

福州深空®資訊技術有限公司

DIY 硬體 WEB 應用 防火牆

By 深空®web 應用防火牆系統研發團隊

最新資訊請訪問官網：<http://www.sky-deep.com>

DIY 硬體 web 應用防火牆

目錄

I.	準備軟、硬體材料.....	2
II.	安裝.....	2
1.	打開預設應用程式池的屬性配置介面.....	3
2.	調整預設應用程式池屬性配置.....	3
3.	將深空 WAF 軟體按預設安裝到 WAF 主機上.....	4
4.	調整 WAF 主機的 TCP/IP 處理能力.....	5
III.	部署.....	6
1.	旁路部署模式（適合單網卡的 WAF 主機）.....	8
2.	橋接器部署模式（適合有 2 個網卡的 WAF 主機）.....	9
IV.	其它說明.....	11
1.	配套視頻操作演示.....	11
2.	提高併發性能的硬體途徑.....	11
3.	提高併發性能的軟體途徑.....	12
4.	增強 WAF 主機自身的安全性.....	12
5.	使用用戶端作業系統作為 WAF 主機作業系統.....	12

DIY 硬體 web 應用防火牆

Web 應用防火牆（Web Application Firewall，後文統一簡稱為 **WAF**），是通過執行一系列針對 HTTP/HTTPS 的安全性原則來專門為 web 應用提供保護的產品，從形態上分為軟體和硬體兩種形式。

市面上的硬體 WAF 琳琅滿目，而且價格不菲，從十幾萬到幾十萬甚至上百萬不等。下面給大家介紹一種經濟實惠的硬體 WAF 的 DIY，不但功能豐富而且性能良好，適合中小型企業、單位和租用 VPS 的網站站長。相關配套視頻操作演示請訪問：

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

I. 準備軟、硬體材料

➤ 硬體材料：

裝有 IIS 的主機一台(後文簡稱“**WAF 主機**”)。

比如 Windows Server 2000/2003/2008/2008 R2/2012/2012 R2 作業系統的 IIS5.0/IIS6.0/IIS7.0/IIS7.5/IIS8.0/IIS8.5 電腦或伺服器。

➤ 軟體材料：

深空®web 應用防火牆系統（評估版）一套(後文簡稱“**深空 WAF 軟體**”)，下載位址：

服務端英文版，管理端支持英文、繁體中文、簡體中文：

<http://www.sky-deep.com/skydeep-waf-trial-en.zip>

服務端簡體中文版，管理端支持英文、繁體中文、簡體中文：

<http://www.sky-deep.com/skydeep-waf-trial.zip>

II. 安裝

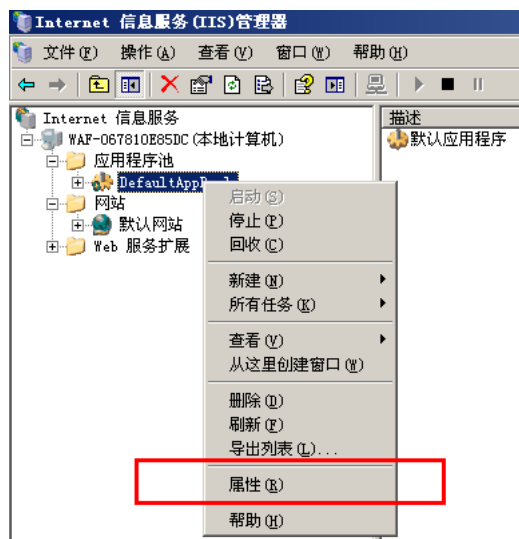
準備好上述軟、硬體材料後，依照下面的步驟製作一台硬體 WAF。注意：操作前請確保 WAF 主機上已經安裝好 IIS，這裡以純淨安裝的 **32 位 Windows Server 2003 SP2 + IIS6.0** 環境為例。如果 WAF 主機是 64 位元系統或 Windows Vista 及其以後更新的作業系統，則有一些注意事項，詳情請參考[深空 web 應用防火牆系統-管理員指南](#)中的“不同環境下的注意事項”一章，或者參考[配套視頻操作演示](#)。

