



Module 11 10 1001 01010110 WIRELESS NETWORK SECURITY

CERTIFIED CYBERSECURITY TECHNICIAN

Copyrights @ 2021 EC-Council International Ltd.







Module 11: Wireless Network Security

Exercise 1: Configure Security on a Wireless Router







LAB SCENARIO

The cyberspace is heading toward a new era of technological evolution by using wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing the physical connection or cable, individuals can use networks in newer ways that make data portable, mobile, and accessible. A wireless network can be insecure if proper care has not been taken while configuring it. Insecure configurations can pose a great risk to the wireless networks.

A security professional must have the required knowledge to configure a wireless network as per the wireless according to the wireless security policy of an organization.

LAB OBJECTIVE

The objective of this lab is to provide expert knowledge in implementing wireless security policies. This includes knowledge of the following tasks:

Configuration of security policies on a wireless router

OVERVIEW OF WIRELESS NETWORK SECURITY

The use of wireless devices in various organizations is continuously growing. Therefore, it becomes increasingly important for organizations to track and manage their wireless assets for security purposes. To ensure effective security, an accurate and up-to-date inventory of wireless devices must be maintained.

The inventory can help in quickly identifying non-functioning and rogue network devices present in a network. This helps in detecting unknown devices in the network. It is important to regularly scan this inventory; accordingly, security professionals can determine the rogue network devices, problematic devices, potential vulnerabilities, and devices that need a patch/update, etc., in a network. A network is only as secure as its weakest link. Information about all devices should be maintained regardless of their configuration settings or vendor.





LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to configure wireless network security policies. The recommended labs that will assist you in learning the implementation of wireless network security controls include:



Configure Security on a Wireless Router

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.



EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER

A wireless router is a device that performs the functions of a router and includes the functions of a wireless access point.

LAB SCENARIO

Organizations allow wireless devices to connect to their network in today's environment (Bring Your Own Device or BYOD). However, the security of the network infrastructure is a major challenge for organizations while adopting wireless devices. A wireless router/access point is the main entry for attackers. Attackers compromise wireless access points to gain access to the organizational network. Organizations should ensure that their wireless access points are configured securely.

A security professional should be able to configure the wireless router securely by applying all possible hardening techniques.

LAB OBJECTIVE

This lab will demonstrate the various hardening techniques on a wireless router.

OVERVIEW OF WIRELESS ROUTER SECURITY

A wireless router is the first line of defense against attackers trying to access the organization's network. To prevent attackers from compromising the security of wireless routers, appropriate configuration changes need to be made in order to make a router more secure.

LAB TASKS

Note: Ensure that PfSense Firewall virtual machine is running.







1. Turn on the **AD Domain Controller** virtual machine.

- 2. Log in with the credentials CCT\Administrator and admin@123.
- 3. Open **Google Chrome** browser. Browse the Linksys Wireless router set up simulator available at http://ui.linksys.com/WRT54G/v8/8.00.0/ in your browser.







4. The **Linksys** router interface window will be displayed in the browser.



Basic Setup	× +	•					0	-	0	×
$\leftrightarrow \rightarrow G$	A Not secure ui.linksy	s.com/WRT54G/v8/8	3.00.0/				1	* *	-	:
	LINKSYS									
	A Division of Cisco Systems, Inc.					Firms	ne Version: v8.00.1			
				Wi	reless-G Bro	adband Router	WRT54G			
	Setup	Setup Wireles	as Security	Access Restrictions	Applications & Gaming	Administration	Status			
		Basic Setup	DONS	MAC Addres	s Clone	Advanced Routing				
1	Internet Setup					Automatic Co.	effective .			
- 1	Internet Connection Type	Automatic Cor	nfiguration - DHC	P ▼		DHCP: This se commonly use	tling is most d by Cable			
	Optional Settings (required by some ISPs)	Router Name:	WRT54G			operators. Host Name: E	nter the bost			
	,,	Host Name:				name provided	by your ISP.			
		Domain Name:				Domain Name	: Enler the			
		MTU:	Auto 🗸			domain name p ISP:	provided by your			
		Size:	1500			More				
	Network Setup	-				Local IP Address of the	reas: This is the router.			
	Router IP	Local IP Address:	192.168.1	. 254		Subnet Mask:	This is the subre			
	10000	Subnet Mask:	255.255.255.0	~		mask of the ros	der.			
	Network Address		-			DHCP Server:	Allows the router			
	Server Settings (DHCP)	DHCP Server.	Enable OD	isable		to manage you	r IP addresses.	1		
		Starting IP Address Maximum Number	192.166.11.100			Starting IP Ad address you w	dress: The ould like to start			
		of DHCP Users		and the second second		-				
		Client Lease Time:	o minutes (0	means one day)		Maximum nun Users: You ma	nber of DHCP ry limit the			
		Static DNS 1				number of add hands out.	resses your route			
		State ONS 2				More				
		Static DNS 3:	0.0.0							







