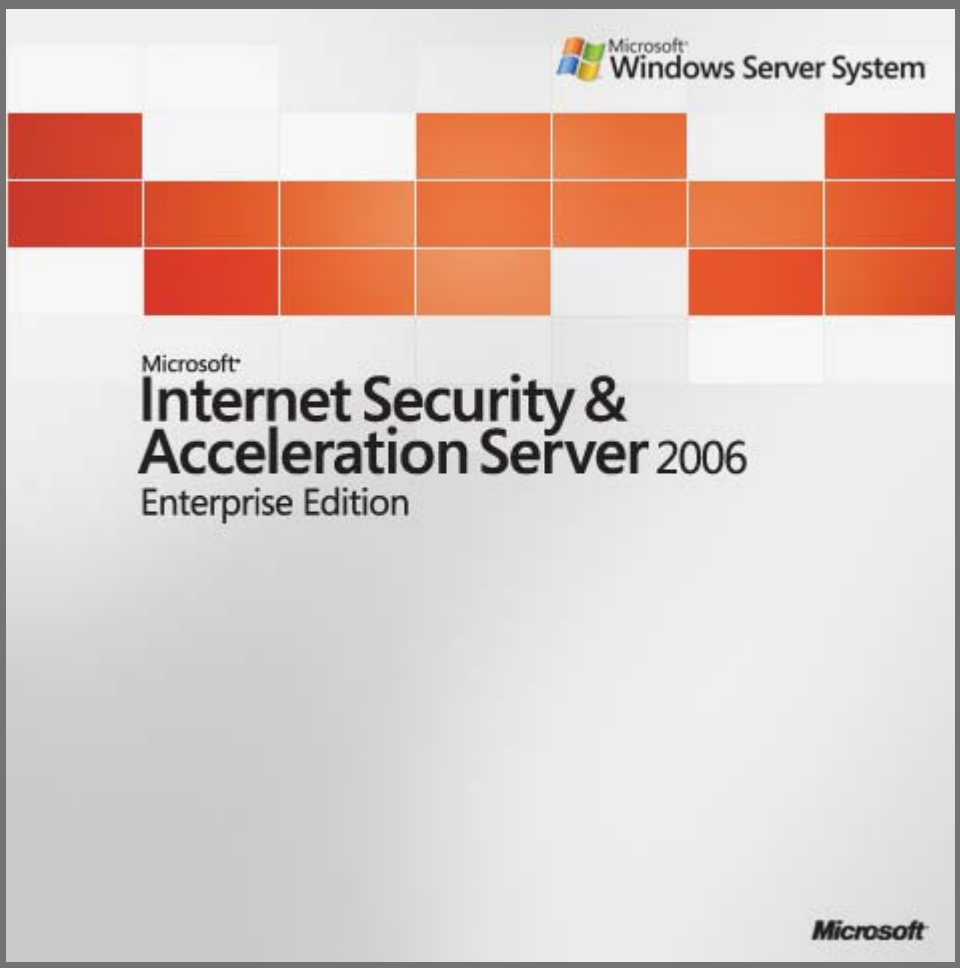
ISA
2006

ISA2006 系列教材

成为 ISA2006 专家的必备书籍

本书文章出自“岳雷的微软网络课堂”，内容涵盖面很大，应该是现在最为全面的 ISA2006 防火墙学习书籍。很感谢岳雷老师抽时间为大家写出这么经典的文章，同时感谢 ISA 中文网的风间子提供的技术支持!



整理制作：丢失的蓝色
http://www.my0745.com.cn
ISA 2006

目录

ISA2006 系列之一：ISA2006 标准版的常规安装和无人值守安装

ISA2006 系列之二：详解 ISA2006 三种客户端

ISA2006 系列之三：WPAD 原理介绍暨故障排查

ISA2006 系列之四：用 DHCP 部署 WPAD

ISA2006 系列之五：实例详解 ISA 防火墙策略元素

ISA2006 系列之六：深入剖析防火墙策略的执行过程：

ISA2006 系列之七：用防火墙客户端限制使用 SKYPE

ISA2006 系列之八：ISA 限制用户上网的技巧

ISA2006 系列之九：举例详解 ISA 的 HTTP 过滤功能

ISA2006 系列之十：发布多个 Web 站点完全攻略

ISA2006 系列之十一：发布 Web 服务器上的虚拟主机

ISA2006 系列之十二：让你的 Web 服务器不再裸奔

ISA2006 系列之十三：灵活运用 ISA 的链接转换功能

ISA2006 系列之十四：发布安全 Web 站点详细攻略

ISA2006 系列之十五：妙用通配符证书发布多个安全 Web 站点

ISA2006 系列之十六：探讨防火墙内核监听模式

ISA2006 系列之十七：发布 Exchange OWA 方法及故障分析

ISA2006 系列之十八：发布 Exchange 的 SMTP，POP3 服务器

ISA2006 系列之十九：发布 Exchange 的 RPC 以及 RPC Over HTTPS

ISA2006 系列之二十：用 ISA2006 搭建 VPN 服务器

ISA2006 系列之二十一：配置 VPN 服务器中的 L2TP/IPSEC

ISA2006 系列之二十二：详解 Radius 服务器在 VPN 中的应用

ISA2006 系列之二十三：用智能卡构建身份验证的马其诺防线

ISA2006 系列之二十四：多图详解 VPN 用户隔离

ISA2006 系列之二十五：创建基于 PPTP 的站点到站点 VPN 连接

ISA2006 系列之二十六：创建基于 L2TP 的站点到站点的 VPN 连接

ISA2006 系列之二十七：配置单网卡的 ISA 缓存服务器

ISA2006 系列之二十八：用组策略实现用户证书的自动注册申请

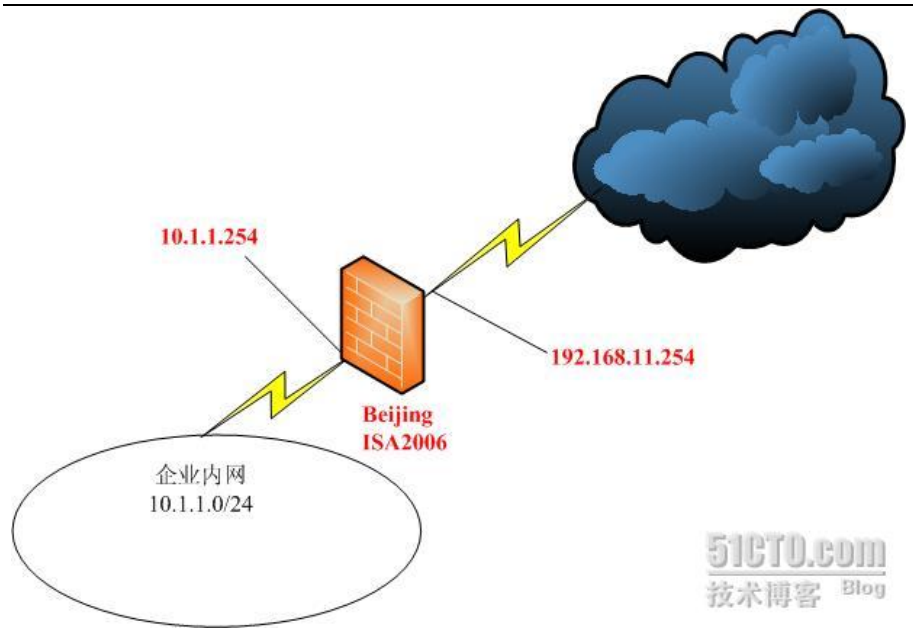
ISA2006 系列之二十九:详解 DMZ 的部署与配置

ISA2006 标准版的常规安装和无人值守安装：ISA2006 系列之一

ISA2006（Internet Security and Acceleration）是微软公司推出的一款重量级的网络安全产品，被公认为 X86 架构下最优秀的企业级路由软件防火墙。ISA 凭借其灵活的多网络支持、易于使用且高度集成的 VPN 配置、可扩展的用户身份验证模型、深层次的 HTTP 过滤功能、经过改善的管理功能，在企业中有着 广泛的应用。从今天开始的一系列课程中我们将陆续介绍 ISA 的管理和使用技巧，内容重点是访问控制，服务器发布和 VPN 三部分。今天我们从 ISA2006 的部署开始介绍。

ISA2006 分为标准版和企业版，两种版本的结构和功能都存在一定差异。标准版部署起来相对容易，适合中小企业使用，也适合 ISA 爱好者的入门学习；企业版由于引入了配置存储服务器，部署起来有一定难度，我们将它放在后期课程中介绍。

今天我们准备给大家分别介绍 ISA2006 标准版的常规安装和无人值守安装。拓扑如下图所示，服务器 Beijing 有两块网卡，内网网卡的 IP 地址为 10.1.1.254，外网网卡的 IP 地址为 192.168.11.254。Beijing 的操作系统为 Win2003SP1，准备安装 ISA2006 作为企业的边缘防火墙。



ISA2006 的安装要求如下：

带有 Service Pack 1 (SP1) 的 Microsoft Windows Server™ 2003 或 Microsoft Windows Server 2003 R2 操作系统。

256 MB 内存。

150 MB 可用硬盘空间。这是专门用于缓存的硬盘空间。

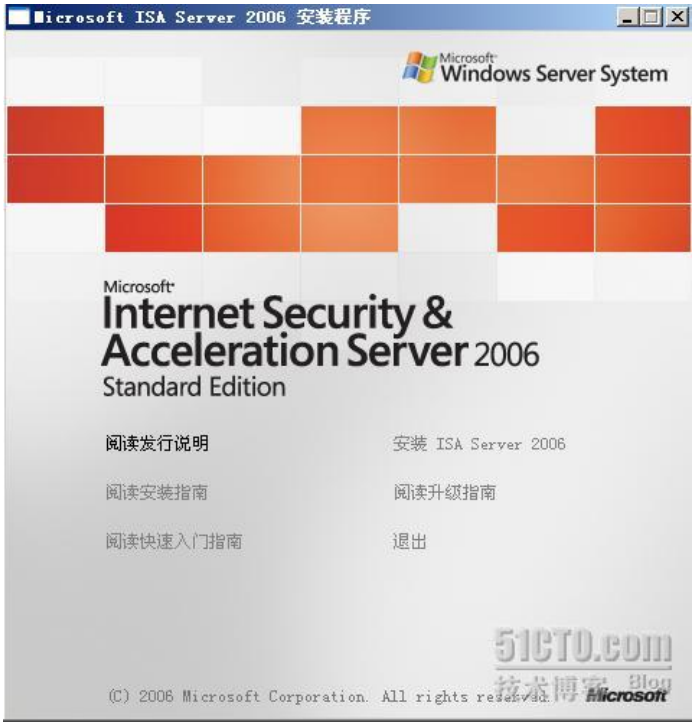
至少两块网卡（如果只有一块网卡，只能安装成缓存服务器）。

一个采用 NTFS 文件系统格式的本地硬盘分区。

安装 ISA2006 的服务器上不能有进程占用 80 和 8080 端口。

一 ISA2006 标准版的常规安装

在 Beijing 上放入 ISA2006 的安装光盘，如下图所示，启动 ISA2006 的安装程序，点击“安装 ISA Server 2006”。



出现 ISA2006 的安装向导，选择“下一步”。

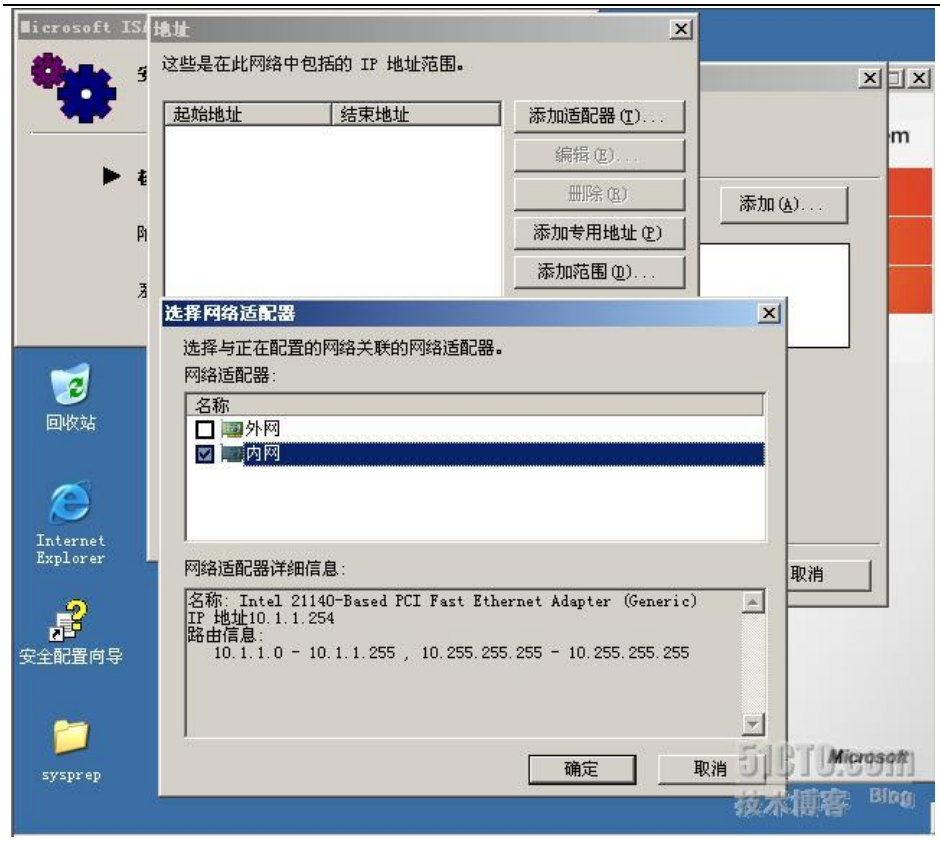
同意软件许可协议，选择下一步。

输入用户名，单位及序列号等参数后，来到安装类型界面，如下图所示，选择自定义安装。

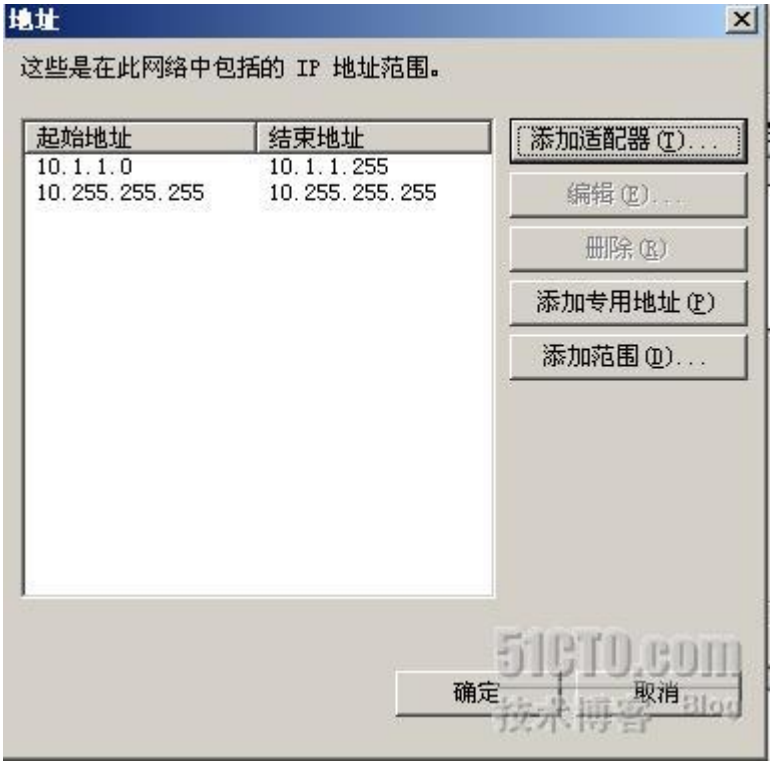
选择 ISA2006 的安装组件，从下图可知，只有 ISA 服务器和 ISA 服务器管理两个组件。有 ISA2004 经验的管理员要注意，ISA2004 中的 ISA 客户端共享和消息筛选两个组件已经不再被支持，消息筛选被 Forenfront 取代，ISA 客户端共享需要用手工共享的方法实现。

接下来设置内网的地址范围，点击“添加”按钮。顺便提一下，这个参数很重要，因为在 ISA 中网络是防火墙策略中最基本的一个考虑因素，具体我们回头再说

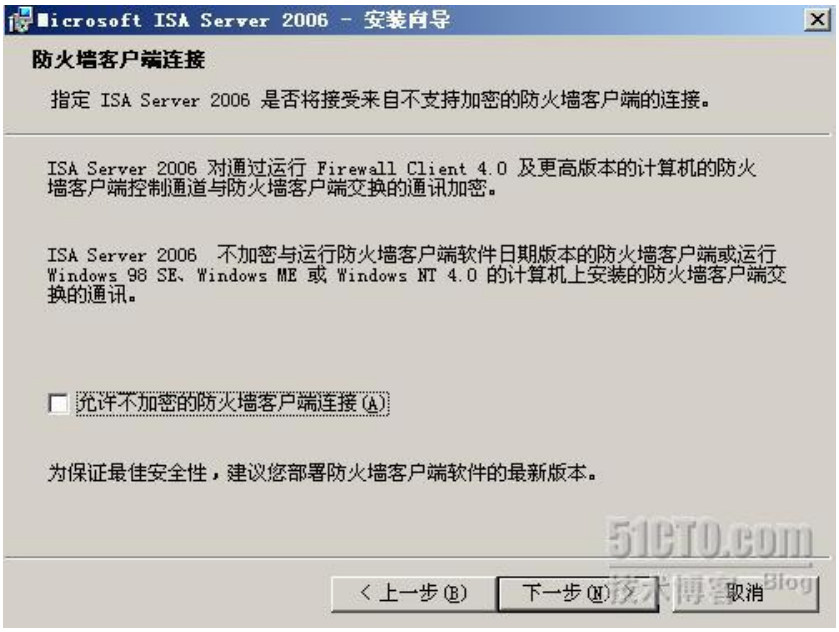
设置内网范围时，点击“添加适配器”，如下图所示，选择与内网相连的网卡，点击确定。这里建议大家最好把 ISA 上的网卡根据实际连接情况命名为内网，外网，外围等，以方便后续使用。



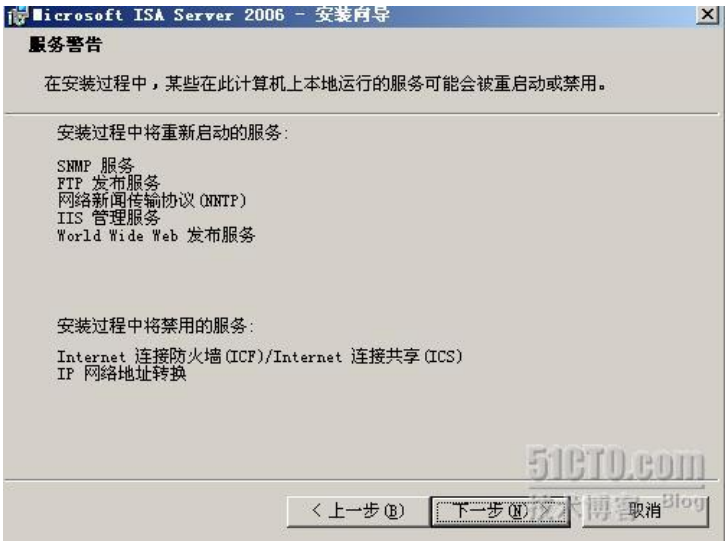
根据我们提供的网卡，ISA 将内网的地址范围设置为 10.1.1.0-10.1.1.255，点击确定。



安装程序询问是否允许不加密的防火墙客户端连接。不加密的防火墙客户端指的是 ISA 2000 之前的防火墙客户端，ISA2000 之后的防火墙客户端支持数据加密，安全性更好，由于在实验环境中不需要使用早期防火墙客户端，因此我们不用勾选“允许不加密的防火墙客户端连接”。



安装程序警告我们在安装过程中有些服务会重新启动，选择“下一步”。



完成了参数设置，终于开始安装了。

如下图所示，点击“完成”，结束了 ISA2006 的常规安装。

至此，我们完成了 ISA2006 的常规安装。安装过程并不复杂，相信大家都可以完成，难的地方在后面的管理部分，慢慢来吧。

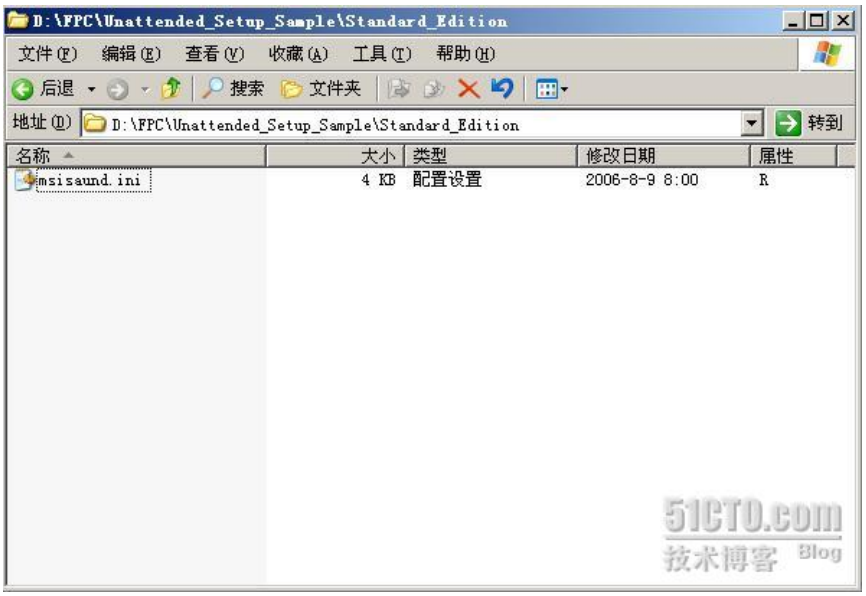
二 ISA2006 标准版的无人值守安装

ISA2006 的无人值守安装原理是很简单的，常规安装时我们通过交互方式输入安装参数，无人值守时只需事先将安装参数写到答案文件中，然后让 ISA 的安装程序从答案文件中获取参数就可以了。因此我们实现 ISA2006 的无人值守只需要注意两点：

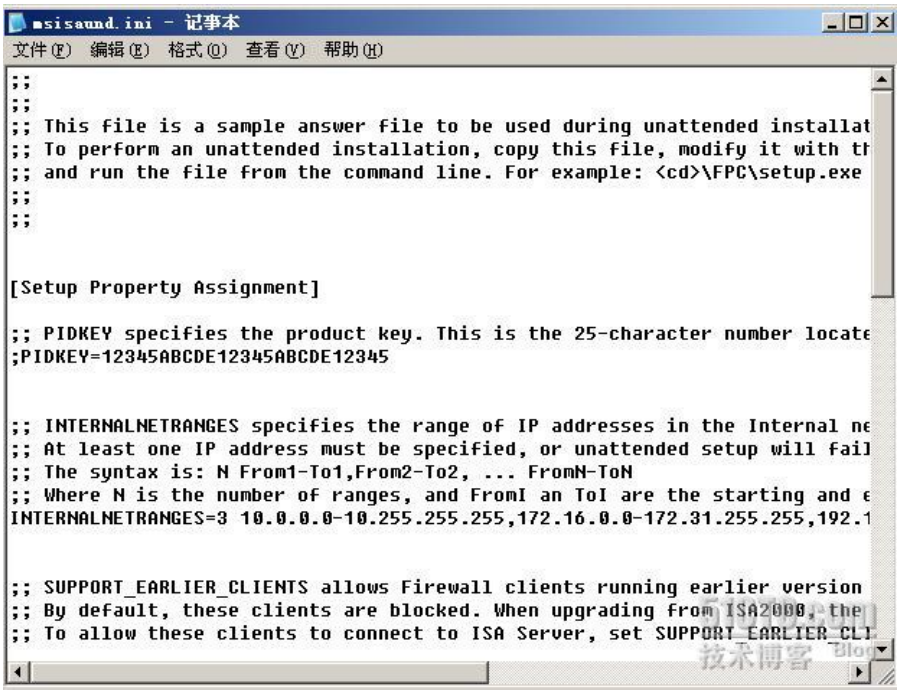
1） 如何创建答案文件

2） 如何让安装程序调用答案文件

先解决第一个问题。ISA2006 的安装光盘中有一个无人值守答案文件的示例，如下图所示，在 ISA2006 的安装光盘 FPCUnattended_Setup_SampleStandard_Edition 目录下，有一个 msisaund.ini 文件，这就是示例文件。我们只要对示例文件进行简单修改，就可以满足我们无人值守安装的需求。



打开模板文件看看，如下图所示，文件中有各种参数的解释。如果觉得 E 文看起来很吃力，我们可以在 ISA2004 标准版的安装光盘中找到 FPCmsisaund.ini，这个文件是 ISA2004 无人值守安装的示例文件。



打开 ISA2004 的示例文件，内容和 ISA2006 基本相同，但帮助是中文的，呵呵，这回 E 文不好的兄弟可以好好参考一下了。

将光盘中的 msisaund.ini 复制到 C:，然后对文件中的内容进行修改，我们就可以创建自己的 ISA2006 无人值守答案文件了。修改后的内容如下图所示，原文件中以分号开头的内容为注释，我们就不保留了。

对答案文件中的内容解释一下：

IDKEY=××××××××××××……

这里应该填写 25 位长度的产品序列号

INTERNALNETRANGES=1 10.1.1.0-10.1.1.255

设置内网的地址范围，1 代表只有一个地址范围，10.1.1.0-10.1.1.255 是具体的范围内容

SUPPORT_EARLIER_CLIENTS=0

不允许早期的防火墙客户端连接

INSTALLDIR=C:Program FilesMicrosoft ISA Server

ISA2006 的安装目录为 C:Program FilesMicrosoft ISA Server

COMPANYNAME=ITET

公司名称为 ITET

ADDLOCAL=ALL

安装所有组件

其实 ISA2006 无人值守安装还有一个很实用的功能，可以导入防火墙策略的 XML 配置文件，这样 ISA 安装完毕后，配置也就完成了，非常方便。语法是：

IMPORT_CONFIG_FILE=配置文件名

设置好答案文件后，我们就要考虑如何让 ISA 的安装程序调用这个答案文件了。我们在 Beijing 上输入 D:FPCsetup.exe /v"/qb FULLPATHANSWERFILE="c:msisaund.ini"",如下图所示，这样安装程序就会将 C:MSISAUND.INI 作为 ISA2006 的无人值守答案文件了。

ISA2006 的安装开始启动了，如下图所示，整个安装过程无需用户参与。

安装完毕后，打开 ISA2006 管理器，如下图所示，安装已经顺利完成。

至此，我们完成了 ISA2006 标准版的部署，在下次课程中，我们将介绍 ISA2006 的三种客户端。

详解 ISA2006 三种客户端：ISA2006 系列之二

上一篇我们介绍了如何部署 ISA2006，本文我们要让部署好的 ISA 来干活了。ISA 能干什么活？从字面意思看，ISA 的意思是互联网安全加速器，安全指的是防火墙功能，加速器则是代理服务器功能。今天我们就要部署 ISA 的代理服务器功能，看看内网用户如何利用 ISA 来访问互联网。

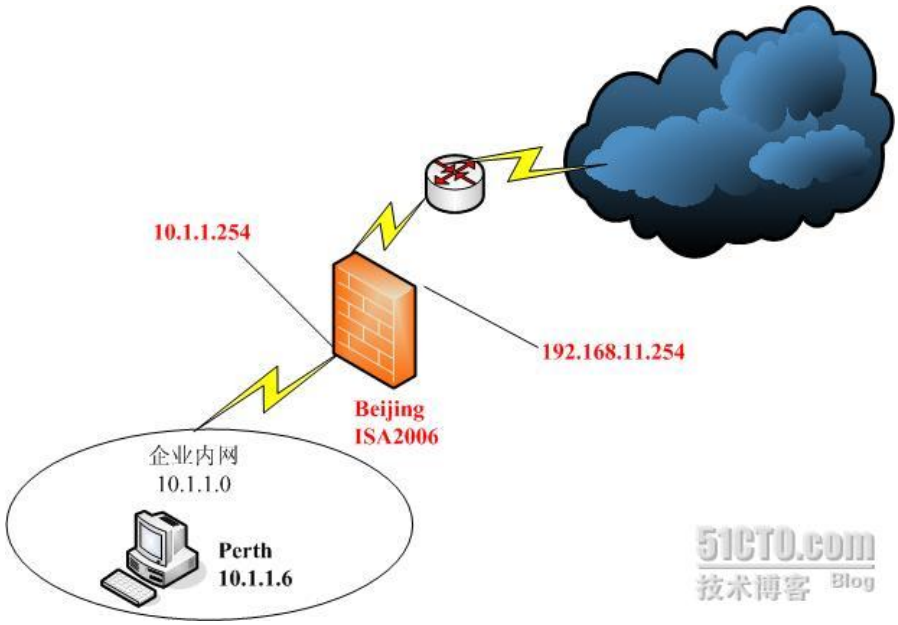
ISA 的代理服务支持三种客户端，分别是:

Web 代理客户端

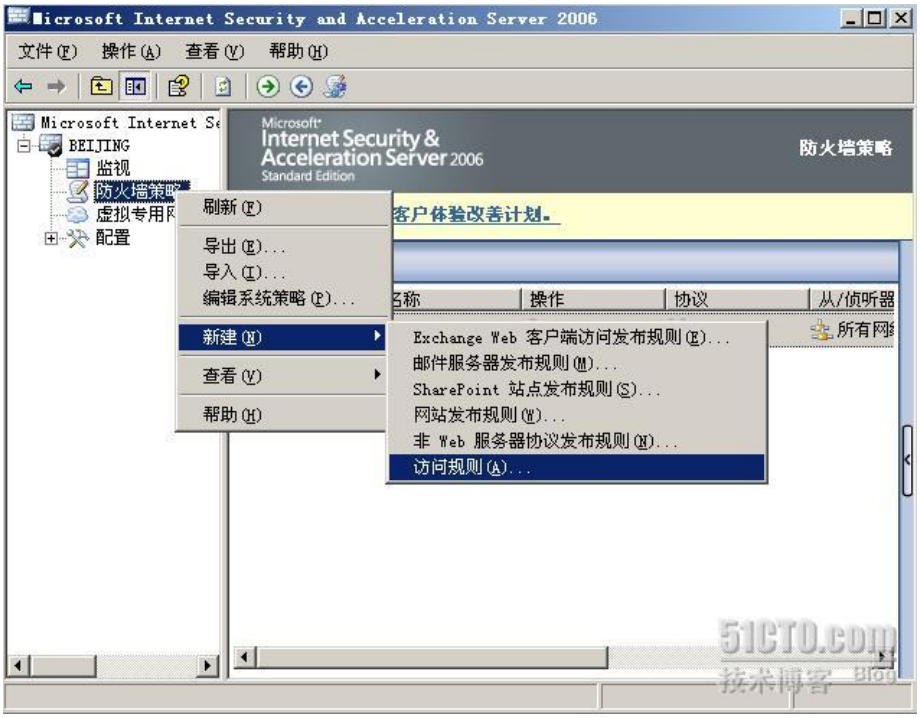
防火墙客户端

SNAT 客户端

我们搭建一个实验环境测试三种客户端的具体应用，实验拓扑如下图所示，Beijing 安装了 ISA2006 标准版，Perth 是内网客户机。

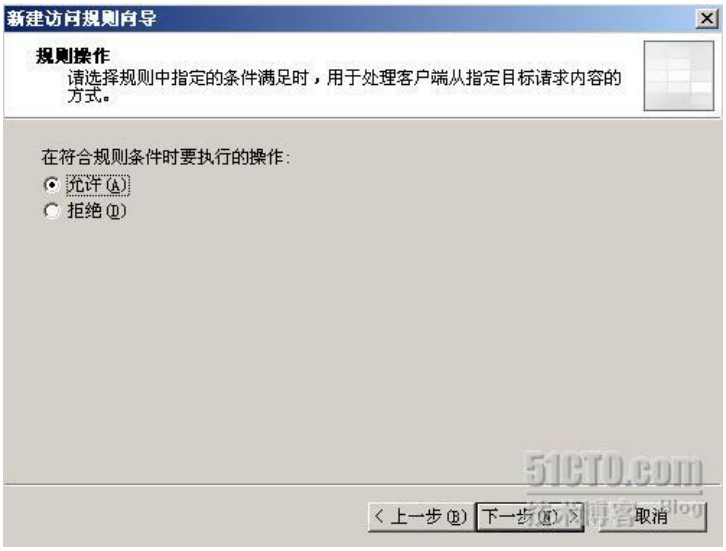


因为 ISA 默认的防火墙策略是拒绝一切通讯，所以实验之前我们需要先在 ISA 上创建一条访问规则，允许内网用户访问互联网。由于当前的主要目的是测试 ISA 的代理服务器功能，因此我们在防火墙上暂时不做任何限制。在 Beijing 上依次点击 开始－程序－Microsoft ISA Server－ISA 服务器管理，如下图所示，右键点击防火墙策略，选择新建“访问规则”。



给新建的访问规则取名为“允许内网用户任意访问”，如下图所示。

设置当客户端的访问行为与规则设定匹配时，防火墙将允许客户端进行访问。

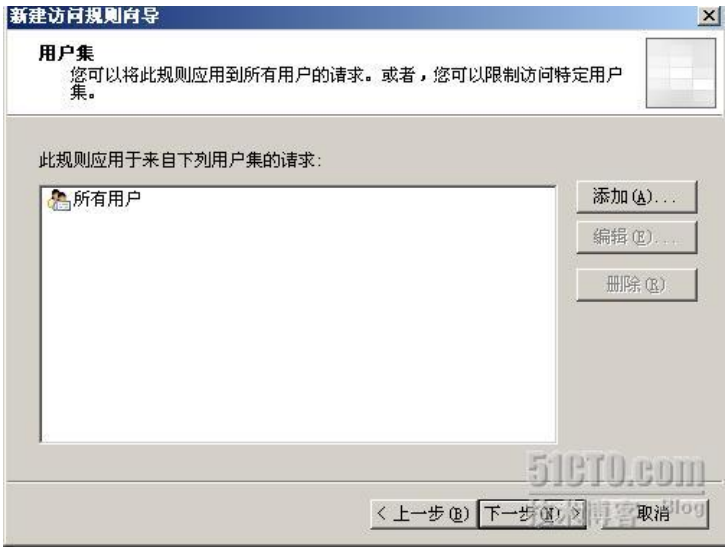


接下来要设置通讯源，如下图所示，点击“添加”，在网络中选择“内部”，然后点击“添加”，这样“内部”就成了规则的访问源。再用同样方法，将“本地主机”设置为访问源，这是为了测试方便，我们特意允许 ISA 服务器也能访问互联网。

设置好通讯源后，点击下一步。

现在该设置通讯目标了，我们将通讯目标设定为“外部”网络。

用户我们则选择“所有用户”，注意，所有用户中包括未经身份验证的用户。



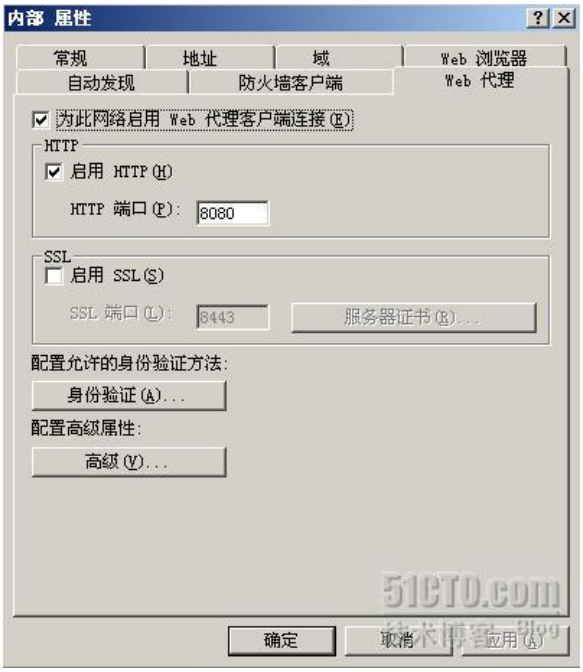
如下图所示，规则创建完毕。这条规则用通俗的话解释，就是凡是由内网计算机或 ISA 本机发起的访问外网的请求，无论是什么时间，无论使用什么协议，无论是哪些用户，ISA 一律允许。怎么样，这个规则很宽泛吧。

如下图所示，点击“应用”，使规则生效。好了，我们可以开始客户机访问测试了。

一 Web 代理

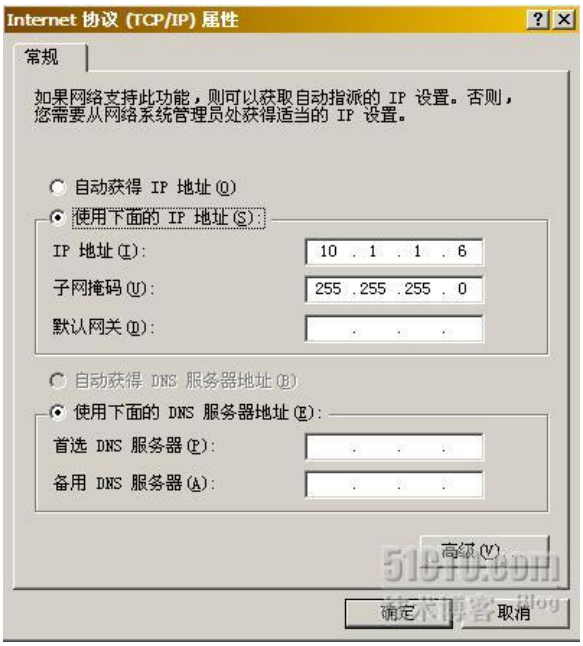
客户机使用 ISA 提供的 Web 代理就可以很方便地用浏览器访问互联网。Web 代理设置起来很容易，以 IE 浏览器为例，在客户机上打开 IE，依次点击 工具－Internet 选项－连接－局域网设置，如下图所示。我们将代理服务器设置为 ISA 内网网卡的 IP，端口为 8080。这下大家就明白了为什么安装 ISA2006 时要求服务器上不能有进程占用 8080 端口，因为 8080 端口被 ISA 用于为内网用户提供 Web 代理服务。

默认情况下 ISA 已经启用了 Web 代理服务，如果不放心可以检查一下。打开“ISA 服务器管理”，展开 配置－网络－内部，查看内部网络的属性，切换到“Web 代理”标签，如下图所示，我们发现 ISA 的 Web 代理服务已经在 8080 端口启动了。



在客户端测试一下，如下图所示，我们在客户机上成功地使用 Web 代理访问了互联网上的网站。

下图是客户机的 TCP/IP 设置，我们发现，客户机并没有设置 DNS 参数，那客户机访问网站时怎么解析域名呢？答案是转发至 ISA 服务器由 ISA 进行解析。

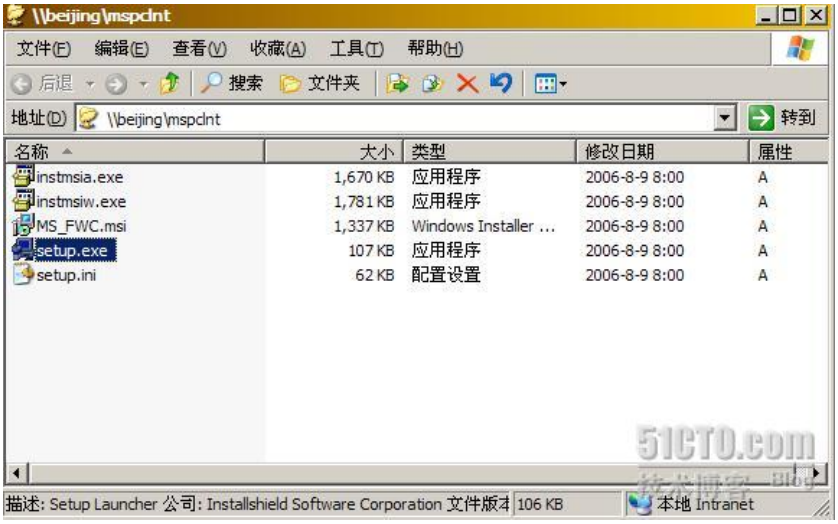


Web 代理配置简单，但功能也受限制，用户只能以浏览器作为客户端对互联网进行访问。

二 防火墙客户端代理

由于 Web 代理只能使用浏览器访问互联网，功能不够全面，因此微软在 ISA 中提供了防火墙客户端代理。用户只要安装防火墙客户端软件，就能通过 ISA 的防火墙客户端代理访问所有基于 Winsock 的网络服务。那该怎么安装防火墙客户端软件呢？这个软件在 ISA2006 安装光盘的 Client 目录下，我们将 Client 目录复制到 ISA 服务器的硬盘上，然后将目录共享，共享名为 Mspclnt（和老版本的 ISA 保持一致），如下图所示。

客户机访问 eijingmspclnt，运行 Setup.exe，如下图所示。

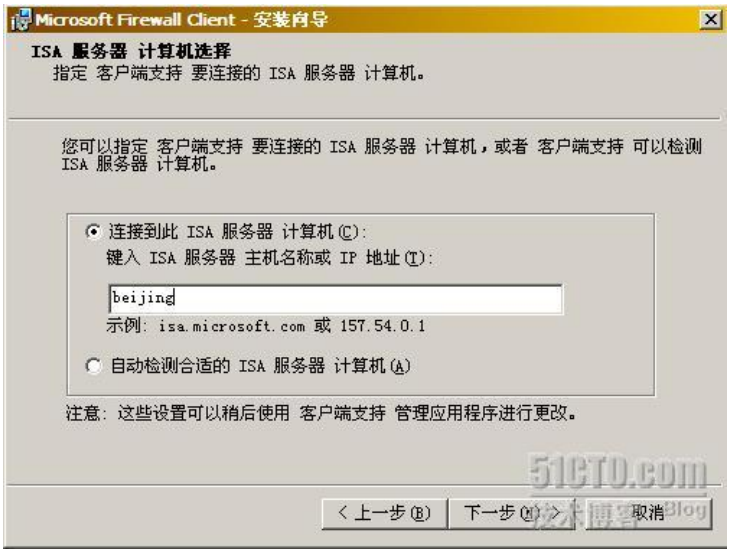


出现防火墙客户端的安装向导，点击下一步。

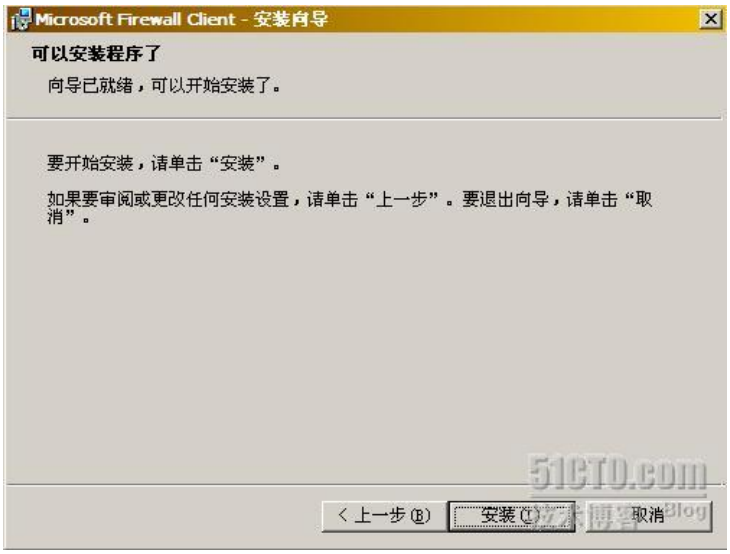
同意软件许可协议，点击下一步。

选择软件安装文件夹，我们取默认值。

指定 ISA 服务器，用计算机名或 IP 均可。

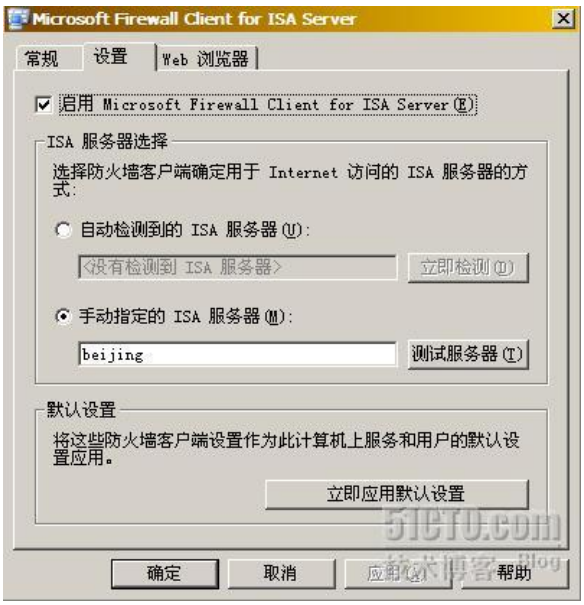


准备开始安装。



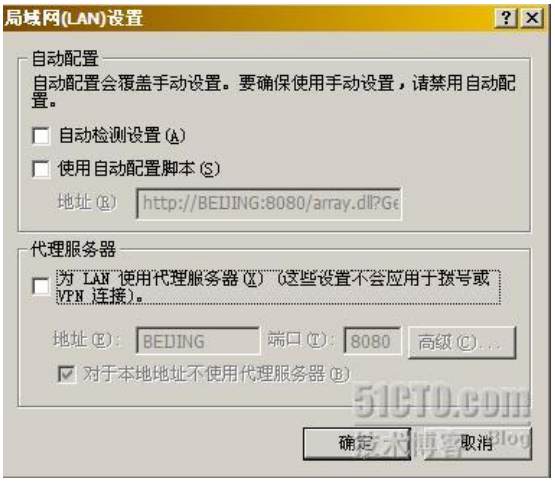
安装过程很快完成。

安装结束后，我们测试一下客户机和服务器之间的通讯状况。双击客户机桌面右下角的防火墙客户端图标，在程序界面中切换到“设置”标签，如下图所示，点击“测试服务器”。



如果测试结果如下图所示，那就代表防火墙客户端和服务器之间的通讯正常。

接下来准备测试客户机使用防火墙客户端访问互联网，在测试之前，先在客户机的浏览器中取消 Web 代理设置，如下图所示。因为如果同时使用 Web 代理和防火墙客户端，访问网站时优先使用 Web 代理。



用浏览器访问微软网站进行测试，如下图所示，OK，防火墙客户端工作正常。同时应注意，防火墙客户端也具有 DNS 转发功能。

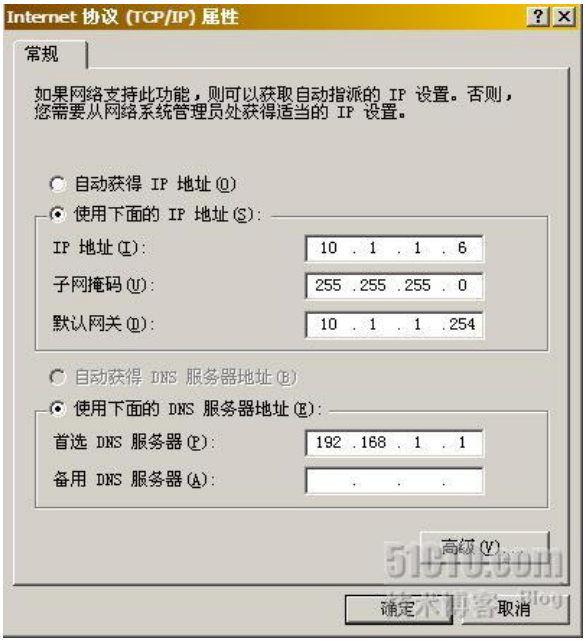
三　SNAT 客户端

微软推荐用户使用 Web 代理和防火墙代理，因为这两种方式都支持用户身份验证。但 Web 代理的功能有限，而防火墙客户端需要在微软操作系统上安装，因此如果用户使用 Linux 等系统，就只能选择 ISA 的 SNAT 代理了。SNAT 代理其实是 Win2003 的路由和远程访问组件所提供的功能，ISA 安装之后接管了路由和远程访问，客户机使用 SNAT 代理是很

方便的，只需将默认网关指向 ISA 的内网 IP 即可。如果配合 DHCP 服务器就更简单了，客户机无需任何设置。

客户机尝试 SNAT 之前先将防火墙客户端关闭，点击桌面右下角的防火墙客户端图标，如下图所示，取消“启用 Microsoft Firewall Client for ISA Server”，这样就可以把防火墙客户端功能禁用了。

设置客户机的 TCP/IP 属性，将默认网关设置为防火墙内网 IP，注意，要设置 DNS 参数，SNAT 服务器不具有 DNS 转发功能。



如下图所示，用 SNAT 访问互联网也很轻松。

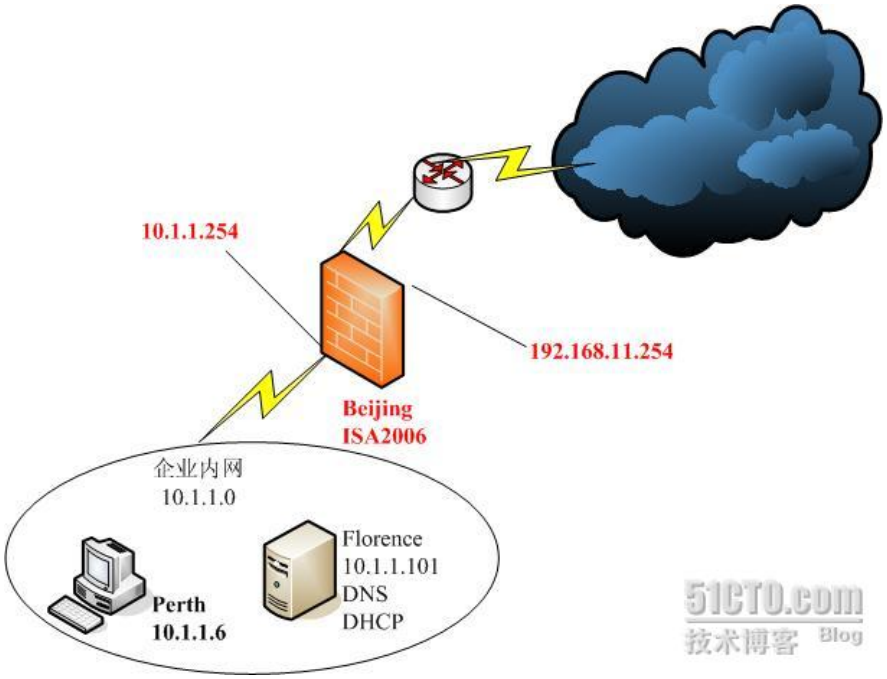
总结：ISA 的三种客户端都能提供访问互联网的功能，Web 代理只允许用户使用浏览器访问互联网，而防火墙客户端和 SNAT 则没有功能方面的限制。如果需要对用户进行身份验证，Web 代理和防火墙客户端就可以大显身手了，事实上，微软推荐用户同时使用 Web 代理和防火墙客户端。为什么不单独使用防火墙客户端呢？因为 Web 代理可以使用 ISA

缓存，真正起到加速作用。如果你希望为用户上网提供尽可能的便利，而且你也不愿意去设置客户端的浏览器或在客户机上安装什么客户端软件，那么 SNAT 必然是你的最爱，只需配好 DHCP 就一切 OK 了。最后要提醒大家的是，Web 代理和防火墙代理都有 DNS 转发功能，而 SNAT 则不存在这个问题。

WPAD 原理介绍暨故障排查：ISA2006 系列之三

WPAD 是 Web Proxy Auto Discovery 的缩写，意思是 Web 代理服务器自动发现。WPAD 的设计目的是让浏览器能自动发现代理服务器，这样用户可以轻松访问互联网而且无需知道哪台计算机是代理服务器。在 ISA2006 中，WPAD 不仅能让客户机浏览器自动发现代理服务器，还可以用于防火墙客户端自动发现代理服务器。显然，WPAD 对代理服务器的透明处理让管理员轻松了不少，管理员不再需要去每台客户机上设置代理服务器参数了。但樱桃好吃树难栽，WPAD 的部署并非都是一帆风顺，WPAD 的部署可以借助 DNS 服务器或 DHCP 服务器，容易出问题的是用 DNS 服务器进行部署，尤其是在工作组环境下问题更多。今天我们就来构造一个实验环境，为大家剖析 WPAD 的工作原理以及故障原因。

实验拓扑如下图所示。内网计算机在工作组环境，Florence 是 DNS 服务器，Perth 是客户机，Beijing 是 ISA2006 服务器。



用 DNS 来实现 WPAD，原理如下：

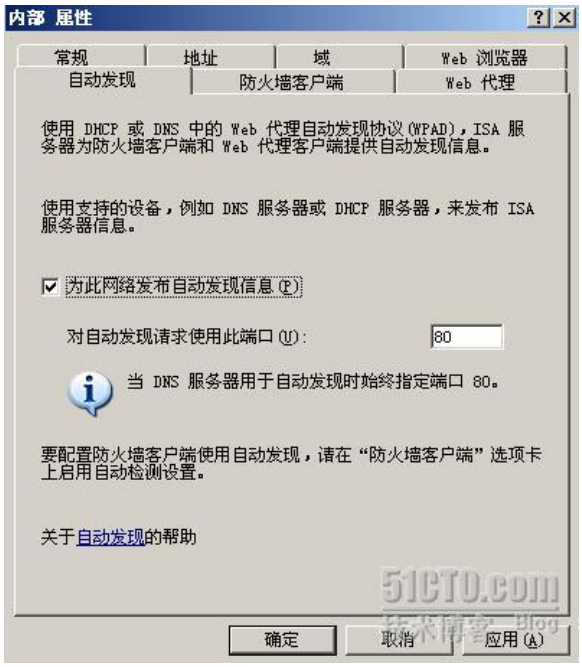
1 Perth 向 DNS 服务器发出查询请求，要求获得 WPAD 主机的 IP 地址。

2 Perth 根据查询到的 IP 地址，去 WPAD 主机的 80 端口下载 WPAD.DAT 或 WSPAD.DAT。WPAD.DAT 可用于配置客户机浏览器，让浏览器自动发现代理服务器；WSPAD.DAT 则用于配置客户机上的防火墙客户端自动发现代理服务器。

从以上的原理分析，首先 WPAD 主机要在 80 端口提供 wpad.dat 和 wspad.dat，有了这两个文件，客户机上的浏览器或防火墙客户端才能实现自动配置。其次，DNS 服务器要创建相关记录，当客户机来查询时，将解析结果指向 WPAD 主机。

好，我们先来解决第一个问题，WPAD 主机如何能够提供 WPAD.DAT 和 WSPAD.DAT 两个文件呢？最简单的办法是让 ISA 服务器作 WPAD 主机，同时提供两个配置文件，具体做法是，在 ISA 服务器上依次点击 开始－程序－Microsoft ISA Server－ISA 服务器管理－配置－网络－内部，右键点击“内部”，选择属性，如下图所示，切换到“自动发现”标签，

勾选“为此网络发布自动发现信息”，这样 ISA 就可以在 80 端口提供 WPAD.DAT 和 WSPAD.DAT 两个文件了。

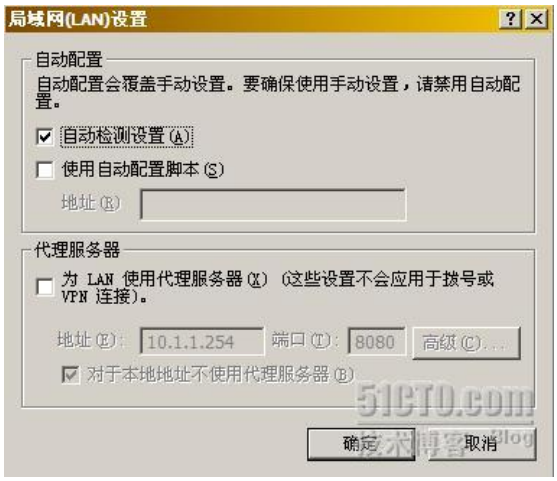


测试一下，看看 ISA 服务器是否提供了配置文件。如下图所示，在浏览器中输入 http://10.1.1.254/wpad.dat，测试结果如下图所示，这表明 ISA 服务器已经在 80 端口发布了 WPAD.DAT，用同样的方法可知 ISA 也发布了 WSPAD.DAT。

WPAD 主机已经在 80 端口提供了 WPAD.DAT 和 WSPAD.DAT，一个问题解决了，接下来我们考虑另一个问题，客户机到底是怎么通过 DNS 来查询 WPAD 主机呢？具体是这样的，客户机向 DNS 发出一个查询请求，请求解析的域名为 WPAD+X。怪了，怎么会是 X 呢？X 代表不确定性，如果客户机所在的域为 itet.com，那么客户机就请求解析 wpad.itet.com；如果客户机没加入域，但计算机名的后缀为 abc.com，那么客户机就请求解析 wpad.abc.com；如果客户机既没有加入域，也没有计算机名后缀，那客户机就请求解析 wpad。这里是 WPAD 配置的关键所在，为什么论坛上很多管理员在域环境配置 WPAD 很正常，换到工作组环境就容易出问题呢？因为域环境下有统一的名称边界，客户机请求解析的域名后缀是固定的，而工作组的有组织无纪律特性决定了它的解析请求是无规律的。

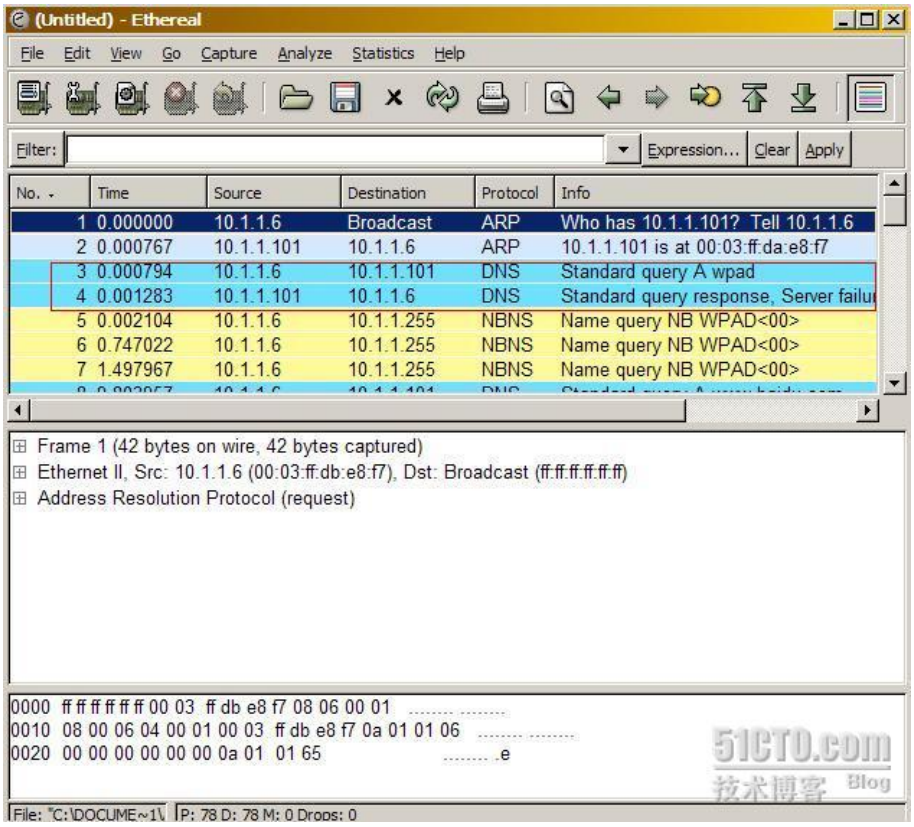
下面举个具体的例子。如下图所示，Perth 属于工作组，Perth 将 10.1.1.101 作为自己的 DNS 服务器，我们分析一下 Perth 是如何利用 DNS 来自动发现代理服务器的。

将 Perth 的浏览器配置为自动检测发现，在 IE 浏览器中依次点击 工具－Internet 选项－连接－局域网设置，如下图所示，勾选“自动检测设置”。



在 Perth 上打开浏览器访问一个网站，同时启用 Ethereal 抓包追踪，抓包结果如下图所示，我们可以看到 Perth 请求 DNS 服务器解析域名 WPAD，服务器解析失败后 Perth 又试图用广播进行名称解析，名称解析失败后 Perth 无法找到 WPAD 主机去下载 WPAD.DAT，代理服务器自动发现失败。

很多朋友在论坛中发帖说自己在工作组中配置 WPAD 时出问题，其实问题就出在 DNS 服务器无法解析域名 WPAD。



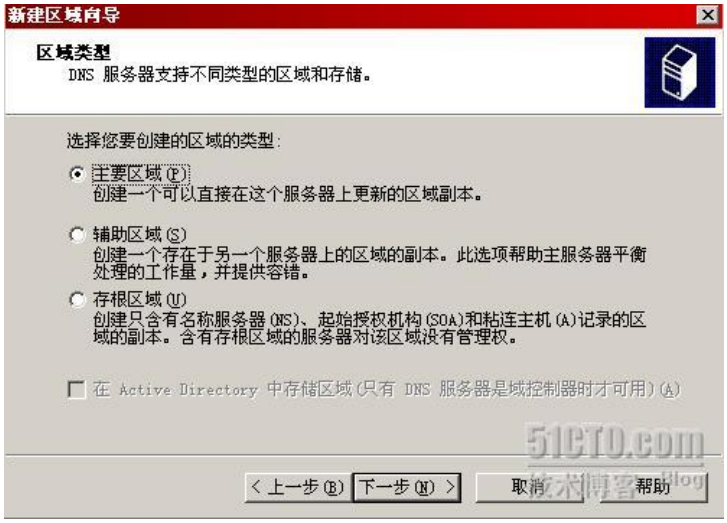
好，WPAD 配置出问题了，而且是意料之中的，那如何解决呢？两种思路，一是想办法让 DNS 服务器能解析出域名 WPAD，二是想办法让 Perth 查询一个 DNS 服务器容易回答的域名。我们沿着这两种思路来尝试一下。

一　让 DNS 服务器能解析域名 WPAD

WPAD 这个域名为何难以解析呢？从结构上分析，WPAD 域名隶属于根域，一般 DNS 服务器对根域根本就没有解析资格，因此解析这种域名有点勉为其难。兄弟不才，尝试用 DNS 私有根来解决这个问题，在 DNS 服务器中右键点击正向查找区域，如下图所示，选择“新建区域”。

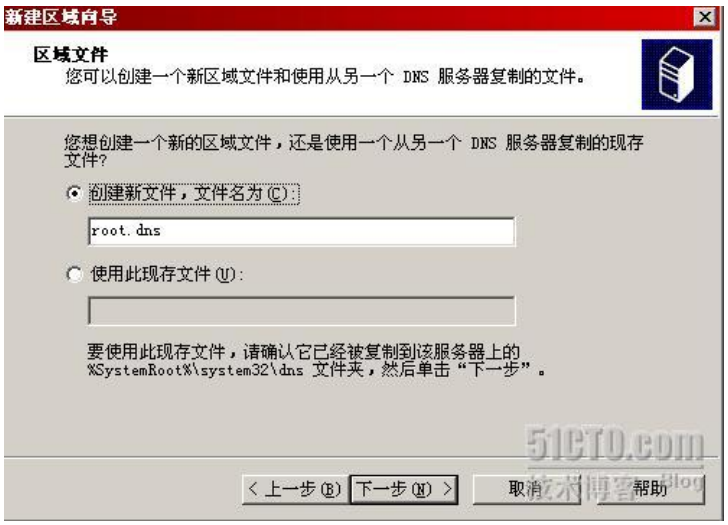
出现新建区域向导，下一步。

新建区域类型为主要区域，下一步。

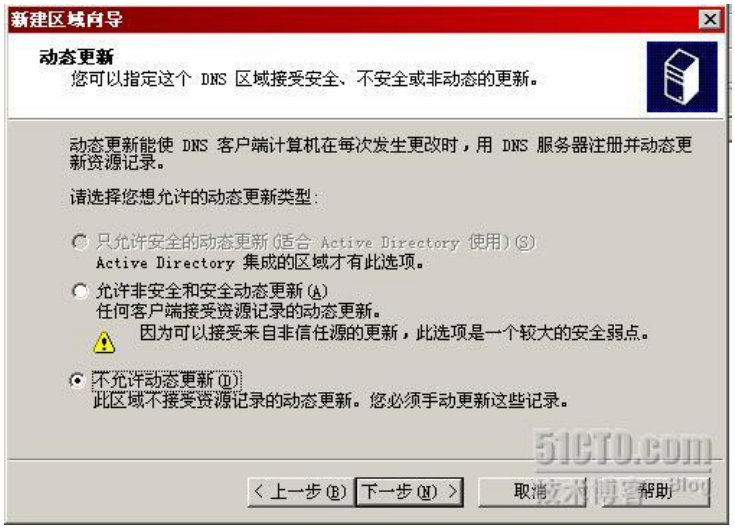


区域名称为. ，这就是传说中的根域。

根域的区域数据文件为 root.dns。



不需要允许动态更新，下一步后结束私有根域创建。

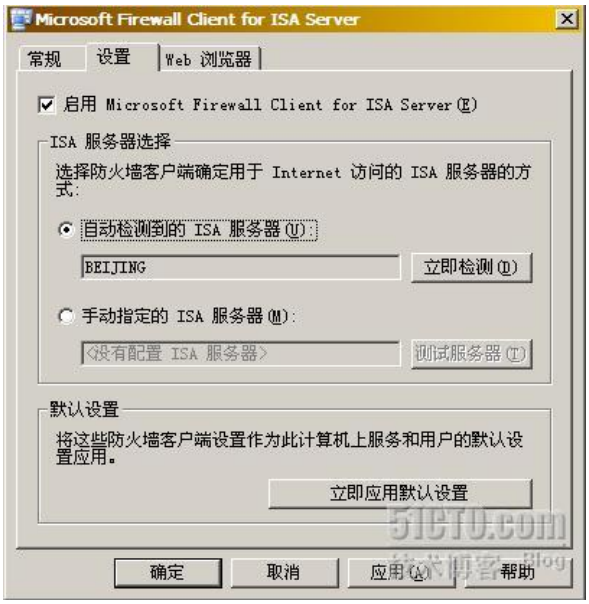


创建根域后，我们需要在根域中为 WPAD 主机创建 A 记录，如下图所示，选择“新建主机”。

完全合格域名为 WPAD.，IP 为 ISA 服务器的内网地址。

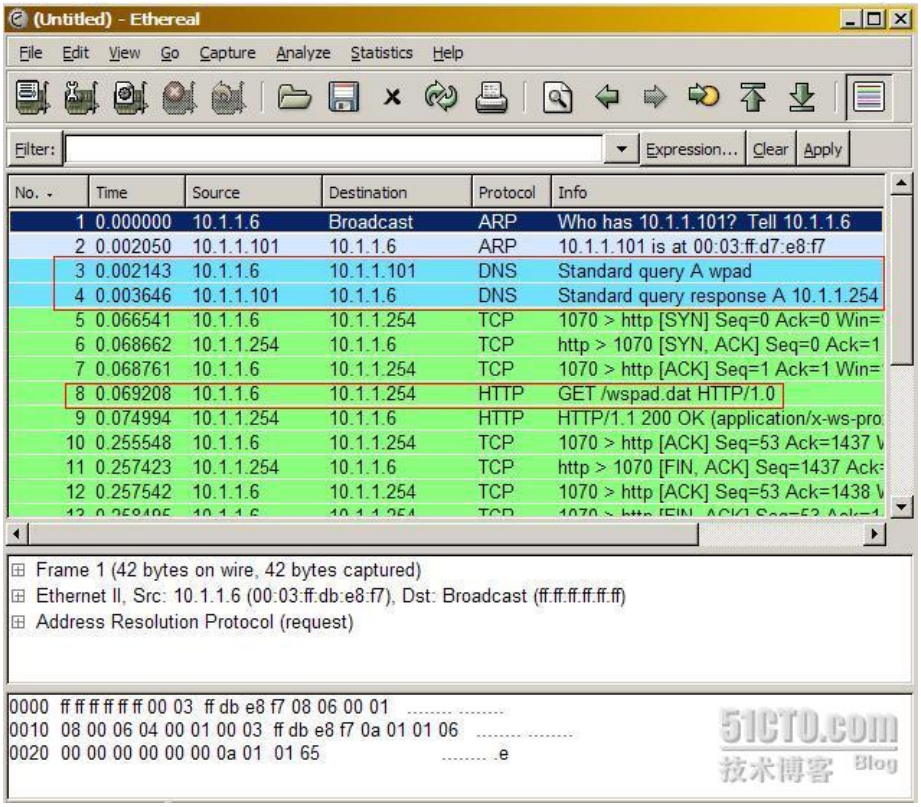
OK，如下图所示，WPAD 记录已经创建完毕，我们来试试能否发挥作用呢？

这次我们在 Perth 上安装上防火墙客户端，从理论上分析，防火墙客户端需要从 WPAD 主机下载 WSPAD.DAT，我们双击防火墙客户端，切换到“设置”标签，选择“自动检测到的 ISA 服务器”，点击“立即检测”。

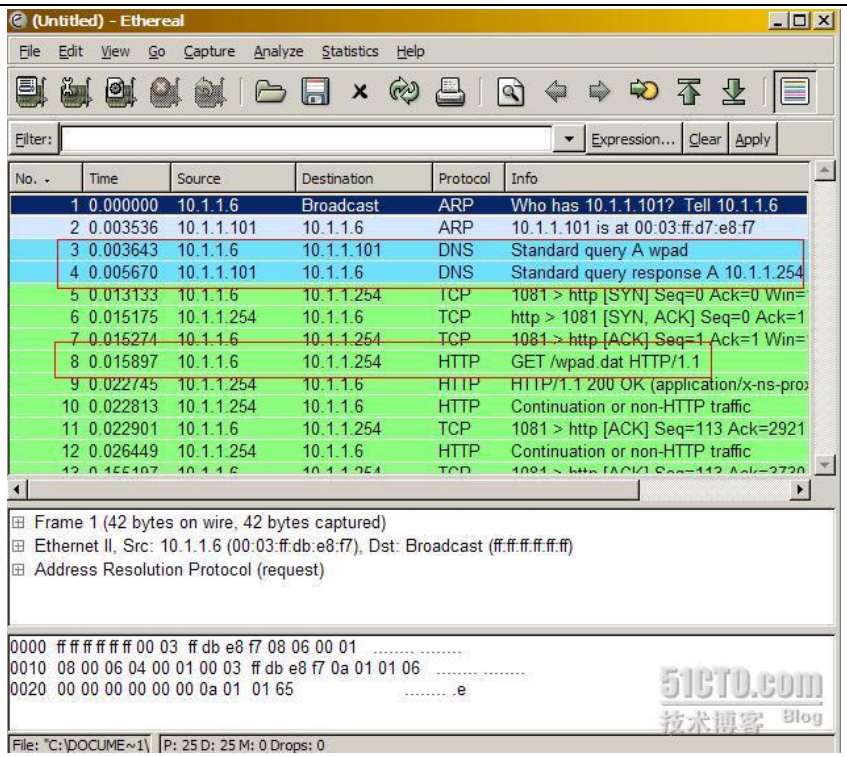


测试结果如下，防护器客户端成功地发现了代理服务器。

别忘了把自动检测的过程用 Ethereal 抓下来，如下图所示，我们可以很清楚地看到，Perth 请求 DNS 服务器解析域名 WPAD，DNS 服务器将域名解析为 10.1.1.254（私有根起作用了），Perth 接下来就去 10.1.1.254 下载 WSPAD.DAT，用此文件将防火墙客户端所使用的代理服务器设置为 Beijing。



上次我们用浏览器自动检测失败了，这次再试试，用 Ethereal 抓包，结果如下图所示。我们可以看到客户机也是先请求 DNS 服务器对 wpad 进行域名解析，然后根据解析结果到 ISA 服务器请求下载 WPAD.DAT，文件下载之后就可以用于配置浏览器了。



从上述实验来看，通过 DNS 的私有根来解决 WPAD 域名解析在技术层面是可行的，但这种方法其实有很大隐患。创建了私有根后会影响互联网上的域名解析，而且转发器也不能使用，

兄弟至此也没找到两全其美的办法，如果哪些弟兄有经验，还望不吝赐教。因此，我的结论是，除非你的单位本来就要部署私有根，否则还是别用这种方法解决问题，实在是弊大于利。

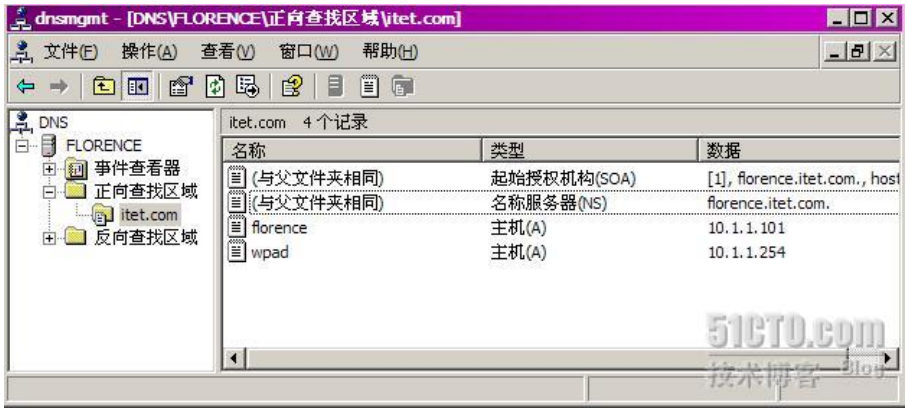
二　Perth 换查询域名

既然 Perth 发起的 WPAD 域名解析让 DNS 服务器处理起来很为难，那能否让 Perth 换一个域名查询呢？例如让 Perth 查询 wpad.itet.com，这样的域名 DNS 处理起来不要太轻松哦！问题是，如何能让 Perth 更换查询域名呢？秘密就在 Perth 的计算机名中，如果我们希望 Perth 查询的域名是 wpad.itet.com，只需将 Perth 的计算机名的 DNS 后缀改为 itet.com 即可。操作具体如下，在 Perth 上用右键单击“我的电脑”，在属性中切换到“计算机名”标签，如下图所示，点击“更改”。

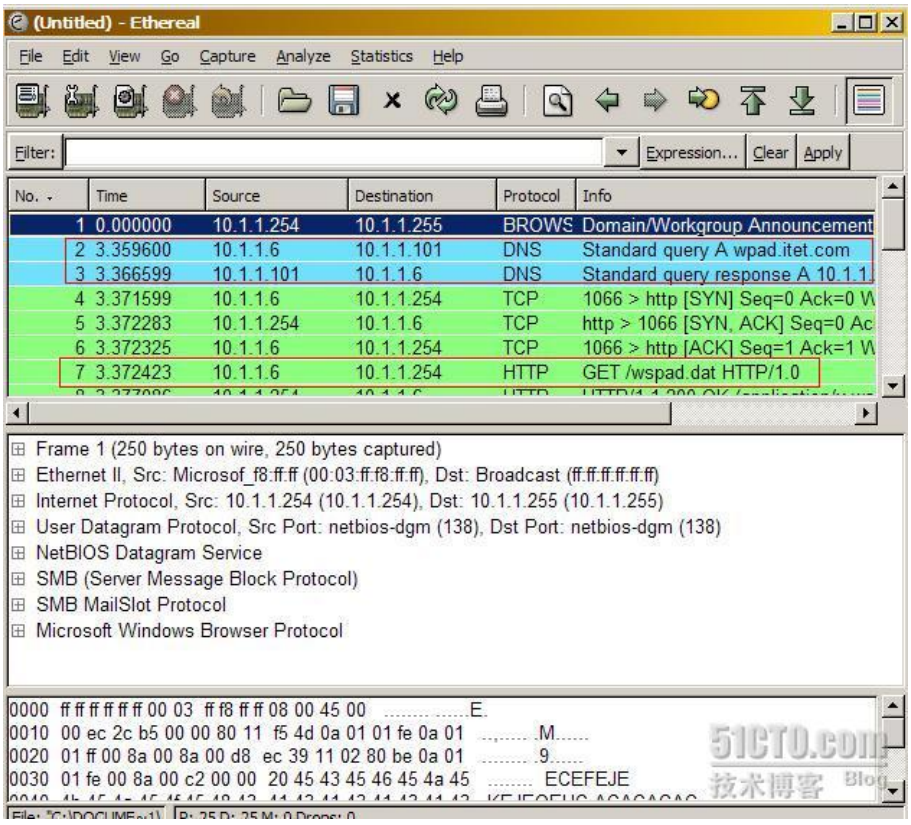
在计算机名称更改中，点击“其他”，如下图所示。

在计算机的 DNS 后缀处填写“itet.com”，点击确定后重新启动计算机。

在 DNS 服务器上创建区域 itet.com，并新建一个名为 WPAD 的 A 记录，如下图所示。现在 WPAD 记录已经有了，就等着客户机来查询了。



在客户机上用防火墙客户端测试一下，如下图所示，我们可以看到客户机发出的查询已经改为 wpad.itet.com 了，服务器把域名解析为 ISA 的内网 IP，随后客户机就去 ISA 下载 wspad.dat 了。呵呵，如果客户机是在域环境下，根本就无需更改计算机名后缀，想想其实还是有 AD 比较方便。



总结：用 DNS 部署 WPAD 在域环境下比较合适，在工作组环境下就需要进行一些调整，但无论是创建 DNS 私有根还是更改客户机的计算机名后缀，都不算是非常完美的解决方案。因此我们建议在工作组环境下可以考虑用 DHCP 来解决这个问题，我们在下篇博文中将介绍如何利用 DHCP 来解决 WPAD 部署的问题。

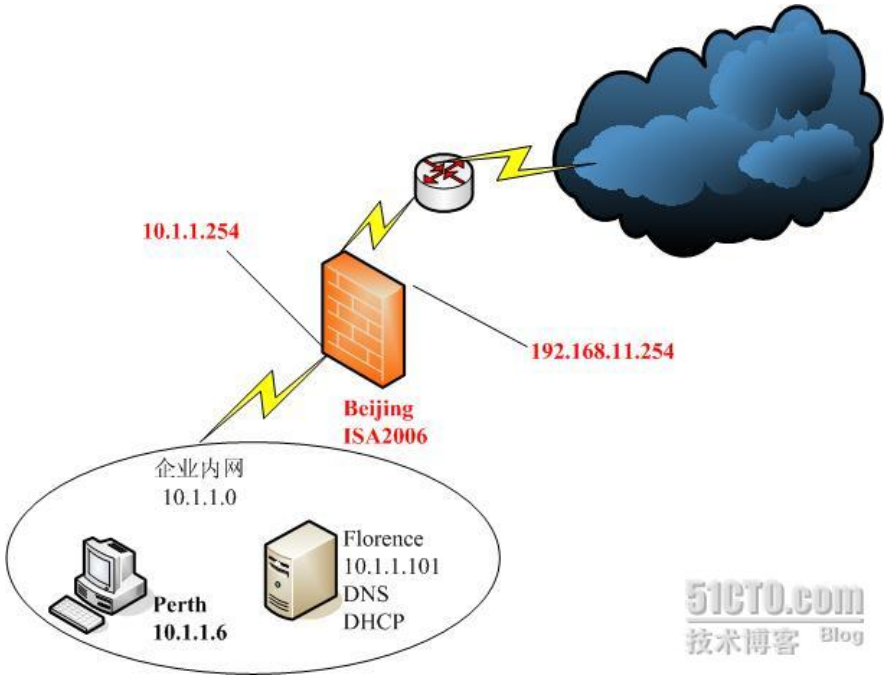
用 DHCP 部署 WPAD：ISA2006 系列之四

上篇博文中我们分析了用 DNS 部署 WPAD 的原理，然后得出一个结论，在域环境下用 DNS 部署 WPAD 很方便，在工作组下效率就不是很理想。因此今天我们介绍另外一种 WPAD 部署方案作为补充，即通过 DHCP 实现 WPAD。这样大家可以更好地根据自己的实际环境选择合适的技术方案，其实在部署 WPAD 时，我们既可以单独使用 DNS 或 DHCP，也可以将两种技术结合起来使用，已达到最佳效果。

DHCP 部署 WPAD 的原理是这样的。DHCP 服务器中有一个 252 选项，252 项通常被当作查询或注册用的指针，我们可以通过 252 项发现打印机，时间服务器，WPAD 主机以

及其他的网络服务器。既然 252 项有如此神通，那我们只要在 DHCP 服务器中添加一个用于查找 WPAD 主机的 252 项就行了，252 项是一个字符串值，内容是 WPAD 主机的 URL。这样一来，DHCP 客户机就能知道 WPAD 主机的位置，当客户机需要对浏览器或防火墙客户端进行自动配置时，就可以到 WPAD 主机下载所需的配置文件了。

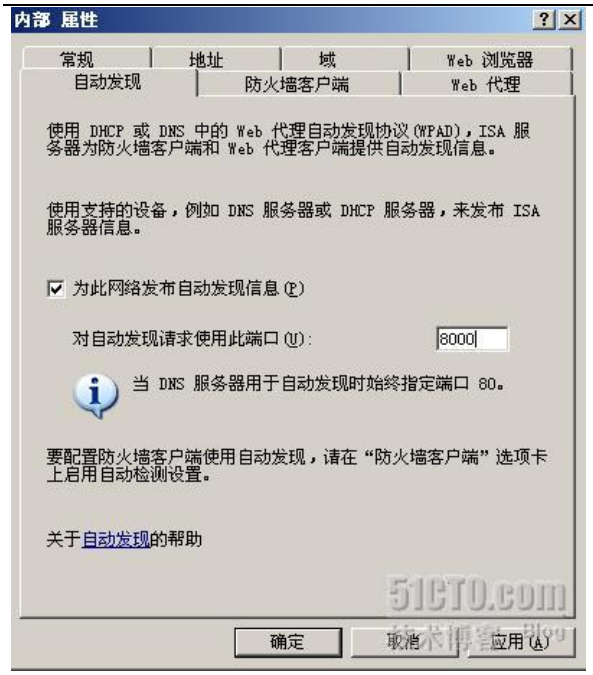
构建一个实验环境，实验拓扑如下图所示，Beijing 是 ISA2006 服务器，Florence 是 DHCP 服务器，Perth 是客户机，所有计算机都在工作组环境下。



51CTO.com
技术博客 Blog

一 ISA 服务器提供配置文件

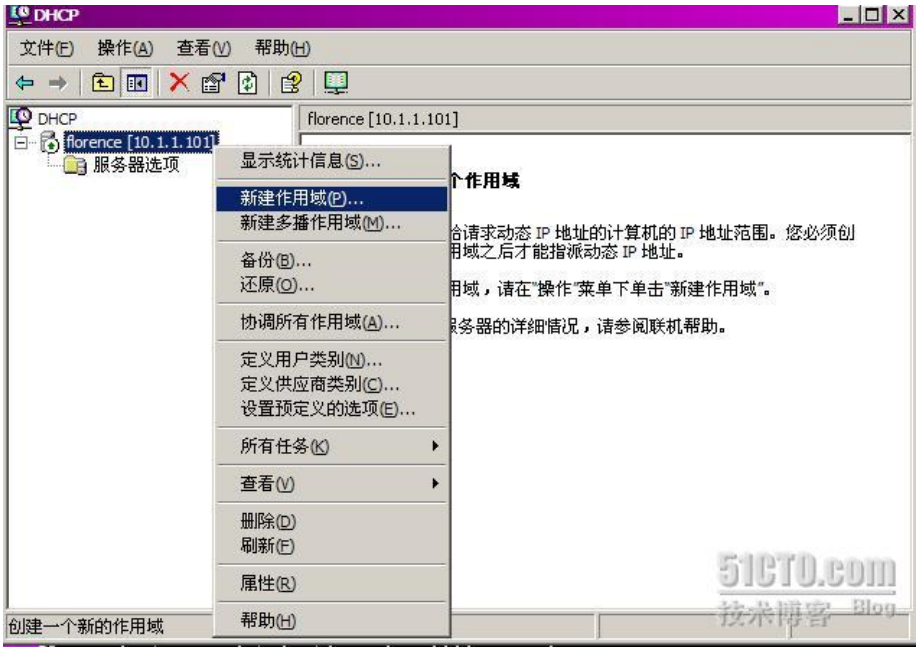
用 DHCP 部署 WPAD 具有很大的灵活性，ISA 可以在任意端口提供 WPAD.DAT 和 WSPAD.DAT，不象 DNS 那样，必须限制在 80 端口。我们准备在 ISA 的 8000 端口提供配置文件，在 ISA 服务器上依次点击 开始－程序－Microsoft ISA Server－ISA 服务器管理－配置－网络－内部，在内部网络属性中切换到自动发现标签，如下图所示，我们将自动发现的端口设置为 8000。



二 DHCP 服务器配置

1）创建作用域

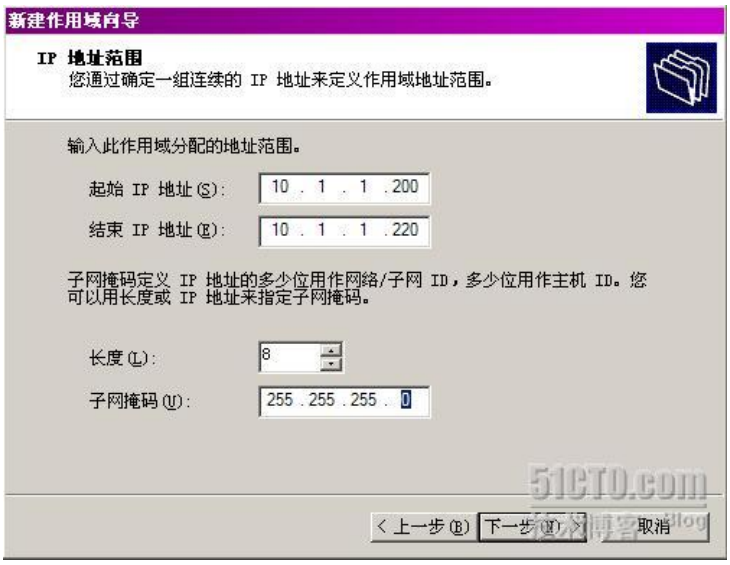
在DHCP服务器上依次点击 开始－程序－管理工具－DHCP，右键点击DHCP服务器，如下图所示，选择“新建作用域”。



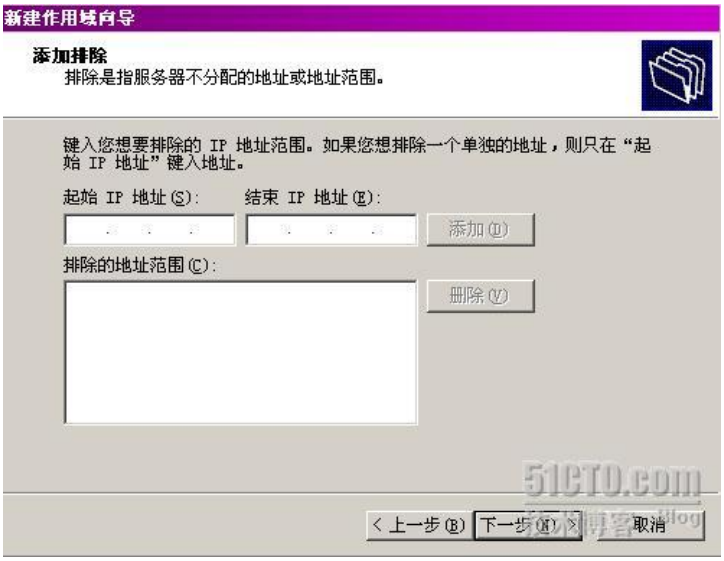
出现新建作用域向导，点击下一步。

输入作用域的名称和描述，点击下一步。

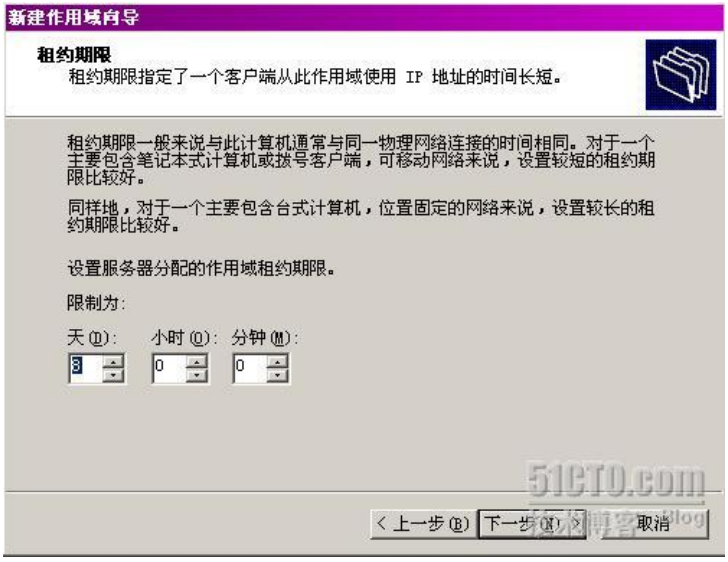
为作用域定义地址范围，如下图所示，我们将地址范围定义为 10.1.1.200-10.1.1.220，子网掩码为 C 类网掩码。



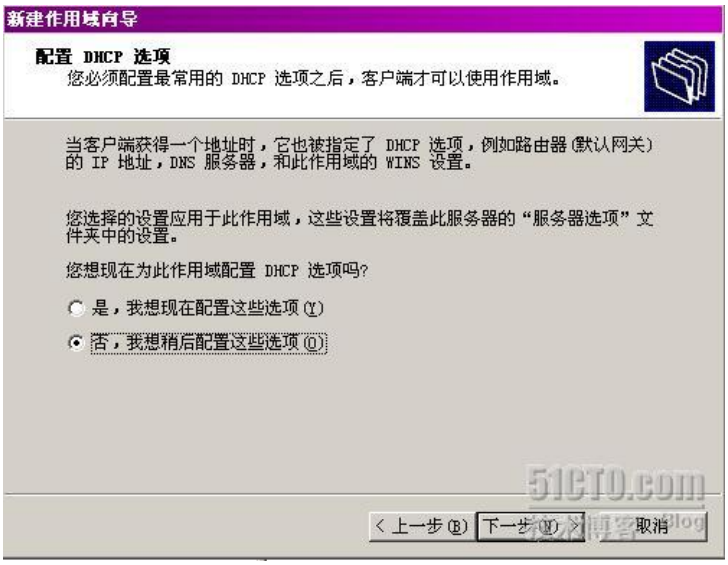
创建地址排除范围，本例中我们不排除任何地址。



地址租约我们选择用默认期限。



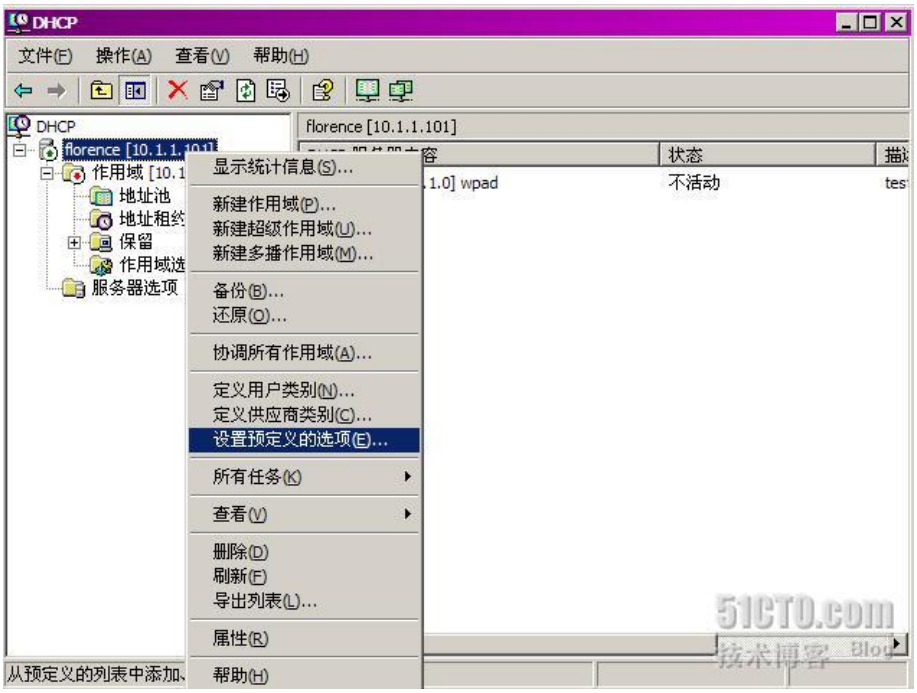
以上我们创建了一个作用域，然后我们暂时不要配置作用域选项，等我们创建了 252 项后再配置作用域选项。



点击“完成”结束作用域创建。

2）在 DHCP 选项中创建 252 项

在 DHCP 管理器中右键单击服务器，如下图所示，选择“设置预定义的选项”。



在预定义选项中，选择“添加”。

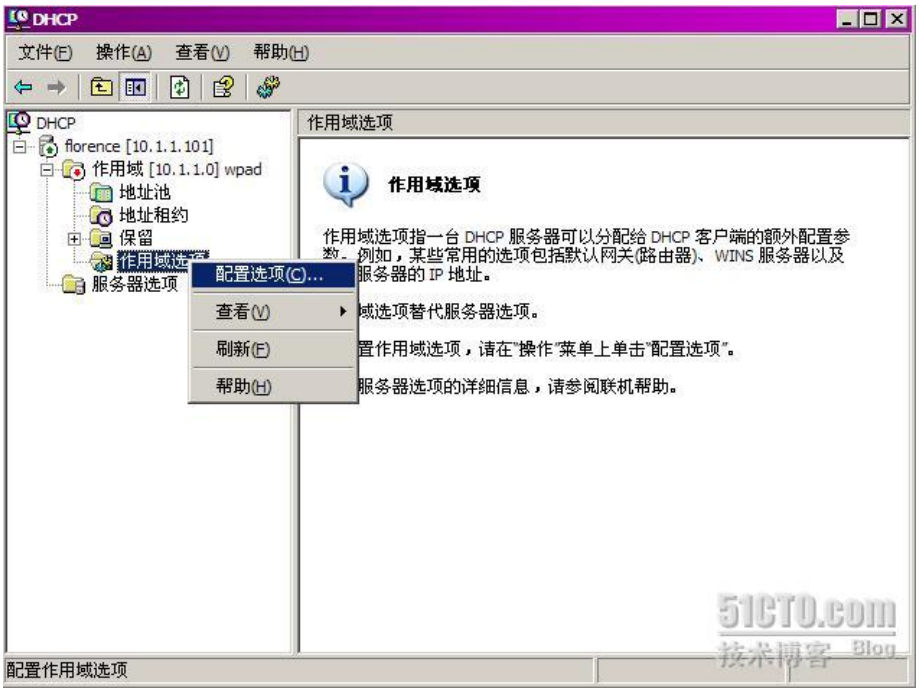
添加一个 DHCP 选项，名称为 WPAD（大写），数据类型为字符串，代码为 252。

为添加的 252 选项赋值为 http://10.1.1.254:8000/wpad.dat，这样 DHCP 服务器就可以通过 252 选项为客户机指示 WPAD 主机了。要注意的是，虽然从我们在 252 项中填写的内容来看似乎只能为浏览器提供自动发现代理服务，但实际上防火墙客户端也可以使用 252 项，当防火墙客户端需要寻找代理服务器时，防火墙客户端会自动访问 http://10.1.1.254:8000/wspad.dat。

3）配置 DHCP 作用域选项。

我们在 DHCP 作用域选项中配置 252 选项和 DNS 选项，为了避免让客户机使用 SNA T 客户端，我们就不配置路由器选项了。

如下图所示，右键单击作用域选项，选择“配置选项”。

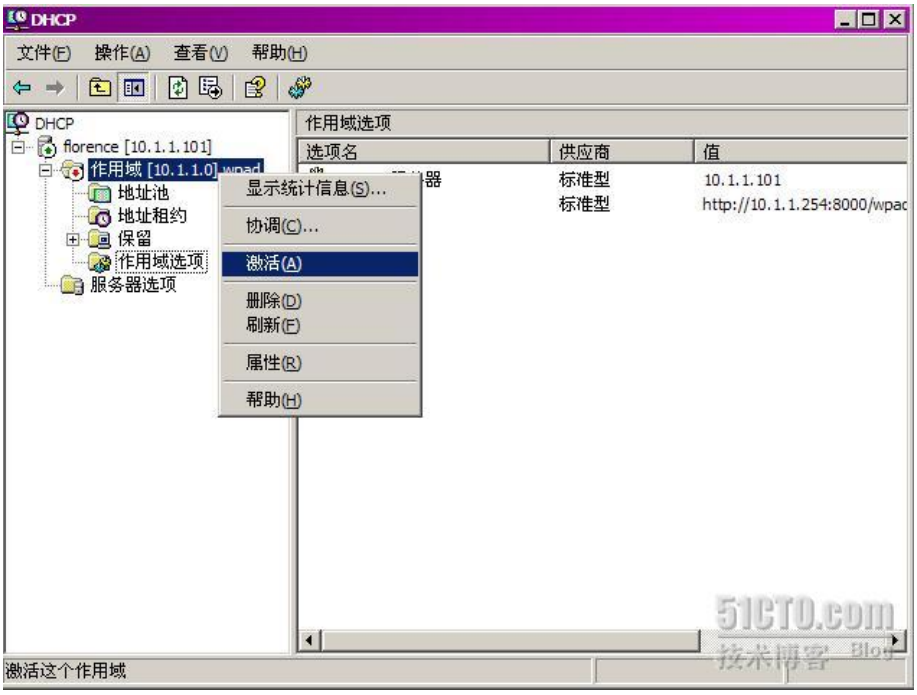


确保在作用域选项中选中了 WPAD 项，如下图所示。

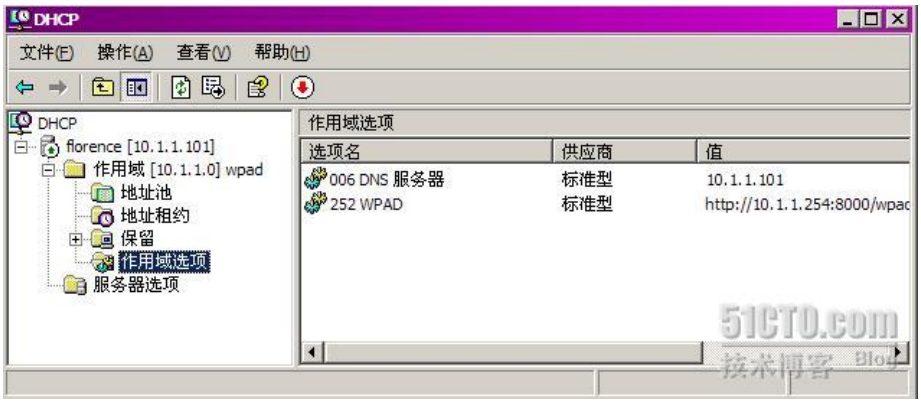
DNS 项也配置一下，虽然理论上 Web 代理和防护器客户端都具有 DNS 转发功能。

