OPNsense高可用测试

一、OPNsense介绍

OPNsense是一个开源，易于使用且易于构建的基于FreeBSD的防火墙和路由平台。OPNsense于2014年开始作为pfSense®和m0n0wall的分支，于2015年1月首次正式发布。

m0n0wall®项目于2015年2月15日永久终止 。其创始人Manuel Kasper鼓励所有用户使用OPNsense®。

硬件需求（版本24）

	最低配置	标准配置	推荐配置
CPU	1Ghz dual core cpu	1 GHz dual core cpu	1.5 GHz multi core cpu
内存	2 GB	4 GB	8 GB
磁盘	4 GB	40 GB	120 GB

注：

a. 最低配置中的4GB磁盘需求只能保证运行标准功能，不包括运行需要磁盘写入的功能，例如缓存代理（缓存）或入侵检测和预防（警报数据库）；
b. 标准配置能运行OPNsense的标准功能，但可能不是在大量用户或高负载的情况下。
c. 推荐配置适合绝大部分场景。

硬件与吞吐量

硬件需求	吞吐量（Mbps）	功能
最低配置	11-150	缩减功能
标准配置	151-350	全部功能
推荐配置	350-750+	全部功能

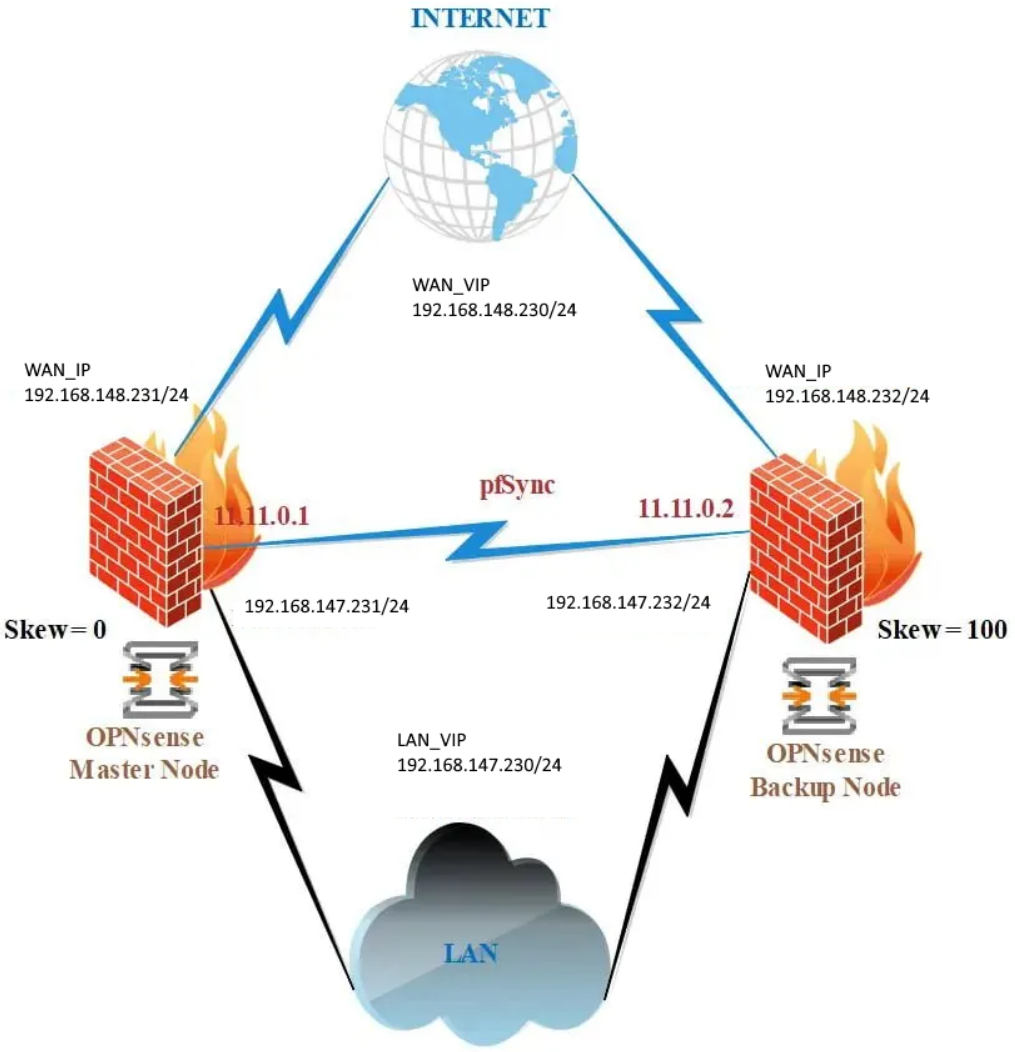
OPNsense支持的功能（版本24.7）

- 流量整形
- 基于黑名单的转发缓存代理

- VPN（包括ipsec、openvpn、wireguard）
- 高可用性和硬件故障转移（带配置同步和同步状态表）
- 入侵检测与防御
- DHCP服务器和中继
- 状态检测防火墙
- 802.1Q VLAN支持

二、测试环境

1. 测试拓扑



2. 测试环境

软件版本：24.7

	设备1	设备2

设备名	opnsense-1	opnsense-2
LAN IP	192.168.147.231/24	192.168.147.232/24
LAN_VIP	192.168.147.230/24	192.168.147.230/24
WAN IP	192.168.148.231/24	192.168.148.232/24
WAN_VIP	192.168.148.230/24	192.168.148.230/24
pfSync（同步接口）	11.11.0.1/24	11.11.0.2/24

在ESXI环境下部署需要注意以下事项：

1. 虚拟交换机存在多条上行链路且上游交换机未配置端口聚合，需要调整宿主机的高级系统参数，将Net.ReversePathFwdCheckPromisc的值置为1；
2. 必须将虚拟机的网卡设置为混杂模式（**不开混杂模式的现象是vip地址不可访问**）（ESXI上混杂模式生效范围根据分布式交换机和标准交换机有区别，标准交换机分为虚拟交换机级和端口组级，分布式交换机分为端口组级和端口级）；
3. 在修改Net.ReversePathFwdCheckPromisc前已经开启了混杂模式，必须先关闭混杂模式，再重新开启；

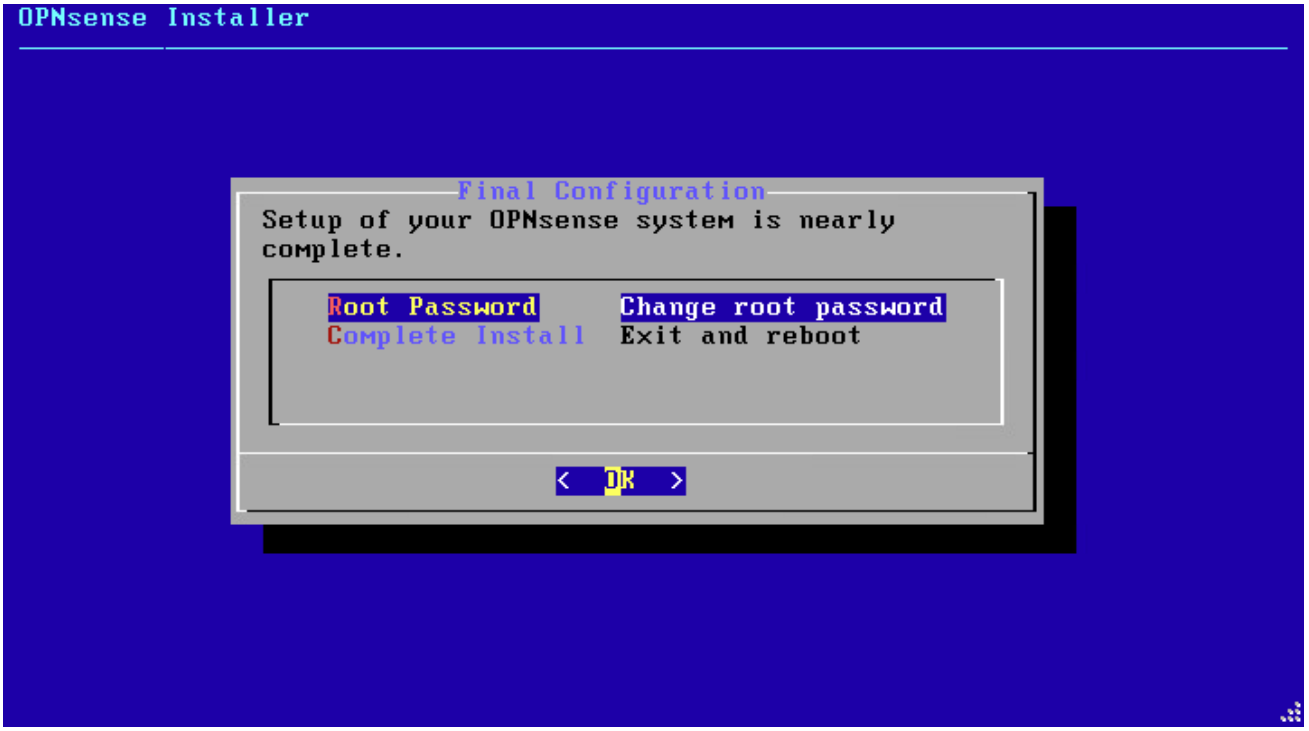
三、OPNsense安装和初始化配置

OPNsense的状态同步依赖pfSync协议，强烈建议使用专用接口在主机之间传输 pfSync 数据包，以增强安全性（防止状态注入）并提高速度。为了使状态信息准确地跨两个防火墙应用，它们必须使用相同的接口名称来访问相同的网络。举例来说，如果防火墙 1 的内部网络 (LAN) 通过 igb0 接口链接，则防火墙 2 也必须将 igb0 分配给该 LAN。

