

# T-ZINE

Trojan Magazine



BY ANTRAX  
ANTRAX@E-ROOT.NET

# NO-IP

Existen una Gran variedad de Troyanos, Explicare la configuración de los mas utilizados en la red.

Los Troyanos utilizados en este tutorial, pueden ser descargados de [www.e-r00t.net](http://www.e-r00t.net) o [www.e-r00t.org](http://www.e-r00t.org) o en cualquiera de las webs que gusten.

Personalmente recomiendo que traten de buscar buenas fuentes para descargarlos, ya que mucha gente lo infecta a propósito y terminaran siendo una victima de ellos.

A la hora de descargar un Troyano traten de que el que lo haya posteado sea una persona de confianza o alguien de alto nivel.

Pasemos a las configuraciones.

Primero que nada, debemos determinar si tenemos Router o modem.

En el caso de modem es muy sencillo, ya que nuestra IP es una sola, y esta no varia. De todas formas, recomiendo crear una NO-IP para cuando necesiten monitorear las victimas desde otro lado que no sea su PC.

En el caso de los Routers evidentemente necesitaran una NO-IP debido a que la IP varia cada vez que encendemos la PC o nos conectamos a Internet.

Para crear una NO-IP entren a [www.no-ip.com](http://www.no-ip.com) y sigan los siguientes pasos:

The screenshot shows the No-IP website interface. At the top left is the No-IP logo with the tagline 'The DNS Service Provider'. Navigation tabs include Home, Download, Services, Support, and Company. A large banner for 'Managed DNS' features the text 'No-IP Plus, The complete managed DNS Solution' and lists benefits like 'Easy to use interface' and 'FREE dynamic DNS update client'. A 'User Login' section on the right contains fields for Username and Password, and a 'Create Account' button highlighted with a red box. Handwritten annotations in Spanish are present: 'click en create account para crear una cuenta' with an arrow pointing to the 'Create Account' button, and 'ANTRAX' written in red.

Seguido a esto, nos llevara a un formulario que debemos llenar para poder registrarnos.

El formulario es algo así:

**Email:**

**Password:**

**Confirm Password:**

 **About You:**

**First Name:**

**Last Name:**

**How did you hear about us?:**

**Zip/Postal Code:**

 **Account Access:**

**Security Question:**

**Your Answer:**

**Birthday:**

Aceptamos los términos y condiciones que están un poco mas abajo y le damos click al botón para crearnos la cuenta.

Seguido a esto, mostrara algo como lo siguiente:

## Confirmation email is on its way!

A [confirmation email](#) has been sent to the email address you provided. The confirmation email will include a link that you must click on to verify your email address. Once your account is confirmed you will be able to login and use our services.

### Preview of email

**From:** No-IP Registration <unmonitored-webmaster@no-ip.com>  
**To:** antrax@e-root.net  
**Subject:** No-IP.com Activation

Please visit our [support section](#) to view our [Getting Started Guide](#) and review our FAQ and knowledge base.

If you have a dynamic IP address and wish to take advantage of our dynamic DNS service you will need to download our dynamic DNS update client (DUC). While you're waiting for that confirmation email to arrive go ahead and download the client. Just select your OS below.

Note: You must confirm your account before you can utilize the No-IP DUC (Dynamic Update Client) software

#### Select your Operating System:



Windows



Mac



Linux/BSD/Unix

Lo que nos dice esto es que fue enviado un mail a nuestro correo para poder activar la cuenta.

Y de acá deben descargar el programa "DUC", lo único que deben hacer es hacer click en la plataforma que estén utilizando. Ya sea Windows, Mac o Linux. Solo hagan click para que comience la descarga.

A nuestro correo llegara algo como lo siguiente:

#### No-IP.com Activation

De: **No-IP Registration** (unmonitored-webmaster@no-ip.com)

Es posible que no conozcas a este remitente. [Marcar como seguro](#) | [Marcar como correo no deseado](#)

Enviado: lunes, 18 de mayo de 2009 18:10:43

Para: antrax@e-root.net

Congratulations, the No-IP account 'antrax@e-root.net' has been created. To activate your account please click on the activation URL below.

No-IP's basic dynamic DNS service is free, made possible by our paid services. If you are interested in dynamic DNS for your own domain please consider our No-IP Plus service. For more information about our paid services visit <http://www.no-ip.com/services> .

To activate your account please click the following URL:

<http://www.no-ip.com/activate?lid=050fe91311cd3873>

**click para activar la  
cuenta e ir al siguiente  
paso**

Remember that you can use our dynamic update client to automatically update your host when your dynamic IP address changes. You can download the client at <http://www.no-ip.com/downloads.php> .

If you have any further questions, please refer to our FAQ at <http://www.no-ip.com/faq.php> and guides section at <http://www.no-ip.com/guides.php>. If you still have questions contact support by opening a trouble ticket at <http://www.no-ip.com/ticket/> .

