis da Entrust e Verisign e LSAP (Lightweight Directory Access Protocol). A estrutura proporciona integração ininterrupta de funções criptográficas, confiáveis e de segurança fornecidas pelos módulos de provedores de serviços independentes.

O produto IBM KeyWorks Toolkit pode fornecer funções administrativas críticas, incluindo:

- Proteção contra a omissão de etapas vitais em um processo suportado pelo KeyWorks
- Garantia de que os módulos plugin do Provedor de Serviços não foram alterados antes da utilização
- Utilização dos módulos plugin do Provedor de Serviços apenas através da estrutura
- Suporte para criptografia específica do país e específica da empresa, e utilização de critérios confiáveis

O produto IBM KeyWorks Toolkit oferece à sua empresa os seguintes benefícios:

- Permite a alteração ou substituição de módulos do Provedor de Serviços sem que seja necessário reescrever seus aplicativos e middleware
- Fornece suporte ininterrupto para criptografia por hardware e assinatura digital
- Suporta diretórios LDAP e o padrão de assinatura DSA
- Não requer a utilização de nenhum CA (Autoridade de Certificado) específico

Mais informações sobre o produto IBM KeyWorks Toolkit podem ser encontradas na publicação *IBM KeyWorks Toolkit Developer's Guide.*

Interação do IBM KeyWorks Toolkit com o IBM SecureWay Trust Authority

Não instale o produto IBM KeyWorks Toolkit no mesmo servidor do produto IBM SecureWay Trust Authority.

IBM Key Recovery Service Provider Toolkit 1.1

O produto IBM Key Recovery Service Provider 1.1.3.0 , fornecido no formato de conjunto de ferramentas, é um módulo de Provedor de Serviços que utiliza as funções padrão fornecidas pelo IBM KeyWorks Toolkit. O produto IBM Key Recovery Service Provider permite a recuperação de informações criptografadas armazenadas e transmitidas, sem coletar e intitular chaves privadas e sem criar pontos únicos de vulnerabilidade criptográfica.

Como o produto IBM Key Recovery Service Provider utiliza as funções padrão fornecidas pelo IBM KeyWorks Toolkit, a função de recuperação de chave pode ser utilizada com diferentes fornecedores criptográficos, certificados padrão de várias autoridades de certificado, critérios assegurados da Verisign e Entrust, e qualquer diretório que possa ser acessado pelo LDAP. O produto IBM Key Recovery Service Provider cria informações de

recuperação de chave com base na chave de sessão associada à comunicação entre correspondentes.

Mais informações sobre o produto IBM Key Recovery Service Provider estão localizadas na publicação *Key Recovery Server Installation and Usage Guide*, que é fornecida no Pacote de Documentação do produto FirstSecure.

Capítulo 16. Documentação fornecida com o produto FirstSecure

Cada produto componente incluído no software FirstSecure contém sua própria documentação. Este capítulo fornece informações sobre a documentação incluída com cada produto componente do software FirstSecure.

Um pacote de mídia e um pacote de documentação estão disponíveis para os produtos SecureWay FirstSecure, SecureWay Policy Director e SecureWay Boundary Server. Os pacotes de mídia contêm CDs do produto utilizados para instalar os produtos componentes da oferta e alguns destes CDs contêm documentação online. Os pacotes de documentação contêm a versão impressa de publicações dos produtos componentes que os inclui. A “Pacote de documentação do FirstSecure” na página 95 lista o conteúdo dos pacotes de documentação.

Policy Director

A documentação a seguir é fornecida com os produtos componentes do Policy Director.

IBM SecureWay Policy Director Up and Running
: Informa como instalar e configurar o IBM SecureWay Policy Director.

IBM SecureWay Policy Director Administration Guide
: Informa como administrar o IBM SecureWay Policy Director. Este manual é fornecido em formato PDF.

IBM SecureWay Policy Director Programming Guide and Reference
: Informa como escrever programas para o IBM SecureWay Policy Director. Este manual é fornecido em formato PDF.

Readme do produto
: Estas informações estão disponíveis na Web, no endereço www.ibm.com/software/security/policy

SecureWay Boundary Server

Os manuais a seguir descrevem os produtos componentes do SecureWay Boundary Server, seus requisitos e suas interações.

IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running
: Um manual impresso que descreve os produtos componentes do SecureWay Boundary Server.

As seções a seguir descrevem a documentação fornecida com os produtos componentes do SecureWay Boundary Server.

IBM SecureWay Firewall

Toda a documentação do produto IBM Firewall é fornecida em cópia eletrônica. O produto IBM Firewall fornece a seguinte documentação:

IBM SecureWay Firewall for AIX Setup and Installation
: Instruções para a instalação e configuração do produto IBM SecureWay Firewall para AIX.

IBM SecureWay Firewall for Windows NT Setup and Installation
: Instruções para instalação e configuração do produto IBM SecureWay Firewall para Windows NT.

IBM SecureWay Firewall for AIX User's Guide
: Instruções para instalação e configuração do produto IBM SecureWay Firewall para Windows NT.

