

2. Connect a EasyMesh agent to this controller by following the setup instructions in the agent's manual. The agent will be listed on the controller's Mesh page.

Note: To check full list of TP-Link EasyMesh devices, visit https://www.tp-link.com.

3. If you have set up the agent to join the EasyMesh network, it will be listed on the controller's EasyMesh page.

_	nogy				Add	Mesh De	evice
		EX510	ц°			— E	thernet Vireless
			•				
		H0C220,					) Refresh
	Device Name	IP Address	MAC Address	Connection Type	Signal Strength	Link Rate	Operation
0							
1					-	-	-

Otherwise, you need to find it in the Add Mesh Device list and click Add to add it to the EasyMesh network.



Done! Now your controller and agents successfully form a EasyMesh network!

## 10.2. Manage Devices in the EasyMesh Network

In a EasyMesh network, you can manage all mesh devices and connected clients on your router's web page.

- To view mesh devices and connected clients in the network:
- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Basic > Network Map.
- 3. Click 🚔 to view all mesh devices, and click 💷 垕 to view all connected clients.

	Main AP
Wirefess Cherits Wired Cherits	

- To manage a EasyMesh device in the network:
- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Basic > Network Map.

	logy				Add	Mesh D	evice
		Ш	பீ			F	Thernet Vineless
			0				
		HX220	(and				
		H0(220)	_				) Retrest
ID	Device Name	IP Address	MAC Address	Connection Type	Signal Strength	Link Rate	Operation
1D	Device Name	IP Address	MAC Address	Connection Type -	Signal Strength -	Link Rate	D Retrest

3. Click the Mesh device's IP Address to redirect to the web management page of this device and view detailed information.



- 4. Manage the EasyMesh device as needed. You can:
  - Change device information.
  - Delete this device from the EasyMesh network.

# Chapter 11

# **Guest Network**

This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy.

It contains the following sections:

- <u>Create a Network for Guests</u>
- <u>Customize Guest Network Options</u>

## 11.1. Create a Network for Guests

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > Guest Network. Locate the Wireless section.
- 3. Create a guest network as needed.
  - 1) Tick the Enable checkbox for the 2.4GHz or 5GHz wireless network.
  - 2) Customize the SSID. Don't select Hide SSID unless you want your guests to manually input the SSID for guest network access.
  - 3) Select the Security type and customize your own password. If No security is selected, no password is needed to access your guest network.

Wireless	
2.4GHz Wireless:	Enable Guest Network Share Network
Network Name (SSID):	TP-Link_1011_Guest Hide SSID
50Hz Wireless:	Enable Guest Network Share Network
Network Name (SSID):	TP-Link_1011_5G_Guest Hide SSID
Security:	WPA2-PSK[AES]
Password.	tplinkpassword
6GHz Wireless:	Enable Guest Network Share Network
Network Name (SSID):	TP-Link_1011_6G_Guest Hide SSID
Security:	WPA3-Personal 👻
Password:	tplinkpassword
	Save

4. Click Save. Now your guests can access your guest network using the SSID and password you set!

#### Ø Tips:

To view guest network information, go to Network Map and locate the Guest Network section. You can turn on or off the guest network function conveniently.

## 11.2. Customize Guest Network Options

1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.

- 2. Go to Advanced > Guest Network. Locate the Settings section.
- 3. Customize guest network options according to your needs.

Settings			
See each other	F Allow Guesta in Access Lech Office		
		Save	

• Allow guests to see each other

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with each other via methods such as network neighbors and Ping.

4. Click Save. Now you can ensure network security and privacy!

# Chapter 12

# **NAT Forwarding**

The router's NAT (Network Address Translation) feature makes devices on the LAN use the same public IP address to communicate with devices on the internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that an external host cannot initiatively communicate with a specified device on the local network.

With the forwarding feature the router can penetrate the isolation of NAT and allows devices on the internet to initiatively communicate with devices on the local network, thus realizing some special functions.

The TP-Link router supports four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Port Forwarding, Port Triggering, UPNP and DMZ.

It contains the following sections:

- <u>ALG</u>
- Set Up Public Services on The Local Network by Virtual Servers
- Open Ports Dynamically by Port Triggering
- Make Applications Free from Port Restriction by DMZ
- <u>Make Xbox Online Games Run Smoothly by UPnP</u>

# 12.1. ALG

ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc. It is recommended to keep the default settings.

You may need to disable SIP ALG when you are using voice and video applications to create and accept a call through the router, since some voice and video communication applications do not work well with SIP ALG.

Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router. Go to Advanced > Security > ALG.

ALC:		
FFFF Poss-Incoph	F) Looble	
121PTresthough	F) Loadie	
PSec Pass-through	F) Loadie	
EIPAIG		
IT IPALS		
1000 ALG	F) Loadie	
RESPACE	F) Loade	
SIPALC	E Londin	
		Save

# 12. 2. Set Up Public Services on The Local Network by Virtual Servers

Virtual Servers are used to set up public services on the local network. A virtual server is defined as an external port, and all requests from the Internet to this external port will be redirected to a designated computer, which must be configured with a static or reserved IP address. When you build up a server on the local network and want to share it on the Internet, Virtual Servers can realize the service and provide it to the Internet users.

