VIA

HOW TO CONFIGURE A ‘DMZ’ FOR SECURE COLLABORATION

By Lars Duziack

KRAMER WHITE PAPER

WWW.TRUE-COLLABORATION.COM

TABLE OF CONTENTS

INTRODUCTION

DMZ is an abbreviation for 'Demilitarized Zone.' In a world of ever-increasing and sophisticated security threats and hacks, a DMZ will be an essential part of your network to help you guard against unauthorized access. It is positioned specifically between your internal & guest IP networks to allow safe and simultaneous communication and collaboration between those networks.

The DMZ you'll read about in this paper securely isolates any Kramer VIA product – Collage, Campus, or Connect PRO - that can be accessed from any and all other devices on your internal and external (guest) networks. This additional layer of security ensures that users of an external network cannot directly address and access an internal network in a "back door" manner through any VIA product.

Internal networks always contain more proprietary and/or valuable information than guest or external networks. And the simplest way to differentiate internal and external networks is to determine which network needs protection from the other.

A DMZ is usually located on external networks that have an Internet connection to the outside world. It is common practice to run a separate web server inside a DMZ. However; in our case, the DMZ described in this manual will be used to isolate a connected VIA product from all other devices located on both internal and guest networks.

The concept of a DMZ is familiar to companies that already operate multiple subnets to separate guest computers, internal computers, and other IP-addressable devices. Since different IT applications have specific QoS and bandwidth requirements, it's common practice to create specific subnets to run these applications.

The same principle is at work here. Adding a DMZ to create network separation for VIA products may slow down network speeds to some extent, but if the DMZ is configured correctly, any reduction in speed will be minimized - and the increase in internal network security will be significant.

HOW TO DESIGN A DMZ

Let's start with the basics.

STEP 1: Determine which devices are assigned to internal or guest networks

STEP 2: Secure the entrance port for your network

At first glance, these steps might seem easy to follow. But you may find more than one entryway to your network, and this will mean more points to monitor for security. For the example in this paper, we'll focus on a single entrance port.
Minimalism should be your goal when implementing network security.

Determining which devices are assigned to internal or guest networks

After verifying which devices you need to protect, you must first locate them on your secure internal network. Also, make sure you know how these devices will communicate with the VIA platform that you're going to install in the DMZ. Kramer's IT Deployment Guide will provide you with details about all of the relevant ports that are needed for communication with VIA. You will also need to set up your existing network firewall to allow only VIA-specific traffic. Again, cross-check with Kramer's IT Deployment guide to determine which protocols and ports are used.

Guests will bring their own devices to collaborate through VIA and accordingly will require their own subnet within your existing network. The access point for this subnet will be separate from your internal network. (Make sure all such access points are part of your guest network!) You may also want your firewall to provide DHCP addressing to your guests. (DHCP addresses can be also assigned by a router or server within or outside the guest network.)

Securing the entrance port for your network

Typically, this will be an ISP router with an integrated modem. Locate the entrance port and ensure your network firewall is working correctly. Check for passwords and usernames that may not comply with today's advanced security terms – passwords should contain at least 16 characters and include a mix of small letters, capital letters and special characters. Usernames should be changed from factory default settings like "admin" or "root" to something more advanced.

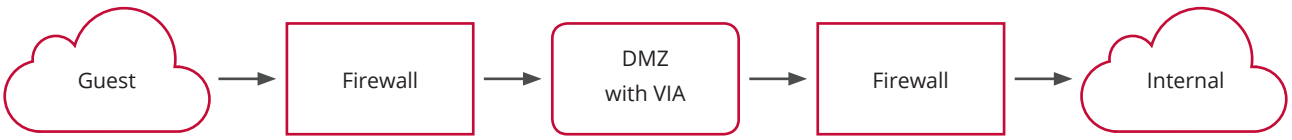
Example: Common default username and password combinations that must always be changed

User: admin / Password: password
Or
User: root / Password: toor

SETTING UP A DMZ WITHIN A FIREWALL

You can use one or more firewalls to set up a proper DMZ. In this paper, we will focus on a single firewall configuration with a guest network connected to our VIA system within the DMZ.

You can add additional firewalls for increased security. In this case, it is common practice to configure one firewall to be in front of the DMZ and the other one behind it.



The “front” firewall should be located between the guest network and your DMZ, while the “rear” firewall sits between the DMZ and your internal network. In this scenario; even if one firewall fails, guest traffic will still be blocked from your internal network. It’s also a good idea to use different vendors for each firewall, as it’s unlikely that an attacker will know how to get past two different firewall designs.

How to configure your firewall interfaces

For a single-firewall dual-network solution, you will need to define three interfaces.

Internal
Guest
DMZ

Check to see if these interfaces need to provide DHCP addressing, or if you already have a DHCP server running elsewhere in the specific subnet where the VIA platform will be connected. It is highly recommended to run DHCP addressing within your guest network environment to provide flexible and easy IP address assignments to BYOD (Bring Your Own Device) clients.

Next, limit administrative access to your interfaces. Make sure you close off all unnecessary access modes to prevent unauthorized access.

Select the correct IP addressing mode for your Firewall interfaces (static or DHCP) and advise users of the correct IP address and subnet if static addressing is used. All configuration information will be provided by the firewall through DHCP requests from clients. Note that you may need to configure static routes if you’re running an additional device that provides DHCP.
(Never run more than one DHCP server per subnet!)

Activate **“Multicast”** policies in your firewall. This option is usually deactivated to prevent overloading the network with data packages from applications like Bonjour. Multicast policies must be activated to permit AirPlay operation through a specific subnet. To allow AirPlay on all subnets, define a new policy with a list of all source interfaces and the outgoing interface to the DMZ. You will also have to add two more firewall policies from the incoming interface DMZ to the outgoing interfaces **internal** and **guest**. If your Firewall allows adding multiple interfaces into one policy, you can define the policy as “internal, guest“.

All Airplay/Bonjour packages sent through the network have a characteristic **TTL (Time To Live)** that typically has a value "**1**". This can create a problem because the router / firewall starts requesting the package after 85% of its TTL. At this point, you can see the AirPlay device on your subnet, but you can't view your display. Most firewalls can set different TTL values or otherwise alter the TTL after a package request. **Make sure your firewall / router does not change the TTL.**

We will now define the services from each subnet to the **DMZ** and from the **DMZ** to the **internal** and **guest** networks. Locate the **Service Options** menu for your firewall and create and name a new service. Add the specific ports and protocols for each service. The minimum number of services you will create here is two, with the first defining traffic from all clients to VIA and from VIA to your clients. (It is highly recommended to define multiple services for guest and internal devices. Make sure you also add a service for AirPlay.)

Ports from/to VIA

TRAFFIC CLIENT TO VIA	TYPE	FUNCTION
5222	TCP	communication Data TLS/SSL
7001 - 7024	TCP	Audio
7777	TCP	File Sharing
5555	TCP	File Sharing
9955	TCP	Streaming Video
9954	TCP	Streaming Video
9985	TCP	Authentication
9982	TCP	API Commands
9986	TCP/TLS	API Commands -TLS
9994	TCP	Android mirroring /Step-In
9987	TCP	unresolved (maybe iPad mirroring)
9989	TCP	Collaboration
9990	TCP	Step-IN
9993	TCP	Step-IN
80 / 8080	TCP	HTTP
443	TCP	HTTPS
9992	TCP	View Main Display
22	TCP	SSH
9984	TCP	Replaced with 9985 SSL based

iOS TO VIA	TYPE	FUNCTION
46000 - 46200*	TCP	Server Port / Initialisation
8000 - 8200*	TCP	Event Port
7100 - 7300*	TCP	Data
5001 - 5201*	UDP	Control & Data iOS
2001 - 2201*	UDP	Time Port
5353	mDNS/UDP	mDNS Bonjour/Airplay Broadcast
7010	UDP	RoomCode Replaced included in 46000+ now

* If Port is busy or not available will jump to next available Port and try to bind (Max Range 200 Ports)

VIA TO iOS	TYPE	FUNCTION
5353	mDNS/UDP	mDNS Bonjour/Airplay Broadcast

VIA TO CLIENT	TYPE	FUNCTION
9954	TCP	Streaming from OSX to VIA static Port at Client
3500-3599	TCP	Range of ports to send data from Client
80	TCP	Andorid/ iOS app straming
8080	TCP	Andorid/ iOS app straming
12345	TCP	Streaming Sync & ACK iOS Only

VIA TO SRV	TYPE	FUNCTION
389	TCP/UDP	AD/LDAP
53	TCP/UDP	DNS

VSM TO VIA	TYPE	FUNCTION
9988	TCP	API server used by VIA to VSM
5555	TCP	Files server for update firmware and wallpaper etc
80 / 8080	TCP	Webserver HTTP
443	TCP	Webserver - not in use now but we will use it for https

