NetKeeper-2000
加密认证网关（十兆型）用户手册

南京南瑞集团公司信息通信技术分公司

注意：

南瑞加密认证网关（十兆型）用户手册

Version2.9　2016-12-7

南瑞集团公司信息通信技术分公司

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：chengongsheng@sgepri.sgcc.com.cn

南京南瑞集团公司信息通信技术分公司

南京市南瑞路 8 号，210003

电话（TEL）：025-81082222(技术支持)

传真（FAX）：025-81082218

目　录

一、产品介绍

1.1 产品部署环境

电力专用加密认证网关（十兆型）安置在电力调度配网终端与公网（或专网）的网络边界，保障配电终端与主站之间的数据传输过程中的数据机密性、完整性和真实性。

按照“分级管理”要求，纵向加密认证网关（十兆型）部署在各级调度中心及下属的各终端设备上，根据电力调度通信关系建立加密隧道（原则上只在上下级之间建立加密隧道），加密隧道拓扑结构是部分网状结构。

1.2 产品外观与结构

NetKeeper-2000 纵向加密认证网关（十兆型）是南京南瑞集团公司信息通信技术分公司研制的高性能加密认证网关产品。NetKeeper-2000 纵向加密认证网关（十兆型）在网络环境接入的适应性、数据加密性能、网络吞吐率、系统高可靠性保障技术等方面代表了加密认证网关（十兆型）的发展趋势，在行业内处于领先水平，设备如下图：

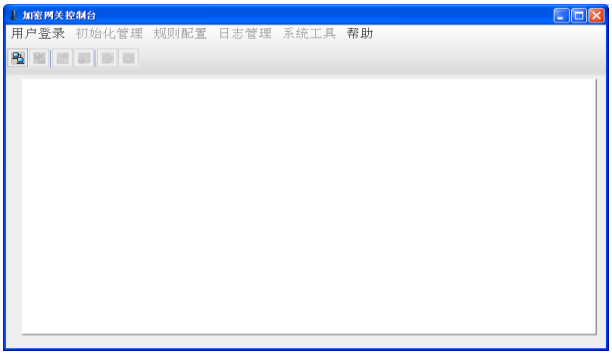
图表 2　NetKeeper-2000 纵向加加密认证网关（十兆型）

二、产品分发与安装

NetKeeper-2000 加密认证网关（十兆型）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，请勿使用并及时与我公司取得联系，处理相关事宜。为了保障产品稳定、可靠的运行，用户请勿私自打开加密认证网关（十兆型）机箱。

加密认证网关（十兆型）随机带有配置软件光盘一张、网络配置线一根、串口配置

线一根（需要使用装置附带串口线），配置软件可以安装在 Windows7/Windows2000/XP/NT/9x 操作系统的计算机上。(注:配置计算机必须要有 java 运行环境支持)。安装完成后，即可开始配置。



图表 3 加密网关配置软件

加密认证网关（十兆型）用于电力安全区的广域网边界保护，网关部署对应用完全透明。通过加密网关的内网接口和外网接口，分别与内部局域网和外部广域网连接，为网关机之间的广域网通信提供具有认证、加密功能的 VPN，实现数据传输的机密性、完整性保护。用户可以通过配置管理程序对加密网关进行相应的设置，具体的配置管理请参见下节。

三、加密认证网关（十兆型）配置管理

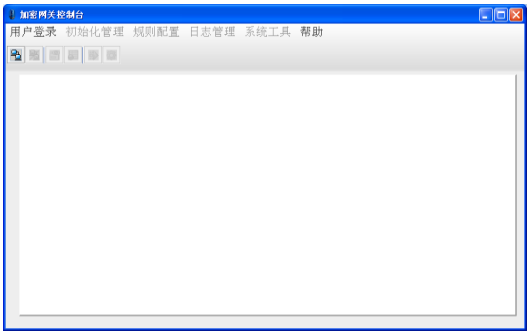
3.1 系统初始化

加密认证网关（十兆型）投入使用前，需要进行设备的初始化操作，初始化操作内容包括安装调度证书服务系统根证书、装置管理系统证书、本装置的主备操作员证书、与本装置通信的对端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（十兆型）的安全存储区中。

3.1.1 通信初始化

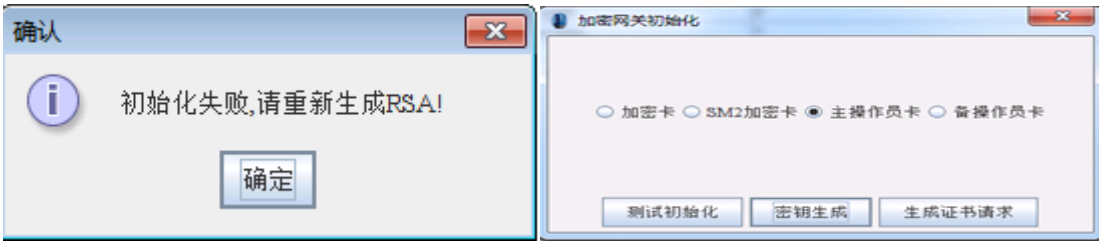
1) 将本地配置计算机地址设置为 11.22.33.43， 掩码为 255.255.255.0 ，用随机附带的网络配置线连接到加密认证网关（十兆型）的配置接口 eth1，并且将设备配件盒里的 USBkey 卡插入加密装置（金属片朝下）。

2) 启动加密认证网关（十兆型）配置软件，出现如图表 4 软件主界面：



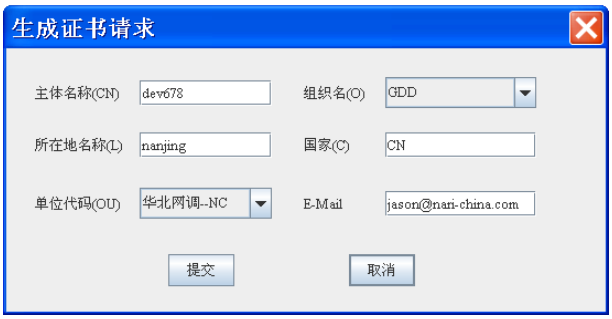
图表 4 加密认证网关（十兆型）配置软件主界面

点击确定，软件系统会自动和加密网关服务程序建立连接，显示初始化失败，开始初始化操作员卡和加密卡：



图表 5 初始化操作员卡和加密卡

3）点击“生成证书请求”，生成加密卡和操作员证书请求后，将证书请求发给当地证书签发中心；



图表 6 生成证书请求

主体名称：加密网关的唯一标识，建议采用装置所在厂站名称(注意要使用英文字母)。

组织名：国调 GDD（默认）南网 ZD

所在地名称：厂站所在地名称

国家：CN（默认）

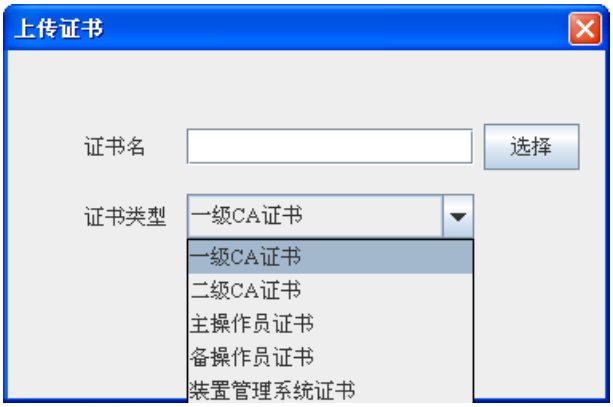
单位代码：签发单位名称

E-Mail： 该字段为扩展字段可以不填写

3.1.2 初始化

1） 导入调度 CA 的根证书。

本步骤是后续对其它实体证书进行验证的基础，点击“初始化管理” → “证书管理”，将由主界面转到证书管理界面，如图表 7 所示。选择上传证书  系统会弹出上传证书界面，选择证书路径，并选择证书类型为“一级 CA 证书”并导入，系统会提示验证成功与否，一般情况下一级 CA 证书为国网根证书或南网根证书。



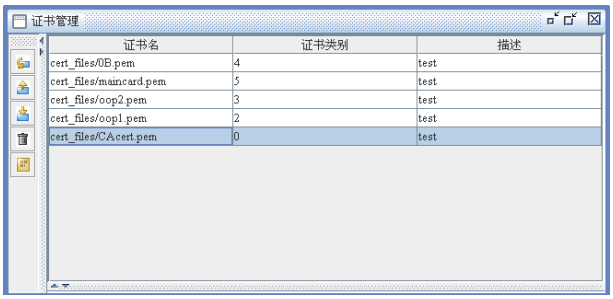
图表 7 上传证书

2） 导入二级 CA 证书(网省调证书)。操作方法同上。

3） 导入主备操作员证书。操作方法同上（执行此步系统即初始化完成）。

4） 导入装置管理系统证书。操作方法同上。

5） 导入和本地加密网关通讯的对端加密网关证书。操作方法同上。



图表 8 初始化完成后的证书界面

3.1.3 设备登录

导入操作员证书后，设备即被初始化，保持 IC 卡插入状态，重启配置软件登录设

备

图表 9 登录初始化完成的设备

插入 usbkey，点“确定”，输入操作员 pin 码：Nari6702，即可正常登陆

图表 10 成功登录系统

点击确定，开始配置纵向加密网关（十兆型）。

注意：Nari6702 为初始密码,建议登陆后修改。

3.2 安全管理

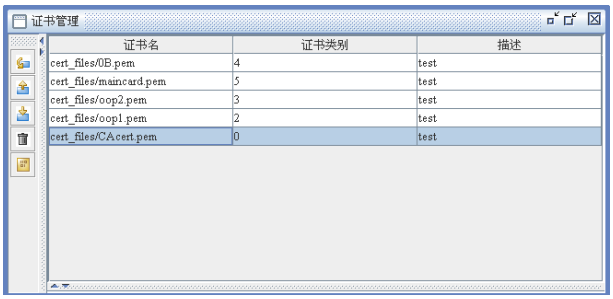
加密认证网关（十兆型）的安全管理包括证书管理、远程监控等。

3.2.1 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“初始化管理” → “证书管理”，进入证书管理界面，然后单击下载证书列表按钮  ，如图表 11 所示。

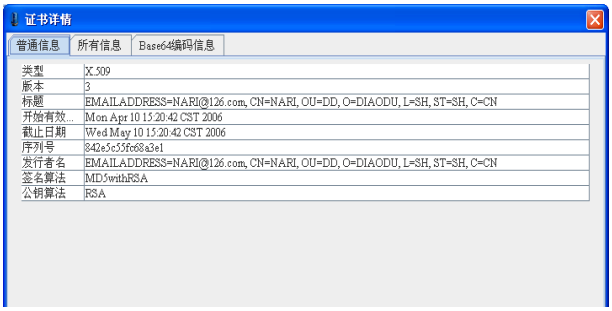
图表 11 证书下载等待信息

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，如图表 12 所示。（图表 16 显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。）

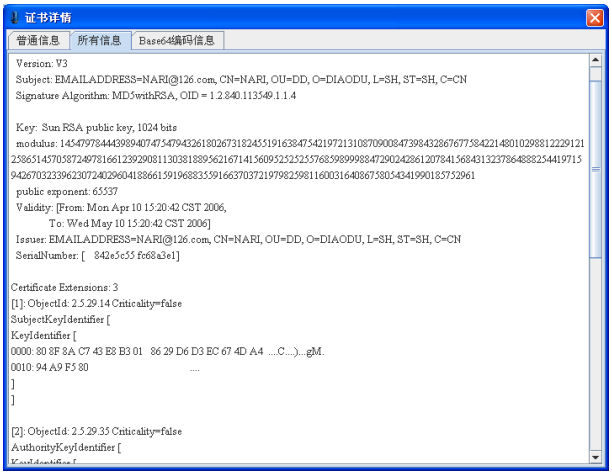


图表 12 加密网关证书管理界面

选中目标证书，并点击 “察看证书”按钮，可以显示证书详细信息及证书编码信息，如图表 13、图表 14 所示。此时证书被下载到配置程序安装目录下的 config 文件夹中。同样，选中目标证书，并点击“删除证书”按钮，将删除装置中此证书。



图表 13 证书详细信息



图表 14 证书编码信息

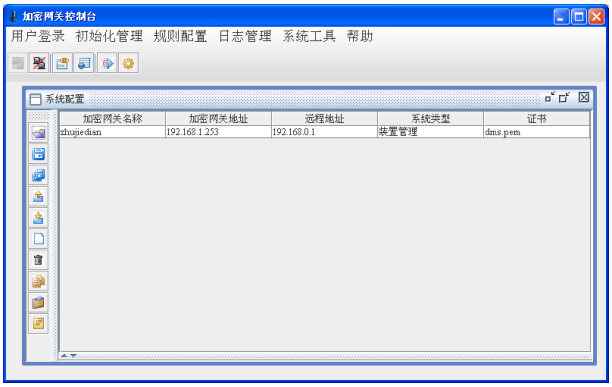
3.2.2 远程监控

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（十兆型）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。调度中心的加密网关及下属的加密网关由装置管理系统