The table displays the relevant parameters of the virtual server.

To set up a Virtual Server rule:

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > NAT Forwarding > Virtual Servers and click 😌 🖽.
- 3. Select an interface name from the drop-down list.

							0.44	0.085
	Ð	Service Type	Edama Part	Internal IP	Plantat Port	Protect	tinis	Mut
	-		100				13	10
11.00/ 201 201	idemai Nemai Nemai (	Port P.			0	X XX er XX) X or Blank, 1	455241	
₹	YOBOE		707	and The Property	.*			

4. Click View Existing Applications to select a service from the list to automatically populate the appropriate port number in the External Port and Internal Port fields. If the service is not listed, enter the External Port number (e.g. 21) or a range of ports (e.g. 21-25). Leave the Internal Port blank if it is the same as the External Port or enter a specific port number (e.g. 21) if the External Port is a single port. The following picture takes application FTP as an example.

							0.40	O Dete
	m	Service Type	External Port	Internal IP	(Hoamia) Port	Peter	Taba	Wedt
	-	-			12		-	5
Service Type Eidernal Port Internal (P Internal Port		21	21 (XXXX er XX) 21 (XX xr Bark, 1-45					
100	teris)	tert	1.1.		P	or on answer, it	999330	

- 5. Enter the IP address of the computer running the service application in the Internal IP field.
- 6. Select a protocol for the service application: TCP, UDP, or All from the Protocol dropdown list.
- 7. Select Enable This Entry.
- 8. Click OK.
- Ø Tips:
- If you want to disable this entry, click the Bulb icon.
- It is recommended to keep the default settings of Internal Port and Protocol if you are not clear about which port or protocol to use.
- If the local host device is hosting more than one type of available services, you need to create a rule for each service. Please note that the External Port should NOT be overlapped.

## 12.3. Open Ports Dynamically by Port Triggering

Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the internet return to the external ports, the router can forward them to the corresponding host. Port Triggering is mainly applied to online games, VoIPs, video players and common applications including MSN Gaming Zone, Dialpad and Quick Time 4 players, etc.

Follow the steps below to configure the Port Triggering rules:

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > NAT Forwarding > Port Triggering and click 😌 🕍.

								0.40	O Deid
D	(D)	Approation	Trippe	ring Port	fliggering Protocol	External Port	External Protocol	Distort .	510179
	=:	- 22		Ξ.		5	2	334	5
In	nertiace	Name		ipoe	0,0,0	۲			
A	spicali	01					Vine Experie	g Applica	
To	ogern	g Port					(XX, 1-65538)		
To	0,04111	g Protocal		TCP					
Ð	ternai	Part					(XX or XX-XX, 1 perts)	-85535, at	most 5
Ð	demai	Protocol		TOP		19			
				Q Ente	The Lots				

3. Click View Existing Applications, and select the desired application. The Triggering Port, Triggering Protocol and External Port will be automatically filled in. The following picture takes application MSN Gaming Zone as an example.

							😋 Add	00
D ID Application Trig			Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Mo
	-	-	-	-	-	-	-	
in	terface	Name:	lpoe	_0_0_d	Ŧ			
A	ppicat	ion:	MSN	Gaming Z	one	View Existin	g Applicat	ions
Т	riggerin	ig Port	4763	24		(XX, 1-65535)		
T	riggerin	g Protocal:	ALL		r			
E	xtemal	Port	2300	0-2400,288	00-29000	(XX or XX-XX, pairs)	1-65535, at r	most 5
E	xternal	Protocol:	ALL		Ŧ			
			🕑 Enal	ble This Entry				
					_			_

4. Click OK.

ort In	ggor	ing						
							G ant	O Delete
	ID	Application	Triggering Port	Inggering Protocol	External Port	Esternal Protocol	Status	Modity
	1	MSN Gaming Zo	47824	TCP or UD P	2300 2400, 28800 25000	TOP or U DP	8	0 🖬

Ø Tips:

- You can add multiple port triggering rules according to your network need.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the Existing Applications list, please enter the parameters manually. You should verify the external ports the application uses first and enter them into External Port field according to the format the page displays.

# 12.4. Make Applications Free from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host on the local network, it is totally exposed to the internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the PC to be a DMZ host.

#### Note:

When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

### I want to:

Make the home PC join the internet online game without port restriction.

For example, due to some port restriction, when playing the online games, you can log in normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ host with all ports open.

### How can I do that?

- 1. Assign a static IP address to your PC, for example 192.168.0.100.
- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > NAT Forwarding > DMZ and tick to enable DMZ.
- 2. Enter the PC's IP address 192.168.0.100 manually in the DMZ Host IP Address field.

UMZ	
DM2	[7] Lostie
DMZ Host IP Address	142 . 168 . 0 . 100
	Save

### 3. Click SAVE.

## Done!

The configuration is completed. You've set your PC to a DMZ host and now you can make a team to game with other players.

# 12.5. Make Xbox Online Games Run Smoothly by UPnP

The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with each other thus realizing the seamless connection of the network. You may need to enable the UPnP if you want to use applications for multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) or remote assistance, etc.

Tips:

- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the corresponding ports allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



If necessary, you can follow the steps to change the status of UPnP.

1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.

