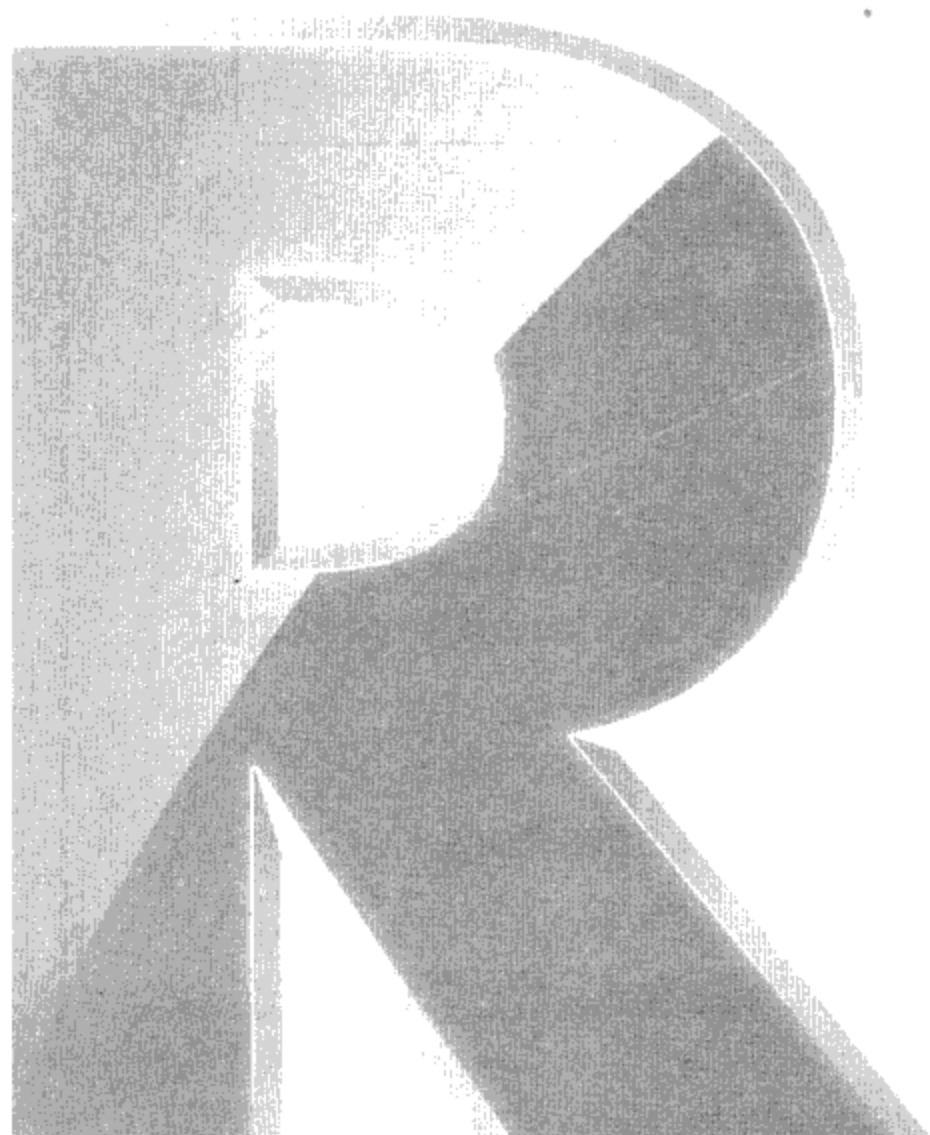


# 第 10 章

## IPSec与网络安全

第6章我们介绍过利用PKI（Public Key Infrastructure）来确保数据在网络上传送的安全，本章将介绍另外一种可在IP网络上使用的安全协议：IPSec（Internet Protocol Security）。

- IPSec概述
- 独立服务器之间的IPSec设置
- 路由器的IPSec设置
- 通过域组策略来设置IPSec
- 采用计算机证书的IPSec设置
- 启用旧版Windows系统的IPSec
- IPSec跨越NAT的问题



## 10-1 IPSec概述

IPSec提供以下功能来让计算机之间能够安全地发送数据:

- 在开始发送数据之前会先相互验证对方的身份 (authentication)。
- 检查所收到的数据是否在发送过程中被恶意者截取与篡改, 也就是确认数据的完整性 (integrity)。
- 将发送的数据加密 (encryption), 以免数据内容外泄。

在两台计算机之间要开始将数据安全地发送出去之前, 它们之间必须先协商 (negotiate), 以便双方同意如何交换与保护所发送的数据, 此协商结果被称为SA (Security Association), 它就好像是双方所签订的**合约书**。SA内包含着双方所协商出来的安全协议与SPI (security parameter index, 见附注) 等数据。所采用的协商方法是标准的IKE (Internet Key Exchange), 如图 10-1所示。

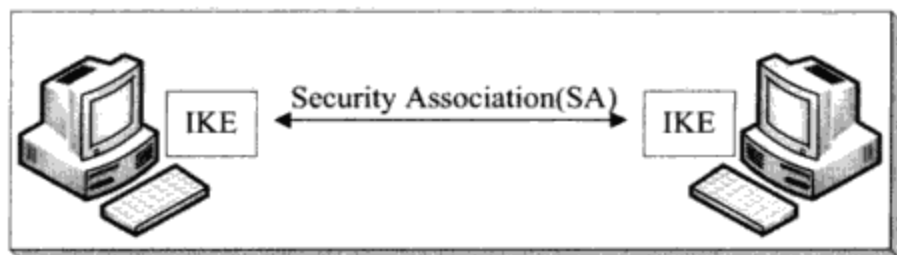


图 10-1

### 提示

如果一台计算机同时与多台计算机利用IPSec来通信, 则此计算机必然会有多个SA, 因此为了避免混淆, IPSec利用SA内的SPI来判断此SA是与哪一台计算机所协商出来的。

### 10-1-1 IKE两阶段协商

IKE将协商工作分为两个阶段 (phase), 这两个阶段所协商出来的SA分别被称为**主模式SA**与**快速模式SA**。

#### 第1阶段: 主模式SA (main mode SA)

此阶段所新建的SA又称为**IKE SA**或**phase I SA**, 它是为了在两台计算机之间新建一个安全的、计算机或用户身份 (identity) 经过验证的通信管道, 之后双方在第2阶段中协商**快速模式SA**时, 便能够通过这个安全的信道来通信。此阶段会经过以下程序:

- **策略协商:** 这个程序会协商出以下四个必要参数:
  - **加密方法:** 例如AES-256、AES-192、AES-128 (默认)、3DES或DES。
  - **完整性检查方法:** 例如SHA1 (默认) 或MD5。

- **创建密钥的方法**: 可以是ECC P-384 (Elliptic Curve Diffie-Hellman P-384)、ECC P-256、DH Group 14 (Diffie-Hellman Group 14)、DH Group 2 (默认) 或DH Group 1。其中ECC P-384与ECC P-256只有Windows Vista与Windows Server 2008 或之后的版本才支持。
- **验证方法**: 例如Kerberos V5 (默认)、证书或预共享密钥 (Preshared key) 等方法, 其中的Kerberos V5只适合于域成员计算机。
- **交换“密钥要素”并创建主要密钥**: 为了增加安全性, 因此密钥并不会在网络上发送, 而是双方各自创建密钥, 不过双方必须先交换创建密钥所需的要素 (keying material), 然后再利用此**密钥要素**来各自创建相同的**主要密钥** (master key)。
- **验证身份**: 为了避免man-in-the-middle (中间人攻击) 等类型的攻击行为, 因此双方身份必须经过验证后才可以开始相互通信, 而在验证身份时所发送的验证数据会通过前一个步骤所创建的**主要密钥**来加密与解密。

#### 第2阶段: 快速模式SA (quick mode SA)

此阶段所创建的SA又称为**IPSec SA**或**phase II SA**, 双方之后所发送的数据会通过这个SA内的参数来确保发送的安全性。此阶段会经过以下程序:

- **策略协商**: 这个程序会协商出以下几个参数:
  - **IPSec协议**: 例如AH或ESP (默认)。
  - **完整性与验证方法的散列算法** (hash algorithm): 例如MD5或SHA1 (默认)。
  - **加密方法**: 例如AES-256、AES-192、AES-128 (默认)、3DES或DES。
- **创建“会话密钥”**: 第2阶段之后双方所发送的数据会通过**会话密钥** (session key) 来加密。创建会话密钥时可使用之前第1阶段的**密钥要素**, 也可以双方重新交换**密钥要素**, 然后利用新的**密钥要素**来创建**会话密钥**。
- **将SA、密钥与SPI传给IPSec驱动程序**: 双方的IPSec驱动程序会根据**快速模式SA**内的参数与密钥来确保数据发送的安全性。

第2阶段会创建两个SA, 一个用在传入通信, 一个用在传出通信。虽然有两个SA, 但您利用IPSec监视工具查看时, 界面上只会显示一个SA。第2阶段在协商安全策略与交换**密钥要素**时, 双方所发送数据都会受到第1阶段的**主要密钥**的保护。

### 10-1-2 IPSec的运行模式

Windows计算机的IPSec运行分为以下两种模式:

- **传输模式** (transport mode): 表示此计算机与任何一台计算机通信时, 都需要双方来协商使用IPSec, 例如图 10-2中左边的Windows 7要与其他两台计算机通信时, 都要求对方来协商使用IPSec。

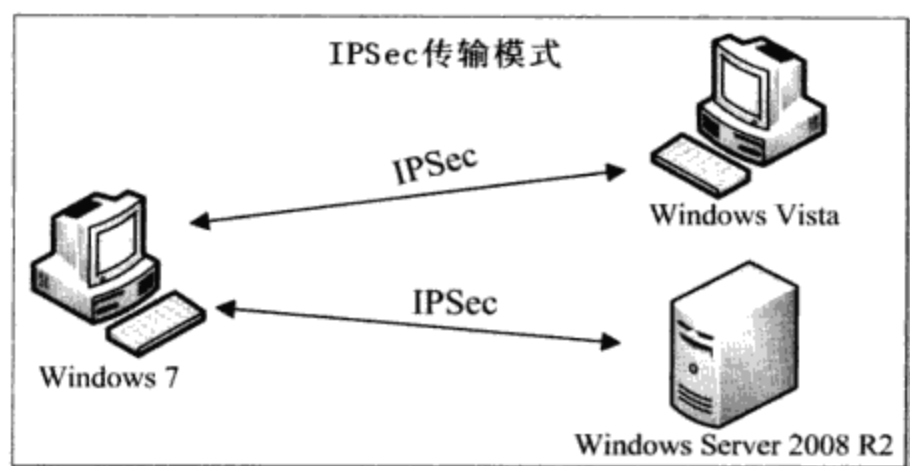


图 10-2

✎ **信道模式 (tunnel mode):** 表示此计算机只有与特定计算机通信时才需要协商使用IPSec, 此模式适合于扮演路由器角色的Windows Server 2008 R2等计算机来使用, 如图 10-3所示。

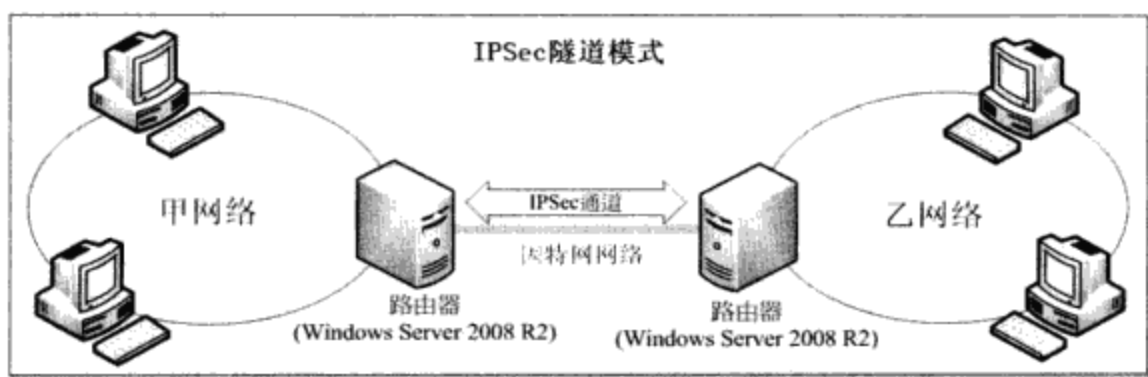


图 10-3

图中两台由Windows Server 2008 R2所扮演的路由器只有与对方通信时才使用IPSec。甲乙两个网络内的其他计算机并不需要使用IPSec, 这两个不同网络内的计算机要相互通信时, 会通过路由器来发送, 因而可以通过两个路由器之间的IPSec通信, 来确保数据在因特网上发送的安全性。

### 10-1-3 IPSec协议

您可以通过以下两种IPSec协议来保护数据发送的安全:

✎ **AH (Authentication Header):** AH会签署 (sign) 所发送的数据, 也就是它可以确认所收到的数据没有被篡改 (即确认数据完整性, integrity)、可以确认数据确实是由所要通信的计算机传来的 (身份验证, authentication)。不过AH却不会将数据加密。图 10-4 为IP数据包经过AH处理前后的数据包结构图。

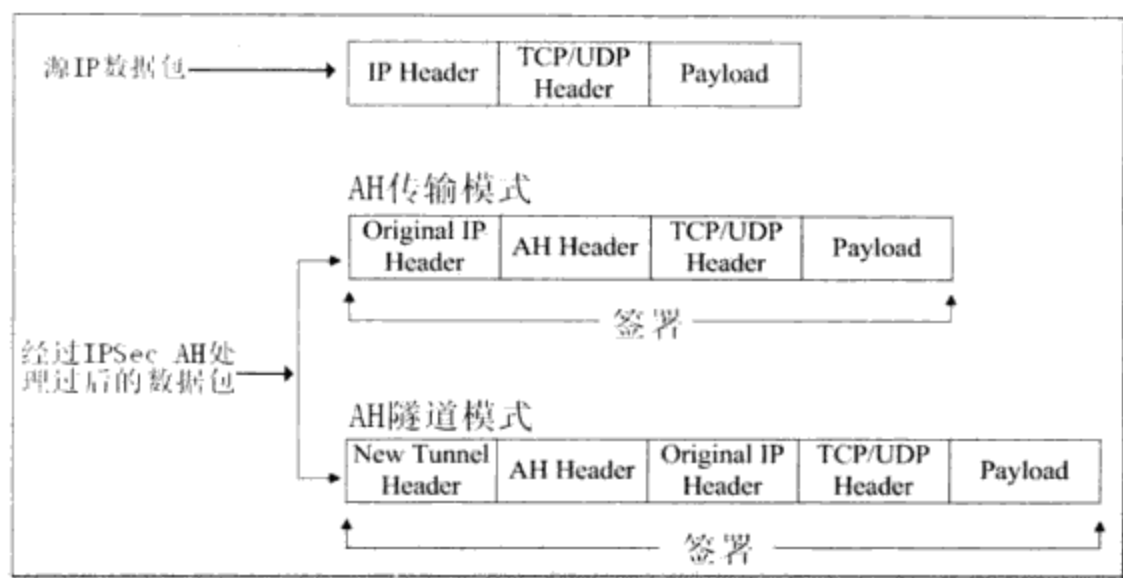


图 10-4

- **ESP (Encapsulating Security Protocol):** ESP也会签署所发送的数据, 也就是它可以确认所收到的数据没有被篡改, 可以确认数据确实是由所要通信的计算机传来的, 而且ESP会将数据加密 (encryption)。图 10-5为IP数据包经过ESP处理前后的数据包结构图。

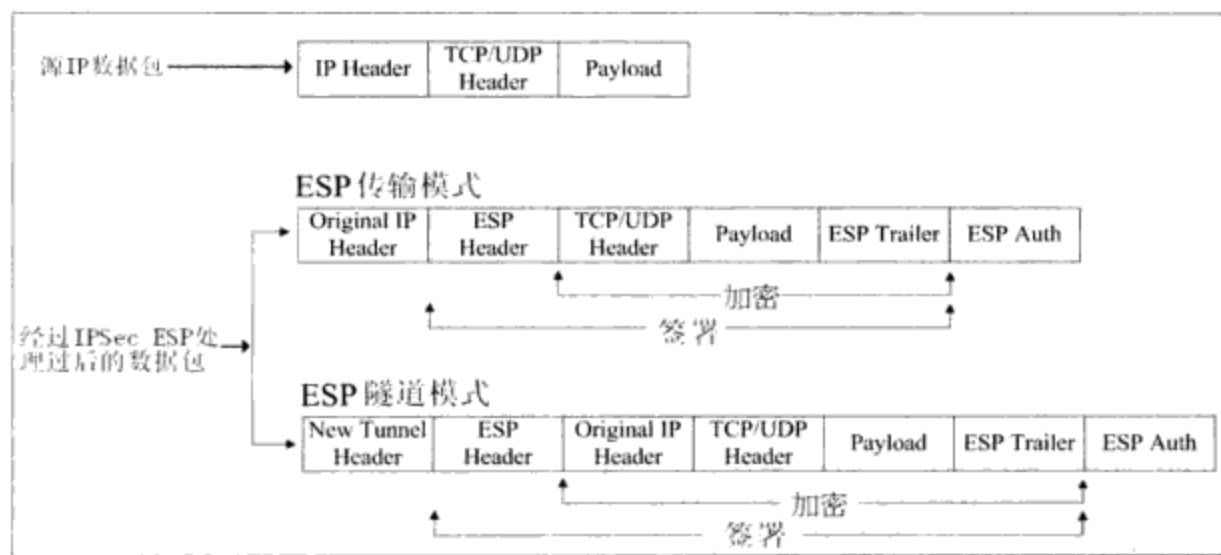


图 10-5

#### 10-1-4 Windows Server 2008 R2的IPSec设置

Windows Server 2008 R2 (或Windows Server 2008、Windows 7、Windows Vista) 计算机的IPSec可以通过新建**连接安全规则**来启用, 而**连接安全规则**的创建是通过**高级安全Windows防火墙**:

