

# SINFOR AC 产品测试/实施手册

## (Ver 1.1)

**SINFOR<sup>®</sup> 深信服科技**  
—— 提 升 带 宽 价 值 ——

2009 年 7 月

# 目录

1. 网络环境确认.....	3
2. 测试/实施前准备工作.....	3
2.1. 若自带产品，需先走设备自检流程.....	3
2.2. 通过电话与用户沟通，获取用户信息和预约上门安装时间.....	3
2.2.1. 获取用户的详细资料.....	3
2.2.2. 获取用户的软硬件环境.....	3
2.2.3. 约定上门的时间.....	4
2.3. 整理安装实施所需要的资料.....	4
3. 设备上架规范.....	4
3.1. 设备上架准备.....	4
3.2. 设备安装.....	5
3.3. 设备安装检查.....	6
4. Webagent实施规范.....	6
5. bypass功能检测.....	7
6. 各种网络环境下的基本配置规范.....	7
6.1. 目的.....	7
6.2. AC路由模式部署基本配置规范.....	7
6.2.1. AC路由模式（WAN口直接拨号或接固定Internet IP 线路）.....	7
6.2.2. AC路由模式（通过前置网关设备上网）.....	10
6.2.3. AC 路由模式（支持VLAN环境）.....	12
6.2.4. AC 路由模式（内网通过代理服务器上网）.....	14
6.2.5. AC路由模式（双机热备）.....	17
6.3. AC网桥模式部署基本配置规范.....	19
6.3.1. 基本网桥模式配置规范.....	19
6.3.2. AC网桥模式（支持VLAN穿透）.....	21
6.3.3. AC网桥模式（内网通过代理服务器上网环境一）.....	24
6.3.4. AC网桥模式（内网通过代理服务器上网环境二）.....	27
6.3.5. AC网桥模式（前置设备双机热备）.....	29

6.3.6.	AC网桥模式（VRRP环境） .....	31
6.3.7.	AC网桥模式（穿透动态路由） .....	34
6.3.8.	AC网桥模式（双机热备环境） .....	36
6.3.9.	AC网桥部署（启用Bypass功能） .....	39
6.4.	AC旁路模式部署基本配置规范 .....	41
6.4.1.	基本旁路模式配置规范 .....	41
6.4.2.	AC旁路模式（通过代理服务器上网环境） .....	43
6.4.3.	AC旁路模式（双机热备环境） .....	46
7.	紧急事件处理规范 .....	48
8.	常见问题处理规范 .....	49
9.	测试/实施完成后扫尾规范 .....	52

## 1. 网络环境确认

详见《环境确认表》。

## 2. 测试/实施前准备工作

### 2.1. 若自带产品，需先走设备自检流程

### 2.2. 通过电话与用户沟通，获取用户信息和预约上门安装时间

#### 2.2.1. 获取用户的详细资料

包括：企业名称、通讯地址、联系人、联系电话。

#### 2.2.2. 获取用户的软硬件环境

例如：客户的网络环境、AC 数据中心服务器的操作系统版本、是否有域服务器、

是否使用代理服务器等信息，完成《网络环境确认表》。确保客户网络环境具备安装条件再安排上门实施。如客户网络不具备安装条件，跟客户协商网络整改时间。待整改后具备安装条件再跟客户约定上门实施时间。

### 2.2.3. 约定上门的时间

同客户确认上门时间，以保证客户方有对公司内部网络情况较为熟悉的人员配合实施。

## 2.3. 整理安装实施所需要的资料

整理安装实施过程中需要携带的设备和资料，例如：笔记本电脑，交叉线，常用的软件，上门反馈表，工牌等。

# 3. 设备上架规范

## 3.1. 设备上架准备

### (1) 安装场所准备

要求	具体内容
温度/湿度环境要求	标准工作在温度 0~ 45 °C,湿度 5~90%,非冷凝。
输入电压要求	110—230V
抗干扰要求	远离强功率无线电发射台、雷达发射台、高频大电流设备。
接地要求	良好的接地系统是设备稳定可靠运行的基础。建议接地电阻值宜小于 5 欧姆。
机架要求	通风散热、牢固承重、接地良好。
供电要求	具体数值请参考产品硬件参数文档。

### (2) 注意事项

注意事项	具体内容
------	------

<p>用电注意事项</p>	<p>1: 仔细检查在您的工作区域内是否存在潜在的危险，比如电源未接地、电源接地不可靠，地面潮湿等。</p> <p>2: 在安装前，要知道设备所在房间的紧急电源开关的位置，当发生意外时，要先切断电源开关。</p> <p>3: 请不要将设备放置在潮湿的地方，也不要让液体进入机箱内。</p>
<p>工具准备注意</p>	<p>安装前需提前准备好紧固工具、钳工工具。（螺丝刀、水晶头压线钳等）</p>

### 3.2. 设备安装

<p>设备搬移</p>	<p>在移动设备前一定要拔掉所有电源线和外部电缆。</p>
<p>设备上架</p>	<p>1: M5500 以上（含 M5500）设备必须安装托盘或导轨。</p> <p>2: 用户并不具备标准机柜情况下，可将设备安装在干净的工作台上。并保证保证安装工作台足够牢固，足以承担设备及电缆的重量，设备四周留出 10cm 散热空间。</p> <p>3: 不可在设备上放置重物。</p> <p>4: 在机器上架安装过程中，注意同一机柜中其它设备，避免在安装过程中碰掉其他设备的电源，网线接口等。</p>
<p>设备耳片安装</p>	<p>设备安装托盘或导轨后，可视情况不安装耳片。其他情况都必须安装耳片。</p>
<p>电源接线</p>	<p>有冗余电源设备必须接通冗余电源。</p>
<p>标签</p>	<p>线缆必须贴标签注明</p>

	<p>1: 电源线标签: 内容为电缆对端位置信息, 填写标签所在电缆侧对端设备、控制柜、分线盒或插座的位置信息。</p> <p>2: 信号线标签: 标签两面内容分别标识电缆两端所连端口的的位置信息。</p> <p>3: 粘贴标签之前先在整版标签纸上填写或打印好标签内容, 然后揭下、粘贴在电缆或标识牌线扣上。</p>
--	--

### 3.3. 设备安装检查

检查事项	具体操作
上电前检查	<p>1: 网络设备是否安放牢固。</p> <p>2: 所有通信电缆、光纤以及电源线和地线连接正确。</p> <p>3: 供电电压是否与网络设备的要求一致。</p>
设备上电	<p>1: 打开网络设备供电电源开关。</p> <p>2: 打开网络设备电源开关。</p>
上电后检查	<p>1: 网络设备上电以后, 通风系统工作, 应该可以听到风扇旋转的声音, 网络设备的通风孔有空气排出。</p> <p>2: 查看设备面板上的系统各种指示灯是否正常。</p>

## 4. Webagent 实施规范

如客户中心端有固定 IP 的情况, 技术交流、测试 (实施) 时优先选择并引导客户使用固定 IP。

如客户有自己的 Web 服务器 (该服务器必须单独部署于 IDC 机房或者与 VPN 设

备使用不同的网络出口)的情况,技术交流、测试(实施)时优先选择并引导客户将 Webagent 服务部署在自己的服务器上。

在上述条件都无法满足的情况下,我司可以为客户提供免费的 Webagent 服务,同时,请在实施(测试)时与客户进行事前沟通,让客户了解我司会尽可能为客户提供稳定的 Webagent 服务,但我司无法保证 Webagent 服务不因 Internet 网络故障、IDC 机房故障等无法控制的因素而导致中断。

## 5. bypass 功能检测

所有支持 bypass 的设备,在做网桥模式部署的时候,必须在实施时检测设备的 bypass 功能是否生效,以避免因为硬件故障引起客户的业务中断。

建议检测方法如下: bypass 接口默认是 LAN 口和 WAN 口,部署好设备之后,关闭电源,从 LAN 口所接的电脑上 ping 前置设备的接口或者公网 IP,如果可以通,表示 bypass 功能生效。

## 6. 各种网络环境下的基本配置规范

### 6.1. 目的

通过基本配置,能保证 SINFOR 设备上架后客户网络的正常运转,AC 的各种策略可以实现,客户的各种业务系统均能正常运行。

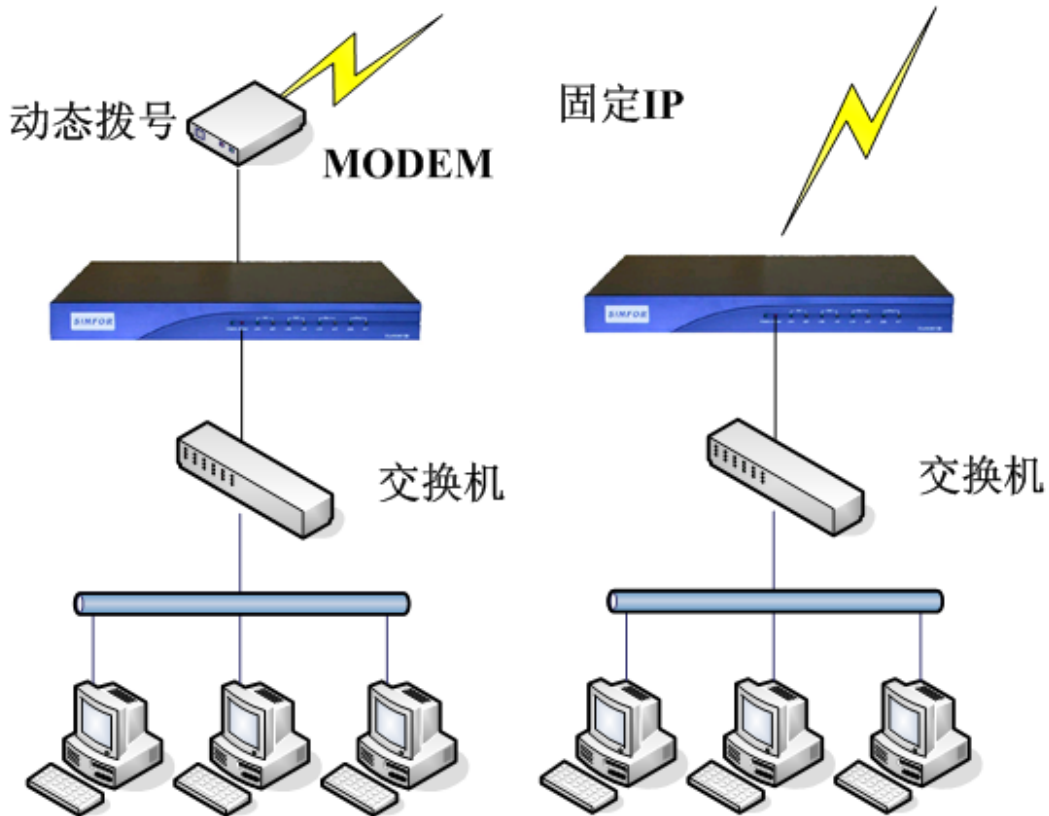
### 6.2. AC 路由模式部署基本配置规范

#### 6.2.1. AC 路由模式( WAN 口直接拨号或接固定 Internet IP 线路)

##### 6.2.1.1. 网络拓扑

环境描述:设备路由模式部署, WAN 口与 MODEN 相连进行拨号, LAN 口连接局域网交换机;

或者路由模式部署，WAN 口配置固定的公网 IP 地址，LAN 口连接局域网交换机。



### 6.2.1.2. 接线规范

- 1、AC 设备 WAN 口连接前置 MODEM 或者光纤收发器，AC 设备 LAN 口连接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.2.1.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10.251.251.251/24、LAN 口子接口: 128.127.125.252/29  
DMZ: 10.252.252.252/24、WAN: 10.250.250.250/24
- 2、配置 AC 设备为路由模式。正确配置 AC 内网 IP 地址和外网 IP 地址，当外网是多条线路