4）激活

配置完 DHCP 选项后，我们来激活 DHCP 作用域，如下图所示，右键点击作用域，选择“激活”。

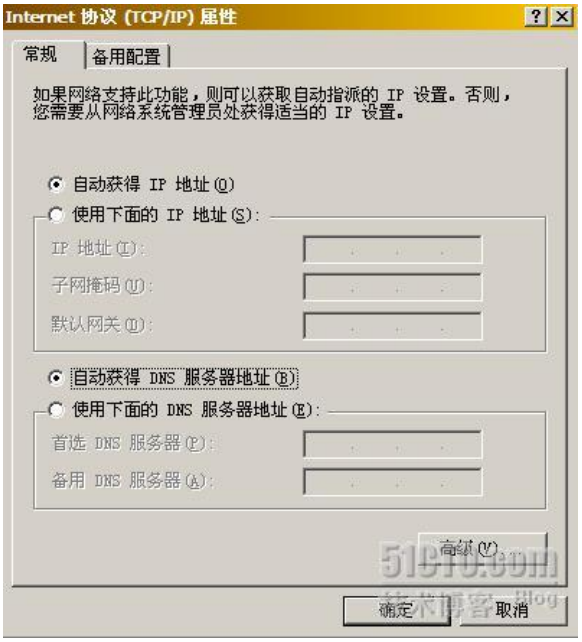


如下图所示，DHCP 作用域已被激活。



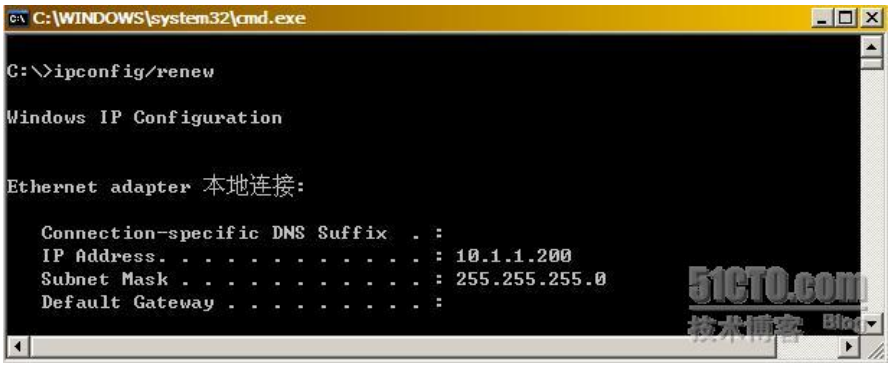
三 客户机测试

ISA 服务器和 DHCP 服务器都已经作好准备了，最后我们在客户机上测试一下，看看我们之前做的是不是有用功。如下图所示，在客户机 Perth 上将 TCP/IP 属性设置为自动获得 IP 地址。

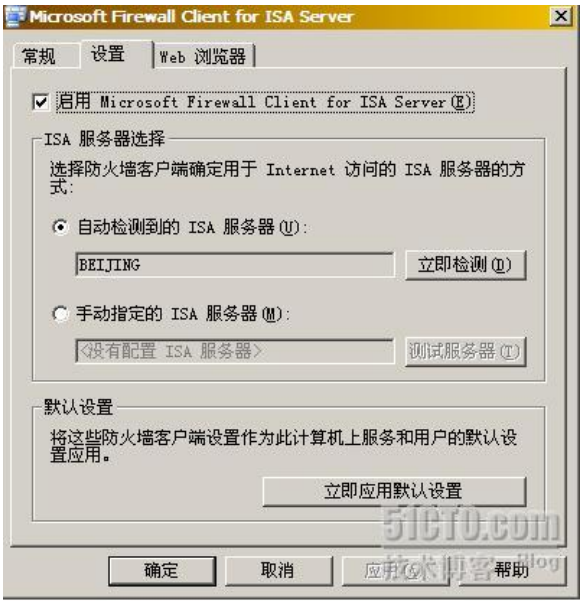


如果不能立即获得 IP，可以用命令 IPCONFIG/RENEW，强制客户机发出 DHCP Discover，

如下图所示，命令使用后立竿见影，客户机获得了 IP 地址。



那客户机有没有获得最关键的 252 选项呢？我们在客户机上用防护器客户端来测试一下，在防护器客户端属性的设置标签中选择“自动检测到的 ISA 服务器”，如下图所示，点击“立即检测”。



如下图所示，检测成功，哈哈，DHCP 部署 WPAD 成功了。

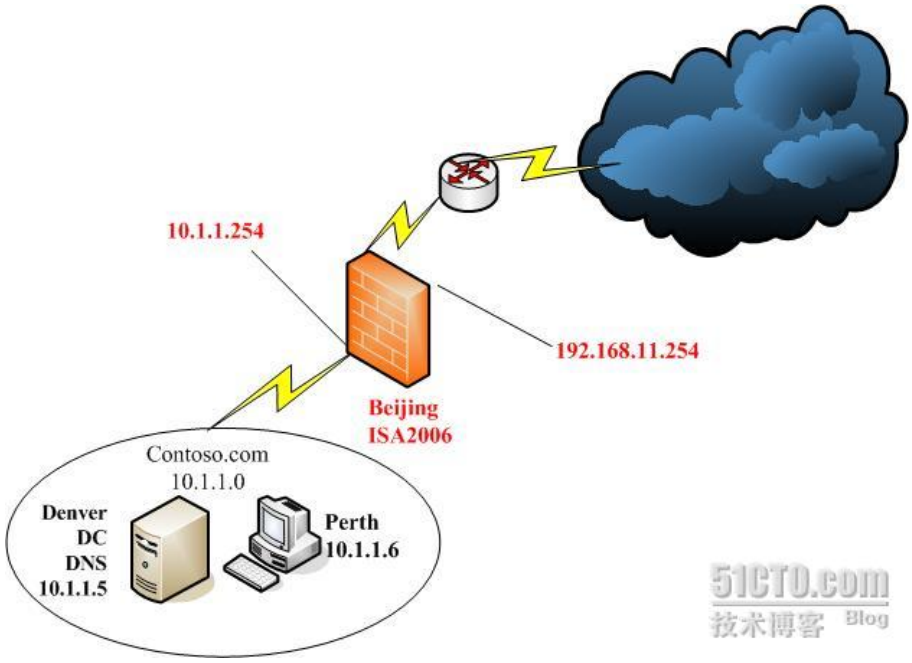
小结：用 DHCP 部署 WPAD 还是很方便的，既不限制端口，又不受客户机计算机名影响，无论是工作组还是域都能很好地工作，个人建议管理员应更多考虑。DHCP 精练使用，确实是居家旅行，杀人灭口之必备良药，哈哈：）

实例详解 ISA 防火墙策略元素：ISA2006 系列之五

我们在前面的工作中已经实现了 ISA2006 的代理服务器功能，接下来我们要实现 ISA 的访问控制功能。很多公司都有控制员工访问外网的需求，例如有的公司不允许员工访问游戏网站，有的公司不允许员工使用 QQ 等即时通讯工具，有的公司禁止员工下载视频文件，还有的公司只允许访问自家的门户网站.....这些需求都可以通过 ISA2006 防火墙策略中的访

问规则来加以实现。既然如此，那我们赶紧来写上几条访问规则测试一下吧。别急，访问规则是由策略元素构成的，我们要想写出访问规则，首先要掌握策略元素，还是让我们从学习策略元素开始吧。

准备一下实验环境，拓扑如下图所示，Denver 是 Contoso.com 的域控制器，Perth 是域内的工作站，Beijing 是 ISA2006 服务器，Beijing 也加入了域。



我们的目标是先写出一条访问规则：允许在午休时间（12:00-13:00），人事部和财务部的员工可以访问互联网上除百度之外的网站，而且访问网站时不能访问视频和音频内容，我们通过这条规则的实现过程来学习策略元素。

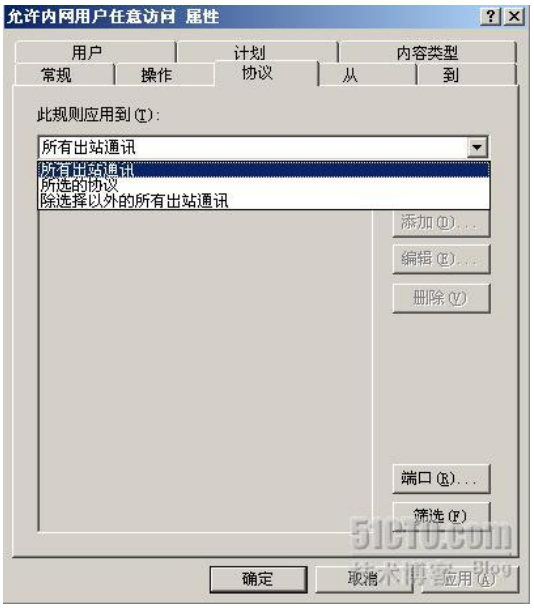
如下图所示，打开 ISA 服务器管理，选中防火墙策略，此时右侧面板的工具箱中显示的就是策略元素，大家看到的有协议，用户，内容类型，计划，网络对象等，下面我们一一展开分析。

一 协议

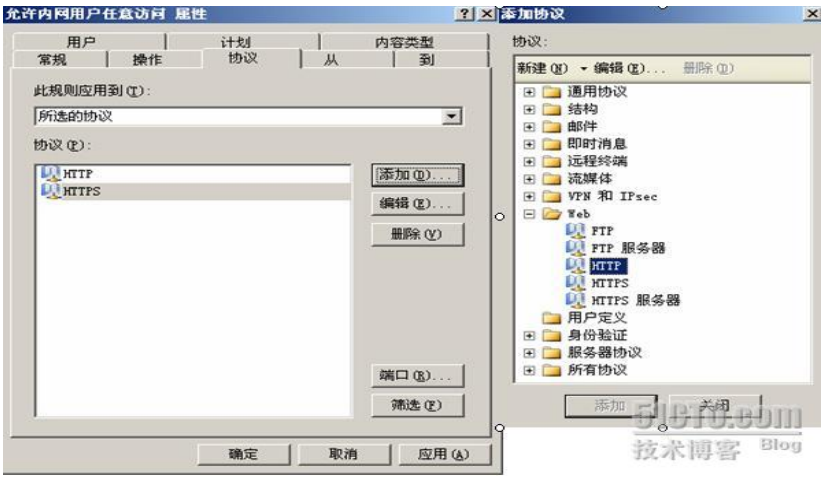
协议元素限制了用户问外网时所使用的网络协议。例如我们此次实验的目标是只允许部分用户访问一些特定网站，那我们就可以在访问规则的协议元素中限定用户只可以使用 HTTP 和 HTTPS，这样就保证了用户只能访问网站。当前 ISA 中有一个很宽泛的访问规则，如下图所示，允许内网和本地主机可以使用任何协议，在任何时间，以任何用户的身份，访问任意网络的任意内容。这条规则是我们在前面测试代理服务器的时候创建的，现在我们对它动动手术，只允许用户用 HTTP 和 HTTPS 访问外网。

下图是当前的访问规则，我们可以看到 ISA 允许使用任何协议对外访问，右键点击规则，查看规则属性。

在规则属性中切换到“协议”标签，如下图所示，将规则的应用范围从原先的“所有出站通讯”改为“所选的协议“，只允许使用特定的协议。



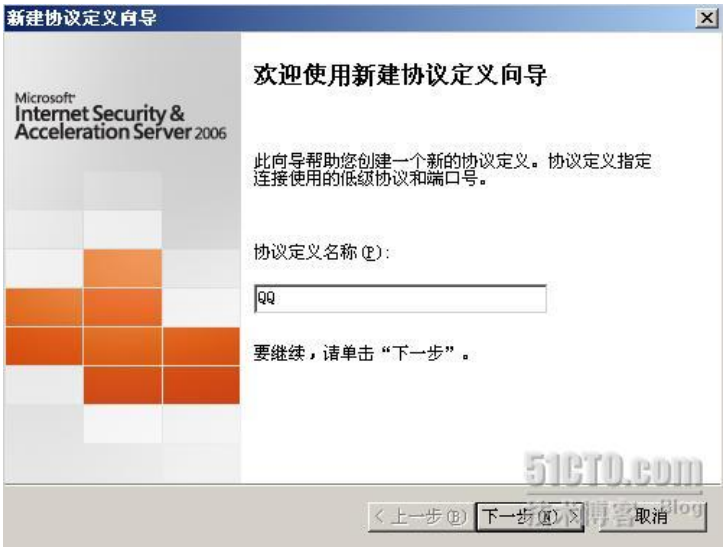
点击“添加”按钮，在协议中选择 HTTP 和 HTTPS 添加进来，如下图所示，添加完协议后点击确定。



如下图所示，访问规则已经被修改为 ISA 只允许 HTTP 和 HTTPS 协议通过。

我们使用协议元素可以在访问规则中轻松实现对协议的控制，但如果我们要控制的协议没有在 ISA 的协议元素中被定义那该怎么办呢？我们可以自定义协议元素，例如我们希望禁止用户使用 QQ 的通讯协议，我们就可以在防火墙策略的工具箱中选择“新建协议”，如下图所示。

出现新建协议向导，我们为新建的协议命名为 QQ，下一步。



接下来我们定义协议参数，点击“新建”。

我们定义 QQ 协议使用 UDP，方向为发送接受，端口为 8000。

QQ 不需要使用辅助连接，但有些协议例如 FTP 需要使用辅助连接。

结束新建协议向导。

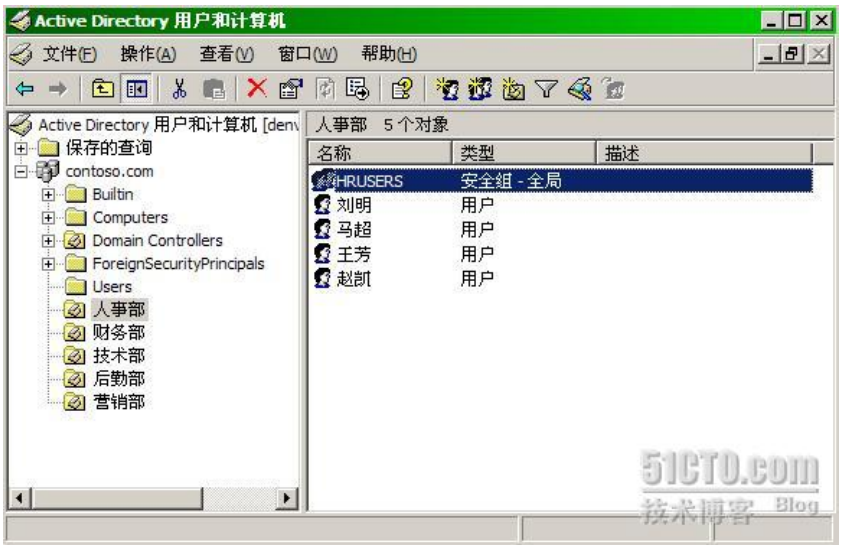
这样我们就创建了一个自定义协议 QQ，按照这种办法，我们可以将所需的协议元素都创建出来，然后就可以在访问规则中灵活地加以控制了。

二 用户

用户元素可以控制有哪些人能访问外网，尤其在域环境下，用户元素更是可以大显身手。依靠用户元素控制网络访问远比用 IP 控制来得更方便灵活。记得我刚工作时曾经在路由器

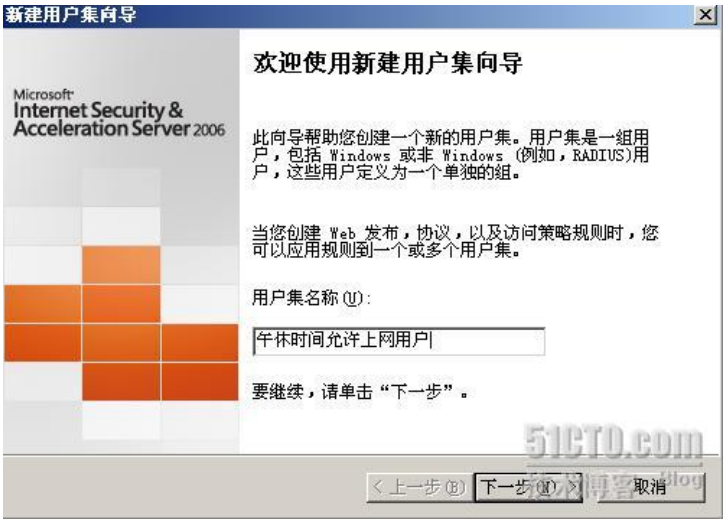
上用 IP 控制用户上网，没过多久，就被很多人发现了秘密，一时间大家纷纷抢占那几个能上网的 IP，IP 冲突此起彼伏。虽然可以用 ARP 静态绑定来解决，但处理起来还是感觉麻烦。因此奉劝诸位，部署网络架构时如果有可能还是应该上 Active Directory，无论如何管理起来都感觉方便得多。

在本例中我们希望只允许人事部和财务部的员工在午休时间访问互联网，那应该怎么定义人事部和财务部的用户呢？这时用户元素就派上用场了，用户元素可以和 Active Directory 中的用户管理接合起来，如下图所示，Active Directory 中已经为所有部门用户都创建了用户账号和组账号。



在 ISA 防火墙策略的工具箱中，展开“用户”，如下图所示，选择“新建”。

为新创建的用户元素命名为“午休时间允许上网用户”，点击下一步。



点击“添加”按钮，选择添加“Windows 用户和组”，如下图所示。

在活动目录中查找对象，输入组名 hrusers 和 financeusers，这是人事部和财务部用户所隶属的组，点击确定。

如下图所示，新创建的用户元素中已经列出了人事部和财务部两个组，点击下一步完成创建。

创建了用户元素，我们就可以修改访问规则了。如下图所示，在访问规则中切换到用户标签，选择“所有用户”，点击“删除”，然后再点击“添加”按钮。

添加“午休时间允许上网用户”。

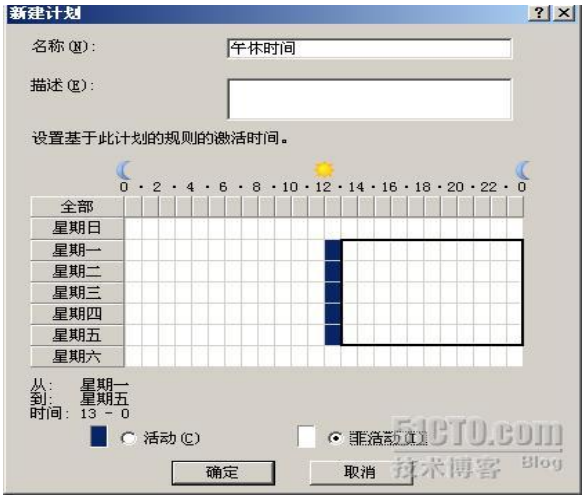
如下图所示，修改后的规则离我们的目标又进了一步。

注意：要实现用户身份验证，必须使用 Web 代理客户端或防火墙客户端，SNAT 客户端不支持用户身份验证。

三 计划

计划元素可以用来表示时间范围，例如我们的目标规则中打算限定财务部和人事部的用户在午休时间有限上网，这午休时间该如何表示呢？通过计划元素就可以轻松完成。在策略工具箱中展开“计划”对象，如下图所示，选择“新建”。

为新建的计划元素取名为“午休时间”，如下图所示，我们将午休时间定义为周一到周五的 12 点至 13 点。

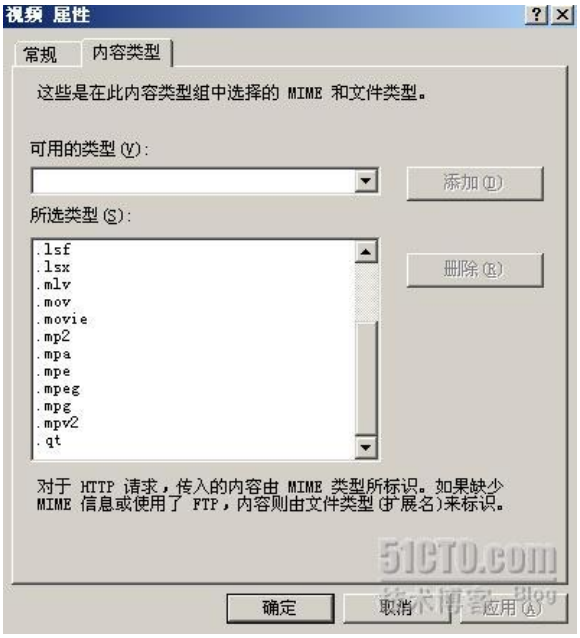


创建了计划元素后，我们又来修改访问规则了，如下图所示，我们将计划从原先的“总是”改为“午休时间”，我们离目标越来越近了。

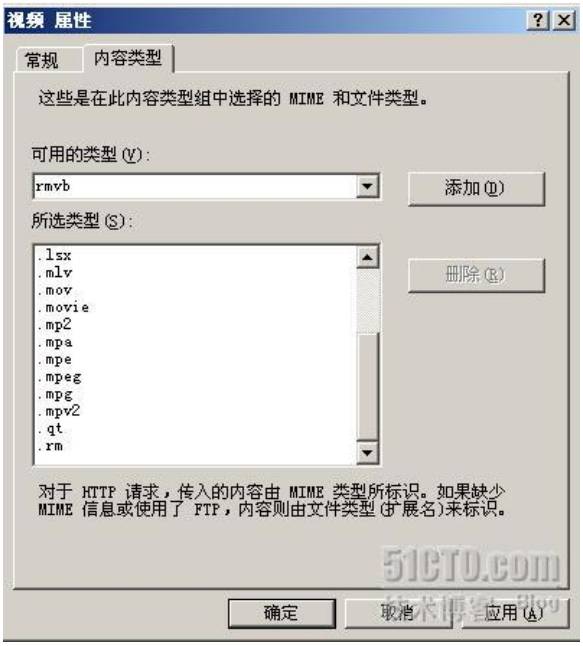
四 内容类型

内容类型元素负责将访问互联网的数据划分为音频，视频，文本，HTML 文档等类型，利用内容类型我们可以更精细地控制用户对网络内容的访问，唯一有些遗憾的就是 ISA 在划分内容类型时，仍然采用了不可靠的文件名检测方法，这有可能会让某些用户有机可乘。我们此次实验的目标之一是不允许访问音频和视频内容，这个目标依靠内容类型可以很容易实现。在策略工具箱中展开“内容类型”，如下图所示，我们看到共有十一种类型，选择视频类型，编辑一下看看。

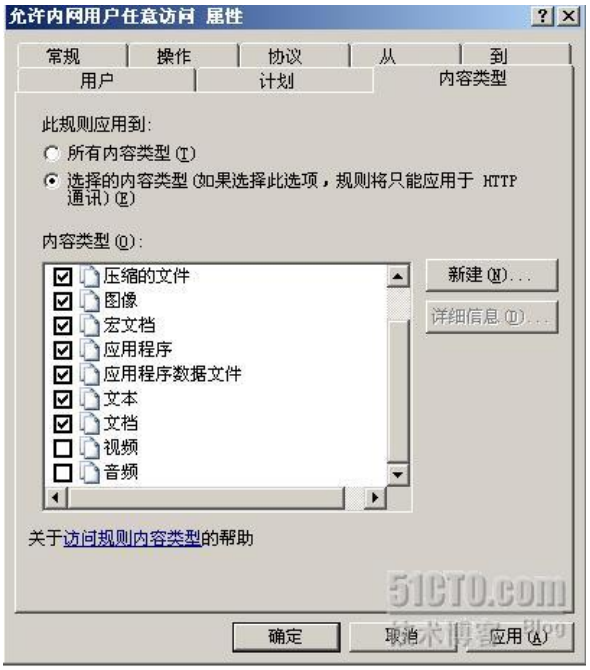
视频类型的文件扩展名如下图所示，我们发现了一个很大的问题，网络上很常用的 rm 和 rmvb 文件怎么没有被包含进去，微软搞什么搞？这么常用的视频文件居然都漏掉了？只好由我们来 DIY 了。



在可用类型中输入 rmvb，如下图所示，点击添加，即可将 rmvb 补充到视频类型中。用同样方法可将被疏漏的视频和音频文件都补充进去。



修改完内容类型后，我们在访问规则的内容类型处进行修改。如下图所示，我们选择使用自选的内容类型，在选定的内容类型中排除了音频和视频。



OK，我们离目标只有一步之遥了！

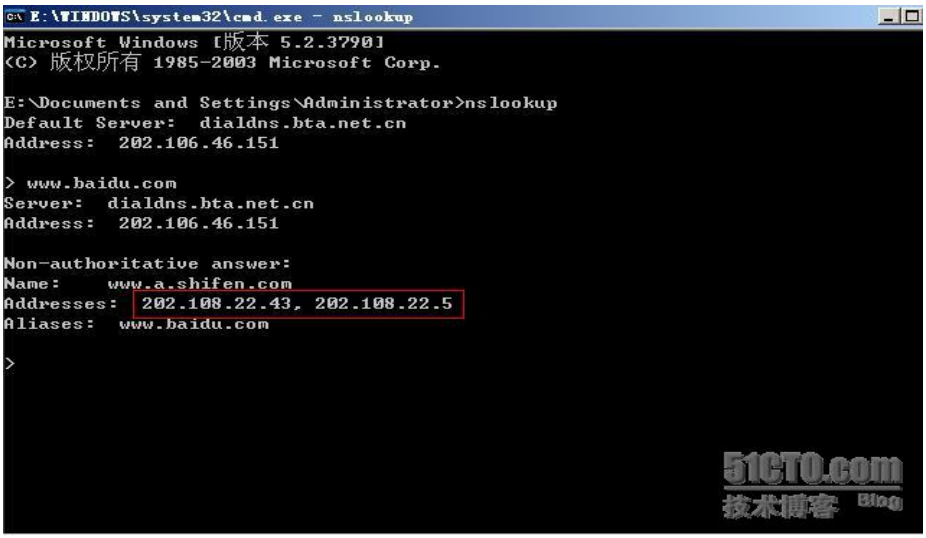
五 网络对象

网络对象中包括了很多策略元素，例如计算机，计算机集，域名集，URL 集等，我们在访问规则中定义源和目标时经常会用到网络对象。本例中我们限定用户不能访问百度，那就必须先通过网络对象对百度进行定义，然后才能在访问规则中加以利用。

要想禁止访问百度，我们需要定义域名集和计算机集两种元素，从域名和 IP 地址两种角度描述百度。我们先创建域名集，如下图所示，在防火墙策略工具箱中展开网络对象，选择新建域名集。

域名集的名称为百度，内容为 www.baidu..com，如果希望限制更多的百度内容，可以考虑使用通配符，例如*.baidu.com。

限制百度只用域名是不够的，我们还需使用 IP 地址（具体原因在下一篇介绍策略执行过程的博文中加以介绍）。我们首先要知道百度网站的 IP 是多少，不要用 ping www.baidu.com 的方法，这种方法不够全面。我们使用 nslookup，如下图所示，输入 www.baidu.com，我们得到了百度的两个 IP，202.108.22.43 和 202.108.22.5。



接下来创建计算机集，如下图所示，在工具箱中选择新建计算机集。

为新建的计算机集取名为百度，选择添加计算机。

添加一个计算机对象，名称为 webserver1，IP 为 202.108.22.43。用同样的方法再添加一个 webserver2，IP 为 202.108.22.5。

创建好的计算机集如下图所示。

创建完网络对象后，我们来修改访问规则。在规则的属性中切换至“到”标签，如下图所示，在“例外“处点击添加，将域名集百度和计算机集百度都添加进来，这样百度就不再被访问规则所允许了。

修改后的规则如下图所示，这就是我们想要的访问规则，只有人事部和财务部的员工在午休时间才可以访问除百度之外的网站，而且不允许访问音频及视频内容。

经过这个访问规则的实现，我们对策略元素已经有了一些基本的认识，应该能写出一些常用的访问规则了。但访问规则的具体执行过程是什么样的？我们写出的规则是否真正符合自己的设计要求呢？这些问题我们在下篇博文中加以介绍。

深入剖析防火墙策略的执行过程：ISA2006 系列之六

很多初次接触 ISA 的管理员，经常会发现自己的管理意图没有得到贯彻。自己明明禁止用户使用 QQ 聊天，可你看这个老兄正在和多个 MM 聊得热火朝天；早就禁止在上班时间访问游戏网站，可这个家伙不正在和别人下棋吗？最郁闷的是就连简单的禁止访问百度搜索引擎都做不到，照样有很多人用百度搜来搜去……不少深感智力受到侮辱的网管愤怒地发出了“ISA 就是不灵”的吼声。ISA 真是不灵吗？不是的，其实发生这些的主要原因是 ISA 管理员并没有真正理解防火墙策略的执行过程。今天我们就来好好地分析一下 ISA 防火墙策略的执行过程，避免在以后的工作中犯类似的错误。

首先声明，我们今天讨论的是 ISA2006 标准版的策略执行过程，企业版比标准版要复杂一些，以后我们再讨论。我们可以把 ISA 当作是信息高速公路上的一个检查站，当有数据包要通过 ISA 时，ISA 就会利用策略对数据包进行检查，检查通过就放行，否则就拒绝。ISA 检查数据包的顺序是：

一 检查是否符合网络规则

二 检查是否符合系统策略

三 检查是否符合防火墙策略

一 网络规则

一个数据包通过 ISA 时，ISA 首先要检查的就是网络规则。网络规则是 ISA 中非常重要而又很容易被忽视的一个因素。ISA 检查数据包时首先要考虑的就是这个数据包是从哪个网络到哪个网络，这两个网络间的网络规则是什么。也就是说 ISA 是基于网络进行控制，而不是很多朋友认为的基于主机进行控制。网络规则只有两种，路由或 NAT。如果 A 网络到 B 网络的网络规则为路由，那么数据包从 A 网络到 B 网络或者从 B 网络到 A 网络都有可能；如果 A 网络到 B 网络的网络规则为 NAT，那么数据包只有可能从 A 到 B，而不可能从 B 到 A。我们可以把两个网络比喻为两个城市，网络规则就象是城市之间的高速公路，如果两个网络之间的网络规则为路由，那就象是两个城市之间有一条双向高速公路；如果网络规则为 NAT，则就相当于两个城市之间有一条单行高速公路。

明白了网络规则的作用，有些问题就很好解释了。有些 ISA 管理员问过这样一个问题：“我在 ISA 的防火墙策略中已经允许外网访问内网，为什么外网机器还是访问不进来？”现在来看这个问题就很简单了，因为 ISA 认为内网和外网之间的网络规则是 NAT，如下图所示，NAT 规则决定了只有可能从内网到外网而不可能从外网到内网，因此当外网访问内网时，ISA 只需检查网络规则就。因此如果你确实需要外网访问内网，你就应该先把内网和外网之间的网络规则改为路由。

还有一个网络规则的例子，有一个管理员用 ISA 把 DMZ 区的一个 FTP 服务器发布到了外网和内网，结果外网用户访问正常，内网用户却无法访问。为什么，因为 DMZ 和外网是 NAT 关系，而 DMZ 和内网是路由关系。由于从 DMZ 到外网是 NAT 关系，外网用户无

法通过访问规则直接访问，所以通过发布规则访问是合理的；而内网和 DMZ 是路由关系，因此内网用户就应该通过访问规则而不是路由规则来访问。

综上所述，网络规则是 ISA 进行访问控制时所要考虑的第一要务，只有从源网络到目标网络被网络规则许可了，ISA 才会继续检查系统策略和防火墙策略；如果访问规则不许可，ISA 会直接拒绝访问，根本不会再向下检查系统策略和防火墙策略。大家写访问规则时一定要注意这点。

二 系统策略

如果一个数据包通过了网络规则的检查，ISA 接下来就要看看它是否符合系统策略了。ISA2006 标准版中预设了 30 条系统策略，系统策略应用于 ISA 本地主机，控制着从其他网络到本地主机或者从本地主机到其他网络的通讯，系统策略中启用了一些诸如远程管理，日志，网络诊断等功能。一般情况下，我们对系统策略只能允许或禁止，或对少数策略的某些属性作一些修改。

以前曾经有朋友问我，为什么 ISA 安装后防火墙策略中明明禁止了所有通讯，但 ISA 主机还是可以 ping 到其他计算机，是否 ISA 本机有某些特权呢？不是的，ISA 能对其他网络进行有限访问完全是由系统策略决定的，只是由于系统策略没有显示出来，因此安装完 ISA 后我们并没有注意到它。

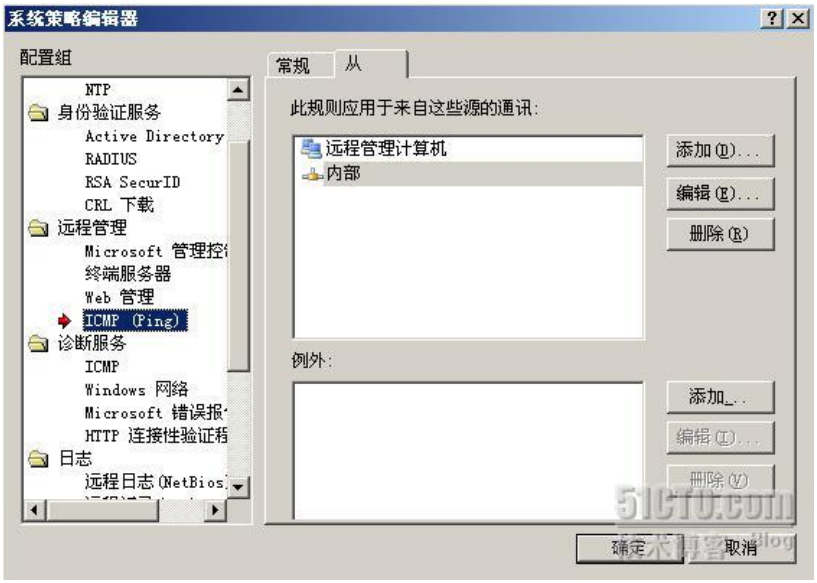
我们来看看系统策略到底有哪些内容，打开 ISA 服务器管理，右键点击防火墙策略，如下图所示，在查看中选择“显示系统策略规则”。

如下图所示，我们看到了 30 条系统策略的内容。

编辑系统策略也可以用系统策略编辑器，系统策略编辑器为管理员提供了更为友好的管理界面，如下图所示，右键点击“防火墙策略”，选择“编辑系统策略”。

如下图所示，我们可以在系统策略编辑器中编辑系统策略。

系统策略的优先级比防火墙策略高，因此如果任务可以用系统策略完成，就不要用防火墙策略。例如有时候我们为了测试需要，允许从内网 ping ISA 服务器，这种需求完全可以用系统策略完成，如下图所示，我们只要把内部网络添加到允许 ping 本地主机的集合中，就可以完成任务了。



三 防火墙策略

防火墙策略用来控制源网络和目标网络的通讯，是 ISA 管理员控制网络访问的常规武器，也是本文讨论的重点所在。防火墙策略的优先级就是按照规则排列的顺序，而不是按照拒绝优先原则。由于系统策略优先级也是按照序号排列，和防火墙策略优先级完全一样，我们甚至可以把防火墙策略看成是从 31 开始编号的系统策略。

数据包通过网络规则的检查后，就要面临系统策略和防火墙策略的考验了。ISA 将从第一条策略开始检查，检查数据包的访问请求是否匹配策略，如果匹配，就按照策略的规定执行，结果无非是禁止或允许。如果不匹配，ISA 就将按顺序检查下一条策略，从第一条系统策略一直检查到最后一条防火墙策略。那有人要问了，如果把所有策略都检查完了还不匹配怎么办？呵呵，这是不可能的，ISA 自带的最后一条防火墙策略内容是禁止所有网络间的一切通讯，如下图所示，这条防火墙策略可以与所有的网络访问相匹配，因此 ISA 实际上使用了隐式拒绝，也就是说如果某个访问请求如果没有被策略显式允许，那肯定会被最后一条防火墙策略所拒绝。

看了上面的介绍，我们要注意两点，一是策略顺序，二是策略匹配。

A 策略顺序

防火墙策略的排列顺序决定了优先级，排在前面的策略优先执行，根据这个原则，我们要好好设计一下防火墙策略的顺序。例如，我们写了两条防火墙策略，一条是允许内网用户任意访问，另外一条是拒绝内网用户访问联众游戏网站。如果排列顺序如下图所示，允许策略排在拒绝策略之前，那就是个错误的决定。拒绝访问联众的策略永远不会被执行，因为当用户访问联众时，访问请求匹配第一条防火墙策略，用户就被防火墙放行了，第二条策略根本没有执行的机会。正确的做法是将拒绝策略放到允许策略之前！

B 策略匹配

策略匹配是 ISA 管理员关注的核心问题。前面我们一直在提如果网络访问和防火墙策略匹配，则按防火墙策略执行允许或禁止的操作。那么，问题是，怎么才算和防火墙策略匹配呢？

只有把这个问题搞清楚了，才能写出符合你设计初衷的策略。

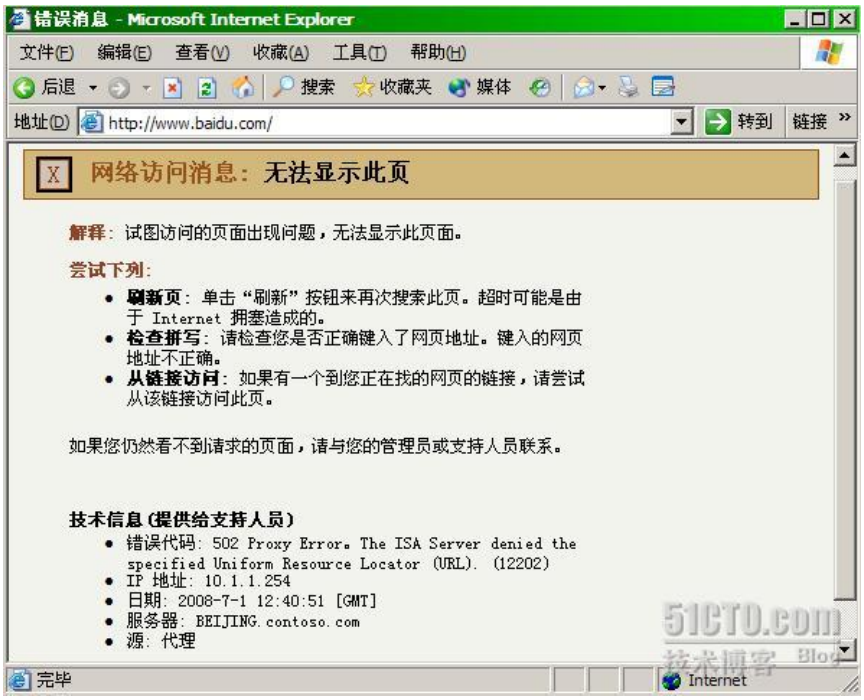
当 ISA 检测到访问请求时，ISA 会检查访问请求能否匹配防火墙策略中的策略元素，策略元素的检查顺序为 协议，从（源网络），计划时间，到（目标网络），用户，内容类型。如果和这些元素都能匹配，ISA 就认为访问请求匹配防火墙策略。

从被检查的策略元素来看， 到（目标网络）元素最容易出问题。

目标网络元素的问题容易出在哪儿呢？容易出现在 DNS 上，确切地说是出现在 DNS 的反向解析上！这个结论估计是很多管理员始料未及的，还是举个例子加以说明吧，假设我们要禁止内网访问百度，我见过很多管理员的处理方法都是这样的，首先创建一个域名集，将 www.baidu.com 包含进去，如下图所示。

然后就写出一条拒绝内网访问百度的访问规则，如下图所示

我们在一台内网计算机 Denver 上测试一下，Denver 使用 Web 代理访问百度，如下图所示，错误信息表明 ISA 拒绝了 Denver 访问百度的请求。这说明访问请求和拒绝百度访问的防火墙策略匹配成功，哈哈，看样子大功告成了？且慢，再向下看。



我们在 Denver 上换用 IP 访问，在 IE 中输入 202.108.22.5，如下图所示，熟悉的百度界面已经出来了，哈哈，貌似严谨的访问规则竟如此不堪一击！这说明这次的访问请求没有和拒绝百度访问的防火墙策略匹配成功，而是和第二条允许内网用户任意访问的防火墙策略匹配成功了。

看到这儿，有些朋友可能得出结论了，哦，原来用域名禁止访问某个网站是不成立的。错！如果 202.108.22.5 的反向解析结果为 www.baidu.com，那么拒绝百度的防火墙策略就是成立的！

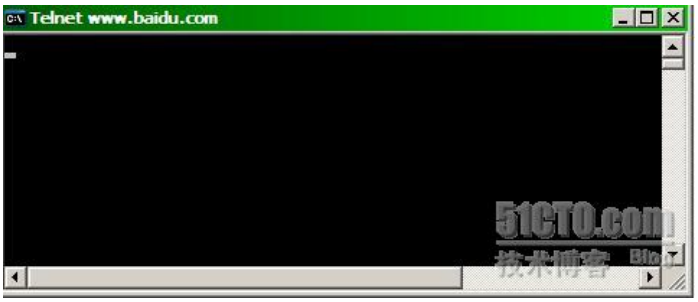
还是来认真分析一下原理吧，当客户机用 HTTP 协议访问目标网络时，ISA 判断目标网络的根据是 HTTP 主机头，主机头的内容显然源自我们在浏览器中的输入。当我们在浏览器中输入 www.baidu.com 时，ISA 开始检查访问请求能否匹配第一条防火墙策略，也就是拒绝内网访问百度的那条策略。ISA 先检查协议，从（源网络），计划时间三个元素，这三个元素都能和访问请求匹配，然后 ISA 检查到（目标网络）元素，ISA 根据主机头内容判断访问请求中的目标网络是 www.baidu.com，而防火墙策略中的目标网络元素也包含了 www.baidu.com，因此 ISA 判断访问请求和到（目标网络）元素也能匹配上。然后 ISA 检查用户和内容类型两个元素也可以匹配，所以 ISA 判断访问请求和拒绝访问百度的防火墙策略完全匹配，于是按照防火墙策略的要求拒绝了这次访问请求。

当我们在浏览器中输入 202.108.22.5 时，ISA 是这么检查的。首先还是判断 协议，从（源网络），计划时间三个元素匹配策略，然后检查到（目标网络）元素，ISA 判断访问请求的目标是 202.108.22.5，而防火墙策略的目标网络是包含 www.baidu.com 的域名集，这时 ISA 会对 202.108.22.5 进行 DNS 反向解析，如果解析的结果等于 www.baidu.com。，ISA 就认为访问请求的目标网络和策略的目标网络也是匹配的。如果反向解析的结果不等于 www.baidu.com（解析的结果确实不是百度的域名），ISA 就认为访问请求的目标网络和防火墙策略的目标网络不匹配。这样 ISA 就会停止匹配第一条拒绝访问百度的防火墙策略，转而匹配第二条允许内网任意访问的防火墙策略，匹配结果是完全成功，因此 ISA 执行第二条防火墙策略规定的动作，允许了对 202.108.22.5 的访问。

如果客户机不是用 HTTP 协议访问目标网络，那么匹配的过程又稍微有些不同。例如客户机用 FTP 协议访问 www.baidu.com，那么客户机在发送访问请求时不会把 www.baidu.com 作为目标网络，而是先对 www.baidu.com 进行域名解析，然后把解析出来的 IP 作为目标网络发送给 ISA。ISA 对访问请求进行匹配时，如果被匹配的防火墙策略用域名描述目标

网络，ISA 就会对访问请求发来的 IP 进行反向解析，看解析出的域名能否和防火墙策略的目标网络相匹配。根据这个结论，我们用 IE 访问 www.baidu.com 会被拒绝，因为刚才分析过了，此时客户机将域名 www.baidu.com 作为访问请求中的目标网络发送给 ISA，ISA 认为访问请求和拒绝访问百度的防火墙策略完全匹配，因此客户机被拒绝访问。但如果客户机在命令行下输入 telnet www.baidu.com 80，如下图所示，直接连接百度的 80 端口，ISA 会如何处理呢？

如下图所示，ISA 对访问请求放行了，显然这次的访问请求没有和拒绝访问百度的策略匹配上，原因是什么呢？



客户机 telnet 百度 80 端口时，我在 ISA 上启用了实时日志，日志记录的结果如下图所示。从日志上我们很清楚地看到，客户机先对 www.baidu.com 进行了 DNS 解析，解析结果为 202.108.22.5，然后客户机把 202.108.22.5 作为访问请求的目标网络发送给 ISA，ISA 对 202.108.22.5 进行反向解析，解析出的域名并不是 www.baidu.com，因此 ISA 认为访问请求和第一条防火墙策略并不匹配。然后 ISA 将访问请求和第二条策略进行匹配，匹配成功后正从我们在日志中看到的那样，访问请求被第二条允许内网用户任意访问的策略放行了。

日志时间	目标 IP	目标端口	协议	操作	规则	客户端 IP
2008-7-1 22:28:21	218.30.26.68	53	DNS	已关闭的连接	允许内网用户...	10.1.1.5
2008-7-1 22:28:21	218.30.26.70	53	DNS	已关闭的连接	允许内网用户...	10.1.1.5
2008-7-1 22:28:21	220.181.38.10	53	DNS	已关闭的连接	允许内网用户...	10.1.1.5
2008-7-1 22:28:21	220.181.3.178	53	DNS	已关闭的连接	允许内网用户...	10.1.1.5
2008-7-1 22:28:23	61.135.165.235	53	DNS	已关闭的连接	允许内网用户...	10.1.1.5
2008-7-1 22:28:23	192.33.14.30	53	DNS	已关闭的连接	允许内网用户...	10.1.1.5
2008-7-1 22:28:25	202.108.22.5	80	HTTP	已启动的连接	允许内网用户...	10.1.1.5
2008-7-1 22:29:23	10.1.1.254	137	NetBIO...	已关闭的连接	允许内网用户	10.1.1.5

我们可以总结一下，客户机使用 HTTP 协议访问时，目标网络取决于主机头，而访问者输入的主机头既可能是域名也有可能是 IP（一般以域名居多）；。客户机使用其他协议访问时，目标网络一定是以 IP 进行描述！

现在我们考虑一下应该如果用 ISA 禁止用户访问某个目标网络，那这个目标网络应该如何描述，显然只用域名描述是不严谨的，除非你确信 DNS 反向解析的结果对你有利（大部分情况下你会失望的）。如果保险一些，我们应该用域名＋IP 来描述目标网络。以刚才的限制百度为例，用 nslookkup 查出 www.baidu.com 的域名解析结果为 202.108.22.43 和 202.108.22.5。创建一个计算机集将这两个地址包含进去，如下图所示。

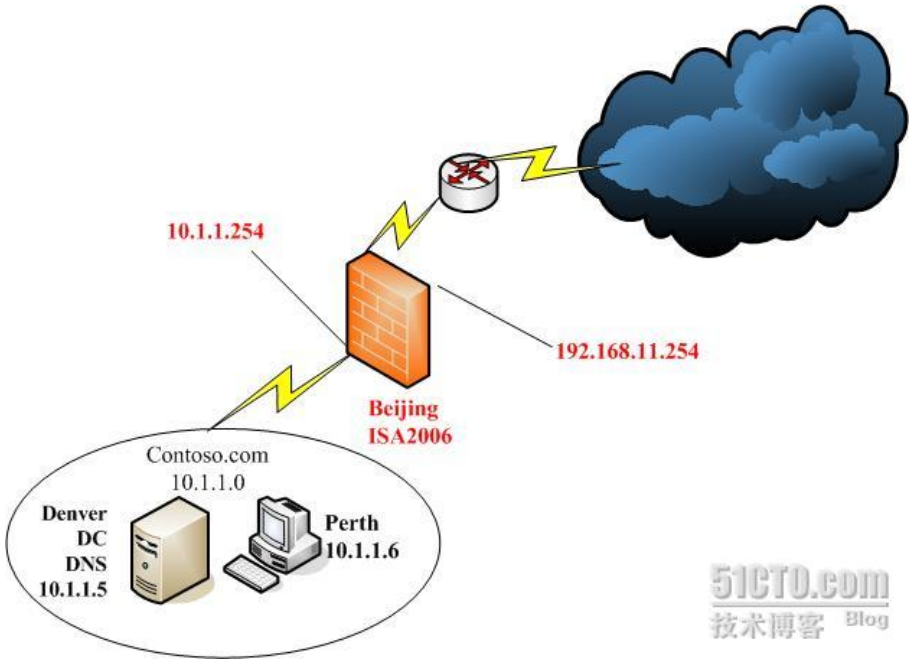
然后就可以在拒绝访问百度的策略中加入刚创建的计算机集，如下图所示，这样做效果如何大家可以自己试试看，肯定比只用域名要好得多。

用防火墙客户端限制使用 SKYPE：ISA2006 系列之七

很多 ISA 管理员都需要对客户机使用的网络应用程序进行限制，有的公司希望限制用户使用 QQ 聊天，有的企业不希望用户使用 BT 下载，还有的单位禁止员工打网络游戏。这些限制如何实现呢？今天我们介绍一种简单易用的方法：利用防火墙客户端限制客户机程序的运行。

防火墙客户端可以根据文件名限制客户机执行的应用程序，虽然根据文件名进行限制不是很保险，但对付一般用户还是有作用的。至于高手嘛，呵呵，反正俺是绕着走.....

实验拓扑如下图所示，Denver 是 contoso.com 的域控制器，Perth 是域内工作站，Beijing 是域内的 ISA2006 服务器，此次的实验目的是限制使用即时通讯软件 SKYPE。



51CTO.com
技术博客 Blog

我们的实验思路是：

1　迫使客户机使用防火墙客户端

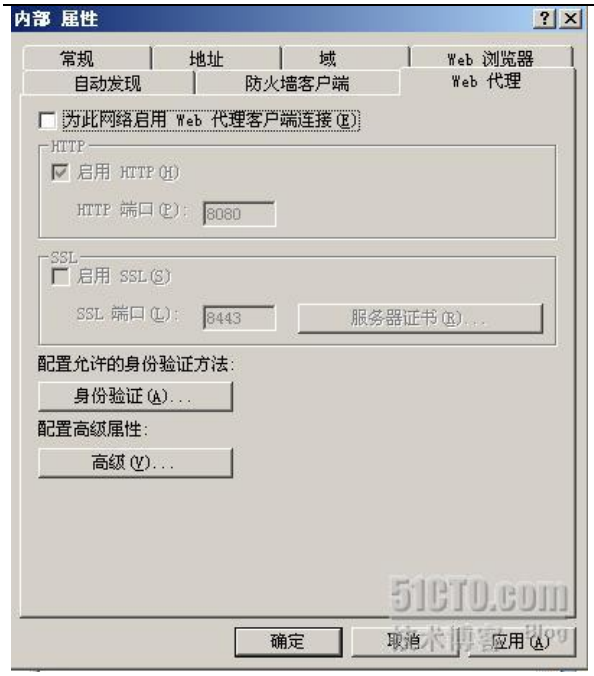
2　利用防火墙客户端禁止特定程序

一 迫使客户机使用防火墙客户端

由于只有防火墙客户端具有限制程序的功能，因此我们必须让客户机使用防火墙客户端。但 ISA 的代理方式有三种，Web 代理，防火墙客户端和 SNAT，怎么才能让用户放弃其他两种选择呢？

首先我们先要禁止用户使用 Web 代理，想做到这一点很容易，只要在 ISA 上关闭 Web 代理就可以了。在 ISA 服务器上依次点击 开始－程序－Microsoft ISA Server－ISA 服务器管理，

展开 配置－网络－内部，在内部网络的属性中切换到“Web 代理”，如下图所示，取消“为此网络启用 Web 代理客户端连接”，这样 ISA 就不再对内网提供 Web 代理服务了。



要禁止客户机使用 SNAT 就要动动脑筋了，我们可以利用 SNAT 不支持用户身份验证的弱点，在访问规则中要求用户必须通过身份验证，这样就可以强迫用户放弃 SNAT。如下图所示，现在的访问规则中允许所有用户任意访问，所有用户包括了未经身份验证的用户，因此我们要对规则进行修改。

编辑规则属性，切换到用户标签，如下图所示，删除“所有用户”，然后点击“添加”按钮，将用户集“所有通过身份验证的用户”添加进来。

由于修改后的访问规则要求用户提供身份验证，但 SNAT 客户端无法提供，这样客户机就被逼上了只能使用防火墙客户端的华山绝路。

二 利用防火墙客户端禁止特定程序

现在客户机只能使用防火墙客户端上网了，我们可以来试试用防火墙客户端限制程序了。我们此次的实验目的是限制使用 SKYPE，SKYPE 是一款功能非常强大的通讯软件，它的分布式计算特点使它获得了非常完美的通话音质，而它凶悍的穿透能力让很多防火墙管理员一筹莫展。今天我们要试试用简单的方法来限制 SKYPE，在没限制之前，客户机的 SKYPE 可以正常使用，如下图所示。

打开 ISA 服务器管理，展开 配置－常规，点击“定义防火墙客户端设置”，如下图所示。

在防火墙客户端设置中切换到“应用程序设置”，如下图所示，点击“新建”。

Skype 的可执行文件名为 skype.exe。在新建的应用程序项目中，我们在应用程序中输入 skype，不用输入 skype.exe，键选择“Disable”，值选择“1”。从字面意义来看是禁止使用 skype。

添加了应用程序设置后，重启客户机，然后启动 skype 进行测试，如下图所示，skype 一直在尝试连接，但始终连接不上，实验成功。

但如果用户意识到问题所在，修改了文件名，那防火墙客户端就无能为力了。如下图所示，我们将 skype.exe 修改为 myskype.exe。

修改用户名后，再次启动 skype，如下图所示，skype 很轻松地突破了防火墙客户端的限制。

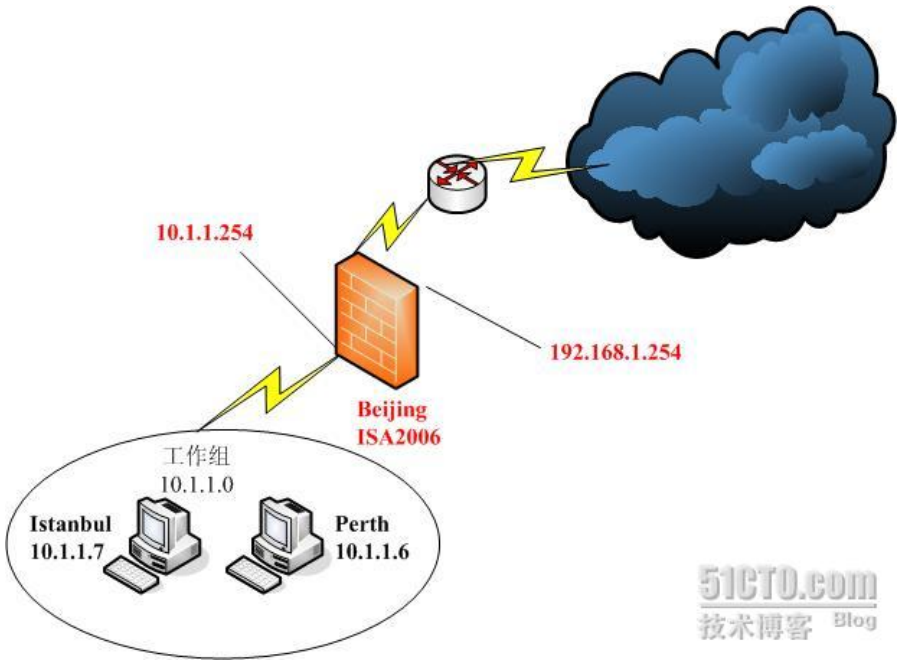
综上所述，防火墙客户端在限制程序方面能起到一定的作用，可以参考使用，但最好辅助其他技术手段，例如用组策略禁用软件等，这样效果才能更好。

ISA 限制用户上网的技巧：ISA2006 系列之八

很多单位在使用 ISA2006 时，都希望用 ISA 对员工上网进行约束，今天我们就为大家介绍一些限制用户上网的技巧。由于在域和工作组环境下使用的方法有所不同，因此我们将内容分为两部分，一部分介绍在工作组环境下如何操作，另一部分则针对域环境。

我们从工作组开始介绍，在工作组环境下，控制用户上网大多采用两种手段，IP 地址或用户身份验证，多数管理员会倾向于利用 IP 控制。

工作组环境的实验拓扑如下图所示，Beijing 是 ISA2006 服务器，Perth 和 Istanbul 是工作组内的两台计算机。



一　利用 IP+Arp 静态绑定

工作组环境下进行身份验证并不方便，因此管理员一般会采用 IP 地址进行访问控制。根据源 IP 限制访问者是包过滤防火墙的基本功能，从技术上看实现起来很简单。如果我们希望只有 Perth 能上网，那我们就可以创建一个允许上网的计算机集合，然后将 Perth 加入此集合即可。

在 ISA 服务器上打开 ISA 服务器管理，在防火墙策略工具箱中选择新建“计算机集”，如下图所示。

为计算机集取名为“允许上网的计算机”，点击添加计算机，准备把 Perth 加进来。

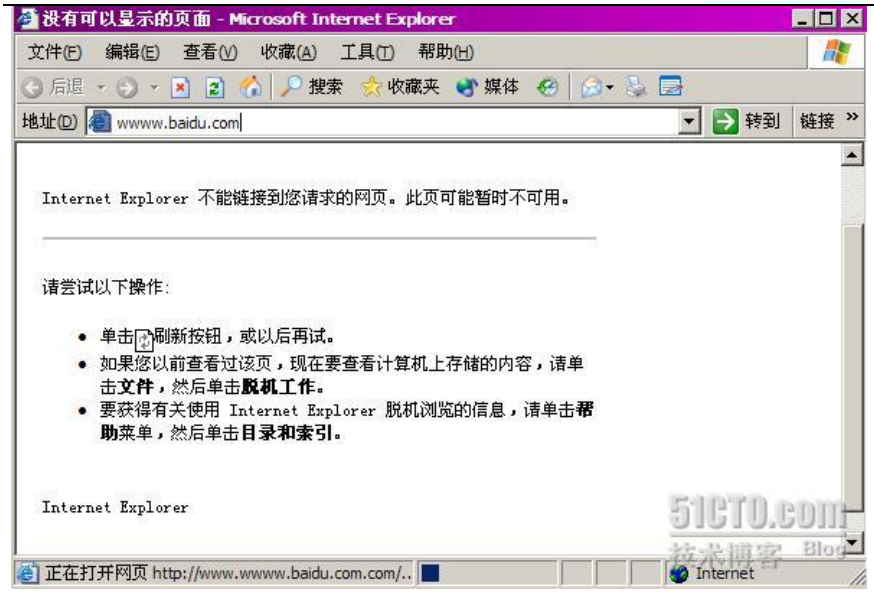
输入 Perth 的名称和 IP 地址，点击“确定“，这样我们就创建了一个计算机集合，集合内包括 Perth。

创建了计算机集合后，我们来修改一下访问规则，现有的访问规则是允许内网和本地主机可任意访问。在访问规则属性中切换到“从”标签，如下图所示，选择“内部”，点击“删除”，然后把刚创建的计算机集合添加进来。

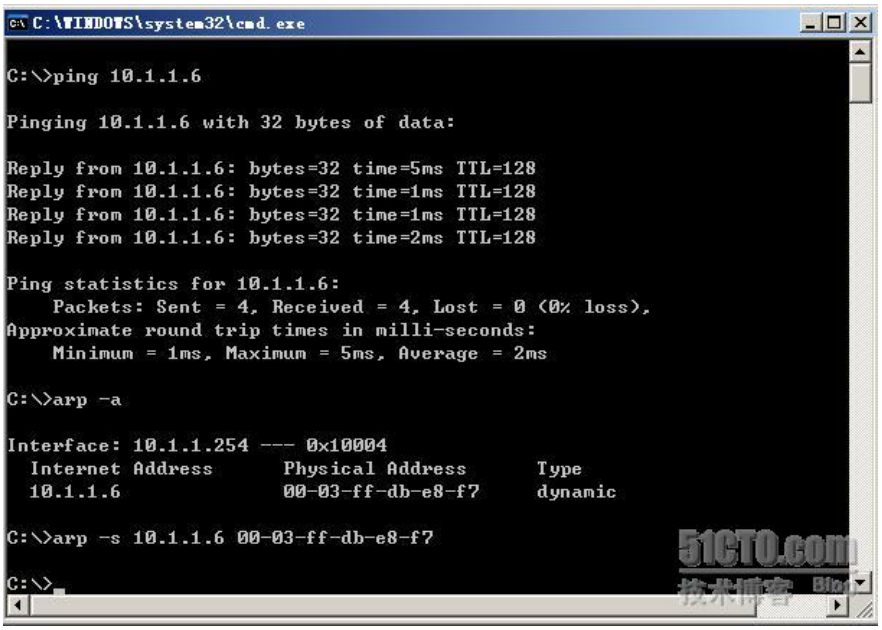
修改后的规则如下图所示。

在 Perth 上访问百度，一切正常，如下图所示。

换到 Istanbul 上访问，如下图所示，Istanbul 无法访问 Internet。



看起来我们达到了用 IP 控制用户上网的目的，问题已经解决，其实不然。由于目前 ISA 只是依靠 IP 地址进行访问控制，过不了多久，ISA 管理员就会发现有“聪明”人开始盗用 IP，冒充合法用户访问外网。为了应对这种情况，我们可以考虑使用 ARP 静态绑定来解决这个问题，即在 ISA 服务器上记录合法客户机的 MAC 地址。在本例中，我们让 ISA 记录 Perth 的 MAC 地址。如下图所示，ISA 先 ping Perth，然后用 Arp –a 查出 Perth 的 MAC 地址，最后用 Arp –s 进行静态绑定，这样就不用担心用户盗用 IP 了。

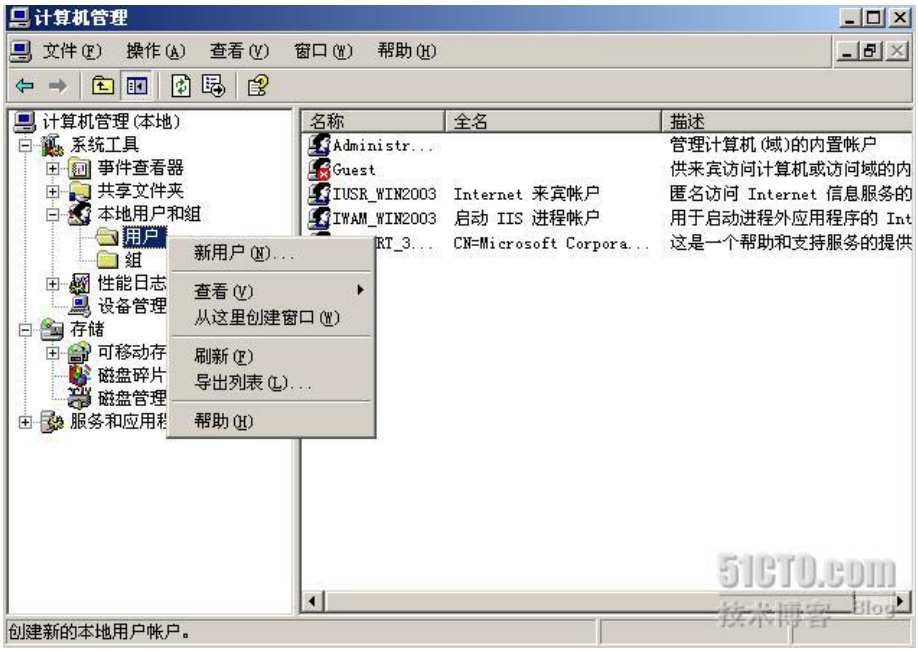


二 用户身份验证

工作组环境下进行用户身份验证并不方便，但不等于无法进行用户身份验证，在工作组中进行身份验证可以使用镜像账号的方式，即在 ISA 服务器和客户机上创建用户名和口令都完全一致的用户账号。例如我们允许员工张强访问外网，张强使用的计算机是 Istanbul，那我们可以进行如下操作。

A 在 ISA 服务器上为张强创建用户账号

在 ISA 的计算机管理中，定位本地用户和组，如下图所示，选择创建新用户。

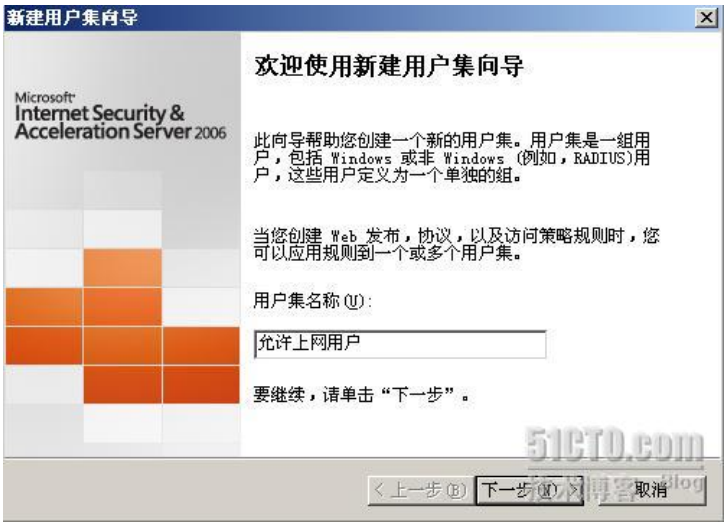


用户名为 zhangqiang，口令为 Itet2008。

B 在 ISA 服务器上创建允许上网的用户集

在防火墙策略工具箱中，展开用户，如下图所示，点击新建。

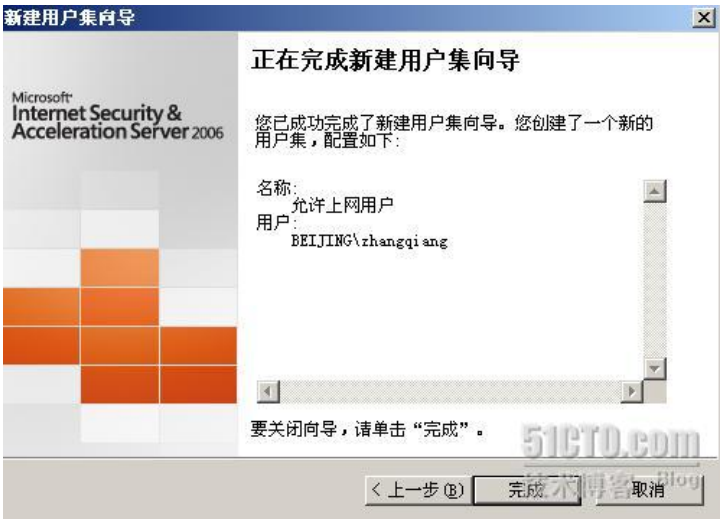
为新建用户集取名为“允许上网用户”。



在新创建的用户集中添加“Windows 用户和组”，如下图所示。

在用户集中添加 beijingzhangqiang，如下图所示。

创建完用户集，点击完成。



接下来我们要修改访问规则，只允许指定用户集访问外网。还是对那条允许内网用户任意访问的访问规则进行修改，这次不修改访问的源网络了，如下图所示，我们对源网络不进行任何限制。

这次限制的重点放在了用户上，在规则属性中切换到用户标签，将“所有用户”删除。

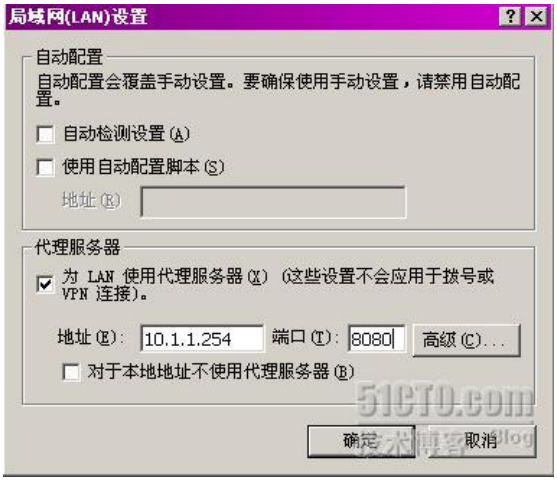
将“允许上网用户”添加进来，如下图所示。

D 在 Istanbul 上创建张强的镜像账号

现在内网的访问用户必须向 ISA 证明自己是 ISA 服务器上的用户张强才能被允许访问外网，那怎么才能证明呢？其实很简单，只要客户机上的某个用户账号，其用户名和口令和 ISA 服务器上张强的用户名和口令完全一致，ISA 就会认为这两个账号是同一用户。这里面涉及到集成验证中的 NTLM 原理，以后我会写篇博文发出来，现在大家只要知道如何操作就可以了。

在 Istanbul 上创建用户账号张强，如下图所示，用户名为 zhangqiang，口令为 Itet2008。

做完上述工作后，我们就可以在 Istanbul 来试验一下了。首先，我们需要以张强的身份登录，其次，由于 SNAT 不支持用户验证，因此我们测试时需使用 Web 代理或防火墙客户端。如下图所示，我们在客户机上使用 Web 代理。



在 Istanbul 上访问百度，如下图所示，访问成功！

在 ISA 上打开实时日志，如下图所示，ISA 认为是本机的张强用户在访问，镜像账号起作用了！

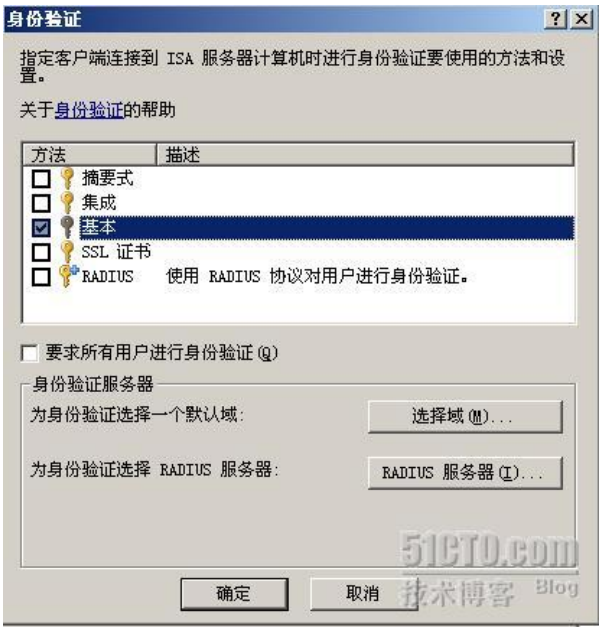
IP	目标端口	协议	操作	规则	客户端 IP	客户端用户名	源网络
255	138	NetBios 数据报	被拒...		10.1.1.7		内部
254	8080	http	被拒...	允许内网用户...	10.1.1.7	anonymous	内部
254	8080	http	失败...	允许内网用户...	10.1.1.7	anonymous	内部
.22.5	80	http	允许...	允许内网用户...	10.1.1.7	BEIJING\zhang...	内部
.22.5	80	http	允许...	允许内网用户...	10.1.1.7	BEIJING\zhang...	内部
22.61	80	http	允许...	允许内网用户...	10.1.1.7	BEIJING\zhang...	内部
254	8080	HTTP 代理	已启...		10.1.1.7		内部

三 Web 代理与基本身份验证

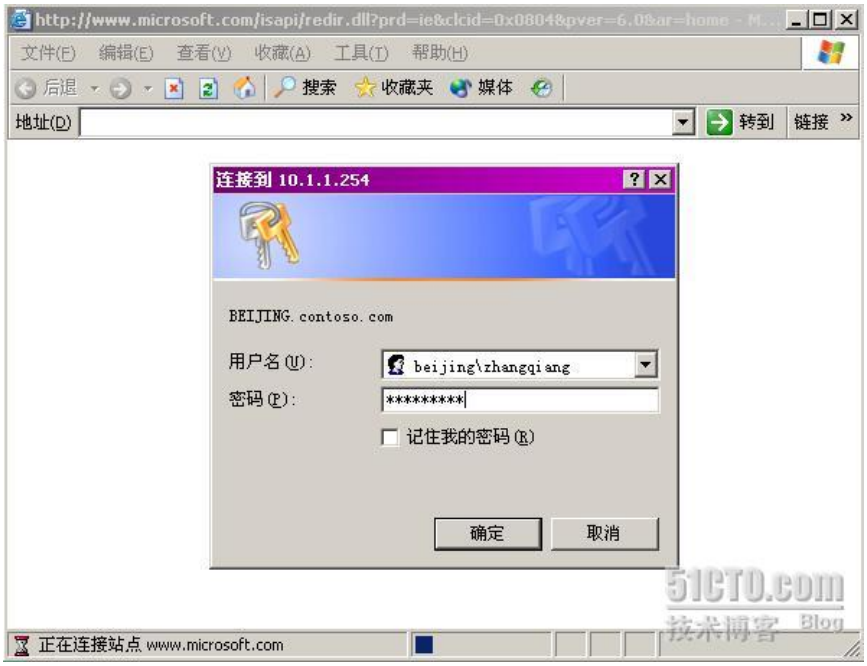
在上面的镜像账号例子中，访问者利用了集成验证证明了自己的身份，其实 ISA 也支持基本身份验证。曾经有朋友问过这个问题，ISA 能否在用户使用浏览器上网时弹出一个窗口，访问者必须答对用户名和口令才可以上网？这个需求是可以满足的，只要访问者使用 Web 代理以及我们将 Web 代理的身份验证方法改为基本身份验证即可。

在 ISA 服务器中查看内部网络属性，如下图所示，切换到 Web 代理标签，点击“身份验证”。

将 Web 代理使用的身份验证方式从“集成”改为“基本”，如下图所示。



防火墙策略生效后，在客户机上测试一下，如下图所示，客户机访问互联网时，ISA 弹出对话框要求输入用户名和口令进行身份验证，我们输入了张强的用户名和口令。

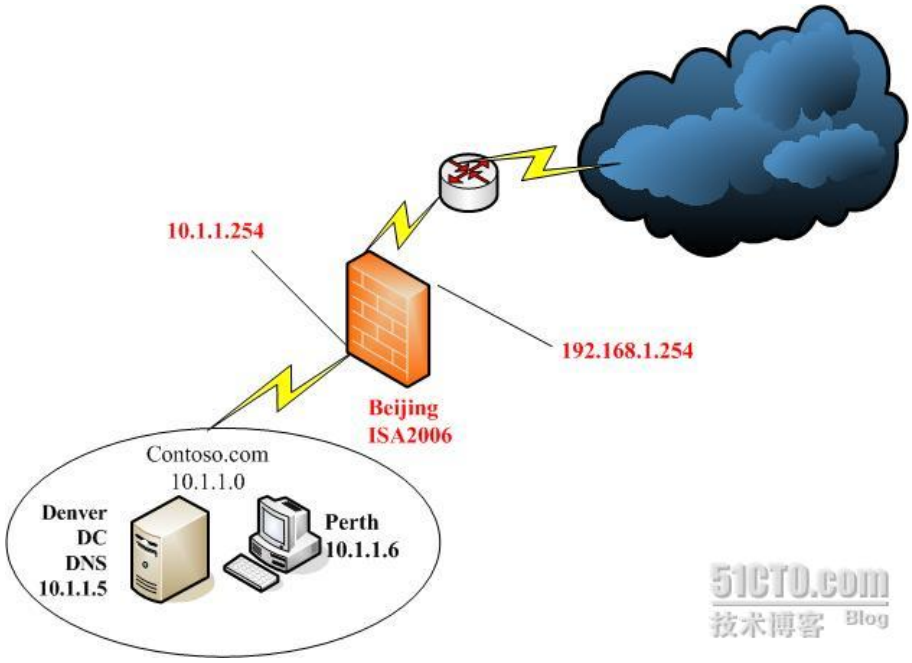


身份验证通过，用户可以访问互联网了！

以上我们简单介绍了如何在工作组环境下控制用户上网，接下来我们要考虑在域环境下如何操作。相比较工作组而言，域环境下控制用户上网是很容易做到的，既然有域控制器负责集中的用户身份验证，既方便又安全，如果不加以利用岂不太过可惜。在域环境下控制用户上网基本都是依靠用户身份验证，除了有极个别的 SNAT 用户我们需要用 IP 控制。具体

的处理思路也很简单，在域中创建一个全局组，例如取名为 Internet Access。然后将允许上网的域用户加入此全局组，最后在 ISA 中创建一个允许访问互联网的用户集，把全局组 Internet Access 加入允许访问互联网的用户集即可。

域环境拓扑如下图所示，Denver 是域控制器和 DNS 服务器，Perth 是域内工作站，Beijing 是加入域的 ISA2006 服务器。



一 DNS 设置问题

ISA 有两块网卡，两块网卡上究竟应该怎么设置 TCP/IP 参数，尤其是 DNS 应该怎么设置？这是个容易被忽略但又很重要的问题，因为 DNS 既负责定位内网的域控制器，也要负责解析互联网上的域名，设置不好轻则影响内网登录，重则严重影响大家上网的速度。我们推荐的设置方式是只在内网网卡设置 DNS，外网网卡不设置 DNS 服务器。

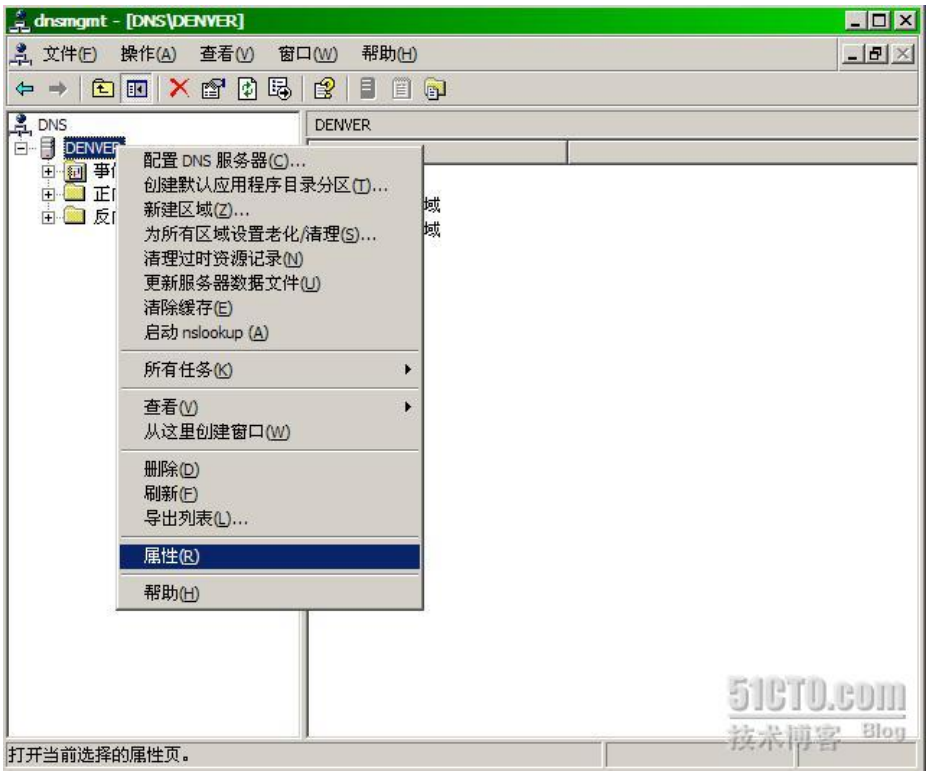
在本例中，ISA 服务器的内网网卡的 TCP/IP 参数是 IP 为 10.1.1.254 ，子网掩码为 255.255.255.0，DNS 为 10.1.1.5；外网网卡的 TCP/IP 参数是 IP 为 192.168.1.254，子网掩码为 255.255.255.0，网关为 192.168.1.1。这样一来，内网的 DNS 既负责为 AD 提供 SRV 记录，也负责解析互联网上的域名，结构简单，易于纠错。

有朋友认为只有电信提供的 DNS 服务器才能解析互联网上的域名，这种看法是不对的。我们在内网中搭建的 DNS 服务器只要能访问互联网，它就可以解析互联网上的所有域名。根据 DNS 原理分析，如果 DNS 服务器遇到一个域名自己无法解析，它就会把这个解析请求送到根服务器，根服务器采用迭代方式指导 DNS 服务器解析出目标域名。因此，想要内网的 DNS 服务器能解析出互联网上的域名，只要允许内网 DNS 服务器能访问互联网即可。

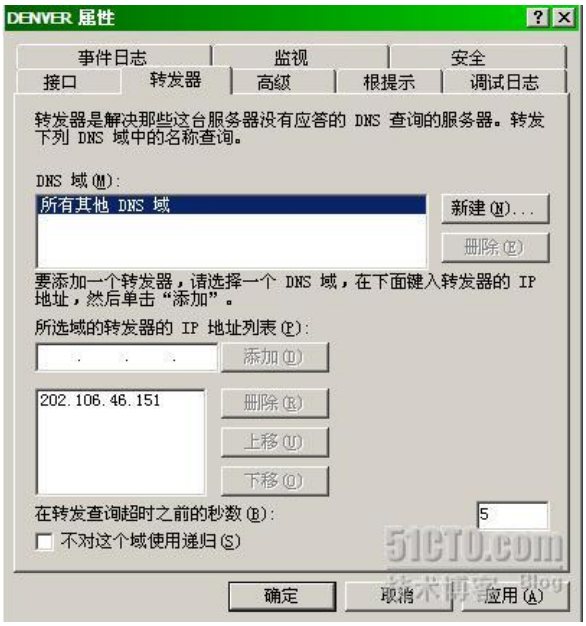
A 我们应该在 ISA 上创建一条访问规则，允许 DNS 服务器任意访问，并且将这条规则放到第一位，如下图所示。

B 为了提高 DNS 的解析速度，可以考虑在 DNS 服务器上设置转发器，将用户发来的 DNS 解析请求转发到电信的 DNS 服务器上。

转发器的设置如下，在 Denver 上打开 DNS 管理器，右键点击服务器，选择“属性”，如下图所示。



在属性中切换到“转发器”，在转发器 IP 地址处填写电信 DNS 服务器的 IP，填写完毕后点击添加，如下图所示。这样我们就设置好了转发器，以后 Denver 解析不了的域名将转发给 202.106.46.151，利用电信 DNS 的缓存来加快解析速度。

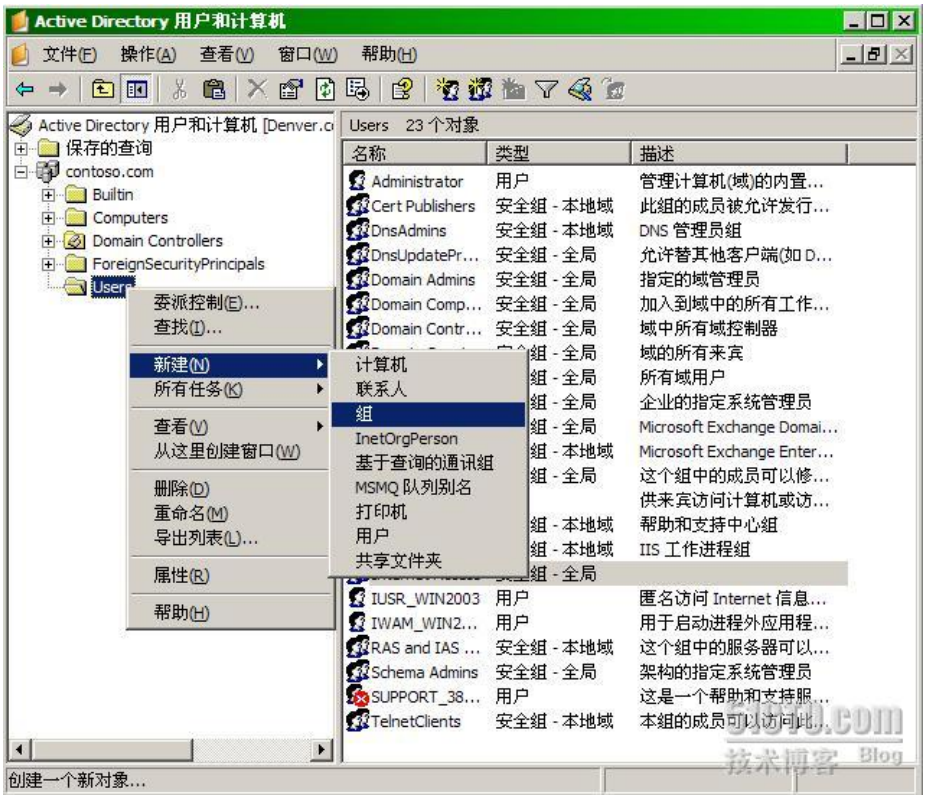


二 依靠身份验证限制用户

解决了 DNS 的问题后，我们就可以利用身份验证来限制用户访问了。

A 创建允许访问互联网的全局组

在域控制器上打开“Active Directory 用户和计算机”，如下图所示，在 Users 容器中选择新建组。



组的名称为 Internet Access，组的类型为全局组。

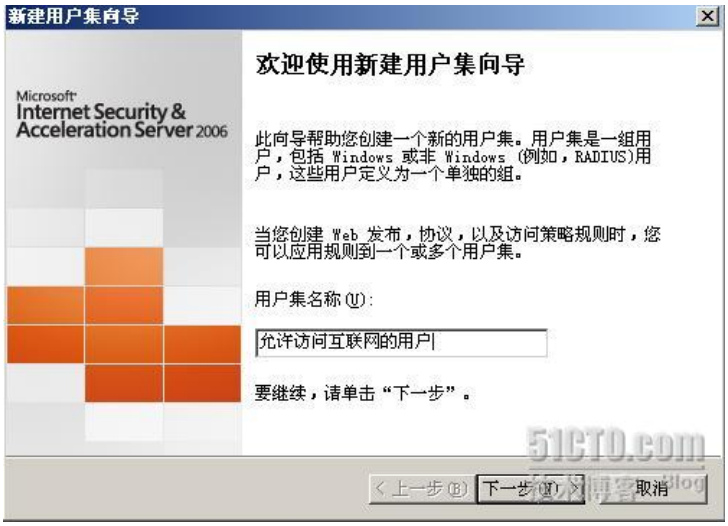
如下图所示，点击完成结束组的创建。

我们只需将允许访问互联网的用户加入 Internet Access 即可，如下图所示。

B 创建允许访问互联网的用户集

在 ISA 服务器防火墙策略的工具箱中展开用户，如下图所示，选择“新建”。

启动用户集创建向导，为用户集取个名字。



在用户集中选择添加“Windows 用户和组”，如下图所示。

我们将查找位置设为“整个目录”，对象名称输入“Internet Access”，如下图所示。

确定将 Contoso.com 域中的 Internet Access 组加入新创建的用户集。

完成用户集的创建。

C 修改访问规则

创建完用户集后，我们修改访问规则，ISA 原先有一条访问规则允许内网用户任意访问，我们对规则进行修改，限制只有特定用户集的成员才可以访问外网。

在访问规则属性中切换到“用户”标签，如下图所示，删除“所有用户”集合。

点击添加，将“允许访问互联网的用户”加进来，如下图所示。

这样就相当于 ISA 服务器将访问互联网的权限赋予了 Internet Access 组，凡是加入组的用户都将继承到这个权限，他们通过 ISA 访问互联网时将不会遇到任何障碍，也不会被提示输入口令进行身份验证，您看，在域环境下用户的透明验证是不是真的很方便呢？

总结：限制用户访问外网是 ISA 管理员经常遇到的管理需求，一般情况下不是用 IP 就是靠身份验证，身份验证在域中实现易如反掌，在工作组中实现就要靠镜像账号了。

举例详解 ISA 的 HTTP 过滤功能：ISA2006 系列之九

记得当初 ISA2004 发布时，微软大肆宣传 ISA2004 带来的各种新特性，其中很有分量的一个就是 HTTP 过滤。HTTP 过滤其实就是 ISA 能够“理解”HTTP 协议的一部分内容，可以根据协议内容对访问请求进行更准确的控制，ISA2004 被当作应用防火墙和这个功能有很大的关系。其实一个全功能的应用防火墙对所有的管理员都是一个不可抗拒的诱惑，试想，传统防火墙根据 IP 和端口限制访问，应用防火墙则可以根据内容限制访问，两者的准确程度根本不在一个档次上。打个比方就象我们要拦截恐怖分子寄来的包裹，传统防火墙是根据包裹的邮寄地址来进行判断，看，这个包裹是伊拉克寄来的，拉出去砍了……这样当然不够准确；应用防火墙则根据包裹内容进行判断，哇，这个包包中居然藏有很多爆炸物，快跑啊！…..