2. Go to Advanced > NAT Forwarding > UPnP and toggle on or off according to your needs.

UMP 💽	
UPnP Service List	
Inial Clerity B	🖒 Refresh
ID Service Description Externel Port Protocol Internel IP Address	Internal Port

Chapter 13

# **Parental Controls**

This function allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time.

I want to: Control what types of websites my children or other home network users can visit and the time of day they are allowed to access the internet.

For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only www.tp-link.com and Wikipedia.org from 18:00 (6 PM) to 22:00 (10 PM) on the weekdays and not other time.

- How can I<br/>do that?1. Visit <a href="http://tplinkwifi.net">http://tplinkwifi.net</a> or <a href="http://tplinkwifi.net">http:/
  - **2.** Go to Basic > Parental Controls or Advanced > Parental Controls.

rental Controls						
						0
Name	Filter Lovel	Time Limits	Devices	Insights	Internet Access	Modify

 Click Add, and then enter the Name manually. Click Add and specify the devices belonging to the family member. Click Next.

						~
Narra	FiletLevel	TreeLines	Oevens	inspire	Marriel Accase	Mode
z = z		÷.,	100	-		
			Chief Library			
			-0		0	
	Dark Tells					
Nere	liame the Pyptie					
Name	Name the Profile					
Name Devices List	liame the Profile					
Name Devices List	liame the Postle					
Dayreas List	Name the Profile					
Devices List	Name the Profile					
Nere Devices List	Name the Profile					
Nerre List	Name the Profile					

4. Select a filter level based on the age of the family member. Blocked content will then be displayed in the Filter Content list. Click Next.

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Mo
		-	-	-		
	•					
	Basic Info					
	100 A 10 A	State State			A	
sed on the r re from Ava	Child (0-7) selected filter level silable Categories o	Pte-Tek (8-12) Adult Content,Soc or by adding a new	n cial Networkin keyword.	Teen (13-17) ng have airea	Adult (>17) dy been fillered for 123	. You can
sed on the r re from Awa	Child (0-7) selected filter level slable Categories ( tent	Pre-Tek (8-12) Adult Content, Soc or by adding a new Add a New Ke	n cal Networkin keyword.	Teen (13-17) ng have airea vailable C	Adult (>17) dy been tillered for 123 atlagories:	. You can
Filter Con	Child (0-7) selected titler level ilable Categories ( tent (	Pre-Ter (8-12) x by adding a new Add a New Ke	n cial Networkin keyword. yword Ar	Teen (13-17) ng have altea vallable C arnes	Adult (>17) dy been filtered for 123 atlagories:	. Yau can
Filter Con Adult Con	Child (0-7) selected filter level islable Categories ( tent tent tent tent	Pre-Ter (8-12) Adult Content, Soc or by adding a new	in Networkin keyword yword Ar	Teen (13-17) ng have alter vailable C arnes edia	Adult (>17) dy been tillered for 123 atlagories:	. You can
Filter Con Adult Con Social Ne	Child (0-7) selected filter level ilable Categories o tent tent tent tvorking	Pre-Ter (8-12) Adult Content Soc r by adding a new Add a New Ker	m cial Networks keyword wword Gi Mit Or	Teen (13-17) Ing have alrea vitallable C arries edia	Adult (>17) dy been filtered for 123 atlagories:	. Yau can
Filter Con Adult Con Social Ne	Child (0-7) selected filter level itable Categories ( tent tent tent tworking	Pre-Ter (8-12) Adult Content, Soc or by adding a new	m cial Networks keyword word Gi Gi Gi Gi Gi Gi Gi	Teen (13-17) ng have altes vailable C ames edia nline Commu sy to Surf	Adult (>17) dy been tillered for 123 atlagories:	. You can ⊕ ⊕ ⊕
Filter Con Adult Con Social Ne	Child (0-7) selected filter level ilable Categories o tent tent tent tvorking	Pre-Ter (8-12) Aduit Content, Soc or by adding a new Add a New Ker	m cial Networks keyword wword Ar Gi Mit Or Pa	Teen (13-17) Ing have alrea vatilable C ames edia nine Commu ay to Surf overloads	Adult (>17) dy been filtered for 123 attagories:	• You can

- (Optional) Delete items from the Filter Content list, add items from the Available Categories list, or click Add a New Keyword to add a filter keyword (for example, "Facebook") or URL.
- 6. Enable Time Limits for Mon to Fri and Sat & Sun, then set the daily internet time allowed. Enable BedTime on School Nights (Sunday to Thursday) and Weekend (Friday and Saturday), then set the time period during devices in the profile cannot access the internet.

