链滴

家庭内网新布局

作者：evling

原文链接：https://ld246.com/article/1615614839403

来源网站：链滴

<h2 id="背景">背景</h2>
近些时日，易雾君忙着对家庭内网结构做了番大调整，kvm 虚机尽全力向 lxc 容器转化，区域划明确，规定好相互访问控制策略，并且让动态增加网络节点提供了便利，使整个网络的管理有章可循重点解决了跨设备的网络隔离问题。
<h2 id="区域划分">区域划分</h2>
根据前期很长一段时间对家庭网络的实践，易雾君初步对内网划分了 9 个区域如下：
<table>
<thead>
<tr>
<th>区域中文名称</th>
<th>区域英文名称</th>
<th>区号</th>
<th>职能描述</th>
</tr>
</thead>
<tbody>
<tr>
<td>网管区</td>
<td>net_mgr</td>
<td>00</td>
<td>放置具有访问全内网需求的机器，如堡垒机、资产测绘机</td>
</tr>
<tr>
<td>内网核心服务区</td>
<td>internal</td>
<td>01</td>
<td>内网站点服务重点聚集的区域</td>
</tr>
<tr>
<td>共享区域</td>
<td>share_center</td>
<td>02</td>
<td>需要给大部分区域提供服务的区域</td>
</tr>
<tr>
<td>备份区域</td>
<td>backup</td>
<td>03</td>
<td>放置用于备份全网数据的资产</td>
</tr>
<tr>
<td>非军事区</td>
<td>dmz</td>
<td>04</td>
<td>与外网密切相关的服务区</td>
</tr>
<tr>
<td>测试区</td>
<td>test_lan</td>
<td>05</td>
<td>主要用于日常试验</td>
</tr>
<tr>
<td>靶场区</td>
</tr>
</tbody>

<td>vulhub_lan</td>
<td>06</td>
<td>各类靶机服务</td>
</tr>
<tr>
<td>家庭无线区</td>
<td>k3_lan</td>
<td>07</td>
<td>连接各设备的核心路由，同时给手机提供无线连接</td>
</tr>
<tr>
<td>虚拟专网区</td>
<td>vpn</td>
<td>08</td>
<td>提供远程节点接入入口，同时监听一个 tcp 和 udp 端口</td>
</tr>
</tbody>
</table>
<h2 id="网段设定">网段设定</h2>
网段的设定也要考虑到有意义，比方说，先规定好每个设备有个编号，网段的第三点分位就依据备号来定，理论可每个区可加入 256 台机器，对于家庭需求，绰绰有余。
<table>
<thead>
<tr>
<th>设备中文名称</th>
<th>设备英文名称</th>
<th>设备号</th>
<th>职能描述</th>
</tr>
</thead>
<tbody>
<tr>
<td>购买的公网服务器</td>
<td>vps</td>
<td>000</td>
<td>提供对外访问的站点入口，只供 CDN 接入</td>
</tr>
<tr>
<td>闲置戴尔笔记本</td>
<td>prod</td>
<td>001</td>
<td>主生产服务器、爬虫</td>
</tr>
<tr>
<td>树莓派 3b</td>
<td>pi3</td>
<td>002</td>
<td>内网网盘服务 nextcloud、kodbox 及 letsencrypt 自动续期服务</td>
</tr>
<tr>
<td>树莓派 3b+</td>
<td>pi3bp</td>
<td>003</td>
<td>waf、外网门户、论坛、kali 终端版</td>

</tr>
<tr>
<td>日常使用台式机</td>
<td>lab</td>
<td>004</td>
<td>全网备份服务、试验环境、靶场、elk、爬虫等</td>
</tr>
<tr>
<td>工作用机</td>
<td>think</td>
<td>008</td>
<td>母机办公，虚机加入内网备用</td>
</tr>
<tr>
<td>斐讯</td>
<td>k3</td>
<td>015</td>
<td>家庭核心路由</td>
</tr>
<tr>
<td>测试机器</td>
<td>test-1</td>
<td>101</td>
<td>测试用机</td>
</tr>
<tr>
<td>靶场机器</td>
<td>vulhub-1</td>
<td>201</td>
<td>靶场用机</td>
</tr>
<tr>
<td>虚拟专网接入网关设备</td>
<td>vpn</td>
<td>044\045</td>
<td>负责连接分支设备的虚拟网关设备</td>
</tr>
</tbody>
</table>
<h2 id="机器命名规范">机器命名规范</h2>
机器多了，管理自然麻烦了，没个命名规则，自个蛋疼去吧。现在咱们区号有了，设备号也有了是不是可以从区号及设备号来做点文章，比方说，测试区的一台终端版 kali ，易霁君想把它放置在树派 3b+ 上，供 24 小时全天候，以便随时能拿到工具开整。像这样 <code>05-003-kali</code> 命名机器，那么咱们就可以用 <code>区号-设备号-名称</code> 的方式统一命名机器，并以它为机名。依据该规则，易霁君展示下部分命名案例如下
<img src="https://ld246.com/images/img-loading.svg" alt="Screenshot20210313080355 png" data-src="https://b3logfile.com/file/2021/03/Screenshot_2021-03-13_08-03-55-1453cd9.png?imageView2/2/interlace/1/format/jpg">
<h2 id="虚拟化选型">虚拟化选型</h2>
最大化程度使用容器也是本次变革最重要的因素之一，变革前，生产主力机器跑个 5 个 kvm 就的一匹，变革后，同时跑上了十几个重量级的容器，都能从容，启动时间也提升了一大节。如下是该器现在的一个运行负载情况，挺宽裕的，还能部署些服务，后期再扩展。
<img src="https://ld246.com/images/img-loading.svg" alt="Screenshot20210313082811 png" data-src="https://b3logfile.com/file/2021/03/Screenshot_2021-03-13_08-28-11-e7ccb8

