PfSense, HAProxy, SoftEther VPN

Introduction

This guide was written in order to assist in setting up HAProxy in PfSense in order to route SSL (443) traffic to either a SoftEther SSL VPN server or a webserver listening on port 443 based on SNI. In actuality, any SSL VPN server will suffice, however SoftEther VPN is the server of choice in this example.

Software Used

- PfSense Version 2.4.4
- HAProxy Version 17-1.7.11_1 for PfSense

Install HAProxy in Pfsense

1. In the PfSense Web GUI, click on **System --> Package Manager --> Available Packages**.
2. Locate the **haproxy** package, click on the **Install** button and wait for the installation to complete.
3. After **haproxy** succesfully installs, click on **Services --> HAProxy --> Backend**

Add SoftEther VPN Backend

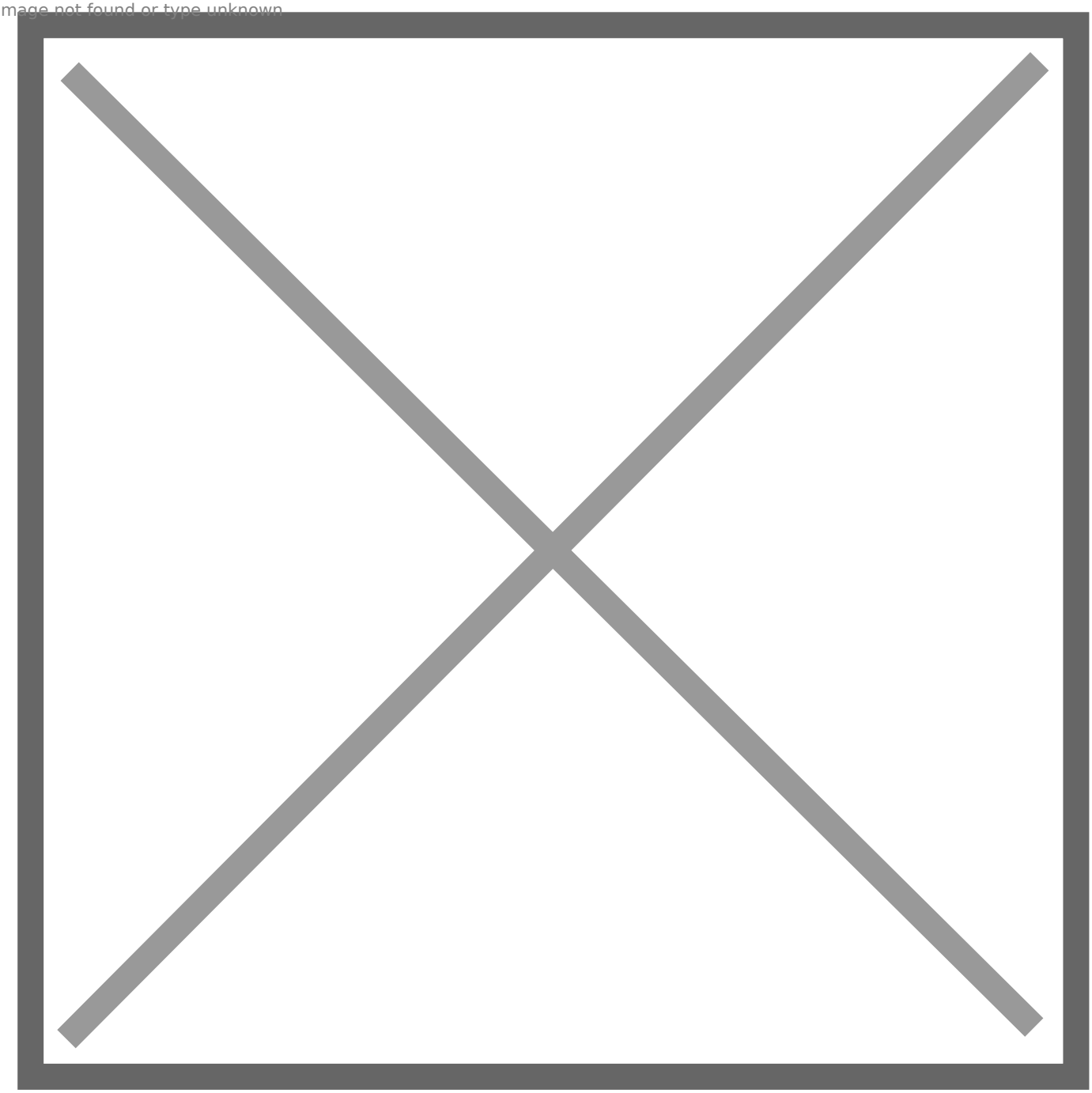
1. In the **Backend** tab, click the Add button.
2. In the **Edit HAProxy Backend server pool** page set the following:

- In the **Name** field, enter a name Ex: SoftEtherVPN.
- In the **Server list** section, click the down arror icon ☒ to add a new server entry.
- In the **Mode** field ensure **active** is selected
- In the **Name** field enter a name Ex: SoftEtherVPN
- In the **Forwardto** field ensure **Address+Port** is selected
- In the **Address** field enter the IP address of your SoftEther VPN Server Ex: 192.168.0.100

- In the **Port** field enter **443**
- Ensure **Encrypt(SSL)** is **unchecked**
- Ensure **SSL checks** is **unchecked**
- Ensure **Weight** is empty
- Scroll down to the **Health checking** section and ensure **None** is selected in the **Health check method** field
- Click the **Save** button at the bottom of the page (**Figure 1**)