							0
Name	Filter Level	Time Limits	Devices	Insights	Internet Acc	ns N	lodif)
-	-	-	-		-		
			liter Level				
	•		•				
	Basic Info				Time Contro	6	
Weekdays		ton 🔽 Tues		The P		Sun	
Time Limits Set daily time lim	its for the total tir	ne spent online.					
			2				
Weekdays	<b>e</b> 1	mable	0.000				1
			21				91
Visalanda	e 6	nable					7
THE REPART							ah.
		3	Omin				
		3	Qmin				
Bed Time	utile this coefficient	C	o internet				
Bed Time Set a time period	while this profile	3 cannot access th	e internet.				
Bed Time Set a time period Weekdays	while this profile	a cannot access th	e internet. From 10	00 PM	≜. ∵ To	06:00 AM	÷
Bed Time Set a time period Weekdays	while this profile	3 cannot access th inable	e internet. From 10	:00 PM	÷ To	06:00 AM	\$
Bed Time Set a time period Weekdays	while this profile	3 cannot access th inable	e internet. From 10	:00 PM	а. То	06:00 AM	\$
Bed Time Set a time period Weekdays Weekends	while this profile	3 cannot access th inable	e internet. From 10 From 10	:00 PM	ф Та ф Та	06:00 AM	0

#### 7. Click Save.

Done!

#### Now you can control your children's internet access as needed.

#### 🖉 Tips:

- To monitor internet usage of a family member:
- 1. Find the profile of the family member, then click the **Insights** icon.
- 2. On the **Top 5 Visits** page, select a day of the last 7 days to check the time spent online and top visited websites. You can block the websites if needed.
- 3. On the **Blocked History** page, select a day of the last 7 days to check the blocked website history. You can **unblock websites** if needed, and click Unblocked Websites to view them.

Name -	Title Level	-time Lines:	Destrat	Incastel	Informati Accesso	Made
120	Pro-Tour:	25	- 24	0	0	BI
		a S Valle		Bidi	of Notice	~
Today						
1011						
			$\square$			

• To pause or resume internet access of a family member: Find the profile of the family member, then click the **Pause/Play** icon.

						. 0
Name	Filler Level	Time Limits	Devices	Insights	Internet Access	Modity
123	the teen	70	1	0	ß	Pi I

Chapter 14

# **Quality of Service**

This function allows you to specify the priority of traffic and minimizes the impact of network congestion.

The router allows you to configure the quality of service (QoS) for optimal throughput and performance when handling differentiated wireless traffic, such as Voiceover-IP (VoIP), other types of audio, video, streaming media, and traditional IP data.

To configure QoS on the routers, you should set parameters on the transmission queues for different types of wireless traffic. In normal use, we recommend that you keep the default values for the routers.

## To set up QoS for the network:

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with the password you set for the router.
- 2. Go to Advanced > QoS.
- 3. Enable QoS.

QoS	
QoS:	Cruble
Upload Bandwidth:	0 Mbps *
IPTV QoS:	C Enable
Advanced	
High	60%
Middle	30%
Low	
	Save

4. Enter the upload and download bandwidths provided by your ISP.

QoS	
QeS:	Crable
Upload Bandwidth:	0 Mbps V
IPTV QoS:	🕑 Enable
Advanced	
High	60%
Middle	30%
Low	
	Save

5. (Optional) Enable IPTV QoS, then set the priority and reserved bandwidth of IPTV traffic.

QoS	
QoS:	C Enable
Upload Bandwidth:	0 Mbps *
IPTV QoS:	C Enable
Advanced	
High	60%
Middle	30%
Law	- 10%
	Save

6. (Optional) Click Advanced and arrange the sliders to set the bandwidth percentage of each priority.

QoS				
QoS:	Enable			
Upload Bandwidth:	0	Mbps	Ŧ	
IPTV QoS:	C Enable			
Advanced				
High			60%	
Middle			30%	
Low	-0		10%	
				Save

7. Click Save to make the settings effective.

## To set up QoS for a specific device:

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.88.1</u>, and log in with the password you set for the router.
- 2. Go to Advanced > QoS.
- 3. In the QoS Rule List table, choose a priority section and click Add.

light Friendy, 80%	Mildle Priority (30%)	Low Priority, 10%
hhA	Add	Add

4. In the QoS Rule window, click scan and click to choose a device, then click OK to add it to the rule.

QoS Rule			
Түрө	(i) By Device.		
Device Name	Unknown	scan	
MAC Address	10.000000000000000000000000000000000000		
		Cancel OK	J

ID	Device Name	IF Address	MAC Address	Operation
1	Disknown	-		0

## Chapter 15

# **Network Security**

This chapter guides you on how to protect your home network from unauthorized users by implementing network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent ARP spoofing and ARP attacks by using IP & MAC Binding.

This chapter contains the following sections:

- Firewall & DoS Protection
- <u>Service Filtering</u>
- <u>Access Control</u>
- IP & MAC Binding
- IPv6 Firewall

## 15.1. Firewall & DoS Protection

The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the router from cyber attacks.

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default, and it is recommended to keep the default settings.

Firewall	
IPM SPIT newsil	
IINS SPEL INVAL	

DoS Protection can protect your home network against DoS attacks from flooding your network with server requests. Follow the steps below to configure DoS Protection.

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with the password you set for the router.
- 2. Go to Advanced > Security > Firewall & DoS Protection.

DoS Protection.		
Do3 Protection		
ICMF Flood Attack Filtering:	-Please Select-	Ψ.
UDP Flood Attack Filtering:	-Please Select-	Ψ.
TOP Flood Attack Filtering:	-Please Select-	Ψ.

