PAKEDGE DEVICE & SOFTWARE, INC.
ROUTER TRAINING BASICS

NETWORK RESPONSIBLY

AGENDA

- Training Goals
- Router Positing within A/V Network
- Basic Functions of a Router
- Pakedge Routers
- Common Sales Objections
- Jumpstart: 5 Things to Do Now
- Resources
- Technical Training/Troubleshooting

NETWORK RESPONSIBLY

TRAINING GOALS

The goals of this presentation are:

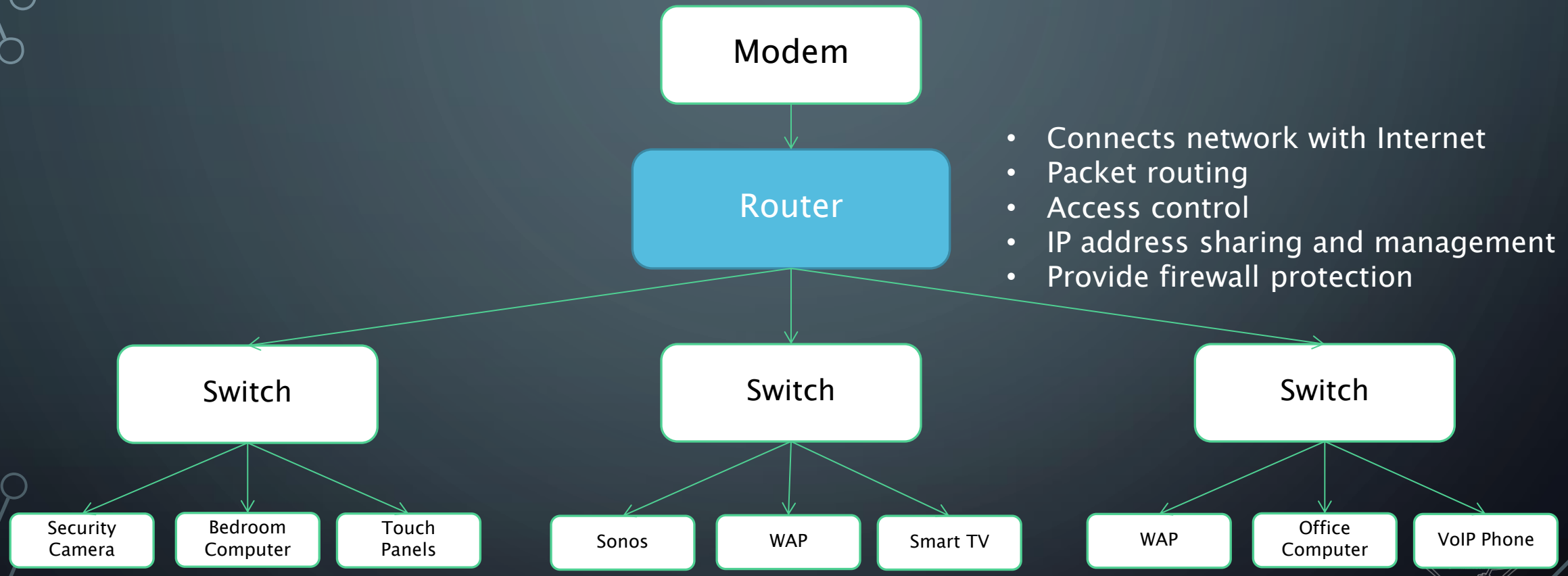
- Increase basic knowledge of Pakedge routers
- Increase technician productivity in the field through awareness of common router setup and configuration tasks

This training is intended for

- Sales and marketing personnel
- Technical personnel

NETWORK RESPONSIBLY

ROUTER POSITIONING WITHIN A/V NETWORK



- Connects network with Internet
- Packet routing
- Access control
- IP address sharing and management
- Provide firewall protection

NETWORK RESPONSIBLY

BASIC FUNCTIONS & KEY ATTRIBUTES

What it Does

- Connects network with Internet
- Packet routing
- Access control
- IP address management
- Provide firewall protection