直接管理。此时，装置管理系统(管理中心)与加密网关是网络上通信的实体。装置管理系统通过经认证加密的管理报文实现对纵向加密认证网关（十兆型）的监测。具体的监控内容及装置管理系统的使用详见《加密认证网关（十兆型）装置管理系统用户使用手册》

3.3 安全策略配置

加密认证网关（十兆型）位于电力控制系统的内部局域网与电力调度数据网的路由器之间，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（十兆型）的安全策略设置主要包括系统配置、网络配置、路由配置、隧道配置、策略配置等(注意这里的所有配置都要使用英文字母或数字，中文不能识别)，主配置界面如图表 15 所示



图表 15 主配置界面

主配置界面左侧的编辑功能按钮功能描述如下：(在其他的信息配置界面中编辑功能按钮的作用类似，下文中只以相应的图标加以表示，具体功能不再赘述。)

 ：打开配置或新建配置文件

 ：保存并上传配置信息至装置

 ：下载装置配置信息至本地

 ：另存配置(将配置信息保存至本地)

 ：建立新的配置信息

 ：删除选择的配置信息

 ：将当前行的资源复制

 ：增加新的一行，内容为之前复制的资源

 ：对当前选择的资源进行编辑

3.3.1 系统信息配置

系统信息配置主要配置加密认证网关（十兆型）的系统信息，包括以下内容：

加密网关名称：装置的名称，便于远程标识装置的基本信息。

加密网关地址：加密网关的外网地址或者外网卡上用于被管理或审计的地址。

远程地址：远程的装置管理系统、日志审计系统或者远程调试计算机的网络地址。

系统类型：可分为装置管理、日志审计、远程调试集中类型。

证书：在系统类型配置为装置管理时必须配置相应的装置管理中心的证书名称。

在这个界面中可以对装置系统信息作一系列操作例如：增加、修改、删除、上传、下载等。

点击“规则配置” → “系统管理”，选中某一条系统信息规则之后点击  （编辑资源），若原先没有相应的网络信息规则可以先点击  （新建资源）并将其选中后点击编辑资源进入具体界面如图表 16 所示

图表 16 装置系统配置信息

3.3.2 网络信息配置

加密认证网关（十兆型）有 2 个以太网接口可以作为通信网口，其中任意网口都可以设置成内网口或者外网口，建议使用 eth1 为内网，eth2 为外网。在实际的配置中，需要对加密认证网关（十兆型）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。

在网络信息配置界面中可以对装置网络信息作一系列的配置如：增加、修改、删除、上传、下载等。

点击“规则配置” → “网络配置”进入配置界面之后选中相应的网络配置信息点击  （编辑资源），若原来没有相应的网络信息规则可先点击  （新建资源），再点击编辑资源进入网络配置界面，如图表 17 所示。

图表 17 装置地址配置

网络接口：所要配置网口的名称，例如 eth1、eth2 等。

接口类型：所要配置网口的类型，分别有 PRIVATE（内网口）、PUBLIC（外网口）、BACKUP（互备口）、CONFIG（配置口）、BRIDGE（桥接口）。

IP 地址：所要配置网口的 IP 地址。

子网掩码：所要配置网口的掩码。

接口描述：所要配置网口的相关描述信息，若是桥接模式的话这里必须与桥接配置里的接口自定义名称完全一致，其他模式下无意义，。

VLANID：所要配置网口的 VLAN ID 信息。

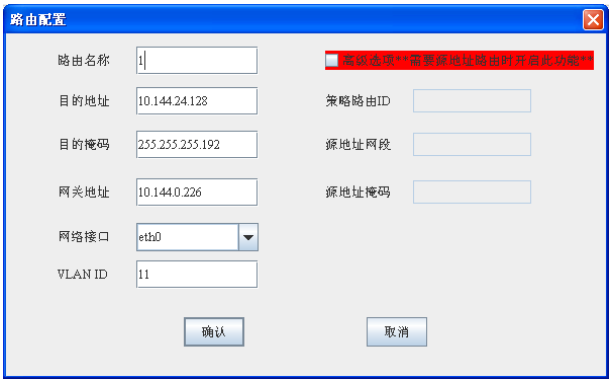
3.3.3 路由信息配置

加密认证网关（十兆型）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。

在这个界面中可以对装置路由信息作一系列的配置例如：增加、修改、删除、上传、下载等。

点击“规则配置” → “路由配置”进入路由配置界面，然后选中相应的路由配置信息点击  进行编辑，若原来没有相应的路由信息规则可以先点击  （新建资源）再点击编辑资源按钮进入路由配置界面，如图表 18 所示。



图表 18 路由信息配置

路由名称：路由信息的名称描述。

网络接口：要用到路由的出口网卡的名称，一般为外网口。

目的网络：要实现通信的目的网络所在网段。

目的掩码：为路由信息的目的网络地址的子网掩码。

网关地址：加密网关的外网口下一跳地址。

VLANID：为所要配置网口的 VLAN ID 信息。

策略路由 ID：用来标识策略路由的集合，相同策略路由 ID 的路由的源地址一般是一样的，符合这个源地址的报文将按照目的地址段的大小匹配这一组路由。

源地址网段：为策略路由的源地址的网段。

源地址掩码：为策略路由的源地址的子网掩码(这三条只在需要根据源地址路由的环境中配置，其他环境置空即可)。

3.3.4 隧道配置

隧道为加密认证网关（十兆型）之间协商的安全传输通道，隧道成功协商之后会生成通信密钥，进入该隧道通信的数据由通信密钥进行加密，隧道可以设置隧道周期和隧

道容量，当隧道的通信时间达到指定传输周期或者数据通信量达到指定容量后，加密网关（十兆型）之间会重新进行隧道密钥协商，保证数据通信安全。

点击“规则配置” → “隧道配置”进入隧道配置界面，然后选中相应的隧道配置信息点击  进行编辑，若原来没有相应的隧道信息规则可以先点击  （新建资源）再点击编辑资源按钮进入隧道配置界面，如图表 19 所示:

图表 19 隧道配置

隧道名称：隧道的相关描述(不可以为中文)。

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、明通。在明通模式下，隧道两端的装置不进行密钥协商，隧道中的所有数据只能通过明文方式（但可以对数据包进行安全过滤与检查，即只有配置了相关的通信策略的数据传输才能通过装置，否则装置会将不合法的报文全部丢弃）进行传输；在加密模式下，隧道中的数据报文会根据协商好的密钥将相关通信策略的数据报文进行封装和加密，保证数据传输的安全性。

隧道本端地址：为本端加密装置的地址，即本侧加密网关的外网虚拟 IP 地址。

隧道对端主地址：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。

主装置证书名称：对端主隧道的证书名称。对端加密网关的主设备证书名称需与初始化导入的对端加密网关证书名称一致。

隧道对端备地址：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 0.0.0.0。

备装置证书：对端备隧道的证书名称。对端加密网关的备设备证书名称需与初始化导入的对端备加密网关证书名称一致

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。

3.3.5 策略配置

加密通信策略用于实现具体通信策略和加密隧道的关联以及数据报文的综合过滤，加密认证网关（十兆型）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。

点击“规则配置” → “策略配置”进入策略配置界面，之后选中相应的策略配置信息点击  进行编辑，若原来没有相应的策略信息规则可以先点击  （新建资源）再点击编辑资源进入策略配置界面，如图表 20 所示:

图表 20 策略配置

注意：如果对端加密认证网关（十兆型）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。

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，以便使用对应隧道的密钥对对需要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。

内网起始地址和内网终止地址：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。

外网起始地址和外网终止地址：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、ICMP 等通信协议。

策略方向：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。

内网起始端口和内网终止端口：通信端口配置范围在 0－65535 之间。

外网起始端口和外网终止端口：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。

3.3.6 地址转换配置

加密认证网关（十兆型）系统支持地址转换（地址伪装、源地址转换和目的地址转

换），保护内网私有地址。

加密认证网关（十兆型）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，发送至下一跳网关。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。

某些环境下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。

点击“规则配置” → “地址转换”进入地址转换配置界面，之后选中相应的地址转换配置信息点击  进行编辑，若原来没有相应的地址转换信息规则可以先点击  （新建资源）再点击编辑资源进入地址转换配置界面，如图表 21 所示：

图表 21 地址转换配置

NAT 描述：地址转换信息的描述。

类型选择：选择地址转换的类型，具体类型有源地址转换、目的地址转换。

内网地址：提供服务的内网主机地址。

内网端口：内网服务端口。

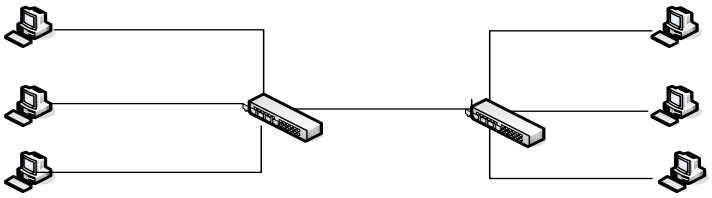
外网地址：加密网关的外网虚拟地址。

外网端口：内网服务端口的映射。

网络接口：配置地址转换的网络接口名称。

3.3.7 桥接配置（多进多出配置）

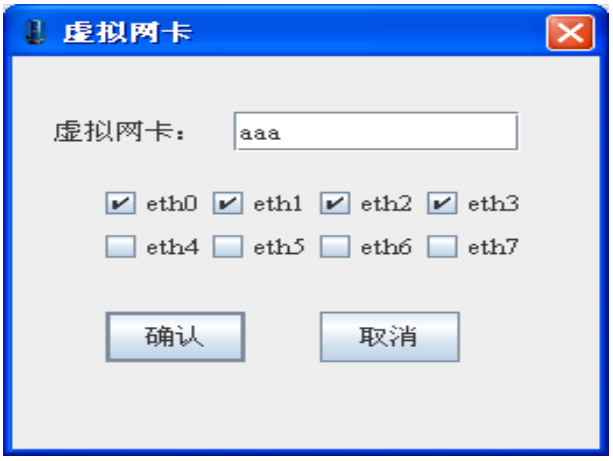
桥接工作模式的作用相当于一个局域网交换机，可以实现将装置的某几个网卡虚拟成一个网卡和外界通信，用户可以将虚拟网卡当成具体的网卡来使用，可以在隧道配置中设置相应的规则，以虚拟网卡地址和对端的加密网关协商从而实现多入多出的通信，相关的网络拓扑如图表 22 所示：



图表 22 桥接示例

具体配置如下：

点击“规则配置” → “网桥配置”进入网桥配置界面，点击编辑资源  ，进入具体网桥配置界面，如图表 23 所示：



图表 23 桥接网络接口选择

可以将某几个网卡加入到一个虚拟网卡中，点击确认保存之后，虚拟网卡的名字即可在以后的配置中使用。例如在配置网络信息时可以为虚拟网卡设置相应的网络地址信息。在网络配置界面中将网络接口设成 BRIDGE，接口描述为虚拟网卡的名称，配置后的界面如图表 24 所示：

图表 24 桥接配置信息

3.3.8 ARP 绑定

借用地址环境下，装置往往需要内网借用外网路由器的地址，外网借用内网交换机的地址，这时候装置不能主动获得路由器和交换机的 MAC 地址，所以需要我们将路由器和交换机的 MAC 地址和各自的 IP 绑定。

具体配置如下

点击“规则配置” → “ARP 绑定”进入 ARP 绑定配置界面，点击编辑资源  ，进入具体 ARP 绑定配置界面，如图表 25 所示：

图表 25　ARP 绑定配置信息

IP 地址：将要绑定的 IP 地址。

MAC 地址：为该 IP 地址即将绑定的 MAC 地址。

网口：该 IP 地址跟装置哪个网口互联。

VlanID：该 IP 地址所处的 Vlan 段。

3.3.9 网口 MAC 配置

在网络管理中，IP 地址盗用现象经常发生，不仅对网络的正常使用造成影响，同时由于被盗用的地址往往具有较高的权限，因而也对用户造成了大量的经济上的损失和潜在的安全隐患。为了防止 IP 地址被盗用，可以在代理服务器端分配 IP 地址时，把 IP 地址与网卡地址进行捆绑。

MAC 地址绑定功能用于实现将具体的通信地址和网卡绑定，只允许具有特定 MAC 地址的网卡使用某个 IP 地址和外界通信，如果更换网卡就必须重新进行相应的配置。

具体配置如下：

点击“规则配置” → “网口 MAC 配置”进入 MAC 绑定的操作界面，界面中有网口、MAC 地址和 VlanID 选项，网口选择相应的网口，MAC 地址中填入将要绑定的 MAC 地址，VlanID 填入相应的 VlanID(如没有划分 Vlan 则填 0)以实现 MAC 地址绑定，如图表 26 所示