- 5. Click on **Setup** followed by **Basic Setup**.
- 6. Specify the Router name, Host name, and Domain name in Optional Settings (required by some ISPs) (here, we are taking Router Name as Linksys-Router Setup, Host Name as host1, Domain Name as domain1)
- 7. Ensure that the Auto option is selected from the drop-down menu for MTU.
- 8. The Local IP Address and Subnet Mask in the Router IP field are displayed. Set DHCP Server to Enable.







E Basic Setup	× +				0	-	ť	3	×
← → C	A Not secure ui.links	com/WRT54G/v8/8.00.0/basic.htm				\$	*	٠	:
	LINKSYS"			Free	eare Version, vil D				
			Wireless-G Broa	dband Router	WRT54G				
	Setup	Setup Wireless Security Access Rest Basic Setup DDNS MA	rictions Applications & Gaming C Address Clone	Administration Advanced Routing	Status				
	Internet Setup Internet Connection Type Optional Settings (required by some (SPs)	Automatic Configuration - DHCP Router Name: Linksys-Router Setup Host Name: host1 Domain Name: domain1 MTU: Auto]	Automatic Co DHCP: This se commonly use operators. Host Name: E name provided Domain Name Gonain Name BP More	infiguration - etting is most d by Cable inter the host I by your ISP is Enter the provided by your				
	Network Setup Router IP	Local IP Address: [192]. [168]. [1]. [284] Subnet Mask: [265.285.285.0 V		Local IP Addm address of the Subnet Mask: mask of the ro	ess: This is the router. : This is the subr uter.	net			
	Network Address Server Settings (DHCP)	DHCP Server: Enable Disable Starting IP Address: 192.168.1		DHCP Server to manage you Starting IP Ad	Allows the rout of IP addresses. Idress: The	*			





- 9. Specify the Starting IP Address and Maximum Number of DHCP Users. Type Client Lease Time in minutes.
- 10. Specify any three DNS server IP addresses in the **Static DNS (1-3)** fields.
- 11. Enter the **WINS** server IP address if you use a WINS server.
- 12. Click on the Save Settings button to save all changes.

Note: If you receive any error message, reload the page and repeat the steps 6 to 11.







	Heatthere hast	name provided by your ISP.		
	Host Name: host1			
	Domain Name: domain1	Domain Name: Enter the domain name provided by your		
	MTU: Auto 🗸	ISP. More		
	Size 1600			
Network Setup		Local IP Address: This is the address of the router.		
Router IP	Local IP Address: 192 . 168 . 1 . 284	Subret Mask: This is the subret		
	Subnet Mask: 255.255.255.0 V	mask of the foulter.		
Network Address Server Settings (DHCP)	DHCP Server: Enable O Disable	DHCP Server: Allows the router to manager your IP addresses.		
	Starting IP Address: 192.168.1 100	Startino IP Address: The		
	Maximum Number 50	address you would like to start with.		
	Client Lease Time: O minutes (0 means one day)	Maximum number of DHCP		
	State DNS 1: 208 . 67 . 222 . 222	Users: You may limit the number of addresses your router		
	Static DNS 2: 208 . 67 . 220 . 220	hands out. More		
	Static DNS 3: 200 . 67 . 220 . 222			
	WINS: 0.0.0.0	Time Setting: Choose the time		
		zone you are in. The router can also adjust automatically for		
Time Setting	Time Zone:	daylight savings time.		
	(GMT+08:00) China, Hong Kong, Australia Western	✓		
	Automatically adjust clock for daylight saving changes			
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		





