# WPAD configuration in TMG 2010

In this tutorial, we will show you how the Web Proxy client provides different security and performance advantages when accessing the TMG web proxy server.

**In this tutorial we will show you how the Web Proxy client provides distinct security and performance advantages when accessing the TMG web proxy server.**

In Forefront Threat Management Gateway (TMG) 2010, there are three client types - SecureNAT, Web Proxy and TMG Firewall. Clients accessing resources through the TMG firewall can be any of these or may be all three because they are not mutually exclusive. However, each type of client has its advantages and disadvantages.

Many network professionals choose SecureNAT clients when designing TMG firewall implementations because they are easy to configure. All that is required is to make a change to the workstation's default gateway and routing table. Although SecureNAT clients are easy to configure, they also have some serious limitations in security and performance. Cannot authenticate because they do not have authentication mechanisms in IP packets. In addition, SecureNAT clients also consume a lot of system resources, reducing the amount of traffic a TMG firewall can handle.

From a security and performance perspective, Web Proxy clients are an ideal choice. When clients are configured to use the TMG firewall as a web proxy server, they help increase user authentication and reduce the need for system resources on the firewall. However, the downside is the need to change the client configuration.

## Configure a Web Proxy client

However, configuring a Web Proxy client is very simple. You can use Internet Explorer to do that, open the web browser and from the menu, select **Tools / Internet Options / Connections / LAN Settings** . Select the option **Use a proxy server for your LAN** and enter the hostname or IP address of the TMG proxy, then specify the port configured for the web proxy listener (the default is port 8080).

