



TrendMicro CDC Enterprise Document

IWSVA 5.6 部署及上线测试配置手册

Document Version 1.5



Update History

Revision #	Revised By	Date of Change	Changes
1.0	Vincent Zhang	2012-11-29	First draft
1.1	Vincent Zhang	2012-12-12	增加半透明模式部署
1.2	Zachary Xu	2012-12-22	增加双链路模式部署
1.5	Vincent Zhang	2013-4-11	增加双链路部署

TABLE OF CONTENTS

1. 简介	1
2. 客户环境检查	2
2.1. 单链路网络部署	2
2.1.1 IWSA透明模式	2
1) IWSA两段式连接	2
2) 透明模式部署局限性	2
2.1.2 简单透明模式	4
2.1.3 WCCP模式	4
2.2. 双链路网络部署	4
2.2.1 常见问题	4
2.2.1.1 非对称路由	4
1) 问题描述	5
2) 非对称路由情况下的IWSA透明模式部署问题	5
3) 解决方案（半透明模式或双链路模式）	6
2.2.1.2 客户端交换机MAC浮动	7
2.2.1.3 服务器端MAC浮动	7
1) 问题描述	7
2) 解决方案	7
2.3. 交叉链路和聚合链路	7
2 网络信息配置	8
2.2 基本配置	8
2.3 修改工作端口地址	9
2.4 修改工作端口的默认网关	9
2.5 修改DNS	9
3 透明模式部署	10
3.2 登录Web UI	10
3.3 IWSA透明模式部署	10
4 简单透明模式部署	16
4.2 使用场景	16
4.3 IWSA简单透明模式部署	16

5	WCCP模式部署	19
5.2	使用场景	19
5.3	IWSA WCCP模式部署	19
6	半透明模式部署	23
6.1	使用场景	23
6.2	IWSA半透明模式部署	23
7	单向扫描模式部署	25
7.1	使用场景	25
7.2	IWSA单向扫描模式部署	25
8	双链路模式部署	27
8.1	使用场景	27
8.2	IWSA双链路部署	27
9	IWSA上线测试指导	29
9.1	测试前准备	29
9.2	测试流程说明	29
9.3	测试配置建议	29
9.4	诊断问题建议	36
10	FAQ	38
10.1	什么是补丁	38
10.2	什么是bypass	38
10.3	硬件bypass	38
10.4	系统bypass (rpolicy)	38
10.5	应用层bypass	39
10.6	访问慢，断网问题的三步骤思路	39



1. 简介

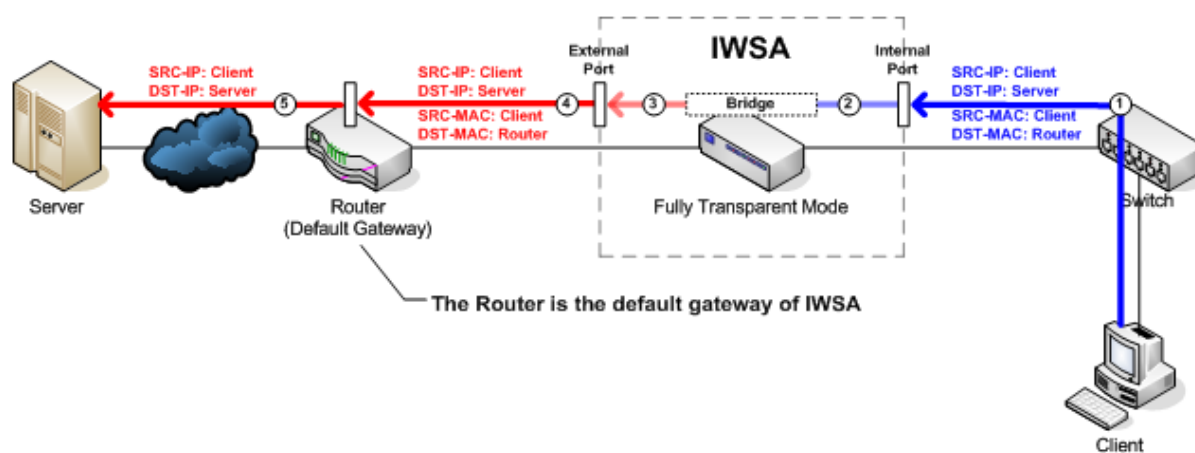
- ◇ 本手册适用于 IWSA 系列 (IWSVA5.6 简中版)。
- ◇ 本手册介绍 IWSA 部署及上线测试等内容。
- ◇ 默认使用对象已熟悉 IWSA 的安装。

