Erstellen sicherer ASP.NET-Anwendungen

Authentifizierung, Autorisierung und sichere Kommunikation

Kapitel 4 - Sichere Kommunikation

J.D. Meier, Alex Mackman, Michael Dunner und Srinath Vasireddy

Microsoft Corporation

Oktober 2002

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

Zusammenfassung

In diesem Kapitel werden die beiden Kerntechnologien vorgestellt, mit denen die Vertraulichkeit und Integrität von Datennachrichten bereitgestellt wird, die im Netzwerk zwischen den Clients und Servern im Internet und im Firmenintranet übertragen werden: SSL und IPSec. Darüber hinaus wird die RPC-Verschlüsselung erläutert, mit der die Kommunikation mit Remote-Serviced Components gesichert werden kann.

Inhalt

Viele Anwendungen übertragen sicherheitssensitive Daten über Netzwerke zu und von Endbenutzern sowie zwischen Zwischenknoten der Anwendung. Sensitive Daten können Anmeldeinformationen für die Authentifizierung oder Daten wie Kreditkartennummern oder Details von Banktransaktionen umfassen. Um die Informationen während der Übertragung vor unerwünschter Offenlegung und die Daten vor unberechtigten Änderungen zu schützen, muss der Kanal zwischen den Kommunikationsendpunkten gesichert werden.

Eine sichere Kommunikation stellt die beiden folgenden Features bereit:

- **Datenschutz** - Der Datenschutz sorgt dafür, dass Daten geheim und vertraulich bleiben und nicht mit einer Netzwerküberwachungssoftware von Lauschern angezeigt werden können. Datenschutz wird in der Regel durch Verschlüsselung sichergestellt.
- **Integrität** - Sichere Kommunikationskanäle müssen außerdem sicherstellen, dass die Daten bei der Übertragung vor versehentlichen oder absichtlichen (böswilligen) Änderungen geschützt sind. Die Integrität wird normalerweise durch Nachrichtenauthentifizierungscodes (Message Authentication Codes oder MACs) sichergestellt.

In diesem Kapitel werden die folgenden Technologien für eine sichere Kommunikation behandelt:

- **Secure Sockets Layer / Transport Layer Security (SSL/TLS)** - Mit diesen Technologien wird der Kanal zwischen einem Browser und einem Webserver gesichert. Darüber hinaus können Nachrichten von Webdiensten und die Kommunikation zu und von einem Datenbankserver mit Microsoft® SQL Server™ 2000 gesichert werden.
- **Internet-Protokollsicherheit (IPSec)** - IPSec stellt eine sichere Kommunikationslösung auf Transportebene bereit, mit der die zwischen zwei Computern, z. B. einem Anwendungsserver und einem Datenbankserver, gesendeten Daten gesichert werden können.
- **RPC-Verschlüsselung (Remote Procedure Call)** - Das von Distributed COM (DCOM) verwendete RPC-Protokoll stellt eine Authentifizierungsstufe (Paketsicherheit) bereit, bei der alle zwischen Client und Server gesendeten Paketdaten verschlüsselt werden.

Ermitteln der zu sichernden Daten

Wenn eine Webanforderung die physischen Bereitstellungsebenen der Anwendung durchläuft, werden mehrere Kommunikationskanäle durchquert. Ein häufig verwendetes Model für die Bereitstellung von Webanwendungen ist in Abbildung 4.1 dargestellt.

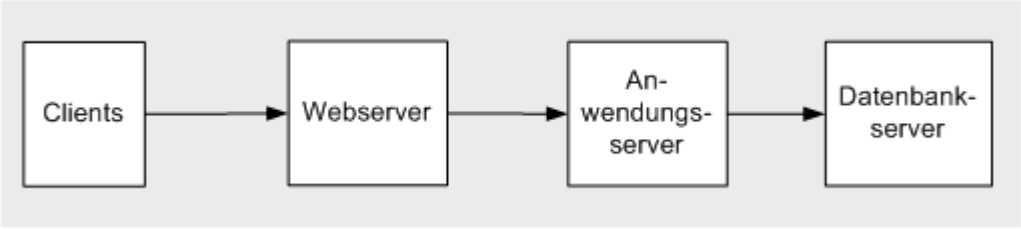

Abbildung 4.1
Ein typisches Bereitstellungsmodell für Webanwendungen

In diesem typischen Bereitstellungsmodel durchläuft eine Anforderung drei verschiedene Kanäle. Die Verbindung zwischen Client und Webserver kann über das Internet oder ein Firmenintranet erfolgen. Dabei wird normalerweise HTTP verwendet. Die restlichen beiden Verbindungen liegen zwischen zwei Servern in der Firmendomäne. Dennoch stellen alle drei Verbindungen potenzielle Sicherheitsrisiken dar. Viele rein intranetbasierende Anwendungen übermitteln sicherheitssensitive Daten zwischen den Ebenen, z. B. Personal- und Gehaltsabrechnungsanwendungen mit vertraulichen Mitarbeiterdaten.

