pfSense - Bug #3484

IPv6 - the gateway address does not lie within one of the chosen interface's subnets

02/24/2014 04:06 PM - Doktor Notor

Status:	Resolved	**Start date:**	02/24/2014
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2.1.1		
Affected Version:	2.1-IPv6	**Affected Architecture:**	

Description

```
2.1.1-PRERELEASE (i386)
built on Sat Feb 22 04:06:07 EST 2014
FreeBSD 8.3-RELEASE-p14
```

I am merely trying to change a **description** of a GW which is perfectly working and has been added about a week ago. The GW IP is 2001:470:xxxx:xx::1 and the interface (IPv6 tunnel) subnet is 2001:470:xxxx:xx::2/64 - cannot really see how's this **not** within the subnet. (P.S. The case is the same in both IPs, the only difference being ::1 vs ::2, so - not in any way related to the case-sensitive link-local stuff bug.)

Associated revisions

Revision 1de88429 - 02/28/2014 06:13 AM - Ermal Luçi

Ticket #3484 Note that for now prefixlen is useless in ipv6 tunnels. IPv4 accepts them

Revision ddb30ebf - 02/28/2014 07:38 AM - Ermal Luçi

Fixes #3484. Provide a dynamic gateway for gif v6 tunnels so it can be used on firewall rules etc. The guide for setting up this tunnels on docs need to change to leave the gif interface as none type. People upgrading need to fix this themselves with a not on release notes. This can be fixed if the kernel condition is relaxed to allow setting the prefixlen on the tunnel as ipv4

Revision c32a6b82 - 02/28/2014 07:49 AM - Ermal Luçi

Fixes #3484. Provide a dynamic gateway for gif v6 tunnels so it can be used on firewall rules etc. The guide for setting up this tunnels on docs need to change to leave the gif interface as none type. People upgrading need to fix this themselves with a not on release notes. This can be fixed if the kernel condition is relaxed to allow setting the prefixlen on the tunnel as ipv4

Revision d2c59808 - 02/28/2014 07:52 AM - Ermal Luçi

Ticket #3484 Note that for now prefixlen is useless in ipv6 tunnels. IPv4 accepts them

Revision cdeaf91e - 02/28/2014 08:11 AM - Ermal Luçi

Ticket #3484 Correct the case for GRE tunnels as well since they behave the same. GRE seems to need the prefixlen 128 specified all the time so do it explicitly to be on safe side

Revision 9cca1a4f - 02/28/2014 08:13 AM - Ermal Luçi

Ticket #3484 Correct the case for GRE tunnels as well since they behave the same. GRE seems to need the prefixlen 128 specified all the time so do it explicitly to be on safe side

History

#1 - 02/24/2014 04:16 PM - Doktor Notor

Afraid it's trying to compare the subnet to the "gif remote address" which is obviously IPv4. No wonder it fails. As said above, this used to work just a week ago, perfectly fine.

#2 - 02/28/2014 06:06 AM - Ermal Luçi

After investigation this seems to be an problem of INET6 implementation of FreeBSD.

It does not allow on gifv6 tunnels to install for point to point a mask other than 128.

Some test will be done to attempt to fix this.

The kernel check can be relaxed just need to be verified why the limitation.

#3 - 02/28/2014 07:40 AM - Ermal Luçi

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset ddb30ebfc686165e00f0155e00df16edc17c31c5.

#4 - 02/28/2014 07:50 AM - Ermal Luçi

Applied in changeset c32a6b82a708149a66c1e477ddc0ba1c54d70440.

#5 - 02/28/2014 09:20 AM - Doktor Notor

OK, thanks for investigating. Please, let me know what should be done to test the fixes, kinda confused by the comments.

#6 - 02/28/2014 10:20 AM - Ermal Luçi

Ah just gitsync to latest code and set the assigned GIF interface to none on the Interfaces configuration screen and you will have a dynamic gateway created on the gateways screen.

No need to the configuration of the gateway manually.