图表 26 MAC 地址绑定配置信息

3.3.10 透传协议配置

透传协议配置是为了配置装置在某些情况下可以不处理特定的报文，直接转发。

具体配置如下：

点击“规则配置” → “透传协议配置”进入透传协议的操作界面，界面中有源 IP，目的 IP，协议号，进网口，出网口 VlanID 等配置项。源 IP 和目的 IP 可以写具体地址，或者 0.0.0.0 表示不限制地址，进网口和出网口标识了报文的方向 VlanID 可限制具体的 Vlan 的透传，如图表 27 所示，表示任意外网地址到内网 10.144.99.80 这个地址的协议号为 89 的报文全部不处理直接透传。

图表 27　透传协议配置

3.4 信息查询

3.4.1 隧道管理

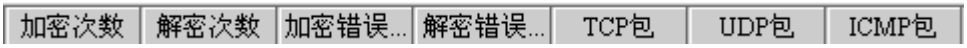
图表 28 隧道列表示意图

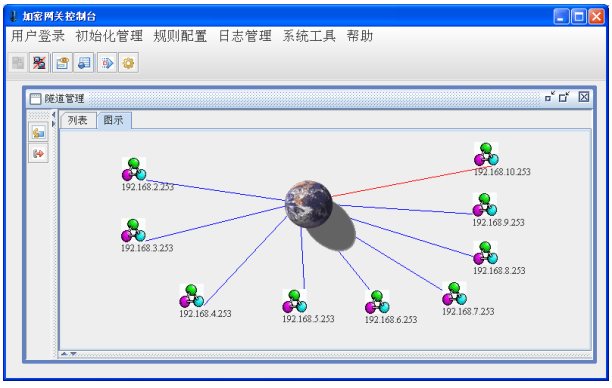
加密认证网关（十兆型）配置管理软件可以实时浏览装置的隧道信息，点击左侧的更新  按钮。 隧道信息按照列表和图标两种显示方式方便用户审阅。选中某个隧道后可以通过重置  按钮，对隧道重置，令其重新协商。

ID： 隧道的 ID 信息。

状态：  隧道正常，  隧道异常。

热备：  对端装置是主机，  对端装置是备机;

统计信息： 



图表 29 隧道拓扑示意图

3.4.2 链路管理

加密认证网关（十兆型）配置管理软件可以实时显示装置链路信息、链路的状态和链路的统计信息。用户只需点击左侧的更新  按钮就可以实时查询。

ID：按照顺序标记链路的记数。

协议：链路的协议，目前只支持 TCP、UDP、ICMP 三种。

状态：  链路状态正常，  链路状态异常，其中异常主要针对 TCP 协议，一旦出现三步握手没有成功则显示链路异常。

源地址和源端口：装置所在内网侧应用信息。

目的地址和目的端口：装置所在外网侧应用信息。

统计信息：IN 为内向外报文个数，OUT 为外向内报文个数。

图表 30 链路实时浏览

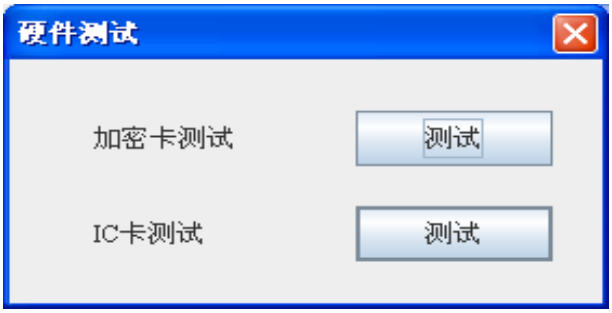
3.5 系统调试

3.5.1 网关硬件诊断

加密认证网关（十兆型）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“硬件卡测试”，则出现如图 31 的界面，点击“加密卡测试”对应的测试按钮，加密网关自动对加密单元进行检测，检测完成后弹出测试结果窗口。



图表 31 加密单元测试界面

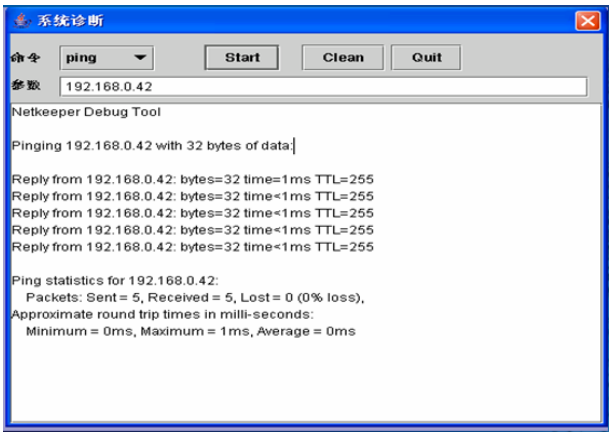
2) 智能 IC 卡单元测试

点击 “IC 卡测试”对应的测试按钮，加密网关自动对智能 IC 读写器单元进行检测，检测完成后弹出测试结果窗口。

如果提示测试失败，请检查您的卡片是否插入正确（带有标签的那一面朝上），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，请及时与我们联系。

3.5.2 SPING 调试

SPING 调试用于确认和对端加密网关的连通情况，在 SPING 调试界面中输入对端加密网关的外网虚拟 IP 地址、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，如图表 32 所示。



图表 32　SPING 诊断

3.6 日志管理

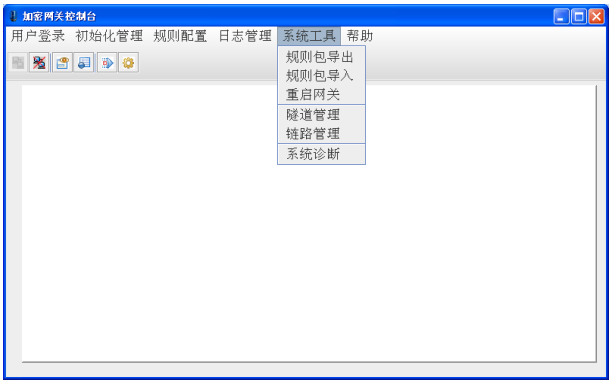
加密认证网关（十兆型）具备专用安全日志存储单元，可以对装置日志进行审计。

点击导航栏或者菜单“日志管理”中的“日志审计”，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，如图表 33 所示。点击  可以刷新当前页面，点击  可以审计历史日志。

图表 33 日志分析界面

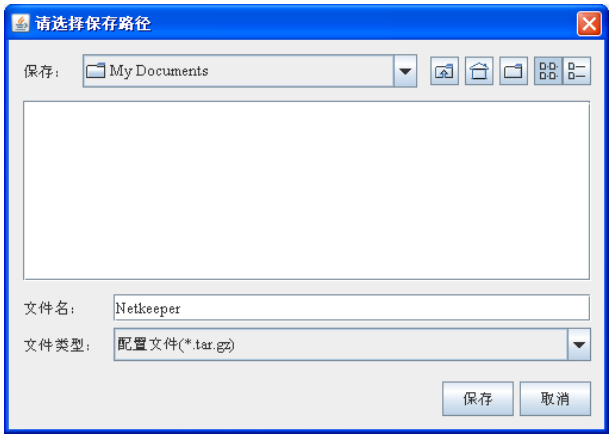
3.7 配置备份和恢复

加密认证网关（十兆型）配置备份模块用于将装置中的相关配置信息备份至本地，配置恢复模块用于将本地的配置文件同步更新到加密网关中，具体操作界面菜单如图表 34 所示：



图表 34 配置备份和恢复

点击“规则包导出”选择相应的保存路径如图表 35 所示：



图表 35 选择备份目录

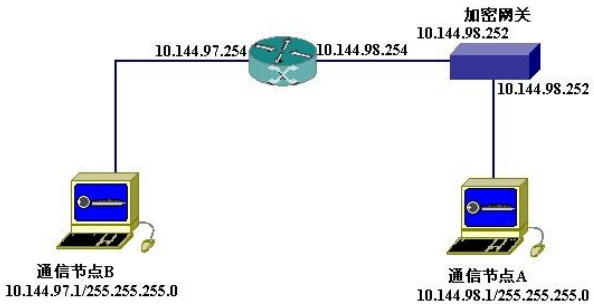
保存成功后会弹出保存成功对话框，将在所选择目录下生成所输入文件名加.tar.gz 后缀名的文件，如图表 36 所示：

图表 36 成功备份文件

四、典型简单应用环境配置案例

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。此时加密认证网关（十兆型）具备硬件防火墙的基本功能，只转发配置通信策略的报文实现报文过滤，但数据不能进行加密保护，明通网络拓扑如图表 37 所示。加密网关配置如下。



图表 37 明通模式拓扑图

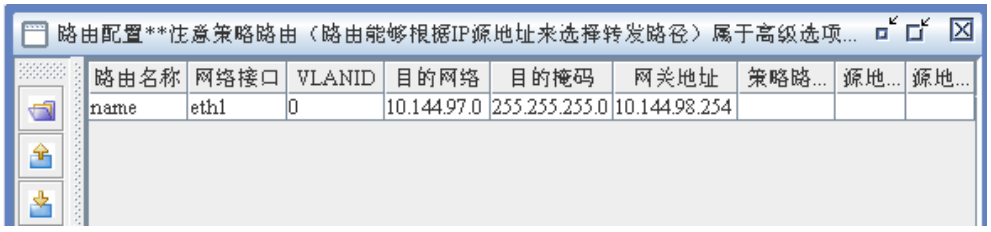
4.1.1 系统配置

图表 38 明通模式-系统配置

4.1.2 网络配置

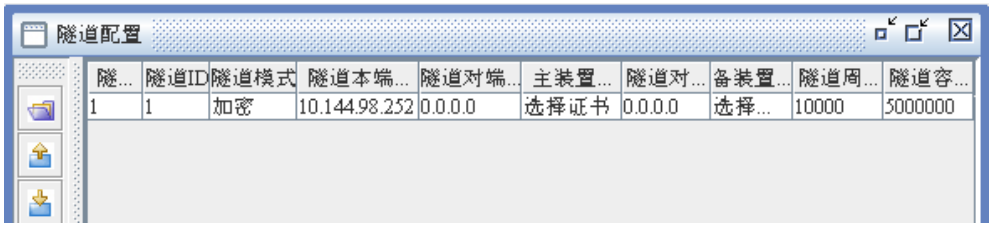
图表 39 明通模式-网络配置

4.1.3 路由配置



图表 40 明通模式-路由配置

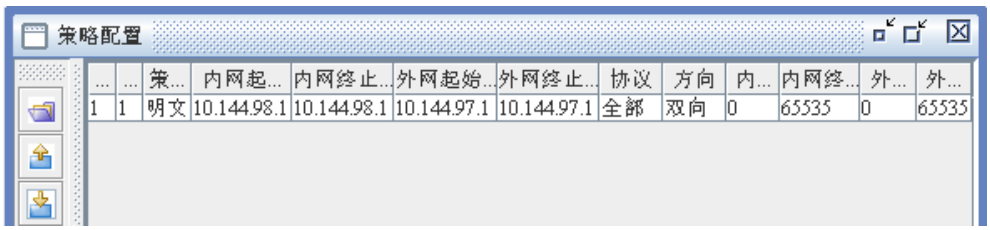
4.1.4 隧道配置



图表 41 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 0.0.0.0，隧道模式为明通。

4.1.5 策略信息配置

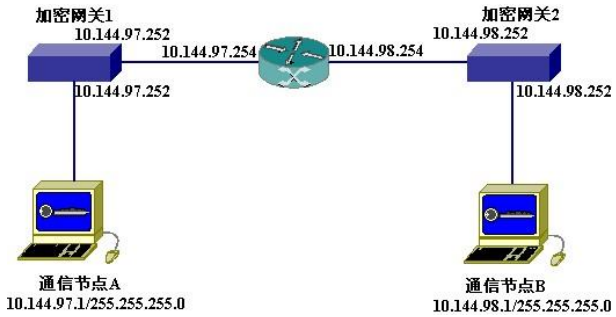


图表 42 明通模式-策略配置

注意：由于对端无加密网关，因此策略配置中策略模式选择为明文。

4.2 路由配置

纵向加密认证网关（十兆型）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，典型网络拓扑如图表 43 所示。策略配置以加密网关 2 为例。