- **【开始 管理工具 高级安全Windows防火墙】:** 它适合您来新建本地计算机的**连接安全规则**。
- 到域控制器上选择**【开始 管理工具 组策略管理】:** 您可以通过组策略内的**高级安全Windows防火墙策略**, 来针对站台、域或组织单位内的一组计算机新建**连接安全规则**。

### 附注

通过高级安全Windows防火墙所新建的连接安全规则，只适用于Windows Server 2008 R2、Windows Server 2008、Windows 7与Windows Vista计算机，若要启用旧版Windows系统的IPSec的话，请通过自定义IP安全策略管理控制台来完成。

## 10-2 独立服务器之间的IPSec设置

我们将通过图 10-6来说明如何让图中的两台服务器利用IPSec来安全地通信。图中两台服务器都是Windows Server 2008 R2独立服务器，因此无法选择Kerberos V5验证方法，故此处我们采用**预共享密钥**（Preshared key）验证方法。请先按照图指示配置其IP地址与子网掩码。

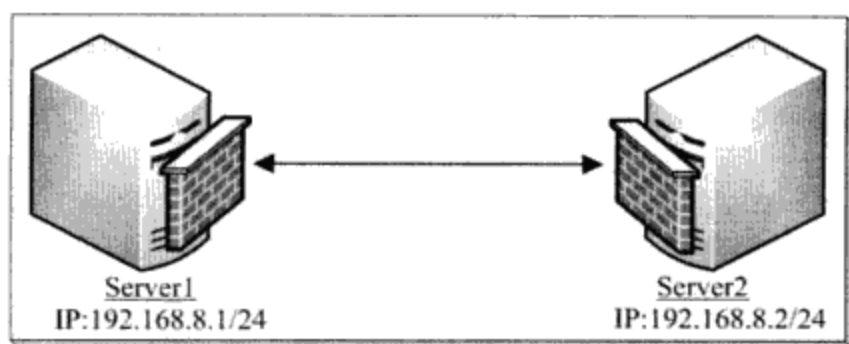


图 10-6

### 提示

系统是以明文（clear text）的方式来发送**预共享密钥**，比较不安全，因此只建议使用在测试环境。

**STEP 1** 我们将在下一个步骤通过ping命令来确认两台服务器之间确实可以正常通信，然而为了避免ping命令被**Windows防火墙**阻止，因此请先分别在两台服务器上开放ICMP的相关流量：选择【开始➤管理工具➤高级安全Windows防火墙➤如图 10-7所示单击入站规则中的文件和打印机共享（回显请求 - ICMPv4-In）➤单击右边的启用规则】。

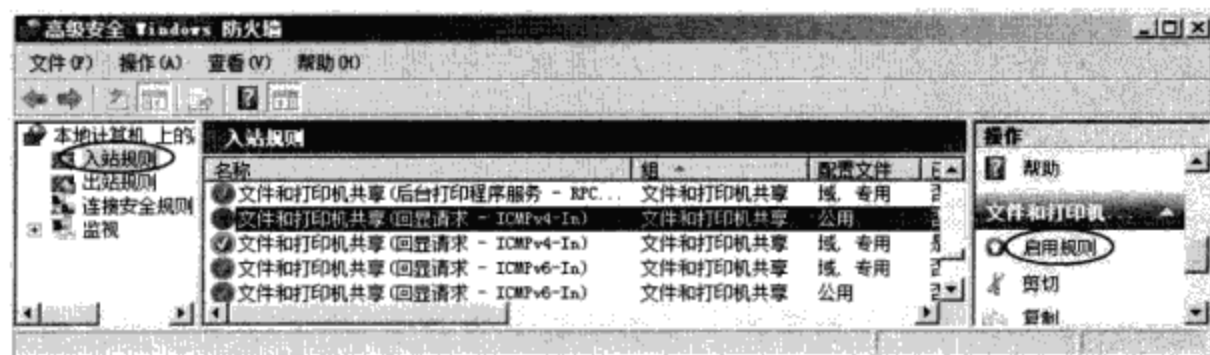


图 10-7

**注意**

请勿将Windows防火墙关闭，否则**连接安全规则**没有作用。

**STEP 2** 请先到Server1上利用ping 192.168.8.2来测试能否与Server2正常通信(如图 10-8所示为正常通信的界面);然后再到Server2上利用ping 192.168.8.1来测试能否与Server1正常通信。请务必执行此测试步骤,以减少之后排错的困难度。

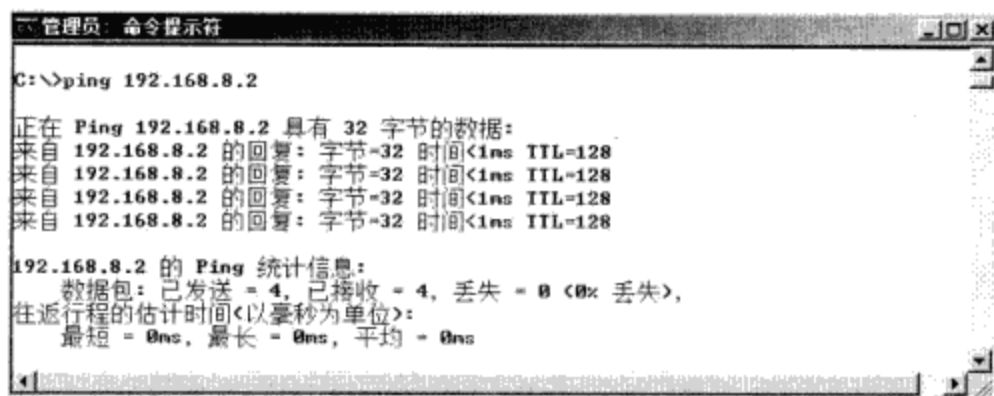


图 10-8

**STEP 3** 请先到Server1上选择【开始→管理工具→高级安全Windows防火墙→如图 10-9所示单击**连接安全规则**右边的**新建规则...**】。

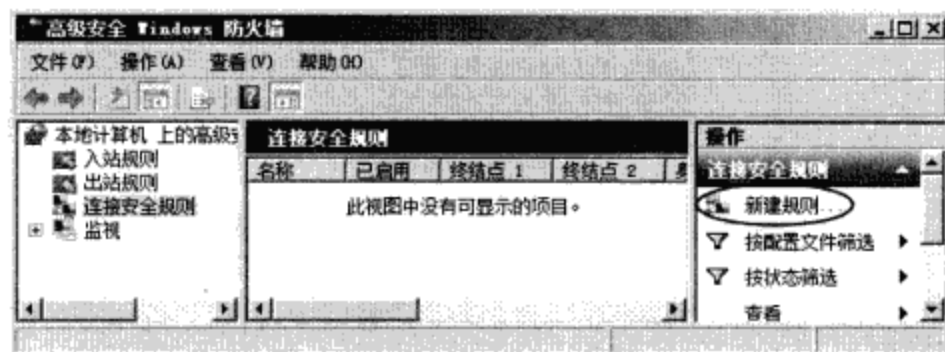


图 10-9

**STEP 4** 在图 10-10中选择默认的**隔离**类型后单击**下一步**。

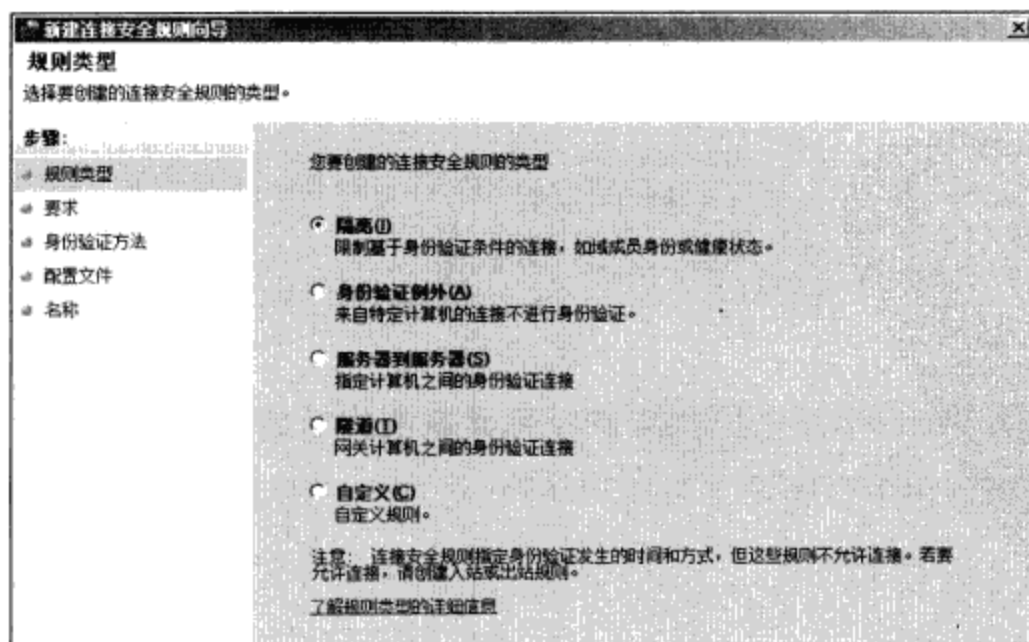


图 10-10



**STEP 5** 在图 10-11 中改选第3个选项后单击 **下一步**。图中的三个选项介绍如下：

- **入站和出站连接请求身份验证**：入站及出站连接都会请求对方采用IPSec。若无法与对方协商成功的话（例如对方不需具备IPSec功能），则采用一般连接方式即可。
- **入站连接要求身份验证，出站连接请求身份验证**：入站连接必须采用IPSec，否则拒绝连接；出站连接仅会请求对方采用IPSec，若无法与对方协商成功的话，则采用一般连接方式即可。
- **入站和出站连接要求身份验证**：无论入站或出站连接都必须采用IPSec，否则拒绝连接。

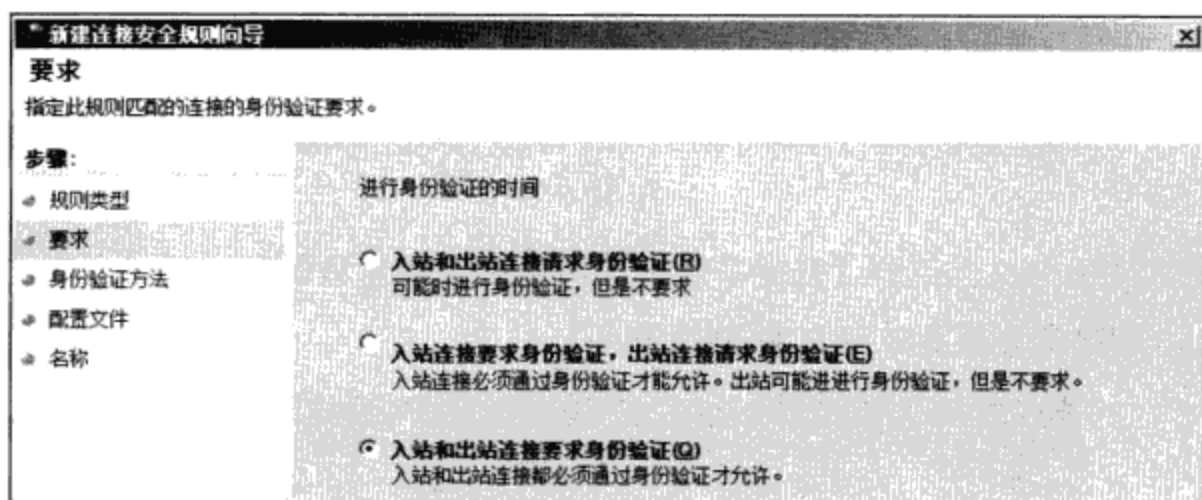


图 10-11

**STEP 6** 在图 10-12 中单击高级处的 **自定义** 来选择 **预共享密钥** 验证方法。

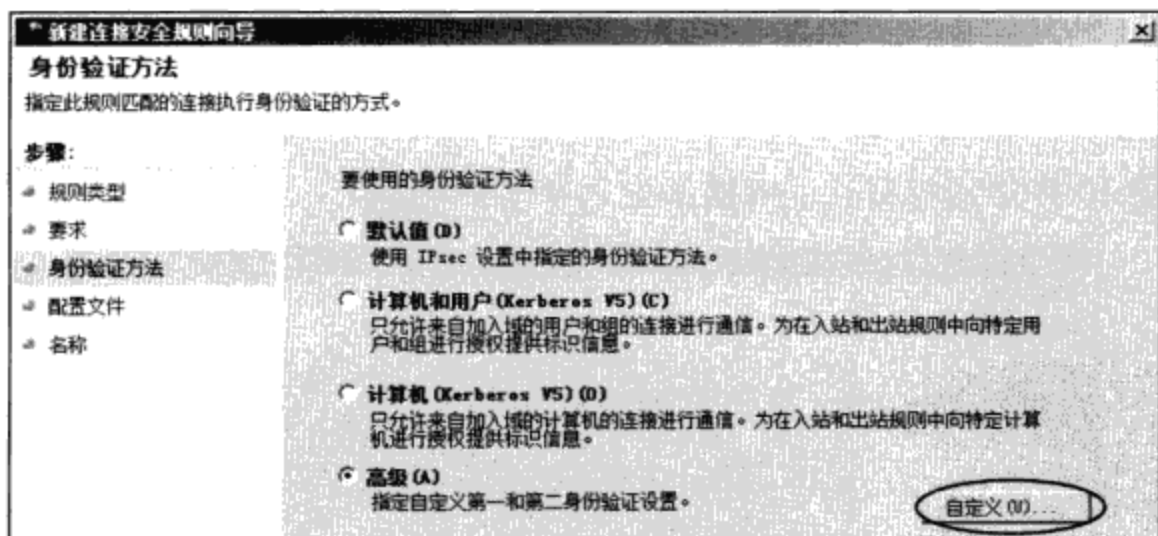


图 10-12

**STEP 7** 请【在图 10-13 中单击 **添加** ➡ 选择 **预共享密钥** 后输入密钥字符串 ➡ 单击 **确定**】，图中我们将密钥字符串设置为 1234567。对方也必须设置相同的密钥字符串。



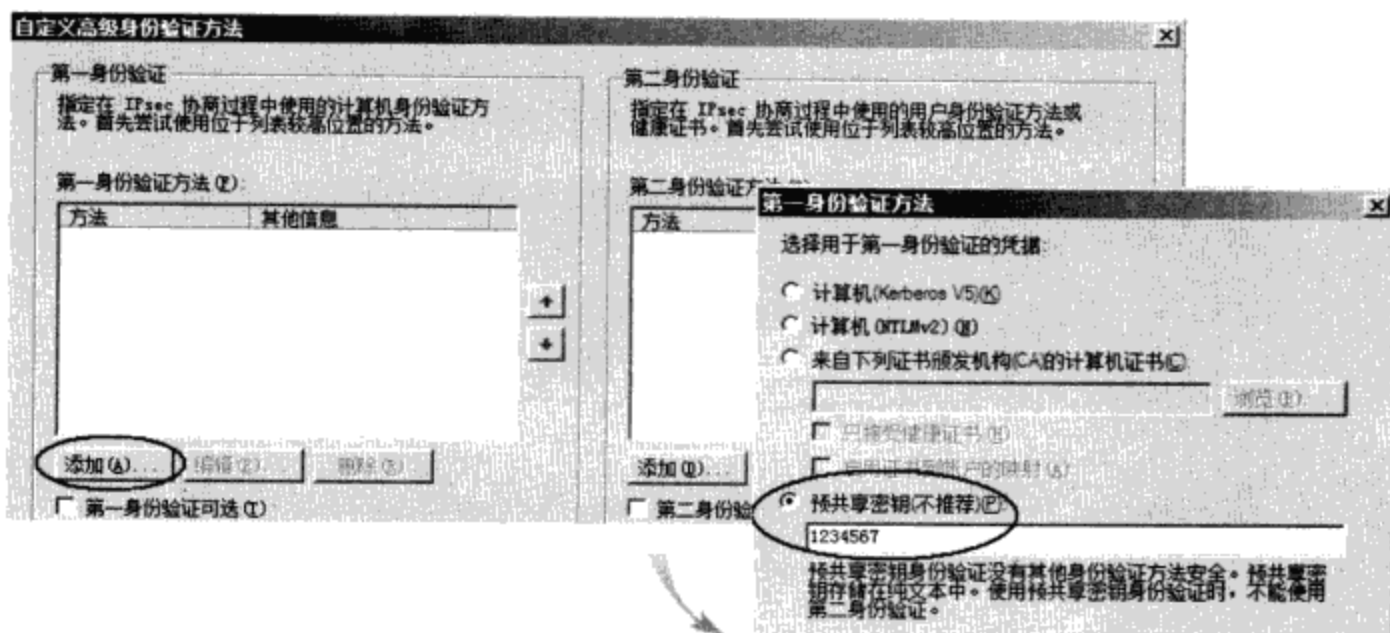


图 10-13

**STEP 8** 回到自定义高级身份验证方法的界面后单击**确定**，回到身份验证方法的界面时单击**下一步**。

**STEP 9** 您可以在图 10-14 中选择此计算机何时要应用此规则，之后单击**下一步**：

- **域**：当此计算机连接网络时，若能够与域控制器通信的话，就应用此规则。
- **专用**：当此计算机连接专用网时，若无法与域控制器通信或该计算机非域成员的话，就应用此规则。
- **公用**：当此计算机连接到公用网络时，就应用此规则。