时，根据客户需要选择合适的线路分配策略，然后根据内网的网段来配置代理上网。

- 3、如果使用设备拨号上网，为了保证设备能够成功拨号，操作时，把设备和 Modem 断电（10 秒左右），然后同时开启。
- 4、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan→lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 5、AC 路由模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 6、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 7、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 8、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 9、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 10、实施完毕后需要将设备的配置进行备份。

#### **6.2.1.4. 注意事项**

- 1、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 2、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，否则会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 3、正常情况下禁止直接将设备的 LAN 和 DMZ 两个电口通过交叉线互联，这样连接会导致 AC 恢复到设备的出厂配置，使得原有配置丢失。
- 4、客户如果要求启用自动拨号，请确认在重新启动设备后可以自动拨号，注意重启拨号服务是不能自动拨号的，这点要和客户说明。（这里主要是针对客服人员的，客户不会到后台重启服务）
- 5、内网有服务器，内网需要根据域名方式来访问的，要注意做 LAN-LAN 的端口映射，并且保证服务器看到的源 IP 地址都为设备 LAN IP 地址，使服务器在回包的时候按照原路返

回，具体操作步骤请参照《SINFOR\_AC\_LAN-LAN 端口映射原理》。

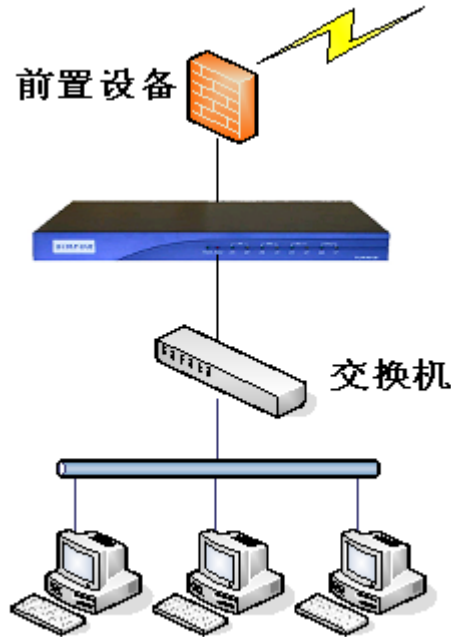
6、设备只支持 ADSL 拨号，其他方式的拨号不支持。

7、在有多个 AC 同时存在的环境下，为了保证准入功能正常使用，应该在最靠近用户的 AC 设备上启用准入。

## 6.2.2. AC 路由模式（通过前置网关设备上网）

### 6.2.2.1. 网络拓扑

环境描述：前置设备做端口映射，AC 设备路由模式部署，WAN 口连接前置网关的内网接口，LAN 口连接内部局域网的交换机。



### 6.2.2.2. 接线规范

- 1、AC 设备 WAN 口接连接前置网关的 LAN 口，AC 设备 LAN 口连接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.2.2.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10.251.251.251/24、 LAN 口子接口: 128.127.125.252/29  
DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24
- 2、配置 AC 设备为路由模式。正确配置 AC 内网 IP 地址和外网 IP 地址，AC 网关设备 WAN 口 IP 地址的网关指向前置设备的内网接口地址。然后根据用户需求和实际网络环境决定是否配置代理上网。
- 3、如果使用设备 VPN 功能，协调客户在前置网关上配置端口映射，将 TCP 和 UDP 4009 端口映射到 VPN 网关设备 WAN 口的地址，并放通前置网关上的防火墙规则。
- 4、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 5、AC 路由模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 6、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 7、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 8、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 9、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 10、实施完毕后需要将设备的配置进行备份。

### 6.2.2.4. 注意事项

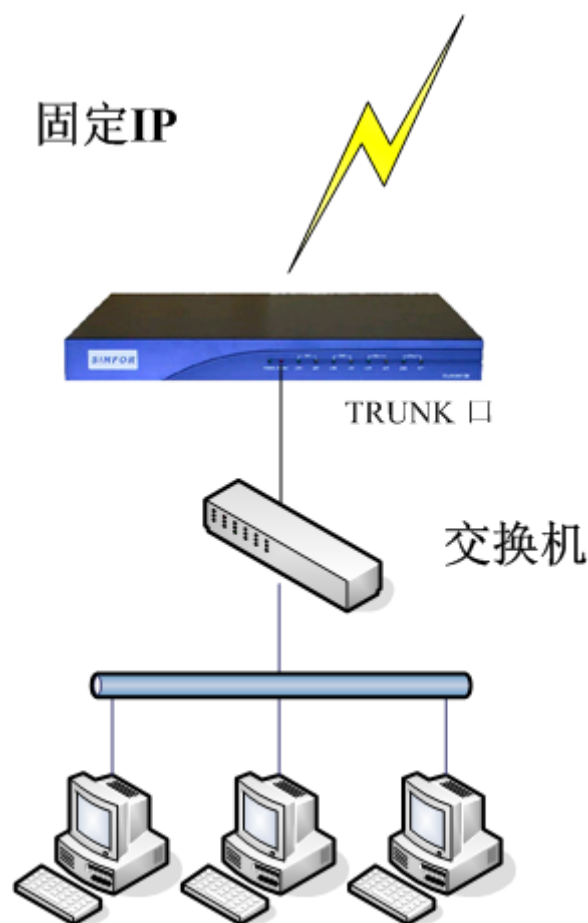
- 1、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 2、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。

- 3、正常情况下禁止直接将设备的 LAN 和 DMZ 两个电口通过交叉线互联，这样连接会导致 AC 恢复到设备的出厂配置，使得原有配置丢失。
- 4、如果使用设备 VPN 功能，协调客户在前置网关上配置端口映射，将 TCP 和 UDP 4009 端口映射到 VPN 网关设备 WAN 口的地址，并放通前置网关上的防火墙规则。
- 5、设备启用 NAT 代理上网，需和客户沟通清楚，并且在路由方式下保证我们设备架上去之后各个路由走向都必需可达。
- 6、在有多个 AC 同时存在的环境下，为了保证准入功能正常使用，应该在最靠近用户的 AC 设备上启用准入。

### 6.2.3. AC 路由模式（支持 VLAN 环境）

#### 6.2.3.1. 网络拓扑

环境描述：设备 WAN 口配置固定的 IP 地址（公网或私网）或 ADSL 拨号，LAN 口连接局域网交换机的 TRUNK 口。



### 6.2.3.2. 接线规范

- 1、AC 设备 WAN 口连接前置设备 LAN 口或 MODEN, AC 设备 LAN 口线连接局域网交换机的 TRUNK 接口。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机或，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.2.3.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10.251.251.251/24、 LAN 口子接口: 128.127.125.252/29  
DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24
- 2、配置 AC 设备为路由模式。正确配置 AC 内网 IP 地址和外网 IP 地址，LAN 口 IP 不能属于任何一个 VLAN。当外网是多条线路时，根据客户需要选择合适的线路分配策略，然后根据内网的网段来配置代理上网。
- 3、在网口配置处配置 VLAN 信息，在 LAN 口设置里面启用 TRUNK，添加内网所有 VLAN 的 VLAN ID 和相应 VLAN 中空闲 IP。
- 4、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 5、AC 路由模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 6、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 7、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 8、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 9、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保

拒绝列表无拦截信息后再关闭直通。

10、实施完毕后需要将设备的配置进行备份。

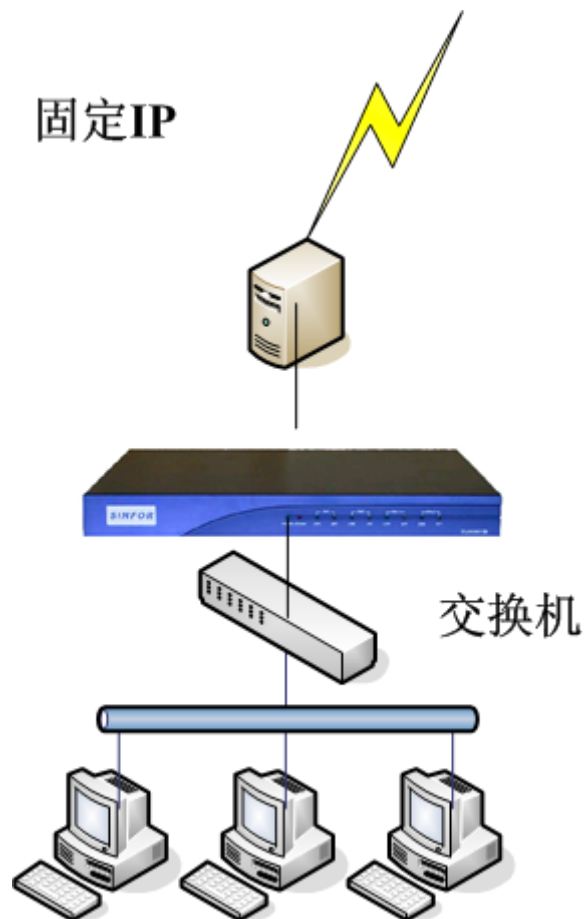
#### **6.2.3.4. 注意事项:**

- 1、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 2、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 3、正常情况下禁止直接将设备的 LAN 和 DMZ 两个电口通过交叉线互联，这样连接会导致 AC 恢复到设备的出厂配置，使得原有配置丢失。
- 4、不支持 VLAN 1。
- 5、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

### **6.2.4. AC 路由模式（内网通过代理服务器上网）**

#### **6.2.4.1. 网络拓扑**

环境描述：AC 设备部署在代理服务器和客户端之间，AC WAN 口连接代理服务器，LAN 口连接局域网交换机



### 6.2.4.2. 接线规范

- 1、AC 设备 WAN 口连接前置 ISA 服务器，AC 设备 LAN 口连接内部局域网交换机。
- 2、如果与设备相连的是 ISA 服务器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.2.4.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10.251.251.251/24、 LAN 口子接口: 128.127.125.252/29  
DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24
- 2、配置 AC 设备为路由模式。正确配置 AC 内网 IP 地址和外网 IP 地址，AC 网关设备 WAN 口 IP 地址的网关指向前置设备的内网接口地址。然后根据用户需求和实际网络环境决定是

否需要配置代理上网。

- 3、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 4、AC 路由模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 5、内网 PC 在 IE 浏览器-INTERNET 选项-连接-局域网设置-代理服务器设置将 AC 的 IP 排除，详细设置请参照《SINFOR\_AC\_案例分析(2009 年度渠道技术培训)\_20090320.ppt》。
- 6、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 7、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 8、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 9、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 10、实施完毕后需要将设备的配置进行备份。

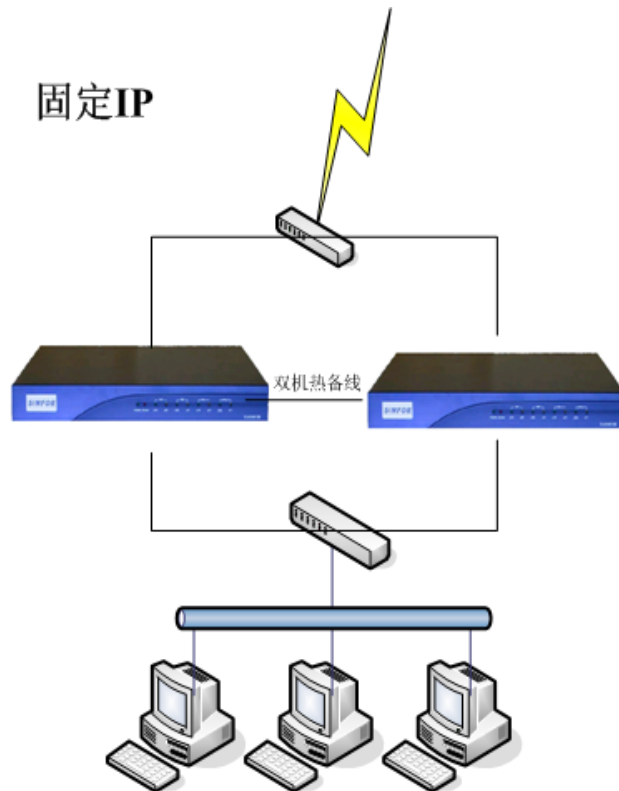
#### **6.2.4.4. 注意事项：**

- 1、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 2、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 3、正常情况下禁止直接将设备的 LAN 和 DMZ 两个电口通过交叉线互联，这样连接会导致 AC 恢复到设备的出厂配置，使得原有配置丢失。
- 4、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