8.png?imageView2/2/interlace/1/format/jpg">
在整个家庭网运营当中，各种虚拟化都能用的上，看需求而定，易雾君的分配原则是，以 lxc 容或 kvm 虚机为单位（具有内部独立 IP），其上统一跑 docker 服务，这就是一个内部分配的主旋律目前除了备份机器使用了 kvm 外，其他全采用 lxc 容器嵌套 docker 的方案，备份机使用 kvm 的原是，需对数据分区进行加密，并依赖 proxmox 自带的备份功能仅备份加密分区到 nfs 服务器，系统区放置有开机解密分区的解密文件，不参与备份。
<h2 id="区域访问控制设定">区域访问控制设定</h2>
规定一个区域访问二维表，左边列为源区域，上边行为目标区域，N 代表不可访问，Y 代表可访，- 代表忽略。如下表仅供参考，各位看官可根据实际情况裁剪或修改。
<table>
<thead>
<tr>
<th>源区\目标区</th>
<th>extranet</th>
<th>net_mgr</th>
<th>internal</th>
<th>share_center</th>
<th>backup</th>
<th>dmz</th>
<th>test_lan</th>
<th>vulhub_lan</th>
<th>k3_lan</th>
<th>vpn</th>
</tr>
</thead>
<tbody>
<tr>
<td>extranet</td>
<td>-</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>net_mgr</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>internal</td>

```
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td><strong>share_center</strong></td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td><strong>backup</strong></td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>dmz</strong></td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td><strong>test_lan</strong></td>
<td>N</td>
<td>N</td>
```

<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>vulhub_lan</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>k3_lan</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>vpn</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>
<h2 id="动态扩展节点">动态扩展节点</h2>
本次的网络改造统一采取每一个独立设备中都要提供一个虚拟路由器与家庭网关 k3 进行连接，里规定所有的路由节点全全搭载 openwrt 系统，该节点路由所涵盖的网段默认纳入内网核心服务区备用，在其上线时，利用其运算资源，统一步伐。新版网络整体布局图如下。

<h2 id="外网访问控制">外网访问控制</h2>
默认情况下除了家庭无线区具有外网访问权限以外，其他所有机器默认不能访问外网的，需要以名单的形式加入到访问外网需求的 ipset 清单，方可访问外网。外网访问控制只作用在网关出口设备讯 k3 那里，其他所有 openwrt 路由统统对外网访问数据包放行。
另外，可能有些家庭客户具有匿名访问需求，如嵌套级联了好多个跳板才访问到目标网站服务，的直接对 tor 有需求，一般情况下会是在本地同时监听一个 socks5 代理端口和 tcp 重定向端口，socs5 端口供浏览器直接指定，而 tcp 重定向端口就是一种针对用户透明无感知的玩法，选哪种还得看人喜好。最好是两种都部署好，易雾君在这里就只提供思路，不给具体方案了。
<h2 id="疑惑排解">疑惑排解</h2>

树梅派上如何如何统一步伐，怎样能部署 lxc ，还要让它有个 arm64 版的 openwrt

众所周知，proxmox 天然具备了 lxc 和 kvm 虚拟化条件啊，当然在树莓派的 64 位操作系统装 lx 不成问题，但要通过命令进行操作，而 proxmox 则能够通过 ui 管理，openwrt 则是易雾君在官方载了树梅派版的镜像，对其根目录下的所有目录打包到树梅派下的 lxc 目录，如若信得过易雾君，可拿去先看下效果，能跑起来，你再自己做份，下面贴个做好的链接
https://pan.evling.me/s/aA95Ny7PB86Z2r
访问密码请到公众号 <code>易雾山庄</code> 输入 <code>获取密码</code> 指令获取访问码，里边的配置文件根据自己环境改，其中 lxc.conf 放到 <code>/etc/lxc/lxc.conf</code>

家庭网分布了多个分支路由节点，网络访问控制如何实施

所有涉及网关作用的路由关卡都应该配置有区域访问控制规则，除了总的核心网关 k3（兼网络口）外，其他分支节点路由可以统一用同一个规则，咱们可以用一个规则服务器，供这些分支路由同步 iptables 区域访问规则，规则分两个文件，一个文件存放主路由 k3 的规则，一个存放分支路由的规

<h2 id="结语">结语</h2>
好了好了，很久没更了，这跟大家伙的关注热度有正关系呢，想关注更多干货，还犹豫什么呢，往微信搜索 <code>易雾山庄</code>，订阅易雾君的独家折腾记。
下篇预告：《家庭网络资产测绘》