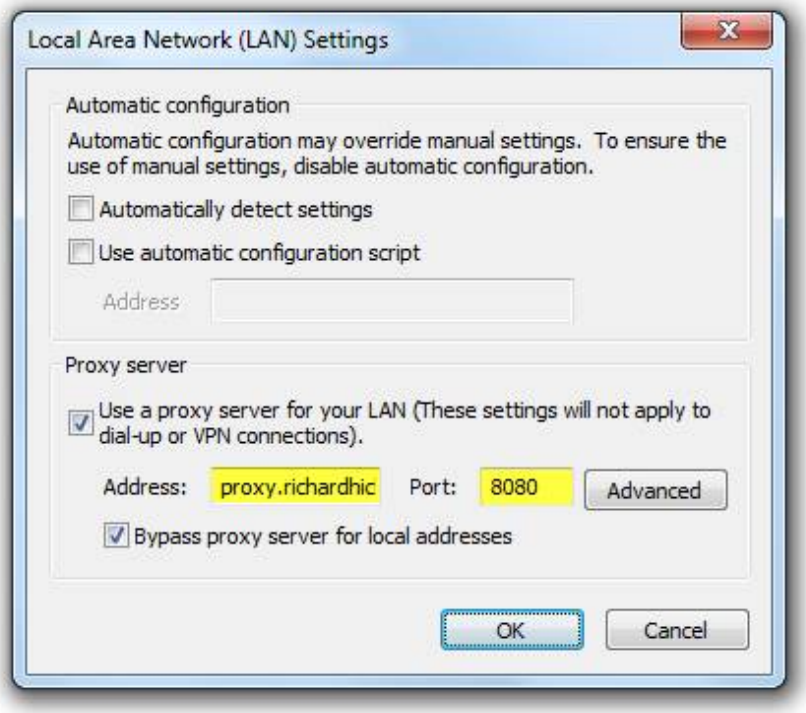



Figure 1

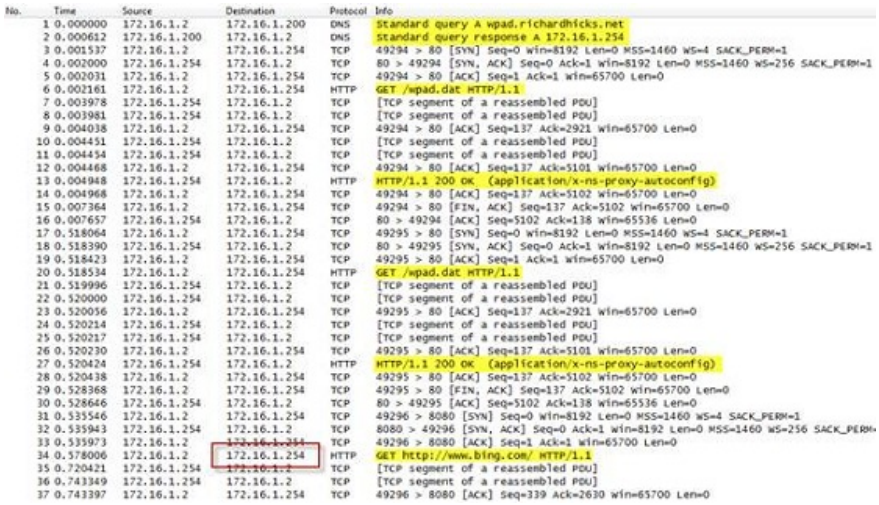
When fully configured, the browser sends a request directly to the specified web proxy server. With this client configuration, we can authenticate users and user groups, reducing the load on the TMG firewall.

# Client configuration and Automatic Web Proxy Discovery

Manually configuring web proxy settings on each client can take a lot of time and effort if the organization has a number of clients. In most cases, you need to use another method to make it more efficient and able to configure automatically. The solution here is to use **Web Proxy Auto Discovery (WPAD).** WPAD is the method where the Web Proxy client will find the proxy server without manual configuration. Most current web browsers are configured to automatically detect the default proxy.


Figure 2

WPAD can be configured using either mechanism - DNS or DHCP. When the Web Proxy client is configured to automatically detect the proxy server, it will try to find the web proxy server first by searching for *options 252* in the settings received from the DHCP server, then by querying DNS to find The host is named WPAD as shown in the network monitoring tool below.



| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | 172.16.1.2 | 172.16.1.200 | DNS | Standard query A wpad.richardhicks.net |
| 2 | 0.000612 | 172.16.1.200 | 172.16.1.2 | DNS | Standard query response A 172.16.1.254 |
| 3 | 0.001537 | 172.16.1.2 | 172.16.1.254 | TCP | 49294 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 4 | 0.002000 | 172.16.1.254 | 172.16.1.2 | TCP | 80 > 49294 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 5 | 0.002031 | 172.16.1.2 | 172.16.1.254 | TCP | 49294 > 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0 |
| 6 | 0.002161 | 172.16.1.2 | 172.16.1.254 | HTTP | GET /wpad.dat HTTP/1.1 |
| 7 | 0.003978 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 8 | 0.003981 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 9 | 0.004038 | 172.16.1.2 | 172.16.1.254 | TCP | 49294 > 80 [ACK] Seq=137 Ack=2921 Win=65700 Len=0 |
| 10 | 0.004451 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 11 | 0.004454 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 12 | 0.004468 | 172.16.1.2 | 172.16.1.254 | TCP | 49294 > 80 [ACK] Seq=137 Ack=5101 Win=65700 Len=0 |
