用户手册

中国电信商务领航定制网关

NAV10V2-WF

目 录

1

简介

NAV10V2-WF 网关是思科系统公司为中国电信定制的一款小型企业客户专用的功能强大、性能出色的无线宽带路由器产品，为您提供一个灵活、完备的企业网络解决方案。它配置简单，操作方便，使用灵活，基于标准且具有灵活的远程管理特性。

为了更有效地了解和使用本产品，请仔细阅读本用户手册。本章节主要介绍 NAV10V2-WF 网关的产品型号、功能特性和典型应用。

产品型号

本系列产品提供以下 2 种型号 （请检查设备后面板上的 SKU 名称以识别产品的具体型号）。本文中如无特别说明，统称为 NAV10V2-WF 网关：

序号	**SKU** 名称	功能配置
1	NAV10V2-WF	具备基本功能和无线接入功能的网关
2	NAV10V2-WF-ADVSEC	具备基本功能、高级安全功能和无线接入功能的网关

主要功能

NAV10V2-WF 网关为用户提供了灵活的功能选项，用户可以根据自己的需求进行功能选择，包括：

- 宽带上网功能，包括 PPPOE、 PPTP、 L2TP、静态 IP 和自动配置 DHCP
- 基本的路由功能，包括静态路由、 RIP 和 OSPF 协议
- 局域网交换功能，包括 VLAN 功能
- 支持 EVDO 无线上网
- 防火墙功能，包括 URL 过滤和关键字过滤
- 最多至 2 个广域网端口，可按需均衡负载流量
- 最多至 9 个局域网端口

- 具备无线接入功能 (802.11b/g/n）
- 具备高级安全功能(仅适用于NAV10V2-WF-ADVSEC型号)，包括IPSEC-VPN和Full Tunnel SSL VPN
- 病毒过滤，黑客攻击防御和控制网聊网游等应用 (仅适用于 NAV10V2-WF-ADVSEC 型号)

典型应用

NAV10V2-WF 网关适用于以下场合：

- **宽带互联网接入**：可以利用 TR069 或者 SNMP 对 NAV10V2-WF 网关进行远程配置和管理，并支持 HTTPS ；
- **安全互联网网关**：NAV10V2-WF 网关能够应对来自互联网上的恶意攻击，如 FW、 DMZ 等功能。 NAV10V2-WF-ADVSEC 型号还支持高级安全功能，如 IPS 和反病毒等功能；
- **远程 VPN 网关 / 接入**：支持远程站点 VPN 接入和远程用户 VPN 接入；
- **无线热点接入**：可用于办公室的 WLAN 接入，或者公共场所的 WiFi 热点接入。

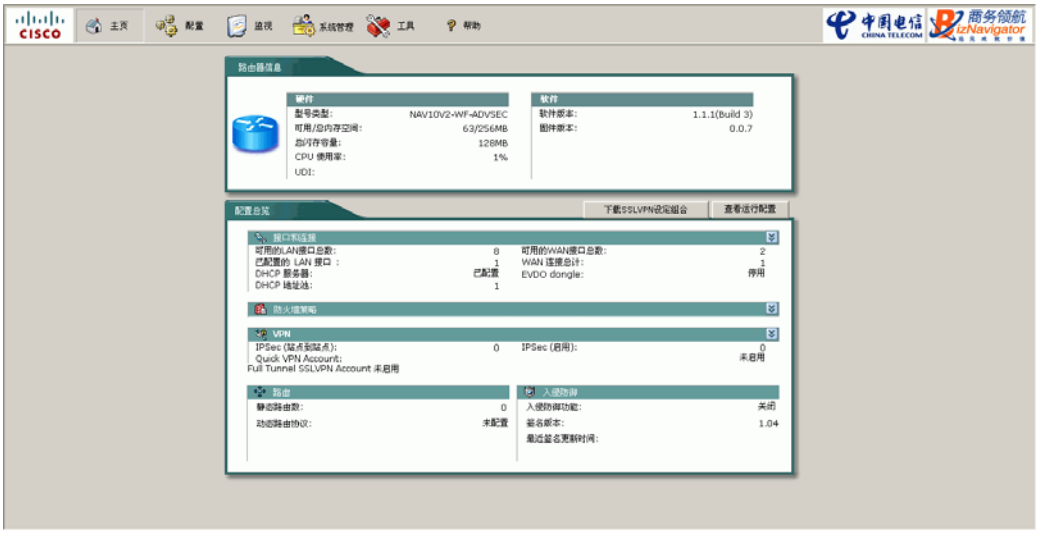
2

主页

登录 **web** 配置界面

用户可以使用 web 配置界面来远程或本地管理 NAV10V2-WF 网关。

1. 打开浏览器，输入 NAV10V2-WF 网关默认的 IP 地址 192.168.1.1 （如用户修改了默认 IP 地址，请输入用户修改后的 IP 地址）。
2. 打开登录界面，输入用户名和密码。默认的管理员帐号为 telecomadmin，密码为 nE7jA%5m。
3. 点击 “登录”按钮，打开主页。主页显示 NAV10V2-WF 网关的基本信息。



4. 显示 NAV10V2-WF 网关硬件和软件方面的基本信息，包含以下字段：
   - 型号类型：显示路由器型号；
   - 可用 / 总内存空间： 显示可用 RAM 和总 RAM 的兆字节 （MB）数；
   - 总闪存容量： 闪存的兆字节 （MB）数；
   - CPU 使用率： 按百分比 （%）显示当前 CPU 的利用率；

- UDI： 显示设备的 “通用设备标识”号；
- 软件版本：NAV10V2-WF 网关当前所运行的软件版本；
- 固件版本：NAV10V2-WF 网关当前所运行的固件版本。

5. 显示 NAV10V2-WF 网关所有关键特性的配置。
   - 接口和连接：
     - 可用的 LAN 接口总数：显示可用的 LAN 接口数。
     - 已配置的 LAN 接口：显示已经配置的 LAN 接口数。
     - 可用的 WAN 接口总数：显示可用的 WAN 接口数。
     - WAN 连接总计：显示已连接的 WAN 接口数。
     - DHCP 服务器：显示 DHCP 服务器的配置状态。
     - DHCP地址池：显示配置在NAV10V2-WF网关上的DHCP服务器地址池的个数。
     - EVDO Dongle：显示 EVDO dongle 的连接状态。将带有 3G 无线上网卡的 USB 适配器插入 USB 接口， NAV10V2-WF 网关检测到 EVDO 上网卡时，EVDO Dongle 的连接状态显示为 UP。
   - 防火墙策略：显示当前的 “防火墙”策略设置。
   - VPN：
     - IPsec （站点到站点）： 显示站点到站点 VPN 的个数。
     - IPsec （启用） ： 显示 IPsec 是否启用。
     - Quick VPN Account： 显示 Quick VPN Account 的状态 （启用或停用）。
     - Full Tunnel SSL VPN Account：显示 Full Tunnel SSL VPN Account 的状态（启用 / 未启用）。

注释 如果 IPSec VPN 和 SSL VPN 未启用，此处显示将显示 “VPN 未启用”和 “Full Tunnel SSLVPN Account 未启用”字样。

   - 路由：
     - 静态路由数：显示已配置的静态路由数。
     - 动态路由协议：显示已配置的动态路由协议。

- 入侵防御 （仅高级安全型号 NAV10V2-WF-ADVSEC 支持）：
  - 入侵防御功能： 显示 IPS 功能是否开启。
  - 签名版本： 显示 IPS 签名的版本。
  - 最近签名更新时间： 显示最近的签名更新时间。

6. 点击 “查看运行配置”按钮，可查看 NAV10V2-WF 网关当前运行的所有配置信息。

下载 SSL VPN 设定组合

在主页上提供了 Full Tunnel SSL VPN 设定组合的下载链接，通过该链接，用户可下载 OpenVPN 客户端以及相关的证书、配置文件等。

请遵照以下步骤下载 Full Tunnel SSL VPN 设定组合：

1. 选择 “配置” -〉“VPN” -〉“VPN” -〉“Full Tunnel SSL VPN”，添加并启用 Full Tunnel SSL VPN Account。
2. 选择 “主页”，在主页上提供了 Full Tunnel SSL VPN 的设定组合下载链接。点击 “下载 SSL VPN 设定组合”按钮，转到下载界面。
   - 勾选 “Download OpenVPN GUI for Windows ” 选项，下载并安装 OpenVPN 客户端到您的本地 windows 主机。
   - Download Client config for：下载 GigabitEthernet0 或 GigabitEthernet1 的客户端配置文件到本地。如果 GigabitEthernet0 或 GigabitEthernet1 接口断开，不能下载客户端配置。
3. 点击 “download”，弹出下载界面，选择下载文件保存位置。
4. 找到下载文件并解压缩，包括 CA 证书 （ca.crt）、 OpenVPN 安装程序 （OpenVPN-install.exe）、客户端配置文件 （ovpn_config_wanx.ovpn）和连接脚本文件 (ovpn_wanx.bat)。
5. 运行 openVPN-installer.exe，依照安装向导将 OpenVPN 客户端安装到本地 window 主机上。

3

配置

“配置”任务栏可设置 NAV10V2-WF 网关的各种接口参数以及相关的关键特性。左侧的任务列表显示了 “配置”任务栏所有可执行的任务。

快速设置

“快速设置”任务栏为快速配置 NAV10V2-WF 网关提供了一种简单方便的方法。快速设置要求用户通过 WAN0 接口提供 Internet 连接服务。

请按照如下步骤，快速配置 NAV10V2-WF 网关：

1. 选择 “配置” -> “快速设置”，打开 “快速设置”界面。
2. 设置 WAN0 接口参数：
   - Internet 连接类型：选择 WAN0 端口的 Internet 连接类型。NAV10V2-WF 网关支持 5 种类型的 Internet 连接 -- 自动配置 DHCP、静态 IP、 PPPoE、 PPTP 和 L2TP。以下为各个 Internet 连接类型的详细配置说明：

表 1 Internet 连接类型设置

Internet 连接类型	配置说明
自动配置 -DHCP	默认情况下， NAV10V2-WF 网关的 Internet 连接类型被设置为“自动配置 - DHCP”。 NAV10V2-WF 网关将从 ISP 的 DHCP 服务器上获取其 IP 地址。大多数线缆调制解调器 （cable modem） ISP 采用本选项。

表 1 Internet 连接类型设置

Internet 连接类型	配置说明
静态 IP	如果您使用固定 IP 地址连接到 Internet，请选择 “静态 IP”。 • IP 地址：指 NAV10V2-WF 网关 WAN0 端口 （可以从 Internet 到达该端口）的 IP 地址。您的 ISP 将向您提供此处所需的 IP 地址。 • 子网掩码：指 NAV10V2-WF 网关在 WAN0 端口上的子网掩码。 ISP 向您提供 IP 地址的同时会提供该信息。 • 默认网关：您的 ISP 将向您提供连接到 Internet 的默认网关的 IP 地址。 • 主 DNS （必填）和备用 DNS （选填）：您的 ISP 将至少向您提供一个 DNS （域名系统）服务器的 IP 地址以便将主机名解析到 IP 地址映像。
PPPoE	大多数 DSL 类型的 ISP 使用 PPPoE （点到点以太网协议）来建立 Internet 连接。如果您通过 DSL 线连接到 Internet，您的 ISP 将向您提供使用 PPPoE 的信息。 • 用户名和密码：输入 ISP 为您提供的用户名和密码以便进行 PPPoE 验证。 • 按需连接：最大空闲时间。您可以将 NAV10V2-WF 网关配置为在指定的时间段 （“最大空闲时间”）不活动后终止 PPPoE 会话。当 Internet 连接由于不活动而终止时，一旦再次访问 Internet，“按需连接”可使 NAV10V2-WF 网关自动重新建立连接。要使用此选项，请点击该单选按钮并在 “最大空闲时间”栏内输入您希望 Internet 连接终止之前所经过的分钟数。在按时间计费的情况下，使用此选项可使 DSL 连接时间降至最低。默认情况下停用此选项。 • 保持活动：该选项可使 NAV10V2-WF 网关保持 PPPoE 会话始终处于活动状态。如果连接被 ISP 断开， NAV10V2-WF 网关会自动重新建立连接。默认情况下启用此选项。由于使用本选项将始终保持连接，因此可使 Internet 连接的响应时间降至最低。

表 1 Internet 连接类型设置

Internet 连接类型	配置说明
PPTP	“点到点隧道协议”（PPTP）是一种连接服务。 • IP 地址：指 WAN0 端口的 IP 地址，可以从 Internet 到达该端口。您的 ISP 将向您提供此处所需的 IP 地址。 • 子网掩码：指 WAN0 接口的子网掩码。您的 ISP 将向您提供子网掩码和 IP 地址。 • 默认网关：您的 ISP 将向您提供默认网关的 IP 地址。 • PPTP 服务器 IP：输入 PPTP 服务器的 IP 地址。 • 用户名和密码：输入您的 ISP 提供的用户名和密码。 • 按需连接：最大空闲时间。您可以将 NAV10V2-WF 网关配置为指定的时间段 （最大空闲时间）不活动后终止 Internet 连接。当 Internet 连接由于不活动而终止时，一旦再次访问 Internet，“按需连接”可使 NAV10V2-WF 网关自动重新建立连接。要使用此选项，请点击该单选按钮并在 “最大空闲时间”栏内输入您希望 Internet 连接终止之前所经过的分钟数。在按时间计费的情况下，使用此选项可使 DSL 连接时间降至最低。默认情况下停用此选项。 • 保持活动：使 NAV10V2-WF 网关保持 PPTP 会话始终处于活动状态。如果连接被 ISP 断开， NAV10V2-WF 网关会自动重新建立连接。默认情况下启用此选项。由于使用本选项将始终保持连接，因此可使 Internet 连接的响应时间降至最低。
L2TP	“第二层隧道协议”（L2TP）是一种通过隧道 “点到点协议”（PPP）连接 Internet 的服务。请向 ISP 索取所需的设置信息。 • IP 地址：指从 WAN0 或 Internet 上所看到的 NAV10V2-WF 网关 IP 地址。您的 ISP 将向您提供此处所需的 IP 地址。 • 子网掩码：指 NAV10V2-WF 网关 WAN0 接口的子网掩码。您的 ISP 将向您提供子网掩码和 IP 地址。 • 默认网关：您的 ISP 将向您提供默认网关的 IP 地址。 • L2TP 服务器 IP：输入 L2TP 服务器的 IP 地址。 • 用户名和密码：输入您的 ISP 提供的用户名和密码。

- MTU：最大传输单位。此参数规定 WAN0 接口允许的第三层数据包的最大长度。如果希望人工输入该值，请选择手动。要使 NAV10V2-WF 网关自动协商最佳的 MTU 值，则请保持默认设置 “自动”。
- MTU 容量：如果选择手动模式，请输入 MTU 大小。如果选择了自动模式，NAV10V2-WF 网关将自动选择 MTU。

3. LAN 设置：定义 NAV10V2-WF 网关默认的 LAN 接口的 IP 地址。
   - LAN IP 地址：配置 NAV10V2-WF 网关 LAN 接口默认的 IP 地址 （默认 192.168.1.1）。
   - 子网掩码：默认为 255.255.255.0。
4. DHCP 设置：定义 NAV10V2-WF 网关 LAN 接口的 DHCP 设置，包括是否启用 DHCP 服务器、 DHCP 地址池的 IP 范围和租用时间等。
   - DHCP 服务器：选择启用或停用 DHCP 服务器。
   - DHCP 地址池网段：根据用户设置的 LAN IP 地址，DHCP 地址池网段将该 IP 地址所在的网段相对应。
   - 子网掩码：默认为 255.255.255.0。
   - DHCP 地址池起始 IP 和终止 IP：定义该地址池中的第一个和最后一个 IP 地址。
   - 租用时间：定义所分配 IP 地址保持有效的时间。租用到期后 DHCP 客户机将发送更新请求。
5. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

接口和连接

“接口和连接”任务栏允许用户设置 NAV10V2-WF 网关的 WAN 接口、 LAN 接口、无线网络接口的参数，查看各个接口和 Internet 连接的状态和详细信息。

WAN

NAV10V2-WF 网关可通过 DHCP、静态 IP、 PPPOE、 PPTP 以及 L2TP 等方式通过 WAN 接口连接到 Internet。

WAN0 设置

1. 选择 “配置” -〉“接口和连接” -〉“WAN” -〉“WAN0 设置”，打开 WAN0 接口配置界面。

a. Internet 连接类型：选择 WAN0 端口的 Internet 连接类型。 NAV10V2-WF 网关支持 5 种类型的 Internet 连接方式 —— 自动配置 DHCP、静态 IP、PPPoE、PPTP 和 L2TP。

b. 设置 MTU：最大传输单位。如果希望人工输入该值，请选择手动。要使 NAV10V2-WF 网关自动协商最佳的 MTU 值，则请保持默认设置 “自动”。如果选择手动模式，请输入 MTU 大小。如果选择了自动模式， NAV10V2-WF 网关将自动选择 MTU。

2. 设置 WAN0 子接口。一个物理端口可以分成多个逻辑接口，每一个逻辑接口叫子接口。用户可以在 WAN0 接口上设置不超过 8 个子接口。

注意 VPN、Firewall、IPS、QoS 和 DMZ 功能无法套用在 WAN 子接口上，WAN 子接口功能和 OSPF 不能同时使用。

注意 当双 WAN 功能选项被设置为 “智能连接备份”或 “负载均衡”时，将无法使用子接口功能。如需同时启用双 WAN 和子接口功能，将将双 WAN 设置为 “路由表选路”。

- 启动 WAN 子接口：启用 / 停用 WAN 子接口功能。启用 WAN0 子接口功能，请确认 WAN0 接口的上行连接到一台 Trunk 交换机。
- 操作模式：子接口的操作模式有路由模式 （Routing）和桥接模式（Bridging）两种。

3. 桥接模式设置：
   - VID：指定该 WAN 子接口所对应的上行 Trunk 交换机的 VLAN ID。
   - Bridging VLAN ：指定该 WAN 子接口桥接指向的 VLAN 组。
4. 路由模式设置：
   - VID：指定该 WAN 子接口所对应的上行 Trunk 交换机的 VLAN ID。
   - NAT：在此路由子接口上是否启用 NAT 功能。
   - 服务类型：NAV10V2-WF 网关支持四种子接口的服务类型，分别是 Management、 Internet、 Management+Internet 和 Other。其中：
     - Management：表示此连接仅用来作为管理通道。
     - Internet：表示此连接仅用来作为上网通道。
     - Management+Internet：表示此连接可以同时用来作为管理和上网通道。
     - Other：其他连接。

注释 如果启用的服务类型为 Management 或 Managemetn+Internet，管理服务需要与服务运营商的设置相匹配。

   - Internet 类型：指定此路由接口的 Internet 连接方式，仅支持静态 IP、PPPoE 和自动配置 DHCP 三种连接方式。
     - 选择静态IP连接，需要分别定义IP地址、子网掩码和主DNS和备用DNS等参数，如上图所示。
     - 选择 PPPoE，需要分别定义拨号的账号和密码，以及按需连接或保持活动等选项。

- 或选择自动配置 -DHCP。

- MTU：设置接口允许通过的最大传输单元。如果选择手动模式，请输入 MTU 大小。
- MAC 地址：手动输入 12 位的 MAC 地址，或者点击“自动”按钮，将自动将用户 PC 的网卡 MAC 地址复制到子接口上。

5. 查看 WAN0 子接口的状态。子接口状态栏显示了 WAN0 接口上当前设置的子接口列表及详细信息，包括网络名称、运作模式等信息，点击 “编辑”按钮可修改子接口的参数，点击 “删除”按钮可删除选择的子接口。
6. 完成以上所有设置后，点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

WAN1 设置

1. 选择 “配置” -〉“接口和连接” -〉“WAN” -〉“WAN1 设置”，打开 WAN1 接口配置界面。

2. 选择 WAN1， GigaEthernet 1 可作为一个 WAN 接口。如果设为 WAN 接口，请参考 “**WAN0** 设置”设置其参数。

3. 选择 LAN， GigaEthernet 1 可作为一个扩展的 LAN 接口。如果设为 LAN 接口，请参考 “**LAN**”设置其参数。此时，子接口功能将被禁用。
4. 如果启用子接口功能，请参考 “**WAN0** 设置”设置子接口参数。
5. 完成以上所有设置后，点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

