pfsense 2.4 with Always-On Load Balanced OpenVPN Connections

Following this guide will allow you to create always-on load-balanced OpenVPN connections to your favorite VPN provider and force all your Internet traffic through the OpenVPN connections.

This guide was developed using [Newshosting VPN](#) account. The information contained will probably work with most other VPN providers with little or no modifications.

This guide is written for the privacy conscious who do not want their activities monitored by their ISP or other entities since the OpenVPN traffic is encrypted.

This guide is NOT written in order to assist you in conducting nefarious activities on the Internet undetected. A simple VPN connection is not enough to completely hide your digital tracks. Be warned!!

Import VPN Provider CA Certificate

1. Obtain the CA Certificate from the VPN Provider.
2. Navigate to **System --> Cert. Manager**.
3. Click the **Add** button.
4. Under the **Descriptive name** field, enter a description for the CA certificate your are importing.
5. Under the **Certificate data**, paste the certificate contents including the **-----BEGIN CERTIFICATE-----** and the ***-----END CERTIFICATE-----*** parts.
6. Click the **Save** button (**Figure 1**).

Figure 1
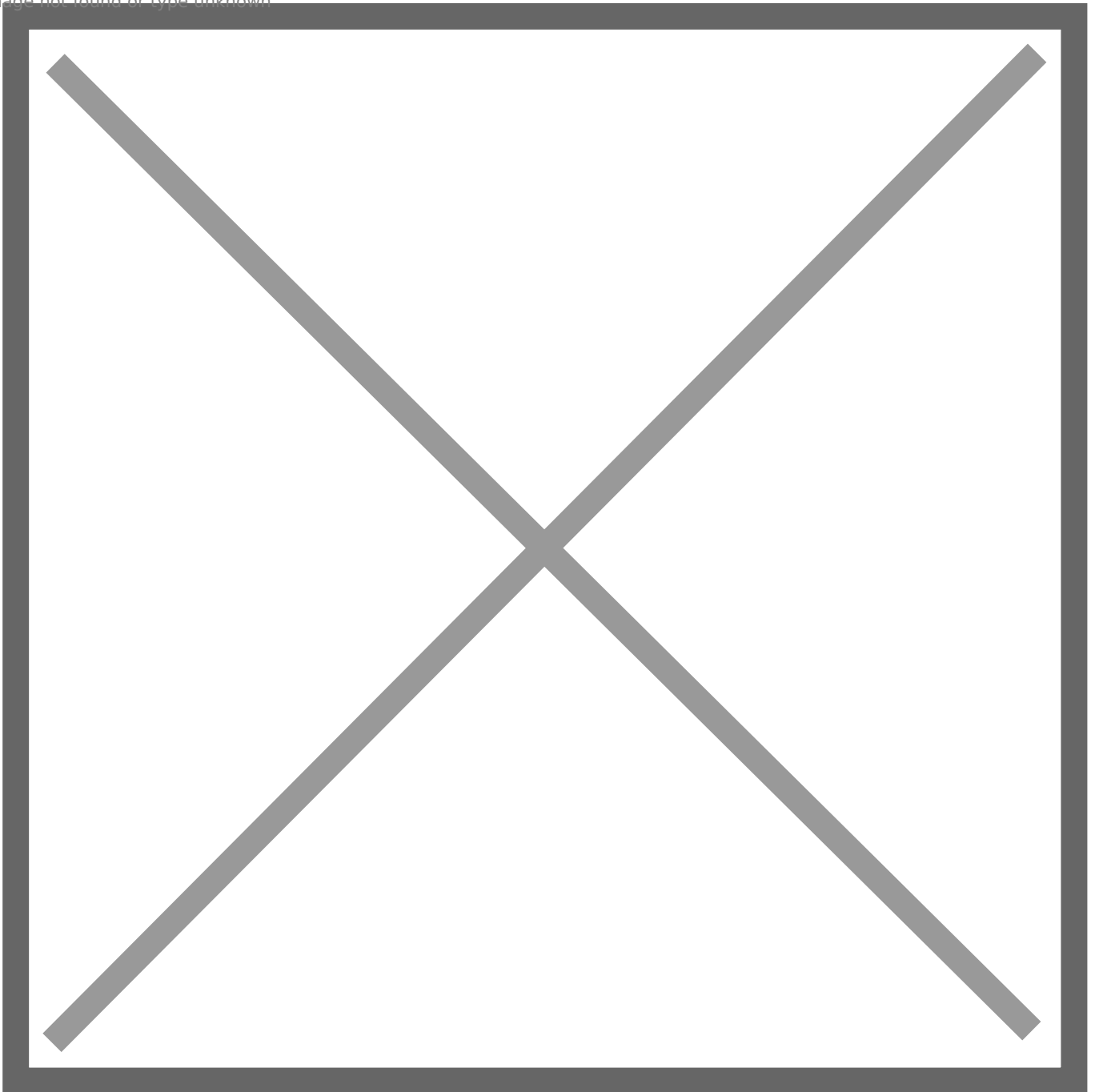
Create OpenVPN client connections

1. Navigate to **VPN --> OpenVPN --> Clients.**
2. Click the **Add** button.
3. In the **Server Mode** field, ensure **Peer to Peer (SSL/TLS)** is selected.
4. In the **Protocol** field, select either **UDP on IPv4 Only** or **TCP on IPv4 Only** depending on your VPN provider's requirements. Most of the time, UDP on port 1194 is used.
5. In the **Device mode** field, ensure **tun - Layer 3 Tunnel Mode** is selected.
6. In the **Interface** field, ensure **WAN** is selected.

7. In the **Server host or address field**, enter the address to your VPN provider's OpenVPN server.
8. In the **Server port** field, enter the port number to your VPN provider's OpenVPN server (most likely 1194).
9. In the **Description** field, enter a description for this connection if desired (**Figure 2**).

Figure 2
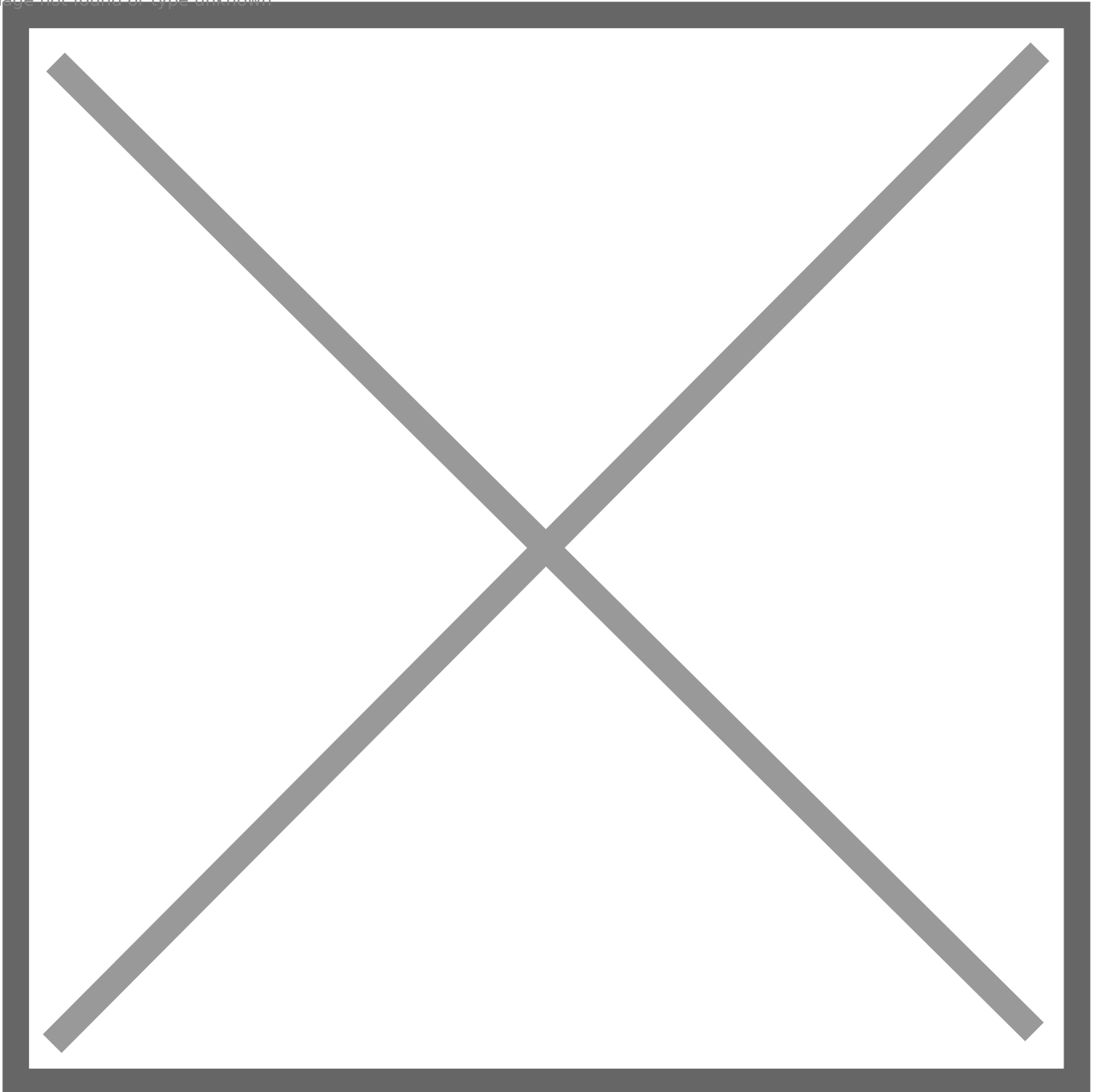
10. In the **Username** field, enter the username for your VPN Provider.
11. In the **Password** field, enter the password for your VPN Provider.
12. Ensure the **Use a TLS Key** field is **unchecked**.

13. In the **Peer Certificate Authority** field, ensure you select the CA that you created in the **import VPN Provider CA Certificate** section above.
14. In the **Client Certificate** field, ensure that **None (Username and/or Password required)** is selected. Please note that this field may need to be adjusted to your VPN provider's requirements, however most of the VPN providers I've used, Username/Password has been sufficient.
15. In the **Encryption Algorithm** field, select the highest encryption that your VPN provider supports. I've used **AES-256-CBC (256 bit key, 128 bit block)** with no problems (**Figure 3**).
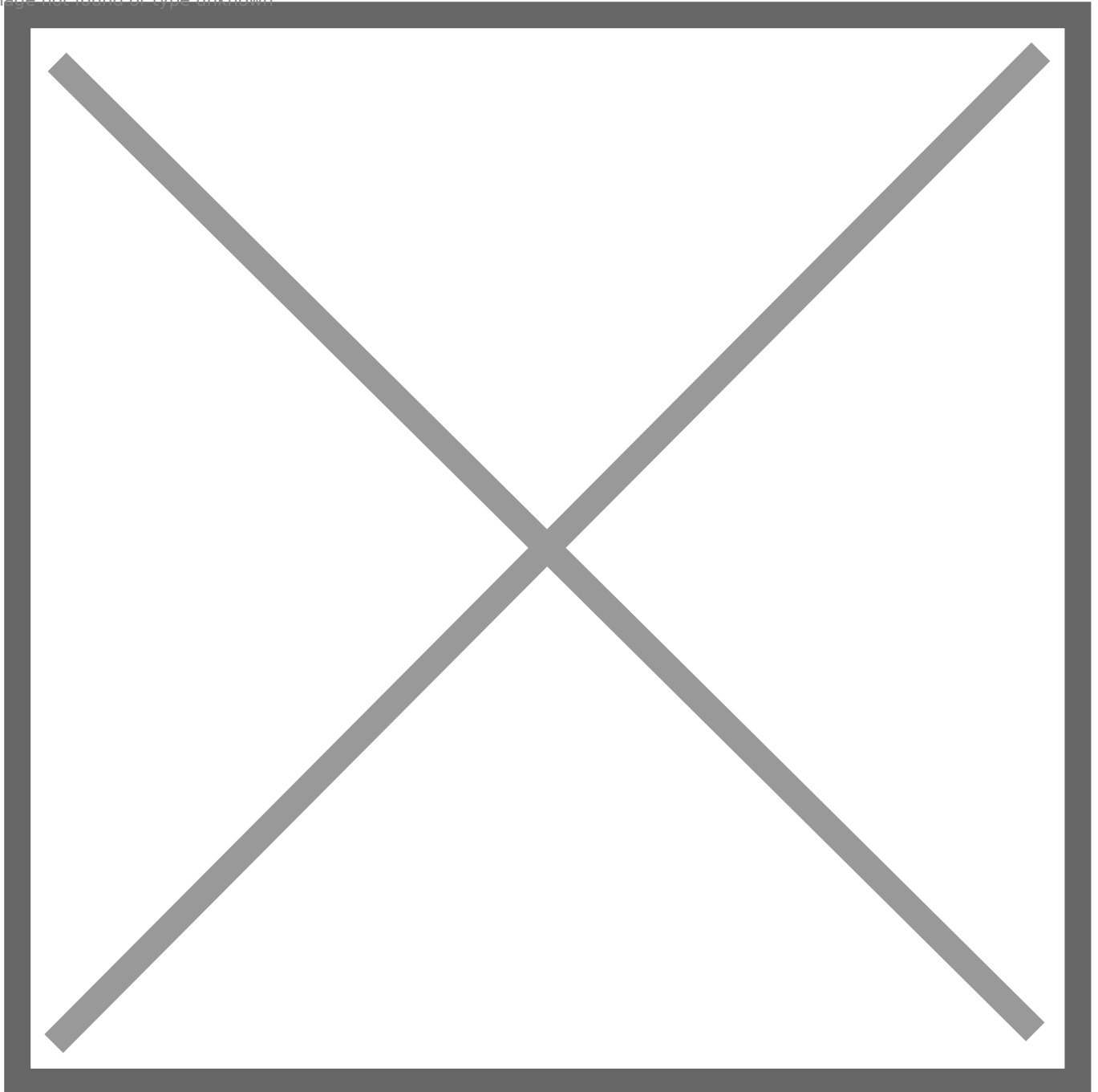
Figure 3
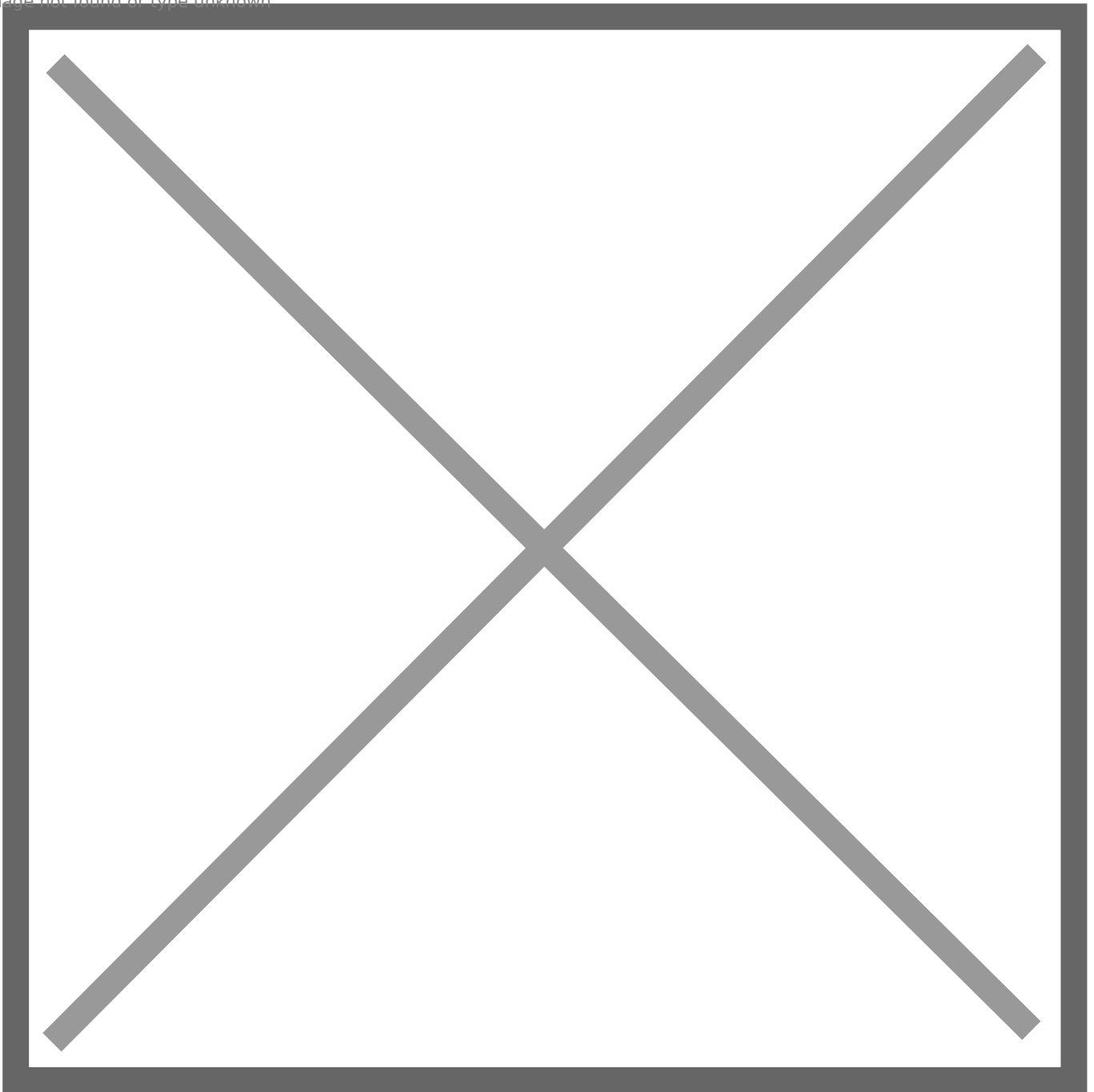
10. Ensure the **Enable NCP** field is **unchecked**.
11. In the **Auth digest algorithm** field, select the auth digest algorithm supported by your VPN provider. I've used **SHA256 (256-bit)** with no problems.
12. In the **Hardware Crypto** field, ensure **No Hardware Crypto Acceleration** is selected (**Figure 4**).
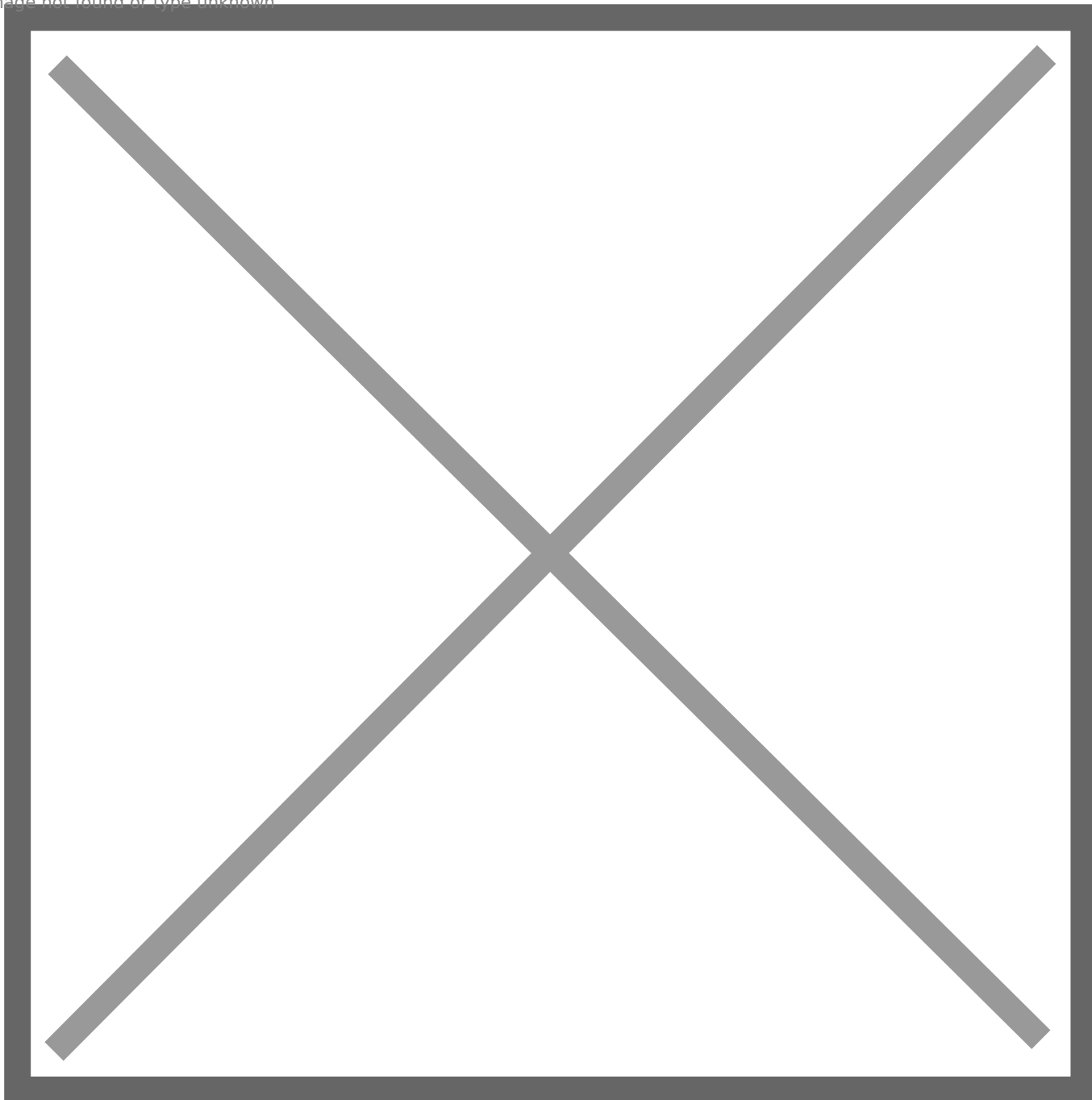
Figure 4