13. A prompt indicating that Settings are successful is displayed. Click on Continue.











14. Next, click on MAC Address Clone.

15. Ensure that Mac Clone is set to Disable.









16. Next, click on **Advanced Routing**.

17. Set the **Operating Mode** to **Gateway**.

18. Select a number from the Static Routing drop-down menu Select set number.

19. Enter the following details:

- Router Name
- Destination LAN IP
- Subnet Mask
- Default Gateway

20. Next, select an Interface from the drop-down menu (LAN & Wireless).

21. Click on Save Settings.







Wireless-G Broadband Router WRT54G Setup Wireless Security Access Restrictions Applications & Gaming Administration Status Basic Setup I DDNS I MAC Address Clone Advanced Routing Advanced Routing Gatewray Coperating Mode: If the router is select Setup Operating Mode: If the router is select Setup Static Routing Select set number: 3() Delete This Entry Delete This Entry
Advanced Rosting Operating Mode Gateway Gateway Static Routing Select set number: 3() Delete This Entry
Enter Route Name: test1 Select Set Number: This is the unsign route number, you may set up to 20 routes. Destination LAN IP: 10 10 20 Subnet Mask: 285 285 0 Default Gateway: 10 10 10 Interface: LAN & Wireless Subnet Mask: Determines the house the basing to this route. Show Routing Table Subnet Mask: Determines the house the basing to this route.





22. A prompt indicating that **Settings are successful** is displayed. Click on **Continue**.



ullinksys.com/WRT54G/v8/8.000 × +	0	-	σ	×
← → C ▲ Not secure ui.linksys.com/WRT54G/v8/8.00.0/AdvRoute.html		☆	* 2	:
Settings are successful.				
Continue				







- 24. Click on the **Basic Wireless Settings** tab.
- 25. Set Wireless SSID Broadcast to Disable.



		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		_					
	LINKSYS"					Free	are Version: v8.00		
				Wire	less-G Broad	dband Router	WRT54G		
	Wireless	Setup Wireless	Security Access	Restrictions	Applications & Gaming	Administration	Status		
		Basic Wireless Settings \	Nireless Security	Wreless MAC I	Filter ^{Ad}	Vanced Wireless Settings			
	Wireless Network	Vilreless Network Mode: Vilreless Network Name (SSIC Vilreless Channek Vilreless SSID Broadcast	Mixed WRT54Gv8 6 - 2.437GHz Catabase Disate Status : SES inactive Reset Security	• sie		Wireless Notw with to exclude clerely, choose you would like 1 wereleve access Disable More	ork Mode: If yo Whetens-G B-Orby Mode. I Io dinabile I, choose	u T	
			Save Se	ttings Cano	el Changes		ence conce allocadho		





26. Click on the Wireless Security tab next to the Basic Wireless Settings tab.



L Wireless S	iecurity	×	+						0	-	C	3	×
← → C	A Not secure	ui.lir	ksys.com/WRT5-	4G/v8/8.00.0	0/WSecurity.h	itm				☆	*	4	:
	LINKS A Division of Cisco Sys	YE terrs, in) °					Firm	ure Version: vil.				
						w	ireless-G Broa	dband Router	WRT54G				
	Wireles	S	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Administration	Status				
			Basic Wireless	Settings	Wireless Securi	ty Wireless M/	IC Filter A	dvanced Wireless Settings					
	Wireless	Securi	Security	Mode:	Disabled	v		Security Mod choose from D Personal, WP WW2 Person Enterprise, R devices on you use the same to order to comen Micre	e: You may isaable, WPA A Enterprise, al, WPA2 ADRUS, WEP. ar network mus security mode unicate.	All dis			
					5	Save Settings Ca	ancel Changes		alb_alb	h			





27. Select the strongest and most appropriate encryption mode from the drop-down menu for Security Mode.
Note: Here, we consider WPA2 Personal as the strongest encryption mode for wireless security.
Note: If you are unable to change the Security Mode, then follow the steps given below:

- In the browser window, press Ctrl+H to open History window. In the left-pane click on Clear browsing data.
- In the pop-up ensure that the Advanced tab is selected, and All Time is selected from the Time range drop down.
- Ensure that all the options are checked in the Clear browsing data window and click on Clear data to clear all the cookies and cached data.
- Reload the simulator tab and in the router interface window navigate to **Wireless** tab in the menu bar and click on **Wireless Security** tab. Then, perform **Step#27** again.

