Web 服务器安全设置

Web 服务器安全设置

本专题将介绍如何策划并进行 Web 服务器操作系统和服务的安装，并列出了在 Web 服务器的安装和使用的过程中，所面临的主要的威胁和攻击类型。此外本专题还将详细解释了加固步骤以及如何保护其他的诸如 SMTP 之类的网络服务。

Web 服务器安装重点列表

在这一小节中，列出了 Web 服务器在安装过程中需要特别注意的安全方面的一些要点，例如 Web 服务器的主要服务和非主要服务，以及 Windows IIS 服务器的中需要加固的帐户、文件和目录、共享、端口等处的清单。

- Windows Web 服务器之主要与非主要服务
- Windows IIS 服务器安全加固清单

Web 服务器为什么危险

黑客们拥有的资源和时间甚至比最大的机构都要多，而且他们不受办公室政治、财政预算等常规的组织约束，而专业安全人员常常要面对这些约束。事实上，为了达到目的，黑客们可以组织起令人羡慕的在线合作，分享各种信息。本小节可以帮助你了解黑帽（black hat）组织的工具、策略和动机，这样你就能更好地了解你的网站受到哪些威胁，了解网站赖以运行的系统，以及保护系统的重要性。

- 了解你的敌人：为什么你的网站处于危险之中

Web 服务器的主要威胁

入侵者攻击 Web 服务器和网站时，有一个简单的杀手锏，即寻找常见的漏洞。TechTarget 中国的特约专家列出了运行微软 IIS 的网站最常见的安全漏洞，例如操作系统与应用软件的默认安装、帐户密码很弱或者没有、大量的开放端口等。其中有些漏洞，比如开放端口，并不是 IIS 所特有的。

- 常见 IIS 安全漏洞清单
- 什么类型的 Web 服务能够危害 Web 服务器安全?

Web 服务器相关服务的安全

本小节是和 Web 服务器相关的 SMTP 邮件中继服务的安全性相关的，在本小节中，将介绍如何利用 IIS SMTP 的邮件中继服务阻止垃圾邮件直接接触到你的 Microsoft Exchange Server。

- 网络配置：IIS SMTP 邮件中继服务

Windows Web服务器之主要与非主要服务

非主要服务	主要服务
Alerter	COM+ Event System
ClipBook Server	Event Log
Computer Browser	IIS Admin Service
DHCP Client	IPSEC Policy Agent
Distributed File System	Logical Disk Manager
Distributed Link Tracking (Client and Server)	Network Connections
Distributed Transaction Coordinator	Performance Logs and Alerts
DNS Client	Plug and Play
FTP Publishing Service (unless FTP services required)	Protected Storage
Licensing Logging Service	Remote Procedure Call (RPC)
Logical Disk Manager Administrator Service	Remote Registry Service
Messenger	Security Accounts Manager
Net Logon*	System Event Notification
Network DDE	Uninterruptible Power Supply
Network DDE DSDM	Windows Management Instrumentation
Print Spooler	WMI Driver Extensions
Remote Registry Service	World Wide Web Publishing Service
Removable Storage	
Remote Access Connection Manager	
Routing and Remote	
Access RPC Locator (unless remote administration required)	
RunAS Service	
Server Service (unless SMTP or NNTP required)	
Task Scheduler	
TCP/IP NetBIOS Helper	
Telephony	
Telnet	
Windows Installer	

Windows Time	
Workstation*	

*服务是作为企业内部网 Windows 域的一部分所需的服务

(作者：Michael Cobb 来源：TechTarget 中国)