Figure 1

Image not found or type unknown



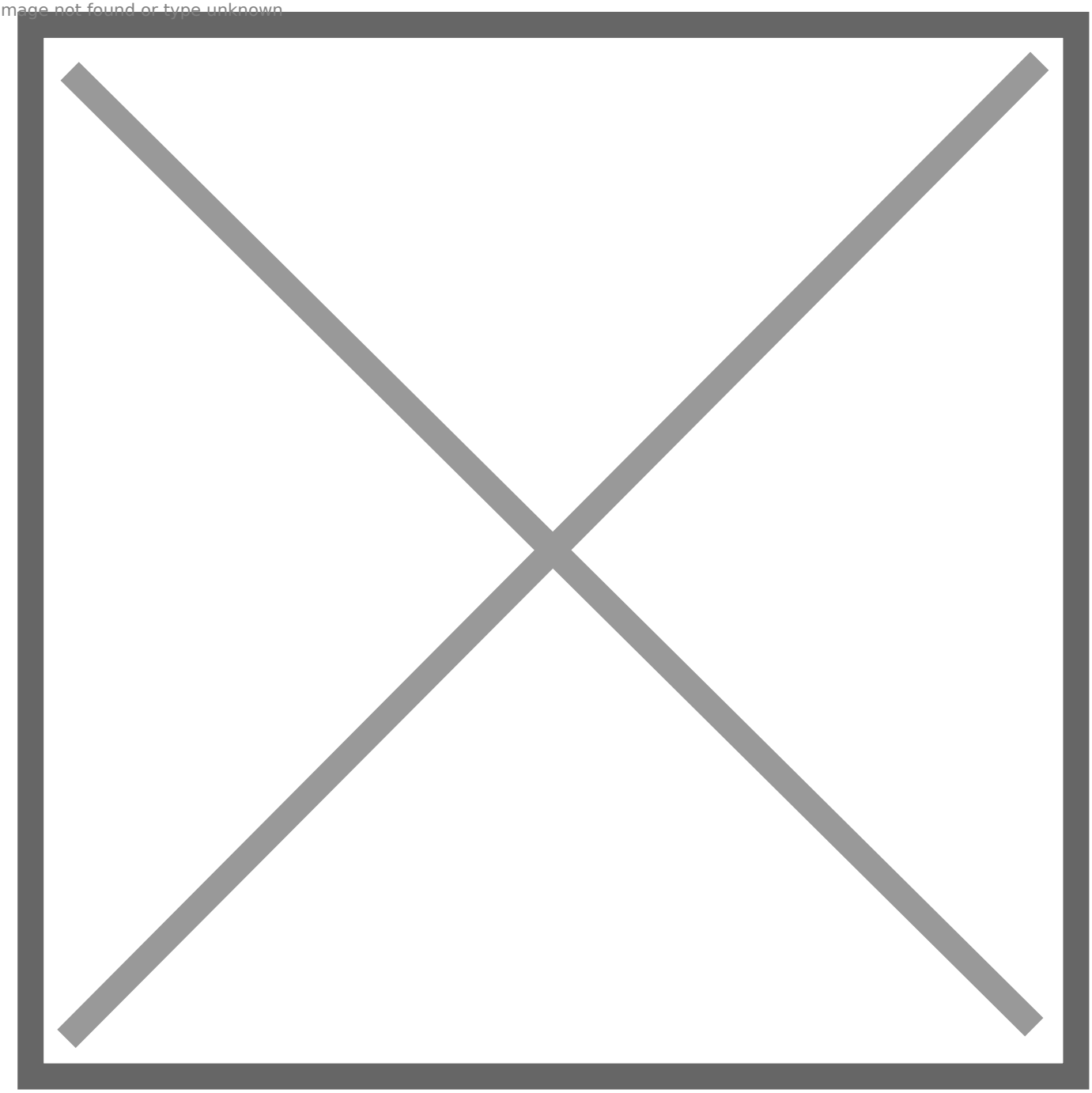
Add Webserver Backend

1. Back the **Backend** tab, click the Add button.
2. In the **Edit HAProxy Backend server pool** page set the following:

- In the **Name** field, enter a name Ex: Webserver.
- In the **Server list** section, click the down arrow icon ☒ to add a new server entry.
- In the **Mode** field ensure **active** is selected
- In the **Name** field enter a name Ex: Webserver
- In the **Forwardto** field ensure **Address+Port** is selected
- In the **Address** field enter the IP address of your SoftEther VPN Server Ex: 192.168.0.200
- In the **Port** field enter **443**
- Ensure **Encrypt(SSL)** is **unchecked**
- Ensure **SSL checks** is **unchecked**
- Ensure **Weight** is empty
- Scroll down to the **Health checking** section and ensure **None** is selected in the **Health check method** field
- Click the **Save** button at the bottom of the page (**Figure 2**)

