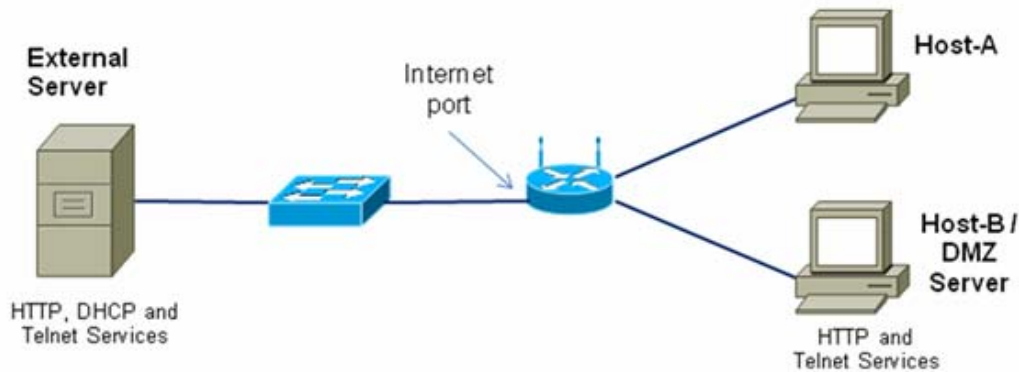


Lab 8.4.2 Configuring Access Policies and DMZ Settings



Objectives

- Log in to a multi-function device and view security settings.
- Set up Internet access policies based on IP address and application.
- Set up a DMZ for an open access server with a static IP address.
- Set up port forwarding to limit port accessibility to only HTTP.
- Use the Linksys WRT300N Help features.

Background / Preparation

This lab provides instructions for configuring security settings for the Linksys WRT300N. The Linksys provides a software-based firewall to protect internal, local-network clients from attack by external hosts. Connections from internal hosts to external destinations can be filtered based on the IP address, destination website, and application. The Linksys can also be configured to create a demilitarized zone (DMZ) to control access to a server from external hosts. This lab is done in teams of two, and two teams can work together to test each other's access restrictions and DMZ functionality. It is divided into 2 parts:

- Part 1 – Configuring access policies
- Part 2 – Configuring DMZ settings

The following resources are required:

- Linksys WRT300N or other multi-function device with the default configuration
- User ID and password for the Linksys device if different than the default
- Computer running Windows XP Professional to access the Linksys GUI
- Internal PC to act as a server in the DMZ with HTTP and Telnet servers installed (preconfigured or Discovery Live CD server)
- External server to represent the ISP and Internet (with preconfigured DHCP, HTTP, and Telnet servers running (real server with services installed or Discovery Live CD server)
- Cabling to connect the PC hosts, Linksys WRT300N or multi-function device, and switches

Part 1 – Configuring access policies

Step 1: Build the network and configure the hosts

- a. Connect the host computers to switch ports on the multi-function device as shown in the topology diagram. Host-A is the console and is used to access the Linksys GUI. Host-B is initially a test machine but later becomes the DMZ server.
- b. Configure the IP settings for both hosts using Windows XP Network Connections and TCP/IP properties. Verify that Host-A is configured as a DHCP client. Assign a static IP address to Host-B in the 192.168.1.x range with a subnet mask of 255.255.255.0. The default gateway should be the internal local network address of the Linksys device.

NOTE: If Host-B is already a DHCP client, you can reserve its current address and make it static using the DHCP Reservation feature on the Linksys Basic Setup screen.

- c. Use the *ipconfig* command to display the IP address, subnet mask, and default gateway for Host-A and Host-B and record them in the table. Obtain the IP address and subnet mask of the external server from the instructor and record it in the table.

Host	IP Address	Subnet Mask	Default Gateway
Host-A			
Host-B / DMZ Server			
External Server			

Step 2: Log in to the user interface

- a. To access the Linksys or multi-function device web-based GUI, open a browser and enter the default internal IP address for the device, normally 192.168.1.1.
- b. Log in using the default user ID and password, or check with the instructor if they are different.



- c. The multi-function device should be configured to obtain an IP address from the external DHCP server. The default screen after logging in to the multi-function device is Setup > Basic Setup. What is the Internet connection type?

- d. What is the default router (internal) IP address and subnet mask for the multi-function device?

- e. Verify that the multi-function device has received an external IP address from the DHCP server by clicking the Status > Router tab.
- f. What is the external IP address and subnet mask assigned to the multi-function device?

