IPSEC 配置说明

示例说明:

1、PC1 和 PC2 是两台终端电脑,它们的 IP 地址分别 为 PC1(IP 地址:192.168.201.100 子网掩码:255.2 55.255.0 默认网关:192.168.201.1); PC2(IP 地址: 192.168.208.100 子网掩码:255.255.255.0 默认网 关:192.168.208.1)

2、R 是一台主干路由器,它的两个网口的 IP 地址分别为 172.16.16.1 和 172.16.17.1

3、SR1和 SR2 是我们的网络安全设备, SR1 配置为: 一个 LAN 口(eth6)和一个 WAN 口(eth7), LAN 口 IP 地址为 192.168.201.1, WAN 口 IP 地址为 172.16.16.5; SR2 配置为:一个 LAN 口(eth6)和一个 WAN 口(eth7), LAN 口 IP 地址为 192.168.208.1, WAN 口 IP 地址为 172.16.17.3

4、网络拓扑:SR1 的 eth6 网口连接 PC1 , SR1 的 eth7 网口连接 R 的 WAN3;SR2 的 eth6 网口连接 PC2 , SR2 的 eth7 网口连接 R 的 LAN3

网络拓扑示意图如下







一. SR1 机器的配置

1. 配置 LAN 口

进入管理页面的【网络配置】->【接口配置】->【物 理接口】, 以 eth6 为例 , 点击 eth6 的【修改】, 弹 出下列修改页面:

2404-12781					
• 设备状态					
▶ 实时监控	修改物推荐口经数				構定 道面
▼网络配图		eths			
	Hit S				
安主达地	我口夾型				
> 二层接口配置	所憲区域	三层内网 🗸			
→ 接口配置	基本属性	WANGEL WHEPING			
▶ 物理接口		IPv4 IPv6			
> 网络		途接供型 ● 静态PP			
▶ VLAN接口	IP地址	192. 168. 201. 1/24			
▶ 聚合接口		静态iP地址	æ		
↓ 4to65810					
	MAC地址	00:18:81:89:f7:38 统制数认MAC			
P bto4%E通	工作模式	自由の第 ~	MTU	1500	
■ OSPF路由	星大較长(byte)	1522	屬小帔长(byte)	64	
■ RIP諸由	上行带宽(KB)	0	下行带宽(KB)	0	
 第由设置 	服务带宽(KB)	0			
DINSIES	空务最高配額(百分比)	P2P下號 85 P2P視鏡 100 多洲体視鏡 80 未知的	12 90 保健等意 70		
DDAUGED TH	把绝以太网顿英型	_ethiisnaplc802.3raw			
 DDNSHERE 	UCC禁止转发端口	🔄 eth0 🗋 eth1 🗋 eth2 📄 eth3 📄 eth4 🛄 eth5 🖂 eth6 📄 eth7 🜅	eth8 🗌 eth9 🛄 eth10 🗌 eth11		
● 智能DNS	- UCC接収速率 (Kbyte)	64			
 DHCP配置 	UMC禁止转发跳口	🗌 eth0 📄 eth1 📄 eth2 📄 eth3 📄 eth4 📄 eth5 🗹 eth6 📄 eth7	eth8 eth9 eth10 eth11		
▶ ARP表	UMC接收速率 (Kbyte)	64			
▶防火場	BC禁止转发端口	eth0 eth1 eth2 eth3 eth4 eth5 eth6 eth7	eth8 eth9 eth10 eth11		
Interda	BC接收速率 (Kbyte)	64			
NHXL					
* IPS					
▶ VPN					

填写 LAN 口的主要信息,

接口类型:路由

所属区域:三层内网

允许 PING: 勾选

静态 IP:192.168.201.1/24

见图中的红色框。其他的次要信息保持系统默认即

可。再点击【确定】按钮。

2. 配置 WAN 口



(1)进入管理页面的【网络配置】->【接口配置】-> 【物理接口】, 以 eth7 为例 , 点击 eth7 的【修改】, 弹出下列修改页面:

• 设备状态	(A) (A) (B) (A) (A) (A) (A) (A) (A) (A) (A) (A) (A		
实时监控	NOT OF BERKLINGER		1812
▼网络配盟	SLI-MP		
> 安全区域	5R/2 1204-RI		
	75.400.46		
● 接口配数	SE 4 ABILE		
■ OSPF路由		IPvi IPvi	
Image: RIP路由		法接触型 ● ● DHCP ○ ADSL版号	
 語由设置 		172. 16. 16. 5/24	
> DNSIRG	IP地址	静态中均址	
D D D D D D D D D D D D D D D D D D D			
DUNSMEAR		P	
● 智能DNS			
● DHCP配置			
▶ ARP表	上行带宽	100 Mpps V	
▶防火墙	下行带宽	100 Mbps v	
・山田中心	线路健康检测	②五 · · · · · · · · · · · · · · · · · · ·	
- PHERE	MACHBAL	00:18:81:89:f7:39	
* IPS	工作模式	mathet v 1500 V	
• VPN	毫大較长(byte)	1522 最小粉长(byte) 64	
• 用户认证	服务带宽(KB)	<u>b</u>	
流量控制	並毎最高配額 (百分比)	P2P下載 85 P2P88期 100 多個体規則 80 未完於以 90 保障等效 70	
▶ 系统对象	拒绝以太同帧类型	Dethii Disnap Dic D802.3raw	
▶ 可达职团	UCC禁止转发跳口	_ mb0 _ mb1 _ mb2 _ mb3 _ mb4 _ mb5 _ mb5 _ mb7 _ mb8 _ mb9 _ mb9 _ mb10 _ mb11	
· MARIEN	ÜCC接收速率 (Kbyte)	64	
* 系统日志	UMC禁止转发展口	_ mm0 _ mm1 _ mm2 _ mm3 _ mm4 _ mm5 _ mm5 _ mm7 _ mm8 _ mm9 _ mm10 _ mm11	
・HA 配置	UMC接收速率 (Kbyte)	64	
▶配置向导	BC禁止转发纳口	_ em0_ em1_ em2_ em3_ em4_ em5_ em5 ≥ em7_ em8_ em9_ em10_ em 11	
・报表中心	BC接收速率 (Kbjte)	64	

填写 WAN 口的主要信息,

接口类型:路由

所属区域:三层外网

WAN 端口:勾选

允许 PING: 勾选

静态 IP:172.16.16.5/24

下一跳网关:172.16.16.1

见图中的红色框。其他的次要信息保持系统默认即

可。再点击【确定】按钮。

(2)为了跨路由访问,必须为WAN口设置一条静态默认路由,进入管理页面的【网络配置】->【路由设置】->【静态路由】,点击【新增】按钮,弹出如下页

面:						
· 设备状态						
* 本財告約	IPV4 IPV6					
マの将の思想	新增静态路由				ate	波見
 安全区域 	美型	● 单个静志路由 ○ 多个静态路由				
	目的网段	0.0.0.0/0.0.0				
● 接口腔隙	下一期P地址	172.16.16.1				
■ OSPERISE	接口	eth7 v				
RIPIRth	3cmm	0 (0-255)				
 第4629 						
→ 約8m →						
1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1						
Catala Pituda						
DANSED TO						
DIVISION						
APOR						
h Physics and						
· N#ge						
* IPS						
• VPN						
• MPWE						
 洗服形制 						
* 形玩可欺						
* 所统尾波						

填写静态路由的主要信息,

目的网段:0.0.0.0/0.0.0.0

下一跳 IP 地址: 172.16.16.1

接口:eth7

见图中的红色框。其他的次要信息保持系统默认即

可。再点击【确定】按钮。

3. 配置 IPSEC

(1) 设置 IPSec 隧道

进入管理页面的【VPN】->【IPSec】->【IPSec 隧

道】, 点击【新增】按钮, 弹出如下页面:







填写 IPSec 隧道的主要信息,

名称: ipsectunn

本端网关->固定 IP:172.16.16.5

对端网关->固定 IP:172.16.17.3

共享密钥->预共享密钥:123456

见图中的红色框。其他的次要信息保持系统默认即

可。再点击【确定】按钮。

(2) 设置 IPSec 规则

进入管理页面的【防火墙】->【安全策略】,点击【新

增】按钮,弹出如下页面:

采甲导航		
 设备状态 		
• 实时监控	新增安全兼賠加別	
▶ 网络副纲	規則名称	[becule]
The steam	策略万円	
防天潮		192 0 0/24
▶ 安全策略	源地址	
■ NAT規則		ψ
DOS/DDOS防护		1978k v
ARPROMISSO	目的地址	192.168.208.0/24
▶ 应用层网关		
1584/V	服务	13.师 (唐以已选全部服务)
· ANETO TO	生效时间	<u>@</u> ,
• 内容安全	安全配置	
• IPS	动作	○ 允许 ○ 把他 ○ PNT ○ 需要认证 ● VPN
• VPN	隧道名称	pectum v
•用户认证	方向	● 刘颖→本荫 ○ 刘颖→本荫
▶流量控制	271 (sc) 12.4%	○日用●第用
• 系体对像	RENT KLAR.	(行对如本基形態对生效)
b ar constraint	状态	● 屈用 ○ 期用
· 3032408	快速路接 [IP组] [生效时间] [安全配置] [B	最近 [PAT)法]
▶系统日志		
▶ HA 配置		
• 配置向导		
•报表中心		



