# 中安云科 IPSEC/SSL VPN 综 合安全网关网关 用户操作手册

中安云科科技发展(山东)有限公司

2023年04月20日

1.	手册打	指南				 	1 -
	1.1.	概述				 	1-
	1.2.	目的				 	1-
	1.3.	适用对	象			 	1 -
	1.4.	名词解	释			 	2 -
2.	环境i	说明				 	3 -
	2.1.	产品检	查			 	3 -
	2.2.	默认网	络配置	۔		 	3 -
	2.3.	环境准	备			 	3 -
	2.4.	开机				 	4 -
	2.5.	关机				 	4 -
3. 7	力能操	作使用访	兑明			 	5 -
	3.1	初始化				 	5 -
		3.1.1	初始	化系统超级管	理员	 	6 -
		3.1.2	初始	化系统审计管	理员	 	6 -
	3.2	SSL VPN	登录			 	7 -
	3.3	超组	吸管理	员用户		 	9 -
		3.3.1 用	户管理	里		 	9 -
		3.3.	1.1	f增用户		 	9 -
		3.3.	1.2 丿	、员列表		 	10 -
	3.4	系统管理	員用	户		 	10 -
		3.4.1	设备	导航(重新截图	])	 	11 -
		3.4.2	设备	授权		 	11 -
		3.4.3	网络	管理		 	11 -
		3.4.	3.1	网络配置		 	11 -
		3.4.	3.2	Bond 配置		 	12 -
		3.4.	3.3	路由配置		 	13 -
		3.4.	3.4	双机热备		 	14 -
		3.4.4	时间	配置		 	15 -
		3.4.	4.1	系统时间配置		 	15 -
		3.4.5	设备	状态		 	16 -
		3.4.	5.1	自检状态		 	16 -
		3.4.	5.2	运行状态		 	17 -
		3.4.6	设备	运维		 	18 -
		3.4.	6.1	运维管理		 	18 -
		3.4.	6.2	SSH 功能		 	19 -
		3.4.7	设备	重置		 	19 -
		3.4.	7.1	密码卡初始化		 	19 -
		3.4.	7.2	恢复出厂设置		 	19 -
		3.4.8	设备	更新		 	20 -
		3.4.	8.1	离线升级		 	20 -
	3.5	安全管理	1员用,	户		 	21 -

# 目录

3.5.1 密	钥管理	23 -
3.5.1.1	SM2 密钥管理	23 -
3.5.1.2	RSA 密钥管理	25 -
3.5.1.3	ECC 密钥管理	27 -
3.5.2 证书管	管理	29 -
3.5.2.1	设备证书	29 -
3.5.2.2	证书吊销列表	32 -
3.5.3 隧道	服务	34 -
3.5.4 用户(	言息管理	38 -
3.5.4.1	用户组管理	38 -
3.5.4.2	用户管理	39 -
3.5.4.3	特征码管理	
3.5.4.4	认证管理	43 -
3.5.5 资源管	管理	44 -
3.5.5.1	资源配置	44 -
3.5.5.1	资源组管理	45 -
3.5.6 网关-	客户端模式	48 -
3.5.6.1	配置网关	48 -
3.5.6.2	访问记录	49 -
3.5.7 IPSEC 管理		50 -
3.5.7.1	策略配置	50 -
3.5.7.1	隧道监控	51 -
3.5.8 系统	备份与恢复	52 -
3.5.8.1	系统备份	52 -
3.5.8.2	系统恢复	53 -
3.6 审计管理员	用户	54 -
3.6.1 日志管	管理	54 -
3.5.1.4	日志配置	54 -
3.5.1.5	日志查看	55 -
3.5.1.6	日志归档	56 -

# 1. 手册指南

#### 1.1. 概述

本手册主要介绍中安云科 IPSEC/SSL VPN 综合安全网关网关的使用及维护。其中涵盖了中安云科 IPSEC/SSL VPN 综合安全网关网关所涉及的配置方法及其使用说明。

我们将以提供具体实例的方法来引导使用者安装配置符合自己应用环境的网关。

#### 1.2. 目的

本手册详细描述了如何部署、配置、管理和使用中安云科 IPSEC/SSL VPN综合安全网关网关,目的是指导用户能正确的管理和 使用本产品。

#### 1.3. 适用对象

本手册适用对象为网络管理员、网关实施人员、售前支持人员和 技术支持人员,需要具备以下概念知识:

(1) 网络拓扑

- (2) 网络地址和路由
- (3) 数字证书、VPN、HTTPS
- (4) Web 服务器

#### 1.4. 名词解释

虚拟局域网(VPN):虚拟专用网指的是依靠 ISP (Internet 服务提供商)和其它 NSP (网络服务提供商),在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中,任意两个节点之间的连接并没有传统专网所需的端到端的物理链路,而是利用某种公众网的资源动态组成的。

SSL VPN:应用层的一种 VPN,一般以客户端与服务端形式存在, 一般用于认证客户端身份和加密应用层数据,例如对 WEB 资源进行访 问控制,并对其进行数据加密。

证书认证机构(Certificate Authority):一个产生和确定公开 密钥证书的可靠和可信的第三方机构。它发行数字证书并确保证书的 可信性,或证明一个用户和它们的公共密钥的身份。认证机构也可以 为实体产生和确定密钥。习惯上又称作认证中心(CA)。

数字证书(Certificate):数字证书中心签发的用于代表实体身份的一段电文。本手册中涉及代表用户身份的用户证书和代表服务端身份的站点证书(服务器证书)。

LDAP: (Lightweight Directory Access Protocol)是一种轻量 级的目录存取协定,提供客户从各个角落连接到目录服务器中。本手 册中专指 CA 用于发布证书及黑名单的 LDAP 服务。

黑名单:通常所说的 CRL (Certificate Revoke List),因时间 或者安全原因被废除的证书列表,一般发布在 LDAP 上。

- 2 -

# 2. 环境说明

本章讲述安装中安云科 IPSEC/SSL VPN 综合安全网关网关需要进行的工作和步骤,以及正式配置前的环境准备工作。

#### 2.1. 产品检查

在安装中安云科 IPSEC/SSL VPN 综合安全网关网关之前应对照着 产品清单确保所有部件都已存在,并检查所有部件是否完好。如果有 任何部件缺少或者损坏,请不要进行安装,应立即与厂商进行联系。

2	2	默认网络配置	ļ
4.	4.	<u> </u>	

网络接口	用途	出厂接口地址
eth0	管理口	192. 168. 5. 10
eth1	应用口	192. 168. 6. 10
eth2	应用口	192. 168. 7. 10
eth3	应用口	192. 168. 8. 10
•••	•••	•••

注: 如果 5 个及以上网口均按照以上结构进行出厂配置

#### 2.3. 环境准备

1) 中安云科 IPSEC/SSL VPN 综合安全网关网关产品工作环境:

工作温度:0 ℃--40℃

存储温度: -40℃--70℃

工作湿度: 5%--95%RH, 不凝结

工作电源: 100---240VAC, 50-60Hz

2) 中安云科 IPSEC/SSL VPN 综合安全网关网关工作时需要以下 连接线接入设备:

- ▶ 2根电源线。(连接电源时所需)
- ▶ 连接外网口与外部网络的 RJ-45 网线。(接入 WAN 接口时 所需)
- ▶ 连接内网口与内部服务器网络的 RJ-45 网线。(接入 LAN 接口)
- ▶ 连接管理口接口的 RJ-45 网线(接入管理口时所需)

## 2.4. 开机

确保连接线连接无误后,打开设备后面板的电源开关,开机后会发出刺耳响声,按一下面板后面的红色按钮即可。

启动约为1分钟。一旦设备加电,则系统前面板上的指示灯将显示系统的状态:

- 电源灯闪烁显示系统加电成功
- 磁盘灯亮表示正在读取磁盘
- 故障灯亮表示设备故障
- 运行状态灯闪烁表示运行正常

## 2.5. 关机

关闭中安云科 IPSEC/SSL VPN 综合安全网关网关电源即可。

# 3. 功能操作使用说明

在使用 VPN 配置管理系统进行管理之前, 您需要完成下面的准备工作:

1、将中安云科 IPSEC/SSL VPN 综合安全网关网关开机。

2、使用网线将中安云科 IPSEC/SSL VPN 综合安全网关网关的 NET1(LAN)口,与计算机网卡相连。

3、将本地计算机的 IP 地址设置成与中安云科 IPSEC/SSL VPN 综 合安全网关网关 NET1(LAN) 口同一子网的地址(默认情况下, NET3 接口 IP 为 192.168.8.10)。

## 3.1 初始化

在初始化界面和登录页面选择 Ukey 登录界面,点击右下角【下载托盘程序】,即可在浏览器完成下载。下载完成后,解压压缩包,点击安装程序,根据提示安装即可。

10000	① ①始化超级管理员	② 初始化审计管理员	3 完成		
· 登录账号:	superAdmin	性别:	男		理平台 / 专注于密码服务管理
*静态口令:	admin@2030 ©	*确认静态口令:		0	UKey登录
手机号码:	请输入手机号码	Email:	请输入邮箱地址		n
IUKEY信息					
* 验证UKEY口令:	·······	UKEY证书序列号:	654774019792801792		1.7
UKEY证书:	HIIOC2CCA&GgAVIBAGIJZUHDAZO52B2BNAGCCQBBB DYQQDDADQZDDDBSCDTILBDIVODBWTEVOYQDDATI4A kGAIUBC2VCHTEXCZADBJWRAANAJBHDBSVDYJEGZJ t5ZOpb3LzbhmdWqDWYTav9mjOCDARvt0c/qDAxo0d	M9VAYNIMDoxCzAJBgNVBAYTAŁNOWQO ADIWODEWNTEWOVOWYTELMAŁGAIUEBŁI EhvcNAQŁBFgIzMTELMAŁGAIUEAWWCNT AZLVORÓTZYÓBVZpbŁFwOExteHj7upmu	ccvyDVqqxDaROZXHOMQOvcvyDVqqLDARC KQQ04cCxAjBgRVBagMajBzMOzvCqyDVqq HEwWTATBgcqbkjOPQIBBggqRaPVqQCLC qtjqbjDBo3kwdzAdBgRVBQ4EFgQUDTVkJ	ZIGOMQOWCWY HDAIXWTELMA MCAASI8PsoE TOGHçSwkRVL	登录
	下載UKEY	氏盘程序 提交 重打	Ξ.		

