
NetKeeper-2000 纵向加密 认证网关技术说明书

南京南瑞集团公司

注意：

本白皮书中的内容是南瑞纵向加密认证关技术说明书。本材料的相关权利归南瑞集团公司所有。技术说明书的任何部分未经本公司许可，不得转印、影印或复印。

NetKeeper-2000 纵向加密认证网关 技术说明书

Version1.0 2007-5-8

南瑞集团公司

All rights reserved

本资料将定期更新，如预获取最新相关信息，

请访问南瑞集团公司网站：<http://www.nari-china.com>

您的意见和建议请发送至：corba@vip.sina.com

南瑞集团公司

南京南瑞路 8 号，210003

电话（TEL）：025-83096601(市场部)

025-83096702(技术支持)

传真（FAX）：025-83096701

一、产品介绍	1
二、产品分发与安装	2
三、加密认证网关配置管理	3
3.1 系统初始化	3
3.1.1 通信初始化.....	3
3.1.2 初始化向导.....	5
3.2 证书申请.....	10
3.3 安全管理	11
3.3.1 人机卡认证.....	11
3.3.2 操作员卡口令修改.....	12
3.3.3 证书管理.....	12
3.3.4 远程监控.....	13
3.4 安全策略配置	14
3.4.1 系统信息配置.....	14
3.4.2 网络信息配置.....	14
3.4.3 路由信息配置.....	15
3.4.4 装置管理信息配置.....	15
3.4.5 隧道配置.....	16
3.4.6 策略配置.....	17
3.4.7 地址转换配置.....	18
3.5 隧道信息查询	18
3.6 系统调试	19
3.6.1 网关硬件诊断.....	19
3.6.2 SPING 调试.....	20
3.7 日志管理	21
四、典型应用环境配置案例	22
4.1 明通模式配置	22
4.1.1 系统配置.....	22

4.1.2 网络配置.....	23
4.1.3 路由配置.....	23
4.1.4 隧道配置.....	24
4.1.5 策略信息配置.....	24
4.2 同一网段配置	25
4.2.1 系统配置.....	25
4.2.2 网络配置.....	26
4.2.3 隧道配置.....	26
4.2.4 策略配置.....	27
4.3 路由模式配置	27
4.3.1 系统配置.....	28
4.3.2 网络配置.....	28
4.3.3 路由配置.....	29
4.3.4 隧道配置.....	29
4.3.5 策略配置.....	30
4.4 VLAN 环境配置.....	30
4.4.1 系统配置.....	31
4.4.2 网络配置.....	31
4.4.3 路由配置.....	32
4.4.4 隧道配置.....	32
4.4.5 策略配置.....	33
4.5 NAT 模式配置	33
4.5.1 系统配置.....	34
4.5.2 网络配置.....	34
4.5.3 路由配置.....	35
4.5.4 隧道配置.....	35
4.5.5 地址转化配置.....	35
4.5.6 策略配置.....	37
4.6 双进双出配置	37

4.6.1 系统配置.....	38
4.6.2 网络配置.....	38
4.6.3 路由配置.....	39
4.6.4 隧道配置.....	40
4.6.5 策略配置.....	41
五、证书签发说明	错误！未定义书签。

一、产品介绍

NetKeeper-2000 纵向加密认证网关用于电力控制系统安全区 I/II 的广域网边界保护，为网关机之间的广域网通信提供具有认证、与加密功能的 VPN，实现数据传输的机密性、完整性保护。

加密网关的硬件结构框图如下图所示，硬件系统基于 RISC 体系结构的嵌入式微处理器(Motorola PowerPC)，嵌入式主板集成四个以太网接口：分别是内网接口、外网接口、双机热备接口、日志告警接口；配置串口用于对加密认证网关进行监控管理，支持采用专用智能 IC 卡接口进行身份验证，保证配置管理的安全性；电力专用密码卡单元(内嵌电力专用密码算法和 RSA 公私密钥算法)对网络通信数据进行加密与认证；双机接口支持加密认证网关的双机热备和链路冗余备份，避免重要数据的丢失；硬件看门狗时刻监控系统状态，保证加密认证网关稳定、可靠运行。

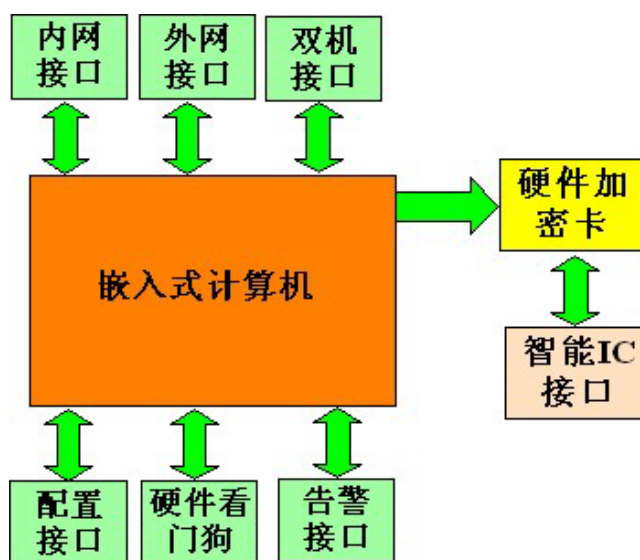


图 1.1 加密网关硬件结构框图

加密网关的的前面板图有 8 组指示灯，分别是电源指示灯（Power）、告警灯（Alarm）、加解密指示灯（Encrypt Status/Action）、读写器指示灯（CRW Status/Action）、内网网络接口指示灯（Eth0 Status/Action）、外网网络接口指示灯（Eth1 Status/Action）、双机热备接口指示灯（Eth2 Status/Action）、日志接口指

示灯 (Eth3 Status/Action)。电源指示灯标识网关电源的工作状态,红灯亮表示电源模块工作正常 ;告警灯亮并伴有声音告警表示加密认证网关受到不明网络报文网络恶意攻击,管理员可以通过日志信息判断攻击的种类 ;加解密 Status 亮表示加密网关内置有电力专用数据密码卡,加解密 Action 灯闪烁表示密码卡正在加解密数据 ;智能读写器 Status 灯亮表示加密认证网关智能读写器插槽中有智能 IC 卡,智能读写器 Action 灯闪烁表示数据正在被读取。四组网络接口 Status 灯亮表示网口与网络正确连接,网络接口 Action 灯闪烁表示网卡数据正在接收或发送。

加密网关的后面板图设计有双电源,有一个电源作为主电源供电,一个作为辅电源作备份,这种设计可以有效地提高电源工作的可靠性及延长整个系统的平均无故障工作时间,最右边是电源开关 1,然后是电源插座 1,电源开关 2,电源插座 2 ;Console 口用来对加密网关进行监控 ;内网网口 (Eth0)用来连接内网,外网网口 (Eth1)用来连接外网外网,双机接口 (Eth2) 用于加密网关的双机热备份,日志接口指示灯 (Eth3) 用于加密网关的日志报警,也支持采用网络方式对加密网关进行配置管理。

二、产品分发与安装

NetKeeper-2000 纵向加密认证网关完整的产品分发包包括硬件和软件两大部分。用户在使用本产品时,应先检查硬件产品是否具有 NARI 标志,外观是否有损坏现象。如有以上现象,请勿使用并及时与本公司取得联系,处理相关事宜。为了产品稳定、可靠的运行,请勿私自打开加密认证网关机箱。

加密认证网关随机带有一张配置软件安装光盘、一根网络配置线、一根串口配置线,用于在安装 Windows2000/XP/NT/9x 操作系统的计算机上配置加密网关。安装完成后,启动配置管理软件,软件界面如图 2.1 所示。



图 2.1 加密网关配置软件

三、加密认证网关配置管理

3.1 系统初始化

加密认证网关投入使用前，须首先进行设备的初始化操作，初始化操作的内容包括安装调度证书服务系统根证书、装置管理系统的设备证书、本装置的主备操作员证书、与本装置通信节点的设备证书以及本装置的设备私钥。上述证书由调度证书服务系统生成并签名，存储在纵向加密认证网关中。