2. 客户环境检查

注意：本章是针对客户环境而设置，如果是上线测试，请先了解下面客户的网络情况。

2.1. 单链路网络部署

2.1.1 IWSA透明模式

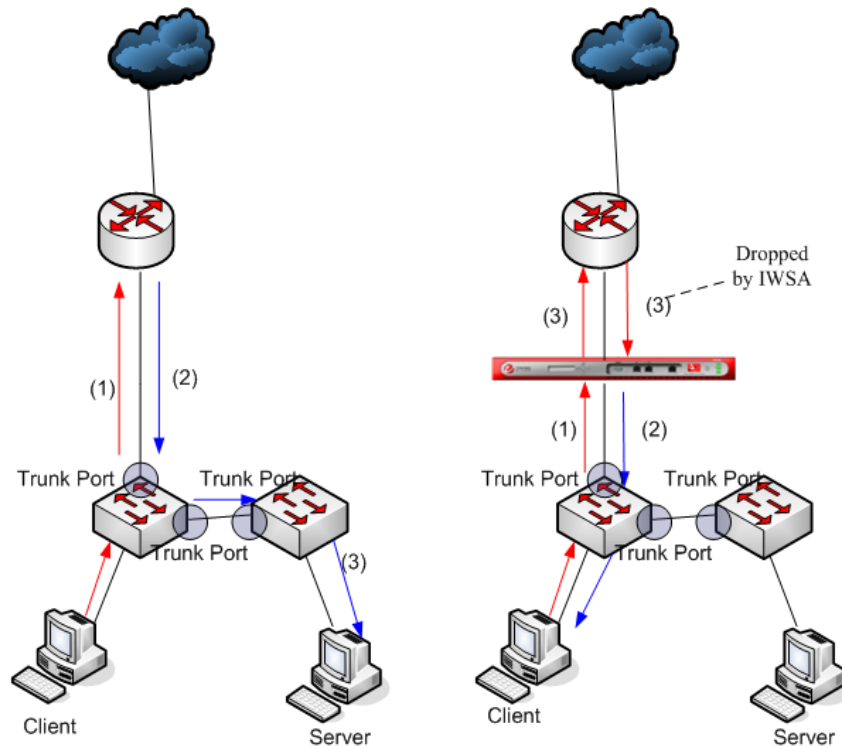


1) IWSA两段式连接

- ✧ 客户端先和IWSA建立连接，IWSA再和服务器建立连接
 - ✧ 客户端以为是和服务器建的连接，其实是和IWSA建立的
- 详细部署过程请见第四节。

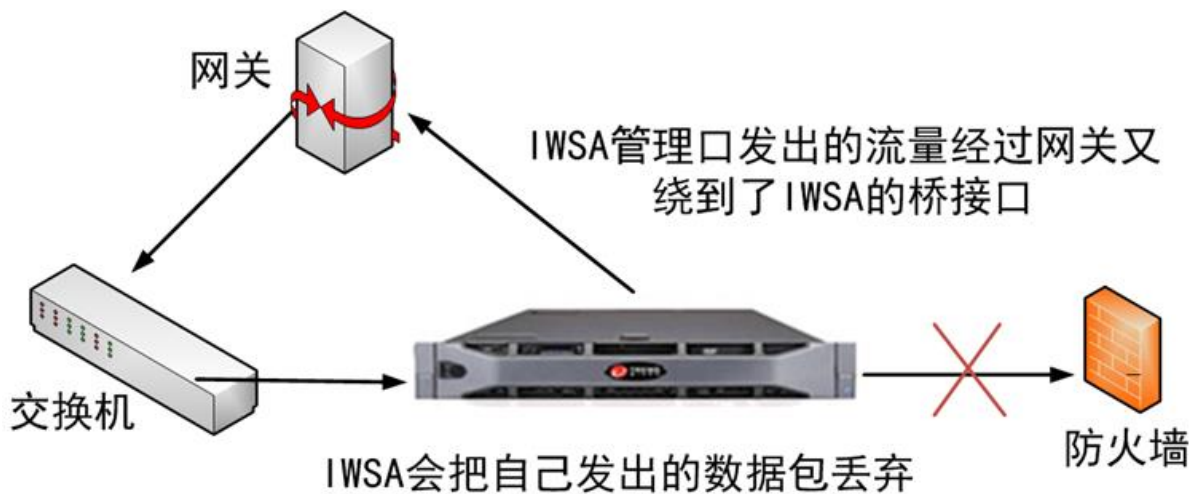
2) 透明模式部署局限性

- ✧ U-Turn症状：Client无法访问内网的Server



解决方案：部署为单向扫描模式，详细步骤见第8节

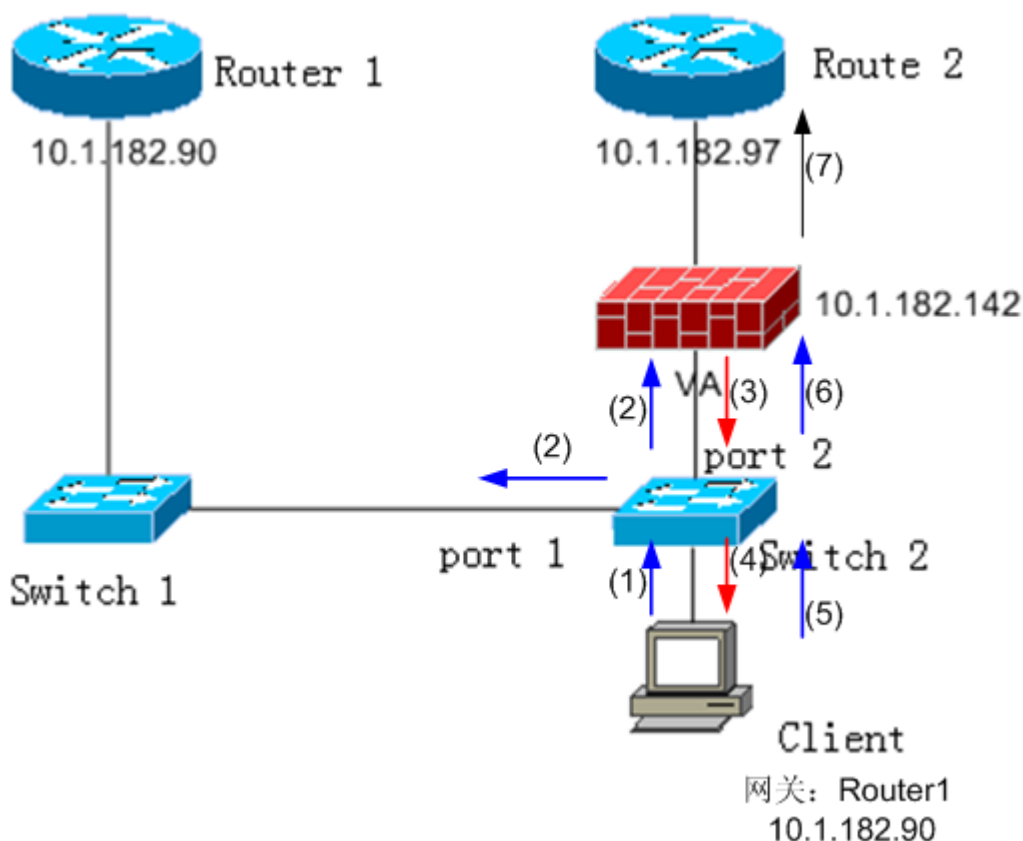
✧ IWSA回流症状：AU WRS不能工作



解决方案：Rpolicy Bypass源IP是IWSA管理口的流量，**建议设置为默认配置**

✧ 交换机MAC浮动症状：Client没法访问外部服务器

- ✓ Client网关为Router1
- ✓ Switch2广播SYN包
- ✓ IWSA通过Port2优先回复SYN_ACK
- ✓ Switch2学习后会转发后续Client的包到Port2



解决方案: Bypass目标MAC不是Route2的数据包

2.1.2 简单透明模式

- ✧ 检查客户环境中是否存在F5设备
- ✧ 存在F5设备, 并且确定IWSA需要接入F5设备
- ✧ 采用简单透明模式部署, IWSA部署过程详见第四节

2.1.3 WCCP模式

- ✧ 检查客户环境中是否存在支持WCCP的思科设备, 例如Cisco 2821路由器, Cisco 3750交换机等
- ✧ 存在, 并且确定IWSA需要接入此类设备
- ✧ 采用WCCP模式, IWSA部署过程详见第五节

2.2. 双链路网络部署

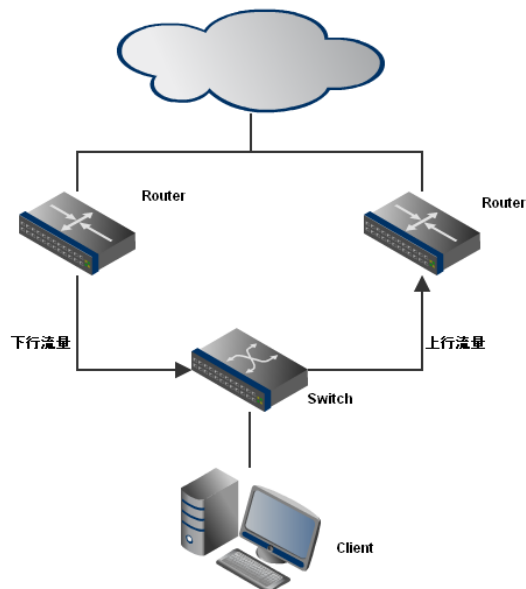
- ✧ 如果用户环境中支持WCCP的设备如F5, CISCO, 建议部署在WCCP模式下。

2.2.1 常见问题

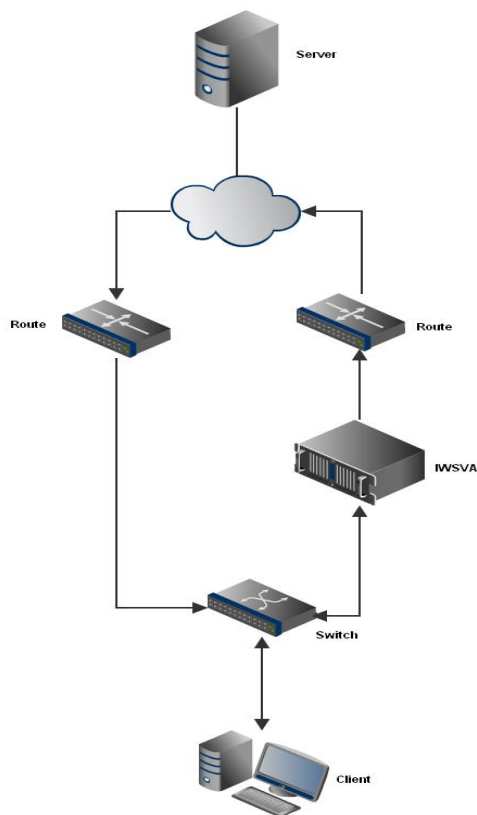
2.2.1.1 非对称路由

1) 问题描述

非对称路由（Asymmetric routing）是指往返某一节点的路径不一致，即指上行流量和下行流量分别从不同的网路流经。



2) 非对称路由情况下的IWSVA透明模式部署问题



- ✓ 当 IWSVA 完成和客户端的连接后，发起和服务器的 TCP 请求。此时 IWSVA 伪装成客户端，在非对称路由情况下，服务器回复的包会从另一路径到达客户端而非 IWSVA。

- ✓ 因此 IWSA 不能和服务端正确完成 TCP 连接，客户端也会因为服务器的回复包非法而丢弃。
- ✓ 此时，IWSA 不能正常工作，并会导致客户端不能进行正常的 HTTP 访问。
- ✓ 此问题在部署一台或者主备链路二台 IWSVA 时都有可能出现

3) 解决方案（半透明模式或双链路模式）

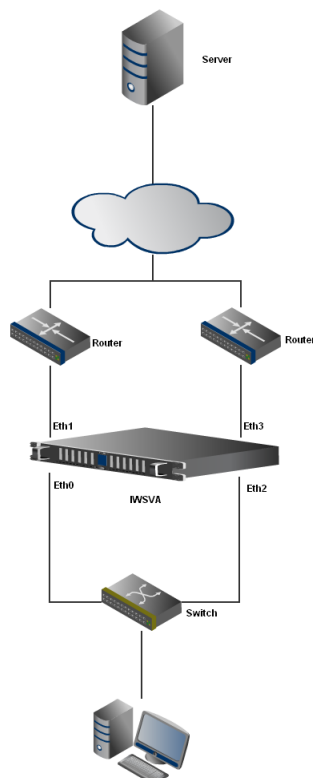
- IWSA 可以部署在半透明模式下。

当 IWSA 部署在半透明模式下，处理方式如下：

- ✧ 客户端发起的请求经过 IWSVA 时，IWSVA 先伪装成服务器和客户端建立连接
- ✧ IWSA 收到来自客户端的 HTTP 请求之后，IWSVA 以自己的 IP 地址作为源地址和服务器建立连接 TCP 连接，并发起 HTTP 请求
- ✧ IWSA 收到服务器响应后，再次伪装成服务器把响应发给客户端

此方案中，IWSA 对于外网口设备，视为一个网络节点。因此服务器发给 IWSA 的响应，会到达 IWSA，从而避免非对称路由问题的发生。对于内网口设备，IWSA 仍然作为网桥，即透明设备。详细部署过程请见第六节。

- IWSVA 可以部署在双链路模式下。



- ✧ Eth0, Eth1 分别作为 Br0 的内网口与外网口；Eth2, Eth3 分别作为 Br1 的内网口与外网口。
- ✧ 当 IWSVA 从 Eth0 收到客户端发送的请求并建立连接后，由 Eth1 向服务端发送请求。
- ✧ 此时，如果发生非对称路由，即服务端的回复报文由 Eth3（Br1）收到。IWSVA 会把此报文作为 Br0 报文处理。
- ✧ IWSVA 处理完后，会发送回复报文由 Eth0（Br0）或 Eth2（Br1）（可配）发送给客户端。