| 13 | 0.004948 | 172.16.1.254 | 172.16.1.2 | HTTP | HTTP/1.1 200 OK (application/x-ns-proxy-autoconfig) |
| 14 | 0.004968 | 172.16.1.2 | 172.16.1.254 | TCP | 49294 > 80 [ACK] Seq=137 Ack=5102 Win=65700 Len=0 |
| 15 | 0.007364 | 172.16.1.2 | 172.16.1.254 | TCP | 49294 > 80 [FIN, ACK] Seq=137 Ack=5102 Win=65700 Len=0 |
| 16 | 0.007657 | 172.16.1.254 | 172.16.1.2 | TCP | 80 > 49294 [ACK] Seq=5102 Ack=138 Win=65536 Len=0 |
| 17 | 0.518064 | 172.16.1.2 | 172.16.1.254 | TCP | 49295 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 18 | 0.518390 | 172.16.1.254 | 172.16.1.2 | TCP | 80 > 49295 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 19 | 0.518423 | 172.16.1.2 | 172.16.1.254 | TCP | 49295 > 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0 |
| 20 | 0.518534 | 172.16.1.2 | 172.16.1.254 | HTTP | GET /wpad.dat HTTP/1.1 |
| 21 | 0.519996 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 22 | 0.520000 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 23 | 0.520056 | 172.16.1.2 | 172.16.1.254 | TCP | 49295 > 80 [ACK] Seq=137 Ack=2921 Win=65700 Len=0 |
| 24 | 0.520214 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 25 | 0.520217 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 26 | 0.520230 | 172.16.1.2 | 172.16.1.254 | TCP | 49295 > 80 [ACK] Seq=137 Ack=5101 Win=65700 Len=0 |
| 27 | 0.520424 | 172.16.1.254 | 172.16.1.2 | HTTP | HTTP/1.1 200 OK (application/x-ns-proxy-autoconfig) |
| 28 | 0.520438 | 172.16.1.2 | 172.16.1.254 | TCP | 49295 > 80 [ACK] Seq=137 Ack=5102 Win=65700 Len=0 |
| 29 | 0.528368 | 172.16.1.2 | 172.16.1.254 | TCP | 49295 > 80 [FIN, ACK] Seq=137 Ack=5102 Win=65700 Len=0 |
| 30 | 0.528646 | 172.16.1.254 | 172.16.1.2 | TCP | 80 > 49295 [ACK] Seq=5102 Ack=138 Win=65536 Len=0 |
| 31 | 0.535546 | 172.16.1.2 | 172.16.1.254 | TCP | 49296 > 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 32 | 0.535943 | 172.16.1.254 | 172.16.1.2 | TCP | 8080 > 49296 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM |
| 33 | 0.535973 | 172.16.1.2 | 172.16.1.254 | TCP | 49296 > 8080 [ACK] Seq=1 Ack=1 Win=65700 Len=0 |
| 34 | 0.578006 | 172.16.1.2 | 172.16.1.254 | HTTP | GET http://www.bing.com/ HTTP/1.1 |
| 35 | 0.720421 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 36 | 0.743349 | 172.16.1.254 | 172.16.1.2 | TCP | [TCP segment of a reassembled PDU] |
| 37 | 0.743397 | 172.16.1.2 | 172.16.1.254 | TCP | 49296 > 8080 [ACK] Seq=339 Ack=2630 Win=65700 Len=0 |