Windows IIS 服务器安全加固清单

常规

- 如果 IIS 服务器没有完全加固，就不要将其连接到网络
- 将服务器放置在一个安全的地点
- 不要在域控制器上安装 IIS 服务器
- 不要安装打印机
- 在服务器上使用两个网络接口，一个用于管理，一个用于网络
- 安装服务包(Service Pack) 、补丁以及 hot fixes
- 在服务器上运行 IIS Lockdown
- 安装并配置 URLScan
- 确保服务器的远程管理的安全并设置密码，低 session 暂停时间和帐户锁定
- 禁止不必要的 Windows 服务
- 确保服务运行在最低权限的帐户上
- 禁用不需要的 FTP, SMTP 和 NNTP
- 禁用 Telnet 服务
- 如果应用程序不需要则禁用 ASP.NET 服务
- 如果应用程序不需要则禁用 webDAV 服务，如果需要则确保它安全（具体方法参见：support.microsoft.com 网站的 Create a secure webDAV Publishing Directory）
- 不要安装数据访问组件,除非指定需要
- 不要安装 Internet 服务管理器的 HTML 版本
- 不要安装不必要的索引服务
- 不要安装不必要的 FrontPage 服务
- 加固 TCP/IP 栈

- 禁用 NetBIOS 和 SMB（关闭 137, 138, 139 和 445 端口）
- 重新配置回收站和页面文件系统数据分配策略
- 确保 CMOS 设置的安全
- 确保物理介质的安全（软盘驱动器，CD-ROM 驱动器等等）

帐户

- 删除服务器上不用的帐户
- 禁用 Windows 上的 Guest 帐户
- 重命名管理员帐户并设置一个复杂的密码
- 如果没有应用程序使用则禁用 IUSR_MACHINE 帐户
- 如果应用程序需要匿名访问则创建一个定制的最低权限的匿名帐户
- 不要赋予匿名帐户对网页内容目录的写访问权或者允许它执行命令行工具
- 如果你的主机有多个 Web 应用程序，则对每一个应用程序配置一个单独的匿名用户帐户
- 设置 ASP.NET 访问帐户为最低权限（只有当你不使用具有最低权限的默认 ASP.NET 帐户时才使用这个帐户）
- 加强服务器帐户和密码安全策略
- 限制远程登录（删除 Everyone group 中 “通过网络访问这台计算机”的用户权限）
- 不要在管理员中共享帐户
- 禁止 NULL session（匿名登录）
- 帐户的授权使用需要得到正式批准
- 不要允许用户和管理员共享帐户
- 在一个管理组中不要创建多于两个的帐户
- 要求管理员本地登录或者确保远程登录安全的方案

文件和目录

- 使用多个磁盘或分区，不要将 web 服务器根目录和操作系统文件夹安装在同一个分区
- 将文件和目录放在 NTFS 格式的分区上
- 将 web 站点内容放在非 NTFS 格式的分区上
- 创建一个新的站点，禁用默认站点
- 将日志文件放在非 NTFS 格式的分区上，但不要和 web 站点内容放在同一个分区
- 限制 Everyone group（不能访问\WINNT\system32 或者 web 目录）
- 确保 Web 站点根目录拒绝匿名 Internet 帐户的写访问
- 确保内容目录拒绝匿名 Internet 帐户的写访问
- 删除远程 IIS 管理应用(\WINNT\System32%#92;Inetsrv\IISAdmin)删除资源 kit tools, utilities and SDKs
- 删除示例应用（\WINNT\Help\IISHelp, \Inetpub\IISSamples）
- 删除 Content-Location 标头中的 IP 地址

共享

- 删除所有不必要的共享（包括默认管理员共享）
- 限制对必要共享的访问（Everyone group 没有这个权限）
- 删除不必要的管理共享（C$ and Admin$）（微软管理服务（SMS）和微软操作管理（MOM）需要这些共享）

端口

- 限制面向网络的接口为 80 端口（如果 SSL 使用则端口为 443）
- 在服务器上运行 IIS Lockdown

注册

- 限制远程注册访问

- 确保 SAM 的安全（HKLM\System\CurrentControlSet\Control\LSA\NoLMHash），这个只对单独的服务器有效
- 审核与日志
- 审核失败登录
- 重置 IIS 日志文件并确保其安全
- 根据应用安全需要配置一个合适文件大小的日志文件
- 定期存档并分析日志文件
- 审核对 Metabase.bin 文件的访问权限
- 设置 IIS 对 W3C 扩展日志文件格式的审核
- 在 support.microsoft.com 上阅读如何用 SQL 服务器分析 web 日志