10. In the **Compression** field, ensure that **Adaptive LZO Compression [Legacy style, comp-lzo adaptive]** is selected.
11. Ensure **Don't add or remove routes** field is **checked**.
12. In the **Custom options** field, paste the following options (**Figure 5**):

persist-key;

persist-tun;

persist-remote-ip;

resolv-retry infinite;

Figure 5

22. Click the **Save** button.
23. Create additional OpenVPN client connections as needed.

Verify OpenVPN Client Connections are Up

1. Navigate to **Status --> OpenVPN**. Under the **Client Instance Statistics** section, you should be able to see the connections you created and ideally if configured correctly, the status for each connections should be **up** (**Figure 6**).

**Figure 6**

Image not found or type unknown
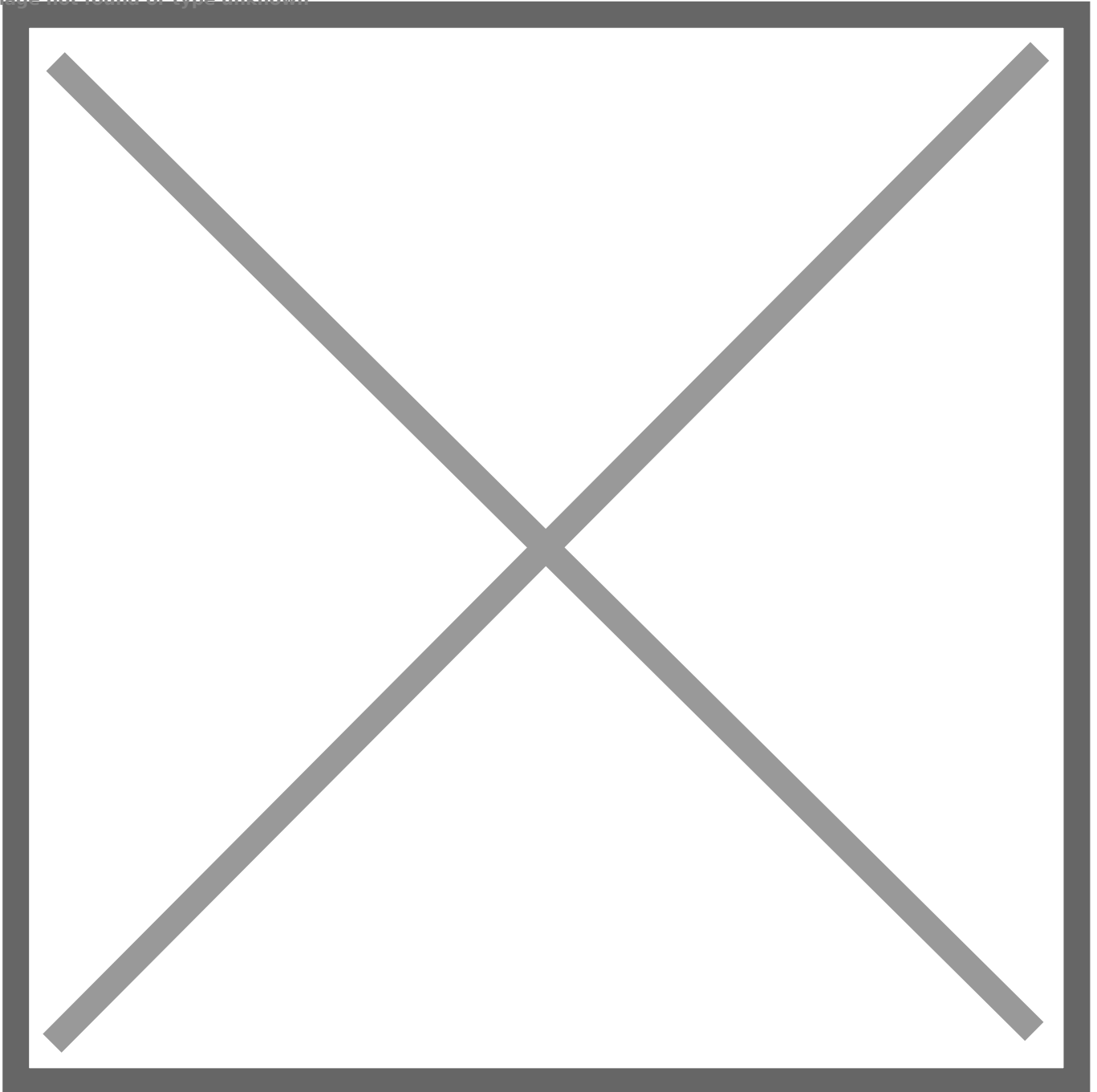
Assign Interfaces to each OpenVPN Connection

1. Navigate to **Interfaces --> Assignments**.
2. Next to the **Available network ports** field, select each of the OpenVPN connections you created earlier from the **Network port** drop-down field and click the **Add** button to assign the network port. The OpenVPN connections are named **ovpncX** where **X** is number assigned by the system. In this example, I created two OpenVPN connections and they are named **ovpnc4 for newshosting.com OpenVPN 1** connection and **ovpnc5 for newshosting.com OpenVPN 2** connection (**Figure 7**).
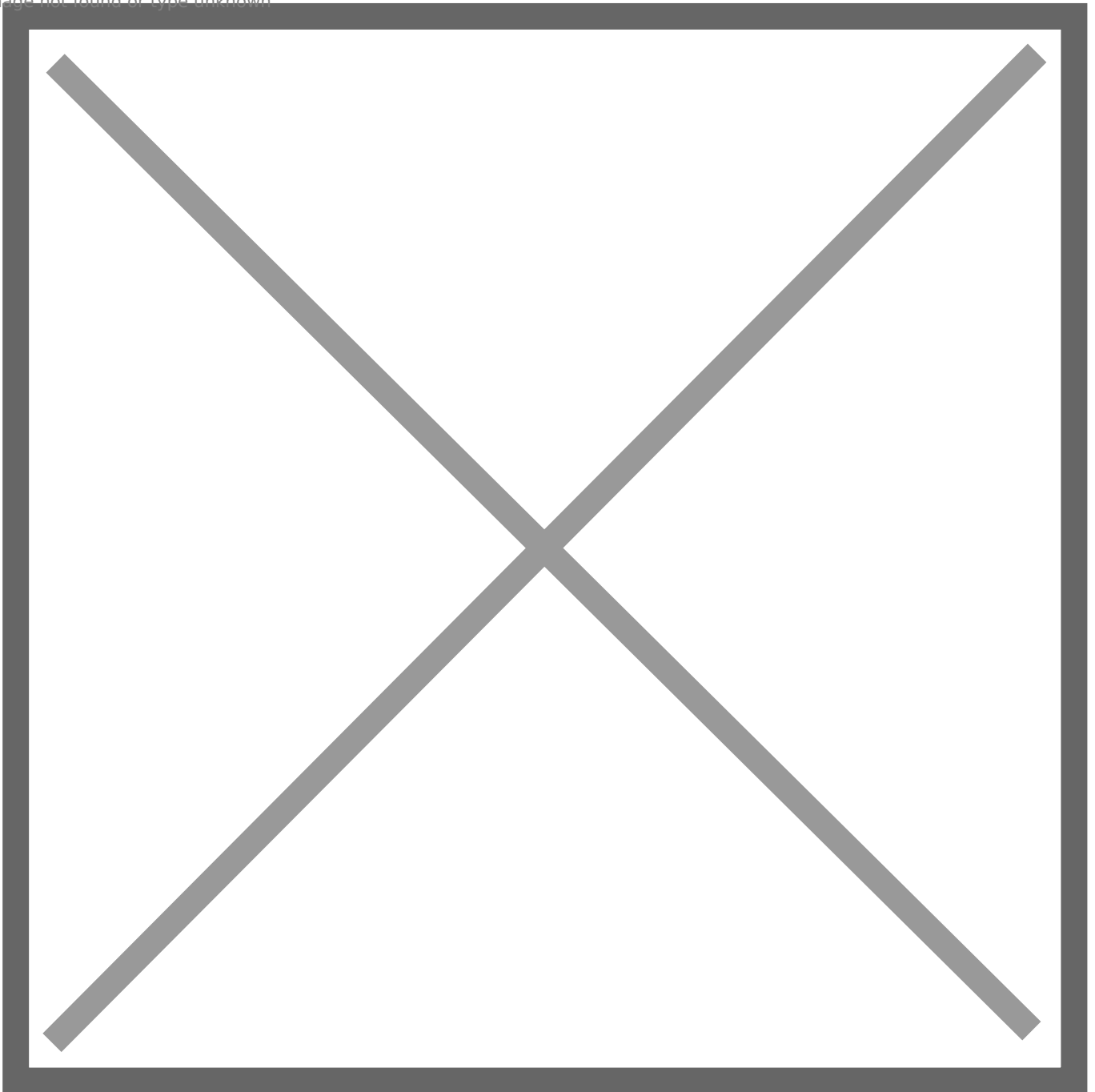
Figure 7
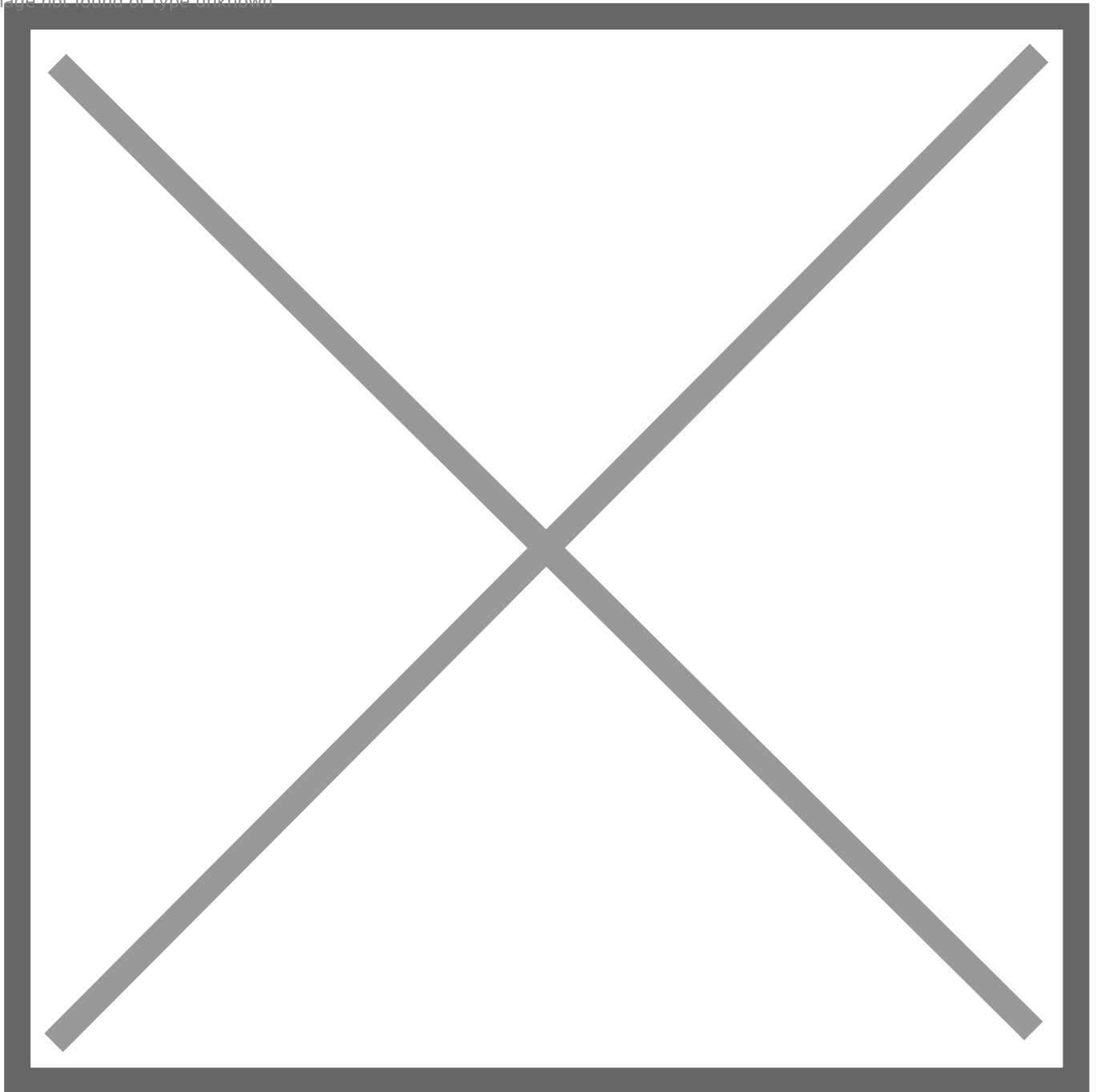
3. Assign all the OpenVPN connections you created and you will end up with your OpenVPN connections having been assigned an **OPTX** interface name where **X** is a number assigned by the system. Ensure you click the **Save** button at the bottom of the screen to save your changes. (**Figure 8**).

Figure 8

9. Next, click on each of the **OPTX** interfaces that were assigned to your OpenVPN connections and you will be re-directed to the **Interfaces / OPTX** configuration page where X is the interface number assigned by the system.
10. Ensure the **Enable** field is checked.
11. In the **Description** field enter a name for this connection (Ex: **NewsHostingOpenVPN1**).
12. Ensure **IPv4 Configuration Type** is set to None.
13. Ensure **IPv6 Configuration Type** is set to None (**Figure 9**).

