福建深空®信息技术有限公司

DIY 硬件 WEB 应用防火墙

By 深空®web 应用防火墙系统研发团队

最新信息请访问官网：http://www.sky-deep.com

目录

Web 应用防火墙（Web Application Firewall，后文统一简称为 **WAF**），是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 web 应用提供保护的产品，从形态上分为软件和硬件两种形式。

市面上的硬件 WAF 琳琅满目，而且价格不菲，从十几万到几十万甚至上百万不等。下面给大家介绍一种经济实惠的硬件 WAF 的 DIY，不但功能丰富而且性能良好，适合中小型企业、单位和租用 VPS 的网站站长。相关配套视频操作演示请访问：http://www.sky-deep.com/news/waf-movies.html

I. 准备软、硬件材料

- **硬件材料：**

装有 IIS 的主机一台(后文简称“**WAF 主机**”)。

比如 Windows Server 2000/2003/2008/2008 R2/2012/2012 R2 操作系统的 IIS5.0/IIS6.0/IIS7.0/IIS7.5/IIS8.0/IIS8.5 电脑或服务器。

- **软件材料：**

深空®web 应用防火墙系统（评估版）一套(后文简称“**深空 WAF 软件**”)，下载地址：http://www.sky-deep.com/skydeep-waf-trial.zip

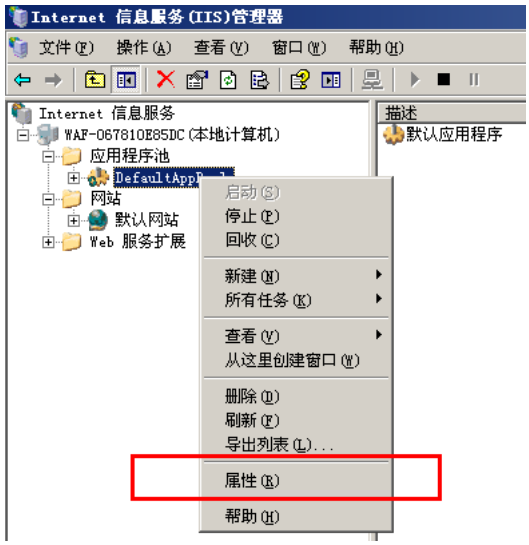
II. 安装

准备好上述软、硬件材料后，依照下面的步骤制作一台硬件 WAF。注意：操作前请确保 WAF 主机上已经安装好 IIS，**这里以纯净安装的 32 位 Windows Server 2003 SP2 + IIS6.0 环境为例。**如果 WAF 主机是 64 位系统或 Windows Vista 及其以后更新的操作系统，则有一些注意事项，详情请参考**深空 web 应用防火墙系统-管理员指南**中的**“不同环境下的注意事项”**一章，或者参考**配套视频操作演示**。

1. 打开默认应用程序池的属性配置界面

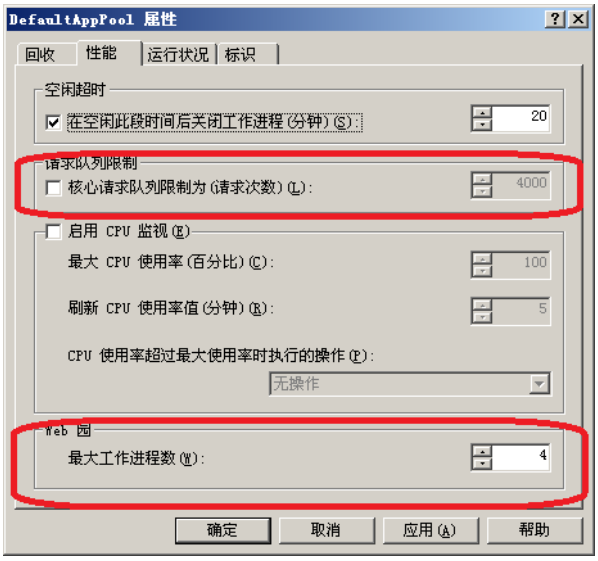
首先在 WAF 主机上打开默认应用程序池的属性配置界面：

在运行中输入“**inetmgr**”打开 IIS 管理器，然后“**应用程序池**”→“**DefaultAppPool**”→“**右键**”→“**属性**”,如下图所示：