IBM SecureWay Firewall for Windows NT User's Guide
: Informações sobre a utilização do produto IBM Firewall para Windows NT.

IBM SecureWay Firewall for Windows NT Reference
: Contém material de referência para utilização do produto IBM Firewall para Windows NT.

IBM SecureWay Firewall for AIX Reference
: Contém material de referência para utilização do produto IBM Firewall para AIX.

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
: Contém instruções para determinação de problemas.

IBM SecureWay Firewall VPN Client User's Guide
: Informa como configurar e utilizar uma rede privada virtual.

MIMEsweeper

O produto MIMEsweeper inclui a seguinte documentação:

MIMEsweeper Administrator's Guide
: Contém uma seção de Notas de Release (Release Notes), seguida de informações para o administrador, incluindo informações de planejamento e instalação.

  Este manual é fornecido no formato HTML, no CD do produto. Você pode exibi-lo online através do arquivo denominado \DOC\MANUAL.HTM, com um navegador da Web.

MIMEsweeper Release Notes
Contém documentação atualizada, incluindo informações sobre instalação e instruções para exibição da documentação online.

Este manual é fornecido no formato HTML, no CD do produto. Você pode exibi-lo online através do arquivo denominado \DOC\RELNOTES.HTM, com um navegador da Web.

MIMEsweeper Configuration Editor Help
Contém informações sobre a edição de arquivos de configuração do MIMEsweeper.

Este manual é fornecido no formato HTML, no CD do produto.

SurfinGate

O produto SurfinGate inclui a seguinte documentação em cópia eletrônica:

SurfinGate Installation Guide
Informações sobre a instalação e configuração dos componentes do SurfinGate 4.05 no Windows NT. Uma versão PDF da publicação *SurfinGate Installation Guide* é fornecida no CD do produto, no arquivo: \docs\install.pdf.

SurfinGate User Guide
Informações sobre planejamento e utilização do produto SurfinGate. Uma versão PDF da publicação *SurfinGate User Guide* é fornecida no CD do produto, no arquivo: \docs\manual.pdf.

SurfinGate 4.05 for Windows NT Release Notes
Informações sobre o produto SurfinGate 4.05, incluindo requisitos do sistema e limitações do produto. Uma versão PDF da publicação *SurfinGate 4.05 for Windows NT Release Notes* é fornecida no CD do produto, no arquivo: \docs\relnotes.pdf.

SurfinGate for Windows NT/UNIX Solaris Release Notes, Appendix A
Documentação online que discute alterações ao produto SurfinGate. Este documento está localizado no CD do produto, no arquivo: \docs\rnappen.pdf.

Intrusion Immunity

A seção a seguir descreve a documentação fornecida com o produto componente Intrusion Immunity.

Tivoli Cross-Site for Security

O produto Tivoli Cross-Site for Security, Version 1.1 inclui a seguinte documentação em formato .pdf:

Tivoli Cross-Site for Security Installation
: Este documento fornece os requisitos detalhados para a instalação e o dá instruções das etapas de instalação.

Tivoli Cross-Site for Security User's Guide
: Este documento fornece uma visão geral do produto, instruções para utilização do console e realização de tarefas, informações de referência como interfaces de linha de comando, os arquivos de configuração e um glossário. Você pode acessar este documento no CD-ROM do produto.

Norton AntiVirus

O produto Norton AntiVirus inclui a seguinte documentação para os componentes suportados no software FirstSecure. Todos os documentos, exceto o arquivo contents.txt, são fornecidos no formato PDF, no CD do Norton AntiVirus. O arquivo contents.txt é um arquivo ASCII, incluído no CD do produto.

Conteúdo da documentação do CD Norton AntiVirus Solution Release 3.04

O arquivo do CD do Norton AntiVirus Solution Release 3.04 denominado \contents.txt lista todas as documentações incluídas no CD.

Soluções de administração

Norton AntiVirus Solution Implementation Guide
: Consulte o arquivo \docs\admin\navimp.pdf no CD do produto.

Norton AntiVirus Command-Line Scanner
: Consulte o arquivo \docs\navc\navcugd.pdf no CD do produto.

Criação do Emergency Rescue Disk
: Consulte o arquivo \navc\readme.txt no CD do produto.

Soluções para servidores

Norton AntiVirus for Windows NT Server Administrator's Guide
: Consulte o arquivo \docs\admin\navnts50.pdf no CD do produto.

Norton AntiVirus for NetWare User's Guide
: Consulte o arquivo \docs\NAVNLM\NVN4.pdf no CD do produto.

Norton AntiVirus for Lotus Notes Installation Guide
: Consulte o arquivo \docs\NAVNOTES\NAVNOTES.pdf no CD do produto.

Norton AntiVirus for Lotus Notes Installation Guide
: Consulte o arquivo \docs\NAVNOTES\NAVNOTES.pdf no CD do produto.

Norton AntiVirus for OS/2 Lotus Notes Installation Guide
Consulte o arquivo \docs\NOTESOS2\NOTESOS2.pdf no CD do produto.