站点和虚目录

- 将 web 站点放在非系统分区上
- 禁用“父路径”设置
- 删除具有潜在危险的虚目录，包括 IISSamples, IISAdmin, IISHelp and Scripts
- 删除或者确保 MSADC 虚目录（RDS）的安全
- 不要允许目录的读 web 访问权限
- 限制虚目录下的匿名帐户的写和执行 web 的权限
- 确保只有对支持内容创建的文件夹有脚本资源访问权限
- 确保只有对支持内容创建和被配置成电文鉴别（如果需要还有 SSL 加密）的文件夹有写访问权限
- 删除未使用的 FrontPage 服务扩展（FPSE），如果 FPSE 被使用，更新并且限制对它们的访问权限
- 删除 IIS 因特网打印虚目录

脚本映射

- 将不需要的文件扩展映射到 404.dll（.idq, .htw, .ida, .shtml, .shtm, .stm, idc, .htr, .printer）
- 将不必要的 ASP.NET 文件类型扩展映射到 Machine.config 中的 "HttpForbiddenHandler"

ISAPI 筛选器（ISAPI Filters）

- 删除服务器中不必要或者不用的 ISAPI 筛选器（ISAPI Filters）

IIS Metabase

- 通过使用 NTFS 许可（%systemroot%\system32\inetsrv\metabase.bin)限制对 metabase 的访问权限
- 限制 IIS 的标志信息（在内容中禁用 IP 地址）

服务器证书

- 确保证书日期范围是合有效的
- 服务器证书只限于运用于预期的用途（例如，服务器证书不用于 e-mail）
- 确保证书的公钥有效，所有通向信得过的根目录的路径得到核准
- 确认证书没有被废除

Machine.config

- 将保护资源映射到 HttpForbiddenHandler
- 删除不用的 HttpModules
- 禁用跟踪信息（<trace enable="false"/>）
- 关闭调试编译器（<compilation debug="false" explicit="true" defaultLanguage="vb">）

（作者：SearchSecurity.com 译者：张艳丽 来源：TechTarget 中国）

了解你的敌人：为什么你的网站处于危险中

对于互联网的标签行——“网站建好了，人们自然会来”——我愿意加上一句“试着侵入网站、攻击网站、滥用网站、破坏网站或者盗用网站。”

黑客们拥有的资源和时间甚至比最大的机构都要多，而且他们不受办公室政治、财政预算等常规的组织约束，而专业安全人员常常要面对这些约束。事实上，为了达到目的，黑客们可以组织起令人羡慕的在线合作，分享各种信息。本文可以帮助你了解黑帽（black hat）组织的工具、策略和动机，这样你就能更好地了解你的网站受到哪些威胁，了解网站赖以运行的系统，以及保护系统的重要性。

统计资料让你晚上也无法入睡

2004 年 9 月，《今日美国》进行了一次为期两周的测试，期间黑客试图闯入 6 台联网计算机 305，922 次。毫不夸张地说，计算机刚连到网络，攻击就开始了，两台计算机平均每小时遭受 300 多次攻击，其中一台装有 Windows XP Service Pack 1，但未安装防火墙；另一台是 Apple Macintosh。一台小型企业服务器（Windows Small Business Server）平均每小时遭受 60 次攻击。测试中，两台 Windows 操作系统的计算机都遭到破坏。

这些数据显示黑客组织异常活跃。任何联网计算机都处于危险中，连接 web 服务器的计算机尤为危险。相比其他类型的网站，电子商务网站更容易成为攻击的目标。不过如果你的网站被盯上，攻击只是迟早的事。