- **3.** Enable DoS Protection.
- 4. Set the protection level (Low, Middle or High) for ICMP-Flood Attack Filtering, UDP-Flood Attack Filtering and TCP-Flood Attack Filtering.
  - ICMP-Flood Attack Filtering Enable to prevent the ICMP (Internet Control Message Protocol) flood attack.
  - UDP-Flood Attack Filtering Enable to prevent the UDP (User Datagram Protocol) flood attack.
  - TCP-Flood Attack Filtering Enable to prevent the TCP (Transmission Control Protocol) flood attack.
- 5. Click Save.
  - Ø Tips:
  - 1. The level of protection is based on the number of traffic packets. You can specify the level under DoS Protection Level Settings.

Luw	1200	(5.3500) packets/sec
Middle	2400	(5.3500) packets/sec
Ligh	3500	(5.3500) packets/sec
Luw	1200	(5.3500) packets/sec
Matthe	2400	(5.3500) packets/sec
Ligh	3500	(5.3500) packets/sec
Luw	1200	(5.3500) packets/sec
Midtle	2400	(5.3500) packets/sec
Linch	3500	(5 3600) packets/sec
	Low Makte Digh Low Makte Ligh Low	Low         1200           Mobble         2400           Lingh         3500           Low         1200           Mobble         2400           Lingh         3500           Lingh         3500           Lingh         3500           Lingh         3500           Lingh         3500           Lingh         2400           Lingh         3500           Lingh         2400

2. The protection will be triggered immediately when the number of packets exceeds the preset threshold value, and the vicious host will be displayed in the Blocked DoS Host List.

Final Number 0			💍 Refrecti 🤤 Delete
	D	IP Address	MAC Address

## 15.2. Service Filtering

With Service Filtering, you can prevent certain users from accessing the specified service, and even block internet access completely.

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with the password you set for the router.
- 2. Go to Advanced > Security > Service Filtering, and enable Service Filtering.

	Service Filtering		
s	Service Filtering:		

3. Click Add.

	0	Barvce Type	Pot		# Address	State	Mont
+	-	-			-		-
16vi	a Type:	Any(ALL)					
Prenoc	in the second se	TOPUDP					
Starte	g Port	1			(1-66535)		
Endio	a Port	65535			(1-69535)		
Servic	e Type:	Any(ALL)					
Filler 2	Service For	O Stige P A	ates O PA	001005	Range 🐞 🖊 📼	4.4295826	

- 4. Select a Service Type from the drop-down list and the following four fields will be automatically filled in. Select Custom when your desired service type is not listed, and enter the information manually.
- 5. Specify the IP address(es) that this filtering rule will apply to.
- 6. Click Save to make the settings effective.

Note: If you want to disable an entry, click the  $\mathbb{Q}$  icon.

## 15.3. Access Control

Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

l want to:	Block or allow specific client devices to access my network (via wired or wireless).
How can I do that?	<ol> <li>Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with the password you set for the router.</li> </ol>
	2. Go to Advanced > Security > Access Control and enable Access Control.
	Access Control Access Control

**3.** Select the access mode to either block (recommended) or allow the device(s) to access your network.

#### To block specific device(s):

1) Select Blacklist and click Save.

Access Mode		
Access Mode:	· Dachist	
	<ul> <li>Whitelist</li> </ul>	
		Save

- 2) Select the device(s) to be blocked in the Online Devices table (or click the Add under the Devices in Blacklist and enter the Device Name and MAC Address manually).
- 3) Click Block above the Online Devices table. The selected devices will be added to Devices in Blacklist automatically.

					O has O trees
		E Description	ing the second sec	MAC Address	Shutty
-				1.00	1
ne Dev	-				
nii Dev	ces				0 (tenur 2 200
ne Dev	011	Desce Name	# Agama	MAC Address	O tomor 2 ton

#### To allow specific device(s):

1) Select Whitelist and click Save.

Access Mode		
Access Mode:	<ul> <li>Blackint</li> </ul>	
	<ul> <li>Whitekst</li> </ul>	
		Save

2) Click Add in the Devices in Whitelist section.

				O A O D
Π.	0	Oeme Name	MAC Address	More the local data
Device	WHE			
NAC.Re				

- 3) Enter the Device Name and MAC Address. (You can copy and paste the information from Online Devices table if the device is connected to your network.)
- 4) Click Save.

**Done!** Now you can block or allow specific client devices to access your network (via wired or wireless) by Blacklist or Whitelist.

## 15.4. IP & MAC Binding

IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind a network device's IP address to its MAC address. This will prevent ARP spoofing and other ARP attacks by denying network access to a device with a matching IP address in the Binding list, but an unrecognized MAC address.

I want to: Prevent ARP spoofing and ARP attacks.

- How can Ido that?1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with the password you set for the router.
  - Go to Advanced > Security > IP & MAC Binding, and enable IP & MAC Binding.

IP & MAG	- Briding					
P & MAC I	andreg .					
lindea I	int					
					0.	Den
(O)	æ.	MAC Address	IF Addmin	State	Trotte	Mieth
- 2		5a.	5a	12	141	1.2
ARP List					0~	
10)	- 10)	MAC ADDress	IP.Address	- 89	nit:	Methy

3. Bind your device(s) according to your needs.

### To bind the connected device(s):

- 1) Select the device(s) to be bound in the ARP List.
- 2) Click Bind to add to the Binding List.

#### To bind the unconnected device:

1) Click Add in the Binding List section.