Norton AntiVirus for Microsoft Exchange Installation Guide
Consulte o arquivo \docs\NAVXCHNG\NAVXCHNG.pdf no CD do produto.

Soluções para gateway

Norton AntiVirus for Internet Email Gateway User's Guide
Consulte o arquivo \docs\navieg\navieg.pdf no CD do produto.

Norton AntiVirus for Firewalls Administrator's Guide
Consulte o arquivo \docs\navfw\navfw.pdf no CD do produto.

Soluções para desktop

Norton AntiVirus User's Guide for Windows 3.1/DOS
Consulte o arquivo \docs\navwks\nav4dusr.pdf no CD do produto.

Norton AntiVirus Reference Guide for Windows 3.1/DOS
Consulte o arquivo \docs\navwks\nav4dref.pdf no CD do produto.

Norton AntiVirus for Windows 95/98 User's Guide
Consulte o arquivo \docs\navwks\nav98usr.pdf no CD do produto.

Norton AntiVirus for Windows 95/98 Reference Guide
Consulte o arquivo \docs\navwks\nav98ref.pdf no CD do produto.

Norton AntiVirus for Windows NT User's Guide
Consulte o arquivo \docs\navwks\nav5nusr.pdf no CD do produto.

Norton AntiVirus for Windows NT Reference Guide
Consulte o arquivo \docs\navwks\nav5nref.pdf no CD do produto.

Norton AntiVirus v4.0 User's Guide for Windows NT
Consulte o arquivo \docs\351\navntugd.pdf no CD do produto.

Norton AntiVirus v4.0 Reference Guide for Windows NT
Consulte o arquivo \docs\351\navntref.pdf no CD do produto.

Norton AntiVirus User's Guide for OS/2
Consulte o arquivo \docs\navos2\navos2ug.pdf no CD do produto.

Norton AntiVirus Distribution Guide for OS/2
Consulte o arquivo \docs\navos2\navos2dg.pdf no CD do produto.

Norton AntiVirus for Macintosh User's Guide
Consulte o arquivo \docs\navmac\navmac.pdf no CD do produto.

Informes oficiais no CD do Norton AntiVirus Solution Release 3.04: O CD também contém informes oficiais no diretório \sarc. Cada informe oficial está no formato .pdf.

Vídeos no CD do Norton AntiVirus Solution Release 3.04: O CD também contém vídeos. Para exibir um vídeo, você deve ter o programa Media Player ou outro programa capaz de reproduzir arquivos .AVI. Os vídeos estão nos seguintes arquivos:

SARC \sarc\sarc.avi

About Viruses (Sobre Vírus)
\sarc\aboutvir.avi

Norton AntiVirus: the Guided Tour (Tour Guiado)
\navtour\guided\demo32.exe

How to Respond When Norton AntiVirus Alerts You (Como responder quando o Norton AntiVirus envia alertas)
\navtour\alert\demo32.exe

A Tour of Norton System Center (Um tour do Norton System Center)
\nsctour\setup.exe

ou, para executar o tour diretamente do CD,

\nsctour\demo32.exe

Mais informações sobre o tour estão no arquivo \ncstour\readme.txt

Trust Authority

A documentação do produto IBM SecureWay Trust Authority está disponível no formato PDF (Portable Document Format) e no formato HTML no CD-ROM de documentação do *Trust Authority*. A maioria das informações foram traduzidas para os idiomas suportados pelo Trust Authority. Para obter instruções sobre o acesso à publicação no idioma de sua escolha, consulte o arquivo *Readme* do produto. A versão mais recente do arquivo *Readme* está sempre disponível na página da Biblioteca do site do IBM SecureWay Trust Authority na web, no endereço
http://www.ibm.com/software/security/trust/library

A biblioteca Trust Authority inclui a seguinte documentação:

IBM SecureWay Trust Authority Up and Running
Este manual fornece uma visão geral do produto. Ele lista os requisitos do produto, inclui procedimentos para instalação e fornece informações sobre como acessar a ajuda online disponível para cada componente do produto. Além de estar disponível no CD-ROM de *Documentação*, este manual é impresso e distribuído com o produto.

IBM SecureWay Trust Authority System Administration Guide
Este manual contém informações gerais sobre administração do sistema Trust Authority. Ele inclui procedimentos para início e encerramento dos servidores, alteração de senhas, administração de

autoridade de certificado, realização de auditorias e execução de verificação de integridade de dados.

IBM SecureWay Trust Authority Configuration Guide
: Este manual contém informações sobre como utilizar o Assistente para Configuração para configurar um sistema Trust Authority. Você pode acessar a versão HTML deste manual na ajuda online do Assistente.

IBM SecureWay Trust Authority Registration Authority Desktop Guide
: Este manual contém informações sobre como utilizar o RA Desktop para administrar certificados ao longo do ciclo de vida do certificado. Você pode acessar a versão HTML deste manual na ajuda online do Área de Trabalho.

