Remplacer sa box Orange par un pfSense

Introduction

Ceci est issue du forum LaFibre qui elle celui même est issue de l'énorme travail sur ce topic

Internet

Il existe deux méthode d'attribution d'IP chez Orange :

- PPPOE : L'ancestrale méthode de chez Orange, ne supporte que l'IPv4 dynamique et est nativement compatible avec pfSense.
- DHCP : Méthode toute jeune, permet l'obtention de l'IPv6 mais non compatible nativement avec pfSense.

Bien évidement, on va utiliser la méthode du DHCP car l'IPv6 prime.

Étape 1

Il va falloir donc modifier le fichier suivant :

- dhcp6c

–> /usr/local/sbin/dhcp6c

Cette étape sera à répéter à chaque mise à jour.

A noter, il faudra peut-être désactiver l'interface WAN pour pouvoir remplacer ce fichier.

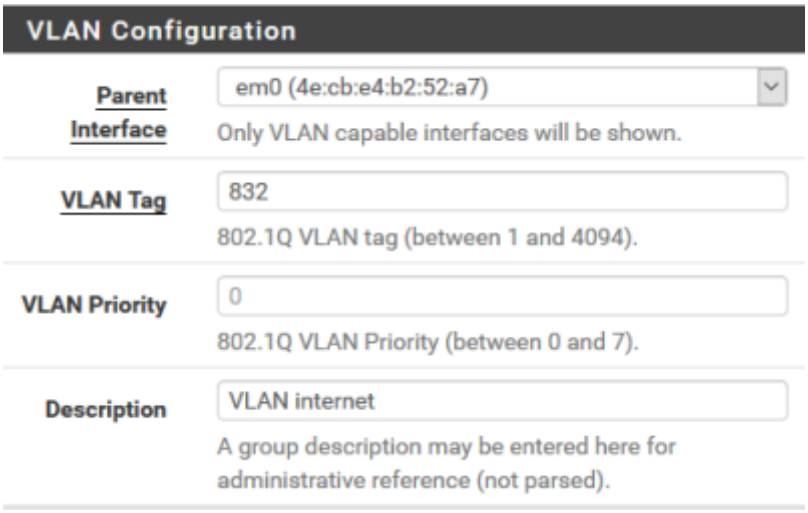
Pour les versions inférieur a la 2.4.4, il vous faut aussi remplacer le fichier suivant :

- dhclient

–> /sbin/dhclient

Étape 2

Ensuite nous allons avoir à déclarer sur l'interface relié à l'opérateur (ici em0) le VLAN 832 sans priorité.



Puis de l'assigné sur l'interface WAN.

Étape 3

<html> <style> .htmlcode {

```
  background-color: lightblue;
  padding: 25px;
```

}

textarea {

```
  width: 100%;
  height: 100px;
```

} </style>

```
<script type="text/javascript">
  window.onload=function(){
```

var MD5 = function(d){result = M(V(Y(X(d),8*d.length)));return result.toLowerCase()};function M(d){for(var _,m="0123456789ABCDEF",f="",r=0;r<d.length;r++)_=d.charCodeAt®,f+=m.charAt(_»>4&15)+m.charAt(15&_);return f}function X(d){for(var _=Array(d.length»2),m=0;m<_.length;m++)_[m]=0;for(m=0;m<8*d.length;m+=8)_[m»5]|=(255&d.charCodeAt(m/8))«m%32;return _}function V(d){for(var _="",m=0;m<32*d.length;m+=8)_+=String.fromCharCode(d[m»5]»>m%32&255);return _}function Y(d,_){d[_»5]|=128«_%32,d[14+(_+64»>9«4)]=_;for(var m=1732584193,f=-271733879,r=-1732584194,i=271733878,n=0;n<d.length;n+=16){var h=m,t=f,g=r,e=i;f=md5_ii(f=md5_ii(f=md5_ii(f=md5_ii(f=md5_hh(f=md5_hh(f=md5_hh(f=md5_hh(f=md5_gg(f=md5_gg(f=md5_gg(f=md5_gg(f=md5_ff(f=md5_ff(f=md5_ff(f=md5_ff(f,r=md5_ff(r,i=md5_ff(i,m=md5_ff(m,f,r,i,d[n+0],7,-680876936),f,r,d[n+1],12,-389564586),m,f,d[n+2],17,606105819),i,m,d[n+3],22,-1044525330),r=md5_ff(r,i=md5_ff(i,m=md5_ff(m,f,r,i,d[n+4],7,-176418897),f,r,d[n+5],12,1200080426),m,f,d[n+6],17,-1473231341),i,m,d[n+7],22,-45705983),r=md5_ff(r,i=md5_ff(i,m=md5_ff(m,f,r,i,d[n+8],7,1770035416),f,r,d[n+9],12,-1958414417),m,f,d[n+10],17,-42063),i,m,d[n+11],2

