wpad 實作

#參照:http://findproxyforurl.com/

環境:

防火牆pfsense 2-使用squid 啓用**Transparent proxy**

原因:

爲了要控制使用者的facebook的上網時間,它是個人社交工具,但是facebook會轉址爲https連線,若要控制https連線,就不可以使用transparent 代理,但是若改爲該設定,必須爲所有電腦設定代理伺服器,如何簡化該工作讓電腦自動取得我的設定,如dhcp讓電腦自動取得,而不用一台一台設?

答案:

web proxy auto discovery protocol (就是自動設定代理伺服器協定),(我的觀點,它並不是一個我們稱的正式協定,而是比較像是一個流程)

原理:

要讓電腦自動取得代理的設定,會借用目前存在的二個協定(dhcp或dns)讓使用端取得相關設定值
這裏,會再引進一和檔案pac,以javascript的寫法,讓client 端判斷如何上網

1.PAC(Proxy Automatic Configuration)檔:是一個檔案,內容包含相關的代理伺服器設定

2.WPAD:設定代理伺服器的協定,因爲不同的瀏覽器支援不同的方式因此會主要有下兩種模式:

dhcp wpad: 使用dhcp來取得存放pac檔案所在,當瀏覽器勾選自動偵測,

由dhcp中找尋代碼252,內存放格式http://主機:連接埠/wpad.dat

#其中主機可以是IP,也可以是名稱而wpad.dat必須放在該主機提供的web的根目錄下

若:http://10.10.1.6/wpad.dat ,就是找該檔案

dns wpad : 使用dns 來取得存放pac檔案所在,當瀏覽器勾選自動偵測,由dns中找尋wpad.yourdomain ,

其中yourdomain變成你的網域名稱,假設爲,mycompany.com.tw

則找尋http://wpad.mycompany.com.tw/wpad.dat

- dhcp 一般firefox不支援(除了在Mac OS X支援),Google Chrome,Apple Safari在作業系統windows 7 不支援外,其它均支援
- 若爲相容性:建議兩個都設定,若爲安全:則只要設定dhcp就好了
- 上述得知,可能需要的設定的有dhcp,dns及web server
- 若兩者都設定,則其優先權dhcp有較高的優先權比dns
- dns會有安全性的問題,如果有人(電腦在系統中)串改dns,可能就會造成上網的問題

PAC 基本

PAC是javascript 函式

支援的函式(已略過不重要的函式)

函式名稱	說明	範例
dnsDomainIs	檢查主機名稱,是否包含某網域	if (dnsDomainIs(host,"google.com")) return "DIRECT";
shExpMatch	檢查主機名稱或是URL合乎,shExpMatch(host,"主機")，shExpMatch(url,"網址")	if(shExpMatch(host,"vpn.domain.com") ‖ shExpMatch(url, "http://abcdomain.com/folder/*")) return "DIRECT";
isInNet	檢查IP在某個範圍內	if(isInNet(dnsResolve(host),"10.10.1.0","255.255.255.0")) return "DIRECT";
myIpAddress	傳回瀏覽器所在主機的IP(client端的IP)	if(isInNet(myIpAddress(),"10.10.1.0","255.255.255.0")) return "PROXY 10.10.5.1:8080");
dnsResolve	使用DNS解析主機名稱爲IP	if(isInNet(dnsResolve(host), "10.10.1.0","255.255.255.0") return "DIRECT"
isPlainHostName	檢查host是否只含名稱,不含dot(.)	isPlainHostName(host) 1.若host爲www 傳爲真值 2.若host爲www.chung-hong.com 傳回假值
isResolvable	查詢dns是否可反解主機名稱爲IP	
weekdayRange	星期的範圍	weekdayRange("MON","FRI")
dateRange	日期的範圍	dateRange("JAN","MAR")
timeRange	時間的範圍	timeRange(8,18)

#url 你上網的網址
#host由上網的網址中,取出的主機名稱

PAC檔案範例

基本的良好的 PAC檔案是清楚簡潔的程式. 不同的方法可以產生相同的結果(程式寫法不同,但是結果相同).

本頁包含了一個 PAC檔案的範例是穩定和容易更新.

特性

- 內部IP,內部主機,和主機包含 .local的規則 .
  - 當其它規則在例子中可以是選項, 大部份部署開始在這個區塊中 (第 3-10行).
- 主機名稱規則.
- 協定和URL規則.
- 機器根據 IP路由規則.
- 預設代理規則, 如果上述不合乎.

