PAKEDGEDEVICE&SOFTWARE INC.

K60D

PRECONFIGURED AUDIO/VIDEO BRIDGING ROUTER

USER MANUAL

VERSION 1.1

FCC Declaration of Conformity

Pakedge Device & Software, Inc., 3847 Breakwater Avenue, Hayward, CA, declares under sole responsibility that the R60D comply with 47 CFR Parts 2 and 15 of the FCC Rules as a Class B digital device. These devices comply with Part 15 of FCC Rules. Operation of the devices is subject to the following two conditions: (1) These devices may not cause harmful interference, and (2) these devices must accept any interference that may cause undesired operation.

WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. THE UNIT MUST NOT BE EXPOSED TO DRIPPING OR SPLASHING WATER. CAUTION: DO NOT OPEN THE UNIT. DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL. CAUTION: THIS DEVICE MUST BE INSTALLED AND USED IN STRICT ACCORDANCE WITH THE MANUFACTURER'S INSTRUCTIONS AS DESCRIBED IN THE USER DOCUMENTATION THAT COMES WITH THE PRODUCT. WARNING: POSTPONE INSTALLATION UNTIL THERE IS NO RISK OF THUNDERSTORM OR LIGHTNING ACTIVITY IN THE AREA.

SAFETY PRECAUTIONS:

When using this device, always follow basic safety precautions to reduce the risk of fire, electric shock, and injury to persons, including the following:

- Comply with all warning and caution statements in the instructions.
- Retain instructions for future reference.
- Observe all warning and caution symbols that are affixed to this equipment.
- Comply with all instructions that accompany this equipment.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.
- Installation of this product must be in accordance with national wiring codes and must conform to local regulations.
- Avoid using this product during an electrical storm. There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug the power supply and disconnect the CAT5e. This will prevent damage to the product due to lightning and power surges.
- Give particular attention to all safety precautions.
- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure what type of power is supplied to your home, consult your dealer or local power company.
- It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damage to the equipment from lightning strikes and other electrical surges.
- Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use compressed air to remove dust.
- Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.
- Do not directly cover the device or block the airflow to the device with insulation or any other objects.

CONTENTS

INTRODUCTION

The popularity and affordability of IP networking has driven audio/video and control networks to share the same physical wiring with computer networks. However, computer data can tolerate unpredictable latency in ways that audio/video streaming and control systems cannot. Sophisticated systems require the same robustness as an enterprise network, ensuring that IP-based controls occur instantly and audio/video packets arrive in time.

Note: **If this is your first time installing this product, please read this manual in its entirety.**

Preset IP Address Values: The K60D is preconfigured for "out-of-box" VLAN installations. Therefore, the IP addresses of all VLANs are predefined. Please note that changing IP addresses may affect other preconfigured features. Contact Pakedge support for more information.

****Warning****

Factory Reset: Pakedge does not recommend performing a factory reset unless absolutely necessary. If you would like to reset the device, please contact technical support at: support@pakedge.com or (650)385-8703.

NOTE: Using the router's hardware reset button will erase all Pakedge configurations and make the device unreliable on your network.

CUSTOMER SERVICE AND TECHNICAL SUPPORT

Pakedge Device & Software, Inc. is committed to providing you with exceptional support on all of our products. If you wish to speak with one of our representatives, you may contact us at:

Customer Service

Email: **customerservice@pakedge.com**

Phone: (**650)385-8701**

Technical Support

Email: **support@pakedge.com**

Phone: (**650)385-8703**

Website: **www.pakedge.com**

Visit our website for up-to-date support information.

Please be prepared to provide your product's model and serial number when contacting Pakedge Support. Your model and serial numbers are printed on a label located on the electronic housing.

Pakedge Device & Software, Inc.

3847 Breakwater Avenue

Hayward, CA 94545

USA

INSTALLING

For installation procedures, please refer to the Quick Start Guide that came with the K60D. You can also visit the Dealer Portal on our website for all the current manuals and Quick Start Guides.

NOTE: If you install the K60D in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room temperature. Make sure you install the equipment somewhere within the recommended temperature range.

For rack installations, make sure that the amount of air flow required for safe operation of the equipment is not compromised.

For free-standing installation, make sure that the R60D has at least 1.5 in. (3.75cm) of clearance on each side to allow for adequate air flow and cooling.

CONNECTING TO THE INTERNET

The K60D supports the three main types of internet connections:

- **DHCP** (typically used by cable companies and DSL basic service)
- **Static IP** (fixed public IP address mostly used by Business Class Broadband services)
- **PPPoE** (used by DSL companies such as AT&T)

Determine what type of internet connection you have from your Internet Service Provider (ISP), then follow one of the three instruction sets below to connect the router to the internet.

DHCP:

If your ISP uses DHCP, no configuration changes are necessary. The router already connects to the internet in DHCP mode by default.

Static IP:

To configure the router to a static IP, complete the following steps:

A. Determine the following information provided by the ISP:
   i. Your assigned IP address
   ii. Subnet mask
   iii. Default gateway
   iv. DNS server(s)
B. Plug your PC into any numbered port on the router using an Ethernet cable.
C. Open any internet browser on the PC and go to http://192.168.1.99.
D. Log in to the router using **pakedge / pakedgef** as the username and password.
E. Navigate to **Network** under **System** on the left-hand side of the screen and click on **Interface**.
F. Next, click on the **wan1** row. You should see the configuration page for **wan1**.
G. Start by selecting **Manual** under the **Addressing Mode** heading. Enter the IP address and subnet mask information provided by the ISP. Once you are done, hit **OK** at the bottom of the page.
H. Next, click on **DNS** under the **Network** heading.
I. Type in the DNS values that you received from your ISP under **Primary** and **Secondary DNS.** Hit **Apply**.
J. Navigate to the **Router** tab on the left and click **Static Route.**
K. Click **Create New** located right above the checkboxes.
L. In the **Gateway** field, type in the default gateway provided by the ISP and hit **OK**. Note: Make sure that the **Device** field is set to **wan1** and that the **Destination/IP Mask** field is set to **0.0.0.0/0.0.0.0**.
M. The router is now configured and ready for use.

PPPoE:

To configure the router using a PPPoE connection, you will need to complete the following steps:

A. Determine the following information provided by the ISP:
   i. PPPoE username
   ii. PPPoE password
B. Plug your PC into the router using an Ethernet cable.
C. Open any internet browser on the PC and go to http://192.168.1.99.
D. Log in to the router using **pakedge / pakedgef** as the username and password.
E. Navigate to **System -> Network** on the left-hand side of the screen and select **Interface**.
F. Next, click on **wan1**. You should see its configuration page.
G. Click on the **PPPoE** radio button under the **Addressing Mode** heading.
H. Enter the username and password information provided by the ISP. Hit **OK** at the bottom of the screen.
I. The router is now configured and ready for use. You can now access the internet.

PAKEDGE SUPPORTED FEATURES

The complex K60D router comes pre-configured for easy installation. In addition to basic configurations, Pakedge also supports the following features:

- **Changing Administrative Password**
- **Port Forwarding**
- **VPN**
- **Disabling DHCP on a VLAN**
- **Dual WAN Redundancy**
- **Dynamic DNS**
- **Changing Subnets**
- **DHCP Reservation**
- **DMZ**
- **Guest VLAN**
- **Universal Threat Management**
- **Device Discovery**
- **Disclaimer Page**

Each of these features is independent of one another and sequence of installation does not matter. Please visit the Dealer Portal of our website for the latest user manuals: http://pakedge.com/for-dealers-portal.html

The K60D is a kit that comes with the R60D router and the mounting kit. For the purposes of this manual, we will now refer to the router as the R60D.

NOTE: Pakedge does not support anything outside of the features/topics outlined in this manual. If you need more advanced features, please contact Pakedge Support for the complete Fortinet Administrator Guide.

GETTING TO KNOW YOUR PRODUCT

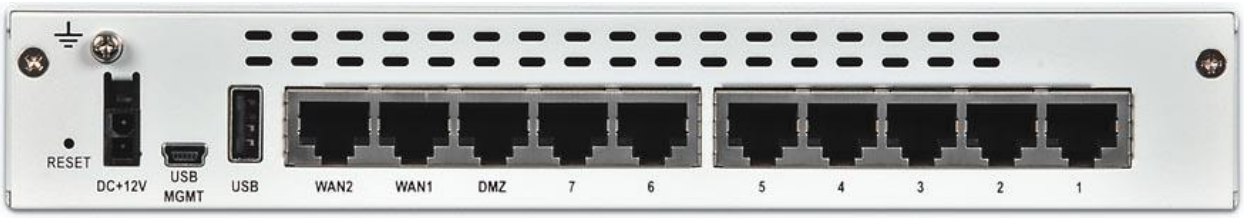
Package Contents:

R60D- Audio-Video Bridging Router
Mounting Brackets
Power Supply
Power Cable
1ft CAT5E Cable
Quick Start Guide

You will find a description of the LED lights on the front of the R60D router below. These lights appear on any of the preconfigured kits.

Front of router

LED	Status		Operation
POWER	Green		The router is powered on
	Off		The router is turned off
STATUS	Green		The unit is operating normally
	Off		The unit is off
HA	Green		Unit is being used in an HA cluster
Ports 1 – 7	LINK/ACT	Green	Port is online (link established)
		Flashing Green	Activity
	SPEED	Green	Connected at 1000 Mbps
		Amber	Connected at 100 Mbps
		Off	Connected at 10 Mbps
WAN1, WAN2, DMZ	LINK/ACT	Green	Port is online (link established)
		Flashing Green	Activity
	SPEED	Green	Connected at 1000Mbps
		Amber	Connected at 100 Mbps
		Off	Connected at 10 Mbps

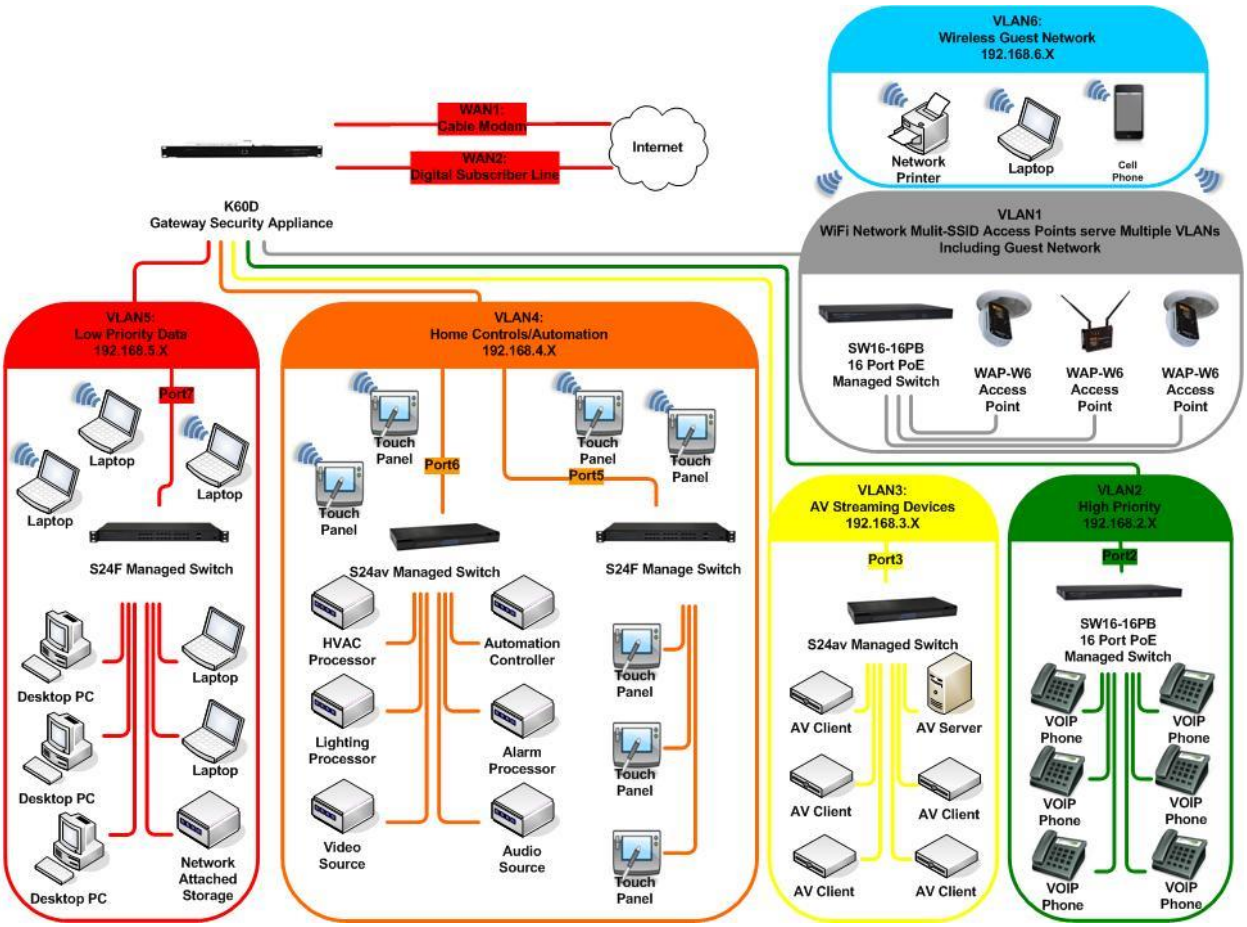


Back of router

The router ports are listed below.