3.1.1 通信初始化

- 1) 将本地配置计算机地址设置为 11.22.33.43，掩码为 255.255.255.0，用随机附带的网络配置线（交叉线）连接到加密认证网关的配置接口(eth3)。
- 2) 首次启动加密认证网关的配置软件，出现如下的软件主界面：



图 3.1 加密认证网关配置软件启动界面

- 3) 软件系统会自动和加密网关服务程序建立连接，并提示成功或是失败消息。配置软件进行 **5 次重连操作**，如果都失败，则程序自动退出，并提示用户检查网线连接或重新启动加密网关，如下图所示。



图 3.2

- 4) 成功连接后，系统会提示用户插入密钥管理卡。插入密钥管理卡后，点击“确定”，则程序会自动检测当前加密网关是否已经创建过密钥管理卡，并进行相应的提示。

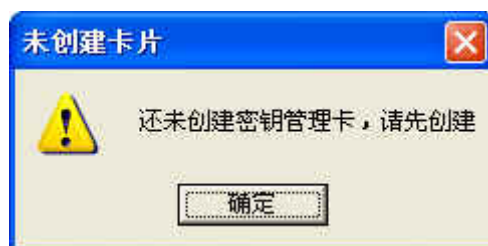


图 3.3

如果是首次执行初始化操作，则需要创建密钥管理卡，系统将自动弹出初始化向导，引导用户一步步的进行设置，最后完成整个系统的初始化过程，在以后的系统维护中，也可以利用向导跳过某些步骤更新某些文件，下面介绍加密网关的初始化向导。

3.1.2 初始化向导

初始化向导第一步主要提示用户需要进行的初始化步骤，主要如下图所示（以下过程结合电力二次系统实际情况进行描述）：

1. 生成密钥管理卡和装置密钥对，并对装置密钥进行保护、主备操作员卡两张，并制作导出证书请求文件。
2. 导入调度 CA 根证书。
3. 导入网省调的根证书(中级证书)。
4. 导入装置管理系统证书。
5. 导入与本装置通信的对端节点设备证书。
6. 导入主操作员证书。
7. 导入备份操作员证书。

以上的步骤，第 1、2、6、7 是初始化过程必须的操作，不可以略过，其他的操作步骤由用户根据现场实际情况进行选择。



图 3.4 初始化向导步骤

- 1) 生成密钥管理卡和装置公私密钥对，以及操作员卡的公私密钥对。如下图所示。



图 3.5 证书请求文件生成

点击硬件类型中的加密网关 → “生成密钥保护卡/装置密钥对”，创建密钥管理卡和网关公私密钥对，如图 3.6 所示。网关系统自动用生成的密钥保护卡对设备密钥进行保护。



图 3.6 装置密钥对生成

成功创建密钥管理卡后，系统会提示是否成功的信息。

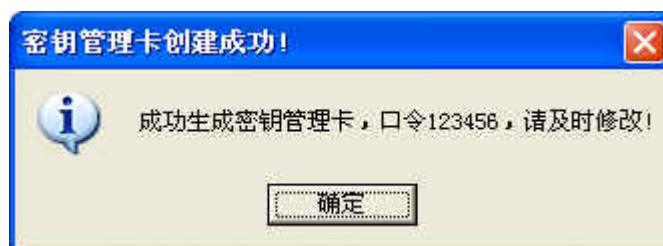


图 3.7

- 2) 制作加密网关设备证书请求文件。点击“制作证书请求”按钮，则弹出填写设备证书请求的对话框，如下图所示：



图 3.8

按照上述说明填写后，点击“生成证书请求”按钮，将生成的证书请求文件保存在本地安全存储介质中并提交给调度证书管理系统进行签发。具体签发过程请参见 3.2 节证书申请。

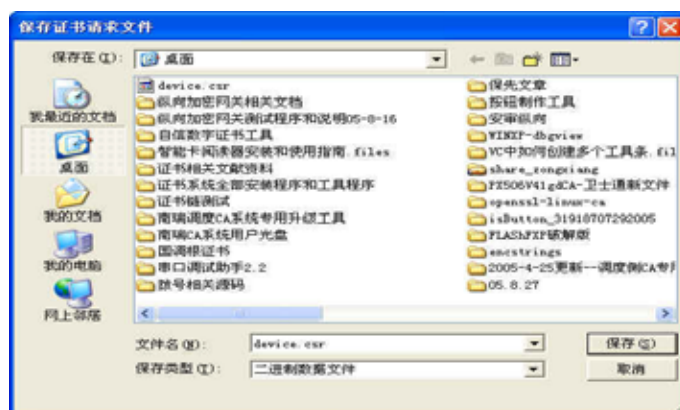


图 3.9

与此类似，“操作员卡(包括主、备操作员卡)密钥对生成”也是按照类似的步骤,先产生操作员卡密钥对，然后生成证书请求文件并提交调度证书服务系统签发。

3) **导入调度 CA 的根证书。**这是后续对其他实体证书进行验证的基础 ,如图 3.10 所示,选择 CA 根证书并且导入，则系统会提示成功验证与否，如图 3.11 所示。



图 3.10



图 3.11

4) 导入中级 CA 证书(网省调证书)。



图 3.12 导入中级证书

5) 导入和本地加密网关通讯的对端设备证书。



图 3.13 导入对端设备证书

6) 导入主、备操作员证书，如下图所示。



图 3.14 导入并验证主操作员证书



图 3.15 导入并验证备操作员证书

导入全部证书后，配置管理系统会自动进行探测，如前所述。先插入密钥管理卡，并进行登陆，系统会检查当前的初始化状态，判断装置是否正确初始化，并提示用户。

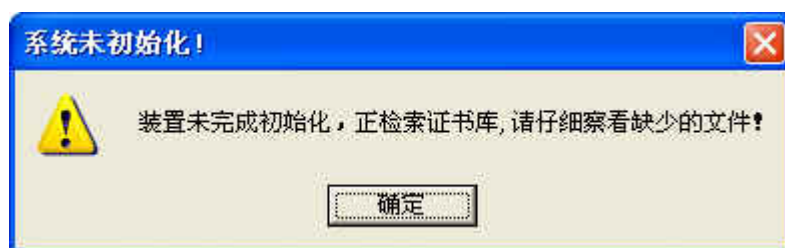


图 3.16

如果提示不成功，则会自动查询加密网关的证书列表并载出，如下图所示。背景显示为红色的即是未满足要求的字段项（注意：针对用户的不同情况，装置初始化的必要条件是装置已经生成了密钥保护卡，生成了装置 RSA 密钥对，并导入验证通过了的调度 CA 系统根证书、主操作员证书和备操作员证书，其他条件不是必需的）。

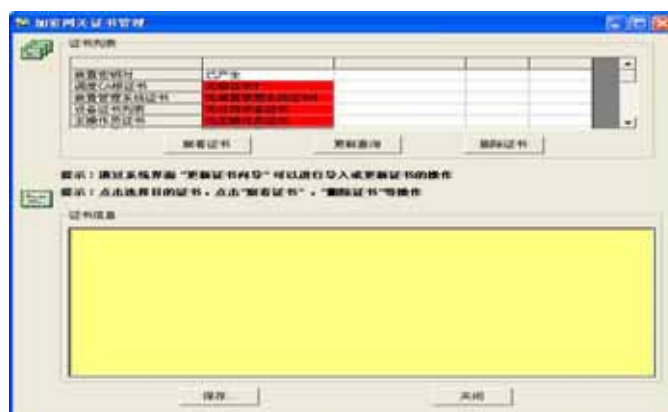


图 3.17 加密认证网关证书管理列表

3.2 证书申请

在加密认证网关初始化的过程中,需要将生成的加密网关证书请求文件和操作员卡证书请求文件提交给电力调度证书服务系统进行签发,生成网关设备证书和操作员卡设备证书。具体流程如下所述。

