Objetivos
Use este módulo para:

• Configurar um canal de comunicação segura entre dois computadores Microsoft® Windows® 2000 Server usando o IPSec.

Início da página
Aplica-se a
Este módulo aplica-se aos seguintes produtos e tecnologias:

• Windows 2000 Server (com Service Pack 3)

• Monitor de rede Microsoft

• Microsoft .NET Framework versão 1.0 (com Service Pack 2) e versões posteriores

• Microsoft Visual Studio® 1.0 .NET e versões posteriores

• Microsoft Visual C#® .NET

• Microsoft SQL Server– 2000 (com Service Pack 2) e versões posteriores

Início da página
Como usar este módulo
Para obter o máximo deste módulo:

• Você deve ter dois computadores executando o sistema operacional Windows 2000 Server e configurados da seguinte maneira:

• Endereços IP fixos.

• SQL Server 2000 no computador do servidor de banco de dados com o banco de dados Northwind de exemplo instalado.

****
****

Protocolo de Segurança IP (IP Security Protocol, mais conhecido pela sua sigla, IPSec) é uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para uma localidade da internet, como bancos), integridade dos dados (garantindo que o mesmo conteúdo que chegou ao seu destino seja a mesma da origem) e autenticidade das informações ou identity spoofing (garantia de que uma pessoa é quem diz ser), quando se transferem informações através de redes IP pela internet.

IPSec é um protocolo que opera sob a camada de rede (ou camada 3) do modelo OSI. Outros protocolos de segurança da internet como SSL e TLS operam desde a camada de transporte (camada 4) até a camada de aplicação (camada 5).

Isto torna o IPsec mais flexível, como pode ser usado protegendo os protocolos TCP e UDP, mas aumentando sua complexidade e despesas gerais de processamento, porque não se pode confiar em TCP (camada 4 do modelo OSI) para controlar a confiabilidade e a fragmentação.

Índice [esconder]

[editar] Características

De acordo com Eduardo Rapoport do Departamento de Engenharia Eletrônica e de Computação (DEL) da Escola Politécnica/Universidade Federal do Rio de Janeiro [1] o IPSec combina diferentes e diversas tecnologias para prover uma melhor segurança, como um mecanismo de troca de chaves de Diffie-Hellman; criptografia de chave pública para assinar as trocas de chave de Diffie-Hellman, garantindo assim a identidade das duas partes e evitando ataques do tipo man-in-the-middle (onde o atacante se faz passar pela outra parte em cada um dos sentidos da comunicação); algoritmos de encriptação para grandes volumes de dados, como o DES (Data Encryption Standard); algoritmos para cálculo de hash (resto de uma divisão, de tamanho fixo) com utilização de chaves, com o HMAC, combinado com os algoritmos de hash tradicionais como o MD5 ou SHA, autenticando os pacotes e certificados digitais assinados por uma autoridade certificadora, que agem como identidades digitais.

[editar] O que é um protocolo

Ver artigo principal: Protocolo

Ao pé da letra, Protocolo significa algo que se pré-dispõe a pôr algo pronto a ser utilizado, através de recursos a ele atribuídos ou, ainda, é a padronização de leis e procedimentos que são dispostos na execução de uma determinada tarefa.

Na comunicação de dados e na interligação em rede, protocolo é um padrão que especifica o formato de dados e as regras a serem seguidas. Sem protocolos, uma rede não funciona. Um protocolo especifica como um programa deve preparar os dados para serem enviados para o estado seguinte do processo de comunicação.

[editar] O que é o protocolo IP
Ver artigo principal: Protocolo IP
IP é um acrónimo para a expressão inglesa "Internet Protocol" (ou Protocolo de Internet), que é um protocolo usado entre duas máquinas em rede para encaminhamento dos dados.

Os dados, numa rede IP, são enviados em blocos referidos como pacotes ou datagramas (os termos são basicamente sinónimos no IP, sendo usados para os dados em diferentes locais nas camadas IP). Em particular, no IP nenhuma definição é necessária antes do host tentar enviar pacotes para um host com o qual não comunicou previamente.

O IP oferece um serviço de datagramas não confiável (também chamado de melhor esforço); ou seja, o pacote vem quase sem garantias. O pacote pode chegar desordenado (comparado com outros pacotes enviados entre os mesmos hosts), também podem chegar duplicados, ou podem ser perdidos por inteiro. Se a aplicação precisa de confiabilidade, esta é adicionada na camada de transporte.

O IP é o elemento comum encontrado na internet pública dos dias de hoje. É descrito no RFC 791 da IETF, que foi pela primeira vez publicado em Setembro de 1981. Este documento descreve o protocolo da camada de rede mais popular atualmente em uso. Esta versão do protocolo é designada de versão 4, ou IPv4. O IPv6 tem endereçamento de origem e destino de 128 bits, oferecendo mais endereçamentos que os 32 bits do IPv4.

[editar] O que é VPN
Ver artigo principal: Rede Privada Virtual
Uma Rede Privada Virtual (Virtual Private Network - VPN) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída usando como suporte uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.

VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

[editar] Arquitetura de segurança
IPSec é o protocolo de criptografia da internet para tunelamento, encriptação e autenticação. Existem dois modos, consoante a unidade o que se está protegendo. No

modo transporte se protege o conteúdo útil do pacote IP e no modo túnel se protege o pacote IP completo.

[editar] Modo de transporte
No modo transporte, somente a mensagem (payload) é criptografada. O roteamento permanece intacto, desde que o cabeçalho do IP não seja modificado e nem cifrado; entretanto, quando o cabeçalho da autenticação é usado, os endereços IP não podem ser traduzidos, porque isto invalida o valor de hash. As camadas de transporte e de aplicação são fixas sempre pelo hash, assim, não podem sofrer nenhuma modificação. O modo transporte é usado para comunicações de host-a-host.

[editar] Modo de tunelamento
No modo de tunelamento, o pacote IP é criptografado por inteiro. Deve, assim, encapsular um novo pacote IP para distribuí-lo. O tunelamento é usado para comunicações da rede-a-rede (túneis seguros entre roteadores) ou comunicações de host-a-rede e de host-a-host sobre a internet.

[editar] Estado atual do padrão
IPsec é a parte majoritária do IPv6, e é opcional para o uso com IPv4. O padrão foi projetado para ser indiferente às versões do IP, à distribuição atual difundida e às implementações do IPv4. Os protocolos do IPsec foram definidos originalmente pelas RFCs 1825-1829, publicado em 1995. Em 1998, foram substituídos pelos RFCs 2401-2412. Os RFCs 2401-2412 não são compatíveis com os 1825-1829, embora sejam conceitualmente idênticos. Em dezembro de 2005, foi lançada a terceira geração dos documentos, os RFCs 4301-4309, tendo sido também provido o padrão Internet Key Exchange (IKE), que o IPsec utiliza para associação segura de chaves. São largamente baseados nos RFCs 2401-2412, mas fornecem um segundo padrão de troca da chave da internet. Estes novos documentos padronizam a abreviatura IPsec com "IP" em letras maiúsculas e "sec" em letras minúsculas.

[editar] Características técnicas
Dois protocolos foram desenvolvidos para prover um nível de segurança para os fluxos dos pacotes e mudanças de chaves como:

Encapsulating Security Payload (ESP), que provê autenticação, confidencialidade dos dados e integridade da mensagem.
Cabeçalho de autenticação (AH), que provê a autenticação e integridade dos dados, mas não a confidencialidade.