图表 43 路由配置网络拓扑图

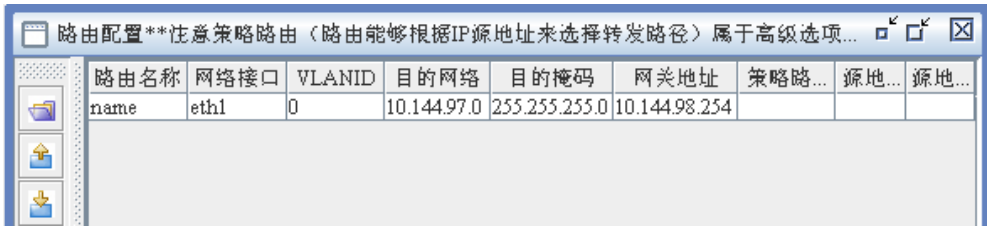
4.2.1 系统配置

图表 44 路由模式-系统配置

4.2.2 网络配置

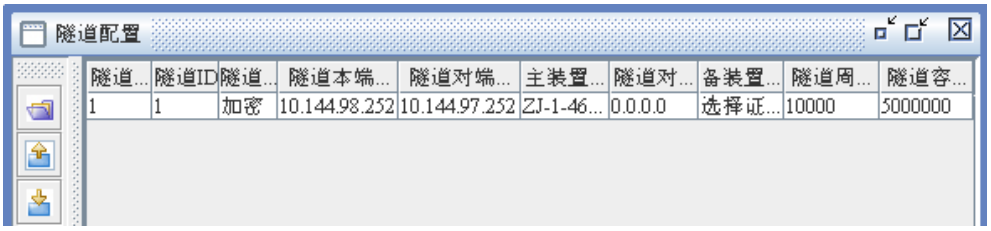
图表 45 路由模式-网络配置

4.2.3 路由配置



图表 46 路由模式-路由配置

4.2.4 隧道配置



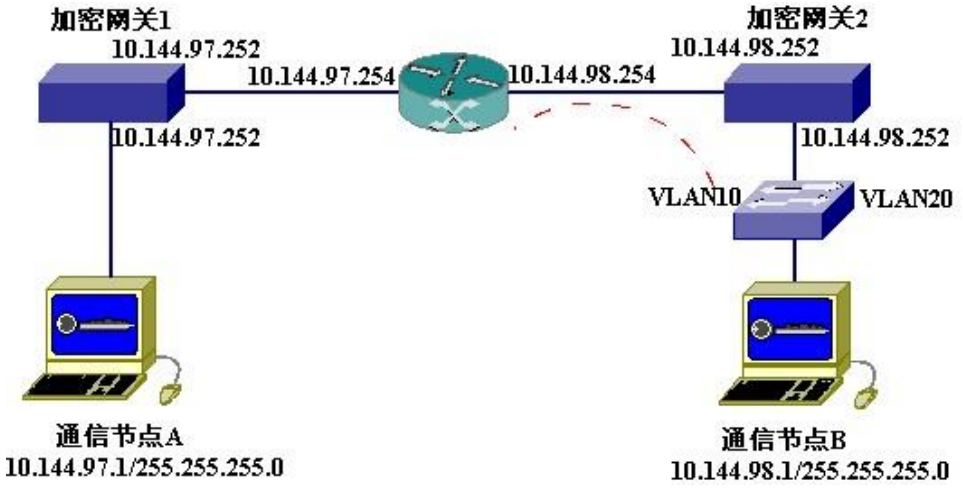
图表 47 路由模式-隧道配置

4.2.5 策略配置

图表 48 路由模式-规则配置

4.3 VLAN 环境配置

加密认证网关（十兆型）支持 VLAN 接入，典型配置拓扑如图表 49 所示。交换机上划分了两个 VLAN 网段（VLAN 10/VLAN 20），在路由器与交换机相连的端口划分子端口，使子端口与交换机上的 VLAN 通过 802.1Q 建立对应通信关系。通信节点 B 位于交换机的 VLAN10 网段。策略配置以加密网关 2 为例。

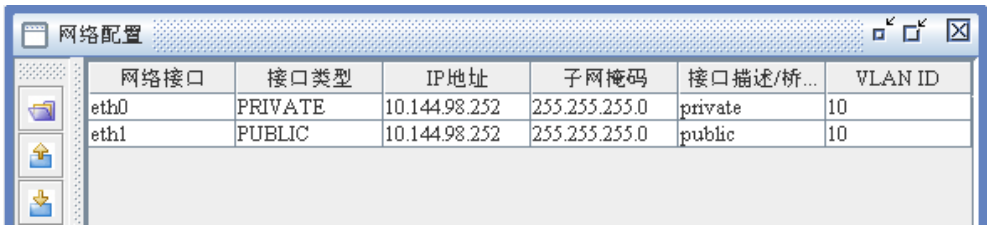


图表 49 VLAN 环境网络拓扑

4.3.1 系统配置

图表 50 VLAN 环境-系统配置

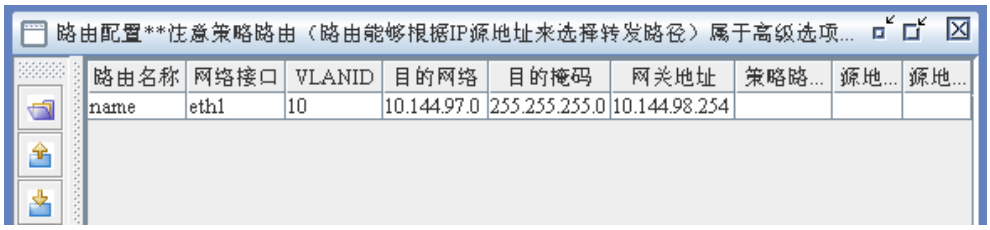
4.3.2 网络配置



图表 51 VLAN 环境-网络配置

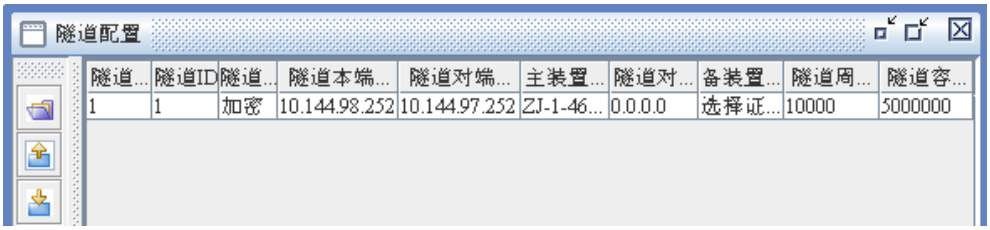
注意：此处需要配置网络的 VLAN ID。

4.3.3 路由配置



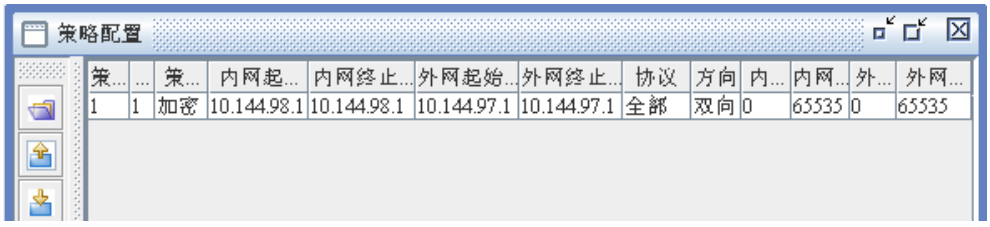
图表 52 VLAN 环境-路由配置

4.3.4 隧道配置



图表 53 VLAN 环境-隧道配置

4.3.5 策略配置

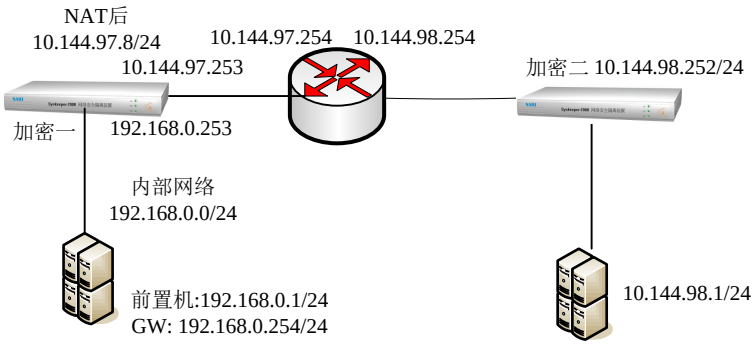


图表 54 VLAN 环境-策略配置

4.4 NAT 模式配置

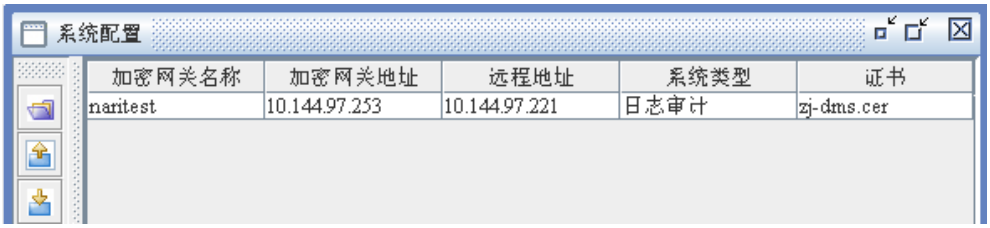
加密认证网关（十兆型）系统支持 NAT 地址转换（地址伪装和目的地址转换），保护内网私有地址，典型网络拓扑如图表 55 所示。加密网关 1 启动地址转化功能，策略

配置以加密网关 1 为例。



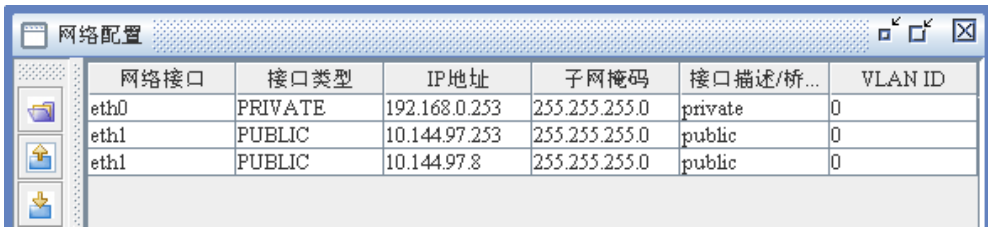
图表 55 NAT 环境网络拓扑

4.4.1 系统配置



图表 56 NAT 模式－系统配置

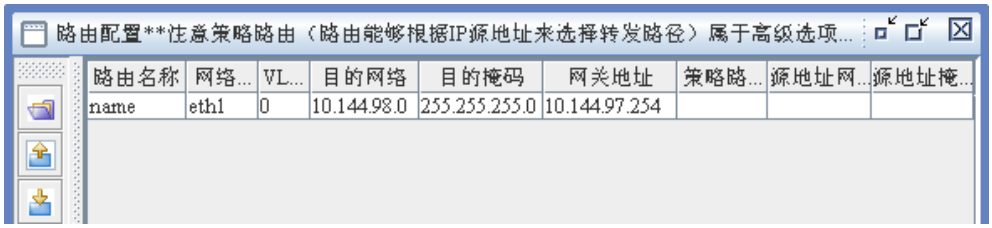
4.4.2 网络配置



图表 57 NAT 模式－网络配置

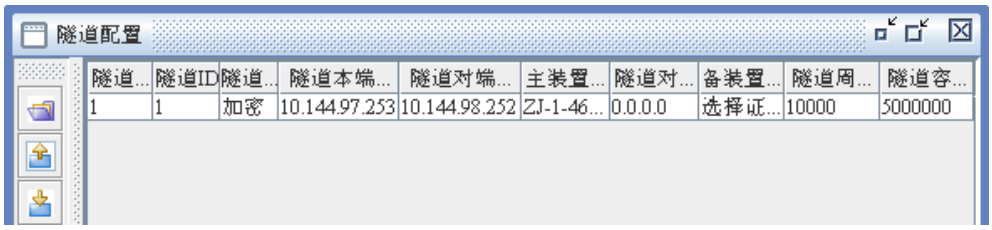
这里需要注意的是内网配置内部网段的地址，外网除了配置外部网段地址外，还需要配置内网业务机映射在外网的地址。

4.4.3 路由配置



图表 58 NAT 模式-路由配置

4.4.4 隧道配置



图表 59 NAT 模式-隧道配置

4.4.5 地址转化配置

只需要配置一条源地址转换规则，用于对本端发出去的报文进行地址转换匹配，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。