Script kiddies 与有组织犯罪

大多数的攻击都是自发而随意的，因为黑客并不会在意攻击的什么系统。攻击某个网站的多个远程系统很有可能无意中成为共犯，而网站的系统管理员根本不知道系统感染了

木马病毒（Trojan）。根据赛门铁克（Symantec）公布的《互联网安全威胁报告》，超过40%的针对互联网计算机的蠕虫攻击，其源 IP 地址来自于《财富》100 强公司控制的计算机！

这些攻击背后人通常称为 script kiddies，这是个贬义用语，并不能反映他们所造成的破坏情况。许多 script kiddies 缺乏技术竞争力。他们只是利用单个工具随意监控大量系统，然后攻击其中最薄弱的系统，就能造成严重的后果。这些攻击的高峰期与学校日历紧密相关，说明攻击背后有很多是青少年。

大多数情况下，script kiddies 使用的技术与以获取经济利益为主要目标的犯罪分子使用的技术相同。通常，当这些攻击由犯罪组织供给资金时，其目的就在于欺骗或者窃取网上财产，而不是造成破坏。

攻击背后的策略、工具和动机

Script kiddies 的目的在于尽可能使用最简单的方法获得计算机的控制权。Script kiddies 随意选择目标，也不关注造成的破坏，这使他们成为网站非常危险的攻击者，而且长久寄居在联网系统中。

网站攻击中使用的策略十分简单：建立能够被扫描的 IP 地址数据库（正在运行并可连接的系统），扫描并找出具有特定漏洞的地址，攻击这些地址。一旦 script kiddies 找出系统漏洞获得控制权，第一步通常是掩盖其踪迹。他们希望确保系统主人无法检测到病毒入侵。Script kiddies 会先检查是否有遭发现的危险，然后清除日志文件，替换或者修改各种关键文件。

Script kiddies 使用的工具简单易用，几乎不需要交互作用，而且随处可得。建立 IP 地址数据库时需要使用工具。一些工具会随意选择扫描哪个 IP 网络，另一些则会针对指定域名及其子域实行区域转换。扫描结果通常会存档或与其它黑客共享，以备日后攻击新的漏洞所用，这样就不用建立新的数据库。

明确数据库中哪个系统正在运行具有漏洞的操作系统后（利用 Fyodor’s nmap 等工具），入侵者就能很容易设定目标予以攻击。 新漏洞公布几天内，探测漏洞的工具就会出现。

正如攻击有自动运行的脚本，掩盖入侵者在系统中的行迹也有自动运行的工具，如 lrk4。这样的工具通常称为 rootkits。

入侵者一旦得到安全隐藏，往往会两者选其一：要不利用该系统扫描或者攻击其它系统，要不就攻击该系统。通常，它们会使用 sniffer 安静地监控系统，一段时间后再回来看看有没有获得密码、银行信息等有价值的数据。Script kiddies 攻击网站最常见的后果就是网站被涂改。这些攻击的动机可能纯粹是恶意破坏——出于积怨或者政治目的。其他 Script kiddies 可能是为了寻找挑战的乐趣，或者为了与别的黑客组织竞争，创造攻击最高级网站的记录。罪犯的动机单纯，只是想要进行欺骗、盗窃或者勒索。一些计算机业内人士坚持认为黑客（hackers）不同于骇客（crackers），因为黑客的动机并非恶意。但是对系统操作者而言，这仅仅是语义上的区别。

网站的风险与威胁

网站攻击分为两大类。影响网站的可访问性及可靠性的威胁可归为“拒绝服务（DoS）事件”。其他威胁则针对网站的内容和数据，侵入者试图剽窃、篡改、删除网页内容或者在网页上留下痕迹。这类事件最普遍，称为“骇客（cracking）事件”。两种威胁各有典例——分布式拒绝服务（DDoS）和蠕虫（worms）。

分布式拒绝服务（DDoS）

DDoS 攻击是一个用户控制上百甚至上千的受感染系统，使这些系统进行远程协作攻击受害者或受害群。受感染的系统越多，DDoS 攻击就越强烈。要防御和确定这类攻击源极为困难。蠕虫（worms）通常用于发起 DDoS 攻击。