		AAAT AATTAY	PANNER	Shifty	53459	SALAR
M	CARDAN		84 - 16 - F9 - 03 - E2 - 83			
à.	Address		112 168 8 199			
			In Route Des Lints			

- 2) Enter the MAC address and IP address that you want to bind.
- 3) Select the Enable This Entry check box to enable the entry and click Save.
- **Done!** Enjoy the internet without worrying about ARP spoofing and ARP attacks.

## 15.5. IPv6 Firewall

IPv6 Firewall protects your IPv6 network by preveting access from the internet. However, when you are hosting a service, such as a file sharing server in your local network, you can choose to allow access to the server from the internet by adding entries on this page. This feature is available only when you've set up an IPv6 connection.

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with the password you set for the router.
- 2. Go to Advanced > Security > IPv6 Firewall.

IPv	8 Fire	swall						
							🕒 Add	🖨 Delete
		D	Service Type	Internet II *	Internal Fort	Profocal	Siaha	Modify

3. Click Add.

					0 /41	O Denis
🖙 i Densie	Yape.	( Internal IP )	indernal Part	Protocel	( Distan	Modely
		÷		1	- 22	1
interface Name		No interface	.,	6		
Записа Тури				Men Land	ing Applicat	N/m
Internal IP		11				
Hitemal Port				(200)		
Frotocor.		TCP		9		
		E Louis Die Lat	73			

- 4. Select an interface name from the drop-down list. Interface names are names of the internet connections you have set up.
- 5. Click View Existing Applications to select a service from the list to automatically populate the Port field with an propriate port number. It is recommended to keep the default Port if you are unsure about which one to use. If the service is not listed, manually enter the Service Type and the Port number (e.g., 21 or 21-25). The following picture takes application FTP as an example.

						0.44	O Develo
	æ	Denica Tupe	Internal IP	Part	Pentsoni	State	Abotts
	4	10			1		1 5
	ientere	Martwr	Ro interface		1		
\$	evice 1	Pythe	579		Ver Let	<b>HEARDON</b>	
'n	(arrai)	P.	共				
	ternal I	hat	31		(XX)		
Ð	ali an		TCF		9		
			iff drame the time				

- 6. Select the local host device running the service. Enter its global IPv6 address in the Global IPv6 Address field.
- 7. Select a protocol for the service from the drop-down list.
- 8. Select Enable This Entry.
- 9. Click OK.
- Ø Tips:
- If you want to disable this entry, click the Bulb icon.
- If the local host device hosts more than one type of available service, you need to create a rule for each service. Please note that ports should NOT be used by multiple services.

# Chapter 16

# **VPN Server&Client**

The router offers several ways to set up VPN connections:

**VPN Server** allows remote devices to access your home network in a secured way through the internet. The router supports three types of VPN Server:

**OpenVPN** is somewhat complex but with higher security and more stability, suitable for restricted environments such as campus network and company intranet.

**PPTP VPN** is easy to use with the built-in VPN software of computers and mobile devices, but it is vulnerable and may be blocked by some ISPs.

**L2TP/IPSec VPN** is more secure but slower than PPTP VPN, and may have trouble getting around firewalls.

**VPN Client** allows devices in your home network to access remote VPN servers, without the need to install VPN software on each device.

This chapter contains the following sections:

- Use OpenVPN to Access Your Home Network
- <u>Use PPTP VPN to Access Your Home Network</u>
- Use IPSec VPN to Access Your Home Network
- <u>VPN Connections</u>

## 16. 1. Use OpenVPN to Access Your Home Network

OpenVPN Server is used to create an OpenVPN connection for remote devices to access your home network.

To use the VPN feature, you need to enable OpenVPN Server on your router, and install and run VPN client software on remote devices. Please follow the steps below to set up an OpenVPN connection.



### Step1. Set up OpenVPN Server on Your Router

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > VPN > OpenVPN, and tick the box of Enable VPN Server.

OpenVEN	
Note: No certificate currently, pic	aso Generate one before enabling VFN Server.
	🕑 Enable VPN Server
Service Type:	8 UDP C TOP
Service Port	1194
VPN Subnet/Netmasic	10 8 0 0 255 255 255 0
Client Access:	8 Home Network Only C Internet and Home Network
	Rave

#### Note:

- Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.
- The first time you configure the OpenVPN Server, you may need to generate a certificate before you enable the VPN Server.
- 3. Select the Service Type (communication protocol) for OpenVPN Server: UDP, TCP.
- 4. Enter a VPN Service Port to which a VPN device connects, and the port number should be between 1024 and 65535.
- 5. In the VPN Subnet/Netmask fields, enter the range of IP addresses that can be leased to the device by the OpenVPN server.
- 6. Select your Client Access type. Select Home Network Only if you only want the remote device to access your home network; select Internet and Home Network if you also want the remote device to access internet through the VPN Server.

### 7. Click SAVE.

8. Click GENERATE to get a new certificate.

Certificate		
Generate the certificate		
	GENERATE	

Note: If you have already generated one, please skip this step, or click GENERATE to update the certificate.