28. Select AES for WPA Algorithms and enter a valid key value in the WPA Shared Key field.

29. Click on Save Settings.







E → C ▲ N	ot secure ui.linksys	.com/WRT54G/v8/8.00.0	/WSecurity.h	tm			\$	*	2
A Divis	NKSYS [®] on of Claco Systems, Inc.					Firm	ura Version vil 00 0		
				wi	reless-G Broad	Iband Router	WRT54G		
	Vireless	Setup Wireless	Security	Access Restrictions	Applications & Gaming	Administration	Status	1	
		Basic Wireless Settings	Wreless Securit	y Wireless MA	CFilter Ad	vanced Wireless Settings			
	Wireless Security	Security Mode:	WPA2 Pers	onal 👻		Security Mode choose from D Personal, WP	c You may isable, WIVA A Enterprise,		
		WPA Algorithms	AES	~		WPA2 Person Enterprise, RA devices on you	al, WEV2 ADIUS, WEP, All In network must		
		Group Key Renewal:	3600	seconds		order to comm More	vecurity mode in unicate.		
							Cisco Svattma	1	
			5	ave Settings Ca	ncel Changes		db_db_		







30. A prompt indicating that **Settings are successful** is displayed. Click **Continue**.

Mentan MAC Da

- 31. Click on Wireless MAC Filter.
- 32. Set the Wireless MAC Filter option to Enable.



	· ·				
← → C ▲ Not secure uilli	nksys.com/WRT54G/v8/8.00.0/WFilter.htm	r :	*	1	:
	S C Fermana Version vel.00				
	Wireless-G Broadband Router WRT54G				
Wireless	Setup Wireless Security Access Restrictions & Applications Administration Status				
	Basic Weeless Settings Weeless Security Wireless MAC Filer Advanced Weeless Settings				
Wireless MAC Fit	Wireless MAC Filter: Wireless MAC Filter: Prevent: Prevent: Permit only: Permit only PCs listed from accessing the wireless Permit only: Edit MAC Filter List Cittle Sestaws Cittle Sestaws				
	Save Settings Cancel Changes				





33. Next, go to the **Security** tab to enable firewall restrictions in the router.

Note: Select the options Block Anonymous Internet Requests and Filter IDENT (Port 113).



Firewall	× +						•	-	C	3	×
← → C	A Not secure ui.linksys	s.com/WRT54G/v8/8.00.0/	Firewall.htm					☆	*	-	1
	LINKSYS" A Division of Claco Systems, Inc.					Free	name Version: v8.	00.0			
				wi	ireless-G Broad	Iband Router	WRT54G				
	Security	Setup Wireless	Security	Access Restrictions	Applications & Gaming	Administration	Status				
		Firewall VPN				_					
	Firewall					More					
	Block WAN Requests	Filter Multicast	ternet Request	•							
		Filter Internet NAT F	Redirection								
							Cisco System	MS			
			s	ave Settings Ca	incel Changes		dh.dh				







35. Next, configure the appropriate internet access restrictions.



Internet Access	× +				0	-	0	×
← → C ▲ Not secure	ui.linksys.com/WRT54G/v8/	8.00.0/Filters.htm				\$	*	
	YS [®] Inns, Inc.			Farme	are Version: vil.00			
		w	ireless-G Broad	Iband Router	WRT54G			
Restrictio	S Setup Wirele	ess Security Access Restrictions	Applications & Gaming	Administration	Status			
	Internet Access							
Internet	Internet Access Po	licy: 1() V Delete Summary		Internet Acces may define up policies. Click I policy or Summ summary of the Status: Enable	as Policy: You to 10 access Delete to delete many to see a policy. or disable a	•		
	Status	O Enable 🖲 Disable		Policy Name:	You may assign			
	Enter Policy Name			Policy Type: C	necy. hoose from			
	PCs	Edit List of PCs		Internet Access Traffic.	or inbound			
	Deny Allow Days	Internet access during selected days and I	hours.	Days: Choose week you would to be applied.	the day of the d like your policy	,		
	Z Everyday	Sun Mon Tue	Wed	Times: Enter 8 you would like y apply.	he time of the da your policy to			
	Times	Thu Fri Sat		Blocked Servi choose to block certain services	ces: You may access to Click Add/Edi			
	24 Hours	○ From: 12 v : 00 v AM v		settings.	uny treste			
		Te: 12 ♥ : 00 ♥ AM ♥		Website Block can block acce websites by en	ing by URL: Yo ss to certain lering their URL			
Blocked	Services			Website Block You can block	ing by Keywon access to certain	d:		





