Erstellen sicherer ASP.NET-Anwendungen

Authentifizierung, Autorisierung und sichere Kommunikation

Auf der Orientierungsseite finden Sie einen Ausgangspunkt und eine vollständige Übersicht zum *Erstellen sicherer ASP.NET-Anwendungen*.

Zusammenfassung

IPSec ist eine von Windows 2000 bereitgestellte Technologie, die es Ihnen ermöglicht, verschlüsselte Kommunikationskanäle zwischen zwei Servern einzurichten. Mit IPSec kann IP-Datenverkehr gefiltert und können Server authentifiziert werden. In dieser Vorgehensweise wird erläutert, wie IPSec für die Bereitstellung eines sicheren (verschlüsselten) Kommunikationskanals konfiguriert wird.

Vorgehensweise: Verwenden von IPSec zum Sichern der Kommunikation zwischen zwei Servern

Mit IPSec (Internet Protocol Security) können die zwischen zwei Computern, z. B. einem Anwendungsserver und einem Datenbankserver, gesendeten Daten gesichert werden. IPSec ist für Anwendungen vollkommen transparent, da Verschlüsselungs-, Integritäts- und Authentifizierungsdienste auf der Transportebene implementiert sind. Die Anwendungen kommunizieren weiterhin in normaler Weise über TCP- und UDP-Ports.

IPSec zeichnet sich durch die folgenden Merkmale aus:

- Bereitstellen der Vertraulichkeit von Nachrichten, indem alle zwischen zwei Computern gesendeten Daten verschlüsselt werden.
- Bereitstellen der Integrität von Nachrichten zwischen zwei Computern (ohne Verschlüsselung der Daten).
- Bereitstellen einer gegenseitigen Authentifizierung zwischen zwei Computern. Sie können beispielsweise einen Datenbankserver sichern, indem Sie eine Richtlinie erstellen, die Anforderungen nur von einem bestimmten Clientcomputer zulässt (z. B. einer Anwendung oder einem Webserver).
- Einschränken, welche Computer miteinander kommunizieren können. Die Kommunikation kann auch auf bestimmte IP-Protokolle und TCP/UDP-Ports beschränkt werden.

In dieser Vorgehensweise wird gezeigt, wie Sie den Kommunikationskanal zwischen einem Anwendungsserver und einen Datenbankserver sichern können, auf dem SQL Server 2000 ausgeführt wird. Hierbei verwendet der Anwendungsserver die empfohlene TCP/IP-Clientnetzwerkbibliothek für die Herstellung der Verbindung zu SQL Server sowie den standardmäßigen SQL Server-TCP-Port 1433. Die Konfiguration ist in Abbildung 1 dargestellt.

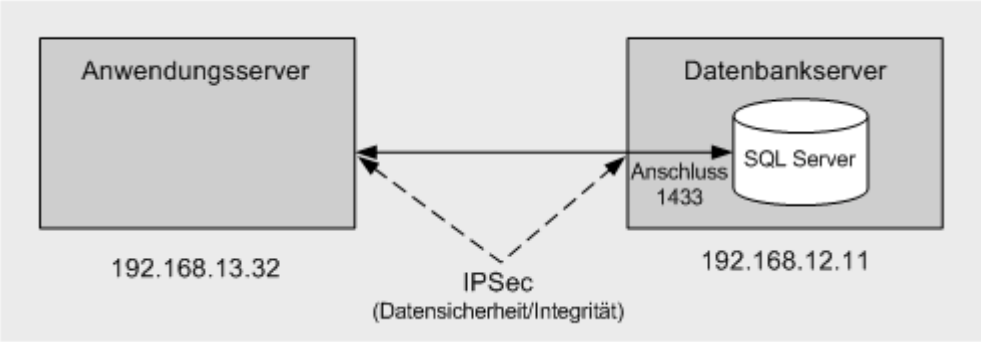

Abbildung 1

Konfiguration der in dieser Vorgehensweise beschriebenen Lösung

Nachstehend wird erläutert, wie eine einfache IPSec-Richtlinie verwendet wird, um Folgendes durchzusetzen:

- Der Anwendungsserver kann per TCP nur über Port 1433 mit SQL Server kommunizieren.
- Alle anderen IP-Pakete einschließlich ICMP (Ping) werden zurückgewiesen.
- Alle zwischen den beiden Computern gesendeten Daten werden verschlüsselt, um deren Vertraulichkeit sicherzustellen.