Figure 2

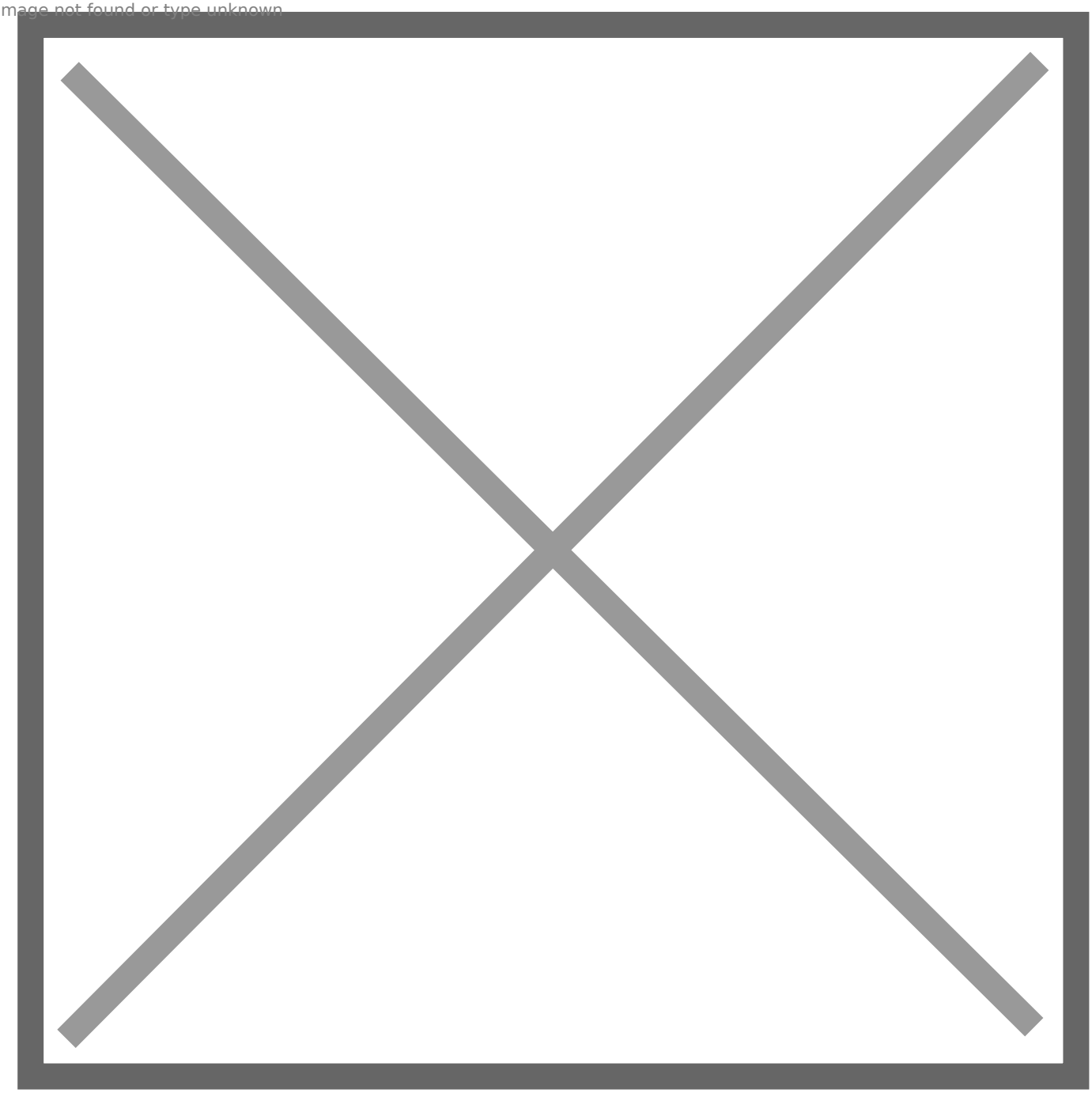
Image not found or type unknown



14. Back in the **Backend** tab, click on the **Apply Changes** button (**Figure 3**)

Figure 3

Image not found or type unknown



Add Frontend

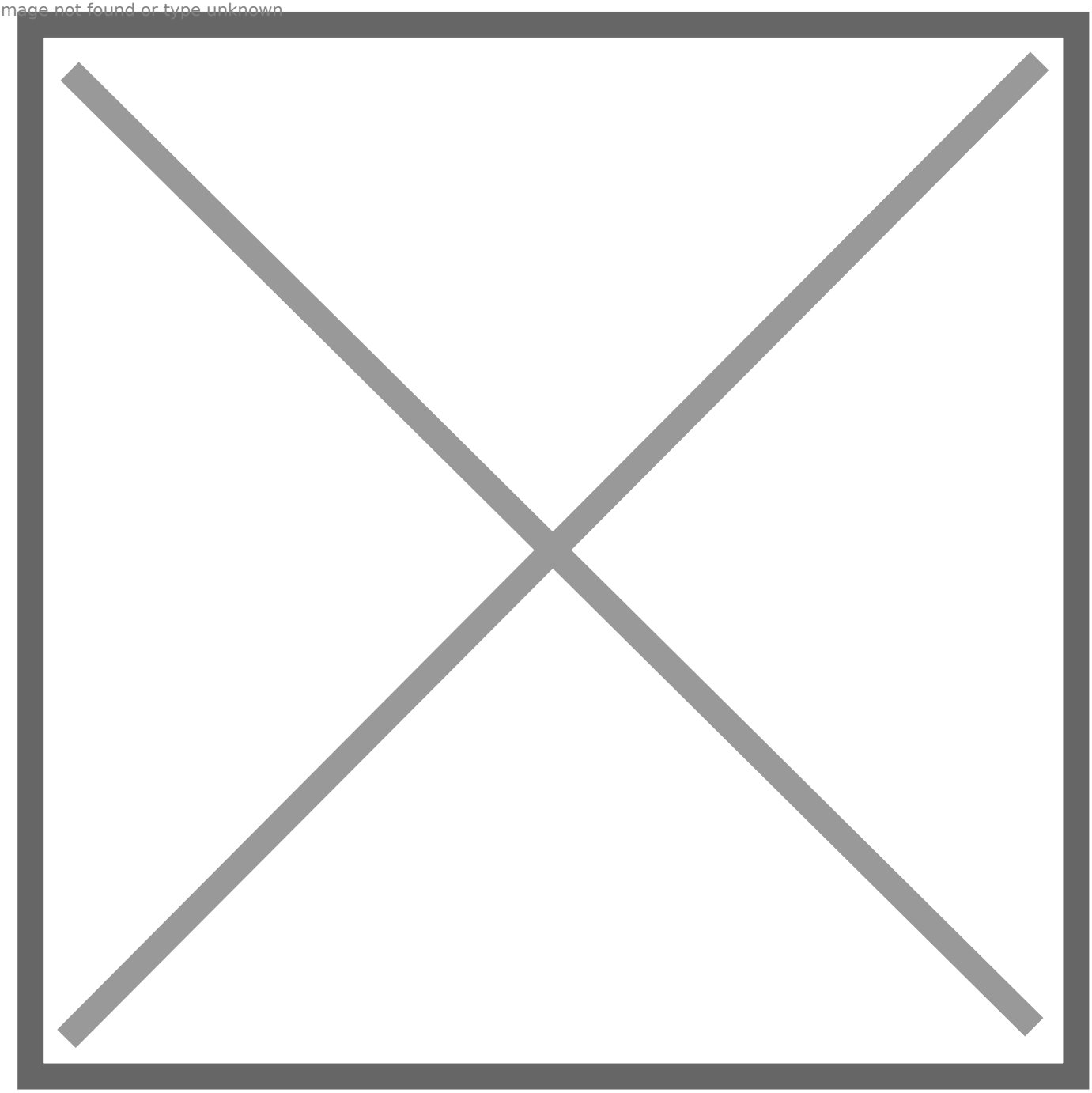
1. Click on **Services --> HAProxy --> Frontend**
2. Click the **Add** button
3. In the **Edit HAProxy Frontend** page set the following:

- In the **Name** field enter a friendlyname Ex: widgetsinc-frontend
- Ensure the **Status** field is set to **Active**
- Under the **External Address --> Table** section, ensure the **Listen Address** field is set to **WAN address (IPv4)**
- Ensure the **Type** field is set to **ssl /https(TCP mode)**

- Under the **External Address --> Table** section, ensure the **Port** field is set to **443**
- Under the **External Address --> Table** section, ensure the **SSL Offloading** field is **unchecked**
- Under the **External Address --> Table** section, ensure the **Advanced** field is **empty**
- Under the **Type** section, ensure **ssl/https(TCP mode)** is selected
- Under the **Default backend, access control lists and actions --> Access Control lists** section, click the down arrow icon ☒ to add an ACL entry for the SoftEther VPN Server
- In the **Name** field enter a name for this ACL Ex: SoftetherACL
- In the **Expression** field ensure **Server Name Indication TLS extension matches** is selected
- Ensure the **CS** field is unchecked
- Ensure the **Not** field is unchecked
- In the **Value** field, enter the FQDN to reach your SoftEther VPN server Ex: vpn.domain.tld
- Again, click the down arrow icon ☒ to add an ACL entry for the Webserver
- In the **Name** field enter a name for this ACL Ex: WebserverACL
- In the **Expression** field ensure **Server Name Indication TLS extension matches** is selected
- Ensure the **CS** field is unchecked
- Ensure the **Not** field is unchecked
- In the **Value** field, enter the FQDN to reach your Webserver Ex: www.domain.tld
- Under the **Default backend, access control lists and actions --> Actions** section, click the down arrow icon ☒ to add an action for the SoftEther VPN ACL we created above
- In the **Action** field, ensure **Use Backend** is selected and ensure the SoftetherVPN backend we created earlier is selected
- In the **Condition acl names** field, enter the ACL name you set for the Softether ACL Ex: SoftetherACL
- Again, click the down arrow icon ☒ to add an action for the Webserver ACL we created above
- In the **Action** field, ensure **Use Backend** is selected and ensure the Webserver backend we created earlier is selected
- In the **Condition acl names** field, enter the ACL name you set for the Webserver ACL Ex: WebserverACL (**Figure 4**)