[editar] Cabeçalho de autenticação (AH)
0 - 7 bit 8 - 15 bit 16 - 23 bit 24 - 31 bit
Próximo cabeçalho Tamanho da mensagem RESERVADO
Identificação dos Parâmetros de Segurança (SPI)
Número de Sequência
Dados de autenticação (variável)

Descrição dos campos:

Próximo cabeçalho
Identifica o protocolo de dados de transferência.
Tamanho da mensagem
Tamanho do pacote AH.
RESERVADO
Reservado para uso futuro.
Identificação dos Parâmetros de Segurança (SPI)
A Identificação dos Parâmetros de Segurança (SPI) que, em combinação com o endereço IP, identifica a Associação de Segurança (SA) implementada para este pacote.
Número de Sequência
Um número crescente, usado para impedir ataques repetitivos.
Dados de Autenticação
Contém o valor da verificação da integridade (ICV) necessário para autenticação do pacote.

[editar] Encapsulating Security Payload (ESP)
O diagrama ESP:

0 - 7 bit 8 - 15 bit 16 - 23 bit 24 - 31 bit
Identificação dos Parâmetros de Segurança (SPI)
Número de Sequência

Dados de payload (variável)

Padding (0-255 bytes)
Tamanho do Pad Próximo cabeçalho
Dados de autenticação (variável)

Descrição dos campos:

Identificação dos Parâmetros de Segurança (SPI)
Identifica os parâmetros de segurança em combinação com o endereço de IP.
Número de sequência
Um número crescente, usado para impedir ataques repetitivos.
Dados da mensagem
Os dados a serem transferidos.
Padding
Usado por alguns algoritmos criptográficos para reordenar por inteiro o conteúdo dos blocos.
Tamanho do Pad

Tamanho do Pad em bytes.
Próximo cabeçalho
Identifica o protocolo para transferência dos dados.
Dados de autenticação
Contém os dados usados para autenticação do pacote.

[editar] Implementações
O suporte ao IPsec é geralmente incluído no kernel do sistema operativo com gerência de chave e ISAKMP/IKE entre as negociações realizadas no espaço do usuário-final. Existem implementações do IPsec que tendem a incluir ambas as funcionalidades. Entretanto, porque há uma relação padrão para a gerência de chave, é possível controlar uma pilha do IPsec no kernel usando uma ferramenta de gerência de chave com implementação diferente.

Por esta causa, há confusão a respeito das origens da implementação do IPsec que está no kernel do Linux. FreeS/WAN é o projeto que primeiro implementou uma solução completa e de código aberto do IPsec para Linux, e o projeto foi encerrado em março de 2004. Openswan e strongSwan são as continuações do FreeS/WAN. KAME project também implementou um suporte completo ao IPsec para o NetBSD e FreeBSD. O OpenBSD fez seu próprio daemon de ISAKMP/IKE, nomeado simplesmente como isakmpd (que foi movido também a outros sistemas, incluindo Linux).

Entretanto, nenhumas destas pilhas do IPsec foram integradas no kernel do Linux. Alexey Kuznetsov e David S. Moleiro escreveram uma implementação de IPsec para o kernel do Linux em torno do fim de 2002. Esta pilha foi liberada subseqüentemente como parte do Linux 2.6.

Conseqüentemente, contrariando a opinião popular, a pilha do IPsec no Linux não se originou do projeto KAME. Como suporta o protocolo padrão PF_KEY (RFC 2367) e a relação nativa XFRM para a gerência de chave, a pilha do IPsec no Linux pode ser usada conjuntamente com qualquer uma das implementações citadas abaixo.

6WINDGate, Network processor MPU Fast Path IPsec stack
NRL [1] IPsec, [2]
OpenBSD, com seu próprio código derivado da NRL IPsec
KAME, usado no Mac OS X, NetBSD e FreeBSD
"IPsec" da Cisco IOS Software [3]
"IPsec" no Microsoft Windows, incluindo Windows XP [4] [5], Windows 2000 [6], e Windows 2003 [7]
SafeNet QuickSec toolkits [8]
IPsec no Solaris [9]
IBM AIX
IBM z/OS
IPsec e IKE na HP-UX (HP-UX IPSec)
"IPsec and IKE" in VxWorks[10]

[editar] Citações e referências
↑ Curso de "Redes Privadas Virtuais" por Eduardo Rapoport

[editar] Ver também

Segurança da informação
IP spoofing é uma máscara de pacotes IP com endereços remetentes falsificados.
NAT transversal ou NAT-T
Layer 2 Tunneling Protocol (L2TP) ou Protocolo de Tunelamento sob a Camada 2.
Sistema de prevenção de intrusos
Firewall

[editar] RFCs relacionadas ao IPsec
RFC 2367
Interface PF_KEY
RFC 2401 (substituída pela RFC 4301)
Arquitetura de Segurança para o Protocolo Internet
RFC 2402 (substituída pela RFC 4302 e RFC 4305)
Cabeçalho de Autenticação
RFC 2403
O uso de HMAC-MD5-96 com ESP e AH
RFC 2404
O uso de HMAC-SHA-1-96 com ESP e AH
RFC 2405
ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2406 (substituída pela RFC 4303 e RFC 4305)
Encapsulating Security Payload (ESP)
RFC 2407 (substituída pela RFC 4306)
IPsec Domain of Interpretation for ISAKMP (IPsec DoI)
RFC 2408 (substituída pela RFC 4306)
Internet Security Association e Key Management Protocol (ISAKMP)
RFC 2409 (substituída pela RFC 4306)
Internet Key Exchange (IKE)
RFC 2410
O NULL Encryption Algorithm e o uso com IPsec
RFC 2411
IP Security Document Roadmap
RFC 2412
The OAKLEY Key Determination Protocol
RFC 2451
The ESP CBC-Mode Cipher Algorithms
RFC 2857
O uso de HMAC-RIPEMD-160-96 com ESP e AH
RFC 3526
More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3706
A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3715
IPsec-Network Address Translation (NAT) Compatibility Requirements
RFC 3947
Negociação de NAT-Traversal com IKE
RFC 3948
UDP Encapsulation of IPsec ESP Packets
RFC 4106

The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 4301 (substituída pela RFC 2401)
Security Architecture for the Internet Protocol
RFC 4302 (substituída pela RFC 2402)
IP Authentication Header
RFC 4303 (substituída pela RFC 2406)
IP Encapsulating Security Payload (ESP)
RFC 4304
Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
RFC 4305
Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 4306 (substituída pela RFC 2407, RFC 2408 e RFC 2409)
Internet Key Exchange (IKEv2) Protocol
RFC 4307
Cryptographic Algorithms para uso com Internet Key Exchange Version 2 (IKEv2)
RFC 4308
Cryptographic Suites for IPsec
RFC 4309
Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)
RFC 4478
Repeated Authentication in Internet Key Exchange (IKEv2) Protocol
RFC 4543
The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
RFC 4555
IKEv2 Mobility and Multihoming Protocol (MOBIKE)
RFC 4621
Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol
RFC 4806
Online Certificate Status Protocol (OCSP) Extensions to IKEv2
RFC 4809
Requirements for an IPsec Certificate Management Profile
RFC 4835 (substituída pela RFC 4305)
Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload
• Você deve ter experiência em programação usando Visual C# .NET.

• Você deve ter experiência no uso do ambiente de desenvolvimento Visual Studio .NET.

• Você deve ter experiência na configuração do Windows 2000 Server usando as Ferramentas Administrativas do Windows.

• Você deve ter experiência no uso da ferramenta Monitor de Rede.