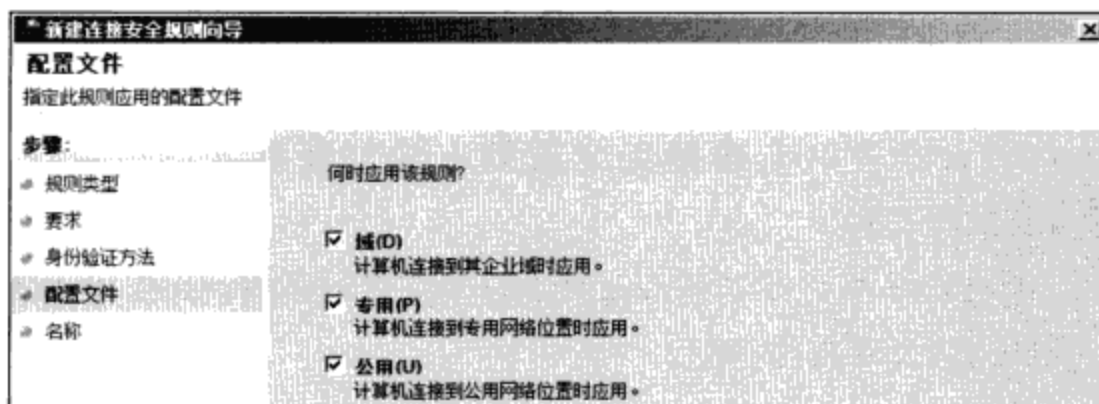


图 10-14

**STEP 10** 在图 10-15 中为此规则命名后单击**完成**。

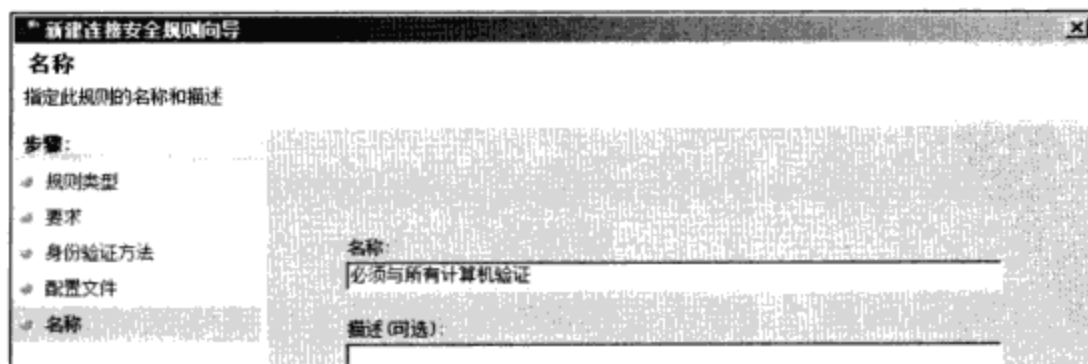


图 10-15

**STEP 11** 图 10-16为完成后的界面。您可以双击此规则来更改规则设置，也可以通过【对着此规则单击右键 $\Rightarrow$ 禁用规则】的方式来禁用此规则。

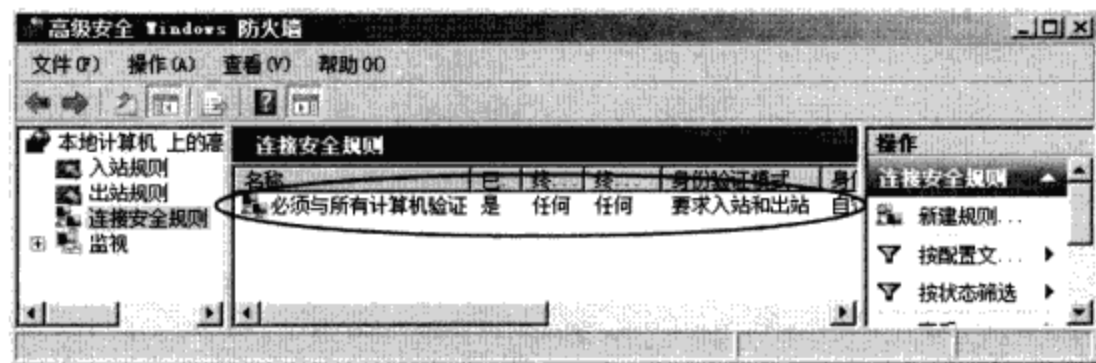


图 10-16

**STEP 12** 由于我们所新建的规则要求无论入站或出站连接都必须采用IPSec，然而目前Server2尚未新建**连接安全规则**，也就是尚未启用IPSec，故此时若在Server1上利用ping命令来与Server2通信的话，会被Server1拒绝，并显示如图 10-17请求超时的信息。

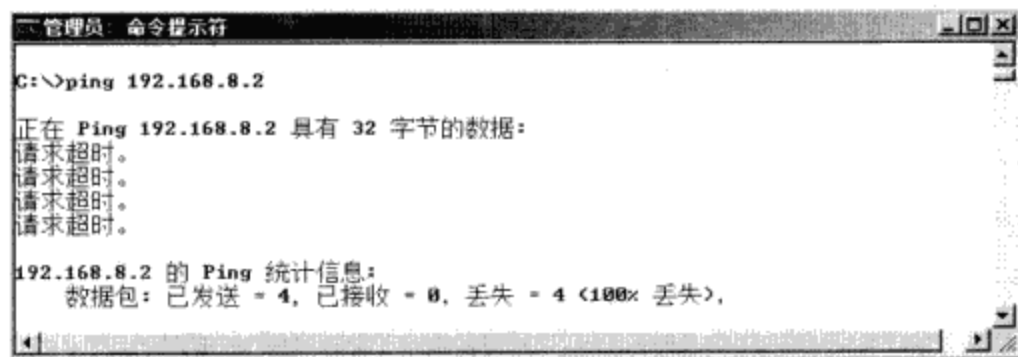


图 10-17

**STEP 13** 换到Server2上来新建相同设置的**连接安全规则**：选择【开始 $\Rightarrow$ 管理工具 $\Rightarrow$ 高级安全Windows 防火墙 $\Rightarrow$ 单击**连接安全规则**右边的**新建规则...** $\Rightarrow$ 重复**STEP 4**到**STEP 10**的步骤】。

**STEP 14** 完成后，两台服务器之间利用ping命令应该就可以通信，如图 10-18所示为在Server2上执行ping 192.168.8.1的界面。

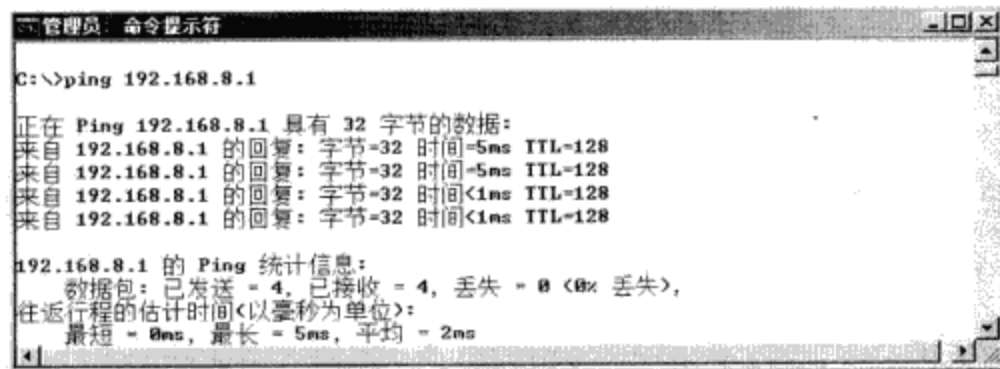


图 10-18

**STEP 15** 如图 10-19所示可通过【单击**监视** $\Rightarrow$ **安全关联** $\Rightarrow$ **主模式或快速模式**】来查看主模式SA或快速模式SA的相关数据。

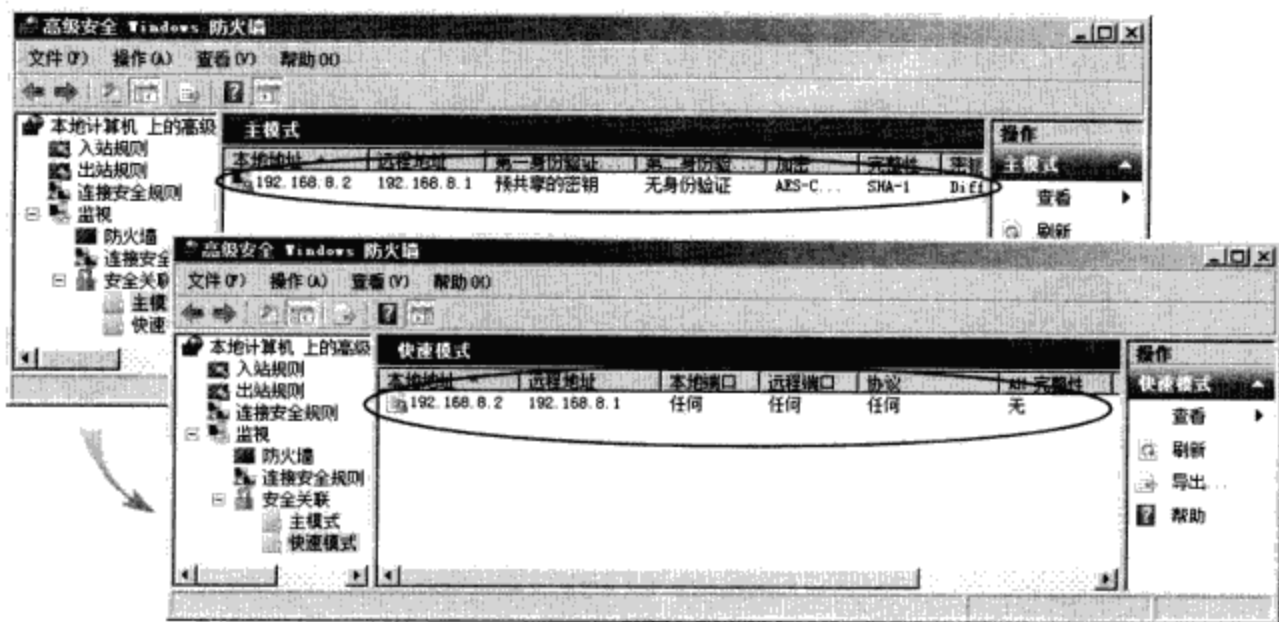


图 10-19

若要更改IPSec默认值的话，请选择【如图 10-20所示对着本地计算机上的高级安全 Windows 防火墙单击右键→属性→IPSec设置标签→单击IPSec默认值右边的自定义】，以后所新建的连接安全规则就会采用此默认值。

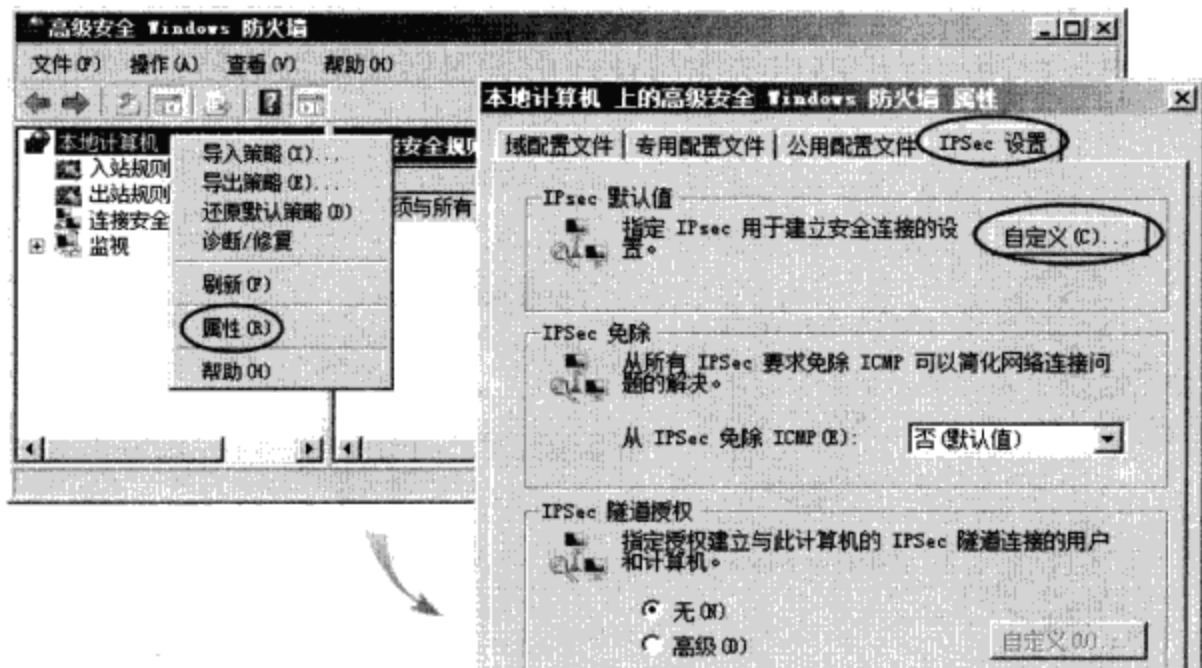


图 10-20

图中您也可以通过IPsec免除来将ICMP排除，也就是只要是ICMP流量都不需要利用IPSec来通信，这个设置可让您利用ping命令来检测网络计算机之间的通信是否正常时，免于遭受IPSec的干扰。

### 10-3 路由器的IPSec设置

分别位于两地的网络之间若要通过因特网来安全发送数据的话，可以在两地的路由器之间创建IPSec隧道 (tunnel)，如图 10-21所示，图中只有两台路由器之间相互通信才需要IPSec，

例如当甲网络内的计算机要与乙网络内的计算机通信时，它会以一般方式将数据传给甲路由器，再由甲路由器通过**IPSec隧道**将数据传给乙路由器，最后再由乙路由器以一般方式将数据传给乙网络的计算机。

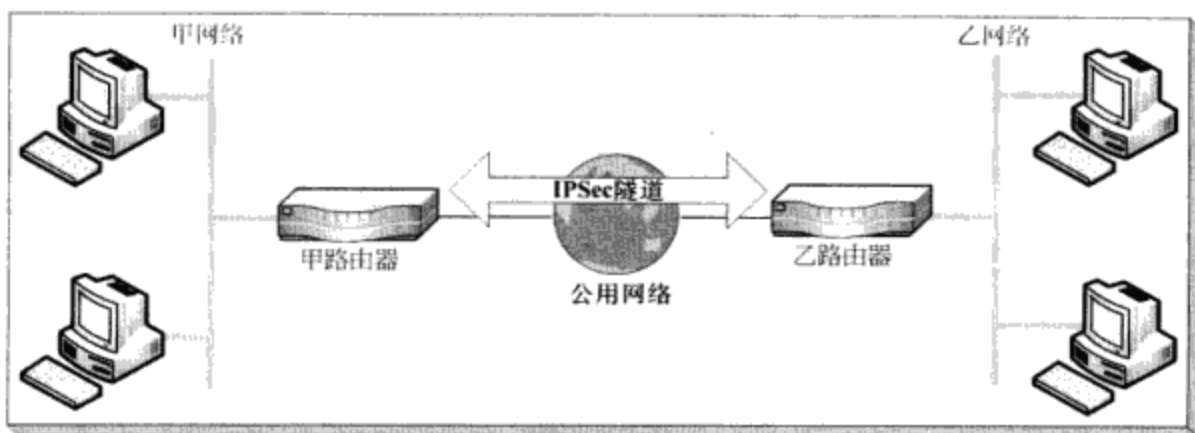


图 10-21

我们将通过图 10-22来说明如何在图中两台扮演路由器角色的Windows Server 2008 R2服务器之间创建IPSec隧道。图中两台服务器都是独立服务器，因此无法选择Kerberos V5验证方法，故此处采用**预共享密钥**（Preshared key）验证方法。请先按照图指示配置其IP地址与子网掩码，并启用两台路由器的路由功能与在路由表内创建适当的路径（需先参考章节11-2的说明）。