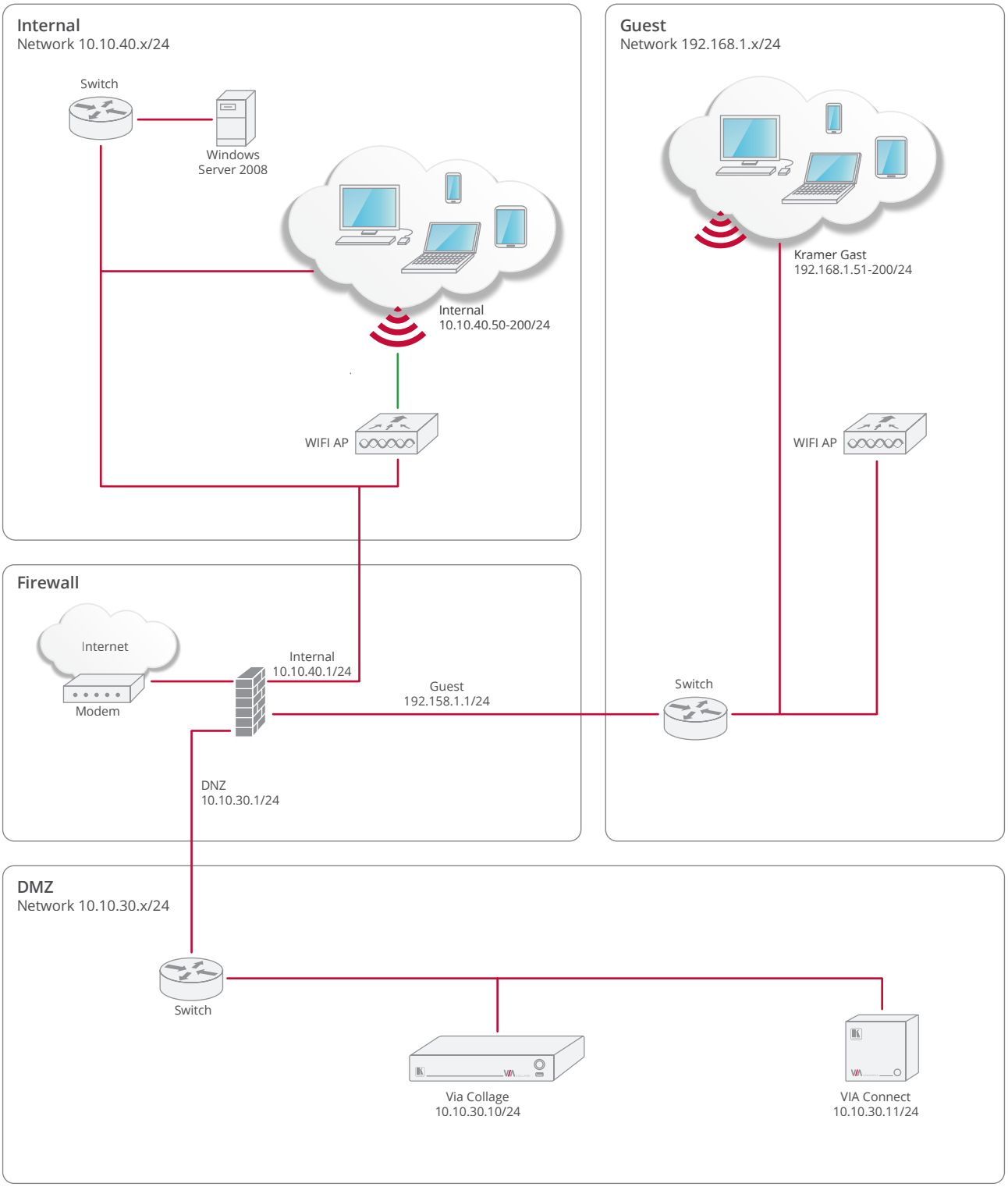
PC TO MOBILE DEVICES	TYPE	FUNCTION
12345	TCP	Webbrowser data transfer
20000	TCP	FTP Data Transfer

PORTS TO “ENABLE INTERNET” IN ACCESS POINT MODE (Connect PRO)

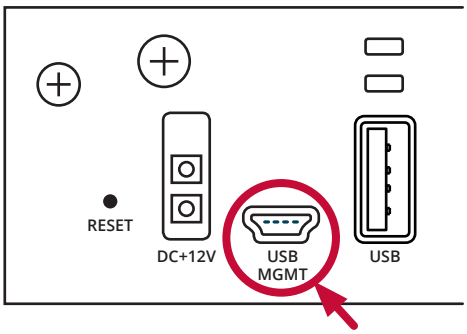
PORT	TYPE	FUNCTION
80	TCP	HTTP
443	TCP	HTTPS
25	TCP	SMTP
465	TCP	SMTP over SSL
587	TCP	SMTP message submission
53	TCP	DNS
53	UDP	DNS

STEP-BY-STEP GUIDE TO INSTALL A FORTINET FIREWALL

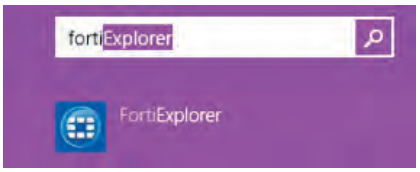
1. Download and install the software program "**FortiExplorer**". This will allow you to connect to the FortiGate 60D.
   Download Link: http://www.fortinet.com/resource_center/product_downloads.html



2. After installing the software, you can power up the FortiGate 60D and connect it via a USB cable to your computer.

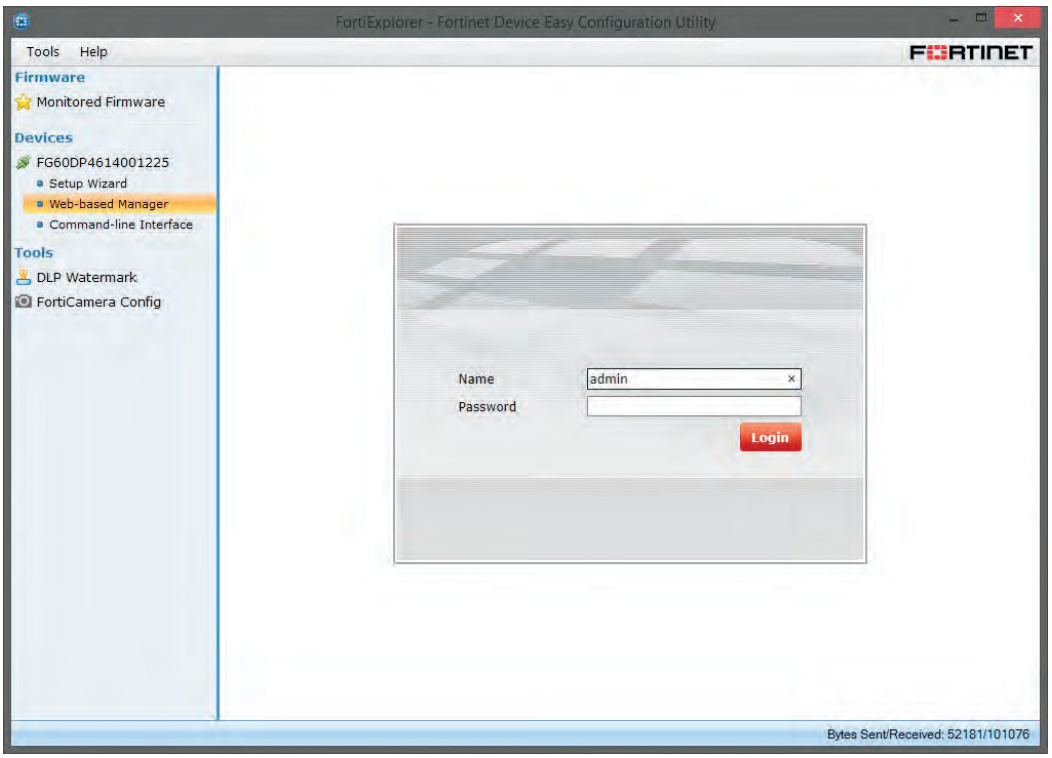


3. Launch the **FortiExplorer** program.



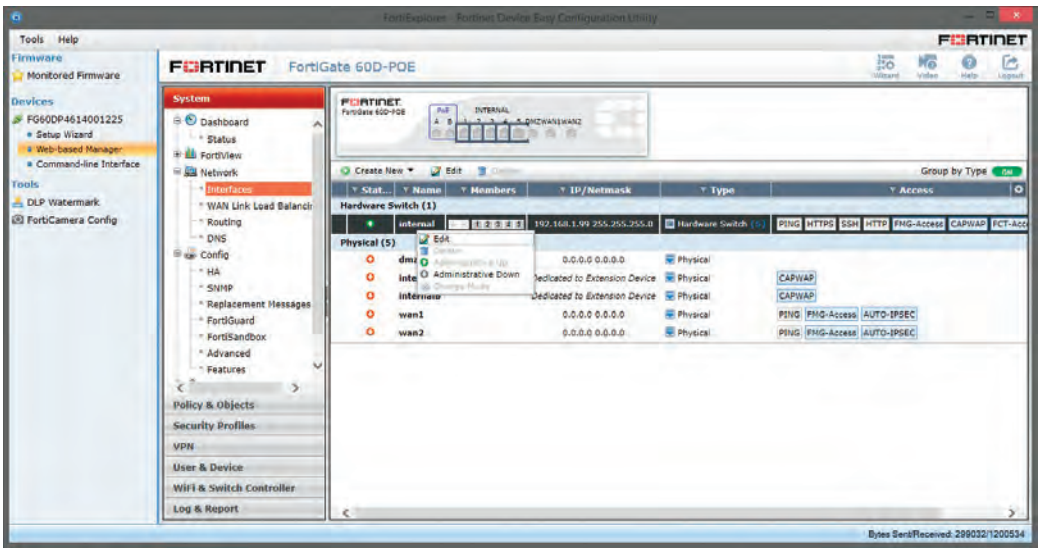
4. Under the **Devices** tab, select the **FortiGate 60D**.

5. Select the **Web-based Manager** tab on the left side.
   a. Enter the default username and password (Username: admin / Password: -Blank-)
   b. Login to start configuring the FortiGate 60D.

