

快速配置指南

HUAWEI USG6000, USG6000E, USG9500, NGFW Module
(新界面版)

文档版本: 04 (2021-05-07)

目录

	<u>登录Web配置界面</u>	005
	<u>Example 1：通过静态IP接入互联网</u>	008
	<u>Example 2：通过PPPoE接入互联网</u>	015
	<u>Example 3：通过多个运营商（ISP）接入互联网</u>	023
	<u>Example 4：私网用户通过NAPT访问Internet</u>	032
	<u>Example 5：公网用户通过NAT Server访问内部服务器</u>	038
	<u>Example 6：内外网用户同时通过公网IP访问FTP服务器</u>	046
	<u>Example 7：点到点IPSec隧道</u>	054
	<u>Example 8：点到多点IPSec隧道（策略模板）</u>	065
	<u>Example 9.1：客户端 L2TP over IPSec 接入（SecoClient）</u>	081

目录

	<u>Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)</u>	093
		
	<u>Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)</u>	104
		
	<u>Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)</u>	115
		
	<u>Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)</u>	126
		
	<u>Example 9.6: 客户端 L2TP over IPSec 接入 (Android)</u>	136
		
	<u>Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)</u>	145
		
	<u>Example 10.1: SSL VPN隧道接入 (网络扩展+本地认证)</u>	154
		
	<u>Example 10.2: SSL VPN隧道接入 (网络扩展+证书挑战认证)</u>	166
		
	<u>Example 11: 防火墙透明接入的负载分担场景</u>	181
		
	<u>Example 12: 防火墙旁挂在三层设备上的主备备份场景</u>	192
		

目录

	<u>Example 13：防火墙旁挂在三层设备上的负载分担场景</u>	208
	<u>Example 14：防火墙直路部署的主备备份场景</u>	230
	<u>Example 15：防火墙直路部署的负载分担场景</u>	241
	<u>Example 16：基于源地址的策略路由</u>	255
	<u>Example 17：基于用户的带宽管理</u>	264
	<u>Example 18：应用控制（限制P2P流量、禁用QQ）</u>	274

说明：

- 本文档基于USG6000E V600R007C00版本写作，可供USG6000E V600R007C00、USG6000/9500 V500R005C20、NGFW Module V500R005C20及后续版本参考。不同版本之间Web界面可能存在差异，您可以参考此案例的配置步骤，实际Web界面呈现请以所用设备为准。
- 本文档仅介绍防火墙典型场景的Web界面配置，如您需要了解详细的特性原理、通过命令行界面的配置方法以及获取更丰富的场景配置案例，请登录[华为企业技术支持网站](#)下载对应产品的文档；如果您需要了解防火墙常见故障定位及处理方法的相关信息，请登录[华为企业技术支持网站](#)下载对应产品的维护宝典。

登录 Web 配置界面

组网图



缺省配置

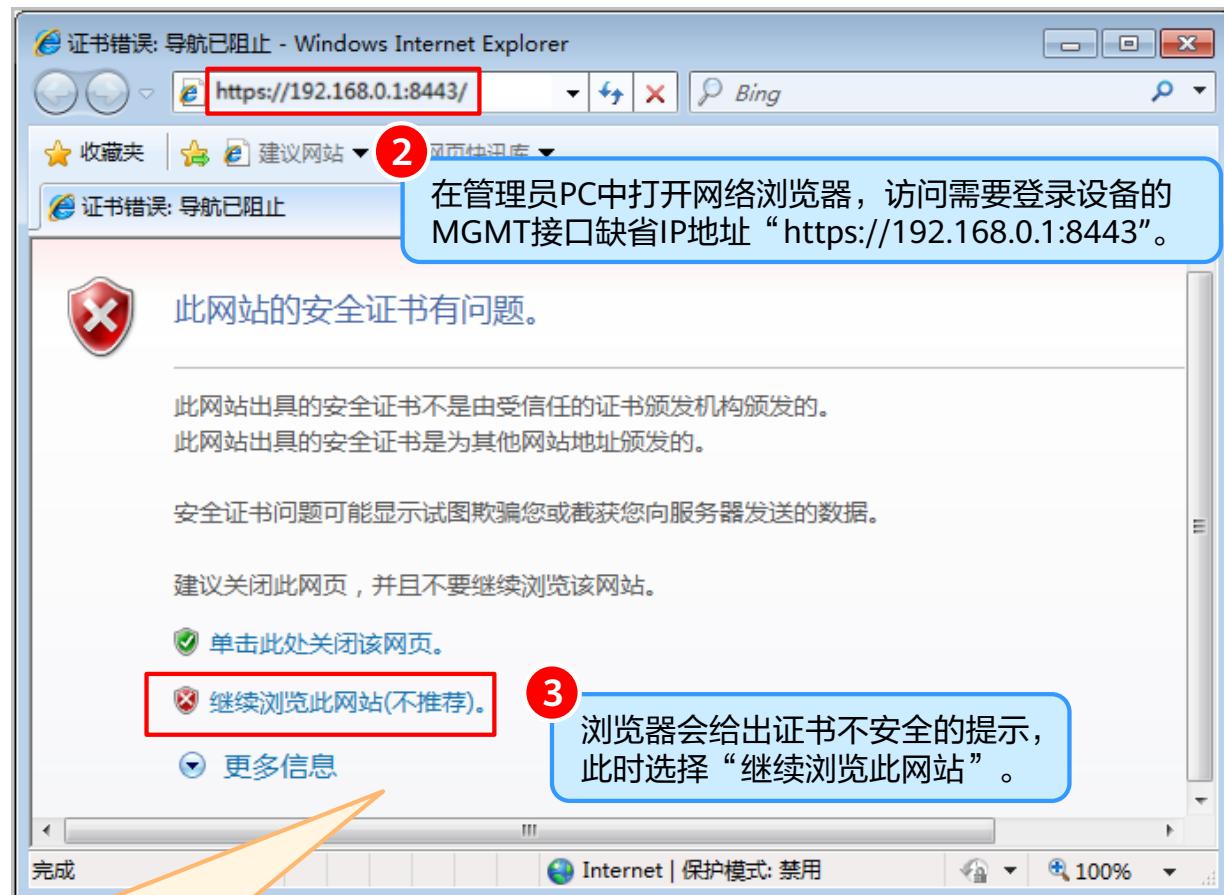
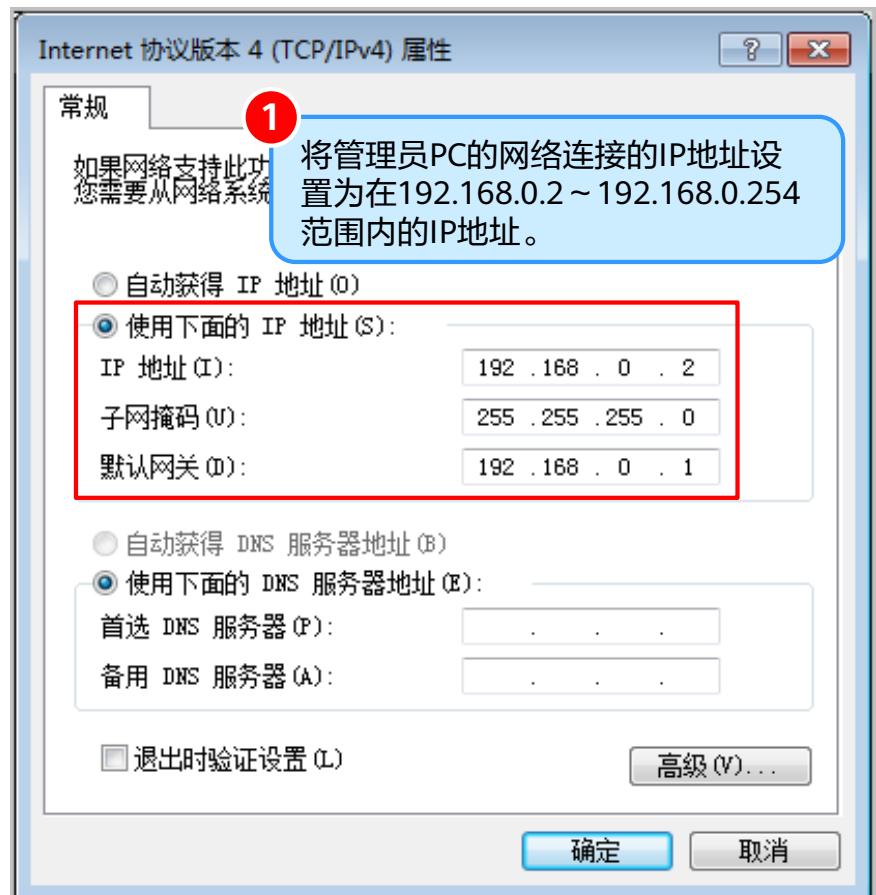
推荐的浏览器及版本

管理接口	GE0/0/0		10–11版本
IP 地址	192.168.0.1/24		62及以上版本
用户名 / 密码	您可以在《 华为安全产品缺省帐号与密码 》文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。		64及以上版本

说明：对于USG6000EV600R007C20及后续版本，缺省情况下无管理员。第一次登录Web界面时，须注册管理员账号和密码。通过该方式创建的管理员，拥有系统管理员角色权限和Web的服务类型，且不能是"manager-user@@vsys-name"虚拟系统管理员账号。

登录 Web 配置界面

登录步骤（以 IE 浏览器为例）



进入登录界面后，可单击“下载根证书”按钮下载由设备颁发的证书，并将下载到本地的证书导入管理员PC的浏览器，下次登录时将不会再出现证书不安全的提示。

登录 Web 配置界面

4 输入登录名、密码

5 进入Web配置界面

Web界面功能区域划分

板块页签

操作按钮

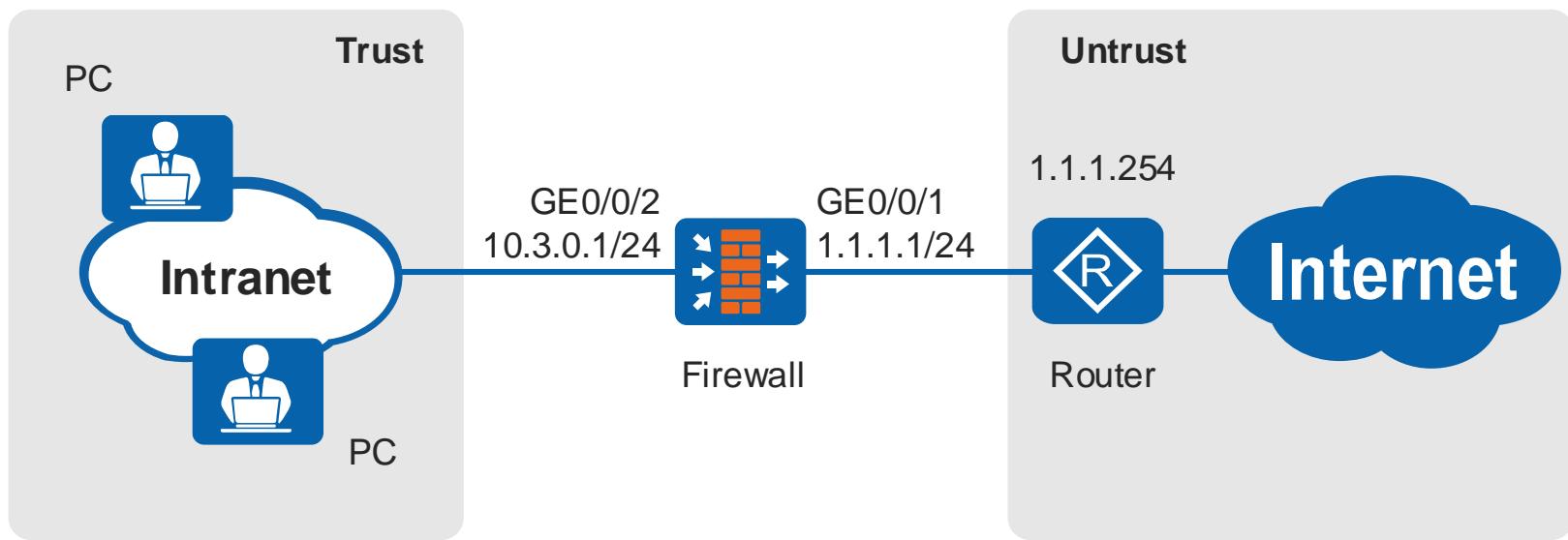
菜单导航树

操作区

CLI控制台

Example 1：通过静态IP接入互联网

组网图



局域网内所有PC都部署在10.3.0.0/24网段，均通过DHCP动态获得IP地址。

企业从运营商处获取的固定IP地址为1.1.1.1/24。企业需利用防火墙接入互联网。

项目	数据	说明
DNS服务器	1.2.2.2/24	向运营商获取。
网关地址	1.1.1.254/24	向运营商获取。

Example 1：通过静态IP接入互联网

Step1 配置接口

1. 在左侧导航栏中，点击“网络”图标（带红色圆圈）。

2. 在左侧子菜单中，点击“接口”图标（带红色圆圈）。

3. 在右侧列表中，选择“GE0/0/1”并点击编辑图标（带红色圆圈）。

4. 在“修改GigabitEthernet”对话框中，配置外网接口参数。设置“接口名称”为“GigabitEthernet0/0/1”，“虚拟系统”为“public”，“安全区域”为“untrust”，“模式”选择“路由”，“连接类型”选择“静态IP”，“IP地址”输入“1.1.1.1/24”，“默认网关”输入“1.1.1.254”，“首选DNS服务器”输入“1.2.2.2”，“备用DNS服务器”输入“”。勾选“多出口选项”。

5. 在右侧列表中，选择“GE0/0/2”并点击编辑图标（带红色圆圈）。

6. 在“修改GigabitEthernet”对话框中，配置内网接口参数。设置“接口名称”为“GigabitEthernet0/0/2”，“虚拟系统”为“public”，“安全区域”为“trust”，“模式”选择“路由”，“连接类型”选择“静态IP”，“IP地址”输入“10.3.0.1/24”，“默认网关”输入“”，“首选DNS服务器”输入“”，“备用DNS服务器”输入“”。取消勾选“多出口选项”。

Example 1：通过静态IP接入互联网

Step2 配置DHCP服务

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes icons for Home, Panel, Monitoring, Objects, Network (highlighted with a red box), and System. On the right, there are user authentication (admin), save (保存), and refresh (刷新) buttons, along with dropdown menus for Virtual System (public) and Language.

The left sidebar menu is expanded to show the 'DHCP服务器' (DHCP Server) section, which is further expanded to '服务' (Service). A red box labeled '2' highlights the '服务' option. A red arrow points from this box down to the '新建' (New) button in the main content area.

The main content area displays the 'DHCP服务列表' (DHCP Service List) with a table header: '接口名称' (Interface Name), '类型' (Type), '服务类型' (Service Type), and '选项' (Options). A red box labeled '1' highlights the '新建' (New) button. A red box labeled '3' highlights the first row of the table.

A modal window titled '新建DHCP服务' (New DHCP Service) is open. It contains the following configuration fields:

- 接口名称:** GE0/0/2 (selected)
- 类型:** IPv4 (selected)
- 服务类型:** 服务器 (Server) (selected)
- 可分配IP地址范围:** 10.3.0.2 - 10.3.0.254
- 子网掩码:** 255.255.255.0
- 默认网关:** 10.3.0.1
- DNS服务:** 使用系统的DNS设置 (Use system's DNS settings) (selected)
- 首选DNS服务器:** 1.2.2.2
- 备用DNS服务器:** (empty)

A red box highlights the entire configuration form. A callout bubble labeled '4' provides the following note:

配置内网接口GE0/0/2的DHCP服务，使其为局域网内的PC分配IP地址。

At the bottom of the modal are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 1：通过静态IP接入互联网

Step3 配置安全策略

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes the HUAWEI logo, user information (admin), and system buttons (提交, 保存, ...). The left sidebar has a tree view with '安全策略' expanded, showing '安全策略' selected. The main content area is titled '安全策略列表'.

1 A red circle highlights the '策略' icon in the top navigation bar.

2 A red circle highlights the '安全策略' link in the sidebar.

3 A red circle highlights the '新建安全策略' button in the top-left of the list area. A red arrow points from this circle to the '新建安全策略' dialog box.

4 A red circle highlights the '配置允许内网IP地址访问外网' callout box, which points to the '源与目的' section of the dialog box.

对话框内容 (New Security Policy Configuration):

- 常规设置:**
 - 名称: trust2untrust *
 - 描述:
 - 策略组: -- NONE --
 - 标签:
- 源与目的:**
 - 源安全区域: trust
 - 目的安全区域: untrust
 - 源地址/地区: 10.3.0.0/24
 - 目的地址/地区:
- VLAN ID:** 请输入 VLAN ID <1-4094>
- 用户与服务:**
 - 用户:
 - 接入方式:
 - 终端设备:
 - 服务:
 - 应用:
 - URL 分类:
 - 时间段:
- 动作设置:**
 - 动作: 允许 (radio button)

底部显示了关于反病毒、入侵防御、URL过滤等的说明文字。

Example 1：通过静态IP接入互联网

Step4 新建源NAT

The screenshot shows the HUAWEI USG6300 firewall's configuration interface. The top navigation bar includes icons for Home, Panel, Monitoring, Object, Network, and System, with the Strategy icon highlighted. The left sidebar has a tree view with 'NAT策略' (NAT Policy) selected, and a sub-menu 'NAT策略' is also highlighted. A red circle labeled '1' points to the '新建' (Create) button in the main toolbar. A red circle labeled '2' points to the 'NAT策略' link in the sidebar. A red circle labeled '3' points to the search bar. A red box highlights the '新建NAT策略' (Create NAT Policy) dialog box.

新建NAT策略

功能介绍

名称	policy_nat_1	
描述		
标签	请选择或输入标签	
NAT类型	<input checked="" type="radio"/> NAT <input type="radio"/> NAT64 <input type="radio"/> NAT66	
转换模式	仅转换源地址	
时间段	请选择时间段	
原始数据包	源安全区域: trust 目的类型: <input checked="" type="radio"/> 目的安全区域 <input type="radio"/> 出接口 [多选]	
源地址	10.3.0.0/24	[多选]
目的地址	请选择或输入地址	
服务	请选择或输入服务	
转换后的数据包	地址池中的地址 <input type="radio"/> 出接口地址 <input checked="" type="radio"/>	

提示: 为保证设备顺利转发NAT业务, 需要配置安全策略。[新建安全策略]

4 新建源NAT, 实现内网用户正常访问Internet。

Bottom right buttons: 确定 (Confirm), 取消 (Cancel).

Example 1：通过静态IP接入互联网

Step5 结果验证（1）

The screenshot shows the HUAWEI USG6300 network management interface. The left sidebar has a '接口' (Interface) tab selected, showing various interface configurations. The main area displays a table of interfaces:

接口名称	安全区域	虚拟系统	IP地址	连接类型	VLAN/VXLAN	模式	物理	状态	IPv4	IPv6	启用	编辑
GE0/0/0	trust	public	192.168.1.1	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/1	untrust	public	192.168.1.2	物理端口	untagged	透传	DOWN	DOWN	DOWN	DOWN	checked	
GE0/0/2	trust	public	192.168.1.3	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/3	untrust	public	192.168.1.4	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/4	trust	public	192.168.1.5	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/5	untrust	public	192.168.1.6	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/6	trust	public	192.168.1.7	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/7	untrust	public	192.168.1.8	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/8	trust	public	192.168.1.9	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/9	untrust	public	192.168.1.10	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/10	trust	public	192.168.1.11	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/11	untrust	public	192.168.1.12	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/12	trust	public	192.168.1.13	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/13	untrust	public	192.168.1.14	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/14	trust	public	192.168.1.15	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/15	untrust	public	192.168.1.16	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/16	trust	public	192.168.1.17	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/17	untrust	public	192.168.1.18	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/18	trust	public	192.168.1.19	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/19	untrust	public	192.168.1.20	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/20	trust	public	192.168.1.21	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/21	untrust	public	192.168.1.22	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/22	trust	public	192.168.1.23	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/23	untrust	public	192.168.1.24	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/24	trust	public	192.168.1.25	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/25	untrust	public	192.168.1.26	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/26	trust	public	192.168.1.27	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/27	untrust	public	192.168.1.28	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/28	trust	public	192.168.1.29	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/29	untrust	public	192.168.1.30	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/30	trust	public	192.168.1.31	物理端口	untagged	透传	UP	UP	UP	UP	checked	
GE0/0/31	untrust	public	192.168.1.32	物理端口	untagged	透传	UP	UP	UP	UP	checked	

A red box highlights the '物理' (Physical) and 'IPv4' columns for the GE0/0/1 interface, which are both shown as 'UP'. A callout bubble with the number '1' points to this highlighted area. A text box contains the validation instruction: '接口GigabitEthernet 0/0/1的物理状态和IPv4状态应为Up'.

Example 1: 通过静态IP接入互联网

Step5 结果验证（2）

2

在内网PC上执行命令ipconfig /all，PC正确分配到IP地址和DNS地址。

```
C:\> ipconfig /all

Windows IP Configuration

    Host Name          : test
    Primary Dns Suffix : test.com
    Node Type          : Hybrid
    IP Routing Enabled: No
    WINS Proxy Enabled: No
    DNS Suffix Search List: test.com

Ethernet adapter 1 :

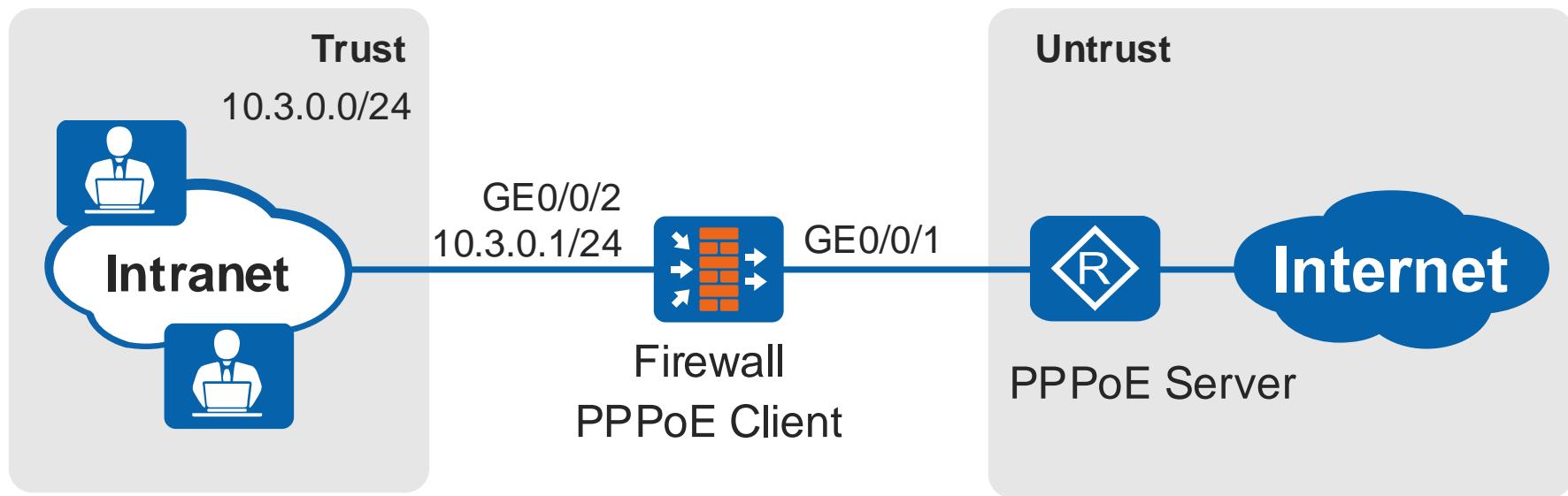
    Connection-specific DNS Suffix  . : dhcpserver.com
    Description                   : Realtek RTL8139/810x Family Fast Ethernet NIC
    Physical Address              : 00-1B-B9-7A-7D-61
    Dhcp Enabled                  : Yes
    Autoconfiguration Enabled     : Yes
    IP Address                   : 10.3.0.100
    Subnet Mask                  : 255.255.255.0
    Default Gateway               : 10.3.0.1
    DHCP Server                  : 10.3.0.1
    DNS Servers                  : 1.2.2.2
    Lease Obtained                : 2014年10月16日 15:00:00
    Lease Expires                 : 2014年10月17日 15:00:00
```

3

局域网内PC能通过域名访问Internet

Example 2：通过PPPoE接入互联网

组网图



局域网内所有PC都部署在10.3.0.0/24网段，均通过DHCP动态获得IP地址。

设备作为Client，通过PPPoE协议向Server（运营商设备）拨号后获得IP地址，实现接入Internet。

项目	数据	说明
GigabitEthernet 0/0/1	安全区域: Untrust	通过拨号向PPPoE Server（运营商设备）拨号获得IP地址、DNS地址。 拨号用户名: user 拨号密码: Password@
GigabitEthernet 0/0/2	IP地址: 10.3.0.1/24 安全区域: Trust	通过DHCP，给局域网内PC动态分配IP地址。
DNS服务器	1.2.2.2/24	向运营商获取。

Example 2: 通过PPPoE接入互联网

Step1 配置接口

1 点击“网络”图标进入网络配置界面。

2 在左侧导航栏中点击“接口”图标。

3 在右侧列表中选择外网接口（GE0/0/1）并点击编辑图标。

4 在“修改GigabitEthernet”对话框中，配置外网接口参数。设置接口名称为“GigabitEthernet0/0/1”，虚拟系统为“public”，安全区域为“untrust”，模式为“路由”，连接类型选择“PPPoE”，用户名输入“user”，密码输入“*****”，在线方式选择“一直在线”，勾选“自动获得IP地址”。
配置外网接口参数

5 在右侧列表中选择内网接口（GE0/0/2）并点击编辑图标。

6 在“修改GigabitEthernet”对话框中，配置内网接口参数。设置接口名称为“GigabitEthernet0/0/2”，虚拟系统为“public”，安全区域为“trust”，模式为“路由”，连接类型选择“静态IP”，IP地址输入“10.3.0.1/24”，勾选“多出口选项”。
配置内网接口参数

Example 2: 通过PPPoE接入互联网

Step2 配置DHCP服务

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes the HUAWEI logo, user information (admin), and system buttons (提交, 保存, ...). The main menu on the left has sections like 接口, 接口对, 安全区域, VXLAN, DNS, and DHCP服务器, with '服务' selected. The top right shows a 'DHCP服务列表' table with columns: 接口名称, 类型, 服务类型, 选项. A red box labeled '1' highlights the '新建' (New) button. A red arrow labeled '2' points to the '服务' section in the sidebar. A red box labeled '3' highlights the '接口名称' dropdown set to 'GE0/0/2'. A red box labeled '4' highlights the configuration area for the new service, which includes fields for IP range (10.3.0.2 to 10.3.0.254), subnet mask (255.255.255.0), and gateway (10.3.0.1). A callout bubble states: '配置内网接口GE0/0/2的DHCP服务，使其为局域网内的PC分配IP地址。' (Configure the DHCP service for the internal network interface GE0/0/2, so that it can allocate IP addresses to PCs in the local network.)

1

2

3

4

配置内网接口GE0/0/2的DHCP服务，使其为局域网内的PC分配IP地址。

接口名称	类型	服务类型	选项
GE0/0/2	IPv4	服务器	IPv6 中继 指定
10.3.0.2	255.255.255.0	10.3.0.1	
使用系统的DNS设置	指定	1.2.2.2	

确定 取消

Example 2: 通过PPPoE接入互联网

Step3 配置安全策略

1 新建安全策略

2 安全策略

3 新建安全策略

4 配置允许内网IP地址访问外网

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。 [选择策略模板] 交换源和目的?

常规设置	名称: <input type="text" value="trust2untrust"/> * 描述: 策略组: -- NONE -- 标签: 请选择或输入标签
源与目的	源安全区域: trust 目的安全区域: untrust 源地址/地区 ? : 10.3.0.0/24 目的地/地区 ? : 请选择或输入地址 VLAN ID: 请输入VLAN ID <1-4094>
用户与服务	用户 ? : 请选择或输入用户 接入方式 ? : 请选择接入方式 终端设备 ? : 请选择或输入终端设备 服务 ? : 请选择或输入服务 应用: 请选择或输入应用 URL分类: 请选择或输入URL分类 时间段: 请选择时间段
动作设置	动作: <input checked="" type="radio"/> 允许 <input type="radio"/> 禁止
内容安全	反病毒:NONE;入侵防御:NONE;URL过滤:NONE;文件过滤:NONE;内容过滤:NONE;应用行为控制:NONE;云接入安全感知:NONE;邮件过滤:NONE;APT防御:NONE;DNS过滤:NONE;
其他选项	记录流量日志:NONE;记录策略命中日志:禁用;记录会话日志:禁用;会话老化时间:NONE;自定义长连接:禁用;

确定 **确定并复制** **命令预览** **取消**

Example 2: 通过PPPoE接入互联网

Step4 新建源NAT

The screenshot shows the HUAWEI USG6300 firewall's configuration interface. The top navigation bar includes icons for Home, Panel, Monitoring, Policies (highlighted with a red box and circled 1), Objects, Network, and System. The left sidebar menu is expanded under the 'NAT策略' (NAT Policy) section, with 'NAT策略' also highlighted with a red box and circled 2. A search bar at the top has a red circle 3 pointing to it. The main content area displays a table of existing NAT policies and a modal window for creating a new policy.

New NAT Policy Configuration:

- Name:** policy_nat_1
- Description:** (empty)
- Label:** (empty)
- NAT Type:** NAT (radio button selected)
- Conversion Mode:** Only convert source address
- Time Range:** (empty)
- Original Data包 (Data Packets):**
 - Source Security Zone:** trust
 - Destination Type:** Destination security zone (radio button selected)
 - Source Address:** 10.3.0.0/24
 - Destination Address:** (empty)
 - Service:** (empty)
- Converted Data包 (Converted Data Packets):**
 - Source Address Conversion:** Interface address (radio button selected)

提示: To ensure smooth NAT forwarding, please configure a security policy. [Create Security Policy]

操作按钮: 确定 (Confirm) | 取消 (Cancel)

右侧面板: 每页 50 | 1 | GO | CLI 控制台 (CLI Control Console)

右侧悬浮框: 4 新建源NAT, 实现内网用户正常访问Internet。

Example 2：通过PPPoE接入互联网

Step5 配置缺省路由

The screenshot shows the HUAWEI USG6300 network management interface. The top navigation bar includes icons for Home, Panel, Monitoring, Objects, Network (highlighted with a red box and labeled 1), System, and user Admin. The left sidebar lists various network components: Interface, Interface Pair, Security Zone, VXLAN, DNS, DHCP Server, and a expanded 'Route' section containing Intelligent Routing, Virtual Router, ISP Routing, RIP, OSPF, BGP, Dynamic Routing Monitoring Table, and Route Table. Under 'Route', the 'Static Routing' option is selected and highlighted with a red box (labeled 2). The main content area has two tabs: 'Configure Default Priority' (显示) and 'Static Route List'. The 'Configure Default Priority' tab shows fields for IPv4 and IPv6 default priorities (both set to 60) with a 'Apply' button. The 'Static Route List' tab shows a table of routes with columns: Original Virtual Router, Destination Address/Mask, Destination Virtual Router, Next Hop, Priority, Interface, Bound IP-Link Name, Bound BFD Name, Description, and Edit. A new route entry is being created in a modal dialog (labeled 3). The 'New Static Route' dialog contains the following fields:

Protocol Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Original Virtual Router	public
Destination Address/Mask	0.0.0.0/0.0.0.0 *
Destination Virtual Router	public
Interface	GE0/0/1
Next Hop	
Priority	60 <1-255>
Reliability Detection	<input checked="" type="radio"/> No Detection <input type="radio"/> Bind BFD <input type="radio"/> Bind IP-Link
Description	

A callout bubble (labeled 4) points to the priority field with the text: "Configure default route to ensure internal network users can access the Internet route." At the bottom of the dialog are 'Confirm' and 'Cancel' buttons.

Example 2: 通过PPPoE接入互联网

Step6 结果验证 (1)

The screenshot shows the Huawei Network Management System (NMS) interface. The left sidebar has a tree view with '接口' (Interface) selected. The main area is titled '接口列表' (Interface List) and displays a table of interfaces. A red circle labeled '1' points to the row for 'GE0/0/1'. A callout box with a blue border contains the text: '接口GigabitEthernet 0/0/1的物理状态和IPv4状态应为Up' (The physical state and IPv4 state of interface GigabitEthernet 0/0/1 should be Up). The table columns include: 接口名称 (Interface Name), 安全区域 (Security Zone), 虚拟系统 (Virtual System), IP地址 (IP Address), 连接类型 (Connection Type), VLAN/VXLAN, 模式 (Mode), 状态 (Status) with sub-fields IPv4 and IPv6, 启用 (Enabled), and 编辑 (Edit). The 'GE0/0/1' row shows '物理' (Physical) and 'IPv4' both in green, indicating they are Up. Other interfaces like GE0/0/0, GE0/0/2, etc., show mixed colors or red.

Example 2: 通过PPPoE接入互联网

Step6 结果验证（2）

2

在内网PC上执行命令ipconfig /all，PC正确分配到IP地址和DNS地址。

```
C:\> ipconfig /all

Windows IP Configuration

        Host Name          : test
        Primary Dns Suffix  . . . . . : test.com
        Node Type           . . . . . : Hybrid
        IP Routing Enabled. . . . . : No
        WINS Proxy Enabled. . . . . : No
        DNS Suffix Search List. . . . . : test.com

Ethernet adapter 1 :

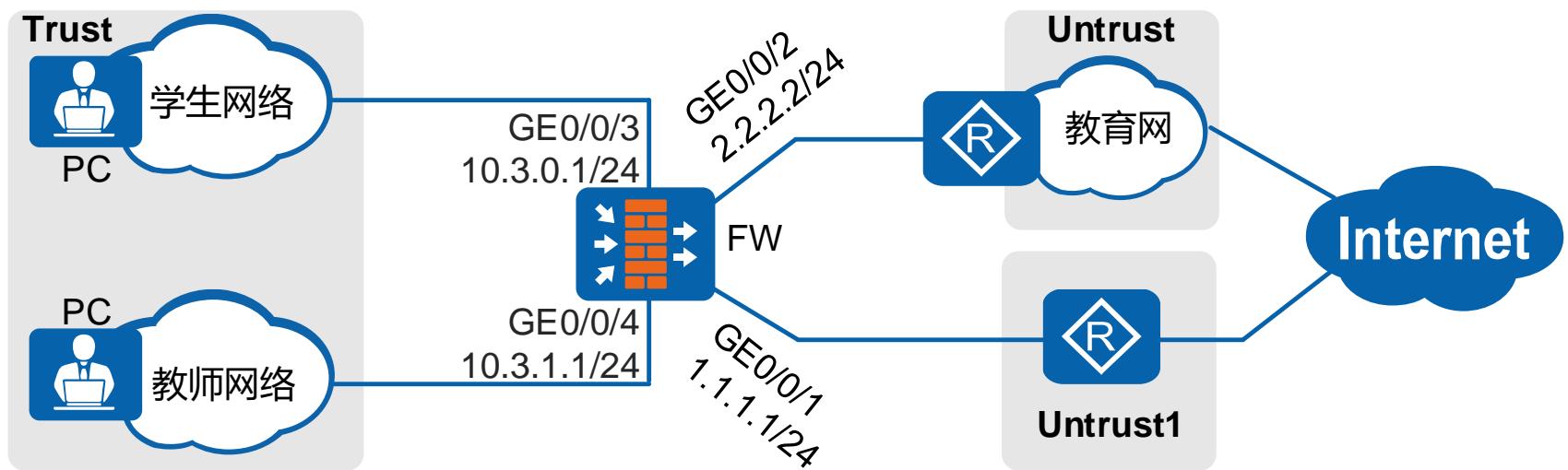
        Connection-specific DNS Suffix  . : dhcpserver.com
        Description . . . . . . . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-1B-B9-7A-7D-61
        Dhcp Enabled. . . . . . . . . . : Yes
        Autoconfiguration Enabled. . . . . : Yes
        IP Address. . . . . . . . . . . : 10.3.0.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.3.0.1
        DHCP Server . . . . . . . . . . . : 10.3.0.1
        DNS Servers . . . . . . . . . . . : 1.2.2.2
        Lease Obtained. . . . . . . . . . : 2014年10月16日 15:00:00
        Lease Expires . . . . . . . . . . : 2014年10月17日 15:00:00
```

3

局域网内PC能通过域名访问Internet

Example 3: 通过多个运营商 (ISP) 接入互联网

组网图



某高校在网络边界处部署了FW作为安全网关，要求学生网络中的PC只能通过教育网访问Internet，教师网络中的PC只能通过运营商网络访问Internet。

项目	策略路由policy_route_1	策略路由policy_route_2
类型	入接口	入接口
入接口	GE0/0/3	GE0/0/4
源地址	10.3.0.0/24	10.3.1.0/24
动作	转发	转发
出接口类型	单出口	单出口
出接口	GE0/0/2	GE0/0/1
下一跳	2.2.2.254	1.1.1.254

Example 3: 通过多个运营商 (ISP) 接入互联网

Step1 配置安全区域

The screenshot shows the HUAWEI USG6300 network management interface. The top navigation bar includes the HUAWEI logo, user 'admin', and tabs for 面板 (Panel), 监控 (Monitoring), 对象 (Object), 网络 (Network, highlighted with a red box), and 系统 (System). The left sidebar lists various network components like DNS, DHCP, and IPsec. The main area shows a '安全区域列表' (Security Zone List) table with columns for 名称 (Name), 优先级 (Priority), 描述 (Description), and 接口数 (Interface Count). A red box highlights the '新建' (New) button. A red arrow points from the '新建' button to a modal dialog titled '新建安全区域' (Create New Security Zone). The dialog contains fields for '名称' (Name) set to 'untrust1' and '优先级' (Priority) set to '2'. A blue callout box labeled '创建安全区域untrust1' (Create security zone untrust1) is positioned over the dialog. At the bottom of the dialog are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 3: 通过多个运营商 (ISP) 接入互联网

Step2 配置接口 (1)

1 网络

2 接口

3 编辑

4 配置外网接口参数

5

6 配置外网接口参数

接口名称	安全区域	虚拟系统	IP地址	连接类型	VLAN	模式	状态	启用
GE0/0/0(GE0/MGMT)							物理	IPv4 + +
GE0/0/1							物理	IPv4 + +
GE0/0/2							物理	IPv4 +
GE0/0/3							物理	IPv4 +
GE0/0/4							物理	IPv4 +
GE0/0/5							物理	IPv4 +
GE0/0/6							物理	IPv4 +
GE0/0/7							物理	IPv4 +
GE0/0/8							物理	IPv4 +
GE0/0/9							物理	IPv4 +
GE0/0/10							物理	IPv4 +
GE0/0/11							物理	IPv4 +
GE0/0/12							物理	IPv4 +
GE0/0/13							物理	IPv4 +
GE0/0/14							物理	IPv4 +
GE0/0/15							物理	IPv4 +
GE0/0/16							物理	IPv4 +
GE0/0/17							物理	IPv4 +
GE0/0/18							物理	IPv4 +
GE0/0/19							物理	IPv4 +
GE0/0/20							物理	IPv4 +
GE0/0/21							物理	IPv4 +
GE0/0/22							物理	IPv4 +
GE0/0/23							物理	IPv4 +
GE0/0/24							物理	IPv4 +
GE0/0/25							物理	IPv4 +
GE0/0/26							物理	IPv4 +
GE0/0/27							物理	IPv4 +
GE0/0/28							物理	IPv4 +
GE0/0/29							物理	IPv4 +
GE0/0/30							物理	IPv4 +
GE0/0/31							物理	IPv4 +
GE0/0/32							物理	IPv4 +
GE0/0/33							物理	IPv4 +
GE0/0/34							物理	IPv4 +
GE0/0/35							物理	IPv4 +
GE0/0/36							物理	IPv4 +
GE0/0/37							物理	IPv4 +
GE0/0/38							物理	IPv4 +
GE0/0/39							物理	IPv4 +
GE0/0/40							物理	IPv4 +
GE0/0/41							物理	IPv4 +
GE0/0/42							物理	IPv4 +
GE0/0/43							物理	IPv4 +
GE0/0/44							物理	IPv4 +
GE0/0/45							物理	IPv4 +
GE0/0/46							物理	IPv4 +
GE0/0/47							物理	IPv4 +
GE0/0/48							物理	IPv4 +
GE0/0/49							物理	IPv4 +
GE0/0/50							物理	IPv4 +
GE0/0/51							物理	IPv4 +
GE0/0/52							物理	IPv4 +
GE0/0/53							物理	IPv4 +
GE0/0/54							物理	IPv4 +
GE0/0/55							物理	IPv4 +
GE0/0/56							物理	IPv4 +
GE0/0/57							物理	IPv4 +
GE0/0/58							物理	IPv4 +
GE0/0/59							物理	IPv4 +
GE0/0/60							物理	IPv4 +
GE0/0/61							物理	IPv4 +
GE0/0/62							物理	IPv4 +
GE0/0/63							物理	IPv4 +
GE0/0/64							物理	IPv4 +
GE0/0/65							物理	IPv4 +
GE0/0/66							物理	IPv4 +
GE0/0/67							物理	IPv4 +
GE0/0/68							物理	IPv4 +
GE0/0/69							物理	IPv4 +
GE0/0/70							物理	IPv4 +
GE0/0/71							物理	IPv4 +
GE0/0/72							物理	IPv4 +
GE0/0/73							物理	IPv4 +
GE0/0/74							物理	IPv4 +
GE0/0/75							物理	IPv4 +
GE0/0/76							物理	IPv4 +
GE0/0/77							物理	IPv4 +
GE0/0/78							物理	IPv4 +
GE0/0/79							物理	IPv4 +
GE0/0/80							物理	IPv4 +
GE0/0/81							物理	IPv4 +
GE0/0/82							物理	IPv4 +
GE0/0/83							物理	IPv4 +
GE0/0/84							物理	IPv4 +
GE0/0/85							物理	IPv4 +
GE0/0/86							物理	IPv4 +
GE0/0/87							物理	IPv4 +
GE0/0/88							物理	IPv4 +
GE0/0/89							物理	IPv4 +
GE0/0/90							物理	IPv4 +
GE0/0/91							物理	IPv4 +
GE0/0/92							物理	IPv4 +
GE0/0/93							物理	IPv4 +
GE0/0/94							物理	IPv4 +
GE0/0/95							物理	IPv4 +
GE0/0/96							物理	IPv4 +
GE0/0/97							物理	IPv4 +
GE0/0/98							物理	IPv4 +
GE0/0/99							物理	IPv4 +
GE0/0/100							物理	IPv4 +
GE0/0/101							物理	IPv4 +
GE0/0/102							物理	IPv4 +
GE0/0/103							物理	IPv4 +
GE0/0/104							物理	IPv4 +
GE0/0/105							物理	IPv4 +
GE0/0/106							物理	IPv4 +
GE0/0/107							物理	IPv4 +
GE0/0/108							物理	IPv4 +
GE0/0/109							物理	IPv4 +
GE0/0/110							物理	IPv4 +
GE0/0/111							物理	IPv4 +
GE0/0/112							物理	IPv4 +
GE0/0/113							物理	IPv4 +
GE0/0/114							物理	IPv4 +
GE0/0/115							物理	IPv4 +
GE0/0/116							物理	IPv4 +
GE0/0/117							物理	IPv4 +
GE0/0/118							物理	IPv4 +
GE0/0/119							物理	IPv4 +
GE0/0/120							物理	IPv4 +
GE0/0/121							物理	IPv4 +
GE0/0/122							物理	IPv4 +
GE0/0/123							物理	IPv4 +
GE0/0/124							物理	IPv4 +
GE0/0/125							物理	IPv4 +
GE0/0/126							物理	IPv4 +
GE0/0/127							物理	IPv4 +
GE0/0/128							物理	IPv4 +
GE0/0/129							物理	IPv4 +
GE0/0/130							物理	IPv4 +
GE0/0/131							物理	IPv4 +
GE0/0/132							物理	IPv4 +
GE0/0/133							物理	IPv4 +
GE0/0/134							物理	IPv4 +
GE0/0/135							物理	IPv4 +
GE0/0/136							物理	IPv4 +
GE0/0/137							物理	IPv4 +
GE0/0/138							物理	IPv4 +
GE0/0/139							物理	IPv4 +
GE0/0/140							物理	IPv4 +
GE0/0/141							物理	IPv4 +
GE0/0/142							物理	IPv4 +
GE0/0/143							物理	IPv4 +
GE0/0/144							物理	IPv4 +
GE0/0/145							物理	IPv4 +
GE0/0/146							物理	IPv4 +
GE0/0/147							物理	IPv4 +
GE0/0/148							物理	IPv4 +
GE0/0/149							物理	IPv4 +
GE0/0/150							物理	IPv4 +
GE0/0/151							物理	IPv4 +
GE0/0/152							物理	IPv4 +
GE0/0/153							物理	IPv4 +
GE0/0/154							物理	IPv4 +
GE0/0/155							物理	IPv4 +
GE0/0/156							物理	IPv4 +
GE0/0/157							物理	IPv4 +
GE0/0/158							物理	IPv4 +
GE0/0/159							物理	IPv4 +
GE0/0/160							物理	IPv4 +
GE0/0/161							物理	IPv4 +
GE0/0/162							物理	IPv4 +
GE0/0/163							物理	IPv4 +
GE0/0/164							物理	IPv4 +
GE0/0/165							物理	IPv4 +
GE0/0/166							物理	IPv4 +
GE0/0/167							物理	IPv4 +
GE0/0/168							物理	IPv4 +
GE0/0/169							物理	IPv4 +
GE0/0/170							物理	IPv4 +
GE0/0/171							物理	IPv4 +
GE0/0/172							物理	IPv4 +
GE0/0/173							物理	IPv4 +
GE0/0/174							物理	IPv4 +
GE0/0/175							物理	IPv4 +
GE0/0/176							物理	IPv4 +
GE0/0/177							物理	IPv4 +
GE0/0/178							物理	IPv4 +
GE0/0/179							物理	IPv4 +
GE0/0/180							物理	IPv4 +
GE0/0/181							物理	IPv4 +
GE0/0/182							物理	IPv4 +
GE0/0/183							物理	IPv4 +
GE0/0/184							物理	IPv4 +
GE0/0/185							物理	IPv4 +
GE0/0/186							物理	IPv4 +
GE0/0/187							物理	IPv4 +
GE0/0/188							物理	IPv4 +
GE0/0/189							物理	IPv4 +
GE0/0/190					</td			

Example 3: 通过多个运营商 (ISP) 接入互联网

Step2 配置接口 (2)

1 点击“网络”图标。

2 点击“接口”图标。

3 选择要配置的内网接口，如 GE0/0/3、GE0/0/4、GE0/0/5、GE0/0/6。

4 在“修改GigabitEthernet”对话框中配置内网接口参数。设置接口名称为 GigabitEthernet0/0/3，连接类型为静态IP，IP地址为 10.3.0.1/24，模式为路由。

5 在“修改GigabitEthernet”对话框中配置内网接口参数。设置接口名称为 GigabitEthernet0/0/4，连接类型为静态IP，IP地址为 10.3.1.1/24，模式为路由。

6 在“修改GigabitEthernet”对话框中配置内网接口参数。设置接口名称为 GigabitEthernet0/0/5，连接类型为静态IP，IP地址为 10.3.2.1/24，模式为路由。

配置内网接口参数

配置内网接口参数

Example 3：通过多个运营商（ISP）接入互联网

Step3 配置安全策略

1 策略

2 安全策略

3 新建安全策略

4 允许学生网络中的PC访问Internet

5 允许教师网络中的PC访问Internet

The screenshot shows the Huawei Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 保存' buttons. The main menu has tabs: '面板' (Dashboard), '监控' (Monitoring), '策略' (Policy), '对象' (Object), '网络' (Network), and '系统' (System). A red box highlights the '策略' tab. On the left, a sidebar under '安全策略' (Security Policy) has '安全策略' selected, with a red box around it. A red arrow points from '3' to the '新建安全策略' (Create Security Policy) button. Below the sidebar is a search bar with placeholder '请输入要查询的内容' (Enter search content) and a '添加查询项' (Add search item) button. The main area is titled '安全策略列表' (Security Policy List) and displays a table of existing policies. The table columns include: 序号 (Index), 名称 (Name), 描述 (Description), 标签 (Label), VLAN ID, 源安全区域 (Source Security Zone), 目的安全区域 (Target Security Zone), 目的地址/地区 (Destination Address/Region), 用户 (User), 服务 (Service), 应用 (Application), 时间段 (Time Period), 动作 (Action), and 内容安全 (Content Security). A red box highlights the '新建安全策略' button. The bottom section shows two '新建安全策略' (Create Security Policy) dialog boxes. Both dialogs have a red border and contain identical fields: '常规设置' (General Settings) with '名称' (Name) set to 'policy_sec_1' or 'policy_sec_2'; '源与目的' (Source and Destination) with '源安全区域' (Source Security Zone) set to 'trust' and '目的安全区域' (Target Security Zone) set to 'untrust' or 'untrust1'; '用户与服务' (User and Service) with '源地址/地区' (Source Address/Region) set to '10.3.0.0/24' or '10.3.1.0/24'; '动作设置' (Action Settings) with '动作' (Action) set to '允许' (Allow); '内容安全' (Content Security) with '反病毒:NONE;入侵防御:NONE;URL过滤:NONE;文件过滤:NONE;内容过滤:NONE;应用行为控制:NONE;云接入安全感知:NONE;邮件过滤:NONE;APT防御:NONE;DNS过滤:NONE'; and '其他选项' (Other Options) with '记录流量日志:NONE;记录策略命中日志:禁用;记录会话日志:禁用;会话老化时间:NONE;自定义长连接:禁用;'. The right dialog box has a red box highlighting its content.

Example 3: 通过多个运营商 (ISP) 接入互联网

Step4 配置源NAT地址池

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 保存' buttons. The main menu has tabs: '面板' (Panel), '监控' (Monitoring), '策略' (Policy), '对象' (Object), '网络' (Network), and '系统' (System). A red box highlights the '策略' tab. The left sidebar menu under 'NAT策略' (NAT Policy) has 'NAT策略' selected, indicated by a red box and the number 2. The main content area shows three tabs: 'NAT策略' (selected), '源转换地址池' (Source NAT Address Pool), and '目的转换' (Destination NAT). A red box highlights the '源转换地址池' tab and the number 1. Below it, a red box highlights the '新建' (Create) button and the number 3.

New Source NAT Address Pool Configuration (address_1):

- Address Pool Name:** address_1
- IP Address Range:** 2.2.2.10-2.2.2.15
- Health Check:** Please select health check [Configure]
- Black Hole Routing:** Enabled (switch on)
- Port Address Translation:** Enabled (switch on)
- Advanced Options:** [Open]

New Source NAT Address Pool Configuration (address_2):

- Address Pool Name:** address_2
- IP Address Range:** 1.1.1.10-1.1.1.15
- Health Check:** Please select health check [Configure]
- Black Hole Routing:** Enabled (switch on)
- Port Address Translation:** Enabled (switch on)
- Advanced Options:** [Open]

At the bottom, a red box highlights the 'Create NAT address pool address_1' button and the number 4. Another red box highlights the 'Create NAT address pool address_2' button and the number 5.

Example 3: 通过多个运营商 (ISP) 接入互联网

Step5 配置源NAT策略

1 策略 - NAT策略

2 NAT策略

3 新建

4 学生网络中的PC访问 Internet时进行地址转换

5 教师网络中的PC访问 Internet时进行地址转换

新建NAT策略	
功能介绍	功能介绍
名称 policy_nat_1	名称 policy_nat_2
描述	描述
标签 请选择或输入标签	标签 请选择或输入标签
NAT类型 <input checked="" type="radio"/> NAT <input type="radio"/> NAT64 <input type="radio"/> NAT66	NAT类型 <input checked="" type="radio"/> NAT <input type="radio"/> NAT64 <input type="radio"/> NAT66
转换模式 仅转换源地址	转换模式 仅转换源地址
时间段 请选择时间段	时间段 请选择时间段
原始数据包	原始数据包
源安全区域 trust	源安全区域 trust
目的类型 <input checked="" type="radio"/> 目的的安全区域 <input type="radio"/> 出接口	目的类型 <input checked="" type="radio"/> 目的的安全区域 <input type="radio"/> 出接口
untrust	untrust
源地址⑦ 请选择或输入地址	源地址⑦ 请选择或输入地址
目的地址⑦ 请选择或输入地址	目的地址⑦ 请选择或输入地址
服务⑦ 请选择或输入服务	服务⑦ 请选择或输入服务
转换后的数据包	转换后的数据包
源地址转换为 <input checked="" type="radio"/> 地址池中的地址 <input type="radio"/> 出接口地址	源地址转换为 <input checked="" type="radio"/> 地址池中的地址 <input type="radio"/> 出接口地址
源转换地址池 address_1	源转换地址池 address_2
提示：为保证设备顺利转发NAT业务，需要配置安全策略。[新建安全策略]	

确定 **取消**

Example 3: 通过多个运营商 (ISP) 接入互联网

Step6 配置策略路由

The screenshot shows the HUAWEI Network Management System interface with the following steps highlighted:

- 1**: Click on the **网络** (Network) icon in the top navigation bar.
- 2**: Click on the **智能选路** (Smart Routing) option in the left sidebar under the **路由** (Routing) category.
- 3**: Click on the **新建** (New) button in the top toolbar of the **新建策略路由** (Create Policy Route) dialog.
- 4**: Configuration for **policy_route_1**:
 - 名称**: policy_route_1
 - 匹配条件** (Matching Conditions):
 - 类型**: 入接口 (In Interface)
 - 入接口**: GE0/0/3
 - 源地址**: 10.3.0.0/24
 - 目的地址**: 请选择或输入地址
 - 用户**: 请选择或输入用户
 - 服务**: 请选择或输入服务
 - 应用**: 请选择或输入应用
 - 时间段**: 请选择时间段
 - DSCP优先级**: any
 - 动作**: 转发 (Forwarding)
 - 出接口类型**: 单出口 (Single Exit)
 - 单出口配置** (Single Exit Configuration):
 - 出接口**: GE0/0/2
 - 下一跳**: 2.2.2.254
 - 监控**: 监控 (Monitoring) checkbox
- 5**: Configuration for **policy_route_2**:
 - 名称**: policy_route_2
 - 匹配条件** (Matching Conditions):
 - 类型**: 入接口 (In Interface)
 - 入接口**: GE0/0/4
 - 源地址**: 10.3.1.0/24
 - 目的地址**: 请选择或输入地址
 - 用户**: 请选择或输入用户
 - 服务**: 请选择或输入服务
 - 应用**: 请选择或输入应用
 - 时间段**: 请选择时间段
 - DSCP优先级**: any
 - 动作**: 转发 (Forwarding)
 - 出接口类型**: 单出口 (Single Exit)
 - 单出口配置** (Single Exit Configuration):
 - 出接口**: GE0/0/1
 - 下一跳**: 1.1.1.254
 - 监控**: 监控 (Monitoring) checkbox

Annotations in blue boxes:

- 学生网络中的PC通过接口 GigabitEthernet 0/0/2经由教育网访问Internet**
- 教师网络中的PC通过接口 GigabitEthernet 0/0/1直接访问Internet**

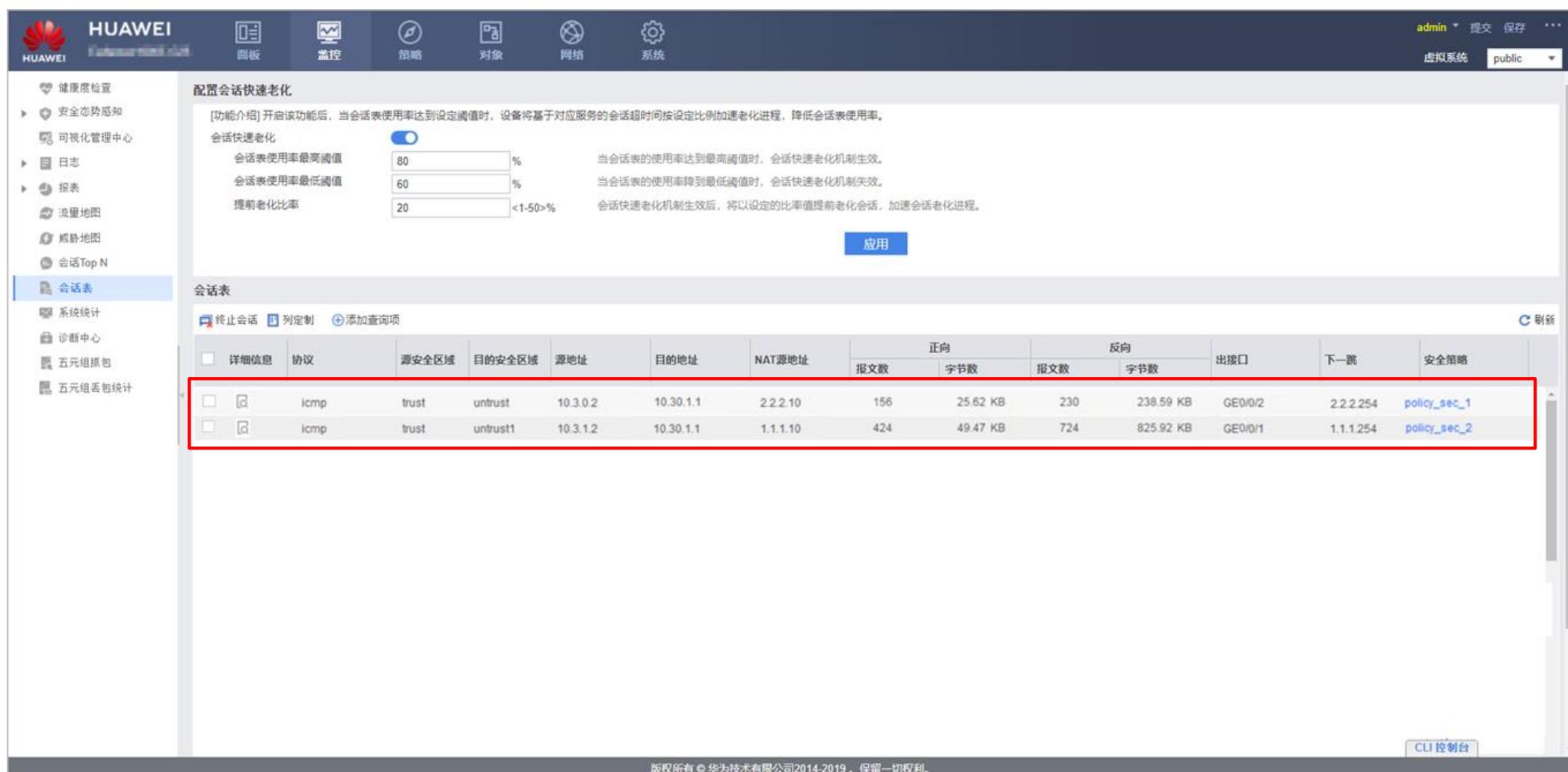
Example 3：通过多个运营商（ISP）接入互联网

Step7 结果验证

学生网络中的PC通过接口GigabitEthernet 0/0/2经由教育网访问Internet。

教师网络中的PC通过接口GigabitEthernet 0/0/1通过运营商网络直接访问Internet。

某学生PC 10.3.0.2和某教师PC 10.3.1.2分别访问外网某主机10.30.1.1的会话表信息



The screenshot shows the HUAWEI Network Management System interface. On the left, there is a navigation bar with various icons and links such as '健康度检查', '安全态势感知', '可视化管理中心', '日志', '报表', '流量地图', '威胁地图', '会话Top N', and '会话表'. The '会话表' link is highlighted with a blue background.

In the main area, there are two sections: '配置会话快速老化' (Configure Session Fast Aging) and '会话表' (Session Table).

配置会话快速老化 section:

- [功能介绍] 开启该功能后, 当会话表使用率达到设定阈值时, 设备将基于对应服务的会话超时时间按设定比例加速老化进程, 降低会话表使用率。
- 会话快速老化开关:
- 会话表使用率最高阈值: 80 %
- 会话表使用率最低阈值: 60 %
- 提前老化比率: 20 <1-50>%
- 描述: 当会话表的使用率达到最高阈值时, 会话快速老化机制生效。当会话表的使用率降到最低阈值时, 会话快速老化机制失效。会话快速老化机制生效后, 将以设定的比率值提前老化会话, 加速会话老化进程。

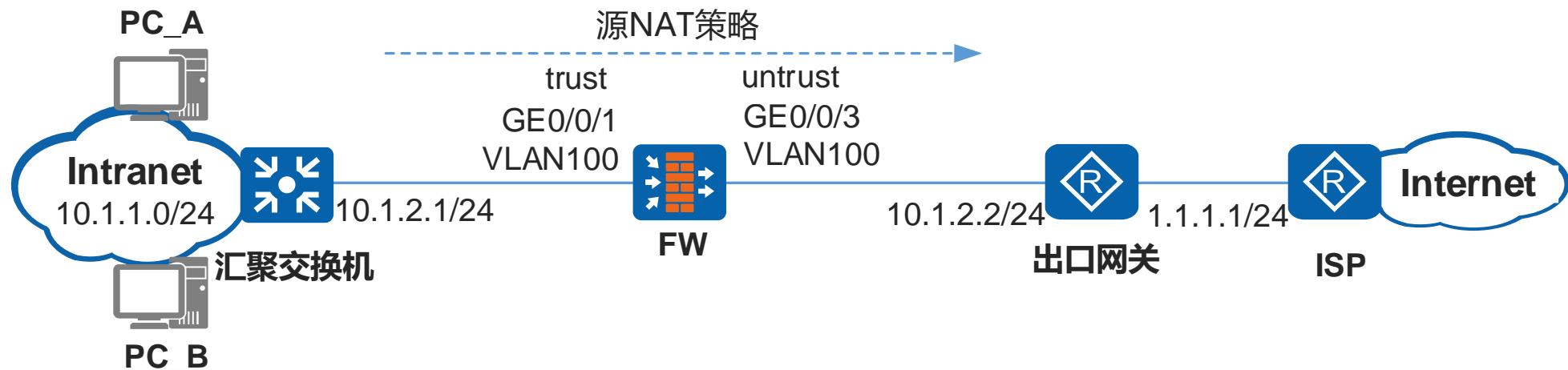
会话表 section:

详细信息	协议	源安全区域	目的安全区域	源地址	目的地址	NAT源地址	正向		反向		出接口	下一跳	安全策略	
							报文数	字节数	报文数	字节数				
<input type="checkbox"/>	<input checked="" type="checkbox"/>	icmp	trust	untrust	10.3.0.2	10.30.1.1	2.2.2.10	156	25.62 KB	230	238.59 KB	GE0/0/2	2.2.2.254	policy_sec_1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	icmp	trust	untrust1	10.3.1.2	10.30.1.1	1.1.1.10	424	49.47 KB	724	825.92 KB	GE0/0/1	1.1.1.254	policy_sec_2

At the bottom of the page, there is a footer note: 版权所有 © 华为技术有限公司2014-2019。保留一切权利。

Example 4：私网用户通过NAPT访问Internet

组网图



FW以透明方式部署在网络边界处，上下行业务接口均工作在二层模式。

本例将在FW上配置源NAT策略，使私网中10.1.1.0/24网段的用户可以正常访问Internet。

项目	数据	说明
允许访问Internet的私网网段	10.1.1.0/24	-
转换后的公网地址	1.1.1.10 ~ 1.1.1.15	由于私网地址比公网地址多，无法做到地址一一映射，所以需要开启允许端口转换，通过端口转换实现公网地址复用。
汇聚交换机的黑洞路由	目的地址: 1.1.1.10 ~ 1.1.1.15 下一跳: NULL 0	为了避免Internet用户主动访问转换后的公网地址时，在汇聚交换机和出口网关路由器之间形成路由环路。
出口网关路由器静态路由	目的地址: 1.1.1.10 ~ 1.1.1.15 下一跳: 10.1.2.1	请配置目的地址为32位的静态路由。
ISP路由器静态路由	目的地址: 1.1.1.10 ~ 1.1.1.15 下一跳: 1.1.1.1	由于转换后的公网地址不存在实际接口，通过路由协议无法直接发现，所以需要在ISP路由器上配置到公网地址的静态路由。

Example 4: 私网用户通过NAPT访问Internet

Step1 配置FW的接口

1 点击“网络”图标进入网络配置界面。

2 在左侧菜单栏中点击“接口”图标，进入接口列表页。

3 在右侧“启用”列中，将GE0/0/1和GE0/0/3两个端口的启用来电（上行）方向设为“是”，并点击编辑图标进行配置。

4 在“修改GigabitEthernet”对话框中，配置内网接口参数。将GE0/0/1端口的模式设为“交换”，连接类型设为“Access”，Access VLAN ID设为100。入方向带宽设为60-1000000 kbps，出方向带宽设为60-1000000 kbps。勾选“高级”选项。

5 在“修改GigabitEthernet”对话框中，配置外网接口参数。将GE0/0/3端口的模式设为“交换”，连接类型设为“Access”，Access VLAN ID设为100。入方向带宽设为60-1000000 kbps，出方向带宽设为60-1000000 kbps。勾选“高级”选项。

6 点击“确定”按钮完成配置。

Example 4：私网用户通过NAPT访问Internet

Step2 配置FW的安全策略

1 新建安全策略

2 安全策略

3 状态：已开启策略备份加速功能，加速成功。[配置] 当前状态：已开启基础协议报文过滤。[配置]

4 允许私网用户访问 Internet网络

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。 [选择策略模板]

常规设置

- 名称：policy1
- 描述：
- 策略组：-- NONE --
- 标签：

源与目的

- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：10.1.1.0/24
- 目的地址/地区：
- VLAN ID：请输入VLAN ID <1-4094>

用户与服务

- 用户:any;接入方式:any;终端设备:any;服务:any;应用:any;URL分类:any;时间段:any;

动作设置

- 动作：允许

内容安全

- 反病毒:NONE;入侵防御:NONE;URL过滤:NONE;文件过滤:NONE;内容过滤:NONE;应用行为控制:NONE;云接入安全感知:NONE;邮件过滤:NONE;APT防御:NONE;DNS过滤:NONE;

其他选项

- 记录流量日志:NONE;记录策略命中日志:禁用;记录会话日志:禁用;会话老化时间:NONE;自定义长连接:禁用;

确定 确定并复制 命令预览 取消

Example 4: 私网用户通过NAPT访问Internet

Step3 配置FW的NAT地址池

The screenshot shows the HUAWEI Firewall configuration interface. The top navigation bar includes icons for Home, Panel, Monitoring, Policies (highlighted with a red box and circled 1), Objects, Networks, and System. The top right corner shows the user is logged in as 'admin' with options to submit, save, and exit. A dropdown menu for 'Virtual System' is open, showing 'public'.

The left sidebar menu is expanded under 'NAT策略' (NAT Policies), with 'NAT策略' also highlighted with a red box and circled 2. Under this, '源转换地址池' (Source NAT Address Pool) is selected. A red arrow points from circled 2 down to the '新建' (Create) button in the main content area, which is circled 3.