Key Parameters

- Routing Performance
  - # of concurrent sessions
  - Throughput – firewall, IPSec, VPN
  - # of concurrent and VPN users
- Secure compartmentalized access
  - VPN
  - Port forwarding
  - DMZ
  - Guest networks
- IP Address Management
  - ISP address management
  - Device IP address management (DHCP/Static, Reservations)
- Threat management – intrusion protection, anti-virus, web filtering, firewall policies

NETWORK RESPONSIBLY

PAKEDGE ROUTER COMPARISON CHART

Router Products	Switch Capacity Gbps	Port Speeds 10/100/1000 Mbps	Console Port	# of LAN Ports (Router / Switch)	# of PoE Ports	# of High Power PoE Ports	# of SFP Ports	Port Orientation	Cooling
K60D	N/A	Yes	Yes	7	N/A	N/A	N/A	Rear	Fanless
K60D-S8Mpd	16	Yes	Yes	7 / 8	N/A	N/A	1	Rear	Fanless
K60D-S8Hav	24	Yes	Yes	7 / 8	8	4	4	Rear	Fan
K60D-S24av	64	Yes	Yes	7 / 24	N/A	N/A	2	Rear	Fanless
K60D-S24F	64	Yes	Yes	7 / 24	N/A	N/A	2	Front	Fanless
K60D-S24Hav	64	Yes	Yes	7 / 24	24	12	4	Rear	Fan
K60D-S24Hf	64	Yes	Yes	7 / 24	24	12	4	Front	Fan
K60D-S24P8av	64	Yes	Yes	7 / 24	8	N/A	4	Rear	Fan
K60D-S24P16av	64	Yes	Yes	7 / 24	16	N/A	4	Rear	Fan
K60D-S24Pav	64	Yes	Yes	7 / 24	24	N/A	4	Rear	Fan

*All kits are also available in UTM configurations.
*Part numbers will change to *"R60DU-"* followed by the switch model of your choice.

NETWORK RESPONSIBLY

WHY PAKEDGE ROUTERS?

- Enterprise Performance "out of the box":
  - Up to 400,000 concurrent sessions, with capability to add 3,000 new sessions/second
  - Enterprise level reliability
- Enterprise level features and services:
  - IP Address Management – DHCP, Static, or PPPoE
  - Port Forwarding: Access a device or server directly over the internet
  - Secure and Remote Access to Internal Network with SSL VPN
  - Dual WAN redundancy: Enable backup connectivity to Internet
  - Dynamic DNS: Access the router via non-IP address
  - DMZ and guest networks for compartmentalized access to network
- Pre-configured setup files for faster and trouble free installations
- Unified Threat Management: Intrusion protection, Parental Website Control and System Antivirus protection
- Remote management and monitoring through cloud – Bakpak compatible
- Rack mountable metal housing with AV aesthetics

NETWORK RESPONSIBLY

SALES OPPORTUNITIES

- High-End A/V networks with latency-sensitive equipment
- Networks which can't tolerate the intermittent downtime that comes alongside consumer-grade routers.
- Networks which require the ability to talk across VLANs – for example, networks with a VLAN dedicated to streaming equipment (Apple TVs, Sonos, etc.)

NETWORK RESPONSIBLY

COMMON CUSTOMER OBJECTIONS

- "The routers are too expensive."
  - The network is the backbone of the entire home and business system.
    - Your control systems, lighting, audio and video, VoIP phones, and IP cameras are all connected to your network.
      - With Pakedge Equipment, you'll have a strong network in place to handle all the incoming and outgoing traffic
- Time is money.
  - What is the typical cost of a service call?
  - How often do you call because something's not working on the network?
    - With a reliable network, you will save time and money on troubleshooting your network issues

NETWORK RESPONSIBLY

COMMON RESELLER OBJECTIONS

- "My customer doesn't need an enterprise class router."
  - Enterprise Class routers prevent network outages that otherwise cost the dealer time and money to support.
  - Enterprise Class routers are the only equipment on the market fully capable of handling high-end, latency-sensitive A/V equipment.
- What's the difference between Pakedge routers and Apple Airport Extreme?
  - Apple equipment is still consumer grade, and not built for the speed and reliability required by enterprise-grade networks.
  - Pakedge routers have available UTM services for complete end-to-end network protection right at the gateway.