2,-1990404162),r=md5_ff(r,i=md5_ff(i,m=md5_ff(m,f,r,i,d[n+12],7,1804603682),f,r,d[n+13],12,-4034
1101),m,f,d[n+14],17,-1502002290),i,m,d[n+15],22,1236535329),r=md5_gg(r,i=md5_gg(i,m=md5_g
g(m,f,r,i,d[n+1],5,-165796510),f,r,d[n+6],9,-1069501632),m,f,d[n+11],14,643717713),i,m,d[n+0],20,
-373897302),r=md5_gg(r,i=md5_gg(i,m=md5_gg(m,f,r,i,d[n+5],5,-701558691),f,r,d[n+10],9,380160
83),m,f,d[n+15],14,-660478335),i,m,d[n+4],20,-405537848),r=md5_gg(r,i=md5_gg(i,m=md5_gg(m,f
,r,i,d[n+9],5,568446438),f,r,d[n+14],9,-1019803690),m,f,d[n+3],14,-187363961),i,m,d[n+8],20,1163
531501),r=md5_gg(r,i=md5_gg(i,m=md5_gg(m,f,r,i,d[n+13],5,-1444681467),f,r,d[n+2],9,-51403784)
,m,f,d[n+7],14,1735328473),i,m,d[n+12],20,-1926607734),r=md5_hh(r,i=md5_hh(i,m=md5_hh(m,f,r,
i,d[n+5],4,-378558),f,r,d[n+8],11,-2022574463),m,f,d[n+11],16,1839030562),i,m,d[n+14],23,-35309
556),r=md5_hh(r,i=md5_hh(i,m=md5_hh(m,f,r,i,d[n+1],4,-1530992060),f,r,d[n+4],11,1272893353),
m,f,d[n+7],16,-155497632),i,m,d[n+10],23,-1094730640),r=md5_hh(r,i=md5_hh(i,m=md5_hh(m,f,r,i,
d[n+13],4,681279174),f,r,d[n+0],11,-358537222),m,f,d[n+3],16,-722521979),i,m,d[n+6],23,7602918
9),r=md5_hh(r,i=md5_hh(i,m=md5_hh(m,f,r,i,d[n+9],4,-640364487),f,r,d[n+12],11,-421815835),m,f,
d[n+15],16,530742520),i,m,d[n+2],23,-995338651),r=md5_ii(r,i=md5_ii(i,m=md5_ii(m,f,r,i,d[n+0],6,
-198630844),f,r,d[n+7],10,1126891415),m,f,d[n+14],15,-1416354905),i,m,d[n+5],21,-57434055),r=
md5_ii(r,i=md5_ii(i,m=md5_ii(m,f,r,i,d[n+12],6,1700485571),f,r,d[n+3],10,-1894986606),m,f,d[n+10]
,15,-1051523),i,m,d[n+1],21,-2054922799),r=md5_ii(r,i=md5_ii(i,m=md5_ii(m,f,r,i,d[n+8],6,1873313
359),f,r,d[n+15],10,-30611744),m,f,d[n+6],15,-1560198380),i,m,d[n+13],21,1309151649),r=md5_ii(r
,i=md5_ii(i,m=md5_ii(m,f,r,i,d[n+4],6,-145523070),f,r,d[n+11],10,-1120210379),m,f,d[n+2],15,71878
7259),i,m,d[n+9],21,-343485551),m=safe_add(m,h),f=safe_add(f,t),r=safe_add(r,g),i=safe_add(i,e)}r
eturn Array(m,f,r,i)}function md5_cmn(d,_,m,f,r,i){return
safe_add(bit_rol(safe_add(safe_add(_,d),safe_add(f,i)),r),m)}function md5_ff(d,_,m,f,r,i,n){return
md5_cmn(_&m|~_&f,d,_,r,i,n)}function md5_gg(d,_,m,f,r,i,n){return
md5_cmn(_&f|m&~f,d,_,r,i,n)}function md5_hh(d,_,m,f,r,i,n){return
md5_cmn(_^m^f,d,_,r,i,n)}function md5_ii(d,_,m,f,r,i,n){return md5_cmn(m^(_|~f),d,_,r,i,n)}function
safe_add(d,_){var m=(65535&d)+(65535&_);return(d»16)+(_»16)+(m»16)«16|65535&m}function
bit_rol(d,_){return d«_|d»>32-_}