• Leia o módulo 4 "Comunicações seguras". Ele fornece uma visão geral dos problemas associados aos canais de comunicação segura e uma introdução ao IPSec.

Início da página
Resumo
O IPSec (segurança de protocolo de Internet) é um mecanismo de camada de transporte por meio do qual é possível garantir a confidencialidade e a integridade das comunicações com base em TCP/IP entre computadores. O IPSec também oferece suporte à autenticação com base em computadores. Esses recursos tornam o IPSec ideal para proporcionar um canal de comunicação segura entre computadores que seja transparente para todos os aplicativos.

Este módulo descreve como configurar um canal de comunicação segura entre dois computadores usando o IPSec.

Início da página
O que é necessário saber
O IPSec pode ser usado para proteger os dados transmitidos entre dois computadores, como, por exemplo, um servidor de aplicativos e um servidor de banco de dados. O IPSec torna-se completamente transparente para os aplicativos porque os serviços de criptografia, integridade e autenticação são implementados no nível de transporte. Os aplicativos continuam a se comunicar uns com os outros, da maneira habitual, usando as portas TCP e UDP.

Usando o IPSec, você pode:

• Agregar confidencialidade às mensagens, criptografando todos os dados transmitidos entre dois computadores.

• Proporcionar integridade às mensagens transmitidas entre dois computadores (sem criptografar os dados).

• Proporcionar autenticação mútua entre dois computadores. Por exemplo, você pode ajudar a proteger um servidor de banco de dados estabelecendo uma diretiva que permita enviar solicitações somente a partir de um determinado computador cliente (por exemplo, um servidor de aplicativo ou um servidor Web).

• Restringir quais computadores podem se comunicar entre si. Pode também restringir a comunicação com protocolos IP e portas TCP/UDP específicos.

Este módulo mostra como proteger o canal de comunicação entre um servidor de aplicativos e um servidor de banco de dados executando o SQL Server 2000. O servidor de aplicativos usa a biblioteca de rede cliente TCP/IP recomendada para conectar-se ao SQL Server e usa a porta TCP padrão 1433 do SQL Server. A configuração é mostrada na Figura 1.

Figura 1
Configuração da solução do módulo Como

Este módulo descreve como usar uma diretiva simples do IPSec para aplicar o seguinte:

• Permitir comunicações com o SQL Server apenas do servidor de aplicativos usando o protocolo TCP através da porta 1433.

• Ignorar todos os outros pacotes IP, inclusive ICMP (ping).

• Criptografar todos os dados transmitidos entre os dois computadores para garantir a confidencialidade.

As vantagens dessa abordagem são:

• A confidencialidade de dados é fornecida a todos os dados transmitidos entre os dois computadores.

• A superfície de ataque no SQL Server é significativamente reduzida. Os únicos pontos de ataque restantes são fazer logon interativamente no servidor de banco de dados ou obter o controle do servidor de aplicativos e tentar atacar o SQL Server através da porta TCP 1433.

• A diretiva IPSec é extremamente simples de definir e implementar.

Esta diretiva apresenta as seguintes desvantagens:

• O SQL Server não pode se comunicar com os controladores de domínio e como resultado:

• A diretiva de grupo não pode ser aplicada (o servidor de banco de dados deve ser um servidor autônomo).

• A autenticação do Windows entre o servidor de aplicativos e o servidor de banco de dados requer contas locais sincronizadas (com o mesmo nome de usuário e senha) nos dois computadores.

• Não é possível usar métodos mais robustos de aplicação do IPSec (Windows 2000 padrão / Kerberos).

• O SQL Server não conseguirá se comunicar com outros computadores, inclusive servidores DNS.

• A abordagem apresentada neste módulo usa autenticação de chave pré-compartilhada, que não é recomendada para cenários de produção. Os sistemas de produção devem usar certificados ou a autenticação de domínio do Windows 2000. As diretivas do IPSec que usam segredos pré-compartilhados são apropriadas para uso apenas nos ambientes de desenvolvimento ou de teste.

• Os dois computadores devem ter endereços IP estáticos.

Observações
• Uma diretiva IPSec consiste em um conjunto de filtros, ações de filtro e regras.

• Um filtro consiste em:

• Um endereço IP de origem ou um intervalo de endereços.

• Um endereço IP de destino ou um intervalo de endereços.

• Um protocolo IP, como TCP, UDP ou "any".

• Portas de origem e de destino (apenas para TCP ou UDP).

• Os filtros também podem ser espelhados em dois computadores. Um filtro espelhado aplica a mesma regra no computador cliente e no servidor (com os endereços de origem e de destino invertidos).

• Uma ação de filtro especifica ações a serem tomadas quando um determinado filtro é chamado. Pode ser uma das seguintes:

• Permitir. O tráfego não é protegido. Ele pode ser enviado e recebido sem intervenção.

• Bloquear. O tráfego não é permitido.

• Negociar segurança. Os pontos de extremidade devem concordar e, em seguida, usar um método seguro de comunicação. Se eles não puderem concordar quanto a um método, a comunicação não ocorrerá. Se a negociação falhar, é possível especificar se será permitida a comunicação não segura ou se toda comunicação deverá ser bloqueada.

• Uma regra associa um filtro a uma ação de filtro.

• Uma diretiva espelhada é aquela que aplica regras a todos os pacotes com o inverso exato dos endereços IP de origem e de destino especificados. Uma diretiva espelhada é criada neste módulo.

Início da página
Criar um filtro IP
• Para criar um novo filtro IP no computador do servidor de banco de dados

1.
Faça logon no servidor de banco de dados como administrador.

2.
Inicie o snap-in MMC (Console de Gerenciamento Microsoft) da Diretiva de Segurança Local a partir do grupo de programas Ferramentas Administrativas.

3.
No painel à esquerda, clique com o botão direito do mouse em Diretivas de Segurança IP na Máquina Local e clique em Gerenciar listas de filtros IP e ações de filtro.
Você verá que duas listas de filtros já estão definidas para todo o tráfego ICMP e todo o tráfego IP.

4.
Clique em Adicionar.

5.
Na caixa de diálogo Lista de Filtros IP, digite Porta SQL no campo Nome.

6.
Clique em Adicionar e clique em Avançar para sair da caixa de diálogo de boas-vindas do Assistente de Filtro IP.

7.
Na caixa de diálogo Origem do Tráfego IP, marque Um Endereço IP Específico na lista suspensa Endereço de origem e digite o endereço IP do computador do servidor de aplicativos.

8.
Clique em Avançar.

9.
Na caixa de diálogo Destino do Tráfego IP, marque Um Endereço IP Específico na lista suspensa Endereço de destino e digite o endereço IP do computador do servidor de banco de dados.

10.
Clique em Avançar.

11.
Na caixa de diálogo Tipo de Protocolo IP, marque TCP como o tipo do protocolo e clique em Avançar.

12.
Na caixa de diálogo Porta do Protocolo IP, marque De qualquer porta e, em seguida, Para esta porta. Digite 1433 como o número da porta.

13.
Clique em Avançar e, em seguida, em Concluir para fechar o assistente.

14.
Clique em Fechar para fechar a caixa de diálogo Lista de Filtros IP.

Início da página

Criar ações de filtro

Este procedimento cria duas ações de filtro. A primeira será usada para bloquear todas as comunicações de computadores especificados e a segunda para aplicar o uso de criptografia entre computadores do servidor de aplicativos e do servidor de banco de dados.