ISA2006 的 HTTP 过滤功能基本和 ISA2004 完全一样，对于大多数用户来说，最常使用的的服务器就是 Web 服务器，因此了解 ISA2006 中提供的 HTTP 过滤功能对更好地进行访问控制有很大的意义。

ISA Server 2006 究竟能够过滤 HTTP 数据包中的哪些内容，在此列举如下：

头长度的上限。

要求负载长度的上限。

URL 与查询长度的上限。

验证正则化与阻止高位字符

阻止可执行 Windows 命令的数据包通过。

阻止指定的 HTTP 连接方法（Method）。

阻止执行或下载指定的扩展名文件。

阻止指定的请求头或响应头的内容。

阻止包含的签名内容。

看完了上述 HTTP 数据包过滤策略的说明之后，接下来就让我们来看看它的设置方法。目前我的 ISA2006 中只有一条访问规则 Allow all，内容是允许内网和本地主机任意访问，我们如果想在这条访问规则上设置 HTTP 过滤，只要在规则属性中切换到“协议”标签，如下图所示，点击右下角的“筛选”，选择“配置 HTTP“，就可以进行 HTTP 过滤设置了。

一 常规设置

如下图所示，在 HTTP 策略的“常规“标签中，我们可以设置头长度的上限、负载长度的上限、URL 长度上限、查询长度、验证正则化与阻止高位字符以及阻止可执行 Windows 命令的数据包通过，具体解释如下：

头长度的上限：此参数设置为较小的值可有效防止一些会导致缓冲区溢出的黑客程序的攻击，不过在此不建议设置小于 10000 字节的大小，因为它可能也会导致一些合法的应用程序无法访问。

负载长度的上限：有效地设置此值，可防止企业内部所发布的网站遭受到通过 HTTP 中的 POST 方法传送大量的恶意数据包，而导致网站系统的负载过大。

URL 长度上限：设置超过此设限的网址长度将被阻止掉。

查询长度上限：在过去有一些蠕虫程序就是通过传送大量的 GET 要求给受害的目的地网站，藉此来瘫痪该网站的系统资源。

验证正则化与阻止高位字符：对于一些连接要求的数据包中，如果含有非正则化的字符与高位的内容可以在此加以阻止，不过必须注意的是如果网站是全中文化的，那么阻止高位的设置将会导致该网页无法正常显示，例如中文版 Exchange Server 2003 OWA 的发布就是如此。

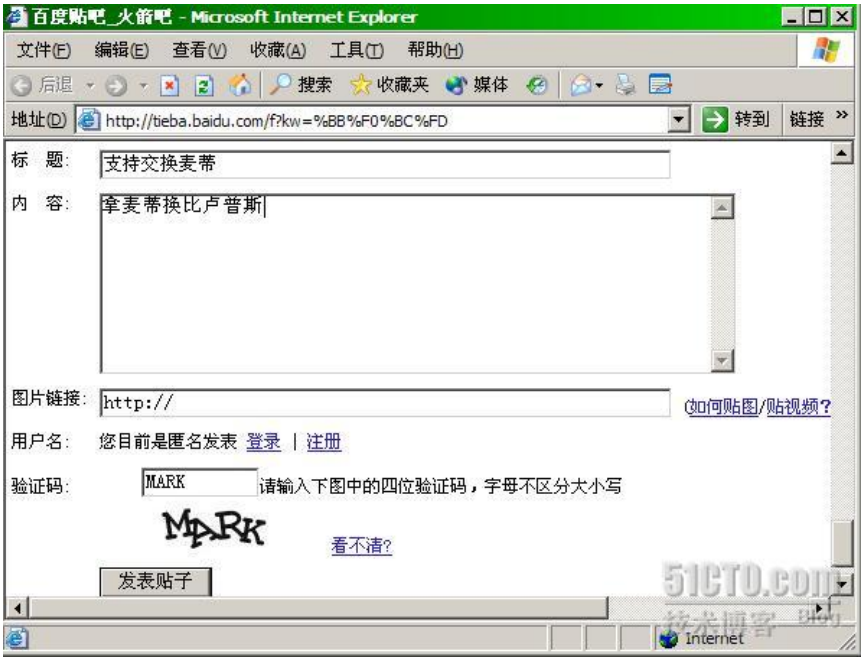
阻止包含 Windows 可执行文件内容的响应：还记得最早以前的红色警戒病毒吗？它就是凭借传送带有可执行 Windows 命令（CMD/C）的数据包给目的地的 IIS 网站，来藉此入侵该网站的操作系统。ISA 现在可以利用 HTTP 过滤有效阻止这种攻击。

二 方法

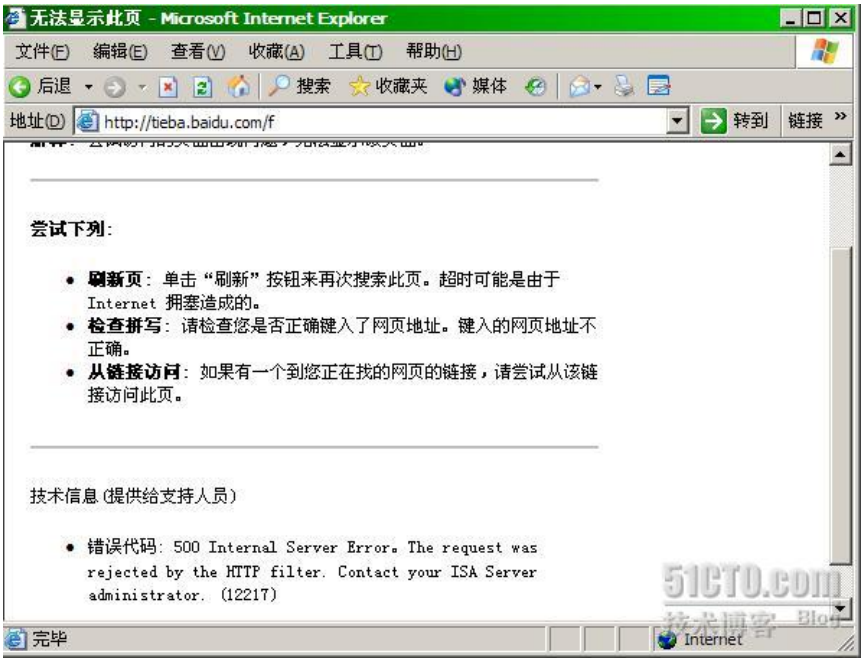
切换到 HTTP 策略的“方法“标签，如下图所示，我们可以阻止特定的 HTTP 方法。例如有些公司不希望员工在上班时间去论坛发贴子，我们就可以通过阻止 POST 方法来完成。

如下图所示，我们阻止了客户机使用 HTTP 的 POST 方法，我们看看能否起到作用？

在客户机上访问百度的贴吧，准备发个帖子测试一下，如下图所示。



测试结果如下图所示，ISA 的 HTTP 过滤器拒绝了这个访问请求。

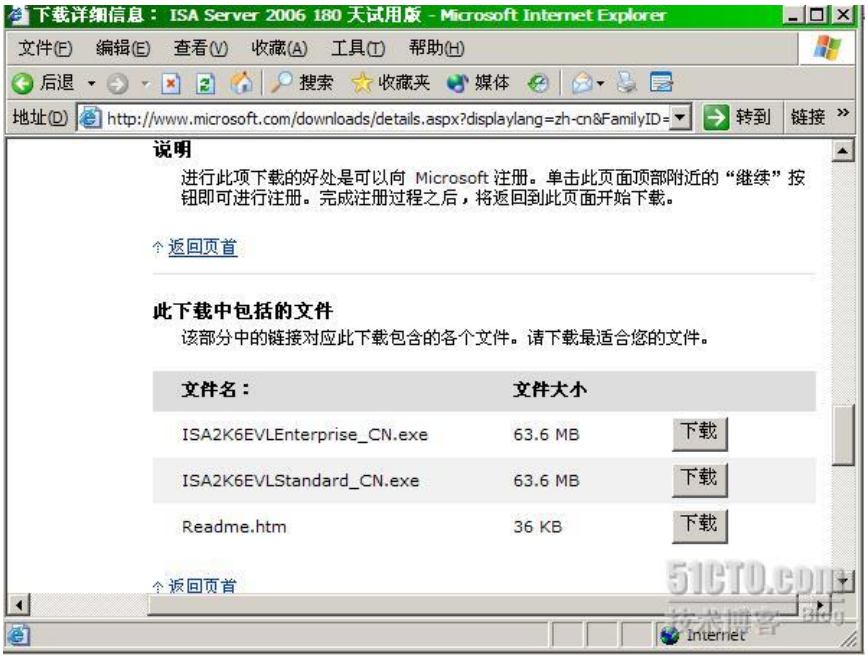


阻止方法还可以用于别的用途，例如我们想禁止用户访问代理服务器，就可以考虑阻止 CONNECT 方法，这样一来用户就不能和 Web 代理服务器建立连接了。

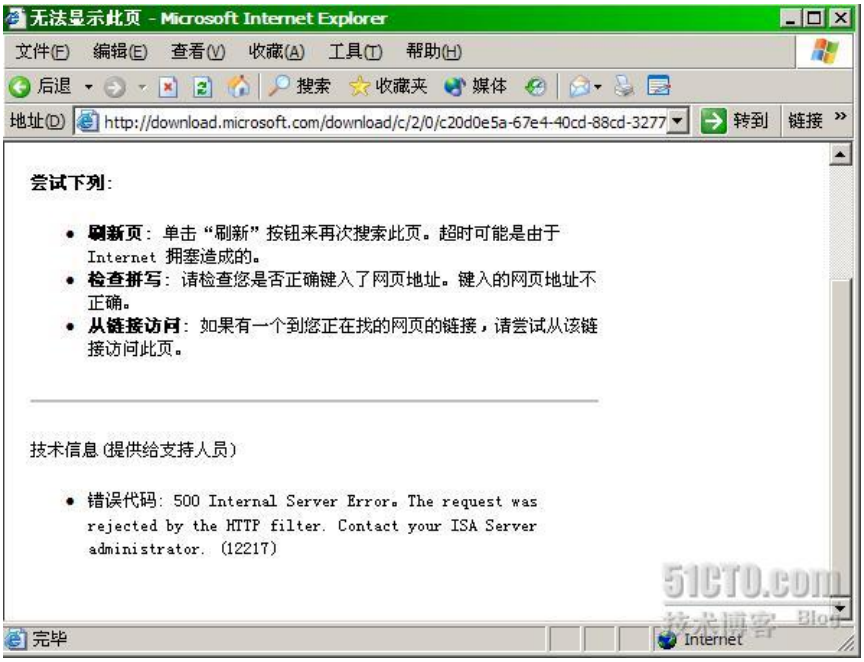
三 扩展名

切换到 HTTP 过滤的“扩展名”标签，如下图所示，我们在此可以阻止通过 HTTP 协议访问一些具有特定扩展名的文件。如果我们希望阻止用户不小心从网站下载或执行恶意代码，那么就可以在扩展名中阻止*.exe、*.vbs、*.js、*.com 等。

在 HTTP 过滤中阻止了访问*.exe 扩展名后，我们来实验一下，如下图所示，我们在客户机上下载 ISA2006 的 180 天试用版，下载的文件扩展名是 exe。



结果如下图所示，下载请求被 ISA 过滤器阻止了。



四 HTTP 头

在 HTTP 策略属性中切换到“头”标签，如下图所示，我们可以阻止指定的请求头或响应头。

下面是一些最常见的请求头，大家可以参考使用。

Accept：浏览器可接受的 MIME 类型。

Accept-Charset：浏览器可接受的字符集。

Accept-Encoding：浏览器能够进行解码的数据编码方式，比如 gzip。Servlet 能够向支持 gzip 的浏览器返回经 gzip 编码的 HTML 页面。许多情形下这可以减少 5 到 10 倍的下载时间。

Accept-Language：浏览器所希望的语言种类，当服务器能够提供一种以上的语言版本时要用到。

Authorization：授权信息，通常出现在对服务器发送的 WWW-Authenticate 头的应答中。

Connection：表示是否需要持久连接。如果 Servlet 看到这里的值为“Keep-Alive”，或者看到请求使用的是 HTTP 1.1（HTTP 1.1 默认进行持久连接），它就可以利用持久连接的优点，当页面包含多个元素时（例如 Applet，图片），显著地减少下载所需要的时间。要实现这一点， Servlet 需要在应答中发送一个 Content-Length 头，最简单的实现方法是：先把内容写入 ByteArrayOutputStream，然 后在正式写出内容之前计算它的大小。

Content-Length：表示请求消息正文的长度。

Cookie：这是最重要的请求头信息之一

From：请求发送者的 email 地址，由一些特殊的 Web 客户程序使用，浏览器不会用到它。

Host：初始 URL 中的主机和端口。

Pragma：指定“no-cache”值表示服务器必须返回一个刷新后的文档，即使它是代理服务器而且已经有了页面的本地拷贝。

Referer：包含一个 URL，用户从该 URL 代表的页面出发访问当前请求的页面。

User-Agent：浏览器类型，如果 Servlet 返回的内容与浏览器类型有关则该值非常有用。

UA-Pixels，UA-Color，UA-OS，UA-CPU：由某些版本的 IE 浏览器所发送的非标准的请求头，表示屏幕大小、颜色深度、操作系统和 CPU 类型。

五 签名

很多文档在介绍 ISA 的 HTTP 过滤功能时都会重点介绍签名，签名其实就是 HTTP 数据包中有规律出现的特征数据。我们想阻止一些 HTTP 应用程序，就可以分析一下这些程序在通讯时有哪些特征数据，然后把这些特征数据以签名的形式提交给 ISA，这样 ISA 就可以阻止这些应用程序了。最典型的例子就是即时通讯软件，如 QQ，MSN 等。

XP 中自带了一个 MSN 客户端软件 Windows Messenger，以此软件为例，Windows Messenger 登录服务器时有三种方式

1 使用 MSN Messenger 协议直接连接 MSN 服务器的 1863 端口。

2 使用 HTTP 协议连接 MSN 服务器的 80 端口。

3 使用代理服务器连接到 MSN 服务器的 80 端口。

其中第一种和第二种连接方式是很容易控制的，我们在 ISA 上封掉 MSN 服务器即可，虽然 MSN 服务器数量不少，但毕竟只是时间问题。第三种方法就不太好控制了，访问者通过代理服务器绕到 MSN 服务器上，从 ISA 的角度来看这只是内网的一台客户机访问外网的一台服务器而已。我们不可能封掉所有的代理服务器，这时就要靠签名了，我们要找出 MSN 客户端通过代理服务器访问 MSN 服务器时的特征数据，依靠这个来封掉 MSN。

微软网站给出了常用的即时通讯软件的签名，如下表所示。

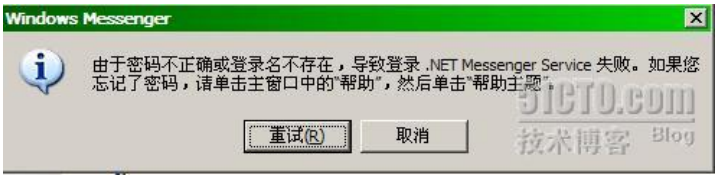
应用程序名称	搜寻范围	HTTP 头定义	签名内容

MSN Messenger	Request headers （请求头）	User-Agent:	MSN Messenger
Windows Messenger	Request headers （请求头）	User-Agent:	MSMSGS
Netscape 7	Request headers （请求头）	User-Agent:	Netscape/7
Netscape 6	Request headers （请求头）	User-Agent:	Netscape/6
AOL Messenger	Request headers （请求头）	User-Agent:	Gecko/
Yahoo Messenger	Request headers （请求头）	Host	msg.yahoo.com
Kazaa	Request headers （请求头）	P2P-Agent	Kazaa Kazaaclient:
Kazaa	Request headers （请求头）	User-Agent:	KazaaClient
Kazaa	Request headers	X-Kazaa-Network:	KaZaA

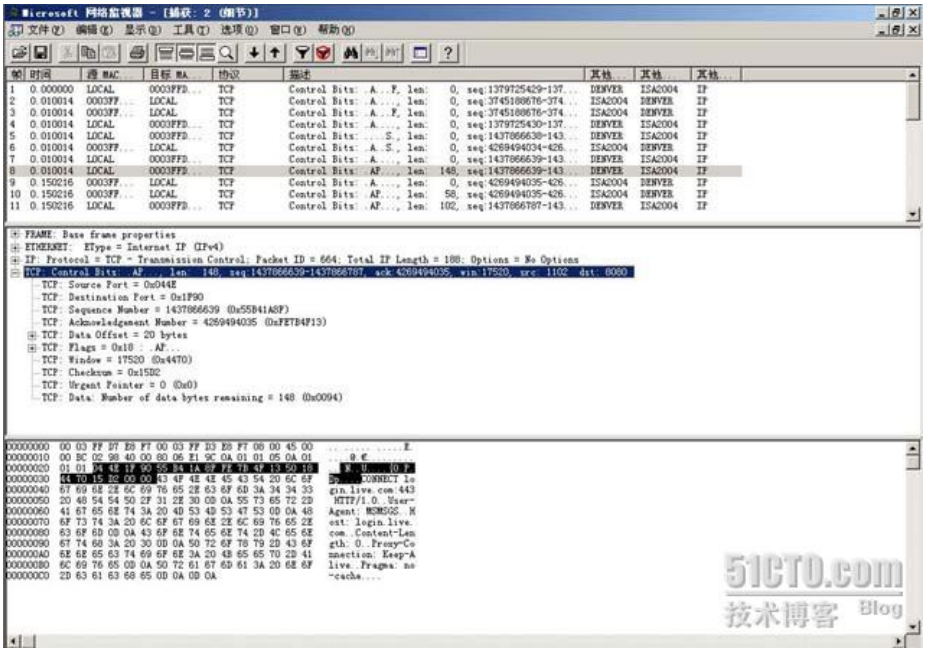
	（请求头）		
Gnutella	Request headers （请求头）	User-Agent:	Gnutella Gnucleus
Edonkey	Request headers （请求头）	User-Agent:	e2dk
Internet Explorer 6.0	Request headers （请求头）	User-Agent:	MSIE 6.0
Morpheus	Response header （响应头）	Server	Morpheus
Bearshare	Response header （响应头）	Server	Bearshare
BitTorrent	Request headers （请求头）	User-Agent:	BitTorrent
SOAP over HTTP	Request headers （请求头） Response headers （响应头）	User-Agent:	SOAPAction

按照表中内容，我们在 ISA 中利用签名封锁 MSN。在 HTTP 策略属性的“签名”标签处点击“添加”，如下图所示，我们为签名取名为“MSN”，查找范围是“请求头”，HTTP 头是“User-Agent”，签名内容是“MSMSGS”。

在 HTTP 过滤中阻止了 MSN 签名后，再用 Windows Messenger 通过代理服务器登录，原本是可以登录的，现在只能收到如下图的错误提示，签名设置成功了。



那如果我们要的签名在表中没有怎么办呢？我们可以通过抓包器来抓包分析。以 Windows Messenger 为例，如果我们想获取签名，只要在一台客户机上用 Windows Messenger 登录，然后启动抓包器抓包就可以了。抓包器我一般喜欢用 Ethereal，其实用 Windows 自带的网络监视器也可以，我们甚至可以用网络监视器抓包，然后用 Ethereal 解码分析。下图就是网络监视器抓到的 Windwos Messenger 登录服务器时的数据包，图中很明显地看到 User-Agent 的内容是 MSMSGS，这就是我们要的签名。



分析签名是比较复杂的，尤其是有些程序的签名会发生改变，例如 QQ，想要准确地分析签名需要能够熟练使用抓包工具并能深入理解 HTTP 协议。以后有时间我会写篇介绍使用抓包工具的博文，希望大家都能利用好 HTTP 过滤提供的高级功能，做好 ISA 的访问控制。

发布多个 Web 站点完全攻略：ISA2006 系列之十

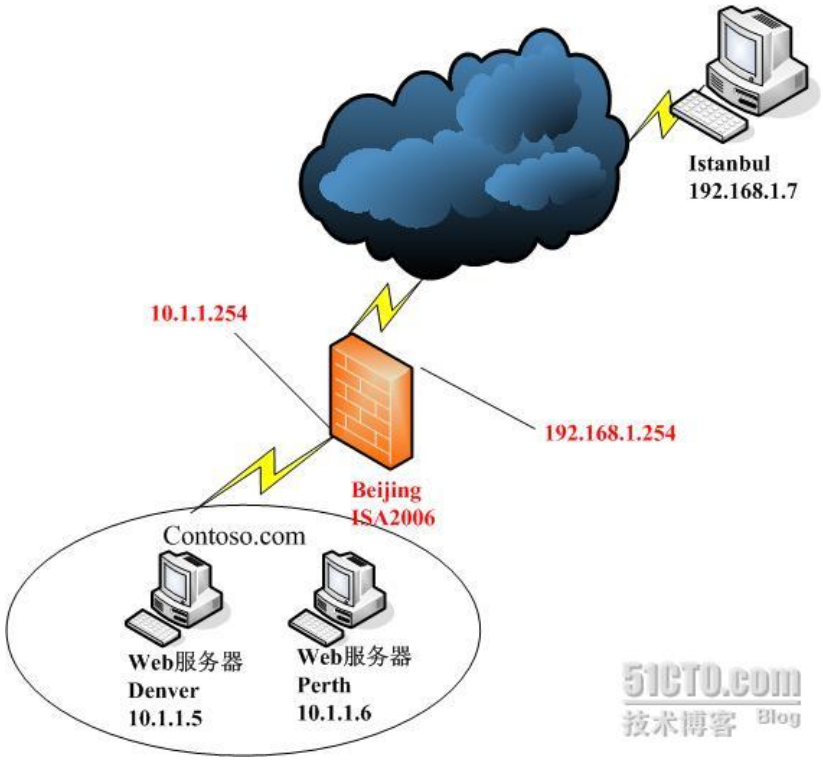
ISA2006 最常用的三大功能是访问控制，服务器发布和 VPN。访问控制我们在之前的博文中已经谈了不少，今天我们来讨论一下服务器发布。ISA 把服务器发布分为 Web 服务器发布和非 Web 服务器发布，Web 服务器发布又可以细分为安全 Web 站点发布和 Web 站点发布，今天我们讨论的是 Web 站点发布，也就是不使用证书的 Web 服务器发布。本文将介绍发布 Web 站点常用的一些技巧以及注意事项，希望能对大家有所帮助。

服务器发布简单地说就是把内网或 DMZ 的服务器发布到 ISA 的外网网卡上，让外网用户通过 ISA 的外网 IP 就能访问到被发布的服务器。但为什么需要用发布规则呢？为什么不能用访问内规则呢？创建一条访问规则允许外网访问内网被发布的服务器岂不是很简单，而且有些朋友还真就这么做过。俺来解释一下这个问题，什么时候该用访问规则，什么时候该

用发布规则取决于源网络和目标网络的网络规则（请参考 http://yuelei.blog.51cto.com/202879/84995）。如果源网络和目标网络间的网络规则允许访问，那我们就应该使用访问规则；如果源网络和目标网络间的网络规则不允许访问，那我们就应该使用发布规则。举个例子，内网到外网的网络关系是 NAT，网络规则允许从内网到外网单向访问。如果内网访问外网的服务器，我们应该用访问规则；但如果外网要访问内网的服务器，就只能通过发布规则了。

访问规则和发布规则还有一个地方有区别，访问规则使用的协议，方向都是出站；而发布规则使用的协议，方向都是入站。

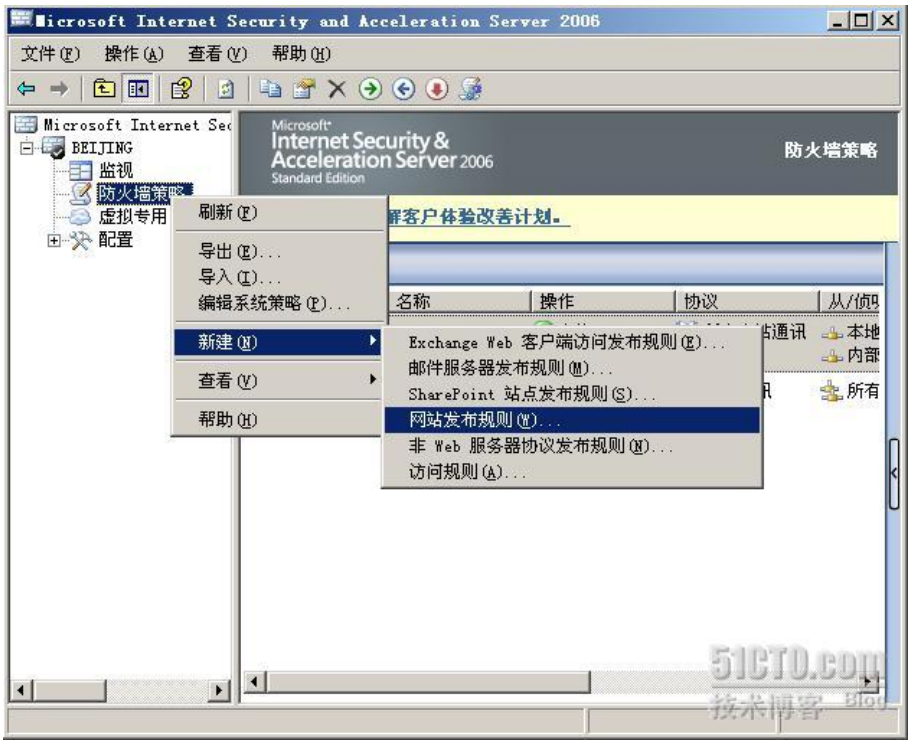
介绍了一些发布规则的理论，接下来就通过几个实验来介绍如何发布 Web 服务器。实验拓扑如下图所示，Denver 和 Perth 是内网的 Web 服务器，Istanbul 是外网的测试计算机，Denver 同时也是内网的 DNS 服务器，我们在内网部署了域环境，实际上域并非实验必须，在工作组环境下也是完全可以的。



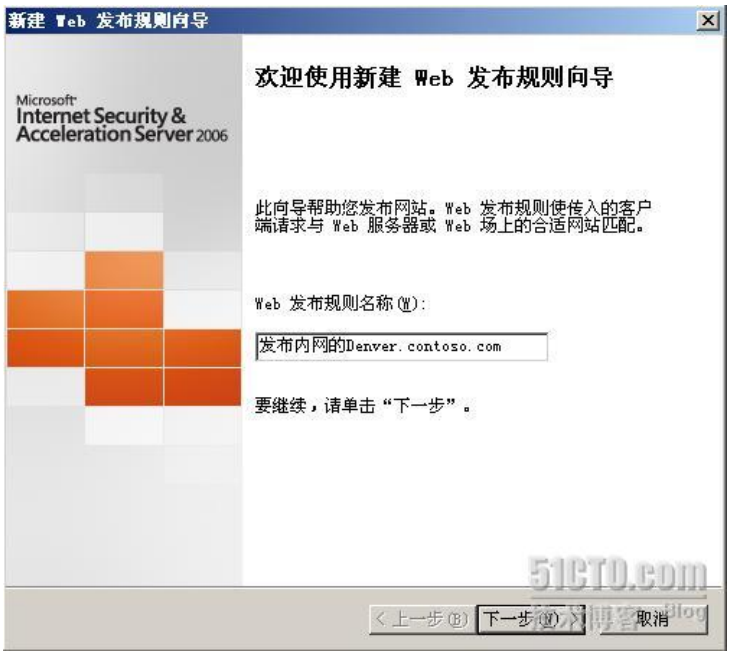
一 发布单个 Web 站点

先处理一种最简单的发布场景，我们把内网的一个 Web 站点发布出来即可。我们要发布的目标是 Denver 上的默认 Web 站点，Denver 的域名为 Denver.contoso.com，现在我们来看看应该如何操作。

在 ISA 服务器上以此点击 开始－程序－Microsoft ISA Server－ISA 服务器管理，右键点击防火墙策略，如下图所示，选择新建“网站发布规则”。

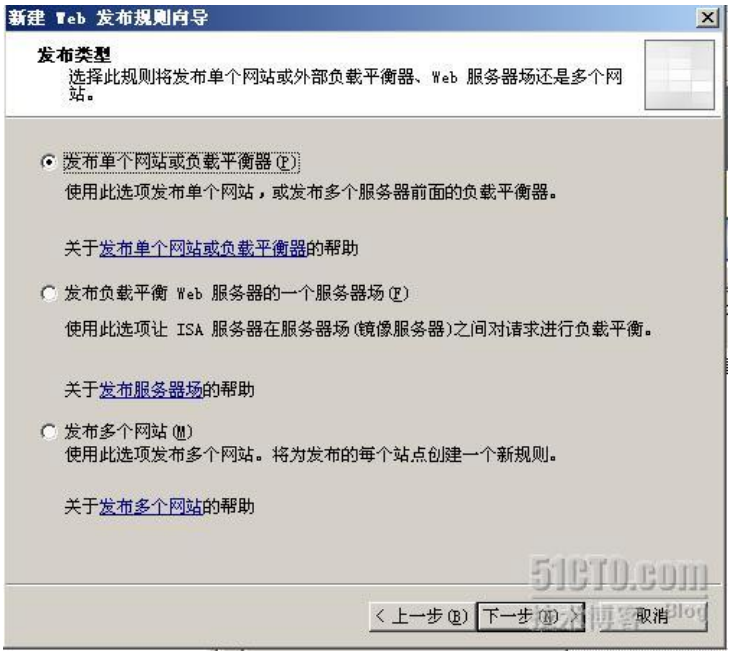


为新建的发布规则取名为“发布内网的 Denver.contsoo.com”。



当访问请求符合规则要求时，ISA 允许访问请求。

选择“发布单个网站或负载平衡器”。



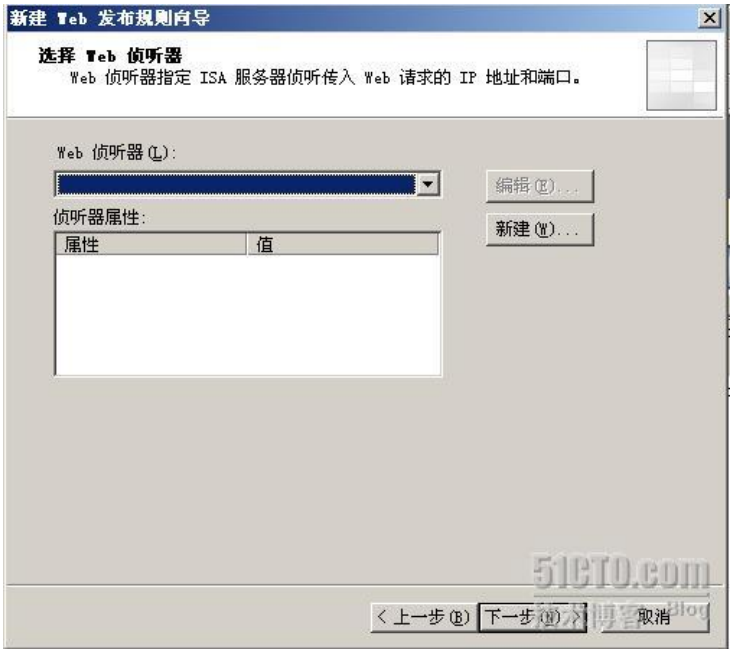
由于此次发布没有使用证书，因此我们选择使用不安全的连接发布 Web 站点。

内部被发布的站点是 Denver.contoso.com，如果担心 ISA 解析 Denver.contoso.com 有问题，可以输入 Denver 的 IP 地址 10.1.1.5。

我们选择发布路径为 /*，/*代表根目录，意思是要把 Denver 网站的所有内容都发布出来。

接下来要设置被发布站点的公共名称，也就是外网访问被发布站点时应采用哪种形式。如下图所示，如果我们在接受请求中选择“任何域名”，那意味着外网的访问者可以不限定访问域名，只要访问者使用的域名能解析为 ISA 的外网 IP 就可以，甚至可以直接用 IP 访问。

接下来我们要使用侦听器来监听 ISA 的 80 端口，安装 ISA 时要求不能有进程监听 80 端口，就是为了避免和 ISA 的 Web 侦听器冲突。由于当前没有可用的侦听器，我们点击“新建”，准备创建一个侦听器。



出现新建侦听器向导，我们为侦听器取名为“Listen 80”。

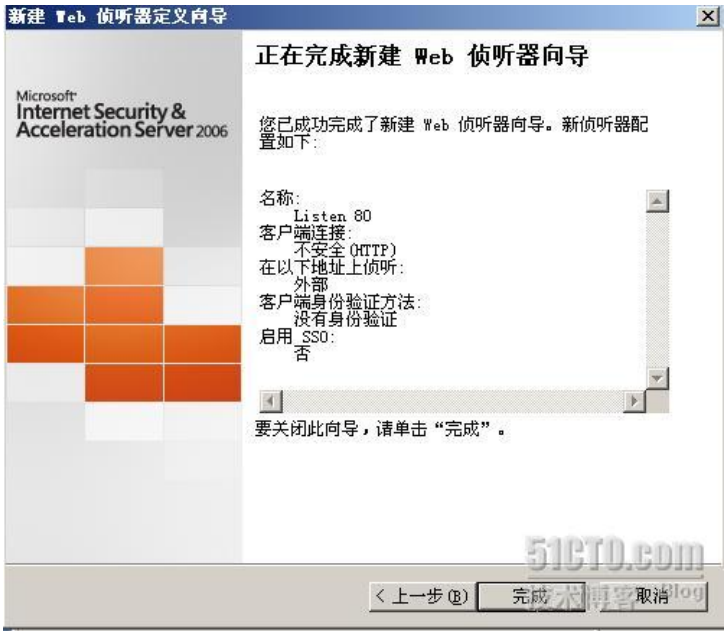
此次发布没有使用证书，不需要于客户端建立 SSL 安全连接。

让侦听器监听外部网络，也就是说侦听器将监听 192.168.1.254 的 80 端口。

侦听器不需要对用户进行身份验证，我们选择“没有身份验证”。

这次发布不需要单一登录设置。

点击完成结束创建侦听器。



回到创建发布规则向导，选择使用刚刚创建的侦听器“Listen 80”。

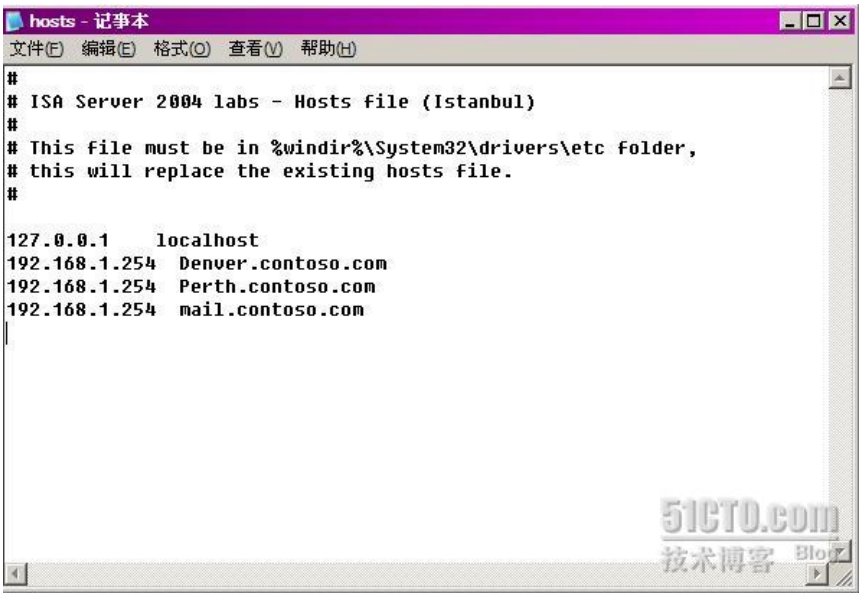
不要求客户端进行身份验证。

此发布规则适用于所有用户。

点击完成结束发布向导的创建。

等发布规则生效后，我们在外网客户机 Istanbul 上测试一下发布效果。首先我们用 IP 直接访问，如下图所示，我们在浏览器中输入 192.168.1.254，结果如下图所示，发布成功！

再用域名访问，为简单起见，我们在外网没有部署 DNS，域名解析用 hosts 文件完成，hosts 文件在 windowssystem32driversetc 目录下，内容如下图所示。在真正的生产环境下，自然会有公网的 DNS 服务器帮助解析。



有了 Hosts 文件帮助解析，在 Istanbul 上用 IE 访问 denver.contoso.com，结果如下图所示，也成功了！

由此可见，如果用 ISA 发布单个站点，还是一件相当容易的事情。

二 发布多个 Web 站点

现在我们要加点难度了，这次的发布任务是发布多个站点，内网的 Denver 和 Perth 上都有 Web 站点需要发布。我们该如何处理呢？解决思路有两个，一是创建两个侦听器，分别监听 ISA 外网 IP 的不同端口。然后创建两个发布规则，一个发布 Denver，另一个发布 Perth，两个发布规则中分别调用两个侦听器；二是只用一个侦听器，创建两个发布规则分别发布 Denver 和 Perth，两个发布规则依靠 ISA 的 Web 过滤能力进行区分。

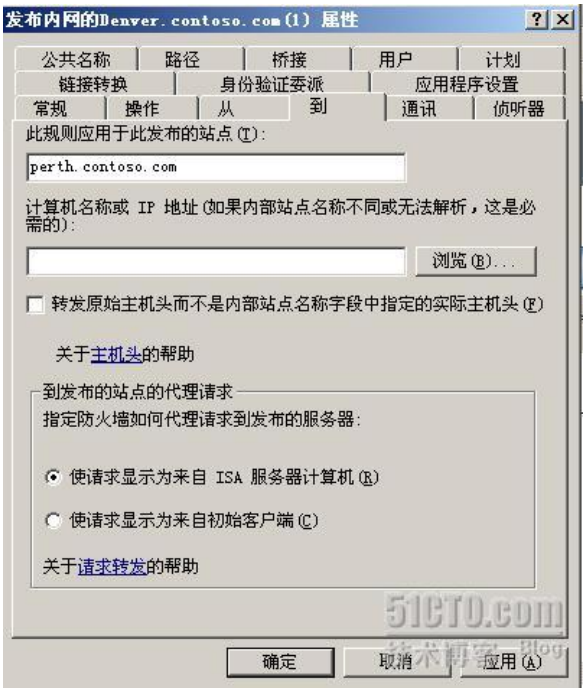
考虑到如果创建两个侦听器，那外网用户访问其中一个网站时肯定要用到非标准的 80 端口，这并非一个好的选择，因此我们倾向于采用第二种方法。那现在我们就面临一个问题，当外网用户访问 ISA 外网 IP 的 80 端口时，我们怎么能区分出访问者是要访问 Denver 还是 Perth 呢？我们可以利用发布网站的公共名称来加以区分，例如我们可以规定 Denver 网站的公共名称是 Denver.contoso.com，Perth 网站的公共名称是 Perth.contoso.com，这样根据外网用户访问域名的不同，我们就可以区分出外网用户访问的目标网站到底是谁。

我们看看具体该如何去做，首先我们要为 Perth 网站创建一条发布规则，考虑到这条发布规则和发布 Denver 的规则有类似之处，我们就使用简单些的办法，将 Denver 的发布规则复制过来，然后稍加修改即可。如下图所示，在右键单击 Denver 的发布规则，选择“复制”。

在 Denver 的发布规则上中单击右键，选择“粘贴”，即可复制 Denver 的发布规则，如下图所示，就是复制发布规则后的场景。

接下来我们要修改复制的发布规则，让它能够用于发布 Perth 站点。编辑“发布内网的 Denver.contoso.com（1）”，如下图所示，切换到常规标签，将发布规则名称改为“发布内网的 Perth.contoso.com”。

切换至发布规则的“到”标签，将发布的站点改为“perth.contoso.com”。



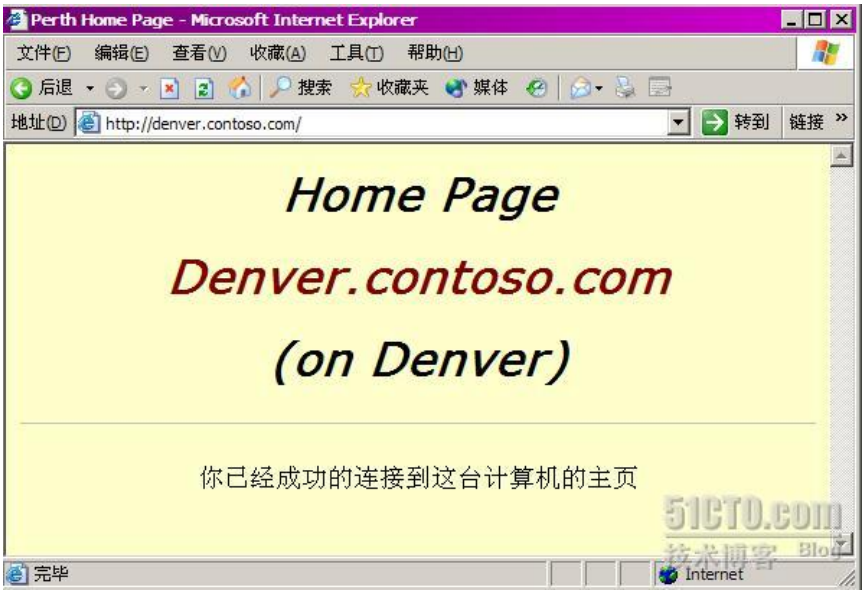
切换到发布规则的“公共名称”标签处，选择此规则应用到“以下网站的请求”，如下图所示，点击“添加”按钮，在公共名称对话框中输入 perth.contoso.com。这样以后访问者必须用域名 perth.contoso.com 访问，才能和这条发布规则匹配。

这样 Perth 的发布规则就修改完成了，接下来对 Denver 的发布规则也要进行修改，我们对 Denver 的发布规则只修改公共名称一项。原先的公共名称是允许“任何请求”，这样的公共名称可以匹配任何访问请求，外网用户无论是访问 Perth 还是 Denver 都能和这条规则匹配上，这样一来其他的 Web 站点发布规则就等于无用了。因此我们要把 Denver 发布规则的公共名称改为 Denver.contsoo.com，如下图所示。

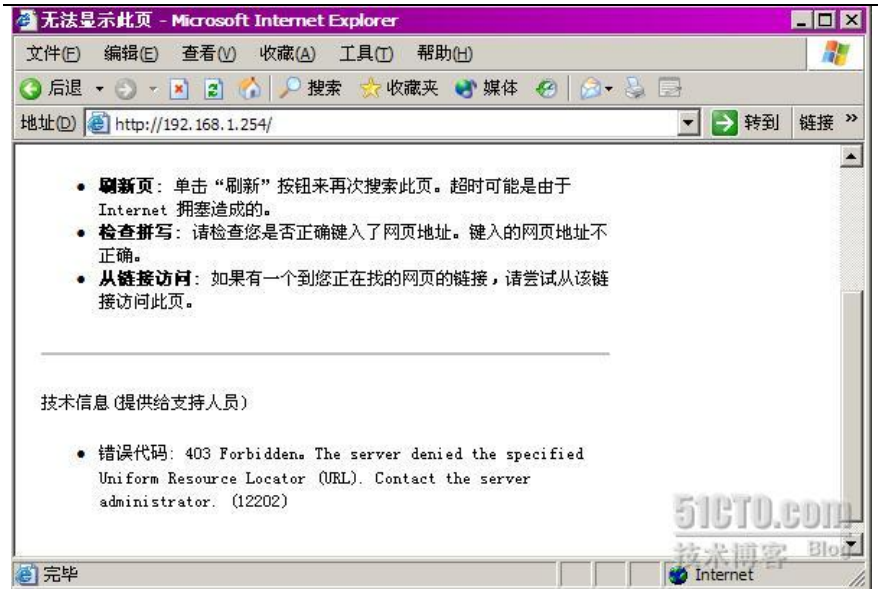
修改后的发布规则如下图所示。

好了，万事俱备，只欠测试了，我们在 Istanbul 上开始测试，首先用 IE 访问 Perth，如下图所示，访问成功了。

再来访问 Denver，如下图所示，也成功了！

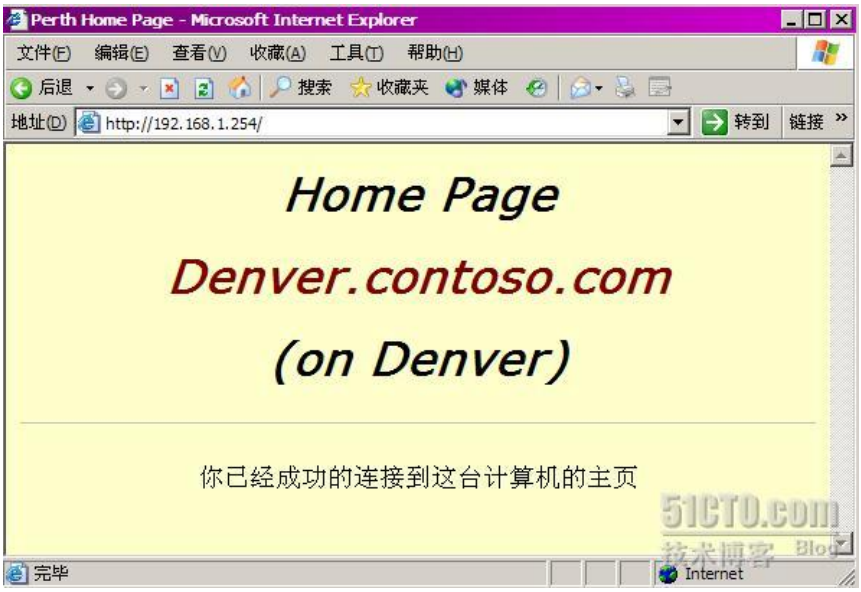


有的朋友可能会想，如果 Istanbul 用 IP 访问，会访问到哪个内网的网站呢？看看下图的访问结果，大家很可能会大吃一惊，为什么用 IP 访问会被 ISA 拒绝呢？因为目前两个发布规则的公共名称没有一个能和 192.168.1.254 匹配，因此 ISA 认为 Istanbul 的访问请求无法匹配任何一条发布规则，只能用默认规则进行拒绝。



如果我们希望用 IP 访问能够访问到 Denver，那就修改 Denver 的发布规则，在发布规则的公共名称加上一条 IP 地址，如下图所示。

这次再用 IP 访问，由于 IP 地址可以和 Denver 发布规则中的公共名称匹配上，因此顺理成章地访问到了 Denver，如下图所示。



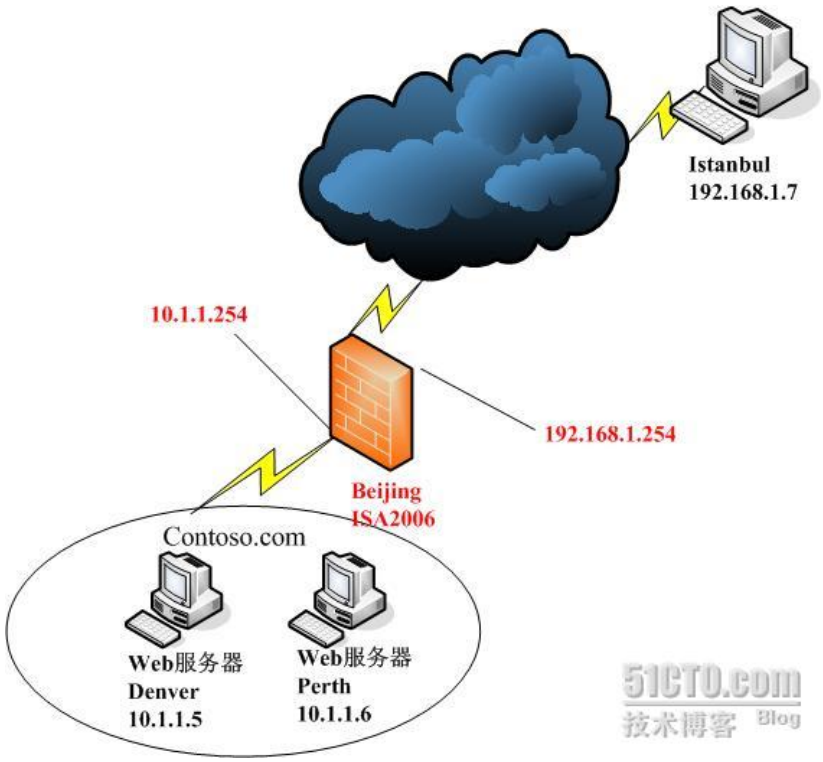
总结：由此可见，ISA 可以根据发布规则的公共名称对外网的访问请求进行 Web 过滤，功能远远强于一般路由器的端口映射发布单个站点非常简单。从实验过程来看，发布单个站点非常简单，发布多个网站只要注意用公共名称区分发布规则，其实也不难。但发布 Web 站点还有不少棘手的问题，我们在后续文章中继续讨论。

发布 Web 服务器上的虚拟主机：ISA2006 系列之十一

在上一篇博文中，我们讨论了如何利用 ISA2006 发布内网的多个 Web 站点，这些 Web 站点分布在不同的 Web 服务器上，我们只要用发布规则中的公共名称加以区分就可以了。今天我们要把难度再加大一些，如果一台 Web 服务器上有虚拟主机，这些虚拟主机该如何发布呢？

其实发布这些虚拟主机也不难，我们知道 IIS 实现虚拟主机有三种方法，IP，端口和主机头，一般在工作中大都采用主机头区分虚拟主机。既然如此，那在发布虚拟主机时，我们就可以依靠访问者提交的主机头来匹配发布规则，恰好 ISA 又有转发原始主机头的功能，这下子问题就全都解决了。

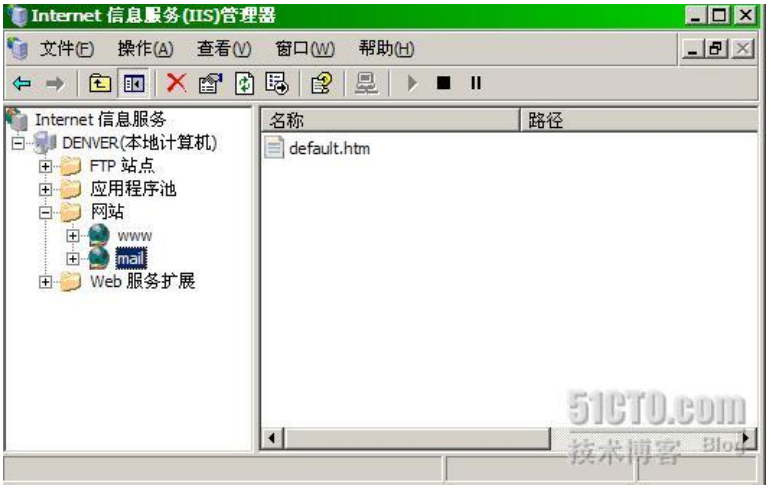
举个例子来说明，实验拓扑和上篇博文中一样，Denver 和 Perth 是内网的两台 Web 服务器。现在 Denver 上有两个网站，分别是 www.contoso.com 和 mail.contoso.com，我们的目标就是把这两个虚拟主机发布到外网。这个目标实现起来并不难，在 ISA 上为 Denver 的两个网站各自创建一条发布规则，两条发布规则依靠公共名称区分两个网站，然后 ISA 启用转发原始主机头功能，这样就一切 OK 了。当外网访问 www.contoso.com 时，ISA 根据访问域名匹配发布规则，然后按照发布规则的要求将原始主机头 www.contoso.com 转发给 Denver，Denver 根据转发来的原始主机头就可以判断出访问者要访问哪个虚拟主机，然后将目标网站的内容返回给访问者。



实验步骤如下：

一　准备虚拟主机

在 Denver 上准备好两个虚拟主机，如下图所示，我们在 Denver 的 IIS 中看到了两个网站，www 和 mail。



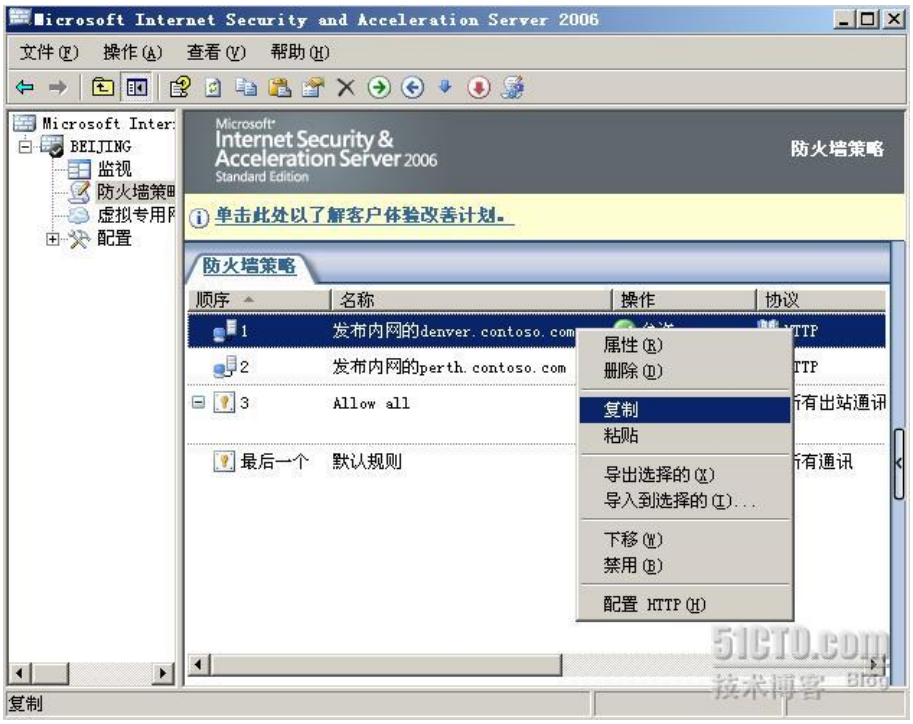
两个网站的主机头分别是 mail.contoso.com 和 www.contoso.com。，如下图所示。

用浏览器访问，两个网站都访问正常，如下图所示。

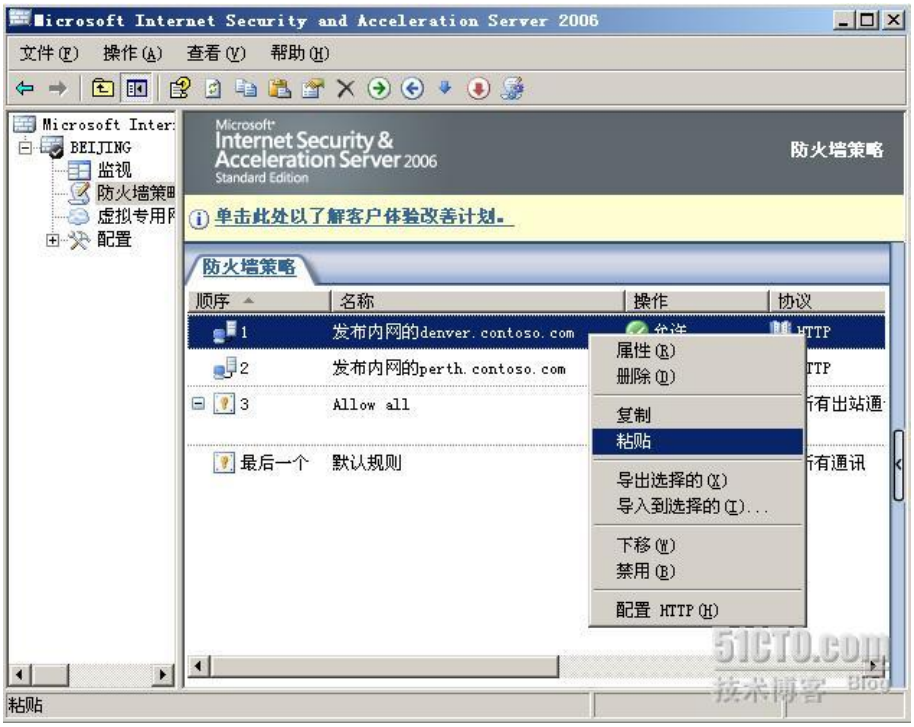
OK，实验用的虚拟主机已经准备好了！

二 在 ISA 上创建访问规则

上篇博文中我们在 ISA 上创建了两条发布规则，这次实验我们只要把发布规则复制一下再稍作修改就可以了。如下图所示，我们在发布 denver.contoso.com 的规则上点击右键，选择“复制”。



然后在发布规则上点击右键，如下图所示，选择“粘贴”。

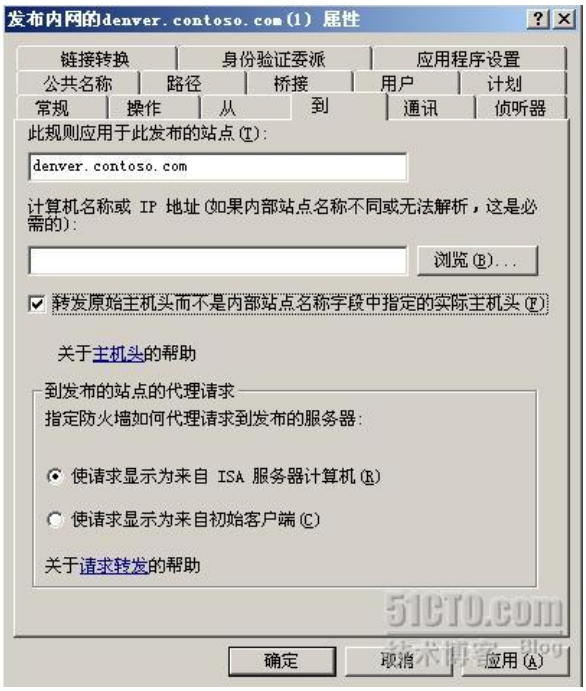


这样我们就有了两条发布规则，我们只要修改这两条规则就可以满足发布虚拟主机的需求。

首先修改第一条发布规则，我们要利用这条规则发布 denver 上的 www.contoso.com，如下图所示，在规则属性的常规标签中，修改规则的名称为“发布内网的 www.contoso.com”。

切换到规则属性的“公共名称”标签，编辑原有的公共名称 denver.contoso.com，如下图所示，把公共名称修改为 www.contoso.com。

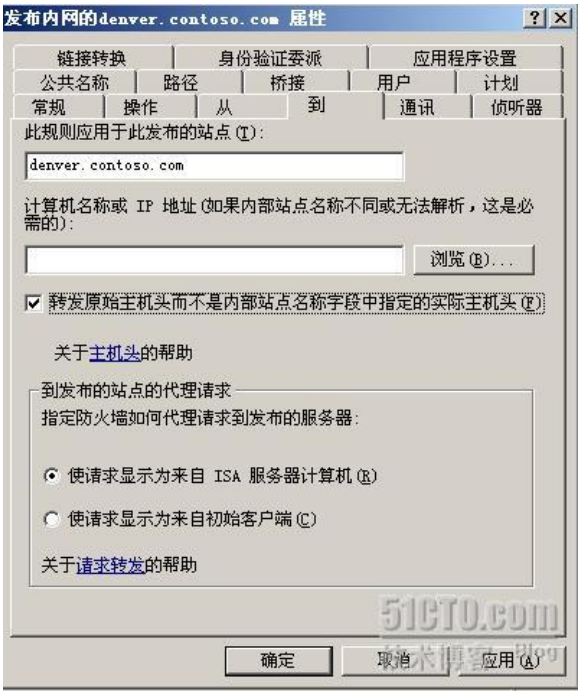
切换至规则属性的“到”标签，如下图所示，勾选“转发原始主机头而不是内部站点名称字段中指定的实际主机头”，这是关键之处，它要求 ISA 将访问者的原始主机头转发给 Web 服务器，Web 服务器正式凭借原始主机头才能判断出访问目标是哪个虚拟主机。



好了，为发布 www.contoso.com 而修改的规则已经完成，接下来我们要修改第二条发布规则，让它能够发布 mail.contoso.com。如下图所示，在第二条发布规则属性的“常规”标签中，修改规则名称为“发布内网的 mail.contoso.com”。

切换到规则属性的“公共名称”标签，编辑原有的公共名称 denver.contoso.com，如下图所示，把公共名称改为 mail.contoso.com。

切换到规则属性的“到”标签，勾选“转发原始主机头而不是内部站点名称字段中指定的实际主机头”。



修改后的发布规则如下图所示。

三 在客户机上测试

在 ISA 上做好发布规则后，我们在 Istanbul 上测试一下，首先 Istanbul 仍然是利用简单的 Hosts 文件进行域名解析，解析结果如下图所示。

测试一下，先访问 www.contoso.com，如下图所示，非常理想。

再来测试一下 mail.contoso.com，如下图所示，一切正常，OK，实验成功！

做了这么多工作，其实发布虚拟主机关键之处就是要在 ISA 上转发原始主机头，掌握了这点，就基本上能够掌控全局了！

让你的 Web 服务器不再裸奔：ISA2006 系列之十二

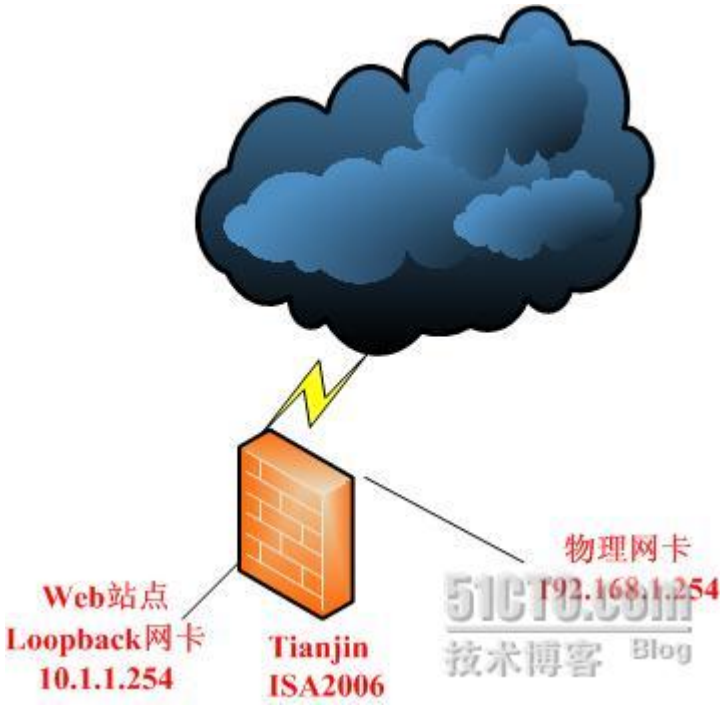
很多小型企业限于资金紧缺，无法让 Web 服务器得到很好的安全防护，往往就把一台 Web 服务器孤零零地扔在 IDC 机房里。这么处理的结果可想而知，Web 服务器要么被黑客们当成了练兵场，要么沦为肉鸡，成为下一次网络攻击的踏板，能够毫发无伤全身而退的基本是凤毛麟角。其实，只要在 Web 服务器上用防火墙保护一下，效果就要好上很多，一般普通的攻击都可以挡住。提到这里，有些老板又要邹眉头了，“防火墙好是好，就是这个成本，太，太高了一些.....”。错！今天我们提供的这种保护 Web 服务器的方案并不需要额外的硬件投入，只要在 Web 服务器上安装上软件防火墙 ISA2006，利用 ISA 的 Web 服务器发布功能就能享受到低投入高安全的乐趣。

我们准备了一台 Web 服务器 SERVER1 进行测试，如下图所示，SERVER1 有个测试用的网站，我们来看看如何利用 ISA2006 保护这个可怜的 Web 服务器。

大致思路是这样的，在 Web 服务器上安装一块虚拟网卡，将 Web 站点建在虚拟网卡上，在 ISA 上用 Web 发布规则把虚拟网卡上的 Web 站点发布到物理网卡上。这个过程听起来平淡无奇，为什么还值得大书特书一番呢？关键就是要避免 IIS 和 Web 侦听器的冲突。两者都要监听 8 0 端口，前面安装 ISA 时，我们提到过 ISA 服务器上不应该有进程守护 80

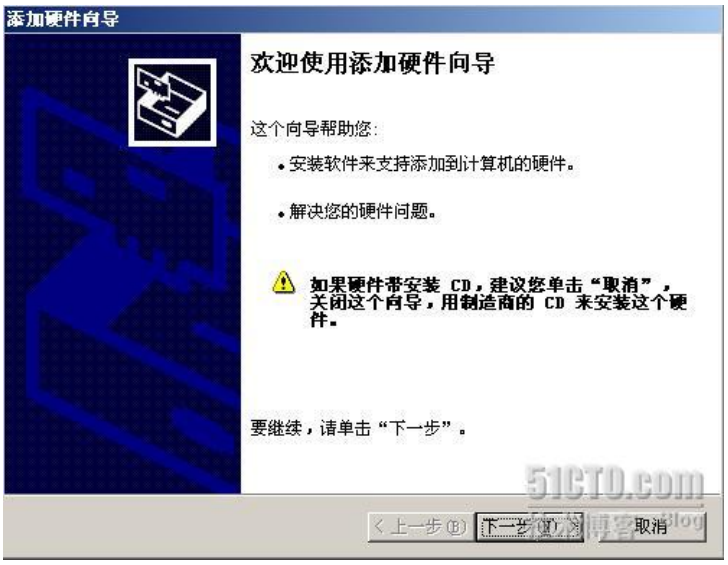
端口，就是为了避免和 Web 侦听器冲突。但现在我们不得不考虑如何解决 80 端口的冲突问题，这篇文章关键之处就在这里。

解决冲突有两种方法，端口重定向和取消 HTTP 套接字池，具体容我一一道来。但之前先将实验环境搭好，包括创建虚拟网卡，安装 ISA2006 等。搭好后的实验拓扑如下图所示。



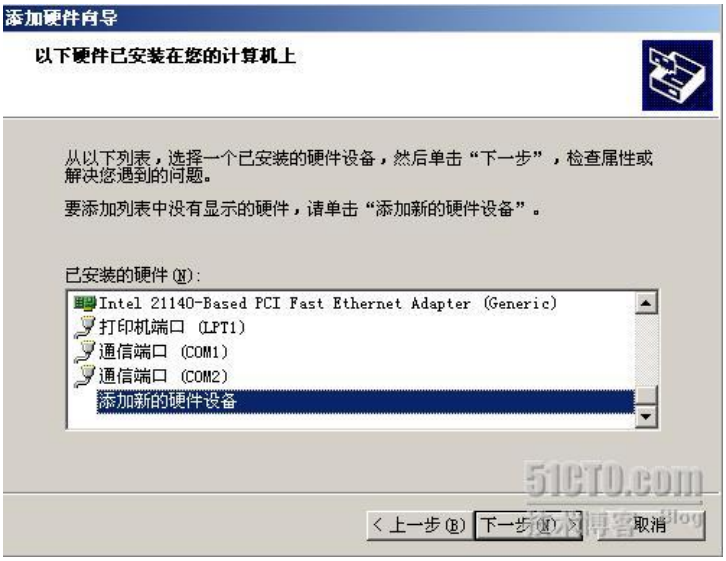
一 安装虚拟网卡

要在 Web 服务器上安装 ISA，首先要有两块以上的网卡，这倒用不着专门去买一块新网卡，我们在 Web 服务器上添加一块虚拟网卡就可以了。微软在系统中提供了 Loopback 回路网卡，Loopback 网卡就是能提供协议绑定的虚拟网卡，我们只要添加一块 Loopback 网卡就可以了。在 Web 服务器的控制面板中选择“添加硬件”，如下图所示，出现添加硬件向导。

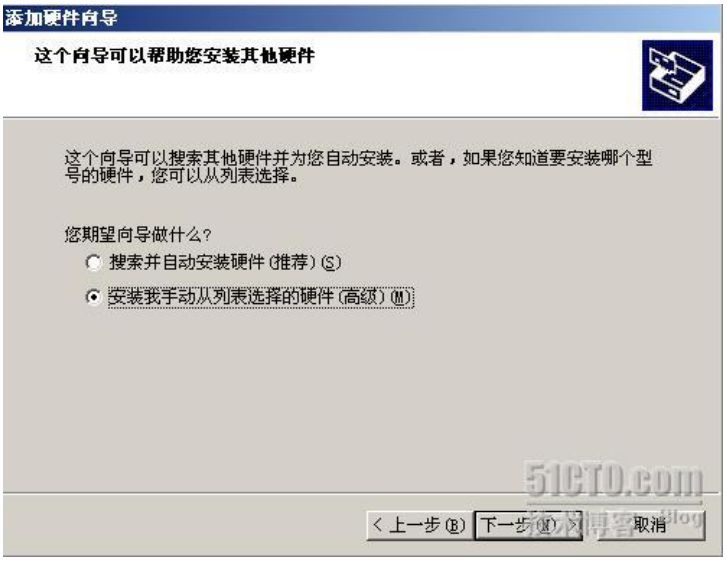


选择硬件已连接好。

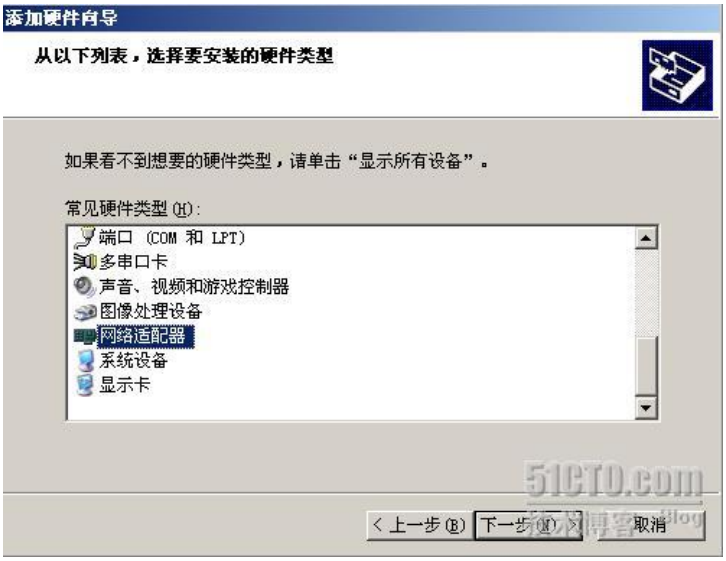
选择“添加新的硬件设备”。



选择手工添加硬件。



硬件类型为网络适配器。



网卡型号要选择微软公司的 Loopback 网卡。

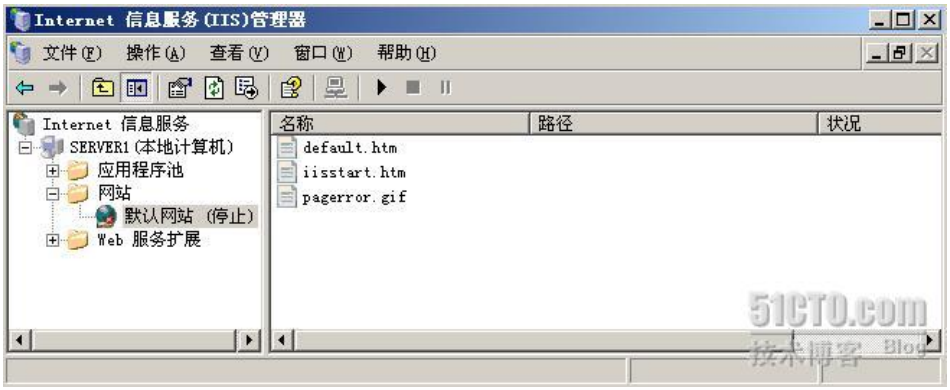
安装完 Loopback 网卡后，如下图所示，计算机中有了两块网卡，Loopback 网卡的 IP 地址为 10.1.1.254，255.255.255.0；物理网卡为 192.168.1.254 255.255.255.0，虽然添加的是一块虚拟网卡，但在 ISA 看来和物理网卡并没有区别。

二 安装 ISA2006

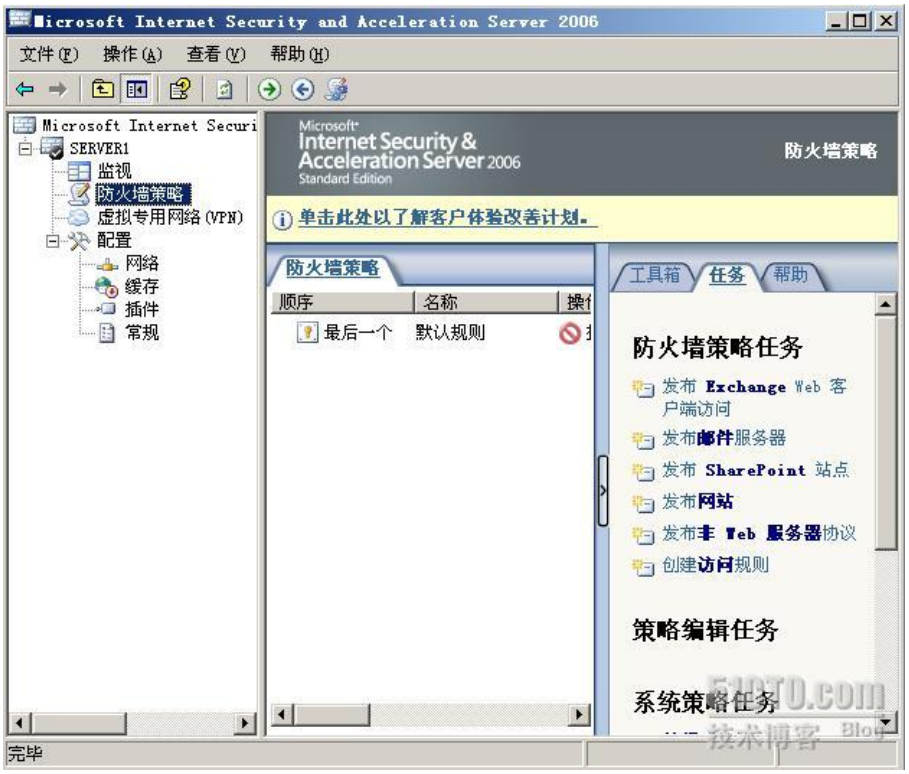
既然 Web 服务器上已经有了两块网卡，那安装 ISA2006 就没有问题了。ISA2006 的安装过程就不具体介绍了，前面的博文已经提及，大家只要注意两点：

1） ISA 内网的地址范围是 10.1.1.0 255.255.255.0，和虚拟网卡关联。

2） ISA 安装之前要关闭 IIS 网站，如下图所示，因为我们目前还没有找到解决冲突的办法，因此只能先把站点关闭。



ISA2006 安装完毕，如下图所示，好了，环境已经搭好，我们要开始了！

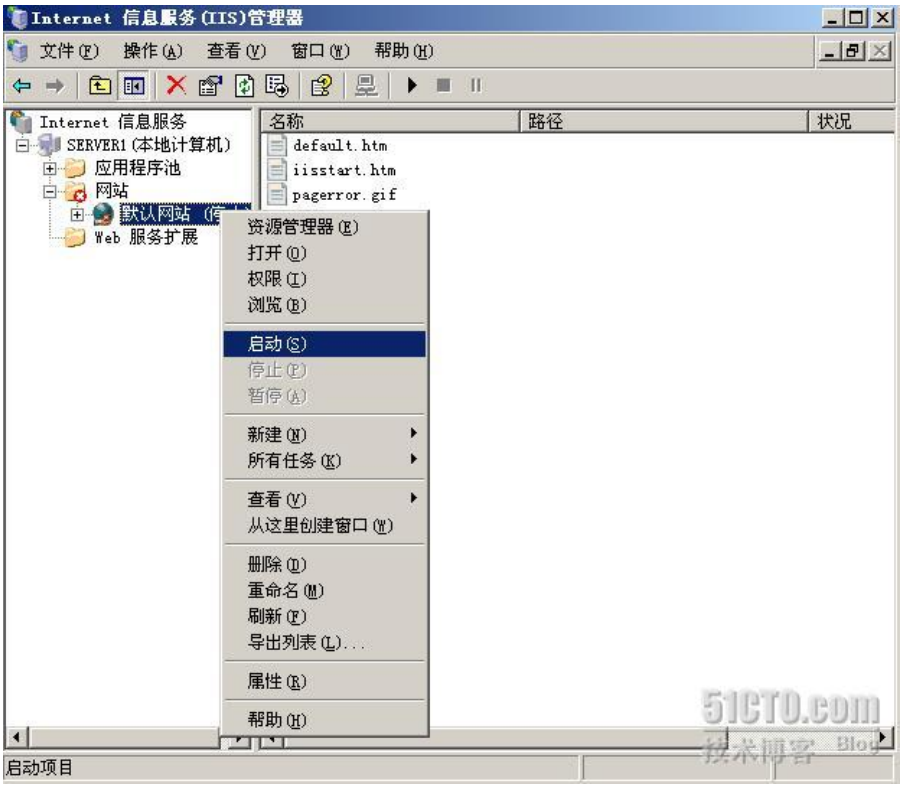


三 端口重定向

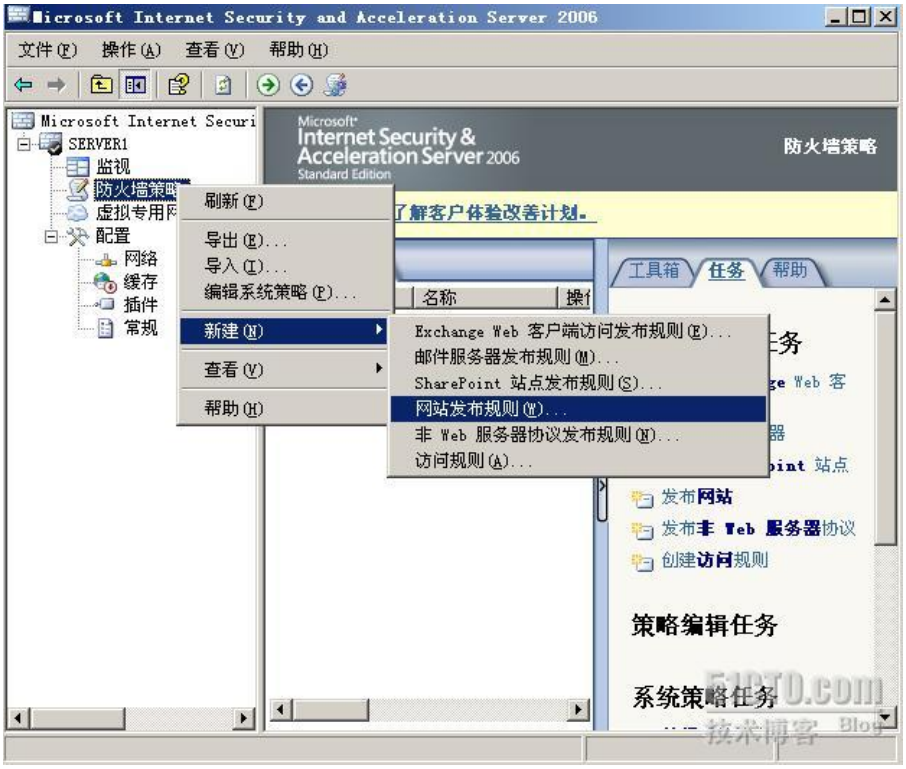
我们先考虑简单的解决方法，如果 Web 站点不放在 80 端口，而放在其他端口如 81，这样就不会和 Web 侦听器有冲突了。发布规则也恰好支持端口重定向，因此这个解决方法简单易行，如果网站对 80 端口没有特殊要求，建议用此方法解决问题。

首先我们修改网站端口，如下图所示，在默认站点的属性中将 TCP 端口改为 81。

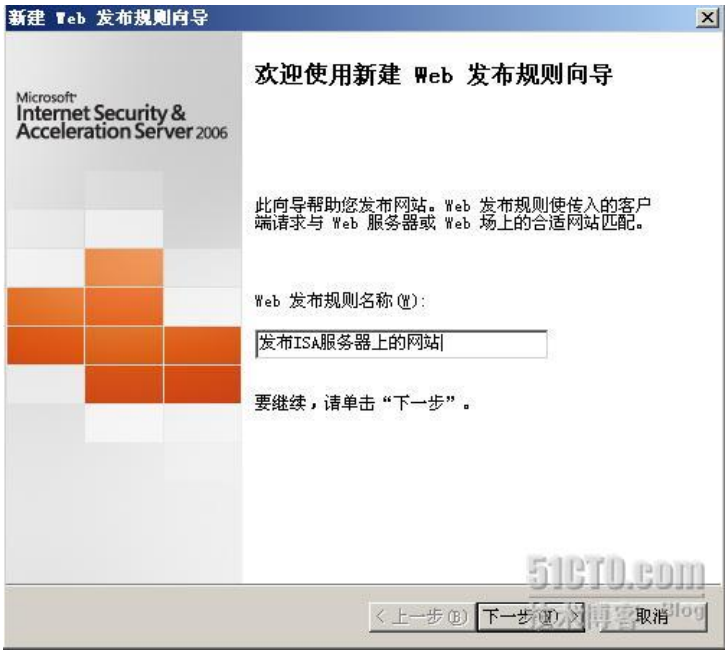
然后就可以启动 Web 站点了，如下图所示，右键点击默认网站，选择“启动”。



接下来要在服务器上创建一条 Web 发布规则，如下图所示，新建一条网站发布规则。



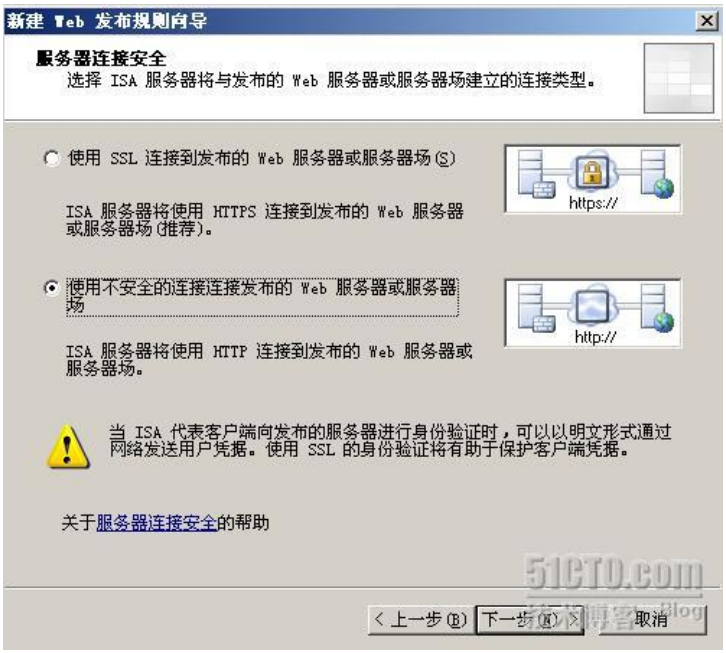
为发布规则取个名字。



当访问请求匹配发布规则时允许访问。

发布单个网站。

此次发布不使用证书加密。



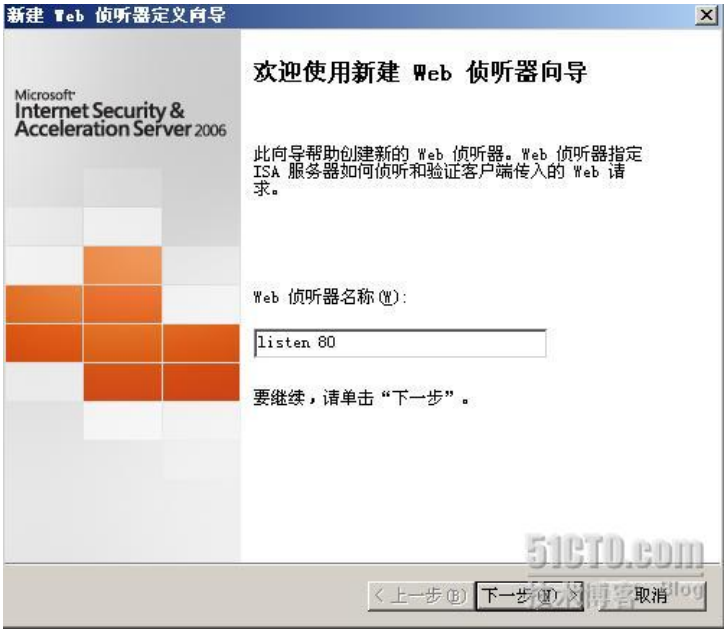
被发布的网站是 10.1.1.254，注意，目前 ISA 认为被发布的服务器在 10.1.1.254 的 80 端口，其实是在 81 端口，我们过一会要修改这个参数。

发布整个网站，从根目录开始。

对访问请求的格式不作任何限制，域名或 IP 均可。

目前还没有 Web 侦听器，选择“新建”。

为侦听器取个名字。



侦听器不对访问请求加密。

侦听器负责监听外网。

不对用户进行身份验证。

不使用 SSO 单一登录设置。

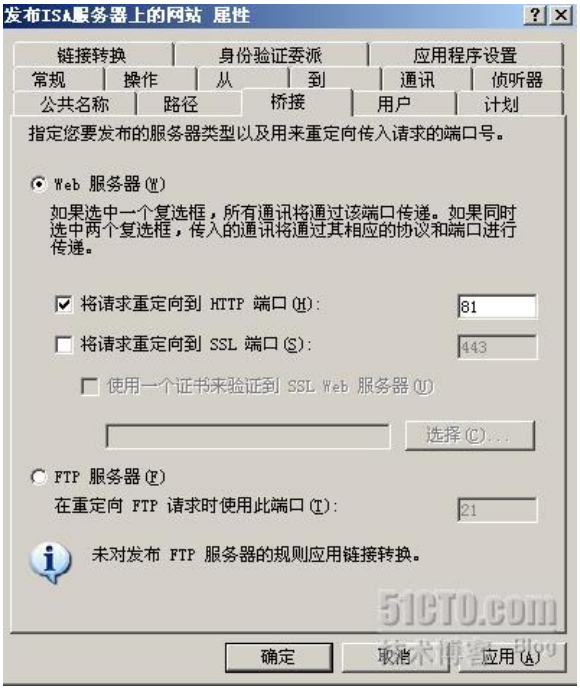
选择使用新创建的 Web 侦听器。

被发布的服务器不要求身份验证。

发布规则适用于所有用户。

如下图所示，发布规则已经创建，只是此规则中认为发布的网站在 10.1.1.254 的 80 端口，我们要修改端口。

切换到发布规则属性的“桥接”标签，如下图所示，勾选“将请求重定向到 HTTP 端口”，端口值填写 81。



好了，我们来测试一下发布规则，如下图所示，客户机访问 ISA 的外网地址，访问到了内网网卡 81 端口上的网站，发布 ISA 服务器上的网站成功了！

四 配置 HTTP 套接字池

端口重定向为我们提供了一种简单的解决方法，但它改变了发布网站的端口，如果某些网站出于某种原因必须在 80 端口，那我们就必须想想其他办法了。我们能否让 IIS 监听内网的 80 端口，Web 侦听器监听外网的 80 端口，这样不就可以和平共处了？有些朋友立刻想到了 IIS 中可以把网站绑定到一个指定的 IP 上，他们说干就干，立即动手，如下图所示，在 IIS 中将网站绑定到了 10.1.1.254 上，这么做是否能如愿以偿呢？

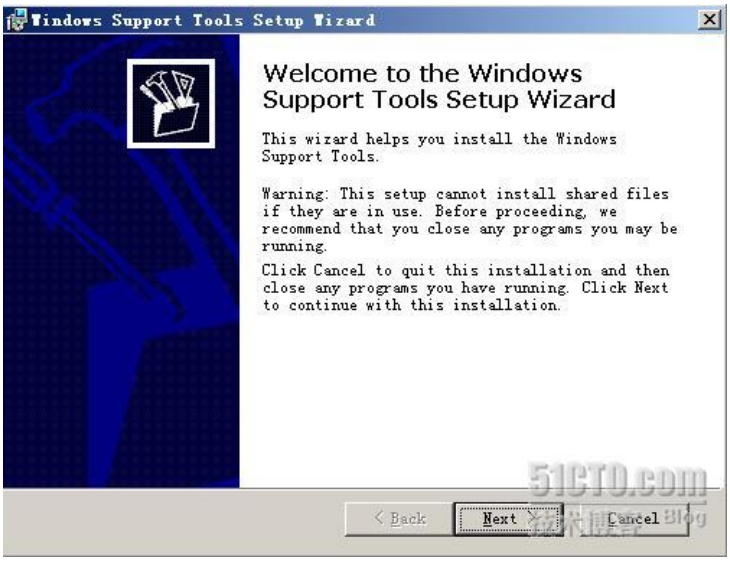
如下图所示，我们用 netstat 检查端口监听情况，如下图所示，发现 IIS 监听的可不止 10.1.1.254 的 81 端口，而是在所有 IP 的 81 端口都进行监听，这是为什么呢？

IIS 的这种特性称为 Socket Pooling（套接字池）。套接字（Socket ）是 IP 地址和端口的组合，用于进行网络通讯，任何应用程序需要和网络上的其他应用程序进行通许时，必

须具有相应的套接字。例如 Web 站点侦听客 户的 HTTP 请求，那么它就绑定在相应的套接字（IP 地址和端口，例如端口为标准的 TCP 80）上。在 IIS 4.0 中，微软发现当多个 Web 站点分别通过不同的套接字绑定在不同的 IP 地址时，会占用较多的系统资源，于是在 IIS 5.0 中引入了 Socket Pool（套接字池）这个概念。它的工作原理是这样的：IIS 启动时会将所有 Web 站点配置的服务端口绑定在计算机的所有 IP 地址上，而不管这些 IP 地址是否分配给了这些 Web 站点，IIS 把绑定的这些套接字称为套接字池；然后 IIS 再将套接字池中的套接字根据 Web 站点的配置分配到相应的 Web 站点，这样 避免了不同 Web 站点占用不同 IP 地址的相同 Web 服务端口时需要不同的套接字，从而减少了系统资源的占用，提高了 IIS 的性能。

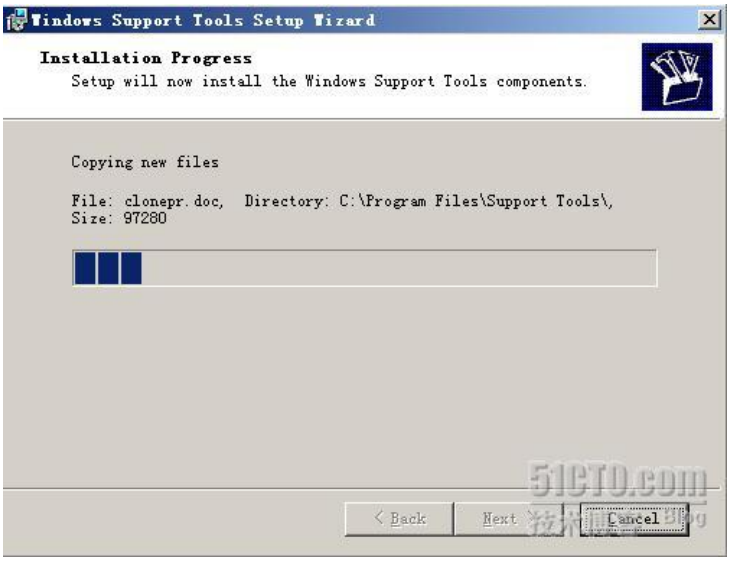
听了上面的介绍，您明白了套接字池是怎么回事，在目前的实验环境中，套接字池显然起了负作用，我们要想办法消除套接字池。Win2003 安装光盘的支持工具集中有一个工具 httpcfg 可以帮我们完成这个任务，我们先安装支持工具，在服务器上放入 Win2003 的安装光盘，如下图所示，在安装光盘的 SupportTools 目录下，双击 suptools.msi。

启动安装向导。

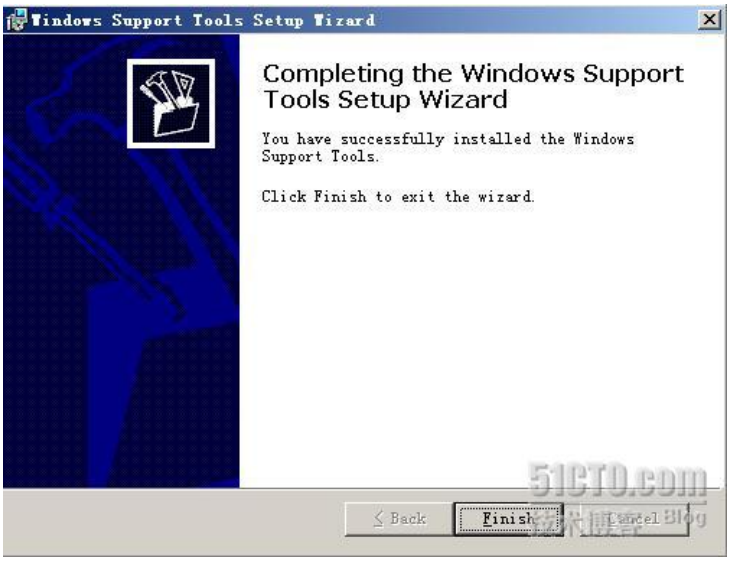


同意最终用户许可协议。

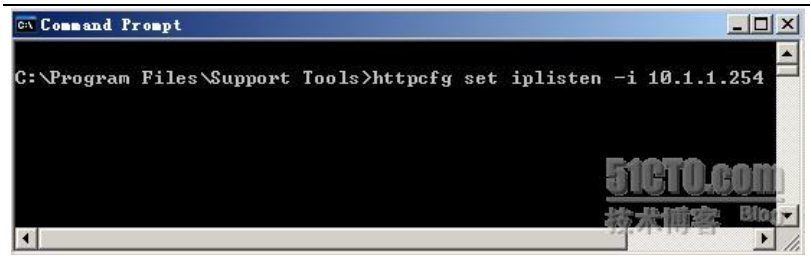
回答完软件安装路径等问题后开始安装支持工具了。



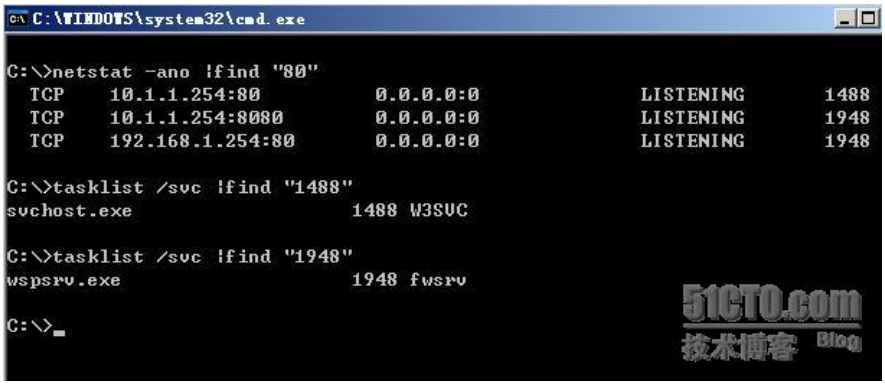
支持工具很快安装完成。



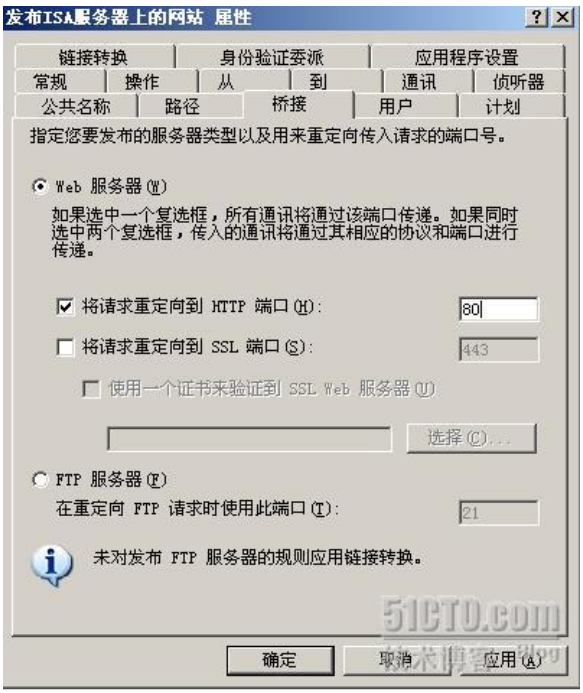
在服务器上依次点击 开始－程序－Windows Support Tools－Command Prompt，如下图所示，输入 httpcfg set iplisten –i 10.1.1.254，这条指令的目的是让 IIS 只在 10.1.1.254 上监听端口。



重启服务器让配置生效，然后我们在 IIS 中将默认网站的端口从 81 改为 80，如下图所示，用 netstat 查看端口状况，我们发现构想已经实验，ISA 监听外网 80 端口，IIS 监听内网 80 端口。



对发布规则进行修改，如下图所示，将发布网站从 81 端口改为 80 端口。



好了，现在测试一下，如下图所示，发布网站工作正常，HTTP 套接字池配置成功！

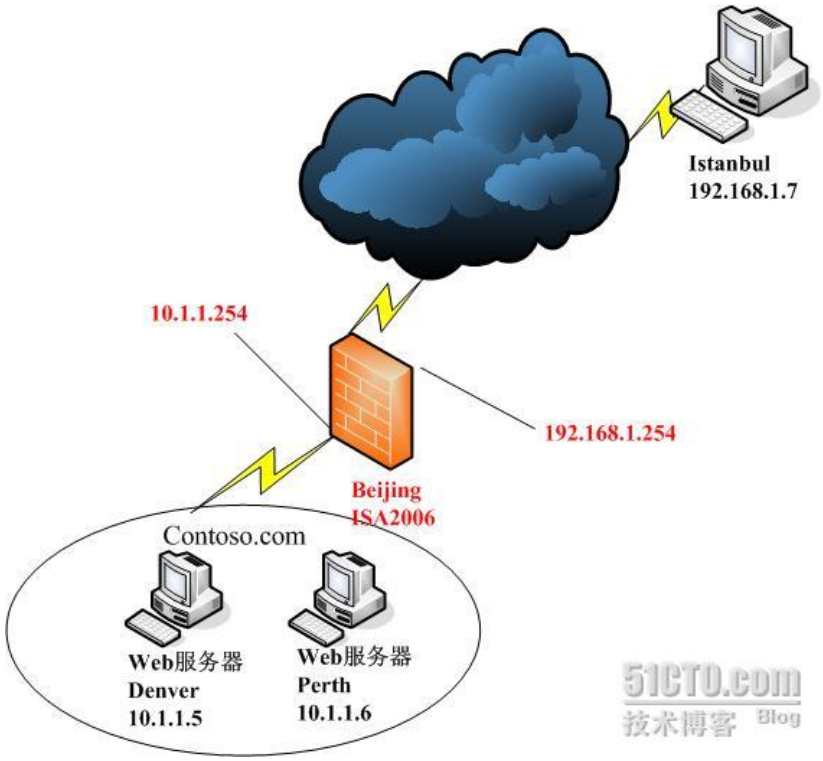
总结：两种方法中端口重定向比较简单，如果网站对端口没有特殊要求，推荐使用这种方法，否则只能借助 HTTPCFG 配置套接字池了。理论上可以考虑让 Web 侦听器监听其他端口，但其实缺乏可行性。

灵活运用 ISA 的链接转换功能：ISA2006 系列之十三

在 ISA 的发布规则中有一个链接转换的选项，不少朋友都问过这个功能有什么用？今天我们设计一个实验对这一功能加以说明。我们先来看看微软是怎么介绍链接转换的，微软是这么说的：“从已发布的 Web 服务器上发送回外部客户端的 Web 页可能会有包含内部主机名的链接。 由于外部客户端不能解析这些受保护主机的名称，因此这些链接会被阻断。同时，将内部主机名发送给外部客户端也会使这些名称暴露在潜在黑客的威胁下。为了解 决这些问题， ISA Server 中提供了一个 Web 过滤器，称为链接转换过 滤器。在启用此 Web 过滤器时，ISA 就会针对相应的 Web 发布规则根据一组默认规则或用户定义的词典（用于将包含内部主机名的字符串映射为包含可解析主机名的字符串）进行链接转换。”

看了上面一段介绍，您明白链接转换的作用了吗？其实很简单，我们发布的内网网站中可能有些页面的超链接使用了内网的计算机名，这些内网的计算机名无法被互联网上的用户解析，因此外网用户访问这些超链接时肯定会出错。链接转换的作用就是把内网的计算机名转换为能被外网用户识别的完全合格域名。那有些朋友可能会问，网站的设计者为什么不直接在超链接中使用完全合格域名呢，？还要用 ISA 来帮忙！其实有时候设计内网网站时，可能并没有考虑到以后要把它发布到公网上去，因此设计师无法超前地使用完全合格域名来表现一些超链接。微软考虑到这种情形不可避免，而且并非所有的公司遇到这种情况都愿意把网站代码重写一遍，因此特意在 ISA 中实现了链接转换功能。

今天我们的实验拓扑如下图所示，内网的 Perth 是被发布的 Web 服务器，Perth 上有些网页需要用到链接转换功能。

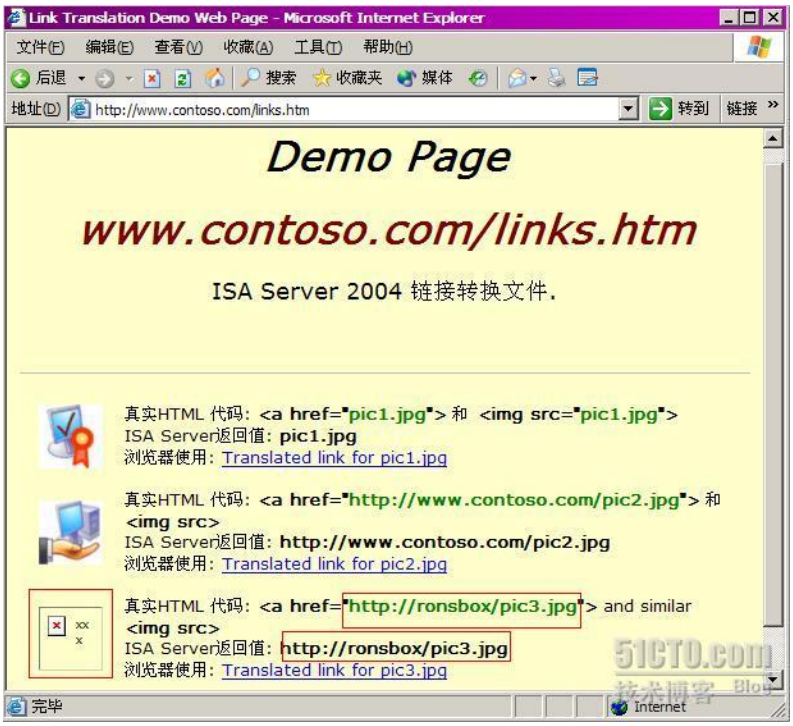


首先我们要把 Perth 上的 Web 站点通过 ISA 发布出来，具体方法请参考之前的博文，在此不再赘述。如下图所示，我们已经在 ISA 中创建了负责发布 Perth 的网站发布规则。

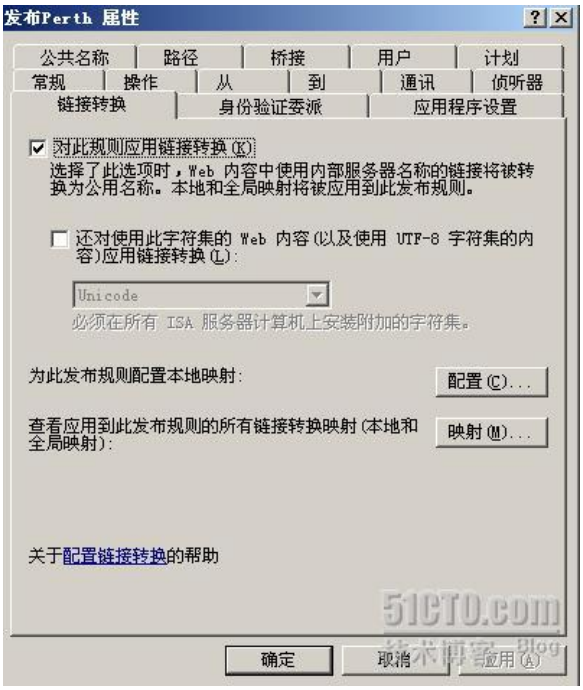
Perth 被发布到外网的公共名称是 www.contoso.com，如下图所示。

我们在外网的客户机 Istanbul 上测试一下发布结果，如下图所示，Perth 发布成功！

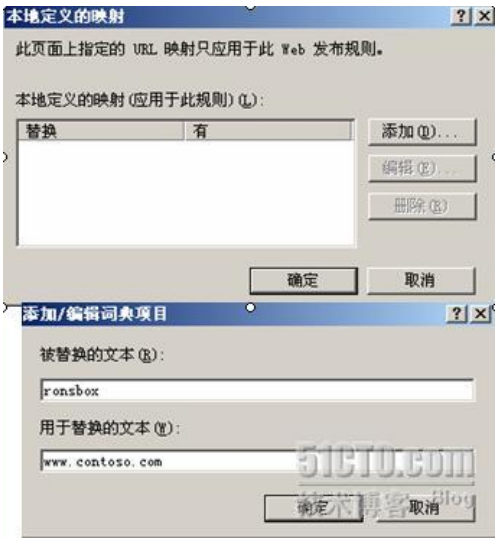
接下来我们来访问 Perth 上的一个链接转换 Demo 网页，这个网页源于微软的 ISA2004 实验室。如下图所示，我们发现网页中的第三幅图片没能正确显示，为什么呢？仔细看看，原来这幅图片的超链接是 http://ronsbox/pic3.jpg，ronsbox 是 perth 曾用过的计算机名，而且又是 netbios 名称格式。这样外网用户无法对计算机名 ronsbox 进行解析，自然更无法访问 ronsbox 上的文件了。



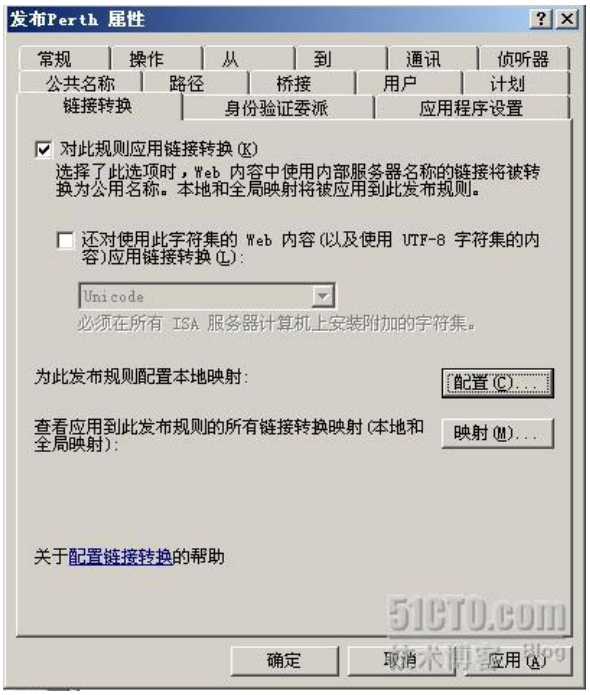
这时链接转换就可以出马了，我们只要用链接转换把计算机名 ronsbox 转换为 www.contoso.com 就万事大吉了。如下图所示，在 Perth 的发布规则中切换到“链接转换”标签，点击“配置”。



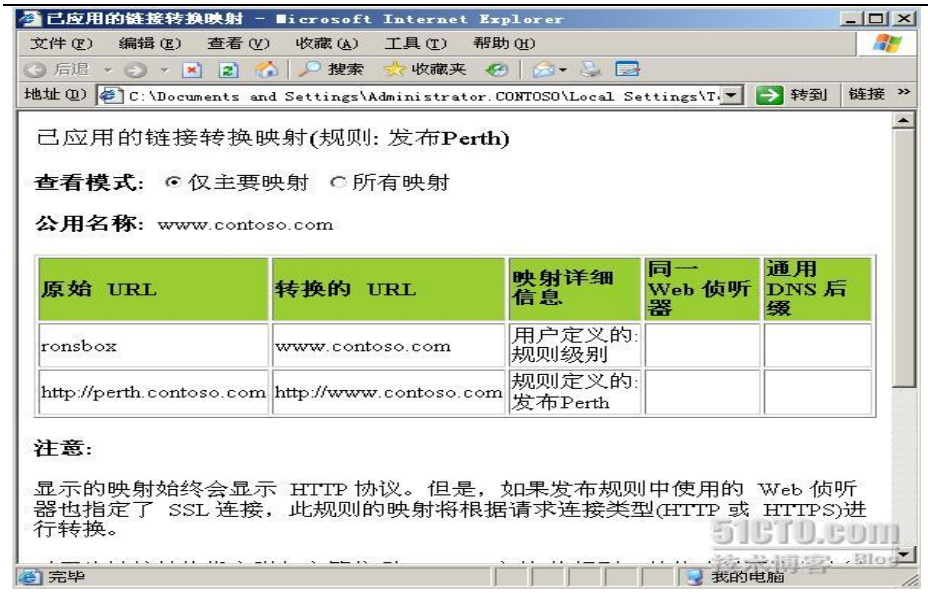
如下图所示，点击“添加”按钮来定义链接映射，我们把 ronsbox 转换为 www.contoso.com。



想查看定义了哪些链接转换可以在发布规则的链接转换标签中点击“映射”按钮，如下图所示。



链接转换的映射关系如下图所示，我们发现 ronsbox 被转换成了 www.contoso.com，这时我们定义的，不足为奇。可为什么还有一条从 perth.contoso.com 到 www.contoso.com 的映射关系呢？这是 ISA2006 自动添加的。我们在发布规则中将内网的 perth.contoso.com 发布到了外网，而且公共名称是 www.contoso.com，这时 ISA 会自动将 Perth 站点中 URL 包含的 perth.contoso.com 一律转换为 www.contoso.com。怎么样，ISA 还是很聪明的。



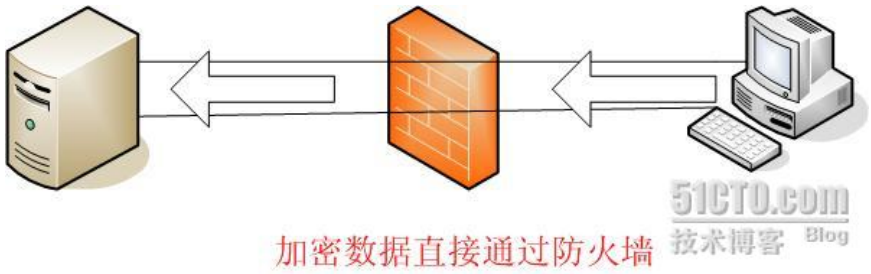
做完了链接转换，看看效果如何？如下图所示，第三幅图片终于露出了庐山真面目，链接转换起作用了。

链接转换是 ISA 中一个比较简单的功能，但在发布内网网站时非常实用，大家根据具体情况灵活使用链接转换，一定可以收到良好效果。

发布安全 Web 站点详细攻略:ISA2006 系列之十四

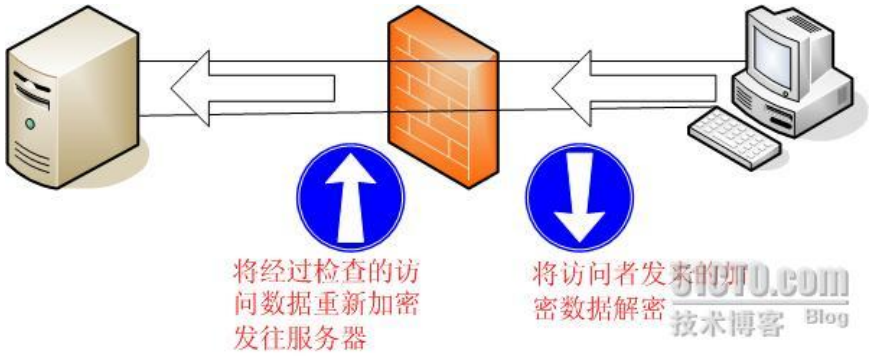
到目前为止，我们已经对 ISA 发布 Web 站点进行了很多介绍，但还没有涉及到安全 Web 站点。其实在很多领域，安全 Web 站点都由于高安全性而受到广泛应用，例如在电子商务，电子邮件，OA 等用用中基本都会使用安全站点来加强对数据的保护。既然安全站点如此重要，今天我们就来讨论一下如何用 ISA2006 来发布安全 Web 站点。