图表 60 NAT 模式-地址转化配置

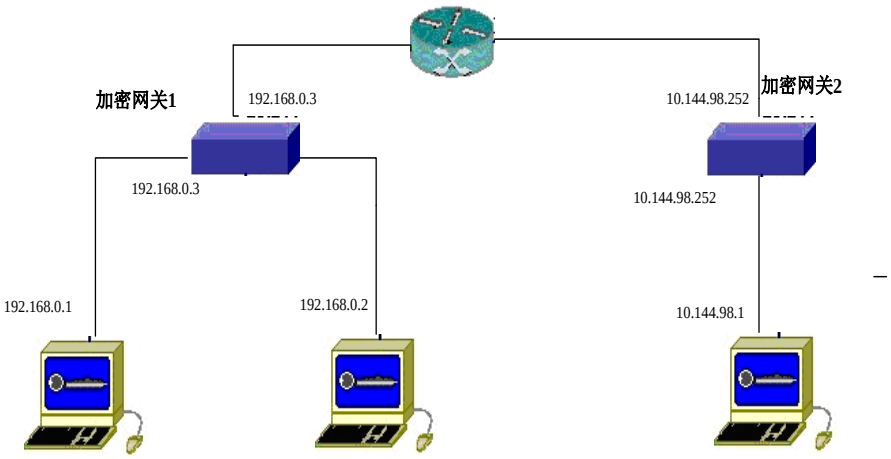
4.4.6 策略配置

图表 61 NAT 模式-策略配置

这里需要配置两条策略规则，一条是从内网 NAT 前地址到外网的策略，一条是 NAT 以后地址到外网的策略。

4.5 网桥模式配置

当加密认证网关（十兆型）具备多进多出功能时，需要对装置的网桥模式进行配置。典型拓扑如下所示，假设加密网关 1 启动网桥功能，策略配置以加密网关 1 为例。



图表 62 网桥模式网络拓扑图

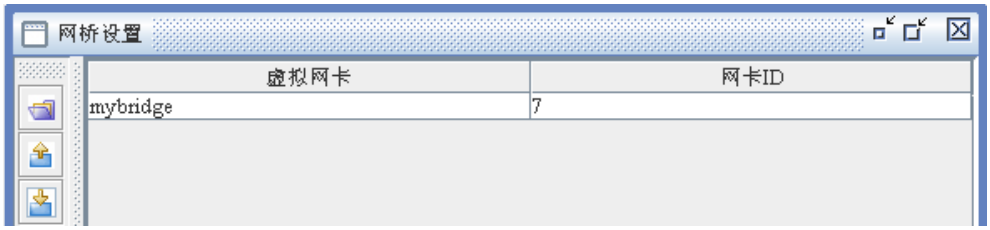
4.5.1 系统配置

图表 63 网桥模式-系统配置

4.5.2 桥接配置

图表 64 网桥模式-桥接接口配置

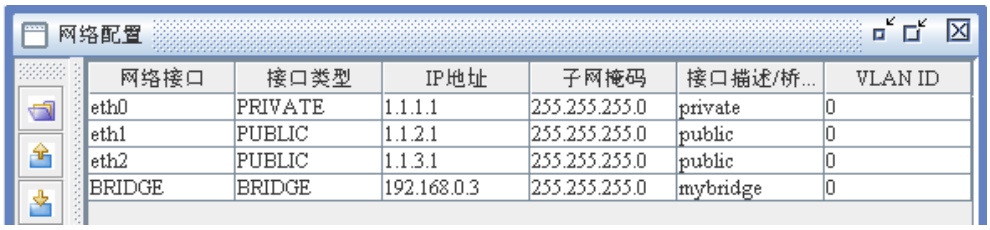
这里将装置的 eth0、eth1、eth2 划分在一个桥接组中，定义虚拟网卡名称为 mybridge，保存后的界面如图表 65，网卡 ID 是根据用户选择的各个网卡所得到的一个值。



图表 65　网桥模式-网桥配置

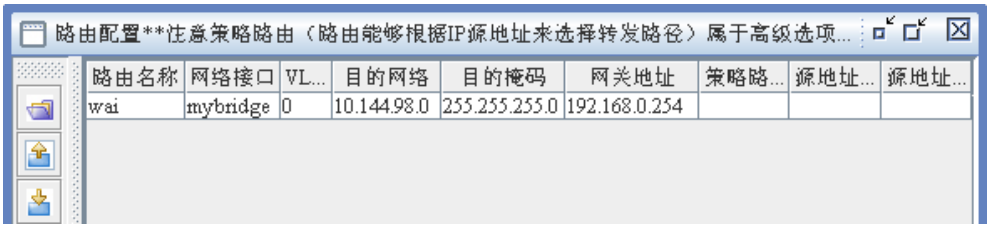
4.5.3 网络配置

先设置两个虚拟网络接口 eth0，eth1 ，接口类型为 PRIVATE，再设置一个虚拟网络接口 eth2，接口类型为 PUBLIC，这三个接口地址随意填；然后设置桥的网络接口，接口类型为 BRIDGE，接口描述为桥接配置中设置的虚拟网卡的名称 mybridge，将分配的 ip 地址作为桥的 ip 地址，具体配置界面如图表 66 所示：



图表 66 网桥模式-网络配置

4.5.4 路由配置



图表 67 网桥模式-路由配置

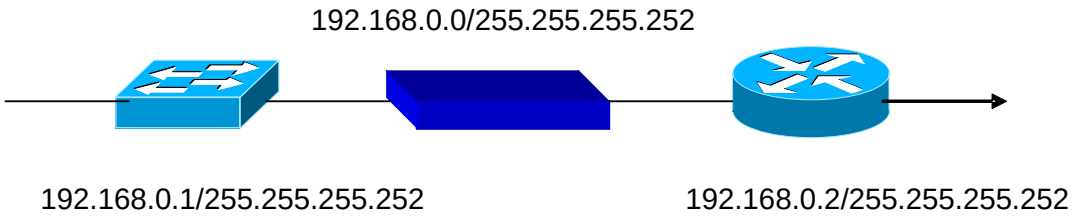
路由网络接口这里需要手动双击该单元表格输入 mybridge 即定义的桥的名称，网关地址为 192.168.0.254（拓扑图中未标注），由路由器完成不同网段之间的数据转发。

4.5.5 隧道配置

图表 68 网桥模式-隧道配置

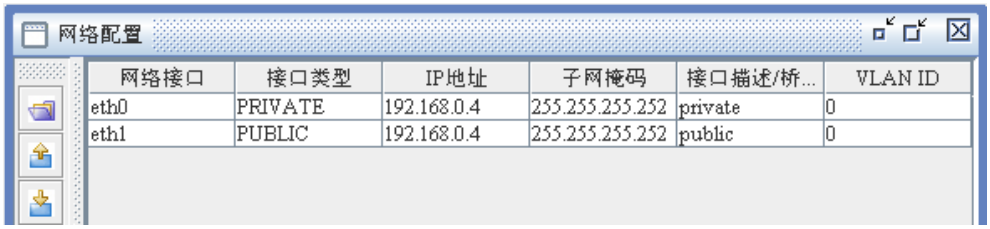
4.6 借用地址配置

在实际的网络接入环境中，用户从安全考虑将网络地址子网掩码设置为255.255.255.252，共 4 个地址，如图表 69 所示。由于网络地址、广播地址占用两个地址，所以加密网关没有办法配置可用的虚拟地址，为此需要进行借用地址配置。



图表 69 借用地址网络拓扑图

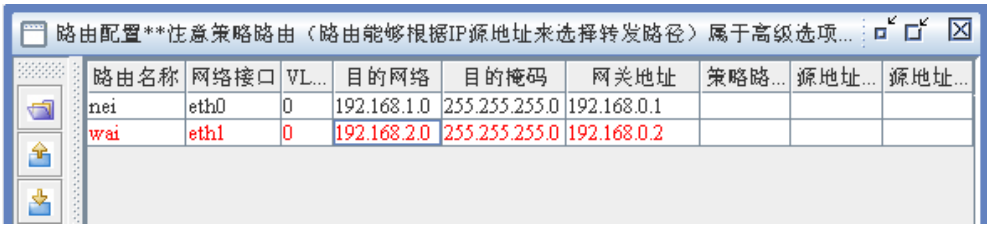
4.6.1 网络配置



图表 70 借用地址-网络配置

这里 192.168.0.4 是根据路由器和交换机地址虚拟出来的地址，一般为其中大的地址尾数加 2。

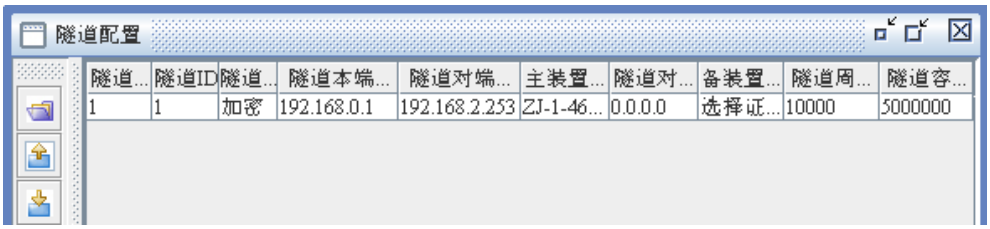
4.6.2 路由配置



图表 71 借用地址-路由配置

这里有两条路由，一是指向内网的 192.168.1.0/24 网段，网关地址指向交换机地址192.168.0.1，二是指向外网的 192.168.2.0/24 网段，网关地址指向路由器地址 192.168.0.2。

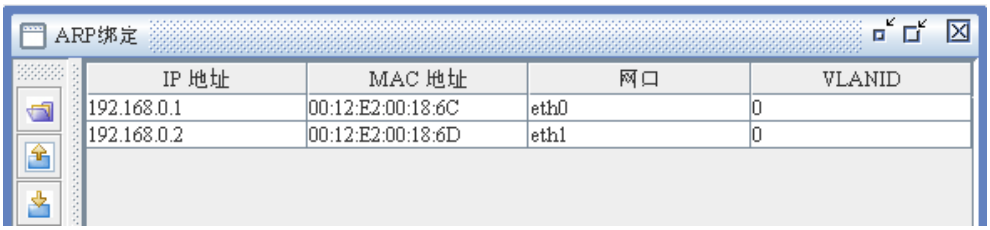
4.6.3 隧道配置



图表 72 借用地址-隧道配置

这里隧道本端地址应借用交换机地址 192.168.0.1，与外网通信。

4.6.4 ARP 绑定配置



图表 73 借用地址-ARP 绑定配置

由于借用地址环境下，装置不能主动获得路由器交换机的 MAC 地址，所以需要将路由器和交换机的 MAC 地址和各自的 IP 地址进行绑定。

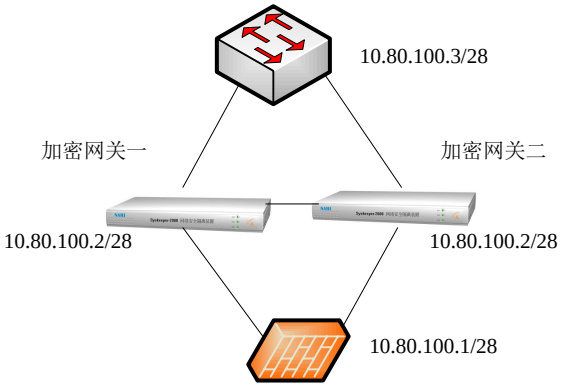
4.6.5 网口 MAC 配置

图表 74 借用地址-网口 MAC 配置

这里需要将内网交换机的 MAC 地址绑定到装置的外网口上，将外网路由器的 MAC 地址绑定到装置的内网口上，使外网路由器将装置认作交换机，内网交换机将装置认作路由器，达到借用地址的目的。

4.7 双机配置

图表 75 为某现场的双机工作网络拓扑，双机位于同一网段。



图表 75 双机工作拓扑图

双机主备对等，所以其双机配置相同，下面以加密网关一为例。

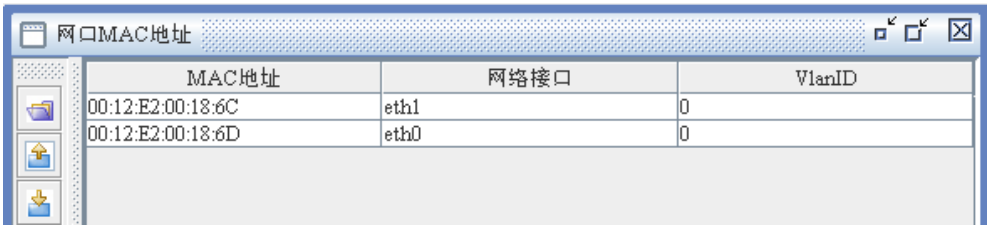
4.7.1 网络配置

网络接口	接口类型	IP地址	子网掩码	接口描述/桥...	VLAN ID
eth0	PRIVATE	10.80.100.2	255.255.255.0	private	0
eth1	PUBLIC	10.80.100.2	255.255.255.0	public	0
eth3	BACKUP	0.0.0.0	0.0.0.0	Just a desc	0