Figure 9
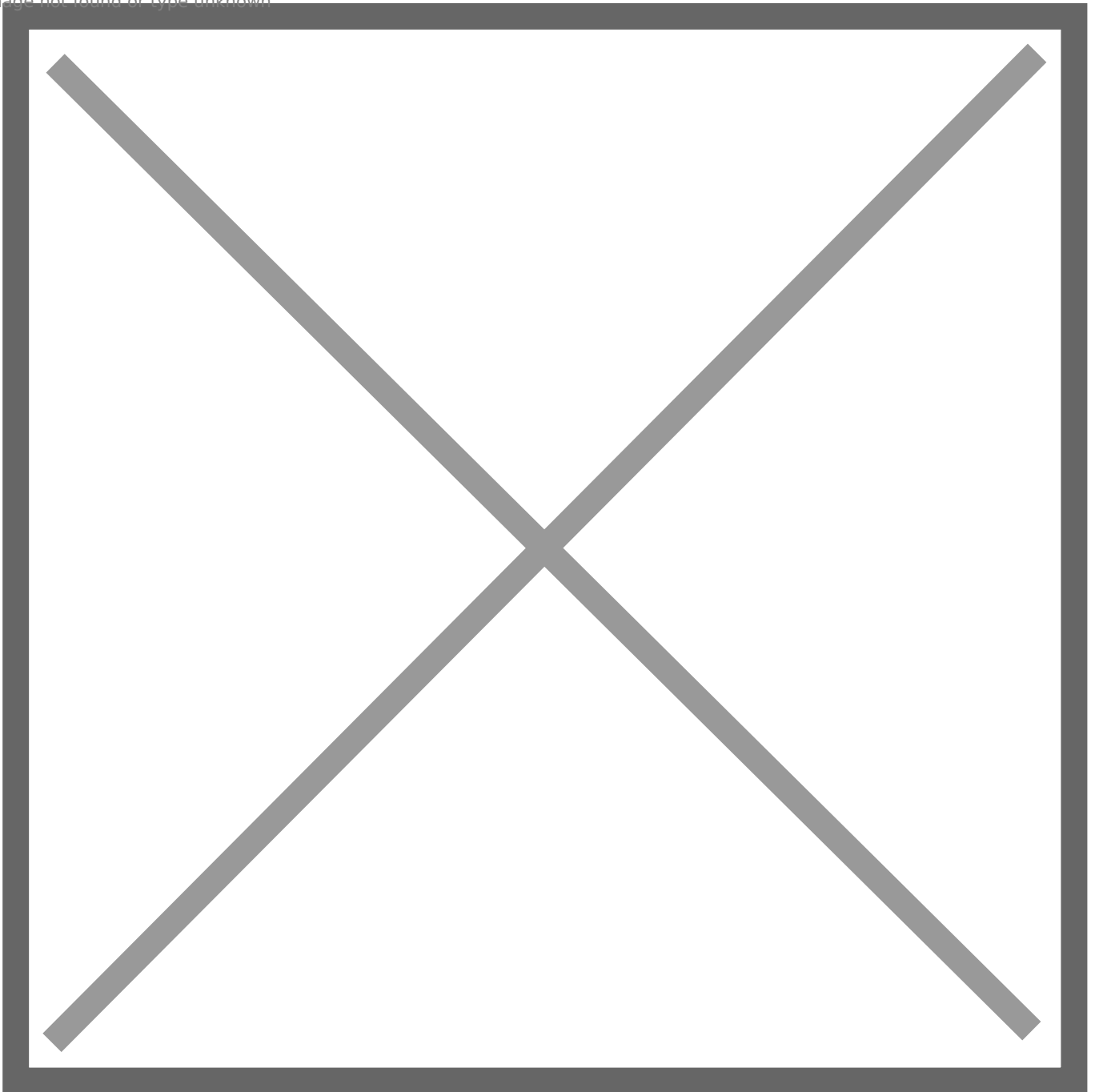
14. Click the **Save** button at the bottom of the page and then click the **Apply Changes** that appears on the top of the page after clicking the Save button.
15. Navigate back to **Interfaces --> Assignments** and repeat **Steps 9 through 14** from above to assign the rest of the OpenVPN connections.
16. In the end you should end up with a listing like below under **Interfaces -->Assignments** (**Figure 10**).
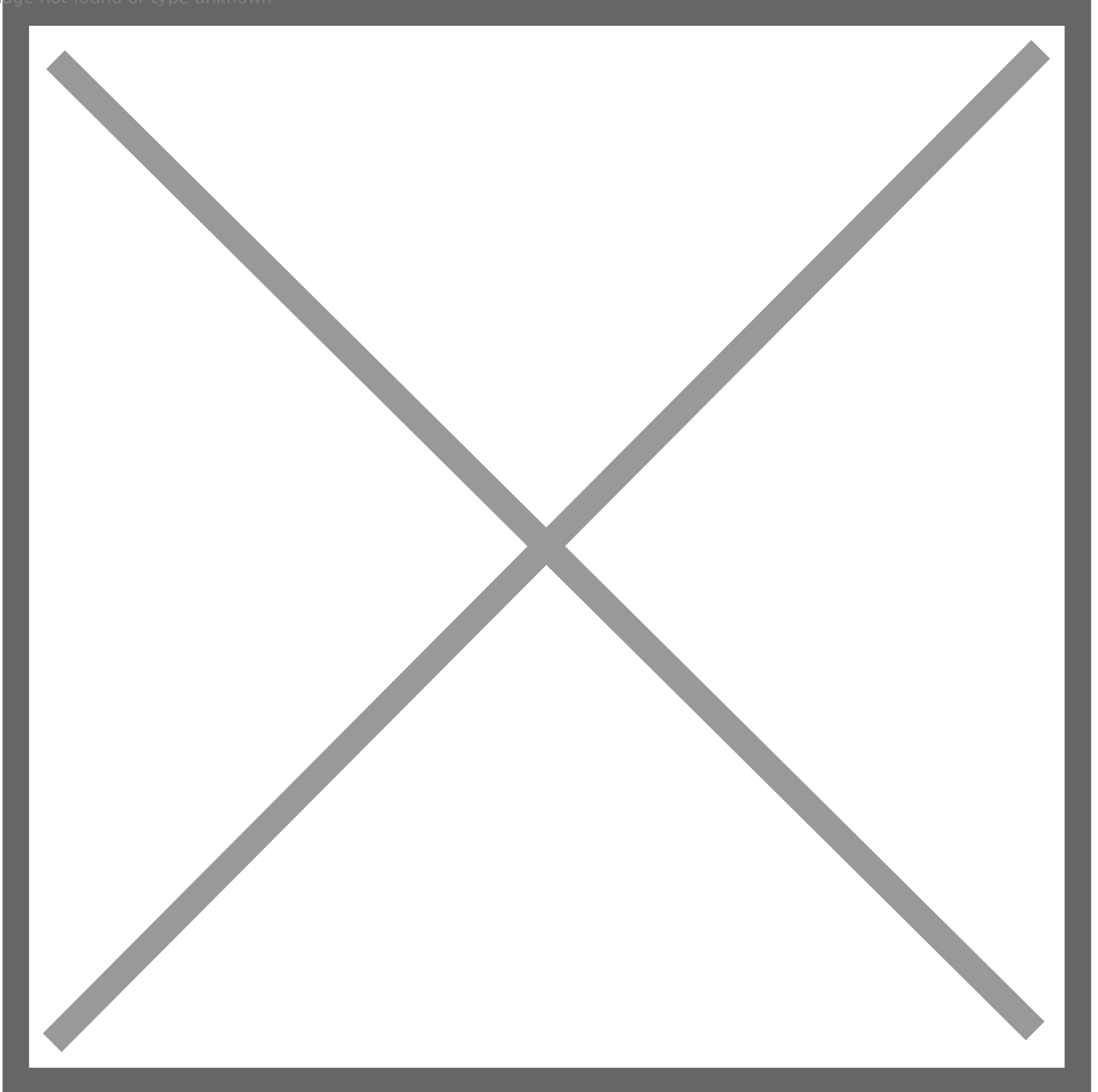
Figure 10
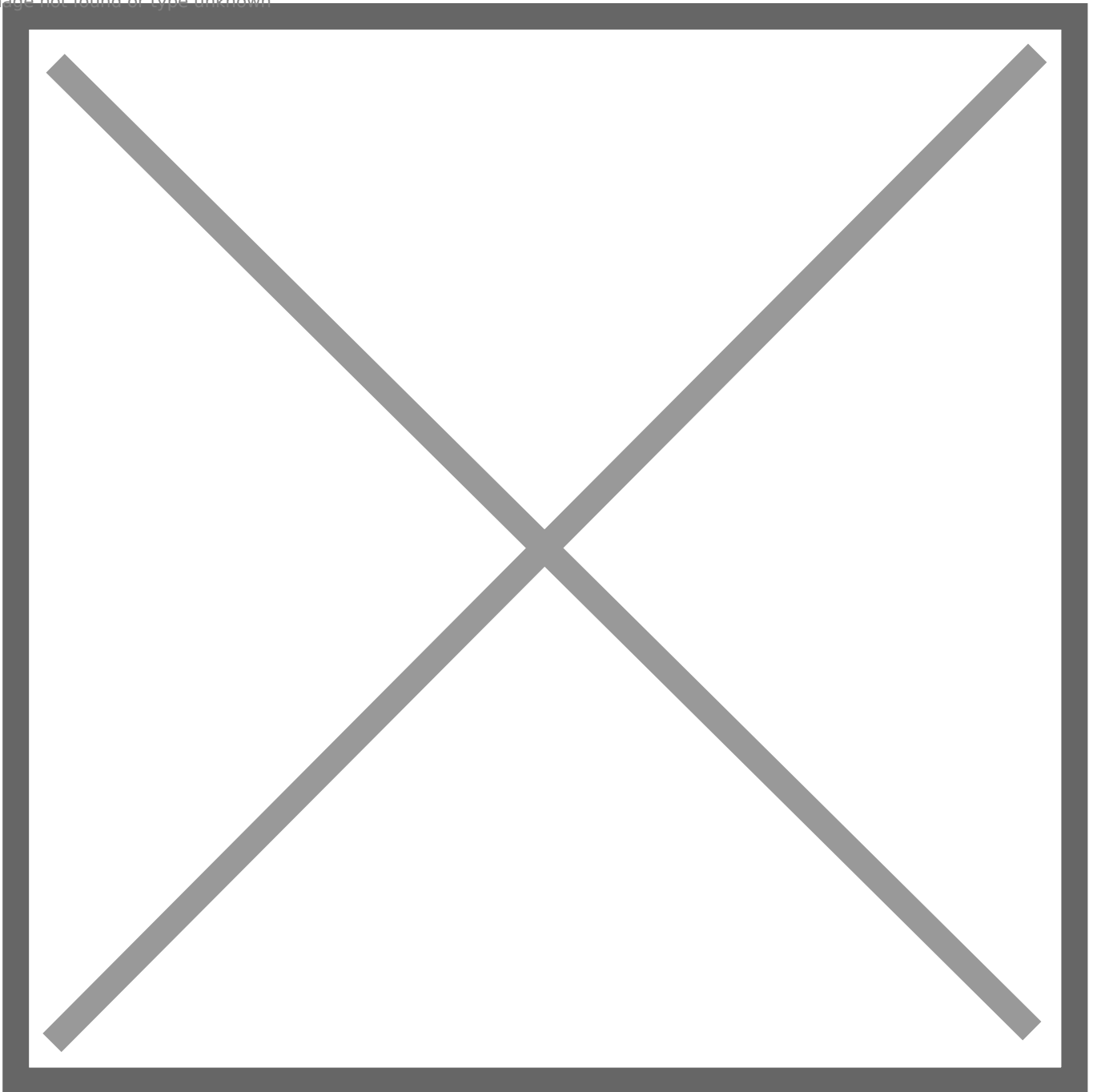
Create OpenVPN Gateway Group

In this section, we are going to be creating a Gateway Group that's going to include all the OpenVPN gateways that were automatcially created by the system when we assigned the OpenVPN connections to Interfaces in the previous section. Using this method, we willl be having more than one connection available for load balancing as well as failover in case one of the OpenVPN connections goes down. You will notice below that we will give both OpenVPN gateways the same priority (Tier 1) which will effectively create a load-balanced connection using multiple OpenVPN gateways.

1. Navigate to **System --> Routing** and ensure the **Gateways** tab is selected. You should be able to **IPv4** gateways, denoted by a **_VPNV4** suffix and **IPv6** gateways, denoted by a **_VPNV6** suffix entries for each interface you assigned to an OpenVPN connection from the section above. (**Figure 11**).
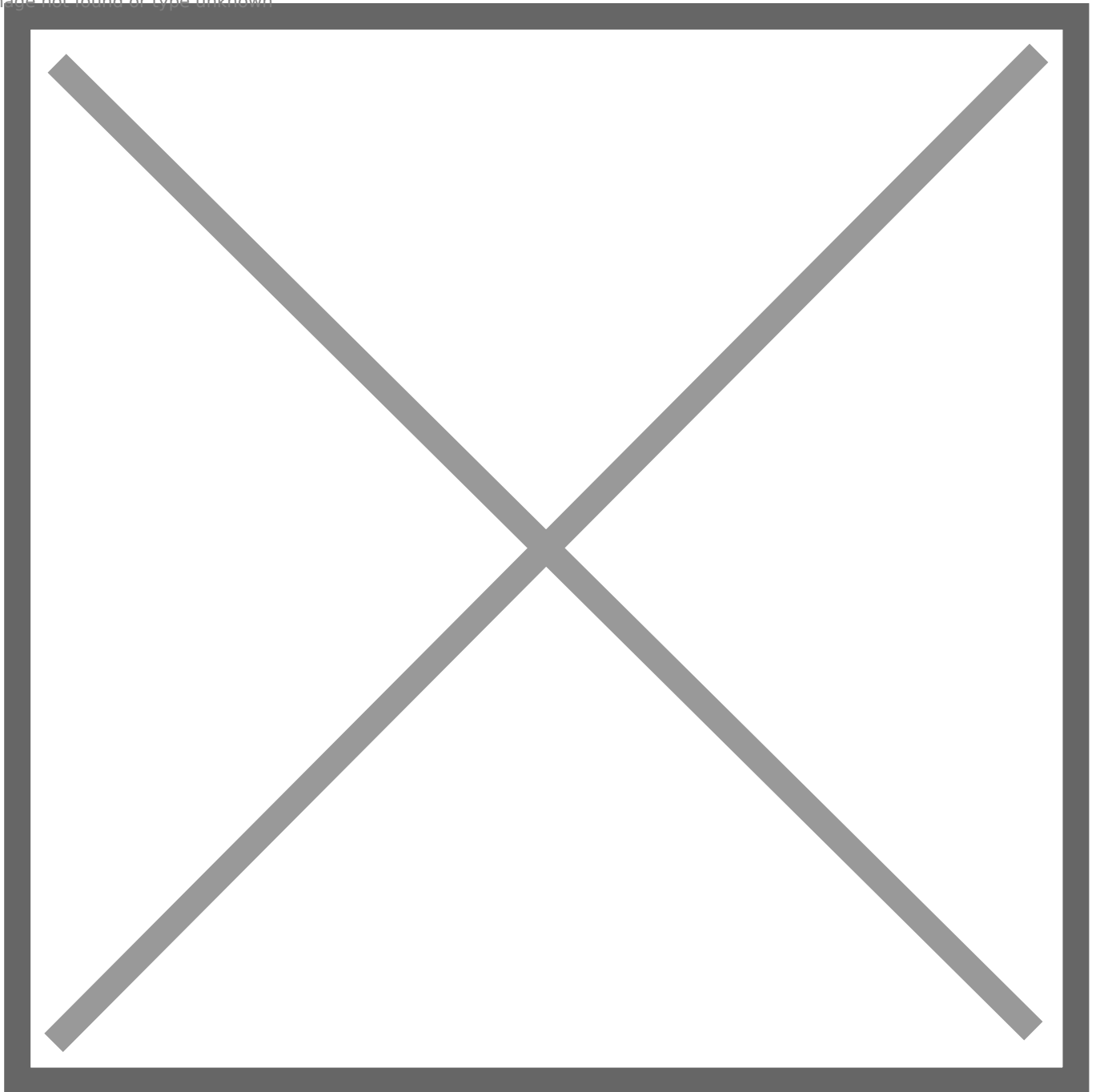
Figure 11

Image not found or type unknown

2. Next, click on the **Gateway Groups** tab and then click the **Add** button **(Figure 12)**.
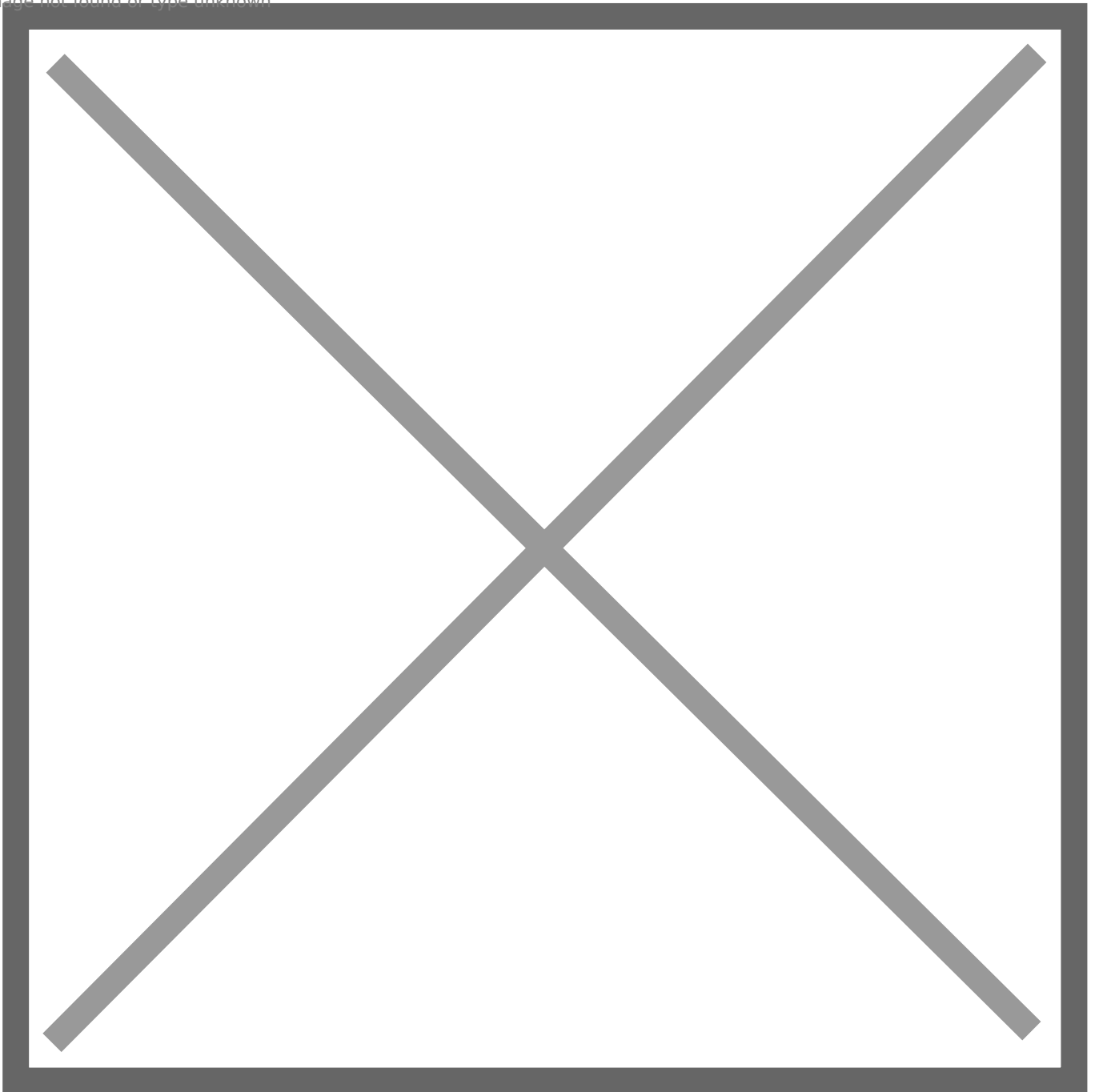
Figure 12

Image not found or type unknown

3. You will be re-directed to the **Edit Gateway Group Entry** page
4. In the **Group Name** field, enter a name for your Gateway Group (Ex: OpenVPNGatewayGroup).
5. Under the **Gateway Priority** section, ensure your **main WAN gateway is set to Never**.
6. Ensure all the *OpenVPN IPv4 gateways denoted with a _VPNV4 suffix are set to Tier 1*. **Ensure that any OpenVPN IPv6 gateways denoted with a _VPNV6 suffix are NOT set to Tier 1 and if necessary be set to Never just like the main WAN gateway.**
7. Ensure the **Trigger Level** field is set to Member down
8. Optionally, enter a description in the **Description** field.
9. Click the **Save** button (**Figure 13**).