用 ISA2006 发布安全站点并不是一件困难的事，相反，ISA2006 为管理员发布安全站点提供了灵活且强大的技术支持。以往防火墙在发布安全 Web 站点时，处理方法并不令人满意。由于安全 Web 站点对 HTTP 数据进行了加密，这使得防火墙无法对数据内容进行分析，当然也没办法判断这些数据是否不利于安全。防火墙遇到这种情况，往往就采用“隧道”模式，如下图所示，“隧道”模式让外网的访问请求直接通过防火墙抵达内网的安全站点，防火墙对访问请求直接放行，透明通过。这种方法自然无法让管理员满意，买个防火墙发布网站不就是希望利用防火墙过滤有害数据嘛，现在防火墙让加密数据透明通过，那防火墙还有什么用呢，不如直接把安全网站放到外网好了。



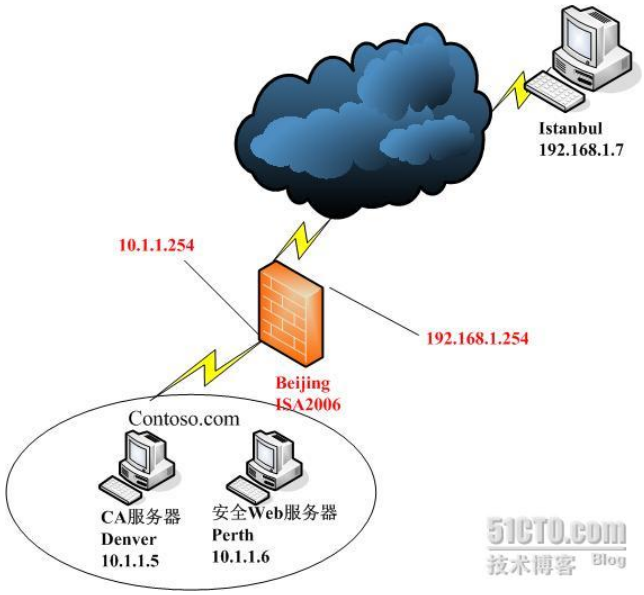
加密数据直接通过防火墙

ISA2006 对发布安全站点做了很好的改进，ISA2006 在发布安全站点时可以采用“桥接”模式，如下图所示，这种模式可以让 ISA 对外网的发来的加密数据先进行解密，然后过滤检查，发来的数据被证实没问题了才会被重新加密送往内网的 Web 服务器。显然，桥接模式比隧道模式更能发挥防火墙的功效，对网站的安全更为有利。



ISA 并不是随随便便就能启用桥接模式，发布安全 Web 站点和发布 Web 站点有所不同，区别就在于安全 Web 服务器必须提供证书用于数据加密。在桥接模式下，ISA 要对外网发来的加密的数据进行解密，这就要求 ISA 必须拥有证书及配套私钥。例如 ISA 发布的安全站点是 perth.contoso.com，那 ISA 必须拥有名为 perth.contoso.com 的证书以及配套的私钥，如果没有证书，ISA 无法对外网的访问者证明自己就是他们要访问的 perth.contoso.com，如果没有私钥，ISA 则无法对加密数据进行解密。因此，ISA 启用桥接模式发布安全网站的关键就在于如何让 ISA 拥有证书以及私钥，我们解决这个问题的方法是让安全 Web 服务器导出证书及私钥，然后 ISA 再进行导入操作。

实验拓扑如下图所示，Perth 是内网要发布的安全站点，Denver 是内网的域控制器兼 CA 服务器，Beijing 是 ISA2006 服务器，我们看看如何用 ISA 发布安全 Web 站点。



一 创建 CA 服务器

既然 Perth 上的 Web 站点是安全 Web 站点，那 Perth 的站点肯定要有证书，谁来发这个证书呢？CA！我们既可以选择去国际 CA 公司申请证书，也可以自己创建 CA 服务器来颁发证书。平时经常有朋友问这个问题：到底应该选择去国际 CA 申请证书还是自己创建一个 CA 来颁发呢？这个问题我觉得应该根据被发布安全站点的用途来决定，如果你发布的安全站点针对的群体是互联网上的用户，那我认为还是应该去国际 CA 申请证书，这样申请到的证书自动会被所有的用户所信任，使用起来很方便。否则你自己创建 CA 颁发证书，但互联网上其他用户都不信任，每个用户都要手工信任你创建的 CA，这样就很麻烦了。当然，去国际 CA 申请是要付出代价的，一年估计要 1W 多 RMB，这银子花得很心疼的。如果发布的安全站点主要是给公司员工使用的，那就可以自己创建 CA 来颁发证书了，因为公司员工人数有限，即使手工信 CA 任也不用花太多时间。这时自己创建的 CA 就能体现出使用方便，节省成本的优点了。

回到本例中，我们准备在 Denver 上创建一个 CA 服务器，用以在域内为计算机颁发证书。在 Denver 上依次点击 开始－设置－控制面板－添加或删除程序－添加/删除 Windows 组件，如下图所示，勾选“证书服务”，这时会弹出对话框提示你安装证书服务后不能改变计算机名称以及身份，选择“是“按钮。

CA 类型设置为企业根，这样可以更好地利用域的管理优势。

CA 命名为 TESTCA。

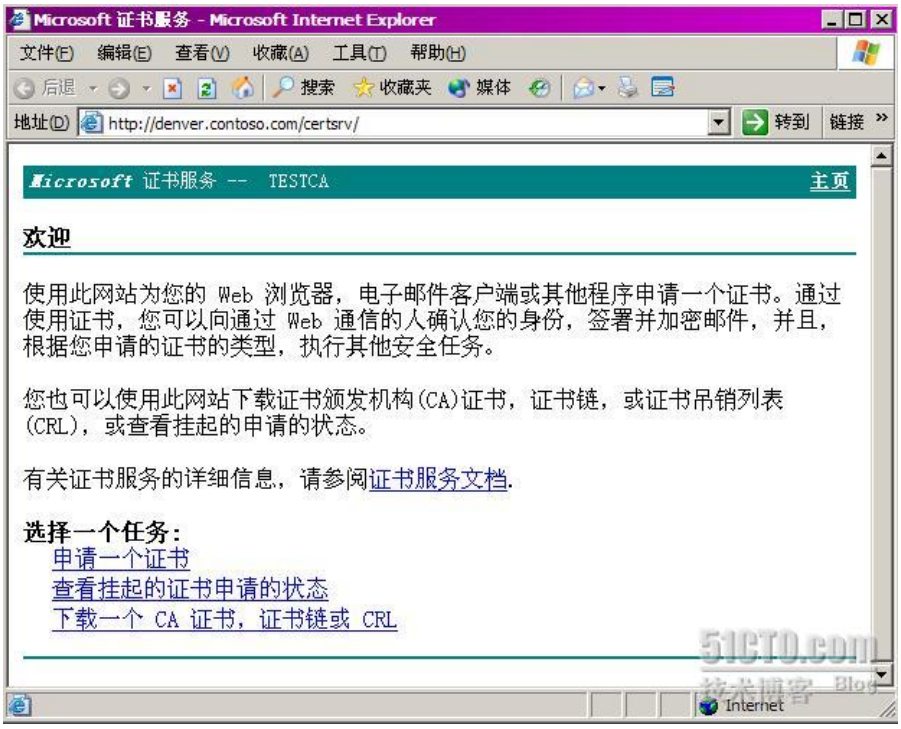
证书数据库的存储路径取默认值即可。

安装程序提示需要重启 IIS 服务，在插入 Win2003 的安装光盘后，如下图所示，安装结束。

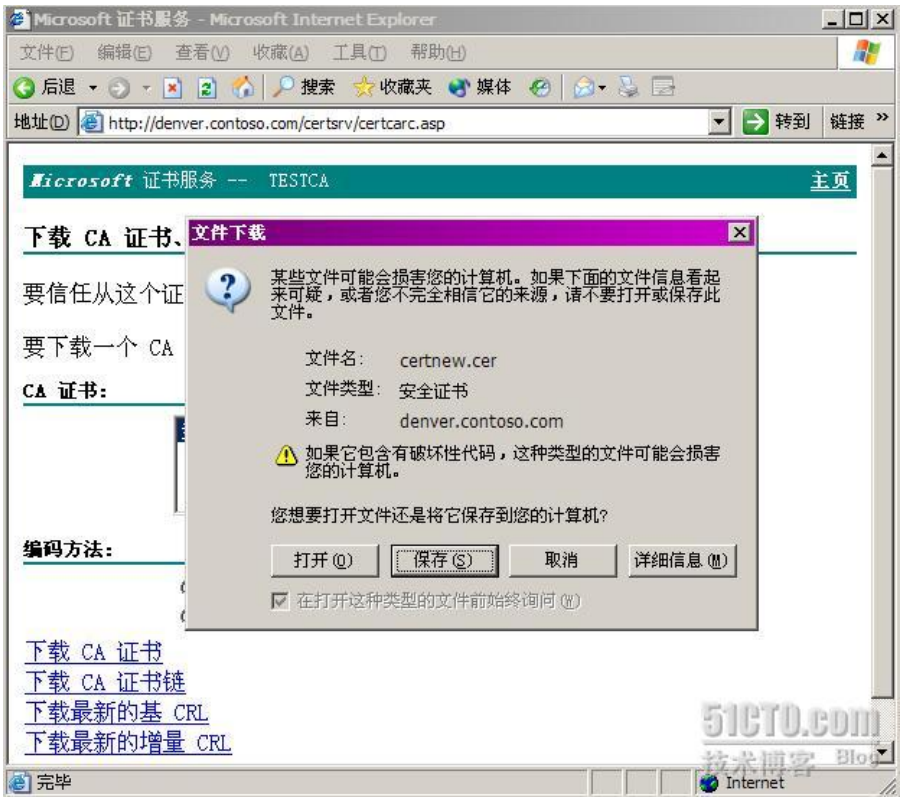
创建完 CA 服务器后，这个服务器必须得到其他计算机的认可，域内的计算机如本例中的 Perth 和 Beijing 都不用担心，组策略会告诉他们 TESTCA 是个可以信任的 CA 服务器。如果你觉得组策略生效时间太长，还可以运行 Gpupdate/force 来加快组策略生效时间。域外的计算机如本例中的 Istanbul 就需要手工信任这个 CA 服务器了，具体操作方法如下。我

们先把 Denver 的网站用 ISA 发布出来，然后在 Istanbul 上访问 http://denver.contoso.com /certsrv，如下图所示，网站要求进行身份验证，我们输入域管理员的用户名和口令。

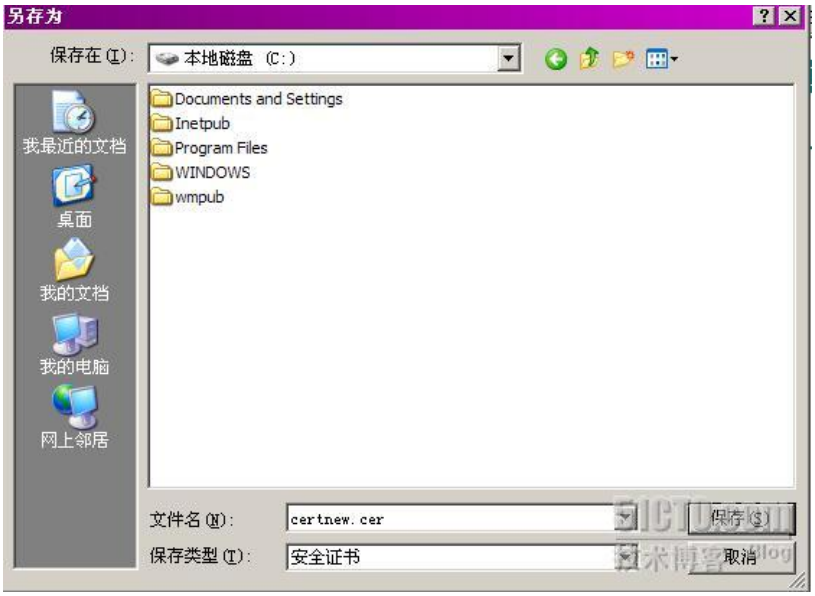
通过身份验证后我们可以通过网站访问 CA 服务器了，如下图所示，选择“下载一个 CA 证书，证书链或 CRL”。



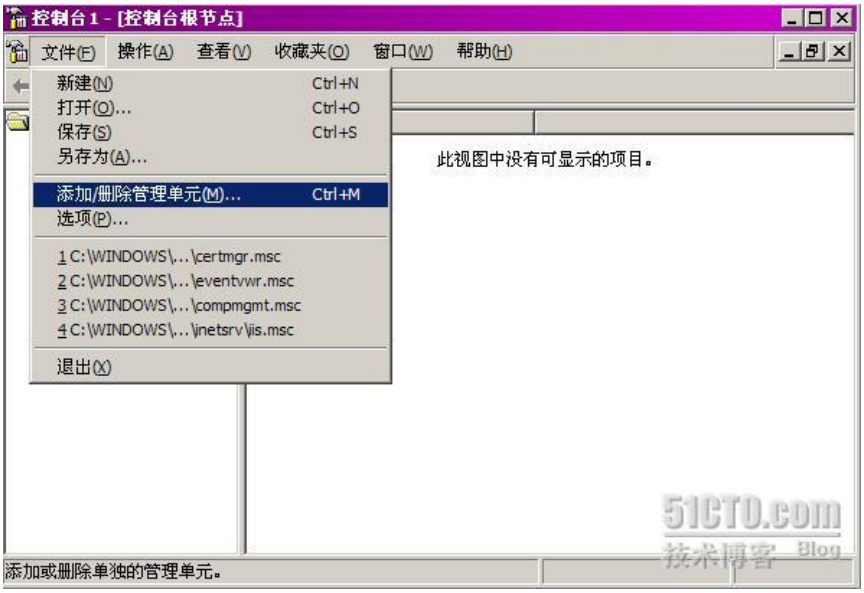
如下图所示，选择“下载 CA 证书”，网站弹出文件下载的对话框，选择“保存”。



把下载的 CA 根证书保存到 C:certnew.cert。

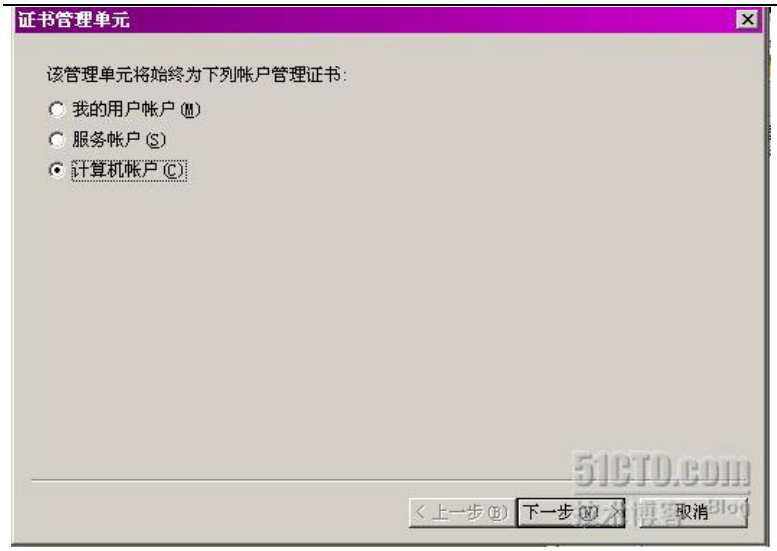


有了 CA 根证书之后，我们要把它手工导入被信任的根证书颁发机构中。在 Istanbul 上运行 mmc，如下图所示，在 mmc 控制台中选择“添加删除管理单元”。

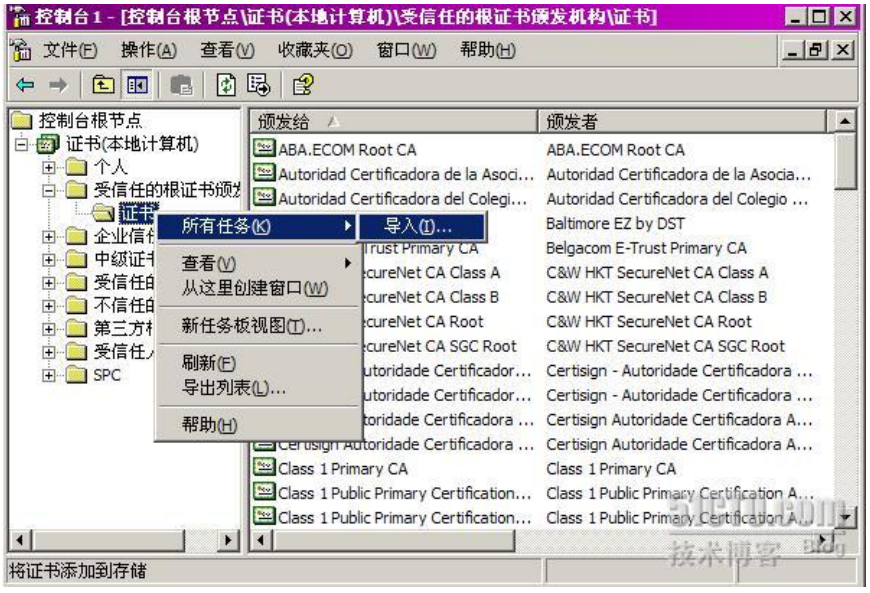


如下图所示，点击“添加”，选择添加“证书”管理单元。

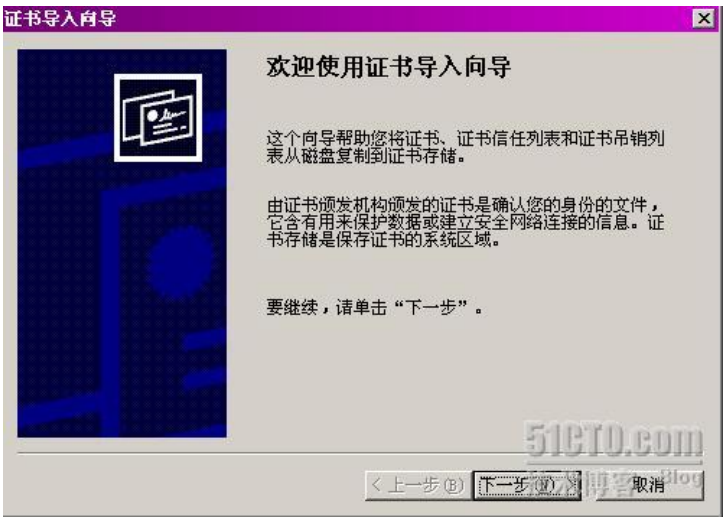
证书管理单元负责对计算机账号管理证书。



在新添加的证书管理单元中定位到“受信任的根证书颁发机构－证书”，如下图所示，在所有任务中选择“导入”。

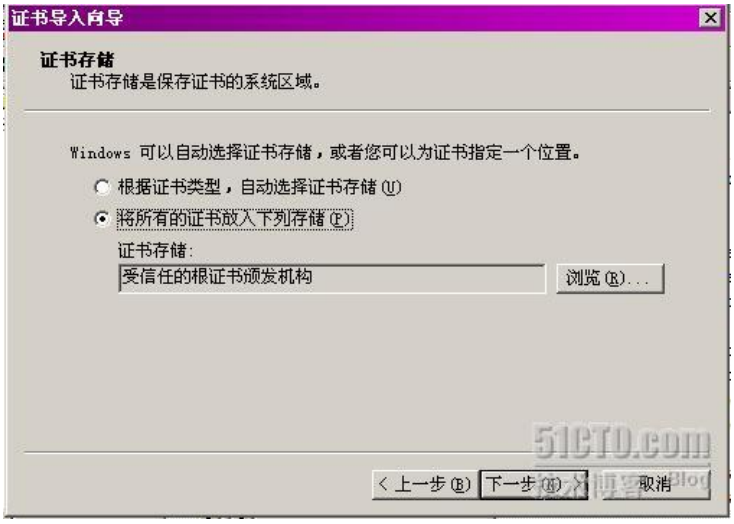


启动证书导入向导。

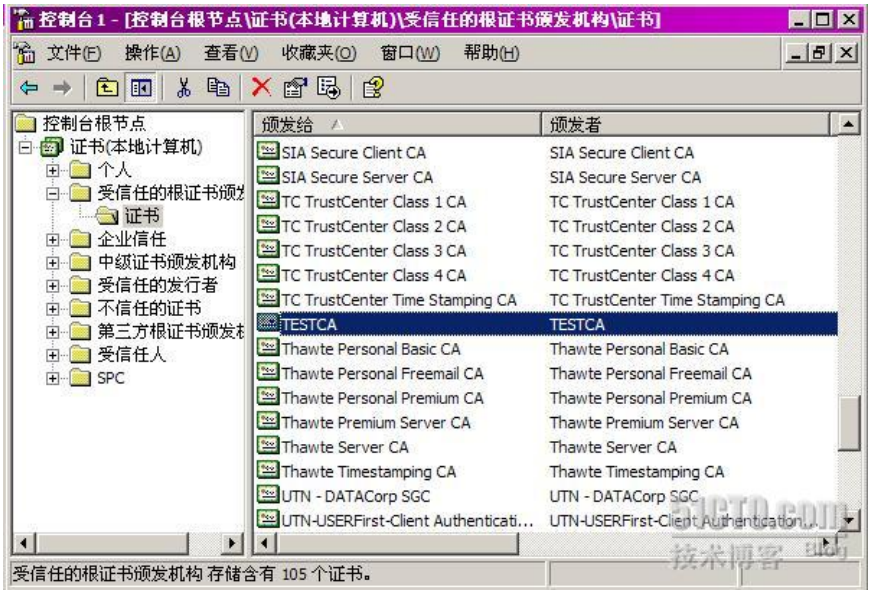


将 CA 根证书文件导入，如下图所示。

选择证书的存储区域。



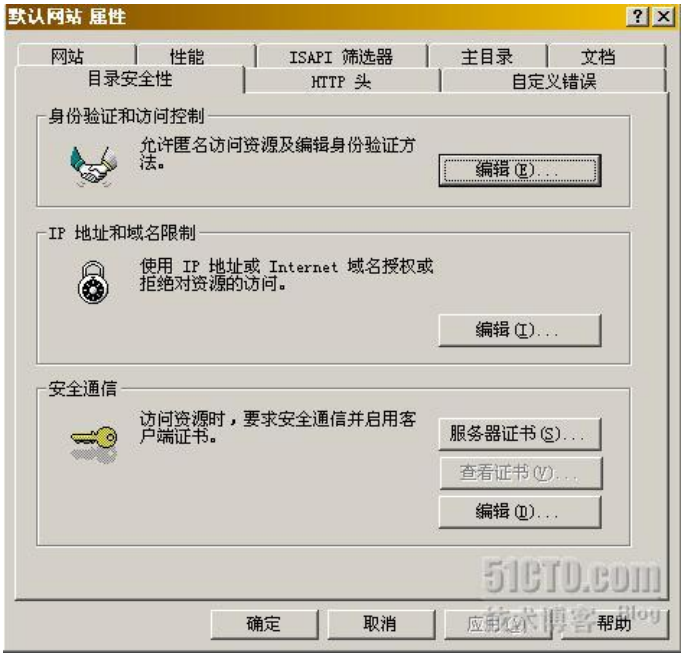
证书导入后，如下图所示，TESTCA 已经成了被 Istanbul 信任的根证书颁发机构。



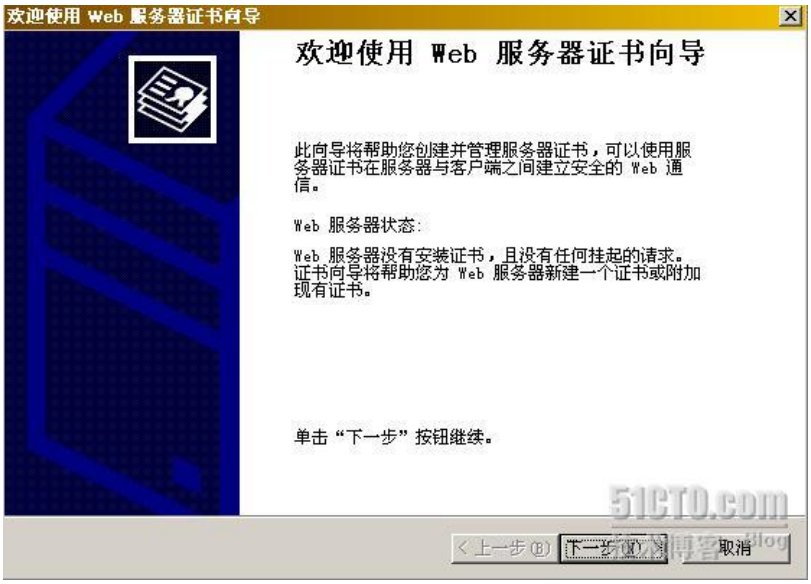
至此，我们完成了 CA 服务器的创建以及对 CA 服务器的信任，切记，所有访问安全 Web 站点的计算机都要信任证书颁发机构。

二 为安全 Web 站点申请证书

创建了 CA 服务器之后，我们就可以为 Perth 的 Web 站点申请证书了。在 Perth 的 IIS 管理器中查看默认站点的属性，如下图所示，切换到站点属性的“目录安全性”标签，点击“服务器证书”。



弹出服务器证书申请向导。



选择“新建证书”。

由于之前创建的 CA 类型是企业根，因此我们可以直接在线申请证书。

证书的名称和加密位数取默认值即可。

单位和部门参数也不重要。

证书的公用名称至关重要，公用名称一定要和外网用户访问此安全网站时所使用的域名完全匹配。如果不匹配，安全 Web 站点将发布失败。

填写证书的地理信息。

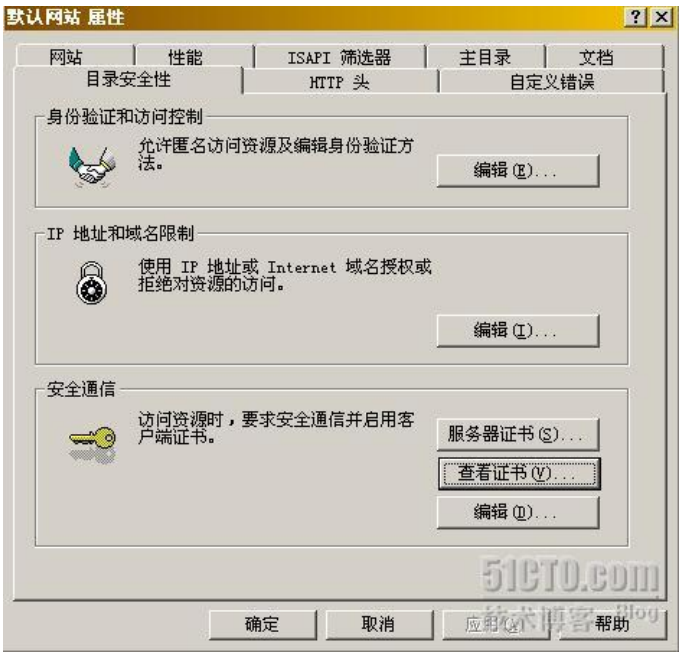
安全 Web 站点使用默认的 443 端口。

从 Active Directory 中选择所使用的证书颁发机构。

证书申请完成，CA 已经给 Perth 的 Web 站点颁发了证书，现在 Perth 已经是一个安全 Web 站点了。

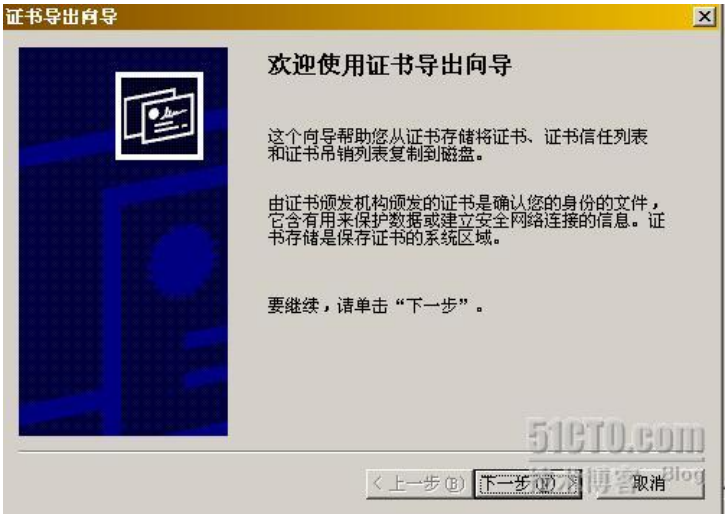
三 导出证书

接下来我们要在 Perth 上把申请到的证书导出给文件，然后再让 ISA 服务器导入。在 Perth 的 IIS 管理器中切换到默认 Web 站点的“目录安全性”标签，如下图所示，点击“查看证书”。

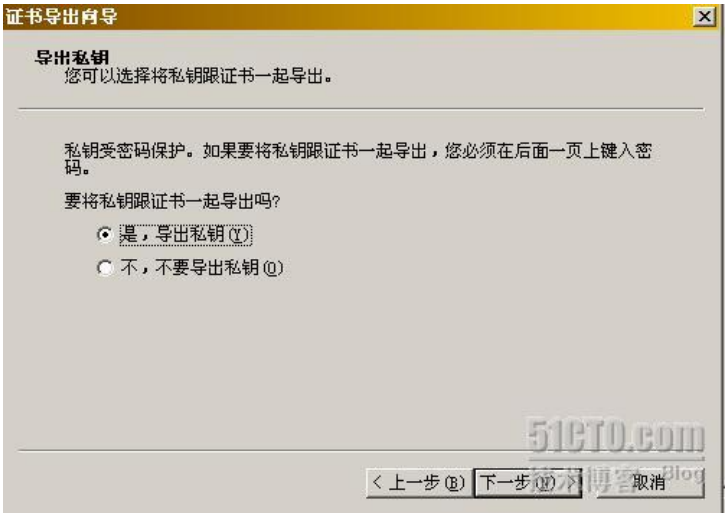


切换到证书的“详细信息”属性，如下图所示，点击“复制到文件”。

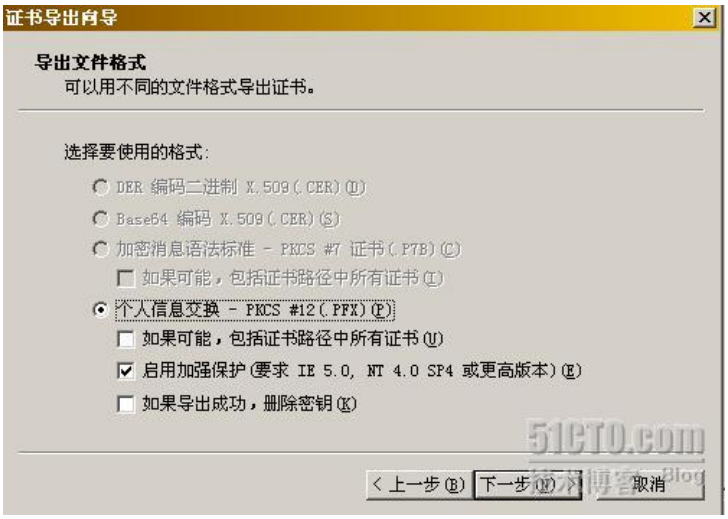
出现证书导出向导。



一定要连同私钥一起导出。



导出为 pfx 格式文件。

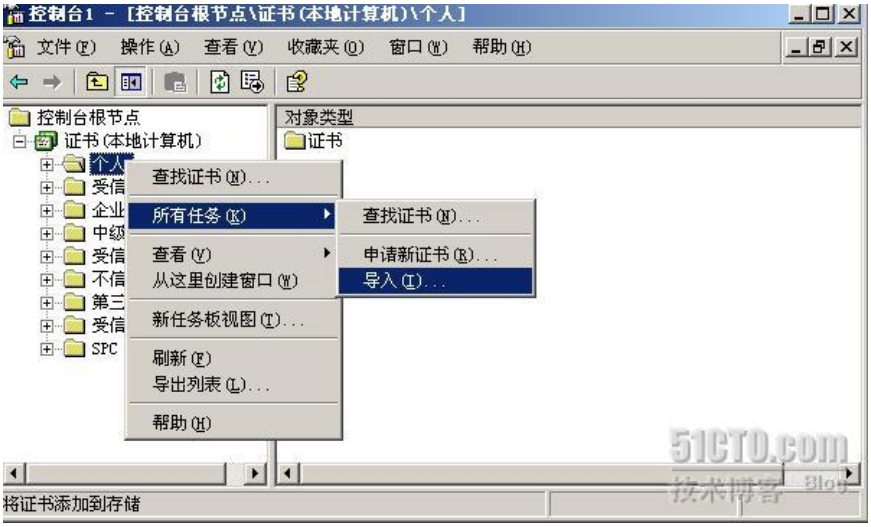


输入私钥保护密码。

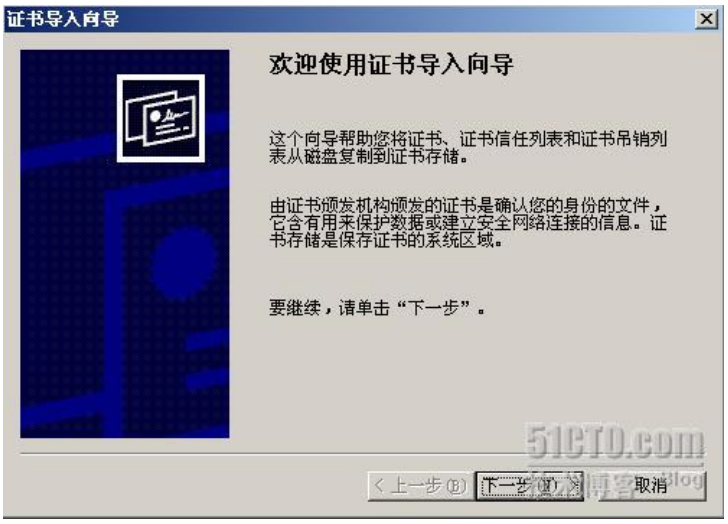
把证书及私钥导出为 c:perth.pfx。

四 导入证书

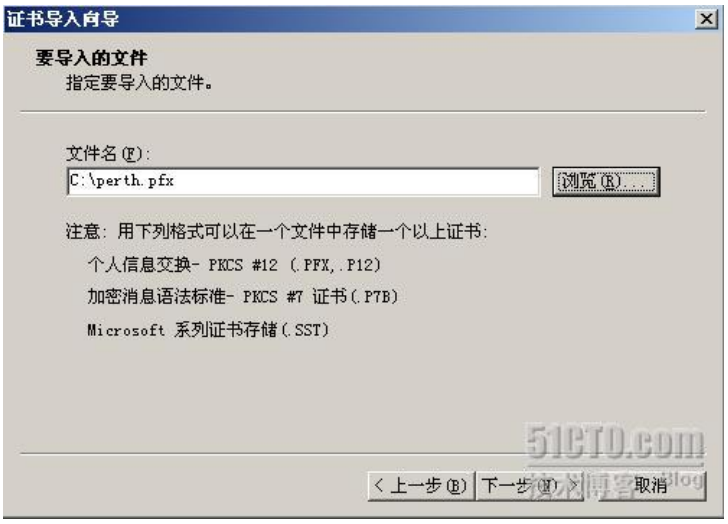
我们把 perth 导出的证书文件复制到 ISA 服务器上，然后 ISA 就可以进行证书的导入操作了。参考在 Istanbul 上用 mmc 创建证书管理单元的步骤，在 ISA 上也创建一个证书管理单元管理计算机账号的证书，如下图所示，右键单击“个人”容器，在所有任务中选择“导入”。



出现证书导入向导。

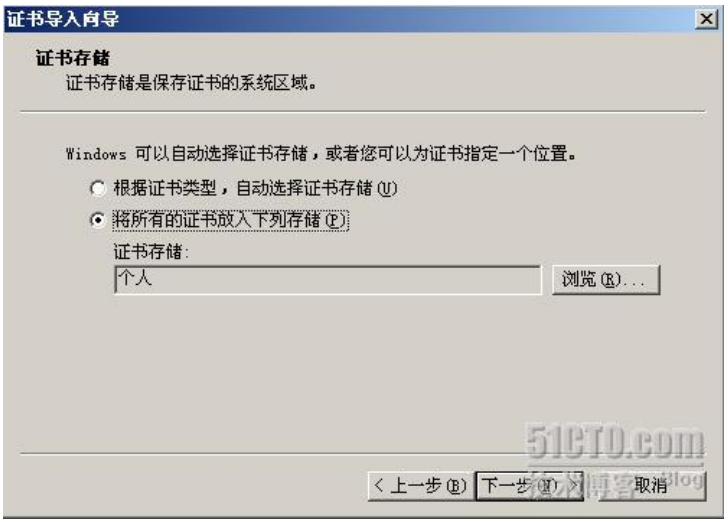


选择导入 perth.pfx 文件。



输入 pfx 文件中的私钥保护口令。

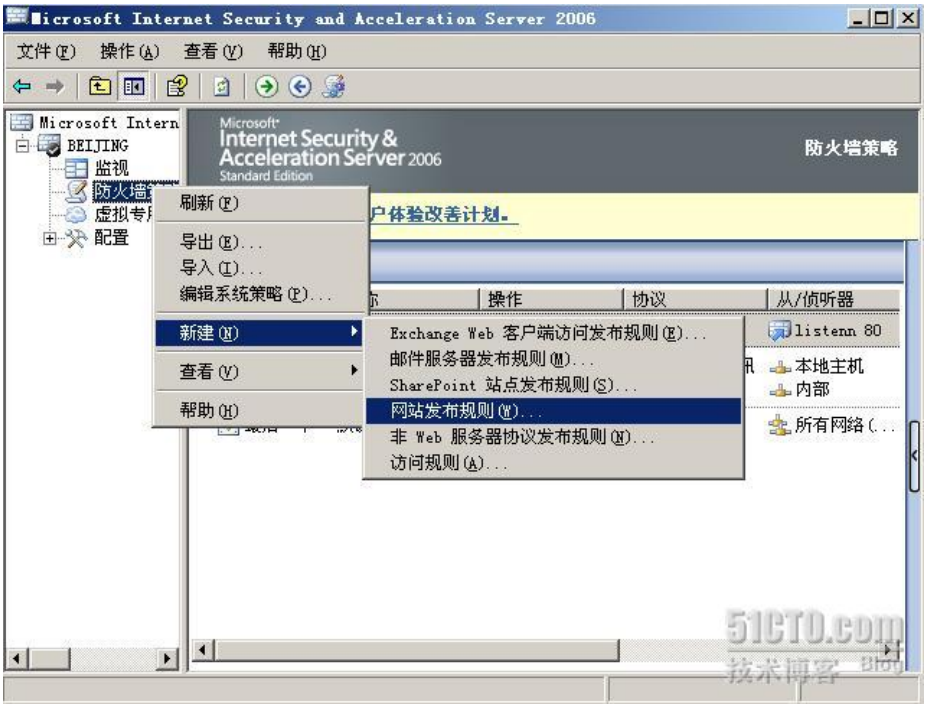
将导入的证书放到个人存储中。



如下图所示，导入成功，ISA 服务器上有了 perth.contoso.com 的证书以及相关私钥。

五 创建安全 Web 站点发布规则

万事俱备，只欠东风。我们现在可以在 ISA 服务器上发布 Perth 上的安全 Web 站点了。如下图所示，在 ISA 服务器管理器中选择新建“网站发布规则”。



为发布规则取名。

访问请求满足规则要求 ISA 则允许访问。

发布类型为发布单个网站。

使用 SSL 加密 ISA 与安全 Web 站点之间的数据。

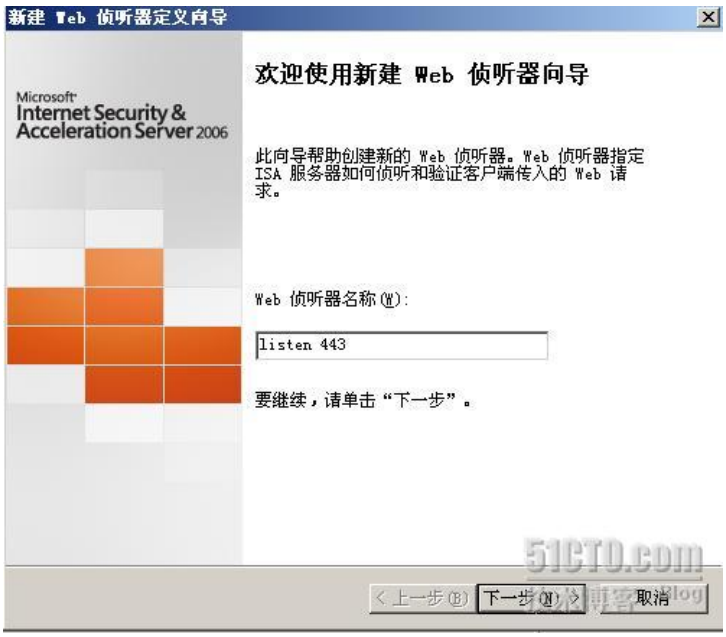
内部站点的名称为 perth.contoso.com，注意，内部站点的名称应该和安全站点证书中的公用名称完全一致，否则会导致发布失败。

从根目录开始发布整个网站。

安全站点的公共名称也应该和证书中的公用名称完全一致。

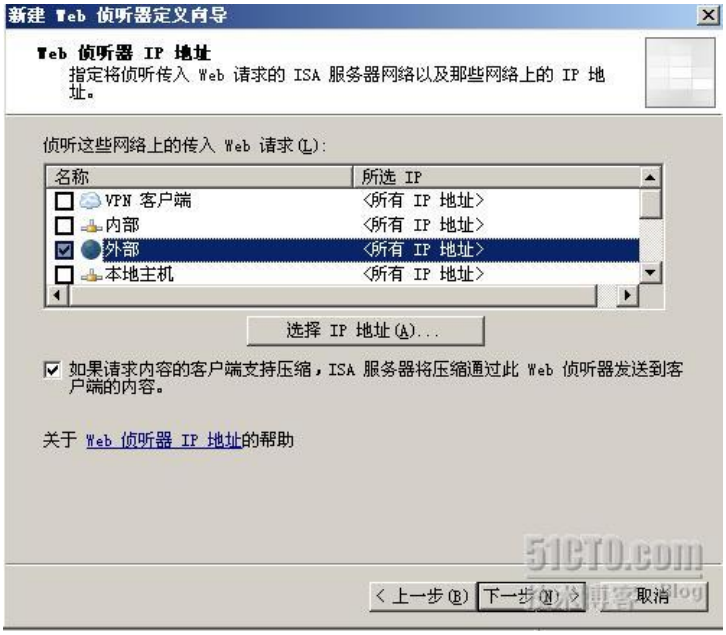
由于没有监听 443 端口的侦听器，因此我们选择“新建”。

出现 Web 侦听器创建向导，我们为新创建的 Web 侦听器取个名字。



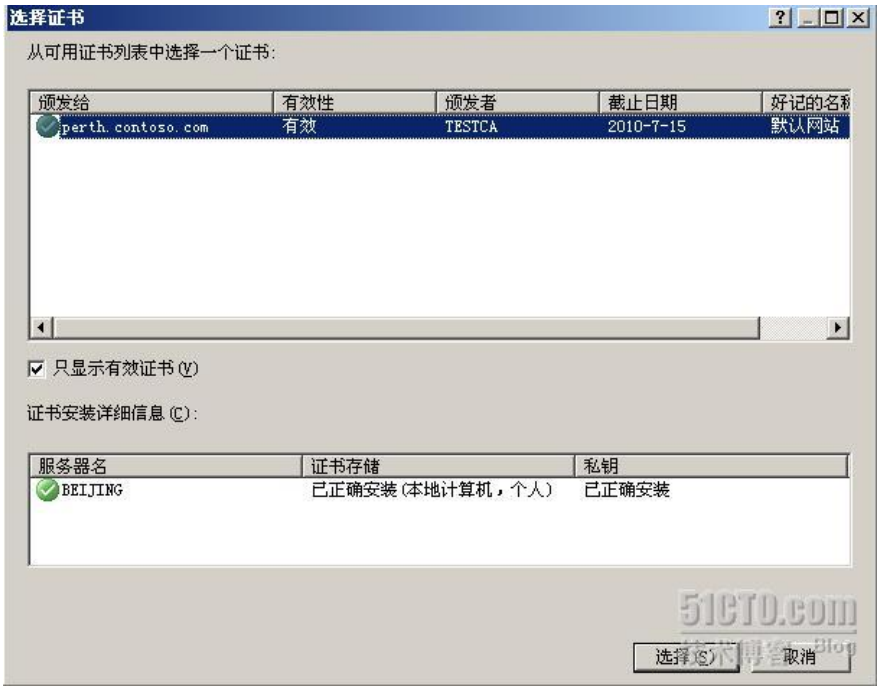
侦听器与外网访问者之间的数据需要用 SSL 加密。

侦听器对外网进行监听。



由于侦听器需要对外网访问者的数据进行加密，因此侦听器需要提供证书，如下图所示，点击“选择证书”。

在侦听器中选择使用导入的 perth.contoso.com 证书，这样外网访问者才会相信 ISA 服务器就是他们要访问的 perth.contoso.com。



侦听器选择证书之后，继续下一步。

本例中发布的安全 Web 站点不需要用户进行身份验证，发布其他的安全 Web 站点就未必不需要身份验证了，例如发布 Exchange 就需要进行身份验证。

本例中不需要设置单点登录。

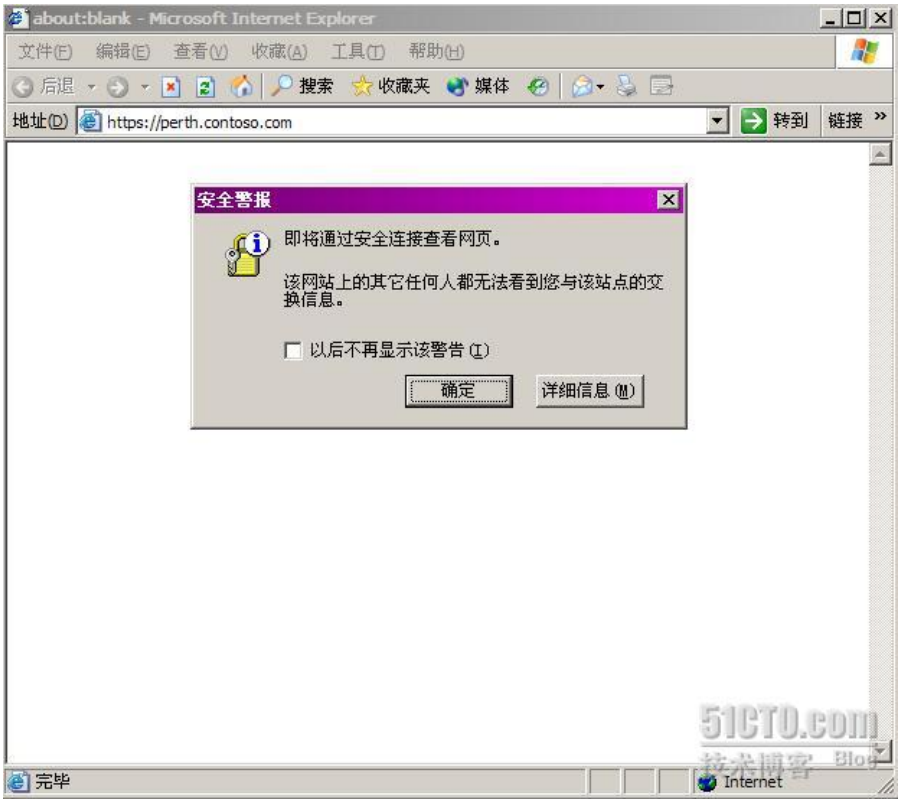
在发布规则中使用新创建的 Web 侦听器。

安全 Web 站点没有委派 ISA 对客户端进行身份验证。

此规则适用于所有用户。

完成安全 Web 站点发布规则，呵呵，终于结束了。

好了，一切都就绪了，我们在 Istanbul 上测试一下，如下图所示，在 Istanbul 上访问 https://perth.contoso.com，系统弹出对话框提示即将通过安全连接查看网页。



访问结果正常，OK，发布安全 Web 站点成功！

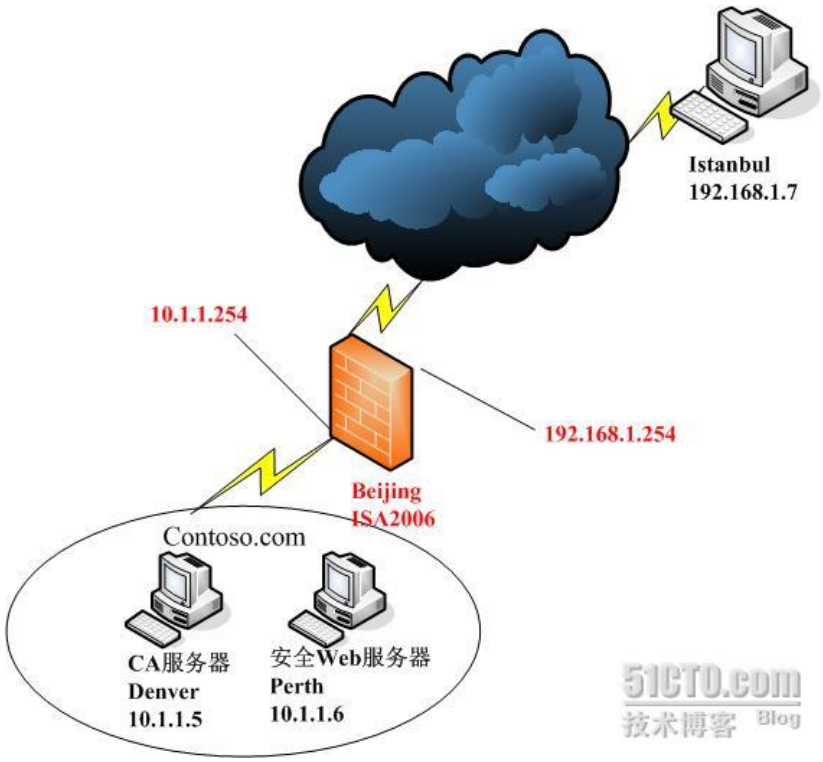
发布安全 Web 站点时问题基本都处在证书上，要么是证书的公用名称写得不对，要么导出证书的格式有问题，要么有些计算机不信任证书颁发机构等等，如果能先理解证书原理，那发布安全 Web 站点时就可以事半功倍了。

妙用通配符证书发布多个安全 Web 站点：ISA2006 系列之十五

在上一篇博文中，我们介绍了如何利用 ISA2006 发布内网的安全 Web 站点，想必大家已经能用 ISA 在内网中发布一个安全站点了。今天我们把难度加大一些，要求在内网发布多个安全站点时。有的朋友可能一听到这儿就很不以为然，发布多个 Web 站点是很简单的事情嘛，干嘛搞得神秘兮兮的。注意，我们要发布的不是 Web 站点，而是安全 Web 站点！发布安全 Web 站点时侦听器需要用证书向访问者提供身份证明，问题就在这里，当发布多个安全 Web 站点时，侦听器上到底应该使用什么样的证书呢？

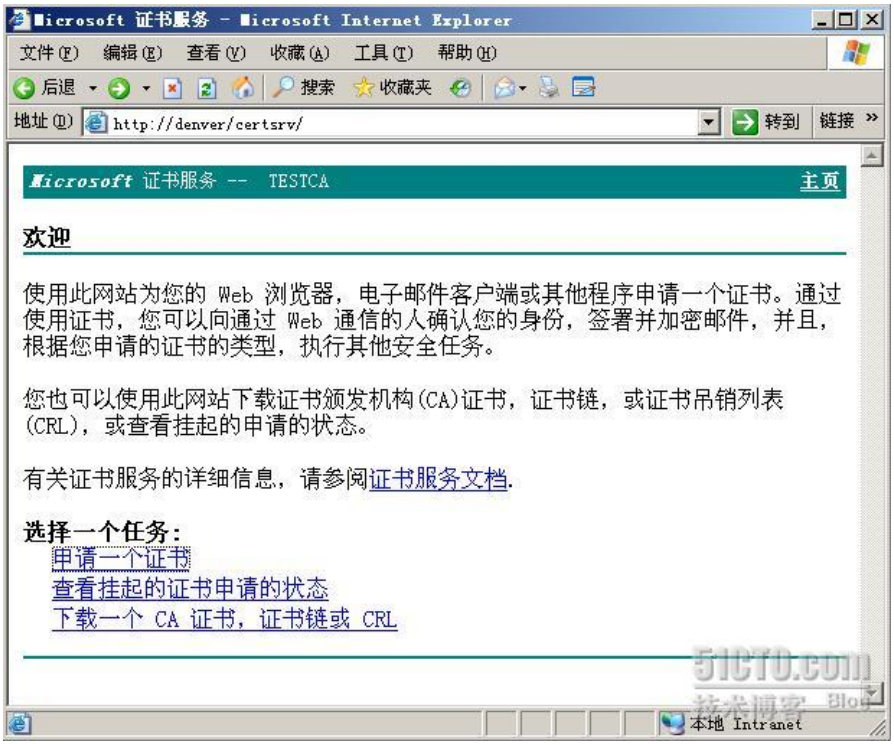
例如在下图的拓扑中，我们要在 ISA 上发布两个安全 Web 站点，一个是 Denver 上的 denver.contoso.com，另一个是 Perth 上的 perth.contoso.com。我们在 ISA 侦听器上使用

的证书，既要能向访问者证明自己是 denver.contoso.com，又要能证明自己是 perth.contoso.com。什么样的证书才能满足这样的要求呢？通配符证书！通配符证书利用通配符的模糊匹配特性可以和多个 Web 站点匹配，例如 *.contoso.com 就能同时匹配 denver.contoso.com 和 perth.contoso.com。因此，我们只要在侦听器中使用通配符证书，再针对每个安全 Weh 站点创建相应的发布规则，发布多个安全 Web 站点的问题就解决了。

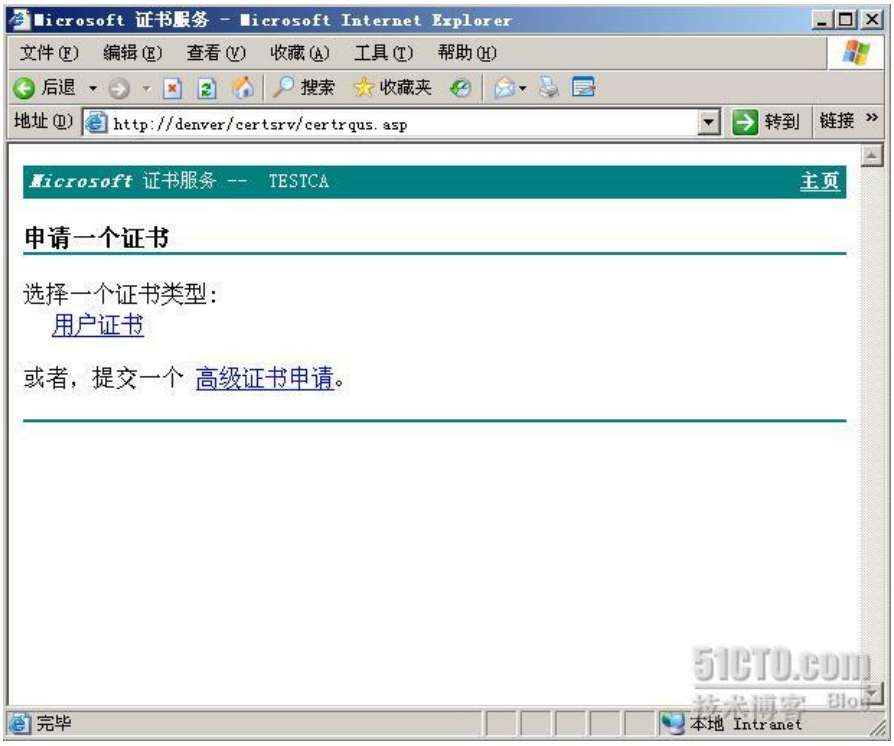


一 申请通配符证书

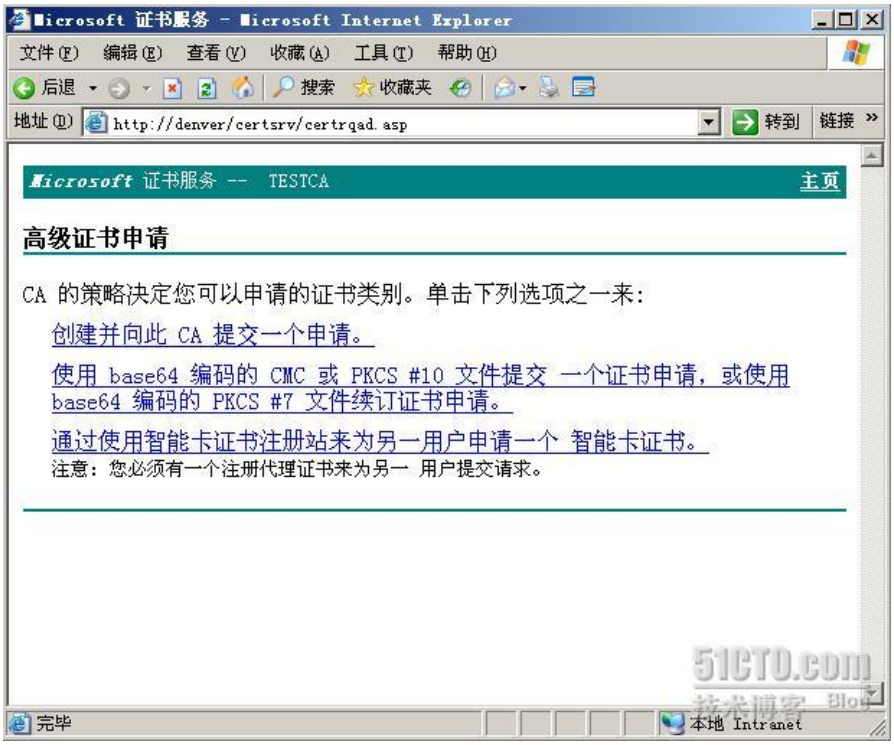
我们仍然利用上篇博文中的实验环境，由于 ISA 服务器加入了域，我们可以在 ISA 服务器上直接申请通配符证书，在 ISA 服务器上用浏览器访问 http://denver/certsrv，如下图所示，选择“申请一个证书”。



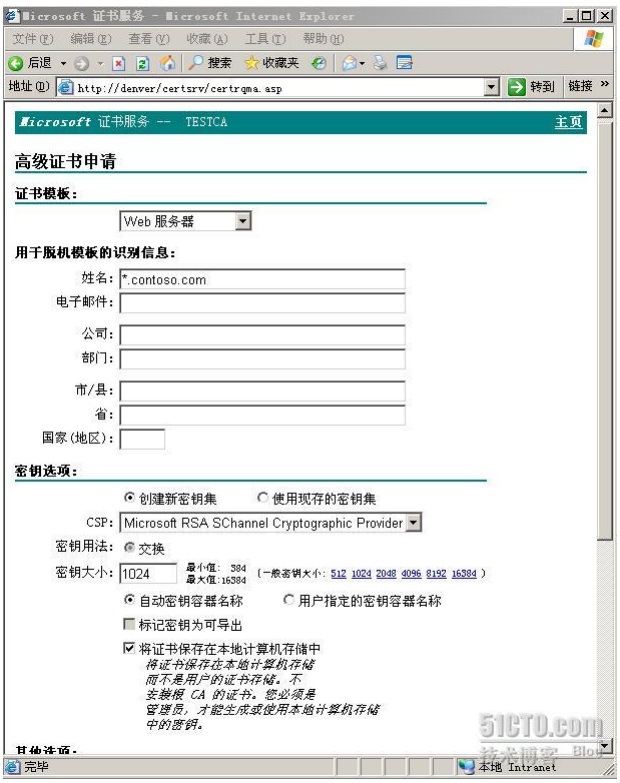
选择“提交一个高级证书申请”，准备申请服务器证书。



选择“创建并向此 CA 提交一个申请”，准备手工输入证书参数。

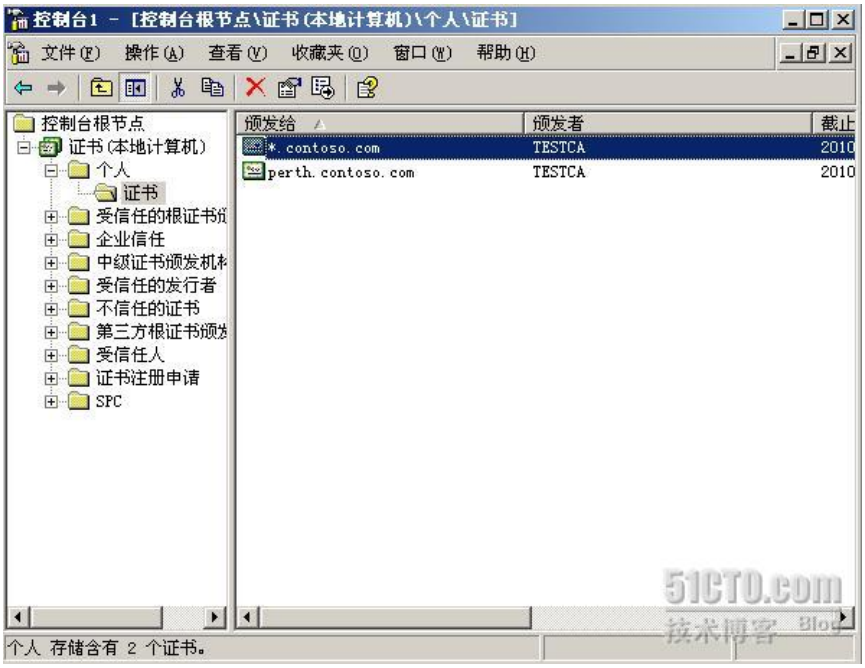


申请证书时，如下图所示，模板选择“Web 服务器”，姓名填写“*.contoso.com”，勾选“将证书保存在本机计算机存储中”。注意，姓名是关键参数。



由于 CA 服务器的类型是企业根，因此申请的证书被自动颁发了，如下图所示，我们选择“安装此证书”。

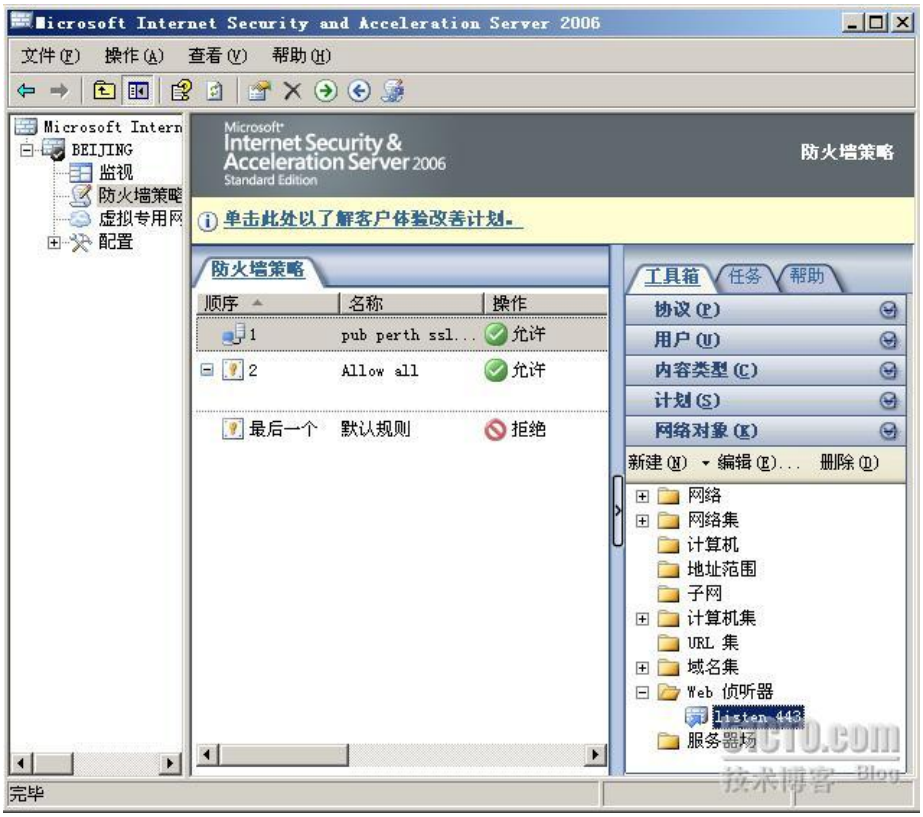
安装完证书后，如下图所示，我们在 ISA 的计算机存储中已经看到了颁发的通配符证书。



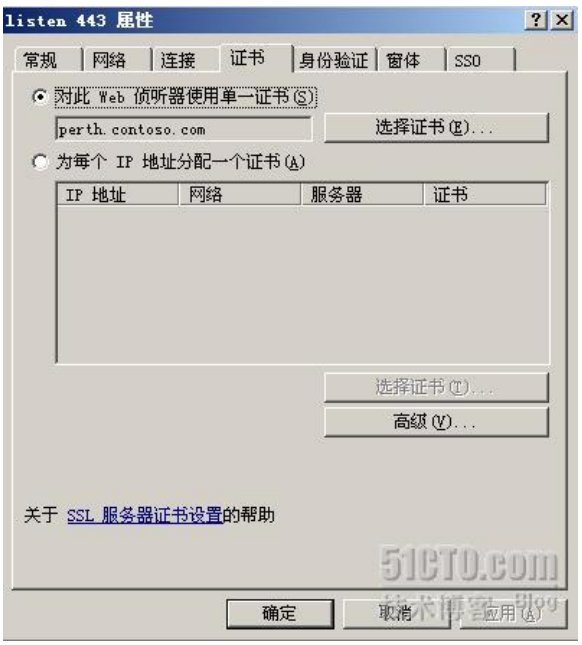
二 修改 Web 侦听器

如下图所示。在上篇博文中我们发布了 perth 上的安全 Web 站点，Web 侦听器使用的证书也是由 perth 导出的，现在我们要修改 Web 侦听器使用的证书，让侦听器使用通配符证书。

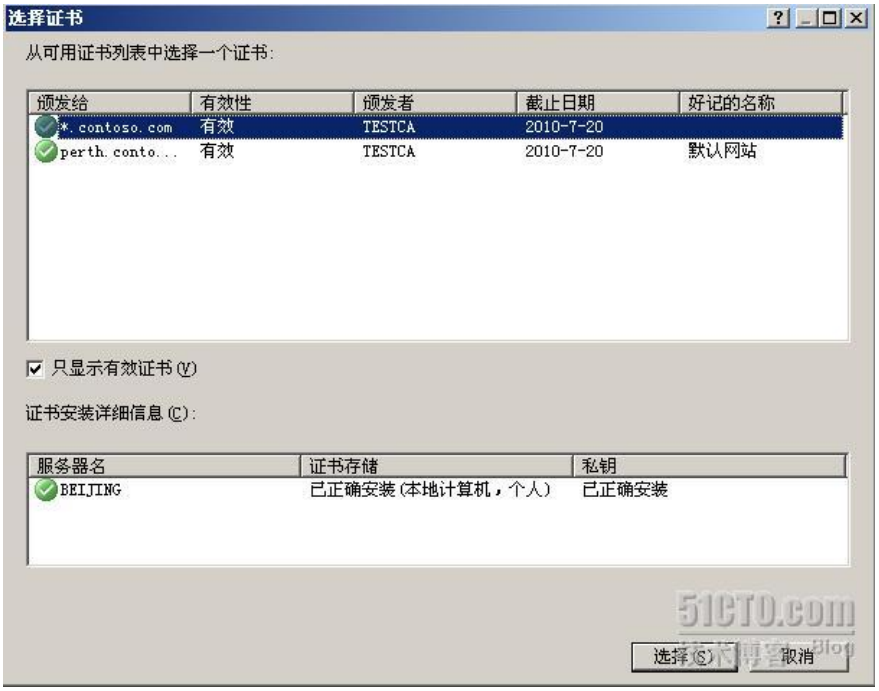
如下图所示，在防火墙策略工具箱中找到 Web 侦听器“Listen 443”，双击侦听器。



在侦听器属性中切换到“证书”标签，如下图所示，现在侦听器上使用的证书是 perth.contoso.com，点击“选择证书”。



如下图所示，选择使用*.contoso.com 的通配符证书。



OK，Web 侦听器修改完成。

三 修改发布规则

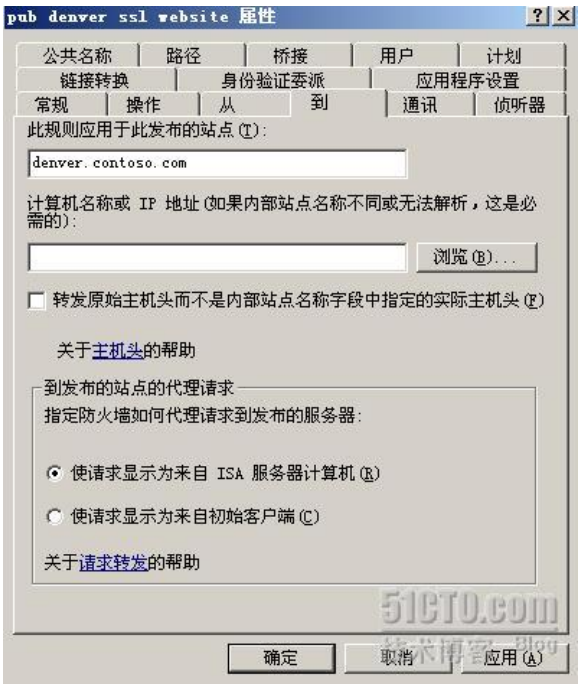
现在 ISA 服务器中有一条发布规则用来发布 Perth 上的安全站点，这条发布规则的 Web 侦听器使用了通配符证书，我们利用这条规则复制出一条新的发布规则，再稍加修改就可以用于发布 Denver 上的安全站点了。如下图所示，右键点击防火墙策略，选择“复制”。

复制完规则后，选择“粘贴”。

如下图所示，复制后的规则如下图所示，我们编辑发布规则“pub perth ssl website（1）”。

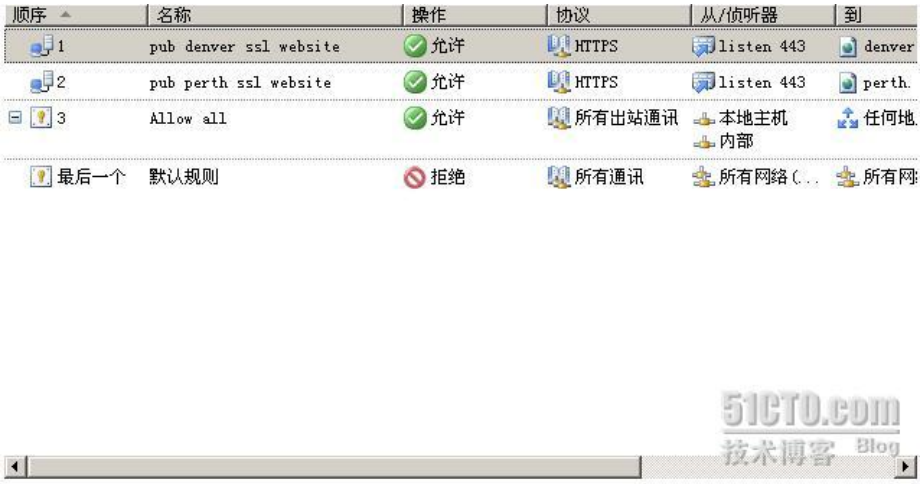
在发布规则属性中切换到“常规”标签，将名称改为“pub denver ssl website”。

切换至发布规则的“到”标签，在发布站点处填写“denver.contoso.com”。



切换到发布规则的“公共名称”标签，如下图所示，将公共名称从 perth.contoso.com 改为 denver.contoso.com。

修改后的发布规则如下图所示，现在我们有两条发布规则分别用于发布 denver 和 perth 上的安全站点。



四 测试

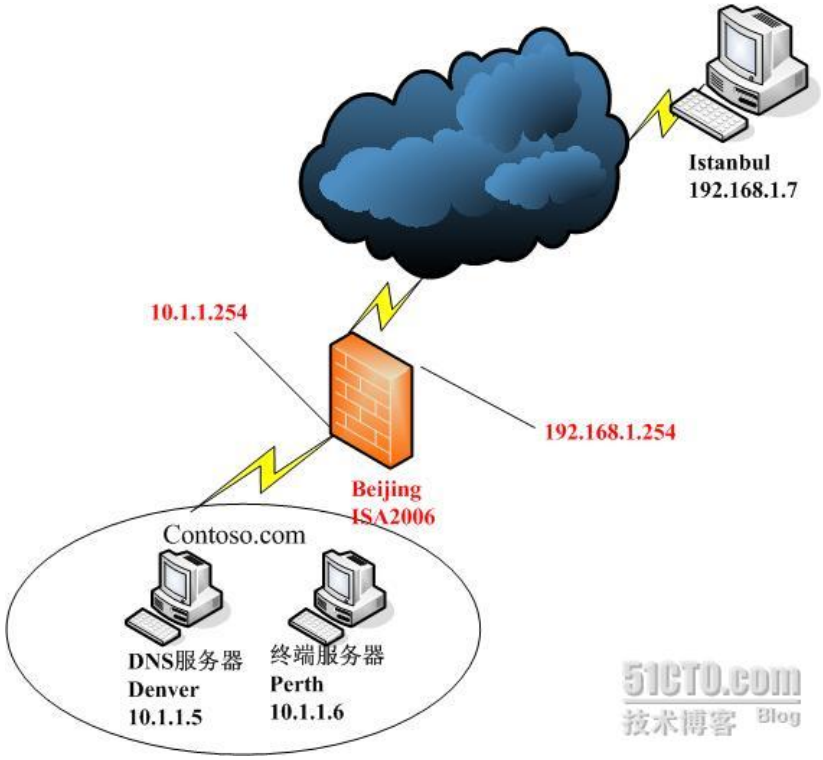
最后，我们在 Istanbul 上进行测试，首先访问 denver 上的安全站点，如下图所示，访问正常。

再来访问 perth 上的安全站点，仍然正常，OK，利用通配符发布多个安全站点成功了！

发布多个安全 Web 站点除了使用通配符证书，还可以考虑使用多个 Web 侦听器，每个侦听器守护不同端口，只是这样一来势必访问某些安全站点时就不能在标准的 443 端口了，可能会给访问者带来麻烦。如果 ISA 的外网网卡帮定了多个 IP，也可以在每个 IP 上绑定不同的证书。总之，希望大家在发布多个安全发布站点时，因地制宜，找出最适合自己的解决方法。

探讨防火墙内核监听模式：ISA2006 系列之十六

在前面的一系列博文中我们已经介绍了很多发布 Web 站点的内容，今天我们来发布一些其他的服务器，然后再来探讨一下发布这些服务器和发布 Web 站点有什么区别。我们先举两个例子，发布内网的 DNS 服务器和终端服务器，拓扑如下图所示，Perth 是要发布的终端服务器服务器，Denver 是要发布的 DNS 服务器。



首先我们来发布 Perth 上的终端服务器，在 ISA 服务器上右键点击防火墙策略，如下图所示，选择新建“非 Web 服务器协议发布规则”。

为发布规则取名为“发布 Perth 上的终端服务器”。

终端服务器 Perth 的 IP 为 10.1.1.6。

选择使用的发布协议，注意，发布规则使用的协议方向都是入站，而访问规则使用的协议方向都是出站。

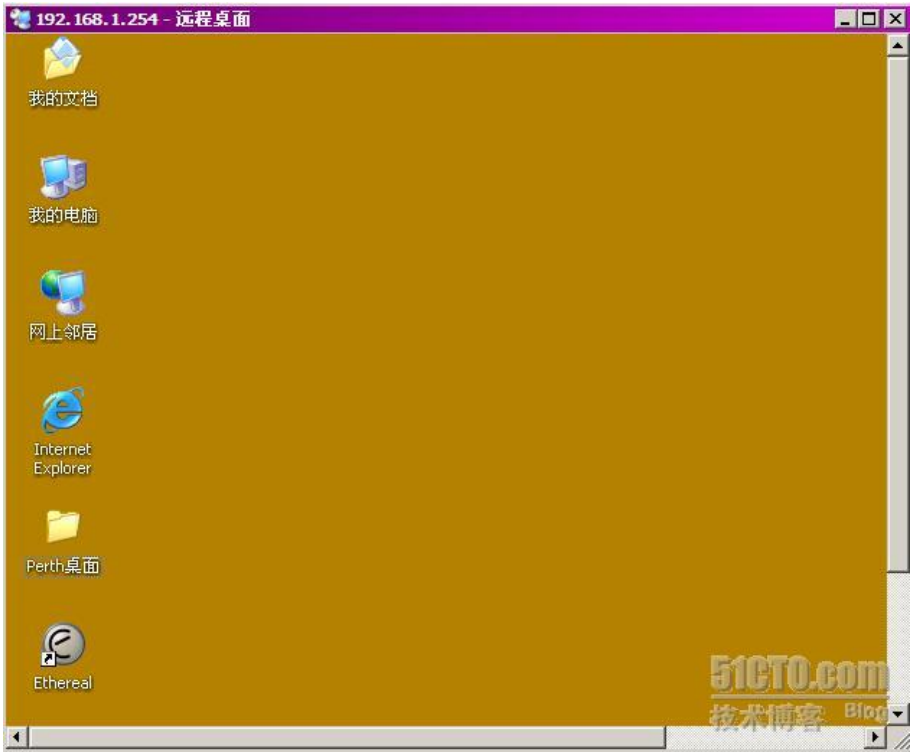
监听外网的访问请求。

完成服务器发布规则向导。

终端服务器发布规则生效之后，我们在外网客户机 Istanbul 上测试一下。在 Istanbul 上依次点击 开始－程序－附件－通讯－远程桌面连接，如下图所示，填入 ISA 服务器外网 IP 作为要连接的远程桌面服务器。

出现远程桌面的连接界面，如下图所示，输入用户名和口令登录系统。

OK，我们用远程桌面登录进入了 Perth，发布终端服务器成功了！



这个实验很简单，我们再来尝试一下发布内网的 DNS 服务器，如下图所示，在 ISA 服务器上新建“非 Web 服务器协议发布规则”。

为发布规则取名为“发布 Denver 上的 DNS 服务器”。

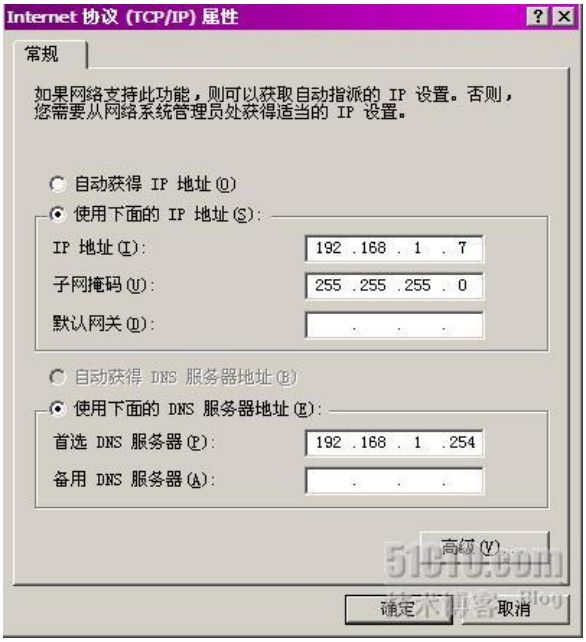
填入 DNS 服务器地址 10.1.1.5。

这次使用的发布协议是 DNS 服务器。

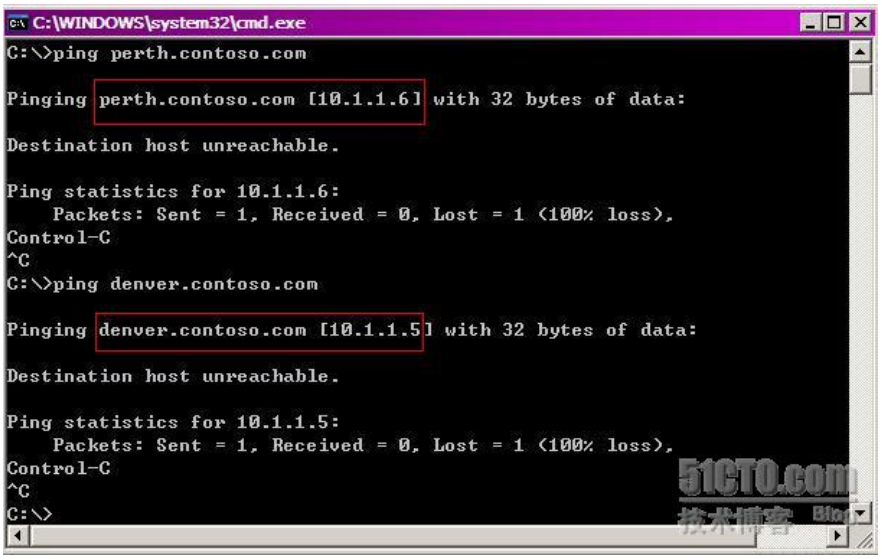
监听外网的访问请求。

结束发布规则。

好了，我们还是在 Istanbul 上测试一下发布的效果，如下图所示，Istanbul 已经在 TCP/IP 的设置中将 DNS 服务器指向了 ISA 的外网网卡。



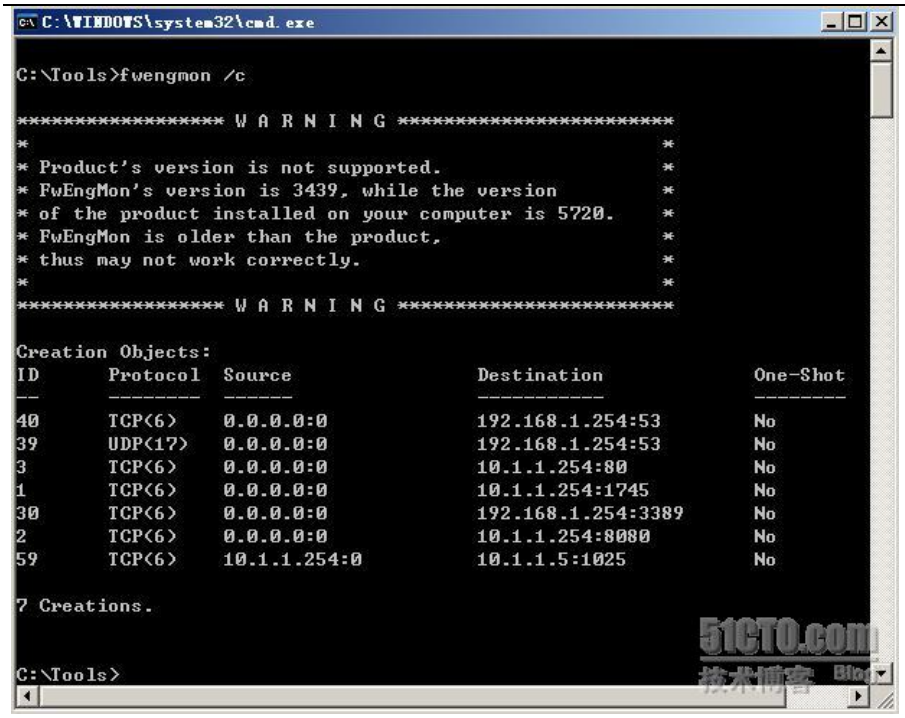
在 Istanbul 上测试一下 DNS 服务器的解析能力，如下图所示，域名解析成功，DNS 服务器的发布也没有问题。



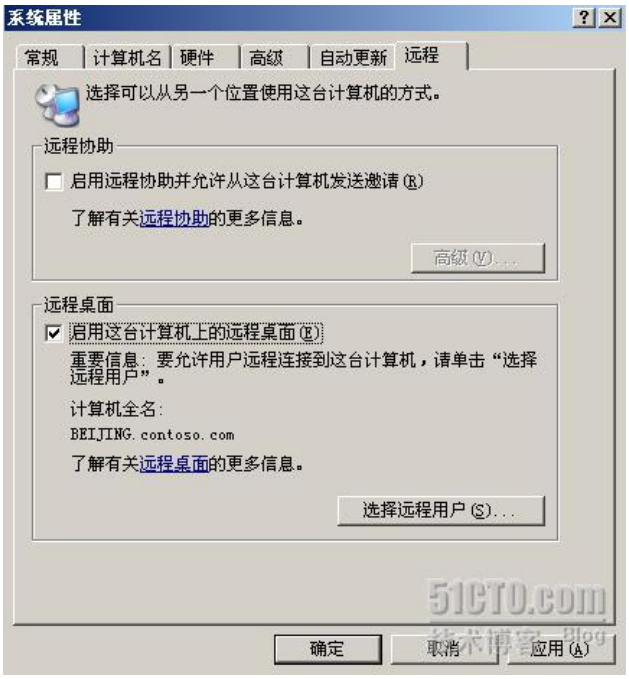
好了，举了两个发布服务器的例子之后，我们要考虑一下为什么 ISA 要强调这些服务器是非 Web 服务器，发布 Web 服务器和发布非 Web 服务器有什么区别呢？区别就在于监听模式，发布 Web 服务器时 ISA 委托 TCP 监听端口，而发布非 Web 服务器时 ISA 采用防火墙内核监听端口。例如刚才我们发布了终端服务器，那 ISA 的外网 IP 肯定要开放 3389

端口，否则外网用户无法访问终端服务器。我们在 ISA 上检查一下端口监听状况，如下图所示，我们用 NETSTAT –ANO | FIND “3389”来查看 3389 端口的监听状况。奇怪的事发生了，3389 端口竟然没有进程监听，这是怎么一回事？外网访问者连接 3389 端口时为什么不报错呢？

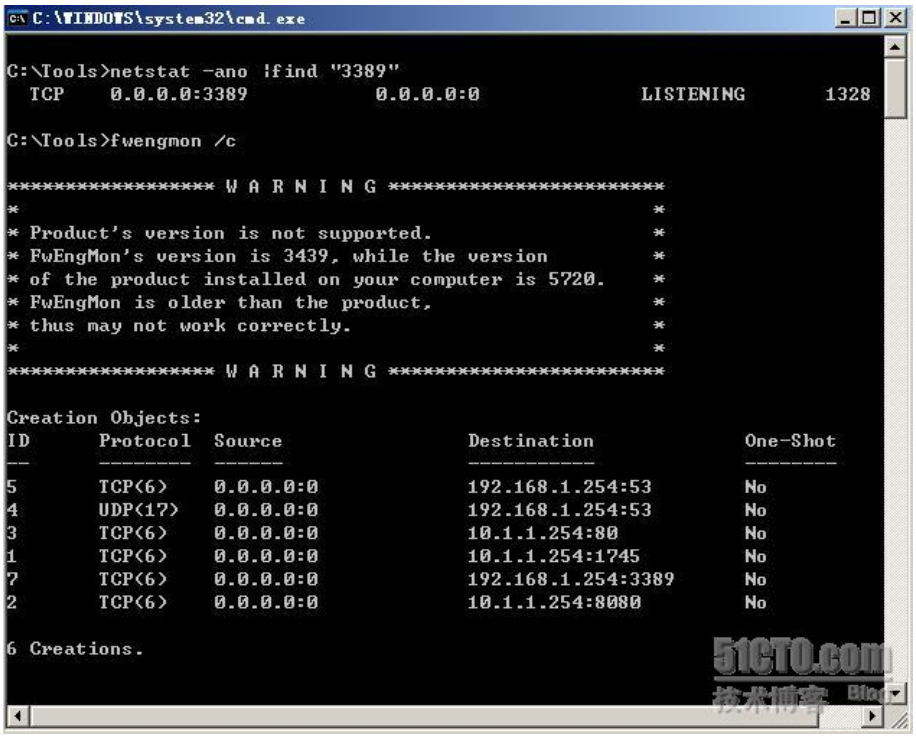
其实，3389 端口是有进程监听的，刚才我们说了，发布非 Web 服务器时由防火墙内核负责端口监听。由于防火墙内核工作在数据链路层和网卡驱动之间，因此我们用 NETSTAT 命令查看不到防火墙内核对端口的监听状况。那怎么才能知道防火墙内核在监听哪些端口呢？我们可以使用一个工具 fwengmon，这个工具可以在微软网站下载，从文件名可以看出，这个工具可以监控防火墙内核引擎的工作。我们在 ISA 上允许 fwengmon /c，如下图所示，我们可以很清楚地看到防火墙内核正在监听 3389，53 等端口。这下我们明白了，端口监听不一定非要委托 TCP 或 UDP，防火墙内核也可以进行隐性的端口监听。



那接下来再考虑这个问题，如果 ISA 用防火墙内核监听 3389 端口，同时又委托 TCP 监听 3389 端口，那两者的优先级哪个高呢？从理论上分析，应该是防火墙内核优先级更高，因为解码后的物理层数据先要经过防火墙内核才能到达 TCP。我们用实验证实一下，我们先停止 ISA 的防火墙服务，然后在 ISA 上打开远程桌面连接，如下图所示，最后再启动防火墙服务。



如下图所示，现在 ISA 服务器上 TCP 驱动程序和防火墙内核都在监听 3389 端口，它们谁的优先级更高呢？我们用 Istanbul 连接 3389 来测试一下，如果能连接到 Perth 的远程桌面，那说明是防火墙内核优先级高；如果访问被 ISA 拒绝，那说明是 TCP 优先级高，因为 ISA 不允许外网访问本机的远程桌面。



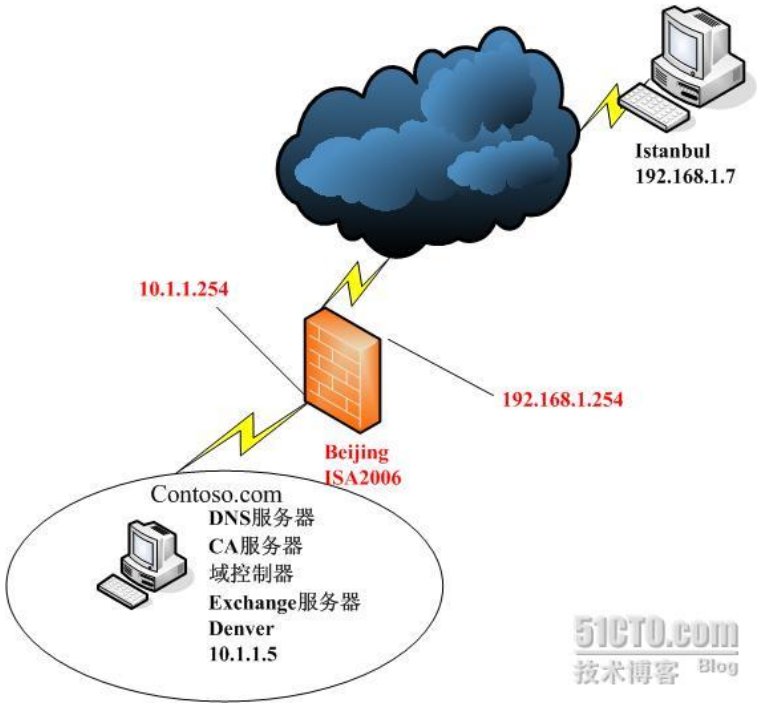
在 Istanbul 上测试，结果如下图所示，Instanbul 连接到了 Perth，这证实了防火墙内核的优先级确实要比 TCP 驱动高。

总结：以后如果遇到 ISA 发布服务器的故障，一定不要忘了可以用 fwengmon 检查防火墙内核对端口的监听状况，防火墙内核的端口盗用非常隐蔽，引发的故障不易发现，大家要注意到这个环节的问题。

发布 Exchange OWA 方法及故障分析：ISA2006 系列之十七

Exchange 服务器是微软公司重量级的邮件服务器，也是目前企业内网中邮件解决方案的代表作，鉴于 Exchange 服务器在微软产品中的重要性，我们准备组织几篇文章，以专题的形式系统地介绍如何用 ISA 发布 Exchange 服务器。今天我们从介绍发布 Exchange OWA 开始，OWA 是 Outlook Web Access 的缩写，OWA 允许用户通过浏览器访问 Exchange 邮箱，是使用最广泛的 Exchange 访问方法之一，下面我们就通过实例来来说明 Exchange OWA 具体应该如何发布，实验完成后后再分析一下常见的 Exchange OWA 发布故障。

实验拓扑如下图所示，Denver 是 Contoso.com 域中的域控制器，DNS 服务器，Exchange 服务器和 CA 服务器。Beijing 是 ISA2006 服务器，Istanbul 是外网的测试客户机。



51CTO.com
技术博客 Blog

实验前已做好下列准备：

一　Denver 已经创建 CA 服务器，类型是企业根，已被所有的计算机承认。

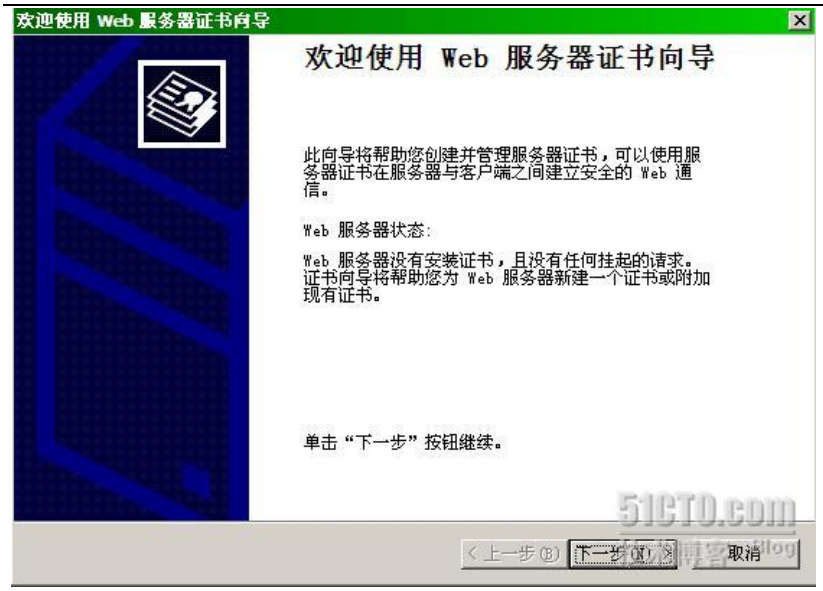
二　Istanbul 已经利用 Hosts 文件把 denver.contoso.com 解析为 ISA 的外网地址 192.168.1.254

我们推荐的发布方法是利用 SSL 保护 OWA 数据，ISA 使用桥接方法检查外网发来的加密数据，在 ISA 上启用表单验证，这样对 Exchange 的安全非常有利，具体步骤如下：

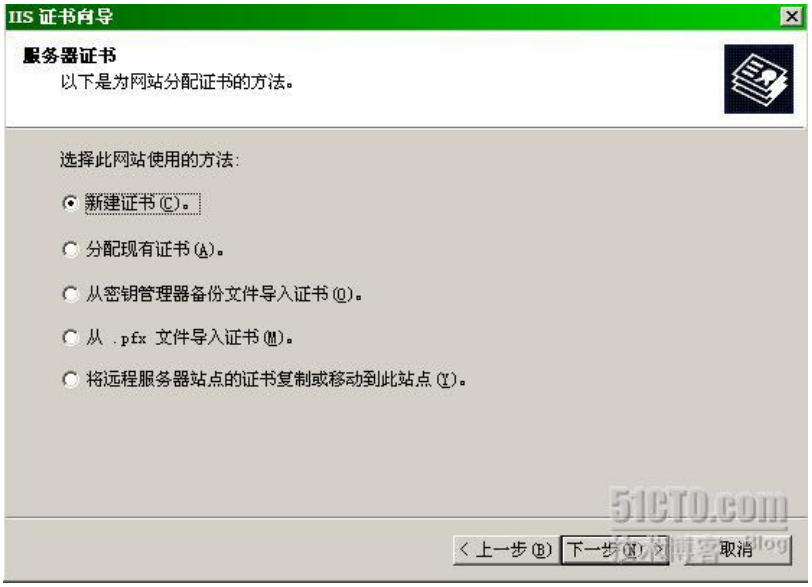
一　证书申请

发布 Exchange OWA 可以使用 HTTP，也可以使用 HTTPS，从安全角度考虑，我们推荐使用 HTTPS 对数据进行加密保护。既然想用 HTTPS，那肯定要在 Denver 的 IIS 上申请证书，在 Denver 的 IIS 管理器中打开默认站点属性，切换到目录安全性标签，如下图所示，点击“服务器证书”。

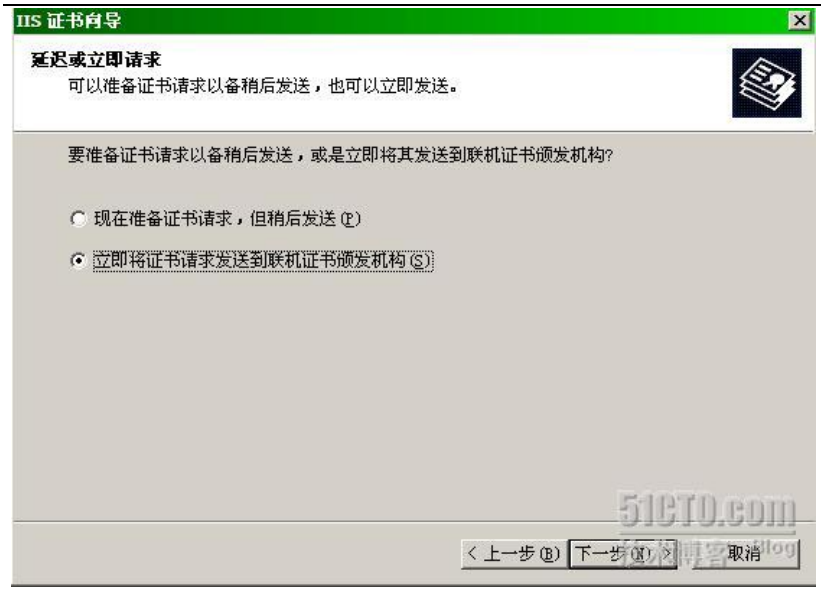
出现 Web 服务器证书申请向导，下一步。



选择“新建证书”。

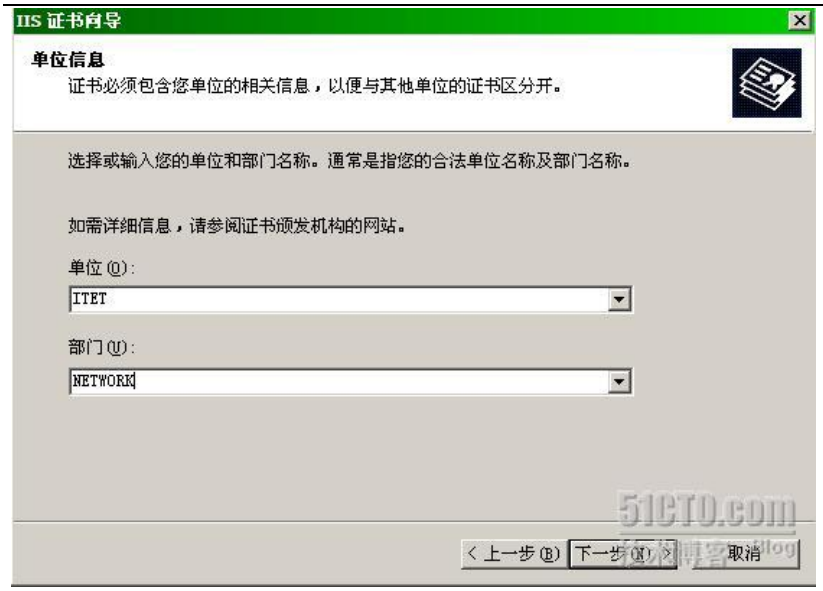


由于 Denver 上的证书服务器是企业根，支持在线颁发证书，因此我们选择“立即把证书请求发送到联机证书颁发机构”。



证书的名称和位长都可以使用默认值。

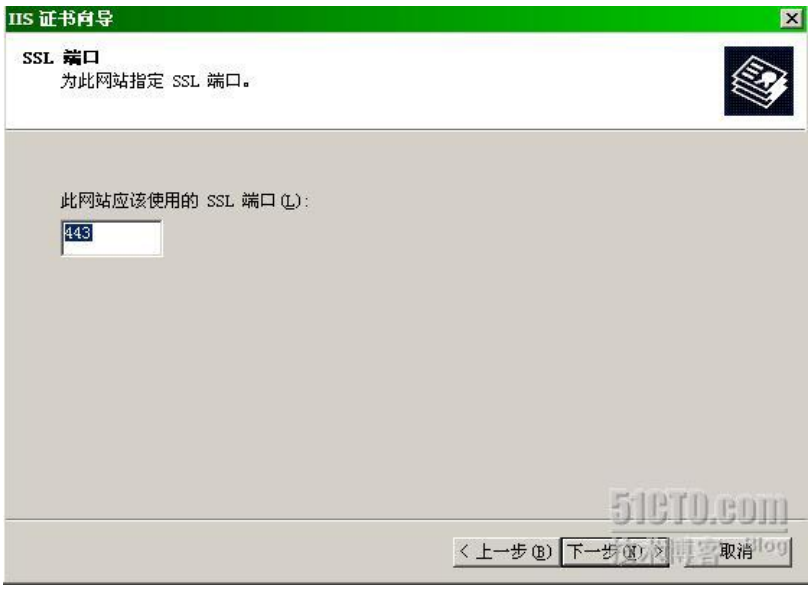
单位和部门属于描述信息，随便填填就可以了。



证书的公用名称是关键，这个名称需要和 Exchange 服务器发布到公网上的完全合格域名一模一样，而且 ISA 在发布规则中也需要使用这个名称来表示 Exchange 服务器。

