翼安VPN综合安全网关
用户手册

山东华翼微电子技术股份有限公司

版本更新记录表			
序号	版本号	版本更改说明	更改日期
1	V1.0	首次发布	
2			
3			
4			
5			
6			
7			
8			
9			
10			

声 明

版权声明

本文档的版权属山东华翼微电子技术股份有限公司所有。

本文档的版权受到中华人民共和国国家法律和国际公约的保护。未经书面许可，任何单位和个人不得以任何形式或通过任何途径非法使用、拷贝、修改、扩散本文档的全部或部分内容。

特别提示

我们做了大量的努力使本文档尽可能的完备和准确，但疏漏和缺陷之处在所难免。任何人或实体由于本文档提供的信息造成的任何损失或损害，山东华翼微电子技术股份有限公司不承担任何义务或责任。

山东华翼微电子技术股份有限公司保留未经通知用户对本文档内容进行修改的权利。

联系我们

如果您对本文档有任何疑问、意见或建议，请与我们联系。对您的帮助，我们十分感激。

公司电话：0531-66680161

公司邮箱：shandonghuayi@holichip.com

公司地址：山东济南高新区舜泰北路933号19层

目 录

1 概述

1.1 简介

VPN综合安全网关利用PPTP/L2TP、SNMP、DHCP及NTP时间同步、SMTP服务器等关键技术，实现网络业务数据的安全访问，包括SSL VPN和IPSEC VPN两大部分。通过SSL VPN提供安全、加密、可信的外网访问内网功能，实现外网访问内网时对应用及数据的安全保护。通过IPSEC VPN对公司或者机构内部各不同网络直接的联通，方便公司及子公司之间组成虚拟私有网络用于安全有效的数据和业务流转。

2 产品安装说明

2.1 安装环境要求

产品为1U机架式服务器，安装前须准备2U机位、2个AC220V/50Hz交流电源插座、设备接入网络环境（设备IP地址、路由、安全策略等）。

2.2 产品安装

可部署在外网与内网之间，应用沟通的私有虚拟网络之间，为安全数据提供服务。外网与内网之间示例部署VPN设备，通过VPN设备安全访问应用平台。

3 产品操作说明

为了方便网络或设备管理员对安全接入网关设备进行配置操作及维护,安全接入网关产品支持通过HTTPS协议建立安全的Web连接实现Web网管功能。管理员可以通过Web界面更加直观和便捷地管理和维护安全接入网关设备

3.1 系统说明

3.1.1 登录管理系统

Web管理的具体访问步骤如下：

1. 连接设备和 PC

2. 用交叉以太网线将 PC 和设备的默认管理口（面板从左往右第一个电口，非 console 口）相连

3. 为 PC 配置 IP 地址，保证能与设备互通

4. 修改管理 PC 的 IP 地址为 192.168.18.0/24（192.168.18.0/24 网段内除 192.168.18.1、192.168.18.199 的任意地址即可），例如 192.168.18.198

5. 启动浏览器输入访问地址 https://192.168.18.199:8181

3.1.2 初始化操作

首次打开管理页面需要进行初始化的操作，包括授权码及序列号验证、加密卡初始化，根证书设备证书初始化以及登录方式的选择。

3.1.2.1 设备配置详情

设备配置详情页面显示设备的配置信息，点击【下一步】即可。

3.1.2.2 CA证书类型选择

初始化时默认使用内置证书，第三方证书可以在进入系统后切换，所以直接点击【下一步】。

3.1.2.3 CA证书初始化

在CA证书初始化页面，填写证书名称，选择有效起始日期和有效终止日期，其他参数按照需要进行设置，点击【下一步】，完成CA证书初始化。

3.1.2.4 设备证书初始化

在设备证书初始化页面，填写证书名称，选择有效起始日期和有效终止日期，其他参数按照需要进行设置，点击【下一步】，完成内置设备证书初始化。

3.1.2.5 主机key初始化

本版本key为国标版本，所以需要安装新版KEY-SERVER，来保证key的正常使用。在页面上点击【下载KEY-SERVER】，得到安装包后进行安装。

安装后插入两把key，点击【刷新KEY】，选择主USB-KEY和从USB-KEY，点击【下一步】完成主机KEY的初始化。完成后将它们拔下，换上即将要初始化的管理员KEY。

注意

在主机 KEY 初始化完成后，需要将两把主机 KEY 都插到 VPN 设备的 USB 口上，否则在设备重启后，VPN 管理项目将无法启动。如果在未插入主机 KEY 的情况下重启了项目，则需要插入主机 KEY 后重启 VPN 设备。

3.1.2.6 管理员初始化

安全接入终端的管理页面访问需要通过智能密码钥匙此处的初始化目的是创建管理系统所需的三种管理员账号。

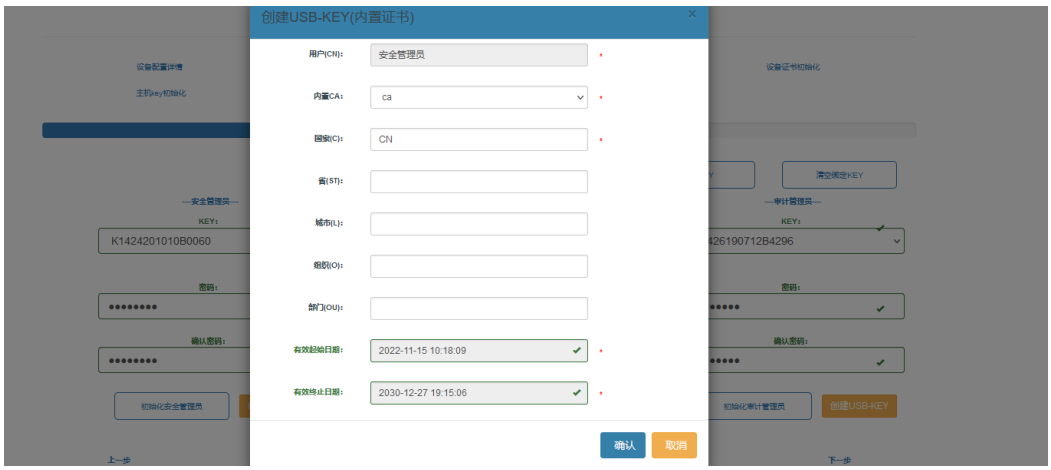
管理员账号分为三种：安全管理员，系统管理员和审计管理员，不同类型的管理员

拥有不同的权限，对应的具体权限可对照下述各功能说明。

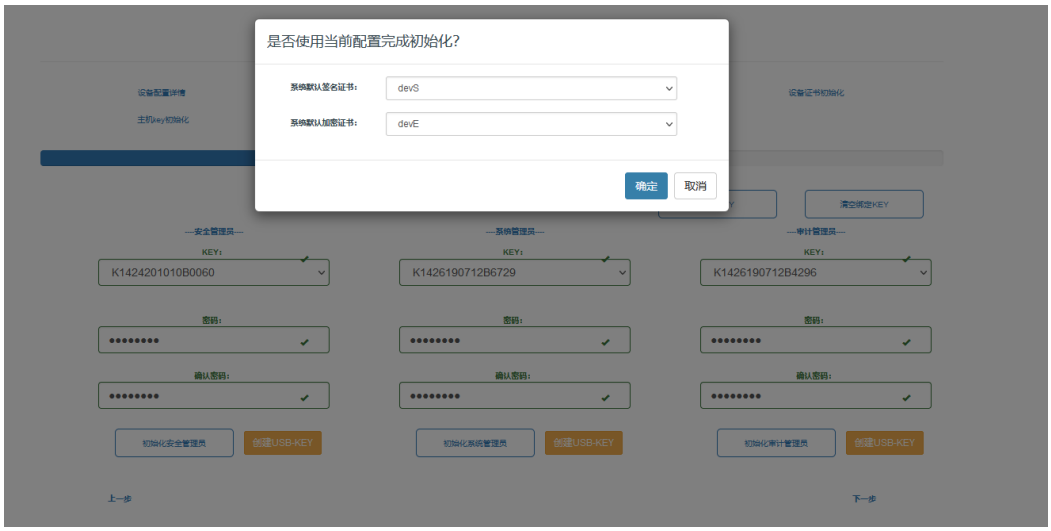
初始化时分别插入三把智能密码钥匙，更换智能密码钥匙后需要点击【刷新KEY】，在下拉框重新选择要使用的智能密码钥匙，输入对应的密码。

依次点击对应的管理员【初始化】按钮完成初始化，然后点击【创建USB-KEY】，弹出USB-KEY创建框，输入必填信息后完成创建。

如果在初始化管理员的过程中使用了错误的KEY，可以点击【清空绑定KEY】按钮，清除管理员与KEY的绑定关系，然后重新初始化管理员。



完成后点击【下一步】，会提示“是否使用当前配置完成初始化”，并显示当前系统默认证书，单击【确定】完成初始化。



注意

全新的智能密码钥匙的默认密码为 12345678

3.1.3 管理员权限说明

系统默认有三大管理员：系统管理员，安全管理员，审计管理员。各管理员职能唯一，实现对系统的分权管理。
系统管理员负责对软件环境日常运行的管理和维护，以及对系统的备份。
安全管理员负责证书管理，及设备密钥的备份，管理员账号管理。
系统审计员负责对系统中的日志进行安全统计。

3.1.4 管理员登录

初始化完成之后，会自动跳转到登录页面，插入相应的管理员KEY，输入密码和验证码完成登录。

在一个浏览器中只能同时登录一个管理员。也就是说，如果同一浏览器中的多个标签页中分别登录了多个不同的管理员，最终只会以最后登录的管理员为准。

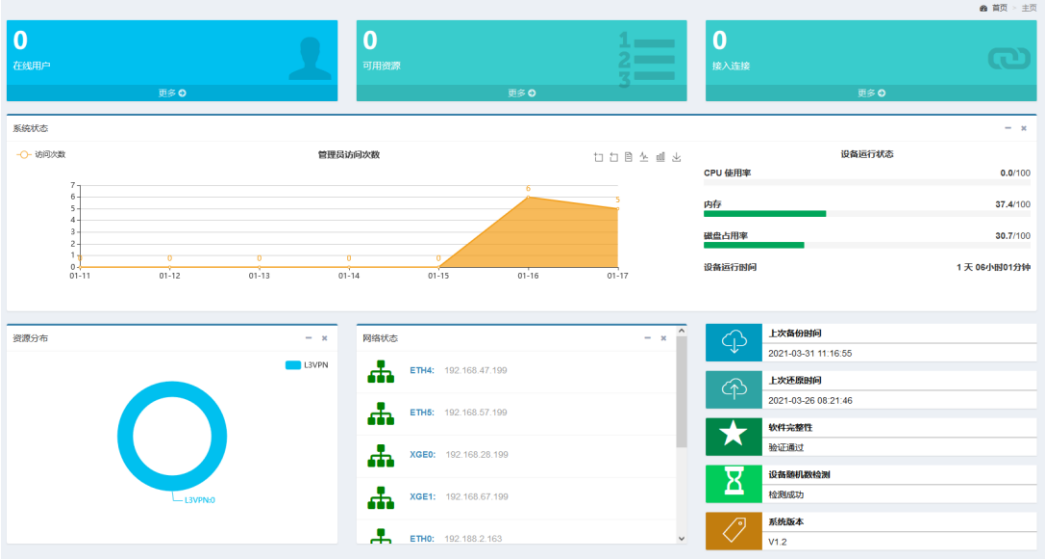
注意

如果在登录后提示“SM3 运算失败”，通常是因为这把智能密码钥匙还没有完成初始化。考虑是否插入了错误的 KEY

在有的版本的 Chrome 浏览器中，使用无痕模式时，可能会出现读取不到 key，无法登录的情况。出现这种情况时需要重启 keyserver

3.2 运行状态

管理员登录后的Web UI界面如下图所示，为监控面板页面，它显示了关键的系统信息和系统统计数据的概要信息。



- 状态监控：根据设备的 CPU、内存、硬盘使用率计算出当前设备的健康状态
- 管理员访问次数：显示最近七天中管理员登录系统的次数
- 资源分布：显示 SSL 服务配置的各种资源占比饼状图
- 网络状态：设备各网口及 IP 信息
- 系统信息

3.3 系统设置

3.3.1 **系统配置**

3.3.1.1 时间与日期

功能说明：时间与日期功能为用户提供了修改安全接入网关时间与日期的功能。

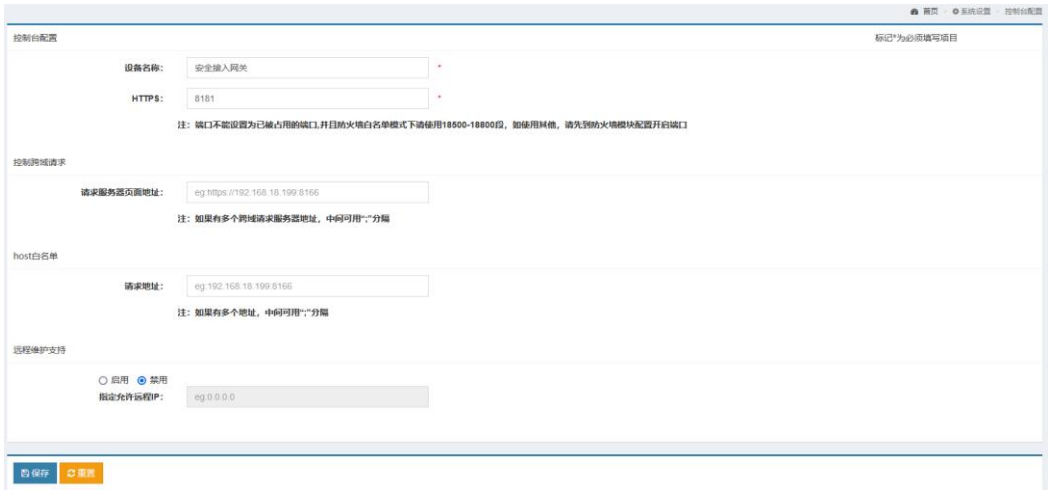
以系统管理员身份登录管理页面，选择【系统设置 > 系统配置 > 时间与日期】，点击【日期】可修改安全接入网关的日期，点击【时间】可修改安全接入网关的时间。勾选【自动与时间服务器同步】，选择要同步的时间服务器，点击【保存】，可使刚刚修改的时间生效。