此方案中，IWSVA作为全透明设备存在，对于客户端和服务端不可见。详细部署过程请见第八节。

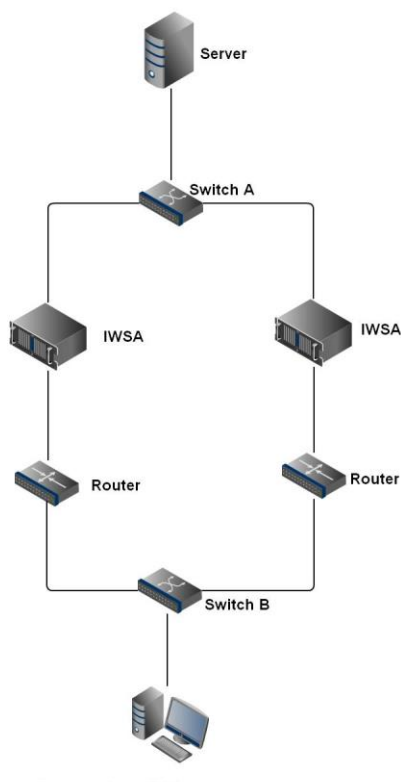
2.2.1.2 客户端交换机MAC浮动

此问题在部署一台或者主备链路二台IWSVA时经常出现，详细情况请参考2.1.1透明模式部署局限性章节

2.2.1.3 服务器端MAC浮动

1) 问题描述

当需要在主备链路同时部署IWSA时此问题经常出现



- ✧ 当服务器端网口某台交换机（如图中Switch A）因MAC-Address表老化或其他出现广播时
- ✧ 备链路路上的IWSA可能会收到从主链路上发来的SYN包
- ✧ 此时备链路路上的IWSA会伪装成服务器回复请求造成网络中断

2) 解决方案

在此种环境中，IWSA可以设置为单向扫描，即只扫描客户端发来的请求。因此但收到从服务器端网口发来的请求，不做处理，直接透传。详细部署过程请见第七节。

2.3. 交叉链路和聚合链路

IWSA不支持此类部署

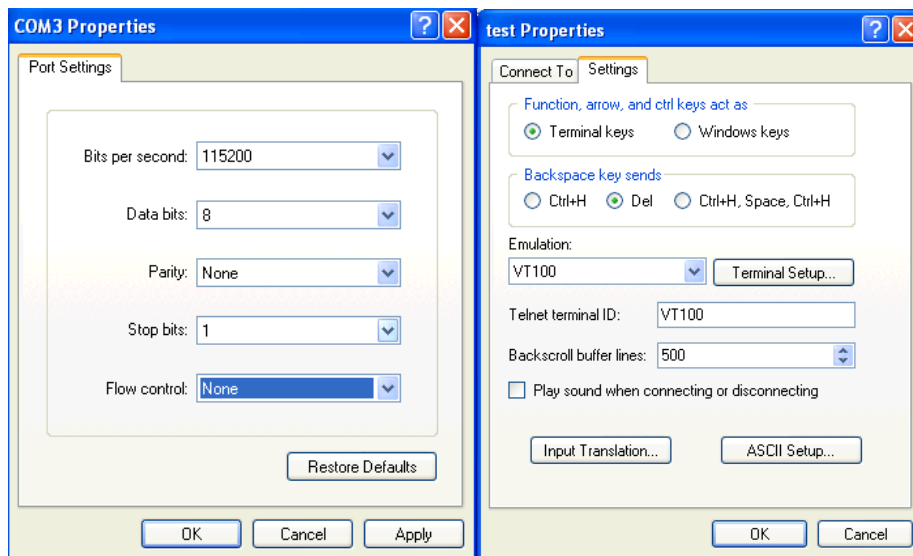
2 网络信息配置

注意：使用 ISO 安装完毕后，如果可以登录 Admin Web UI，则可以忽略该章步骤，直接进入第三章进行配置。该章为无法登录管理界面而设计的。

2.2 基本配置

1) 当你拿到一台新机器时，请先通过COM口进行连接：

注意：该步骤不一定要通过COM口连接，可以直接用键盘和显示器连接即可。



2) 接下来就是配置网络地址等信息，基本步骤如下：

用root帐号登录执行“clish”命令，进入配置页面，再键入“enable”命令后(变成了enable帐户的身份)，就可进行系统设置，如下图：

```
[root@IWSVA56VINEN ~]# clish
*****
*                IWSVA                *
*                *                      *
*  WARNING: Authorized Access Only  *
*                *                      *
*****
Welcome root it is Mon Nov 26 16:05:14 CST 2012

> enable
Entering privileged mode...

enable#

configure  Configure system settings
exit       Turn off privileged commands
ftpput    Upload file through FTP protocol
help      Display an overview of the CLI syntax
history   Display the current session's command line history
ping      Ping
ping6     Ping6
reboot    Reboot this computer immediately or after the specified delay.
resolve   Resolve a Web address either IP or FQDN on the network
resolve6  Resolve a Web address either IPV6 or FQDN on the network
restart   Restart a services
show      Show commands
shutdown  Shut down this computer immediately or after the specified delay.
start     Start a service, process or task
stop      Stop a s service, process
traceroute TraceRoute
traceroute6 TraceRoute IPV6 version
wget      Download file through HTTP/FTP protocols

enable#
```

其中configure network命令可以设置很多网络相关的设置，如下图所示

```
enable# configure network
bonding          bridge          dns              dualbridge
hostname         interface       lanbypass       mgmt
portgroup        proxy           route           semi-Transparent
```

2.3 修改工作端口地址

在上图中，使用configure network interface ipv4 static eth0 <IP of IWSA> <netmask>（中间用空格）修改地址。

该IP地址应由企业内部管理员提供，内网可达并可连通外网。

2.4 修改工作端口的默认网关

在上图中，使用configure network route ipv4 default <IP of gateway>修改默认网关。

该网关地址应由企业内部管理员提供，在IWSA上可以ping通。

2.5 修改DNS

在上图中，使用configure network dns ipv4 x.x.x.x可修改DNS（中间用空格）

查看DNS是否正确：在IWSA上ping baidu.com，没有丢包

```
[root@IWSVA56VINEN ~]# ping baidu.com
PING baidu.com (220.181.111.86) 56(84) bytes of data.
64 bytes from 220.181.111.86: icmp_seq=1 ttl=53 time=30.0 ms
64 bytes from 220.181.111.86: icmp_seq=2 ttl=53 time=28.0 ms
64 bytes from 220.181.111.86: icmp_seq=3 ttl=53 time=28.1 ms
64 bytes from 220.181.111.86: icmp_seq=4 ttl=53 time=27.9 ms
64 bytes from 220.181.111.86: icmp_seq=5 ttl=53 time=30.9 ms
64 bytes from 220.181.111.86: icmp_seq=6 ttl=53 time=28.5 ms
64 bytes from 220.181.111.86: icmp_seq=7 ttl=53 time=28.6 ms
64 bytes from 220.181.111.86: icmp_seq=8 ttl=53 time=29.1 ms
64 bytes from 220.181.111.86: icmp_seq=9 ttl=53 time=28.6 ms
64 bytes from 220.181.111.86: icmp_seq=10 ttl=53 time=27.9 ms
^C
--- baidu.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9540ms
rtt min/avg/max/mdev = 27.916/28.805/30.909/0.939 ms
```

3 透明模式部署

3.2 登录Web UI

访问http://<IWSA的IP地址>:1812/来访问IWSA的UI

登录帐号: admin , 密码: xxxxxx

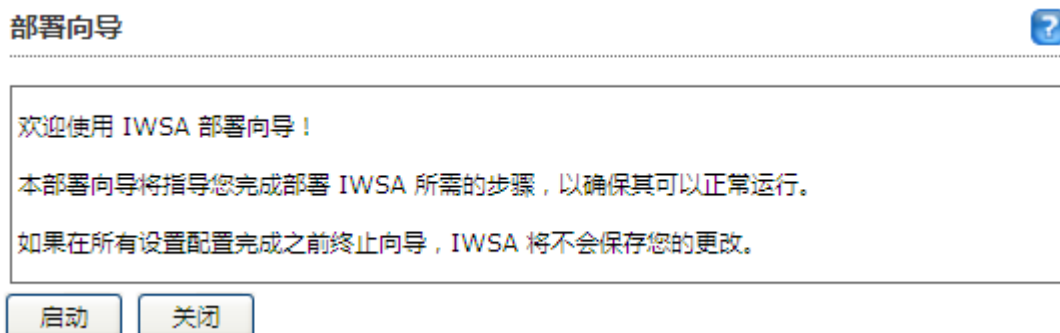


© 版权所有 2001-2012 趋势科技 (中国) 有限公司/Trend Micro Incorporated. 保留所有权利。

3.3 IWSA透明模式部署

首次登陆Web UI部署向导会自动运行

- 1) 首先点击“启动”按钮



- 2) 选择“透明桥接”模式，然后点“下一步”按钮



部署模式



IWSVA 可在不同模式下运行，而不同的模式会影响其接入网络和扫描通信的方式。IWSVA 可作为一个单元或群集运行。在群集中，两个或更多 IWSVA 一起工作以提供容错功能。