填写证书的地理信息，这些不是关键参数，随便填填就可以了。

使用 SSL 的默认端口 443。



把证书申请直接发送到 Active Directory 中的 CA 服务器。

开始提交证书申请。

证书申请成功，CA 服务器已经满足了 IIS 的证书申请要求。

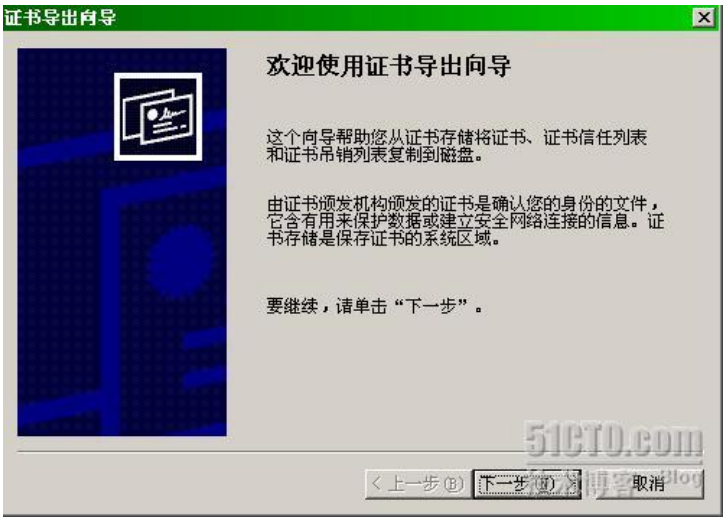
在 IIS 默认站点属性中切换到目录安全性标签，点击“查看证书”，如下图所示，证书是由 CA 服务器颁发给 denver.contoso.com 服务器的。

二 导出证书

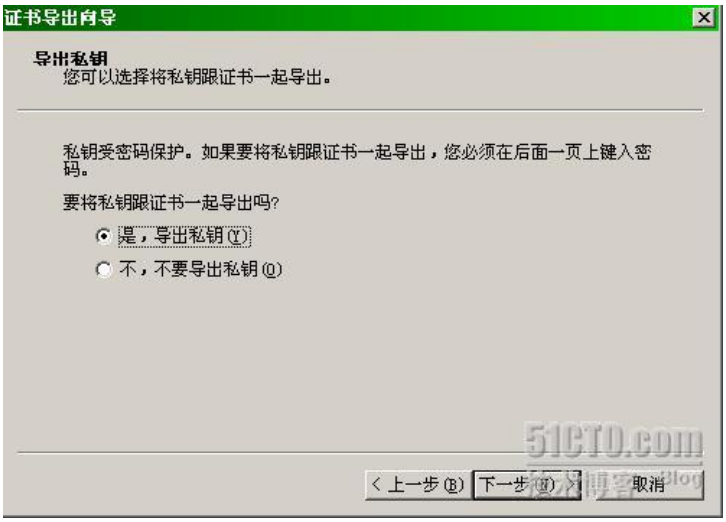
IIS 申请证书之后，由于 ISA 准备采用桥接的方法发布 Exchange 站点，因此 ISA 服务器需要用证书向外网用户证明自己就是他们要访问的 denver.contoso.com，ISA 需要的证书从何而来呢？答案是从 Denver 上导出。下面我们就来看看如何进行证书导出，在 denve

r 的 IIS 管理器中打开默认站点属性，切换到目录安全性标签，点击“查看证书”，切换到证书的“详细信息”标签，如下图所示，点击“复制到文件”。

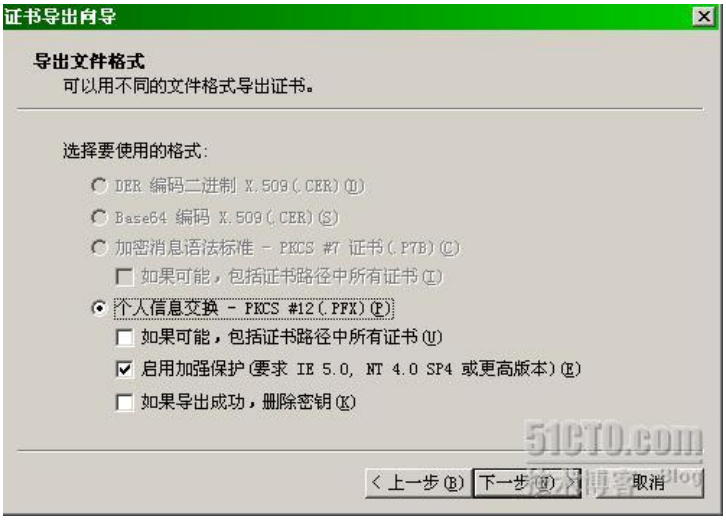
出现证书导出向导，下一步。



注意，必须导出私钥，否则 ISA 服务器无法解密数据。

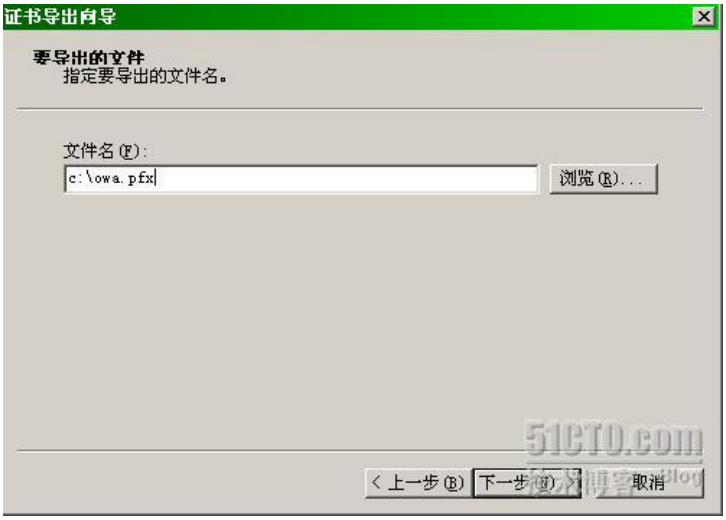


导出为 PFX 格式的证书文件。



输入保护私钥的密码，导入证书时必须回答出此密码才能导入私钥。

设置导出文件的路径和文件名。



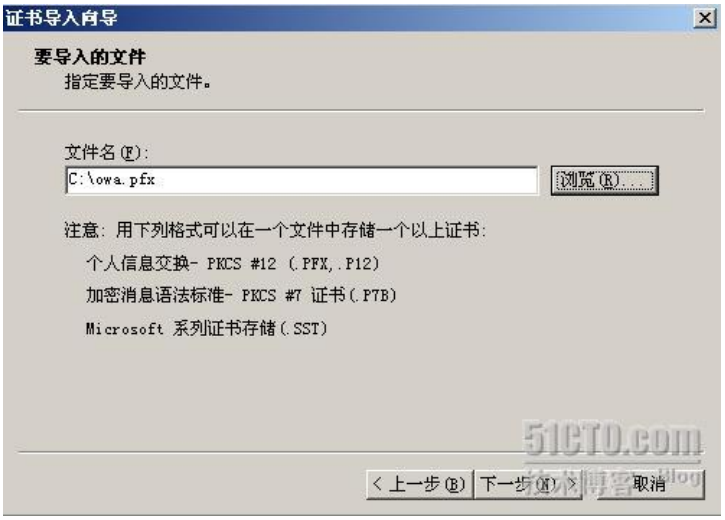
如下图所示，证书导出成功，接下来我们把证书文件复制到 ISA 服务器上，为下一步的证书导入做好准备。

三 导入证书

ISA 服务器需要导入此前 Denver 导出的证书，这样才能用于 Web 侦听器上加密外网用户发来的数据。在 ISA 服务器上用 MMC 自定义一个证书管理工具，负责管理计算机存储的证书（具体的定义方法请参见之前博文），如下图所示，在证书管理工具中选择“导入”。

出现证书导入向导，下一步。

导入的 owa.pfx 文件就是 Denver 导出的证书文件。



输入私钥保护密码。

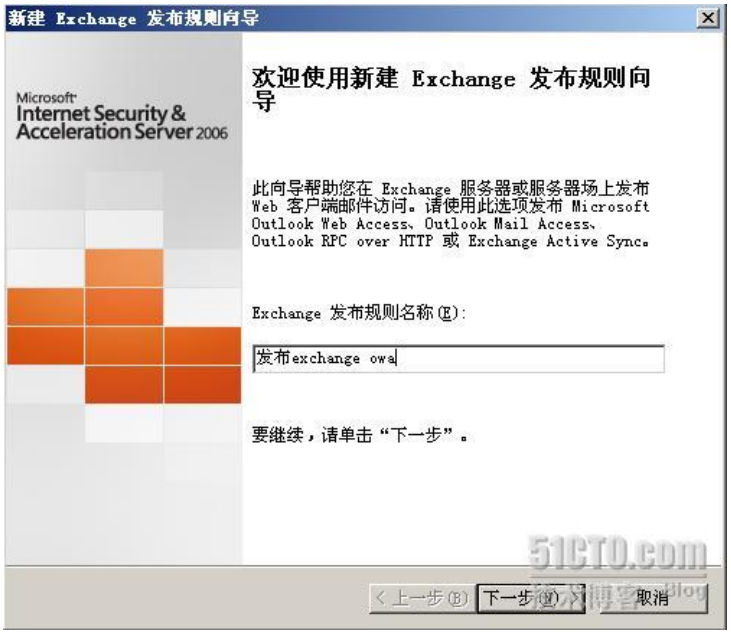
将证书存储在个人区域。

如下图所示，证书导入成功。

四 创建 OWA 发布规则

证书的申请，导出，导入等工作已经完成，接下来就可以在 ISA 服务器上进行 Exchange 的 OWA 发布了，如下图所示，我们在 ISA 服务器上选择新建“Exchange Web 客户端访问发布规则”。其实 ISA 只有两个发布规则，Web 服务器和非 Web 服务器，其余的都是在上述两种发布规则的基础上衍生出来的。

输入发布规则的名称。



选择 Exchange 版本为 Exchange 2003，客户端的访问方式是 Outlook Web Access。

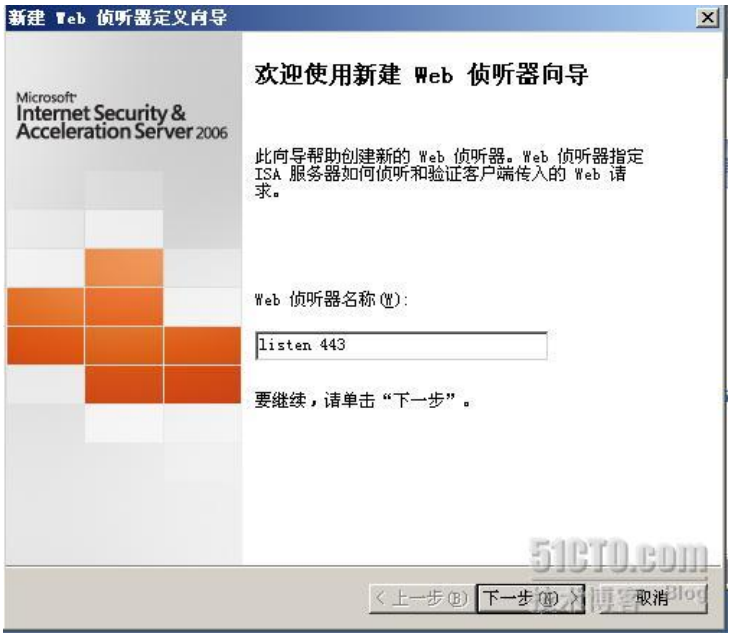
网站发布类型为发布单个网站。

选择使用 SSL 连接到被发布的 Exchange 服务器。

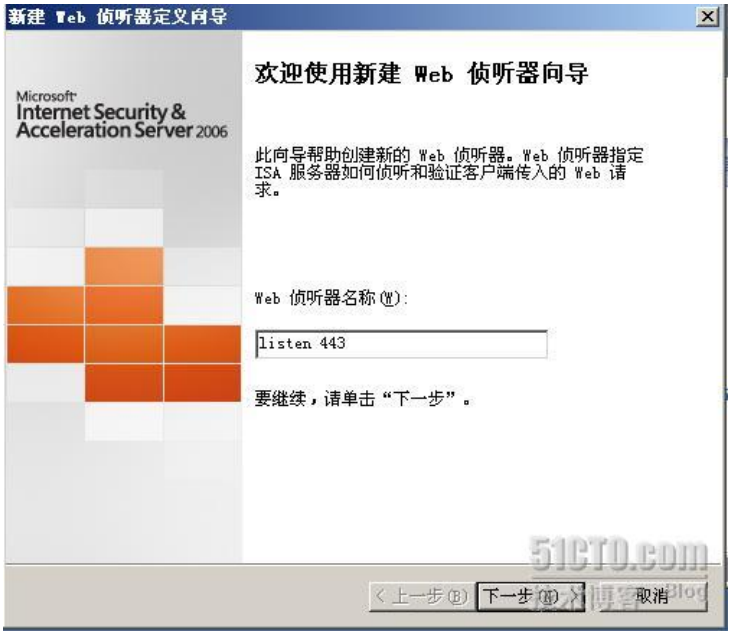
内部站点名称为 denver.contoso.com，注意，这个名称应该和证书的公用名称保持一致。

Exchange 服务器对外的公用域名也是 denver.contoso.com。

由于没有 Web 侦听器，我们选择新建一个。



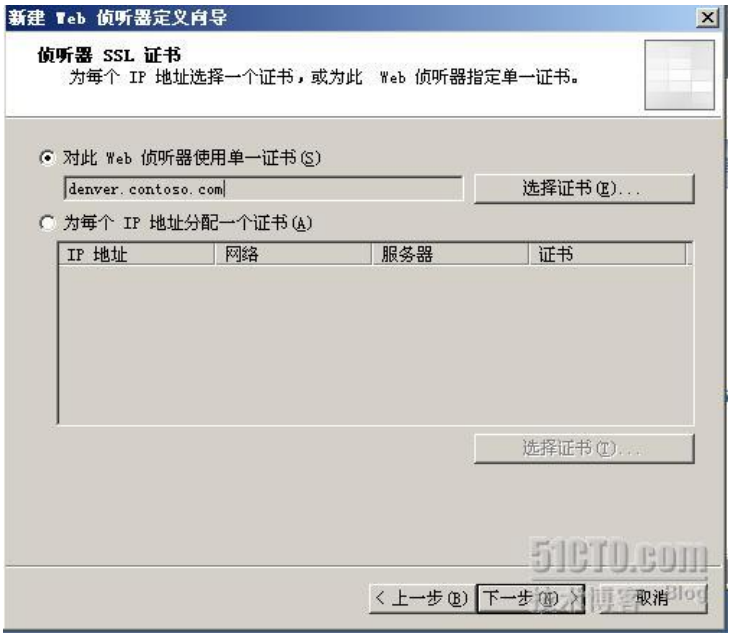
出现新建 Web 侦听器向导，我们为侦听器取名为 listen 443。



侦听器与外网访问者之间的数据传递也用 SSL 进行加密。

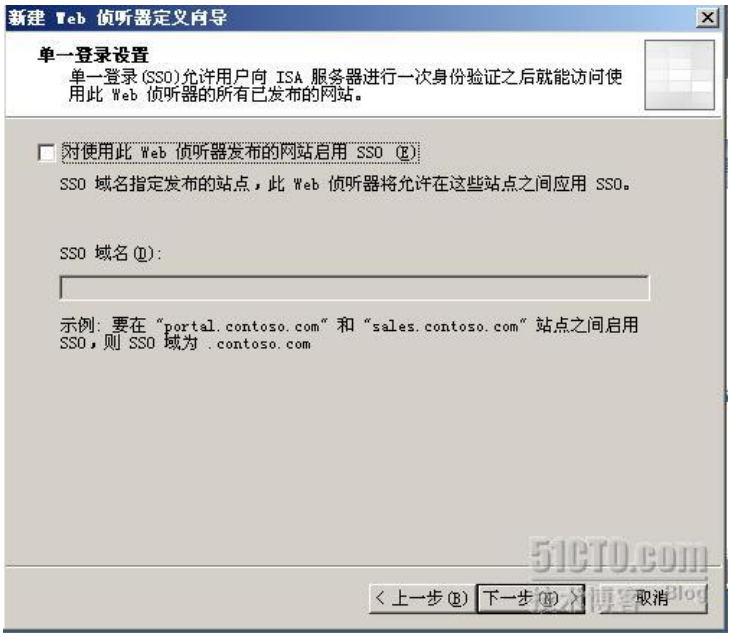
侦听器监听的区域是外网。

在侦听器中选择使用导入的 denver.contoso.com 证书。

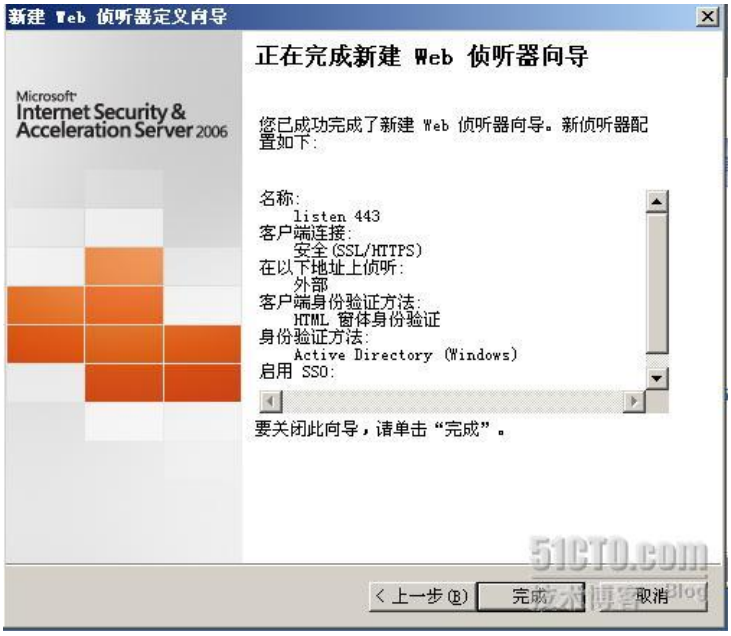


客户端验证方式可以选择 HTML 窗体验证，窗体验证对于使用公用计算机的外网用户来说更加灵活安全。

在本例中我们不需要使用单一登录设置。



好了，Web 侦听器创建完毕。



在 Exchange OWA 的发布规则中选择使用刚创建的 Web 侦听器。

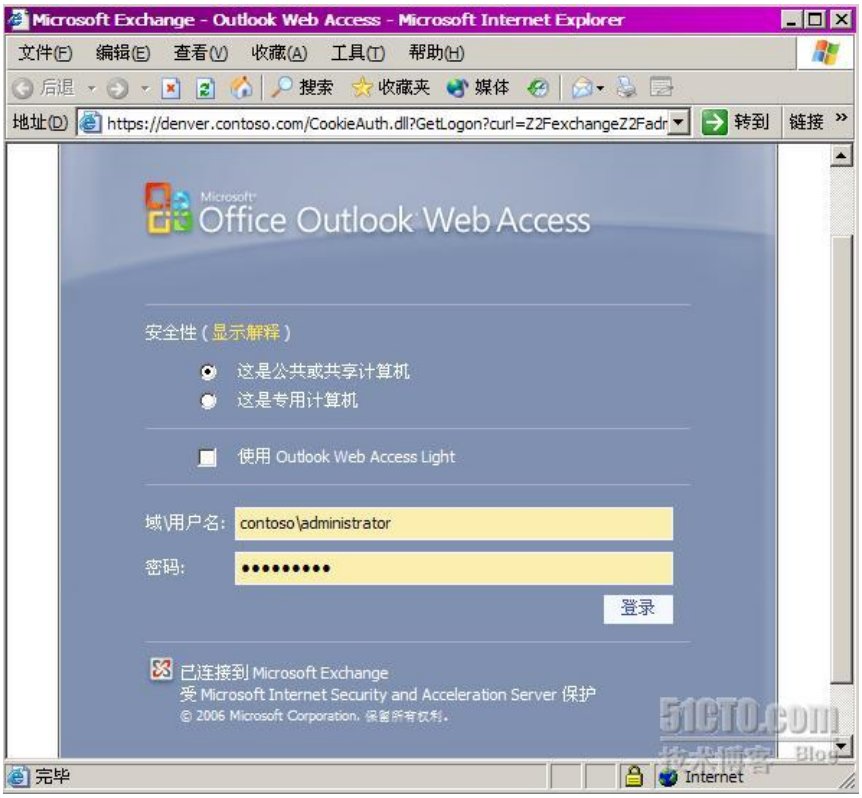
ISA 使用基本身份验证来进行验证委派，虽然基本身份验本身对数据没有进行加密保护，但由于使用了 SSL，基本身份验证也是很安全的。如果使用集成验证委派，那需要我们在 Actively Directory 中配置相关的 SPN。

由于发布的 Exchange OWA 需要对用户进行身份验证，因此发布规则针对的用户应该是所有通过身份验证的用户。

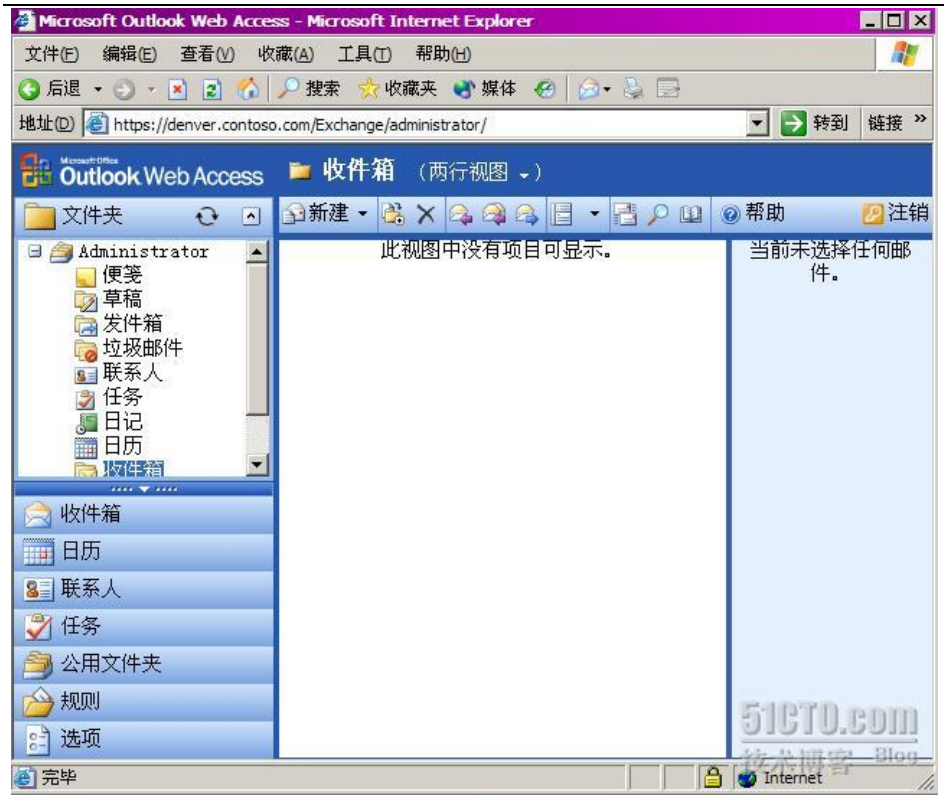
好了，终于完成了发布规则！

五 测试

完成了 OWA 的发布之后，我们在外网的 Istanbul 上测试一下，在 Istanbul 的浏览器中输入 https://denver.contoso.com/exchange/administrator，结果如下图所示，出现表单登录界面，选择我们使用的计算机是公用计算机上，输入用户名和密码，点击登录。



登录后的结果如下图所示，我们进入了 Exchange 邮箱，OWA 发布成功！



上述是我们推荐的 Exchange OWA 发布方法，建议大家参考使用，在此将发布 OWA 时的一些常见问题共总结如下：

1 建议发布 OWA 时使用 HTTPS 保护数据安全，注意，如果证书是从自己创建的 CA 服务器申请的，那公网的访问者必须信任证书颁发机构，否则访问会失败。

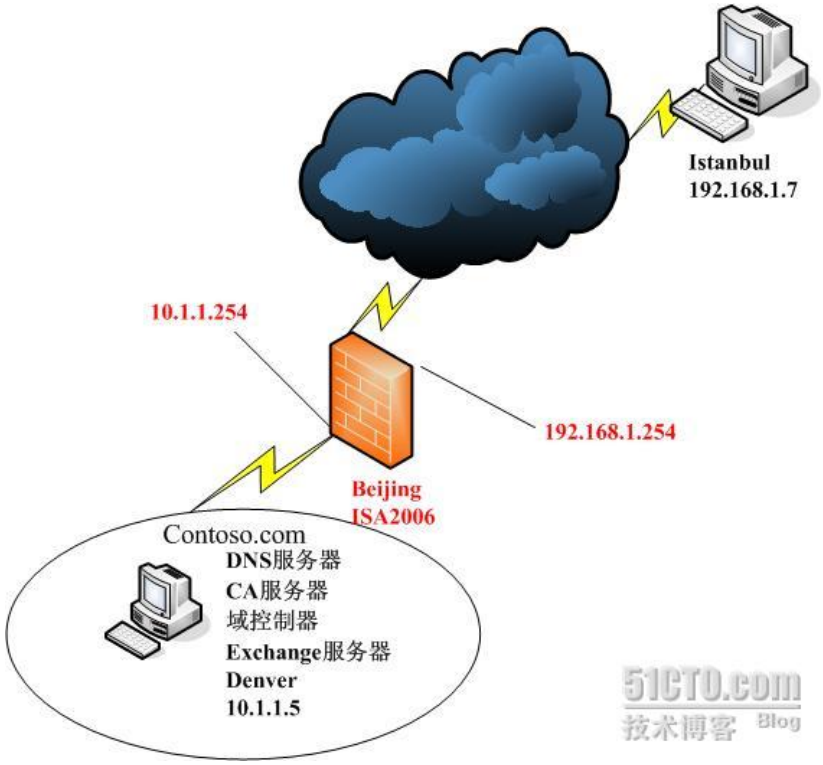
2 如果发布 OWA 时使用 HTTP 协议，那要注意 ISA2006 默认不允许在 HTTP 协议中进行身份验证，客户机访问 Exchange 时会被 ISA 拒绝，前不久为一位博友解决的 Exchange OWA 发布故障就是因为这个原因。解决方法是在 Web 侦听器属性－身份验证－高级中勾选“允许通过 HTTP 进行客户端身份验证”。

3 如果在 ISA 中不是通过创建 Exchange Web 访问规则来发布 OWA，而是通过创建网站发布规则来发布 OWA，那有可能会出现无法显示邮箱的故障。原因是发布规则的 HTTP 过滤中阻止了高位字符，汉字也在被阻止的范围之内，因此无法显示中文邮箱。解决方法是在发布规则中配置 HTTP 过滤，取消阻止高位字符即可。

发布 Exchange 的 SMTP，POP3 服务器：ISA2006 系列之十八

上篇博文中我们介绍了如何发布 Exchange OWA，今天我们来介绍如何发布 Exchange 的 SMTP 和 POP3 服务器。用 SMTP，POP3 客户端访问 Exchange 服务器也是邮件用户常用的选择，用 ISA 发布 Exchange 的 SMTP，POP3 服务器并不困难，只要用非 Web 服务器发布规则把 Exchange 服务器的 SMTP 和 POP3 发布到 ISA 服务器外网网卡即可，我们举例加以说明。

实验拓扑如下图所示，Denver 是域控制器，DNS 服务器，CA 服务器，Exchange 服务器，Beijing 是 ISA2006 服务器，Istanbul 是外网的客户机。

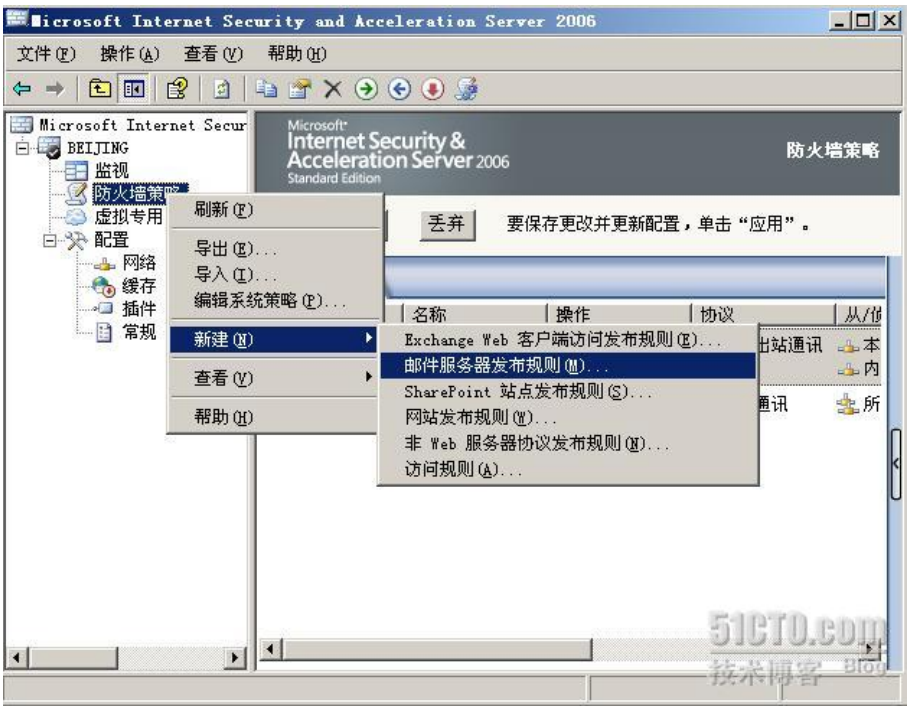


发布之前我们已经做好下列准备

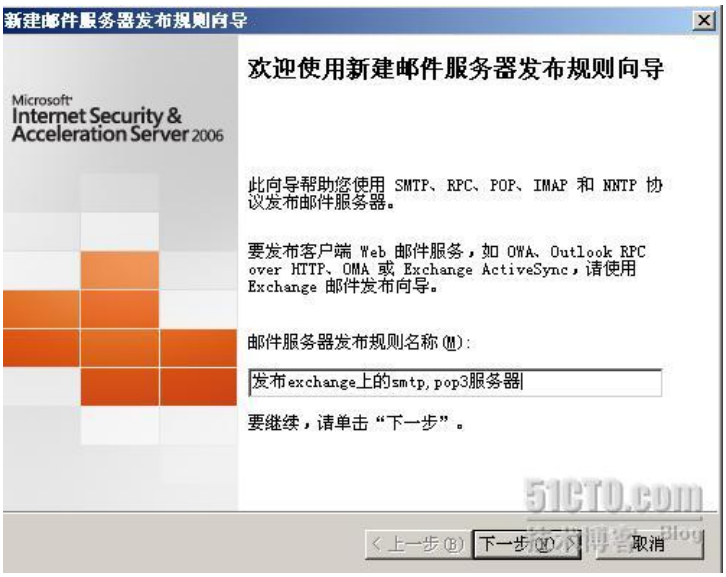
1 所有的计算机都信任 Denver 上的 CA

2 Istanbul 利用 hosts 文件把 denver.contoso.com 解析为 192.168.1.254

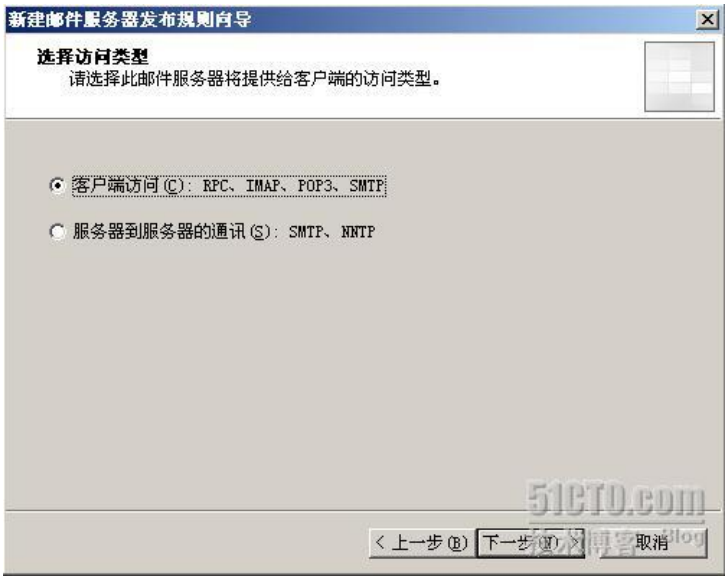
在 ISA 服务器的防火墙策略中选择新建“邮件服务器发布规则”，如下图所示，当然，如果我们原意，使用非 Web 服务器协议发布规则也可以。但使用邮件服务器发布规则自有它的好处，后面我们就明白了。



为发布规则取个名称。



访问类型属于客户端访问 SMTP，POP3 服务器。



此次发布的服务是 POP3 和 SMTP。

Exchange 服务器的 IP 地址是 10.1.1.5。

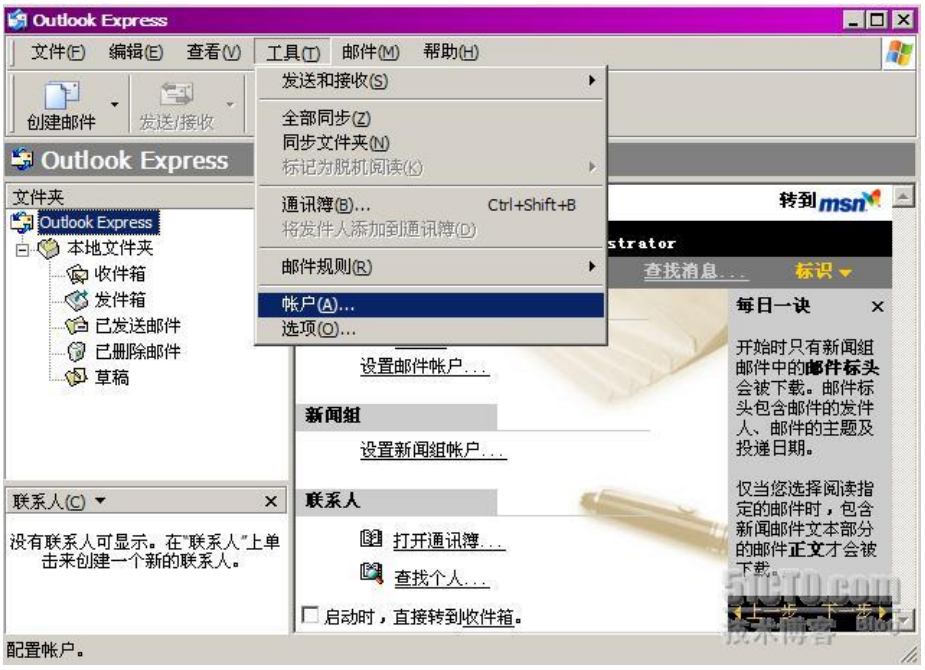
监听外网网络的访问请求。

好，完成了服务器发布向导。

查看 ISA 的防火墙策略，我们发现虽然只进行了一次发布操作，但发布向导却帮我们创建了两条服务器发布规则，一条是 SMTP，另一条是 POP3，这就是我们在前面提到的方便之处。

ISA 发布了 Exchange 的 SMTP 和 POP3 服务器，我们利用外网的 Istanbul 测试一下，Istanbul 使用系统内置的 Outlook Express 作为 SMTP/POP3 的客户端，我们在 Istanbul

上打开 Outlook Express 之后，如下图所示，选择“工具”菜单中的“帐户”，准备创建一个访问 Exchange 邮箱的邮件帐户。



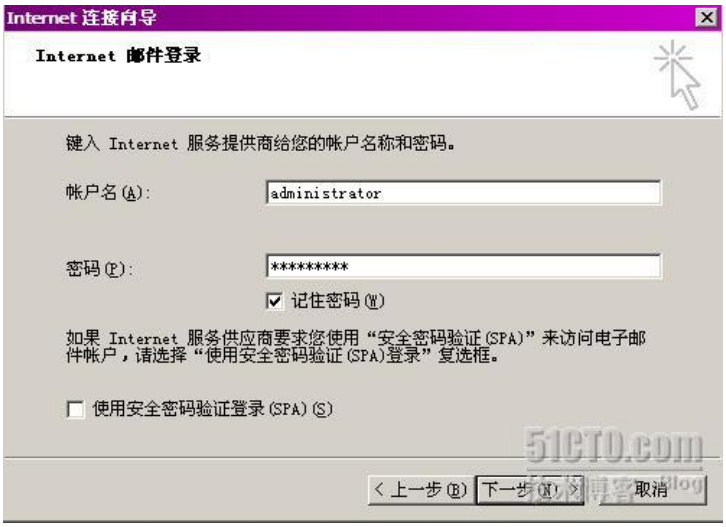
如下图所示，点击添加邮件帐户。

显示名为 administrator。

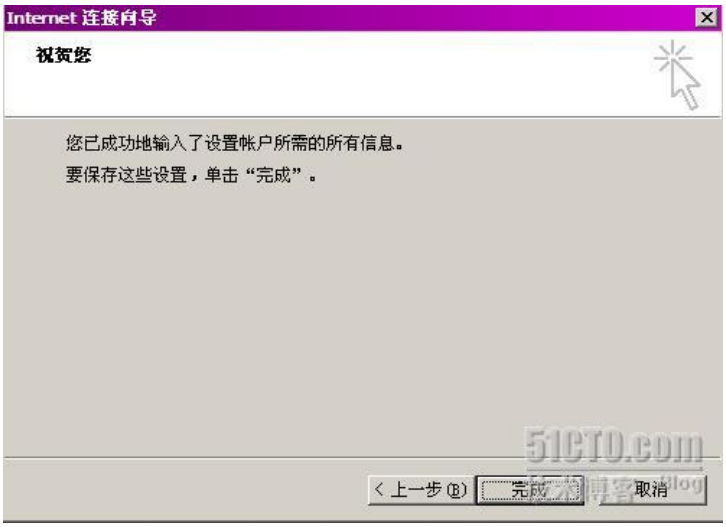
邮件地址是 administrator@contoso.com。

填写 SMTP 服务器和 POP3 服务器的域名或 IP 都可以，注意，域名 denver.contoso.com 已经被解析到 ISA 的外网 IP 了。

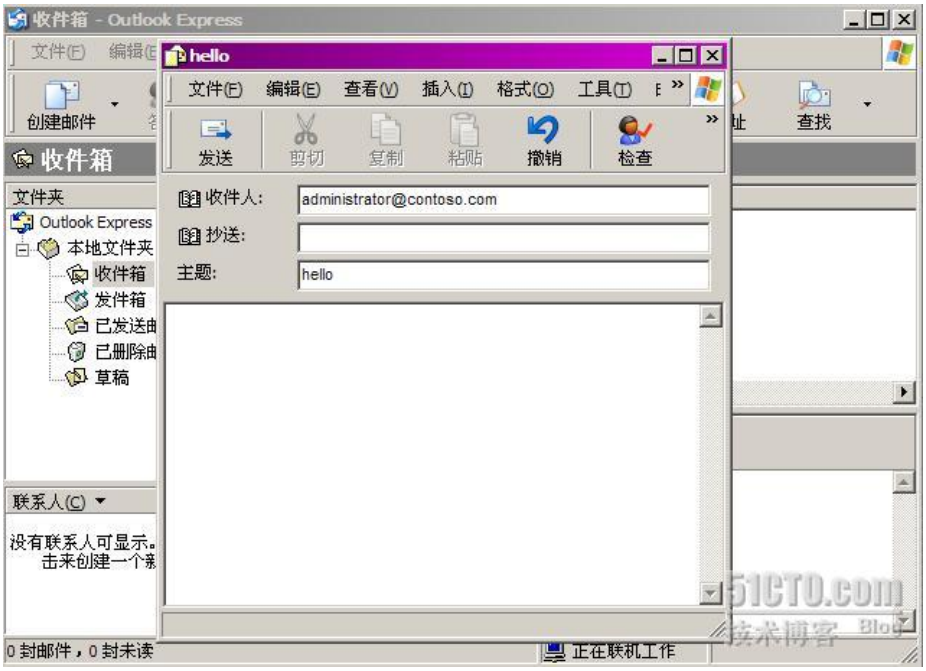
输入 administrator 邮箱的用户名和密码。



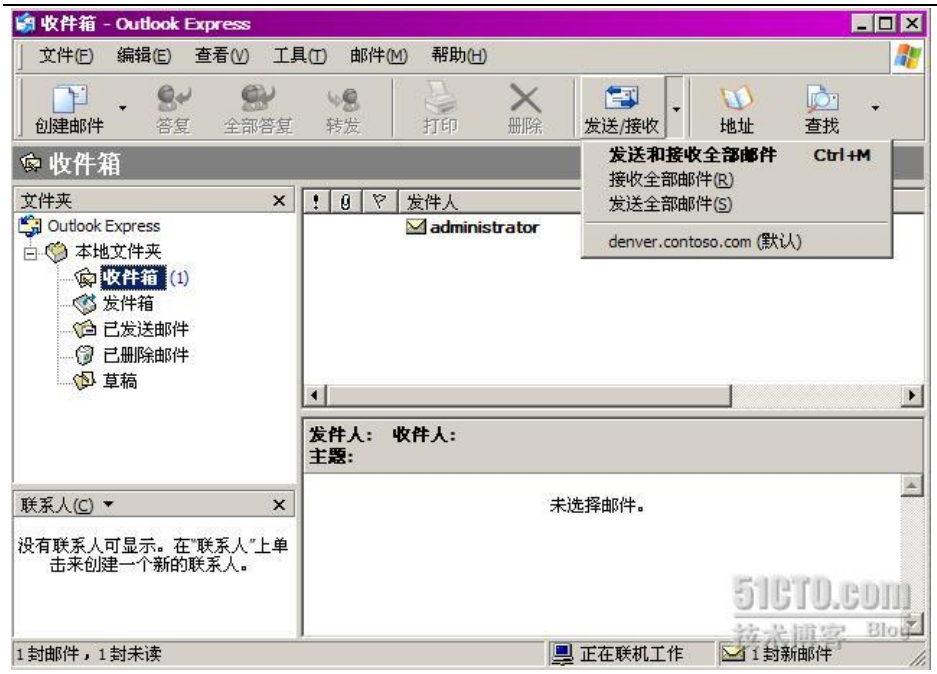
终于完成设置。



如下图所示，首先给自己发一封信，测试一下 SMTP。



发完测试邮件后，如下图所示，点击“接收全部邮件”，我们发现在收件箱中已经收到了刚刚发出的测试邮件，这表明发布的 SMTP 和 POP3 都成功了。

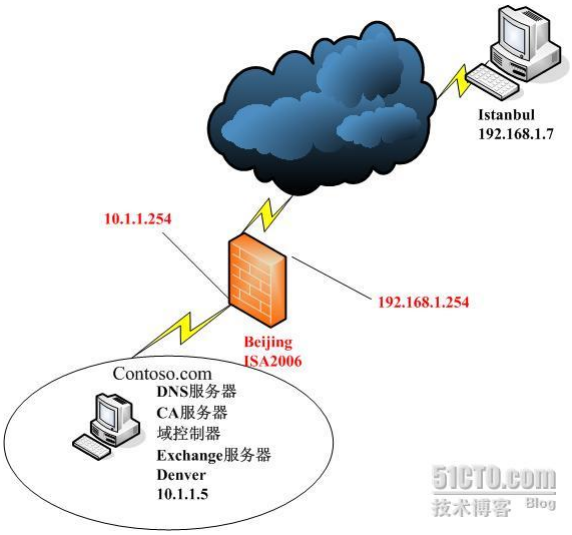


发布 Exchange 的 SMTP 和 POP3 服务器是 Exchange 发布问题中最简单的，下篇博文中我们将介绍 Exchange 发布中最麻烦的的发布方式－PC Over HTTPS，敬请期待。

发布 Exchange 的 RPC 以及 RPC Over HTTPS：ISA2006 系列之十九

在前几篇博文中，我们介绍了如何使用 OWA，SMTP/POP3 来发布 Exchange 服务器，今天我们介绍如何利用 RPC 或 RPC Over HTTPS 来发布 Exchange，这也是 Exchange 发布系列的最后一篇博文，OWA，SMTP/POP3，RPC，RPC Over HTTPS 已经涵盖了目前发布 Exchange 所使用的全部技术。

实验拓扑和以前一样，Denver 是域控制器，CA 服务器，DNS 服务器，Exchange 服务器，Beijing 是 ISA2006 服务器，Istanbul 是外网测试客户机。



一 利用 RPC 发布 Exchange 服务器

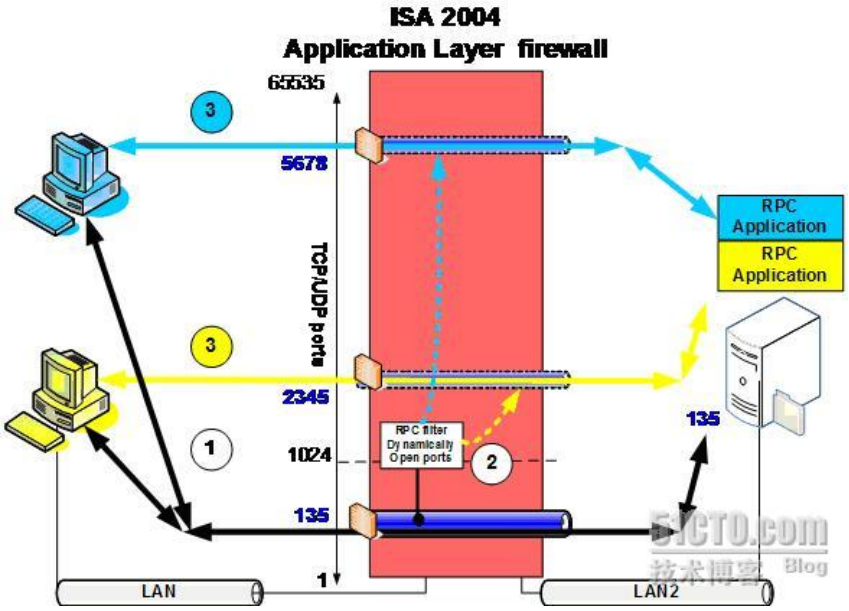
以前我们在 Exchange 系列博文中（http://yuelei.blog.51cto.com/202879/d-3）曾经介绍过，Exchange 的最佳客户端是使用 RPC 协议的 Outlook，Outlook 是微软为 Exchange 量身定做的客户端软件，可以发挥出 Exchange 的所有功能，如果从性能角度考虑，Outlook 应该是 Exchange 客户端的首选。

Outlook 这么好，为什么以前大家经常用 OWA 访问呢？一是 OWA 使用起来相对简单，二是 Outlook 使用的 RPC 协议对防火墙是个很大的考验.。RPC 的特点是什么？我们在 Exchange 系列博文中曾经分析过，基于 RPC 的服务端口并不固定，每次服务启动时把自己的端口号以及 UUID 注册到 135 端口的终点映射器上。客户端要访问 RPC 服务，首先要连接到 RPC 服务器的 135 端口，向终点映射器提交要访问的服务的 UUID，根据 UUID 查询这个服务本次启动对应的端口号是多少。这么折腾一番后，客户端才明白自己要访问的服务在哪个端口等着自己，这时才赶紧去连接那个端口。

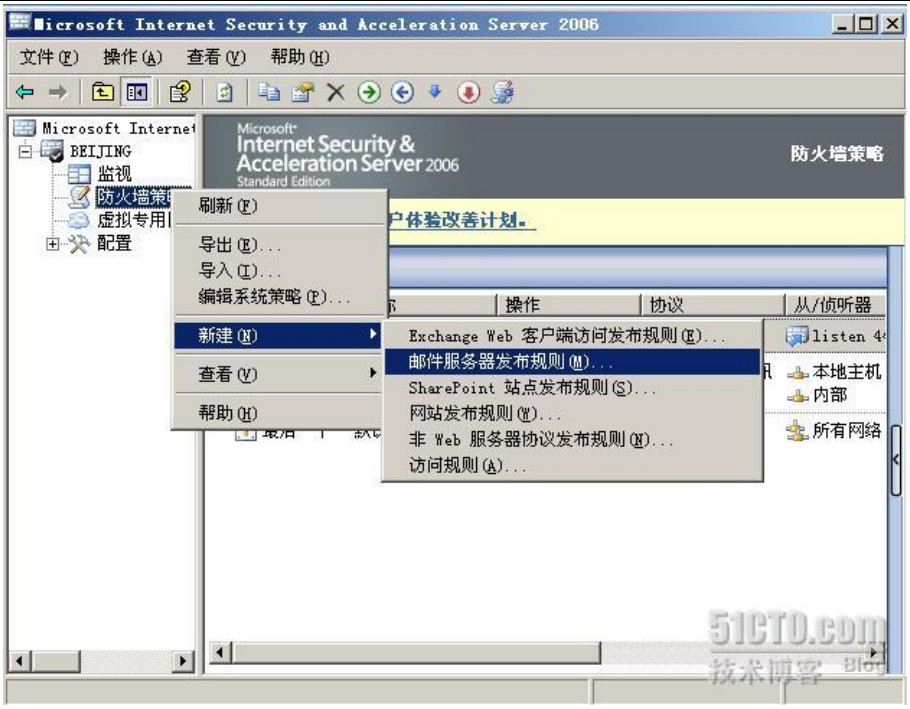
RPC 的这个特性如果用在局域网内，客户机和服务器能直接访问到，本来也算不了什么。问题是如果客户端和服务器之间还隔了一道防火墙，那防火墙就很头疼了，为什么？你想啊，客户端访问 RPC 服务器的端口号不是固定的，防火墙怎么开放端口呢？如果开放 RPC 有可能使用的全部端口，那就要把 1024 以上的端口都打开，那防火墙就成筛子了。如

果只开放固定端口，那就要想办法让 RPC 服务器的管理员配合自己，把 RPC 的服务端口限定在一个范围内。但是这么做一方面比较麻烦，另一方面需要牺牲 RPC 的灵活的特性，并不是好的解决方案。因此如果你是防火墙，你是否也会头疼呢？这个问题尤其是对硬件防火墙来说是很难解决的，但是！但是！ISA 已经彻底解决了这个问题，确切地说，ISA2004 就已经很完美地解决了这个问题。

ISA 解决 RPC 发布的问题其实很简单，ISA 能够听懂 RPC 客户端和 RPC 服务器之间的会话内容，ISA 根据会话内容可以判断出 RPC 客户端要访问的服务端口号是多少，当 RPC 客户端通过 ISA 访问 RPC 服务时，ISA 会动态地，临时地开放相关端口，允许 RPC 客户端访问进去。当 RPC 客户端访问结束后，端口会自动关闭。你看，这个解决方案如何，ISA 号称是应用层防火墙，和它对 RPC 的完美支持也是有关系的。ISA 对 RPC 的支持可以通过下图来说明。

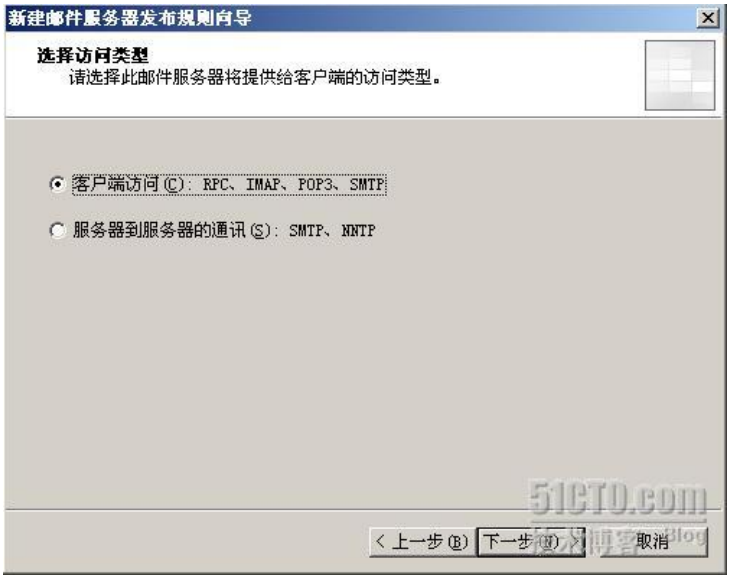


说了这么半天，无非是和大家介绍一下 RPC 的原理，希望大家理解 ISA 发布 RPC 服务器从操作上看很简单，但实际上对防火墙的过滤器有很高的技术要求。好，让我们通过实例来看看如何发布 Exchange 的 RPC 服务。如下图所示，在 ISA 服务器上选择新建“邮件服务器发布规则”。



为发布规则取个名字。

访问类型属于客户端访问 RPC 服务器。



用 ISA 发布 Exchange 服务器上的 RPC 服务。

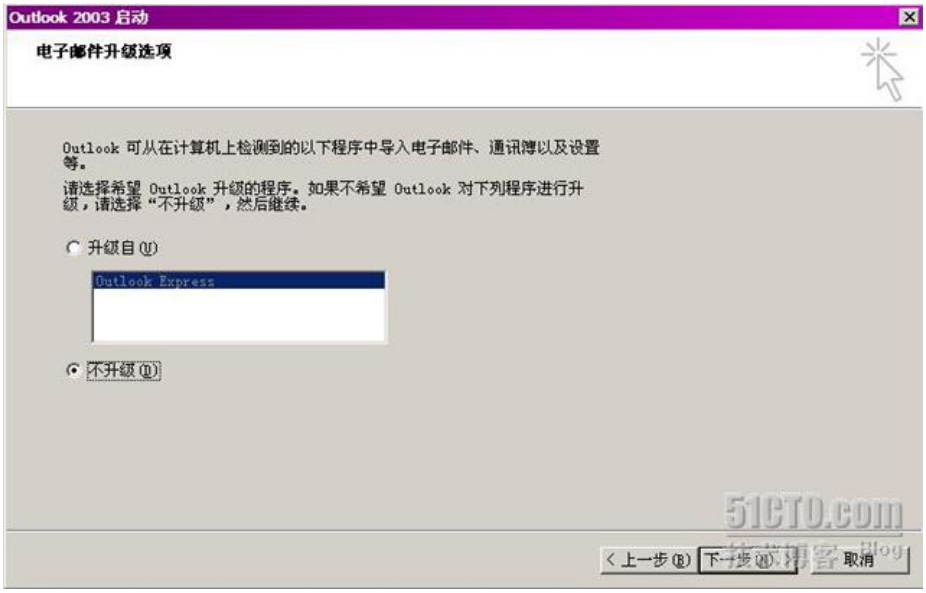
填写 RPC 服务器的 IP 地址。

侦听外部网络。

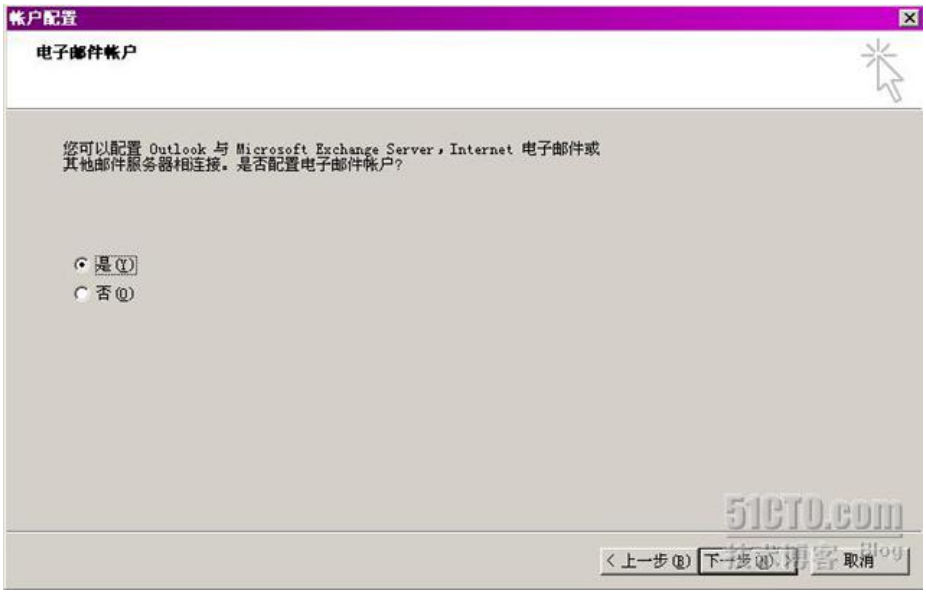
完成 RPC 服务器的发布。这条发布规则看起来似乎只是把 Exchange 服务器的 RPC 服务发布出来了，其实 Exchange 服务器上所有基于 RPC 的服务现在都可以访问了。

在外网的 Istanbul 上测试一下，启动 Outlook 2003，如下图所示，选择“下一步”。

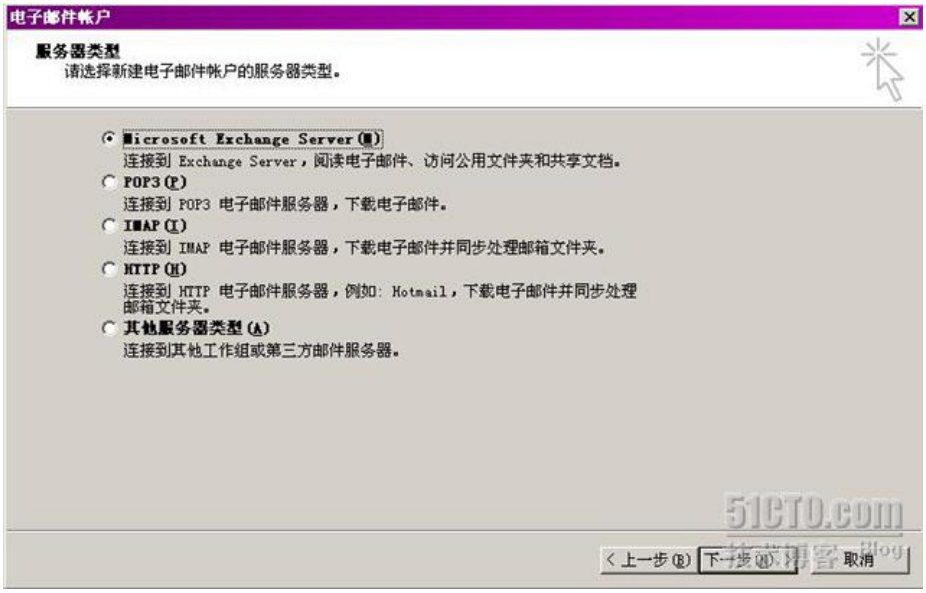
Outlook 询问是否需要升级电子邮件账号，选择“不升级”，准备创建一个 Outlook 配置文件。



选择配置一个电子邮件账号。



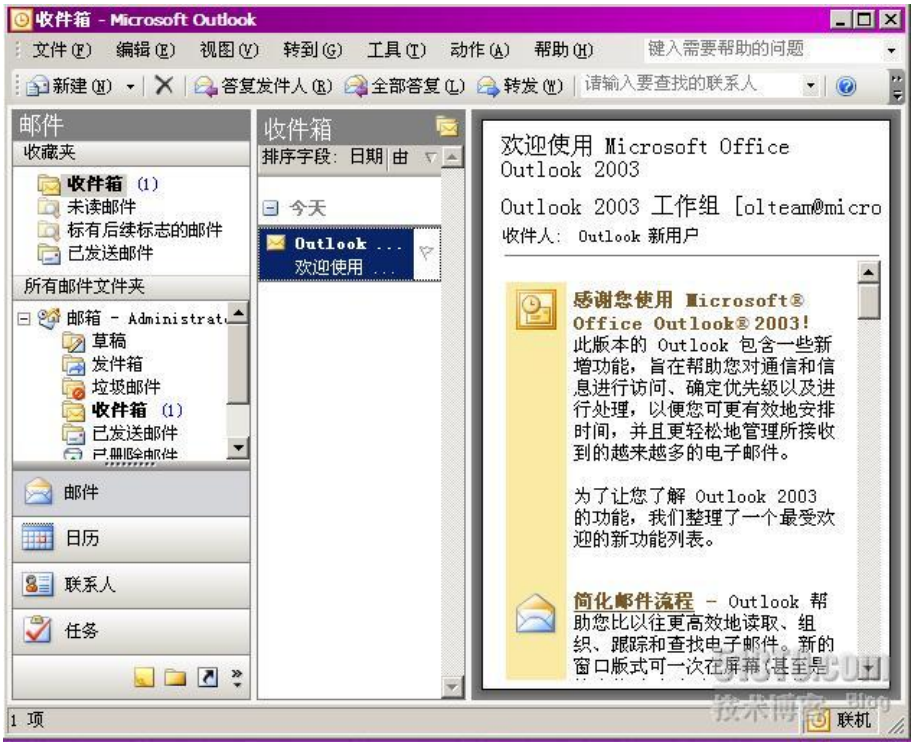
后台邮件服务器的类型是 Exchange 服务器。



Exchange 服务器的域名是 denver.contoso.com，不使用缓存模式，要访问的邮箱是 administrator。

终于完成了 Outlook 的配置文件。

创建完配置文件后，Outlook 登录进入了管理员邮箱，如下图所示，这说明发布 Exchange 的 RPC 服务成功了。



二　利用 RPC Over HTTPS 发布 Exchange 服务器

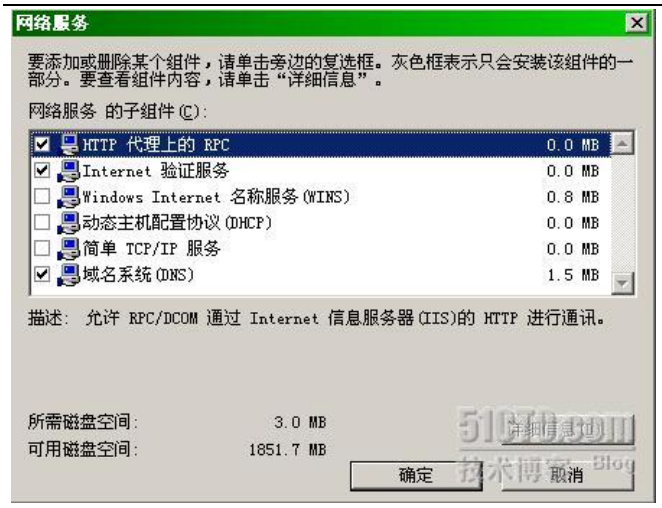
RPC 发布成功之后，我们就要来考虑一下 RPC Over HTTPS 了，RPC Over HTTPS 我们在 Exchange 系列博文中已经介绍过了，它主要就是考虑到电信部门可能会在公网上封锁 RPC 协议，因此把 RPC 协议封装成 HTTP 或 HTTPS 格式，这样就可以躲过电信的封杀，等封装后的数据包到达 RPC 服务器后，由 RPC 服务器再进行解封装操作，这样就借助 HTTP 的伪装完成了 RPC 数据的传递。

发布 RPC Over HTTPS 并不复杂，其实就是把 Exchange 服务器上的一个 RPC 虚拟目录发布出来。麻烦的是要搭建 RPC Over HTTPS 的环境，做这个实验要有点耐心，我们慢慢来吧。

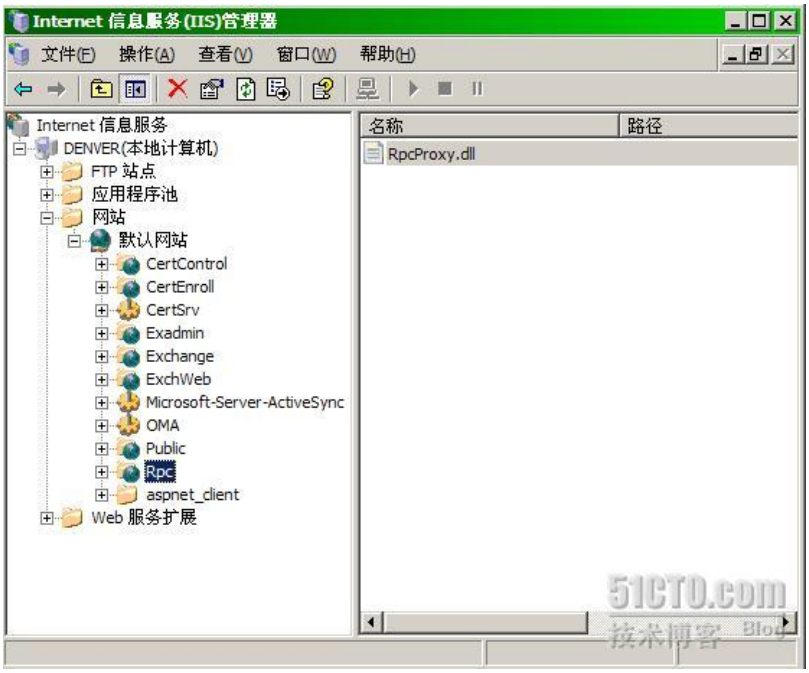
1）安装"HTTP 代理上的 RPC"

首先我们需要让 Exchange 服务器在收到封装成 HTTP 格式的 RPC 数据包后，具有解封装能力，这个功能可以通过安装一个组件"HTTP 代理上的 RPC"来完成。组件的安装方式是，在 Exchange 服务器上依次点击 开始－设置－控制面板－添加或删除程序－添加 / 删除 Windows 组件，如下图所示，选择"网络服务"，点击"详细信息"。

在网络服务的子组件中选择"HTTP 代理上的 RPC"，如下图所示。



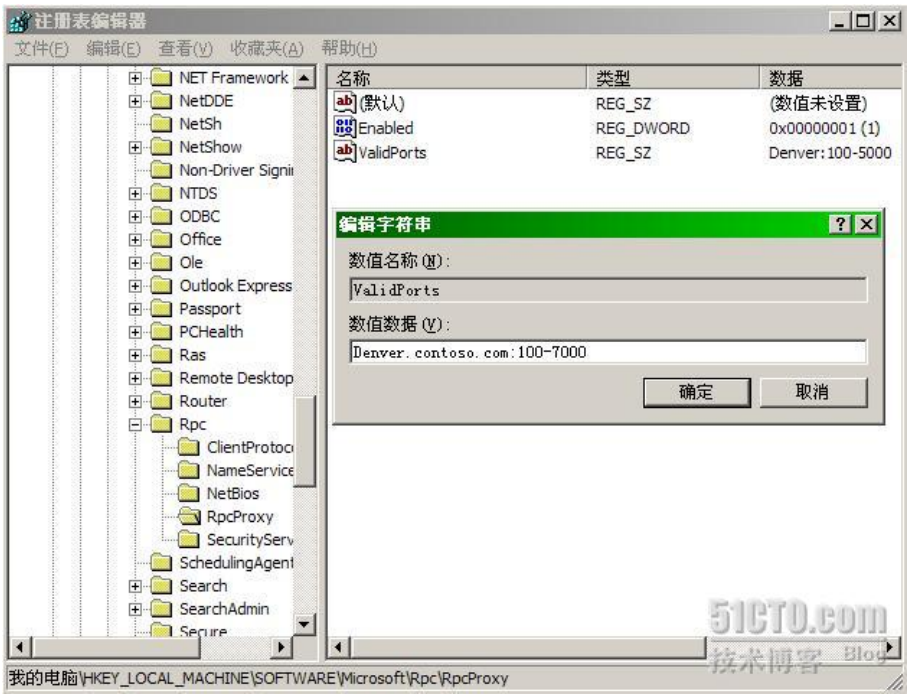
安装完组件后，检查 IIS，发现 IIS 的默认站点中多了一个 RPC 虚拟目录，虚拟目录中有一个 rpcproxy.dll 的动态链接库，其实就是这个文件具有解封装的功能，客户端也会把封装好的 RPC 数据按照约定发到 Exchange 的 RPC 虚拟目录下。



2）配置“HTTP 代理上的 RPC”

Exchange 服务器上安装了“HTTP 代理上的 RPC”后，我们还需要对这个组件进行简单的配置，主要是配置端口。默认情况下，“HTTP 代理 RPC”代理的 RPC 协议端口范围在 1 00－5000，但 Exchange 使用的 RPC 服务端口范围超过了 6000，因此我们需要对此进行

一番设置。在 Exchange 服务器上运行 Regedit，在注册表中定位到下列键值[HKEY_LOCAL_MACHINESOFTWAREMicrosoftRpcRpcProxyValidPorts]，如下图所示，我们把 Valid Ports 的键值改为 denver.contoso.com:100-7000。100-7000 是扩大了端口范围，计算机名设置为 denver.contoso.com 是为了和用户访问 Exchange 服务器的域名相匹配。值得注意的是，改完之后无需重启即可生效。



3）IIS 支持 HTTPS

把 RPC 数据包封装成 HTTP 格式后，再利用 SSL 对数据进行加密保护就更安全了，因此我们需要在 Exchange 服务器的 IIS 中申请证书，用以满足客户端进行 HTTPS 访问的需求。好在前面的 OWA 发布实验中我们已经申请过证书了，如下图所示，IIS 中已经有一个颁发给 denver.contoso.com 的服务器证书，这样 Exchange 就可以支持客户端用 HTTP 封装 RPC 后再用 SSL 进行加密了。

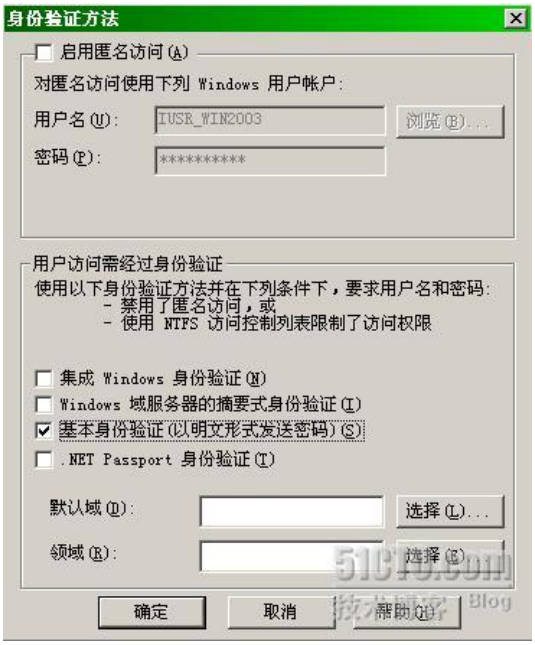
上次做 Exchange 的 OWA 发布时，我们把 Exchange 服务器证书导出给了 ISA 服务器，而且 ISA 服务器在侦听器中使用了 Exchange 的证书，如下图所示，这些我们在后续操作中都会用到。

4）配置 RPC 虚拟目录的身份验证

接下来需要配置 RPC 虚拟目录的验证方式，考虑到互联网上用户使用操作系统的多样性，我们准备使用兼容性最好的基本验证方式，虽然基本验证不对用户名和口令进行任何加

密保护，但好在 HTTPS 可以帮我们解决这个问题。如下图所示，在 Exchange 的 IIS 管理器中查看 RPC 虚拟目录属性，切换到目录属性的“目录安全性”标签，点击身份验证和访问控制处的“编辑”。

如下图所示，我们把 RPC 虚拟目录的身份验证方式改为“基本验证”。



5）创建 ISA 发布规则

准备工作就绪后，我们准备在 ISA 上创建发布规则了，我们只要通过发布规则把 Exchange 的 RPC 虚拟目录发布到 ISA 服务器外网网卡上就可以了。如下图所示，我们在 ISA 服务器上选择新建“Exchange Web 客户端访问发布规则”。

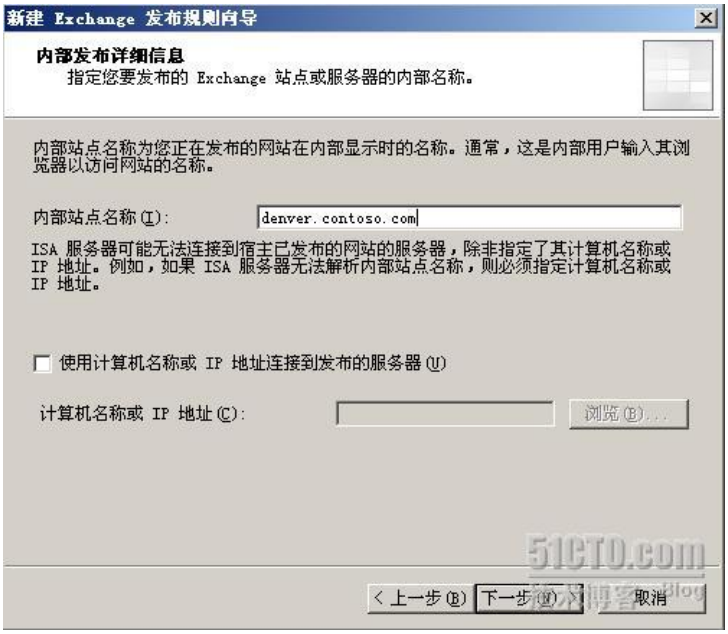
为发布规则取个名字。

选择 Exchange 服务器的版本号为 Exchange 2003，客户端访问类型是 Outlook RPC /HTTP(S)。

选择发布单个网站或负载平衡器。

利用 SSL 加密 ISA 与 Exchange 服务器之间的数据。

用完全合格域名 denver.contoso.com 来表示 Exchange 服务器。



Exchange 服务器的公用域名为 Denver.contoso.com，这些名称都和 Exchange 服务器证书中的计算机名称保持一致。

选择使用之前发布 Exchange OWA 时创建的 Web 侦听器，注意将身份验证方法改为基本验证。

ISA 服务器委派身份验证也使用基本身份验证。

此发布规则仅适用于通过身份验证的用户。

发布规则完成，此发布规则仅仅把 Exchange 服务器的 RPC 虚拟目录发布了出来。

6）配置 Outlook

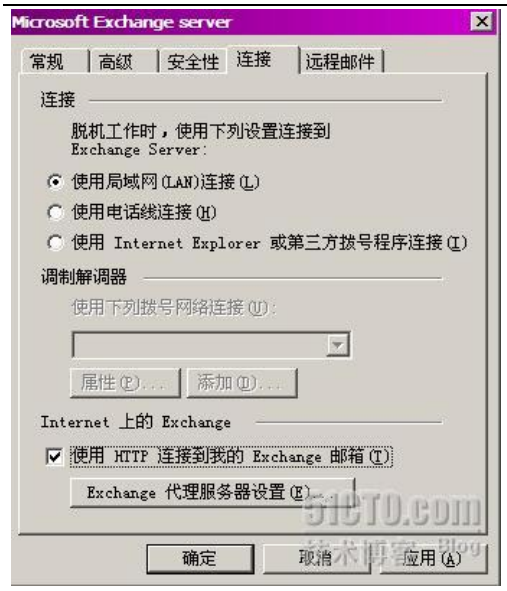
好了，最好我们要配置客户端的 Outlook，让 Outlook 把 RPC 数据封装为 HTTPS 格式。在 Istanbul 上 打开控制面板中的邮件，如下图所示，选择“电子邮件帐户”。

选择“查看或更改现有电子邮件帐户”。

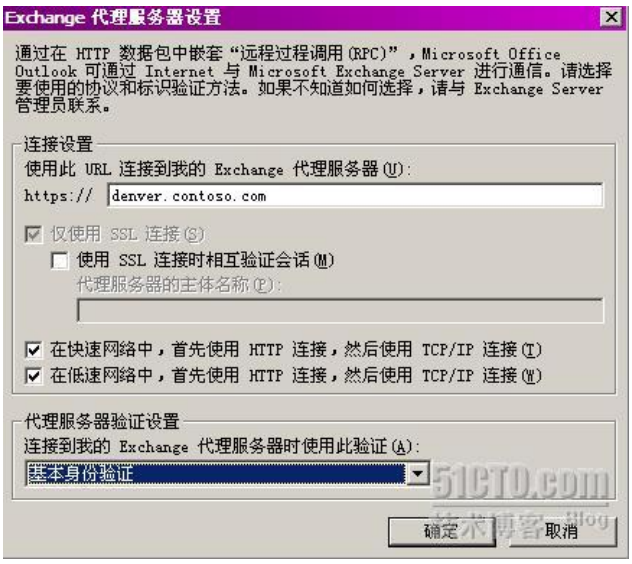
在电子邮件帐户的属性中点击“更改”。

点击下图中的“其他设置”。

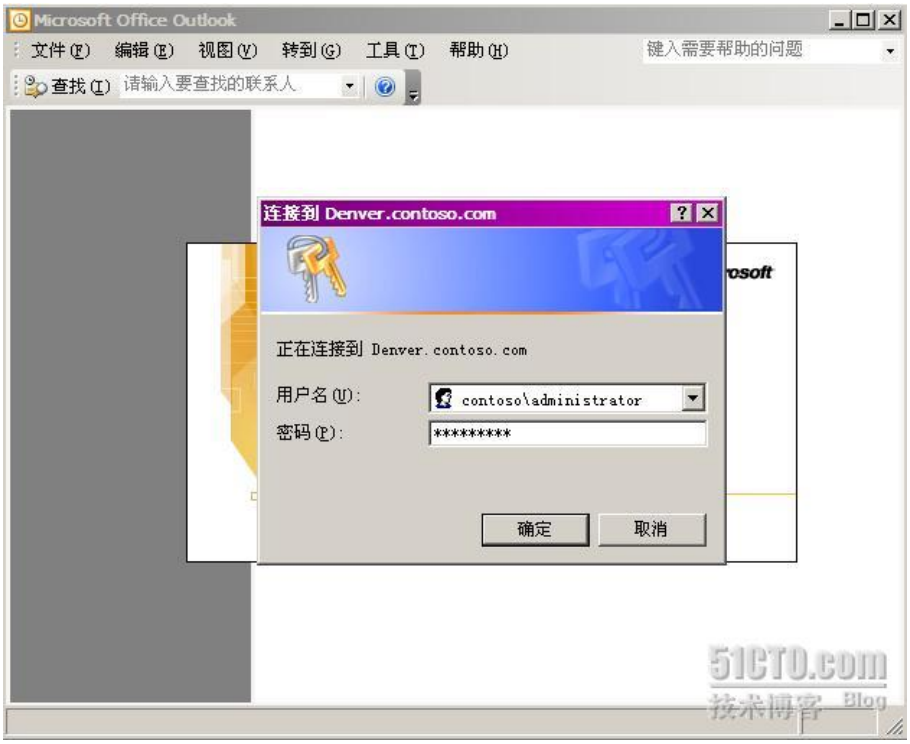
在其他设置中切换到“连接”标签，勾选“使用 HTTP 连接到我的 Exchange 邮箱”，点击“Exchange 代理服务器设置”。



如下图所示，在 Exchange 代理服务器设置中，输入 Exchange 代理服务器为 denver.contoso.com，选择无论是快速网络还是低速网络，都优先使用 HTTP 连接。身份验证方式为基本身份验证。

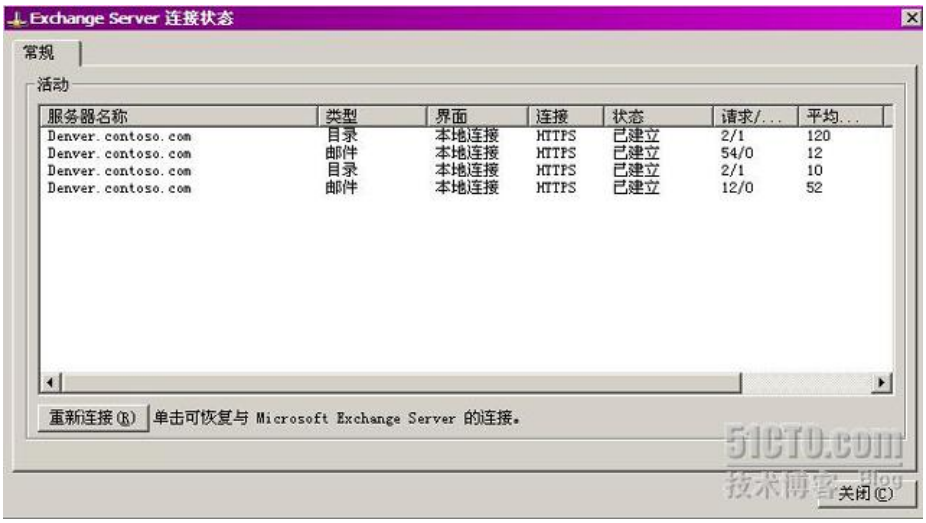


Outlook 更改完配置后，我们启动 Outlook 来访问一下，如下图所示，Outlook 要求进行身份验证，我们以 contosoadministrator 的身份进行身份验证。



身份验证通过后，进入了 Exchange 邮箱，按住 Ctrl 键，用右键点击屏幕右下角的 Outlook 图标，如下图所示，选择“连接状态”。

如下图所示，连接协议使用的是 HTTPS，这证明我们发布 RPC Over HTTPS 成功了！



用 Exchange 发布 RPC Over HTTPS 非常考验管理员的耐心，大家作此操作时一定要小心谨慎，尤其要注意证书和身份验证的问题。

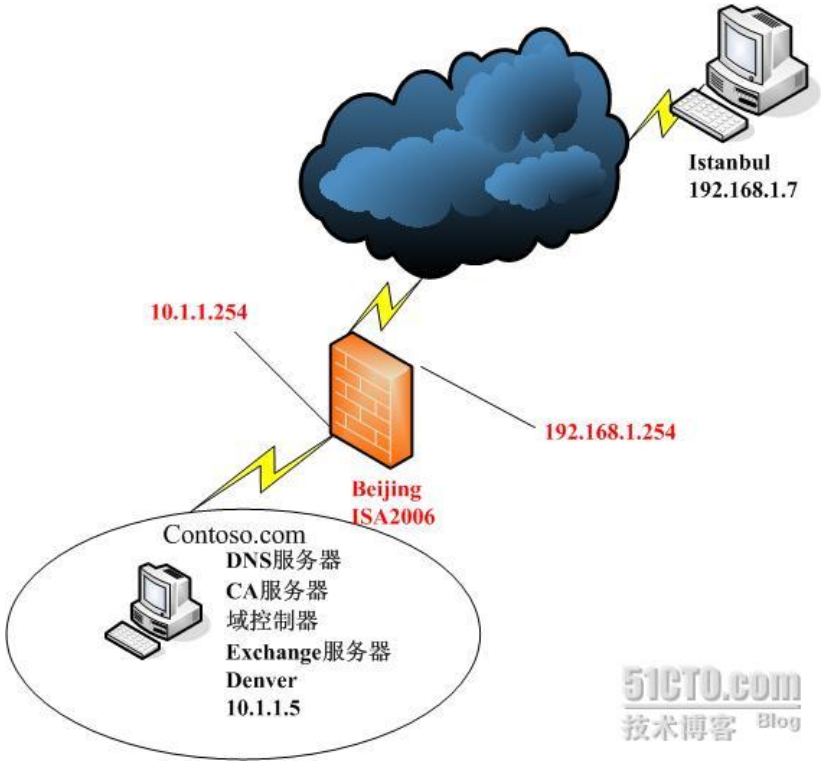
用 ISA2006 搭建 VPN 服务器：ISA2006 系列之二十

VPN 服务器在目前的网络中应用得越来越广泛，正在成为企业网络中不可或缺的角色，如何才能创建出自己的 VPN 服务器？怎么才能管理好 VPN 服务器？从今天起我们将组织一个 VPN 专题，系统地为大家介绍 VPN 服务器的配置和管理，内容包括 VPN 服务器的单点拨入，站点到站点的 VPN，VPN 用户隔离，VPN 结合 Radius 验证，VPN 接合智能卡和证书等。今天先就为大家介绍一下如何利用 ISA2006 来搭建一个自己的 VPN 服务器。

VPN 是虚拟专用网络的缩写，属于远程访问技术，简单地说就是利用公网链路架设似有网络。例如公司员工出差到外地，他想访问企业内网的服务器资源，这种访问就属于远程访问。怎么才能让外地员工访问到内网资源呢？VPN 的解决方法是在内网中架设一台 VPN 服务器，VPN 服务器有两块网卡，一块连接内网，一块连接公网。外地员工在当地连上互联网后，通过互联网找到 VPN 服务器，然后利用 VPN 服务器作为跳板进入企业内网。为了保证数据安全，VPN 服务器和客户机之间的通讯数据都进行了加密处理。有了数据加密，我们可以认为数据是在一条专用的数据链路上进行安全传输，就好像我们专门架设了一个专用网络一样。但实际上 VPN 使用的是互联网上的公用链路，因此只能称为虚拟专用网。这

下您肯定明白了，VPN 实质上就是利用加密技术在公网上封装出一个数据通讯隧道。有了 VPN 技术，用户无论是在外地出差还是在家中办公，只要能上互联网就能利用 VPN 非常方便地访问内网资源，这就是为什么 VPN 在企业中应用得如此广泛。上述介绍的 VPN 应用属于 VPN 用户的单点拨入，VPN 还有一种常见的应用是在两个内网之间架设站点到站点的 VPN，我们今天先介绍如何创建单点拨入的 VPN，站点到站点的 VPN 架设我们在后续博文中介绍。

实验拓扑如下，Denver 是内网的域控制器，DNS 服务器，CA 服务器，Beijing 是 ISA 2006 服务器，Istanbul 模拟外网的客户机。



51CTO.com
技术博客 Blog

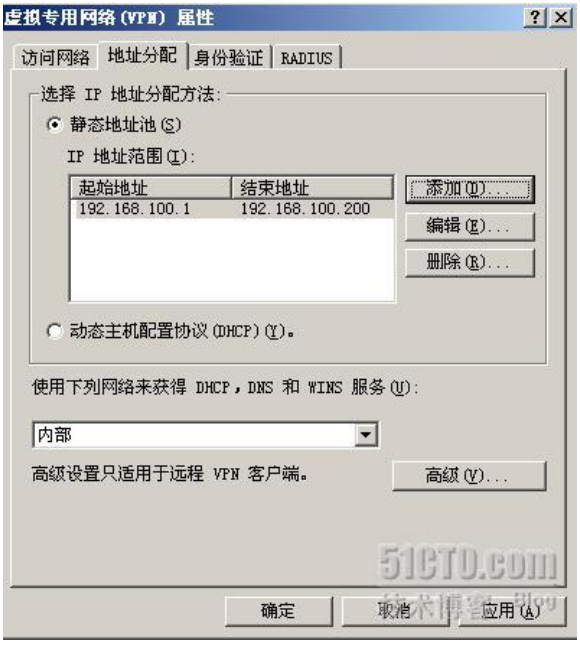
ISA2006 调用了 Win2003 中的路由和远程访问组件来实现 VPN 功能，但我们并不需要事先对 ISA 服务器上的路由和远程访问进行配置，ISA2006 会自动实现对路由和远程访问的调用。我们先来看看 ISA2006 如果要实现 VPN 功能需要进行哪些设置？

一 定义 VPN 地址池

配置 VPN 服务器的第一步就是为 VPN 用户分配一个地址范围，这里有个误区，很多人认为既然要让 VPN 用户能访问内网资源，那就给 VPN 用户直接分配一个内网地址就行了。例如本次实验的内网地址范围是 10.1.1.1－10.1.1.254，那 VPN 用户的地址池就放在 10.1.1.100－10.1.1.150 吧。如果你的 VPN 服务器是用 Win2003 的路由和远程实现的，那这么做是可以的，路由和远程访问本身就只提供了 VPN 的基本功能，对地址管理并不严格。但这么做在 ISA 上是不可以的，因为 ISA 是基于网络进行管理的！内网是一个网络，VPN 用户是另一个网络，两个网络的地址范围是不能重叠的！虽然我们使用 DHCP 技术可以使 VPN 用户也获得内网地址，但绝不推荐这么做！因为在后期的管理中我们会发现，把 VPN 用户放到一个单独的网络中，对管理员实现精确控制是非常有利的，管理员可以单独设定 VPN 用户所在网络与其他网络的网络关系，访问策略，如果把 VPN 用户和内网用户混在一起，就享受不到这种管理的便利了。因此直接给 VPN 用户分配内网地址并不可取，我们本次实验中为 VPN 用户设置的地址池是 192.168.100.1－192.168.100.200，虽然这个地址范围和内网大不相同，但不用担心，ISA 会自动在两个网络之间进行路由。

如下图所示，在 ISA 服务器中定位到虚拟专用网络，点击右侧任务面板中的“定义地址分配”。

分配地址可以使用静态地址，也可以使用 DHCP，在此我们使用静态地址池来为 VPN 用户分配地址，点击添加按钮，为 VPN 用户分配的地址范围是 192.168.100.1－192.168.100.200，如下图所示。

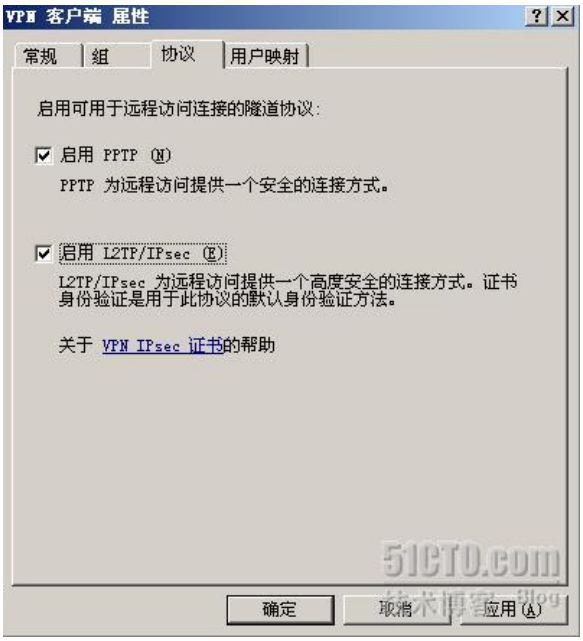


二 配置 VPN 服务器

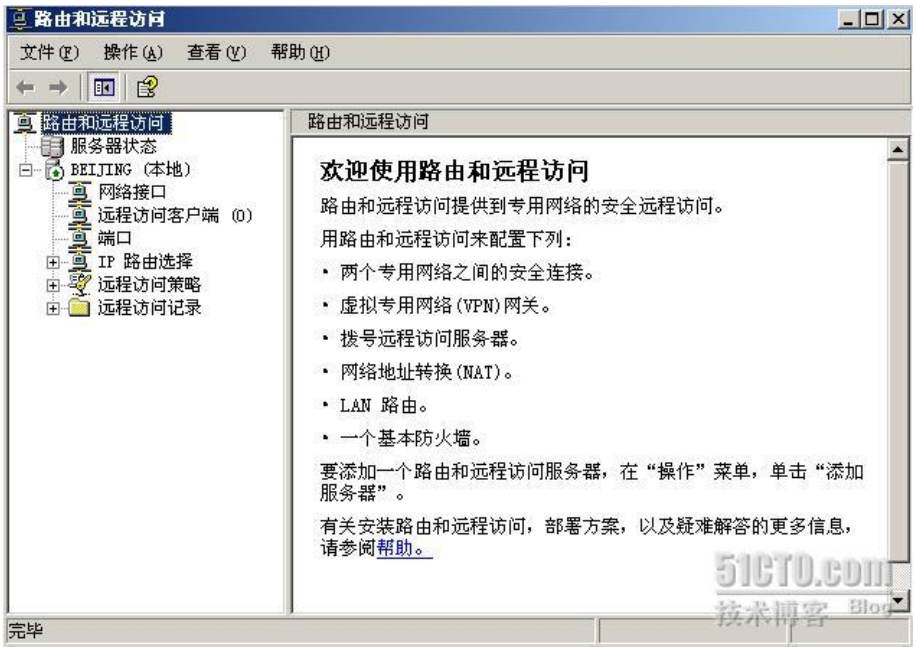
设置好了 VPN 地址池后，我们来配置 VPN 服务器的客户端设置。如下图所示，点击虚拟专用网络右侧任务面板中的“配置 VPN 客户端访问”。在常规标签中，我们勾选“启用 VPN 客户端访问”，同时设置允许最大的 VPN 客户端数量为 100.，注意 VPN 客户端的最大数量不能超过地址池中的地址数。

切换到 VPN 客户端属性的“组”标签，配置允许远程访问的域组，一般情况下，管理员会事先创建好一个允许远程访问的组，然后将 VPN 用户加入这个组，本次实验中我们就简单一些，直接允许 Domain Users 组进行远程访问。

接下来选择 VPN 使用的隧道协议，默认选择是 PPTP 协议，我们把 L2TP 也选择上。设置完 VPN 客户端访问后，我们应重启 ISA 服务器，让设置生效。



重启 ISA 服务器之后，如下图所示，我们发现 ISA 服务器的路由和远程访问已经自动启动了。



三 网络规则

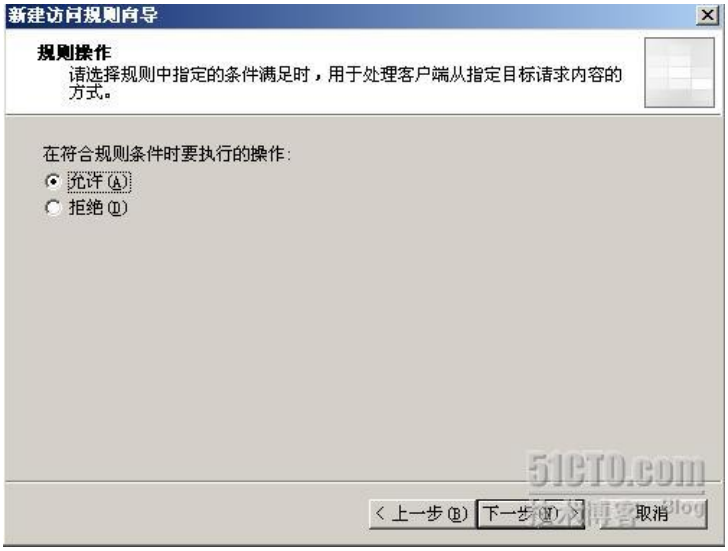
想让 VPN 用户访问内网，一定要设置网络规则和防火墙策略，ISA 默认已经对网络规则进行了定义，如下图所示，从 VPN 客户端到内网是路由关系，这意味着 VPN 客户端和内网用户互相访问是有可能的。

四 防火墙策略

既然网络规则已经为 VPN 用户访问内网开了绿灯，那我们就可以在防火墙策略中创建一个访问规则允许 VPN 用户访问内网了。当然，如果需要的话，也可以在访问规则中允许内网访问 VPN 用户。如下图所示，在防火墙策略中选择新建“访问规则”。

为访问规则取个名字。

当访问请求匹配规则时允许操作。



此规则可以应用到所有的通讯协议。

规则的访问源是 VPN 客户端网络。

访问规则的目标是内网。

此规则适用于所有用户。

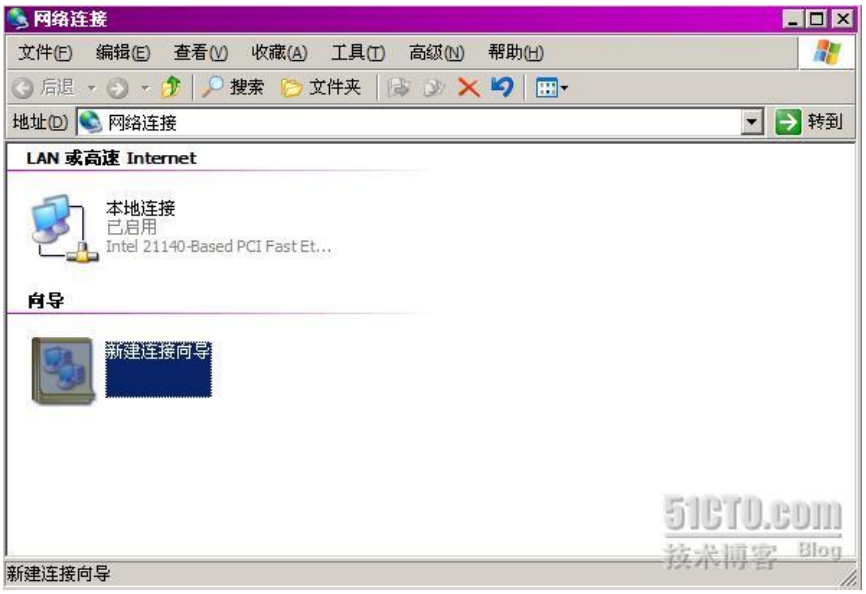
完成向导，好了，现在 ISA 已经允许 VPN 用户拨入了。

五　用户拨入权限

最后一步不要忘记，域用户默认是没有远程拨入权限的，我们准备以域管理员的身份拨入，如下图所示，在 Active Directory 用户和计算机中打开 administrator 的属性，切换到“拨入”标签，如下图所示，设置拨入权限为“允许访问”。

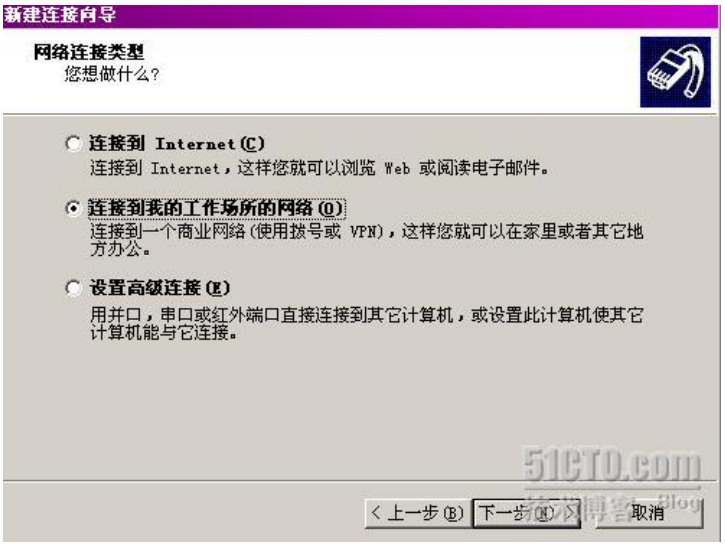
好，至此为止，VPN 服务器已经配置完毕了，接下来我们用客户机来测试一下，看看能够通过 VPN 服务器拨入内网。ISA 支持 PPTP 和 L2TP 两种隧道协议，今天我们在客户机上先对 PPTP 协议进行测试。