注意

同步时间需配置安全接入网关，使设备可以使用互联网

3.3.1.2 控制台配置

以系统管理员身份登录管理页面，选择【系统设置 > 系统配置 > 控制台配置】，此功能可修改访问安全控制网关页面的端口号，包括https，系统出厂默认https访问端口号为8181。



3.3.1.3 邮件服务器

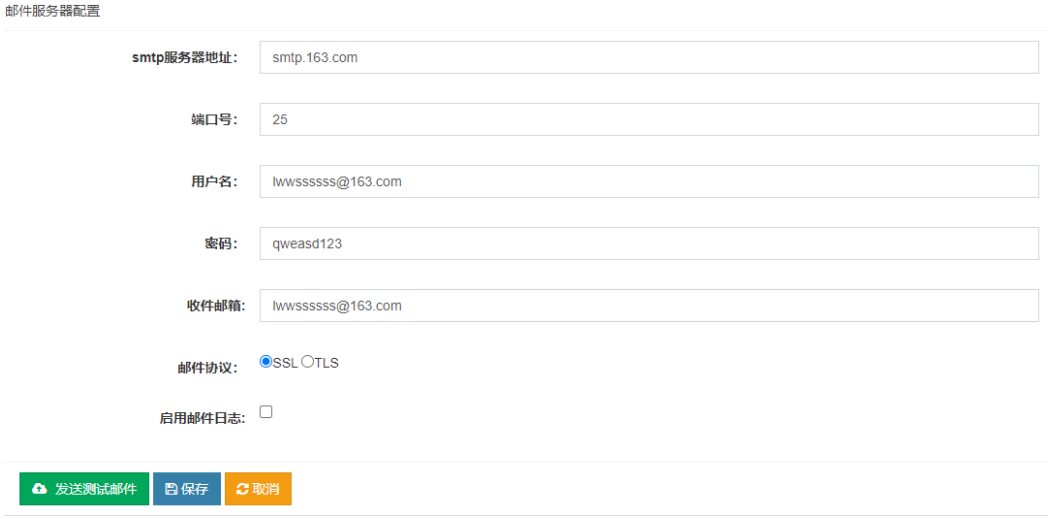
功能说明：主要针对设备的 SMTP 服务器的设置，使设备能够对外发送邮件。以系统管理员身份登录管理页面，选择【系统设置 > 系统配置 > 邮件服务器】，进入邮件服务器配置界面。

参数说明：

- SMTP 服务器地址：填写相应 SMTP 服务器地址，例如 QQ 邮箱的服务器地址为 smtp.qq.com，网易的服务器地址为 smtp.163.com

- 端口号：设置 SMTP 服务器提供服务的端口号
- 用户名：填写发送邮箱的邮箱地址
- 密码：填写发送邮箱的密码
- 收件邮箱：填写接收邮箱的邮件地址
- 邮件协议：选择所需的邮件安全协议
- 启用邮件日志：勾选上，则会向收件邮箱发送服务端的管理日志

参数配置完成后，点击【保存】，进行邮件服务器的配置。点击【取消】，可重置邮件服务器的配置。点击【发送测试邮件】，可测试保存的邮件服务器配置是否正确。



注意

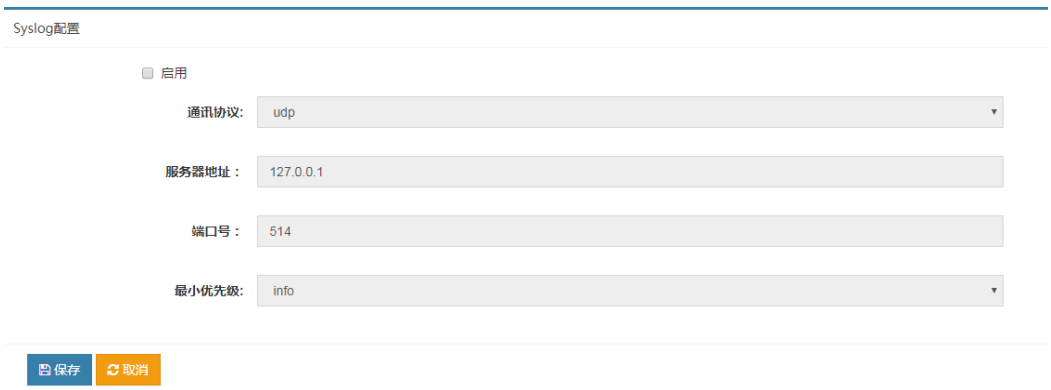
使用邮件服务器需配置安全接入网关，使设备可以使用互联网

用户名即发件人邮箱，必须开启 SMTP 服务

3.3.1.4 Syslog

功能说明：可配置向日志服务器发送管理员日志的功能。

以系统管理员身份登录管理页面，选择【系统设置 > 系统配置 > Syslog】，进入Syslog配置界面。



参数说明：

- 启用：是否启用邮件服务器。
- 通讯协议：日志传输使用的协议类型。
- 服务器地址：日志服务器的 IP 地址。
- 端口号：邮件服务器用于接收日志的端口号。
- 最小优先级：发送到日志服务器的日志等级。

配置完成后点击【保存】完成Syslog功能的配置。

3.3.2 证书管理

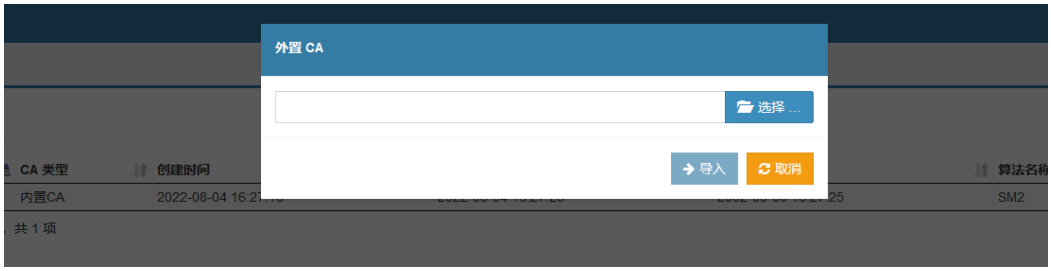
3.3.2.1 CA管理

功能说明：本功能可以生成内置CA证书或导入外置CA。
以安全管理员身份登录管理页面，选择【证书管理 >CA管理】，打开CA证书页面。
内置CA
参数说明：

- 名称：生成的根证书名称
- 国家、省、城市、组织、部门：可根据需要填写
- 有效起始日期：证书生效的起始时间
- 有效终止日期：证书生效的终止时间
- 密钥类型：SM2
- 密钥长度：256

外置CA

点击【导入第三方 CA】，上传外置CA

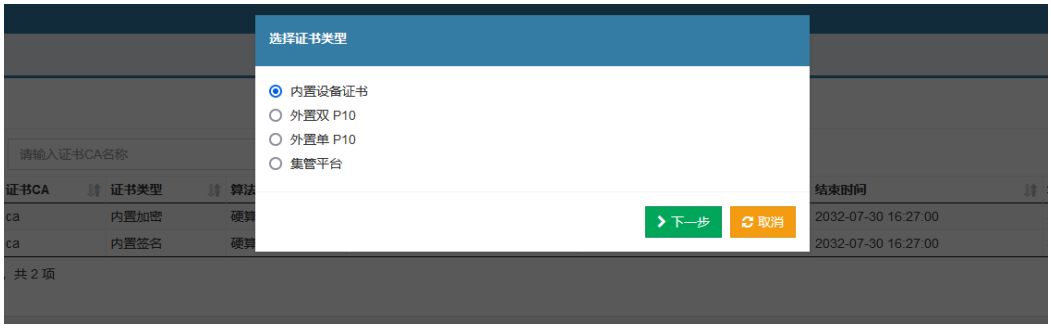


3.3.2.2 （CA）设备证书

功能说明：以CA证书为基础生成用于SSL和IPSEC服务使用的设备证书。

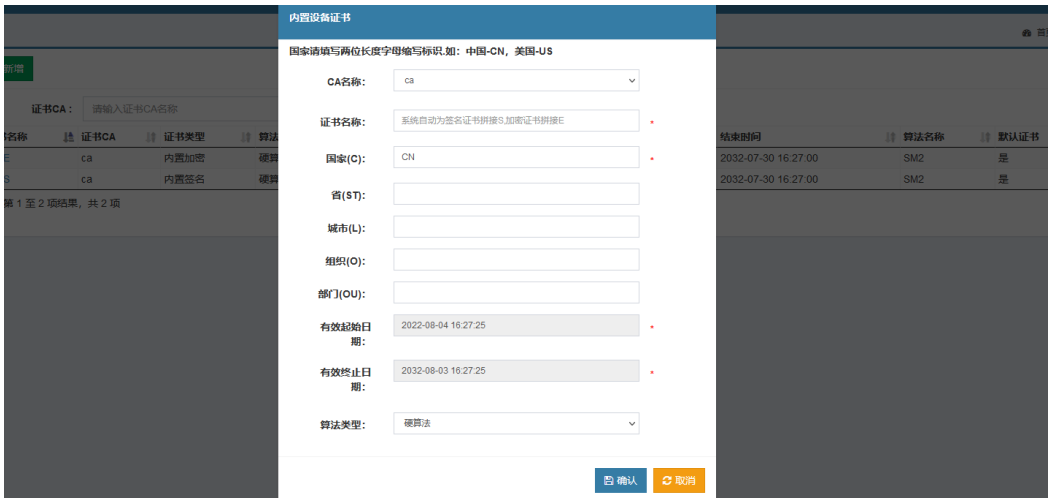
以安全管理员身份登录管理系统，选择【证书管理 > （CA）设备证书】，进入设备证书页面。

因为根证书分为使用内置CA和使用外置证书两种情况,对应的设备证书也需随根证书类型做调整，单击新增，选择内置、外置双p10、外置单p10或集管平台。



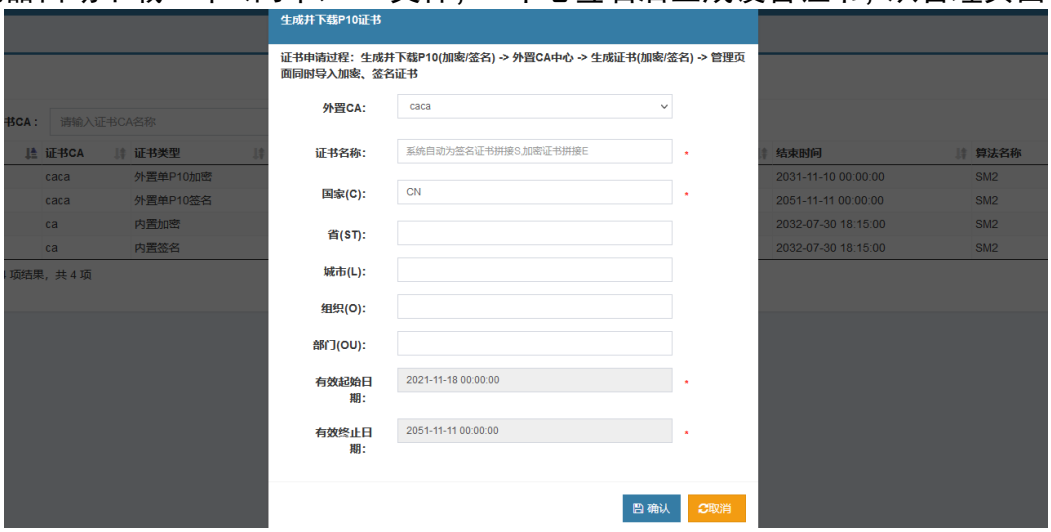
3.3.2.3 使用内置CA生成设备证书

选择内置设备证书后，弹出内置设备证书生成窗口，输入必填项目，单击确认，生成证书。

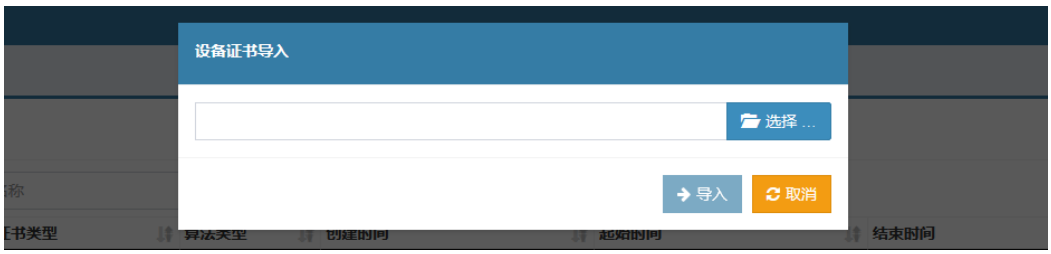


3.3.2.4 使用外置单（双）P10生成设备证书

选择外置单（双）P10，弹出内置设备证书生成窗口，输入必填项目，单击确认，浏览器自动下载一个（两个）P10文件，CA中心签名后生成设备证书，从管理页面导入。



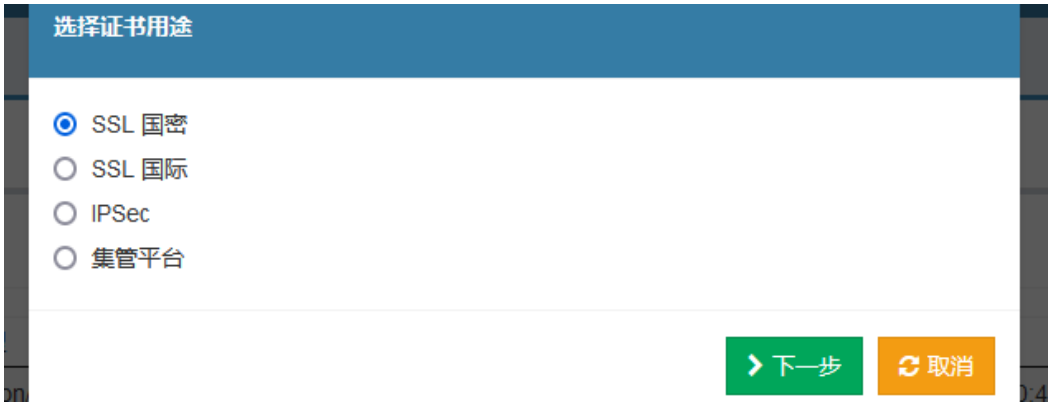
生成p10证书后浏览器会自动下载，在管理页面点击导入证书按钮来导入对应证书即可。