Figure 3

When the client finds the proxy server, it will connect and retrieve the automatic configuration script, a file called WPAD.DAT, from the TMG firewall at the IP address resolved by WPAD. This automatic configuration script will have information about the proxy servers configured and how to handle the request. The information contained in this scenario is dynamically built from the web proxy settings and network configuration set in the TMG management console. The configuration script does not reside on the TMG firewall file system. It is only stored in memory and dynamically upgraded whenever an administrator makes changes to the TMG firewall configuration.

## Activate Auto Discovery

To enable automatic proxy search mode, open the TMG management console, select the **Web Access Policy** button in the interface tree, then click the **Configure Web Proxy link** in the task pane.


Figure 4

Select the **Auto Discovery** tab and check the checkbox next to **Publish automatic discovery information for this network** . If you plan to use DNS for WPAD, you must leave the default port at 80. This default port may be changed if you use DHCP for WPAD.

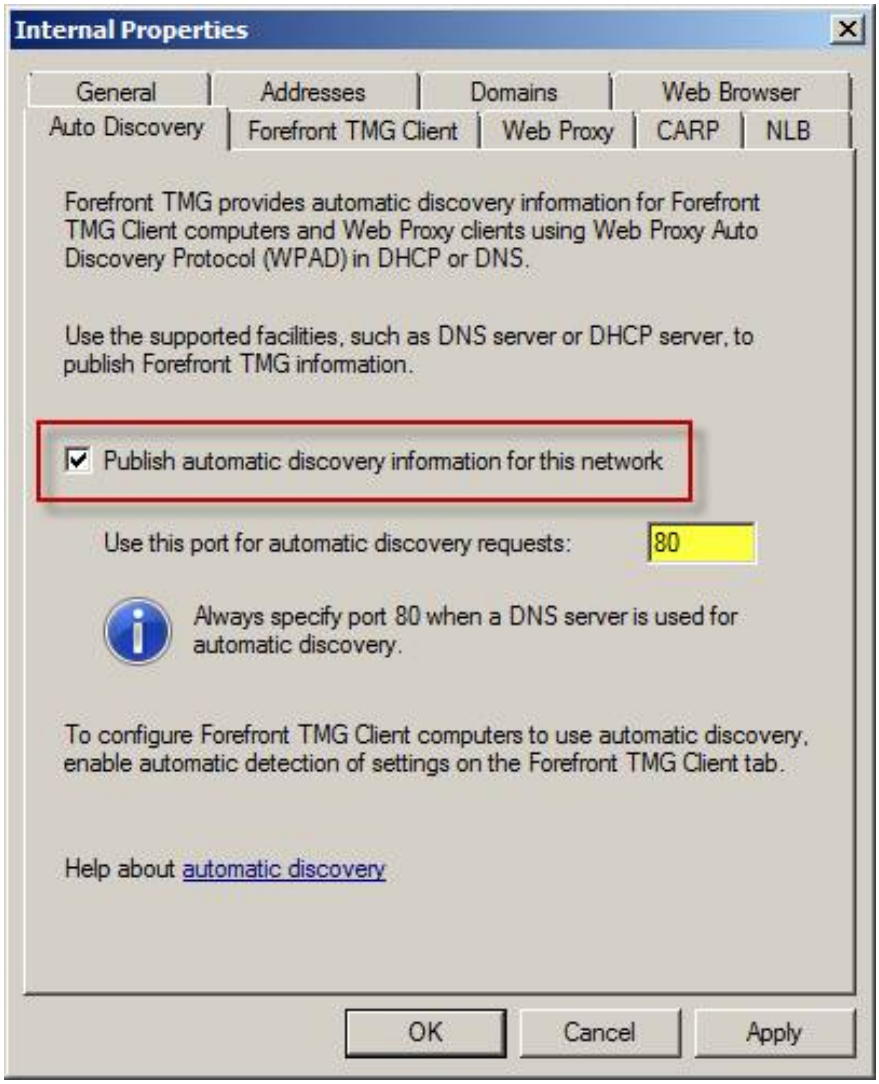



Figure 5

---

# WPAD with DNS

Using DNS for WPAD is the simplest automatic detection option for Web Proxy clients. On the DNS server side, create an A resource record named WPAD that points to the IP address of your TMG firewall's internal network interface. If there is a firewall array that serves as a web proxy server, you can create a CNAME record named WPAD that points to resource records A for each array, or you can create multiple A resource records to resolve the address. Internal IP only of each array.