Interface	Type	Speed	Protocol	Description
USB Management	Mini		USB	Client port for management.
CONSOLE	RJ-45	9600 bps	RS-232 serial	Optional connection to the management computer. Provides access to the command line interface (CLI). Note: The console port is located on the front of the R60D.
USB	USB A		USB	Optional connection for FortiUSB key, modem, or firmware backup and installation.
DMZ	RJ-45	10/100/1000	Ethernet	Optional connection to a DMZ network.
WAN1 and WAN 2	RJ-45	10/100/1000	Ethernet	Redundant connections to the Internet.
Internal	RJ-45	10/100/1000	Ethernet	7-port switch connections on the internal network.

The R60D comes preconfigured on VLANs 2-6, allowing you to isolate the traffic on various network devices. Below is an example of a network with multiple VLANs and their devices.



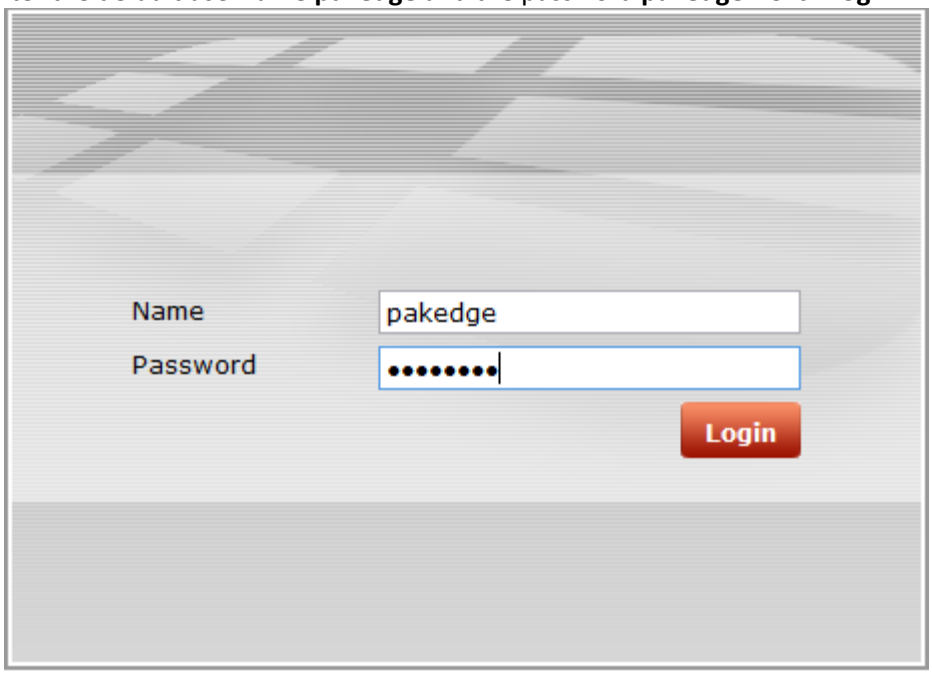
Pakedge Factory Default Settings for the K60D

R60D Username and Password		pakedge / pakedgef
Network	Internal Interface (VLAN1)	192.168.1.99 (Router Default IP Address)
	VLAN2	192.168.2.1
	VLAN3	192.168.3.1
	VLAN4	192.168.4.1
	VLAN5	192.168.5.1
	VLAN6	192.168.6.1
DHCP	WAN1 Interface	Dynamic IP Service
	WAN2 Interface	Dynamic IP Service
	DHCP Server on Internal Interface (VLAN1)	192.168.1.110 to 192.168.1.199
	DHCP VLAN 2	192.168.2.110 to 192.168.2.199
	DHCP VLAN 3	192.168.3.110 to 192.168.3.199
	DHCP VLAN 4	192.168.4.110 to 192.168.4.199
	DHCP VLAN 5	192.168.5.110 to 192.168.5.199
	DHCP VLAN 6	192.168.6.110 to 192.168.6.199

ACCESSING THE ROUTER

To access the router's GUI, please follow the steps below:

1. Plug an Ethernet cable from the router to a PC.
2. Make sure your network card is set to obtain an IP address automatically. Then open any internet browser (e.g. Mozilla, Chrome, etc.) and go to the address http://192.168.1.99.
3. Enter the default username **pakedge** and the password **pakedgef**. Click **Login**.



It is highly recommended that you change this default password. Please see the section titled Changing Administrative Password.

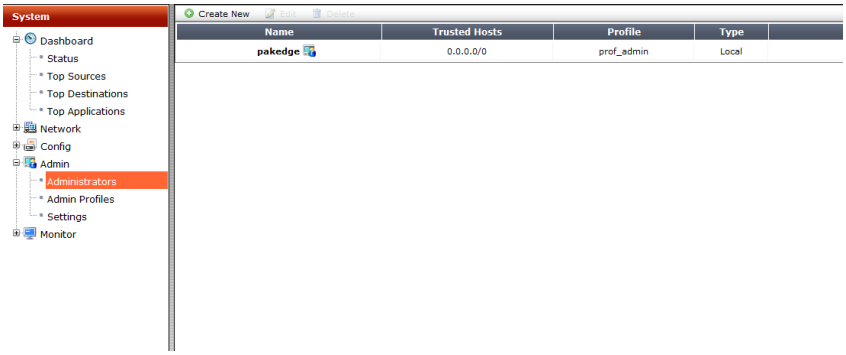
OVERVIEW

This manual will now focus on various configuration topics that were listed under the **Pakedge Support Features** section.

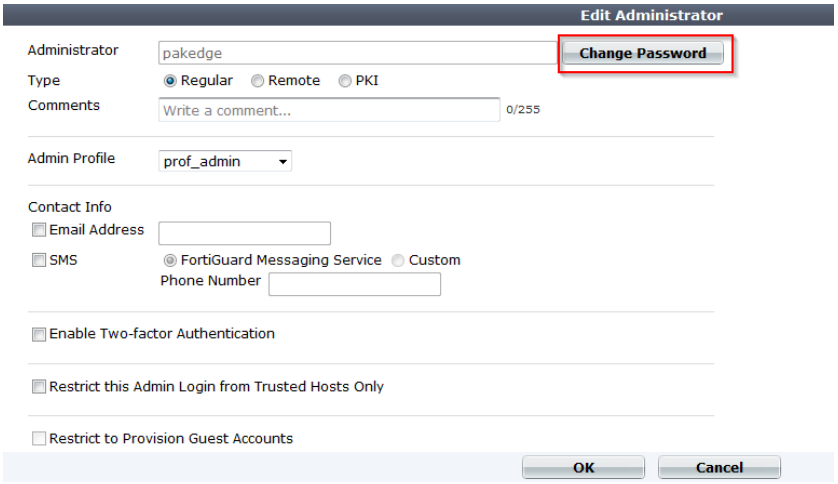
CHANGING ADMINISTRATIVE PASSWORD

It is strongly recommended that you change the default password for the R60D. To change the password, please take the following steps.

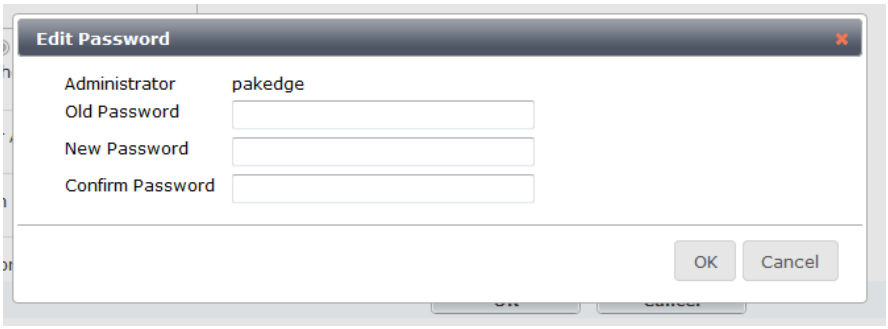
1. Log in to the router using the steps mentioned two sections ago under Accessing the Router. Then navigate to **System**->**Admin**->**Administrators**. Double-click the default **pakedge** username.



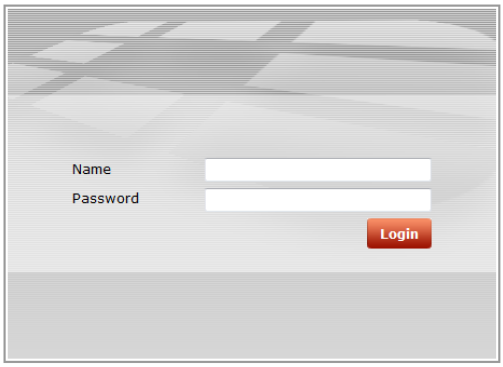
2. Click on **Change Password**.



3. Enter your password information. Click **OK**.



4. You will then be prompted to log in to the unit with the new password.

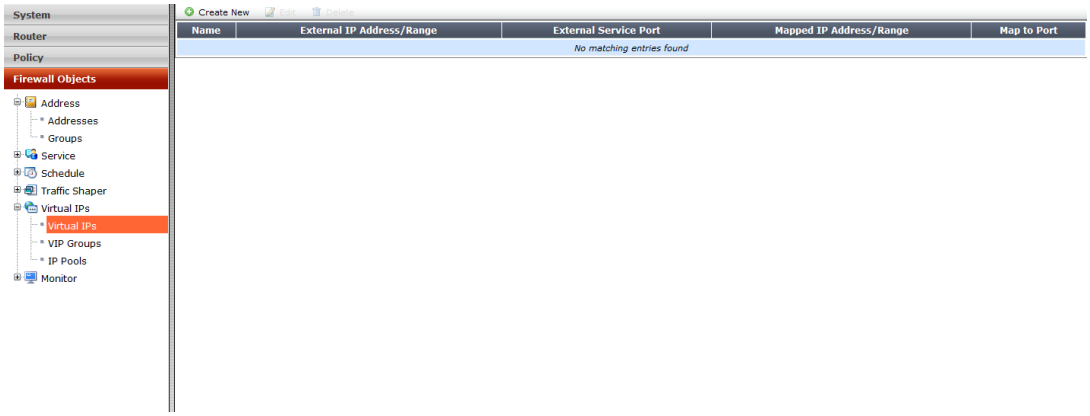


PORT FORWARDING

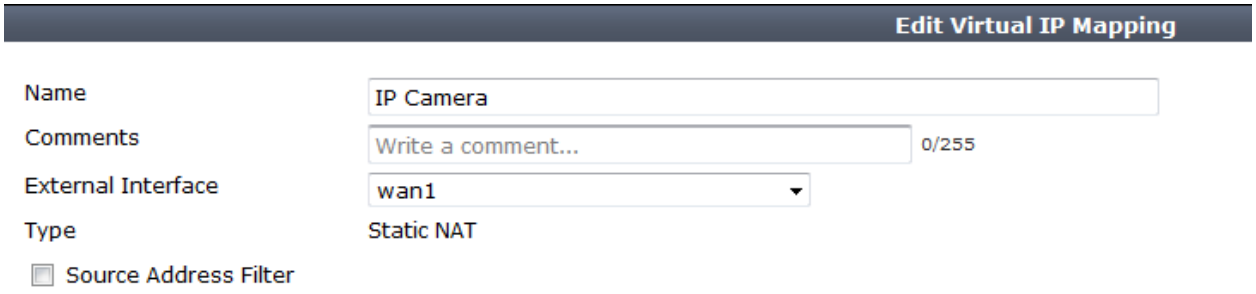
Port forwarding allows services inside the network to be available from the internet. If you have an IP camera on your network, port forwarding would allow you to remotely view the camera.

To configure port forwarding, please take the following steps.

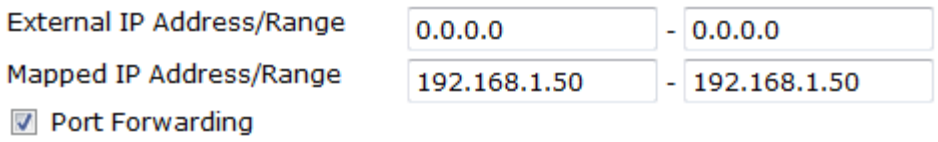
1. Navigate to **Firewall Objects**->**Virtual IPs**->**Virtual IPs**. Click **Create New**.