密码登录   UKe	ey登录
合 请输入PIN	
请输入PIN	
6 请输入密码	
请输入您的密码	坐下载托盘程序
登	录
登	录

## 3.1.1 初始化系统超级管理员

首先初始化系统超级管理员,将超级管理员 UKey 插入计算机的 USB 接口, 按照提示 输入两次口令,点击"初始化超级管理员",初始化成功后自动跳转到下一个页面。

* 放業時号: SuperAdmin 住翁: 男 / / / / / / / / / / / / / / / / / /	* 登政務等:         superAdmin         世期: 男   <		
* 砂白白:       admin@2000       ・ 改正       VKey登录       UKey登录         手机見弱:       3mk込手引号码       Email:       3mk込が目台:       ************************************	*##dDe: adming2000 • *#kk##dDe: • UKey@# ##fi@#: imit_0.000 • *#kk##dDe: • UKey@# ##fi@#: imit_0.000 • *#kk##dDe:	性別: 男	~
手引导発: (時心入手引导発)             ・ 近辺いたビロ今:          ・ 一	手切信号:         面積人生引信号         Email:         面積人出目相同位:            IUKEY指言:         ●         新正         UKEY呈書         ●	◎ * 确认额恋□今:	◎ UKey登录
I UKEY信息 * 独立UKEY口令: ① 验证 UKEY证书序列号: 654774015752201752	I UKEY協想         ● 新臣         UKEY怪共協会         ● 新臣         UKEY怪共協会         ● 新臣         UKEY怪共協会         ● 新臣         UKEY怪共協会         ● 新臣         UKEY優大協会         ● 新臣         ● 新日	Email: 调输入邮箱地址	n
* 验证UKEY口令:	* MAEU/KEYCI+         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		
	UKEYVEH:         INTICCSCALO/petTLagTZDEALC+g6=08400CC_08889782TE0-04-24.07 g4704713408000-04709000 LADDINONO-VT PROLADDINONO-VT         Image: https://doi.org/10.00000000000000000000000000000000000	金证 UKEY证书序列号: 65477401979280	01792.
レビアン理由:	kaliecydre staledrautaiene dal johan alene darfin alene dal johan a Alene dal johan alene dal	SGCC gBEBBS VAYNLIND 0 XC XAJE gNVEAYTALENONQOUCUVD VQQKDAROZIODONQ F0 IDTT 4 ND I VO DEWHTE VO VOW TTEL MARGAI UEBLNCQO 4 XC XAJE gNVEA gNA	IOVCVTDTQLLABOZZEXNAQVCVY
kola (BC-pectrae) ola (B-preslanda) je lateno krytitaci i kredina krytitaci i kryt		DwYJKoZIhwoNagkBFgIxWTELNAkGALUEAwwCWTEWWTATBgoqhkjOPqIB gDaxcOdm2LWGn6Tro6BVZpbkFsOEatsHj7upnqtJqbjDBo3kwdzàdBgN	BBgggggRoPWQCLQNCAASIBPsoB
UKEYNE-SE MITOCHOLADORHITAHTTUNKALE SERVEN PROCEMULATION AND THE INFORMATION IALIIIIS-AUTOMATION I INFO		· · · · · · · · · · · · · · · · · · ·	

## 3.1.2 初始化系统审计管理员

初始化完系统的超级管理员之后,会自动跳转到初始化系统审计管理员,初始化方式与

用户信息	刃始化超级管理员		初始化审计管理员	完成	
* 是规策登*	audAdmin		性别:		
*静态□令:	•••••	۵	*确认静态口令:	••••••	
手机号码:			Email:		
UKEY信息					
*验证UKEY口令:	•••••	◎ 脸证	UKEY证书序列	05673342284370513921755598276916	
			룩:		
UKEY证书:	MIIC dDCCAhugAwIBAgIUBWcz W5nZG9uZzEOMAwGAIUEBwwFa YDVQQDDAxITIIgUx9PVCAgQO MBuWxsSS4nDEFMAOGAIUEBww AIUEAwwYMDAyMjAxMTI2Mzgy	QihDoFE5IXWVm mluYW4xEzARBg EwHhcNMjMwMzM G5rW05Y2XMRUw NDU00DMzMzIzN	CdpFlWGSRYwCgYIKoEcz1UBg3Uw NYBAOMCINJTk9DSVBIUIQxGjAYB xMDcONTE4WacNNggwWzMxMDcONT EvYDVQQKDAzkuK31ronkupHnp5E TMOMFkwEwYHKoZIzjOCAQYIKoEc	eTELMAKGA1UEBhMCQ04xEjAQBgNVBAgMCXNoY gNVBAsMEVNJTk9DSVBIRVIgLVRSVNUMRUWEw E4WjGBgDELMAKGA1UEBhMCQ04xDzANBgNVBAg xFFATBgNVBASMDOS4reWuieSSkeenkTEBMB96 ziUBgiDDQgAEFvze8IWqG/ickj7MLyCFho41	< >//

初始化系统超级管理员相同,初始化完毕后,自动跳转登陆界面。

## 3.2 SSL VPN 登录

管理员有两种登录方式分别是密码登录和 UKey 登录。

密码登录:点击【密码登录】,填写账号、密码、图片验证码,然后点击【登录】按钮,系统验证通过,进入服务器综合安全网关。

密码设备管理系统 / 专注于密码服务管理
<b>密码登录</b> UKey登录
SupAdmin
1 记住密码
登录

UKey 登录:点击【UKey 登录】,插入 Web 页面 Ukey,填写 PIN、密码, 然后点击【登录】按钮,系统验证通过,进入服务器综合安全网关。

密码登录   UKey	登录
a	
请输入您的密码	土下载UKEY托盘程序
	登录

## 3.3 超级管理员用户

## 3.3.1 用户管理

管理员管理包括新建管理员、管理员列表。

#### 3.3.1.1 新增用户

点击【新增】,管理员类型可以选择系统管理员、系统安全管理员(注:这 里新增管理员的时候,已经插在计算机上的超级管理员的 key 不动,直接将新的 key 插到计算机上即可),插入新的 key,选择要生成的管理员类型,输入口令, 点击"提交"按钮,管理员生成成功。

*认证模式:	静态口令	~	* 用户名:	test	
*静态口令:	qwer1234!%	٢	*确认静态口令:		
手机号码:	17888888888		邮箱:	123@qq.com	
归属部门:	请选择归属部门		*角色:	系统管理员 🛞	$\sim$

#### 3.3.1.2 人员列表

可以在管理员列表中查看生成的管理员,如下图所示。内容包括管理员的登录名、管理员类型、管理员状态。处于正常状态的管理员可以登录,处于锁定状态的管理员不可以登录。对于管理员 key 丢失的情况,我们可以对丢失的 key 的管理员进行锁定操作,以提高系统使用的安全性。

第 密码设备管理	系統										오 supAdmin ~
用户管理 人员管理	*	C INFAN STR	用户名称		<b>FN58</b> 3867±1.58		KZ Brits		1 There Are and a second	の機械の服	9
			+ 新増	2. Mat 0. B	◎ 土 考入 <u>×</u> 考出						00
				用户编号	用户名称	用戶暇称	部门	手机号码	状态	创建时间	證作
				140	supAdmin	167772209				2023-04-21 11:53:27	ん修改 白融時 > 更多
				142	audAdmin	167772209				2023-04-21 14:05:30	2.1822 回日期 > 图多
				144	sysAdmin	167772209				2023-04-21 14:26:45	2.18改 回题除 > 更多
				145	secAdmin	167772209				2023-04-21 14:27:34	之修改 回動時 > 更多
									共4条 10条	页 ~ < 1	前往 1 页

## 3.4 系统管理员用户

以系统管理员身份登陆 WEB 管理系统,该管理员用户下支持系统 管理、系统监控、网口管理、防火墙、运维工具等功能,并支持查看 设备基础信息。

## 3.4.1 设备导航

可以进行系统配置的快捷跳转,以便更方便的进行操作。

## 3.4.2 设备授权

可以查看授权信息,下载授权码和更新授权证书。

系统导航	授权信息
设备导航	系统信息 2.7年8803
服务配置	产品名称:《一般必管理平台
anex.	作品版本: v100
网络管理	按双体显 ● Manifold's
87月6日期	席码構心部件序列号: 新元信息
28KS	播版状态: 未损积 有效期: 新无功息
设备运输	援权日期: 新元信息
公共開発	
设备更新	

## 3.4.3 网络管理

#### 3.4.3.1 网络配置

点击【网络管理】,点击【网络配置】进入到网络配置页面。

网口名称	IPV4181	t [ millionni	IPV6888E	0.82	の意思				
C 重曲网络									
MOSR	IPV4Bbb	IPV6884£	7140883	macilitä	BUARDA	DN SHULE	R.W.	RORE	1845
eth0	192.168.5.10		255 255 255 0	3c ec of 94-46 fa			Ethernet	管理口	ight while
eth1	192.168.6.93		255 255 255 0	3c.ec.ef 94:46.fb			Ethemet	管理业务口	inter and
eth2	192.168.7.10		255 255 255 0	3c ec ef 94.46 fc			Ethernet	管理口	10500 MARIN
eth3	192 168 8 93		255.255.255.0	3c ec of 94:46.fd			Ethernet	問題日	igat wat

#### 3.4.3.1.1 编辑

点击【编辑】,在弹出的对话框中可修改 IPV4 地址、IPV6 地址、子网掩码、默认网关、 DNS 地址,然后【确认】完成编辑。注意每个的格式都要填写正确。点击重启后生效。

网口名称 请输入网门名称	IP\	编辑网络配置				×				
		网口名称	eth0	IPV4地址	192.168.5.134					
+ 重启网络		IPV6地址	192.168.6.12	子网掩码	255.255.255.0					
阿口名称	IPV4地址	默认网关	255.255.255.0	<ul> <li>DNS地址</li> </ul>	请输入DNS地址		也址	类型	阿口配置	操作
eth0	192.168.5.134							Ethernet	管理/业务口	设置编辑
eth1	192.168.6.134				确定	取消		Ethernet	管理/业务口	设置 網道
eth2	192.168.8.134		255.255.255.0	3c.ec.ef.94:49:74				Ethernet	业务口	设置 编辑
eth3	192.168.10.134		255.255.255.0	3c.ec.ef.94:49:75				Ethernet	业务口	设置 编辑