填写 IPSec 规则的主要信息,

名称: ipsecrule

源地址->IP 地址:192.168.201.0/24

目的地址->IP 地址: 192.168.208.0/24

动作:VPN

隧道名称:ipsectunn

见图中的红色框。其他的次要信息保持系统默认即

可。再点击【确定】按钮。

(3) 启用 IPSec

进入管理页面的【VPN】->【IPSec】->【IPSec规

则】,如下图所示:



点击上图右上角的【应用】按钮,就可启用 IPSec 功能。

二. SR2 机器的配置

1. 配置 LAN 口

进入管理页面的【网络配置】->【接口配置】->【物



理接口】, 以 eth6 为例 , 点击 eth6 的【修改】, 弹 出下列修改页面:

菜単导航						
•设备状态 ^						
 	位改物證證口參数				構定	道臣
「同体和問	接口名称	eth6				
Pyriodal	描述					
2 2 2 X X	接口供型					
> 二层接口和置	所屬区域	三层内网				
○ 接口配置	基本履性	□ WAN第□ ☑ 允许PING				
1 物理接口		IPv4 IPv6				_
▶ 同桥		追接类型 ● 静态	P			
► VIAN#□	伊地址	192.1	68. 208. 1/24			
N MARCI		静态P地址				
R T M L			ų.			
▶ 4to6版E面	MAC 地址	00:18:81:89:17:38 (59:80.00)	AC			
▶ 6to4認識	工作機式	自动协商 🗸	MTU	1500		
 OSPF諸由 	最大較长(b)te)	1522	最小帧长(byte)	64		
■ RIP諸由	上行带宽(KB)	0	下行带宽(KB)	0		
 語由设置 	服务带宽(KB)	0				
DNSB/07	並隽最高配額 (百分比)	P2P下載 85 P2P税绩 100	多媒体规模 80 未知协议 90 保障带宽 70			
PONCES.	拒绝以太同顿类型	_ethii _snap _lc _802.3raw				
P DUNSIEBE	UCC施止转发编口	eth0 eth1 eth2 eth3 eth-	4 🗌 eth 5 🖂 eth 6 🛄 eth 7 🛄 eth 8 🛄 eth 9 💭 eth 10 🛄 eth 11			
BRDNS	ÜCC接收速率 (Kbyte)	64				
● DHCP配置	UMC禁止转发跳口	eth0 eth1 eth2 eth3 eth-	4 🗌 eth5 🗹 eth6 🔲 eth7 🛄 eth8 🛄 eth9 🛄 eth10 🛄 eth11			
▶ ARP衷	UMC接改速率 (Kbyte)	64				
▶防火墙	BC禁止转发跳口	eth0 eth1 eth2 eth3 eth4	4 🗌 eth6 🔄 eth6 🔲 eth7 📋 eth8 📄 eth9 💭 eth10 🛄 eth11			
・内容中全	BC腹纹速率 (Kbyte)	64				
hine						
115						
* VPN						
• 用户认证						

填写 LAN 口的主要信息,

接口类型:路由

所属区域:三层内网

允许 PING: 勾选

静态 IP:192.168.208.1/24

见图中的红色框。其他的次要信息保持系统默认即

可。再点击【确定】按钮。

2. 配置 WAN 口

(1)进入管理页面的【网络配置】->【接口配置】
->【物理接口】,以 eth7 为例,点击 eth7 的【修改】, 弹出下列修改页面:



IPSEC 配置手册

菜单导航					
▶ 设备状态					
▶ 实时监控	将改物到涂口是数				桃 定 道口
「図体配の	選口名称	eth.7			
	描述				
· 女主心相	現山東型	調由			
> 二层按口配置	所憲区域	三层外列			
- 接口配置	益 4/通恒	M WANGHLI M 7634-PING			
> 物理接口		IPv4 IPv6			
▶ 网标		注接発型 ● 静志P O DHCP O) ADSL拨号		
VLAN#□		172. 16. 17. 3/24			
▶ 聚合接口	萨地址	静态IP地址	4		
▶ 4to6隧道		下一跳网头 172.16.17.1 (4)	· · · · · · · · · · · · · · · · · · ·		
6to4880		〇 中間pat			
■ OSPF路由		O PAT35			
(a) pinter	上行带意	100 Mbps ~			
	下行带意	100 Mbps ~			
▲ 第田役置	线路健康检测	设置 ④ 查看任路洋情			
▶ DNS配置	MAC地址	00:18:81:89:f7:39 ###KAMAC			
▶ DDNS配置	工作模式	自动协用 🗸	MTU	1500	
● 智能DNS	最大較长(byte)	1522	最小顿长(byte)	64	
● DHCP配置	服务带宽(KB)	0			
ARP表	业务最高配额 (百分比)	P2P下載 85 P2P視頭 100 参媒体視頭 80	未知协议 90 保障带宽 70		
P Pri str att	拒绝以太网顿美型	_ethiisnaplic802.3raw			
* 80 X 40	UCC禁止转发跳口	📄 eth0 📄 eth1 📄 eth2 📄 eth3 📄 eth4 📄 eth5 📄 eth6 🖂	eth7 🔄 eth8 🔄 eth9 🔄 eth10 🛄 eth11		
• 内容安全	ÜCC撮吹速率 (Kbyte)	64			
• IPS	UMC禁止转发进口	eth0 eth1 eth2 eth3 eth4 eth5 eth6	eth7 🔄 eth8 🔄 eth9 🔄 eth10 📄 eth11		
• VPN	UMC接收速率 (Kbyte)	64			
▶用户认证	BC禁止转发銷口	🗌 eth0 🗋 eth1 🗋 eth2 📄 eth3 📄 eth4 📄 eth5 📄 eth6 🖂	eth7 🗋 eth8 🔄 eth9 🛄 eth10 🛄 eth11		
 ·	BC接收速率 (Kbyte)	64			