## 6.2.5. AC 路由模式（双机热备）

### 6.2.5.1. 网络拓扑

环境描述：两台 AC 设备，一台做主机运行，一台做备份运行，主机的配置会自动同步到备机上。主机死机或掉电后，备机接替主机工作，起到冗余备份的作用。



### 6.2.5.2. 接线规范

- 1、AC 设备 WAN 口连接前置交换机，AC 设备 LAN 口连接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。
- 5、两台 AC 设备使用串口线连接起来。

### 6.2.5.3. 基本配置规范

- 1、两台 AC 设备使用串口线连接起来。
- 2、先启动其中一台 AC 设备，对该设备进行配置，此设备即为主机。
- 3、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10.251.251.251/24、 LAN 口子接口: 128.127.125.252/29  
DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24
- 4、配置 AC 设备主机为路由模式。正确配置 AC 内网 IP 地址和外网 IP 地址，然后根据内网的实际环境来配置代理上网。
- 5、主设备配置完毕后，再启动另一 AC 设备，后启动的 AC 设备即为备机，备机启动完成后告警灯会有规律的闪烁。备机告警灯有规律闪烁即说明双机已经成功实施，此时主机会自动把配置同步到备机。
- 6、AC 路由模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 7、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 8、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 9、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 10、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 11、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 12、完成实施后把主机电源关闭，测试备机是否能接替主机工作。
- 13、实施完毕后需要将设备的配置进行备份。

### 6.2.5.4. 注意事项

- 1、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交

换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。

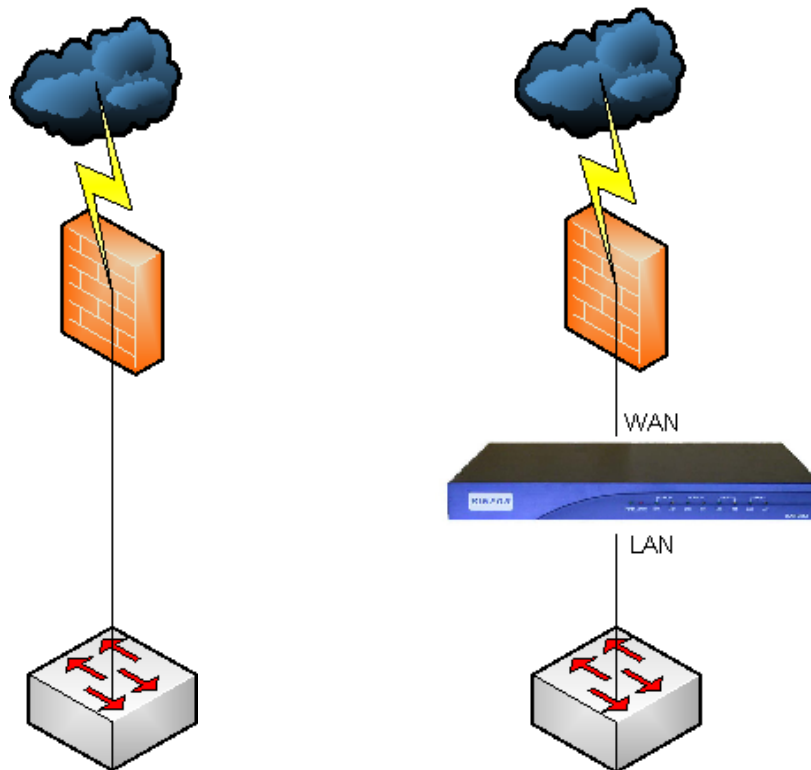
- 2、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 3、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 4、在有多台 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。
- 5、双机设备做升级操作时，尽量先升一台设备，设备运行稳定后再升级另外一台。

## 6.3. AC 网桥模式部署基本配置规范

### 6.3.1. 基本网桥模式配置规范

#### 6.3.1.1. 网络拓扑

环境描述：防火墙 WAN 口连接互联网，LAN 口连接局域网交换机，将设备部署在防火墙和局域网交换机之间。



部署设备前后对比

### 6.3.1.2. 接线规范

- 1、AC 设备 WAN 口接前置网关的 LAN 口，AC 设备 LAN 口接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.3.1.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10.251.251.251/24、LAN 口子接口: 128.127.125.252/29  
DMZ: 10.252.252.252/24、WAN: 10.250.250.250/24
- 2、配置 AC 设备为网桥模式。
  - 1) 配置 AC 网桥 IP，网桥 IP 和前置网关的 LAN 口在同一网段，网关指向前置网关设备的 LAN 口，并正确配置 DNS 服务器地址。
  - 2) 如果设备不需穿透 VLAN，则禁用 VLAN 功能。
  - 3) 选择正确的网桥接口，并放通网口的桥接方向。
- 3、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 4、AC 网桥模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 5、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 6、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 7、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 8、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。

9、实施完毕后需要将设备的配置进行备份。

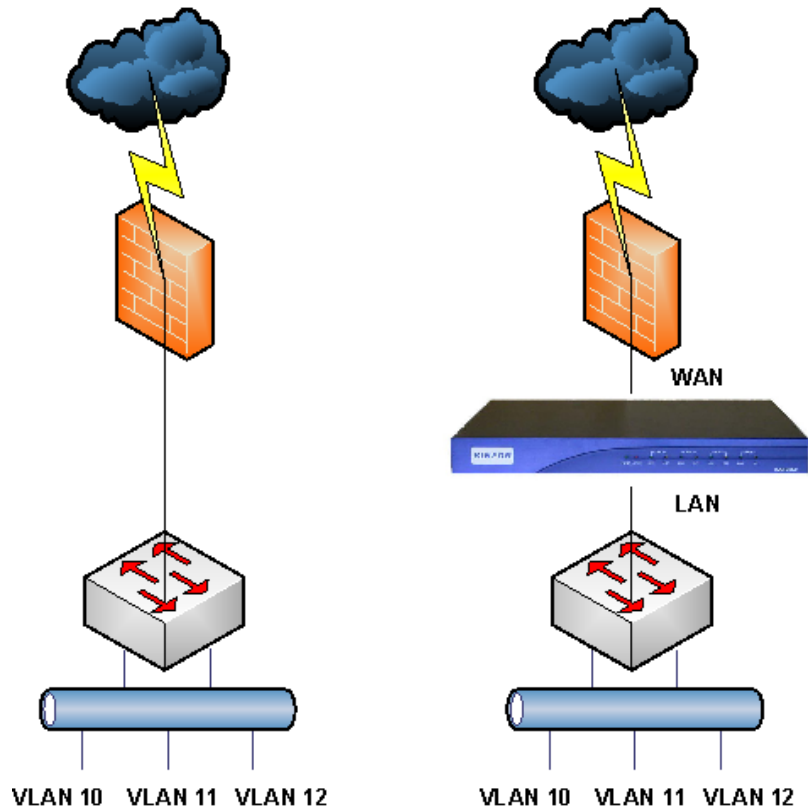
#### **6.3.1.4. 注意事项**

- 1、AC 做网桥模式部署，不要添加 NAT 规则。
- 2、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 3、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 4、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 5、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

### **6.3.2. AC 网桥模式（支持 VLAN 穿透）**

#### **6.3.2.1. 网络拓扑**

环境描述：局域网交换机与防火墙相连的接口启用了 TRUNK。将设备部署在防火墙和局域网交换机之间，设备 WAN 口连接防火墙内网接口，设备 LAN 口连接局域网交换机。



部署设备前后对比

### 6.3.2.2. 接线规范

- 1、AC 设备 WAN 口接前置网关的 LAN 口，AC 设备 LAN 口接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.3.2.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：

LAN: 10.251.251.251/24、LAN 口子接口: 128.127.125.252/29

DMZ: 10.252.252.252/24、WAN: 10.250.250.250/24

- 2、配置 AC 设备为网桥模式。

1) 配置 AC 网桥 IP，网桥 IP 不能属于任何一个 VLAN，并正确配置 DNS 服务器地址。

- 2) AC 网关本身要上外网，网关填任意 VLAN 的网关即可，注意添加 DNS。
- 4) 启用 VLAN 功能，添加内网所有 VLAN 的 VLAN ID 和相应 VLAN 中的空闲 IP。
- 4) 选择正确的网桥接口，并放通网口的桥接方向。
- 3、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 4、AC 网桥模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 5、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 6、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 7、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 8、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 9、实施完毕后需要将设备的配置进行备份。

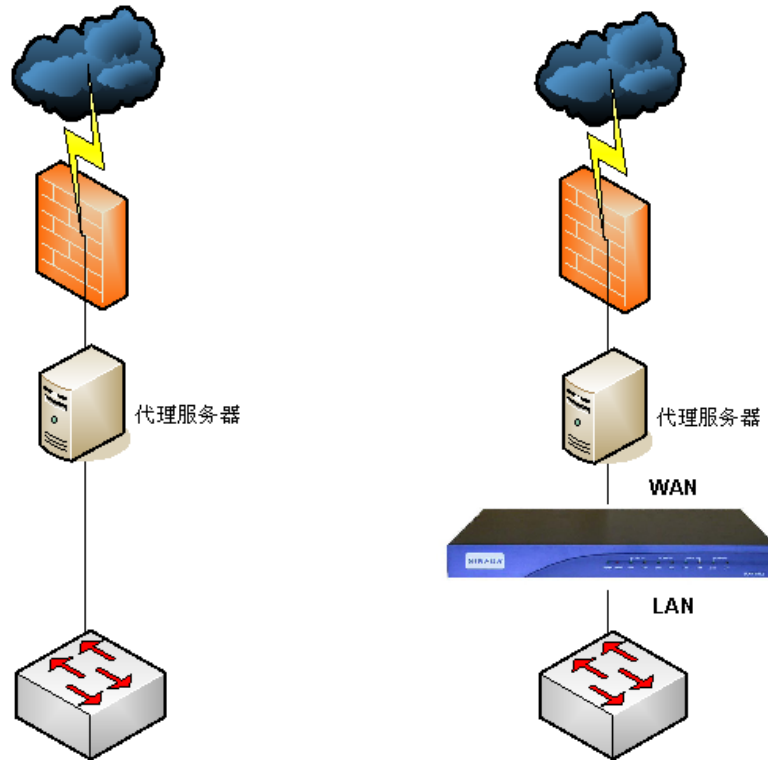
#### **6.3.2.4. 注意事项**

- 1、不支持 VLAN 1
- 2、AC 做网桥模式部署，不要添加 NAT 规则。
- 3、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 4、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 5、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 6、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