## 3.4.3.1.2 设置网口类型

点击【设置】,在弹出的对话框中可选择管理口、业务口,然后【确认】完成设置。点 击重启后生效。

	网口名称 清输入网口含物	: IPV	修改网络配置信息		×	1			
			网口 eth3						
-+	- 重启网络		网口配置 💿 管理小业务口 💿 管理	口 💿 业务口					
	网口名称	IPV4地址				也址	类型	网口配置	操作
	eth0	192.168.5.134			确定取消		Ethernet	管理/业务口	设置 编辑
	eth1	192.168.6.134	255.255.255.0	3c:ec:ef:94:49:73			Ethernet	管理/业务口	设置 编辑
	eth2	192.168.8.134	255.255.255.0	3c:ec:ef:94:49:74			Ethernet	业务口	设置 编辑
	eth3	192.168.10.134	255.255.255.0	3c:ec:ef:94:49:75			Ethernet	业务口	设置编辑

## 3.4.3.2 Bond 配置

点击【网络管理】,点击【Bond 配置】进入到 Bond 配置页面。

<b>ジ</b> 密码设备管闭	理系统							sysAdmin ~
系统导航		Bond名称 语输入Bond名称						
设备导航								
服务配置		L ACHE IN BASS IN BRATER						
设备授权		1.1008 U.ADVC C.BOAPIN						
网络管理		Bond名称	Bond授氏	概定端口	IP地址	子网推码	阅关	操作
网络配用								
Bondicar								
致由研究								
双机热备								
D-1P-JAC-302					1 1 9			
设备状态	~				帽无数据			
设备运维	Ŷ							
设备重置	×							
设备更新								

#### 3.4.3.2.1 新增

点击【新增】,在弹出的对话框中选择 Bond 模式、子网掩码,输入 IPV4 地址、网关、 使用网口,点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

Bond名称 请输入Bond名称 Q	新增Bond配置	
	Bond模式 主备模式 > IPV4地址 192.168.6.12	
+新編 自 勤除 () 重屈网络	子网编码 255 255 255 0 网关 192 168.6.1	
Bond 答称	使用网口 _ eth0 _ eth1 g eth2 g eth3 网络码 月关	操作
	授示:Bond鄉式每交換印區起限則	
	<b>确</b> :定 取 消	

#### 3.4.3.2.2 编辑

点击【编辑】,在弹出的对话框中可修改 Bond 模式、IPV4 地址、子网掩码、网关、使用网口,点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

Bond答称 bond0 S	修改Bond配置 ×	
	Bond模式 主备模式 ~ IPV4地址 192.168.6.12	
+新聞 自動会 ② 聖忠网络	子网挽码 255 255 255 0 网关 192.168.6.1	
Bond名称	Bond名称 bond0 网络时 网络	操作
bond0	使用网口 eth0 bond0 eth1 55 255.0 192 168.6.1	之编辑 自動除
	携示: Eond類式与交換机匹配規则 能動物機模式→-分類物酸脂酸合 王登模式 (>-3級特別能置 中諸模式 (>->->線酸脂酸合 (>->	※ 1 》 前往 1 页

## 3.4.3.3 路由配置

点击【网络管理】,点击【路由配置】进入到路由配置页面。

BBP852/RB = 102.063.2024	使用用口 自由小田田口	<u>○ 189</u> ○ 世話	
+ 912 0 209 o 2093			0.0
上一颗地址	下一簇地址	使用编口	證作
	· · · · · · · · · · · · · · · · · · ·		

#### 3.4.3.3.1 新增

点击【新增】,在弹出的对话框中输入上一条地址、下一条地址、使用网口,点击【确 定】。注意每个的格式都要填写正确。点击重启后生效。

上一部地址 新版入上一部地址 下一部地址	新增路由配置		×	
	上一就地址 19:	192.168.6.10		
	下一跳地址 19.	192.168.7.213		• •
上一院地址	使用网口 〇 el	eth0 obond0 virbr0 eth1 bond1 eth2 eth3		Binci Shri
/usr/bin/bash:				2.編載 ②動味
		确定	取消	共1条 10条页 -> 前在 1 页

#### 3.4.3.3.2 编辑

点击【编辑】,在弹出的对话框中可修改 Bond 模式、IPV4 地址、子网掩码、网关、使 用网口,点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

上一新地址 通過入上一部地址	下一新地址 書記	修改路由配置				×			
		上一熟地址	192.168.7.230						
+ \$42 3 Bit 0 E276		下一跳地止	192.168.6.34						
上一预地址		使用网口	eth0 bond0 eth2 eth3	virbr0 et	h1 🔘 bond1		制编口	操作	
/usr/bin/bash:								2. 编辑 自動時	
					确定	取消		共1条 10級(页 ~ < 1 > 前往 1	Ø

#### 3.4.3.4 双机热备

点击【网络管理】,点击【双击热备】进入到双击热备页面。

28	86458	\$1084 Internet	虚料地址 100人の1000	0.228 0.225			
+ 848		o activant					۵ ۵
	88	出版图d	虚穷地址	क्षम	MERIC	主机省机地址	89
				<b>裕元</b> 政語			

#### 3.4.3.4.1 新增

点击【新增】,在弹出的对话框中输入虚拟组 id、虚拟地址、绑定模式、绑定网口、主 机地址,点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

各称 西德入名称	新增双机热备				×	2 里音		
	名称	test	虚拟组ld	12				
	虚拟地址	192.168.6.23	绑定模式	请选择绑定模式				
名称	绑定网口	eth0 obond0	eth1			定网口	主机器机地址	操作
C zjx						eth2	192.168.6.74	之编辑 回删除
Zjx001				确定	取消		8.9.8.9	之编辑 自動除

#### 3.4.3.4.2 编辑

点击【编辑】,在弹出的对话框中可修改虚拟组 id、虚拟地址、绑定模式、绑定网口、 主机地址,点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

<b>名称</b> 请输入名称	编辑 * *	
	名称 zpi001 虚拟组d 8.8.8.8	
+ 新編 合 勤快 @ 开启双机热量提择 ◎ 5	虚拟地址 192.168.6.11 柳定模式 1 ·	
名称	主机地址 192.168.6.12 定期日 主机滑机地址	操作
zjx	報定网口eth2	<b>之編載</b> 白服除
□ z x001	8.9.8.9	么编辑 自動除
	<b>100</b> 122 - 110 -	

## 3.4.4 时间配置

#### 3.4.4.1 系统时间配置

点击【时间配置】,点击【系统时间配置】进入到系统时间配置页面,可以设置当前系

统时间,同步时间服务器上的时间,保证系统时间的精准性。勾选仅同步时间,则时间必须 填写。勾选同步时区与时间,则必须填写时区、日期、时间。同步间隔和最大调整时间都得 填写,保存配置后,系统时间每相隔指定时间将从 time.windows.com 时间服务器上同步一 次。

系统时间配置	置 2023-03-02 20:02:12:	.934 点击刷新						
与本地时间同步:	<ul> <li>仅同步时间</li> <li>同步</li> <li>时间:</li> <li>(0) 法选择时间</li> </ul>	附区与时间						
启用NTP:								
	服务	5器名称	1	P/域名		端口	首选服	服务器
	sei	rver 0	192.168.6.134		13559			
同步间隔	300 🕸 (1-360	i00)秒,缺省值: 300,系统与NTP服务	器同步的间隔时间。					
最大调整时间	3600 😢 (1-360	00)秒,缺省值:10,0标识没有时间限	),					
_	_							

#### 保存配置

## 3.4.5 设备状态

设备状态包括【自检状态】和【运行状态】。

#### 3.4.5.1 自检状态

点击【设备状态】,点击【自检状态】进入到自检状态页面。

REPARTINES:     REPARTINES:     REPARTINES:       REFERENCE:     REFERENCE:     REFERENCE:       REFERENCE:     REFERENCE:     REFERENCE:	检状态		
EURODERAARIikkii EURODERAARIikkii IV ARTARODIIKA: MIAARIAARIIKKII IV IIIIAKA	程序完整性检测:	程序完整性自检递过	947
BREZENSBORINGER: BREZENSBORBECZ POT	图明和取取完整性检测:	密明和政策完整性自检通过	847
Radan Radada Pr	制机数间期检测:	赫机政论测施过	847
	算法检测:	算法由检通过	947

程序完整性检测:检查程序完整性,防止程序中途被篡改,开机会检测,也 可手动执行检测。

密钥和数据完整性检测:检测密钥和数据的完整性,防止数据和密钥中途被 篡改,开机会检测,也可手动执行检测。 随机数周期检测、算法检测:随机数周期自检检查加密机系统随机数生成机制正常;算法自检检查加密机系统的算法是否正常。

#### 3.4.5.2 运行状态

点击【设备状态】,点击【运行状态】进入到运行状态页面。

设备运行状态			
设备状态:	就绪状态		
服务运行状态:	已启动	启动 停止	
SNMP状态:	已开启	启动停止	
SSH状态:	已开启	启动停止	
重启服务器:	· <u> </u>	重启	
关闭服务器:	s <u></u> 2	关闭	

运行状态包括服务状态和关机重启。点击服务状态的【启动】或者【停止】 按钮,则会手动开启或者关闭服务。重启表示重新启动综合安全网关服务器,关 闭则关闭系统。

#### 设备运行状态



## 3.4.6 设备运维

设备运维包括【运维管理】【SSH 功能】功能。

#### 3.4.6.1 运维管理

输入地址,点击【连接】。若中断连接,点击【停止】。

Ping管理		
DNS查询	清输入内容	激活 停止
Ping	192.168.6.74	湖武 停止
Traceroute	请输入内容	湖近 终止
Telent	请输入内容	潮波停止
PING 192.168.6 64 bytes from 64 bytes from 64 bytes from 64 bytes from	.74 (192.168.6.74) 56(84) bytes of data. 192.168.6.74: icmp_seq=1 ttl=64 time=0.283 ms 192.168.6.74: icmp_seq=2 ttl=64 time=0.335 ms 192.168.6.74: icmp_seq=3 ttl=64 time=0.318 ms 192.168.6.74: icmp_seq=4 ttl=64 time=0.398 ms	