**ANTRAX**

## Account Confirmed!

Your account has been confirmed and is now ready for use. Please use the login box above to [login](#) to your account.

Please note: Your No-IP Free host names must be updated every 60 days to keep your account active. For an account with no expiration and many other benefits consider [No-IP Enhanced](#) or [No-IP Plus](#)

## ANTRAX

### Limited Time Offer

Sign-up for No-IP Enhanced within the next 4 hours for only \$5.95 (Save \$4)

- Save time because your account won't expire - no need to update your account every 60 days to keep it active.
- Create up to 20 host names
- Choose from over 50 domain names that are less impacted so you can find the name you want.

Just enter coupon code **EN934** upon checkout to take advantage of this offer.

Listo! Ya esta confirmado!

Ahora volvemos a ir a la página principal para loguearnos.

Entramos a [www.no-ip.com](http://www.no-ip.com)

The screenshot shows the No-IP website interface. At the top right, there are navigation links for Home, Contact Us, and Login (the Login link is highlighted with a red box). The main header includes the No-IP logo and the tagline 'The DNS Service Provider'. Below the header are navigation buttons for Home, Download, Services, Support, and Company. The main content area is titled 'Client Login'. On the right side, there is a 'User Login' section with input fields for 'Username' and 'Password', and a 'Login' button. Below these fields are links for 'Create Account' and 'Forgot password?'. Further down, there is an 'Additional Services' section with two options: 'No-IP Enhanced' (with a red shield icon) and 'No-IP Backup DNS' (with a globe icon). In the center of the page, there is a light blue login box. It contains an 'Email' field with the text 'antrax@e-00t.net', a 'Password' field with masked characters, and a large red 'ANTRAX' coupon code. Below the coupon code is a 'Login' button and a link that says 'Forgot your password? No problem, Click Here'. At the bottom of this box, there is a note: 'If you are not currently a registered user of No-IP.com, and would like to be for FREE, register as a new user.'

Una vez que entramos, debemos crear nuestra no-ip

Veremos algo como en la siguiente imagen y debemos hacer click en Add a Host

Need redundancy for your mail server?  
[Click here for more info](#)

24/7 Server Monitoring and Failover  
[Click here for more info](#)

Need Help?  
+ Support Center  
+ Basic Troubleshooting Guide

 **Your No-IP** **ANTRAX****ANTRAX, welcome to your No-IP!**Last Login: 2009-05-18 10:14:17 from IP [\[redacted\]](#)

You have successfully logged into No-IP's member section. To start using No-IP's services select an icon below or choose an item from the navigation above.

**Manage Domains****Add Domain****Refer Friend****Add a Host****Manage Hosts**

Al hacer click nos llevara a una parte como esta:

### Hostname Information

<b>Hostname:</b>	<input type="text" value="w300"/>	<input type="text" value="no-ip.info"/>	
<b>Host Type:</b>	<input checked="" type="radio"/> DNS Host (A) <input type="radio"/> DNS Host (Round Robin) <input type="radio"/> DNS Alias (CNAME) <input type="radio"/> Port 80 Redirect <input type="radio"/> Web Redirect		
<b>IP Address:</b>	<input type="text"/>		
<b>Assign to Group:</b>	<input type="text" value="- No Group -"/>	<a href="#">Configure Groups</a>	
<b>Enable Wildcard:</b>	Wildcards are a Plus / Enhanced feature. <a href="#">Upgrade Now!</a>		

**ANTRAX****Accept Mail for your Domain**

Let No-IP do the dirty work. Setup POP or forwarding for your name.

**Mail Options****MX Record****MX Priority**Enter the name of your external mail exchangers (mx records) as hostnames **not IP addresses**.If you would like a more MX records, please upgrade to [No-IP Plus](#) or [Enhanced](#).[Revert](#)[Create Host](#)

Solo deben modificar lo que esta en el recuadro rojo. Yo puse w300.no-ip.info, pero pueden poner la que quieran.

El resto no toquen nada y hagan click en Create Host.

De todas maneras, les explicare para que es cada cosa para que vean que es una revista completa...

**DNS Host (A):** Este tipo es aquella DNS dinámica que usaremos con nuestro PC en condiciones normales.

**DNS Host (Round Robin):** Este tipo es aquella DNS que usaremos cuando queremos que las peticiones a ese dominio se repartan entre varias IP (servidores con balanceo de carga).

En caso de que elijas esta opción te llevará a una pantalla en la que debes poner un nombre a al primer servidor, con su IP, y lo mismo con el segundo.

**DNS alias (CNAME):** Este tipo es aquella DNS que asocia las peticiones con otra DNS ya existente. Si eliges esta opción te llevará a una pantalla donde incluir esa otra DNS a la que enlazar.