1. OPNsense安装

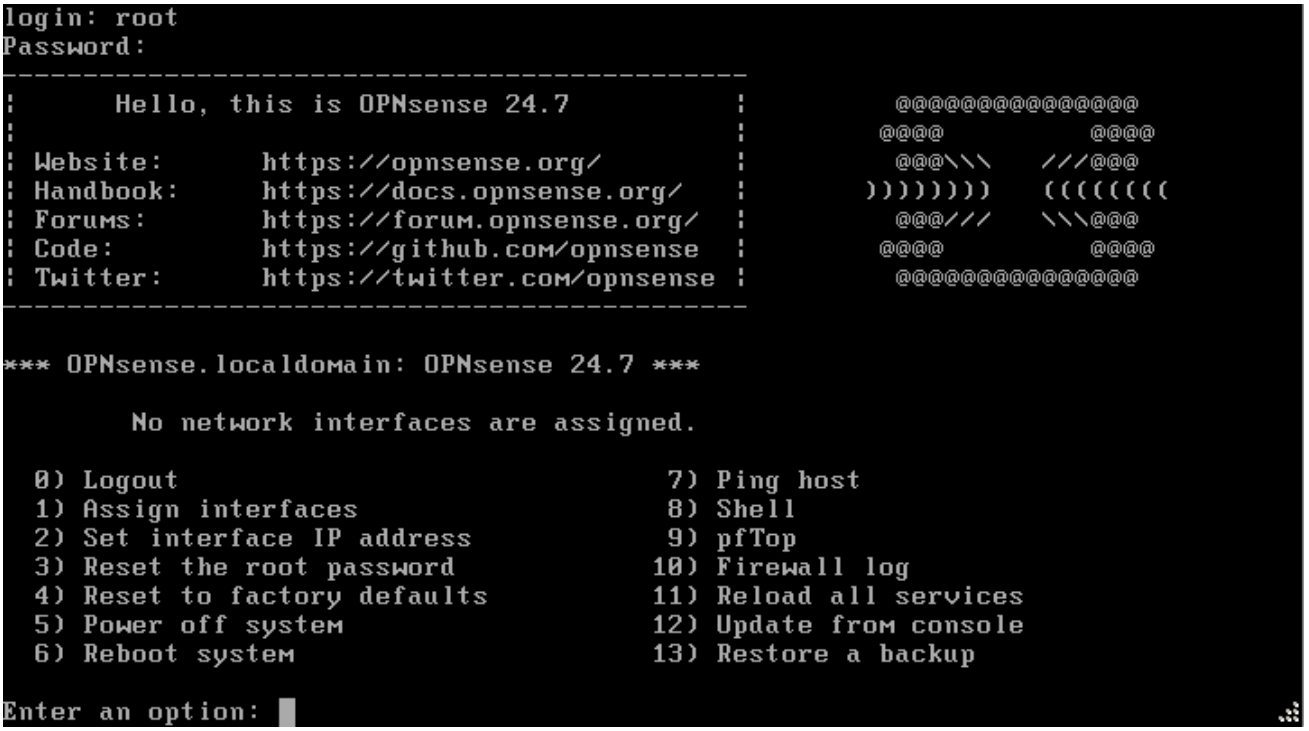
从OPNsense DVD启动时，进入的是LiveCD模式，用 root 登陆，所有的功能都支持，但所有的存储全部在RAM虚拟盘上！一旦关机或重启，全部配置丢失！如需安装，需用installer用户登录（登录密码都是opnsense）。在ESXI里安装客户机操作系统选FreeBSD12及以上版本。

安装完成的最后一步是修改root密码，如果不修改默认密码是opnsense。



2. OPNsense初始化配置

安装完成后，网卡处于默认状态（只有2个接口分别定义为LAN和WAN，其余接口均未定义，LAN设置为默认固定IP，WAN为DHCP Client），需要通过控制台进行设置。



第一步：定义接口（可选，默认网卡1为LAN，网卡2为WAN）

选择1，进入定义接口，设置是否使用端口聚合、是否使用VLAN接口，LAN、WAN接口对应的网卡，同时可以查看每个网卡对应的MAC地址。

```
  5) Power off system                  12) Update from console
  6) Reboot system                     13) Restore a backup

Enter an option: 1

Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:

vmx0            00:0c:29:a5:81:7c VMware VMXNET3 Ethernet Adapter
vmx1            00:0c:29:a5:81:86 VMware VMXNET3 Ethernet Adapter

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: vmx1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): vmx0

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):
```

第二步：设置接口IP

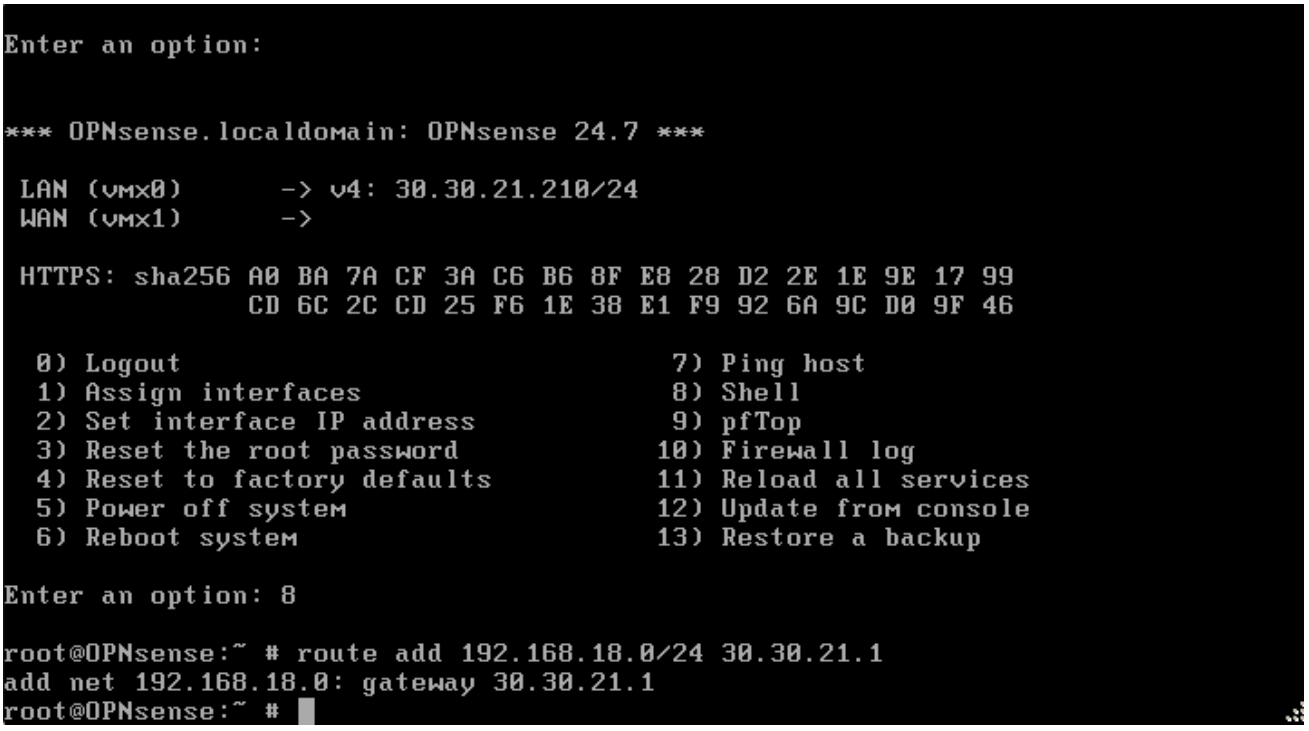
选择2，进入设置接口IP，默认状态下LAN口为静态IP，WAN口为DHCP。在这里仅需要设置LAN口IP方便web方式管理，其余的设置通过web方式进行设置更简单。

```
*** OPNsense.localdomain: OPNsense 24.7 ***

 LAN (vmx0)       -> v4: 192.168.1.1/24
 WAN (vmx1)       ->

 HTTPS: sha256 A0 BA 7A CF 3A C6 B6 8F E8 28 D2 2E 1E 9E 17 99
               CD 6C 2C CD 25 F6 1E 38 E1 F9 92 6A 9C D0 9F 46

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option: 2

Available interfaces:

1 - LAN (vmx0 - static, track6)
2 - WAN (vmx1 - dhcp, dhcp6)

Enter the number of the interface to configure:
```

第三步：设置内网路由（可选）

设置完LAN口IP后，并没有内网其他网段的路由，只有与LAN口直连的网段能够web方式访问防火墙，需要手工临时添加路由，以便通过web方式远程访问防火墙。

选择8，使用route命令添加临时路由，具体命令如下：route add <目标网络> <网关>。



添加完成后，输入exit退出shell模式。

在shell模式下设置路由在设备重启或web方式下对接口进行配置都会使手动添加的路由消失。

第四步：通过web方式完成初始化设置

1. 登录防火墙

   使用https方式访问LAN口地址，用户名/密码与控制台相同。首次登录会进入向导模式引导完成初始化设置，设置内容包括主机名、语音、时区、WAN口IP地址、LAN口IP、修改root密码等等，设置完成后将重新加载配置。