• Para criar ações de filtro

1. Clique na guia Gerenciar Ações de Filtro.

Observe que já estão estabelecidas várias ações predefinidas.

2. Clique em Adicionar para criar uma nova ação de filtro.

Nas próximas etapas, você criará uma ação de bloqueio que poderá ser usada para bloquear todas as comunicações dos computadores selecionados.

3. Clique em Avançar para ir à caixa de diálogo inicial do Assistente de Ação de Filtro.

4. No campo Nome, digite Bloquear e clique em Avançar.

5. Na caixa de diálogo Opções Gerais da Ação de Filtro, marque Bloquear e clique em Avançar.

6. Clique em Concluir para fechar o assistente.

7. Clique em Adicionar para reiniciar o Assistente da Ação de Filtro.

Nas próximas etapas, você criará uma ação de filtro para forçar o uso de criptografia entre computadores do servidor de aplicativos e do servidor de banco de dados.

8. Clique em Avançar para ir para a caixa de diálogo inicial do Assistente de Ação de Filtro.

9. No campo Nome, digite Requer Alta Segurança e clique em Avançar.

10. Marque Negociar segurança e clique em Avançar.

11. Marque Não se comunicar com computadores que não dêem suporte para segurança IP e clique em Avançar.

12.

Marque Personalizado e clique em Configurações.

13.
Verifique se a caixa de seleção Integridade e criptografia de dados (ESP) está marcada.

14.
Marque SHA1 na lista suspensa Algoritmo de integridade.

15.
Marque 3DES na lista suspensa Algoritmo de criptografia.

16.
Marque as duas caixas de seleção no grupo Configurações de Chave de Sessão para gerar uma nova chave a cada 100.000 Kb e 3.600 segundos respectivamente.

17.
Clique em OK para fechar a caixa de diálogo Configurações Personalizadas do Método de Segurança e clique em Avançar.

18.
Marque a caixa de seleção Editar Propriedades e clique em Concluir.

19.
Desmarque a caixa de seleção Aceitar comunicação não protegida, mas sempre responder usando o IPSec.

20.
Marque a caixa de seleção Sigilo Total na Transferência de Chave da Sessão e clique em OK.

21.
Clique em Fechar para fechar a caixa de diálogo Gerenciar listas de filtros IP e ações de filtro.

Início da página

Criar regras

Este procedimento cria duas novas regras que serão usadas para associar o filtro criado no primeiro procedimento às duas ações de filtro criadas no procedimento anterior.

• Para criar regras

1.
No painel à esquerda, clique com o botão direito do mouse em Diretivas de Segurança IP na Máquina Local e clique em Criar Diretiva de Segurança IP.

2.
Clique em Avançar para ir para a caixa de diálogo inicial do Assistente de Diretiva de Segurança IP.

3.
No campo Nome, digite Proteger SQL e clique em Avançar.

4.
Desmarque a caixa de seleção Ativar a regra de resposta padrão e clique em Avançar.

5.
Deixe a caixa de seleção Editar propriedades marcada e clique em Concluir.

6.
Clique em Adicionar para iniciar o Assistente de Regra de Segurança.

7.
Clique em Avançar para sair da caixa de diálogo inicial do Assistente de Regra de Segurança.

8.
Clique em Esta regra não especifica um encapsulamento e clique em Avançar.

9.
Clique em Todas as conexões de rede e clique em Avançar.

10.
Clique em Usar esta seqüência para proteger a troca de chaves (chave pré-compartilhada).

11.
Digite MySecret como uma chave "secreta" na caixa de texto.

Observação: Esta chave deve ser a mesma para os dois computadores para que eles se comuniquem com êxito. Você deve usar um número aleatório longo, mas para este módulo, "MySecret" é suficiente.

12.
Clique em Avançar.

13.
Marque a opção Porta SQL.

Observação: É necessário clicar no círculo (botão de opção) e não no texto da opção a ser selecionada.

14.
Clique em Avançar.

15.
Marque a opção Exigir Segurança e clique em Avançar.

16.

Clique em Concluir para retornar à caixa de diálogo Proteger Propriedades do SQL.

17.
Clique em Adicionar para reiniciar o Assistente de Regra de Segurança e clique em Avançar para sair da caixa de diálogo inicial.

18.
Clique em Esta regra não especifica um encapsulamento e clique em Avançar.

19.
Clique em Todas as conexões de rede e clique em Avançar.

20.
Na caixa de diálogo Método de Autenticação, deixe a opção Padrão do Windows 2000 (protocolo V5 Kerberos) marcada e clique em Avançar.

Observação: Esta regra especificará a ação de filtro Bloquear, então nenhuma autenticação será necessária.

21.
Na caixa de diálogo Lista de Filtros IP, clique em Todo Tráfego IP e clique em Avançar.

22.
Na caixa de diálogo Ação de Filtro, marque a opção Bloquear e clique em Avançar.

23.
Clique em Concluir.

24.
Clique em Fechar para fechar a caixa de diálogo Propriedades de Proteger SQL.

Início da página

Exportar a diretiva IPSec para o computador remoto

A diretiva IPSec criada no servidor de banco de dados deve, agora, ser exportada e copiada para o computador do servidor de aplicativos.

• Para exportar a diretiva IPSec para o computador do servidor de aplicativos

1.
No painel à esquerda, clique com o botão direito do mouse no nó Diretivas de Segurança IP na Máquina Local, aponte para Todas as Tarefas e clique em Exportar Diretivas.

2.
No campo Nome, digite Proteger SQL e clique em Salvar para exportar o arquivo para o disco rígido local.

3.
Copie o arquivo .ipsec para o servidor de aplicativos ou disponibilize-o usando um compartilhamento de arquivo.

Importante: Como o arquivo exportado da diretiva contém uma chave pré-compartilhada em texto não criptografado, o arquivo deve ser protegido apropriadamente. Ele não deve ser armazenado no disco rígido de nenhum computador.

4.
Faça logon no servidor de aplicativos como administrador e inicie o snap-in MMC da Diretiva de Segurança Local.

5.
Selecione e clique com o botão direito do mouse em Diretivas de Segurança IP na Máquina Local, aponte para Todas as Tarefas e clique em Importar Diretivas.

6.
Procure o arquivo .ipsec exportado anteriormente e clique em Abrir para importar a diretiva.

Início da página

Atribuir diretivas

Uma diretiva IPSec deve ser atribuída antes de se tornar ativa. Observe que apenas uma diretiva de cada vez pode estar ativa em um computador específico.

• Para atribuir a diretiva Proteger SQL nos computadores do servidor de aplicativos e do servidor de banco de dados

1.
No computador do servidor de aplicativos, clique com o botão direito do mouse na diretiva Proteger SQL importada recentemente e clique em Atribuir.

2.
Repita a etapa anterior no computador do servidor de banco de dados.
A diretiva espelhada está, agora, atribuída nos dois computadores.

As diretivas asseguram que apenas o servidor de aplicativos possa se comunicar com o servidor de banco de dados. Além disso, apenas conexões TCP usando a porta 1433 são permitidas e todo o tráfego transmitido entre os dois computadores é criptografado.

Início da página

Verificar o funcionamento

Este procedimento usa o Monitor de Rede para verificar se os dados transmitidos entre o servidor de aplicativos e o servidor de banco de dados estão criptografados.

• Para verificar o funcionamento

1.
No computador do servidor de aplicativos, use o Visual Studio .NET para criar um novo aplicativo de console C# chamado SQLIPSecClient.