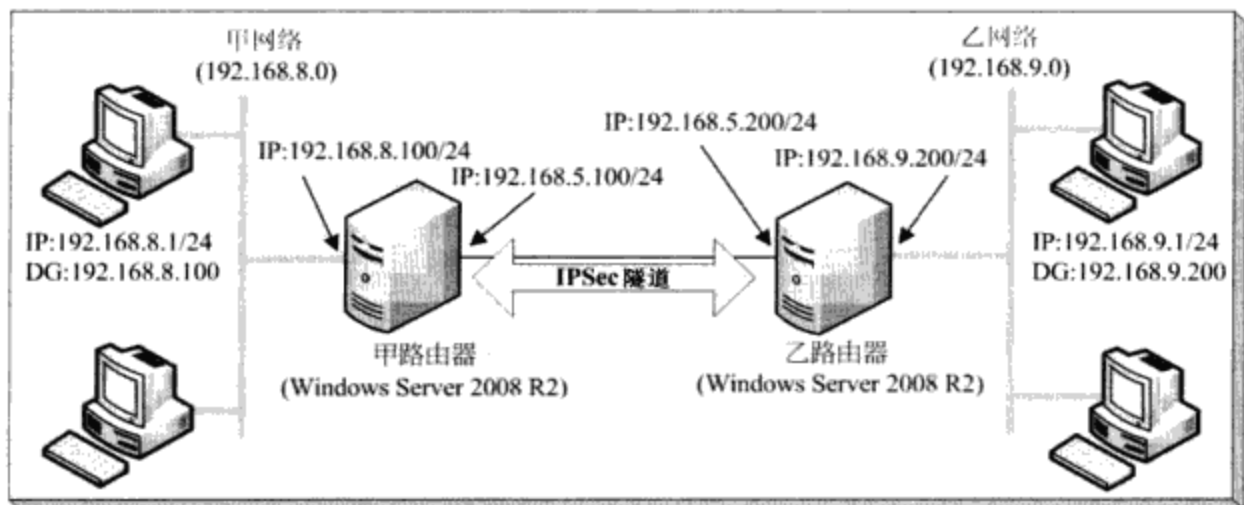


图 10-22



**提示**

系统是以明文（clear text）的方式来发送**预共享密钥**，比较不安全，因此只建议使用在测试环境。

由于新建**连接安全规则**的方法与前一小节类似，因此本节将只说明不同之处。在两台Windows Server 2008 R2路由器通过**高级安全Windows防火墙**来新建**连接安全规则**时，请如图10-23所示选择**隧道、自定义配置**。

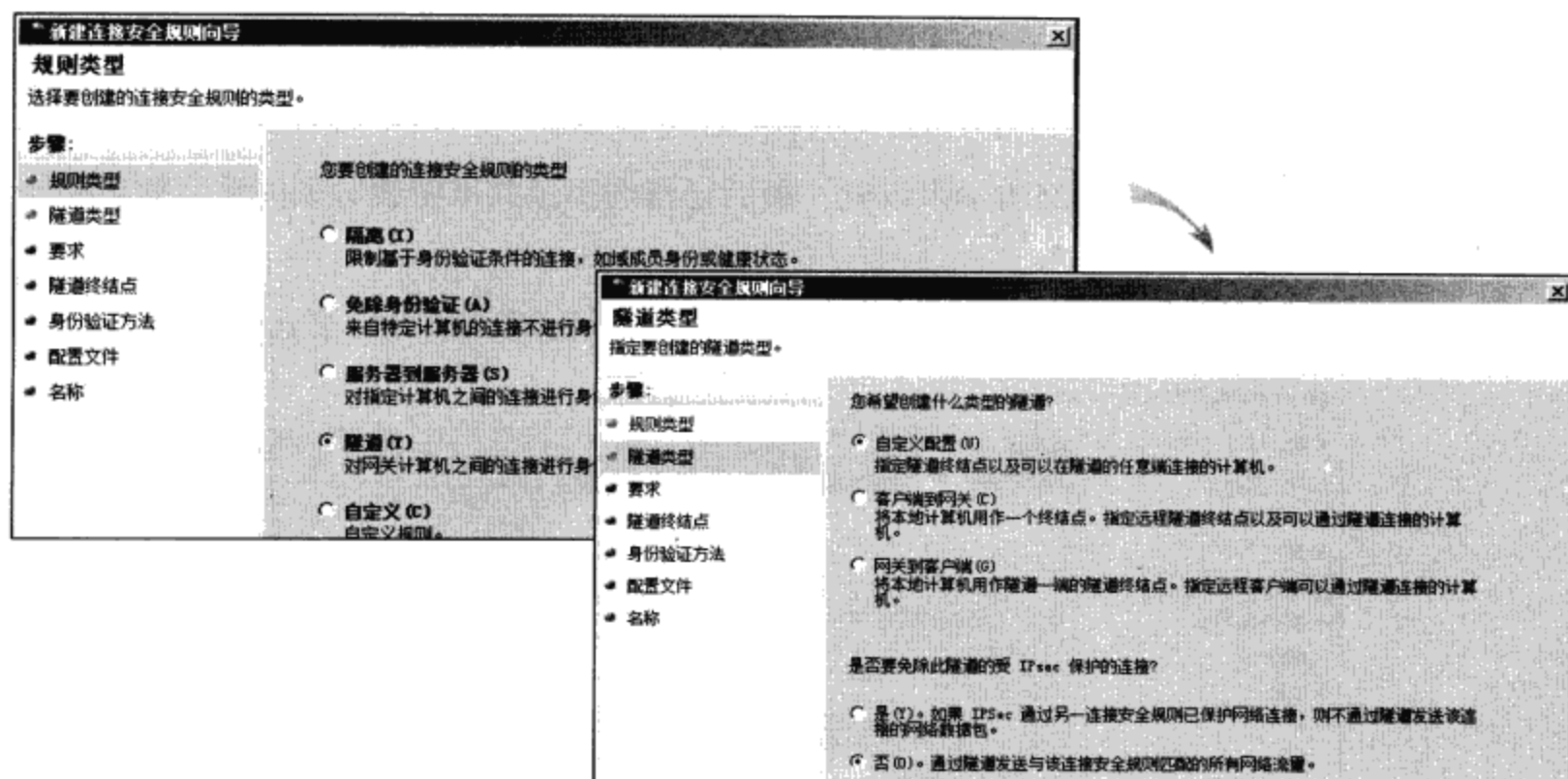


图 10-23

接着在甲路由器需如图 10-24所示来设置（最后记得选择**预共享密钥**验证方法，假设密钥字符串为1234567）：

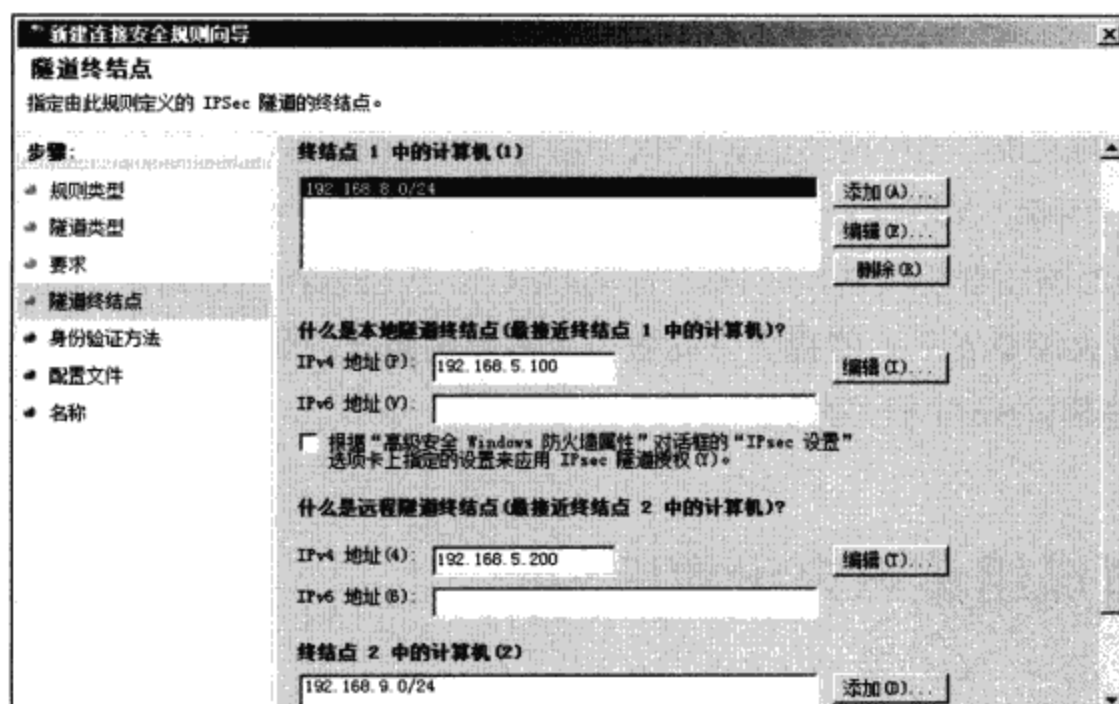


图 10-24

- **终结点1中的计算机：** 请将本地网络（图 10-22中的甲网络）内的计算机的IP地址或网络标识符（network ID）输入到此处，图中我们输入网络标识符192.168.8.0/24。
- **什么是本地隧道终结点（最接近终结点1中的计算机）：** 设置IPSec信道在本地网络（甲网络）这一端的端点，也就是将甲路由器的外网卡的IP地址192.168.5.100输入到此处。
- **什么是本地隧道终结点（最接近终结点2中的计算机）：** 设置IPSec信道在远程网络（乙网络）那一端的端点，也就是将乙路由器的外网卡的IP地址192.168.5.200输入到此处。

- **终结点2中的计算机:** 请将远程网络（乙网络）内的计算机的IP地址或网络标识符输入到此处，图中我们输入网络标识符192.168.9.0/24。

同理在乙路由器需如图 10-25所示来设置（最后记得选择**预共享密钥**验证方法，假设密钥字符串为1234567）：

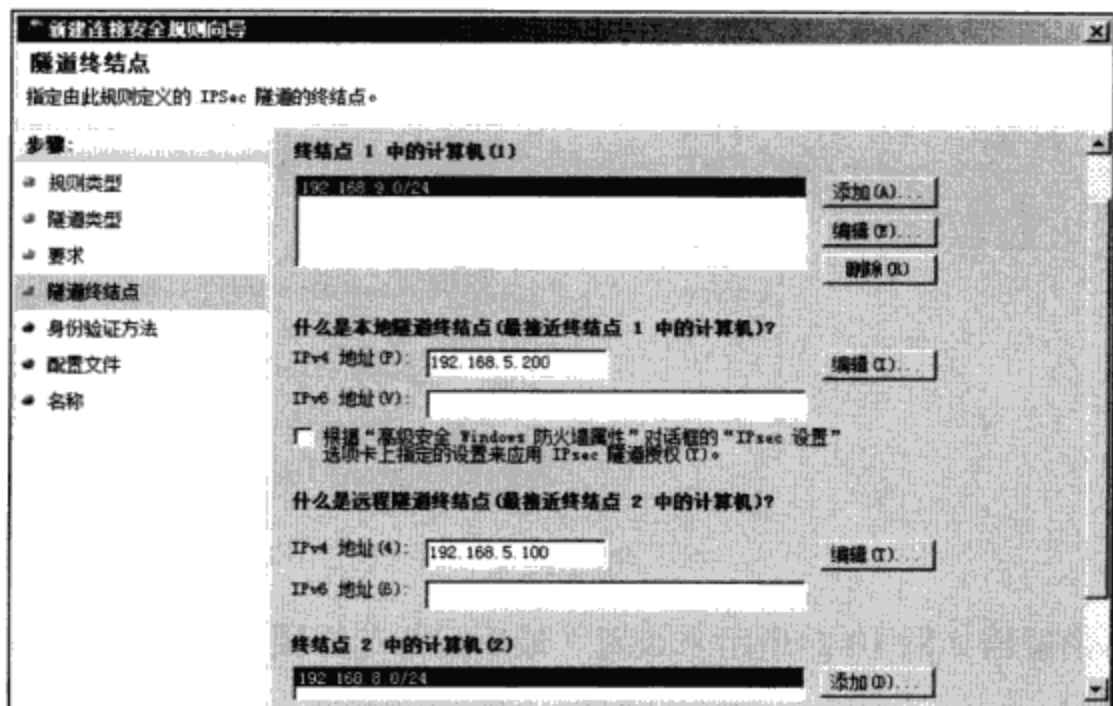


图 10-25

甲乙两个路由器分别完成建立**连接安全规则**后，在两个网络之间便可以通过**IPSec隧道**来安全地通信，举例来说，当甲网络的Win7PC1要与乙网络的Win7PC2通信时，其数据包会先发送给甲路由器，甲路由器便会自动与乙路由器建立**IPSec信道**，然后通过此信道将数据包传给乙路由器，再由乙路由器将其传给乙网络的Win7PC2。您可以在两台路由器上通过【打开**高级安全Windows防火墙**➤展开到**监视**之下的**安全关联**➤主模式或快速模式】来查看IPSec信道的主模式SA或快速模式SA的相关数据。

## 10-4 通过域组策略来设置IPSec

您可以针对Active Directory域的站点、域或组织单位的组策略来新建**连接安全规则**，以便让域成员计算机之间能够利用IPSec来安全通信。由于这些计算机都是隶属于域，因此可以选择Kerberos V5验证方法。

我们需将Active Directory域控制器排除，也就是让域成员与域控制器之间的通信不使用IPSec，因为域成员在利用IPSec验证域控制器之前，就必须先要能够与它们正常通信。域控制器这类型的计算机被称为**基础架构计算机**，除了域控制器之外，CA（Certificate Authority）与DHCP服务器等也是隶属于**基础架构计算机**。若某些计算机或设备（例如路由器）不支持我们

在**连接安全规则**中所选择的协议或不支持IPSec的话，则也必须将它们排除在外。

我们将通过图 10-26来说明，图中左边甲网络的3台计算机都是Windows Server 2008 R2，其中DC是域控制器，而服务器Server1与Server2都是域成员服务器。假设甲网络内的所有域成员计算机相互之间都需要利用IPSec来通信，但是将域控制器DC（192.168.8.200）与路由器（192.168.8.254）排除在外。

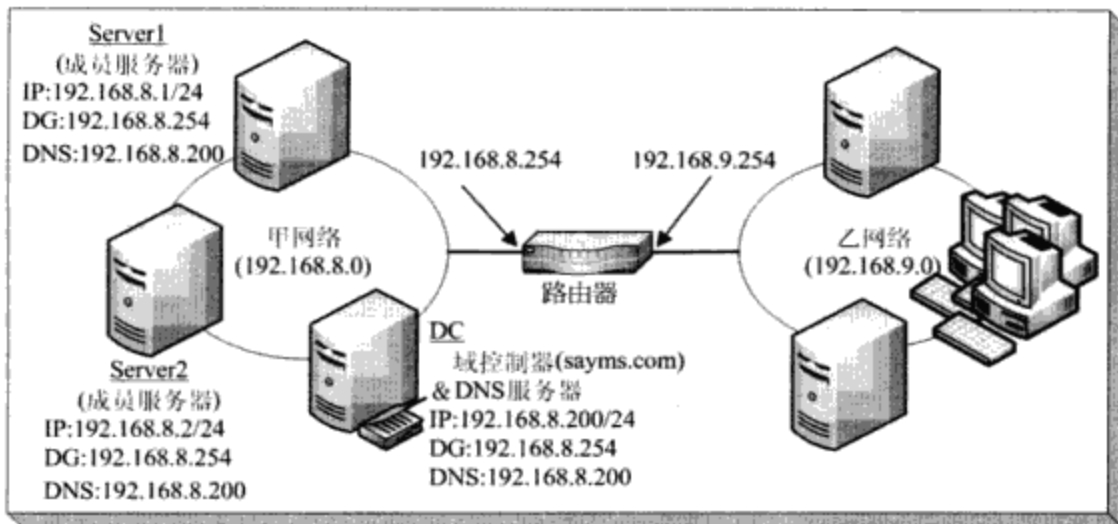


图 10-26

以下将通过Default Domain Policy组策略对象（GPO）来新建**连接安全规则**与排除规则。请先按照图设置好左边3台服务器的IP地址、子网掩码、默认网关、首选DNS服务器，然后创建域与域控制器、将Server1与Server2加入域。可以的话，也可以安装路由器（见第11章）以便做进一步的测试。