2. 调整默认应用程序池属性配置

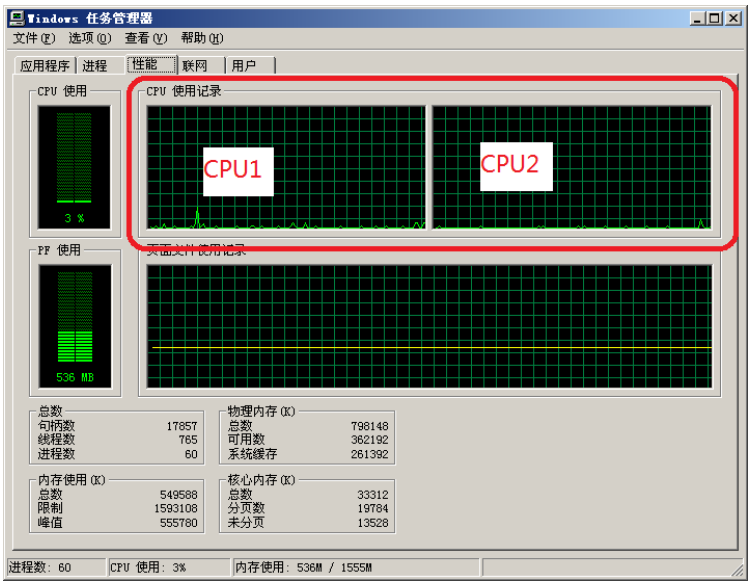
a) 取消请求队列限制,如下图第一个红框所示：



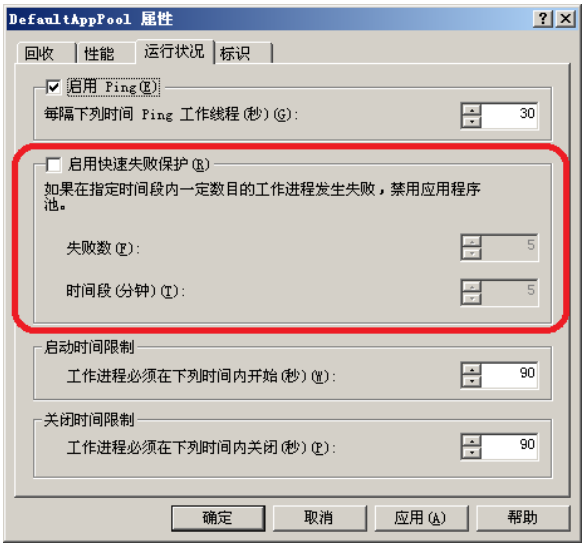
b) 设置 web 园最大工作进程数

至少调整为任务管理器所见 CPU 总核心数的 2 倍,如上图第二个红框所示.

下图任务管理器所示 CPU 总核心数为 2,则可以设置最大工作进程数为 4 或 6 或 8（注意：为增强并发性,无论 CPU 总核心个数为多少,此值都不得小于 4）.



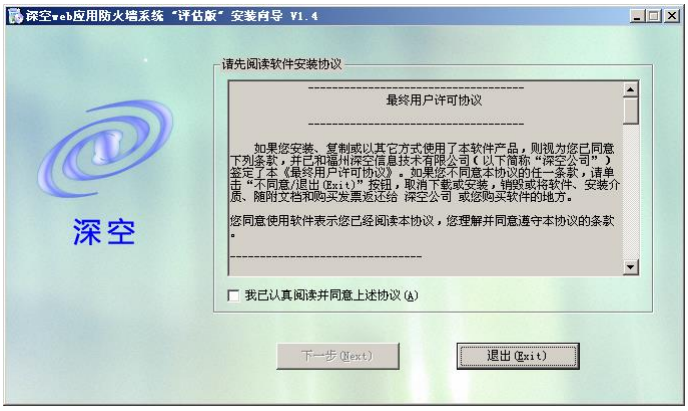
c) 关闭快速失败保护,如下图所示：



d) 完毕,点击“确定”保存.