### 6.3.3. AC 网桥模式（内网通过代理服务器上网环境一）

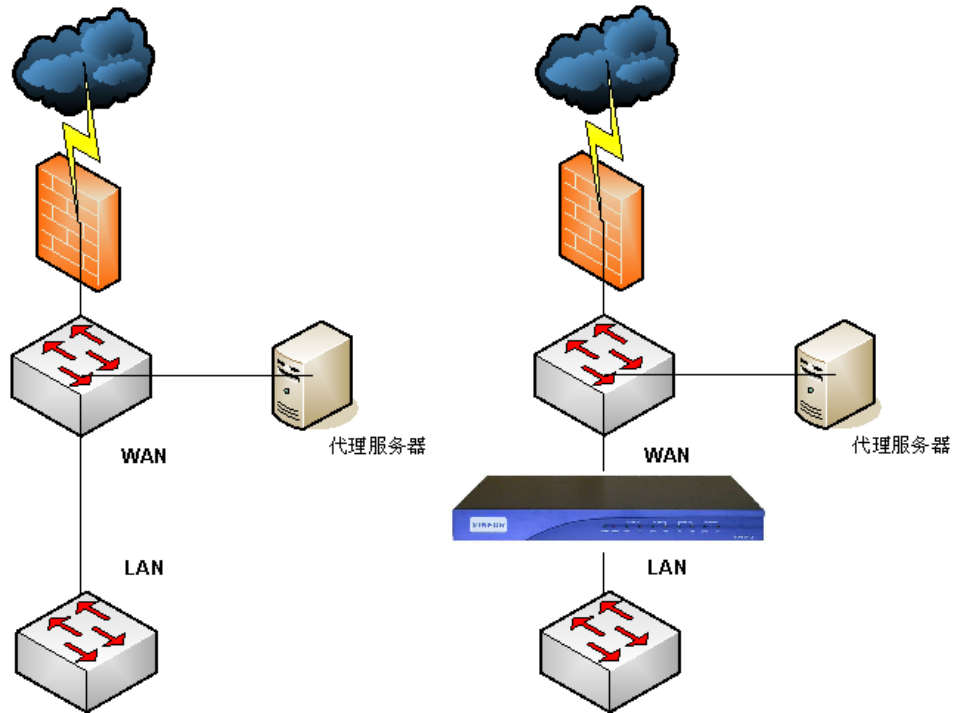
#### 6.3.3.1. 网络拓扑

环境 1 描述：代理服务器路由模式部署在局域网交换机与防火墙之间。将设备部署在代理服务器和局域网交换机之间，设备 WAN 口连接代理服务器内网接口，设备 LAN 口连接局域网交换机。



部署设备前后对比 1

环境 2 描述：代理服务器单臂模式部署。将设备部署在代理服务器和局域网交换机之间，设备 WAN 口与代理服务器方向的交换机相连，设备 LAN 口连接局域网交换机。



部署设备前后对比 2

### 6.3.3.2. 接线规范

- 1、AC 设备 WAN 口接前置交换机或代理服务器，AC 设备 LAN 口接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.3.3.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：
  - LAN: 10.251.251.251/24、 LAN 口子接口: 128.127.125.252/29
  - DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24
- 2、配置 AC 设备为网桥模式。
  - 1) 配置 AC 网桥 IP，网桥 IP 和前置网关的 LAN 口在同一网段，网关指向前置网关设备的 LAN 口，并正确配置 DNS 服务器地址。

- 2) 如果设备不需穿透 VLAN 的则禁用 VLAN 功能。
- 3) 选择正确的网桥接口，并放通网口的桥接方向。
- 3、AC 网桥模式，下面有多个网段时，要在 AC 添加各个网段的回包路由。
- 4、如果设备本身上网也要通过代理服务器，应在系统配置->自动升级选项处配置代理上网的相关信息。
- 5、客户端在 IE 浏览器-INTERNET 选项-连接-局域网设置-代理服务器设置将 AC 的 IP 排除。
- 6、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 7、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 8、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 9、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 10、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 11、实施完毕后需要将设备的配置进行备份。

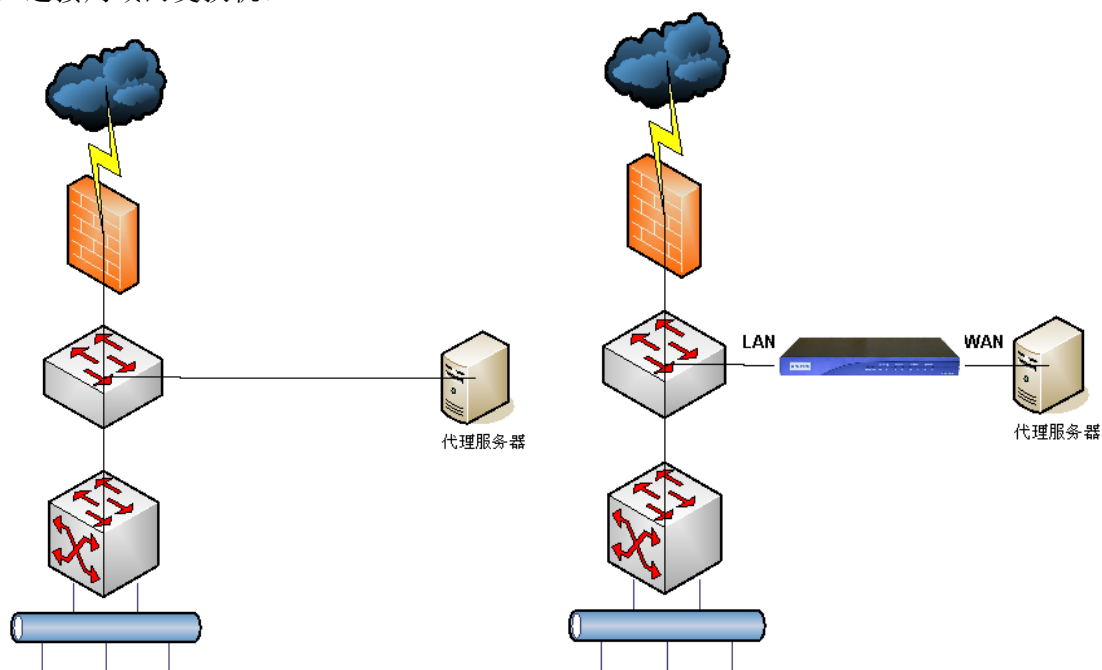
#### **6.3.3.4. 注意事项**

- 1、AC 做网桥模式部署，不要添加 NAT 规则。
- 2、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 3、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 4、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 5、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

## 6.3.4. AC 网桥模式（内网通过代理服务器上网环境二）

### 6.3.4.1. 网络拓扑

环境描述：代理服务器单臂模式部署在局域网交换机与防火墙之间。将设备部署在代理服务器和局域网交换机之间，设备 WAN 口连接代理服务器内网接口，设备 LAN 口连接局域网交换机。



部署设备前后对比

### 6.3.4.2. 接线规范

- 1、AC 设备 WAN 口接代理服务器，AC 设备 LAN 口接内部局域网交换机。
- 2、将设备 WAN 口使用交叉线与代理服务器进行连接；LAN 口用直通线与局域网交换机进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.3.4.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：

LAN: 10.251.251.251/24、LAN 口子接口: 128.127.125.252/29

DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24

- 2、配置 AC 设备为网桥模式。
  - 1) 配置 AC 网桥 IP，网桥 IP 和代理服务器 IP 在同一网段，网关指向设备 LAN 口一侧设备接口的 IP，并正确配置 DNS 服务器地址。
  - 2) 禁用 VLAN 功能。
  - 3) 选择正确的网桥接口，并放通网口的桥接方向。
- 3、AC 网桥模式，下面有多个网段时，要在 AC 添加各个网段的回包路由。
- 4、如果设备本身上网也要通过代理服务器，应在系统配置->自动升级选项处配置代理上网的相关信息。
- 5、客户端在 IE 浏览器-INTERNET 选项-连接-局域网设置-代理服务器设置将 AC 的 IP 排除。
- 6、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 7、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 8、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 9、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 10、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 11、实施完毕后需要将设备的配置进行备份。

#### **6.3.4.4. 注意事项**

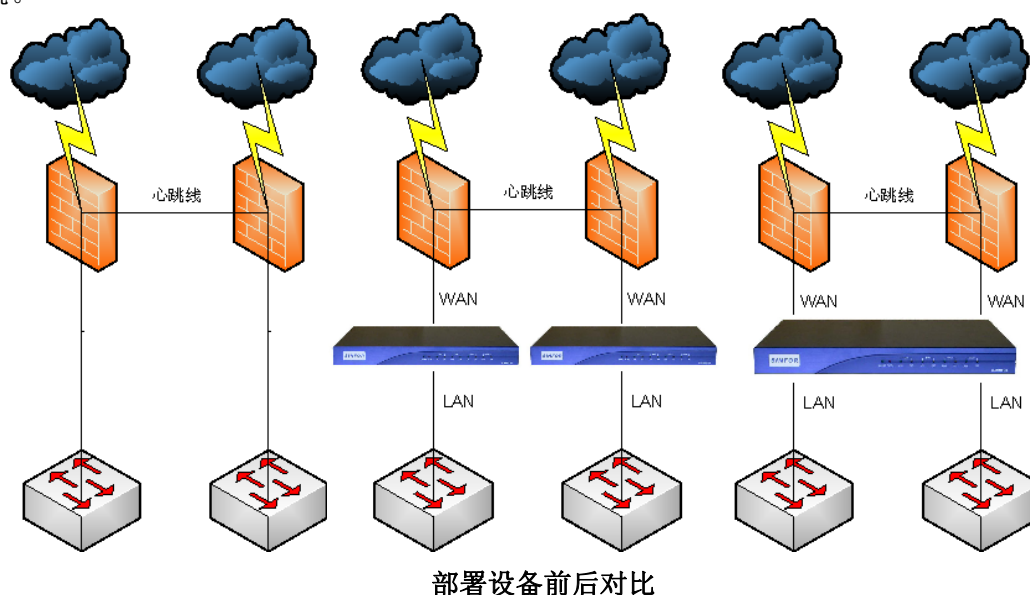
- 1、此部署环境特殊，可能会有公网 IP 地址被当做新用户添加到设备，所以此环境下部署设备时需要联系深信服工程师协助处理。
- 2、AC 做网桥模式部署，不要添加 NAT 规则。
- 3、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。

- 4、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 5、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 6、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

### 6.3.5. AC 网桥模式（前置设备双机热备）

#### 6.3.5.1. 网络拓扑

环境描述：前置设备双机热备，将设备以单网桥或多网桥的方式部署在前置防火墙和局域网交换机之间，设备 WAN 口连接前置防火墙，设备 LAN 口连接局域网交换机。



#### 6.3.5.2. 接线规范

- 1、AC 设备 WAN 口接前置网关的 LAN 口，AC 设备 LAN 口接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.3.5.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10. 251. 251. 251/24、 LAN 口子接口: 128. 127. 125. 252/29  
DMZ: 10. 252. 252. 252/24、 WAN: 10. 250. 250. 250/24
- 2、配置 AC 设备为网桥模式。
  - 1) 配置 AC 网桥 IP，网桥 IP 和前置网关的 LAN 口在同一网段，网关指向前置网关设备的 LAN 口，并正确配置 DNS 服务器地址。
  - 2) 如果设备不需穿透 VLAN 的则禁用 VLAN 功能。
  - 3) 选择正确的网桥接口，并放通网口的桥接方向。
- 3、设备上架前放通相应的防火墙规则。放通前置设备双机热备交互数据包的防火墙规则，建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 4、AC 网桥模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 5、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 6、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 7、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 8、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 9、实施完毕后需要将设备的配置进行备份。

### 6.3.5.4. 注意事项

- 1、此环境下部署设备可能会导致防火墙热备切换不成功，因为有的防火墙只有在检测到接口的灯熄灭后才会进行切换。例如：设备 LAN 口的链路故障，但是 WAN 口的链路还是正常的，导致防火墙不会进行主备的切换。**因此在存在第三方设备双机热备和多网桥的环**