Windows 攻击中的蠕虫

现在大多数系统受感染似乎都是由于蠕虫活动。蠕虫可以执行自动检测，找出并攻击具有漏洞的系统，而且呈指数式地自我复制。

蠕虫攻击最危险的形式是 IRCbot——bot 为 robot 的简称。Bot 是一种网络蠕虫，它的载荷不停地在后台运行，这样就可以通过 IRC 渠道后门访问受感染的计算机。 Bot 能启动 IRC 客户端程序，将其连接到 IRC 专用服务器， 而这个服务器很有可能通过 shell account 建立，且使用窃取的信用卡付帐；然后 bot 会等待下一步指令，接受攻击者的远程控制。攻击者可以通过联合多个 bot 病毒建立所谓的“僵尸网络（botnet）”。即使“僵尸网络（botnet）”相对很小，充分发挥它的力量也能很容易就发起有效的 DDoS 攻击。

W32/Agobot-RJ 是最为知名的 bot 病毒之一。Agobot 有 500 多种变型，一部分原因在于可以通过 GNU 通用公共许可证获得其源代码，这是黑客合作的又一个范。同时，近期的蠕虫还集合恶意代码作者的能力快速更新 bot 网络，趁机发起新的攻击。

哪些资源需要保护？

介绍了网站运行中的敌人和威胁后，我们来简要看看需要保护的四种关键资源。

Web 服务器

显而易见，这是应该首先保护的资源。不过，很多时候服务器并没有放置在安全的地点。如果谁都能实地接触并破坏服务器，那么将注意力集中在技术安全措施上就没什么意义了。路由器、网络电缆、防火墙等所有服务器的附属设备都需要得到像服务器一样的保护。

服务

要理解和保护服务器中运行的任何服务。每一项服务都意味着增加了开放端口和潜在漏洞。有可能的话，Web 服务器应该设为单功能服务器。 任何情况下，运行 Microsoft

IIS 的服务器都不能同时作为网络的域控制器，因为域控制器掌管着整个 Windows 网络域的账户安全。

内容

网站内容上传时不能危及服务器的安全。记住，网站的内容才是许多攻击者真正追求的东西。通常，不注意网站内容的安全性，就相当于许多安全措施都是白费功夫。

内部用户

通常，安全策略应该着重注意网络边界。然而，你预见通过台式机进行的攻击数目不断增加，使得客户端系统的安全越来越重要。攻击者会不断检测客户端软件代码的漏洞，企图找出新的角度攻击互联网系统。向社会工程(Social Engineering)攻击发展，采用像网络钓鱼软件（phishing）和间谍软件（spyware）的攻击策略呈不断增长的趋势，员工的安全意识也应该随之不断加强。

（作者：Michael Cobb 译者：周姝嫣 来源：TechTarget 中国）

常见 IIS 安全漏洞清单

Script Kiddies 攻击网站时，有一个简单的杀手锏，即寻找常见的漏洞。本文中，TechTarget 中国的特约专家列出了运行微软 IIS 的网站最常见的安全漏洞。其中有些漏洞，比如开放端口，并不是 IIS 所特有的。CERT(www.cert.org)和 CIAC(www.ciac.org)是两个不错的网站，提供了最新的影响网站的安全漏洞信息。

你可以通过下载最新补丁，来确保你的系统和网络避免这些攻击。微软 Baseline 安全分析器是微软发明的一个安全修补程序检查器，用于扫描本地或远程系统目前的补丁。你可能还需要考虑将 IIS 安装程序升级为 IIS 6.0，因为它的安全性比以前的版本显著增强。

常见 IIS 安全漏洞

操作系统与应用软件的默认安装

许多用户不知道安装程序在他们的机器上到底安装了什么。Windows 与 IIS 安装了过量的服务和危险的示例。未打补丁的服务、样例程序和代码为黑客提供了攻击网站的工具。