PAC 檔案

```
1  function FindProxyForURL(url, host) {
2
```

```
3  // 如果主機名稱相同,傳回"DIRECT"直接連線.
4     if (dnsDomainIs(host, "intranet.domain.com") ||
5        shExpMatch(host, "(*.abcdomain.com|abcdomain.com)"))
6        return "DIRECT";
7
8  // 如果協定或是 URL相符直接連線.
9     if (url.substring(0, 4)=="ftp:" ||
10       shExpMatch(url, "http://abcdomain.com/folder/*"))
11       return "DIRECT";
12
13 // 如果連線的主機是內部IP,直接連線.
14    if (isPlainHostName(host) ||
15       shExpMatch(host, "*.local") ||
16       isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
17       isInNet(dnsResolve(host), "172.16.0.0",  "255.240.0.0") ||
18       isInNet(dnsResolve(host), "192.168.0.0",  "255.255.0.0") ||
19       isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
20       return "DIRECT";
21
22 // 如果IP位址是內部子網指定到某一個代理伺服器.
23    if (isInNet(myIpAddress(), "10.10.5.0", "255.255.255.0"))
24       return "PROXY 1.2.3.4:8080";
25
26 // 預設規則: 不合乎上述者使用下面代理伺服器.
27    return "PROXY 4.5.6.7:8080; PROXY 7.8.9.10:8080";
28
29 }
```

推薦當部署 URL和主機規則時小心規則必須清楚明確.

Host 範例
if (dnsDomainIs(host, "abcdomain.com"))
return "DIRECT";

URL 範例
if (shExpMatch(url, "http://abcdomain.com/folder/*"))
return "DIRECT";

警告
下面的程式碼是一個非預期的結果因爲使用shExpMatch函式,* ,和主機名稱.
警告範例
// 下面輸入會直接連網:
// 1. www.hotmail.com 2. phishing-scam.com?email=someone@hotmail.com
if (shExpMatch(url, "*hotmail.com*"))
    return "DIRECT";

---

squid transparent 問題

當我啓用squid transparent 時,如果我又指定代理伺服器時,則https
不使用標準443時會產生下面的錯誤
https://abc.com.tw:10000

拿別台squid,改爲非通透式的,就會正常

實作:

環境:

公司網域: abc.com.tw

內部網路:10.10.1.0/24

名稱伺服器: 使用windows2003內建的

代理伺服器:10.10.1.6:3128

web伺服器:10.10.1.6

1.建立pac檔

```
function FindProxyForURL(url, host)
{
 if (isInNet(host, "10.10.1.0", "255.255.255.0"))
 {
  return "DIRECT";
 }
  if (isInNet(myIpAddress(), "10.10.1.0", "255.255.255.0"))
 {
  return "PROXY 10.10.1.6:3128";
 }
}
```

1.當要連線的主機是10.10.1.0/24直接連線 ,

2.client 端是10.10.1.0/24的網段,直接連線

3.其它預設以10.10.1.6:3128代理連線

儲存在c:\wpad.dat

2.測試

ie	firefox
	

ie->網際網路選項->連線

使用自動組態指碼(打勾)->網址(位址)

輸入file:///c:/wpad.dat

firefox ->工具->選項->網路->設定

Proxy自動設定網址(URL):.....

輸入file:///c:/wpad.dat

3.設定web server ,我使用linux的apache

1.將檔案wpad.dat傳送到10.10.1.6的/var/www/html下,讓使用者有r的權限chmod +r /var/www/html/wpad.dat

2.編輯/etc/httpd/conf/httpd.conf,加入AddType application/x-ns-proxy-autoconfig .dat

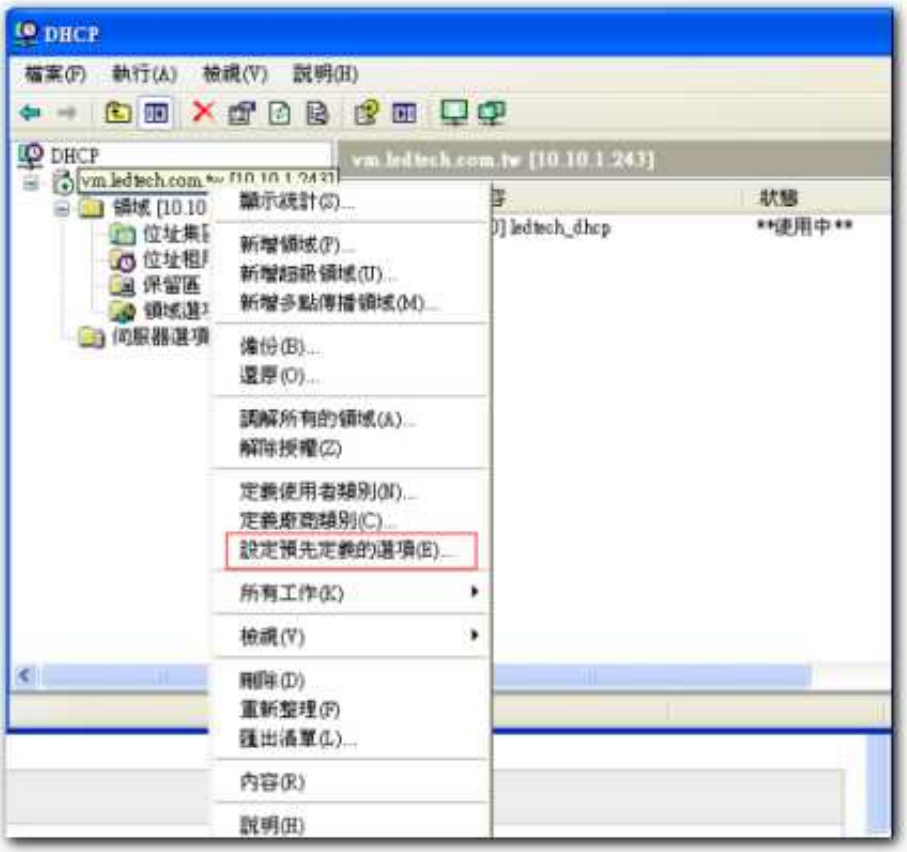
(這好像不一要用)