在 Istanbul 客户机上打开网上邻居的属性，如下图所示，点击新建连接向导。

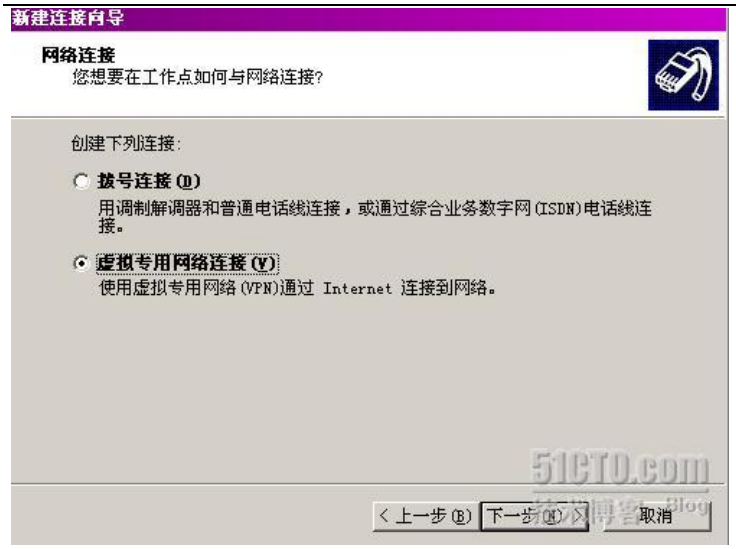


出现新建连接向导，点击下一步。

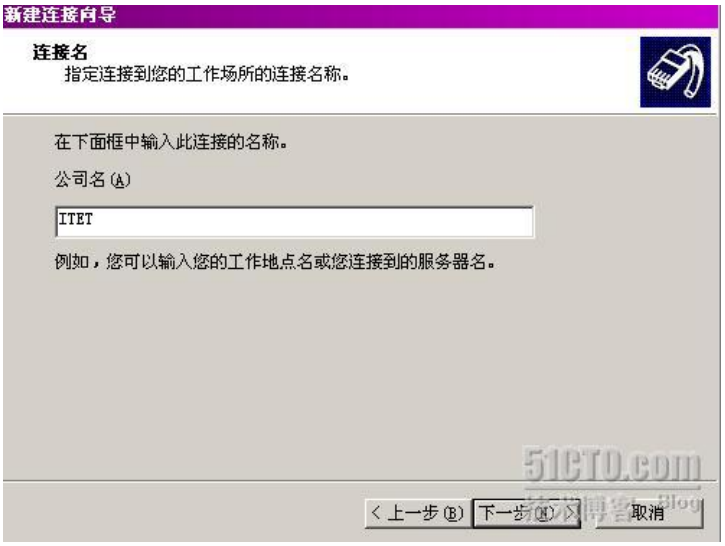
网络连接类型选择“连接到我的工作场所的网络”。



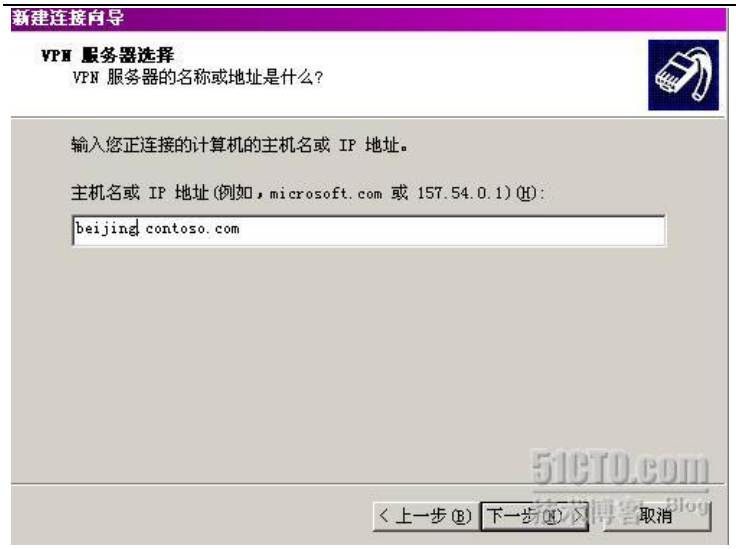
选择创建“虚拟专用网络连接”。



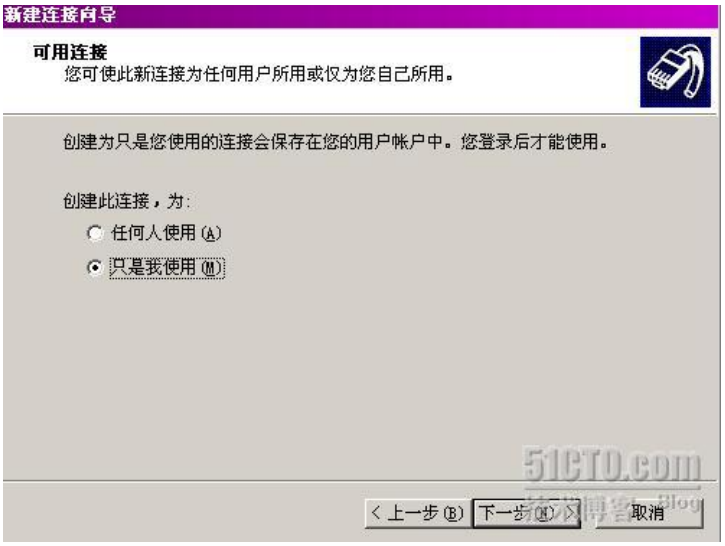
在 VPN 连接中输入公司名称。



输入 VPN 服务器的域名或外网 IP，此例中我们使用域名，注意此域名应该解析到 ISA 的外网 IP，192.168.1.254.。



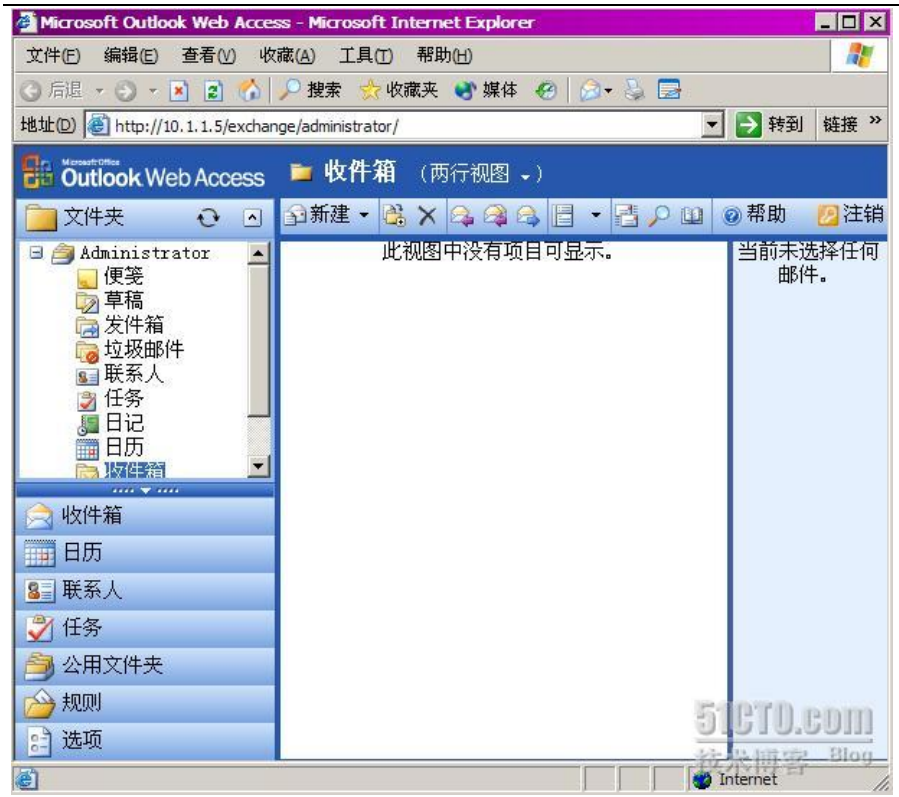
选择此连接“只是我使用”，点击下一步后结束连接向导创建。



双击执行刚创建出来的 VPN 连接，如下图所示，输入用户名和密码，点击“连接”。

输入的用户名和口令通过了身份验证，VPN 连接成功，查看 VPN 连接的属性，如下图所示，我们可以看到当前使用的隧道协议是 PPTP，VPN 客户机分配到的 IP 地址是 192.168.100.4，地址池中的第一个地址总是保留给 VPN 服务器，这个地址被成为隧道终点，也是 VPN 用户连接内网所使用的网关。

既然 VPN 用户已经通过 VPN 服务器进行了拨入，看看能否访问内网的服务器资源，如下图所示，在 Istanbul 上可以成功访问内网的 Exchange 服务器，VPN 拨入成功！



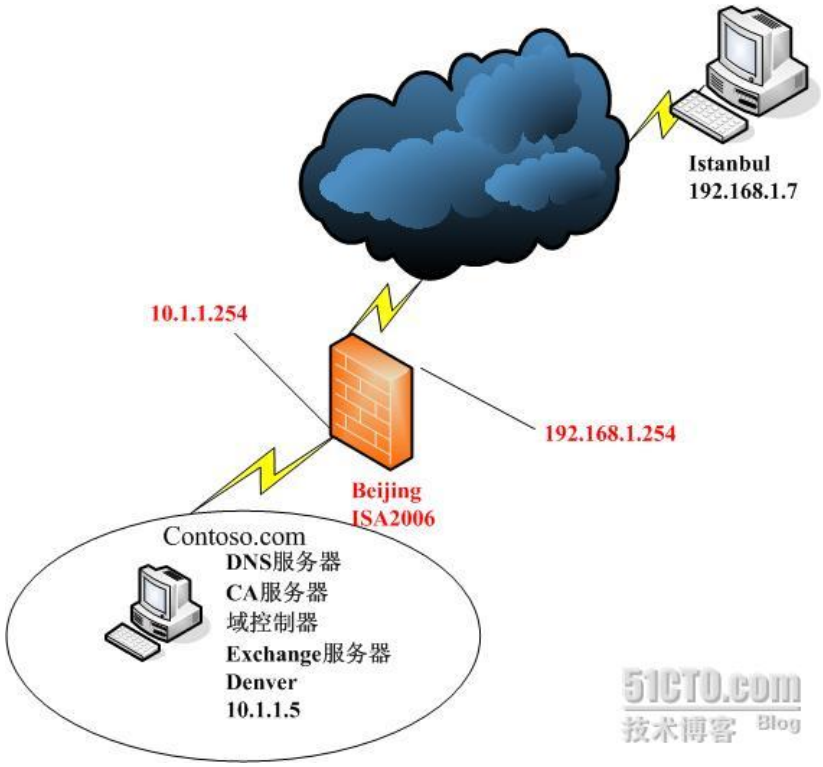
今天我们只是搭建了一个简单的 VPN 服务器，测试了一下客户机使用 PPTP 协议进行拨入，在后续的博文中我们将以今天的环境为基础，把 VPN 的应用推向深入。

配置 VPN 服务器中的 L2TP/IPSEC：ISA2006 系列之二十一

上篇博文中我们介绍了如何使用 ISA2006 来搭建一个 VPN 服务器，我们在 ISA2006 中配置了 VPN 地址池，选择了 VPN 协议，创建了防火墙策略，检查了网络规则，还赋予了用户远程拨入权限。等 VPN 服务器搭建完毕后，我们又利用客户端对 VPN 服务器进行了连接测试，测试的结果令人满意，我们拥有了自己的 VPN 服务器。只是在上次实验中，客户端访问 VPN 服务器时使用的是 PPTP 协议，但 VPN 服务器支持 PPTP 和 L2TP/IPSEC 两种协议，因此在本篇博文中我们将在客户机上测试使用 L2TP/IPSEC 协议访问 VPN 服务器。

L2TP/IPSEC 从字面上理解是在 IPSEC 上跑 L2TP，IPSEC 负责数据的封装加密，L2TP 的作用和 PPTP 类似，负责在 IP 网络上做出 VPN 隧道。从理论上分析 L2TP 协议应该

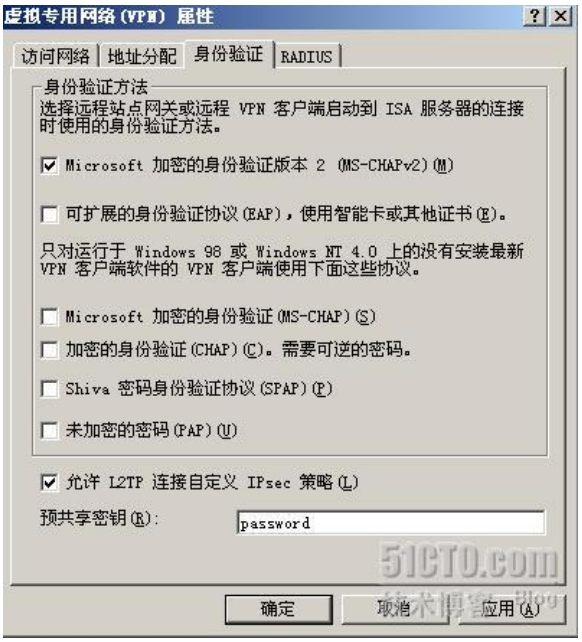
比 PPTP 更安全一些，因为 L2TP 不但能在用户级别实现 PPP 验证，还能实现计算机级别的身份验证；而 PPTP 只考虑了对 VPN 用户的身份验证，不支持对计算机身份进行验证。L2TP 验证计算机身份可以使用两种方法，预共享密钥和证书。预共享密钥比较简单，只要在 VPN 服务器和客户机上使用约定好的密码就可以证实彼此计算机身份，当然安全性也只能说很一般。证书验证则依靠从 CA 申请的计算机证书来证明身份，由于证书的高安全性，这种验证方法在安全方面是令人满意的。下面我们把两种方法都通过实验实现一下，实验拓扑和上篇博文完全相同。



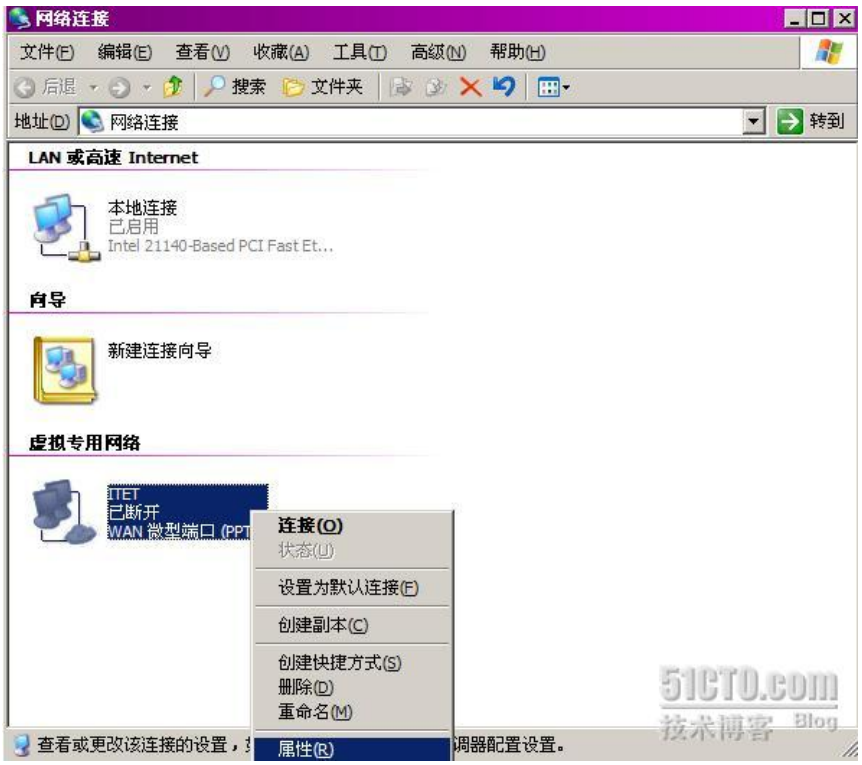
一 预共享密钥

预共享密钥需要在 VPN 服务器和 VPN 客户机上设置一个共同约定的密钥作为身份识别标识，首先我们在 VPN 服务器上进行设置。在 ISA 的管理工具中展开虚拟专用网络，如下图所示，点击右侧面板中的“选择身份验证方法”。

切换到“身份验证”标签，如下图所示，勾选“允许 L2TP 连接自定义 IPSEC 策略”，输入“password”作为预与共享密钥。



VPN 服务器为 L2TP 设置了预共享密钥后，接下来我们在 VPN 客户机上进行预共享密钥的设置，如下图所示，在 Istanbul 的网上邻居属性中，右键点击上篇博文中创建的 VPN 连接“ITET”，选择“属性”。



在 VPN 属性中切换到“网络”标签，选择 VPN 类型是“L2TP IPSEC VPN”。

再在 VPN 属性中切换到“安全”标签，点击“IPSEC 设置”。

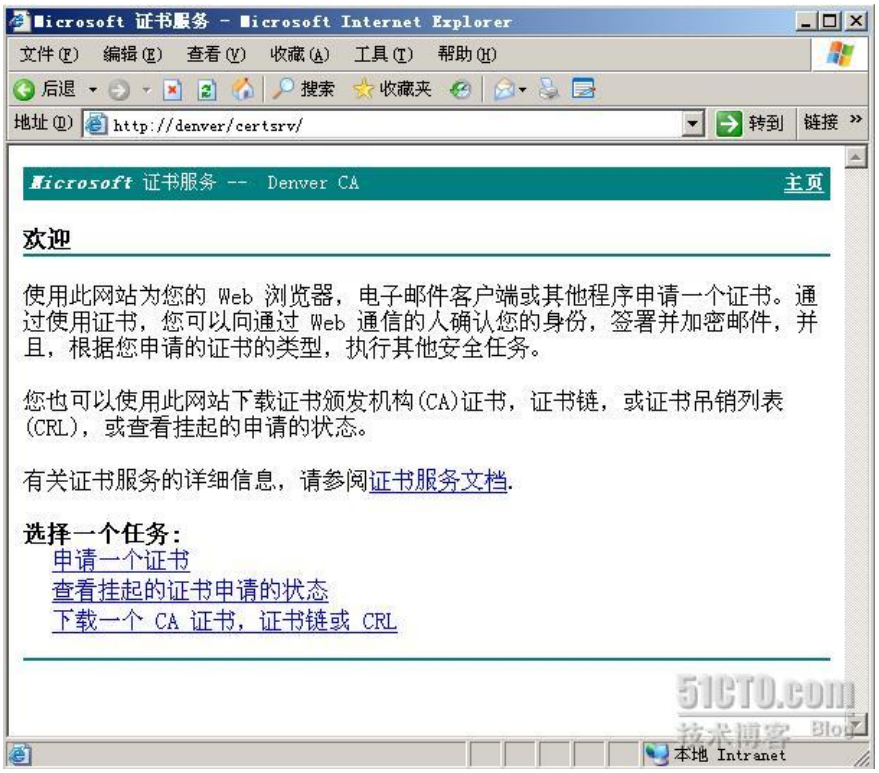
如下图所示，勾选“使用预共享的密钥作身份验证”，输入密钥的值“password”。

在服务器端和客户端都进行预共享密钥设置后，如下图所示，在 Istanbul 上点击“连接”，准备连接到 VPN 服务器。

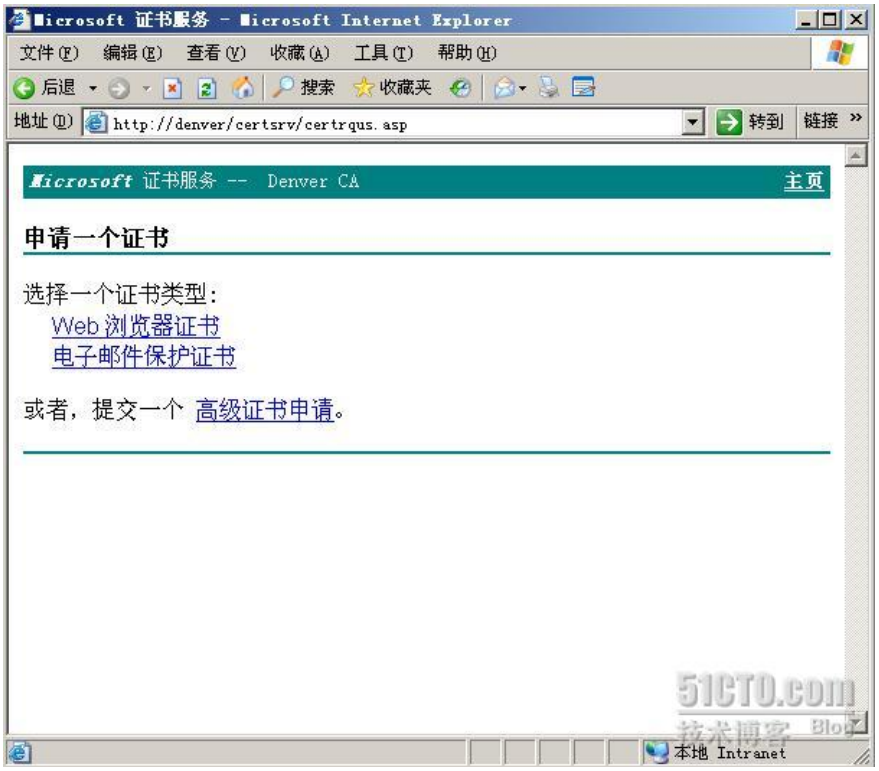
VPN 连接成功后，查看 VPN 连接属性，如下图所示，我们看到当前使用的 VPN 协议是 L2TP。

二　证书

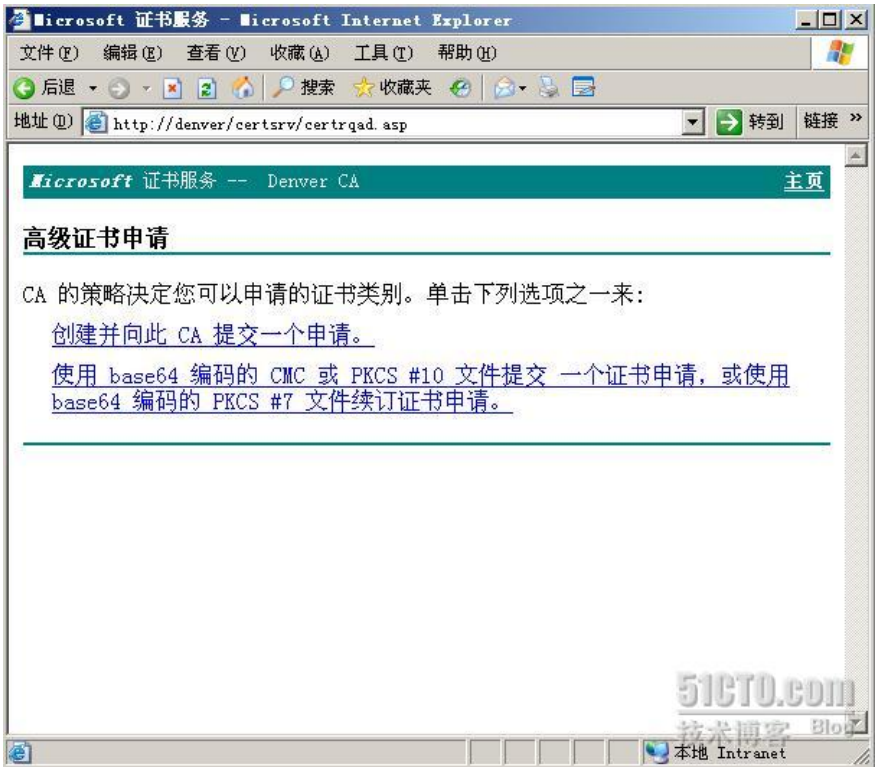
使用预共享密钥方法简单，但安全性不高，接下来我们使用证书验证计算机身份，安全性会有很大提高。使用证书验证计算机身份，VPN 服务器需要申请服务器证书，VPN 客户机需要申请客户端证书。在目前的实验环境中，内网的 Denver 是证书服务器，类型是独立根，已经被实验用到的所有计算机信任。首先我们在 ISA 服务器上申请一个服务器证书，如下图所示，在 ISA 服务器的浏览器中输入 http://denver/certsrv，在证书申请页面中选择“申请一个证书”。


Microsoft 证书服务 -- Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://denver/certsrv/
转到 链接
Microsoft 证书服务 -- Denver CA
主页
欢迎
使用此网站为您的 Web 浏览器，电子邮件客户端或其他程序申请一个证书。通过使用证书，您可以向通过 Web 通信的人确认您的身份，签署并加密邮件，并且，根据您申请的证书的类型，执行其他安全任务。
您也可以使用此网站下载证书颁发机构(CA)证书，证书链，或证书吊销列表(CRL)，或查看挂起的申请的状态。
有关证书服务的详细信息，请参阅证书服务文档.
选择一个任务：
申请一个证书
查看挂起的证书申请的状态
下载一个 CA 证书，证书链或 CRL
本地 Intranet

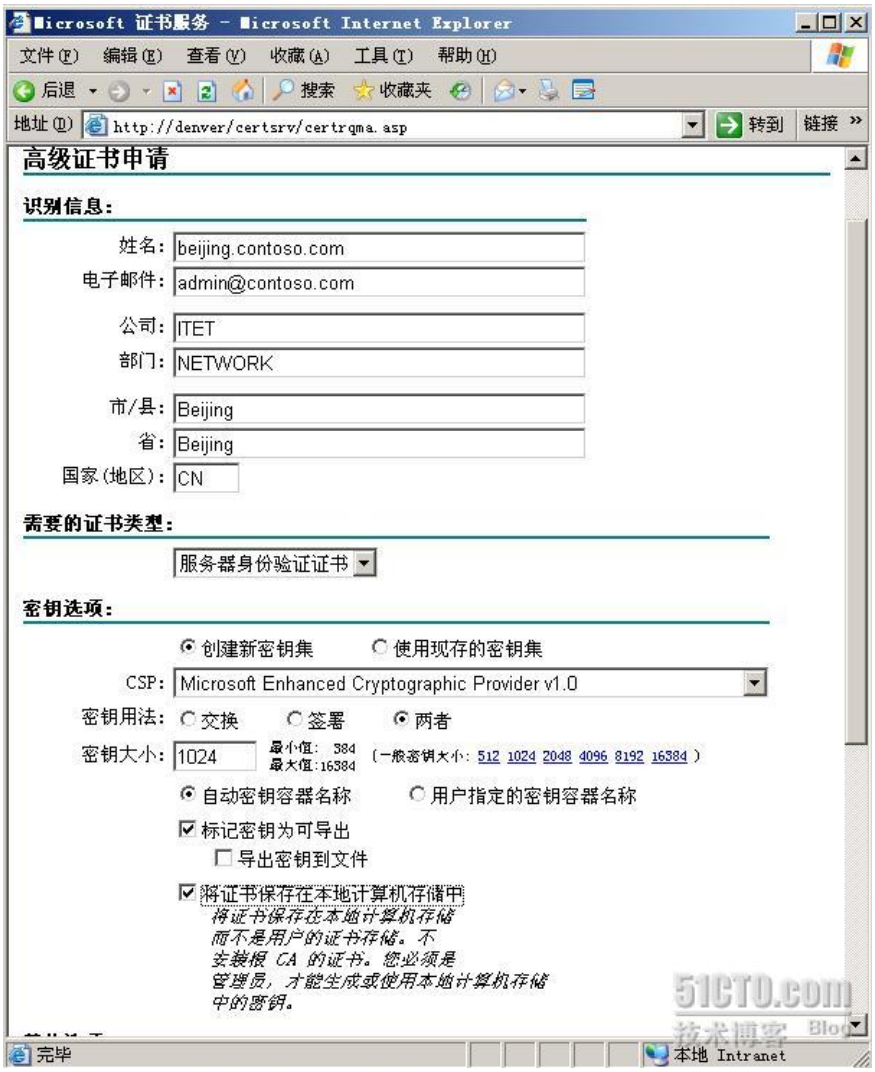
选择“高级证书申请”。


Microsoft 证书服务 -- Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://denver/certsrv/certrqus.asp
转到 链接
Microsoft 证书服务 -- Denver CA
主页
申请一个证书
选择一个证书类型：
Web 浏览器证书
电子邮件保护证书
或者，提交一个 高级证书申请。
本地 Intranet

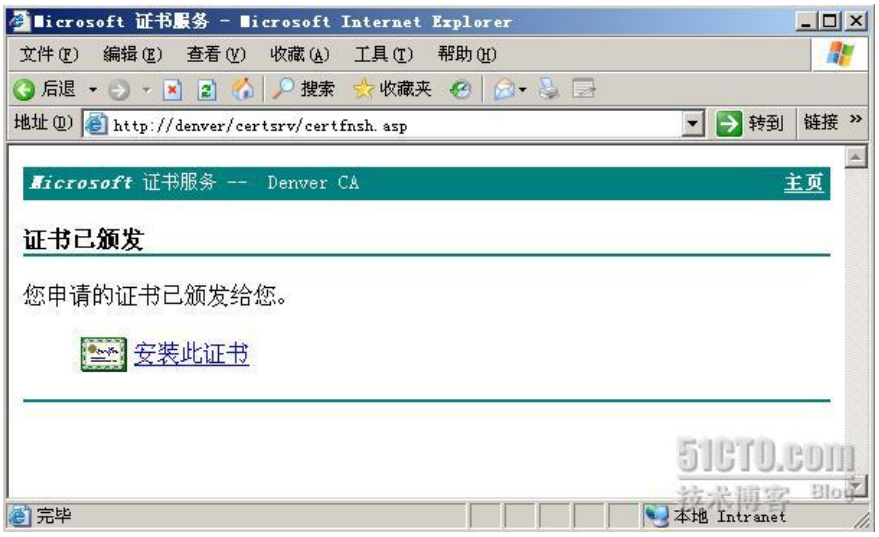
选择“创建并向此 CA 提交一个申请”。



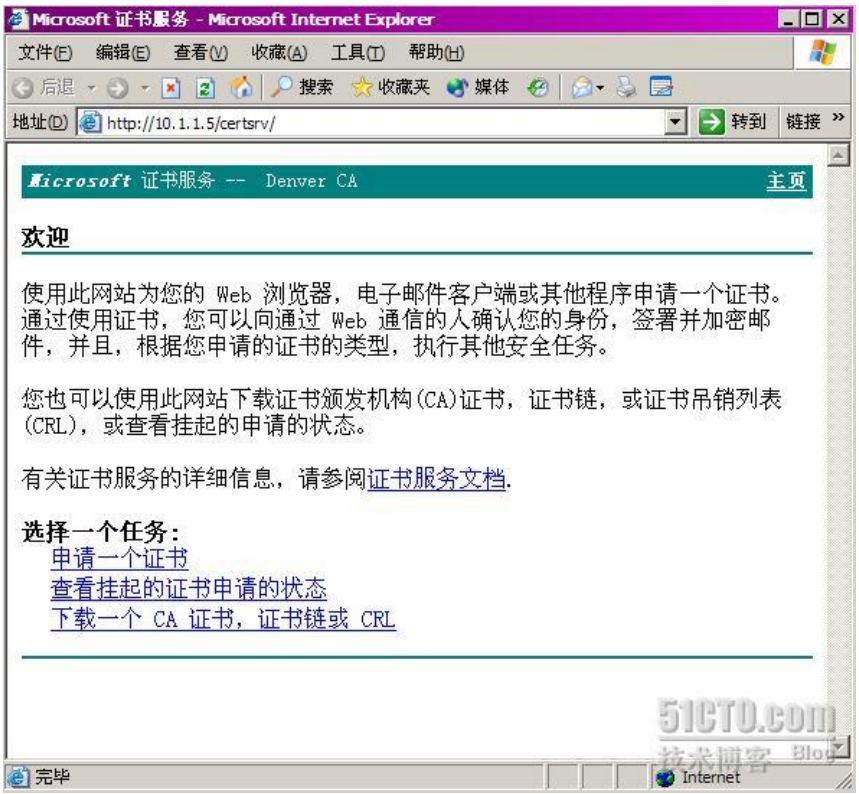
如下图所示，输入证书申请的参数，由于此 CA 类型是独立根，因此需要输入的参数和企业根有所不同。证书姓名中我们输入了 VPN 服务器的域名 Beijing.contoso.com，我们选择的证书类型是“服务器身份验证证书”，然后选择将证书保存在本地计算机存储中，其他参数随便输入即可。



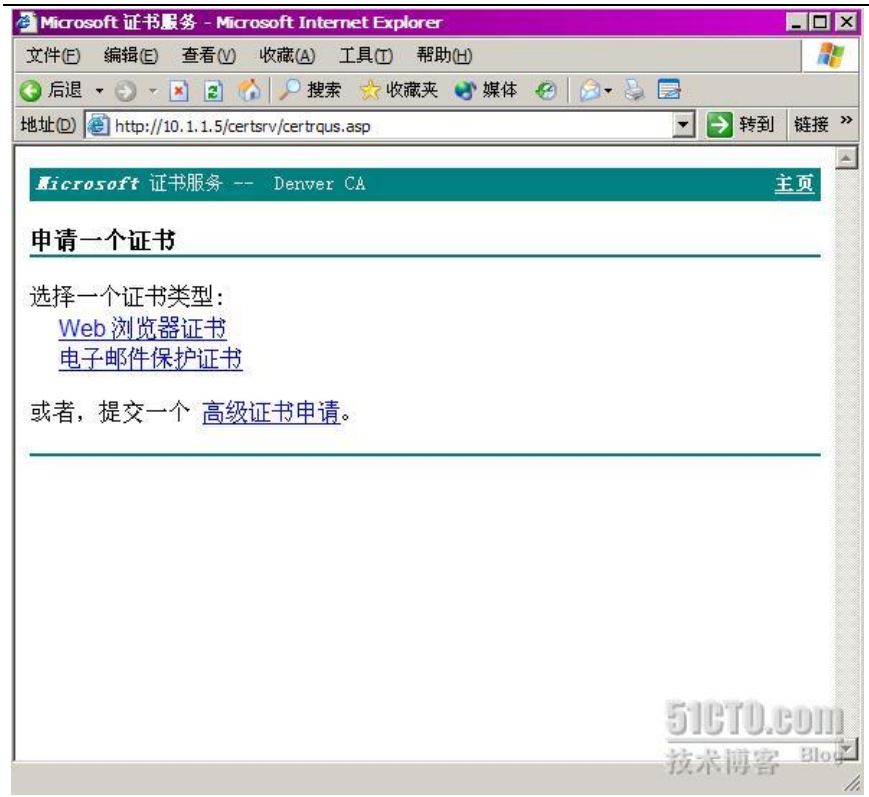
提交申请后，证书服务器颁发了证书，如下图所示，我们选择“安装此证书”即可完成证书申请工作。注意，独立根 CA 默认是需要管理员审核才能进行证书核发，我们修改了独立根 CA 的策略模块，让 CA 服务器可以自动发放证书。



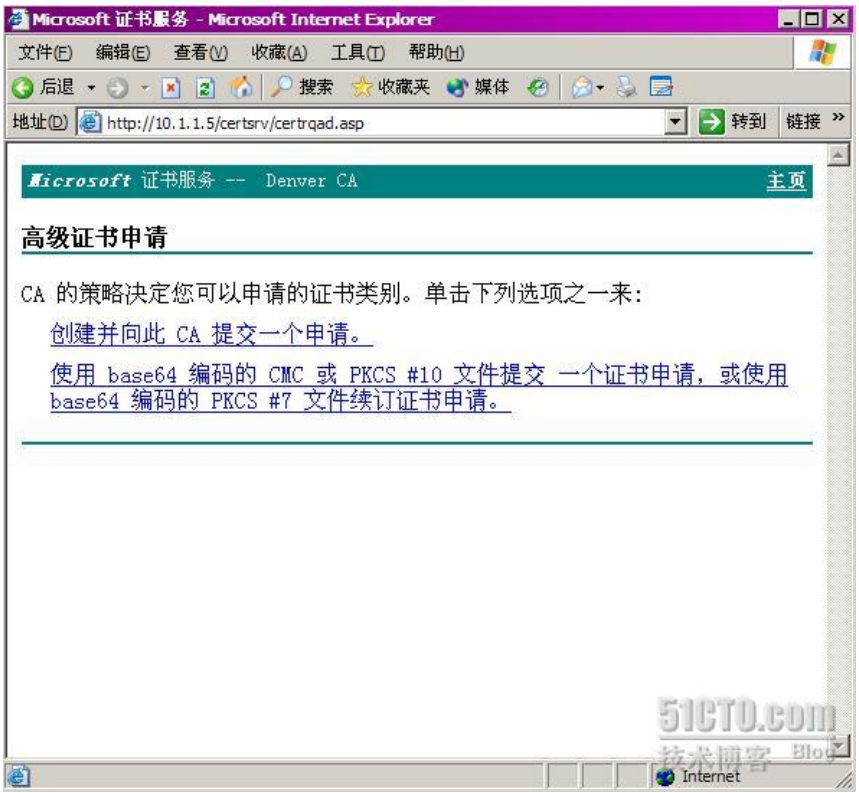
VPN 服务器申请完服务器证书后，接下来我们在 Istanbul 上申请客户端证书，首先让 Istanbul 用 PPTP 协议拨入 VPN 服务器，然后就可以访问内网的 CA 服务器了，如下图所示，在 Istanbul 的浏览器中输入 http://10.1.1.5/certsrv，选择“申请一个证书”。



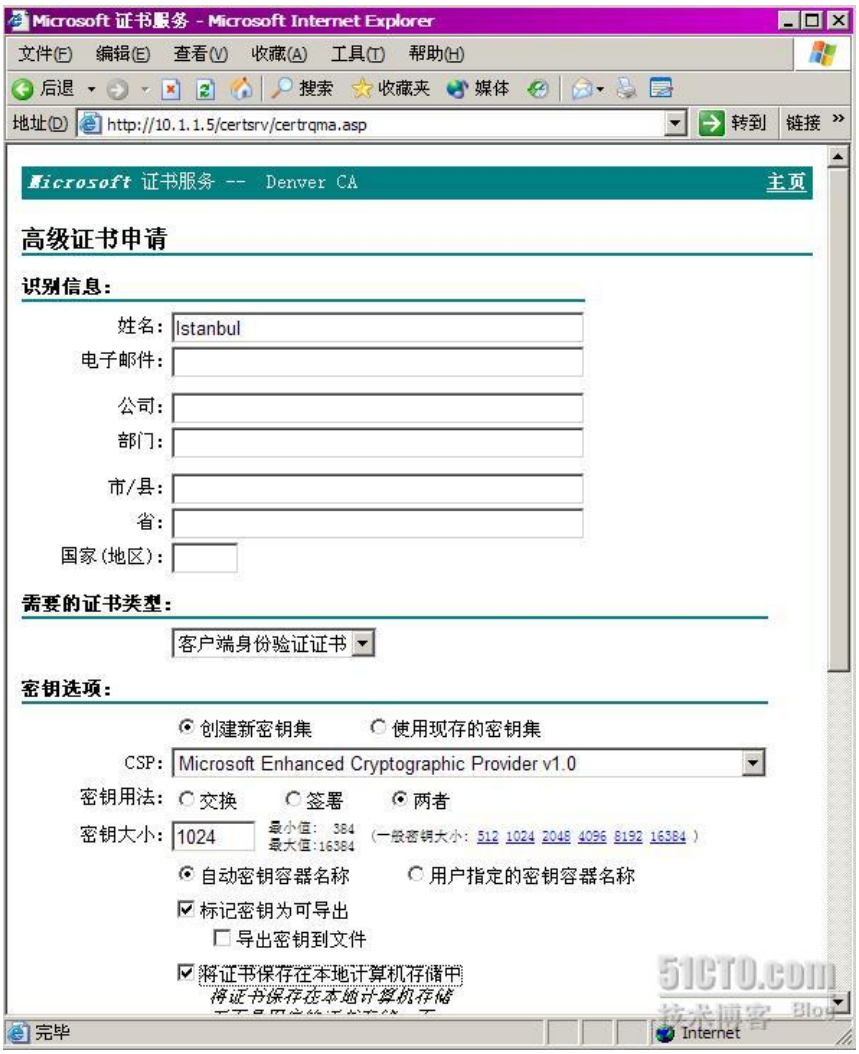
选择提交一个“高级证书申请”。



选择“创建并向此 CA 提交一个申请”，通过表单提交证书申请。

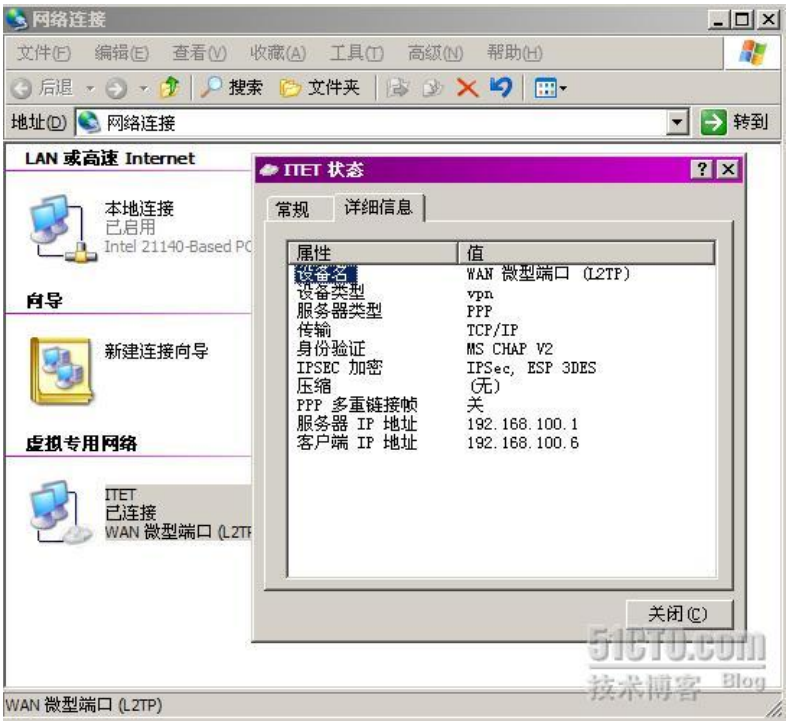


如下图所示，我们选择申请的证书类型是“客户端身份验证证书”，姓名是“Istanbul”，将证书保存在计算机存储中。



提交申请后，CA 自动颁发证书，如下图所示，我们在 Istanbul 上安装了颁发的证书。至此，我们在 VPN 的服务器端和客户端都完成了证书申请，接下来我们分别取消 VPN 服务器端和客户端的预共享密钥设置，重新在 Istanbul 上用 L2TP 连接 VPN 服务器，看是否能够使用证书进行计算机身份验证。

如下图所示，VPN 拨入成功，这次就不是利用预共享密钥而是利用证书验证了，虽然用户使用起来感觉差别不大，其实安全性方面还是改进了许多。

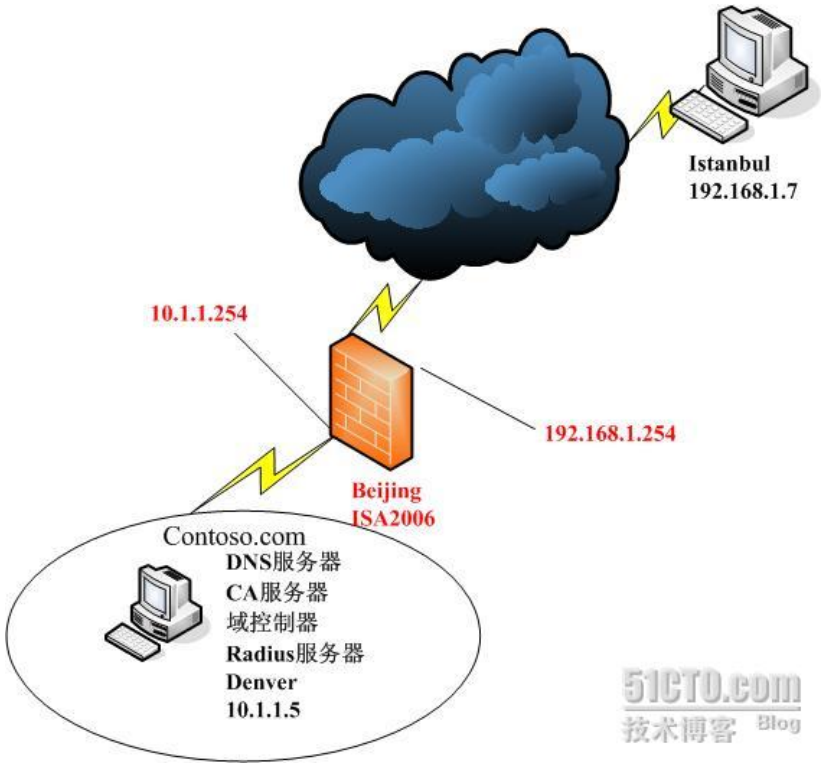


详解 Radius 服务器在 VPN 中的应用：ISA2006 系列之二十二

在前面的博文中，我们介绍了如何利用 ISA2006 创建 VPN 服务器，以及对 VPN 服务器使用的 PPTP 和 L2TP 协议都进行了介绍，今天我们来介绍一种经常和 VPN 配合使用的身份验证服务器－Radius 服务器。

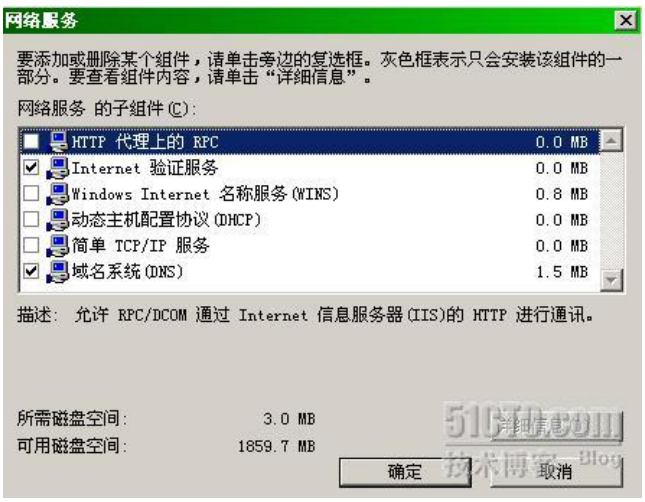
Radius 是 Remote Authentication Dial In User Service 的缩写，意思是远程用户拨号认证服务。Radius 原本设计用于对拨号用户进行身份验证和计费，这些功能经常被电信部门所使用，我们拨号上网后收到的账单就是 Radius 服务器统计出来的。Radius 使用一段时间后，大家发现 Radius 协议功能强大，使用方便且易于扩充，因此经过改进后，Radius 现已成为国际通用的认证计费协议，广泛使用在普通电话上网、ADSL 上网、小区宽带上网、IP 电话等多种场合。

有了 Radius 这样一个专业的认证服务器，VPN 就轻松多了。VPN 服务器只需成为 Radius 客户端，然后把 VPN 用户发来的身份验证凭据转发到 Radius 服务器，自己就可以坐等结果通知了。这样一来 VPN 服务器可以从身份验证工作中解脱出来，专心干好自己的本职工作。而 Radius 服务器也可以发挥自己的专业优势，让用户身份验证能够使用智能卡，双因子验证等高级技术。下面我们先举一个例子，向大家介绍一下 Radius 的应用。如下图拓扑所示，Beijing 是一个工作组环境下的 ISA 服务器，按理说无法对域用户进行身份验证。但我们在域控制器 Denver 上安装了一个 Radius 服务器。这样一来 ISA 服务器只要把域用户发来的验证请求转交给 Radius 服务器，就能通过 Radius 服务器对访问者进行域用户验证，这样是不是很方便呢？顺便说一下，有些硬件防火墙也可以通过 Radius 来对域用户提供支持。



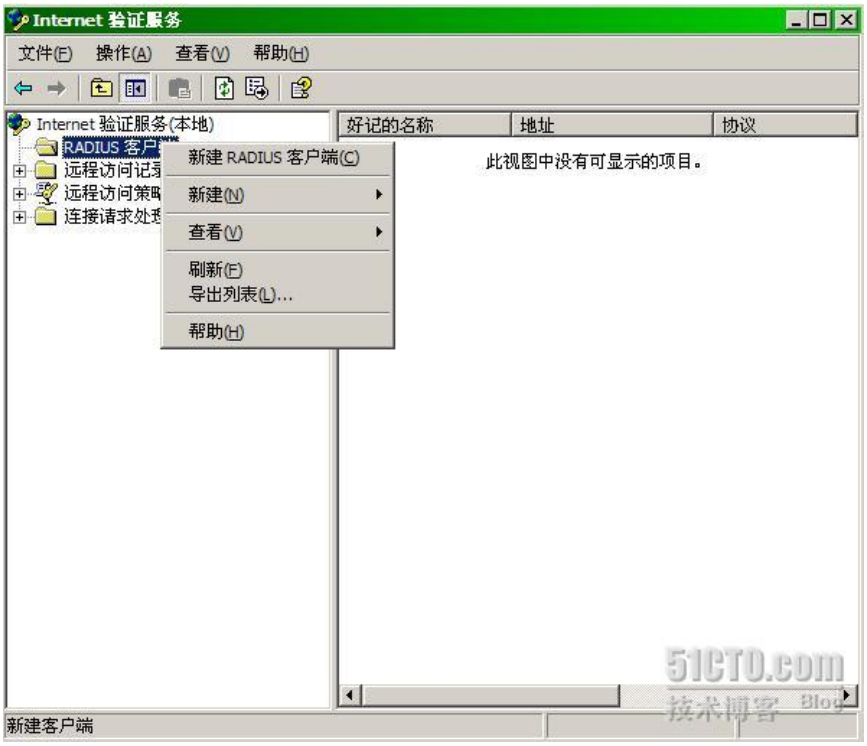
一 Radius 服务器安装

首先我们在 Denver 上安装 Radius 服务器，Radius 服务器并不一定要安装在域控制器上，我们在此完全是为了实验方便才把 Radius 和域控制器集于一身。在 Denver 上依次点击 控制面板－添加或删除程序－添加 / 删除 Windows 组件，如下图所示，选择网络服务组件中的“Internet 验证服务”，点击确定后我们就可以在 Denver 上安装 Radius 服务了。



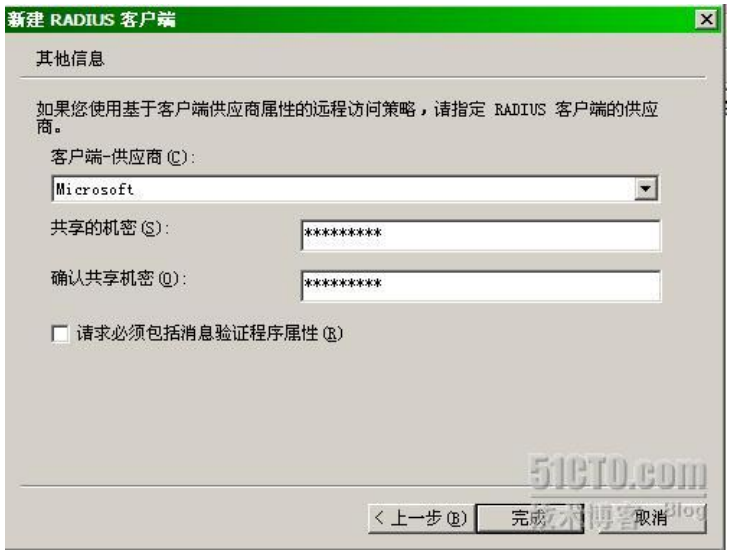
二 Radius 服务器添加客户端

想利用 Radius 服务器对访问者进行身份验证，ISA 首先得成为 Radius 的客户端，下面我们就在 Radius 服务器中把 ISA 服务器添加为客户端。在 Denver 上依次点击 开始－程序－管理工具－Internet 验证服务，如下图所示，右键“点击 Radius 客户端”，选择“新建 Radius 客户端”。

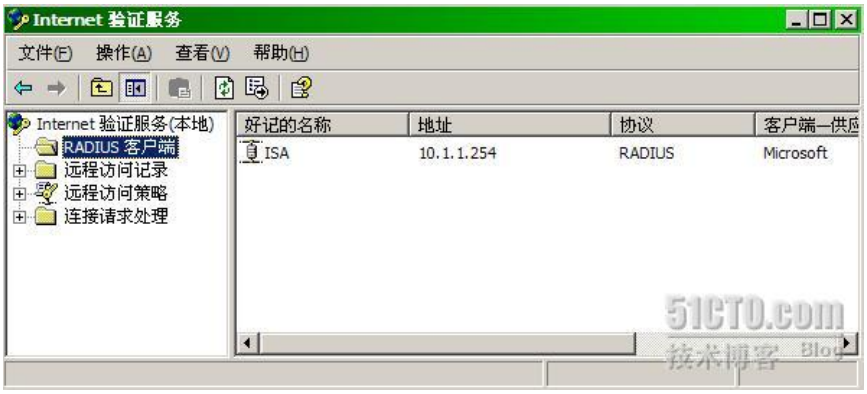


为 Radius 客户端配置一个易于记忆的名字，并填写客户端的 IP。

接下来在客户端-供应商类型中应选择“Microsoft”，注意设置 Radius 服务器和客户端的共享密码。Radius 服务器和客户端依靠这个密码进行彼此的身份验证。这个密码并不在网络上传递，如果 Radius 服务器认为有必要，还会使用挑战/响应的机制向 Radius 客户端提出身份验证请求。具体就是 Radius 服务器生成一个随机字符串，然后用这个共享口令加密，然后把加密后的密文传给客户端，要求客户端对密文解密后再回传给服务器，如果客户端回送的内容和原始的随机字符串一样，那客户端的身份就得到了认可。



如下图所示，Radius 服务器已经把 ISA 服务器添加成了客户端。



三 配置使用 Radius 服务器

Radius 服务器已经把 ISA 服务器添加成了客户端，那我们接下来就需要在 ISA 服务器上配置使用 Radius 服务器进行身份验证。如下图所示，在 ISA 的管理工具中定位到“虚拟专用网络”，点击右侧面板中的“指定 Radius 配置”。

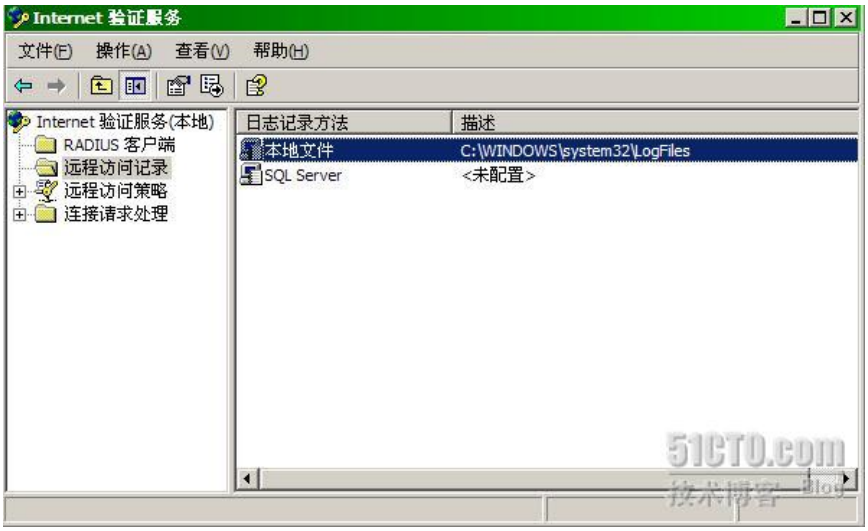
如下图所示，我们勾选“使用 Radius 进行身份验证”以及“使用 Radius 记账”，然后点击“Radius 服务器”。

点击下图中的“添加”按钮，添加 Radius 服务器的配置。

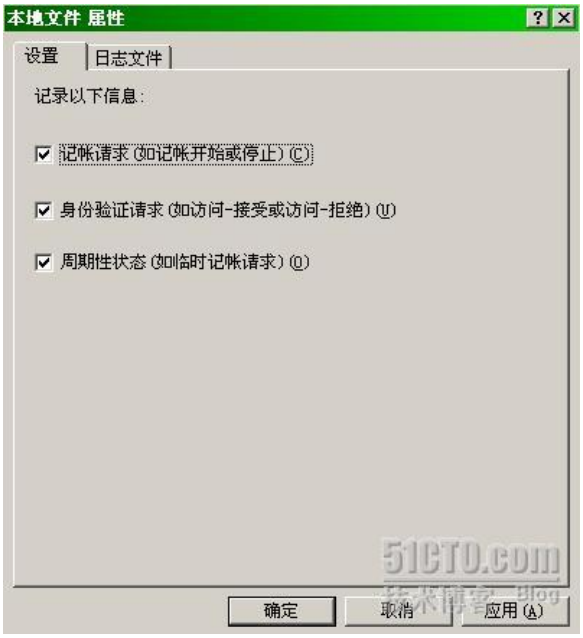
如下图所示，我们在服务器名中填写了 Radius 服务器的完全合格域名，在共享的机密中点击“更改”按钮，填写了 Radius 服务器设置的共享密码，点击确定后完成 Radius 服务器的配置。

四 配置 Radius 服务器启用日志

由于在 ISA 服务器中配置了使用 Radius 服务器进行记账，因此我们在 Radius 服务器中启用日志功能。在 Denver 的管理工具中打开 Internet 验证，点击“远程访问记录”，如下图所示，我们可以选择使用文件记录或数据库记录，今天我们只是简单地实验一下，因此选择“本地文件”。



如下图所示，我们选择在日志中记录“记账请求”，“身份验证请求”和“周期性状态”。

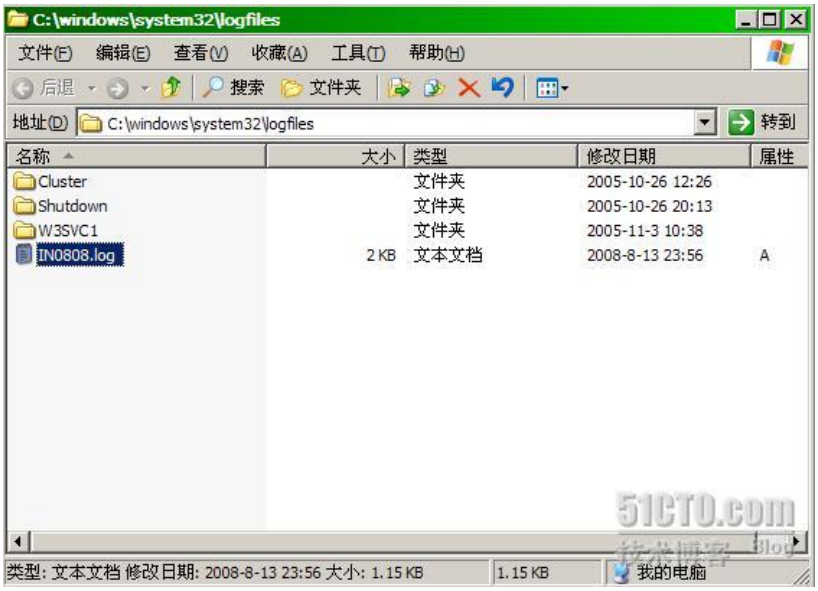


五 VPN 访问实验

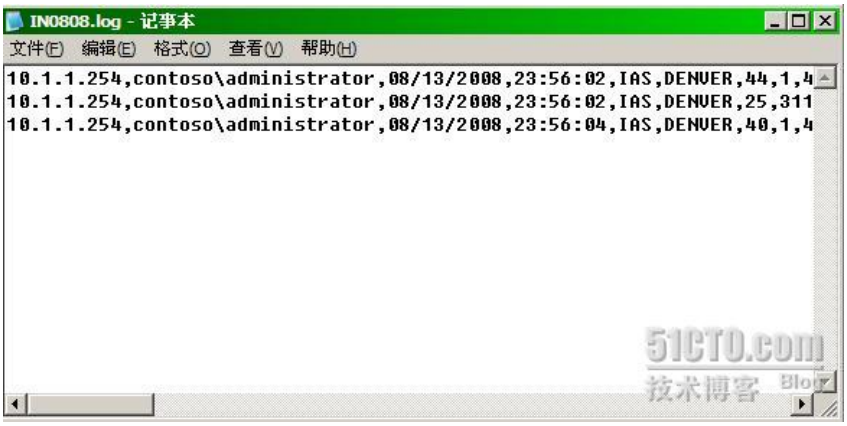
好了，所有的配置都就绪了，我们在客户机 Istanbul 上进行 Radius 实验了，如下图所示，我们在 Istanbul 上准备以 contosoadministrator 的身份进行 VPN 身份验证，由于 ISA 服务器在工作组环境，因此如果不使用 Radius 服务器，ISA 服务器无法验证域用户的身份。点击连接，看看结果如何？

如下图所示，Istanbul 已经成功地拨入了 VPN 服务器，Radius 服务器起作用了。

接下来让我们去 Radius 服务器看看日志中有没有记录这次访问，Radius 的日志文件存储在 C:Windowssystem32logfiles 目录下，如下图所示，我们打开此目录中的 IN0808.log，这就是 Radius 的日志文件。



如下图所示，Radius 服务器的日志中很清晰地记录了客户端的这次访问，OK，Radius 服务器配置成功！



用智能卡构建身份验证的马其诺防线：ISA2006 系列之二十三

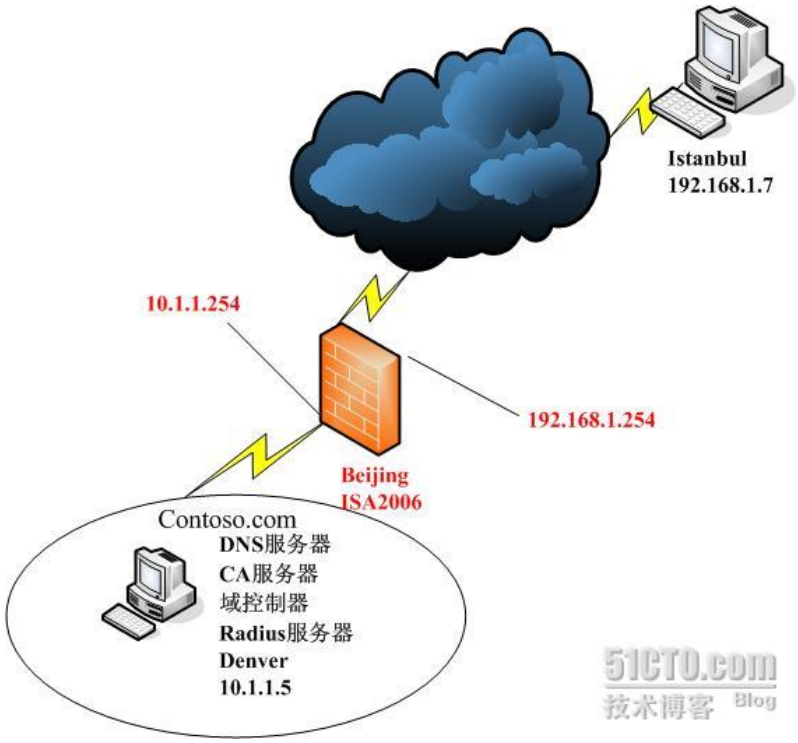
在前面的博文中我们已经介绍了如何用 ISA2006 构建 VPN 服务器，以及如何利用 Radius 服务器负责处理 VPN 的身份验证，今天我们要更进一步，用智能卡实现更安全的用户身份验证。我们知道，传统的用户名/口令的身份验证方法不够安全，存在被人窃听的危险，尤其是公司的 VPN 用户从外网进行访问，安全环境更不容易得到保证。如果我们在 VPN 客户机上使用智能卡进行身份验证，就可以很好地解决这个安全问题。

智能卡(SmartCard)是一个带有微处理器和存储器等微型集成电路芯片、具有标准规格的卡片。智能卡遵循的 ISO7816 标准规定了智能卡的外形、厚度、触点位置、电信号、协议等。一般应用于 PKI 的智能卡，都带有硬件真随机数发生器、RSA 协处理器，可以硬件实现 RSA 的运算。另外，还具有 DES 和 SHA-1 等密码算法，保证在硬件内部产生密钥对，并在硬件内部完成加、解密运算。

因此，从上面的介绍来看，智能卡不仅是个存储设备，智能卡更接近于一台计算机。智能卡对加密解密可以进行很好的硬件支持，而且本身的抗攻击能力也很强，例如可通过总线分层、芯片平坦化、平衡能耗、随机指令冗余等技术抗拒时钟抖动，物理篡改等攻击方法。

这样我们就有了一种新的身份验证思路，用户验证时不再使用用户名和口令，而是利用用户证书来进行验证。为了保证证书的安全，我们再把证书集成到智能卡中！这样用户在进行身份验证时只要插入自己的智能卡然后输入智能卡的 PIN 码就可以了，由于不需要输入用户名和口令，大大减少了泄密的可能性。即使智能卡丢了也问题不大，因为智能卡有 PIN 码保护，一旦输错规定次数的 PIN 码，智能卡就将被锁定，而且丢失了智能卡后还可以及时通知管理员作废智能卡上的证书，这样就可以更好地防止有人利用非授权的智能卡闯过身份验证这一关。

下面我们构思一个实验来完成这个设想，如下图所示，Denver 是 contoso.com 的域控制器，DNS 服务器，CA 服务器和 Radius 服务器，Beijing 是 ISA2006 服务器，而且处在工作组环境，Istanbul 是外网的一台客户机。我们在实验中使用的智能卡是飞天诚信公司出品的 Epass1000，USB 接口。这种智能卡由于使用了标准的 USB 接口，因此可以在驱动程序的支持下，把计算机的 USB 接口当成是智能卡的读卡器，直接把智能卡插入计算机的 USB 口就可以了。而传统的智能卡是由一个读卡器加上一张智能卡组成的，显然不如这样产品方便。



51CTO.com
技术博客 Blog

目前的环境中，我们已经可以具备了下列条件：

1 Denver 上安装了企业根 CA 服务器，注意，这个实验必须要求有企业类型的 CA。

2 所有的实验计算机都信任 Denver 上的 CA 服务器。

3 Beijing 上已经配置成了 VPN 服务器，支持用户用 PPTP 或 L2TP 拨入。

4 Beijing 可以利用 Denver 上的 Radius 服务器对域用户进行身份验证。

我们接下来要做的就是利用 CA 服务器为一个测试用户颁发证书，再把证书集成到智能卡上，然后利用智能卡在外网的客户机上进行 VPN 身份验证，具体步骤如下。

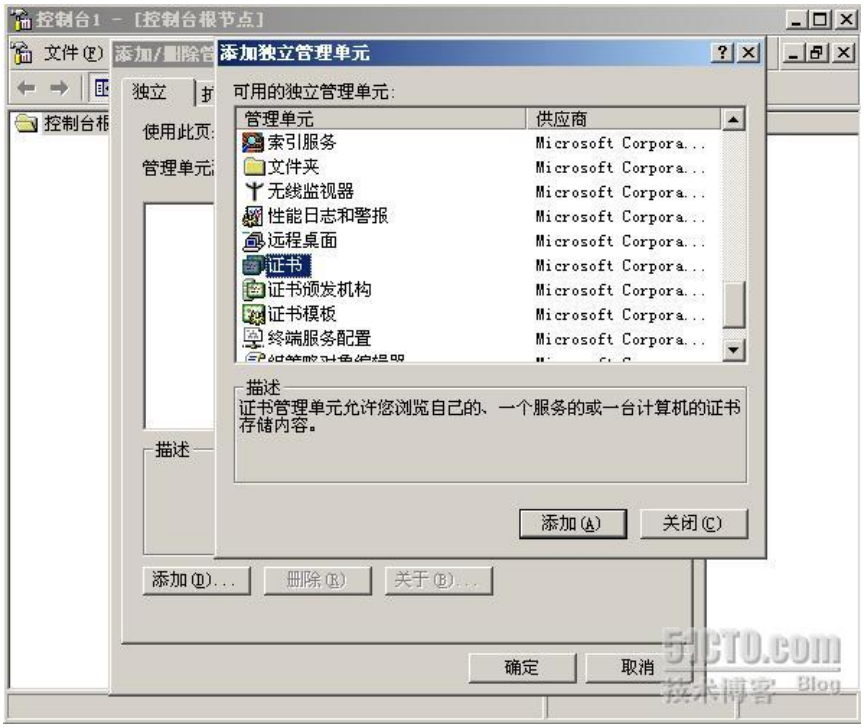
一 添加证书模板

首先我们要对 CA 服务器进行配置，让 CA 服务器可以对智能卡所需要的证书进行支持。我们要做的是在证书模板中添加智能卡验证所需要的模板，如下图所示，在 Denver 的管理工具中打开证书颁发机构，选择新建“要颁发的证书模板”。

如下图所示，我们添加了四个证书模板，分别是“智能卡用户”，“智能卡登录”，“注册代理”，“注册代理（计算机）”，点击“确定”结束证书模板的添加。

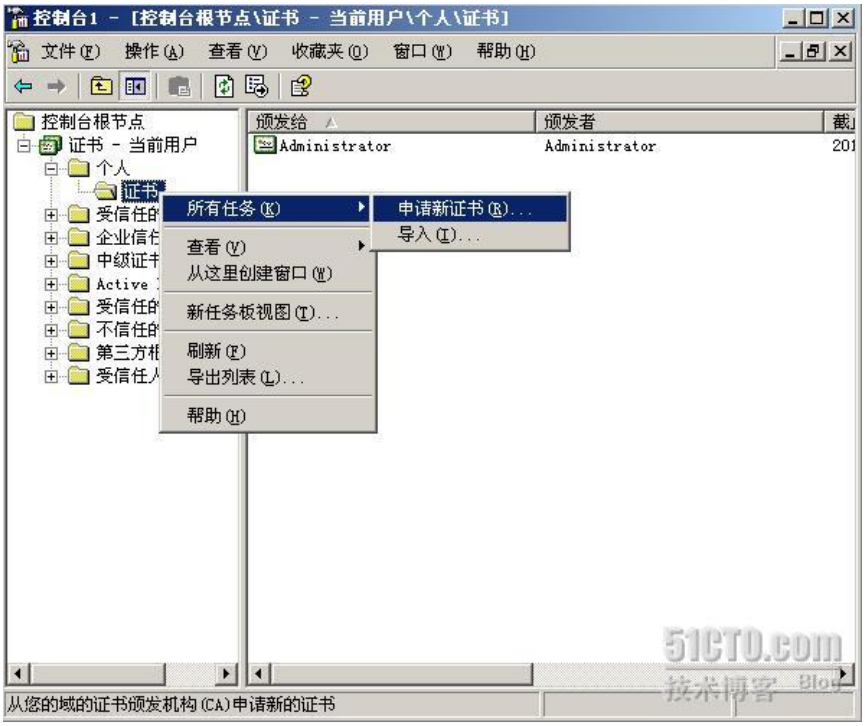
二 申请注册代理证书

在 Win2003 的 CA 服务器中，如果要为智能卡用户申请证书，那么智能卡管理员必须先拥有一个注册代理证书。有了这个注册代理证书后，才有资格为其他用户申请智能卡证书，显然这是为了防止随意颁发智能卡证书而导致安全隐患。要申请注册代理证书，确保在 Denver 上是以域管理员身份登录，然后运行 MMC，如下图所示，添加一个证书管理单元。

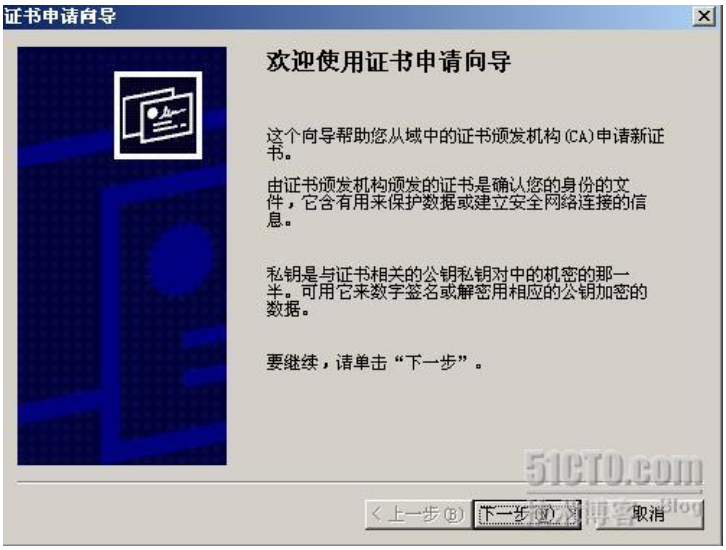


选择使用定制的证书管理单元管理用户账号中的证书。

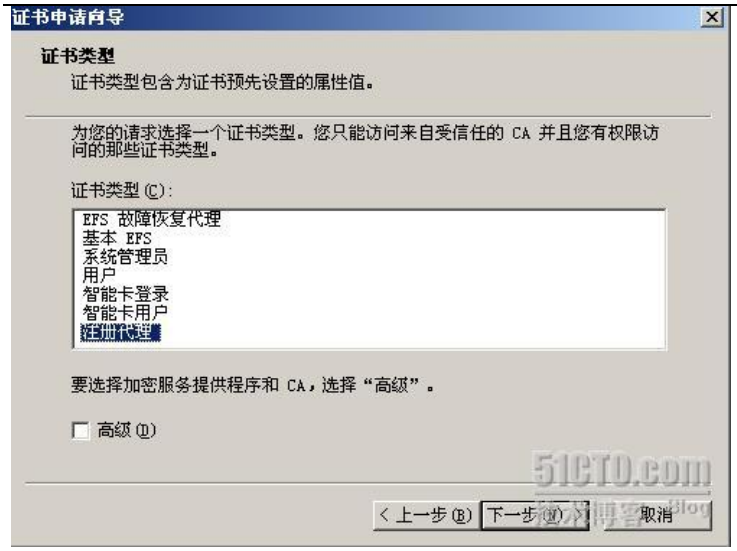
如下图所示，在用户证书管理工具中切换到个人－证书，选择“申请新证书”。



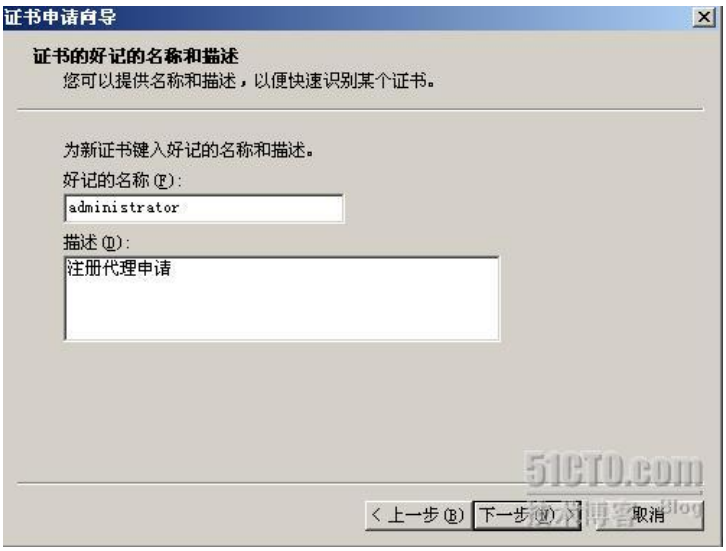
出现证书申请向导，选择“下一步”。



申请的证书类型选择“注册代理”。

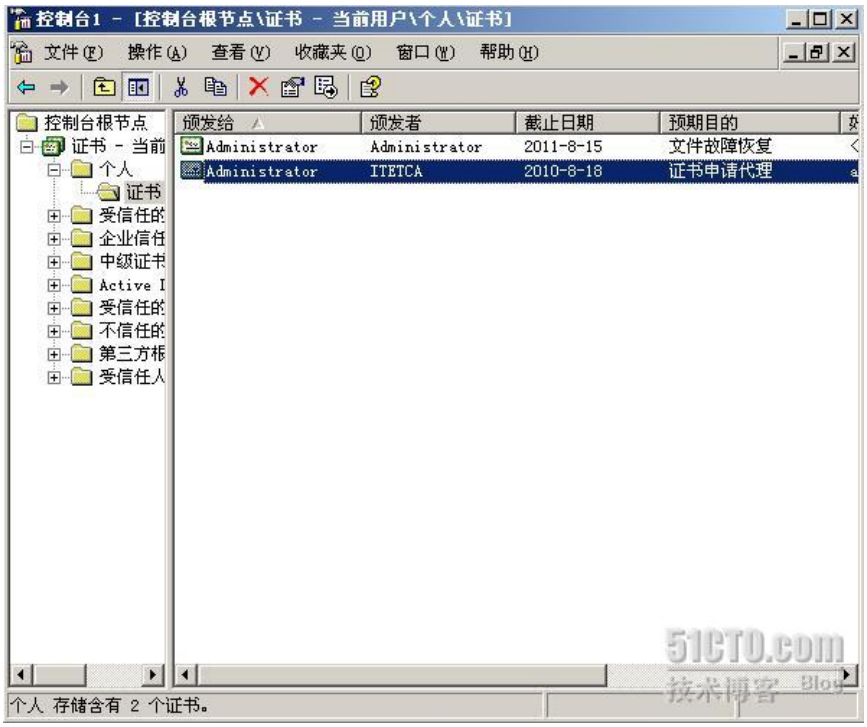


如下图所示，为申请的注册代理证书取个名字以及进行简单描述。



点击“完成”结束申请。

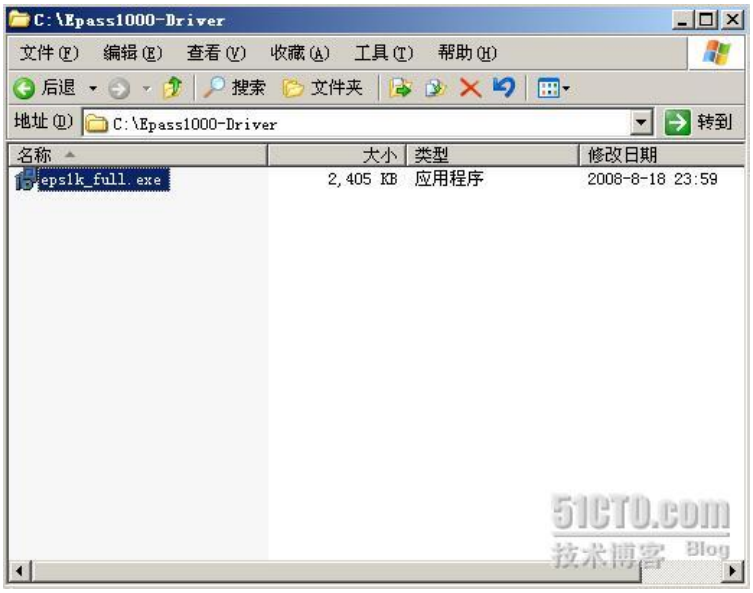
如下图所示，administrator 已经获得了 CA 颁发的注册代理证书，接下来 administrator 就有资格为智能卡用户颁发证书了。



三 安装智能卡驱动

在为智能卡用户申请证书之前，我们先要在 Denver 上安装智能卡驱动。当然，外网的 Istanbul 使用智能卡登录，也需要有智能卡驱动的支持。智能卡驱动的安装方法是一样的，

我们在 Denver 上举例如何进行智能卡的安装。如下图所示，我们双击执行智能卡驱动的安装程序 epslk_full.exe。



出现智能卡驱动的安装向导，点击下一步继续。

勾选“支持智能卡登录操作系统或者 VPN”，点击“安装”。

开始驱动程序的安装。

如下图所示，智能卡驱动安装完成后要求重新启动计算机，点击“完成”结束安装。

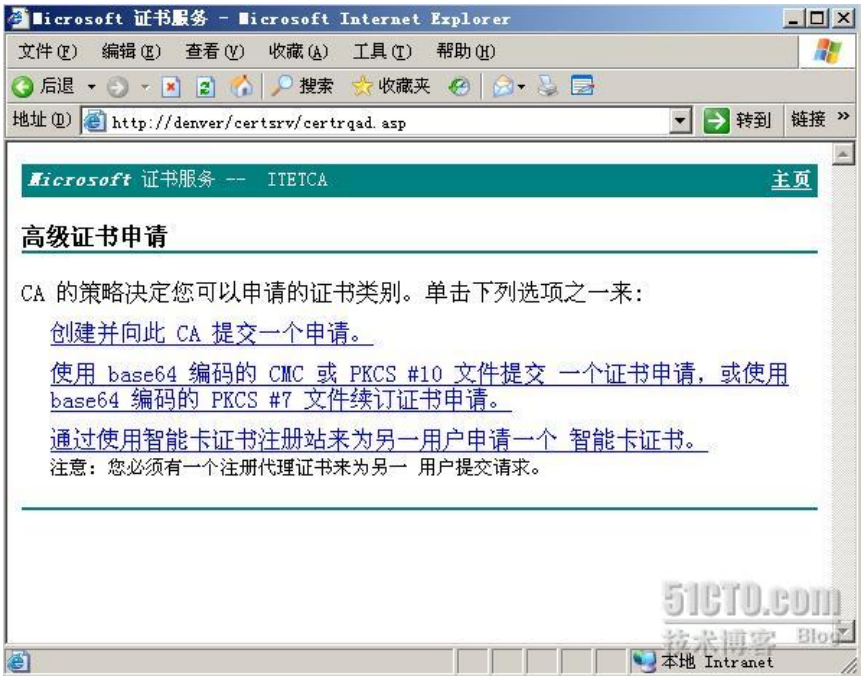
Denver 重启后，桌面的右下角出现了智能卡证书监控器的图标，这就是安装驱动后形成的软件读卡器。

四 为智能卡用户申请证书

Denver 上安装了智能卡驱动之后，我们就可以为智能卡用户申请证书了。我们创建了一个智能卡测试用户 vpnuser，下面就来看看如何为这个用户申请智能卡证书。在 Denver 的浏览器中输入 http://denver/certsrv，如下图所示，选择“申请一个证书”。

选择提交一个高级证书申请。

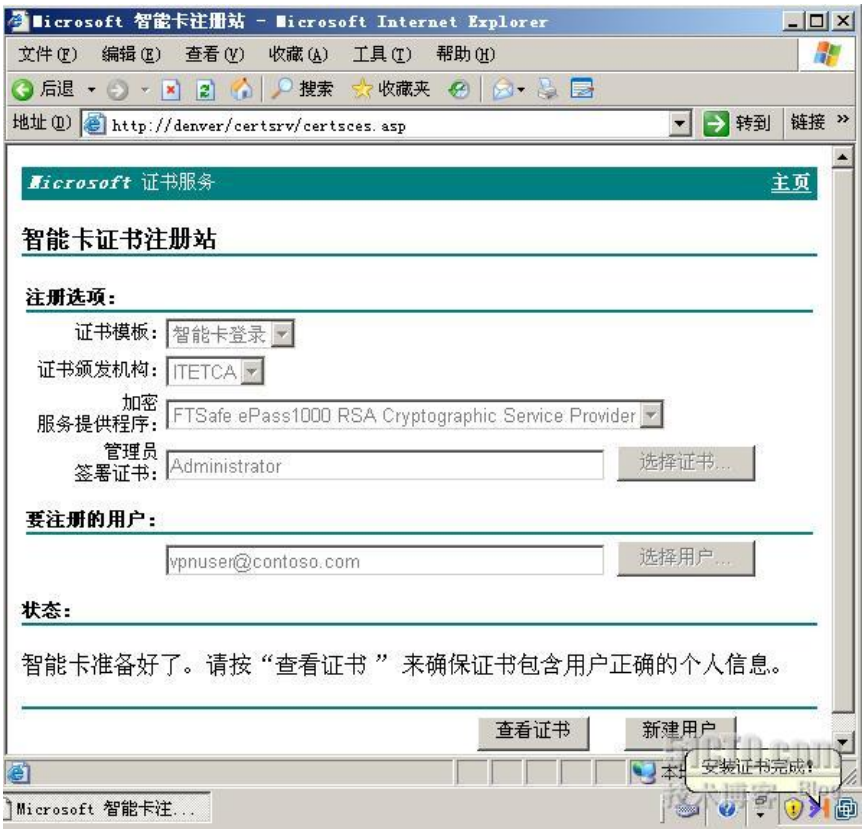
选择“通过使用智能卡注册站来为另一用户申请一个智能卡证书”。



如下图所示，我们在证书模板中选择“智能卡登录”。注意，模板中的“智能卡用户”一般用于配合 Outlook2003 实现邮件加密。加密程序选择使用 Epass1000 智能卡上集成的加密芯片完成，显然是要利用智能卡中的硬件芯片生成配对的公钥私钥。点击“选择用户”，选择 vpnuser 作为智能卡证书的颁发对象。完成了所有申请参数后，插入智能卡，点击“申请”。

如下图所示，申请证书时智能卡需要输入PIN码验证，输入正确的PIN码后点击“登录”。

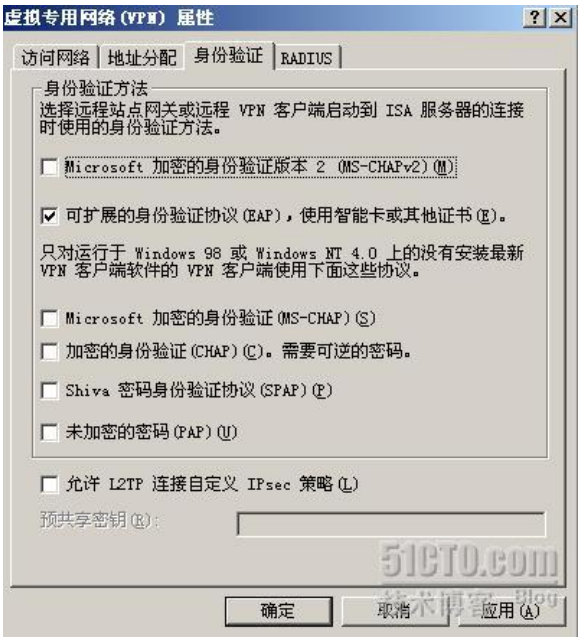
如下图所示，为用户 vpnuser 所申请的智能卡登录证书已经成功地存储在智能卡上了。



五 配置 ISA 服务器

ISA 服务器需要配置身份验证协议，ISA 服务器默认使用的身份验证协议是 MS-CHAP V2，但使用智能卡登录需要使用可扩展的身份验证协议（EAP）。如下图所示，我们在 ISA 管理器中展开到虚拟专用网络，在右侧的任务面板中点击“选择身份验证方法”。

如下图所示，我们选择使用 EAP 协议对 VPN 用户进行身份验证，点击“确定”后完成了对 VPN 服务器的身份验证配置。



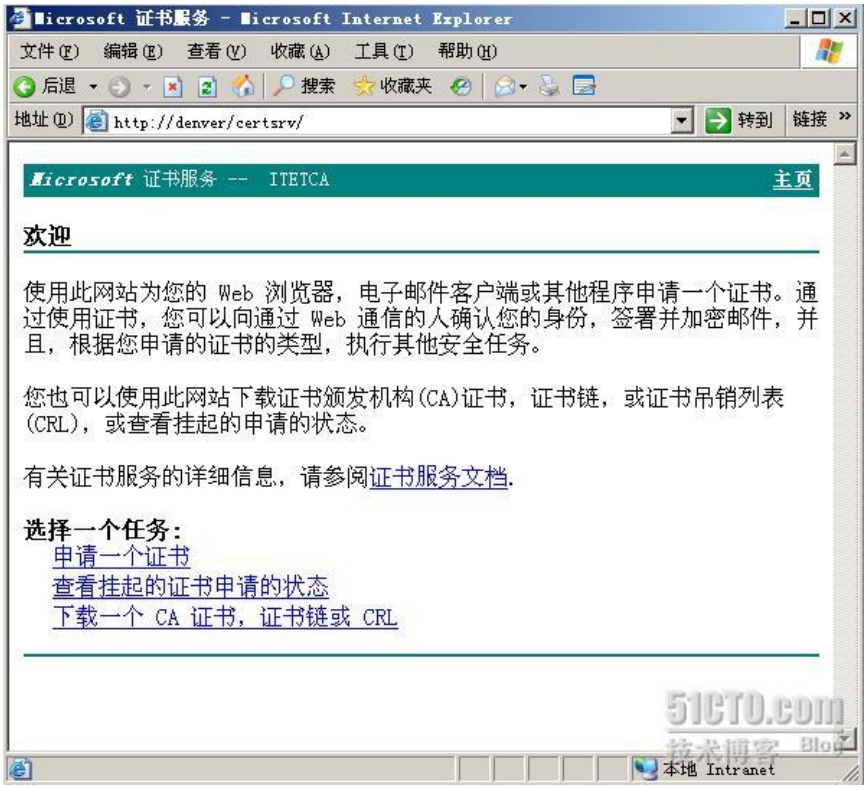
六 配置 Radius 服务器

ISA 服务器收到 VPN 用户发来的身份验证请求后，会把验证请求转到 Radius 服务器，因此我们接下来需要在 Radius 服务器上进行配置。一方面要配置 Radius 服务器支持 EAP

协议，另一方面要在 Radius 服务器上申请服务器证书，以便 VPN 客户机对 Radius 服务器进行身份验证。

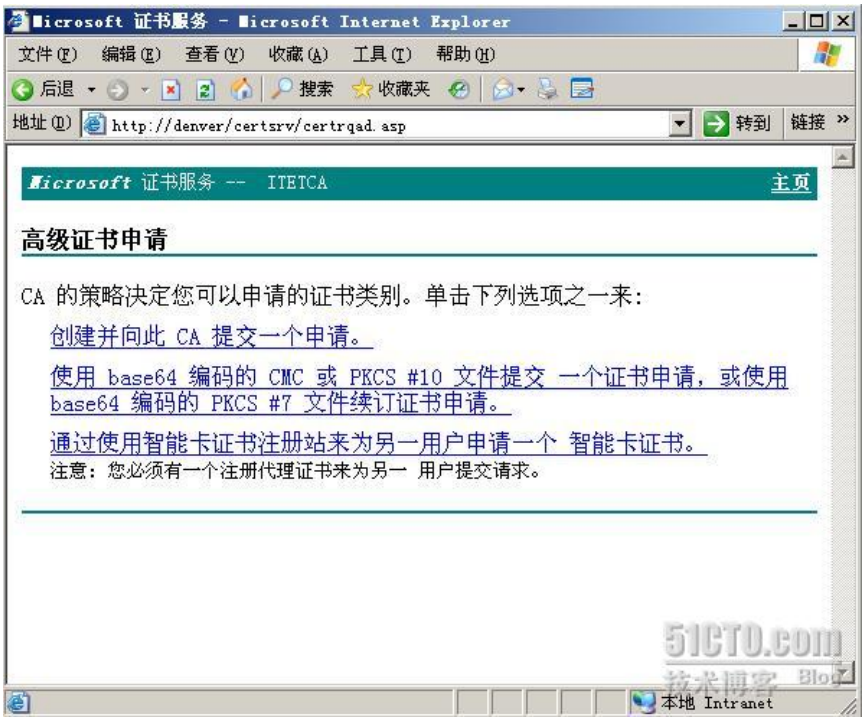
1） 申请服务器证书

我们在 Radius 服务器上申请一个服务器证书，这样 VPN 客户机使用智能卡登录时可以利用这个证书验证 Radius 服务器的身份，避免登录到了错误的服务器上，提高整体安全性。我们在 Denver 的浏览器中输入 http://denver/certsrv，如下图所示，选择“申请一个证书”。

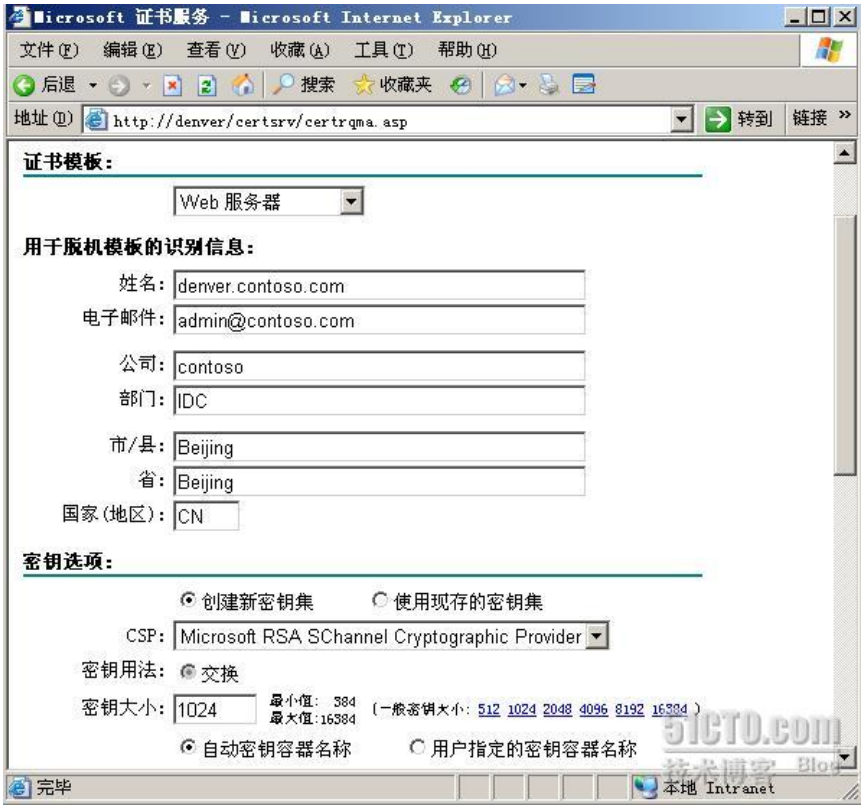


选择提交一个高级证书申请。

选择“创建并向此 CA 提交一个申请”。



选择申请一个 Web 服务器证书，证书姓名输入 denver.contoso.com，选择把证书保存在计算机存储中。参数填写完毕后，点击“申请”。



如下图所示，申请的证书已经颁发，选择安装此证书。

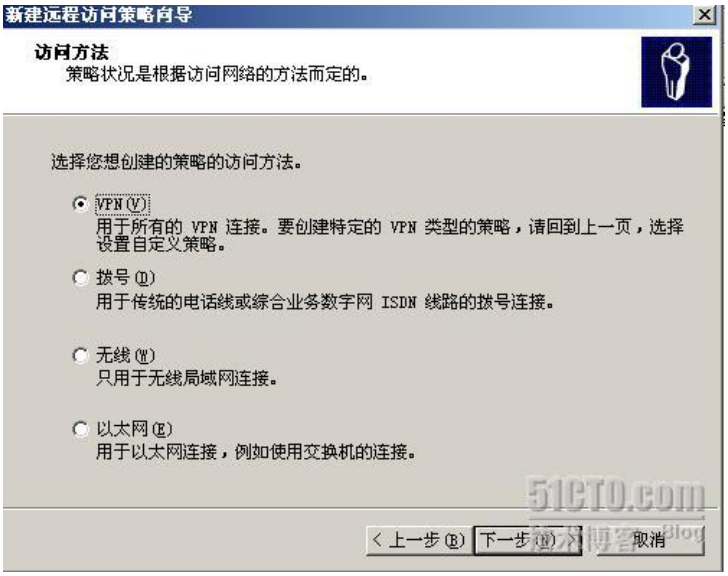
2） 配置 Radius 远程访问策略

我们在 Radius 服务器中创建一个新的远程访问策略，在这个策略中配置使用 EAP 协议验证用户请求。在 Denver 的管理工具中打开 Internet 验证服务，如下图所示，选择“新建远程访问策略”。

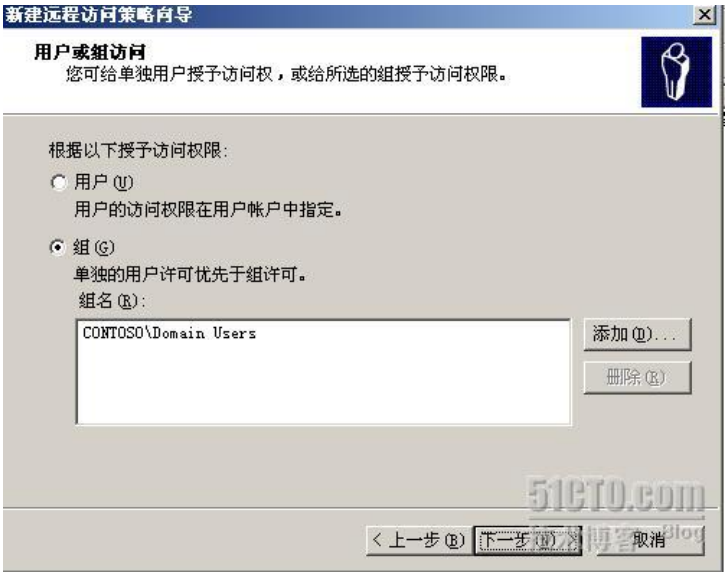
如下图所示，出现远程访问策略创建向导，选择下一步。

选择使用向导完成远程访问策略的设置，为策略命名为 VPN。

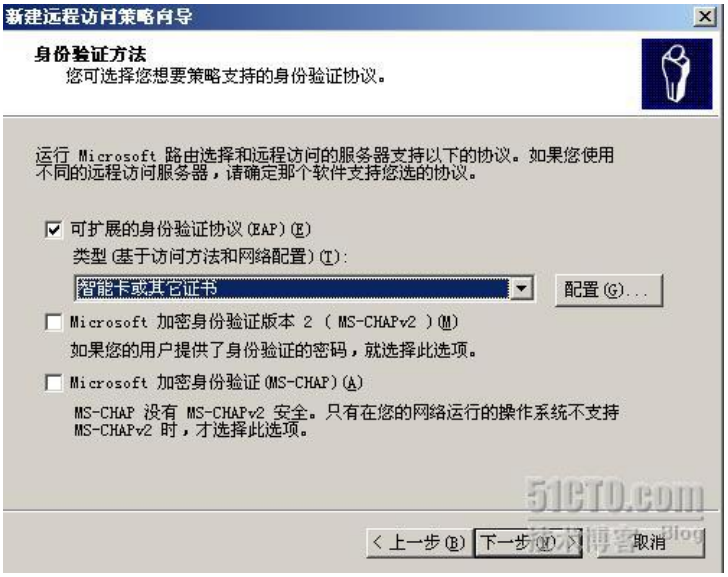
远程访问的类型是 VPN。



授予 contoso.com 域中的 Domain users 组远程访问权限。

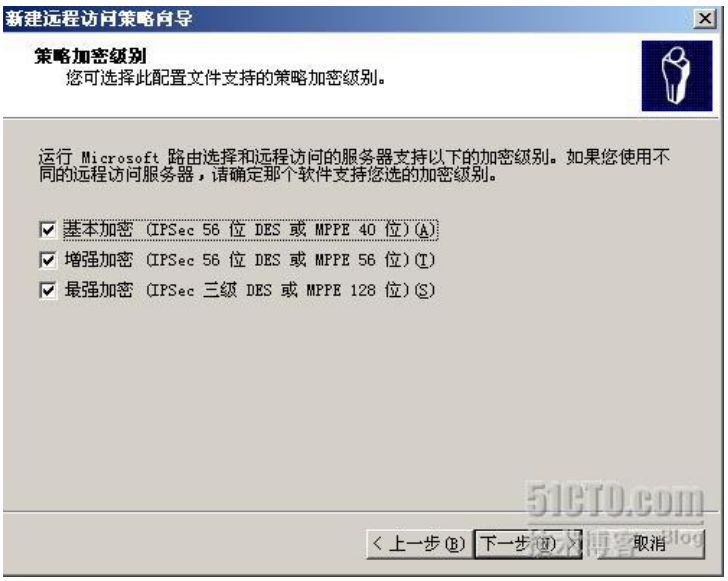


勾选使用 EAP 协议，类型选择“智能卡或其他证书”，点击“配置”按钮。



点击“配置”按钮后，选择使用刚才申请的 denver.contoso.com 证书来证明自己的身份。

接下来选择远程访问策略支持的加密级别，我们使用默认设置选择支持所有加密级别即可。



点击完成结束新建远程访问策略的创建。

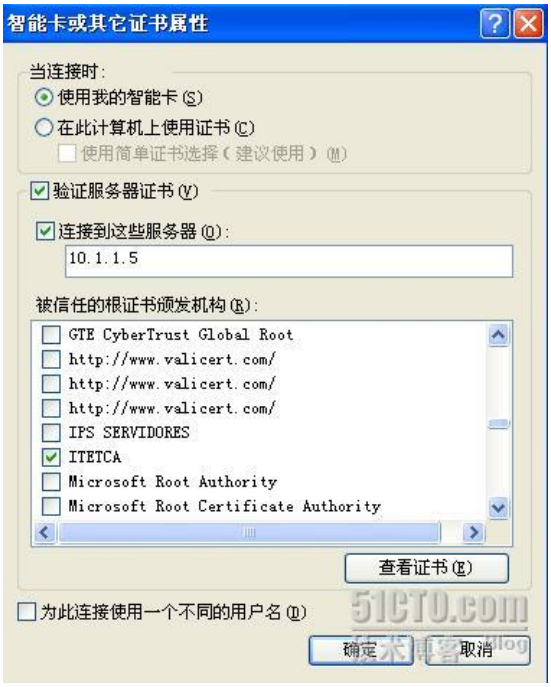
七 配置 VPN 拨号连接

配置完 ISA 服务器和 Radius 服务器后，最后我们来配置 VPN 客户机 Istanbul，让 Istanbul 在进行 VPN 访问时使用智能卡验证自己的身份。如下图所示，在 Istanbul 上双击事先创建好的 VPN 连接，点击“属性”。