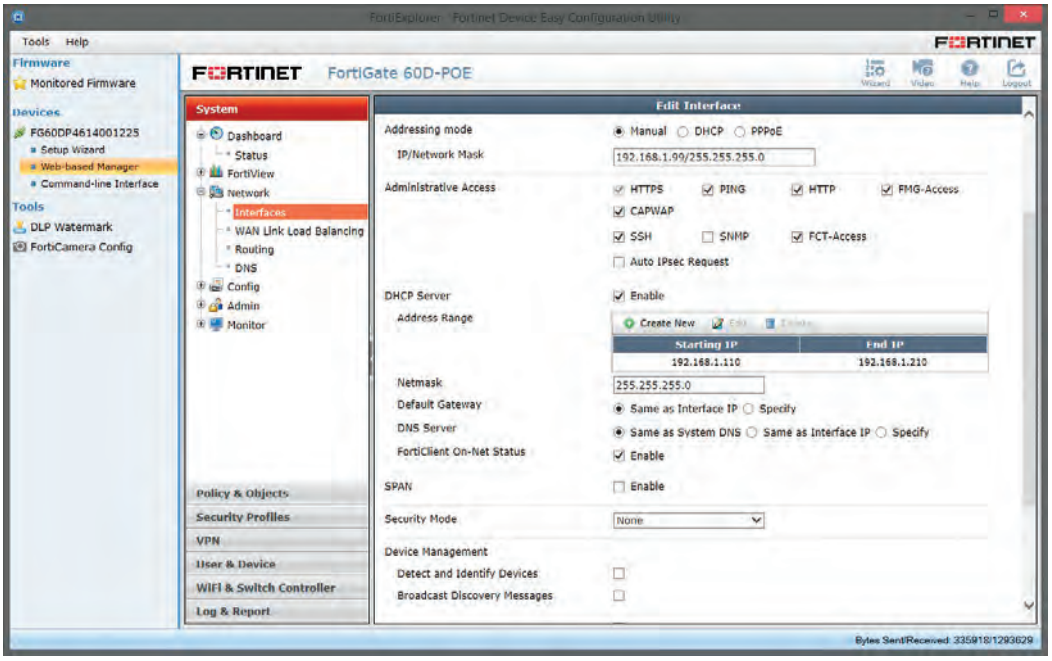


6. We will now configure the interfaces for these networks:
   a. **DMZ** (with VIA Collage / VIA ConnectPro / VIA Campus)
   b. **Internal** (with all your internal devices that belong to the company and are trusted)
   c. **Guest/Internal** (with all untrusted devices that will connect to VIA)

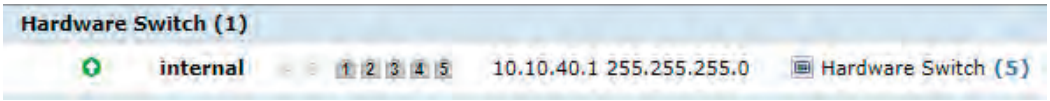
7. Select the top level interface. In this case, it's the **Internal** network interface.
   a. Right-click this interface and click **Edit** to enter the settings page.



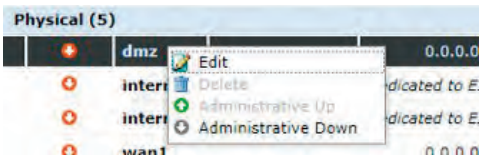
8. You will need to change the **IP/Network Mask** settings. In most cases, these initial settings will not work with your network. (Our Internal network is set to "**10.10.40.x/24**" and you may change this value as required.) After changing the **IP/Network Mask** field to "**10.10.40.1/255.255.255.0**" you will need to change the DHCP range as well. Set DHCP values to start at "**10.10.40.50**" and end at "**10.10.40.200**", as shown in our schematic view. If you're already running a DHCP server on your network, you can disable DHCP on that interface.



Once configured, your **Interfaces** overview will display the Internet interface as follows:

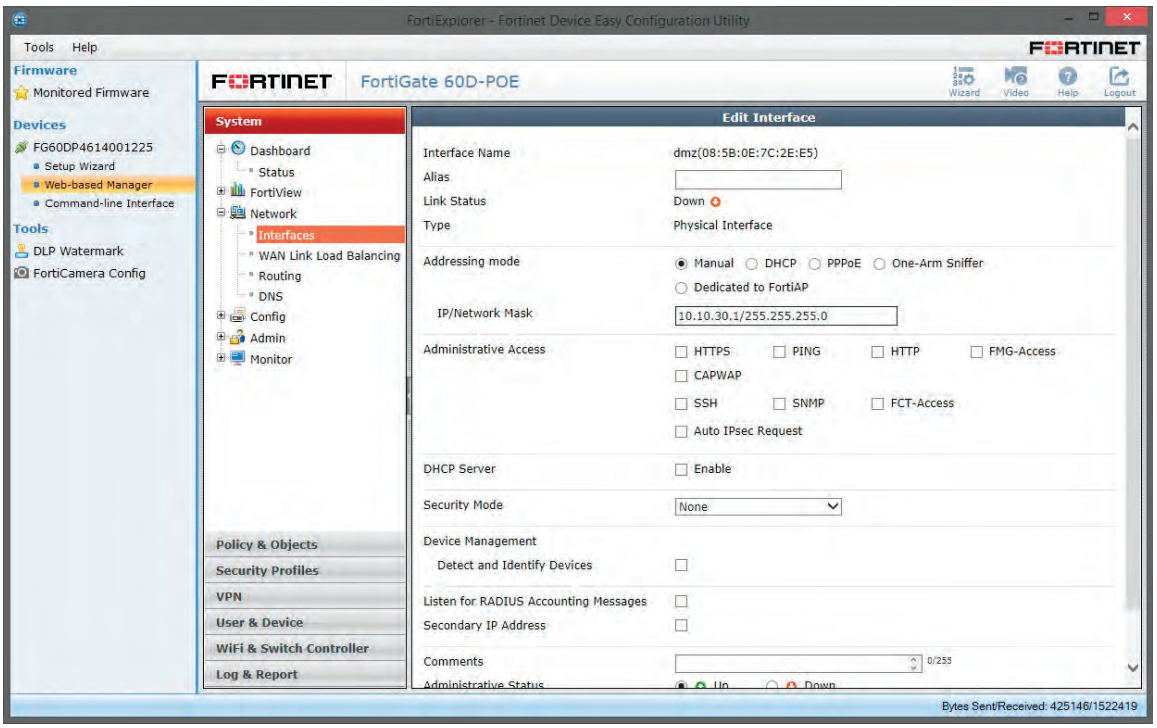


9. Now, continue to edit the **DMZ** and **Guest** interfaces. Follow the previous steps and edit each interface as required.
Right-click on DMZ and choose edit.

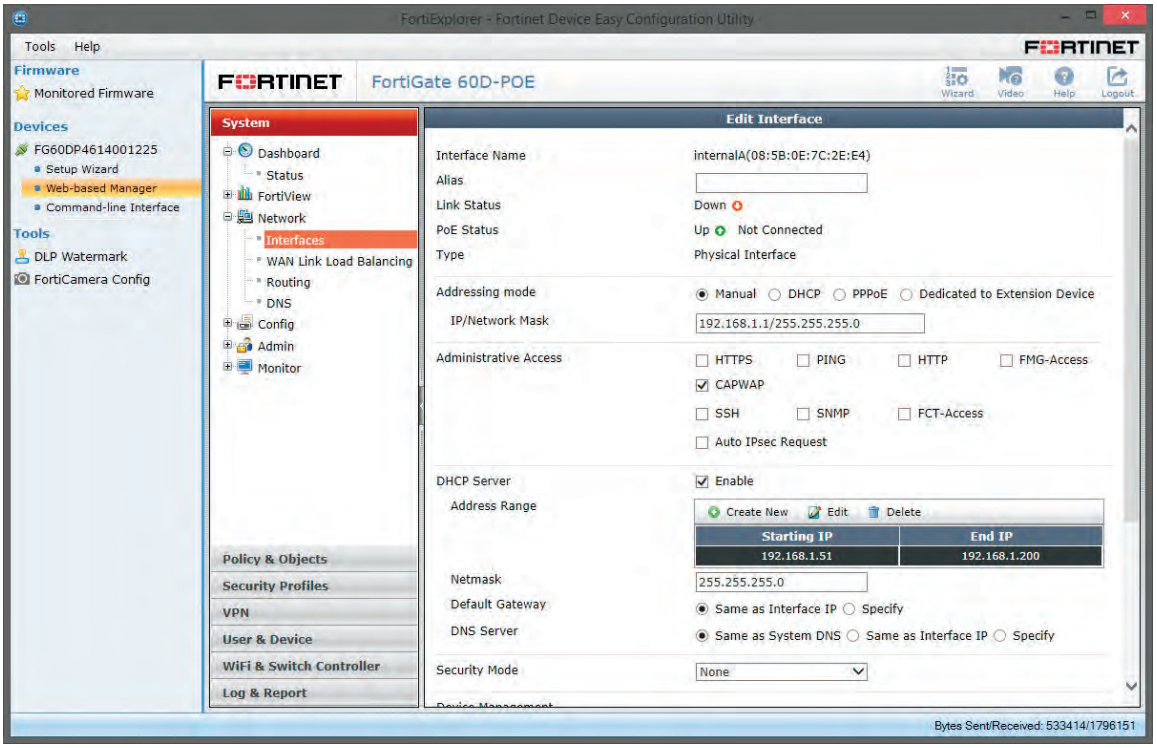


Edit the IP/Network Mask field to:
"10.10.30.1/255.255.255.0"
Remember: You can enter your preferred IP and network mask.