#7 - 02/28/2014 11:23 AM - Doktor Notor

This totally messed up my IPv6 connectivity. Cannot even ping an IPv6 from the firewall due to some nonsense about buffer space.

```
ping6: sendmsg: No buffer space available
```

IPv6 unusable from LAN as well, even though I get IPv6 address via radvd.

#8 - 02/28/2014 11:40 AM - Doktor Notor

OK, back to static IPv6, manually created GW, everything working again. So, assigned GIF interface set to None definitely does not work at all. I also wonder, what's really the problem here, when it lets you create the gateway without any complaints, and then all of a sudden decides that it's outside

of subnet when trying to change the description.

#9 - 03/03/2014 10:38 AM - Renato Botelho

I pushed more fixes today, please try tomorrow's snapshot or gitsync it to latest RELENG_2_1 and let me know the results. It's working fine on my test environment with interface IPv6 set to none and automatic created routing.

#10 - 03/05/2014 02:38 AM - Doktor Notor

Sorry, this does not work. GW autoconfigured, shows up (required a reboot to even get that far), the assigned tunnel interface shows up as well with proper IP, yet there absolutely no IPv6 connectivity, neither from the FW box, nor from LAN clients. (The WAN is PPPoE, in case it could be relevant.)

#11 - 03/05/2014 02:44 AM - Doktor Notor

And indeed, when I look at the routes, with the dynamic GW, it shows just complete nonsense.

Dynamic, non-working GW:

```
Destination                       Gateway                       Flags      Netif Expire
default                           fe80::230:88ff:fe04:9597%pppoe0 UGS      pppoe0
```

Manually created, working GW:

```
Destination                       Gateway                       Flags      Netif Expire
default                           2001:470:xx:yy::1             UGS        gif0
```

#12 - 03/05/2014 05:50 AM - Renato Botelho

Could you show your config.xml (without sensitive data)?

#13 - 03/05/2014 06:07 AM - Doktor Notor

The working one, or the broken one?

#14 - 03/05/2014 07:33 AM - Renato Botelho

Doktor Notor wrote:

> The working one, or the broken one?