The main content area displays the '新建源转换地址池' (Create Source NAT Address Pool) dialog box. It contains the following fields:

- 地址池名称:** addressgroup1 (highlighted with a red box)
- IP地址范围:** 1.1.1.10-1.1.1.15
- 健康状态检查:** (dropdown menu set to '请选择健康检查' (Please select health check))
- 配置黑洞路由:** (switch is off)
- 允许端口地址转换:** (switch is on)
- 高级:** (checkbox is checked)

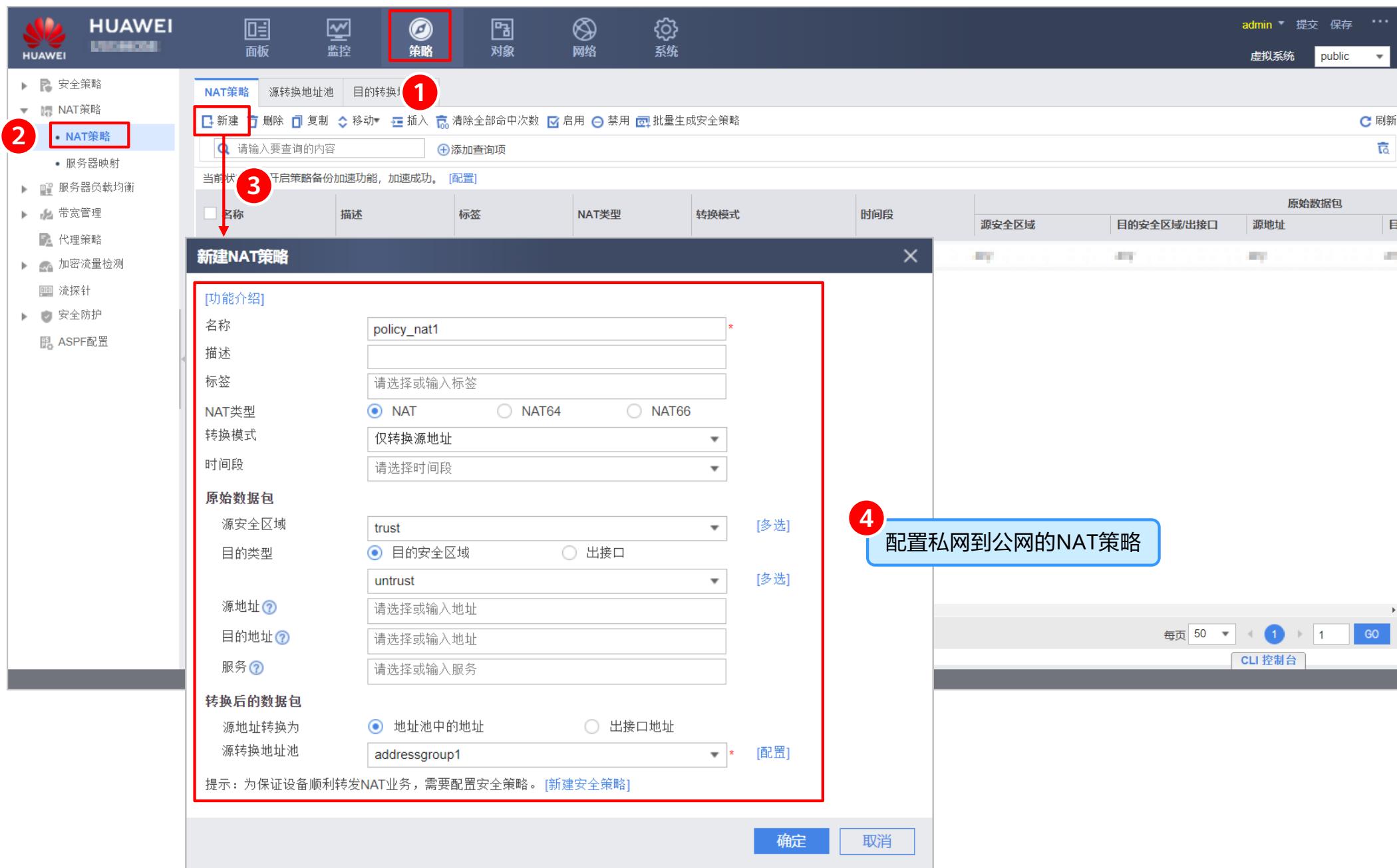
A note below the IP range says: '每行可输入一个地址范围或单个IP, 行之间用回车分隔。' (You can input one address range or a single IP per line, separated by carriage return.) Below that are two example entries: 192.168.10.10-192.168.10.20 and 192.168.10.30.

On the right side of the dialog box, a blue callout box with the number 4 contains the text: '配置NAT地址池, 为私网用户提供公网地址' (Configure NAT address pool to provide public network addresses to private network users).

At the bottom right of the dialog box are '确定' (Confirm) and '取消' (Cancel) buttons. The bottom right corner of the interface shows page navigation (Page 50, Go), a CLI control panel, and other system status indicators.

Example 4: 私网用户通过NAPT访问Internet

Step4 配置FW的NAT策略



The screenshot shows the HUAWEI Firewall Management System interface. The top navigation bar includes icons for Home, Panel, Monitoring, Policies (highlighted with a red box and labeled 1), Objects, Networks, and System. On the right, there are user information (admin), and save/submit buttons. The left sidebar menu is expanded under NAT Strategies, with 'NAT Strategies' highlighted (labeled 2). A sub-menu 'NAT Strategies' is also shown. The main content area displays the 'NAT Strategies' configuration page. A search bar and a message about backup acceleration are present. The table columns include: Name, Description, Tag, NAT Type, Transformation Mode, Time Period, Source Security Zone, Destination Security Zone/Interface, and Original Data包 (labeled 目标数据包). A new policy 'policy_nat1' is being created, as indicated by the '新建' button and the '新建NAT策略' dialog box. The dialog box contains fields for Name (policy_nat1), Description, Tag, NAT Type (selected NAT), Transformation Mode (Selected Only transform source address), Time Period, Original Data包 (Source Security Zone: trust, Destination Type: Selected Destination security zone, Source Address, Destination Address, Service), and Transformation后的数据包 (Selected Address pool, Source NAT address pool: addressgroup1). A note at the bottom says: '提示：为保证设备顺利转发NAT业务，需要配置安全策略。[新建安全策略]' (Note: To ensure smooth NAT forwarding, a security policy needs to be configured. [Create security policy]). Buttons at the bottom are '确定' (Confirm) and '取消' (Cancel). A callout box labeled 4 points to the 'Original Data包' section of the dialog box.

1 策略

2 NAT策略

3 新建

4 配置私网到公网的NAT策略

Example 4: 私网用户通过NAPT访问Internet

Step5 结果验证

1

私网用户可以正常访问Internet。

2

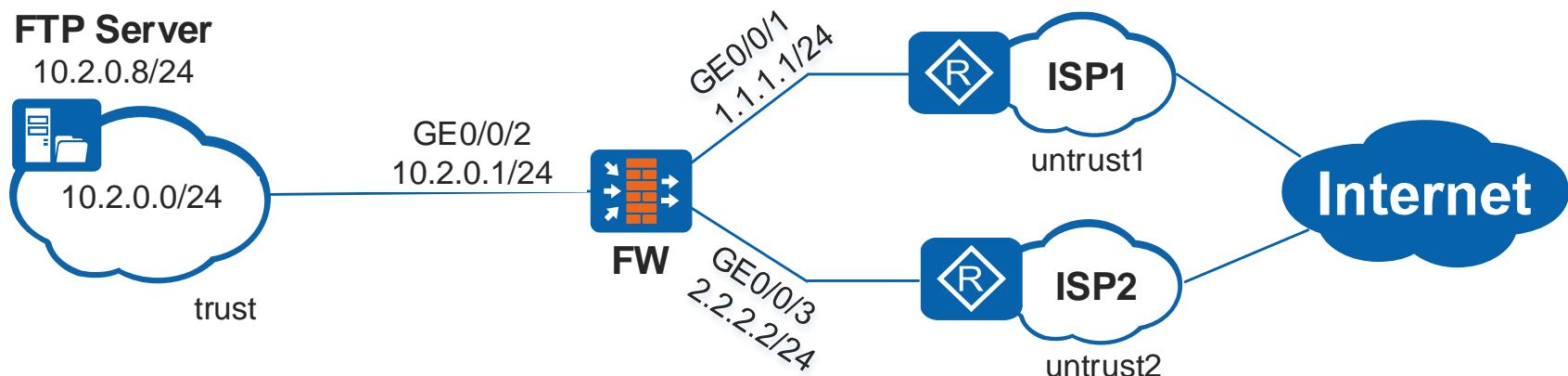
查看源NAT策略列表信息时，可以观察到源NAT策略的命中情况。

The screenshot shows the HUAWEI USG6300 firewall management interface. The left sidebar navigation includes '安全策略' (Security Policies), 'NAT策略' (NAT Policies) which is selected and highlighted in blue, and other options like '服务器负载均衡' (Server Load Balancing), '带宽管理' (Bandwidth Management), '代理策略' (Proxy Policies), '加密流量检测' (Encrypted Traffic Detection), '流探针' (Flow Probe), '安全防护' (Security Protection), and 'ASPF配置' (ASPF Configuration). The main content area displays the 'NAT策略' (NAT Policies) list. The top navigation bar for this section includes tabs for 'NAT策略' (selected), '源转换地址池' (Source Translation Address Pool), and '目的转换地址池' (Destination Translation Address Pool). Below the tabs are buttons for '新建' (New), '删除' (Delete), '复制' (Copy), '移动' (Move), '插入' (Insert), '清除全部命中次数' (Clear all hits), '启用' (Enable), '禁用' (Disable), and '批量生成安全策略' (Batch generate security policies). A search bar with placeholder '请输入要查询的内容' (Enter search content) and a '添加查询项' (Add search item) button are also present. The table below lists the NAT policies. The first row, 'policy_nat1', is highlighted with a red box and shows the following details: Name: policy_nat1, NAT Type: NAT, Transformation Mode: Only transform source address, Source Security Zone: trust, Destination Security Zone: untrust, Source IP: any, Destination IP: any, Service: any, and Address Pool: add... (with a delete icon). The 'Hits' column shows 9. The second row, 'default', shows the transformation mode as 'No transformation', and its 'Hits' column shows 99. The columns include: 名称 (Name), 描述 (Description), 标签 (Label), NAT类型 (NAT Type), 转换模式 (Transformation Mode), 时间段 (Time Range), 原始数据包 (Raw Data), 转换后的数据包 (Transformed Data), 命中次数 (Hits), 启用 (Enable), and 编辑 (Edit).

名称	描述	标签	NAT类型	转换模式	时间段	原始数据包				转换后的数据包		命中次数	启用	编辑
						源安全区域	目的安全区域/出接口	源地址	目的地址	服务	源地址转换			
policy_nat1	NAT		仅转换源地址	any	trust	untrust	any	any	any	地址池: add...	9	清除	<input checked="" type="checkbox"/>	<input type="checkbox"/>
default	This ...		不做转换	any	any	any	any	any	any		99	清除	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Example 5：公网用户通过NAPT访问内部服务器

组网图



FW作为安全网关部署在网络边界处，并通过两个不同的ISP接入Internet。

本例将在FW上配置NAT Server功能，为内部服务器对不同ISP的公网用户提供不同的服务地址。

项目	数据	说明
NAT Server1	公网地址: 1.1.1.10 私网地址: 10.2.0.8 公网点端口: 21 私网点端口: 21 安全区域: untrust1	通过该映射，使用外网用户访问1.1.1.10的流量能够发 送给内网的FTP服务器
NAT Server2	公网地址: 2.2.2.20 私网地址: 10.2.0.8 公网点端口: 21 私网点端口: 21 安全区域: untrust2	通过该映射，使用外网用户访问2.2.2.20的流量能够发 送给内网的FTP服务器
ISP1路由器静态路由	目的地址: 1.1.1.10 下一跳: 1.1.1.1	-
ISP2路由器静态路由	目的地址: 2.2.2.20 下一跳: 2.2.2.2	-

Example 5：公网用户通过NAPT访问内部服务器

Step1 新建FW的安全区域

The screenshot shows the HUAWEI USG6300 firewall configuration interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and tabs for '面板' (Dashboard), '监控' (Monitoring), '策略' (Policy), '对象' (Object), '网络' (Network), and '系统' (System). The 'Network' tab is highlighted with a red box and circled with a red number 1.

The left sidebar menu lists various network components: '接口' (Interface), '接口对' (Interface Pair), '安全区域' (Security Zone) (highlighted with a red box and circled with a red number 2), 'DNS', 'DHCP服务器', '路由', 'IPSec', 'L2TP', 'L2TP over IPSec', 'GRE', 'DSVPN', and 'SSL VPN'. A red arrow points from the '安全区域' menu item down to the '新建安全区域' (Create New Security Zone) dialog boxes.

The main area displays a '安全区域列表' (Security Zone List) table with columns: '名称' (Name), '优先级' (Priority), '描述' (Description), '接口数' (Interface Count), and '编辑' (Edit). A red box highlights the '新建' (Create) button, and a red circle with number 3 points to the first row in the list.

Two '新建安全区域' (Create New Security Zone) dialog boxes are open:

- 左侧对话框 (untrust1):** '名称' (Name) is set to 'untrust1' (highlighted with a red box), '优先级' (Priority) is set to '11' (highlighted with a red box), and the '接口' (Interface) section shows a '可选' (Selectable) list of interfaces.
- 右侧对话框 (untrust2):** '名称' (Name) is set to 'untrust2' (highlighted with a red box), '优先级' (Priority) is set to '15' (highlighted with a red box), and the '接口' (Interface) section shows a '可选' (Selectable) list of interfaces.

A blue box with a red number 4 contains the text: '新建安全区域untrust1和untrust2' (Create security zones untrust1 and untrust2).

At the bottom right of the dialog boxes are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 5：公网用户通过NAPT访问内部服务器

Step2 配置 FW的接口（1）

1. 在左侧菜单栏中，选择“网络”图标。

2. 在“接口”选项卡下，选择“接口列表”。

3. 在右侧列表中，选择要配置的接口（如GE0/0/1），并点击编辑图标（笔形图标）。

4. 在“修改GigabitEthernet”对话框中，配置连接ISP1的接口参数。设置接口名称为“GigabitEthernet0/0/1”，虚拟系统为“public”，安全区域为“untrust1”，模式为“路由”，连接类型为“静态IP”，IP地址为“1.1.1.1/255.255.255.0”，默认网关为“1.1.1.254”，并勾选“多出口选项”。
注：一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

5. 在右侧列表中，选择另一个接口（如GE0/0/3），并点击编辑图标（笔形图标）。

6. 在“修改GigabitEthernet”对话框中，配置连接ISP2的接口参数。设置接口名称为“GigabitEthernet0/0/3”，虚拟系统为“public”，安全区域为“untrust2”，模式为“路由”，连接类型为“静态IP”，IP地址为“2.2.2.2/255.255.255.0”，默认网关为“2.2.2.254”，并勾选“多出口选项”。
注：一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

完成配置后，点击“确定”按钮。

Example 5：公网用户通过NAPT访问内部服务器

Step2 配置 FW的接口（2）

1. 在“网络”模块下，进入“接口”列表。

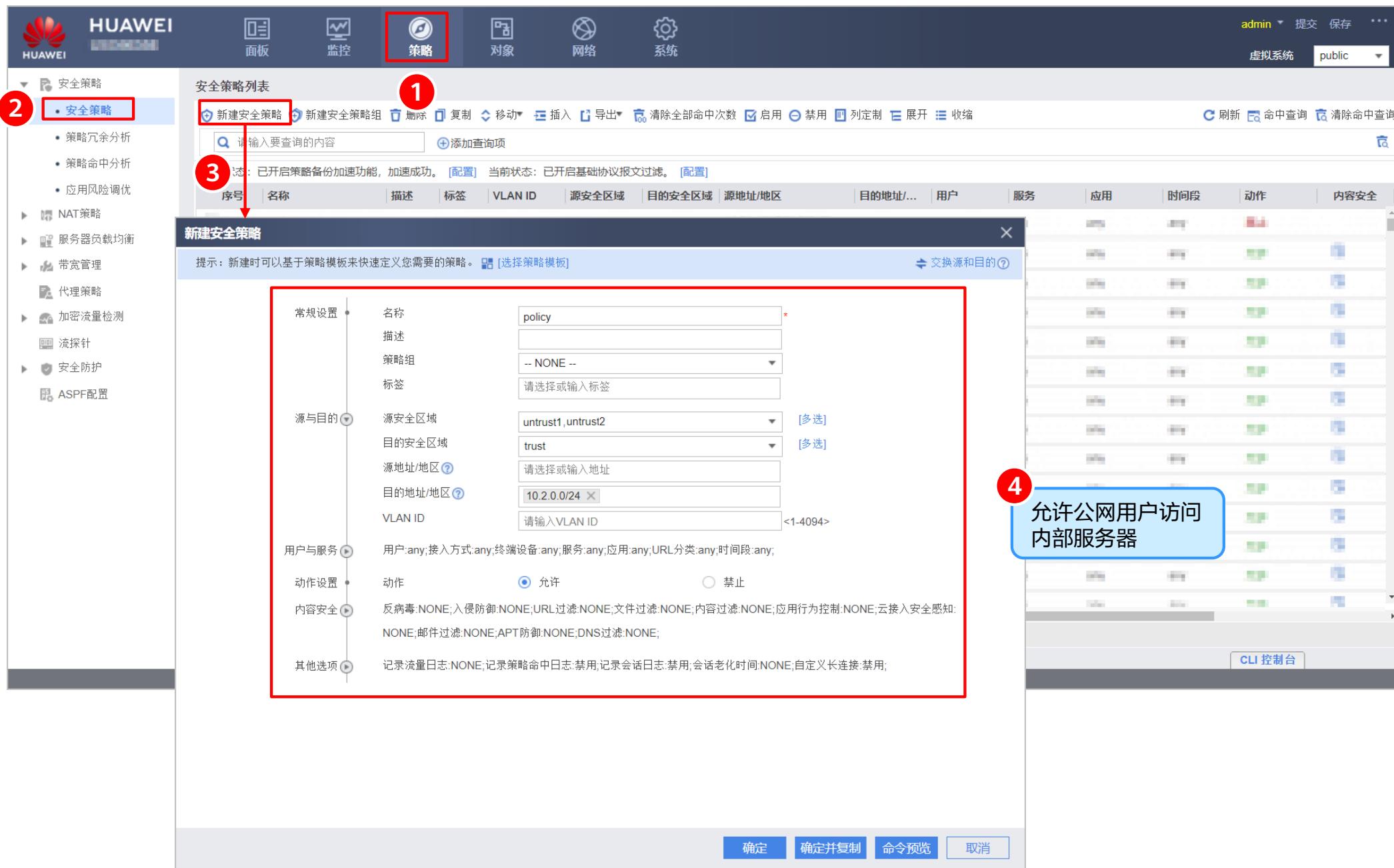
2. 选择“接口”选项卡。

3. 选中要配置的接口（例如 GE0/0/2），并点击右侧的编辑图标。

4. 弹出“修改GigabitEthernet”对话框，显示了接口参数配置界面。在IPv4 tab下，配置IP地址为10.2.0.1/255.255.255.0，并输入说明文字：“一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

Example 5：公网用户通过NAPT访问内部服务器

Step3 配置 FW 的安全策略



The screenshot shows the HUAWEI Firewall configuration interface. The top navigation bar includes the HUAWEI logo, user 'admin', and tabs for 面板 (Dashboard), 监控 (Monitoring), 对象 (Objects), 网络 (Network), 策略 (Policy), and 系统 (System). The '策略' tab is highlighted with a red box and a circled '1'. The left sidebar has a tree view with '安全策略' expanded, showing '安全策略' (selected) and other options like '策略冗余分析', '策略命中分析', '应用风险调优', 'NAT策略', '服务器负载均衡', '带宽管理', '代理策略', '加密流量检测', '流探针', '安全防护', and 'ASPF配置'. A circled '2' highlights the '安全策略' item in the sidebar.

The main area is titled '安全策略列表' (Security Policy List). It shows a table with columns: 序号 (Index), 名称 (Name), 描述 (Description), 标签 (Label), VLAN ID, 源安全区域 (Source Security Zone), 目的区域 (Destination Zone), 目的地址/地区 (Destination Address/Region), 用户 (User), 服务 (Service), 应用 (Application), 时间段 (Time Period), 动作 (Action), and 内容安全 (Content Security). A message at the top states: '已开启策略备份加速功能, 加速成功。[配置] 当前状态: 已开启基础协议报文过滤。[配置]'.

A modal window titled '新建安全策略' (Create New Security Policy) is open. It contains fields for '常规设置' (General Settings), '源与目的' (Source and Destination), '用户与服务' (User and Service), '动作设置' (Action Settings), and '内容安全' (Content Security). The '名称' field is set to 'policy'. The '源安全区域' dropdown shows 'untrust1, untrust2' (多选). The '目的区域' dropdown shows 'trust' (多选). The 'VLAN ID' field is set to '10.2.0.0/24'. Under '动作设置', the '允许' (Allow) radio button is selected. A note below says: '反病毒:NONE;入侵防御:NONE;URL过滤:NONE;文件过滤:NONE;内容过滤:NONE;应用行为控制:NONE;云接入安全感知:NONE;邮件过滤:NONE;APT防御:NONE;DNS过滤:NONE;'. The bottom of the modal has buttons for '确定' (Confirm), '确定并复制' (Confirm and Copy), '命令预览' (Command Preview), and '取消' (Cancel).

A blue callout box with a circled '4' and the text '允许公网用户访问 内部服务器' (Allow public network users to access internal servers) points to the 'allow' action setting in the modal.

Example 5：公网用户通过NAPT访问内部服务器

Step4 配置 FW的NAT Server

1 在策略界面，点击“新建”按钮。

2 在左侧菜单栏中，选择“NAT策略”下的“服务器映射”。

3 在“新建服务器映射”对话框中，配置以下参数：

名称	policy_ftp1
安全区域	untrust1
公网地址	1.1.1.10
私网地址	10.2.0.8
指定协议	<input checked="" type="checkbox"/>
协议	TCP
公网端口	21
私网端口	21
允许服务器使用公网地址上网	<input type="checkbox"/>
配置黑洞路由	<input checked="" type="checkbox"/>

4 在“新建服务器映射”对话框中，配置以下参数（与上一步相同）：

名称	policy_ftp2
安全区域	untrust2
公网地址	2.2.2.10
私网地址	10.2.0.8
指定协议	<input checked="" type="checkbox"/>
协议	TCP
公网端口	21
私网端口	21
允许服务器使用公网地址上网	<input type="checkbox"/>
配置黑洞路由	<input checked="" type="checkbox"/>

提示：为保证设备顺利转发NAT业务，需要配置安全策略。 [[新建安全策略](#)]

配置服务器映射policy_ftp1和policy_ftp2

确定 **取消**

Example 5：公网用户通过NAPT访问内部服务器

Step5 配置 FTP的NAT ALG功能

The screenshot shows the HUAWEI Web UI interface for network configuration. The top navigation bar includes the HUAWEI logo, user status (admin), and system buttons (提交, 保存, ...). The main menu on the left lists various configuration options like 安全策略, NAT策略, 服务器负载均衡, 带宽管理, 代理策略, 加密流量检测, 流探针, and 安全防护. The 'ASPF配置' link under the '策略' tab is highlighted with a red box and labeled '2'. The central configuration area is titled 'ASPF配置' and contains a note: '当需要传输多通道协议时, 请配置对应协议的ASPF功能。ASPF功能可以保证系统对多通道协议中临时协商的端口正常进行报文过滤和NAT。'. It lists several protocols with checkboxes: DNS, ILS, NetBIOS, RTSP, MGCP, PPTP, SCCP, H.323, MMS, QQ, SIP, ICQ, MSN, RSH, and SQL*NET. The 'FTP' checkbox is checked and highlighted with a red box and labeled '3'. A large blue '应用' (Apply) button is at the bottom of the configuration section and is also highlighted with a red box and labeled '4'.

Example 5：公网用户通过NAPT访问内部服务器

Step6 结果验证

1

公网用户可以通过不同ISP访问内部服务器。

2

单击“诊断”，查看服务器映射的当前状态。如当前状态显示为“已连通”表示内网服务器可达。

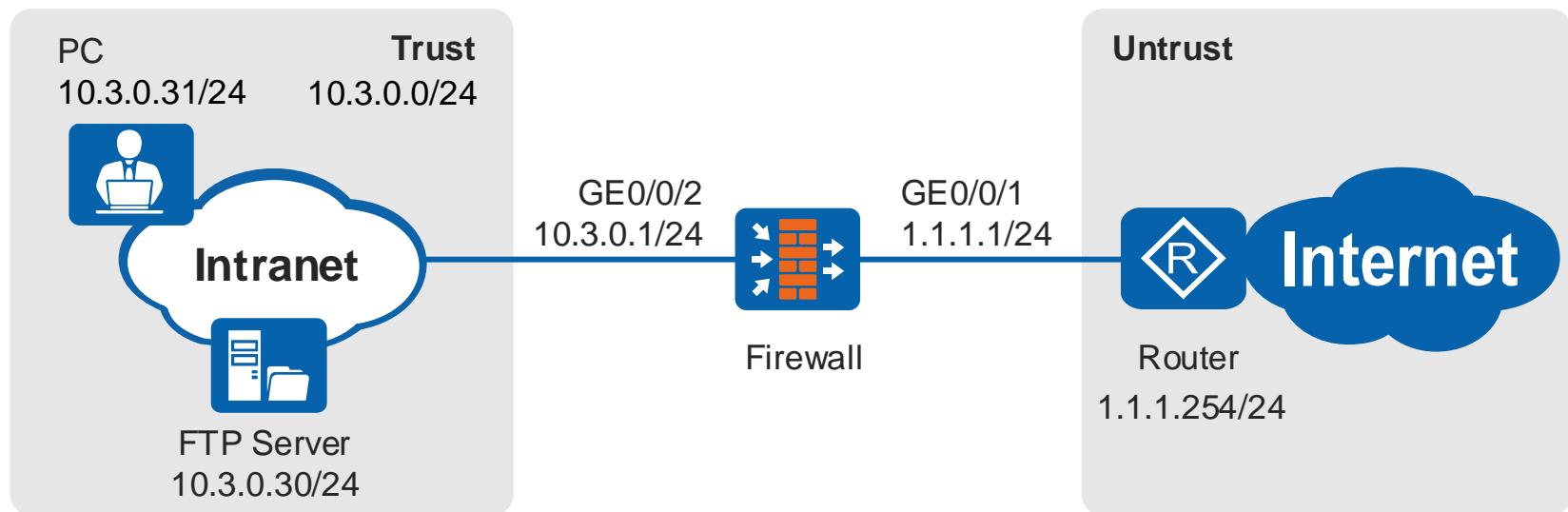
The screenshot shows the HUAWEI USG Firewall management interface. The left sidebar navigation includes '安全策略' (Security Policy), 'NAT策略' (NAT Policy), and '服务器映射' (Server Mapping), which is currently selected and highlighted with a blue background. The main content area displays the '服务器映射列表' (Server Mapping List) with the following data:

名称	公网地址	私网地址	协议	公网点口	私网点口	当前状态	启用	编辑
policy_ftp2	2.2.2.10	10.2.0.8	TCP	21	21	已连通: [诊断]	<input checked="" type="checkbox"/>	<input type="checkbox"/>
policy_ftp1	1.1.1.10	10.2.0.8	TCP	21	21	已连通: [诊断]	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The 'Current Status' column for both rows is highlighted with a red box, indicating that the internal servers are reachable via NAPT.

Example 6：内外网用户同时通过公网IP访问FTP服务器

组网图



企业内网用户和FTP服务器均在同一网段10.3.0.0/24，且均放在Trust安全区域。

企业采用上行接入Internet（固定IP方式），IP地址向ISP申请获得。

内网用户和外网用户均通过公网地址1.1.1.2和端口2121访问FTP服务器，内网用户通过公网地址1.1.1.1访问Internet。

项目	数据	说明
GigabitEthernet 0/0/2	安全区域: Trust IP地址: 10.3.0.1/24	FTP服务器需要将默认网关配置为10.3.0.1。
GigabitEthernet 0/0/1	安全区域: Untrust IP地址: 1.1.1.1/24	实际配置时需要按照ISP的要求进行配置。
FTP服务器	对外公布的公网地址: 1.1.1.2 公网点口: 2121	-
DNS服务器	1.2.2.2/24	向ISP获取。
网关地址	1.1.1.254/24	向ISP获取。

Example 6：内外网用户同时通过公网IP访问FTP服务器

Step1 配置接口

1 网络

2 接口

3 编辑

4 配置外网接口参数

5 编辑

6 配置内网接口参数

接口名称	安全区域	虚拟系统	IP地址	连接类型	VLAN	模式	状态	启用
GE0/0/0(GE0/MGMT)							物理	+
GE0/0/1		public	1.1.1.1/24	静态IP			IPv4	+
GE0/0/2		trust	10.3.0.1/24	静态IP			IPv4	+
GE0/0/3							IPv6	-
GE0/0/4							IPv6	-
GE0/0/5							IPv6	-
GE0/0/6							IPv6	-

Example 6：内外网用户同时通过公网IP访问FTP服务器

Step2 配置安全策略

1 策略

2 安全策略

3 新建安全策略

4 允许内网IP地址访问外网

5 允许外网用户访问内网FTP服务器

The screenshot shows the Huawei Network Management System interface. The top navigation bar includes 'HUAWEI' logo, '面板' (Dashboard), '监控' (Monitoring), '策略' (Policy), '对象' (Object), '网络' (Network), and '系统' (System). The '策略' button is highlighted with a red box and a circled '1'. The left sidebar has a tree view with '安全策略' expanded, showing '安全策略' (selected) and other options like '策略冗余分析', '策略命中分析', '应用风险调优', 'NAT策略', '服务器负载均衡', and '带宽管理'. A red box highlights '安全策略' with a circled '2'. Below it, a red box highlights the '新建安全策略' button with a circled '3'. The main area is titled '安全策略列表' (Security Policy List) with a sub-section '新建安全策略' (Create New Security Policy). It displays a table with columns: 序号 (Index), 名称 (Name), 描述 (Description), VLAN ID, 源安全区域 (Source Security Zone), 目的区域 (Destination Zone), 目的地址/地区 (Destination Address/Region), 用户 (User), 服务 (Service), 应用 (Application), 时间段 (Time Period), 动作 (Action), and 内容安全 (Content Security). A search bar at the top says '请输入要查询的内容' (Enter search content) and '添加查询项' (Add search item). A note at the bottom says '当前状态: 已开启策略备份加速功能, 加速成功。[配置] 当前状态: 已开启基础协议报文过滤。[配置]' (Current status: Policy backup acceleration function is enabled, accelerated successfully. [Configure]. Current status: Basic protocol message filtering is enabled. [Configure]). The '新建安全策略' dialog box on the right contains fields for '常规设置' (General Settings) and '源与目的' (Source and Destination). The '常规设置' section includes '名称' (Name: trust2untrust), '描述' (Description), '策略组' (Policy Group: -- NONE --), and '标签' (Label). The '源与目的' section includes '源安全区域' (Source Security Zone: trust), '目的安全区域' (Destination Zone: untrust), '源地址/地区' (Source Address/Region: 10.3.0.0/24), '目的地址/地区' (Destination Address/Region: 10.3.0.30/32), and 'VLAN ID' (VLAN ID: <1-4094>). The '动作设置' (Action Settings) section has '允许' (Allow) selected. The '内容安全' (Content Security) section lists various security rules. The '确定' (Confirm) button is at the bottom.

Example 6: 内外网用户同时通过公网IP访问FTP服务器

Step3 新建NAT地址池

The screenshot shows the HUAWEI USG6300 firewall's configuration interface. The top navigation bar includes icons for Home, Panel, Monitoring, Policies (highlighted with a red box), Objects, Networks, and System. The top right corner shows the user is logged in as 'admin' with tabs for '提交' (Submit), '保存' (Save), and more. The left sidebar menu is collapsed, but the 'NAT策略' (NAT Policies) section is selected and highlighted with a red box. The main content area shows the '源转换地址池' (Source NAT Address Pool) tab selected under the 'NAT策略' tab. A red circle labeled '1' is on the '新建' (Create) button. A red circle labeled '2' is on the 'NAT策略' link in the sidebar. A red circle labeled '3' points to the '地址池名称' (Address Pool Name) input field where 'addresspool1' is entered. A red box highlights the '地址池名称' and 'IP地址范围' (IP Address Range) sections. A blue callout box labeled '4' indicates that the public IP address 1.1.1.1 is being added to the address pool. The bottom right of the dialog shows '确定' (Confirm) and '取消' (Cancel) buttons.

新建源转换地址池

地址池名称: addresspool1

IP地址范围: 1.1.1.1

每行可输入一个地址范围或单个IP, 行之间用回车分隔。
192.168.10.10-192.168.10.20
192.168.10.30

健康状态检查: 请选择健康检查 [配置]

配置黑洞路由:

允许端口地址转换:

高级

4 新建公网地址为1.1.1.1的NAT地址池

Example 6：内外网用户同时通过公网IP访问FTP服务器

Step4 新建源NAT

The screenshot shows the HUAWEI USG6300 firewall's configuration interface. The top navigation bar includes 'HUAWEI', '面板' (Panel), '监控' (Monitoring), '策略' (Policy) (highlighted with a red box and circled with a red number 1), '对象' (Object), '网络' (Network), and '系统' (System). The top right corner shows 'admin', '提交' (Submit), '保存' (Save), and a dropdown for '虚拟系统' (Virtual System) set to 'public'.

The left sidebar menu has sections like '安全策略' (Security Policy), 'NAT策略' (NAT Policy) (highlighted with a red box and circled with a red number 2), '服务器映射' (Server Mapping), '服务器负载均衡' (Server Load Balancing), and '带宽管理' (Bandwidth Management). Under 'NAT策略', there is a 'NAT策略' section with a '新建' (Create) button (circled with a red number 3).

The main content area has two parallel configuration windows:

- New NAT Policy 1 (Left Window):** A blue callout box contains the text: "新建源NAT，实现内网用户使用公网地址访问Internet。" (Create a source NAT policy to allow internal network users to access the Internet using public network addresses). The configuration fields include:
 - 名称:** policy_nat1
 - NAT类型:** NAT (radio button selected)
 - 转换模式:** 仅转换源地址
 - 时间段:** 请选择时间段
 - 原始数据包:**
 - 源安全区域:** trust
 - 目的类型:** 目的安全区域 (radio button selected)
 - 源地址:** 10.3.0.0/24
 - 目的地址:** 请选择或输入地址
 - 服务:** 请选择或输入服务
 - 转换后的数据包:**
 - 源地址转换为:** 地址池中的地址 (radio button selected)
 - 源转换地址池:** addresspool1
 A note at the bottom says: "提示: 为保证设备顺利转发NAT业务, 需要配置安全策略。[新建安全策略]" (Tip: To ensure smooth NAT forwarding, security policies need to be configured. [Create security policy]).
- New NAT Policy 2 (Right Window):** A blue callout box contains the text: "新建源NAT，实现内网用户使用公网地址访问FTP 服务器。" (Create a source NAT policy to allow internal network users to access the FTP server using public network addresses). The configuration fields are identical to the first window but with different source and destination IP ranges:
 - 名称:** policy_nat2
 - NAT类型:** NAT (radio button selected)
 - 转换模式:** 仅转换源地址
 - 时间段:** any
 - 原始数据包:**
 - 源安全区域:** trust
 - 目的类型:** 目的安全区域 (radio button selected)
 - 源地址:** 10.3.0.0/24
 - 目的地址:** 10.3.0.30/32
 - 服务:** 请选择或输入服务
 - 转换后的数据包:**
 - 源地址转换为:** 地址池中的地址 (radio button selected)
 - 源转换地址池:** addresspool1
 A note at the bottom says: "提示: 为保证设备顺利转发NAT业务, 需要配置安全策略。[新建安全策略]" (Tip: To ensure smooth NAT forwarding, security policies need to be configured. [Create security policy]).

Both windows have a '确定' (Confirm) button at the bottom right and a '取消' (Cancel) button at the bottom left.

Example 6：内外网用户同时通过公网IP访问FTP服务器

Step5 配置服务器映射



The screenshot shows the HUAWEI USG6300 firewall's configuration interface. The top navigation bar includes the HUAWEI logo, user 'admin', and tabs for 面板 (Dashboard), 监控 (Monitoring), 策略 (Policy), 对象 (Object), 网络 (Network), and 系统 (System). The '策略' tab is highlighted with a red box and a circled '1'. The left sidebar menu under 'NAT策略' has '服务器映射' selected, indicated by a red box and circled '2'. A red arrow points from the '服务器映射' link to the '新建' button in the top toolbar of the main content area, which is circled '3'. The main content area displays a table titled '服务器映射列表' with columns: 名称 (Name), 公网地址 (Public Address), 私网地址 (Private Address), 协议 (Protocol), 公网端口 (Public Port), 私网端口 (Private Port), and 当前状态 (Current Status). The bottom right corner of the interface shows a CLI control panel with buttons for 50, 1, 1, GO, and CLI控制台 (CLI Control Console).

新建服务器映射

[功能介绍]

名称	policy_ftp1
安全区域	选择下拉菜单
公网地址	1.1.1.2
私网地址	10.3.0.30
指定协议	<input checked="" type="checkbox"/>
协议	TCP
公网端口	2121
私网端口	21
允许服务器使用公网地址上网	<input type="checkbox"/>
配置黑洞路由	<input checked="" type="checkbox"/>

提示：为保证设备顺利转发NAT业务，需要配置安全策略。 [新建安全策略]

4 配置FTP服务器的私网地址
映射为公网地址1.1.1.2

底部按钮：确定 取消

Example 6：内外网用户同时通过公网IP访问FTP服务器

Step6 配置NAT ALG功能

The screenshot shows the HUAWEI router's configuration interface. The top navigation bar includes icons for Home, Strategy (highlighted with a red circle 1), Object, Network, and System, along with user admin, and tabs for virtual systems public and system.

The left sidebar menu lists: 安全策略, NAT策略, 服务器负载均衡, 带宽管理, 代理策略, 加密流量检测, 流探针, 安全防护, and ASPF配置 (highlighted with a red circle 2). The main content area is titled "ASPF配置" and contains the following text: "当需要传输多通道协议时, 请配置对应协议的ASPF功能。ASPF功能可以保证系统对多通道协议中临时协商的端口正常进行报文过滤和NAT。". A list of protocols follows:

<input type="checkbox"/> DNS	<input checked="" type="checkbox"/> FTP	<input type="checkbox"/> H.323	<input type="checkbox"/> ICQ
<input type="checkbox"/> ILS	<input type="checkbox"/> MGCP	<input type="checkbox"/> MMS	<input type="checkbox"/> MSN
<input type="checkbox"/> NetBIOS	<input type="checkbox"/> PPTP	<input type="checkbox"/> QQ	<input type="checkbox"/> RSH
<input type="checkbox"/> RTSP	<input type="checkbox"/> SCCP	<input type="checkbox"/> SIP	<input type="checkbox"/> SQL*NET

A large blue button labeled "应用" (Apply) is highlighted with a red circle 4. A callout bubble on the right states: "缺省情况下, FTP协议已开启NAT ALG功能。" (By default, the FTP protocol has NAT ALG functionality enabled.)

At the bottom right is a "CLI 控制台" (CLI Console) button.

Example 6：内外网用户同时通过公网IP访问FTP服务器

Step7 结果验证

1. 内网PC能访问Internet。
2. 外网用户可以通过公网地址1.1.1.2和端口2121访问FTP服务器；内网用户可以通过公网地址1.1.1.2和端口2121访问FTP服务器。
3. 如果想查看命中NAT策略的命中情况，可以选择“策略 > NAT策略 > NAT策略”，在源NAT策略列表中查看NAT策略的命中次数。

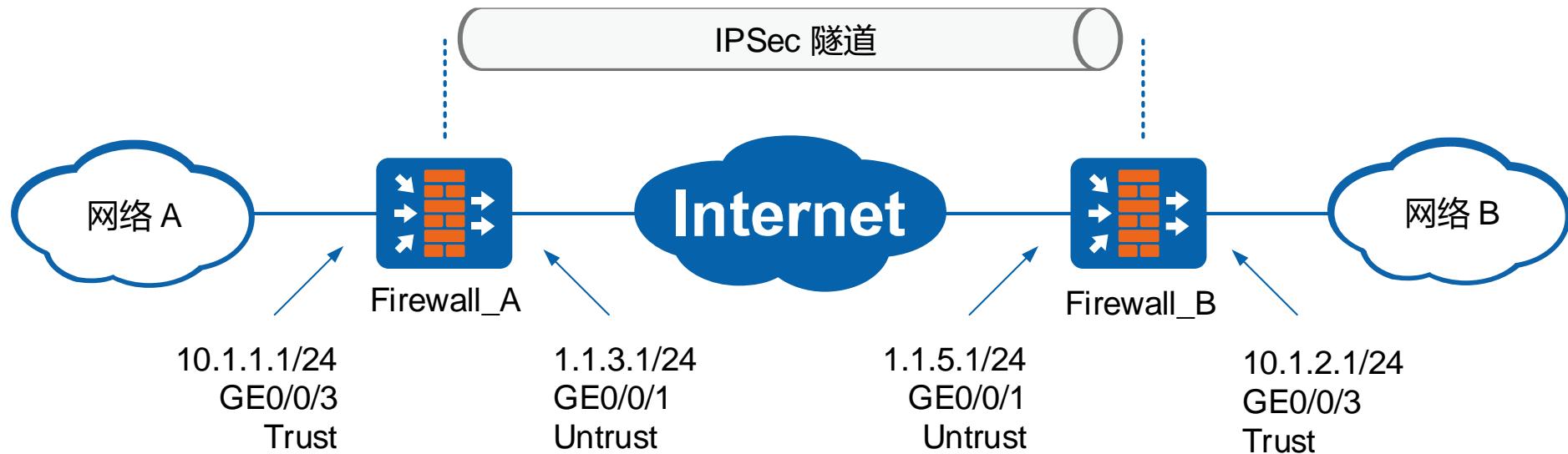
名称	描述	标签	NAT类型	转换模式	时间段	原始数据包	转换后的数据包	命中次数	启用	编辑
policy_nat1			NAT	仅转换源地址	any	trust	untrust	10.3.... any any 地址池: add... 3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
policy_nat2			NAT	仅转换源地址	any	trust	trust	10.3... 10.3.0.3... any 地址池: add... 10	<input checked="" type="checkbox"/>	<input type="checkbox"/>
default	This ...			不做转换	any any any	any any any	任何任何任何	3.1*10 ⁵ 清除	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4. 如果想查看服务器映射和源NAT过程中地址和端口的转换信息，可以选择“监控 > 会话表”，通过搜索找到目的地址为1.1.1.2的表项，查看详细的转换信息。其中，端口的转换信息，请单击对应表项的 查看。

详细信息	创建时间	会话超时剩余时间	协议	应用	源虚拟系统	目的虚拟系统	源安全区域	目的安全区域	源地址	目的地址	NAT源地址
	2019/9/16 16:30:52	00:20:00	ftp	FTP	public	public	trust	trust	10.3.0.31	1.1.1.2	1.1.1.1
	2019/9/16 16:30:17	00:19:33	ftp	FTP	public	public	untrust	trust	1.1.1.254	1.1.1.2	

Example 7: 点到点 IPSec 隧道

组网图



Firewall_A和Firewall_B分别是网络A和网络B的出口网关，采用固定IP地址接入Internet，Firewall_A和Firewall_B相互路由可达。
本例将在Firewall_A和Firewall_B之间建立IKE协商方式的点到点IPSec隧道，实现两个网络之间安全的互访。

项目	Firewall_A	Firewall_B
场景	点到点	点到点
对端地址	1.1.5.1	1.1.3.1
认证方式	预共享密钥	预共享密钥
预共享密钥	Admin@123	Admin@123
本端ID	IP地址	IP地址
对端ID	IP地址	IP地址

Example 7: 点到点 IPSec 隧道

Step1 配置 Firewall_A 的接口

1. 在 HUAWEI USG6000E 路由器管理界面中，进入“网络”->“接口”模块。

2. 在左侧树状菜单中，选择“接口”->“接口对”。

3. 在列表中选择外网接口 GE0/0/1，并点击“编辑”按钮。

4. 在“修改 GigabitEthernet”对话框中，配置外网接口参数。设置接口名称为“GigabitEthernet0/0/1”，虚拟系统为“public”，安全区域为“untrust”，模式为“路由”。在 IPv4 选项卡下，连接类型选择“静态IP”，IP 地址输入为“1.1.3.1/24”。完成配置后点击“确定”。

5. 在列表中选择内网接口 GE0/0/3，并点击“编辑”按钮。

6. 在“修改 GigabitEthernet”对话框中，配置内网接口参数。设置接口名称为“GigabitEthernet0/0/3”，虚拟系统为“public”，安全区域为“trust”，模式为“路由”。在 IPv4 选项卡下，连接类型选择“静态IP”，IP 地址输入为“10.1.1.1/24”。完成配置后点击“确定”。

Example 7: 点到点 IPSec 隧道

Step2 配置 Firewall_A 的安全策略

1 在 HUAWEI 设备管理界面中，进入“策略”模块。

2 选择“安全策略”。

3 点击“新建安全策略”按钮。

4 在“新建安全策略”对话框中，配置以下参数：

常规设置	名称: policy_ipsec_1
源与目的	源安全区域: trust 目的安全区域: untrust 源地址/地区: 10.1.0.0/24 目的地址/地区: 10.1.2.0/24 VLAN ID: 请输入 VLAN ID
动作设置	动作: 允许
内容安全	反病毒: NONE; 入侵防御: NONE; URL过滤: NONE; 文件过滤: NONE; 内容过滤: NONE; 应用行为控制: NONE; 云接入安全感知: NONE; 邮件过滤: NONE; APT防御: NONE; DNS过滤: NONE;
其他选项	记录流量日志: NONE; 记录策略命中日志: 禁用; 记录会话日志: 禁用; 会话老化时间: NONE; 自定义长连接: 禁用;

5 在“新建安全策略”对话框中，配置以下参数：

常规设置	名称: policy_ipsec_2
源与目的	源安全区域: untrust 目的安全区域: trust 源地址/地区: 10.1.2.0/24 目的地址/地区: 10.1.0.0/24 VLAN ID: 请输入 VLAN ID
动作设置	动作: 允许
内容安全	反病毒: NONE; 入侵防御: NONE; URL过滤: NONE; 文件过滤: NONE; 内容过滤: NONE; 应用行为控制: NONE; 云接入安全感知: NONE; 邮件过滤: NONE; APT防御: NONE; DNS过滤: NONE;
其他选项	记录流量日志: NONE; 记录策略命中日志: 禁用; 记录会话日志: 禁用; 会话老化时间: NONE; 自定义长连接: 禁用;

6 在“新建安全策略”对话框中，配置以下参数：

常规设置	名称: policy_ipsec_3
源与目的	源安全区域: local 目的安全区域: untrust 源地址/地区: 1.1.3.1/32 目的地址/地区: 1.1.5.1/32 VLAN ID: 请输入 VLAN ID
动作设置	动作: 允许
内容安全	反病毒: NONE; 入侵防御: NONE; URL过滤: NONE; 文件过滤: NONE; 内容过滤: NONE; 应用行为控制: NONE; 云接入安全感知: NONE; 邮件过滤: NONE; APT防御: NONE; DNS过滤: NONE;
其他选项	记录流量日志: NONE; 记录策略命中日志: 禁用; 记录会话日志: 禁用; 会话老化时间: NONE; 自定义长连接: 禁用;

7 在“新建安全策略”对话框中，配置以下参数：

常规设置	名称: policy_ipsec_4
源与目的	源安全区域: untrust 目的安全区域: local 源地址/地区: 1.1.5.1/32 目的地址/地区: 1.1.3.1/32 VLAN ID: 请输入 VLAN ID
动作设置	动作: 允许
内容安全	反病毒: NONE; 入侵防御: NONE; URL过滤: NONE; 文件过滤: NONE; 内容过滤: NONE; 应用行为控制: NONE; 云接入安全感知: NONE; 邮件过滤: NONE; APT防御: NONE; DNS过滤: NONE;
其他选项	记录流量日志: NONE; 记录策略命中日志: 禁用; 记录会话日志: 禁用; 会话老化时间: NONE; 自定义长连接: 禁用;

Example 7: 点到点 IPSec 隧道

Step3 配置 Firewall_A 的路由

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes the HUAWEI logo, user information (admin), and tabs for 面板 (Dashboard), 监控 (Monitoring), 对象 (Objects), 网络 (Network), and 系统 (System). The 网络 tab is highlighted with a red box and a circled number 1.

The left sidebar lists various network components: 接口, 接口对, 安全区域, DNS, DHCP服务器, 路由 (selected), 智能选路, 虚拟路由器, 静态路由 (selected), ISP路由, RIP, OSPF, BGP, 动态路由监控表, 路由表, IPsec, L2TP, L2TP over IPsec, GRE, DSVPN, and SSL VPN.

The main content area has two sections:

- 配置默认优先级**: Shows IPv4 and IPv6 default priorities set to 60. A red box highlights the IPv4 priority input field, circled with number 1.
- 静态路由列表**: Shows a table of existing static routes. A red box highlights the "新建" (New) button, circled with number 2.

A red arrow points from the "新建" button to a modal dialog titled "新建静态路由" (Create New Static Route).

新建静态路由 dialog fields (highlighted by a red box and circled with number 3):

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	10.1.2.0/255.255.255.0
目的虚拟路由器	public
出接口	-- NONE --
下一跳	1.1.3.2
优先级	60
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link
描述	

A callout bubble with a red border and circled number 4 contains the text: "配置到网络B中私网IP地址的路由，此处假设Firewall_A到Internet的下一跳IP地址为1.1.3.2。"

The bottom of the dialog has "确定" (Confirm) and "取消" (Cancel) buttons.

Example 7: 点到点 IPSec 隧道

Step4 配置 Firewall_A 的 IPSec

The screenshot shows the HUAWEI USG6300 network management interface with the following steps highlighted:

- 1** 在“网络”选项卡下的“IPSec策略列表”中，点击“新建”按钮。
- 2** 在左侧导航栏中，选择“IPSec”。
- 3** 在“新建IPSec策略”对话框中，选择“点到点”场景，并完成基本配置（策略名称：policy1，本地接口：GE0/0/1，本地地址：1.1.3.1，对端地址：1.1.5.1，认证方式：预共享密钥，本地ID：IP地址 1.1.3.1，对端ID：IP地址 1.1.5.1）。
- 4** 在右侧的“安全提议”配置窗口中，完成IKE参数和IPSec参数的配置。注意：本例中安全提议参数全部使用缺省值，如果您对参数有明确要求，请修改，并注意与Firewall_B上的配置保持一致。
- 5** 在“待加密的数据流”配置窗口中，点击“新建”按钮。
- 6** 在“新建待加密的数据流”对话框中，增加待加密的数据流（源地址/地址组：10.1.1.0/24，目的地址/地址组：10.1.2.0/24，协议：any，动作：加密）。
- 7** 在右侧的“安全提议”配置窗口中，完成IKE/IPSec安全提议的配置。

预共享密钥为Admin@123

增加待加密的数据流

Example 7: 点到点 IPSec 隧道

Step5 配置 Firewall_B 的接口

1. 在 HUAWEI USG防火墙管理界面中，进入“网络”->“接口”模块。

2. 在左侧树状菜单中，选择“接口”。

3. 在右侧列表中，选择外网接口（GE0/0/1）并点击编辑图标（笔形图标）。

4. 在“修改GigabitEthernet”对话框中，配置外网接口参数。包括：接口名称（GigabitEthernet0/0/1）、虚拟系统（public）、安全区域（untrust）、模式（路由）、连接类型（静态IP）、IP地址（1.1.5.1/24）等。

5. 在右侧列表中，选择内网接口（GE0/0/3）并点击编辑图标（笔形图标）。

6. 在“修改GigabitEthernet”对话框中，配置内网接口参数。包括：接口名称（GigabitEthernet0/0/3）、虚拟系统（public）、安全区域（trust）、模式（路由）、连接类型（静态IP）、IP地址（10.1.2.1/24）等。

Example 7: 点到点 IPSec 隧道

Step6 配置 Firewall_B 的安全策略

1 新建安全策略

2 安全策略

3 搜索框

4 允许网络B中的私网IP地址访问网络A中的私网IP地址

5 允许网络A中的私网IP地址访问网络B中的私网IP地址

6 允许Firewall_B自身访问Firewall_A的公网IP地址

7 允许Firewall_A的公网IP地址访问Firewall_B自身

Example 7: 点到点 IPSec 隧道

Step7 配置 Firewall_B 的路由

The screenshot shows the Huawei Network Management System interface. The top navigation bar includes the HUAWEI logo, user 'admin', and tabs for 面板 (Dashboard), 监控 (Monitoring), 对象 (Objects), 网络 (Network) [highlighted with a red box], and 系统 (System). The left sidebar lists various network components like 接口 (Interfaces), 安全区域 (Security Zones), DNS, DHCP服务器, 路由 (Routers), and various protocols (ISP, RIP, OSPF, BGP, 动态路由监控表, 路由表). Under 路由, '静态路由' is selected and highlighted with a red box.

1: 在 '配置默认优先级' (Configure Default Priority) 配置页，显示 IPv4 默认优先级为 60 <1-255> 和 IPv6 默认优先级为 60 <1-255>。应用按钮位于右侧。

2: 在左侧路由列表中，'静态路由' 选项被选中并用红色框标注。

3: 在 '静态路由列表' 中，'新建' (New) 按钮被标注为 3。

4: 在 '新建静态路由' (Create Static Route) 对话框中，所有输入项均被标注为 4，并包含一个说明框：配置到网络A中私网IP地址的路由，此处假设Firewall_B到Internet的下一跳IP地址为1.1.5.2。

参数	值
协议类型	IPv4
源虚拟路由器	public
目的地址/掩码	10.1.1.0/255.255.255.0
目的虚拟路由器	public
出接口	-- NONE --
下一跳	1.1.5.2
优先级	60
可靠性检测	不检测
描述	

对话框底部有 确定 和 取消 按钮。

Example 7: 点到点 IPSec 隧道

Step8 配置 Firewall_B 的 IPSec

The screenshot shows the HUAWEI USG6300 network management interface. The main window displays the 'IPSec策略列表' (IPSec Policy List) under the 'IPSec' category. A callout box with red border and blue arrow points to the right side of the interface, containing the following text:

本例中安全提议参数全部使用缺省值，
如果您对参数有明确要求，请修改，并
注意与Firewall_A上的配置保持一致。

The configuration steps are numbered as follows:

- ① Click the 'Network' icon in the top navigation bar.
- ② In the left sidebar, click 'IPSec' and then 'IPSec' again.
- ③ Click the 'New' button ('新建') in the top toolbar of the policy list.
- ④ A blue callout box contains the text: '先选择场景，然后完成基本配置。' (First select the scenario, then complete the basic configuration.)
- ⑤ In the 'Basic Configuration' section, set the 'Policy Name' to 'policy1', 'Local Interface' to 'GE0/0/1', and 'Local Address' to '1.1.5.1'. Set the 'Remote Address' to '1.1.3.1'. Under 'IKE Parameters', the 'IKE Version' is set to 'v1' and 'Encryption Algorithm' includes 'AES-256'. The 'IPsec Parameters' section shows 'ESP' selected as the protocol.
- ⑥ A blue callout box contains the text: '增加待加密的数据流' (Add Encrypted Data Flow). In the 'New Encrypted Data Flow' dialog, add a flow from 'Source Address/Address Group: 10.1.2.0/24' to 'Destination Address/Address Group: 10.1.1.0/24' with 'Protocol: any' and 'Action: Encryption'.
- ⑦ A blue callout box contains the text: '配置IKE/IPSec 安全提议' (Configure IKE/IPSec Security Proposals). This step involves configuring the security proposals on the right panel, which lists various parameters like IKE version, encryption algorithms, and IPsec protocols.

Example 7: 点到点 IPSec 隧道

Step9 结果验证 (1)

配置成功后，查看 IPSec 策略列表和 IPSec 监控信息，能够看到建立的 IPSec 隧道。此时，网络 A 中的主机能够成功访问网络 B 中的主机或服务器；同样地，网络 B 中的主机也能够成功访问网络 A 中的主机或服务器。

Firewall_A的IPSec策略列表和IPSec隧道监控信息

The screenshot shows the Huawei firewall interface. On the left, the navigation tree is expanded to show the IPsec section, with 'IPSec' and '监控' (Monitoring) selected. The main area displays the 'IPSec策略列表' (IPSec Policy List). A single policy named 'policy1' is listed, configured for 'public' virtual system, '点到点' (Point-to-Point) scenario, local interface 'GE0/0/1', remote address '1.1.5.1', and successful negotiation. A callout bubble points to this row with the text: '配置完成后如果IPSec隧道没有成功建立，请单击“诊断”查看错误原因和解决办法。' (After configuration is completed, if the IPSec tunnel does not successfully establish, click 'Diagnose' to view the error cause and solution method.)

The screenshot shows the 'IPSec监控列表' (IPSec Monitoring List) page. It lists the established 'policy1' tunnel. The table includes columns for policy name, virtual system, status, local and remote addresses, and various monitoring metrics like duration and rates. The '监控' (Monitoring) section in the navigation bar is highlighted.

策略名称	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (...)	发送/接收速率 (...)	最近一次建立时间	最近一次断开时间	断开原因	当日断开次数
policy1	public	IKE协商成功 IPSec协商成功	1.1.3.1	1.1.5.1	IP地址	1.1.5.1	ESP:AES-SHA2	源地址: 10.1.1.0/255.255.255.0 目的地址: 10.1.2.0/255.255.255.0 协议: any; 源端口: any; 目的端口: any	2046	0/0				

Example 7: 点到点 IPSec 隧道

Step9 结果验证 (2)

Firewall_B的IPSec策略列表和IPSec隧道监控信息

IPSec策略列表

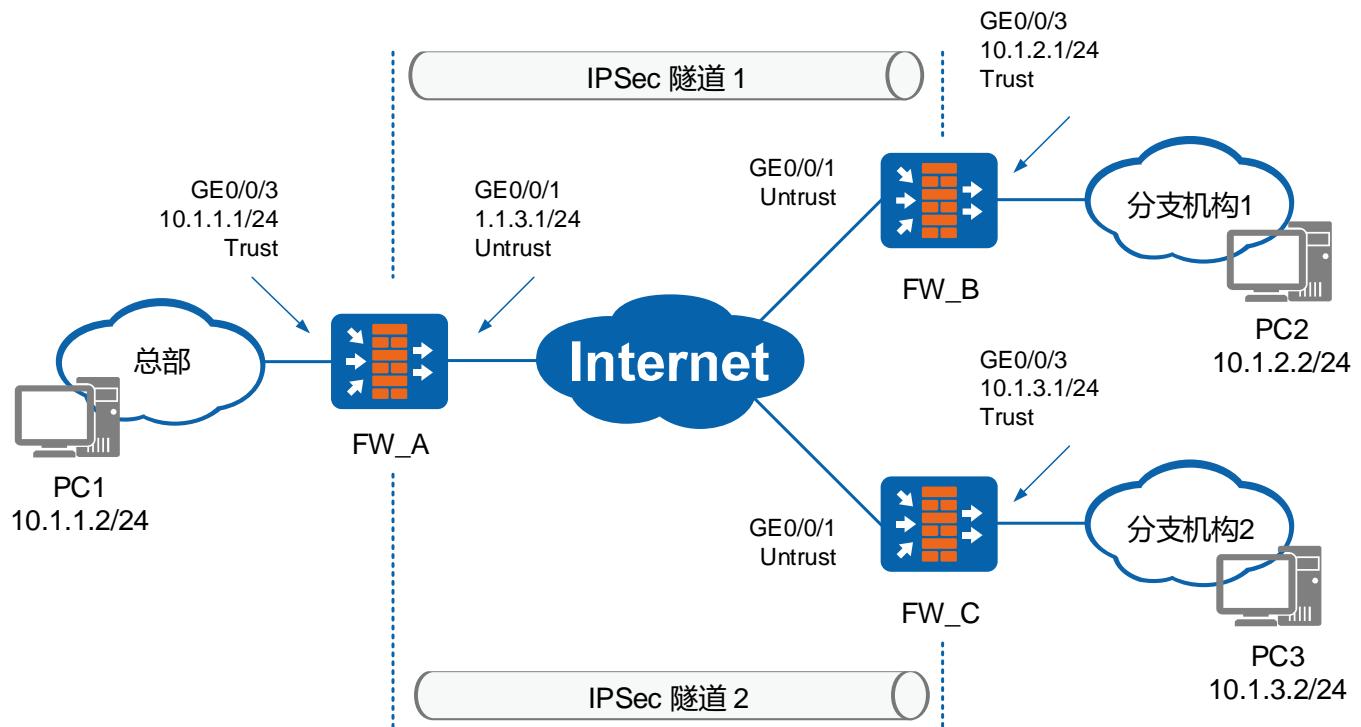
策略名称	虚拟系统	场景	本端接口	本端地址	对端地址	协商状态	启用	编辑
policy1	public	点到点	GE0/0/1	1.1.5.1	1.1.3.1	成功: 1 失败: 0 正在协商: 0	详情	<input checked="" type="checkbox"/>

IPSec监控列表

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (...)	发送/接收速率 (...)	最近一次建立时间	最近一次断开时间	断开原因	当日断开次数
policy1	public		IKE协商成功 IPSec协商成功	1.1.5.1	1.1.3.1	IP地址	1.1.3.1	ESP:AES-SHA2	源地址: 10.1.2.0/255.255.255.0 目的地址: 10.1.1.0/255.255.255.0 协议: any; 源端口: any; 目的端口: any	2046	0/0				

Example 8: 点到多点IPSec隧道（策略模板）

组网图



Firewall_A是总部的出口网关，Firewall_B和Firewall_C分别是分支机构1和分支机构2的出口网关，Firewall_A采用固定IP地址接入Internet，Firewall_B和Firewall_C采用动态获取到的IP地址接入Internet。

在Firewall_A和Firewall_B之间、Firewall_A和Firewall_C之间分别建立IPSec隧道，使分支机构1和分支机构2的设备能主动发起到总部的连接（总部不能主动发起到分支机构的连接）。

项目	Firewall_A (总部)	Firewall_B (分支1)	Firewall_C (分支2)
场景	点到多点	点到点	点到点
对端地址	不指定对端网关地址	1.1.3.1	1.1.3.1
认证方式	预共享密钥	预共享密钥	预共享密钥
预共享密钥	Admin@123	Admin@123	Admin@123
本端ID	IP地址	IP地址	IP地址
对端ID	接受任意对端ID	IP地址	IP地址

Example 8: 点到多点IPSec隧道（策略模板）

Step1 配置Firewall_A（总部）的接口

1 网络 -> **2** 接口 -> **3** 编辑 -> **4** 配置外网接口参数 -> **5** 配置内网接口参数 -> **6** 确定

The screenshot shows the Huawei Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin', '提交' (Submit), '保存' (Save), and a '...' button. Below the navigation bar are tabs: '面板' (Panel), '监控' (Monitoring), '策略' (Policy), '对象' (Object), '网络' (Network) which is highlighted with a red box and has a red circle with '1' above it, and '系统' (System). On the left sidebar, under '接口' (Interface), there are links for '接口对' (Interface Pair), '安全区域' (Security Zone), 'DNS', 'DHCP服务器' (DHCP Server), '路由' (Routing), 'IPSec', 'L2TP', 'L2TP over IPSec', 'GRE', and 'DSVPN'. The main area shows a table of interfaces:

接口名称	安全区域	虚拟系统	IP地址	连接类型	VLAN	模式	状态	物理 IPv4	IPv6	启用	编辑
GE0/0/0(GE0/MGMT)								+	+	+	
GE0/0/1								+	+	+	
GE0/0/2								+	+	+	
GE0/0/3								+	+	+	
GE0/0/4								+	+	+	
GE0/0/5								+	+	+	
GE0/0/6								+	+	+	

Two specific rows are highlighted with red boxes and numbered 3 and 5 respectively. A red box labeled '4' points to the '修改GigabitEthernet' dialog for the GE0/0/1 interface. A red box labeled '6' points to the '修改GigabitEthernet' dialog for the GE0/0/3 interface.

修改GigabitEthernet (Outer Network Interface Configuration):

- 接口名称: GigabitEthernet0/0/1
- 别名:
- 虚拟系统: public
- 安全区域: untrust
- 模式: 路由
- IPv4**:
 - 连接类型: 静态IP
 - IP地址: 1.1.3.1/24
 - 默认网关:
 - 首选DNS服务器:
 - 备用DNS服务器:
 - 多出口选项

修改GigabitEthernet (Inner Network Interface Configuration):

- 接口名称: GigabitEthernet0/0/3
- 别名:
- 虚拟系统: public
- 安全区域: trust
- 模式: 路由
- IPv4**:
 - 连接类型: 静态IP
 - IP地址: 10.1.1.1/24
 - 默认网关:
 - 首选DNS服务器:
 - 备用DNS服务器:
 - 多出口选项

At the bottom right of the interface configuration dialogs are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 8: 点到多点IPSec隧道（策略模板）

Step2 配置Firewall_A（总部）的安全策略

1 在Huawei路由器管理界面中，进入“策略”模块。

2 选择“安全策略”。

3 点击“新建安全策略”按钮。

4 允许总部的私网IP地址访问分支1和分支2的私网IP地址。

5 允许分支1和分支2的私网IP地址访问总部的私网IP地址。

6 允许分支1和分支2的公网IP地址访问Firewall_A自身。由于分支的公网IP地址不固定，因此不配置源地址。

7 允许Firewall_A自身访问分支1和分支2的公网IP地址。由于分支的公网IP地址不固定，因此不配置目的地址。

策略名称	源安全区域	目的安全区域	源地址/地区	目的地址/地区	动作
policy_ipsec_1	trust	untrust	10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24		允许
policy_ipsec_2	untrust	trust		10.1.2.0/24, 10.1.3.0/24	允许
policy_ipsec_3	untrust	local		1.1.3.1/32	允许
policy_ipsec_4	local	untrust	1.1.3.1/32		允许

Example 8: 点到多点IPSec隧道（策略模板）

Step3 配置Firewall_A（总部）的路由

1. 在Huawei USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“静态路由”。

3. 点击“新建”按钮，打开“新建静态路由”对话框。

4. 在“新建静态路由”对话框中，配置以下参数：

- 协议类型：IPv4
- 源虚拟路由器：public
- 目的地址/掩码：10.1.2.0/24
- 目的虚拟路由器：public
- 出接口：-- NONE --
- 下一跳：1.1.3.2
- 优先级：60
- 可靠性检测：不检测
- 描述：配置到分支1私网IP地址的路由，此处假设Firewall_A到Internet的下一跳IP地址为1.1.3.2。

5. 在“新建静态路由”对话框中，配置以下参数（与步骤4相同）：

- 协议类型：IPv4
- 源虚拟路由器：public
- 目的地址/掩码：10.1.3.0/24
- 目的虚拟路由器：public
- 出接口：-- NONE --
- 下一跳：1.1.3.2
- 优先级：60
- 可靠性检测：不检测
- 描述：配置到分支2私网IP地址的路由，此处假设Firewall_A到Internet的下一跳IP地址为1.1.3.2。

Example 8: 点到多点IPSec隧道（策略模板）

Step4 配置Firewall_A（总部）的IPSec

The screenshot shows the HUAWEI USG6300 firewall's configuration interface. The main window displays the 'IPSec策略列表' (IPSec Policy List) with a red box highlighting the '新建' (New) button. A red circle labeled '1' is on the '网络' (Network) icon in the top navigation bar.

