

Troubleshooting and Advanced Customer Manual

Host Name:	Huawei
Model Number:	HG8245W5
Firmware Version:	HWTCA51910110
Serial Number:	48575443D150E29D (HWTCD150E29D)

Autor: Adam Husár, Ľuboš Lendáč

Date: 7.11.2019

Version: 2



1 Contents

2	Mož	źné p	roblémy so zariadením Huawei HG8245W5 a ich riešenie	3								
	2.1	Žela	ný stav	3								
	2.2	Рор	opis LED kontroliek a možných problémov									
	2.3	Nast	astavenie Wi-Fi									
	2.4	Kon	trola fyzického zapojenia	5								
	2.5	Kon	trola pripojenia	7								
3	Adv	ance	d Customer Manual	3								
	3.1	IPv4	٤٤	3								
	3.1.	1	Static LAN DHCP	3								
	3.1.2	2	Port forwarding a DMZ	9								
	3.2	IPv6	j	2								
	3.2.	1	Port Mapping Configuration12	2								
	3.2.2	2	IPv6 Firewall Configuration14	1								
	3.2.3	3	Filter Configuration14	1								
	3.2.4	4	PCP	5								
	3.2.	5	Zmena prefixu1	7								
	3.2.	6	Prístup z WAN)								
	3.3	IPv4	and IPv62:	1								
	3.3.	1	MAC Filter22	1								
	3.3.2	2	Smart Wi-Fi22	L								
	3.3.3	3	Parental Control	2								
	3.3.4	4	Guest Wi-Fi23	3								
	3.3.	5	Wi-Fi automatic shutdown24	1								
	3.3.	6	Firewall25	5								
	3.3.	7	Reštart zariadenia	5								
	3.3.	8	Obnovenie továrenských nastavení22	7								
	3.3.9	9	Zmena prihlasovacieho hesla27	7								
	3.3.	10	Firewall záznamy	3								



2 Možné problémy so zariadením Huawei HG8245W5 a ich riešenie

2.1 Želaný stav

Zariadenie Huawei HG8245W5 je funkčné ak svietia LED kontrolky, ktoré sú zelené (POWER a PON). Kontrolky LAN 1-4, TEL1-2, USB, WLAN môžu svietiť alebo blikať v závislosti na tom či je pripojené nejaké zariadenie a či práve komunikuje.

Prvá kontrolka zľava (POWER) indikuje, že je zariadenie zapnuté. Druhá kontrolka (PON) indikuje, že zariadenie je pripojené do optickej siete a užívateľ by mal byť schopný pripojiť sa na internet.

Ak nesvieti (ani nebliká) žiadna kontrolka, užívateľ by mal skontrolovať napájanie a napájacie tlačidlo.



2.2 Popis LED kontroliek a možných problémov

LED	Popis	Stav kontrolky	Popis stavu	Možné riešenie problému				
POWER	Kontrolka zapnutia	Svieti	Zaradenie je zapnuté					
		Nesvieti	Zaradenie je vypnuté	Skontrolujte tlačidlo napájania a napájací kábel.				
PON	Autentifikačná LED	Viď tabuľka 2						
LOS	LED spojenia		Viď tabuľka 2					
LAN1-4 Kontrolka portov		Stále svieti	Pripojenie je v normále					
		Bliká	Prebieha prenos dát					
		Nesvieti	Pripojenie nie je	Pripojte počítač k				
			zostavené	jednému zo štyroch LAN				
				portov				
TEL1-2	Kontrolka	Svieti	Zariadenie je pripravené					
	telefónneho		na telefónne spojenie					
	spojenia	Bliká	Prebieha telefónne					
			spojenie					
		Nesvieti	Pripojenie nie je	Pripojte telefón				
			zostavené	k jednému z TEL portov				

Tabuľka 1.

orange

Troubleshooting and Advanced Customer Manual

USB	Kontrolka USB	Svieti	Je pripojené USB	
			zariadenie ale neprebieha	
			prenos dát	
		Bliká	Prebieha prenos dát	
		Nesvieti	Nie je pripojené	
			zariadenie do USB portu	
WLAN	Kontrolka WLAN	Svieti	Funkcia WLAN je	
	(Wi-Fi)		zapnutá	
		Bliká	Prenášajú sa dáta	
		Nesvieti	Funkcia WLAN je	Kapitola Nastavenie Wi-
			vypnutá	Fi
WPS	Kontrolka WPS	Svieti	Funkcia WPS je zapnutá	
		Bliká	Terminál Wi-Fi	
			pristupuje k systému	
		Nesvieti	Funkcia WPS je vypnutá	

Tabul'ka 2. Popis PON a LOD LED kontroliek

	Stav	v LED	Popis stavu
	PON	LOS	
1	Nesvieti	Nesvieti	OLT zamedzilo prístupu ONT
2	Bliká rýchlo (dvakrát	Nesvieti	ONT nadväzuje spojenie s OLT
	za sekundu)		
3	Svieti Nesvieti		Spojenie medzi ONT a OLT je nadviazané
4	Nesvieti	Bliká pomaly (jedenkrát	Nie je pripojené optické vlákno alebo nie je
		za sekundu)	neprijímaný optický signál
5	Bliká rýchlo (dvakrát	Bliká rýchlo (dvakrát za	OLT deteguje že zariadenie je neautorizované
	za sekundu)	sekundu)	
6	Bliká rýchlo (dvakrát	Bliká pomaly (jedenkrát	Prijímaný signál je mimo rozsah citlivosti
	za sekundu)	za sekundu)	prijímača

2.3 Nastavenie Wi-Fi

Ak na zariadení nesvieti kontrolka WLAN pre bezdrôtovú sieť, užívateľ by mal skontrolovať nastavenie Wi-Fi siete vo webovom rozhraní zariadenia.

Po prihlásení do webového rozhrania na IP adrese zariadenia 192.168.100.1, pomocou mena "root" a hesla, ktoré je napísané na zariadení (toto meno a heslo je pôvodné a malo by byť funkčné, pokiaľ ho užívateľ nezmenil), v hlavnom hornom menu kliknite na záložku WLAN. Po načítaní stránky v ľavom menu vyberte možnosť 2.4G/5G Basic Network Settings.

Pre zapnutie Wi-Fi treba zaškrtnúť možnosť *Enable WLAN (Obr.2*, číslo 1). Užívateľ tu môže zmeniť aj názov siete Wi-Fi (*Obr.2*, číslo 2). Heslo k sieti Wi-Fi sa nachádza na štítku umiestnenom na spodku zariadenia. V prípade zmeny hesla je potrebné prejsť do kolónky *WPA PreSharedKey (Obr.2*, číslo 3) a tam vložiť nové heslo. Vedľa tejto kolónky je možnosť schovať/zobraziť heslo k Wi-fi