Figure 13

Image not found or type unknown

10. You will be re-directed back to **Gateway Groups** page where the you will be able to see the Gateway Group you just created. Click on the **Apply Changes** button on the top of the page to apply your changes (**Figure 14**).
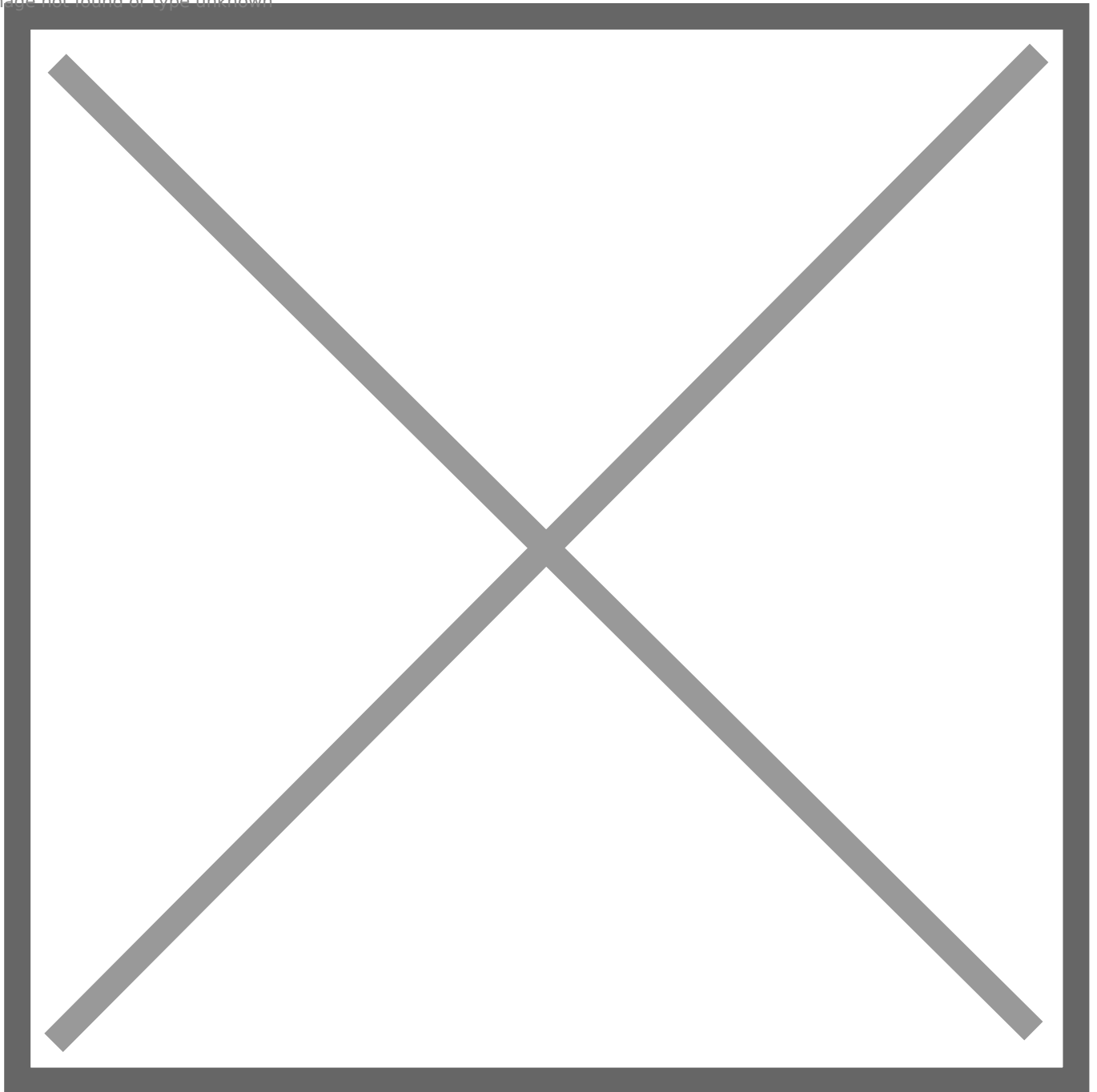
Figure 14
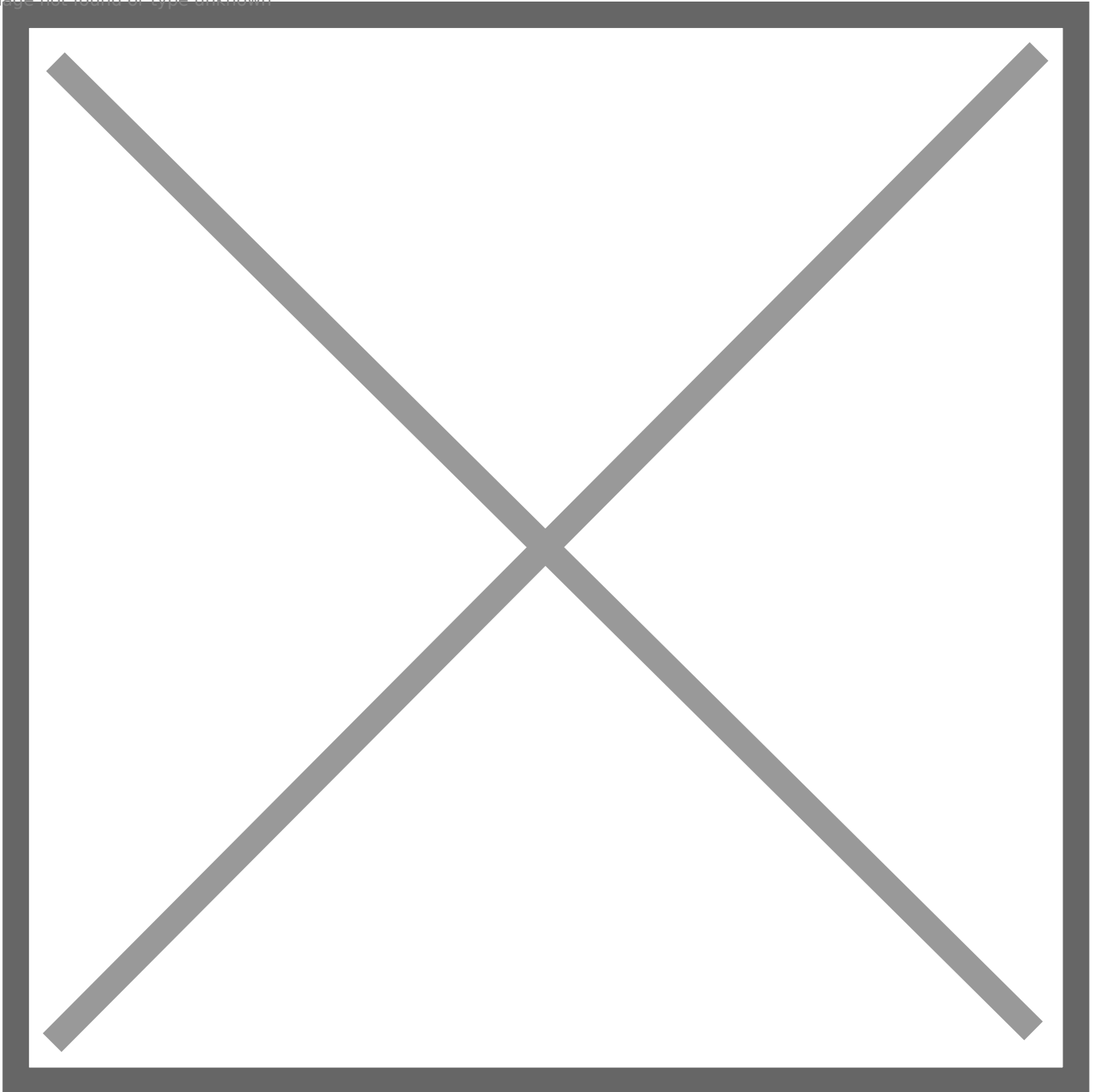
Create Firewall Rules

In this section, we are going to create a floating firewall rule to Reject any LAN outbound packets that are tagged as **NO_WAN_OUTBOUND** and then we are going to create a LAN rule that will tag all traffic as **NO_WAN_OUTBOUND** as well as use the OpenVPNGatewayGroup we created in the section above as the default gateway for that traffic. Using this method, we are going to ensure that ALL LAN traffic will ONLY go through the OpenVPN connections.

1. Navigate to **Firewall --> Rules** and ensure the **Floating** tab is selected. (**Figure 15**).

Figure 15

2. Click the Add button with the down arrow on the bottom of the page to add a rule to the end of the list (**Figure 16**).

Figure 16
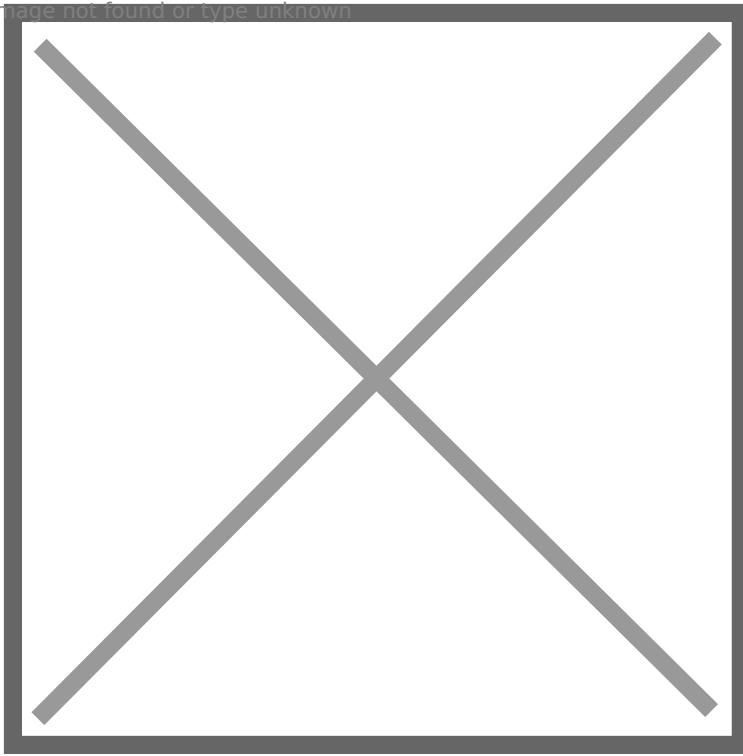
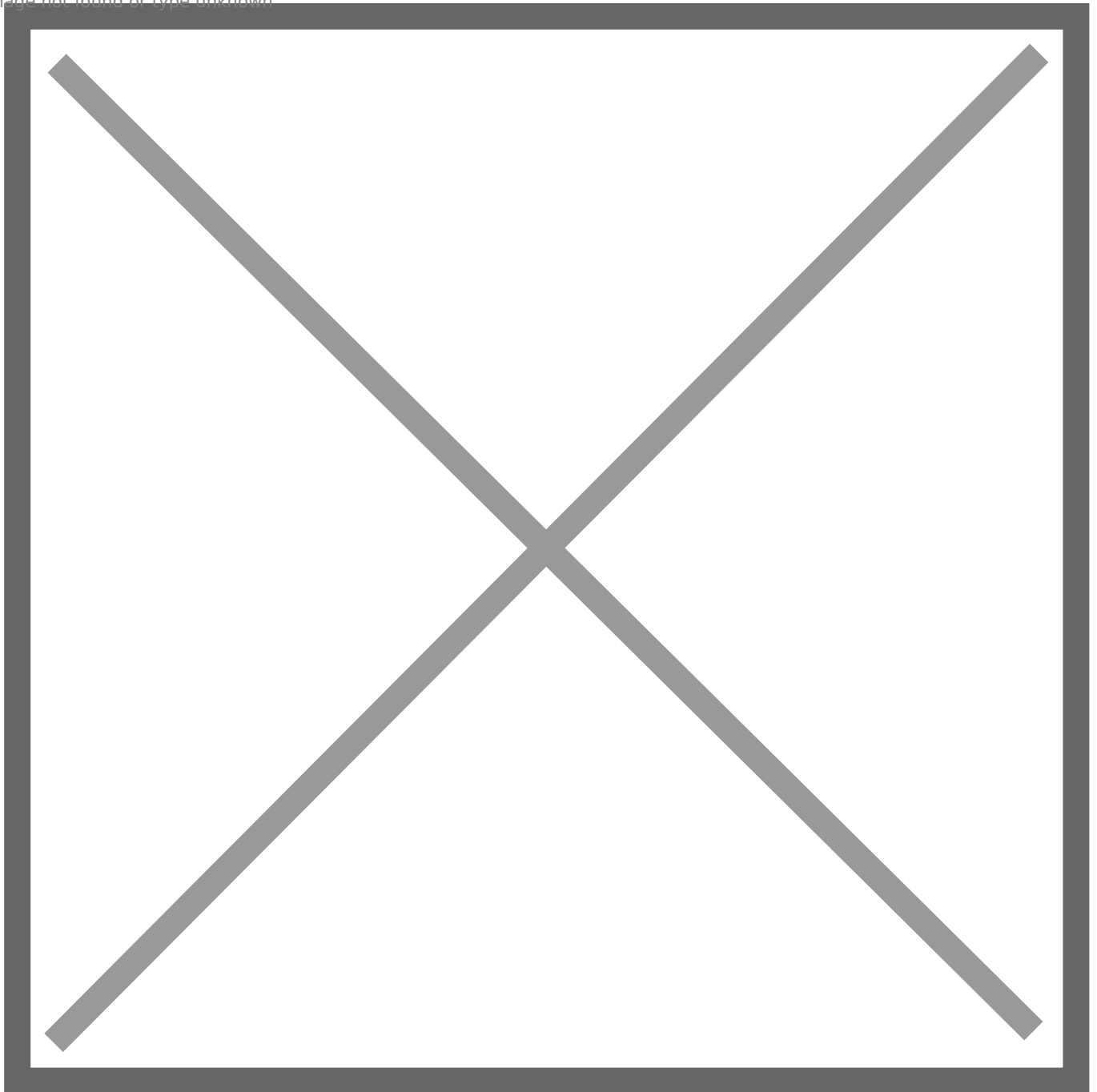3. You will be re-directed to the **Edit firewall Rule** page.
4. In the **Action** field ensure **Reject** is selected.
5. In the **Interface** field ensure the **WAN** interface is selected.
6. In the **Direction** field ensure **out** is selected.
7. In the **Address Family** ensure **IPv4** is selected.
8. In the **Protocol** field ensure **Any** is selected(**Figure 17**).