   如果是通过手动添加临时路由才能远程访问的，不建议使用向导完成初始化设置。重新加载配置会覆盖掉手动添加的临时路由，造成无法远程访问。

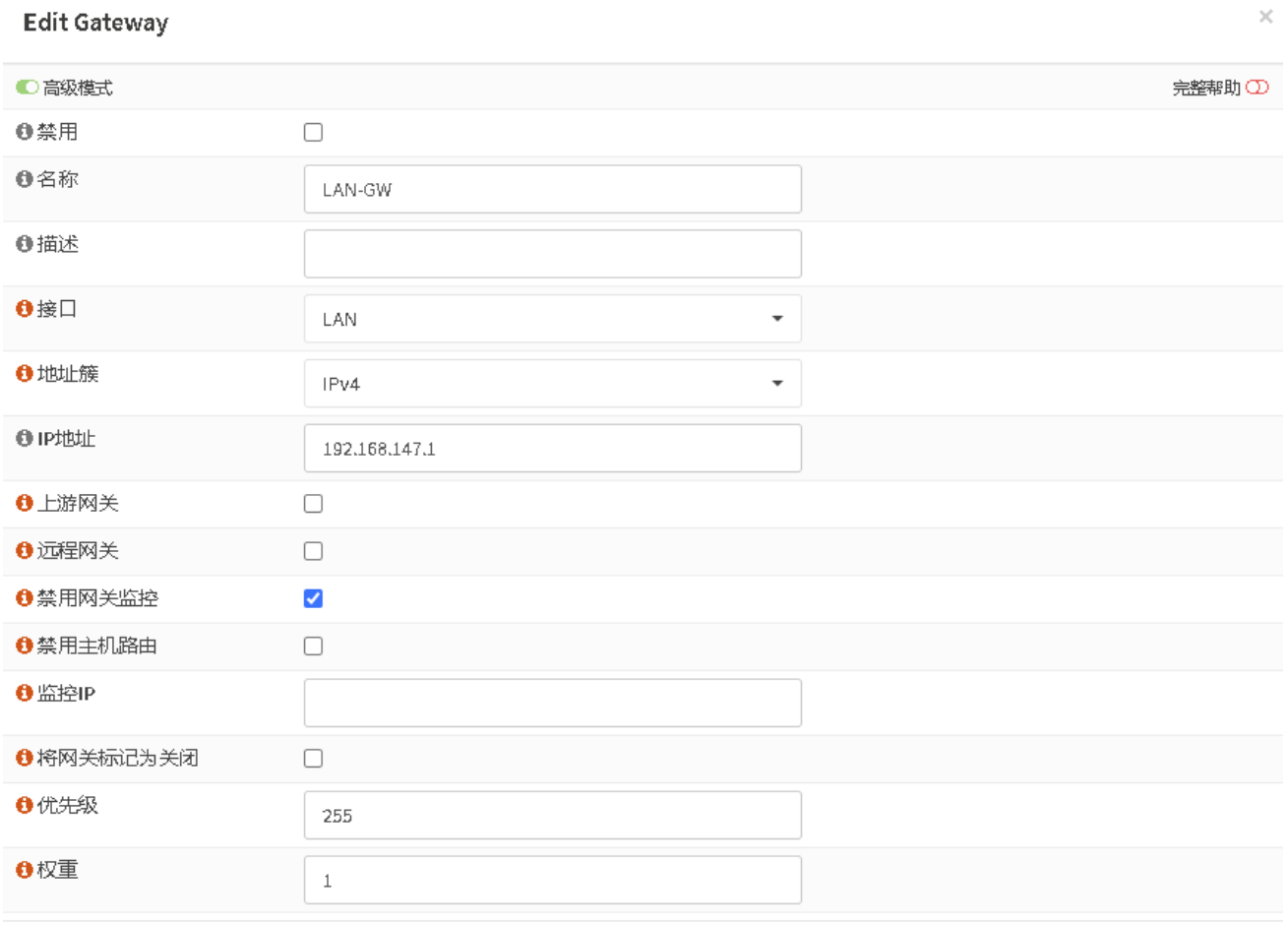
2. 设置主机名、语言、时区、DNS

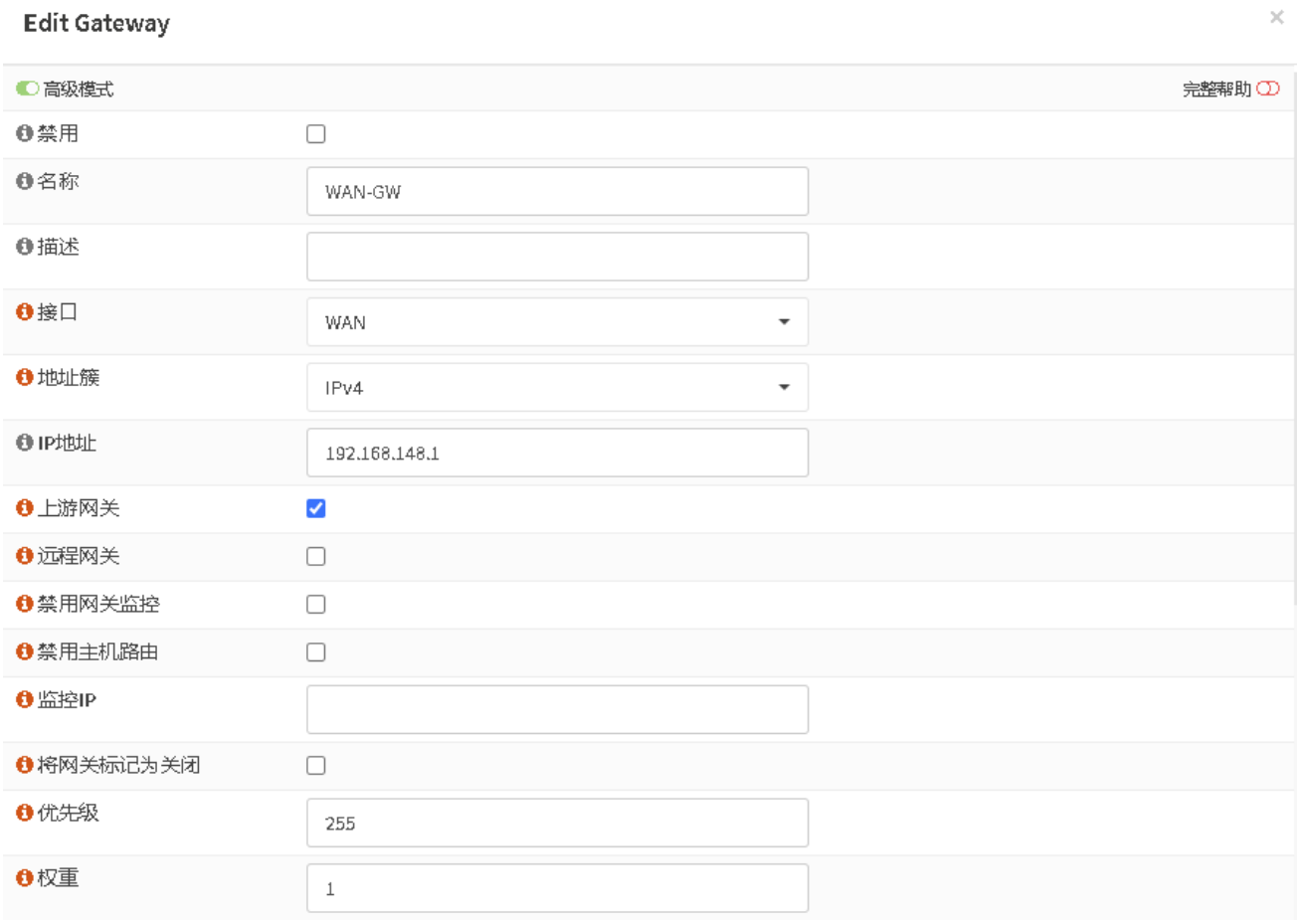
   在 system - setting - general 进行设置。

3. 添加网关

   OPNsense在设置路由前必须先添加网关。

   在 系统 - 网关 - 配置 里添加网关。在此处分别添加LAN口和WAN口路由。

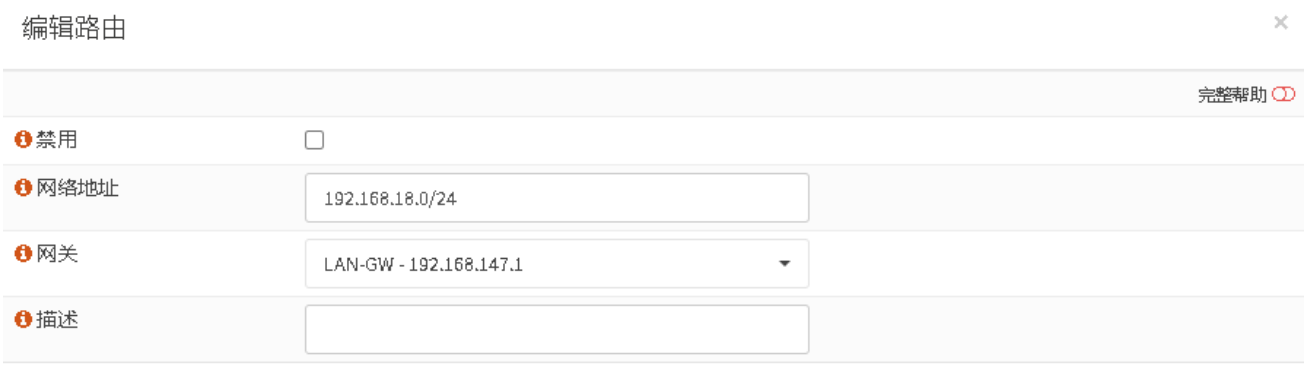




注：WAN接口使能上游网关选项后，将自动产生缺省路由。

4. 添加内网路由

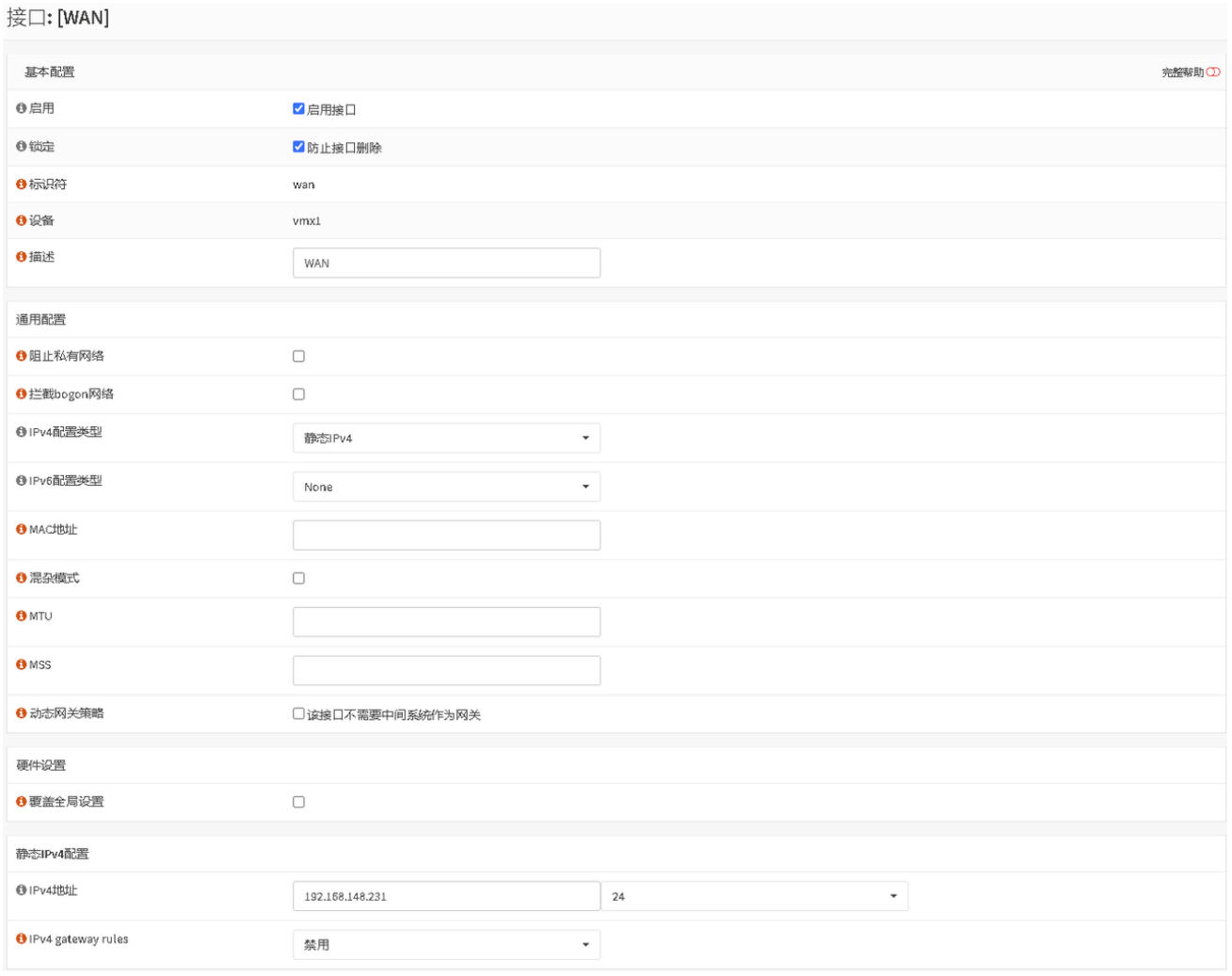
在 系统 - 路由 - 配置 中添加静态路由。在此处添加的路由不会因为重启而丢失。