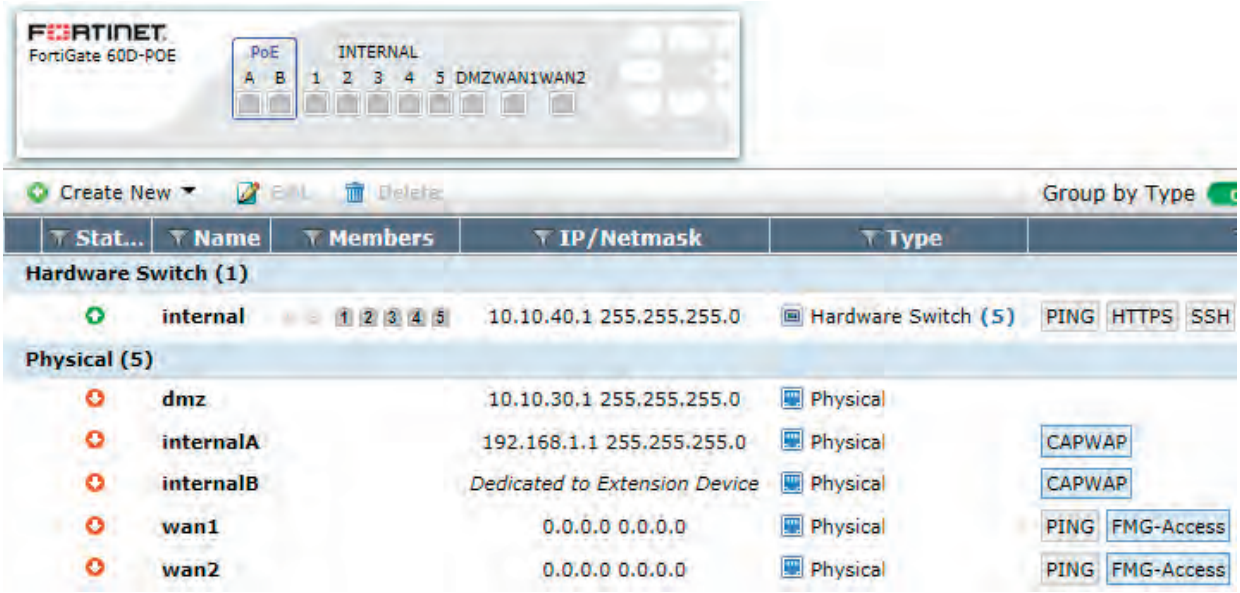
It is not necessary to have a DHCP server running in the DMZ, so disable it if this option is enabled.



10. Now, configure the internal interface settings for your **Guest** network. Edit the **IP/Network** mask again as required. For our example, we will use "**192.168.1.1/255.255.255.0**". Also, we will need the DHCP server to run on our firewall with a range from "**192.168.1.51**" to "**192.168.1.200**".

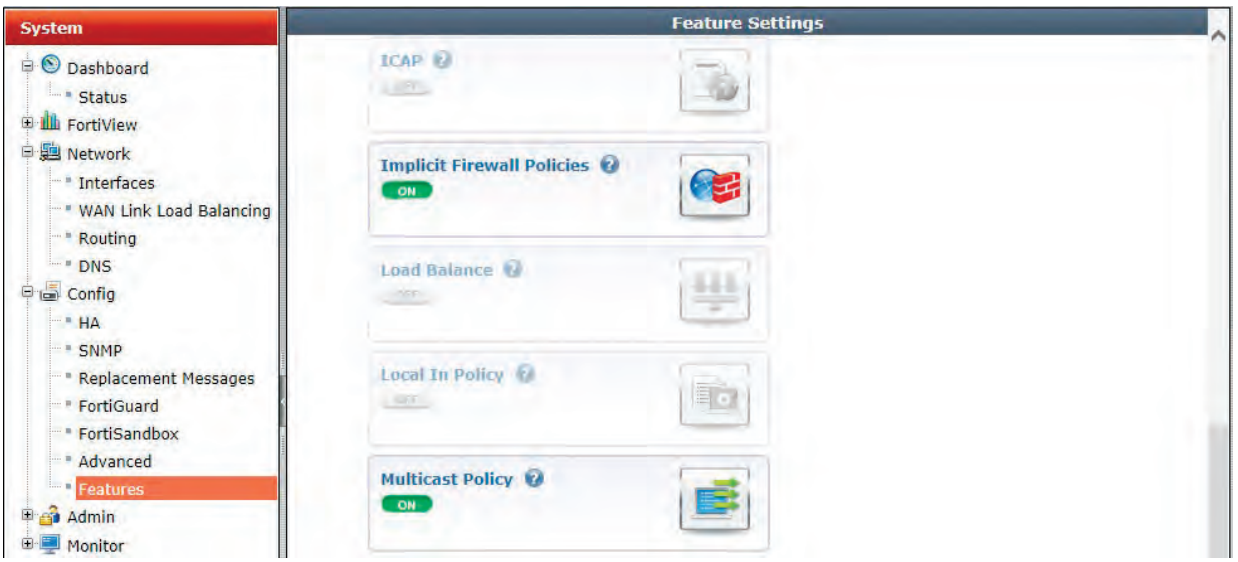


After you've completed these steps, your Physical Interface view should look like this:

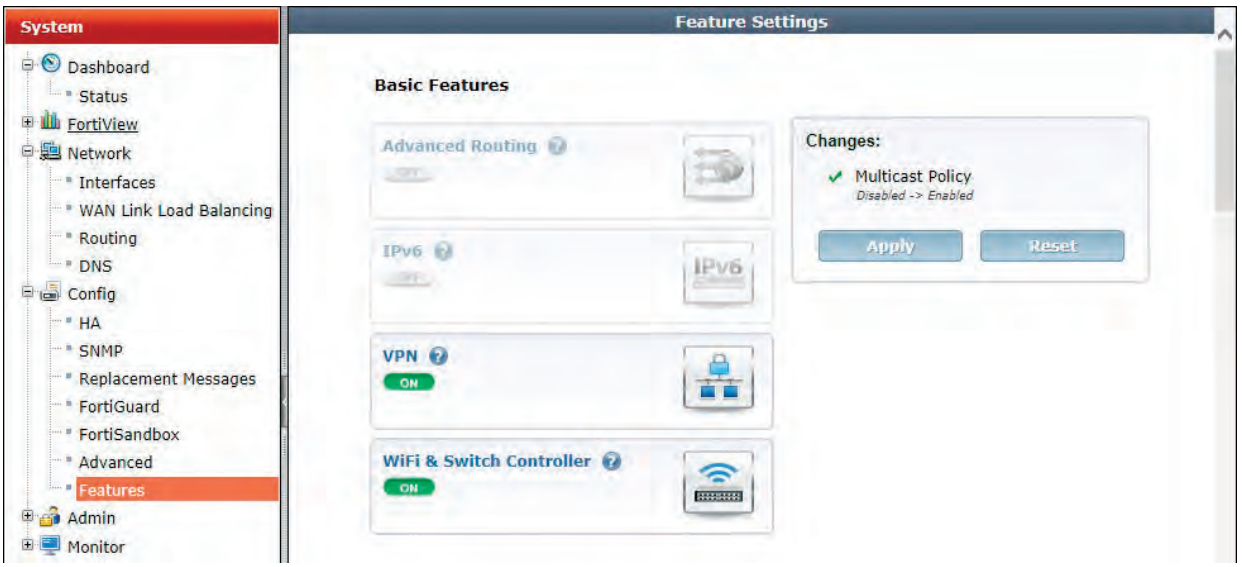


11. In the default configuration, our firewall will not allow for multicasting. However, since the VIA product line uses AirPlay and Bonjour, you should enable multicasting.

    Go to: **System → Config → Features**
    Scroll down to **Multicast Policy**. (You may need to click "show more" to see this option.)



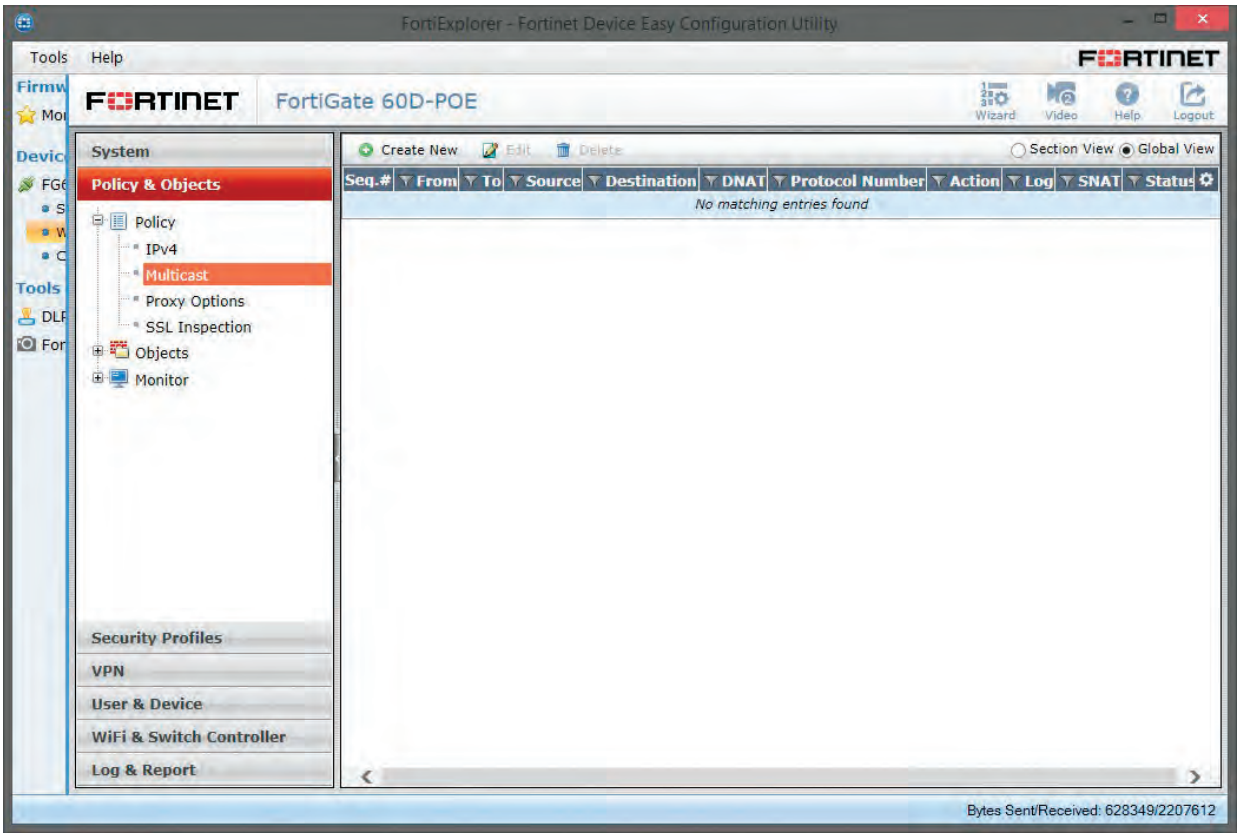
To save your changes, scroll back to the top of **Feature Settings** and click on **Apply**.