Step 1: Click the '新建' button to start creating a new IPSec policy.

Step 2: In the left sidebar, click on 'IPSec' under the 'IPSec' category.

Step 3: In the '新建 IPSec策略' (Create New IPSec Policy) dialog, select '点到多点' (Site-to-Multipoint) as the scenario. A red box highlights this selection. A red circle labeled '3' is on the '场景' (Scenario) section.

Step 4: Configure the basic policy settings. A red box highlights the configuration area. A red circle labeled '4' is on the '配置IPSec策略' (Configure IPSec Policy) button.

Step 5: In the '待加密的数据流' (Encrypted Data Flow) section, click the '新建' (New) button. A red box highlights this button. A red circle labeled '5' is on the '新建' button.

Step 6: In the '新建待加密的数据流' (Create New Encrypted Data Flow) dialog, add the first encrypted data flow. Source address group: 10.1.1.0/24, Destination address group: 10.1.2.0/24, Protocol: any, Action: 加密 (Encrypt). A blue box highlights the source and destination address groups. A red circle labeled '6' is on the '增加待加密的数据流' (Add Encrypted Data Flow) button.

Step 7: In the '新建待加密的数据流' (Create New Encrypted Data Flow) dialog, add the second encrypted data flow. Source address group: 10.1.1.0/24, Destination address group: 10.1.3.0/24, Protocol: any, Action: 加密 (Encrypt). A blue box highlights the source and destination address groups. A red circle labeled '7' is on the '增加待加密的数据流' (Add Encrypted Data Flow) button.

Note: If static routes to branches have not been configured according to Step 3, check the '反向路由注入' (Reverse Route Injection) option in the '待加密的数据流' (Encrypted Data Flow) configuration. An orange callout points to this option with the text: '如果没有按照 Step3 配置到分支的静态路由，请勾选“待加密的数据流”中的“反向路由注入”，总部将自动生成到分支私网的路由。' (If static routes to branches have not been configured according to Step 3, check the "Reverse Route Injection" option in the "Encrypted Data Flow" configuration. The headquarter will automatically generate routes to branch private networks.)

Example 8: 点到多点IPSec隧道（策略模板）

Step5 配置Firewall_B（分支1）的接口

1. 在Huawei USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中选择“接口”。

3. 在右侧列表中选择外网接口（假设为GE0/0/1），并点击编辑图标（笔图标）。

4. 在“修改GigabitEthernet”对话框中，配置外网接口参数。连接类型选择“DHCP”。（注意：此处假设连接类型为DHCP。）

5. 在右侧列表中选择内网接口（假设为GE0/0/3），并点击编辑图标（笔图标）。

6. 在“修改GigabitEthernet”对话框中，配置内网接口参数。连接类型选择“静态IP”，IP地址输入为“10.1.2.1/24”。（注意：一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。）

Example 8: 点到多点IPSec隧道（策略模板）

Step6 配置Firewall_B（分支1）的安全策略

1. 在HUAWEI网管平台上，进入“策略”模块。

2. 选择“安全策略”。

3. 点击“新建安全策略”。

4. 新建安全策略1：允许分支1中的私网IP地址访问总部的私网IP地址。

5. 新建安全策略2：允许总部的私网IP地址访问分支1的私网IP地址。

6. 新建安全策略3：允许总部的公网IP地址访问Firewall_B自身。由于分支1的公网IP地址不固定，因此不配置目的地址。

7. 新建安全策略4：允许Firewall_B自身访总部的公网IP地址。由于分支1的公网IP地址不固定，因此不配置源地址。

策略名称	源安全区域	目的安全区域	动作
policy_ipsec_1	trust	untrust	允许
policy_ipsec_2	untrust	trust	允许
policy_ipsec_3	untrust	local	允许
policy_ipsec_4	local	untrust	允许

Example 8: 点到多点IPSec隧道（策略模板）

Step7 配置Firewall_B（分支1）的路由

1. 在Huawei USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“静态路由”。

3. 点击“新建”按钮，打开“新建静态路由”对话框。

4. 在“新建静态路由”对话框中，配置以下参数：

参数	值
协议类型	IPv4
源虚拟路由器	public
目的地址/掩码	10.1.1.0/24
目的虚拟路由器	public
出接口	GE0/0/1
下一跳	（空）
优先级	60
可靠性检测	不检测

5. 点击“确定”按钮，完成配置。

6. 在右侧的“静态路由列表”中，可以看到新添加的静态路由条目。

Example 8: 点到多点IPSec隧道（策略模板）

Step8 配置Firewall_B（分支1）的IPSec

The screenshot shows the HUAWEI USG6300 user interface for configuring an IPSec policy template. The steps are outlined as follows:

- 1** Click the **网络** (Network) icon in the top navigation bar.
- 2** In the left sidebar under **IPSec**, click **IPSec**.
- 3** Click the **新建** (New) button in the **IPSec策略列表** (IPSec Policy List).
- 4** Select **点到点** (Point-to-Point) as the scenario. A callout notes: "先选择场景，然后完成基本配置。" (Select the scenario first, then complete the basic configuration.)
- 5** Click the **新建** (New) button in the **待加密的数据流** (Encrypted Data Flow) list.
- 6** Set the source and destination address groups, protocol to **any**, and action to **加密** (Encryption). A callout notes: "增加待加密的数据流 (分支1到总部)" (Add encrypted data flow (Branch 1 to Headquarter)).
- 7** Open the **安全提议** (Security Proposal) dialog. This dialog contains two main sections: **IKE参数** (IKE Parameters) and **IPSec参数** (IPSec Parameters). The **IKE参数** section includes fields for IKE version (V1 selected), proposal mode (Automatic), encryption algorithms (AES-256 selected), and integrity algorithms (SHA2-256 selected). The **IPSec参数** section includes fields for封装模式 (Tunnel mode selected), security protocols (ESP selected), and encryption algorithms (AES-256 selected). A callout notes: "本例中安全提议参数全部使用缺省值，如果您对参数有明确要求，请修改。" (In this example, all security proposal parameters use default values. If you have specific requirements for parameters, please modify them.)

Example 8: 点到多点IPSec隧道（策略模板）

Step9 配置Firewall_C（分支2）的接口

1. 在左侧导航栏中，选择“网络”图标。

2. 在左侧子菜单中，选择“接口”。

3. 在右侧列表中，选择外网接口（假设为GE0/0/1），并点击“编辑”按钮。

4. 在“修改GigabitEthernet”对话框中，配置外网接口参数。连接类型选择为DHCP。

5. 在右侧列表中，选择内网接口（假设为GE0/0/3），并点击“编辑”按钮。

6. 在“修改GigabitEthernet”对话框中，配置内网接口参数。IP地址输入为10.1.3.1/24。

Example 8: 点到多点IPSec隧道（策略模板）

Step10 配置Firewall_C（分支2）的安全策略

1 在HUAWEI网管平台上，进入“策略”模块。

2 选择“安全策略”。

3 点击“新建安全策略”。

4 允许分支2中的私网IP地址访问总部的私网IP地址。

5 允许总部的私网IP地址访问分支2的私网IP地址。

6 允许总部的公网IP地址访问Firewall_C自身。由于分支2的公网IP地址不固定，因此不配置目的地址。

7 允许Firewall_C自身访总部的公网IP地址。由于分支2的公网IP地址不固定，因此不配置源地址。

策略名称	源安全区域	目的安全区域	源地址/地区	目的地址/地区	动作
policy_ipsec_1	trust	untrust	10.1.3.0/24	10.1.0/24	允许
policy_ipsec_2	untrust	trust	10.1.1.0/24	10.1.3.0/24	允许
policy_ipsec_3	untrust	local	1.1.3.1/32	(未配置)	允许
policy_ipsec_4	local	untrust	(未配置)	1.1.3.1/32	允许

Example 8: 点到多点IPSec隧道（策略模板）

Step11 配置Firewall_C（分支2）的路由

1. 在Huawei USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“静态路由”。

3. 在“新建”对话框中配置静态路由参数。

4. 配置到总部私网IP地址的路由。

参数	值
协议类型	IPv4
源虚拟路由器	public
目的地址/掩码	10.1.1.0/24
目的虚拟路由器	public
出接口	GE0/0/1
下一跳	
优先级	60
可靠性检测	不检测

Example 8: 点到多点IPSec隧道（策略模板）

Step12 配置Firewall_C（分支2）的IPSec

The screenshot shows the HUAWEI USG6300 network management interface with the following steps highlighted:

- 1** Click the **网络** (Network) icon in the top navigation bar.
- 2** In the left sidebar, click **IPSec**.
- 3** Click the **新建** (New) button in the **IPSec策略列表** (IPSec Policy List).
- 4** In the **新建IPSec策略** (New IPSec Policy) dialog, select **点到点** (Point-to-Point) under **场景** (Scenarios). A callout notes: 先选择场景，然后完成基本配置。 (Select the scenario first, then complete the basic configuration.)
- 5** Click the **新建** (New) button in the **待加密的数据流** (Encrypted Data Flow) list.
- 6** In the **新建待加密的数据流** (New Encrypted Data Flow) dialog, add a flow entry: 源地址/地址组: 10.1.3.0/24, 目的地址/地址组: 10.1.1.0/24, 协议: any, 动作: 加密. A callout notes: 增加待加密的数据流 (分支2到总部) (Add encrypted data flow (Branch 2 to Headquarter)).
- 7** On the right, the **安全提议** (Security Proposal) configuration page is shown. A callout notes: 本例中安全提议参数全部使用缺省值，如果您对参数有明确要求，请修改。 (In this example, all security proposal parameters use default values. If you have specific requirements for parameters, please modify them.)

IKE参数 (IKE Parameters)

IKE版本	v1	v2 可以响应v1和v2，但是发起协商时仅使用v2。		
协商模式	自动	主模式		
加密算法	AES-256	AES-192		
认证算法	SHA2-512	SHA2-384		
完整性算法	SHA2-512	SHA2-384		
PRF算法	SHA2-512	SHA2-384		
DH组	24	21	20	19
SA超时时间	86400	<60-604800>秒		

IPSec参数 (IPSec Parameters)

封装模式	自动	传输模式	隧道模式	
安全协议	ESP	AH	AH-ESP	
ESP加密算法	SM4	GCM256	GCM192	
ESP认证算法	SHA1	SHA2-512	SHA2-384	
PFS	NONE	24	21	20
SA超时	3600	<30-604800>秒		
基于流量	20971520	<0, 256-200000000>KB		

DPD (对端状态检测) (DPD (Peer Status Detection))

检测方式	周期性发送	需要时才发送
检测时间间隔	30	<10-3600>秒
重传时间间隔	15	<2-60>秒

Example 8：点到多点IPSec隧道（策略模板）

Step13 结果验证（1）

配置成功后，查看 IPSec 策略列表和 IPSec 监控信息，能够看到建立的 IPSec 隧道。且使用分支机构中的主机访问总部的某台主机或服务器时，能够成功访问。

Firewall_A（总部）的IPSec策略列表和IPSec隧道监控信息

配置完成后如果IPSec隧道没有成功建立，请单击“诊断”查看错误原因和解决办法。

The screenshot shows the Huawei firewall interface under the 'IPSec' section. In the 'IPSec策略列表' (IPSec Policy List) table, there is one entry: 'policy1' for 'public' virtual system, '点到多点' (Point-to-Multipoint) scenario, local interface 'GE0/0/1', remote address '1.1.3.1', and a status bar indicating '成功: 2 失败: 0 正在协商: 0'. A red box highlights this row. An orange arrow points from the text '配置完成后如果IPSec隧道没有成功建立,请单击“诊断”查看错误原因和解决办法。' to the '详细诊断' (Detailed Diagnosis) link in the table.

The screenshot shows the 'IPSec监控列表' (IPSec Monitoring List) table. It lists two entries for 'policy1' under the 'public' virtual system. Both entries show 'IKE协商成功' (IKE negotiation successful) and 'IPSec协商成功' (IPSec negotiation successful). The first entry has a source address of '10.1.1.0/255.255.255.0' and a destination address of '10.1.2.0/255.255.255.0'. The second entry has a source address of '10.1.1.0/255.255.255.0' and a destination address of '10.1.3.0/255.255.255.0'. Both entries have a duration of '2046' days and '0/0' bytes sent/received. A red box highlights the entire table.

Example 8: 点到多点IPSec隧道（策略模板）

Step13 结果验证（2）

Firewall_B（分支1）的IPSec策略列表和IPSec隧道监控信息

IPSec策略列表

策略名称	虚拟系统	场景	本端接口	本端地址	对端地址	协商状态	启用	编辑
policy1	public	点到点	GE0/0/1	1.1.5.1	1.1.3.1	成功: 1 失败: 0 正在协商: 0	<input checked="" type="checkbox"/>	<input type="checkbox"/>

IPSec监控列表

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (...)	发送/接收速率 (...)	最近一次建立时间	最近一次断开时间	断开原因	当日断开次数
policy1	public		IKE协商成功	1.1.5.1	1.1.3.1			ESP:AES-SHA2	源地址: 10.1.2.0/255.255.255.0 目的地址: 10.1.1.0/255.255.255.0 协议: any; 源端口: any; 目的端口: any	2046	0/0				

Example 8: 点到多点IPSec隧道（策略模板）

Step13 结果验证（3）

Firewall_C（分支2）的IPSec策略列表和IPSec隧道监控信息

IPSec策略列表

策略名称	虚拟系统	场景	本端接口	本端地址	对端地址	协商状态	启用	编辑
policy1	public	点到点	GE0/0/1	1.1.6.1	1.1.3.1	成功: 1 失败: 0 正在协商: 0	详情	编辑

IPSec监控列表

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (...)	发送/接收速率 (...)	最近一次建立时间	最近一次断开时间	断开原因	当日断开次数
policy1	public		IKE协商成功	1.1.6.1	1.1.3.1			ESP:AES-SHA2	源地址: 10.1.3.0/255.255.255.0 目的地址: 10.1.1.0/255.255.255.0 协议: any; 源端口: any; 目的端口: any	2046	0/0				

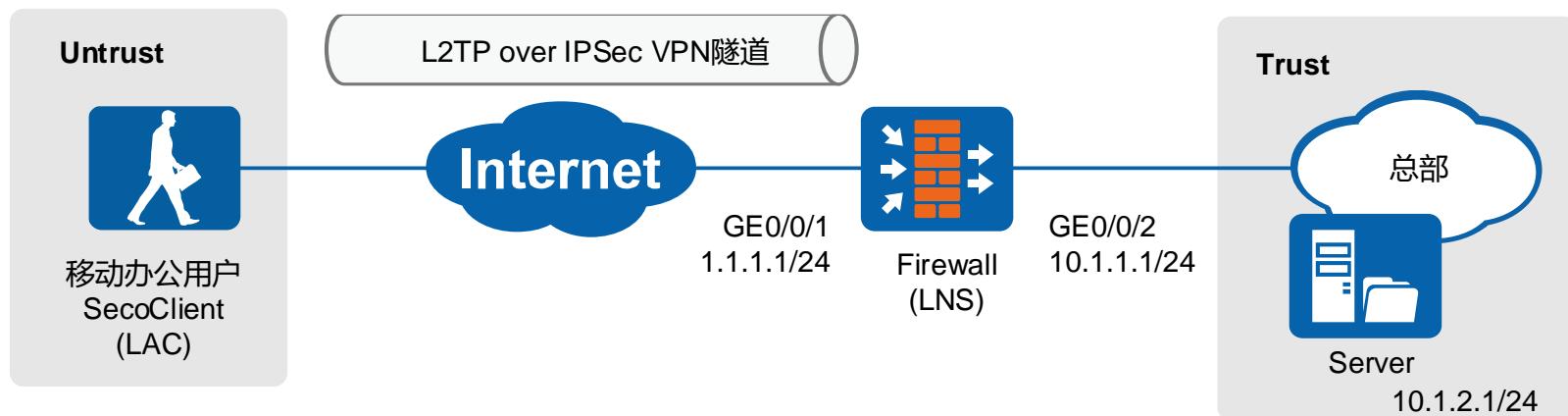
IPSec策略列表

策略名称	虚拟系统	场景	本端接口	本端地址	对端地址	协商状态	启用	编辑
policy1	public	点到点	GE0/0/1	1.1.6.1	1.1.3.1	成功: 1 失败: 0 正在协商: 0	详情	编辑

IPSec监控列表

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (...)	发送/接收速率 (...)	最近一次建立时间	最近一次断开时间	断开原因	当日断开次数
policy1	public		IKE协商成功	1.1.6.1	1.1.3.1			ESP:AES-SHA2	源地址: 10.1.3.0/255.255.255.0 目的地址: 10.1.1.0/255.255.255.0 协议: any; 源端口: any; 目的端口: any	2046	0/0				

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

[组网图](#)


LAC客户端通过Internet连接到公司总部的LNS侧。出差员工使用SecoClient (LAC) 直接向LNS侧发起连接请求，与LNS的通讯数据通过隧道 Tunnel传输。先使用L2TP封装第二层数据，对身份进行认证；再使用IPSec对数据进行加密。

项目		数据
LNS	L2TP配置	组名: default 用户名: user0001 用户密码: Password@123 用户地址池pool: 172.16.1.1 ~ 172.16.1.100 隧道验证密码: Hello@123
	IPSec配置	预共享密钥: Admin@123 本端ID: IP地址 对端ID: 接受任意对端ID
LAC	L2TP配置	用户认证名称: user0001 用户认证密码: Password@123 隧道验证密码: Hello@123
	IPSec配置	预共享密钥: Admin@123 对端地址: 1.1.1.1/24

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step1 配置接口

1. 在左侧导航栏中选择“网络”图标。

2. 在左侧子菜单中选择“接口”。

3. 在右侧列表中选择外网接口（GE0/0/1）并点击编辑图标。

4. 在“修改GigabitEthernet”对话框中配置外网接口参数，包括IP地址、子网掩码、网关和DNS服务器。

5. 在右侧列表中选择内网接口（GE0/0/2）并点击编辑图标。

6. 在“修改GigabitEthernet”对话框中配置内网接口参数，包括IP地址、子网掩码、网关和DNS服务器。

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step2 配置安全策略

1. 在 HUAWEI 网络管理界面中，进入“策略”模块。

2. 选择“安全策略”。

3. 点击“新建安全策略”。

4. 新建安全策略 I2tpipsec_ul，配置如下：

- 名称：I2tpipsec_ul
- 源安全区域：untrust
- 目的安全区域：local
- 源地址/地区：1.1.1.1/32
- 动作：允许

5. 新建安全策略 I2tpipsec_ue，配置如下：

- 名称：I2tpipsec_ue
- 源安全区域：local
- 目的安全区域：untrust
- 源地址/地区：1.1.1.1/32
- 目的地址/地区：1.1.1.1/32
- VLAN ID：1
- 动作：允许

6. 新建安全策略 I2tpipsec_ut，配置如下：

- 名称：I2tpipsec_ut
- 源安全区域：untrust
- 目的安全区域：trust
- 源地址/地区：172.16.1.1-172.16.1.100
- 目的地址/地区：10.1.2.0/24
- VLAN ID：1
- 动作：允许

7. 新建安全策略 I2tpipsec_tu，配置如下：

- 名称：I2tpipsec_tu
- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：10.1.2.0/24
- 目的地址/地区：172.16.1.1-172.16.1.100
- VLAN ID：1
- 动作：允许

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step3 配置路由

The screenshot shows the HUAWEI SecoClient configuration interface. The top navigation bar includes icons for Home, Panel, Monitoring, Objects, Network (highlighted with a red box and circled with a red number 1), and System. On the right, there are user authentication (admin), and save/submit buttons.

The left sidebar lists various configuration categories: Interface, Interface Pair, Security Zone, DNS, DHCP Server, and Routing (selected). Under Routing, it lists Intelligent Routing, Virtual Router, and Static Routing (highlighted with a red box and circled with a red number 2).

The main content area has two tabs: 'Configure Default Priority' (显示) and 'Static Route List'. The 'Configure Default Priority' tab contains fields for IPv4 and IPv6 default priorities (both set to 60). The 'Static Route List' tab shows a table of existing static routes. A red box highlights the 'New' button in the table header, and a red arrow points from it to the 'Create New Static Route' dialog box.

The 'Create New Static Route' dialog box is open, showing the following configuration:

- Protocol Type:** IPv4 (radio button selected)
- Source Virtual Router:** public
- Destination Address/Mask:** 0.0.0.0/0.0.0.0
- Destination Virtual Router:** public
- Interface:** --NONE--
- Next Hop:** 1.1.1.2
- Priority:** 60
- Reliability Detection:** Unchecked (Not Checked)
- Description:** (Empty)

A callout bubble with a red border and a red number 4 contains the text: "Configure the route to Internet, assuming the next hop IP address is 1.1.1.2 in this example."

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step4 配置L2TP用户

The screenshot shows the HUAWEI SecoClient configuration interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 提交 保存 ...' buttons. The main menu on the left lists various configuration categories like '证书' (Certificates), '地址' (Addresses), '地区' (Regions), '服务' (Services), '应用' (Applications), and '用户' (Users). A red box labeled '1' highlights the '对象' (Objects) icon in the top navigation.

The central '用户管理' (User Management) page has a red box labeled '3' around its top section, which contains '场景' (Scenarios) checkboxes: '上网行为管理' (Browsing Behavior Management), 'SSL VPN接入' (SSL VPN Access), 'L2TP/L2TP over IPSec' (L2TP/L2TP over IPSec), 'IPSec接入' (IPSec Access), and '管理员接入' (Administrator Access). Below this is a red box labeled '2' containing the 'default' configuration profile. The '用户所在位置' (User Location) section shows '本地' (Local) checked and '认证服务器' (Authentication Server) uncheckable.

A red box labeled '4' points to the '新建' (New) button in the '用户管理列表' (User Management List) table header. The table lists several users, with one row highlighted.

A callout bubble with orange arrowheads points from the '新建' button to a note: '本例中，用户登录名设置为user0001，密码设置为Password@123。' (In this example, the user login name is set to user0001, and the password is set to Password@123.)

A red box labeled '5' points to the '新建用户' (Create User) dialog box. This dialog contains fields for '登录名' (Login Name) set to 'user0001', '显示名' (Display Name), '描述' (Description), '密码' (Password) set to 'Password@123', and '确认密码' (Confirm Password) also set to 'Password@123'. A note below the password field specifies: '密码不能和用户名相同，长度为6~16个字符，且密码必须包含数字、大写字母、小写字母、特殊字符中的至少3种，如：Password@或password8#等。' (The password cannot be the same as the username, and it must be 6~16 characters long, containing at least 3 types of characters: digits, uppercase letters, lowercase letters, and special characters like @ or #.)

The bottom right of the dialog has '确定' (Confirm) and '取消' (Cancel) buttons.

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step5 新建地址池

The screenshot shows the HUAWEI SecoClient configuration interface. The top navigation bar includes 'HUAWEI', 'admin', and tabs for '提交' (Submit), '保存' (Save), and '...'. The left sidebar lists various configuration categories, with '地址池' (Address Pool) highlighted by a red box and the number '2'. The main content area shows a '对象' (Object) tab selected, indicated by a red box and the number '1'. A sub-menu '地址池列表' (Address Pool List) is open, showing a table with columns for '名称' (Name), '地址池范围' (Address Pool Range), 'DNS服务器' (DNS Server), and 'NBNS服务器' (NBNS Server). A red box highlights the '新建' (Create) button, and the number '3' is placed next to it. A red arrow points from the '新建' button down to the '新建IP地址池' (Create IP Address Pool) dialog box. This dialog box contains fields for '名称' (Name) set to 'pool' and '地址池范围' (Address Pool Range) set to '172.16.1.1-172.16.1.100'. To the right of these fields is a note: '每行可配置一个IP地址/范围, 行之间用回车分隔, 示例: 110.10.1.2 10.10.1.2-10.10.1.10'. A blue callout bubble with the number '4' contains the text: '新建名称为pool的地址池, 地址池范围设置为172.16.1.1-172.16.1.100。'. At the bottom of the dialog are '确定' (Confirm) and '取消' (Cancel) buttons. The bottom right corner of the interface shows pagination controls ('每页 50', 'GO') and a 'CLI 控制台' (CLI Console) button.

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step6 配置L2TP over IPSec

The screenshot shows the HUAWEI USG6300 network management interface. The main window displays the 'IPSec策略列表' (IPSec Policy List) and the '新建 IPSec 策略' (Create New IPSec Policy) dialog box.

1: Click the '新建' (New) button in the top right of the policy list.

2: Select 'IPSec' from the left sidebar.

3: In the '新建 IPSec 策略' dialog, click the '场景' (Scenario) tab.

4: Select '点到多点' (Point-to-Multipoint) as the scenario. A callout box notes: '先选择场景，然后完成基本配置。' (Select the scenario first, then complete the basic configuration).

5: In the '基本配置' (Basic Configuration) section, set the '策略名称' (Policy Name) to 'ipsec', '本端接口' (Local Interface) to 'GE0/0/1', and '对端地址' (Remote Address) to '1.1.1.1'. A callout box notes: '在本例中，预共享密钥设置为Admin@123。' (In this example, the pre-shared key is set to Admin@123).

6: In the '待加密的数据流' (Encrypted Data Flow) configuration dialog, click the '新建' (New) button to add a new flow entry. A callout box notes: '新建待加密数据流，使所有经过L2TP封装的报文都走IPSec隧道。' (Create a new encrypted data flow so that all messages encapsulated by L2TP pass through the IPSec tunnel).

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step7 配置L2TP组

The screenshot shows the HUAWEI SecoClient configuration interface. The left sidebar lists various network services: Interface, Interface Pair, Security Zone, DNS, DHCP Server, Route, IPsec, L2TP, L2TP over IPSec, GRE, DSVPN, and SSL VPN. The L2TP node is selected, indicated by a red box labeled ②.

The main area has several tabs: 面板 (Panel), 监控 (Monitoring), 策略 (Policy), 对 (Peer), and 网络 (Network). The 网络 tab is selected, indicated by a red box labeled ①.

步骤 1: 启用L2TP

In the top configuration panel, the L2TP toggle switch is turned on. The tunnel inactivity timeout is set to 1800 seconds. A blue box labeled ③ points to the "应用" (Apply) button.

步骤 2: 新建L2TP组

The L2TP group list shows a group named "default-Ins". A red box labeled ④ points to the "修改L2TP" (Modify L2TP) button next to the group name. A blue box labeled ⑤ points to the "新建" (Create) button in the list header.

步骤 3: 在本例中，隧道验证密码为 Hello@123。

A callout bubble provides the tunnel verification password: "Hello@123".

修改L2TP Group Configuration (弹窗)

The "修改L2TP" dialog shows the following configuration:

- 组名称: default-Ins
- 本端隧道名称:
- 对端隧道名称: ipsec_tunnel_split
- 隧道密码认证:
- 隧道密码: *
- 确认隧道密码: *
- 认证域: default
- 隧道关联安全域: trust
- L2TP认证模式: PAP CHAP
- 提示: 为保证协商报文互通, 需要开启双向安全策略。[新建安全策略]
- 用户地址分配设置:
 - 服务器地址/子网掩码: 172.16.1.1/255.255.255.255 *
 - 地址池: 用户地址池 对端地址
 - 用户地址池: pool

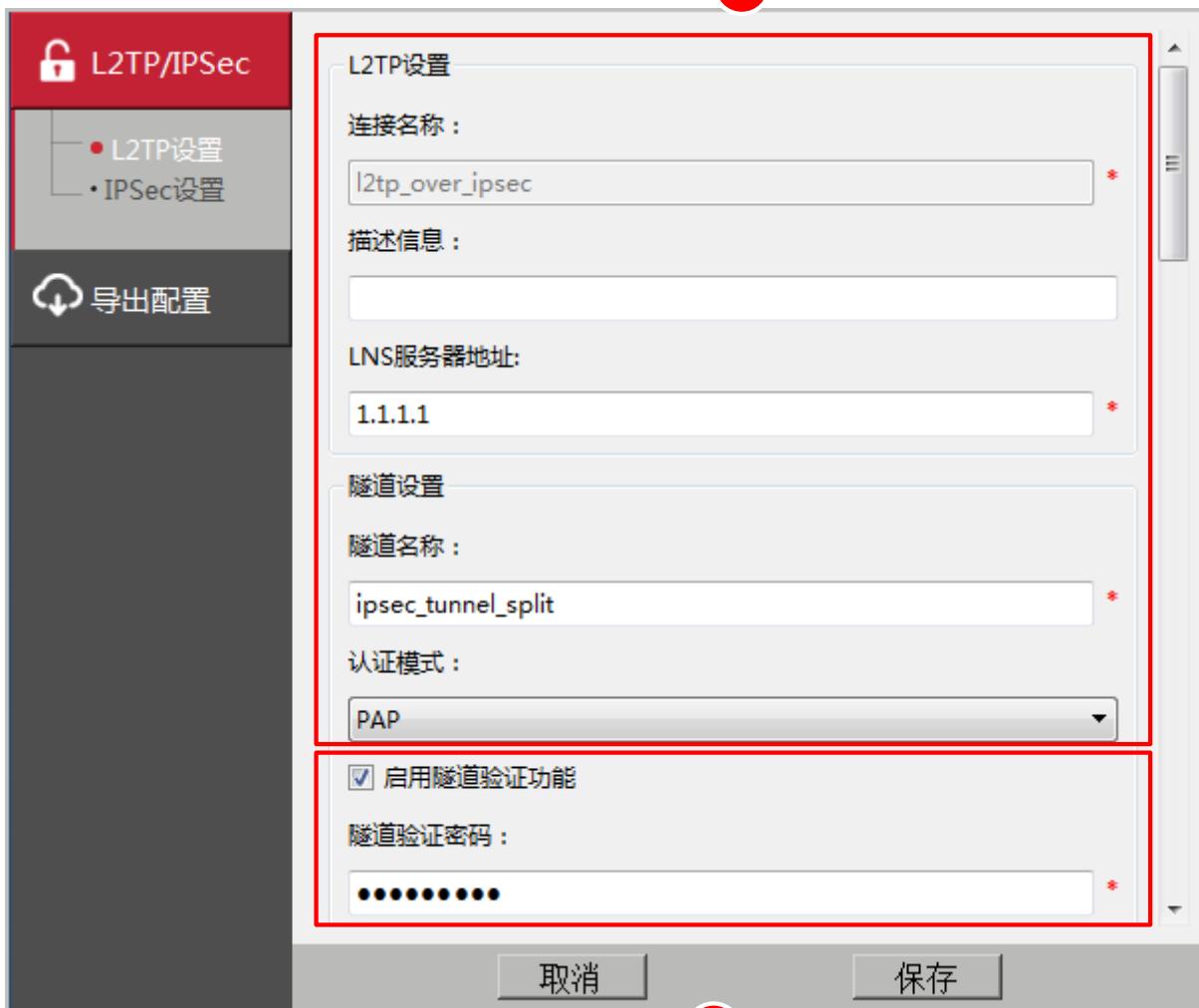
At the bottom of the dialog are "高级" (Advanced) and "确定" (Confirm) buttons.

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step8 配置SecoClient (1)

SecoClient是华为公司推出的一款用于VPN远程接入的终端软件，主要为移动办公用户远程访问企业内网资源提供安全、便捷的接入服务。目前可在华为企业技术支持网站 (<http://support.huawei.com/enterprise>) 上搜索并下载。

在LAC侧PC上打开SecoClient客户端



配置L2TP连接参数

3

4

启用隧道验证功能，隧道验证密码为Hello@123。

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step8 配置SecoClient (2)

启用IPSEC安全协议

预设共享密钥 USBKey 数字签名认证

身份认证字：
Admin@123

IPSEC设置

IPSEC服务器地址：
192.168.1.1

使用LNS服务器地址

封装模式：
 隧道模式 传输模式

ESP协议验证算法：
SHA2-256

ESP协议加密算法：
AES-256

选择预共享密钥验证，身份
认证字为Admin@123。

IKE设置

协商模式：
 主模式 野蛮模式

ID类型：
IP地址

本端名字：

安全网关名字：

验证算法：
SHA2-256

加密算法：
AES-256

DH组标志：
Group2 (1024 bit)

IKE高级设置

启用PFS特性

安全参数：
Group1 (768 bit)

安全联盟生存周期：
86400 秒 范围：60-604800

IPSEC高级设置

安全联盟生存周期：
3600 秒 范围：30-604800

2 配置IPSec封装模式及算法

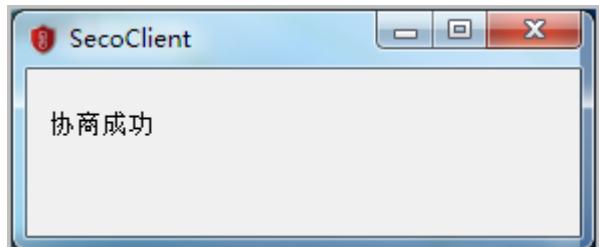
3 配置IKE协商模式及算法

Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step9 结果验证 (1)



接入成功后，系统界面右下角会弹出“协商成功”的提示信息。



Example 9.1: 客户端 L2TP over IPSec 接入 (SecoClient)

Step9 结果验证 (2)

登录FW查看L2TP监控列表，可以看到user0001用户已经登录成功。

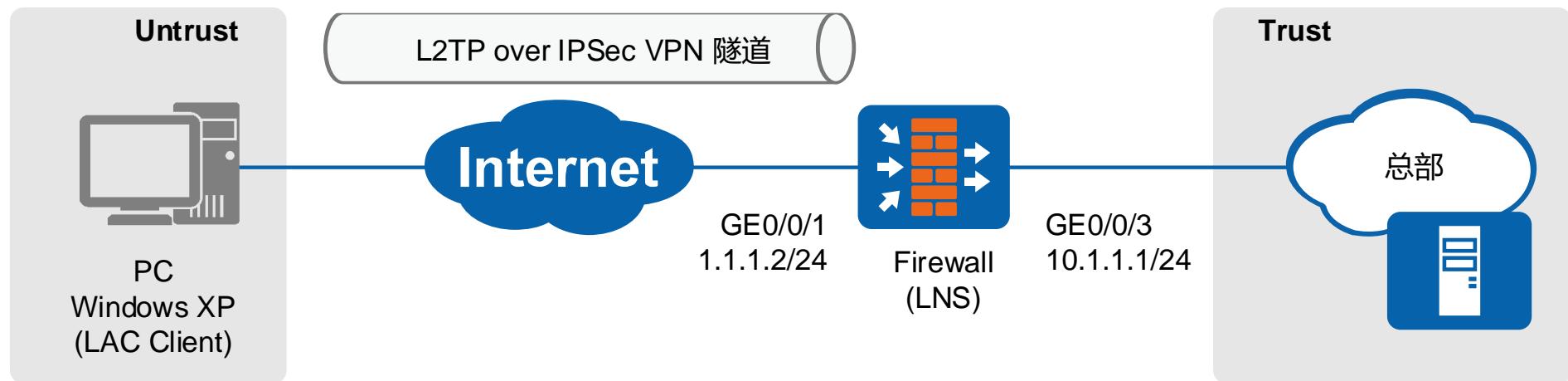
本端通道ID	对端通道ID 本地地址	对端地址	端口	会话数	对端名称
1	1 1.1.1.1	172.16.1.100	5524	1	ipsec_tunnel_split

查看IPSec监控列表，可以看到IPSec隧道建立成功。

策略名称	IKE用户描述	虚拟系统	状态	本地地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (... 发送/接收速率 (... 最近一次建立时间 最近一次断开时间 断开原因 当日断开次数
ipsec		public	IKE协商成功 IPSec协商成功	1.1.1.1	172.16.1.100			ESP-AES-256-SHA2-256	源地址[端口]: 1.1.1.1[1701] 目的地址[端口]: 172.16.1.100[5524] 协议: UDP	41 0/0

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

组网图



LAC客户端通过Internet连接到公司总部的LNS侧。出差员工使用搭载Windows XP操作系统的便携机直接向LNS侧发起连接请求，与LNS的通讯数据通过隧道Tunnel传输。先使用L2TP封装第二层数据，对身份进行认证；再使用IPSec对数据进行加密。

项目	数据
LNS	L2TP配置 组名: default 用户名: vpdnuser 用户密码: Hello@123
	IPSec配置 预共享密钥: Admin@123 本端ID: IP地址 对端ID: 接受任意对端ID
	用户地址池pool 10.1.2.2 ~ 10.1.2.100 请确保总部设备和地址池中地址路由可达。路由下一跳指向防火墙连接总部内网的接口GE0/0/3。
LAC	L2TP配置 用户认证名称: vpdnuser 用户认证密码: Hello@123
	IPSec配置 预共享密钥: Admin@123 对端地址: 1.1.1.2/24

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step1 配置接口

1. 在左侧导航栏中选择“网络”图标。

2. 在左侧子菜单中选择“接口”。

3. 在右侧列表中找到外网接口（GE0/0/0(GE0/MGMT)）并启用（启用来复选框）。

4. 在下方的“修改GigabitEthernet”对话框中配置外网接口参数。包括：接口名称（GigabitEthernet0/0/1）、连接类型（静态IP）、IP地址（1.1.1.2/24）、默认网关（1.1.1.254）。

5. 在右侧列表中找到内网接口（GE0/0/1）并启用（启用来复选框）。

6. 在下方的“修改GigabitEthernet”对话框中配置内网接口参数。包括：接口名称（GigabitEthernet0/0/3）、连接类型（静态IP）、IP地址（10.1.1.1/24）、默认网关、首选DNS服务器、备用DNS服务器。

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step2 配置安全策略

1. 在 HUAWEI 网络管理界面中，进入“策略”模块。

2. 选择“安全策略”。

3. 点击“新建安全策略”。

4. 新建安全策略 policy1，配置如下：

- 名称：policy1
- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：10.1.1.0/24
- 动作：允许

说明：允许总部服务器访问外网。

5. 新建安全策略 policy2，配置如下：

- 名称：policy2
- 源安全区域：untrust
- 目的安全区域：trust
- 源地址/地区：10.1.1.0/24
- 动作：允许

说明：允许 LAC 访问总部服务器。

6. 新建安全策略 policy3，配置如下：

- 名称：policy3
- 源安全区域：untrust
- 目的安全区域：local
- 源地址/地区：1.1.1.2/32
- 动作：允许

说明：允许 LAC 与防火墙通信。

7. 新建安全策略 policy4，配置如下：

- 名称：policy4
- 源安全区域：local
- 目的安全区域：untrust
- 源地址/地区：1.1.1.2/32
- 动作：允许

说明：允许防火墙与 LAC 通信。

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step3 新建L2TP用户

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 提交 保存 ...' buttons. The main menu on the left lists categories like '证书' (Certificates), '地址' (Addresses), '地区' (Regions), '服务' (Services), '应用' (Applications), and '用户' (Users). Under '用户', 'default' is selected. The top right has tabs for '对象' (Objects) and '策略' (Policies), with '对象' highlighted by a red circle labeled '1'. The central panel shows '用户管理' (User Management) with a red box around the '场景' (Scenarios) section. It includes checkboxes for '上网行为管理' (Browsing Behavior Management), 'SSL VPN接入' (SSL VPN Access), **L2TP/L2TP over IPSec** (selected), 'IPSec接入' (IPSec Access), and '管理员接入' (Administrator Access). Below this is a '用户配置' (User Configuration) section with '用户所在位置' (User Location) set to '本地' (Local). A red box highlights this area. A blue callout '3 选择接入场景及认证类型' (Select access scenario and authentication type) points to the scenarios section. In the '用户管理列表' (User Management List) table, a red box highlights the '新建' (New) button. A red circle labeled '4' points to the '新建' button. A blue callout '5 新建L2TP用户' (Create L2TP User) points to the '新建' button. The bottom '新建用户' (Create User) dialog box is shown with a red box around its input fields. The '登录名' (Login Name) field contains 'vpdnuser'. The '密码' (Password) and '确认密码' (Confirm Password) fields both contain 'Hello@123'. A note in the dialog states: '密码不能和用户名相同, 长度为6~16个字符, 且密码必须包含数字、大写字母、小写字母、特殊字符中的至少3种, 如: Password@或password8#等。' (The password cannot be the same as the username, must be 6~16 characters long, and must contain at least 3 types of characters: digits, uppercase letters, lowercase letters, and special characters. Examples: Password@ or password8#). A blue callout '本例中, 用户登录名设置为vpdnuser, 密码设置为Hello@123。' (In this example, the user login name is set to vpdnuser, and the password is set to Hello@123.) points to the password fields. The bottom right of the dialog has '确定' (Confirm) and '取消' (Cancel) buttons.

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step4 新建地址池

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI', 'admin', and tabs for '对象' (Object), '策略' (Policy), '网络' (Network), and '系统' (System). The left sidebar menu is collapsed, and the main area displays the '地址池列表' (Address Pool List) with a '新建' (New) button highlighted by a red circle labeled '1'. A red arrow points from this button to a modal window titled '新建IP地址池' (Create New IP Address Pool). Inside the modal, the '名称' (Name) field is set to 'pool' and the '地址池范围' (Address Pool Range) field contains '10.1.2.2-10.1.2.100'. A note on the right specifies that each row can configure an IP address range, separated by a carriage return, with examples like '110.10.1.2' and '10.10.1.2-10.10.1.10'. Below the modal, the '扩展网络属性' (Advanced Network Properties) section is partially visible, showing fields for '首选DNS服务器' (Primary DNS Server) and '备选DNS服务器' (Secondary DNS Server). The bottom right of the modal has '确定' (Confirm) and '取消' (Cancel) buttons.

1 新建

2 地址池

3 新建

4 新建名称为pool的地址池，地址池范围设置为10.1.2.2-10.1.2.100。

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step5 配置L2TP over IPSec

1. 在 HUAWEI USG6300 网络管理界面中，进入“网络”模块。

2. 在左侧树状菜单中，选择“IPSec”下的“IPSec”。

3. 点击“新建”按钮（带③号）。

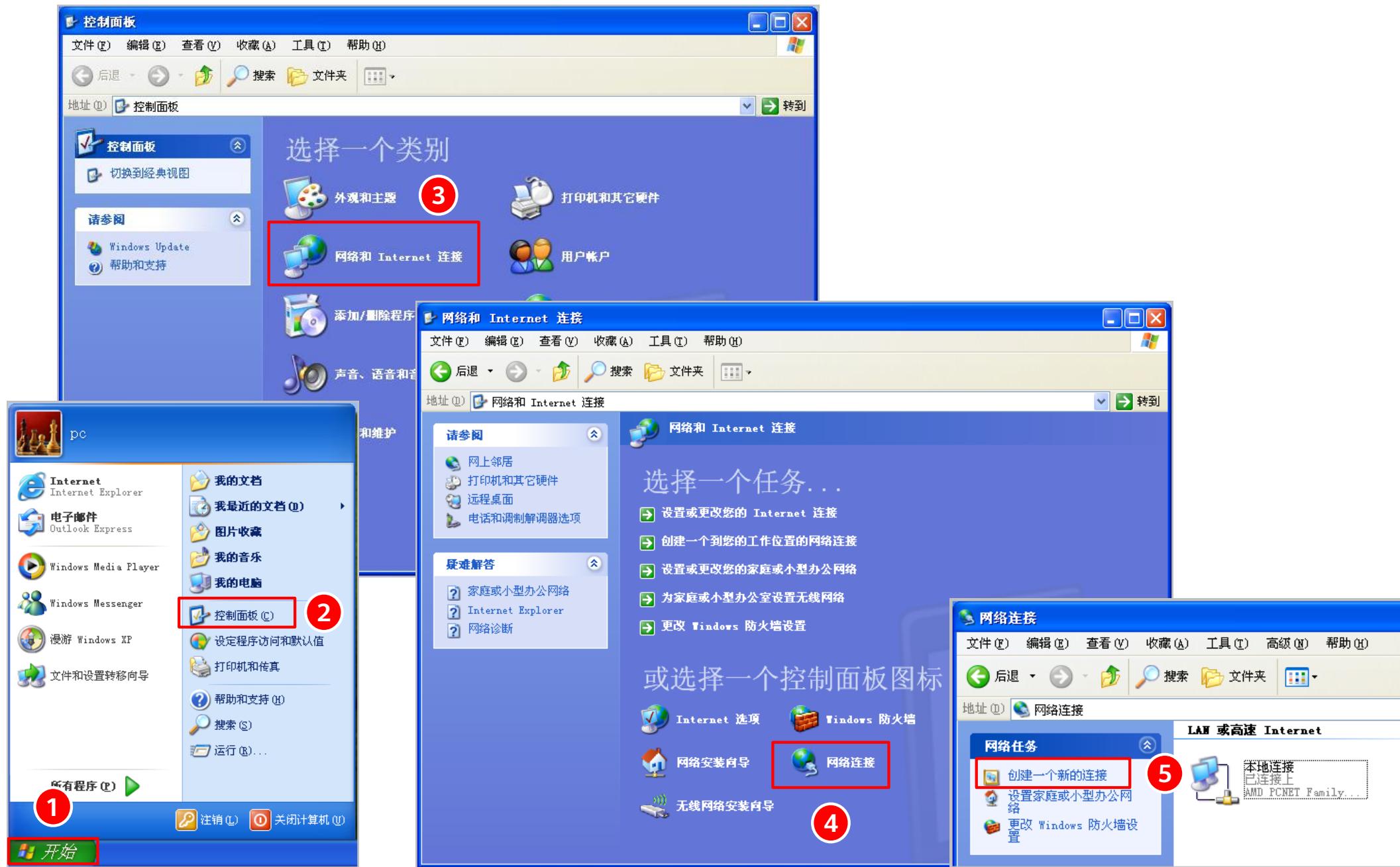
4. 在“新建IPSec策略”对话框中，先选择“场景”为“点到多点”，然后完成基本配置。注意预共享密钥输入框内显示“预共享密钥：Admin@123”。

5. 在“拨号用户配置”部分，选择“用户地址池”为“pool”。

6. 在右侧“新建待加密的数据流”对话框中，新建待加密数据流，使所有经过L2TP封装的报文都走IPSec隧道。

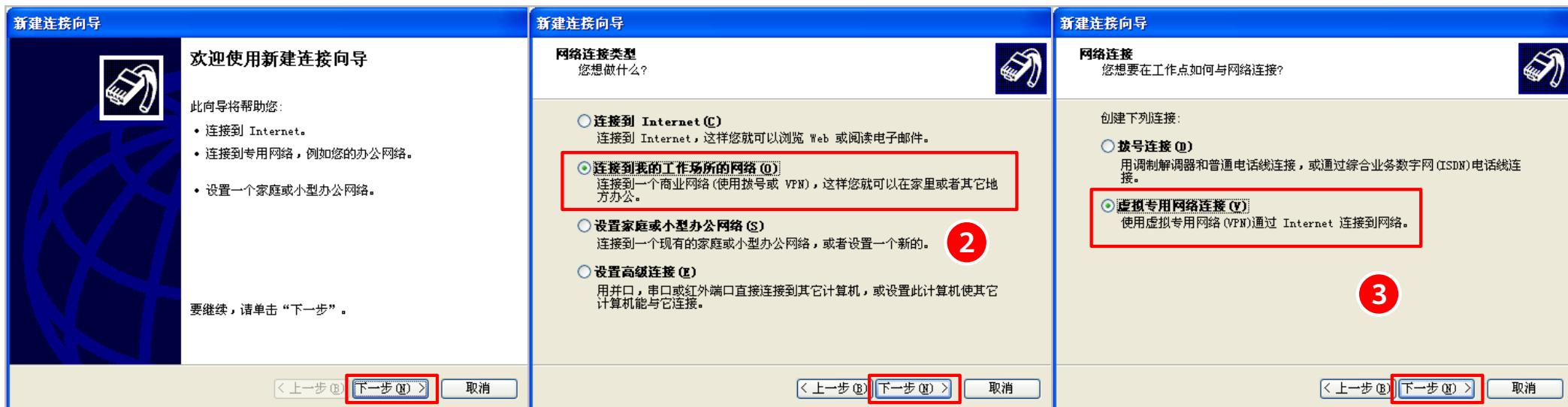
提示：先选择场景，然后完成基本配置。

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP) Step6 配置LAC拨号参数 (1)

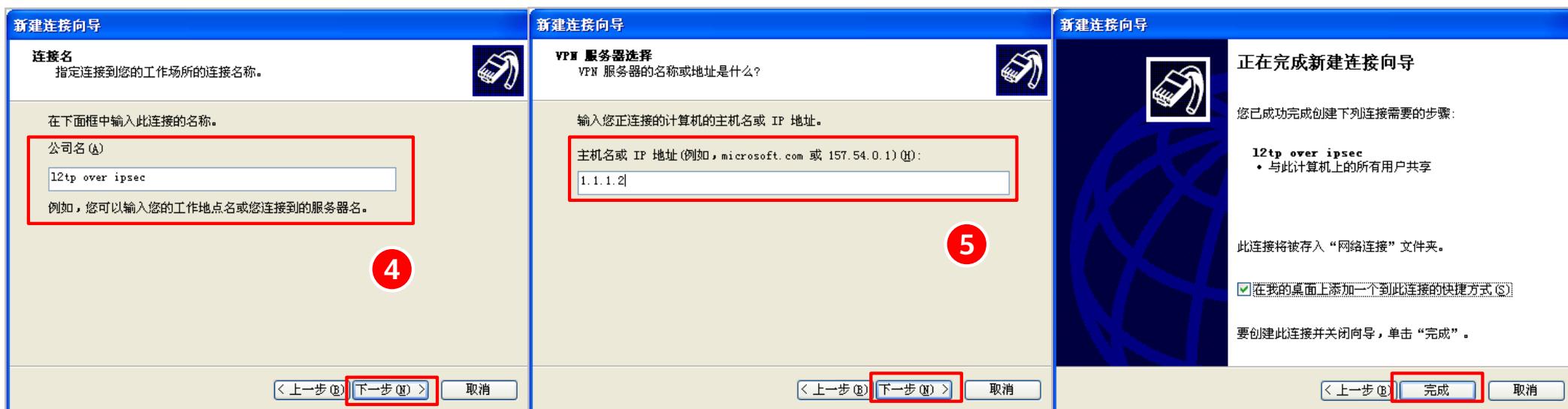


Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step6 配置LAC拨号参数 (2)



1



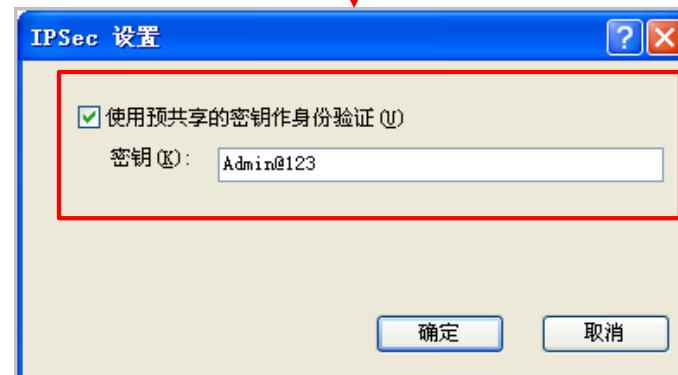
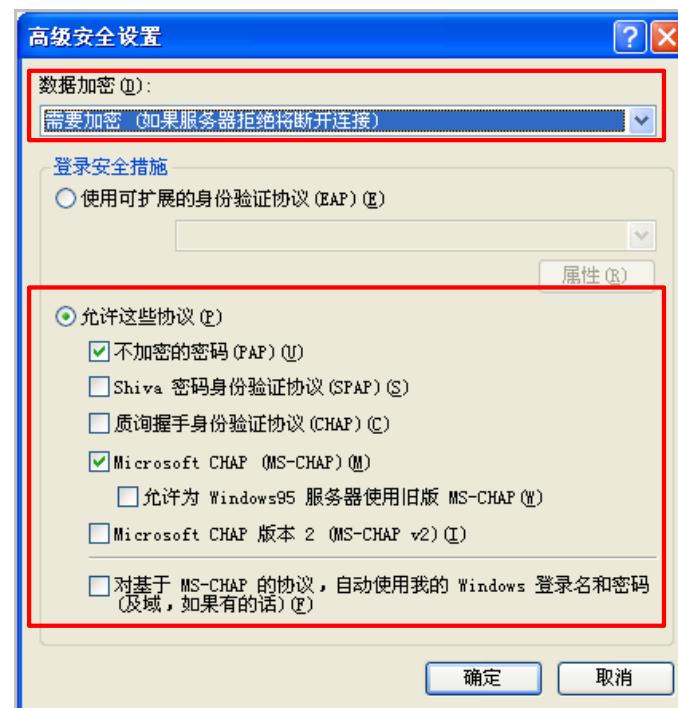
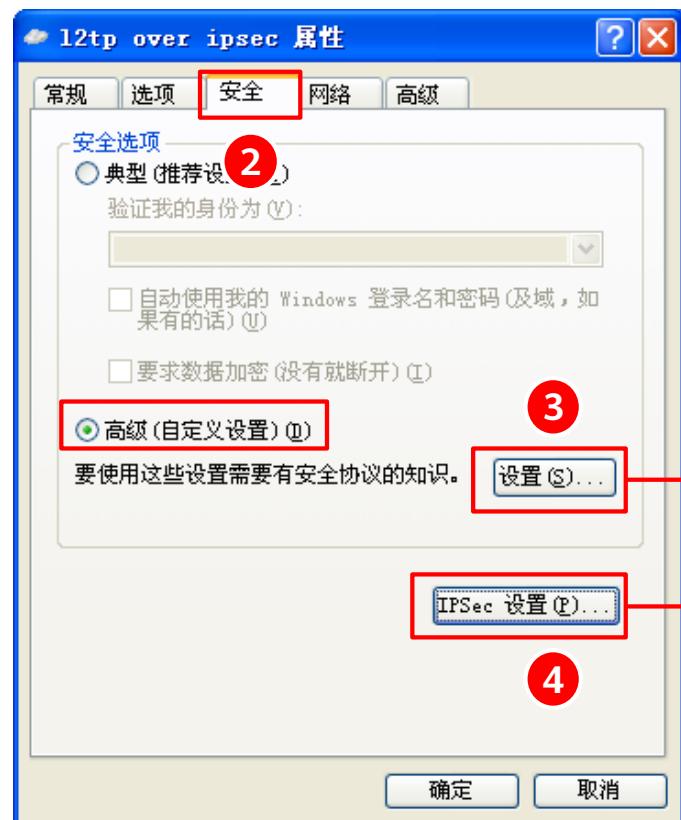
4

5

6

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step6 配置LAC拨号参数 (3)



Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step7 结果验证 (1)

用户名为vpdnuser，密码为Hello@123。

1 输入用户名、密码

2 单击“连接”，系统提示VPN连接成功。

3 在任务栏通知区域显示的连接状态图标上单击，以获得更详细的信息。

4 在“网络连接”中可以查看VPN的连接状态。

属性	值
设备名	WAN 微型端口 (L2TP)
设备类型	vpn
服务器类型	PPP
传输	TCP/IP
身份验证	MD5 CHAP
IPSEC 加密	IPSec, ESP 3DES
压缩	(无)
PPP 多重链接帧	关
服务器 IP 地址	10.1.2.2
客户端 IP 地址	10.1.2.100

Example 9.2: 客户端 L2TP over IPSec 接入 (Windows XP)

Step7 结果验证 (2)

登录防火墙查看L2TP监控列表，可以看到用户已经登录成功。



L2TP通道监控列表

本端通道ID	对端通道ID 本端地址	对端地址	端口	会话数	对端名称
1	5 1.1.1.2	[REDACTED]	1701	1	[REDACTED]

查看IPSec监控列表，可以看到IPSec隧道建立成功。

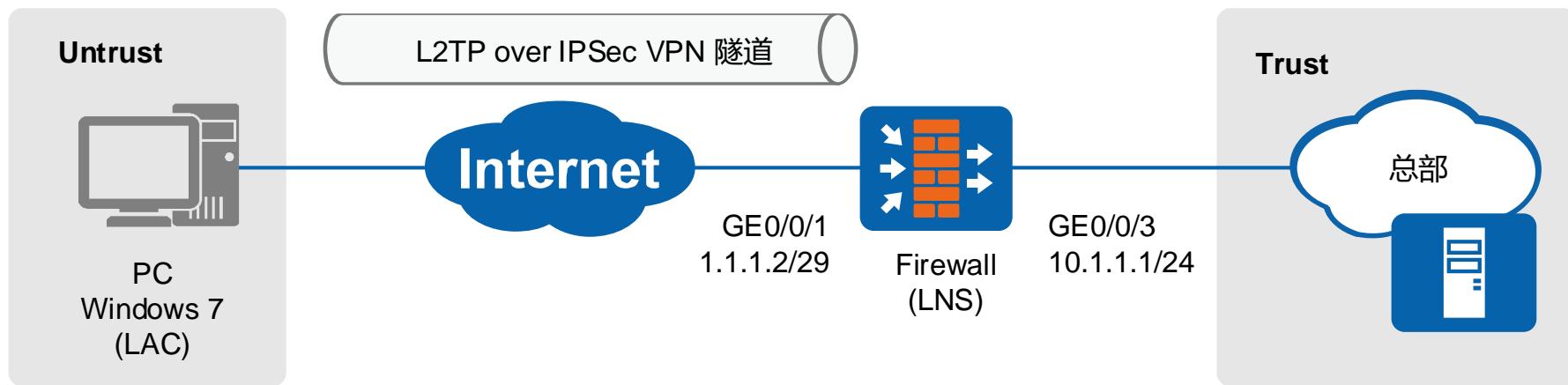


IPSec监控列表

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (... 发送/接收速率 (... 最近一次建立时间 最近一次断开时间 断开原因 当日断开次数
ipsec_policy	public		IKE协商成功	1.1.1.2	[REDACTED]			ESP-3DES-SHA1	源地址[端口]: 1.1.1.2[1701] 目的地址[端口]: [REDACTED][1701] 69 0/0 协议: UDP	

Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

组网图



LAC客户端通过Internet连接到公司总部的LNS侧。出差员工使用搭载Windows 7操作系统的便携机直接向LNS侧发起连接请求，与LNS的通讯数据通过隧道Tunnel传输。先使用L2TP封装第二层数据，对身份进行认证；再使用IPSec对数据进行加密。

项目	数据
LNS	L2TP配置 组名: default 用户名: vpnuser001 用户密码: Password@123
	IPSec配置 预共享密钥: Admin@123 本端ID: IP地址 对端ID: 接受任意对端ID
	用户地址池pool 10.1.2.2 ~ 10.1.2.100 请确保总部设备和地址池中地址路由可达。路由下一跳指向防火墙连接总部内网的接口GE0/0/3。
LAC	L2TP配置 用户认证名称: vpnuser001 用户认证密码: Password@123
	IPSec配置 预共享密钥: Admin@123 对端地址: 1.1.1.2/29

Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step1 配置接口

1. 在左侧导航栏中选择“网络”图标。

2. 在左侧子菜单中选择“接口”。

3. 在右侧列表中勾选“启用”复选框。

4. 在左侧子菜单中选择“L2TP over IPSec”，进入外网接口参数配置界面。

5. 在右侧列表中勾选“启用”复选框。

6. 在左侧子菜单中选择“IPSec”，进入内网接口参数配置界面。

修改GigabitEthernet (GE0/0/0) - 外网接口参数配置

接口名称	GigabitEthernet0/0/0
别名	
虚拟系统	public
安全区域	untrust
模式	路由
连接类型	静态IP
IP地址	1.1.1.2/29
默认网关	1.1.1.254
首选DNS服务器	
备用DNS服务器	
<input type="checkbox"/> 多出口选项	

修改GigabitEthernet (GE0/0/3) - 内网接口参数配置

接口名称	GigabitEthernet0/0/3
别名	
虚拟系统	public
安全区域	trust
模式	路由
连接类型	静态IP
IP地址	10.1.1.1/24
默认网关	
首选DNS服务器	
备用DNS服务器	
<input type="checkbox"/> 多出口选项	

Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step2 配置安全策略

1. 在 HUAWEI 网络管理界面中，进入“策略”模块。

2. 选择“安全策略”。

3. 点击“新建安全策略”。

4. 新建安全策略 policy1，配置如下：

- 名称：policy1
- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：10.1.1.0/24
- 动作：允许

说明：允许总部服务器访问外网。

5. 新建安全策略 policy2，配置如下：

- 名称：policy2
- 源安全区域：untrust
- 目的安全区域：trust
- 源地址/地区：10.1.1.0/24
- 动作：允许

说明：允许 LAC 访问总部服务器。

6. 新建安全策略 policy3，配置如下：

- 名称：policy3
- 源安全区域：untrust
- 目的安全区域：local
- 源地址/地区：1.1.1.2/32
- 动作：允许

说明：允许 LAC 与防火墙通信。

7. 新建安全策略 policy4，配置如下：

- 名称：policy4
- 源安全区域：local
- 目的安全区域：untrust
- 源地址/地区：1.1.1.2/32
- 动作：允许

说明：允许防火墙与 LAC 通信。

Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step3 新建L2TP用户

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 提交 保存 ...' buttons. The main menu on the left lists categories like '证书' (Certificates), '地址' (Addresses), '地区' (Regions), '服务' (Services), '应用' (Applications), and '用户' (Users). Under '用户', 'default' is selected. The top right has tabs for '对象' (Objects) and '策略' (Policies), with '对象' highlighted by a red circle labeled '1'. The central panel shows '用户管理' (User Management) with a red box around the '场景' (Scenarios) section. It includes checkboxes for '上网行为管理' (Browsing Behavior Management), 'SSL VPN接入' (SSL VPN Access), **L2TP/L2TP over IPSec** (selected), 'IPSec接入' (IPSec Access), and '管理员接入' (Administrator Access). Below this is a '用户配置' (User Configuration) section with '用户所在位置' (User Location) set to '本地' (Local). A red box highlights this area. A blue box labeled '3' indicates the step '选择接入场景及认证类型' (Select access scenario and authentication type). In the '用户管理列表' (User Management List) table, a red box highlights the '新建' (New) button. A red circle labeled '4' points to the 'vpdnuser001' entry in the list. A red box highlights the '新建用户' (Create New User) dialog box. A blue box labeled '5' indicates the step '新建L2TP用户' (Create L2TP User). Inside the dialog, the '登录名' (Login Name) field contains 'vpdnuser001'. The '密码' (Password) and '确认密码' (Confirm Password) fields both contain 'Password@123'. A note below the password fields states: '密码不能和用户名相同, 长度为6~16个字符, 且密码必须包含数字、大写字母、小写字母、特殊字符中的至少3种, 如: Password@或password8#等。' (The password cannot be the same as the username, must be 6~16 characters long, and must contain at least 3 types of characters: digits, uppercase letters, lowercase letters, and special characters. Examples: Password@ or password8#). An orange callout bubble provides additional information: '本例中, 用户登录名设置为vpdnuser001, 密码设置为Password@123。' (In this example, the user login name is set to vpdnuser001, and the password is set to Password@123.). The bottom right of the dialog has '确定' (Confirm) and '取消' (Cancel) buttons.

Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step4 新建地址池

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI', 'admin', and tabs for '对象' (selected), '面板', '监控', '策略', '网络', and '系统'. The left sidebar menu is collapsed, with '地址池' highlighted. The main content area displays a table for '地址池列表' (Address Pool List) with columns for '名称' (Name), '地址池范围' (Address Pool Range), 'DNS服务器' (DNS Server), and 'NBNS服务器' (NBNS Server). A red circle labeled '1' points to the '新建' (New) button. A red circle labeled '2' points to the '地址池' (Address Pool) item in the sidebar. A red circle labeled '3' points to the '名称' (Name) input field in the '新建IP地址池' (Create IP Address Pool) dialog. A red circle labeled '4' points to a callout box containing the text: '新建名称为pool的地址池，地址池范围设置为10.1.2.2-10.1.2.100。' (Create a new address pool named 'pool', with the address pool range set to 10.1.2.2-10.1.2.100.). The dialog also contains fields for '地址池范围' (Address Pool Range) with the value '10.1.2.2-10.1.2.100' and '扩展网络属性' (Advanced Network Properties) sections for DNS and NBNS servers.