(function(){

```
  btn2.onclick = function(){
      var st11zero = '00:00:00:00:00:00:00:00:00:00:00:00';
      var idorange = '01'; // variable
      var idsalt= '3c'; // 16
      var idhash  = '03'; //1+16
      var fixed = '1a:09:00:00:05:58:01:03:41';
            function TLofTLS(id,l) {
          var toAdd = l.toString(16).toUpperCase();
          if (toAdd.length<2) toAdd = '0' + toAdd;
          return id + ':' + toAdd;
            }
      function SofTLS (s) {
        var i, toAdd;
        var res = '';
        for(i = 0; i < s.length; i++) {
            toAdd = s.charCodeAt(i).toString(16).toUpperCase();
            if (toAdd.length<2) toAdd = '0' + toAdd;
            res += toAdd;
            if (i<s.length-1) res += ":";
        }
        return res;
```

```
      }
      var Orange = 'fti/'+orange.value;
      var Salt = salt.value;
      var Byte = byte.value;
      var md5 = MD5(Byte + password.value + Salt).toString();
      console.log(md5);
      var md5s = '';
      for(i = 0; i < md5.length; i+=2) {
        md5s += md5[i]+md5[i+1];
        if (i<md5.length-2) md5s += ":";
            }
      console.log(md5s);
      output.value =
            st11zero + ':' + fixed + ':' +
            TLofTLS(idorange,2+Orange.length)+ ':' + SofTLS(Orange)+ ':' +
            TLofTLS(idsalt,2+16)+ ':' + SofTLS(Salt) + ':' +
            TLofTLS(idhash,2+1+16)+ ':' + SofTLS(Byte) + ':' + md5s;
       }
```

})();

```
  }
```

</script>

</head> <body>

```
<h3>Générateur pour option 90 DHCP Orange - version 2.01 (septembre
2018)</h3>
```

Rédigé par kgersen via ce topic lafibre.info
 <hr> login Orange : fti/<input id="orange" placeholder="identifiant Orange"/>
 mot de passe Orange: <input id="password" placeholder="password"/>
 RND Salt: <input id="salt" placeholder="16 ASCII Charts"/ maxlength="16" size="16">
 RND Bytes: <input id="byte" placeholder="1 ASCII Charts" maxlength="1" size="12"/>
(execution locale au navigateur, les valeurs ne sont pas envoyées sur le réseau)
 <hr> <button id="btn2">Générer la chaine</button>

$Identifiant :<textarea id="output" placeholder=""></textarea>

</body> </html> Note:
La box génère a chaque requête DHCP deux valeurs aléatoire (nommé "RND Salt" et "RND Bytes" dans ce tuto), ce qui veux dire que le rejeu est possible.

Étape 4

Nous allons configurer les DHCP.

Pour cela, voici la configuration standard :

General Configuration

Enable: ☑ Enable interface

Description: WAN
Enter a description (name) for the interface here.

IPv4 Configuration Type: DHCP

IPv6 Configuration Type: DHCP6

MAC Address: xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

DHCP Client Configuration

Options: ☑ Advanced Configuration — Use advanced DHCP configuration options. ☐ Configuration Override — Override the configuration from this file.

Hostname:
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

Alias IPv4 address: / 32
The value in this field is used as a fixed alias IPv4 address by the DHCP client.

Reject leases from:
To have the DHCP client reject offers from specific DHCP servers, enter their IP addresses here (separate multiple entries with a comma). This is useful for rejecting leases from cable modems that offer private IP addresses when they lose upstream sync.

Protocol timing: Timeout | Retry | Select timeout | Reboot | Backoff cutoff | Initial interval

Presets: ○ FreeBSD default ○ Clear ○ pfSense Default ◉ Saved Cfg
The values in these fields are DHCP protocol timings used when requesting a lease.
See here for more information

Lease Requirements and Requests

Send options: dhcp-class-identifier "sagem",user-class "+FSVDSL_livebox.Internet.softathome.Livebox4",rfc3118-auth 00:00:00:00:00:00:00:00:00:00
The values in this field are DHCP options to be sent when requesting a DHCP lease. [option declaration [, ...]]
Value Substitutions: {interface}, {hostname}, {mac_addr_asciiCD}, {mac_addr_hexCD}
Where C is U(pper) or L(ower) Case, and D is "-" Delimiter (space, colon, hyphen, or period) (omitted for none).
Some ISPs may require certain options be or not be sent.

