CSBN-HCNA-Security

上机指导书

（学员用书）

ISSUE 1.00



目录

[1 手册说明 6](#_Toc300328561)

[1.1 适用范围 6](#_Toc300328562)

[1.2 防火墙产品描述 6](#_Toc300328563)

[1.2.1 USG2100产品描述 6](#_Toc300328564)

[1.2.2 USG2200产品描述 8](#_Toc300328565)

[1.2.3 USG5120产品描述 9](#_Toc300328566)

[1.2.4 USG5150产品描述 10](#_Toc300328567)

[1.2.5 物理接口编号方法 12](#_Toc300328568)

[1.3 终端安全产品描述 12](#_Toc300328569)

[1.3.1 TSM产品概述 12](#_Toc300328570)

[1.3.2 TSM系统部署 12](#_Toc300328571)

[1.3.3 TSM性能指标 14](#_Toc300328572)

[1.4 图示 15](#_Toc300328573)

[2 防火墙基础实验 16](#_Toc300328574)

[2.1 安全连接USG2000/5100防火墙 16](#_Toc300328575)

[2.1.1 实验目的 16](#_Toc300328576)

[2.1.2 组网设备 16](#_Toc300328577)

[2.1.3 实验拓扑图 16](#_Toc300328578)

[2.1.4 配置步骤 16](#_Toc300328579)

[2.1.5 验证结果 19](#_Toc300328580)

[2.2 防火墙区域间连接 20](#_Toc300328581)

[2.2.1 实验目的 20](#_Toc300328582)

[2.2.2 组网设备 20](#_Toc300328583)

[2.2.3 实验拓扑图 20](#_Toc300328584)

[2.2.4 实验步骤 20](#_Toc300328585)

[2.2.5 验证结果 21](#_Toc300328586)

[2.3 防火墙软件升级 22](#_Toc300328587)

[2.3.1 实验目的 22](#_Toc300328588)

[2.3.2 组网设备 22](#_Toc300328589)

[2.3.3 实验拓扑图 22](#_Toc300328590)

[2.3.4 配置步骤 22](#_Toc300328591)

[2.3.5 验证结果 24](#_Toc300328592)

[2.4 防火墙静态路由实验 24](#_Toc300328593)

[2.4.1 实验目的 24](#_Toc300328594)

[2.4.2 组网设备 25](#_Toc300328595)

[2.4.3 实验拓扑图 25](#_Toc300328596)

[2.4.4 配置步骤 25](#_Toc300328597)

[2.4.5 验证结果 30](#_Toc300328598)

[2.5 防火墙OSPF动态路由实验 30](#_Toc300328599)

[2.5.1 实验目的 30](#_Toc300328600)

[2.5.2 组网设备 30](#_Toc300328601)

[2.5.3 实验拓扑图 30](#_Toc300328602)

[2.5.4 配置步骤： 30](#_Toc300328603)

[2.5.5 验证结果 36](#_Toc300328604)

[3 防火墙域间包过滤实验 37](#_Toc300328605)

[3.1 本地策略实验 37](#_Toc300328606)

[3.1.1 实验目的 37](#_Toc300328607)

[3.1.2 组网设备 37](#_Toc300328608)

[3.1.3 实验拓扑图 37](#_Toc300328609)

[3.1.4 配置步骤 37](#_Toc300328610)

[3.1.5 结果检查 38](#_Toc300328611)

[3.2 转发策略实验 39](#_Toc300328612)

[3.2.1 实验目的 39](#_Toc300328613)

[3.2.2 组网设备 39](#_Toc300328614)

[3.2.3 实验拓扑图 39](#_Toc300328615)

[3.2.4 配置步骤 39](#_Toc300328616)

[3.2.5 结果检查 44](#_Toc300328617)

[4 防火墙网络地址转换实验 45](#_Toc300328618)

[4.1 基于源IP地址的NAT实验 45](#_Toc300328619)

[4.1.1 实验目的 45](#_Toc300328620)

[4.1.2 组网设备 45](#_Toc300328621)

[4.1.3 实验拓扑图 45](#_Toc300328622)

[4.1.4 配置步骤 45](#_Toc300328623)

[4.1.5 结果检查 48](#_Toc300328624)

[4.2 基于目的IP地址的NAT实验 48](#_Toc300328625)

[4.2.1 实验目的 48](#_Toc300328626)

[4.2.2 组网设备 49](#_Toc300328627)

[4.2.3 实验拓扑图 49](#_Toc300328628)

[4.2.4 配置步骤 49](#_Toc300328629)

[4.2.5 结果检查 51](#_Toc300328630)

[4.3 双向NAT实验 51](#_Toc300328631)

[4.3.1 实验目的 51](#_Toc300328632)

[4.3.2 组网设备 51](#_Toc300328633)

[4.3.3 实验拓扑图 51](#_Toc300328634)

[4.3.4 配置步骤 52](#_Toc300328635)

[4.3.5 结果检查 54](#_Toc300328636)

[5 防火墙网络互联实验 55](#_Toc300328637)

[5.1 防火墙VLAN实验 55](#_Toc300328638)

[5.1.1 实验目的 55](#_Toc300328639)

[5.1.2 组网设备 55](#_Toc300328640)

[5.1.3 实验拓扑图 55](#_Toc300328641)

[5.1.4 配置步骤 56](#_Toc300328642)

[5.1.5 验证结果 57](#_Toc300328643)

[5.2 防火墙E1实验 58](#_Toc300328644)

[5.2.1 实验目的 58](#_Toc300328645)

[5.2.2 组网设备 58](#_Toc300328646)

[5.2.3 实验拓扑图 58](#_Toc300328647)

[5.2.4 配置步骤 58](#_Toc300328648)

[5.2.5 验证结果 60](#_Toc300328649)

[5.3 防火墙SA实验 60](#_Toc300328650)

[5.3.1 实验目的 60](#_Toc300328651)

[5.3.2 组网设备 60](#_Toc300328652)

[5.3.3 实验拓扑图 60](#_Toc300328653)

[5.3.4 配置步骤 60](#_Toc300328654)

[5.3.5 验证结果 62](#_Toc300328655)

[5.4 防火墙ADSL实验 62](#_Toc300328656)

[5.4.1 实验目的 62](#_Toc300328657)

[5.4.2 组网设备 62](#_Toc300328658)

[5.4.3 实验拓扑图 62](#_Toc300328659)

[5.4.4 配置步骤 62](#_Toc300328660)

[5.4.5 验证结果 65](#_Toc300328661)

[5.5 防火墙WLAN实验 66](#_Toc300328662)

[5.5.1 实验目的 66](#_Toc300328663)

[5.5.2 组网设备 66](#_Toc300328664)

[5.5.3 实验拓扑图 66](#_Toc300328665)

[5.5.4 配置步骤 66](#_Toc300328666)

[5.5.5 验证结果 68](#_Toc300328667)

[5.6 防火墙3G实验 69](#_Toc300328668)

[5.6.1 实验目的 69](#_Toc300328669)

[5.6.2 组网设备 69](#_Toc300328670)

[5.6.3 实验拓扑图 69](#_Toc300328671)

[5.6.4 配置步骤 69](#_Toc300328672)

[5.6.5 验证结果 71](#_Toc300328673)

[6 VPN实验 72](#_Toc300328674)

[6.1 L2TP VPN实验 72](#_Toc300328675)

[6.1.1 实验目的 72](#_Toc300328676)

[6.1.2 组网设备 72](#_Toc300328677)

[6.1.3 实验拓扑图 72](#_Toc300328678)

[6.1.4 配置步骤 73](#_Toc300328679)

[6.1.5 结果检查 88](#_Toc300328680)

[6.2 GRE VPN实验 88](#_Toc300328681)

[6.2.1 实验目的 88](#_Toc300328682)

[6.2.2 组网设备 88](#_Toc300328683)

[6.2.3 实验拓扑图 89](#_Toc300328684)

[6.2.4 配置步骤 89](#_Toc300328685)

[6.2.5 结果检查 93](#_Toc300328686)

[6.3 IPSEC VPN实验 94](#_Toc300328687)

[6.3.1 实验目的 94](#_Toc300328688)

[6.3.2 组网设备 94](#_Toc300328689)

[6.3.3 实验拓扑图 94](#_Toc300328690)

[6.3.4 配置步骤 94](#_Toc300328691)

[6.3.5 结果检查 102](#_Toc300328692)

[6.4 SSL VPN实验 103](#_Toc300328693)

[6.4.1 实验目的 103](#_Toc300328694)

[6.4.2 组网设备 103](#_Toc300328695)

[6.4.3 实验拓扑图 103](#_Toc300328696)

[6.4.4 配置步骤 104](#_Toc300328697)

[6.4.5 结果验证。 108](#_Toc300328698)

[7 TSM终端安全实验 110](#_Toc300328699)

[7.1 安装TSM管理器+TSM控制器 110](#_Toc300328700)

[7.1.1 实验目的 110](#_Toc300328701)

[7.1.2 组网设备 110](#_Toc300328702)

[7.1.3 实验拓扑图 110](#_Toc300328703)

[7.1.4 配置步骤 110](#_Toc300328704)

[7.2 安装TSM代理 112](#_Toc300328705)

[7.2.1 实验目的 112](#_Toc300328706)

[7.2.2 组网设备 112](#_Toc300328707)

[7.2.3 实验拓扑图 112](#_Toc300328708)

[7.2.4 配置步骤 112](#_Toc300328709)

[7.3 初始化TSM管理器 113](#_Toc300328710)

[7.3.1 实验目的 113](#_Toc300328711)

[7.3.2 组网设备 113](#_Toc300328712)

[7.3.3 实验拓扑图 113](#_Toc300328713)

[7.3.4 配置步骤 114](#_Toc300328714)

[7.4 配置TSM策略 117](#_Toc300328715)

[7.4.1 实验目的 117](#_Toc300328716)

[7.4.2 组网设备 117](#_Toc300328717)

[7.4.3 实验拓扑图 117](#_Toc300328718)

[7.4.4 配置步骤 117](#_Toc300328719)

[7.5 配置SACG接入控制 118](#_Toc300328720)

[7.5.1 实验目的 118](#_Toc300328721)

[7.5.2 组网设备 119](#_Toc300328722)

[7.5.3 实验拓扑图 119](#_Toc300328723)

[7.5.4 配置步骤 119](#_Toc300328724)

# 手册说明

本手册用于指导学员学习华为安全产品的配置和部署技术，学员可以通过教材的实验说明，掌握本手册中的实验内容。

## 适用范围

适用于华为系统安全工程师培训安全课程中涉及的实验内容。

适用防火墙系列包括：

* USG2100 V100R005
* USG2200&5100 V100R005

特殊说明：USG2100的8个LAN口为交换网口，需要划分VLAN，只有在VLAN接口上才能配置IP地址，并且只有三层VLAN(vlanif)口才能加入安全区域。

## 防火墙产品描述

### USG2100产品描述

* 机箱尺寸

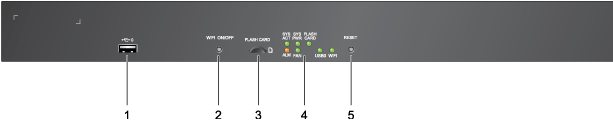
USG2100由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为420mm×255mm×43.6mm（宽×深×高），可以安装在19英寸标准机柜中。

* 前面板

USG2100系列包含USG2130、USG2130W、USG2160和USG2160W；均为交流机型。

USG2130和USG2130W提供1个MIC插槽，USG2160和USG2160W提供2个MIC插槽。USG2130W和USG2160W支持WiFi功能。USG2100的前面板如下图所示。

USG2100前面板图



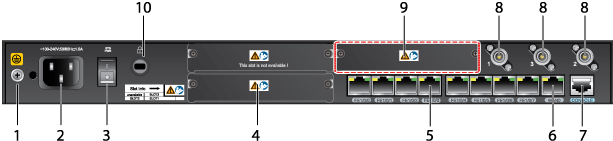
|  |  |  |
| --- | --- | --- |
| 1. USB2.0接口 | 2. WiFi开关 | 3. 闪存接口 |
| 4. 指示灯 | 5. 系统复位键 |  |

**提示**：USG2130/USG2160产品不支持WiFi功能，前面板上无WiFi开关和WiFi指示灯。

* 后面板

如下图所示，USG2100后面板包括交流电源模块、MIC(Mini Interface Card)插槽、Console接口和以太网口等。其中WAN口为路由口，可直接配置IP地址，并直接划到具体的区域里。LAN口为交换口，不能在接口上配置IP地址，需要先创建VLAN，然后在VLAN上配置VLAN interface，再把该VLAN 划到具体的区域里。

USG2100 后面板



|  |  |  |
| --- | --- | --- |
| 1. 接地端子 | 2. 交流电源插座 | 3. 交流电源开 |
| 4. MIC1/DMIC插槽 | 5. LAN接口 | 6. WAN接口 |
| 7. Console接口  10. 安全锁孔 | 8. WiFi天线接头 | 9. MIC2插槽 |

**提示**：

USG2130和USG2130W产品的MIC2插槽不可用，如红框所示；

USG2130/USG2160产品不支持WiFi功能，后面板无WiFi天线接头；

* 槽位分布和排列顺序

USG2100不支持WiFi接口卡，支持其他的MIC、DMIC接口卡，不支持FIC、DFIC接口卡。SLOT1提供固定接口，SLOT2为MIC1，SLOT3为MIC2。SLOT2可以插入MIC接口卡，也可插入DMIC接口卡，使用DMIC接口卡时需将SLOT2上方假面板拆除。如下图所示。

USG2100槽位编号及排列顺序示意图



**提示**：USG2130和USG2130W不支持SLOT3；

### USG2200产品描述

* 机箱尺寸

USG2200由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为442mm×414mm×43.6mm（宽×深×高），可以安装在19英寸标准机柜中。

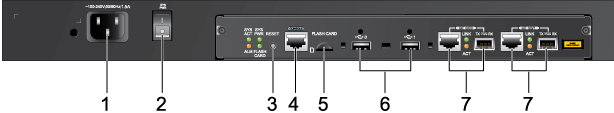
* 前面板

USG2200的电源和风扇采用内置式，因此从外观上看不到电源和风扇。USG2200包括USG2210、USG2220、USG2230、USG2250四种型号。这四种型号都支持交流机型，其中USG2250还有支持直流电源的机型。如下图所示。

USG2200 前面板（直流机型）



USG2200 前面板（交流机型）

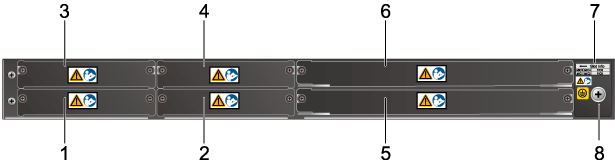


|  |  |  |
| --- | --- | --- |
| 1. 交流/直流电源插座 | 2. 交流/直流电源开关 | 3. 系统复位键 |
| 4. Console 接口 | 5. 闪存接口 | 6. USB2.0接口 |
| 7. GE ombo接口 |  |  |

* 后面板

USG2210、USG2220、USG2230、USG2250 后面板布局相同，如下图所示，左侧和中间是4 个MIC 插槽，右侧为2 个FIC 插槽。

USG2200后面板



|  |  |  |
| --- | --- | --- |
| 1. MIC1/DMIC1插槽 | 2. MIC2/DMIC2插槽 | 3. MIC3插槽 |
| 4. MIC4插槽 | 5. FIC5/DFIC5插槽 | 6. FIC6插槽 |
| 7.槽位标识 | 8. 接地端子 |  |

* 槽位分布和排列顺序

FIC5可插入一个DFIC接口卡。如下图所示。

USG2200槽位编号及排列顺序示意图



**提示**：MIC1和MIC3两个槽位可以插入两个MIC接口卡或插入一个DMIC接口卡；

MIC2和MIC4两个槽位可以插入两个MIC接口卡或插入一个DMIC接口卡；

### USG5120产品描述

* 机箱尺寸

USG5120由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为442mm×414mm×86.1mm（宽×深×高），可以安装在19英寸标准机柜中。

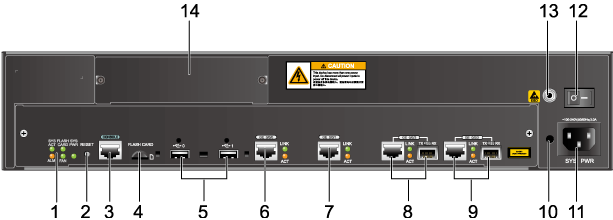
* 前面板

USG5120有交流和直流两种机型。USG5120的前面板如下图所示。

USG5120前面板（直流机型）



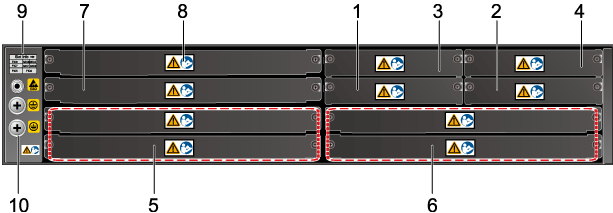
USG5120前面板（交流机型）



|  |  |  |
| --- | --- | --- |
| 1.指示灯 | 2.系统复位键 | 3. Console接口 |
| 4.闪存接口  7. 10/100/1000M以太网品  10. 卡扣插孔 | 5. USB2.0接口  8. GE Combo接口2  11. 交流/直流电源插座 | 6. 10/100/1000M以太网接口  09. GE Combo接口3  12. 交流/直流电源开关 |
| 13. 防静电手腕带插孔 | 14. 防尘面板 |  |

* 后面板

USG5120后面板

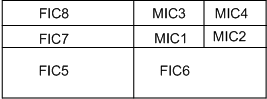


|  |  |  |
| --- | --- | --- |
| 1. MIC1/DMIC1插 | 2. MIC2/DMIC2插槽 | 3. MIC3插槽 |
| 4. MIC4插槽  7. FIC7插槽  10.接地端子 | 5. FIC5/DFIC5插槽  8. FIC8插槽 | 6. FIC6/DFIC6插槽  9. 槽位标识 |

* 槽位分布和排列顺序

USG5120的FIC5和FIC6槽位除了可插入一个DFIC接口卡外，还可只在下半部分插入一个FIC接口卡。此时，为了防尘需要在DFIC槽位的上半部分安装一个假面板，以封闭后面板。FIC7可插入一个DFIC接口卡。如下图所示。

USG5120槽位编号及排列顺序示意图



### USG5150产品描述

* 机箱尺寸

USG5150由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为442mm×414mm×130.5mm（宽×深×高），可以安装在19英寸标准机柜中。

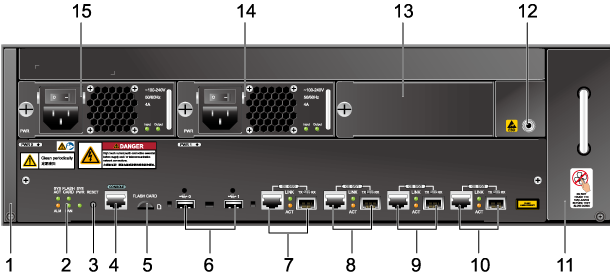
* 前面板

USG5150的电源和风扇模块均可热插拔，其前面板如下图所示。

USG5150前面板（直流机型）

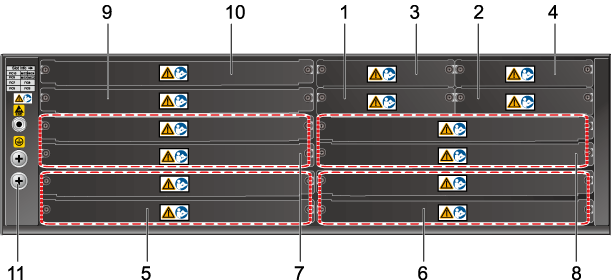


USG5150前面板（交流机型）



|  |  |  |
| --- | --- | --- |
| 1.防尘网 | 2. 指示灯 | 3.系统复位键 |
| 4. Console接口  7. GE Combo接口0  10. GE Combo接口3  13. 防尘挡板 | 5. 闪存接口  8. GE Combo接口1  11. 风扇框  14. 交流/直流电源模块1 | 6. USB2.0接口  9. GE Combo接口2  12. ESD 防静电插孔  15.交流/直流电源模块0 |

* 后面板

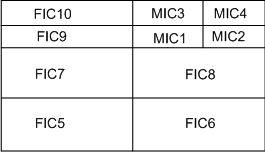
USG5150后面板 

|  |  |  |
| --- | --- | --- |
| 1. MIC1/DMIC1插槽 | 2. MIC2/DMIC2插槽 | 3. MIC3插槽 |
| 4. MIC4插槽  7. FIC7/DFIC7插槽  10. FIC10插槽 | 5. FIC5/DFIC5插槽  8. FIC8/DFIC8插槽  11. 接地端子 | 6. FIC6/DFIC6插槽  9. FIC9插槽 |

* 槽位分布和排列顺序

USG5150的FIC5、FIC6、FIC7和FIC8槽位除了可插入一个DFIC接口卡外，还可只在下半部分插入一个FIC接口卡。此时，为了防尘需要在DFIC槽位的上半部分安装一个假面板，以封闭后面板。如下图所示。

USG5150槽位编号及排列顺序示意图



**提示**：FIC9和FIC10两个槽位可以插入两个FIC接口卡，但不可以使用DFIC接口卡；

FIC9和FIC10两个槽位不支持1GE接口卡、4GE接口卡、1GPON接口卡、16POTS接口卡和32POTS接口卡；

### 物理接口编号方法

**设备物理接口采用的编号原则如下**：

各接口按照从下到上，从左到右的顺序依次编号。物理接口编号为interface-type X/0/Y，interface-type为接口类型（如Ethernet等），X表示槽位号，0为板卡号，目前支持的接口卡没有子卡，所以此位均为0。Y表示接口序号。主板的槽位号为0。

例如，USG的2号槽位安装了5FSW接口卡，那么各接口的编号为：Ethernet2/0/0、Ethernet2/0/1、Ethernet2/0/2、Ethernet2/0/3、Ethernet2/0/4。

## 终端安全产品描述

### TSM产品概述

TSM, 终端安全管理（Terminal Security Management）。为了解决企业内部网络管理失控的问题，保障企业内部网络的畅通、终端主机的安全和公司信息数据的安全，实现企业网络安全建设的目标，华为科技有限公司推出TSM这款产品，该产品为企业提供整合的内部网络安全解决方案，实现从终端到业务系统的控制和管理功能。

TSM基于TSM代理为企业提供安全接入控制、终端安全管理、补丁管理、终端用户的行为管理、软件分发和资产管理六大功能。其核心思想是建立网络准入控制机制，基本要素是安全检查、访问控制和安全修复。有效控制网络日渐增多的接入点，包括企业员工、外部访客、合作伙伴和临时雇员等对网络的访问，发现并隔离带有威胁的终端主机，提升网络防御安全威胁的能力。