1 新建

2 地址池

3 名称

4 新建名称为pool的地址池，地址池范围设置为10.1.2.2-10.1.2.100。

Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step5 配置L2TP over IPSec

1 点击“网络”图标。

2 点击左侧菜单栏中的“IPSec”。

3 点击“新建”按钮。

4 先选择场景，然后完成基本配置。

5 选择用户地址池pool。

6 新建待加密数据流，使所有经过L2TP封装的报文都走IPSec隧道。

Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step6 创建VPN连接 (1)



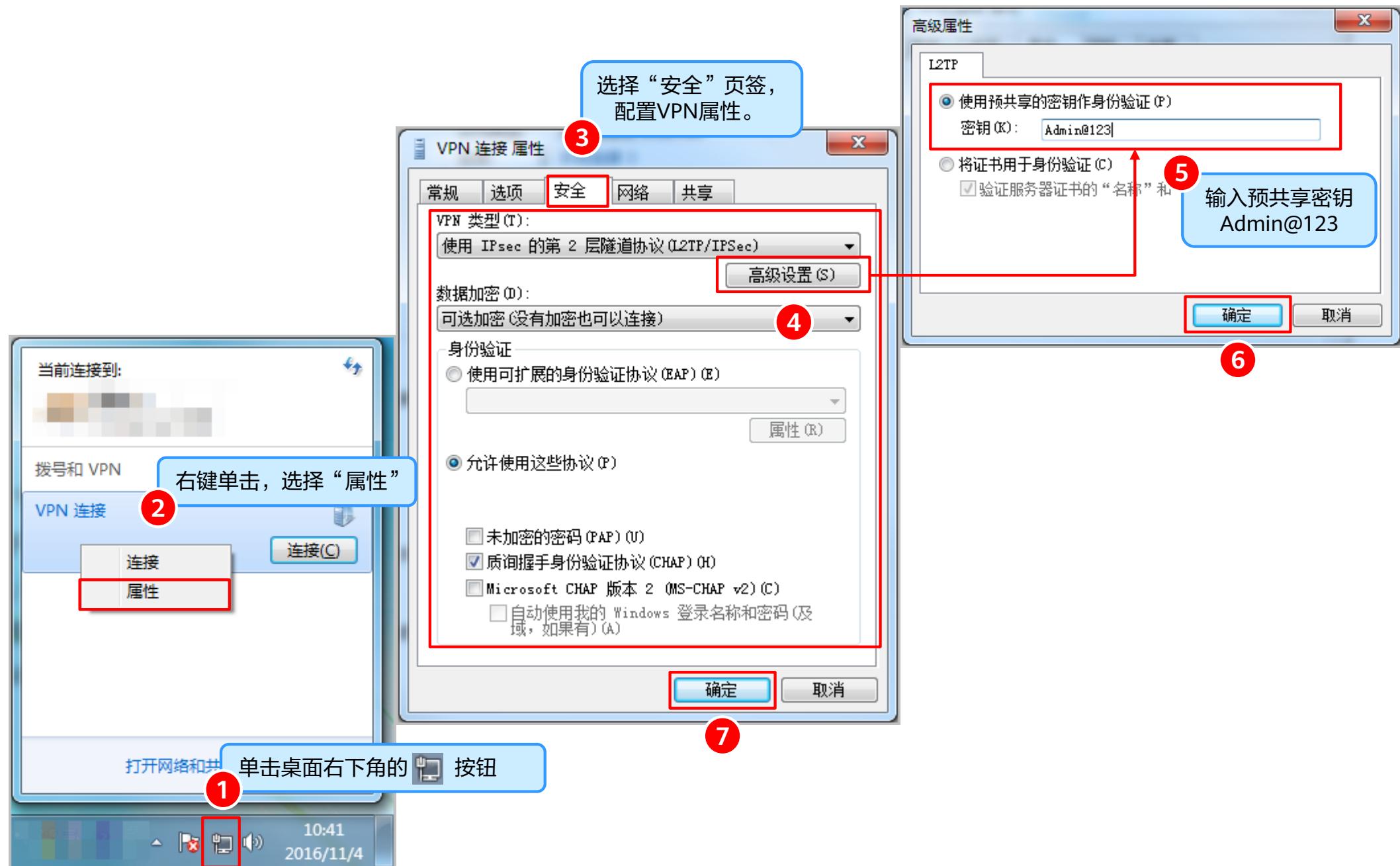
Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step6 创建VPN连接 (2)



Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step7 配置VPN属性



Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step8 结果验证 (1)



Example 9.3: 客户端 L2TP over IPSec 接入 (Windows 7)

Step8 结果验证 (2)

登录FW查看L2TP监控列表，可以看到用户已经登录成功。



L2TP通道监控列表

本端通道ID	对端通道ID 本端地址	对端地址	端口	会话数	对端名称
1	5 1.1.1.2	1.1.1.1	1701	1	l2tp_user_1

查看IPSec监控列表，可以看到IPSec隧道建立成功。

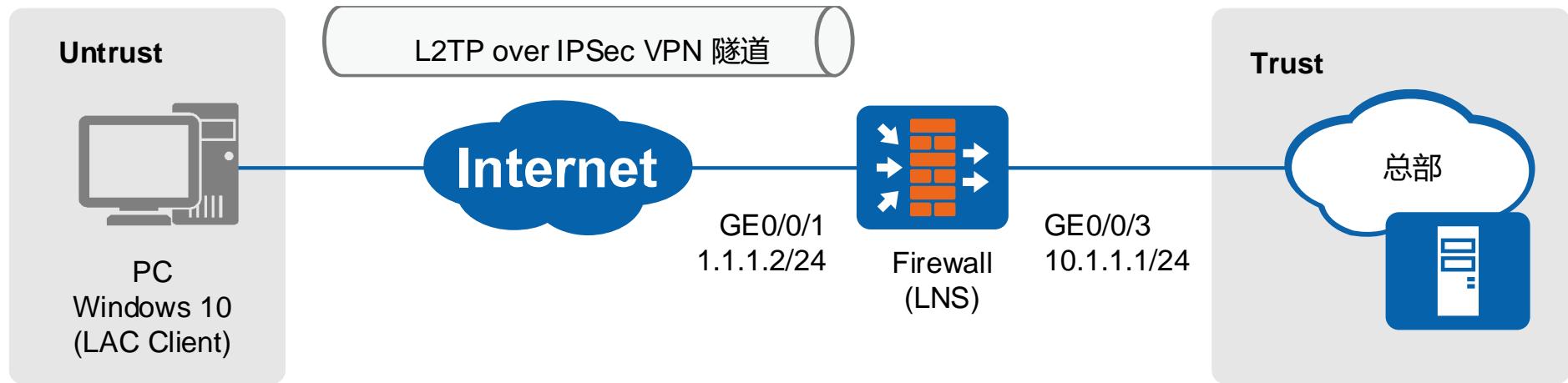


IPSec监控列表

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (...)	发送/接收速率 (...)	最近一次建立时间	最近一次断开时间	断开原因	当日断开次数
ipsec_policy	public	<input checked="" type="checkbox"/>	IKE协商成功 IPSec协商成功	1.1.1.2	1.1.1.1			ESP-3DES-SHA1	源地址[端口]: 1.1.1.2[1701] 目的地址[端口]: 1.1.1.1[1701]	69	0/0				

Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)

组网图



LAC客户端通过Internet连接到公司总部的LNS侧。出差员工使用搭载Windows 10操作系统的便携机直接向LNS侧发起连接请求，与LNS的通讯数据通过隧道Tunnel传输。先使用L2TP封装第二层数据，对身份进行认证；再使用IPSec对数据进行加密。

项目	数据	
LNS	L2TP配置	组名: default 用户名: vpdnuser 用户密码: Hello@123
	IPSec配置	预共享密钥: Admin@123 本端ID: IP地址 对端ID: 接受任意对端ID
	用户地址池pool	10.1.2.2 ~ 10.1.2.100 请确保总部设备和地址池中地址路由可达。路由下一跳指向防火墙连接总部内网的接口GE0/0/3。
LAC	L2TP配置	用户认证名称: vpdnuser 用户认证密码: Hello@123
	IPSec配置	预共享密钥: Admin@123 对端地址: 1.1.1.2/24

Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)

Step1 配置接口

1. 在左侧导航栏中选择“网络”图标。

2. 在左侧树状菜单中选择“接口”。

3. 在右侧列表中勾选“启用”复选框。

4. 在左侧树状菜单中选择“L2TP over IPSec”，进入外网接口参数配置界面。

5. 在右侧列表中勾选“启用”复选框。

6. 在左侧树状菜单中选择“IPSec”，进入内网接口参数配置界面。

修改GigabitEthernet

接口名称: GigabitEthernet0/0/1
别名:
虚拟系统: public
安全区域: untrust
模式: 路由
连接类型: 静态IP
IP地址: 1.1.1.2/24
默认网关: 1.1.1.254
首选DNS服务器: 1.1.1.1
备用DNS服务器: 1.1.1.1
多出口选项:

IPv4

连接类型: 静态IP
IP地址: 1.1.1.2/24
默认网关: 1.1.1.254
首选DNS服务器: 1.1.1.1
备用DNS服务器: 1.1.1.1
多出口选项:

接口带宽:

确定 取消

修改GigabitEthernet

接口名称: GigabitEthernet0/0/3
别名:
虚拟系统: public
安全区域: trust
模式: 路由
连接类型: 静态IP
IP地址: 10.1.1.1/24
默认网关:
首选DNS服务器:
备用DNS服务器:
多出口选项:

IPv4

连接类型: 静态IP
IP地址: 10.1.1.1/24
默认网关:
首选DNS服务器:
备用DNS服务器:
多出口选项:

接口带宽:

确定 取消

Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)

Step2 配置安全策略

1. 在 HUAWEI 网络管理界面中，进入“策略”模块。

2. 选择“安全策略”。

3. 点击“新建安全策略”。

4. 新建安全策略 policy1，配置如下：

- 名称：policy1
- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：10.1.1.0/24
- 动作：允许

允许总部服务器访问外网

5. 新建安全策略 policy2，配置如下：

- 名称：policy2
- 源安全区域：untrust
- 目的安全区域：trust
- 源地址/地区：10.1.1.0/24
- 动作：允许

允许LAC访问总部服务器

6. 新建安全策略 policy3，配置如下：

- 名称：policy3
- 源安全区域：untrust
- 目的安全区域：local
- 源地址/地区：1.1.1.2/32
- 动作：允许

允许LAC与防火墙通信

7. 新建安全策略 policy4，配置如下：

- 名称：policy4
- 源安全区域：local
- 目的安全区域：untrust
- 源地址/地区：1.1.1.2/32
- 动作：允许

允许防火墙与LAC通信

Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)

Step3 新建L2TP用户

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 保存 ...' buttons. The main menu on the left has '对象' (Object) highlighted with a red circle labeled '1'. The '用户管理' (User Management) page is displayed. A red box highlights the '场景' (Scenarios) section where 'L2TP/L2TP over IPSec' is checked. A blue box labeled '3' highlights the '选择接入场景及认证类型' (Select access scenario and authentication type) step. On the left sidebar, 'default' is selected under '认证域' (Authentication Domain). A red box labeled '4' highlights the '新建' (New) button in the user management list. A red box labeled '5' highlights the '新建L2TP用户' (Create L2TP User) step in the '新建用户' (New User) dialog. The dialog shows fields for '登录名' (Login Name) set to 'vpdnuser', '密码' (Password) set to 'Hello@123', and '确认密码' (Confirm Password) also set to 'Hello@123'. A note in the dialog specifies that the password must be at least 6-16 characters long and contain at least three types of characters (numbers, uppercase, lowercase, and special). An orange callout bubble provides example password formats: 'Password@' or 'password8#'. The bottom right of the dialog has '确定' (Confirm) and '取消' (Cancel) buttons.

3 选择接入场景及认证类型

4

5 新建L2TP用户

本例中，
用户登录名设置为vpdnuser，
密码设置为Hello@123。

Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)

Step4 新建地址池

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and tabs for '对象' (selected), '面板', '监控', '策略', '网络', and '系统'. The left sidebar menu is collapsed, with '地址池' highlighted. The main content area displays the '地址池列表' (Address Pool List) with a '新建' (Create) button. A red circle labeled '1' is on the '新建' button. A red arrow labeled '2' points to the '地址池' item in the sidebar. A red box labeled '3' highlights the '名称' (Name) field in the '新建IP地址池' (Create IP Address Pool) dialog. The dialog shows 'pool' as the name and '10.1.2.2-10.1.2.100' as the address pool range. A note on the right specifies that each row can configure an IP address range separated by a carriage return. A blue callout labeled '4' indicates that the new address pool is named 'pool' with a range of '10.1.2.2-10.1.2.100'. The bottom of the dialog has '确定' (Confirm) and '取消' (Cancel) buttons.

Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)

Step5 配置L2TP over IPSec

The screenshot shows the Huawei USG6300 network management interface. The main title is "Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10) Step5 配置L2TP over IPSec". The top navigation bar includes "admin", "提交", "保存", and "..." buttons. The left sidebar lists various network services: 接口, 接口对, 安全区域, DNS, DHCP服务器, 路由, IPSec, L2TP, L2TP over IPSec, GRE, DSVPN, and SSL VPN. The "IPSec" service is selected, indicated by a red box labeled "2". The main content area shows the "IPSec策略列表" (IPSec Policy List) and the "新建IPSec策略" (Create New IPSec Policy) dialog.

步骤 1: 在 "IPSec策略列表" 中点击 "新建" 按钮 (1)。

步骤 2: 在左侧树状菜单中选择 "IPSec" (2)。

步骤 3: 在 "新建IPSec策略" 对话框中点击 "新建" 按钮 (3)。

步骤 4: 在 "新建IPSec策略" 对话框中选择 "点到多点" 场景 (4)。提示框显示: "先选择场景, 然后完成基本配置。"

步骤 5: 在 "新建IPSec策略" 对话框中选择 "L2TP over IPSec客户端" (5)。提示框显示: "选择用户地址池pool"。下方显示预共享密钥: Admin@123。

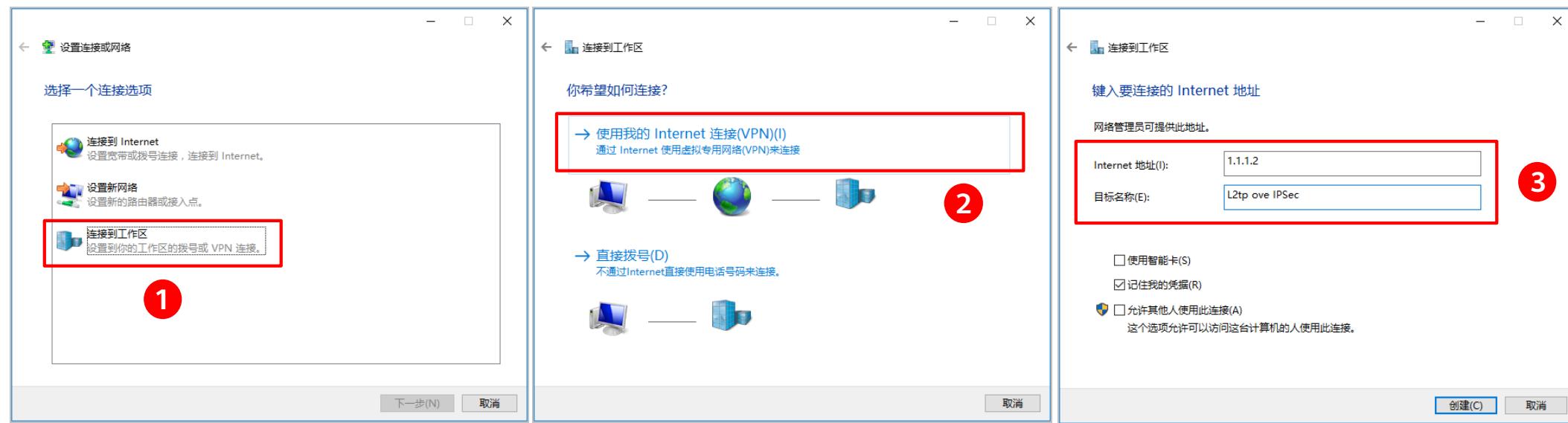
步骤 6: 在右侧的 "新建待加密的数据流" 对话框中点击 "新建" 按钮 (6)。提示框显示: "新建待加密数据流, 使所有经过L2TP封装的报文都走IPSec隧道。"

右侧对话框展示了待加密的数据流配置，包括源地址/地址组、目的地址/地址组、协议 (UDP)、源端口 (1701)、目的端口 (any) 和动作 (加密)。

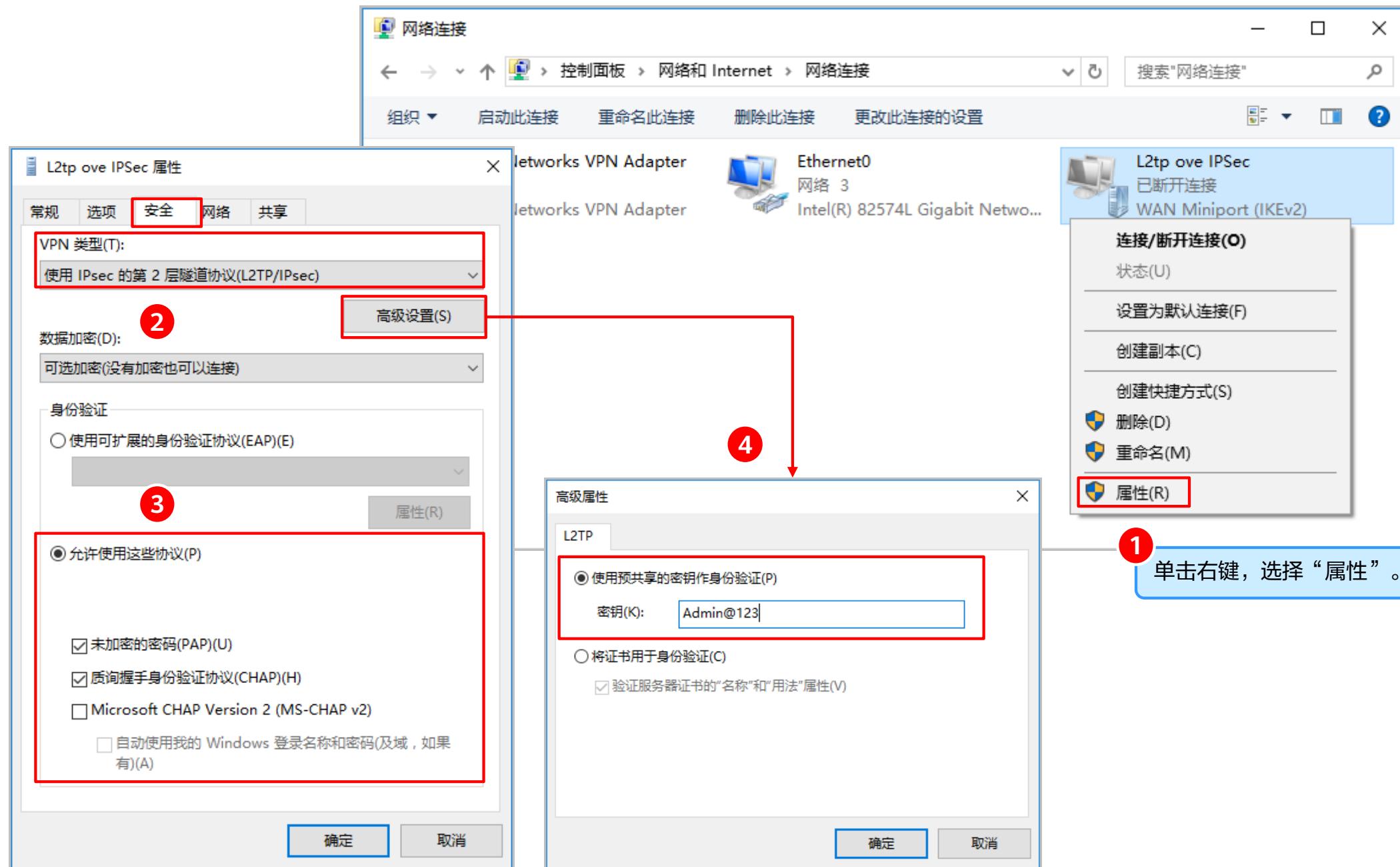
Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10) Step6 配置LAC拨号参数 (1)



Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10) Step6 配置LAC拨号参数 (2)



Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10) Step6 配置LAC拨号参数 (3)



Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)

Step7 结果验证 (1)



The screenshot shows the Windows Control Panel > Network and Internet > Network Connections window. It lists several network adapters: Array works VPN Adapter (disabled), Ethernet0 (Network 3, Intel(R) 82574L Gigabit Network Adapter), and L2tp ove IPSec (disconnected, WAN Miniport (L2TP)). A red box highlights the '启动此连接' (Start this connection) button above the list.

设置

VPN

添加 VPN 连接

L2tp ove IPSec

连接 高级选项 删除

高级选项

允许通过按流量计费的网络进行 VPN 连接 (开关: 开)

允许漫游时进行 VPN 连接 (开关: 开)

Windows 安全性

登录: vpdnuser
域:
确定

系统显示VPN已成功连接

用户名为vpdnuser，密码为Hello@123。

2 单击“连接”
3 输入用户名及密码，单击“确定”。
4 系统显示VPN已成功连接

Example 9.4: 客户端 L2TP over IPSec 接入 (Windows 10)

Step7 结果验证 (2)

登录防火墙查看L2TP监控列表，可以看到用户已经登录成功。



L2TP通道监控列表

本端通道ID	对端通道ID 本端地址	对端地址	端口	会话数	对端名称
1	5 1.1.1.2	1.1.1.1	1701	1	l2tp_user_1

查看IPSec监控列表，可以看到IPSec隧道建立成功。

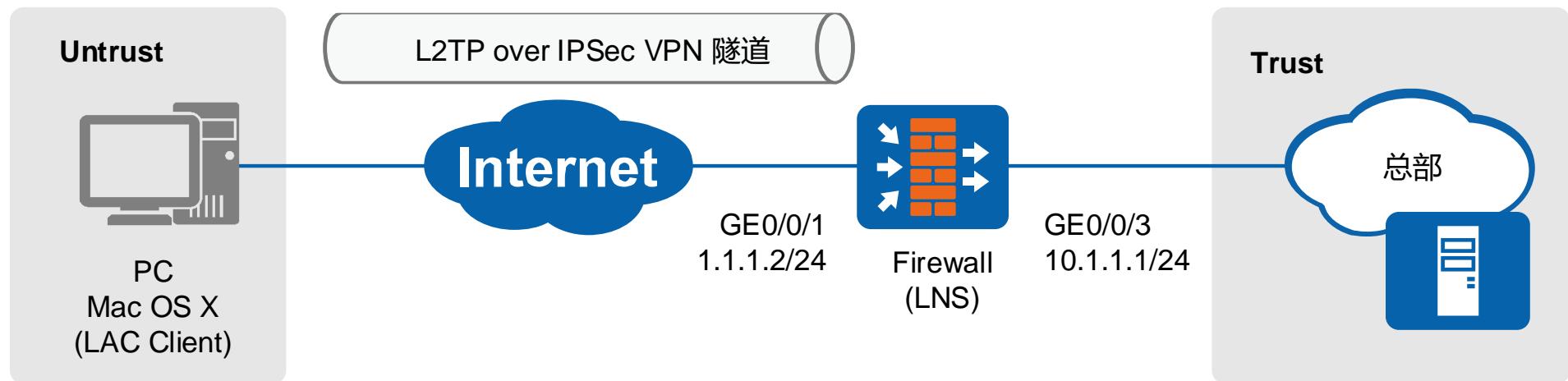


IPSec监控列表

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (... 发送/接收速率 (... 最近一次建立时间 最近一次断开时间 断开原因 当日断开次数
ipsec_policy	public		IKE协商成功 IPSec协商成功	1.1.1.2	1.1.1.1			ESP-3DES-SHA1	源地址[端口]: 1.1.1.2[1701] 目的地址[端口]: 1.1.1.1[1701] 69 0/0 协议: UDP	

Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

组网图



LAC客户端通过Internet连接到公司总部的LNS侧。出差员工使用搭载Mac OS X操作系统的便携机直接向LNS侧发起连接请求，与LNS的通讯数据通过隧道Tunnel传输。先使用L2TP封装第二层数据，对身份进行认证；再使用IPSec对数据进行加密。

项目	数据	
LNS	L2TP配置	组名: default 用户名: macuser 用户密码: Hello@123
	IPSec配置	预共享密钥: Admin@123 本端ID: IP地址 对端ID: 接受任意对端ID
	用户地址池pool	10.1.2.2 ~ 10.1.2.100 请确保总部设备和地址池中地址路由可达。路由下一跳指向防火墙连接总部内网的接口GE0/0/3。
LAC	L2TP配置	用户认证名称: macuser 用户认证密码: Hello@123
	IPSec配置	预共享密钥: Admin@123 对端地址: 1.1.1.2/24

Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step1 配置接口

1. 在左侧导航栏中选择“网络”图标。

2. 在左侧子菜单中选择“接口”。

3. 在右侧列表中勾选“启用”复选框。

4. 在左侧子菜单中选择“L2TP over IPSec”，进入外网接口参数配置界面。

5. 在右侧列表中勾选“启用”复选框。

6. 在左侧子菜单中选择“IPSec”，进入内网接口参数配置界面。

修改GigabitEthernet (Left Panel - Outer Network Interface Configuration)

- 接口名称: GigabitEthernet0/0/1
- 别名:
- 虚拟系统: public
- 安全区域: untrust
- 模式: 路由
- IPv4:
 - 连接类型: 静态IP
 - IP地址: 1.1.1.2/24
 - 默认网关: 1.1.1.254
 - 首选DNS服务器:
 - 备用DNS服务器:
 - 多出口选项

修改GigabitEthernet (Right Panel - Inner Network Interface Configuration)

- 接口名称: GigabitEthernet0/0/3
- 别名:
- 虚拟系统: public
- 安全区域: trust
- 模式: 路由
- IPv4:
 - 连接类型: 静态IP
 - IP地址: 10.1.1.2/24
 - 默认网关:
 - 首选DNS服务器:
 - 备用DNS服务器:
 - 多出口选项

Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step2 配置安全策略

1. 在 HUAWEI 网络管理界面中，进入“策略”模块。

2. 选择“安全策略”。

3. 点击“新建安全策略”。

4. 新建安全策略 policy1，配置如下：

- 名称：policy1
- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：10.1.1.0/24
- 动作：允许

说明：允许总部服务器访问外网。

5. 新建安全策略 policy2，配置如下：

- 名称：policy2
- 源安全区域：untrust
- 目的安全区域：trust
- 源地址/地区：10.1.1.0/24
- 动作：允许

说明：允许 LAC 访问总部服务器。

6. 新建安全策略 policy3，配置如下：

- 名称：policy3
- 源安全区域：untrust
- 目的安全区域：local
- 源地址/地区：1.1.1.2/32
- 动作：允许

说明：允许 LAC 与防火墙通信。

7. 新建安全策略 policy4，配置如下：

- 名称：policy4
- 源安全区域：local
- 目的安全区域：untrust
- 源地址/地区：1.1.1.2/32
- 动作：允许

说明：允许防火墙与 LAC 通信。

Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step3 新建L2TP用户

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 保存 ...' buttons. The main menu on the left lists categories like '证书', '地址', '地区', '服务', '应用', and '用户'. Under '用户', 'default' is selected. The top right has tabs for '对象' (selected), '策略', '网络', and '系统'. The central area is titled '用户管理' (User Management) and shows a '场景' (Scenario) section with checkboxes for '上网行为管理', 'SSL VPN接入', 'L2TP/L2TP over IPSec' (which is checked), 'IPSec接入', and '管理员接入'. Below this is a '用户配置' (User Configuration) section with '用户所在位置' set to '本地' (Local). A red box highlights this configuration area with the number '1'. To the right, a blue box labeled '3 选择接入场景及认证类型' (Select access scenario and authentication type) points to the 'L2TP/L2TP over IPSec' checkbox.

In the middle section, there's a '用户管理列表' (User Management List) table with columns '名称' (Name) and '描述' (Description). A red box highlights the '新建' (New) button in the toolbar above the table, with the number '2'. A red arrow points from this button down to a '新建用户' (Create User) dialog box. This dialog box contains fields for '登录名' (Login Name) set to 'macuser', '显示名' (Display Name), '描述' (Description), '密码' (Password) set to 'Hello@123', and '确认密码' (Confirm Password) also set to 'Hello@123'. A red box highlights this form with the number '4'. To the right of the dialog, a yellow callout bubble states: '本例中, 用户登录名设置为macuser, 密码设置为Hello@123。' (In this example, the user login name is set to macuser, and the password is set to Hello@123.). A blue box labeled '5 新建L2TP用户' (Create L2TP User) points to the '确定' (Confirm) button at the bottom right of the dialog.

Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step4 新建地址池

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI', 'admin', and tabs for '对象' (Object), '面板' (Panel), '监控' (Monitoring), '策略' (Policy), '网络' (Network), and '系统' (System). The '对象' tab is highlighted with a red box and a circled '1'. On the left sidebar, under the '地址池' (Address Pool) section, the '新建' (Create) button is highlighted with a red box and circled '2'. A red arrow points from the '新建' button to the '新建IP地址池' (Create IP Address Pool) dialog box. Inside the dialog box, the '名称' (Name) field contains 'pool' and the '地址池范围' (Address Pool Range) field contains '10.1.2.2-10.1.2.100'. A note on the right side of the dialog box states: '每行可配置一个IP地址/范围，行之间用回车分隔，示例：110.10.1.2 10.10.1.2-10.10.1.10' (A line can configure one IP address/range, separated by carriage return, example: 110.10.1.2 10.10.1.2-10.10.1.10). A blue callout box with circled '4' contains the text: '新建名称为pool的地址池，地址池范围设置为10.1.2.2-10.1.2.100。' (Create a new address pool named 'pool', and set the address pool range to 10.1.2.2-10.1.2.100.). At the bottom of the dialog box are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step5 配置L2TP over IPSec

1 点击“网络”图标。

2 在左侧树状菜单中，选择“IPSec”下的“IPSec”。

3 点击“新建”按钮。

4 先选择场景，然后完成基本配置。

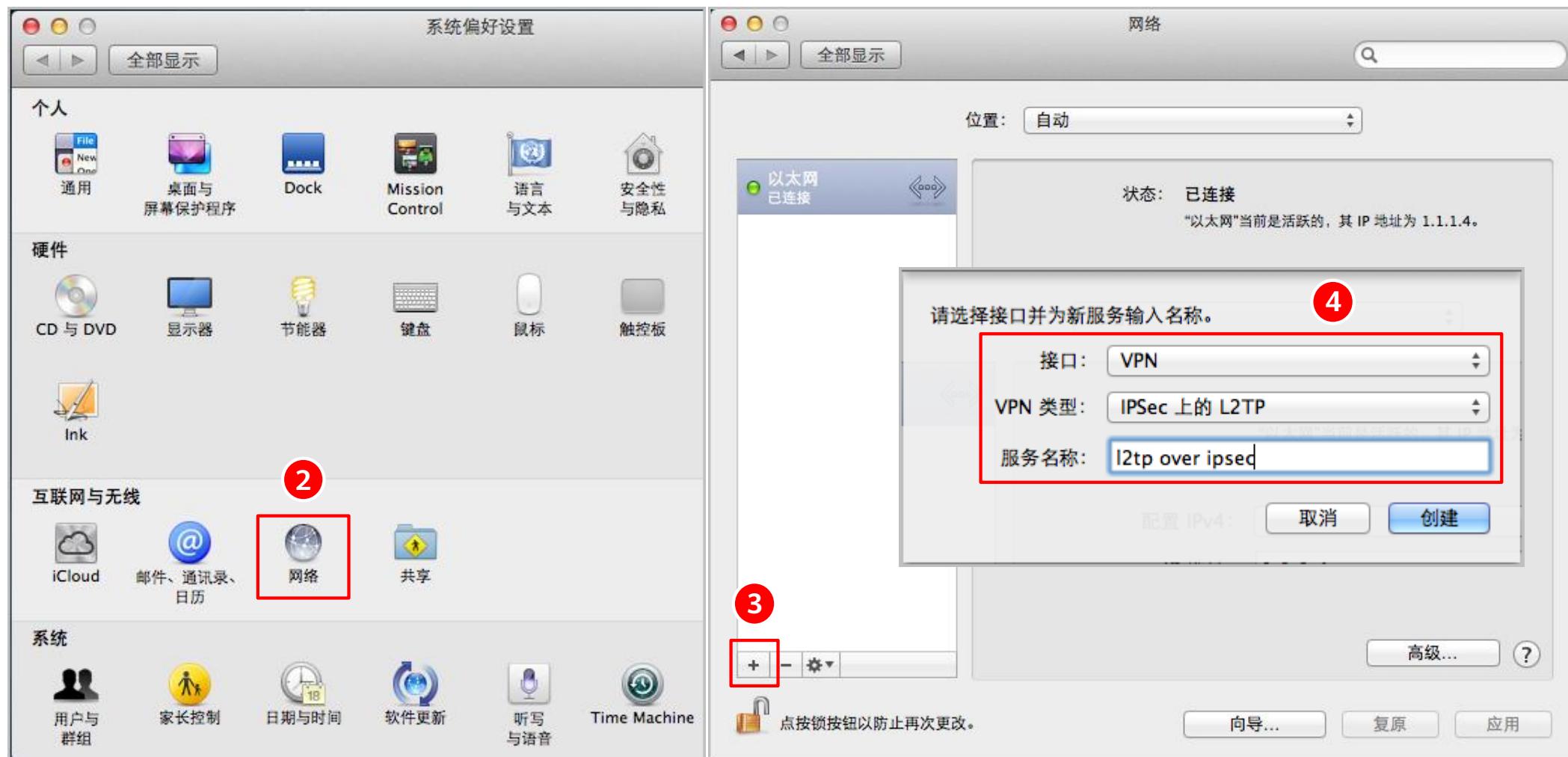
5 选择用户地址池pool。

6 新建待加密数据流，使所有经过L2TP封装的报文都走IPSec隧道。

The screenshot shows the Huawei USG6300 network management interface. The main window displays the 'IPSec策略列表' (IPSec Policy List) with a red box around the '新建' (New) button. Step 1 highlights the 'Network' icon in the top navigation bar. Step 2 highlights the 'IPSec' section in the left sidebar. Step 3 highlights the 'New' button in the policy list. Step 4 is a callout pointing to the 'Scene' selection in the 'Create IPSec Policy' dialog, which is set to 'Point-to-Multipoint'. Step 5 highlights the 'User Address Pool' dropdown in the 'Dial-up User Configuration' section, which is set to 'pool'. Step 6 highlights the 'New' button in the 'New Encrypted Traffic Flow' dialog.

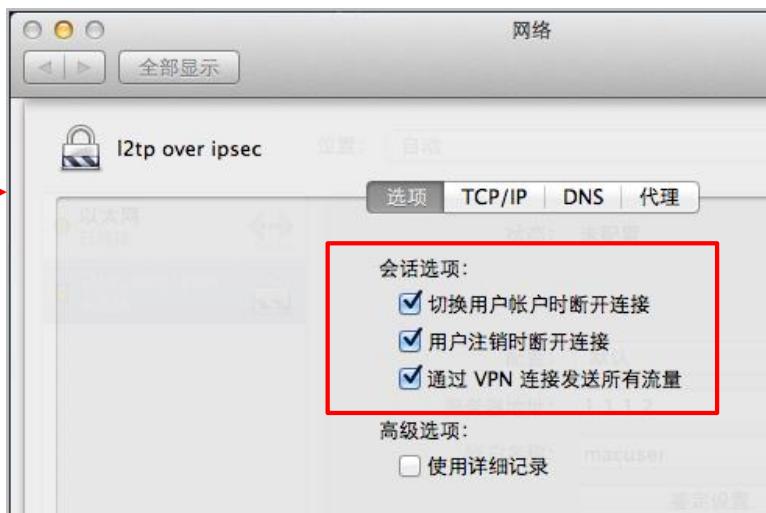
Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step6 配置LAC拨号参数 (1)



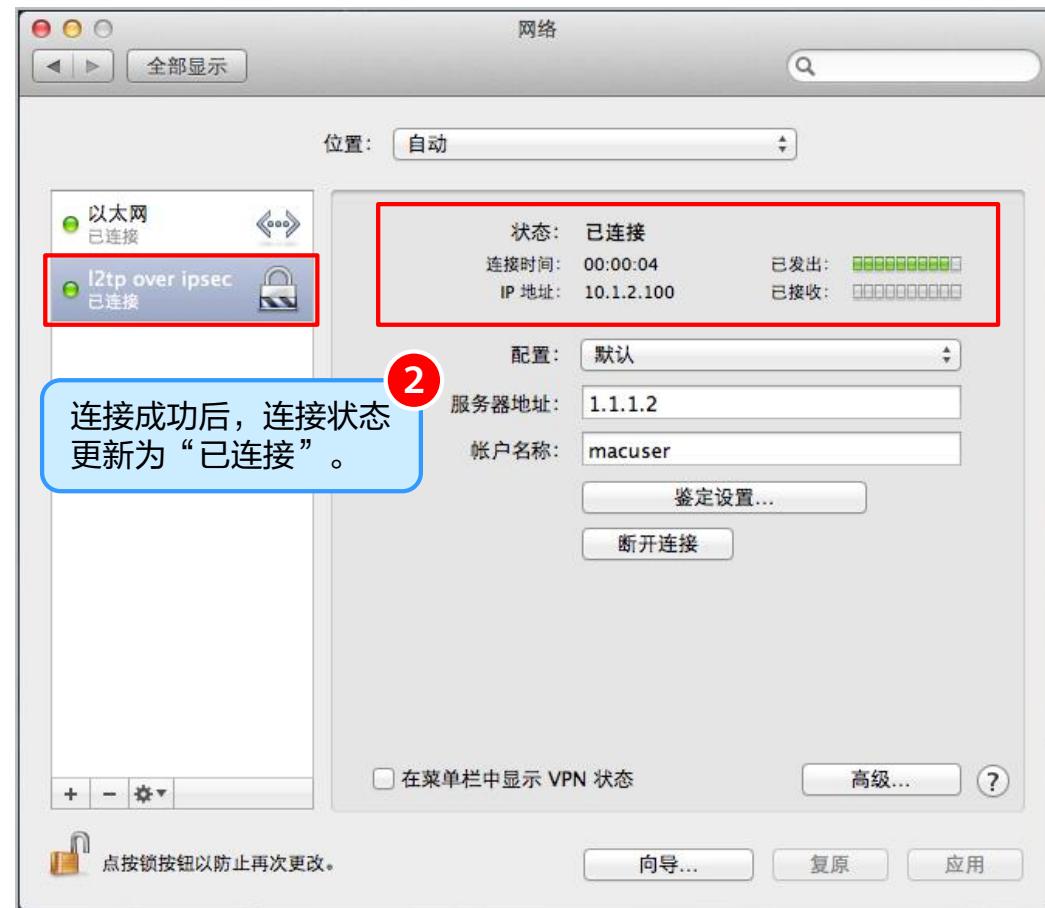
Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step6 配置LAC拨号参数 (2)



Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step7 结果验证 (1)



Example 9.5: 客户端 L2TP over IPSec 接入 (Mac OS X)

Step7 结果验证 (2)

登录防火墙查看L2TP监控列表，可以看到用户已经登录成功。



L2TP通道监控列表

本端通道ID	对端通道ID 本端地址	对端地址	端口	会话数	对端名称
1	5 1.1.1.2	[REDACTED]	1701	1	[REDACTED]

查看IPSec监控列表，可以看到IPSec隧道建立成功。

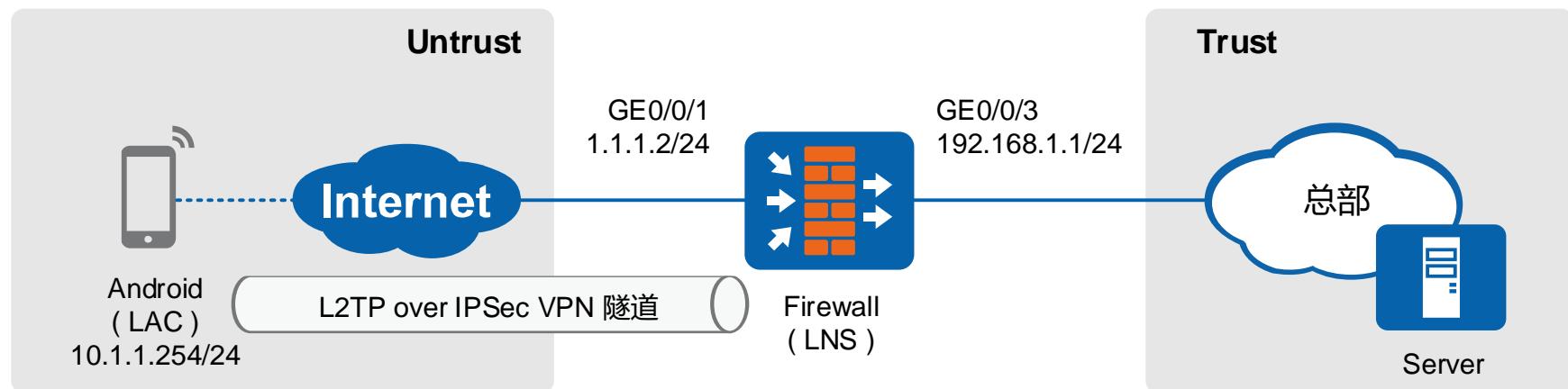


IPSec监控列表

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (... 发送/接收速率 (... 最近一次建立时间 最近一次断开时间 断开原因 当日断开次数
ipsec_policy	public		IKE协商成功	1.1.1.2	[REDACTED]			ESP-3DES-SHA1	源地址[端口]: 1.1.1.2[1701] 目的地址[端口]: [REDACTED][61861] 69 协议: UDP	0/0

Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

组网图



LAC客户端通过Internet连接到公司总部的LNS侧。出差员工使用搭载Android操作系统的手机（LAC）直接向LNS侧发起连接请求，与LNS的通讯数据通过隧道Tunnel传输。先使用L2TP封装第二层数据，对身份进行认证；再使用IPSec对数据进行加密。

项目		数据
LNS	L2TP配置	组名: default 用户名: vpdnuser 用户密码: Hello@123
	IPSec配置	预共享密钥: Admin@123 本端ID: IP地址 对端ID: 接受任意对端ID
	用户地址池	100.1.1.2 ~ 100.1.1.100 请确保总部设备和地址池中地址路由可达，路由下一跳指向防火墙连接总部内网的接口GE0/0/3。
LAC	IP地址	10.1.1.254/24
	L2TP配置	用户认证名称: vpdnuser 用户认证密码: Hello@123
	IPSec配置	预共享密钥: Admin@123 对端地址: 1.1.1.2/24

Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

Step1 配置接口

1. 在左侧导航栏中选择“网络”图标。

2. 在左侧子菜单中选择“接口”。

3. 在右侧列表中找到外网接口 GE0/0/1，将其启用并配置参数。

4. 在右侧列表中找到内网接口 GE0/0/3，将其启用并配置参数。

5. 在右侧列表中找到内网接口 GE0/0/2，将其启用并配置参数。

6. 在右侧列表中找到内网接口 GE0/0/0，将其启用并配置参数。

修改GigabitEthernet

接口名称: GigabitEthernet0/0/1 *别名:

虚拟系统: public *安全区域: untrust

模式: 路由

IPv4

连接类型: 静态IP

IP地址: 1.1.1.2/24

默认网关:

首选DNS服务器:

备用DNS服务器:

多出口选项

接口带宽:

确定 **取消**

修改GigabitEthernet

接口名称: GigabitEthernet0/0/3 *别名:

虚拟系统: public *安全区域: trust

模式: 路由

IPv4

连接类型: 静态IP

IP地址: 192.168.1.1/24

默认网关:

首选DNS服务器:

备用DNS服务器:

多出口选项

接口带宽:

确定 **取消**

Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

Step2 配置安全策略

1. 在 HUAWEI 网络管理界面中，进入“策略”模块。

2. 选择“安全策略”。

3. 点击“新建安全策略”。

4. 新建安全策略 policy1，配置如下：

- 名称：policy1
- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：192.168.1.0/24
- 动作：允许

允许总部服务器访问外网

5. 新建安全策略 policy2，配置如下：

- 名称：policy2
- 源安全区域：untrust
- 目的安全区域：trust
- 源地址/地区：192.168.1.0/24
- 动作：允许

允许LAC访问总部服务器

6. 新建安全策略 policy3，配置如下：

- 名称：policy3
- 源安全区域：untrust
- 目的安全区域：local
- 源地址/地区：1.1.1.2/32
- 动作：允许

允许LAC与防火墙通信

7. 新建安全策略 policy4，配置如下：

- 名称：policy4
- 源安全区域：local
- 目的安全区域：untrust
- 源地址/地区：1.1.1.2/32
- 动作：允许

允许防火墙与LAC通信

Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

Step3 配置L2TP用户

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 保存 ...' buttons. The main menu on the left lists categories like '证书', '地址', '地区', '服务', '应用', and '用户'. Under '用户', 'default' is selected. The top right has tabs for '对象' (selected), '策略', '网络', and '系统'. The central area is titled '用户管理' (User Management) under '对象'.

步骤 1: 在 '对象' 标签下，选择 'L2TP/L2TP over IPSec' 场景。图中显示 'L2TP/L2TP over IPSec' 前的复选框被选中。

步骤 2: 在左侧 '用户' 菜单下，选择 'default'。

步骤 3: 在 '用户管理' 页面上，选择接入场景及认证类型。图中显示 'L2TP/L2TP over IPSec' 前的复选框被选中。

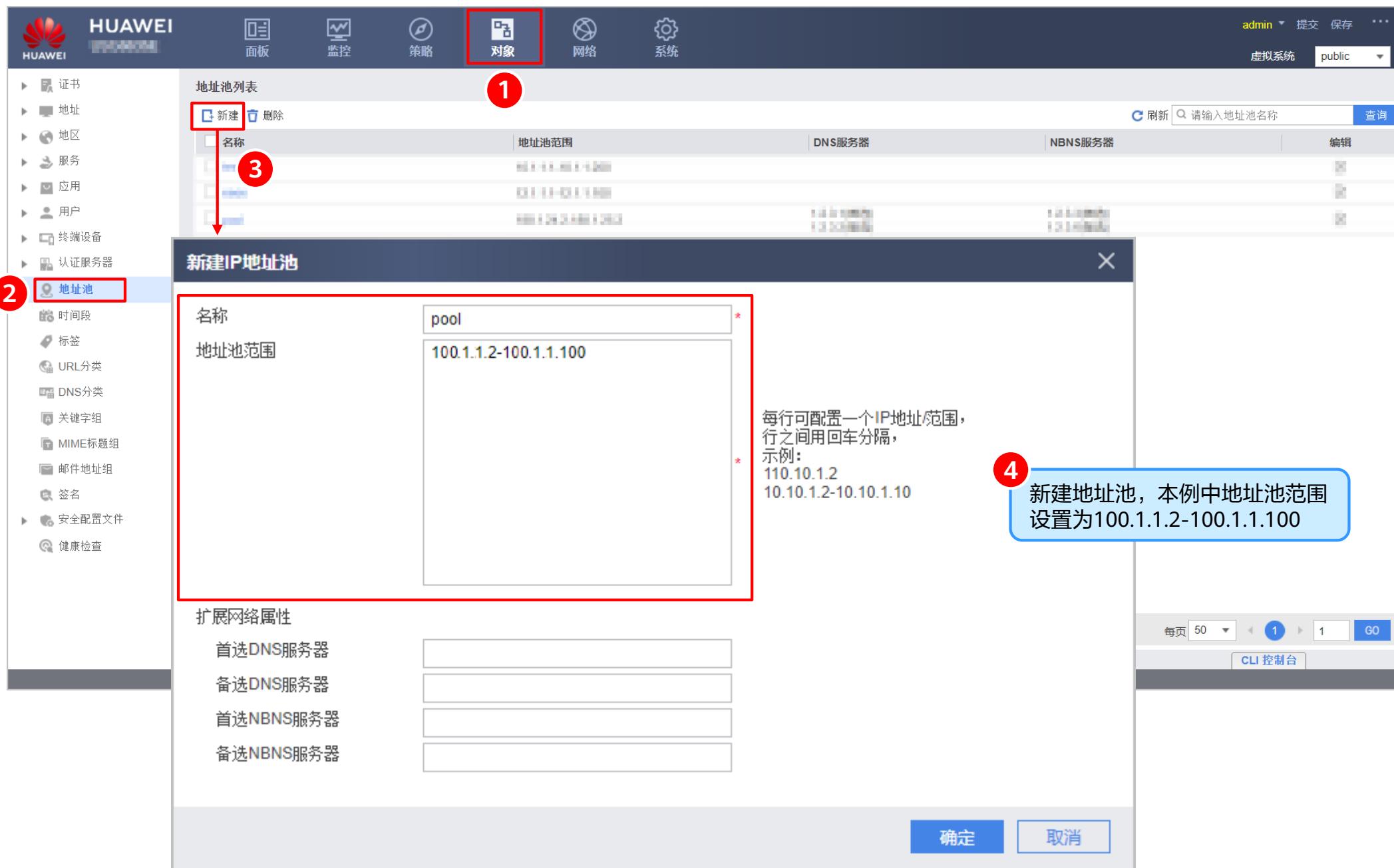
步骤 4: 在 '用户管理列表' 中，点击 '新建' 按钮。

步骤 5: 在 '新建用户' 对话框中，输入用户名 'vpdnuser'，密码 'Hello@123'，并确认。对话框内有提示：密码不能和用户名相同，长度为6~16个字符，且密码必须包含数字、大写字母、小写字母、特殊字符中的至少3种，如： Password@或password8#等。

右侧有一个黄色气泡框说明：本例中，用户登录名设置为 vpdnuser，密码设置为 Hello@123。

Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

Step4 新建地址池



The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes icons for Home, Panel, Monitoring, Policies, Objects (highlighted with a red box and labeled 1), Networks, and Systems. The top right corner shows the user is logged in as 'admin' with options to submit, save, and exit. A dropdown menu for 'Virtual System' is open, showing 'public'. The left sidebar contains links for Certificates, Addresses, Regions, Services, Applications, Users, Terminal Devices, and Authentication Servers. The 'Address Pool' link is highlighted with a red box and labeled 2.

The main content area displays the 'Address Pool List' page. It features a search bar at the top right and a table with columns for Address Pool Range, DNS Server, and NBNS Server. A 'New' button is highlighted with a red box and labeled 1. Below the table, a 'Create New IP Address Pool' dialog box is open. The dialog has a red border and contains fields for 'Name' (set to 'pool') and 'Address Pool Range' (set to '100.1.1.2-100.1.1.100'). A note on the right side of the dialog says: '每行可配置一个IP地址/范围，行之间用回车分隔，示例：110.10.1.2 10.10.1.2-10.10.1.10' (A line can contain one IP address/range, separated by carriage return, example: 110.10.1.2 10.10.1.2-10.10.1.10). A blue callout box labeled 4 indicates: '新建地址池，本例中地址池范围设置为100.1.1.2-100.1.1.100' (Create address pool, in this example, the address pool range is set to 100.1.1.2-100.1.1.100). The bottom of the dialog has 'Confirm' and 'Cancel' buttons.

Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

Step5 配置L2TP over IPSec

1 点击“网络”图标。

2 点击左侧菜单栏中的“IPSec”。

3 点击“新建”按钮。

4 先选择场景，然后完成基本配置。

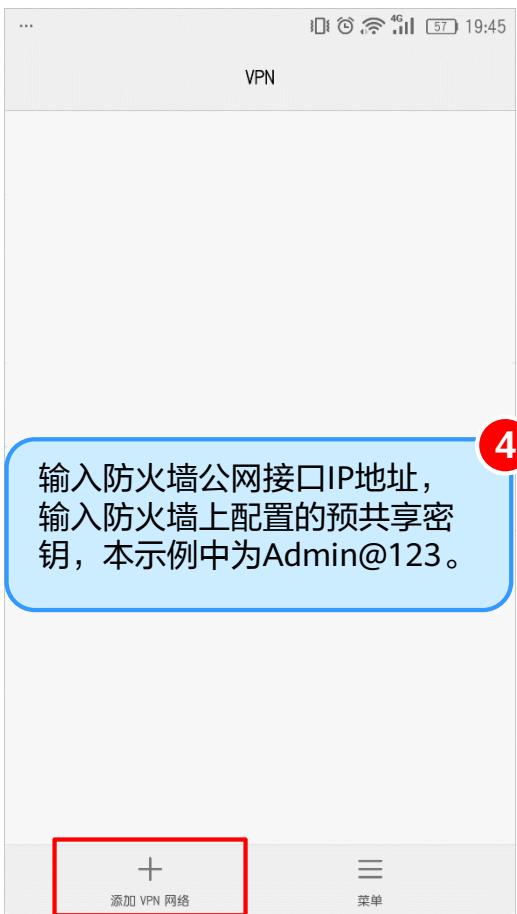
5 选择用户地址池pool。

6 新建待加密数据流，使所有经过L2TP封装的报文都走IPSec隧道。

Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

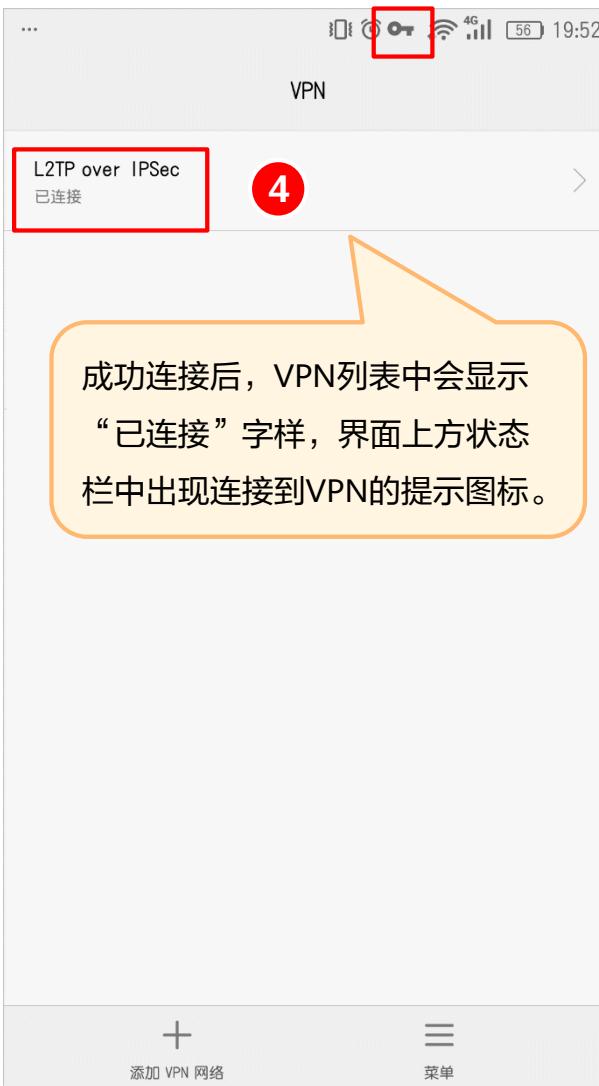
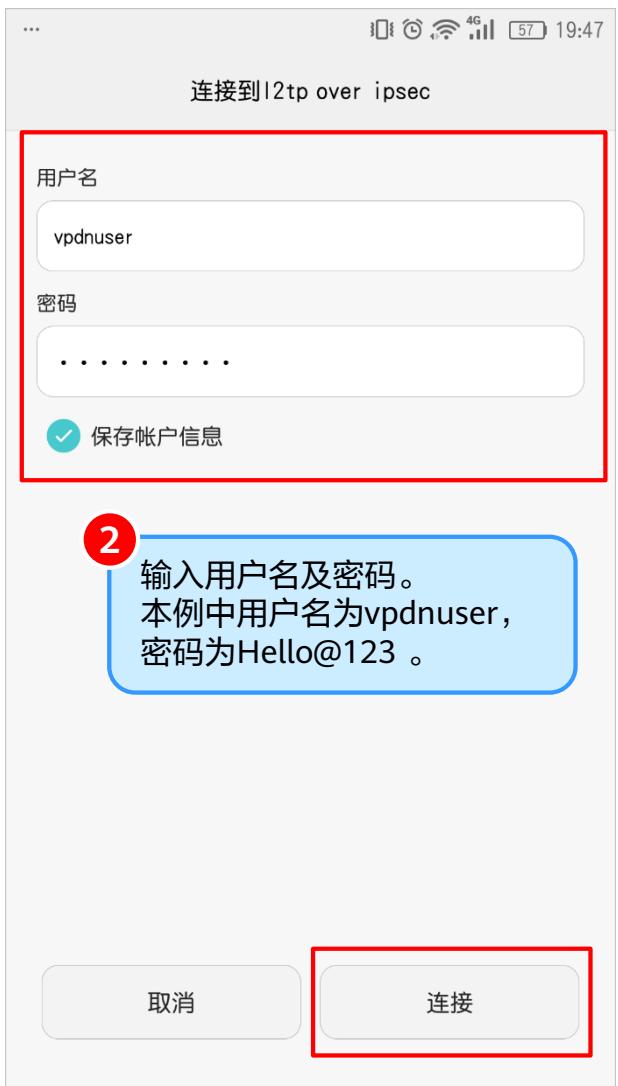
Step6 配置LAC的拨号参数

本例中使用的Android版本为Android6.0



Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

Step7 结果验证 (1)



3 确认输入无误后,
点击“连接”。

Example 9.6: 客户端 L2TP over IPSec 接入 (Android)

Step7 结果验证 (2)

在防火墙上可查看到IPSec隧道监控信息



The screenshot shows the Huawei firewall's configuration interface. The left sidebar navigation includes: 接口, 接口对, 安全区域, DNS, DHCP服务器, 路由, IPsec (selected), L2TP, and L2TP over IPSec. The top menu bar has tabs: 面板, 监控 (selected), 对象, 网络, and 系统. On the right, there are user roles (admin, public), system status (提交, 保存, ...), and virtual system selection (public). The main content area is titled 'IPSec监控列表' (IPSec Tunnel Monitoring List). It displays a table with columns: 策略名称 (Policy Name), IKE用户描述 (IKE User Description), 虚拟系统 (Virtual System), 状态 (Status), 本端地址 (Local Address), 对端地址 (Remote Address), 对端ID类型 (Remote ID Type), 对端ID内容 (Remote ID Content), 算法 (Algorithm), 协商数据流 (Negotiated Data Flow), 持续时间 (Duration), 发送/接收速率 (Send/Receive Rate), 最近一次建立时间 (Last Connection Time), 最近一次断开时间 (Last Disconnect Time), 断开原因 (Disconnect Reason), and 当日断开次数 (Daily Disconnect Count). A specific row is highlighted with a red box: 'ipsec_policy' (策略名称), 'public' (虚拟系统), 'IKE协商成功' (IKE协商成功), '1.1.1.2' (本端地址), '...' (对端地址), 'IPSec协商成功' (IPSec协商成功), 'ESP-AES-256-SHA2-256' (算法), '源地址[端口]: 1.1.1.2[1701]' (协商数据流), '目的地址[端口]: ...[0-65535] 69' (持续时间), '0/0' (发送/接收速率), '...' (最近一次建立时间), '...' (最近一次断开时间), '...' (断开原因), and '...' (当日断开次数).

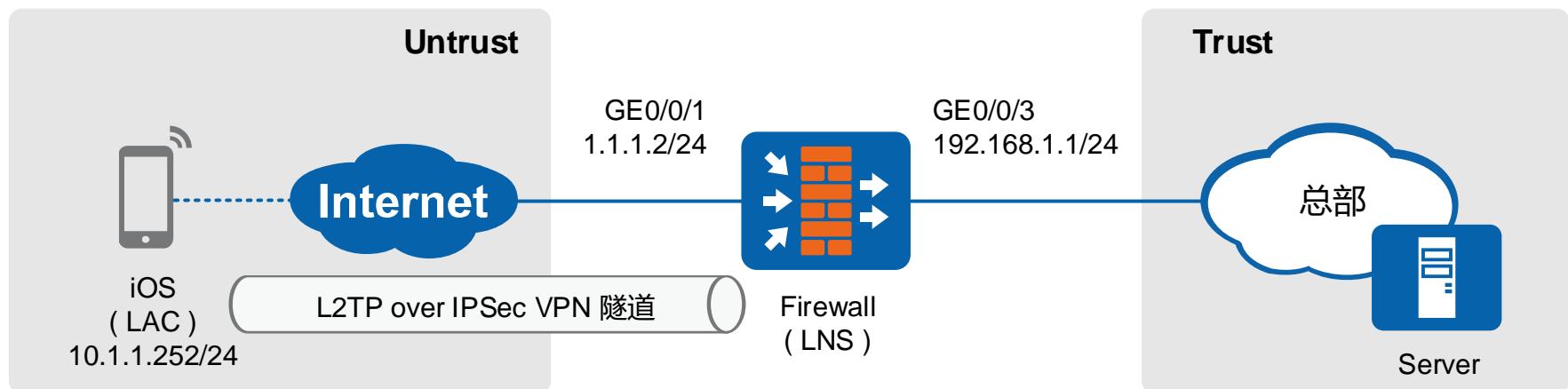
在防火墙上可查看到L2TP通道监控信息



The screenshot shows the Huawei firewall's configuration interface. The left sidebar navigation includes: 接口, 接口对, 安全区域, DNS, DHCP服务器, 路由, IPsec, L2TP (selected), and L2TP over IPSec. The top menu bar has tabs: 面板, 监控 (selected), 对象, 网络, and 系统. On the right, there are user roles (admin, public), system status (提交, 保存, ...), and virtual system selection (public). The main content area is titled 'L2TP通道监控列表' (L2TP Tunnel Monitoring List). It displays a table with columns: 切断 (Disconnect), 切断所有 (Disconnect All), 本地通道ID (Local Tunnel ID), 远端通道ID | 本地地址 (Remote Tunnel ID | Local Address), 远端地址 (Remote Address), 端口 (Port), 会话数 (Session Count), and 对端名称 (Peer Name). A specific row is highlighted with a red box: '1' (本地通道ID), '5' (远端通道ID), '1.1.1.2' (本地地址), '...' (远端地址), '1701' (端口), '1' (会话数), and 'Android' (对端名称).

Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

组网图



LAC客户端通过Internet连接到公司总部的LNS侧。出差员工使用搭载iOS操作系统的手机（LAC）直接向LNS侧发起连接请求，与LNS的通讯数据通过隧道Tunnel传输。先使用L2TP封装第二层数据，对身份进行认证；再使用IPSec对数据进行加密。

项目	数据
LNS	L2TP配置 组名: default 用户名: vpdnuser 用户密码: Hello@123
	IPSec配置 预共享密钥: Admin@123 本端ID: IP地址 对端ID: 接受任意对端ID
	用户地址池 100.1.1.2 ~ 100.1.1.100 请确保总部设备和地址池中地址路由可达，路由下一跳指向防火墙连接总部内网的接口GE0/0/3。
LAC	IP地址 10.1.1.252/24
	L2TP配置 用户认证名称: vpdnuser 用户认证密码: Hello@123
	IPSec配置 预共享密钥: Admin@123 对端地址: 1.1.1.2/24

Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

Step1 配置接口

1 网络

2 接口

3 启用

4 配置外网接口参数

5

6 配置内网接口参数

接口名称	安全区域	虚拟系统	IP地址	连接类型	VLAN	模式	状态	物理 IPv4	IPv6	启用
GE0/0/0(GE0/MGMT)										3
GE0/0/1										5
GE0/0/2										5
GE0/0/3										5
GE0/0/4										5
GE0/0/5										5
GE0/0/6										5

修改GigabitEthernet

接口名称: GigabitEthernet0/0/1

别名:

虚拟系统: public

安全区域: untrust

模式: 路由

IPv4

连接类型: 静态IP

IP地址: 1.1.1.2/24

默认网关:

首选DNS服务器:

备用DNS服务器:

多出口选项

修改GigabitEthernet

接口名称: GigabitEthernet0/0/3

别名:

虚拟系统: public

安全区域: trust

模式: 路由

IPv4

连接类型: 静态IP

IP地址: 192.168.1.1/24

默认网关:

首选DNS服务器:

备用DNS服务器:

多出口选项

Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

Step2 配置安全策略

1. 在 HUAWEI 网络管理界面中，进入“策略”模块。

2. 选择“安全策略”。

3. 点击“新建安全策略”。

4. 新建安全策略 policy1，配置如下：

- 名称：policy1
- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：192.168.1.0/24
- 动作：允许

允许总部服务器访问外网

5. 新建安全策略 policy2，配置如下：

- 名称：policy2
- 源安全区域：untrust
- 目的安全区域：trust
- 源地址/地区：192.168.1.0/24
- 动作：允许

允许 LAC 访问总部服务器

6. 新建安全策略 policy3，配置如下：

- 名称：policy3
- 源安全区域：untrust
- 目的安全区域：local
- 源地址/地区：1.1.1.2/32
- 动作：允许

允许 LAC 与防火墙通信

7. 新建安全策略 policy4，配置如下：

- 名称：policy4
- 源安全区域：local
- 目的安全区域：untrust
- 源地址/地区：1.1.1.2/32
- 动作：允许

允许防火墙与 LAC 通信

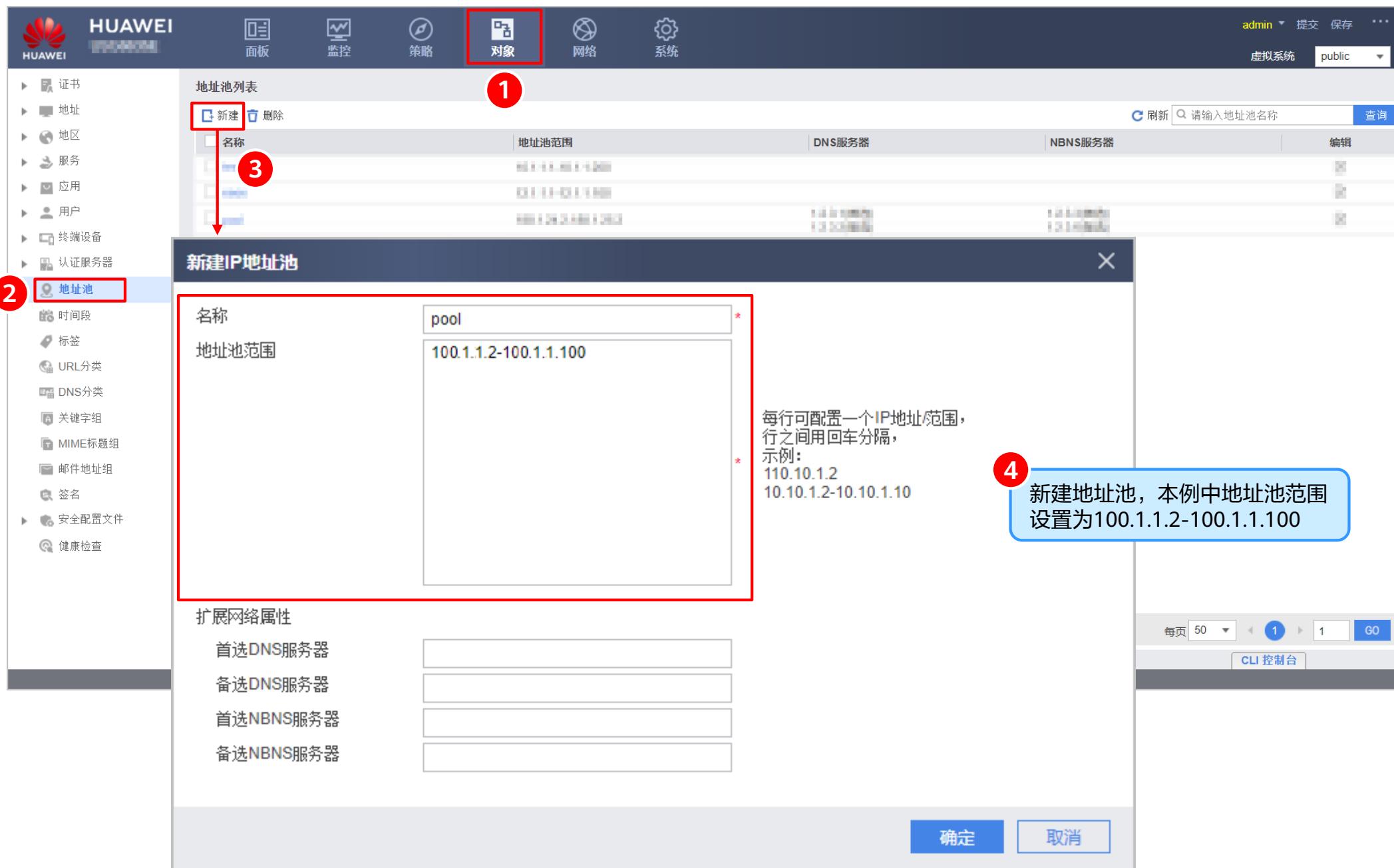
Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

Step3 配置L2TP用户

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 保存 ...' buttons. The main menu on the left lists categories like '证书', '地址', '地区', '服务', '应用', and '用户'. The '对象' (Objects) icon is highlighted with a red circle and labeled '1'. The '用户管理' (User Management) page is displayed. A red box highlights the '场景' (Scenarios) section, which includes '上网行为管理', 'SSL VPN接入', 'L2TP/L2TP over IPSec' (checked), 'IPSec接入', and '管理员接入'. Below it, '用户所在位置' is set to '本地' (Local). A blue box labeled '2' highlights the 'default' tab under '认证域' (Authentication Domains). A red box labeled '3' highlights the '选择接入场景及认证类型' (Select access scenario and authentication type) step. A red box labeled '4' highlights the '新建' (New) button in the user management list. A red box labeled '5' highlights the '新建L2TP用户' (Create L2TP User) step in the '新建用户' (New User) dialog box. An orange callout bubble provides example values: '用户名设置为vpdnuser，密码设置为Hello@123。' (Username is set to vpdnuser, password is set to Hello@123.). The '新建用户' dialog contains fields for '登录名' (Login Name: vpdnuser), '显示名' (Display Name), '描述' (Description), '密码' (Password: masked), and '确认密码' (Confirm Password: masked). A note below the password field states: '密码不能和用户名相同, 长度为6~16个字符, 且密码必须包含数字、大写字母、小写字母、特殊字符中的至少3种, 如: Password@或password8#等。' (The password cannot be the same as the username, length is 6~16 characters, and the password must contain at least 3 types of characters: digits, uppercase letters, lowercase letters, and special characters. Examples: Password@ or password8#). The bottom right of the dialog has '确定' (Confirm) and '取消' (Cancel) buttons.

Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

Step4 新建地址池



The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes icons for Home, Panel, Monitoring, Policies, Objects (highlighted with a red box and labeled 1), Networks, and Systems. The top right corner shows the user is logged in as 'admin' with options to submit, save, and exit. A dropdown menu indicates the current virtual system is 'public'. The left sidebar lists various management categories, with 'Address Pool' selected and highlighted with a red box and labeled 2. The main content area displays the 'Address Pool List' screen. It features a 'Create' button (labeled 3) and a search bar. Below the search bar are tabs for 'Address Pool Range', 'DNS Server', and 'NBNS Server'. A large modal window titled 'Create IP Address Pool' is open. Inside the modal, the 'Name' field is filled with 'pool' (marked with a red box and labeled 4). The 'Address Pool Range' field contains the value '100.1.1.2-100.1.1.100'. A note on the right side of the modal provides instructions: 'Each row can configure one IP address range, separated by a carriage return, for example: 110.10.1.2, 10.10.1.2-10.10.1.10'. At the bottom of the modal are 'Confirm' and 'Cancel' buttons.

Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

Step5 配置L2TP over IPSec

1 点击“网络”图标。

2 在左侧树状菜单中，选择“IPSec”下的“IPSec”。

3 点击“新建”按钮。

4 先选择场景，然后完成基本配置。

5 选择用户地址池pool。

6 新建待加密数据流，使所有经过L2TP封装的报文都走IPSec隧道。

先选择场景，然后完成基本配置。

新建待加密的数据流

用来指定需要IPSec加密的报文。[配置举例]

源地址/地址组: any
目的地址/地址组: any
协议: UDP
源端口: 1701
目的端口: any
动作: 加密

提示：为保证数据流业务互通，需要开启双向安全策略。[新建安全策略]

确定 取消

待加密的数据流

地址类型: IPv4
新建 按钮

源地址/地址组: [空]

目的端口 动作 编辑

没有记录

反向路由注入: 关闭
安全提议
接受对端提议: 开启

警告：可以使用任意本端支持的算法建立隧道，可能存在安全风险。

应用 返回

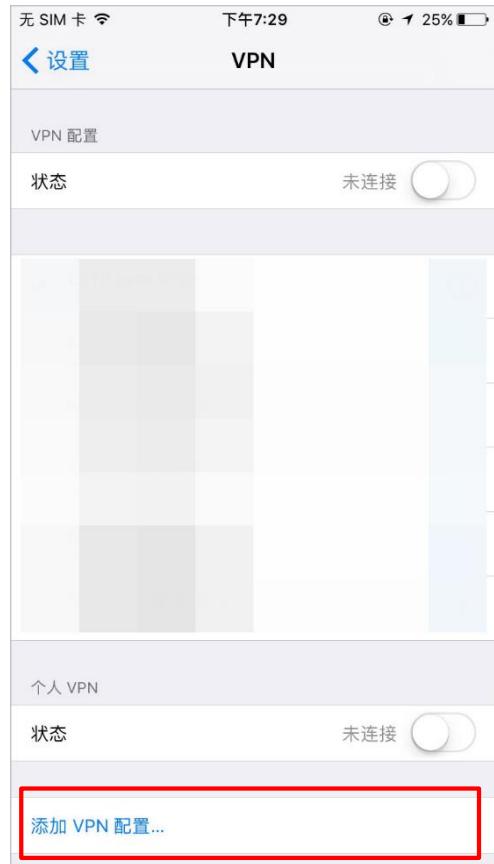
预共享密钥: Admin@123

5

6

Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

Step6 配置LAC的拨号参数



3 添加VPN网络

本例中使用的iOS版本为iOS 10.0



5 完成

输入防火墙公网接口IP地址

输入防火墙上配置的预共享密钥，本示例中为 Admin@123。

输入用户名及密码。
本例中用户名为 vpdnuser，密码为 Hello@123

4

Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

Step7 结果验证 (1)



Example 9.7: 客户端 L2TP over IPSec 接入 (iOS)

Step7 结果验证 (2)

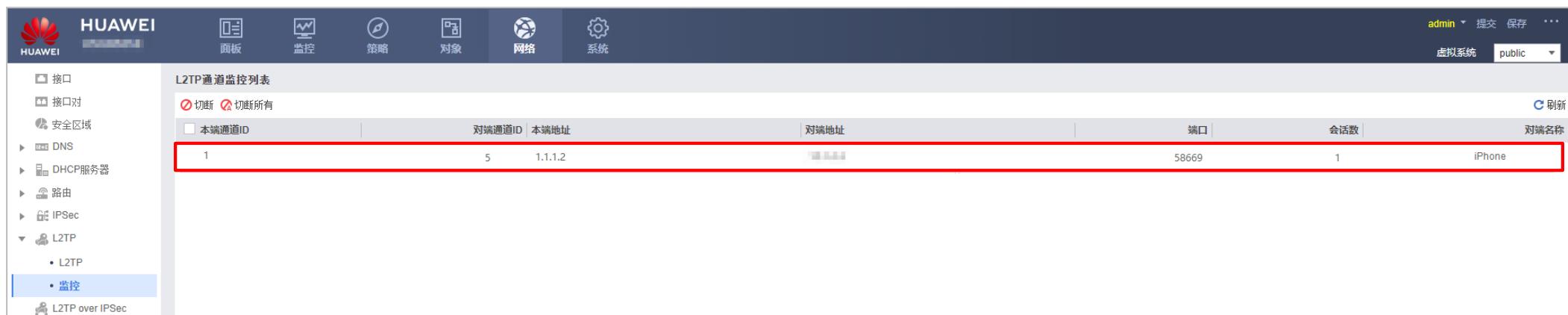
在防火墙上可查看到IPSec隧道监控信息



The screenshot shows the Huawei firewall's configuration interface. On the left, the navigation tree includes 'IPSec' and 'IPSec -> 监控'. The main panel displays the 'IPSec 监控列表' (IPSec Tunnel Monitoring List) with one entry highlighted by a red box:

策略名称	IKE用户描述	虚拟系统	状态	本端地址	对端地址	对端ID类型	对端ID内容	算法	协商数据流	持续时间 (...)	发送/接收速率 (...)	最近一次建立时间	最近一次断开时间	断开原因	当日前断次数
ipsec_policy		public	IKE协商成功 IPSec协商成功	1.1.1.2	1.1.1.1			ESP-AES-256-SHA1	源地址[端口]: 1.1.1.2[1701] 目的地址[端口]: 1.1.1.1[58669] 69	0/0					

在防火墙上可查看到L2TP通道监控信息

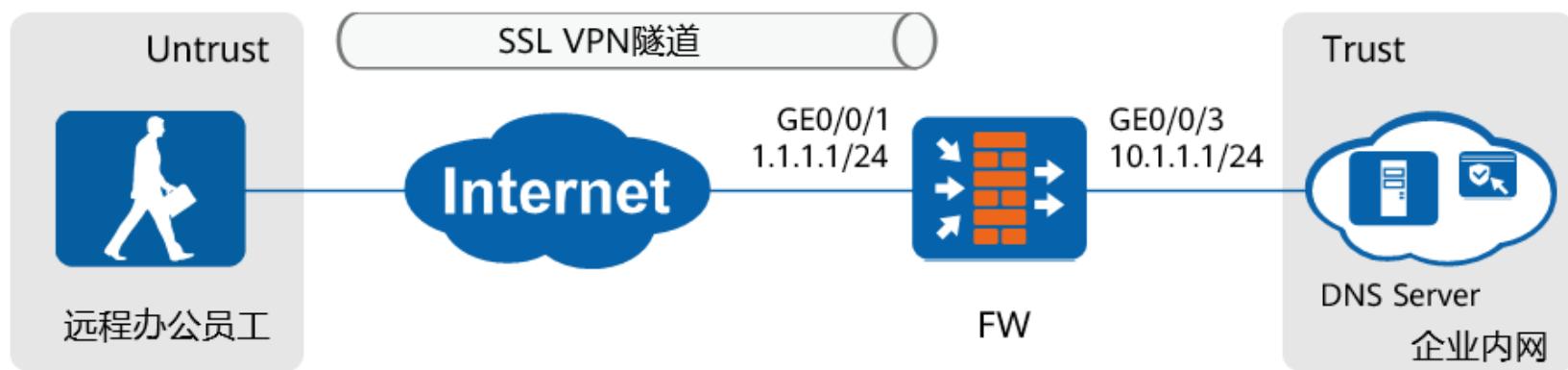


The screenshot shows the Huawei firewall's configuration interface. On the left, the navigation tree includes 'L2TP' and 'L2TP -> 监控'. The main panel displays the 'L2TP 通道监控列表' (L2TP Channel Monitoring List) with one entry highlighted by a red box:

本地通道ID	对端通道ID 本地地址	对端地址	端口	会话数	对端名称
1	5 1.1.1.2	1.1.1.1	58669	1	iPhone

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

组网图



企业希望远程办公的员工也能够获得一个内网IP地址，像在局域网一样访问企业内部的各种资源。另外为了增强安全性，采用本地认证的方式对远程办公用户的身份进行认证。

项目	数据
DNS服务器	IP地址: 10.1.1.2/24
认证方式	本地认证
SSL VPN用户	用户名: user 密码: Admin@1234
网络扩展虚拟IP地址池	10.1.1.50~10.1.1.100 远程办公设备通过SSL VPN接入公司并启用网络扩展业务后，防火墙会为该设备分配一个地址池中的地址。
可访问内网网段	10.1.1.0/24

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step1 配置接口

1 网络

2 接口

3 编辑

4 配置外网接口参数

5 编辑

6 配置内网接口参数

The screenshot shows the Huawei Network Management System interface. The top navigation bar includes 'HUAWEI' logo, '面板' (Dashboard), '监控' (Monitoring), '策略' (Policy), '对象' (Object), '网络' (Network) which is highlighted with a red box and has a red number '1' above it, and '系统' (System). The left sidebar under '接口' (Interface) has a red box around it with a red number '2' above it, listing options like '接口对', '安全区域', 'VXLAN', 'DNS', 'DHCP服务器', '路由', 'IPSec', 'L2TP', 'L2TP over IPSec', and 'GRE'. The main area is titled '接口列表' (Interface List) with '新建' (New) and '删除' (Delete) buttons. It displays a table of interfaces:

接口名称	安全区域	虚拟系统	IP地址	连接类型	VLAN/VXLAN	模式	物理	状态	启用	编辑
GE0/0/0			---	静态IP (IPv4) 静态IP (IPv6)		路由	↑ ↑	IPv4 IPv6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/1			---	静态IP (IPv4) 静态IP (IPv6)		路由	↑ ↑	IPv4 IPv6	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/2			---	静态IP (IPv4) 静态IP (IPv6)		路由	↓ ↓	IPv4 IPv6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/3			---	静态IP (IPv4) 静态IP (IPv6)		路由	↓ ↓	IPv4 IPv6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/4			---	静态IP (IPv4) 静态IP (IPv6)		路由	↑ ↑	IPv4 IPv6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/5			---	静态IP (IPv4) 静态IP (IPv6)		路由	↓ ↓	IPv4 IPv6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/6			---	静态IP (IPv4)		路由	↑ ↑	IPv4 IPv6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Two configuration windows are open at the bottom:

- 修改GigabitEthernet** (Configure GigabitEthernet) for GE0/0/1 (External Interface):
 - 接口名称: GigabitEthernet0/0/1*
 - 别名:
 - 虚拟系统: public*
 - 安全区域: untrust
 - 模式: 路由 (selected)
 - IPv4** tab:
 - 连接类型: 静态IP (selected)
 - IP地址: 1.1.1.1/255.255.255.0
 - 默认网关:
 - 首选DNS服务器:
 - 备用DNS服务器:
 - 多出口选项
 - IPv6** tab: (empty)
- 修改GigabitEthernet** (Configure GigabitEthernet) for GE0/0/3 (Internal Interface):
 - 接口名称: GigabitEthernet0/0/3*
 - 别名:
 - 虚拟系统: public*
 - 安全区域: trust
 - 模式: 路由 (selected)
 - IPv4** tab:
 - 连接类型: 静态IP (selected)
 - IP地址: 10.1.1.1/255.255.255.0
 - 默认网关:
 - 首选DNS服务器:
 - 备用DNS服务器:
 - 多出口选项
 - IPv6** tab: (empty)

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step2 创建用户组和用户

The screenshot illustrates the configuration steps for creating a user group and a user in the HUAWEI USG6300 device's user management interface.

- 步骤 1:** 在“对象”模块下，配置“SSL VPN接入”场景。
- 步骤 2:** 在左侧菜单栏的“用户”选项下，选择“/default”域。
- 步骤 3:** 在“用户管理”界面中，勾选“本地”并点击“[导入用户]”按钮。
- 步骤 4:** 在“新建用户组”对话框中输入“sslvpn”作为用户组名，选择所属用户组为“/default”，勾选“允许多人同时使用该组下账号登录”，并点击“新建用户组”按钮。
- 步骤 5:** 在“新建用户”对话框中输入用户名“user”，密码（示例：password@），并点击“新建用户”按钮。
- 步骤 6:** 点击“新建用户”按钮后，显示新建用户的详细信息。
- 步骤 7:** 在“新建用户”对话框中，显示“新建用户”的操作按钮。

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step3 配置SSL VPN网关（1）

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes icons for HUAWEI logo, 面板 (Panel), 监控 (Monitoring), 策略 (Policy), 对象 (Object), 网络 (Network) (highlighted with a red box and circled 1), and 系统 (System). The left sidebar lists various network components: 接口, 接口对, 安全区域, VXLAN, DNS, DHCP服务器, 路由, IPSec, L2TP, L2TP over IPsec, GRE, DSVPN, and SSL VPN (highlighted with a red box and circled 2). Under SSL VPN, there are sub-options: 公共配置, 监控, and SAGC. The main content area shows the 'SSL VPN 列表' (SSL VPN List) with a '新建' (New) button highlighted with a red box and circled 3. A modal window titled '新建 SSL VPN' (Create SSL VPN) is open, containing the following configuration fields:

① 网关配置	网关名称: gateway *
② SSL 配置	类型: 独占型 (Exclusive Type) (selected)
③ 业务功能选择	网关地址: GE0/0/1 * 1.1.1.1 * 端口: 443 <1024-50000>或443
④ 角色授权/用户	提示: 为保证用户登录网关, 需要开启安全策略。[新建安全策略]
用户认证	
客户端CA证书: default [多选]	
证书认证方式: -- NONE --	
认证域: 请选择认证域	
DNS服务器	
首选DNS服务器: 10.1.1.2	
备选DNS服务器 1: [empty]	
快速通道端口号: 443 <1-49999>	
最大用户数: 100 <1-10000>	
最大并发用户数: 50 <1-5000>	
最大资源数: 1024 <1-1024> (系统总资源: 51200, 剩余: 50176)	

At the bottom of the modal window are buttons for <上一步>, 下一步>, and 取消 (Cancel).

A callout box with a red border and circled 4 contains the text: 按照组网需求配置SSL VPN网关基本信息 (Configure SSL VPN gateway basic information according to networking requirements).

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step3 配置SSL VPN网关（2）

The screenshot shows the HUAWEI Network Management System interface. On the left, a sidebar lists various network services: Interface, Interface Pair, Security Zone, VXLAN, DNS, DHCP Server, Routing, IPSec, L2TP, L2TP over IPSec, GRE, DSVPN, and SSL VPN. Under SSL VPN, 'SSL VPN' is selected. In the main area, the 'SSL VPN List' is displayed with columns for Gateway Name, Gateway Address: Port, Domain, and Local Certificate. A new configuration dialog titled 'New SSL VPN' is open, showing steps 1 through 4. Step 2, 'SSL Configuration', is highlighted with a red box and a blue callout bubble containing the text 'Configure SSL version, encryption suite, etc.'.

SSL版本

TLS 1.0 TLS 1.1 TLS 1.2

公钥算法切换为SM2将会导致使用RSA算法的VPN客户端无法登录，请使用支持SM2算法的VPN客户端，并且公钥算法的切换也会造成对应网关的所有用户下线。

RSA SM2

本地证书: default

加密套件:

256-bit AES encryption with RSA and a SHA MAC
 168-bit Triple DES encryption with RSA and a SHA MAC
 128-bit AES encryption with RSA and a SHA MAC

会话超时时间: 5 <1-1440>分钟 默认为5

生命周期无限制

生命周期: 1440 <60-2880>分钟 默认为1440

5 配置SSL版本、加密套件等。

<上一步 下一步 取消

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step3 配置SSL VPN网关（3）

请选择您需要开启的业务

- ① 网关配置
- ② SSL 配置
- ③ **业务功能选择**
- ④ 网络扩展
- ⑤ 角色授权/用户

网络扩展 配置外网用户通过SSL隧道访问内网的所有资源。

web代理 配置外网用户可以访问的内网Web资源。

文件共享 配置外网用户可以访问的内网系统服务器的共享资源。

端口转发 配置外网用户可以访问的内网TCP应用服务（如：SSH、Telnet）开启的资源。

主机检查 检查用户访问内网资源的终端是否符合安全要求。

6 选择需要开启的业务功能

SSL VPN开启网络扩展功能，默认不需要配置从虚拟网关到用户IP的路由。但当FW开启IP欺骗攻击防范时，用户送到虚拟网关的报文会当做IP欺骗报文被丢弃。这种情况下，配置网络扩展功能时需要配置虚拟网关到用户IP地址的静态路由（其中，目的地址为用户地址池中的IP地址，下一跳为虚拟网关到Internet的下一跳IP地址）。

<上一步 下一步> 取消

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step3 配置SSL VPN网关（4）

HUAWEI

SSL VPN 列表

新建 删除

网关名称	网关地址:端口	域名	本地证书
------	---------	----	------

新建 SSL VPN

① 网关配置
② SSL 配置
③ 业务功能选择
④ 网络扩展
⑤ 角色授权/用户

配置网络扩展

保持连接 隧道保活间隔 ② 120 <10-3600>秒

可分配IP地址池范围
10.1.1.50-10.1.1.100/24

路由模式
手动路由模式
① 修改路由模式和内网网段会导致用户下线。在手动模式下，至少需配置一条手工路由，否则该模式无效。

7 配置网络扩展

可访问内网网段列表

该功能是为了灵活控制用户业内网和本地局域网，不能同时访问

新建 删除

IP网段

没有记录

8 新建可访问内网网段

新建网段

IP网段 10.1.1.0 *

子网掩码 255.255.255.0 *

提示：为保证用户使用网络扩展，需要开启安全策略。[\[新建安全策略\]](#)

确定 取消 GO

<上一步 下一步 取消

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step3 配置SSL VPN网关（5）

SSL VPN 列表

新建 SSL VPN

① 网关配置
② SSL 配置
③ 业务功能选择
④ 网络扩展
⑤ 角色授权/用户

角色授权列表

新建 删除

角色

关联用户（组）

业务启用 网络扩展 Web代理 文件共享

资源授权列表

选择 删除

资源名称

描述

没有记录

策略检查

主机检查策略通过条件

所有策略都满足
任一策略满足

请选择主机检查策略 [多选]

确定 取消

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step4 配置安全策略

1 安全策略列表

2 安全策略

3 允许远程办公员工登录SSL VPN网关

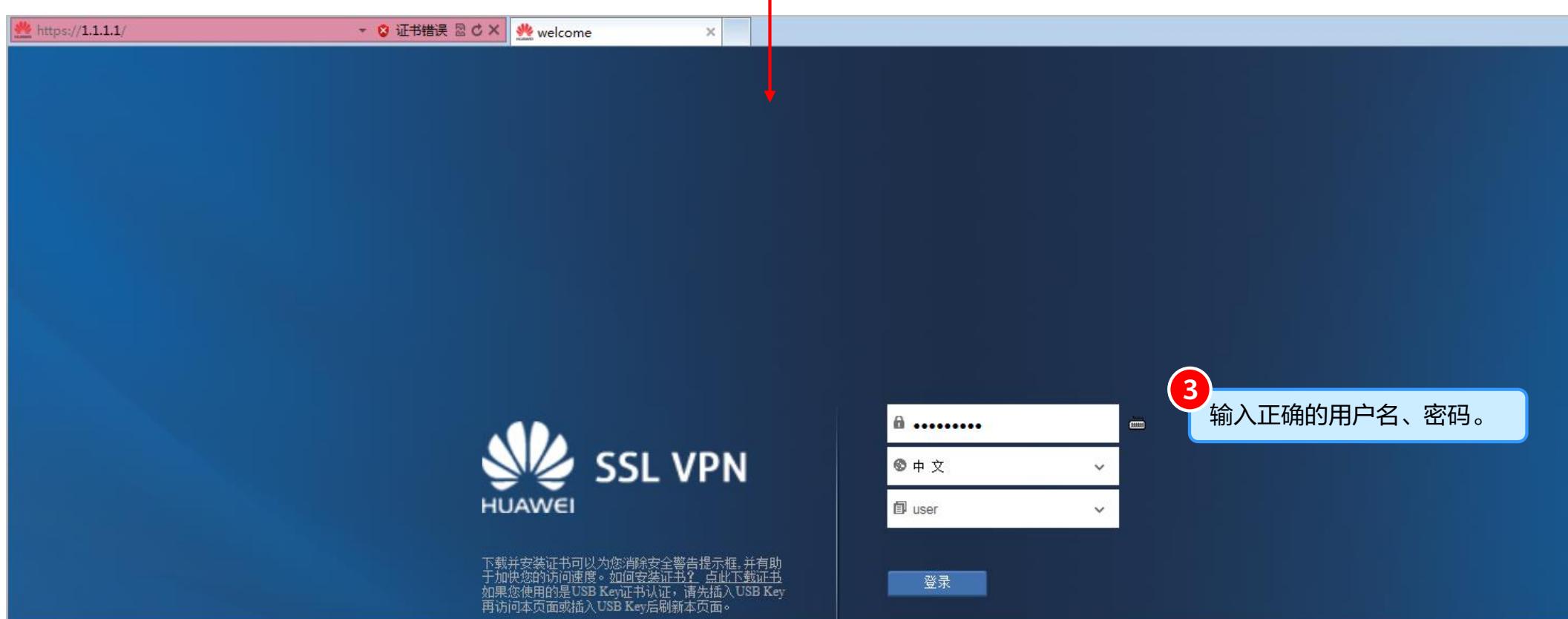
4 允许远程办公员工访问内网资源

源地址配置为网络扩展地址池地址，目的地址配置为远程办公用户可访问的内网资源地址。

The screenshot shows the Huawei Network Management System interface. The top navigation bar includes the HUAWEI logo, a search bar, and tabs for 面板 (Panel), 监控 (Monitoring), 策略 (Policy), 对象 (Object), 网络 (Network), and 系统 (System). The '策略' tab is highlighted with a red box and labeled '1'. The left sidebar has a '安全策略' section with a '安全策略' button highlighted by a red box and labeled '2'. Below it are other options like 策略冗余分析, 策略命中分析, 应用风险调优, NAT策略, 服务器负载均衡, and 带宽管理. A red arrow points from '2' down to a '新建安全策略' button in the main content area. The main content area is titled '安全策略列表' and shows a table with columns: 序号 (Index), 名称 (Name), 描述 (Description), 标签 (Label), VLAN ID, 源安全区域 (Source Security Zone), 目的安全区域 (Destination Security Zone), 源地址/地区 (Source Address/Region), 目的地址/地区 (Destination Address/Region), 用户 (User), 服务 (Service), and 应用 (Application). A blue box highlights the '允许远程办公员工登录SSL VPN网关' row (labeled '3'). Another blue box highlights the '允许远程办公员工访问内网资源' row (labeled '4'). A callout bubble on the right side of the interface states: '源地址配置为网络扩展地址池地址，目的地址配置为远程办公用户可访问的内网资源地址。' (Source address is configured as the network extension address pool, and the destination address is configured as the internal network resources accessible by remote office users.)

Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step5 结果验证（1）



Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step5 结果验证（2）



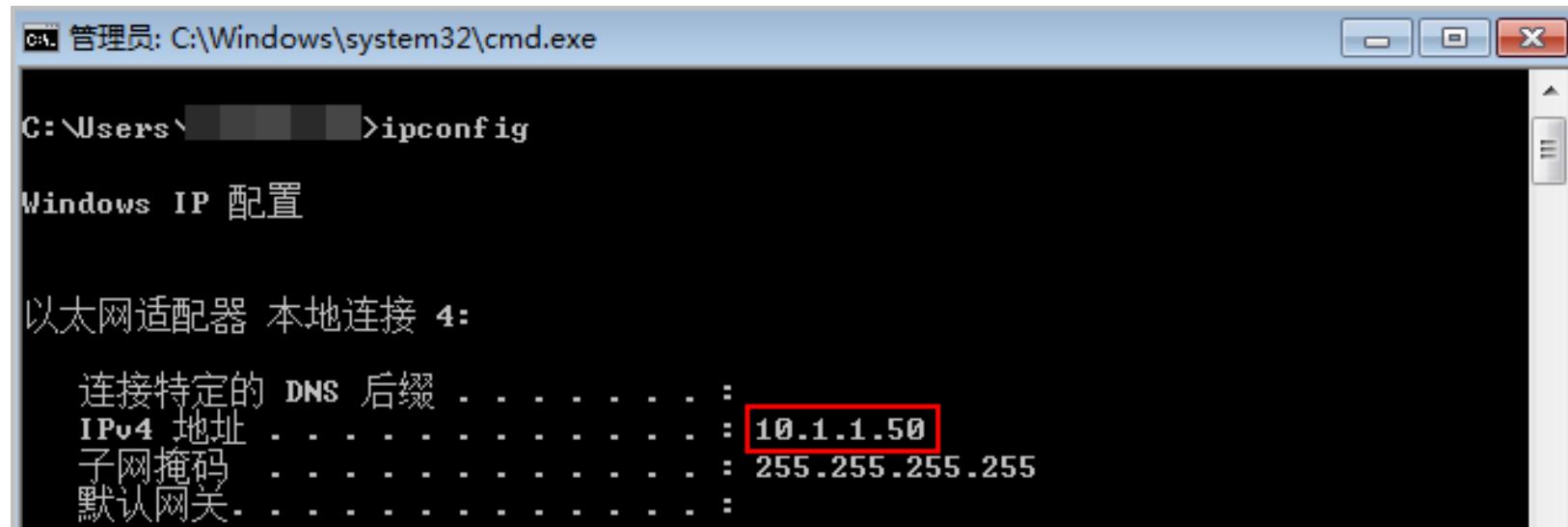
6 网络扩展启动成功后显示如上状态

5 根据提示安装虚拟网卡

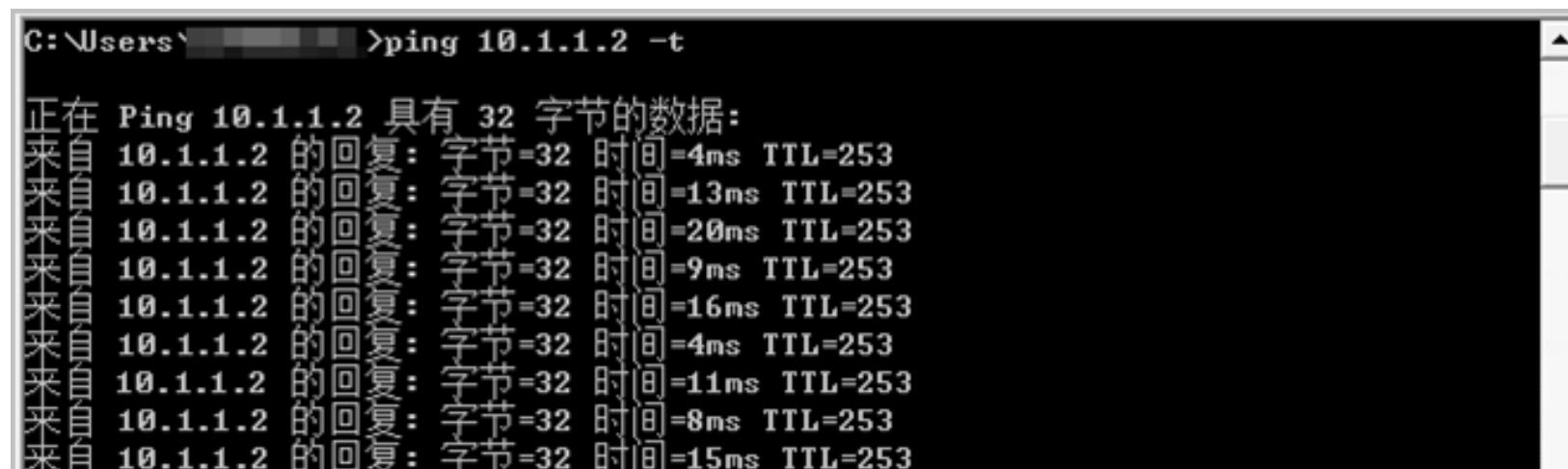
Example 10.1: SSL VPN隧道接入（网络扩展+本地认证）

Step5 结果验证（3）

客户端获取到防火墙分配的虚拟IP地址。

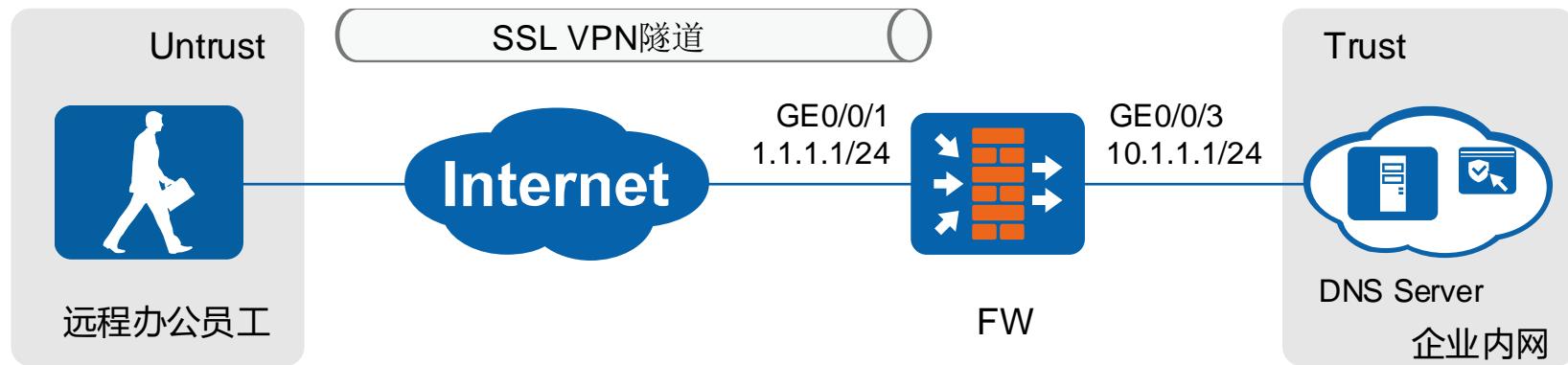


客户端能访问内网的资源。例如，在客户端上能够ping通内网DNS服务器10.1.1.2。



Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

组网图



企业希望远程办公的员工也能够获得一个内网IP地址，像在局域网一样访问企业内部的各种资源。另外为了增强安全性，采用证书结合本地认证的方式（证书挑战方式）对远程办公用户的身份进行认证。

项目	数据
DNS服务器	IP地址: 10.1.1.2/24
认证方式	证书挑战 辅助认证方式: 本地认证
SSL VPN用户	用户名: user 密码: Admin@1234
客户端证书	user.p12 将客户端证书导入远程办公设备的浏览器中，防火墙通过验证客户端证书来确认用户身份（使用客户端证书的主题CN字段取值作为用户名），制作客户端证书时，其主题CN字段取值必须和SSL VPN用户名（user）保持一致。
客户端CA证书	ca.crt CA证书是颁发客户端证书的CA服务器的CA证书。导入防火墙后，用于防火墙验证客户端证书的合法性。
网络扩展虚拟IP地址池	10.1.1.50~10.1.1.100 远程办公设备通过SSL VPN接入公司并启用网络扩展业务后，防火墙会为该设备分配一个地址池中的地址。

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step1 配置接口

The screenshot shows the HUAWEI Network Management System interface for configuring SSL VPN interfaces.

1. 网络: Selected in the top navigation bar.

2. 接口: Selected in the left sidebar under the "接口" category.

3. 编辑: A red circle highlights the edit icon for the selected interface.

4. 配置外网接口参数: A blue box highlights the configuration dialog for the external network interface (GE0/0/0/0(GE0/MGMT)).

5. 配置内网接口参数: A blue box highlights the configuration dialog for the internal network interface (GE0/0/3).

Configuration Details (Left Dialog - GE0/0/0(GE0/MGMT)):

接口名称	GigabitEthernet0/0/0
别名	
虚拟系统	public
安全区域	untrust
模式	<input checked="" type="radio"/> 路由
IPv4	连接类型: <input checked="" type="radio"/> 静态IP IP地址: 1.1.1.1/24 <small>一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。</small>
接口带宽	

Configuration Details (Right Dialog - GE0/0/3):

接口名称	GigabitEthernet0/0/3
别名	
虚拟系统	public
安全区域	trust
模式	<input checked="" type="radio"/> 路由
IPv4	连接类型: <input checked="" type="radio"/> 静态IP IP地址: 10.1.1.1/24 <small>一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。</small>
接口带宽	

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step2 创建用户组和用户

The screenshot shows the HUAWEI Network Management System interface with the following steps highlighted:

- 1**: Click on the "对象" (Object) icon in the top navigation bar.
- 2**: In the left sidebar under "用户" (User), click on the "/default" link.
- 3**: In the main panel, under "用户管理" (User Management), select the "SSL VPN接入" (SSL VPN Access) scenario.
- 4**: In the "用户/用户组/安全组管理列表" (User/User Group/Security Group Management List) table, click on "新建用户组" (Create New User Group).
- 5**: Fill in the "新建用户组" (Create New User Group) dialog with the following details:
 - 用户组名: sslvpn
 - 所属用户组: /default
 - 允许多人同时使用该组下账号登录 (Checkmark)
 - 警告: 禁用此功能将导致使用此用户帐号登录的所有IP全部下线 (Warning message)
 Click the "新建用户组" (Create New User Group) button.
- 6**: In the "用户/用户组/安全组管理列表" table, click on "新建用户" (Create New User).
- 7**: Fill in the "新建用户" (Create New User) dialog with the following details:
 - 登录名: user
 - 所属用户组: /default/sslvpn
 - 密码: (Leave empty)
 - 确认密码: (Leave empty)
 - 用户属性 (Checkmark)
 Click the "新建用户" (Create New User) button.

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step3 上传客户端CA证书

The screenshot shows the HUAWEI USG6300 firewall's configuration interface. The top navigation bar includes icons for Home, Dashboard, Monitoring, Policies, Objects (highlighted with a red box), Networks, and System. The top right corner shows the user 'admin' and buttons for Submit, Save, and More. A dropdown menu indicates the virtual system is 'public'. The left sidebar lists various configuration categories, with 'Certificates' expanded, showing options like Local Certificates, CA Certificates (highlighted with a red box), CRLs, Certificate Filtering, and SSL Decryption Certificates. The main content area is titled 'CA Certificate List' and shows a table with columns for Name and Subject DN. A red box highlights the 'Upload' button. A red arrow points from this button to a modal dialog titled 'Upload CA Certificate'. This dialog has fields for 'Upload Method' (Local Upload selected), 'Certificate File' (containing 'C:\fakepath\ca.crt'), and 'Password'. It includes 'OK' and 'Cancel' buttons. A red box highlights the 'Upload Method' and 'Certificate File' fields. A callout bubble with the number 4 contains the text: '申请或制作客户端CA证书、客户端证书后，将客户端CA证书上传到防火墙中。' (After applying or creating the client CA certificate and client certificate, upload the client CA certificate to the firewall). The bottom of the interface shows pagination controls ('每页 50', '共 2 条') and a CLI Control button.

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step4 配置SSL VPN网关（1）

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and tabs for '面板' (Dashboard), '监控' (Monitoring), '策略' (Policy), '对象' (Object), '网络' (Network) [highlighted with a red box], and '系统' (System). The 'SSL VPN' icon in the sidebar is also highlighted with a red box. A red circle labeled '1' points to the '新建' (New) button in the 'SSL VPN 列表' (SSL VPN List) table header. A red arrow labeled '3' points from the 'SSL VPN' icon in the sidebar to the '新建' button. A red box highlights the 'SSL VPN' section in the sidebar. A blue callout box labeled '4' contains the text: '按照组网需求配置SSL VPN网关基本信息' (Configure SSL VPN gateway basic information according to networking requirements). The main window displays the '新建 SSL VPN' (Create New SSL VPN) dialog box, which is also highlighted with a red box. The dialog box contains four sections: ① 网关配置 (Gateway Configuration) with fields for '网关名称' (Gateway Name) set to 'gateway', '类型' (Type) selected as '独占型' (Exclusive), '网关地址' (Gateway Address) set to 'GE0/0/1' and '1.1.1.1', and port '443'; ② SSL 配置 (SSL Configuration) with '客户端CA证书' (Client CA Certificate) set to 'ca.crt' and '证书挑战' (Challenge Certificate) selected; ③ 业务功能选择 (Service Function Selection) with '用户过滤字段' (User Filter Field) set to '主题-CN (Common name)' and '组过滤字段' (Group Filter Field) set to '主题-OU (Organizational unit)'; ④ 角色授权/用户 (Role Authorization/User) with '认证域' (Authentication Domain) set to 'default'. At the bottom of the dialog box are buttons for '<上一步' (Previous Step), '下一步>' (Next Step), and '取消' (Cancel).

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step4 配置SSL VPN网关（2）

SSL VPN列表

新建 SSL VPN

① 网关配置

② SSL 配置

③ 业务功能选择

④ 角色授权/用户

SSL版本

TLS 1.0 TLS 1.1 TLS 1.2

公钥算法

RSA SM2

本地证书

default

加密套件

256-bit AES encryption with RSA and a SHA MAC
 168-bit Triple DES encryption with RSA and a SHA MAC
 128-bit AES encryption with RSA and a SHA MAC

会话超时时间

5 <1-1440>分钟 默认为5

生命周期无限制

生命周期

1440 <60-2880>分钟 默认为1440

5 配置SSL版本、加密套件等。

每页 50 < > 1 / 1 GO

CLI 控制台

<上一步 **下一步** 取消

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step4 配置SSL VPN网关（3）

SSL VPN列表

新建 SSL VPN

请选择您需要开启的业务

① 网关配置

② SSL 配置

③ 业务功能选择

④ 网络扩展

⑤ 角色授权/用户

⑥ 选择需要开启的业务功能

SSL VPN开启网络扩展功能，默认不需要配置从虚拟网关到用户IP的路由。但当FW开启IP欺骗攻击防范时，用户送到虚拟网关的报文会当做IP欺骗报文被丢弃。这种情况下，配置网络扩展功能时需要配置虚拟网关到用户IP地址的静态路由（其中，目的地址为用户地址池中的IP地址，下一跳为虚拟网关到Internet的下一跳IP地址）。

网关名称 | 网关地址:端口 | 域名 | 本地证书 | 客户端CA证书 | 证书认证方式 | 编辑

刷新 | **请输入名称** | **查询**

admin 提交 保存 ...

虚拟系统 public

接口 | **接口对** | **安全区域** | **DNS** | **DHCP服务器** | **路由** | **IPSec** | **L2TP** | **L2TP over IPSec** | **GRE** | **DSVPN** | **SSL VPN** | **SSL VPN** | **公共配置** | **监控**

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step4 配置SSL VPN网关（4）

HUAWEI 网络管理

SSL VPN 列表

网关名称 网关地址:端口 域名 本地证书 客户端CA证书 证书认证方式 编辑

刷新 搜索: 请输入名称 查询

新建 SSL VPN

① 网关配置
② SSL 配置
③ 业务功能选择
④ 网络扩展
⑤ 角色授权/用户

配置网络扩展

保持连接: 120 <10-3600>秒
可分配IP地址池范围: 10.1.1.50-10.1.1.100/24
路由模式: 手动路由模式

⑦ 配置网络扩展

每行可配置一个IP地址池，
行之间用回车分隔。示例:
10.10.1.1-10.10.1.254/255.255.255.0
10.10.1.1-10.10.1.254/24

⑧ 新建可访问内网网段

可访问内网网段列表

新建 IP网段

IP网段: 10.1.1.0 子网掩码: 255.255.255.0

提示: 为保证用户使用网络扩展, 需要开启安全策略。[新建安全策略]

确定 取消

<上一步 下一步> 取消

接口
接口对
安全区域
DNS
DHCP服务器
路由
IPSec
L2TP
L2TP over IPSec
GRE
DSVPN
SSL VPN
• SSL VPN
公共配置
监控

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step4 配置SSL VPN网关（5）

HUAWEI 网络管理

admin 提交 保存 ...
虚拟系统 public

SSL VPN 列表 新建 删除 刷新 请输入名称 查询

新建 SSL VPN

① 网关配置
② SSL 配置
③ 业务功能选择
④ 网络扩展
⑤ 角色授权/用户

角色授权列表
+新建 -删除
角色 default
共 1 条

新建角色授权

⑨ 新建角色授权

角色: sslvpn
关联用户(组): /default/sslvpn
[多选]
业务启用: 网络扩展 Web代理 文件共享
资源授权列表
+选择 -删除
资源名称
描述
没有记录

策略检查
主机检查策略通过条件
所有策略都满足
任一策略满足
主机检查策略: 请选择主机检查策略 [多选]

确定 取消

The screenshot shows the configuration of an SSL VPN role authorization. The 'sslvpn' role is selected, and the 'Network Extension' service is enabled. A red box highlights the 'New Role Authorization' button, which is step 9 in the process. Another red box highlights the 'Business Activation' section where the 'Network Extension' checkbox is checked.

Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step5 配置安全策略

该策略的源、目的安全区域不要配置。
源地址配置为网络扩展地址池地址，目的地址配置为远程办公用户可访问的内网资源地址。

The screenshot shows the Huawei Network Management System interface. The top navigation bar includes the HUAWEI logo, user 'admin', and buttons for Dashboard, Monitoring, Policies (highlighted with a red box), Objects, Networks, and Systems. The left sidebar has sections like Security Policies (selected), NAT Policies, Server Load Balancing, Bandwidth Management, and Proxy Policies. The main area is titled 'Security Policy List'.

Left Panel (Main View):

- 1:** Shows the 'New Security Policy' button and search/filter fields.
- 2:** Shows the 'Security Policies' section in the sidebar.
- 3:** Shows the configuration for 'Allow Remote Office Employees to Log in to the SSL VPN Gateway'. It includes fields for Source/Destination (untrust/local), Destination Address (1.1.1.1/24), VLAN ID (1-4094), and Action (Allow). A note says: '提示: 新建时可以基于策略模板来快速定义您需要的策略'.

Right Panel (Modals):

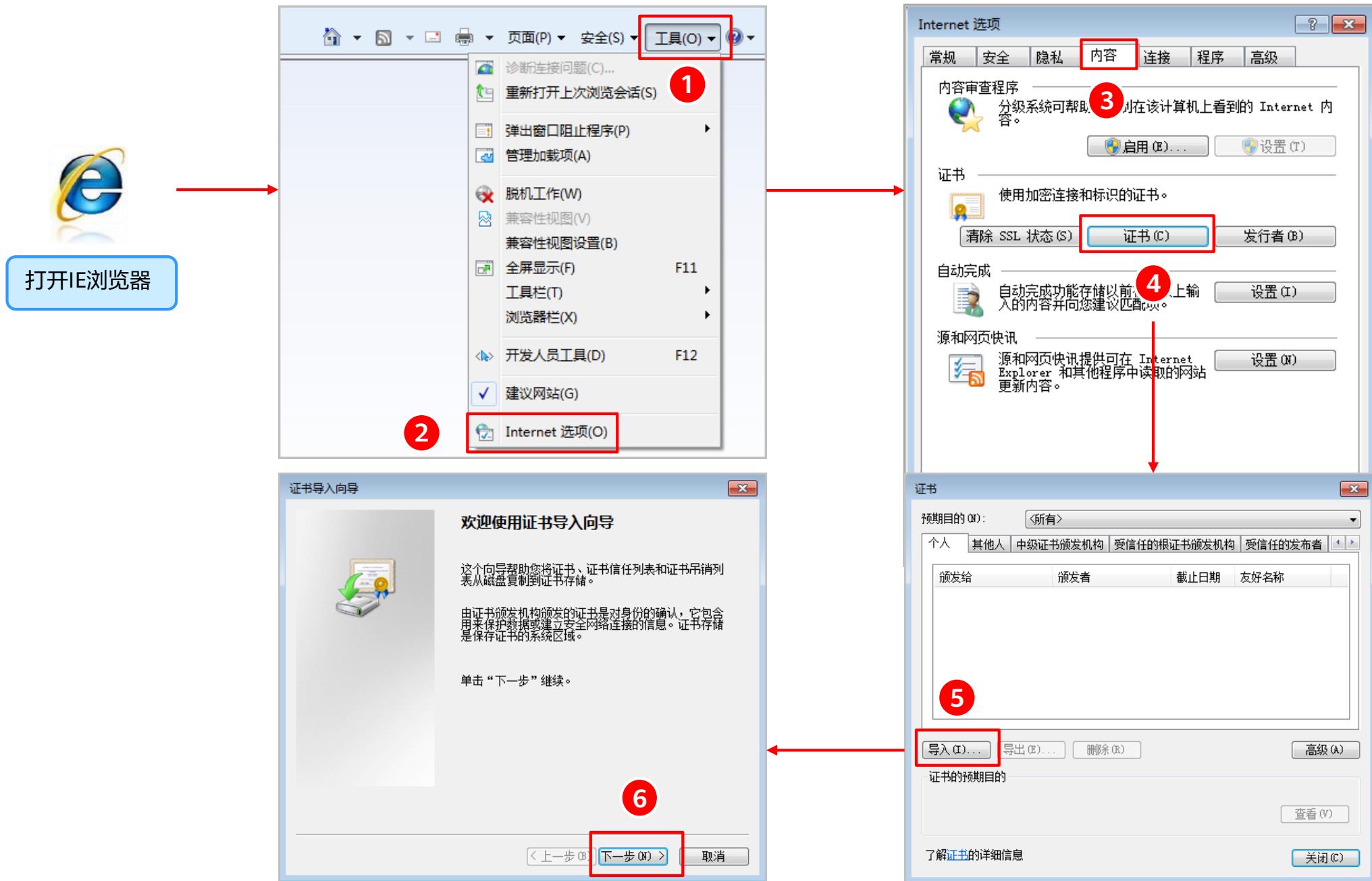
- 4:** Shows the configuration for 'Allow Remote Office Employees to Access Internal Network Resources'. It includes fields for Source/Destination (local/untrust), Destination Address (10.1.1.0/24), VLAN ID (1-4094), and Action (Allow). A note says: '提示: 新建时可以基于策略模板来快速定义您需要的策略'.

Bottom Buttons:

- 确定 (Confirm)
- 确定并复制 (Confirm and Copy)
- 命令预览 (Command Preview)
- 取消 (Cancel)

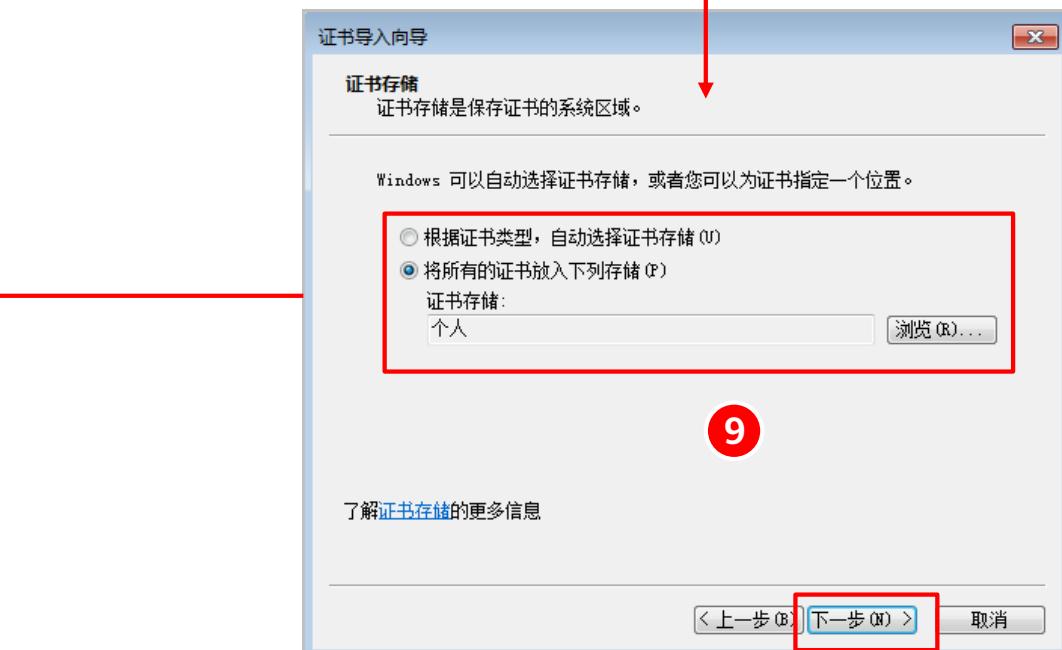
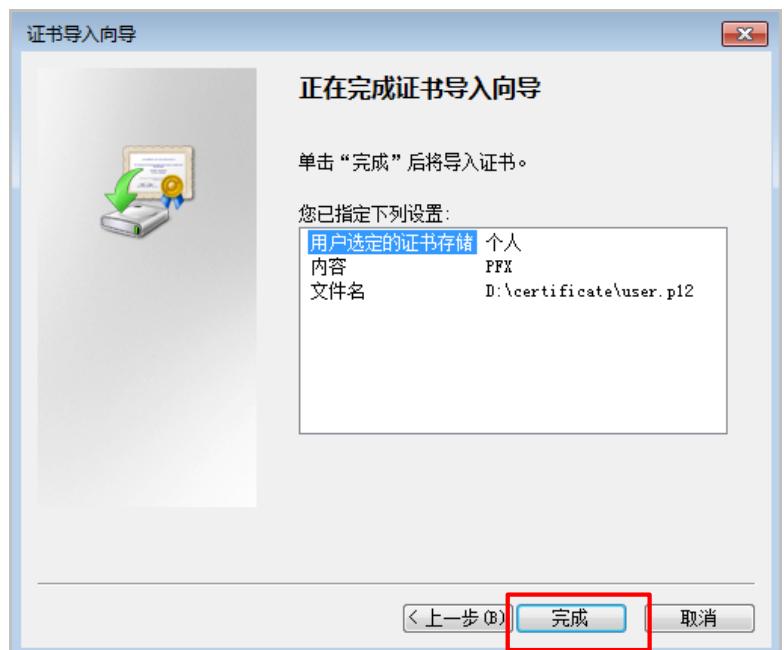
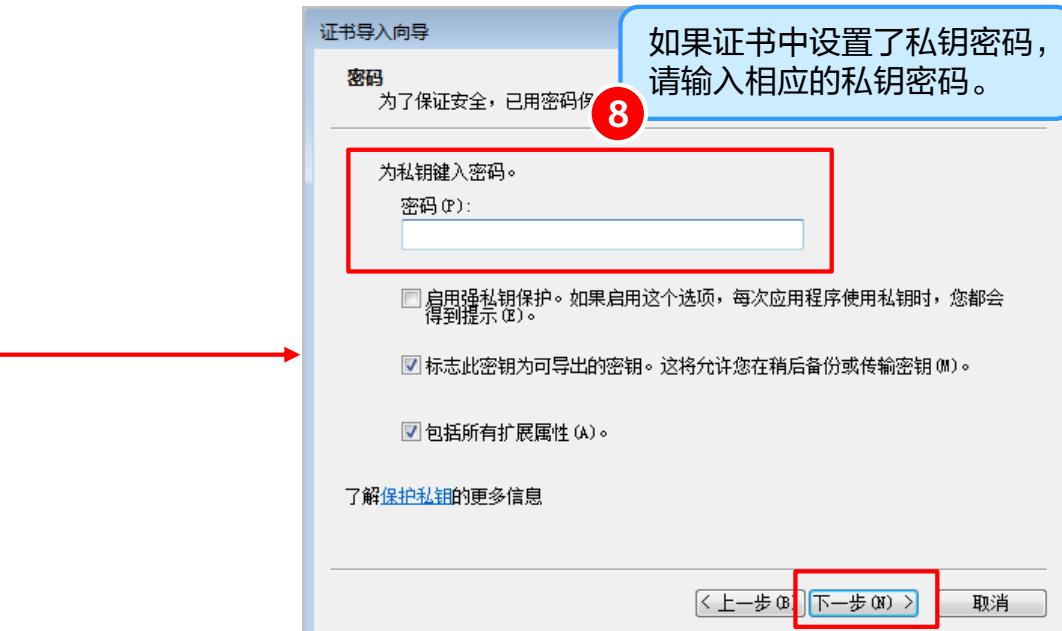
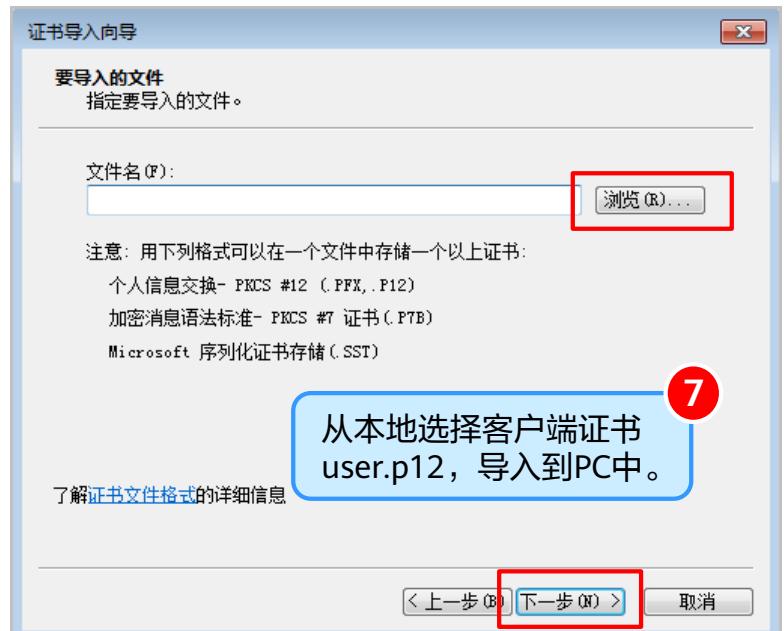
Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step6 安装客户端证书（1）



Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step6 安装客户端证书（2）



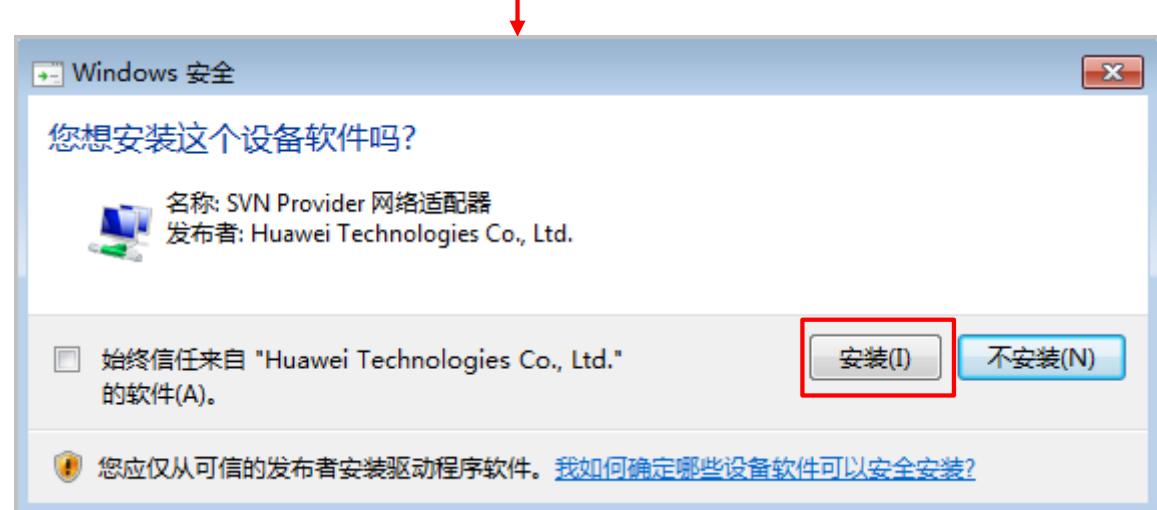
Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step7 结果验证 (1)



Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step7 结果验证（2）



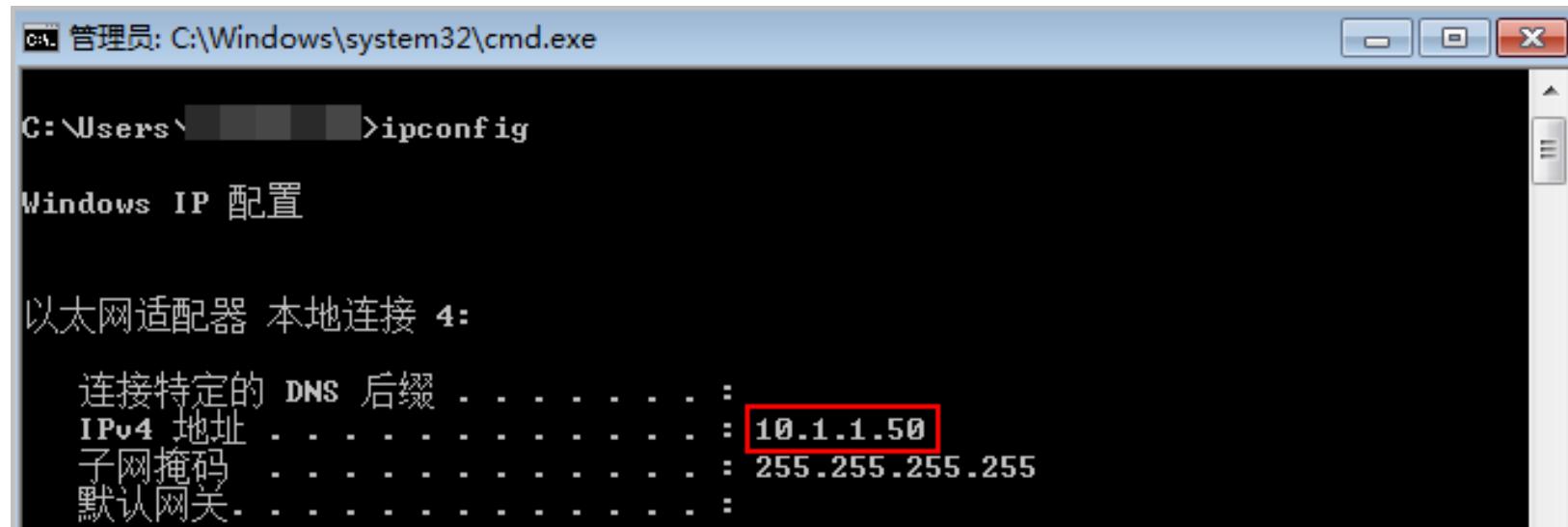
6 网络扩展启动成功后显示如上状态

5 根据提示安装虚拟网卡

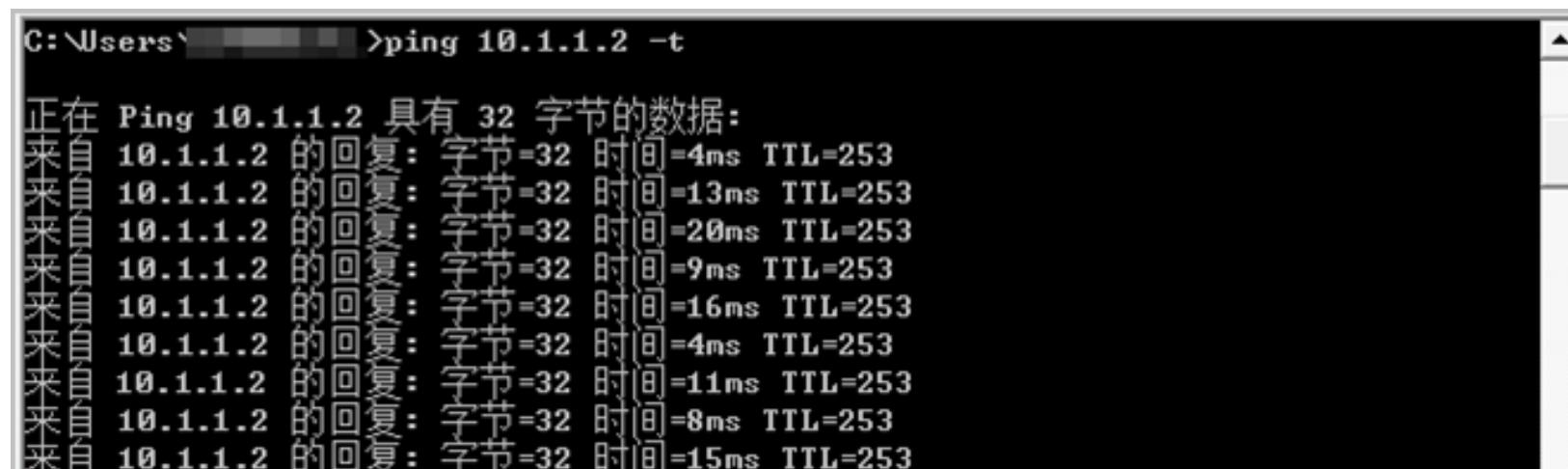
Example 10.2: SSL VPN隧道接入（网络扩展+证书挑战认证）

Step7 结果验证（3）

客户端获取到防火墙分配的虚拟IP地址。

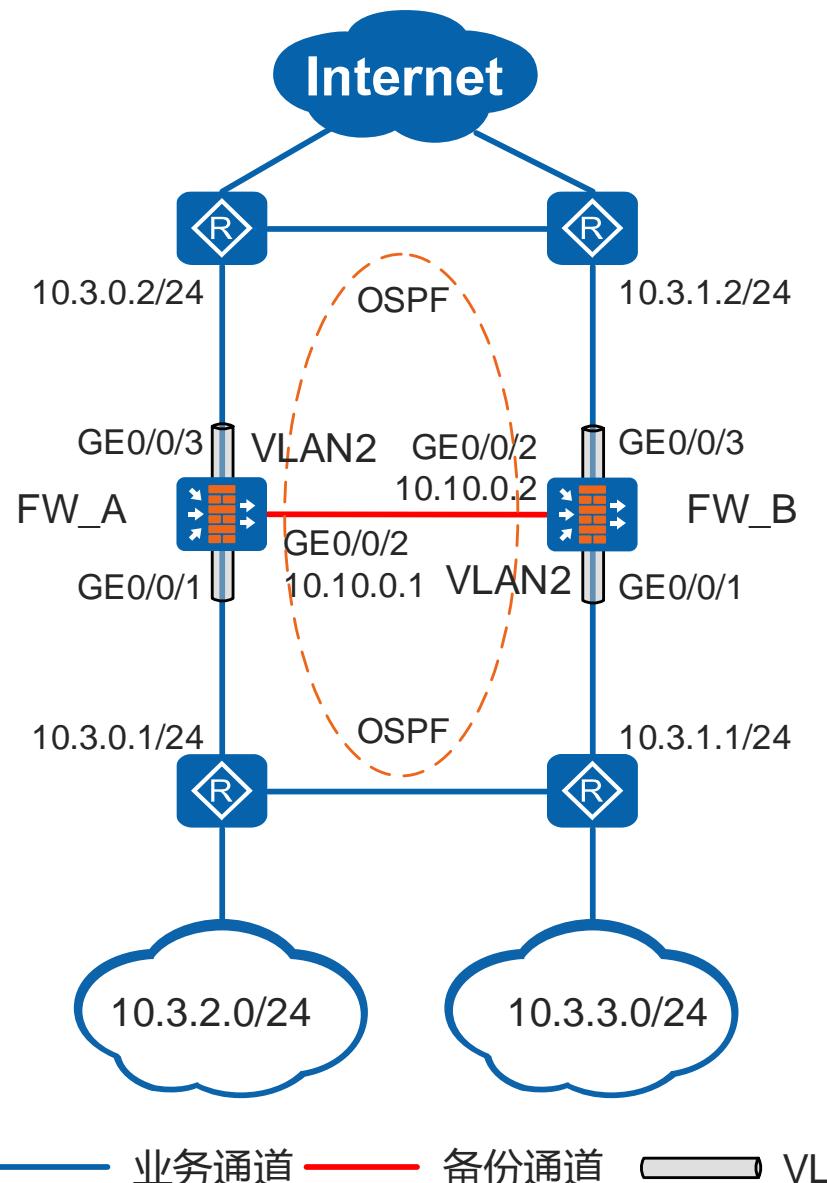


客户端能访问内网的资源。例如，在客户端上能够ping通内网DNS服务器10.1.1.2。



Example 11：防火墙透明接入的负载分担场景

组网图



两台FW的业务接口都工作在二层，上下行分别连接路由器。FW的上下行业务接口都加入到相同VLAN中。上下行路由器之间运行OSPF协议，FW作为二层设备透传OSPF协议报文，不参与路由协议计算。

本例希望两台FW以负载分担方式工作。正常情况下，FW_A和FW_B共同转发流量。当其中一台FW出现故障时，另外一台FW转发全部业务，保证业务不中断。

项目	FW_A	FW_B
运行模式	负载分担	负载分担
心跳接口	GE0/0/2 10.10.0.1/24	GE0/0/2 10.10.0.2/24

Example 11：防火墙透明接入的负载分担场景

Step1 配置FW_A的接口（1）

1. 在HUAWEI USG防火墙管理界面中，进入“网络”->“接口”模块。

2. 在左侧树状菜单中，选择“接口”。

3. 在右侧列表中，选择要配置的上行接口（GE0/0/1），并点击“编辑”按钮。

4. 在“修改GigabitEthernet”对话框中，配置下行接口参数。设置“接口名称”为“GigabitEthernet0/0/1”，“安全区域”为“trust”，“模式”为“Access”，“连接类型”为“Access”，“Access VLAN ID”为“2”。并配置“接口带宽”。

5. 在右侧列表中，选择要配置的下行接口（GE0/0/3），并点击“编辑”按钮。

6. 在“修改GigabitEthernet”对话框中，配置上行接口参数。设置“接口名称”为“GigabitEthernet0/0/3”，“安全区域”为“untrust”，“模式”为“Access”，“连接类型”为“Access”，“Access VLAN ID”为“2”。并配置“接口带宽”。

Example 11：防火墙透明接入的负载分担场景

Step1 配置FW_A的接口（2）

1. 在HUAWEI USG6000E管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“接口”选项。

3. 在右侧列表中，选择要配置的心跳接口（GE0/0/2），并点击编辑图标。

4. 弹出“修改GigabitEthernet”对话框，显示了接口的基本配置信息。对话框内所有输入框均被红色方框高亮显示。

参数	值
接口名称	GigabitEthernet0/0/2
别名	
虚拟系统	public
安全区域	dmz
模式	路由
连接类型	静态IP
IP地址	10.10.0.1/24
默认网关	
首选DNS服务器	
备用DNS服务器	

注：IP地址输入框下方有提示：“一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

5. 在对话框底部，点击“确定”按钮完成配置。

Example 11：防火墙透明接入的负载分担场景

Step2 配置FW_B的接口（1）

1. 在HUAWEI USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中选择“接口”选项。

3. 在右侧列表中选择要配置的上行接口（GE0/0/1），并点击“编辑”按钮。

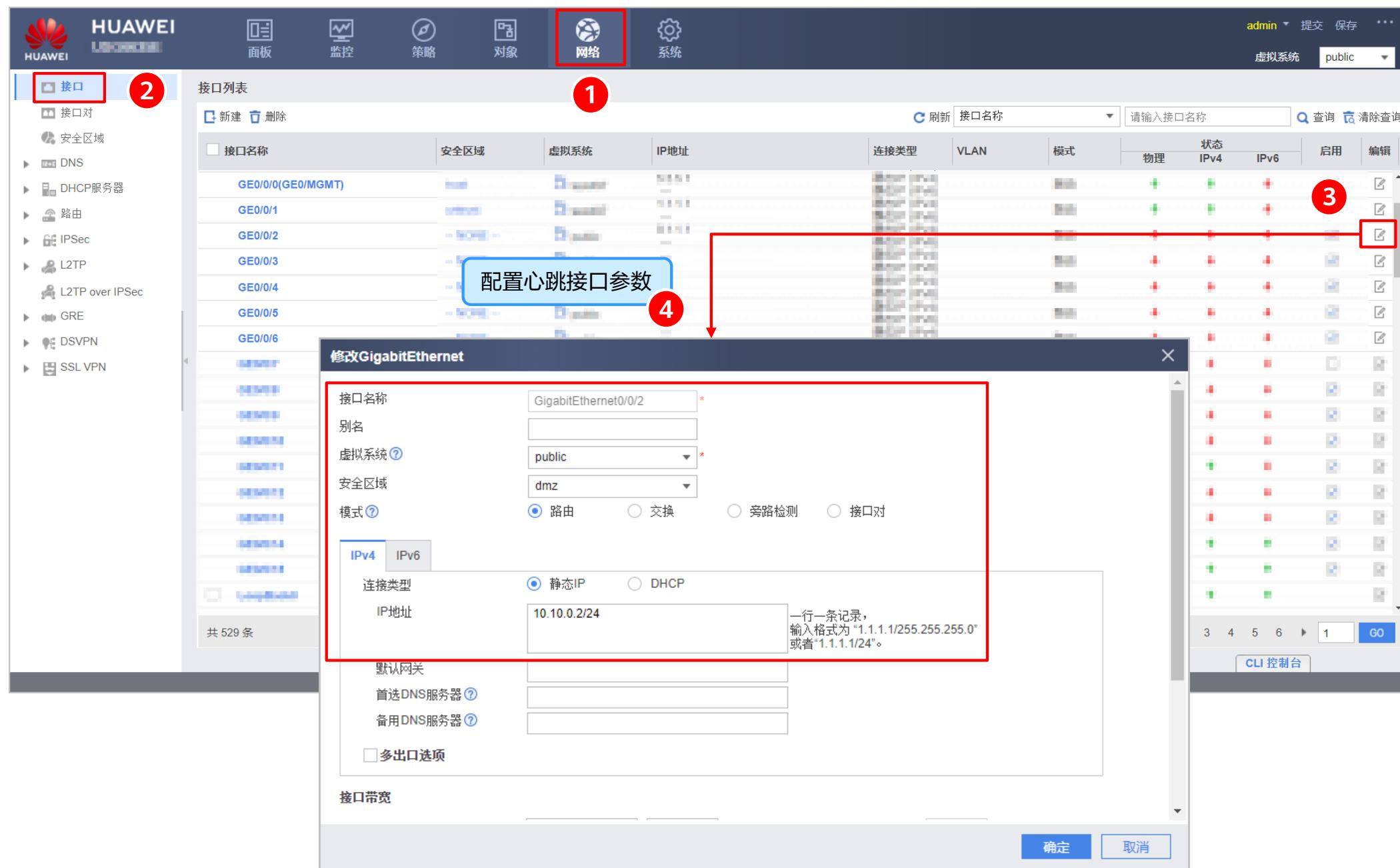
4. 在“修改GigabitEthernet”对话框中，配置下行接口参数。设置接口名称为“GigabitEthernet0/0/1”，安全区域为“trust”，模式为“Access”，连接类型为“Trunk”，并将“Access VLAN ID”设置为“2”。同时配置入方向带宽和出方向带宽。

5. 在右侧列表中选择要配置的下行接口（GE0/0/3），并点击“编辑”按钮。

6. 在“修改GigabitEthernet”对话框中，配置上行接口参数。设置接口名称为“GigabitEthernet0/0/3”，安全区域为“untrust”，模式为“Access”，连接类型为“Trunk”，并将“Access VLAN ID”设置为“2”。同时配置入方向带宽和出方向带宽。

Example 11: 防火墙透明接入的负载分担场景

Step2 配置FW_B的接口 (2)



Example 11：防火墙透明接入的负载分担场景

Step3 配置FW_A为负载分担模式

The screenshot shows the HUAWEI USG6300 configuration interface. The main menu on the left includes: 配置 (Configuration), 用户体验计划 (User Experience Plan), 管理员 (Administrator), 虚拟系统 (Virtual System), 跨数据中心集群 (Cross Data Center Cluster), 高可靠性 (High Reliability), 双机热备 (Dual Homing Backup) (highlighted with a red box), IP-Link, BFD, Link-Group, 邮件服务设置 (Email Service Settings), 日志配置 (Log Configuration), License Management, 升级中心 (Upgrade Center), 系统更新 (System Update), 配置文件管理 (Configuration File Management), VPN客户端升级 (VPN Client Upgrade), 快速向导 (Quick Guide), and 链接配置 (Link Configuration). The top navigation bar includes: HUAWEI, 面板 (Panel), 监控 (Monitoring), 策略 (Policy), 网络 (Network), 系统 (System) (highlighted with a red box), admin, 提交 (Submit), 保存 (Save), and other system icons.