broken one

#15 - 03/05/2014 09:15 AM - Doktor Notor

OK, tried to nuke most of the irrelevant/sensitive info.

```
<?xml version="1.0"?>
<pfsense>
    <version>10.1</version>
    <lastchange/>
    <theme>pfsense_ng</theme>
    <sysctl>
        <item>
            <descr><![CDATA[Enable mounting the FS read only with more checks.]]></descr>
            <tunable>vfs.forcesync</tunable>
            <value>default</value>
        </item>
        <item>
            <tunable>debug.pfftpproxy</tunable>
            <value>default</value>
            <descr><![CDATA[Disable the pf ftp proxy handler.]]></descr>
        </item>
        <item>
            <descr><![CDATA[Increase UFS read-ahead speeds to match current state of hard drives and NCQ.]]></
descr>
            <tunable>vfs.read_max</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Set the ephemeral port range to be lower.]]></descr>
            <tunable>net.inet.ip.portrange.first</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Drop packets to closed TCP ports without returning a RST]]></descr>
            <tunable>net.inet.tcp.blackhole</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Do not send ICMP port unreachable messages for closed UDP ports]]></descr>
            <tunable>net.inet.udp.blackhole</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Randomize the ID field in IP packets (default is 0: sequential IP IDs)]]></descr>
            <tunable>net.inet.ip.random_id</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Drop SYN-FIN packets (breaks RFC1379, but nobody uses it anyway)]]></descr>
            <tunable>net.inet.tcp.drop_synfin</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Enable sending IPv4 redirects]]></descr>
            <tunable>net.inet.ip.redirect</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Enable sending IPv6 redirects]]></descr>
            <tunable>net.inet6.ip6.redirect</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Enable privacy settings for IPv6 (RFC 4941)]]></descr>
            <tunable>net.inet6.ip6.use_tempaddr</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Prefer privacy addresses and use them over the normal addresses]]></descr>
            <tunable>net.inet6.ip6.prefer_tempaddr</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Generate SYN cookies for outbound SYN-ACK packets]]></descr>
            <tunable>net.inet.tcp.syncookies</tunable>
            <value>default</value>
```

```
        </item>
        <item>
            <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (receive)]]></descr>
            <tunable>net.inet.tcp.recvspace</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (send)]]></descr>
            <tunable>net.inet.tcp.sendspace</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[IP Fastforwarding]]></descr>
            <tunable>net.inet.ip.fastforwarding</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Do not delay ACK to try and piggyback it onto a data packet]]></descr>
            <tunable>net.inet.tcp.delayed_ack</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Maximum outgoing UDP datagram size]]></descr>
            <tunable>net.inet.udp.maxdgram</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Handling of non-IP packets which are not passed to pfil (see if_bridge(4))]]></des
cr>
            <tunable>net.link.bridge.pfil_onlyip</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Set to 0 to disable filtering on the incoming and outgoing member interfaces.]]></
descr>
            <tunable>net.link.bridge.pfil_member</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Set to 1 to enable filtering on the bridge interface]]></descr>
            <tunable>net.link.bridge.pfil_bridge</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Allow unprivileged access to tap(4) device nodes]]></descr>
            <tunable>net.link.tap.user_open</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Randomize PID's (see src/sys/kern/kern_fork.c: sysctl_kern_randompid())]]></descr>
            <tunable>kern.randompid</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Maximum size of the IP input queue]]></descr>
            <tunable>net.inet.ip.intr_queue_maxlen</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Disable CTRL+ALT+Delete reboot from keyboard.]]></descr>
            <tunable>hw.syscons.kbd_reboot</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Enable TCP Inflight mode]]></descr>
            <tunable>net.inet.tcp.inflight.enable</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Enable TCP extended debugging]]></descr>