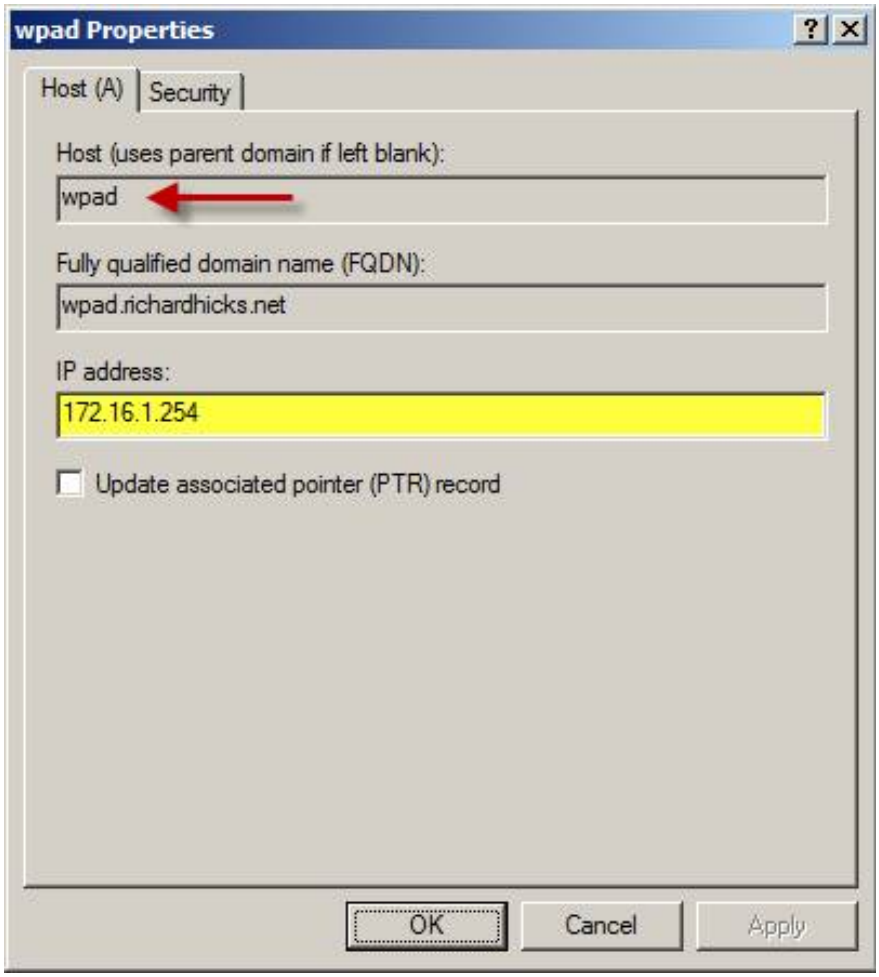



Figure 6

In most cases, the DNS server will not respond to queries about WPAD records by default. This is a security feature built into Windows Server 2008 and 2008 R2 designed to prevent 'man-in-the-middle' attacks, the type of attack that an attacker can configure a fake proxy server on the network. and secretly register WPAD names with dynamic DNS or other techniques. This feature is also enabled in Windows Server 2003 DNS servers installed with MS09-008 upgrade.

To allow a Windows Server 2008 or 2008 R2 DNS server to respond to WPAD queries, open a command prompt on the DNS server and enter the following command:

*dnscmd / config / globalqueryblocklist isatap*

**Note** : If you have configured and deployed DirectAccess, ISATAP may be required in the environment. If so, skip ISATAP from the previous command.

To allow the Windows Server 2003 DNS server to install the security upgrade MS09-009 in response to WPAD queries, edit the following registry key and uninstall WPAD entry:

*HKLMSystemCurrentControlServerServicesDNSParametersGlobalQueryBlockList*

Using DNS for WPAD works well on networks with only one gateway. If there are multiple gateways on the network, DNS may still work but requires a weighted load balancing service (eg F5 Global Traffic Manager).

# WPAD with DHCP

For complex networks with multiple gateways or entry points, DHCP is a better option than DNS. Now the user will be configured to use the proxy server closest to their geographical location.

To configure WPAD using DHCP, open the DHCP management console, right-click **IPv4** , and then select **Set Predefined Options…** .