	151/5				Lonout
	+3W3				Logout
HUAWEI Status WAI	N LAN IPv6 WLAN Secu	rity Forward Rules Netwo	ork Application Syst	em Tools	
.4G Basic Network Settings	WLAN > 2.4G Basic Network Se	ttings			
.4G Advanced Network Settings					
G Basic Network Settings	On this page, you can set th	e basic parameters of 2.4 GH:	z wireless network(Wh	en the 2.4 GHz wire	ess network is disabled,
G Advanced Network Settings	Caution:				
utomatic WiFi Shutdown	Wireless network services It is recommended that yo	may be interrupted temporar	ily after you modify wir	eless network param	eters.
ViFi Coverage Management	L. H lo roconintona da unar yo			for cocarry parpeor	
iuest Wi-Fi	Enable WLAN 1.				
					New Delete
	SSID Index SSID Name	SSID Status Number of	Associated Devices	Broadcast \$SID	Security Configuration
	1 A_2.4	Enabled 32		Enabled	Configured
	SSID Configuration Details				
	SSID Name:	A_2.4 *	(1-32 characters)	•	
	Enable SSID:	✓			
	Number of Associated	32 * ((1-32)		
	Broadcast SSID:				
	Enable WMM				
	Authentication Mode:	WPA2 PreSharedKey	•		
	Encryption Mode:	AFS	TKIP&AES m	ode is recommende	d)
	WPA PreSharedKey		Hide * (8-63 ch	aracters or 64 hexad	ecimal characters)
	WPA Group Key Regeneratio	n	- 1100 (0 00 011		J.
	Interval:	3600	*(600-86400s)		
	Enable WPS:				
	WPS Mode:	PBC	•		
	PBC:	Start WPS			
		Apply Cancel			
		Apply Cancel			

Obrázok 2 Nastavenie Wi-Fi

2.4 Kontrola fyzického zapojenia

Pri kontrole fyzického zapojenia musí byť optické vlákno zapojené do zariadenia tak ako na *Obr. 3.* Pokiaľ je takto zapojený nie je potrebné ho vyberať. Kábel RJ-45, ktorým sa prepojí počítač s HG8245W5, musí byť zapojený do jedného zo štyroch LAN portov, na zariadení sú žltej farby (*Obr. 5*, číslo 1). Kábel RJ-11, ktorým sa prepojí telefónny prístroj a HG8245W5 sa pripája do jedného z dvoch TEL portov, na zariadení sú šedej farby (*Obr. 5*, číslo 2). Vľavo sa potom nachádza vstup pre pripojenie adaptéra (*Obr. 5*, číslo 3) a tlačidlo napájania (*Obr. 5*, číslo 4).

Na pravej strane sa tiež nachádza tlačidlo pre resetovanie zariadenia do výrobných nastavení (*Obr.* 6, číslo 1).



Obrázok 3 Pripojenie optického vlákna do HG8245W5



Obrázok 4 Káble RJ-45 a RJ-11



Obrázok 5 Rozhrania HG8245W5





Obrázok 6 Umiestnenie tlačidla Reset

2.5 Kontrola pripojenia

Funkčnosť fyzického pripojenia a linkovej vrstvy môžete skontrolovať vo webovom rozhraní zariadenia. Po prihlásení kliknite na možnosť *Status* v hornej časti obrazovky a potom v menu na ľavej časti obrazovky kliknite na WAN Information. Na *Obr.* 7 v označenej časti vidieť stav pripojenia, Connected znamená že pripojenie bolo úspešné a užívateľ má prístup na internet. Po kliknutí na pripojenie sú vidieť aj ďalšie informácie o pripojení ako napr. IP adresy. *Obr.* 7 zobrazuje IPv6 pripojenie. *Obr.* 7*a* zobrazuje IPv4 pripojenie.

HIGO2	245W5 WAN LAN IPv6 WLAN Security F	Forward Rule	es Network Application	System Tools		Logo			
/AN Information	Status > WAN Information								
oIP Information									
/LAN Information	On this page, you can query the co	onnection and	d line status of the WAN p	ort.					
ome Network Information									
th Port Information	IPv4 Information (Click any table of	ell for detail	s)						
HCP Information	WAN Name	St	tatus IP Addre	ess VLAN/Prio	rity C	onnect			
ntical Information	5_TR069_R_VID_851	Con	nected 10.34.0.	179 851/6	Alv	ways On			
evice Information	WAN Information	50.00.50	00.0D.50						
evice information	MAC Address:	F0:63:F9	(86)6D(F8						
ser Device Information	VLAN:	851							
ervice Provisioning Status	Policy:	Use the s	specified value						
	Priority:	6							
	NAT: Disable								
	IP Acquisition Mode: DHCP								
	IP Address/Subnet Mask: 10.34.0.179/255.255.255.192								
	Gateway:	10.34.0.129							
	DNS Servers: 213.151.208.161,213.151.208.162								
	Lease Time: 151200 s								
	Remain Lease:	127368 s							
	NTP Servers:	10.14.12	7.149,10.14.127.150						
	Time Zone Info:								
	SIP Servers:								
	Static Route:	213.151.223.0/25>10.34.0.129 85.237.225.0/25>10.34.0.129 85.237.225.230/32>10.34.0.129							
	Vendor Info:	dsiforum.org							
	Online Duration (dd:hh:mm:ss):	04:15:40	:12						
	IPv6 Information (Click any table of	cell for detail	s)						
	WAN Name	Status	Prefix	IP Address	VLAN/Priority	Conne			
	1_IPTV_INTERNET_R_VID_837	Connected	2a01:c846:f40:300::/56	fe80::f263:f9ff:fe86:6df4	837/0	Always			

Obrázok 7 Webové rozhranie zariadenia

orange [™]		Troubleshoo	oting and Adv	anced Custo	mer Manu		
HG82	45W5				Logout		
HUAWEI Status	WAN LAN IPv6 WLAN Security F	Forward Rules Network	Application System T	ools			
WAN Information	Status > WAN Information						
VoIP Information							
WLAN Information	On this page, you can query the co	onnection and line status o	of the WAN port.				
Home Network Information							
Eth Port Information	IPv4 Information (Click any table c	ell for details)	ID Address	VI AN/Driority	Connect		
DHCP Information	1 INTERNET R VID 836	Connected	213 151 242 12	836/0	Always On		
Optical Information	5 TR069 R VID 851	Connected	10.34.0.177	851/6	Always On		
Device Information	WAN Information				,		
User Device Information	MAC Address:	44:00:4D:31:E4:89					
Service Provisioning Status	VLAN:	836					
	Policy:	Policy: DSCP to Pbit mapping					
	Default Priority:	0					
	NAT:	Enable					
	IP Acquisition Mode:	DHCP					
	IP Address/Subnet Mask:	213.151.242.12/255.2	255.255.240				
	Gateway:	213.151.242.1					
	DNS Servers:	213.151.233.250,213.151.233.251					
	Lease Time:	111600 s					
	Remain Lease:	110724 s					
	NTP Servers:						
	Time Zone Info:						
	SIP Servers:						
	Static Route:						
	Vendor Info:						
	Online Duration (dd:hh:mm:ss):	00:00:14:36					

Obrázok 7a Webové rozhranie zariadenia

3 Advanced Customer Manual

3.1 IPv4

3.1.1 Static LAN DHCP

V hlavnom menu klikneme na záložku LAN. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "DHCP Static IP Configuration". Pre vytvorenie nového záznamu klikneme na "New". Do políčka "MAC Address" napíšeme fyzickú (MAC) adresu zariadenia, a do políčka "IP Address" napíšeme IP adresu ktorú bude router prideľovať tomuto zariadeniu. Po vyplnení políčok klikneme na "Apply" pre uloženie záznamu. Pre vymazanie konkrétneho záznamu označíme záznam zaškrtnutím kolónky pri zázname a klikneme na "Delete". Druhou možnosťou pre nastavenie statickej IP adresy je vybraním možnosti "Satus" na hlavnej lište, následne "User Device information". Pri vybranom zariadení vyberte možnosť "Network application" a po načítaní stránky vyberte "Configure Reversed DHCP IP Adresses".