            <tunable>net.inet.tcp.log_debug</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Set ICMP Limits]]></descr>
```

```
            <tunable>net.inet.icmp.icmplim</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[TCP Offload Engine]]></descr>
            <tunable>net.inet.tcp.tso</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[UDP Checksums]]></descr>
            <tunable>net.inet.udp.checksum</tunable>
            <value>default</value>
        </item>
        <item>
            <descr><![CDATA[Maximum socket buffer size]]></descr>
            <tunable>kern.ipc.maxsockbuf</tunable>
            <value>default</value>
        </item>
    </sysctl>
    <system>
        <optimization>normal</optimization>
        <hostname>gw</hostname>
        <domain>testdomain.local</domain>
        <timezone>Europe/Prague</timezone>
        <time-update-interval/>
        <timeservers>192.168.0.151</timeservers>
        <webgui>
            <protocol>https</protocol>
            <ssl-certref>5228d97bef5af</ssl-certref>
            <port/>
            <max_procs>2</max_procs>
            <disablehttpredirect/>
            <nodnsrebindcheck/>
            <beast_protection/>
            <noautocomplete/>
            <authmode>Active Directory</authmode>
            <backend/>
            <althostnames></althostnames>
        </webgui>
        <disablesegmentationoffloading/>
        <disablelargereceiveoffloading/>
        <ipv6allow/>
        <powerd_ac_mode>hadp</powerd_ac_mode>
        <powerd_battery_mode>hadp</powerd_battery_mode>
        <bogons>
            <interval>daily</interval>
        </bogons>
        <ssh>
            <sshdkeyonly>enabled</sshdkeyonly>
        </ssh>
        <enableserial/>
        <serialspeed>115200</serialspeed>
        <enablesshd>enabled</enablesshd>
        <sshdkeyonly/>
        <maximumstates/>
        <aliasesresolveinterval/>
        <maximumtables/>
        <maximumtableentries>500000</maximumtableentries>
        <enablenatreflectionpurenat>yes</enablenatreflectionpurenat>
        <enablebinatreflection>yes</enablebinatreflection>
        <enablenatreflectionhelper>yes</enablenatreflectionhelper>
        <reflectiontimeout/>
        <gitsync>
            <repositoryurl>git://github.com/pfsense/pfsense.git</repositoryurl>
            <branch>RELENG_2_1</branch>
            <synconupgrade/>
        </gitsync>
        <language>en_US</language>
        <dns1gw>none</dns1gw>
        <dns2gw>none</dns2gw>
        <dns3gw>none</dns3gw>
        <dns4gw>none</dns4gw>
        <authserver>
        </authserver>
        <use_mfs_tmp_size/>
```

```
        <use_mfs_var_size/>
        <kill_states/>
        <dnsserver>127.0.0.1</dnsserver>
        <dnsserver>192.168.0.151</dnsserver>
        <dnsserver>192.168.0.150</dnsserver>
        <firmware>
            <allowinvalidsig/>
            <disablecheck/>
            <alturl>
                <enable/>
                <firmwareurl>http://snapshots.pfsense.org/FreeBSD_RELENG_8_3/i386/pfSense_RELENG_2_1/.updaters
/</firmwareurl>
            </alturl>
        </firmware>
        <earlyshellcmd>/usr/local/bin/php -f /usr/local/bin/apply_patches.php</earlyshellcmd>
    </system>
    <interfaces>
        <wan>
            <if>pppoe0</if>
            <descr><![CDATA[WAN]]></descr>
            <blockbogons/>
            <spoofmac/>
            <enable/>
            <ipaddr>pppoe</ipaddr>
            <blockpriv/>
        </wan>
        <lan>
            <enable/>
            <if>nfe0</if>
            <descr><![CDATA[LAN]]></descr>
            <spoofmac/>
            <ipaddr>192.168.0.254</ipaddr>
            <subnet>24</subnet>
            <ipaddrv6>2001:470:xxx:xxx:192:168::254</ipaddrv6>
            <subnetv6>64</subnetv6>
        </lan>
        <opt2>
            <descr><![CDATA[HEIPv6]]></descr>
            <if>gif0</if>
            <enable/>
            <spoofmac/>
            <mtu>1452</mtu>
            <blockbogons/>
            <blockpriv/>
        </opt2>
        <opt3>
            <descr><![CDATA[ModemAccess]]></descr>
            <if>rl0</if>
            <spoofmac/>
            <enable/>
            <ipaddr>192.168.255.254</ipaddr>
            <subnet>24</subnet>
            <gateway>ModemAccessGW</gateway>
        </opt3>
    </interfaces>
    <staticroutes/>
    <dhcpd>
        <lan>
            <range>
                <from>192.168.0.10</from>
                <to>192.168.0.245</to>
            </range>
        </lan>
    </dhcpd>
    <pptpd>