5. 设置WAN口IP地址

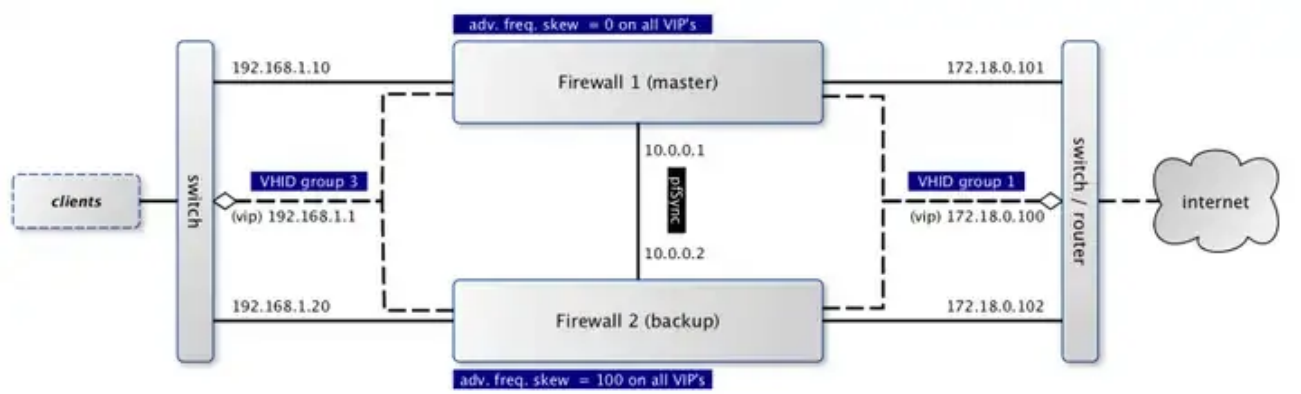
在 接口 - WAN 设置WAN口的IP地址。

注意：如果WAN口的地址是私网地址，需要去使能“阻止私有网络”和“拦截bogon网络”



四、OPNsense的高可用

OPNsense可以将两个或多个防火墙配置为一个故障转移组。如果主设备上的一个接口出现故障或主服务器完全脱机，则从设备变为活动状态。



OPNsense支持状态同步即防火墙的状态表被复制到所有配置了故障转移的防火墙，当发生故障时，所有的连接不会中断。

OPNsense配置高可用的时候建议使用专用的接口作为状态同步使用，即防火墙至少有3个接口，LAN、WAN和同步接口。**对防火墙添加完新网卡后，还必须在防火墙配置中为接口分配名字后才能使用**。新添加的接口默认状态下所有入站连接都会被阻止，需要将同步接口上允许所有的数据包通过。

OPNsense利用CARP协议来实现硬件故障转移，Common Address Redundancy Protocol，公共地址冗余协议，使用IP协议号112，与VRRP和HSRP功能类似，主要使用在OpenBSD和FreeBSD操作系统上。使用组播向邻居发送有关其状态的信号（在OPNsense 24.7版本开始支持使用单播来发送通告报文）。

OPNsense的高可用包括以下几个部分：

1. 自动故障转移：当主防火墙不可用时，辅助防火墙将在没有用户干预和最小中断的情况下接管。
2. 同步状态表：防火墙的状态表将复制到所有故障转移配置的防火墙。当发生故障时将保持现有连接。在启用状态同步时，建议选用单独的接口作为会话同步使用，防止在接口发生拥塞时导致间歇性状态丢失。
3. 配置同步：在主系统上进行的配置更改会同步（手动触发）到辅助防火墙。如果需要自动同步配置可以在 系统 - 设置 - 任务 中配置定时任务来完成配置同步（为了限制非运行主机对活动主机的更新，只有当所有 CARP 接口设置为 MASTER 模式时才会执行HA 更新和重新配置备份。）。

1. OPNsense高可用配置流程

配置OPNsense的高可用有以下几个步骤：

1. 配置接口

2. 配置防火墙规则
    a. 在主节点上添加防火墙规则
    b. 在备份节点上添加防火墙规则
3. 配置虚拟IP地址
4. 配置出站NAT
5. 配置DHCP服务器（可选）
6. 配置pfSync和HA同步（xmlrpc）