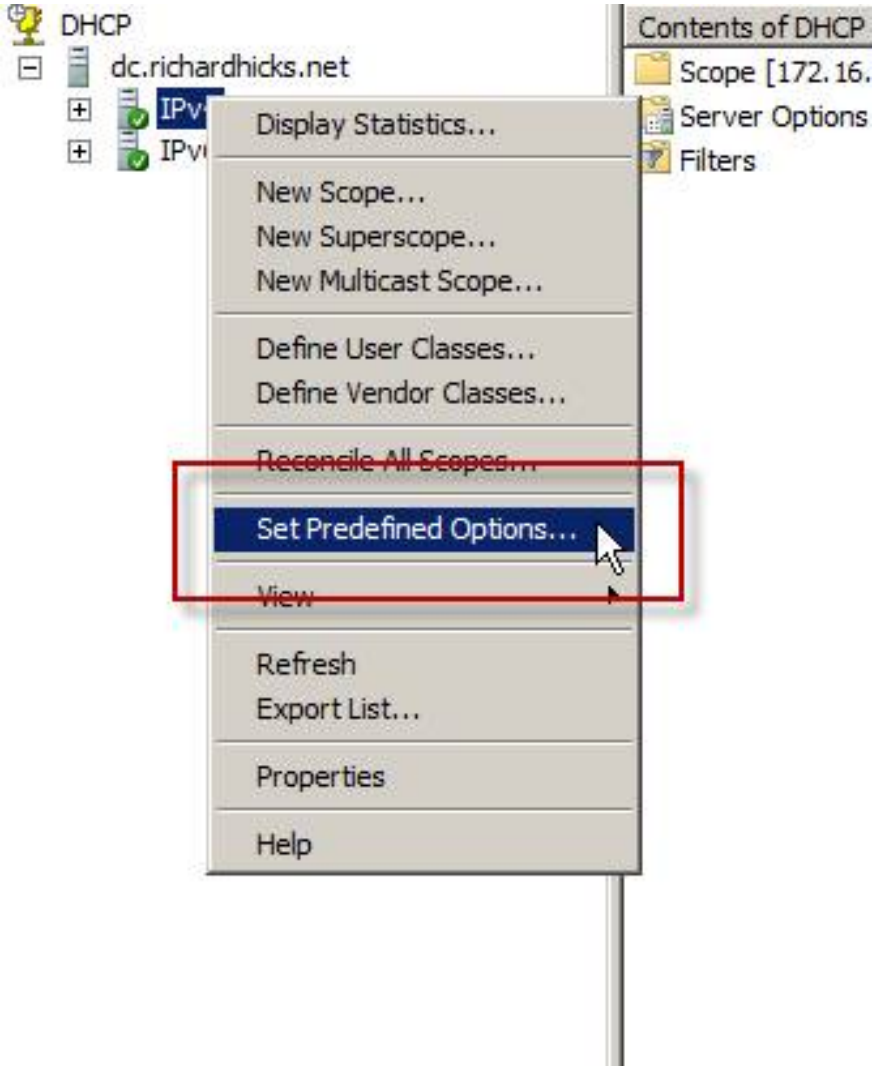



Figure 7

Select the **DHCP Standard Options** layer and select **Add .** Enter **WPAD** name, select **String** data type, specify **252** code and enter **Web Proxy Auto Discovery** description **.**

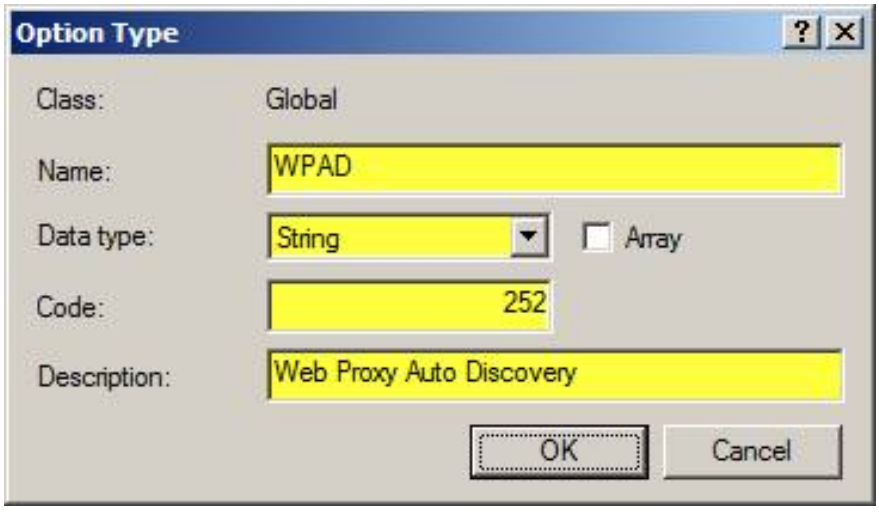



Figure 8

Select a DHCP to configure WPAD, right-click **Scope Options** then select **Configure Options .**

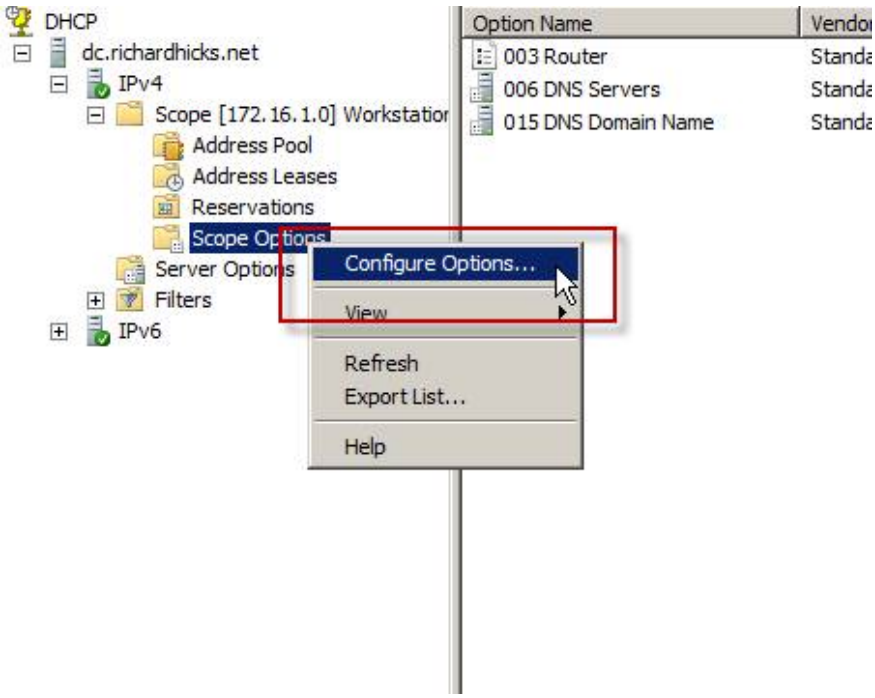



Figure 9

Look at the bottom of the list and select **Option 252 WPAD** . With **String value:** enter the name of the appropriate web proxy server or array of subnets in the following format:

*http:////wpad.dat*

Repeat these steps for each DHCP in the network.