12. After successfully activating the **Multicast** feature, a new sub-menu will appear under **Policy & Objects**.

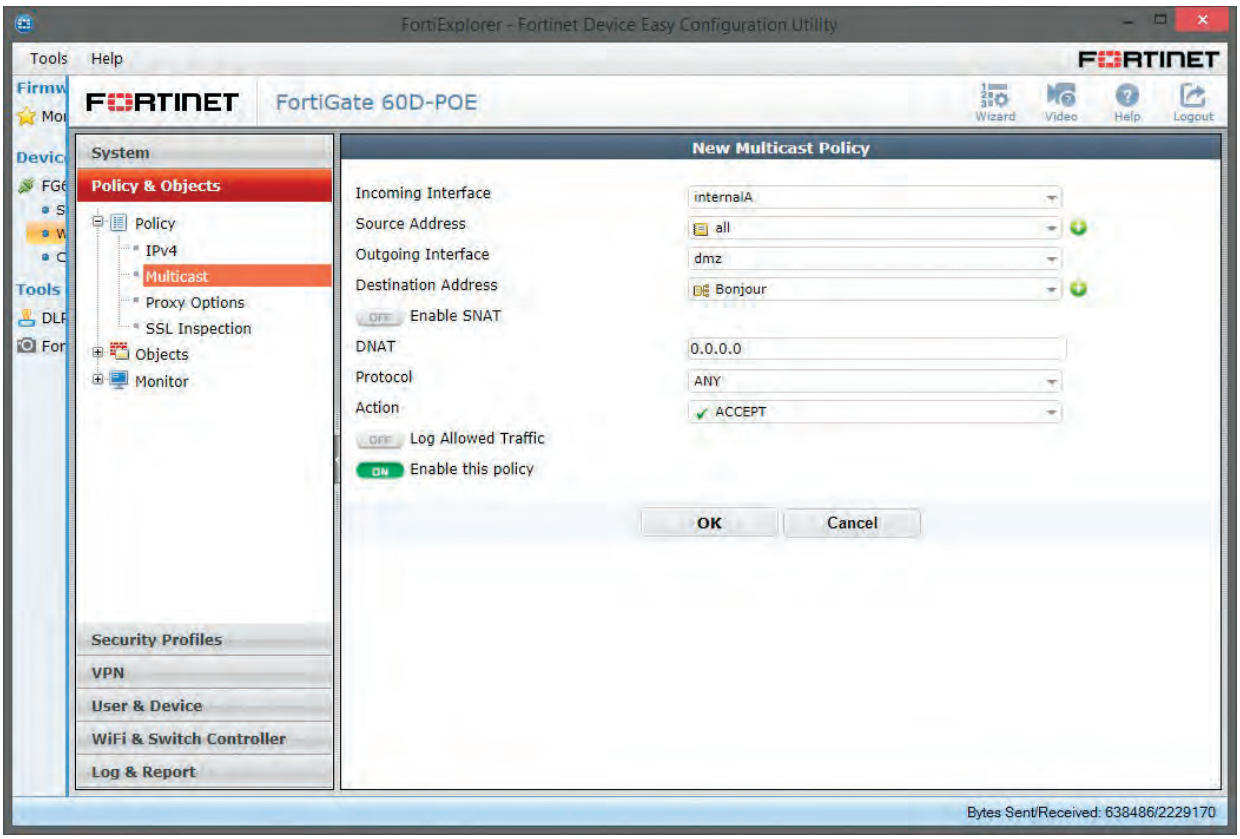
    Go to: **Policy & Objects → Policy → Multicast**

    To allow AirPlay and Bonjour through our networks, we will first need to add four policies to our firewall. Click on **Create New**.

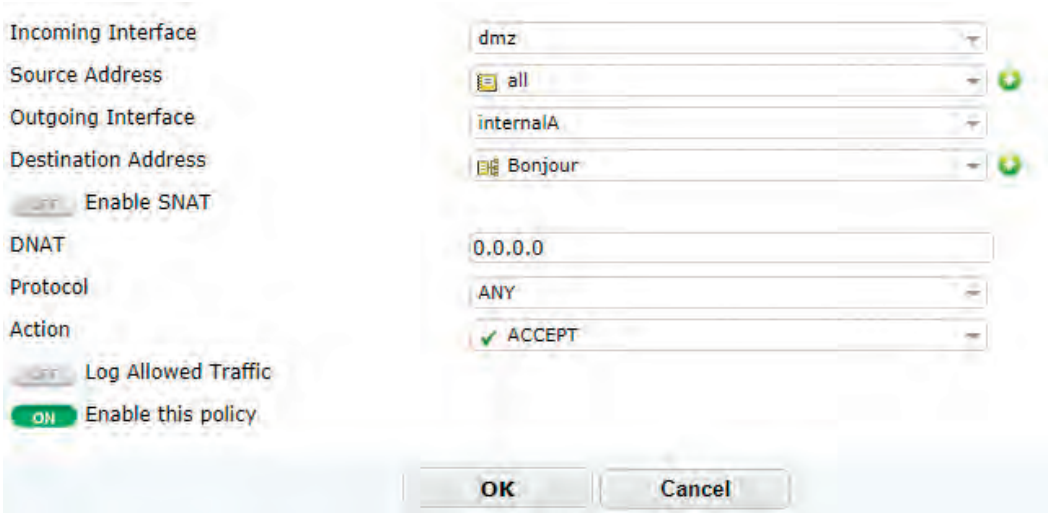


13. Our first policy will allow AirPlay/Bonjour from the **internalA (Guest)** interface to the DMZ.

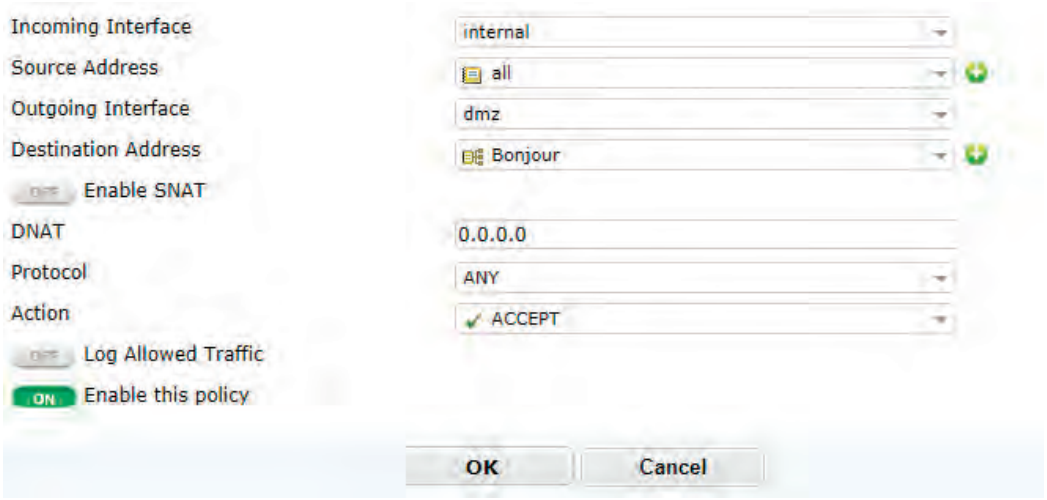
For the incoming interface, choose **internalA**
For source address, choose **all**
For the outgoing interface, choose **DMZ**
The destination address is **Bonjour**
Select **OK** to save your changes



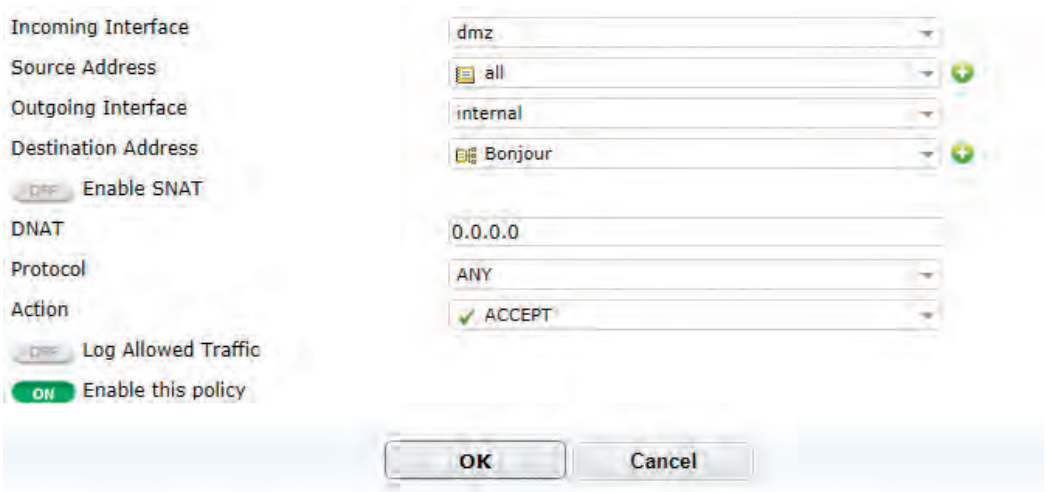
14. Our second policy will define traffic in the opposite direction from **DMZ** to **internalA**. Confirm the settings shown below by selecting **OK**.