3.3.2.5 可信证书列表

系统支持可信证书上传，安全管理员登陆系统，【证书管理 > 可信/吊销证书管理 >

可信证书列表】，进入可信证书管理页面，单击上传证书，弹出证书类型选择框



选择后单击下一步，上传可信证书

通过菜单【证书管理 > 可信/吊销证书管理 > 吊销证书列表】可进入吊销证书列表管理页面，可以上传用于 SSL 和 IPSec 的 CRL 吊销证书列表。

3.3.3 管理员账号

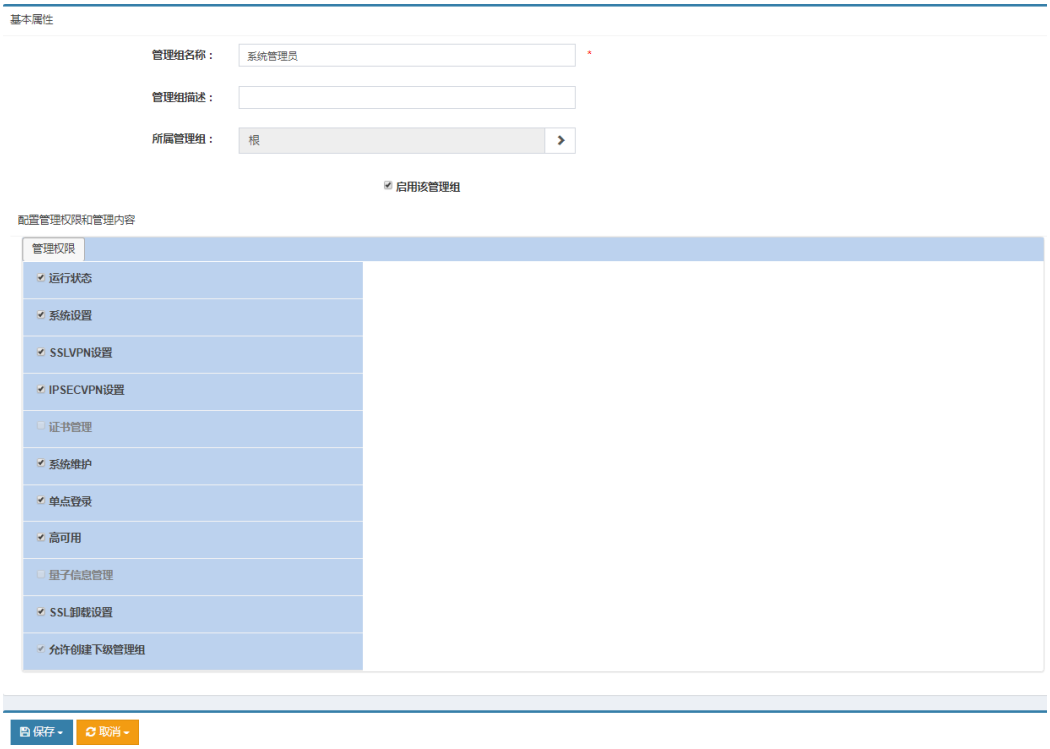
功能说明：管理员账号提供管理员及管理组的新增、编辑和删除。

以安全管理员身份登录管理页面，选择【系统设置 > 管理员账号】，进入管理员账号页面。

3.3.3.1 管理组管理

管理组新建/编辑：

在左边管理组树状结构上选择一个节点，点击新建管理组，打开新建/编辑管理组页面。



参数说明：

- 管理组名称：新增管理组的名称
- 管理组描述：配合管理组名称，方便管理员对管理组进行管理
- 所属管理组：要新建的管理组所属父级管理组
- 启用该管理组：新建管理组是否启用
- 配置管理权限和管理内容：该管理组有用的管理权限，勾选上代表有

点击保存，可新增/编辑管理组。

注意

组内管理员不可编辑所在管理组

删除管理组其下级管理组及管理员都将被删除

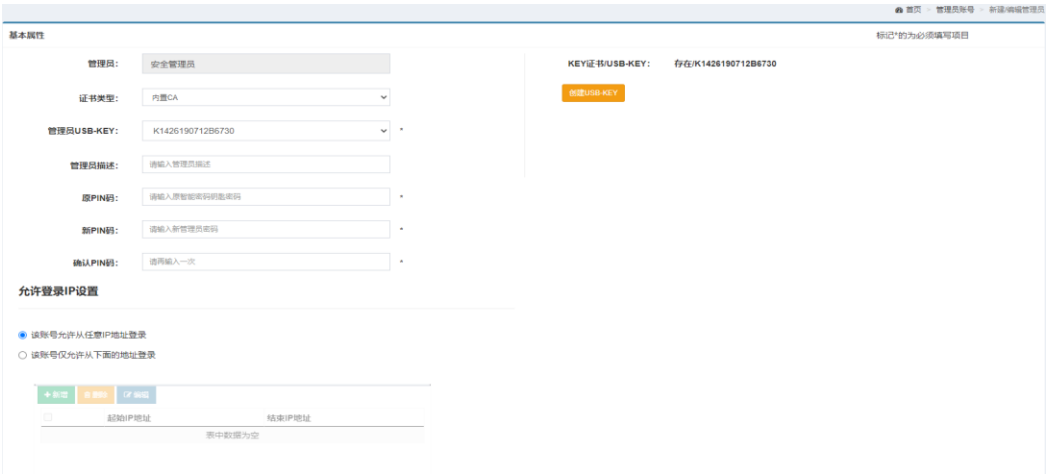
管理组删除：

选中要删除的管理组，点击【删除】，在打开的删除确认模态框中点击【确定】，即可删除该管理组及组下管理员。

3.3.3.2 管理员管理

管理员新建/编辑：

选中管理组，点击【新增】，选择管理员，打开管理员新增/编辑页面。



参数说明：

- 管理员：管理员名称
- 证书类型：生成 USB-KEY 使用的证书类型（内置/外置双 P10/外置单 P10）
- 管理员 USB-KEY：与管理员绑定使用的智能密码钥匙
- 管理员描述：配合管理员名称，方便对管理员的管理
- 原 PIN 码：KEY 原密码
- 新 PIN 码：要使用的密码
- 确认 PIN 码：确认 PIN 码与新 PIN 码一致
- 所属管理组：管理员所属管理组
- 允许登录 IP 设置：是否对该管理员使用的设备 IP 做限制，若选择‘该账号允许从下面的地址登录’，则该管理员只能从被限制的 IP 访问，该限制可以是一个 IP，也可以是一段 IP

配置完成后，点击【保存】即可完成管理员新增/编辑。

注意

新增/编辑管理员时，该管理员使用的智能密码钥匙必须插在进行操作的设备上，不然 PIN 值无法同步会造成问题

管理员删除：

选中要删除的管理员，点击【删除】，在弹出的确认删除提示框中点击【确定】，即可删除该管理员。

3.3.4 网络配置

3.3.4.1 部署模式

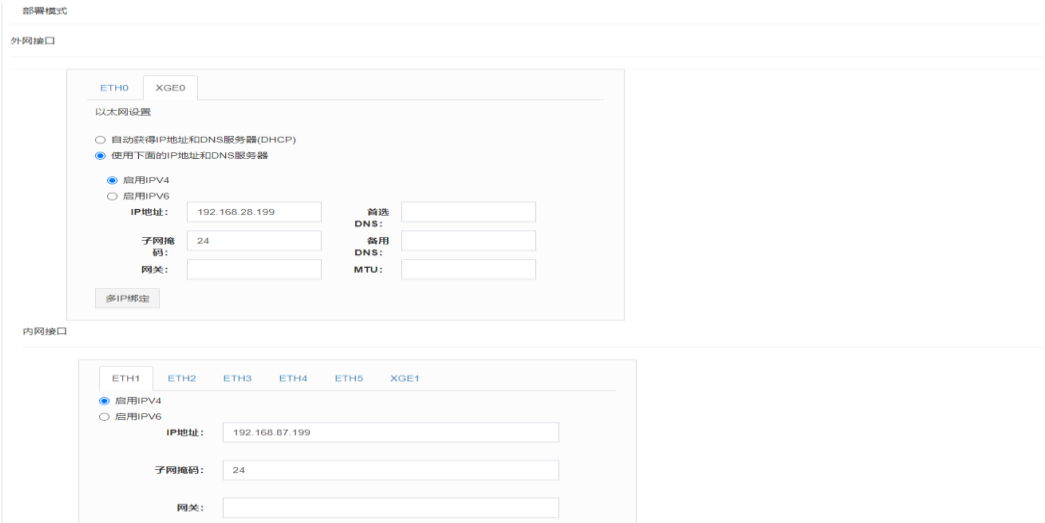
IP修改：

功能说明：部署模式可修改 安全接入网关各网口的IP、掩码、默认网关等配置。

以系统管理员身份登录管理页面，选择【系统设置 > 网络配置 > 部署模式】，进入部署模式页面。

参数说明：

- IP 获取方式：分为自动获取和手动设置，选择 DHCP 为自动，否则为手动
- IP 协议类型：可选择 IPv4 或者 IPv6
- IP 地址：该网口修改后生效的 IP 地址
- 子网掩码：该网口所在网络的掩码长度，单位为 8/16/24/32
- DNS：分为首选和备选，当首选 DNS 失效时会启用备选
- MTU：最大传输单元



注意

IP 获取方式、DNS、最大传输单元仅外网接口可以设置

多IP设置：

功能说明：此功能可为网口配置多个IP。

参数说明：

- IP 地址：要创建的多 IP 地址
- 子网掩码：该 IP 匹配的掩码长度，单位为 8/16/24/32

默认网关：
功能说明：此功能可配置安全接入网关的默认网关。
选择要设置为默认网关的网卡即可。

配置好上述参数后，点击【保存】，此时系统提示“正在配置网络部署，请等待配置保存成功提示后再操作”，点击【确定】，等待提示成功即可。

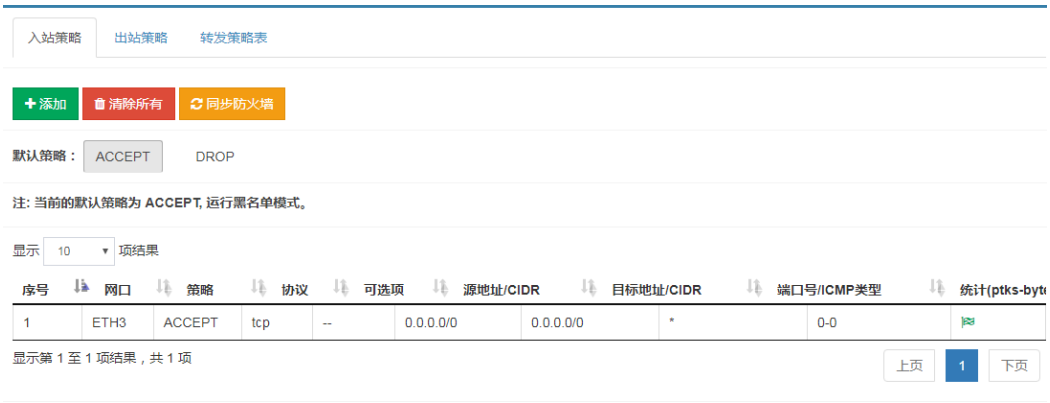
3.3.4.2 防火墙

功能说明：防火墙是借助硬件和软件的作用于内部和外部网络的环境间产生一种保护的屏障，从而实现对计算机不安全网络因素的阻断，只有匹配了防火墙规则的情况下，数据才能顺利通过。

以系统管理员身份登录选择【系统设置 > 网络配置 > 防火墙】，进入防火墙配置页面。

防火墙策略分为三种：

- 入站策略：针对目的地是 VPN 设备的数据包
- 出站策略：针对 VPN 发往别的设备的数据包
- 转发策略：针对经过 VPN 转发的数据包



添加防火墙策略：

上述三种策略的配置方式是相同的，此处以入站策略为例介绍。

默认策略ACCEPT和DROP分别代表黑名单和白名单模式，若为ACCEPT，默认不拦截，可以添加特定的拦截规则；DROP模式默认丢弃所有数据包，除非增加放行的规则。

点击【添加】按钮，可以打开添加规则窗口，如下图

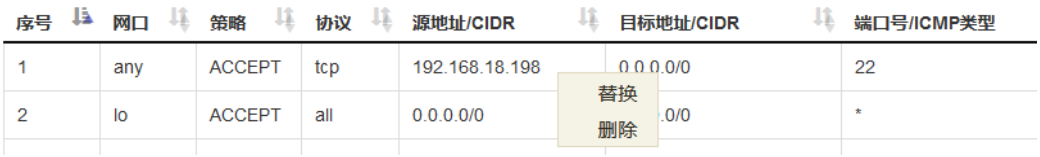
参数说明：

- 编号：表示规则的编号，一般按顺序填写即可
- 目的：ACCEPT 代表放行，DROP 代表丢弃，REJECT 表示拒绝，在默认策略 ACCEPT 时，通过添加 DROP 或者 REJECT 规则，来增加黑名单；在默认策略为 DROP 时，通