IBM SecureWay Trust Authority User's Guide
: Este manual contém informações sobre como obter certificados. Ele fornece procedimentos para utilização dos formulários de inscrição do Trust Authority para solicitar certificados para navegadores, servidores e dispositivos. Ele também mostra aos usuários como pré-registrar para um certificado PKIX e como utilizar o Trust Authority Client para armazenar e administrar certificados PKIX. Você pode acessar a versão HTML deste manual na ajuda online do Client.

Toolbox

As seções a seguir descrevem a documentação fornecida com os produtos componentes do Toolbox.

As APIs do Toolbox

Toda a documentação do Toolbox está disponível no seguinte site da web: `www.ibm.com/software/security/firstsecure/library`. A documentação a seguir é incluída:

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference
: Fornece uma visão geral das APIs e do iKeyman. Define cada API, sua sintaxe e sua utilização.

IBM SecureWay Directory Client SDK Programming Reference
: Inclui vários programas clientes de amostra LDAP e uma biblioteca de cliente LDAP que fornece acesso a aplicativos para os servidores LDAP. É fornecido suporte para C e Java.

IBM SecureWay Policy Director Programming Guide and Reference
: Define cada API, sua sintaxe e sua utilização.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide
Fornece instruções e requisitos de instalação.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference
Fornece informações para programadores que desenvolvem aplicativos que utilizam o IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms, também denominado PKIX. Inclui uma visão geral do produto, instruções para escrever programas para componentes separados do PKIX e descrições das APIs do PKIX.

IBM KeyWorks Toolkit

Toda documentação fornecida com o produto IBM KeyWorks Toolkit está disponível online, no formato PDF, no CD do produto. Documentação disponível:

IBM KeyWorks Toolkit Developer's Guide
Apresenta uma visão geral do conjunto de ferramentas. Também explica como integrar o conjunto de ferramentas com aplicativos e contém um aplicativo de amostra.

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
Define a interface que os desenvolvedores de aplicativos utilizam para acessar os serviços de segurança fornecidos pelos módulos de estrutura e do provedor de serviços.

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
Descreve recursos comuns a todos os módulos do provedor de serviços do conjunto de ferramentas. Este documento deve ser utilizado juntamente com as Especificações de Interface do Provedor de Serviços, para criar um módulo do provedor de serviços.

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
Define a interface com a qual os módulos do provedor de serviços de criptografia devem estar em conformidade, a fim de que possam ser acessados através do conjunto de ferramentas.

IBM Key Recovery Service Provider Interface (KRSPI) Specification
Define a interface com a qual os módulos do provedor de serviços de recuperação de chave devem estar em conformidade para poderem ser acessados através do conjunto de ferramentas.

IBM KeyWorks Toolkit Trust Policy Interface Specification
Define a interface com a qual os criadores de critérios, como Autoridades de Certificado, Emissores de Certificados e desenvolvedores de aplicativos de criação de critérios devem estar em conformidade, para expandir o conjunto de ferramentas com critérios modelos ou critérios específicos para aplicativos.

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification
Define a interface com a qual os desenvolvedores de biblioteca de certificados devem estar em conformidade para fornecer serviços de manipulação de certificados específicos de formatos a vários aplicativos conjunto de ferramentas e módulos de critérios confiáveis.

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification
Define a interface com a qual os desenvolvedores de biblioteca devem estar em conformidade para fornecer armazenamento de certificados persistente, específico de formato ou independente de formato.

IBM Key Recovery Service Provider

A documentação apresentada a seguir é fornecida com o produto IBM Key Recovery Service Provider no formato PDF, no CD do produto:

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide
Fornece um entendimento dos conceitos de recuperação de chave, orientação na configuração de uma solução de recuperação de chave para uma organização, e procedimentos para instalação, configuração e operação do IBM Key Recovery Server.

Redbooks sobre segurança

Os redbooks apresentados a seguir, produzidos pela IBM ITSO (International Technical Support Organization) apresentam produtos e processos relacionados a segurança. Eles estão disponíveis no endereço www.us.ibm.com/redbooks.

Understanding the IBM SecureWay FirstSecure Framework

IBM eNetwork Firewall de Alta Disponibilidade

Pacotes de documentação

Os pacotes de documentação a seguir estão disponíveis para o produto IBM SecureWay FirstSecure.

Pacote de documentação do FirstSecure

O pacote de documentação do FirstSecure contém os seguintes manuais:

FirstSecure License Information

IBM SecureWay FirstSecure Planning and Integration

IBM SecureWay Policy Director Up and Running

IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running

IBM SecureWay Trust Authority Up and Running

Tivoli Cross-Site for Security Installation

Pacote de documentação do Policy Director

O pacote de documentação do Policy Director contém os seguintes manuais:

Policy Director License Information

IBM SecureWay Policy Director Up and Running

Pacote de documentação do SecureWay Boundary Server

O pacote de documentação do SecureWay Boundary Server contém os seguintes manuais:

SecureWay Boundary Server License Information

IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running

Parte 4. Apêndices

Apêndice A. Avisos

Consulte o representante IBM local para saber quais produtos e serviços são oferecidos em sua região. Referências a produtos, programas ou serviços IBM não significam que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição ao produto, programa ou serviço. A avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM é 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. Pedidos de licença podem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais - IBM Brasil
Avenida Pasteur, 138-146 - Botafogo
Rio de Janeiro, RJ
CEP 22.290-240
Brasil

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO", SEM GARANTIA DE ESPÉCIE ALGUMA, EXPLÍCITA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS DE NÃO VIOLAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM FIM ESPECÍFICO. Alguns países não permitem a exclusão de garantias explícitas ou implícitas em certas transações; portanto, esta declaração pode não se aplicar a você.