**STEP 1** 我们将在下一个步骤通过ping命令来确认图 10-26中左边3台服务器之间确实可以正常通信，然而为了避免ping命令被**Windows防火墙**阻止，因此请先分别在Server1与Server2上开放ICMP的相关流量：**【开始☞管理工具☞高级安全Windows防火墙☞单击入站规则中的文件和打印机共享（回显请求 - ICMPv4-In）☞单击右边的启用规则】**。域控制器DC默认已开放，不需另外开放。



#### 注意

请勿将Windows防火墙关闭，否则连接安全规则没有作用。

**STEP 2** 请分别到每一台服务器上利用ping命令来测试是否可以与其他2台服务器、路由器正常通信，以便稍后来验证我们的设置。

**STEP 3** 请到域控制器DC上选择 **【开始☞管理工具☞组策略管理☞如图 10-27所示展开到域 sayms.com☞对着Default Domain Policy单击右键☞编辑】**。



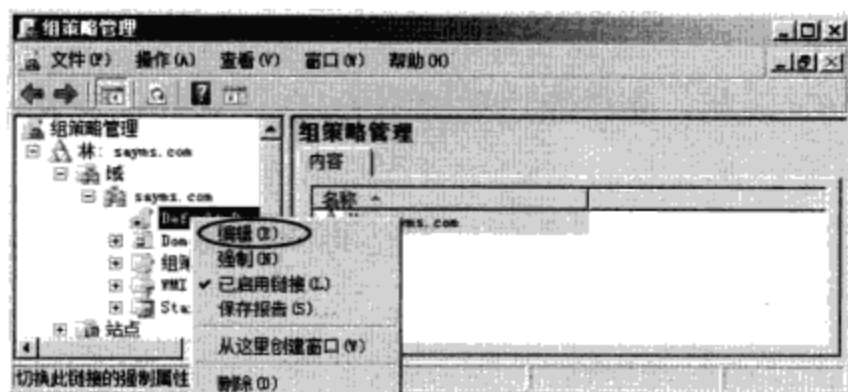


图 10-27

**STEP 4** 如图 10-28 所示【展开计算机配置策略 Windows 设置安全设置高级安全 Windows 防火墙高级安全 Windows 防火墙对着连接安全规则单击右键新建规则】。

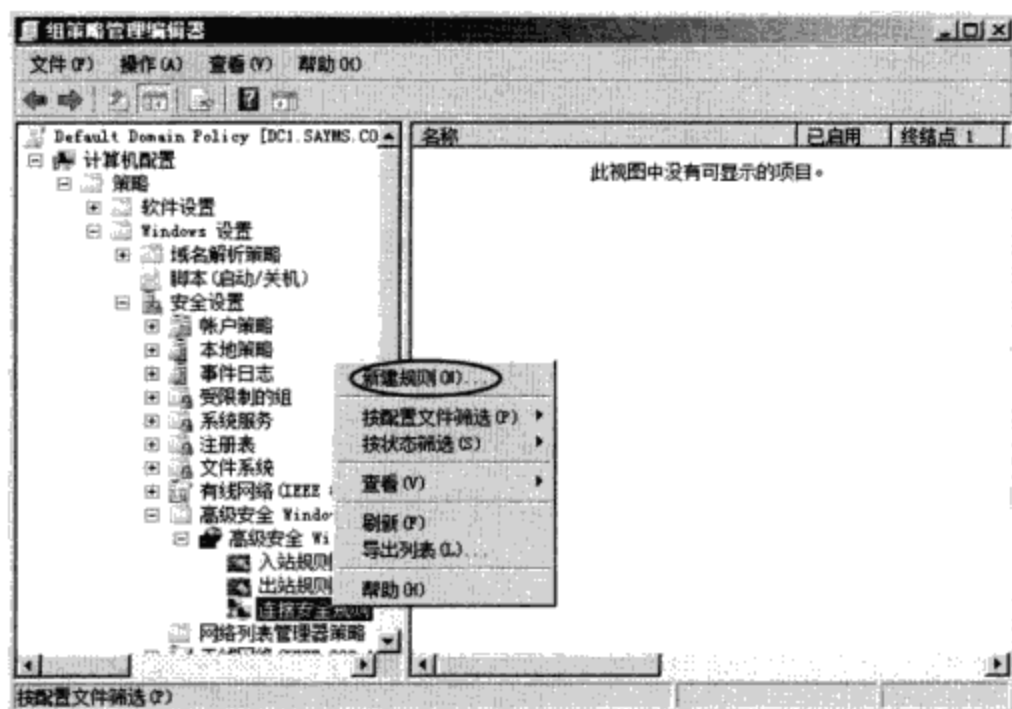


图 10-28

**STEP 5** 我们要先创建一个将域控制器与默认网关（路由器）排除的规则。请在图 10-29 中选择身份验证例外后单击下一步。

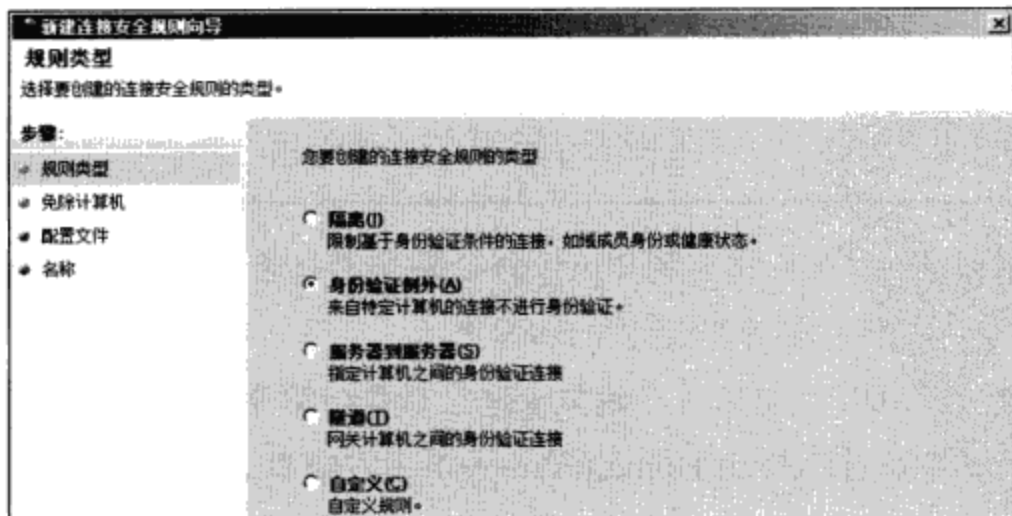


图 10-29

**STEP 6** 如图 10-30 所示【单击添加输入要被排除的域控制器的 IP 地址 192.168.8.200 单击

击**确定**】。

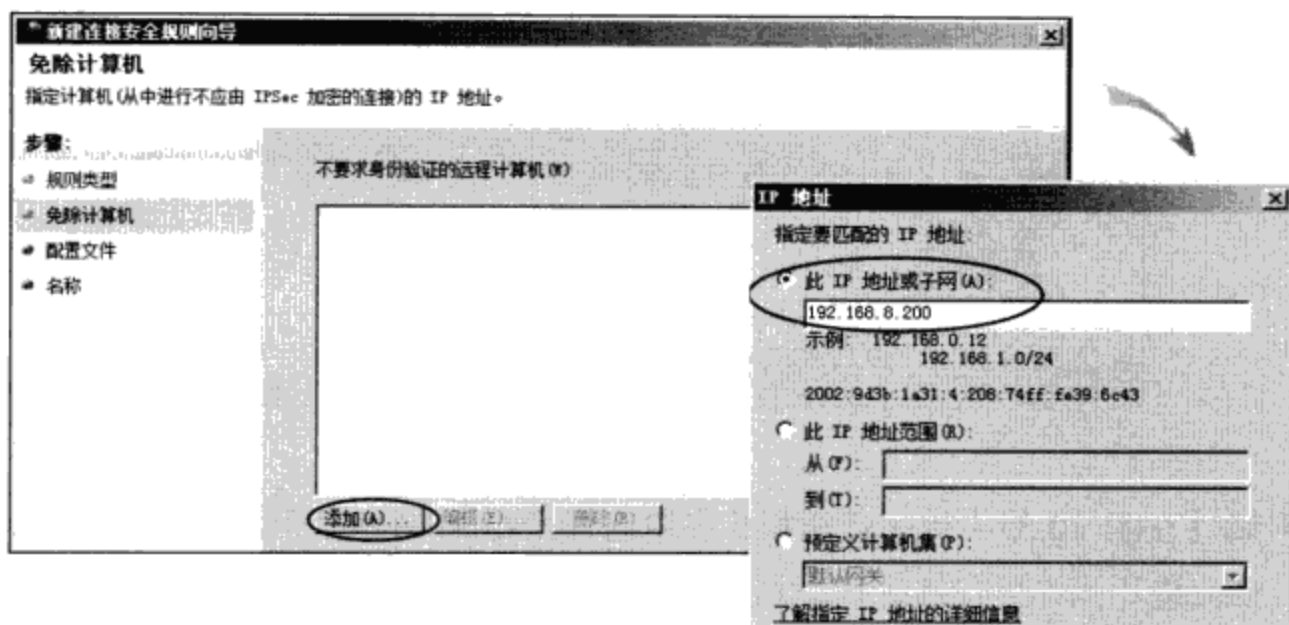


图 10-30

**STEP 7** 如图 10-31 所示【继续单击**添加**在**预定义计算机集**中选择**默认网关**单击**确定**】。您也可以如前一个步骤所示自行在此**IP 地址或子网**处输入默认网关的 IP 地址 192.168.8.254。

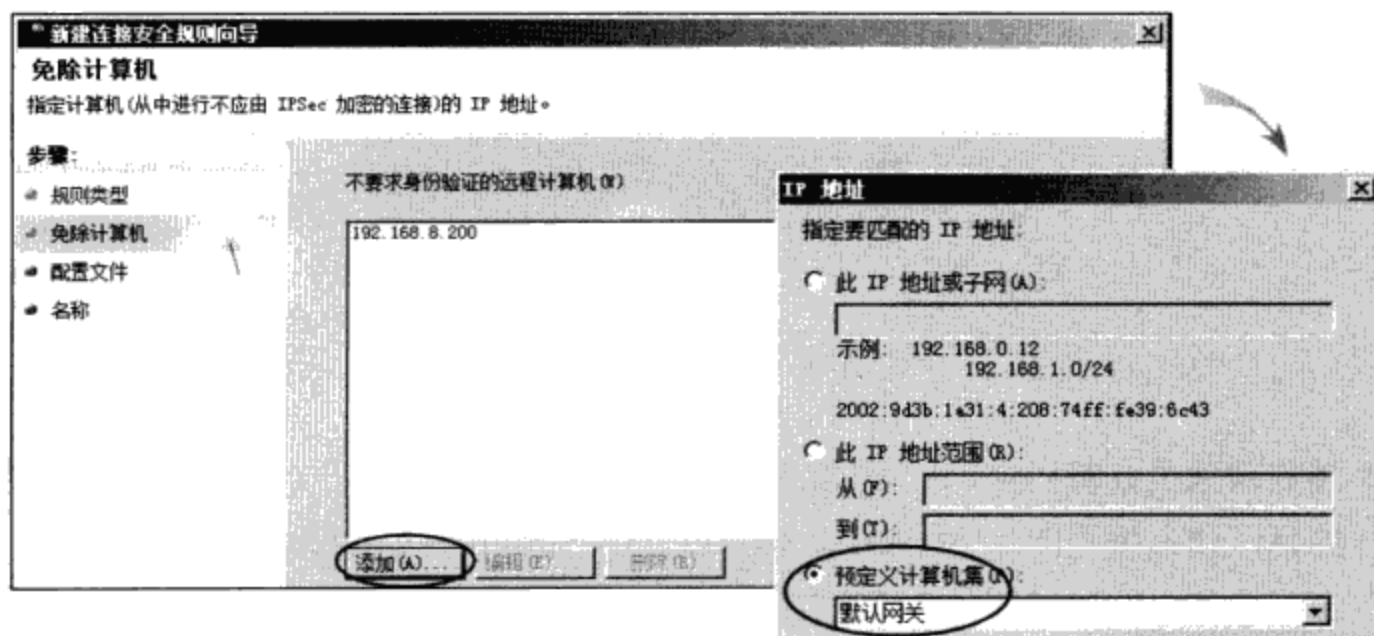


图 10-31

**提示**

系统内置了一些**计算机集** (computer set) 供您直接来选择, 例如默认网关、DHCP 服务器、WINS 服务器、DNS 服务器与本地子网等。

**STEP 8** 回到**免除计算机**界面时单击**下一步**。

**STEP 9** 在**配置文件**界面中单击**下一步**。

**STEP 10** 在**名称**界面中为此规则设置一个友好的名称, 例如**排除域控制器与默认网关**。单击**完成**。

**STEP 11** 双击图 10-32中刚才所新建的排除规则。

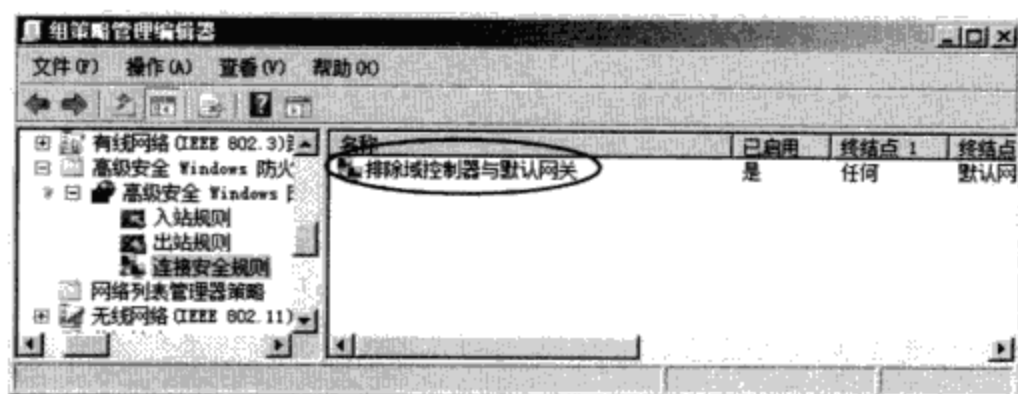


图 10-32

**STEP 12** 请【在图 10-33中单击**计算机**标签选择终结点1处的下列IP地址通过单击**添加**来添加图中所示的IP地址192.168.8.0/24】，此图表示终结点1处192.168.8.0/24子网内的所有计算机与终结点2处的默认网关、192.168.8.200之间相互通信时不需要使用IPSec。

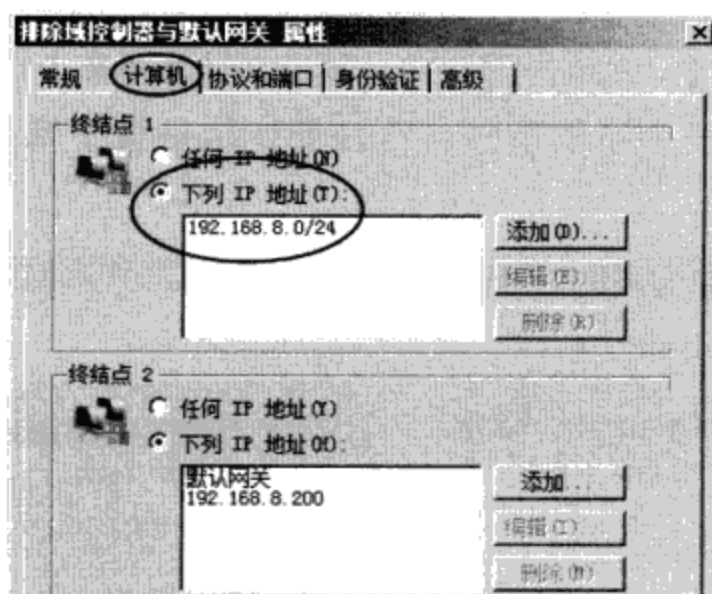


图 10-33

**STEP 13** 请等域成员计算机自动或手动应用组策略设置后再继续下一个步骤。若要手动应用的话，请直接到DC、Server1与Server2上执行**gpupdate /force**命令，然后分别在这3台服务器上通过【开始**管理工具**高级安全Windows防火墙**连接安全规则**】来查看是否已经应用成功，若应用成功的话，该规则就会如图 10-34所示显示在界面上。请务必确认这3台计算机都成功应用此规则后再继续下一个步骤。