orange [™]				Troubl	eshooting an	d Advanced Custo	omer Manual
	HG824	5W5					Logout
HUAWEI	Status WAN	LAN IPv6	WLAN Security	y Forward Rules	Network Application	System Tools	
LAN Host Configurat	ion	LAN > DHCP St	atic IP Configuration	on			
DHCP Server Configu	uration						
DHCP Static IP Confi	guration	On this page	e, you can configur	e the reserved IP a	Idress that is assigned u	sing DHCP for the specified MAC	address.
							New Delete
				MAC Addres	s	IP Address	,
					(44,00,00,00,00,00		
		MAC Address	5.		(AA:BB:CC:DD:EE	.FF)	
		IP Address:					
				Apply Cancel			

Obrázok 8 Pridelenie statickej DHCP adresy

3.1.2 Port forwarding a DMZ

Port forwarding je aplikácia (NAT), ktorá presmeruje komunikáciu z internetu na daný port zariadenia ONT na port Vami definovaného zariadenia v LAN (PC). Výhodou Port forwarding je možnosť pripojiť sa na PC v LAN z internetu. Oproti DMZ má bezpečnostnú výhodu v tom, že si môžeme zvoliť rozsah portov zariadenia v LAN, ktorý chceme sprístupniť do internetu a taktiež si môžeme vybrať verejné IP adresy, ktoré sa budú môcť pripojiť.

Demilitarizovaná zóna (DMZ) pracuje podobne ako port forwarding s tým rozdielom, že sú zo strany internetu prístupné všetky porty vybraného zariadenia (PC) a prístup má akékoľvek zariadenie z internetu.

3.1.2.1 Port forwarding

V hlavnom hornom menu kliknite na záložku "Forward Rules". Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "Port Maping Configuration". Na tejto stránke môžete vytvárať pravidlá, ktoré budú uplatnené vo Firewale. Pre vytvorenie nového pravidla kliknite na tlačidlo "New". Ako môžete vidieť na *Obr.9*.

orange [™] With the status wan	SW5 LAN IPv6 WLAN Securit	Troublesho y Forward Rules Netwo	noting and Ad	Ivanced Custon	ner Manual
LAN Address Configuration	IPv6 > Port Mapping Configuration	1			
DHCPv6 Static IP Configuration			un vielent annun an tha t	Able should and allow the	
Firewall Configuration	access the Internet.	mapping parameters to set	up virtual servers on the t	LAIN NELWORK and allow these	e servers to
Port Mapping Configuration	Note: 1) The well-known ports 2) The configured port r	for voice services cannot be mapping rule takes effect onl	in the range of the mapp y after the IPv6 firewall or	ving ports. ontrol on packet forwarding i	s enabled.
IP Filter Configuration					
					New Delete
	Mapping Name	WAN Name	Internal Host	External Host	Enable
	Туре:	User-defined Appli	cation		
	Application:	Web Server (HTTP)	•		
	Enable Port Mapping:				
	Mapping Name:	HTTP_name			
	WAN Name:	1_IPTV_INTERNET_R_	•		
	Internal Host:	2a01:c846:f40:300:fc43:51	01:715d:a346	LuboThinkpad	•
	External Source IP Address:			-	
	Protocol:	TCP V	Port number:	80 8	0 *
	Delete				
	Add				
					Apply Cancel

Obrázok 9 Vytvorenie nového pravidla.

V otvorenom menu na vytvorenie nového pravidla *Obr. 9: Vytvorenie nového pravidla*. si najskôr vyberte typ nastavenia:

User-Defined - manuálne vyplnenie položiek v menu "Add"

Application – menu doplní porty danej aplikácie na základe vybraného protokolu (pozrite aj *Obr. 10* . *Vopred definovane aplikácie.*).

Pri voľbe "User-Defined" pokračujeme doplnením "Internal Host" a "External Source IP Address" do poľa "Internal Host" zadáme verejnú adresu zariadenia, ktoré chceme aby bolo dostupné z internetu. A do poľa "External Source IP Address" zadáme verejnú adresu zariadenia z ktorého sa budeme pripájať na zariadenie uložene v LAN sieti.



Troubleshooting and Advanced Customer Manual



Obrázok 10 Vopred definované aplikácie

3.1.2.2 DMZ

V hlavnom hornom menu kliknite na záložku Forward Rules. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "DMZ Configuration". Pre vytvorenie nového pravidla kliknite na tlačidlo "New".

	HG8	245	5W5	;					L	ogout
HUAWEI	Status	WAN	LAN IF	v6 WLA	N Security	Forward Ru	les Network Application	System [*]	Fools	
PCP Configuration		F	orward R	tules > DM	Z Configurati	on				
DMZ Configuration										
Port Mapping Config	uration		On thi	s page, you	i can configu	re DMZ parame	eters. The DMZ device restric	ts unreliab	e external connections from linking u	p to
Port Trigger Configu	ration		table,	the applica	tion requests	from the WAN	connection are forwarded to	the DMZ d	evice.	9
									New [Delete
					WAN Na	me	Enable DMZ		Host Address	
			Enable	DMZ:						
			WAN N	lame:		1_INTERNE	T_R_VID_836	T		
			Host A	ddress:		192.168.100.	2	* Lu	boThinkpad 🔹	
						Apply Can	cel			

Obrázok 11 Vytvorenie novej DMZ

Enable DMZ – zapnutie/vypnutie DMZ pravidla

WAN Name - Meno pripojenia

Host Address – IP adresa zariadenia ktoré má byť umiestnené v DMZ, je odporúčané zariadeniu určiť statickú adresu



Pozn. Pokial' je FTP server umiestnený v DMZ, tak pre jeho správne fungovanie v tejto konfigurácii je dôležité nastaviť číslo portu na ktorom počúva na iné ako 21. Porty 21, 80 a 443 sú použité na interné účely v ONT takže servery v LAN ktoré poskytujú služby FTP, HTTP alebo HTTPS musia pre účely DMZ bežať na iných portoch.

3.2 IPv6

3.2.1 Port Mapping Configuration

Pre IPv6 konfiguráciu v hlavnom hornom menu kliknite na IPv6 záložku. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "Port Mapping Configuration". Na tejto stránke môžete vytvárať pravidlá, ktoré budú uplatnené v IPv6 Firewale. Pre vytvorenie nového pravidla kliknite na tlačidlo "New". Ako môžete vidieť na *Obr. 12*..

HG82 4	5 W	5 W5 L										
HUAWEI Status WAN	I LAN	IPv6 WLAN Security	Forward Rules Netw	ork Application System	Tools							
LAN Address Configuration	IPv6 >	Port Mapping Configuration										
DHCPv6 Static IP Configuration												
Firewall Configuration	Or	On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to access the Internet. Note: 1) The well-known ports for voice services cannot be in the range of the mapping ports.										
Port Mapping Configuration	No											
IP Filter Configuration		2) The conligured port fila	pping rule takes ellect o	niy alter the involuewall co	ntroi on packet forwarding is	enableu.						
						New Delete						
		Mapping Name	WAN Name	Internal Host	External Host	Enable						

Obrázok 12 Nastavenie port mapping pravidla pre IPv6

V otvorenom menu na vytvorenie nového pravidla Obr. 13 si najskôr vyberte typ nastavenia:

User-Defined - manuálne vyplnenie položiek v menu "Add"

Application – menu doplní porty danej aplikácie na základe vybraného protokolu (pozrite aj *Obr. 14: Vopred definovane aplikácie.*).