Figure 4

Image not found or type unknown

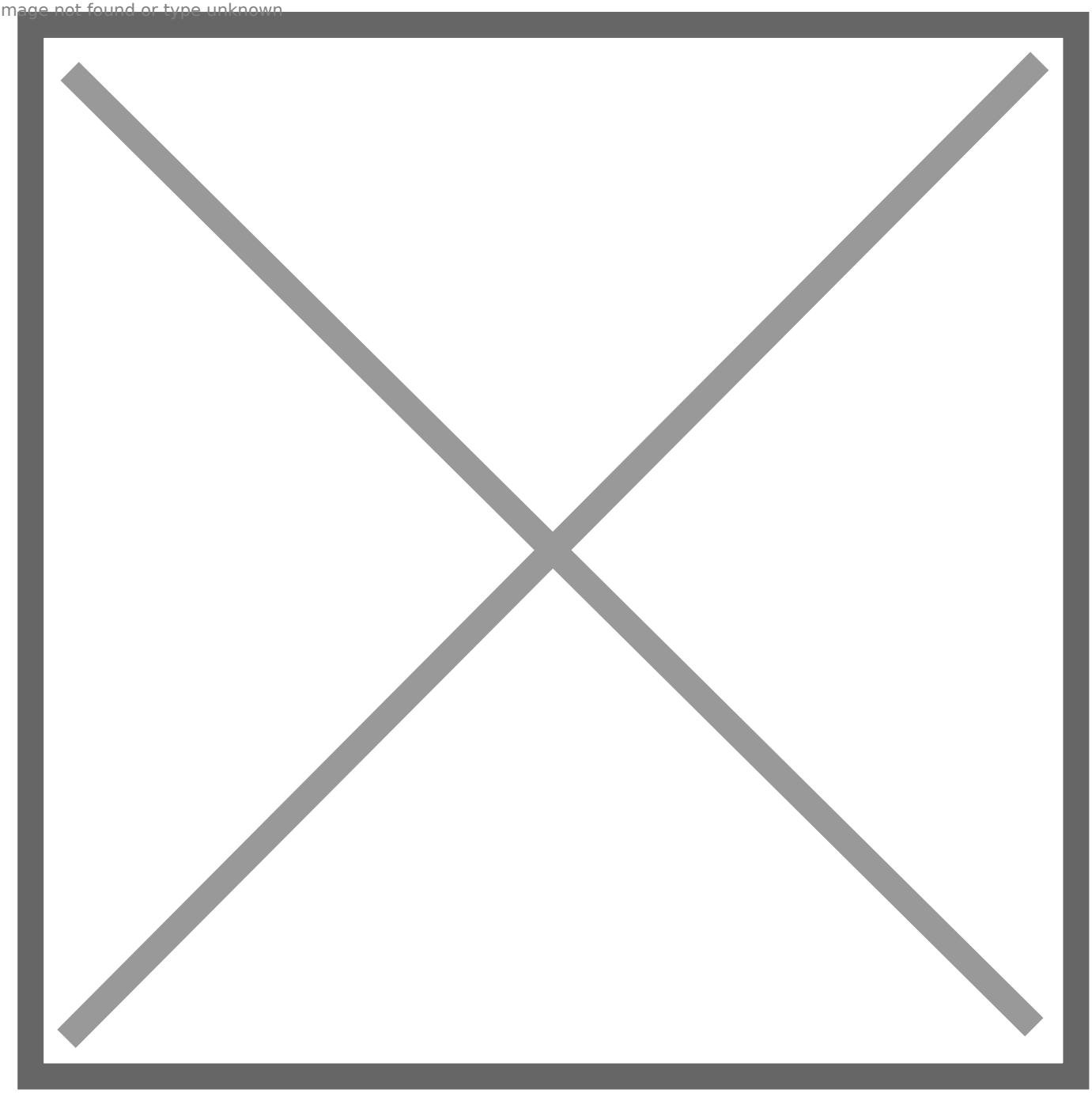


Enable HAProxy

1. Click on **Services --> HAProxy --> Settings**
2. Under **General Settings --> Enable HAProxy** field is checked
3. In the **General Settings --> Maximum Connections** field, enter the number of connections per process Ex: 1000
4. Click the **Save** button on the bottom of the page (**Figure 5**)