Esta publicação pode incluir imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode fazer aperfeiçoamentos e/ou alterações nos produtos e/ou programas descritos nestas informações, a qualquer momento, sem aviso prévio.

Quaisquer referências nesta publicação a sites da Web que não sejam controlados pela IBM são fornecidas apenas por conveniência e não constituem endosso desses sites da Web. Os materiais contidos nesses sites da Web não fazem parte dos materiais deste produto IBM e a utilização desses sites da Web é de inteira responsabilidade do cliente.

Quando você envia informações à IBM, concede a ela direitos não exclusivos de utilização ou distribuição das informações, da forma que julgar adequada, sem incorrer em obrigações para com você.

O programa licenciado descrito neste documento e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos do Contrato de Cliente IBM (IBM Customer Agreement), Contrato de Licença de Programa Internacional IBM (IBM International Program License Agreement) ou qualquer contrato equivalente.

Todos os dados de desempenho contidos aqui foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sito feitas em sistemas a nível de desenvolvimento e não há garantias de que estas medidas serão iguais nos sistemas normalmente disponíveis. Além disso, algumas medidas podem ter sido estimadas através da extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seus ambientes específicos.

As informações sobre produtos não-IBM foram obtidas junto aos fornecedores desses produtos, seus anúncios publicados e outras fontes disponíveis publicamente. A IBM não efetuou nenhum teste desses produtos e não pode afirmar a precisão de seu desempenho, compatibilidade ou outras reclamações relacionadas a produtos não-IBM. Perguntas sobre recursos de produtos não-IBM devem ser endereçadas aos fornecedores desses produtos.

Todas as declarações a respeito de futuras instruções ou intenções da IBM estão sujeitas à alteração ou remoção sem aviso prévio e representam apenas objetivos e metas.

Todos os preços IBM apresentados são preços de revenda sugeridos pela IBM, são atuais e sujeitos a alterações sem aviso prévio. Os preços do revendedor podem variar.

Estas informações tem apenas objetivo de planejamento. As informações aqui contidas estão sujeitas a mudança antes dos produtos descritos serem disponibilizados.

Marcas

Os termos a seguir são marcas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

AIX
AIX/6000
DB2
DB2 Universal Database

eNetwork
Global Sign-On
GSO
IBM
Netfinity
OS/2
RS/6000
SecureWay
Websphere

Intel e Pentium são marcas ou marcas registradas da Intel Corporation nos Estados Unidos e em outros países.

Java e todas as marcas e logotipos Java são marcas ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e em outros países.

Lotus, Lotus Notes, Domino e cc:Mail são marcas da Lotus Development Corporation nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas ou marcas registradas da Microsoft Corporation nos Estados Unidos e em outros países.

Tivoli é marca da Tivoli Systems Inc. nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada nos Estados Unidos e em outros países licenciado exclusivamente pela X/Open Company Limited.

Outros nomes de empresas, produtos e serviços podem ser marcas ou marcas de serviço de terceiros.

Glossário

Este glossário define termos e abreviações utilizadas neste manual, que podem ser novas ou não familiares, bem como termos que podem ser de seu interesse. Ele inclui termos e definições do:

The IBM Dictionary of Computing, New York: McGraw-Hill, 1994.

The American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.

The Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1996.

.

A

ACL. Lista de Controle de Acesso.

ActiveX. Em programação da Microsoft, um conjunto de tecnologias e termos orientados por objeto.

agente. No produto Tivoli Cross-Site for Security, um monitor de pacote IP inteligente que mantém pacotes em cache, verifica neles anormalidades em diferentes camadas de rede e mantém conhecimento do status de conexões e estatísticas estabelecidas.

ambiente de desenvolvimento integrado. Um programa para desenvolvimento de aplicativos que permite a você codificar o aplicativo, executá-lo em pontos de interrupção e receber ajuda de diagnóstico para erros de programa.

API. Interface de programa aplicativo

Aplicativo da Web. Um aplicativo projetado para acesso através da World Wide Web.

Applet. Um programa de computador gravado em Java que executa dentro de navegadores compatíveis com Java, como o Netscape Navigator. Também denominado applet Java.

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

autenticação. O processo de determinação confiável da identidade de um interlocutor de comunicação.

autoridade de certificado. A entidade, aplicativo de software ou pessoa responsável pelo cumprimento de critérios de segurança de uma organização e atribuição de identidades eletrônicas seguras na forma de certificados. Os pedidos de processos de autoridade de certificado para emitir, renovar e anular certificados.