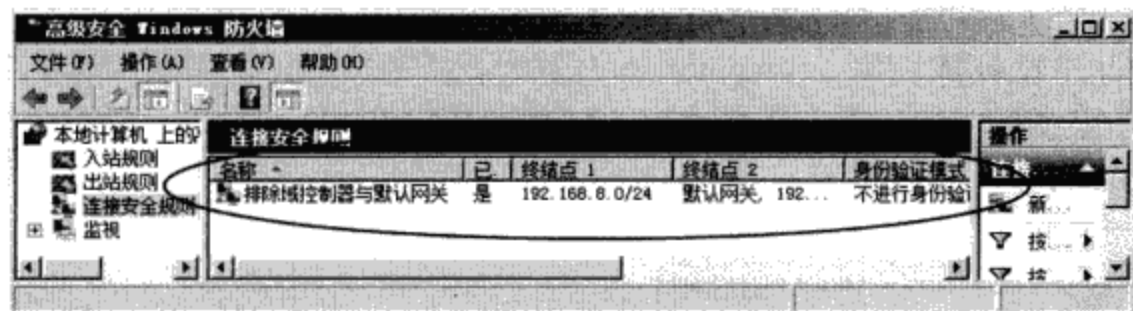


图 10-34

**STEP 14** 接下来我们将新建一个要求域成员之间需IPSec的规则。请继续编辑组策略：如图 10-35所示【对着连接安全规则单击右键新建规则】。

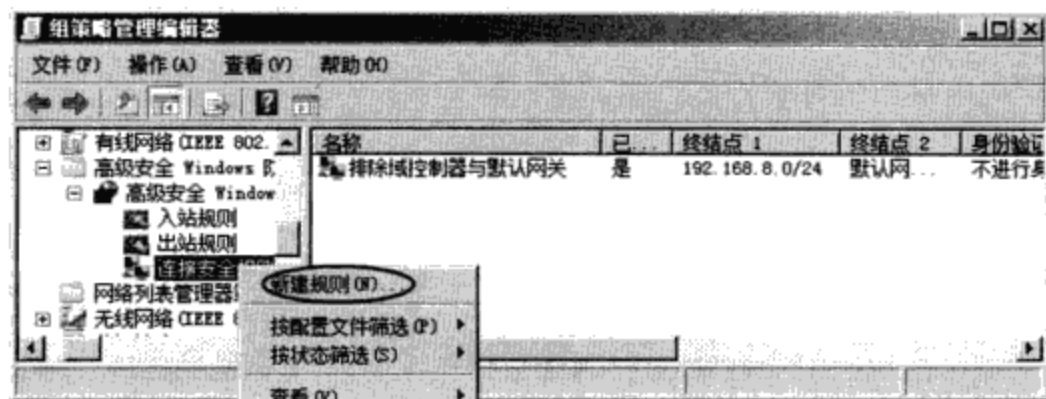


图 10-35

**STEP 15** 在图 10-36中选择服务器到服务器后单击下一步。

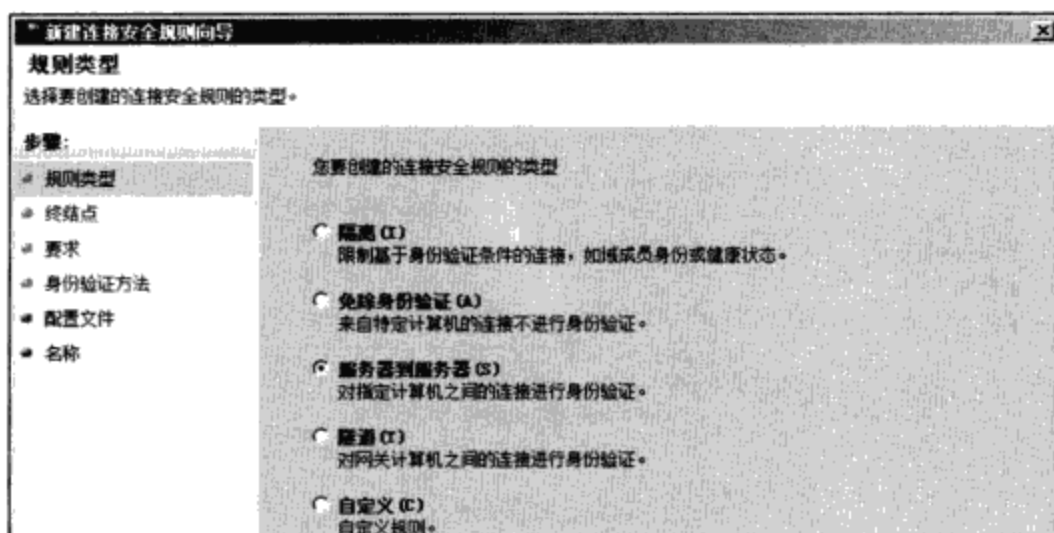


图 10-36

**STEP 16** 在图 10-37通过单击添加来设置终结点1与终结点2内的IP地址范围，表示终结点1与终结点2之间的服务器相互通信时需IPSec。图 10-37为完成设置后的界面，图中终结点1与终结点2我们都将其设置为192.168.8.0这个子网。

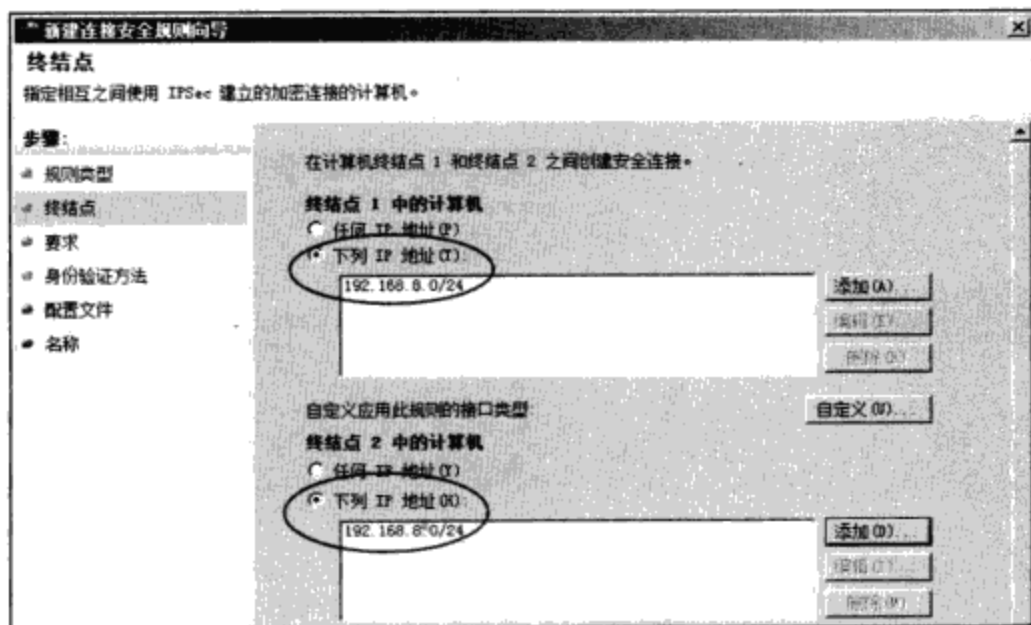


图 10-37

**STEP 17** 在图 10-38 选择入站和出站连接需要身份验证后单击 **下一步**。

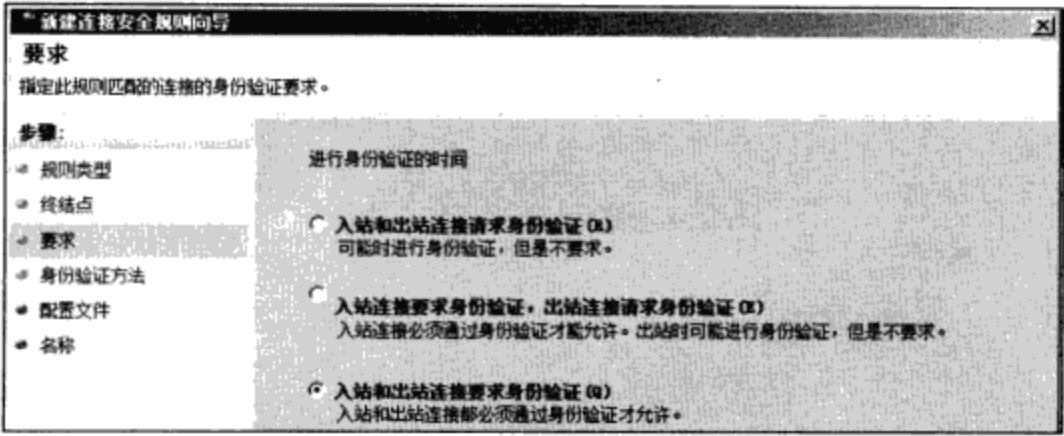


图 10-38

**STEP 18** 通过图 10-39 中高级处的 **自定义** 来选择 Kerberos V5 验证。

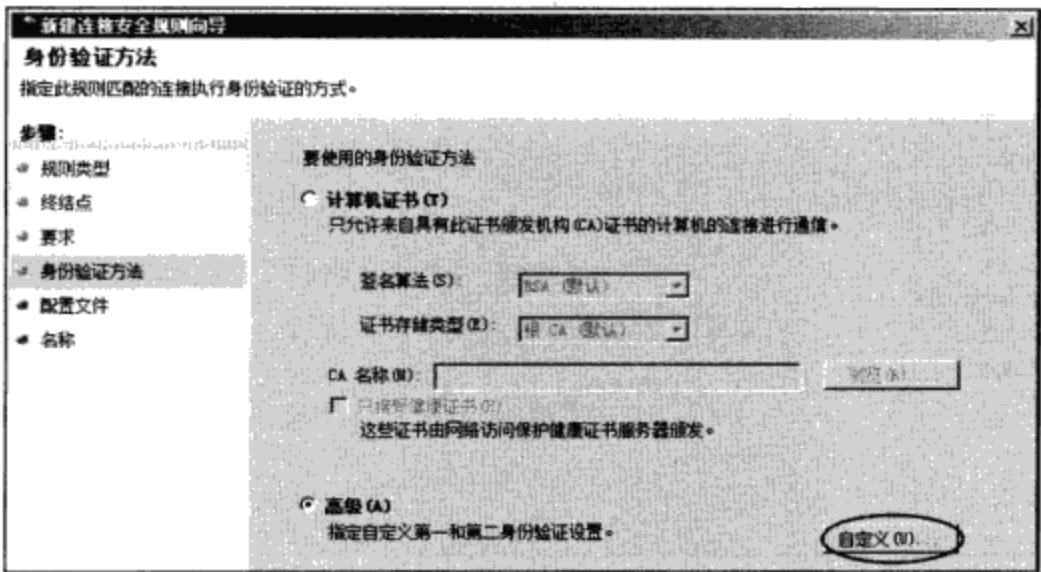


图 10-39

**STEP 19** 在图 10-40 中 **单击添加**  选择计算机 (Kerberos V5)  **单击确定**。

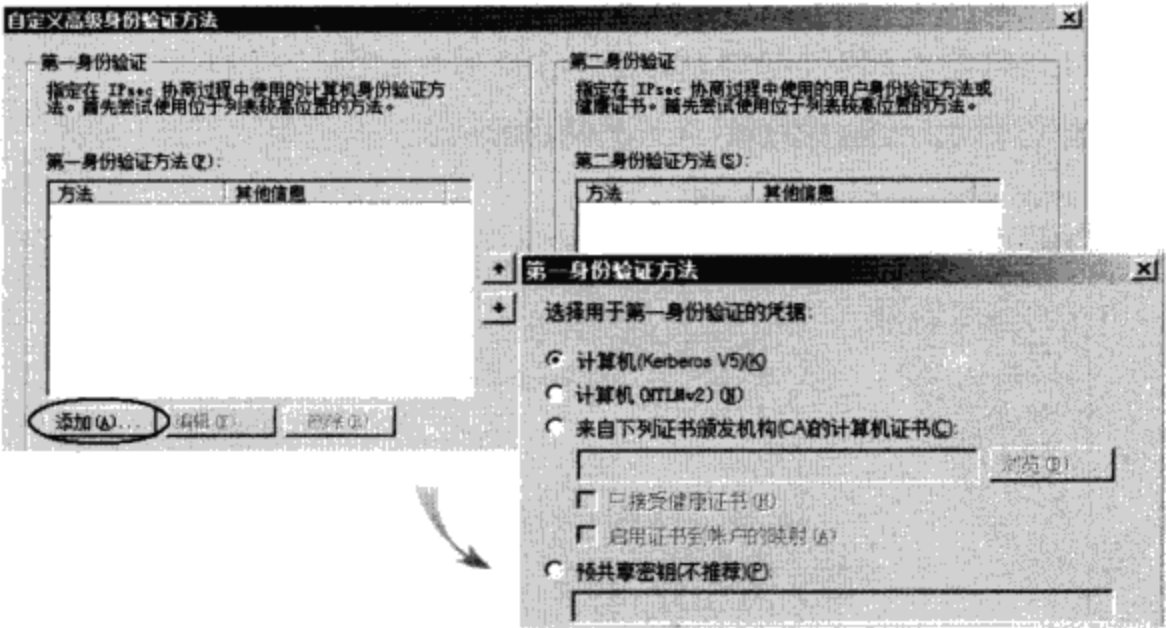


图 10-40

**STEP 20** 回到图 10-41 的界面时单击 **确定**。

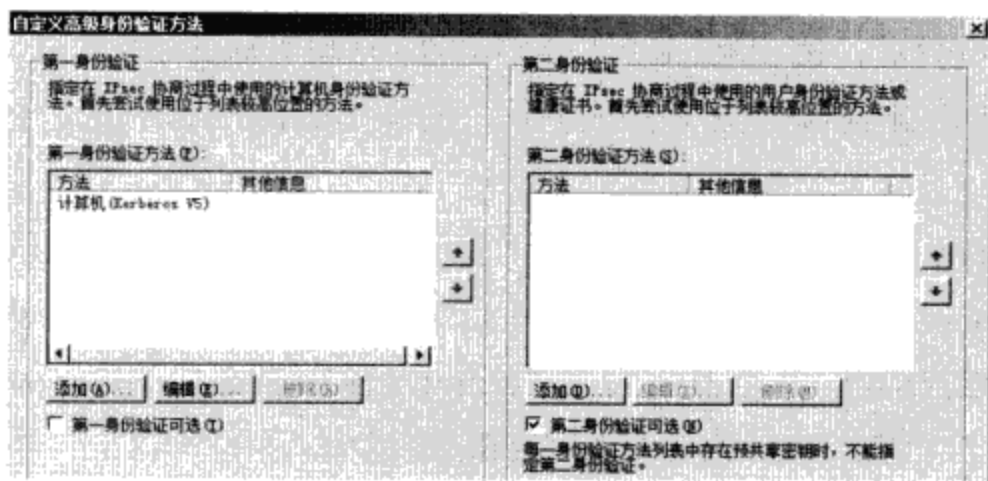


图 10-41

**提示**

图中只验证计算机身份，若您也要验证用户身份的话，请通过界面右方**第二身份验证**的**添加**来增加选择**用户 (Kerberos V5)**，此时除了验证计算机身份之外，还需要验证用户身份，也就是连接对方时，必须利用域用户账户来连接，而系统默认会利用用户登录的账户来连接。

**STEP 21** 回到**验证方法**界面时单击**下一步**。

**STEP 22** 在**配置文件**界面中单击**下一步**。

**STEP 23** 在**名称**界面中为此规则设置一个友好的名称，例如**位于192.168.8.0的域成员需验证**。单击**完成**。

**STEP 24** 图 10-42为完成后的界面。

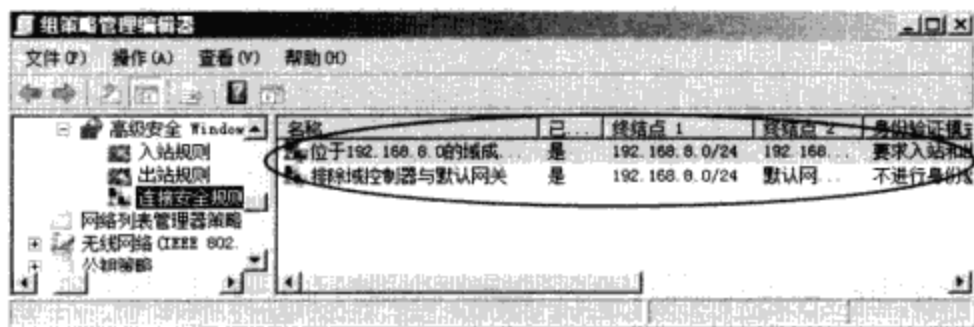


图 10-42

**STEP 25** 请等域成员计算机自动应用这个策略设置，或直接到DC、Server1与Server2上运行 `gpupdate /force` 命令来手动应用。

**注意**

若您先建立图中的**位于192.168.8.0的域成员需验证**规则，并让3台服务器应用此规则的话，则之后两台成员服务器将无法与域控制器通信，因为域成员无法通过IPSec来与域控制器等基础结构计算机通信，因此就算之后您新建了排除规则，Server1与Server2也无法从域控制器取得并应用这个规则。此时您可以先暂时将Server1、Server2与域控制器的**Windows防火墙**关闭，以便让**连接安全规则**的IPSec设置无效，然后在域控制器上利用 `gpupdate /force` 手动应用排除规则，完成后再分别到两台服务器上利用 `gpupdate /force` 来应用验证规则，最后再重新启用这3台计算机的**Windows防火墙**。