NETWORK RESPONSIBLY

COMMON RESELLER OBJECTIONS

- How will this boost performance?
  - Higher session counts and better processing provides better overall network performance than consumer-grade equipment.

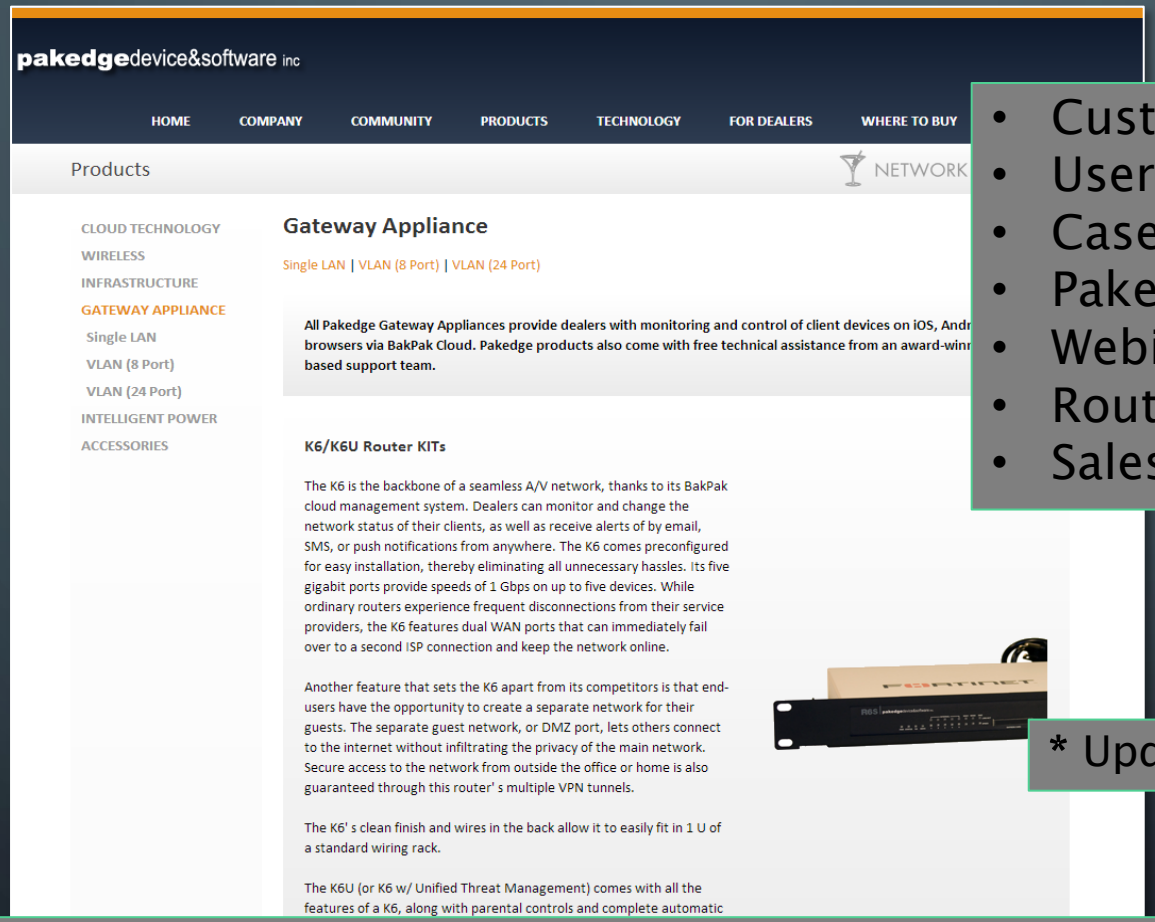
NETWORK RESPONSIBLY

JUMPSTART – 5 THINGS YOU CAN DO

1. **Bookmark** and familiarize yourself with the Pakedge Router Resources page – www.pakedge.com/router (shortcut URL)
2. **List** the router information and product brochure on your business website. Send/email the brochure to past and future customers.
3. **Contact your Pakedge rep** to develop a profile of the ideal router opportunity and a custom sales plan.
4. **Upsell previous customers** by reviewing and identifying customers who have purchased switches and wireless products but not a router
5. **Quote** Pakedge routers with every potential "systems" opportunity

NETWORK RESPONSIBLY

RESOURCES – ONE STOP REFERENCE



- Customer brochure
- User manual
- Case studies
- Pakedge contacts
- Webinar recording
- Router resources
- Sales and Marketing Resources

* Updated page will be up Wednesday

Shortcut URL: www.pakedge.com/router

NETWORK RESPONSIBLY

THANK YOU!

NETWORK RESPONSIBLY

sales@pakedge.com

NETWORK RESPONSIBLY

PAKEDGE ESSENTIALS

BY: LUIS SERRANO

NETWORK RESPONSIBLY

WHAT'S IN STORE

- Learn how to port forward on R6S/R6V
- Learn how to SSL & PPTP VPN
- Learn how to change IP address for a network
- Change IP address to the router
- Setting up WAN address
- Setting up DDNS
- W6/W7 recommended settings
- Changing IP address in PoE switch
- Change/Add gateway in PoE switch
- Setting up VLANs on switches
- Setting up QoS
- C36 configuration
- NP36 Configuration
- PDU set up

NETWORK RESPONSIBLY

PORT FORWARDING

- We port forward to allow access for remote devices to connect to a specific device or server in the private local-area network (LAN)