        <mode/>
        <redir/>
        <localip/>
        <remoteip/>
    </pptpd>
    <dnsmasq>
    </dnsmasq>
    <snmpd>
    </snmpd>
    <diag>
```

```
        <ipv6nat>
            <ipaddr/>
        </ipv6nat>
    </diag>
    <bridge/>
    <syslog>
        <reverse/>
        <nentries>200</nentries>
        <filterdescriptions>1</filterdescriptions>
    </syslog>
    <nat>
        <ipsecpassthru>
            <enable/>
        </ipsecpassthru>
        <advancedoutbound/>
    </nat>
    <filter>
        <rule>
            <id/>
            <type>pass</type>
            <ipprotocol>inet46</ipprotocol>
            <tag/>
            <tagged/>
            <direction>any</direction>
            <floating>yes</floating>
            <max/>
            <max-src-nodes/>
            <max-src-conn/>
            <max-src-states/>
            <statetimeout/>
            <statetype>keep state</statetype>
            <os/>
            <protocol>icmp</protocol>
            <source>
                <any/>
            </source>
            <destination>
                <any/>
            </destination>
            <descr><![CDATA[Allow IPv4/IPv6 ICMP packets]]></descr>
        </rule>
```

```
        <rule>
            <id/>
            <type>pass</type>
            <interface>wan</interface>
            <ipprotocol>inet46</ipprotocol>
            <tag/>
            <tagged/>
            <max/>
            <max-src-nodes/>
            <max-src-conn/>
            <max-src-states/>
            <statetimeout/>
            <statetype>keep state</statetype>
            <os/>
            <protocol>tcp</protocol>
            <source>
                <address>RAS</address>
            </source>
            <destination>
                <network>wanip</network>
                <port>ManagementPorts</port>
            </destination>
            <descr><![CDATA[Allow remote firewall management]]></descr>
        </rule>
        <rule>
            <descr><![CDATA[OpenVPN testdomain OpenVPN wizard]]></descr>
            <direction>in</direction>
            <source>
                <any/>
            </source>
            <destination>
                <network>wanip</network>
                <port>1194</port>
```

```
            </destination>
            <interface>wan</interface>
            <protocol>udp</protocol>
            <type>pass</type>
            <enabled>on</enabled>
        </rule>
        <rule>
            <type>pass</type>
            <ipprotocol>inet</ipprotocol>
            <descr><![CDATA[Default allow LAN to any rule]]></descr>
            <interface>lan</interface>
            <source>
                <network>lan</network>
            </source>
            <destination>
                <any/>
            </destination>
        </rule>
        <rule>
            <type>pass</type>
            <ipprotocol>inet6</ipprotocol>
            <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
            <interface>lan</interface>
            <source>
                <network>lan</network>
            </source>
            <destination>
                <any/>
            </destination>
        </rule>
        <rule>
            <id/>
            <type>pass</type>
            <interface>enc0</interface>
            <ipprotocol>inet</ipprotocol>
            <tag/>
            <tagged/>
            <max/>
            <max-src-nodes/>
            <max-src-conn/>
            <max-src-states/>
            <statetimeout/>
            <statetype>keep state</statetype>
            <os/>
            <source>
                <any/>
            </source>
            <destination>
                <any/>
            </destination>
            <descr><![CDATA[Allow IPSec IPv4 to any rule]]></descr>
        </rule>
        <rule>
            <id/>
            <type>pass</type>
            <interface>enc0</interface>
            <ipprotocol>inet6</ipprotocol>
            <tag/>
            <tagged/>
            <max/>
            <max-src-nodes/>
            <max-src-conn/>
            <max-src-states/>
            <statetimeout/>
            <statetype>keep state</statetype>
            <os/>
            <source>
                <any/>
            </source>
            <destination>
                <any/>
            </destination>
            <descr><![CDATA[Allow IPSec IPv6 to any rule]]></descr>
        </rule>
        <rule>
```

```
            <descr><![CDATA[OpenVPN testdomain OpenVPN wizard]]></descr>
            <source>
                <any/>
            </source>
            <destination>