3. 将深空 WAF 软件按默认安装到 WAF 主机上

在 WAF 主机上双击运行深空 WAF 软件的安装程序，按提示安装即可，非常简易快捷。



4. 调整 WAF 主机的 TCP/IP 处理能力

在 WAF 主机上把下面的内容另存为 reg 文件,也就是注册表文件,然后双击导入，**注意:导入完成后,必须重新启动 WAF 主机。**

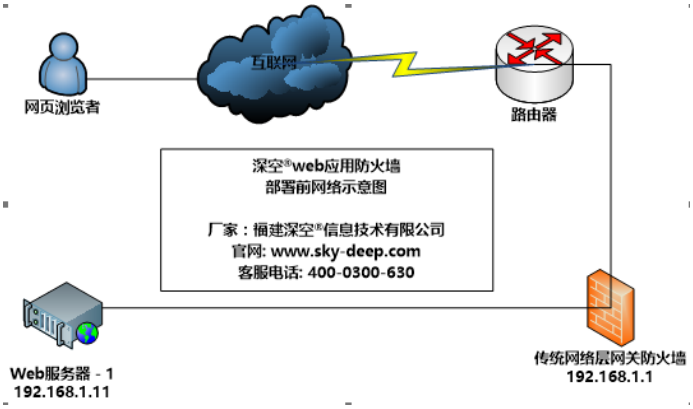
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]