双 -WAN

NAV10V2-WF 网关支持双 WAN 功能，可通过 Internet 连接备份来确保恒定的 Internet 连接，或者在 WAN0 和 WAN1 之间建立负载均衡以使带宽效率最大化。

注意 只有在 GibabitEthernet1 端口被设为 WAN1 接口时，双 WAN 功能可用。如果您将 GibabitEthernet1 端口设为扩展的 LAN 接口，双 WAN 功能不可用。

注意 当 EVDO PPPoE 功能启用后，双 WAN 功能将不可用。此时如需配置双 WAN，请停用 EVDO PPPoE 功能。

请依照以下步骤，设置双 WAN 功能：

1. 选择“配置”-〉“接口和连接”-〉“WAN”-〉“双 WAN”，打开双 WAN 配置界面。

2. 选择双 WAN 功能模式：

   - 智能连接备份: 选择 Internet 连 接的主 WAN 端口，另一个则成为备份的 Internet 连接接口。主 WAN 端口的 Internet 连接断开时， 备份的 Internet 连接接口将处于活动状态。
   - 负载均衡：设置通过 WAN0 接口和 WAN1 接口进行 Internet 通信的百分比。此时， WAN0 和 WAN1 接口都处于活动状态， NAV10V2-WF 网关将按设定的百分比在两个接口之间分配 Internet 通信。通常较快的 Internet 连接服务应分配到负载较高的接口。
   - 路由表选路：您需要在“静态路由”页面添加一个缺省路由并指向一个 WAN 端口 (比如 WAN0)，另外再添加其它的多个静态路由到另外一个 WAN 端口 (比如 WAN1)。

注意 一旦选择 “路由表选路”，则 “网络服务检测”和 “协定绑定”功能将被停用。

3. 设置网络服务检测。“网络服务检测”有助于管理连接并在连接出现问题时给出报告。

   - 网络服务检测：选择启用或停用网络服务检测。

注释 如果启用网络服务检测功能，用户必须指定 WAN0 和 WAN1 端口用于网络检测的 IP 地址 （默认网关地址或远程主机地址）。

- 重试次数：如果连接失败， NAV10V2-WF 网关将按此处所指定的次数尝试重新连接。
- 重试超时：表示 NAV10V2-WF 网关超时前尝试与 ISP 建立连接的次数。
- WAN0 和 WAN1：“网络服务检测”既可通过 ping 默认网关也可通过 ping 特定 IP 地址 （“ISP 主机”、“远程主机”或 “DNS 查找主机”等）来测试 Internet 连通性。

4. 设置协定绑定。端口绑定允许用户指定内部 IP 以及服务通过指定的 WAN 端口。NAV10V2-WF 网关最多可设置 16 条端口绑定规则。
   - 启用 / 停用：启用或停用协定绑定功能。

     注释 如果选择 “智能连接备份”模式，协议绑定功能被禁用。

   - 服务：使用下拉框来选择一个服务，或点击 “服务管理”增加新的服务。
   - 服务管理：可添加或删除服务。
     - 服务名称：定义服务名称。
     - 协议：选择服务采用的协议类型， TCP 或则 UDP 协议。
     - 端口范围； 定义该服务采用的端口。
     - 添加到列表：设置好以上参数后，点击该按钮可将该服务添加到服务列表中。
     - 删除选择的服务：从服务列表中选择一个服务，然后点击此按钮，可删除该服务。
   - 源接口：选择服务的来源接口。
   - 源 IP 范围：指定允许通过指定 WAN 端口的内部 IP，如果使用者只需要服务绑定，源 IP 可以是空白。如果使用者需要 IP 绑定，可由下拉框中选取。
   - 目标 IP 范围：指定被允许通过 WAN 端口从内部源 IP 访问的目标 IP 范围。如果使用者只需要服务绑定，目标 IP 可以是空白。如果使用者需要 IP 绑定，可以选择单个 IP 或者某一网段内的 IP。

- 接口：选定 WAN0 或 WAN1。

5. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

MAC 复制

MAC 地址由 12 个数字组成，分配给网络上的设备做识别用途。有些运营商会要求客户注册一组 MAC 地址。将 NAV10V2-WF 网关的 MAC 地址设为之前已经注册过的网卡 MAC 地址，就不用再联系运营商去把新增的 NAV10V2-WF 网关 MAC 地址登记进入自己的注册 MAC 地址表里了。

请依照以下步骤设置 MAC 复制功能：

1. 选择 “配置” -〉“接口和连接” -〉“WAN” -〉“MAC 复制”，打开 MAC 复制配置界面。
2. 启用或停用 MAC 地址复制功能：
   - 启用 / 禁用：开启或关闭 MAC 复制功能。
   - WAN0/WAN1 MAC 地址：手动输入 12 位的 MAC 地址，或者点击 “复制用户 MAC 地址” 按钮，将用户 PC 的网卡 MAC 地址复制到 WAN0/WAN1 接口上。

注释 如果用户端经由 WAN 端连接或其设置于 NAT 装置后端时，无法使用 “复制用户 MAC 地址” 功能。

3. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

端口镜像

端口镜像功能可以通过指定一个或两个端口当成监控或分析的端口，接收来自被监控或分析的端口的报文。被监控或分析的端口称为被镜像端口，拿来做监控或分析的端口称为分析端口。

1. 选择 “配置” -〉“接口和连接” -〉“WAN” -〉“端口镜像”，打开端口镜像配置界面。
2. 启用或停用端口镜像功能。
3. 设置镜像端口和分析端口：
   - 端口镜像：启用或停用端口镜像功能。

- 镜像端口：指定被监控或分析的端口。
- 分析端口：指定用来做监控或分析的端口。

4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。
5. 注意事项：
   - 被镜像端口不可与分析端口在同一个桥接上。
   - DMZ 的端口只能被镜像而不能当成分析端口。
   - 允许最多两个被镜像端口以及最多两个分析端口。
   - 改变 VLAN 设定且所改变的端口原先已被设成分析端口或被镜像端口，则原本的镜像功能会消除而必须重新设定。
   - GE0 不支持端口镜像。

EVDO

NAV10V2-WF 网关支持 3G EVDO （Evolution-Data Optimized）无线上网功能，可满足移动高速数据业务的要求。 3G EVDO 支持高速数据传输，当 NAV10V2-WF 网关的 WAN 连接工作正常时， 3G EVDO 可作为备用的 WAN 连接，一旦监测到 NAV10V2-WF 网关的 WAN 连接断开或者上级路由服务断开时， 3G EVDO 自动 PPPoE 拨号上网，实现无线上网功能。

请遵循以下步骤设置 3G EVDO 上网功能：

1. 将插有 3G 无线上网卡的 USB 适配器插入 NAV10V2-WF 网关的 USB 接口。
2. 选择 “配置” -> “接口和连接” -> “WAN” -> “EVDO”，打开 3G EVDO 配置界面。
3. 查看 NAV10V2-WF 网关是否能检测得到 3G EVDO 上网设备。用户需要将运营商提供的 3G 无线上网卡正确插入 NAV10V2-WF 网关所支持的 USB 适配器内 （推荐使用 Huawei EC1260，Huawei EC169，ZTE AC2726，ZTE AC560 等型号的 3G 无线上网适配器），并将该 USB 适配器插入 NAV10V2-WF 网关的 USB 接口，NAV10V2-WF 网关检测到该 USB 适配器， EVDO dongle 的连接状态显示为 UP。如果 “EVDO Dongle 连接状态”为 “DOWN”，刷新界面。如果提示 “3G 卡设备未安装，将无法进行配置！”，请确认 3G 无线上网卡是否正确插入 USB 适配器，或将 USB 适配拔出后再次插入，刷新界面查看 EVDO Dongle 连接状态，确保 EVDO Dongle 连接状态为 UP。
4. 启用 PPPoE。一旦启用 PPPoE， NAV10V2-WF 网关将自动启用 Failover 功能。

注意 PPPoE 启用或停用操作不要切换太快，请至少间隔 10 秒钟。

注意 当 3G EVDO 启用且 PPPoE 的连接状态为 UP 时，NAV10V2-WF 网关的双 WAN 功能将不可用。

5. 输入用户名、密码和拨号号码。
   - 用户名：3G 无线上网卡的帐号。
   - 密码：3G 无线上网卡的帐号密码。
   - 拨号号码：3G 无线上网的 PPPoE 拨号号码。依照当地运营商提供的拨号号码。
6. 根据 NAV10V2-WF 网关的实际情况，配置 Failover 功能。 Failover 功能将监控 WAN 接口的状态，当 WAN 接口无法上网时立即启用 3G EVDO 自动拨号上网，当 WAN 接口恢复上网状态时，自动将 3G EVDO 断开。用户需手动选择监控的主 WAN 接口，并将主 WAN 接口的默认网关地址设为 Failover 功能的侦测 IP 地址。当侦测 IP 预设为 0.0.0.0 时， NAV10V2-WF 网关会自动选择主 WAN 接口的网关地址作为侦测 IP 地址。
   - 主 WAN：选择 NAV10V2-WF 网关的主 WAN 接口作为 Failover 检测接口。
   - 侦测 IP：将 NAV10V2-WF 网关的主 WAN 接口的默认网关地址设为 Failover 功能的侦测 IP。
7. 点击 “保存设置”按钮，保存设置。
8. 检查 PPPoE 连接状态。连接成功， PPPoE 连接状态为 up，反之为 down。当 PPPoE 的连接状态为 up 时，表示 3G EVDO 成功拨号上网。此时 NAV10V2-WF 网关通过 3G EVDO 提供 Internet 连接服务。

注释 如果 NAV10V2-WF 网关没有接入任何 WAN 连接， NAV10V2-WF 网关可直接通过 3G EVDO 实现无线上网。

LAN

VLAN 设置

NAV10V2-WF 网关最多支持 32 个 VLAN 组，其中 native 为 NAV10V2-WF 网关的默认 VLAN 组。

1. 选择“配置”->“接口和连接”->“LAN”->“VLAN 设置”，打开 VLAN 设置界面。

2. 填写 VLAN 的基本信息：
   - VLAN 名称：定义 VLAN 组的名称。
   - VLAN ID：定义 VLAN 组的 ID 号。
   - VLAN IP 地址：定义 VLAN 组的 IP 地址。
   - 子网掩码：定义 VLAN 组的子网掩码。
   - 启用生成树协议（Enable Spanning Tree Protocol）：启用或停用 NAV10V2-WF 网关生成树协议。

3. 启用 DMZ （可选）：选中复选框以启用 DMZ 功能。 DMZ 功能将使用 LAN7 接口， LAN7 将被所加入的 VLAN 组删除。启用 DMZ 功能，将关闭该 VLAN 组的 DHCP 服务，且禁用生成树协议。

注意 WAN0 或 WAN1 的 Internet 连接类型必须设置为静态 IP 地址才能使用 DMZ 功能。

4. DHCP 设置：为 VLAN 组设置 DHCP 服务器的参数。
   - 地址池名称：定义 DHCP 地址池的名称。
   - DHCP 服务器：启用或停用在该 VLAN 组上的 DHCP 服务器，或选择 DHCP 中继，并填写中继服务器的 IP 地址。
   - IP 地址：VLAN 组的 IP 地址。
   - DHCP 地址池网络：显示该 VLAN 组上的 DHCP 地址池的网络地址。
   - 子网掩码：DHCP 地址池的子网掩码。
   - 起始 IP 和终止 IP：定义 VLAN 组的 DHCP 地址池分配的 IP 范围。
   - 租用时间：定义用户租用 DHCP 地址池内 IP 地址的时间。
   - DHS 服务器 1 和 2：可选项，分别指定 VLAN 组的 DNS 服务器地址。
   - WINS 服务器 1 和 2：可选项，分别指定 VLAN 组的 WINS 服务器地址。
   - 域名：可选项，指定 VLAN 组的域名地址。
   - 默认路由器：可选项，指定 VLAN 组默认的路由器地址。
5. 设置好以上参数后，点击 “新增” 按钮，将新增的 VLAN 组添加到 VLAN 组状态列表。
6. 查看 VLAN 状态。 VLAN 组状态列表显示 NAV10V2-WF 网关默认的本地 VLAN 组和新建的 VLAN 组的状态信息：
7. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

Port 设置

在此界面，用户可以设置 LAN 接口的工作模式、指定其所属的 VLAN 组等。如果某 VLAN 组启用了 DMZ 功能， LAN7 将从其他 VLAN 组自动删除。

1. 选择 “配置” -> “接口和连接” -> “LAN” -> “Port 设置”，打开端口设置界面。

2. 选择要设置的目标端口。从 Port 下拉框中选择要设置的端口。
3. 选择端口工作的工作模式，包括接入模式 （Access）和干线模式 （Trunk）两种工作模式。
4. 为端口选择 VLAN 组：
   - 可使用的 VLAN：可用的 VLAN 组。选择一个 VLAN 组，点击 “增加 >>” 按钮，可将选择的 VLAN 组添加到 “已被选择的 VLAN” 列表。
   - 已被选择的 VLAN：已选择的 VLAN 组。选择一个 VLAN 组，点击 “移除 >>” 按钮，可将 VLAN 组从 “已被选择的 VLAN” 列表中移除。
5. 修改好后点击 “更新” 按钮，保存端口设置修改。
6. 完成以上设置后，点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

基于端口的访问控制

此选项可用来设置目标端口的访问控制功能。在页面的下方显示所有端口当前的访问控制策略。点击 “编辑” 按钮，可修改指定端口的访问控制设定。

1. 选择“配置” -> “接口和连接” -> “LAN” -> “基于端口的访问控制”，打开端口访问控制设置界面。

2. 从下拉框内选择目标端口。
3. 启用或停用基于端口的访问控制功能。
4. 设置 RADIUS 属性。从 Radius 属性下拉框中选择一个 Radius 服务器组，导入选定的 Radius 服务器组定义。
   - RADIUS 服务器组：显示导入的 RADIUS 服务器组的定义。
5. 点击 “更新”按钮，可将设置修改更新到对应的端口。
6. 完成以上设置后，点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

DHCP 绑定

DHCP 绑定为特定主机保留单独的 “IP 地址”。一旦建立 DHCP 绑定 （通过将主机的硬件地址映像到某个 IP 地址）， DHCP 地址池便将同一 IP 地址租借给具有指定硬件地址的主机。 NAV10V2-WF 网关最多支持 32 个 DHCP 绑定。

1. 选择 “配置” -> “接口和连接” -> “LAN” -> “DHCP 绑定”，打开 DHCP 绑定设置界面。
2. 分别设置以下参数：
   - 名称：DHCP 绑定的名称。

- 主机 IP 地址：DHCP 绑定的主机 IP 地址。
- MAC 地址：DHCP 绑定的主机 MAC 地址。

3. 点击 “新增” 按钮，添加到状态栏内。
4. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

以太网访问控制

1. 选择 “配置” -> “接口和连接” -> “LAN” -> “以太网访问控制”，打开以太网访问控制设置界面。
2. 选择访问控制的策略：
   - 停用有线访问控制：选择以停用访问控制。
   - 阻止下列 MAC 地址连接到有线网络：选择此选项以启用 “以太网访问控制”。此选项将阻止您输入的 MAC 地址访问以太网。
   - 允许下列 MAC 地址连接到有线网络：选择此选项以启用 “以太网访问控制”，此选项只允许您输入的 MAC 地址访问以太网。
3. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

VLAN 隔离

1. 选择 “配置” -> “接口和连接” -> “LAN” -> “VLAN 隔离”，打开 VLAN 隔离设置界面。
2. 启用或停用 VLAN 隔离功能。
3. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

无线设置

基本无线设置

在此界面上可修改无线网络设置。 NAV10V2-WF 网关最多支持 3 个无线网络。

1. 选择 “配置” -> “接口和连接” -> “无线设置” -> “基本无线设置”，打开基本无线设置界面。
2. 选择无线网络模式，默认设置为 **B/G/N 混合**。

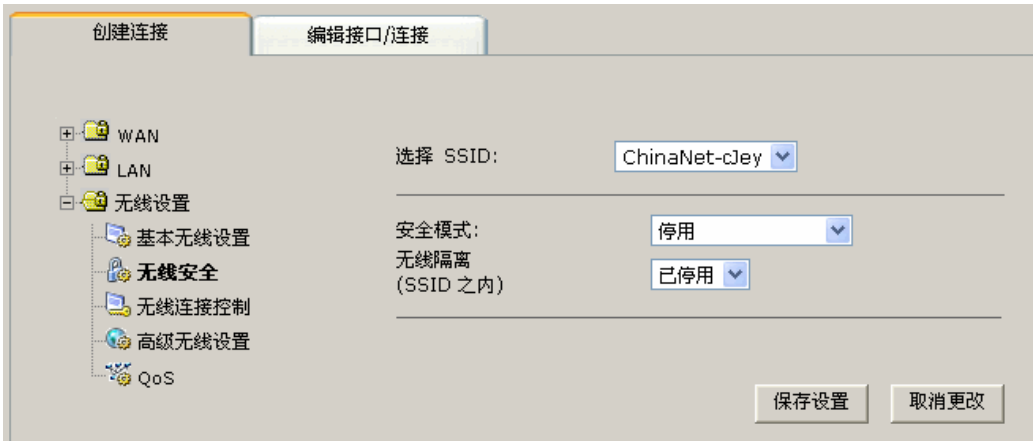
- **B-Only**：所有无线客户机设备能够以 Wireless-B 数据传输率 （最大速度 11Mbps）连接到 “无线接入点”。
- **G-Only**：只能以 Wireless-G 数据传输率（最大速度 54Mbps）连接 Wireless-G 无线客户机设备。此模式下无法连接 Wireless-B 客户机。
- **N-Only**：只能以 Wireless-N 数据传输率连接 Wireless-N 无线客户机设备。
- **B/G 混合**: 可以同时以其各自的数据传输率连接 Wireless-B 和 Wireless-G 客户机设备。
- **G/N 混合**: 可以同时以其各自的数据传输率连接 Wireless-N 和 Wireless-G 客户机设备。
- **B/G/N 混合**：可以同时以其各自的数据传输率连接 Wireless-B、Wireless-N 和 Wireless-G 客户机设备。
- **停用** ：完全停用无线连通性。系统维护期间可能用到这种模式。

3. 选择无线信道：为 “无线接入点”与客户机设备之间的通信选择合适的信道。默认设置为自动。这样当系统通电时，“无线接入点”将选择具有最少无线接口数量的信道。点击 “保存设置”后自动信道选择将启动，将持续数秒来重新启动并扫描所有的信道以便找出最佳信道。
4. 您可以在 SSID 表中为每一个 SSID 设置 SSID 名称及广播特性。
   - SSID 名称：SSID 是无线网络中所有设备共享的唯一名称。该名称区分大小写，长度不能超过 32 个字母数字字符，可以是任何键盘字符。请确保无线网络中所有设备的此项设置相同。只有定义了 SSID 名称才可启用该 SSID。
   - SSID 广播：此选项允许在您的网络上广播 SSID。配置网络时可能需要启用此项功能，但要确保在结束配置时停用此选项。如果启用此选项，其他人可以用地址查看软件或 Windows XP 轻易获取 SSID 信息，并可不经授权对网络进行访问。点击 “已启用”可以向网络范围内的所有无线设备广播 SSID ； 点击 “已停用”可提高网络安全性，并防止联网的电脑看到 SSID。为了便于用户在使用前对网络进行配置，默认设置为已启用。
   - SSID 启用 / 停用：启用或停用 SSID。
5. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