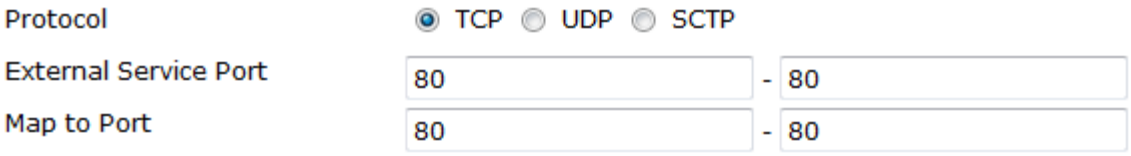
2. We will forward TCP port 80 to an IP camera on the IP address 192.168.1.50. Enter **IP Camera** as the name. Leave a brief description under the **Comments** section. Select the WAN port you are using for the **External Interface**. You can specify which public IP addresses would be allowed to use this virtual IP with the **Source Address Filter**, but we recommend leaving it unchecked.



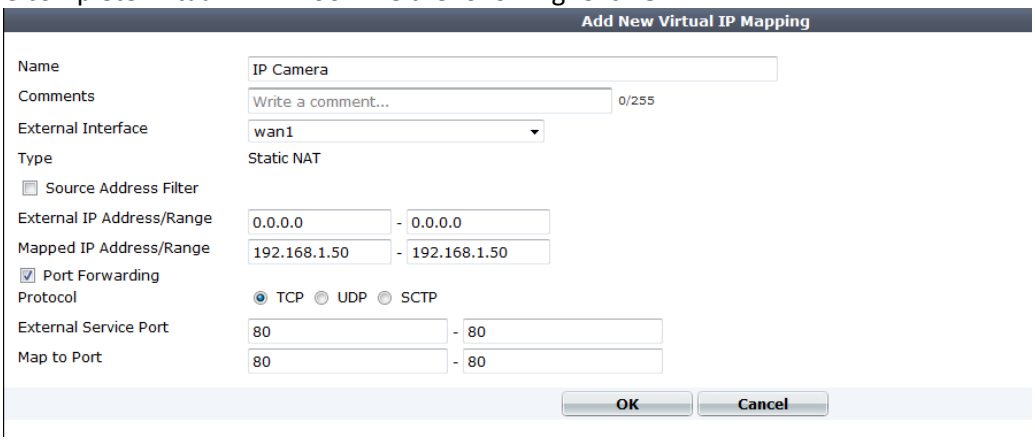
We will leave the **External IP Address/Range** as all 0's. This will tell the router to use the public IP address currently on the WAN port. We will enter the internal IP address of the device we are forwarding the port to under **Mapped IP Address/Range.** In our example, this is the IP address, so we will fill in 192.168.1.50. Check the **Port Forwarding** box.



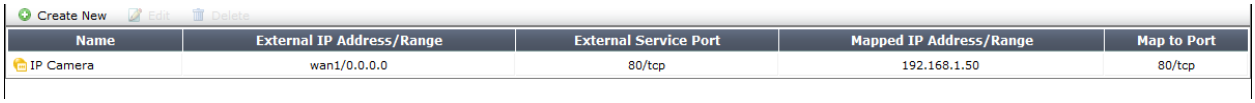
For **Protocol,** we will need to select either **TCP** and **UDP**. This will depend on the application you are using—TCP is recommended for web-browsing and emails, while UDP is recommended for VoIP and online games. In our example, we will select **TCP**. The **External Service Port** is the port that the traffic is coming into the router from. We will use port 80 in our example, which is most often used for HTTP. We will confirm it in the right-hand side box. **Map to Port** refers to the port that the traffic will use when it enters the internal network. In our example we will use **80**. We will also enter it in the right-hand side box.



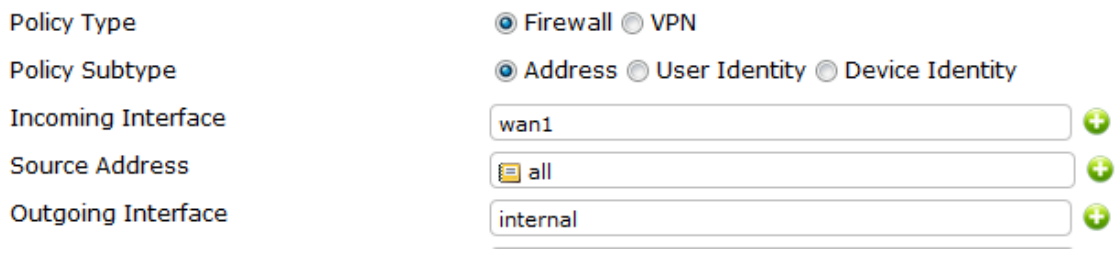
The complete virtual IP will look like the following. Click **OK**.



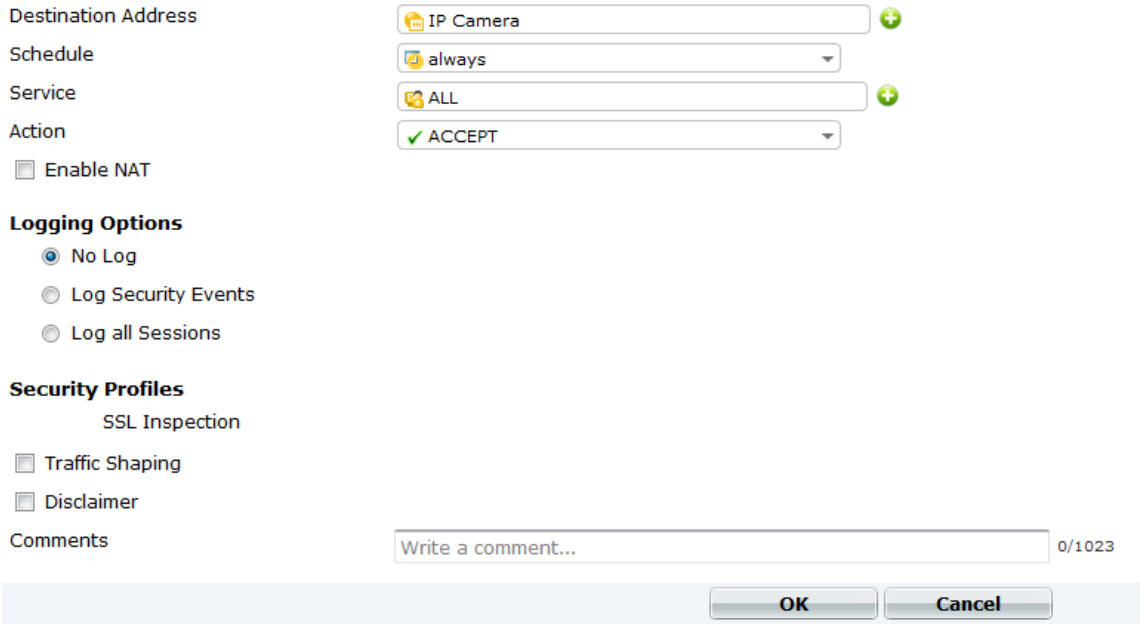
3. You should now see your Virtual IP listed.



4. Now we will need to create a policy for this Virtual IP. Navigate to **Policy**->**Policy**->**Policy**. Click **Create New**.
5. Select **Firewall** as the **Policy Type**. For the **Policy Subtype,** select **Address**. For the **Incoming Interface,** we will select the WAN port being used. We will use **wan1** in our example. Enter **All** as the **Source Address**. This will tell the router to allow connections from any public IPs through for this policy. **Outgoing Interface** refers to the interface the destination device is on. In our example, the IP camera is on the internal network so we will select **internal**.



The **Destination Address** is the device that we are forwarding the port to. In our example, we will select the virtual IP that we created earlier. **Schedule** allows us to select a time at which the policy will be active. In our example, we will select **always**. **Service** allows us to specify the allowed port for this policy. We select **ACCEPT** as the **Action**. The **Enable NAT** option would allow the router to perform a network address translation on this policy when the traffic is coming into the router from the internet. We normally don't need this so we will leave it unchecked. We will set the **Logging Options** to **No Log** and leave the **Traffic Shaping** and **Disclaimer** checkboxes unchecked. Click **OK**. Port Forwarding is now complete.



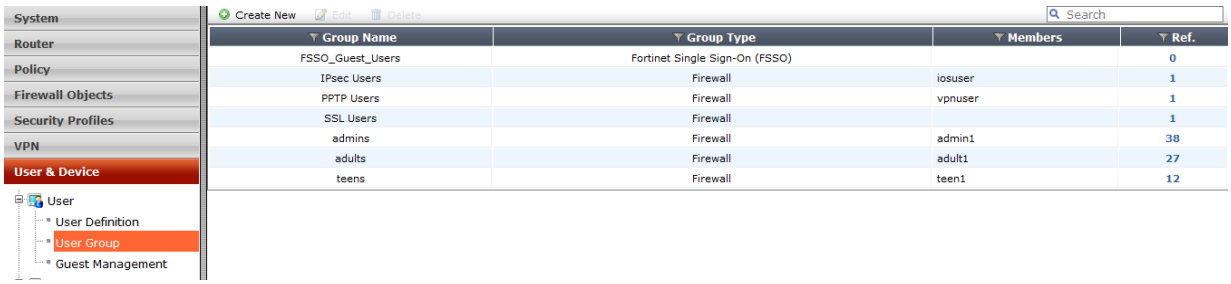
VPN

VPNs, or virtual private networks, allow you to remotely access your network. The R60D supports both SSL and PPTP VPN services.

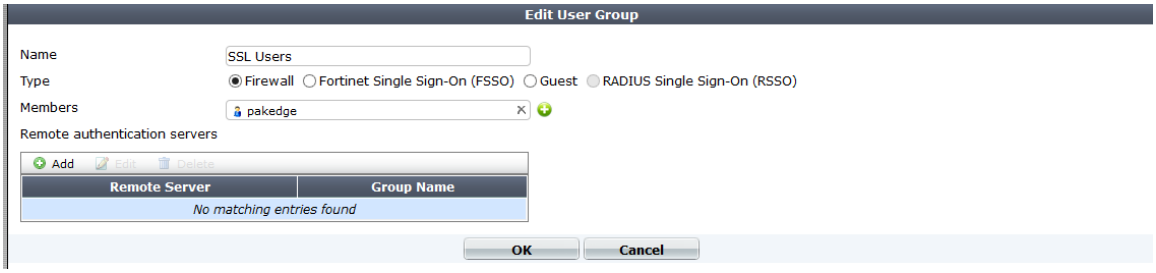
SSL

Secure Socket Layer VPN allows you to use the router's SSL VPN portal to access devices on the local network. The SSL VPN comes preconfigured on the R60D. In order to log in to the SSL VPN, you will first need to add Pakedge to the SSL VPN group. To do this, please take the following steps.

1. Navigate to **User & Device->User->User Group**.



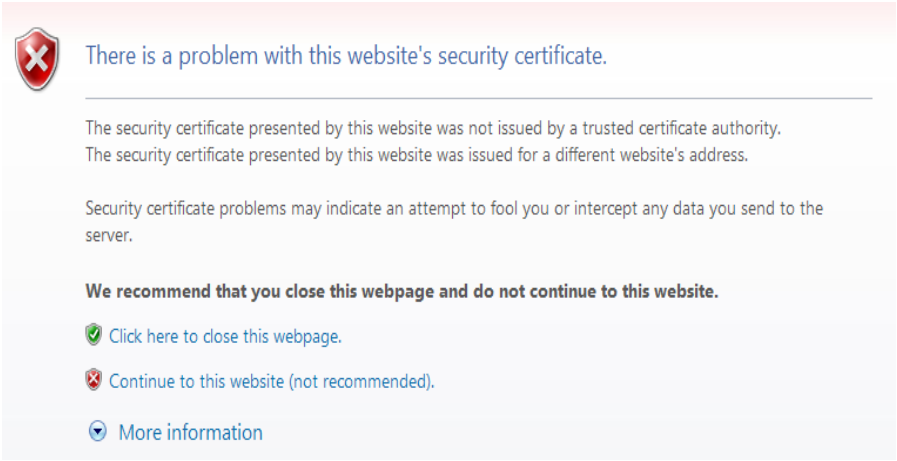
2. Double-click the **SSL Users** group.



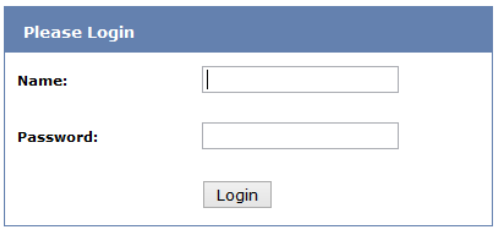
3. Click the **Members** drop-down menu, select **pakedge**, and hit **OK**. Now that Pakedge has been added, you will be able to log in to the SSL VPN with it.

To access the SSL VPN please take the following steps.