### TSM系统部署

TSM包括TSM管理中心、TSM管理器、TSM控制器、扫描器、安全接入控制网关、802.1x交换机和TSM代理几个部件。

**TSM管理中心**

TSM管理中心是为分级式组网专门设立的组件，主要负责为TSM管理器分配License、分配Microsoft Windows操作系统补丁模板、分配策略模板、分配软件分发任务。

TSM管理中心的具体功能有：管理TSM管理器，管理TSM管理器的License，管理策略模板，管理Microsoft Windows操作系统补丁，管理软件分发任务。

**TSM管理器**

TSM管理器是TSM的管理服务器。管理员通过IE浏览器登录TSM管理器进行日常维护操作。

TSM管理器的主要功能包括：系统配置，组织人员管理，安全策略管理，补丁管理，软件分发，资产管理，公告管理，报表管理。

**TSM控制器**

TSM控制器是TSM的控制服务器。TSM控制器主要负责验证终端用户的身份、对终端主机进行安全检查，以及与准入控制设备联动实现最小授权的访问控制等。

TSM控制器的主要功能包括：向TSM代理、Web Agent插件和Web客户端提供服务，与安全接入控制网关联动控制终端主机接入受控网络，与支持802.1x的交换机联动控制终端主机接入受控网络。

**扫描器**

扫描器的作用是发现和管理网络中现有的设备，尤其是已经安装TSM代理终端主机数量和未安装TSM代理的终端主机数量，在管理员制定或调整TSM代理的部署策略时作为参考的依据。

部署TSM代理是终端安全管理业务逐步推行的过程，按阶段分可分为试点和推广两个阶段，最终的目标是实现终端安全业务全覆盖。在终端安全管理业务逐步推行的过程中，管理员重点关注的是，如何确保所有的终端主机全部安装TSM代理，确保终端安全不会成为网络安全中最薄弱的环节。

扫描器是为了帮助管理员发现没有安装TSM代理的终端主机而开发的，主要功能有：通过扫描任务发现网络中的设备，能够识别已经安装TSM代理的终端主机和尚未安装TSM代理的终端主机，允许管理员标识需要安装TSM代理的终端主机和不需要安装TSM代理的终端主机，支持实时启动和停止扫描任务，支持周期性的扫描任务和一次性的扫描任务，支持按IP地址段和按ARP表两种方式发现设备，在发现新的设备接入受控网络和TSM代理被卸载时以告警邮件的方式提醒管理员，支持对设备进行分组管理。

**安全**接入控制**网关**

安全接入控制网关用于控制终端访问受控网络的权限，向隶属不同角色的终端用户和不同安全状况的终端用户开放不同的权限。

安全接入控制网关的主要功能包括：根据TSM控制器反馈的信息开放终端用户访问受控网络的权限，防止外部非授权的终端用户访问企业的受控网络，防止内部合法但不安全的终端用户访问企业的受控网络，隔离连接到受控网络但没有进行安全认证的终端用户，支持逃生通道。

**802.1x**交换机

802.1x交换机的主要功能是对终端主机进行接入控制。通过端口控制技术，保证只有通过身份认证的终端主机才能接入受控网络，防止未经授权的终端主机接入受控网络。

TSM服务器对应于IEEE802.1x的认证服务器系统，用户接入层设备则实现IEEE802.1x的接入控制单元，IEEE802.1x的用户接入系统集成在TSM代理中。

接入控制单元的每个物理端口内部有受控端口和非受控端口等逻辑划分。非受控端口始终处于双向连通状态，主要用来传递EAPOL协议帧，可保证随时接收用户接入系统发出的认证EAPOL报文。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。

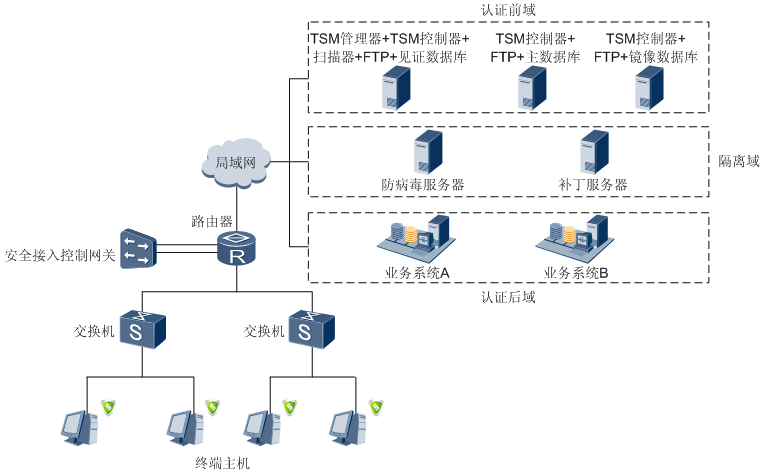
**TSM代理**

TSM代理是TSM中的一个组件，作为TSM的客户端安装在终端主机侧，负责与TSM管理器联动，实施管理员在TSM管理器定制的安全管理规则。

TSM代理根据安装过程的不同可以分为需要依照安装向导在终端主机安装的TSM代理和通过插件注册方式实现的Web Agent插件。

TSM代理的主要功能包括：身份认证，安全认证，资产管理，补丁管理，软件分发，公告管理。

TSM系统部署组网图



### TSM性能指标

* **TSM控制器性能指标**

介绍TSM代理在进行身份认证和执行策略时的性能指标。

|  |  |
| --- | --- |
| **性能项目** | **性能指标** |
| 单台TSM控制器支持的最大终端用户数 | 10000 |
| 单台TSM控制器平均每分钟处理进行认证的终端主机数量 | 2500 |
| 终端主机上线成功率 | 在单台TSM控制器平均每分钟完成2500次身份认证的情况下，终端主机上线成功率大于99%。 |
| 终端主机认证时延 | 在单台TSM控制器平均每分钟完成2500次身份认证的情况下，终端主机的认证时延小于等于10s。 |
| 违规信息保存的最长时间 | 6个月 |
| 与安全接入控制网关心跳检测时间 | 30s |

* **TSM代理性能指标**

介绍TSM代理在进行身份认证和执行策略时的性能指标。

|  |  |
| --- | --- |
| **性能项目** | **性能指标** |
| 在不执行任何策略时Microsoft Windows XP的认证时间 | ≤3s |
| 在不执行任何策略时Microsoft Windows XP最大内存占用 | 29MB |
| 在执行所有策略时Microsoft Windows XP最大内存占用 | 35MB |
| 在不执行任何策略时Microsoft Windows Vista的认证时间 | ≤3s |
| 在不执行任何策略时Microsoft Windows Vista最大内存占用 | 30MB |
| 在执行所有策略时Microsoft Windows Vista最大内存占用 | 36MB |
| CPU平均占用率 | 15% |
| 与TSM控制器之间的心跳检测时间 | 30s |

## 图示



# 防火墙基础实验

## 安全连接USG2000/5100防火墙

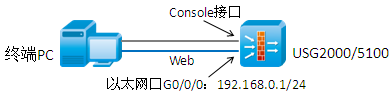
### 实验目的

实现Web方式远程安全管理，Web 登录认证使用AAA认证方式。

### 组网设备

终端PC 1台、USG2000/5100防火墙1台

### 实验拓扑图



### 配置步骤

步骤一：终端PC连接USG防火墙以太网口，进入Web配置界面

**提示**：USG防火墙缺省配置如下：

* 设备已配置默认管理IP地址，IP地址为192.168.0.1/24。其中USG2110-X/2100和USG2100BSR/HSR设备配置在Vlanif1接口上，8个LAN口默认加入到了VLAN1,可以将PC连接到任意一个LAN口。USG2200/5100、USG2200BSR/HSR和USG5100BSR/HSR设备配置在GE0/0/0接口上。
* 在配置了默认管理IP的接口上已开启了DHCP服务，可以为下挂PC自动分配范围为192.168.0.2/24～192.168.0.254/24的IP地址。
* 已开启Web管理功能（缺省配置基于http，建议修改为https）。
* 已创建一个超级管理员用户，用户名为admin，密码为Admin@123，管理员权限为3级。为保证系统安全，登录后请尽快修改密码；

1. 在终端PC上单击“开始 > 程序 > Internet Explorer”，或双击图标，启动IE浏览器；
2. 在浏览器地址栏输入http://192.168.0.1显示Web登录框；
3. 在“语言”中选择“简体中文”，在“用户名”中输入Web用户名“admin”，在“密码”中输入密码“Admin@123”，见下图所示；

**IE浏览器登录框**

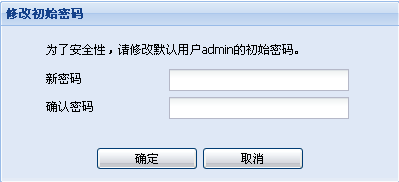


**提示:**Web系统支持“简体中文”和“English”两种语言；

系统默认用户admin是一个具有管理员权限的3级用户，其用户名为admin，密码为Admin@123;为了系统安全，使用默认用户admin登录时，建议尽快修改初始密码。

1. 单击“登录”，显示“修改初始密码”界面，见下图所示；

**修改初始密码**



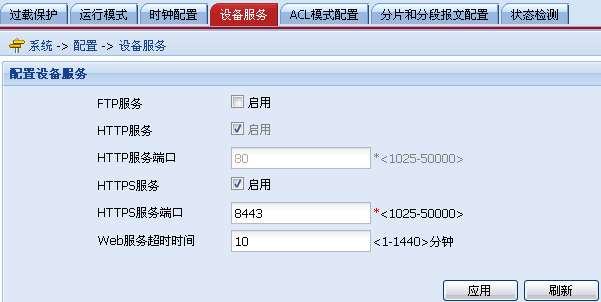
**提示:**

* 在培训实验环境，请单击“取消”，无需进行密码修改；
* 在实际应用环境，请根据客户要求输入新密码。新密码为字符串形式，是字母、数字或其他特殊字符中两种及以上的组合。不支持空格和问号，长度范围是1～16，且不能为Admin@123。
* 取消密码修改或完成密码修改后，将进行Web配置界面；

步骤二：启用Web安全管理功能，禁用Web管理功能

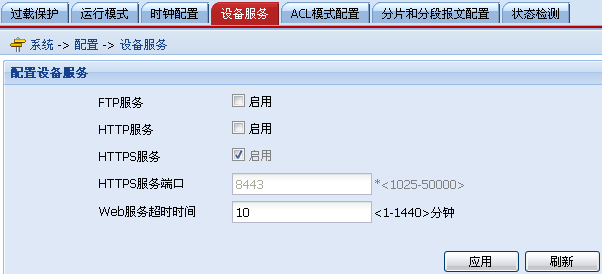
1. 在“菜单”导航树中选择“系统->配置->设备服务”，启用“HTTPS服务”，在“HTTPS服务端口”输入“8443” 后单击“应用”，见下图所示；

**设备服务(启用HTTPS服务)**



1. 在浏览器地址栏输入<https://192.168.0.1:8443>，在“用户名”中输入Web用户名“admin”，在“密码”中输入密码“Admin@123”进入Web安全配置界面；
2. 在“菜单”导航树中选择“系统->配置->设备服务”，禁用“HTTP服务”后单击“应用”，见下图所示；

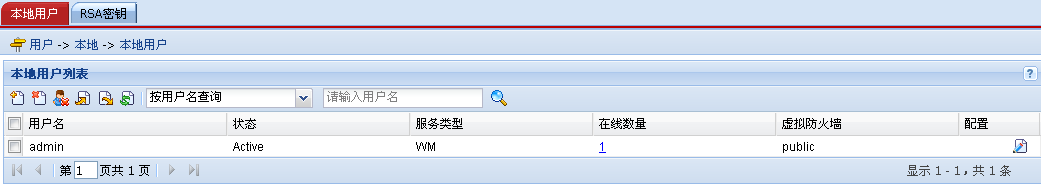
**设备服务(禁用HTTP服务)**



步骤三：新建Web安全管理功能用户帐号

1. 在“菜单”导航树中选择“用户->本地->本地用户”，见下图所示；

**本地用户**

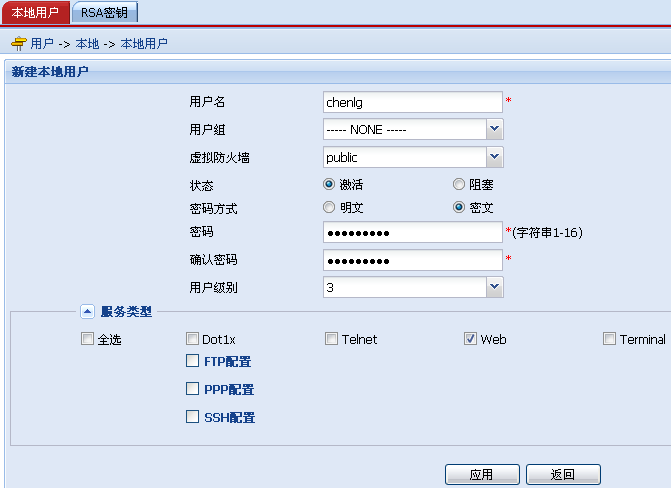


1. 单击“”新建本地用户帐号，在“用户名”中输入Web用户名“chenlg”，选择密码方式“密文”后在“密码”和“确认密码”中输入密码“Admin@123”。用户级别输入“3”，服务类型可只选择“Web” 后单击“应用”。见下图所示；

**提示:**

* 为了体现分级分权安全管理，建议根据企业IT业务管理需求设置不同权限管理员或操作员帐号；

**新建本地用户帐号**



### 验证结果

1. 在浏览器地址栏输入https://192.168.0.1显示安全Web登录框；
2. 在“语言”中选择“简体中文”，在“用户名”中输入Web用户名“chenlg”，在“密码”中输入密码“Admin@123”，成功进入Web安全配置界面。

## 防火墙区域间连接

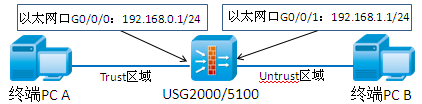
### 实验目的

实现USG防火墙接口IP地址与安全区域之间的关系，为后续域间包过滤配置提供基础。

### 组网设备

终端PC 2台、USG2000/5100防火墙1台

### 实验拓扑图



### 实验步骤

步骤一：配置防火墙接口IP地址和与安全区域之间对应关系

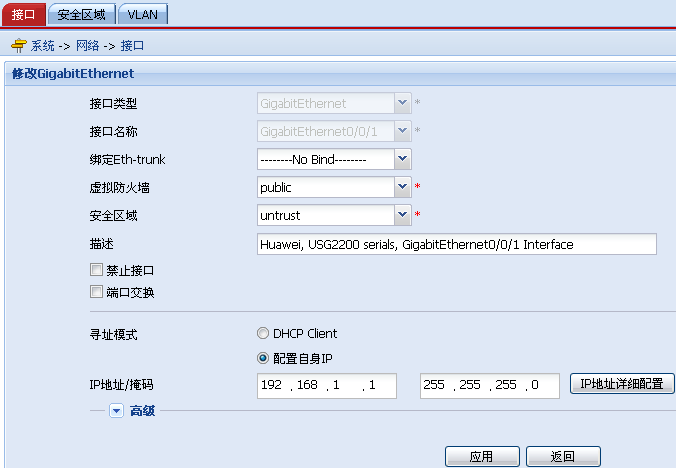
1. 在“菜单”导航树中选择“系统->网络->接口”，完成接口IP地址和安全区域配置，见下图所示；

**配置三层接口信息**



1. 单击“”进入“修改GigabitEthernet0/0/1”，，在“安全区域”中选择“untrust”，在“IP地址/掩码”中输入“192.168.1.1、255.255.255.0”后单击“应用”，见下图所示；

**配置三层接口IP地址和安全区域**



### 验证结果

1. 在“菜单”导航树中选择“系统->网络->接口”，检查G0/0/0、G0/0/1所对应的IP地址和安全区域，见下图所示；

**验证配置结果**



## 防火墙软件升级

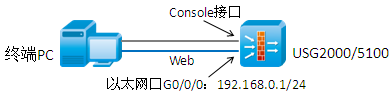
### 实验目的

采用Web的方式对防火墙进行版本升级

### 组网设备

终端PC 1台、USG2000/5100防火墙1台

### 实验拓扑图

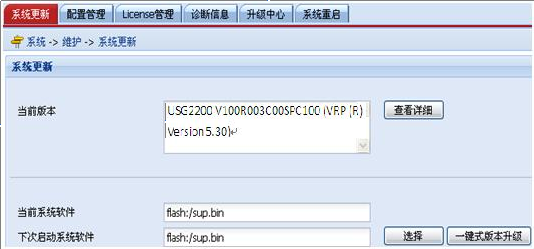


### 配置步骤

步骤一：进入Web升级界面

1. 在“菜单”导航树中选择“系统->维护”；
2. 选择“系统更新”页签，“当前系统软件”和“下次启动系统软件”对应的显示信息即为系统软件信息，见下图所示；

**一键式版本升级**



步骤二：上传升级版本文件

1. 单击“一键式版本升级”，显示“一键式版本升级”界面；
2. 可选：在升级系统软件前，建议保存当前系统配置，并将设备上的告警信息、日志信息和配置信息导出到本地；

1）单击“告警信息”对应的“导出”，显示“文件下载”界面，单击“保存”，将告警信息保存到本地；

2）单击“日志信息”对应的“导出”，显示“文件下载”界面，单击“保存”，将日志信息保存到本地；

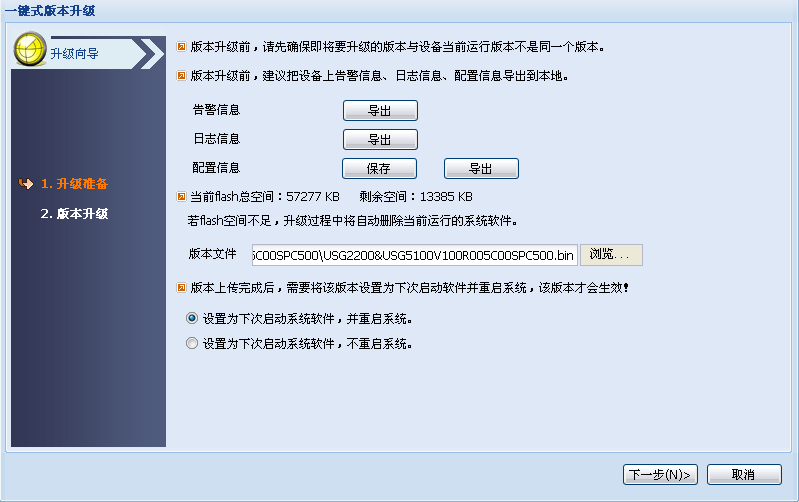
3）单击“保存”，保存当前系统配置；

4）这里可以选择覆盖当前配置文件或另存一份配置文件，请根据需要进行选择；

5）单击配置信息对应的“导出”，显示“文件下载”界面，单击“保存”，将配置信息保存到本地；

1. 单击“浏览”，选择版本文件“USG2200&USG5100V100R005C00SPC500.bin”；
2. 根据当前网络是否允许设备升级后立即重启，选中“设置为下次启动系统软件，并重启系统”或“设置为下次启动系统软件，不重启系统”前的单选框，单击“下一步”，见下图所示；

**一键式版本升级**



步骤三：版本文件升级

1. 单击“下一步”，设备将开始自动升级系统软件，见下图所示；

**版本文件升级**



**提示:**进行下一步操作前，请确认待升级的系统软件版本不同于当前使用的系统软件版本。

在升级过程中，请勿手动中断升级。

### 验证结果

1. 在“菜单”导航树中选择“系统->维护”，选择“系统更新”页签，查看“当前版本”信息，见下图所示；

**版本升级状态**



## 防火墙静态路由实验

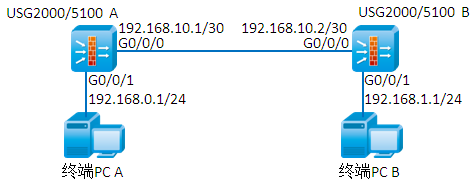
### 实验目的

通过配置静态路由，使两台终端PC之间能够通过USG防火墙互通。

### 组网设备

终端PC 2台、USG2000/5100防火墙2台

### 实验拓扑图



### 配置步骤

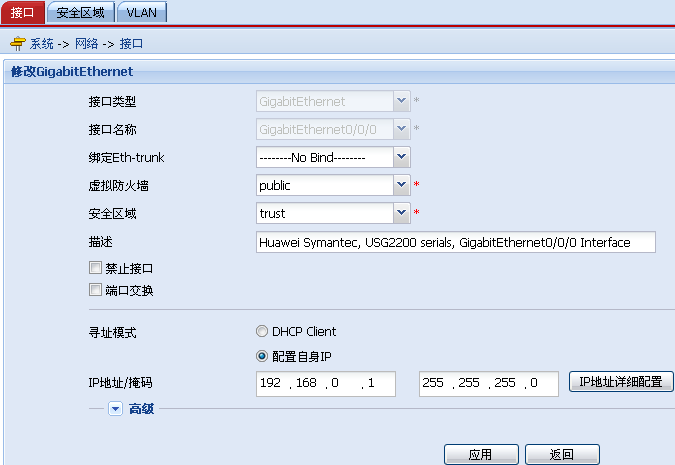
步骤一：静态路由配置举例数据规划表

|  |  |  |
| --- | --- | --- |
| **设备信息** | **接口信息** | **IP地址规划** |
| USG2000/5100 A | G0/0/0 | 192.168.10.1/30 |
| G0/0/1 | 192.168.0.1/24 |
| USG2000/5100 B | G0/0/0 | 192.168.10.2/30 |
| G0/0/1 | 192.168.1.1/24 |
| 终端PC A | 本地连接接口 | 192.168.0.2/24 |
| 终端PC B | 本地连接接口 | 192.168.1.2/24 |

步骤二：配置USG A接口IP地址(G0/0/0)，并将接口加入Trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“Trust”，“IP地址/掩码”选择“192.168.0.1”、“255.255.255.0”；
3. 单击“应用”，见下图所示；

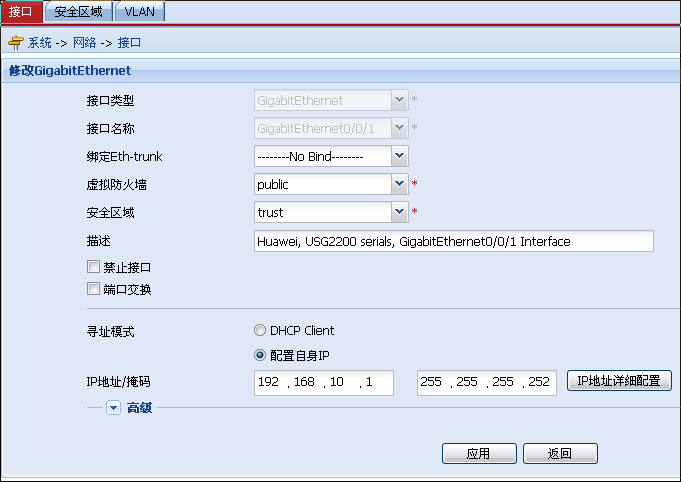
**USG A接口IP地址配置(G0/0/0)**



步骤三：配置USG A接口IP地址(G0/0/1)，并将接口加入Untrust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“trust”，“IP地址/掩码”选择“192.168.10.1”、“255.255.255.252”；
3. 单击“应用”，见下图所示；