无线安全

在此界面上为每个 SSID 配置 “无线接入点”的无线安全设置。每个无线网络都可以有自己的安全设置。

1. 选择 “配置” -> “接口和连接” -> “无线设置” -> “无线安全”，打开无线安全设置界面。



2. 选择 SSID：选择您想要配置安全设置的 SSID。
3. 选择您想要采用的无线安全模式。NAV10V2-WF 网关支持的无线安全模式包括 WPA 个人级、 WPA2 个人级、 WPA2 个人混合级、 WPA 企业级、 WPA2 企业级、 WPA2 企业混合级、RADIUS 和 WEP。要完全停用无线安全性，则请选择停用。默认设置为停用 。 以下说明了无线安全模式的详细配置选项。
   - **停用**：该模式无配置选项。
   - **WEP**：本安全模式在 IEEE 802.11 标准中有定义。由于其脆弱的安全保护，因此目前不推荐采用此模式。强烈要求用户转换到 WPA 或 WPA2。
     - 验证类型：为 802.11 验证类型选择开放系统或共享密钥。默认设置为开放系统。
     - 默认传输密钥：选择数据加密时所采用的密钥。
     - WEP 加密：选择 WEP 加密等级，64 位（10 位十六进制数）或 128 位（26 位十六进制数）。
     - 密语：如果希望用 “密语” 生成 WEP 密钥，请在相应栏中输入 “密语”，然后点击 “Generate” 按钮。这些自动生成的密钥不如手动输入的 WEP 密钥强大。
     - 密钥 1-4 如果希望手动输入 WEP 密钥，请在相应的栏中输入。每个 WEP 密钥可由字母 “A” 到 “F” 和数字 “0” 到 “9” 组成。对于 64 位加密，其长度应为 10 个字符；对于 128 位加密，长度应为 26 个字符。
   - **WPA 个人级 （又称 WPA-PSK）**

- WPA 算法：WPA 提供 TKIP 和 AES 两种加密方法进行数据加密。请选择希望使用的算法类型， TKIP 或 AES。默认设置为 TKIP。
- WPA 共享密钥：输入 8 ~ 63 个字符的 WPA 共享密钥。
- 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 3600 秒。

- **WPA2 个人级**
  - WPA 算法：WPA2 始终采用 AES 进行数据加密。
  - WPA 共享密钥：输入 8-63 个字符的 WPA 共享密钥。
  - 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 3600 秒。
- **WPA2 个人混合级**：此安全模式支持从 “WPA 个人级”到 “WPA2 个人级”的转换。您可以同时拥有 “WPA 个人级”和 “WPA2 个人级”的客户机设备。“无线接入点”会自动选择每台客户机设备所用的加密算法。
  - WPA 算法：“混合模式”自动选择 TKIP 或 AES 进行数据加密。
  - WPA 共享密钥：输入 8 ~ 63 个字符的 WPA 共享密钥。
  - 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 3600 秒。
- **WPA 企业级**：此选项可使 WPA 与进行客户机验证的 RADIUS 服务器配合使用（只有当 RADIUS 服务器连接到 “无线接入点”时才能使用此选项）。
  - RADIUS 服务器 IP 地址：输入 RADIUS 服务器的 IP 地址。
  - RADIUS 服务器端口：输入 RADIUS 服务器所用的端口号。默认端口号为 1812。
  - 共享密钥：输入无线接入点和 RADIUS 服务器所用的 “共享密钥”。
  - WPA 算法：WPA 提供 TKIP 和 AES 两种加密方法进行数据加密。请选择希望使用的算法类型， TKIP 或 AES。默认设置为 TKIP。
  - 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 3600 秒。
- **WPA2 企业级**：此选项可使 WPA2 与进行客户机验证的 RADIUS 服务器配合使用（只有当 RADIUS 服务器连接到 “无线接入点”时才能使用此选项）。
  - RADIUS 服务器 IP 地址：输入 RADIUS 服务器的 IP 地址。

- RADIUS 服务器端口：输入 RADIUS 服务器所用的端口号。默认端口号为 1812。
- 共享密钥：输入无线接入点和 RADIUS 服务器所用的 “共享密钥”。
- WPA 算法：WPA2 始终采用 AES 进行数据加密。
- 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 3600 秒。

• **WPA2 企业混合级**：此安全模式支持从 “WPA 企业级”到 “WPA2 企业级”的转换。您可以同时拥有 “WPA 企业级”和 “WPA2 企业级”的客户机设备。“无线接入点”会自动选择每台客户机设备所用的加密算法。

- RADIUS 服务器 IP 地址：输入 RADIUS 服务器的 IP 地址。
- RADIUS 服务器端口：输入 RADIUS 服务器所用的端口号。默认端口号为 1812。
- 共享密钥：输入无线接入点和 RADIUS 服务器所用的 “共享密钥”。
- WPA 算法：“混合模式”自动选择 TKIP 或 AES 进行数据加密。
- 密钥更新超时：输入 “密钥更新超时”的时间段，该时间段指示 “无线接入点”多长时间更改一次加密密钥。默认设置为 3600 秒。

• **RADIUS**：本安全模式又称为 “IEEE 802.1x 动态 WEP 加密”。采用 RAIDUS 服务器进行客户机验证，并使用 WEP 进行数据加密。 WEP 密钥由 RADIUS 服务器自动生成。为了兼容 Microsoft Windows 工具，现已不再支持手动 WEP 密钥 （由于其脆弱的验证能力）。

- RADIUS 服务器 IP 地址：输入 RADIUS 服务器的 IP 地址。
- RADIUS 服务器端口：输入 RADIUS 服务器所用的端口号。默认端口号为 1812。
- 共享密钥：输入无线接入点和 RADIUS 服务器所用的 “共享密钥”。

4. 无线隔离 （SSID 之内）：停用无线隔离时，关联到同一 “网络名称”（SSID）的无线 PC 可以彼此看到并互相传递文件。启用此特性时，无线 PC 将无法互相看到。这一功能在设置无线热点位置时非常有用。默认设置为已停用。
5. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

无线连接控制

此界面允许您配置 “连接控制列表”，以便允许或阻止特定的无线客户机设备连接到 “无线接入点”（或与之发生关联）。每个 SSID 拥有其独有的连接控制列表。

1. 选择 “配置” -> “接口和连接” -> “无线设置” -> “无线连接控制”，打开无线连接控制设置界面。
2. 选择 SSID：选择您想要配置其连接控制列表的 SSID。
3. 连接控制：可以 “停用连接控制”，也可以阻止特定设备连接到 “无线接入点”，或只允许特定客户机设备连接到 “无线接入点”。通过 MAC 地址来指定客户机设备。默认设置为停用连接控制。
    - 无线客户机列表：“无线接入点”提供了一种从客户机列表中选择特定客户机设备的便利方法，以替代手动输入每一客户机的 MAC 地址。点击 “无线客户机列表”按钮，将出现 MAC 地址选择窗口。所选的 MAC 地址将被输入 “连接控制列表”。
    - 连接控制列表 MAC01-16：输入您想要控制的无线客户机设备的 MAC 地址。
4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

高级无线设置

您可以在此界面上配置 “无线接入点”的高级设置。

1. 选择 “配置” -> “接口和连接” -> “无线设置” -> “高级无线设置”，打开高级无线设置界面。
2. 设置以下参数：
    - CTS 保护模式：“CTS （Clear-To-Send，清除发送）保护模式”功能增强了无线接入点捕获所有 Wireless-G 传输的能力，但会严重降低性能。请保持默认设置自动，这样当 Wireless-G 产品在 802.11b 通信繁忙的环境中无法传输到 “无线接入点”时，无线接入点便能根据需要使用这一特性。选择已停用可以永久停用该特性。
    - 基本数据速率：此项设置是根据 IEEE 802.11 中所定义的规格通知其它无线设备的一系列速率，这样它们就知道 “无线接入点”能够支持哪些速率。
    - 无线隔离 （SSID 之间）：无线隔离可防止网络窃听。启用无线隔离后，该 “无线接入点”所收到的无线数据帧不会被转发到其他无线网络 （SSID）。例如，如果您有一个无线热点，您可能希望使该无线网 （SSID）与其他无线网 （其他 SSID）隔离开。该选项为适用于所有 SSID 的通用选项。默认设置为启用。
    - 功率输出：可以调节 “无线接入点”的输出功率，以使您的无线网络具有合适的覆盖范围。请为您的环境选择所需的级别，如果不能确定选择哪种设置，则保持默认设置 100%。
    - 信标间隔：该值指示信标的频率间隔。信标是由 “无线接入点”广播的保持网络同步的数据包。信标包含无线网络服务区域、“无线接入点”地址、“广播”

目标地址、时间标记、“传送流量指示图”（DTIM）以及 “流量指示消息”（TIM）。

- DTIM 间隔：该值表示无线接入点发送 “传送流量指示图”（DTIM）的频率。较低的设定值会使网络运行更有效，但会阻止电脑进入节电休眠模式。较高的设定值则允许电脑进入休眠模式而节省电力，但会干扰无线传输。
- RTS 阈值：此设置决定 “无线接入点”调整收发之前的数据包大小，以确保有效的通信。其值应保持默认设置 2347。如果出现不一致的数据流，建议只做略微修改。
- 分割阈值：规定拆分数据包或创建新数据包之前数据包的最大长度。其值应保持默认设置 2346。设置较小则意味着数据包较小，这会导致每次传输产生更多的数据包。如果数据包的错误率很高，可以减小该值，但很可能会降低整个网络的性能。建议只对该值做轻微改动。
- SNR 模式：此配置决定无线带宽调整的方式。停用 SNR 模式，将会使用微调的方式来调整无线的带宽；启用 SNR 模式， NAV10V2-WF 网关将根据环境快速调整带宽。

3. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

无线 QoS

您可以在此界面上为 “无线接入点”配置相关的 QoS 设置。

1. 选择 “配置” -> “接口和连接” -> “无线设置” -> “QoS”，打开无线 QoS 设置界面。
2. U-APSD （自动省电传输模式）：只有当所有 SSID 启用 WMM 时，才可使用本选项。如果希望客户机设备具有 U-APSD 能力以利用省电模式，请选择已启用。默认设置为已停用。
3. SSID 配置表：下面的表格为 VLAN 和 QoS 提供特殊的 SSID 设置。
   - SSID 名称：此处显示 “基本无线设置”中所定义的 SSID 名称。对于停用的 SSID，其选项将变为灰色。
   - 传输速率限制：可以限制网络中使用的最大数据传输率，以便节省带宽和客户机设备的功率消耗。实际的数据传输率由 “无线接入点”和客户机设备之间的 “自动回调”机制来决定。“混合”或 G-Only 无线模式的默认值为 54 Mbps，B-Only 模式为 11 Mbps。
   - WMM：“Wi-Fi 多媒体”是 WiFi 联盟在 IEEE 802.11e 制订之前所定义的一种 QoS 特性。现在是 IEEE 802.11e 的组成部分。启用时， WMM 可以为不同类型的通信提供四种优先队列。根据 QoS 设置 （IP 或第 2 层数据头中）， WMM

自动将入站的有线数据包映射到合适的队列。 WMM 在您的环境中为无线通信提供优先排序的能力。默认设置为停用。

4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

编辑接口 / 连接

此页面可以查看和编辑 NAV10V2-WF 网关的接口设置以及连接状态等信息。

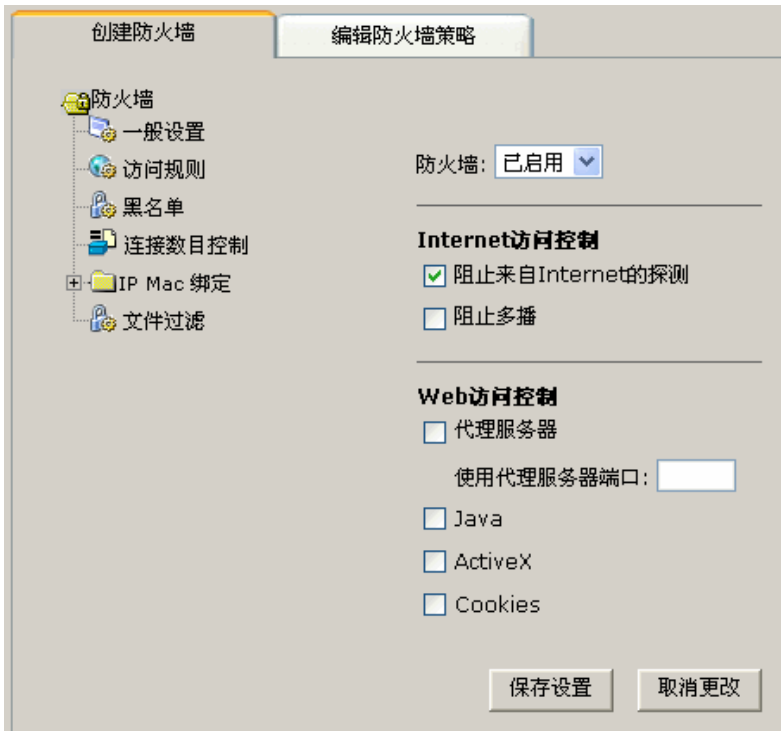
- 从接口列表中仅能显示接口或连接的名称、IP 地址、类型和 MAC 地址等信息，如需查看该接口或连接的详细信息，点击选中的接口或连接，在下方的窗口中将显示该接口或连接的详细信息。
- 刷新：点击以更新连接的接口列表信息。
- 编辑：点击以更改接口配置。请参考 “**WAN** ”、“**LAN**”和 “**EVDO**”等小节了解如何设置 WAN 接口、 LAN 接口、 EVDO 连接等。

防火墙和 **ACL**

使用防火墙功能可应用预先定义的规则或自定义规则来保护用户的专有网络不受大多数常见攻击的影响，用户也可以启用系统日志来记录防火墙日志。

一般设置

1. 选择“配置”->“防火墙和 ACL”->“防火墙”->“一般设置”，打开防火墙设置界面。



2. 选择在 NAV10V2-WF 网关上启用或停用防火墙功能。
3. Internet 访问控制：
   - 阻止来自 Internet 的探测：此选项可使网络避开“ping”或侦测，并通过隐藏网络端口来加强网络安全，这样入侵者将更加难以进入您的网络。选中复选框可启用此特性。
   - 阻止多播：多播允许在同一时间向特定的客户机群提供多个传输。如果允许多播，则 NAV10V2-WF 网关将允许从 WAN 端口向 LAN 端口转发 IP 多点传送包。多播通信会占用 NAV10V2-WF 网关 CPU 资源和网络带宽。选中复选框可停用此特性。
4. Web 访问控制：选择要限制的 Web 特性。所有这些特性都会给 LAN 侧的计算机带来安全问题。您需要在这些应用需求和安全之间进行权衡。默认设置为不选。
   - 代理服务器：如果本地用户有权访问 WAN 代理服务器，他们就可能绕过“NAV10V2-WF 网关”的内容过滤并访问被 NAV10V2-WF 网关阻止的 Internet 站点。拒绝代理服务器可阻止对任何 WAN 代理服务器的访问。当选取

代理服务器选项，请于此栏位输入代理服务器所使用之端口，防火墙将会依此设置阻止对 WAN 代理服务器的访问。

- Java：Java 是一种网站编程语言。如果拒绝 Java 程序，您将无法访问使用这种编程语言创建的 Internet 站点。
- ActiveX：ActiveX 是一种 Microsoft （Internet Explorer）网站编程语言。如果拒绝 ActiveX，您将无法访问使用这种编程语言的 Internet 站点。而且 Windows 更新要使用 ActiveX，因此如果阻止 ActiveX， Windows 更新将不再工作。
- Cookies：Cookie 是您与 Internet 站点交互时由该站点使用的数据， cookie 保存在您的电脑上，因此您可能不希望拒绝 cookie。

5. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

访问规则

NAV10V2-WF 网关最多支持用户创建 100 条防火墙的访问规则。

1. 选择 “配置” -> “防火墙和 ACL” -> “防火墙” -> “访问规则”，打开防火墙访问规则设置界面。

2. 定义防火墙的访问规则：
   - 策略类型：选择要将访问规则应用于 “出方向访问控制”还是 “入方向访问控制”。默认情况下， NAV10V2-WF 网关的 “出方向访问控制”策略的动作为允

许，“入方向访问控制”策略的动作为拒绝。用户可以手动添加 ACL 规则，拒绝出方向的访问服务，或允许入方向的访问服务。

- 服务：在列表中选择要应用访问控制设置的服务 （通信类型 / 端口号）。点击“服务管理”可添加或删除服务。
- 日志：选择 “匹配此规则时记入日志”，可在 NAV10V2-WF 网关的日志审核文件中记录与该访问规则所匹配的通信。选择 “不记入日志”，可停用访问规则记录。
- 源接口：在要应用访问规则的 WAN 网络中为“入方向访问控制”类型的策略选择来源接口。“出方向访问控制”策略的来源接口不受限制。
- 源地址：为 Internet 类型的访问策略选择要应用访问规则的来源 IP 地址或 MAC 地址。使用 “入方向访问控制”类型的策略时，只有来源 IP 可选。
- 目标地址：选择要应用访问规则的目标 IP 地址。
- 应用此规则：设置应用此规则的时间和日期。
- 按 URL 过滤：选择该功能，输入您要阻隔的网站并将其添加到列表。
- 按关键字过滤：选择该功能，输入您要阻隔的关键词并将其添加到列表。

3. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

注释 NAV10V2-WF 网关最多可设置 10 条按关键字过滤的防火墙访问规则和 10 条按 URL 过滤的防火墙访问规则。

黑名单

本功能可阻止特定的使用者对 NAV10V2-WF 网关的访问。用户可以查看、添加、删除、编辑防火墙的黑名单设置。

1. 选择 “配置” -> “防火墙和 ACL” -> “防火墙” -> “黑名单”，打开防火墙黑名单设置界面。
2. 用户可以查看、添加、删除、编辑防火墙的黑名单设置。例如，点击 “添加”按钮，添加一个黑名单。
   - 来源 IP 地址：想要阻止的主机 IP 地址，可以是任何 IP 地址。
   - 来源端口：想要组织的来源端口，可以是任何的端口。

3. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

连接数目控制

本功能可限制特定区域或网络 IP 地址所发起的 TCP 连接数目。

1. 选择 “配置” -> “防火墙和 ACL” -> “防火墙” -> “连接数目控制”，打开防火墙连接数量控制设置界面。
2. 点击 “添加”按钮，可添加一条连接数目控制的设置，防火墙将据此限制特定 IP 的最大 TCP 连接数目。
   - 源 IP 地址：设定希望限制的主机的 IP 地址。
   - 允许连接数目：设定希望限制的 TCP 连接最大值。
3. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

IP Mac 绑定

基本设置

使用 IP Mac 绑定功能可以保护 NAV10V2-WF 网关内部网络的 IP/Mac 资料不被攻击所破坏。

1. 选择 “配置” -> “防火墙和 ACL” -> “IPMac 绑定” -> “基本设置”，打开 IPMac 绑定设置界面。
2. 启用或停用 IP Mac 绑定功能。
3. 启动或停用自动学习：若启动自动学习机制，系统会根据使用者的上网形态来判定该 IP/MAC 是否为合法的 IP/MAC。若判定为合法的 IP/MAC 位置，则系统会进行自动绑定 IP/MAC 的动作。
4. 设置 ARP Flooding 阀值：该数值决定每一秒系统接受 ARP 包的数目。当值设得越大，代表系统该秒内可允许收到的 ARP 包越多，若要防止系统被 ARP Flooding 攻击而瘫痪，这个值必须设为较小的值。
5. 设置 ARP 广播隔离：为了要让所有网络使用者可以得到正确的系统 IP/MAC 值，系统会定期的发出信息更新网络使用者系统的 IP/MAC，这个数值代表的是系统发信息的间隔时间，单位是秒。 0 代表系统关闭该功能。
6. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

IP Mac 绑定表

查看用户设置的 IP Mac 绑定信息。

1. 选择“配置”->“防火墙和 ACL”->“IPMac 绑定”->“IPMac 绑定表”，打开 IPMac 绑定表设置界面。
   - 扫描：按下后系统会自动扫描所有局域网，并把局域网下的网络用户列举出来。
   - 刷新：更新 IP/MAC 绑定表信息。
   - 添加：添加一个固定的 IP/MAC 设置。
     - IP Address：欲设置的 IP 地址。
     - MAC：欲设置的 MAC 地址。
   - 编辑：编辑选定的 IP/MAC 设置。
   - 删除：删除选定的 IP/MAC 设置。
   - 删除全部：删除全部 IP/MAC 设置。
   - 定义全部未定义项目：对 IP/MAC 绑定表内的所有信息，进行保存的动作，并设置为永久合法 IP/MAC 设置。
2. 完成对此界面的更改后，点击“保存设置”按钮保存所做的修改，或点击“取消更改”按钮撤消所做的修改。