#### 3.4.6.2 SSH 功能

点击【设备运维】,点击【SSH功能】进入到运维管理页面。 输入主机名、端口、用户名、密码,点击【连接】。注意端口号要输入正确。



#### 3.4.7 设备重置

设备重置包括【密码卡初始化】【恢复出厂设置】功能。

#### 3.4.7.1 密码卡初始化

如果确认初始化,则点击"初始化密码卡"按钮,初始化功能不可逆,请谨 慎处理。注意初始化会将全部密钥和密码卡用户信息清空。

密码卡初始化	
	您确定初始化密码卡吗? • 读集作考全编员所有信息,请谨慎处理

#### 3.4.7.2 恢复出厂设置

恢复出厂设置是将系统配置信息、网络配置信息、密码卡信息等所有配置将 还原到初始化状态。注意恢复出厂设置会将整个系统重置,请谨慎操作。

恢复出厂设置

您确定恢复出厂设置吗? ●恢复出厂设置会将设备配置信息、网络配置信息、白名单配置信息、密码卡配置信息等所有配置还原列初始状态	
确定	

## 3.4.8 设备更新

点击【设备更新】进入到设备更新界面。

€ ™ V1.0.0			在线升级 2016年8月1日7月8日-1885 2017月日 并日前日第	离线升级 第52月第459年688月79年 35月第48555		
开握他名称	文件大小	版本	发布的词	STAN	升级振送	Bn
zaSecUp CardAccessControl zip	643.00B		2023-04-14 10:13:39		他的中权限	RR UR
2222 txt	380.00B		2023-03-31 10:06:18		1111	开接 國國
2222 bit	380.00B		2023-03-31 10:06:18		01111 2	开设。通照
2222.txt	380.00B		2023-03-31 10:06:18		1111	开设 道西
2222.txt	380.00B		2023-03-31 10:06:18		81111	9402 LBIR
2222. bit	380.00B		2023-03-31 10:06:18		1111	118 all
2222 tot	380.00B		2023-03-31 10:06:18		1111	7492 UBIT
enc	716.00B		2023-03-30 17:21:13		11111111111111111111111111122222222	开级 追加
zaykpack3.zip	32.54KB	V1.1.0	2023-03-02 10:55:12		1	开设 道田
zaykpack3.zip	32.54KB	V1.1.0	2023-03-02 10:56:12		4	开绕: 追問

#### 3.4.8.1 离线升级

点击【选择离线包】,然后上传安装包,输入升级描述,点击【升级】。注意升级的版本 号会从离线包里面获取。

V3.	● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	上传升级文件		<b>在由上作</b>	X		<b>离线升级</b> 通过上标电线安装加出行升级 选择电缆包	
		11 (T +97) L	zaykpack3.zip					
升级包名称	文件大小	开级曲述	测试升级			安装时间	升级描述	操作
zaykpack3.zip	32.54KB						1	升级 還回
zaykpack3.zip	32.54KB			确定	取消		i -	升级 退回
zaykpack3.zip	32.54KB		V1.2.2	2023-03-02 10:55:12			1	升级 透回
zaykpack3.zip	32.54KB		V1.2.2	2023-03-02 10:55:12			1	升级 退回
zaykpack3.zip	32.54KB		V1.2.2	2023-03-02 10:55:12			1	升级 退回
zaykpack3.zip	32.54KB		V1.2.2	2023-03-02 10:55:10			t.	升级 週回

#### 3.5 安全管理员用户

以安全管理员身份登陆 WEB 管理系统,该管理员用户支持密钥管理、证书管理、隧道服务、用户信息管理、资源管理、网关-客户端模式、系统备份与恢复等配置功能。

VPN 支持隧道代理和客户端两种模式建立 SSL 隧道,使用这两种模式时,需要在安全管理员下进行相关的配置。

1) VPN 服务器证书配置

●依次打开证书管理→设备证书菜单,点击"生成 P10"按钮生成签名 P10 证书请求,然后使用该证书请求到 CA 中心签发证书。
●CA 中心成功下发证书后,根据以下步骤将证书导入到 VPN 设备中。

依次打开证书管理->设备证书菜单,首先,点击"导入根证"按钮,导入 CA 证书对应的跟证书链。然后,点击"导入设备证书"按钮,导入设备证书。

2) 隧道代理模式

点击菜单栏的隧道服务功能菜单,进入隧道服务配置界面,根 据界面提示添加隧道代理。

添加成功后,可以使用国密浏览器或国密安全传输中间件,通 过该隧道以安全的方式访问被代理的应用资源。

3) VPN 客户端模式

●账号方式拨号登陆

首先,修改客户端认证方式为"账号密码"认证。

依次打开"网关-客户端模式->配置网关"功能菜单,点击编辑按 钮,认证方式选择"账号密码",并根据操作手册说明配置允许用户 访问的内网网段信息,确定后保存并重启服务;

然后,新建用户信息。

依次打开"用户信息管理->用户管理"功能菜单,根据操作手册 说明新建用户。建立用户成功后,使用新建的用户信进行登陆。登陆 后接口访问内网资源。

●账号方式拨号登陆

首先,修改客户端认证方式为"数字证书"认证。

依次打开"网关-客户端模式->配置网关"功能菜单,点击编辑按 钮,认证方式选择"数字证书",并根据操作手册说明配置允许用户 访问的内网网段信息,确定后保存并重启服务;

然后通过 VPN 客户端使用 ukey 进行拨号登陆。

详细配置说明,请参考以下功能配置说明。

## 3.5.1 密钥管理

#### 3.5.1.1 SM2 密钥管理

点击【密钥管理】,点击【SM2 密钥管理】进入 SM2 密钥管理页面。

密钥索引 1940人工的	密切用注 的现在分词			
+ 生成表明 2 日				0 0
	<b>密明</b> 隶引	Sturilie	激明模长	證件
	1	結合進調	256	0.000 2.000 2.00000000 2.0002240
	1	scretered	256	0.80% <b>《現</b> 新 ————————————————————————————————————
	2	製合計明	256	合制制 化氯新 之法问题制品 之称出公明
	2	sureneering	256	白粉味 上班新
	3	52,45 WHI	256	合植物 之道斯 之边问题物质 之界出公明
	3	toreentil	256	0.88% <b>《</b> 現新 ———— 《明出公明
	4	<b>新合用的</b>	256	自動物 龙顶新 龙动网络动物 龙导出公明
	4	52454648	256	0.894 2.895 2.94550
	5	語合書明	256	合動物 点面新 点讷问验制品 点导出公明
	5	scretered (	256	回翻除 龙斑新 ———————————————————————————————————
			共5000条 10銀/页 - <	1 2 3 4 5 6 500 > 前往 1 页

#### 3.5.1.1.1 生成密钥

密钥标签内可输入密钥索引,密钥用途可选择签名密钥/加密密钥/签名和加密密钥,密钥模长 256,点击【生成密钥对】按钮完成指定密钥的生成并安全保存。

2020) assumed 20982 assesses	生成密明		
	1899年31 * 注: 前初表3//范围(1-2500)支持输入1.3版5-12版单个密钥 * 密明用金 签名密明 ~		
Serves .		證明劇长	操作
(B) #	确定 取消	256	Q BBB 之道所 之外问题和新 之母出公明
ia i		256	0809 J.R.M J.Burra
2	医分布的	256	CHM LINE LOCATES LALIN

#### 3.5.1.1.2 导入加密密钥

点击【导入加密密钥】,输入密钥索引、选择密钥格式类型、选择文件,点击【确定】。 注意证书要上传正确。

<b>密钥索引</b> 一 法能入密钥索	密明用途 签名密明	导入密钥		×			
		*密钥索引	2				
+ 生成素明 (1) 号入)	10 <b>1111111</b>	* 密钥格式类型	GM/T 0010				
	密明索引	导入密钥			生命周期起始时间	生命周期结束时间	操作
	4.		•		2023-02-01 00:02:00	2023-02-28 00:02:00	合觀除 之更新 之讷问控制码 之等出公明
	1		点击上传		2023-02-01 00:02:00	2023-02-28 00:02:00	○删除 《 更新 ──── 《 母出公明
	2		∋ iữ‡cer	J			自動除 心里新 之讷问控制码 心界出公明
	2		The factory				白銅除 人更新 人居出公明
	3		W.S.	10%			自動除 之更新 之讷问故制码 之母出公钥
	3	加密密制	0				②删除 之更新 ────
	4	签名密码	0				自動時 之夏新 之讷问战制码 之导出公明
0	4	加密被明	0				回删除 《 <b>更新</b> 《导出公明
	5	签名密制	0				自動時 之裏新 之讷问控制码 之导出公明
, <b>D</b> ,	5	ACHEREN	0				直删除 之関新
					共 5000 祭 10祭/页 ~	< 1 2 3 4	5 6 500 > 前往 1 页

#### 3.5.1.1.3 更新

点击【更新】,在弹出的对话框中选择密钥模长,点击【确定】,修改用户对应的用户密 钥模长。

密钥索引 油罐	2人前时至31 密明用途 签名或明	→ 更新密钥		×			
		* 密钥索引					
十生成素明		*密钥用途	加密密钥 ~				
	密明索引	<b>密明</b> 密钥模长	256 ~		生命問題起始时间	生命周期结束时间	操作
	n	業部					自動除 龙更新 龙访问控制码 龙导出公明
	11	2060	确定	取消	2023-02-21 08:02:38	2023-02-21 08:02:41	白銀時 化面新 化导出公明
(C)	12	法名志明		0			自動除 龙翼新 龙访问控制码 龙导出公明
	12	208/8849		256	2023-02-21.08:02:38	2023-02-21 08:02:41	白銅鈴 龙丽新 ———— 龙易出公明
<u></u>	13	盖名密码		0			自動除 龙翼新 龙访问控制码 龙导出公明
	13	加速速制		0			自删除 <b>《画新 ————</b> 《号出公铜
<u></u>	14	签名密码		0			自動除 化更新 化访问控制码 化导出公明
	14	加速速制		256	2023-02-21 08:02:38	2023-02-21 08:02:41	白樹除 <b>《画新 ————</b> 《号出公明
<u>ģ</u>	15	盖名密码		0			自動除 化更新 化访问控制码 化导出公明
E.	15	加速速制		256	2023-02-21 08:02:38	2023-02-21 08:02:41	心删除 《画新 ———— 《号出公钥
					共5000条 10余/页 ~	< 1 2 3	4 5 6 500 > 能往 3 页