Abbildung 4.2 zeigt, wie die einzelnen Kanäle mit einer Kombination aus SSL, IPSec und RPC-Verschlüsselung gesichert werden können.

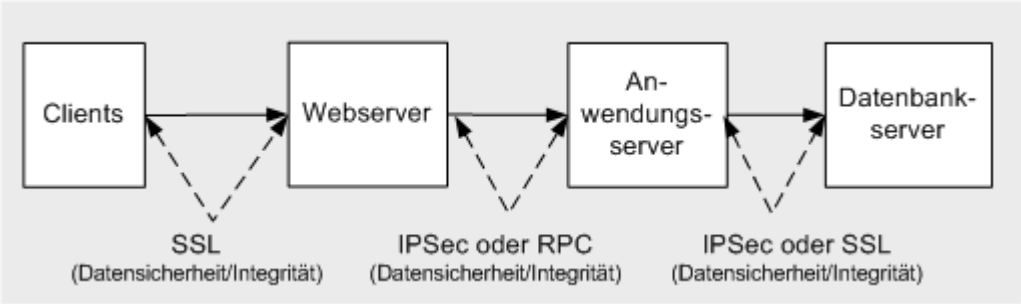

Abbildung 4.2
Ein typisches Bereitstellungsmodell für Webanwendungen mit sicherer Kommunikation

Die Auswahl der jeweiligen Technologien hängt von einer Reihe von Faktoren ab, wie z. B. Transportprotokoll, Technologien der Endpunkte sowie Erwägungen zur Umgebung (wie Hardware, Betriebssystemversionen, Firewalls usw.).

SSL/TLS

Mit SSL/TLS wird ein verschlüsselter Kommunikationskanal zwischen Client und Server eingerichtet. Der Handshakemechanismus, mit dem der sichere Kanal eingerichtet wird, ist umfassend dokumentiert. Weitere Informationen finden Sie in der Microsoft Knowledge Base in den folgenden Artikeln:

- Q257591, "Description of the Secure Sockets Layer (SSL) Handshake" (US)
- Q257587, "Description of the Server Authentication Process During the SSL Handshake" (US)
- Q257586, "Description of the Client Authentication Process During the SSL Handshake" (US)

Verwenden von SSL

Wenn Sie SSL verwenden, müssen Sie Folgendes beachten:

- Der Client verwendet das HTTPS-Protokoll (und gibt einen URL mit **https://** an), wenn SSL verwendet wird. Der Server empfängt auf TCP-Port 443.
- Sie sollten die Leistung der Anwendung überwachen, wenn Sie SSL aktivieren.
  SSL verwendet komplexe kryptographische Funktionen, um die Daten zu ver- und entschlüsseln, sodass die Leistung der Anwendung beeinflusst wird. Die größte Auswirkung auf die Leistung tritt beim ersten Handshake auf, bei dem eine asymmetrische Verschlüsselung mit öffentlichen/privaten Schlüsseln verwendet wird. Danach (nachdem ein sicherer Sitzungsschlüssel generiert und ausgetauscht wurde) wird eine schnellere symmetrische Verschlüsselung verwendet, um die Anwendungsdaten zu verschlüsseln.
- Sie sollten Seiten, die SSL verwenden, optimieren, indem Sie in diesen Seiten weniger Text und einfache Grafiken einfügen.
- Da die Leistungsbeeinträchtigung bei SSL beim Einrichten der Sitzung am größten ist, müssen Sie sicherstellen, dass das Zeitlimit nicht überschritten wird.
  Sie können dazu den Wert des Registrierungseintrags **ServerCacheTime** erhöhen. Weitere Informationen finden Sie im Artikel Q247658, "HOW TO: Configure Secure Sockets Layer Server and Client Cache Elements" (US) in der Microsoft Knowledge Base.
- Bei SSL muss auf dem Webserver (bzw. dem Datenbankserver, wenn Sie SSL für die Kommunikation mit SQL Server 2000 verwenden) ein Serverauthentifizierungszertifikat installiert sein. Weitere Informationen zum Installieren von Serverauthentifizierungszertifikaten finden Sie unter "Vorgehensweise: Einrichten von SSL auf einem Webserver" im Abschnitt "Referenz" dieses Handbuchs.