- To do this you will need to know the IP address of what you are trying to get to and the port number also if it is TCP or UDP.
- There are 2 parts to create the port forward. The first part is to create the rule to tell the router where to send the traffic, second is allowing the traffic through the firewall.
- *If the client device is set with a static IP make sure that it has the correct default gateway.*

NETWORK RESPONSIBLY

PORT FORWARDING CONTINUED

- First go to Firewall Objects > Virtual IP > Virtual IP
- Click Create New at top left
- Enter in a unique name
- Enter in the clients address under Mapped IP Address/Range
- Check the box for Port Forwarding and make sure you have the correct Protocol (TCP or UDP)
- The External Service Port and Map to Port will have the same port numbers

NETWORK RESPONSIBLY

FortiGate 60C

Help | Logout | FORTINET

System
Router
Policy
Firewall Objects
- Address
  - Address
  - Group
- Service
- Schedule
- Traffic Shaper
- Virtual IP
  - Virtual IP
  - VIP Group
  - IP Pool
- Monitor

UTM Profiles
VPN
User
WiFi Controller
Log&Report

Name	Rule name
External Interface	wan1
Type	Static NAT
Source Address Filter	(e.g.: x.x.x.x, x.x.x.x-y.y.y.y, x.x.x.x/y)
External IP Address/Range	0.0.0.0 -
Mapped IP Address/Range	192.168.1.1 -
Port Forwarding	
Protocol	TCP UDP SCTP
External Service Port	80 -
Map to Port	80 -

OK Cancel

PORT FORWARDING CONTINUED

- Next, go to Policy > Policy > Policy
- Click on Create New

- Source Interface/Zone – wan1
- Source Address – All
- Destination Interface/Zone – internal (where device lives)
- Destination Address – port forward rule/rule's
- Schedule – always
- Service – ANY
- Action – ACCEPT

FortiGate 60C

Help | Logout | FORTINET

System
Router
Policy
- Policy
  - Policy
  - Sniffer Policy
  - Protocol Options
- Monitor