过添加 ACCEPT 规则来添加白名单

- 源 IP：数据包的源 IP
- 目的 IP：数据包的目的 IP
- 端口/icpm 类型：若协议为 ICMP，则端口/icmp 一栏填写 icmp 类型

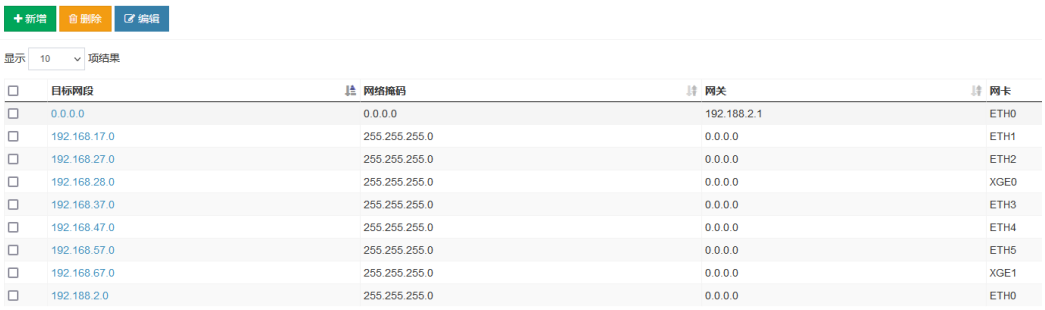
参数配置完成后点击【保存】即可新增一条规则。
清除所有防火墙：
点击【清除所有】会清除已添加的所有规则。
同步防火墙：
点击【同步防火墙】，可以将添加的规则保存并生效。
修改策略：
右击已添加的策略，可以进行修改等操作。



3.3.4.3 路由设置

功能说明：安全接入网关在实际使用环境中，可能根据网络环境需要添加路由，此时可在路由设置中进行操作。

以系统管理员身份登录管理页面，选择【系统设置 > 网络配置 > 路由设置】，进入路由配置页面。



新增路由：
点击【新增】，在打开的新增路由框中输入要配置的路由信息。
参数说明：

- 目标网段：路由指向的目标地址段
- 网络掩码：目标地址段的子网掩码
- 网卡：路由的载体

- 网关：到达目标地址段的下一跳地址
-

点击【保存并继续添加】，保存当前路由，继续添加新的路由；点击【保存】，保存当前路由；点击【取消】放弃本次添加。

编辑路由：

选中要修改的路由，点击【编辑】，在打开的路由编辑界面修改参数，点击【保存】即可完成修改。

删除路由：

选中要删除的路由，点击【删除】，在弹出的确认选择框中选择【确定】，即可删除该路由。

注意

- 目标网段与网络掩码必须同段，比如目标网段为 192.168.4.0，网络掩码可以为 255.255.255.0 或 255.255.255.255，但不能为 255.255.0.0。网关为可选项，首次添加新路由时，不需指定网关。添加成功后可点击编辑，进行网关的指定
- 目前的【路由设置】功能中只支持 IPv4 路由的显示，暂不支持 IPv6

3.3.4.4 Hosts

功能说明：host可以将主机地址与主机名进行对应，配置后用户只需记住对应地址的主机名即可，该页面可对安全接入网关上的Hosts信息进行管理。

以系统管理员身份登录管理页面，选择【系统设置 > 网络配置 > Hosts】，进入Hosts配置页面。

参数说明：

- 添加：点击【新增】，选择【新增主机映射】，输入对应配置信息即可点击【保存】
- 删除：选中要删除的 host，点击【删除】即可删除本条 host

- 编辑：选中要编辑的 host，点击【编辑】，在打开的模态框中输入要修改的参数，点击【保存】即可完成修改

3.3.4.5 NAT

功能说明：配置NAT可以实现使用少量的公有IP地址代表较多的私有IP地址的方式，NAT不仅能解决IP地址不足的问题，而且还能够有效的避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

以系统管理员身份登录管理页面，选择【系统设置 > 网络配置 > NAT]，进入NAT配置页面。

NAT策略分为：

- 预路由策略：即目标网络地址转换，一般用于外网访问内网
- 后路由策略：即源网络地址转换，一般用于内网访问外网

添加预路由：

应用场景为安全接入网关上的ETH0口和ETH1口IP地址分别为192.168.18.199,192.168.17.199，并分别接入两台设备A和B，IP地址分别为192.168.18.100和192.168.17.100，若A想访问B，可以直接访问安全接入网关的ETH0网口，安全接入网关会将数据包的目的地址转为ETH1的地址。

点击【添加】，打开添加窗口。填写配置如下图所示。

点击【保存】，即可完成添加。

将B设备的默认路由设为安全接入网关的ETH1网口（192.168.17.199），A设备即可通过在浏览器中访问安全接入网关的ETH0网口(192.168.18.199)和端口访问到B设备，此时访问A访问192.168.18.199:51实际上访问的是192.168.17.100:8080。

后路由添加：

网络配置为与安全接入网关相同，连接在ETH0上的设备A，连接在ETH1上的设备B，此时A若想访问B，参照下图配置。

点击【保存】，即可完成添加。

将A设备的默认路由设置为安全接入网关的ETH0网口192.168.18.199，A设备即可通过在浏览器中访问安全接入网关的ETH0网口（192.168.18.199）和端口访问到B设备，此时访问A访问192.168.17.100:8080实际上访问的是192.168.17.199:8080。

清除所有：

点击【清除所有】会清除已添加的所有规则。

同步NAT策略：

点击【同步NAT策略】，可以将添加的规则保存并生效。

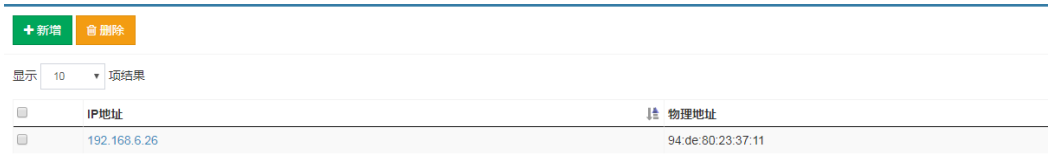
修改策略：

右击已添加的策略，可以进行修改等操作。

3.3.4.6 ARP

功能说明：ARP记录了安全接入网关收到的ARP应答消息终端IP及MAC地址。

以系统管理员身份登录管理页面，选择【系统设置 > 网络配置 >ARP】，进入ARP页面。



点击【新增】，在打开的添加ARP窗口中输入ARP信息，点击【保存】即可。

参数说明：

- IP 地址：设备的 IP 地址。
- 物理地址：设备的 MAC 地址。

选择要删除的ARP记录，点击【删除】，在弹出的确认删除对话框中选择【确定】，即可删除该ARP。

3.3.4.7 链路聚合

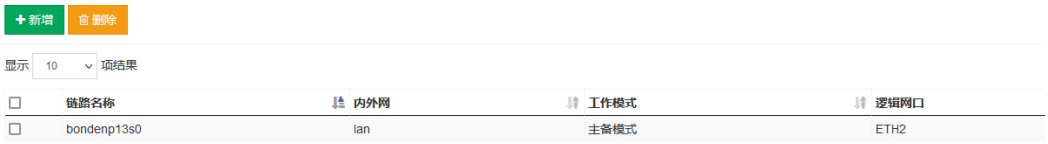
功能说明:将多个物理端口汇聚一起,形成一个逻辑端口,以实现负载均衡或主备。

主备模式：多个网卡聚合，只有一个网卡工作，当这个网卡出现异常停止工作时，

其他网卡立刻顶上，替换其进行工作，有效防止因网卡损坏带来的损失。。

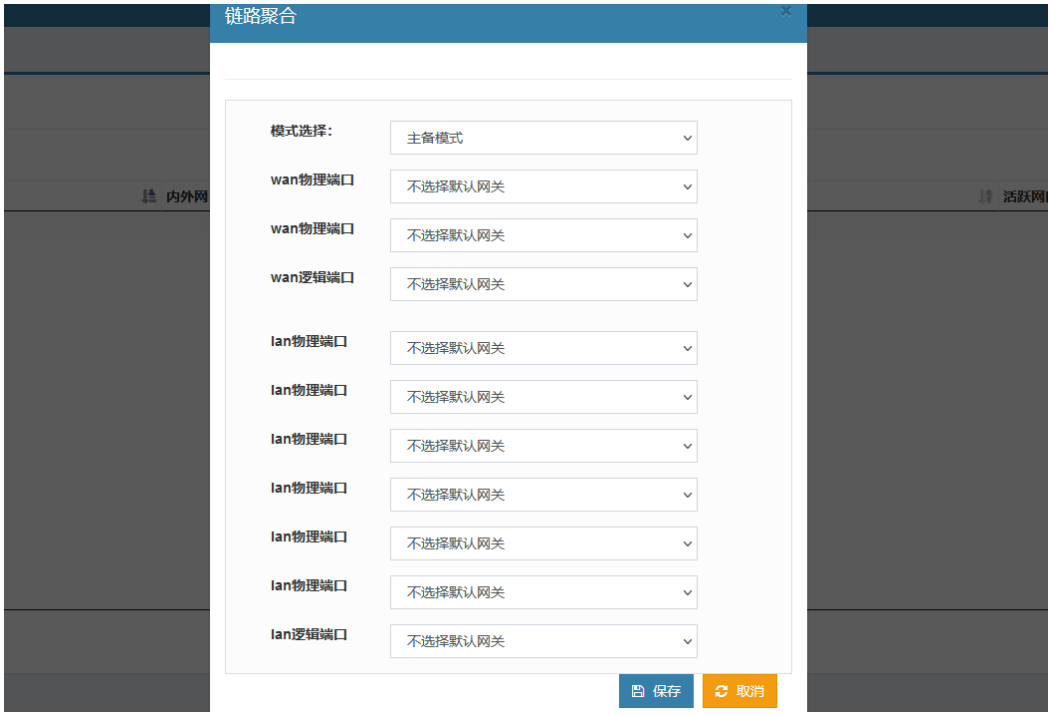
负载均衡模式：实现出入流量吞吐量在各成员端口的负荷分担，增加带宽，提高网络访问速度。

要求：配置链路聚合前需要先完成部署模式的配置，且需要聚合的网卡要保证网络正常。



点击【新增】，以下图为例，选择工作模式，主备或者负载均衡，然后选择逻辑网卡和物理网卡，逻辑网卡必须是物理网卡中的一个，否则无法保存（例：若物理端口为ETH1，ETH2，ETH3，ETH4,则逻辑网卡只能选择这四个中的一个），之后点击保存，进行链路聚合配置。完成后，会在主界面生成一条记录，点击该条记录，即可查看此记录的详细信息。负载模式不显示活跃网卡信息。参与聚合的物理网卡的网关均会清除。

点击删除，会将选中记录中所有的物理网卡的IP、子网掩码、网关信息全部删除，需要重新在部署模式中配置。（例：若删除逻辑网口为ETH0,物理端口为ETH0，ETH1，ETH2的链路聚合记录后，想用端口ETH1和ETH5进行聚合，必须要在部署模式中重新配置ETH1的网卡信息。）

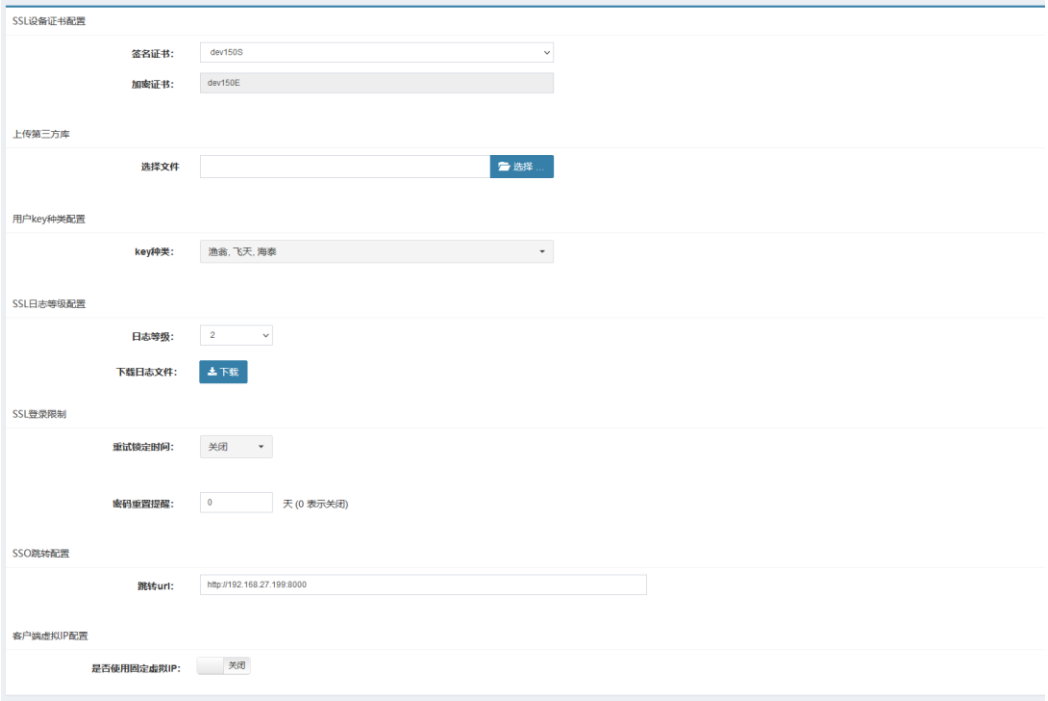


3.4 SSL VPN设置

3.4.1 接入选项

功能说明：此功能可以修改SSL服务使用的端口号、证书，上传 key 库，下载日志，配置SSO URL等。

以系统管理员身份登录管理页面，选择【SSLVPN设置 > 接入选项】，进入接入选项配置界面，选择SSL服务使用的设备证书，单击保存进行证书修改。



3.4.2 用户管理

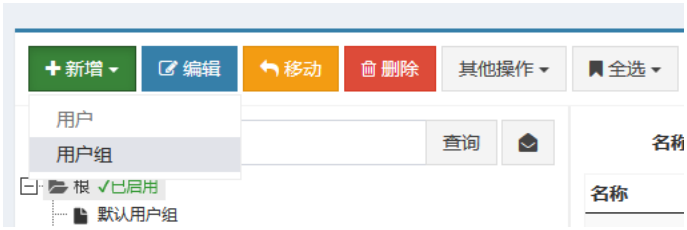
功能说明：用户管理页面提供SSLVPN用户的配置功能（注：该用户是指实际使用SSL功能的用户，并非系统管理员用户）。