文件过滤

NAV10V2-WF 网关支持对通过 HTTP 方式和 FTP 方式上传和下载文件的类型进行过滤。

1. 选择“配置”->“防火墙和 ACL”->“文件过滤”，打开文件过滤设置界面。
2. 分别选择启用或停用基于 HTTP 协议和基于 FTP 协议的文件过滤功能。
3. 如启用文件过滤功能，请输入文件类型，点击“添加”按钮添加要过滤得文件类型。
4. 完成对此界面的更改后，点击“保存设置”按钮保存所做的修改，或点击“取消更改”按钮撤消所做的修改。

编辑防火墙策略

“编辑防火墙策略”任务栏允许用户查看和编辑定义的防火墙策略。

1. 选择 “配置” -> “防火墙和 ACL” -> “编辑防火墙策略”，打开编辑防火墙策略设置界面。
   - 出方向访问控制默认值：允许所有通信从任一 LAN 到任一 WAN。
   - 入方向访问控制默认值：拒绝所有通信从任一 WAN 到任一 LAN。
2. 点击 “刷新”按钮，可以刷新 NAV10V2-WF 网关当前定义的防火墙控制策略列表。
3. 添加新规则：点击 “添加新规则”按钮，可添加新的访问规则。
4. 应用规则：从防火墙策略列表中选择一条或多条策略，然后点击 “应用规则”按钮，可将选中的防火墙策略应用到 NAV10V2-WF 网关上。
5. 恢复默认规则：点击 “恢复默认规则”按钮，可恢复 NAV10V2-WF 网关默认的防火墙策略。

VPN

虚拟专用网络 （VPN）可以在不安全的公共网络上 （如 Internet）建立安全的连接。经 VPN 发送的通信经过加密并且不能被该 VPN 之外的任何人读取。

1. 选择 “配置” -> “VPN”，打开设置 VPN 类型的界面。用户可以选择启用站点到站点 VPN 或禁用 VPN。

   - IPSec(站点到站点)VPN：选择本选项将启用 “站点到站点 VPN”。
   - 禁用 VPN 选项：选择本选项将同时禁用 “站点到站点 VPN”。
2. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

站点到站点 VPN

使用本选项可以配置从 NAV10V2-WF 网关到另一台 VPN 设备 (使用预共享密钥) 的 VPN 隧道。要完成本配置，必须知道远程设备的 IP 地址。如果使用预共享密钥进行验证，该密钥必须与远程设备上配置的预共享密钥相匹配。

NAV10V2-WF 网关最多可建立 25 条站点到站点 VPN 通道。

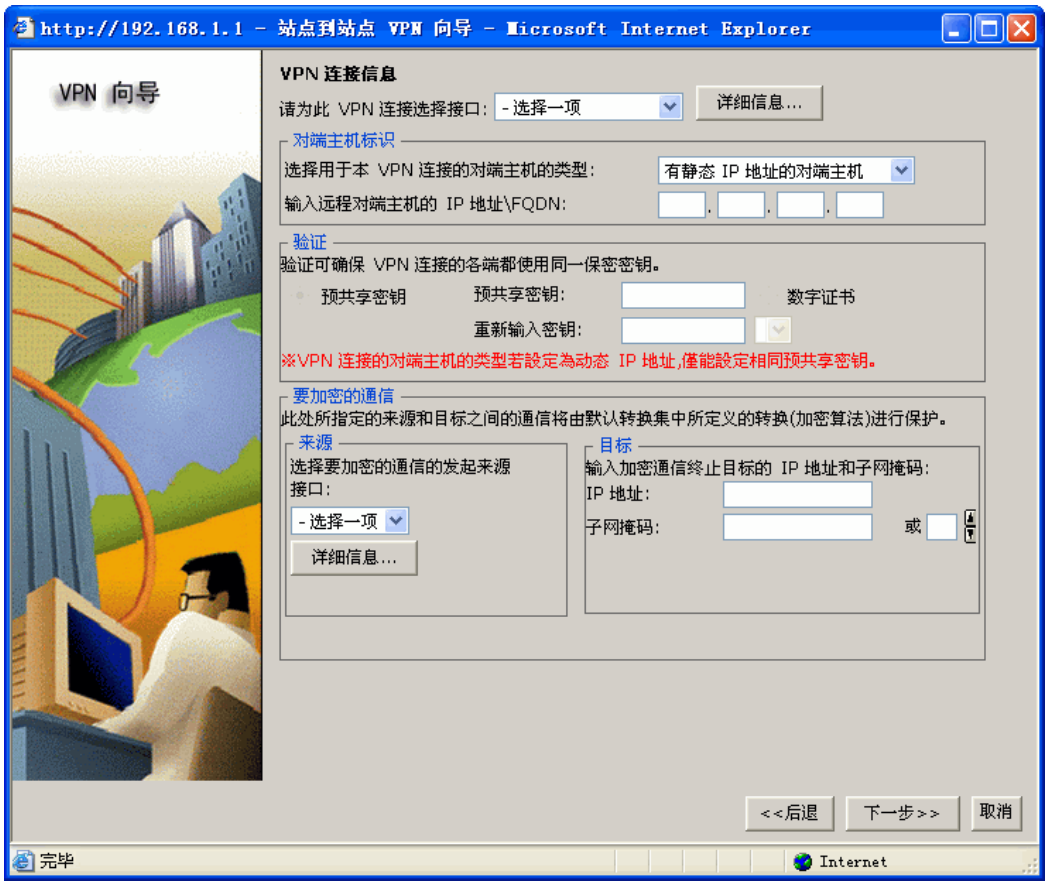
创建站点到站点 VPN

此向导将引导您完成站点到站点 VPN 信道的单端配置。为使通道正常工作，必须用相同的 VPN 配置内容配置对端主机。请选择 以下设置之一，然后点击 “下一步” 按钮开始操作。

- 快速安装：使用快速安装向导，用户只需输入很少信息并采用默认值，即可快速创建站点到站点 VPN 通道。在两台思科 NAV10V2-WF 网关之间建立 VPN 隧道时建议使用。
- 逐步操作向导：逐步操作向导允许您指定默认配置或自定义配置。

快速安装

1. 选择 “快速安装”，并点击 “下一步”，开始创建站点到站点 VPN。
2. 点击 “查看默认值”，在弹出的窗口中显示 SDM VPN 的默认配置，包括默认的 IKE 策略和转换集。这些默认的 IKE 策略和转换集将会应用到创建的站点到站点 VPN 通道上。
3. 配置 VPN 连接信息：在此窗口中设置 VPN 连接指定接口、对端主机的 IP 地址或者主机名称，和 VPN 各端用于验证的的保密密钥。此处所指定的来源和目标之间的通信将由默认转换集中所定义的转换 (加密算法) 进行保护。



- 请为此 VPN 连接选择接口：选择要连接到远端对端主机的接口。
- 对端主机标识：
  - 有静态 IP 地址的对端主机：如果对端主机是固定 IP 地址，请选择这个项目。
  - 有动态 IP 地址的对端主机：如果对端主机是动态 IP 地址，请选择这个项目。
  - 主机名称或 FQDN 的对端主机：使用主机名称或者 FQDN，请选择这个项目。
- 验证：
  - 预共享密钥：请输入预共享密钥，为了确保正确性，必须重新重新输入一次，请与对端主机的管理者通过安全保密的方式交换预共享密钥。
  - 数字证书：通过数字证书进行认证。“快速安装”选项中不可使用数字证书进行认证。

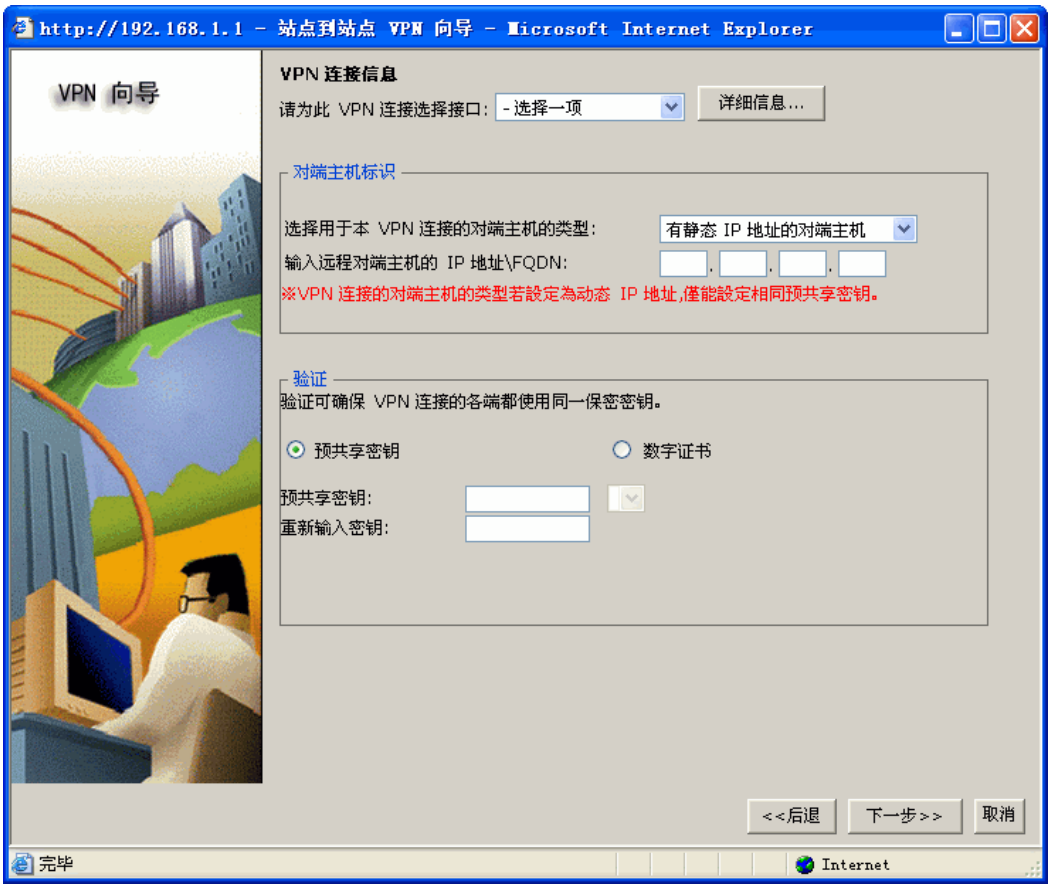
- 要加密的通信：如果使用快速安装站点到站点 VPN，必须指定来源接口和目标子网。
- 来源：请选择此 VPN 连接的加密通信的来源接口，所有经由此接口通往设定的目标 IP 地址的通信将会被加密。点击 “详细信息” 按钮，可查看选择的来源端口的详细信息。
- 目标：请输入加密通信终止的目标 IP 地址和子网掩码。

4. 完成好以上设置之后，点击 “下一步”，查看配置汇总信息。
5. 勾选 “立即启用” 并点击 “保存” 按钮，可立即启用该站点到站点 VPN。

逐步操作向导

逐步操作向导将引导用户逐步完成站点到站点 VPN 的创建。

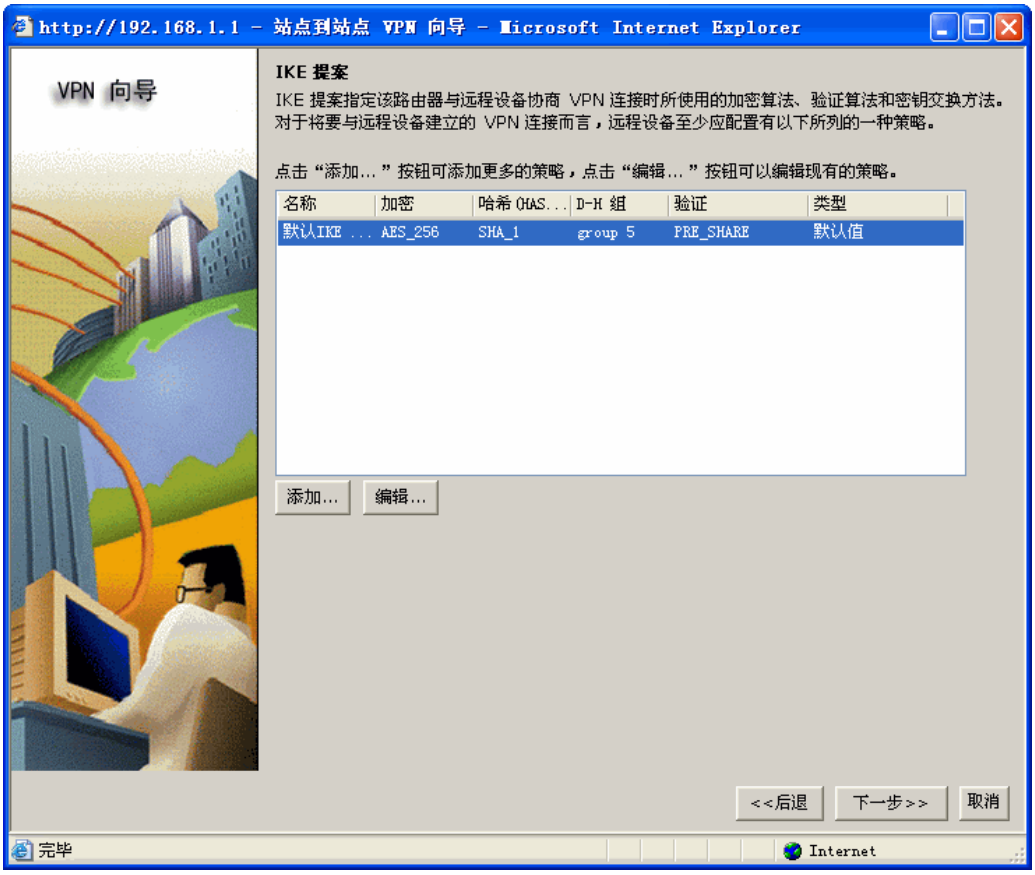
1. 选择 “逐步操作向导”，并点击 “下一步”，开始创建新的站点到站点 VPN。
2. 配置 VPN 连接信息：



- 请为此 VPN 连接选择接口：选择要连接到远端对端主机的接口。
- 对端主机标识：
  - 有静态 IP 地址的对端主机：如果对端主机是固定 IP 地址，请选择这个项目。
  - 有动态 IP 地址的对端主机：如果对端主机是动态 IP 地址，请选择这个项目。
  - 主机名称或 FQDN 的对端主机：使用主机名称或者 FQDN，请选择这个项目。
- 验证：
  - 预共享密钥：请输入预共享密钥，为了确保正确性，必须重新重新输入一次，请与对端主机的管理者通过安全保密的方式交换预共享密钥。
  - 数字证书：选择 x.509 数字证书进行认证。

注意 VPN 连接的对端主机的类型若设定为动态 IP 地址，只支持使用相同的预共享密钥进行认证。

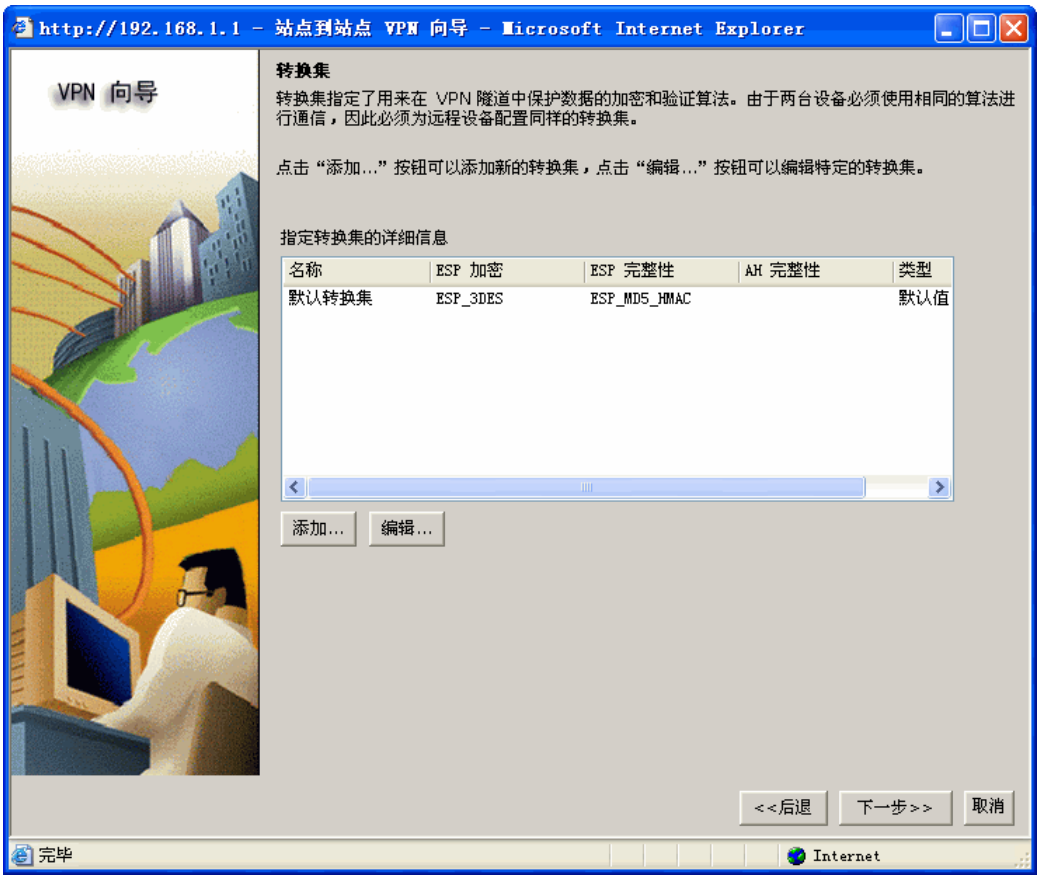
3. 点击 “下一步”，开始配置 IKE 提案。 IKE 提案指定该 NAV10V2-WF 网关与远程设备协商 VPN 连接时所使用的加密算法、验证算法和密钥交换方法。对于将要与远程设备建立的 VPN 连接而言，远程设备至少应配置有以下所列的一种策略。用户可选择默认的 IKE 提案，也可以添加新的 IKE 提案，或者编辑并选择现有的 IKE 提案。



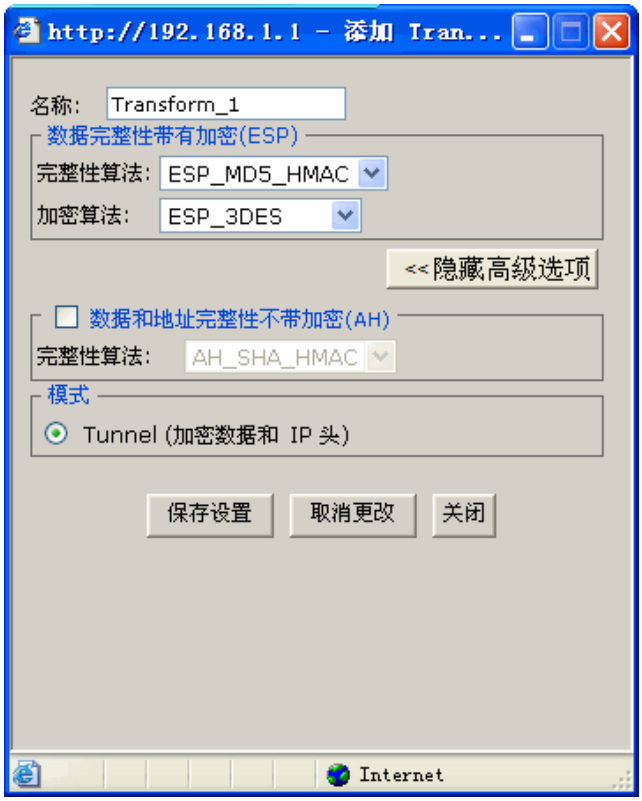
4. 点击“添加”按钮，打开“配置 IKE 策略”页面，如下所示：

- 名称：请输入此 IKE 策略的名称。
- 验证：IKE 策略的类型应为 PRE_SHARE。
- 加密：NAV10V2-WF 网关支持下列的加密算法，更安全的算法将使用越高的 CPU 处理能力。
  - 3DES ：比 DES 更加安全的加密算法，支持 168-bit 加密。
  - AES128：128-bit AES 加密。AES 提供比 DES 安全的加密和比 3DES 更高的运算效率。
  - AES192：192-bit AES 加密。
  - AES256：256-bit AES 加密。
- 哈希 (HASH) 算法：在 VPN 连接沟通过程中的验证算法，NAV10V2-WF 网关支持下列的算法。
  - SHA_1：用于验证报文验证的哈希 (HASH) 算法。
  - MD5：用于验证报文验证的哈希 (HASH) 算法。
- D-H 组：Diffie-Hellman 是一个公开金钥密码协议，此 协议允许两台 NAV10V2-WF 网关在一个不安全的通信通道共同建立一个共享金钥。
  - Group2：1024- 位组。
  - Group5：1536- 位组。这个组比 Group2 提供更高的安全性，但是也需要更多的 CPU 处理时间。
  - Group14：2048- 位组。这个组比 Group5 提供更高的安全性，但是也需要更多的 CPU 处理时间。
- 使用寿命：此 IKE 策略应该被重新协商的时间。