Firewall Objects
UTM Profiles
VPN
User
WiFi Controller
Log&Report

New Policy

Source Interface/Zone	wan1
Source Address	all
Destination Interface/Zone	internal
Destination Address	Port forward rule
Schedule	always
Service	ANY
Action	✓ ACCEPT

☐ Log Allowed Traffic

☐ Enable NAT

☐ Enable Identity Based Policy
☐ Resolve User Names Using FSSO Agent

☐ UTM
☐ Traffic Shaping
☐ Enable Endpoint Security [Please Select]

Comments Write a comment... 0/63

OK Cancel

VIRTUAL PRIVATE NETWORK (VPN)

- Extends a private network across a public network.
- It will enables a computer to send and receive data across a public networks as if it were directly connected to the private network.
- The 3 types that are supported is PPTP, SSL, and site-to-site IPSec

PPTP/SSL SET UP

- To set up PPTP go to Users > Users
- Create New or Edit an existing user
- Check add users to group check box
- The rest of the set up is on the client device, i.e. PC, Mac, Phone, Tablet

PPTP/SSL SET UP CONTINUED

FortiGate 60C

Help | Logout | FORTINET

System
Router
Policy
Firewall Objects
UTM Profiles
VPN
User
- User
  - User
  - Authentication
- User Group
- Remote
- FortiToken
- Single Sign-On
- Monitor

Edit User

User Name: pakedge

Disable

Password: ••••••

Match user on LDAP server [Please Select]

Match user on RADIUS server [Please Select]

Match user on TACACS+ server [Please Select]

Enable Two-factor Authentication

Add this user to groups

- IPsec Users
- PPTP Users
- SSL Users

OK | Cancel

NETWORK RESPONSIBLY

HOW TO CHANGE THE IP ADDRESS FOR A NETWORK

- We would want to change the IP range is for a few reasons:
  1. Was an existing network and to many static address to change
  2. Just don't like the 192.168.1.x network range
  3. It is just the way you like your network to be set up

NETWORK RESPONSIBLY

HOW TO CHANGE THE IP ADDRESS FOR A NETWORK CONTINUED

- There are 3 different locations to go to if you want to change the network subnet.
  1. Change the DHCP range under System > Network > DHCP Server then edit desired network
     - Change the "IP" to the network range you want the router to had out, i.e. 192.168.10.110 – 192.168.10.199
     - Next change the Default Gateway and DNS Server 0 to the address that you want the router to be, i.e. 192.168.10.1
  2. Now we can change the interface address under System > Network > Interface and edit the same network from the above step.
     - Change the IP/Netmask to what you want the router to be, i.e. 192.168.10.1/255.255.255.0
  3. Finally we need to go to Firewall Objects > Addresses > Address and edit the network that we want to change.
     - Change the Subnet / IP Rage, i.e. 192.168.10.0/255.255.255.0

NETWORK RESPONSIBLY

HOW TO CHANGE THE IP ADDRESS FOR A NETWORK CONTINUED

FortiGate 60C

System
- Dashboard
  - Status
- Network
  - Interface
  - DNS
  - DNS Server
  - DHCP Server
  - Explicit Proxy
  - Modem
- Config
- Admin
- Certificates
- Monitor