加密网关和操作员卡在生成证书请求文件后,将证书请求文件以可存储介质形式拷贝到各级调度证书系统上(国调、网调、省调),并以系统“录入员”身份用 UsbKey 登陆证书系统;选择“导入证书请求信息”按钮,点击“导入”按钮,则将请求信息输入到证书系统,根据电力证书系统操作规范的流程,经由“审核员”审核,“签发员”签发出设备证书和操作员证书。

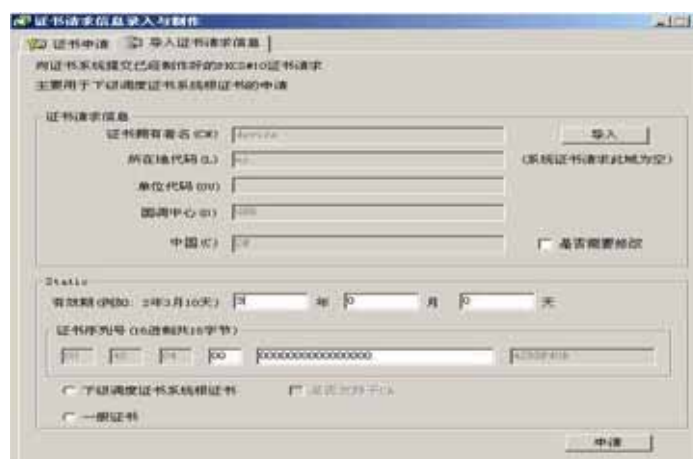


图 3.18 加密认证网关证书请求信息录入与制作

注:在不具备调度证书系统的条件下,可以采用配套光盘里的专用证书工具签发证书。具体使用请参考附录一《证书签发说明》

3.3 安全管理

加密认证网关的安全管理包括人机卡认证、操作员卡口令修改、证书管理、远程监控等。

3.3.1 人机卡认证

加密网关初始化完成后，需要插入密钥管理卡进行登陆管理。

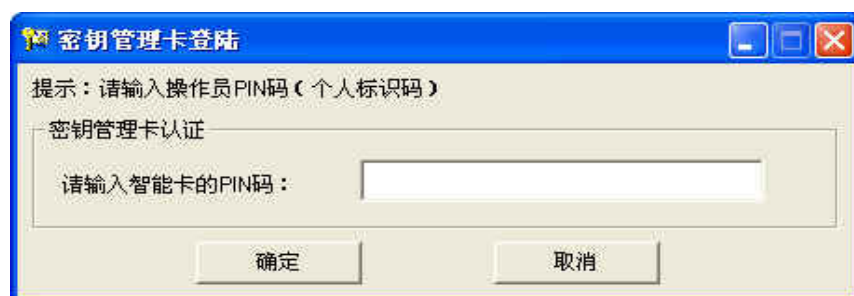


图 3.19

验证通过后，密钥管理卡将加密卡安全模块设置为可用状态，但此时使用权限还未放开，需要用户插入操作员卡，进行人机卡认证。加密网关配置管理程序的主界面如图 3.20 所示。用户首先插入操作员卡片，输入 PIN 码 (**初始 PIN 码为 006702**)，验证登录用户的合法性（**注意**，操作员卡必须由电力调度数字证书服务系统签发，内含标识操作员身份的信息）。只有成功登录后才能进行后续的隧道策略和规则配置，完成和对端的加密网关安全通讯设置。（**注意**，为了系统安全起见，输错三次 PIN 码将强行退出，防止非法用户尝试口令，同时，智能卡安全机制保证输错 3 次 PIN 码将锁死卡片，使其失效，必须重新发卡）



图 3.20 人机卡登录验证

3.3.2 操作员卡口令修改

密钥管理卡和操作员卡为了增强安全性，可以经常更换 PIN 码，点击 “卡片管理” → “修改密钥管理卡 PIN” 及 “修改操作员卡 PIN”，显示界面如下图所示：

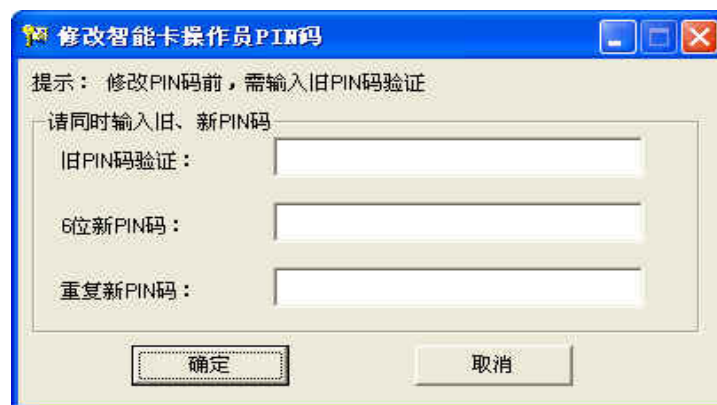


图 3.21 人机卡口令修改

用户首先必须输入旧的 PIN 码，待验证通过后，方可修改成新的 PIN 码。其中的人机认证流程和 3.3.1 节所述是一致的。

3.3.3 证书管理

装置在初始化和正常工作状态下，用户均可对装置的证书列表进行查询，以便对当前合法的证书列表进行管理。单击工具栏上的“证书管理”或者左侧导航栏中的“证书管理” → “证书查询”，系统会询问是否要查询，确认之后，如果加密网关内有合法 x.509 证书文件存在，则会自动导出其文件列表，如下所示。



图 3.22

证书文件列表导出后，加密网关配置管理程序会自动解析信息并且显示在当前证书管理界面上，如下图所示。（表示当前加密网关已经配置了 CA 根证书，主、备操作员卡证书，已经基本完成了初始化，处于工作状态。）

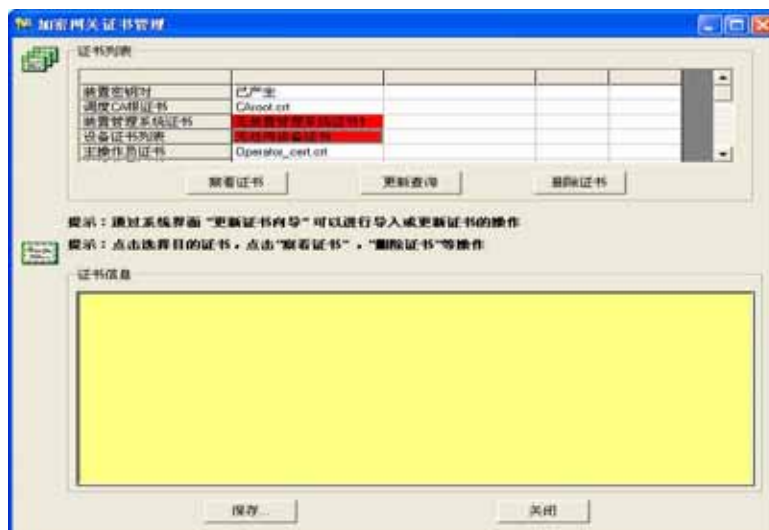


图 3.23 加密网关证书管理界面

选中目标证书，并点击“察看证书”按钮，则会显示证书详细信息，如下图所示。同样，选中目标证书，并点击“删除证书”按钮，将删除对应证书。

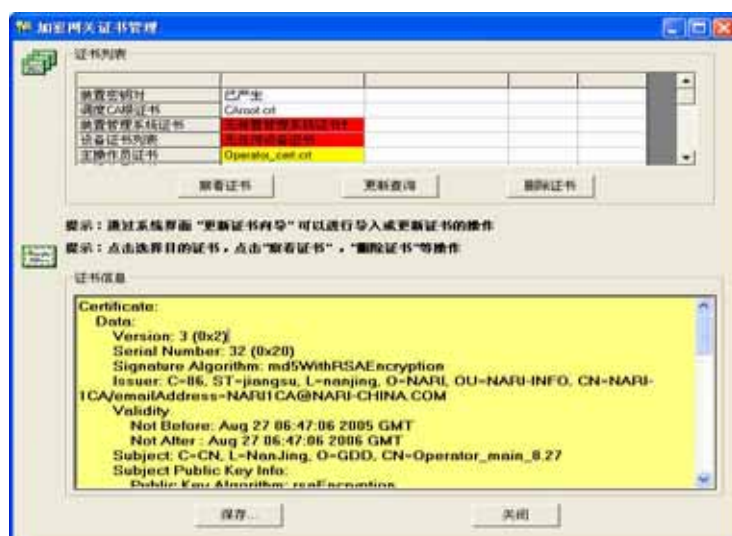


图 3.24 加密网关证书信息查询

3.3.4 远程监控

根据电力二次系统安全防护的规定和纵向加密认证装置的管理体制,加密认证网关支持远程集中监控管理。装置管理系统(管理中心)为调度中心所辖的加密认证装置提供远程安全管理服务。调度中心的加密装置及下属的加密装置由装置管理系统直接管理。此时,装置管理系统(管理中心)与加密装置是网络上通信的实体。装置管理系统通过经过认证加密的管理报文实现对纵向加密认证网关的监测。具体的监控内容及装置管理系统的使用见《加密认证网关装置管理系统用户使用手册》