图表 76 双机网络配置

这里除了内外网地址配置为分配的 IP 地址外，还需要配置 eth3 口为心跳口，心跳口地址填 0.0.0.0，掩码也填 0.0.0.0。

4.7.2 MAC 地址绑定配置



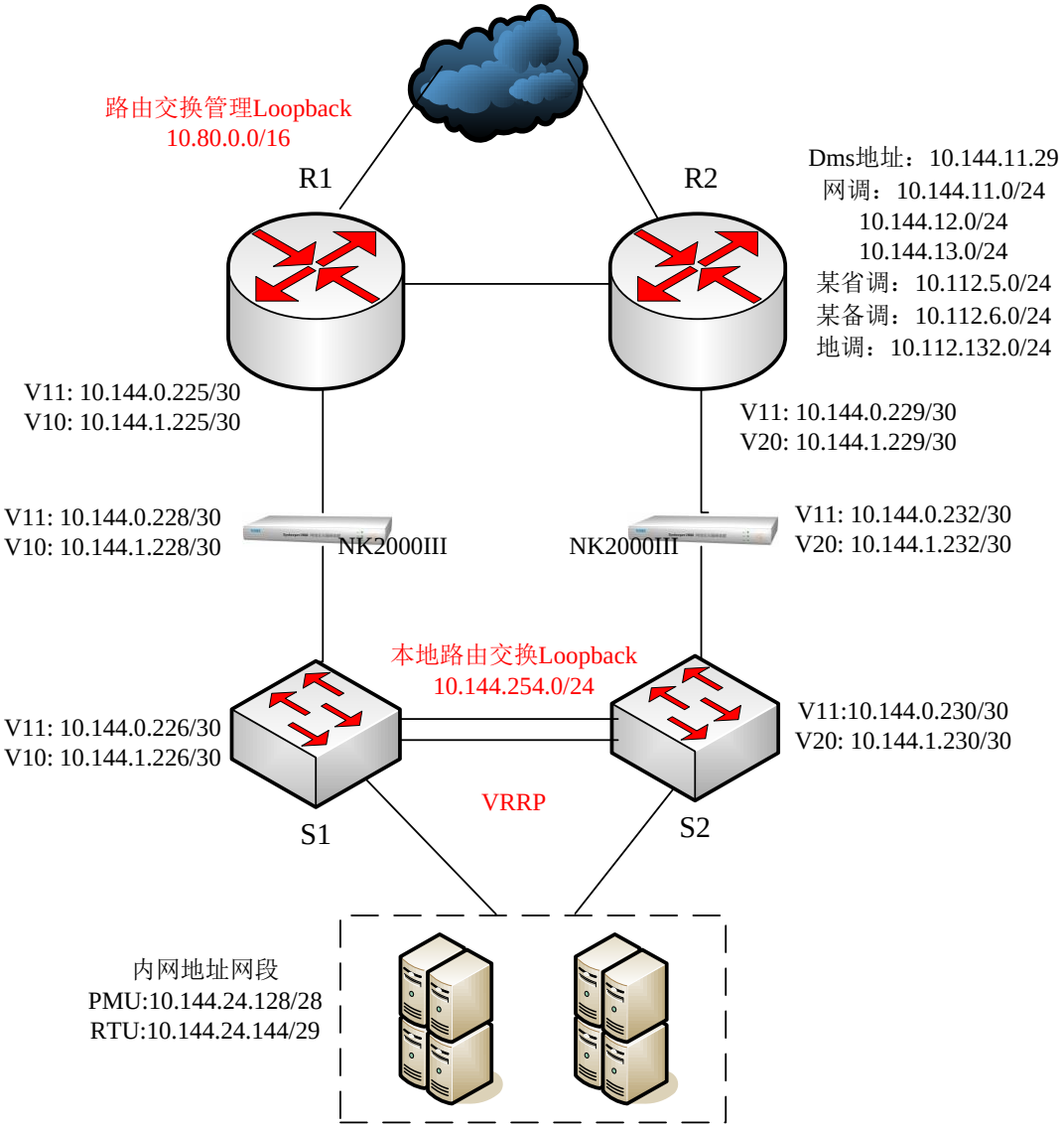
MAC地址	网络接口	VlanID
00:12:E2:00:18:6C	eth1	0
00:12:E2:00:18:6D	eth0	0

图表 77 双机 MAC 地址绑定配置

这里需要将 MAC 地址绑定，加密网关二的配置可由加密网关一导出并直接导入重启。注意需要将两装置的心跳口即配置的 Eth3 口用交叉线连接。

五、典型复杂应用环境配置案例

5.1 典型环境一



图

表 78 典型环境一拓扑

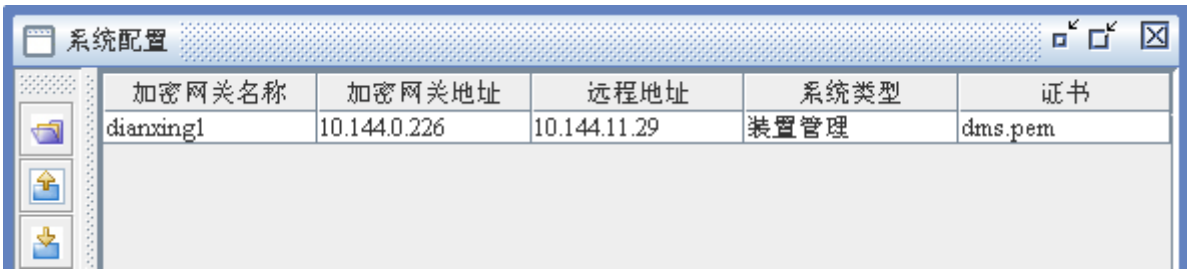
图表 78 所示环境为双交换双路由的方形接入模式：两台交换机启用 vrrp 协议，针对每个 VLAN 业务段分别虚拟出一个网关地址供内部业务使用；路由器交换机之间启用 OSPF 协议以实现交换机路由器的主备交互及动态切换。

对于内部应用来说，1 区业务优先通过 S1-R1 通信，当 S1-R1 间链路不畅时，利用两交换机之间的 TRUNK 经 S1-S2-R2 进入广域网；类似的，2 区业务优先通过 S2-R2 通

信。

这个环境结合了借用地址，OSPF，VRRP 等环境，我们以 S1-R1 间的加密网关为例。

5.1.1 系统配置



图表 79 典型环境一系统配置

这里加密网关地址借用的 S1 的 Vlan11 的地址作为装置外网口地址对外通信，远程地址是远程装置管理系统地址。

5.1.2 网络配置

图表 80 典型环境一网络配置

这里两个 VLAN 需要分别配置 IP 地址。

5.1.3 路由配置

图表 81 典型环境一路由配置

第一条路由是业务段指向内网业务，网关是交换机的业务 VLAN 互联地址。

第二条路由是业务段指向外网业务，网关是路由器的业务 VLAN 互联地址。

第三条路由是管理段指向内网管理 Loopback 地址段，网关是交换机的管理 VLAN 互联地址。

第四条路由是管理段指向外网管理 Loopback 地址段，网关是路由器的管理 VLAN 互联地址。

5.1.4 隧道配置

隧道名称	隧道ID	隧道模式	隧道本端...	隧道对端主...	主装...	隧道...	备装置...	隧道...	隧道...
1	1	加密	10.144.0.226	10.144.11.33	517.cer	0.0.0.0	选择证...	10000	50000...
2	2	加密	10.144.0.226	10.144.11.34	448.cer	0.0.0.0	选择证...	10000	50000...
3	3	加密	10.144.0.226	10.144.12.33	487.cer	0.0.0.0	选择证...	10000	50000...
4	4	加密	10.144.0.226	10.144.12.34	459.cer	0.0.0.0	选择证...	10000	50000...

图表 82 典型环境一隧道配置

隧道本端地址借用交换机实时段互联地址。

5.1.5 策略配置

策...	隧...	策...	内网起始地...	内网终止地址	外网起始...	外网终止地址	协议	方向	内...	...	外...	外...
1	1	明文	10.0.0.0	10.255.255.255	10.0.0.0	10.255.255.255	ICMP	双向	0	6...	0	65...
2	1	明文	10.144.254.0	10.144.254.255	10.0.0.0	10.255.255.255	全部	双向	0	6...	0	65...
3	1	加密	10.144.24.128	10.144.24.191	10.144.11.1	10.144.11.254	全部	双向	0	6...	0	65...
4	2	加密	10.144.24.128	10.144.24.191	10.144.11.1	10.144.11.254	全部	双向	0	6...	0	65...
5	3	加密	10.144.24.128	10.144.24.191	10.144.12.1	10.144.12.254	全部	双向	0	6...	0	65...
6	4	加密	10.144.24.128	10.144.24.191	10.144.12.1	10.144.12.254	全部	双向	0	6...	0	65...
7	1	明文	10.144.24.128	10.144.24.191	10.112.5.1	10.112.5.254	全部	双向	0	6...	0	65...
8	1	明文	10.144.24.128	10.144.24.191	10.112.6.1	10.112.6.254	全部	双向	0	6...	0	65...
9	1	明文	10.144.24.128	10.144.24.191	10.112.132	10.112.132.254	全部	双向	0	6...	0	65...

图表 83 典型环境一策略配置

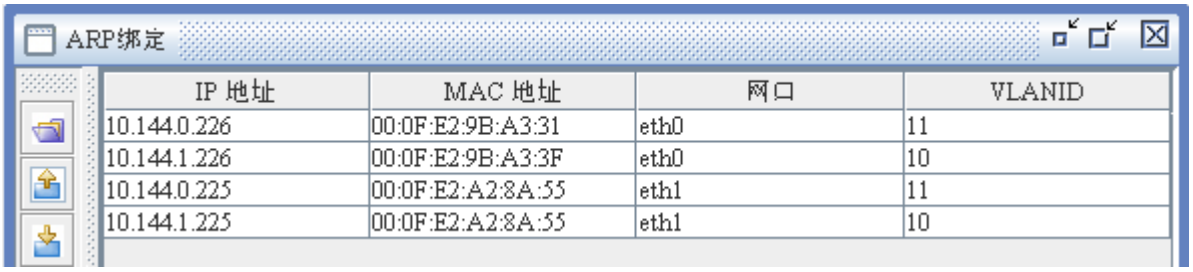
第一条是明文放过所有的 ICMP 报文(ping 包)

第二条是明文让内网 Loopback 地址可以被外网集中管理

第三到六条是内网业务机到分别到网调四台装置下面的业务加密

第七到九条是内网业务机到省调，备调和地调的业务暂时明文，因为对端无加密机。

5.1.6 ARP 绑定配置



图表 84 典型环境一 ARP 绑定配置

分别将两个 VLAN 的路由器交换机的 IP 地址与 MAC 地址绑定。

5.1.7 网口 MAC 配置

图表 85 典型环境一网口 MAC 配置

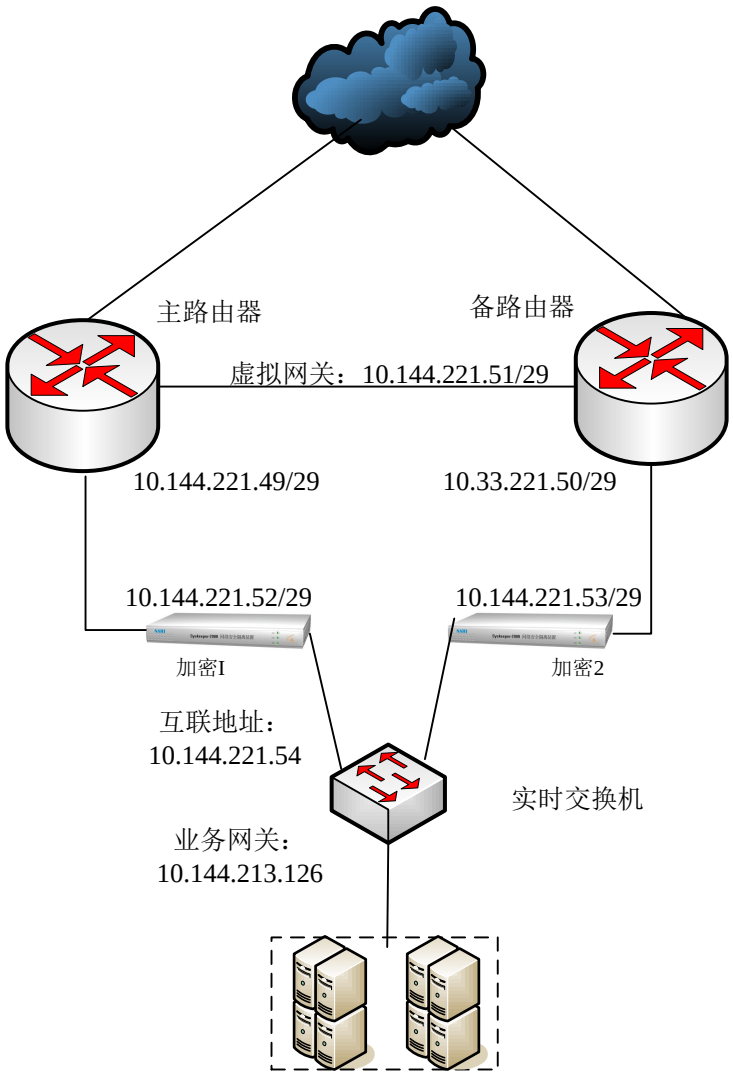
将装置的内网管理段 MAC 地址绑定为路由器管理段 MAC 地址，外网管理段 MAC 地址绑定为交换机管理段 MAC 地址。业务段的网口 MAC 不需要绑定。

5.1.7 透传协议配置

图表 86 典型环境一透传协议配置

这四条规则放开了这两个网段从内到外，从外到内的 OSPF 协议(协议号 89)，使得 OSPF 协议可以在该环境下生效。

5.2 典型环境二



图表 87 典型环境二拓扑

图表 87 所示环境是两路由器单交换机，两个路由器之间起 VRRP 协议，虚拟出 10.144.221.51 这个网关，两个路由器和交换机的互联地址是 10.144.221.49/50/54，业务网关 10.144.213.126 在交换机上。两台加密网关分别接在两个路由器和交换机之间，装置地址为 10.144.221.52/53。