Figure 5

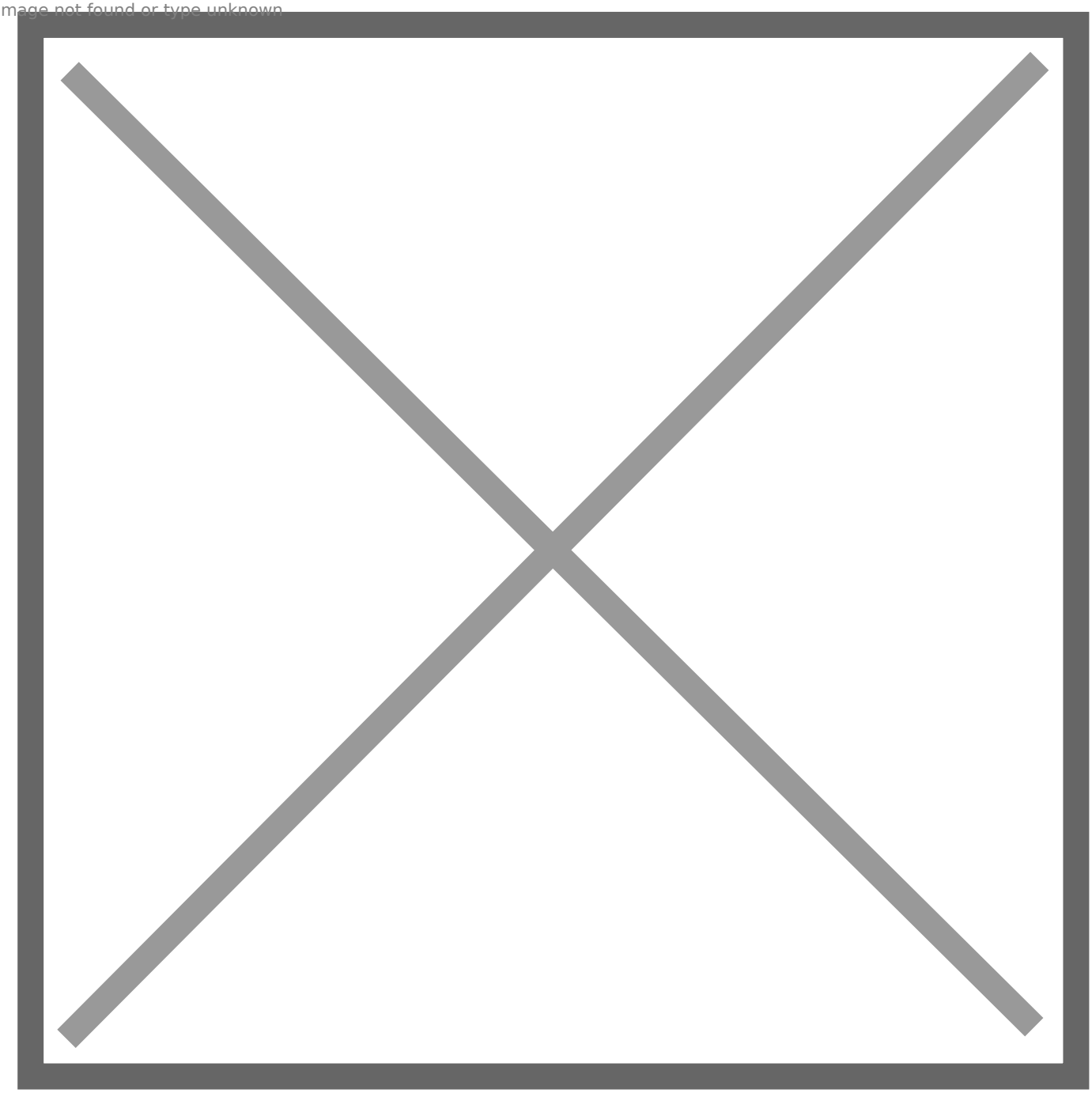
Image not found or type unknown



5. Back in the **Settings** tab, click on the **Apply Changes** button (**Figure 6**)

Figure 6

Image not found or type unknown



Add Firewall Rule

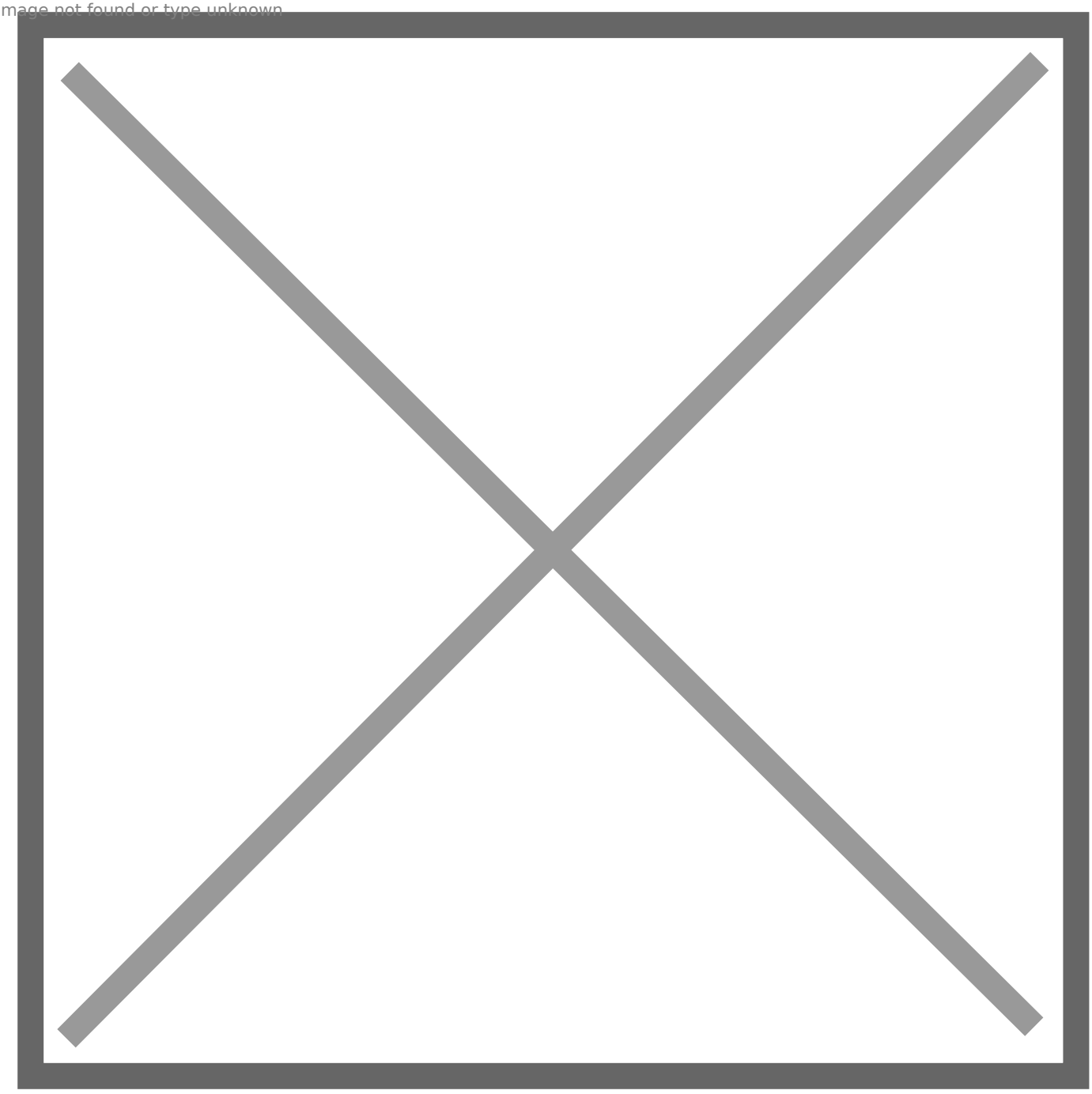
1. Click on **Firewall --> Rules**
2. Click the **Add** button
3. n the **Edit Firewall Rule** page set the following:

- Ensure the **Interface** field is set to **WAN**
- Ensure the **Address Family** field is set to **IPv4**
- Ensure the **Protocol** field is set to **TCP**
- Under the **Source** section, ensure **Source** field is set to **any**
- Under the **Destination** section, ensure **Destination** is set to **WAN address**