"TcpMaxHalfOpen"=dword:000001f4

"SynAttackProtect"=dword:00000001

"TcpMaxHalfOpenRetried"=dword:00000190

"EnablePMTUDiscovery"=dword:00000000

"TcpMaxPortsExhausted"=dword:00000005

"KeepAliveTime"=dword:00000bb8

"KeepAliveInterval"=dword:000003e8

"TcpMaxDataRetransmissions"=dword:00000002

"NoNameReleaseOnDemand"=dword:00000001

"DefaultTTL"=dword:00000040

"TcpTimedWaitDelay"=dword:00000005

"TcpNumConnections"=dword:00fffffe

"MaxUserPort"=dword:0000fffe

"MaxHashTableSize"=dword:00010000
```

```
"MaxFreeTcbs"=dword:ffffffff
```

注意:导入完成后,必须重新启动 WAF 主机.

III. 部署

现在假设部署前 web 服务器 IP 是 **192.168.1.11**，web 服务器端口是 **80**，网关是 **192.168.1.1**，网络示意图如下：

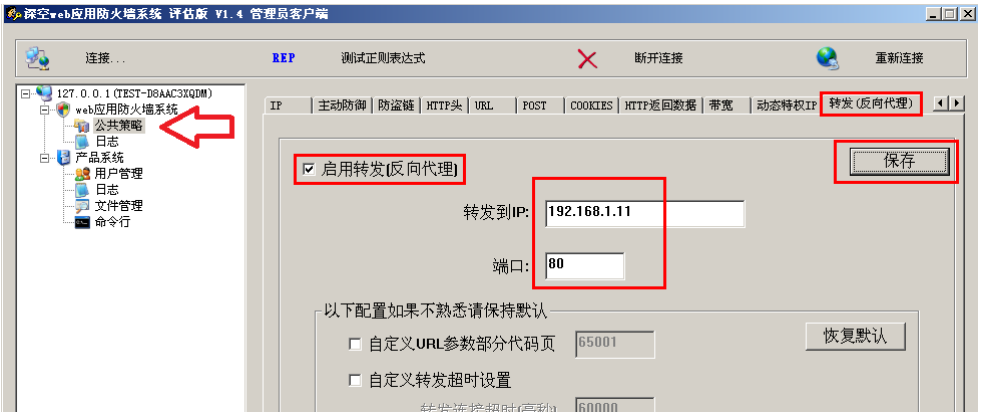


首先需要在 WAF 软件中开启转发（反向代理）功能。在 WAF 主机上打开深空 WAF 软件的管理端程序，输入 IP（127.0.0.1）、用户名（默认是 admin）、密码（默认是 admin-12345），如下图所示：

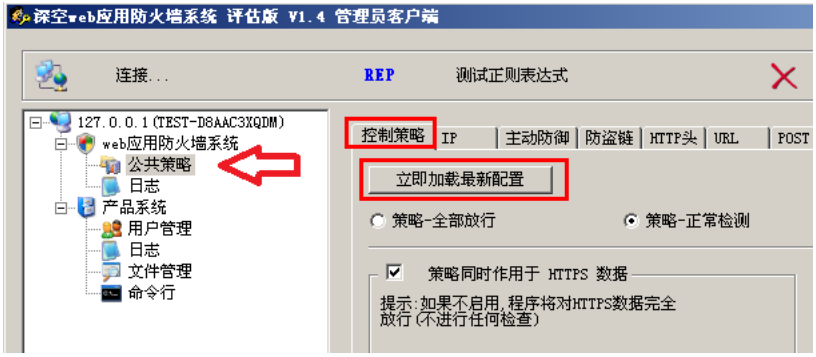
然后点击“**确定**”登录。

接着，我们要告诉深空 WAF 软件把接收到的 80 端口数据（经 WAF 安全策略检测正常的 HTTP/HTTPS 数据）转发到指定的 web 服务器 IP（192.168.1.11）和端口（80），如下操作：

“**web 应用防火墙系统**”→“**公共策略**”→“**转发（反向代理）**”，启用转发功能，并设置转发目的 IP 和端口，如下图所示：



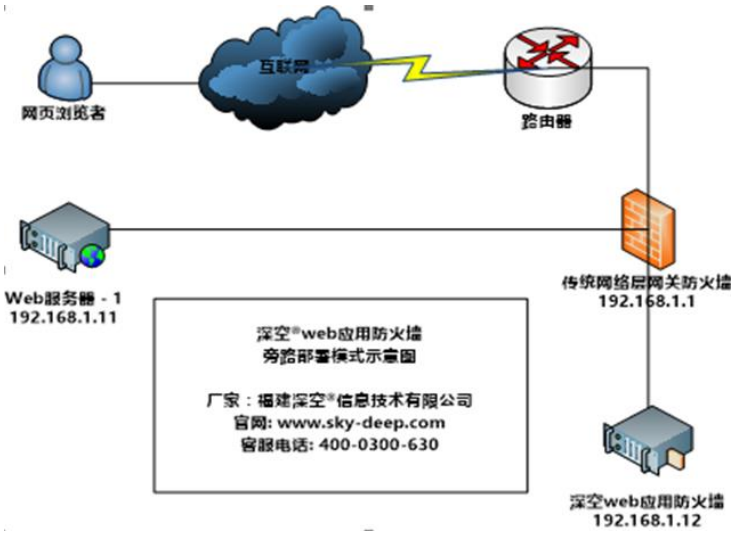
设置完后，点击“**保存**”使配置写入磁盘，然后点击 “**控制策略**”的“**立即加载最新配置**”使配置立即生效，如下图所示：



上面操作好后，下面开始介绍 2 种部署模式：**网桥部署模式**和**旁路部署模式。**