Ďalej doplníme "Internal Host" a "External Source IP Address" do poľa "Internal Host" zadáme verejnú IPv6 adresu zariadenia. V našom pripade tam je IPv6 adresa zariadenia na ktorom je HTTP server Do poľa "External Source IP Address" zadáme verejnú adresu zariadenia s ktorého sa budeme pripájať na zariadenie uložené v LAN sieti. Ak "External Source IP Address" nevyplníte zariadenie bude dostupné z celého internetu. Na *Obr.13*. Môžeme vidieť vytvorenie pravidla pre HTTP komunikáciu pomocou Type – Application z ktorej sme si vybrali HTTP. Stránka nám automaticky doplní ďalšie potrebné nastavenia pre konkrétny HTTP protokol.

orange [™]		Troubleshoo	oting and Aa	lvanced Custon	ner Manı
HG824	45W5				Logout
HUAWEI Status WA	N LAN IPv6 WLAN Securi	ity Forward Rules Network	Application System	n Tools	
LAN Address Configuration	IPv6 > Port Mapping Configuratio	n			
DHCPv6 Static IP Configuration					
Firewall Configuration	On this page, you can set por	t mapping parameters to set up	o virtual servers on the	LAN network and allow these	e servers to
Port Mapping Configuration	Note: 1) The well-known ports	s for voice services cannot be in	n the range of the mapp	ping ports.	
IP Filter Configuration	2) The configured port	mapping rule takes effect only	after the IPv6 firewall c	ontrol on packet forwarding is	s enabled.
					New Delete
	Mapping Name	WAN Name	Internal Host	External Host	Enable
	Type:	User-defined • Applica	ation		
	Application:	Web Server (HTTP) V]		
	Enable Port Mapping:	v			
	Mapping Name:	HTTP_name]		
	WAN Name:	1_IPTV_INTERNET_R_' V]		
	Internal Host:	2a01:c846:f40:300:fc43:510	1:715d:a346	LuboThinkpad	'
	External Source IP Address:]]	
	Protocol:	TCP	Port number:	80 8) *
	Delete				
	Add				
					Apply Cancel

Obrázok 13 Vytvorenie nového pravidla.

Select
Domain Name Server (DNS)
FTP Server
IPSEC
Mail (POP3)
Mail (SMTP)
PPTP
Real Player 8 Plus
Secure Shell Server (SSH)
Secure Web Server (HTTPS)
SNMP
SNMP Trap
Telnet Server
TFTP Server
TFTP
Web Server (HTTP)

Obrázok 14 Vopred definovane aplikácie

Na poslednom obrázku môžete vidieť vytvorené pravidlo, ktoré povoľuje HTTP komunikáciu na zariadenie umiestnené v LAN sieti.

orange [™]			Troubles	hooting an	nd Advanced Cu	stomer N	Лапиа
	HG824	5W5					Logout
HUAWEI	Status WAN	I LAN IPv6 WLAN	Security Forward Rules No	etwork Application	System Tools		
LAN Address Config	guration	IPv6 > Port Mapping Con	figuration				
DHCPv6 Static IP Co	onfiguration						
Firewall Configuration	on	On this page, you can access the Internet.	n set port mapping parameters to	set up virtual server	s on the LAN network and al	low these servers	s to
Port Mapping Config	guration	Note: 1) The well-kno	wn ports for voice services cann	ot be in the range of	the mapping ports.	warding is enable	bd
IP Filter Configuration	on	2) The comigu	red port mapping rule takes eller	ct only after the h vo	mewan control on packet for	warding is chable	su.
						New	Delete
		Mapping Name	WAN Name	I	nternal Host	External Host	Enable
		HTTP_name	1_IPTV_INTERNET_R_VID_8	37 2a01:c846:f40	:300:fc43:5101:715d:a346		Enable

Obrázok 15 Vytvorené pravidlo

3.2.2 IPv6 Firewall Configuration

V hlavnom hornom menu kliknite na IPv6 záložku. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti, z ktorých vyberieme "Firewall Configuration". Na tejto stránke môžete kliknutím alebo odkliknutim vypnúť a zapnúť Ipv6 firewall, ako môžete vidieť na *Obr.16*. Nastavenie firewalu potvrdíte stlačením tlačidla Apply. Firewall je v defaultnom nastavení zapnutý.

	HG8245W5								
HUAWEI	Status	WAN	LAN IPv6	WLAN	Security	Forward Rules	Network Application	System Tools	
LAN Address Config	juration	IP	v6 > Firewall	Configura	ition				
DHCPv6 Static IP Co	onfiguration								
Firewall Configuration	on		On this page	je, you ca	n set the er	able status of the	IPv6 firewall control on	packet forwarding	. The configured port mapping rule
Port Mapping Config	guration		und ir into	Ture ture	chect only		wai control on packet lo	warang is chable	-u.
IP Filter Configuration	on		Enable the	Pv6 firewa	all control	•			
			on packet fo	orwarding:		•			
						Apply Cancel			

Obrázok 16 Nastavenie IPv6 firewalu.

3.2.3 Filter Configuration

V hlavnom hornom menu kliknite na IPv6 záložku. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti z ktorých vyberieme "IP Filter Configuration". Na tejto stránke môžete vytvárať filtrovacie pravidlá, ktoré budú uplatnené v Ipv6 Firewale. Na stránke zakliknite "Enable IP Filter" pre zapnutie IP filtra. Položka Filter Mode označuje akým spôsobom budú uplatňované pravidlá, Blacklist zakáže prístup zadanej adrese a Whitelist povolí prístup len zadanej adrese. Ďalej na vytvorenie nového pravidla kliknite na tlačidlo "New". Ako môžete vidieť na *Obr. 17*



HG824	15W5 n lan <mark>IPv6</mark> wlan :	Security Forward Rules Ne	twork Application System Tools	Logout
LAN Address Configuration	IPv6 > IP Filter Configuration	on		
DHCPv6 Static IP Configuration				
Firewall Configuration	On this page, you can of	configure WAN-to-LAN filter to p	rohibit some WAN IP addresses from	accessing LAN. The configured IP
Port Mapping Configuration	inter fulle takes effect of	niy alter ir vo niewali control is e	nabled on packet forwarding.	
IP Filter Configuration	Enable IP Filter:	(Device forwarding perform	nance will deteriorate if the IP filterin	g function is enabled.)
	Filter Mode:	Blacklist •		
				New Delete
	Rule name	Protocol Direction	LAN-Side IP Address	WAN-Side IP Address
			-	

Obrázok 17 Vytvorenie filtrovacieho pravidla

Zadáme názov Filtrovacieho pravidla do poľa "Rule name". Toto pole je povinné. Ďalej zadáme do poľa "LAN-side IP Address" adresu alebo rozsah adries, ktoré chceme v LAN sieti blokovať. A do poľa "WAN-side IP Adress" zadáme adresu alebo rozsah adries, ktoré budú blokované pre zariadenia v LAN. Nastavenie filtra potvrdíte stlačením tlačidla "Apply".