Autorização. O processo de determinação dos tipos de atividades que um usuário tem permissão de realizar. Geralmente, autorização ocorre após a autenticação.

B

Bloodhound. No programa Norton AntiVirus, o componente que rastreia um vírus.

bomba de macro. Uma seqüência gravada de comandos enviados para outro usuários para causar resultados indesejáveis.

C

Canal. Um caminho por onde os sinais podem ser enviados.

célula. No DCE, um grupo de usuários, sistemas e recursos que são geralmente centralizados em um objetivo comum e que compartilham limites de segurança, administrativos e de nomeação. Uma célula geralmente é formada por usuários, máquinas e recursos que armazenam um objetivo comum e um grande nível de confiança entre eles, mais do que em relação a usuários, máquinas e recursos de fora da célula.

Certificado digital. Uma credencial eletrônica emitida por terceiros confiáveis para uma pessoa

ou entidade. Um certificado contém informações sobre a entidade que certifica.

chamada de procedimento remoto. (1) Uma função que um cliente utiliza para solicitar a execução de uma chamada de procedimento de um servidor. Esta função inclui uma biblioteca de procedimentos e representação de dados externos. (2) Um pedido de cliente para um provedor de serviço existente em outro nó.

chave pública. A chave em um par de chaves pública/privada que é disponibilizada para terceiros. Ela permite que eles direcionem uma transação para o proprietário da chave ou para confirmar uma assinatura digital. Dados criptografados com a chave pública podem ser decriptografados apenas com a chave privada correspondente. *Veja também* par de chave pública/privada.

Cliente. (1) Uma unidade funcional que recebe serviços compartilhados de um servidor. (2) Um computador ou programa que solicita um serviço de outro computador ou programa.

código móvel. Relativo à computação que é realizada em um computador portátil por um usuário que está freqüentemente se movendo entre várias localizações e utilizando diferentes tipos e conexões de rede (por exemplo, dial-up, LAN, ou sem cabo).

Controle de acesso. Em segurança de computadores, o processo de assegurar que os recursos de um sistema de computadores pode ser acessado apenas por usuários autorizados, de maneiras autorizadas.

criptografar. Misturar informações para que apenas alguém que saiba o código de decodificação apropriado possa obter as informações originais através de decodificação.

D

daemon. No AIX, um programa que permanece residente aguardando um pedido de serviço.

DCE. Distributed Computing Environment.

Distributed Computing Environment. Serviços e ferramentas que suportam a criação, uso e manutenção de aplicativos distribuídos em um ambiente de computação heterogêneo.

E

e-business. A condução de transações comercias através de redes e computadores. Inclui a compra e venda de bens e serviços. Também inclui a transferência de fundos através de comunicações digitais.

e-commerce. Condução de transações de empresa a empresa. Inclui a compra e venda de bens e serviços (com clientes, revendedores, fornecedores e outros) na Internet. É o elemento principal do e-business.

espaço de nome. Relativo ao Directory, a estrutura externa de nomes que é acessível a usuários.

extranet. Uma derivação da Internet que utiliza tecnologia similar. Empresas estão começando a aplicar publicação na Web, e-commerce, mensagens e groupware para múltiplas comunidades de clientes, parceiros e equipes internas.

F

Filtragem de conteúdo. Desmontagem de uma transmissão para ler seu conteúdo com objetivo de determinar se a transmissão atende a padrões de conteúdo específicos.

filtragem de endereço de rede. O processo de verificação do endereço de e-mail recebido ou enviado para comprovar se o destinatário ou o emissor são aceitáveis.

firewall. Um sistema ou combinação de sistemas que reforçam os limites entre duas ou mais redes.

FTP (File Transfer Protocol). Um protocolo cliente/servidor da Internet que pode ser utilizado para transferir arquivos entre computadores.

G

gateway. Um sistema que permite que redes ou aplicativos incompatíveis estabeleçam comunicação um com o outro.

Gateway de nível de circuito. Em um firewall, um servidor proxy que redireciona um pedido de cliente através do firewall até o servidor desejado.

H

hacker. Uma pessoa que tenta acessar uma máquina ou sistema sem autorização apropriada. Hackers geralmente utilizam recursos sem permissão.

I

IDE. Integrated development environment.

Implementation Services. O suporte para instalação on-site fornecido pela IBM

incidente. No programa Tivoli Cross-Site for Security, uma atividade suspeita que pode ser um ataque no sistema.

interface de programa aplicativo. Uma interface funcional que permite a um programa aplicativo gravado em linguagem de alto nível utilizar funções específicas.

Internet. Um conjunto mundial de redes que fornece comunicação eletrônica entre computadores. Permite comunicação entre eles através de dispositivos de software como correio eletrônico ou navegadores da Web. Por exemplo, algumas universidades possuem uma rede, que por sua vez, são ligadas a outras redes semelhantes pela Internet.

intranet. Um rede dentro de uma empresa que geralmente reside atrás de firewalls. É uma derivação da Internet que utiliza tecnologia similar. Tecnicamente, intranet é uma mera extensão da Internet. HTML (a linguagem utilizada para representação gráfica de informações) e HTTP (um protocolo que move arquivos de hypertexto através da Internet) são algumas das semelhanças.