Die Vorteile dieses Ansatzes sind die folgenden:

- Für sämtliche zwischen den beiden Computern übertragene Daten wird Vertraulichkeit gewährleistet.
- Die Angriffsfläche von SQL Server wird wesentlich reduziert. Die einzig verbleibenden Angriffsmöglichkeiten bestehen darin, sich entweder interaktiv am Datenbankserver anzumelden oder die Kontrolle über den Anwendungsserver zu erlangen und zu versuchen, SQL Server über TCP-Port 1433 anzugreifen.
- Die IPSec-Richtlinie ist außerordentlich einfach zu definieren und zu implementieren.

Diese spezielle Richtlinie weist jedoch die folgenden Nachteile auf:

- SQL Server kann nicht mit Domänencontrollern kommunizieren, woraus sich folgende Auswirkungen ergeben:
  - Es kann keine Gruppenrichtlinie verwendet werden (bei dem Datenbankserver sollte es sich um einen eigenständigen Server handeln).
  - Die Windows-Authentifizierung zwischen Anwendungsserver und Datenbankserver setzt synchronisierte lokale Konten (mit dem gleichen Benutzernamen und Kennwort) auf beiden Computern voraus.
  - Die robusteren Methoden der Implementierung von IPSec (Windows 2000-Standard/Kerberos) können nicht verwendet werden.
- SQL Server ist nicht in der Lage, mit anderen Computern zu kommunizieren, was auch DNS-Server einschließt.
- Bei dem in dieser Vorgehensweise vorgestellten Ansatz erfolgt die Authentifizierung mithilfe von vorinstallierten Schlüsseln, was in Produktionsszenarien nicht empfehlenswert ist. Produktionssysteme sollten mit Zertifikaten oder der Windows 2000-Domänenauthentifizierung arbeiten. IPSec-Richtlinien, die mit vorinstallierten Schlüsseln arbeiten, eignen sich nur für Entwicklungs- oder Testumgebungen.
- Beide Computer müssen über statische IP-Adressen verfügen.

Hinweise

- Eine IPSec-Richtlinie setzt sich aus einer Reihe Filter, Filteraktionen und Regeln zusammen.
- Ein *Filter* besteht aus folgenden Elementen:
  - Einer Quell-IP-Adresse oder einem Adressbereich.
  - Einer Ziel-IP-Adresse oder einem Adressbereich.
  - Einem IP-Protokoll wie beispielsweise TCP, UDP oder "beliebig".
  - Quell- und Zielports (nur für TCP oder UDP).
- Filter können auch auf beiden Computern gespiegelt werden. Bei einem gespiegelten Filter wird die gleiche Regel auf dem Client- und dem Servercomputer angewendet (wobei Quell- und Zieladressen exakt umgekehrt werden).
- Eine *Filteraktion* gibt die Aktionen an, die unternommen werden sollen, wenn ein gegebener Filter aufgerufen wird. Die folgenden Aktionen stehen jeweils zur Verfügung:
  - **Zulassen –** Der Datenverkehr wird nicht gesichert; Daten können ohne Intervention gesendet und empfangen werden.
  - **Blockieren –** Der Datenverkehr wird nicht zugelassen.
  - **Sicherheit aushandeln –** Die Endpunkte müssen sich auf eine sichere Kommunikationsmethode einigen und diese dann verwenden. Wenn sie sich nicht auf eine gemeinsame Methode einigen können, findet keine Kommunikation statt. Für den Fall eines Fehlschlags der Sicherheitsaushandlung können Sie festlegen, ob eine unsichere Kommunikation erlaubt oder die gesamte Kommunikation blockiert werden soll.
- Über eine *Regel* wird ein Filter mit einer Filteraktion verbunden.
- Eine *gespiegelte Richtlinie* ist eine Richtlinie, bei der die Regeln auf alle Pakete angewendet werden, wobei die angegebenen Quell- und Ziel-IP-Adressen exakt umgekehrt werden. In dieser Vorgehensweise wird eine gespiegelte Richtlinie erstellt.

Anforderungen

Im Folgenden finden Sie eine Liste der empfohlenen Hardware und Software und eine Beschreibung der Netzwerkinfrastruktur, der Fähigkeiten und Kenntnisse sowie der Service Packs, die Sie benötigen.