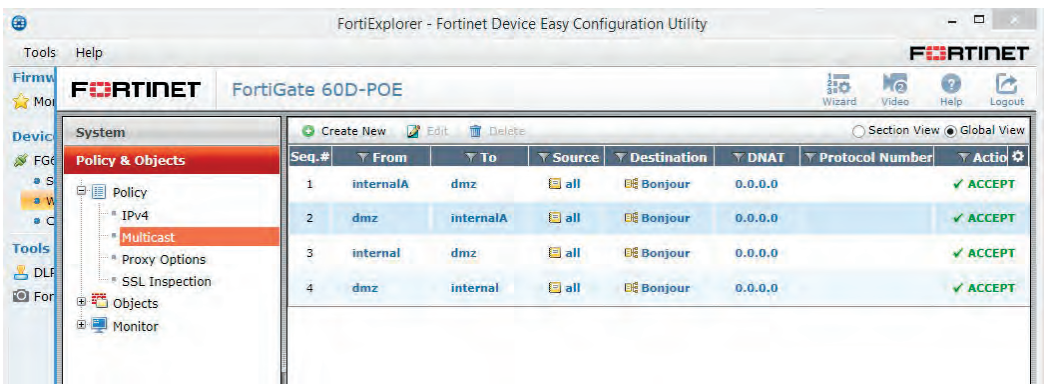
15. Our third policy will allow communication from the **internal** network to the **DMZ** network. Confirm the settings as shown below and select **OK**.



16. Finally, the last policy we have to create is to allow communication from **DMZ** back to **internal**. Confirm the settings as shown below, and select **OK**.



17. The **Multicast** tab overview should look like this now.

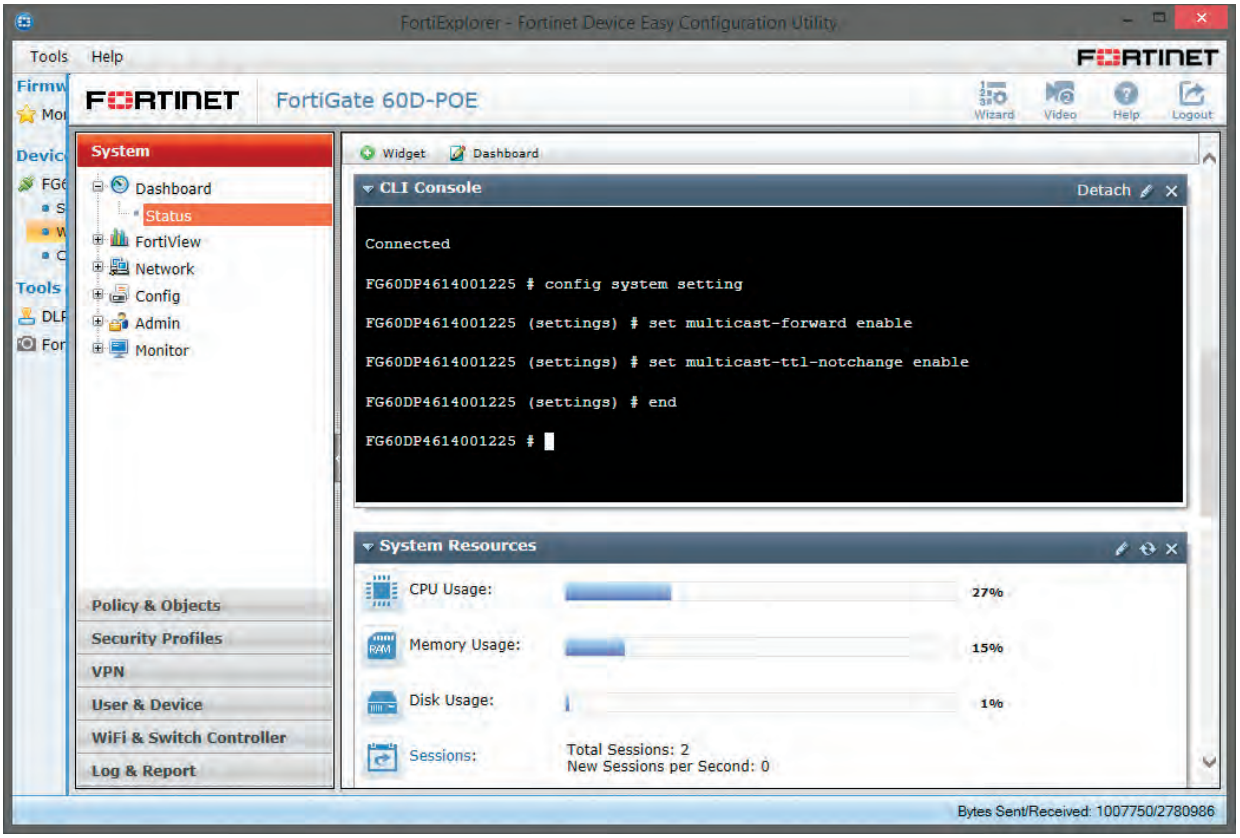


18. As mentioned earlier, the **Time To Live (TTL)** value for each package is very important. Our entire AirPlay/Bonjour package should pass through the firewall unaltered. To enable this, we will first have to enter some CLI commands into the firewall.
Go to: **System → Dashboard → Status**
Scroll down till you find the **CLI** console

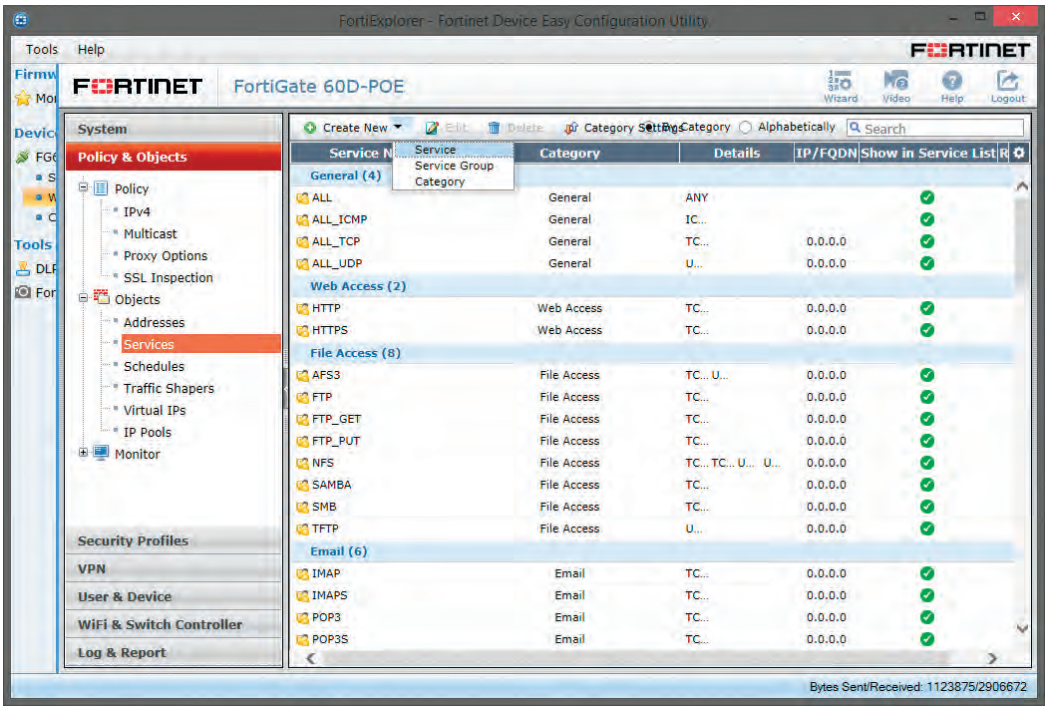
Click into the black area, and enter the following lines of text.
Note: you cannot copy and paste text here!

a. config system setting
b. set multicast-forward enable
c. set multicast-ttl-notchange enable
d. end