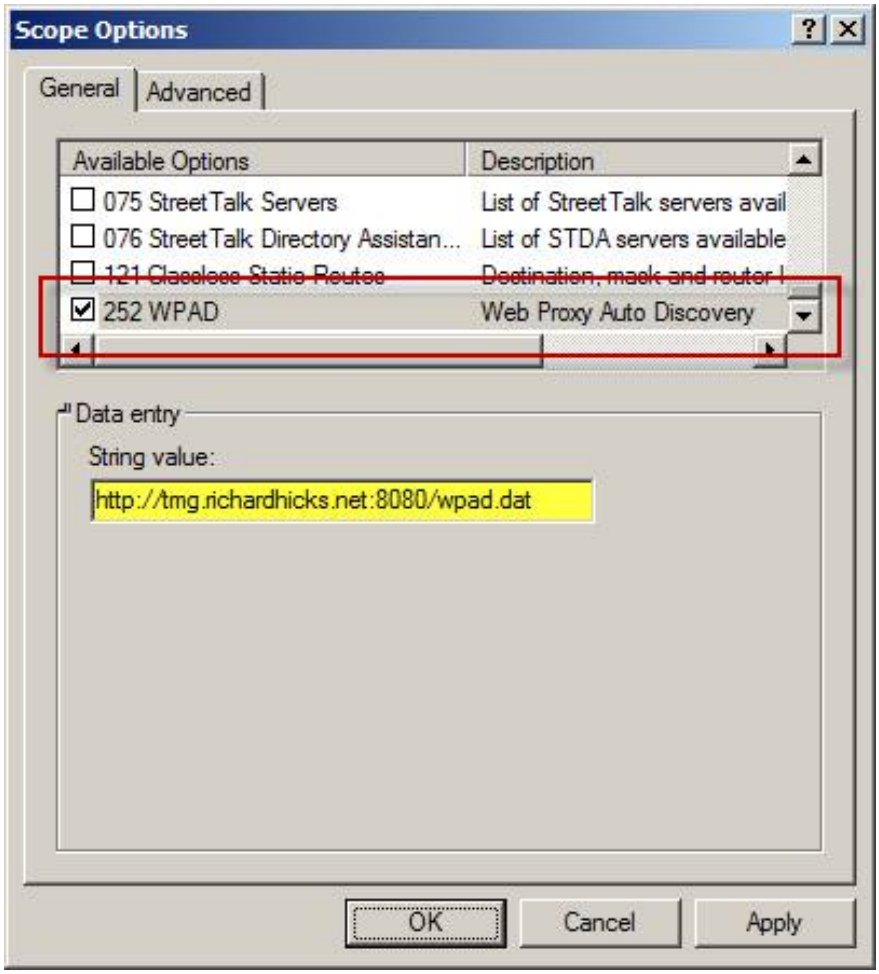



Figure 10

## Automatic configuration of TMG Firewall client

In addition to the above issues, TMG Firewall clients can also use Active Directory (AD) markers. The AD marker automatic configuration option is safer than using DNS or DHCP, but it has many limitations for the TMG Firewall client. Please refer here for more information on configuring Active Directory markers.

## Conclude

Web Proxy clients offer many different security and performance advantages when accessing the TMG web proxy server. However, with changes to browser settings on each desktop that require Internet access, configuring automatically using DNS or DHCP can simplify deployment as well as eliminate the need for manual intervention. For networks that have only one access point, enabling WPAD using DNS is an effective way of configuring Web Proxy clients. For complex networks with multiple access points, enabling WPAD using DHCP will allow administrators to define multiple gateways for different subnets, ensuring that clients use the nearest web proxy server without care about their position.

You finished reading the article "**WPAD configuration in TMG 2010**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com