                <any/>
            </destination>
            <interface>openvpn</interface>
            <type>pass</type>
            <enabled>on</enabled>
        </rule>
        <rule>
            <id/>
            <type>pass</type>
            <interface>openvpn</interface>
            <ipprotocol>inet6</ipprotocol>
            <tag/>
            <tagged/>
            <max/>
            <max-src-nodes/>
            <max-src-conn/>
            <max-src-states/>
            <statetimeout/>
            <statetype>keep state</statetype>
            <os/>
            <source>
                <any/>
            </source>
            <destination>
                <any/>
            </destination>
            <descr><![CDATA[Allow OpenVPN IPv6 to any rule]]></descr>
        </rule>
        <rule>
            <id/>
            <type>pass</type>
            <interface>opt2</interface>
            <ipprotocol>inet46</ipprotocol>
            <tag/>
            <tagged/>
            <max/>
            <max-src-nodes/>
            <max-src-conn/>
            <max-src-states/>
            <statetimeout/>
            <statetype>keep state</statetype>
            <os/>
            <protocol>tcp</protocol>
            <source>
                <address>RAS</address>
            </source>
            <destination>
                <network>opt2ip</network>
                <port>ManagementPorts</port>
            </destination>
            <descr><![CDATA[Allow remote firewall management]]></descr>
        </rule>
        <rule>
            <id/>
            <type>pass</type>
            <interface>opt2</interface>
            <ipprotocol>inet6</ipprotocol>
            <tag/>
            <tagged/>
            <max/>
            <max-src-nodes/>
            <max-src-conn/>
            <max-src-states/>
            <statetimeout/>
            <statetype>keep state</statetype>
            <os/>
            <protocol>udp</protocol>
            <source>
                <any/>
            </source>
```

```
            <destination>
                <network>opt2ip</network>
                <port>1194</port>
            </destination>
            <descr><![CDATA[OpenVPN testdomain]]></descr>
        </rule>
    </filter>
    <shaper>
    </shaper>
    <ipsec>
        <phase1>
            <ikeid>1</ikeid>
            <interface>wan</interface>
            <remote-gateway>188.xx.xx.xx</remote-gateway>
            <mode>main</mode>
            <protocol>inet</protocol>
            <myid_type>asn1dn</myid_type>
            <myid_data/>
            <peerid_type>asn1dn</peerid_type>
            <peerid_data/>
            <encryption-algorithm>
                <name>aes</name>
                <keylen>128</keylen>
            </encryption-algorithm>
            <hash-algorithm>sha1</hash-algorithm>
            <dhgroup>2</dhgroup>
            <lifetime>28800</lifetime>
            <pre-shared-key/>
            <private-key/>
            <certref>52297a823fe8a</certref>
            <caref>522978178c796</caref>
            <authentication_method>rsasig</authentication_method>
            <generate_policy/>
            <proposal_check>strict</proposal_check>
            <nat_traversal>on</nat_traversal>
            <dpd_delay>10</dpd_delay>
            <dpd_maxfail>5</dpd_maxfail>
        </phase1>
        <phase1>
            <ikeid>2</ikeid>
            <interface>wan</interface>
            <mobile/>
            <mode>aggressive</mode>
            <protocol>inet</protocol>
            <myid_type>myaddress</myid_type>
            <myid_data/>
            <peerid_type>user_fqdn</peerid_type>
            <peerid_data>vpnusers@testdomain.local</peerid_data>
            <encryption-algorithm>
                <name>aes</name>
                <keylen>128</keylen>
            </encryption-algorithm>
            <hash-algorithm>sha1</hash-algorithm>
            <dhgroup>2</dhgroup>
            <lifetime>86400</lifetime>
            <pre-shared-key><prefixrange>
                <from/>
                <to/>
                <prefixlength>64</prefixlength>
            </prefixrange>
            <defaultleasetime/>
            <maxleasetime/>
            <netmask/>
            <domain/>
            <domainsearchlist/>
            <ddnsdomain/>
            <tftp/>
            <ldap/>
            <nextserver/>
            <filename/>
            <rootpath/>
            <dhcpv6leaseinlocaltime>yes</dhcpv6leaseinlocaltime>
            <numberoptions/>
            <radnsserver>2001:470:xx:xx::151</radnsserver>