HG824	5W5				Logout
HUAWEI Status WAN	LAN IPv6 WL	AN Security Forw	ard Rules Net	work Application System Tools	
LAN Address Configuration	IPv6 > IP Filter Confi	guration			
DHCPv6 Static IP Configuration					
Firewall Configuration	On this page, you	I can configure WAN-t	o-LAN filter to pr	ohibit some WAN IP addresses from	n accessing LAN. The configured IP
Port Mapping Configuration	liner fulle takes e	lect only alter if vo inc	swall control is er	labled on packet forwarding.	
IP Filter Configuration	Enable IP Filter:	(Device for	rwarding perform	nance will deteriorate if the IP filterin	g function is enabled.)
	Filter Mode:	Blacklist 🔻			
					New Delete
	Rule na	ne Protocol	Direction	LAN-Side IP Address	WAN-Side IP Address
	Rule name:	test_name	*		
	Protocol:	All	•		
	Direction:	Bidirectional	V		
	IP Mode	IP Prefix	T		
	LAN-Side IP Addr	ess: 2a01:c846:f4	0:300:fc43:510/1	28 (IPv6 add	dress/n 0 ≤ n ≤ 128)
	WAN-Side IP Add	ress:	/	(IPv6 add	dress/n 0 ≤ n ≤ 128)
		Apply Can	cel		

Obrázok 18 Vytvorenie filtrovacieho pravidla



V hlavnom hornom menu kliknite na záložku "Forward Rules". Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "PCP".

Po kliknutí na "New" vytvoríme nové pravidlo. V našom príklade je vytvorené pravidlo pre HTTP komunikáciu port 80. Počítač, pre ktorý je pravidlo vytvorené má pridelenú IPv4 adresu 192.168.100.6. Preto do poľa "Internal IPv4 Address" zadáme192.168.100.6. Do poľa "Required External IPv4 Address" môžete zadať adresu CGN, cez ktorú chcete na ONT zariadenie pristupovať. Ďalšie pole je "Required External Port" cez ktorého chcete pristupovať na ONT zariadenie. Tieto polia nie sú povinné. Nevyplnené polia znamenajú, že prístup na nastavený port bude z celého internetu.

	HG8	24	5W	5										Logout
HUAWEI	Status	WAN	LAN	IPv6	WLAN	Security	Forv	vard F	Rules Netw	ork Applicati	on System 1	Fools		
PCP Configuration			Forwar	d Rules	> PCP C	configurati	on							
DMZ Configuration														
Port Mapping Configu	iration		On	this pag	ge, you c	an set PC	P mappi	ing pa	irameters.					
Port Trigger Configura	ation													
													Ne	w Release
\triangleright					Config M	juration ode	Extern IPv4 Addre	nal 1 955	External Port	Internal Port	Protocol	Internal IPv4 Address	PCP Server Result Code	Allow PCP Port Proposal [Y/N]
											<< < 0/0	> >>	Page	Go
			Inte	rnal IPv	4 Addres	s:		192.	168.100.6	*				
			Inte	rnal Por	t			80		*(1-6	65535)			
			Prot	ocol:				TCF	> ▼ *					
			Req	uired E	xternal IP	v4 Addres	6 S :							
			Req	uired E	xternal P	ort:				(0-6	5535)			
			Allo	w PCP	Port Prop	osal:		Y۰	*					
								Арр	oly Cancel					

Obrázok 19 Vytvorenie nového PCP pravidla

Internal IPv4 Address - IPv4 adresa cieľa v LAN sieti

Internal port – port na ktorý je posielaná komunikácia

Protocol – komunikačný protokol TCP/UDP

Required External IPv4 Address – žiadaná externá IPv4 adresa

Required External Port - žiadaný externý port

Allow PCP Port Proposal – Y / N –> Yes/No



Po úspešnom vyjednaní parametrov ich uvidíme v kolónkach "External IPv4 Address" a "External Port" blikať načerveno.

MG8245W5								Logout			
HUAWEI	Status WA	N LAN	N IPv6	WLAN Securi	ty Forward F	Rules Netw	ork Applicat	ion System	Tools		
PCP Configuration		Forwa	ard Rules	> PCP Configura	ation						
DMZ Configuration											
Port Mapping Configu	uration	0	n this pag	ge, you can set P	CP mapping pa	rameters.					
Port Trigger Configura	ation										
										Ne	w Release
				Configuration Mode	External IPv4 Address	External Port	Internal Port	Protocol	Internal IPv4 Address	PCP Server Result Code	Allow PCP Port Proposal [Y/N]
				Manual	178.143.43.11	1801	80	TCP	192.168.100.6	Success	Y
								<< < 1/1	> >>	Page	Go

Obrázok 20 Vytvorenie nového PCP pravidla

3.2.5 Zmena prefixu

Orange Slovensko prideľuje zákazníkom prefix /56 (prvých 56 bitov z ľavej strany). Rozlišujeme Statický a Dynamický prefix pre zákazníka. V Statickom sa prefix /56 nemení ani po reštarte zariadenia ale pre Dynamický sa po každom reštarte, vyp./zap. zariadenia zmení delegovaný prefix /56.

Defaultné nastavenie je, že k delegovanému prefixu /56, zariadenie automaticky doplní + 8 núl (Subnet ID - 0). Viď na *Obr. 21*. Tento prefix /64 je pridelený pre zariadenia v LAN sieti.



Obrázok 21 Prefix

Zákazník si môže zmeniť svoj prefix /64 v LAN tým, že zmení Subnet ID. Alebo aktuálna verzia firmware umožňuje zmenu prefixu od /56 do /64.

3.2.5.1 Zmena Subnet ID

V záložkách kliknite na záložku IPv6 a v ľavom menu vyberte "LAN Address Configuration". Na tejto stránke *Obr.22.* v sekcii "Interface Address Information" zmeníme "Method of obtaning prefixes" z "WAN Agent" na "Static configuration". Objaví sa pridelený prefix od Orange Slovensko, ktorý budete meniť. V prefixe meníte posledné dve hexadecimálne číslice pred ::/64 v poli prefix (*POZOR ! Môžete zadávať len od 0 po 255 čo je v hexadecimálne sústave 00 až FF*). Na *Obr. 23.* môžete vidieť zmenu Subnet ID na hodnotu 50.

orange [™]		Troubleshooting an	nd Advanced Customer Manual
HG82	45W5		Logout
HUAWEI Status WA	AN LAN IPv6 WLAN Security	y Forward Rules Network Application	System Tools
LAN Address Configuration	IPv6 > LAN Address Configuration		
DHCPv6 Static IP Configuration			
Firewall Configuration	On this page, you can set IPv6	-related feature parameters.	
Port Mapping Configuration			
IP Filter Configuration	Interface Address Information	fo001	*
	Method of Obtaining Profivos:	WAN agent	
	Parent Profix:		•
	Child Prefix Mask:		*(IPv6 address/64)
	MTU:	1472	*(1280-1500)
			(120 100)
	DNS Information	DNO second	
	DINS Source on the LAN Side.	DNS agent	▼.
	Resource Allocation Informatio	on	
	Enable Route Advertisement:		
	Enable DHCPv6 Server:		
	Resource Allocation Mode:	Manual	•
	Address/Prefix Assignment Mode:	O DHCPv6 SLAAC	
	Other Information Assignment Mode:	● DHCPv6 ○ SLAAC	
	ULA information		
	ULA Mode:	Disabled	▼
		Apply Cancel	

Obrázok 22 Pôvodné nastavenia

Nastavenia vykonané v LAN sieti si môžete skontrolovať na pripojenom PC. Otvorenie príkazovom riadku (win + r), zadáte *cmd* a následne v príkazovom riadku *ipconfig*. Výsledok a zmenu nastavení nájdete v informáciách o interface, ktorým ste pripojený do LAN siete *Obr. 24*. Adresy budú obsahovať vami zvolený prefix. Tento prefix bude pridelený všetkým zariadeniam v LAN sieti.