2.
Copie o código a seguir para o arquivo class1.cs substituindo todo o código existente.

Observação: Substitua o endereço IP na seqüência de conexões pelo endereço IP do servidor de banco de dados.

```
using System;
using System.Data;
using System.Data.SqlClient;
namespace SQLIPSecClient
{
 class Class1
 {
  [STAThread]
  static void Main(string[] args)
  {
   // Replace the IP address in the following connection string with
   the IP
   // address of your database server
   SqlConnection conn = new SqlConnection(
    "server=192.168.12.11;database=NorthWind;Integrated Security=
    'SSPI'");
   SqlCommand cmd = new SqlCommand(
                    "SELECT ProductID, ProductName FROM
                    Products");
   try
   {
    conn.Open();
    cmd.Connection = conn;
    SqlDataReader reader = cmd.ExecuteReader();
    while (reader.Read())
    {
     Console.WriteLine("{0} {1}",
            reader.GetInt32(0).ToString(),
            reader.GetString(1) );
    }
    reader.Close();
   }
   catch( Exception ex)
   {
   }
   finally
   {
    conn.Close();
   }
```

```
    }
  }
}
```

3.
No menu Build, clique em Build Solution.

4.
Para que a autenticação do Windows seja bem-sucedida entre os dois computadores, é necessário duplicar a conta com a qual você fez logon interativamente no computador do aplicativo, no computador do servidor de banco de dados. Verifique se o nome do usuário e a senha correspondem.

Também é necessário usar o SQL Server Enterprise Manager para criar um logon para a conta criada recentemente e adicionar um novo usuário para este logon ao banco de dados Northwind.

5.
Cancele temporariamente a atribuição da diretiva IPSec do SQL Seguro em ambos os computadores:

1.
Inicie a opção Configurações Locais de Segurança no computador do servidor de aplicativos.

2.
Clique em Diretivas de Segurança IP na Máquina Local.

3.
No painel à direita, clique com o botão direito do mouse em Proteger SQL e clique em Cancelar atribuição.

4.
Repita as Etapas a – c no computador do servidor de banco de dados.

6.
No computador do servidor de banco de dados, clique em Monitor de Rede no grupo de programas Ferramentas Administrativas.

Observação: Uma versão limitada do Monitor de Rede está disponível com o Windows 2000 Server. Uma versão completa está disponível com o Microsoft SMS.

Se o Monitor de Rede não estiver instalado, vá para Adicionar ou Remover Programas no Painel de controle, clique em Adicionar ou Remover Componentes do Windows, marque Ferramentas de Gerenciamento e Monitoramento na lista Componentes do Windows, clique em Detalhes e marque Ferramentas de Monitoria de Rede. Clique em OK e, em seguida, em Avançar para instalar a versão limitada do Monitor de Rede. Um CD do Windows 2000 Server poderá ser solicitado.

7.
No menu Capturar, clique em Filtro para criar um novo filtro configurado para exibir o tráfego de rede TCP/IP transmitido entre o servidor de aplicativos e o servidor de banco de dados.

8.
Clique no botão Iniciar Captura.

9.
Retorne ao computador do servidor de aplicativos e execute o aplicativo do console de teste. Uma lista de produtos do banco de dados Northwind deve ser exibida na janela do console.

10.
Retorne ao servidor de banco de dados e clique no botão Parar e Visualizar a Captura no Monitor de Rede.

11.
Clique duas vezes no primeiro quadro capturado para exibir os dados capturados.

12.
Role pelos quadros capturados. Você deve ver a instrução SELECT em texto não criptografado seguida por uma lista de produtos recuperados do banco de dados.

13.
Atribua a diretiva IPSec de Proteger SQL a ambos os computadores:

1.
Inicie a opção Configurações Locais de Segurança no computador do servidor de aplicativos.

2.
Clique em Diretivas de Segurança IP na Máquina Local.

3.
No painel à direita, clique com o botão direito do mouse em Proteger SQL e clique em Atribuir.

4.
Repita as Etapas a – c no computador do servidor de banco de dados.

14.
No Monitor de Rede, feche a janela de captura.

15.
Clique no botão Iniciar Captura e, em seguida, clique em Não na caixa de mensagem Salvar Arquivo.

16.
Retorne ao computador do servidor de aplicativo e execute o aplicativo do console de teste mais uma vez.

17.
Retorne ao computador de servidor de banco de dados e clique em Parar e Visualizar a Captura no Monitor de Rede.

18.
Confirme se os dados agora estão ininteligíveis (porque estão criptografados).

19.
Feche o Monitor de Rede.

Início da página

Recursos adicionais

Para obter mais informações sobre o IPSec, consulte "IP Security and Filtering" no TechNet em:http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/Windows/XP/all/reskit/en-us/prcc_tcp_erqb.asp.

Para obter mais informações sobre o Monitor de Rede, consulte a seção "Network Monitor" do Microsoft Platform SDK no MSDN em: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netmon/netmon/network_monitor.asp.

****

O Protocolo de Segurança IP (IP Security Protocol, mais conhecido pela sua sigla, IPSec) visa a ser o método padrão para o fornecimento de privacidade, integridade e autenticidade das informações transferidas através de redes IP.

A Internet tem mudado a maneira como negócios são feitos, mas até mesmo o rápido crescimento da Internet tem sido atingido pela inerente falta de segurança, por ser uma rede pública. Algumas das principais ameaças a que ela está sujeita são:

perda de privacidade na troca de dados: os dados podem ser vistos por terceiros;
perda da integridade dos dados: em algum local no caminho entre a origem e o destino, os dados podem ser modificados por terceiros;
falsificação de identidade: a origem dos dados pode ser forjada, fazendo com que pessoas assumam o papel de outras;
ataques de negação de serviço (Denial of Service, DoS): muitas vezes feitos através da união de diversas máquinas, que fazem requisições excessivas de um determinado serviço, tornando-o indisponível aos outros usuários.
O IPSec tem como objetivo tratar de todas estas ameaças na própria camada de rede (camada Internet do modelo TCP/IP), para que não sejam necessárias modificações nos

terminais (host) ou aplicativos. Um dos meios para se conseguir isto, por exemplo, é através da implementação de IPSec nos roteadores de borda, por onde passa todo o tráfego externo de uma empresa/instituição; desta forma, a segurança atuaria de forma transparente para o usuário.

O IPSec é voltado para a encriptação de camada IP, e seu padrão define alguns formatos de pacote novos: Autenticação de Cabeçalho (Authentication Header, AH) para fornecer a integridade dos pacotes entre origem e destino, e o Encapsulamento Seguro da Informação (Encapsulating Security Payload, ESP). O gerenciamento de chaves, associações de segurança (Security Associations, SA) e os parâmetros para a comunicação IPSec entre dois dispositivos são negociados através do IKE (Inernet Key Exchange, anteriormente chamado de Internet Security Association Key Management Protocol ou ISAKMP/Oakley). O IKE utiliza Certificados Digitais (que garantem a identidade de uma pessoa, evitando a falsificação de identidades) para autenticação de dispositivos, permitindo a criação de grandes redes seguras. Sem o suporte dos Certificados Digitais, as soluções IPSec não seriam escaláveis para a Internet. Todos estes elementos serão explicados ao longo do texto. Atualmente, o protocolo já é encontrado em roteadores, firewalls e em sistemas operacionais Windows e UNIX.

Começaremos com a motivação para o desenvolvimento do IPSec, para depois entrar em detalhes de seus mecanismos de segurança.