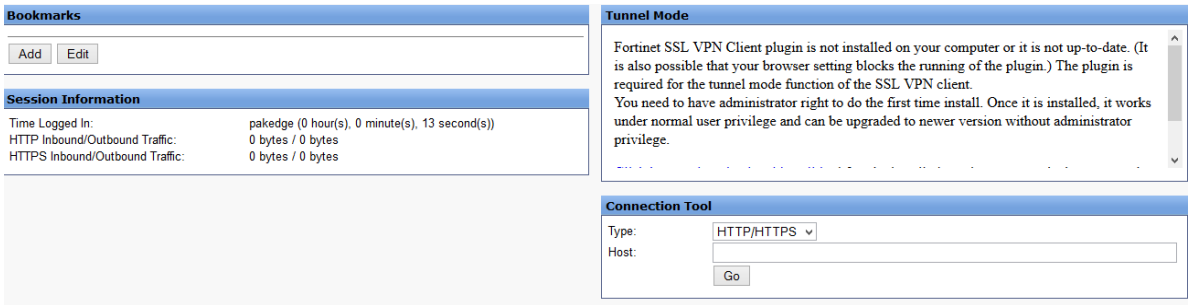
1. Open your web browser and type in the router's public IP (or DDNS name if configured) followed by the SSL VPN port number,10443. This would follow the format of **https://X.X.X.X:10443**. You may get an error page when you first access the SSL VPN page. Disregard the error message and click **Continue to this website**.



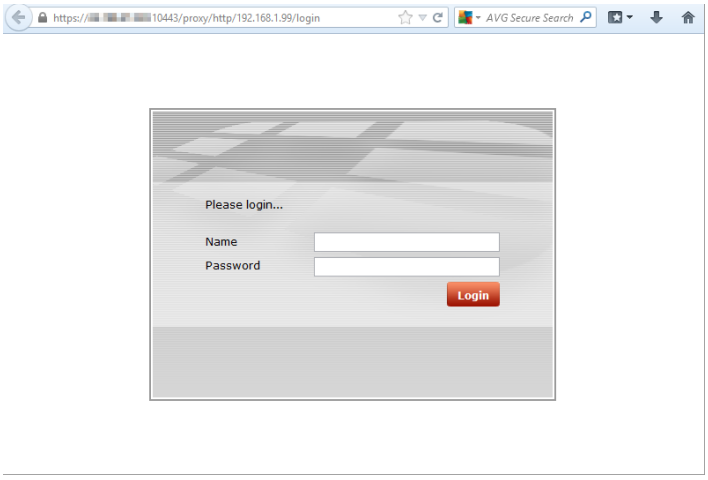
2. You will be redirected to the SSL VPN portal, as shown below.



3. Once you have logged in to the SSL VPN, you will see the following:

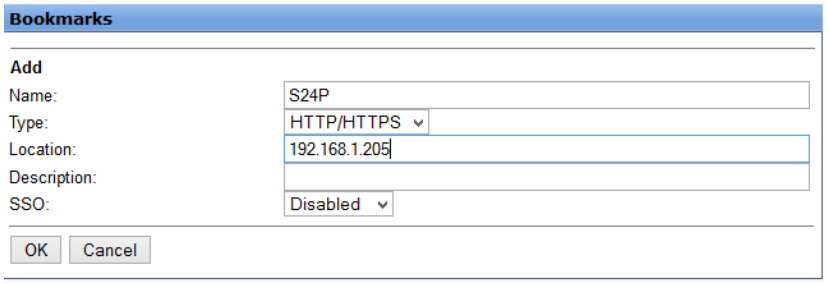


4. The **Connection Tool** allows you to enter the IP address of an internal device and view its GUI. If you enter the IP address of the router (192.168.1.99 by default) and click **Go**, you will see the login window.

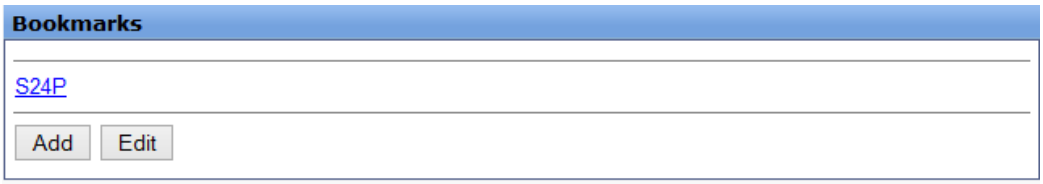


5. You can also create bookmarks in the SSL VPN that allow you to directly view the device on the network. To create a bookmark, click **Add** in the **Bookmarks** window.

6. Enter a name for the device that you are creating a bookmark for. See the S24P below as an example. Skip the **Type** field and enter the internal IP address of the switch in **Location**. The **Description** field is optional, but **SSO** must be **Disabled**. Hit **OK** when finished.



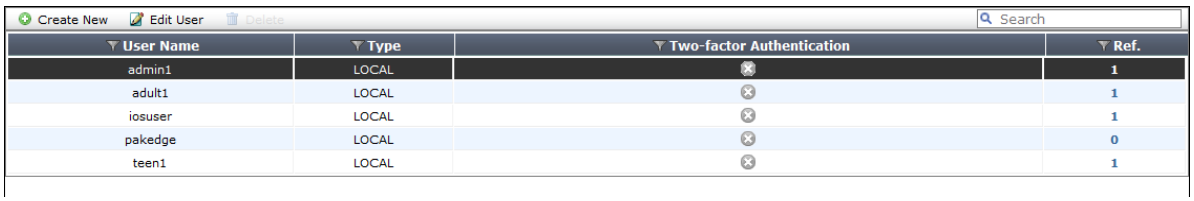
7. Your bookmark should now be listed. Whenever you log in to the SSL VPN, your bookmark will be there.



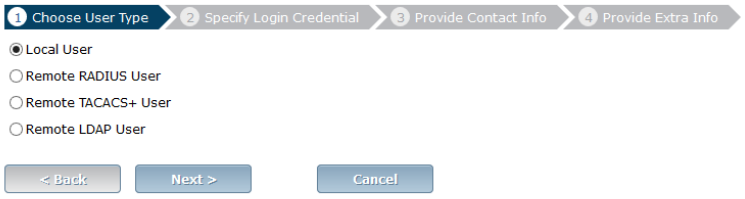
PPTP

Point to Point Tunneling Protocol is a VPN that allows your computer to remotely connect to the network and have full network access. This means your computer will be given an IP address and become part of the network. The PPTP VPN is preconfigured, so all you will need to do is create a user for yourself. This requires the following steps.

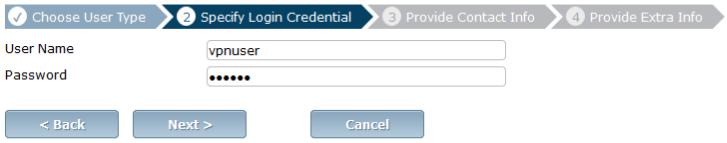
1. Navigate to **User & Device**->**User**->**User Definition** and click **Create New**.



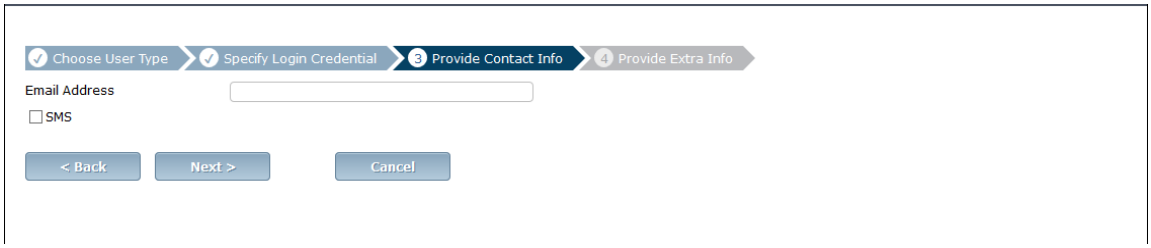
2. Select **Local User** and hit **Next**.



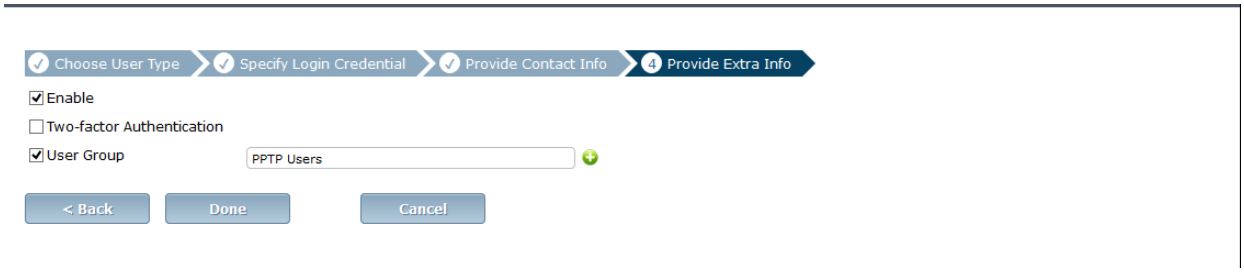
3. Enter a username and password for the user and hit **Next**.



4. Leave this page on its default settings and hit **Next**.



5. Check the box for **User Group**, select **PPTP Users**, and hit **Done**.

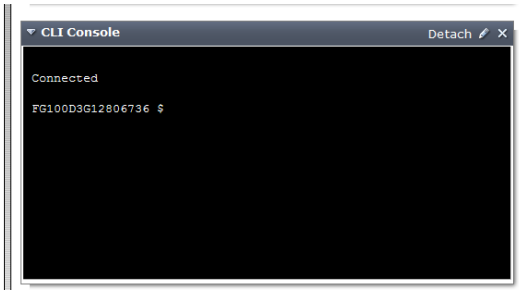


You have now created a new user and added it to the PPTP VPN group. This gives the user access to the PPTP VPN on the router.

CHANGE VPN SUBNET

When you connect to the router remotely via PPTP VPN, you will be given an IP address from 10.0.191.110 to 10.0.191.210 by default. If you would like to change the PPTP VPN subnet, please take the following steps.

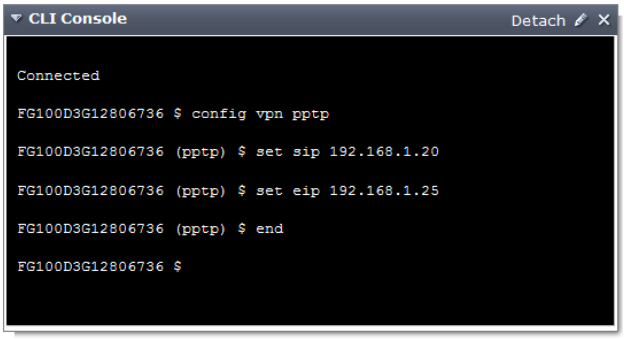
1. Navigate to **System->Dashboard->Status** and click on the CLI widget.



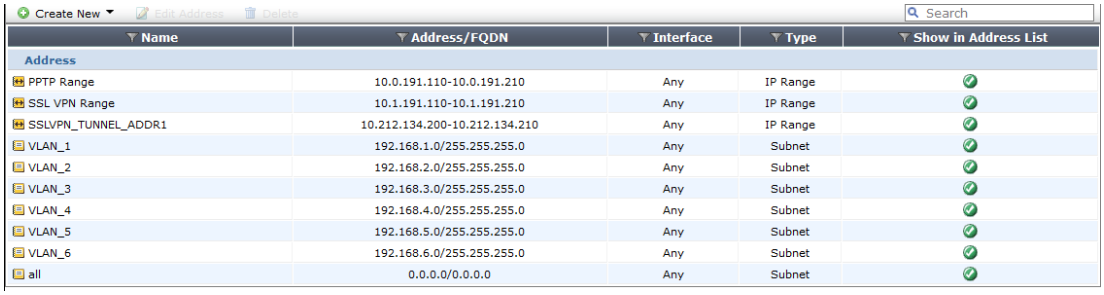
2. The following commands are used to change the PPTP VPN subnet:

   config vpn pptp
   set sip *starting IP*
   set eip *ending IP*
   end

   The following example shows the commands to change the VPN IP range from 192.168.1.20 to 192.168.1.25.

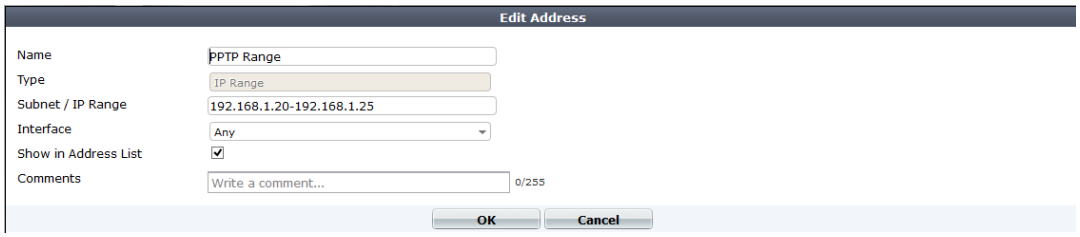


3. You will also need to adjust the firewall object for the PPTP VPN IP range. Navigate to **Firewall Objects->Address->Addresses**.