**Port 80 redirect:** Sirve para que si tu ISP te bloquea el puerto 80, configurando tu Apache en un puerto que tenga abierto (veremos como hacer esto en la segunda parte de este tutorial), el sistema redirija a los usuarios que hagan una petición por el puerto 80, que es el default Pag. 19

para las webs al puerto que tu especifiques. Si seleccionas esta opción te llevará a un pantalla en la que debes poner el puerto en el que vas a ejecutar el servicio web.

**Web Redirect:** Finalmente, esta opción permite una redirección como la de cualquier otro servicio de redirección de webs, como pudiera ser

<http://www.dot.tk> o <http://www.cjb.net>.

Seleccionando esta opción, te llevará a una pantalla donde debes poner la web a la que estás redirigiendo y especificar si usa protocolo seguro (https) o no (http).

Una vez creado, verán algo así:



## Manage Hosts



Host w300.no-ip.info created. Update will be applied within 1 minute.

Current Hosts: 1 of 5

Need More Hosts? Enhance Your Account!

[Upgrade Now!](#)

Host	IP/URL	Action
<b>Hosts By Domain</b>		
no-ip.info		
w300.no-ip.info	<b>ANTRAX</b>	<a href="#">Modify</a> <a href="#">Remove</a>

[Add a Host](#)

Ya pueden cerrar la web...

Una vez cerrada, procederemos a instalar el programa que descargamos, el "DUC"

Es de fácil instalación, solo poner todo siguiente y listo...

Al finalizar, veremos algo así:

No-IP DUC

Please enter your e-mail address and password. If you don't have an account? No problem, [click here](#) to sign-up free! Forgot your password? Even better, [click here](#) to have it e-mailed to you!

E-Mail Address

Password

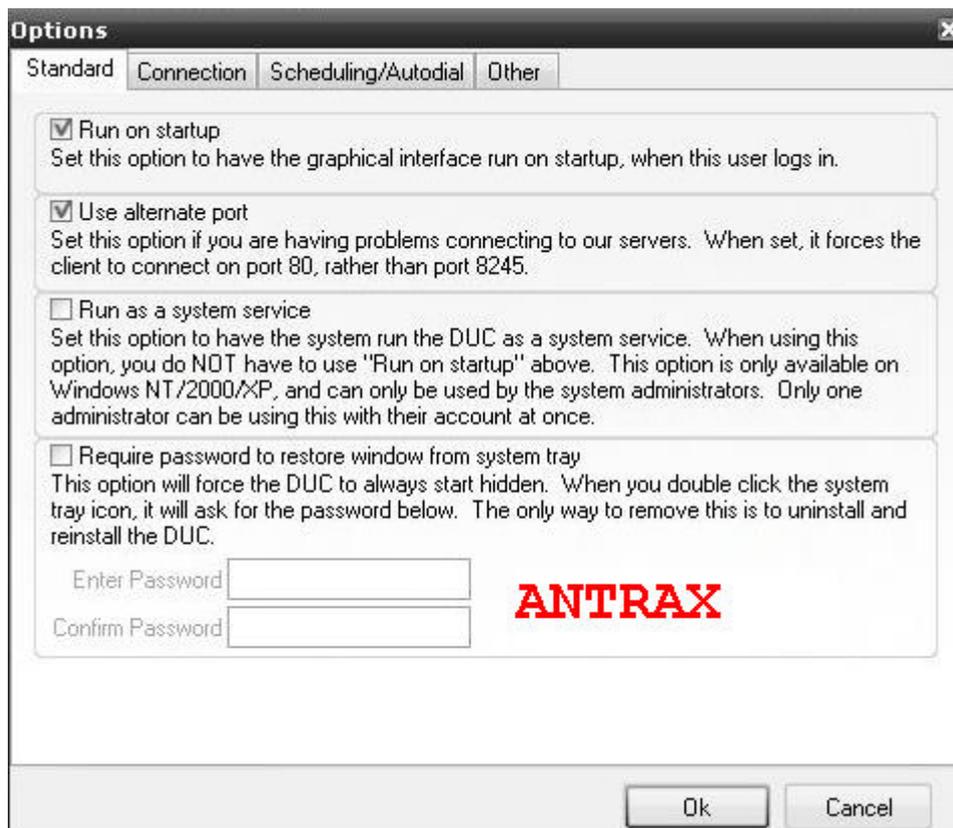
Ponemos el correo y la password del registro. Y le damos a OK.



Marque el cuadrito en rojo por que debe permanecer tildado.

Una vez hecho esto y que la carita quede como en la imagen, quiere decir que todo esta en orden.

En caso de que no funcione, pongan en options y que quede algo así:



En caso de seguir teniendo problemas, puede de que el Firewall este ocasionándolo, como lo puede hacer el antivirus o en pocas ocasiones el Router.