1. Fundamentos

Uma rede, para ser considerada segura, deve basear-se numa forte política de segurança, que defina a liberdade de acesso à informação para cada usuário, assim como a localização dos mecanismos de segurança na rede. Há várias soluções para se construir uma infra-estrutura segura para a Internet, Extranets, Intranets e redes para acesso remoto, que oferecem autenticação do usuário, acompanhamento de suas ações e privacidade dos dados. Privacidade, integridade e autenticidade são conseguidas através encriptação na camada de rede, certificação digital e autenticação de dispositivos, palavras-chave quando falamos de IPSec, ou mais genericamente, de mecanismos de segurança em redes públicas.

2. Mudança na comunicação das empresas

A Internet está modificando rapidamente a forma como são feitos os negócios. Ao mesmo tempo em que a velocidade de comunicação aumenta, seu custo diminui. Há um grande espaço para o aumento de produtividade, aproveitando esta situação, através das seguintes topologias, também mostradas na figura 1:

- Extranet: as companhias podem facilmente estabelecer enlaces com seus fornecedores, clientes ou parceiros. Até pouco tempo atrás, isto era feito através de linhas privadas (dedicadas) ou ligações telefônicas (de baixa velocidade). A Internet permite uma comunicação instantânea, de alta velocidade e sempre disponível.

- Intranet: a maior parte das empresas utiliza WANs (Wide-Area Networks) para conectar as redes de sua sede e filiais. Esta solução é cara, e apesar de seu custo ter caído nos últimos anos, ainda há uma grande margem de redução de custos pelo uso da Internet.

- Usuários remotos: a Internet fornece uma alternativa de baixo custo para a conexão destes usuários às redes corporativas. Em vez de a empresa ter que manter bancos de modens e arcar com os custos das ligações telefônicas (muitas vezes interurbanas ou até internacionais), elas podem permitir que seus usuários acessem sua rede através da Internet. Com uma ligação local a um provedor de acesso à Internet (Internet Service Provider, ISP), um usuário pode ter acesso à rede corporativa.

Compartilhamento da rede interna de uma empresa

Estas e outras aplicações da Internet estão mudando a forma com as empresas se comunicam. A Internet fornece uma infra-estrutura pública de comunicações que faz com que tudo isso se torne possível. No entanto, há fraquezas geradas por esta infra-estrutura compartilhada: segurança, qualidade de serviço e confiabilidade. Neste momento aparece o IPSec como peça-chave no fornecimento de segurança nas comunicações de rede.

3. Qual a função do IPSec?

Como visto nos itens anteriores, a Internet apresenta grandes vantagens, mas também alguns riscos. Sem os mecanismos adequados de controle, os dados estão sujeitos a diversos tipos de ataques. Estes ataques são:

3.1 Perda de privacidade

O atacante pode observar dados confidenciais enquanto eles atravessam a Internet. Esta é uma das principais ameaças ao comércio pela Internet hoje. Sem encriptação, todas as mensagens enviadas podem ser lidas por pessoas não autorizadas, como mostrado na figura 2. Estas técnicas são chamadas de “sniffing”, e os programas utilizados para isso de “sniffers”; até usuários com pouco conhecimento já são capazes de bisbilhotar o conteúdo que trafega na rede.

Pessoas não autorizadas podem bisbilhotar o conteúdo de mensagens

3.2 Perda de integridade dos dados

Mesmo que os dados não sejam confidenciais, também devemos nos preocupar com a integridade deles. Por exemplo, uma pessoa pode não se importar que alguém veja suas mensagens do dia a dia, mas certamente se preocupará se os dados puderem ser alterados; uma ordem para a promoção de um funcionário geralmente não precisa ser secreta, mas quem a enviou estará realmente preocupado ser ela puder ser trocada por uma outra indicando uma demissão. O mesmo vale para mensagens secretas, já que o emissor deseja que seus bits não sejam alterados no caminho, o que poderia causar uma alteração no significado da mesma. Mecanismos de integridade dos dados garantem que a mensagem chega ao destino como saiu da origem.

3.3 Falsificação de identidade (Identity spoofing)

Além da proteção do dado, também devemos ter a garantia de que uma pessoa é realmente quem ela diz ser. Como mostrado na figura 3, um atacante pode tentar se passar por uma outra pessoa, para ter acesso a informações confidenciais. Muitos sistemas ainda confiam no endereço IP para identificar um usuário de forma única; no entanto, este sistema já é facilmente enganado.

Uma pessoa se passa por diretor da empresa, obtendo acesso à informações confidenciais

3.4 Negação de serviço (DoS)

Ao migrar para a Internet, uma organização deve tomar as medidas necessárias para garantir que seus sistemas estarão disponíveis aos usuários. Aproveitando brechas de segurança, atacantes fazem com que computadores da empresa sejam levados ao limite, até o ponto em que parem de oferecer o serviço que deveriam. Mesmo que o atacante não consiga acesso a informações privilegiadas, ele sem dúvida causará danos à empresa.

4. IPSec: Visão

4.1 Abordando o problema

Não há respostas simples para a segurança na Internet. Todas as soluções necessitam de muitos elementos, incluindo uma boa política de segurança, padrões que definam o que deve ser protegido, um conjunto de procedimentos que detalham como implementar as políticas e um conjunto de tecnologias que forneçam a proteção.

Confidencialidade, integridade e autenticidade são os serviços-chave para a proteção contra as ameaças descritas na seção anterior. Com a encriptação garantimos a privacidade dos dados, com uma forte autenticação feita na camada de rede podemos garantir a origem dos dados.

4.2 O que é IPSec

IPSec não é o mecanismo de encriptação ou autenticação, mas sim o que vem gerenciar estes. Em poucas palavras, é um framework (um conjunto de diversas ferramentas, compondo um sistema) de padrões abertos que visa a garantir uma comunicação segura em redes IP. Baseado em padrões desenvolvidos pela IETF (Internet Engineering Task Force, organização que desenvolve os padrões da Internet), o IPSec busca garantir confidencialidade, integridade e autenticidade nas comunicações de dados em uma rede IP pública.

Encriptação e autenticação podem ser implementadas tanto na camada de rede, quanto na de enlace ou aplicação. Antes do IPSec, as redes adotavam soluções parciais, que resolviam apenas parte dos problemas. Por exemplo, a utilização de SSL (Secure Sockets Layer, que simulam túneis seguros entre aplicativos) fornece encriptação no nível de aplicação, muito usado em navegadores de Internet, por exemplo, para acesso à serviços bancários. Uma das deficiências da encriptação no nível de aplicação é que ela protege somente os dados enviados pela aplicação que a está usando, mas não de todas as outras. Cada sistema ou aplicativo deve estar adaptado a SSL, para que uma segurança geral possa ser garantida. Atualmente, a maior parte dos aplicativos não utiliza SSL.

Já em instituições militares, o que vem sendo usado há anos é a encriptação no nível do enlace de dados. Neste esquema, todas as comunicações estarão protegidas por dispositivos de encriptação colocados em cada fim do enlace. Apesar de oferecer excelente cobertura, este tipo de encriptação necessita de um par de dispositivos de encriptação a cada enlace, o que pode ser inviável; também não é adequado para a Internet, já que apenas os enlaces dentro de um sistema autônomo estarão ao alcance das empresas/instituições.