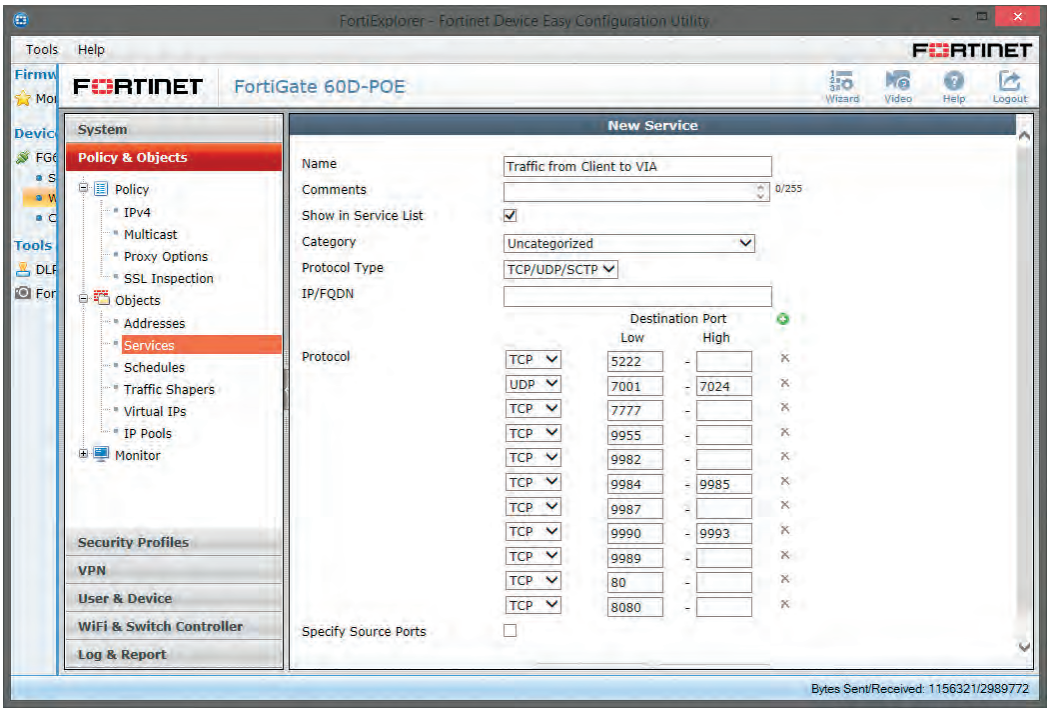
```
Connected

FG60DP4614001225 # config system setting

FG60DP4614001225 (settings) # set multicast-forward enable

FG60DP4614001225 (settings) # set multicast-ttl-notchange enable

FG60DP4614001225 (settings) # end

FG60DP4614001225 #
```



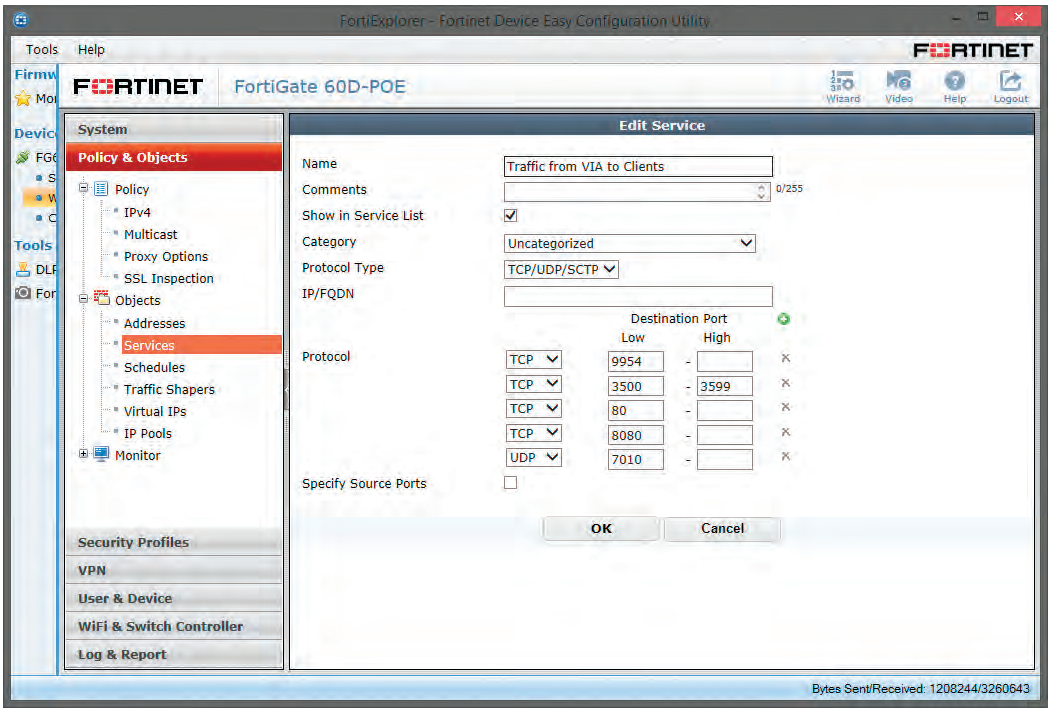
19. We're halfway there! Now, we have to define policies for the VIA Ports.
Go to: **Policy & Objects → Objects → Services**
Click on **Create New** and choose **Service**



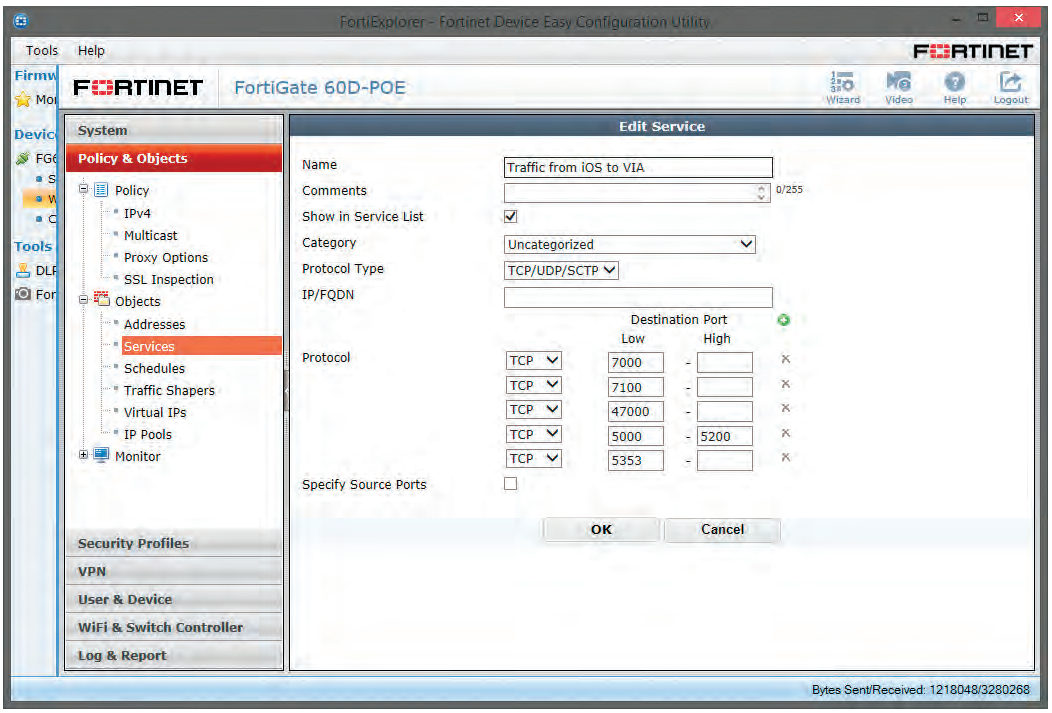
20. Name the new service **Traffic from Client to VIA**, or choose a name that fits your needs. All the ports that will be needed for communication are well-documented in our IT Deployment guide. Additional ports can easily be added by clicking on the green "plus" sign.