以系统管理员身份登录管理页面，选择【SSLVPN设置 > 用户管理】，进入用户管理页面。

3.4.2.1 用户组管理

用户组添加：

为方便将用户与所需访问的网络资源关联并进行统一管理，安全接入网关引用用户组概念。在实际使用时，建议根据实际使用情况先进行用户组的添加操作，具体为：选择‘根’用户组（注：该用户组只是方便进行用户组的展示，并无法实际使用，切勿在‘根’用户组进行用户添加、移动和删除操作），单击【新增】并选择用户组，跳转至用户组添加页面按照提示进行操作。



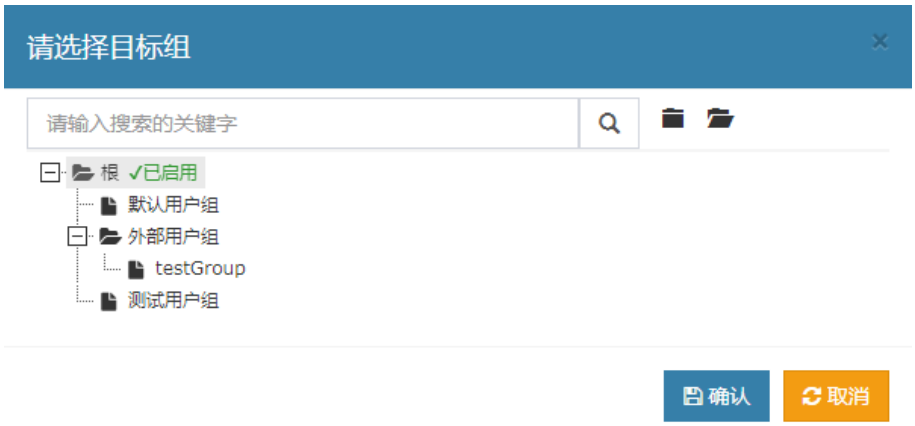
参数说明：

- 名称：用户组的名称，为方便管理可以填入部门简称如:网络支持 1 组等
- 描述：配合用户组名称，方便系统管理员对用户组进行识别
- 所属组：用于展示当前用户组所在的层级
- 所属虚卡：该用户组内用户分配 IP 时使用的虚卡
- 继承上级用户组关联资源：如果该用户组为二级用户组，当选择此选项时，【关联资源】选项只可选择父组分配的资源组
- 主要认证
  - 用户名/密码：适用于所有的客户端，是最基本也是最普通的认证方式
  - UKEY 认证：使用 USB 智能密码钥匙，配合对应密码进行用户登录认证，适用于 Linux 和 Windows 客户端
- 强制该组用户继承本组认证选项：强制指定用户组内的用户使用认证方式中的一种或多种
- 关联资源：指定该用户组内用户可以使用的具体资源，通过关联相应的资源组进行具体资源的关联

⚠ 注意

用户组内的用户个数不能超过所能分配的最大虚拟 IP 个数，理论上一个用户组的最大用户数量不能超过 255-1=254 个用户用

用户组编辑：
选择用户组后点击【编辑】，即可对该用户组进行编辑，具体参数同用户组添加。
用户组删除：
选择用户组后点击【删除】，即可删除该用户组及组下的所有用户。
用户组移动：
选择用户组后点击【移动】，会打开下图窗口，选择目标组后点击【确认】，即可将该用户组移动到目标组下



3.4.2.2 用户管理

新增用户：

选择需要使用的用户组，点击绿色【新增】，在弹出的下拉条中选择用户，进行具体SSL用户的的添加操作。用户添加页面如图所示：

参数说明：

- 名称：SSL 用户名称，当用户使用用户名和密码进行登录时，名称将作为登录用户的唯一身份标识
- 描述：便于系统操作员对不同用户进行辨别及管理，不参与任何功能的实现及管理
- 密码：用户密码
- 确认密码：需和用户密码保持一致
- 手机号：功能类似‘描述’，仅便于系统操作员对用户进行管理，不参与任何功能的实现及管理
- 所属组：当前新建用户所属的用户组。可以通过点击‘所属组’内容框在弹出的用户组树状图上进行新建用户与其他用户组的关联

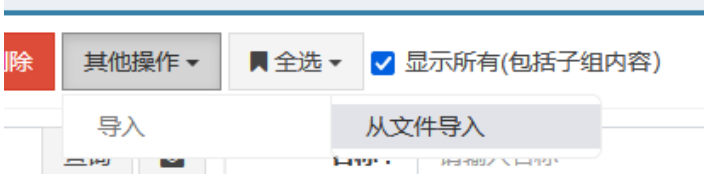
- 认证选项：在用户‘基本属性’最下方，提供额外的选择项‘继承所属组认证和账户状态选项’，该选择项可以指定，新建用户是否继承所在用户组的认证方式。如选择继承所在用户组认证方式，即勾选该选项，认证选项将变成灰色，不允许进行更改。相反即可对当前新建用户进行额外认证操作
- 不同认证方式的申请：SSL 用户一共可选择两种认证方式（如用户组或具体用户在‘认证选项’进行限定，用户可使用的认证方式可能会有所减少），如果选择使用 USB 智能密码钥匙认证可在此处进行申请（注：系统操作员需先点击‘保存’，新建用户成功后才可）。具体如下图所示：

- 创建 USB-KEY：将智能密码钥匙插入操作电脑（系统管理员正在使用的工作电脑，并非安全接入网关本身）。点击【刷新】，在选择智能密码钥匙下拉框选择需要绑定的智能密码钥匙，并输入密码钥匙口令。在绑定智能密码钥匙时，安全接入网关会将智能密码钥匙以用户名称进行重新命名，系统管理员可自行决定是否重新命名，智能密码钥匙名称并不影响正常使用

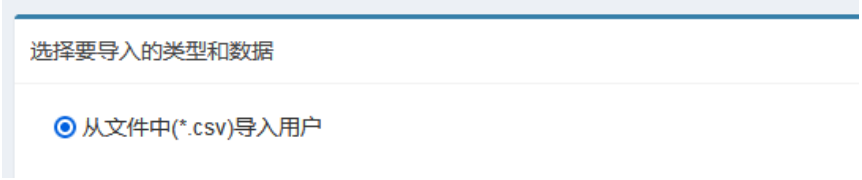
设置用户虚拟 IP 的获取方式：自动或者手动

设置用户过期时间：永不过期或者手动设置

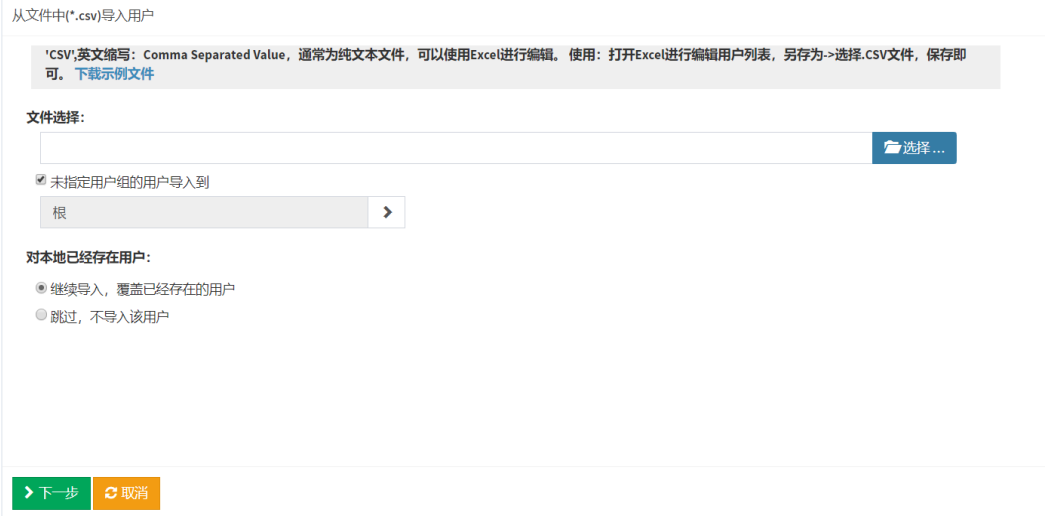
批量导入用户：
点击【其他操作】，选择【导入 > 从文件导入】



跳转到选择导入类型数据页面。页面如图所示：



点击【下一步】，进行具体的用户导入操作，在此页面选择用户模板文件上传，勾选【未指定用户组的用户导入到】，选择用户将要导入的用户组，最后点击【下一步】，页面如图所示：



下一步进入确认导入页面，可以在此页面看到将要导入用户的信息，确认导入信息无误后可以点击【开始导入】，进行导入用户信息的操作，页面如图所示：

3.4.3 资源管理

功能说明：资源管理功能可以添加资源组和资源，这些资源可以分配用户组使用。

以系统管理员身份登录管理页面，选择【SSLVPN设置 > 资源管理】，进入资源管理页面。

3.4.3.1 资源组管理

新增资源组：

选择一个资源组，点击【新增】，在列表中选择资源组，进入资源组添加界面。

参数说明：

- 名称：资源组名称
- 描述：备注资源组信息
- 启动资源组：是否使用该资源组

编辑资源组：

选中要编辑的资源组，点击【编辑】，在打开的资源组编辑页面可编辑资源组属性。

删除资源组：

选中要删除的资源组，点击【删除】，在打开的确认删除提示框中点击【确定】，即可删除资源组。

3.4.3.2 资源管理

资源添加/编辑：

- L3VPN 应用：适用于所有客户端，不区分 TCP 和 UDP 协议，也不对端口进行控制。

参数说明：

- 名称：L3VPN 应用名称
- 描述：只在管理页面进行展示方便系统管理员对该 L3VPN 应用进行管理
- 资源地址：具体要转发的网络资源。L3VPN 应用的地址通过 IP 配合掩码长度来控制
- 所属组：该 L3VPN 应用所属的资源组，系统管理员可以通过‘选择资源组’，指

定该 L3VPN 应用所属的资源组

- 启用资源：是否启用该资源

添加完成后点击【保存】，保存成功后会跳转至资源管理页面，新建的 L3VPN 应用会在页面右侧列表处展示

注意

L3VPN 应用，在添加资源地址时，可以添加多个地址，已达到批量添加的目的，但是可能存在某一应用资源地址在其他应用中重复添加的问题，安全接入网关不会进行重复判断，需要系统管理员在添加时自行判断。为防止分配的资源范围过大，从而导致的权限或信息溢出问题，建议在分配资源时，不要分配超过所需资源的最大范围

资源删除：

选中要删除的资源，点击【删除】，在确认删除提示框中点击【确定】即可删除该资源。

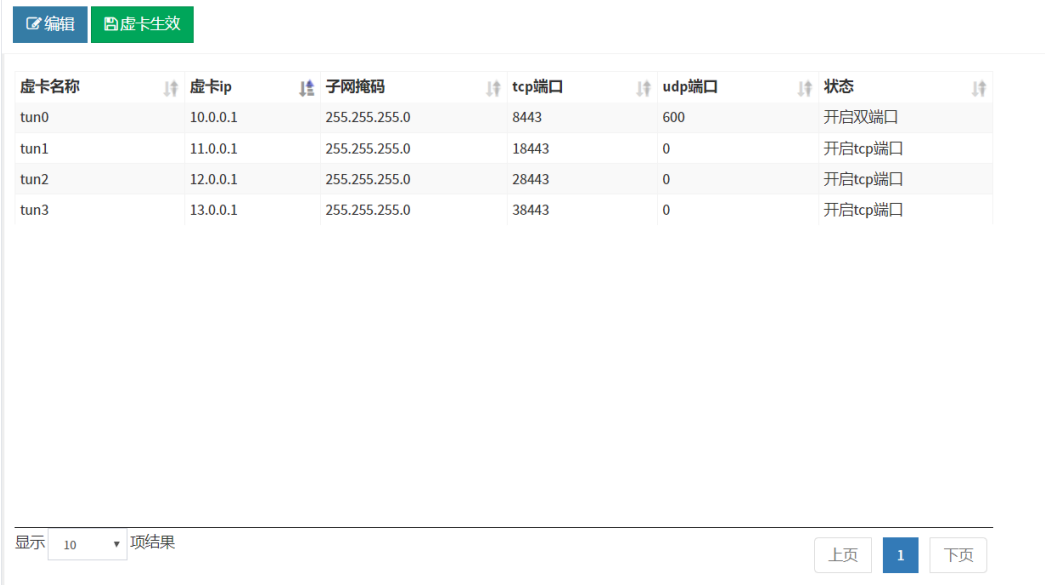
资源移动：

选中要移动的资源，点击【移动】，在弹出的确认框中选中要移动到的资源组，点击【确认】即可完成资源的移动。

3.4.4 虚卡配置

功能说明：虚卡配置功能可以编辑和开启服务用到的虚卡，为这些虚卡分配IP和端口。

以系统管理员身份登录管理页面，选择【SSLVPN设置 > 虚卡配置】，进入虚卡配置页面。



编辑虚卡配置：

选中一条虚卡数据，点击【编辑】，打开编辑虚卡配置对话框。

参数说明：

- 虚拟网卡名称：配置虚卡名称
- 虚拟网卡 IP：配置虚卡 IP 地址
- 子网掩码长度：配置子网掩码，默认 24
- tcp 端口：配置 tcp 端口
- udp 端口：配置 udp 端口
- 端口启用：选择开启 tcp 或 udp 端口，默认开启 tcp 端口