3.4 安全策略配置

加密认证网关位于电力控制系统的内部局域网与电力调度数据网络的路由器之间，为透明安全防护装置。网关的内网接口连接内部局域网，外网接口连接数据网，每个网络接口可以设置一个或者多个虚拟地址。加密认证网关的安全策略设置主要包括系统配置、IP 地址配置、IP 路由，VLAN，规则，隧道信息，管理信息等。

3.4.1 系统信息配置

系统配置主要配置加密认证网关的系统信息，主要包括以下几个内容：

装置标识名：装置的名称，便于远程标识装置的基本信息。

默认策略：默认策略选项表示没有配置安全策略时对网络报文的处理方式，若选择丢弃则对不在规则范围内的报文直接丢弃，选择明通则对不在规则范围内的报文直接明通。

审计点位置：表示日志接收服务器所在位置，分为内网、外网。

审计地址：日志接收服务器的 IP 地址。

装置地址：加密认证网关发送日志报文的源地址，如果审计点位置为内网则该地址为装置内网虚拟地址，如果审计点位置为外网则该地址设为装置外网虚拟地址。

3.4.2 网络信息配置

加密认证网关共有 4 个网络接口，其中 eth0 接口连接内网，eth1 接口连接外网。eth2 和 eth3 接口为备用网络通道接口，其中 eth2 接口可以连接另一网段的内网，eth3 接口可以连接另一网段的外网。用户需要对加密认证网关的网络接口配置虚拟地址以便和内外网进行通信，内外网虚拟地址可以为相同网段，也可以为不同网段。

网络标识：加密认证网关可以处于多个网络中，支持设置多个虚拟地址，网络标识方便用户判断装置所在的网段信息。

内网虚拟地址和内网掩码：内网虚拟地址和子网掩码。

外网虚拟地址和外网掩码:外网虚拟地址和子网掩码，外网地址为加密网关的隧道地址，对加密网关内外两侧的网络终端和网络设备透明，用于和远程加密认证网关进行密钥协商、数据加解密等。

双机地址:为加密认证网关（备机）的外网虚拟地址。如果主备地址不在相同网段，此时两台机器可以为负载均衡配置。如果在相同网段则，两台机器可以为双机热备配置，也可以为负载均衡配置。如果本端无备机，默认地址为 0.0.0.0。

VLAN ID：加密认证网关所在网络的 vlan 信息，如果加密认证网关所处网络无 vlan trunk，则此项 vlanid 设置为 0。

网络通道：装置有四个网口，支持“双进双出”接入方式，其中 eth0 和 eth1、eth2 和 eth3 各为一路加密通道，默认通道为 eth0-eth1。

3.4.3 路由信息配置

加密认证网关需要对加密和解密过的 IP 报文进行路由选择。路由配置信息针对加密网关的内外网虚拟地址，通过路由地址关联内外网的网络地址信息。

路由地址：为路由下一跳地址。

目的网络：为路由信息的目的网络地址。

目的掩码：为路由信息的目的网络地址的子网掩码。

3.4.4 装置管理信息配置

加密认证网关支持多个管理系统的管理，每个管理系统因所处位置和角色不同而具有不同的管理权限。装置管理配置界面中的位置信息（通过网络接口选项进行选择）有内外网之分，作为纵向加密认证网关的路由使用。装置管理系统的证书通过证书名进行关联。

装置管理的权限分为两类，分别为配置管理权限和信息查询权限。具有配置管理权限的管理系统可以对加密认证网关进行策略配置、系统复位、隧道配置、相关信息查询等；具有信息查询权限的系统只可对装置的状态信息、策略信息，隧道信息等进行浏览。装置管理系统的管理报文采用电力专用分组密码算法进行加密，通信密钥一次一变。加密网关收到装置管理报文后，会根据管理策略进行

相应的处理。

管理地址：为装置管理系统实际的 IP 地址信息。

装置地址：为加密网关的虚拟地址。

所处位置：标识装置管理系统的位置信息，分为内网与外网。

管理权限：分为浏览与配置两种管理权限。

证书名称：装置管理系统的证书名称，需要与系统初始化导入的装置管理证书名称一致。

3.4.5 隧道配置

隧道为加密认证网关之间协商的传输通道，数据包在隧道内进行安全传输。

隧道 ID:隧道的标识，关联隧道的所有信息。

隧道模式：隧道模式分为两类：加密和明通。明通模式下，隧道两端装置不进行密钥协商，隧道中的所有数据只能通过明通方式（但可以对数据包进行安全过滤与检查）；进行传输。加密模式下，隧道中的数据报文会根据协商好的密钥进行封装和加密。

装置隧道地址：为本端隧道的地址，即加密网关的外网虚拟 IP 地址。

对端主隧道地址：为对端隧道的主地址，即对端加密网关（主机）的外网虚拟 IP 地址。

对端主隧道证书名称：对端主隧道的证书名称。为对端加密网关的主设备证书名称，与初始化导入的对端加密网关证书名称一致。

对端备隧道地址：为对端隧道的备用地址，即对端加密网关（备机）的外网虚拟 IP 地址。如果对端无备用装置，则隧道备地址为 0。

隧道周期：隧道密钥的存活周期（以小时为基本计量单位）。超过设定的存活周期，装置会自动重新协商密钥。

隧道容量：为隧道内可加解密报文总字节数的最大值，在隧道内加解密报文的总字节数一旦超过此值，隧道密钥立刻失效，装置会自动重新协商密钥。

3.4.6 策略配置

加密认证网关具有双向报文过滤功能，与加密机制分离，独立工作，在实施加密之前进行。过滤策略支持：

源 IP 地址（范围）控制；

目的 IP 地址（范围）控制；

源 IP（范围）+ 目的 IP 地址（范围）控制；

协议控制；

TCP、UDP 协议 + 端口（范围）控制；

源 IP 地址（范围）+ TCP、UDP 协议 + 端口（范围）控制；

目标 IP 地址（范围）+ TCP、UDP 协议 + 端口（范围）控制。

隧道 ID：为隧道配置中设定的隧道 ID 信息。通过此信息，可以将策略关联到具体的隧道，以便对经过过滤的报文进行加解密处理。

工作模式：工作模式分为明通、加密或者选择性保护。选择性保护需要根据两端前置机通信程序的 TCP 报文头 option 选项指示。

源起始地址和源目的地址：本端通信网段的起始和终止地址，如果为单一通信节点，则源起始地址和源目的地址设置为相同。

目的起始地址和目的终止地址：对端通信网段的起始和终止地址，如果为单一通信节点，则目的起始地址和目的终止地址设置为相同。如果对端网关启用地址转化功能，则目的地址为对端网关的外网虚拟 IP 地址。