            <radnsserver>2001:470:xx:xx::150</radnsserver>
```

```
        </lan>
    </dhcpdv6>
    <ppps>
        <ppp>
            <ptpid>0</ptpid>
            <type>pppoe</type>
            <if>pppoe0</if>
            <ports>xl0</ports>
            <username></username>
            <password></password>
            <provider/>
        </ppp>
    </ppps>
    <gifs>
        <gif>
            <ipaddr/>
            <if>wan</if>
            <tunnel-local-addr>2001:470:xx:xx::2</tunnel-local-addr>
            <tunnel-remote-addr>2001:470:xx:xx::1</tunnel-remote-addr>
            <tunnel-remote-net>64</tunnel-remote-net>
            <remote-addr>216.66.86.122</remote-addr>
            <descr><![CDATA[HE IPv6 Tunnel]]></descr>
            <gifif>gif0</gifif>
        </gif>
    </gifs>
    <gateways>
        <gateway_item>
            <interface>opt3</interface>
            <gateway>192.168.255.1</gateway>
            <name>ModemAccessGW</name>
            <weight>1</weight>
            <ipprotocol>inet</ipprotocol>
            <interval/>
            <descr><![CDATA[VDSL Modem Access]]></descr>
        </gateway_item>
    </gateways>
    <ntpd>
        <interface>lan</interface>
    </ntpd>
    <ezshaper>
    </ezshaper>
    <dhcrelay>
    </dhcrelay>
    <dhcrelay6>
    </dhcrelay6>
    <dyndnses>
    </dyndnses>
    <ovpnserver>
        <step10>
            <interface>wan</interface>
            <protocol>UDP</protocol>
            <localport>1194</localport>
            <descr><![CDATA[testdomain OpenVPN]]></descr>
            <tlsauth>on</tlsauth>
            <gentlskey>on</gentlskey>
            <dhkey>2048</dhkey>
            <crypto>AES-256-CBC</crypto>
            <engine>none</engine>
            <tunnelnet>10.20.30.0/24</tunnelnet>
            <localnet>192.168.0.0/24</localnet>
            <concurrentcon>5</concurrentcon>
            <compression>on</compression>
            <dynip>on</dynip>
            <addrpool>on</addrpool>
            <dns1>192.168.0.150</dns1>
            <dns2>192.168.0.151</dns2>
            <ntp1>192.168.0.151</ntp1>
            <nbttype>0</nbttype>
        </step10>
        <step11>
            <ovpnrule>on</ovpnrule>
            <ovpnallow>on</ovpnallow>
        </step11>
    </ovpnserver>
</pfsense>
```

```
</pre>
            <private-key/>
            <certref/>
            <caref/>
            <authentication_method>xauth_psk_server</authentication_method>
            <generate_policy>unique</generate_policy>
            <proposal_check>strict</proposal_check>
            <nat_traversal>force</nat_traversal>
            <dpd_delay>60</dpd_delay>
            <dpd_maxfail>5</dpd_maxfail>
        </phase1>
        <client>
            <enable/>
            <user_source>Active Directory</user_source>
            <group_source>system</group_source>
            <pool_address>192.168.30.0</pool_address>
            <pool_netbits>24</pool_netbits>
            <net_list/>
            <save_passwd/>
            <dns_domain>testdomain.local</dns_domain>
            <dns_server1>192.168.0.151</dns_server1>
            <dns_server2>192.168.0.150</dns_server2>
            <dns_server3/>
            <dns_server4/>
            <wins_server1>192.168.0.151</wins_server1>
            <wins_server2/>
            <login_banner/>
        </client>
        <phase2>
            <ikeid>1</ikeid>
            <mode>tunnel</mode>
            <localid>
                <type>network</type>
                <address>192.168.0.0</address>
                <netbits>24</netbits>
            </localid>
            <remoteid>
                <type>network</type>
                <address>10.0.0.0</address>
                <netbits>24</netbits>
            </remoteid>
            <protocol>esp</protocol>
            <encryption-algorithm-option>
                <name>aes</name>
                <keylen>128</keylen>
            </encryption-algorithm-option>
            <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
            <pfsgroup>2</pfsgroup>
            <lifetime>3600</lifetime>
            <pinghost/>
        </phase2>
        <phase2>
            <ikeid>2</ikeid>
            <mode>tunnel</mode>
            <localid>
                <type>network</type>
                <address>192.168.0.0</address>
                <netbits>24</netbits>
            </localid>
            <remoteid>
                <type>mobile</type>
            </remoteid>
            <protocol>esp</protocol>
            <encryption-algorithm-option>
                <name>aes</name>
                <keylen>128</keylen>