- Zwei Computer mit Microsoft® Windows® 2000 Server als Betriebssystem
  Sie müssen die IP-Adressen dieser Computer kennen.
- Microsoft® SQL Server™ 2000 auf dem Datenbankservercomputer

Zusammenfassung

Diese Vorgehensweise enthält folgende Verfahren:

1. Erstellen eines IP-Filters
2. Erstellen von Filteraktionen
3. Erstellen von Regeln
4. Exportieren der IPSec-Richtlinie auf den Remotecomputer
5. Zuweisen von Richtlinien
6. Überprüfen der Funktionstüchtigkeit

1. Erstellen eines IP-Filters

▶ **So erstellen Sie einen IP-Filter auf dem Datenbankservercomputer**

1. Melden Sie sich als Administrator am Datenbankserver an.
2. Starten Sie das MMC-Snap-In Lokale Sicherheitsrichtlinie aus der Programmgruppe **Verwaltung**.
3. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf lokalem Computer**, und klicken Sie dann auf **IP-Filterlisten und Filteraktionen verwalten**.

   Wie Sie sehen, sind bereits zwei Listen für den gesamten ICMP-Verkehr und den gesamten IP-Verkehr definiert.
4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie im Dialogfeld **IP-Filterliste** den Eintrag **SQL Port** in das Feld **Name** ein.
6. Klicken Sie auf **Hinzufügen** und dann auf **Weiter**, um das Begrüßungsdialogfeld des IP-Filter-Assistenten zu schließen.
7. Wählen Sie im Dialogfeld **Quelle des IP-Verkehrs** den Eintrag **Spezielle IP-Adresse** aus dem Dropdown-Listenfeld **Quelladresse**, und geben Sie dann die IP-Adresse Ihres Anwendungsservers ein.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie im Dialogfeld **Ziel des IP-Verkehrs** den Eintrag **Spezielle IP-Adresse** aus dem Dropdown-Listenfeld **Zieladresse**, und geben Sie dann die IP-Adresse Ihres Datenbankservers ein.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie im Dialogfeld **Typ des IP-Protokolls** als Protokolltyp **TCP** aus, und klicken Sie dann auf **Weiter**.
12. Wählen Sie im Dialogfeld **Port des IP-Protokolls** zunächst die Option **Von jedem Port**, und wählen Sie dann **Zu diesem Port**. Geben Sie als Portnummer **1433** ein.
13. Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**, um den Assistenten zu schließen.
14. Klicken Sie auf **Schließen**, um das Dialogfeld **IP-Filterliste** zu schließen.

2. Erstellen von Filteraktionen

In diesem Verfahren werden zwei Filteraktionen erstellt. Die erste wird verwendet, um die gesamte Kommunikation von angegebenen Computern zu blockieren, und die zweite dient dazu, den Einsatz der Verschlüsselung zwischen Anwendungsserver und Datenbankserver realisieren.

▶ **So erstellen Sie Filteraktionen**

1. Klicken Sie auf die Registerkarte **Filteraktionen verwalten**.

   Beachten Sie, dass bereits einige vordefinierte Aktionen vorhanden sind.
2. Klicken Sie auf **Hinzufügen**, um eine neue Filteraktion zu erstellen.

   In den nun folgenden Schritten erstellen Sie eine Blockierungsaktion, mit der die gesamte Kommunikation von ausgewählten Computern blockiert werden kann.
3. Klicken Sie auf **Weiter**, um den Begrüßungsdialog des Filteraktions-Assistenten zu schließen.
4. Geben Sie im Feld **Name** den Namen **Block** ein, und klicken Sie dann auf **Weiter**.
5. Wählen Sie im Dialogfeld **Allgemeine Optionen der Filteraktion** den Eintrag **Blockieren**, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.
7. Klicken Sie auf **Hinzufügen**, um den Filteraktions-Assistenten erneut zu starten.

   In den nun folgenden Schritten erstellen Sie eine Filteraktion, mit der der Einsatz von Verschlüsselung zwischen Anwendungsserver und Datenbankserver erzwungen wird.