DIY 硬體 web 應用防火牆

1. 打開預設應用程式池的屬性配置介面

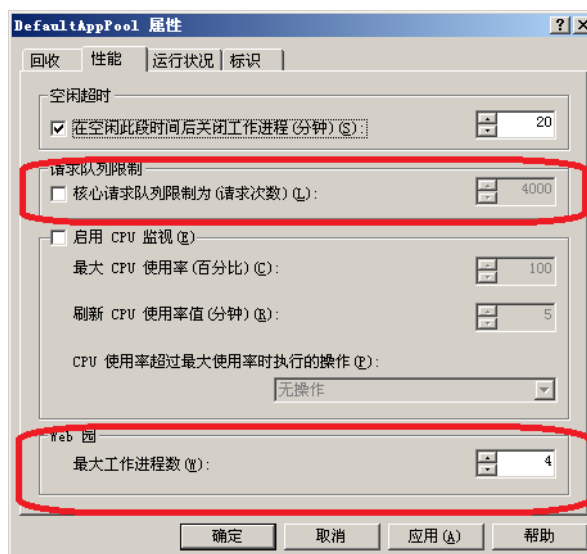
首先在 WAF 主機上打開預設應用程式池的屬性配置介面：

在運行中輸入 “inetmgr” 打開 IIS 管理器，然後 “應用程式池” → “DefaultAppPool” → “右鍵” → “屬性”，如下圖所示：



2. 調整預設應用程式池屬性配置

a) 取消請求佇列限制,如下圖第一個紅框所示：

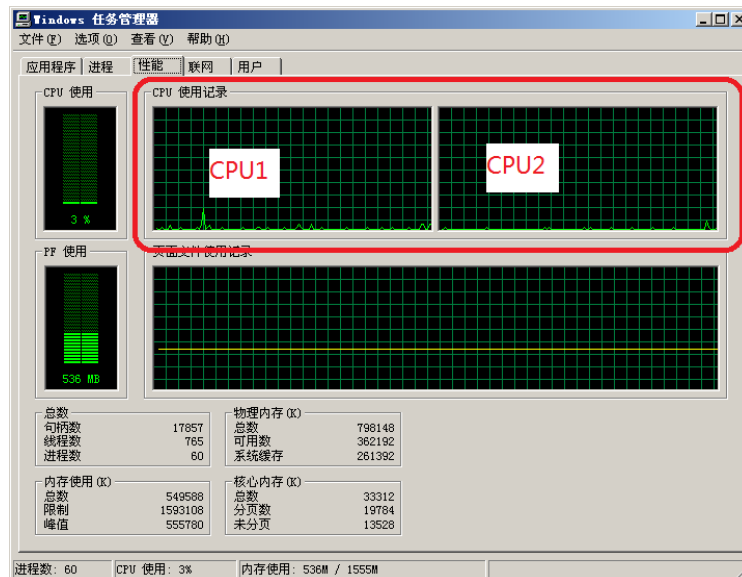


b) 設置 web 園最大工作進程數

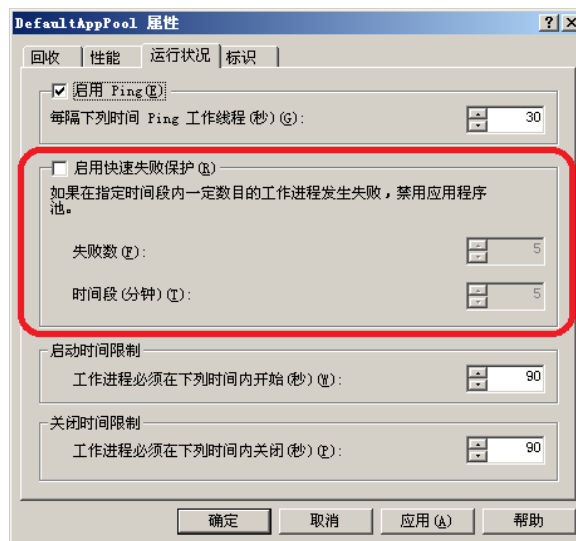
DIY 硬體 web 應用防火牆

至少調整為工作管理員所見 CPU 總核心數的 2 倍,如上圖第二個紅框所示。

下圖工作管理員所示 CPU 總核心數為 2,則可以設置最大工作進程數為 4 或 6 或 8 (注意: 為增強併發性,無論 CPU 總核心個數為多少,此值都不得小於 4)。



c) 關閉快速失敗保護,如下圖所示:

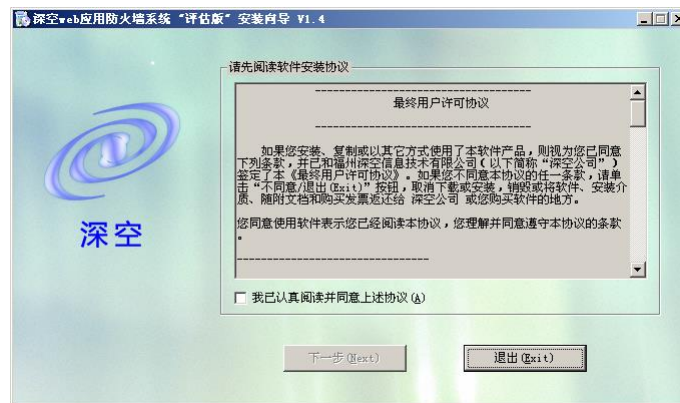


d) 完畢,點擊“確定”保存。

3. 將深空 WAF 軟體按預設安裝到 WAF 主機上

DIY 硬體 web 應用防火牆

在 WAF 主機上按兩下運行深空 WAF 軟體的安裝程式，按提示安裝即可，非常簡易快捷。



4. 調整 WAF 主機的 TCP/IP 處理能力

在 WAF 主機上把下面的內容另存為 reg 檔,也就是註冊表檔,然後按兩下導入，
注意:導入完成後,必須重新開機 WAF 主機。

```
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:00ffffff
```

DIY 硬體 web 應用防火牆

```
"MaxUserPort"=dword:0000fffe
```

```
"MaxHashTableSize"=dword:00010000
```

```
"MaxFreeTcbs"=dword:ffffff
```

注意:導入完成後,必須重新開機 WAF 主機.

III. 部署

現在假設部署前 web 伺服器 IP 是 **192.168.1.11**，web 伺服器埠是 **80**，閘道是 **192.168.1.1**，網路示意圖如下：



首先需要在 WAF 軟體中開啟轉發（反向代理）功能。在 WAF 主機上打開深空 WAF 軟體的管理端程式，輸入 IP（127.0.0.1）、用戶名（預設是 admin）、密碼（預設是 admin-12345），如下圖所示：

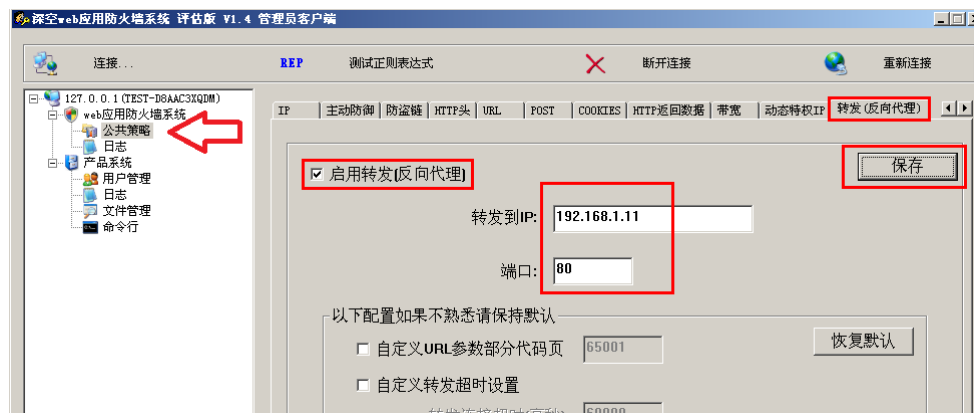
DIY 硬體 web 應用防火牆



然後點擊“確定”登錄。

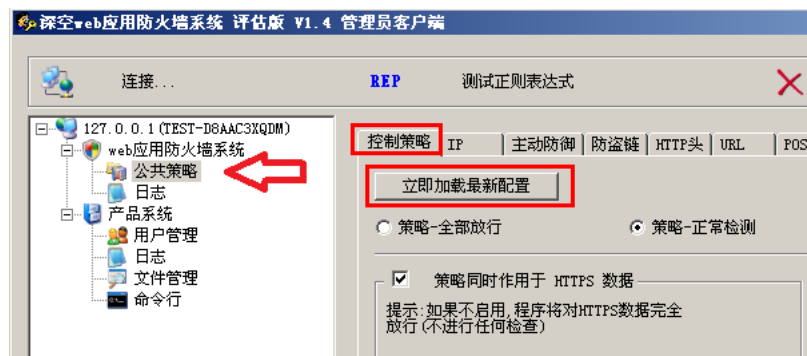
接著，我們要告訴深空 WAF 軟體把接收到的 80 埠資料（經 WAF 安全性原則檢測正常的 HTTP/HTTPS 資料）轉發到指定的 web 伺服器 IP（192.168.1.11）和埠（80），如下操作：