步骤

1. 部署模式
2. 部署设置
3. 网络接口
4. 静态路由
5. 产品激活
6. 系统时间
7. 摘要
8. 结果

模式选择

- 透明桥接模式
- 透明桥接模式 — 高可用性 (需要至少四个 NIC。)
- 正向代理服务器模式
- 反向代理服务器模式
- ICAP 模式
- 简单透明性模式
- Web 缓存协调协议 (WCCP) 模式

透明桥接模式 在此模式下，IWSVA 充当两个网络设备 (交换机、路由器或防火墙) 之间的桥梁，并透明地扫描 HTTP 和 FTP 通信。透明桥接模式是将 IWSVA 部署到现有网络拓扑的最简单的方法，而且无需对客户端、路由器或交换机做任何修改。要部署该模式，IWSVA 计算机需要至少两个网络适配器。



< 返回

下一页 >

取消

- 3) 选择 **Silicom** 网卡接口作为数据口。必须选择板载网卡接口作为单独管理接口，然后设置管理 IP 地址，数据口的 IP 地址与管理 IP 不在同一网段的 IP 地址，**建议将数据口 IP 设置成 1.1.1.1**，以保证数据口(br0)内部和外面均不可达。然后点“下一步”按钮，如下图所示：



网络接口



请指定 IWSA 的相关网络接口设置。

步骤

1. 部署模式
2. 部署设置
3. 网络接口
4. 静态路由
5. 产品激活
6. 系统时间
7. 摘要
8. 结果

主机信息	
主机名: *	<input type="text" value="iwsva56sctest"/>
接口状态	
D=数据 M=管理 H=高可用性	
数据接口	
以太网接口:	<input type="text" value="br0"/> <input type="checkbox"/> 启用 Ping
内部接口: *	<input type="text" value="eth1"/>
外部接口: *	<input type="text" value="eth2"/>
<input type="checkbox"/> 从 DHCP 获取	
IPv4 地址: *	<input type="text" value="1.1.1.1"/>
网络掩码: *	<input type="text" value="255.255.255.0"/>
<input type="checkbox"/> 启用 VLAN ID:	<input type="text" value="0"/> (1-4094)
<input checked="" type="checkbox"/> 单独管理接口	
以太网接口: *	<input type="text" value="eth0"/> <input checked="" type="checkbox"/> 启用 Ping
IPv4 地址: *	<input type="text" value="10.64.75.118"/>
网络掩码: *	<input type="text" value="255.255.254.0"/>
其他设置	
<input type="checkbox"/> 从 DHCP 获取	
网关: *	<input type="text" value="10.64.74.1"/>
主 DNS 服务器: *	<input type="text" value="10.64.1.55"/>
辅助 DNS 服务器:	<input type="text"/>
<input type="checkbox"/> 启用 IPv6 协议	
<input style="margin-right: 10px;" type="button" value=" < 返回 "/> <input style="margin-right: 10px;" type="button" value=" 下一页 > "/> <input style="margin-right: 10px;" type="button" value=" 取消 "/>	

例如上图表示eth0为板载网卡接口，eth1,eth2为Silicom lanbypass卡接口。

单独管理接口IP地址必须是内外网均可达的。

这一章节设置完后，可以ping外网试验，检查网关、DNS是否正确：在IWSA上ping baidu.com，没有丢包。如：


```
[root@IWSVA56VINEN ~]# ping baidu.com
PING baidu.com (220.181.111.86) 56(84) bytes of data.
64 bytes from 220.181.111.86: icmp_seq=1 ttl=53 time=30.0 ms
64 bytes from 220.181.111.86: icmp_seq=2 ttl=53 time=28.0 ms
64 bytes from 220.181.111.86: icmp_seq=3 ttl=53 time=28.1 ms
64 bytes from 220.181.111.86: icmp_seq=4 ttl=53 time=27.9 ms
64 bytes from 220.181.111.86: icmp_seq=5 ttl=53 time=30.9 ms
64 bytes from 220.181.111.86: icmp_seq=6 ttl=53 time=28.5 ms
64 bytes from 220.181.111.86: icmp_seq=7 ttl=53 time=28.6 ms
64 bytes from 220.181.111.86: icmp_seq=8 ttl=53 time=29.1 ms
64 bytes from 220.181.111.86: icmp_seq=9 ttl=53 time=28.6 ms
64 bytes from 220.181.111.86: icmp_seq=10 ttl=53 time=27.9 ms
^C
--- baidu.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9540ms
rtt min/avg/max/mdev = 27.916/28.805/30.909/0.939 ms
```

注：对于带有硬件bypass卡的设备，必须要设置单独的管理口。否则在硬件bypass期间，无法连接上IWSA。

4) 设置静态路由信息(通常情况下不用)

为管理端口配置静态路由(在某些情况下，需要管理网段能够访问其它网段，这时需要为管理口设置静态路由)，如下图所示，设置好网络 ID，网络掩码，路由，接口之后，点击“添加到列表”按钮加入一条路由。

重复上述步骤加入所有路由项后，点击“下一步”按钮。

静态路由设置

请指定静态路由设置。

步骤

1. 部署模式
2. 部署设置
3. 网络接口
4. 静态路由
5. 产品激活
6. 系统时间
7. 摘要
8. 结果

设置

网络 ID: 172.16.0.0

网络掩码: 255.255.0.0

路由器: 10.64.75.1

接口: 管理

添加到列表

网络 ID	网络掩码	路由器	接口
172.16.0.0	255.255.0.0	10.64.75.1	管理

< 返回 下一页 > 取消

5) 输入激活码

输入激活码如下图所示，然后点击“Next”按钮。

注意：如果暂时没有激活码，可以先跳过该步骤，以后在管理界面(管理->产品使用授权)可以激活。

6) 设置系统时间和 NTP 配置

7) 显示相关配置的 Summary

点击“确认”后，IWSA开始切换到透明桥接，并重启IWSA

8) 重启完成，登录 Web console 界面，点击“绕开通信”，激活 lanbypass 卡功能。

确认lanbypass卡正常工作：

可以查看“摘要”中流量监控信息，没有任何流量信息显示说明lanbypass成功（如果测试环境没有流量，可以使用一台机器访问外部网络制造流量）。

也可以查看机器上的lanbypass卡的bypass灯是否开启。

9) 点击“禁用绕开通信”，关闭 bypass。



10) 检查过载保护功能有没有打开

打开文件/etc/iscan/network.ini，找有没有名为ct_redir_max的项，如果有，且该项的值和IWSA的型号一致(IWSA3600是3600，IWSA6600是6600以此类推)，则配置完成。