8. Klicken Sie auf **Weiter**, um den Begrüßungsdialog des Filteraktions-Assistenten zu schließen.
9. Geben Sie im Feld **Name** den Namen **Require High Security** ein, und klicken Sie dann auf **Weiter**.
10. Wählen Sie **Sicherheit aushandeln**, und klicken Sie dann auf **Weiter**.
11. Wählen Sie **Keine Kommunikation mit Computern zulassen, die IPSec nicht unterstützen**, und klicken Sie auf **Weiter**.
12. Klicken Sie auf **Benutzerdefiniert**, und klicken Sie dann auf **Einstellungen**.
13. Vergewissern Sie sich, dass das Kontrollkästchen **Datenintegrität und -verschlüsselung (ESP)** aktiviert ist.
14. Wählen Sie in der Dropdownliste **Integritätsalgorithmus** den Eintrag **SHA1**.
15. Wählen Sie in der Dropdownliste **Verschlüsselungsalgorithmus** den Eintrag **3DES**.
16. Aktivieren Sie die beiden Kontrollkästchen im Bereich **Sitzungsschlüssel-einstellungen**, um alle 100.000 KB bzw. alle 3.600 Sekunden einen neuen Schlüssel zu erzeugen.
17. Klicken Sie auf **OK**, um das Dialogfeld **Einstellungen für Sicherheitsmethoden anpassen** zu schließen, und klicken Sie auf **Weiter**.
18. Aktivieren Sie das Kontrollkästchen **Eigenschaften bearbeiten**, und klicken Sie dann auf **Fertig stellen**.
19. Deaktivieren Sie das Kontrollkästchen **Unsichere Kommunikat. annehmen, aber immer mit IPSec antworten**.
20. Aktivieren Sie das Kontrollkästchen **Sitzungsschlüssel mit Perfect Forward Secrecy (PFS)**, und klicken Sie auf **OK**.
21. Klicken Sie auf **Schließen**, um das Dialogfeld **IP-Filterlisten und Filteraktionen verwalten** zu schließen.

3. Erstellen von Regeln

In diesem Verfahren werden zwei neue Regeln erstellt, mit denen der in Verfahren 1 erstellte Filter den in Verfahren 2 erstellten Filteraktionen zugewiesen wird.

▶ **So erstellen Sie Regeln**

1. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf lokalem Computer**, und klicken Sie dann auf **IP-Sicherheitsrichtlinie erstellen**.
2. Klicken Sie auf **Weiter**, um den Begrüßungsdialog des IP-Sicherheitsrichtlinien-Assistenten zu schließen.
3. Geben Sie im Feld **Name** den Namen **Secure SQL** ein, und klicken Sie dann auf **Weiter**.
4. Deaktivieren Sie das Kontrollkästchen **Die Standardantwortregel aktivieren**, und klicken Sie auf **Weiter**.
5. Lassen Sie das Kontrollkästchen **Eigenschaften bearbeiten** aktiviert, und klicken Sie dann auf **Fertig stellen**.
6. Klicken Sie auf **Hinzufügen**, um den Sicherheitsregel-Assistenten zu starten.
7. Klicken Sie auf **Weiter**, um den Begrüßungsdialog des Sicherheitsregel-Assistenten zu schließen.
8. Klicken Sie auf **Diese Regel spezifiziert keinen Tunnel**, und klicken Sie dann auf **Weiter**.
9. Klicken Sie auf **Alle Netzwerkverbindungen** und dann auf **Weiter**.
10. Klicken Sie auf **Diese Zeichenfolge zum Schutz des Schlüsselaustauschs verwenden**.
11. Geben Sie **MySecret** als geheimen Schlüssel in das Textfeld ein.

Hinweis: Dieser Schlüssel muss auf beiden Computern der gleiche sein, damit diese erfolgreich kommunizieren können. In der Praxis sollten Sie eine lange Zufallszahl verwenden, zum Zwecke der Erläuterung in dieser Vorgehensweise ist "MySecret" jedoch ausreichend.

12. Klicken Sie auf **Weiter**.
13. Wählen Sie die Option **SQL Port**.

Hinweis: Sie müssen auf den Kreis (das runde Optionsfeld) und nicht auf den Text klicken, damit die Option ausgewählt wird.

14. Klicken Sie auf **Weiter**.
15. Wählen Sie **Require High Security**, und klicken Sie dann auf **Weiter**.
16. Klicken Sie auf **Fertig stellen**, um zum Dialogfeld **Eigenschaften von "Secure SQL"** zurückzukehren.
17. Klicken Sie auf **Hinzufügen**, um den Sicherheitsregel-Assistenten erneut zu starten, und klicken Sie dann auf **Weiter**, um den Begrüßungsdialog zu schließen.
18. Klicken Sie auf **Diese Regel spezifiziert keinen Tunnel**, und klicken Sie dann auf **Weiter**.
19. Klicken Sie auf **Alle Netzwerkverbindungen** und dann auf **Weiter**.
20. Lassen Sie im Dialogfeld Authentifizierungsmethode die Option **Windows 2000-Standard (Kerberos V5-Protokoll)** aktiviert, und klicken Sie auf **Weiter**.