## 3.5.1.1.4 访问控制码

点击【访问控制码】,在弹出对话框中输入新口令、确认口令,点击【确认】。

	· 後期 / 设置私钥访问控制码	×		
	*密钥索引 1			
	* □令	۵		
· 参明索引	• 确认口令	0	生命周期起始时间生命周期结束时间	操作
0 1			2023-02-01 00.02.00 2023-02-28 00.02.00	白影時 点面新 之讷问检教院 之导出公明
I 1		确定 取消	2023-02-01 00:02:00 2023-02-28 00:02:00	自删除 之 <b>更新 ————————————————————————————————————</b>
2	圣书谢明	0		自動除 心更新 心访问控制器 心导出公明
2	加速電視	0		京樂除 之黃新 之号出公明
3	派名臣树	0		②影除 企業新 心访问控制码 心导出公钥
3	2086849	0		○删除 心更新 ────
	逐奏思想	0		自動除 点面新 点访问放制码 点看出公钥
. 4	108-849	0		企業時 企業新 ———————————————————————————————————
5	经名称明	0		②胞除 化更新 化访问控制器 化导出公钥
5	加密總領	0		宫撒除 之面新 之号出公钥
			共5000条 10条页 🗸 1 2 3 4	5 6 500 > 前往 1 页

#### 3.5.1.2 RSA 密钥管理

点击【密钥管理】,点击【RSA 密钥管理】进入 RSA 密钥管理页面。

密明教计	密明用途			
+ 1:088	D nimedamos			(a) (a
	密钥索引	波·N9FBah	激明微长	證作
	1	20-42 (West)	2048	日前時 点 肥料 点 达的现在分词
	1	2018年8月	2048	日期時 《 第55
	2	基本审判	2048	白田市 化原料 化初间检验器
	2	100000	2048	CE08 4.055
	3	篮衣荷则	2048	回動時 企業時 企动问题制度
	3	10008859	2048	EBM 4.855
	4	族自由明	2048	白田時 之東新 之功可能制度
	4	20/82/89/83	2048	0899 4.895
	5	新品質型	2048	日日100 点 第15 点 边内社市555
	5	加高可能	2048	E899 2.85
			共400条 10衡/页 - < 1	2 3 4 5 6 40 > 前往 1 页

#### 3.5.1.2.1 生成密钥

密钥标签内可输入密钥密钥索引,密钥用途可选择签名密钥/加 密密钥/签名和加密密钥,密钥模长1024,2048,设置生命周期(默 认生效时间为当前),配置完成后点击【确定】按钮完成指定密钥的 生成并安全保存。

NRASI (max-enter	straniaa	生成密钥	×		
( see ) ( see of		- 00093491 1 建: 1024102048世纪第二十/短期(1-100) 30725,409 /22期(101-200)支付给入1,305-1230年个世初 * 密明用建 签款密明	(王句太子) 9 ~		
10	雷明森引			Respective.	1819
-	A.	* 肥明欄长 1024	× .	2048	CBN 4.84 2003098
[24]	1			2048	1800 4.815
0	2	97 JA	8.75	2648	DARK LINE LINES
εï.	2.	200000		2048	CBN 2.86
<i>a</i> ;	<u>a</u> .	a areas		2048	DBR LBR LOODEN
61	<b>3</b>	200000		2648	2809 ABD
13	4:	能将南明		2048	白田時 之間時 之功可能制印
0	4	(Same)		2648	180 4.85
<u>ev</u>	5	15 ALMAN		2048	OBN ARE ANOTHER
- E1(	6	STRIMM		2048	080 ARE
				并400 统 10 新/页 - 1 2	3 4 5 6 40 3 mile 1 51

#### 3.5.1.2.2 更新

点击【更新】,在弹出的对话框中选择密钥模长,点击【确定】,修改用户对应的密钥模

长。

<b>密明索引</b> 請編入密钥索引		更新密钥		×				
		*密钥索引						
+ 1486 2 ROBHER		*密钥用途	签名密钥 >>					
- 21	用漱引	· 密钥模长	2048 ^		生命。	明期起始时间	生命周期结束时间	樱作
	11	3	1024					自動除 化画新 之访问控制码
	11	2	2048	12 取消				自動除 心里新
	12	签名密码		2048				自動除 之更新 之访问控制码
	12	加速电机		2048				回激除 <b>企画新</b>
	13	签名密明		0				自動除 《更新 之访问控制码
	13	加速期间		0				回勤除 <b>《</b> 更新
	14.	签名密码		0				自動除 么重新 之访问控制码
	14	20353816		0				回服除 化更新
	15	签名密码		0				自動除 必要新 之访问按照码
	15	加密密制		0				②激除 化氟新
					共 400 条	10条/页 🗸	( 1 2 3 4 5	6 40 > 前往 3 页

## 3.5.1.2.3 访问控制码

点击【访问控制码】,在弹出对话框中输入新口令、确认口令,点击【确认】。

密钥索引	新新入業的新計 <b>空切用注</b>	· · · · · · · · · · · · · · · · · · ·	回控制码	×			
		*密明索引	12				
+ 生成密码		*□\$-	*****	•			
12	密明索引	遭 • 确认口令		•	生命周期起始时间	生命周期结束时间	操作
	11	2					自制除 龙黄新 龙动间控制码
(i)	11	21	确定	取消			①謝除 之面新
0	12	签合审制	2048				自制除 龙麗新 之词问控制码
	12	108-209	2048				自删除 之更新
	13	经名称明	0				自制除 龙翼新 之访问控制码
	13	\$1980-8846F	0				回撤除 《更新
	14	经名数间	0				合制体 之更新 之访问拉用码
	14	\$08886	0				白樹除 <b>人面新</b>
	15	委会定制	0				合服除 之靈新 之访问控制码
	15	108-8-19	0				白銀除 之重新
					共400条 10条/页 🗸	< 1 2 3 4	5 6 40 > 載往 3 页

#### 3.5.1.3 ECC 密钥管理

点击【密钥管理】,点击【ECC密钥管理】进入 ECC密钥管理页面。

密明末引	密約用途 20000000		85	
+ <u>3 devi</u> 2 0.000				0.0
	雷阳本引	密明用油	意明朝任	<b>股</b> 作
		N PART	9 2	

#### 3.5.1.3.1 生成密钥

密钥标签内可输入密钥索引,密钥长度可选择 B-163, B-233, B-283, B-409, B-571, K-163, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521, ED25519(默认 P-256) 设置生命周期(默认生效时间为当前),配置完成后点击【确定】按钮完成指定密钥的生成并安全保存。

<b>密钥用途</b> 网络萨罗拉用途	生成密钥			×	
_	*密钥索引	1			
	注: 请输入	、密钥索引/范围,支持轴	入1,3或5-12或单个密钥号		
	* 密钥用途	签名密钥			
「索引	* 密钥模长	P-256	×		密钥模长
1					B-163
1			确定取测	ij.	P-256
2		签名密钥			P-256

#### 3.5.1.3.2 更新

点击【更新】,在弹出的对话框中选择密钥模长,点击【确定】,修改用户对应的密 钥模长。

密钥索引				×				
		*密铜索引						
+ 生成密制		注: 感明費了 単个数明号 ※照用途	I/密钥索引范围(1-100),支持输入1,3	或者5-12或者是				
	密钥索引	8			生命周	明起始时间生命	。周期结束时间	操作
	24	* 密钥模长	K-233	J	2023-02-	21 11:02:18		回動除 足質新 之讷问控制码
	25	2	B-163 B-233		2023-02-	21 11:02:18		回避時 之質新 之功可控制码
	26	2	B-283	創定 取消	2023-02-	21 11:02:43		自動除 人更新 人物间控制码
	26	加度表明	B-409 B-571	К-233	2023-02-	21 11:02:58 2023	02-21 11:02:01	回勤時 《更新
	27	经合面明	K-163	B-163	2023-02-	21 11:02:43		回到時 之面新 之讷问控制码
	27	108889	R-233	к-233	2023-02-	21 11.02.58 2023	02-21 11:02:01	①影除 2.更新
	28	蓝名密明		B-163	2023-02-	21 11:02:43		回動時 化更新 化访问控制码
	28	20年84月		К-233	2023-02-	21 11:02:58 2023	-02-21 11:02:01	○勤時 必更新
	29	经指数间		B-163	2023-02-	21 11:02:43		自制除 之更新 之访问控制码
	30	208849		K-233	2023-02-	21 11:02:58 2023	-02-21 11:02:01	①勤除 之面折
							共 10 祭	10条页 前往 1 页

## 3.5.1.3.3 访问控制码

点击【访问控制码】,在弹出对话框中输入新口令、确认口令,点击【确认】。

密钥索引 词称入家	899A	<ul> <li>金融新聞</li> <li>27</li> <li>27</li> </ul>	到码	×		
十生成密码		*00	••• ©			
	密钥索引	a · 确认口令 ····	••	生命周期起始时间	生命周期结束时间	操作
	24	8		2023-02-21 11:02:18		口服除 化离新 人讷问控制码
	25	a.	确定 取消	消 2023-02-21 11:02:18		回日期 化更新 化液用控制器
	26	蓝石面积	B-163	2023-02-21 11:02:43		回顧時 企業新 之功问控制码
0	26	104Martin	K-233	2023-02-21 11:02:58	2023-02-21 11:02:01	自動除 2.更新
	27	圣名歌明	B-163	2023-02-21 11:02:43		自動除 之更新 之访问控制码
	27	加密密码	K-233	2023-02-21 11:02:58	2023-02-21 11:02:01	②删除 之面新
	28	签名图码	B-163	2023-02-21 11:02:43		自制除 《萧新 《波列绘制码
	28	加密密制	K-233	2023-02-21 11:02:58	2023-02-21 11:02:01	②删除 《更新
	29	签名密制	B-163	2023-02-21 11:02:43		自動時 名夏新 名访问控制码
	30	20878819	K-233	2023-02-21 11:02:58	2023-02-21 11:02:01	回翻除 《東新
					共 10 条	10条页 🗸 🚺 🔰 齡往 1 页

## 3.5.2 证书管理

#### 3.5.2.1 设备证书

依次点击菜单栏的证书管理-> 设备证书,进入设备证书页面,如 下图所示:

证书类型	所有		• 密钥类型	型 所有		¥		搜索	重置	
	4-204		+D/T	R) Martin	1					
	±200P10			寻入设置证书	and to an	18 14	1			
业书DN	业书主然时间	业书天众时间	业书英型	出明英型	密钥衣度	媒作 详情 删除				

1) 自签证书

点击自签证书按钮,弹出如下页面,依次添加根证以及设备证书, 提示操作成功后表示添加成功,否则添加失败。

上级根证:	请选择上级根	īΕ			v	
*名称(CN)			部门(OU1)			
部门(OU2)			组织(O)			
省份(ST)			市(L)			
证书生效时间	]:		证书失效时间:			
密钥类型:	SM2	•	密钥长度:	256	۲	
	(	保存		关闭		

2) 生成 P10 证书请求

其主要功能为生成 PKCS10 证书请求。在界面中输入证书的主题信息并选择所用密钥 后,点击【生成证书请求】按钮即可生成 PKCS10 格式的证书请求。证书请求的文件内容显示在 PKCS10 文 本框中。管理员可以保存 PKCS10 后,去证书机构申请证书,然后导入到签名验签服务器中。

	SM2	-		
"密钥类型"	SIVIZ		出出了	
*名称(CN)			部门(OU1)	
部门(OU2)			组织(O)	
省份(ST)			市(L)	

4) 导入根证书

点击"导入根证"按钮,弹出导入根证书对话框,选择需要导入的根证书后,点击"导入",提示操作成功,导入成功,否则导入失败。

_		
删除		
	制除	

6) 导入设备证书

点击导入设备证书,弹出导入设备证书对话框,如下图所示,选 择证书类型,密钥号,签名证书,加密证书,加密私钥,点击导入, 提示操作成功,导入成功,否则导入失败。

证书类型:	● SM2证书 〇	RSA证书	
*密钥号:	1		¥
*签名证书:	请选择证书文件	( >>选择 )	
*加密证书:	请选择证书文件	( >>选择 )	
*加密私钥:	[ >>ì	选择并导入	
		关闭	

#### 3.5.2.2 证书吊销列表

依次点击菜单栏的证书管理→ CRL 管理, 进入证书吊销列表页面, 如下图所示:

CRL管理

+添加	批量删除					
□全选	CRL名称	CRL地址	更新频率	更新时间	下次更新时间	操作
□全选	aa	/home/xx.crl				编辑 详情 删除
□全选	bb	https://www				编辑(详情)  删除

1) 添加证书吊销信息

点击添加按钮,弹出添加证书吊销列表对话框:

选择添加本地文件,如下图所示,输入 CRL 名称,以及 CRL 文件, 点击确定按钮,提示操作成功,证明添加成功,否则添加失败。

CRL管理		添加证书吊	睄列表			1		
+添加	批量	配置方式:	◉ 添加本地文件	○ 配置在线	起更新			
□全选	CRL名称						操作	
□全选	aa	CRL名称:				编辑	详情	删除
□全选	bb	CRL文件:	支持文件拖入	l	浏览	编辑	详情	删除
					ſ			
			「備定」					

选择配置在线更新,如下图所示,依次输入相关信息后,点击确定 按钮。

置方式: 〇	)添加本	地文件	● 配置	在线更	颕
			200		
启用:		用目动更想	新CRL		
CRL名称:					10111111000-216.02
硕发点地址:					立即更新
更新频率:	<ul> <li>crl扔</li> </ul>	←展项中核	示记时间自	目动更新	Ť
	〇毎	分钟	自动更新	沂	
	~=	星期- •	21:00	•	
	〇母[				切史新

2) 编辑吊销证书信息

点击编辑按钮,可以修改 CRL 名称及 CRL 文件,或在线更新相关 信息。修改完成后,点击确定按钮,进行数据保存,提示操作成功, 证明修改成功,否则修改失败。

3) 删除吊销证书信息

点击删除按钮,弹出提示框后点击确认,提示操作成功,则删除 成功,否则删除失败。

#### 3.5.3 隧道服务

点击菜单栏的隧道服务菜单,如下图所示,进入隧道服务配置界 面:

隧道名称	请输入隧道名称	<b>监听端口</b> 读输入监听闭口	(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)				
+ 新聞	白 新除 区 修改						
	隧道名称	隧道类型	证书名称	监听端口	协议	服务节点	操作
	111	HTTP服务	使用本设备出厂默认X.509证书	0	TLSv1.1	192.168.6.1:0	删除 编辑 URL访问控制
						共1条 20条/页 V	1 > 前往 1 页

1) 新建隧道服务

点击新建按钮,弹出新建隧道服务对话框,如下图所示,包括基本配置,高级配置,其它配置三个配置标签页。其中高级配置,其它 配置项的内容为非必输项,根据具体需要选择使用。

基本配置:

●服务名称: 该隧道代理的别名, 一般用于说明该隧道代理的功

能。

●监听端口: 该隧道代理使用的端口号, 配置隧道后, 使用 VPN 设备地址+监听端口进行方式;

●通道类型:支持国密和国际两种通道类型;

●协议类型:通道类型为国密时,支持国密 SSL 协议;通道类型为国际时,支持国际 TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3 协议版本;

●国密/国际证书: VPN 设备证书;

●握手策略:支持单向认证,双向认证,单/双向自适应;

●用户根证:双向认证时,该项必填,为客户端证书的根证;

●服务节点:被代理的后端应用服务信息,存在多条时,可实现 后端应用的负载均衡;

447.0 / A A.				
▲ 価信息				
*服务名称	测试服务	*监听端口	- 1900	)1 +
* 22	Trate	1-th -th -th -th -th		
通道交型	道路	以名地址	请 制入 财	
*协议类型	国家密码管理局SSL协议标	示准v1.1 (GM/T 0024-2014)		~
国密证书	使用本设备出厂默认X.509	证书		~
*握手策略	等级0 - 不认证对端证书	~ 用户根证	© 点击配置用户	根证书
*隧道类型	9 HTTP服务 〇 TCF	服务 OFTP服务	<ul> <li>UDP服务</li> </ul>	
服务节点				
服务地址	服务端口	权重		操作
192 168 6 113	9000	+ - 1	+	(+)

高级配置:

确定

取消

新建隧道服务	×
基础配置 高级配置 其他配置	
I HTTP服务高级配置	
证书信息透传到应用 开启在线证书状态验 (OCSP) 开启内容提换	
● 负载均衡策略配置	
IP_HASH 是否启用根据源地址引导流量	
重试次数     -     5     +     超时时间(秒)     -     20     +	
【代理客户端证书配置	
证书配置 注: 被代理服务器使用双向认证时, 需开启此项	
确定取》	ľ
其它配置:	
新建隧道服务	×
基础配置 高级配置 其他配置	
连接超时时间(秒) - 30 +	
开启防DDOS攻击 开启防sweet32攻击) 开启防host头部攻击	

## 3.5.4 用户信息管理

依次打开用户信息管理->用户管理菜单,进入用户管理操作页面, 如下图所示:

用户名	请输入用户名 用户状态 前近	探状态 > 0 放気 2 聖雪			
+ 新増	∠ 排政 自動除 全导入 主导3	★ 导出所有 ↓ 下號模板			
	用户名	所屬组	状态	备注	操作
	hello	中安云科,测试,的	蒙用	事实上	编辑 删除重量宽码

#### 3.5.4.1 用户组管理

1)新建用户分组

点击"新建"按钮,弹出新建对话框,如下图所示,选择新建用 户组。根据页面提示,依次输入用户组相关信息,点击保存后退出。

选择类型	● 新建用户组 ○ 新	建用户			
建用户组					
分组名称	请输入分组名称		分组描述	请输入分组描述	
分组状态	请选择状态	~	辅助认证方式	请选择辅助认证方式	Ŷ
关联资源	<ul> <li>Θ 关联资源     <li>⊡</li> </li></ul>	新建并选择资源	组		

## 3.5.4.2 用户管理

1) 新建用户

点击"新建"按钮,弹出新建对话框,如下图所示,选择新建用 户。根据页面提示,依次输入用户基本属性信息,根据需要配置高级 属性信息,点击保存后退出。

新增 ▲ 新建类型		
选择类型 〇 新	新建用户组 💿 新建用户	
基本属性配置	高级配置	
用户名称	TestUser	用户密码默认是vpn@1234
用户描述	测试用户	
所属分组	◎ 关联用户组	
有效期	<sub>③</sub> 2023-04-23 ( <u></u> <b>至</b> 2023-05-31 (	
用户状态	● 启用 ○ 禁用	



确定

取消

选择类型 〇 身	新建用户组 💿	健用户	
配置			
基本属性配置	高级配置		
登录过期时长	0	时	说明:设置登录超过xx小时,需重新登录。默认值为0表示不启用 该功能
闲置禁用时长	0	月	说明:设置距离账号末次使用闲置时长,需重新启用。默认值为0 表示不启用该功能
客户端策略	无	~	
*客户端黑名单			
时间访问控制	⑤ 2023-04-23 ( 至	2023-05-31 (	说明:设置用户可访问的时间段。默认为全时段
	<b></b>	-	

3) 编辑用户信息

如下图所示,在用户列表中选择需要编辑的用户,点击编辑按钮,可修改用户的基本属性信息和高级属性信息,修改完成点击保存。

置		 		
基本属性配置	高级配置			
用户名称	TestUser			
用户描述	测试用户修改功能			
所属分组	© 关联用户组			
有效期	⑤ 2023-04-11 ( <u></u> 2023-05-17 (			
用户状态	● 启用 ○ 禁用			
			确定	耶

#### 3.5.4.3 特征码管理

依次打开用户信息管理->特征码管理菜单,进入特征码管理页面, 如下图所示:

名称	请输入名称	计算机名 计算机名	MAC地址	诺输入MAC地址	<b>审批状态</b> 请选择审批状态	~ <b>a</b>	被茶 ○ 重量	
+ 新増	自動給日日市批	▲ 导入 ★ 导出用户组 ★ 下载导入模板						
	名称	分组	计算机名	MAC地址	特征码		审批状态	操作
	hello	中安云科,测试,的		192.168.7.112			已审批	驳回 审批 修改 删除
	hello	中安云料,测试,的	555	555			已审批	驳回 审批 修改 删除