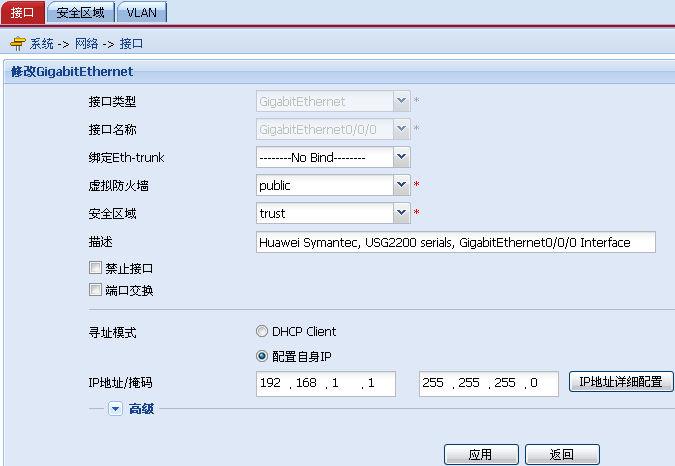
**USG A接口IP地址配置(G0/0/1)**



步骤四：配置USG B接口IP地址(G0/0/0)，并将接口加入Trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“trust”，“IP地址/掩码”选择“192.168.1.1”、“255.255.255.0”；
3. 单击“应用”，见下图所示；

**USG B接口IP地址配置(G0/0/0)**



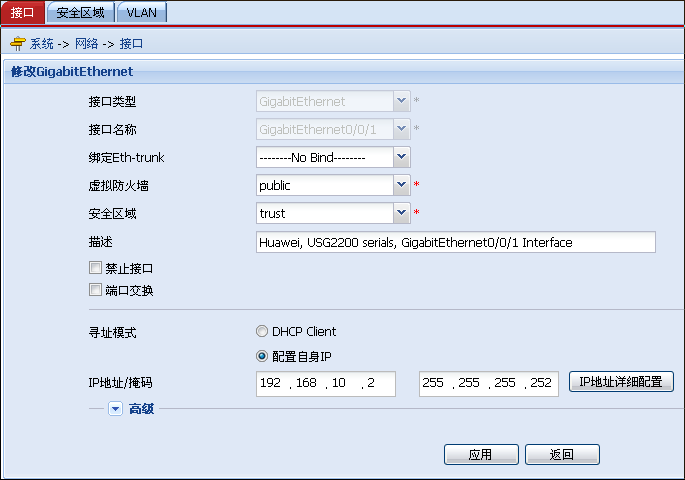
**提示：**

* 将G0/0/0接口更改为192.168.1.1后，需要将PC机的IP地址修改为192.168.1.X网段地址，通过<http://192.168.1.1>来重新登陆防火墙继续配置。

步骤五：配置USG B接口IP地址(G0/0/1)，并将接口加入trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“trust”，“IP地址/掩码”填入“192.168.10.2”、“255.255.255.252”；
3. 单击“应用”，见下图所示；

**USG A接口IP地址配置(G0/0/1)**



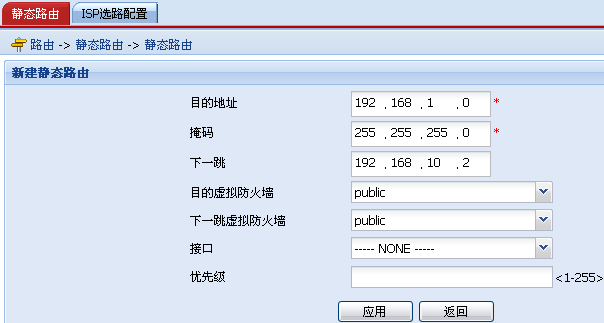
**提示:** 配置接口若为交换LAN接口（二层接口）将不能配置IP地址。如果需要通过交换LAN口进行三层通信，需要把交换LAN口加入VLAN，在VLAN对应的Vlanif接口上配置IP地址。

缺省情况下，任何一个LAN接口都已加入VLAN 1，且Vlanif 1接口IP地址为192.168.0.1/24。修改Vlanif 1接口IP地址将会导致Telnet和Web用户通信中断，需要使用新的IP地址重新登录。建议使用其他Vlanif接口。

步骤六：配置USG A静态路由

1. 在“菜单”导航树中选择“路由 > 静态路由> 静态路由”。选择“静态路由”页签，默认已选择此标签；
2. 单击，在“新建静态路由”界面中“目的地址”填写“192.168.1.0”，“掩码”选择“255.255.255.0”，“下一跳”选择“192.168.10.2”。
3. 单击“应用”，见下图所示；

**USG A静态路由配置**

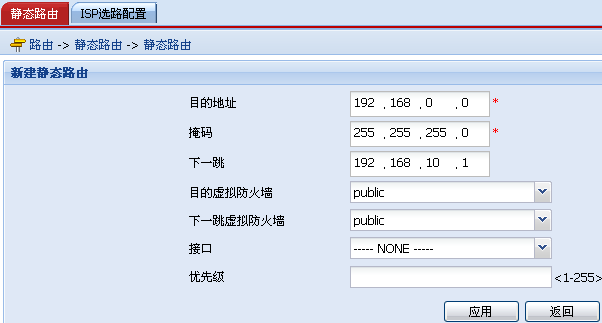


**提示**:对于USG系列，将接口加入安全区域，并配置域间包过滤，以保证网络基本通信正常。对于USG BSR/HSR系列，不需要将接口加入安全区域以及配置包过滤。

步骤七：配置USG B静态路由

1. 在“菜单”导航树中选择“路由 > 静态路由> 静态路由”。选择“静态路由”页签，默认已选择此标签；
2. 单击，在“新建静态路由”界面中“目的地址”填写“192.168.0.0”，“掩码”选择“255.255.255.0”，“下一跳”选择“192.168.10.1”。
3. 单击“应用”，见下图所示；

**USG B静态路由配置**



**提示**: 对于USG系列，将接口加入安全区域，并配置域间包过滤，以保证网络基本通信正常。对于USG BSR/HSR系列，不需要将接口加入安全区域以及配置包过滤。接口加入到同一安全区域时，接口之间可以互相访问，不需要配置域间包过滤。

### 验证结果

1. 在终端PC A（192.168.0.2） ping 终端PC B（192.168.1.2），IP可达；
2. 在终端PC B（192.168.1.2） ping 终端PC A（192.168.0.2），IP可达；

## 防火墙OSPF动态路由实验

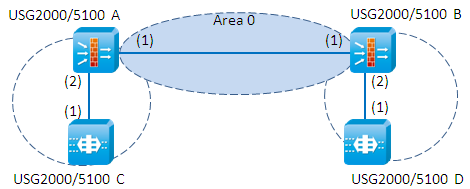
### 实验目的

通过配置OSPF路由协议，使两台终端PC之间能够通过USG防火墙互通。

### 组网设备

USG2000/5100防火墙4台

### 实验拓扑图



### 配置步骤：

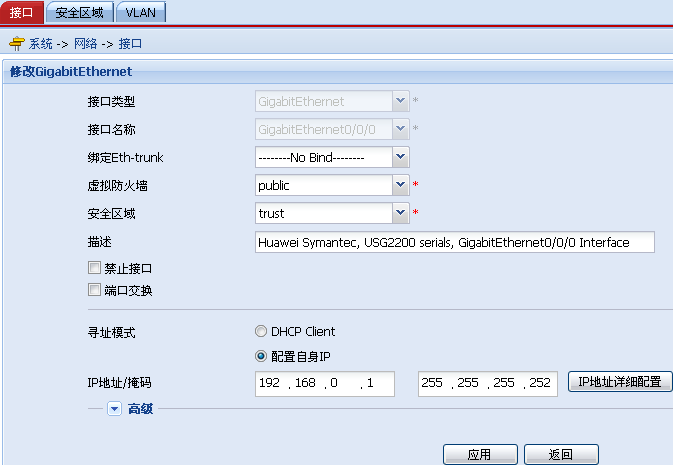
步骤一：OSPF动态路由配置举例数据规划表

|  |  |  |
| --- | --- | --- |
| **设备信息** | **接口信息** | **IP地址规划** |
| USG2000/5100 A | （1）G0/0/0 | 192.168.0.1/30 |
| （2）G0/0/1 | 192.168.1.1/30 |
| USG2000/5100 B | （1）G0/0/0 | 192.168.0.2/30 |
| （2）G0/0/1 | 192.168.2.1/30 |
| USG2000/5100 C | （1）G0/0/1 | 192.168.1.2/30 |
| USG2000/5100 D | （1）G0/0/1 | 192.168.2.2/30 |

步骤二：配置USG A接口IP地址(G0/0/0)，并将接口加入Trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“Trust”，“IP地址/掩码”选择“192.168.0.1”、“255.255.255.252”；
3. 单击“应用”，见下图所示；

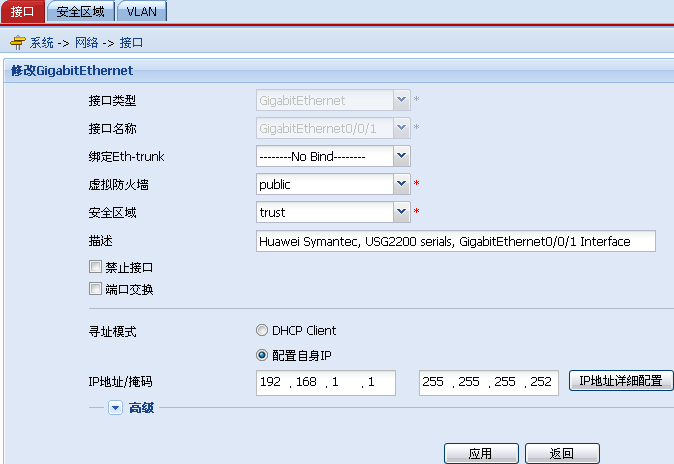
**USG A接口IP地址配置(G0/0/0)**



步骤三：配置USG A接口IP地址(G0/0/1)，并将接口加入Trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“Trust”，“IP地址/掩码”选择“192.168.1.1”、“255.255.255.252”；
3. 单击“应用”，见下图所示；

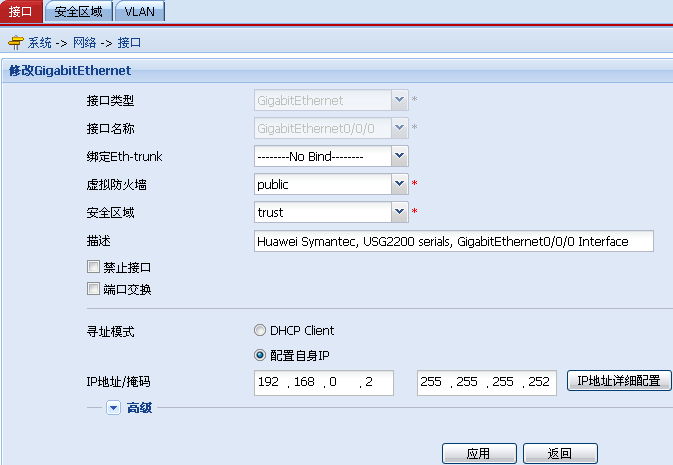
**USG A接口IP地址配置(G0/0/1)**



步骤四：配置USG B接口IP地址(G0/0/0)，并将接口加入Trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“Trust”，“IP地址/掩码”选择“192.168.0.2”、“255.255.255.252”；
3. 单击“应用”，见下图所示；

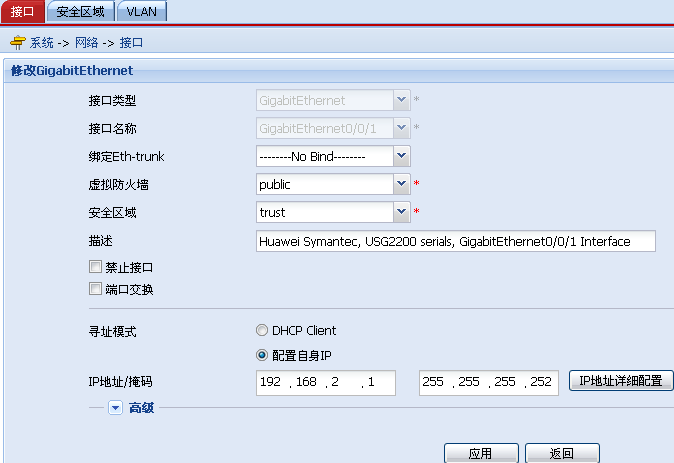
**USG B接口IP地址配置(G0/0/0)**



步骤五：配置USG B接口IP地址(G0/0/1)，并将接口加入Trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“Trust”，“IP地址/掩码”选择“192.168.2.1”、“255.255.255.252”；
3. 单击“应用”，见下图所示；

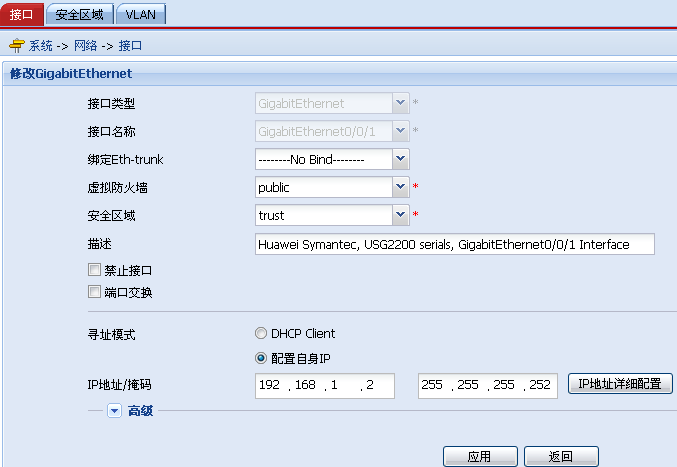
**USG B接口IP地址配置(G0/0/1)**



步骤六：配置USG C接口IP地址(G0/0/1)，并将接口加入Trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“Trust”，“IP地址/掩码”选择“192.168.1.2”、“255.255.255.252”；
3. 单击“应用”，见下图所示；

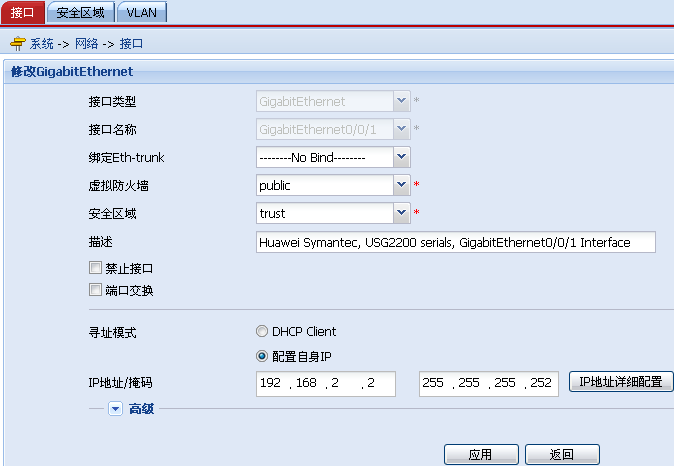
**USG C接口IP地址配置(G0/0/1)**



步骤七：配置USG D接口IP地址(G0/0/1)，并将接口加入Trust安全区域

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签；
2. 单击，在“系统 > 网络 > 接口”界面中“安全区域”选择“Trust”，“IP地址/掩码”选择“192.168.2.2”、“255.255.255.252”；
3. 单击“应用”，见下图所示；

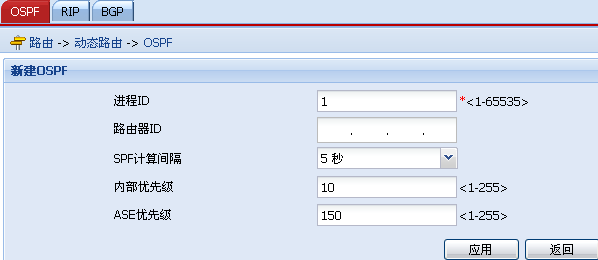
**USG D接口IP地址配置(G0/0/1)**



步骤八：配置OSPF动态路由

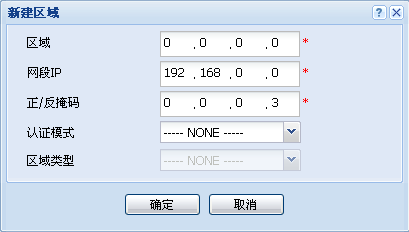
1. 在“菜单”导航树中选择“路由 > 动态路由> OSPF”。选择“OSPF”页签，默认已选择此标签；
2. 单击，在“新建OSPF”界面中“路由器ID”填写“0.0.0.0”，单击“应用”，见下图所示；

**USG A OSPF动态路由配置**



1. 单击“高级”，完成“区域配置列表”；
2. 单击，显示“新建区域”界面。在“区域”填写“0.0.0.0”，“网段IP”填写“192.168.0.0”，“正/反掩码”填写“0.0.0.3”。单击“确定”，见下图所示；

**USG A 新建骨干区域配置**

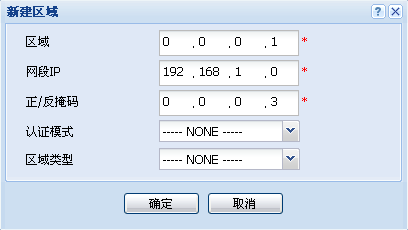


**提示**：对于USG系列，将接口加入同一个安全区域（例如Trust），无需配置域间包过滤，就可以保证网络基本通信正常；

区域0.0.0.0是专门提供给骨干区域使用；

1. 配置OSPF区域1，并将192.168.1.0/30网段加入区域1。单击，显示“新建区域”界面。在“区域”填写“0.0.0.1”，“网段IP”填写“192.168.1.0”，“正/反掩码”填写“0.0.0.3”。单击“确定”，见下图所示；

**USG A 新建其它区域配置**



1. 配置USG B：USG B和USG A配置过程基本相同，不同之处在于：
   * USG B接口的IP地址与USG A各接口的IP地址不相同；
   * USG B配置OSPF时的路由器ID与USG A不同，USG B配置OSPF时的路由器ID设为2.2.2.2；
   * USG B上配置区域及加入网段与USG A不相同。USG B上配置OSPF区域0，将192.168.0.0/30网段加入区域0，配置OSPF区域2，将192.168.2.0/30网段加入区域2；
2. 配置USG C。 USG C和USG A的配置过程基本相同，不同之处在于：
   * USG C接口的IP地址与USG A各接口的IP地址不相同；
   * USG C配置OSPF时的路由器ID与USG A不同，USG C配置OSPF时的路由器ID设为3.3.3.3；
   * USG C上配置区域及加入网段与USG A不相同。USG C上配置OSPF区域1，将192.168.1.0/30网段加入区域1；
   * 配置USG D：USG D和USG A的配置过程基本相同，不同之处在于：
   * USG D接口的IP地址与USG A各接口的IP地址不相同。
   * USG D配置OSPF时的路由器ID与USG A不同，USG D配置OSPF时的路由器ID设为4.4.4.4。
   * USG D上配置区域及加入网段与USG A不相同。USG D上配置OSPF区域2，将192.168.2.0/30网段加入区域2。

### 验证结果

1. 在USG C ping 终端USG D，IP可达；
2. 在USG D ping 终端USG C，IP可达；

# 防火墙域间包过滤实验

## 本地策略实验

### 实验目的

通过配置本地策略，实现其他安全区域和本地区域（Local）间的数据控制。

**提示：**

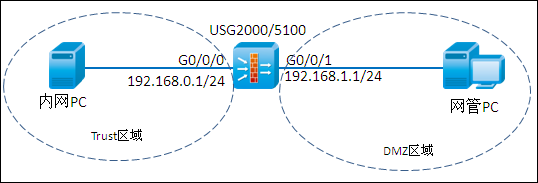
出厂配置情况下，USG2200/5100的Gibitethernet0/0/0属于trust区域，trust区域和Local区域可以互相访问。USG2100的8个LAN口属于VLAN1,VLAN1的三层口属于属于trust区域，trust区域和Local区域可以互相访问。

### 组网设备

USG2000/5100防火墙1台、网管PC 1台

### 实验拓扑图

1. 允许DMZ区域内网管PC对USG防火墙设备进行管理；



### 配置步骤

步骤一：配置接口IP地址和所属安全区域

1. 选择菜单栏中的“系统—>网络”，选择“接口”页签，查看三层接口列表，见下图所示；

**查看三层接口列表**



1. G0/0/0、G0/0/1、G6/0/0接口的IP地址和所属安全区配置，请参见《2.2 防火墙区域间连接》；
   * G0/0/0: 所属安全区域为trust，IP地址为192.168.0.1/24；
   * G0/0/1: 所属安全区域为DMZ，IP地址为192.168.1.1/24；

步骤二：配置本地策略（DMZ至Local）

1. 选择菜单栏中的“防火墙—>策略”，选择“本地策略”页签；
2. 在“对设备访问控制列表”栏单击“”进入“新建对设备访问控制”，在“源安全区域”中选择“DMZ”，在“源地址”中填入“192.168.1.0\0.0.0.255”，在“时间段”中选择“all”，在“动作”中选择“permit”后单击“应用”。见下图所示；

**新建本地策略（DMZ至Local）**



### 结果检查

1. 网管PC可以对USG防火墙进行Web管理；

## 转发策略实验

### 实验目的

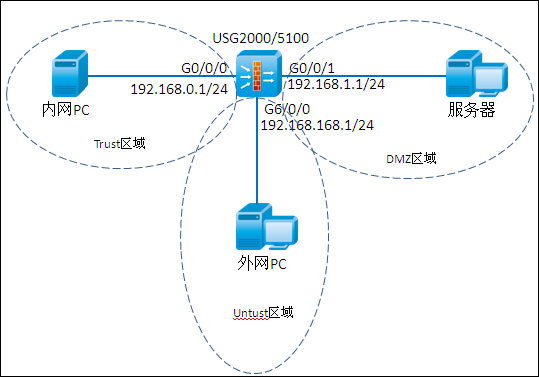
通过配置转发策略，实现除本地区域（Local）外的其他安全域间的数据控制。

### 组网设备

内网服务器1台、USG2000/5100防火墙1台、终端PC 2台

### 实验拓扑图

1. DMZ区域允许Trust区域和Untrust区域PC对其进行访问；
2. 禁止其它安全区域之间的互访；



### 配置步骤

步骤一：配置接口IP地址和所属安全区域

1. 选择菜单栏中的“系统—>网络”，选择“接口”页签，查看三层接口列表，见下图所示；

**查看三层接口列表**

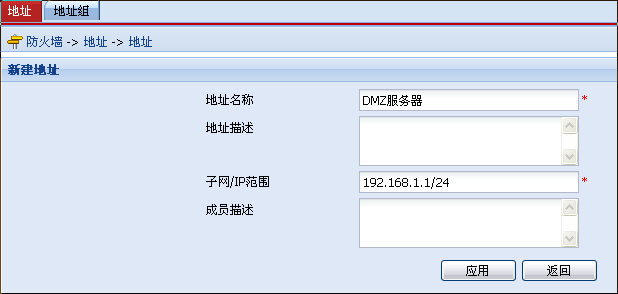


1. G0/0/0、G0/0/1、G6/0/0接口的IP地址和所属安全区配置，请参见《2.2 防火墙区域间连接》；
   * G0/0/0: 所属安全区域为Trust，IP地址为192.168.0.1/24；
   * G0/0/1: 所属安全区域为DMZ，IP地址为192.168.1.1/24；
   * G6/0/0: 所属安全区域为Untrust，IP地址为192.168.168.1/24；