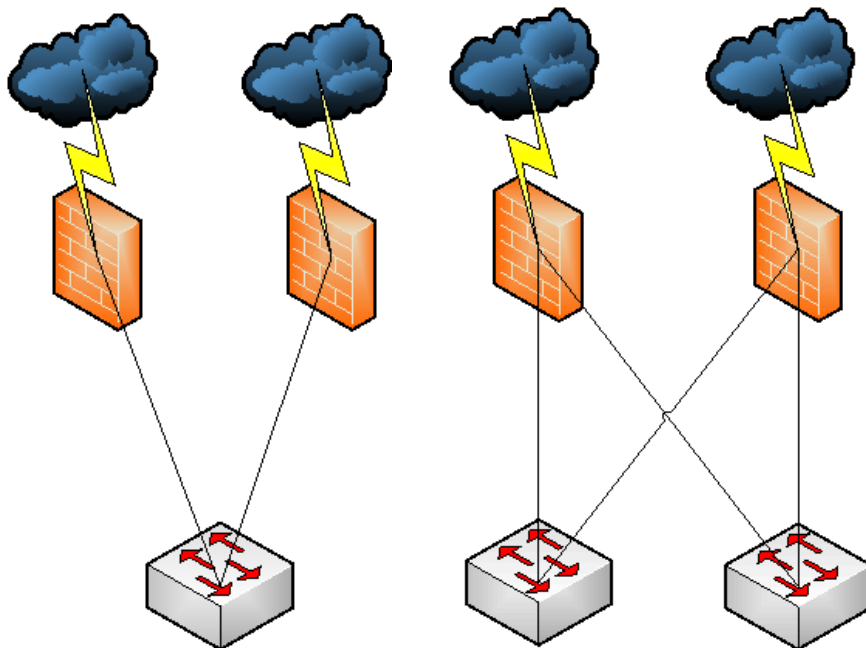
境下，请联系深信服工程师协助处理。

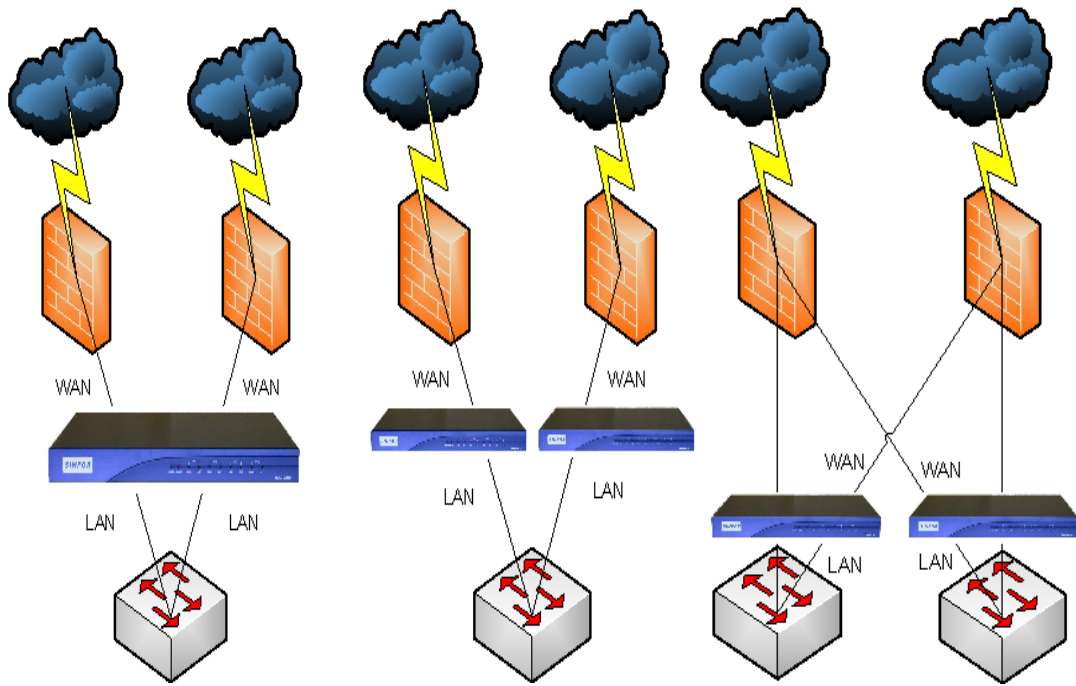
- 2、设备真正的双网桥部署时，两个网桥的 IP 地址不能是同网段的，如果存在冲突，第一对网桥的 IP 地址可以随意配置，第二对网桥配置正确的 IP 地址和网关，此时设备的系统路由会指向第二对网桥的网关地址。
- 3、AC 做网桥模式部署，不要添加 NAT 规则。
- 4、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 5、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 6、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 7、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

## 6.3.6. AC 网桥模式（VRRP 环境）

### 6.3.6.1. 网络拓扑

环境描述：前置设备启用 VRRP 协议，将设备以单网桥或多网桥的方式部署在前置设备和局域网交换机之间，设备 WAN 口连接前置设备，设备 LAN 口连接局域网交换机。





部署设备前后对比

### 6.3.6.2. 接线规范

- 1、AC 设备 WAN 口接前置网关的 LAN 口，AC 设备 LAN 口接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.3.6.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：
  - LAN: 10.251.251.251/24、LAN 口子接口: 128.127.125.252/29
  - DMZ: 10.252.252.252/24、WAN: 10.250.250.250/24
- 2、配置 AC 设备为网桥模式。
  - 1) 配置 AC 网桥 IP，网桥 IP 和前置网关的 LAN 口在同一网段，网关指向前置网关设备的 LAN 口，并正确配置 DNS 服务器地址。
  - 2) 如果设备不需穿透 VLAN 的则禁用 VLAN 功能。

- 3) 选择正确的网桥接口，并放通网口的桥接方向。
- 3、设备上架前放通相应的防火墙规则。放通 VRRP 协议交互数据包的防火墙规则, 建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 4、AC 网桥模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 5、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 6、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 7、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 8、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 9、实施完毕后需要将设备的配置进行备份。

#### 6.3.6.4. 注意事项

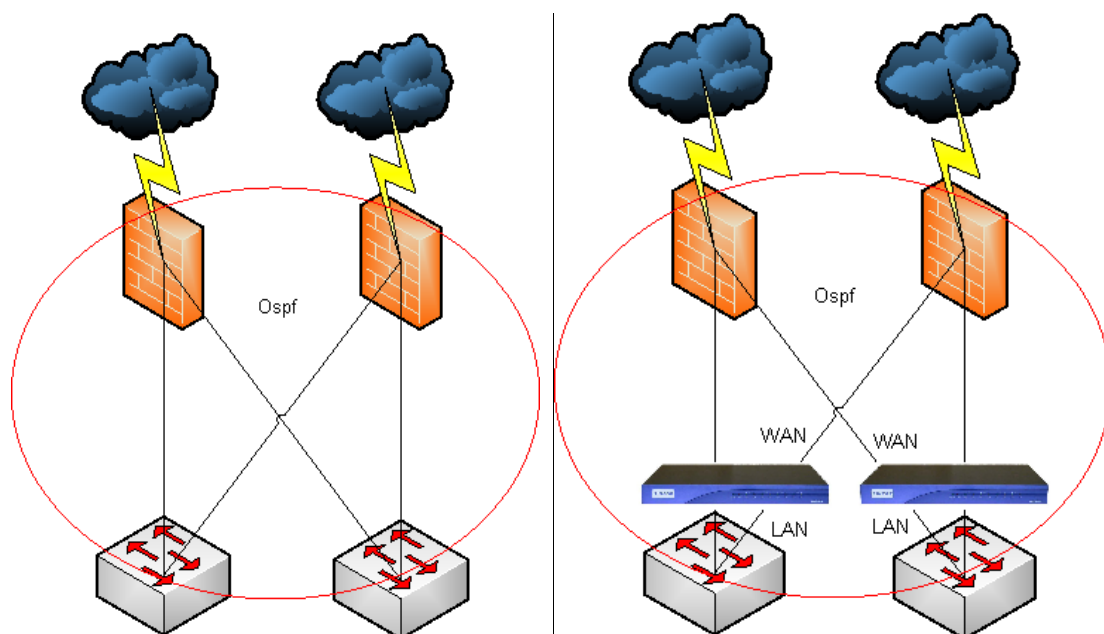
- 1、此环境下部署设备可能会导致 VRRP 主备切换不成功。例如：设备 LAN 口的链路故障，但是 WAN 口的链路还是正常的，此时主备切换就会出现异常，导致两台 VRRP 设备都处于主机的状态。**因此在存在 VRRP 和多网桥的环境下，请联系深信服工程师协助处理。**
- 2、设备真正的双网桥部署时，两个网桥的 IP 地址不能是同网段的，如果存在冲突，第一对网桥的 IP 地址可以随意配置，第二对网桥配置正确的 IP 地址和网关，此时设备的系统路由会指向第二对网桥的网关地址。
- 3、AC 做网桥模式部署，不要添加 NAT 规则。
- 4、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 5、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 6、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。

7、在有多 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

## 6.3.7. AC 网桥模式（穿透动态路由）

### 6.3.7.1. 网络拓扑

环境描述：交换机和前置防火墙之间启用动态路由协议（ospf），将设备以多网桥的方式部署在前置设备和局域网交换机之间，设备 WAN 口连接前置设备，设备 LAN 口连接局域网交换机。



部署设备前后对比

### 6.3.7.2. 接线规范

- 1、AC 设备 WAN 口接前置网关的 LAN 口，AC 设备 LAN 口接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.3.7.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10.251.251.251/24、 LAN 口子接口: 128.127.125.252/29  
DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24
- 2、配置 AC 设备为网桥模式。
  - 1) 配置 AC 网桥 IP，网桥 IP 和前置网关的 LAN 口在同一网段，网关指向前置网关设备的 LAN 口，并正确配置 DNS 服务器地址。
  - 2) 禁用 VLAN 功能。
  - 3) 选择正确的网桥接口，并放通网口的桥接方向。
- 3、设备上架前放通相应的防火墙规则。放通动态路由协议交互数据包的防火墙规则，Ospf: ip 的 89 端口。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。
- 4、AC 网桥模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 5、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 6、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 7、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 8、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 9、实施完毕后需要将设备的配置进行备份。

### 6.3.7.4. 注意事项

- 1、存在多网桥的环境下，请联系深信服工程师协助处理。
- 2、设备真正的双网桥部署时，两个网桥的 IP 地址不能是同网段的，如果存在冲突，第一对网桥的 IP 地址可以随意配置，第二对网桥配置正确的 IP 地址和网关，此时设备的系统