36. Select Applications & Gaming from the main menu. Enter the following details:

- Application Enter the name of the program.
- Start / End Enter the range of ports.
- Protocol Select either of the protocols or both.
- IP Address Enter the IP address of the port receiving the port traffic.
- Enable Enable or disable the port forwarding rule.

	A Division of Cisco Systems, Inc.	ŝ						Firms	are Version: v8.00.0	
	Applications					Wire	less-G Broad	Iband Router	WRT54G	
	& Gaming	Setup Port Range For	Wireless ward P	Security ort Triggering	Access I	Restrictions DMZ	Applications & Gaming I QuS	Administration	Status	
	Port Range Forward			Port	Bance			Port Range Fo Certain applicat	orwarding: Bors may require	
M III		Application	Start	End	Protocol	IP Address	Enable	it to function co of these applica	erectly. Examples ations include	
		pubg	3434 to	4500	Both 🗸	192.168.1. 1		games. When a certain port con	a request for a mes in from the	
			0 10	0	Both 🛩	192.168.1.0		data to the com specify. Due to	security	
			0 to	0	Both 🗸	192.168.1.0		port forwarding ports you are u	may want to limit to only those sing, and	
			0 10	•	Both V	192.168.1.0		uncheck the En after you are fin More	nable checkbox nished.	
			0 10		Both V	192.168.1.0				
$(\mathcal{G}) \gg \square$			0 10		Both ¥	192 168 1 0				
			0 10	0	Both ¥	192.168.1.0				
			0 to	0	Both 🗸	192.168.1.0				
			0 to	0	Both 🛩	192.168.1.				
									Cisco Systems	





37. Click on Save Settings, a prompt indicating that Settings are successful will be displayed. Click on Continue.



I	U uilinksys.com/WRT54G/48/8.00.0 × +	0	-	0		×
l	← → C ▲ Not secure ui.linksys.com/WRT54G/v8/8.00.0/ptrigger.html		$\dot{\mathbf{r}}$	*	1	:
	Cattings are successful					
	Settings are successful.					
	Continue					





38. Next, click on the **DMZ** tab and set DMZ to **Disable**.



DMZ	× -	ŀ				0 -		0	×
← → C	A Not secure ui.links	ys.com/WRT54G/v8/8.00.0/	dmz.htm			\$	*	4	:
	LINKSYS [®] A Division of Cisco Systems, Inc.				Free	are Version: v8.00.0			
	Applications			Wireless-G Broad	Iband Router	WRT54G			
	& Gaming	Setup Wireless	Security Access Res	trictions & Gaming	Administration	Status			
		Port Range Forward Po	rt Triggering C	MAZ QoS					
	DM2	C Enable C Disable DM2 Host IP Address:	192,168.1. 0		DM2: Enabling expose your rou Intermet. All port accessible from More	this option will der to the is will be the internet			
			Save Setting	s Cancel Changes		enco Systems adhoodhoo			





39. Next, click on the **QoS** tab and set QoS to **Disable**.



QoS	×	+					•		a	>
← → C	A Not secure ui.link	sys.com/WRT54G/v8	3/8.00.0/qos.htm				☆	*	4	-
	LINKSYS" A Division of Cisco Systems, Inc.					Ferror	are Version: v8.00.0			
	Applications			Wir	eless-G Broad	Iband Router	WRT54G			
	& Gaming	Setup Wire	less Security	Access Restrictions	Applications & Gaming	Administration	Status			
		Port Range Forward	Port Triggering	I DMZ	QoS					
	QoS	Upstream Bandwidth	O Enable 🧧 Auto 👻 0	Disable Kbps		Two types of Q features are av QoS which com plugged in to th	uality of Service allable, Wired trols devices re router with a			
	Device Priority	Device name	Priority	MAC Address	0	Ethernet cable, QoS, which cor are wirelessly c router.	and Wireless shol devices that connected to the			
		Device name	Low v 00:	00:00:00:00:0	0	Device Priority specify priority a device on you	r : You may for all traffic from ar network by			
	Enternet Port Priority		Priority	Flow Control		Name, specifyin entering its MA	ng priority and C address.			
		Port 1 Port 2	Low V	Enable V		Ethernet Port I may control you	Priority : You or data rate			
		Port 3	Low Y	Enable ~		port your device	c is plugged into.			
		Port 4	Low ~	Enable 🗸		priority to data 1 devices connec 1 through 4.	traffic from ded on LAN ports			
	Application Priority		Optimize Gan Priority	ning Applications Specific Port		Application Pr control your dat respect to the a consuming ban	iority : You may ta rate with pplication that is dwidth. Check			
		Application Name	Low	> >	0	to automatically game application higher priority. 1	y allow common on ports to have a You may a wight			
		Application Name	Low	¥	0	applications by number they us	entering the port re.			