步骤二：配置服务器地址集

1. 选择菜单栏中的“防火墙—>地址”，选择“地址”页签；
2. 单击“”进入“新建地址”，在“地址名称”填写“DMZ服务器”，在“子网/IP范围”中输入“192.168.1.0/24”后单击“应用”，见下图所示；

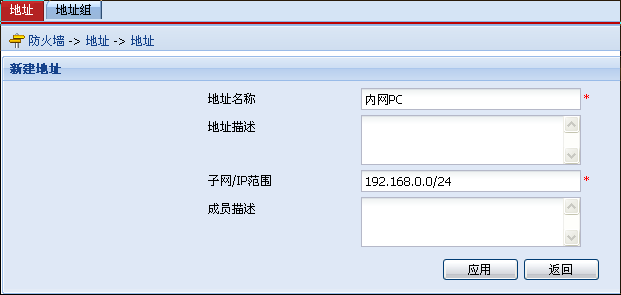
**新建地址（DMZ服务器）**



步骤三：配置内网PC地址集

1. 选择菜单栏中的“防火墙—>地址”，选择“地址”页签；
2. 单击“”进入“新建地址”，在“地址名称”填写“内网PC”，在“子网/IP范围”中输入“192.168.0.0/24”后单击“应用”，见下图所示；

**新建地址（内网PC）**



步骤四：配置外网PC地址集

1. 选择菜单栏中的“防火墙—>地址”，选择“地址”页签；
2. 单击“”进入“新建地址”，在“地址名称”填写“外网PC”，在“子网/IP范围”中输入“192.168.168.0/24”后单击“应用”。见下图所示；

**新建地址（外网PC）**



步骤五：配置服务器服务集

1. 选择菜单栏中的“防火墙—>服务”，选择“自定义服务”页签；
2. 单击“”进入“新建自定义服务”，在“自定义服务名称”填写“公共业务服务资源”，在“自定义服务描述”中输入“主要包括：Web、FTP、E-mail等提供给内外部人员访问服务。”。在本配置页面单击“”配置协议类型，协议类型选择“TCP”，目的端口输入“80、21、25、110” 后单击“应用”。见下图所示；

**自定义服务（DMZ服务器）**



步骤六：配置时间段

1. 选择菜单栏中的“防火墙—>时间段”，选择“时间段”页签；
2. 单击“”进入“新建时间段”，在“时间段名称”填写“Workday”，在“开始时间”中选择“08:30”, 在“结束时间”中选择“18:00”。在“每周生效时间”中选择“星期一 至 星期五”后单击“应用”。见下图所示；

**新建时间段**



步骤七：配置转发策略（Trust至DMZ）

1. 选择菜单栏中的“防火墙—>策略”，选择“转发策略”页签；
2. 单击“”进入“新建转发策略”，在“源安全区域”中选择“Trust”，在“目的安全区域”中选择“DMZ”, 在“源地址”中选择“内网PC” 在“目的地址”中选择“dmz服务器”，在“服务”多选中选择“公共业务服务资源和icmp”。在“时间段”中选择“all”，在“动作”中选择“permit”后单击“应用”。见下图所示；

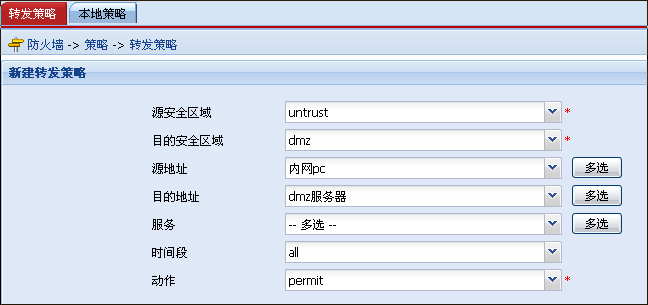
**新建转发策略（Trust至DMZ）**



步骤八：配置转发策略（Untrust至DMZ）

1. 选择菜单栏中的“防火墙—>策略”，选择“转发策略”页签；
2. 单击“”进入“新建转发策略”，在“源安全区域”中选择“Untrust”，在“目的安全区域”中选择“DMZ”, 在“源地址”中选择“外网PC” 在“目的地址”中选择“dmz服务器”，在“服务”多选中选择“公共业务服务资源”和icmp””。在“时间段”中选择“all”，在“动作”中选择“permit”后单击“应用”。见下图所示；

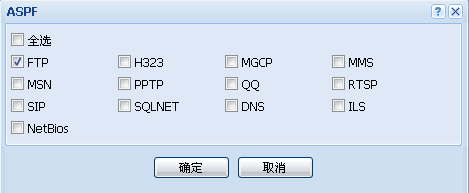
**新建转发策略（Untrust至DMZ）**



步骤九：启用ASPF（Trust与Untrust至DMZ）

1. 选择菜单栏中的“防火墙—>策略”，选择“转发策略”页签；
2. 单击“”进入“ASPF”配置页面选择“FTP”后单击“确定”。见下图所示；

**启用ASPF功能**



### 结果检查

1. 内网PC可以访问DMZ服务器，包括FTP等多通道协议服务；
2. 外网PC可以访问DMZ服务器，包括FTP等多通道协议服务；
3. 内网PC与外网PC不能互相访问；
4. DMZ服务器不能向内网PC或外网PC连接；

# 防火墙网络地址转换实验

## 基于源IP地址的NAT实验

### 实验目的

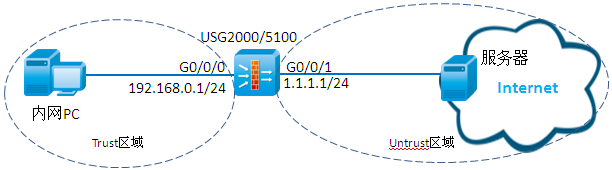
掌握防火墙基于源IP地址的NAT配置。

### 组网设备

终端PC 1台、PC服务器1台、USG2000/5100防火墙1台

### 实验拓扑图

1. 允许Trust区域内网PC访问Internet服务器系统，并进行源IP地址转换。地址池为1.1.1.1-1.1.1.10；



### 配置步骤

步骤一：配置接口IP地址和所属安全区域

1. 选择菜单栏中的“系统—>网络”，选择“接口”页签，查看三层接口列表，见下图所示；

**查看三层接口列表**



1. G0/0/0、G0/0/1接口的IP地址和所属安全区配置，请参见《2.2 防火墙区域间连接》；
   * G0/0/0: 所属安全区域为Trust，IP地址为192.168.0.1/24；
   * G0/0/1: 所属安全区域为Untrust，IP地址为1.1.1.0/24；

步骤二：配置内网PC地址集

1. 选择菜单栏中的“防火墙—>地址”，选择“地址”页签；
2. 单击“”进入“新建地址”，在“地址名称”填写“内网PC”，在“子网/IP范围”中输入“192.168.0.0/24”后单击“应用”，见下图所示；

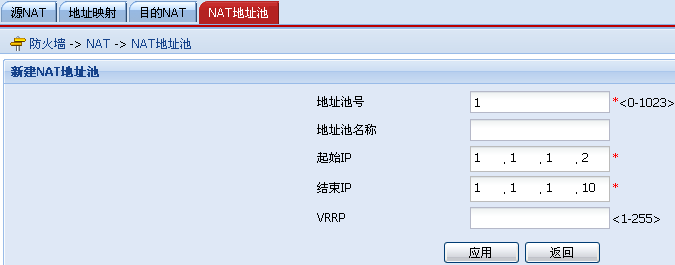
**新建地址（内网PC）**



步骤三：配置NAT地址池

1. 在“菜单”导航树中选择“防火墙 > NAT”。 选择“NAT地址池”页签。单击，显示“新建NAT地址池”界面；
2. 配置NAT地址池的各项参数，在“地址池号”栏输入“1”，在“起始IP” 栏输入“1.1.1.2”，在“结束IP” 栏输入“1.1.1.10”，后单击“应用”。见下图所示；

**NAT地址池**



步骤四：配置源NAT

1. 在“菜单”导航树中选择“防火墙 > NAT”。 选择“源NAT”页签。单击，显示“新建源NAT”界面；
2. 配置NAT地址池的各项参数，在“源安全区域”中选择“Trust”，在“目的安全区域”中选择“Untrust”，在“源地址”中选择“内网PC”，在“目的地址”中选择“any”，在“NAT地址池”中选择“1”，其它选择默认后单击“应用”。见下图所示；

**新建源NAT**



步骤五：配置域间包过滤规则

1. 选择菜单栏中的“防火墙—>策略”，选择“转发策略”页签；
2. 单击“”进入“新建转发策略”，在“源安全区域”中选择“Trust”，在“目的安全区域”中选择“Untrust”, 在“源地址”中选择“内网PC” 在“目的地址”中选择“any”，其它选择默认后单击“应用”。见下图所示；

**新建转发策略（Trust至Untrust）**

****

### 结果检查

1. 192.168.0.0/24 网段用户可以访问Internet，该安全区域其它网段的用户不能访问。提供访问Internet合法IP 地址池为1.1.1.2～1.1.1.10；
2. 源IP地址段192.168.0.0/24访问Internet被转化为1.1.1.2～1.1.1.10；

## 基于目的IP地址的NAT实验

### 实验目的

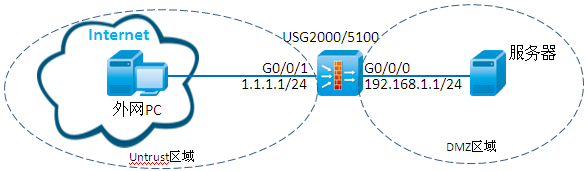
掌握防火墙基于目的IP地址的NAT配置。

### 组网设备

终端PC 1台、PC服务器1台、USG2000/5100防火墙1台

### 实验拓扑图

1. 内部服务器所在网段为192.168.1.0/24，客户端所在网段为1.1.1.0/24，可泛指Internet网段；
2. 内部服务器对外发布IP地址为1.1.1.2，外部PC访问1.1.1.2时将会被USG防火墙转换为192.168.1.2；

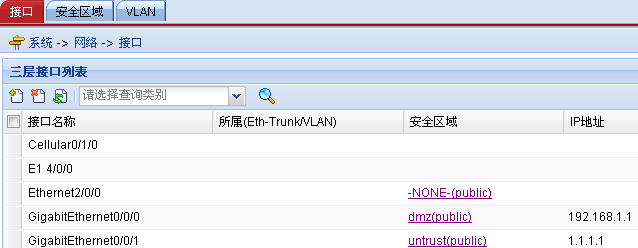


### 配置步骤

步骤一：配置接口IP地址和所属安全区域

1. 选择菜单栏中的“系统—>网络”，选择“接口”页签，查看三层接口列表，见下图所示；

**查看三层接口列表**



1. G0/0/0、G0/0/1接口的IP地址和所属安全区配置，请参见《2.2 防火墙区域间连接》；
   * G0/0/0: 所属安全区域为DMZ，IP地址为192.168.1.1/24；
   * G0/0/1: 所属安全区域为Untrust，IP地址为1.1.1.0/24；

步骤二：配置内部服务器地址集

1. 选择菜单栏中的“防火墙—>地址”，选择“地址”页签；
2. 单击“”进入“新建地址”，在“地址名称”填写“内部服务器”，在“子网/IP范围”中输入“192.168.1.0/24”后单击“应用”，见下图所示；

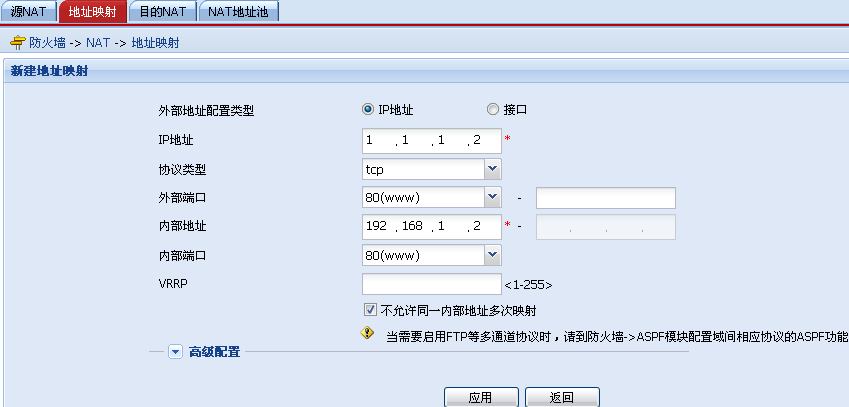
**新建地址（内部服务器）**



步骤三：配置内部服务器地址映射

1. 选择菜单栏中的“防火墙—>NAT”，选择“地址映射”页签；
2. 单击“”进入“新建地址映射”，在“IP地址”填写“1.1.1.2”，在“协议类型”选择“TCP”，在“外部端口”选择“80（www）”，在“内部地址”填写“192.168.1.2” ，在“内部端口”选择“80（www）”后单击“应用”，见下图所示；

**地址映射**



步骤四：配置域间包过滤规则

1. 选择菜单栏中的“防火墙—>策略”，选择“转发策略”页签；
2. 单击“”进入“新建转发策略”，在“源安全区域”中选择“Untrust”，在“目的安全区域”中选择“DMZ”, 在“源地址”中选择“any”， 在“目的地址”中选择“内部服务器”，在“服务”中选择“http”,其它选择默认后单击“应用”。见下图所示；

**新建转发策略（Trust至Untrust）**



### 结果检查

1. 选取1.1.1.0/24网段外部终端PC（Internet终端），尝试访问内部服务器的Web服，并在USG上查看会话表：
2. 选择“系统 > 信息”。选择“会话表”页签，查看会话表项信息。
3. 显示HTTP协议类型的会话表项，其中源IP地址为1.1.1.0/24网段IP地址、目的地址为Web服务器地址对外发布IP地址1.1.1.2和Web服务器内部IP地址192.168.1.2；
4. 以上显示说明内网服务器被成功访问，即基于目的IP地址的NAT策略（内部服务器）已命中；

## 双向NAT实验

### 实验目的

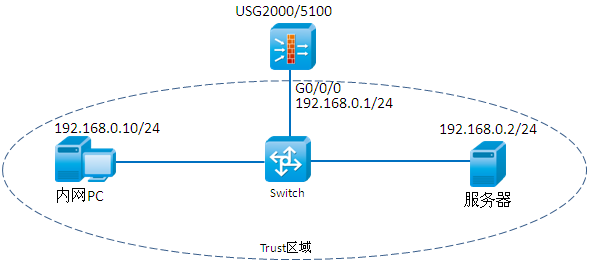
了解域内NAT使用场景，掌握域内NAT配置。

### 组网设备

终端PC 1台、PC服务器1台、USG2000/5100防火墙1台、交换机1台

### 实验拓扑图

1. FTP服务器和 内网PC 均在 USG2000/5100的 Trust 安全区域；
2. WWW服务器IP地址为 192.168.0.2，内网PC IP地址为 192.168.0.10，二者通过交换机与USG2000/5100相连；

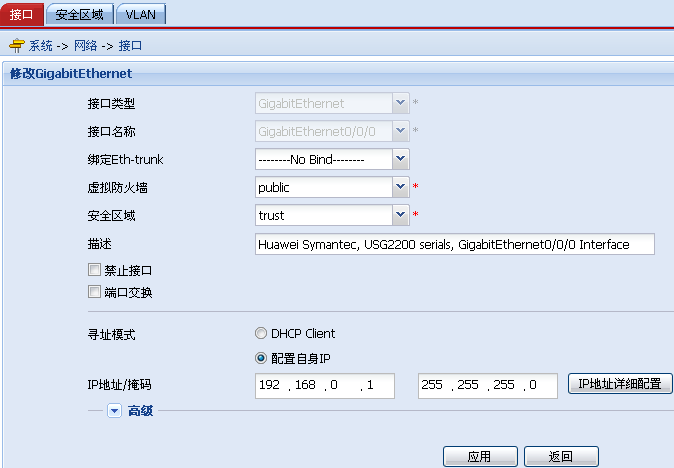


### 配置步骤

步骤一：配置接口IP地址和所属安全区域

1. 选择“系统>网络>接口”，更改G0/0/0口配置，将接口加入trust区域，更改ip地址为192.168.0.1/255.255.255.0。见下图所示；

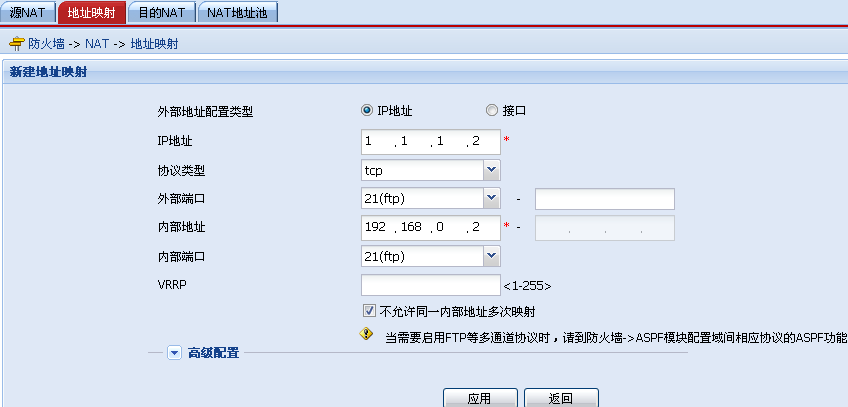
**修改G0/0/0接口配置信息**



步骤二：NAT地址映射配置

1. 配置 NAT地址映射。选择“防火墙>NAT>地址映射”，单击按钮；
2. 配置外部和内部服务器IP地址及协议类型服务信息，见下图所示；

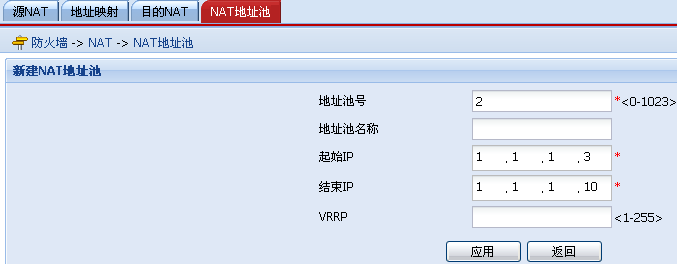
**新建地址映射**



步骤三：域内地址池配置

1. 配置域内地址池。选择“防火墙>NAT”，选择“NAT地址池”页签；
2. 单击按钮，在“地址池号”填写“2”，在“地址IP”和“结束IP”分别填写“1.1.1.3”和“1.1.1.10”，后单击“应用”，见下图所示；

**域内地址池配置**



步骤四：域内NAT配置

1. 配置域内NAT。选择“防火墙>NAT>源NAT”，单击按钮；
2. 配置源与目的安全区域均选择“Trust”，“源地址”选择“内部PC”, “NAT地址池”选择前面已配置的NAT地址池“2”。见下图所示；

**域内NAT配置**



### 结果检查

1. 内网PC可以通过公网地址访问内部服务器Server；

# 防火墙网络互联实验

## 防火墙VLAN实验

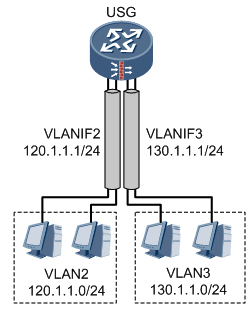
### 实验目的

配置VLAN，实现多个VLAN之间的互相通信功能

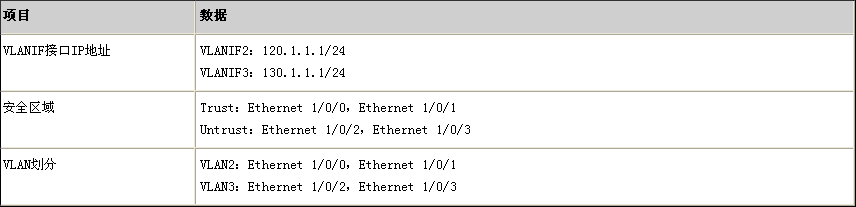
### 组网设备

4台主机、1台USG防火墙

### 实验拓扑图



配置VLAN间通过VLANIF接口通信举例的数据规划



### 配置步骤

步骤一：创建VLAN2，并加入相应接口。

1. 在“菜单”导航树中选择“系统 > 网络”。选择“VLAN”页签。
2. 单击，显示“新建VLAN”界面。参数配置如下图所示。



1. 单击“应用”。
2. 在“二层接口列表”中，单击，显示“加入接口”界面。参数配置如下图所示。



1. 单击“确定”。
2. 在“二层接口列表”中，单击，显示“加入接口”界面。参数配置如下图所示。



1. 单击“确定”。

步骤二：创建并配置VLANIF2。

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签。
2. 在“三层接口列表”界面中，单击，显示“新建接口”界面。
3. 在“接口类型”中选择“Vlanif”，“接口名称”中的接口号设为2。
4. 单击“应用”，显示“修改Vlanif”界面。参数配置如下：
   * 寻址模式：配置自身IP
   * IP地址/掩码：120.1.1.1 255.255.255.0
5. 单击“应用”。

步骤三：创建并配置VLANIF3。

1. 在“菜单”导航树中选择“系统 > 网络”。选择“接口”页签。
2. 在“三层接口列表”界面中，单击，显示“新建接口”界面。
3. 在“接口类型”中选择“Vlanif”，“接口名称”中的接口号设为3。
4. 单击“应用”，显示“修改Vlanif”界面。参数配置如下：
   * 寻址模式：配置自身IP
   * IP地址/掩码：130.1.1.1 255.255.255.0
5. 单击“应用”。

步骤五：对于USG系列，将接口加入安全区域，并配置域间包过滤，以保证网络基本通信正常，具体步骤略。对于USG BSR/HSR系列，不需要将接口加入安全区域以及配置包过滤。