IPSec

Mit IPSec 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 normal über TCP- und UDP-Ports.

IPSec bietet folgende Möglichkeiten:

- 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 (keine Authentifizierung von Benutzern). Sie können beispielsweise einen Datenbankserver sichern, indem Sie eine Richtlinie einrichten, 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.

Hinweis: IPSec soll nicht die Sicherheit auf Anwendungsebene ersetzen, sondern wird heute als tief greifender Verteidigungsmechanismus oder zum Sichern unsicherer Anwendungen, ohne diese zu ändern, sowie zum Sichern von anderen Protokollen als TLS vor Angriffen aus dem Netzwerk verwendet.

Verwenden von IPSec

Wenn Sie IPSec verwenden, müssen Sie Folgendes beachten:

- IPSec kann sowohl für Authentifizierung als auch für Verschlüsselung verwendet werden.
- Es gibt keine IPSec-APIs für Entwickler, um Einstellungen programmatisch zu steuern. IPSec wird vollständig in Microsoft Management Console (MMC) über das IPSec-Snap-In in **Lokale Sicherheitsrichtlinie** gesteuert und konfiguriert.
- IPSec im Betriebssystem Microsoft Windows® 2000 kann nicht alle Arten von IP-Verkehr sichern.

  Insbesondere kann damit nicht Broadcast-, Multicast-, Internetschlüsselaustausch- oder Kerberos-Datenverkehr (dabei handelt es sich bereits um ein sicheres Protokoll) gesichert werden.

  Weitere Informationen finden Sie in der Microsoft Knowledge Base in Artikel Q253169, "Traffic That Can and Cannot Be Secured by IPSec" (US).
- Zur Steuerung werden IPSec-Filter verwendet, wenn IPSec verwendet wird.

  Die IPSec-Richtlinien können Sie mit dem IPSec-Monitor überwachen. Der IPSec-Monitor (**Ipsecmon.exe**) stellt Informationen über die aktive IPSec-Richtlinie und die Einrichtung eines sicheren Kanals zwischen Computern bereit.

  Weitere Informationen finden Sie in den folgenden Knowledge Base-Artikeln:

  - Q313195, "HOW TO: Use IPSec Monitor in Windows 2000" (US)
  - Q231587, "Using the IP Security Monitor Tool to View IPSec Communications" (US)
- Sie können IPSec mit gegenseitiger Authentifizierung verwenden, um zwischen zwei Servern eine Vertrauensstellung einzurichten. Zum Authentifizieren beider Computer werden Zertifikate verwendet.

  Weitere Informationen finden Sie in den folgenden Knowledge Base-Artikeln:

  - Q248711, "Mutual Authentication Methods Supported for L2TP/IPSec" (US)
  - Q253498, "HOW TO: Install a Certificate for Use with IP Security" (US)

- Wenn Sie IPSec verwenden möchten, um die Kommunikation zwischen zwei Computern zu sichern, die durch einen Firewall getrennt sind, darf der Firewall keine Netzwerkadressübersetzung (NAT) verwenden. IPSec funktioniert nicht mit NAT-basierten Geräten.

  Weitere Informationen und Konfigurationsschritte finden Sie im Microsoft Knowledge Base-Artikel Q233256, "HOW TO Enable IPSec Traffic through a Firewall" (US) sowie im Abschnitt "Referenz" dieses Handbuchs unter "Vorgehensweise: Verwenden von IPSec zum Sichern der Kommunikation zwischen zwei Servern".

RPC-Verschlüsselung

RPC ist der zugrunde liegende Transportmechanismus, der von DCOM verwendet wird. RPC stellt eine Reihe von konfigurierbaren Authentifizierungsstufen bereit, die von keiner Authentifizierung (ohne Datenschutz) bis zur vollständigen Verschlüsselung des Parameterstatus reichen.

Bei der sichersten Stufe (RPC-Paketsicherheit) wird der Parameterstatus für jeden Remoteprozeduraufruf (und daher jeden Aufruf einer DCOM-Methode) verschlüsselt. Die Stufe der RPC-Verschlüsselung, 40-Bit oder 128-Bit, hängt von der Version des Windows-Betriebssystems ab, das auf den Client- und Servercomputern ausgeführt wird.