如果没有这项或者是值不对，请手工添加，并将值设置为和IWSA型号一致。

例如: ct_redir_max=3600

通过重启网络服务使设置生效

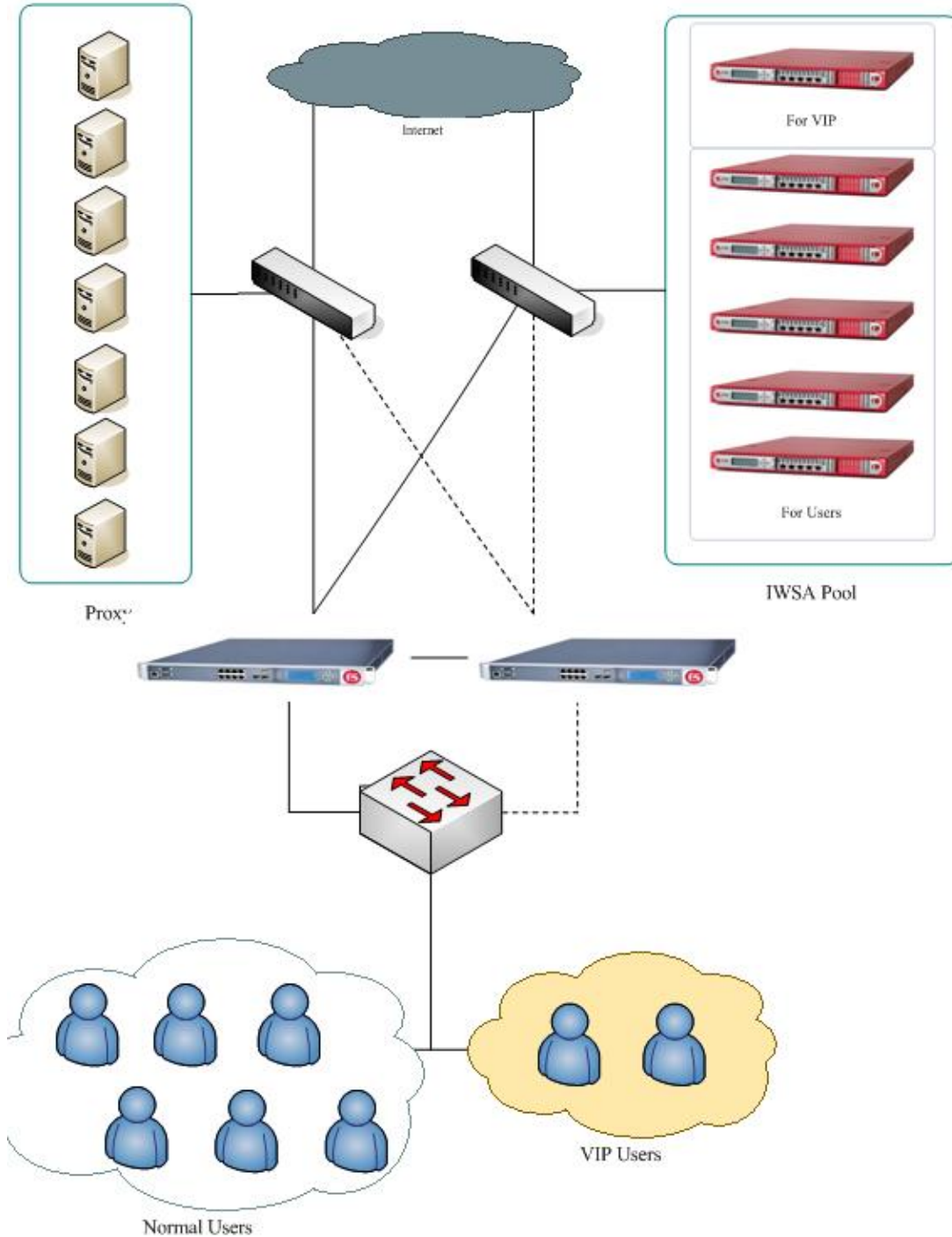
```
>/etc/init.d/network restart
```

如果需要关闭过载保护，删除ct_redir_max即可。

4 简单透明模式部署

4.2 使用场景

如果客户环境中存在F5设备，并且使IWSA接入F5设备，建议使用简单透明模式部署。部署方式：通过L4交换机对多台IWSA作负载均衡的处理。部署拓扑图如下：



4.3 IWSA简单透明模式部署

- 1) 打开部署向导后，选择“简单透明模式”，然后点“下一步”按钮



部署模式



IWSVA 可在不同模式下运行，而不同的模式会影响其接入网络和扫描通信的方式。IWSVA 可作为一个单元或群集运行。在群集中，两个或更多 IWSVA 一起工作以提供容错功能。

步骤

1. 部署模式
2. 透明性设置
3. 网络接口
4. 静态路由
5. 产品激活
6. 系统时间
7. 摘要
8. 结果

模式选择

- 透明桥接模式
- 透明桥接模式 — 高可用性
- 正向代理服务器模式
- 反向代理服务器模式
- ICAP 模式
- 简单透明性模式
- Web 缓存协调协议 (WCCP) 模式

警告：此模式将禁用 HTTPS 解密功能。
 简单透明模式 在此模式下，会设置一台 L4 交换机负责将 HTTP/FTP 通信定向到 IWSVA(注意：此部署模式当前不提供 IPv6 支持)。

< 返回 下一页 > 取消

2) 输入端口号和邮件地址



简单透明性设置



请指定相关的简单透明性设置。

步骤

1. 部署模式
2. 简单透明性设置
3. 网络接口
4. 静态路由
5. 产品激活
6. 系统时间
7. 摘要
8. 结果

HTTP 侦听端口

端口号:

基于 HTTP 的匿名 FTP

电子邮件地址:

< 返回 下一页 > 取消

3) 选择板载网卡接口作为数据口，此模式不需要 lanbypass 卡。



网络接口



请指定 IWSVA 的相关网络接口设置。

步骤

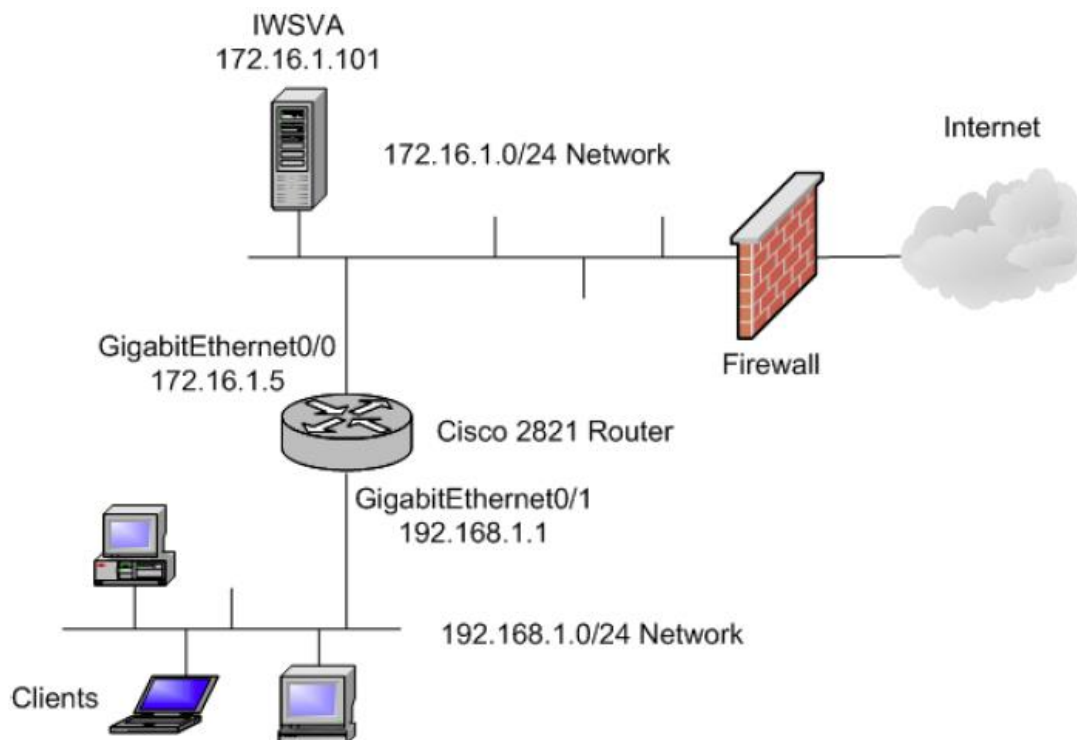
主机信息	步骤
主机名: * <input type="text" value="iwsva56sctest"/>	1. 部署模式
接口状态 D=数据 M=管理 H=高可用性	
数据接口	
以太网接口: * <input type="text" value="eth0"/> <input checked="" type="checkbox"/> 启用 Ping	2. 简单透明性设置
<input type="checkbox"/> 从 DHCP 获取	3. 网络接口
IPv4 地址: * <input type="text" value="10.64.75.118"/>	4. 静态路由
网络掩码: * <input type="text" value="255.255.254.0"/>	5. 产品激活
<input type="checkbox"/> 单独管理接口	
以太网接口: * <input type="text" value="-选择-"/> <input type="checkbox"/> 启用 Ping	6. 系统时间
IPv4 地址: * <input type="text" value="10.64.75.118"/>	7. 摘要
网络掩码: * <input type="text"/>	8. 结果
其他设置	
<input type="checkbox"/> 从 DHCP 获取	
网关: * <input type="text" value="10.64.74.1"/>	
主 DNS 服务器: * <input type="text" value="10.64.1.55"/>	
辅助 DNS 服务器: <input type="text"/>	
<input type="checkbox"/> 启用 IPv6 协议	
<input type="button" value=" < 返回"/> <input type="button" value=" 下一页 >"/> <input type="button" value=" 取消"/>	

- 4) 设置静态路由信息
- 5) 输入激活码
- 6) 设置系统时间和 NTP 配置
- 7) 显示相关配置的 Summary
- 8) 点击“确认”后，IWSVA 开始切换到简单透明模式

5 WCCP模式部署

5.2 使用场景

如果客户环境中支持WCCP的思科设备，例如Cisco 2821路由器，Cisco 3750交换机等，建议使用WCCP模式部署。部署拓扑图如下：



5.3 IWSVA WCCP模式部署

- 1) 打开部署向导后，选择“Web 缓存协调协议(WCCP)模式”，然后点“下一步”按钮



部署模式



IWSVA 可在不同模式下运行，而不同的模式会影响其接入网络和扫描通信的方式。IWSVA 可作为一个单元或群集运行。在群集中，两个或更多 IWSVA 一起工作以提供容错功能。

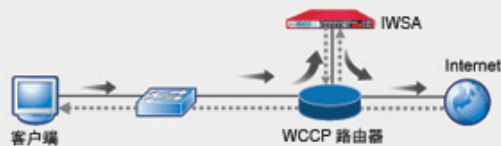
步骤

1. 部署模式
2. WCCP 设置
3. 网络接口
4. 静态路由
5. 产品激活
6. 系统时间
7. 摘要
8. 结果

模式选择

- 透明桥接模式
- 透明桥接模式 — 高可用性
- 正向代理服务器模式
- 反向代理服务器模式
- ICAP 模式
- 简单透明性模式
- Web 缓存协调协议 (WCCP) 模式

WCCP 模式 在此模式下，IWSVA 可处理从启用了 WCCP 的路由器重定向的通信。Web 缓存通信协议 (WCCP) 是 Cisco 开发的内容路由协议，该协议提供了实时重定向通信流的机制。它具有内置的负载均衡、缩放、容错和服务保障 (故障安全) 机制。配置为使用 WCCP 模式的 IWSVA 可处理从启用了 WCCP 的路由器重定向的通信(注意: 此部署模式当前不提供 IPv6 支持)。