协议：支持 TCP、UDP 通信协议。

传输方向：此配置字段可以控制数据通信的流向，分为内->外、外->内和双向。

源起始端口和源终止端口：通信端口配置范围在 0 - 65535 之间。

目的起始端口和目的终止端口：通信端口配置范围在 0 - 65535 之间。对于通信进程的服务端，起始和终止端口可配置为相同。

注意：如果对端加密认证网关存在备机，应该配置两条相同的策略，只是关联

的隧道 ID 不同。

3.4.7 地址转换配置

加密认证网关系统支持地址转换（地址伪装和目的地址转换），保护内网私有地址。

网关开启 IP 伪装功能时，当数据包经过加密网关发送到外部网络时，会将数据包的源地址改变成加密网关的外网虚拟地址，而经过转换的数据包可以在外网中完整路由。此时内网地址为需要地址转换的内网网络地址。外网地址为伪装地址。

有时候内网私有地址对外提供网络服务，为了保证内网资源的安全，这时可以将内网的网络服务映射到加密网关的外网虚拟地址上，外网用户可通过访问加密网关的外网虚拟地址的服务达到访问内网服务的目的。在这种转换方式下，需要开启加密网关的目的地址转换功能。**内网地址**为提供服务的内网主机地址，**内网端口**为服务端口。**外网地址**为加密网关的虚拟地址，**外网端口**为服务端口的映射。

3.5 隧道信息查询

加密网关配置管理软件支持根据隧道号对网关的隧道状态进行查询或对所有隧道状态进行浏览，方便用户分析与管理。隧道信息查询的内容主要包括隧道状态、隧道地址、通信信息、报文信息等。

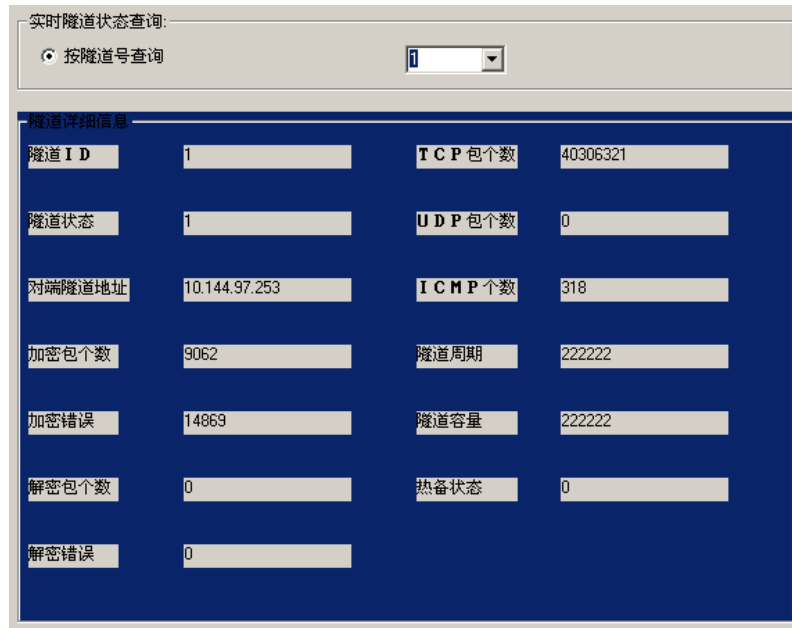


图 3.25 隧道查询界面

3.6 系统调试

3.6.1 网关硬件诊断

加密网关内嵌电力专用密码模块和智能 IC 接口模块，为了排查加密网关系统有可能出现的数据通信错误，配置管理软件提供了对数据加密模块和智能读写器设备的调试诊断功能。

1) 加密单元设备调试

点击工具栏中的“加密卡调试”，则出现下面的界面，选择硬件类型中的“加密卡硬件”，点击“开始”，加密网关自动对加密单元进行检测，测试结果显示到调试界面上。



图 3.26 加密单元调试界面

2) 智能 IC 卡单元调试

选择硬件类型中的“操作员卡硬件”，点击“开始”，加密网关自动对智能 IC 读写器单元进行检测，测试结果显示到调试界面上。



图 3.27 智能 IC 卡调试界面

如果提示测试失败，请检查您的卡片是否插到位，面板上的 CRW 读卡器指示灯是否正常闪烁，如果在测试过程中，CRW 灯不闪烁，请与我们联系。

3.6.2 SPING 调试

SPING 调试用于确认和对端加密网关的连通情况，在 SPIN 调试界面中输入装置的虚拟 IP 地址（外网虚拟 IP）、对端装置的 IP 地址（外网虚拟 IP）、测试次数和时间，点击“开始”，网关自动探测对端装置并返回测试结果，如下图所示。

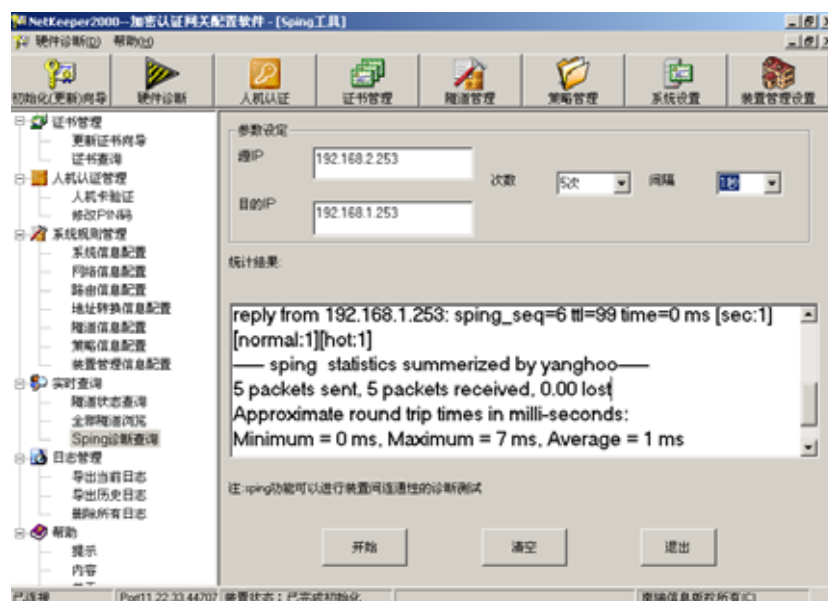


图 3.28 SPING 调试界面

3.7 日志管理

加密网关具备专用安全日志存储单元，可以对日志进行存储备份。配置管理软件支持本地导出近期日志和历史日志并分析，点击导航栏或者菜单中的”导出当前日志并分析”或“导出历史日志并分析”，则将从装置中载入加密日志并自动解密分析其内容，为安全审计提供基础数据源，如下图所示。

系统近期日志分析：

日期	时间戳	类型	内容
2036-03-11	01:42:42	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	01:42:44	人员操作	Msg Exporting config file success>File: /log/route_temp.txt Type: c...
2036-03-11	01:43:24	人员操作	Msg Exporting config file success>File: /log/ip_temp.txt Type: conf ...
2036-03-11	01:43:27	人员操作	Msg Exporting config file success>File: /log/ip_temp.txt Type: conf ...
2036-03-11	01:45:09	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	01:47:27	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	01:49:46	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	01:52:07	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	01:53:15	系统信息	EMHTTP:netkeeper user login!
2036-03-11	01:54:31	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	01:56:20	人员操作	Msg Exporting config file success>File: /log/route_temp.txt Type: c...
2036-03-11	01:56:42	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	01:58:51	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	02:01:02	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	02:03:12	通信信息	POST IKE succes: 10.144.98.252>10.144.98.252
2036-03-11	02:04:19	人员操作	Msg Connect serial port success!
2036-03-11	02:04:20	人员操作	Msg The ca dir exist!
2036-03-11	02:04:20	人员操作	Msg Check_working_status1: check dir ok!
2036-03-11	02:04:21	人员操作	Msg sm_Login::Open secmodule success!
2036-03-11	02:04:21	人员操作	Msg user logout !
2036-03-11	02:04:21	人员操作	Msg Check_initialized() ok,has init!
2036-03-11	02:04:21	人员操作	Msg Check_working_status() system has been initialized!
2036-03-11	02:04:28	人员操作	Msg Operator Card and Machine verify success!
2036-03-11	02:04:33	人员操作	Msg Exporting config file success>File: /log/tunnel_temp.txt Type: ...