5. 从 IKE 提案列表中选择一条 IKE 提案，点击 “下一步”，开始配置转换集。转换集指定了用来在 VPN 隧道中保护数据的加密和验证算法。由于两台设备必须使用相同的算法进行通信，因此必须为远程设备配置同样的转换集。



6. 用户可选择默认的转换集，也可以添加新的转换集，或者编辑并选择现有的转换集。点击“添加 ...”按钮，打开“添加转换集”页面：



- 名称：请输入此转换集的名称。
- 数据完整性带有加密 (ESP)：
  - 完整性算法：ESP 完整性算法的型态。

    ESP_MD5_HMAC

    ESP_SHA_HMAC
  - 加密算法：ESP 加密算法的型态。

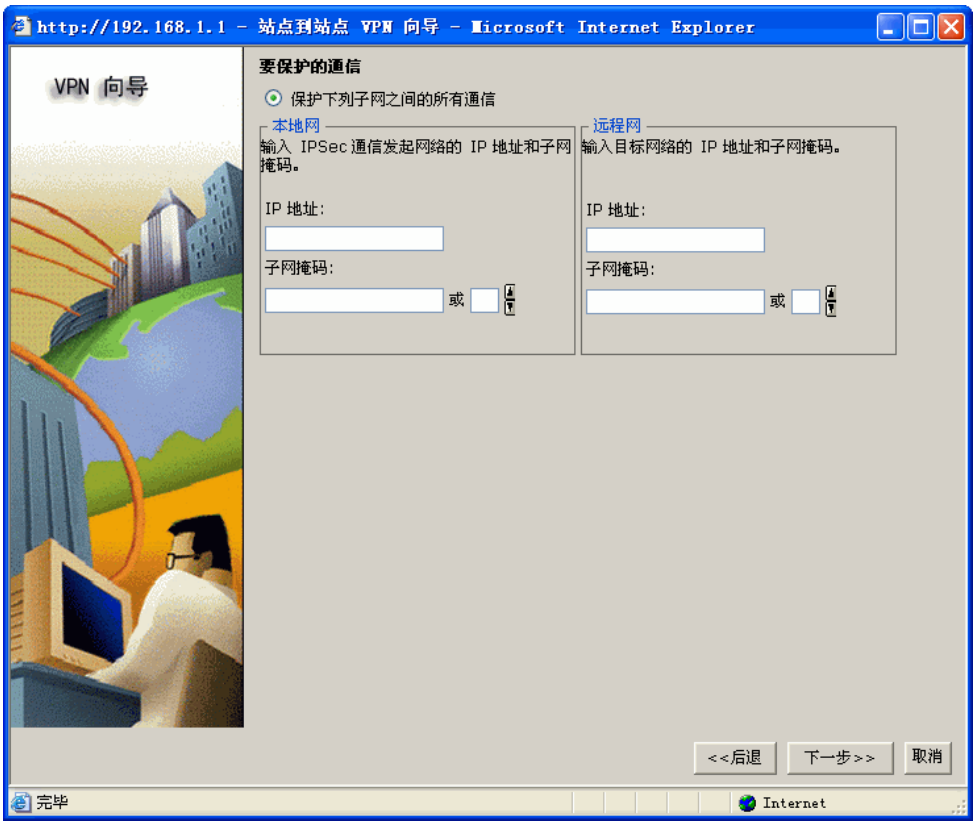
    ESP_3DES

    ESP_AES_128

    ESP_AES_192

    ESP_AES_256
- 数据和地址完整性不带加密 (AH)：AH 完整性算法的型态 AH_SHA_HMAC。
- 模式：Tunnel (加密数据和 IP 头)。

7. 从转换集列表中选择一条转换集，点击 “下一步”，开始配置要保护的通信。



- 本地网：请输入欲保护的子网 IP 地址和掩码，所有通往远程网的所有本地网通信将被保护。
- 远程网：请输入欲保护的远程 IP 地址和掩码，所有通往此远程网主机群的通信将被保护。

8. 点击 “下一步”，查看配置汇总信息。
9. 勾选 “立即启用”并点击 “保存”按钮，可立即启用该站点到站点 VPN。

编辑站点到站点 VPN

使用本选项可以编辑在 “创建站点到站点 VPN”选项中所配置的 VPN 隧道。

- 添加：点击此按钮创建新的站点到站点 VPN。
- 编辑：点击此按钮编辑站点到站点 VPN。
- 删除：点击此按钮删除站点到站点 VPN。

- 连接：选择您想要连接的 IPSec 策略，点击此按钮即可连接 VPN。
- 断开：选择您想要连接的 IPSec 策略，点击此按钮即可断开 VPN 连接。
- 刷新：点击此按钮刷新页面中的 IPSec 策略状态。

Quick VPN Account

NAV10V2-WF 网关最多可创建 50 个 Quick VPN Accout。用户需在本地站点上安装对应的 QVPN 客户端，以指定的快速 VPN 帐号登录 VPN 通道，以建立与主机之间的连接。

1. 选择“配置”-〉“VPN”-〉“VPN”-〉“Quick VPN Account”，打开快速 VPN 帐号设置界面：

2. 点击“添加”按钮，新增一组账号密码，每组账号可设定是否允许使用者修改密码。
   - 账号：登录账号。
   - 密码：账号登录密码。
   - 请再输入一次密码：确认密码。
   - 是否允许改变密码：设定使用账号是否可以改变密码。
3. 启用快速 VPN 帐号。用户需要在远程主机上安装 VPN 客户端，通过设定的帐号和密码与 NAV10V2-WF 网关建立 host to site（主机到站点）的通道。请与您所购买本产品的代理商或销售代表联系，获得最新版本的 QVPN utility，并安装到本地主机上。

4. 进阶设定：指定是否为选中的 Quick VPN Account 启用虚拟 IP 服务器和虚拟 IP Tunnel 模式等。点击 “进阶设定” 按钮，打开虚拟 IP 服务器设置界面。
   - 虚拟 IP 服务器：启用或停用虚拟 IP 服务器。
   - 虚拟IP Tunnel模式：IP管道技术是在IP报文上再次封装IP报文协议的一种技术。允许将一个目标为 A 的 IP 数据报文封装成为目标为 B 的 IP 数据报文，在特定的 IP 管道中传输。 NAV10V2-WF 网关支持 2 种 IP 管道技术，分别是 Split Tunnel 和 Full Tunnel，用户可分别选择其中一种或选择两者都支持。这种模式要求操作系统支持 IP Tunnel，通过对 IP 报文再次封装转发，达到负载均衡的目的。
   - 使用VLAN网段为虚拟IP网段：是否使用NAV10V2-WF网关定义的VLAN组的网段作为虚拟 IP 网段。
     - 默认为 “停用”，用户需要分别设定虚拟 IP 服务器地址、起始 IP 和结束 IP。
     - 如果选择 “启用”，用户需要选择要使用的 VLAN 网段，并分别定义起始 IP 和结束 IP。
5. 点击 “停用” 按钮，可停用 Quick VPN Account，不允许任何远程主机以账号建立通道。
6. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

TIP 以下简单介绍如何使用 QVPN 客户端，建立与 QVPN 服务器的连接。

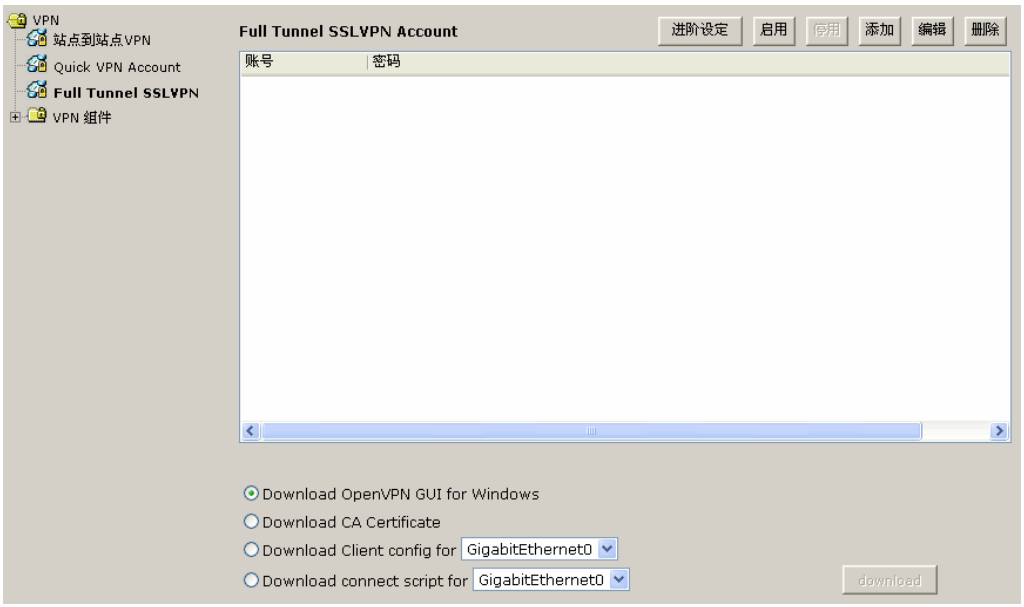
1. 请与您所购买本产品的代理商或销售代表联系，获得最新版本的 QVPN utility，并安装到本地主机上。
2. 打开 QVPN utility，设置以下参数：
   - User Name：输入 Quick VPN Account 的用户名。
   - Password：输入 Quick VPN Account 的用户名。
   - Server Address：输入创建的虚拟 IP 服务器的地址。
   - Tunnel Mode：选择通道模式。
   - Use Remote DNS Server：是否使用远程 DNS 服务器？选择启用，QVPN 客户端的主机将使用远程的 DNS 服务器。
3. 点击 “Connect” 按钮，开始连接远程 QVPN 服务器。

Full Tunnel SSL VPN

NAV10V2-WF 网关支持 Full Tunnel SSL VPN （完全隧道 SSL VPN），在 NAV10V2-WF 网关上设定好 VPN 用户账号后，用户可以通过安全的 https 连接下载并安装 OpenVPN 客户端、CA 证书和相关的配置文件和连接脚本到本地 windows 主机上，通过 OpenVPN 建立与 NAV10V2-WF 网关的 SSL VPN 通道。

NAV10V2-WF 网关最多支持建立 50 条 SSL VPN 隧道。

1. 选择 “配置” -〉“VPN” -〉“VPN” -〉“Full Tunnel SSL VPN”，打开 Full Tunnel SSL VPN 帐号设置界面：



- 添加：创建新的 Full Tunnel SSL VPN 账号。
- 编辑：编辑已有 Full Tunnel SSL VPN 账号信息。
- 删除：删除 Full Tunnel SSL VPN 账号。
- 启用 / 停用：启用或停用选择的 Full Tunnel SSL VPN 账号。
- 进阶设定：指定通过什么接口提供 Full Tunnel SSL VPN 连接服务。

2. 添加 Full Tunnel SSL VPN 账号：
   - 账号：输入 SSL VPN 账号名称。
   - 密码：输入 SSL VPN 的账号密码。
   - 请再输入一次密码：输入确认密码。

3. 选择 SSL VPN 账号，然后点击 “启用” 按钮，启用添加的 SSL VPN 账号。
4. 进阶设定：您可以选择通过 GigabitEthernet0、 GigabitEthernet1 或 2 个接口提供 Full Tunnel SSL VPN 连接服务。选择一个 SSL VPN 账号，然后点击 “进阶设定” 按钮，设置提供 SSL VPN 连接服务的接口。
5. 下载并安装 OpenVPN 客户端。运行 openVPN-installer.exe，依照安装向导将 OpenVPN 客户端安装到本地 window 主机上。请参考 “下载 **SSL VPN** 设定组合” 了解更多信息。
6. 安装好 OpenVPN 客户端后，双击 “ovpn_wanx.bat”，弹出一个命令行窗口。
7. 输入用户名和密码，开始建立与 NAV10V2-WF 网关的 SSL VPN 连接。

VPN 组件

VPN 组件任务栏允许用户查看、新增、删除或编辑 NAV10V2-WF 网关默认或新增的转换集策略和 IKE 策略。

IPSec 转换集

请参阅 “创建站点到站点 **VPN**”。

IKE 策略

请参阅 “创建站点到站点 **VPN**”。

路由

NAV10V2-WF 网关允许用户在路由表中输入静态路由或使用路由协议建立动态路由表。

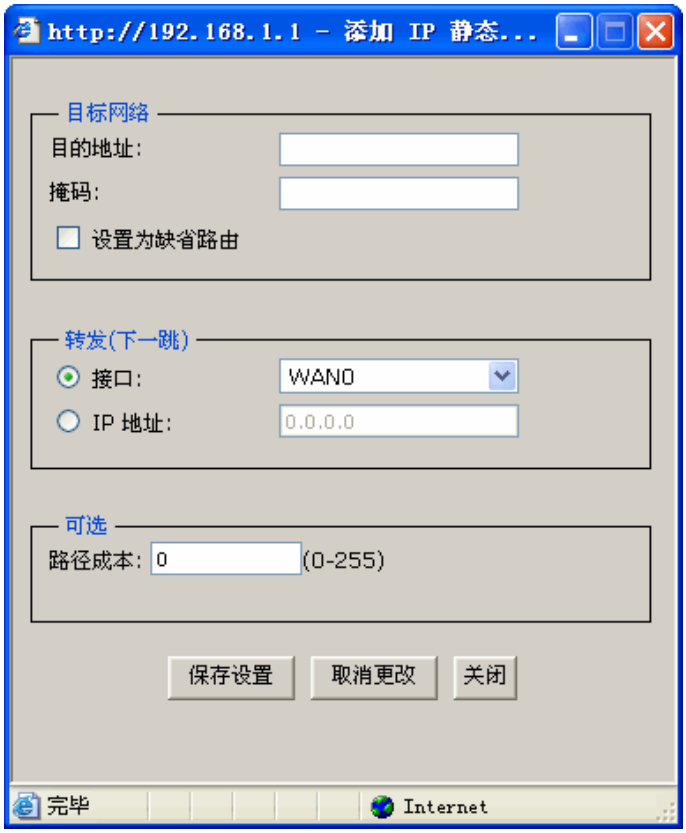
静态路由

用户可以查看、添加、编辑、删除、导入或导出 NAV10V2-WF 网关的静态路由配置。

1. 选择 “配置” -〉“路由” -〉“路由” -〉“静态路由”，打开静态路由设置界面。
   - 点击 “汇入” 按钮，可从本地 PC 上导入静态路由表。
   - 点击 “汇出” 按钮，可将 NAV10V2-WF 网关的静态路由表导入到本地 PC。
   - 点击 “添加” 按钮，可将新增静态路由；

- 点击 “编辑” 按钮，可编辑现有的静态路由；
- 点击 “删除” 按钮，可删除现有的静态路由；
- 点击 “删除全部” 按钮可删除表格中的全部静态路由设置。

2. 下面是添加静态路由界面：



3. 可以通过网络前缀号码和网络掩码来指定 “目标网络”。对于默认路由，选取下方的复选框。
4. “转发 （下一跳）” 可指定将数据包转发到目标网络的何处。可通过外发接口 （下拉菜单）或下一跳 NAV10V2-WF 网关的 IP 地址来指定。
5. 定义路由条目的距离度量单位。当两个路由条目同时到达目标网络时，该选项可定义其优先级。数值越小，优先级越高。
6. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

注释 用户如需批量输入静态路由表，可先添加单个静态路由，点击 “导出”按钮，将静态路由配置表 （routes.cfg）导入到本地主机上，将所有需要输入的静态路由配置按照输入到该配置文件，然后点击 “导入”按钮，批量导入到 Nav10V2-WF 网关。

下列为静态路由的参考格式：

```
###Cisco-Navigator-Static-Routing-Rules###
0.0.0.0,0.0.0.0,1,WAN0,0.0.0.0,0
58.0.0.0,255.0.0.0,0,WAN1,0.0.0.0,0
59.0.0.0,255.0.0.0,0,WAN1,0.0.0.0,0
60.0.0.0,255.0.0.0,0,WAN1,0.0.0.0,0
113.0.0.0,255.255.0.0,0,WAN1,0.0.0.0,0
114.0.0.0,255.255.0.0,0,WAN1,0.0.0.0,0
202.0.0.0,255.255.255.0,0,WAN1,0.0.0.0,0
203.0.0.0,255.255.255.0,0,WAN1,0.0.0.0,0
……
```

动态路由

NAV10V2-WF 网关可经由动态路由来动态地检测目前的网络变动情况。可选择 RIP 或 OSPF 路由协议来配置动态路由。

RIP

1. 选择 “配置”-〉“路由”-〉“路由”-〉“动态路由” -〉“RIP”，打开 RIP 设置界面。
2. 启用 RIP：若希望启用 RIP 动态路由请选中此项。
3. 选择 RIP 版本，用户可选择版本 1、版本 2 或是默认值。
4. 设置可用接口列表：

注意 当启动 RIP V1 时，请注意此接口是否设为有分级网络。如是设为无分级网络， RIP V1 将不会广播此接口网络。

- 如果 WAN0 或 WAN1 接口设置有子接口，子接口将会被视为一个可用接口添加到对应的 “可用接口列表”中。
- 将接口被动化：若不需要发送侦测网络状态包，则勾选 “将接口被动化”，但此时仍会接收及回应接收的侦测报文。对 WAN 接口的子接口，必须将其被动化。

- Authentication：如果选择的 RIP 版本为 “版本 1” 或 “默认”，接口将采用默认的认证方式，如果选择的 RIP 版本为 “版本 2”，可自定义 RIP 接口的认证方式。
  - None：不认证。
  - Simple Password Authentication：简单密码认证，密码长度最多为 16 个字母数字。
  - MD5 Authentication：MD5 认证，MD5 的密钥请使用 13 位字母数字或 26 位 16 进制数字。
- 启用 RIP：使用者可针对个别接口启动 RIP 动态路由。

注意 当防火墙的 阻止多播 功能启用时， RIP 版本 2 无法作用。

5. 完成对此界面的更改后，点击 “保存设置” 按钮保存所做的修改，或点击 “取消更改” 按钮撤消所做的修改。

OSPF 基本设置

1. 选择 “配置” -〉“路由” -〉“路由” -〉“动态路由” -〉“OSPF” -〉“基本设置”，打开 OSPF 基本设置界面。
2. 启用 OSPF：启用或禁用 OSPF 进程。
3. 路由器 ID：必选项，指定路由器 ID 给 OSPF 的进程。路由器 ID 可以是 NAV10V2-WF 网关上的实体 IP 地址或是一组由任意的 32 个数值所组成的字符串 (如：192.168.1.1)。然而，路由器 ID 必须在这个 OSDF 域内唯一存在，若是在不同的 NAV10V2-WF 网关上设定了相同的路由器 ID 将导致错误发生。若不指定路由器 ID (空的)，将无法启用 OSPF。
4. 将接口被动化：让接口不主动发送 OSPF-Hello 包，待接收到来自邻接路由的 Hello 报文才会被动发送。
5. 设置网路 / 掩码 / 区域：必选项，指定 OSPF 启用哪些接口网路，发送 Hello 报文与路由表信息。
   - 网路 / 掩码：OSPF 透过此接口向指定的网路范围发送网路信息给此范围中的其它 OSPF 路由器。
   - 区域：指定接口网络属于哪一个 OSPF 区域。
6. 完成对此界面的更改后，点击 “保存设置” 按钮保存所做的修改，或点击 “取消更改” 按钮撤消所做的修改。