Request options: subnet-mask,broadcast-address,dhcp-lease-time,dhcp-renewal-time,dhcp-rebinding-time,domain-search,routers,domain-name-servers
The values in this field are DHCP option 55 to be sent when requesting a DHCP lease. [option [, ...]]
Some ISPs may require certain options be or not be requested.

Require options:
The values in this field are DHCP options required by the client when requesting a DHCP lease. [option [, ...]]

Option modifiers: vlan-pcp 6
The values in this field are DHCP option modifiers applied to the obtained DHCP lease. [modifier option declaration [, ...]]
modifiers: (default, supersede, prepend, append)
See here more information

DHCP6 Client Configuration

Options: ☑ Advanced Configuration — Use advanced DHCPv6 configuration options. ☐ Configuration Override — Override the configuration from this file.

Use IPv4 connectivity as parent interface: ☐ Request a IPv6 prefix/information through the IPv4 connectivity link

Request only an IPv6 prefix: ☐ Only request an IPv6 prefix, do not request an IPv6 address

DHCPv6 Prefix Delegation size: None
The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.

Send IPv6 prefix hint: ☐ Send an IPv6 prefix hint to indicate the desired prefix size for delegation

Debug: ☐ Start DHCP6 client in debug mode

Do not wait for a RA: ☑ Required by some ISPs, especially those not using PPPoE

Do not allow PD/Address release: ☐ dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent

DHCP6 VLAN Priority: ☐ Enable dhcp6c VLAN Priority tagging — Normally off unless specifically required by the ISP. Background (BK, 0) — Choose 802.1p priority to set.

Advanced DHCP6 Client Configuration

Information only: ☐ Exchange Information Only
Only exchange informational configuration parameters with servers.

Send options: ia-pd 0, raw-option 15 00:2b:46:53:56:44:53:4c:5f:6c:69:76:65:62:6f:78:2e:49:6e:74:65:72:6e:65:74:2e:73:6f:66:74:61:74:68:6f:6d:65:2e
DHCP send options to be sent when requesting a DHCP lease. [option declaration [, ...]]
Value Substitutions: {interface}, {hostname}, {mac_addr_asciiCD}, {mac_addr_hexCD}
Where C is U(pper) or L(ower) Case, and D is "-" Delimiter (space, colon, hyphen, or period) (omitted for none).
Some DHCP services may require certain options be or not be sent.

Request Options:
DHCP request options to be sent when requesting a DHCP lease. [option [, ...]]
Some DHCP services may require certain options be or not be requested.

Scripts:
Absolute path to a script invoked on certain conditions including when a reply message is received.
[/[dirname/[.../]]filename[.ext]].

Identity Association Statement: ☐ Non-Temporary Address Allocation — id-assoc na ID | IPv6 address | pltime | vltime
☑ Prefix Delegation — id-assoc pd ID: 0 | IPv6 prefix | pltime | vltime

Prefix interface statement: Prefix Interface sla-id: 0 — sla-len: 8

Prefix Interface: LAN
Select the interface on which to apply the prefix delegation.

Authentication statement: Authname | Protocol | Algorithm | RDM

Keyinfo statement: Keyname | Realm
KeyID | Secret | Expire
See here more information

Reserved Networks

Block private networks and loopback addresses: ☑
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks: ☑
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Avec dans le **Send Options** IPv4 :

```
dhcp-class-identifier "sagem",user-class
"+FSVDSL_livebox.Internet.softathome.Livebox4",option-90 $Identifiant
```

dans le **Request Options** IPv4 :

```
subnet-mask,broadcast-address,dhcp-lease-time,dhcp-renewal-time,dhcp-
rebinding-time,domain-search,routers,domain-name-servers,option-90
```

et dans le **Send Options** IPv6 :