Verwenden der RPC-Verschlüsselung

Sie sollten die RPC-Verschlüsselung verwenden, wenn die webbasierte Anwendung mit Serviced Components (in Enterprise Services-Serveranwendungen) kommuniziert, die sich auf Remotecomputern befinden.

Um Authentifizierung (und Verschlüsselung) für die RPC-Paketsicherheit zu verwenden, müssen Sie in diesem Fall Client und Server konfigurieren. Zwischen Client und Server erfolgt eine komplexe Aushandlung, die sicherstellt, dass die höherwertige Einstellung (Client oder Server) verwendet wird.

Die Servereinstellungen können bei der Entwicklung auf der Ebene der (Enterprise Services-)Anwendung mit .NET-Attributen in der Serviced Component-Assembly oder mit dem Verwaltungsprogramm für Komponentendienste erfolgen.

Wenn es sich bei dem Client um eine ASP.NET-Webanwendung oder –Webdienst handelt, wird die Authentifizierungsstufe, die vom Client verwendet wird, in der Datei **Machine.config** mit dem **comAuthenticationLevel**-Attribut im <**processModel**>-Element konfiguriert, das die Standardauthentifizierungsstufe für alle ASP.NET-Anwendungen festlegt, die auf dem Webserver ausgeführt werden.

Weitere Informationen

Weitere Informationen zur Verhandlung der RPC-Authentifizierungsstufe und der Serviced Component-Konfiguration finden Sie in Kapitel 9, "Enterprise Services-Sicherheit".

Durchgängige Sicherheit

- Durchgängige Kommunikationsszenarien können weitgehend in die folgenden Themen kategorisiert werden:
- Browser zu Webserver
- Webserver zu Remoteanwendungsserver
- Anwendungsserver zu Datenbankserver

Browser zu Webserver

Verwenden Sie SSL, um vertrauliche Daten zu sichern, die zwischen einem Browser und einem Webserver gesendet werden. Sie müssen SSL in den folgenden Situationen verwenden:

- Sie verwenden die Formularauthentifizierung und müssen die unverschlüsselten Anmeldeinformationen sichern, die von einem Anmeldeformular an einen Webserver gesendet werden.

  In diesem Szenario sollten Sie SSL verwenden, um den Zugriff auf alle Seiten (nicht nur die Anmeldeseite) zu sichern, um sicherzustellen, dass das Authentifizierungscookie, das beim ersten Authentifizierungsvorgang erzeugt wurde, während der Zeitdauer der Clientbrowsersitzung mit der Anwendung sicher bleibt.
- Sie verwenden die Standardauthentifizierung und müssen die (Base64-codierten) unverschlüsselten Anmeldeinformationen sichern.

  Sie sollten SSL verwenden, um den Zugriff auf alle Seiten (nicht nur die erste Anmeldeseite) zu sichern, da die Anmeldeinformationen bei der Standardauthentifizierung bei allen Anforderungen (nicht nur bei der ersten) an die Anwendung unverschlüsselt an den Webserver gesendet werden.

Hinweis: Mit Base64 werden binäre Daten als druckbarer ASCII-Text codiert. Im Gegensatz zu einer Verschlüsselung wird dadurch keine Integrität und kein Datenschutz der Nachrichten bereitgestellt.

- Die Anwendung überträgt vertrauliche Daten zwischen dem Browser und dem Webserver (in beiden Richtungen), beispielsweise Kreditkartennummern oder Details zu Bankkonten.

Webserver zu Remoteanwendungsserver

Der Transportkanal zwischen einem Webserver und einem Remoteanwendungsserver sollte mit IPSec, SSL oder RPC-Verschlüsselung gesichert werden. Die Auswahl hängt von den Transportprotokollen und Umgebungsfaktoren (Betriebssystemversionen, Firewalls usw.) ab.

- **Enterprise Services** - Wenn der Remoteserver eine oder mehrere Serviced Components (in einer Enterprise Services-Serveranwendung) hostet und damit direkt kommuniziert wird (aufgrund der Verwendung von DCOM), verwenden Sie die Verschlüsselung für die RPC-Paketsicherheit.

  Weitere Informationen zum Konfigurieren der RPC-Verschlüsselung zwischen einer Webanwendung und einer Remote-Serviced Component finden Sie in Kapitel 9, "Enterprise Services-Sicherheit".
- **Webdienste** - Wenn der Remoteserver einen Webdienst hostet, können Sie zwischen IPSec und SSL auswählen.