21. Two more services must be defined. Create a new service and name it **Traffic from VIA to Clients**.

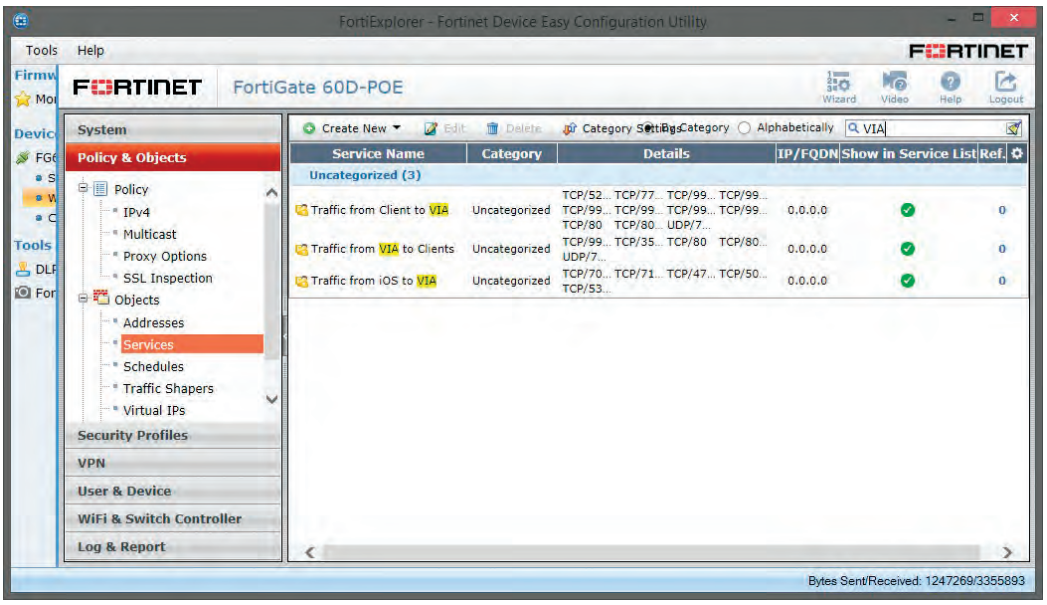


22. Our last service will contain all iOS ports in use. Name this service **Traffic from iOS to VIA**.



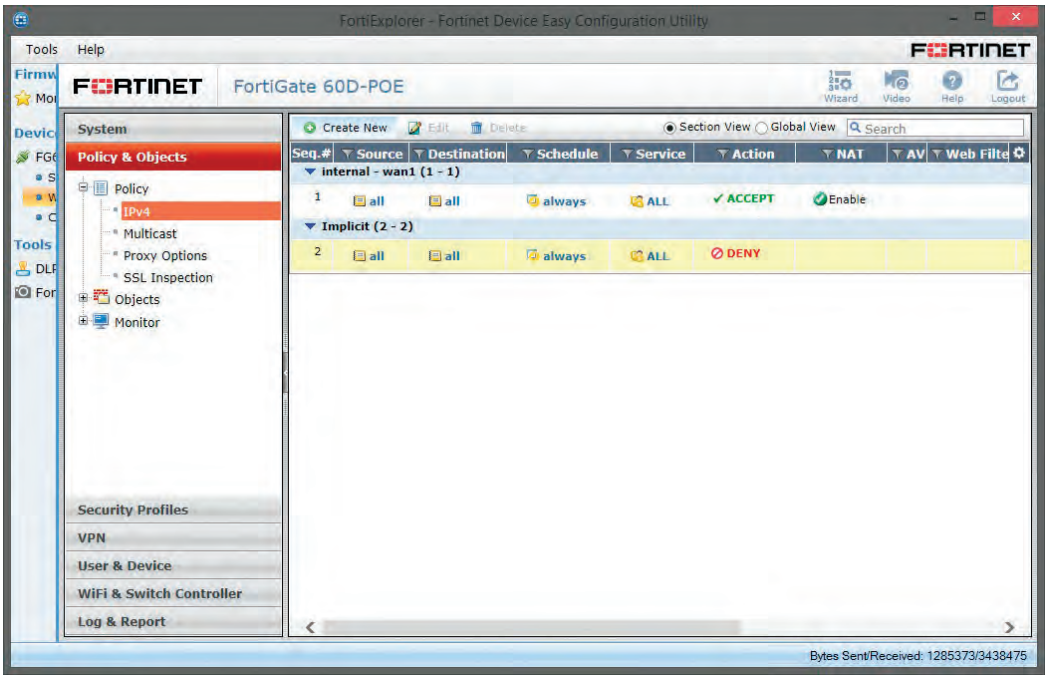
23. In the **Services** menu overview, you can filter for specific content within the service names. Search for **VIA** to see all related services.

    The menu should look like this:



24. Now, we need to create the traffic rules between the networks. This step will show how to allow communication for **internal** to **DMZ**, **InternalA(Guest)** to **DMZ**, and in reverse directions for both.

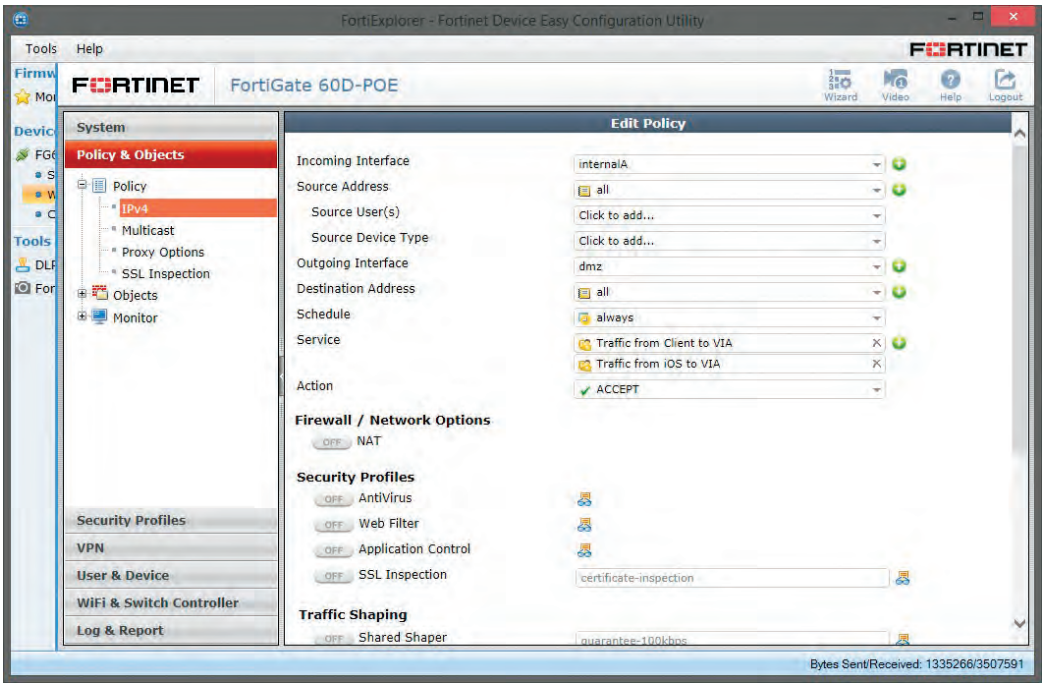
    GoTo: **Policy & Objects → Policy → IPv4**
    Create a new policy by clicking on **Create New.**



25. To create this new policy, we will re-enter all the previous policy information again.

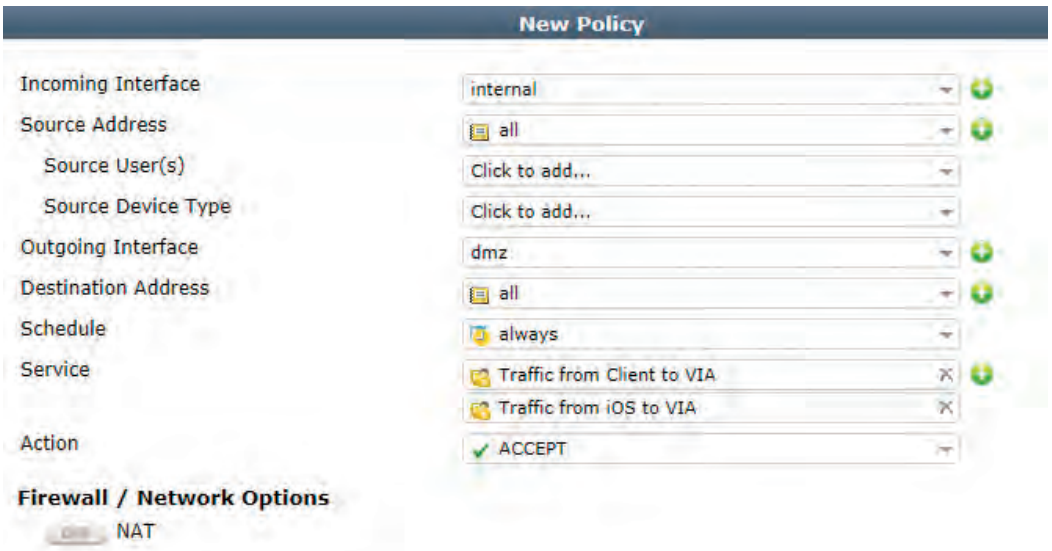
    Select for the incoming interface: **internalA**
    Source address: **all**
    Outgoing interface will be: **DMZ**
    Destination address: **all**
    Schedule: **always**
    Service: **Traffic from Client to VIA** and **Traffic from iOS to VIA**

    Make sure you have **NAT** (under **Firewall/Network Options**) deactivated.

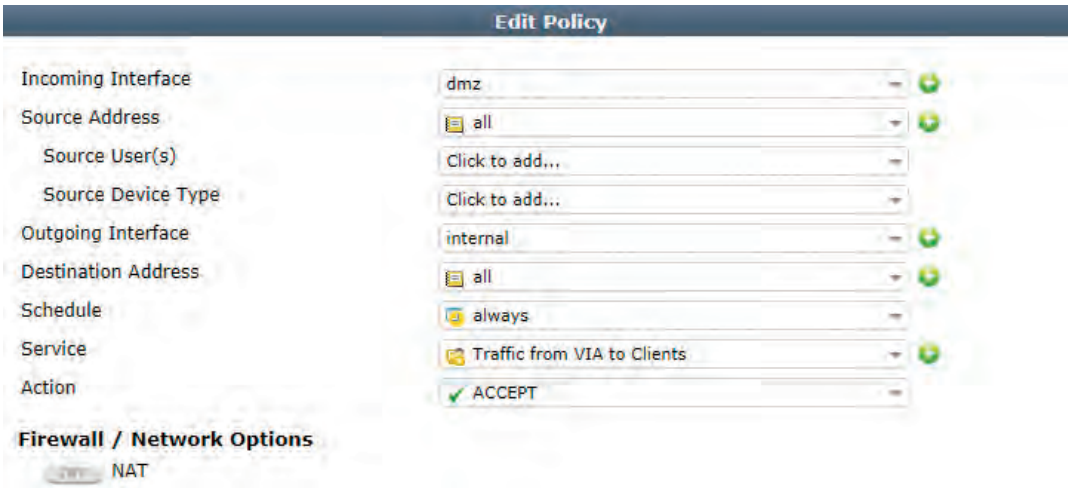


26. The next policy you define will enable communication from **DMZ** to **internalA**.
    Make sure you have **NAT** deactivated here as well.

27. Create the same policies for the **internal** interface now.



28. Finally, create a policy to allow communication back from **DMZ** to **internal**.



29. **Congratulations – you're done!** The configurations and policies you've defined in the previous steps will allow two networks to collaborate securely with VIA Collage, Campus, and Connect Pro in a Demilitarized Zone.

    Disclaimer: Keep in mind that we've only defined a basic configuration for the firewall. To make sure that your firewall is completely configured, you will need additional information from your IT Department or firewall distributor. This white paper covers the setup for dual network collaboration only, and no other security functions of this or any other firewall.

KRAMER ELECTRONICS, Ltd.

3 Am VeOlamo St.
Jerusalem, Israel, 9546303
Tel: + 972 73 265 0200
Fax: + 972 2 653 5369
E-mail: info@kramerel.com
Web: www.kramerelectronics.com

KRAMER ELECTRONICS USA, Inc.

Headquarters
6 Route 173 West
Clinton, NJ 08809, USA
Tel: (908) 735 0018
(888) 275 6311
Fax: (908) 735 0515

Tech Support after 6pm EST:
Tel: (888) 275 6311
E-mail: info@kramerus.com
Web: www.kramerus.com