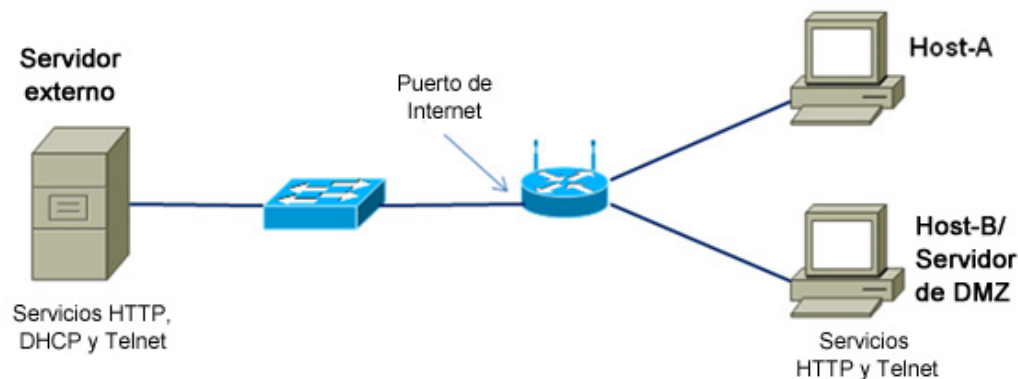


## Práctica de laboratorio 8.4.2 Configuración de políticas de acceso y de valores de DMZ



### Objetivos

- Iniciar la sesión en un dispositivo multifunción y ver los valores de seguridad.
- Configurar políticas de acceso a Internet basadas en una aplicación y una dirección IP.
- Configurar una zona desmilitarizada (DMZ) para un servidor de acceso abierto con una dirección IP estática.
- Configurar el reenvío de puertos para limitar la accesibilidad de los puertos a HTTP solamente.
- Utilizar las funciones de ayuda del dispositivo Linksys WRT300N.

### Información básica/Preparación

Este laboratorio imparte instrucciones para configurar valores de seguridad para el dispositivo Linksys WRT300N. Este dispositivo proporciona un firewall basado en software para proteger a los clientes internos de redes locales contra ataques provenientes de hosts externos. Las conexiones que se realizan desde hosts internos hasta destinos externos se pueden filtrar en función de la dirección IP, el sitio Web de destino y la aplicación. Además es posible configurar el Linksys para crear una zona desmilitarizada (DMZ) y controlar el acceso a un servidor desde hosts externos. Este laboratorio se realiza en equipos de dos, y dos equipos pueden trabajar en conjunto para probar uno al otro las restricciones de acceso y la funcionalidad de la DMZ. El laboratorio está dividido en dos partes:

- Parte 1: Configuración de políticas de acceso
- Parte 2: Configuración de valores de DMZ

Se necesitan los siguientes recursos:

- Linksys WRT300N u otro dispositivo multifunción con la configuración por defecto.
- Identificación y contraseña del usuario para el dispositivo Linksys, en caso de que sean distintas de las por defecto.
- Computadora con Windows XP Professional para acceder a la GUI de Linksys.
- Computadora interna que actúe como servidor en la DMZ con servidores HTTP y Telnet instalados (servidor preconfigurado o del CD de Discovery Live).

- Servidor externo que represente al proveedor de servicios de Internet (ISP, *Internet Service provider*) y con Internet (con servidores de DHCP, HTTP y Telnet preconfigurados) (el servidor actual con servicios instalados o el servidor del CD de Discovery Live).
- Cables necesarios para conectar los hosts de la computadora, Linksys WRT300N o el dispositivo multifunción y los switches.

## Parte 1: Configuración de políticas de acceso

### Paso 1: Construya la red y configure los hosts

- Conecte los equipos host a los puertos del switch del dispositivo multifunción, como se muestra en el diagrama de topología. El host A es la consola y se utiliza para acceder a la GUI de Linksys. El host B es, en principio, una máquina de prueba, pero luego se convierte en el servidor DMZ.
- Configure los valores de IP para los dos hosts utilizando las conexiones de red de Windows XP y las propiedades de TCP/IP. Verifique que el host A esté configurado como cliente de protocolo de configuración dinámica de host (DHCP, *Dynamic Host Configuration Protocol*). Asigne una dirección IP estática al host B en el rango de 192.168.1.x con una máscara de subred 255.255.255.0. La gateway por defecto debe ser la dirección de red local interna del dispositivo Linksys.