The main content area shows the '双机热备' (Dual Homing Backup) configuration. A red box highlights the '配置' (Configure) button under the '双机热备' section. A red circle with the number '1' is on the '系统' icon in the top navigation. A red circle with the number '2' is on the '双机热备' link in the sidebar. A red circle with the number '3' is on the '配置' button. A blue callout bubble with the text 'FW_A设置为负载分担模式' (FW_A is set to Load Balancing mode) points to the configuration area. A red box surrounds the '双机热备' configuration panel, which includes fields for '运行模式' (Operation Mode) (selected: 负载分担 Load Sharing), '心跳接口' (Heartbeat Interface) (GE0/0/2), 'IP地址' (IP Address) (10.10.0.1), '对端接口IP' (Peer Interface IP) (10.10.0.2), '主动抢占' (Preemptive夺回) (Enabled), '静态路由自动备份' (Automatic Backup of Static Routes) (Disabled), '策略路由自动备份' (Automatic Backup of Policy Routes) (Disabled), and 'Hello报文周期' (Hello Message Period) (1000 ms). Below this is the '配置监控对象' (Configure Monitoring Object) section, which includes tabs for 接口监控 (Interface Monitoring), VRRP监控 (VRRP Monitoring), IP-Link监控 (IP-Link Monitoring), BFD监控 (BFD Monitoring), OSPF监控 (OSPF Monitoring), and BGP监控 (BGP Monitoring). A red box highlights the 'VLAN' tab under '接口监控'. A blue callout bubble with the text '配置VLAN监控: 选择接口类型为VLAN, 设置VLAN ID为2, 单击添加按钮' (Configure VLAN monitoring: Select interface type as VLAN, set VLAN ID to 2, click the add button) points to the 'VLAN' tab. A red box highlights the 'VLAN' dropdown and the '添加' (Add) button. A red circle with the number '4' is on the 'VLAN' tab. A red circle with the number '5' is on the '添加' button. At the bottom right are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 11：防火墙透明接入的负载分担场景

Step4 配置FW_B为负载分担模式

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes the HUAWEI logo, user information (admin), and tabs for Dashboard, Monitoring, Policies, Networks, and System. The System icon is highlighted with a red box and a red number 1.

The left sidebar menu is expanded, showing the '双机热备' (Dual-Hotstandby) section under '配置' (Configuration). A red box labeled 2 highlights the '双机热备' section. A red box labeled 3 highlights the '配置' (Configure) button in the '双机热备' list.

The main content area displays the 'Configure Dual-Hotstandby' dialog box. It shows the '双机热备' (Dual-Hotstandby) section with a red box around it. The '运行模式' (Operation Mode) is set to '负载分担' (Load Balancing). A callout 4 indicates that 'FW_B is set to Load Balancing mode'. The '心跳接口' (Heartbeat Interface) is set to 'GE0/0/2'. The 'IP地址' (IP Address) is '10.10.0.2' and the '对端接口IP' (Peer Interface IP) is '10.10.0.1'. The 'Hello报文周期' (Hello Message Period) is '1000' ms.

Below the main dialog, there is a '监控对象' (Monitoring Object) configuration section with a red box around it. It shows a table for monitoring interfaces. A callout 5 indicates that 'Configure VLAN monitoring: select interface type as VLAN, set VLAN ID to 2, and click the add button.' The table lists '接口名称 | VLAN' (Interface Name | VLAN) as 'vlan 2' with a green status indicator.

At the bottom right of the dialog, there are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 11：防火墙透明接入的负载分担场景

Step5 配置FW_A的安全策略（1）

1. 在HUAWEI防火墙管理界面中，进入“策略”模块。

2. 在左侧导航栏中，选择“安全策略”。

3. 点击“新建安全策略”按钮。

4. 在“新建安全策略”对话框中，配置第一个策略（policy_ospf_1）：

- 名称：policy_ospf_1
- 源安全区域：trust
- 目的安全区域：untrust
- 源地址/地区：10.3.0.1/32, 10.3.1.1/32
- 目的地址/地区：10.3.0.2/32, 10.3.1.2/32
- VLAN ID：请输入 VLAN ID <1-4094>
- 服务：ospf
- 动作：允许

5. 在“新建安全策略”对话框中，配置第二个策略（policy_ospf_2）：

- 名称：policy_ospf_2
- 源安全区域：untrust
- 目的安全区域：trust
- 源地址/地区：10.3.0.2/32, 10.3.1.2/32
- 目的地址/地区：10.3.0.1/32, 10.3.1.1/32
- VLAN ID：请输入 VLAN ID <1-4094>
- 服务：ospf
- 动作：允许

配置允许OSPF报文通过FW。

Example 11：防火墙透明接入的负载分担场景

Step5 配置FW_A的安全策略（2）

The screenshot shows the HUAWEI Firewall Management System interface. The top navigation bar includes icons for Home, Panel, Monitoring, Policies (highlighted with a red box), Objects, Networks, and System. The left sidebar menu is expanded under '安全策略' (Security Policies) with options like '安全策略' (selected and highlighted with a red box), '策略冗余分析', '策略命中分析', '应用风险调优', 'NAT策略', '服务器负载均衡', '带宽管理', '代理策略', '加密流量检测', '流探针', '安全防护', and 'ASPF配置'. The main content area is titled '安全策略列表' (Security Policy List). A red circle labeled '1' points to the '新建安全策略' (Create New Security Policy) button. A red box highlights the '新建安全策略' button. A red circle labeled '2' points to the '安全策略' option in the sidebar. A red circle labeled '3' points to the search bar. A red box highlights the search bar. A red circle labeled '4' points to a callout bubble containing the text: '配置策略，允许内网用户访问外网IP地址。' (Configure the policy to allow internal network users to access external network IP addresses.) The bottom right corner of the interface has a 'CLI 控制台' (CLI Console) button.

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。 [选择策略模板](#)

常规设置

- 名称: policy_sec *
- 描述:
- 策略组: -- NONE --
- 标签: 请选择或输入标签

源与目的

- 源安全区域: trust
- 目的安全区域: untrust
- 源地址/地区: 10.3.2.0/24 × 10.3.3.0/24 ×
- 目的地址/地区: 请选择或输入地址
- VLAN ID: 请输入 VLAN ID <1-4094>

用户与服务

- 用户: any; 接入方式: any; 终端设备: any; 服务: any; 应用: any; URL分类: any; 时间段: any;

动作设置

- 动作: 允许 禁止

内容安全

- 反病毒: NONE; 入侵防御: NONE; URL过滤: NONE; 文件过滤: NONE; 内容过滤: NONE; 应用行为控制: NONE; 云接入安全感知: NONE; 邮件过滤: NONE; APT防御: NONE; DNS过滤: NONE;

其他选项

- 记录流量日志: NONE; 记录策略命中日志: 禁用; 记录会话日志: 禁用; 会话老化时间: NONE; 自定义长连接: 禁用;

底部按钮: 确定, 确定并复制, 命令预览, 取消

Example 11：防火墙透明接入的负载分担场景

Step6 结果验证（1）

配置成功后，分别查看 FW_A 和 FW_B 双机热备的运行状况，能够看到 FW_A 和 FW_B 已成功建立负载分担，流量通过两台 FW 共同转发。

FW_A



The screenshot shows the HUAWEI Firewall Management System interface for FW_A. The left sidebar is collapsed, and the main menu bar includes: 面板 (Dashboard), 监控 (Monitoring), 策略 (Policy), 对象 (Object), 网络 (Network), and 系统 (System). The top right corner shows the user is 'admin' with tabs for '提交' (Submit), '保存' (Save), and '...' (More). Below the top bar, it says '虚拟系统 public'. The central panel displays the '双机热备' (Dual-Homing) configuration under the '配置' (Configuration) tab. A red box highlights the '监控项' (Monitoring Items) section, which shows the following details:

	当前状态	详细
当前运行模式	负载分担	
当前运行角色	主用 (切换后运行的时间: 1 天 13 时 20 分)	详细
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)	
主动抢占	已启用	
配置一致性 (检测时间: 0/0/0 00:00:00)		详细 一致性检查
接口监控 (接口名称 VLAN) vlan2	 up	

FW_B



The screenshot shows the HUAWEI Firewall Management System interface for FW_B. The layout is identical to FW_A, with the same menu bar and top right settings. The central panel displays the '双机热备' (Dual-Homing) configuration under the '配置' (Configuration) tab. A red box highlights the '监控项' (Monitoring Items) section, which shows the following details:

	当前状态	详细
当前运行模式	负载分担	
当前运行角色	主用 (切换后运行的时间: 1 天 13 时 20 分)	详细
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)	
主动抢占	已启用	
配置一致性 (检测时间: 0/0/0 00:00:00)		详细 一致性检查
接口监控 (接口名称 VLAN) vlan2	 up	

Example 11：防火墙透明接入的负载分担场景

Step6 结果验证（2）

FW_A出现故障，FW_A切换成主备备份模式的备用设备，FW_B切换成主备备份模式的主用设备，流量通过FW_B正常转发。

FW_A：设备故障后切换成主备备份模式的备用设备



The screenshot shows the HUAWEI firewall configuration interface. The left sidebar menu is expanded to show '双机热备' (Dual-Hotstandby) under '高可靠性'. The main panel displays the '双机热备' configuration page. A red box highlights the '监控项' (Monitoring Items) section. Key details shown include:

- 当前运行模式:** 主备备份 (Primary-backup mode)
- 当前运行角色:** 备用 (Switched to backup role after 1 day 13 hours 20 minutes)
- 当前心跳接口:** GE0/0/2 (带宽使用率: 0.00%)
- 主动抢占:** 已启用 (Enabled)
- 配置一致性:** 初始 (检测时间: 0/0/0 00:00:00)
- 接口监控:** 显示了GE0/0/2和VLAN2的监控状态。GE0/0/2显示为Down接口，VLAN2显示为Down状态。

FW_B：切换成主备备份模式的主用设备，转发流量

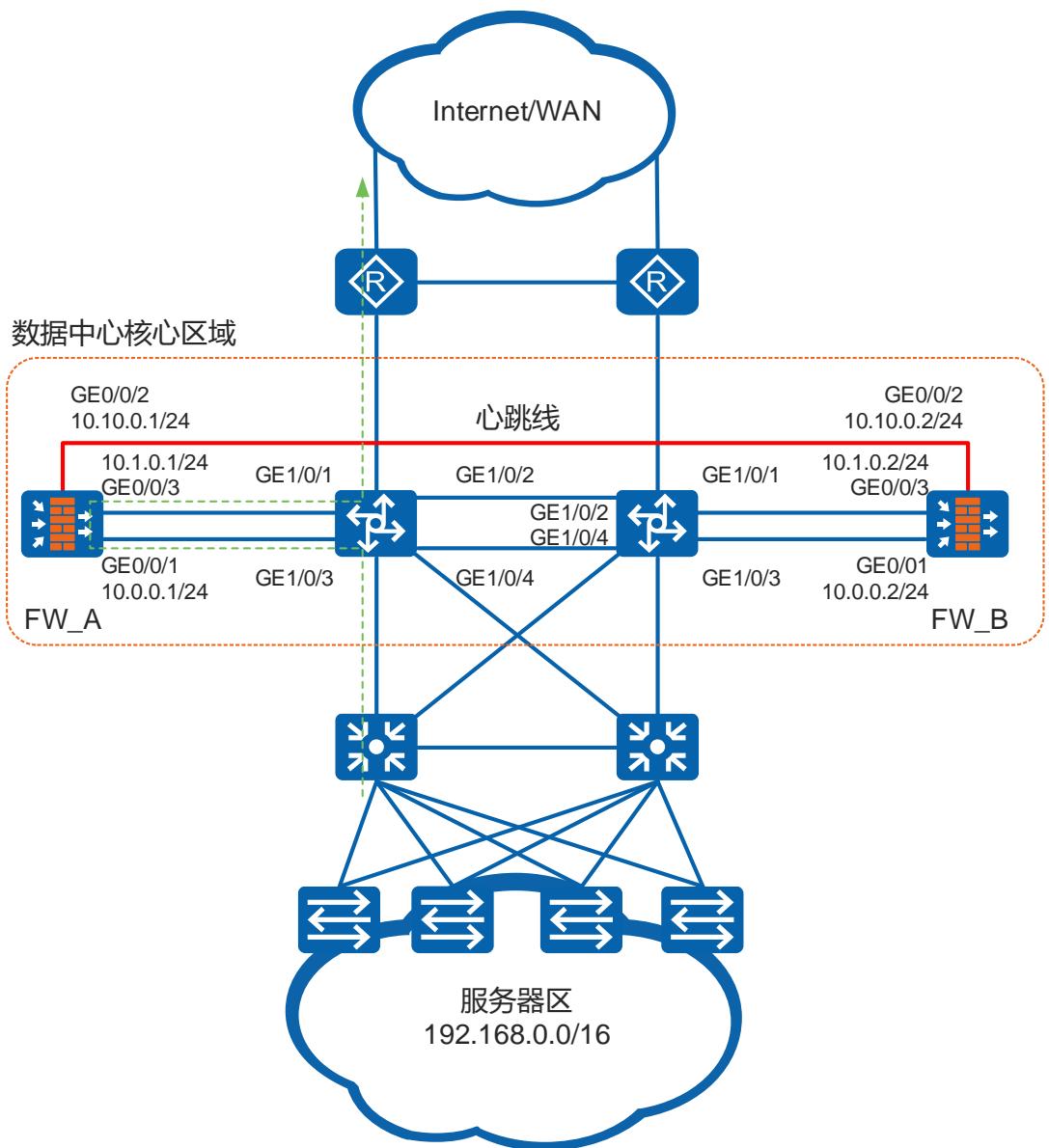


The screenshot shows the HUAWEI firewall configuration interface. The left sidebar menu is expanded to show '双机热备' under '高可靠性'. The main panel displays the '双机热备' configuration page. A red box highlights the '监控项' (Monitoring Items) section. Key details shown include:

- 当前运行模式:** 主备备份 (Primary-backup mode)
- 当前运行角色:** 主用 (Switched to primary role after 1 day 13 hours 20 minutes)
- 当前心跳接口:** GE0/0/2 (带宽使用率: 0.00%)
- 主动抢占:** 已启用 (Enabled)
- 配置一致性:** 初始 (检测时间: 0/0/0 00:00:00)
- 接口监控:** 显示了GE0/0/2和VLAN2的监控状态。GE0/0/2显示为up状态，VLAN2显示为up状态。

Example 12: 防火墙旁挂在三层设备上的主备备份场景

组网图



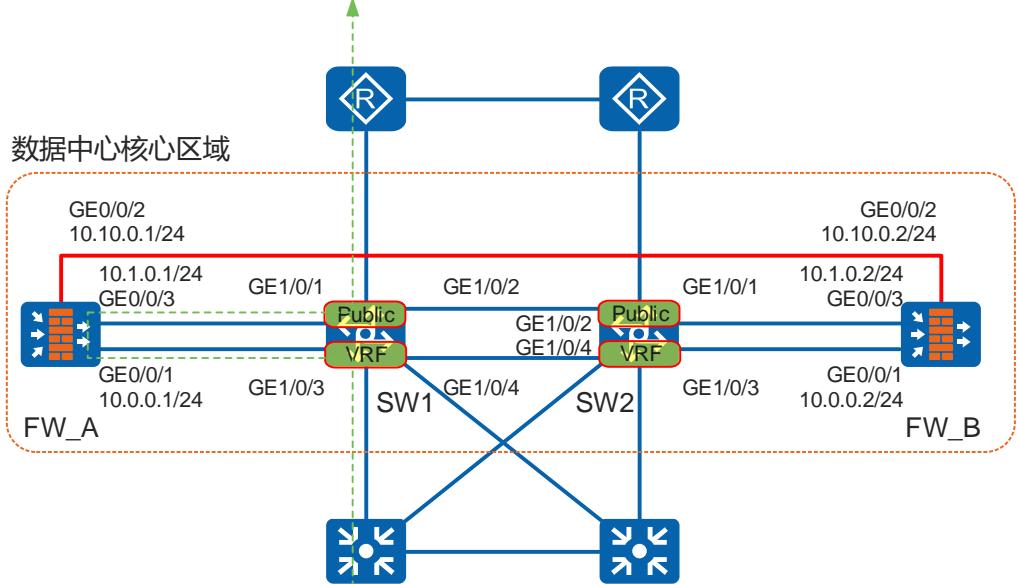
两台FW旁挂在数据中心的核心交换机侧，保证数据中心网络安全。通过核心交换机的流量都会被引流到旁挂的FW上进行安全检测，引流的方式为静态路由方式。企业希望两台FW以主备备份方式工作。正常情况下，流量通过FW_A转发。当FW_A出现故障时，流量通过FW_B转发，保证业务不中断。

项目	FW_A	FW_B
运行模式	主备备份	主备备份
运行角色	主用设备	备用设备
心跳接口	GE0/0/2 10.10.0.1/24	GE0/0/2 10.10.0.2/24

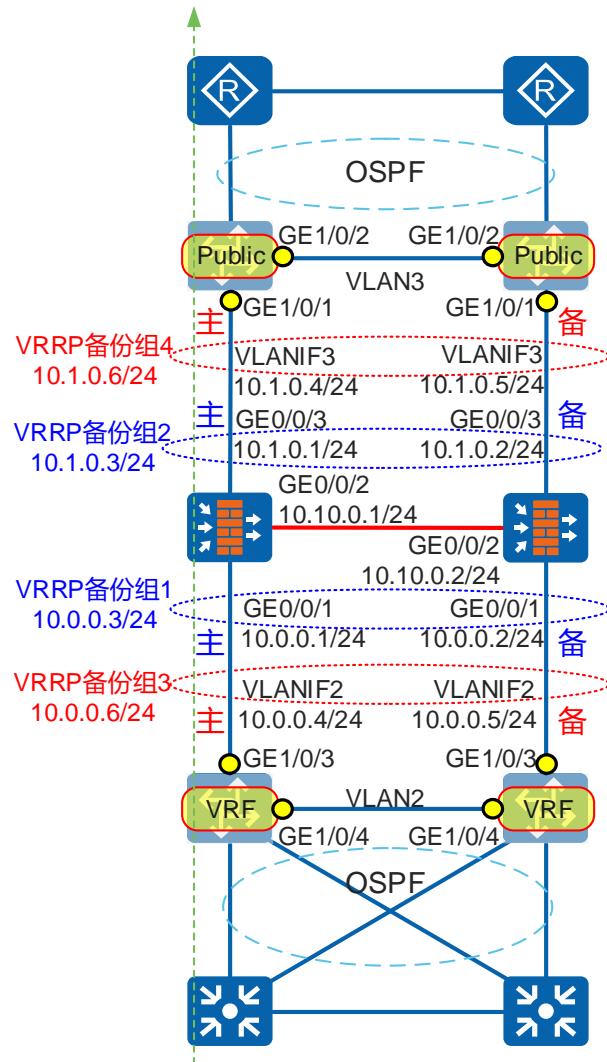
Example 12：防火墙旁挂在三层设备上的主备备份场景

组网图

如下图所示，在核心交换机上配置VRF功能，将一台交换机虚拟成连接上行的交换机（根交换机Public）和连接下层的交换机（虚拟交换机VRF）。



防火墙和交换机均采用VRRP实现链路备份，防火墙和交换机的VRRP备份组配置如下图所示。



Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step1 配置FW_A的接口 (1)

1. 在HUAWEI USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“接口”选项。

3. 在右侧列表中，选择要配置的上行接口（GE0/0/1）。

4. 在下方的“修改GigabitEthernet”对话框中，配置下行接口参数。设置接口名称为“GigabitEthernet0/0/1”，虚拟系统为“public”，安全区域为“trust”，模式为“路由”，连接类型为“静态IP”，IP地址为“10.0.0.1/24”。注意：输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

5. 在右侧列表中，选择要配置的下行接口（GE0/0/3）。

6. 在下方的“修改GigabitEthernet”对话框中，配置上行接口参数。设置接口名称为“GigabitEthernet0/0/3”，虚拟系统为“public”，安全区域为“untrust”，模式为“路由”，连接类型为“静态IP”，IP地址为“10.1.0.1/24”。注意：输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step1 配置FW_A的接口 (2)

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI', '网络' (Network), and 'admin'. The left sidebar has a '接口' (Interface) section with various network components like DNS, DHCP, and L2TP.

The main interface displays a table of interfaces. A red circle labeled '1' is on the 'GE0/0/2' row. A red box labeled '2' is on the '接口' tab. A red box labeled '3' is on the '编辑' (Edit) button for the 'GE0/0/2' row. A blue callout box labeled '4' points to the '修改GigabitEthernet' dialog for 'GE0/0/2'.

The '修改GigabitEthernet' dialog shows the following configuration for 'GigabitEthernet0/0/2':

- 接口名称: GigabitEthernet0/0/2
- 别名:
- 虚拟系统: public
- 安全区域: dmz
- 模式: 路由 (selected)
- IPv4 tab selected
- 连接类型: 静态IP (selected)
- IP地址: 10.10.0.1/24
- 提示: 一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。
- 默认网关:
- 首选DNS服务器:
- 备用DNS服务器:
- 多出口选项:

At the bottom right of the dialog are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step2 配置FW_B的接口（1）

The screenshot shows the HUAWEI USG6300 network management interface. The top navigation bar includes icons for Home, Panels, Monitoring, Objects, Network (highlighted with a red box and number 1), and System. On the far right, there are user information (admin), and system status (提交 提交, 保存 Save, 虚拟系统 Virtual System, public) buttons.

The left sidebar contains a tree view of network components: Interface (highlighted with a red box and number 2), Interface Pairs, Security Zones, DNS, DHCP Server, Routes, IPSec, L2TP, L2TP over IPSec, GRE, DSVPN, and SSL VPN.

The main interface is titled "Interface List". It displays a table with columns: Interface Name, Security Zone, Virtual System, IP Address, Connection Type, VLAN, Mode, Status (Physical, IPv4, IPv6), and Edit (with a red box and number 3). The table lists interfaces GE0/0/0(GE0/MGMT), GE0/0/1, GE0/0/2, GE0/0/3, GE0/0/4, GE0/0/5, and GE0/0/6.

Two large blue callout boxes provide instructions:

- Box 4: 配置下行接口参数 (Configure downstream interface parameters) points to the configuration for GE0/0/1.
- Box 6: 配置上行接口参数 (Configure upstream interface parameters) points to the configuration for GE0/0/3.

Below the interface list are two configuration dialog boxes:

- 修改GigabitEthernet** (Modify GigabitEthernet): This dialog is for GE0/0/1. It shows fields for Interface Name (GigabitEthernet0/0/1), Alias, Virtual System (public), Security Zone (trust), Mode (Route selected), Connection Type (Static IP selected), IP Address (10.0.0.2/24), Subnet Mask (255.255.255.0), Default Gateway, Primary DNS Server, Secondary DNS Server, and Multi-Exit Options. A note indicates: "一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”" (One line per record, input format: "1.1.1.1/255.255.255.0" or "1.1.1.1/24").
- 修改GigabitEthernet** (Modify GigabitEthernet): This dialog is for GE0/0/3. It shows fields for Interface Name (GigabitEthernet0/0/3), Alias, Virtual System (public), Security Zone (untrust), Mode (Route selected), Connection Type (Static IP selected), IP Address (10.1.0.2/24), Subnet Mask (255.255.255.0), Default Gateway, Primary DNS Server, Secondary DNS Server, and Multi-Exit Options. A note indicates: "一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”" (One line per record, input format: "1.1.1.1/255.255.255.0" or "1.1.1.1/24").

At the bottom right are "确定" (Confirm) and "取消" (Cancel) buttons.

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step2 配置FW_B的接口 (2)

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes the HUAWEI logo, user information (admin), and tabs for 面板 (Dashboard), 监控 (Monitoring), 对象 (Objects), 网络 (Network) [highlighted with a red box], and 系统 (System). Below the dashboard, the '接口' (Interface) tab is selected, indicated by a red box with the number 2. A red box with the number 1 highlights the '网络' tab in the top navigation.

The main interface displays a table of interfaces. A red box with the number 3 highlights the edit icon for the GE0/0/2 interface. A blue callout bubble with the text '配置心跳接口参数' (Configure heartbeat interface parameters) points to the edit icon. A red box with the number 4 highlights the '修改GigabitEthernet' (Modify GigabitEthernet) dialog box.

The '修改GigabitEthernet' dialog box contains the following fields:

- 接口名称: GigabitEthernet0/0/2
- 别名: (empty)
- 虚拟系统: public
- 安全区域: dmz
- 模式: 路由 (selected)
- IPv4 tab is selected
- 连接类型: 静态IP (selected)
- IP地址: 10.10.0.2/24
- 提示: 一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”
- 默认网关: (empty)
- 首选DNS服务器: (empty)
- 备用DNS服务器: (empty)
- 多出口选项: (unchecked)

At the bottom right of the dialog box are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step3 配置FW_A的静态路由

1. 在HUAWEI USG6300管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“静态路由”。

3. 点击“新建”按钮，开始配置上行方向静态路由。

4. 在“新建静态路由”对话框中，配置如下参数：

协议类型	<input checked="" type="radio"/> IPv4	<input type="radio"/> IPv6	
源虚拟路由器	public		
目的地址/掩码	0.0.0.0/0.0.0.0	*	
目的虚拟路由器	public		
出接口	-- NONE --		
下一跳	10.1.0.6		
优先级	60	<1-255>	
可靠性检测	<input checked="" type="radio"/> 不检测	<input type="radio"/> 绑定BFD	<input type="radio"/> 绑定IP-Link

5. 在“新建静态路由”对话框中，配置如下参数（与步骤4相同）：

协议类型	<input checked="" type="radio"/> IPv4	<input type="radio"/> IPv6	
源虚拟路由器	public		
目的地址/掩码	192.168.0.0/255.255.0.0	*	
目的虚拟路由器	public		
出接口	-- NONE --		
下一跳	10.0.0.6		
优先级	60	<1-255>	
可靠性检测	<input checked="" type="radio"/> 不检测	<input type="radio"/> 绑定BFD	<input type="radio"/> 绑定IP-Link

6. 点击“确定”，完成配置。

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step4 配置FW_B的静态路由

1. 在HUAWEI USG B5200管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“静态路由”。

3. 点击“新建”按钮，开始配置上行方向静态路由。

4. 在“新建静态路由”对话框中，配置如下参数：

协议类型	<input checked="" type="radio"/> IPv4	<input type="radio"/> IPv6	
源虚拟路由器	public		
目的地址/掩码	0.0.0.0/0.0.0.0	*	
目的虚拟路由器	public		
出接口	-- NONE --		
下一跳	10.1.0.6		
优先级	60	<1-255>	
可靠性检测	<input checked="" type="radio"/> 不检测	<input type="radio"/> 绑定BFD	<input type="radio"/> 绑定IP-Link

5. 在“新建静态路由”对话框中，配置如下参数（与步骤4相同）：

协议类型	<input checked="" type="radio"/> IPv4	<input type="radio"/> IPv6	
源虚拟路由器	public		
目的地址/掩码	192.168.0.0/255.255.0.0	*	
目的虚拟路由器	public		
出接口	-- NONE --		
下一跳	10.0.0.6		
优先级	60	<1-255>	
可靠性检测	<input checked="" type="radio"/> 不检测	<input type="radio"/> 绑定BFD	<input type="radio"/> 绑定IP-Link

6. 点击“确定”，完成配置。

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step5 配置FW_A为主备备份模式

The screenshot shows the HUAWEI Network Management System interface. The main window displays the 'System' configuration page under the 'Dual-link Backup' section. A red box highlights the configuration tab. A blue callout box labeled '4' indicates that FW_A is set as the primary backup device. Two smaller blue callout boxes labeled '6' and '7' show the configuration of VRRP backup groups 1 and 2 respectively.

1 点击系统图标进入系统配置。

2 在左侧菜单栏中选择“双机热备”。

3 在“双机热备”配置页中，点击“配置”选项卡。

4 FW_A设置为主备备份的主用设备。

5 在VRRP监控界面，点击“新建”按钮。

6 配置VRRP备份组1的虚拟IP地址。

7 配置VRRP备份组2的虚拟IP地址。

配置双机热备

双机热备

运行模式 ② 主备备份 负载分担

运行角色 ② 主用 备用

提示：双机热备的协议报文不受安全策略控制

心跳接口 ② GE0/0/2 * [配置] IP地址 10.10.0.1 * 对端接口IP 10.10.0.2 *

主动抢占 ②

静态路由自动备份 ②

策略路由自动备份 ②

Hello报文周期 ② 1000 <500-60000>毫秒

配置监控对象 ②

接口监控 VRRP监控 IP-Link监控 BFD监控 OSPF监控 BGP监控

提示：当业务接口工作在三层且连接交换机时，需要配置VRRP备份组。

新建 删除

VRID ② 1 *-<1-255>

接口 GE0/0/1 * [配置]

接口IP地址/掩码 10.0.0.1/24 *

虚拟IP地址/掩码 ② 10.0.0.3/24 *

虚拟MAC ②

每页 50 确定 取消

新建虚拟IP地址

VRID ② 2 *-<1-255>

接口 GE0/0/3 * [配置]

接口IP地址/掩码 10.1.0.1/24 *

虚拟IP地址/掩码 ② 10.1.0.3/24 *

虚拟MAC ②

每页 50 确定 取消

新建虚拟IP地址

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step6 配置FW_B为主备备份模式

1. 在系统菜单中选择“双机热备”配置。

2. 在左侧菜单栏中选择“双机热备”。

3. 在“双机热备”配置界面中，选择“配置”选项卡。

4. FW_B设置为主备备份的备用设备。

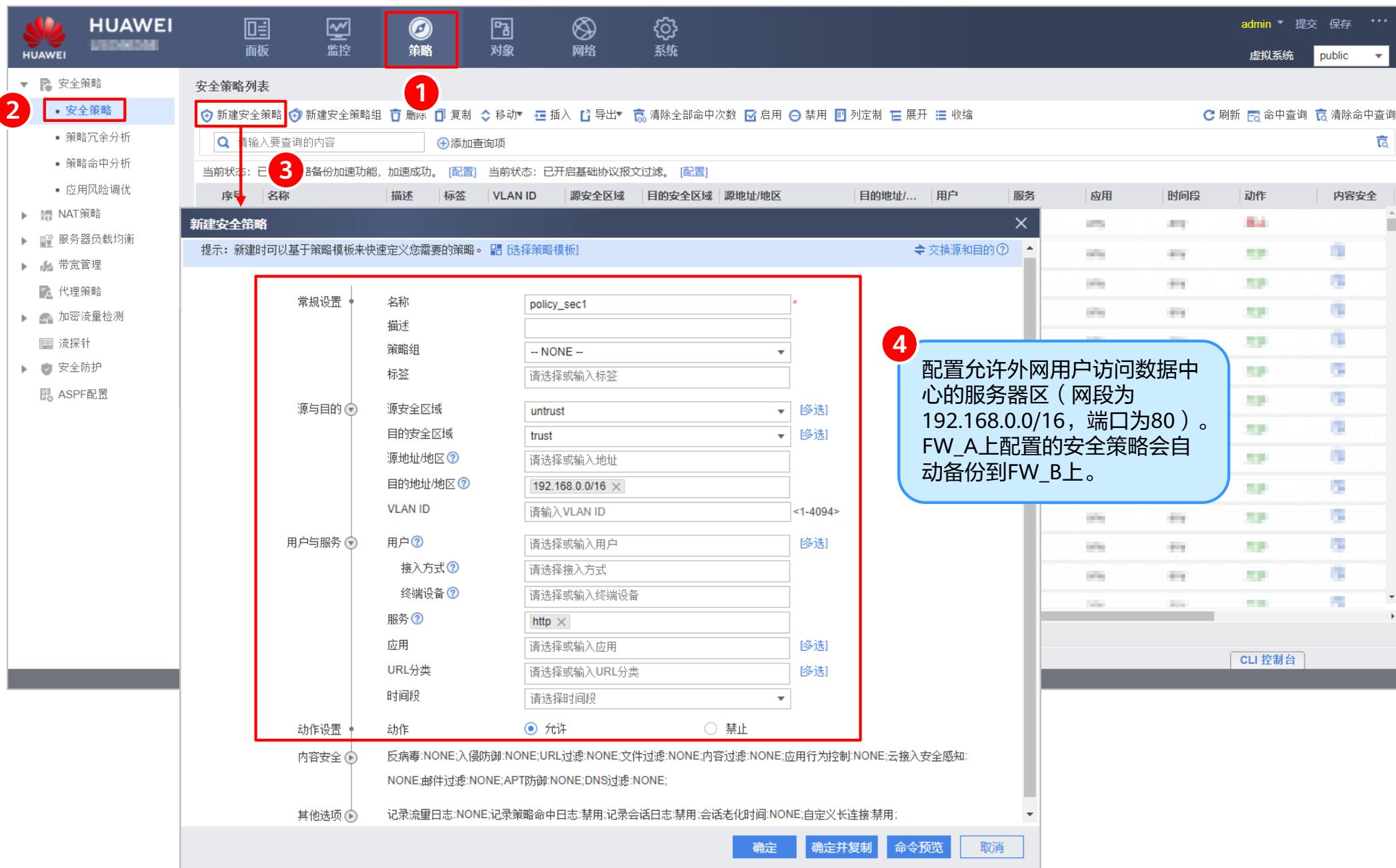
5. 在VRRP监控界面中，点击“新建”按钮。

6. 配置VRRP备份组1的虚拟IP地址。

7. 配置VRRP备份组2的虚拟IP地址。

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step7 配置FW_A的安全策略



The screenshot shows the HUAWEI Firewall Management System interface. The top navigation bar includes icons for Home, Dashboard, Monitoring, Policies (highlighted with a red box), Objects, Networks, and System. On the far right, there are user authentication (admin), save (保存), and other system settings.

The left sidebar menu is expanded under the 'Security Policies' section, with 'Policy Configuration' selected. A secondary menu on the left shows 'Policy Configuration' is also selected.

The main content area displays the 'Policy List' with a search bar and various filter options. A message at the top states: 'Current status: Policy backup acceleration function has been successfully enabled. [Configure] Current status: Basic protocol报文 filtering is enabled. [Configure]'.

A modal window titled 'Create New Policy' is open. It contains several sections:

- General Settings:** Name: policy_sec1, Description: (empty), Policy Group: --NONE--, Tag: (empty).
- Source and Destination:** Source Security Zone: untrust, Destination Security Zone: trust, Source Address/Region: (empty), Destination Address/Region: 192.168.0.0/16, VLAN ID: (empty).
- User and Service:** User: (empty), Access Method: (empty), Terminal Device: (empty), Service: http, Application: (empty), URL Category: (empty), Time Period: (empty).
- Action Settings:** Action: Allow (radio button selected).
- Content Security:** Content security rules: None.
- Other Options:** Record flow log: None; Record policy命中日志: None; Ban: None; Record session log: None; Ban: None; Session aging time: None; Custom long connection: None; Ban: None.

Numbered callouts point to specific elements:

- Red box around the 'Policies' icon in the top navigation bar.
- Red box around the 'Policy Configuration' item in the left sidebar.
- Red box around the 'Create New Policy' button in the top-left of the main content area.
- A blue callout box points to the 'Action' setting in the 'Action Settings' section, containing the following text:

配置允许外网用户访问数据中心的服务器区（网段为192.168.0.0/16，端口为80）。FW_A上配置的安全策略会自动备份到FW_B上。

Example 12：防火墙旁挂在三层设备上的主备备份场景

Step8 配置核心交换机（1）

配置Switch1。

```
[Switch1] ip vpn-instance VRF //创建VRF
[Switch1-vpn-instance-VRF] ipv4-family
[Switch1-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[Switch1-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[Switch1-vpn-instance-VRF-af-ipv4] quit
[Switch1-vpn-instance-VRF] quit
[Switch1] vlan 2
[Switch1-vlan2] port gigabitetherent 1/0/3 to 1/0/4 //将接口加入VLAN2
[Switch1-vlan2] quit
[Switch1] interface Vlanif 2
[Switch1-Vlanif2] ip binding vpn-instance VRF //将VLANIF2绑定至VRF
[Switch1-Vlanif2] ip address 10.0.0.4 24
[Switch1-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6 //配置VRRP备份组3
[Switch1-Vlanif2] vrrp vrid 3 priority 120 //配置优先级为120，优先级高的为主用
[Switch1-Vlanif2] quit
[Switch1] vlan 3
[Switch1-vlan3] port gigabitetherent 1/0/1 to 1/0/2 //将接口加入VLAN3
[Switch1-vlan3] quit
[Switch1] interface Vlanif 3
[Switch1-Vlanif3] ip address 10.1.0.4 24
[Switch1-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6 //配置VRRP备份组4
[Switch1-Vlanif3] vrrp vrid 4 priority 120 //配置优先级为120，优先级高的为主用
[Switch1-Vlanif3] quit
[Switch1] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3 //在VRF中配置缺省路由，下一跳为VRRP备份组1的虚拟地址
[Switch1] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3 //在根交换机Public中配置静态路由，下一跳为VRRP备份组2的虚拟地址。
```

该案例中仅提供交换机与
防火墙对接的相关配置。

Example 12：防火墙旁挂在三层设备上的主备备份场景

Step8 配置核心交换机（2）

配置Switch2。

```
[Switch2] ip vpn-instance VRF //创建VRF
[Switch2-vpn-instance-VRF] ipv4-family
[Switch2-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[Switch2-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[Switch2-vpn-instance-VRF-af-ipv4] quit
[Switch2-vpn-instance-VRF] quit
[Switch2] vlan 2
[Switch2-vlan2] port gigabitetherent 1/0/3 to 1/0/4 //将接口加入VLAN2
[Switch2-vlan2] quit
[Switch2] interface Vlanif 2
[Switch2-Vlanif2] ip binding vpn-instance VRF //将VLANIF2绑定至VRF
[Switch2-Vlanif2] ip address 10.0.0.5 24
[Switch2-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6 //配置VRRP备份组3
[Switch2-Vlanif2] vrrp vrid 3 priority 100 //配置优先级为100，优先级低的为备用
[Switch2-Vlanif2] quit
[Switch2] vlan 3
[Switch2-vlan3] port gigabitetherent 1/0/1 to 1/0/2 //将接口加入VLAN3
[Switch2-vlan3] quit
[Switch2] interface Vlanif 3
[Switch2-Vlanif3] ip address 10.1.0.5 24
[Switch2-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6 //配置VRRP备份组4
[Switch2-Vlanif3] vrrp vrid 4 priority 100 //配置优先级为100，优先级低的为备用
[Switch2-Vlanif3] quit
[Switch2] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3 //在VRF中配置缺省路由，下一跳为VRRP备份组1的虚拟地址
[Switch2] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3 //在根交换机Public中配置静态路由，下一跳为VRRP备份组2的虚拟地址
```

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step9 结果验证 (1)

配置成功后，分别查看 FW_A和FW_B双机热备的运行状况，能够看到FW_A是主备备份模式的主用设备，FW_B是主备备份模式的备用设备。

FW_A

FW_A 双机热备 - 配置

监控项	当前状态	详细
当前运行模式	主备备份	
当前运行角色	主用 (切换后运行的时间: 1 天 18 时 33 分)	详细
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)	
主动抢占	已启用	
配置一致性 (②)	初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
▲ 接口监控 (接☐名称 VLAN 品)		
▲ VRRP监控		
10.1.0.3 (GE0/0/3)	绿色勾	主状态
10.0.0.3 (GE0/0/1)	绿色勾	主状态

FW_B

FW_B 双机热备 - 配置

监控项	当前状态	详细
当前运行模式	主备备份	
当前运行角色	备用 (切换后运行的时间: 1 天 18 时 33 分)	详细
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)	
主动抢占	已启用	
配置一致性 (②)	初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
▲ 接口监控 (接☐名称 VLAN 品)		
▲ VRRP监控		
10.1.0.3 (GE0/0/3)	绿色勾	备状态
10.0.0.3 (GE0/0/1)	绿色勾	备状态

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step9 结果验证 (2)

FW_A出现故障，FW_A切换成主备备份模式的备用设备，FW_B切换成主备备份模式的主用设备，流量通过FW_B正常转发。

FW_A: 设备故障后切换成主备备份模式的备用设备

监控项			当前状态	详细
当前运行模式			主备备份	
当前运行角色			备用 (切换后运行的时间: 1天 18时 33分)	详细
当前心跳接口			GE0/0/2 (带宽使用率: 0.00%)	
主动抢占			已启用	
配置一致性			初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
接口监控 (接☐名称 VLAN号)				
10.1.0.3 (GE0/0/3)		×	备状态 (应该是“主状态”)	
10.0.0.3 (GE0/0/1)		×	初始化	

FW_B: 切换成主备备份模式的主用设备，转发流量

监控项			当前状态	详细
当前运行模式			主备备份	
当前运行角色			主用 (切换后运行的时间: 1天 18时 33分)	详细
当前心跳接口			GE0/0/2 (带宽使用率: 0.00%)	
主动抢占			已启用	
配置一致性			初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
接口监控 (接☐名称 VLAN号)				
10.1.0.3 (GE0/0/3)		×	主状态 (应该是“备状态”)	
10.0.0.3 (GE0/0/1)		×	主状态 (应该是“备状态”)	

Example 12: 防火墙旁挂在三层设备上的主备备份场景

Step9 结果验证 (3)

FW_A故障恢复后，FW_A主动抢占恢复成主备备份模式的主用设备，FW_B切换成主备备份模式的备用设备，流量通过FW_A正常转发。

FW_A: 主动抢占恢复成主备备份模式的主用设备

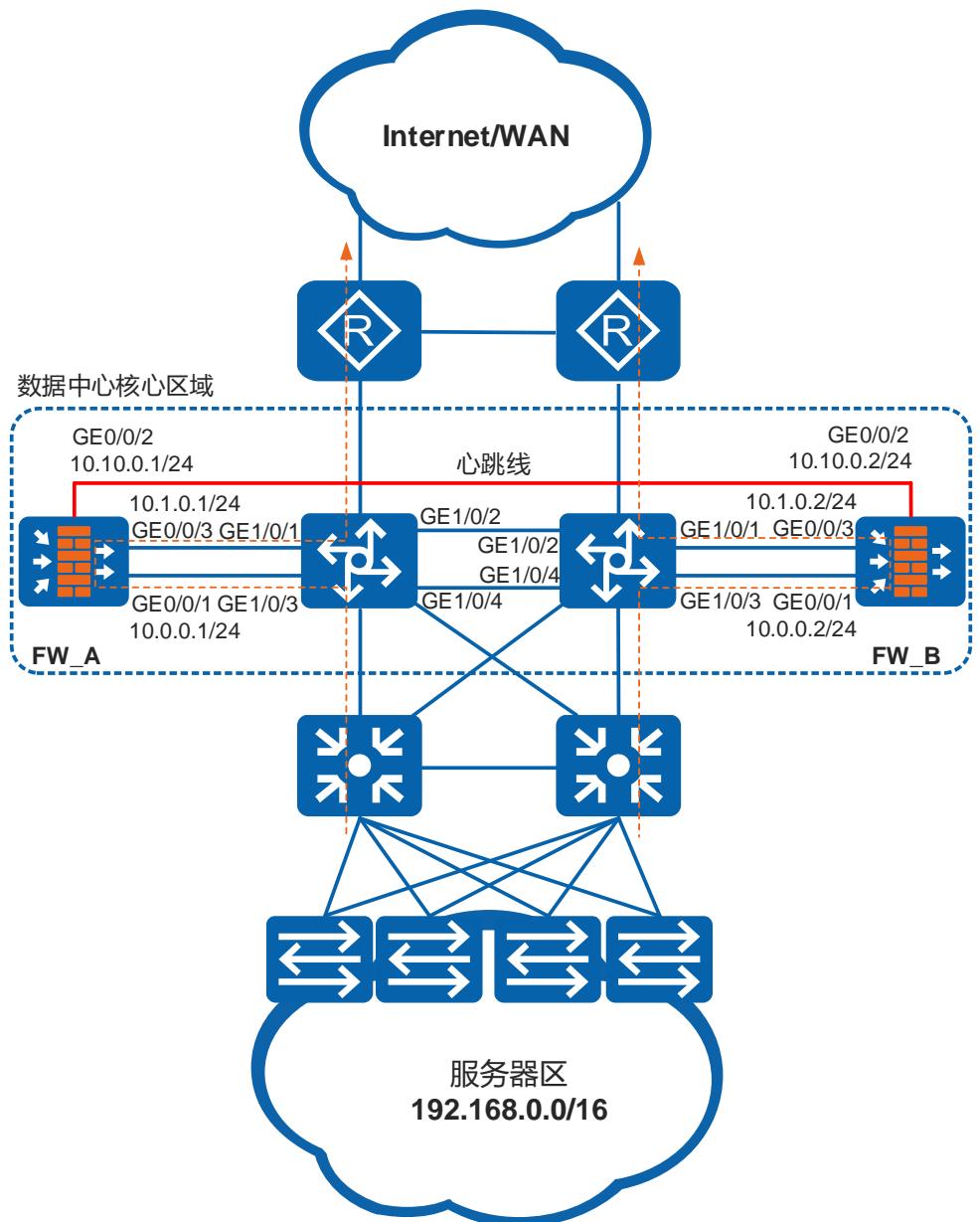
监控项			当前状态	详细
当前运行模式			主备备份	
当前运行角色			主用 (切换后运行的时间: 1 天 18 时 33 分)	详细
当前心跳接口			GE0/0/2 (带宽使用率: 0.00%)	
主动抢占			已启用	
配置一致性			初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
▲ 接口监控	(接口名称 VLAN)			
▲ VRRP监控				
10.1.0.3 (GE0/0/3)			主状态	
10.0.0.3 (GE0/0/1)			主状态	

FW_B: 切换成主备备份模式的备用设备

监控项			当前状态	详细
当前运行模式			主备备份	
当前运行角色			备用 (切换后运行的时间: 1 天 18 时 33 分)	详细
当前心跳接口			GE0/0/2 (带宽使用率: 0.00%)	
主动抢占			已启用	
配置一致性			初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
▲ 接口监控	(接口名称 VLAN)			
▲ VRRP监控				
10.1.0.3 (GE0/0/3)			备状态	
10.0.0.3 (GE0/0/1)			备状态	

Example 13: 防火墙旁挂在三层设备上的负载分担场景

组网图



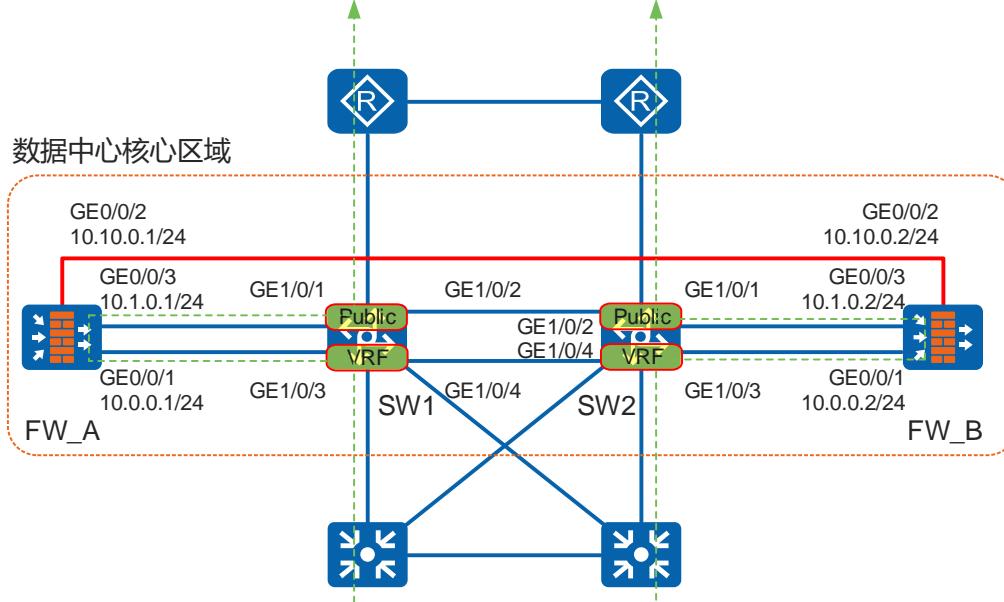
两台FW旁挂在数据中心的核心交换机侧，保证数据中心网络安全。通过核心交换机的流量都会被引流到旁挂的FW上进行安全检测，引流的方式为静态路由方式。企业希望两台FW以负载分担方式工作。正常情况下，FW_A和FW_B共同转发流量。当其中一台FW出现故障时，另外一台FW转发全部业务，保证业务不中断。

项目	FW_A	FW_B
运行模式	负载分担	负载分担
心跳接口	GE0/0/2 10.10.0.1/24	GE0/0/2 10.10.0.2/24

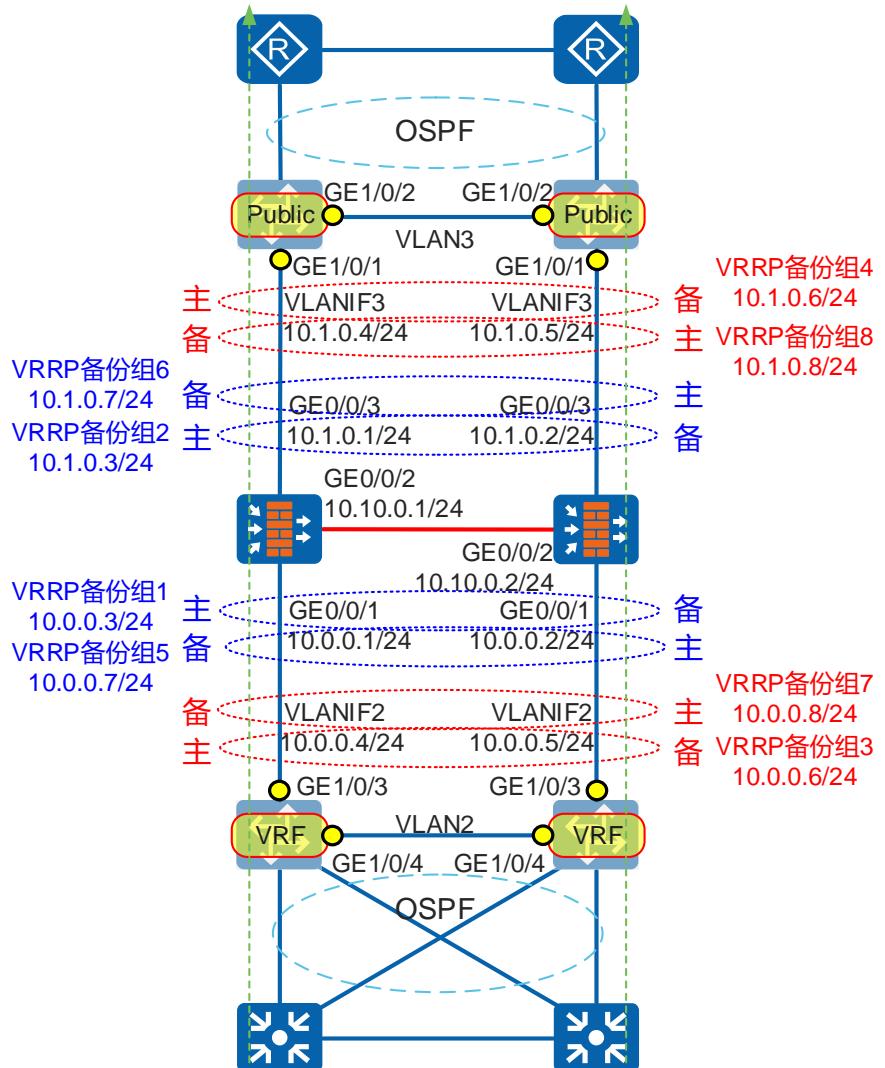
Example 13：防火墙旁挂在三层设备上的负载分担场景

组网图

如下图所示，在核心交换机上配置VRF功能，将一台交换机虚拟成连接上行的交换机（根交换机Public）和连接下层的交换机（虚拟交换机VRF）。



防火墙和交换机均采用VRRP实现链路备份，防火墙和交换机的VRRP备份组配置如下图所示。



Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step1 配置FW_A的接口 (1)

1. 在HUAWEI USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“接口”选项。

3. 在右侧列表中，选择要配置的上行接口（GE0/0/1）。

4. 在下方的“修改GigabitEthernet”对话框中，配置下行接口参数。设置接口名称为“GigabitEthernet0/0/1”，虚拟系统为“public”，安全区域为“trust”，模式为“路由”，连接类型为“静态IP”，IP地址为“10.0.0.1/24”。注意：输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

5. 在右侧列表中，选择要配置的下行接口（GE0/0/3）。

6. 在下方的“修改GigabitEthernet”对话框中，配置上行接口参数。设置接口名称为“GigabitEthernet0/0/3”，虚拟系统为“public”，安全区域为“untrust”，模式为“路由”，连接类型为“静态IP”，IP地址为“10.1.0.1/24”。注意：输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step1 配置FW_A的接口 (2)

1. 在HUAWEI USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“接口”选项。

3. 在右侧列表中，找到并选中要配置的心跳接口（例如：GE0/0/2），然后点击编辑图标。

4. 在弹出的“修改GigabitEthernet”对话框中，完成以下配置：

- 接口名称：GigabitEthernet0/0/2
- 虚拟系统：public
- 安全区域：dmz
- 模式：路由
- 连接类型：静态IP
- IP地址：10.10.0.1/24
- 默认网关、首选DNS服务器、备用DNS服务器：（未填写）
- 多出口选项：（未勾选）

注意：在IP地址输入框下方有提示：“一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。”

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step2 配置FW_B的接口 (1)

1. 在HUAWEI USG6300管理界面中，进入“网络”模块。

2. 在左侧菜单栏中，选择“接口”选项。

3. 在右侧列表中，选择要配置的上行接口（GE0/0/1）。

4. 在下方的“修改GigabitEthernet”对话框中，配置下行接口参数。包括：接口名称（GigabitEthernet0/0/1）、虚拟系统（public）、安全区域（trust）、模式（路由）、连接类型（静态IP）、IP地址（10.0.0.2/24）。

5. 在右侧列表中，选择要配置的下行接口（GE0/0/3）。

6. 在下方的“修改GigabitEthernet”对话框中，配置上行接口参数。包括：接口名称（GigabitEthernet0/0/3）、虚拟系统（public）、安全区域（untrust）、模式（路由）、连接类型（静态IP）、IP地址（10.1.0.2/24）。

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step2 配置FW_B的接口 (2)

1. 在“网络”模块下，进入“接口”列表。

2. 选择要配置的心跳接口，如GE0/0/2。

3. 点击“编辑”按钮。

4. 在“修改GigabitEthernet”对话框中，配置心跳接口参数。

配置界面截图：

参数	值
接口名称	GigabitEthernet0/0/2
别名	
虚拟系统	public
安全区域	dmz
模式	路由
连接类型	静态IP
IP地址	10.10.0.2/24
默认网关	
首选DNS服务器	
备用DNS服务器	
多出口选项	<input type="checkbox"/>

注：一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step3 配置FW_A的静态路由 (1)

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 提交 保存 ...' buttons. The '网络' (Network) icon is highlighted with a red box and a red number '1'. The left sidebar lists '接口' (Interface), '接口对' (Interface Pair), '安全区域' (Security Zone), 'DNS', 'DHCP服务器' (DHCP Server), and '路由' (Route). Under '路由', '静态路由' is selected and highlighted with a red box and a red number '2'. A red arrow points from the '静态路由' button in the sidebar to the '新建' (New) button in the '静态路由列表' (Static Route List) table header. The table has columns: 源虚拟路由器 (Source Virtual Router), 目的地址/掩码 (Destination Address/Mask), 目的虚拟路由器 (Destination Virtual Router), 下一跳 (Next Hop), 优先级 (Priority), 出接口 (Output Interface), 绑定IP-Link名称 (Bind IP-Link Name), 绑定BFD名称 (Bind BFD Name), 描述 (Description), and 编辑 (Edit). A red box and a red number '3' highlight the '新建' button.

新建静态路由 (Left Panel)

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	0.0.0.0/0.0.0.0 *
目的虚拟路由器	public
出接口	-- NONE --
下一跳	10.1.0.6
优先级	60 <1-255>
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link
描述	

新建静态路由 (Right Panel)

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	0.0.0.0/0.0.0.0 *
目的虚拟路由器	public
出接口	-- NONE --
下一跳	10.1.0.8
优先级	60 <1-255>
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link
描述	

Configuration Instructions:

- ④ 在左侧 '新建静态路由' 对话框中配置上行方向静态路由，下一跳为交换机VRRP备份组4的地址。
- ⑤ 在右侧 '新建静态路由' 对话框中配置上行方向静态路由，下一跳为交换机VRRP备份组8的地址。

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step3 配置FW_A的静态路由 (2)

The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes 'HUAWEI' logo, 'admin' dropdown, and '提交 提交 保存 ...' buttons. The '网络' (Network) icon is highlighted with a red box and a red number '1'. The left sidebar lists '接口' (Interface), '接口对' (Interface Pair), '安全区域' (Security Zone), 'DNS', 'DHCP服务器' (DHCP Server), and '路由' (Route). Under '路由', '静态路由' is selected and highlighted with a red box and a red number '2'. The main area shows the '配置默认优先级' (Configure Default Priority) dialog with 'IPv4默认优先级' set to 60 and 'IPv6默认优先级' set to 60. Below it is the '静态路由列表' (Static Route List) table with one entry. A red box and a red number '3' point to the '新建' (New) button in the table header.

新建静态路由 (Left Dialog)

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	192.168.0.0/255.255.0.0 *
目的虚拟路由器	public
出接口	-- NONE --
下一跳	10.0.0.6
优先级	60 <1-255>
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link
描述	

新建静态路由 (Right Dialog)

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	192.168.0.0/255.255.0.0 *
目的虚拟路由器	public
出接口	-- NONE --
下一跳	10.0.0.8
优先级	60 <1-255>
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link
描述	

步骤说明:

- ① 在'配置默认优先级'对话框中设置IPv4和IPv6的默认优先级为60。
- ② 在左侧路由列表中选择'静态路由'。
- ③ 点击'新建'按钮开始配置第一条静态路由。
- ④ 在'新建静态路由'对话框中，配置源虚拟路由器为'public'，目的地址为'192.168.0.0/255.255.0.0'，下一跳为'10.0.0.6'，优先级为60，可靠性检测选择'不检测'。描述框说明：配置下行方向静态路由，下一跳为交换机VRRP备份组3的地址。
- ⑤ 在'新建静态路由'对话框中，配置源虚拟路由器为'public'，目的地址为'192.168.0.0/255.255.0.0'，下一跳为'10.0.0.8'，优先级为60，可靠性检测选择'不检测'。描述框说明：配置下行方向静态路由，下一跳为交换机VRRP备份组7的地址。

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step4 配置FW_B的静态路由 (1)

1 在“配置默认优先级”界面，设置IPv4默认优先级为60。

2 在左侧导航栏中，选择“静态路由”。

3 在“静态路由列表”界面，点击“新建”按钮。

4 在“新建静态路由”对话框（左侧）中，配置如下参数：

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	0.0.0.0/0.0.0.0 *
目的虚拟路由器	public
出接口	-- NONE --
下一跳	10.1.0.6
优先级	60 <1-255>
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link

5 在“新建静态路由”对话框（右侧）中，配置如下参数：

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	0.0.0.0/0.0.0.0 *
目的虚拟路由器	public
出接口	-- NONE --
下一跳	10.1.0.8
优先级	60 <1-255>
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link

4 配置上行方向静态路由，下一跳为交换机VRRP备份组4的地址。

5 配置上行方向静态路由，下一跳为交换机VRRP备份组8的地址。

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step4 配置FW_B的静态路由 (2)

1. 在HUAWEI USG B5200管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“静态路由”。

3. 点击“新建”按钮，进入“新建静态路由”配置界面。

4. 在“新建静态路由”界面中，配置如下参数：

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	192.168.0.0/255.255.0.0 *
目的虚拟路由器	public
出接口	-- NONE --
下一跳	10.0.0.6
优先级	60 <1-255>
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link

5. 在“新建静态路由”界面中，配置如下参数（与步骤4相同）：

协议类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
源虚拟路由器	public
目的地址/掩码	192.168.0.0/255.255.0.0 *
目的虚拟路由器	public
出接口	-- NONE --
下一跳	10.0.0.8
优先级	60 <1-255>
可靠性检测	<input checked="" type="radio"/> 不检测 <input type="radio"/> 绑定BFD <input type="radio"/> 绑定IP-Link

4. 配置下行方向静态路由，下一跳为交换机VRRP备份组3的地址。

5. 配置下行方向静态路由，下一跳为交换机VRRP备份组7的地址。

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step5 配置FW_A为负载分担 (1)

The screenshot shows the HUAWEI Network Management System interface with the following steps highlighted:

- 1**: Click the **系统** (System) button in the top navigation bar.
- 2**: Click the **双机热备** (Dual-link Redundancy) link in the left sidebar.
- 3**: Click the **配置** (Configure) tab in the dual-link redundancy configuration window.
- 4**: FW_A is set to **负载分担** (Load Sharing) mode.
- 5**: Click the **新建** (Create) button in the VRRP backup group configuration window.
- 6**: Configure VRRP backup group 1 virtual IP address.
- 7**: Configure VRRP backup group 2 virtual IP address.