Name	Address/FQDN	Interface	Type	Show in Address List
Address				
PPTP Range	10.0.191.110-10.0.191.210	Any	IP Range	✓
SSL VPN Range	10.1.191.110-10.1.191.210	Any	IP Range	✓
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210	Any	IP Range	✓
VLAN_1	192.168.1.0/255.255.255.0	Any	Subnet	✓
VLAN_2	192.168.2.0/255.255.255.0	Any	Subnet	✓
VLAN_3	192.168.3.0/255.255.255.0	Any	Subnet	✓
VLAN_4	192.168.4.0/255.255.255.0	Any	Subnet	✓
VLAN_5	192.168.5.0/255.255.255.0	Any	Subnet	✓
VLAN_6	192.168.6.0/255.255.255.0	Any	Subnet	✓
all	0.0.0.0/0.0.0.0	Any	Subnet	✓

4. Double-click the PPTP Range object to reach the **Edit Address** screen. Change the IP range to match what you entered earlier and click OK. The example below lists the range 192.168.1.20 to 192.168.1.25.

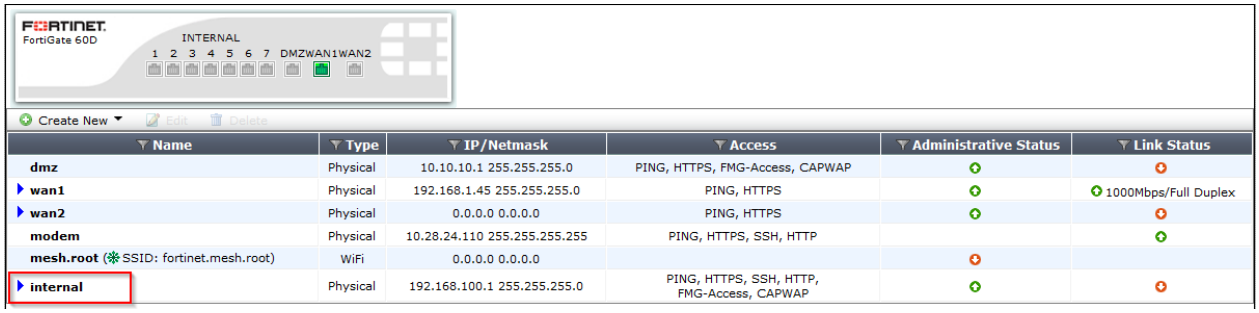


5. The VPN IP range has now been changed.

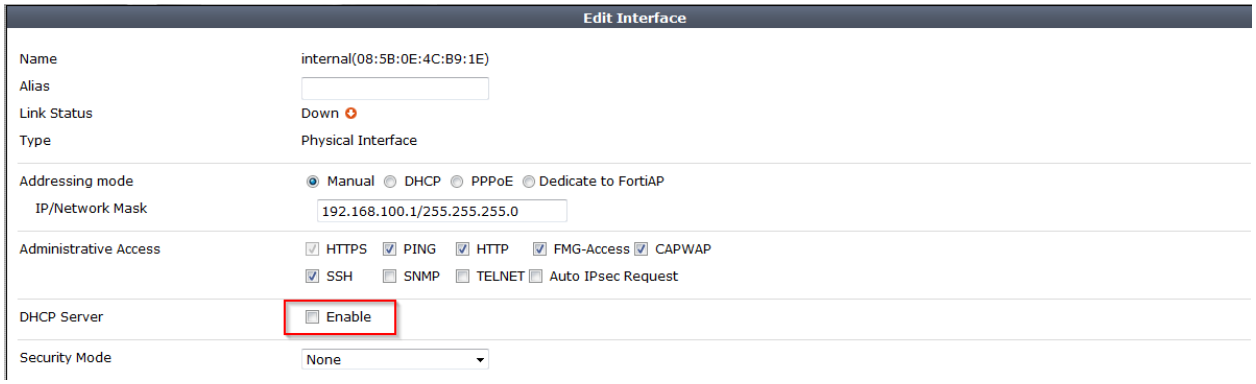
DISABLING DHCP ON A VLAN

Dynamic Host Configuration Protocol allows your devices on the network to automatically get an IP address. In case you may have an existing DHCP server on your network, you can disable DHCP on the router. To do this, please take the following steps.

1. Navigate to **System**->**Network**->**Interfaces**. Double-click on the **internal** interface.



2. Uncheck the **Enable** box under the DHCP Server section.

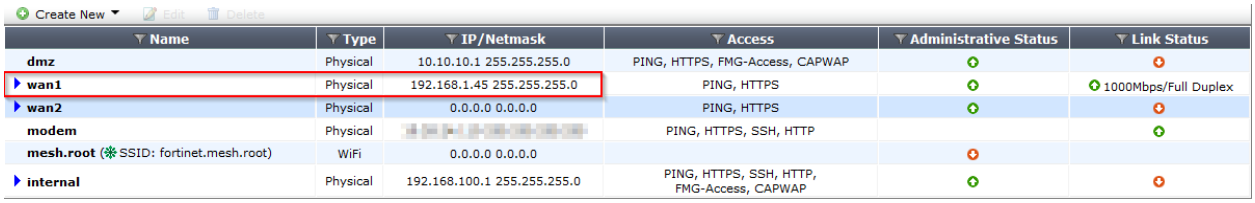


3. Click **OK**. DHCP is now disabled on the internal network.

DUAL WAN REDUNDANCY

Dual Wan Redundancy allows the router to fail over to a secondary internet connection when the first goes down. The R60D uses wan1 as the primary internet connection and wan2 as the secondary connection. To set up dual wan redundancy, please take the following steps.

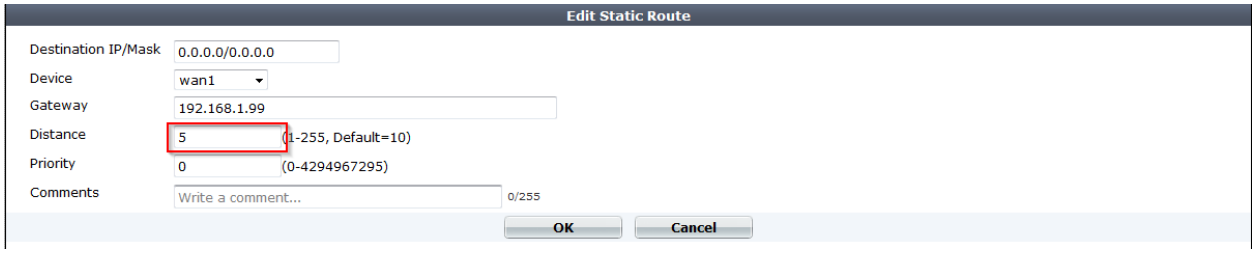
1. If wan1 is NOT using DHCP, skip to Step 3. If wan1 is using DHCP, navigate to **System**->**Network**->**Interfaces**. Double click **wan1**.



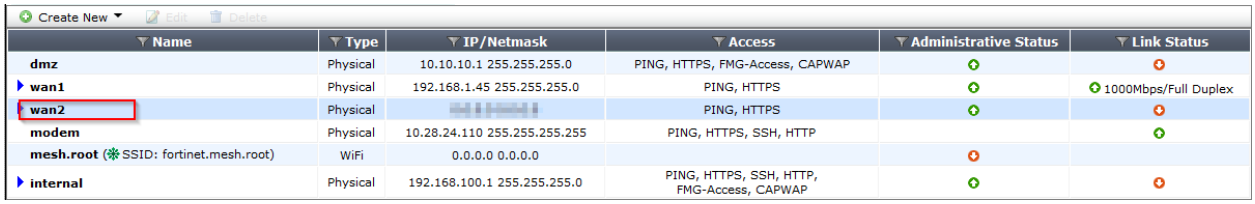
2. Set the **Distance** field to 5. Click **OK**.

3. If wan1 is using a static IP, navigate to **Router**->**Static**->**Static Routes**. Double-click on the static route that you created.

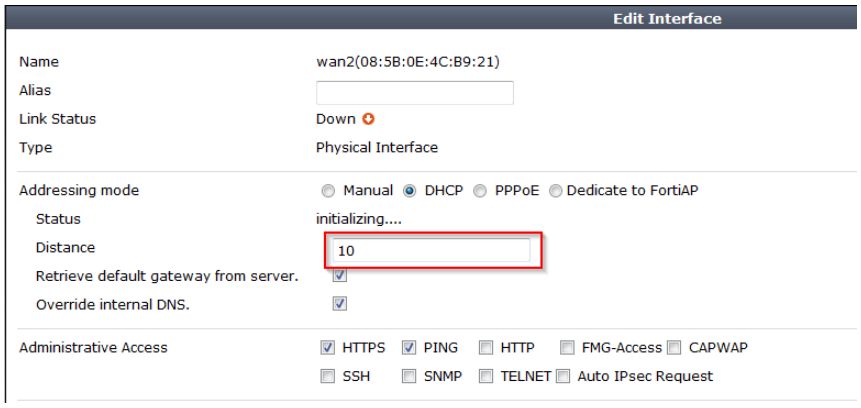
4. Set the distance field to 5. Click **OK**.



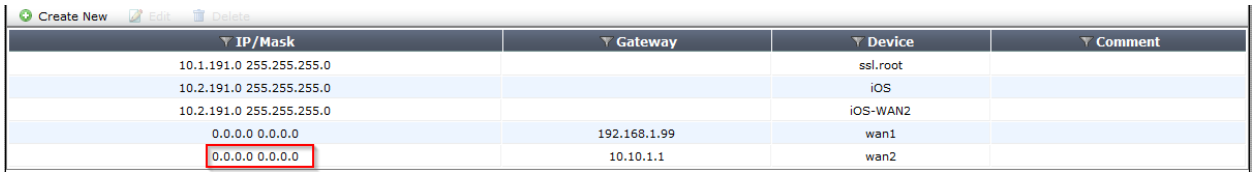
5. If wan2 does not use DHCP, skip to step 7. If wan2 uses DHCP, navigate back to **System->Network->interfaces**. Double click on **wan2**.



6. Set the **distance** field to 10. Click **OK**.

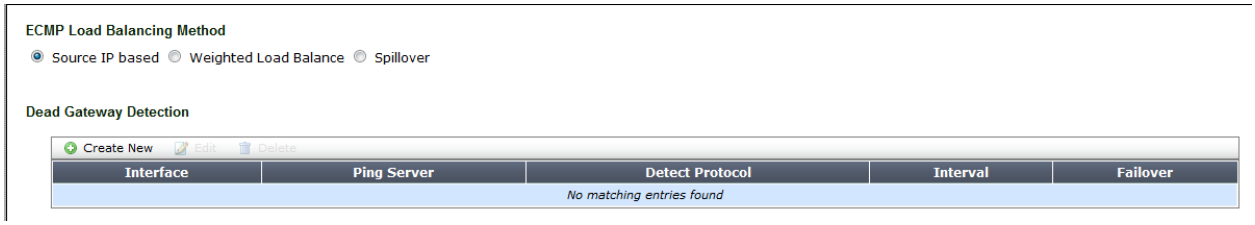


7. If wan2 is set to a static IP, navigate to **Router->Static->Static Routes**. Double-click on the static route that you created to get internet access for this wan port.