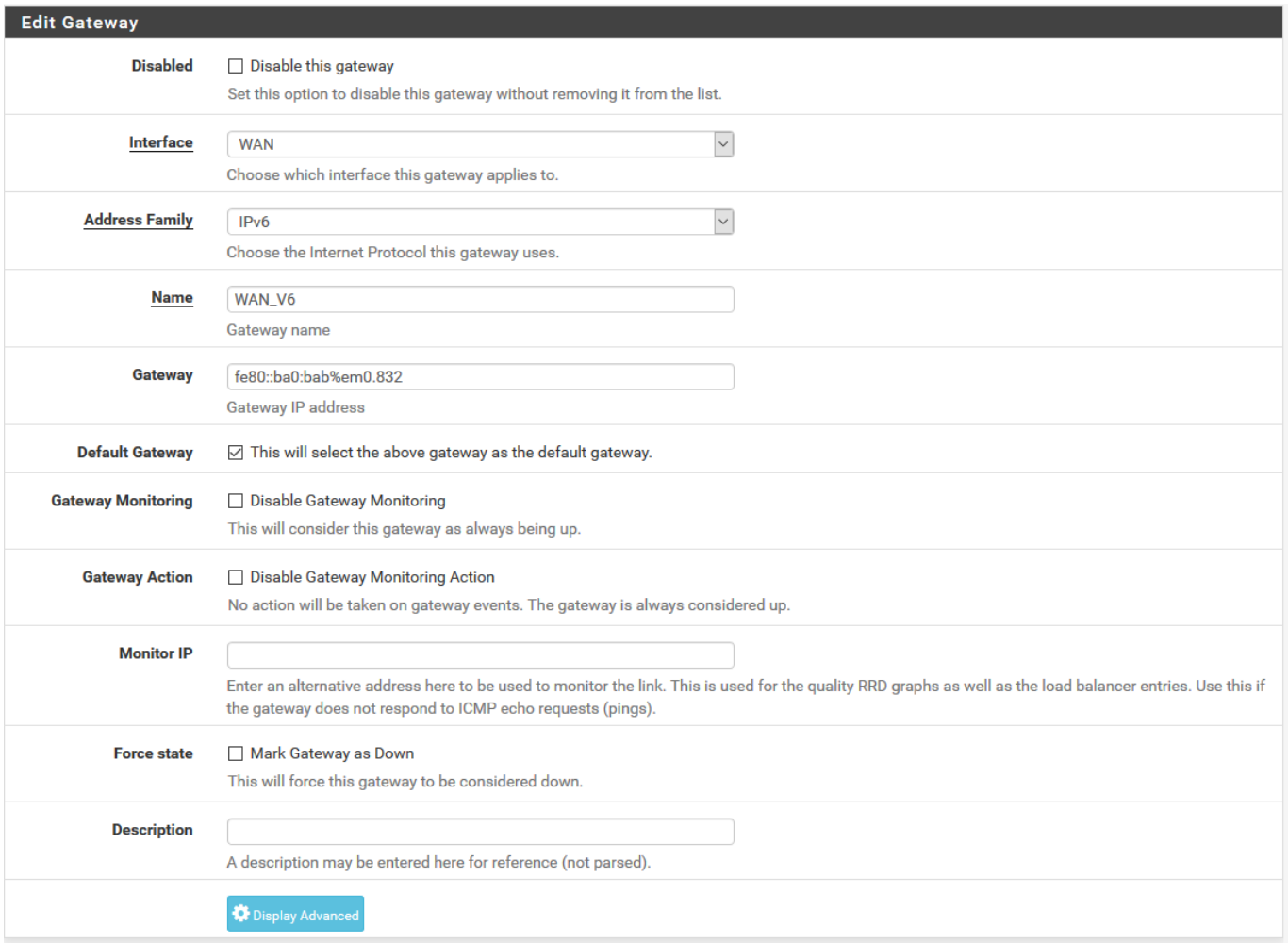
```
ia-pd 0, raw-option 15
00:2b:46:53:56:44:53:4c:5f:6c:69:76:65:62:6f:78:2e:49:6e:74:65:72:6e:65:74:2
e:73:6f:66:74:61:74:68:6f:6d:65:2e:6c:69:76:65:62:6f:78:33,raw-option 16
00:00:04:0e:00:05:73:61:67:65:6d,raw-option 6 00:0b:00:11:00:17:00:18,raw-
option 11 $Identifiant
```

Oubliez pas de remplacer la valeur “$Identifiant” de l'option 90 en IPv4 et de l'option 11 en IPv6 par celle généré a l'étape 3

Vous devriez recevoir une IPv4 et un /56 IPv6.

Étape 5

Il faudra ajouter la route suivante pour pouvoir profiter de l'IPv6 :



A noter qu'il faudra changer le nom de l'interface par la votre.

Étape 6

Vous pouvez désormais mettre des IPv6 fixe a vos adresses LAN de votre pfSense et activer le Router Advertisement.

Vous avez la complète liberté sur vos préfixes.

Télévision

Étape 1

Génération de l'identifiant :

Étape 2

Il vous faut créer les deux interfaces VLAN 838 et 840

Étape 3

Ajout du DHCP sur l'interface vlan 838 comme ceci :

Picture

avec pour options :

Fix Me!

Étape 4

Création des règles de pare-feu

Fix Me!

Étape 5

Création de bail statique pour le décodeur

Fix Me!