OSPF 高级设置

区域设置

1. 选择“配置”-〉“路由”-〉“路由”-〉“动态路由”-〉“OSPF”-〉“高级设置”-〉“区域设置”，打开区域设置界面。
2. 范围设置：显示区域范围设定，新增 OSPF 范围请按 “添加”，修改请按 “编辑”，删除请按 “删除”。
3. 下图为添加 OSPF 范围对话框：

- 区域识别码：

  数值格式 <0-4294967295> 与 IP 格式相对应， area 0 对应到 area 0.0.0.0，area 255 对应到 area 0.0.0.255， area 256 对应到 area 0.0.1.0， area 511 对应到 area 0.0.1.255。 area 0 称为骨干区域 (Backbone area)。

- 范围：表示 LSA 向骨干区域宣告某一个范围内应至少包含一个内部区域 (intra-area)。

  - 无：不指定区域范围的其它参数。

- 广播：将这个范围的内部区域路径公布到其它区域中。
- 成本：指定并公布这个区域范围的 metric 成本。
- 广播成本：指定并公布这个区域范围的 metric 成本。
- 非广播：不将这个范围的内部区域路径公布到其它区域中 (边界路由器参数 / ABR only)。
- Substitute：包含路由信息 （Substitute）的 LSA 向骨干区域宣告某个范围至少包含一个内部区域 (边界路由器参数 /ABR only)。

4. 设置 AUTH/STUB/NSSA：设置区域中的 认证设置 (auth)、末梢区域 (stub)、半末梢区域 (nssa)。
5. 点击 “添加”按钮，可添加新的 AUTH/STUB/NSSA。

- 区域识别码：指定欲设置的区域 ID。
- Authentication：设置身份认证。
  - 明文认证：使用一般密码认证。
  - 认证 message-digest 算法：使用 MD5 HMAC 算法。
- stub/nssa：设置末梢区域或半末梢区域。

- stub：设置此区域为末梢区域。
- stub no-summary：防止 ABR 引入区域内部 (inter-area) 的路由信息。
- nssa：设置此区域为半末梢区域。
- nssa no-summary：防止 ABR 引入区域内部 (inter-area) 的路由信息。
- nssa options：设置半末梢区域的 translate 选项。
- 预设成本：设置 default-summary 的成本。

6. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

虚拟连接设置

注释 用户必须先设置好 OSPF 区域后，才能设置虚拟连接的时间间隔和认证方式。

1. 选择 “配置” -〉“路由” -〉“路由” -〉“动态路由” -〉“OSPF” -〉“高级设置” -〉“虚拟连接设置”，打开虚拟连接设置界面。
2. 设置时间间隔：可用来延伸骨干区域的范围。点击 “添加” 按钮，可新增 OSPF 虚拟连接设置的时间间隔：

- 区域识别码：指定中间的 ArealD。
- 远程路由器识别码：指定衔接在 area0 上的 ABR 路由器 ID。
- Hello 间隔：设置 hello 时间间隔。
- 重传间隔：设置重传时间间隔。
- 传送推迟：设置传送推迟时间。
- Dead 间隔：设置 Dead 时间间隔。

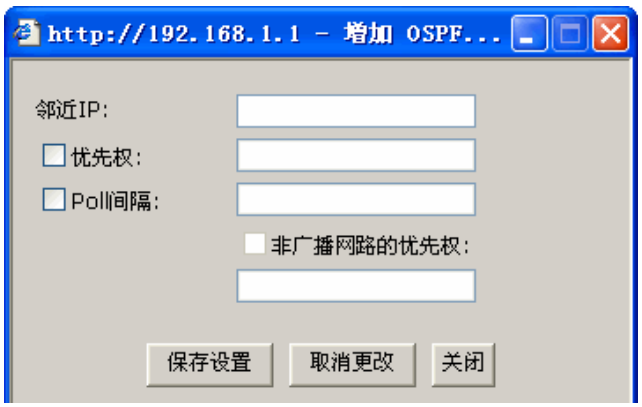
3. 认证设置：指定虚拟连线所使用的认证方法。点击 “添加”按钮，可添加虚拟连接设置的认证方法：

- 区域识别码：指定中间的 Area ID。
- 远程路由器识别码：指定衔接在 area 0 上的 ABR 路由器 ID。
- Message digest Key：<1-255> MD5 KEY，使用 MD5 算法认证，指定密码。
- Authentication Key （身份认证密钥）：使用一般认证，指定密码。

4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

邻接设置

1. 选择 “配置”-〉“路由”-〉“路由”-〉“动态路由”-〉“OSPF”-〉“高级设置”-〉“邻接设置”，打开邻接设置界面。
2. 点击 “添加”按钮，可增加新的邻接设置：



- 邻近 IP：指定邻接路由器。
- 优先权：<0-255> 设置优先权值。
- Poll 间隔：<1-65535> 设置判断邻接路由器已断线的轮询时间间隔。
- 非广播网络的优先权：＜ 0-255 ＞设置非广播网络上的邻接路由器的优先权。

3. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

界面设置

1. 选择 “配置”-〉“路由”-〉“路由”-〉“动态路由”-〉“OSPF”-〉“高级设置”-〉“界面设置”，打开界面设置界面。
2. 基本设置：指定某个界面，其成本、优先权、 Hello 时间间隔、 Dead 时间间隔、重传时间间隔、传送推迟时间、网络形态等。从界面设置列表中选择一条界面设置，点击 “编辑”按钮，可以编辑界面设置：

- 成本：<1 - 65535> 设置指定界面的连接成本。
- 优先权：<0 - 255> 选择 DR 时使用。设置为 0 表示不成为 DR。预设值为 1。
- Hello 间隔：<1 - 65535> 传送 hello 报文的时间间隔。
- Dead 间隔：<1 - 65535> 判断邻接路由器是否存在的时间间隔。
- 重传间隔：重传 database description （数据库描述）和 Link state request （连接状态请求）报文的时间间隔。
- 传送推迟：传送 LSA 报文时，须以这个值增加 LSA 的 age。
- 网络类别：设置明确的网络类别给此界面。类别如：广播网、非广播网、点到多点型网络和点到点型网络。

3. 认证：指定接口以何种认证方式进行。点击 “添加” 按钮，为界面添加新的认证方式：

- 无：不使用认证界面。
- 指定认证码：指定一般认证的认证密码。
- 指定 MD5 认证码：指定 MD5 认证的认证密码。

4. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

Redistribute setting

Redistribute setting （再分配设置）是指由外部路径导入路由信息。

1. 选择 “配置”-〉“路由”-〉“路由”-〉“动态路由”-〉“OSPF”-〉“高级设置”-〉“Redistribute setting”，打开再分配设置界面。
   - 无：不做设置。
   - 连接：导入路由类型为连接 (Connected) 的路由信息。
   - 核心：导入由核心所提供的路由信息。
   - 静态路由：导入由静态路由设置的路由信息。
   - RIP：导入由 RIP 路由协定所产生的路由信息。
   - BGP：导入由 BGP 路由协定所产生的路由信息。
   - 距离：< 0-16777214> 在导入的路由表报文中夹带距离信息。

- 距离类型：<12 > 在导入的路由表报文中夹带距离类型信息
- 路由图：以指定的路由图过滤路由表。

2. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

NAT

NAT （Network Address Translation）是一种把内部私有网络地址 （IP 地址）翻译成合法网络 IP 地址的技术。当用户的 LAN 上具有需要访问 Internet 服务的 PC 或主机，且有网络外部用户需要访问网络内部的服务器 （如网络服务器、电子邮件服务器等），可以配置 NAT 任务。

动态 NAT

如果 NAV10V2-WF 网关有 Internet 连接，指定您希望 LAN 上的 PC 和主机如何共享该连接。选择连接到 Internet 或 Internet 服务提供商的 WAN 接口。

1. 选择 “配置”-〉“NAT”-〉“NAT”-〉“动态 NAT”，打开动态 NAT 设置界面。
2. 列表中列出被分配给直接连接到 NAV10V2-WF 网关的网络的 IP 地址范围。
3. 选中 WAN0 或 WAN1，将该网络共享给指定的连接。
4. 选择 “Indirect NAT”，可将 IP 地址范围之外的 IP 地址进行 NAT 转换。
5. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

静态 NAT （DMZ）

由于某些应用服务器使用专有的 IP 地址，因此网络外的用户将无法访问 LAN 上的应用服务器。用户必须通过建立网络地址转换 （NAT）规则来提供访问，该规则将公共 IP 地址 （外部用户可以使用）与服务器的专用 IP 地址联系在一起。

要使用此功能，用户必须拥有多个由 ISP 分配的公共 IP 地址，并且 NAV10V2-WF 网关的 WAN 设置必须设为静态 IP。

注意 用户需要在 LAN 设置任务栏中启用 DMZ，并将 WAN0/WAN1 设为静态 IP 地址后，才能够使用静态 NAT 功能。

1. 选择 “配置”-〉“NAT”-〉“NAT”-〉“静态 NAT （DMZ）”，打开静态 NAT 设置界面。
2. 分别设置起始私有地址、起始公网地址、接口和地址数量等参数。
3. 点击 “添加到列表”按钮，添加该 NAT 规则。
4. 用户也可以删除 NAT 规则。选择要删除的 NAT 规则，点击 “删除选择的范围”按钮，将其删除。
5. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

端口转发

此特性是 NAPT （网络地址端口转换）特性中的一种。“端口转发”界面允许您在网络上建立公共服务，如 web 服务、 ftp 服务、 e-mail 服务或其他使用一个或多个端口号的特殊 Internet 应用程序 （如视频会议）。转发到本地网络时正在使用的端口号不会改变。这一特性可使 Internet 用户通过使用 WAN 端口 IP 地址和预先定义的端口号来访问该服务器。当用户通过 Internet 向 WAN 端口 IP 地址发送此类请求时，“NAT 路由器”将这些请求转发到 LAN 上的正确服务器。

1. 选择 “配置”-〉“NAT”-〉“NAT”-〉“端口转发”，打开端口转发设置界面。
2. 添加或删除端口转发策略：
   - 应用名称：输入您想要配置的应用的名称。前 5 条端口转发的应用程序可以从 NAV10V2-WF 网关提供的应用程序下拉框中选择。
   - 开始：指端口范围的开始。输入服务器或 Internet 应用程序所用端口号 （外部端口）的起始范围。必要时查看 Internet 应用程序的软件资料以获取更多信息。
   - 终止：指端口范围的结束。输入服务器或 Internet 应用程序所用端口号 （外部端口）的终止范围。必要时查看 Internet 应用程序的软件资料以获取更多信息。
   - 协议：选择用于此应用的协议， TCP、 UDP 或两者都选。
   - IP 地址：对于每一种应用，输入运行该特定应用的 PC 的 IP 地址。
3. 点击 “启用”复选框，启用端口转发策略。
4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

端口触发

“端口触发”用于外发端口与输入端口不相同的特殊 Internet 应用程序。启用此功能时，NAV10V2-WF 网关将监视特定端口号的外发数据。NAV10V2-WF 网关会记住发送传输请求数据的 PC （LAN 侧）的 IP 地址，所以当被请求数据经 NAV10V2-WF 网关 （从 WAN 侧）返回时，数据借助于 IP 地址和端口映像规则被转发到正确的 PC。

1. 选择 “配置”-〉“NAT”-〉“NAT”-〉“端口触发”，打开端口触发设置界面。
2. 添加或删除端口触发策略：
   - 应用程序：在此栏中输入您为该应用程序起的名字。每个名字最多为 12 个字符。
   - 触发范围开始端口 / 终止端口：为每个应用程序列出触发端口号范围。外发通信将使用这些端口。所需的端口号请查看该 Internet 应用程序的文件。在第一栏中输入 “触发范围”的开始端口号，在第二栏中输入 “触发范围”的终止端口号。
   - 转发范围：为每个应用程序列出被转发的端口号范围。输入通信将使用这些端口。所需的端口号请查看该 Internet 应用程序的文件。在第一栏中输入 “转发范围”的开始端口号，在第二栏中输入 “转发范围”的终止端口号。
   - 协议：输入该应用程序所用的协议， TCP、 UDP 或两者都选。
3. 选择 “已启用”选项，可启用表格中特定项的端口触发。
4. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

虚拟服务器

虚拟服务器界面允许将一台本地电脑暴露到 Internet，以便使用特殊用途服务 （如通过 “虚拟服务器”的 Internet 游戏和视频会议）。虽然 “端口转发”最多只能转发 15 个端口范围，但虚拟主机可在同一时间转发一台电脑的所有端口。

1. 选择 “配置”-〉“NAT”-〉“NAT”-〉“虚拟服务器”，打开虚拟服务器设置界面。
2. 启用或停用虚拟服务器：启用虚拟服务器，允许将一台本地电脑暴露到 Internet，以便使用如 Internet 游戏和视频会议之类的特殊用途服务。要使用此特性，请选择 已启用 。
3. 虚拟服务器主机 IP 地址：要暴露某台电脑，请输入该电脑的 IP 地址。
4. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

私有地址域名绑定

用户可设定内部网络地址和 DMZ 中服务器域名的映射关系，以便局域网内的 PC 可以通过在浏览器内键入域名来访问 DMZ 中服务器上的网站。(注：最大限制 20 笔)

当设定私有地址绑定域名时， WAN 需要有 DNS 服务器信息才会发生作用。

1. 选择 “配置”-〉“NAT”-〉“NAT”-〉“私有地址域名绑定”，打开私有地址域名绑定设置界面。
2. 输入私有地址及其绑定的域名地址，点击 “添加列表”按钮，添加域名绑定规则。
3. 选择某一域名绑定规则，然后点击 “删除选择的范围”按钮，删除域名绑定规则。
4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

NAT 连线控制

1. 选择 “配置”-〉“NAT”-〉“NAT”-〉“NAT 连线控制”，打开 NAT 连线控制设置界面。
2. 设置以下选项：
   - NAT 连线数目：显示当前 NAV10V2-WF 网关的 NAT 连接数量。
   - 清除 NAT 连线：清除 NAV10V2-WF 网关当前的 NAT 连接，并重新计算 NAV10V2-WF 网关的 NAT 连接数量。
   - 设定最大 NAT 连线数目: 设定 NAV10V2-WF 网关最多可支持的 NAT 连接数量。
   - 设定 TCP 超时：输入 TCP 超时数值。
   - 设定 UDP 超时：输入 UDP 超时数值。
3. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

编辑 NAT 设置

在 “编辑 NAT 设置”页面，可以查看 NAV10V2-WF 网关的 NAT 设置，点击 “编辑”按钮，可返回到对应的 NAT 设置项，修改该 NAT 设置项的配置。

入侵防御 （仅 NAV10V2-WF-ADVSEC 支持）

IPS 设置

1. 选择 “配置” -〉“入侵检测” -〉“IPS” -〉“IPS 设置”，打开 IPS 设置界面。

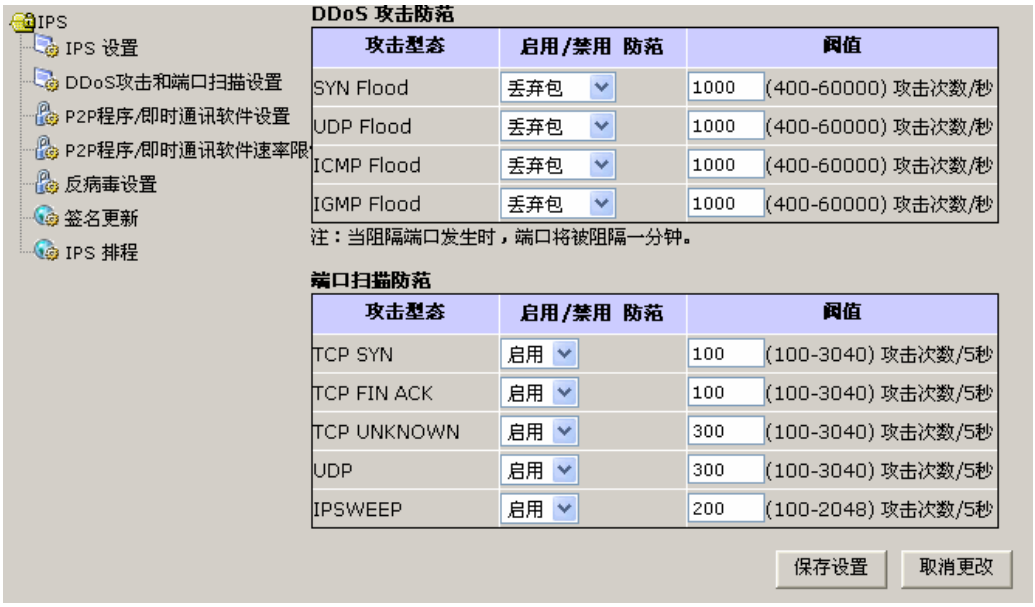
2. 启用或停用 IPS 功能切换。当 IPS 启用时，所有的 WAN/LAN 都将受到保护而免于遭受来自 WAN 端的攻击，用户可以通过设定 “是否检测该 VLAN” 选项以避免遭受来自 LAN 端的攻击。
3. TCP Reset：TCP 重置，当侦测到 TCP 的攻击 (须完成三次握手) 时， IPS 将会对攻击端以及被攻击端发出 TCP 重置包，藉以切断已经建立起来的连接。
4. 是否检测该 VLAN：
   - 检测：IPS 将会侦测来自这个 VLAN 的包。
   - 不检测：IPS 将不会侦测来自这个 VLAN 的包。
5. 协议异常检测：依据 RFC 的规范对 HTTP、 FTP、 TELNET 以及 RPC 的包进行检测。

6. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

DDos 攻击和端口扫描设置

分别定义 DDos 攻击和端口扫描等攻击的防范措施。

1. 选择 “配置” -〉“入侵检测” -〉“IPS” -〉“DDoS 攻击和端口扫描设置”，打开 DDoS 攻击和端口扫描设置界面。



2. DDoS 攻击防范：NAV10V2-WF 网关支持四种 DDoS 攻击的防范措施，包括 SYN Flood、UDP Flood、ICMP Flood、IGMP Flood 四种 DDoS 攻击防范。用户如启用 DDoS 攻击防范，须定义防范措施类型并设定触发的阈值数。当用户选择阻隔端口来防范 DDoS 攻击，被攻击的端口将被阻隔一分钟。

3. 端口扫描防范：NAV10V2-WF 网关支持五种端口扫描防范措施，包括 TCP SYN、TCP FIN ACK、 TCP UNKNOWN、 UDP 和 IPSWEEP 等。用户可选择启用或停用端口扫描防范，如果选择启用，须定义端口扫描防范触发的阈值数。

4. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

P2P 程序 / 即时通讯软件设置

本选项支持用户通过 NAV10V2-WF 网关阻隔某些 P2P 程序或即时通讯软件。请注意，此功能必须在 P2P/IM 软件登入之前开启，否则将无法有效的进行阻挡。

注意 如果用户启用了 “IPS 排程” 功能时，那么 NAV10V2-WF 网关将优先支持 IPS 排程设置，而忽略此处定义的 P2P/ 即时通讯软件设置。

1. 选择 “配置” -〉“入侵检测” -〉“IPS” -〉“P2P 程序 / 即时通讯软件设置”，打开 P2P/ 即时通讯软件设置界面。
2. NAV10V2-WF 网关支持的即时通讯软件设置 /P2P 程序：
   - 即时通讯软件：
     - MSN 2009 (14.0.8064.206)
     - ICQ 6.5 build:1042
     - YAHOO_Messenger 9.0.0.2162
     - SKYPE 3.8.180
     - IRC 6.35
     - ODIGO 4.0 689
     - REDIFF 8.0 build 315
     - GOOGLE_TALK 1.0.0.105
     - IM_QQ 2009 正式版 SP3 (1025)
   - P2P 程序：
     - GNUTELLA _EZPEER 2.0.0.20
     - FASTTRACK iMesh 9.1
     - eMule/eDonkey2000 0.49c
     - BITTORRENT 6.2 Build 15918
     - DIRECTCONNECT DC++ 0.75
     - PIGO 3.0
     - WINMX 3.54 beta 4
     - PPLIVE 2.3.1
     - PPSTREAM 2.6.86.8800
     - Thunder 5.9.6.1018