IPSec. Um padrão de Internet Protocol Security desenvolvido pela IETF. IPSec é um protocolo de camada de rede projetado para fornecer serviços de segurança criptográfica que suportam flexivelmente combinações de autenticação, integridade, controle de acesso e confidencialidade. Devido a seus fortes recursos de autenticação, ele foi adotado por vários fornecedores de produtos VPN para o estabelecimento de conexões seguras de ponto a ponto através da Internet.

ISV. Independent Software Vendor.

J

Java. Um conjunto de tecnologias de computador reconhecidos pela rede, sem plataforma específica desenvolvidos pela Sun Microsystems, Incorporated. O ambiente Java consiste no Sistema Operacional Java, as máquinas virtuais para várias plataformas, a linguagem de programação Java orientada em objetos e várias bibliotecas de classe.

JavaScript. Uma linguagem de script que se parece com Java e foi desenvolvida pela Netscape para ser utilizada com o navegador Netscape.

K

Kerberos. Um método seguro de autenticação de um serviço que solicita um computador. Kerberos foi desenvolvido no Athena Project no MIT (Massachusetts Institute of Technology). Na mitologia grega; Kerberos foi um cão de três cabeças que guardava os portões do Hades. Kerberos permite que um usuários solicite um ticket criptografado de um processo de autenticação que depois pode ser utilizado para solicitar um serviço específico de um servidor. A senha do usuário não precisa passar pela rede.

L

LDAP. Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol. No IBM SecureWay Directory, LDAP fornece uma maneira para manter informações de diretório em uma localização central para armazenamento, atualização, recuperação e troca.

lista de controle de acesso. Um mecanismo de limitação de uso de um recurso especificado a usuários autorizados.

M

MPEG. O padrão sob desenvolvimento pelo Moving Pictures Experts Group para compressão e armazenamento de vídeo e animação em formato digital.

N

não-repudiação. O uso de uma chave privada digital para enviar que o assinante de um documento negue que o tenha assinado.

navegador da Web. Software cliente que executa em seu PC desktop e permite que você navegue na World Wide Web ou em páginas locais. É uma ferramenta de recuperação que fornece acesso universal à grande coleção de material de hypermídia disponível na Web e na Internet. Exemplos são os programas Netscape Navigator e Microsoft Internet Explorer. *Veja também* servidor.

O

object request broker. Em programação orientada para objetos, o software que serve como um intermediário permitindo que objetos troquem pedidos e respostas de maneira transparente.

objeto da Web. Dados disponibilizados através de um navegador da Web. Um objeto da Web pode ser uma página da Web, uma parte de uma página da Web, um arquivo, uma imagem, um diretório, um programa CGI ou um applet Java.

OEM. Original equipment manufacturer (Fabricante do equipamento original).

P

par de chaves pública/privada. Um par de chave pública/privada é parte do conceito de criptografia de par de chaves (apresentado em 1976 pela Diffie and Hellman para solucionar problemas de gerenciamento de chave). Em seu conceito, cada pessoa obtém um par de chaves, uma denominada a chave pública e outra a chave privada. A chave pública de cada pessoa é tornada pública enquanto a chave privada é mantida em segredo. O emissor e receptor não precisa compartilhar informações secretas: todas as comunicações envolvem apenas chaves públicas, a chave privada nunca é transmitida ou compartilhada. Não é mais necessário confiar alguns canais de comunicação para ser ter segurança contra bisbilhoteiros ou traição. O único requisito é que as chaves públicas sejam associadas com seus usuários de uma maneira confiável (autenticada), por exemplo em um diretório confiável. Qualquer pessoa pode enviar uma mensagem confidencial utilizando informações de chave pública. Entretanto, a mensagem pode ser decriptografada apenas com a chave privada, que esta em posse do destinatário desejado. Além disso, criptografia de par de chaves pode ser utilizada não apenas para privacidade (criptografia), mas também para autenticação (assinaturas digitais).

plug-in. Um programa que pode ser utilizado como parte de seu navegador da Web.

principal. Em DCE, uma entidade que pode comunicar seguramente com outra entidade através da segurança de DCE. Principais podem ser usuários, servidores ou computadores.

protocolo SOCKS. Um protocolo que permite a um aplicativo em uma rede segura estabelecer comunicação através de um firewall através de um servidor socks.

pulsação. Uma comunicação de um programa com um programa de gerenciamento para confirmar atividade; o programa informa ao programa de gerenciamento que ainda está ativo, realizando suas tarefas.