帐户密码很弱或者没有

IIS 使用内置或默认帐户。黑客一般会寻找这些帐户。如果这些账户没有从系统中删除的话，就会被发现并被更改。

大量的开放端口

每一位访问者，无论是善意还是恶意，都可以通过开放端口连接到站点和系统。在默认情况下，Windows 与 IIS 的开放端口远远多于为了正常运行所需的端口。保持系统的开放端口应该保持最少数量，这一点很重要。所有其他的端口都需要关闭。

Windows License Logging Service 溢出

通过发送一条经过特殊格式化的信息到运行 License Logging Service 的 Web 服务器，黑客能够对未检查的缓冲区进行攻击。这可以导致服务失效，为黑客打开一个开放端口，从而使用“System”权限在服务器上执行代码。

微软服务器信息块(SMB)漏洞

服务器信息块协议被 Windows 用于文件和打印机的共享以及计算机之间的通信。黑客的 SMB 服务器可以利用这项功能来使用“System”权限，对客户机执行任意代码。

ISAPI 扩展缓冲区溢出

IIS 安装后，就会自动安装多个 Internet ISAPI 服务器扩展。ISAPI 服务器扩展实际上是动态链接库（DLL），是用来增强 IIS 服务器的功能的。一些动态链接库，比如 idq.dll ，包含编程错误，可让黑客发送数据到 ISAPI 服务器扩展，这就是“缓冲区溢出”攻击。因此，攻击者可以完全控制 Web 服务器。

Unicode 漏洞（Web Server Folder Traversal）

通过向 IIS 服务器发送一个精心构造、包含非法 Unicode 序列的 URL，黑客可以绕过正常的 IIS 安全检查，迫使服务器逐字“进入或退出”目录，并执行任意脚本。

（作者：Michael Cobb　译者：王云辉 来源：TechTarget 中国）

什么类型的Web服务能够危害Web服务器安全?

问:有没有能够对Web服务器的安全构成威胁的服务?

答:绝对有。作为一个一般的规律，你不能在无法让Web服务功能正常运行的Web服务器上运行任何服务。根据你使用的操作系统和Web平台，这种情况有些不同。但是，你应该一直努力保持最低限度的一套服务运行。无关的服务能够为恶意黑客提供可以用来实施攻击的漏洞，在没有向你提供任何商业好处的同时攻破你的系统安全。

根据这个线索，你应该把你的重要组件分开，以便让每一台服务器仅托管一项重要的服务。例如，如果你拥有一个动态Web应用程序，好的做法是在不同的系统上托管数据库和Web服务器。这将提供某种程度的隔离，允许你更方便地实施分层次的防御攻击的保护措施。

(作者：Mike Chapple 来源：TechTarget中国)

网络配置：IIS SMTP 邮件中继服务

你可以利用 IIS SMTP 的邮件中继服务阻止垃圾邮件直接接触到你的 Microsoft Exchange Server。

你的 Exchange Server 可能是建在内部网络，为域内用户接收不断发过来的所有邮件。如果你启动 Exchange Server 的 SMTP 服务，互联网用户可以将邮件直接发到你的 Exchange Server。允许互联网直接连接你的 Exchange Server 可不是什么好主意。要想阻止这种直接接触，你需要设置 IIS SMTP 中继服务，启动 IIS SMTP 服务而不是 Exchange Server 的 SMTP 服务。这样，发送到你的域名中的邮件会首先到达防火墙的外部接口，然后转发到 SMTP 中继服务器。SMTP 中继服务器继而将邮件转发到 Exchange Server。现在，设置 Exchange Server，使 SMTP 外发邮件先发送到 IIS SMTP 中继服务器，再转发到互联网。