填写 WAN 口的主要信息,

- 接口类型:路由
- 所属区域:三层外网
- WAN 端口:勾选
- 允许 PING: 勾选
- 静态 IP:172.16.17.3/24
- 下一跳网关:172.16.17.1
- 见图中的红色框。其他的次要信息保持系统默认即 可。再点击【确定】按钮。

(2)为了跨路由访问,必须为WAN口设置一条静态默认路由,进入管理页面的【网络配置】->【路由设置】->【静态路由】,点击【新增】按钮:



			and the second
•设备状态 ^			
• 实时监拉	IPV4 IPV6		
▼网络配盟	新培静态路由		検定 認知
 安全区域 	黄型	● 単个器を語由 ○ 多个器を語出	
▶ 二层接口配置	目的网段	0.0.0/0.0.0	
● 接口配置	►		
■ OSPF路由	2011	0 0.255)	
■ RIP路由			
- 語由设置			
▶ 主机器由			
E ANGERA			
● 策略路由			
▶ DNS配置			
▶ DDNS配置			
■ 智能DNS			
● DHCP配置			
▶ ARP表			
▶ 筋火墙			
• 内容安全			
▶ IPS			
▶ VPN			
▶用户认证			
流量控制			
• 系统对象			
• 系統配置			
▶ 奚姊日志			

填写静态路由的主要信息,

目的网段:0.0.0.0/0.0.0.0

下一跳 IP 地址: 172.16.17.1

接口:eth7

见图中的红色框。其他的次要信息保持系统默认即

可。再点击【确定】按钮。

3. 配置 IPSEC

(1) 设置 IPSec 隧道

进入管理页面的【VPN】->【IPSec】->【IPSec 隧

道】, 点击【新增】按钮:





填写 IPSec 隧道的主要信息,

名称: ipsectunn

本端网关->固定 IP:172.16.17.3

对端网关->固定 IP:172.16.16.5

共享密钥->预共享密钥:123456

见图中的红色框。其他的次要信息保持系统默认即

可。再点击【确定】按钮。

(2) 设置 IPSec 规则

进入管理页面的【防火墙】->【安全策略】,点击【新 增】按钮:

来申号机 🔪		
设备状态	新田安全放動原則	
• 实时监控	初期になっていたのでの	ipserule au
• 网络配盟	策略方向	M ALL THE ALL T
▼防火墙		
> 安全策略	源地址	192. 168. 208, 0/24
● NAT規則		4
● DOS/DDOS防护		
ARP#X988559	目的地址	192. 108. 201. 0/ 24
> 应用层网关		ų.
> 加速电化	服务	25個 (飲い)(25個級分)
• 内容安全	生双时间	
► IPS	动作	
• VPN	隧道名称	
▶用户认证	方向	● 別談→→本請 ○ 別談→→本請
 流量控制 	田町に己愛	○ 日刊 ● 第月 ○ 日刊 ● 第月
• 系统对象		(+0)(#T###DB#235X)
▶ 系统配置	状态	
▶ 系統日志		09] [PAT78]
▶ HA 配盟		
• 配置向导		
・报表中心		

填写 IPSec 规则的主要信息,

名称:ipsecrule 源地址->IP 地址:192.168.208.0/24 目的地址->IP 地址:192.168.201.0/24 动作:VPN



隧道名称:ipsectunn

见图中的红色框。其他的次要信息保持系统默认即 可。再点击【确定】按钮。

(3) 启用 IPSec

进入管理页面的【VPN】->【IPSec】->【IPSec 规

则】,如下图所示:



点击上图右上角的【应用】按钮,就可启用 IPSec 功能。