Step 3: View multi-function device firewall settings

- The Linksys WRT300N provides a basic firewall that uses Network Address Translation (NAT). In addition, it provides additional firewall functionality using Stateful Packet Inspection (SPI) to detect and block unsolicited traffic from the Internet.
- From the main screen, click the **Security** tab to view the **Firewall** and **Internet Filter** status. What is the status of SPI Firewall protection? _____
- Which **Internet Filter** checkboxes are selected? _____
- Click **Help** to learn more about these settings. What benefits does filtering IDENT provide? _____

Security

Setup | Wireless | **Security** | Access Restrictions | Applications & Gaming | Administration

Firewall | VPN Passthrough

Firewall

SPI Firewall Protection: ☒ Enabled ☐ Disabled

☒ Filter Anonymous Internet Requests

☐ Filter Multicast

☐ Filter Internet NAT Redirection

☒ Filter IDENT (Port 113)

☐ Proxy ☐ Java ☐ ActiveX ☐ Cookies

[Help...](#)

Save Settings **Cancel Changes**

Step 4: Set up Internet access restrictions based on IP address

In Lab 7.3.5, you saw that wireless security features can be used to control which wireless client computers can access the multi-function device, based on their MAC address. This prevents unauthorized external computers from connecting to the wireless access point (AP) and gaining access to the internal local network and the Internet.

The multi-function device can also control which internal users can get out to the Internet from the local network. You can create an Internet access policy to deny or allow specific internal computers access to the Internet based on the IP address, MAC address, and other criteria.

- From the main multi-function device screen, click the **Access Restrictions** tab to define **Access Policy 1**.
- Enter **Block-IP** as the policy name. Select **Enabled** to enable the policy, and then select **Deny** to prevent Internet access from a specified IP address.

The screenshot shows the 'Access Restrictions' configuration page. The left sidebar has a menu with 'Internet Access Policy' selected. The main content area has a top navigation bar with 'Setup', 'Wireless', 'Security', 'Access Restrictions', and 'Applications & Gaming'. Below this is a sub-header 'Internet Access Policy'. The configuration form includes: 'Access Policy:' with a dropdown showing '1 ()' and buttons 'Delete This Entry' and 'Summary'; 'Enter Policy Name:' with a text box containing 'Block-IP'; 'Status:' with radio buttons for 'Enabled' (selected) and 'Disabled'; an 'Edit List' button and a note '(This Policy applies only to PCs on the List.)'; 'Access Restriction' with radio buttons for 'Deny' (selected) and 'Allow', with a description 'Internet access during selected days and hours.'; 'Days:' with checkboxes for 'Everyday' (checked), 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'; and 'Times:' with radio buttons for '24 Hours' (selected) and a time range selector showing '12 AM : 00 to 12 AM : 00'.

- Click the **Edit List** button and enter the IP address of Host-B. Click **Save Settings** and then **Close**. Click **Save Settings** to save Internet Access Policy 1 – Block IP.
- Test the policy by attempting to access the external web server from Host-B. Open a browser and enter the IP address of the external server in the address area. Are you able to access the server?
- Change the status of the Block-IP Policy to **Disabled** and click **Save Settings**. Are you able to access the server now?
- What other ways can access policies be used to block Internet access?

Step 5: Set up an Internet access policy based on an application

You can create an Internet access policy to block specific computers from using certain Internet applications or protocols on the Internet.

- From the main Linksys GUI screen, click the Access Restrictions tab to define an Internet Access Policy.
- Enter Block-Telnet as the policy name. Select Enabled to enable the policy, and then click Allow to permit Internet access from a specified IP address as long as it is not one of the applications that is blocked.
- Click the Edit List button and enter the IP address of Host-B. Click Save Settings and then Close.

What other Internet applications and protocols can be blocked?

- Select the **Telnet** application from the list of applications that can be blocked and then click the double right arrow to add it to the **Blocked List**. Click **Save Settings**.

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)	>> <<	Telnet (23 - 23)
Ping (0 - 0)		
HTTP (80 - 80)		
HTTPS (443 - 443)		
FTP (21 - 21)		
POP3 (110 - 110)		
IMAP (143 - 143)		

- Test the policy by opening a command prompt using **Start > All Programs > Accessories > Command Prompt**.
- Ping the IP address of the external server from Host-B using the **ping** command.
Are you able to ping the server? _____
- Telnet to the IP address of the external server from Host-B using the command **telnet A.B.C.D** (where A.B.C.D is the IP address of the server).
Are you able to telnet to the server? _____

NOTE: If you are not going to perform lab Part 2 at this time and others will be using the equipment after you, skip to Step 3 of Part 2 and restore the multi-function device to its default settings.