保存分析结果 退出窗口

图 3.29 日志分析界面

四、典型应用环境配置案例

4.1 明通模式配置

当对端通信节点没有部署加密网关时,可以采用明通模式。此时加密网关具备硬件防火墙的基本功能,但数据不能进行加密保护,明通网络拓扑如下图所示。加密网关配置如下。

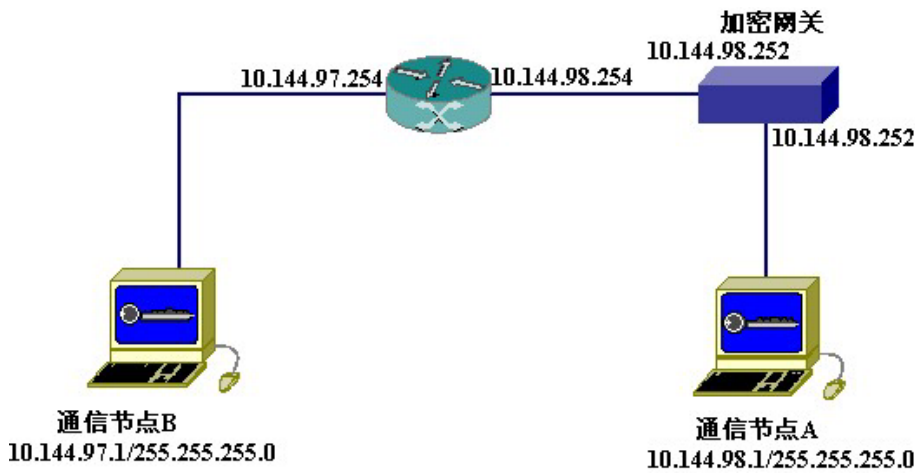


图 4.1 明通模式拓扑图

4.1.1 系统配置

装置信息设置

装置标识名: NJDD

默认策略: 丢弃

审计点位置: 外网

审计地址: 10.144.98.180

装置地址: 10.144.98.252

导入装置

装置导出

保存本地

本地载出

图 4.2 明通模式-系统配置

4.1.2 网络配置

网络标识

network1

内网子网掩

255.255.255.0

外网子网掩

255.255.255.0

VLANID

0

内网虚拟地

10.144.98.252

外网虚拟地

10.144.98.252

双机地址

0

网络通道

eth0-eth1

网络标识	内网虚拟地址	内网子网掩码	外网虚拟地址
network1	192.168.8.253	255.255.255.0	192.168.8.254

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地导出

图 4.3 明通模式-网络配置

4.1.3 路由配置

目的网络地址

10.144.97.0

目的网络子网掩码

255.255.255.0

路由地址

10.144.98.254

网络选择

外网

目的网络地址	目的网络子网掩码	路由地址	网络选择
10.144.97.0	255.255.255.0	10.144.98.254	1

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地导出

图 4.4 明通模式-路由配置

4.1.4 隧道配置

隧道ID1

隧道模式明通

装置隧道地址10.144.98.252

对端主隧道地址0

对端主隧道证书名cert.pem

对端备隧道地址0

隧道容量(个)5000000

隧道周期(小时)24

隧道ID	隧道模式	装置隧道地址	对端主隧道地址	对端装置证书	对端备隧道地址	隧道容
1	1	10.144.98.252	0	cert.pem	0	500000

提示:修改规则时选择视图中规则,在视图上方填写修改内容,并点击“修改规则”按钮

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载入

图 4.5 明通模式-隧道配置

注意：由于对端无加密网关，因此对端主、备隧道地址为 0，隧道模式为明通。

4.1.5 策略信息配置

隧道ID1

模式明通

源起始地址10.144.98.1

源终止地址10.144.98.1

源目的地址10.144.97.1

目的终止地址10.144.97.1

协议ALL

方向双向

源起始端口0

源终止端口65535

目的起始端口0

目的终止端口65535

隧道	模式	源地址	源终止地址	目的地址	目的终止地	协议	方向	源起始端口	源终止端口
1	1	10.144.98.1	10.144.98.1	10.144.97.1	10.144.97.1	0	0	0	65535

提示:修改规则时选择视图中规则,在视图上方填写修改内容,并点击“修改规则”按钮

图 4.6 明通模式-策略配置

注意：由于对端无加密网关，因此策略配置中模式选择为明通。

4.2 同一网段配置

当加密网关部署到同一网段或进行测试时，可以采用此配置模式。加密网关具备硬件防火墙的基本功能，同时对数据数据进行加密保护。网络拓扑如下图所示，策略配置以加密网关 1 为例。

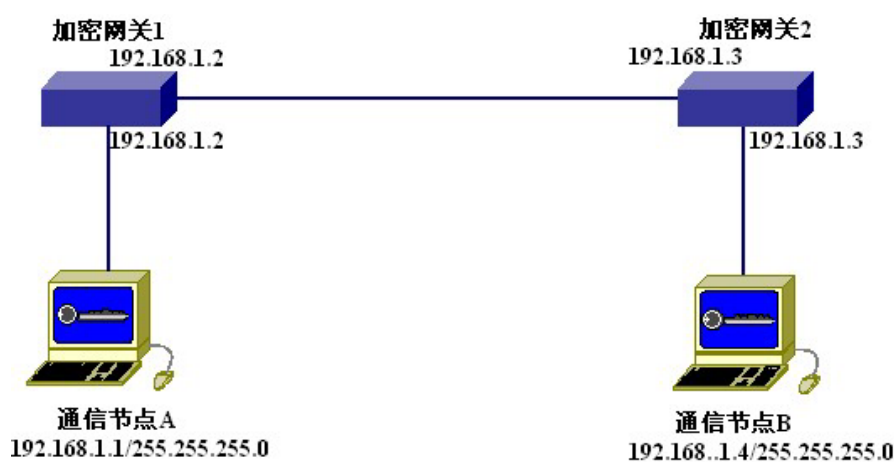


图 4.7 同一网段配置网络拓扑图

4.2.1 系统配置

装置信息设置	
装置标识名:	NJDD
默认策略:	丢弃
审计点位置:	外网
审计地址:	192.168.1.111
装置地址:	192.168.1.2

导入装置装置导出保存本地本地载出

图 4.8 同一网段-系统配置

4.2.2 网络配置

网络标识

内网虚拟地址

内网子网掩

外网虚拟地址

外网子网掩

双机地址

VLANID

网络通道

网络标识	内网虚拟地址	内网子网掩码	外网虚拟
network1	192.168.8.253	255.255.255.0	192.168.8

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载出

图 4.9 同一网段-网络配置

4.2.3 隧道配置

隧道ID

隧道模式

装置隧道

对端主隧道地址

对端主隧道证

对端备隧道地址

隧道容量(个)

隧道周期(小时)

隧道ID	隧道模式	装置隧道地址	对端主隧道地址	对端装置证书	对端

提示:修改规则时选择视图中规则,在视图上方填写修改内容,并点击'修

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载入

图 4.10 同一网段-隧道配置

4.2.4 策略配置

[illegible]