< 返回

下一页 >

取消

2) 输入端口号，路由器 IP 地址、密码等信息，根据需求选择重定向的协议。



Web 缓存协调协议 (WCCP) 设置



请指定 WCCP 设置。

步骤

HTTP 侦听端口

端口: (缺省值 = 8080)

WCCP 设置

路由器 IP 地址:
使用英文半角逗号","隔开多个地址

密码: (使用密码安全)

自动协商:
要查看用于在 WCCP 模式下部署 IWSA 的自动协商值, 请转到“管理 > 网络配置 > WCCP”

服务组: (51-255; 缺省值 = 80)

已重定向的协议: HTTP (80) HTTPS (443) FTP (21)

基于 HTTP 的匿名 FTP

电子邮件地址:

1. 部署模式
2. WCCP 设置
3. 网络接口
4. 静态路由
5. 产品激活
6. 系统时间
7. 摘要
8. 结果

3) 选择板载网卡接口作为数据口, 此模式不需要 lanbypass 卡。



网络接口



请指定 IWSA 的相关网络接口设置。

步骤

主机信息	
主机名: *	<input type="text" value="iwsva56sctest"/>
接口状态 D=数据 M=管理 H=高可用性	
数据接口	
以太网接口: *	<input type="text" value="eth0"/> <input checked="" type="checkbox"/> 启用 Ping
<input type="checkbox"/> 从 DHCP 获取	
IPv4 地址: *	<input type="text" value="10.64.75.118"/>
网络掩码: *	<input type="text" value="255.255.254.0"/>
<input type="checkbox"/> 单独管理接口	
以太网接口: *	<input type="text" value="-选择-"/> <input type="checkbox"/> 启用 Ping
IPv4 地址: *	<input type="text" value="10.64.75.118"/>
网络掩码: *	<input type="text" value="255.255.254.0"/>
其他设置	
<input type="checkbox"/> 从 DHCP 获取	
网关: *	<input type="text" value="10.64.74.1"/>
主 DNS 服务器: *	<input type="text" value="10.64.1.55"/>
辅助 DNS 服务器:	<input type="text"/>
<input type="checkbox"/> 启用 IPv6 协议	
<input type="button" value=" < 返回"/> <input type="button" value=" 下一页 >"/> <input type="button" value=" 取消"/>	

1. 部署模式
2. WCCP 设置
3. 网络接口
4. 静态路由
5. 产品激活
6. 系统时间
7. 摘要
8. 结果

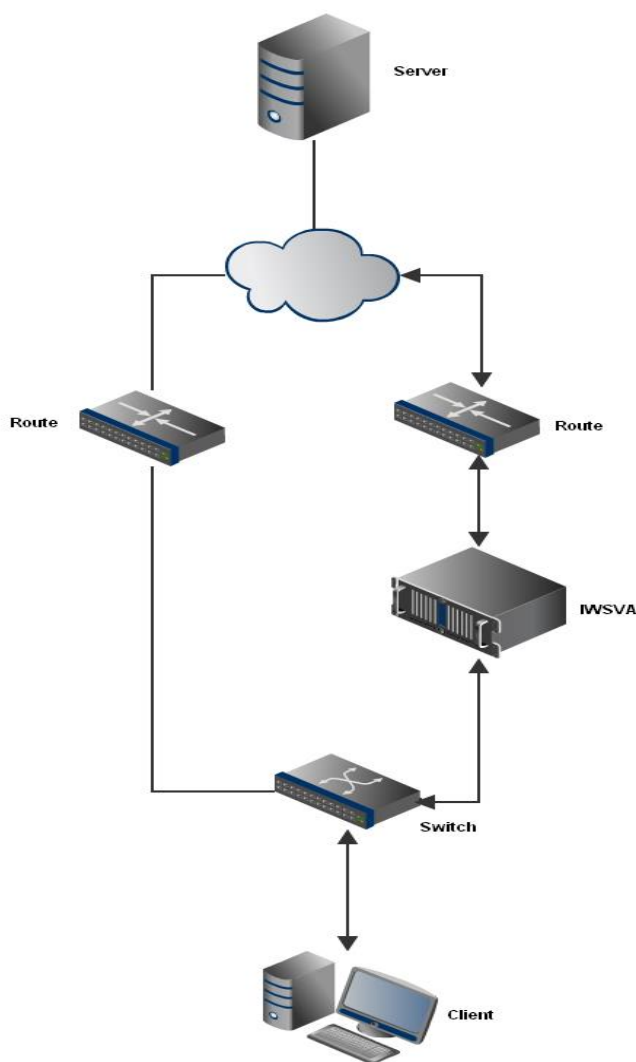
- 4) 设置静态路由信息
- 5) 输入激活码
- 6) 设置系统时间和 NTP 配置
- 7) 显示相关配置的 Summary
- 8) 点击“确认”后，IWSA 开始切换到 WCCP 模式

6 半透明模式部署

此模式为桥接模式的衍生模式，请先部署为桥接模式

6.1 使用场景

如果客户环境中存在非对称路由，建议使用半透明模式部署。部署拓扑图如下：



注意：

- 1) IWSVA 的数据口（br0）需要配置能够访问外网的 IP 地址，并且 IWSVA 上行方向的防火墙等设备必须允许 IWSVA 发起的访问请求，从而能够和服务器建立连接；
- 2) 此方案中假定所有上行流量（参见 2.4）都从 IWSVA 一侧通过。如果两条链路上都存在上行流量，那么需要两台 IWSVA，以半透明模式分别部署在两条链路上。

6.2 IWSVA半透明模式部署

开启半透明模式

- 1) IWSVA 部署为透明模式
- 2) 进入 clish 特权模式
- 3) 运行以下命令：
“configure network semi-Transparent enable”

```
Leaving privileged mode...

> exit
[root@IWSVA56PHASE2 ~]# clish
*****
*                               *
*                               *
*      WARNING: Authorized Access Only      *
*                               *
*****
Welcome root it is Fri Apr 15 15:23:39 CST 2011

> e
enable exit
> enable
Entering privileged mode...

enable# configure network semi-Transparent enable █
```

关闭半透明模式

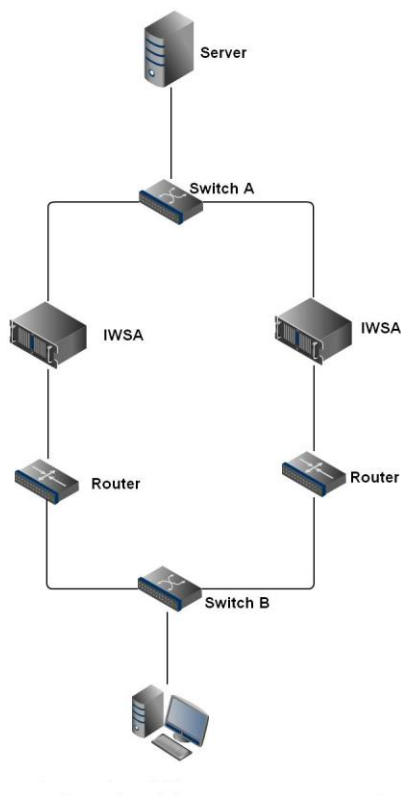
- 1) 进入 clish 特权模式
- 2) 运行以下命令：
“configure network semi-Transparent disable”

7 单向扫描模式部署

此模式为桥接模式的衍生模式，请先部署为桥接模式

7.1 使用场景

如果客户环境中存在MAC地址浮动，还可以使用此种模式部署。部署拓扑图如下：



7.2 IWSA单向扫描模式部署

开启单向扫描

- 1) IWSA 部署为桥接模式
- 2) 编辑/etc/iscan/network.ini文件
- 3) 加入字段onlyscan_interface=[interface]

此处interface为桥内网口端口，即所需要扫描的端口

```
#setting dual bridge
enable_multilink=no
ifduel_internal=eth2
ifduel_external=eth3
obtain_from_dhcp6=yes

onlyscan_interface=eth0
```

- 4) 重启网络服务
“ service network restart”
- 5) 重启服务
“ /etc/iscan/rcIwss restart”

关闭单向扫描

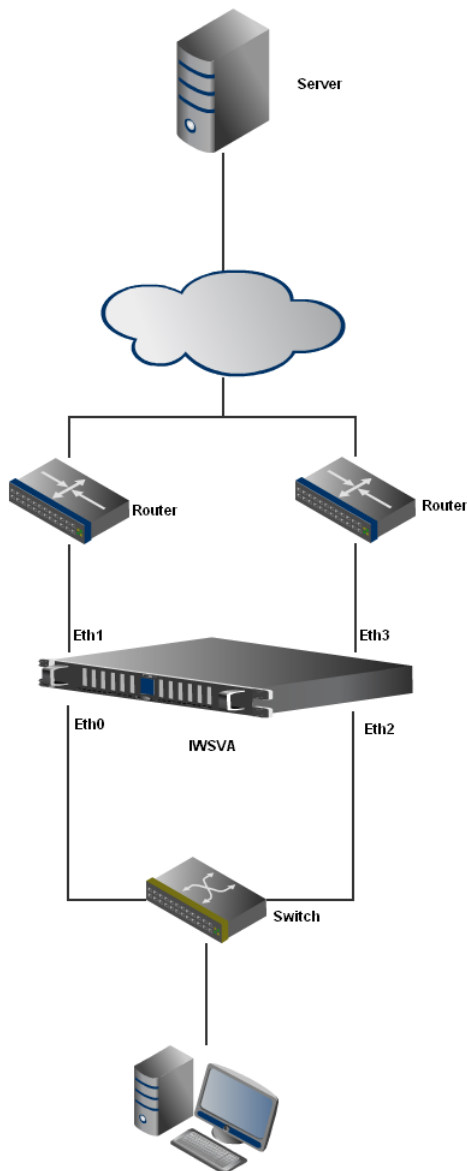
- 1) 编辑/etc/iscan/network.ini文件
- 2) 删除或注释字段onlyscan_interface=[interface]
- 3) 重启网络服务
“ service network restart”
- 4) 重启服务
“ /etc/iscan/rcIwss restart”