Edit DHCP Service

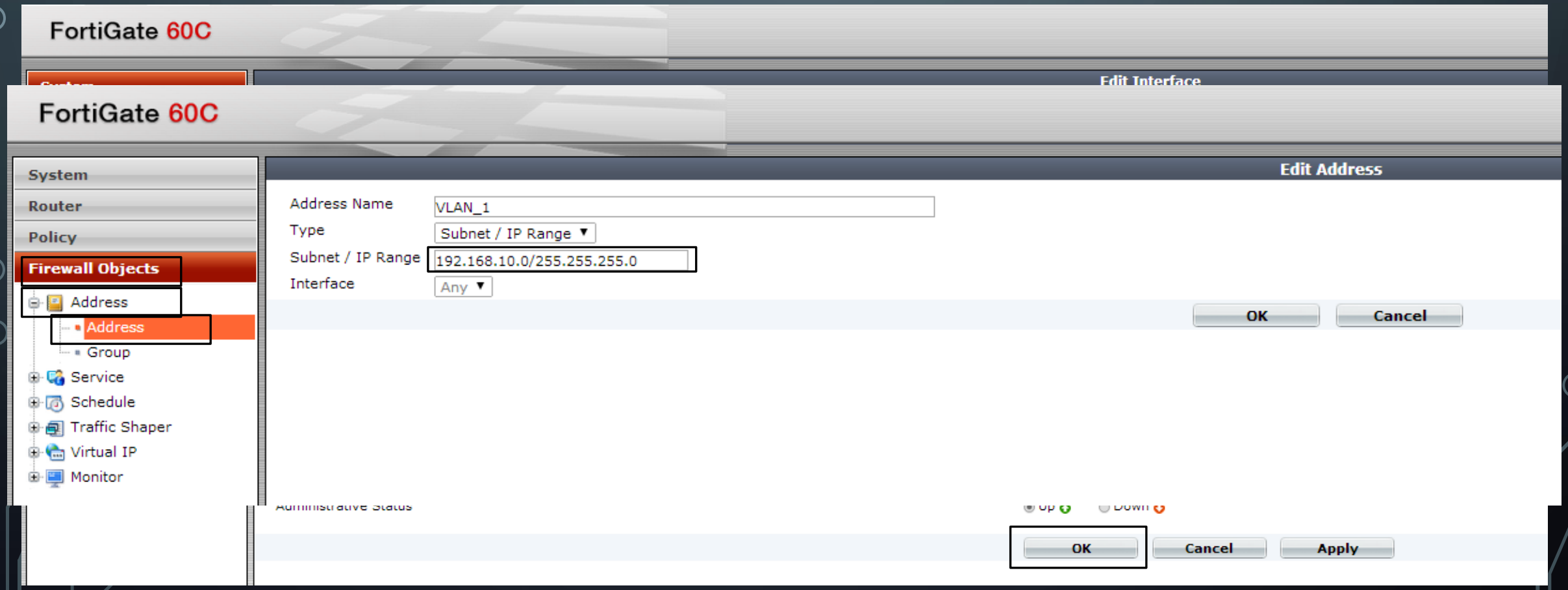
Interface Name	internal
Mode	Server
Enable	☑
Type	◉ Regular ○ IPsec
IP	192.168.10.110 - 192.168.10.199
Network Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Service	○ Use System DNS Setting ◉ Specify
DNS Server 0	192.168.10.1
DNS Server 1	

☐ IP Reservation

▸ **[Advanced...]** (DNS, WINS, Custom Options, Exclude Ranges.)

OK Cancel

HOW TO CHANGE THE IP ADDRESS FOR A NETWORK CONTINUED



HOW TO CHANGE THE ROUTER TO BE 192.168.1.1

- Many people call about how to do this
  - 1.1 just makes sense to them
  - Replacing other router that was set at 1.1
  - Setting to 1.1 will make it easier to widen DHCP range
- To change go to System > Network > DHCP Server then edit internal
  - Change only the Default Gateway and DNS Server 0 to be 192.168.1.1
- Then go to System > Network > Interface and again edit internal
  - Change IP/Netmask to be 192.168.1.1/255.255.255.0

NETWORK RESPONSIBLY

HOW TO CHANGE THE ROUTER TO BE 192.168.1.1 CONTINUED

FortiGate 60C

System
- Dashboard
  - Status
- Network
  - Interface
  - DNS
  - DNS Server
  - DHCP Server
  - Explicit Proxy
  - Modem
- Config
- Admin
- Certificates
- Monitor

Edit DHCP Service

Interface Name	internal
Mode	Server
Enable	☑
Type	◉ Regular ○ IPsec
IP	192.168.1.110 - 192.168.1.199
Network Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Service	○ Use System DNS Setting ◉ Specify
DNS Server 0	192.168.1.1
DNS Server 1	8.8.8.8

☐ IP Reservation

▸ **[Advanced...]** (DNS, WINS, Custom Options, Exclude Ranges.)