Figure 17

9. In the **Log** field, check the Log packets that are handled by this rule.
10. In the **Description** field, enter the following description: **Reject Packets tagged with NO_WAN_OUTBOUND**.
11. In the **Advanced Options** field, click **Display Advanced** button (**Figure 18**).
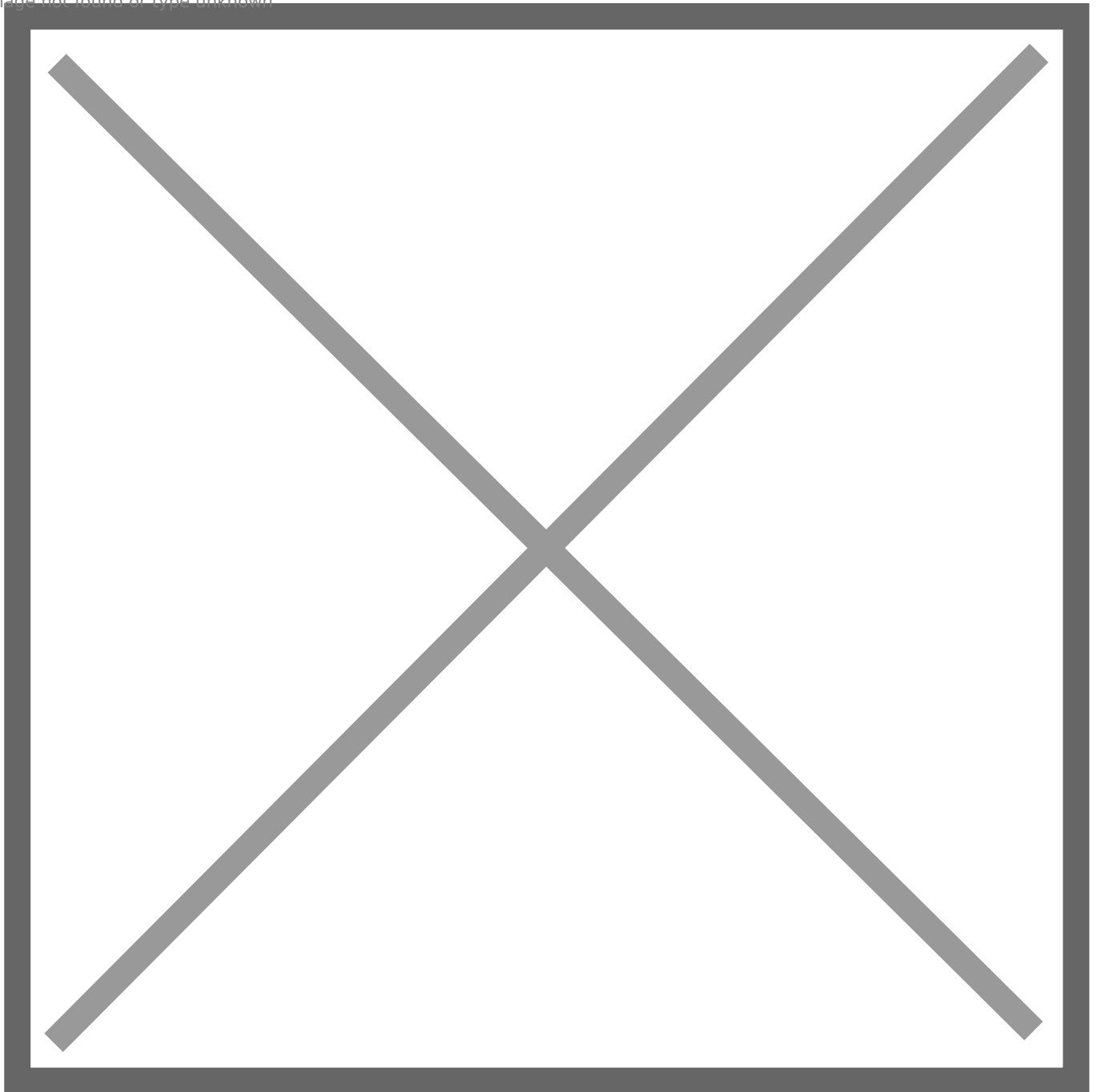
Figure 18
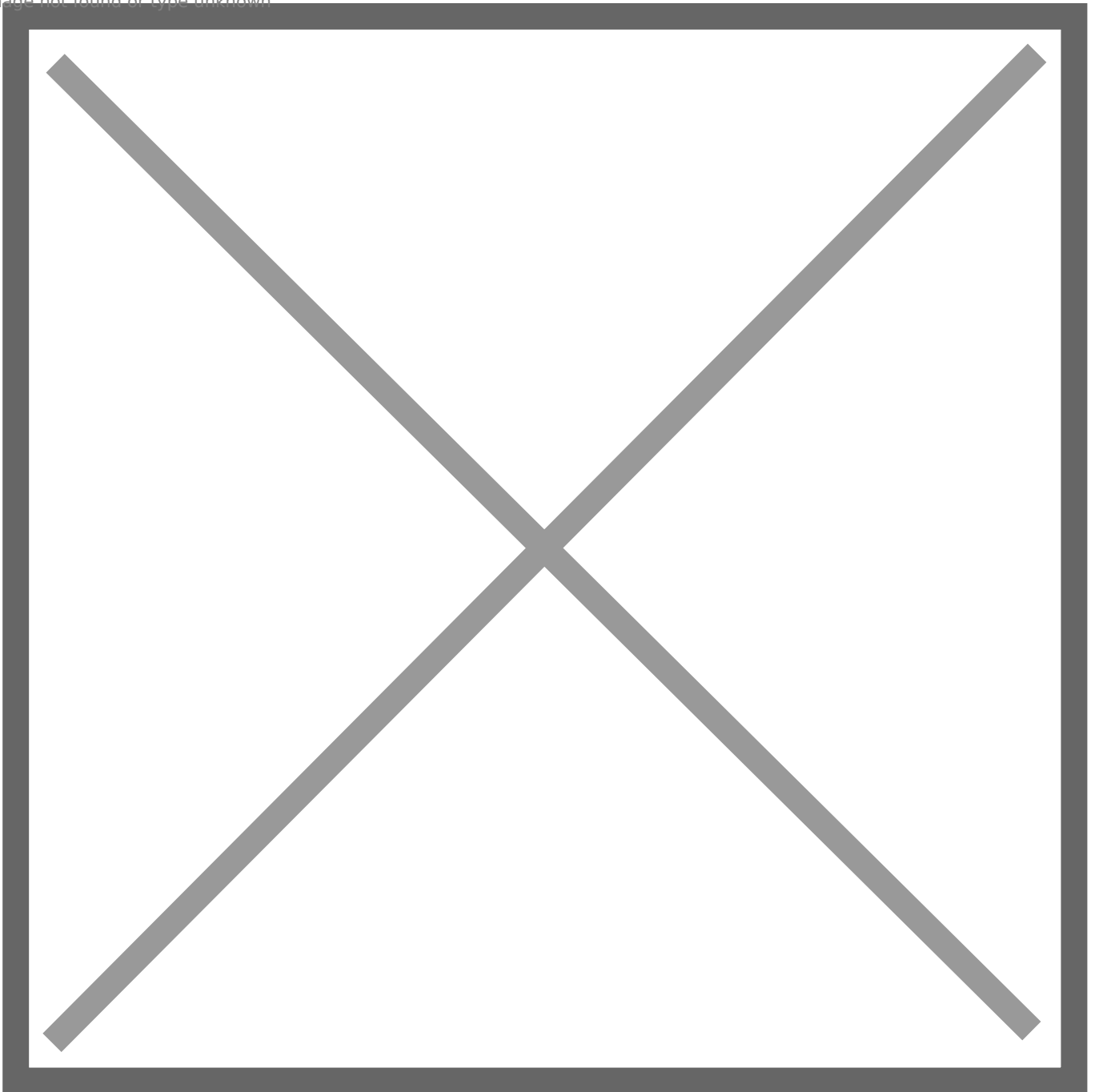
12. Clicking the Advanced Options button from the previous step, will display the Advanced Options section.
13. In the **Tagged** field, enter the following: **NO_WAN_OUTBOUND** (**Figure 19**)**.** Ensure you make a note of the **NO_WAN_OUTBOUND** tag because we are going to be using it in LAN rule we are going to be creating next.
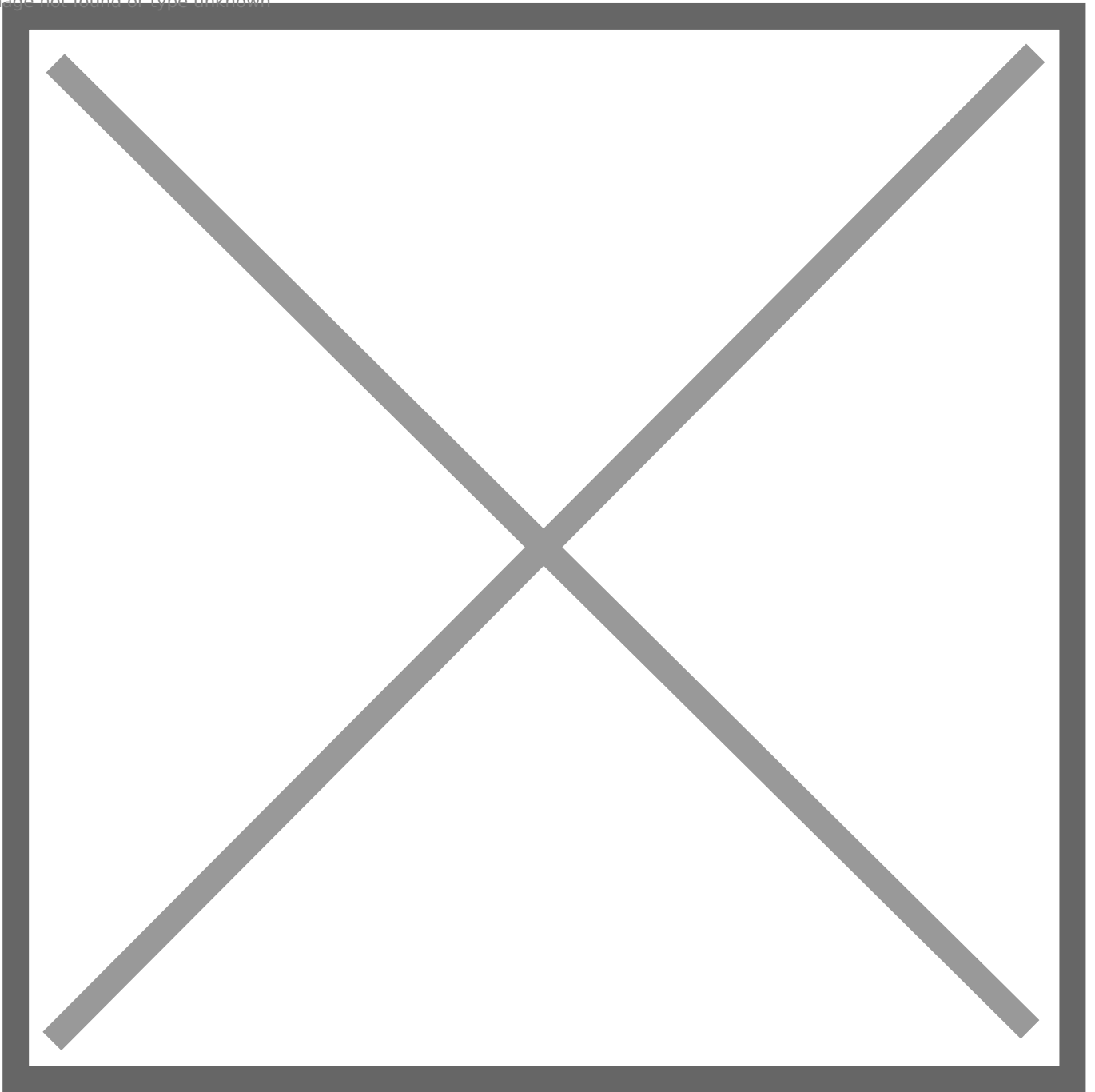
Figure 19

14. Click the **Save** button at the bottom of the page.
15. You will be re-directed back to the **Floating** rules tab page.
16. Click on the **Apply Changes** button on the top of the page to apply the changes (**Figure 20**).
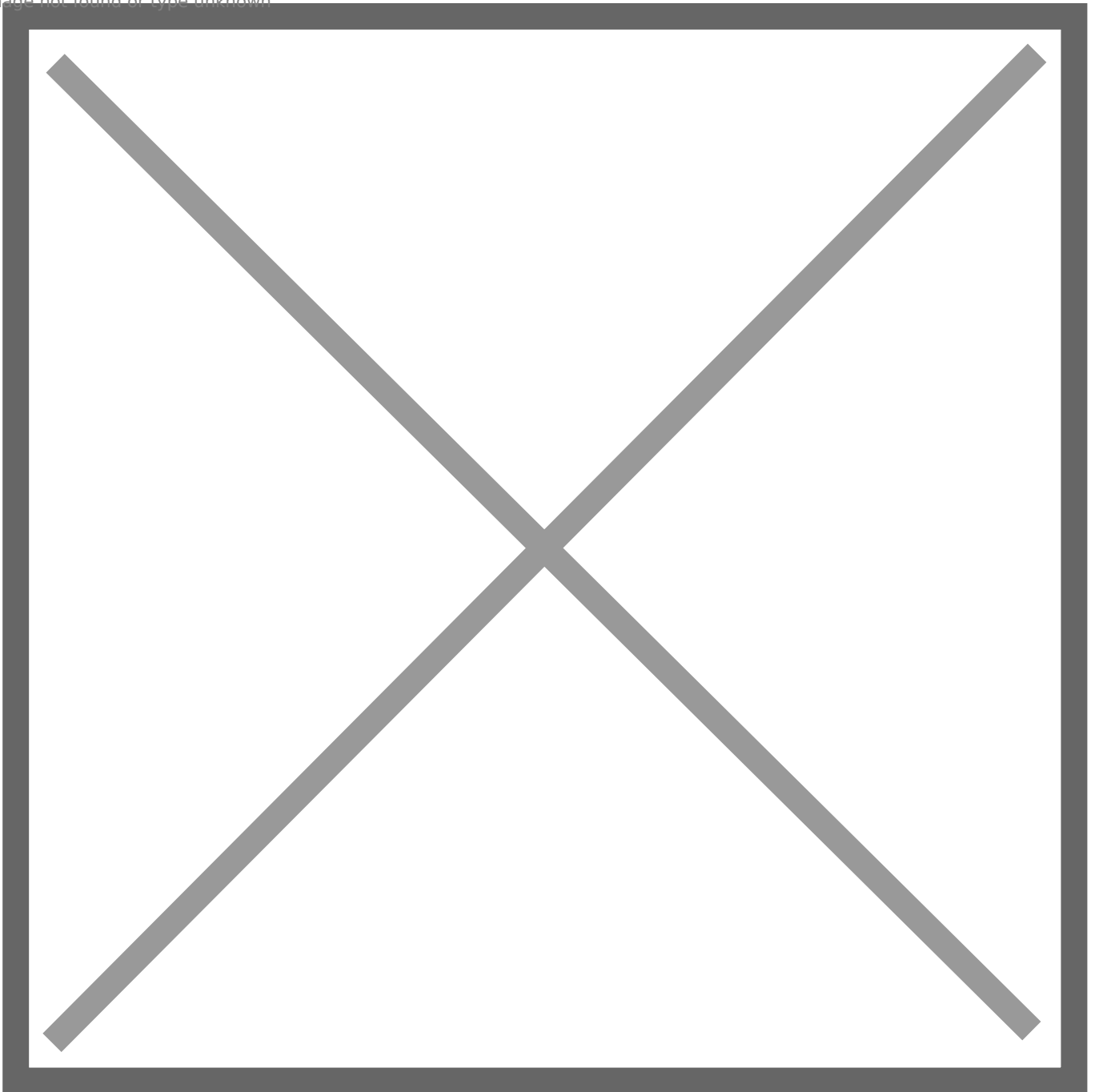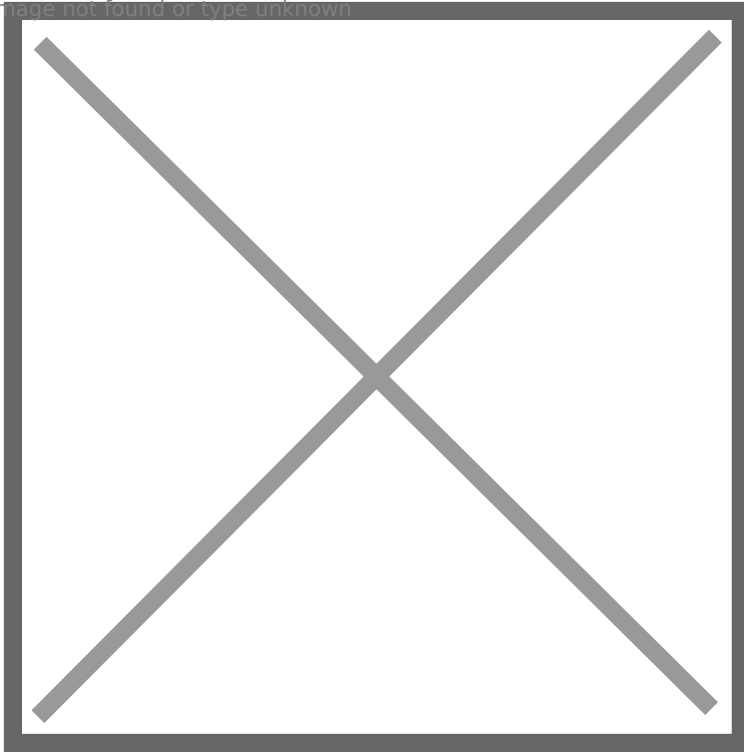
Figure 20

17. Next click on the **LAN** tab (**Figure 21**).

Figure 21

18. Click the Add button with the down arrow on the bottom of the page to add a rule to the end of the list (**Figure 22**).

Figure 22

Image not found or type unknown

19. You will be re-directed to the **Edit firewall Rule** page.
20. In the **Action** field ensure **Pass** is selected.
21. In the **Disabled** field ensure **Disable this rule** is **Unchecked**.
22. In the **Interface** field ensure the **LAN** interface is selected.
23. In the **Address Family** ensure **IPv4** is selected.
24. In the **Protocol** field ensure **Any** is selected (**Figure 23**).