8 双链路模式部署

此模式为桥接模式的衍生模式，请先部署为桥接模式

8.1 使用场景

如果客户环境中存在非对称路由，建议使用双链路模式部署。部署拓扑图如下：



- 1) Eth0, Eth1 分别作为 Br0 的内网口与外网口；Eth2, Eth3 分别作为 Br1 的内网口与外网口。
- 2) 当 IWSVA 从 Eth0 收到客户端发送的请求并建立连接后，由 Eth1 向服务端发送请求。
- 3) 此时，如果发生非对称路由，即服务端的回复报文由 Eth3（Br1）收到。IWSVA 会把此报文作为 Br0 报文处理。
- 4) IWSVA 处理完后，会发送回复报文由 Eth0 (Br0) 或 Eth2 (Br1) (可配) 发送给客户端。
- 5) 此方案中，IWSVA 作为全透明设备存在，对于客户端和服务端不可见。

8.2 IWSA双链路部署

开启双链路模式

9 IWSA 上线测试指导

9.1 测试前准备

- 1) 客户网络情况调研，参考第二节客户环境检查
 - ✓ 有 F5 设备，应该采用简单透明模式
 - ✓ 有非对称路由情况，请使用双桥模式
 - ✓ 有聚合链路、交叉网络情况存在，暂时不支持桥模式部署
- 2) 如果采用的是测试机，建议对测试机系统进行重新灌装；
- 3) 通过 Web 界面，升级最新的操作系统和应用程序补丁：



9.2 测试流程说明

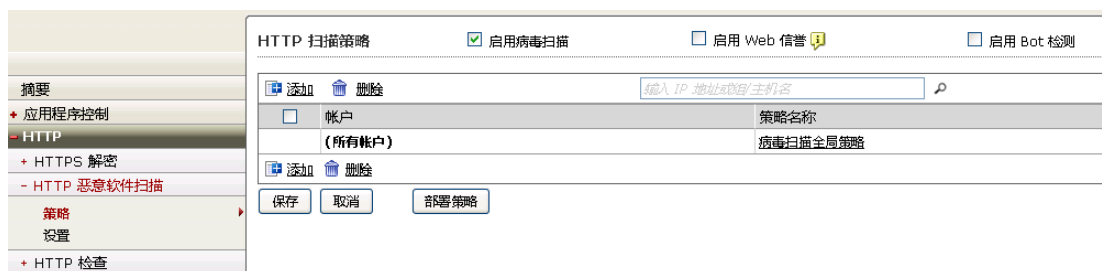
- 1) 上线后先确认网络连通状态,通过ping命令确认从IWSA访问外部站点或客户端需要访问的站点是否正常。
- 2) 确认是否能够连接AU server,通过ping命令确认从IWSA访问AU server正常。对于5.6版本，AU Server为iwsva56-p.activeupdate.trendmicro.com。

注：新版本的IWSA将会提供诊断工具进行网络状态的检查。

- 3) 启用 HTTP 恶意软件扫描 /FTP 扫描、全局 URL 阻止、全局可信 URL 功能，其它如 Web 信誉、Bot 检测、Applets 和 ActiveX 安全、URL 过滤、数据丢失防护、HTTPS 解密、应用程序控制等功能暂不启用，待运行平稳一段时间后，再根据用户要求决定是否启用；
- 4) 在正式上线前，建议先在用户网络环境中做小范围测试，尽可能根据用户的网络特点来做测试；
- 5) 在正式上线时，建议将 IWSA 处于硬件 bypass 状态。所有扫描功能关闭，接入网络后，待确认网络通讯正常，取消硬件 bypass，此时再逐项启用功能(此时启用 HTTP/FTP 扫描、全局 URL 阻止功能，其它功能暂不启用)。

9.3 测试配置建议

- 1) 测试初期配置启用 HTTP 恶意软件扫描，暂不启用 Web 信誉和 Bot 检测功能：



- 2) 配置 HTTP 不扫描超过 2M 的文件、配置 HTTP 对超过 10KB 的文件采用同步流扫描，转发率

为 80%，配置如下图所示：

大文件处理

不扫描超过以下大小的文件: MB ?

启用特殊处理

如果文件大于 KB ?

递交之前扫描 (扫描时显示一个进度页面)

同步流扫描: 交付部分页面而不扫描, 扫描剩余部分 (使客户端连接处于活动状态)。

已接收数据中不进行扫描并定期发送到客户端的百分比: %

- 3) 配置 MIME 内容类型，选择“要跳过的 MIME 内容类型”，请勾选“其他”；

扫描以下文件类型 (如果不阻止)

选择一种方法:

所有可扫描文件

IntelliScan: 使用“真实文件类型”识别 ?

特定文件 扩展名...

要跳过的 MIME 内容类型 ?: 启用 MIME 类型验证 ?

音频 显示详细信息

图像 显示详细信息

视频 显示详细信息

其他: 显示详细信息

- 4) 配置 HTTP 扫描 Spyware/Grayware;


HTTP 扫描策略: 编辑全局策略

策略列表

Web 信誉规则	病毒扫描规则	间谍软件/灰色软件扫描规则
扫描其他威胁:		<input checked="" type="checkbox"/> 全选
<input checked="" type="checkbox"/> 间谍软件	<input checked="" type="checkbox"/> 广告程序	
<input checked="" type="checkbox"/> 拨号程序	<input checked="" type="checkbox"/> 恶作剧程序	
<input checked="" type="checkbox"/> 黑客工具	<input checked="" type="checkbox"/> 远程访问工具	
<input checked="" type="checkbox"/> 密码破解程序	<input checked="" type="checkbox"/> 其他 ?	
<input type="button" value="保存"/> <input type="button" value="取消"/>		

HTTP 扫描策略: 编辑全局策略

策略列表

Web 信誉规则		病毒扫描规则	间谍软件/灰色软件扫描规则	Bot 检测规则	例外	处理措施
文件类型						处理措施
受感染文件:						清除
不可清除文件: 						删除
密码保护的文件:						不予处理
宏:						不予处理
注意						
创建时间:						11/21/12 10:46:31 下午
上次修改时间:						11/25/12 4:31:31 下午
注意:						HTTP 扫描缺省策略
<input type="button" value="保存"/> <input type="button" value="取消"/>						

注: 配置完成后, 请在扫描策略界面中点击“部署策略”, 以使得新配置马上应用。

- 配置 FTP 只扫描下载文件、配置扫描特定类型文件、超过 2MB 不扫描, 启动同步流扫描, 对大于 64KB 的文件使用同步流扫描, 转发率为 80%(与 HTTP 配置相同), 配置扫描 Spyware、配置采用默认处理动作;

FTP 扫描

 启用 FTP 扫描

病毒扫描规则	间谍软件/灰色软件扫描规则	例外	处理措施
扫描说明			
在以下过程中扫描文件:			
<input type="checkbox"/> 上传			
<input checked="" type="checkbox"/> 下载			
阻止以下文件类型:			
<input type="checkbox"/> Office 文档 显示详细信息			
<input type="checkbox"/> 图像 显示详细信息			
<input type="checkbox"/> 可执行文件 显示详细信息			
<input type="checkbox"/> 音频/视频文件 显示详细信息			
<input type="checkbox"/> Java 显示详细信息			
<input type="checkbox"/> 归档 显示详细信息			
<input type="checkbox"/> 其他 显示详细信息			
阻止包含任何选定文件类型的压缩文件? <input checked="" type="radio"/> 是 <input type="radio"/> 否			
扫描以下文件类型 (如果不阻止):			
选择一种方法:			
<input type="radio"/> 所有可扫描文件			
<input type="radio"/> IntelliScan: 使用“真实文件类型”识别 ?			
<input checked="" type="radio"/> 特定文件 扩展名...			
压缩文件处理			
处理措施: <input type="text" value="阻止"/>			
应用到:			
<input type="radio"/> 所有压缩文件			
<input checked="" type="radio"/> 压缩文件 (如果符合以下条件):			
解压后的文件数超过:			<input type="text" value="50000"/> (1-999999)
解压文件大小超过:			<input type="text" value="200"/> <input type="text" value="MB"/> (1-99999)
压缩层数超过:			<input type="text" value="10"/> (0-20)
<input type="checkbox"/> 压缩率超过 99%。(IWSA 自动允许压缩率小于 99% 的文件)			
大文件处理			
<input checked="" type="checkbox"/> 不扫描超过以下大小的文件: <input type="text" value="2"/> <input type="text" value="MB"/> ?			
<input checked="" type="checkbox"/> 对大于以下大小的文件启用同步流扫描: <input type="text" value="10"/> <input type="text" value="KB"/> ?			
同步流扫描: 交付部分页面而不扫描, 扫描剩余部分 (使客户端连接处于活动状态)。			
已接收数据中不进行扫描并定期发送到客户端的百分比: <input type="text" value="80"/> %			
隔离文件的处理			
<input checked="" type="checkbox"/> 加密已隔离文件			
<input type="button" value="保存"/> <input type="button" value="取消"/>			