- QQLive 2009 Beta 3

3. 请为每一个 P2P 程序或即时通讯软件设置动作：
   - 不阻隔：应用程序能够正常通过 NAV10V2-WF 网关进行通信。
   - 阻隔：应用程序将被 NAV10V2-WF 网关阻隔。
   - 速率限制：NAV10V2-WF 网关将对该应用程序的速率进行限制。如果选择速率限制，用户需要在 “**P2P??/????????????**”中对其速率进行设置。
4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

P2P 程序 / 即时通讯软件速率限制设置

如果用户在 “**P2P** 程序 **/** 即时通讯软件设置”中将 P2P 程序或即时通讯软件的动作定义为速率限制，那么可通过此界面定义其速率限制的具体参数。

1. 要使用此功能，必须先启用 QoS。选择 “设置” -〉“服务质量” -> “带宽控制 & 出口队列”，启用 QoS 并设置相关参数。
2. 选择 “设置” -〉“入侵防御” -> “IPS” -〉“P2P 程序 / 即时通讯软件速率限制设置”，打开 P2P 程序 / 即时通讯软件速率限制设置界面。
   - P2P 程序 / 即时通讯软件：选择要限制速率的 P2P 程序 / 即时通讯软件。
   - 限制范围：设置限制范围 （单一 IP 或某一网段）
   - 单一 IP/ 网段：定义单一 IP 或网段。
   - 上行速率限制：限制上行速率。
   - 下行速率限制：限制下行速率。
3. 设置好以上参数后，点击 “更新”按钮，更新到状态列表中。用户也可以点击状态列表中的 “编辑”按钮，修改速率限制策略，或点击 “删除”按钮，删除选择的速率限制策略。
4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

反病毒设置

反病毒功能支持五种通讯协议的病毒扫描，分别为 HTTP、FTP、POP3、SMTP 以及 IMAP。当侦测到病毒时会依据您在动作栏位的设置进行阻挡或破坏。您可以指定最大扫瞄文件大小，当要侦测的文件超过您设置的大小时，反病毒功能将会不予以侦测而直接略过这个文件。

注释 反病毒功能只会针对 FTP 以及 HTTP 的下载资料作侦测的动作，并不支持 FTP 以及 HTTP 的上传资料侦测。

注意 反病毒功能只支持一层的压缩文件病毒扫描。

1. 选择 “设置” -〉“入侵防御” -> “IPS” -〉“反病毒设置”，打开反病毒设置界面。

2. 从 “Anti Virus 功能状态”下拉框中选择启用或停用，启用或停用反病毒功能。
3. 选择需要做病毒监控的协议，包括 HTTP、 FTP、 POP3、 SMTP 和 IMAP 等协议。
4. 选择检测到病毒时执行的动作。
   - 日志：将侦测到的病毒事件写入系统日志。
   - 销毁：当侦测到病毒时，破坏该病毒文件使其无法正常使用。

- 阻挡：当侦测到病毒时，阻断与该病毒有关的连线。

5. 定义最大扫描文件的大小，限制大小为 64KB 以上，设为 0 表示无上限。当正在扫毒中的文件大小超过此设定值时，反病毒功能将会略过此文件中超出设定值的剩余部分。
6. 设置白名单：设置寄件人或者是收件人的 email 地址。当要侦测的 email 中的寄件人或者是收件人栏位包含了您在白名单中所设置的 email 地址时，反病毒功能将会略过此 email 而不予侦测。
7. 完成对此界面的更改后，点击 “保存设置”按钮保存所做的修改，或点击 “取消更改”按钮撤消所做的修改。

签名更新

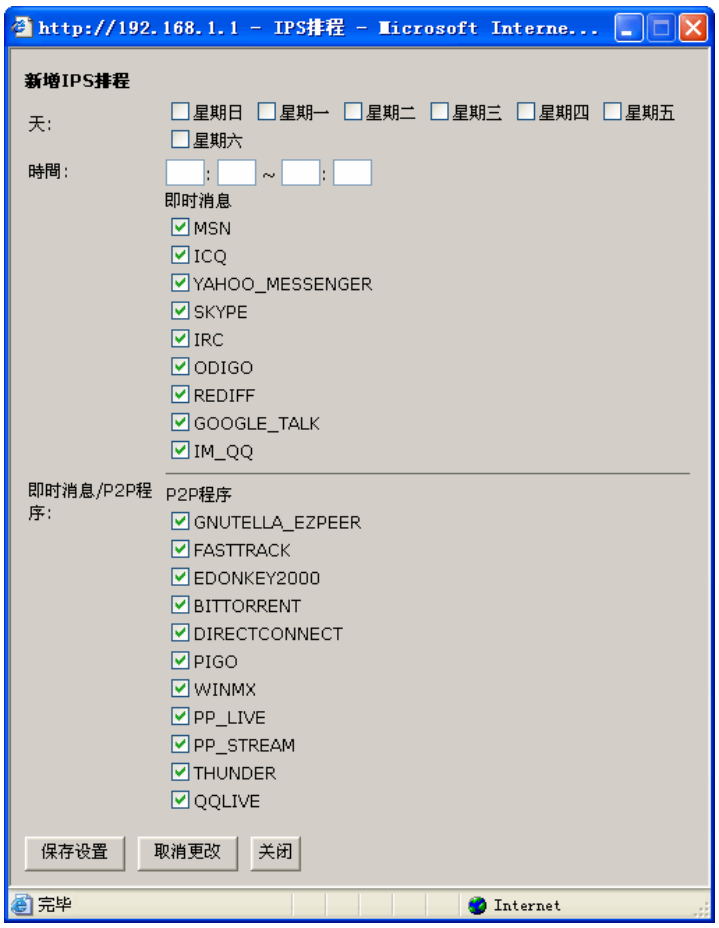
设置更新病毒档的方式，您可以选择手动更新或者是定时自动更新。您也可以更改服务器的 IP 地址。如需更新病毒库签名，用户首先必须订阅 IPS/AV 服务。

1. 要更新签名，首先要启用 IPS 功能。选择 “配置” -〉“入侵检测” -〉“IPS” -〉“IPS 设置”，启用 IPS 切换功能，并设置相关参数。
2. 订阅 IPS/AV 服务。一旦您订阅了 IPS/AV 服务，您将获得病毒库更新服务器的 IP 地址等信息。
3. 选择 “配置” -〉“入侵检测” -〉“IPS” -〉“签名更新”，打开签名更新设置界面。
4. 输入签名更新服务器的 IP 地址，选择更新间隔周期， NAV10V2-WF 网关将自动按期更新病毒库。如果选择手动，点击 “更新”按钮，手动更新病毒库。
5. 查看签名状态，包括当前签名版本、最近更新时间 （最近成功更新的时间）以及更新状态。
6. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

IPS 排程

设置排程中支持的即时通讯软件设置和 P2P 程序。

1. 选择 “配置” -〉“入侵检测” -〉“IPS” -〉“IPS 排程”，打开 IPS 排程设置界面。
2. 点击 “添加”按钮，新增 IPS 排程设置。



3. 分别设置天、时间和即时通讯软件或 P2P 程序。
4. 点击 “保存设置”，保存所作的修改。
5. 从 IPS 排程列表中选择一条策略，点击 “启用”，可启用该策略；点击 “停用”，可停用该策略。
6. 点击 “编辑”，编辑 IPS 排程。点击 “删除”，删除已有 IPS 排程。
7. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

服务质量

服务质量 (Quality of Service， QoS) 是一种在 NAV10V2-WF 网关出口壅塞时，可以让使用者决定何种类型的流量得以以较高的优先权使用有限的带宽。

“服务质量”任务栏将引导用户为 WAN 接口的出局通信设置基本的服务质量策略。QoS 设置将与其关联类别建立第延迟 （LLQ）服务策略，通过在 WAN 端分配带宽比例以及为组成类别所指定的带宽来建立该服务策略。新建立的服务策略将与您选择的 WAN 接口发生关联。

注意　当 QoS 与 VPN 服务同时启用时， QoS 设置不会在 VPN 服务上生效。

带宽控制 & 出口队列

1. 选择 “配置” -〉“服务质量” -〉“QoS” -〉“带宽控制 & 出口队列”，打开带宽控制 & 出口队列设置界面：

2. QoS 设置：

- QoS：启用或禁用 QoS 功能。如果启用 QoS 功能，因为 QoS 预设允许的突发流量峰值为 100000 kbps，请将 ISP 所提供的上行带宽设定值指定到 NAV10V2-WF 网关对应的 WAN 接口。
- 基于端口：启用或禁用基于端口的 QoS 策略类型。
- 基于主机：启用或禁用基于主机的 QoS 策略类型。
- 基于应用程序：启用或禁用基于应用程序的 QoS 策略类型。

注意 以上三种 QoS 策略类型不能同时启用 2 个或 2 个以上。被禁用的 QoS 策略类型将无法设置其通信规则。

3. 带宽基础设置：
   - 带宽基础：当用户启用了 QoS 功能后，可启用或停用带宽控制功能。
   - 上行带宽：针对两个不同的出口设立上行带宽，从设置的出口出去的总流量不得超出此设置值。
   - 允许的突发流量峰值：最多能积累的突发频宽，当设立此值太小会造成大报文无法送出，使出口停止传送报文。而此值太大，会造成突发流量瞬间使用过多频宽。
4. 出口队列设置：出口队列支持以下不同策略：
   - SP (Strict Priority)：高权重优先法则，当有两种不同类别的流量要竞争出口时，一律由高优先权 的流量优先使用，低优先权的流量要一直等到高优先权不使用出口频宽时才可使用。
   - WRR (Weighted Round-Robin)：以使用者定义的权重比来分享频宽。
   - LLQ (Low latency Queuing)：（最高的）和 （高、中、低）成为两个 SP 群组，当最高的需要使用频宽时，一律由 （最高的）优先，其余的才由 （高、中、低）依比例分享。最高的流量必须设置频宽限制，最高的流量不得超过此频宽限制。

注意 当 WAN0 或 WAN1 接口的 Internet 连接类型被设为 PPTP 或 L2TP 时， WAN 接口的出口队列设置组策略仅支持 SP 功能。

5. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

通信规则

使用者可以以不同的方式将报文分类，目前支持以下三种分类方式：

1. 以端口来源为分类法则。
2. 以报文所带的来源 IP、目标 IP、来源端口、目地端口、来源虚拟区域网络、来源物理装置任选一种或多种来分类。

3. 以主机硬件位置或网际网络位置来分类。

分类完成后，使用者可利用出口队列功能来决定当出口壅塞时，如何对待各种不同类别的报文。

服务质量会一直以使用者所设置的出口队列策略来对待各种不同类别的报文，但若出口不壅塞时或壅塞不是发生在本 NAV10V2-WF 网关出口时，可能不会在流量上有所区别，而是每个不同类别的流量皆能满足其带宽需求或每个不同类别的流量皆壅塞在其它壅塞的出口。

基于端口

1. 选择“配置”-〉“服务质量”-〉“QoS”-〉“通信规则”-〉“基于端口”，打开基于端口的通信规则设置界面。
2. 以端口来源为分类法则，包含以下子项目：
   - 信任：选择信任或不信任端口流量。
   - 修改 DSCP：分类之后，以流量类别为基础修改 IP 报文的 DSCP 值，此功能通常作为 diff serv 的 marking 之用，修改的动作包含被信任的报文及不信任的报文。
     - 最高 DSCP=0xc0
     - 高 DSCP=0x80
     - 中 DSCP=0x40
     - 低 DSCP=0x00
     - 若选择不修改，则 DSCP 不会作任何更动。
   - 流量类别：若不信任或选为信任但报文未带 QoS 信息，则强制指定为此流量类别。
3. 请按照上述说明修改这些设置，然后点击“保存设置”使修改生效，或点击“取消更改”放弃所做的修改。

基于主机

1. 选择“配置”-〉“服务质量”-〉“QoS”-〉“通信规则”-〉“基于主机”，打开基于主机的通信规则设置界面。
2. 根据主机的硬件地址或来源 IP 决定流量类别及流量限制。
   - MAC 地址：主机的 MAC 地址
   - 来源 IP：来源 IP 地址

- 流量限制：启用或禁用流量限制功能，如果启用，需设定流量限制的值。设为“0”表示无限制 。
- 流量类别：选择流量类别，分别为低、中、高和最高四种流量类别可选。

3. 请按照上述说明修改这些设置，然后点击“保存设置”使修改生效，或点击“取消更改”放弃所做的修改。

基于应用程序

根据报文的来源 IP、目标 IP、来源端口、目地端口、来源虚拟区域网络、来源物理装置任选一种或多种来分类报文。

1. 选择“配置”-〉“服务质量”-〉“QoS”-〉“通信规则”-〉“基于应用程序”，打开基于应用程序的通信规则设置界面。
2. 分别设置以下参数：
   - 服务：从下拉框中选择应用程序服务。点击“服务管理”可增加、修改和删除服务列表中的服务。
   - 来源接口：选择应用程序服务对应的来源接口，一般不作限制。
   - 来源 IP：选择应用程序服务对应的来源 IP 地址，可为单个 IP 或某一网段，也可以不限制。
   - 目标 IP：选择应用程序服务对应的目标 IP 地址，可为单个 IP 或某一网段，也可以不限制。
   - 流量类别：选择流量类别，分别为低、中、高和最高四种流量类别可选。
   - 修改 DSCP：启用或禁用 DSCP 功能。分类之后，以流量类别为基础修改 IP 报文的 DSCP 值，此功能通常作为 diff serv 的 marking 之用，修改的动作包含被信任的报文及不信任的报文。
   - 流量限制：启用或禁用流量限制功能，如果启用，需设定流量限制的值。当上行或下行值为 “0”时代表无限制
3. 请按照上述说明修改这些设置，然后点击“保存设置”使修改生效，或点击“取消更改”放弃所做的修改。

编辑 **QoS** 策略

编辑 QoS 策略任务栏可查看、编辑定义好的带宽控制策略、基于端口、基于主机和基于应用程序的通行规则等信息。

- 编辑：点击“编辑”按钮，可修改带宽控制和通信规则等设置。

- 恢复默认值：点击 “恢复默认值” 按钮，恢复到 NAV10V2-WF 网关的默认设置。
- 删除：点击 “删除” 按钮，删除定义好的通信规则。

请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

其他任务

此选项卡包含 NAV10V2-WF 网关的其他配置，包括设备名、日期 / 时间、 SNMP、UPnP 等等。

设备属性

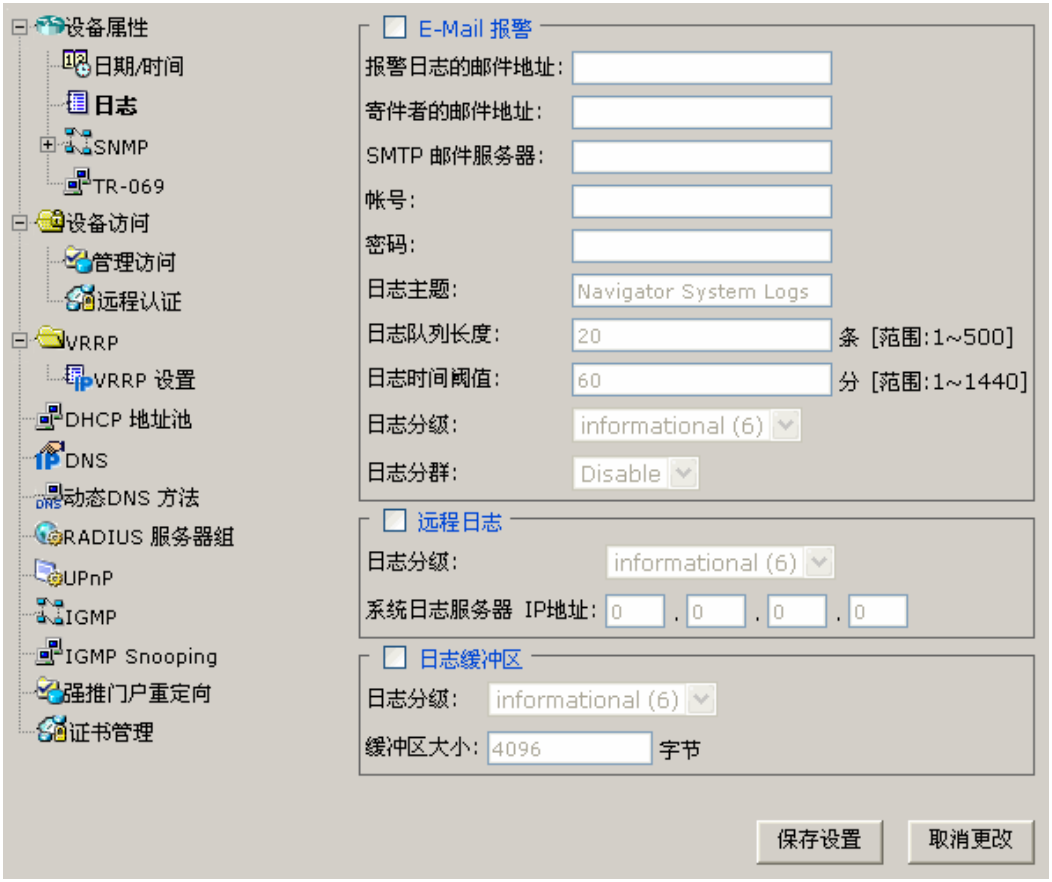
1. 选择 “配置” -〉“其他任务” -〉“设备属性”，打开设备属性设置界面。用户可分别设置日期 / 时间、日志、 SNMP 和 TR-069 等选项。
2. 点击界面右侧的 “编辑” 按钮为此 NAV10V2-WF 网关配置 “主机名” 和 “域名”。用户如果需要使用动态 DNS 功能，需要修改主机名和域名。

日期 / 时间

1. 点击 “日期 / 时间”，可以手动定义或通过 “时间服务器” 自动定义 NAV10V2-WF 网关的时间。默认为自动。
   - 手动：如果希望手动输入时间和日期，请从下拉列表中选择日期并以 24 小时格式在 “时间” 栏内输入小时、分钟和秒 （如晚上 10:00 应输入为 22:00:00）。
   - 自动：
     - 时区：选择时区，利用公共 NTP （网络时间协议）服务器使您的位置和设置利用 Internet 同步。
     - 用户指定的 NTP 服务器: 如果要使用您自己的 NTP 服务器，请选择已启用选项。默认为已停用 。
     - NTP 服务器 IP：输入您自己的 NTP 服务器的 IP 地址。
     - 当前时间：显示手动或自动设置的此 NAV10V2-WF 网关的当前时间。
2. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

日志

1. 点击 “日志”，可以配置日志设置以及特定事件的报警。日志事件可发送到 email 地址、远程系统日志服务器，或两种报警方式都选用。



2. Email 报警：如果希望 NAV10V2-WF 网关在发生确凿攻击时发送 E-mail 报警，请选择已启用。默认设置为已停用 。
   - 报警日志的邮件地址：输入接收日志的邮件地址。
   - 寄件人的邮件地址：输入发件人的邮件地址。
   - SMTP 邮件服务器：输入 SMTP 邮件服务器地址。
   - 帐号：输入 SMTP 邮件服务器帐号。
   - 密码：输入 SMTP 邮件服务器密码。
   - 日志主题：输入日志的主题信息。

- 日志队列长度：可以指定所发送日志的最大长度。默认设置为 20 条，因此在时间阈值到达之前，一旦日志事件达到 20 条，您就会收到一封邮件。
- 日志时间阈值：可以指定发送日志的最大时间间隔，默认为 60 分钟，因此每 60 分钟 （日志中至少有一次事件）您就会收到一封邮件。
- 日志分级：寄送日志内容之级别筛选。
- 日志分群：将内容相似的日志群整合成单一日志。