Configuration Details (Step 4):

双机热备 (Dual-link Redundancy) configuration:

- 运行模式**: **负载分担** (Load Sharing) is selected.
- 心跳接口**: GE0/0/2, IP地址: 10.10.0.1, 对端接口IP: 10.10.0.2.
- Hello报文周期**: 1000毫秒.

新建虚拟IP地址 (Create Virtual IP Address) configuration for VRRP backup group 1:

VRID	1
接口	GE0/0/1
接口IP地址/掩码	10.0.0.1/24
虚拟IP地址/掩码	10.0.0.3/24
虚拟MAC	(radio button)
角色	主 (Master)

新建虚拟IP地址 (Create Virtual IP Address) configuration for VRRP backup group 2:

VRID	2
接口	GE0/0/3
接口IP地址/掩码	10.1.0.1/24
虚拟IP地址/掩码	10.1.0.3/24
虚拟MAC	(radio button)
角色	主 (Master)

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step5 配置FW_A为负载分担 (2)

The screenshot shows the HUAWEI Network Management System interface. On the left, the navigation bar includes '双机热备' (Dual-link Redundancy) under '高可靠性' (Reliability). The main window displays the '配置双机热备' (Configure Dual-link Redundancy) dialog. In the '运行模式' (Operation Mode) section, '负载分担' (Load Sharing) is selected. Below it, the '心跳接口' (Heartbeat Interface) is set to 'GE0/0/2' with IP '10.10.0.1' and '对端接口IP' (Peer Interface IP) '10.10.0.2'. The 'Hello报文周期' (Hello Message Period) is set to 1000 ms. The 'VRRP监控' (VRRP Monitoring) tab is active, showing two configuration windows for VRRP backup groups.

配置VRRP备份组5的虚拟IP地址 (8)

VRID	5
接口	GE0/0/1
接口IP地址/掩码	10.0.0.1/24
虚拟IP地址/掩码	10.0.0.7/24
虚拟MAC	
角色	备

配置VRRP备份组6的虚拟IP地址 (9)

VRID	6
接口	GE0/0/3
接口IP地址/掩码	10.1.0.1/24
虚拟IP地址/掩码	10.1.0.7/24
虚拟MAC	
角色	备

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step6 配置FW_B为负载分担（1）

The screenshot shows the HUAWEI Network Management System interface with the following steps highlighted:

- 1** Click the **系统** button in the top navigation bar.
- 2** Click the **双机热备** link in the left sidebar.
- 3** Click the **配置** link in the sub-menu.
- 4** FW_B is set to **负载分担** mode (highlighted by a blue box).
- 5** Click the **新建** button in the VRRP monitoring section.
- 6** Configure VRRP backup group 1's virtual IP address (highlighted by a blue box).
- 7** Configure VRRP backup group 2's virtual IP address (highlighted by a blue box).

Configuration Details (Step 4):

双机热备 configuration:

- 运行模式:** 负载分担 (selected)
- 心跳接口:** GE0/0/2, 配置, IP地址: 10.10.0.2, 对端接口IP: 10.10.0.1
- Hello报文周期:** 1000毫秒

新建虚拟IP地址 (Step 5):

VRID	1
接口	GE0/0/1
接口IP地址/掩码	10.0.0.2/24
虚拟IP地址/掩码	10.0.0.3/24
虚拟MAC	(radio button)
角色	备 (selected)

新建虚拟IP地址 (Step 7):

VRID	2
接口	GE0/0/3
接口IP地址/掩码	10.1.0.2/24
虚拟IP地址/掩码	10.1.0.3/24
虚拟MAC	(radio button)
角色	备 (selected)

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step6 配置FW_B为负载分担 (2)

配置双机热备

双机热备

运行模式 负载分担 提示：默认启用会话快速备份。

心跳接口 GE0/0/2 * IP地址 10.10.0.2 * 对端接口IP 10.10.0.1 *

主动抢占

静态路由自动备份

策略路由自动备份

Hello报文周期 1000 <500-60000>毫秒

配置监控对象

VRRP监控 IP-Link监控 BFD监控 OSPF监控 BGP监控

提示：当业务接口工作在三层且连接交换机时，需要配置VRRP备份组。

配置VRRP备份组5的虚拟IP地址 **8**

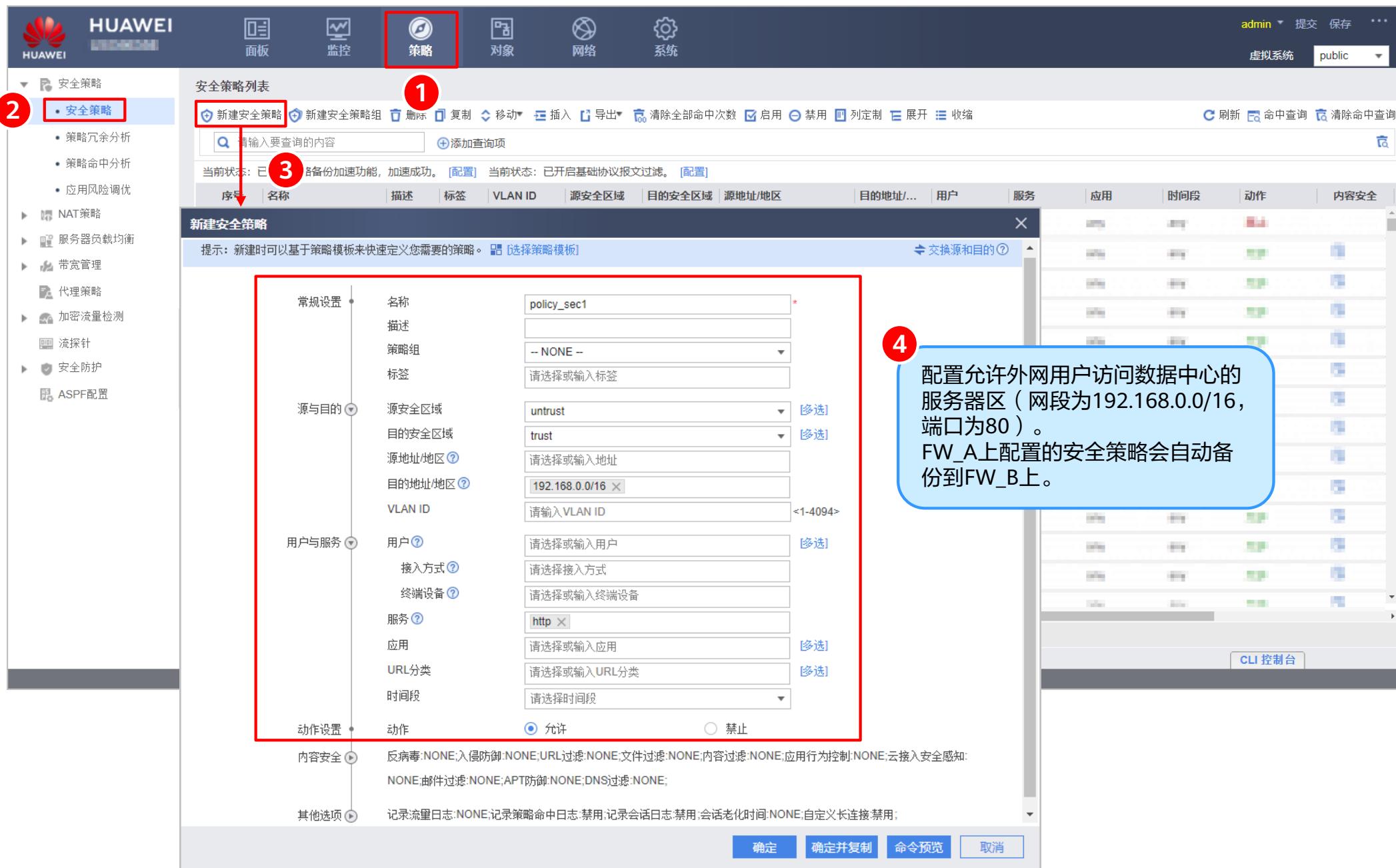
新建虚拟IP地址 VRID 5 接口 GE0/0/1 接口IP地址/掩码 10.0.0.2/24 虚拟IP地址/掩码 10.0.0.7/24 角色 主

配置VRRP备份组6的虚拟IP地址 **9**

新建虚拟IP地址 VRID 6 接口 GE0/0/3 接口IP地址/掩码 10.1.0.2/24 虚拟IP地址/掩码 10.1.0.7/24 角色 主

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step7 配置FW_A的安全策略



The screenshot shows the HUAWEI Firewall configuration interface. The top navigation bar includes the HUAWEI logo, user 'admin', and tabs for 面板 (Dashboard), 监控 (Monitoring), 策略 (Policy), 对象 (Object), 网络 (Network), and 系统 (System). The '策略' tab is highlighted with a red box and a circled '1'. The left sidebar has a tree view with '安全策略' expanded, showing '安全策略' (selected and highlighted with a red box and circled '2') and other options like '策略冗余分析', '策略命中分析', '应用风险调优', 'NAT策略', '服务器负载均衡', '带宽管理', '代理策略', '加密流量检测', '流探针', '安全防护', and 'ASPF配置'. A red box highlights the '新建安全策略' button in the top toolbar, with circled '3' indicating it.

The main area is titled '安全策略列表' (Security Policy List) and displays a table with columns: 序号 (Index), 名称 (Name), 描述 (Description), 标签 (Label), VLAN ID, 源安全区域 (Source Security Zone), 目的区域 (Destination Zone), 源地址/地区 (Source Address/Region), 目的地址/地区 (Destination Address/Region), 用户 (User), 服务 (Service), 应用 (Application), 时间段 (Time Period), 动作 (Action), and 内容安全 (Content Security). A message at the top states: '当前状态: 已 备份加速功能, 加速成功。[配置] 当前状态: 已开启基础协议报文过滤。[配置]'.

A modal window titled '新建安全策略' (Create New Security Policy) is open. It contains a note: '提示: 新建时可以基于策略模板来快速定义您需要的策略。 [选择策略模板]' (Tip: When creating, you can base the policy on a template to quickly define the required policy). The configuration form is divided into sections:

- 常规设置 (General Settings):** 包括名称 (policy_sec1), 描述, 策略组 (None), 标签 (未选择), 源与目的 (Source and Destination): 源安全区域 (untrust), 目的区域 (trust), 源地址/地区 (192.168.0.0/16), 目的地址/地区 (192.168.0.0/16), VLAN ID (1-4094), 用户与服务 (User and Service): 用户 (未选择), 接入方式 (未选择), 终端设备 (未选择), 服务 (http), 应用 (未选择), URL分类 (未选择), 时间段 (未选择), 动作设置 (Action Settings): 动作 (Allow selected).
- 内容安全 (Content Security):** 反病毒:None;入侵防御:None;URL过滤:None;文件过滤:None;内容过滤:None;应用行为控制:None;云接入安全感知:None;邮件过滤:None;APT防御:None;DNS过滤:None;
- 其他选项 (Other Options):** 记录流量日志:None;记录策略命中日志:禁用;记录会话日志:禁用;会话老化时间:None;自定义长连接:禁用;

At the bottom of the modal are buttons: 确定 (Confirm), 确定并复制 (Confirm and Copy), 命令预览 (Command Preview), and 取消 (Cancel). A callout bubble with circled '4' points to the 'Actions' section of the configuration form, containing the note: '配置允许外网用户访问数据中心的服务器区 (网段为192.168.0.0/16, 端口为80)。FW_A上配置的安全策略会自动备份到FW_B上。' (Configure to allow external network users to access the server area of the data center (IP segment 192.168.0.0/16, port 80). The security policies configured on FW_A will be automatically backed up to FW_B.)

Example 13：防火墙旁挂在三层设备上的负载分担场景

Step8 配置核心交换机Switch1 (1)

配置Switch1。

```
[Switch1] ip vpn-instance VRF //创建VRF
[Switch1-vpn-instance-VRF] ipv4-family
[Switch1-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[Switch1-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[Switch1-vpn-instance-VRF-af-ipv4] quit
[Switch1-vpn-instance-VRF] quit
[Switch1] vlan 2
[Switch1-vlan2] port gigabitetherent 1/0/3 to 1/0/4 //将接口加入VLAN2
[Switch1-vlan2] quit
[Switch1] interface Vlanif 2
[Switch1-Vlanif2] ip binding vpn-instance VRF //将VLANIF2绑定至VRF
[Switch1-Vlanif2] ip address 10.0.0.4 24
[Switch1-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6 //配置VRRP备份组3
[Switch1-Vlanif2] vrrp vrid 3 priority 120 //配置优先级为120，优先级高的为主用
[Switch1-Vlanif2] vrrp vrid 7 virtual-ip 10.0.0.8 //配置VRRP备份组7
[Switch1-Vlanif2] vrrp vrid 7 priority 100 //配置优先级为100，优先级低的为备用
[Switch1-Vlanif2] quit
[Switch1] vlan 3
[Switch1-vlan3] port gigabitetherent 1/0/1 to 1/0/2 //将接口加入VLAN3
[Switch1-vlan3] quit
```

该案例中仅提供交换机与
防火墙对接的相关配置。

Example 13：防火墙旁挂在三层设备上的负载分担场景

Step8 配置核心交换机Switch1 (2)

配置Switch1 (续)。

```
[Switch1] interface Vlanif 3
[Switch1-Vlanif3] ip address 10.1.0.4 24
[Switch1-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6    //配置VRRP备份组4
[Switch1-Vlanif3] vrrp vrid 4 priority 120    //配置优先级为120，优先级高的为主用
[Switch1-Vlanif3] vrrp vrid 8 virtual-ip 10.1.0.8    //配置VRRP备份组8
[Switch1-Vlanif3] vrrp vrid 8 priority 100    //配置优先级为100，优先级低的为备用
[Switch1-Vlanif3] quit
[Switch1] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3    //在VRF中配置缺省路由，下一跳为VRRP备份组1的虚拟地址
[Switch1] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.7    //在VRF中配置缺省路由，下一跳为VRRP备份组5的虚拟地址
[Switch1] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3    //在根交换机Public中配置静态路由，下一跳为VRRP备份组2的虚拟地址
[Switch1] ip route-static 192.168.0.0 255.255.0.0 10.1.0.7    //在根交换机Public中配置静态路由，下一跳为VRRP备份组6的虚拟地址
```

Example 13：防火墙旁挂在三层设备上的负载分担场景

Step9 配置核心交换机Switch2 (1)

配置Switch2。

```
[Switch2] ip vpn-instance VRF //创建VRF
[Switch2-vpn-instance-VRF] ipv4-family
[Switch2-vpn-instance-VRF-af-ipv4] route-distinguisher 100:1
[Switch2-vpn-instance-VRF-af-ipv4] vpn-target 111:1 both
[Switch2-vpn-instance-VRF-af-ipv4] quit
[Switch2-vpn-instance-VRF] quit
[Switch2] vlan 2
[Switch2-vlan2] port gigabitetherent 1/0/3 to 1/0/4 //将接口加入VLAN2
[Switch2-vlan2] quit
[Switch2] interface Vlanif 2
[Switch2-Vlanif2] ip binding vpn-instance VRF //将VLANIF2绑定至VRF
[Switch2-Vlanif2] ip address 10.0.0.5 24
[Switch2-Vlanif2] vrrp vrid 3 virtual-ip 10.0.0.6 //配置VRRP备份组3
[Switch2-Vlanif2] vrrp vrid 3 priority 100 //配置优先级为100，优先级低的为备用
[Switch2-Vlanif2] vrrp vrid 7 virtual-ip 10.0.0.8 //配置VRRP备份组7
[Switch2-Vlanif2] vrrp vrid 7 priority 120 //配置优先级为120，优先级高的为主用
[Switch2-Vlanif2] quit
[Switch2] vlan 3
[Switch2-vlan3] port gigabitetherent 1/0/1 to 1/0/2 //将接口加入VLAN3
[Switch2-vlan3] quit
```

Example 13：防火墙旁挂在三层设备上的负载分担场景

Step9 配置核心交换机Switch2 (2)

配置Switch2 (续)。

```
[Switch2] interface Vlanif 3
[Switch2-Vlanif3] ip address 10.1.0.5 24
[Switch2-Vlanif3] vrrp vrid 4 virtual-ip 10.1.0.6    //配置VRRP备份组4
[Switch2-Vlanif3] vrrp vrid 4 priority 100    //配置优先级为100，优先级低的为备用
[Switch2-Vlanif3] vrrp vrid 8 virtual-ip 10.1.0.8    //配置VRRP备份组8
[Switch2-Vlanif3] vrrp vrid 8 priority 120    //配置优先级为120，优先级高的为主用
[Switch2-Vlanif3] quit
[Switch2] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.3    //在VRF中配置缺省路由，下一跳为VRRP备份组1的虚拟地址
[Switch2] ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.0.7    //在VRF中配置缺省路由，下一跳为VRRP备份组5的虚拟地址
[Switch2] ip route-static 192.168.0.0 255.255.0.0 10.1.0.3    //在根交换机Public中配置静态路由，下一跳为VRRP备份组2的虚拟地址
[Switch2] ip route-static 192.168.0.0 255.255.0.0 10.1.0.7    //在根交换机Public中配置静态路由，下一跳为VRRP备份组6的虚拟地址
```

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step10 结果验证 (1)

配置成功后，分别查看 FW_A 和 FW_B 双机热备的运行状况，能够看到 FW_A 和 FW_B 是负载分担模式，FW_A 和 FW_B 共同转发流量。

FW_A

监控项		当前状态	详细
当前运行模式	负载分担		
当前运行角色	主用 (切换后运行的时间: 1天 19时 47分)	详细	
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)		
主动抢占	已启用		
配置一致性 ?	初始化 (检测时间: 0/0/0 00:00:00)	详细	一致性检查
▲ 接口监控 (接口名称 VLAN)			
▲ VRRP监控			
10.1.0.7 (GE0/0/3)	✓	备状态	
10.0.0.7 (GE0/0/1)	✓	备状态	
10.1.0.3 (GE0/0/3)	✓	主状态	
10.0.0.3 (GE0/0/1)	✓	主状态	

FW_B

监控项		当前状态	详细
当前运行模式	负载分担		
当前运行角色	主用 (切换后运行的时间: 1天 19时 47分)	详细	
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)		
主动抢占	已启用		
配置一致性 ?	初始化 (检测时间: 0/0/0 00:00:00)	详细	一致性检查
▲ 接口监控 (接口名称 VLAN)			
▲ VRRP监控			
10.1.0.7 (GE0/0/3)	✓	主状态	
10.0.0.7 (GE0/0/1)	✓	主状态	
10.1.0.3 (GE0/0/3)	✓	备状态	
10.0.0.3 (GE0/0/1)	✓	备状态	

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step10 结果验证 (2)

FW_A出现故障，FW_A切换成主备备份模式的备用设备，FW_B切换成主备备份模式的主用设备，流量通过FW_B正常转发。

FW_A：设备故障后切换成主备备份模式的备用设备

监控项			当前状态	详细
当前运行模式	主备备份			
当前运行角色	备用 (切换后运行的时间: 1天 19时 47分)		详细	
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)			
主动抢占	已启用			
配置一致性 ?	初始化 (检测时间: 0/0/0 00:00:00)		详细	一致性检查
▲ 接口监控 (接口名称 VLAN)				
▲ VRRP监控				
10.1.0.7 (GE0/0/3)			初始化	
10.0.0.7 (GE0/0/1)			备状态	
10.1.0.3 (GE0/0/3)			初始化	
10.0.0.3 (GE0/0/1)			备状态 (应该是“主状态”)	

FW_B：切换成主备备份模式的主用设备，转发流量

监控项			当前状态	详细
当前运行模式	主备备份			
当前运行角色	主用 (切换后运行的时间: 1天 19时 47分)		详细	
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)			
主动抢占	已启用			
配置一致性 ?	初始化 (检测时间: 0/0/0 00:00:00)		详细	一致性检查
▲ 接口监控 (接口名称 VLAN)				
▲ VRRP监控				
10.1.0.7 (GE0/0/3)			主状态	
10.0.0.7 (GE0/0/1)			主状态	
10.1.0.3 (GE0/0/3)			主状态 (应该是“备状态”)	
10.0.0.3 (GE0/0/1)			主状态 (应该是“备状态”)	

Example 13: 防火墙旁挂在三层设备上的负载分担场景

Step10 结果验证（3）

FW_A故障恢复后，FW_A和FW_B均切换成负载分担模式，流量通过FW_A和FW_B共同转发。

FW_A：主动抢占后恢复成负载分担模式

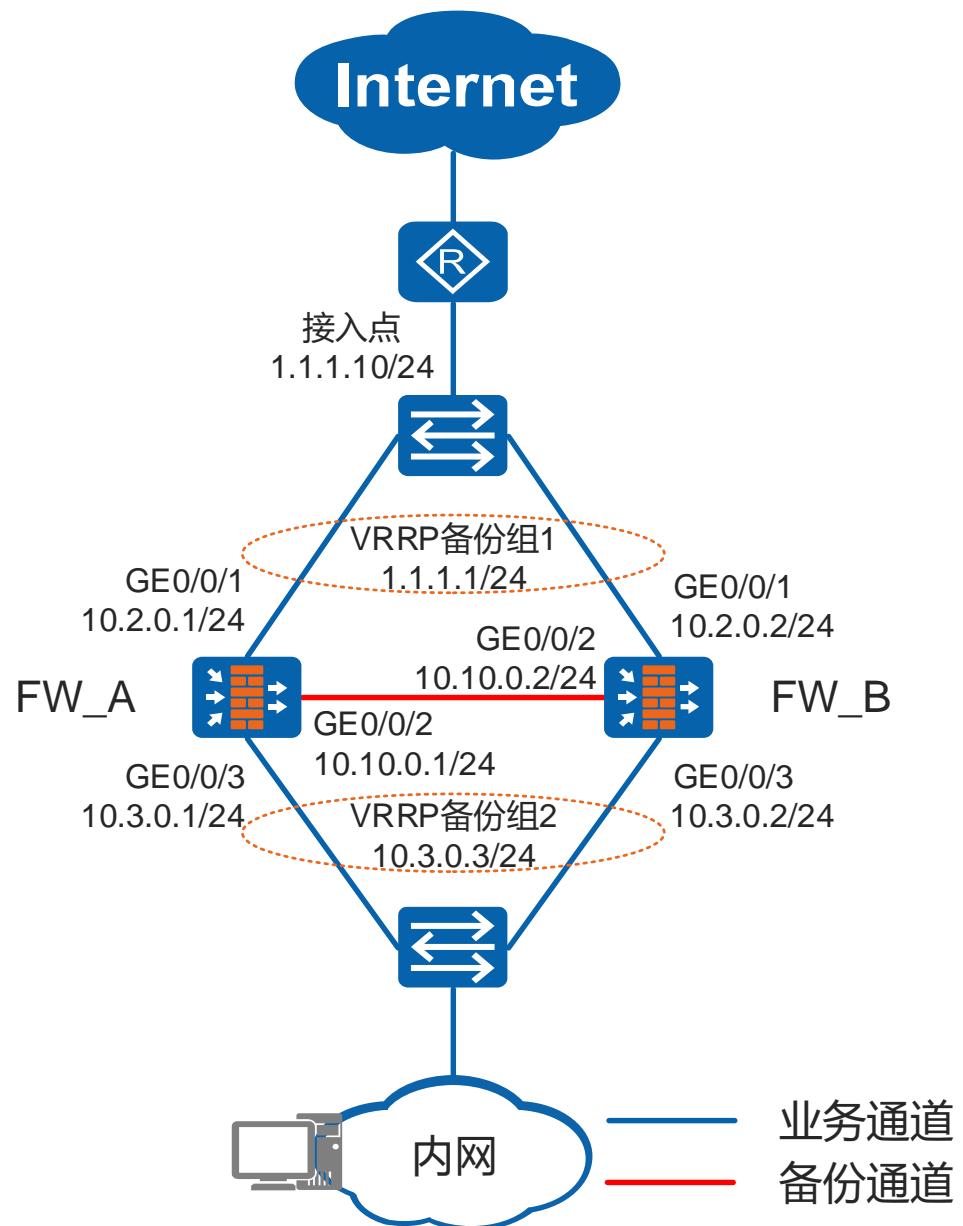
监控项		当前状态	详细
当前运行模式	负载分担		
当前运行角色	主用 (切换后运行的时间: 1天 19时 47分)	详细	
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)		
主动抢占	已启用		
配置一致性?	初始化 (检测时间: 0/0/0 00:00:00)	详细	一致性检查
▲ 接口监控 (接口名称 VLAN)			
▲ VRRP监控			
10.1.0.7 (GE0/0/3)	✓	备状态	
10.0.0.7 (GE0/0/1)	✓	备状态	
10.1.0.3 (GE0/0/3)	✓	主状态	
10.0.0.3 (GE0/0/1)	✓	主状态	

FW_B：切换成负载分担模式

监控项		当前状态	详细
当前运行模式	负载分担		
当前运行角色	主用 (切换后运行的时间: 1天 19时 47分)	详细	
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)		
主动抢占	已启用		
配置一致性?	初始化 (检测时间: 0/0/0 00:00:00)	详细	一致性检查
▲ 接口监控 (接口名称 VLAN)			
▲ VRRP监控			
10.1.0.7 (GE0/0/3)	✓	主状态	
10.0.0.7 (GE0/0/1)	✓	主状态	
10.1.0.3 (GE0/0/3)	✓	备状态	
10.0.0.3 (GE0/0/1)	✓	备状态	

Example 14：防火墙直路部署的主备备份场景

组网图



企业的两台FW的业务接口都工作在三层，上下行分别连接二层交换机。上行交换机连接运营商的接入点，运营商为企业分配的IP地址为1.1.1.1。现在希望两台FW以主备备份方式工作。正常情况下，流量通过FW_A转发。当FW_A出现故障时，流量通过FW_B转发，保证业务不中断。

项目	FW_A	FW_B
运行模式	主备备份	主备备份
运行角色	主用	备用
心跳接口	GE0/0/2 10.10.0.1/24	GE0/0/2 10.10.0.2/24

Example 14：防火墙直路部署的主备备份场景

Step1 配置FW_A的接口（1）

1. 在Huawei USG防火墙管理界面中，进入“网络”->“接口”模块。

2. 在“接口列表”中，选择要配置的上行接口（GE0/0/1）。

3. 在“启用”列中，将GE0/0/1接口的启用来到“启用”状态。

4. 在“修改GigabitEthernet”对话框中，配置上行接口参数。包括：接口名称（GigabitEthernet0/0/1）、虚拟系统（public）、安全区域（untrust）、模式（路由）、连接类型（静态IP）、IP地址（10.2.0.1/24）、默认网关（1.1.1.10）。

5. 在“接口列表”中，选择要配置的下行接口（GE0/0/3）。

6. 在“修改GigabitEthernet”对话框中，配置下行接口参数。包括：接口名称（GigabitEthernet0/0/3）、虚拟系统（public）、安全区域（trust）、模式（路由）、连接类型（静态IP）、IP地址（10.3.0.1/24）、默认网关（1.1.1.10）。

Example 14：防火墙直路部署的主备备份场景

Step1 配置FW_A的接口（2）

1. 在“网络”模块下，进入“接口”列表。

2. 选择要配置的心跳接口，如GE0/0/2。

3. 在右侧操作栏中，点击“修改”图标。

4. 在“修改GigabitEthernet”对话框中，完成以下配置：

- 接口名称：GigabitEthernet0/0/2
- 虚拟系统：public
- 安全区域：dmz
- 模式：路由
- 连接类型：静态IP
- IP地址：10.10.0.1/24
- 默认网关：（未填写）
- 首选DNS服务器：（未填写）
- 备用DNS服务器：（未填写）
- 多出口选项：（未勾选）

注意：IP地址输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。

Example 14：防火墙直路部署的主备备份场景

Step2 配置FW_B的接口（1）

1. 在HUAWEI USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“接口”选项。

3. 在右侧列表中，选择要配置的上行接口（GE0/0/1）并点击编辑图标。

4. 在“修改GigabitEthernet”对话框中，完成上行接口参数配置。配置内容包括：

- 接口名称：GigabitEthernet0/0/1
- 虚拟系统：public
- 安全区域：untrust
- 模式：路由
- 连接类型：静态IP
- IP地址：10.2.0.2/24
- 默认网关：1.1.1.10

5. 在右侧列表中，选择要配置的下行接口（GE0/0/3）并点击编辑图标。

6. 在“修改GigabitEthernet”对话框中，完成下行接口参数配置。配置内容包括：

- 接口名称：GigabitEthernet0/0/3
- 虚拟系统：public
- 安全区域：trust
- 模式：路由
- 连接类型：静态IP
- IP地址：10.3.0.2/24
- 默认网关：（未填写）

注意：在配置IP地址时，显示了提示信息：“一行一条记录，输入格式为“1.1.1.1/255.255.255.255”或者“1.1.1.1/24”。”

Example 14：防火墙直路部署的主备备份场景

Step2 配置FW_B的接口（2）

The screenshot shows the HUAWEI USG6300 configuration interface. The top navigation bar includes 'HUAWEI' logo, '网络' (Network) icon (highlighted with a red box and circled with a red arrow), '系统' (System), and user information 'admin'. Below the navigation bar is a left sidebar with icons for '接口' (Interface) (highlighted with a red box and circled with a red arrow), '安全区域' (Security Zone), 'DNS', 'DHCP服务器' (DHCP Server), '路由' (Routing), 'IPSec', 'L2TP', 'L2TP over IPSec', 'GRE', 'DSVPN', and 'SSL VPN'. The main area is titled '接口列表' (Interface List) and shows a table of interfaces. A red box highlights the 'GE0/0/2' row. A blue callout bubble with the text '配置心跳接口参数' (Configure heartbeat interface parameters) points to the 'GE0/0/2' row. A red circle labeled '4' is placed on the callout bubble. A red box highlights the 'GE0/0/2' row in the table. A red circle labeled '3' is placed on the right side of the table. A red box highlights the '修改GigabitEthernet' (Modify GigabitEthernet) dialog box. The dialog box contains fields for '接口名称' (Interface Name) set to 'GigabitEthernet0/0/2', '虚拟系统' (Virtual System) set to 'public', '安全区域' (Security Zone) set to 'dmz', and '模式' (Mode) set to '路由' (Routing). The 'IPv4' tab is selected, showing '连接类型' (Connection Type) set to '静态IP' (Static IP) and 'IP地址' (IP Address) set to '10.10.0.2/24'. A note below the IP address field states: '一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”' (One record per line, input format: "1.1.1.1/255.255.255.0" or "1.1.1.1/24"). Other fields include '默认网关' (Default Gateway), '首选DNS服务器' (Primary DNS Server), '备用DNS服务器' (Secondary DNS Server), and '多出口选项' (Multi-Exit Options). At the bottom of the dialog box are '确定' (Confirm) and '取消' (Cancel) buttons.

Example 14：防火墙直路部署的主备备份场景

Step3 配置FW_A为主用设备

The screenshot shows the HUAWEI Firewall configuration interface with the following steps highlighted:

- 1** Click the **系统** button in the top right corner.
- 2** Click the **双机热备** link in the left sidebar.
- 3** Click the **配置** button in the **双机热备** list.
- 4** FW_A is set as the primary backup device. (Note: This step is indicated by a callout box.)
- 5** Click the **新建** button in the VRRP monitoring tab.
- 6** Configure VRRP backup group 1's virtual IP address. (Note: This step is indicated by a callout box.)
- 7** Configure VRRP backup group 2's virtual IP address. (Note: This step is indicated by a callout box.)

Configuration Details (Main Window):

- 双机热备**: Enabled (radio button)
- 运行模式**: 主备备份 (radio button)
- 运行角色**: 主用 (radio button)
- 心跳接口**: GE0/0/2 (selected)
- IP地址**: 10.10.0.1 (selected)
- 对端接口IP**: 10.10.0.2 (selected)
- 主动抢占**: Enabled (checkbox)
- 静态路由自动备份**: Enabled (checkbox)
- 策略路由自动备份**: Disabled (checkbox)
- Hello报文周期**: 1000 (ms)

Configuration Details (VRRP Monitoring Tab):

- 新建** button is selected.
- VRID**: 1 (selected)
- 接口**: GE0/0/1 (selected)
- 接口IP地址/掩码**: 10.2.0.1/24 (selected)
- 虚拟IP地址/掩码**: 1.1.1.1/24 (selected)
- 虚拟MAC**: Disabled (checkbox)

Configuration Details (Second VRRP Monitoring Tab):

- VRID**: 2 (selected)
- 接口**: GE0/0/3 (selected)
- 接口IP地址/掩码**: 10.3.0.1/24 (selected)
- 虚拟IP地址/掩码**: 10.3.0.3/24 (selected)
- 虚拟MAC**: Disabled (checkbox)

Example 14：防火墙直路部署的主备备份场景

Step4 配置FW_B为备用设备

The screenshot shows the HUAWEI Firewall Management System interface with the following steps highlighted:

- 1** Click the **系统** button in the top navigation bar.
- 2** Click the **双机热备** link in the left sidebar.
- 3** Click the **配置** tab in the dual-link hot standby configuration dialog.
- 4** FW_B is set as the backup device for the primary backup device. (Note: This step is indicated by a callout box, not a numbered step in the UI.)
- 5** Click the **+新建** button in the VRRP monitoring interface.
- 6** Configure the virtual IP address for VRRP group 1. (Note: This step is indicated by a callout box, not a numbered step in the UI.)
- 7** Configure the virtual IP address for VRRP group 2. (Note: This step is indicated by a callout box, not a numbered step in the UI.)

Configuration Details:

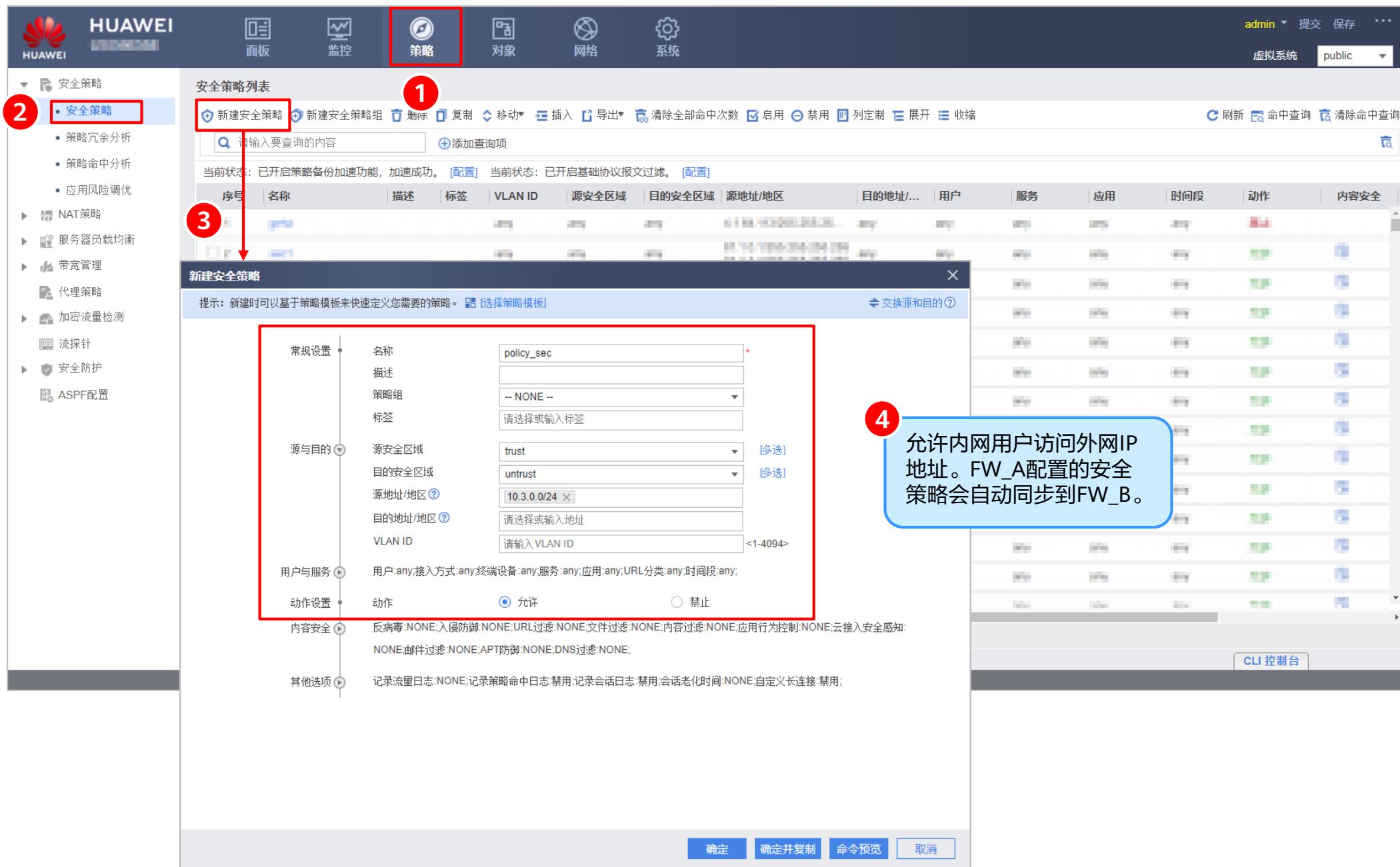
- 双机热备** configuration:
 - 运行模式: 主备备份
 - 运行角色: 备用
 - 心跳接口: GE0/0/2, 对端接口IP: 10.10.0.1
 - Hello报文周期: 1000毫秒
- 新建虚拟IP地址** for VRRP group 1:

VRID	1
接口	GE0/0/1
接口IP地址/掩码	10.2.0.2/24
虚拟IP地址/掩码	1.1.1.1/24
- 新建虚拟IP地址** for VRRP group 2:

VRID	2
接口	GE0/0/3
接口IP地址/掩码	10.3.0.2/24
虚拟IP地址/掩码	10.3.0.3/24

Example 14：防火墙直路部署的主备备份场景

Step5 配置FW_A的安全策略



The screenshot shows the HUAWEI Firewall management interface. The top navigation bar includes icons for Home, Dashboard, Monitoring, Policies (highlighted with a red box), Objects, Networks, and System. The left sidebar menu is collapsed, showing options like Security Policies, NAT Policies, and ASPF Configuration. The main content area is titled 'Security Policy List'.

Step 1: Click the 'New Security Policy' button (highlighted with a red box).

Step 2: Select 'Security Policies' from the left sidebar (highlighted with a red box).

Step 3: Fill in the 'New Security Policy' dialog box:

- 常规设置 (General Settings):**
 - 名称 (Name): policy_sec
 - 描述 (Description):
 - 策略组 (Policy Group): -- NONE --
 - 标签 (Label):
- 源与目的 (Source and Destination):**
 - 源安全区域 (Source Security Zone): trust
 - 目的安全区域 (Destination Security Zone): untrust
 - 源地址/地区 (Source IP/Region): 10.3.0.0/24
 - 目的地址/地区 (Destination IP/Region):
 - VLAN ID (VLAN ID): <1-4094>
- 用户与服务 (User and Service):**
 - 用户: any; 接入方式: any; 终端设备: any; 服务: any; 应用: any; URL分类: any; 时间段: any;
- 动作设置 (Action Settings):**
 - 动作 (Action): 允许 (Allow) (selected)

Step 4: A callout bubble indicates: "Allow internal network users to access external network IP addresses. FW_A's security policies will automatically synchronize to FW_B."

At the bottom of the dialog are buttons for 确定 (Confirm), 确定并复制 (Confirm and Copy), 命令预览 (Command Preview), and 取消 (Cancel).

Example 14：防火墙直路部署的主备备份场景

Step6 结果验证（1）

配置成功后，分别查看 FW_A和FW_B双机热备的运行状况，能够看到FW_A和FW_B已成功建立主备关系。其中，FW_A为双机热备的主用设备，FW_B为双机热备的备用设备。

FW_A为主用设备：

	当前状态	详细
当前运行模式	主备备份	
当前运行角色	主用 (切换后运行时间: 1天 18时 33分)	详细
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)	
主动抢占	已启用	
配置一致性 ?	配置不同 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
接口监控 (接口名称 VLAN)		
VRP监控		
10.3.0.3 (GE0/0/3)		主状态
1.1.1.1 (GE0/0/1)		主状态

FW_B为备用设备：

	当前状态	详细
当前运行模式	主备备份	
当前运行角色	备用 (切换后运行时间: 1天 18时 33分)	详细
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)	
主动抢占	已启用	
配置一致性 ?	配置不同 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
接口监控 (接口名称 VLAN)		
VRP监控		
10.3.0.3 (GE0/0/3)		备状态
1.1.1.1 (GE0/0/1)		备状态

Example 14：防火墙直路部署的主备备份场景

Step6 结果验证（2）

主用设备FW_A异常，备用设备FW_B自动切换成主用设备：

The screenshot shows the HUAWEI USG6300 firewall management interface. The left sidebar menu is expanded, showing options like '双机热备' (Dual Homing Backup) which is currently selected. The main content area displays the '双机热备' configuration for '配置' (Configuration). A red box highlights the '监控项' (Monitoring Items) section, which includes fields for '当前状态' (Current Status), '当前运行模式' (Current Operation Mode), '当前运行角色' (Current Operation Role), '当前心跳接口' (Current Heartbeat Interface), '主动抢占' (Active夺回), '配置一致性' (Configuration Consistency), '接口监控' (Interface Monitoring), and 'VRRP监控' (VRRP Monitoring). The '接口监控' section lists two interfaces: '10.3.0.3 (GE0/0/3)' and '1.1.1.1 (GE0/0/1)', both marked with a red 'X' indicating they are in '主状态 (应该是“备状态”)' (Master state (should be "Standby state")).

Example 14：防火墙直路部署的主备备份场景

Step6 结果验证（3）

原主用设备FW_A设备异常恢复后：

FW_A资源抢占恢复成主用设备。

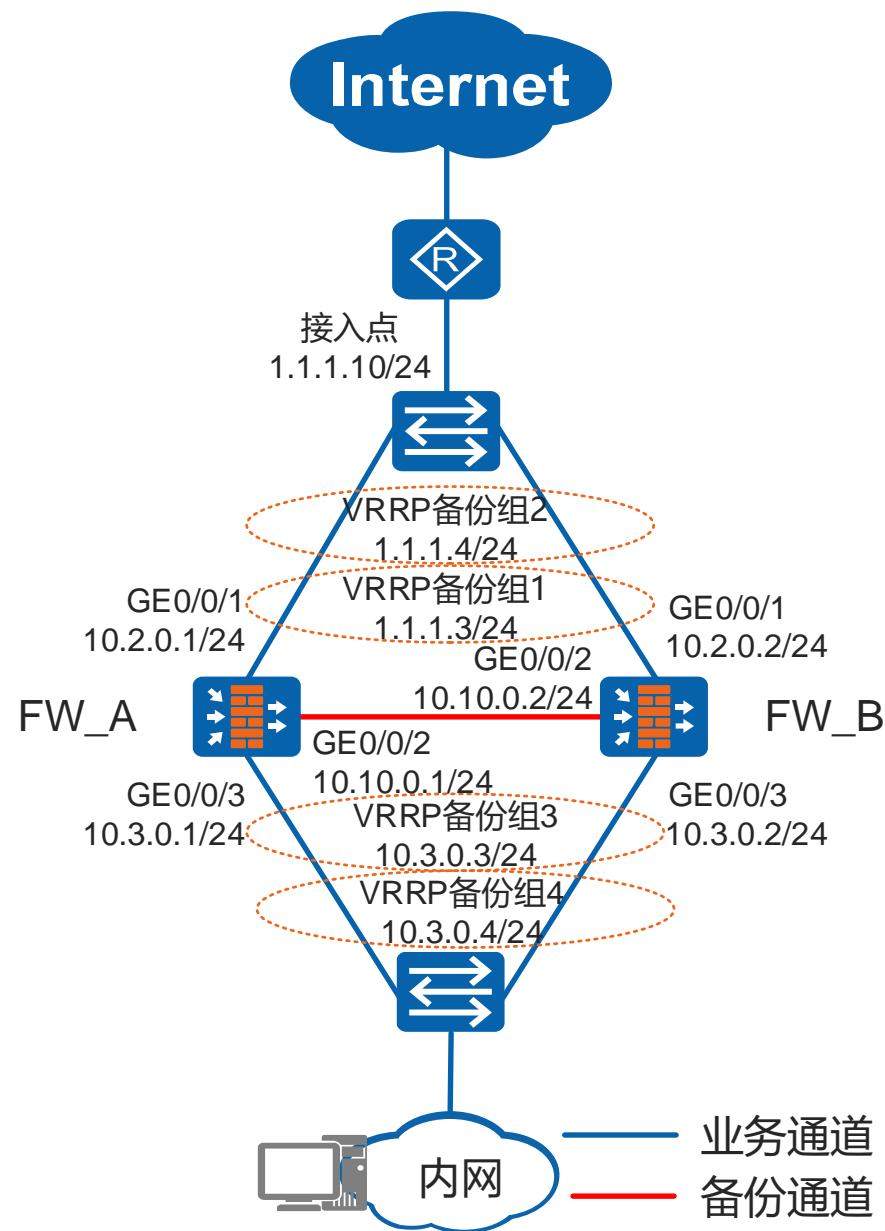
双机热备		
配置		
监控项		
当前运行模式	当前状态	详细
当前运行角色	主备备份	
当前心跳接口	主用 (切换后运行的时间: 1天 18时 33分)	详细
主动抢占	GE0/0/2 (带宽使用率: 0.00%)	
配置一致性 ?	已启用	
接口监控 (接口名称 VLAN)		
VRRP监控		
10.3.0.3 (GE0/0/3)		主状态
1.1.1.1 (GE0/0/1)		主状态

FW_B切换成备用设备。

双机热备		
配置		
监控项		
当前运行模式	当前状态	详细
当前运行角色	主备备份	
当前心跳接口	备用 (切换后运行的时间: 1天 18时 33分)	详细
主动抢占	GE0/0/2 (带宽使用率: 0.00%)	
配置一致性 ?	已启用	
接口监控 (接口名称 VLAN)		
VRRP监控		
10.3.0.3 (GE0/0/3)		备状态
1.1.1.1 (GE0/0/1)		备状态

Example 15：防火墙直路部署的负载分担场景

组网图



企业的两台FW的业务接口都工作在三层，上下行分别连接二层交换机。现在希望两台FW以负载分担方式工作。正常情况下，FW_A和FW_B共同转发流量。当其中一台FW出现故障时，另外一台FW转发全部业务，保证业务不中断。

项目	FW_A	FW_B
运行模式	负载分担	负载分担
心跳接口	GE0/0/2 10.10.0.1/24	GE0/0/2 10.10.0.2/24

Example 15：防火墙直路部署的负载分担场景

Step1 配置FW_A的接口（1）

1. 在HUAWEI USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中选择“接口”选项。

3. 在右侧列表中选择上行接口GE0/0/1，并点击编辑图标（笔形图标）。

4. 在“修改GigabitEthernet”对话框中，配置上行接口参数。设置接口名称为GigabitEthernet0/0/1，虚拟系统为public，安全区域为untrust，模式选择路由，连接类型选择静态IP，IP地址输入10.2.0.1/24，单击“确定”按钮完成配置。

5. 在右侧列表中选择下行接口GE0/0/3，并点击编辑图标（笔形图标）。

6. 在“修改GigabitEthernet”对话框中，配置下行接口参数。设置接口名称为GigabitEthernet0/0/3，虚拟系统为public，安全区域为trust，模式选择路由，连接类型选择静态IP，IP地址输入10.3.0.1/24，单击“确定”按钮完成配置。

Example 15：防火墙直路部署的负载分担场景

Step1 配置FW_A的接口（2）

The screenshot shows the HUAWEI USG6300 configuration interface. The top navigation bar includes 'HUAWEI' logo, '网络' (Network) icon (highlighted with a red box and circled with a red arrow), '系统' (System) icon, and user information 'admin'. Below the navigation bar is a toolbar with '提交' (Submit), '保存' (Save), and other icons.

The left sidebar menu includes '接口' (Interface) (highlighted with a red box and circled with a red arrow), '安全区域' (Security Zone), 'DNS', 'DHCP服务器' (DHCP Server), '路由' (Routing), 'IPSec', 'L2TP', 'L2TP over IPSec', 'GRE', 'DSVPN', and 'SSL VPN'.

The main interface shows a table of interfaces. A red box highlights the 'GE0/0/2' row. A red circle labeled '1' is on the 'GE0/0/2' row. A red box labeled '2' is on the '接口' tab in the sidebar. A red box labeled '3' is on the '编辑' (Edit) button for the 'GE0/0/2' row. A blue callout bubble labeled '配置心跳接口参数' (Configure heartbeat interface parameters) points to the 'GE0/0/2' row.

A modal window titled '修改GigabitEthernet' (Modify GigabitEthernet) is open. It contains fields for '接口名称' (Interface Name) set to 'GigabitEthernet0/0/2', '别名' (Alias), '虚拟系统' (Virtual System) set to 'public', '安全区域' (Security Zone) set to 'dmz', and '模式' (Mode) set to '路由' (Routing). The 'IPv4' tab is selected, showing '连接类型' (Connection Type) set to '静态IP' (Static IP) and 'IP地址' (IP Address) set to '10.10.0.1/24'. A note below the IP address field says: '一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”' (One record per line, input format: "1.1.1.1/255.255.255.0" or "1.1.1.1/24"). Other fields include '默认网关' (Default Gateway), '首选DNS服务器' (Primary DNS Server), '备用DNS服务器' (Secondary DNS Server), and '多出口选项' (Multi-Exit Options). Buttons at the bottom of the modal are '确定' (Confirm) and '取消' (Cancel).

Example 15：防火墙直路部署的负载分担场景

Step2 配置FW_B的接口（1）

1. 在HUAWEI USG防火墙管理界面中，进入“网络”模块。

2. 在左侧导航栏中，选择“接口”选项。

3. 在右侧列表中，选择要配置的上行接口（GE0/0/1）并点击编辑图标。

4. 在“修改GigabitEthernet”对话框中，完成上行接口参数配置。配置内容包括：

- 接口名称：GigabitEthernet0/0/1
- 虚拟系统：public
- 安全区域：untrust
- 模式：路由
- 连接类型：静态IP
- IP地址：10.2.0.2/24
- 默认网关：（未输入）
- 首选DNS服务器：（未输入）
- 备用DNS服务器：（未输入）
- 多出口选项：不勾选

5. 在右侧列表中，选择要配置的下行接口（GE0/0/3）并点击编辑图标。

6. 在“修改GigabitEthernet”对话框中，完成下行接口参数配置。配置内容包括：

- 接口名称：GigabitEthernet0/0/3
- 虚拟系统：public
- 安全区域：trust
- 模式：路由
- 连接类型：静态IP
- IP地址：10.3.0.2/24
- 默认网关：（未输入）
- 首选DNS服务器：（未输入）
- 备用DNS服务器：（未输入）
- 多出口选项：不勾选

Example 15：防火墙直路部署的负载分担场景

Step2 配置FW_B的接口（2）

1. 在“网络”模块下，进入“接口”列表。

2. 选择要配置的心跳接口，如GE0/0/2。

3. 在右侧操作栏中，点击“编辑”图标。

4. 在“修改GigabitEthernet”对话框中，完成以下配置：

- 接口名称：GigabitEthernet0/0/2
- 虚拟系统：public
- 安全区域：dmz
- 模式：路由
- 连接类型：静态IP
- IP地址：10.10.0.2/24
- 默认网关、首选DNS服务器、备用DNS服务器：未配置
- 多出口选项：未勾选

配置心跳接口参数

Example 15：防火墙直路部署的负载分担场景

Step3 配置FW_A的双机热备功能 (1)

1. 在HUAWEI USG防火墙管理界面中，进入“系统”->“双机热备”->“配置”。

2. 在左侧导航栏中，选择“双机热备”。

3. 在“双机热备”配置界面，选择“运行模式”为“负载分担”，并配置心跳接口为GE0/0/2，对端IP为10.10.0.2，Hello报文周期为1000毫秒。

4. FW_A设置为负载分担模式。

5. 在VRRP监控界面，点击“新建”按钮。

6. 在“新建虚拟IP地址”对话框中，配置VRID为1，接口为GE0/0/1，接口IP地址为10.2.0.1/24，虚拟IP地址为1.1.1.3/24，角色为主。

7. 在“新建虚拟IP地址”对话框中，配置VRID为2，接口为GE0/0/1，接口IP地址为10.2.0.1/24，虚拟IP地址为1.1.1.4/24，角色为备。

Example 15：防火墙直路部署的负载分担场景

Step3 配置FW_A的双机热备功能（2）

双机热备

配置双机热备

双机热备

运行模式 负载分担 主备备份 提示：默认启用会话快速备份。

心跳接口 GE0/0/2 * [配置] IP地址 10.10.0.1 * 对端接口IP 10.10.0.2 *

主动抢占

静态路由自动备份

策略路由自动备份

Hello报文周期 1000 <500-60000>毫秒

配置监控对象

VRRP监控 **IP-Link监控** **BFD监控** **OSPF监控** **BGP监控**

配置VRRP备份组3的虚拟IP地址 (8)

新建 **删除** **刷新**

VRID	接口	地址/掩码	虚拟MAC	角色	编辑
3	GE0/0/3	10.3.0.1/24		主	
		10.3.0.3/24		备	

新建虚拟IP地址

VRID 3 *<1-255>

接口 GE0/0/3 * [配置]

接口IP地址/掩码 10.3.0.1/24 *

虚拟IP地址/掩码 10.3.0.3/24 *

虚拟MAC

角色 主 备

新建虚拟IP地址

VRID 4 *<1-255>

接口 GE0/0/3 *

接口IP地址/掩码 10.3.0.1/24 *

虚拟IP地址/掩码 10.3.0.4/24 *

虚拟MAC

角色 主 备

Example 15：防火墙直路部署的负载分担场景

Step4 配置FW_B的双机热备功能（1）

1. 在系统菜单中选择“双机热备”。

2. 在左侧导航栏中选择“双机热备”。

3. 点击“配置”按钮。

4. FW_B设置为负载分担模式。

5. 点击“新建”按钮。

6. 配置VRID 1 的虚拟IP地址。

7. 配置VRID 2 的虚拟IP地址。

Example 15：防火墙直路部署的负载分担场景

Step4 配置FW_B的双机热备功能（2）

HUAWEI admin 提交 保存 ...

虚拟系统 public

双机热备

配置

监控项 | **当前状态** | **详细**

配置双机热备

双机热备

运行模式 主备备份 负载分担 提示：默认启用会话快速备份。

心跳接口 GE0/0/2 配置 **IP地址** 10.10.0.2 配置 **对端接口IP** 10.10.0.1 +

主动抢占

静态路由自动备份

策略路由自动备份

Hello报文周期 1000 <500-60000>毫秒

配置监控对象

接口监控 **VRPP监控** **IP-Link监控** **BFD监控** **OSPF监控** **BGP监控**

配置VRPP备份组3的虚拟IP地址

新建 **删除**

VRID **接口** 8 **VRID** **接口** 9

新建虚拟IP地址

VRID 3 <1-255>

接口 GE0/0/3 配置

接口IP地址/掩码 10.3.0.2/24

虚拟IP地址/掩码 10.3.0.3/24

虚拟MAC

角色 主 备

新建虚拟IP地址

VRID 4 <1-255>

接口 GE0/0/3 配置

接口IP地址/掩码 10.3.0.2/24

虚拟IP地址/掩码 10.3.0.4/24

虚拟MAC

角色 主 备

Example 15：防火墙直路部署的负载分担场景

Step5 配置FW_A的路由

1 配置默认优先级

2 静态路由

3 新建

4 配置FW_A的缺省路由

配置默认优先级

IPv4默认优先级	60 <1-255>
IPv6默认优先级	60 <1-255>

应用

静态路由列表

原虚拟路由器	目的地址/掩码	目的虚拟路由器	下一跳	优先级	出接口	绑定IP-Link名称	绑定BFD名称	描述	编辑
public	0.0.0.0/0.0.0.0	public	1.1.1.10	80	--NONE--				
public	0.0.0.0/0.0.0.0	public	1.1.1.10	80	--NONE--				

新建静态路由

协议类型 IPv4

源虚拟路由器 public

目的地址/掩码 0.0.0.0/0.0.0.0 *

目的虚拟路由器 public

出接口 --NONE--

下一跳 1.1.1.10

优先级 80 <1-255>

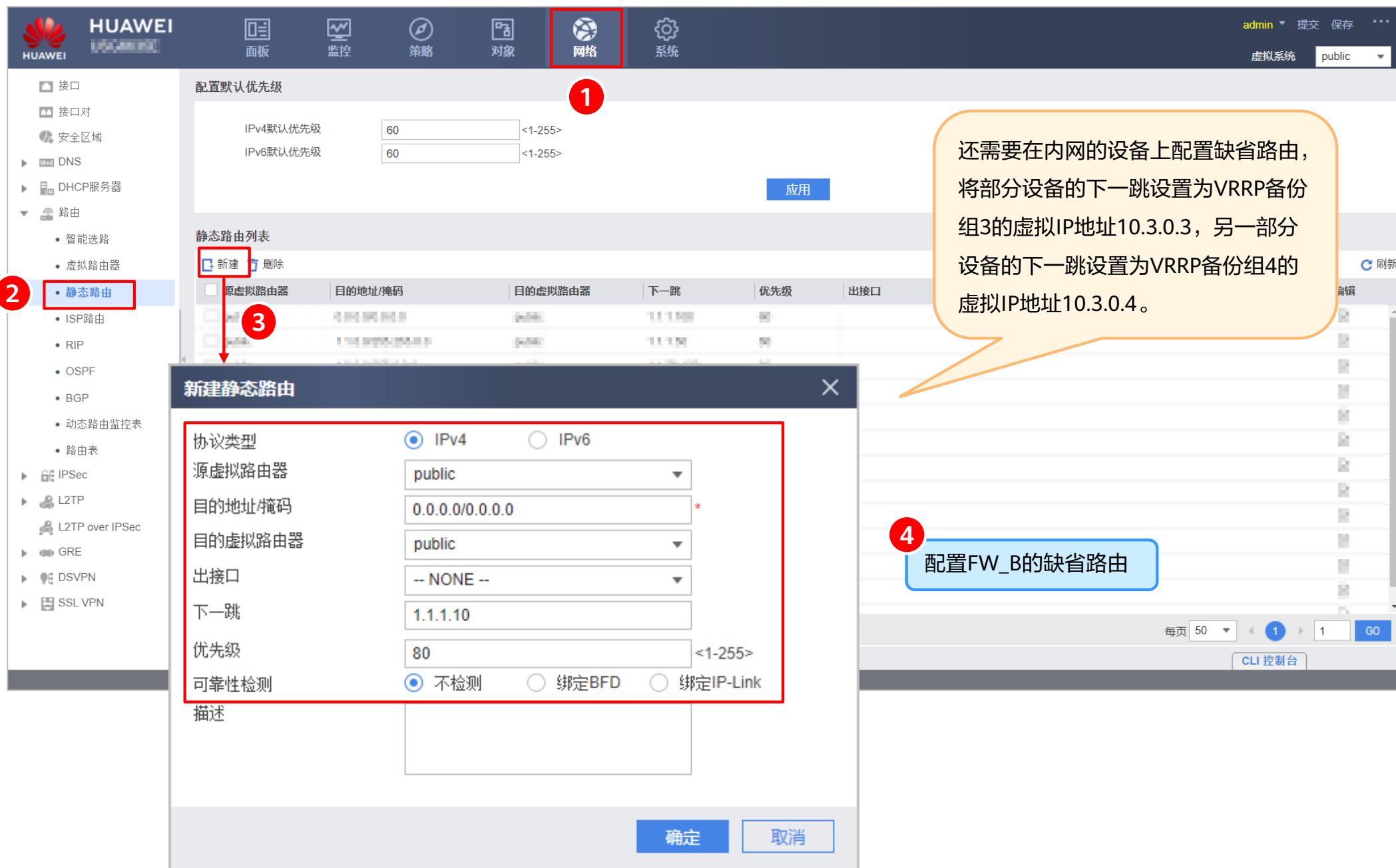
可靠性检测 不检测

描述

确定 取消

Example 15：防火墙直路部署的负载分担场景

Step6 配置FW_B的路由



The screenshot shows the Huawei Network Management System interface. The top navigation bar includes the HUAWEI logo, user information (admin), and tabs for 面板 (Panel), 监控 (Monitoring), 对象 (Object), 网络 (Network) [highlighted with a red box], and 系统 (System). Below the navigation bar is a sidebar with various network configuration options. The main content area shows the 'Configure Default Priority' section and a 'Static Route List' table. A callout bubble provides instructions for configuring default routes and VRRP backup groups. A modal window titled 'Create Static Route' is open, showing fields for protocol type (IPv4 selected), source virtual router (public), destination address/mask (0.0.0.0/0.0.0.0), destination virtual router (public), output interface (None), next hop (1.1.1.10), priority (80), and reliability detection (Uncheckable). Buttons at the bottom of the modal are '确定' (Confirm) and '取消' (Cancel).

1. 配置默认优先级

2. 路由 > 静态路由

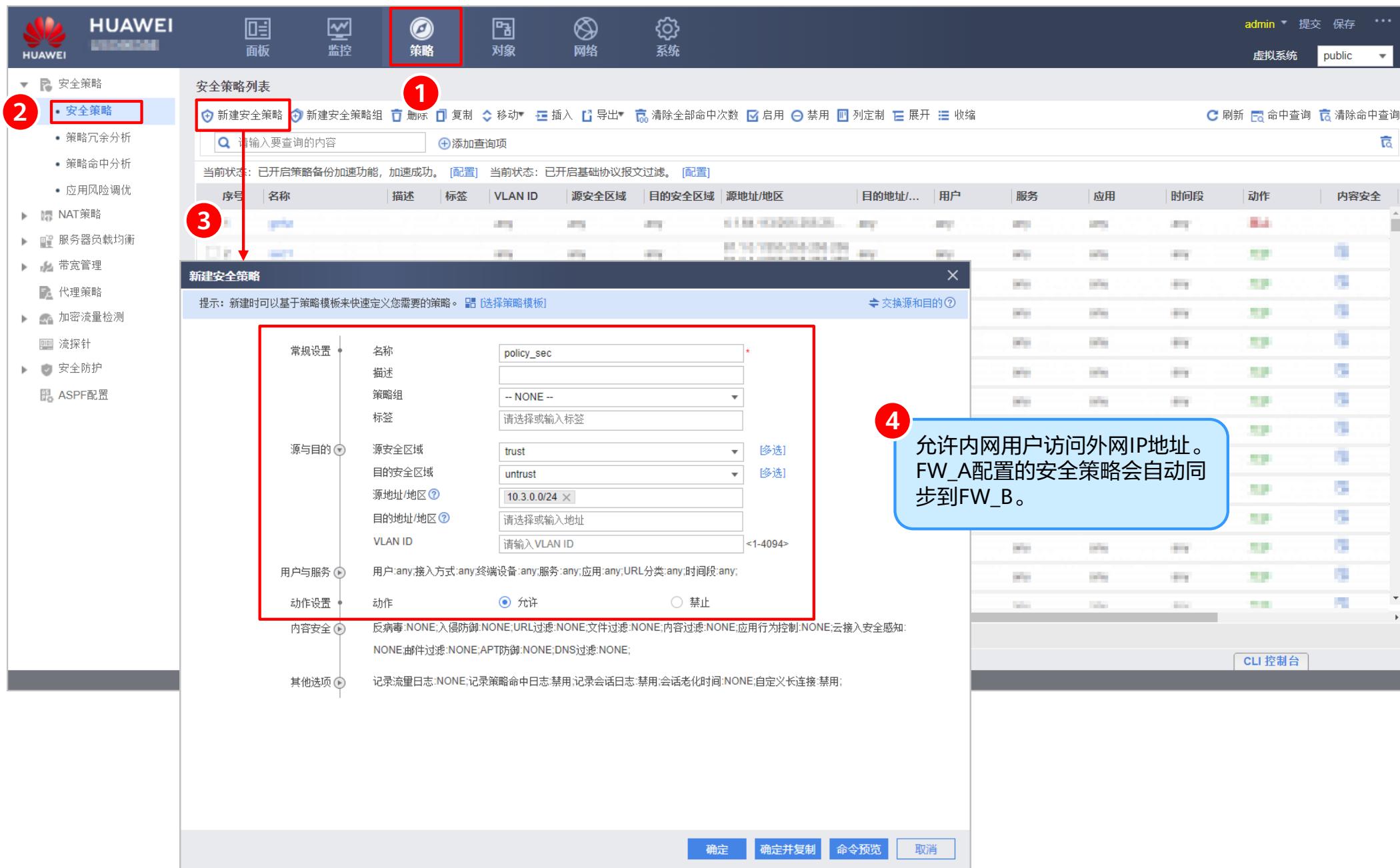
3. 新建

4. 配置FW_B的缺省路由

还需要在内网的设备上配置缺省路由，将部分设备的下一跳设置为VRRP备份组3的虚拟IP地址10.3.0.3，另一部分设备的下一跳设置为VRRP备份组4的虚拟IP地址10.3.0.4。

Example 15：防火墙直路部署的负载分担场景

Step7 配置FW_A的安全策略



The screenshot shows the HUAWEI Firewall configuration interface. The top navigation bar includes the HUAWEI logo, user 'admin', and tabs for 面板 (Dashboard), 监控 (Monitoring), 策略 (Policy), 对象 (Object), 网络 (Network), and 系统 (System). The '策略' tab is highlighted with a red box and a circled '1'. The left sidebar has a tree view with '安全策略' expanded, showing '安全策略' (selected and highlighted with a red box) and other options like '策略冗余分析', '策略命中分析', and '应用风险调优'. Under '安全策略', there's a 'NAT策略', '服务器负载均衡', '带宽管理', '代理策略', '加密流量检测', '流探针', '安全防护', and 'ASPF配置'. A red box labeled '2' highlights the '安全策略' item.