其中1、2步需要在两个防护墙分别配置，3-5步在主防火墙上配置后，通过同步机制同步到备份防火墙上，第6步主备防护墙的配置有所不同。

2. OPNsense高可用配置步骤

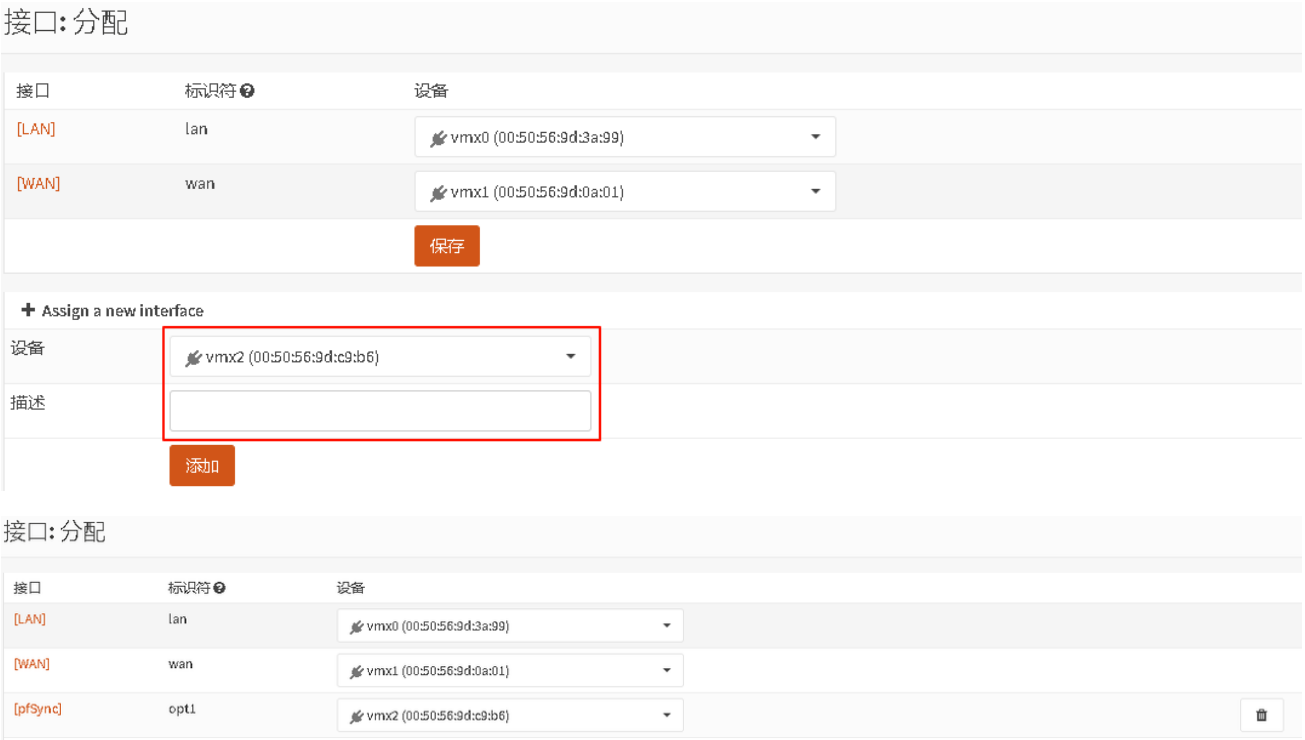
2.1 配置接口

按照规划配置主、备防火墙的接口IP，并增加同步接口。

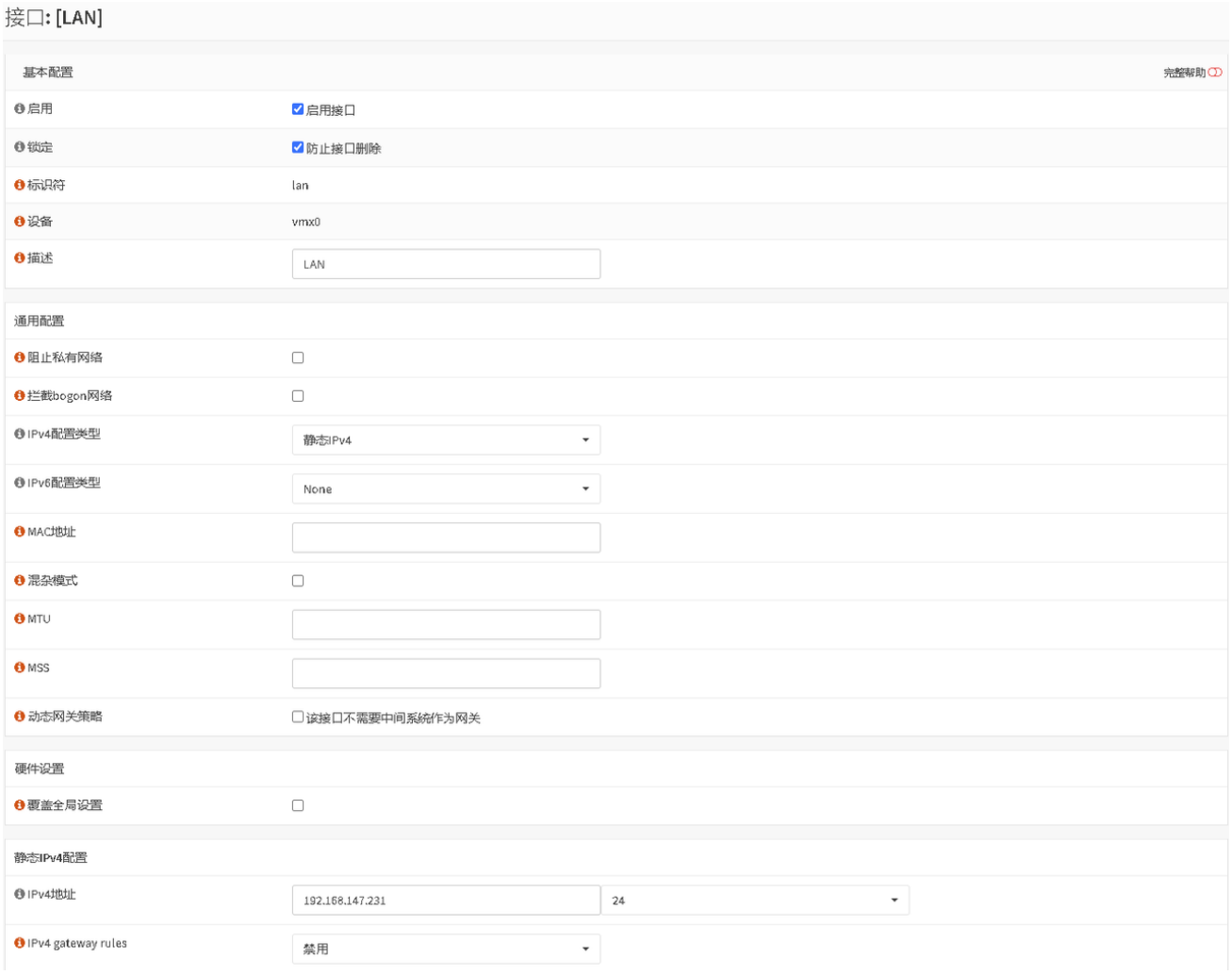
为了防止接口被误操作删除，建议勾选锁定选项。

增加同步接口，将同步接口的名字定义为pfSync。

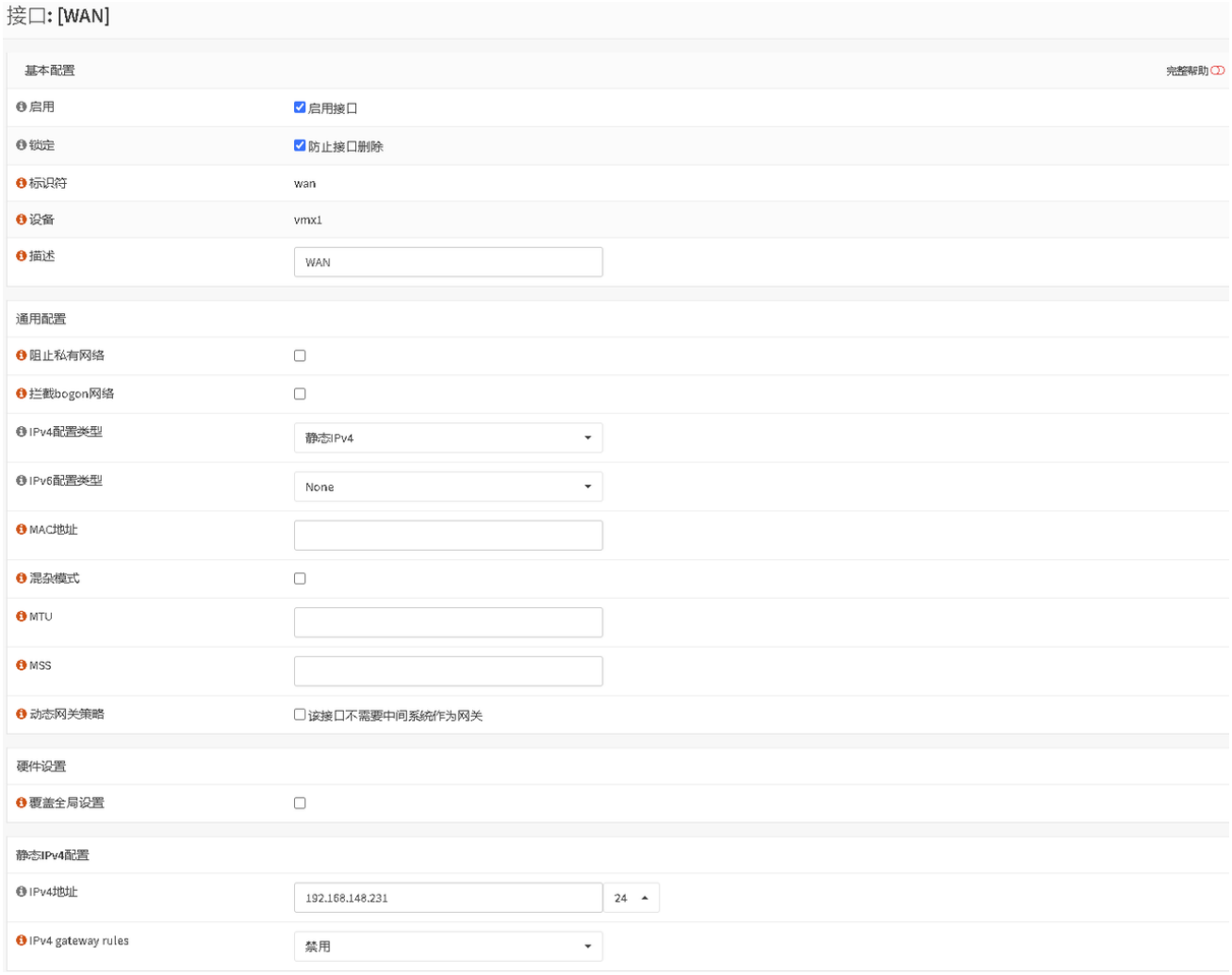
OPNsense默认状态下只定义了LAN和WAN两个接口，其余网卡均处于未分配状态，需要在 接口 - 分配 中完成网卡的定义，在描述处填写网卡名称点击添加即可。



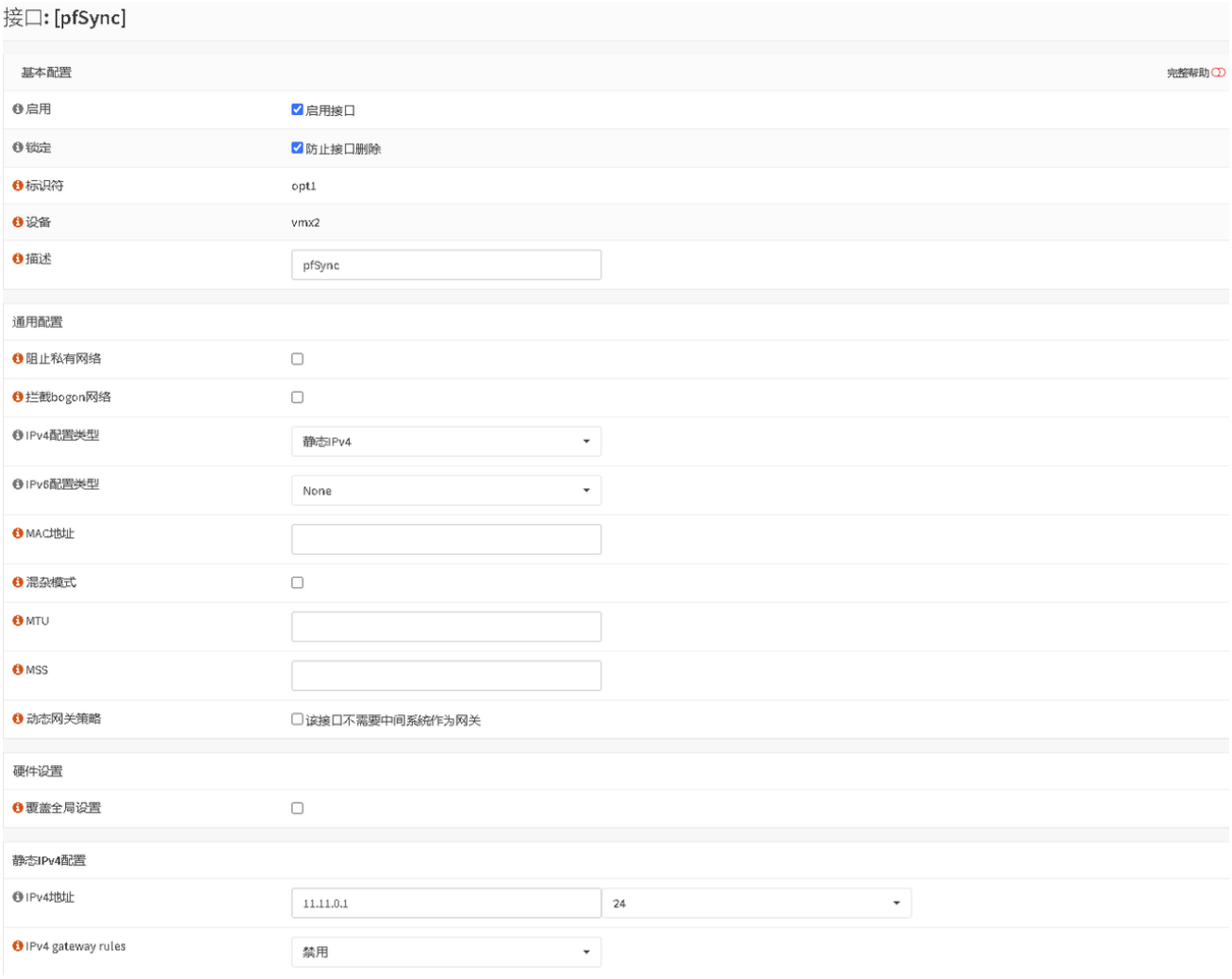
LAN口配置


接口: [LAN]
基本配置
完整帮助
启用
启用接口
锁定
防止接口删除
标识符
lan
设备
vmx0
描述
LAN
通用配置
阻止私有网络
拦截bogon网络
IPv4配置类型
静态IPv4
IPv6配置类型
None
MAC地址
混杂模式
MTU
MSS
动态网关策略
该接口不需要中间系统作为网关
硬件设置
覆盖全局设置
静态IPv4配置
IPv4地址
192.168.147.231
24
IPv4 gateway rules
禁用