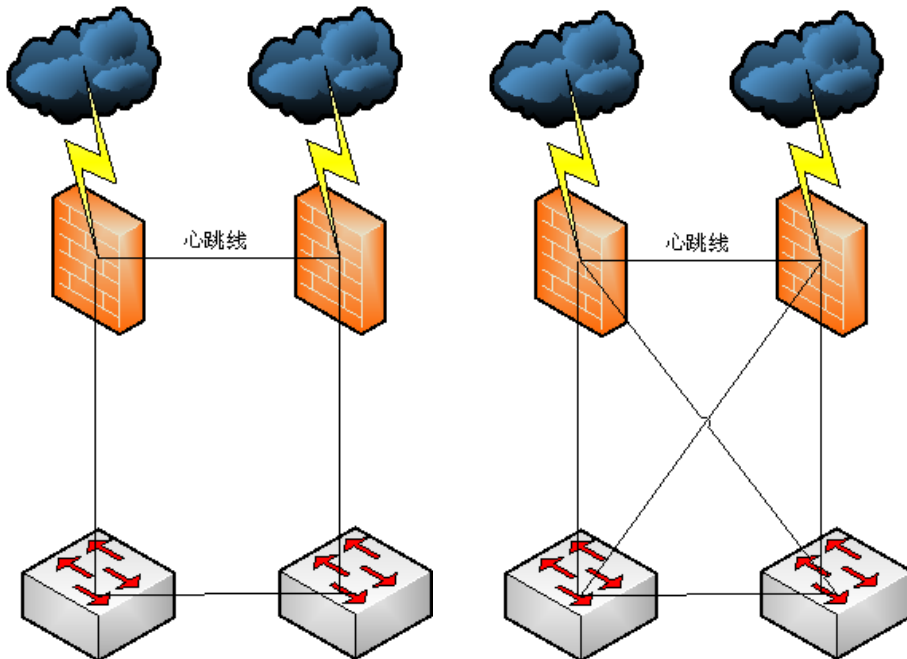
路由会指向第二对网桥的网关地址。

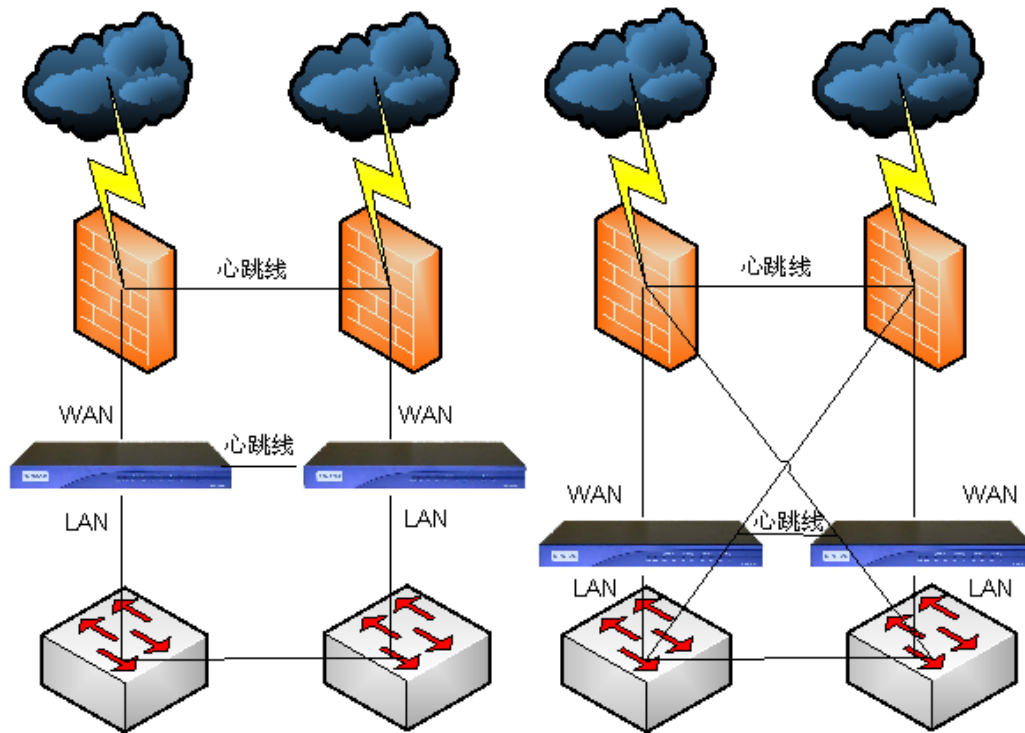
- 3、AC 做网桥模式部署，不要添加 NAT 规则。
- 4、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 5、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 6、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 7、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

## 6.3.8. AC 网桥模式（双机热备环境）

### 6.3.8.1. 网络拓扑

环境描述：前置设备采用双机热备方式部署，AC 设备也采用双机热备方式部署。将设备以单网桥或多网桥的方式部署在前置设备和局域网交换机之间，设备 WAN 口连接前置设备，设备 LAN 口连接局域网交换机。





部署设备前后对比

### 6.3.8.2. 接线规范

- 1、AC 设备 WAN 口连接前置交换机，AC 设备 LAN 口连接内部局域网交换机。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。
- 5、两台 AC 设备使用串口线连接起来。

### 6.3.8.3. 基本配置规范

- 1、两台 AC 设备使用串口线连接起来。
- 2、先启动其中一台 AC 设备，对该设备进行配置，此设备即为主机。主设备配置完毕后再启动另一 AC 设备，后启动的 AC 设备即为备机，备机启动完成后告警灯会有规律的闪烁。备机告警灯有规律闪烁即说明双机已经成功实施，此时主机会自动把配置同步到备机。
- 3、通过默认 IP 登录设备，设备接口默认的 IP 地址为：

LAN: 10.251.251.251/24、 LAN 口子接口: 128.127.125.252/29

DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24

#### 4、配置 AC 设备为网桥模式。

1) 配置 AC 网桥 IP, 网桥 IP 和前置网关的 LAN 口在同一网段, 网关指向前置网关设备的 LAN 口, 并正确配置 DNS 服务器地址。

2) 禁用 VLAN 功能。

3) 选择正确的网桥接口, 并放通网口的桥接方向。

#### 5、设备上架前放通相应的防火墙规则。放通前置设备双机热备交互数据包的防火墙规则。

建议客户不要放通防火墙规则 wan->lan 的所有数据, 只放通需要通过的数据即可, 因为放通 wan 到 lan 的规则, AC 无法识别 P2P 的反向连接行为特征, 无法对这种反向连接进行流控。

#### 6、AC 网桥模式, 下面有多个网段时, 要在 AC 中添加各个网段的回程路由。

7、设备上架以后, 建议通过升级客户端登陆设备, ping 外网地址, ping 内网设备地址, 看是否有丢包现象; 查看网卡工作状态, 是否有错误包等, 是否适应为全双工, 是否需要锁定网口, 判断是否存在兼容性问题; 查看设备路由表, arp 表是否正确。

8、开启网关自动升级和各种规则的自动升级, 保证设备的规则得到及时的更新, 使设备工作在最佳状态。

9、开放内网服务器和网络设备的全部上网权限, 保证服务器和网络设备的正常运行。

10、为了保证设备平稳的接入到网络中, 设备上架前先将设备开直通, 查看拒绝列表, 确保拒绝列表无拦截信息后再关闭直通。

11、完成实施后把主机电源关闭, 测试备机是否能接替主机工作。

12、实施完毕后需要将设备的配置进行备份。

### 6.3.8.4. 注意事项

1、AC 做网桥模式部署, 不要添加 NAT 规则。

2、此环境下要保证网络内其他的热备设备和 AC 设备能够达到同步的切换。

3、AC 网关开启防 DOS 攻击时, 如果 AC 网关设备下面接三层交换机或者路由器, 将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。

4、内网有三层交换机的情况下, 自动认证用户后不要选择绑定 IP/MAC 或 MAC, 不然会把三

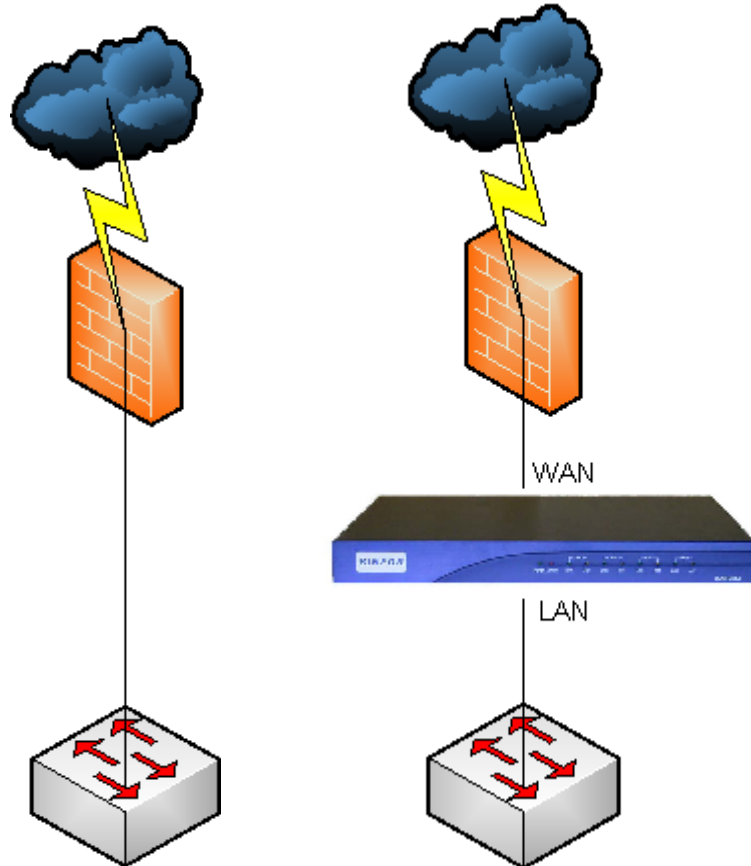
层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。

- 5、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 6、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。
- 7、双机设备做升级操作时，尽量先升一台设备，设备运行稳定后再升另外一台。

### 6.3.9. AC 网桥部署（启用 Bypass 功能）

#### 6.3.9.1. 网络拓扑

环境描述：设备网桥模式部署，将设备部署在防火墙和局域网交换机之间，WAN 口连接前置防火墙，LAN 口连接局域网交换机，并启用 Bypass 功能。



部署设备前后对比

#### 6.3.9.2. 接线规范

- 1、Bypass 只在 LAN 和 WAN 一对网口之间有效，因此 AC 设备 WAN 口接前置网关的 LAN 口，

AC 设备 LAN 口接内部局域网交换机。

- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。

### 6.3.9.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：

LAN: 10.251.251.251/24、 LAN 口子接口: 128.127.125.252/29

DMZ: 10.252.252.252/24、 WAN: 10.250.250.250/24

- 2、配置 AC 设备为网桥模式。

- 1) 配置 AC 网桥 IP，网桥 IP 和前置网关的 LAN 口在同一网段，网关指向前置网关设备的 LAN 口，并正确配置 DNS 服务器地址。

- 2) 如果设备不需穿透 VLAN 的则禁用 VLAN 功能。

- 3) 选择正确的网桥接口，并放通网口的桥接方向。

- 3、设备上架前放通相应的防火墙规则。建议客户不要放通防火墙规则 wan->lan 的所有数据，只放通需要通过的数据即可，因为放通 wan 到 lan 的规则，AC 无法识别 P2P 的反向连接行为特征，无法对这种反向连接进行流控。

- 4、AC 网桥模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。

- 5、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。

- 6、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。

- 7、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。

- 8、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。

- 9、完成实施后把设备电源关闭，测试 Bypass 功能是否生效。

- 10、实施完毕后需要将设备的配置进行备份。

#### 6.3.9.4. 注意事项

- 1、设备只有在 LAN 口和 WAN 口一对网口之间存在 Bypass 的功能，所以接线的时候只能接 LAN 口和 WAN 口。
- 2、AC 做网桥模式部署，不要添加 NAT 规则。
- 3、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 4、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 5、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 6、在有多个 AC 同时存在的环境下，应该在最靠近用户的 AC 设备上启用准入。