- Under the **Destination** section, ensure **Destination Port Range From** is set to **HTTPS (443)** and **To** is set **HTTPS (443)**
- Under **Extra Options** section, set the **Description** field
- Click the **Save** button at the bottom of the page (**Figure 7**)

Figure 7

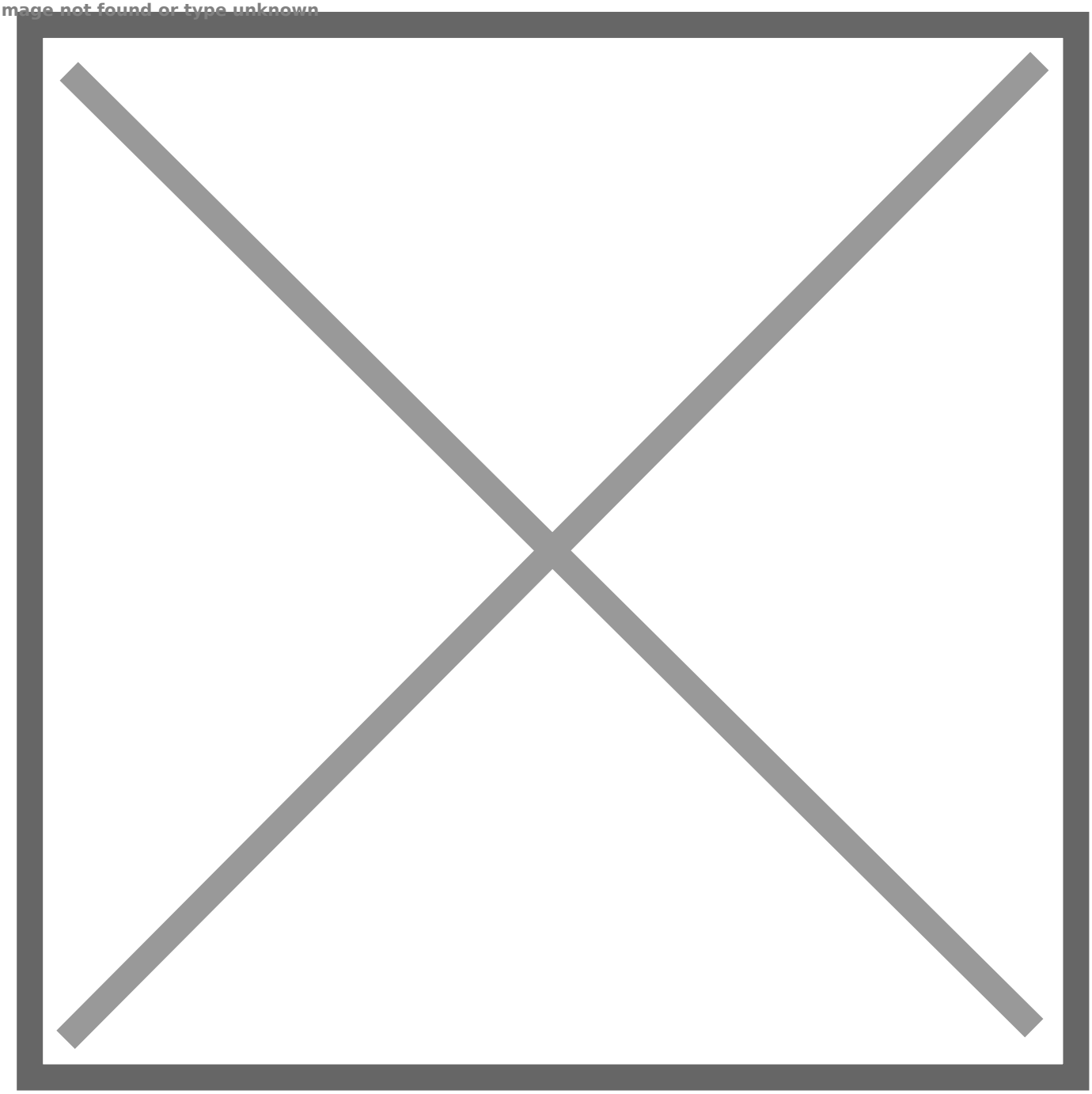
Image not found or type unknown



4. Back in the **Firewall/ Rules / Wan** tab, click on the **Apply Changes** button (**Figure 8**)

Figure 8

Image not found or type unknown



Install Service Watchdog in PfSense

This setup has the potential to expose the PfSense Web GUI to the Internet if the HAProxy service ever fails. In order to mitigate this issue, it's a good idea to install the Service Watchdog package in PfSense so that it can monitor the HAProxy service and start it automatically if it ever fails.