该环境结合了 VRRP，桥接，主主模式等，策略配置以加密一为例。

5.2.1 系统配置

图表 88 典型环境二系统配置

5.2.2 网络配置

图表 89 典型环境二网络配置

桥接模式下将分配给装置的地址配在桥上。

5.2.3 路由配置

图表 90 典型环境二路由配置

外网路由指向外网，下一跳为主路由器网关，内网路由指向内网业务网段，下一跳为交换机互联地址，注意这里不能填交换机的业务网关，因为从装置到业务网关不是直接可达的，要通过互联地址转发。

5.2.4 隧道配置

图表 91 典型环境二隧道配置

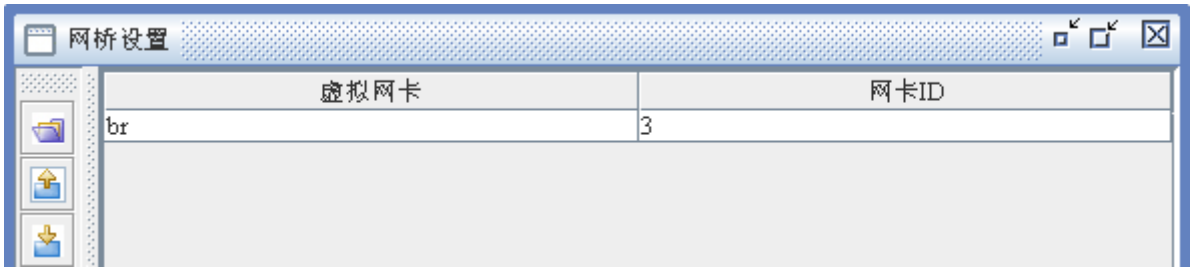
5.2.5 策略配置

图表 92 典型环境二策略配置

第一条为放过所有经过装置的 ICMP 包(ping 包)。

第二、三条是从内网业务机到对端业务机的加密策略。

5.2.6 桥接配置



图表 93 典型环境二桥接配置

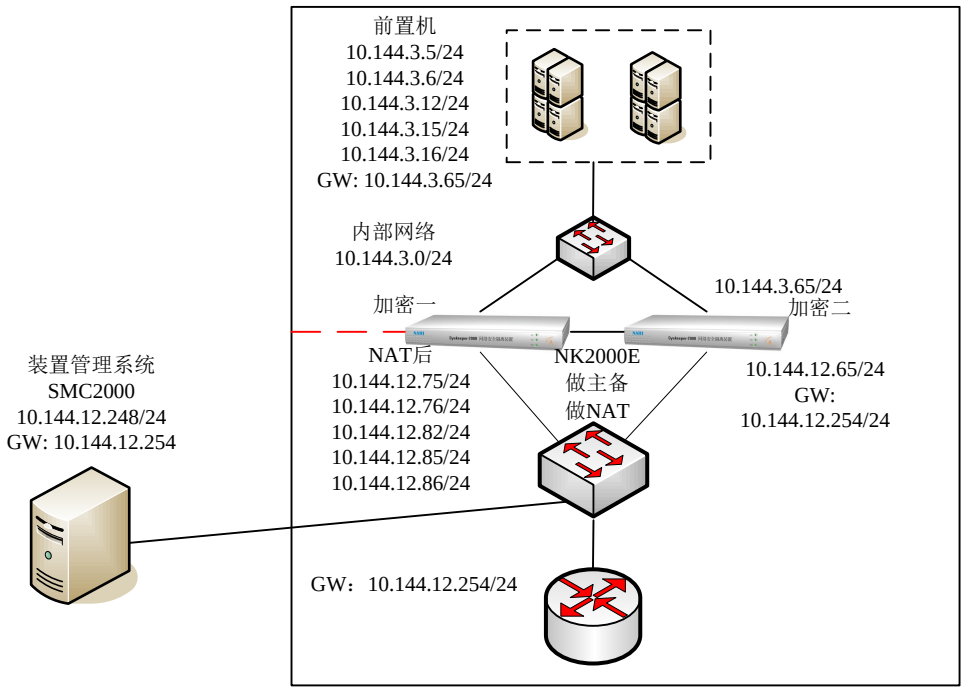
将 eth0 口和 eth1 口绑在一个桥上，命名为 br。

5.2.7 透传协议配置

图表 94 典型环境二透传协议配置

这里需要放过 Vrrp 协议(协议号 112)。

5.3 典型环境三



图表 95 典型环境三拓扑

该环境是单路由单交换，加密认证网关（十兆型）接在两者之间，作地址转换，两台加密认证网关（十兆型）做主备，配置完全一样；装置管理系统接在本地路由器上。配置以其中一台为例。

5.3.1 系统配置

图表 96 典型环境三系统配置

这里装置使用 10.144.12.65 作为外网地址对外通信

5.3.2 网络配置

图表 97 典型环境三网络配置

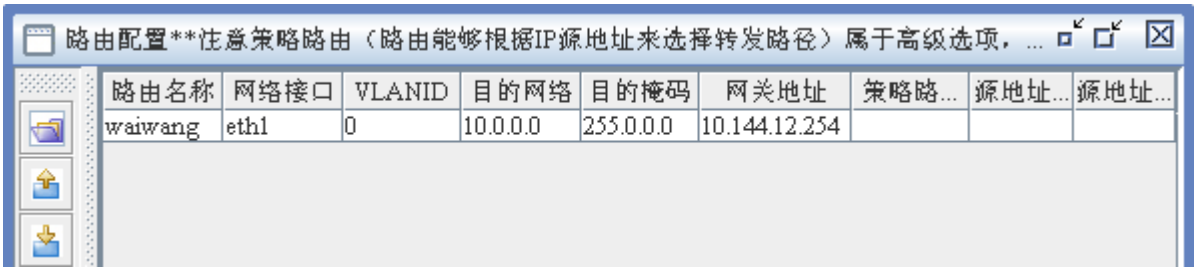
内网定义一个 10.144.3.65 作为装置内网口的地址，10.144.19.65 作为装置外网口地址，另外还需要定义内网 NAT 出来的所有地址作为装置外网口地址。

5.3.3 地址转换配置

图表 98 典型环境三地址转换配置

定义了五条地址转换规则，类型为源地址转换，分别将内网 10.144.3.5/6/12/15/16 转换为外网 10.144.12.65/66/72/75/76，网络接口为 eth1。

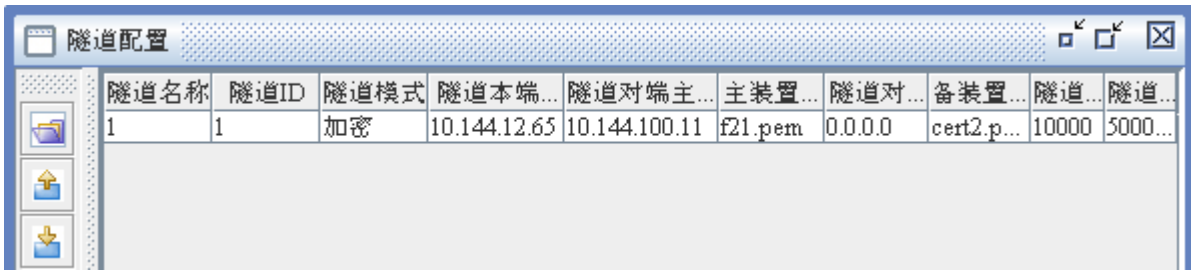
5.3.4 路由配置



图表 99 典型环境三路由配置

这里只需要定义一条外网路由指向路由器网关 10.144.12.254，接口为 eth1。

5.3.5 隧道配置



图表 100 典型环境三隧道配置

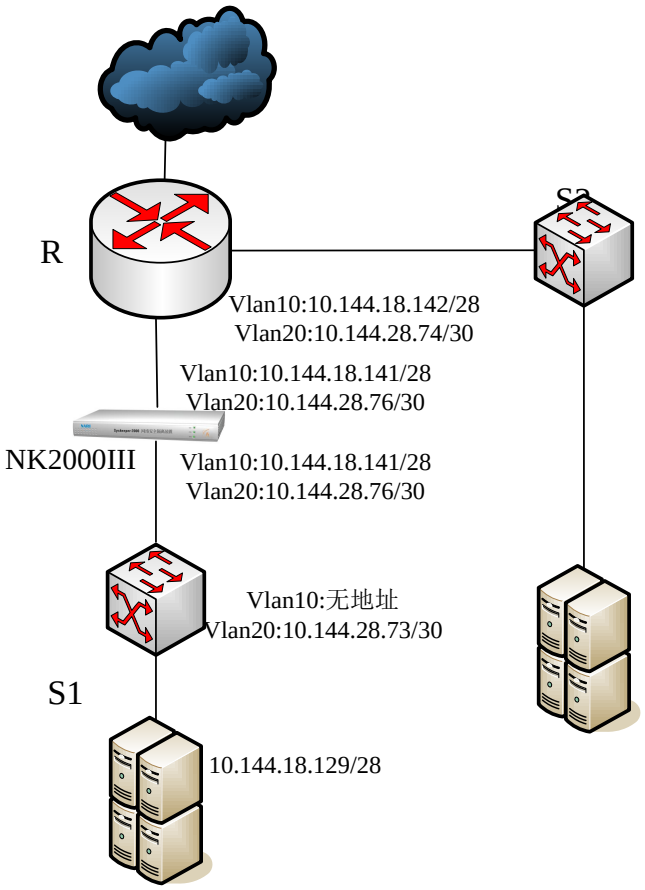
以 10.144.12.65 作为加密认证网关（十兆型）地址与对端装置建立隧道。

5.3.6 策略配置

图表 101 典型环境三策略配置

这里要写两条密文策略，一条内网地址为 NAT 前的业务地址，另一条内网地址外 NAT 以后的业务地址。注意对端装置若填写策略外网起始地址应填写 NAT 以后的地址，即 10.144.12.75/76/82/85/86。

5.4 典型环境四



图表 102 典型环境四拓扑

该环境是单路由，双交换，加密装置接在 R 和 S1 之间，划分了 2 个 vlan——10 和 20，10 是业务 vlan，20 是管理 vlan。业务段网关在路由器上，管理段掩码 30 位。该环境结合了划分 vlan，借用地址等模式。

5.4.1 系统配置

图表 103 典型环境四系统配置

10.144.18.141 是分配给装置使用的 vlan10 的地址。

5.4.2 网络配置


网络配置

网络接口	接口类型	IP地址	子网掩码	接口描述/桥...	VLAN ID
eth0	PRIVATE	10.144.18.141	255.255.255.240	Just a desc	10
eth1	PUBLIC	10.144.18.141	255.255.255.240	Just a desc	10
eth0	PRIVATE	10.144.28.76	255.255.255.252	Just a desc	20
eth1	PUBLIC	10.144.28.76	255.255.255.252	Just a desc	20

图表 104 典型环境四网络配置

Vlan10 内外网口都配 10.144.18.141，Vlan20 的地址由交换机和路由器地址虚拟出来，一般是两者之中大的那个加 2。

5.4.3 路由配置


路由配置**注意策略路由（路由能够根据IP源地址来选择转发路径）属于高级选项，...

路由名称	网络接口	VLANID	目的网络	目的掩码	网关地址	策略...	源...	源...
waiwang-yewu	eth1	10	10.144.0.0	255.255.0.0	10.144.18.142			
neiwang-guanli	eth0	20	10.144.28.73	255.255.255.2...	10.144.28.73			
waiwang-guanli	eth1	20	10.0.0.0	255.0.0.0	10.144.28.74			

图表 105 典型环境四路由配置

业务网段只需要写一个外网路由指向路由器网关，出口 eth1。

管理段需要写两个路由，一是指向外网路由器 20Vlan 互联地址，出口 eth1。

二是指向内网交换机 Vlan20 互联地址，出口 eth0。

5.4.4 隧道配置


隧道配置

隧道名称	隧道ID	隧道模式	隧道本端地址	隧道对端...	主装置证书	隧道...	备装...	隧...	隧...
1	1	加密	10.144.18.141	10.144.1.11	ZJ-1-462.cer	0.0.0.0	cert2....	100...	500...
2	2	加密	10.144.18.141	10.144.1.12	ZJ-2-474.cer	0.0.0.0	cert2....	100...	500...

图表 106 典型环境四隧道配置

5.4.5 策略配置

策...	...	策...	内网起始...	内网终止地址	外网起...	外网终止地址	协议	方向	内网...	内...	...	...
1	1	明文	10.0.0.0	10.255.255.255	10.0.0.0	10.255.255.255	ICMP	双向	0	65...	0	6...
2	1	加密	10.144.18.128	10.144.18.140	10.144.1.1	10.144.1.63	全部	双向	0	65...	0	6...
3	2	加密	10.144.18.128	10.144.18.140	10.144.1.1	10.144.1.63	全部	双向	0	65...	0	6...
4	1	明文	10.144.28.73	10.144.28.73	10.144.0.0	10.144.255.255	全部	双向	0	65...	0	6...