FTP 扫描

 启用 FTP 扫描

病毒扫描规则	间谍软件/灰色软件扫描规则	例外	处理措施
扫描其他威胁:		<input checked="" type="checkbox"/> 全选	
<input checked="" type="checkbox"/> 间谍软件		<input checked="" type="checkbox"/> 广告程序	
<input checked="" type="checkbox"/> 拨号程序		<input checked="" type="checkbox"/> 恶作剧程序	
<input checked="" type="checkbox"/> 黑客工具		<input checked="" type="checkbox"/> 远程访问工具	
<input checked="" type="checkbox"/> 密码破解程序		<input checked="" type="checkbox"/> 其他	
<input type="button" value="保存"/> <input type="button" value="取消"/>			

- 6) 全局可信 URL 功能建议将常用的网址加在白名单中，同时启用全局 URL 阻止功能，将不禁止访问的网址加入，并使用通过特征码文件(网络钓鱼)对 URL 进行阻止，配置建议如下：

可信 URL

 启用可信 URL

匹配:

Web 站点 (例如: "xxx.com" 与 "xxx.com" 及其所有子站点匹配)
 字符串 (严格匹配, 例如: "z.zz.com/file" 只与 "z.zz.com/file" 匹配)

导入可信列表和例外:

不扫描以下 URL

163.com*
 baidu.com*
 download.windowsupdate.com*
 v4.windowsupdate.microsoft.com*
 v5.windowsupdate.microsoft.com*
 windowsupdate.microsoft.com*
 update.microsoft.com*
 www.download.windowsupdate.com*
 www.windowsupdate.com*
 www.update.microsoft.com*
 au.download.windowsupdate.com*

可信 URL 例外列表

URL 阻止 启用 URL 阻止 ?

通过本地列表 **通过特征码文件 (网络钓鱼)**

阻止以下网络钓鱼类别: ⓘ

- 网络钓鱼: 欺诈性收集机密信息
- 间谍软件: 隐藏但合法的程序, 秘密收集机密信息
- 病毒释放器: 由于恶意代码的已知行为而产生的出站 HTTP 访问
- 恶意站点: 为恶意用途而存在的 Web 站点

将网络钓鱼 URL 提交到 TrendLabs:

网络钓鱼 URL:

网络钓鱼类别:

发件人电子邮件地址:

注意:

- 7) 在“日志设置”中, 请**只启用**“收集性能数据”(每 1 分钟 1 次)

- 日志	URL 阻止日志:	/var /fiwss/log
+ 日志查询	URL 访问日志:	/var /fiwss/log
系统日志配置	性能日志:	/var /fiwss/log
+ 日志设置	系统事件日志:	/var /fiwss/log
+ 更新	选项	
通知	<input checked="" type="checkbox"/> 收集性能数据	
+ 管理	日志记录时间间隔 (按分钟): <input type="text" value="1"/>	
	<input type="checkbox"/> 记录 HTTP/HTTPS/FTP 访问事件	
	日志记录时间间隔 (按分钟): <input type="text" value="1"/>	
	<input type="radio"/> 记录用户访问以及所有下载的文件和对象 (详细)	
	<input type="radio"/> 记录用户访问以及超出以下大小的任何下载文件和对象 <input type="text" value="1024"/> KB	
	<input type="radio"/> 记录至少以下大小的下载文件和对象 <input type="text" value="1024"/> KB	
	在数据库中存储日志的天数: <input type="text" value="30"/> 天	
	数据库日志更新时间间隔 (秒): <input type="text" value="30"/>	

- 8) 配置代码库每小时更新一次, 其它组件每天更新一次。

更新时间表



病毒、间谍软件、Bot、网络钓鱼特征码和 IntelliTrap 更新时间表	
<input type="radio"/>	每间隔以下时间 (分钟) <input type="text" value="15"/>
<input checked="" type="radio"/>	每小时
<input type="radio"/>	每日
<input type="radio"/>	每周一次, 在 <input type="text" value="星期日"/>
<input type="radio"/>	仅手动更新
开始时间:	<input type="text" value="02"/> <input type="text" value="00"/>
	时 分
扫描引擎更新时间表	
<input checked="" type="radio"/>	每日
<input type="radio"/>	每周一次, 在 <input type="text" value="星期四"/>
<input type="radio"/>	仅手动更新
开始时间:	<input type="text" value="02"/> <input type="text" value="00"/>
	时 分
URL 过滤引擎更新时间表	
<input checked="" type="radio"/>	每日
<input type="radio"/>	每周一次, 在 <input type="text" value="星期二"/>
<input type="radio"/>	仅手动更新
开始时间:	<input type="text" value="04"/> <input type="text" value="00"/>
	时 分
<input type="button" value="保存"/>	<input type="button" value="取消"/>

9) IWSA 查看病毒日志:



9.4 诊断问题建议

如果测试中遇到问题，请收集抓包和debug日志信息。

- 1) Debug日志信息，需要打开intscan.ini文件

```
vim /etc/iscan/intscan.ini
```

如果是HTTP问题，请修改[http]下面的verbose=0 ->verbose=1

如果是FTP问题，请修改[ftp]下面的verbose=0 ->verbose=1

保存并退出。

重启服务，

如果是HTTP问题，重启HTTP服务。 `/etc/iscan/S99ISproxy stop; /etc/iscan/S99ISproxy start`

如果是FTP问题，重启FTP服务。 `/etc/iscan/S99ISftp stop; /etc/iscan/S99ISftp start`

- 2) 重新问题，需要在客户端和IWSVA端抓包。

IWSVA端抓包：



选择所有的网络接口，点击“添加”；然后点击“开始捕获”。

问题重现后，点击“停止捕获”，下载并保存抓包文件。

3) 收集CDT。



点击“生产系统信息文件”，下载并保存文件

4) 将收集的CDT、抓包文件和案件一起提交给技术支持团队分析。

10 FAQ

10.1 什么是补丁

- 修补了IWSA已解决问题的文件包
- 补丁分为hotfix和Patch
- Hotfix可以理解为小补，一般修复单个问题
- Patch可以理解为大补，是一系列Hotfix的积累
- Patch又分为应用层Patch和内核层Patch
- Hotfix都基于最新的应用层Patch

10.2 什么是bypass

- bypass的作用
当IWSA部署在桥接模式以及其衍生模式时，意外的情况下保证网络不断掉
IWSA不能处理的应用流量
- bypass的机制
硬件bypass
系统bypass
应用层bypass
- bypass的强度
硬件 > 系统 > 应用层

10.3 硬件bypass

- 原理：基于硬件lanbypass卡，如果被启用，IWSA就像一根网线，流量不过IWSA
- 适用场景：如果IWSA出现硬件故障，需要暂时bypass；或者如果需要重启网络；或者需要重启IWSA
- 好处：启用后完全不影响客户网络流量

注意事项：在启用lanbypass功能之前，需要设置IWSA的**管理口**连接，否则无法管理机器，因为在lanbypass启用之后，只用通过管理口或者COM口才能连上IWSA。

- 设置方法：
 - 使能：通过WebUI点击绕开通信
 - 关闭：通过WebUI点击禁止绕开通信

10.4 系统bypass (rpolicy)

- 原理：利用IWSA操作系统内核contrack进行bypass，即通常所说的rpolicy bypass；内核会根据rpolicy中的策略对流量进行相应处理，策略可以基于目标端口，源/目标IP，并发连接数，源/目标mac，网口，vlan
- 优势：无须重启网络，修改即时生效；灵活定制(可基于目标端口，目标IP，源IP，并发连接数等)
- 应用场景：

在性能测试中，IWSA的吞吐量不够 – 清空rpolicy

在某些时段，客户流量达到一定的并发值之后，上网会变慢 – 基于并发连接数的bypass

在某些情形下，内网通过IWSA不能访问某些网站 – bypass目标IP

在某些情形下，某些特殊的客户端或者某个子网不能上网 – bypass源IP

➤ 设置方法:

- 使能: 运行以下命令:

- echo "" > /proc/contrack/rpolicy

- 关闭: 运行以下命令:

- service network restart
- /etc/iscan/rcIwss restart

10.5 应用层bypass

➤ 原理: 配置Global Trusted URL list, 扫描程序会检查当前请求的URL是否在list里面, 是就不做扫描

➤ 应用场景: bypass常用门户网站, 如新浪、百度、搜狐; bypass常用视频网站、优酷、土豆; 某些特殊的网站扫描后无法正常访问

➤ 设置方法:

- 使能: 通过WebUI关闭virus scan, WRS, url filtering等功能

- 关闭: 通过WebUI开启virus scan, WRS, url filtering等功能

10.6 访问慢, 断网问题的三步骤思路