Hinweis: Mit dieser Regel wird die Filteraktion **Blockieren** festgelegt, also ist keine Authentifizierung erforderlich.

21. Klicken Sie im Dialogfeld **IP-Filterliste** auf **Gesamter IP-Verkehr**, und klicken Sie dann auf **Weiter**.
22. Wählen Sie im Dialogfeld **Filteraktion** die Option **Block**, und klicken Sie dann auf **Weiter**.
23. Klicken Sie auf **Fertig stellen**.
24. Klicken Sie auf **Schließen**, um das Dialogfeld **Eigenschaften von "Secure SQL"** zu schließen.

4. Exportieren der IPSec-Richtlinie auf den Remotecomputer

Die IPSec-Richtlinie, die Sie soeben auf dem Datenbankserver erstellt haben, muss nun auf den Anwendungsserver exportiert und kopiert werden.

▶ **So exportieren Sie die IPSec-Richtlinie auf den Anwendungsserver**

1. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf den Knoten **IP-Sicherheitsrichtlinien auf lokalem Computer**, zeigen Sie auf **Alle Tasks**, und klicken Sie dann auf **Richtlinien exportieren**.
2. Geben Sie im Feld **Name** den Namen **Secure SQL** ein, und klicken Sie dann auf **Speichern**, um die Datei auf die lokale Festplatte zu exportieren.
3. Nun können Sie die IPSEC-Datei entweder auf den Anwendungsserver kopieren oder sie unter Verwendung einer Dateifreigabe verfügbar machen.

Wichtig: Da die exportierte Richtliniendatei einen vorinstallierten Schlüssel im Klartext enthält, muss die Datei sorgfältig gesichert werden. Sie sollte nicht auf der Festplatte des jeweiligen Computers gespeichert werden.

4. Melden Sie sich als Administrator am Anwendungsserver an, und starten Sie das MMC-Snap-In Lokale Sicherheitsrichtlinie.

5. Markieren Sie **IP-Sicherheitsrichtlinien auf lokalem Computer**, klicken Sie mit der rechten Maustaste darauf, zeigen Sie auf **Alle Tasks**, und klicken Sie dann auf **Richtlinien importieren**.
6. Suchen Sie nach der vorher exportierten IPSEC-Datei, und klicken Sie auf **Öffnen**, um die Richtlinie zu importieren.

5. Zuweisen von Richtlinien

Eine IPSec-Richtlinie muss zugewiesen werden, bevor sie in Kraft treten kann. Beachten Sie, dass auf einem Computer immer nur jeweils eine Richtlinie aktiv sein kann.

▶ **So weisen Sie die Richtlinie "Secure SQL" auf dem Anwendungsserver und dem Datenbankserver zu**

1. Klicken Sie auf dem Anwendungsserver mit der rechten Maustaste auf die soeben importierte Richtlinie **Secure SQL**, und klicken Sie dann auf **Zuweisen**.
2. Wiederholen Sie den vorstehenden Schritt auf dem Datenbankserver.

   Die gespiegelte Richtlinie wurde damit auf beiden Computern zugewiesen.

   Die Richtlinie stellt sicher, dass nur der Anwendungsserver mit dem Datenbankserver kommunizieren kann. Darüber hinaus sind nur TCP-Verbindungen über Port 1433 zulässig, und der gesamte Datenverkehr zwischen den beiden Computern wird verschlüsselt.

6. Überprüfen der Funktionstüchtigkeit

In diesem Verfahren wird mithilfe des Netzwerkmonitors sichergestellt, dass die Datenströme zwischen Anwendungsserver und Datenbankserver verschlüsselt werden.

▶ **So überprüfen Sie die Funktionstüchtigkeit**

1. Erstellen Sie auf dem Anwendungsserver mit Visual Studio .NET in C# eine neue Konsolenanwendung mit Namen **SQLIPSecClient**.
2. Kopieren Sie den folgenden Code in **Class1.cs**, und ersetzen Sie damit allen vorhandenen Code.