  In der Regel sollten Sie SSL verwenden, da der Webdienst bereits den HTTP-Transport verwendet. SSL ermöglicht außerdem nur, die vom und zum Webdienst gesendeten Daten zu verschlüsseln (und nicht den gesamten gesendeten Datenverkehr zwischen den beiden Computern). Bei IPSec wird der gesamte Datenverkehr verschlüsselt, der zwischen den beiden Computern gesendet wird.

Hinweis: Mit der Sicherheit auf Nachrichtenebene (einschließlich der Datenverschlüsselung) beschäftigt sich die GXA-Initiative (Global XML Web Services Architecture) und insbesondere die WS-Security-Spezifikation. Microsoft stellt das Web Services Development Toolkit bereit, damit Sie Lösungen für die Sicherheit auf Nachrichtenebene entwickeln können. Dieses Toolkit steht unter http://msdn.microsoft.com/webservices/building/wsdk/ zum Download zur Verfügung.

- **.NET-Komponenten (mit .NET Remoting)** - Wenn der Remoteserver eine oder mehrere .NET-Komponenten hostet und über den TCP-Kanal eine Verbindung zu diesen Komponenten hergestellt wird, können Sie mithilfe von IPSec eine sichere Kommunikationsverbindung bereitstellen. Wenn die .NET-Komponenten in ASP.NET gehostet werden, können Sie SSL verwenden (Konfiguration mit IIS).

Anwendungsserver zu Datenbankserver

Um die Daten zu sichern, die zwischen einem Anwendungsserver und einem Datenbankserver gesendet werden, können Sie IPSec verwenden. Wenn auf dem Datenbankserver SQL Server 2000 ausgeführt wird (und die SQL Server 2000-Netzwerkbibliotheken auf dem Anwendungsserver installiert sind), können Sie SSL verwenden. Bei der letzten Option muss im Speicher des Datenbankservercomputers ein Serverauthentifizierungszertifikat installiert sein.

Sie sollten die Verbindung zum Datenbankserver in den folgenden Situationen sichern:

- Sie stellen eine Verbindung mit dem Datenbankserver her und verwenden keine Windows-Authentifizierung. Sie verwenden eventuell die SQL-Authentifizierung bei SQL Server, oder Sie stellen eine Verbindung zu einer anderen Datenbank als SQL Server her. In diesen Fällen werden die Anmeldeinformationen unverschlüsselt übertragen, sodass ein erhebliches Sicherheitsrisiko entstehen kann.

  Hinweis: Einer der Hauptvorteile dessen, die Windows-Authentifizierung bei SQL Server zu verwenden, liegt darin, dass die Anmeldeinformationen niemals über das Netzwerk übertragen werden. Weitere Einzelheiten zur Windows- und SQL-Authentifizierung finden Sie in Kapitel 12, "Datenzugriffssicherheit".

- Die Anwendung sendet und empfängt vertrauliche Daten von der Datenbank (z. B. Gehaltsinformationen).

Verwenden von SSL zu SQL Server

Berücksichtigen Sie die folgenden Punkte, wenn Sie den Kanal zu einer SQL Server-Datenbank mit SSL sichern:

- Damit SSL funktioniert, müssen Sie im Computerspeicher des Datenbankservercomputers ein Serverauthentifizierungszertifikat speichern. Darüber hinaus muss der Clientcomputer über ein Stammzertifikat derselben (bzw. einer vertrauenden) Zertifizierungsstelle verfügen, von der das Serverzertifikat ausgestellt wurde.
- Auf den Clients müssen die SQL Server 2000-Verbindungsbibliotheken installiert sein. Frühere Versionen oder generische Bibliotheken funktionieren nicht.
- SSL funktioniert nur für TCP/IP (das empfohlene Kommunikationsprotokoll für SQL Server) und Named Pipes.
- Sie können den Server so konfigurieren, dass die Verwendung der Verschlüsselung für alle Verbindungen (von allen Clients) erzwungen wird.
- Auf dem Client bestehen die folgenden Möglichkeiten:
  - Erzwingen der Verwendung der Verschlüsselung für alle ausgehenden Verbindungen.
  - Ermöglichen, dass Clientanwendungen anhand der Verbindungszeichenfolge auswählen, ob die Verschlüsselung für einzelne Verbindungen verwendet werden soll.
- Im Gegensatz zu IPSec sind keine Konfigurationsänderungen erforderlich, wenn sich die IP-Adresse von Clients oder Servern ändert.