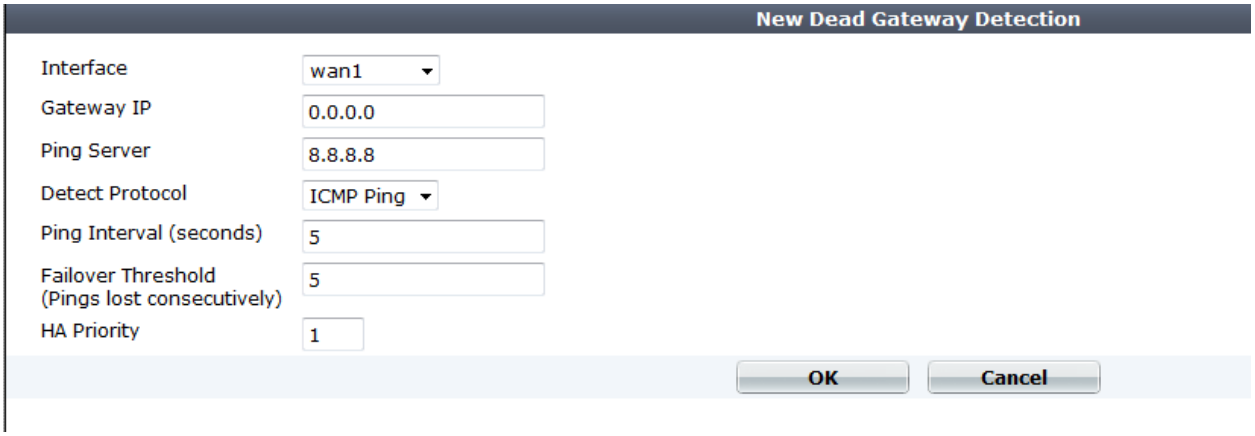


8. Set the **distance** field to 10. Click **OK**.

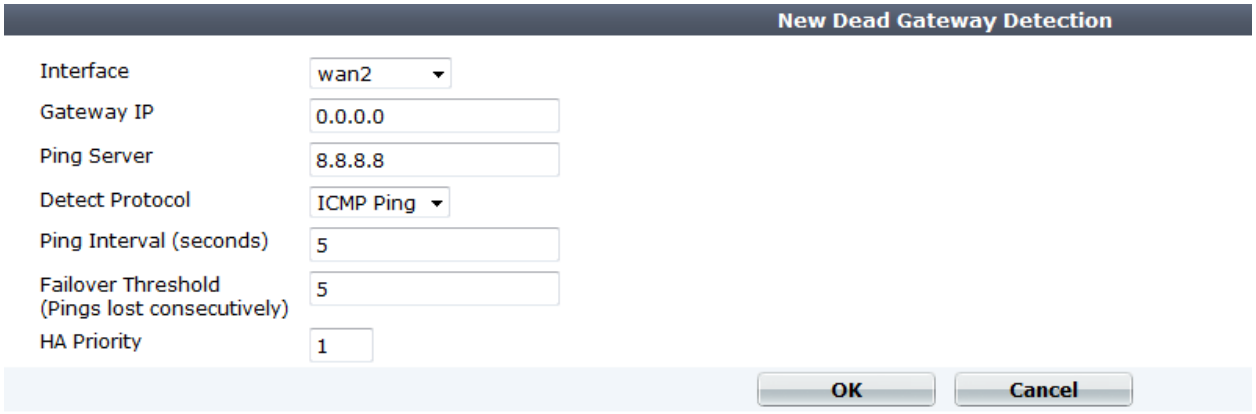
9. Now we will need to set up the dead gateway detection to allow the router to ping an IP address on the Internet in order to determine if a WAN port is down. Navigate to **Router->Static->Settings**. Click **Create New**.



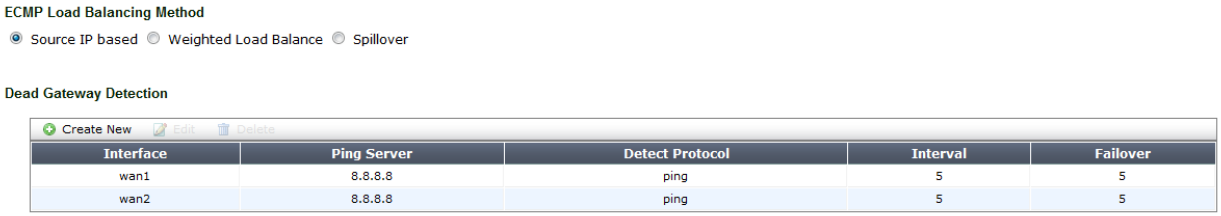
10. Select wan1 as the **Interface**. Leave the **Gateway IP** at all 0's. The **ping server** is the IP address that the router will continuously ping. We recommend using 8.8.8.8. We will leave the **detect protocol** at ICMP Protocol. The **ping interval** specifies how often the router will ping the IP address used in the ping server. The **failover threshold** specifies how many times the pings must fail in order for the router to failover to wan2.



11. Click **Create New** again. We will now create another gateway detection entry for wan2.
12. The settings will be the same as they were in step 10. We will now select **wan2** for **Interface**.



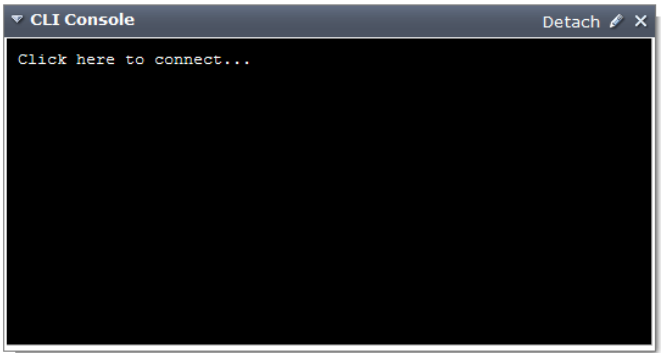
13. You should now have two dead gateway detections listed. The dual wan redundancy setup is complete. If wan1 fails, the router will automatically switch to wan2. If wan1 comes back up, the router will switch back to wan1.



DDNS

Dynamic DNS lets users with non-static IP address have a static DNS name. Many services let you register Dynamic DNS, some of which are free. To configure DDNS, enter the appropriate CLI-commands on the router. To configure a DNS name of pakedgerouter.dyndns.org from the DDNS provider DynDNS, please take the following steps.

1. Navigate to **System->Dashboard->Status** and scroll down to the CLI widget.



2. Click on the widget to enter commands onto the router. You will need to enter the following commands:

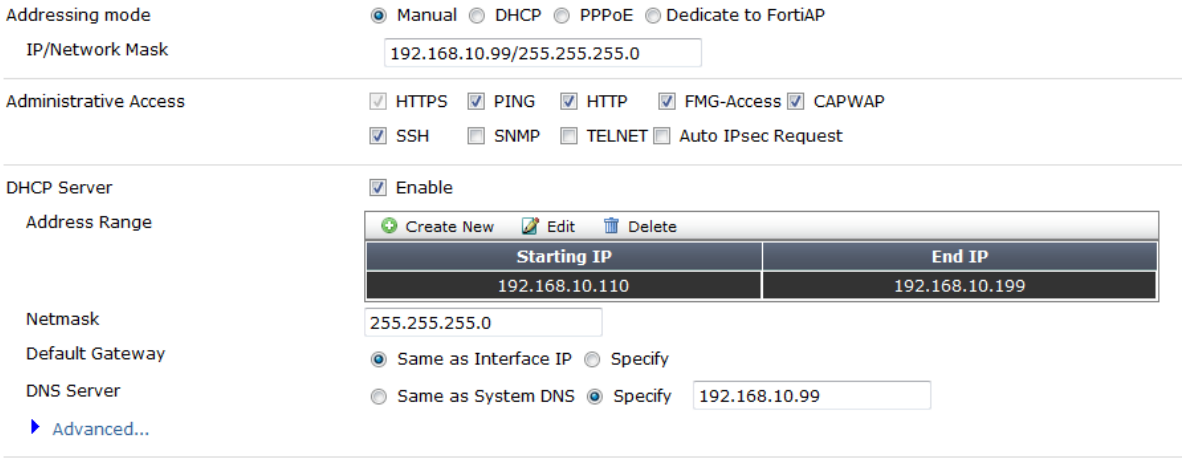
   config system ddns
   edit 1
   set ddns-server *DDNS provider*
   set ddns-domain *DNS name*
   set ddns-user *username to the DDNS account*
   set ddns-password *password to the DDNS account*
   set monitor-interface *wan port that you are using*
   end

3. The DDNS setup is now complete.

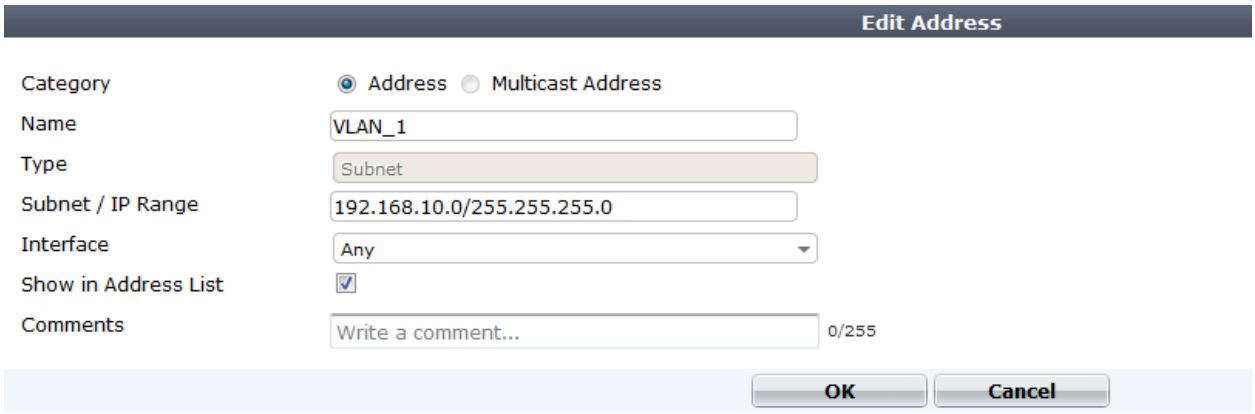
CHANGING IP SUBNET

The IP address is set to 192.168.1.99 by default, but you can change that according to your network needs. To change the IP subnet of the router, please take the following steps.

1. Navigate to **System->Network->Interfaces**. As an example, we will change the IP subnet of the internal network to be on the 192.168.10.x subnet.
2. Double-click on the **internal network**.
3. Enter **192.168.10.99/255.255.255.0** in the **IP/Network Mask** field. Under **Address Range**, adjust the starting and ending address to match the new subnet. Change the DNS server to **192.168.10.99**. Click **OK**.



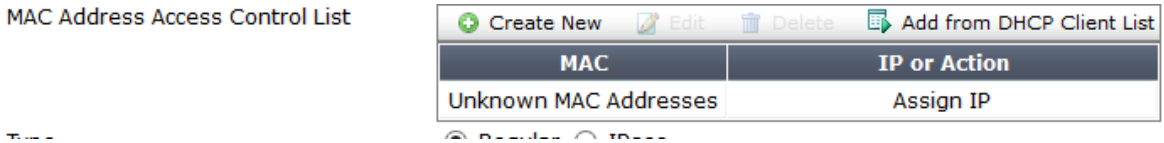
4. Navigate to **Firewall Objects->Address->Addresses**.
5. Double-click on **VLAN_1** to edit it. Change the **Subnet/IP Range** field to **192.168.10.0/255.255.255.0**. Hit **OK** to finalize.



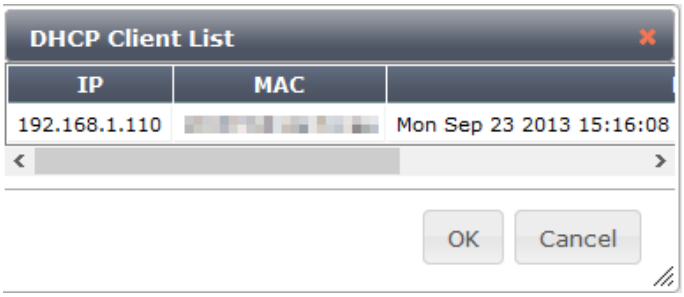
DHCP RESERVATION

The DHCP reservation function allows the router to hand out the same IP address for a particular MAC address. To set a reservation, please take the following steps.

1. Navigate to **System**->**Network**->**Interfaces**.
2. Edit the **internal network**.
3. Click on **Advanced**.
4. Click **Add from DHCP Client List**.



5. You will then see a new box titled **DHCP Client List**.



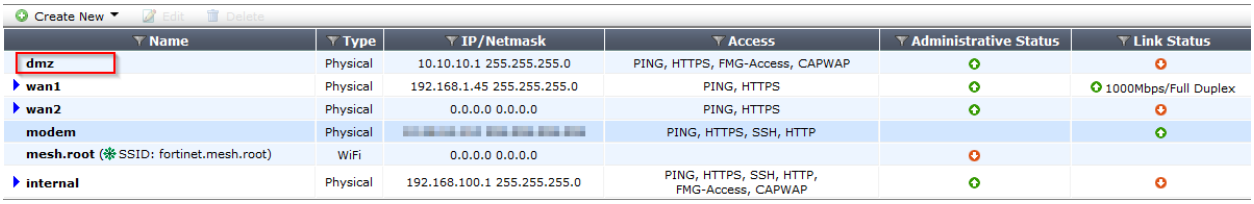
6. Select the IP address that you want to reserve by clicking on it. Click **OK** to finalize the settings. You will return to the **Edit Interface** screen. Hit **OK** at the bottom to finalize the DHCP reservation.