完成以上所有设置后，请到Server1（192.168.8.1）利用ping命令测试，请同时开启3个命令提示符窗口，然后分别执行以下3个命令：ping 192.168.8.2、ping 192.168.8.200与ping 192.168.8.254。

由于我们已经开放所有服务器的ICMP连入流量，因此应该3个连接测试都会成功收到对方的响应。接着请在Server1上选择【开始→管理工具→高级安全Windows防火墙→监视→安全关联→主模式或快速模式SA】，从图 10-43可知Server1（192.168.8.1）与Server2（192.168.8.2）之间已经成功地新建了主模式SA，也就是通过IPSec在通信。

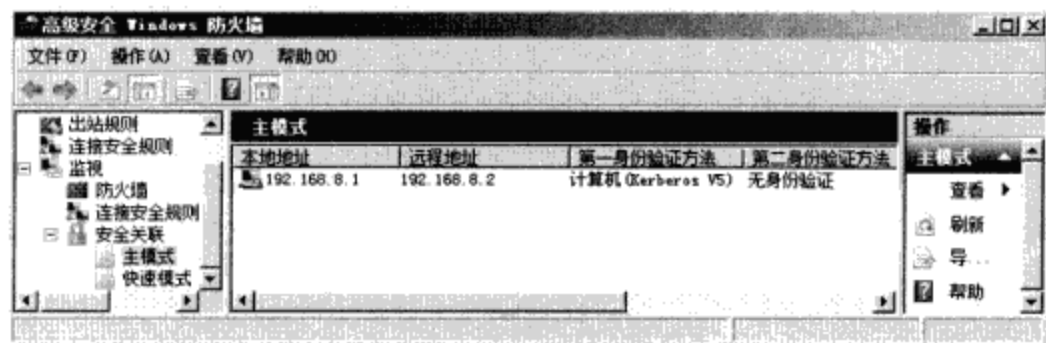


图 10-43

图中为何没有看到Server1与域控制器、默认网关之间的IPSec连接呢？因为Server1与域控制器（192.168.8.200）、默认网关（192.168.8.254）之间的通信并不需要IPSec（通过排除规则）。

## 10-5 采用计算机证书的IPSec设置

我们将通过图 10-44来说明如何让图中的两台服务器利用IPSec来安全地通信，并且采用计算机证书的验证方式。图中3台服务器为Windows Server 2008 R2独立服务器或成员服务器皆可，其中CA是用来发放计算机证书的服务器，假设其为独立CA。请按照图指示设置3台计算机的IP地址与子网掩码。本节将仅列出重点说明，其中与证书申请有关的步骤，有需要的话，请参考第6章。

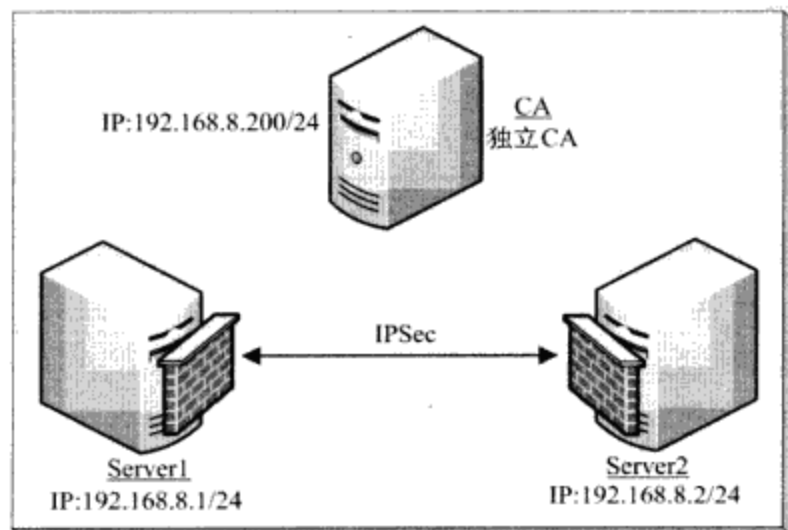















图 10-44



- ✎ 请分别在 Server1 与 Server2 上开放 ICMP 的相关流量：【开始  管理工具  高级安全 Windows 防火墙  单击入站规则中的文件和打印机共享（回显请求 - ICMPv4-In）  单击右边的启用规则】。
- ✎ 到 Server1 上执行 ping 192.168.8.2、Server2 上执行 ping 192.168.8.1，测试双方是否能够正常通信。
- ✎ 到 CA 计算机上安装 Active Directory 证书服务角色：【单击左下角服务器管理器图标   角色  添加角色  单击  勾选 Active Directory 证书服务角色  单击两次   添加勾选证书颁发机构单位 Web 注册  ...】。
- ✎ 到 Server1 计算机上申请计算机证书、安装此证书。

在 Windows Server 2008 R2（Windows Vista、Windows Server 2008 与 Windows 7）计算机上利用浏览器向 CA 网站申请计算机证书时需要利用以下两种方式之一，否则申请证书会失败：

- 利用 https 方式来连接 CA 网站，但需将 CA 网站加入到信任的网站
- 利用 http 方式来连接 CA 网站，但请暂时将 Internet Explorer 的本地 Intranet 的安全级别降为低级别，同时将 CA 网站加入到本地 Intranet

其中第 1 种方法的 CA 网站必须申请与安装 SSL 证书，比较麻烦，故此处我们采用第 2 种方法来为 Server1 申请计算机证书。

















- 先利用 <http://192.168.8.200/certsrv/> 来信任 CA（将 CA 证书安装到 Server1）。若是企业 CA 的话，因为域成员会自动信任企业 CA，故域成员可免除此步骤。信任 CA 的步骤请参考章节 6-2 的说明。
- 将 Internet Explorer 的本地 Intranet 的安全级别降为低级别，同时也将 CA 网站加入到本地 Intranet：【打开 Internet Explorer  工具菜单  Internet 选项  安全标签  单击本地 Intranet  将安全级别降为低  按右边的  单击  将 CA 网站 <http://192.168.8.200/> 加入此区域后单击 、依次单击 】。
- 打开 Internet Explorer，然后利用 <http://192.168.8.200/certsrv/> 来向 CA 申请证书：【申请证书  高级证书申请  向这个 CA 新建并提交一个请求  如图 10-45 所示在需要的证书类型处选择客户端身份验证证书  勾选标记密钥为可导出  单击 】（若是企业 CA 的话，请在证书模板处选择管理员，并且可直接下载与安装证书文件，因此请跳过以下两个步骤）。

图 10-45



### 注意

我们需将所申请的证书保存到本地计算机证书缓存区，然而利用Internet Explorer向Windows Server 2008 R2 CA申请证书时，界面中并没有将证书存放在本地计算机证书缓存区的选项，因此所申请的证书会被储存在用户证书缓存区。我们将通过以下方法来解决此问题：先将此证书从用户证书缓存区导出，再将其导入到本地计算机证书缓存区。

- 到CA计算机上通过【开始☞管理工具☞证书颁发机构☞挂起的申请☞对着证书申请单击右键☞所有任务☞发布】的方法来发放证书。
- 到Server1下载与安装证书：【在Internet Explorer内输入http://192.168.8.200/certsrv/☞查看挂起的证书申请状态☞...☞安装这个证书】。
- 选择【开始☞运行☞输入MMC后按Enter键☞文件菜单☞添加/删除管理单元☞从可用的管理单元列表中选择证书后单击添加☞确认我的用户账户被选取后单击完成☞重新从可用的管理单元列表中选择证书后单击添加☞改选计算机账户后单击下一步、完成与确定】。
- 通过【如图 10-46所示展开证书 - 当前的用户☞个人☞证书☞对着之前安装的证书单击右键☞所有任务☞导出☞单击下一步☞选择是，导出私钥☞...】的方法将证书导出保存。

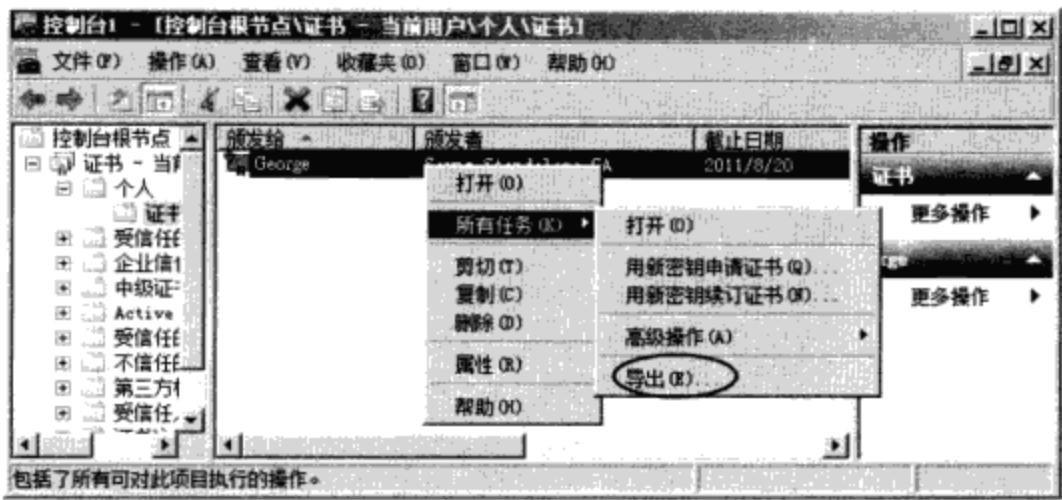


图 10-46

■ 通过如图 10-47 所示【展开证书（本地计算机）】对着个人单击右键所有任务导入...的方法将之前导出的证书导入。

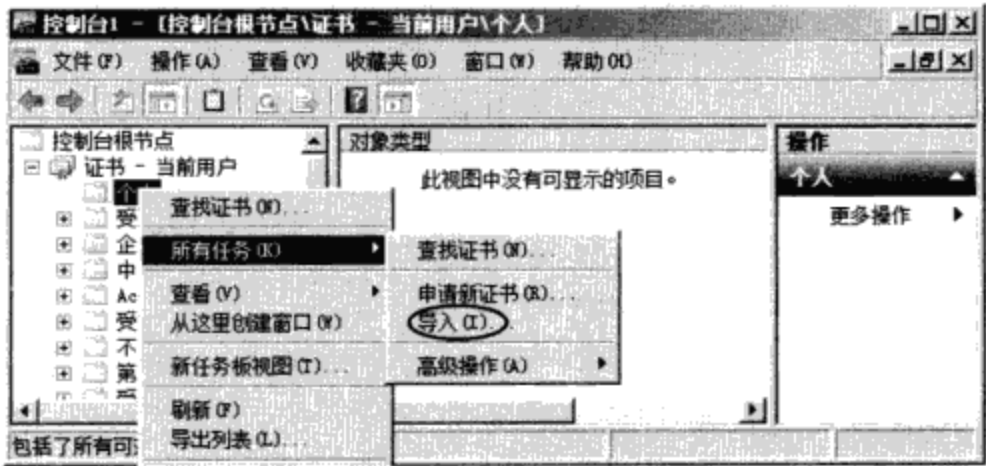


图 10-47

■ 将Internet Explorer的本地Intranet的安全级别恢复为中低级别。

在Server1上通过高级安全Windows防火墙来新建连接安全规则：【如图 10-48 所示在验证方法界面中单击高级处的自定义单击图 10-49 中添加在前图中通过浏览来选择放计算机证书的CA...】。

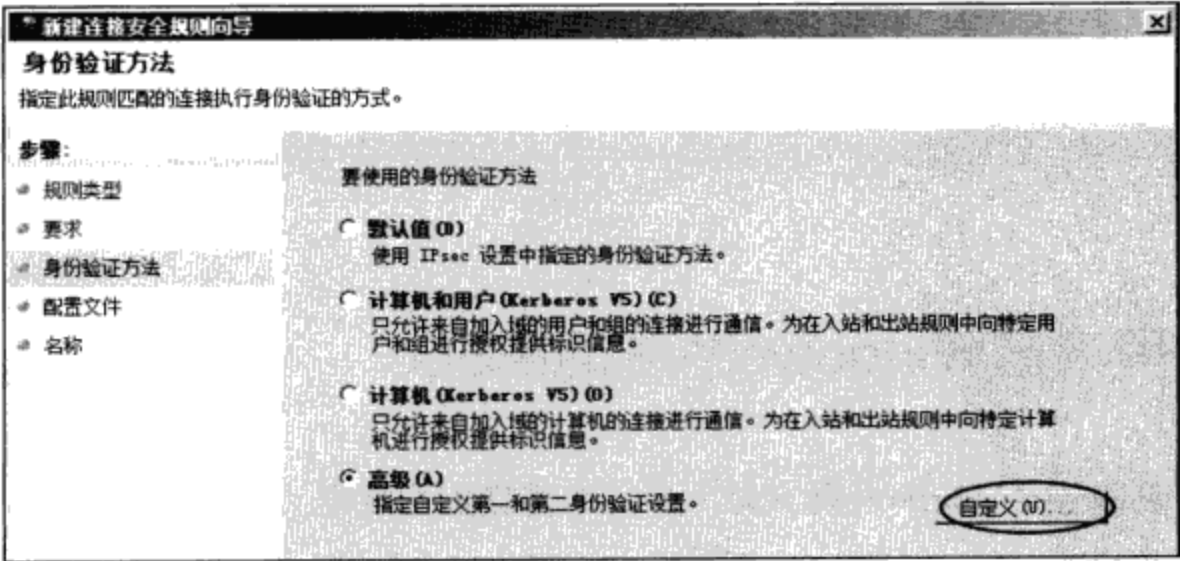


图 10-48

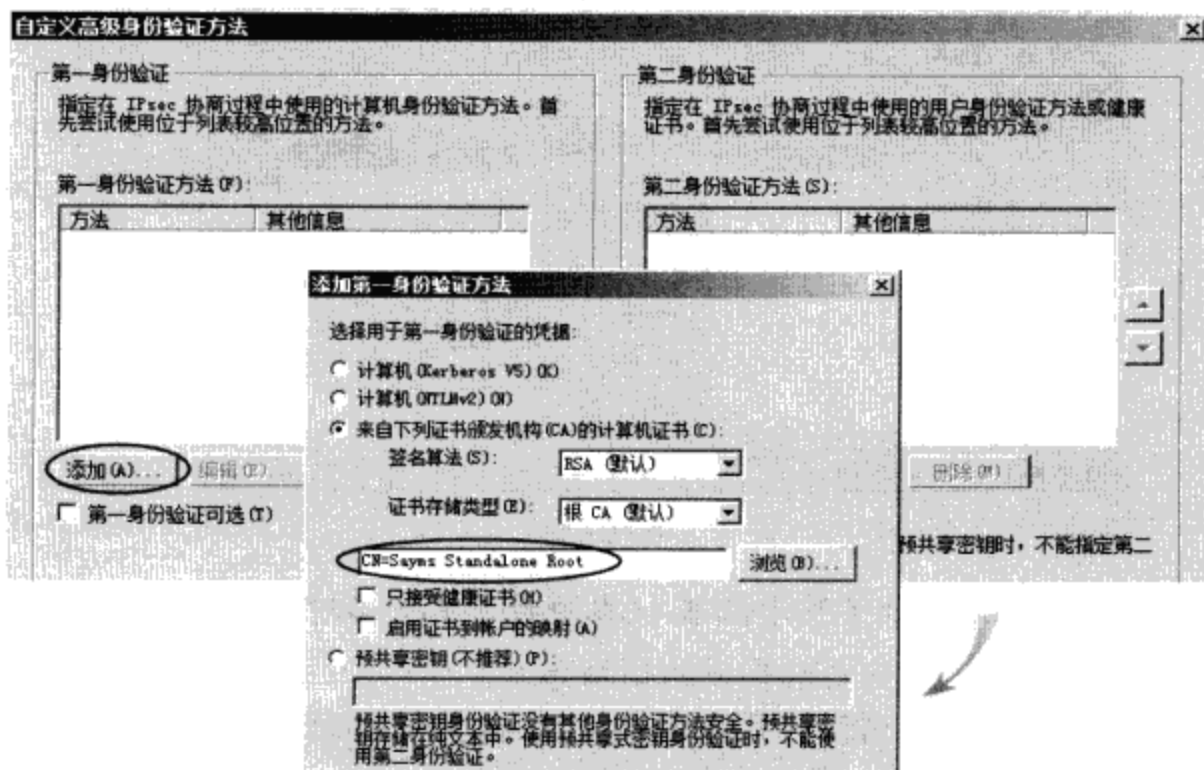


图 10-49

- 由于所新建的规则要求无论入站或出站连接都必须采用IPSec，然而目前Server2尚未新建连接安全规则，也就是尚未启用IPSec，故此时若在Server1上利用ping命令来与Server2通信的话，此连接会被Server1拒绝。
- 到Server2计算机上重复上述步骤：申请计算机证书、安装此证书、通过高级安全Windows防火墙来新建连接安全规则。
- 在两台服务器上利用ping命令来测试，此时双方应该可通过IPSec来相互通信。图 10-50 为其所新建的主模式SA，其验证方法为计算机证书。