R

rede privada virtual. Uma rede de dados privada que utiliza a Internet ao invés de linhas telefônicas para estabelecer conexões remotas. Devido ao fato de usuários acessarem recursos de rede corporativos através de um ISP (Internet Service Provider) ao invés de uma linha telefônica, as organizações podem reduzir significantemente custos de acesso remoto. Um VPN também melhora a segurança de trocas de dados. Em tecnologia de firewall tradicional, uma mensagem pode ser criptografada, mas os

endereços de origem e destino não podem. Em tecnologia VPN, os usuários podem estabelecer uma conexão de túnel em que o pacote todo de informações (conteúdo e cabeçalho) é criptografado e encapsulado.

RPC. Em DCE, uma chamada de procedimento remoto

S

Secure Sockets Layer (SSL). (1) Um protocolo de comunicação padrão IETF com serviços de segurança internos que são o mais transparentes possível para o usuário final. Ele fornece um canal de comunicação seguro digitalmente. (2) Um servidor que suporta SSL geralmente aceita pedidos de conexão SSL em uma porta diferente dos pedidos HTTP padrão. SSL cria uma sessão durante a qual o protocolo de reconhecimento deve acontecer apenas uma vez. Após o protocolo de reconhecimento ter sido concluído, a comunicação é criptografada. Verificações de integridade de mensagem são realizadas até que a sessão SSL expire.

Serviço de diretório de célula. Um componente de um DCE (Distributed Computing Environment) que gerencia um banco de dados de informações sobre recursos no interior de uma célula DCE.

servidor. (1) Em uma rede, a estação de dados que fornece funções para outras estações; por exemplo, um servidor de arquivos. (2) Em TCP/IP, um sistema em uma rede que identifica os pedidos de um sistema para outro site, denominado cliente/servidor.

servidor Apache. Um conjunto de software de servidor da web livremente disponível.

servidor da Web. Um programa servidor que responde a pedidos para recursos de informações de programas navegadores.

Servidor IntraVerse. No programa IntraVerse, um sistema na rede que contém o software de servidor IntraVerse e que pode comunicar com a maioria dos sistemas de host em execução no software cliente NetSEAT. O servidor IntraVerse faz referência a um sistema ou combinação de sistemas que executam os programas relacionados ao produto.

servidor proxy. Um intermediário entre o computador solicitando acesso (A) e o computador sendo acessado (B). Assim, se um usuário final faz um pedido para um recurso a partir do computador A, este pedido é direcionado para um servidor proxy. O servidor proxy faz o pedido, recebe a resposta do computador B, e depois encaminha a resposta para o usuário final. Servidores proxy são úteis para acessar recursos da World Wide Web de dentro de um firewall.

servidor socks. Um gateway de nível de circuito que fornece conexão unidirecional através de um firewall para aplicativos de servidor em uma rede não segura.

spam. e-mail não solicitado, geralmente enviado para destinatário múltiplos.

T

TCP/IP. Transmission Control Protocol/Internet Protocol.

telnet. No conjunto de protocolos da Internet, um protocolo que fornece serviço de conexão de terminal remoto. Ele permite aos usuários de um host iniciar sessão em um host remoto e interagir como usuários diretamente conectados a este terminal.

Token SecurID. O método de autenticação do ACE/Server da Security Dynamics inclui um ID de usuário e um token SecurID. Quando você inicia sessão remotamente, recebe sua senha do token SecurID. A senha é trocada a cada 60 segundos e é eficiente para usuários de uma vez apenas. Mesmo que alguém intercepte sua senha através da rede aberta, a senha não é válida para uso adicional.

Transmission Control Protocol/Internet Protocol. Um conjunto de protocolos de comunicação que suportam funções de conectividade ponto a ponto para redes locais e remotas.

trilha de auditoria. Dados, no formato de um caminho lógico, que liga uma seqüência de eventos. Uma trilha de auditoria pode ser utilizada para rastrear transações ou o histórico

de uma dada atividade. Por exemplo, ele pode rastrear atividade em uma conta de cliente.

U

Universal Resource Locator. A convenção de denominação utilizada para comunicações na World Wide Web onde o caminho do objeto da Web começa com o nome do serviço, o nome da organização, o caminho e o nome do arquivo, por exemplo
http://www.ibm.com/software/security/firstsecure.

URL. Universal Resource Locator.

V

vault. Um vault utiliza criptografia para proteger informações contra revelação para pessoas não autorizadas, como administradores de sistema e proprietários de outros vaults. Ele também utiliza assinatura digital para proteger contra falsificação e certificação digital para proteger contra comunicação com pessoas não conhecidas. Ele também utiliza criptografia, assinatura e certificação para transmitir informações seguramente para outros vaults.

VPN. Virtual Private Network.

W

worm. Um vírus de computador que não apresenta perigo.

X

X.509. Um certificado amplamente aceito projetado para suportar gerenciamento e distribuição segura de certificados PKI assinados digitalmente através de redes da Internet seguras. O certificado X.509 define estruturas de dados que acomodam procedimentos relacionados a distribuição de chaves públicas digitalmente assinadas por terceiros confiáveis.

Índice Remissivo

O

P

R

S

T

U

V

W

X

Número da Peça: CT7EHBP

Impresso no Brasil

CT7EHBP