步骤六：在VLAN2中的主机上配置缺省网关为VLANIF2接口的IP地址120.1.1.1/24，在VLAN3中的主机上配置缺省网关为VLANIF3接口的IP地址130.1.1.1/24。

### 验证结果

1. 配置完成后，VLAN2中的主机能够ping通VLAN3中的主机。

## 防火墙E1实验

### 实验目的

两台安装CE1接口卡的设备直接相连，USG\_A接口地址为10.0.0.1/24,USG\_B接口地址为10.0.0.2/24,互相可以实现三层通信。

### 组网设备

2台USG防火墙,两条E1线缆。

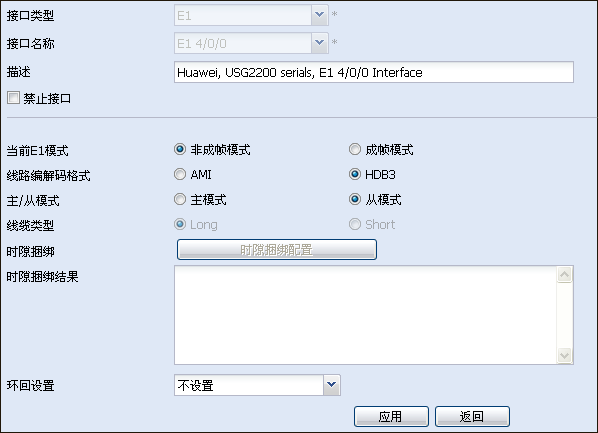
### 实验拓扑图



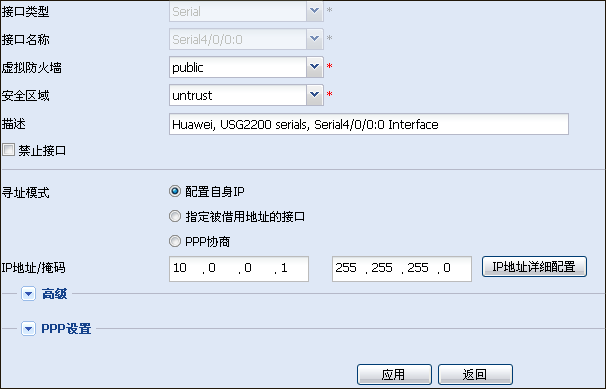
### 配置步骤

USG\_A配置步骤：

1. 在“菜单”导航树中选择“系统 > 网络”。
2. 选择“接口”页签。
3. 在“三层接口列表”界面中，单击***E1***接口对应的change1。
4. 在“修改***E1***”界面中，配置***E1***接口的各项参数，本实验采用非成帧模式。

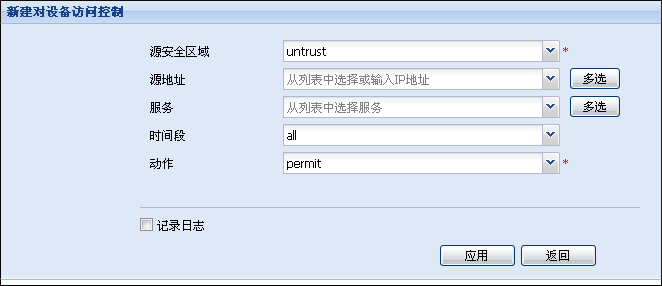


1. 在同步串口列表中，选择对应的串口，选择change1。

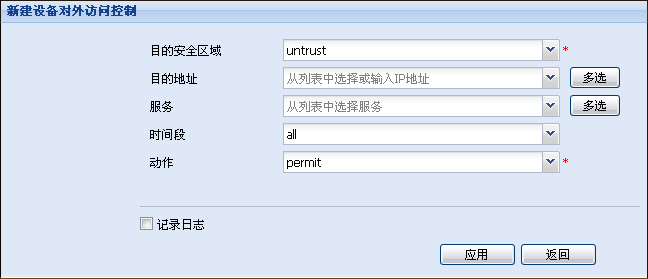


1. 配置域间包过滤，选择“防火墙>策略>本地策略”

1）配置untrust区域对设备访问



2）配置设备对untrust区域的访问



USG\_配置步骤省略，请参考USG\_A配置步骤。

### 验证结果

1. 配置完成后，从USG\_A能ping通USG\_B。

## 防火墙SA实验

### 实验目的

两台安装SA接口卡的设备直接相连，USG\_A接口地址为10.0.0.1/24,USG\_B接口地址为10.0.0.2/24,互相可以实现三层通信。

### 组网设备

2台USG防火墙,两条SA线缆。

### 实验拓扑图



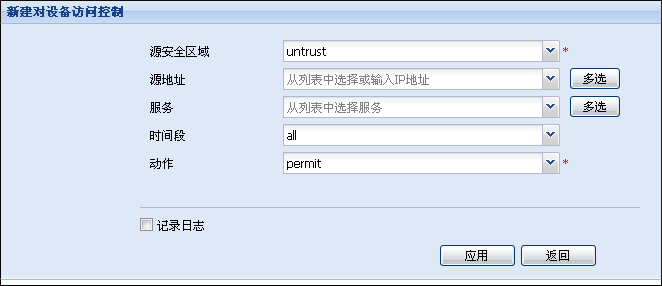
### 配置步骤

* USG\_A配置步骤：
  1. 在“菜单”导航树中选择“系统 > 网络”。
  2. 选择“接口”页签。
  3. 在“三层接口列表”界面中，单击Serial3/0/0对应的change1。
  4. 在“修改Serial”界面中，配置Serial接口的各项参数，

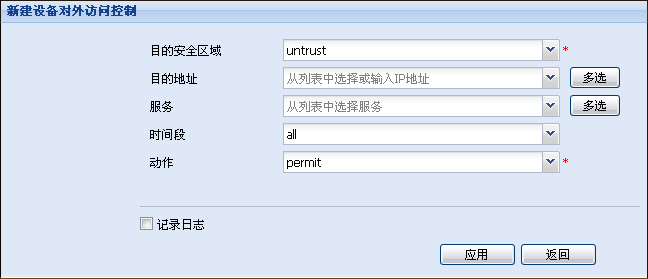


* 1. 配置域间包过滤，选择“防火墙>策略>本地策略”

1）配置untrust区域对设备访问



2）配置设备对untrust区域的访问



USG\_配置步骤省略，请参考USG\_A配置步骤。

### 验证结果

配置完成后，从USG\_A能ping通USG\_B。

## 防火墙ADSL实验

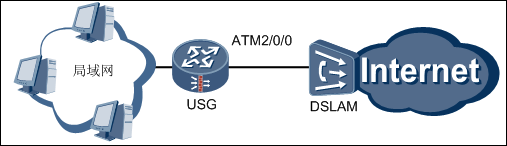
### 实验目的

运营商分配给PPPoE拨号的用户名和密码时请选择通过PPPoE或者ADSL上网。通过配置可以实现内网用户通过PPPoE拨号方式上网

### 组网设备

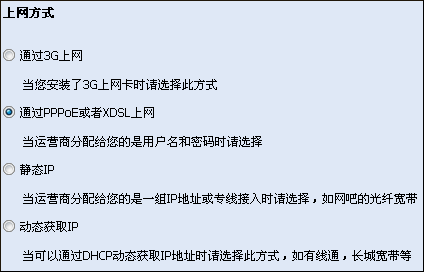
主机一台，USG2110-X防火墙1台，model一台

### 实验拓扑图



### 配置步骤

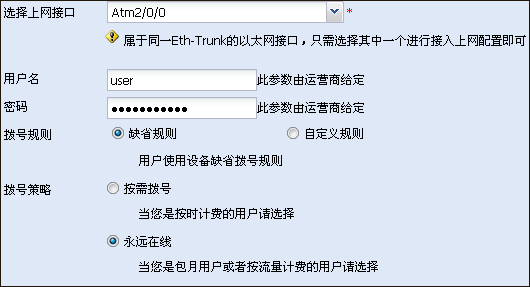
1. 在“菜单”导航树中选择“快速接入向导 > 接入互联网”。
2. 在“上网方式选择”界面中，选中“通过PPPoE或者XDSL上网”前的单选框，选择上网方式为PPPoE或者XDSL上网，如下图所示。



3. 单击“下一步”。

4.在“配置上网参数”界面中，配置通过PPPoE或者XDSL上网的各项参数，如[图](mk:@MSITStore:C:\Documents%20and%20Settings\huawei\桌面\CSA%20LAB\merge.chm::/web/sec_vsp_web_guide_0003.html#sec_vsp_web_guide_0003__fig4)所示。

***Notes：具体用户名和密码需要咨询当地运营商。本举例中用户名为user，密码为Password123。***



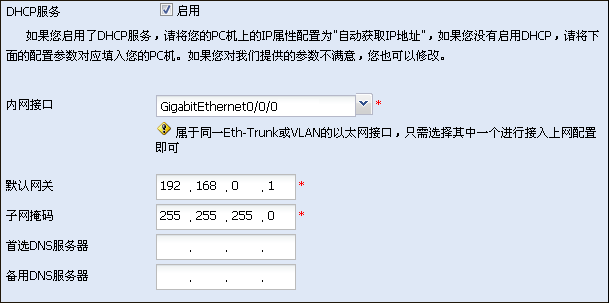
拨号规则用来实现对拨号接口的报文发送控制。

* 使用“缺省规则”时，允许拨号接口发送IP报文。
* 用户可以通过“自定义规则”控制拨号接口的报文发送。自定义规则的配置请参见配置拨号规则。

5. 单击“下一步”

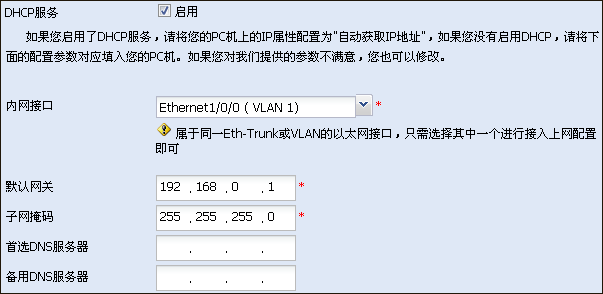
6. 在“配置局域网”界面中，配置局域网的各项参数。根据连接局域网的接口类型不同，以下两种局域网配置选择其一即可。

* 当USG连接局域网的接口为三层接口时，局域网配置如下图所示



***Notes：设备已配置默认管理IP地址，IP地址为192.168.0.1/24。其中USG2110-X/2100和USG2100BSR/HSR设备配置在Vlanif1接口上，USG2200/5100、USG2200BSR/HSR和USG5100BSR/HSR设备配置在GE0/0/0接口上。***

* 当USG连接局域网的接口为二层接口时，局域网配置如下图所示



***Notes：***

* ***缺省情况下，USG的所有二层接口都在VLAN1中。选择VLAN中的一个接口作为“内网接口”并配置局域网参数，相当于对该VLAN所对应的VLANIF接口进行了配置。***
* ***设备已配置默认管理IP地址，IP地址为192.168.0.1/24。其中USG2110-X/2100和USG2100BSR/HSR设备配置在Vlanif1接口上，USG2200/5100、USG2200BSR/HSR和USG5100BSR/HSR设备配置在GE0/0/0接口上。***

7.单击“下一步”。

8.在“下发配置”界面中，可以查看配置的参数。

9.单击“应用”，下发配置。

10.可选：在“下发配置”界面中，单击“检测”，可以检测网络的连通性。

11.单击“完成”，完成通过PPPoE或者XDSL上网的配置。

12.可选：如果您需要以WLAN（无线局域网）方式接入USG，在弹出的对话框中选择“是”，显示WLAN配置界面。如果不需要以WLAN（无线局域网）方式接入USG，选择“否”。

### 验证结果

防火墙通过model拨号接入到internet，主机可以通过USG防火墙接入到internet。

## 防火墙WLAN实验

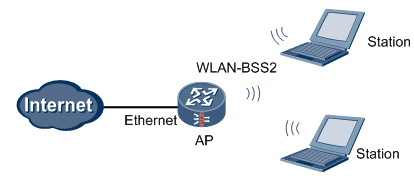
### 实验目的

新建无线服务后，无线用户可以搜索到无线服务的网络名称（SSID）并连接到无线局域网。

### 组网设备

带有无线网卡的主机一台，USG2110-X防火墙1台

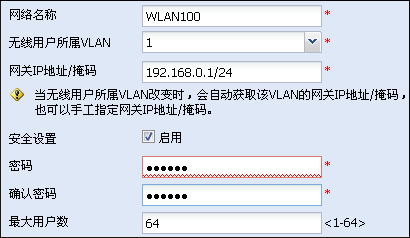
### 实验拓扑图



### 配置步骤

步骤一：新建无线服务

1. 在“菜单”导航树中选择“接入服务 > 无线局域网”。
2. 选择“无线局域网”页签。
3. 在“无线服务列表”工具栏中单击。
4. 在“新建无线服务”界面中，新建WLAN100，如下图所示。



步骤二：配置网络参数

1. 在“菜单”导航树中选择“接入服务 > 无线局域网”。
2. 选择“无线局域网”页签。
3. 在“无线服务列表”界面中，单击网络名称“WLAN100”。
4. 选择“WLAN100网络参数”页签。
5. 配置WLAN100网络参数，如下图所示。



步骤三：配置MAC地址限制

1. 在“菜单”导航树中选择“接入服务 > 无线局域网”。
2. 选择“无线局域网”页签。
3. 在“无线服务列表”界面中，单击网络名称“WLAN100”。
4. 选择“MAC地址限制”页签。
5. 在“MAC地址列表”工具栏中，单击。
6. 在“新建MAC地址过滤”界面中，配置MAC地址限制，如下图所示。



步骤四：全局配置WLAN

1. 在“菜单”导航树中选择“接入服务 > 无线局域网”。
2. 选择“全局参数配置”页签。
3. 在“配置全局参数”界面中，取消勾选“启用”前的复选框。
4. 单击“应用”，关闭射频开关。
5. 在“配置全局参数”界面中，全局配置WLAN的参数。
6. 选择“启用”前的复选框。
7. 单击“应用”，开启射频开关，完成配置。

### 验证结果

1. 使用带有无线网卡的主机搜索SSID为WLAN100的无线信号，并输入正确的验证密钥，接入网路，使用无线网路。

## 防火墙3G实验

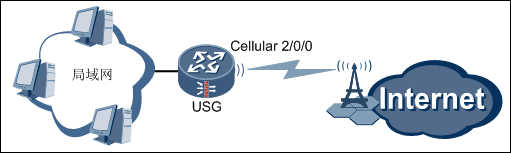
### 实验目的

在USG上安装了3G接口卡时，可以通过配置使内网用户通过3G方式连接到Internet。

### 组网设备

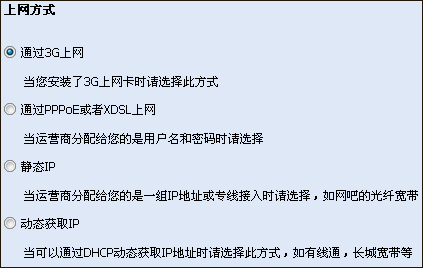
USG2110-X设备一台，USB无线网卡一张，主机一台

### 实验拓扑图



### 配置步骤

1. 在“菜单”导航树中选择“快速接入向导 > 接入互联网”。
2. 在“上网方式选择”界面中，选中“通过3G上网”前的单选框，选择上网方式为3G，如图所示。



3.单击“下一步”。

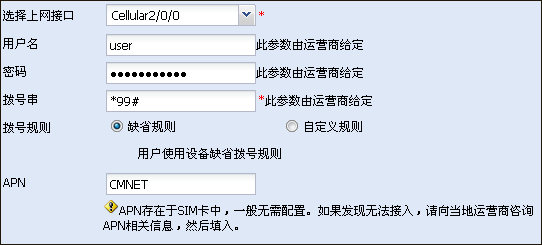
4.在“配置上网参数”界面中，配置通过3G上网的各项参数，如[图](mk:@MSITStore:C:\Documents%20and%20Settings\huawei\桌面\CSA%20LAB\merge.chm::/web/sec_vsp_web_guide_0002.html#sec_vsp_web_guide_0002__fig4)所示。

***Notes：***

***具体用户名和密码需要咨询当地运营商。本举例中用户名为user，密码为Password123。***

***具体拨号串取值需要咨询当地运营商。对于中国移动（TD-SCDMA标准）和中国联通（WCDMA标准）的3G数据卡，对端号码为\*99#；对于中国电信的3G数据卡，对端号码为#777。***

***不同运营商的APN不同，APN的获取需要咨询当地运营商。常用的如中国移动（TD-SCDMA标准）的APN为CMNET，中国联通（WCDMA标准）的APN为UNINET。***

******

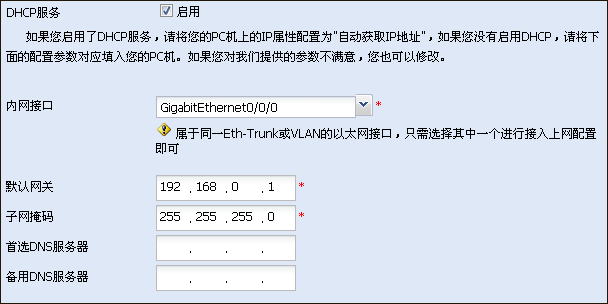
拨号规则用来实现对拨号接口的报文发送控制。

* 使用“缺省规则”时，允许拨号接口发送IP报文。
* 用户可以通过“自定义规则”控制拨号接口的报文发送。自定义规则的配置请参见配置拨号规则。

5.单击“下一步”。

6.在“配置局域网”界面中，配置局域网的各项参数。根据连接局域网的接口类型不同，以下两种局域网配置选择其一即可。

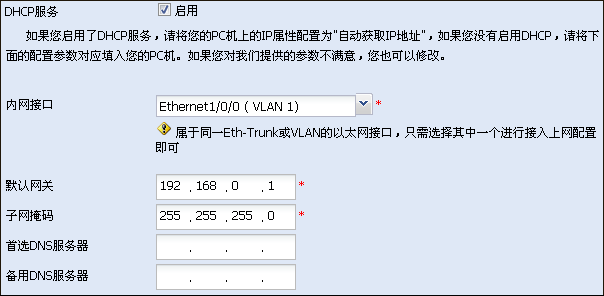
* 当USG连接局域网的接口为三层接口时，局域网配置如图4所示。



***Notes：***

***设备已配置默认管理IP地址，IP地址为192.168.0.1/24。其中USG2110-X/2100和USG2100BSR/HSR设备配置在Vlanif1接口上，USG2200/5100、USG2200BSR/HSR和USG5100BSR/HSR设备配置在GE0/0/0接口上。***

* 当USG连接局域网的接口为二层接口时，局域网配置如下图所示



***Notes：***

* ***缺省情况下，USG的所有二层接口都在VLAN1中。选择VLAN中的一个接口作为“内网接口”并配置局域网参数，相当于对该VLAN所对应的VLANIF接口进行了配置。***
* ***设备已配置默认管理IP地址，IP地址为192.168.0.1/24。其中USG2110-X/2100和USG2100BSR/HSR设备配置在Vlanif1接口上，USG2200/5100、USG2200BSR/HSR和USG5100BSR/HSR设备配置在GE0/0/0接口上。***

7.单击“下一步”。

8.在“下发配置”界面中，可以查看配置的参数。

9.单击“应用”，下发配置。

10.可选：在“下发配置”界面中，单击“检测”，可以检测网络的连通性。

11.单击“完成”，完成通过3G上网的配置。

12.可选：如果您需要以WLAN（无线局域网）方式接入USG，在弹出的对话框中选择“是”，显示WLAN配置界面。如果不需要以WLAN（无线局域网）方式接入USG，选择“否”。

### 验证结果

防火墙已经通过3G无线网卡拨入到internet，主机可以通过防火墙接入到internet。

# VPN实验

## L2TP VPN实验

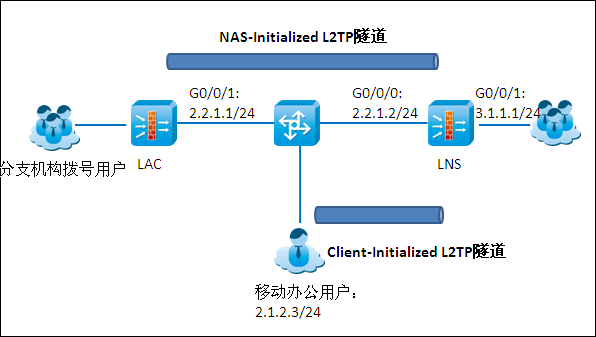
### 实验目的

* 某公司建有自己的VPN网络，在公司总部的公网出口处，放置了一台VPN网关，即USG防火墙。
* 要求公司分支机构人员能够通过L2TP隧道与公司内部其他用户进行通信，并且移动办公人员也可以通过L2TP隧道访问公司内部。

### 组网设备

主机、一台USG作为LAC、一台USG作为LNS、VPN Client。Internet可以采用路由器或者防火墙模拟。

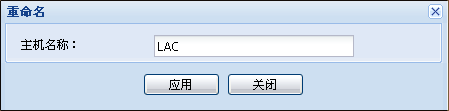
### 实验拓扑图



### 配置步骤

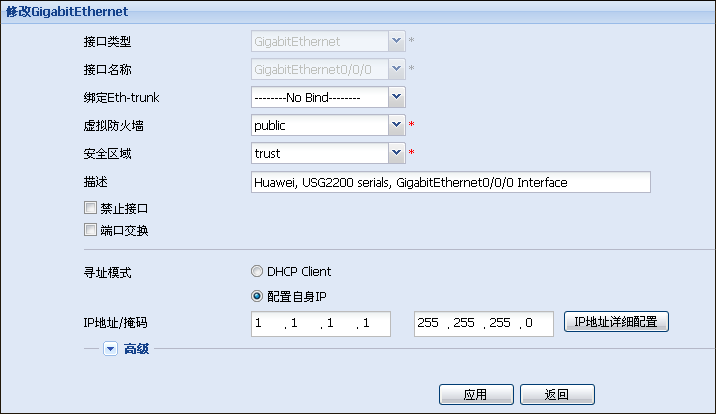
步骤一 完成LAC侧的配置

1. 登陆配置界面
2. 配置本端设备的名称。选择“系统->状态->系统信息”,然后选择“主机名称->更改”，输入“LAC”，选择“应用”。

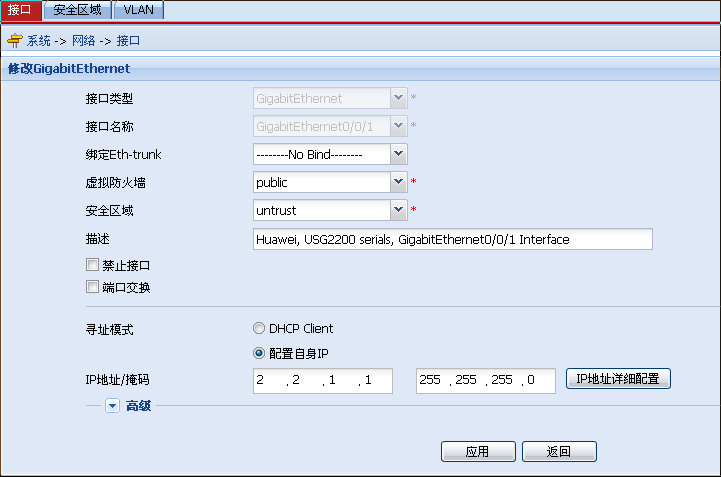


1. 配置GigabitEthernet 0/0/0的IP地址，并将接口加入到trust区域。选择“网络->接口”，选择GigabitEthernet 0/0/0口然后选择，输入新的IP地址后选择“应用”。