图 4.11 同一网段-策略配置

4.3 路由模式配置

纵向加密认证网关部署在各级调度中心及下属的各厂站,根据电力调度通信关系建立加密隧道,典型网络拓扑如下图所示。策略配置以加密网关 2 为例。

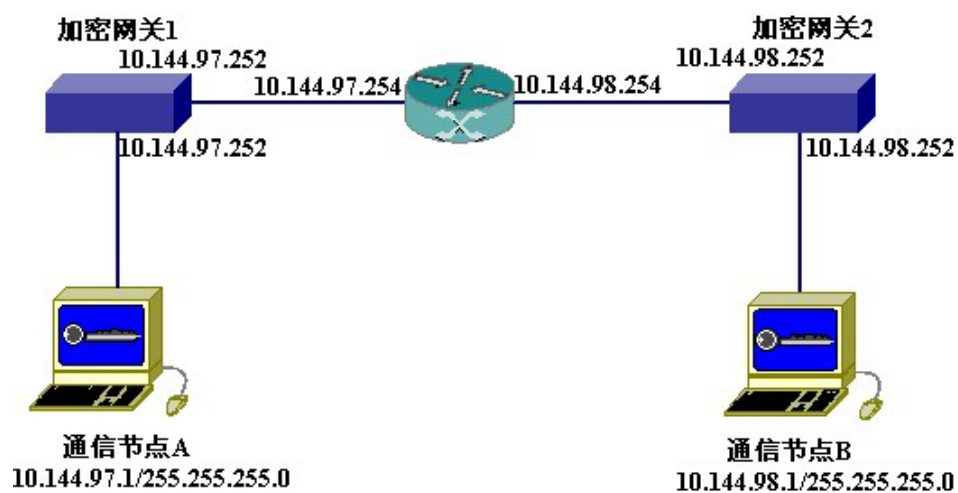


图 4.12 典型配置网络拓扑图

4.3.1 系统配置

装置信息设置

装置标识名: NJDD 默认策略: 丢弃

审计点位置: 外网 审计地址: 10.144.98.180

装置地址: 10.144.98.252

导入装置 装置导出 保存本地 本地载出

图 4.13 路由模式-系统配置

4.3.2 网络配置

网络标识: network1 内网虚拟地址: 10.144.98.252

内网子网掩: 255.255.255.0 外网虚拟地址: 10.144.98.252

外网子网掩: 255.255.255.0 双机地址: 0

VLANID: 0 网络通道: eth0-eth1

网络标识	内网虚拟地址	内网子网掩码	外网虚拟地址
network1	192.168.8.253	255.255.255.0	192.168.8.253

添加规则 修改规则 删除规则 全部删除

导入装置 装置导出 保存本地 本地载出

图 4.14 典型模式-网络配置

4.3.3 路由配置

目的网络地址10.144.97.0

目的网络子网掩码255.255.255.0

路由地址10.144.98.254

网络选择外网

目的网络地址	目的网络子网掩码	路由地址	网络选择
10.144.97.0	255.255.255.0	10.144.98.254	1

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地导出

图 4.15 典型模式-路由配置

4.3.4 隧道配置

隧道ID1

隧道模式加密

装置隧道地址10.144.98.252

对端主隧道地址10.144.97.252

对端主隧道证书名cert.pem

对端备隧道地址0

隧道容量(个)5000000

隧道周期(小时)24

隧道ID	隧道模式	装置隧道地址	对端主隧道地址	对端装置证书	对端备隧道地址	隧道容
1	0	10.144.98.252	10.144.97.252	cert.pem	0	5000000

提示:修改规则时选择视图中规则,在视图上方填写修改内容,并点击“修改规则”按钮

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载入

图 4.16 典型模式-隧道配置

4.4.1 系统配置

装置信息设置

装置标识名:

NJDD

默认策略:

丢弃

审计点位置

外网

审计地址:

10.144.98.180

装置地址:

10.144.98.252

导入装置

装置导出

保存本地

本地载出

图 4.19 VLAN 环境-系统配置

4.4.2 网络配置

网络标识

network1

内网虚拟地址

10.144.98.252

内网子网掩

255.255.255.0

外网虚拟地址

10.144.98.252

外网子网掩

255.255.255.0

双机地址

0

VLANID

0

网络通道

eth0-eth1

网络标识	内网虚拟地址	内网子网掩码	外网虚拟地址
network1	192.168.8.253	255.255.255.0	192.168.8.253

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载出

图 4.20 VLAN 环境-网络配置

注意：此处需要配置网络的 VLAN ID。

4.4.3 路由配置

目的网络地址

10.144.97.0

目的网络子网掩码

255.255.255.0

路由地址

10.144.98.254

网络选择

外网

目的网络地址	目的网络子网掩码	路由地址	网络选择
10.144.97.0	255.255.255.0	10.144.98.254	1

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地导出

图 4.21 VLAN 环境-路由配置

4.4.4 隧道配置

隧道ID

1

隧道模式

加密

装置隧道地址

10.144.98.252

对端主隧道地址

10.144.97.252

对端主隧道证书名

cert.pem

对端备隧道地址

0

隧道容量(个)

5000000

隧道周期(小时)

24

隧道ID	隧道模式	装置隧道地址	对端主隧道地址	对端装置证书	对端备隧道地址	隧道容
1	0	10.144.98.252	10.144.97.252	cert.pem	0	5000000

提示:修改规则时选择视图中规则,在视图上方填写修改内容,并点击“修改规则”按钮

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载入

图 4.22 VLAN 环境-隧道配置

4.4.5 策略配置

[illegible]

图 4.23 VLAN 环境-规则配置

4.5 NAT 模式配置

加密认证网关系统支持 NAT 地址转换(地址伪装和目的地址转换),保护内网私有地址,典型网络拓扑如下图所示。加密网关 1 启动地址转化功能,策略配置以加密网关 1 为例。

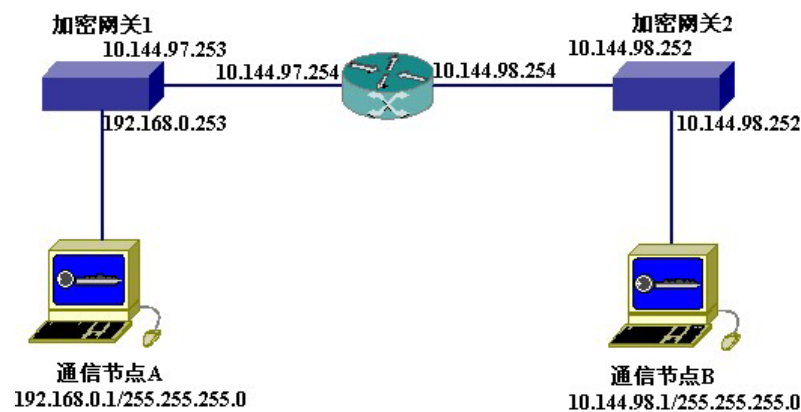


图 4.24 VLAN 环境网络拓扑

4.5.1 系统配置

装置信息设置

装置标识名:

NJDD

默认策略:

丢弃

审计点位置

外网

审计地址:

10.144.97.180

装置地址:

10.144.97.253

导入装置

装置导出

保存本地

本地载出

图 4.25 NAT 模式 - 系统配置

4.5.2 网络配置

网络标识

network1

内网虚拟地址

10.144.0.253

内网子网掩

255.255.255.0

外网虚拟地址

10.144.97.253

外网子网掩

255.255.255.0

双机地址

0

VLANID

0

网络通道

eth0-eth1

网络标识	内网虚拟地址	内网子网掩码	外网虚拟地址
network1	192.168.8.253	255.255.255.0	192.168.8.253

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载出

图 4.26 NAT 模式 - 网络配置

4.5.3 路由配置

目的网络地址10.144.98.0

目的网络子网掩码255.255.255.0

路由地址10.144.97.254

网络选择外网

目的网络地址	目的网络子网掩码	路由地址	网络选择
10.144.98.0	255.255.255.0	10.144.97.254	1

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地导出

图 4.27 NAT 模式-路由配置

4.5.4 隧道配置

隧道ID1

隧道模式加密

装置隧道地址10.144.97.253

对端主隧道地址10.144.98.252

对端主隧道证书名cert.pem

对端备隧道地址0

隧道容量(个)1000000

隧道周期(小时)10

隧道ID	隧道模式	装置隧道地址	对端主隧道地址	对端装置证书	对端备隧道地址	隧道容量
1	0	10.144.97.253	10.144.98.252	cert.pem	0	100000