DMZ

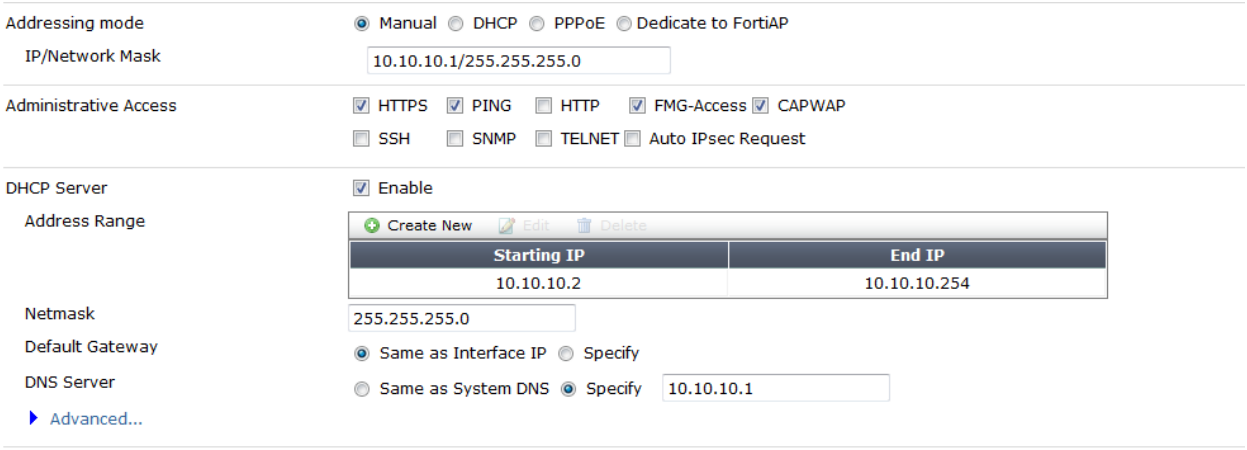
The DMZ port is a separate network on its own subnet. This port does not have access to the normal internal VLANs; however, all the internal networks have access to it (except for the guest network on VLAN 6).

The purpose of placing a device on the DMZ port is to add security to the network. If an intruder gains access to the DMZ network, they will have no access to the internal network. To view the IP subnet settings on the DMZ, please take the following steps.

1. Navigate to **System->Network->Interfaces**. Double-click on DMZ.



2. In case you need to make any changes to the DMZ port, this page will display the IP subnet settings. Click **OK**.



GUEST VLAN

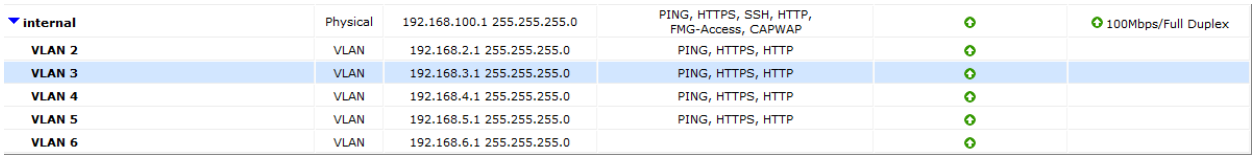
The guest network on VLAN 6 does not have access to any other devices on the internal network. However, other networks can communicate with devices on the guest network.

If you would like to utilize the guest network, connect a VLAN-capable wireless access point directly to the router and configure it to broadcast on VLAN 6. Once the setup is complete, any device that connects to that signal will join the guest network.

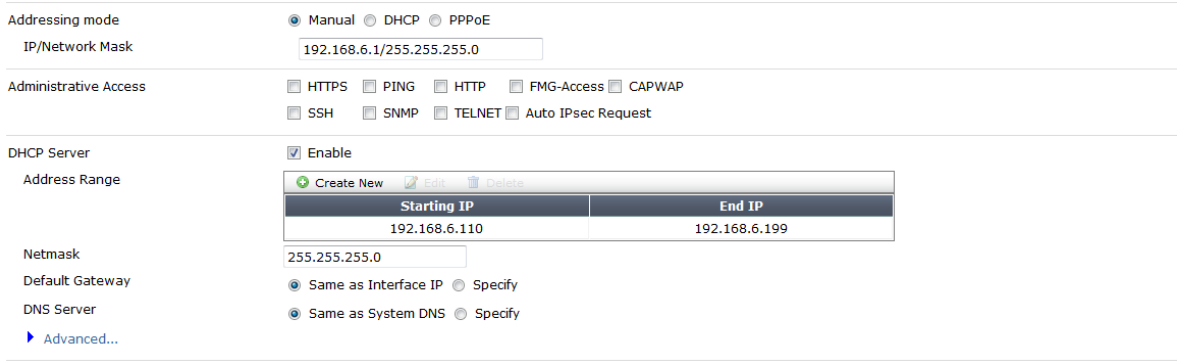
Pakedge has a full line of 802.1q or VLAN-capable wireless access points. Please contact Pakedge for the exact model numbers that support 802.1q or VLAN-tagging.

To view the IP subnet settings for the guest VLAN, please take the following steps.

1. Navigate to **System**->**Network**->**Interfaces**. Click on the blue triangle to view the guest VLAN. Double-click on **VLAN6**.



2. In case you need to make any changes to the guest VLAN, this page will display the IP subnet settings. Click **OK**.



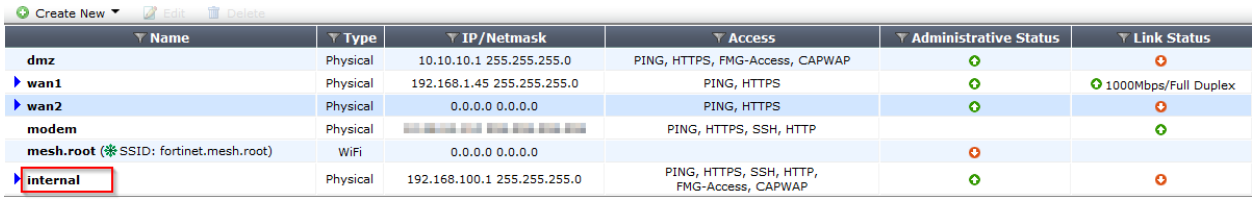
UNIVERSAL THREAT MANAGEMENT

The R60D supports UTM services such as antivirus, web filtering, email filtering, intrusion prevention system (IPS), and application control. Please see the supplemental manual for R60D UTM assistance.

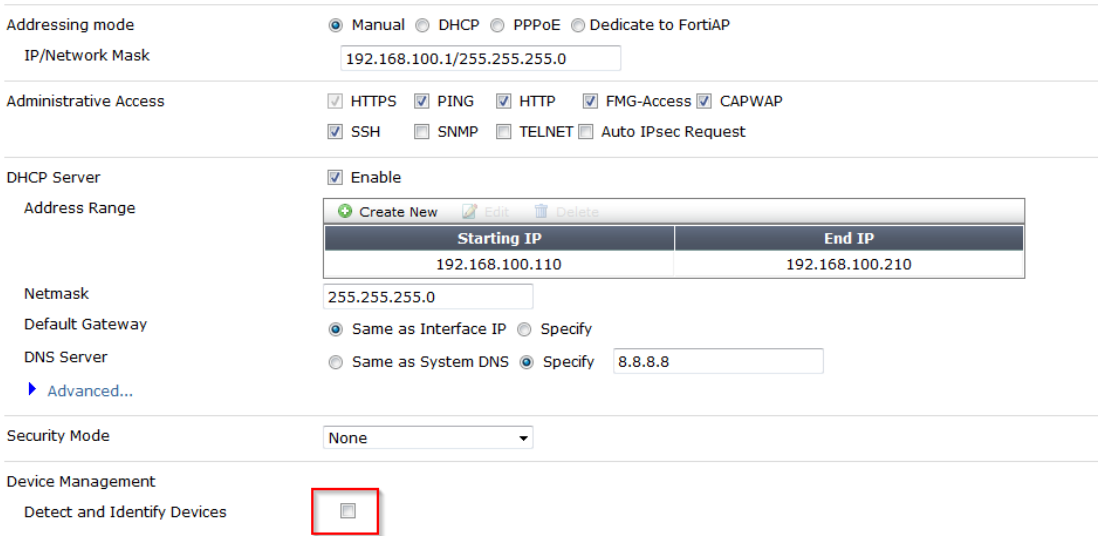
DEVICE DISCOVERY

Device Discovery will allow the router to discover devices on your network. This will allow you to keep track of all the devices you connect on the network. Please take the following steps to configure the Device Discovery.

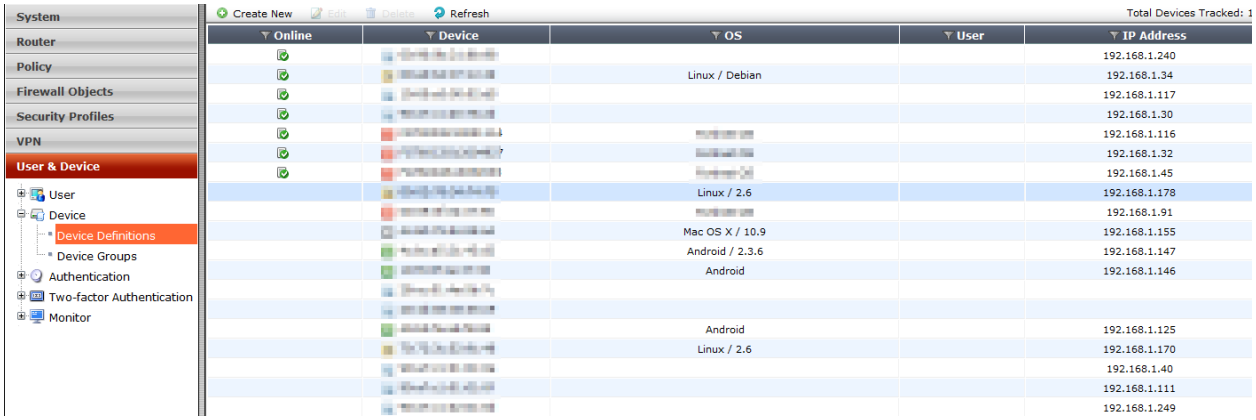
1. Device Discovery is disabled by default. To enable it, navigate to **System**->**Network**->**Interfaces**. Double-click on the **internal network**.



2. Check the box titled **Detect and Identify Devices**. Click **OK**.



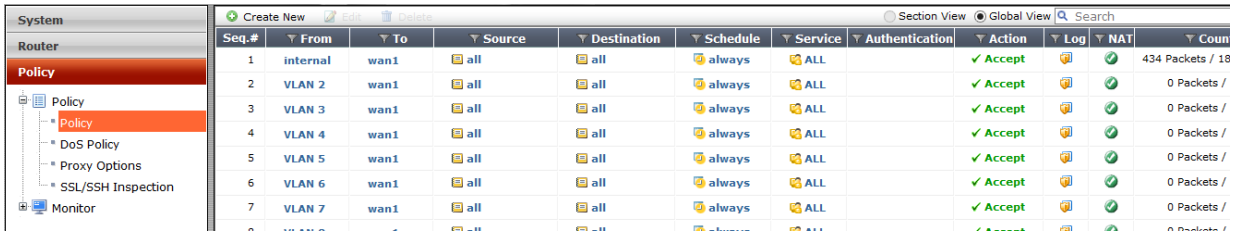
3. The router will now begin discovering devices on the internal network. Discovered devices will be listed under **User & Device**->**Device**->**Device Definitions**. Please note that it will take the router some time to discover all of your devices on the network.



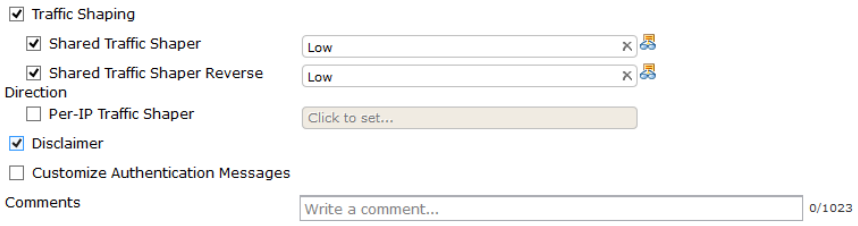
DISCLAIMER PAGE

You can configure a disclaimer message for when users connect to the internet. This may be useful if users must sign on to a guest network to agree to a set of terms. You can enable the disclaimer option through the **Policy** section. Please take the following steps to configure the disclaimer page.

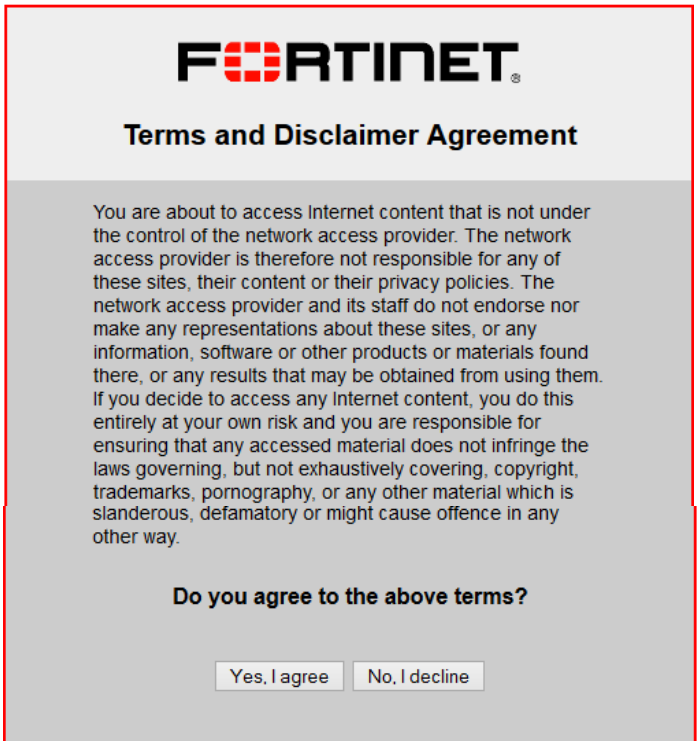
1. Navigate to **Policy->Policy->Policy**.