Figure 23

Image not found or type unknown
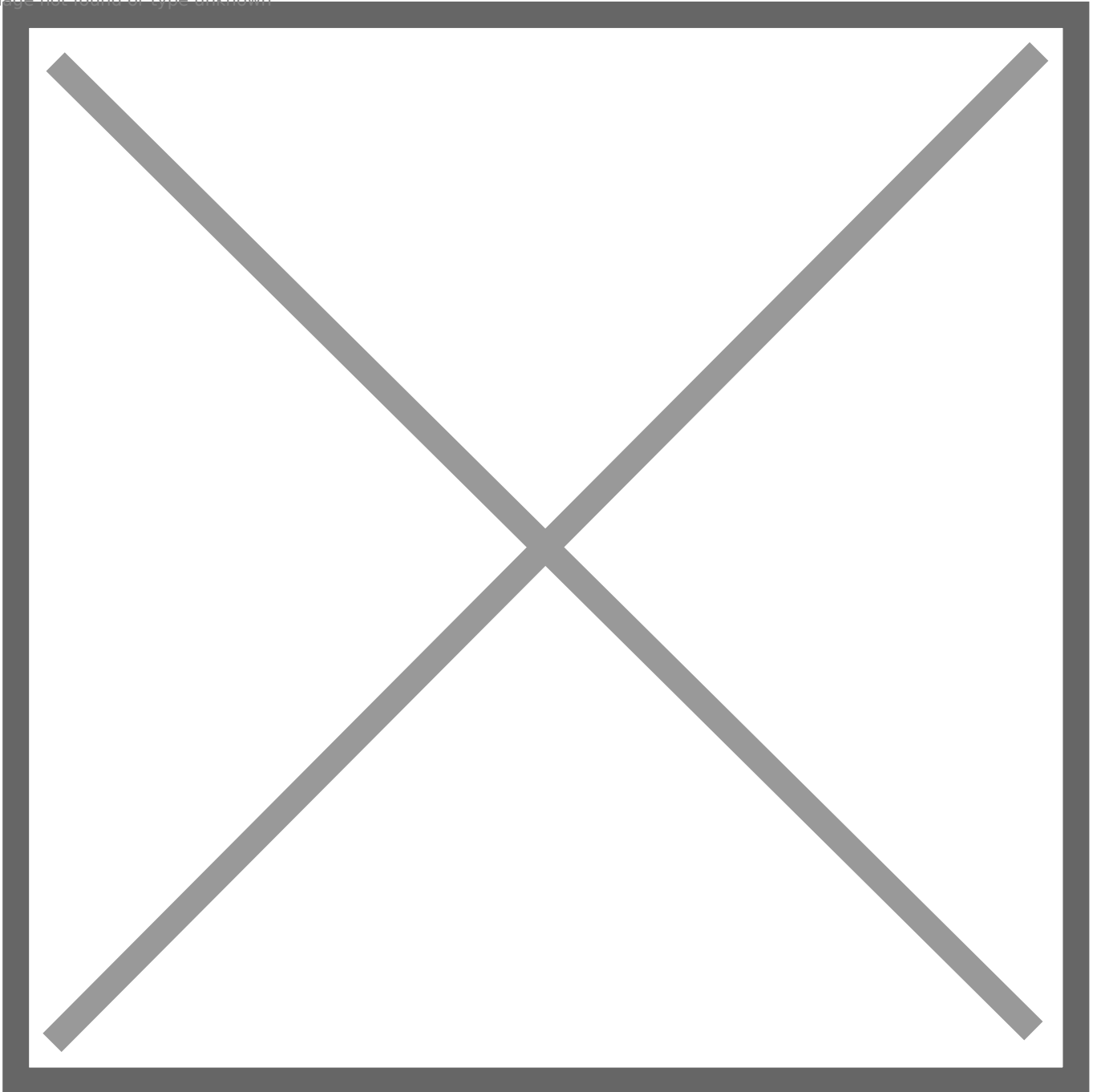
25. Under the **Source** section, in the **Source** field, ensure **LAN net** is selected.
26. Under the **Destination** section, in the **Destination** field, ensure **any** is selected.
27. Under the **Extra Options** section, in the **Log** field, ensure **Log packets that are handled by this rule** is checked.
28. Under the **Extra Options** section, in the **Description** field, enter a description for this rule (Ex: Allow LAN to any via VPN Only).
29. Under the **Extra Options** section, in the **Advanced Options** field, click the **Display Advanced** button (**Figure 24**).
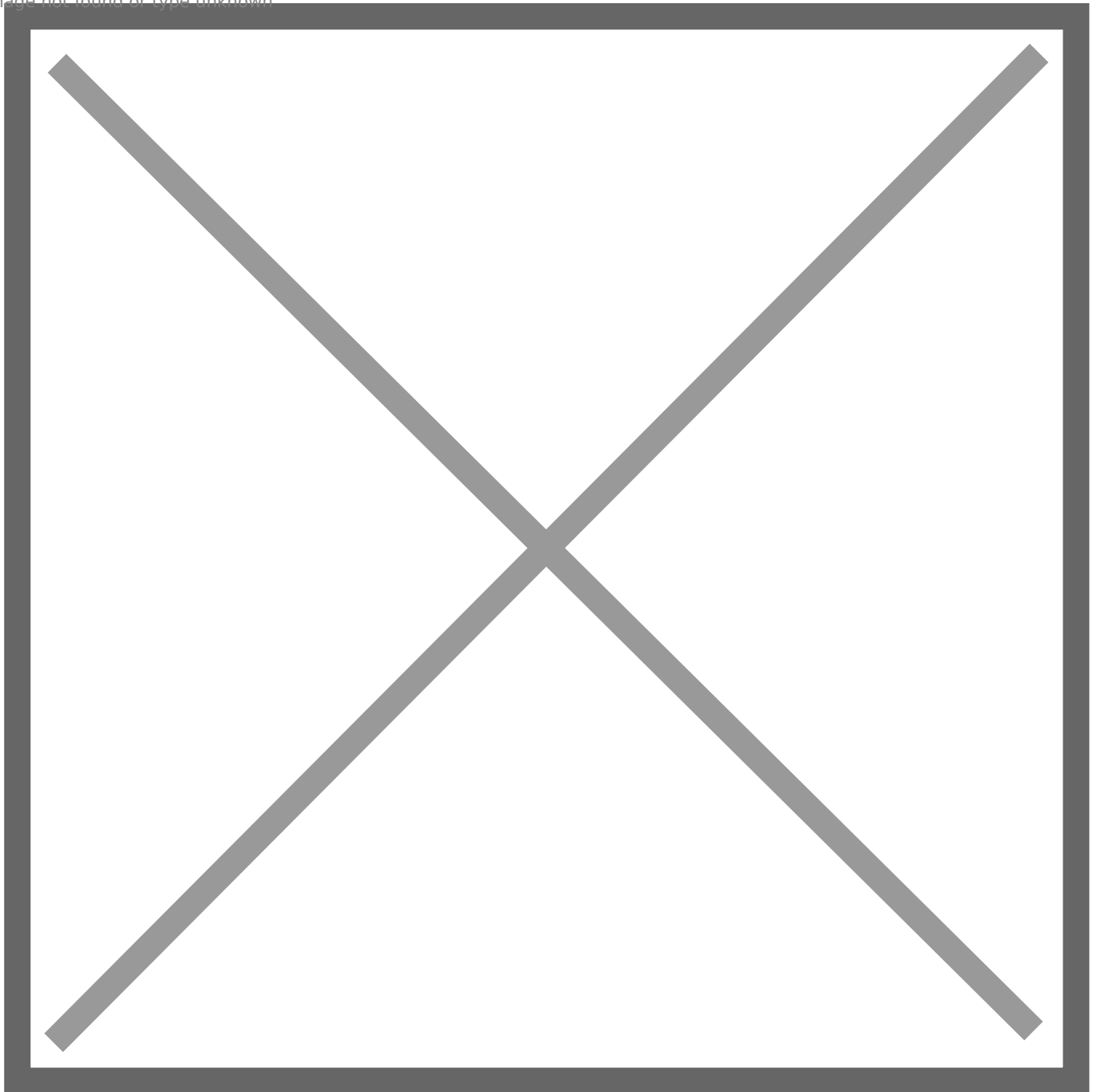
Figure 24

Image not found or type unknown
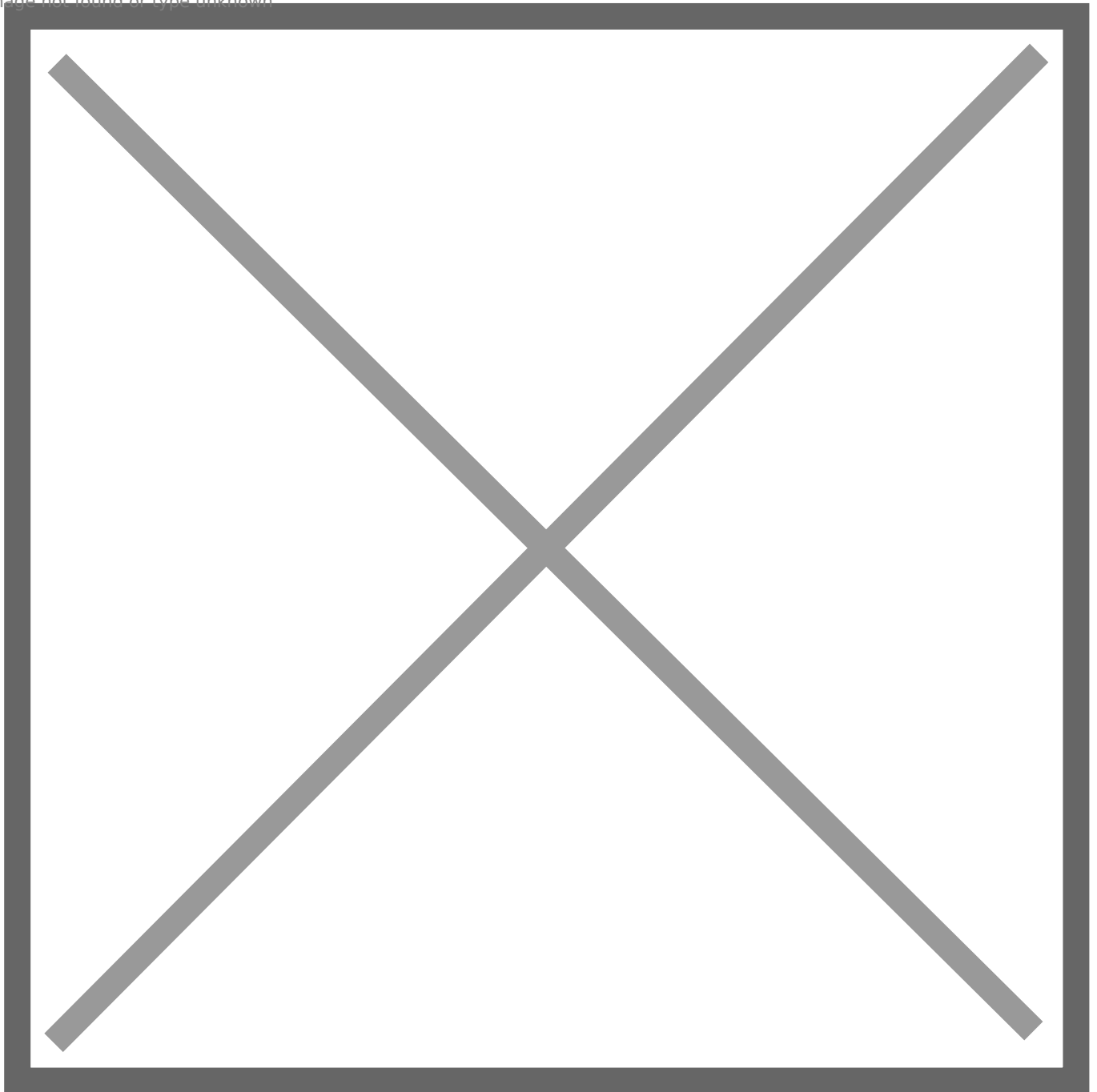
30. Clicking the Advanced Options button from the previous step, will display the Advanced Options section.
31. Under the **Advanced Options** section, in the **Tag** field, enter **NO_WAN_OUTBOUND** (**Figure 25**).
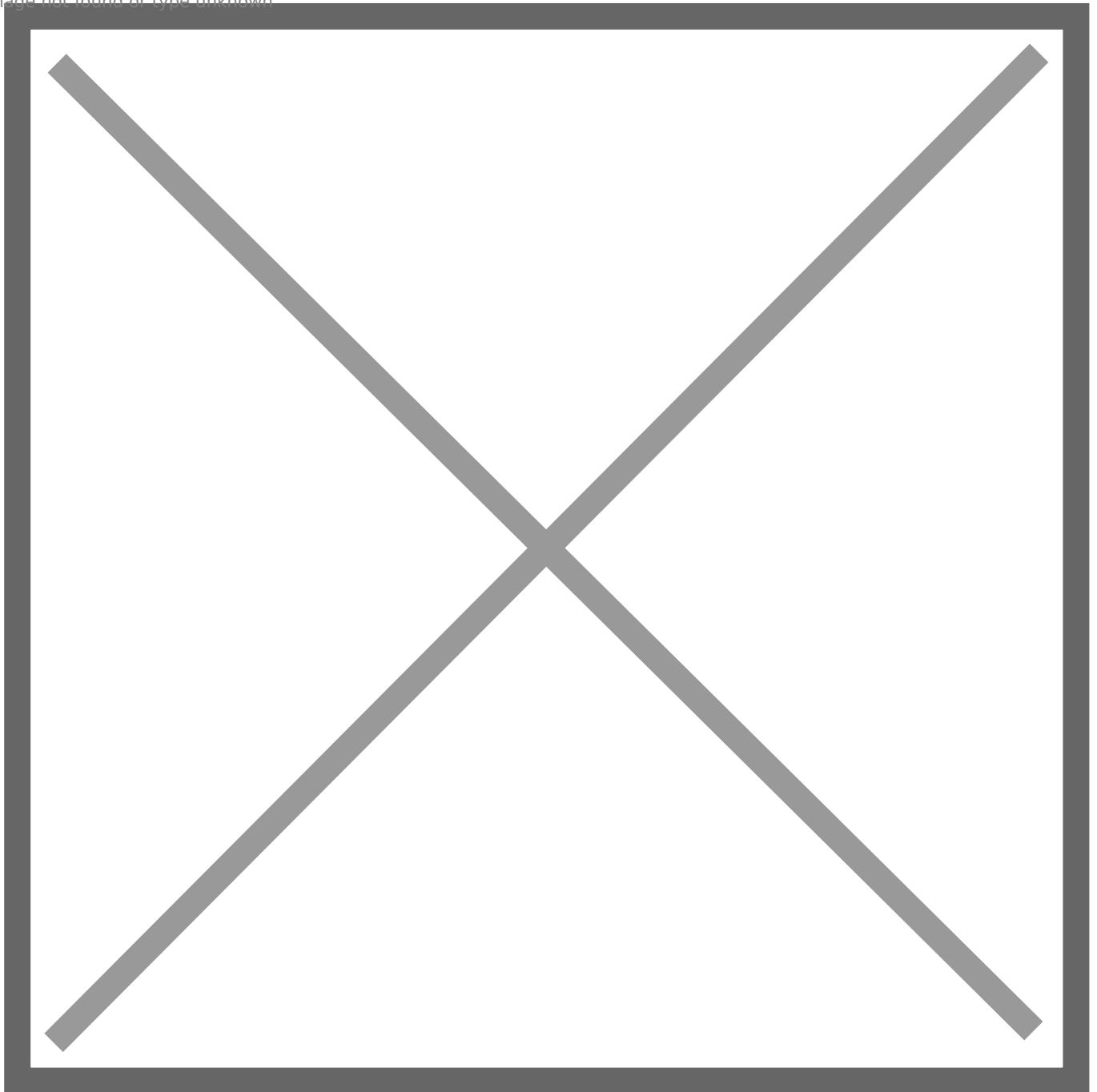
Figure 25

32. Under the A**dvanced Options** section, in the **Gateway** field, ensure the **OpenVPNGatewayGroup** gateway is selected (**Figure 26**).
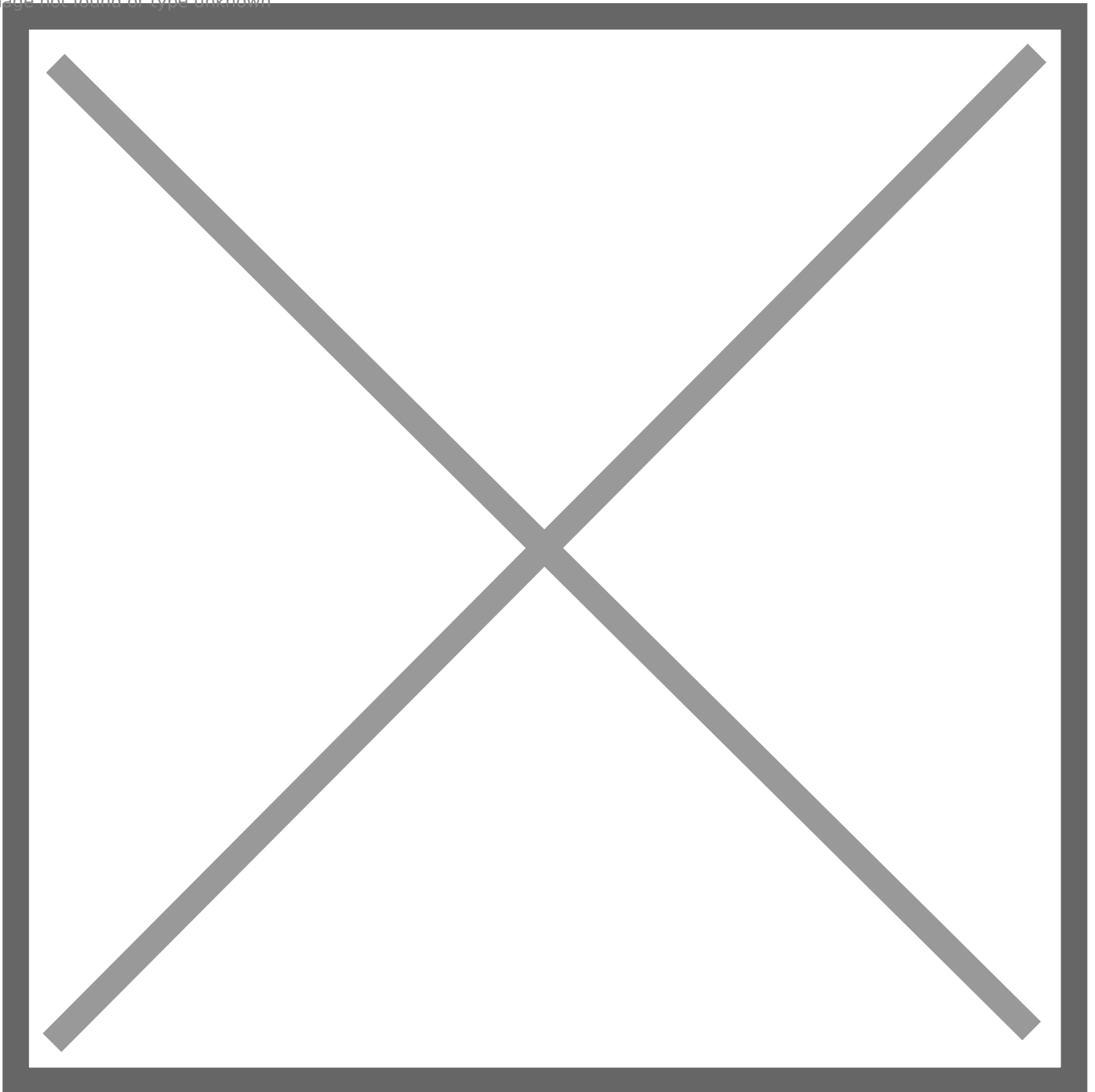
Figure 26

32. Click the **Save** button at the bottom of the page.
33. You will be re-directed back to the **LAN** rules tab page.
34. Click on the **Apply Changes** button on the top of the page to apply the changes (**Figure 27**).