提示:修改规则时选择视图中规则,在视图上方填写修改内容,并点击"修改规则"按钮

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载入

图 4.28 NAT 模式-隧道配置

4.5.5 地址转化配置

需要配置两条 NAT 规则，一条规则为地址伪装规则，用于对本端发出去的报文进行地址伪装匹配，另一条规则为端口映射规则，用于对端访问本端内网提供的网络服务。

1) 源地址转化（地址伪装）规则

地址转换类型

源地址转换

内网地址

192.168.0.0

外网地址

10.144.97.253

地址转换类型	内网地址	外网地址	内网端口
0	192.168.0.0	10.144.97.253	0
1	192.168.0.1	10.144.97.253	7070

添加规则

修改规则

删除规则

全部删除

导入装置

装置载出

保存本地

本地载出

图 4.29 NAT 模式-源地址转化配置

2) 目的地址转化（端口映射）规则

地址转换类型

目的地址转换

内网地址

192.168.0.1

内网端口

7070

外网地址

10.144.97.253

外网端口

7070

地址转换类型	内网地址	外网地址	内网端口
0	192.168.0.0	10.144.97.253	1000
1	192.168.0.1	10.144.97.253	7070

添加规则

修改规则

删除规则

全部删除

导入装置

装置载出

保存本地

本地载出

图 4.30 目的地址转换配置

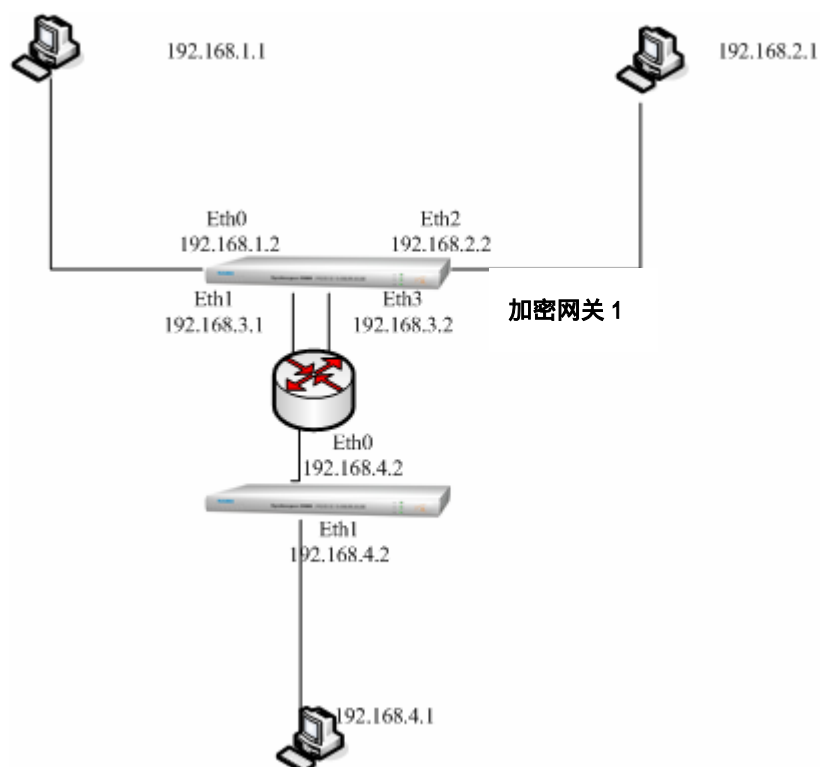
4.5.6 策略配置

[illegible]

图 4.31 NAT 模式-策略配置

4.6 双进双出配置

加密认证网关目前为四个 10/100M 以太网接口,支持“双进双出”接入模式。即变电站实时控制区和非控制生产区分别接入加密认证网关的内网接口(eth0 和 eth2), 加密认证网关出口 (eth1 和 eth3) 连接在调度数据的路由器上 (路由器的地址分别为 192.168.3.254 和 192.168.4.254)。接入方案如下图所示,策略配置以加密网关 1 为例。



4.6.1 系统配置

装置信息设置

装置标识名: NNDD

默认策略: 丢弃

审计点位置: 外网

审计地址: 192.168.3.100

装置地址: 192.168.3.1

导入装置

装置导出

保存本地

本地载出

图 4.33 双进双出模式-系统配置

4.6.2 网络配置

1) 1 号网络通道配置

网络标识: network1

内网子网掩: 255.255.255.0

外网子网掩: 255.255.255.0

VLANID: 0

内网虚拟地: 192.168.1.2

外网虚拟地: 192.168.3.1

双机地址: 0

网络通道: eth0-eth1

网络标识	内网虚拟地址	内网子网掩码	外网虚拟地址
network1	192.168.8.253	255.255.255.0	192.168.8.253

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载出

图 4.34 双进双出模式-网络配置 1

2) 2 号网络通道配置

网络标识	network1	内网虚拟地址	192.168.2.2
内网子网掩	255.255.255.0	外网虚拟地址	192.168.3.2
外网子网掩	255.255.255.0	双机地址	0
VLANID	0	网络通道	eth2-eth3

网络标识	内网虚拟地址	内网子网掩码	外网虚拟地址
network1	192.168.8.253	255.255.255.0	192.168.8.254

添加规则
修改规则
删除规则
全部删除

导入装置
装置导出
保存本地
本地导出

图 4.35 双进双出模式-网络配置 2

注意：需要配置两条网络通道

4.6.3 路由配置

目的网络地址	192.168.0.0	目的网络子网掩码	255.255.0.0
路由地址	192.168.3.254	网络选择	外网

目的网络地址	目的网络子网掩码	路由地址	网络选择
192.168.0.0	255.255.0.0	192.168.8.254	1

添加规则
修改规则
删除规则
全部删除

导入装置
装置导出
保存本地
本地导出

图 4.36 双进双出模式-路由配置

4.6.4 隧道配置

1) 1 号加密隧道配置

隧道ID1隧道模加密

装置隧道192.168.3.1对端主隧道地192.168.4.2

对端主隧道证cert.pem对端备隧道地0

隧道容量(个)500000隧道周期(小时)24

隧道ID	隧道模式	装置隧道地址	对端主隧道地址	对端装置证书	对端备隧道地址

提示:修改规则时选择视图中规则,在视图上方填写修改内容,并点击“修

添加规则修改规则删除规则全部删除

导入装置装置导出保存本地本地载入

图 4.37 双进双出模式- 隧道配置 1

2) 2 号加密隧道配置

隧道ID2隧道模加密

装置隧道192.168.3.2对端主隧道地192.168.4.2

对端主隧道证cert.pem对端备隧道地0

隧道容量(个)500000隧道周期(小时)24

隧道ID	隧道模式	装置隧道地址	对端主隧道地址	对端装置证书	对端备隧道地址

提示:修改规则时选择视图中规则,在视图上方填写修改内容,并点击“修

添加规则修改规则删除规则全部删除

导入装置装置导出保存本地本地载入

图 4.38 双进双出模式- 隧道配置 2

注意：需要配置两条加密隧道

4.6.5 策略配置

1) 1 号隧道策略配置

隧道ID	<input type="text" value="1"/>	模式	<input type="text" value="加密"/>
源起始地	<input type="text" value="192.168.1.1"/>	源终止地	<input type="text" value="192.168.1.1"/>
源目的地	<input type="text" value="192.168.4.1"/>	目的终止	<input type="text" value="192.168.4.1"/>
协议	<input type="text" value="ALL"/>	方向	<input type="text" value="双向"/>
源起始端	<input type="text" value="0"/>	源终止端	<input type="text" value="65535"/>
目的起始端	<input type="text" value="0"/>	目的终止端	<input type="text" value="65535"/>

隧道ID	模式	源地址	源终止地址	目的地址	目的终止地址	协议	方向

提示：修改规则时选择视图中规则，在视图上方填写修改内容，并

添加规则

修改规则

删除规则

全部删除

导入装置

装置导出

保存本地

本地载入

图 4.39 双进双出模式- 策略配置 1

3) 2号隧道策略配置

[illegible]

图 4.40 双进双出模式- 策略配置 2