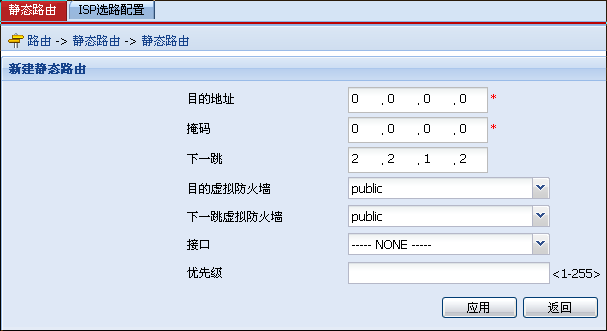
注意：修改IP地址后，使用新的IP地址重新登陆。



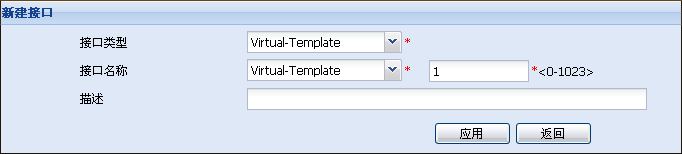
1. 配置GigabitEthernet 0/0/1的IP地址，并将接口加入到untrust区域。配置GigabitEthernet 0/0/1的IP地址。选择“网络->接口”，选择GigabitEthernet 0/0/1口然后选择，输入IP地址，安全区域选择untrust，然后选择“应用”。



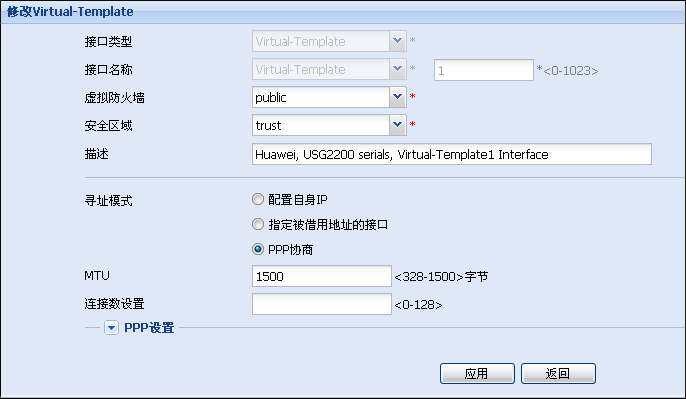
1. 配置缺省路由，2.2.1.2为LAC的下一跳设备的IP地址。选择“路由->静态路由”，选择，输入缺省路由。



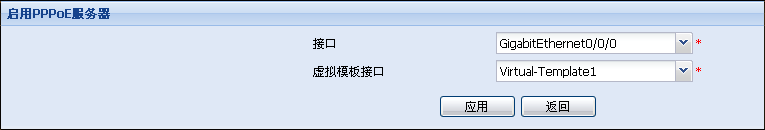
1. 创建虚拟接口模板。选择“系统->网络->接口”，选择，选择接口类型为Virtual-Template，选择“应用”。



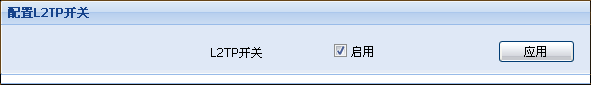
1. 将Virtual-Template1加入trust区域，选择“应用”，寻址模式为“PPP协商”。



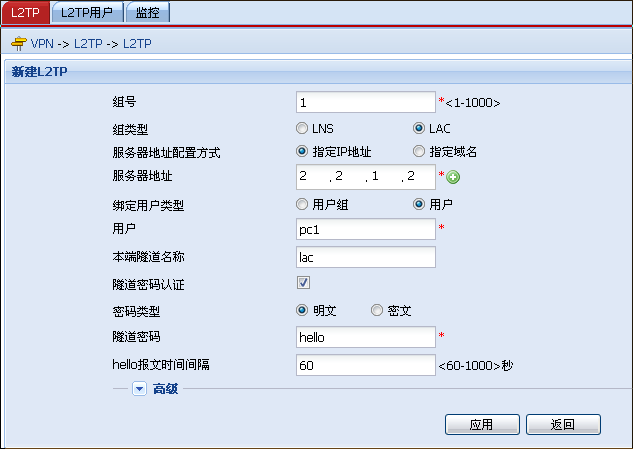
1. 配置接口绑定虚拟接口模板。选择“接入服务->PPPOE->PPPOE服务器基本配置”，将GigabitEthernet 0/0/0和Virtual-Template1绑定。



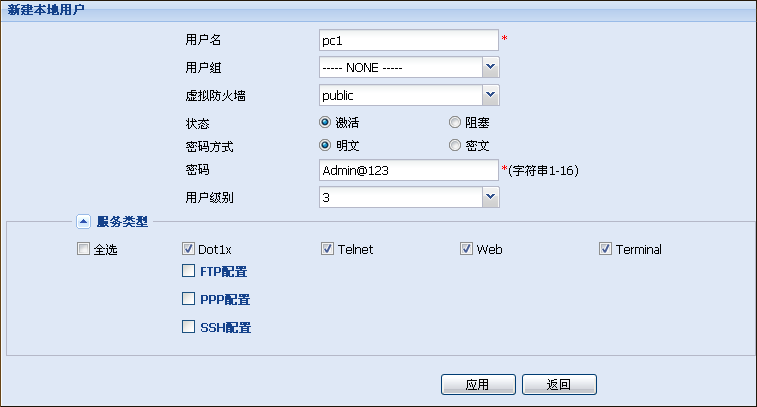
1. 启用l2tp功能。选择“VPN->L2TP->配置L2TP开关”。选择“启用”－“应用”。



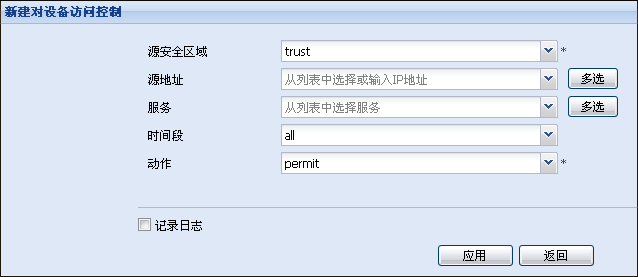
1. 创建L2TP组。选择“VPN->L2TP->L2TP列表”，选择。输入组号，组类型选择“LAC”。



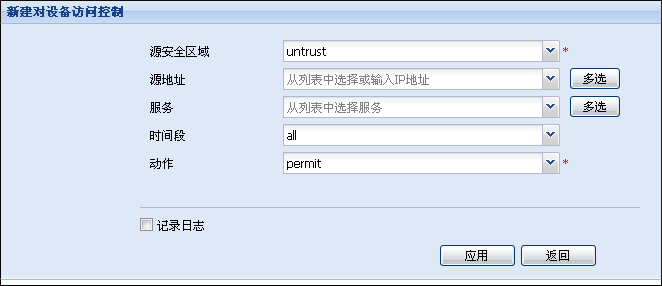
1. 创建L2TP用户。选择“用户->本地->本地用户列表”，选择。



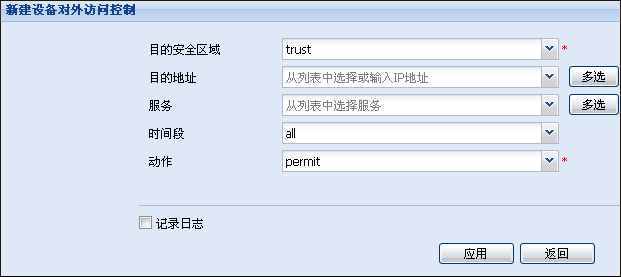
1. 配置域间缺省包过滤规则。由于LAC需要与LNS设备进行PPP协商，也需要传输PC1的连接请求，故配置上述两个域间的缺省包过滤规则。选择“防火墙”－“策略”－“本地策略”。
2. 配置trust区域对设备访问



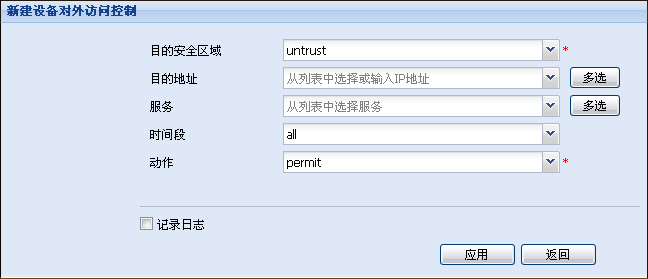
1. 配置untrust区域对设备访问



1. 配置Local 对trust区域的访问

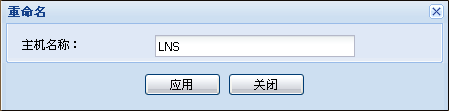


1. 配置Local 对untrust区域的访问



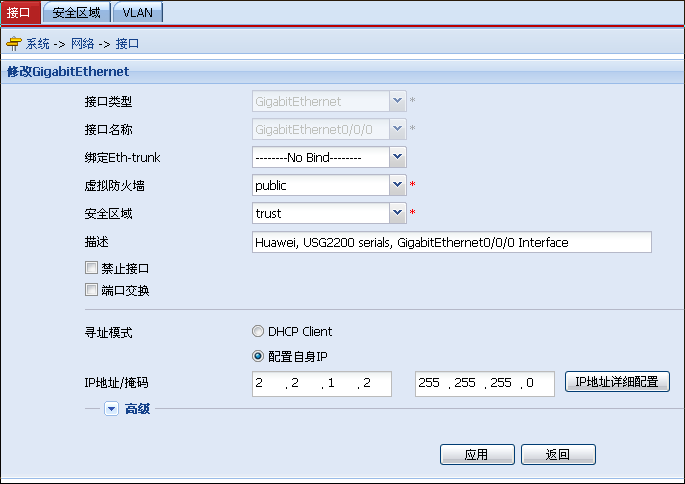
步骤二 完成LNS侧的配置

1. 登陆配置界面
2. 配置本端设备的名称。选择“系统>状态>系统信息>主机名称>更改”，输入“LNS”，选择“应用”。

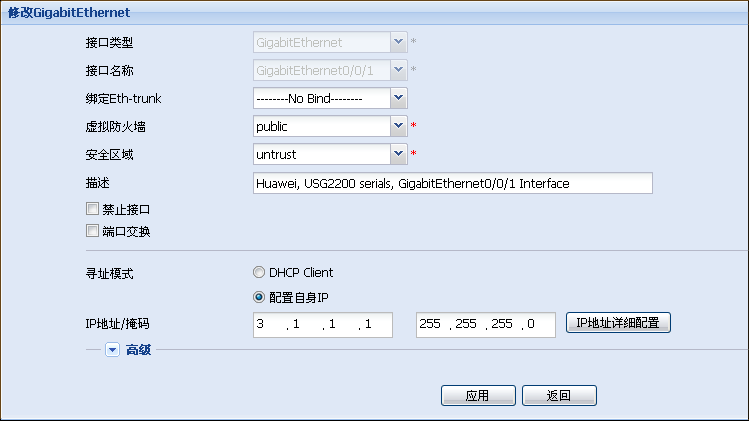


1. 配置GigabitEthernet 0/0/0的IP地址，并将接口加入到trust区域。选择“网络”－“接口”，选择GigabitEthernet 0/0/0口然后选择，输入新的IP地址后选择“应用”。

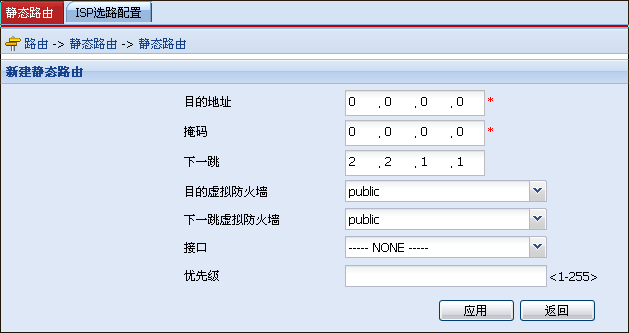
注意：修改IP地址后，使用新的IP地址重新登陆。



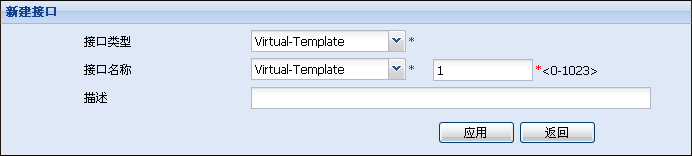
1. 配置GigabitEthernet 0/0/1的IP地址，并将接口加入到untrust区域。配置GigabitEthernet 0/0/1的IP地址。选择“网络”－“接口”，选择GigabitEthernet 0/0/1口然后选择，输入IP地址，安全区域选择untrust，然后选择“应用”。



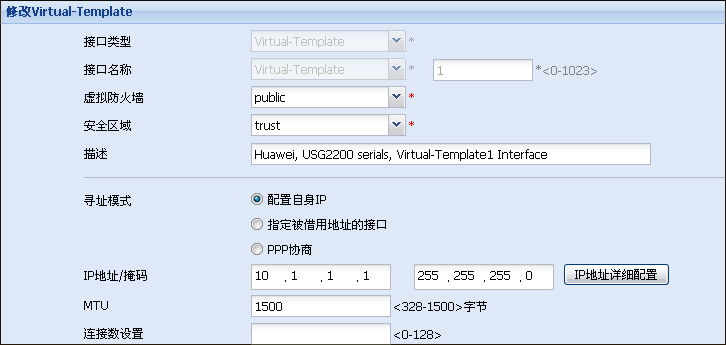
1. 配置缺省路由。2.2.1.1为LNS的下一跳设备的IP地址。选择“路由”－“静态路由”，选择，输入缺省路由。



1. 创建虚拟接口模板。选择“系统>网络>接口”，选择，选择接口类型为Virtual-Template，选择“应用”。



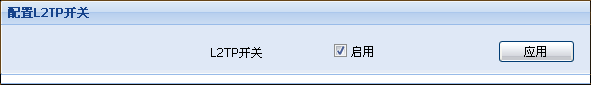
1. 配置虚拟接口模板的IP地址。配置虚拟接口模板的IP地址为LNS侧的必配项。



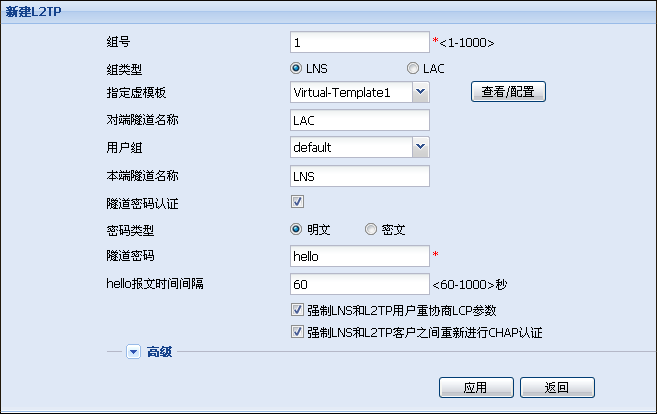
1. 配置PPP认证方式。配置为对端接口分配IP地址池中的地址。此处引用的地址池号需要与AAA视图下的相对应。否则LNS无法为PC1分配地址。



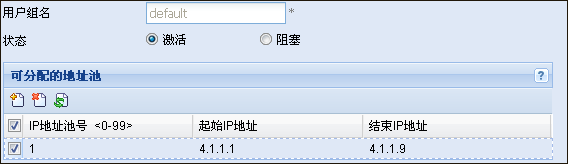
1. 启用l2tp功能。选择“VPN>L2TP>配置L2TP开关”。选择“启用”－“应用”。



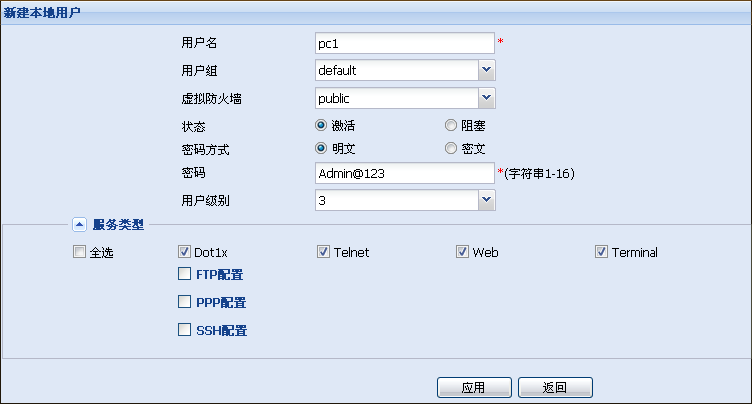
1. 创建L2TP组。选择“VPN”－“L2TP”－“L2TP列表”，选择。输入组号，组类型选择“LNS”。



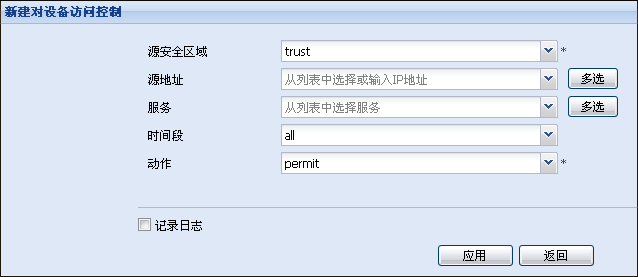
1. 创建L2TP用户组及地址池。本实验采用默认的用户组“default”，选择“VPN->L2TP->L2TP用户”，在“default”组后面选择，配置地址池1。



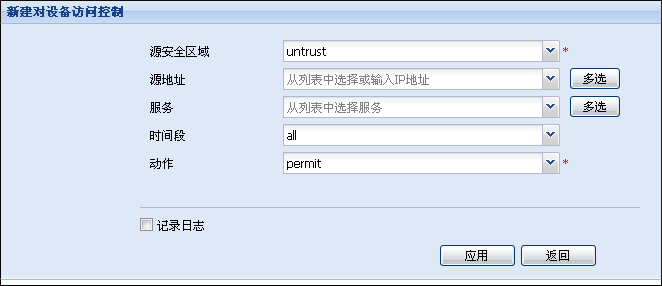
1. 创建本地用户名和密码。“选择用户>本地用户”，选择，选择“用户”。



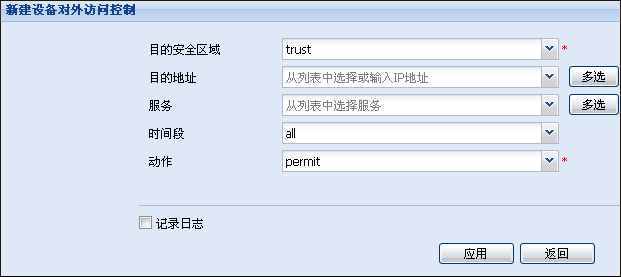
1. 配置域间缺省包过滤规则。由于LNS需要给PC1分配IP地址，此时不能配置确切的ACL及域间规则。同时，需要打开local和untrust域间的缺省过滤规则。选择“防火墙”－“策略”－“本地策略”。
2. 配置trust区域对设备访问



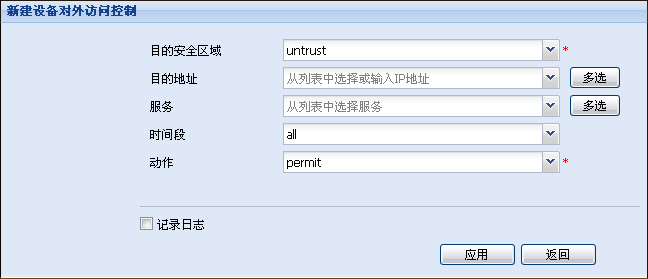
1. 配置untrust区域对设备访问



1. 配置Local区域对trust区域的访问



1. 配置Local区域对untrust区域的访问



步骤三 完成移动办公用户PC的配置。

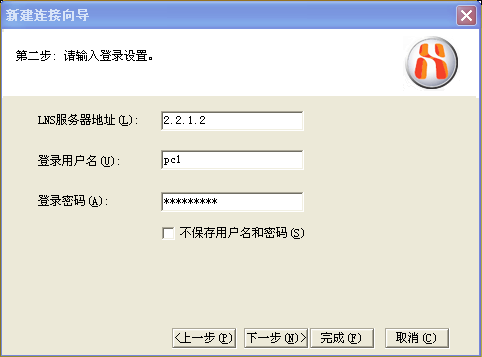
1. 配置PC的IP地址、掩码以及网关，使PC能够PING通LNS出口地址2.2.1.2。
2. 在PC上安装Secoway VPN Client软件。（安装过程略）
3. 打开VPN Client软件，如下图所示：



1. 点击“新建”后选择“通过输入参数创建连接”，然后点击“下一步”，如下图所示：



1. 输入登录设置，包括LNS的IP地址、登录用户名以及登录密码，输入后点击“下一步”，如下图所示：



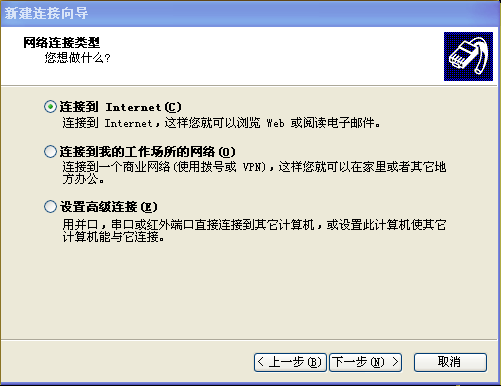
1. 输入其他L2TP的设置，先随意给本端隧道名称命名，本例中使用“client”，然后根据配置选择认证模式。最后根据需要选择是否启用隧道认证，本例中LNS启用了隧道认证。设置后可点击“完成”结束设置，也可点击下一步设置连接名称。设置如下图所示：