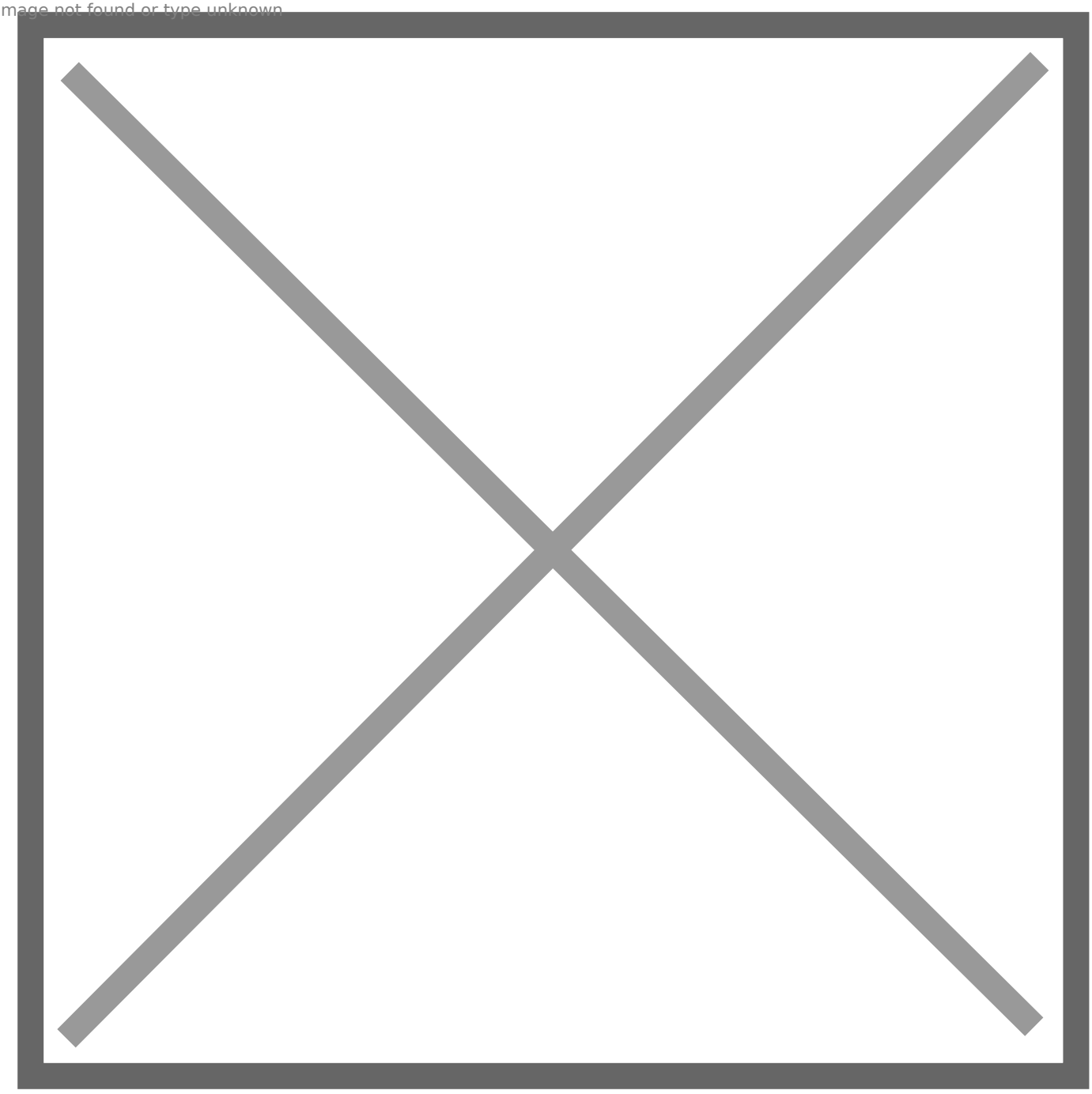
Alternatively, you can change the PfSense Web GUI to another port other than 443.

1. In the PfSense Web GUI, click on **System --> Package Manager --> Available Packages**.
2. Locate the **Service_Watchdog** package, click on the **Install** button and wait for the installation to complete.

3. After **Service_Watchdog** succesfully installs, click on **Services --> Service Watchdog**
4. Click on the **Add New Service** button
5. In the A**dd Service to Monitor** page, in the **Service to Add** field, select **haproxy: TCP/HTTP(S) Load Balancer** from the drop-down and click the **Add** button (**Figure 9**)

Figure 9

Image not found or type unknown



If you are NOT using HAProxy on PfSense

If you are trying to implement HAProxy standalone i.e. not part of PfSense, below is the configuration generated by the PfSense package. Hopefully it will assist someone in their own

HAProxy implementation. Ensure you change **widgetsinc-frontend**, **PUBLIC_IP_ADDRESS**, **vpn.domain.tld** and **www.domain.tld** to fit your needs.

```
global
    maxconn           1000
    stats socket /tmp/haproxy.socket level admin
    uid           80
    gid           80
    nbproc           1
    hard-stop-after       15m
    chroot              /tmp/haproxy_chroot
    daemon
    server-state-file /tmp/haproxy_server_state
frontend widgetsinc-frontend
    bind           PUBLIC_IP_ADDRESS:443 name PUBLIC_IP_ADDRESS:443
    mode           tcp
    log           global
    timeout client       30000
    tcp-request inspect-delay    5s
    acl           SoftetherACL    req.ssl_sni -i vpn.domain.tld
    acl           WebserverACL    req.ssl_sni -i www.domain.tld
    tcp-request content accept if { req.ssl_hello_type 1 }
    use_backend SoftetherVPN_ipvANY  if  SoftetherACL
    use_backend Webserver_ipvANY  if  WebserverACL
backend SoftetherVPN_ipvANY
    mode           tcp
    id           100
    log           global
    timeout connect       30000
    timeout server       30000
    retries           3
    server           SoftEtherVPN 192.168.0.100:443 id 101
backend Webserver_ipvANY
    mode           tcp
    id           102
    log           global
    timeout connect       30000
    timeout server       30000
    retries           3
```

```
server          Webserver 192.168.0.200:443 id 103/
```

Revision #1
Created 22 December 2020 12:14:54 by Dino Edwards
Updated 22 December 2020 12:18:06 by Dino Edwards