O IPSec implementa encriptação e autenticação na camada de rede, fornecendo uma solução de segurança fim-a-fim, ao contrário da anterior (enlace), que é ponto-a-ponto. O IPSec pode ser implementado nos roteadores ou no sistema operacional dos

terminais, assim os aplicativos não precisam de alterações para poder utilizar comunicações seguras. Como os pacotes encriptados têm o mesmo formato de pacotes IP comuns, eles podem ser roteados sem problemas em qualquer rede IP, e sem qualquer alteração nos equipamentos de rede intermediários. Os únicos dispositivos de rede que precisam ser alterados são os do início e fim das comunicações IPSec, reduzindo assim os custos de implementação e gerenciamento.

A figura 4 mostra onde a encriptação atua nas diferentes camadas.

Encriptação na camada de enlace, na de rede e na aplicação.

4.3 Tecnologias

IPSec combina diversas tecnologias diferentes de segurança em um sistema completo que provê confidencialidade, integridade e autenticidade, empregando atualmente:

mecanismo de troca de chaves de Diffie-Hellman;
criptografia de chave pública para assinar as trocas de chave de Diffie-Hellman, garantindo assim a identidade das duas partes e evitando ataques do tipo man-in-the-middle (onde o atacante se faz passar pela outra parte em cada um dos sentidos da comunicação);
algoritmos de encriptação para grandes volumes de dados, como o DES (Data Encryption Standard);
algoritmos para cálculo de hash (resto de uma divisão, de tamanho fixo) com utilização de chaves, com o HMAC, combinado com os algoritmos de hash tradicionais como o MD5 ou SHA, autenticando os pacotes;
certificados digitais assinados por uma autoridade certificadora, que agem como identidades digitais.

4.4 Detalhes do IPSec

Na realidade, além das tecnologias mencionadas no item anterior, o IPSec também se refere a diversos outros protocolos (mencionados nas RFCs 2401-2411 e 2451) para proteger datagramas IP. Estes padrões são:

Protocolo de Segurança IP, que define que informações adicionar ao pacote IP para permitir o controle da confidencialidade, autenticidade e integridade, assim como a forma em que os dados devem ser encriptados;
Internet Key Exchange (IKE), que negocia Associações de Segurança (Security Association, SA) entre duas entidades e realiza a troca de chaves. O uso da IKE não é

obrigatório, mas a configuração manual de Associações de Segurança é difícil e trabalhosa, torna-se impossível para comunicações seguras em larga escala.

Pacotes IPSec

É definido um novo conjunto de cabeçalhos a serem adicionados em datagramas IP. Os novos cabeçalhos são colocados após o cabeçalho IP e antes do cabeçalho da camada superior (como o dos protocolos de transporte TCP ou UDP). Estes novos cabeçalhos é que dão as informações para proteção das informações (payload) do pacote IP:

Authentication Header (AH): este cabeçalho, ao ser adicionado a um datagrama IP, garante a integridade e autenticidade dos dados, incluindo os campos do cabeçalho original que não são alterados entre a origem e o destino; no entanto, não fornece confidencialidade. É utilizada uma função hash com chave, ao invés de assinatura digital, pois o mecanismo de assinatura digital é bem mais lento e poderia reduzir a capacidade da rede.
Encapsulating Security Payload (ESP): este cabeçalho protege a confidencialidade, integridade e autenticidade da informação. Se o ESP for usado para validar a integridade, ele não inclui os campos invariantes do cabeçalho IP.

AH e ESP podem ser usados separadamente ou em conjunto, mas para a maioria das aplicações apenas um deles é suficiente. Para os dois cabçalhos, o IPSec não especifica quais algoritmos de segurança devem ser utilizados, mas dá uma relação dos possíveis algoritmos, todos padronizados e bastante difundidos. Inicialmente, quase todas as implementações trabalham com MD5 (da RSA Data Security) e o Secure Hash Algorithm (SHA, do governo dos EUA) para integridade e autenticação. O DES é o algoritmo mais comumente usado para a encriptação dos dados, apesar de muitos outros estarem disponíveis, de acordo com as RFCs, como o IDEA, Blowfish e o RC4.

Modos de operação

O IPSec fornece dois modos de operação, como mostrado nas figuras 5 e 6.

No modo de transporte, somente a informação (payload) é encriptada, enquanto o cabeçalho IP original não é alterado. Este modo tem a vantagem de adicionar apenas alguns octetos a cada pacote, deixando que dispositivos da rede pública vejam a origem e o destino do pacote, o que permite processamentos especiais (como de QoS) baseados no cabeçalho do pacote IP. No entanto, o cabeçalho da camada 4 (transporte) estará encriptado, limitando a análise do pacote. Passando o cabeçalho sem segurança, o modo de transporte permite que um atacante faça algumas análises de tráfego, mesmo que ele não consiga decifrar o conteúdo das mensagens.

No modo de tunelamento, todo o datagrama IP original é encriptado e passa a ser o payload de um novo pacote IP. Este modo permite que um dispositivo de rede, como um roteador, aja como um Proxy IPSec (o dispositivo realiza a encriptação em nome dos terminais). O roteador de origem encripta os pacotes e os envia ao longo do túnel IPSec; o roteador de destino decripta o datagrama IP original e o envia ao sistema de destino. A grande vantagem do modo de tunelamento é que os sistemas finais não

precisam ser modificados para aproveitarem os benefícios da segurança IP; além disto, esse modo também protege contra a análise de tráfego, já que o atacante só poderá determinar o ponto de início e de fim dos túneis, e não a origem e o destino reais.

Cabeçalho genérico para o modo de transporte

Exemplo de um cabeçalho do modo túnel

Como definido pelo IETF, o modo de transporte só pode ser utilizado quanto tanto a origem quanto o destino “entendem” IPSec. Na maior parte dos casos, é mais fácil trabalhar com o modo de tunelamento, o que permite a implementação do IPSec sem que sistemas operacionais ou aplicativos nos terminais e servidores precisem ser alterados.

Associações de Segurança (Security Association, SA)

Como visto, o IPSec fornece diversas opções para executar a encriptação e autenticação na camada de rede. Quando dois nós desejam se comunicar com segurança, eles devem determinar quais algoritmos serão usados (se DES ou IDEA, MD5 ou SHA). Após escolher os algoritmos, as chaves de sessão devem ser trocadas. Como vemos, há uma certa quantidade de informações que precisam ser negociadas. A Associação de Segurança é o método utilizado pelo IPSec para lidar com todos estes detalhes de uma determinada sessão de comunicação. Uma SA representa o relacionamento entre duas ou mais entidades que descreve como estas utilizarão os serviços de segurança para se comunicarem. As SAs também podem ser utilizadas por outras entidades, como IKEs, para descrever os parâmetros de segurança entre dois dispositivos IKE.

As SAs são unidirecionais, o que significa que para cada par de sistemas que se comunicam, devemos ter pelo menos duas conexões seguras, uma de A para B e outra de B para A. As SAs são identificadas de forma única pela associação entre um número aleatório chamado SPI (Security Parameter Index) e o endereço IP de destino. Quando um sistema envia um pacote que requer proteção IPSec, ele olha as SAs armazenadas em seus banco de dados, processa as informações, e adiciona o SPI da SA no cabeçalho IPSec. Quando o destino IPSec recebe o pacote, ele procura a SA em seus banco de dados de acordo com o endereço de destino a de SPI, e então processa o pacote da forma necessária. As SAs são simplesmente o relatório das políticas de segurança que serão usadas entre dois dispositivos.

Protocolo de gerenciamento de chaves (Internet Key Management Protocol, IKMP)

O IPSec assume que as SAs já existem para ser utilizado, mas não especifica como elas serão criadas. O IETF decidiu dividir o processo em duas partes: o IPSec fornece o processamento dos pacotes, enquanto o IKMP negocia as associações de segurança. Após analisar as alternativas disponíveis, o IETF escolheu o IKE como o método padrão para configuração das SAs para o IPSec.