WAN口配置


接口: [WAN]
基本配置
完整帮助
启用
启用接口
锁定
防止接口删除
标识符
wan
设备
vmx1
描述
WAN
通用配置
阻止私有网络
拦截bogon网络
IPv4配置类型
静态IPv4
IPv6配置类型
None
MAC地址
混杂模式
MTU
MSS
动态网关策略
该接口不需要中间系统作为网关
硬件设置
覆盖全局设置
静态IPv4配置
IPv4地址
192.168.148.231
24
IPv4 gateway rules
禁用

pfSync口配置



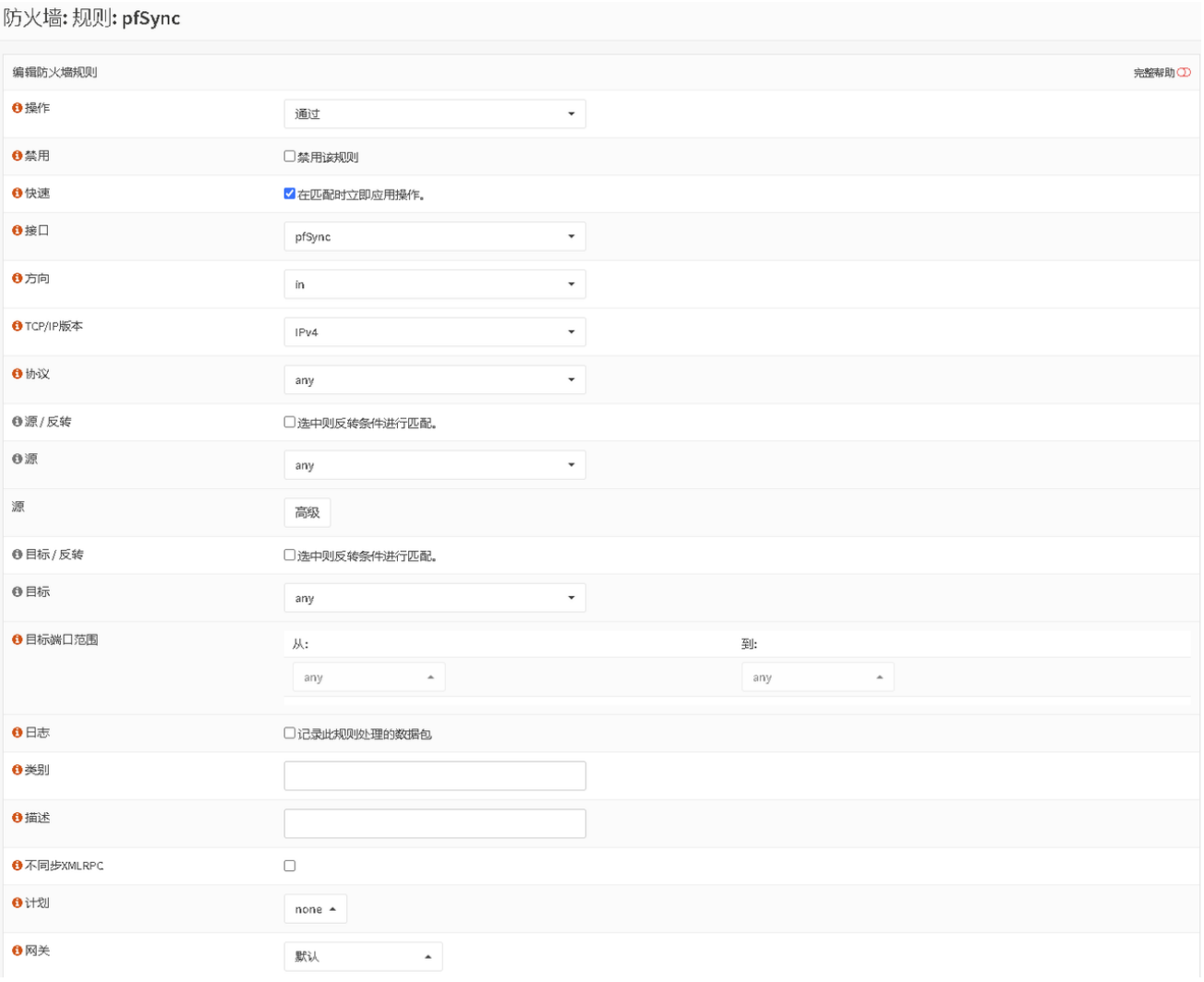
2.2 配置防火墙规则

在主防火墙和备份防火墙上创建相同的防火墙规则。在这里调整防火墙规则只为能够完成主备防火墙的协商和完成防火墙配置同步，需要在主备防火墙上分别设置，构建高可用系统后，再添加的防火墙策略可以通过同步的方式来保证主备防火墙的策略一致。

需要调整防火墙全部端口的防火墙策略（除LAN口上的防火墙策略默认是允许LAN网络的数据包接入以外，其余接口默认都是拒绝全部数据包进入防火墙）。

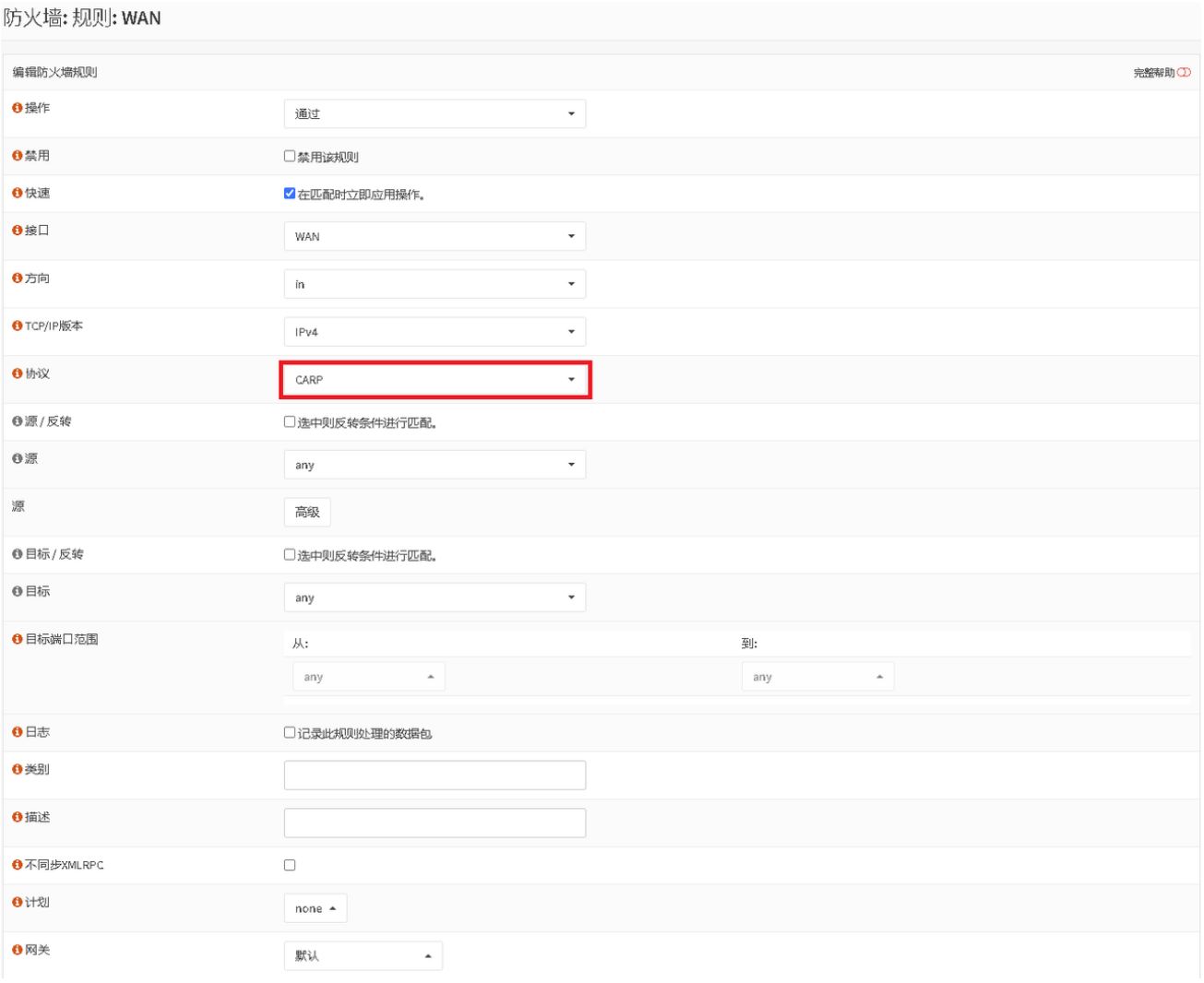
由于pfSync接口只做内部通信使用，不连接外部网络，建议两台防火墙的pfSync接口全部允许数据包进入。