40. Click on **Save Settings** as shown in the screenshot below.

CURITY 00

				•			
← → C ▲ Not secure ui	linksys.com/WRT54G/v8	/8.00.0/qos.htm			* *	F (#	
Ehternet Port Prio	rity	Priority	Flow Control	Name, specifying priority and entering its MAC address	•		
	Port 1	Low 🛩	Enable 🛩	Ethernet Port Priority : You			
	Port 2	Low 🛩	Enable 🛩	may control your data rate according to which physical			
	Port 3	Low 🛩	Enable 🛩	port your device is plugged in You may assign High or Low	NBD.		
	Port 4	Low ~	Enable 🛩	priority to data traffic from devices connected on LAN p 1 through 4.	ots		
Application Prio	rity	Optimize Gami	ng Applications	Application Priority : You n control your data rate with	ay .		
		Priority	Specific Port #	respect to the application that consuming bandwidth. Chec	k		
	Application Name	Low	v 0	to automatically allow commo	on a		
	Application Name	Low	v 0	higher priority. You may customize up to eight			
	Application Name	Low	~	applications by entering the number they use.	port		
	Application Name	Low		Wireless QoS			
	Application Name	LOW		Wreless QoS is also referre	110		
	Application Name	Low	•	as we-ri MultiMedia TM (W) by the WI-Fi AllianceTM. Set	ed.		
	opproation many	Low	~	using other wireless devices are also WMM certified	that		
	Application Name	Low	v 0	No Acknowledgement : En	attin		
	Application Name	Low	v 0	this option if you would like to disable acknowledgement. If	Dris .		
				option is enabled, the router not re-send data if an error	will .		
Wireless Q	o\$			occurs.			
	WMM Support:	Disable V (Defa	ult : Disable)				
	No Acknowledgement	Disable V (Defa	ult : Disable)				
				Cisco Svate			
			ave Settings Cancel (Chappes			
		Ľ	Cancer				





41. A prompt indicating that **Settings are successful** is displayed. Click on **Continue**.

42. Click on the **Administration** tab. Click on the **Management** tab under **Administration**.



Wireles Wireless Security Access Restrictions A	Firmus ss-G Broadband Router ppications Gaming Administration	re Version: v6.00.0 WRT54G Status
Wireles Wireles Security Access Restrictions	ess-G Broadband Router pplications Gaming Administration	WRT54G Status
Wireless Security Access Restrictions &	pplications Gaming Administration	Status
Log Diagnostics Factory Defaults		
	Firmware Upgrade Config 1	Vanagement
	Local Router Ac	ccess: You can
	thange the Rout from here. Enter	er's password a new Router en hree il anain
confirm:	in the Re-enter to confirm.	o confirm field to
	Web Access: Al	lows you to
	router's web utilit More	y.
Enable Disable	Remote Router	Access: Allows
	you to access yo remotely. Choose world like to use	e the port you
t Enable Disable	change the pass router if it is still	word to the using its default
	password.	
	UPnP: Used by o programs to auto	certain smatically open
	confirm:	





43. In the **Password** field, set a very strong password for a wireless router.

- 44. Type a new password and re-type it in the **Re-enter to Confirm** field. **Note**: Passwords should be changed periodically to restrict unauthorized access to the wireless network
- 45. Next, in Web Access, set Access Server to HTTPS.
- 46. In Remote Router Access, set Remote Management to Disable.