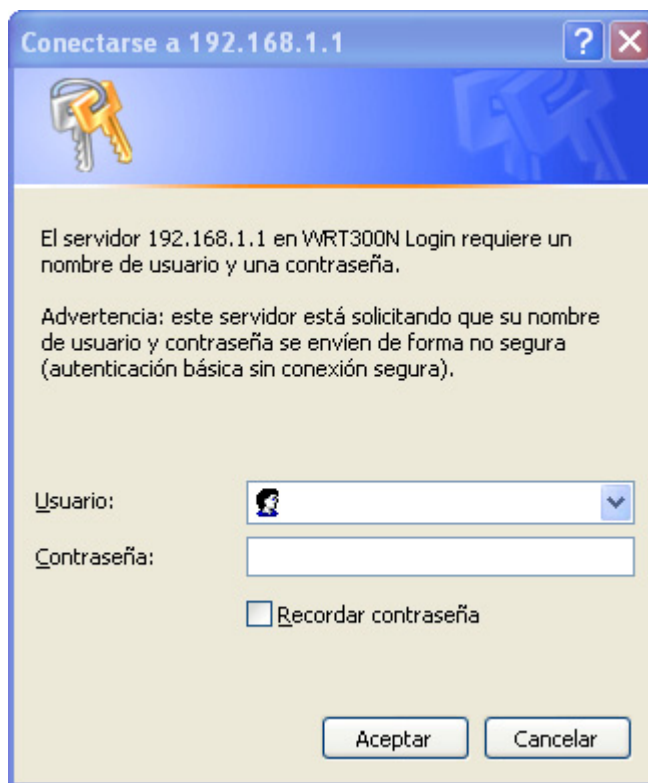
**NOTA:** Si el host B ya es un cliente de DHCP, puede reservar su dirección actual y hacerla estática utilizando la característica de Reserva de DHCP en la pantalla de configuración básica del dispositivo Linksys.

- Utilice el comando *ipconfig* para ver la dirección IP, la máscara de subred y la gateway por defecto para el host A y el host B, y regístrelos en la tabla. Pregúntele al instructor la dirección IP y la máscara de subred del servidor externo y regístrelas en la tabla.

Host	Dirección IP	Máscara de subred	Gateway por defecto
Host-A			
Host-B/ Servidor DMZ			
Servidor externo			