在 防火墙 - 规则 里pfSync接口下添加规则（切记在配置同步前，一定要将防火墙的pySync接口的防火墙改为允许any）



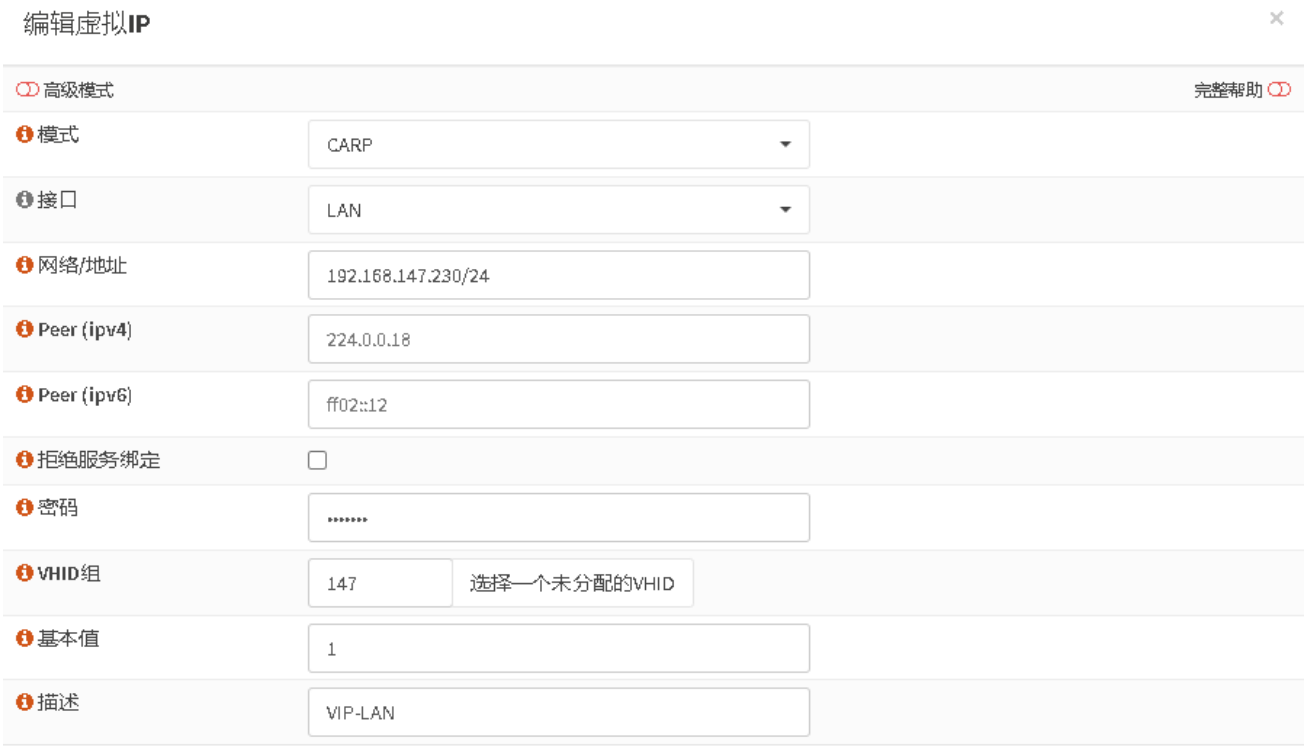
LAN接口默认规则是允许所有放行，不需要进行调整。

WAN接口默认无规则，需要添加允许接收CARP协议。



2.3 配置虚拟IP地址

在 接口 - 虚拟IP - 设置下设置虚拟IP地址（VIP地址），要保证CARP中IP的子网掩码与主接口相同。



注：

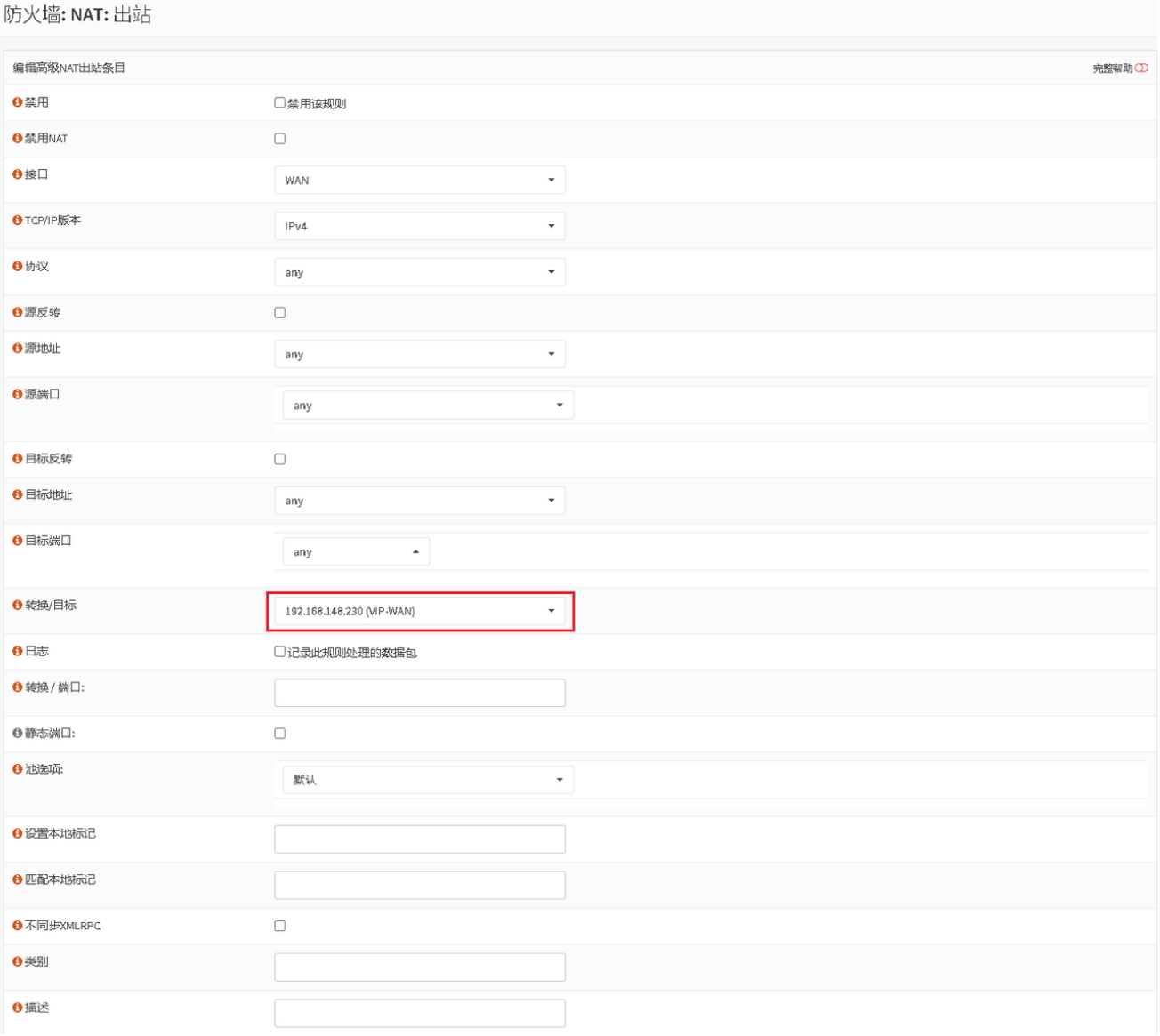
1. VHID组等同于VRRP的VRID，取值范围为1~255。
2. 基本值（advbase）相当于VRRP的通告间隔，单位是秒。
3. 偏移值（advskew）类似于VRRP的优先级，advskew越小越优先，取值范围从0~254，步长是1/256秒（偏移值默认值是0，同步到备防火墙的偏移值是100）。
4. CARP协议支持组播通告或单播通告，当网络环境不支持组播时（公有云环境），可以使用单播通告，默认使用224.0.0.18的组播地址通告。

2.4 配置出站NAT

为了保证防火墙出现主备切换时，原有连接不中断，出站的流量应该使用与WAN接口关联的虚拟 IP 地址。默认情况下，OPNsense的NAT出站为“自动出站 NAT规则生成”（使用防火墙WAN口的地址进行NAT），这会影响数据流量的平滑过渡，需要修改成使用WAN口虚拟地址。

在 防火墙 - NAT - 出站 里修改，先将模式调整为手动生成出站NAT规则，再添加手动规则。

对外NAT规则



2.5 配置pfSync和HA同步（xmlrpc ）

为了启动同步过程，必须在主防火墙上分别配置pfSync和HA同步 (xmlrpc)。在备份防火墙上只配置 pfSync不配置xmlrpc。

主防火墙配置

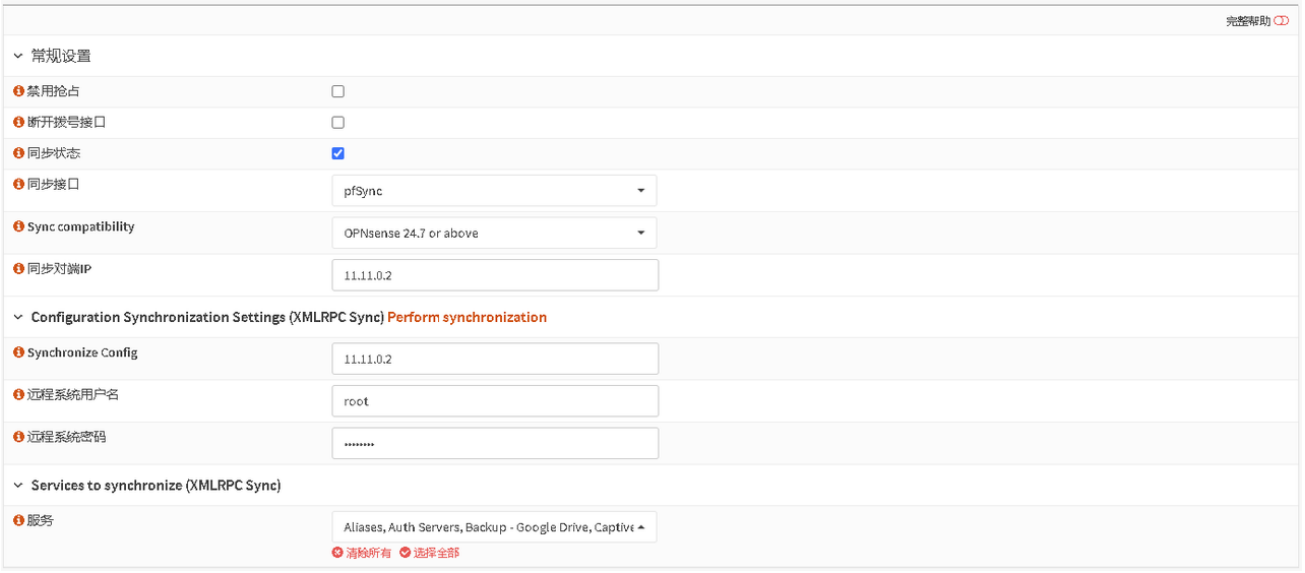
状态同步：

在 系统 - 高可用 - 设置 里配置高可用，**去使能“禁用抢占”、使能“同步状态”，**选择同步接口为pfSync，同步地址设置成对端防火墙（备份防火墙）的pfSync接口地址。