OK Cancel

SETTING UP WAN CONNECTION

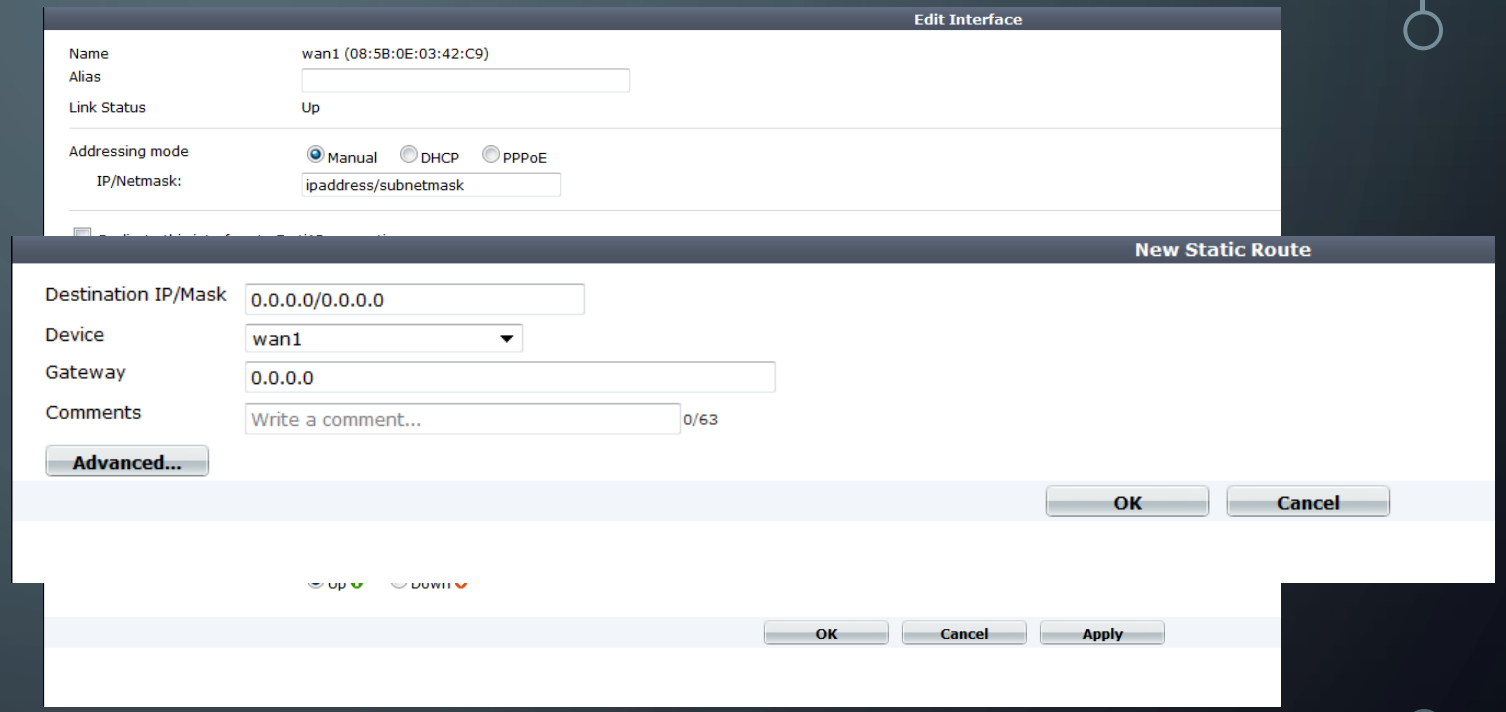
- There are 3 different types that you can run into when seeing up internet on the router.