**Paso 2: Inicie la sesión en la interfaz de usuario**

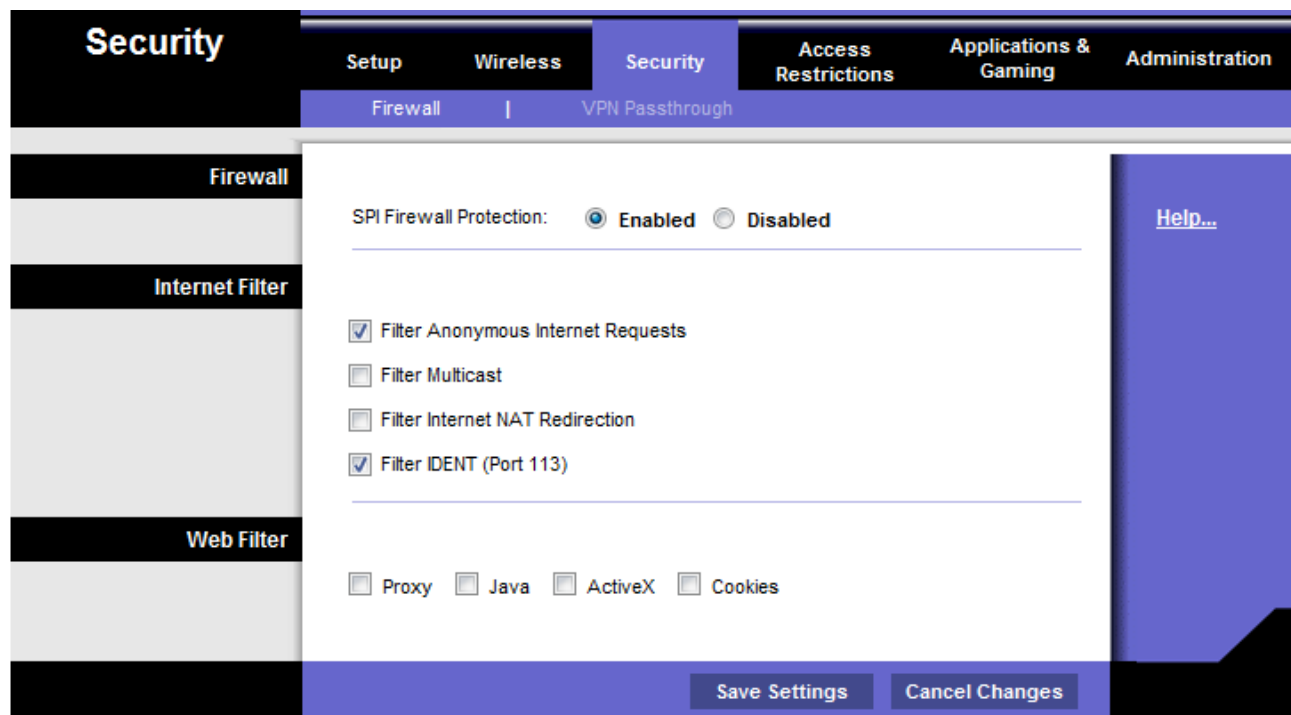
- a. Para acceder a la GUI Web del dispositivo Linksys o del dispositivo multifunción abra un explorador y escriba la dirección IP interna por defecto para el dispositivo, que normalmente es 192.168.1.1.
- b. Inicie la sesión con la ID de usuario y la contraseña por defecto o consulte al instructor si son diferentes.



- c. El dispositivo multifunción deberá estar configurado para poder obtener una dirección IP del servidor de DHCP externo. La pantalla por defecto después de iniciar la sesión en el dispositivo multifunción es Setup > Basic Setup (Configuración > Configuración básica). ¿Cuál es el tipo de conexión a Internet?
- d. ¿Cuáles son la dirección IP y la máscara de subred (internas) del router por defecto para el dispositivo multifunción?
- e. Verifique que el dispositivo multifunción haya recibido una dirección IP externa del servidor de DHCP haciendo clic en la ficha Status > Router (Estado > Router).
- f. ¿Cuáles son la dirección IP y la máscara de subred externas asignadas al dispositivo multifunción?

**Paso 3: Vea los valores del firewall del dispositivo multifunción**

- a. El dispositivo Linksys WRT300N proporciona un firewall básico que utiliza la traducción de direcciones de red (NAT). También proporciona la funcionalidad de firewall adicional utilizando la inspección de paquetes con estado (SPI, *Stateful Packet Inspection*) para detectar y bloquear el tráfico no solicitado de Internet.
  - b. En la pantalla principal haga clic en la ficha **Security** (Seguridad) para ver el estado de los campos **Firewall** y **Internet Filter** (Filtro de Internet). ¿Cuál es el estado de la protección del firewall SPI?
  - c. ¿Qué casillas de verificación del campo **Internet Filter** (Filtro de Internet) están seleccionadas?
  - d. Haga clic en **Help** (Ayuda) para obtener más información sobre estos valores. ¿Qué beneficios brinda la opción “Filter IDENT” (Filtrar IDENT)?
- 



#### Paso 4: Configure las restricciones de acceso a Internet basadas en la dirección IP

En el laboratorio 7.3.5, aprendió a usar las características de seguridad inalámbrica para controlar las computadoras cliente inalámbricas que pueden acceder al dispositivo multifunción en función de la dirección MAC. Esto impide que computadoras externas no autorizadas se conecten al punto de acceso inalámbrico y obtengan acceso a la red local interna y a Internet.

El dispositivo multifunción también puede controlar qué usuarios internos acceden a Internet desde la red local. Es posible crear una política de acceso a Internet para denegar o permitir el acceso de computadoras internas específicas a Internet según la dirección IP, la dirección MAC u otros criterios.