**Figure 27**

Image not found or type unknown

Create a Rule to Bypass OpenVPN Connections

If you have a need for certain IPs inside your LAN to bypass the OpenVPN connections and go through the WAN gateway like normally, you would simply create a LAN rule and place it **ABOVE** the **Allow LAN to any via VPN Only** rule we created above.

1. Navigate to **Firewall --> Aliases** and ensure **IP** tab is selected (**Figure 28**).

Figure 28
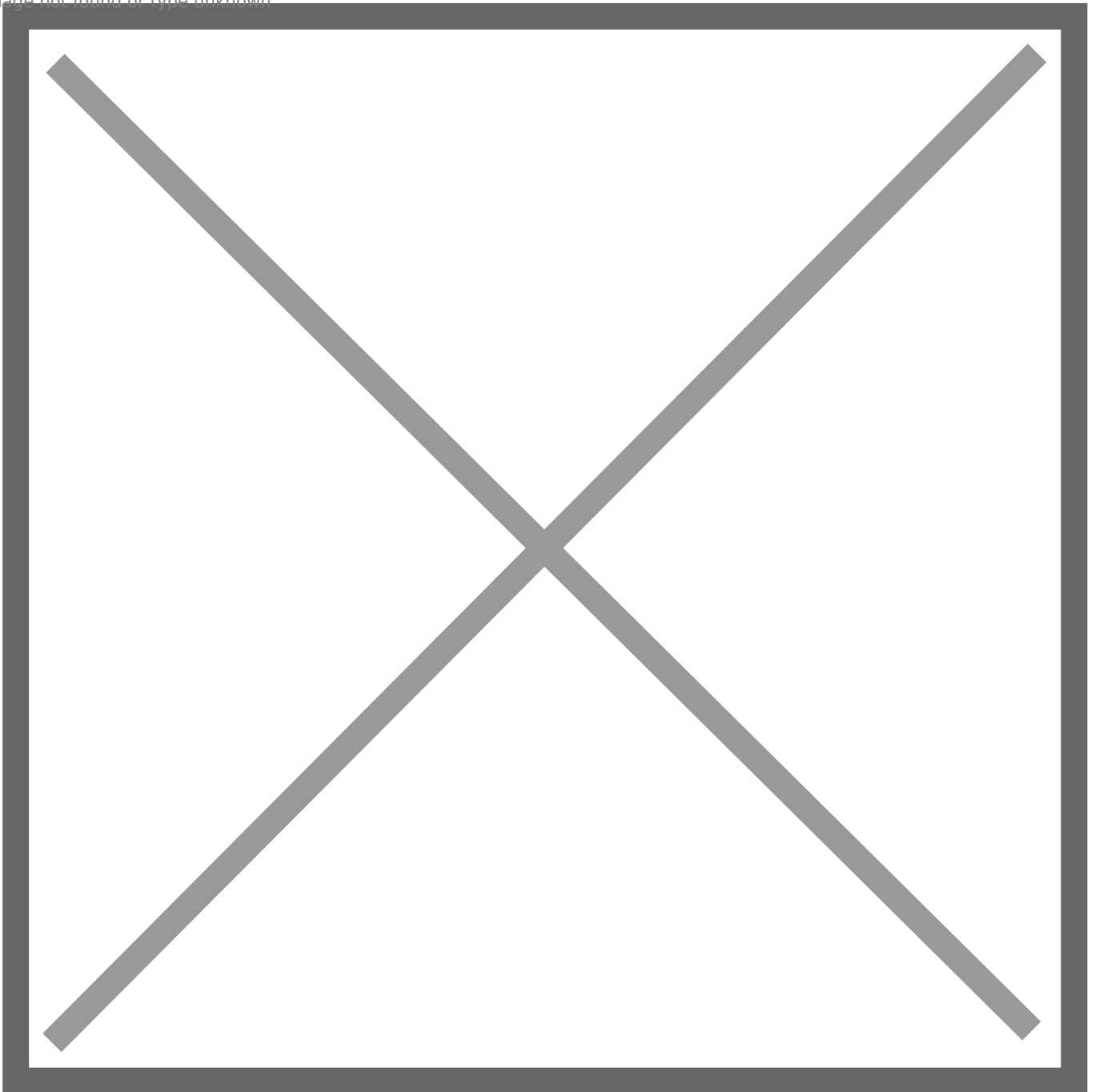
2. Click the **Add** button at the bottom of the page.
3. You will be re-directed to the **Firewall / Aliases / Edit** page.
4. Under the **Properties** section, in the **Name** field, enter a name for this alias (Ex: **Outbound_Direct_NO_VPN**). Ensure you take note of the alias name you assigned because we are going to use it in the LAN rule we will be creating below.
5. Under the **Properties section**, in the **Type** field, ensure **Host(s)** is selected (**Figure 29**).
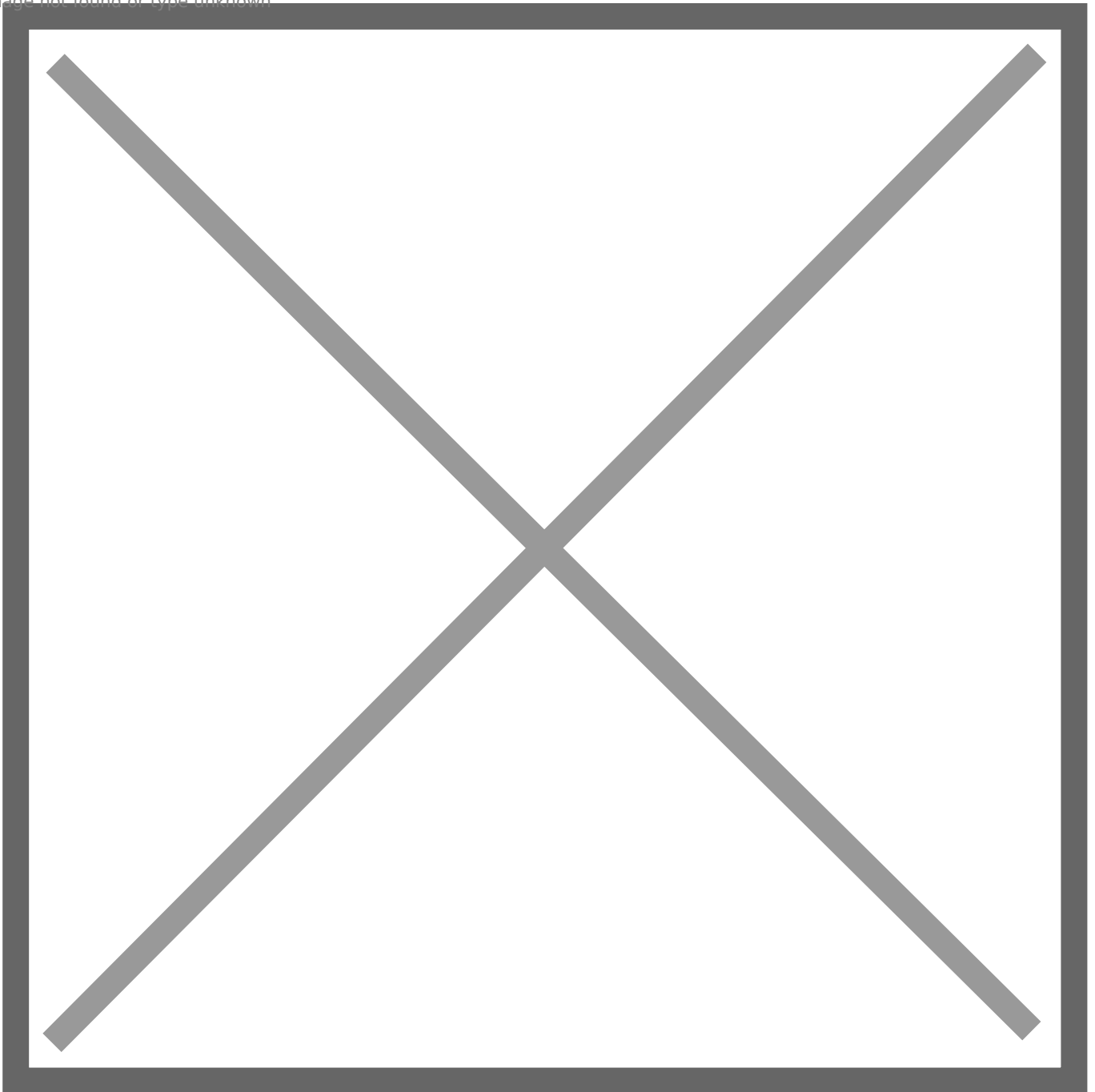
Figure 29
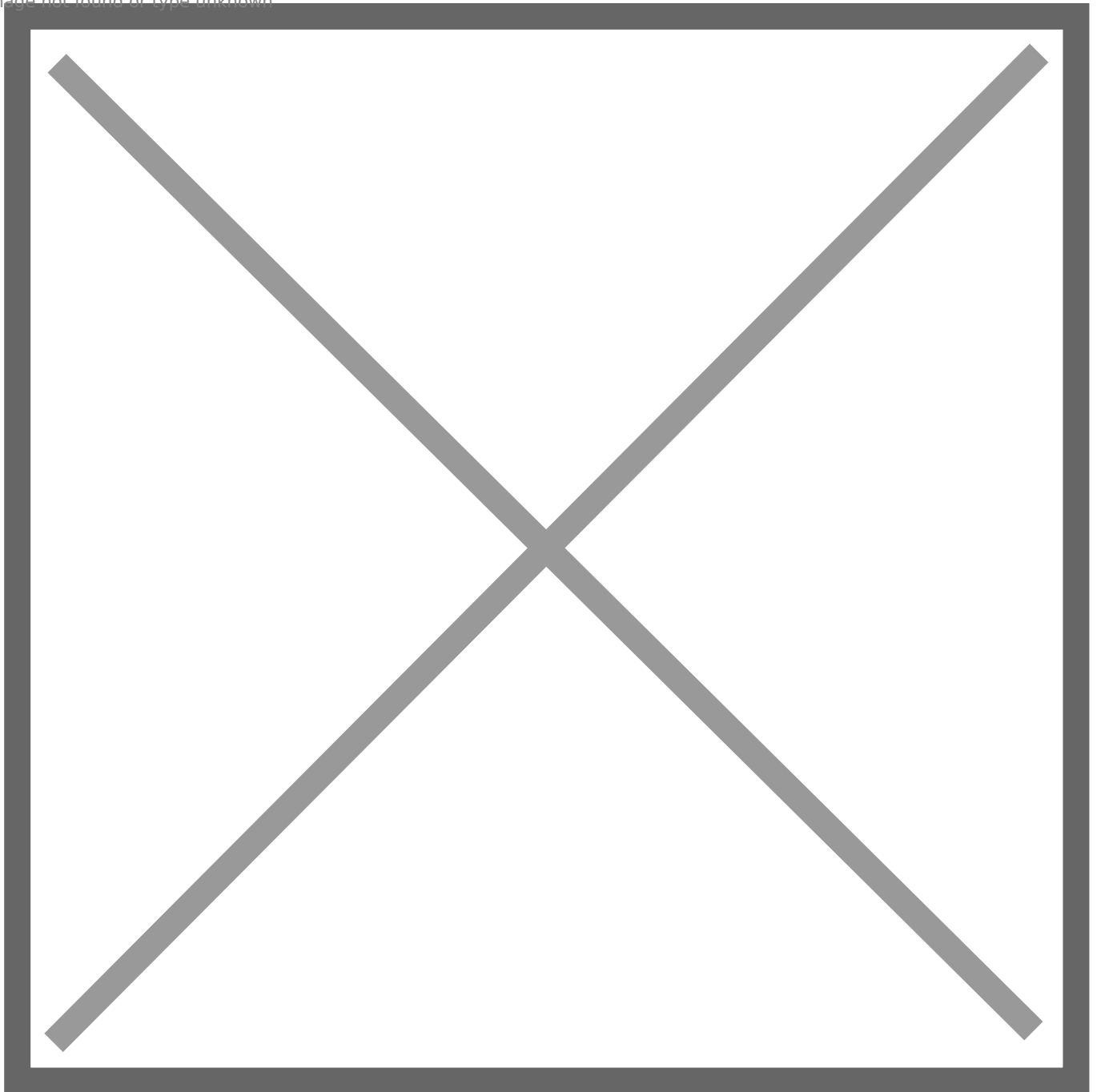
2. Under the **Host(s)** section, enter any LAN IPs (one per line) that you want to bypass the OpenVPN connections (You can add more lines by clicking the **Add Host** button at the bottom of the page).
3. When finished, click the **Save** button at the bottom of the page (**Figure 30**).
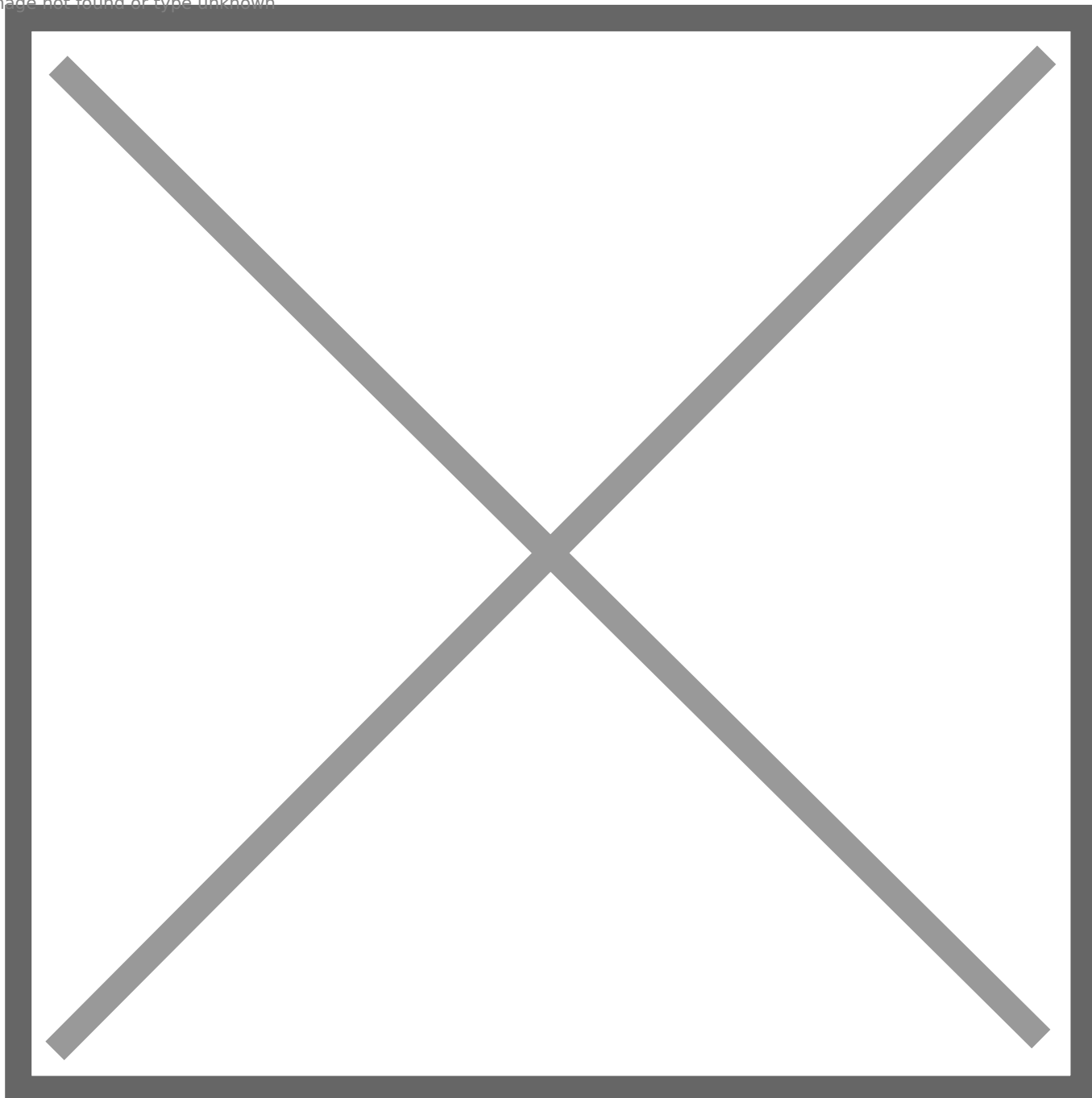
Figure 30