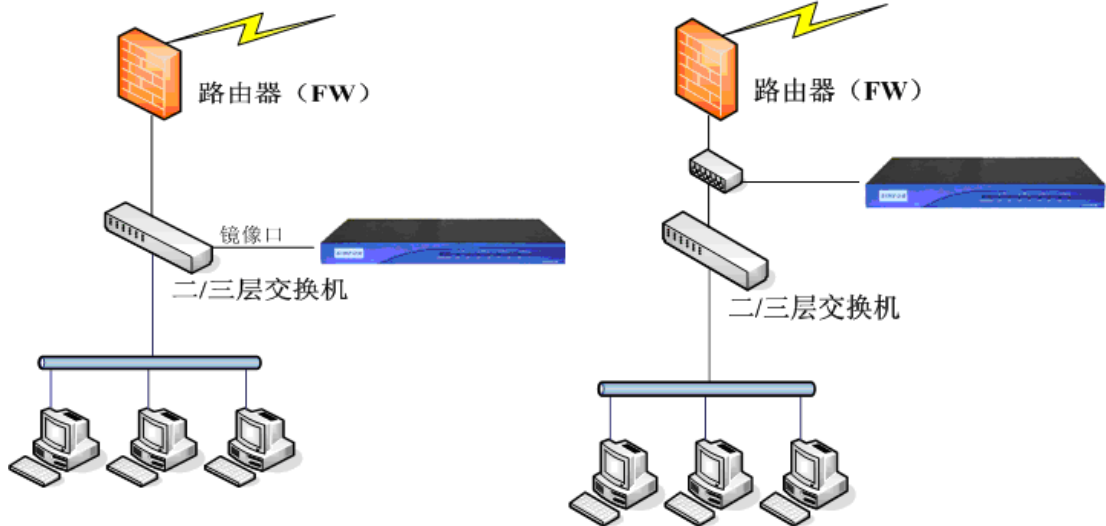
### 6.4. AC 旁路模式部署基本配置规范

AC 设备非 DMZ 口的网口接内部局域网交换机镜像口或者 HUB。首选使用 LAN 口监听交换机镜像口。

#### 6.4.1. 基本旁路模式配置规范

##### 6.4.1.1. 网络拓扑

环境描述：设备旁路模式部署，LAN 口或 WAN 口连接交换机的镜像接口，或者用 LAN 口连接 HUB 接口。



### 6.4.1.2. 接线规范

- 1、AC 设备 WAN 口或者 LAN 口接交换机的镜像口，如果交换机不支持镜像功能，可以通过添加 HUB 的方式来部署设备，但是设备的 WAN 口不能连接 HUB.
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。
- 5、将 DMZ 接口连接到内网的交换机接口上，保证设备能通过 DMZ 口来上网，并通过 DMZ 口来管理设备。

### 6.4.1.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：
  - LAN: 10.251.251.251/24、LAN 口子接口: 128.127.125.252/29
  - DMZ: 10.252.252.252/24、WAN: 10.250.250.250/24
- 2、配置 AC 设备为旁路模式。
  - 1) 配置管理接口 (DMZ 口) 的 IP 地址、网关和 DNS 服务器地址，确保设备能够通过 DMZ 接口来上网和管理设备。
  - 2) 配置监控网段列表和监控服务器列表。
  - 3) 根据需求配置排除 IP 地址列表。

- 3、AC 网桥模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 4、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 5、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 6、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 7、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 8、实施完毕后需要将设备的配置进行备份。

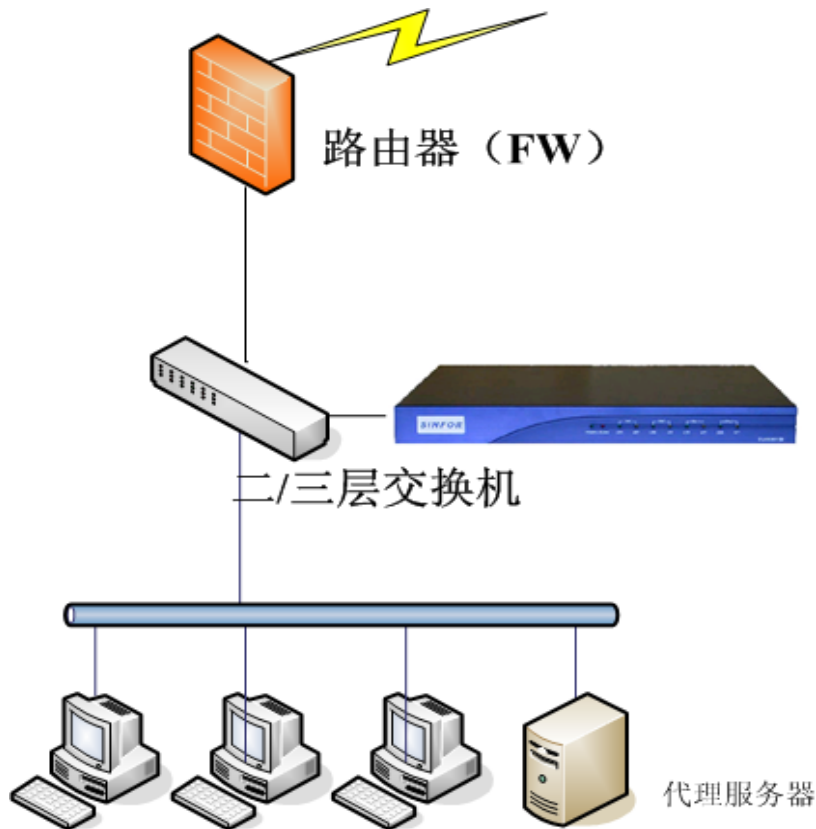
#### **6.4.1.4. 注意事项**

- 1、为了保证稳定性，AC 网关的 WAN 口不准接 HUB。
- 2、M5600 以上 AC，内网数据量大的情况下，为了保证设备能及时处理用户的上网数据，要分上下行链路分别接入设备的两个监听接口。
- 3、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 4、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 5、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。

### **6.4.2. AC 旁路模式（通过代理服务器上网环境）**

#### **6.4.2.1. 网络拓扑**

环境描述：设备旁路模式部署，LAN 口或 WAN 口连接交换机的镜像接口或用 LAN 口连接 HUB 接口。



### 6.4.2.2. 接线规范

- 1、AC 设备 WAN 口或者 LAN 口接交换机的镜像口，如果交换机不支持镜像功能，可以通过添加 HUB 的方式来部署设备，但是设备的 WAN 口不能连接 HUB。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。
- 5、将 DMZ 接口连接到内网的交换机接口上，保证设备能通过 DMZ 口来上网，并通过 DMZ 口来管理设备。

### 6.4.2.3. 基本配置规范

- 1、通过默认 IP 登录设备，设备接口默认的 IP 地址为：

LAN: 10.251.251.251/24、LAN 口子接口: 128.127.125.252/29

DMZ: 10.252.252.252/24、WAN: 10.250.250.250/24

- 2、配置 AC 设备为旁路模式。
  - 1) 配置管理接口 (DMZ 口) 的 IP 地址、网关和 DNS 服务器地址, 确保设备能够通过 DMZ 接口来上网和管理设备。
  - 2) 配置监控网段列表和监控服务器列表。
  - 3) 根据需求配置排除 IP 地址列表。
- 3、AC 网桥模式, 下面有多个网段时, 要在 AC 中添加各个网段的回程路由。
- 4、设备上架以后, 建议通过升级客户端登陆设备, ping 外网地址, ping 内网设备地址, 看是否有丢包现象; 查看网卡工作状态, 是否有错误包等, 是否适应为全双工, 是否需要锁定网口, 判断是否存在兼容性问题; 查看设备路由表, arp 表是否正确。
- 5、开启网关自动升级和各种规则的自动升级, 保证设备的规则得到及时的更新, 使设备工作在最佳状态。
- 6、开放内网服务器和网络设备的全部上网权限, 保证服务器和网络设备的正常运行。
- 7、为了保证设备平稳的接入到网络中, 设备上架前先将设备开直通, 查看拒绝列表, 确保拒绝列表无拦截信息后再关闭直通。
- 8、实施完毕后需要将设备的配置进行备份。

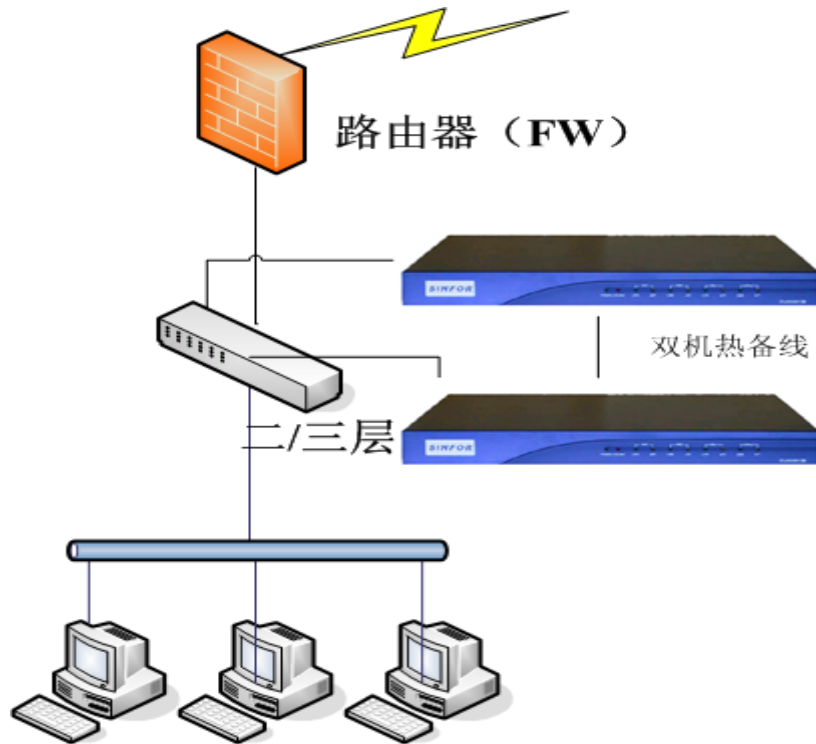
#### **6.4.2.4. 注意事项**

- 1、为了保证稳定性, AC 网关的 WAN 口不准接 HUB。
- 2、M5600 以上 AC, 内网数据量大的情况下, 为了保证设备能及时处理用户的上网数据, 要分上下行链路分别接入设备的两个监听接口。
- 3、AC 网关开启防 DOS 攻击时, 如果 AC 网关设备下面接三层交换机或者路由器, 将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 4、内网有三层交换机的情况下, 自动认证用户后不要选择绑定 IP/MAC 或 MAC, 不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定, 导致全网中断。
- 5、正常情况下禁止直接将设备的两个电口用交叉线互联, 因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置, 导致原有配置丢失。

### 6.4.3. AC 旁路模式（双机热备环境）

#### 6.4.3.1. 网络拓扑

环境描述：设备旁路模式部署，LAN 口或 WAN 口连接交换机的镜像接口或用 LAN 口连接 HUB 接口。两台设备做双机热备，主机死机或掉电后，备机接替主机工作，起到冗余备份的作用。



#### 6.4.3.2. 接线规范

- 1、AC 设备 WAN 口或者 LAN 口接交换机的镜像口，如果交换机不支持镜像功能，可以通过添加 HUB 的方式来部署设备，但是设备的 WAN 口不能连接 HUB。
- 2、如果与设备相连的是防火墙或路由器，使用交叉线进行连接；如果与设备相连的是交换机，使用直通线进行连接。
- 3、网线连接设备任意网口的时候，要听到“咔”的一声，表示网线和设备已经连接好了。
- 4、网线与设备的接口连接以后，设备的 Link 灯常亮，Act 灯闪烁，表示接口正常工作。
- 5、将 DMZ 接口连接到内网的交换机接口上，保证设备能通过 DMZ 口来上网，并通过 DMZ 口来管理设备。
- 6、两台 AC 设备使用串口线连接起来。