3.重啓service httpd reload

4. 使用瀏覽器輸入http://10.10.1.6/wpad.dat ,能夠連線就是正常

4.dns設定(如果你決定使用dns來提供pac檔案
在內部dns主機在abc.com.tw 新增一台主機A記錄 wpad.abc.com.tw 10.10.1.6
#確認client端dns設定是對的,然後執行 nslookup wapd.abc.com.tw
#如果你是使用windows內建的dns,可能會有問題,是因爲global block list的問題,請參照windows 2003/2008 dns 問題

5.dhcp設定(如果你決定使用dhcp來提供 pac檔案
使用windows dhcp



同2測試,變更爲自動偵測,ie會找dhcp,firefox爲使用dns

---

windows 2003/2008 dns 問題

windows server 2008 DNS 伺服器新增了一個 global query block list來降低動態更新 DNS 的危險.
#雖然是2008引進的,但是2003版本5.2.3790.4460以上也都包含了這個功能,說明在 KB961063.

windows 2003 dns

啓用, 停用, 或是設清單必須修改登錄檔 Windows 2003.

執行regedit ,到如下的key值

Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
名稱 EnableGlobalQueryBlockList
類型 REG_DWORD (DWORD Value)
資料 啓用: 1; 停用: 0

預設是停用.若啓用將上述值改爲0,就會停用

管理 Global Query Block List
Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
名稱 GlobalQueryBlockList
類型 REG_MULTI_SZ (Multi-String Value)
資料 wpad isatap

注意wpad 和isatap 是預設值.
該登錄值並不會在dns主機間自動同步,也就是你要到每一台的dns中設定

windows 2008 dns

使用dnscmd 命令工具來管理global query block list.開啓一個指示命令列,執行下面的工作:

1.檢查global query block是否啓用:

```
dnscmd /info /enableglobalqueryblocklist
```

2.顯示目前封鎖清單中的主機名稱:

```
dnscmd /info /globalqueryblocklist
```

3.停用封鎖清單,並確定DNS伺服器沒有忽略對封鎖清單的名稱查詢:

```
dnscmd /config /enableglobalqueryblocklist 0
```

4.啓用封鎖清單,並確定DNS伺服器忽略封鎖清單中的名稱查詢:

```
dnscmd /config /enableglobalqueryblocklist 1
```

5.移除封鎖清單中的所有的名稱:

```
dnscmd /config /globalqueryblocklist
```

6.以指定的名稱清單取代目前的封鎖清單:

```
dnscmd /config /globalqueryblocklist name [name]…
```

附錄:

squidguard 設定範例

說明:10.10.1.0/24,10.10.2.0/24 連線 facebook_domain,在work_time 時間內會被導引到一個 10.10.1.6/facebook.html的說明檔

不在work_time時間內則可以正常上

```
#其中facebook_domain 位於/var/squidGuard/facebook_domain ,內容是
        facebook.com
        akamaihd.net

#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/squidGuard/
logdir /var/log/squidGuard
#logdir /var/log/squid

#
# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

#work time
time work_time {
   weekly * 08:00 - 12:00
   weekly * 13:00 - 18:00
}

#
# REWRITE RULES:
#

src lan {
   ip      10.10.2.0/24
   ip      10.10.1.0/24
}
```

```
destination facebook_domain {
    domainlist    facebook_domain
}

rew dmz {
    s@://admin/@://admin.foo.bar.de/@i
    s@://foo.bar.de/@://www.foo.bar.de/@i
}

#
# SOURCE ADDRESSES:
#

#
# DESTINATION CLASSES:
#

dest good {
}

dest local {
}



acl {
    lan within work_time {
        pass !facebook_domain all
        redirect 301:http://10.10.1.6/facebook.html
            log facebook.log
    } else {
        pass facebook_domain all

    }
    default {
        pass any
        }
}
```