1. The most common is DHCP. This is what you run into most likely everyday you don't have to do anything just connect it to the modem provided by the ISP and you have a public IP address. Nothing you have to do set by default.
2. The next type is PPPoE, more commonly used with DSL providers. This is they way they authenticate to make sure that a subscribed customer is able to use there service. This requires a username (typically email address) and a password.

NETWORK RESPONSIBLY

MANUAL/STATIC ADDRESS

1. Manual aka Static IP address. Normally you have to pay extra for static IP addresses and the address is provided by the ISP.
   - Go under System > Network > Interface and edit wan1, set mode to Manual and enter IP and Subnet provide by the ISP, i.e. 69.227.93.157/255.255.255.252
   - Next go to Router > Static > Static Route and Create New, add the default gateway provided by the ISP, i.e. 69.227.93.156



NETWORK RESPONSIBLY

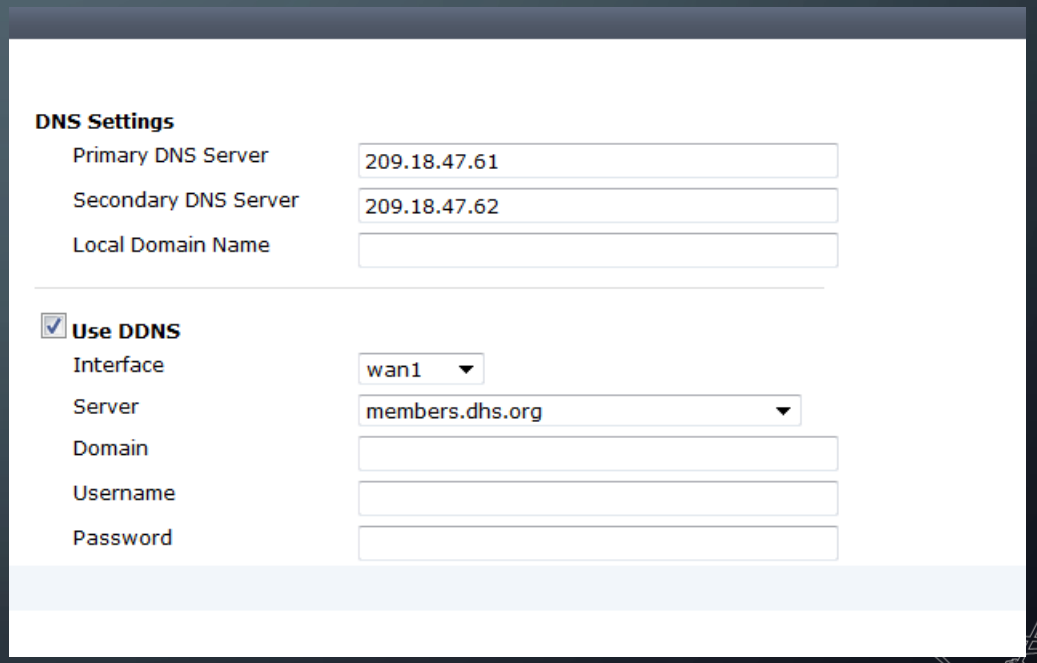
SETTING UP DDNS

- If you have a location with a dynamic public IP address (router set to DHCP) and you want to VPN, remotely manage, or access services from the outside you will need to know the IP address.
- This can be very difficult depending on the ISP because of how frequent it changes
- DDNS is the solution, it automatically updates the host name that you registered, often in real time, with the public IP address.

NETWORK RESPONSIBLY

SETTING UP DDNS CONTINUED

- To do this go to System > Network > DNS and check Use DDNS, select the correct sever from the drop down list and enter in your credentials and hostname.



NETWORK RESPONSIBLY

THANK YOU!

BY LUIS SERRANO

ON BEHALF OF PAKEDGE DEVICE&SOFTWARE INC.

NETWORK RESPONSIBLY