            </encryption-algorithm-option>
            <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
            <pfsgroup>0</pfsgroup>
            <lifetime>28800</lifetime>
            <pinghost/>
            <mobile/>
        </phase2>
        <enable/>
    </ipsec>
```

```
    <aliases>
        <alias>
            <name>DNSServers</name>
            <address></address>
            <descr><![CDATA[DNS Servers]]></descr>
            <type>host</type>
        </alias>
        <alias>
            <name>ManagementPorts</name>
            <address>22 443</address>
            <descr><![CDATA[Ports used for firewall management]]></descr>
            <type>port</type>
        </alias>
        <alias>
            <name>Modem</name>
            <address>192.168.255.1</address>
            <descr><![CDATA[VDSL modem]]></descr>
            <type>host</type>
        </alias>
        <alias>
            <name>PrivateNetworks</name>
            <address>10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 127.0.0.0/8</address>
            <descr><![CDATA[RFC 1918 networks]]></descr>
            <type>network</type>
        </alias>
        <alias>
            <name>RAS</name>
            <address></address>
            <descr><![CDATA[Hosts with remote access allowed]]></descr>
            <type>network</type>
        </alias>
    </aliases>
    <proxyarp/>
    <cron>
    </cron>
    <wol>
    </wol>
    <rrd>
        <enable/>
    </rrd>
    <load_balancer>
    </load_balancer>
    <widgets>
    </widgets>
    <revision>
    </revision>
    <openvpn>
        <openvpn-server>
            <vpnid>1</vpnid>
            <mode>server_tls_user</mode>
            <authmode>Active Directory</authmode>
            <protocol>UDP</protocol>
            <dev_mode>tun</dev_mode>
            <ipaddr/>
            <interface>wan</interface>
            <local_port>1194</local_port>
            <description><![CDATA[testdomain OpenVPN]]></description>
            <custom_options/>
            <tls></tls>
            <caref>522badb76e1c4</caref>
            <crlref>522bb51a85c3c</crlref>
            <certref>522bb03963c1a</certref>
            <dh_length>2048</dh_length>
            <cert_depth>1</cert_depth>
            <strictusercn/>
            <crypto>AES-256-CBC</crypto>
            <engine>none</engine>
            <tunnel_network>10.22.33.0/24</tunnel_network>
            <tunnel_networkv6>2001:470:xxxx:xxxx::/64</tunnel_networkv6>
            <remote_network/>
            <remote_networkv6/>
            <gwredir/>
            <local_network>192.168.0.0/24</local_network>
            <local_networkv6>2001:470:xx:xx::/64</local_networkv6>
            <maxclients>5</maxclients>
```

```
            <compression>yes</compression>
            <passtos/>
            <client2client/>
            <dynamic_ip>yes</dynamic_ip>
            <pool_enable>yes</pool_enable>
            <topology_subnet>yes</topology_subnet>
            <serverbridge_dhcp/>
            <serverbridge_interface>none</serverbridge_interface>
            <serverbridge_dhcp_start/>
            <serverbridge_dhcp_end/>
            <dns_domain>testdomain.local</dns_domain>
            <dns_server1>192.168.0.151</dns_server1>
            <dns_server2>192.168.0.150</dns_server2>
            <dns_server3/>
            <dns_server4/>
            <ntp_server1>192.168.0.151</ntp_server1>
            <ntp_server2/>
            <netbios_enable/>
            <netbios_ntype>0</netbios_ntype>
            <netbios_scope/>
        </openvpn-server>
    </openvpn>
    <l7shaper>
        <container/>
    </l7shaper>
    <dnshaper/>
    <dhcpdv6>
        <lan>
            <ramode>unmanaged</ramode>
            <rapriority>medium</rapriority>
            <rainterface/>
            <range>
                <from/>
                <to/>
            </range>
```

#16 - 03/05/2014 09:22 AM - Doktor Notor

- File config.xml added

Argh, this Redmine thing really does not handle inlined code in any usable way. Attached instead.

#17 - 03/05/2014 11:38 AM - Renato Botelho

Your setup is almost the same I have here. The only difference is I forced the dynamic gif gateway to be default. Just edit the automatically created dynamic TUNNELv6 gateway, set it as default gw and save it. Could you try it please?

#18 - 03/05/2014 11:51 AM - Doktor Notor

Ah, OK. Yes, that worked.

#19 - 03/05/2014 11:55 AM - Renato Botelho

- Status changed from Feedback to Resolved

Thanks, I'll update the how to on docs.

Files

config.xml	20.6 KB	03/05/2014	Doktor Notor