“web 應用防火牆系統” → “公共策略” → “轉發（反向代理）”，啟用轉發功能，並設置轉發目的 IP 和埠，如下圖所示：



設置完後，點擊“保存”使配置寫入磁片，然後點擊“控制策略”的“立即載入最新配置”使配置立即生效，如下圖所示：

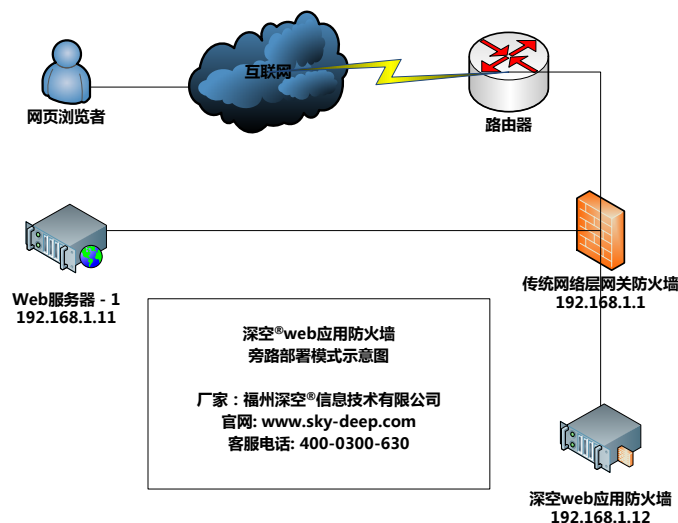
DIY 硬體 web 應用防火牆



上面操作好後，下面開始介紹 2 種部署模式：**橋接器部署模式**和**旁路部署模式**。

1. 旁路部署模式（適合單網卡的 WAF 主機）

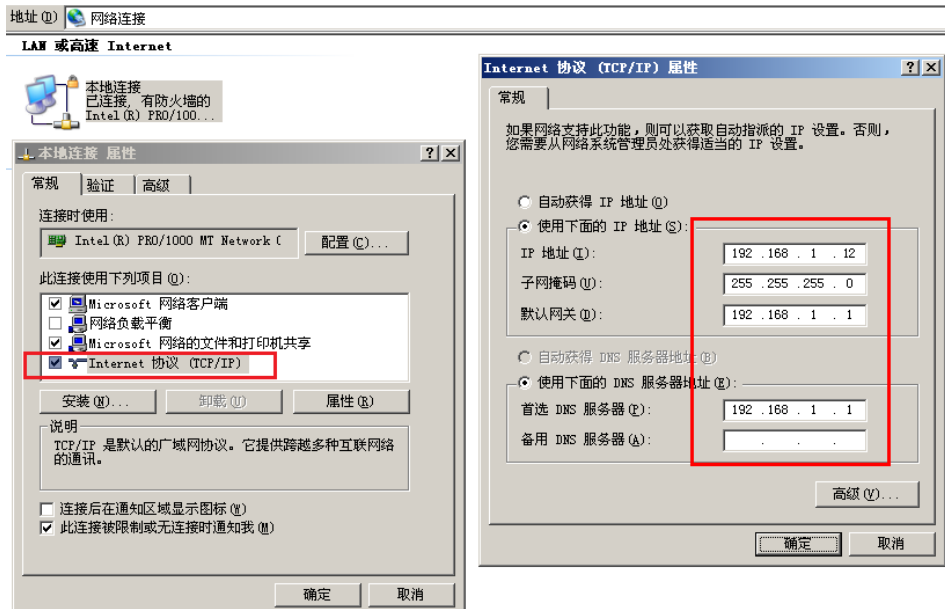
這種模式適合只有 1 張網卡的 WAF 主機，部署起來最為簡易、快捷。如下圖所示：



先用網線把 WAF 主機網卡接到閘道上，然後給這個 WAF 主機設置一個固定 IP，最後在閘道處把原本發給 192.168.1.11 的 80 埠的數據改成發給 192.168.1.12 的 80 埠。操作步驟如下：

- 用網線把 WAF 主機網卡接到閘道上。
- WAF 主機：“控制台” → “網路連接” → “本地連接” → “右鍵” → “屬性” → “Internet 協定 (TCP/IP)” 然後設置 IP 為 192.168.1.12，閘道為 192.168.1.1，DNS 為 192.168.1.1，如下圖所示：

DIY 硬體 web 應用防火牆



c) 確定，保存。

d) 測試：在 WAF 主機上打開瀏覽器，訪問 <http://127.0.0.1>，如果可以看到 192.168.1.11 伺服器上的網站，說明 WAF 主機已經配置正確。