点击【保存】即可完成编辑虚卡配置

虚卡生效：

点击【虚卡生效】，实现虚卡配置重启。

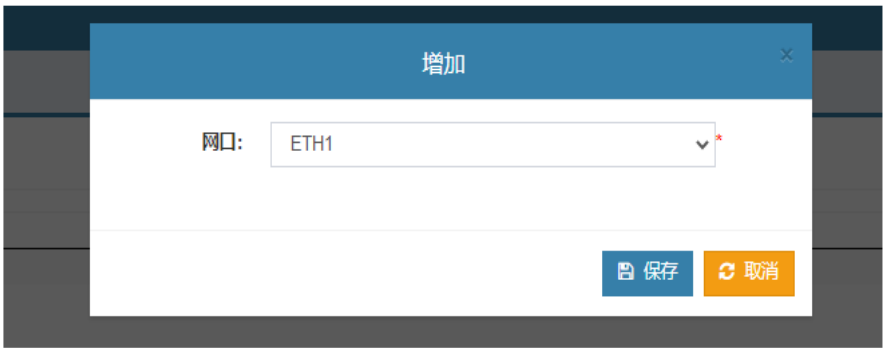
3.4.5 映射配置

功能说明：将安全接入网关收到的数据进行解析处理后，发送给真实的网络资源，安全接入网关的 SSL 用户所分配的虚拟 IP 为 10.0.0.0/24 即最大 254 个用户。

以系统管理员身份登录管理页面，选择【SLVPN 设置 > 映射配置】，进入映射配置页面。

新增/编辑映射配置：

点击【新增】，打开新增映射配置对话框。



参数说明：

- 网口：L3VPN 资源对应的网口。以安全接入网关默认网络配置为例，若资源是 192.168.17.0/24 网段的，此时的网口选择 ETH1

点击【保存】即可完成新增映射配置。

删除映射配置：

选中要删除的映射配置，点击【删除】，在打开的确认对话框中点击【确认】，即可删除该映射配置。

3.5 SSL卸载设置

3.5.1 SSL卸载

SSL卸载功能是将http服务映射成https服务的模块。目前认证了红莲花浏览器，分为国际和国密。

进入SSLVPN设置菜单，单击SSL卸载，进入SSL卸载管理页面。

单击【新增】按钮，弹出新增映射窗体，选择新增国密或者国际

国密：

国际：

在SSL卸载管理页面点击【编辑】按钮可以修改配置信息。配置完成后点击【生效】按钮来重启服务使配置生效。防火墙需要放开资源IP、本机映射端口，或者使用默认开

放端口18500-18800

注意

限制：资源如果在通过卸载端口访问后会自行重定向到另一个网址，那么新的网址将不会被继续卸载

3.6 IPSEC VPN设置

IPsec（IP Security）是IETF制定的三层隧道加密协议，它为Internet上传输的数据提供了高质量的、可互操作的、基于密码学的安全保证。特定的通信方之间在IP层通过加密与数据源认证等方式，提供了以下的安全服务：

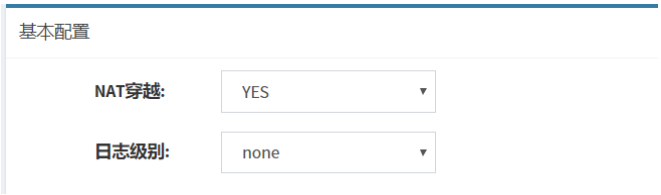
- 数据机密性（Confidentiality）：IPsec 发送方在通过网络传输包前对包进行加密
- 数据完整性（Data Integrity）：IPsec 接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改
- 数据来源认证（Data Authentication）：IPsec 在接收端可以认证发送 IPsec 报文的发送端是否合法
- 防重放（Anti-Replay）：IPsec 接收方可检测并拒绝接收过时或重复的报文

配置IPSEC连接需要至少两台安全接入网关。

3.6.1 基本设置

功能说明：该功能提供配置IPSEC的基本设置。

以系统管理员身份登录系统，选择【IPSECVPN设置 > 基本设置】，打开基本设置页面。



参数说明：

- NAT 穿越：是否需要穿越网络
- 日志级别：IPSEC 服务产生的日志等级

点击【保存】，完成基本设置的配置。

3.6.2 连接管理

功能说明：连接管理提供IPSEC隧道的具体配置信息。

以系统管理员身份登录管理页面，选择【IPSECVPN设置 > 连接管理】，进入连接管理界面。

新增SA策略：

切换到SA策略tab页，点击【新增】，在打开的新增SA策略页面填入相关配置：

新增保护节点：

切换到保护节点tab页，点击【新增】，在打开的新增保护节点页面填入相关配置：

新增IPSEC连接：

切换到IPSEC连接tab页，点击【新增】，在打开的新增IPSEC连接页面填入相关配置：

注意

两台安全接入网关配置的内部子网地址不能重复

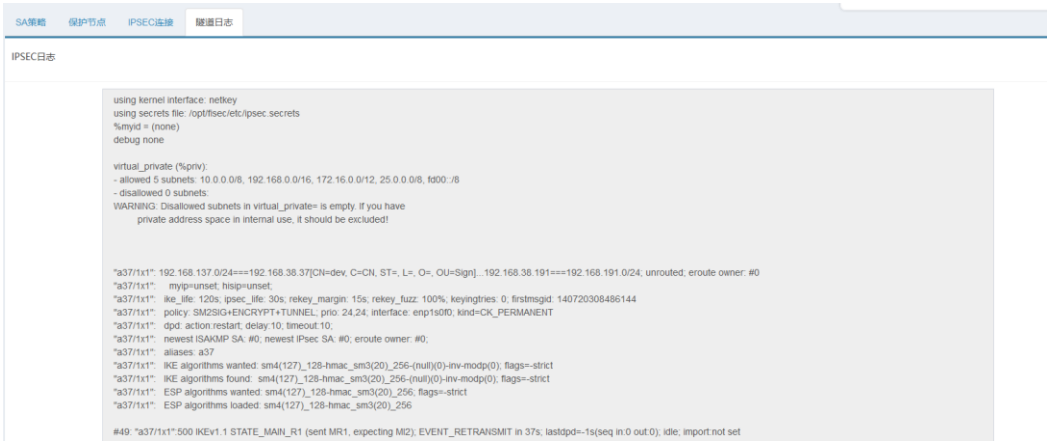
两端子网内的设备需要将默认网关设置为各自连接的安全接入网关的网口地址

删除连接/保护节点/SA策略：

选中要删除的数据，点击【删除】，在弹出的确认删除提示框中点击【确定】，即可删除该连接。

查看隧道日志：

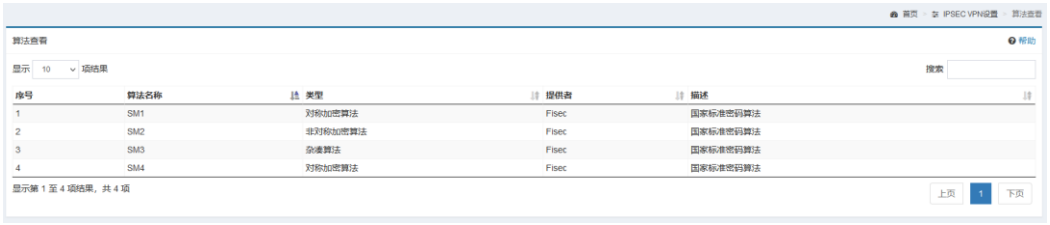
切换到隧道日志tab页，可查看隧道日志



3.6.3 算法查看

功能说明：算法查看提供IPSEC服务支持的国密算法类型查看。

以系统管理员身份登录系统，选择【IPSECVPN设置 > 算法查看】，打开算法查看页面。



3.7 系统维护

3.7.1 日志管理

功能说明：用于查看设备的运行日志。运行日志包括管理日志和用户日志两种类型。选择要查看的日期，会显示相应时间下的日志记录，同时可以对日志进行审计和验签。

以审计管理员身份登录管理系统，选择【系统维护 > 日志管理】，进入日志管理页面。

参数说明：

- 日志类型
  - 管理日志：记录管理员操作的日志
  - 用户日志：记录用户在客户端上的操作日志
- 日期：点击可以选择查看指定时间的日志，选择好时间后点击刷新

- 查看全部：可以显示当前选择的日志类型下系统中所有时间的日志
- 导出日志：导出当前选择的日志类型下在页面上显示的所有日志
- 清除日志：清除当前选择的日志类型下一段时间内的所有日志

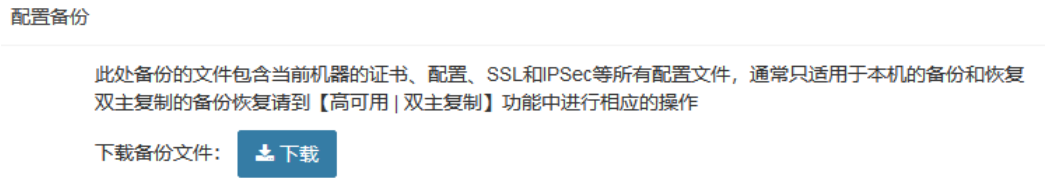
3.7.2 备份/恢复

功能说明：备份/恢复功能可以备份数据库及相关配置文件，并可以恢复已备份的文件。

以系统管理员身份登录管理页面，选择【系统维护 > 备份/恢复】，打开备份/恢复页面。

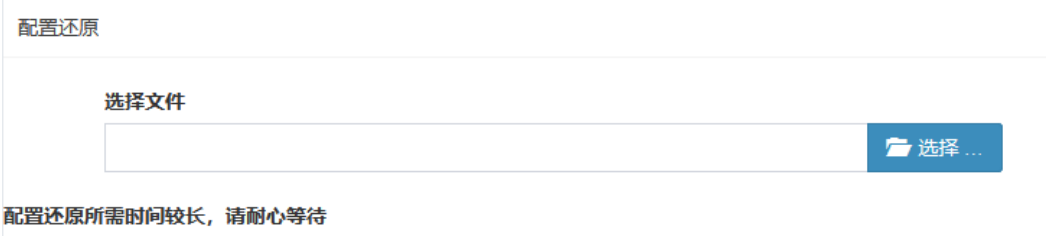
3.7.2.1 配置备份

点击【下载】。可以将相关服务的配置文件及数据库等文件备份成备份文件并下载到终端。



3.7.2.2 配置还原

选择要恢复的备份文件，点击【上传】即可恢复相关配置文件及数据库。



3.7.3 重启/关机

功能说明：重启/关机功能提供重启、关闭安全接入网关、恢复出厂，查看系统版本等功能。

以系统管理员身份登录管理页面，选择【系统维护 > 重启/关机】，进入重启/关机页面。

3.7.3.1 重启/关机

注意

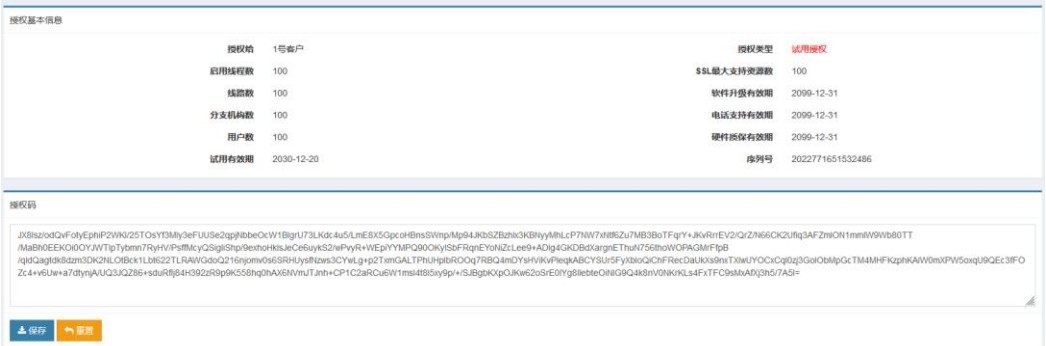
不建议在这里重启安全接入网关，管理页面上的【重启设备】可能造成安全接入网关内部的加密卡出现异常，若需重启设备，可点击【关闭设备】，待设备充分放电（面板上的灯全部熄灭）后再开机

3.7.3.2 查看系统版本信息

3.7.4 授权码管理

功能说明：查看授权信息和更新授权码。

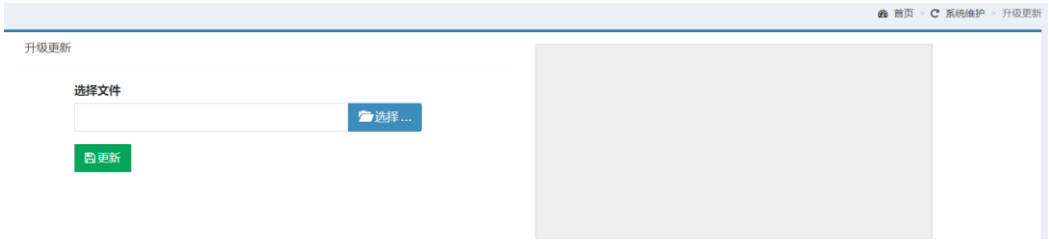
以系统管理员身份登录管理系统，选择【系统维护 > 授权码管理】，打开授权码管理页面。