### 6.4.3.3. 基本配置规范

- 1、两台 AC 设备使用串口线连接起来。
- 2、先启动其中一台 AC 设备，对该设备进行配置，此设备即为主机。主设备配置完毕后再启动另一 AC 设备，后启动的 AC 设备即为备机，备机启动完成后告警灯会有规律的闪烁。备机告警灯有规律闪烁即说明双机已经成功实施，此时主机会自动把配置同步到备机。
- 3、通过默认 IP 登录设备，设备接口默认的 IP 地址为：  
LAN: 10.251.251.251/24、LAN 口子接口: 128.127.125.252/29  
DMZ: 10.252.252.252/24、WAN: 10.250.250.250/24
- 4、配置 AC 设备为旁路模式。
  - 1) 配置管理接口 (DMZ 口) 的 IP 地址、网关和 DNS 服务器地址，确保设备能够通过 DMZ 接口来上网和管理设备。
  - 2) 配置监控网段列表和监控服务器列表。
  - 3) 根据需求配置排除 IP 地址列表。
- 5、AC 网桥模式，下面有多个网段时，要在 AC 中添加各个网段的回程路由。
- 6、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象；查看网卡工作状态，是否有错误包等，是否适应为全双工，是否需要锁定网口，判断是否存在兼容性问题；查看设备路由表，arp 表是否正确。
- 7、开启网关自动升级和各种规则的自动升级，保证设备的规则得到及时的更新，使设备工作在最佳状态。
- 8、开放内网服务器和网络设备的全部上网权限，保证服务器和网络设备的正常运行。
- 9、为了保证设备平稳的接入到网络中，设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 10、完成实施后把主机电源关闭，测试备机是否能接替主机工作。
- 11、实施完毕后需要将设备的配置进行备份。

### 6.4.3.4. 注意事项

- 1、DMZ 口的接入内网某一 VLAN 并设置 DMZ 口的 IP，确保设备能上外网。
- 2、AC 网关的 WAN 口不准接 HUB。

- 3、M5600 以上 AC，内网数据量大的情况下要分上下行链路分别接入设备的两个监听接口。
- 4、AC 网关开启防 DOS 攻击时，如果 AC 网关设备下面接三层交换机或者路由器，将三层交换机或路由器与 AC 网关接口的 IP 和 MAC 填入内网路由器列表。
- 5、内网有三层交换机的情况下，自动认证用户后不要选择绑定 IP/MAC 或 MAC，不然会把三层交换机接口的 MAC 和内网一个 PC 的 IP 绑定，导致全网中断。
- 6、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 7、正常情况下禁止直接将设备的两个电口用交叉线互联，因为 AC 在将两个电口直接连接的时候会恢复到设备的出厂配置，导致原有配置丢失。
- 8、设备上架以后，建议通过升级客户端登陆设备，ping 外网地址，ping 内网设备地址，看是否有丢包现象，ping 大包，判断是否存在兼容性问题。
- 9、使用 ifconfig 等命令，查看网卡工作状态，是否有错误包等，查看设备路由表，arp 表是否正确。
- 10、百兆网口使用 mii-tool 命令查看设备适应模式，千兆网口使用 ethtool 命令查看接口模式，是否适应为全双工，是否需要锁定网口。
- 11、开放内网服务器和其他网络设备的全部上网权限，保证服务器和其他网络设备的正常运行。
- 12、设备上架前先将设备开直通，查看拒绝列表，确保拒绝列表无拦截信息后再关闭直通。
- 13、双机设备做升级操作时，尽量先升一台设备，设备运行稳定后再升另外一台。

## 7. 紧急事件处理规范

- 1、处理原则：在故障持续时间和规模上尽量减小对客户的影响，如果客户承载的是核心业务系统，通过一切有效手段来优先恢复客户的网络。  
若设备上架后导致整个内网上网异常，5 分钟内无法定位问题，如设备网桥模式部署，则设备断电 BYPASS；如设备网关模式部署，则先把设备下架，恢复客户以前网络原样。
- 2、准备 2 根备用跳线，便于快速恢复到原来网络状态。
- 3、当发现网络通讯异常时，先对设备开启直通，如果此时网络正常，则迅速检查并调整设备的配置；如果开直通后网络故障仍然存在，向客户争取调试时间，在客户允许的情况下进行调试，如果客户要求马上恢复网络，则先把设备下架，恢复客户以前网络原样。

- 4、当网络可以通讯，但是设备有网口发现有错误的数据包或者丢弃的数据包时，查看设备网口适应模式，尝试锁定网口工作模式进行调整。

## 8. 常见问题处理规范

### 1、将 AC 设备架入网络后，内网的用户上不了网

- a、在【策略故障排除】处开启直通，观察开启直通后观察是否可以上网，如果开直通就好了，请查看拒绝列表，看是被设备的哪个模块拒绝的，然后调整相应的设置。如果开启直通还是不可以上网请检查第二步。
- b、确认上网数据经过 AC。
- c、检查 AC 的配置是否有误，您需要检查的配置包括防火墙规则、NAT 规则、防 DOS 攻击设置以及回包路由等。
- d、检查客户端的配置，您需要检查的配置包括电脑网关、电脑路由、个人防火墙设置、代理以及 DNS 等。
- e、确认公网线路是否正常，如果 AC 做路由模式或者网桥模式，您可以通过登录网关升级维护客户端，从 AC 设备进行简单的 ping 公网的操作，看是否是公网线路的问题。
- f、检查 AC 和直连设备的兼容性，您可以登录网关升级维护客户端，查看【工具】-【查看网络配置】，看内外网口是否有很多错误的数据包，如果有的话可能是设备之间兼容性的问题，请设置并调整网卡的工作模式，通过【工具】-【设置网卡工作模式】来设置。
- g、查看 AC 的【系统日志】看是否有错误提示。
- h、明确网络拓扑，确认拓扑是否有问题。

### 2、某些应用不能正常访问

- a、在【策略故障排除】处开启直通，观察开启直通后观察应用是否可以正常使用，如果开直通就好了，请查看拒绝列表，看是被设备的哪个模块拒绝的，然后调整相应的设置。如果开启直通还是不可以访问请检查第二步。
- b、确认上网数据经过 AC。
- c、检查 AC 的配置是否有误，您需要检查的配置包括防火墙规则、NAT 规则、防 DOS 攻击设置以及回包路由等。
- d、检查客户端的配置，您需要检查的配置包括电脑网关、电脑路由、个人防火墙设置、代理以及 DNS 等。

- e、检查 AC 的策略路由是否配置错误，遇到类似网上银行之类的应用，因为服务器端可能存在检查源 IP 的机制，当有多条线路时，会存在访问 IP 不一样的问题，导致应用访问不了，这时需要设置策略路由指定从固定的一条线路去访问此类应用。
- f、查看 AC 的【系统日志】看是否有错误提示。
- g、尝试绕过 AC 访问看是否正常。

### 3、经过 AC 访问公网速度变慢

- a、从内网电脑上 ping 及下载测试，判断速度是否较慢。
- b、通过网关升级维护系统登录 AC 设备，从 AC 上 ping，测试速度是否较慢。
- c、在【策略故障排除】处开启直通，观察开启直通后是否速度会变快，查看拒绝列表看数据是由设备的哪个模块丢弃的，建议设置开启条件，设置源、目标 IP 等，缩小记录的拒绝内容便于快速定位问题。
- d、单机接 AC，看是否还存在较慢的问题。
- e、检查公网带宽，看是否是带宽被耗尽了，如果是这种情况，建议做适当的流控，保证正常业务的数据传输。
- f、检查 AC 的性能是否足够，您可以查看设备的 CPU 占用率是否一直持续较高，另外实际带宽值是否超过了设备所能支持的带宽值，AC 设备各种型号支持的带宽值您可以参考 sinfor 网站上发布的参数。
- g、开启防 DOS 攻击，看内网是否有攻击。
- i、检查 AC 和直连设备的兼容性，您可以登录网关升级维护客户端，查看【工具】-【查看网络配置】，看内外网口是否有很多错误的数据包，如果有的话可能是设备之间兼容性的问题，请设置并调整网卡的工作模式，通过【工具】-【设置网卡工作模式】来设置。

### 4、觉得 AC 不稳定，CPU 占用率很高

- a、检查 AC 的性能是否足够，您可以查看实际带宽值是否超过了设备所能支持的带宽值，实际会话数是否超过设备 AC 设备各种型号支持的带宽值您可以参考 sinfor 网站上发布的参数。
- b、查看 AC 的【系统日志】看是否有错误提示或攻击报警。
- c、开启防 DOS 攻击，看内网是否有攻击。
- d、试着关闭一些比较耗性能的功能，比如网关杀毒、网页内容审计、未知应用审计、流量控制等。

## 5、某些应用识别不了或者某些业务封堵不了

- a、确认数据经过 AC。
- b、确认应用识别库已经更新到最新的规则库。
- c、确认此应用对应的应用识别规则没有被禁用。
- c、检查配置的策略是否正确。
- d、开启审计所有应用和审计未知应用，再次访问此应用，然后查看数据中心日志对应的记录，看此应用是否识别出来，如果识别成“其他”或者误判，请联系深圳客服中心，我们会提交情况给研发，由研发修改相应的规则。

## 6、封堵了迅雷但还是可以用迅雷下载

- a、确认数据经过 AC。
- b、确认应用识别库已经更新到最新的规则库。
- c、确认迅雷下载相关的应用规则没有被禁用，迅雷下载可能使用的规则包括：文件下载类型中的迅雷资源、多线程下载、大文件下载规则、P2P 类型中的 BT 规则。（大文件下载规则是针对 http\_get 单线程下载设置的规则，通过 http\_get 下载大于 1M 的文件都会识别为大文件下载。）
- d、确认以上规则都设置了封堵策略。
- e、如果需要做迅雷的流控，请注意除了以上规则需要流控外，还需要对智能识别中的“P2P 行为”流控。

## 7、封了所有的 P2P，但是仍然有 P2P 的流量

- a、P2P 包括智能识别中的“P2P 行为”，当“P2P 行为”的识别灵敏度设置为“中”或者“低”时，对于一部分可能误判的数据设备只是标识为“P2P 行为”但是不做控制。
- b、一部分 P2P 行为可能是反向，由外网连接内网的，对于这种反向的 P2P 连接，AC 设备无法识别，建议默认情况下不要放通防火墙中 WAN→LAN 的规则。

## 8、AC 无法更新内置库规则

- a、确认 AC 的内置库升级序列号没有过期。
- b、如果使用代理升级，请确认代理服务器和用户名等信息是否填写正确，AC 是否可以正常连接到代理服务器。
- c、确认 AC 可以正常访问到选择的升级服务器。简单的判断方法，您可以登录网关升级维护客户端，点击【工具】-【ping】，输入服务器的 IP 地址，看是否可以 ping 通服务器。

## 9. 测试/实施完成后扫尾规范

### 1、检查工作

- 1、查看网卡有没有 errors, dropped 的包。
- 2、查看 CPU 占用情况。
- 3、查看设备是否可以ping [www.sinfors.com.cn](http://www.sinfors.com.cn)
- 4、检查识别库是否最新。
- 5、检查 FW 策略是否全放通（如客户没有要求，直接全通包括协议号：0）。
- 6、VRRP 环境请不要开启防 DOS。
- 7、查看在线用户列表是否是正常的内网 IP。
- 8、查看流量识别未识别流量是否在正常范围之内。

### 2、备份工作

开始备份，登陆网关控制台备份配置。

建议命名规则比如 ptac-ac-1.9-20090407-b,备份完成之后，自己备份，另外提交给客户。

### 3、整理工作

在条件允许下将设备连接线路做上标签。

处理因实施产生的垃圾。

整理好包装箱及泡沫装好让客户放到合适的位置。