9. Click EXPORT to save the OpenVPN configuration file which will be used by the remote device to access your router.

Configuration File		
Export the configuration file.		
	EXPORT	

### Step 2. Configure OpenVPN Connection on Your Remote Device

1. Visit <u>http://openvpn.net/index.php/download/community-downloads.html</u> to download the OpenVPN software, and install it on your device where you want to run the OpenVPN client utility.

**Note:** You need to install the OpenVPN client utility on each device that you plan to apply the VPN function to access your router. Mobile devices should download a third-party app from Google Play or Apple App Store.

- 2. After the installation, copy the file exported from your router to the OpenVPN client utility's "config" folder (for example, C:\Program Files\OpenVPN\config on Windows). The path depends on where the OpenVPN client utility is installed.
- 3. Run the OpenVPN client utility and connect it to OpenVPN Server.

## 16.2. Use PPTP VPN to Access Your Home Network

PPTP VPN Server is used to create a PPTP VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up PPTP VPN Server on your router, and configure the PPTP connection on remote devices. Please follow the steps below to set up a PPTP VPN connection.

#### Step 1. Set up PPTP VPN Server on Your Router

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > VPN > PPTP VPN, and tick the box of Enable VPN Server.

PPTP VPN	
	🕑 Enable VPN Server
Client IP Address:	10 7 0 11 10.7.0. 20 (up to 10 clients)
Ознати	
Password	ø
	save

Note: Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

- 3. In the Client IP Address field, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.
- 4. Enter the Username and Password to authenticate clients to the PPTP VPN server.
- 5. Click SAVE.
- 6. On the client devices, create a PPTP VPN connection. The official supported platforms include Windows, Mac OSX, Linux, iOS, and Android.
- 7. Launch the PPTP VPN program, add a new connection and enter the domain name of the registered DDNS service or the static IP address that is assigned to the WAN port, to connect the client device to the PPTP VPN server.

### Step 2. Configure PPTP VPN Connection on Your Remote Device

The remote device can use the Windows built-in PPTP software or a third-party PPTP software to connect to PPTP Server. Here we use the Windows built-in PPTP software as an example.

- 1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.
- 2. Select Set up a new connection or network.



3. Select Connect to a workplace and click Next.

nous	e a connection option
-0	Connect to the Internet. Set up a switchers, broadbard, or dial-up connection to the Internet.
-	Set up a new network Carifigure a new router er access pesitt.
8.	Connect III a sectipliza Set up a dial-up or VEN connection to processmipliant
3	Set up a dial-up connection Connect to the Internet using a dial-up connection
3	Connect to the Internet using a dial-up connection-

4. Select Use my Internet connection (VPN).

Use my Internet connection (VPN)     Connect using a virtual private network (VPN) connection through the Interne	6
Dial directly	
Connect directly to a phone number without going through the Internet.	
What is a VPN connection?	

5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.

Type the Internet a	address to connect to
Your network administs	ator can give you this address.
Internet address:	218181.73
Destination names	VPN Connection
🗇 Use a smart card	
S 20 Allow other peo This option allow	ple to use this connection ws anyone with access to this computer to use this connection.
🔲 Don't connect n	rowc just set it up so I can connect later

6. Enter the User name and Password you have set for the PPTP VPN server on your router, and click Connect.

Type your user nar	me and password	
User name:	ABOX.	
Pasewordt	••••	
	Show characters	
	Remember this password	
Domain (optional):		

7. Click Connect Now when the VPN connection is ready to use.

) lie Cor	mect to a Workplace		No.
The c	onnection is ready to use		
	<b>1</b>	<b>]</b> p	
	Connect now		
			Close

## 16.3. Use IPSec VPN to Access Your Home Network

IPSec VPN Server is used to create a IPSec VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up IPSec VPN Server on your router, and configure theIPSec connection on remote devices. Please follow the steps below to set up the IPSec VPN connection.



Home Network

**Remote Devices** 

### Step 1. Set up IPSec VPN Server on Your Router

- 1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > VPN > IPSec VPN, and enable Dead Peer Detection.

#### Note:

- Firmware update may be required to support IPSec VPN Server.
- · Before you enable Dead Peer Detection, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

IPSoc V	ΡN						
Deathree	r Delection					🗘 Add	0.000
0	Connection Name	Remde Geleway	Local Address	Remole Address	Status	Enable	Modify
-	-	-	-	-	-	-	-

### 3. Click Add.

4. Configure the IPSec VPN server parameters.

	Connection Name	Famole Galessey	Lucal Ambent	Renote Address	Shatus	Enstin	Month
-	+	-	-	+	14		-
iP:	Set Contection Name			Name			
Ple	male IPSec Galeway (U	HILY		0.0.0.0			
To	nmil access from local (P	adminarc		Subnet Addres		Ŧ	
iP.	Address for VPN			0 0	0	0)}	
60	trint Mask:			255 - 255	255	0	
Tu	rinal accass from remola	(P <sup>1</sup> abbesive:		Subset Addres	s	*	
IP.	Address for VPN			0 0	0	0	
34	dnet Mask:			255 255	255	0	
Ke	y Exchange Method			Auto (IKE)		w.	
Ais	thentication Method			Pre-Shared Ke	r .	Ψ.	
Pr	e-finareit Key			ptik_kny			
Pe	Held Forward Secrecy			Enable		· *:	
G	Atvanced						

5. Configure the advanced settings according to the following explanation. We recommend that you keep the default settings. If you want to change these settings, make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Lifetime in both phase1 and phase2.