授权基本信息：
可以查看授权的用户数和有效期等信息。
授权码：
在输入框中填入合法的授权码，然后点击【保存】按钮，可以对授权码进行更新。

3.7.5 升级更新

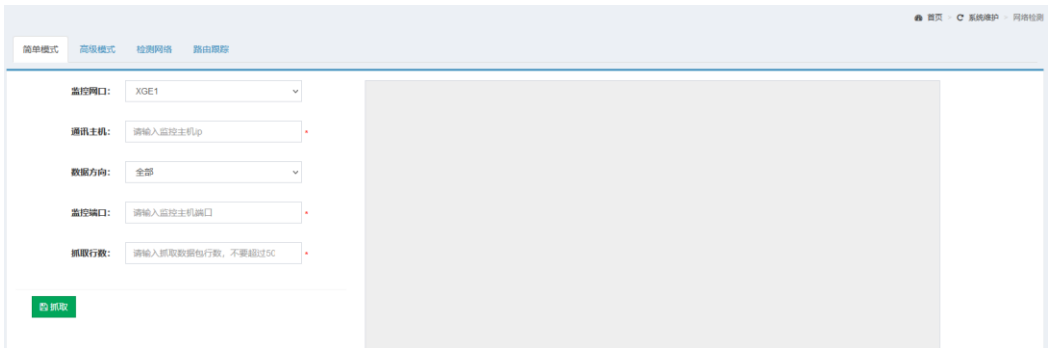
功能说明：升级更新页面提供对安全加密网关功能的升级操作。
以系统管理员身份登录管理系统，选择【系统维护 > 升级更新】，打开升级更新页面。



上传正确的升级包文件后点击【更新】按钮进行升级。

3.7.6 网络检测

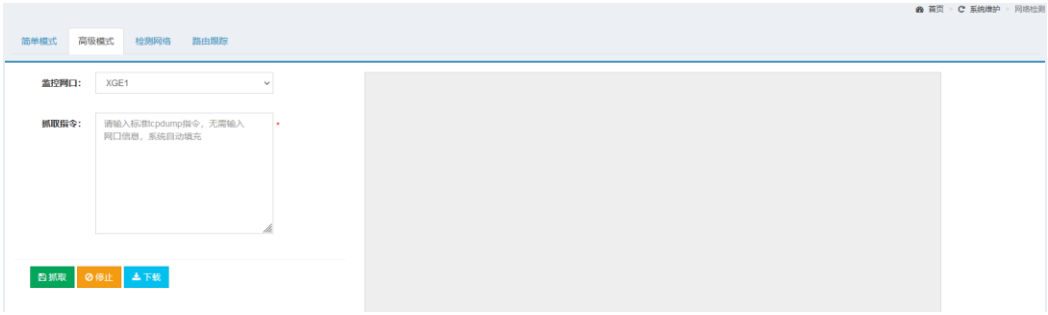
功能说明：网络检测页面提供对网口传输网络数据功能的抓包操作。
以系统管理员身份登录管理系统，选择【系统维护 > 网络检测】，打开网络检测页面。
简单模式：



参数说明：

- 监控网口：选择要监控抓包的网口
- 通讯主机：填写要监控的主机 IP
- 数据方向：选择抓取数据传输方向
- 监控端口：填写要监控的主机端口
- 抓取行数：填写抓取数据包行数

点击【抓取】，完成数据包抓取操作。
高级模式：

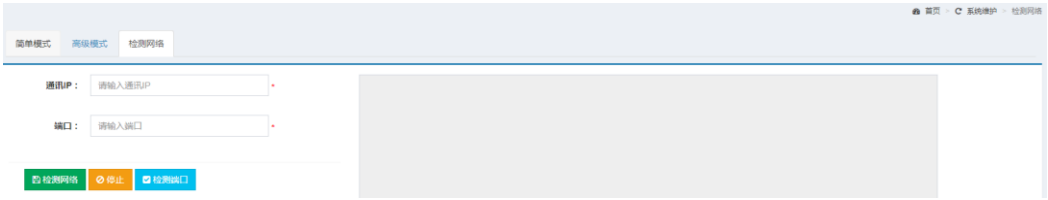


参数说明：

- 监控网口：选择要监控抓包的网口
- 抓取命令：填写标准 tcpdump 指令

点击【抓取】，完成数据包抓取操作，点击【下载】，完成数据包下载操作。

监测网络：

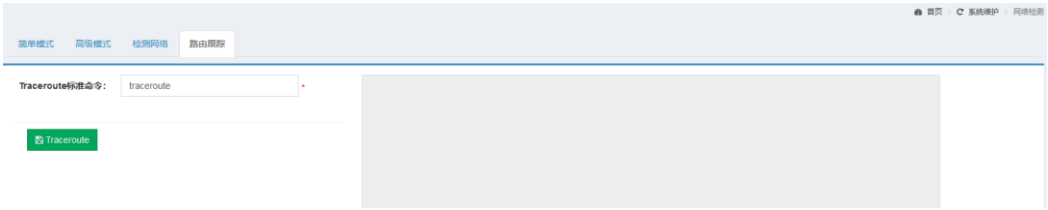


参数说明：

- 通讯 IP：填写要检测的网络 IP
- 端口：填写要检测的网络端口

点击【检测网络】，完成网络地址检测操作，点击【检测端口】，完成网络端口检测操作。

路由跟踪：



参数说明：

- 目的 IP：填写要跟踪的目的 IP

点击【Traceroute】，完成路由跟踪操作。

3.7.7 密钥备份/恢复

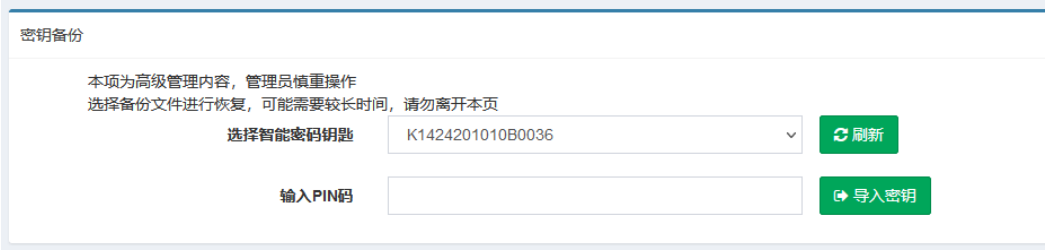
功能说明：密钥备份/恢复功能可以将加密卡中的密钥备份出来，也可以将备份的密钥恢复到加密卡中，备份和恢复需要用到5把智能密码钥匙。

以安全管理员身份登录管理页面，选择【系统维护 > 密钥备份/恢复】，打开密钥备份/恢复页面。

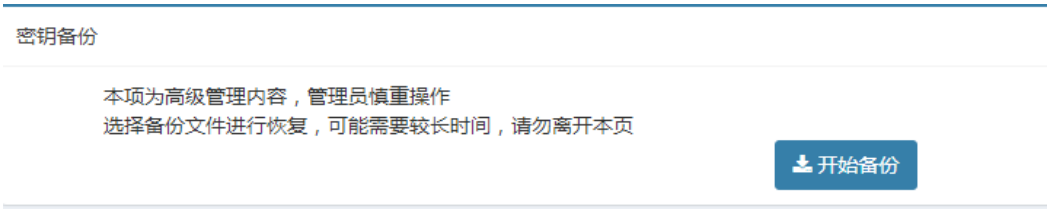
3.7.7.1 密钥备份

点击【备份初始化】，分别插入5把智能密码钥匙，点击【刷新】选中要使用的智

能密码钥匙，输入PIN码值，点击导入密钥，此时会将密钥导入智能密码钥匙中。

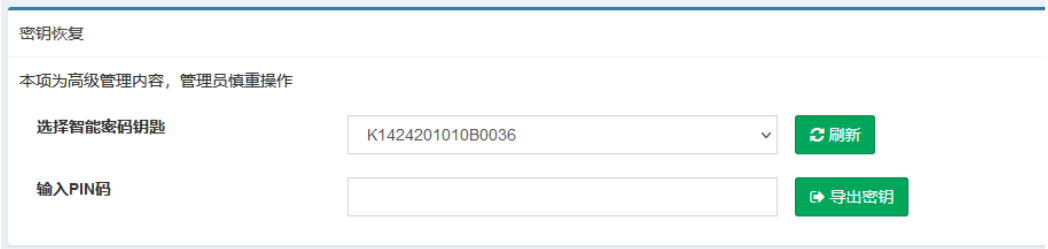


上述操作进行5次后，会出现【开始备份】按钮，点击【开始备份】，即可下载备份文件。

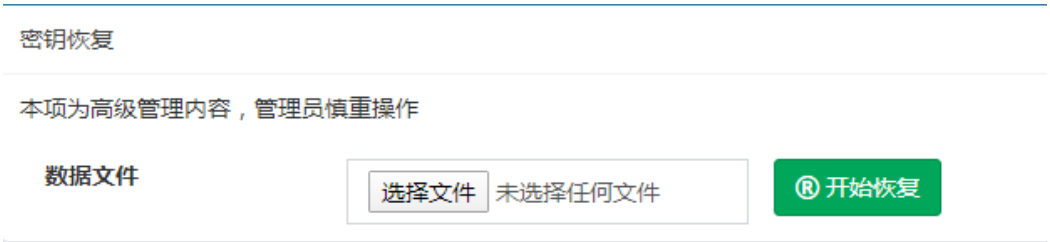


3.7.7.2 密钥恢复

备份密钥时备份了5把智能密码钥匙，恢复时只需要其中的3把智能密码钥匙，分别插上3把智能密码钥匙，输入对应PIN码，点击导出密钥。



3把智能密码钥匙验证通过后，会出现上传备份文件的文本框，选择备份文件后点击【开始恢复】，即可完成密钥恢复。



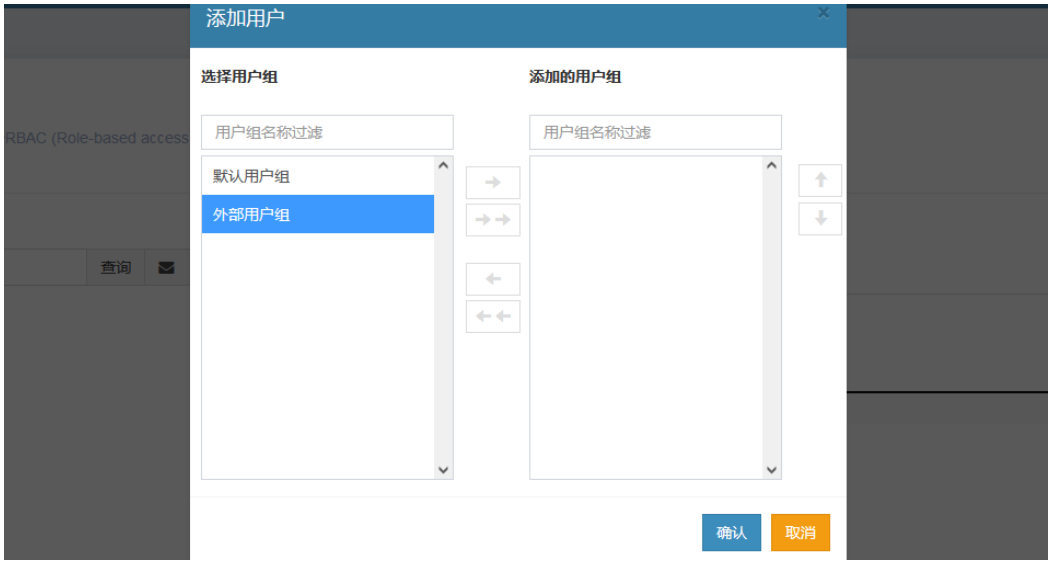
3.8 单点登录

3.8.1 应用管理（SSL）

功能说明：应用权限管理基于RBAC（Role-based access control，基于角色的访问控制），对不同的业务系统进行细粒度的权限控制。此功能用于配置客户端应用以及与用户、角色的绑定关系。

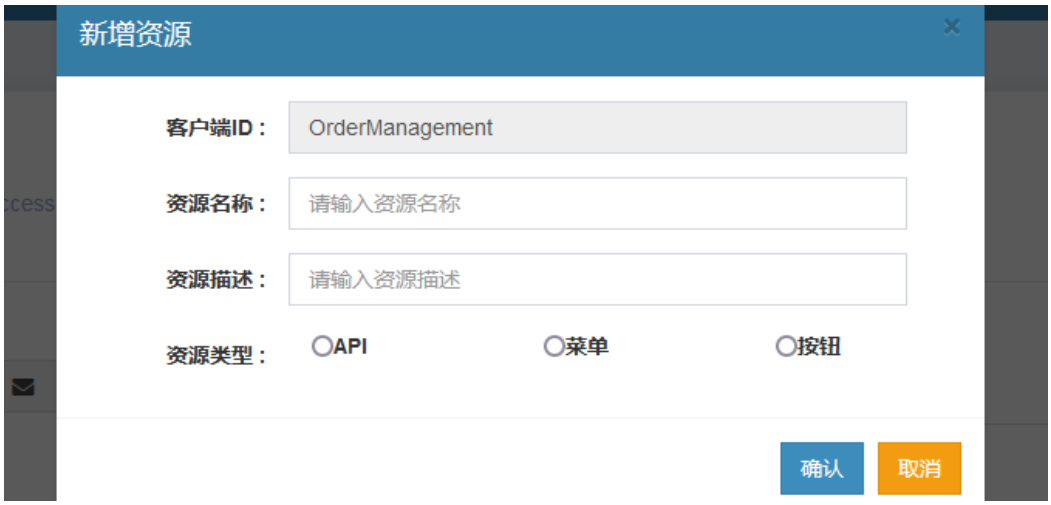
新增客户端应用：

添加用户组：



添加角色：

添加资源：



添加授权：

3.8.2 LDAP同步

功能说明：LDAP（Lightweight Directory Access Protocol）轻量目录访问协议可以用来管理用户、用户组等，在对接了 LDAP 服务器后，可以从 LDAP 中同步用户信息到 SSLVPN 中。