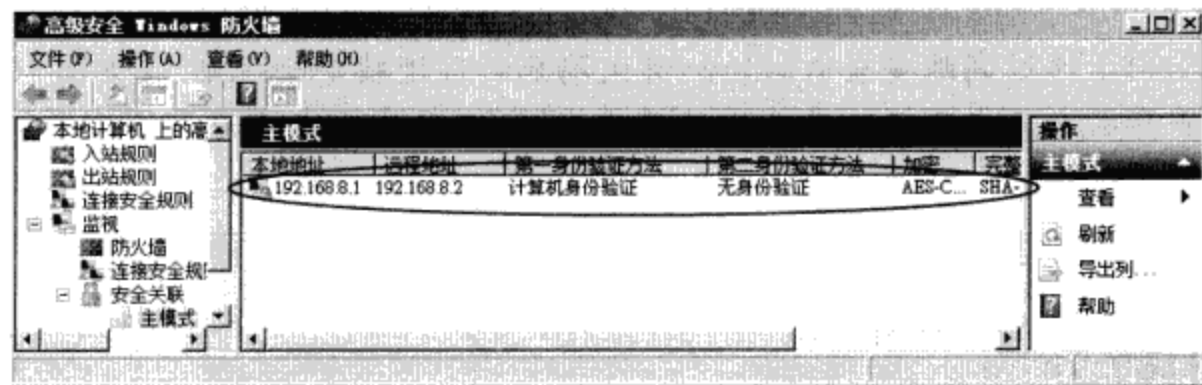


图 10-50

## 10-6 启用旧版Windows系统的IPSec

前面通过高级安全Windows防火墙所新建的连接安全规则，只适用于Windows Server 2008 R2、Windows Server 2008、Windows 7与Windows Vista计算机，如果是Windows Server 2003等旧版操作系统的话，请通过IP安全策略管理控制台的IPSec策略来启用IPSec。

在Windows Server 2003上新建IP安全策略管理控制台的方法为：【开始→运行→输入MMC

后按 **Enter** 键 **→** 文件菜单 **→** 添加/删除管理单元 **→** 单击 **添加** **→** 在图 10-51 中选取 IP 安全策略管理后单击 **添加** **→** 在前图中选择管理本地计算机、Active Directory 域（本域或其他域）或其他计算机的 IPSec **→** ...】，此处我们选择管理本地计算机的 IPSec（如图 10-52 所示）。

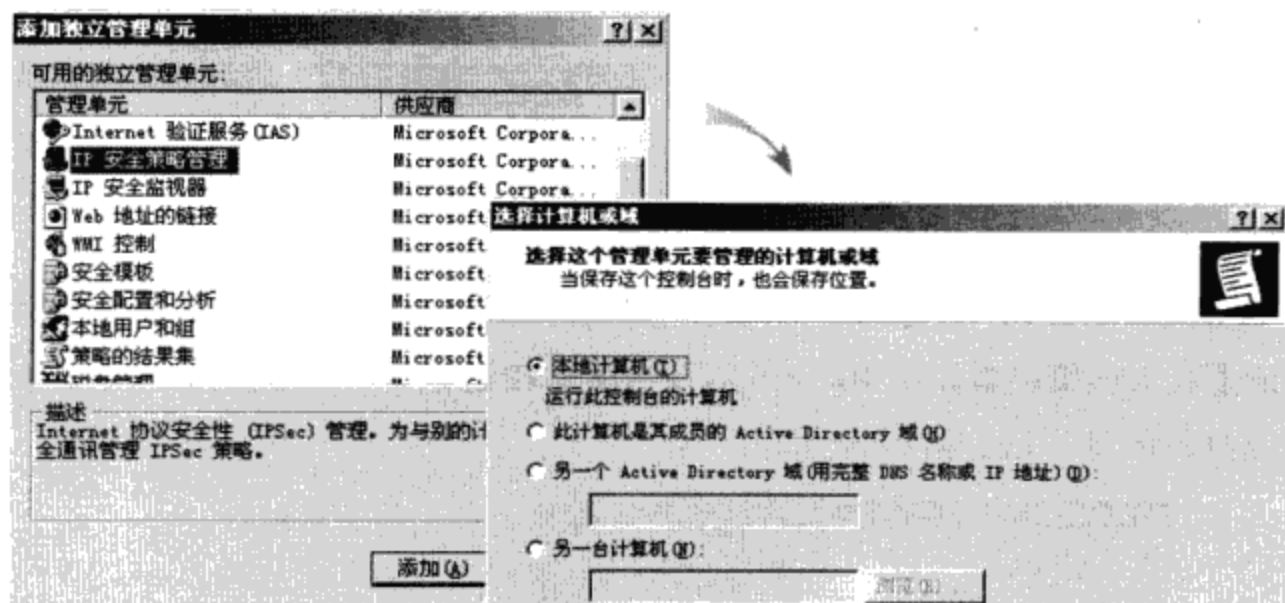


图 10-51

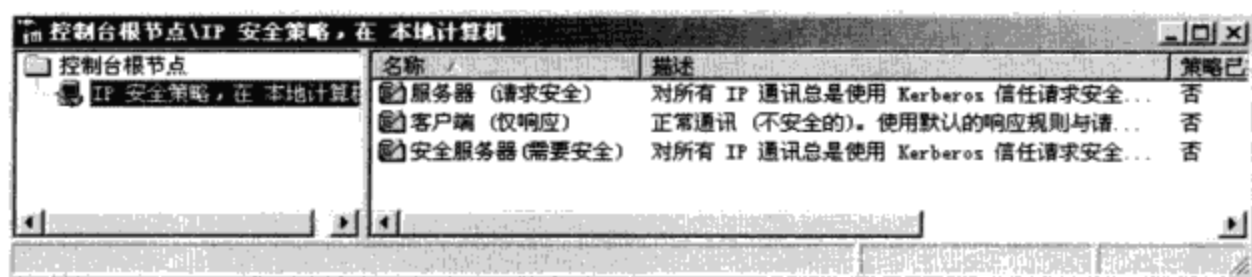


图 10-52

图 10-52 右方有 3 个内置的 IPSec 策略，这 3 个策略的默认值是采用 Kerberos 验证，因此适用于域成员计算机，不过您可以视需要自行修改设置。您可以为您的计算机来启用这 3 个策略之一：

- **客户端（仅响应）**：Client (Response Only)，被动地使用 IPSec，也就是只有其他计算机要求与您的计算机利用 IPSec 来通信时，您的计算机才会使用 IPSec。
- **安全服务器（需要安全）**：Secure Server (Require Security)，主动要求必须使用 IPSec。当其他计算机要与您的计算机通信时，或是您的计算机要与其他计算机通信时，您的计算机都会要求对方必须使用 IPSec，若对方不支持 IPSec 的话，双方无法通信。
- **服务器（请求安全）**：Server (Request Security)，主动请求使用 IPSec。当其他计算机要与您的计算机通信时，或是您的计算机要与其他计算机通信时，您的计算机都会请求对方使用 IPSec，若对方不支持 IPSec 的话，您的计算机还是可以接受以没有 IPSec 的方式来通信。

**提示**

**安全服务器（需要安全）与服务器（要求安全）**都是针对所有的 IP 协议来设置，也就是双方只要是利用 IP 协议来通信，都会要求或请求对方使用 IPSec，但是其中的 ICMP 协议例外，也就是它们允许 ICMP 以没有 IPSec 的方式来通信。

若要启用IPSec策略的话，请如图 10-53所示【对着要启用的策略单击右键➤指派】，图中启用的是**安全服务器（需要安全）**策略。

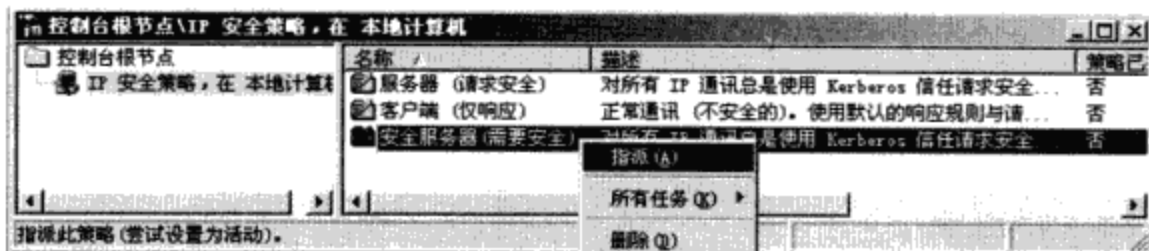


图 10-53

若要更改策略设置，例如要更改**安全服务器（需要安全）**策略内与IP流量有关的策略设置的话，请【双击该策略➤如图 10-54所示双击**所有IP通讯**➤通过编辑规则属性对话框来更改】，例如更改身份验证方法、隧道设置等。

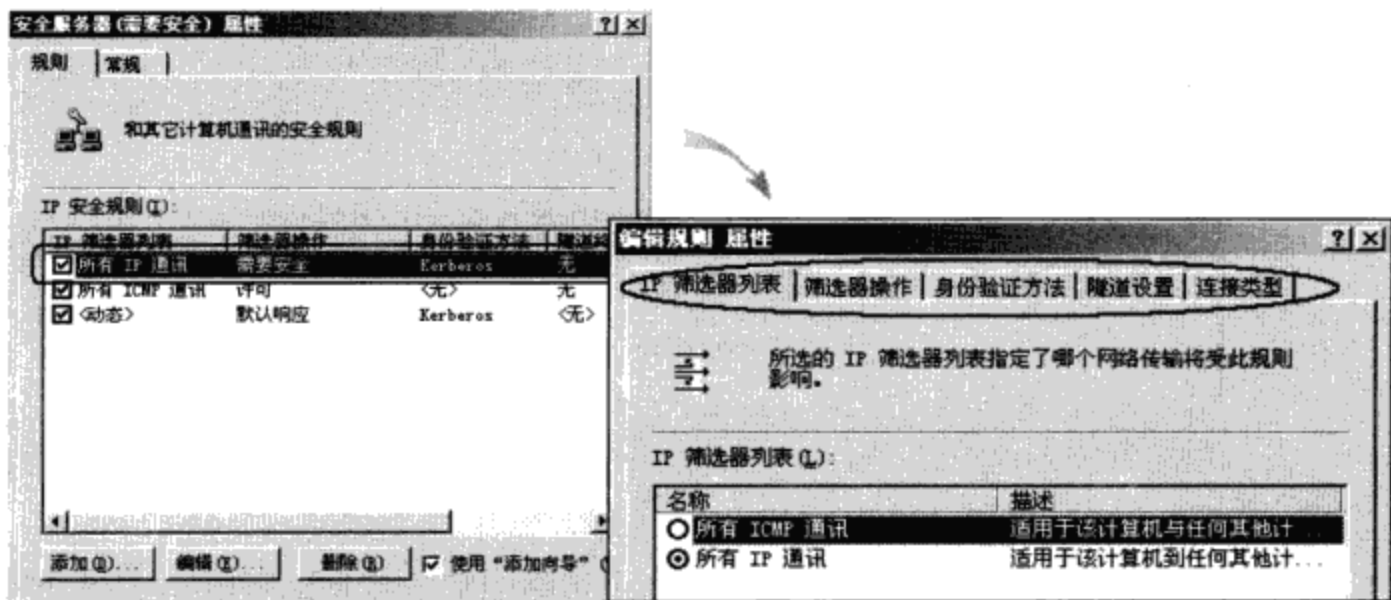


图 10-54

您也可以通过域的组策略来设置IPSec策略，如图 10-55所示。

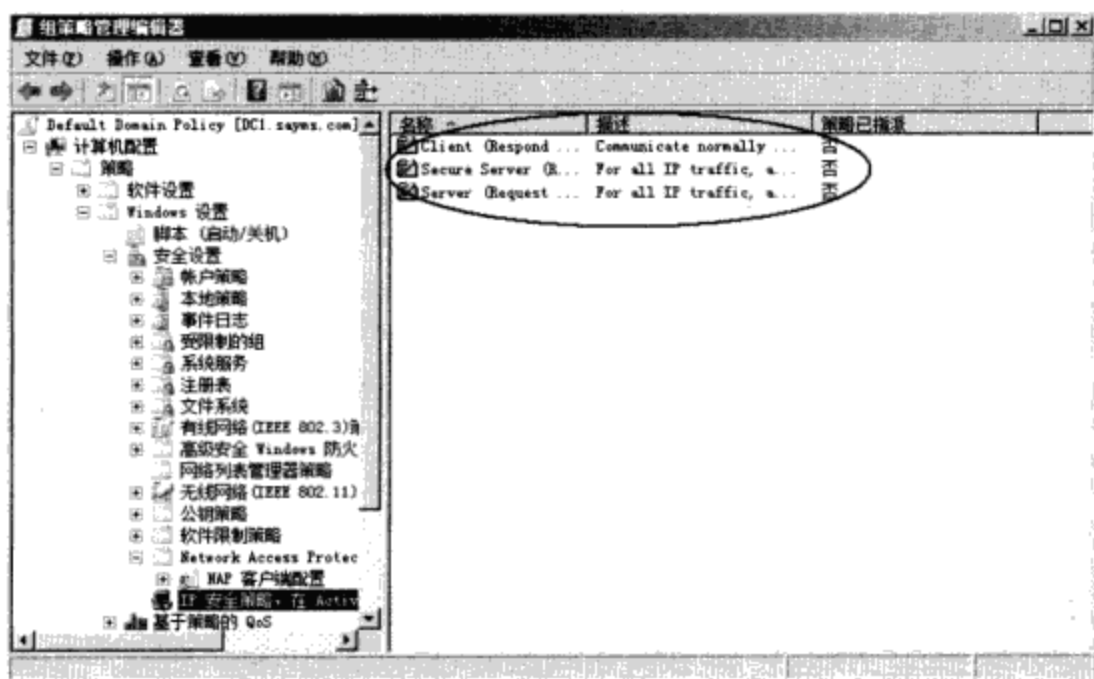


图 10-55

## 10-7 IPSec跨越NAT的问题

使用NAT（Network Address Translation，网络地址转换，见第12章）让位于内部网络的多台计算机只需要共享一个public IP地址，就可以连接因特网、浏览网页与收发电子邮件等，可是若同时采用IPSec来确保数据发送安全性的话，就可能会有问题产生，因为NAT会改变数据包的header，然而IPSec却不允许其数据包内的header被修改：

- **AH传输模式与AH信道模式：**无论是AH传输模式或AH信道模式，IPSec都会将整个数据包签署（见图 10-4），也就是不允许修改数据包内的任何数据，因此NAT更改数据包内的IP地址或TCP/UDP端口号后，IPSec会将此数据包视为无效数据包。
- **ESP传输模式与ESP信道模式：**ESP传输模式的Original IP header（见图 10-5），或ESP信道模式的New Tunnel Header都还是保留原状，并没有被IPSec签署或加密，但是TCP/UDP端口号却被加密无法读取，因此虽然NAT可以更改在传输模式中的客户端IP地址、或是信道模式中的端点（end-point）计算机的IP地址，但是NAT却无法更改端口号，更何況端口号还被签名，不允许更改。

NAT-T（NAT-Traversal）可以解决IPSec无法跨越NAT的问题，Windows Server 2008 R2、Windows Server 2008、Windows 7、Windows Vista与Windows XP SP2等系统都支持NAT-T。若要让IPSec数据包能够跨越NAT的话，请采用ESP协议，因为支持NAT-T的IPSec主机自动检测到NAT的存在，并将IPSec ESP数据包，封装（Encapsulate）到UDP Header内（UDP端口为500），如图 10-56所示（以ESP信道模式为例）。图中ESP Header 被封装到UDP Header 内，数据包内的Original Tunnel Header与UDP Header都没有被加密与签署，因此NAT可以更改其IP地址与UDP端口号。利用IPSec通信的两端计算机都必须支持NAT-T。

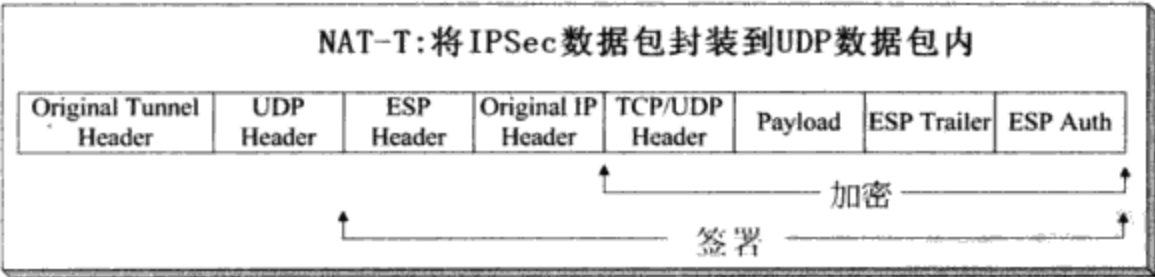


图 10-56