在 VPN 连接的属性中切换到“安全”标签，如下图所示，选择“高级（自定义设置）”，点击“设置”。

如下图所示，在高级安全设置中选择使用 EAP 协议，点击“智能卡或其他证书（启用加密）”的属性。

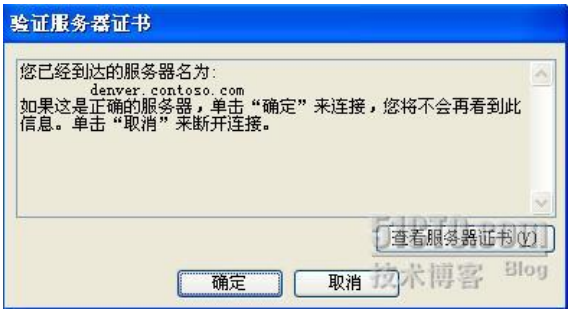
如下图所示，在智能卡或其他证书的属性中选择使用智能卡进行身份验证，勾选“验证服务器证书”，勾选“连接到这些服务器”并输入 Denver 的 IP 地址 10.1.1..5。在被信任的证书颁发机构中选择 Denver 创建的 CA 服务器“ITETCA”。



好了，至此终于完成了所有的前期工作，我们赶快在 Istanbul 上测试一下吧，如下图所示，双击 VPN 连接后，Istanbul 提示我们插入智能卡。

插入智能卡后，我们可以看到 Istanbul 已经识别出智能卡上的证书是颁发给 vpnuser 的，我们需要输入智能卡的 PIN 码，然后点击“确定”。

接下来我们看到 Istanbul 已经连接到了 Radius 服务器 Denver，Denver 出示了一个服务器证书 denver.contoso.com 来证明自己的身份，如果我们认可这个证书，就点击“确定”。

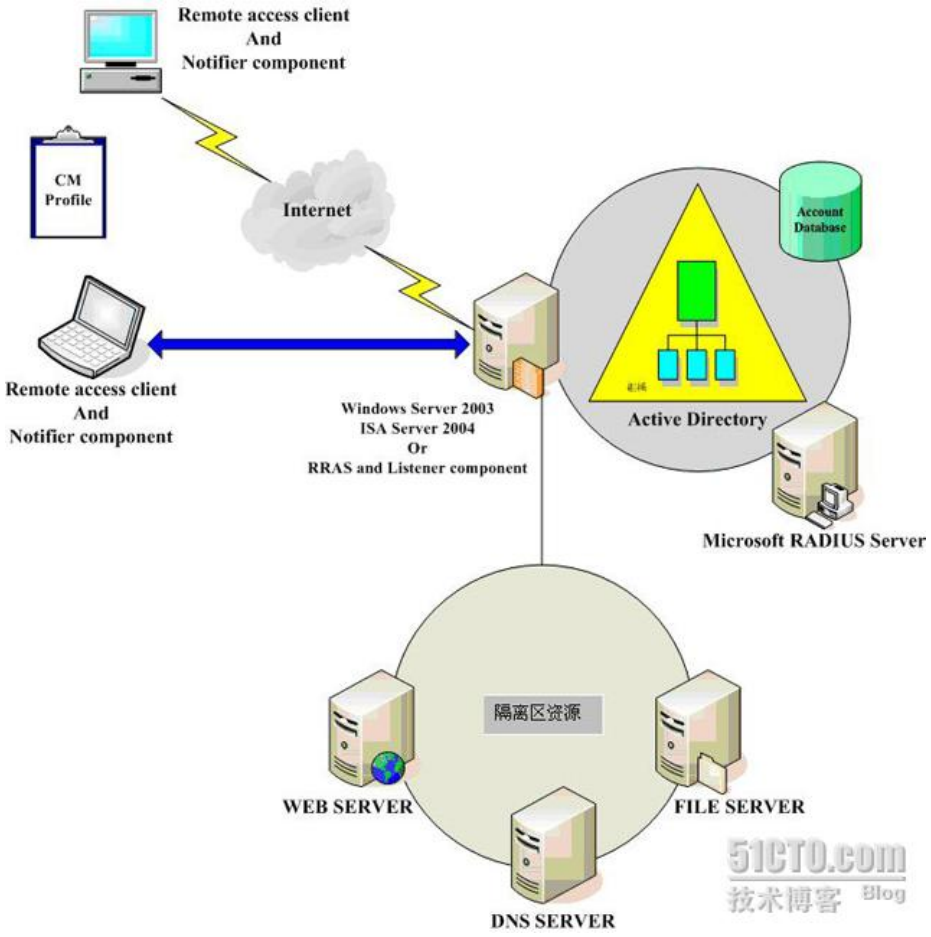


我们在 Istanbul 上终于使用智能卡成功地通过了 VPN 服务器和 Radius 服务器的身份验证，如下图所示，我们在 Istanbul 上已经可以顺利地访问到内网的资源了，实验成功！

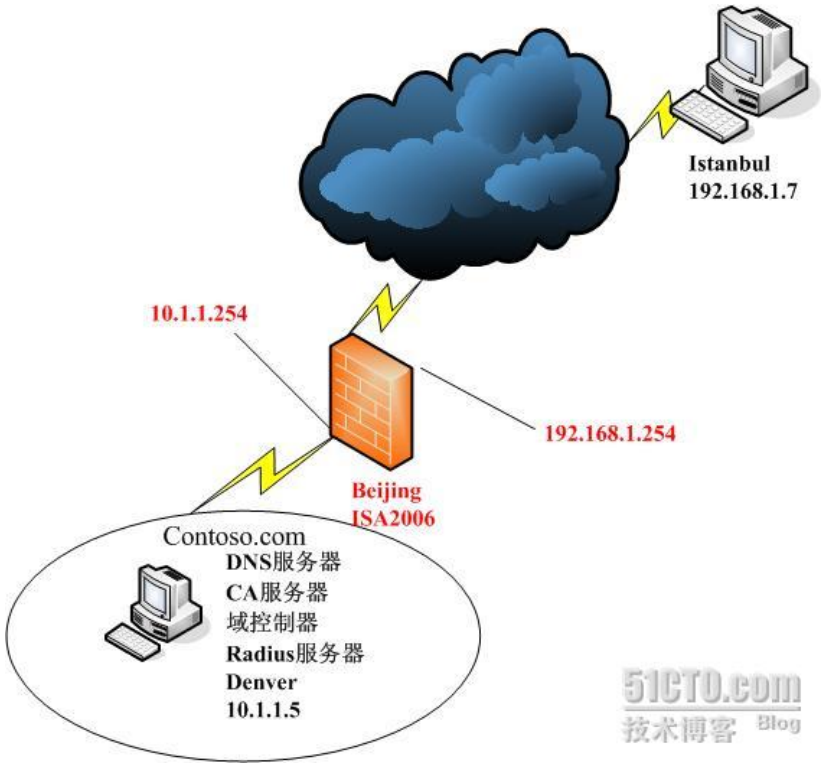
总结：从上述实验可以看出，用智能卡代替传统的用户名/口令进行身份验证，确实在安全性方面提高了一大截。而且智能卡的部署费用不高，一般的公司都承受得起，因此如果公司有经常出差的员工，可以考虑给他们发一个智能卡，让他们可以安全地连接到公司内网。

多图详解 VPN 用户隔离:ISA2006 系列之二十四

VPN 隔离是 ISA2006 中提供的一个强大功能，也是 NAP（网络访问保护）的一个重要组成环节。VPN 隔离指的的是当 VPN 客户机通过 VPN 服务器的身份验证后，VPN 服务器并不立即允许其访问内网，而是将 VPN 客户机放到一个被隔离的网络中。然后通过策略对客户机进行安全检查，例如查看 VPN 客户机是否安装了最新的安全补丁，是否启用了防火墙，防病毒软件是否升级到了最新版本等等。如果 VPN 客户机通过了安全策略的检查，VPN 服务器将允许其访问内网资源；如果不能通过安全策略检查，VPN 客户机将被限定在隔离网络中，无法访问内网资源，而且在隔离网络中停留一段时间后会被逐出。有的企业会在隔离网络中放置一些文件服务器，用以提供杀病毒软件，系统更新补丁等，还有的可能会在隔离网络中放置 Web 服务器，用以提示用户为什么被隔离，接下来要进行什么操作。VPN 隔离的原理如下图所示。



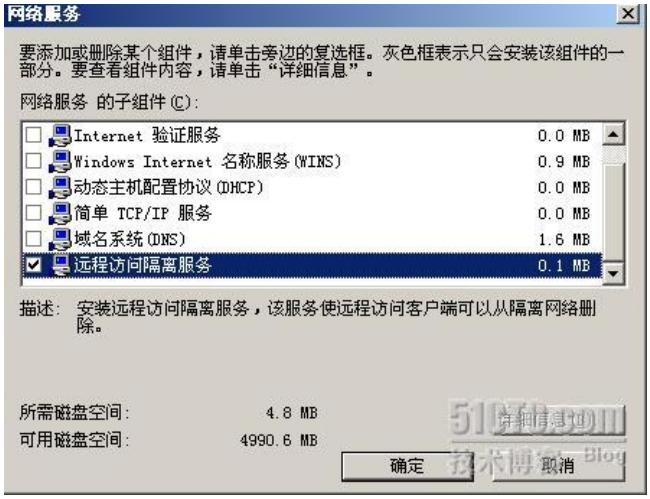
今天我们通过一个实验来简单介绍一下 VPN 隔离的功能，实验拓扑如下图所示，Denver 是域控制器，Beijing 是 ISA2006 服务器，Istanbul 是外网 VPN 客户机。Beijing 上启用了 VPN 隔离，当 VPN 客户机拨入时，VPN 服务器会把 VPN 客户机放入隔离网络，然后检查 VPN 客户机的防火墙是否开启。如果开启了防火墙，那 VPN 客户机就能通过安全检查，被允许访问内网；否则 VPN 客户机就将在规定时间内被逐出隔离网络。



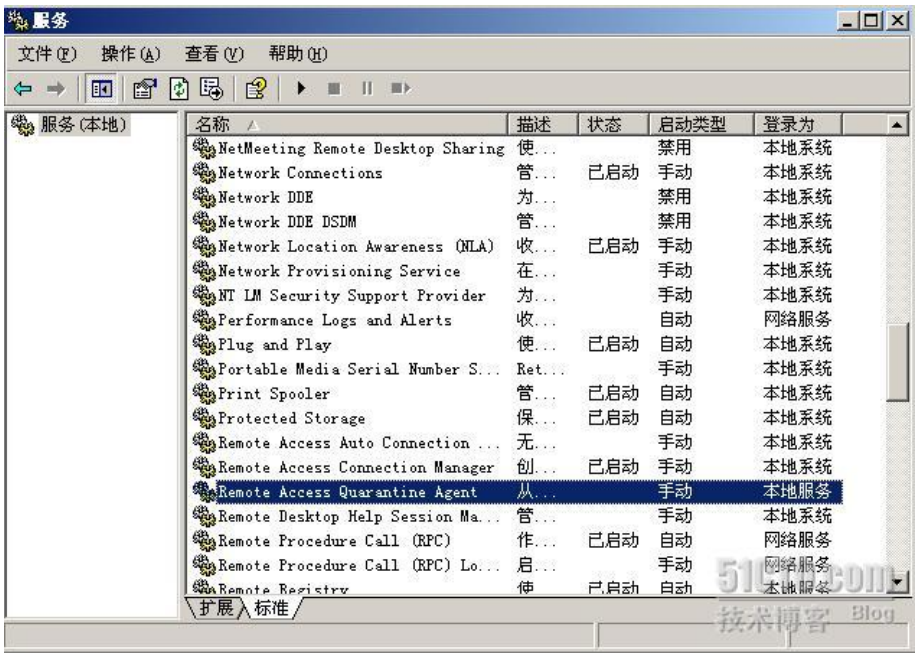
目前我们已经在 Beijing 上配置了 VPN 服务器，VPN 客户机的地址池是 192.168.100.1－192.168.100.200，我们接下来要进行下列步骤。

一 安装隔离服务

ISA2004 安装 VPN 隔离服务时一般是使用 Resource Kits 工具集中提供的 VPN 隔离服务的安装程序，现在由于 Win2003 SP1 中已经集成了 VPN 隔离服务，因此 ISA2006 安装 VPN 隔离就非常简单了。打开控制面板中的添加或删除程序，选择添加/删除 Windows 组件，如下图所示，在网络服务的子组件中勾选“远程访问隔离服务”，点击确定即可完成 VPN 隔离服务的安装。



如下图所示，我们已经在 ISA 服务器上安装了 VPN 隔离服务，这时 ISA 服务器会在 7250 端口提供一个守护进程，用来接收 VPN 客户机上的代理程序发来的策略检查结果，但此时的 VPN 隔离服务还需要对一些参数进行配置。



我们在 Beijing 上打开注册表编辑工具 regedit.exe，定位到[HKEY_LOCAL_MACHINE SYSTEMCurrentControlSetServicesrqs]，编辑“AllowedSet”。如下图所示，我们为键值赋值为“RQVersion3”。这个键值的作用相当于是一个接头暗号，当 VPN 客户机被隔离策略检查安全性之后，VPN 客户机上的代理程序会把检查结果发往 VPN 服务器。VPN 服务器收

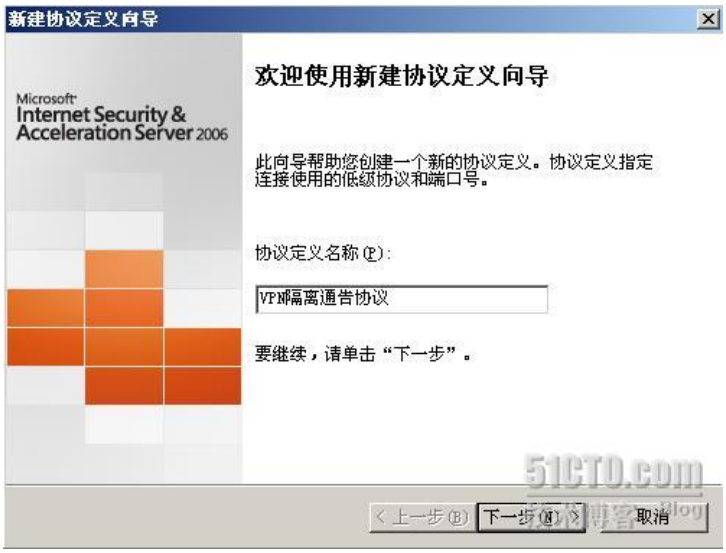
到 VPN 客户机上发来的检查结果后，要查看检查结果中附带的版本标识符是否和注册表中记录的一样，如果是相同的，那 VPN 服务器就认可对 VPN 客户机的检查结果，否则 VPN 服务器就会认为 VPN 客户机上的代理程序把检查结果发错了目标，拒绝承认检查结果。

接下来我们还要添加一个注册表键值，如下图所示，我们在 RQS 服务中新建一个字符串值。

如下图所示，键值命名为 Authenticator，内容为 C:Program FilesMicrosoft ISA Servervpnplgin.dll，这个键值的作用是当 VPN 客户机通过了安全策略检查后，vpnplgin.dll 将解除对 VPN 客户机的隔离。

二 创建 VPN 隔离通告协议

ISA 服务器上安装了 VPN 隔离服务后，在 7250 端口会有一个守护进程等候被隔离客户机上的代理程序传送安全策略检查的结果，但 ISA 的访问规则不会允许被隔离的计算机连接 ISA 的 7250 端口，因此我们需要创建访问规则允许这种访问行为。在创建访问规则前我们需要把访问 7250 端口的行为定义为一种协议，在 ISA 防火墙策略的工具箱中选择新建协议，如下图所示，出现协议创建向导，我们给协议命名为“VPN 隔离通告协议”，点击“下一步”继续。



如下图所示，我们定义协议使用 TCP，端口是 7250，方向是出站。注意，千万别认为 ISA 被其他计算机访问 7250 端口，方向应该算是入站，这是错误的！访问规则中使用的协议方向是出站，而发布规则中使用的协议方向是入站！

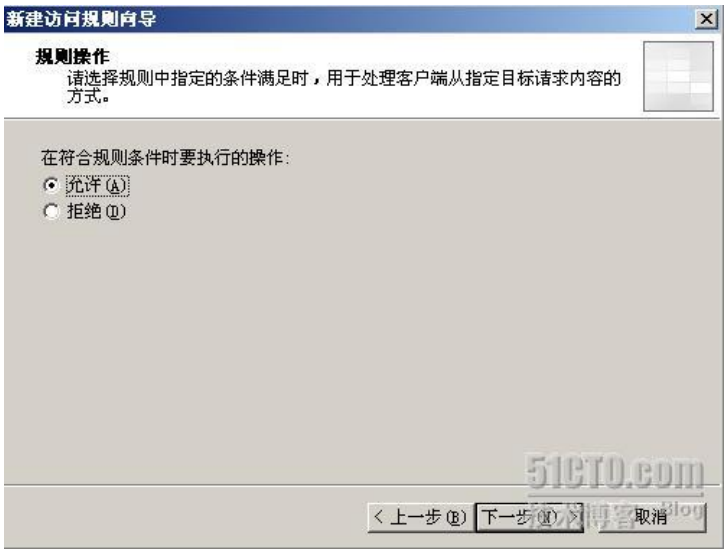
接下来协议创建向导询问是否需要使用辅助连接，我们并不需要，点击下一步继续。

如下图所示，我们顺利完成了 VPN 隔离通告协议的创建。

三 创建访问规则

我们创建了 VPN 隔离通告协议之后，接下来就可以创建访问规则允许被隔离的 VPN 客户机连接 ISA 服务器的 7250 端口报告策略检查结果了。如下图所示，我们在 ISA 管理器中选择新建访问规则，我们为规则命名为“允许 VPN 隔离通告”，点击下一步继续。

当访问请求满足规则条件时允许操作。



规则中只允许使用我们创建的 VPN 隔离通告协议。

规则的访问源是“被隔离的 VPN 客户端”，这也是 ISA 中预设的一个网络。

访问目标是本机主机。

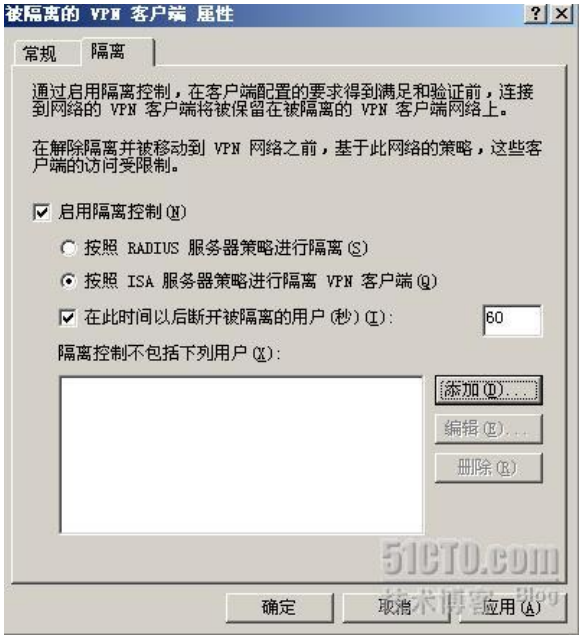
此规则适用于所有用户。

如下图所示，我们完成了访问规则的创建。

四 启用 VPN 隔离

接下来我们可以在 ISA 服务器上启用 VPN 隔离了，如下图所示，我们在 ISA 的网络中找到“被隔离的 VPN 客户端”，点击右键查看属性。

我们在属性中切换到“隔离标签”，如下图所示，勾选“启用隔离控制”，选择按照 ISA 服务器策略进行隔离 VPN 客户端，并设定用户在 60 秒内如果不能被解除隔离，就将被 ISA 服务器中断连接。



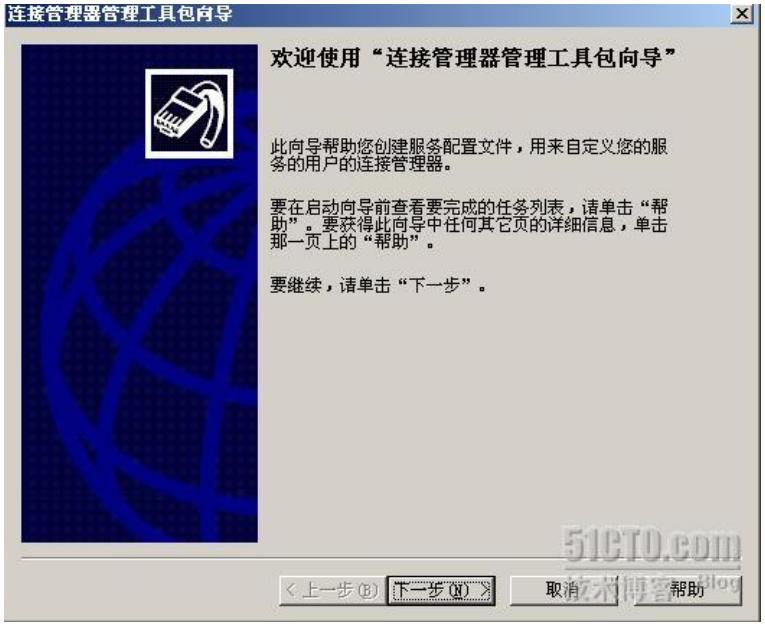
至此，我们在 ISA 服务器上启用了 VPN 隔离服务，接下来我们启动 VPN 隔离服务就可以完成服务器端的配置了。

五 创建连接管理器分发文件

服务器端的配置完成之后，我们接下来就要考虑如何在客户端进行安全策略的检查以及如何把检查结果传送给 ISA 服务器。如下图所示，rqc.exe 负责把策略检查结果发送给 ISA 服务器，rqc.exe 是 VPN 隔离服务的客户端工具，在 Resource kits 工具集中有提供，在 win2003 SP1 中也已经集成了，路径是 C:Program FilesCmakSupport。RQScript.vbs 是一个负责检查客户端安全策略的脚本，这个脚本文件是由微软的 ISA 实验室提供的示例文件，主要负责检查客户端的防火墙有没有开启。我们如果想自定义一些检测项目，就只能自己写脚本了。如果你没有编程基础也不要紧，有一些公司可以提供这种脚本编程的服务，还有的公司把常用的检测项目都封装成应用程序，管理员只要用鼠标选择具体的检测项目即可。

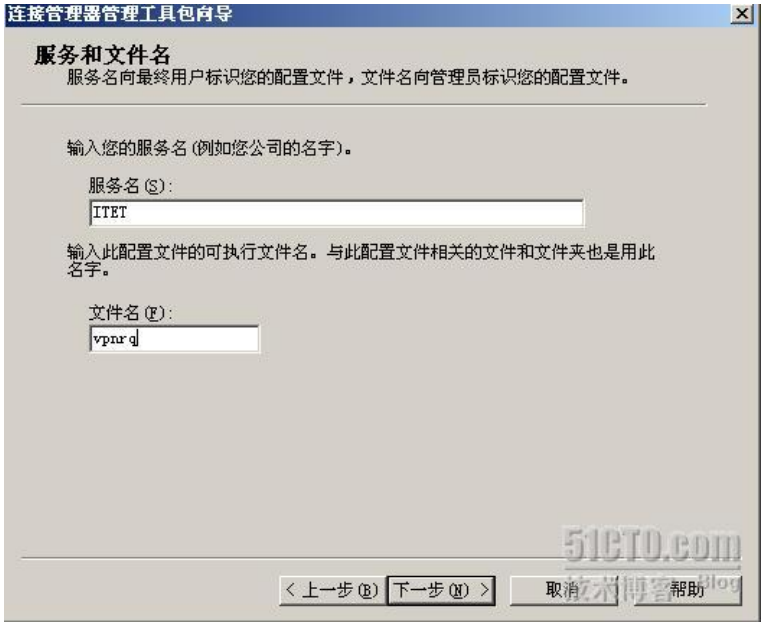
现在我们有了 rqc.exe 和 RQScript.vbs，但怎么才能让这两个文件在客户端进行 VPN 连接时发挥作用呢？我们可以定制一个专用的 VPN 拨号配置文件，在配置文件中集成这两个文件。我们要想定制专用的 VPN 拨号配置文件，首先要安装一个连接管理器管理工具包。我们在 ISA 服务器上打开控制面板中的添加或删除程序，选择添加/删除 Windows 组件，如下图所示，在“管理和监视工具”的子组件中选择“连接管理器管理工具包”。

接下来我们在管理工具中打开“连接管理器管理工具包”，创建定制一个 VPN 拨号配置文件，如下图所示，出现连接管理器管理工具包向导，点击下一步继续。



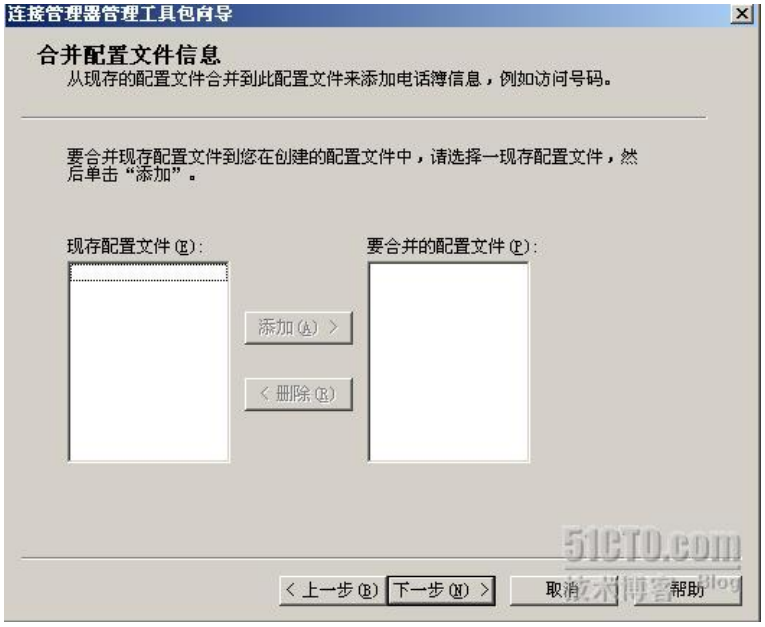
选择新建配置文件，点击下一步继续。

输入服务名和文件名，注意，文件名是 vpnrq，最终生成的配置文件名就是 vpnrq.exe。

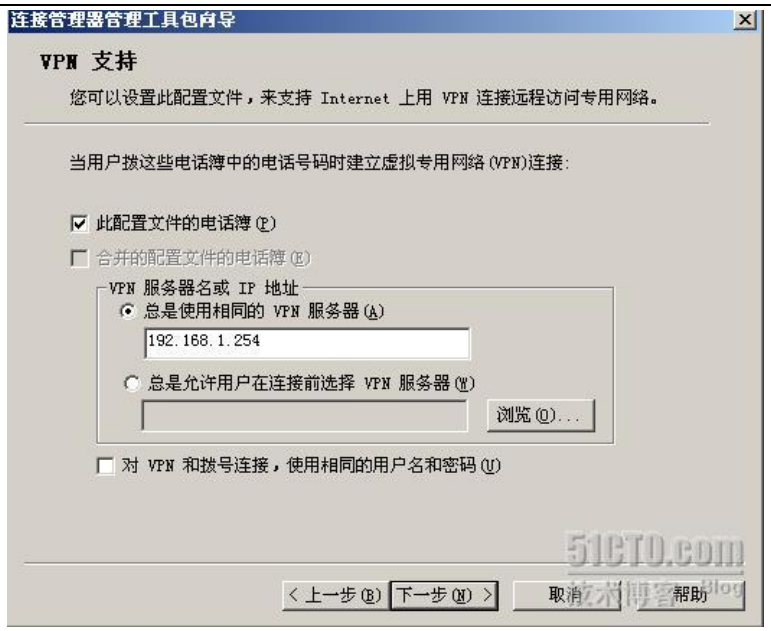


选择不再用户名中添加领域名，下一步继续。

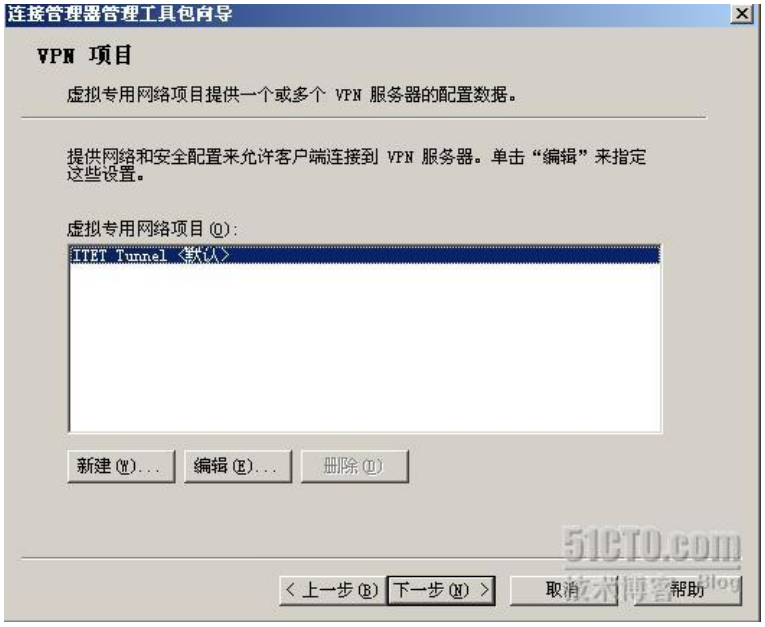
不需要合并配置文件，下一步继续。



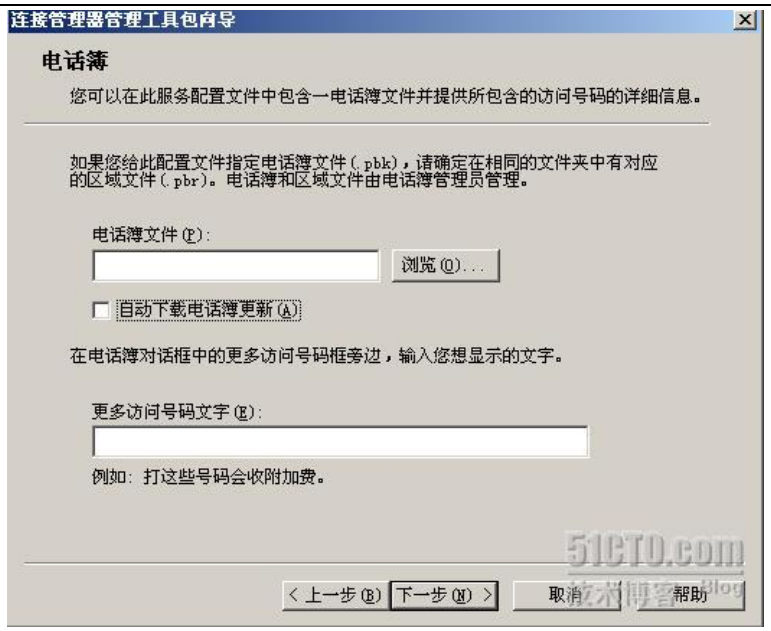
在电话簿中配置 VPN 服务器的 IP 地址或完全合格域名，在此我们使用的是 IP 地址。



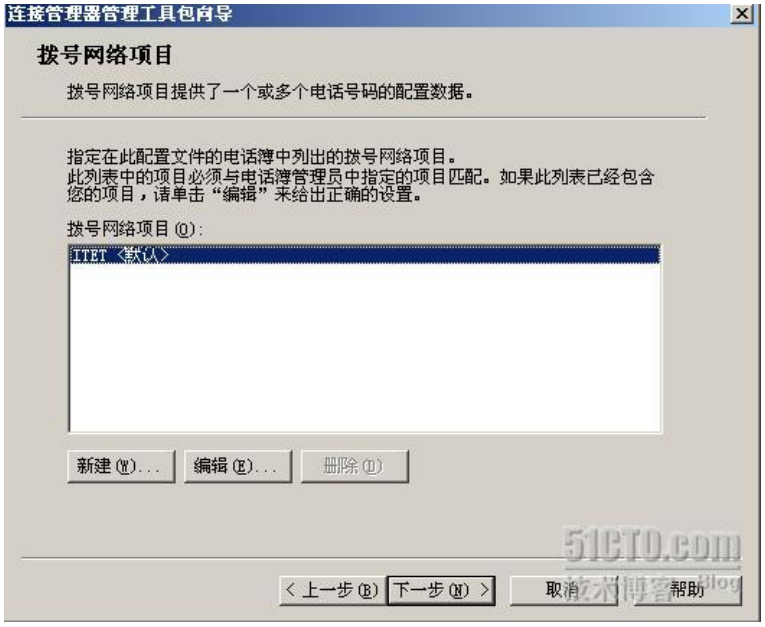
VPN 安全设置使用默认值，点击下一步继续。



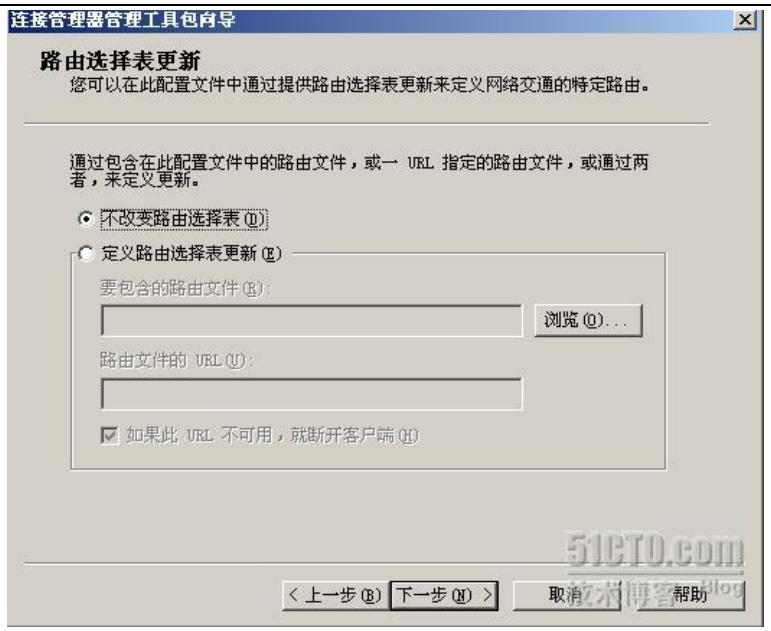
取消勾选“自动下载电话簿更新”，点击下一步继续。



检查拨号设置无误，点击下一步继续。



使用默认设置“不改变路由选择表”，点击下一步继续。



选择“不配置代理设置”，点击下一步继续。

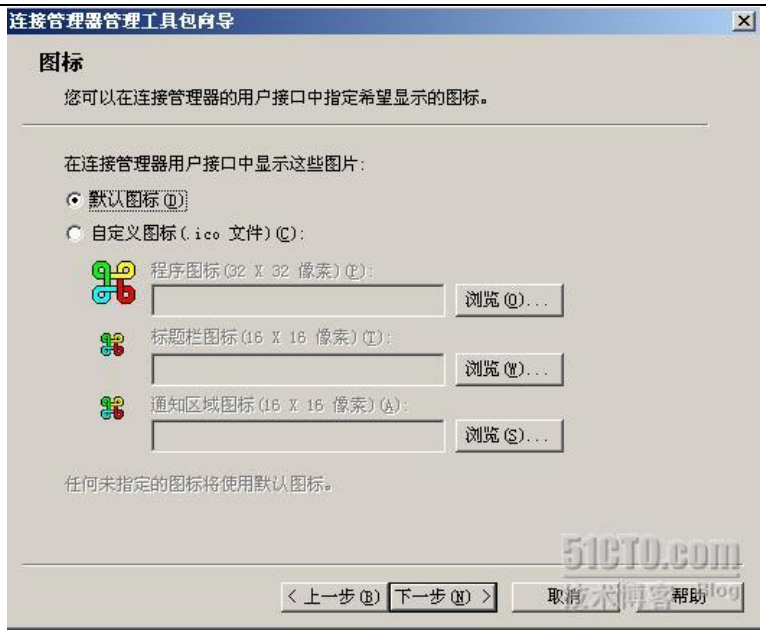
接下来是关键步骤，我们点击“新建”，准备自定义操作。

在新建的自定义操作中，我们选择使用 RQScript.vbs 来检查客户端的安全策略，传递的参数是%DialRasEntry%，%TunnelRasEntry%，%Domain%和%UserName%，操作类型是后连接，点击确定完成新建操作。

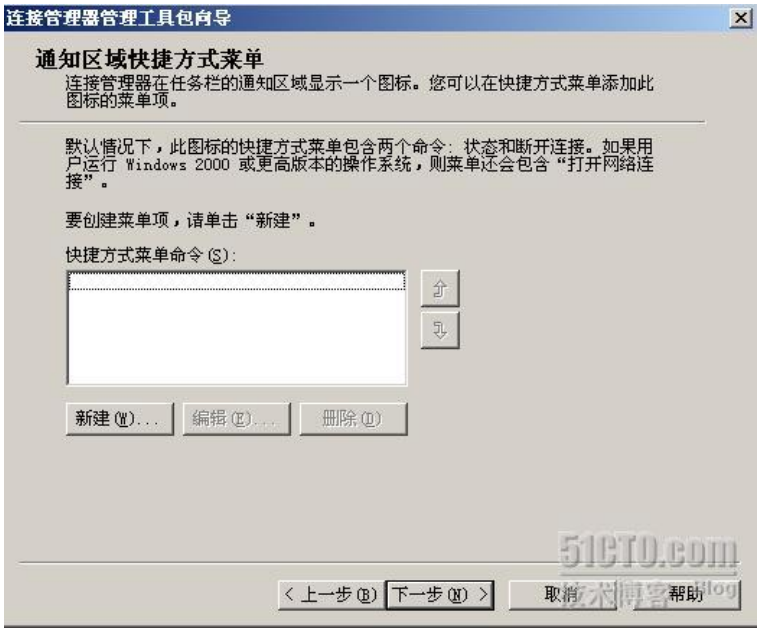
接下来设置登录位图，我们使用默认值，点击下一步继续。

电话簿位图，我们也取默认值，点击下一步继续。

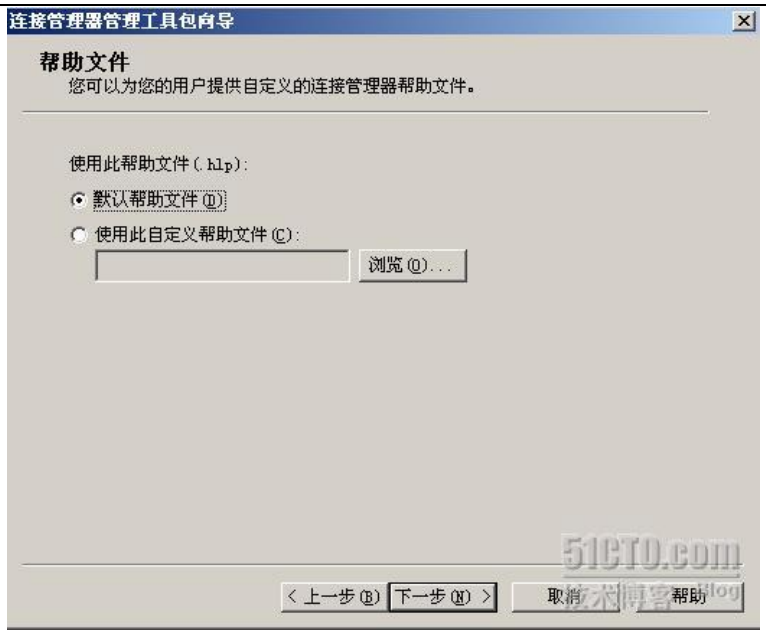
显示图标也使用默认值，点击下一步继续。



不在任务栏创建快捷方式，点击下一步继续。

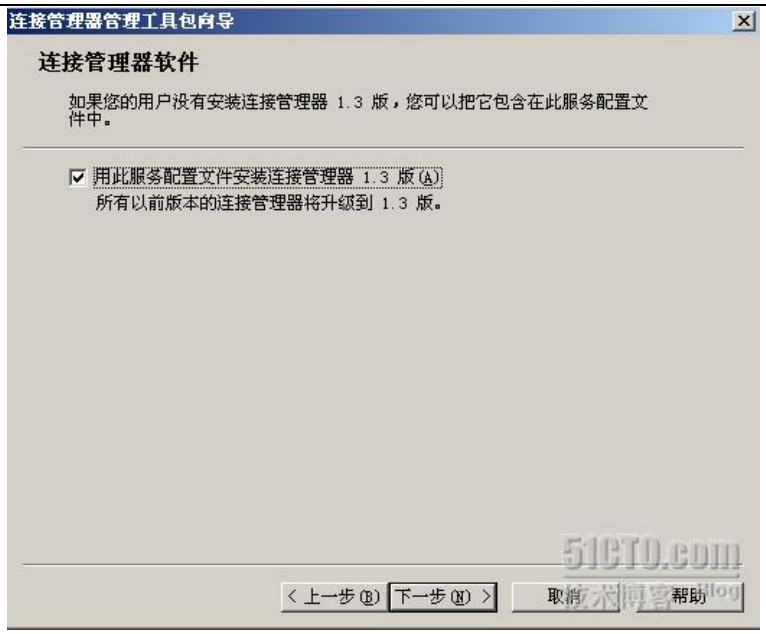


不指定帮助文件，点击下一步继续。



不需要输入登录对话框中的帮助信息，点击下一步继续。

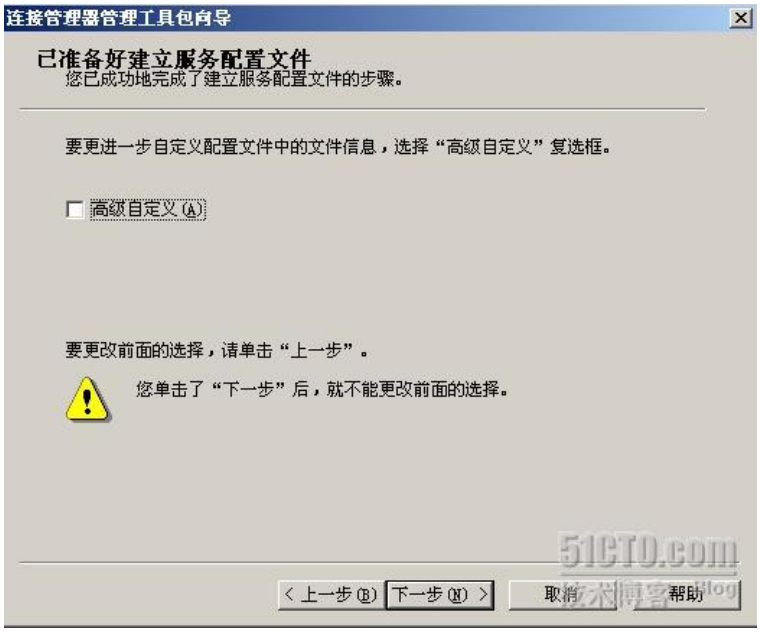
选择把连接管理器 1.3 版本集成在这个配置文件中。



不需要定制许可协议文件，点击下一步继续。

这一步也很重要，我们点击“添加”按钮把 rqc.exe 集成到配置文件中，这个文件在 Resource Kits 工具集中有提供，在 ISA 服务器的 C:Program FilesCmakSupport 中也有。

不选择高级自定义，点击下一步继续。

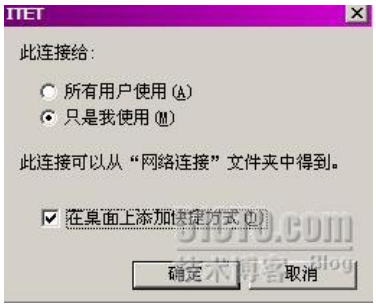


如下图所示，我们终于完成了定制的拨号配置文件，接下来我们只要把 vpnrq.exe 发给客户机，就可以在客户端进行 VPN 隔离的测试了。

六 VPN 隔离测试

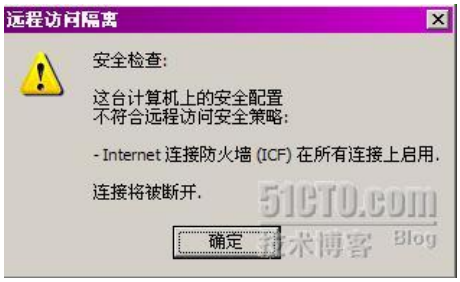
我们现在可以在 VPN 客户机 Istanbul 上开始测试了，首先我们先关闭 Istanbul 的防火墙，看看能否通过 VPN 的安全策略检查。我们在 Istanbul 上双击执行用连接管理器工具生成的配置文件 vpnrq.exe，如下图所示，安装程序询问是否安装 ITET 配置文件，选择“是”继续。

选择在桌面添加快捷方式，点击“确定”结束配置文件的安装。



双击执行桌面上的 ITET 图标，如下图所示，输入用户名和口令，点击“连接”。

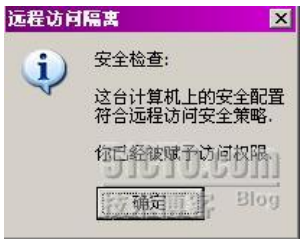
用户名和口令校验成功后，VPN 服务器提示已经成功拨入，但很快就弹出一个消息框，如下图所示，提示我们由于防火墙没有开启，因此 Istanbul 没有满足 VPN 隔离的安全策略检查，即将被断开连接。



过了预设的 60 秒后，VPN 连接被服务器中断，如下图所示，拨号连接询问是否要重新连接，点击“否”。

接下来我们看看在 Istanbul 上开启防火墙是否能够通过 VPN 隔离的安全策略检查，如下图所示，在网络连接的高级属性中，选择开启防火墙的保护。注意，Istanbul 的操作系统是 Win2003，如果操作系统是 Win2003 SP1，那么开启防火墙的方法就不是这样了，检查安全策略的脚本也要进行相应改变。

开启防火墙后再次拨入，如下图所示，系统提示 Istanbul 已经通过了安全策略检查，被赋予了访问权限，至此，VPN 隔离实验成功！

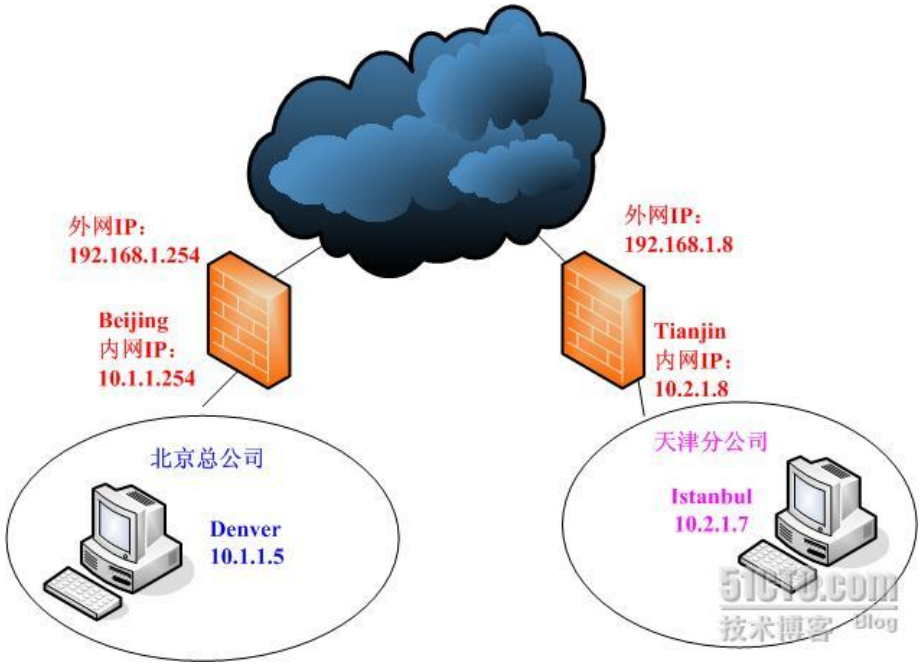


VPN 隔离是微软 NAP 中的一个重要环节，希望大家能够掌握这个功能。中间的步骤很多，但难度不大，真正困难的是安全策略检查脚本的撰写。

创建基于 PPTP 的站点到站点 VPN 连接：ISA2006 系列之二十五

在前面的博文中，我们已经介绍了如何用 ISA2006 创建 VPN 服务器，以及远程用户如何利用 VPN 服务器拨入内网。如果是个别用户在家办公或出差在外，用前文提到的 VPN 解决方案是可以圆满解决的。但如果是一群用户有互相访问的需求，例如某公司总部和分公司需要互相访问，那用 VPN 远程拨入的方式就显得效率不高了。试想一下，公司总部 500 人，分公司 300 人，如果要互相访问，800 人都要拨叫对方的 VPN 服务器，这显然不是一个好的解决方案。

今天我们提供一种站点到站点的 VPN 解决方案，可以很好地解决这个问题。我们引入下面的拓扑图来说明这个方案的构思，某公司北京总部的内网 IP 范围是 10.1.1.0，天津分公司的内网 IP 范围是 10.2.1.0。北京分公司使用一台 ISA 服务器连接到互联网，天津分公司也使用一台 ISA2006 连到公网。站点到站点的 VPN 指的是在两个公司的 ISA 服务器上配置好 VPN 的拨入拨出参数，确保两个 ISA 服务器既可以拨叫对方的 VPN 服务器，也可以接受对方 VPN 服务器的拨叫。这样一来用户只要把默认网关指向自己的 ISA 服务器，就可以不用拨叫对方公司的 VPN 服务器了，全部由 ISA 代劳了。例如北京公司的 Denver 要访问天津公司的 Istanbul，Denver 只要把访问 Istanbul 的请求提交给自己的默认网关－Beijing，剩下的事就不用管了，Beijing 会自动拨叫天津公司的 ISA 服务器 Tianjin，然后在两个 ISA 服务器之间创建完成 VPN 隧道，接下来 Denver 的访问请求就被 Beijing 通过 VPN 隧道路由到天津公司的 Istanbul 上了。你看，这样一来两个公司员工互访时就很方便了，只要把网关指向自己的 ISA 服务器，然后就可以透明地访问对方公司的内网，效率是不是有很大的提高呢？



创建站点间的 VPN 需要在两个 VPN 服务器上都进行设置，两个 ISA 服务器上的操作具有对称性，我们先以 Beijing 上的操作为例进行详细讲解，目前 Beijing 已做了下列准备：

1、 防火墙策略中允许内网和本地主机任意访问。

2、 启用了 VPN，允许使用 PPTP 和 L2TP。

3、 VPN 地址池的范围是 192.168.100.1－192.168.100.200。

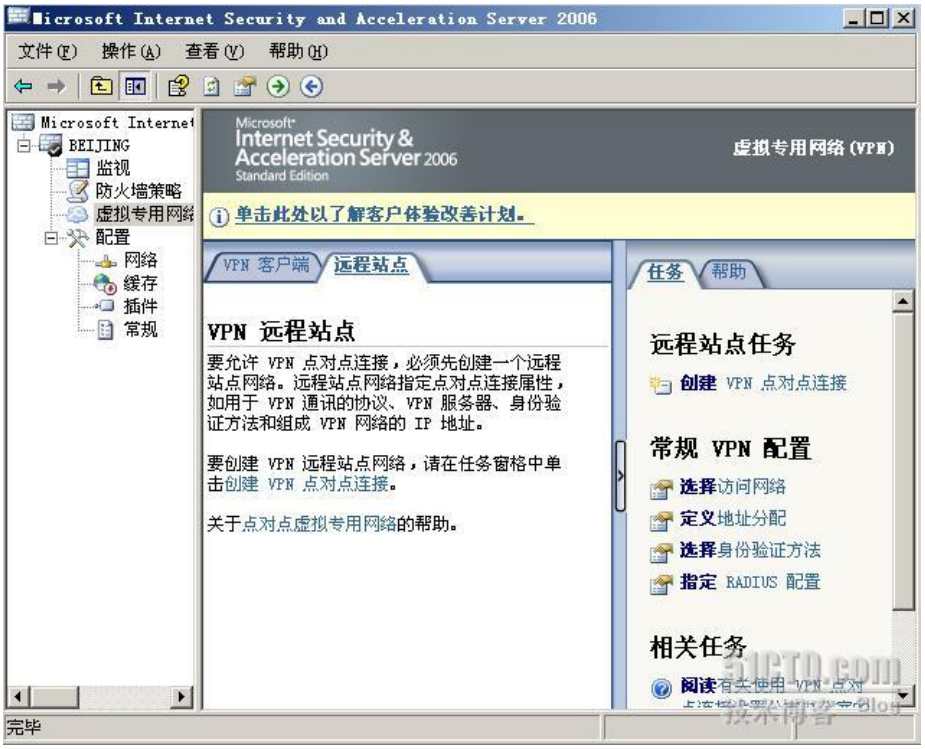
一 创建远程站点

创建远程站点是部署站点间 VPN 最重要的一步，远程站点其实是一个自定义的远程网络，具体到 Beijing，其实就是要把天津分公司的内网 10.2.1.0 定义为一个远程网络。为什么需要把对方公司的内网定义成一个新的网络呢？因为我们知道网络是 ISA 进行访问控制的基本管理单元，ISA 考察一个访问请求时首先要考虑源网络和目标网络的网络规则。如果不定义远程网络，天津分公司对 Beijing 来说属于外网范畴，而内网到外网的网络规则是 NAT，因此 Beijing 不会允许从天津的 Istanbul 访问北京的 Denver。这就是我们为什么要把

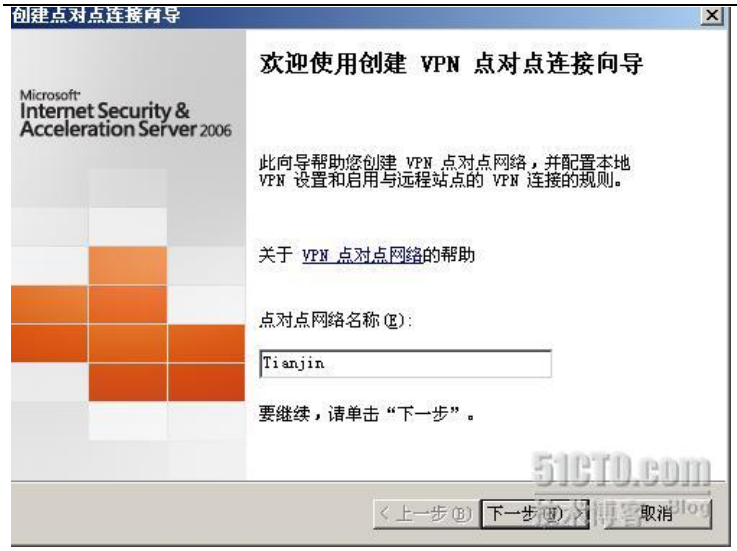
天津公司的内网定义为一个新的网络，只有这样我们才可以重新定义北京内网和天津内网的网络规则，进而制定出符合要求的防火墙策略。

创建远程站点还涉及到创建 VPN 隧道的参数设定，例如 Beijing 把天津分公司的内网定义为远程网络，那 Beijing 上就必须定义好连接这个远程网络要通过哪个 VPN 服务器，两个 VPN 服务器使用哪种协议，如何进行身份验证等，下面我们就来具体看看如何在 Beijing 上创建远程站点。

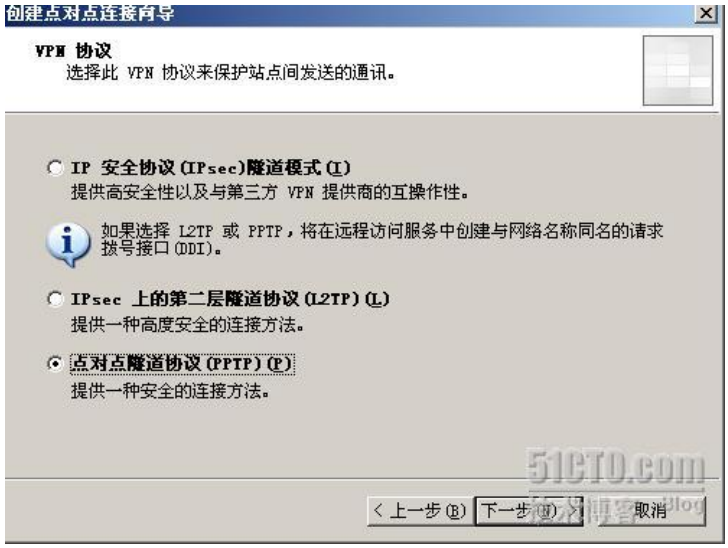
在 Beijing 上打开 ISA 管理器，切换到虚拟专用网络，如下图所示，在“远程站点”标签下选择“创建 VPN 点对点连接”。



出现创建 VPN 点对点连接向导，其实就是远程站点的创建向导，首先我们要为远程站点起个名字，如下图所示，我们为远程站点命名为 Tianjin。这个远程站点的名字可不是随便取的，后面我们会知道 ISA 服务器上必须创建一个和远程站点同名的用户。

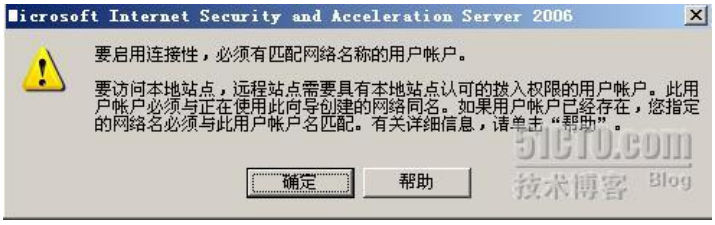


接下来要选择 VPN 站点间连接要使用的协议，如果两个 VPN 服务器都是 ISA，那可以选择 PPTP 或 L2TP，如果是 ISA 和硬件 VPN 组成站点间连接，那应该选择 IPSEC。在这个实验中我们选择使用 PPTP 作为站点间 VPN 使用的隧道协议。



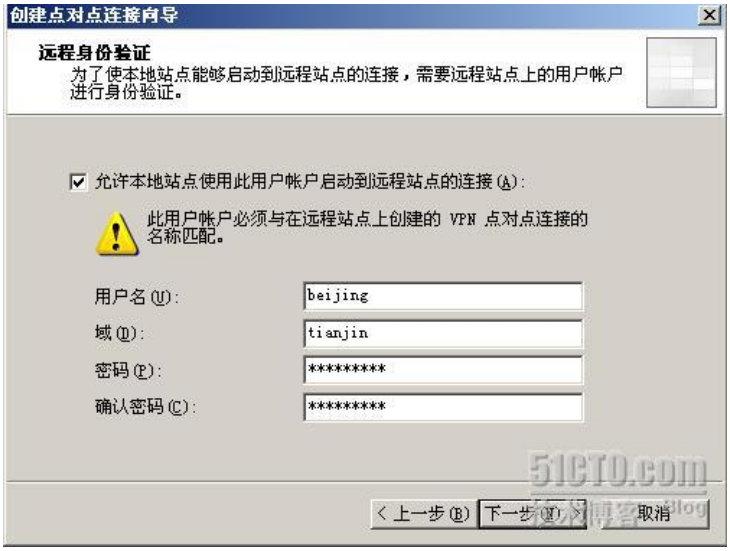
如下图所示，系统会弹出一个对话框提示你在 ISA 服务器上必须有一个和远程站点同名的用户，而且用户必须有拨入权限。也就是说 Beijing 创建了一个远程站点 Tianjin 后，Beijing 服务器上必须有一个名为 Tianjian 的具有远程拨入权限的用户。如果 Beijing 隶属于域，那么 Tianjin 这个用户也可以在域控制器上创建。创建出的这个用户是为天津公司的 VPN 服务器拨叫北京公司的 VPN 服务器准备的，天津公司的用户通过他们的 VPN 服务器拨

叫北京的 VPN 服务器时，如果天津用户源于 tianjin 这个远程网络，那天津的 VPN 服务器必须使用 tianjin 作为用户名进行身份验证。由于微软这么一个奇怪的规定，我们必须在北京的 ISA 服务器上准备好 tianjin 这个用户。



接下来要填写远程站点的 VPN 服务器的 IP 地址或域名，天津的 VPN 服务器 IP 是 192.168.1.8。

下面设定的是 beijing 拨叫天津的 VPN 服务器时进行身份验证的凭据，显然，tianjin 上也要有个名为 beijing 的用户，在后续的操作中我们会在 tianjin 上创建这个用户。



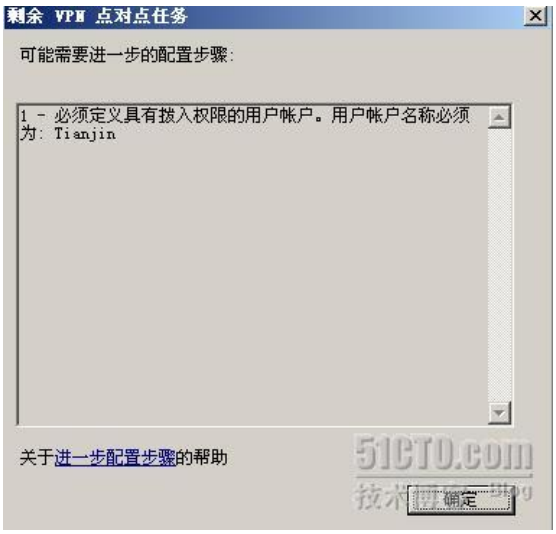
接下来我们要定义远程站点的 IP 地址范围，如下图所示，远程站点的地址范围是 10.2.1.0－10.2.1.255。

接下来 VPN 创建向导建议创建一个网络规则，从远程站点到内网，网络规则是路由关系。这个提示很人性化，是 ISA2006 比 ISA2004 改进的地方。

创建完网络规则后，向导又很贴心地建议我们创建一条访问规则，允许内网和远程站点互相访问。

点击完成结束 VPN 创建向导。

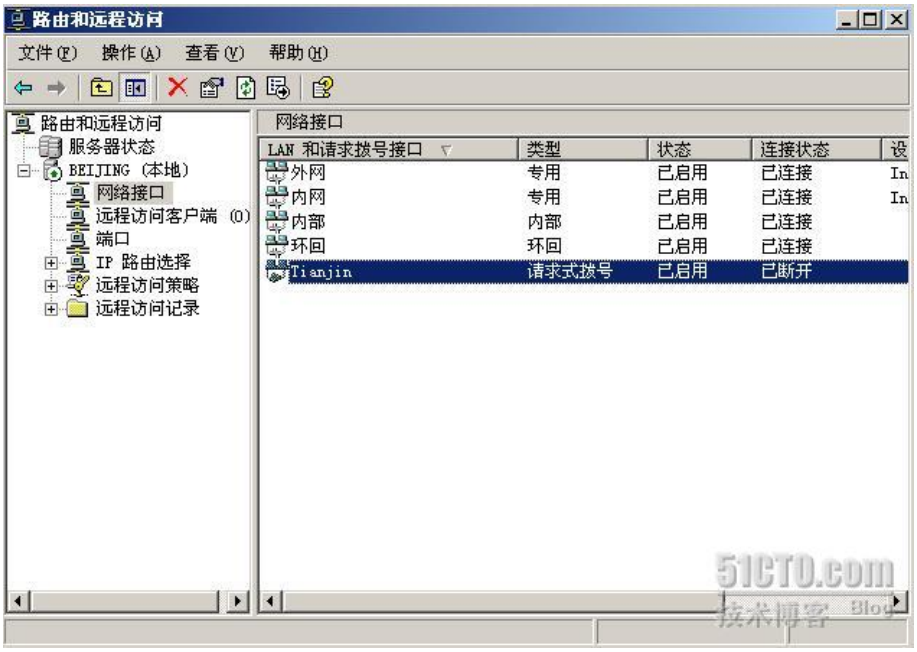
向导结束后再次提示我们要创建一个名为 Tianjin 的用户，而且要允许远程访问。



远程站点创建完毕后，如下图所示，我们发现在向导的指引下，远程站点到内网的网络规则已经被创建了，而且网络关系是路由。

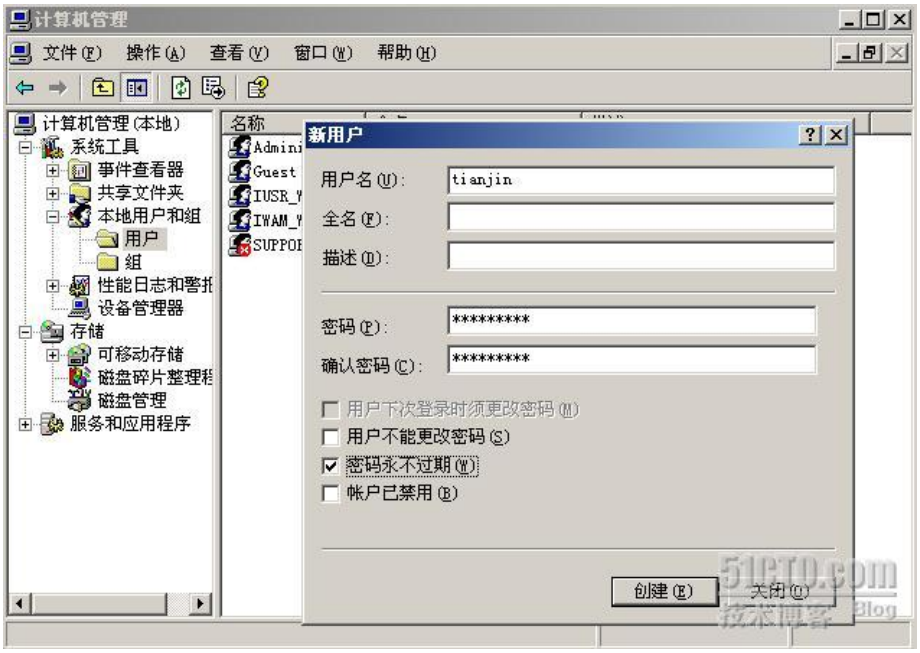
如下图所示，向导还帮助我们创建了访问规则，允许远程站点和内网互相访问。

如下图所示，向导还在路由和远程访问中创建了请求式拨号，当北京公司要访问天津公司时，Beijing 会自动拨叫天津的 VPN 服务器，创建出 VPN 隧道，供用户访问使用。

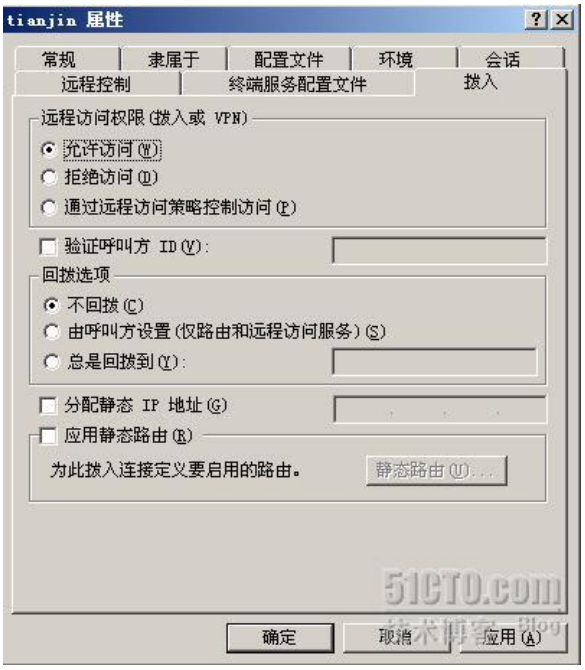


二 创建与远程站点同名的用户

最后不要忘记创建与远程站点同名的用户，如果 Beijing 加入域，那么既可以在 Beijing 服务器上创建这个用户，也可以在域控制器上创建这个用户。由于本例中 Beijing 和 Tianjin 两个 ISA 服务器都在工作组中，因此我们只能在 ISA 服务器上创建这个远程访问用户了。如下图所示，在 Beijing 的计算机管理工具中选择新建一个名为 Tianjin 的用户。



用户创建完毕后不要忘记用户的远程访问权限，如下图所示，在用户属性的拨入标签中将用户的远程访问权限设为允许访问。



OK，至此我们完成了在 Beijing 上的设置，总结如下：

1、 将天津分公司的内网定义成远程站点

2、 创建远程站点和内网的网络规则

3、 创建远程站点和内网的访问规则

4、 创建与远程站点同名的用户

接下来轮到 Tianjin 服务器了，Tianjin 上同样已进行了如下准备：

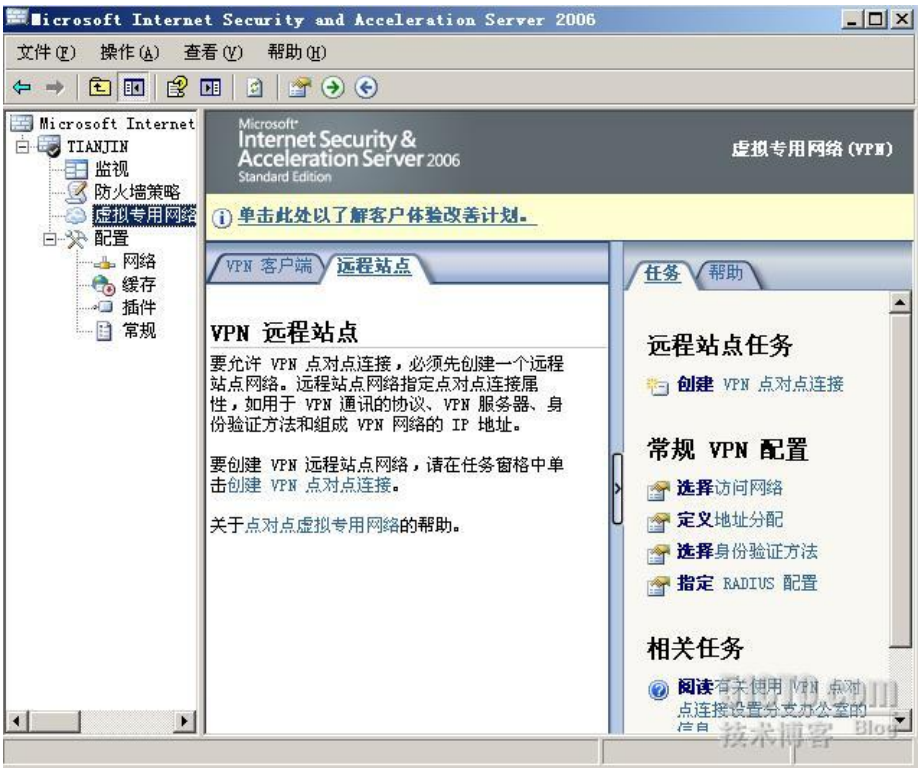
1、 允许内网和本地主机任意访问

2、 启用 VPN

3、 VPN 地址池的范围是 192.168.200.1－192.168.200.200

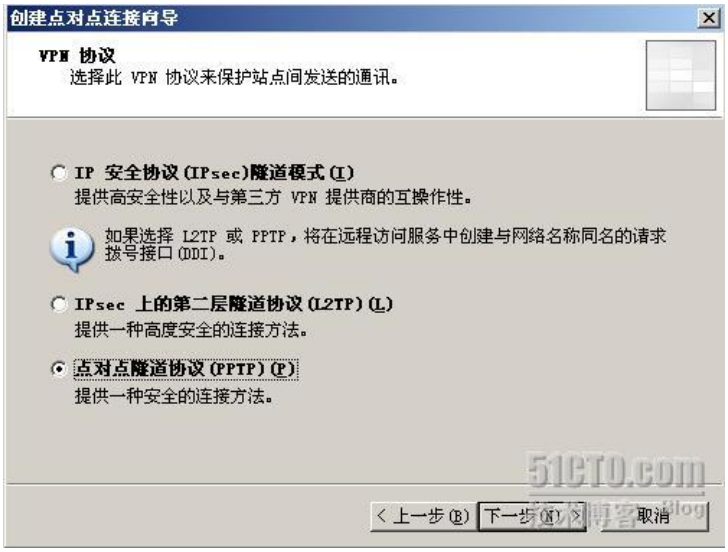
一 创建远程站点

Tianjian 服务器上的设置基本和 Beijing 完全对称，首先仍然是需要创建远程站点。如下图所示，在 Tianjin 的 ISA 管理器中选择“创建 VPN 点对点连接”。



为远程站点命名为 Beijing。

站点间 VPN 连接使用的协议是 PPTP，Tianjin 选择的 VPN 协议要和 Beijing 完全一致。



连接到远程站点，需要经过 192.168.1.254－北京公司的 VPN 服务器。

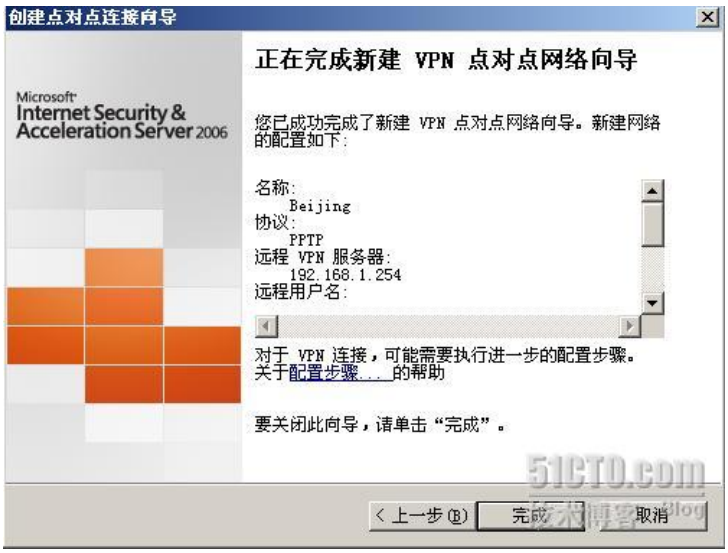
Tianjin 拨叫北京的 VPN 服务器时，进行身份验证时所输入的用户名和密码要匹配 Beijing 服务器上刚创建的用户账号。

定义远程站点的地址范围，输入北京公司的内网范围 10.1.1.0－10.1.1.255。

接下来要创建远程站点和内网的网络规则，仍然是路由关系。

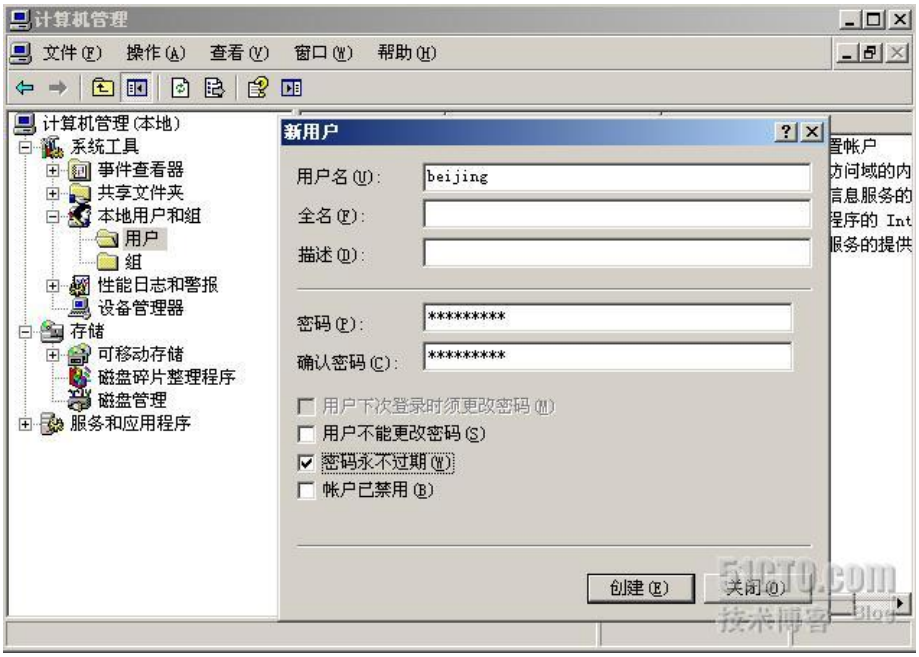
然后创建访问规则允许内网和远程站点互相访问。

点击完成结束远程站点创建。

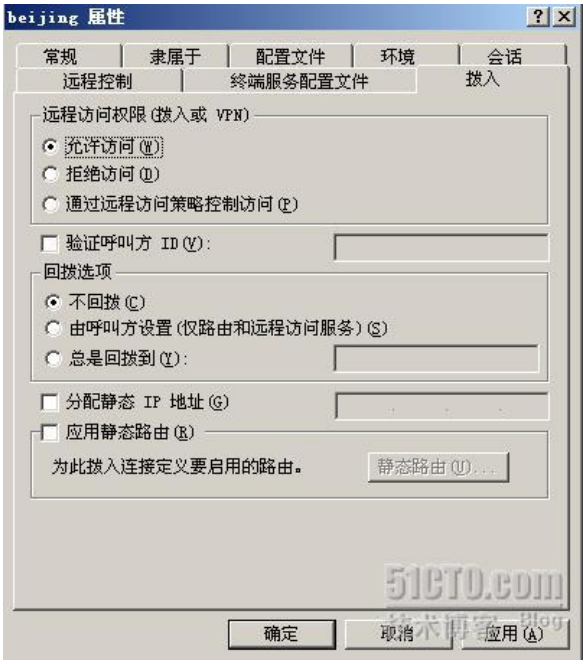


二 创建与远程站点同名的用户

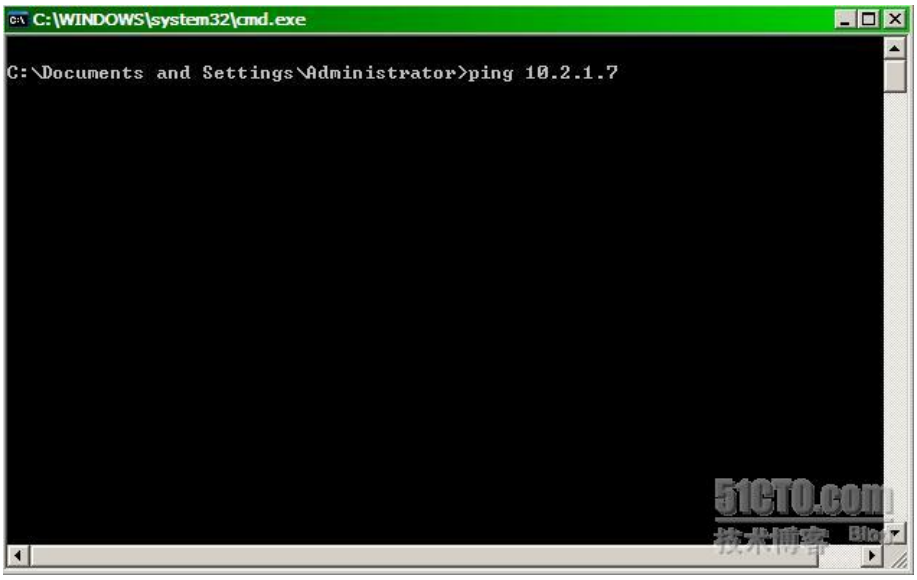
创建完远程站点后，接下来就该创建与远程站点同名的用户了，如下图所示，我们在 Tianjin 服务器上创建了用户 Beijing。注意，在本次实验中为简单起见，Beijing 和 Tianjin 两个 ISA 服务器都没有加入域，因此用户在 ISA 本机创建。如在生产环境中 ISA 已经加入了域，一般会在域控制器上创建这个用户。



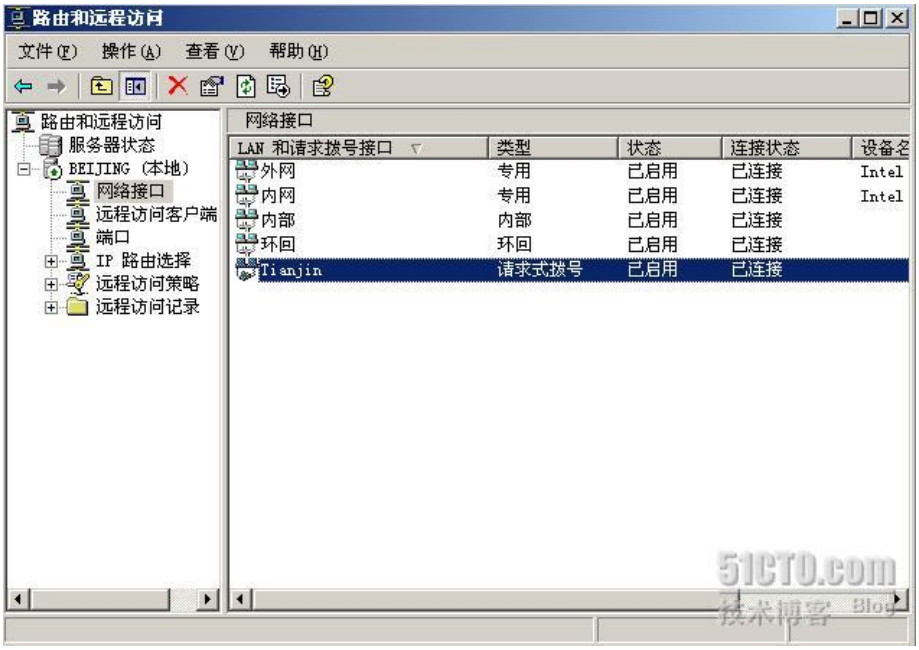
最后别忘了设定用户的远程访问权限，相信在 Beijing 上做完一遍之后，大家在 Tianjin 上进行操作时已经是轻车熟路了。



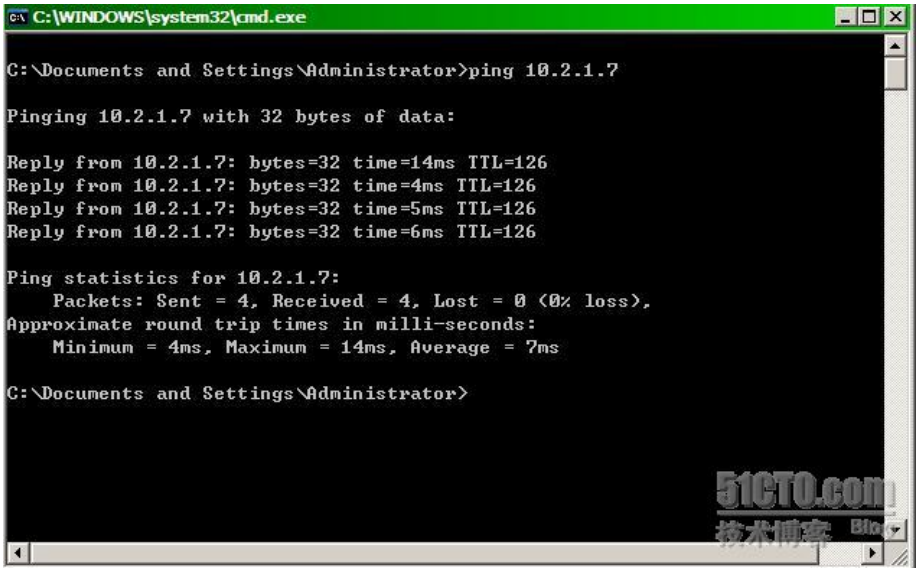
两端的 VPN 服务器配置完毕后，我们接下来要在内网的客户机上进行测试了，如下图所示，我们在北京的 Denver 上 ping 天津公司的 Istanbul。



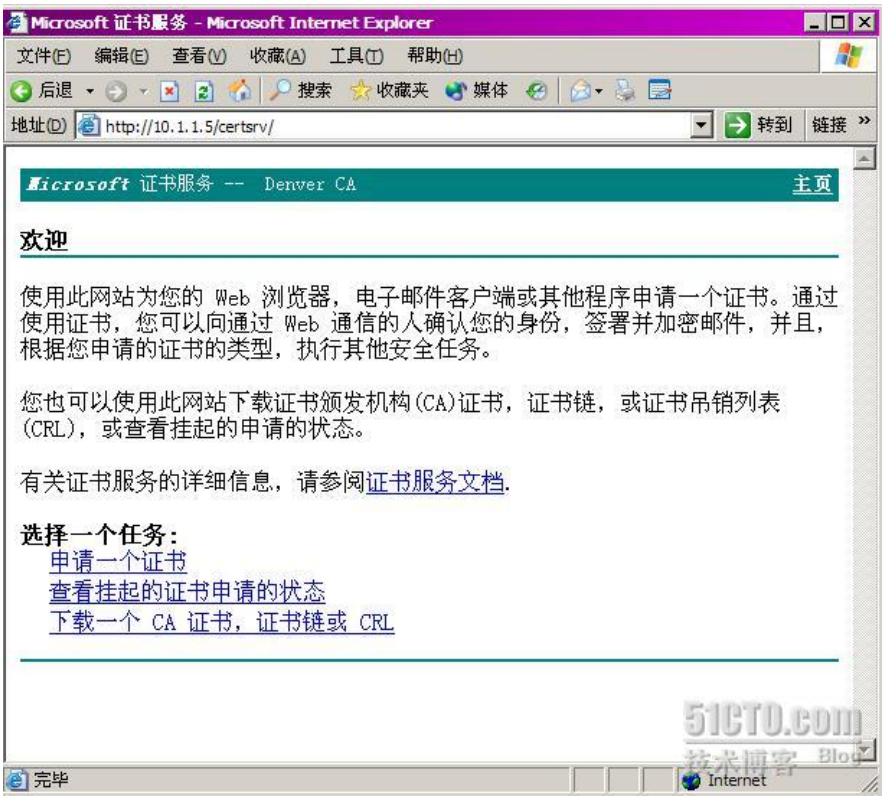
Denver 访问天津内网的 Istanbul 不需要自己进行 VPN 远程拨号，只要把访问请求提交给 Beijing 就可以了。这时打开 Beijing 的路由和远程访问，如下图所示，我们发现 Tianjin 这个请求式拨号的状态已经从断开变成了已连接。



如下图所示，我们发现 Denver 已经可以 ping 到 Istanbul 了，实验成功。有一点要注意，有时请求式拨号连接的时间会稍长一些，可能前面的一些 ping 包会显示 Time out，这是正常现象，稍等片刻即可正常。



最后试试在 Istanbul 上访问 Denver，如下图所示，访问成功，至此，实验顺利完成。

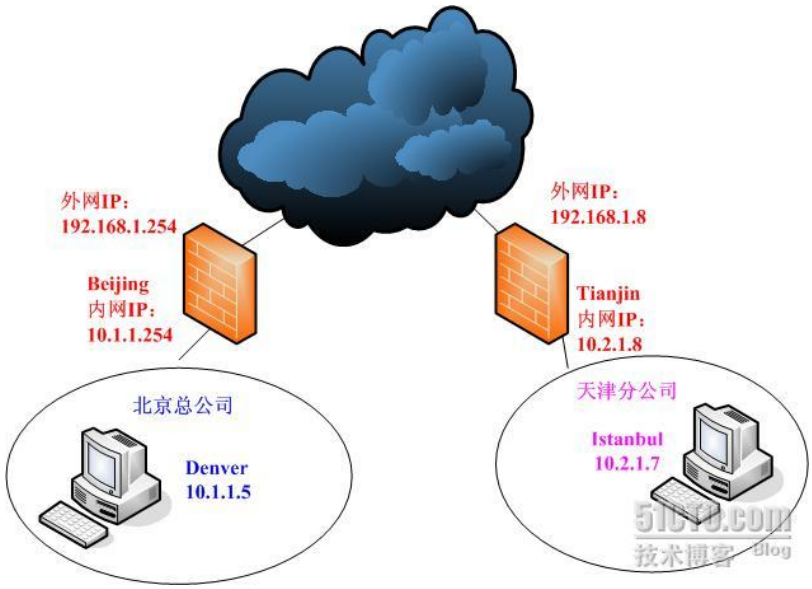


创建站点间的 VPN 不是难度很大的技术问题，如果两端的 VPN 服务器中有硬件 VPN，那就应该使用 IPSEC。如果两端的 VPN 都是微软的 ISA 或路由与远程访问，那就推荐使用 PPTP 或 L2TP。ISA 间并非不能使用 IPSEC，只是使用经验告诉我这种拓扑并不稳定，当然，ISA2006 的 SP1 可能会解决这个问题，大家有兴趣可以测试一下。

创建基于 L2TP 的站点到站点的 VPN 连接：ISA2006 系列之二十六

在上篇博文中我们介绍了如何利用 ISA2006 创建站点间的 VPN，而且站点间 VPN 使用的隧道协议是 PPTP，今天我们更进一步，准备在上篇博文的基础上实现基于 L2TP 的站点间 VPN。L2TP 和 PPTP 相比，增加了对计算机的身份验证，从理论上分析应该比 PPTP 更安

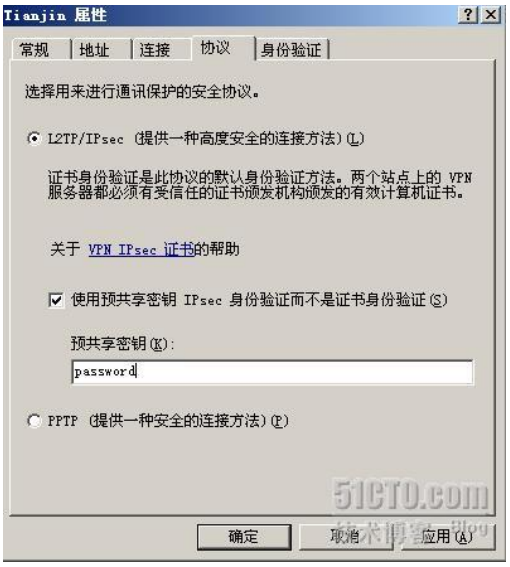
全一些。L2TP 验证计算机身份可以使用预共享密钥，也可以使用证书。我们把两种方式都尝试一下，实验拓扑如下图所示，和上篇博文的环境完全一致。



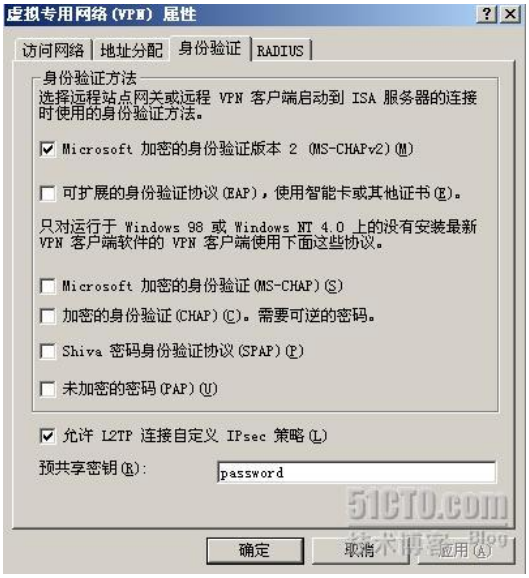
一 使用预共享密钥

使用预共享密钥实现 L2TP 的过程是是比较简单的，我们在 VPN 站点两端的 VPN 服务器上配置一个相同的预共享密钥，就可以用于 L2TP 协议中验证计算机身份。如下图所示，我们在 Beijing 上定位到“虚拟专用网络”，右键点击远程站点 Tianjin，选择“属性”。

我们在远程站点 Tianjin 的属性中切换到“协议”标签，勾选使用“L2TP/IPSEC”，同时勾选使用预共享密钥，并设置预共享密钥为 password。这里的设置会导致 beijing 拨叫 tianjin 时，使用预共享密钥 password 来证明自己的身份。

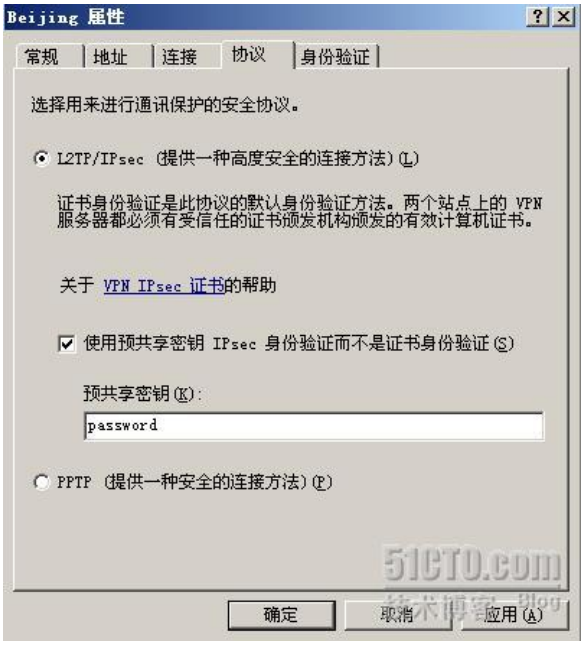


在“常规 VPN 配置”中点击“选择身份验证方法”，如下图所示，勾选“允许 L2TP 连接自定义 IPSEC 策略”，并设置预共享密钥为 password。这个设置则是告诉 beijing，接受 VPN 客户端使用预共享密钥验证计算机身份。这样我们分别设置了 beijing 作为 VPN 服务器和 VPN 客户端都使用预共享密钥验证计算机身份，至此，Beijing 服务器设置完毕。

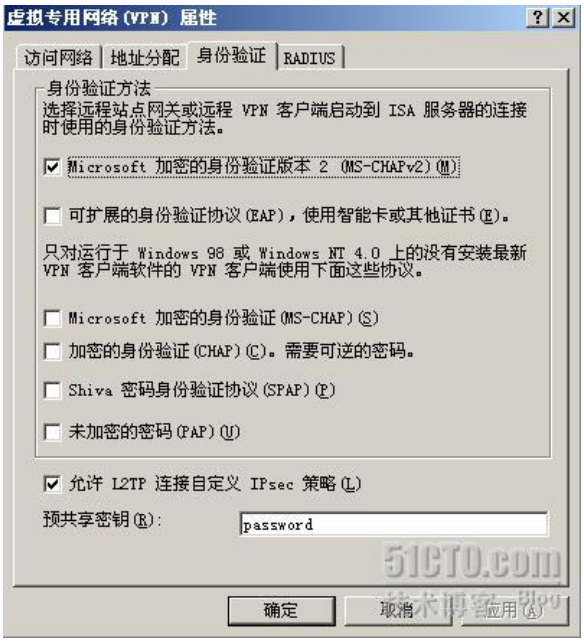


接下来我们在 Tianjin 服务器上如法炮制，如下图所示，选择远程站点 Beijing 的属性。

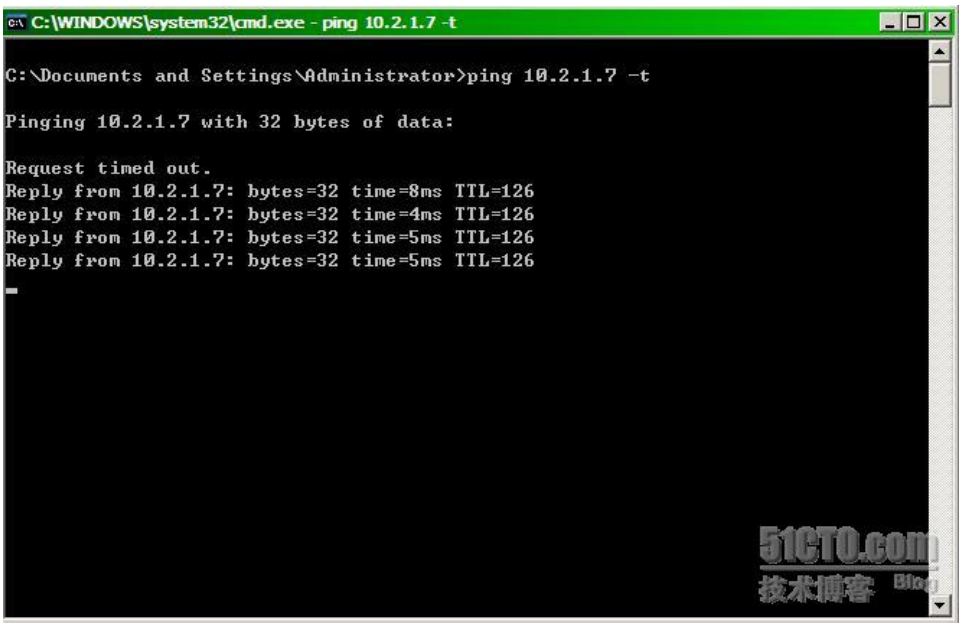
在远程站点的属性中切换到“协议”标签，如下图所示，选择使用 L2TP 作为 VPN 协议，并配置预共享密钥为 password。



然后在“常规 VPN 配置”中点击“选择身份验证方法”，如下图所示，勾选“允许 L2TP 连接自定义 IPSEC 策略”，并设置预共享密钥为 password。至此，Tianjin 服务器也设置完毕。



这时我们来看看站点间 VPN 配置的成果，如下图所示，在北京内网的 Denver 上 ping 天津内网的 Istanbul。第一个包没有 ping 通，这是因为两个 ISA 服务器正在创建 VPN 隧道，接下来的包都可以顺利往返，这证明我们的配置起作用了。