3.8.2.1 配置信息和导入用户

配置LDAP信息：

用户同步字段映射：

用户组配置：

自动导入配置：

3.8.2.2 同步历史

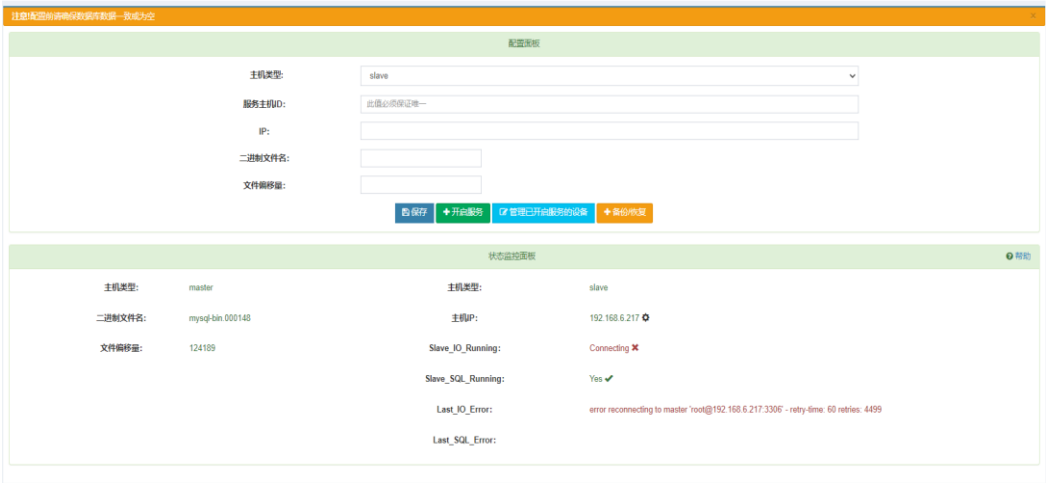
3.9 高可用

3.9.1 双主复制

功能描述：双主复制配置2台服务器MySQL数据库数据同步，在配置好的任何一个库中写入或删除数据，都会同步到另一台机器中，实现了数据库MySQL服务器的热备，结合keepalived的动态切换，实现了自动检查，失败切换机制，实现了MySQL数据库高可用方案。

配置操作：打开双主复制界面，在两台设备上分别点击【开启服务】，输入对端IP，保存。

在其中一台中选择master，填写服务主机ID（不能和从机相同），填完后，点击保存，生成二进制文件名和文件偏移量；然后转到另一台设备，选择slave，填入一个不同的ID,并填写对端主机的IP,以及刚生成的二进制文件名和文件偏移量,点击【保存】。



然后再以这台设备为master，另一台为slave，重复配置一遍，即可完成双主复制配置，这时候SSLVPN相关的用户，资源等就可以互相同步。

管理已开启服务的设备：操作防火墙，开启关闭或者删除。

备份恢复：备份SSLVPN相关内容，并恢复。

3.9.2 keepalived

功能说明：两台完全相同的服务器，使用同一个虚拟IP提供服务，一台为主服务器，另一台作为备服务器. 当主服务器出现故障时，备服务器通过心跳检测到主服务器出现故障，接管主服务器工作，保证不影响应用正常使用. 并在联网的条件下向指定邮箱发送告警邮件；另外通过lvs，实现负载均衡配置以及查看负载节点状态。

3.9.2.1 实例配置

单击【增加实例】，打开窗口，输入相关信息，即可配置keepalived实例。

参数说明：

- 实例名称：keepalived 实例名
- 心跳检测网卡：检测这个网卡是否通，来判断 keepalived 是否切换，一般和实例绑定网卡相同
- VRID 标识：主机和备机必须相同
- 优先级：数值越大，优先级越高
- 虚拟 IP，子网掩码：keepalived 虚拟出的虚拟 IP 和掩码
- 实例绑定网卡：虚拟 IP 绑定的网卡
- 心跳包检测间隔：心跳包的检测时间间隔，判断节点是否在线
- 是否采用非抢占式：如果非抢占，则主机挂了之后切到备机，主机恢复后不会再把虚拟 IP 抢占回来；如果抢占式，主机则会抢占

点击【保存】，完成实例的配置。

若需要生效配置，则点击【配置生效】按钮（修改其他标签中的内容后也需配置生

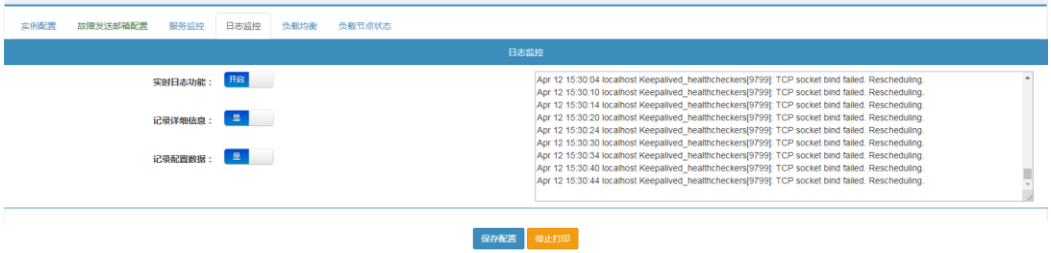
效）

3.9.2.2 故障发送邮箱配置

在这里配置邮箱信息后，在主节点发生故障后可以发送报警邮件。需要连接外网并且在邮箱中配置smtp服务。

3.9.2.3 日志监控

这里可以实时监控keepalived的日志信息，方便调试。

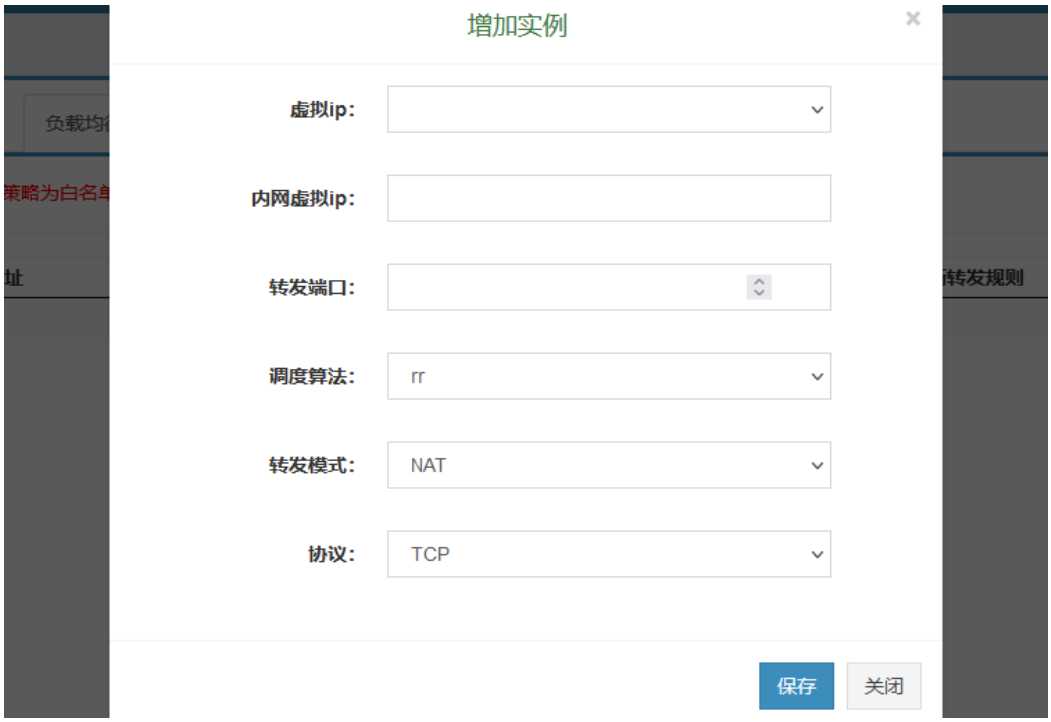


点击【停止打印】，即可不输出。

3.9.2.4 负载均衡

这里可以配置负载均衡，将请求分发到多个真实服务器。一定注意防火墙配置：如果系统防火墙策略为白名单，请先到防火墙模块配置负载机器允许客户端、真实服务数据通过，或者使用默认开放端口18500-18800。

点击【增加实例】，打开负载均衡实例配置界面：



参数说明：

- 虚拟 ip：keepalived 实例配置中配的虚拟 ip
- 内网虚拟 ip：keepalived 实例配置中配的内网虚拟 ip
- 转发端口：虚拟 ip 的端口，一般和真实服务器的端口相同
- 健康检测时间间隔：检测真实服务器状态的时间间隔
- 调度算法：lvs 调度算法
  - rr：轮询调度
  - wrr：加权轮询调度
  - lc：最小连接调度
  - wlc：加权最小连接调度
  - sh：源地址哈希
  - dh：目的地址哈希
- 转发模式：lvs 的工作模式，目前仅支持 NAT
- 协议：TCP 或 UDP

点击【保存】保存实例配置。然后点击实例旁边的加号，打开增加真实服务器窗口。

参数说明：

- 被负载 VPN 管理页面地址：填写真实服务器的 web 地址，如：https://192.168.6.100:8181/
- 端口：真实服务器服务端口，默认为 SSL 服务的端口（8443，18443，28443，38443）
- 权重：数值。用于加权的调度算法
- 检查方式：和实例的协议一致

添加完负载均衡后，需要点击实例配置下的【配置生效】按钮，才可生效。

3.9.2.5 负载节点状态

在这里可以查看真实服务器的负载状态。

4 用户页面及客户端

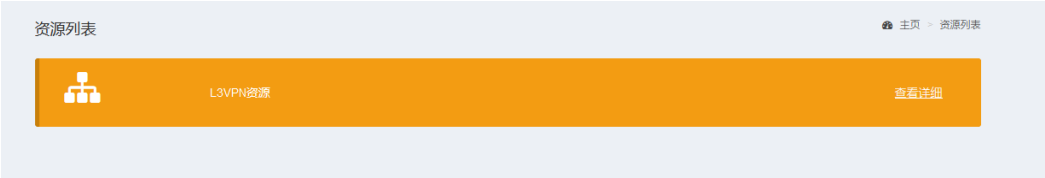
4.1 用户界面

管理员在管理端添加用户及资源后可在用户页面进行访问，默认用户页面访问地址为https://192.168.18.199:9494，可以使用用户名密码或者智能密码钥匙进行登录。

4.1.1 用户登录

4.1.2 资源查看

登录用户页面后可以看到当前用户被分配的资源列表，点击查看详情可以看到具体的资源配置。



4.1.3 修改用户密码

点击右上方的头像，选择【配置】，在弹出的对话框中可以修改用户密码。

4.2 客户端

4.2.1 客户端安装

使用管理员权限运行安装程序，安装完成后出现登录页面。

4.2.2 客户端登录

客户端安装完成后需要修改客户端访问VPN的IP及端口号，点击网络设置，修改服务器IP及web端口中的IP地址为VPN对应网口的IP，端口号默认8443，点击保存。配置完成网络后，用户可以通过智能密码钥匙，用户名密码及用户证书的方式登录客户端。

登录成功后可以看到用户拥有的tcp资源，此时可以访问此资源。可以通过右击状态栏的客户端图标，点击查看资源再次打开此界面

4.2.3 打开 SSO 登录

点击设置界面中的登录设置，打开启用SSO的开关，在登录功能后可显示统一身份门户URL，点击即可打开统一身份门户。

客户端打开SSO：

登录成功后显示统一身份门户 URL：


VPN已开启
统一认证登录：http://192.168.27.199:8000/login
资源名称
资源
test
192.168.27.0/24
VPN已开启
资源检测

统一身份认证门户：


192.168.27.199:8000/clientApplication/applicationManager
论坛
Sign in · GitLab
RDSystem
RDTemplate - Revisi...
用户登录 - 禅道
我的视图 - MantisBT
明鉴漏洞扫描系统
零信任统一身份认证网关
首页 / 客户端应用 / 应用管理
客户端应用
应用管理
首页
应用管理
a
应用跳转

5 常见问题及解答

5.1 数据信息查询失败

问：管理系统无法查询用户数据信息？

答：登录成功之后，长时间没有操作，Session超时导致自动退出，接口访问端口被修改，未重新登录。须重新登录查询数据信息。

5.2 绑定uKey失败

问：新增用户，创建uKey登录无法选择智能密码钥匙？

答：创建uKey登录，需要在IE浏览器下登录，创建。

5.3 登录失败

问：管理员新增用户登录失败？

答：用户名/密码登录：用户是否具有用户名/密码登录权限，用户账号是否过时，对账号重新赋予时间权限。用户密码是否被修改，须按新密码重新登录。

uKey登录：用户是否具有uKey登录权限，uKey登录中，用户是否已绑定Ukey创建证书，证书是否过期，若证书过期，用户须重新创建Ukey更新证书。

证书登录：证书是否过期，用户是否具有证书登录权限，赋予证书登录权限或更新数字证书，重新登陆。

5.4 用户连接失败

问：用户登录连接失败，无法正常登录？

答：首先确认连接地址是否正确，登录账号是否正确，确认无误的情况下，确认服务端是否正常启动。

5.5 用户登录提示“用户无权限登录”

问：用户系统登录时提示“用户无权限登录”

答：用户在创建时不使用默认用户组，改用其他用户组新建用户。