- En la pantalla principal del dispositivo multifunción haga clic en la ficha **Access Restrictions** (Restricciones de acceso) para definir la **Access Policy 1** (Política de acceso 1).
- Escriba **Block-IP** como nombre de la política. Seleccione **Enabled** (Habilitada) para habilitar la política. A continuación seleccione **Deny** (Denegar) para impedir que una dirección IP acceda a Internet.

The screenshot shows the 'Access Restrictions' configuration page. The left sidebar has a menu with 'Internet Access Policy' selected. The main area shows the configuration for 'Access Policy: 1'. The 'Enter Policy Name' field contains 'Block-IP'. The 'Status' is set to 'Enabled'. Below this, there is an 'Edit List' button and a note '(This Policy applies only to PCs on the List.)'. The 'Access Restriction' is set to 'Deny' with the description 'Internet access during selected days and hours.' The 'Days' section has 'Everyday' selected. The 'Times' section has '24 Hours' selected.

- Haga clic en el botón **Edit List** (Editar lista) e introduzca la dirección IP del host B. Haga clic en **Save Settings** (Guardar configuración) y luego en **Close** (Cerrar). Haga clic en **Save Settings** (Guardar configuración) para guardar la política de acceso a Internet 1: Block IP.
- Pruebe la política intentando acceder al servidor Web externo desde el host B. Abra un explorador y escriba la dirección IP del servidor externo en el área de direcciones. ¿Puede acceder al servidor?
- Cambie el estado de la política Block-IP a **Disabled** (Deshabilitada) y haga clic en **Save Settings** (Guardar configuración). ¿Ahora puede acceder al servidor?
- ¿De qué otras maneras es posible utilizar las políticas de acceso para bloquear el acceso a Internet?

## Paso 5: Configure una política de acceso a Internet según una aplicación

Es posible crear una política de acceso a Internet para bloquear computadoras específicas para que no puedan utilizar ciertas aplicaciones o protocolos de Internet.

- En la pantalla principal de la GUI de Linksys haga clic en la ficha Access Restrictions (Restricciones de acceso) para definir la política de acceso a Internet.
- Escriba Block-Telnet como nombre de la política. Seleccione Enabled (Habilitada) para habilitar la política. A continuación haga clic en Allow (Permitir) para permitir el acceso a Internet desde una dirección IP específica, siempre que no sea una de las aplicaciones bloqueada.
- Haga clic en el botón Edit List (Editar lista) e introduzca la dirección IP del host B. Haga clic en Save Settings (Guardar configuración) y luego en Close (Cerrar).

¿Qué otras aplicaciones y protocolos de Internet se pueden bloquear?

- Seleccione la aplicación **Telnet** de la lista de aplicaciones que se pueden bloquear y haga clic en la flecha doble hacia la derecha para agregarla a la lista de bloqueos, **Blocked List**. Haga clic en **Save Settings** (Guardar configuración).

Website Blocking by URL Address

Website Blocking by Keyword

Blocked Applications

URL 1:  URL 3:

URL 2:  URL 4:

Keyword 1:  Keyword 3:

Keyword 2:  Keyword 4:

**Note:** only three applications can be blocked per policy.

Applications		Blocked List
DNS (53 - 53)	<input type="button" value=""/> >>> <input type="button" value=""/> <<<	Telnet (23 - 23)
Ping (0 - 0)		
HTTP (80 - 80)		
HTTPS (443 - 443)		
FTP (21 - 21)		
POP3 (110 - 110)		
IMAP (143 - 143)		

- Pruebe la política abriendo un símbolo del sistema; para hacerlo seleccione **Inicio > Todos los programas > Accesorios > Símbolo del sistema**.
- Haga ping en la dirección IP del servidor externo desde el host B utilizando el **comando ping**.  
¿Puede hacer ping del servidor? \_\_\_\_\_
- Envíe un comando Telnet a la dirección IP del servidor externo desde el host B utilizando el comando Telnet A.B.C.D (donde A.B.C.D corresponde a la dirección IP del servidor).  
¿Puede enviar el comando Telnet al servidor? \_\_\_\_\_