O IKE cria um túnel seguro e autenticado entre duas entidades, para depois negociar SAs para o IPSec. Este processo requer que duas entidades se autentiquem entre si e estabeleçam chaves compartilhadas.

Autenticação

As duas partes devem ser autenticadas entre si. O IKE é bastante flexível e suporta diversos tipos de autenticação. As duas entidades devem escolher o protocolo de autenticação que será utilizado através de negociação. Neste momento, os seguintes mecanismos são implementados:

chaves compartilhadas já existentes: a mesma chave é instalada em cada entidade. Os dois IKEs autenticam-se enviando ao outro um hash com chave de um conjunto de dados que inclui a chave compartilhada existente. Se o receptor conseguir criar o mesmo hash usando sua chave já existente, ele sabe que os dois IKE possuem a mesma chave, autenticando assim a outra parte;
criptografia de chave pública: cada parte gera um número aleatório, e encripta este número com a chave pública da outra parte. A capacidade de cada parte computar um hash com chave contendo o número aleatório da outra parte, decriptado com a chave privada local, assim como outras informações disponíveis pública e privadamente, autentica as duas partes entre si. Este método permite que as transações sejam negadas, ou seja, uma das partes da troca pode, plausivelmente, negar que tenha feito parte da troca. Somente o algoritmo de chave pública RSA é suportado atualmente.
assinatura digital: cada dispositivo assina digitalmente um conjunto de dados e o envia para a outra parte. Este método a similar ao anterior, mas ele não permite que uma entidade repudie a participação na troca. Tanto o algoritmo de chave pública RSA quanto o DSS (Digital Signature Standard) são suportados atualmente.

Tanto a assinatura digital quanto a criptografia de chave pública necessitam o uso de certificados digitais para validar o mapeamento entre a chave pública e a chave privada. O IKE permite que certificados sejam acessados independentemente (por exemplo, através do DNSSEC), ou que dois dispositivos troquem explicitamente os certificados como parte do IKE.

Troca de chaves

As duas partes devem possuir uma chave de sessão compartilhada para poderem encriptar o túnel IKE. O protocolo de Diffie-Hellman é usado para que as entidades concordem em uma chave de sessão. A troca é autenticada como descrito acima para prevenir contra ataques do tipo “man-in-the-middle”.

Utilizando o IKE com o IPSec

A autenticação e a troca de chaves criam a SA entre os IKEs, um túnel seguro entre os dois dispositivos. Um dos lados do túnel oferece um conjunto de algoritmos, e o outro deve aceitar uma das ofertas ou rejeitar a conexão. Quando os dois lados concordam com os algoritmos que serão utilizados, eles devem produzir as chaves que serão utilizadas pelo IPSec no AH ou ESP, ou os dois. A chave compartilhada pelo IPSec é diferente da compartilhada pelos IKEs; ela pode ser obtida pelo método de Diffie-Hellman novamente, para garantir o sigilo, ou atualizando a criada pela troca original para gerar a SA IKE, fazendo o hash com outro número aleatório. O primeiro método, apesar de fornecer maior segurança, é mais lento. Após esse passos, a SA IPSec é estabelecida.

Como mostrado na figura 8, o IPSec usa o IKE para iniciar uma SA. O primeiro pacote de A para B que deve ser encriptado inicia o processo. O processo IKE monta um túnel seguro entre B e A, onde a SA IPSec será negociada. A então pode usar esta SA para enviar dados de forma segura para B.

Uso do IKE pelo IPSec

Juntando todos os passos descritos anteriormente, temos o seguinte exemplo. B quer iniciar uma comunicação segura com A, enviando o primeiro pacote de dados. Quando o roteador de B recebe este pacote, ele olha suas políticas de segurança e vê este pacote deve ser encriptado; a política de segurança, que deve ser configurada anteriormente, também diz que o outro ponto do túnel IPSec será o roteador de A. O roteador de B procura se já há alguma SA IPSec com o roteador. Se ainda não existe, ele pede uma para o IKE; se os dois roteadores já compartilham uma SA IKE, a SA IPSec pode ser rapidamente gerada. Se ainda não compartilham uma SA IKE, ela deve ser criada antes que possa ser negociada uma SA IPSec. Como parte deste processo, os dois roteadores trocam certificados digitais, que estão assinados por alguma autoridade certificadora que os roteadores de A e B confiam. Quando a sessão IKE é ativada, os dois roteadores podem então negociar a SA IPSec; quando esta última é ativada, significa que os dois roteadores concordaram num algoritmo de encriptação (por exemplo o DES) e um de autenticação (como o MD5), e agora compartilham de uma chave de sessão. Agora o roteador de B pode encriptar o pacote IP que B que enviar a A, colocá-lo em um novo pacote IPSec enviá-lo ao roteador de A. Quando o roteador de A recebe o pacote IPSec, ele faz uma busca na SA IPSec, e então processa o pacote e envia o datagrama original para A. Note que todos os passos são feitos pelos roteadores de A e B, deixando o processo transparente aos usuários.

Na prática a política de segurança pode ser bastante flexível: os roteadores podem decidir quais pacotes devem ser encriptados ou autenticados, de acordo com alguma combinação entre os endereços de origem e destino, portas e protocolo de transporte. Cada um dos tipos de comunicação pode ser autenticado e encriptado separadamente, com chaves diferentes.

****

6.3. Instalação do IPsec

A implementação do IPsec requer a instalação do pacote RPM ipsec-tools em todas as máquinas IPsec (se usar uma configuração máquina-a-máquina) ou roteadores IPsec (se usar uma configuração rede-a-rede). O pacote RPM contém bibliotecas, daemons e arquivos de configuração essenciais para auxiliar na configuração da conexão IPsec, incluindo:

/lib/libipsec.so — biblioteca que contém a interface socket de gerenciamento da chave de confiança PF_KEY entre o kernel do Linux e a implementação do IPsec usada no Red Hat Enterprise Linux.

/sbin/setkey — manipula o gerenciamento da chave e atributos de segurança do IPsec no kernel. Este executável é controlado pelo daemon de gerenciamento da chave racoon. Para mais informações sobre o setkey, consulte a página man (8) do setkey.

/sbin/racoon — o daemon de gerenciamento da chave IKE, usado para administrar e controlar as associações de segurança e compartilhamento de chaves entre sistemas conectados pelo IPsec. Este daemon pode ser configurado editando o arquivo /etc/racoon/racoon.conf. Para mais informações sobre o racoon, consulte a página man (8) do racoon.

/etc/racoon/racoon.conf — o arquivo de configuração do daemon do racoon usado para configurar vários aspectos da conexão IPsec, incluindo métodos de autenticação e algoritmos de criptografia usados na conexão. Para uma lista completa das diretivas disponíveis, consulte a página man (5) do racoon.conf.

A configuração do IPsec no Red Hat Enterprise Linux pode ser feita pela Ferramenta de Administração de Rede ou manualmente editando os arquivos de configuração de rede e do IPsec. Para mais informaçõe sobre o uso da Ferramenta de Administração de Rede, consulte o Guia de Administração de Sistemas Red Hat Enterprise Linux.

Para conectar duas máquinas em rede através do IPsec, consulte a Seção 6.4. Para conectar uma LAN/WAN a outra através do IPsec, consulte a Seção 6.5.

****