1. 旁路部署模式（适合单网卡的 WAF 主机）

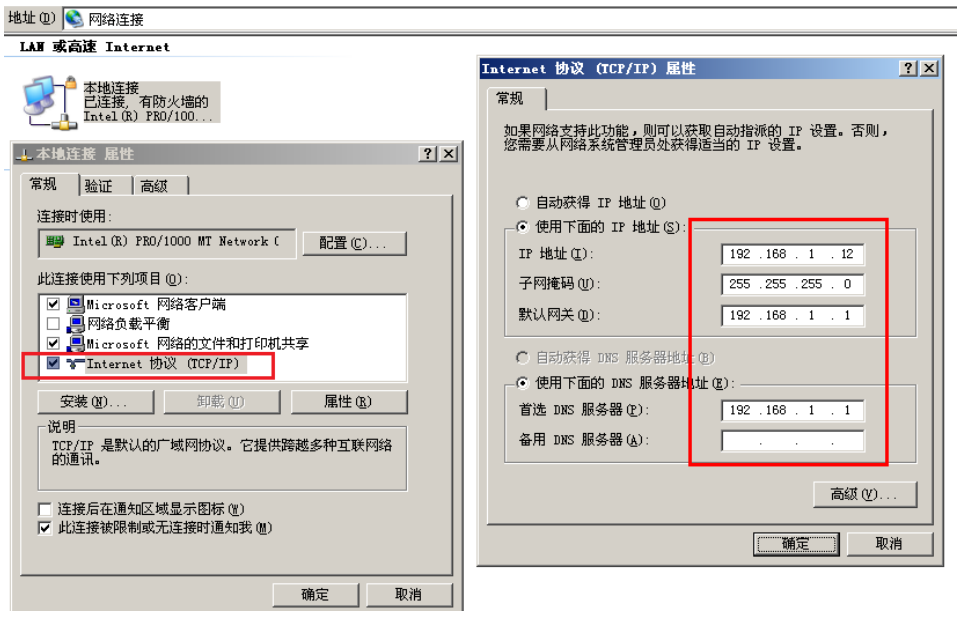
这种模式适合只有 1 张网卡的 WAF 主机，部署起来最为简易、快捷。如下图所示：



先用网线把 WAF 主机网卡接到网关上，然后给这个 WAF 主机设置一个固定 IP，最后在网关处把原本发给 192.168.1.11 的 80 端口的数据改成发给 192.168.1.12 的 80 端口。操作步骤如下：

a) 用网线把 WAF 主机网卡接到网关上。

b) WAF 主机：“**控制面板**”→“**网络连接**”→“**本地连接**”→“**右键**”→“**属性**”→“**Internet 协议（TCP/IP）**”然后设置 IP 为 192.168.1.12，网关为 192.168.1.1，DNS 为 192.168.1.1，如下图所示：



c) 确定，保存。

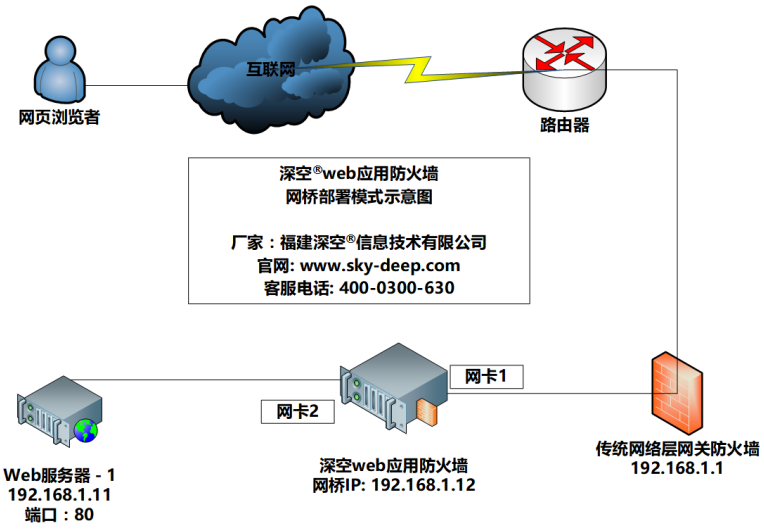
d) **测试**：在 WAF 主机上打开浏览器，访问 http://127.0.0.1，如果可以看到 192.168.1.11 服务器上的网站，说明 WAF 主机已经配置正确。

e) 在网关处把原本发给 192.168.1.11 的 80 端口的数据改成发给 192.168.1.12 的 80 端口。

f) 完毕。

2. 网桥部署模式（适合有 2 个网卡的 WAF 主机）

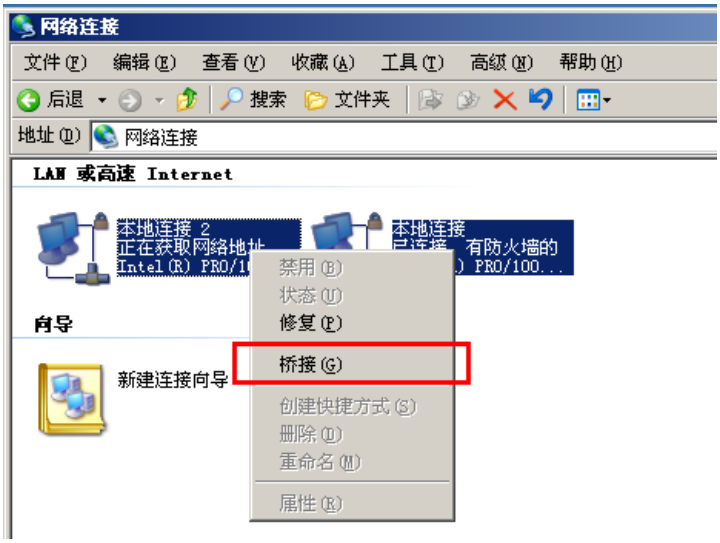
这种部署模式不增加网关的流量压力，但是需要 WAF 主机有 2 个网卡，一个网卡（网卡 1）用于连接到网关，另一个网卡（网卡 2）用于连接到 web 服务器，此时 WAF 主机好比是一个中间人，如下所示：



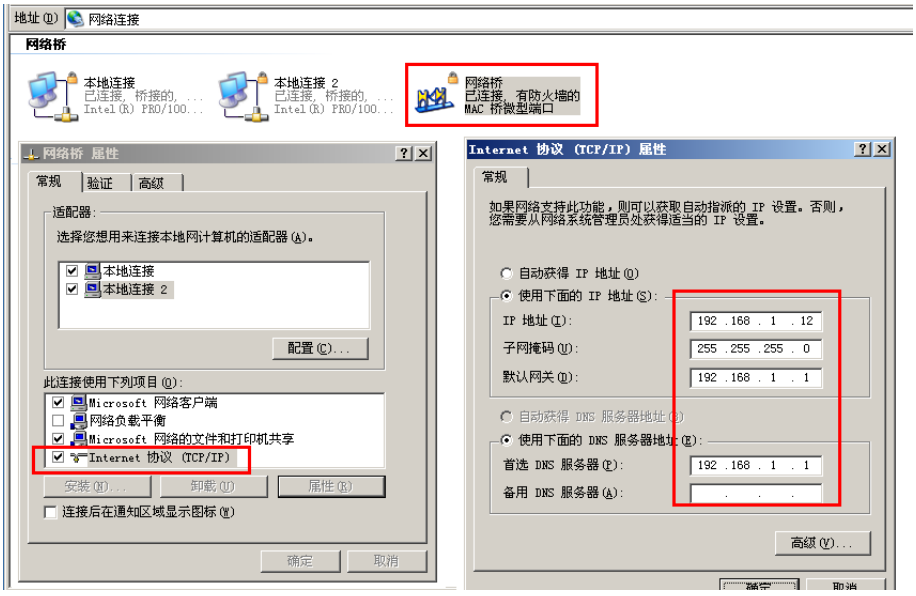
在 WAF 主机上，先把网卡 1 和网卡 2 组成一个网桥，然后给这个网桥设置一个固定 IP，最后在网关处把原本发给 192.168.1.11 的 80 端口的数据改成发给 192.168.1.12 的 80 端口。操作步骤如下：

a) 用网线将 WAF 主机的一个网卡（网卡 1）连接到网关，另一个网卡（网卡 2）连接到 web 服务器；

b) WAF 主机：“**控制面板**”→“**网络连接**”→同时选中已经接线的 2 个网卡→“**右键**”→“**桥接**”,如下图所示：



c) “**网络桥**”→“**右键**”→“**属性**”→“**Internet 协议（TCP/IP）**”然后设置 IP 为 192.168.1.12，网关为 192.168.1.1，DNS 为 192.168.1.1，如下图所示：