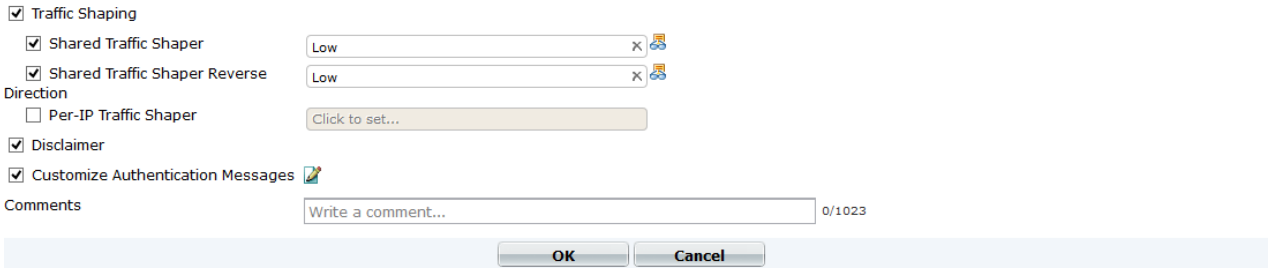
2. Double-click the **VLAN 6** policy to edit it. This policy allows VLAN 6 to connect to the internet.
3. Scroll down to the **Disclaimer** box and check it.



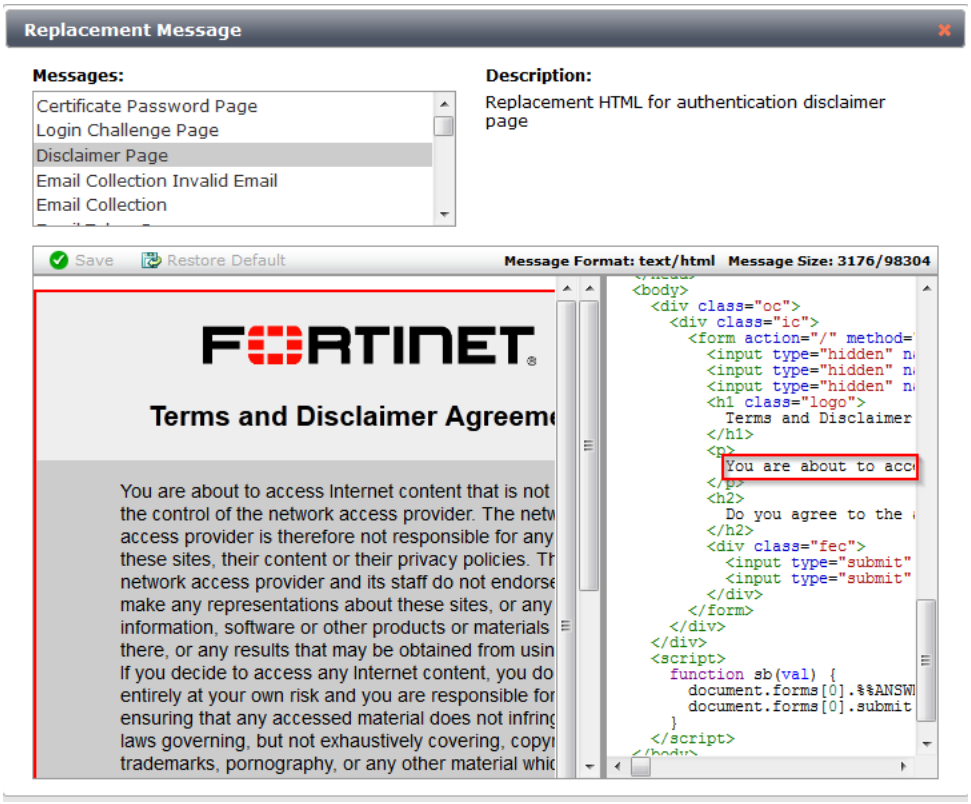
4. If you click **OK** at this point, the disclaimer page will display the following message when a user on VLAN 6 tries to access the internet:



5. The user must agree to the terms to receive internet access.
6. You can customize the message displayed by checking the box **Customize Authentication Messages** and clicking the small icon to the right.



7. On the right-hand side of the **Replacement Message** window, scroll down the HTML code until you see a section titled **Terms and Disclaimer Agreement**. You can delete the following default message, enter your own, and hit **OK**.



8. Users will now see your custom message when accessing the internet.

SHUTTING DOWN THE ROUTER

If you need to shut down the router please do so by issuing the appropriate command on the CLI console window.

1. Navigate to System->Dashboard->status
2. Click on any black area in the CLI console to run a command. Type **exe shutdown** and press enter.

3. The router will now shutdown and only the power light will be left on. It will now be safe to unplug the router.
4. You can reboot the router by running the command **exe reboot**.

APPENDIX A: FAQS

1- **What is the difference between the standard FortiGate 60D and the preconfigured Pakedge version (R60D)?**

The preconfigured Pakedge version comes with a separate login screen. This login screen is limited to a basic set of options to get the network up and running. This allows the powerful Fortigate router/security appliance to be installed in any home without expert help.

2- **Who provides support for the R60D?**

Pakedge provides the basic support for the Pakedge pre-configuration. If an integrator wants to perform any configuration beyond it, they would have to contact Fortinet.

3- **Do I need to purchase antivirus for my router to work?**

The router will work without an antivirus subscription. However, the router will not reach its full potential and malware could potentially penetrate your network. An antivirus subscription gives the router perimeter network protection for as long as the subscription is active.

4- **Can I purchase the antivirus only, without Fortinet support?**

No, Fortinet automatically supplies support when antivirus is purchased.

5- **Does the R60D have UPnP?**

No, the R60D does not support UPnP. UPnP is seen as a security risk for business-class routers.

APPENDIX B: SPECIFICATIONS

R60D ROUTER

Interfaces:

10/100/1000 Internal Switch Interfaces (Copper, RJ-45):	7
10/100/1000 WAN Interfaces (Copper, RJ-45):	2
10/100/1000 DMZ Interfaces (Copper, RJ-45):	1
USB Interfaces:	2 (1 Type-A, 1 Type-B)
Internal Storage	8 GB

System Performance:

Firewall Throughput (1518 byte UDP packets)	1.5 Gbps
Firewall Throughput (512 byte UDP packets)	1.5 Gbps
Firewall Throughput (64 byte UDP packets)	1.5 Gbps
IPSec VPN Throughput (512 byte packets)	1 Gbps
SSL VPN Throughput	30 Mbps
Intrusion Protection Security Throughput	200 Mbps
Antivirus Throughput (Proxy)	35 Mbps
Gateway-to-Gateway IPSec VPN Tunnels	200 Mbps
Client-to-Gateway IPSec VPN Tunnels	500 Mbps
Max Concurrent Firewall Sessions	500,000
New Sessions/Sec	4,000
Max Concurrent SSL-VPN Users	100
Firewall Policies	5,000
Virtual Domains (Max / Default)	10 / 10

Environment:

Power Required Amp Max	100-240 VAC, 50-60 Hz, 1.5
Power Consumption (AVG/MAX)	11.7/14 W
Heat Dissipation	40 BTU/h
Operating Temperature	32 – 104° F (0 – 40° C)
Storage Temperature	-13 – 158° F (-25 – 70° C)
Humidity	5%-90% non-condensing

NETWORKING FEATURES

DHCP/PPPoE Client/Server

Port Forwarding

Static/Dynamic Routing*

Traffic Shaping

Radius, LDAP, Active Dir

Local DB

User Group Support

SECURITY FEATURES

Gateway Antivirus Protection

(Virus, Spyware, Trojan)

Integrated IPS (signature & anomaly)

Integrated URL Filtering

Integrated Spam Filtering

VPN (IPSec, SSL, PPTP)

VOIP Security (H323, SIP)

MECHANICAL

Dimensions *(dimensions are approximate)*

Height x Width x Length: 1.50 x 8.5 x 5.83 in. (38 x 216 x 148 mm)

Weight 1.9 lb (0.9 kg)

OPTIONAL SUBSCRIPTION SERVICES

Automatic and Scheduled

Antivirus and IPS Updates

URL Categorizing

Anti-Spam RBL/SURBL

Web Filtering

CERTIFICATIONS

ICSA: Firewall, IPSec, SSL, Antivirus, IPS

COMPLIANCE

FCC Class A, Part 15, UL/CUL, C Tick,

APPENDIX C: LIMITED WARRANTY

Congratulations on your purchase of a Pakedge Device & Software product! We believe Pakedge designs and manufacture the finest home networking products on the market. With proper installation, setup, and care, you should enjoy many years of unparalleled performance. Please read this consumer protection plan carefully and retain it with your other important documents.

This is a LIMITED WARRANTY as defined by the U.S. Consumer Product Warranty and Federal Trade Commission Improvement Act.

19.1 What Is Covered Under the Terms of This Warranty

SERVICE LABOR: Pakedge will pay for service labor by an approved Pakedge service center when needed as a result of a manufacturing defect for a period of one (1) year from the effective date of delivery to the end user.

PARTS: Pakedge will provide new or rebuilt replacement parts for the parts that fail due to defects in materials or workmanship for a period of one (1) year from the effective date of delivery to the end user. Such replacement parts are then subsequently warranted for the remaining portion (if any) of the original warranty period.

19.2 What Is Not Covered Under the Terms of This Warranty

This warranty only covers failure due to defects in materials and workmanship that occur during normal use and does not cover normal maintenance. This warranty does not cover any appearance item; any damage to living structure; failure resulting from accident (for example: flood, electrical shorts, insulation); misuse, abuse, neglect, mishandling, misapplication, faulty or improper installation or setup adjustments; improper maintenance, alteration, improper use of any input signal and/or power, damage due to lightning or power line surges, spikes and brownouts; damage that occurs during shipping or transit; or damage that is attributed to Acts of God.

The foregoing limited warranty is Pakedge's sole warranty and is applicable only to products sold as new by Authorized Dealers. The remedies provided herein are in lieu of a) any and all other remedies and warranties, whether expressed, implied or statutory, including but not limited to: a) any implied warranty of merchantability, fitness for a particular purpose or non-infringement, and b) any and all obligations and liabilities of Pakedge for damages including but not limited to: incidental, consequential or special damages, or any financial loss, lost profits or expense, or loss of network connection arising

out of or in connection with the purchase, use or performance of the product, even if Pakedge has been advised of the possibility of such damages.

CAUTION: DAMAGE RESULTING DIRECTLY OR INDIRECTLY FROM IMPROPER INSTALLATION OR SETUP IS SPECIFICALLY EXCLUDED FROM COVERAGE UNDER THIS WARRRANTY. IT IS IMPERATIVE THAT INSTALLATION AND SETUP WORK BE PERFORMED ONLY BY AN AUTHORIZED PAKEDGE DEALER TO PROTECT YOUR RIGHTS UNDER THIS WARRANTY. THIS WILL ALSO ENSURE THAT YOU ENJOY THE FINE PERFORMANCE YOUR PAKEDGE PRODUCT IS CAPABLE OF PROVIDING.

19.3 Rights, Limits, and Exclusions

Pakedge limits its obligation under any implied warranties under state laws to a period not to exceed the warranty period. There are no express warranties. Pakedge also excludes any obligation on its part for incidental or consequential damages related to the failure of this product to function properly. Some states do not allow limitations on how long an implied warranty lasts, and some states do not allow the exclusion or limitation of incidental or consequential damages. In this case, the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

19.4 Effective Warranty Date

This warranty begins on the effective date of delivery to the end user. For your convenience, keep the original bill of sale as evidence of the purchase date from your authorized dealer.

19.5 Important: Warranty Registration

Please register your product at www.pakedge.com. It is imperative that Pakedge knows how to reach you promptly if we should discover a safety problem or product update for which you must be notified. In addition, you may be eligible for discounts on future upgrades as new networking standards come about.

19.6 To Obtain Service, Contact Your Pakedge Dealer.

Repairs made under the terms of the Limited Warranty covering your Pakedge product will be performed by an Authorized Pakedge Service Center. These arrangements must be made through the selling Pakedge Dealer. If this is not possible, contact Pakedge directly for further instructions. Prior to returning a defective product directly to Pakedge, you must obtain a Return Material Authorization number and shipping instructions. Return shipping costs will be the responsibility of the owner.

For additional information about this warranty, visit our website:

Pakedge Device & Software, inc.
3847 Breakwater Avenue
Hayward, CA 94545
USA

Email: support@pakedge.com
Phone: (650) 385-8703
www.pakedge.com

pakedgedevice&software inc.

3847 Breakwater Avenue
Hayward, CA 94545

USA

Visit us at:

www.pakedge.com