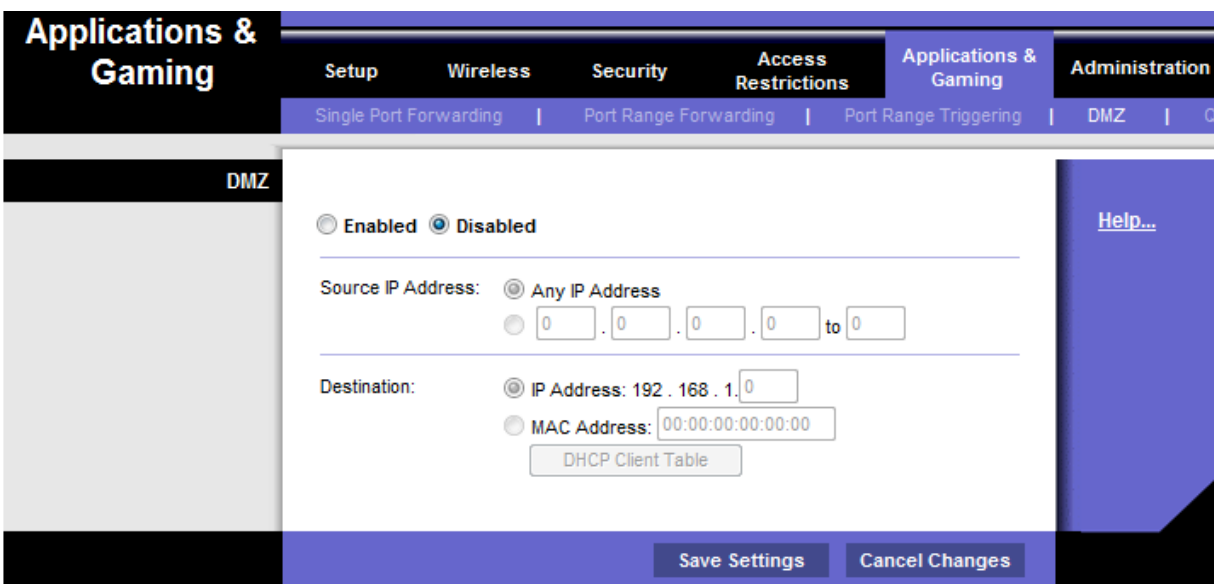
**NOTA:** Si no va a realizar la parte 2 del laboratorio en este momento y otros van a usar el equipo después de usted, diríjase al paso 3 de la parte 2 y restaure el dispositivo multifunción a sus valores por defecto.

## Parte 2: Configuración de una DMZ en el dispositivo multifunción

### Paso 1: Configure una DMZ simple

A veces es necesario permitir el acceso a una computadora desde Internet mientras se siguen protegiendo las otras computadoras de la red local interna. Para lograrlo se puede establecer una zona desmilitarizada (DMZ), que permite el acceso abierto a cualquier puerto y servicio que se ejecute en el servidor especificado. Toda solicitud de servicio a la dirección externa del dispositivo multifunción se redireccionará al servidor especificado.

- El host B actuará como servidor DMZ y deberá tener servidores HTTP y Telnet instalados. Verifique que el host B tenga una dirección IP estática o, si el host B es un cliente de DHCP, podrá reservar su dirección actual y hacerla estática mediante la característica **DHCP Reservation** (Reserva de DHCP) que se encuentra en la pantalla **Basic Setup** (Configuración básica) del dispositivo Linksys.
- En la pantalla principal de la GUI haga clic en la ficha **Applications & Gaming** (Aplicaciones y juegos) y a continuación haga clic en **DMZ**.
- Haga clic en **Help** (Ayuda) para obtener más información sobre la DMZ. ¿Qué otras razones podrían llevarlo a configurar un host en la DMZ?