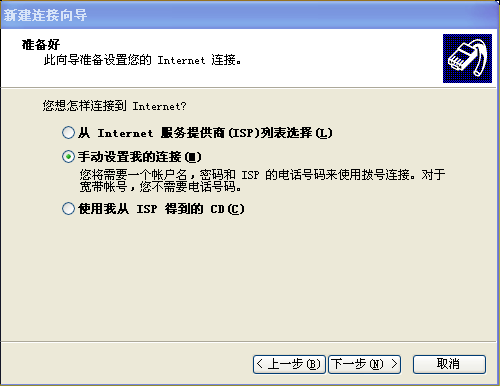
1. 设置完成后可以双机连接，进行L2TP VPN的建立。

步骤四 完成分支机构拨号用户PC设置

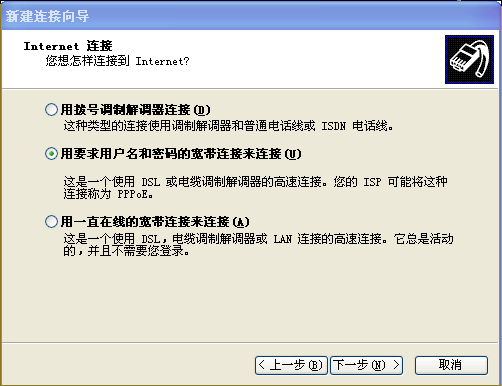
1. 以XP系统为例，选择“开始”－“控制面板”－“网络连接”－“创建一个新的连接”，选择“连接到Internet”。



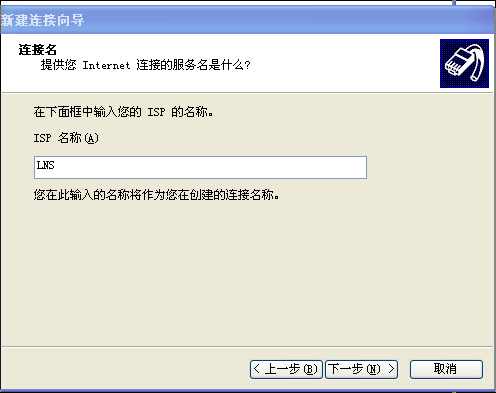
1. 选择“手动设置我的连接”。



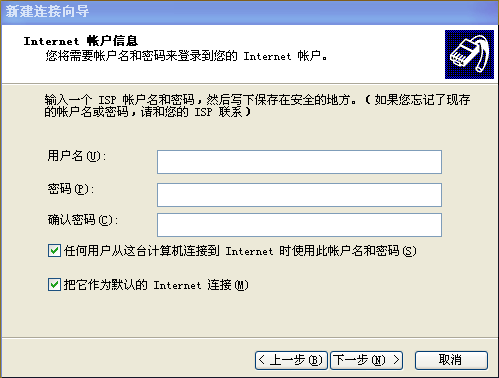
1. 选择“用要求用户名密码的宽带连接来连接”。



1. 输入ISP名称。



1. 选择下一步，最后输入用户名pc1,密码Admin@123



### 结果检查

验证操作：

1. 分支机构拨号用户可以拨号成功并获取IP地址，能访问企业内网。
2. 移动办公用户可以拨号成功并获取IP地址，能访问企业内网。

## GRE VPN实验

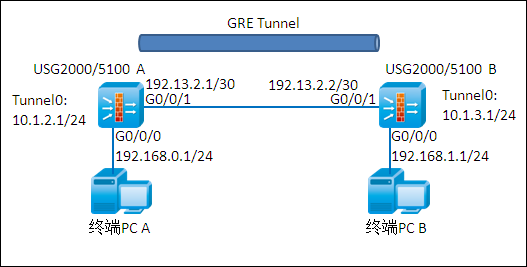
### 实验目的

运行IP协议的两个子网网络1和网络2，通过在防火墙USG A和防火墙USG B之间使用三层隧道协议GRE实现互联。

### 组网设备

主机、USG防火墙

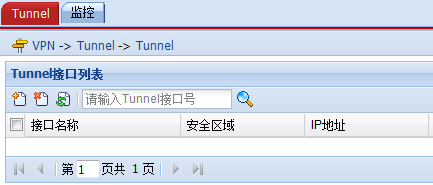
### 实验拓扑图



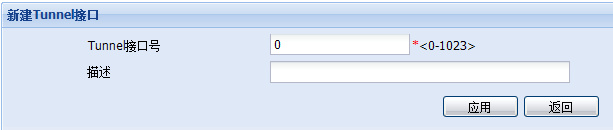
### 配置步骤

步骤一：配置防火墙USG A。

1. 配置G0/0/0、G0/0/1接口的IP地址和所属安全区配置，请参见《2.2 防火墙区域间连接》；
   * G0/0/0: 所属安全区域为Trust，IP地址为192.168.0.1/24；
   * G0/0/1: 所属安全区域为Untrust，IP地址为192.13.2.1/30；
2. 在菜单导航树中选择“VPN > Tunnel”，单击“Tunnel”页签；
3. “Tunnel接口列表”界面中，单击 ；



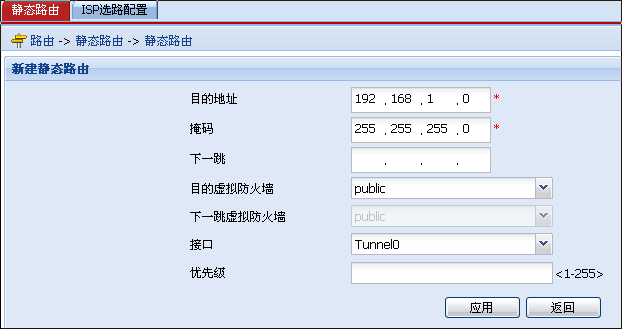
1. 在“新建Tunnel接口”界面中，新建Tunnel接口0，单击“应用”。



1. 在“新建Tunnel接口”界面中，配置Tunnel接口的各项参数，单击“应用”。



1. 在在菜单导航树中选择“路由 > 静态路由”。单击，配置从USG\_A经过Tunnel 0接口到网络B的静态路由。



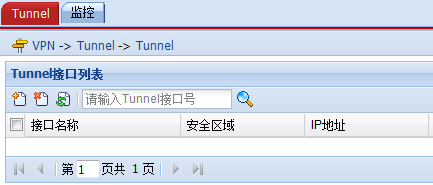
1. 在菜单导航树中选择“策略>防火墙策略>转发策略”。单击单击，配置trust和untrus的域间规则。



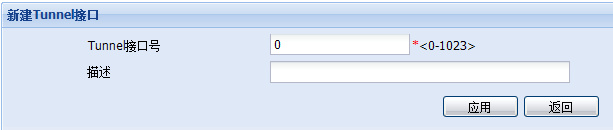
1. 在菜单导航树中选择“策略>防火墙策略>本地策略”。分别在“对设备访问控制列表”和“设备对外访问控制列表”单击，配置Local和untrust的域间规则。

步骤二：配置防火墙USG B。

1. 配置G0/0/0、G0/0/1接口的IP地址和所属安全区配置，请参见《2.2 防火墙区域间连接》；
   * G0/0/0: 所属安全区域为Trust，IP地址为192.168.1.1/24；
   * G0/0/1: 所属安全区域为Untrust，IP地址为192.13.2.2/30；
2. 在菜单导航树中选择“VPN > Tunnel”，单击“Tunnel”页签；
3. “Tunnel接口列表”界面中，单击 ；



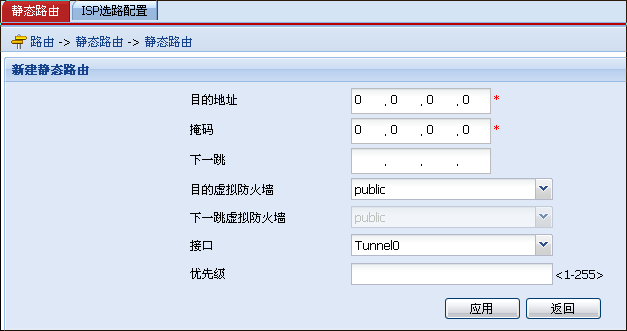
1. 在“新建Tunnel接口”界面中，新建Tunnel接口0，单击“应用”。



1. 在“新建Tunnel接口”界面中，配置Tunnel接口的各项参数，单击“应用”。



1. 在在菜单导航树中选择“路由 > 静态路由”。单击，配置从USG\_B经过Tunnel 0接口到网络A的静态路由。



1. 在菜单导航树中选择“策略>防火墙策略>转发策略”。单击单击，配置trust和untrus的域间规则。



1. 在菜单导航树中选择“策略>防火墙策略>本地策略”。分别在“对设备访问控制列表”和“设备对外访问控制列表”单击，配置Local和untrust的域间规则。

### 结果检查

1. 网络A内的PC可以PING通网络B内的PC

## IPSEC VPN实验

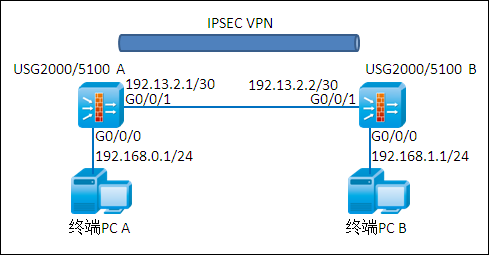
### 实验目的

* 终端PCA与终端PCB之间进行安全通信，在USG A与USG B之间使用IKE自动协商建立安全通道。
* IKE验证方式为预共享密钥。

### 组网设备

主机、USG系列防火墙

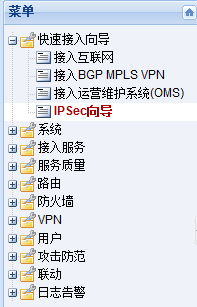
### 实验拓扑图



### 配置步骤

步骤一：配置USG A。

1. 配置G0/0/0、G0/0/1接口的IP地址和所属安全区配置，请参见《2.2 防火墙区域间连接》；
   * G0/0/0: 所属安全区域为Trust，IP地址为192.168.0.1/24；
   * G0/0/1: 所属安全区域为Untrust，IP地址为192.13.2.1/30；
2. 在USG\_A上利用IPSec向导完成配置。
   * 1. 在“菜单”导航树中选择“快速接入向导 > IPSec向导”。



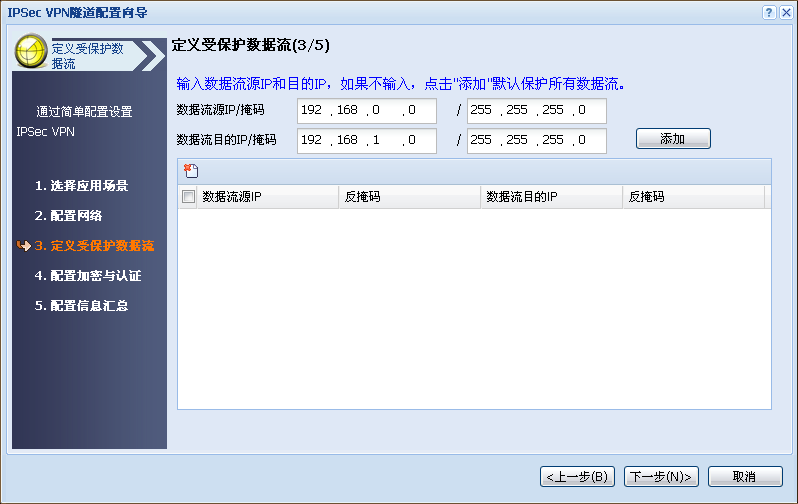
* + 1. 在“选择应用场景”界面中，选中“网关到网关”前的单选框，然后单击“下一步”。



* + 1. 在“配置网络”界面中，选择启用IPSec的接口，如下图所示。



* + 1. 在“定义受保护数据流”界面中，配置数据流源IP和目的IP



* + 1. 在“配置加密与认证”界面中，配置隧道加密与认证的参数（包括IKE和IPSec），



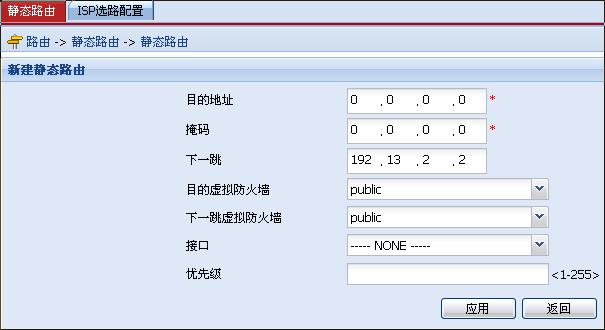
* + 1. 单击“下一步”，会看到配置信息汇总，确认一下配置有没有问题。



* + 1. 单击“应用”，设备会执行前几步的配置，请耐心等待。
    2. 在菜单导航树中选择“策略>防火墙策略>转发策略”。单击单击，配置trust和untrus的域间规则。

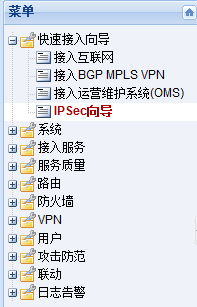


* + 1. 在菜单导航树中选择“策略>防火墙策略>本地策略”。分别在“对设备访问控制列表”和“设备对外访问控制列表”单击，配置Local和untrust的域间规则。
    2. 在在菜单导航树中选择“路由 > 静态路由”。单击，添加缺省路由。



步骤二：配置USG B。

1. 配置G0/0/0、G0/0/1接口的IP地址和所属安全区配置，请参见《2.2 防火墙区域间连接》；
   * G0/0/0: 所属安全区域为Trust，IP地址为192.168.1.1/24；
   * G0/0/1: 所属安全区域为Untrust，IP地址为192.13.2.2/30；
2. 在USG\_A上利用IPSec向导完成配置。
   * 1. 在“菜单”导航树中选择“快速接入向导 > IPSec向导”。



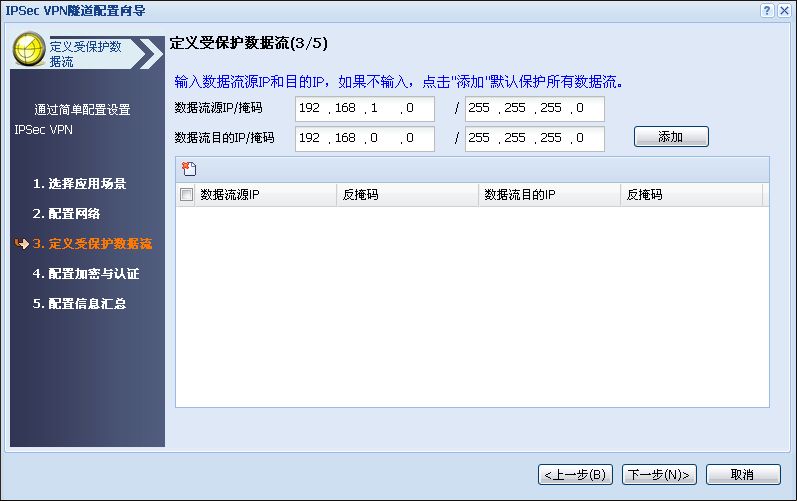
* + 1. 在“选择应用场景”界面中，选中“网关到网关”前的单选框，然后单击“下一步”。



* + 1. 在“配置网络”界面中，选择启用IPSec的接口，如下图所示。



* + 1. 在“定义受保护数据流”界面中，配置数据流源IP和目的IP



* + 1. 在“配置加密与认证”界面中，配置隧道加密与认证的参数（包括IKE和IPSec），



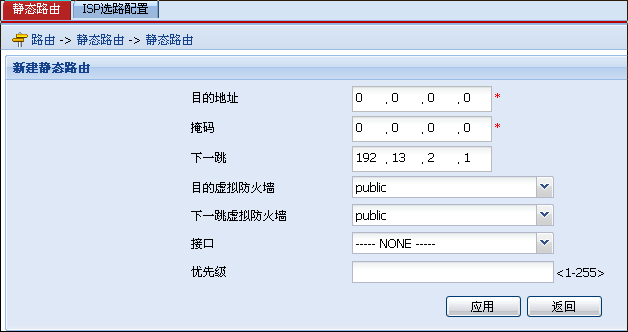
* + 1. 单击“下一步”，会看到配置信息汇总，确认一下配置有没有问题。



* + 1. 单击“应用”，设备会执行前几步的配置，请耐心等待。
    2. 在菜单导航树中选择“策略>防火墙策略>转发策略”。单击单击，配置trust和untrus的域间规则。



* + 1. 在菜单导航树中选择“策略>防火墙策略>本地策略”。分别在“对设备访问控制列表”和“设备对外访问控制列表”单击，配置Local和untrust的域间规则。
    2. 在在菜单导航树中选择“路由 > 静态路由”。单击，添加缺省路由。



### 结果检查

* 完整配置：
* 验证操作：
* 终端PCA向终端PCB进行PING操作，第一个ICMP报文将被丢弃，同时IPSec隧道建立完成，随后终端PCA与终端PCB可以进行正常通信

## SSL VPN实验

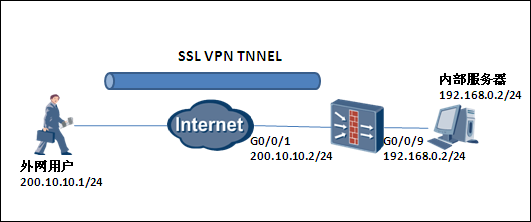
### 实验目的

* 在USG创建一个名为test的虚拟网关，外部用户可通过此虚拟网关访问企业内网资源。虚拟网关的IP地址为202.10.10.2/24。
* 企业内网资源所在的网段为192.168.0.0/24。
* 企业内网的DNS地址为192.168.0.100/24，域名为internal.com。
* 虚拟网关采用VPNDB的认证授权方式。用户名/密码为user/123abcABC。
* 用户从虚拟网关获取的IP地址范围是192.168.100.1～192.168.100.100，子网掩码为255.255.255.0。
* 网络扩展：外网用户通过USG构造的SSL VPN获得内网地址，可与内网设备通信。
* 文件共享：在内网服务器上共享一个文件夹logs，外网用户通过USG构造的SSL VPN进行访问。
* 端口转发：开启内网服务器上的telnet服务，外网用户通过USG构造的SSL VPN进行访问。
* WEB代理：内网服务器192.168.0.2上提供WWW，服务，外网用户可以通过<http://192.168.0.2>来访问。

### 组网设备

主机、防火墙

### 实验拓扑图

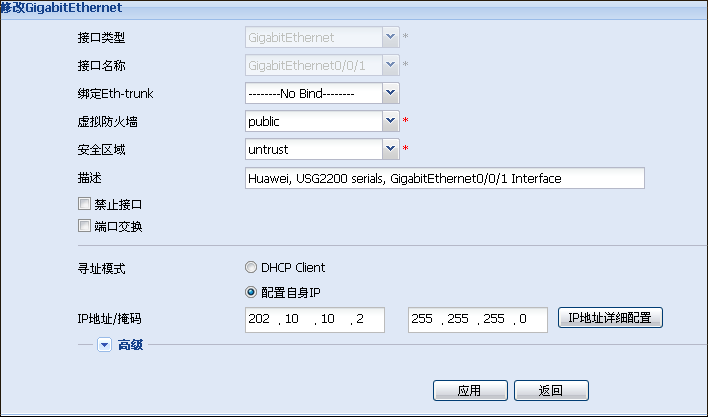


### 配置步骤

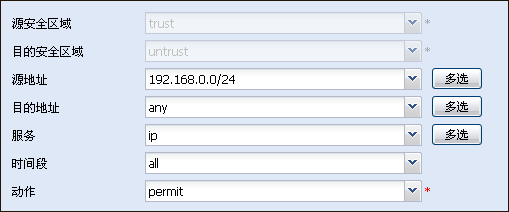
步骤一：将接口加入安全区域，并配置域间包过滤

对于USG BSR/HSR系列，不需要将接口加入安全区域以及配置包过滤。

1. 在菜单导航树中选择“系统>网络>接口”，选择GigabitEthernet0/0/1。GigabitEthernet0/0/0口使用默认IP设置。



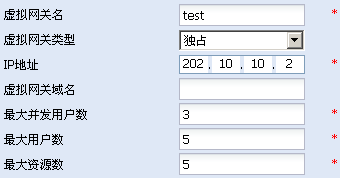
1. 在菜单导航树中选择“防火墙>策略>转发策略”，单击E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\add1.png。



1. 在菜单导航树中选择“防火墙>策略>本地策略>对设备访问控制列表”，配置外网用户能够访问防火墙。



步骤二：创建虚拟网关

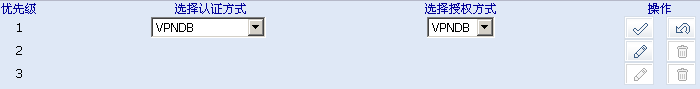
1. 在“菜单”导航树中选择“VPN > SSL VPN”。
2. 选择“虚拟网关管理”页签。
3. 在“虚拟网关管理”区域框中，单击E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\add1.png。
4. 配置虚拟网关基础信息，参数如下图所示。   
   
5. 单击“应用”。

步骤三：配置DNS服务器

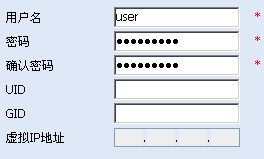
1. 选择“虚拟网关列表”页签。
2. 在“虚拟网关列表”导航树中选择“虚拟网关列表 > test > 网络配置”。
3. 单击“首选DNS服务器 ”和“DNS domain ”对应的E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\modify2.png，配置DNS服务器地址和域名，参数如下图所示。   
   
4. 单击“首选DNS服务器 ”和“DNS domain ”对应的E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\modify2.png，完成配置。

步骤四：配置认证授权方式为VPNDB

1. 在“菜单”导航树中选择“VPN > SSL VPN”。
2. 选择“虚拟网关列表”页签。
3. 在“虚拟网关列表”导航树中选择“虚拟网关列表 > test > 认证授权配置”。
4. 选择“认证授权方式”页签。
5. 单击优先级“1”对应的操作E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\modify2.png，选择认证授权方式。具体参数如下图所示。



1. 单击E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\confirm1.png，完成配置。
2. 配置VPNDB用户。
3. 在“菜单”导航树中选择“VPN > SSL VPN”。
4. 选择“虚拟网关列表”页签。
5. 在“虚拟网关列表”导航树中选择“虚拟网关列表 > test > VPNDB配置”。
6. 选择“用户管理”页签，单击E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\add1.png。
7. 在“添加用户”区域框中，配置VPNDB用户user，配置参数如下图所示。



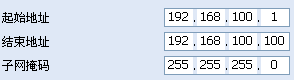
1. 单击“应用”。

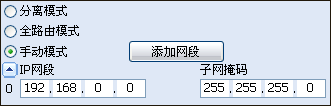
步骤五：配置静态路由

1. 在“菜单”导航树中选择“路由 > 静态路由”。
2. 选择“静态路由”页签。
3. 在“静态路由列表”区域框中，单击E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\add1.png。
4. 配置静态路由，具体参数如下。
5. 目的地址：0.0.0.0
6. 掩码：0.0.0.0
7. 下一跳：202.10.10.1
8. 单击“应用”。