Part 2 – Configuring a DMZ on the multi-function device

Step 1: Set up a simple DMZ

It is sometimes necessary to allow access to a computer from the Internet while still protecting other internal local network computers. To accomplish this, you can set up a demilitarized zone (DMZ) that allows open access to any ports and services running on the specified server. Any requests made for services to the outside address of the multi-function device will be redirected to the server specified.

- Host-B will act as the DMZ server and should be running HTTP and Telnet servers. Verify the Host-B has a static IP address or, if Host-B is a DHCP client, you can reserve its current address and make it static using the **DHCP Reservation** feature on the Linksys device **Basic Setup** screen.
- From the main Linksys GUI screen, click the **Applications & Gaming** tab then click **DMZ**.
- Click **Help** to learn more about the DMZ. For what other reasons might you want to set up a host in the DMZ?

The screenshot shows the Linksys web interface for configuring DMZ. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', and 'Administration'. Under 'Applications & Gaming', there are links for 'Single Port Forwarding', 'Port Range Forwarding', 'Port Range Triggering', 'DMZ', and 'QoS'. The 'DMZ' section is active, showing a 'DMZ' tab. The 'DMZ' status is 'Disabled'. The 'Source IP Address' is set to 'Any IP Address'. The 'Destination' is set to 'IP Address: 192.168.1.0'. There are buttons for 'Save Settings' and 'Cancel Changes'.

- The DMZ feature is disabled by default. Select **Enabled** to enable the DMZ. Leave the **Source IP Address** selected as **Any IP Address**, and enter the IP address of Host-B in the **Destination IP address**. Click **Save Settings** and click **Continue** when prompted.
- Test basic access to the DMZ server by pinging from the external server to the outside address of the multi-function device. Use the **ping -a** command to verify that it is actually the DMZ server responding and not the multi-function device. Are you able to ping the DMZ server?
- Test HTTP access to the DMZ server by opening a browser on the external server and pointing to the external IP address of the multi-function device. Try the same thing from a browser on Host-A to Host-B using the internal addresses.
Are you able to access the web page? _____
- Test Telnet access by opening a command prompt as described in Step 5. Telnet to the outside IP address of the multi-function device using the command **telnet A.B.C.D** (where A.B.C.D is the outside address of the multi-function device).
Are you able to telnet to the server? _____

Step 2: Set up a host with single port forwarding

The basic DMZ hosting set up in Step 6 allows open access to all ports and services running on the server, such as HTTP, FTP, and Telnet. If a host is to be used for a particular function, such as FTP or web services, access should be limited to the type of services provided. Single port forwarding can accomplish this and is more secure than the basic DMZ, because it only opens the ports needed. Before completing this step, disable the DMZ settings for step 1.

Host-B is the server to which ports are forwarded, but access is limited to only HTTP (web) protocol.

- From the main screen, click the **Applications & Gaming** tab, and then click **Single Port Forwarding** to specify applications and port numbers.
- Click the pull-down menu for the first entry under **Application Name** and select **HTTP**. This is the web server protocol port 80.
- In the first **To IP Address** field, enter the IP address of Host-B and select **Enabled**. Click **Save Settings**.

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 checked="" type="checkbox"/>
0	0	Both	192.168.1.0	<input checked="" type="checkbox"/>

- Test HTTP access to the DMZ host by opening a browser the external server and pointing to the outside address of the multi-function device. Try the same thing from a browser on Host-A to Host-B.
Are you able to access the web page? _____
- Test Telnet access by opening a command prompt as described in Step 5. Attempt to telnet to the outside IP address of the multi-function device using the command **telnet A.B.C.D** (where A.B.C.D is the outside IP address of the multi-function device).
Are you able to telnet to the server? _____

Step 3: Restore the multi-function device to its default settings

- a. To restore the Linksys to its factory default settings, click the **Administration > Factory Defaults** tab.
- b. Click the **Restore Factory Defaults** button. Any entries or changes to settings will be lost.

NOTE: The current settings can be saved and restored at a later time using the **Administration > Management** tab and the **Backup Configuration** and **Restore Configuration** buttons.