配置同步：

配置同步采用xmlrpc方式，将配置文件从主防火墙同步到备份防火墙上。同步地址设置为对端防火墙的pfSync接口地址，并填入对方防火墙的管理员用户名和密码，再选择需要同步的服务（必须要同步的服务包括firewall Rule、NAT、virtual IP，建议同步Captive Portal、Firewall Schedules、Static Routes、WEB GUI、Network Time、Shaper、Users and Groups，没有选择同步的服务在修改时必须要在主备防火墙都手动修改）。

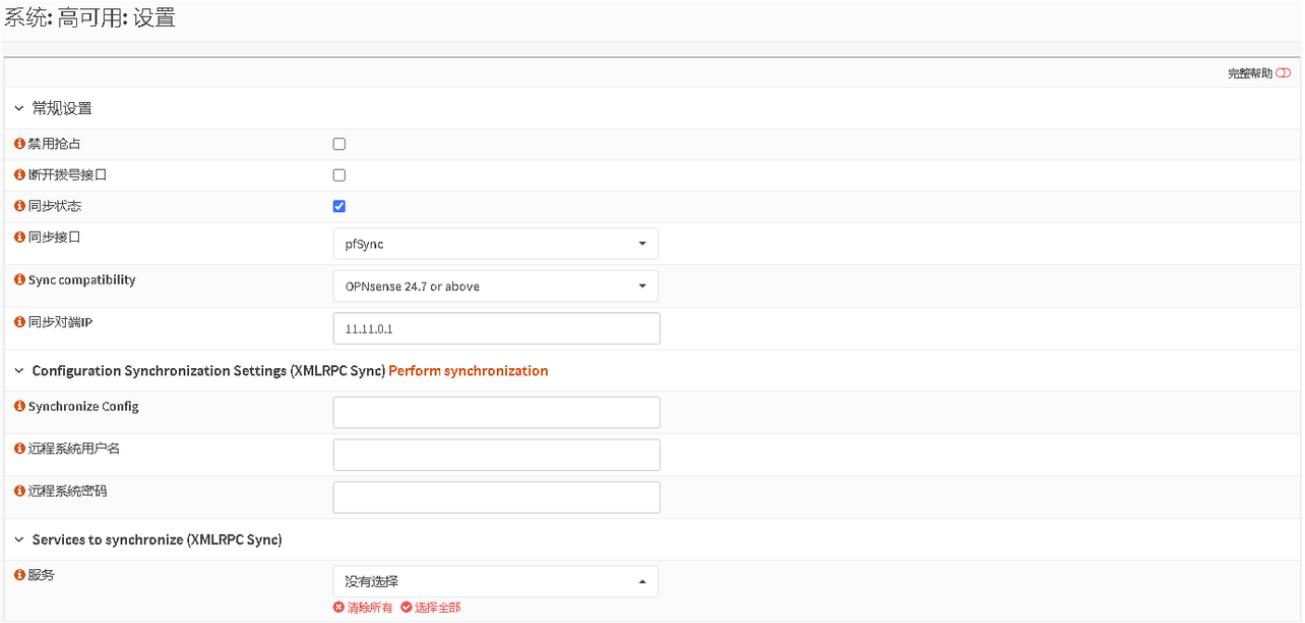
系统: 高可用: 设置



备份防火墙配置

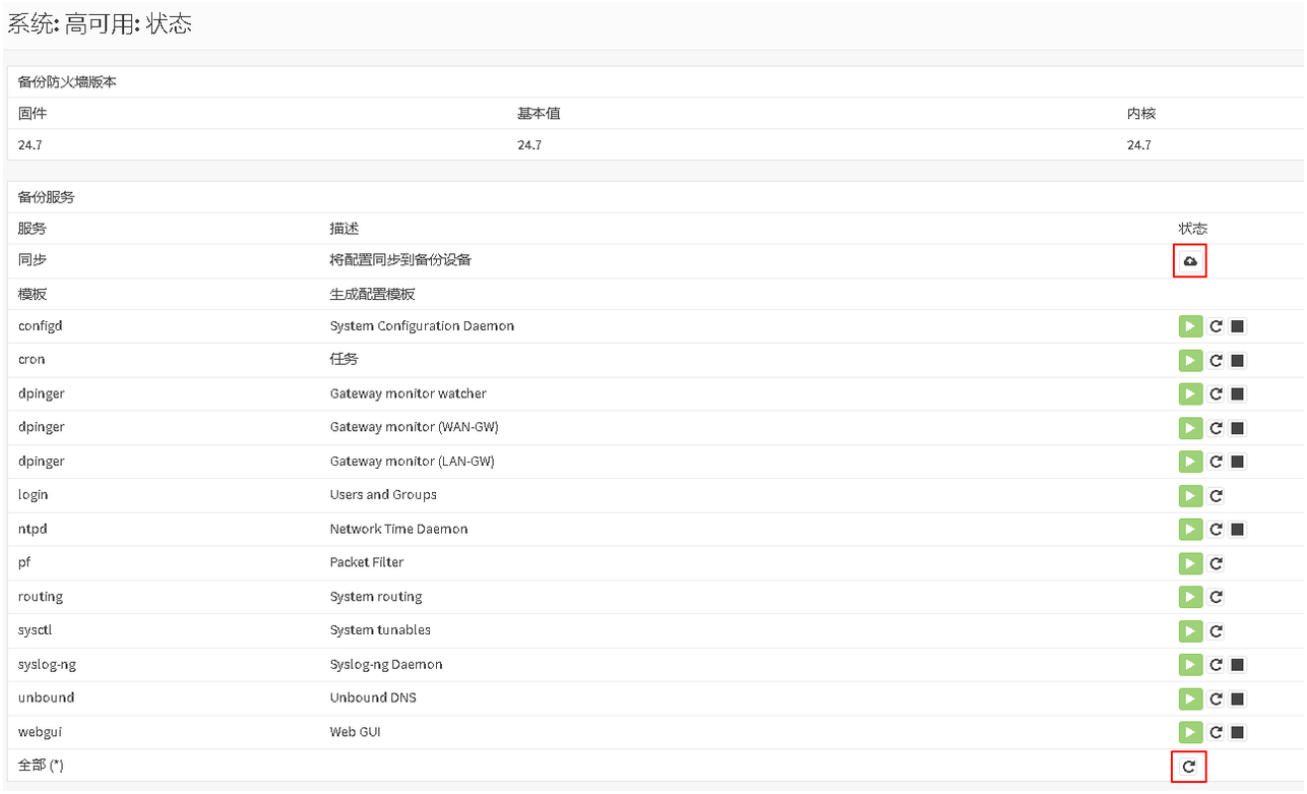
只配置 pfSync不配置xmlrpc，选择同步接口为pfSync，同步地址设置成对端防火墙（主防火墙）的pfSync接口地址。。

系统: 高可用: 设置



2.6 配置同步

配置完成后，在主防火墙的 系统 - 高可用 - 状态 里手动同步配置。点击 同步 按钮进行配置同步，点击最下面的按钮同步并重启所有的服务。



主备防火墙只能手动配置同步或者用计划任务进行配置同步，无自动同步功能。

五、OPNsense虚拟IP切换

1. 同步口的状态不会引起虚拟IP的切换；
2. 配置了虚拟IP的物理接口状态发生变化时，会引起虚拟IP切换；
3. 虚拟IP存活的防火墙的物理端口状态变化，会导致全部虚拟IP从漂移到对端防火墙上，来保证网络的畅通；
4. 在 接口 - 虚拟IP - 状态 里可以手动切换虚拟IP存活的防火墙；

六、OPNsense软件版本升级步骤

软件升级时遵循的原则是最大限度地减少更新执行期间的中断，建议遵循以下步骤：

1. 先升级备份防火墙（虚拟IP不存活的防火墙），升级完成后防火墙会自动重启；
2. 在主防火墙 接口 - 虚拟IP - 状态 里选择进入持久 CARP 维护模式触发虚拟IP漂移到备份防火墙上，检查备份防火墙全部服务可以正常工作；
3. 升级主防火墙，主防火墙重启后，禁用持久 CARP 维护模式，确认工作正常；

七、注意事项

1. OPNsense的高可用的配置同步默认是手动同步，配置自动同步只能通过计划任务来实现；

2. 在ESXI环境下，必须开启混杂模式，多上连链路需要调整宿主机的高级系统配置，将Net.ReversePathFwdCheckPromisc的值设置为1，先调整参数再修改混杂模式；
3. 软件版本升级时需要注意服务组件是否有重大调整，调整的内容是否支持向前兼容；
4. 配置同步只能从设定的主墙同步配置到备份防火墙，不能双向同步，并且只有当所有CARP接口设置为 MASTER 模式时才会执行HA 更新和重新配置备份；
5. OPNsense的状态同步必须使用相同的接口名称来访问相同的网络；
6. 在ESXI里下游服务器与防火墙在同宿主机上有可能会收到重复包（原因未知）；
7. LAN口虚拟IP和WAN口虚拟IP在出现切换时有可能不会联动（原因未知）

八、测试结果

1. 中断时长

测试方法

用ping目标地址方式测试，ping包间隔0.1秒，超时时间0.1秒。

测试数据

初始状态下，虚拟IP存活在主防火墙上，两个防火墙都没有开启抢占模式。

1. 主防火墙WAN口down，全部虚拟IP从主防火墙漂移到备份防火墙上，一般情况下最长中断时间3~4秒，极端情况15秒以上（观察到的现象：WAN虚拟IP在3~4秒漂移成功，LAN虚拟需要等一段时间才漂移，）；
2. 恢复主防火墙WAN口状态，虚拟IP不发生变化；
3. （虚拟IP在备份防火墙上），备份防火墙WAN口down，全部虚拟IP漂移到主防火墙上，没有网络中断；
4. 主防火墙LAN口down，LAN虚拟IP漂移到备份防火墙上，WAN虚拟IP未漂移（原因未知）
5. 在 接口 - 虚拟IP - 状态 里用暂定CARP切换虚拟IP，最长中断3~4秒；
6. 在 接口 - 虚拟IP - 状态 里用进入CARP持久维护模式切换虚拟IP，无网络中断；

2. 会话保持

防火墙在正常工作时，会话信息自动从主防火墙同步到备份防火墙上，虚拟IP在主备防火墙上切换不会出现会话中断。