Zmena SubnetID je perzistentná a zostane platná aj po reštarte zariadenia resp. v prípade Dynamického prefixu aj po pridelení nového /56 subnetu.

HG8245W5			Logout
HUAWEI Status WAN LAN IPv6	WLAN Security Forward Re	ules Network Application Sys	stem Tools
AN Address Configuration IPv6 > LAN Address Configuration	ddress Configuration		
DHCPv6 Static IP Configuration Firewall Configuration On this pa	ge, you can configure IPv6-related	feature parameters.	
Port Mapping Configuration Interface Ac	ddress Information		
IPv6 Addre	ss: fe80::1		*
Method of	obtaining prefixes: Static config	uration	
Prefix:	2a01:c846:17	′e:3400∷/64	*(IPv6 address/n 1 <= n <= 64)
Preferred p	eriod: 604800		*(600s to 4294967295s)
Valid period	d: 604800		*(600s to 4294967295s)
MTU:	1472		*(1280-1500)
DNS Inform	ation		
DNS source	e on the LAN side: DNS agent	•	
Resource A	llocation Information		
Enable rou	te advertisement: 🕑		
Enable DH	CPv6 server:		
Resource a	allocation mode: Manual	,	
Address/Pr Mode:	efix Assignment OHCPv6	SLAAC	
Other Infor Mode:	mation Assignment OHCPv6	SLAAC	
ULA inform	ation		
	Dischlad		

Obrázok 23 Zmena subnet ID

C:\Users\Test_PC_2>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix .: IPv6 Address
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix .: IPv6 Address

Obrázok 24 Kontrola subnet ID



3.2.6 Prístup z WAN

Pokiaľ v sekcii "Security" v lavom menu klikneme na "Device Access Control" a v časti WAN zaškrtneme checkbox pre daný druh pripojenia, umožníme tým pripojenie daného typu na zariadenie HGW-U z WAN pre všetky IP.

Ak chceme umožniť prístup len pre daný rozsah IP adries, tak pod "Wan-side Source Address Whitelist" klikneme na "new" a zadáme rozsah adries, ktorým chceme umožniť pripojenie. Pre aktivovanie nového Whitelist-u je potrebné mať zaškrtnutý checkbox "Enable the WAN-side Source Address Whitelist" a po nastavení rozsahu kliknúť na "Apply".

Defaultne je prístup z Wan umožnený len pre HTTP v sekcii "WAN Access Control Configuration" pre rozsah OSK 2a01:c840:0110:8003::/64. Tu môžeme pridať vlastný rozsah IP adries, ktoré sa môžu pripojiť a taktiež môžeme zvol<u>i</u>ť spôsob pripojenia zaškrtnutím príslušného checkboxu a stlačením "Apply".

HG82	45W5			Logout
HUAWEI Status WA	AN LAN IPv6 WLAN	Security Forward Rules Network	Application System Tools	
Firewall Level Configuration	Security > Device Access	Control		
IP Filter Configuration				
MAC Filter Configuration	On this page, you can	enable or disable permissions to acces	ss the device.	
WLAN MAC Filter Configuration				
URL Filter Configuration	LAN Service	O to oppose the device using ETD:		
Parental Control Configuration	Enable the LAN-side P	C to access the device using FTP.		
DoS Configuration	Enable the LAN-side P	C to access the device using FITF.		
Device Access Control	Enable the LAN-side P	C to access the device using SSH:		
WAN Access Control Configuration	Enable the EAR-side I	o to access the device using cont.		
	Wi-Fi Service			
	Enable devices on the	WI-FI side to access web pages:	✓	
	Enable the PC on the	WI-FI side to access the device using Te		
	WAN Service			
	Enable the WAN-side I	PC to access the device using FTP:		
	Enable the WAN-side I	PC to access the device using HTTP:		
	Enable the WAN-side I	PC to access the device using Telnet:		
	Enable the WAN-side I	PC to access the device using SSH:		
		Apply Cance	l	
	WAN-Side Source Add	ress Whitelist		
	Enable the WAN-side S	Source Address Whitelist:		
				New Delete
			Source IP Address Whitelist	
		213.151.192.0/24		
		85.237.225.128/26		
	Source IP Address:	213.151.192.0/24 *(A.B.0	C.D/E)	
		Apply Cancel		

Obrázok 25 Nastavenie prístupu z WAN



3.3 IPv4 and IPv6

3.3.1 MAC Filter

V hlavnom hornom menu kliknite na záložku "Security". Po načítaní stránky sa nám v ľavom menu zobrazia možnosti z ktorých vyberieme "WLAN MAC Filter Configuration" pre Wi-Fi a "MAC Filter Configuration" pre Ethernet.

HG824	5W5		Logout						
HUAWEI Status WAN	LAN IPv6 WLAN Security For	ward Rules Network Application System Tools							
Firewall Level Configuration	Security > WLAN MAC Filter Configuratio	in .							
IP Filter Configuration									
MAC Filter Configuration On this page, you can configure MAC filter to prohibit some PCs from accessing the Internet.									
WLAN MAC Filter Configuration									
URL Filter Configuration	Enable WLAN MAC Filter:								
Parental Control Configuration	Filter Mode:	Blacklist V							
DoS Configuration			New Delete						
Device Access Control	SSID Index	Source MAC Address							
WAN Access Control Configuration		-							

Obrázok 26 Vytvorenie nového filtrovacieho pravidla

Enable WLAN MAC Filter - zapíname alebo vypíname filter.

Filter Mode – Druh filtrovania

Whitelist – povoľuje prístup iba adresám v zozname

Blacklist – zakazuje prístup adresám zo zoznamu

Pre vytvorenie nového záznamu klikneme na "New"

SSID Index – Názov siete pre ktorú chceme pravidlo vytvoriť (len pre Wi-Fi)

Source MAC Address - MAC adresa zariadenia na ktoré chceme aplikovať pravidlo

3.3.2 Smart Wi-Fi

Smart wifi je aplikácia, ktorá umožnuje pripojiť do LAN ONT viac ako jeden bezdrôtový prístupný bod (Access point) a následne prepínať medzi nimi tak, aby sa PC alebo telefón vždy pripojil na Access point so silnejším signálom respektíve podľa definovaných nastavení.

TBD (Táto časť manuálu bude doplnená)





3.3.3 Parental Control

V hlavnom menu kliknite na záložku "Security". Po načítaní stránky sa nám v ľavom menu zobrazia možnosti z ktorých vyberieme "Parental Control Configuration". V strede stránky sa zobrazia tri možnosti: "Overview", "Template" a "Statistics". Kliknite na možnosť "Template", potom na "New".