步骤六：配置网络扩展

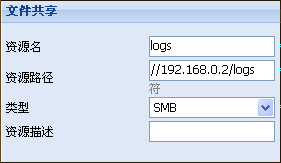
1. 在“菜单”导航树中选择“VPN > SSL VPN”。
2. 选择“虚拟网关列表”页签。
3. 在“虚拟网关列表”导航树中选择“虚拟网关列表 > test > 网络扩展”。
4. 选中“启用网络扩展功能”前的复选框，启用网络扩展功能。
5. 选中“保持连接 ”、“启用点对点通讯”前的复选框。
6. 在“客户端IP分配方式”区域框中，分配客户端使用IP地址，具体参数如下图所示。



1. 在“客户端路由方式”区域框中，选中“手动模式”前的单选按钮。
2. 单击“添加网段”，添加客户端可以通过虚拟网关访问的内网资源的网段，具体参数如下图所示。   
   
3. 在“用户虚拟IP处理方式 ”区域框中，选中“清除不在新地址范围内的用户虚拟IP ”前的单选按钮，清除虚拟网关内不在新地址段内的用户虚拟IP。
4. 单击“应用”。

步骤七：配置文件共享

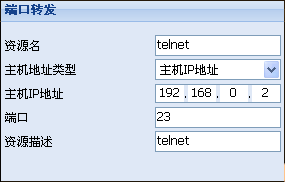
1. 在“菜单”导航树中选择“VPN > SSL VPN”。
2. 选择“虚拟网关列表”页签。
3. 在“虚拟网关列表”导航树中选择“虚拟网关列表 > test > 文件共享”。
4. 选中“启用文件共享功能 ”前的复选框。
5. 单击E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\add1.png，在“文件共享”区域框中，配置SMB类型的文件共享资源，具体参数如下图所示。



1. 单击“应用”。

步骤八：配置端口转发

1. 在“菜单”导航树中选择“VPN > SSL VPN”。
2. 选择“虚拟网关列表”页签。
3. 在“虚拟网关列表”导航树中选择“虚拟网关列表 > test > 端口转发”。
4. 选中“启用端口转发功能 ”前的复选框。
5. 选中“客户端自动启用”、“保持连接 ”前的复选框。
6. 单击E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\add1.png，配置端口转发资源FTP服务，具体参数如下图所示。



1. 单击“应用”。

步骤九：配置WEB代理

1. 在“菜单”导航树中选择“VPN > SSL VPN”。
2. 选择“虚拟网关列表”页签。
3. 在“虚拟网关列表”导航树中选择“虚拟网关列表 > test > Web代理”。
4. 在“Web代理”区域框中，选中“启用Web代理功能”前的复选框，开启Web代理功能。
5. 选中“启用Web-link功能”前的复选框，允许添加Web资源。
6. 在“Web代理资源管理”区域框中，单击E:\产品资料\USG2200\CHN\data\3118G2~1.CDP\outfiles\merge.files\web\images_common\add1.png，添加WWW服务器资源，配置参数如下图所示。  
   
7. 单击“应用

### 结果验证。

远端用户（非7.1.1.0/24网段）在IE浏览器中输入https://202.10.10.2，进入虚拟网关登录界面

1. 输入用户名user及相应密码，单击“登录”，登录虚拟网关。具体界面如下图所示。   
   
2. 在“网络扩展”区域框中，单击“启动”，启用网络扩展功能后，客户端可以获取192.168.100.1～192.168.100.100范围内的IP地址，访问企业内网资源，同时访问Internet不受限制。
3. 在“web链接”区域中，单击“WWW”，可以访问WWW服务。
4. 在“端口转发”区域框中，单击“启动”，启用端口转发后，外网用户可以通过命令telnet 192.168.0.2访问内网服务器的telnet服务器。
5. 在“文件共享”区域中，点击“logs”，输入用户名密码后能访问内网共享资源。

# TSM终端安全实验

## 安装TSM管理器+TSM控制器

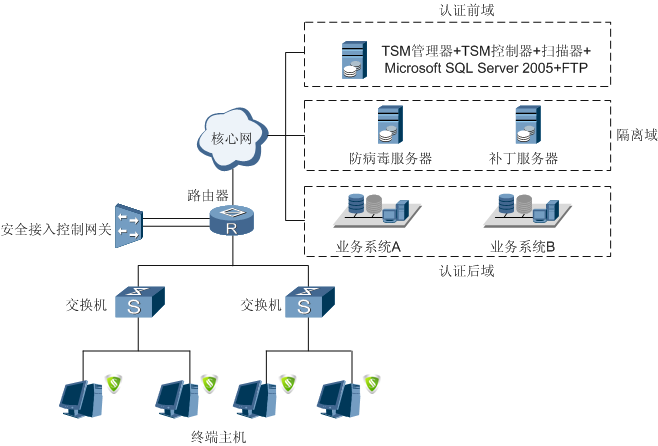
### 实验目的

完成TSM管理＋TSM控制器安装。

### 组网设备

服务器

### 实验拓扑图



### 配置步骤

步骤1、使用“administrator”账号登录Microsoft Windows Server 2003操作系统。

步骤2、关闭所有正在运行的程序。 方便安装程序更新Microsoft Windows 2003操作系统的系统文件而不用重新启动硬件服务器。

步骤3、将TSM的安装光盘插入CD-ROM驱动器。

步骤4、打开资源管理器，进入“Drive:\Server”目录。 其中“Drive:”为光驱所在的盘符，在实际操作中需要替换成实际的盘符。

步骤5、运行“TSMServer.exe”。

步骤6、安装语言选择“chn”。

步骤7、单击“OK”。

步骤8、单击“下一步”。 安装程序将会自动检查1812、1813、3288、8080、8443和17889六个端口是否被其他应用程序占用。如果上述六个端口已经被占用，请停止占用1812、1813、3288、8080、8443或17889六个端口的应用程序

步骤9、单击“确定”。

步骤10、单击“下一步”。

步骤11、认真阅读软件许可协议，确认接受许可协议后选中“我接受该许可协议的条款”。

步骤12、单击“下一步”，分别选中“中文版”和“安全管理器+安全控制器”单选按钮。

步骤13、单击“下一步”，设置TSM管理器和TSM控制器的IP地址。 当TSM管理器和TSM控制器安装在同一台硬件服务器时，TSM管理器和TSM控制器使用相同的IP地址。如果安装TSM管理器和TSM控制器的硬件服务器具有多块网卡，请在下拉列表中选择安装TSM管理器和TSM控制器所使用的网卡

步骤14、单击“下一步”，根据FTP服务器的主目录设置路径。

步骤15、单击“下一步”，设置Microsoft SQL Server 2005的连接参数。 TSM管理器与TSM控制器使用相同的数据库，数据库只需初始化一次。

步骤16、检查Microsoft SQL Server 2005的连接参数并确保输入无误，单击“测试连接并初始化数据库”。

步骤17、单击“下一步”，选择TSM管理器和TSM控制器的安装路径。

步骤18、单击“下一步”，选择需要安装的包。

步骤19、保持默认值，单击“下一步”，开始安装TSM管理器和TSM控制器。

步骤20、单击“下一步”，依次选中“创建快捷方式”、“在桌面创建快捷方式”和“所有用户”。

步骤21、单击“下一步”。

步骤22、单击“完成”。

## 安装TSM代理

### 实验目的

掌握TSM代理安装

### 组网设备

PC

### 实验拓扑图

无

### 配置步骤

步骤1、以超级管理员账号登录Microsoft Windows操作系统。

步骤2、在TSM代理存放目录下双击安装程序“TSM Agent.exe”。

步骤3、选择“中文(简体)”，单击“OK”。

步骤4、单击“下一步”。

步骤5、选择“我同意‘许可协议’中的条款”，单击“下一步”。

步骤6、选择TSM代理的安装目录。

说明：

* 如果TSM代理安装在系统安装盘，请确保系统安装盘至少保留200MB的空闲空间。
* 如果TSM代理安装在系统安装盘以外的分区，请确保所选择的分区至少保留125MB的空闲空间。

步骤7、单击“安装”。

步骤8、单击“确定”。

步骤9、单击“完成”。 安装完成TSM代理后，建议立即重新启动操作系统。

## 初始化TSM管理器

### 实验目的

掌握TSM管理器初始化配置

### 组网设备

服务器

### 实验拓扑图

无

### 配置步骤



步骤1、登陆TSM管理器

1. 打开IE浏览器，在地址栏输入TSM管理器的URL地址，按下“Enter”。 URL地址的格式为“http://TSM-IP:8080/tsm”。其中，“TSM-IP”为TSM管理器的IP地址。例如，假设TSM管理器的IP地址为“10.1.1.1”，请输入“http://10.1.1.1:8080/tsm”。
2. 输入登录参数。
3. 单击“登录”。

步骤2、上传License

1. TSM管理器顶部单击“系统管理”。
2. 在左侧菜单栏选择“License管理 > License信息查看”
3. 在“上传License文件”区域框单击“浏览”。
4. 选择License文件的存放路径。
5. 单击“上传”。
6. 击“确定”。
7. 在TSM管理器顶部单击“系统管理”。
8. 在左侧菜单栏依次选择“License管理 > License信息查看”。
9. 确认License相关的信息正确无误。

步骤3、修改密码

* 1. [登录TSM管理器](mk:@MSITStore:C:\Documents%20and%20Settings\Administrator\桌面\merge.chm::/server/secotsmhlp_tsk_00001.html)。
  2. 在TSM管理器的右上方单击“修改密码”。
  3. 依次输入旧密码、新密码、确认密码。
  4. 单击“确定”。
  5. 单击“确定”。

步骤4、增加TSM控制器

* + 1. 在TSM管理器顶部单击“配置管理”。
    2. 在左侧菜单栏选择“SC配置管理 > SC配置”。
    3. 单击“增加”。
    4. 设置TSM控制器的连接参数。
    5. 单击“确定”。
    6. 单击“确定”。
    7. 重复[3](mk:@MSITStore:C:\Documents%20and%20Settings\Administrator\桌面\merge.chm::/server/cn_smhelp_task_0825.html#cn_smhelp_task_0825__start)～[6](mk:@MSITStore:C:\Documents%20and%20Settings\Administrator\桌面\merge.chm::/server/cn_smhelp_task_0825.html#cn_smhelp_task_0825__end)，将所有规划好的TSM控制器全部加入列表。

步骤5、设置TSM控制器的违规数据上报方式

* + - 1. 在TSM管理器顶部单击“配置管理”。
      2. 在左侧菜单栏选择“SC配置管理 > SC配置”。
      3. 在“SC配置”页面定位需要设置违规数据上报方式的TSM控制器。
      4. 单击该TSM控制器右侧的按钮。
      5. 设置TSM控制器上报违规数据的方式。
      6. 单击“确定”，完成设置TSM控制器的违规数据上报方式。

步骤6、增加归属地

* + - * 1. 在TSM管理器顶部单击“配置管理”。
        2. 在左侧菜单栏选择“SC配置管理 > 归属地配置”。
        3. 单击“增加”。
        4. 设置归属地的相关参数。

步骤7、增加源FTP服务器

在TSM管理器顶部单击“配置管理”。

在左侧菜单栏中选择“应用服务器配置 > FTP服务器配置”，进入“FTP服务器配置”页面。

在“源FTP服务器”区域框中单击“增加”。

输入要新增的源FTP服务器的相关参数。

单击“测试”。

单击“确定”。

单击“确定”。

步骤8、添加镜像FTP服务器

在TSM管理器顶部单击“配置管理”。

在左侧菜单栏中选择“应用服务器配置 > FTP服务器配置”，进入“FTP服务器配置”页面。

在“镜像FTP服务器”区域框中单击“增加”。

输入新增镜像FTP服务器的相关参数。

单击“测试”。

如果参数输入正确，将显示“连接成功”提示框，单击“确定”。

如果参数输入不正确，将显示“FTP连接失败”提示框，单击“确定”，转入[4](mk:@MSITStore:C:\Documents%20and%20Settings\Administrator\桌面\merge.chm::/server/cn_smhelp_task_1690.html#cn_smhelp_task_1690__secotsmhlp_tsk_1690_step_02)重新输入参数。

单击“确定”。

显示“增加成功”提示框。

单击“确定”。

步骤9、为TSM控制器分配FTP服务器

在TSM管理器顶部单击“配置管理”。

在左侧菜单栏中选择“应用服务器配置 > FTP服务器分配”，进入“FTP服务器分配”页面。

单击要分配FTP服务器的TSM控制器右侧的按钮。

单击“首选FTP服务器”区域框右侧的“增加”。

选中要作为首选FTP服务器的FTP服务器。

单击“确定”。

显示“增加成功”提示框。

单击“确定”。

在“首选FTP服务器”区域框中就会看到新增的首选FTP服务器。

增加备选FTP服务器的操作与增加首选FTP服务器的操作相同，请参照[4](mk:@MSITStore:C:\Documents%20and%20Settings\Administrator\桌面\merge.chm::/server/cn_smhelp_task_1691.html#cn_smhelp_task_1691__secotsmhlp_tsk_1691_step_01)～[7](mk:@MSITStore:C:\Documents%20and%20Settings\Administrator\桌面\merge.chm::/server/cn_smhelp_task_1691.html#cn_smhelp_task_1691__secotsmhlp_tsk_1691_step_02)进行操作。

单击“关闭”。

步骤10、上传安全侧路

找到TSM的安装光盘。

将TSM的安装光盘插入光驱。

在TSM管理器顶部单击“策略管理”。

在左侧菜单栏选择“策略配置 > 策略上传”。

单击“增加”。

单击“浏览”，从光盘选择需要上传的策略或策略包。

单击“确定”。

步骤11、注销

确认所有的信息已保存或提交。

在TSM管理器的右上方单击“注销”。

单击“是”。

## 配置TSM策略

### 实验目的

掌握TSM策略设置

### 组网设备

服务器

### 实验拓扑图

无

### 配置步骤

步骤1、创建策略模版

1. 在TSM管理器顶部单击“策略管理”。
2. 在左侧菜单栏中选择“策略配置 > 策略模板”，进入“策略模板”页面。
3. 在“策略模板管理”页签单击“增加”。
4. 输入模板参数。
5. 单击“确定”。
6. 单击“确定”。
7. 如果要进行更多的策略模板配置，请单击“是”进入策略模板配置页面。

步骤2、设置策略的参数，步骤略

步骤3、应用策略

在TSM管理器顶部单击“策略管理”。

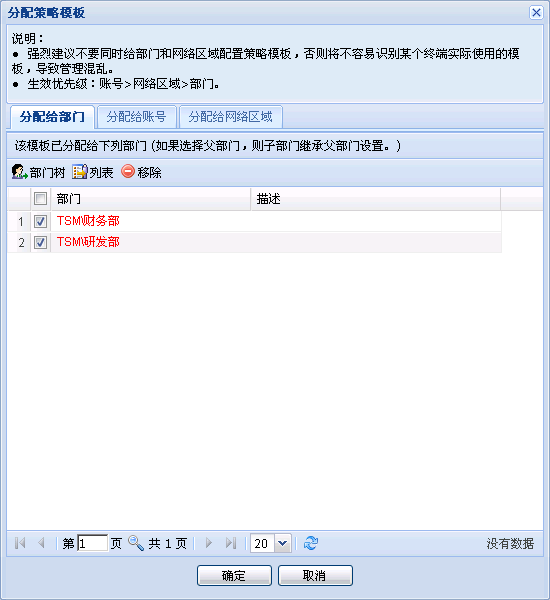
在左侧菜单栏中选择“策略配置 > 策略模板”，进入“策略模板”页面。

单击“查询”，定位要应用到部门的策略模板。

单击要应用到部门的策略模板右侧的按钮。

显示“分配策略模板”页面。

单击“分配给部门”页签。



选择任意一种方式查询目标部门。

如果要从部门导航树选择目标部门，请单击“部门树”，在部门导航树选择目标部门，然后再单击“确定”。

如果要通过部门名称搜索目标部门，请单击“列表”，输入部门名称再单击“查询”，选择目标部门，然后再单击“确定”。

选中要分配策略模板的部门。

单击“确定”。

显示“保存成功”提示框，表示应用策略模板到部门成功。

单击“确定”。

## 配置SACG接入控制

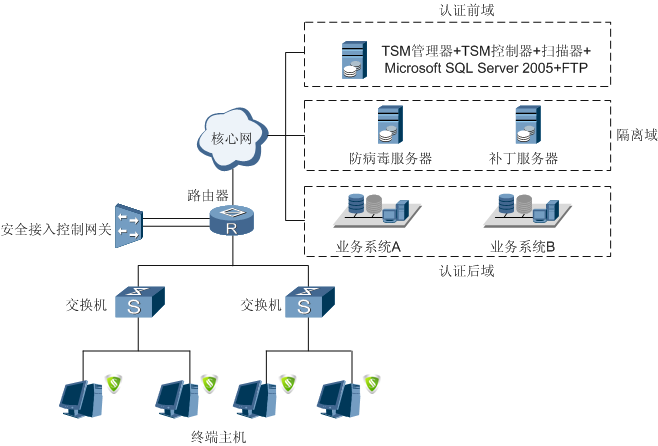
### 实验目的

掌握SACG接入控制配置

### 组网设备

USG防火墙、服务器

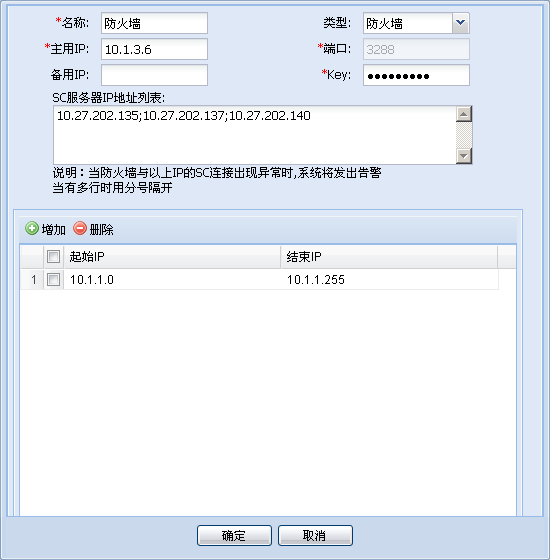
### 实验拓扑图



### 配置步骤

步骤1、增加防火墙

1. 在TSM管理器顶部单击“接入控制”。
2. 在左侧菜单栏选择“接入控制配置 > 硬件SACG”。
3. 选择“硬件SACG”页签。
4. 单击“增加”。
5. 输入硬件安全接入控制网关的连接参数。



1. 单击“确定”。
2. 单击“确定”。

步骤2、增加认证前域

1. 在TSM管理器顶部单击“接入控制”。
2. 在左侧菜单栏选择“接入控制配置 > 硬件SACG”。
3. 选择“前域”页签。
4. 单击“增加”。
5. 设置需要增加到认证前域的网络资源的地址信息。
6. 单击“确定”。
7. 单击“确定”。
8. 将不需要身份认证即可访问并且属于公共类的网络资源均加入认证前域中。

步骤3、增加受控域

1. 在TSM管理器顶部单击“接入控制”。
2. 在左侧菜单栏选择“接入控制配置 > 硬件SACG”。
3. 选择“受控域”页签。
4. 单击“增加”。
5. 输入受控域的相关参数。
6. 单击“增加”。
7. 输入需要加入受控域的网络资源的地址信息。
8. 单击“确定”。
9. 将归属于该受控域的全部相关资源加入该受控域。
10. 单击“确定”。
11. 重复前面的步骤，将规划好的受控域全部加入TSM管理器中。

步骤4、以缺省放行方式增加隔离域

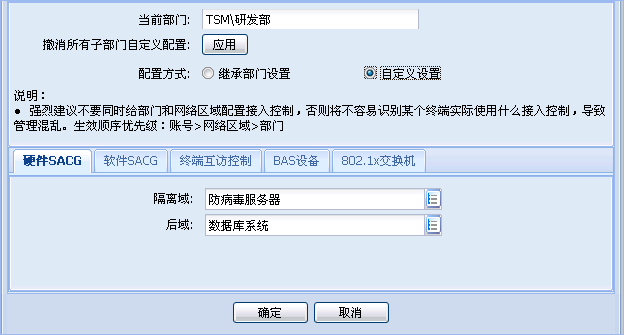
1. 在TSM管理器顶部单击“接入控制”。
2. 在左侧菜单栏选择“接入控制配置 > 硬件SACG”。
3. 选择“隔离域”页签。
4. 单击“增加”。
5. 设置新增加的隔离域的信息。
6. 单击“确定”。
7. 单击“确定”。

步骤5、以缺省放行方式增加认证后域

1. 在TSM管理器顶部单击“接入控制”。
2. 在左侧菜单栏选择“接入控制配置 > 硬件SACG”。
3. 选择“后域”页签。
4. 单击“增加”。
5. 设置新增加的认证后域信息。
6. 单击“确定”。
7. 单击“确定”。

步骤6、应用隔离域和认证后域到部门

1. 在TSM管理器顶部单击“部门管理”。
2. 在左侧菜单栏选择“部门用户 > 部门用户管理”。
3. 选择“部门”页签。
4. 根据需要设置部门的隔离域和认证后域。
5. 要设置顶级部门的隔离域和认证后域，单击“部门接入控制管理”。
6. 要设置非顶级部门的隔离域和认证后域，在部门导航树选择目标部门的上级部门，然后在目标部门的右侧单击按钮。
7. 选择“自定义设置”。
8. 选择“硬件SACG”页签。
9. 在“隔离域”右侧单击按钮。
10. 选择一个隔离域。
11. 击“选择”。
12. 在“后域”右侧单击按钮。



1. 选择一个认证后域。
2. 单击“选择”。
3. 选择隔离域和认证后域的访问控制列表是应用于本部门还是应用于本部门及其下属部门。
4. 单击“确定”。
5. 单击“确定”。

附：SACG配置参考

#

sysname USG

#

firewall packet-filter default permit interzone local trust direction inbound

firewall packet-filter default permit interzone local trust direction outbound

firewall packet-filter default permit interzone local untrust direction inbound

firewall packet-filter default permit interzone local untrust direction outbound

#

undo firewall session link-state check

#

interface GigabitEthernet0/0/4

ip address 10.1.4.2 255.255.0.0

#

interface GigabitEthernet1/0/0

ip address 10.1.5.2 255.255.255.0

#

firewall zone local

set priority 100

#

firewall zone trust

set priority 85

add interface GigabitEthernet0/0/4

#

firewall zone untrust

set priority 5

add interface GigabitEthernet1/0/0

#

firewall zone dmz

set priority 50

#

ip route-static 0.0.0.0 0.0.0.0 10.1.4.1

#

right-manager server-group

default acl 3099

server ip 192.168.1.2 port 3288 shared-key TSM\_Security

server ip 192.168.1.3 port 3288 shared-key TSM\_Security

right-manager server-group enable

right-manager status-detect enable

right-manager authentication url http://192.168.1.2:8080/webauth

right-manager authentication url http://192.168.1.3:8080/webauth

#

policy interzone trust untrust inbound

apply packet-filter right-manager

#

return