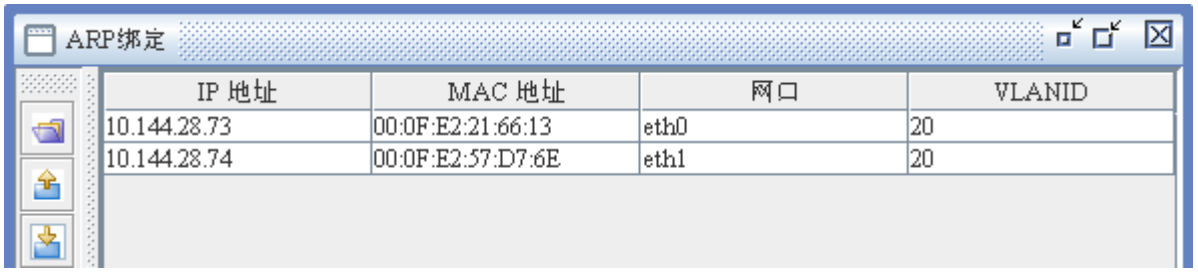
图表 107 典型环境四策略配置

第一条为放过所有的 ICMP 报文(即 ping 包)。

第二三条为内网业务地址到外网的加密策略。

第四条为交换机互联地址到外网的明通策略，使交换机可被远程管理。

5.4.6 ARP 绑定配置



IP 地址	MAC 地址	网口	VLANID
10.144.28.73	00:0F:E2:21:66:13	eth0	20
10.144.28.74	00:0F:E2:57:D7:6E	eth1	20

图表 108 典型环境四 ARP 绑定配置

将路由器和交换机的互联地址与他们的 MAC 地址分别绑定。

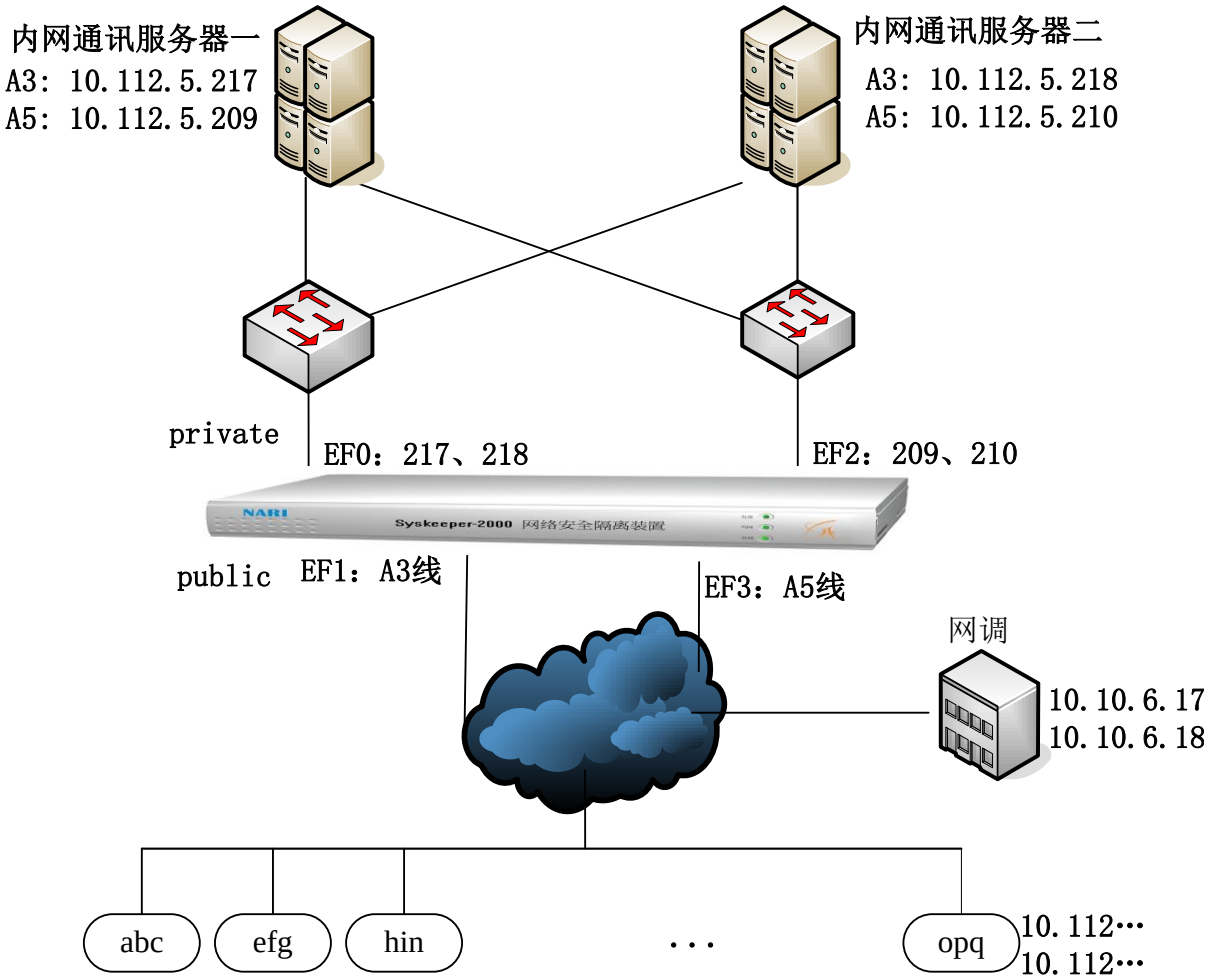
5.4.6 网口 MAC 地址配置

MAC地址	网络接口	VlanID
00:0F:E2:57:D7:6E	eth0	20
00:0F:E2:21:66:13	eth1	20

图表 109 典型环境四网口 MAC 地址配置

将路由器管理段 MAC 地址绑在装置内网口管理段地址上，交换机管理段 MAC 地址绑在装置外网口管理段地址上。

5.5 典型环境五



图表 110 典型环境五拓扑

该环境内网两台通讯服务器接两个交换机然后接路由器，两个交换机分别在 10.112.5.208/29 和 10.112.5.216/29 网段，网关分别为 10.112.5.214 和 10.112.5.222，加密装置采用双进双出接入，桥接模式配置策略路由。以下为详细配置。

5.5.1 系统配置

图表 111 典型环境五系统配置

需要配置两台，两个网段地址都可配置装置管理。

5.5.2 网络配置


网络配置

网络接口	接口类型	IP地址	子网掩码	接口描述/桥...	VLAN ID
eth0	PRIVATE	0.0.0.0	0.0.0.0	Just a desc	0
eth1	PUBLIC	0.0.0.0	0.0.0.0	Just a desc	0
BRIDGE	BRIDGE	10.112.5.221	255.255.255.248	br1	0
eth2	PRIVATE	0.0.0.0	0.0.0.0	Just a desc	0
eth3	PUBLIC	0.0.0.0	0.0.0.0	Just a desc	0
BRIDGE	BRIDGE	10.112.5.213	255.255.255.248	br2	0

图表 112 典型环境五网络配置

将 eth0、eth1、eth2、eth3 都配置虚拟地址，配两个网桥，其中 eth0 和 eth1 一个桥，eth2 和 eth3 一个桥，将两个网段的装置地址分别配在桥上。

5.5.3 路由配置


路由配置**注意策略路由（路由能够根据IP源地址来选择转发路径）属于高级选项，...

路由...	网...	VL...	目的网络	目的掩码	网关地址	策略路由ID	源地址网段	源地址掩码
A31	br1	0	10.112.5.216	255.255.255.248	0.0.0.0	1	10.112.5.216	255.255.25...
A32	br1	0	10.0.0.0	255.0.0.0	10.112.5.222	1	10.112.5.216	255.255.25...
A51	br2	0	10.112.5.208	255.255.255.248	0.0.0.0	2	10.112.5.208	255.255.25...
A52	br2	0	10.0.0.0	255.0.0.0	10.112.5.214	2	10.112.5.208	255.255.25...
default1	br1	0	10.0.0.0	255.0.0.0	10.112.5.222			
default2	br2	0	10.0.0.0	255.0.0.0	10.112.5.214			

图表 113 典型环境五路由配置

路由一用以确定内网业务段之间的通信，使装置知道网段 10.42.5.216/29 内的报文应当在桥内传播，而不需要转发到下一跳网关地址上去。例如，如果不增加该配置会导致内网业务机 ping 加密装置的报文也被转发到下一跳路由上去，导致内网业务机 ping 加密装置不通。

路由二用以确定内网业务网段 10.42.5.216/29 所发出的报文最终是应当转发到 10.42.5.222 这个下一跳地址上去的。

路由五用以确定加密装置本身的报文的默认路由，如果不加本条策略则装置不知道自身的相关报文应当发往何处，其中桥 br 的默认路由为 10.42.5.222。

路由三同一，路由四通二，路由六同五。其中策略路由 ID 用来标识策略路由的集合，相同策略路由 ID 的路由的源地址一般是一样的，符合这个源地址的报文将按照目的地址段的大小匹配这一组路由。

5.5.4 隧道配置

隧道名称	隧道ID	隧道模式	隧道本端...	隧道对端...	主装置证书	隧道...	备装置...	隧道...	隧道...
1	1	加密	10.112.5.221	10.10.6.1	ZJ-1-462.cer	0.0.0.0	选择证...	10000	50000...
2	2	加密	10.112.5.213	10.10.6.1	ZJ-2-474.cer	0.0.0.0	选择证...	10000	50000...

图表 114 典型环境五隧道配置

本地两个网段都和对端 10.10.6.1 建立隧道。

5.5.5 策略配置

策略ID	隧道ID	策略...	内网起始...	内网终止...	外网起始...	外网终止地址	协...	方向	内...	...	...	...
1	1	明文	0.0.0.0	255.255.25...	0.0.0.0	255.255.255.255	IC...	双...	0	6...	0	...
2	1	明文	10.112.5.217	10.112.5.218	10.112.0.1	10.112.255.255	全...	双...	0	6...	0	...
3	1	加密	10.112.5.217	10.112.5.218	10.10.6.1	10.10.6.255	全...	双...	0	6...	0	...
4	2	明文	10.112.5.209	10.112.5.210	10.112.0.1	10.112.255.255	全...	双...	0	6...	0	...
5	2	加密	10.112.5.209	10.112.5.210	10.10.6.1	10.10.6.255	全...	双...	0	6...	0	...

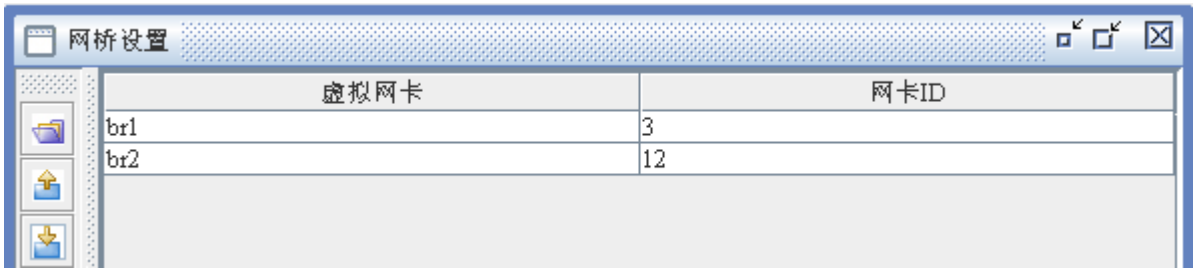
图表 115 典型环境五策略配置

第一条用来放过所有经过装置的 ICMP 报文(ping 包)。

第二、四条用来让内部业务和省内业务明通通讯。

第三、五条用来让内部业务和网调业务加密通讯。

5.5.6 桥接配置



虚拟网卡	网卡ID
br1	3
br2	12

图表 116 典型环境五桥接配置

配置两个网桥，将 eth0 口，eth1 口假设 br1 网桥，eth2 口，eth3 口架设 br2 网桥。

六、系统指标

装置外形:

1）尺寸(长×宽×高): 185mm*100mm*45mm

2）重量：<500g

网络接口: 2 个 RJ45 网口

外设接口： 1 个终端接口(RS232)+1 个 usb 接口

电源接口： 单电源接口

电源指标:

1) 电压：DC 24V
2) 允许偏差：－20％～＋15％
3) 纹波系数：不大于 5％
4) 平均无故障时间(MTBF)>60000 小时(100%负荷)

工作环境:

1) 工作温度：-10℃ - 55℃
2) 工作湿度：5～95%，非冷凝
3) 大气压力：70kPa～106kPa。

性能指标:

1) 最大并发加密隧道数：128 条
2) 10M LAN 环境下，加密隧道建立延迟＜1s
3) 明文数据包吞吐量：100Mbps （50 条安全策略，1024 报文长度）
4) 密文数据包吞吐量：6.5Mbps （10 条安全策略，1024 报文长度）
5) 数据包转发延迟：＜2.5ms （50％密文数据包吞吐量）
6) 满负荷数据包丢弃率：0