d) 确定，保存。

e) **测试**：在 WAF 主机上打开浏览器，访问 http://127.0.0.1，如果可以看到 192.168.1.11 服务器上的网站，说明 WAF 主机已经配置正确。

f) 在网关处把原本发给 192.168.1.11 的 80 端口的数据改成发给 192.168.1.12 的 80 端口。

g) 完毕。

IV. 其它说明

1. 配套视频操作演示

相关配套视频操作演示（包括 WAF 的安全防御功能等演示）请访问：

http://www.sky-deep.com/news/waf-movies.html

2. 提高并发性能的硬件途径

a) 使用核心数更多（如 8 核或 16 核及以上）、主频更高的（如 3.0GHz 及以上）的 CPU；

b) 使用多 CPU（如 2 个 CPU 或 4 个 CPU 及以上）；

c) 增加内存（如 8G 或 16G 及以上）；

d) 网卡确保为千兆以上；

3. 提高并发性能的软件途径

a) 使用最新的 Windows 服务器操作系统，如当前最新的 Windows Server 2012 R2；

b) 确保 WAF 主机的操作系统为默认干净安装；

c) 禁用 WAF 主机上所有不必要的服务和自启动项，比如如果使用 Windows Server 2012 当作 WAF 主机操作系统，可以在部署并调测完 WAF 主机后，把 WAF 主机切换回**服务器核心安装**模式，相关操作请参考配套视频操作演示；

d) 根据任务管理器中所见的核心数，适当增加**默认应用程序池**的**最大工作进程数**，如调整为总核心数的 4 倍。（**注意：应根据实际表现性能逐步找到最佳工作进程数，比如可以按每次增加 2 个工作进程来测试**）；

4. 增强 WAF 主机自身的安全性

a) 开启 Windows 自带的防火墙，仅开放 80 端口和必要的管理端口。

b) 禁用 WAF 主机上所有不必要的服务和自启动项；

c) 开启 Windows 的自动更新，让 WAF 主机能自动下载并安装操作系统补丁。

5. 使用客户端操作系统作为 WAF 主机操作系统

a) 如果没有 Windows 服务器操作系统的主机，也可以用常用的 Windows XP /Vista/7/8/8.1 的客户端操作系统主机。相关操作请参考配套视频操作演示。

b) 由于客户端操作系统在并发请求和稳定性等方面不如服务器操作系统，因此推荐在 Windows Server 系列操作系统上部署，如 Windows 2000 Server，Windows Server 2003，Windows Server 2008，Windows Server 2012 等。