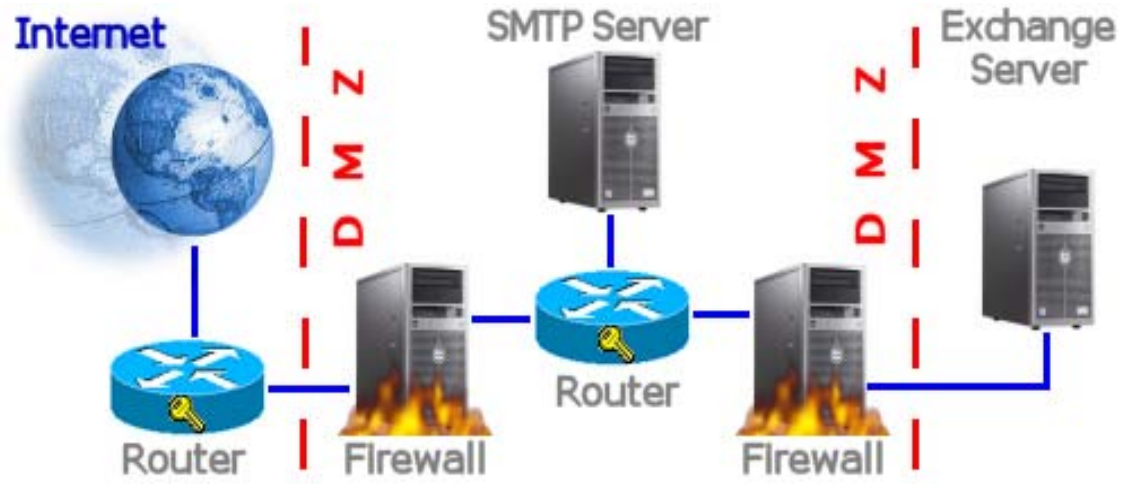

图 1：在这种配置下，Exchange Server 的 SMTP 服务不必与互联网的 SMTP 服务器接触

为使这种设置安全有效，接收邮件时设置 IIS SMTP 服务器只能转发到你的域。发送邮件时则允许 IIS SMTP 服务器转发到所有域。如果你允许需要接收的邮件转发到所有

域，垃圾邮件制造者就会利用邮件开放转发功能，几天之内你就得处理成千上万的垃圾邮件。默认配置下，凡是能通过身份验证的计算机都可以通过服务器转发邮件，不过，身份验证的费用较高，所以最好还是基于 IP 地址转发邮件。由于你只想让 Exchange Server 利用 IIS SMTP 服务器作为开放中继，所以将 Exchange Server 的 IP 地址添加到允许“仅以下列表（Only the list below）”。设置 IIS SMTP 服务作为 Exchange Server 的开放中继，因为 Exchange Server 需要发送 SMTP 邮件到所有的互联网电子邮件域。对外发邮件需要开放中继功能，而对接收邮件则要阻止中继。按照以下步骤配置服务器，就可以只中继发送到自己域中的邮件:

1.在 Internet 服务管理器控制台中，展开“默认 SMTP 虚拟服务器”节点。

2.右击“域节点（Domains node）”，指向“新域（New）”，单击“域（Domain）”。

3.选择“远程(Remote)”选项，单击“下一步（Next）”。

4.输入你的邮件域名，单击“完成（Finish）”。

5.双击新的“远程域名（Remote Domain name）”。

6.检查选项，允许“接收邮件”转发到该域名，这样 SMTP 中继就会删除转发到其它域的内发邮件。

7.在“路由域（Route domain）”对话框中，选择“把所有邮件转发到前端主机（Forward all mail to smart host）”。

8. 将 Exchange Sever 的 IP 地址带中括号填入该选项下方的文本框中，如[192.168.1.254]。

这种设置的另一好处就是在（网站）维护时你可以关闭邮件服务器，而不会丢失任何需要接收的邮件。你也可以通过设置 IIS SMTP 综合服务器，提高容错能力。另外，还可

以再添加一个邮件中继服务器，在邮件转发到 Exchange Sever 之前过滤垃圾邮件或者病毒。

（作者：Michael Cobb 译者：周姝嫣 来源：TechTarget 中国）