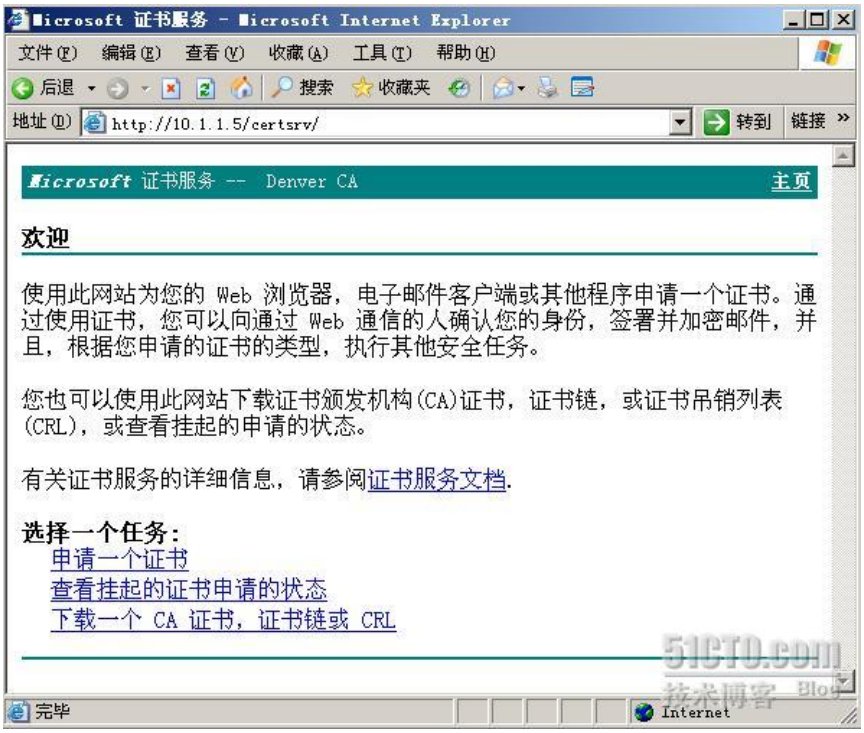


二 使用证书验证

使用证书验证比预共享密钥验证更加安全，只是实现起来要麻烦一些，我们需要有 CA 的配合。在我们的实验环境中，Denver 是一个被所有的实验计算机都信任的 CA，Denver 的 CA 类型是独立根。有了 CA 之后，VPN 服务器需要向 CA 申请证书以证明自己的身份，由于站点间 VPN 中每个 VPN 服务器既是服务器又充当客户机角色，因此每个 VPN 服务器都需要申请两个证书，一个是服务器证书，一个是客户机证书。

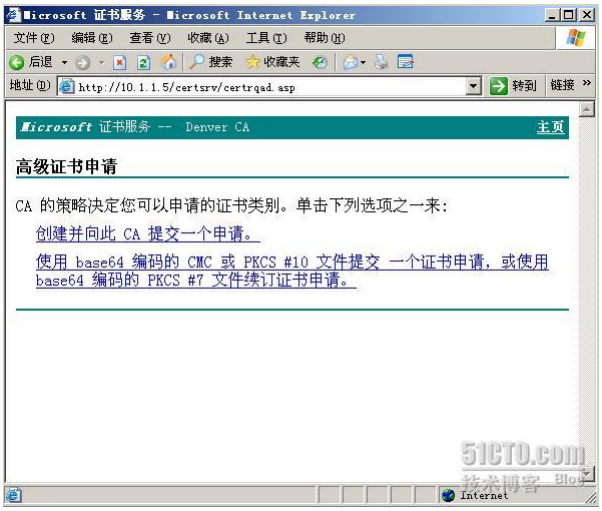
1、 在 Beijing 上进行配置

首先我们要先为 Beijing 申请两个证书，一个是服务器证书，一个是客户机证书。如下图所示，在 Beijing 上我们在 IE 中输入 http://10.1.1.5/certsrv，在 CA 主页中选择“申请一个证书”。

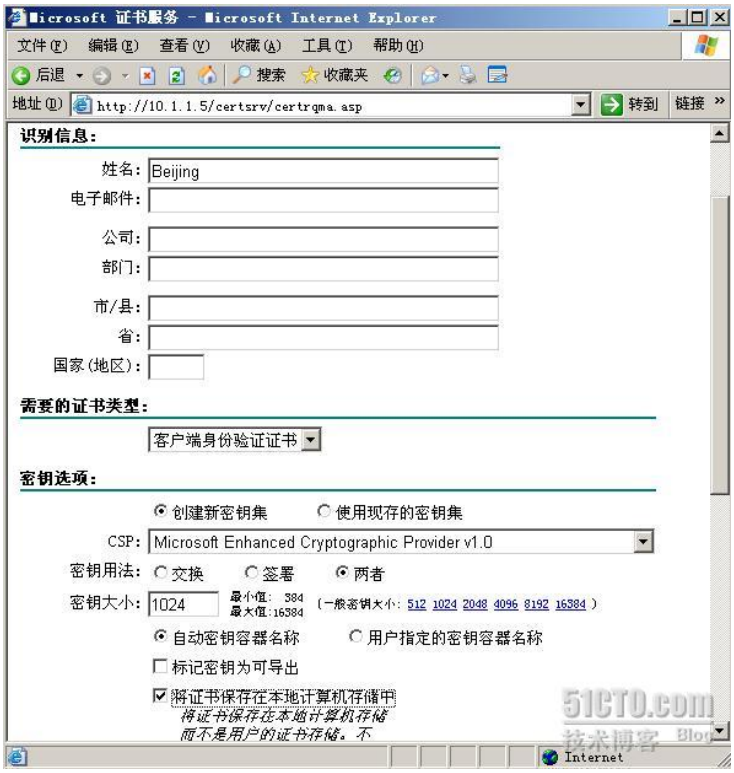


选择“提交一个高级证书申请”。

选择“创建并向此 CA 提交一个申请”。

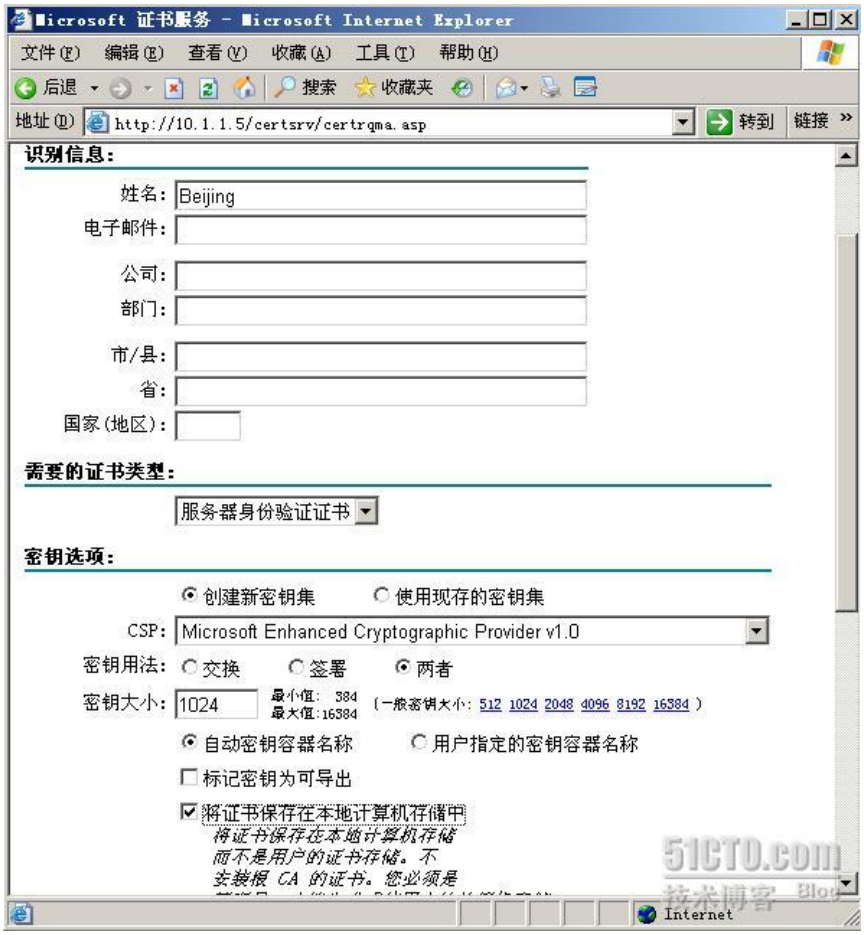


如下图所示，我们在证书申请的表单中选择申请一个客户机证书，并且把证书存储在计算机存储中。



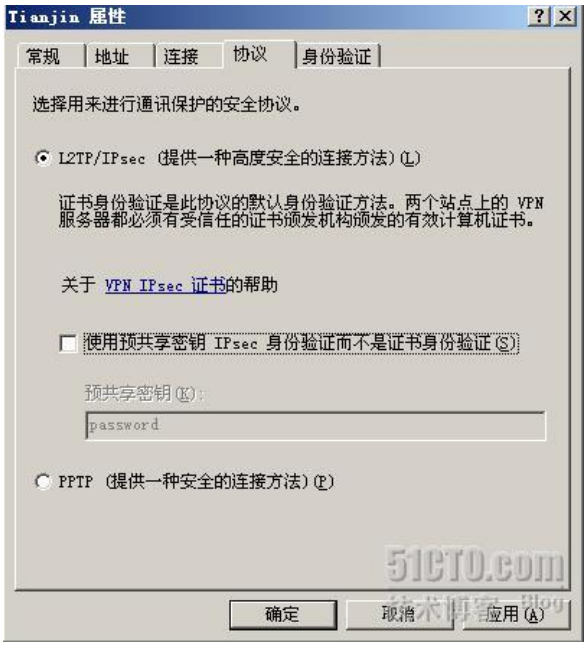
提交证书申请后，如下图所示，我们发现 Beijing 申请的证书已经被 CA 发放了，点击安装此证书即可完成任务。

接下来如法炮制为 Beijing 申请服务器证书，如下图所示，这次为 Beijing 申请的是服务器证书，仍然存储在本地计算机存储中，接下来的证书发放以及安装就不再赘述。

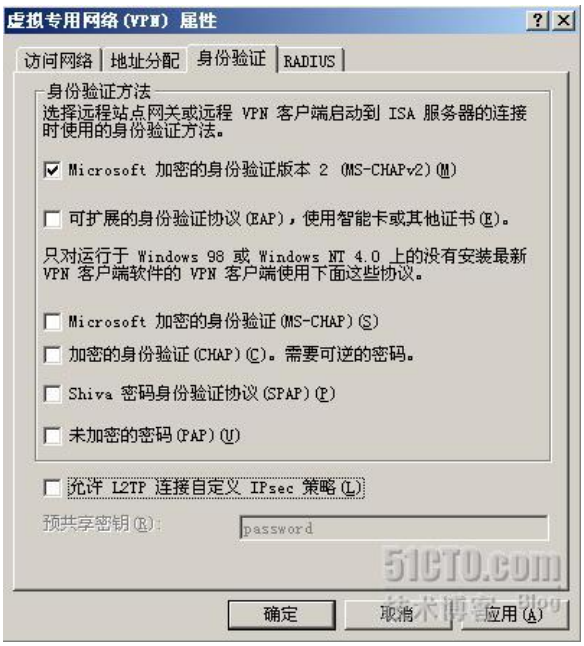


如下图所示，我们可以看到 Beijing 的计算机存储中已经有了刚申请的两个证书，

接下来在远程站点属性中取消使用预共享密钥验证身份。

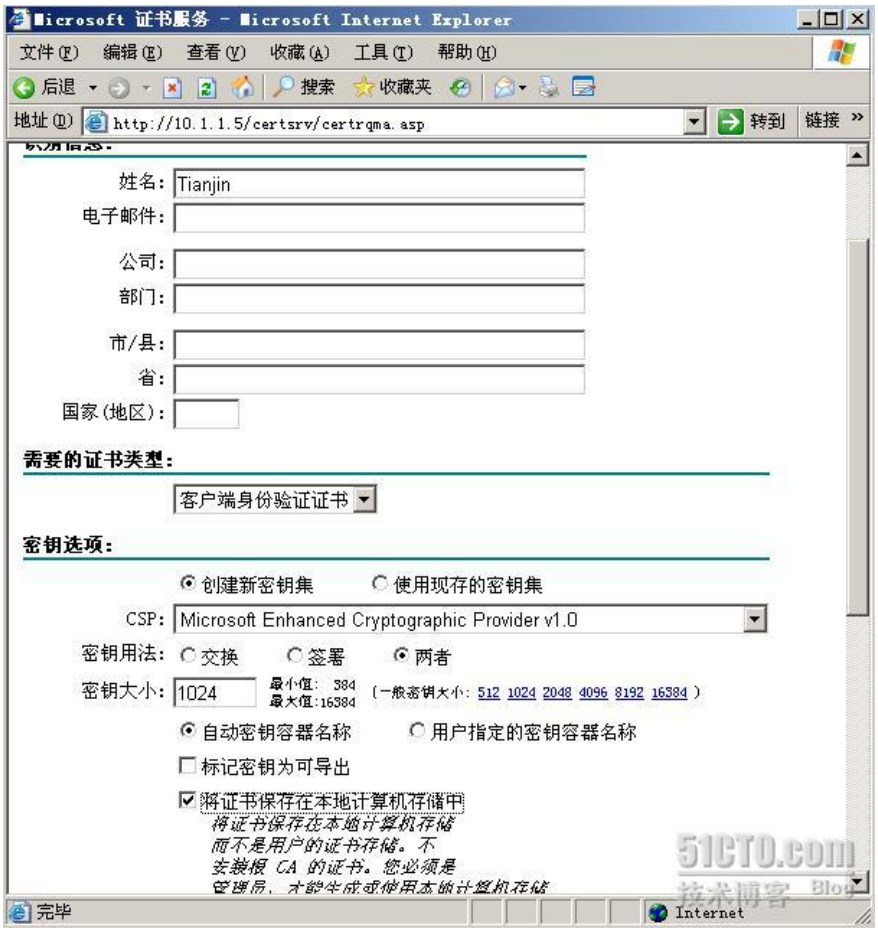


然后在 VPN 常规配置的选择身份验证方法中同样取消使用预共享密钥验证身份，至此，我们在 Beijing 上配置完毕。

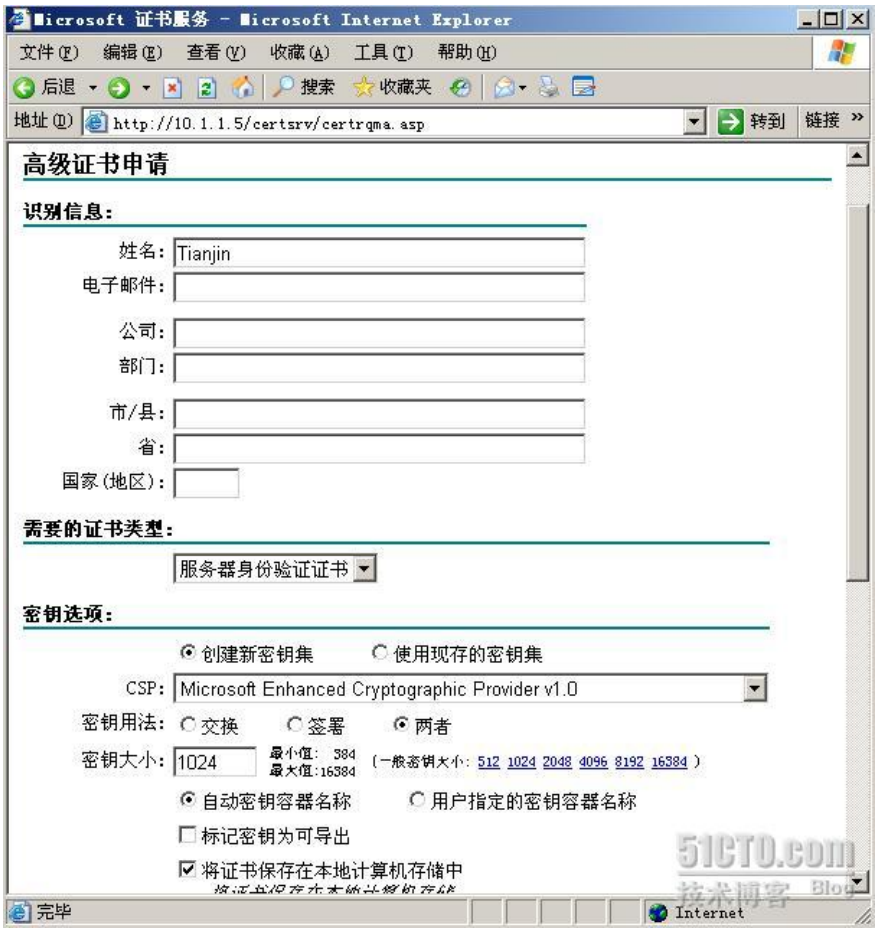


2、 在 Tianjin 上进行配置

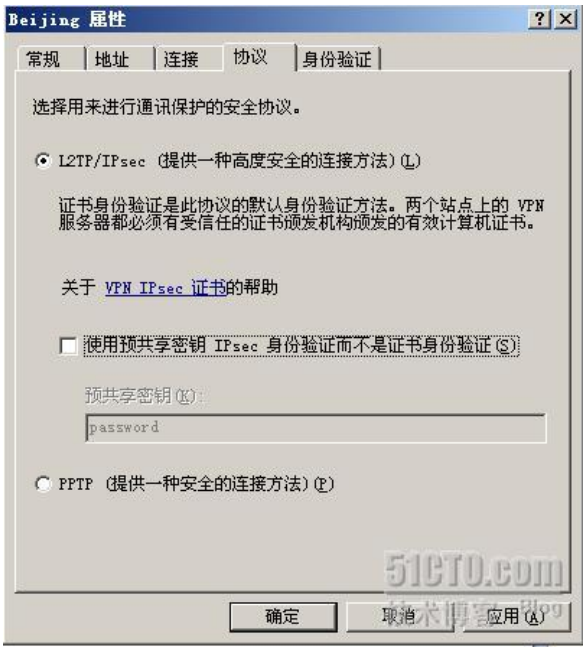
在 Tianjin 上进行配置基本和 Beijing 是一样的，首先也是先从 Denver 申请证书，如下图所示，Tianjin 先申请的是一个客户机证书。



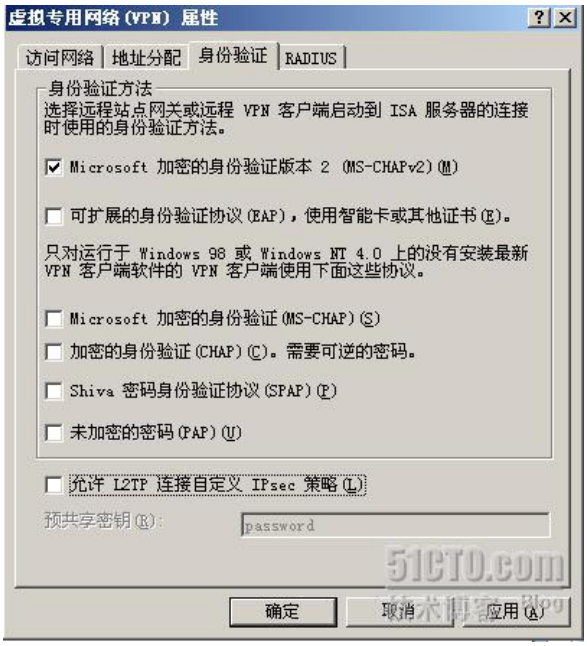
申请完客户机证书后，如下图所示，Tianjin 又申请了一个服务器证书。



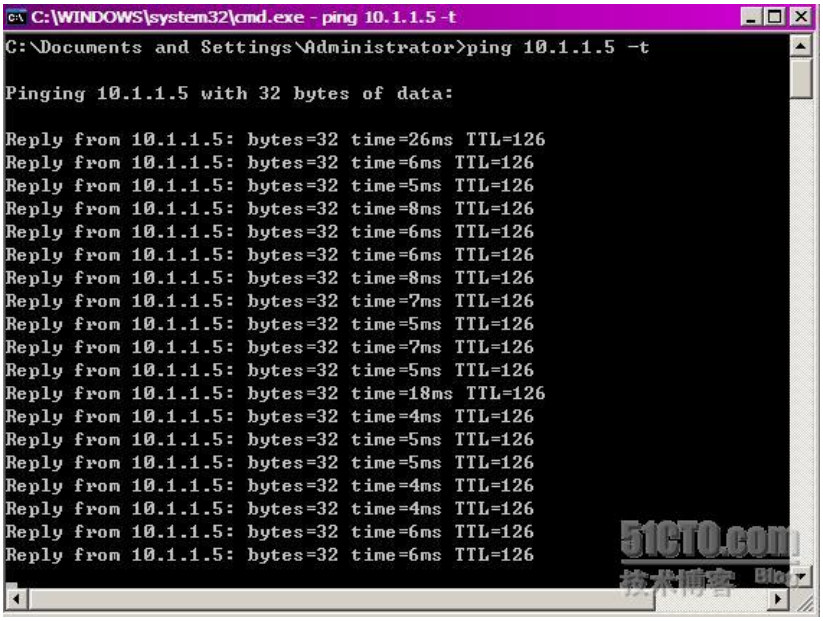
接下来就是在远程站点中取消使用预共享密钥。



最后在 VPN 常规配置的身份验证方法中取消使用预共享密钥。



OK，两个 VPN 服务器都进行了对称配置，这下他们在进行身份验证时只能使用证书了。用客户机测试一下效果吧，如下图所示，在天津的 Istanbul 上 ping 北京的 Denver，结果还是令人满意的，我们用证书实现 L2TP 的身份验证获得了成功！

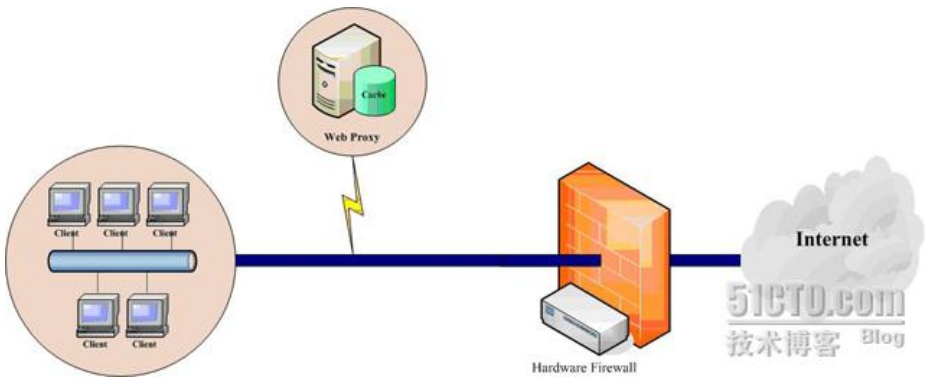


用 L2TP 实现站点间 VPN 并不难，尤其是预共享密钥的实现是很简单的，如果是证书验证，要注意对 CA 的信任，切记，只有从一个被所有机器都认可的 CA 申请证书才是有意义的！

配置单网卡的 ISA 缓存服务器：ISA2006 系列之二十七

ISA 是互联网安全加速器的缩写，安全指的是 ISA 的防火墙功能，而加速则是 ISA 的缓存功能。我们知道，缓存的设计是为了解决两个系统之间速度不匹配的矛盾。一般而言，内网的访问速度要远远大于外网，因此，如果 ISA 能够把用户访问外网获得的数据放在硬盘缓存中，那么当下一个用户从外网请求相同数据时，ISA 就可以利用硬盘缓存的内容对用户进行响应，这样的速度自然要远远大于从外网获得数据，加速器的称呼也就是因为这个。尤其是当公司员工早晨浏览新闻网站或查看产品报价时，这种加速效果非常明显。

有些公司在部署 ISA 服务器之前已经有了自己的网络访问解决方案，例如通过硬件防火墙访问互联网，如果这种网络访问解决方案运行效果较好，公司就未必希望用 ISA 来替代当前的方案，毕竟稳定是第一位的。但在这种情况下，我们可以在内网部署一个 ISA 服务器，内网用户通过使用 ISA 提供的 Web 代理服务，利用 ISA 的缓存功能对网络访问进行加速，拓扑如下图所示。在这种拓扑中，我们只使用了 ISA 的缓存功能，ISA 并不承担边缘防火墙的任务，因此 ISA 只需要一块网卡即可。下面我们就通过一个实例为大家介绍一下如何部署单网卡的 ISA 缓存服务器。



在部署单网卡缓存服务器之前，我们先要了解以下几点：

确认担任缓存服务器的 ISA SERVER 主机，在现有防火墙的保护网络范围中。

确认在目前的防火墙访问规则配置中，已开放缓存服务器的对外访问协议，这些包含了 HTTP、HTTPS 以及 FTP。

对于单网卡的缓存服务器来说，它将无法使用下列功能：

— 防火墙客户端程序安装

二 VPN 网络的架设

三 IP 数据包筛选

四 多重网络架构的防火墙策略

五 企业内部服务器的发布功能

六 应用程序级的数据包过滤

我们具体的实验环境如下图所示，Beijing 是内网的单网卡 ISA2006 服务器，我们准备把 Beijing 部署成 ISA 缓存服务器，大致需要进行下列操作：

1) 使用模板配置

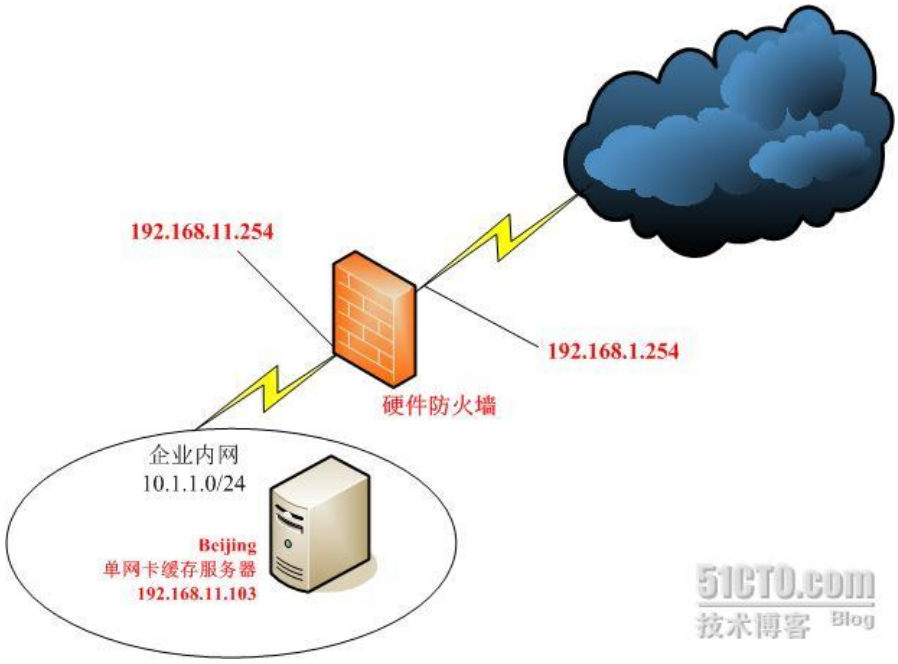
2) 创建访问规则

3) 启用 Web 代理

4) 启用缓存功能

5) 创建缓存规则

6) 创建计划内容下载作业



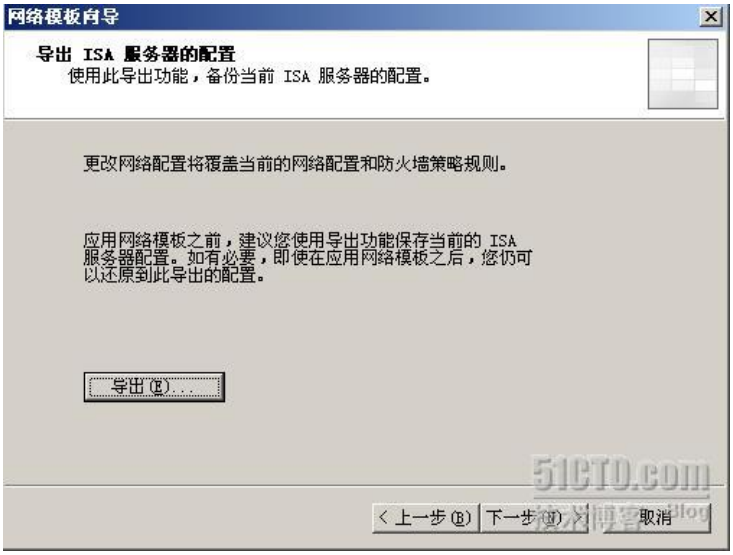
一 使用模板配置

ISA2000 在安装时提供了防火墙，缓存，集成等三种模式供用户选择，虽然 ISA2006 在安装时不能直接选择缓存模式，但 ISA2006 提供了缓存服务器的配置模板，我们可以使用缓存服务器模板把 ISA 服务器配置成单网卡的缓存服务器。

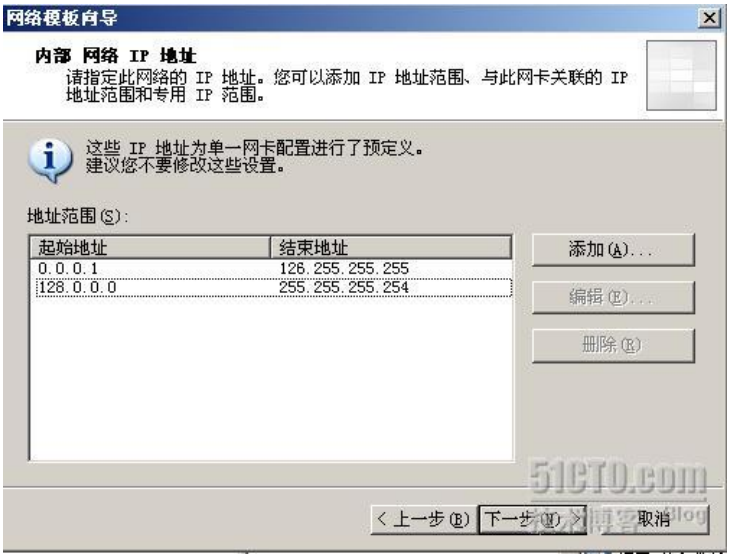
在 Beijing 上打开 ISA 管理器，定位到 配置－网络，如下图所示，在右侧的模板列表中选择“单一网络适配器”模板。

出现网络模板的设置向导，点击下一步继续。

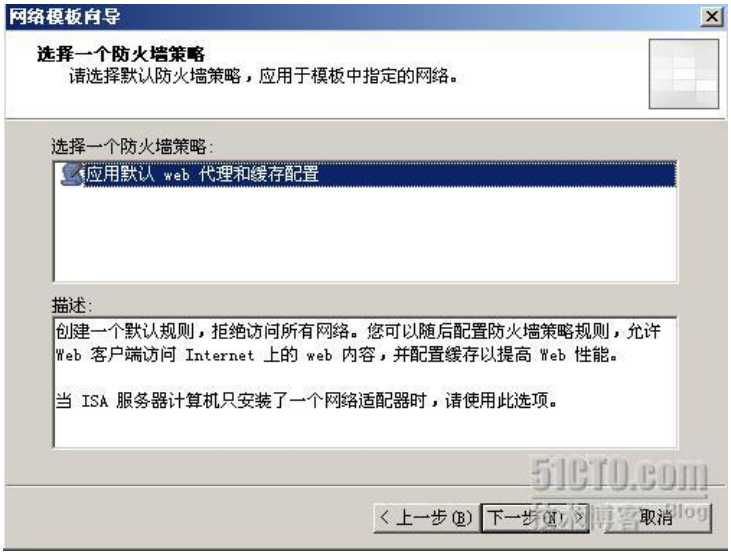
向导提示我们在使用模板之前最好先备份当前的 ISA 配置。



下面要配置单网卡 ISA 的内网地址范围，注意，由于 ISA 只有一块网卡，因此 ISA 的内网应该包括除 127 之外的所有 IP 地址范围。注意，此时 ISA 没有外网的概念了，对单网卡的 ISA 来说，所有的网络地址应该都属于内网范畴。我们在后续创建网络规则时也要注意到这一点。



模板向导提示我们应该选择一个防火墙策略，这个策略拒绝访问所有网络，我们在配置模板结束后可以修改防火墙策略，允许 Web 代理用户访问外网。

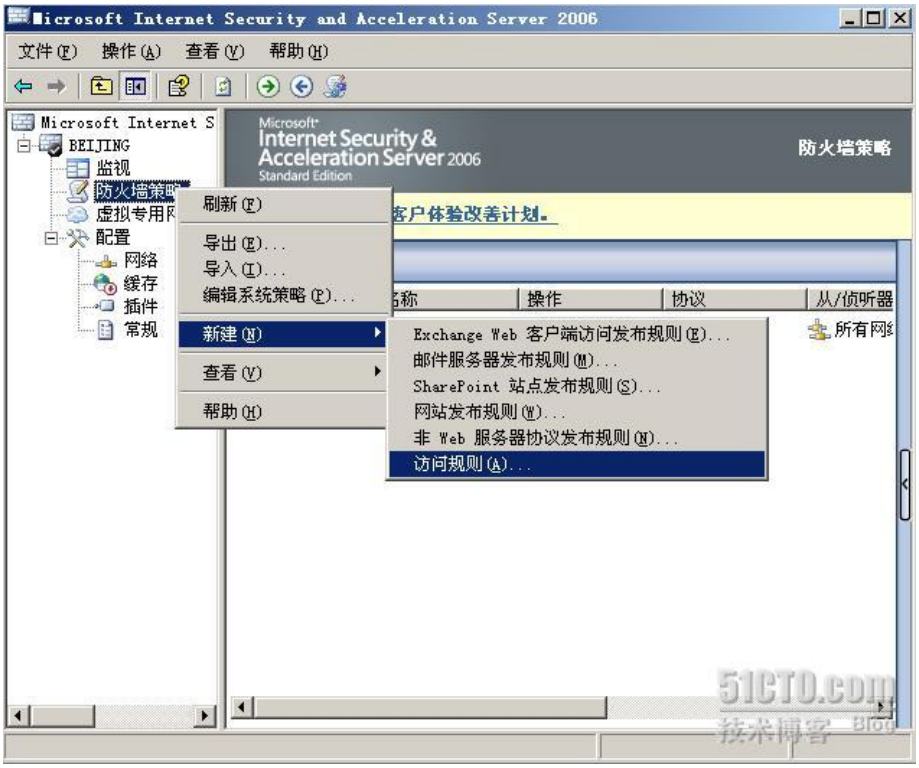


如下图所示，网络模板配置完成。

二 创建访问规则

使用模板配置完 ISA 服务器后，内网的 Web 代理用户并不能通过 ISA 服务器访问互联网，因为 ISA 服务器的访问规则中禁止所有的网络访问请求，因此我们必须创建访问规则允许 Web 代理用户使用 HTTP 协议访问互联网。

在 ISA 管理器中右键点击“防火墙策略”，如下图所示，选择新建“访问规则”。



为访问规则命名为“允许 HTTP 访问”。

当用户的访问请求符合规则时，允许访问请求。

Web 代理用户使用最多的协议就是 HTTP 和 HTTPS，我们允许在规则中使用 HTTP 和 HTTPS 协议。

我们设定访问的源网络是内网。

注意，访问的目标网络仍然是内网，大家可别习惯性地把目标网络设定为外网，注意，内网的范围包括了除 127 之外的所有网络。

访问规则适用于所有用户。

如下图所示，我们完成了访问规则的创建，现在内网用户就可以通过 ISA 访问互联网上的内容了。

三 启用 Web 代理

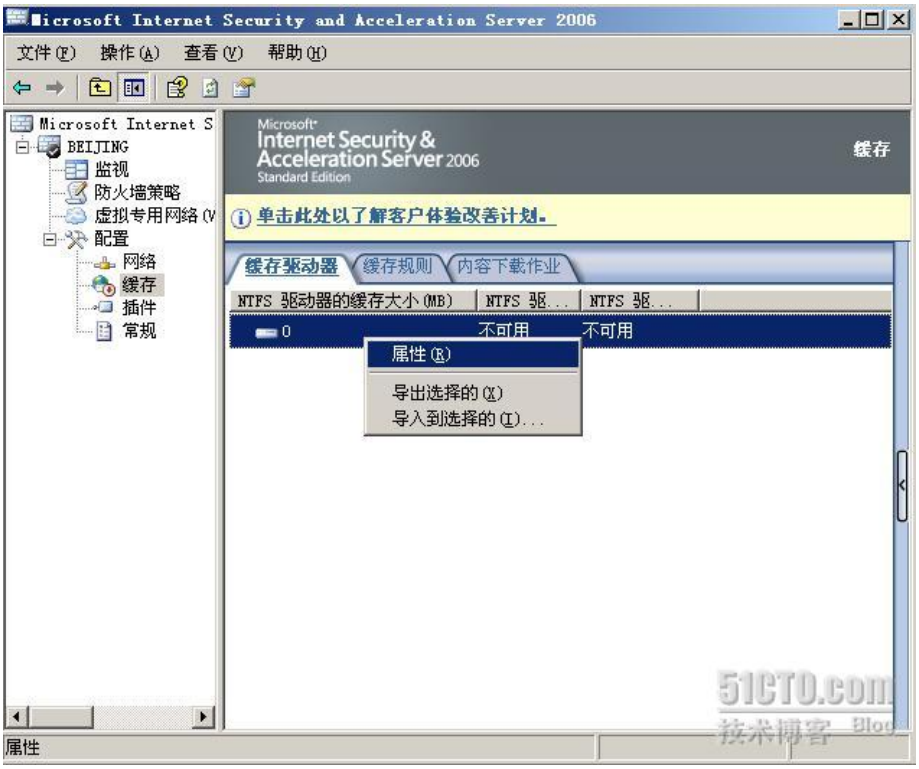
单网卡的 ISA 服务器只能为用户提供 Web 代理服务，因此我们要确保 ISA 启用了 Web 代理功能，如下图所示，在 ISA 管理器中查看内网属性，确保 ISA 服务器在 8080 端口提供 Web 代理服务。

ISA 提供了 Web 代理服务后，要确保内网用户在浏览器中要使用 ISA 提供的 Web 代理服务，在用户的浏览器属性中切换到“连接”标签，如下图所示，点击“局域网设置”。

勾选使用代理服务器，代理服务器的地址设定为 Beijing，端口是 8080。

四 启用缓存功能

虽然我们已经用单一网络适配器模板对 ISA 服务器进行了配置，而且 ISA 服务器也启用了 Web 代理，但由于 ISA 服务器的缓存功能和缓存规则尚未设置，因此 ISA 的缓存功能还未能实现。现在我们就先来启用 ISA 的缓存功能，如下图所示，在 ISA 管理器中定位到配置－缓存，我们可以看到目前缓存驱动器的尺寸是 0，显然当前并没有启用缓存，我们点击“缓存驱动器”的属性，准备对缓存进行设定。

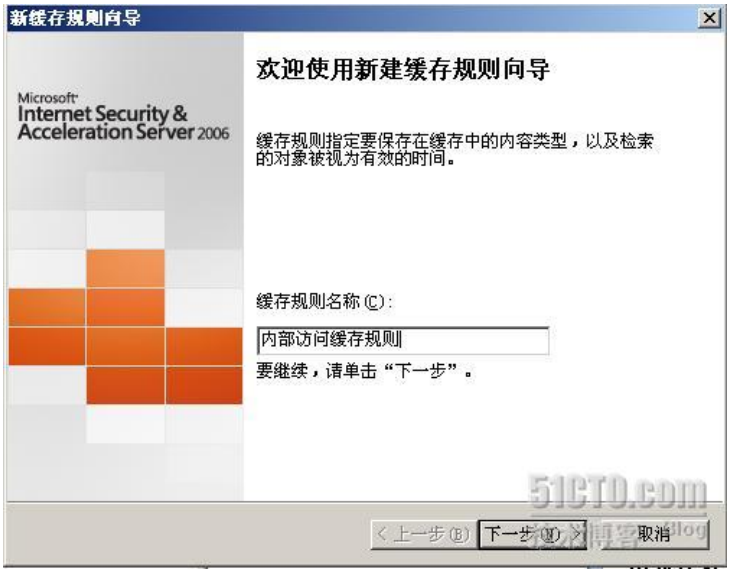


如下图所示，我们把缓存设定在 C 盘，大小定位 200M。缓存尺寸的设定原则是最好不要小于 100M，每增加一个 Web 代理用户就增加 0.5M。设定完缓存尺寸后，不要忘了点击“设置”按钮，而且在设置完成后最好重启一下 ISA 服务器。

五 创建缓存规则

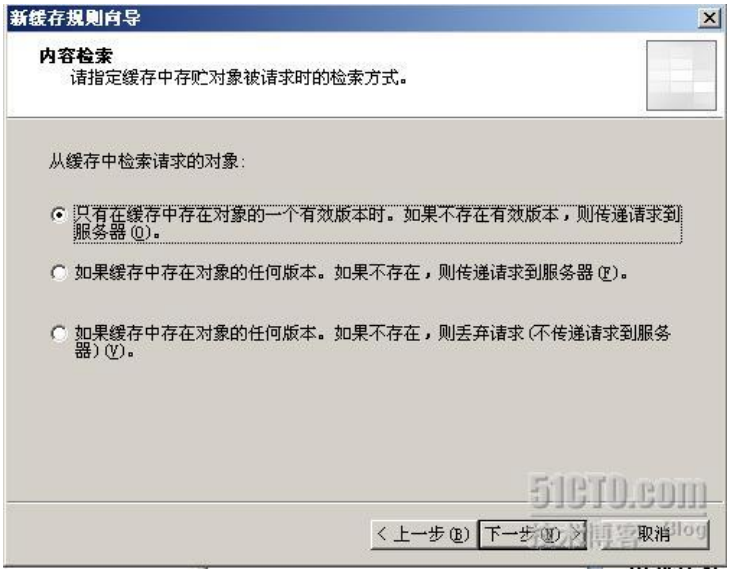
ISA 启用了缓存功能后，我们要制定适合本单位的缓存策略，以便让 ISA 的缓存可以最大限度地发挥作用。如下图所示，在 ISA 管理器中定位到 配置－缓存，在缓存规则的任务中选择“创建缓存规则”。

出现新建缓存规则的向导，点击下一步继续。



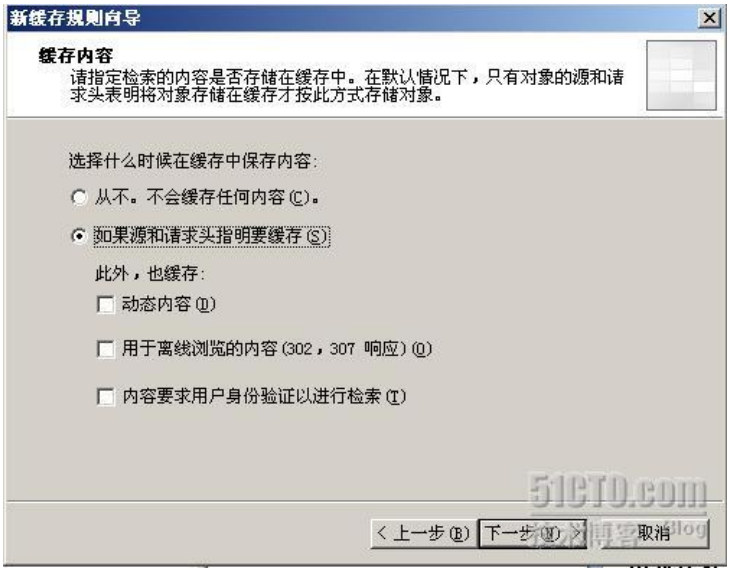
首先要设定缓存规则针对哪些访问目标生效，我们设定规则针对的目标网络是内网，再次提醒，别误写为外网。

接下来我们要设置缓存对象被请求时的检索方式，一般来说，我们大多选择第一项或第二项。第一项是根据 TTL 的到期时间来判断是否存在请求对象的有效版本，第二项则是缓存中只要存在请求对象的任何版本都可以。



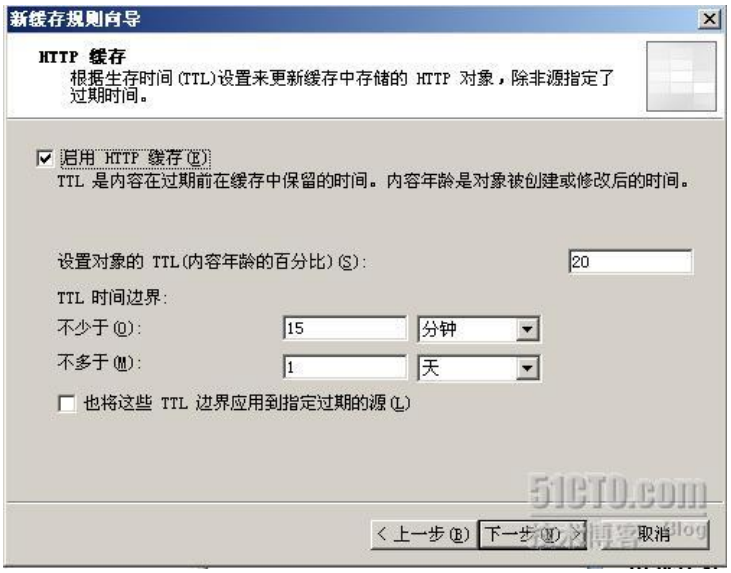
接下来我们设置缓存的内容类型，如果有需要，可以考虑缓存动态内容或离线浏览内容，以便第一时间响应用户的请求。

插入图片



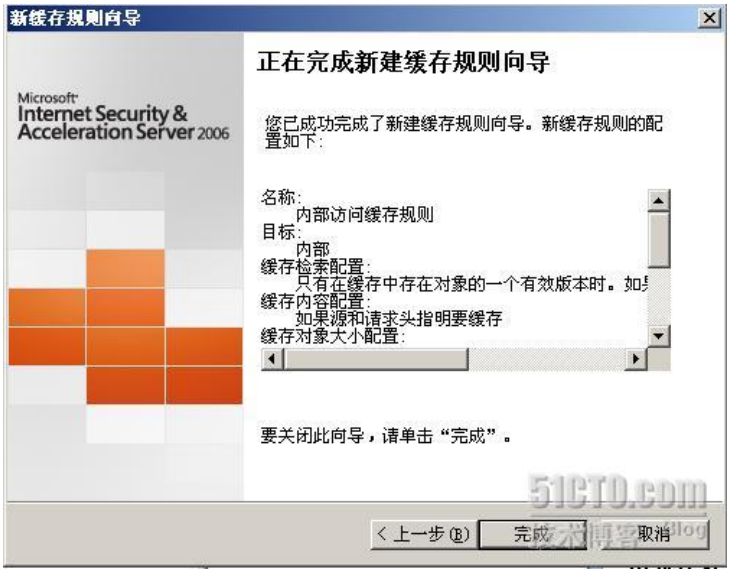
我们对缓存对象的大小也可以进行设置，这样可以避免缓存到太大的数据，例如我们可以规定不缓存 5M 以上的对象。

缓存对象的生存时间可以使用默认设置，也可以根据需求将生存时间延长或缩短，如果请求的 HTTP 数据源制定了生存时间，则以数据源的规定为准。否则将按照 ISA 定义的时间边界定义缓存对象的生存时间。



FTP 缓存的默认生存时间是 1 天。

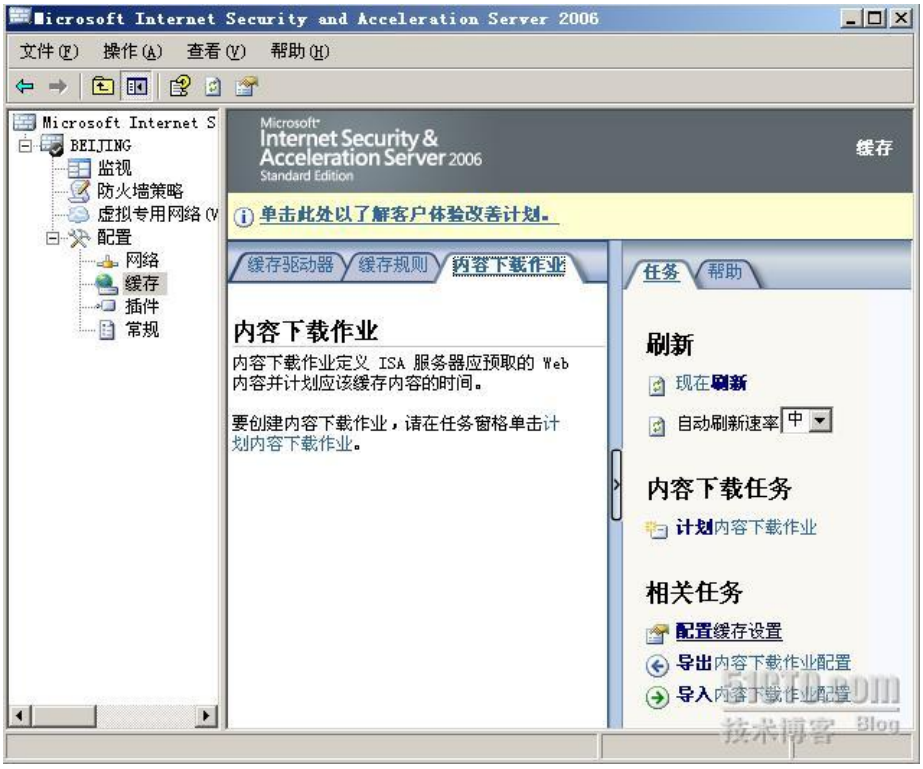
点击完成结束缓存规则的配置，以后 ISA 就会按照我们设定的规则来缓存数据了。



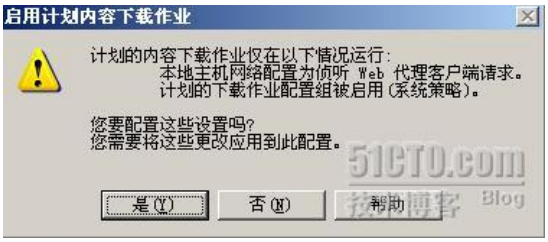
六 创建计划内容下载作业

对于一些用户经常访问的网站，我们还可以采用主动缓存的方式，在用户提出访问请求之前就把数据缓存到 ISA 服务器上，这样一来用户会获得更好的速度体验。例如如果每天 9 点上班的用户都有浏览新浪新闻的习惯，我们就可以让 ISA 在每天的 8:30 先去新浪把新闻缓存到硬盘上，这样用户浏览起来自然对速度非常满意。下面我们来看如何实现这个设想，

在 ISA 管理器中定位到 配置－缓存，如下图所示，在“内容下载作业”的任务中选择“计划内容下载作业”。



ISA 提示我们如果要进行计划内容下载作业，必须满足两个条件，一是在内网要启用 Web 代理，这项要求我们已经满足了；另一个条件是要求在系统策略中启用计划的下载作业配置组，只要我们选择“是”，就可以在系统策略中启用这个设置。



查看系统策略编辑器，如下图所示，计划下载确实已经被启用了。

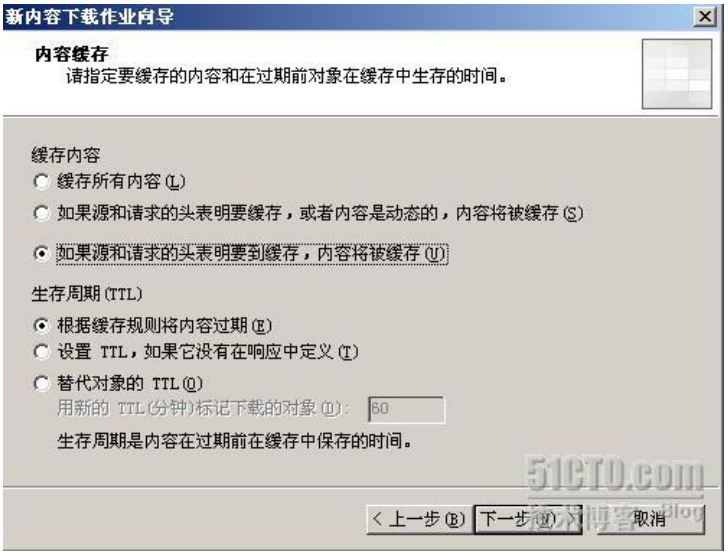
满足了计划下载所需要的两个条件后，再次从内容下载作业中选择“计划内容下载作业”，这次出现了内容下载作业向导，如下图所示，我们为内容下载作业命名为“新浪新闻”，点击下一步继续。

选择作业运行的频率，我们选择每天运行一次。

作业的开始时间我们设定为每天的 8:30。

作业下载的具体地址是 http://news.sina.com.cn，我们设定每页的最大链接深度仅为 1，避免下载的数据量过大。而且设定不从指定的 URL 之外的链接下载。

设定要缓存的内容以及生存周期，我们取默认设置即可。



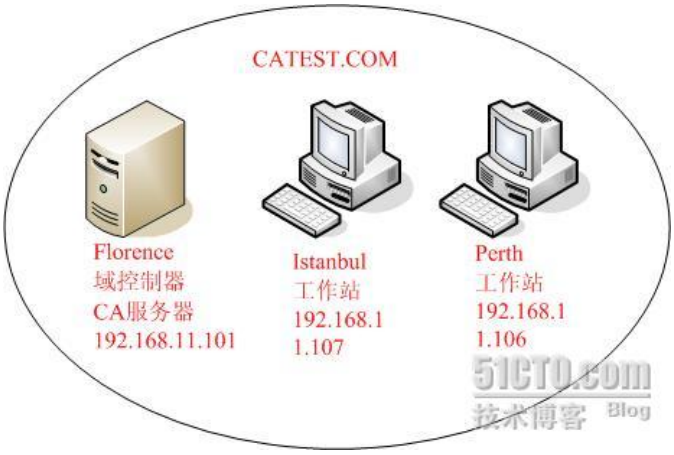
如下图所示，我们配置完成了每天定时下载新浪新闻的计划任务。

ISA 的缓存功能是非常实用的，对提高网络响应速度很有好处，而且 ISA2006 中又增加了对 Bits 数据类型的支持，即使用户用 Bits 从微软网站下载补丁，也可以享受到缓存服务带来的加速体验。如果您已经有了硬件防火墙作为边缘网关，不妨试试用 ISA 作缓存服务器，体验一下两种防火墙和谐相处为您带来的稳定，安全以及高速的网络感受。

用组策略实现用户证书的自动注册申请：ISA2006 系列之二十八

在前面的博文中，我们已经在邮件加密，安全 Web 站点，TLS 通讯，智能卡等诸多的应用领域中接触到了证书，证书在安全领域的重要性已是不言而喻。如果我们在内网搭建了 CA 服务器，用户应该如何获取证书呢？用户申请证书一般有两种方式，如下图所示，用户既可以通过 MMC 控制台也可以利用浏览器进行证书的注册申请。但这两种证书申请方式对普通用户来说都有一定的技术难度，如果管理员代为用户申请证书，在用户众多的环境下又不太现实。那我们在大型企业中应该如何处理用户证书的注册申请呢？

我们可以通过组策略结合 CA 服务器来完成证书的自动注册申请，利用这种方式，我们可以对整个域的用户或某个组织的用户，只要用户在开机后以域用户身份登录，就可以自动完成证书的注册申请。怎么样，听起来是否很不错？下面我们通过一个实验来说明如何实现这个构想，拓扑如下图所示，Florence 是域控制器和 CA 服务器，Perth 和 Istanbul 是用户 User1 和 User2 使用的工作站。



一 创建企业根 CA

要实现用户证书的自动注册，需要有企业级 CA 的支持，因为只有这种类型的 CA 服务器才能和组策略结合使用。由于我们创建的 CA 服务器是域中的第一个证书服务器，因此服务器类型应该选择企业根。

在域控制器 Florence 上打开控制面板－添加或删除程序－添加/或删除 Windows 组件，如下图所示，勾选“证书服务”。

证书服务器的类型应该选择“企业根 CA”。

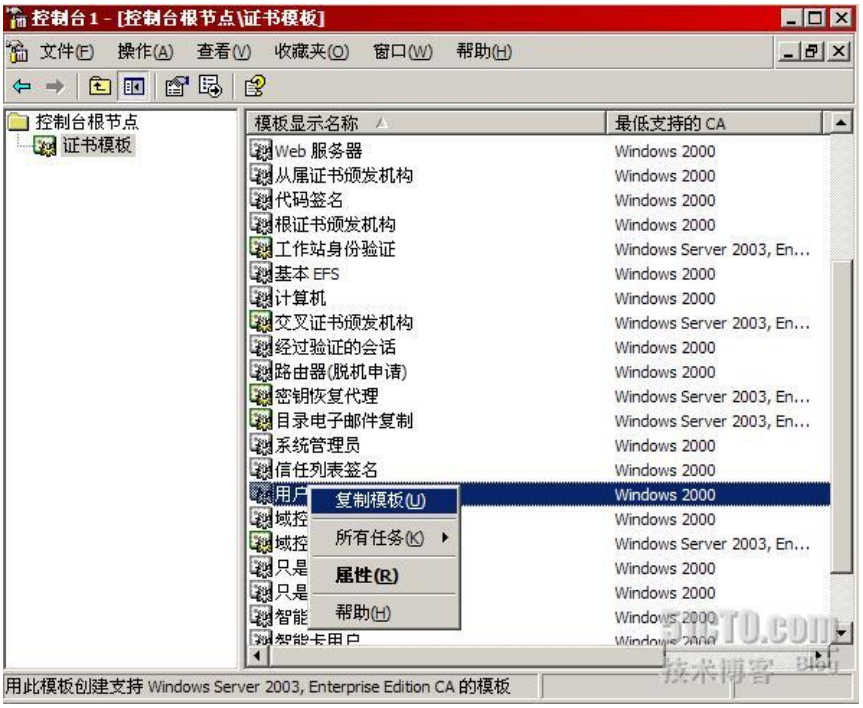
为 CA 命名为 ITETCA，有效期限 5 年。

证书数据库的存储路径取默认值即可。

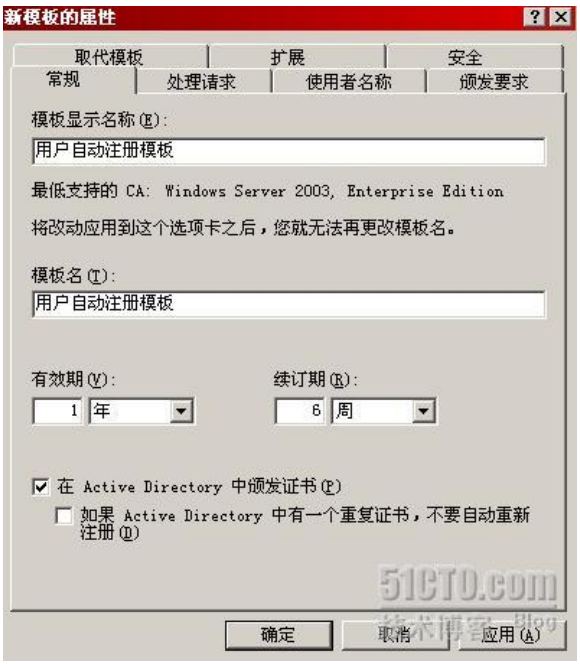
如下图所示，我们成功地完成了企业根 CA 的安装，结束了实验的第一步。

二 创建证书模板

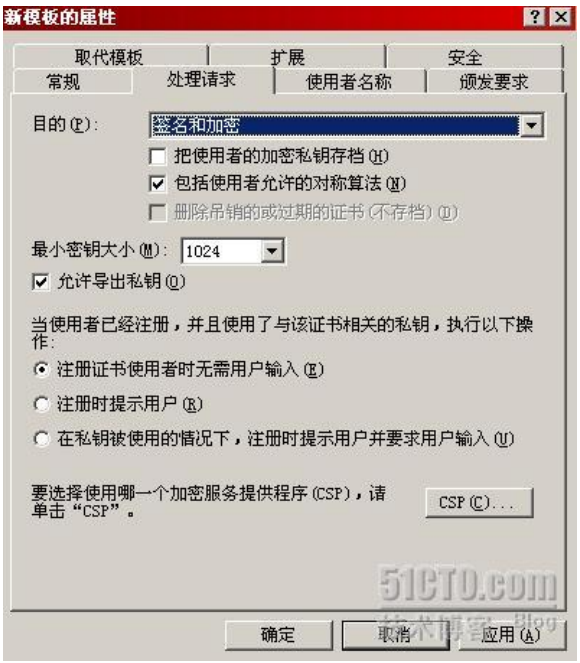
有了 CA 服务器，我们接下来要创建一个支持用户自动注册的证书模板。具体步骤如下，我们在 Florence 上运行 MMC，添加“证书模板”管理单元。如下图所示，右键点击“用户”模板，选择“复制模板”。之所以选择复制出一个新模板，而不是直接在用户模板上进行操作，是因为不希望影响其他应用程序对用户模板的使用。



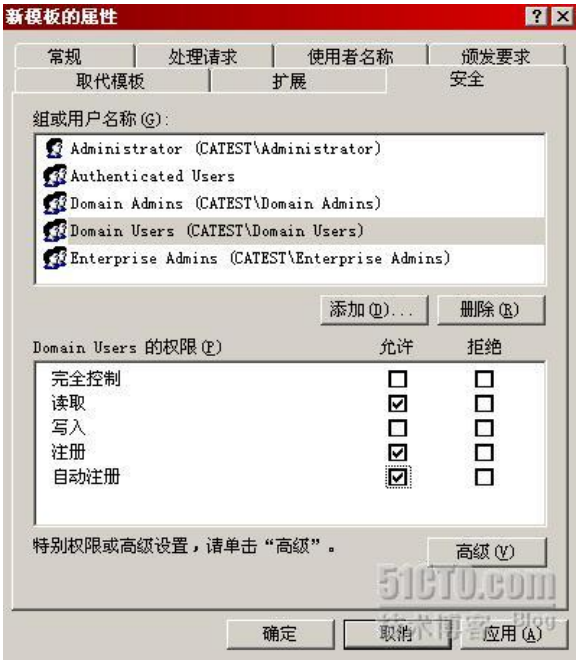
如下图所示，在复制出的新模板的常规标签处，我们为此模板命名为“用户自动注册模板”，注意，模板名称一旦确定就无法更改。同时确保勾选“在 Active Directory 中颁发证书”。



切换到证书模板的“处理请求”标签，如下图所示，确保选择“注册证书使用者时无需用户输入”。

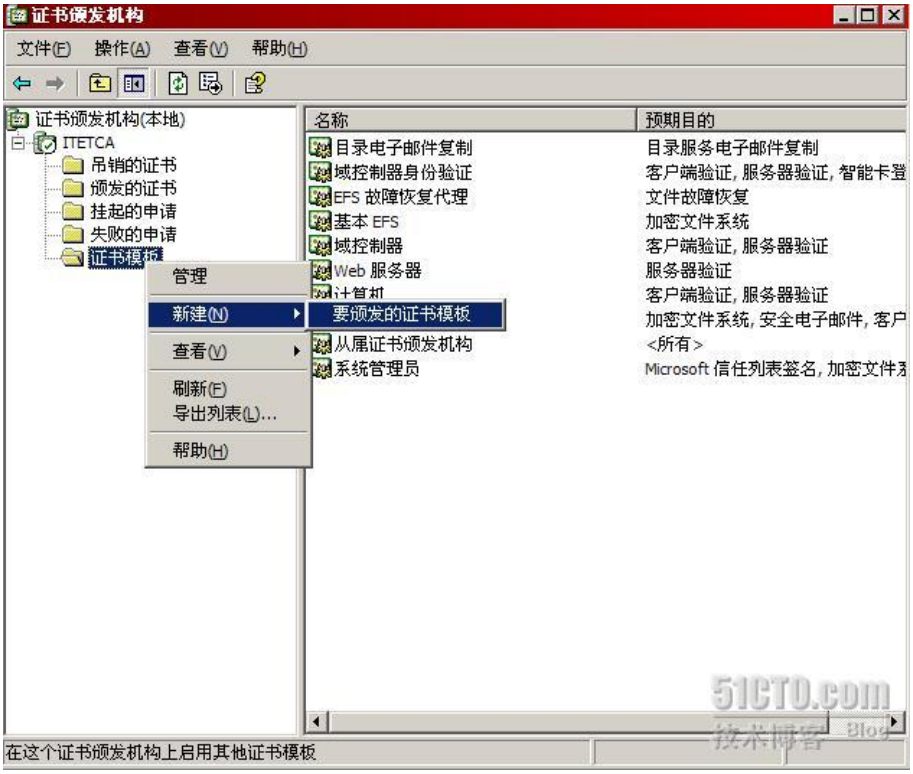


切换到证书模板的“安全”标签，我们在此可以分配证书模板的权限，如果我们希望哪些用户可以利用这个证书模板进行证书的自动注册，一定要为这些用户赋予“读取”，“注册”和“自动注册”的权限。在本次实验中，我们希望域内所有的用户都可以实现证书的自动注册，因此如下图所示，我们为 Domain Users 组的成员赋予了上述三项权限。

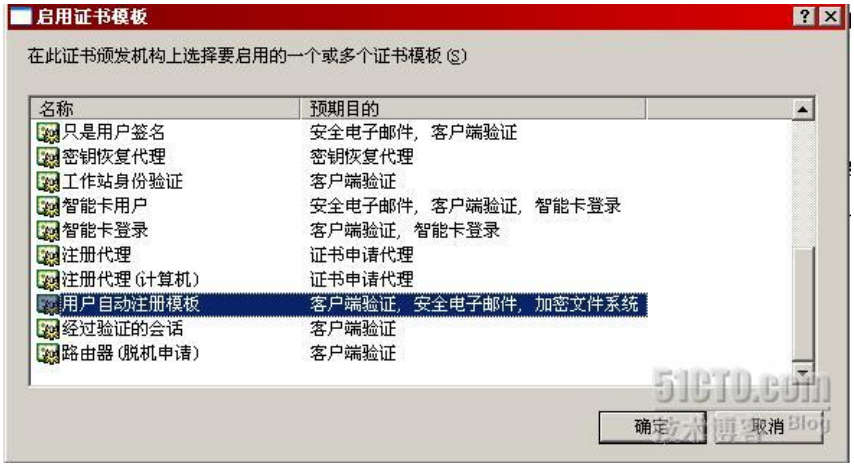


三 使用自动注册的证书模板

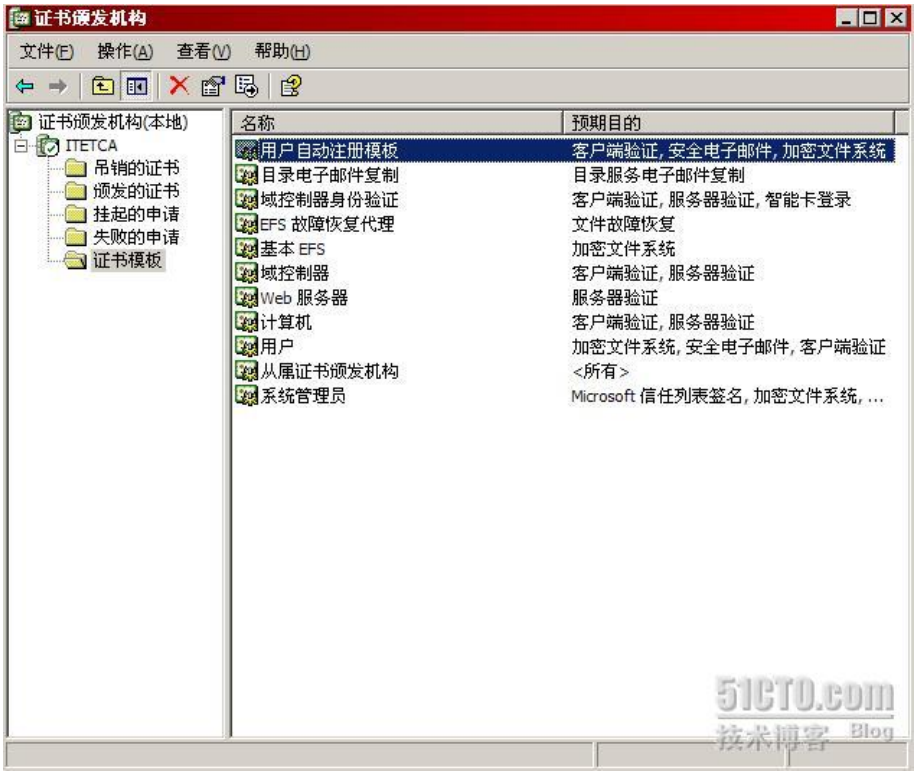
创建了支持自动注册的证书模板，我们就要在证书服务器中使用这种证书模板。在 Florence 的管理工具中打开“证书颁发机构”，如下图所示，右键点击证书模板，选择新建“要颁发的证书模板”。



选择我们新创建的“用户自动注册模板”。

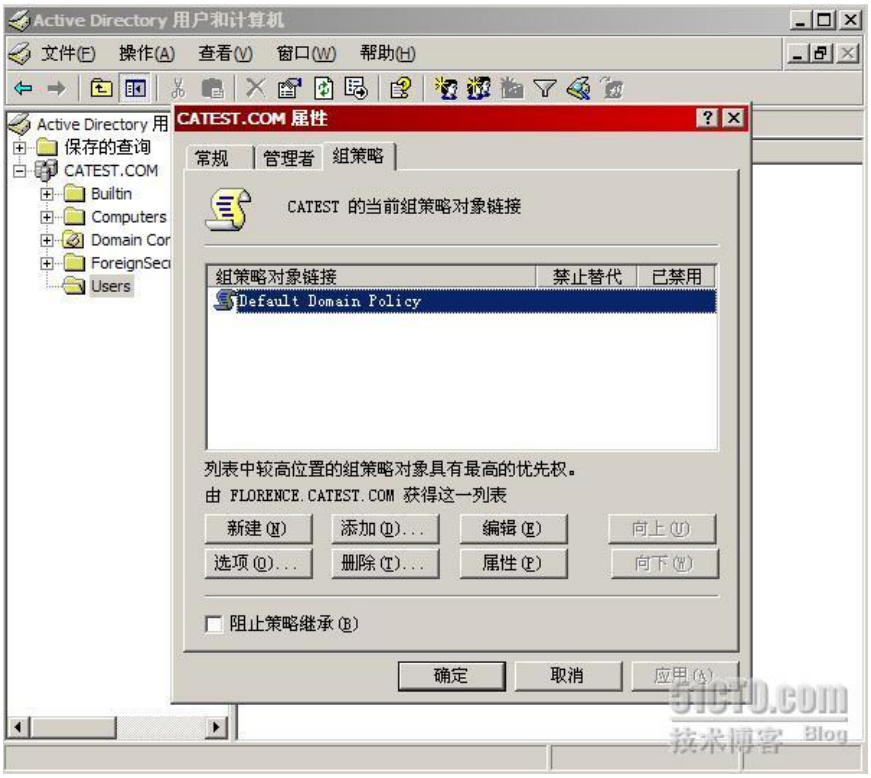


如下图所示，现在证书服务器已经使用了支持用户自动注册的证书模板，证书服务器已经可以支持用户自动进行证书的注册申请了。

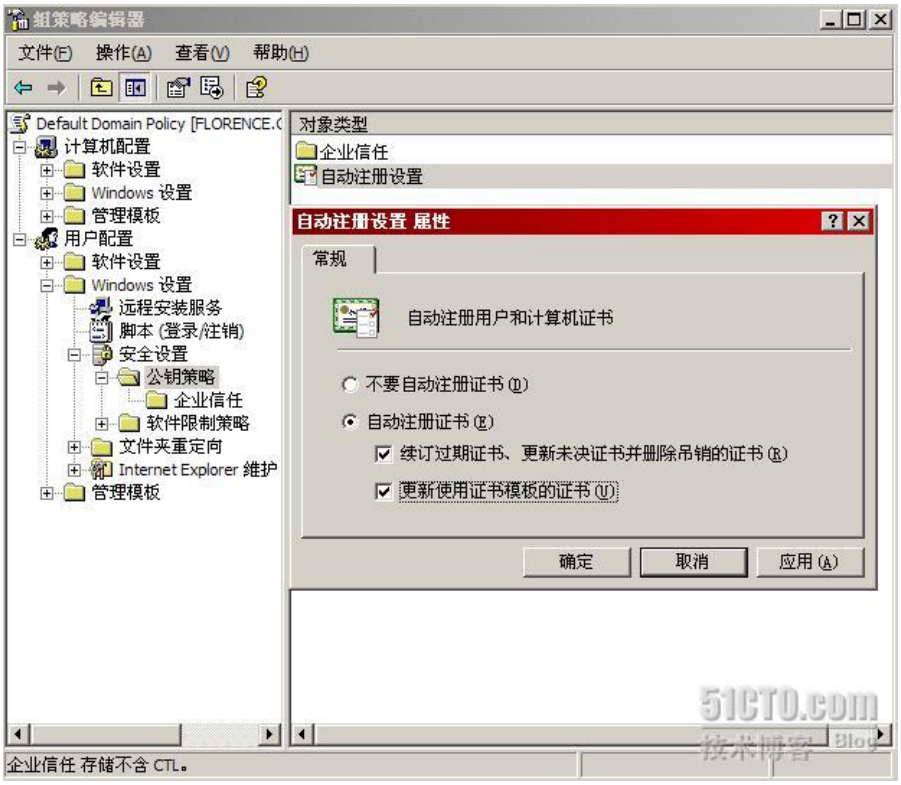


四 配置组策略

证书服务器已经可以支持用户证书的自动注册申请，接下来我们需要在组策略中进行配置，允许用户自动进行证书的注册申请。由于我们希望域内所有用户都能实现证书的自动注册，因此我们需要在域级别进行组策略设置。在 Florence 上打开 Active Directory 用户和计算机，如下图所示，在 CATEST.COM 域的属性中切换到“组策略”标签，由于我们只是进行实验，因此选择编辑默认的域用户策略即可。



如下图所示，在组策略编辑器中定位到 用户配置－Windows 设置－安全设置－公钥策略，编辑右侧面板中的“自动注册设置”。确保选择“自动注册证书”，如有必要，也可选择“续订过期证书，更新未决证书并删除吊销的证书”和“更新使用证书模板的证书”。这样一来，用户不但可以完成证书的自动注册申请，还可以完成证书的自动更新，续订以及吊销。

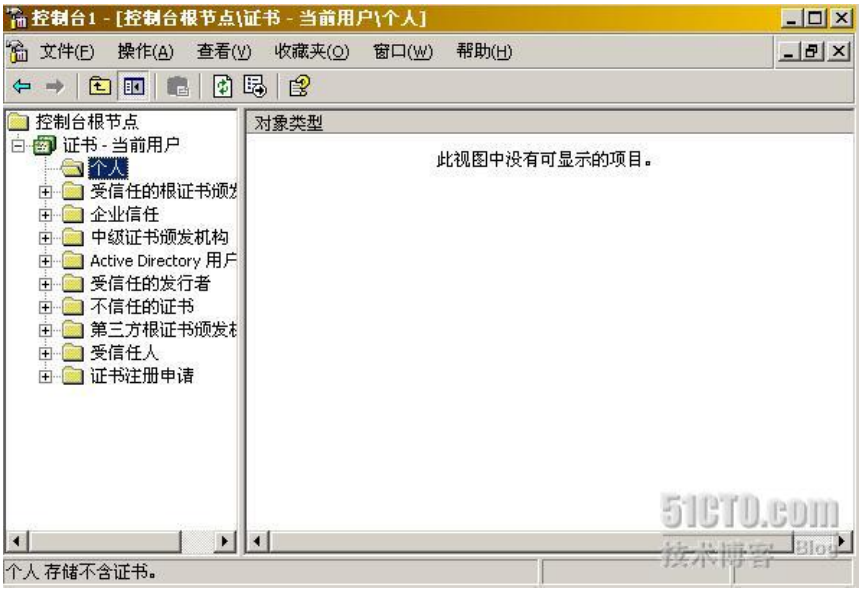


组策略设置完毕后，我们可以在工作站上使用 Gpupdate / Force 来加速组策略的生效。

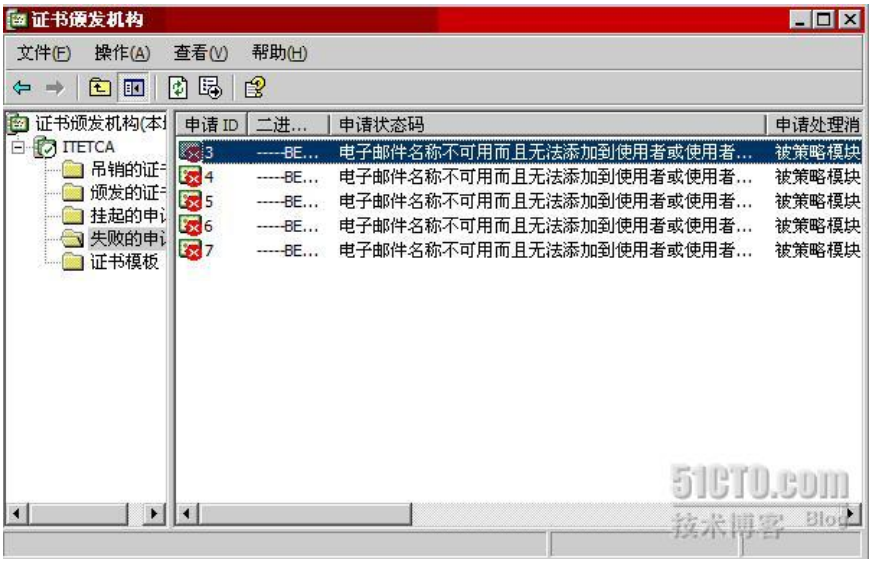
五 用户测试

万事俱备，只欠东风，下面我们就在 Perth 上进行证书的自动注册测试，如下图所示，域用户 User1 在工作站 Perth 上登录。

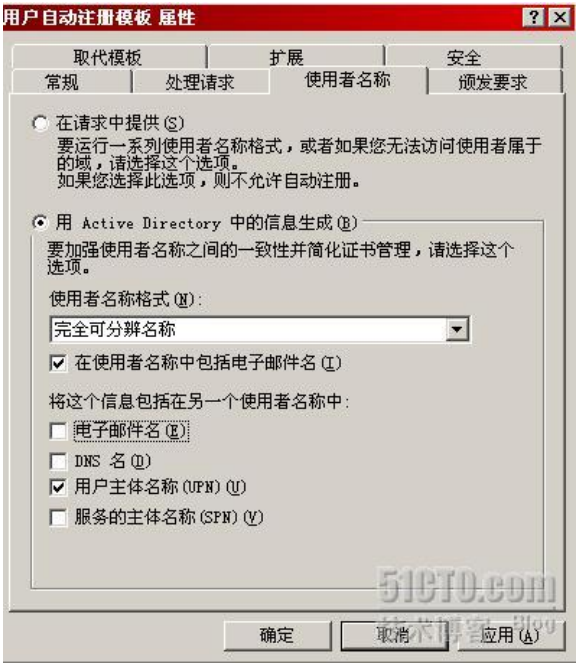
User1 登录后我满怀信心地用 MMC 打开用户证书的管理单元查看成果，咦，怎么回事？如下图所示，User1 没有申请到证书！重新启动 Perth，让 User1 重新登录也无济于事。利用别的用户申请也是无功而返，问题出在哪里呢？



打开 Florence 上的证书颁发机构，如下图所示，在失败的申请中我们发现了问题所在，证书模板要求用户属性中提供电子邮件地址，但我们没有为用户填写电子邮件地址，域内也没有部署 Exchange 服务器，因此用户提供的属性不能满足证书模板的注册需求，这才导致申请被拒绝。



打开用户自动注册证书模板查看，如下图所示，果然证书模板要求用户注册证书时提供电子邮件地址。



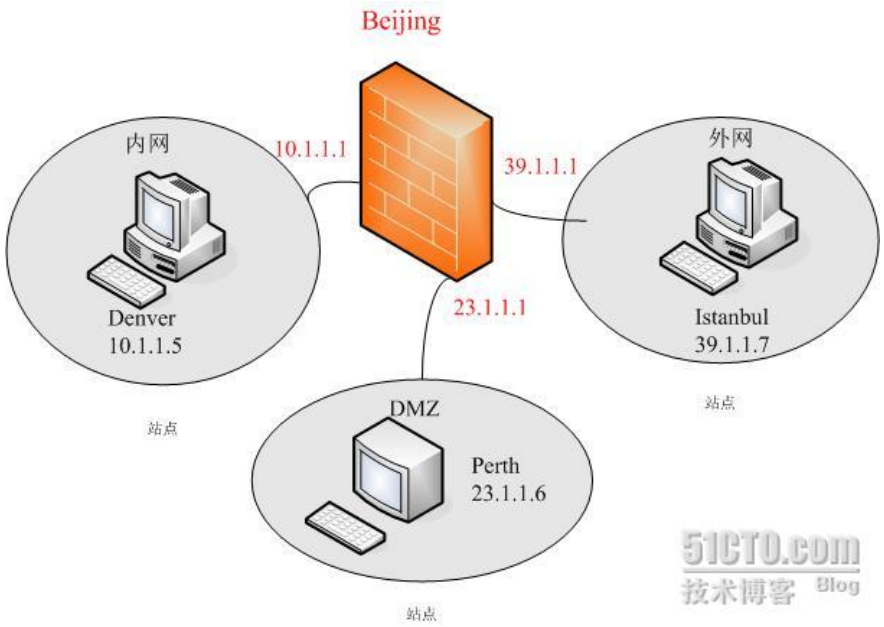
找到了问题的原因，接下来就容易处理了，我们既可以取消证书模板对邮件地址的要求，也可以如下图所示，在 User1 的属性中填写电子邮件地址。

我们填写了 User1 的邮件地址后，让 User1 再次在 Perth 上注销登录，哈哈，如下图所示，这次终于成功了，User1 完成了用户证书的自动注册申请。

详解 DMZ 的部署与配置：ISA2006 系列之二十九

DMZ 是 Demilitarized Zone 的缩写，俗称非军事化隔离区。DMZ 是一个位于内网和外网之间的特殊区域，一般用于放置公司对外开放的服务器，例如 Web 服务器，Ftp 服务器，邮件服务器等。其实从 ISA 的角度来看，DMZ 就是一个网络。有些朋友可能会有些疑问，为什么不把这些服务器直接放到内网呢？为什么需要 DMZ 这个单独的网络呢？被发布的服务器放在内网是可以的，我们在前面的博文中已经讨论了技术上的可能性。但把发布服务器放在内网并非最佳选择，因为内网中还有其他的计算机，这些计算机和发布服务器的安全设置并不相同。例如内网中的域控制器并不适合开放给外网用户，财务室人员使用的工作站更是要严加防护。但如果这些计算机和发布服务器都放在内网，对我们进行访问控制是不利的。一旦发布服务器出现安全问题，有可能会危及内网其他计算机的安全。因此比较安全的解决方法是把发布的服务器放在一个单独的隔离网络中，管理员针对隔离网络进行有别于内网的安全配置，这样一来的话显然对安全更加有利。

下面我们用一个实例来为大家介绍一下如何利用 ISA2006 部署和配置 DMZ，拓扑如下图所示，Beijing 是 ISA2006 服务器，Beijing 有三块网卡，分别连接内网，外网和 DMZ，DMZ 在 ISA 中也被称为外围。Denver 在内网，Perth 是 DMZ，Istanbul 在外网。



一 创建 DMZ

Beijing 是一个有三块网卡的 ISA 服务器，我们准备在 Beijing 上手工创建 DMZ 网络，网络范围是 23.1.1.0－23.1.1.255。这个工作我们也可以通过 ISA2006 自带的三向外围防火墙模板来进行，但这个模板和国内公司的网络环境不太匹配，因为国外公司的 DMZ 使用的往往是公网地址，而国内 DMZ 使用的大多是私网地址，这种环境上的差异会导致网络规则和防火墙策略配置上的差别，因此这个模板不太适合国内大多数公司使用，我们还是来手工创建并配置一个 DMZ 网络。

顺便介绍一个 ISA 中网络的一些基本原则，供大家创建网络时参考：

1、 ISA 防火墙上的每个网络适配器可以有单个或者多个 IP 地址，但是每个 IP 地址只能与一个网络适配器所关联（NLB 的虚拟 IP 地址不在此讨论范围内）。

2、 一个地址只能属于一个网络；ISA 防火墙上任何一个网络适配器都必须并且只能属于一个网络，并且这个网络适配器上的所有地址都必须属于相同的网络；一个网络可以包含一个或者多个网络适配器。

3、 在网络定义的 地址范围中，应包含 ISA 防火墙对应网络适配器接口的 IP 地址。ISA 将没有关联适配器的网络视为暂时断开连接，也就是说，ISA 服务器假定存在与该网络关联的适配器，但该适配器当前被禁用。当 ISA 服务器假定适配器断开连接时，ISA 服务器将拒绝去往或来自属于断开的网络的 IP 地 址的通讯， 因为这些数据并没有通过和此网络相关联的网络适配器来进行转发，并认为这些数据包欺骗所有已启用的适配器。

4、 对于除外部网络之外的其他网络的网络适配器后还有其他子网的情况（即可以通过此网络适配器所关联的网络中的某台路由器到达的其他的网络，称之为网络后面的网络），你必须在 ISA 防火墙对应的网络的定义中，包含这些子网的地址，否则 ISA 防火墙会触发 IP 欺骗或者配置错误的警告。这是因为没有在此网络中定义的 IP 地 址范围，不属于此网络，但是却又必须从此网络相关联的网络适配器进行数据的转发，ISA 防火墙认为这是一种欺骗行为。

5、 通常情况下， 对于一个完整的网络定义，地址范围应该从网络地址起，到子网广播地址为止。例如一个 C 类网络 192.168.0.0/24，那么完整的网络地址范围为 192.168.0.0～192.168.0.255。对于网络地址是从 A 类网络地址、B 类网络地址中划分的子网的情况，在网络地址范围中还需要包含对应 的 A 类网络、B 类网络的广播地址，例如一个 A 类子网 10.1.1.0/24，那么内部网络地址中除了 10.1.1.0～10.1.1.255 外，还需要包 括 A 类网络的广播地址 10.255.255.255～10.255.255.255。建议你总是通过添加适配器来添加内部网络地址。非完整的网络定义不需要遵循此要求。

不过，对于没有关联网络适配器的网络被视为暂时断开连接这一假设存在例外，在这些例外情况中，ISA 服务器将该网络视为网络后面的网络，这些例外包括下列网络：

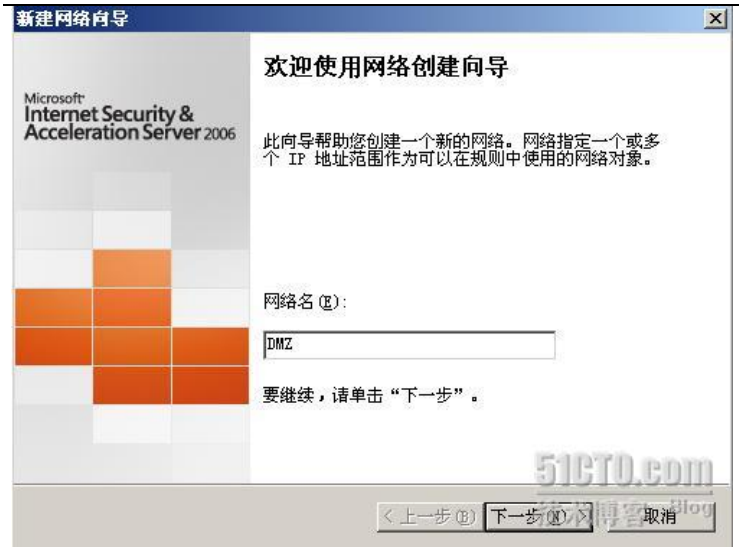
默认的外部网络。ISA 防火墙总是认为默认的外部网络位 于与默认路由所关联的网络适配器（配置了默认网关的网络适配器）所关联的网络的后面，去往或来自外部网络中的地址的通讯必须通过该适配器。来自外部网络中 的地址但是通过其他适配器的任何通讯都将被视为具有欺骗性，并将被丢弃。如果路由表中不存在默认网关项目，ISA 防火墙将认为外部网络暂时断开连接。

配置为使用 IPSec 隧道模式的站点到站点 VPN 网络。

被隔离的 VPN 客户端网络，该网络从不与任何适配器关联，并总是位于与 VPN 拨入适配器关联的 VPN 客户端网络的后面

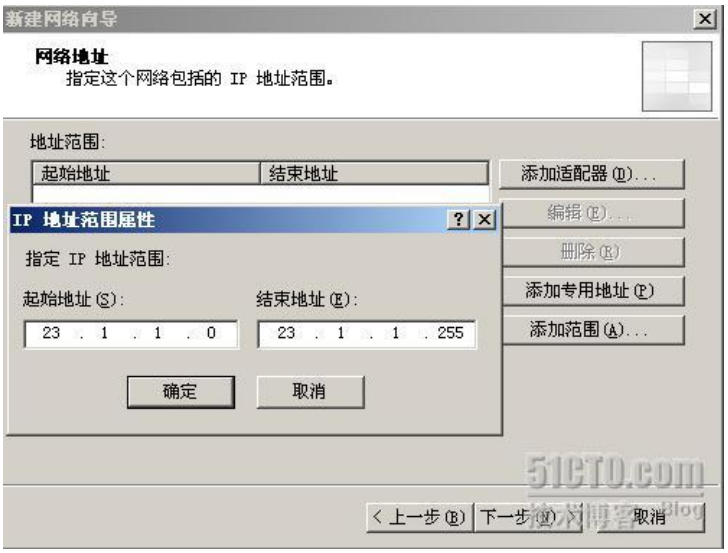
现在我们开始创建 DMZ，在 Beijing 上打开 ISA 管理器，如下图所示，选择新建网络。

为新创建的网络命名为 DMZ。

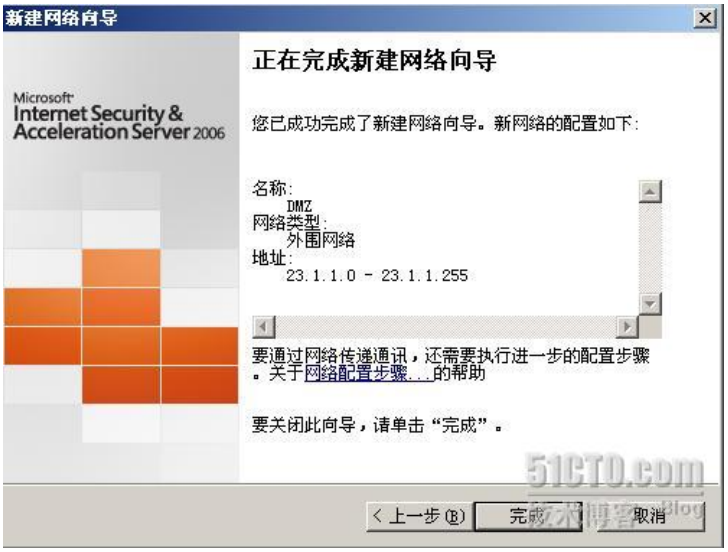


网络类型是外围网络。

DMZ 的地址范围是 23.1.1.0－23.1.1.255，注意，这个地址范围如果之前属于内网，那我们需要把它从内网范围中删除。根据我们刚才提到的网络原则，一个地址只能属于一个网络。



如下图所示，我们成功地完成了 DMZ 网络的创建，是不是很轻松啊。



二 创建网络规则

DMZ 网络创建完毕后，我们需要创建 DMZ 网络和其他网络之间的网络规则。因为我们知道，ISA 处理数据的访问请求，首先考虑的是这个数据包的源网络和目标网络的网络规则，因此网络规则决定了两个网络之间数据通讯的方向性和可能性。网络规则的设定取决于实际的访问需求，在本次实验中，DMZ 的 Perth 拥有网站和 Ftp 服务器。我们希望内网用户和外网用户都可以访问 DMZ 的资源，同时 DMZ 的服务器需要对外网进行访问。基于这

个需求，我们可以把网络规则设定为从内网到 DMZ 是 NAT，从 DMZ 到外网是 NAT。为什么 DMZ 到外网不设定为路由呢？因为 DMZ 使用的是内网地址，外网用户无法直接访问这些 IP 地址。

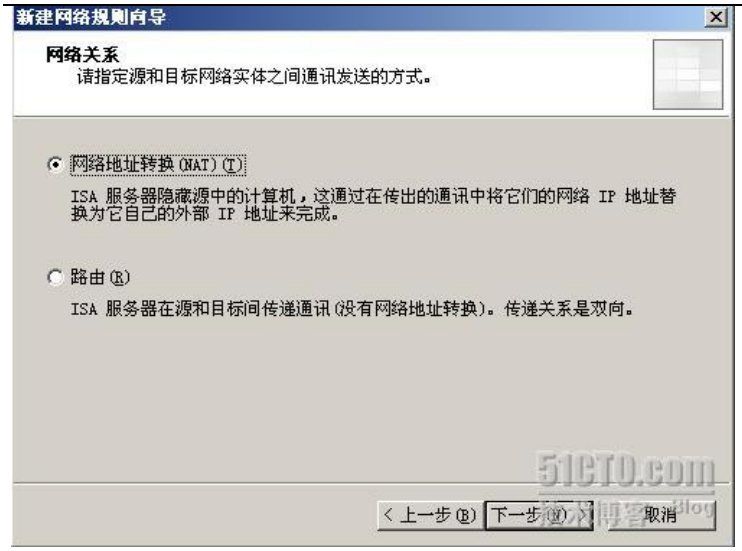
在 Beijing 上打开 ISA 管理器，如下图所示，选择“创建网络规则”。

为网络规则命名为“从内网到 DMZ”。

源网络是内网。

目标网络是 DMZ。

源网络到目标网络的网络关系设定为 NAT。



这样我们就设定了从内网到 DMZ 的网络关系是 NAT，用同样的方法，我们设定从 DMZ 到外网的网络关系是 NAT。

三 创建防火墙访问规则

在我们的实验环境中，我们希望内网能够访问 DMZ，由于内网和 DMZ 的网络关系是 NAT，因此我们应该通过访问规则来完成这个任务。有的朋友可能会想，究竟什么情况下应该使用访问规则，而什么环境下更适用发布规则呢？我们给出使用访问规则的原则：

对于访问规则：

只适用于网络之间具有路由网络关系或正向 NAT 关系（源网络到目的网络为 NAT）的网络间的访问；

一个访问规则可以允许到多个服务器的访问；

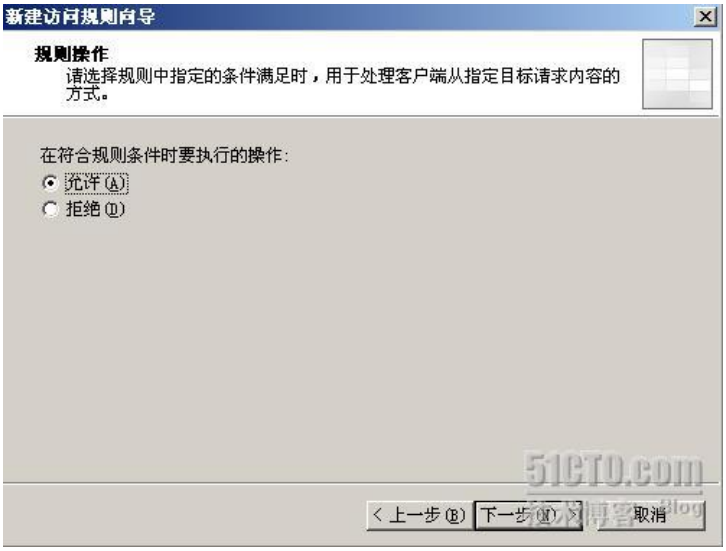
在访问规则中只应使用出站协议定义客户所访问的服务；

用户只能访问协议中所定义的端口

下面我们来具体创建访问规则，在 Beijing 上打开 ISA 管理器，如下图所示，选择新建“访问规则”。

我们在访问规则命名为“允许为内网访问 DMZ”。

当访问请求符合规则时允许访问请求的操作。



允许所有的出站通讯协议。

访问请求的源网络是内网。

访问请求的目标网络是 DMZ。

允许所有用户的访问请求。

如下图所示，顺利完成访问规则的创建。

测试一下访问规则的成果，在内网的 Denver 上访问 DMZ 的 Perth，如下图所示，访问正常。

四 创建发布规则

我们在本次实验中还希望 DMZ 的服务器能够发布到外网，在这种情况下我们应该使用发布规则来完成任务。同样我们会给出使用发布规则的原则：

对于服务发布规则：

适用于源网络和目的网络之间具有路由网络关系或者 NAT 网络关系的网络间的访问。只是根据网络关系的不同，服务发布规则侦听的 IP 地址不同。在目的网络到源网络具有 NAT 网络关系的情况下，服务发布规则侦听的 IP 地址是 ISA 防火墙上连接源网络的网络接口的 IP 地址；而在源网络和目的网络之间具有路由网络关系或者 NAT 网络关系的的情况下，服务发布规则侦听的 IP 地址是被发布的服务器的 IP 地址；

一个发布规则只能允许到一个服务器的访问；

服务发布规则中只能使用入站协议定义所发布的服务；

通过服务发布规则，你可以通过修改服务发布规则的属性轻松的实现端口转换，并且许多内建的应用层过滤器或其某些特性只能通过服务发布规则实现，例如 SMTP 过滤器和 Web 代理过滤器的链接转换功能，就只能通过服务发布规则实现；

服务器应配置为 SNAT 客户；如果服务发布规则的到属性中配置为“使请求显示为来自初始客户端”，那么服务器应该配置 ISA 防火墙为其默认网关。

下面我们来创建发布规则，如下图所示，在 ISA 管理器中选择新建“非 Web 服务器协议发布规则”。

我们为发布规则命名为“发布 Perth 上的 FTP 服务器”。

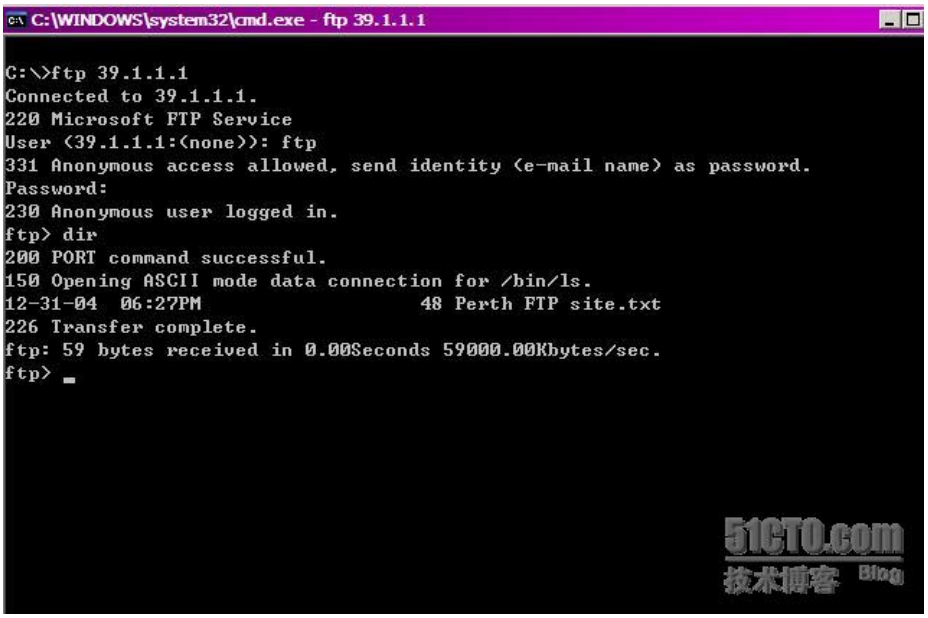
被发布的服务器我们填写 Perth 的 IP 地址 23.1.1.6。

发布协议选择 FTP 服务器。

侦听器监听外网的请求。顺便提一下，以前遇到有朋友想把 DMZ 的服务器发布到内网，但未能成功，他的实验环境和我们完全一样。用发布规则的使用原则分析一下就明白了，内网访问 DMZ 不能通过发布规则而应该使用访问规则。

好，完成发布规则的创建。

在外网的 Istanbul 上测试一下，看能否访问 Perth 的 FTP 服务器。测试结果如下图所示，DMZ 的 FTP 服务器发布成功！



今天我们用一个实例介绍了 DMZ 的部署和配置，DMZ 从 ISA 的角度看，其实只是一个网络。本文的重点在于讨论了一般意义上的网络创建原则，访问规则和发布规则的使用原则。大家如果能够对这些原理融会贯通，一定能够对大家的 ISA 管理大有裨益。