4. You will be re-directed back to the **Aliases IP** tab page.
5. Click on the **Apply Changes** button on the top of the page to apply the changes (**Figure 31**).
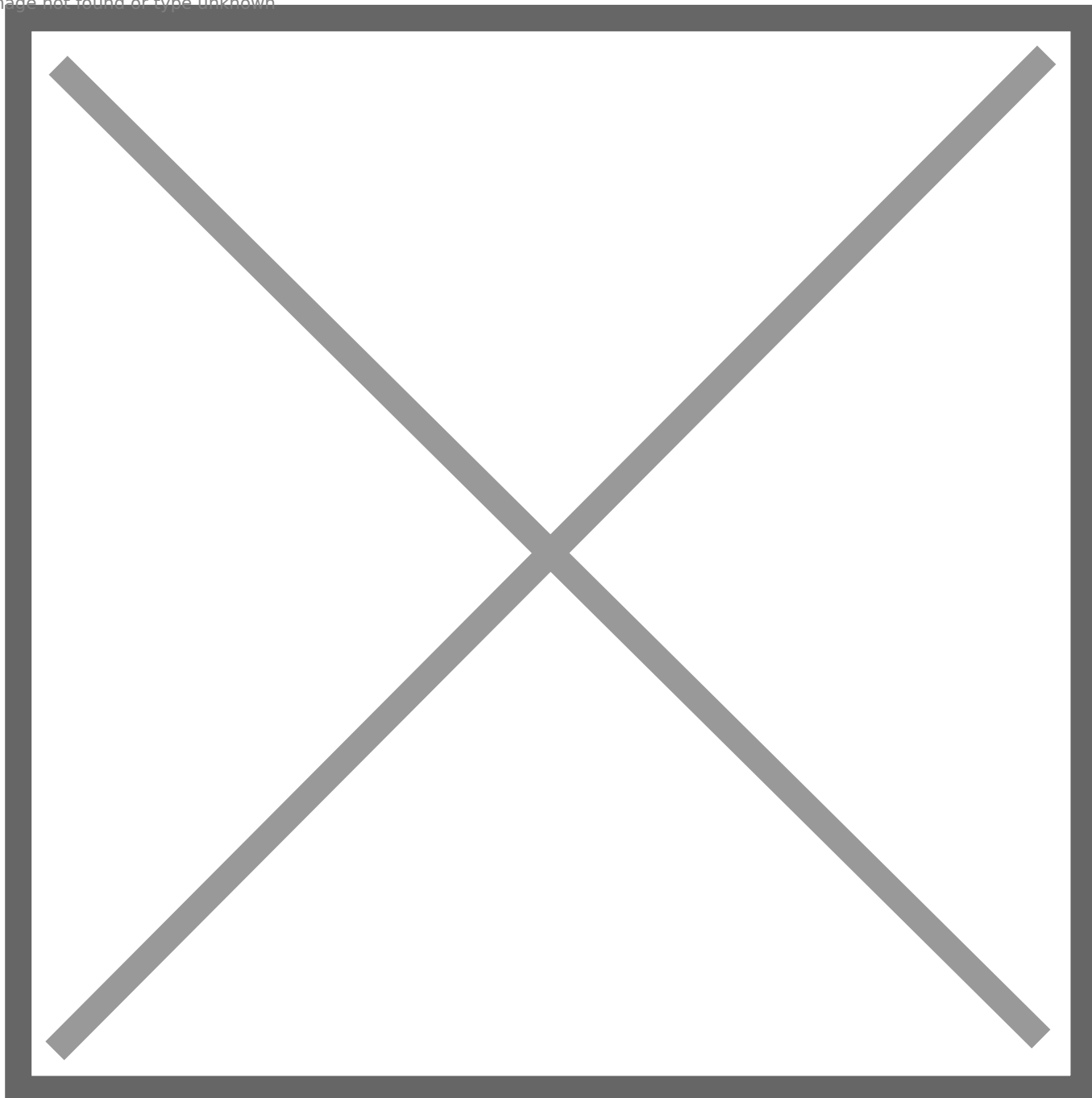
Figure 31

4. Next, navigate to **Firewall --> Rules** and ensure the **LAN** tab is selected. (**Figure 32**).
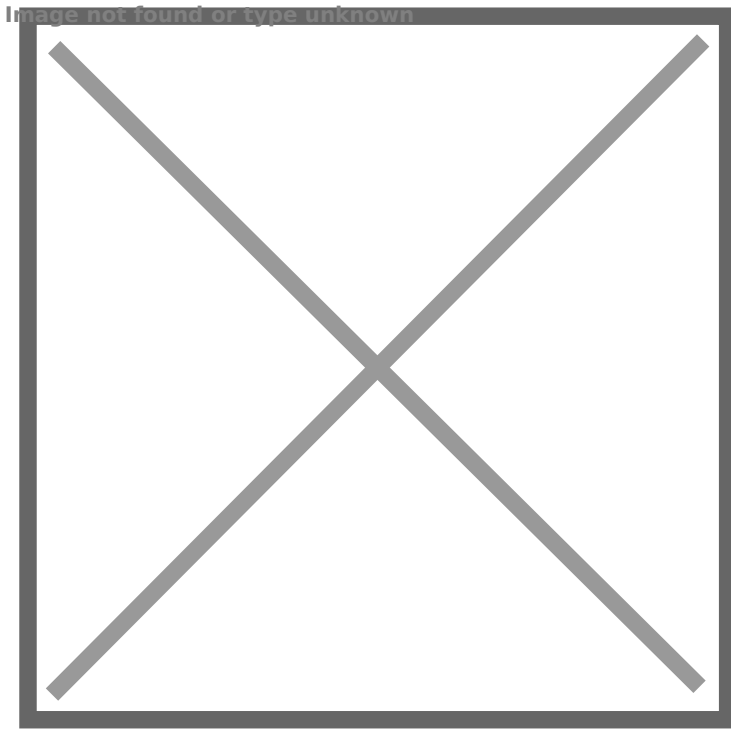
Figure 32

2. Click the Add button with the up arrow on the bottom of the page to add a rule to the top of the list (**Figure 33**).
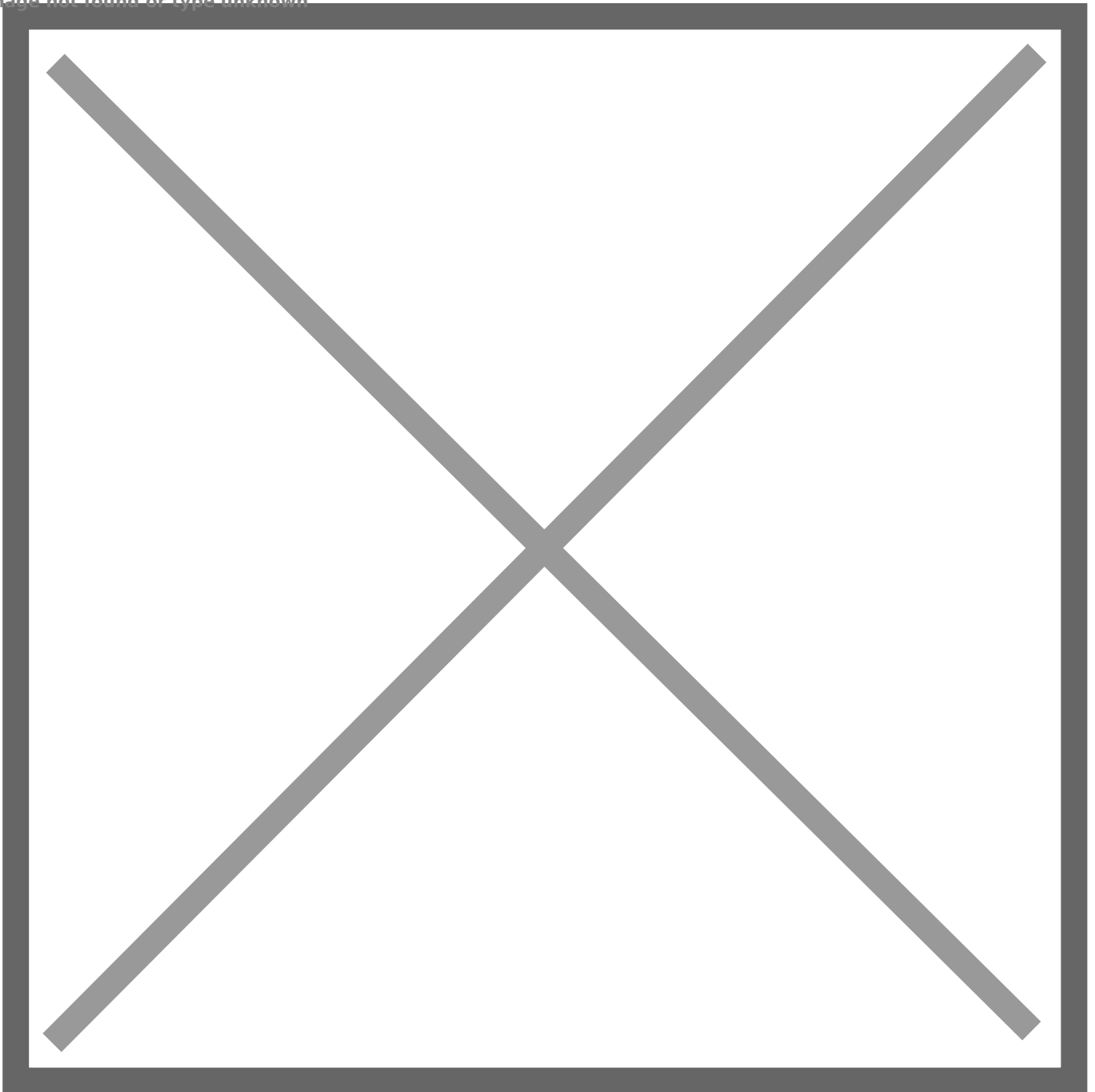
Figure 33

19. You will be re-directed to the **Edit firewall Rule** page.
20. In the **Action** field ensure **Pass** is selected.
21. In the **Disabled** field ensure **Disable this rule** is **Unchecked**.
22. In the **Interface** field ensure the **LAN** interface is selected.
23. In the **Address Family** ensure **IPv4** is selected.
24. In the **Protocol** field ensure **Any** is selected.
25. Uder the **Source** section, in the **Source** field, ensure **Single host or alias** is selected and then enter the name of the alias you created above (**Outbound_Direct_NO_VPN**).
26. Under the **Destination** section, in the **Destination** field, ensure **any** is selected (**Figure 34**).
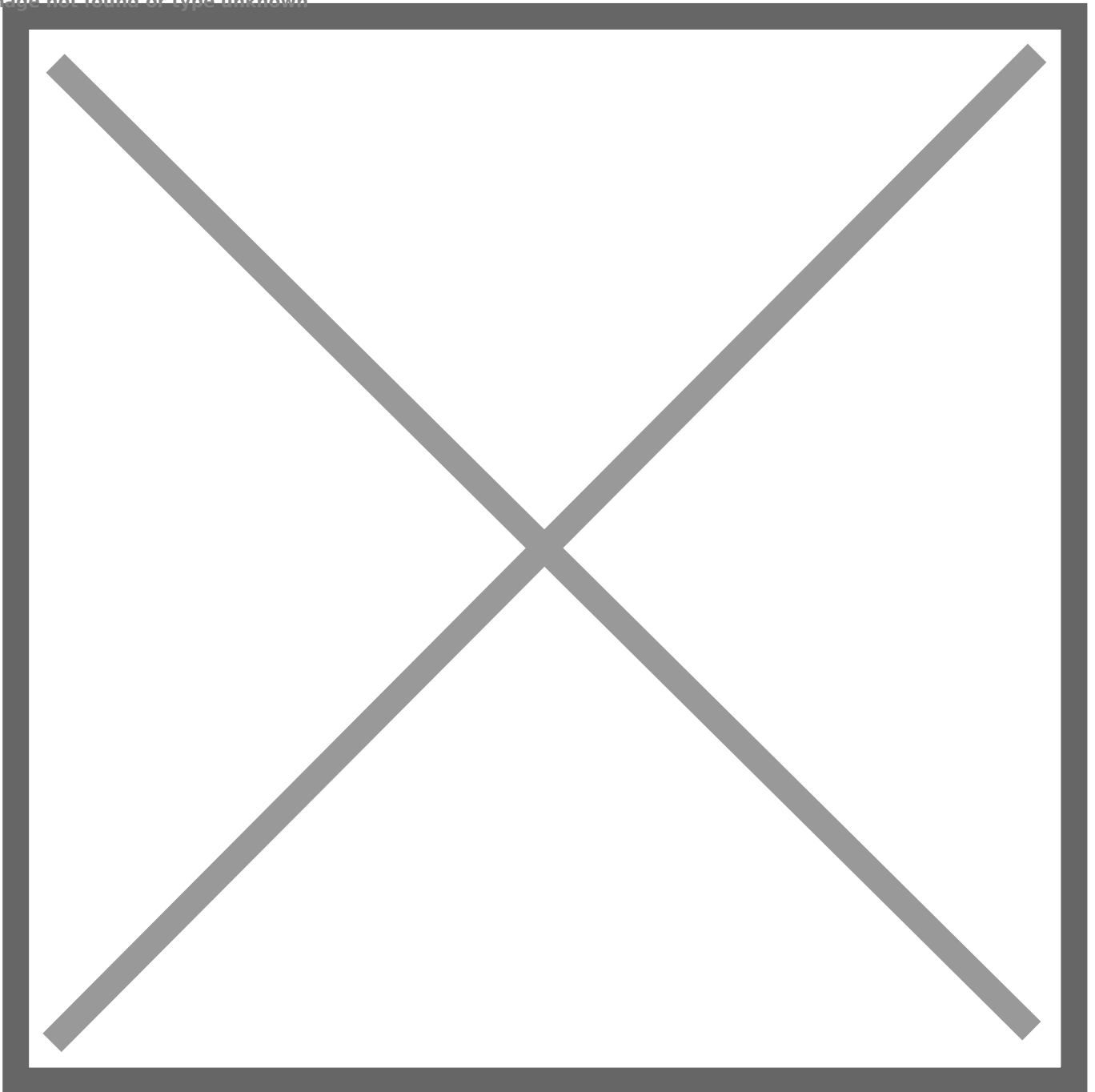
Figure 34

25. Under the **Extra Options** section, in the **Log** field, ensure **Log packets that are handled by this rule** is checked.
26. Under the **Extra Options** section, in the **Description** field, enter a description for this rule (Ex: Allow LAN to any rule NO VPN) (**Figure 35**).
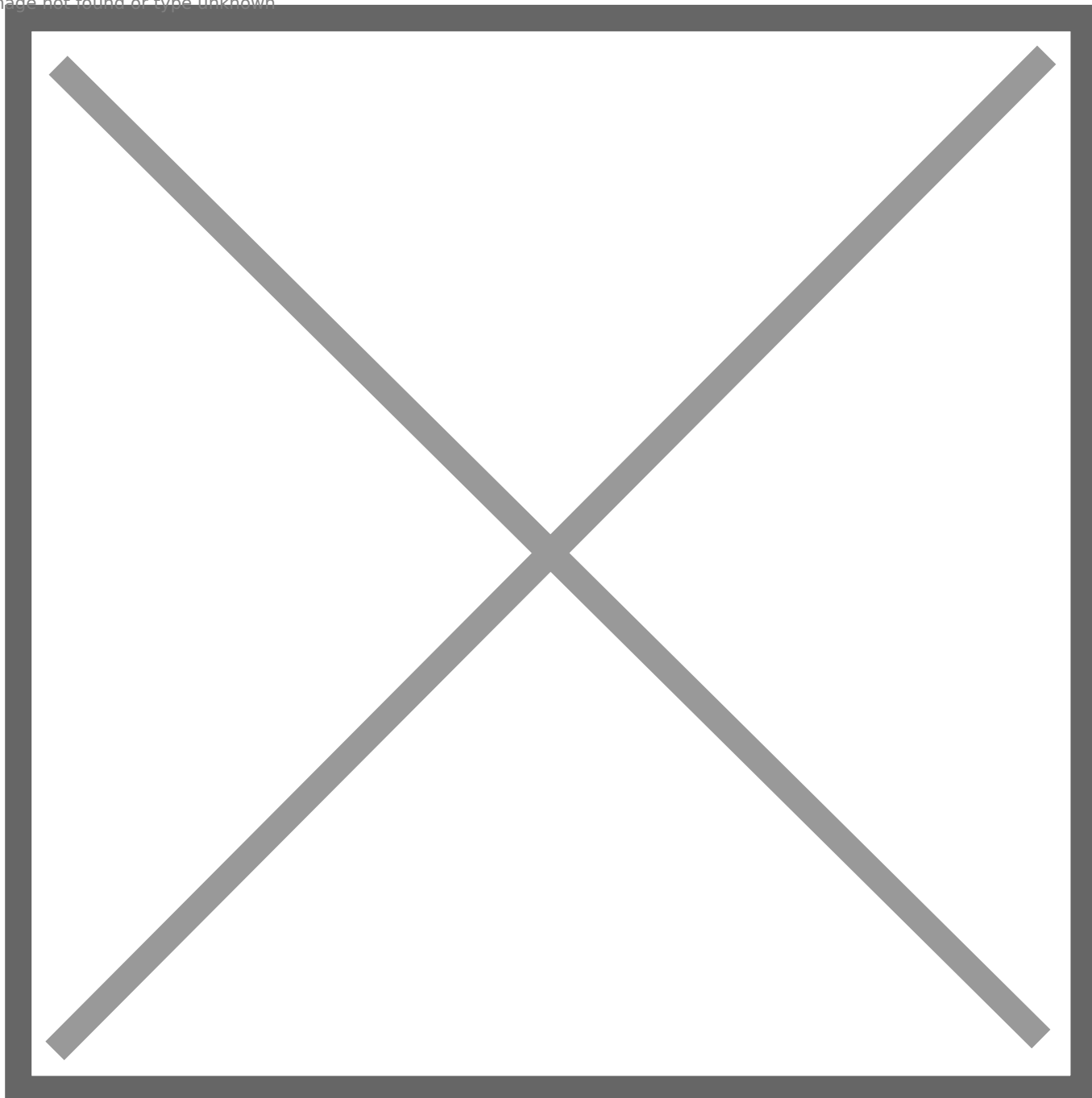
Figure 35

27. Click the **Save** button at the bottom of the page.
28. You will be re-directed back to the **LAN** rules tab page.
29. Click on the **Apply Changes** button on the top of the page to apply the changes (**Figure 36**).

Figure 36

Image not found or type unknown

Revision #2
Created 22 December 2020 12:09:38 by Dino Edwards
Updated 22 December 2020 12:11:20 by Dino Edwards