Hinweis: Ersetzen Sie die IP-Adresse in der Verbindungszeichenfolge durch die IP-Adresse Ihres Datenbankservers.

```
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. Klicken Sie im Menü **Erstellen** auf **Projektmappe erstellen**.
4. Damit zwischen den beiden Computern eine Windows-Authentifizierung stattfinden kann, müssen Sie das Konto, mit dem Sie gegenwärtig interaktiv am Anwendungscomputer angemeldet sind, auf den Datenbankserver kopieren. Stellen Sie sicher, dass Benutzername und Kennwort die gleichen sind.

   Darüber hinaus müssen Sie mithilfe von SQL Server Enterprise Manager einen Datenbankanmeldenamen für das neu erstellte Konto sowie einen Datenbankbenutzer für diese Anmeldung an der Northwind-Datenbank anlegen.
5. Heben Sie die Zuweisung der IPSec-Richtlinie **Secure SQL** auf beiden Computern vorübergehend auf.
   a. Starten Sie das Tool **Lokale Sicherheitseinstellungen** auf dem Anwendungsserver.
   b. Klicken Sie auf **IP-Sicherheitsrichtlinien auf lokalem Computer**.
   c. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf **Secure SQL**, und klicken Sie dann auf **Zuweisung entfernen**.
   d. Wiederholen Sie die Schritte a – c auf dem Datenbankserver.
6. Klicken Sie auf dem Datenbankserver in der Programmgruppe **Verwaltung** auf **Netzwerkmonitor**.

Hinweis: Zum Lieferumfang von Windows 2000 Server gehört eine eingeschränkte Version des Netzwerkmonitors. Die Vollversion steht mit Microsoft SMS zur Verfügung.

Wenn der Netzwerkmonitor noch nicht installiert wurde, wechseln Sie in der Systemsteuerung zu **Software**, klicken Sie auf **Windows-Komponenten hinzufügen/entfernen**, wählen Sie **Verwaltungs- und Überwachungsprogramme** aus der Liste **Windows-Komponenten**, klicken Sie auf **Details**, und klicken Sie dann auf **Netzwerkmonitorprogramme**. Klicken Sie auf **OK** und dann auf **Weiter**, um die eingeschränkte Version des Netzwerkmonitors zu installieren. Sie werden möglicherweise aufgefordert, die Windows 2000 Server-CD einzulegen.

---

7. Klicken Sie im Menü **Sammeln** auf **Filter**, um einen neuen Filter zu erstellen, der für die Anzeige des zwischen Anwendungsserver und Datenbankserver übertragenen TCP/IP-Netzwerkverkehrs konfiguriert ist.
8. Klicken Sie auf die Schaltfläche **Sammlung starten**.
9. Kehren Sie zum Anwendungsserver zurück, und führen Sie die Testkonsolen-anwendung aus. Nun sollte eine Liste der Produkte in der Northwind-Datenbank im Konsolenfenster angezeigt werden.
10. Kehren Sie zum Datenbankserver zurück, und klicken Sie im Netzwerkmonitor auf die Schaltfläche **Sammlung beenden und anzeigen**.
11. Doppelklicken Sie auf den ersten gesammelten Rahmen, um die hierin enthaltenen Daten anzuzeigen.
12. Führen Sie in den gesammelten Rahmen einen Bildlauf nach unten durch. Sie sollten nun die SELECT-Anweisung im Klartext gefolgt von der Liste der Produkte sehen, die aus der Datenbank abgerufen wurde.
13. Weisen Sie die IPSec-Richtlinie **Secure SQL** auf beiden Computern zu:
    a. Starten Sie das Tool **Lokale Sicherheitseinstellungen** auf dem Anwendungsserver.
    b. Klicken Sie auf **IP-Sicherheitsrichtlinien auf lokalem Computer**.
    c. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf **Secure SQL**, und klicken Sie dann auf **Zuweisen**.
    d. Wiederholen Sie die Schritte a – c auf dem Datenbankserver.
14. Schließen Sie im Netzwerkmonitor das Sammlungsfenster.
15. Klicken Sie auf die Schaltfläche **Sammlung starten**, und klicken Sie dann im Meldungsfenster **Datei speichern** auf **Nein**.
16. Kehren Sie zum Anwendungsserver zurück, und führen Sie die Testkonsolen-anwendung erneut aus.
17. Kehren Sie zum Datenbankserver zurück, und klicken Sie im Netzwerkmonitor auf **Sammlung beenden und anzeigen**.
18. Vergewissern Sie sich, dass die Daten nun nicht mehr lesbar sind (da sie verschlüsselt wurden).
19. Schließen Sie den Netzwerkmonitor.

Weitere Ressourcen

Weitere Informationen über IPSec finden Sie unter "IP Security and Filtering" im TechNet (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prcc_tcp_erqb.asp?frame=true>, englischsprachig).

Informationen über den Netzwerkmonitor finden Sie im Abschnitt "Network Monitor" des Microsoft Platform SDKs im MSDN (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netmon/netmon/network_monitor.asp, englischsprachig).