Weitere Informationen

Weitere Informationen zur Verwendung von SSL zu SQL Server finden Sie in den folgenden Ressourcen:

- "How To: Use SSL to Secure Communication with SQL Server 2000" im Abschnitt "Referenz" dieses Handbuchs.
- Webcast: “Microsoft SQL Server 2000: How to Configure SSL Encryption (23. April 2002)” (nur auf Englisch verfügbar)

Auswählen zwischen IPSec und SSL

Beachten Sie bei der Auswahl zwischen IPSec und SSL die folgenden Punkte:

- Mit IPSec kann der gesamte IP-Verkehr zwischen Computern gesichert werden; SSL gilt für eine einzelne Anwendung.
- Bei IPSec handelt es sich um eine computerweite Einstellung, die nicht die ausschließliche Verschlüsselung spezieller Netzwerkverbindungen unterstützt. Die Sites können jedoch so aufgeteilt werden, das SSL verwendet wird oder nicht. Wenn Sie SSL für Verbindungen zu SQL Server verwenden, können Sie weiterhin für einzelne Verbindungen (von der Clientanwendung) auswählen, ob SSL verwendet werden soll.
- IPSec verhält sich Anwendungen gegenüber transparent. IPSec kann daher zusammen mit sicheren Protokollen verwendet werden, die oberhalb von IP liegen, z. B. HTTP, FTP und SMTP. SSL/TLS ist demgegenüber eng an die Anwendung gebunden.
- IPSec kann zusätzlich zur Verschlüsselung auch für die Authentifizierung von Computern verwendet werden. Dies ist insbesondere für Szenarien mit vertrauenswürdigen Subsystemen von Bedeutung, in denen die Datenbank eine feste Identität einer bestimmten Anwendung (die auf einem bestimmten Computer ausgeführt wird) autorisiert. Mit IPSec kann sichergestellt werden, dass nur der jeweilige Anwendungsserver eine Verbindung mit dem Datenbankserver herstellen kann, um Angriffe von anderen Computern zu verhindern.
- Bei IPSec muss auf beiden Computern Windows 2000 oder höher ausgeführt werden.
- SSL kann im Gegensatz zu IPSec über einen NAT-basierten Firewall arbeiten.

Farmen und Lastenausgleich

Wenn Sie SSL zusammen mit mehreren virtuellen Websites verwenden, müssen Sie eindeutige IP-Adressen oder eindeutige Portnummern verwenden. Sie können nicht mehrere Sites mit derselben IP-Adresse und derselben Portnummer verwenden. Bei einem Lastenausgleich können Sie die IP-Adresse problemlos mit einer Serveraffinitätseinstellung kombinieren.

Weitere Informationen

Weitere Informationen finden Sie in der Microsoft Knowledge Base in Artikel Q187504, "HTTP 1.1 Host Headers Are Not Supported When You Use SSL" (US).

Zusammenfassung

In diesem Kapitel wurde beschrieben, wie mit einer Kombination von SSL, IPSec und RPC-Verschlüsselung eine durchgehend sichere Kommunikationslösung für verteilte Anwendungen bereitgestellt werden kann. Zusammenfassend kann festgestellt werden:

- Die Kanalsicherheit ist für Daten von Bedeutung, die über das Internet und im Firmenintranet übertragen werden.
- Berücksichtigen Sie die Sicherheitsanforderungen der Verbindungen vom Webbrowser zum Webserver, vom Webserver zum Anwendungsserver und vom Anwendungsserver zum Datenbankserver.
- Eine sichere Kommunikation sorgt für Datenschutz und Integrität, schützt aber nicht vor Nichtanerkennung (verwenden Sie dafür Clientzertifikate).
- Für die Kanalsicherheit stehen SSL, IPSec und RPC-Verschlüsselung als Optionen zur Verfügung. Die letzte Option trifft zu, wenn die Anwendung DCOM für die Kommunikation mit Remote-Serviced Components verwendet.
- Wenn Sie SSL für die Kommunikation mit SQL Server verwenden, kann die Anwendung für einzelne Verbindungen auswählen, ob die Verbindung verschlüsselt werden soll.
- IPSec verschlüsselt den gesamten IP-Verkehr zwischen zwei Computern.
- Die Auswahl des Sicherheitsmechanismus hängt vom Transportprotokoll, den Betriebssystemversionen und Netzwerkgegebenheiten (z. B. Firewalls) ab.
- Zwischen sicherer Kommunikation und Leistung muss immer ein Kompromiss gefunden werden. Wählen Sie die für die Anforderungen der Anwendung geeignete Sicherheitsstufe aus.