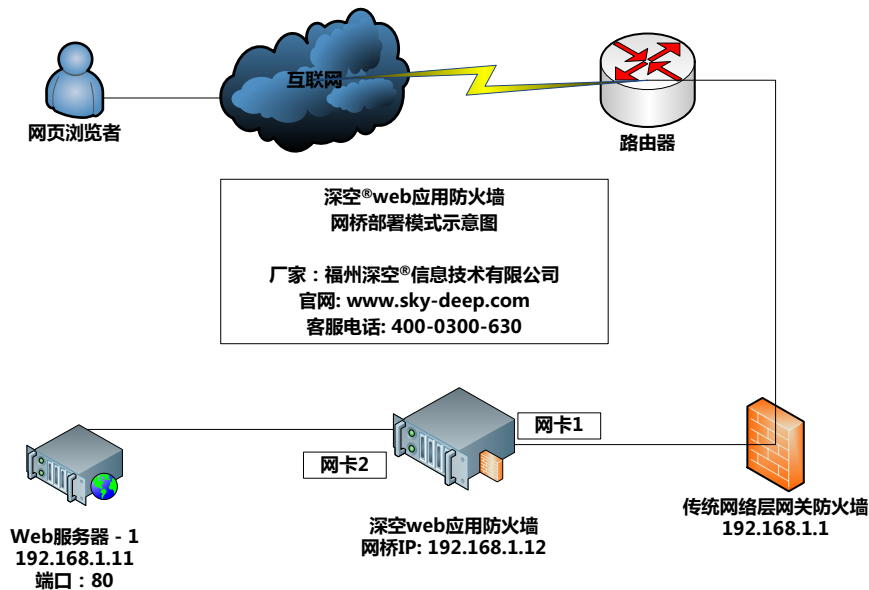
e) 在閘道處把原本發給 192.168.1.11 的 80 埠的數據改成發給 192.168.1.12 的 80 埠。

f) 完畢。

2. 橋接器部署模式（適合有 2 個網卡的 WAF 主機）

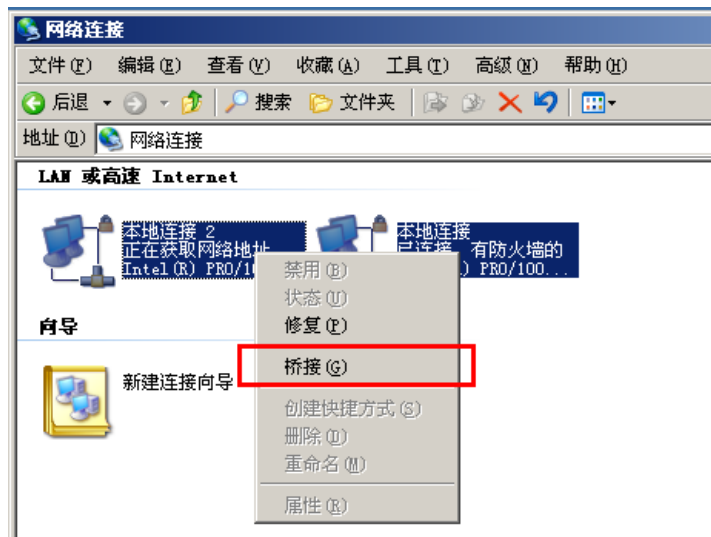
這種部署模式不增加閘道的流量壓力，但是需要 WAF 主機有 2 個網卡，一個網卡（網卡 1）用於連接到閘道，另一個網卡（網卡 2）用於連接到 web 伺服器，此時 WAF 主機好比是一個中間人，如下所示：

