Windows防火墙让IIS7.0安全更加有保障Microsoft认证考试
 在以前，Windows操作系统自带的防火墙可以说是一个鸡肋产品。IIS管理员食之无味、弃之可惜。很多管理员就干脆直接禁用到IIS服务器上的防火墙功能。而购买第三方的防火墙软件来替代它。确实在以前版本的操作系统中，自带的防火墙产品在一定程度上会影响应用服务器的性能，而且配置起来也不是很灵活。 不过在IIS7.0中，这种情况有所改变。特别是在Windows2008操作系统上部署IIS网站应用的话，笔者建议各位管理员可以放心大胆的使用操作系统自带的防火墙产品。因为不仅防火墙软件本身有很大的优化，而且还实现了防火墙与IIS应用服务之间友好的集成。 一、采用默认策略来提高IIS应用服务的安全在IIS7与Windows2008中，防火墙产品已经完全与Server Manager实用程序(如IIS、FTP)及Roles Wizard整合在一起。简单的说，如果管理通过Roles Wizard来安全IIS应用程序，让服务器成为IIS服务器的时候，可以让防火墙仅仅只打开访问IIS服务器所需要的那些端口与协议。这相比以前版本的防火墙来说，是一个很大的改进。在以前，安装完之后管理员还需要去手工的打开或者关闭端口与协议。现在的话，通常情况下只要采用其默认的策略就可以满足常规下的安全需求。 即使出于某些特别的原因，需要采取更高级别的安全机制。如需要禁止HTTP访问，而只允许HTTPS协议等等。只需要在默认策略的基础上，稍微做调整即可。总之笔者认为，在Windows2008上部署IIS7.0应用服务，其自带的防火墙不会再成为鸡肋。而

是一个可以切实提高IIS应用服务器安全的一大法宝。其与操作系统、IIS应用服务友好集成，不仅可以提高服务器的性能，而且还可以提高IIS应用服务的安全。还有比较重要的一点，就是这完全是免费的。用户不需要再掏钱去购买第三方的防火墙产品。 二、创建入站与出站规则提高IIS安全有时候在IIS上可能还部署有其他非微软的第三方产品。如可能会在IIS上实现第三方的邮件系统或者FTP系统。此时由于第三方应用程序没有与微软的Roles Wizard整合在一起。故在部署完成这些第三方服务的时候，就需要手工对防火墙进行调整。如可能需要打开某些端口或者创建一些防火墙规则，以便这些第三方服务能够得到正确的运行。在实际工作中，安全管理员可以根据需要，建立控制业务量流向服务器的入站规则(即用户向IIS服务器发送的请求)服务器向外通信的出站规则(即服务器向客户端发送信息)。通过这个双向的控制，从而保障IIS应用服务器的安全。具体的来说，可以从如下几个方面来进行配置。 一是可以针对应用程序来设置出入站的规则。也就是说，规定某个应用程序是否可以访问互联网等等。在某些特定的情况下，管理员可能只允许某个应用程序访问内网，而不允许访问外网。如FTP文件传输工具，只可以在内部实用。此时管理员就可以创建一个规则，不允许这个FTP应用程序运行时访问外网。建立这个规则之后，防火墙会对这个程序的访问权限进行一定的限制。针对应用程序来设置不同的出入站规则，在实际工作中这个安全措施经常会被采用。特别是应用程序服务可能会涉及到多个不同端口的时候，就可以根据端口来设置出入站规则。当然根据实际的情况，管理员在保障安全的情况下，也可以允许某个应用

程序具有外网的访问权限。 二是针对端口来设置防火墙策略。其实这是第一种情况的衍生品。在应用程序部署过程中或者部署完成后，安全管理员可以在防火墙上打开或者关闭某个端口。如在IIS应用程序的端口中，其会默认打开几个需要用到的端口。但是管理员可能出于某种特殊的需要，如为了提高安全性，会改变某些协议如HTTP或者FTP 协议的默认端口。如果采用了默认端口的话，则攻击者通过扫描工具就可以了解某台应用服务器开启了哪些服务。即攻击者可以轻而易举的了解到攻击所需要的信息。而改变系统相关服务的默认端口，那么端口扫描工具就会失去其应有的作用。这也可以在很大程度上提高IIS应用服务器的安全型。不过这也会带来一个弊端。如对于FTP或者HTTP常用的服务，改变了其端口的话，则在访问时可能需要带上端口参数。为此只有在对于安全比较严格的场合，或者比较专业的环境中才会改变服务的默认端口。通常情况下，是不建议改变这些信息的。因为对于普通用户来说，让他们通过浏览器来访问服务器，在地址后面还需要加上一个端口号，现在要求有点高。所以改变默认端口的防火墙策略，通常只有在特定的场合中采使用。我们针对端口来进行防火墙策略的调整，主要是用来开启或者关闭某个端口。或者改变一些管理所需要的服务的端口，如SSH等等。这些管理所需要用到的服务，其涉及的范围比较少，有可能只有管理员一个人使用。再者其往往具有比较大的权限，故需要对这些服务给与特殊的照顾。为此在部署这些服务的时候，可以在安装向导中更改其所使用的默认端口。 三是可以选择预先定义的规则。如现在需要在一个IIS服务器上同时实现网站、邮件、FTP、OA办公自动化系统等

应用。其中可能只有网站与FTP采用了微软的产品。而邮件与OA办公自动化软件采用的是第三方的产品。在安装过程中，只有微软的产品防火墙才会自动使用默认的规则。这就是应用服务与防火墙整合的好处。而如果采用的是第三方的产品，则微软的防火墙就不会自动谁别，从而也就不会自动套用系统默认的规则。此时管理员也不需要一个个端口或者服务的进行配置。而可以直接选择已有的策略进行配置。在系统中内置了很多预定义的规则，如FTP、BITS等等。只要选择了这些对象规则，则防火墙就会自动启用某些服务与端口。因为不同的应用服务，如FTP、邮件等等，虽然其提供商是不同的。但是往往其所需要的服务与端口都是相同的。故可以采用内置的预定义规则来简化配置。 三、IIS、防火墙、其他安全技术结合使用在Windows2008、IIS7.0应用环境中，自带的系统防火墙不再只是一个替代品。它已经切切实实的成为了提高IIS7服务器安全的一大帮手。在实际工作中，除了防火墙之外，我们管理员还会采用其他的一些安全手段，与这些产品进行整合，从而构建一个立体的防御体系。如防火墙策略其主要作用在应用层。而在IIS中实现IPSec安全策略的话，也可以从传输层来提高IIS应用服务的安全性。也就是说，新增加的基于作用域、配置文件、IPSec状态等因素自定义规则的能力可以进一步似的服务器操作系统集成具有更高程度的安全性。或许在不久的将来，基于微软操作系统的IIS应用服务，不需要第三方的安全产品，也能够在很大程度上满足企业用户的安全需求。 