#### 1) 添加硬件特征码

点击添加按钮,弹出"添加硬件特征码"对话框,如下图所示, 根据页面提示,选择用户名,输入计算机名、MAC地址、硬件特征码 等信息后,点击审批按钮。

* 用户名	hello	⑧ * MAC地均	上 请输入MAC地址
*硬件特征码	请输入硬件特征码	备注	E 请输入备注
状态	○ 已审批 ○ 未审批 (		
状态	○ 已审批 ○ 未审批 (	〇 己驳回	

2) 导入硬件特征码

点击导入按钮,弹出导入硬件特征码对话框,如下图所示。根据 界面提示,依次选择硬件特征码信息文件等信息后,点击保存。

	名称	请输入名称	导入硬件特征码	×	C地址				
8	审批状态	请选择审批状态							
	+ 新増		将文件拖到此处,或点击上传						
		名称	是否更新已经存在硬件特征码		特征码	审批状态		操作	
		hello	确定	取消		已审批	驳回 审	批修改	删除
		hello	Hise Zaret, 2010 000 000			已审批	驳回 审	批 修改	删除
8									

3) 导出硬件特征码

点击导出按钮, 弹出导出硬件特征码对话框, 如下图所示。根据 界面提示,选择需要导出的特征码信息后,点击保存。

#### 3.5.4.4 认证管理

依次打开用户信息管理->认证管理菜单,进入认证管理页面,如 下图所示:

认证管理
硬件特征码认证 设置 *用于设置硬件特征码认证审批方式,每个用户最大支持的特征码数量等

1) 硬件特征码认证配置

点击硬件特征码认证的设置功能按钮,弹出特征码认证设置对话 框,如下图所示,可设置硬件特征码认证的审批方式,每个用户允许 使用的特征码数量。

计正答理	特征码认证设置	×	
以따冒连	*特征码审批方式 💿 自动审批	○ 手动审批	
硬件特征码认证	* 用户特征码数量 5		
*用于设置硬件特征码			<u>.</u>
		确定 取消	

×

## 3.5.5 资源管理

#### 3.5.5.1 资源配置

依次点击菜单栏的资源管理->资源配置功能,进入资源配置页面, 如下图所示:

资源名称	请选择资源名称 >	资源类型	请选择资源关型 > 资源地址	请编入资源地址 Q 推获	の重要	
+ 新聞						
	资源名称		资源类型	资源地址	资源端口	操作
	资源新增		基础密码服务	192.168.6.74	资源新增	编辑 删除
					共1条	10条页 🗸 🤇 1 🔿 前往 1 页

1) 新增资源配置

点击"新增"按钮,打开新建资源对话框,如下图所示: 新建资源

*资源名称	请输入业务系统代理	服务类型	请选择服务类型
*资源地址	192.168.1.1	*资源端口	15001
url路径	1		

根据界面提示依次输入相关要素,点击确定后保存。

2) 修改资源配置

选择需要修改的资源,点击"编辑"按钮,打开修改资源对话框,如下图所示:

资源名称		修改资源				×		
+ 新増	C 899	* 资源名称	资源新增	服务类型	基础密码服务	~		
18	资源名称	* 资源地址	192.168.6.74	* 资源端口	11008		资源端口	操作
	资源新增	url踏径					资源新增	ing Bir
							共1条 10条/页	1 ->
					确定	取消		

根据界面提示,修改对应的信息后,点击确定后保存。

#### 3.5.5.1 资源组管理

依次点击菜单栏的资源管理->资源配置功能,进入资源配置页面, 如下图所示:

资源名称	请选择资源名称	∨ 資源类型	请选择资源类型	~ 资源组	请选择资源组 ~	用户组 请选择用户组	∨ Q 搬室	調査の	
+ 新増資	<b>逻辑</b> 《 编载资源组	<b>由 期</b> 除资源组							
	资源名称		资源类型	地址	E Pris	[资源组	授权给	资源状态	描述
	资源新增		HTTPS应用		测试	资源组			

## 3.5.5.1.1 新增资源组

点击"新增资源组"按钮,打开新建资源组对话框,如下图所示:

×

资源组名称	测试组	资源组描述	测试资源组	
关联用户组	@ 点击关联用户组	资源组状态	◎ 启用 ○ 停用	I
受权资源列表				

根据界面提示信息,依次输入资源组名称、资源组状态等信息,点击 关联用户组按钮,关联用户,如下图所示:

名称 请输入名称	类型	请选择资源类型	∨ 状态	请选择状态 >	Q捜索C重置
中安云科		名称	类型	状态	备注
11 A		∨ 中安云科	用户组	启用	公司
		虾米	用户	启用	描述
				-	1000
		1000			1000
				=	1000
			100		100

点击关联资源按钮,打开关联资源对话框,为该资源组关联资源,如-46-

下图所元	<b>N:</b>				×
大联贷源	请输入名称	<b>类型</b> 请选择资源类型 >>	Q 搜索 0 重雪		
	名称	类型	地址	备注	
	资源新增	HTTPS应用	192.168.6.74:11008		
				关联资源	取消

## 相关信息输入完成后,点击确定保存,如下图所示:

资源组名称	请輸入资源组名称	资源组描述	请输入资	源组描述	
关联用户组	ⓒ 点击关联用户组	资源组状态	) 启用	○ 停用	
授权资源列表					
+ 选择资源					
资源名称	资源类型	访问地址	描述		操作

## 3.5.5.1.1 删除资源组

如下图所示,选择需要删除的资源组,点击"删除资源组"按钮,进行资源组的删除。

资源名称 请选择资源	\$A称	> 资源类型 请选择资料	○ 資源组	测试资源组	> 用户组 游选择用户组	✓ Q 撥索	2 重要	
+ 新增资源组 《	1. 编辑资源组	會 删除资源组						
资源组 测试资源组		资源名称	资源类型	地址	所属资源组	授权给	资源状态	描述
		资源新增	HTTPS应用		测试测试资源组	中安云科		
	¢							
		HTTPS应	用			测试	d.测试资源组	
		系统	提示			>	5	
			是否确认删除数	过据项?				
					取消	确定		

## 3.5.6 网关-客户端模式

#### 3.5.6.1 配置网关

依次点击菜单栏的网关-客户端模式→配置网关,进入配置网关页 面,如下图所示:

服务名称 请输入服务名称	産産 ご 教教 O					
○ 重白服务 □ 編編						
服务名称	服务端口	客户端网段	认证方式	加密方式	证书名称	操作
网关	65535	10.8.0.0	数字证书	SM2	C=CN,O=O1,CN=vpnSM2_8,OU= OU1,T=T1,ST=sd,L=jn,E=	頭環
					共1条 10晩页 ~ く 1 :	前往 1 页

#### 1) 修改网关基本配置

点击编辑按钮,弹出修改网关页面,可以修改网关名称、端口号、 认证方式、加密算法、修改证书等信息,修改完成后,点击确定按钮,

确定

取消

提示操作成功,表示修改成功,否则修改失败。

编辑

服务名称	网关		服务端口	1194	
认证方式	数字证书	۲	加密算法	SM2	~
务端证 <mark>书</mark>	C=CN,O=O1,CN=vp	nSM2_ ~	客户端根证	请选择客户端根证	×
1信息	注: VPN客户端连接时,	推送此路由信息到到	客户端,以允许客户端访	问指定的私有网络	
自信息路	注:VPN客户端连接时, 由地址/网段	推送此路由信息到路	客户端,以允许客户端切 子网掩码	5问指定的私有网络 操作	
<b>由信息</b> 路 192.100.0.0	注: VPN客户端连接时, 由地址/网段	推送此路由信息到 255.255.255	客户端,以允许客户端切 子 <b>网掩码</b> 5.0	5问指定的私有网络	+)
由信息 路 192.100.0.0	注:VPN客户端连接时, 由地址/网段	推送此路由信息到 255.255.255 255.255.255	客户端,以允许客户端订 <b>子网掩码</b> 5.0		+) +)

#### 3.5.6.2 访问记录

该功能用于查看 VPN 客户端用户的登陆信息。

依次点击菜单栏的网关-客户端模式->访问记录菜单,进入访问记录页面,如下图所示:

导出记录						
用户名称	客户端IP	客户端虚拟IP	连接时间	接收数据	发送数据	在线状态

点击导出按钮,可以将访问记录以 Excel 形式导出到本地。

#### 3.5.7 IPSEC 管理

该功能支持 IPSec 服务的策略配置,和加密隧道信息监控。

#### 3.5.7.1 策略配置

依次点击菜单栏的 IPSec 管理->策略配置功能菜单,可查看当前 配置的 IPSec 隧道信息,如下图所示:

		小田地名印		TEH 44.5	·				里且	15.4
<b>⊕</b> I	新建	<b>直</b> 删除	₹.	导入 <b>①</b> 导出	◎ 启用	停止			0	同步
1	食略名称	本地VPN地址	远程VPN地址	本地证书	远程标识	CA证书	密钥交换协议	使用状态	操作	F
	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	赵湖	sm4cbc-sm3-sm2		20182523180	5231
1	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	C=CN,O=ZAYK,CN=Root CA	sm4cbc-sm3-sm2		加密范围	1212
1	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	獣は	sm4cbc-sm3-sm2		加密范围	541
	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	默认	sm4cbc-sm3-sm2		加密范围	181
į.	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	默认	sm4cbc-sm3-sm2		加密范围	编程
	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	默认	sm4cbc-sm3-sm2		加酸氮酮	551
1 (	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	默认	sm4cbc-sm3-sm2		加密范围	19.11
	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	獣认	sm4cbc-sm3-sm2		加密线网	99.8
	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	默认	sm4cbc-sm3-sm2		加密范围	12.12
1	conn1	192.168.6.1	10.0.0.1	C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocipher,CN=Bob	默认	sm4cbc-sm3-sm2		80 BY 73 BH	19.3

1) 新建策略

点击"新建"按钮,打开策略配置对话框,根据界面提示信息配置 策略,如下图所示:

Э	WAR-	□ 脚隊	d	2 毎人 ① 毎出	◎ 启用	◎ 停止						
	策略名称	*** 策略配]	<u>س</u>					×	ESP协议	使用状态	操作	ı
	conn1	10			57 40 44 44 201	and the am	0		sm4cbc	۲	2010/2010	-
	conn1	19 第一阶	©SA	24	本地VPN地址	192 168 6 1	0-5112		sm4cbc	۲	約書面的	1917
	conn1	生存期 19 远程VP	小时) N地址	10.0.0.1	本地证书	C=CN.O=Sir	nocipher,(	CN=Alice V	sm4cbc		2018:1700	-
	conn1	15 本地标	R	C=CN,O=Sinocipher,CN=Alice	远程CA证书	C=CN,O=Sir	nocipher,0	CN=Roo ∨	sm4cbc	۲	wenn	10201
	conn1	19 远程标	R	C=CN,O=Sinocipher,CN=Bob					sm4cbc	۲	ALC: HE TALES	SRVE
	conn1	15				保	存	取消	sm4cbc	۲	10形元用	1811
	conn1	19							sm4cbc		24110270200	14/05
	conn1	192.168.6.1	10.0.0	1 C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocip	her,CN=Bob	默认	sm4cbc-sm3-sm2	sm4cbc	۲	2018/72.09	lant
	conn1	192.168.6.1	10.0.0	1 C=CN,O=Sinocipher,CN=Alice	C=CN,O=Sinocip	ner,CN=Bob	默认	sm4cbc~sm3~sm2	sm4cbc			80
	conn1	192.168,6,1		1 C=CN,O=Sinoclpher,CN=Alloe	C=CN,O=Sinocip	ner,CN=Bob	默认	sm4cbc-sm3-sm2	sm4obc		ANE ID AN	same

#### 2) 配置加密范围

选择需要配置加密范围的策略,点击"加密范围"按钮,打开加密范围对话框,根据界面 提示进行配置即可,如下图所示:

里员				conn1	-加密范围	442							÷
				新建	#1	余							
策略省	柳		19		策略名称	本地网段	端口	远程网段	端口	第二阶段 SA生存期(秒)	ESP协议	传输方式	搱
0					conn1	192.168.6.1/32	TCP	10.0.0.2/32	TCP/80	3600	sm4cbc-sm3-sm2	加密	10
•	\$112 				conn1	192.168.6.1/32	UDP	172.16.0.1/32	TCP/80	3600	sm4cbc-sm3-sm2	路由	3
	策略名称	本地VPN地址	远程VPN地址		conn1	192.168.6.1/32	TCP	10.0.0.2/32	TCP/80	3600	sm4cbc-sm3-sm2	路由	
	conn1	192.168.6.1	10.0.0.1		conn1	192.168.6.1/32	TCP	10.0.0.2/32	UDP/123	3600	sm4cbc-sm3-sm2	路由	1
	conn1	192.168.6.1	10.0.0.1		conn1	192.168.6.1/32	UDP	172.16.0.1/32	UDP/123	3600	sm4cbc-sm3-sm2	路由	
	conn1	192.168.6.1	10.0.0.1		conn1	192.168.6.1/32	UDP	172.16.0.1/32	UDP/123	3600	sm4cbc-sm3-sm2	加密	1
	conn1	192.168.6.1	10.0.0.1		conn1	192.168.6.1/32	UDP	172.16.0.1/32	UDP/123	3600	sm4cbc-sm3-sm2	加密	-
	conn1	192.168.6.1	10.0.0.1		conn1	192.168.6.1/32	UDP	172.16.0.1/32	UDP/123	3600	sm4cbc-sm3-sm2	加密	
	conn1	192.168.6.1	10.0.0.1										
	conn1	192.168.6.1	10.0.0.1										
	conn1	192.168.6.1	10.0.0.1										
	conn1	192.168.6.1	10.0.0.1										
	conn1	192.168.6.1	10.0.0.1										

#### 3.5.7.1 隧道监控

依次点击菜单栏的 IPSec 管理->隧道监控功能菜单,可查看当前 配置的 IPSec 隧道信息,如下图所示:

<u>£</u> 1	8重置									
	隧道名称	本地VPN地址	远程VPN地址	第一阶段隧道计时/秒	第二阶段隧道计时/秒	本地网段	远程网段	传入数据	✓	操作
					1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	
1	conn1	192.168.6.1	10.0.0.1	10830	1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	22
					1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	<b>#</b> #
					1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	
	conn1	192.168.6.1	10.0.0.1	10830	1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	
					1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	
					1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	東西
	conn1	192.168.6.1	10.0.0.1	10830	1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	22
					1012	192.168.6.0/24	192.168.7.0/24	22MB / 21000包	22MB / 21	重要

## 3.5.8 系统备份与恢复

3.5.8.1 系统备份

依次点击菜单栏的恢复与备份->系统备份,可对系统中数据以及 密钥文件进行备份储存。

系统备	<b>番份向导</b>			
1、备份 2、点击 3、如果	的密钥数服将以文件形式存储,请妥善保存. 开始备份后请耐心等待至密钥文件下载完成. 忽确定备份密钥数据,请点击"开始备份"按钮.			
	开始备份	系统提示	×	
		? 确认后开始密钥数据备份	31	
		991	人 取満	
				1

点击确认后耐心等待着备份数据完成 (会有点慢)。

			BAN - ATERN		
*1	首页	系统备份 💿		₩	21
	系统	备份向导			
	1、备 2、点 3、如	份的密钥数据将 击开始备份后请 果您确定备份密	以文件形式存储,请妥善保存. 耐心等待至密明文件下载完成。 明数据,请点击"开始备份"按钮.		
		开始	备 <del>份</del>		
			○ 密閉备份中,请勿操作		

等待数据备份完成后,自动转跳至系统备份文件下载页面,点击保存

41	首页	系統备份 💿							₩	CR
	系约	语份向导								
	服务器内的信息已经备份到文件中,点击保存到本地按钮,下载到本地并妥善保存。									
		保存								
要打	打开或保存	序来自 192.168.6.115 的 zaykhsm	.tar (810 KB)吗?		打开(0)	保存(S) ▼	取消(C) ×			

后可下载备份文件(请妥善保管好备份数据)

## 3.5.8.2 系统恢复

依次点击菜单栏的系统恢复与备份->系统恢复,可对系统中数据 以及密钥文件进行数据恢复,请上传在系统备份中备份的数据后。点 击上传

文件名称	请输入文件名称 时间(	备份恢复		×	
		上传恢复文件			
■ 系统器		18 Y	2件拖到此处,或点击上传		
	文件名称		只能上传zip格式文件		操作
B	crypto20230217003711.tar				下數 你能
	crypto20230217014843.tar			NOT ROM	The star
Q	crypto20230217183237.tar	2020-02-11			下载 物質
	crypto20230217183243.tar	2023-02-17		admin	下载 改变
D	crypto20230217184311.tar	2023-02-17		admin	下载:标准
	crypto20230217184927.tar	2023-02-17		admin	下戰。快速
B	crypto20230218220323.tar	2023-02-18		admin	下载 物調
	crypto20230218220556.tar	2023-02-18		admin	Fill the
	crypto20230218220755.tar	2023-02-18		admin	下班。你放
	crypto20230219014800.tar	2023-02-19			Fait that
				<b>共 39</b> 象	10 新页 ~ 〈 1 2 3 4 〉 前庄 1 页

## 3.6 审计管理员用户

以审计管理员身份登陆 WEB 管理系统,该管理员操作日志、登陆 日志、SSL 用户日志的查看、审计、导出功能。

3.6.1 日志管理

#### 3.5.1.4 日志配置

日志配置页面如下图所示,可以配置日志记录等级,日志记录等级分为"错误、警告、信息、调试",支持同步 syslog 日志功能,以及配置 syslog 所在服务器的 IP,接口。设置审计日志循环签名周期(小时),设置日志阀值。

#### 日志配置

*管理日志级别:	信息    ~	
*日志阈值:	999999 条	
*是否备份到SYSLOG服务器:	0 是 ○ 否	
* 服务器IP地址:	192.168.6.74	
* 🕑 服务器端口号:	514	
保存 重置		

#### 3.5.1.5 日志査看

## 3.5.1.5.1 查看、审计

管理日志、异常日志、服务日志、审计日志,可以根据选择的开始时间、结束时间。日 志等级来过滤查询日志,从右侧多选框选择相对应的日志,点击"审计"按钮,即可对选择 的日志进行审计。

日志基総動置	日志編号 请援	认日志编号	用户名称 谢输入用户名称	○ 検索 ○ 重	Ħ			
日志归档	管理日志 昇	端日志 服务日志 审计	日志					
日志査者		日志编号	用户名称	创建日期 💠	访问IP	详情	审计状态	操作
		448	secAdmin		192.168.6.3	用户密码错误	未審计	之审计
		393	sysAdmin		192.168.6.3	用户密码错误	未审计	之审计
		345	admin		192.168.6.212	用户密码错误	未審计	之审计
		332	admin	2023-02-22 11:43:03	127.0.0.1	用户密码错误	审计成功	之前计
		330	admin	2023-02-22 11:43:01	127.0.0.1	用户密码错误	朱熹计	之审计
		328	admin	2023-02-22 11:42:50	127.0.0.1	用户密码错误	未审计	之审计
		327	admin	2023-02-22 11:42:38	127.0.0.1	用户密码错误	未审计	之审计
		269	sysAdmin	2023-02-22 11:21:03	127.0.0.1	用户密码错误	未审计	之审计
		268	sysAdmin	2023-02-22 11:20:57	127.0.0.1	用户密码错误	朱审计	之审计

医二次复 企下载

2恢复 2下載

共2条 10条/页

< 1 >

## 3.5.1.6 日志归档

## 3.5.1.6.1 归档和恢复

日志归档和日志恢复直接点击按钮即可,在弹出的对话框点击【确定】,即可完成操作。

• <b>1917</b> - Start Skien	所有日志进行归焉!							
0 (SH				0 0				
8	白档编号	月档地址	Giterite	操作				
Ø	10	/root/sqlBak/operLogBak/20230220161319.sql	2023-02-20 16 13 19	之恢复 と下戦				
	8	/root/: 提示 ×	2023-02-20 16:10:44	2次夏 2下数				
		R0H #62		共2条 10条页 ~ ( 1 ) 前在 1 页				
<b>白松病号</b> 滚输入旧档编号								
● <b>臣國施</b> 示:: 点山(3時, 系統局3)所有日初进行(3時)								

取消 商定

提示

() 确定恢复此归档日志吗?