DIY 硬體 web 應用防火牆



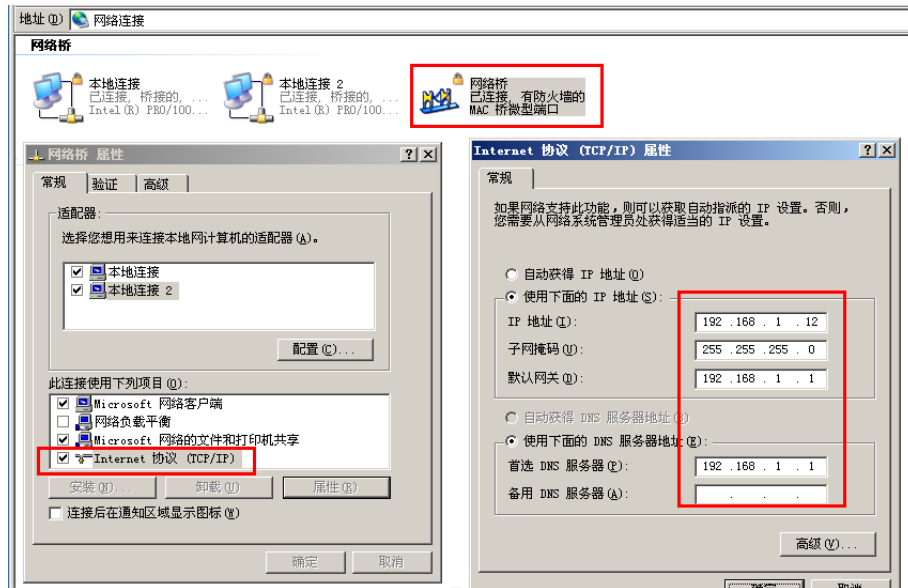
在 WAF 主機上，先把網卡 1 和網卡 2 組合成一個橋接器，然後給這個橋接器設置一個固定 IP，最後在閘道處把原本發給 192.168.1.11 的 80 埠的數據改成發給 192.168.1.12 的 80 埠。操作步驟如下：

- 用網線將 WAF 主機的一個網卡（網卡 1）連接到閘道，另一個網卡（網卡 2）連接到 web 伺服器；
- WAF 主機：“控制台” → “網路連接” → 同時選中已經接線的 2 個網卡 → “右鍵” → “橋接”，如下圖所示：



DIY 硬體 web 應用防火牆

- c) “網路橋” → “右鍵” → “屬性” → “Internet 協定 (TCP/IP)” 然後設置 IP 為 192.168.1.12，網道為 192.168.1.1，DNS 為 192.168.1.1，如下圖所示：



- d) 確定，保存。
- e) 測試：在 WAF 主機上打開瀏覽器，訪問 <http://127.0.0.1>，如果可以看到 192.168.1.11 伺服器上的網站，說明 WAF 主機已經配置正確。
- f) 在網道處把原本發給 192.168.1.11 的 80 埠的數據改成發給 192.168.1.12 的 80 埠。
- g) 完畢。

IV. 其它說明

1. 配套視頻操作演示

相關配套視頻操作演示（包括 WAF 的安全防禦功能等演示）請訪問：

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

2. 提高併發性能的硬體途徑

- a) 使用核心數更多（如 8 核或 16 核及以上）、主頻更高的（如 3.0GHz 及以上）的 CPU；
- b) 使用多 CPU（如 2 個 CPU 或 4 個 CPU 及以上）；

DIY 硬體 web 應用防火牆

c) 增加記憶體（如 8G 或 16G 及以上）；

d) 網卡確保為千兆以上；

3. 提高併發性能的軟體途徑

a) 使用最新的 Windows 伺服器作業系統，如當前最新的 Windows Server 2012 R2；

b) 確保 WAF 主機的作業系統為預設乾淨安裝；

c) 禁用 WAF 主機上所有不必要的服務和自啟動項，比如如果使用 Windows Server 2012 當作 WAF 主機作業系統，可以在部署並調測完 WAF 主機後，把 WAF 主機切換回伺服器核心安裝模式，相關操作請參考[配套視頻操作演示](#)；

d) 根據工作管理員中所見的核心數，適當增加預設應用程式池的最大工作進程數，如調整為總核心數的 4 倍。（注意：應根據實際表現性能逐步找到最佳工作進程數，比如可以按每次增加 2 個工作進程來測試）；

4. 增強 WAF 主機自身的安全性

a) 開啟 Windows 自帶的防火牆，僅開放 80 埠和必要的管理埠。

b) 禁用 WAF 主機上所有不必要的服務和自啟動項；

c) 開啟 Windows 的自動更新，讓 WAF 主機能自動下載並安裝作業系統補丁。

5. 使用用戶端作業系統作為 WAF 主機作業系統

a) 如果沒有 Windows 伺服器作業系統的主機，也可以用常用的 Windows XP /Vista/7/8/8.1 的用戶端作業系統主機。相關操作請參考[配套視頻操作演示](#)。

b) 由於用戶端作業系統在併發請求和穩定性等方面不如伺服器作業系統，因此推薦在 Windows Server 系列作業系統上部署，如 Windows 2000 Server，Windows Server 2003，Windows Server 2008，Windows Server 2012 等。