The main area is titled '安全策略列表' (Security Policy List). It shows a table with columns: 序号 (Index), 名称 (Name), 描述 (Description), 标签 (Label), VLAN ID, 源安全区域 (Source Security Zone), 目的安全区域 (Destination Security Zone), 源地址/地区 (Source Address/Region), 目的地/... (Destination/...), 用户 (User), 服务 (Service), 应用 (Application), 时间段 (Time Period), 动作 (Action), and 内容安全 (Content Security). A red box labeled '1' highlights the '新建安全策略' (Create New Security Policy) button. Below it is a search bar with placeholder '请输入要查询的内容' (Enter search content) and a '添加查询项' (Add Query Item) button. A status message says '当前状态: 已开启策略备份加速功能, 加速成功。[配置] 当前状态: 已开启基础协议报文过滤。[配置]' (Current status: Policy backup acceleration function is enabled, acceleration successful. [Configure] Current status: Basic protocol message filtering is enabled. [Configure]).

A modal window titled '新建安全策略' (Create New Security Policy) is open. It contains fields for '常规设置' (General Settings): 名称 (Name: policy_sec), 描述 (Description), 策略组 (Policy Group: -- NONE --), 标签 (Label), '源与目的' (Source and Destination): 源安全区域 (Source Security Zone: trust), 目的安全区域 (Destination Security Zone: untrust), 源地址/地区 (Source Address/Region: 10.3.0.0/24), 目的地/地区 (Destination Address/Region), VLAN ID (VLAN ID: <1-4094>), '用户与服务' (User and Service), and '动作设置' (Action Settings): 动作 (Action: 允许 - selected). A red box labeled '3' highlights the '常规设置' section. A blue callout bubble labeled '4' points to the '动作' (Action) field with the text: '允许内网用户访问外网IP地址。FW_A配置的安全策略会自动同步到FW_B。' (Allow internal network users to access external network IP addresses. The security policies configured on FW_A will automatically sync to FW_B.)

At the bottom of the modal are buttons: 确定 (Confirm), 确定并复制 (Confirm and Copy), 命令预览 (Command Preview), and 取消 (Cancel).

Example 15：防火墙直路部署的负载分担场景

Step8 结果验证（1）

配置成功后，分别查看 FW_A 和 FW_B 双机热备的运行状况，能够看到 FW_A 和 FW_B 已成功运行负载分担模式。

FW_A

监控项	当前状态	详细
当前运行模式	负载分担	
当前运行角色	主用 (切换后运行的时间: 1 天 19 时 47 分)	详细
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)	
主动抢占	已启用	
配置一致性 ?	初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
▲ 接口监控 (接口名称 VLAN ...)		
▲ VRRP 监控		
10.3.0.4 (GE0/0/3)		备状态
10.3.0.3 (GE0/0/1)		主状态
1.1.1.4 (GE0/0/3)		备状态
1.1.1.3 (GE0/0/1)		主状态

FW_B

监控项	当前状态	详细
当前运行模式	负载分担	
当前运行角色	主用 (切换后运行的时间: 1 天 19 时 47 分)	详细
当前心跳接口	GE0/0/2 (带宽使用率: 0.00%)	
主动抢占	已启用	
配置一致性 ?	初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
▲ 接口监控 (接口名称 VLAN ...)		
▲ VRRP 监控		
10.3.0.4 (GE0/0/3)		主状态
10.3.0.3 (GE0/0/1)		备状态
1.1.1.4 (GE0/0/3)		主状态
1.1.1.3 (GE0/0/1)		备状态

Example 15：防火墙直路部署的负载分担场景

Step8 结果验证（2）

当FW_A异常时：FW_A切换成主备备份模式的备用设备，FW_B切换成主备备份模式的主用设备。这说明流量通过FW_B转发。

FW_A切换成主备备份模式的备用设备



The screenshot shows the HUAWEI firewall configuration interface under the '双机热备' (Dual-Hotstandby) configuration section. The left sidebar highlights '双机热备' under '可靠性' (Reliability). The main panel displays the current status of the dual-hotstandby configuration.

监控项		当前状态	详细
当前运行模式		主备备份	
当前运行角色		备用 (切换后运行的时间: 1天 19时 47分)	详细
当前心跳接口		GE0/0/2 (带宽使用率: 0.00%)	
主动抢占		已启用	
配置一致性?		初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
接口监控 (接口名称 VLAN)			
VRRP监控			
10.3.0.4 (GE0/0/3)	×	初始化	
10.3.0.3 (GE0/0/1)	×	初始化	
1.1.1.4 (GE0/0/3)	×	初始化	
1.1.1.3 (GE0/0/1)	×	初始化	

FW_B切换成主备备份模式的主用设备

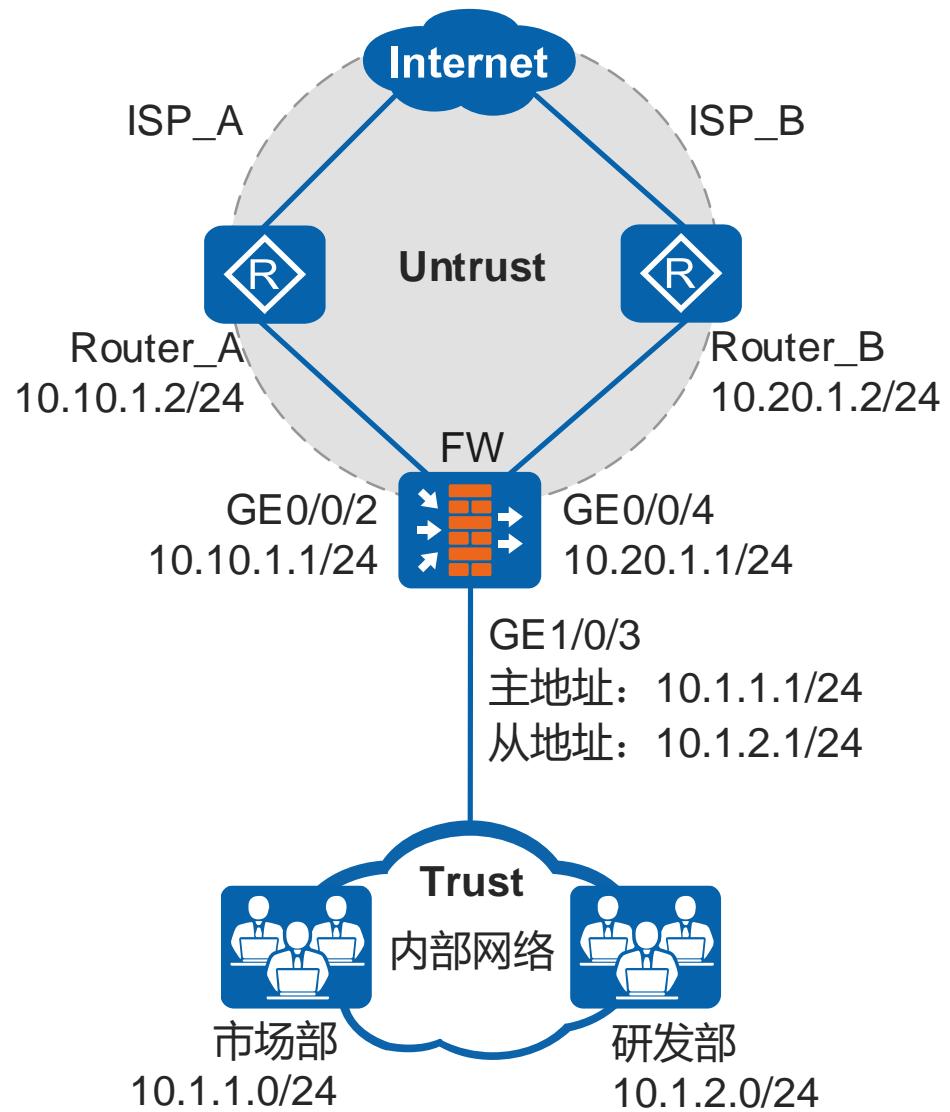


The screenshot shows the HUAWEI firewall configuration interface under the '双机热备' (Dual-Hotstandby) configuration section. The left sidebar highlights '双机热备' under '可靠性' (Reliability). The main panel displays the current status of the dual-hotstandby configuration.

监控项		当前状态	详细
当前运行模式		主备备份	
当前运行角色		主用 (切换后运行的时间: 1天 19时 47分)	详细
当前心跳接口		GE0/0/2 (带宽使用率: 0.00%)	
主动抢占		已启用	
配置一致性?		初始化 (检测时间: 0/0/0 00:00:00)	详细 一致性检查
接口监控 (接口名称 VLAN)			
VRRP监控			
10.3.0.4 (GE0/0/3)	√	主状态	
10.3.0.3 (GE0/0/1)	✗	主状态 (应该是“备状态”)	
1.1.1.4 (GE0/0/3)	√	主状态	
1.1.1.3 (GE0/0/1)	✗	主状态 (应该是“备状态”)	

Example 16：配置基于源地址的策略路由

组网图



某企业主要分为市场部和研发部两个部门，FW位于企业网出口，该企业部署了两条接入Internet的链路ISP_A、ISP_B。

为了便于管理，要求市场部通过链路ISP_A访问Internet，研发部通过链路ISP_B来访问Internet。

项目	策略路由pbr_1	策略路由pbr_2
类型	源安全区域	源安全区域
源安全区域	trust	trust
源地址	10.1.1.0/24	10.1.2.0/24
动作	转发	转发
出接口类型	单出口	单出口
出接口	GE0/0/2	GE0/0/4
下一跳	10.10.1.2	10.20.1.2
可靠性检测	绑定IP-Link	绑定IP-Link
IP-Link名称	pbr_1	pbr_2

Example 16：配置基于源地址的策略路由

Step1 配置接口（1）

1. 在 HUAWEI 网络管理界面中，进入“网络”模块。

2. 在左侧菜单栏中，选择“接口”选项。

3. 在右侧列表中，选择外网接口（GE0/0/2、GE0/0/3、GE0/0/4、GE0/0/5、GE0/0/6）并进行配置。

4. 在右侧列表中，选择内网接口（GE0/0/0/2、GE0/0/3、GE0/0/4、GE0/0/5、GE0/0/6）并进行配置。

5. 在右侧列表中，选择内网接口（GE0/0/0/2、GE0/0/3、GE0/0/4、GE0/0/5、GE0/0/6）并进行配置。

6. 在右侧列表中，选择内网接口（GE0/0/0/2、GE0/0/3、GE0/0/4、GE0/0/5、GE0/0/6）并进行配置。

配置外网接口参数

修改GigabitEthernet

接口名称	GigabitEthernet0/0/2 *
别名	
虚拟系统	public *
安全区域	untrust
模式	<input checked="" type="radio"/> 路由 <input type="radio"/> 交换 <input type="radio"/> 旁路检测 <input type="radio"/> 接口对
IPv4	<input checked="" type="radio"/> IPv6
连接类型	<input checked="" type="radio"/> 静态IP <input type="radio"/> DHCP
IP地址	10.10.1.1/24 一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。
默认网关	
首选DNS服务器	
备用DNS服务器	
<input type="checkbox"/> 多出口选项	
接口带宽	

修改GigabitEthernet

接口名称	GigabitEthernet0/0/3 *
别名	
虚拟系统	public *
安全区域	trust
模式	<input checked="" type="radio"/> 路由 <input type="radio"/> 交换 <input type="radio"/> 旁路检测 <input type="radio"/> 接口对
IPv4	<input checked="" type="radio"/> IPv6
连接类型	<input checked="" type="radio"/> 静态IP <input type="radio"/> DHCP
IP地址	10.1.1.1/24 10.1.2.1/24 一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”。
默认网关	
首选DNS服务器	
备用DNS服务器	
<input type="checkbox"/> 多出口选项	
接口带宽	

Example 16：配置基于源地址的策略路由

Step1 配置接口（2）

HUAWEI USG6300

admin 提交 保存 ...
虚拟系统 public

接口

接口列表

接口名称	安全区域	虚拟系统	IP地址	连接类型	VLAN	模式	状态	物理 IPv4	IPv6	启用	编辑
GE0/0/0(GE0/MGMT)							+	+	+		
GE0/0/1							+	+	+		
GE0/0/2							+	+	+		
GE0/0/3							+	+	+		
GE0/0/4							+	+	+		
GE0/0/5							+	+	+		
GE0/0/6							+	+	+		
GE0/0/7							+	+	+		
GE0/0/8							+	+	+		
GE0/0/9							+	+	+		
GE0/0/10							+	+	+		
GE0/0/11							+	+	+		
GE0/0/12							+	+	+		
GE0/0/13							+	+	+		
GE0/0/14							+	+	+		
GE0/0/15							+	+	+		
GE0/0/16							+	+	+		
GE0/0/17							+	+	+		
GE0/0/18							+	+	+		
GE0/0/19							+	+	+		
GE0/0/20							+	+	+		
GE0/0/21							+	+	+		
GE0/0/22							+	+	+		
GE0/0/23							+	+	+		
GE0/0/24							+	+	+		
GE0/0/25							+	+	+		
GE0/0/26							+	+	+		
GE0/0/27							+	+	+		
GE0/0/28							+	+	+		
GE0/0/29							+	+	+		
GE0/0/30							+	+	+		
GE0/0/31							+	+	+		
GE0/0/32							+	+	+		
GE0/0/33							+	+	+		
GE0/0/34							+	+	+		
GE0/0/35							+	+	+		
GE0/0/36							+	+	+		
GE0/0/37							+	+	+		
GE0/0/38							+	+	+		
GE0/0/39							+	+	+		
GE0/0/40							+	+	+		
GE0/0/41							+	+	+		
GE0/0/42							+	+	+		
GE0/0/43							+	+	+		
GE0/0/44							+	+	+		
GE0/0/45							+	+	+		
GE0/0/46							+	+	+		
GE0/0/47							+	+	+		
GE0/0/48							+	+	+		
GE0/0/49							+	+	+		
GE0/0/50							+	+	+		
GE0/0/51							+	+	+		
GE0/0/52							+	+	+		
GE0/0/53							+	+	+		
GE0/0/54							+	+	+		
GE0/0/55							+	+	+		
GE0/0/56							+	+	+		
GE0/0/57							+	+	+		
GE0/0/58							+	+	+		
GE0/0/59							+	+	+		
GE0/0/60							+	+	+		
GE0/0/61							+	+	+		
GE0/0/62							+	+	+		
GE0/0/63							+	+	+		
GE0/0/64							+	+	+		
GE0/0/65							+	+	+		
GE0/0/66							+	+	+		
GE0/0/67							+	+	+		
GE0/0/68							+	+	+		
GE0/0/69							+	+	+		
GE0/0/70							+	+	+		
GE0/0/71							+	+	+		
GE0/0/72							+	+	+		
GE0/0/73							+	+	+		
GE0/0/74							+	+	+		
GE0/0/75							+	+	+		
GE0/0/76							+	+	+		
GE0/0/77							+	+	+		
GE0/0/78							+	+	+		
GE0/0/79							+	+	+		
GE0/0/80							+	+	+		
GE0/0/81							+	+	+		
GE0/0/82							+	+	+		
GE0/0/83							+	+	+		
GE0/0/84							+	+	+		
GE0/0/85							+	+	+		
GE0/0/86							+	+	+		
GE0/0/87							+	+	+		
GE0/0/88							+	+	+		
GE0/0/89							+	+	+		
GE0/0/90							+	+	+		
GE0/0/91							+	+	+		
GE0/0/92							+	+	+		
GE0/0/93							+	+	+		
GE0/0/94							+	+	+		
GE0/0/95							+	+	+		
GE0/0/96							+	+	+		
GE0/0/97							+	+	+		
GE0/0/98							+	+	+		
GE0/0/99							+	+	+		
GE0/0/100							+	+	+		

修改GigabitEthernet

8 配置外网接口参数

接口名称: GigabitEthernet0/0/4
别名:
虚拟系统: public
安全区域: untrust
模式: 路由
连接类型: 静态IP
IP地址: 10.20.1.1/24
默认网关:
首选DNS服务器:
备用DNS服务器:
多出口选项:
接口带宽:

确定 取消

Example 16：配置基于源地址的策略路由

Step2 配置安全策略

1 策略

2 安全策略

3 新建安全策略

4 允许企业内网用户访问外网资源

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。 [选择策略模板]

常规设置	名称	policy_sec_trust_untrust *
	描述	
	策略组	-- NONE --
	标签	请选择或输入标签
源与目的	源安全区域	trust
	目的安全区域	untrust
	源地址/地区	10.1.1.0/24 × 10.1.2.0/24 ×
	目的地址/地区	请选择或输入地址
	VLAN ID	请输入 VLAN ID <1-4094>
用户与服务	用户:any;接入方式:any;终端设备:any;服务:any;应用:any;URL分类:any;时间段:any;	
动作设置	动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止
内容安全	反病毒:NONE;入侵防御:NONE;URL过滤:NONE;文件过滤:NONE;内容过滤:NONE;应用行为控制:NONE;云接入安全感知:NONE;邮件过滤:NONE;APT防御:NONE;DNS过滤:NONE;	
其他选项	记录流量日志:NONE;记录策略命中日志:禁用;记录会话日志:禁用;会话老化时间:NONE;自定义长连接:禁用;	

确定 确定并复制 命令预览 取消

Example 16：配置基于源地址的策略路由

Step3 配置 IP-Link 功能

1. 在 HUAWEI 网络管理界面中，点击“系统”图标（带红色圆圈）。

2. 在左侧导航栏中，点击“IP-Link”（带红色圆圈）。

3. 在“配置 IP-Link”页面中，确保“IP-Link功能”开关已开启，并点击“应用”按钮（带红色圆圈）。

4. 在“新建IP-Link”对话框中，配置以下参数：

IP-Link名称	pbr_1
虚拟路由器	public
发包间隔	5秒
失败次数	3
最小存活节点数	1

成员链路列表：

协议类型	探测模式	目的IP/域名	出接口	下一跳类型
IPv4	icmp	10.10.1.2	GE0/0/2	自动获取

5. 在“新建IP-Link”对话框中，配置以下参数：

IP-Link名称	pbr_2
虚拟路由器	public
发包间隔	5秒
失败次数	3
最小存活节点数	1

成员链路列表：

协议类型	探测模式	目的IP/域名	出接口	下一跳类型	下一跳
IPv4	icmp	10.20.1.2	GE0/0/4	自动获取	

4. 探测 ISP_A 链路状态。

5. 探测 ISP_B 链路状态。

Example 16：配置基于源地址的策略路由

Step4 配置策略路由

The screenshot shows the Huawei Network Management System interface under the '策略' (Policy) tab. On the left sidebar, '智能选路' (Smart Routing) is selected. The main area displays two policy route configurations:

新建策略路由 pbr_1

- 名称:** pbr_1
- 描述:** for market department
- 匹配条件 (Matching Conditions):**
 - 类型: 源安全区域 (Source Security Zone) - trust
 - 源地址: 10.1.1.0/24
 - 目的地址: 请选择或输入地址
 - 用户: 请选择或输入用户
 - 服务: 请选择或输入服务
 - 应用: 请选择或输入应用
 - 时间段: 请选择时间段
 - DSCP优先级: any
- 动作 (Action):**
 - 动作: 转发 (Forward)
 - 出接口类型: 单出口 (Single Exit Interface)
 - 单出口配置: 出接口 GE0/0/2, 下一跳 10.10.1.2
- 监控 (Monitoring):**
 - 当被监控的链路不可达时, 本策略无法生效。
 - 可靠性检测: 绑定IP-Link (Bind IP-Link), IP-Link名称: pbr_1

新建策略路由 pbr_2

- 名称:** pbr_2
- 描述:** for research department
- 匹配条件 (Matching Conditions):**
 - 类型: 源安全区域 (Source Security Zone) - trust
 - 源地址: 10.1.2.0/24
 - 目的地址: 请选择或输入地址
 - 用户: 请选择或输入用户
 - 服务: 请选择或输入服务
 - 应用: 请选择或输入应用
 - 时间段: 请选择时间段
 - DSCP优先级: any
- 动作 (Action):**
 - 动作: 转发 (Forward)
 - 出接口类型: 单出口 (Single Exit Interface)
 - 单出口配置: 出接口 GE0/0/4, 下一跳 10.20.1.2
- 监控 (Monitoring):**
 - 当被监控的链路不可达时, 本策略无法生效。
 - 可靠性检测: 绑定IP-Link (Bind IP-Link), IP-Link名称: pbr_2

注释 (Annotations):

- 从 Trust 区域接收的属于市场部的报文发送到下一跳 10.10.1.2。 (From Trust area receive traffic for the market department and forward it to the next hop 10.10.1.2.)
- 从 Trust 区域接收的属于研发部的报文发送到下一跳 10.20.1.2。 (From Trust area receive traffic for the research department and forward it to the next hop 10.20.1.2.)
- 绑定IP-Link pbr_1, 当ISP_A链路不可达时, 该策略路由不生效。 (Bind IP-Link pbr_1, when the ISP_A link is unreachable, this policy route will not take effect.)
- 绑定IP-Link pbr_2, 当ISP_B链路不可达时, 该策略路由不生效。 (Bind IP-Link pbr_2, when the ISP_B link is unreachable, this policy route will not take effect.)

Example 16：配置基于源地址的策略路由

Step5 配置缺省路由

1 在“配置默认优先级”界面，设置IPv4默认优先级为60，IPv6默认优先级为60。

2 在左侧导航栏中，选择“静态路由”。

3 点击“新建”，进入“新建静态路由”对话框。

4 在“新建静态路由”对话框中，配置以下参数：

协议类型	<input checked="" type="radio"/> IPv4	<input type="radio"/> IPv6	
源虚拟路由器	public		
目的地址/掩码	0.0.0.0/0.0.0.0	*	
目的虚拟路由器	public		
出接口	-- NONE --		
下一跳	10.10.1.2		
优先级	60	<1-255>	
可靠性检测	<input checked="" type="radio"/> 不检测	<input type="radio"/> 绑定BFD	<input type="radio"/> 绑定IP-Link
描述	当ISP_B链路不可达时，所有流量通过ISP_A链路转发		

5 在“新建静态路由”对话框中，配置以下参数（与步骤4类似）：

协议类型	<input checked="" type="radio"/> IPv4	<input type="radio"/> IPv6	
源虚拟路由器	public		
目的地址/掩码	0.0.0.0/0.0.0.0	*	
目的虚拟路由器	public		
出接口	-- NONE --		
下一跳	10.20.1.2		
优先级	60	<1-255>	
可靠性检测	<input checked="" type="radio"/> 不检测	<input type="radio"/> 绑定BFD	<input type="radio"/> 绑定IP-Link
描述	当ISP_A链路不可达时，所有流量通过ISP_B链路转发		

在内网主机上也需要配置相应的路由，请根据实际场景进行配置。

Example 16：配置基于源地址的策略路由

Step6 结果验证（1）

从市场部（10.1.1.0/24）发出的流量由GigabitEthernet0/0/2转发，通过ISP_A链路访问Internet。

从研发部（10.1.2.0/24）发出的流量由GigabitEthernet0/0/4转发，通过ISP_B链路访问Internet。

市场部某员工10.1.1.1和研发部某员工10.1.2.1分别访问外网某主机10.30.1.1的会话表信息

The screenshot shows the Huawei NMS interface. The left sidebar includes links like Health Check, Security Status, Policy Center, Objects, Network, and System. The main menu has tabs for Dashboard, Monitoring, Policies, Objects, Network, and System. The current tab is 'Session'.

Session Configuration (会话快速老化):

- Enable Session Fast Aging:
- Session Usage Rate Maximum Threshold: 80 %
- Session Usage Rate Minimum Threshold: 70 %
- Anticipatory Aging Ratio: 20 <1-50>%

Session Table (会话表):

详细信息	协议	源虚拟系统	目的虚拟系统	源安全区域	目的安全区域	源地址	目的地址	正向		反向		出口	下一路	安全策略
								报文数	字节数	报文数	字节数			
	icmp	public	public	trust	untrust	10.1.1.1	10.30.1.1	7	839 B	5	1.57 KB	GE0/0/2	10.10.1.2	policy_sec_trust_untrust
	icmp	public	public	trust	untrust	10.1.2.1	10.30.1.1	24 16 K	1.80 MB	0	0 B	GE0/0/4	10.20.1.2	policy_sec_trust_untrust

Page footer: 版权所有 © 华为技术有限公司2014-2019。保留一切权利。

Example 16: 配置基于源地址的策略路由

Step6 结果验证 (2)

当ISP_A链路不可达时，从市场部（10.1.1.0/24）和研发部（10.1.2.0/24）发出的流量均由GigabitEthernet0/0/4转发，通过ISP_B链路访问Internet。
当ISP_B链路不可达时，从市场部（10.1.1.0/24）和研发部（10.1.2.0/24）发出的流量均由GigabitEthernet0/0/2转发，通过ISP_A链路访问Internet。



The screenshot shows the Huawei Network Management System interface. The left sidebar has '会话表' (Session Table) selected. The main area displays session table statistics for two hosts (10.1.1.1 and 10.1.2.1) connecting to 10.30.1.1. The table includes columns for protocol (icmp), source virtual system (public), destination virtual system (public), security zones (trust-trust, trust-untrust), source and destination addresses, and various traffic metrics. A blue callout box highlights the session table information for the market department's route via ISP_B.

协议	源虚拟系统	目的虚拟系统	源安全区域	目的安全区域	源地址	目的地址	正向		反向		出接口	下一跳	安全策略
							报文数	字节数	报文数	字节数			
icmp	public	public	trust	untrust	10.1.1.1	10.30.1.1	7	839 B	5	1.57 KB	GE0/0/4	10.20.1.2	policy_sec_trust_untrust
icmp	public	public	trust	untrust	10.1.2.1	10.30.1.1	24.16 K	1.80 MB	0	0 B	GE0/0/4	10.20.1.2	policy_sec_trust_untrust

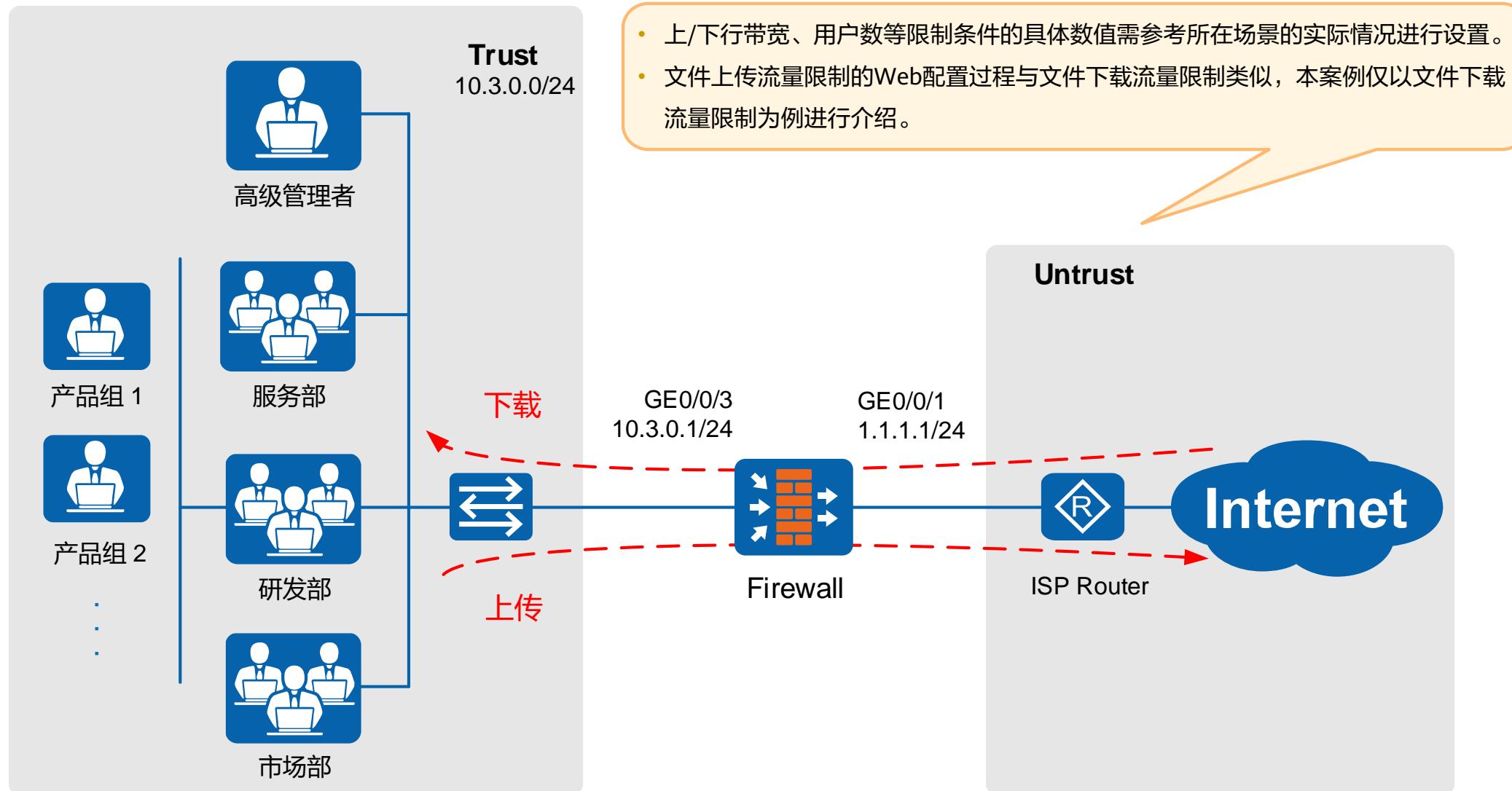


The screenshot shows the same Huawei Network Management System interface after ISP_B link failure. The session table information remains identical to the previous screenshot, indicating that traffic continues to be forwarded via the available path (ISP_A). A blue callout box highlights the session table information for the market department's route via ISP_A.

协议	源虚拟系统	目的虚拟系统	源安全区域	目的安全区域	源地址	目的地址	正向		反向		出接口	下一跳	安全策略
							报文数	字节数	报文数	字节数			
icmp	public	public	trust	untrust	10.1.1.1	10.30.1.1	7	839 B	5	1.57 KB	GE0/0/2	10.10.1.2	policy_sec_trust_untrust
icmp	public	public	trust	untrust	10.1.2.1	10.30.1.1	24.16 K	1.80 MB	0	0 B	GE0/0/2	10.10.1.2	policy_sec_trust_untrust

Example 17 基于用户的带宽管理

组网图



企业下划分研发部、市场部等多个部门，研发部下划分出多个产品组，每个产品组内有多名员工。由于企业带宽有限，当用户数量较多时极易产生拥塞，导致重要业务受到影响。通过多级父子策略，可对部门及部门下指定员工和业务实施带宽管理，实现基于用户的带宽管理，有效解决网络拥塞问题。

Example 17 基于用户的带宽管理

数据规划

请注意根据企业向运营商租用的总带宽、上网人数等实际情况规划带宽管理的数据。

项目	数据	说明
总网络带宽资源	20Mbps	1Mbps=1000kbps=125KB/s
高级管理者	<ul style="list-style-type: none"> • 整体下行保证带宽: 2Mbps • 整体下行最大带宽: 6Mbps • 组 组名: manager 、所属组: default • 用户 登录名: user_0001 、所属组: manager 、认证类型: 本地认证 	-
研发员工	<ul style="list-style-type: none"> • 产品组1和产品组2整体下行最大带宽: 2Mbps • 整体下行最大带宽: 5Mbps • 组 组名: research 、所属组: default 组名: research_product1 、所属组: research 组名: research_product2 、所属组: research • 用户 登录名: user_0003 、所属组: research_product1 、认证类型: 本地认证 登录名: user_0004 、所属组: research_product2 、认证类型: 本地认证 	研发下设置产品组1和产品组2两个子产品组。
市场员工	<ul style="list-style-type: none"> • 整体下行最大带宽: 5Mbps • 每用户下行最大带宽: 2Mbps • 组 组名: marketing 、所属组: default • 用户 登录名: user_0002 、所属组: marketing 、认证类型: 本地认证 	-

Example 17 基于用户的带宽管理

Step1 配置接口参数

为实现内网用户能访问Internet，还需要配置源NAT策略，具体配置请参考“[Example1 通过静态IP接入](#)”。

The screenshot shows the Huawei Network Management System interface. The top navigation bar includes 'HUAWEI', '网络' (Network), '系统' (System), and other tabs like '面板' (Panel) and '监控' (Monitoring). The left sidebar has a '接口' (Interface) section with options like '接口对' (Interface Pair), '安全区域' (Security Zone), 'DNS', 'DHCP服务器' (DHCP Server), '路由' (Routing), 'IPSec', and 'L2TP'. The main area shows an '接口列表' (Interface List) with four entries: 'GE0/0/0(GE0/MGMT)', 'GE0/0/1', 'GE0/0/2', and 'GE0/0/3'. A callout box labeled '4 配置外网接口参数' (Configure External Network Interface Parameters) points to the configuration dialog for 'GE0/0/1'. Another callout box labeled '5 配置接口带宽参数，限制整体网络带宽为20Mbps' (Configure Interface Bandwidth Parameters, Limiting the overall network bandwidth to 20Mbps) points to the bandwidth configuration section. A large red box highlights the 'IPv4' configuration for 'GE0/0/1', showing fields for 'IP地址' (IP Address) set to '1.1.1.1/24' and '默认网关' (Default Gateway) set to '1.1.1.254'. A second configuration dialog for 'GE0/0/3' is also shown, with its 'IPv4' configuration highlighted by a red box, showing 'IP地址' set to '10.3.0.1/24'. A callout box labeled '6 配置内网接口参数' (Configure Internal Network Interface Parameters) points to the configuration dialog for 'GE0/0/3'. A callout box labeled '7 配置内网接口参数' (Configure Internal Network Interface Parameters) points to the configuration dialog for 'GE0/0/3'. A red box highlights the '接口带宽' (Interface Bandwidth) settings for both interfaces, showing '入方向带宽' (Inbound Bandwidth) and '出方向带宽' (Outbound Bandwidth) both set to '20 Mbps'. A note at the bottom states: '一行一条记录，输入格式为“1.1.1.1/255.255.255.0”或者“1.1.1.1/24”'.

Example 17 基于用户的带宽管理

Step2 配置用户组参数

1 在左侧菜单栏中选择“对象”。

2 在左侧菜单栏中选择“用户”，并进入“default”用户组。

3 点击“新建用户组”按钮，进入“新建用户组”对话框。

4 配置高级管理者用户组，填写“用户组名”为“manager”，“所属用户组”为“/default”，并点击“配置高级管理者用户组”。

5 配置市场用户组，填写“用户组名”为“marketing”，“所属用户组”为“/default”，并点击“配置市场用户组”。

6 配置研发用户组，填写“用户组名”为“research”，“所属用户组”为“/default”，并点击“配置研发用户组”。

7 配置研发产品组1用户组，填写“用户组名”为“research_product1”，“所属用户组”为“/default/research”，并点击“配置研发产品组1用户组”。

8 配置研发产品组2用户组，填写“用户组名”为“research_product2”，“所属用户组”为“/default/research”，并点击“配置研发产品组2用户组”。

根据实际情况，可以新建其他用户组。

Example 17 基于用户的带宽管理

Step3 配置用户参数

1 在“对象”模块下，配置上网行为管理。

2 在左侧菜单栏中，选择“default”认证域。

3 在右侧“新建用户”对话框中，添加新用户。

4 配置高级管理者用户（所属用户组：/default/manager）。

5 配置市场用户（所属用户组：/default/marketing）。

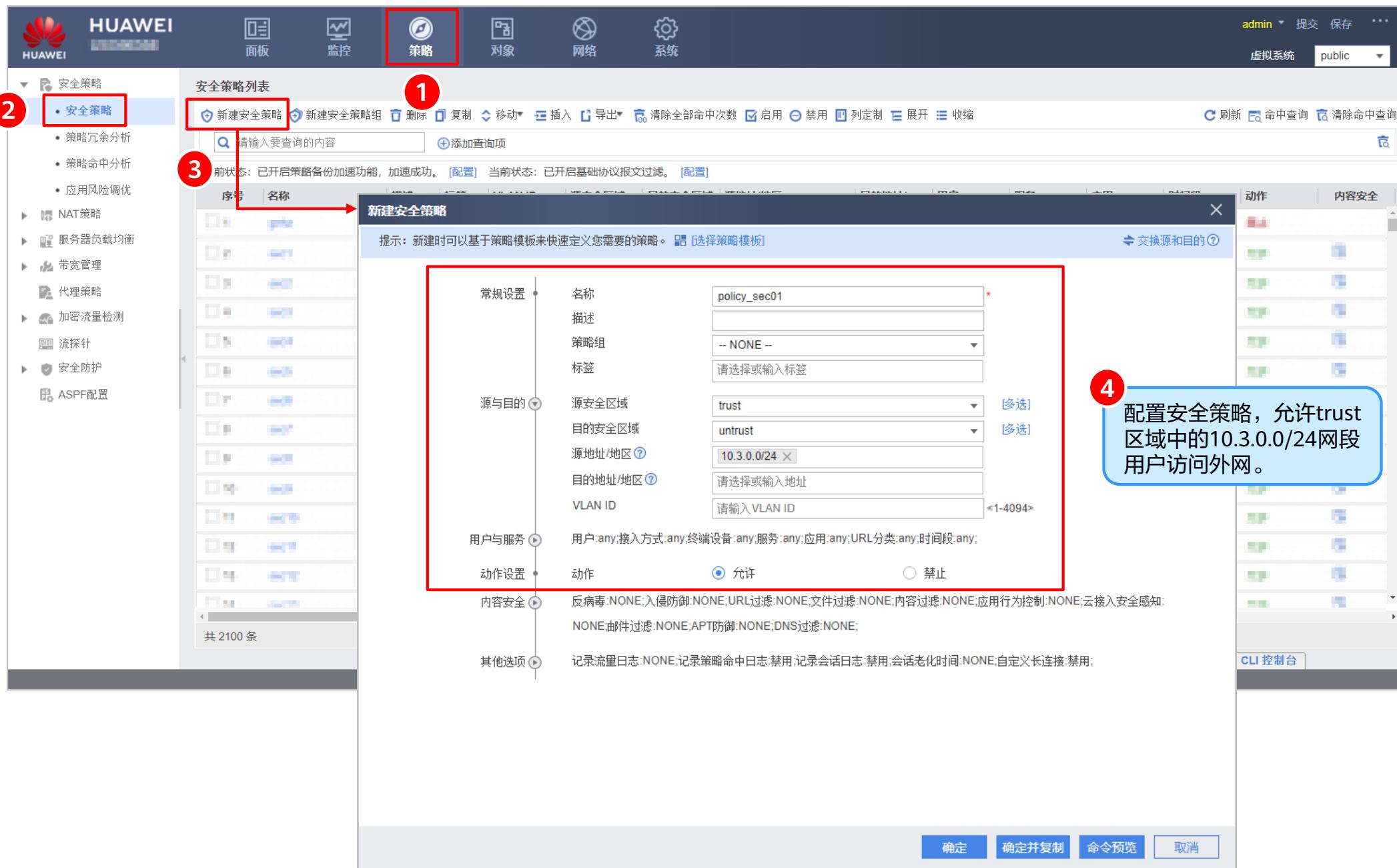
6 配置研发产品组1用户（所属用户组：/default/research/research_product1）。

7 配置研发产品组2用户（所属用户组：/default/research/research_product2）。

根据实际情况，可以在各用户组下添加多个用户。

Example 17 基于用户的带宽管理

Step4 配置安全策略



The screenshot shows the HUAWEI Network Management System interface. The top navigation bar includes links for HUAWEI, 面板 (Panel), 监控 (Monitoring), 策略 (Policy), 对象 (Object), 网络 (Network), and 系统 (System). The right side of the header shows user information (admin) and system status (提交 提交 保存 ...).

The left sidebar menu includes: 安全策略 (Security Policy) (selected), NAT策略 (NAT Policy), 服务器负载均衡 (Server Load Balancing), 带宽管理 (Bandwidth Management), 代理策略 (Proxy Policy), 加密流量检测 (Encrypted Traffic Detection), 流探针 (Flow Probe), 安全防护 (Security Protection), and ASPF配置 (ASPF Configuration). Under 安全策略, there are sub-options: 安全策略 (Security Policy) (selected), 策略冗余分析 (Policy Redundancy Analysis), 策略命中分析 (Policy Hit Analysis), 应用风险调优 (Application Risk Optimization), and 安全策略组 (Security Policy Group).

The main content area is titled "安全策略列表" (Security Policy List). A red circle labeled 1 highlights the "新建安全策略" (Create New Security Policy) button. A red circle labeled 2 highlights the "安全策略" (Security Policy) link in the sidebar. A red circle labeled 3 highlights the search bar and message area.

A modal window titled "新建安全策略" (Create New Security Policy) is open. It contains fields for "常规设置" (General Settings), "源与目的" (Source and Destination), "用户与服务" (User and Service), "动作设置" (Action Settings), and "内容安全" (Content Security). A red box highlights the "常规设置" section. A red circle labeled 4 points to the "动作" (Action) field, which is set to "允许" (Allow). A callout bubble provides instructions: "配置安全策略, 允许trust区域中的10.3.0.0/24网段用户访问外网。" (Configure security policy to allow users in the trust zone of the 10.3.0.0/24 subnet to access the external network.)

At the bottom of the modal are buttons for 确定 (Confirm), 确定并复制 (Confirm and Copy), 命令预览 (Command Preview), and 取消 (Cancel).

Example 17 基于用户的带宽管理

Step5 配置内网用户带宽通道

The screenshot shows the HUAWEI USG6300 management interface with several windows open for configuring bandwidth profiles:

- Main Interface (Top Left):** Shows the '策略' (Policy) tab selected. A red box highlights the '带宽管理' (Bandwidth Management) section, and a red circle labeled '2' is on the '带宽通道' (Bandwidth Channel) item. Another red circle labeled '1' is on the '策略' (Policy) tab.
- New Bandwidth Channel (Top Right):** A window titled '新建带宽通道' (Create New Bandwidth Channel) for 'profile_manager'. It shows configuration for '整体限流' (Overall Flow Control) with '策略独占' (Policy Exclusive) selected. Parameters include:
 - 上行带宽 (Upstream Bandwidth):** Maximum 60-2000000000 kbps, Guarantee 60-2000000000 kbps.
 - 下行带宽 (Downstream Bandwidth):** Maximum 6 Mbps, Guarantee 2 Mbps.
 - 最大连接数 (Maximum Connections):** 1-12000000.
 - 最大连接速率 (Maximum Connection Rate):** 1-5000000/s.
- New Bandwidth Channel (Middle Right):** A window titled '新建带宽通道' (Create New Bandwidth Channel) for 'profile_research_product1'. It shows configuration for '整体限流' (Overall Flow Control) with '策略独占' (Policy Exclusive) selected. Parameters include:
 - 上行带宽 (Upstream Bandwidth):** Maximum 60-2000000000 kbps, Guarantee 60-2000000000 kbps.
 - 下行带宽 (Downstream Bandwidth):** Maximum 2 Mbps, Guarantee 2 Mbps.
 - 最大连接数 (Maximum Connections):** 1-12000000.
 - 最大连接速率 (Maximum Connection Rate):** 1-5000000/s.
- New Bandwidth Channel (Bottom Right):** A window titled '新建带宽通道' (Create New Bandwidth Channel) for 'profile_research_product2'. It shows configuration for '整体限流' (Overall Flow Control) with '策略独占' (Policy Exclusive) selected. Parameters include:
 - 上行带宽 (Upstream Bandwidth):** Maximum 60-2000000000 kbps, Guarantee 60-2000000000 kbps.
 - 下行带宽 (Downstream Bandwidth):** Maximum 2 Mbps, Guarantee 2 Mbps.
 - 最大连接数 (Maximum Connections):** 1-12000000.
 - 最大连接速率 (Maximum Connection Rate):** 1-5000000/s.
- New Bandwidth Channel (Bottom Left):** A window titled '新建带宽通道' (Create New Bandwidth Channel) for 'profile_marketing'. It shows configuration for '整体限流' (Overall Flow Control) with '策略独占' (Policy Exclusive) selected. Parameters include:
 - 上行带宽 (Upstream Bandwidth):** Maximum 60-2000000000 kbps, Guarantee 60-2000000000 kbps.
 - 下行带宽 (Downstream Bandwidth):** Maximum 5 Mbps, Guarantee 2 Mbps.
 - 最大连接数 (Maximum Connections):** 1-12000000.
 - 最大连接速率 (Maximum Connection Rate):** 1-5000000/s.

Annotations:

- 请基于实际业务情况配置, 如需限制上传文件流量, 可增加对上行带宽参数的配置。
- 配置市场部带宽通道参数, 限制整体最大下行带宽为5Mbps, 限制每用户最大下行带宽为2Mbps。
- 配置高级管理者带宽通道参数, 限制整体最大下行带宽为6Mbps, 限制整体保证下行带宽为2Mbps。
- 配置研发产品组1带宽通道参数, 限制整体最大下行带宽为2Mbps。
- 配置研发部带宽通道参数, 限制整体最大下行带宽为5Mbps。
- 配置研发产品组2带宽通道参数, 限制整体最大下行带宽为2Mbps。

Example 17 基于用户的带宽管理

Step6 配置内网用户带宽策略

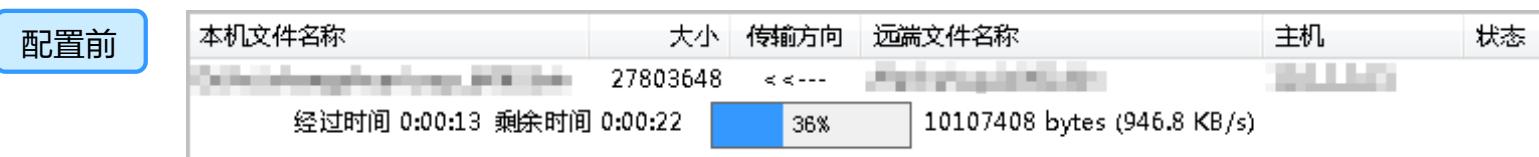
The screenshot shows the HUAWEI Network Management System interface with the following steps:

- Step 1: Create Marketing Department Bandwidth Policy** (请基于实际业务情况配置, 如配置基于IP的流量限制, 需配置相应的源、目的地址区域, 无需配置用户及用户组信息。)
 - Left sidebar: Click on "带宽管理" > "带宽策略".
 - Main menu: Click on "策略" (highlighted with a red box).
 - Action bar: Click on "新建" (highlighted with a red box).
 - Input fields: Name: policy_marketing, Source type: trust, Destination type: untrust, User: /default/marketing, Action: 限流 (highlighted with a red box), Profile: profile_marketing.
- Step 2: Create Manager Bandwidth Policy**
 - Left sidebar: Click on "带宽管理" > "带宽策略".
 - Main menu: Click on "策略" (highlighted with a red box).
 - Action bar: Click on "新建" (highlighted with a red box).
 - Input fields: Name: policy_manager, Source type: trust, Destination type: untrust, User: /default/manager, Action: 限流 (highlighted with a red box), Profile: profile_manager.
- Step 3: Create Research Product 1 Bandwidth Policy**
 - Left sidebar: Click on "带宽管理" > "带宽策略".
 - Main menu: Click on "策略" (highlighted with a red box).
 - Action bar: Click on "新建" (highlighted with a red box).
 - Input fields: Name: policy_research_product1, Source type: trust, Destination type: untrust, User: /default/research/research_product1, Action: 限流 (highlighted with a red box), Profile: profile_research_product1.
- Step 4: Create Manager Bandwidth Policy (Revised)**
 - Left sidebar: Click on "带宽管理" > "带宽策略".
 - Main menu: Click on "策略" (highlighted with a red box).
 - Action bar: Click on "新建" (highlighted with a red box).
 - Input fields: Name: policy_manager, Source type: trust, Destination type: untrust, User: /default/manager, Action: 限流 (highlighted with a red box), Profile: profile_manager.
- Step 5: Create Marketing Department Bandwidth Policy (Revised)**
 - Left sidebar: Click on "带宽管理" > "带宽策略".
 - Main menu: Click on "策略" (highlighted with a red box).
 - Action bar: Click on "新建" (highlighted with a red box).
 - Input fields: Name: policy_marketing, Source type: trust, Destination type: untrust, User: /default/marketing, Action: 限流 (highlighted with a red box), Profile: profile_marketing.
- Step 6: Create Research Product 1 Bandwidth Policy (Revised)**
 - Left sidebar: Click on "带宽管理" > "带宽策略".
 - Main menu: Click on "策略" (highlighted with a red box).
 - Action bar: Click on "新建" (highlighted with a red box).
 - Input fields: Name: policy_research_product1, Source type: trust, Destination type: untrust, User: /default/research/research_product1, Action: 限流 (highlighted with a red box), Profile: profile_research_product1.
- Step 7: Create Research Product 2 Bandwidth Policy**
 - Left sidebar: Click on "带宽管理" > "带宽策略".
 - Main menu: Click on "策略" (highlighted with a red box).
 - Action bar: Click on "新建" (highlighted with a red box).
 - Input fields: Name: policy_research_product2, Source type: trust, Destination type: untrust, User: /default/research/research_product2, Action: 限流 (highlighted with a red box), Profile: profile_research_product2.
- Step 8: Create Research Product 2 Bandwidth Policy (Revised)**
 - Left sidebar: Click on "带宽管理" > "带宽策略".
 - Main menu: Click on "策略" (highlighted with a red box).
 - Action bar: Click on "新建" (highlighted with a red box).
 - Input fields: Name: policy_research_product2, Source type: trust, Destination type: untrust, User: /default/research/research_product2, Action: 限流 (highlighted with a red box), Profile: profile_research_product2.

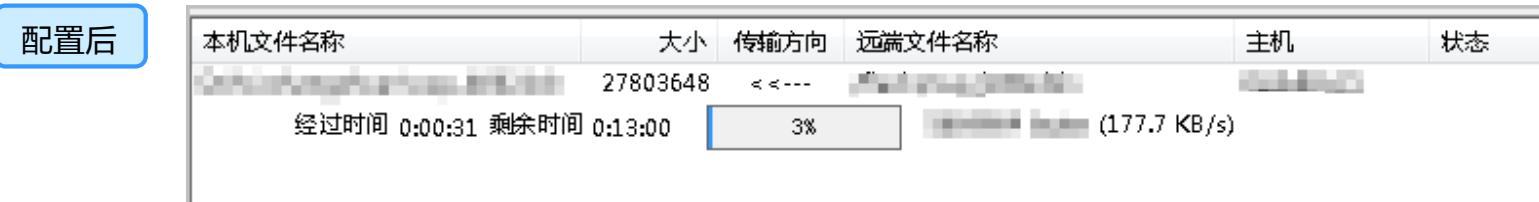
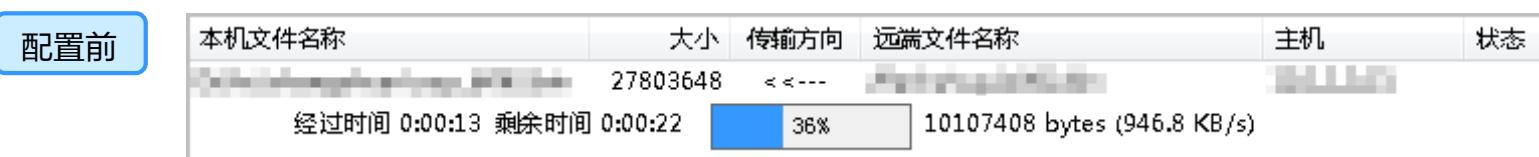
Example 17 基于用户的带宽管理

Step7 结果验证 (1)

1、高级管理者使用FileZilla、FTP等工具从Internet下载文件，其下载速率最大不超过6Mbps。下面以FileZilla为例，配置前，下载的速率超6Mbps（946.8KB/s=7.5744Mbps）；配置后，下载相同的文件速率控制在2Mbps~6Mbps以内（567.0KB/s=4.536Mbps）。



2、市场人员使用FileZilla、FTP等工具从Internet下载文件，每用户下载速率最大不超过2Mbps。下面以FileZilla为例，配置前，下载的速率超2Mbps（946.8KB/s=7.5744Mbps）；配置后，下载相同的文件速率控制在2Mbps以内（177.7KB/s=1.4216Mbps）。



Example 17 基于用户的带宽管理

Step7 结果验证（2）

3、研发产品组1人员使用FileZilla、FTP等工具从Internet下载文件，其下载速率最大不超过2Mbps。下面以FileZilla为例，配置前，下载的速率超2Mbps（946.8KB/s=7.5744Mbps）；配置后，下载相同的文件速率控制在2Mbps以内（175.8KB/s=1.4064Mbps）。

配置前

本机文件名称	大小	传输方向	远端文件名称	主机	状态
.....	27803648	< <---

经过时间 0:00:13 剩余时间 0:00:22 36% 10107408 bytes (946.8 KB/s)

配置后

本机文件名称	大小	传输方向	远端文件名称	主机	状态
.....	27803648	< <---

经过时间 0:00:21 剩余时间 0:14:46 2% 5 99392 bytes (175.8 KB/s)

4、研发产品组2人员使用FileZilla、FTP等工具从Internet下载文件，其下载速率最大不超过2Mbps。下面以FileZilla为例，配置前，下载的速率超2Mbps（946.8KB/s=7.5744Mbps）；配置后，下载相同的文件速率控制在2Mbps以内（190.8KB/s=1.5264Mbps）。

配置前

本机文件名称	大小	传输方向	远端文件名称	主机	状态
.....	27803648	< <---

经过时间 0:00:13 剩余时间 0:00:22 36% 10107408 bytes (946.8 KB/s)

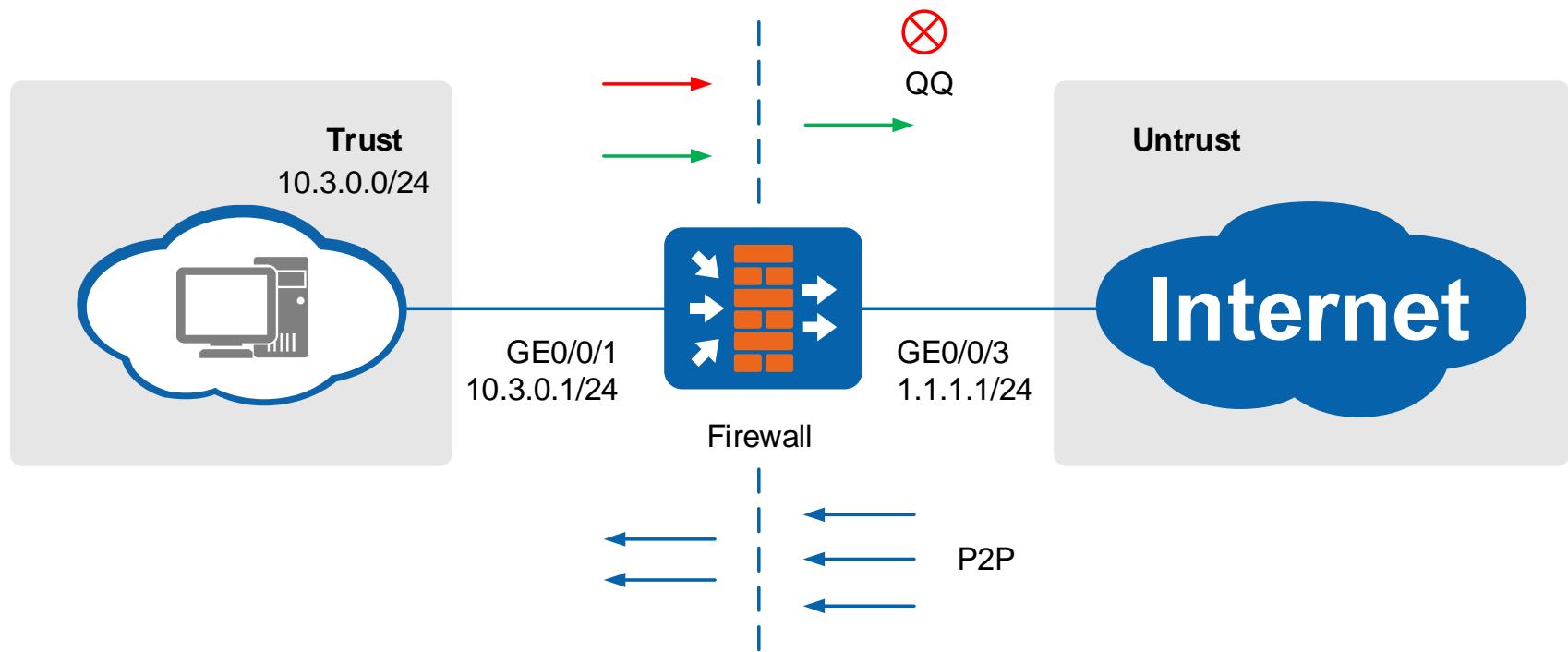
配置后

本机文件名称	大小	传输方向	远端文件名称	主机	状态
.....	27803648	< <---

经过时间 0:03:13 剩余时间 0:10:22 32% 9007003 bytes (190.8 KB/s)

Example 18 应用控制（限制P2P流量、禁用QQ）

组网图



企业允许员工访问Internet，但出于工作效率的考虑，禁止员工使用QQ聊天软件，且企业的出口带宽有限，为不影响正常业务，希望将员工使用P2P协议下载文件的流量速率限制在3Mbps以内。

项目	数据	说明
P2P限流	最大带宽: 3Mbps	1M=1000kbps=125KB/s
安全策略	阻断IM应用分类中的QQ协议。	-

Example 18 应用控制（限制P2P流量、禁用QQ）

Step1 配置接口

为实现内网用户能访问Internet，还需要配置源NAT策略，具体配置请参考“[Example1 通过静态IP接入](#)”。

The screenshot shows the HUAWEI USG6300 network management interface. The main window displays a list of interfaces (GE0/0/0 to GE0/0/6) under the 'Network' tab. A callout box points to the interface configuration area with the text: "为实现内网用户能访问Internet，还需要配置源NAT策略，具体配置请参考“[Example1 通过静态IP接入](#)”。".

1 点击“网络”图标进入网络配置界面。

2 在左侧菜单栏中选择“接口”，并点击“接口”图标。

3 在右侧列表中选择“GE0/0/1”并点击“编辑”图标。

4 在“修改GigabitEthernet”对话框中配置内网接口参数：

- 接口名称：GigabitEthernet0/0/1
- 别名：(空)
- 虚拟系统：public
- 安全区域：trust
- 模式：路由
- IPv4：连接类型选择“静态IP”，IP地址输入10.3.0.1/24
- IPv6：连接类型选择“静态IP”，IP地址输入::1/128
- 其他：勾选“多出口选项”

5 在右侧列表中选择“GE0/0/3”并点击“编辑”图标。

6 在“修改GigabitEthernet”对话框中配置外网接口参数：

- 接口名称：GigabitEthernet0/0/3
- 别名：(空)
- 虚拟系统：public
- 安全区域：untrust
- 模式：路由
- IPv4：连接类型选择“静态IP”，IP地址输入1.1.1.1/24
- IPv6：连接类型选择“静态IP”，IP地址输入::1/128
- 其他：勾选“多出口选项”

底部有“确定”和“取消”按钮。

Example 18 应用控制（限制P2P流量、禁用QQ）

Step2 配置带宽通道

The screenshot shows the HUAWEI USG6300 configuration interface. The top navigation bar includes the HUAWEI logo, user 'admin', and tabs for 面板 (Dashboard), 监控 (Monitoring), 策略 (Policy), 对象 (Object), 网络 (Network), and 系统 (System). The '策略' tab is highlighted.

The left sidebar menu is expanded under '带宽管理' (Bandwidth Management), with '带宽通道' (Bandwidth Channel) selected. A red box labeled '2' highlights this selection. Under '带宽通道', there is a '新建' (New) button, which is also highlighted with a red box labeled '3'.

The main content area displays a table titled '带宽通道列表' (Bandwidth Channel List) with columns: 名称 (Name), 引用方式 (Reference Method), 最大带宽 (Maximum Bandwidth), 保证带宽 (Guaranteed Bandwidth), 最大连接数 (Maximum Connections), 最大连接速率 (Maximum Connection Rate), 限流对象 (Flow Control Object), 最大带宽 (Maximum Bandwidth), and 保证 (Guarantee). A red box labeled '1' highlights the '新建' button.

A modal window titled '新建带宽通道' (Create New Bandwidth Channel) is open. It contains fields for '名称' (Name) set to 'profile_p2p', '整体限流' (Overall Flow Control) settings, and '每IP/每用户限流' (Flow Control per IP/User) settings. The '整体限流' section is highlighted with a red box labeled '4'. The '每IP/每用户限流' section also has a red box labeled '4'.

The '整体限流' section includes '引用方式' (Reference Method) radio buttons for '策略独占' (Strategy Exclusive) (selected) and '策略共享' (Strategy Shared). It also includes '上行带宽' (Upstream Bandwidth) and '下行带宽' (Downstream Bandwidth) settings. The '最大' (Maximum) and '保证' (Guaranteed) values for downstream bandwidth are both set to 3 Mbps. Other parameters like '最大连接数' (Maximum Connections) and '最大连接速率' (Maximum Connection Rate) are also listed.

The '每IP/每用户限流' section includes '限流对象' (Flow Control Object) radio buttons for '每IP' (Per IP) (selected) and '每用户' (Per User). It also includes '上行带宽' (Upstream Bandwidth) and '下行带宽' (Downstream Bandwidth) settings. The '最大' (Maximum) and '保证' (Guaranteed) values for downstream bandwidth are both set to 60 Mbps. Other parameters like '最大连接数' (Maximum Connections) and '最大连接速率' (Maximum Connection Rate) are also listed.

At the bottom of the modal window are '确定' (Confirm) and '取消' (Cancel) buttons.

A blue callout bubble with a red border and a red number '4' points to the text: '配置整体带宽通道参数，限制整体最大下行带宽为3Mbps。' (Configure overall bandwidth channel parameters, limit overall maximum downstream bandwidth to 3Mbps).

Example 18 应用控制（限制P2P流量、禁用QQ）

Step3 配置带宽策略

1 策略

2 带宽管理 > 带宽策略

3 新建

4 新建带宽策略，限制使用P2P协议下载文件的带宽为3Mbps。

新建带宽策略

名称: policy_p2p

描述:

标签:

所属父策略:

源类型: 源安全区域 trust

目的类型: 目的安全区域 untrust

源地址/地区: 10.3.0.0/24

目的地址/地区:

用户:

服务:

应用: P2P文件分享

URL分类:

时间段:

DSCP优先级: any

动作: 限流

带宽通道: profile_p2p

提示: 为保证受带宽策略控制的业务流量顺利转发, 需要配置安全策略。[新建安全策略]

确定 取消

- P2P文件共享表示P2P下载, 该应用协议为P2P应用协议大类, 包含了BT、eDonkey/eMule、迅雷等所有的P2P子应用。
- 您可以根据实际需求对具体某种P2P文件共享业务进行限制, 例如允许使用BT下载, 不允许使用迅雷下载。

Example 18 应用控制（限制P2P流量、禁用QQ）

Step4 配置安全策略

当相同的域间存在多条安全策略时，设备会从上到下依次匹配策略列表，一旦匹配到某条策略，将不再匹配下一条。因此，为确保配置生效，在多条安全策略共存的情况下，请注意调整策略的优先级，将精确的策略移动到宽泛的策略前。

新建安全策略

新建安全策略

1 新建安全策略 **2** 安全策略 **3** 序号

新建安全策略

4 禁止企业员工使用QQ **5** 允许企业员工访问Internet

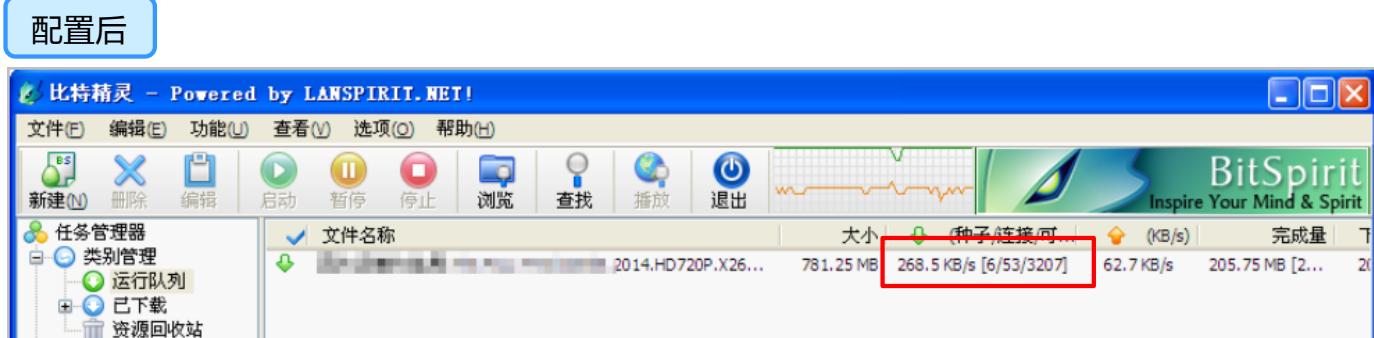
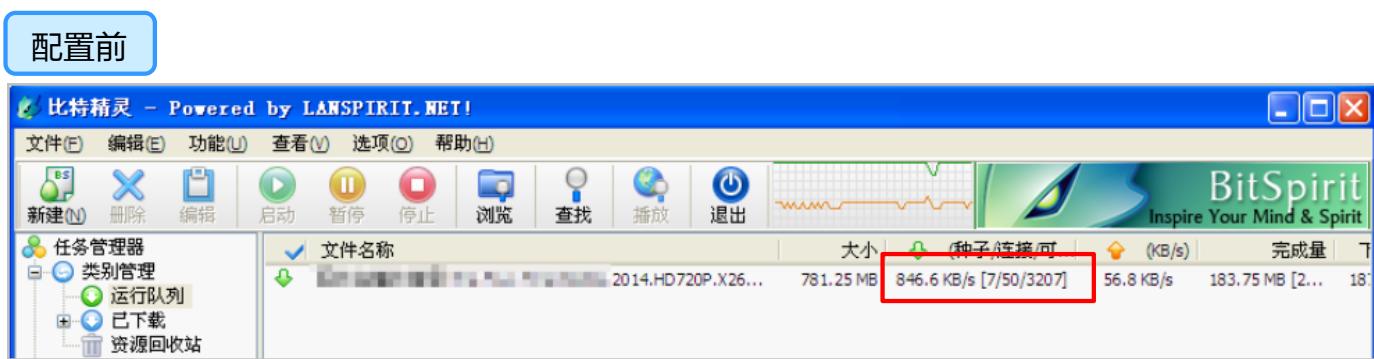
Example 18 应用控制（限制P2P流量、禁用QQ）

Step5 结果验证

1、企业员工可以访问 Internet 网站，但无法登录 QQ，系统提示“登录超时，请检查您的网络或者本机防火墙设置”。



2、企业员工使用BT、eDonkey/eMule、迅雷等工具从Internet下载文件，其下载速率最大不超过3Mbps。下面以BT为例，配置前，下载的速率超3Mbps (846.6KB/s=6.77Mbps)；配置后，下载相同的文件速率控制在3Mbps以内 (268.5KB/s=2.148Mbps)。



版权说明© 华为技术有限公司 2021。保留一切权利。