- La característica de DMZ está desactivada por defecto. Seleccione **Enabled** (Habilitada) para habilitar la DMZ. Deje **Source IP Address** (Dirección IP de origen) seleccionada como **Any IP Address** (Cualquier dirección IP) y escriba la dirección IP del host B en **Destination IP Address** (Dirección IP de destino). Haga clic en **Save Settings** (Guardar configuración) y a continuación en **Continue** (Continuar) cuando aparezca la consulta.
- Pruebe el acceso básico al servidor DMZ haciendo ping desde el servidor externo a la dirección externa del dispositivo multifunción. Utilice el comando **ping -a** para verificar que lo que responde es el servidor DMZ y no el dispositivo multifunción. ¿Puede hacer ping del servidor DMZ?

- f. Pruebe el acceso HTTP al servidor DMZ abriendo un explorador en el servidor externo y seleccionando la dirección IP externa del dispositivo multifunción. Intente lo mismo desde un explorador del host A al host B utilizando las direcciones internas.

¿Puede acceder a la página Web? \_\_\_\_\_

- g. Pruebe el acceso Telnet abriendo un símbolo del sistema según se describe en el paso 5. Envíe el comando Telnet a la dirección IP externa del dispositivo multifunción utilizando el comando **telnet A.B.C.D** (donde A.B.C.D corresponde a la dirección externa del dispositivo multifunción).

¿Puede enviar el comando Telnet al servidor? \_\_\_\_\_

## Paso 2: Configure un host con un reenvío de puerto único

La configuración básica de hosting de DMZ del paso 6 permite el acceso abierto a todos los puertos y servicios que se ejecutan en el servidor, por ejemplo: HTTP, FTP y Telnet. Si un host se va a utilizar para una función en particular, como servicios Web o FTP, el acceso debe estar limitado al tipo de servicios prestados. Esto se logra mediante el reenvío de puerto único, y es más seguro que la configuración básica de DMZ, ya que sólo abre los puertos necesarios. Antes de completar este paso desactive la configuración de DMZ para el paso 1.

El host B corresponde al servidor al que se reenvían los puertos pero el acceso está limitado sólo al protocolo HTTP (Web).

- En la pantalla principal haga clic en la ficha **Applications & Gaming** (Aplicaciones y juegos) y a continuación haga clic en **Single Port Forwarding** (Reenvío de puerto único) para especificar las aplicaciones y los números de puerto.
- Haga clic en el menú desplegable para seleccionar la primera entrada debajo de **Application Name** (Nombre de la aplicación) y seleccione **HTTP**. Éste es el puerto 80 del protocolo del servidor Web.
- En el primer campo **To IP Address** (A dirección IP) escriba la dirección IP del host B y seleccione **Enabled** (Habilitada). Haga clic en **Save Settings** (Guardar configuración).

Externet Port	Internet Port	Protocol	To IP Address	Enabled
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
0	0	Both	192 . 168 . 1 . 0	<input type="checkbox"/>
0	0	Both	192 . 168 . 1 . 0	<input type="checkbox"/>

- d. Pruebe el acceso HTTP al host DMZ abriendo un explorador en el servidor externo y seleccionando la dirección externa del dispositivo. Intente lo mismo desde un explorador del host A al host B.

¿Puede acceder a la página Web? \_\_\_\_\_



- e. Pruebe el acceso Telnet abriendo un símbolo del sistema según se describe en el paso 5. Intente enviar un comando Telnet a la dirección IP externa del dispositivo multifunción utilizando el comando **telnet A.B.C.D** (donde A.B.C.D corresponde a la dirección IP externa del dispositivo multifunción).

¿Puede enviar el comando Telnet al servidor? \_\_\_\_\_

### Paso 3: Restaure el dispositivo multifunción a su configuración por defecto

- a. Para restaurar el dispositivo Linksys a la configuración por defecto de fábrica haga clic en la ficha **Administration > Factory Defaults** (Administración > Configuración por defecto de fábrica).
- b. Haga clic en el botón **Restore Factory Defaults** (Restaurar configuración por defecto de fábrica). Se perderán todas las entradas o los cambios realizados en la configuración.

**NOTA:** La configuración actual se puede guardar y restaurar más adelante en la ficha **Administration > Management** (Administración > Gestión) y con los botones **Backup Configuration** (Copia de seguridad de configuración) y **Restore Configuration** (Restaurar configuración).