HG824	5W5		Logout							
HUAWEI Status WAN	I LAN IPv6 WLAN Security	Forward Rules Network Application System Tools								
Firewall Level Configuration	Security > Parental Control Config	juration								
IP Filter Configuration										
MAC Filter Configuration	On this page, you can set Inte	ernet access restrictions to allow your kids to use the Internet safely without direct set the times when your kids can use the Internet and which websites they can	ct supervision.							
WLAN MAC Filter Configuration	Tarentai control allows you to	set the times when your hus can use the internet and which websites they can	access.							
URL Filter Configuration	Overview Template S	Overview Template Statistics Help								
Parental Control Configuration										
DoS Configuration	Templata	Whather Dound to a Douise	New Delete							
Device Access Control		whether Bound to a Device								
WAN Access Control Configuration	Step 1: Specify the template n	ame and validity period.								
	Template									
	Template	Nazov_Template *								
	Template validation period									
	Template validation period									
	Start Date									
	Expiration Date									
			Next							

Obrázok 27 Smart Wi-Fi Template

Do kolónky Template zadajte názov nového Template. Pokiaľ chcete aby pravidlo platilo len po určitú dobu zaškrtnite checkbox "Template validation period" a do políčka "Start Date" zadajte odkedy a do políčka "Expiration Date" dokedy má dané pravidlo platiť. Kliknite na "Next" a následne na "new". Tu si môžete vybrať, či bude pravidlo platiť celý deň alebo iba vo vybrané hodiny a taktiež dni, počas ktorých sa pravidlo bude pravidelne aplikovať. Kliknite na "next" a následne na "new". Ak chcete zakázať nejakú internetovú stránku (napr. www.facebook.com), zaškrtnite checkbox "Enable website filter" a do políčka "URL Address" zadajte Vami vybranú stránku, na ktorú nechcete umožniť prístup. Kliknite na "Finish" a následne na možnosť "Overview". Po kliknutí na "new" sa zobrazí nasledovná stránka.



Obrázok 28 Smart Wi-Fi Overview

Pokiaľ sa má pravidlo vzťahovať na všetky PC v LAN zaškrtnite "Apply on all devices". V opačnom prípade do kolónky "Specified Device" kliknite na šípku (Popup) a podľa mena PC alebo podľa MAC adresy vyberte počítač, na ktorý sa má pravidlo vzťahovať. Do kolónky "Device Description" môžete dať počítaču prezývku (napr. Michalov_PC). V kolónke "Template" vyberte Vami vytvorený Tamplate a kliknite na "Apply".

Ak chcete vidieť koľkokrát sa PC snažil pripojiť na Vami zakázanú IP alebo vo Vami zakázanej dobe, kliknite na "Statistics".

Po kliknutí na možnosť "Overview" sa zobrazí zoznam zariadení pre ktoré bol nastavený parental control a ku každému vybraný Template.

3.3.4 Guest Wi-Fi

Guest wifi je bezdrôtový prístup do LAN zariadenia pre neautentifikovaných užívateľov, akými sú napríklad hostia. Takýto užívatelia po zadaní hesla budú mať prístup na internet, avšak s obmedzeniami vyplývajúcimi podľa Vášho nastavenia. Napríklad nebudú mať prístup k zmene nastavení zariadenia, alebo k iným užívateľom.

V hlavnom hornom menu kliknite na záložku WLAN. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti, z ktorých vyberieme "Guest Wi-Fi". Po zaškrtnutí Checkboxu "Enable Guest WiFi Network" sa zobrazia nové kolónky. Do kolónky s názvom "Guest access Password" zadajte heslo, ktorým chcete, aby sa hostia autentikfikovali pri pripojení na Guest Wi-Fi. Dobu pripojenia možeme obmedziť v "Activation time limit", kde možeme vybrať ľubovoľný čas v rozsahu 24 až 168 hodín.

orange [™]		Troubleshooting and Advanced Customer N	/anual
HG824	45W5		Logout
HUAWEI Status WA	N LAN IPv6 WLAN Security Fo	rward Rules Network Application System Tools	
2.4G Basic Network Settings	WLAN > Guest Wi-Fi		
2.4G Advanced Network Settings			
5G Basic Network Settings	On this page, you can set basic para	ameters of a guest network.	
5G Advanced Network Settings			
Automatic Wi-Fi Shutdown	Enable Guest Wi-Fi Network		
Wi-Fi Coverage Management	Guest access SSID:	Guestx4SM7Q	
Guest Wi-Fi	Guest access password:	Display characters	
	Activation time limit:	24 Hours, range 24-168	
	Enable Connectivity among Wi-Fi	clients in Guest SSID	
	Host IP Address	192.168.2.1 *	
	Host Subnet Mask	255.255.255.0 *	
	Start IP address:	192.168.2.2 *	
	End IP address:	192.168.2.254 *	
	Lease Time	1 hours 🔻	
		Apply Cancel	

Obrázok 29Nastavenie Guest Wi-Fi

3.3.5 Wi-Fi automatic shutdown

V hlavnom hornom menu kliknite na záložku WLAN. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti, z ktorých vyberieme "Automatic WiFi Shutdown". Checkbox "Enable automatic WiFi shutdown" musí byť zaškrtnutý. V kolónke "Start" zadáme hodinu a minútu, v ktorej sa má WiFi vypnúť a v kolónke "End" zase hodinu a minútu, kedy sa WiFi znovu zapne. Napravo od času si vyberieme dni, v ktorých má príslušné pravidlo platiť a potvrdíme tlačidlom "Apply".

HG82	45W5								Logout
HUAWEI Status WA	N LAN IPv6 WL	AN Security	Forward Rule	s Network	Application	System To	ols		
2.4G Basic Network Settings	WLAN > Automatic V	Vi-Fi Shutdown							
2.4G Advanced Network Settings									
5G Basic Network Settings	On this page, yo	u can enable aut	omatic Wi-Fi sl	hutdown in a	specified per	iod as requir	ed.		
5G Advanced Network Settings									
Automatic Wi-Fi Shutdown	Automatic Shutdo	own Configuration	on						
Automatic Wi-Fi Shutdown Automatic Shutdown Configuration Wi-Fi Coverage Management Image: Enable automatic Wi-Fi shutdown									
Guest Wi-Fi	Start	End	Mon	Tues	Wed	Thur	Fri	Sat	Sun
	1 22 : 00	6 : 00	1		\$	1	\$		
	2 00 : 00	5 : 00							
	3 :								
	4 :	:							
		Α	pply Cance						

Obrázok 30 Nastavenie automatic Wi-Fi shutdown



3.3.6 Firewall

Defaultne nastavená úroveň firewall-u je User-defined. Pokiaľ chcete jeho úroveň zmeniť, v hlavnom hornom menu kliknite na záložku Security. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "Firewall Level Configuration". V časti Firewall Level si môžeme z lišty vybrať niekoľko úrovní firewallu. Výber je treba potvrdiť tlačidlom Apply.. V nižšie uvedených tabuľkách sú uvedené všetky stupne firewall-u a k nim sprístupnené protokoly, pričom krížik znamená, že

protokol pri danej úrovni firewall-u nie je povolený.

- 1	IG82	45W	5						Logout
HUAWEI	Status WA	N LAN	IPv6	WLAN	Security	Forward Rules	Network Application	System Tools	
Firewall Level Configurati	ion	Security	/ > Fire	wall Leve	I Configurat	ion			
IP Filter Configuration									
MAC Filter Configuration		On	this pa	ge, you c	an configure	the firewall level.			
WLAN MAC Filter Configu	iration								
URL Filter Configuration		Curr	ent Fire	ewall Leve	el:		User-defined		
Parental Control Configur	ration	Fire	wall Lev	/el:			User-defined v		
DoS Configuration		i					Apply		
Device Access Control									
WAN Access Control Con	figuration								

Firewall			T	WAN->ON	Γ		
level	Stateful Firewall	PING	ACS	НТТР	FTP	Telnet	Other
High	<	×	~	×	×	×	×
Medium	<	×	~	×	×	×	×
Low	~	×	~	×	~	×	×
User- define	<	×	~	×	×	×	×
Disable	~	~	~	×	~	~	 ✓

Obrázok 31 Nastavenie úrovní firewallu

orange[™]

Troubleshooting and Advanced Customer Manual

Firewall	LAN->ONT											
level	HTTP	Telnet&PING	FTP	DNS&DHCP	Other							
High	>	×	×	 Image: A set of the set of the	×							
Medium	~	 ✓ 	×	 ✓ 	×							
Low	~	 ✓ 	×	 ✓ 	×							
User- defined	~	 ✓ 	×	~	~							
Disable	~	 ✓ 	~	 ✓ 	~							

Einernell level	LAN->WA	AN
Firewall level	FTP&HTTP(S)&DNS	Other
High	 ✓ 	×
Medium	V	 ✓
Low	 ✓ 	 ✓
User-define	 ✓ 	 ✓
Disable	 ✓ 	 ✓

3.3.7 Reštart zariadenia

V hlavnom hornom menu kliknite na záložku System Tools. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "Reboot". Po kliknutí na tlačidlo Restart sa zariadenie reštartuje.