				w	ireless G Broadba	ind Router	WRTSIG	
Adn	ninistration	Setup Wreles	s Security	Access Restrictions	Applications & Garning	Administration	Status	
		Management	Log Diagno	stics Factory Defaul	h 📘 Firmware Upgr	ade Conlig N	Aanagement	
	Router Bassword Local Router Access	Password. Re-enter to confirm:				Local Router Ac change the Route from here. Enter password and the in the Re-enter to	coma: You can er's password a new Router en type it again o continn field to	
	Web Access	Access Server. Wireless Access Web:	HTTP H	TTP5 Disable		content. Web Access: All configure access router's web utilit More	lowes you to copilions to the Y	
	temote Router Access	Remote Management Management Port	C Enable	Disable		Remote Router / you to access yo remotely. Choose would like to use, change the pass router if it is still u password.	Access: Allows ar router the port you You must word to the ming its default	
		Use https:				UPMP: Used by o programs to auto ports for commu	certain matically open sication.	
	UPnP	UPnP.	• Enable	Disable		More_	Control Person Control Perso	







- 48. Set Log to **Enable** as shown in the screenshot below.
- 49. Click on Save Settings.



Log × +		0 -		0	×
← → C ▲ Not secure ui.linksys.	.om/WRT54G/v8/8.00.0/Log.htm	☆	*	1	:
A Debilion of Deco Systems, Inc.	Ferman Vers	on: v1.00.0			
	Wireless-G Broadband Router WR	T\$4G			
Administration	Setup Wireless Security Access Restrictions & Applications & Administration	Status			
Los	Management Log Diagnostics Factory Defaults Firmware Upgrade Config Manag	ement			
	Log: Enable Disable to discuss a constraint of the constraint of t	die the Sulgoing spropriate			
	Incoming Log Outgoing Log				
		durin			
	Save Settings Cancel Changes				







50. A prompt indicating that Settings are successful is displayed. Click on Continue.

51. Next, click on **Status** from the menu bar.

Note: As it is a simulation task explaining the configurations on the router page so the settings that have been shown in this task, will not get saved.



									-		
÷	C A Not se	ecure ui.lir	nksys.com/\	VRTS4G/v8,	/8.00.0/StaRouter	.htm			\$	*	
	A Division of Co	SYS sco Systems, inc.						Fernware	Version: v8.00.0		
						Wi	reless G Broad	Iband Router	WRT54G	2 3	
	Sta	itus	Setup	Wire	ess Security	Access Restrictions	Applications & Gaming	Administration	Status		
			Router	1 6	cal Network	Wreless					
	Route	er Information		mutere Version	x8.00.0 Dec 4.2	106		Firmware Version Router's current fi	n. This is the mware.		
			Cu	rent Time:	Not Available			Current Time. Th time, as you set of Tab.	is shows the in the Setup		
			Ro	C Address: der Name:	00:00:00:00:00:00			MAC Address, Th Router's MAC Address ISP	is is the less, as seen	too.s	
		la la ma	Ho	st Name: main Name:				Router Name. Th specific name for I which you set on I	is is the the Router, the Setup Tab.		
	Con	figuration Type	Log	in Type:	Automatic Config	puration - DHCP		Configuration Ty shows the information	pe. This tion required		
		X A Not secure ui.linksy Configuration Type	Sut	onet Mask:	0.0.0.0			internet. This infor entered on the Se can Connect or D	mation was tup Tab. You Inconnect		
			Det	ault Gateway:	0.0.0.0			your connection is on that button. More	ere by clicking		
			DN	51						t − C t T T T T T T T T T T T T T T T T T T T	
			DN	53							
			мт	U:	1500						
					DHOD D						







52. As described above, a security professional can make configuration changes in the wireless router interface to secure the wireless router.

- 53. Close all open windows.
- 54. Turn off AD Domain Controller and PfSense Firewall virtual machines.

1 10 1001 01010110

EC-COURCI

override for onPageSgrglled(post

override fun onPageSelected (Description Cont

b<u>Layout</u>.getTabAt(<u>selectedTab</u>) bLayout.<u>tabMode</u> = TabLayout.MODE_FIXED bLayout.<u>tabGravity</u> = TabLayout.GRAVITY_FIL bLayout.setupWithVic**O**P1(**(0010Parts))