Phase 5->		
Wate	Main	
Local Identifier Type	Local Wan IP	
Local Identifier		
Remote identifier Type	Remote Wan IP	*
Remote Identifier		
Encryption Algorithm:	3065	
Integrity Algorithm:	MDS	
Diffle-Hellman Group for Kay Exchange	10.24b/t	
Kiry Life Time(Seconds)	3600	
==Plaze 2==		
Encryphan Algorithm	3DE5	.*
Integrity Algorithm.	ND5	
Diffe-Heiman Graup for Key Exchange	1024bit	
Key Life Time(Seconds)	3000	

#### 6. Click OK.

Note:

• For the comprehensive guide, please refer to the User Guide on the product's support page.

#### Step 2. Configure IPSec VPN Connection on Your Remote Device

The remote device can use the Windows or Mac OS built-in IPSec software or a thirdparty IPSec software to connect to IPSec Server. Here we use the Windows built-in IPSec software as an example.

1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.

2. Select Set up a new connection or network.



3. Select Connect to a workplace and click Next.

1005	e a connection option
•	Connect to the Internet. Set up a switches, proodband, or dial-up connection to the Internet.
-	/ Set up a new network Canfigure a new router er access point.
8-	Commet III a workplace Set up a dial-up or VEN convection to processmikplace.
3	Set up a dial-up connection Connect to the Internet using a dial-up connection.

4. Select Use my Internet connection (VPN).

How do you wa	ant to connect?	6			
Use my In Connect unit	ternet connecti g a virtual private o	ion (VPN) etwork (VPN) ci	innection throug	ph the Internet.	
1	- 0	) —	- Do		
Dial direct Connect dire	ly thy to a pitrone num	nber without go	ing through the	Diternet.	
<b>A</b>					
What is a VPN core	ection?				

5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field, and select the checkbox Don't connect now; just set it up so I can connect later. Click Next.

Type the Internet a	ddress to connect to
Your network administr	ator can give you this address.
Internet address	21838.1.73
Destination names	VPN Connection
Use a smart card	
S 20 Allow other peop This option allow	ple to use this connection as anyone with access to this computer to use this connection.
😨 Don't connect n	ovc just set it up so I can connect later

6. Enter the User name and Password you have set for the IPSec VPN server on your router, and click Connect.

Type your user nar	me and password	
User name:	MARK .	
Paspwordt	••••	
	Show characters	
	Remember this password	
Domain (optional):		

7. Click Close when the VPN connection is ready to use

Connect to a Workplace		
The connection is ready to use		
<b>N</b>	<b>@</b> p	
Connect now		
		Close

8. Go to Network and Sharing Center and click Change adapter settings.



9. Find the VPN connection you created, then double-click it.

onection
wrdiad. Frigeat

10. Enter the User name and Password you have set for the IPSec VPN server on your router, and click Properties.

Se Casewet SPM Convertion
Lier same
Degan.
12 See the our range and passes of the file following same B Margo Grow and case the impact
Correct Cancel Properties (548

11. Switch to the Security tab, select Layer 2 Tunneling Protocol with IPsec (L2TP/ IPSec) and click Advanced settings.

INVICATION Properties	14.0
Genual Comme Security Hadwood	a Deta
Taxe of VPM	
Laser & Turretting Paramit with Press	LTIP/Piert +
Date exception	Advanced settings
People brogging illuminant i street	e desiliere i
() De Daniel Advetzan ha	
Contempted parameter (PAP) Contempt garget gardet also Autoreto Contempted parameter (Contempted and Contempted and Contempt	nation Protocol (CrostP) CrostP x() res logics name and Y)
1	OH Carcal

12. Select Use preshared key for authentication and enter the IPSec Pre-Shared Key you have set for the IPSec VPN server on your router. Then click OK.

Advand Projection	
• on polarel in to admittate the 'all	
Can priter is a feetate Eligits forme estimat differentit	and the first sector
C3	a Cent

Done! Click Connect to start VPN connection.

Correct Will Correction
Germania de Deserto de la constante de la con
Const.

## 16.4. VPN Connections

VPN Connections page displays the clients that are currently connected to the OpenVPN servers, PPTP VPN servers and IPSec VPN hosted on the router.

- 1. Visit <u>http://tplinkwifi.net</u> or <u>http://192.168.0.1</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > VPN > VPN connections.

0	Client 14 C. Marine	Shell .
WE CONFICTION		
Ψ.	MIRE CASENI	LKC V
-	-	-
VPU Concern tes		
Trans Is a Marso	Randa Land Alderson De	wie Address - Alabara - Deel de

# Chapter 17

# **Manage Your Router**

This chapter introduces how to change the system settings and administrate your router's network.

This chapter contains the following sections:

- <u>Set System Time</u>
- <u>Control the LED</u>
- <u>Test Internet Connectivity</u>
- <u>Update the Firmware</u>
- Back Up and Restore Configuration Settings
- <u>Reboot the Router</u>
- <u>Administration Management</u>
- <u>System Log</u>
- <u>CWMP Settings</u>
- SNMP Settings
- Monitor the Internet Traffic Statistics