	HG8	324	5W	5						Logout
HUAWEI	Status	WAN	LAN	IPv6	WLAN	Security	Forward Rules	Network Application	System Tools	
Restart		:	System	Tools ?	Restart					
Configuration File										
Restore Default Conf	iguration		On	this pa	ge, you c	an restart f	the device.			
Maintenance										
User Log			Rest	art						
Firewall Log										
ONT Authentication										
Advanced Power Mar	nagement									
Modify Login Passwo	ord									
Indicator Status Mana	agement									
Open Source Softwar	re Notice									

Obrázok 32 Stránka na reštart zariadenia



3.3.8 Obnovenie továrenských nastavení

V hlavnom hornom menu kliknite na záložku System Tools. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "Restore Default Configuration". Po kliknutí na tlačidlo Default sa na zariadení obnovia továrenské nastavenia.

	HG82	45W5					Logout
HUAWEI	Status WA	AN LAN IPv6	WLAN Secu	ity Forward Rules	Network Application	System Tools	
Restart		System Tools	> Restore Defau	t Configuration			
Configuration File							
Restore Default Con	figuration	On this p	age, you can rest	ore the default setting	JS.		
Maintenance							
User Log		Default					
Firewall Log							
ONT Authentication							
Advanced Power Ma	inagement						
Modify Login Passw	ord						
Indicator Status Man	nagement						
Open Source Softwa	re Notice						

Obrázok 33 Stránka na uvedenie zariadenia do továrenských nastavení

3.3.9 Zmena prihlasovacieho hesla

V hlavnom hornom menu kliknite na záložku "System Tools". Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme "Modify Login Password". Na stránke v časti "Change Password" nastavíme nové heslo.

	HG8	24	5W	5						Logout
HUAWEI	Status	WAN	LAN	IPv6	WLAN	Security	Forward Rules	Network Application	System Tools	
Restart			System	Tools :	> Modify I	.ogin Pass	word			
Configuration File										
Configuration File On this page, you can change the password of the current login user to ensure security and make it easy to remember. Maintenance User Name: root 1. The password must contain at least 6 characters. Direct Log Old Password: Old Password: Old Password:						er.				
Maintenance										
User Log			Use	r Name	C.	root		1. The password mus	st contain at least 6 characters.	nations:
Firewall Log			Old	Passw	ord:			digits, uppercase le	etters, lowercase letters	
ONT Authentication			New	v Passv	vord:			and special character \$ % ^ & * () = + \	<pre>cters. Special characters can be the following [[{}];:'"<,.>/?.</pre>	;`~!@#
Advanced Power Mar	agement		Con	ifirm Pa	ssword:			3. The password can	not be any user name or user name in rever	se order.
Modify Login Passwo	rd						Apply Cancel			
Indicator Status Mana	igement									
Open Source Softwar	e Notice									

Obrázok 34 Stránka na zmenu prihlasovacieho hesla



New Password – nové heslo

Confirm Password - potvrdenie hesla

Nové heslo musí mať minimálne 6 znakov, musí obsahovať minimálne dve

- 1. z nasledujúcich: číslo
- 2. veľké písmeno, malé písmeno
- 3. špeciálny znak: `~!@#\$%^&*()-_=+\|[{ }];:'"<,.>/?

3.3.10 Firewall záznamy

FireWall záznam sa rovnako ako systémový záznam nachádza v menu *System Tools*. Zaznamenáva sa 100 výpisov, ktoré sa radia systémom FIFO. V jednoduchosti sa dá tvrdiť, že sa ukladá 100 najaktuálnejších výpisov. Pri zvýšenom zaťažení zariadenia môže zachytávanie výpisov Firewall záznamu znižovať rýchlosť posielania dát.

Je možné súčasne aplikovať štyri smery *Firewall-u: From Internet to LAN, From Internet to local, From LAN to Internet* a *From LAN to local.* Pri každom smere je na výber uplatniť tzv. *Log Rule Action*, či sa jedná o povolený (*Accept*) alebo zamietnutý (*Reject*) typ akcie samotným Firewallom zariadenia. Z toho vyplýva, že maximálny počet kombinácií smerov a typov akcie Firewall záznamov je limitovaný na 8. Pri vytváraní väčšieho počtu je užívateľ touto skutočnosťou oboznámený vyskočením príslušného okna.

Pri systémových hláseniach sa zaznamenávajú všetky druhy hlásenia a je na užívateľovi, aký druh hlásenia chce zobraziť, prípadne uložiť si do počítača. Pri *Firewall Log*-och však treba vytvoriť príslušný druh záznamu, ktorý sa bude následne zaznamenávať. Je možné súčasne aplikovať všetkých spomínaných 8 druhov.

orange [™]				Tr	oubleshooting and	Advanced Custo	omer Ma	anud
	HG824	5W5	5				Lo	ogout
HUAWEI	Status WAN	LAN I	Pv6 WLAN Sec	curity Forward F	Rules Network Application Sys	stem Tools		
Restart	1	System T	ools > Firewall Log					
Configuration File								
Restore Default Confi	guration	On th	is page, you can c	onfigure, downloa	d, and query a firewall log.			
Maintenance								
User Log		Enable	e Firewall Log	(If enabled, o	levice forwarding performance will b	e deteriorated.)		
Firewall Log							New De	elete
ONT Authentication			Log Ru	le Status	Log Access Direction	n Log F	Rule Action	
Advanced Power Man	agement		Enabled		From Internet to LAN	Accept		
Modify Login Passwo	rd	Enable	e Log Rule:					
Indicator Status Mana	igement	Log A	ccess Direction:	From Internet to	DLAN 🔻 *			
Open Source Softwar	e Notice	Log R	ule Action:	Accept • *				
				Apply Cancel				
		Downlo	ad and View Log	s				
		Downl	oad Log File					
		Manufa Produc SerialN IP:10.3 HWVer SWVer	acturer:Huawei Tec tClass:HG8245W5 lumber:485754434 4.0.177; :HWTCA163DA; :HWTCA51910110	hnologies Co., Ltd ; 1F8AC9F; ;	t;			

Obrázok 35: Voľba smerov a typ akcie Firewall záznamu

Pri zobrazenom *Firewall* zázname v GUI zariadenia sa nezobrazujú údaje v reálnom čase. Pre zobrazenie aktuálne doposiaľ zachyteného záznamu je nutné opätovne načítať stránku pre Firewall záznam. Pri stiahnutí do počítača sa vždy uloží najaktuálnejší záznam <u>nehľadiac</u> na zobrazovanú skutočnosť v GUI zariadenia.