3. 远程日志：系统日志是一种用来捕获网络活动相关信息的标准协议。 NAV10V2-WF 网关支持此协议，可将其活动日志发送到外部服务器。要启用远程日志，请选中远程日志复选框。
   - 日志分级：选择要发送到远程系统日志服务器的消息类型。
   - 系统日志服务器 IP 地址：输入远程系统日志服务器的 IP 地址。
4. 日志缓冲区：NAV10V2-WF 网关支持对日志缓冲区的大小进行更改。要启用日志缓冲区，请选中日志缓冲区复选框。
   - 日志级别：选择要发送到远程系统日志服务器的消息类型。
   - 缓冲区大小：输入日志缓冲区的字节数。默认为 4096 字节。
5. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

SNMP

SNMP 是一种流行的网络监控和管理协议。它使网络管理员能够对 NAV10V2-WF 网关的状态进行监控，并在 NAV10V2-WF 网关发生任何重大事件时收到通知。

1. 点击 “SNMP”，打开 SNMP 设置界面。

2. 要启用 SNMP 支持特性，请选择已启用。反之选择已停用 。默认设置为已停用 。
3. 选择 SNMP 版本：NAV10V2-WF 网关支持 SNMP 版本 1、 2 和版本 3。如果不需要版本 3 的增强能力，或者您的管理软件不支持版本 3，请选择 SNMP V1 & V2 ；反之选择 SNMP V3。
4. 设置以下基本参数：
   - 联系人：输入 NAV10V2-WF 网关的联系人的姓名，如网络管理员。
   - 设备名：输入您为 NAV10V2-WF 网关所指定的名称。
   - 位置：输入 NAV10V2-WF 网关的位置。
   - 安全用户名：仅对于 SNMPv3。创建访问和管理 SNMP MIB 对象的管理员帐户。
   - 认证密码：仅对于 SNMPv3。输入管理员帐户的验证密码 （最小长度 8）。
   - 加密密码：仅对于 SNMPv3。输入管理员管理通信时进行数据加密的专用密码（最小长度为 8）。

- SNMP Engine ID：仅对于 SNMPv3。仅限于 MG-SOFT Mib Browser 客户端工具，当发生 usmStatsUnknownEngineIDs 情况时输入访问 NAV10V2-WF 网关 SNMP 实体的 Engine ID。用作两个 SNMP 实体间的唯一标识，以调整请求和响应信息。
- SNMP 只读口令：输入能够以只读方式访问 NAV10V2-WF 网关 SNMP 信息的密码。默认为 public。
- SNMP 读写口令：输入能够以读/写方式访问 NAV10V2-WF 网关 SNMP 信息的密码。默认为 private。
- Trap 口令：输入远程主机接收 NAV10V2-WF 网关所发出的陷阱消息或通知时所需的密码。
- SNMP 信任主机：可通过 IP 地址来限制对 NAV10V2-WF 网关的 SNMP 信息进行访问。在相应栏中输入
- IP 地址，如果此栏留空，则允许从任何 IP 地址访问此信息。
- Trap 接收主机：输入接收陷阱消息的远程主机的 IP 地址。

5. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

TRAP 告警要求

TRAP 告警要求主要应用于侦测 CPU 以及内存目前的使用率，当 SNMP 启动时，每五分钟便会侦测一次 CPU 与内存使用状况，若 CPU 使用率超出 CPU 超阈值设定时或内存使用率超出内存超阈值设定时，会触发 TRAP 的发送。

预设的 CPU 与内存超阈值皆是 80%，管理者在 SNMP 启动后可以由此页面设定超阈值的数值。

1. 在 SNMP 设置里定义 Trap 口令和 Trap 接收主机后，用户可启用或停用 TRAP 告警要求设置。
2. 点击 “TRAP 告警要求”，打开 TRAP 告警要求设置界面。
   - CPU 超阈值：定义当 CPU 使用率超过一定比例，系统发出 TRAP 告警。
   - CPU 超阈值：定义当内存使用率超过一定比例，系统发出 TRAP 告警。

注释 用户必须先设置好 “TRAP 口令” 和 “TRAP 接收主机” 才能使用 “Trap 告警要求” 功能。

3. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

TR-069

CPE 广域网管理协议，它提供了对下一代网络中家庭网络设备进行管理配置的通用框架和协议，用于从网络侧对家庭网络中的网关、路由器、机顶盒等设备进行远程集中管理。

1. 点击 “TR-069”，打开 TR069 设置界面。
2. 启用或停用 TR-069。
3. 指定侦测模式：可手动选择侦测端口，或自动选择侦测端口。如果用户启用了子接口功能，也可以将子接口作为侦测端口。
4. 设置以下参数：
   - ACS URL：设置 ACS 服务器的 URL 位置。
   - 用户名：登录 ACS 服务器 的用户名。
   - 密码：登录 ACS 服务器 的密码。
   - 确认密码：确认输入的密码。
   - 连接请求用户：用于验证 ACS 的使用者名称向 CPE 做出连接要求。
   - 连接请求密码：用于验证 ACS 的密码向 CPE 做出连接要求，除非读取正确值，否则参数返回空白串。
   - 确认连接请求密码：确认输入的连接请求密码。
5. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

设备访问

设备访问任务栏可通过建立用户帐号来控制对 NAV10V2-WF 网关进行访问，包括配置管理访问策略，指定可以用来连接到 NAV10V2-WF 网关的协议以及用来对其进行管理的主机。

管理访问

配置用户帐户，以指定哪些用户可以访问路由器。建立控制访问网络由器和协议基础的策略。可以定义能够对 NAV10V2-WF 网关进行管理的主机，指定用来管理 NAV10V2-WF 网关的协议以及指定可以管理 NAV10V2-WF 网关的接口等。

1. 选择 “配置” -〉“其他任务” -〉“设备访问” -〉“管理访问”，打开管理访问界面。

2. 管理员密码：为了确保 NAV10V2-WF 网关的安全，访问 NAV10V2-WF 网关的 Web 配置界面时将要求您输入密码。 NAV10V2-WF 网关默认的管理员账号为 telecomadmin，默认密码为 nE7jA%5m。

   - 管理员密码：NAV10V2-WF 网关默认的密码为 nE7jA%5m。如需将默认密码修改为其他密码，请在此处输入新的管理员密码。
   - 确认管理员密码：再次输入管理员账号的新密码进行确认。
   - Guest 密码：NAV10V2-WF 网关默认的 Guest 账号为 useradmin，默认密码为 admin!@#$%^。如需修改 Guest 账号的默认密码，请在此处输入 Guest 账号的新密码。
   - 确认 Guest 密码：再次输入 Guest 账号的新密码进行确认。

3. 本地管理：用户可以定义从 LAN 侧 （或通过无线 LAN）管理 NAV10V2-WF 网关的方法。

   - 使用 HTTPS：HTTPS 使用 SSL 加密来增加访问 Web 管理界面时的安全性。启用 HTTPS 后，对 NAV10V2-WF 网关 LAN IP 的 http 请求将被复位向到 HTTPS。默认设置为已停用 。
   - 允许无线 WEB 访问：允许或拒绝无线客户端访问 web 管理界面。默认设置为已停用 。

4. 远程管理 （通过 WAN 端登录）：用户可以定义从 WAN 侧 （通常为 Internet）管理 NAV10V2-WF 网关的方法。出于安全原因通常停用此项。

   - 远程管理：此特性允许您从 WAN 侧管理 NAV10V2-WF 网关，通常为通过 Internet 访问 WAN 端口的 IP 地址进行管理。要启用 “远程管理”，请点击 “已启用”按钮。启用远程管理之前需要更改默认的管理员密码。
   - 使用 HTTPS：要将 SSL 加密用于 HTTP 会话，请选择 “已启用”。
   - 使用 SNMP：使用 SNMP 管理 NAV10V2-WF 网关，请选择 “已启用”。
   - 远程更新：如果希望能够从 WAN 端对 NAV10V2-WF 网关的固件进行升级，请选择 “已启用”（此操作必须首先启用 “远程管理”功能），反之则保持默认设置 “已停用”。
   - 允许的远程 IP 地址：如果希望能够从任何外部 IP 地址访问 NAV10V2-WF 网关，请选择 “任何 IP 地址”。如果希望指定外部 IP 地址或 IP 地址范围，则选择第二个选项并填写相应的 IP 地址或 IP 范围。
   - 远程管理端口：输入外部访问的端口号，默认设置为 8080。

5. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

远程认证

用户可通过 Radius 服务器进行远程认证来登录设备。

1. 选择 “配置” -〉“其他任务” -〉“设备访问” -〉“远程认证”，打开远程认证设置界面。
2. 启用或停用远程认证服务。
3. 如果启用远程认证服务，用户还需要设置 RADIUS 服务器参数：
   - RADIUS 服务器 IP：RADIUS 服务器 IP。
   - RADIUS 服务器端口：RADIUS 服务器端口。
   - 认证密钥：认证密钥。
4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

VRRP 设置

NAV10V2-WF 网关支持 VRRP 容错协议， VRRP (Virtual Router Redundancy Protocol) 是一种 LAN 接入设备容错协议， VRRP 将局域网的一组路由器 （包括一个 Master 即活动路由器和若干个 Backup 即备份路由器）组织成一个虚拟路由器。

1. 选择 “配置” -〉“其他任务” -〉“VRRP” -〉“VRRP 设置”，打开 VRRP 设置界面。
2. 启用或停用 VRRP：点击 “启用”可启用此特性，点击 “停用”可停用此特性。
3. 一旦启用 VRRP，请设置以下参数：
   - 虚拟路由器代号 (VRID)：定义备份路由器 ID 路由器备份角色。
   - 优先数：定义路由器优先数备份角色。
   - 通告间隔时间：定义备份路由器广告通告间隔时间。
   - 验证：定义路由器之间验证方式与密码。
   - 虚拟 IP 地址：定义备份路由器共同维护之虚拟 IP 地址。
4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

DHCP 地址池

用户可以查看 DHCP 地址池的状态和详细信息。

1. 选择 “配置” -〉“其他任务” -〉“DHCP 地址池”。
2. 点击 DHCP 地址池列表中的地址池记录，在下方可查看该地址池的详细信息，包括：
   - DHCP 模式：启用 / 未启用。
   - DHCP 地址池范围：显示 DHCP 地址池的起始 IP 和终止 IP。
   - 默认路由器 IP 地址：向外网发送数据包的主机 IP 地址。
   - 租用时间：定义所分配 IP 地址保持有效的时间。
   - DHCP 选项：对 DHCP 消息交换所用的一些可选条目进行定义。
   - DNS 服务器：即 “域名服务器”，可帮助主机将主机名解析到 IP 地址。
   - WINS 服务器：Windows Internet 命名服务器 （WINS）在 Windows 网络环境下履行名称解析功能 （类似于 DNS）。有助于通过计算机名来确定远程 Windows 电脑的 IP 地址。
   - 域名：所属单位的网络名称。
3. 点击 “地址池状态”，可查看其当前使用状态。

DNS

1. 选择 “配置” -〉“其他任务” -〉“DNS”，打开 DNS 设置界面。
2. 点击 “添加”按钮，可添加 DNS 服务器。
   - IP 地址：输入要用在 NAV10V2-WF 网关中上的 DNS IP 地址。
3. 点击 “启用”按钮，可启用 DNS 服务器。点击 “停用”按钮，可停用 DNS 服务器。
4. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

动态 DNS 方法

NAV10V2-WF 网关提供了一种 “动态域名系统”（DDNS）特性。 DDNS 可使您为动态 Internet 地址分配固定主机和域名。当您将自己的网站、 FTP 服务器或其他服务器的主机置于 NAV10V2-WF 网关之前时这会非常有用。

使用此特性之前，您需要在 PeanutHull、DynDNS.org 、 TZO.com 或 CTDDNS 服务提供商处注册 DDNS 服务。

1. 选择 “配置” -〉“其他任务” -〉“动态 DNS 方法”，打开动态 DNS 方法设置界面。
2. 点击 “添加”按钮，打开添加动态 DNS 方法界面。
3. 从下拉列表中选择 DNS 服务器，输入您注册的 DDNS 帐户的用户名和密码以激活该功能。
4. 从列表选择一条动态 DNS 方法，点击 “启用”按钮，启用该方法。
5. 在界面上会显示当前启用的动态 DNS 方法和更新状态，点击 “更新”可实时更新。
6. 启用并设置好动态 DNS 方法后，还要修改 NAV10V2-WF 网关的主机名和域名。主机名和域名分别您注册的用户名和所分配的域名。
7. 请按照上述说明修改这些设置，然后点击 “保存设置”使修改生效，或点击 “取消更改”放弃所做的修改。

RADIUS 服务器组

使用 RADIUS 服务器进行验证、授权请求，应在 NAV10V2-WF 网关上对 RADIUS 服务器进行配置， NAV10V2-WF 网关将依据 IP 地址和具体的 UDP 端口号对 RADIUS 服务器组进行识别。

出于安全通讯的目的，还可以在 NAV10V2-WF 网关和 RADIUS 服务器上配置共享文本 (密钥)。该密钥将被用来对 NAV10V2-WF 网关与 RADIUS 服务器组之间的通信进行加密。

1. 选择 “配置” -〉“其他任务” -〉“RADIUS 服务器组”，打开 RADIUS 服务器组设置界面。
2. 每个 RADIUS 服务器组都需要设置 2 个 RADIUS 服务器参数：
   - RADIUS 服务器 IP 地址：输入 RADIUS 服务器的 IP 地址。
   - RADIUS 服务器端口：输入 RADIUS 服务器正在使用的端口号。
   - 共享密钥：输入 NAV10V2-WF 网关和 RADIUS 服务器所用的共享密钥。
   - RADIUS 服务器组属性：表格中显示 RADIUS 服务器描述的摘要。
3. 点击 “添加”，添加到 RADIUS 服务器组表。
4. NAV10V2-WF 网关最多可支持 15 条 RADIUS 服务器组记录，用户可根据索引选择查看 RADIUS 服务器的属性。点击 “编辑”对描述进行修改，或点击 “删除”清除描述。

5. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

UPnP

1. 选择 “配置” -〉“其他任务” -〉“UPnP”，打开 UPnP 设置界面。
2. UPnP：点击 “启用” 可启用此特性，点击 “停用” 可停用此特性。
3. 允许用户配置：点击 “启用” 以允许用户使用 UPnP 更改配置。点击 “停用” 则不允许用户使用 UPnP 更改配置。
4. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

IGMP

1. 选择 “配置” -〉“其他任务” -〉“IGMP”，打开 IGMP 设置界面。
2. NAV10V2-WF 网关支持 IGMP 版本 V1/V2 和 V3。如果不需要 V3，请选择 IGMP V1/V2 ；反之选择 IGMP V3。
3. 选择 “启用”，启用 IGMP，反之选择 “停用”。默认设置为 “停用”。
4. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

IGMP Snooping

支持群播路由的路由器，会对其连接接口 (VLAN) 下面的所有端口进行 flooding 的传播。为了避免 Flooding 浪费网络带宽，使用 IGMP Snoopng 可抓取 IGMP 报文，来取得连接接口下的哪些端口需要群播资料，然后针对需要的端口来发送群播报文，而不是对接口下的所有端口进行发送。

1. 选择 “配置” -〉“其他任务” -〉“IGMP Snooping”，打开 IGMP Snooping 设置界面。
2. 选择 “启用”，启用 IGMP Snooping，反之选择 “停用”。默认设置为 “启用”。
3. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

强推门户重定向

1. 选择 “配置” -〉“其他任务” -〉“强推门户重定向”，打开强推门户重定向设置界面。
2. 启用或停用强推门户重定向：强推门户重定向功能可强迫用户在连上网络之前一定要先通过身份认证。当用户打开浏览器后连至任何一个网页时都会被重新导向至一个认证的网页。用户唯有通过身份认证后才可任意的上网。
3. 设置以下参数：
   - 监控的 HTTP 端口：设定欲监控的 HTTP 端口，默认值是 80 及 3128 端口。请务必确认所设定的端口为用户所使用的端口，否则将导致用户完全无法上网。
   - 允许直接访问的网站：允许用户连至特定的网站时不需事先经过认证，但此功能不支持透过用户透过 proxy 联机至因特网的联机方式。
   - 认证网页服务器：认证网页服务器的地址。
   - 认证网页服务器密码：NAV10V2-WF 网关与认证网页服务器之间数据传输需要用到的共享密码。
   - Radius 服务器：设定 Radius 服务器的 IP 地址。
   - Radius 服务器密码：NAV10V2-WF 网关与 Radius 服务器之间数据传输需要用到的共享密码。
   - Radius 服务器端口：设定 Radius 服务器端口，默认值是 1812 端口。
4. 请按照上述说明修改这些设置，然后点击 “保存设置” 使修改生效，或点击 “取消更改” 放弃所做的修改。

证书管理

1. 选择 “配置” -〉“其他任务” -〉“证书管理”，打开证书管理设置界面。
2. 目前 CA 证书：用户可查看、导入、删除和更新 CA 证书。
   a. 点击 “浏览” 按钮，选择要导入的 CA 证书。
   b. 点击 “更新” 按钮，将导入的 CA 证书更新为当前的 CA 证书。
   c. 更新完毕后，用户可查看 CA 证书的基本信息，包括名称、网域、组织名等信息。
   d. 点击 “删除” 按钮，可删除当前的 CA 证书。
3. 目前本机证书：用户可查看、导入、删除和更新本机证书。
   a. 点击 “浏览” 按钮，选择要导入的本机证书。

b. 点击 “更新” 按钮，将导入的本机证书更新为当前的本机证书。

c. 更新完毕后，用户可查看本机证书的基本信息，包括名称、网域、组织名等信息。

d. 点击 “删除” 按钮，可删除当前的本机证书。

4. 生成远程证书：用户可导入远程证书。

a. 点击 “浏览” 按钮，选择要导入的远程证书。

b. 点击 “载入” 按钮，导入远程证书。

5. 导入本机密钥：

a. 点击 “浏览” 按钮，选择要导入的本机密钥。

6. 点击 “更新” 按钮，更新本机的密钥文件。

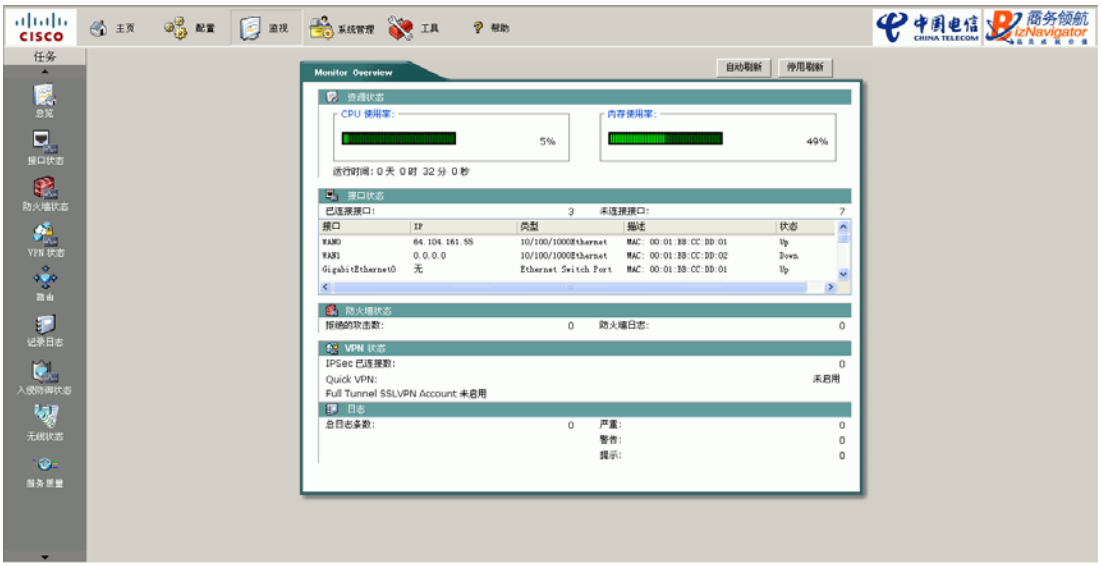
4

监视

监视任务栏显示有关 NAV10V2-WF 网关的系统状态、接口状态、防火墙状态、 VPN 状态、记录日志、无线状态等方面的信息。大多数 “监视”页面上的复位按钮主要用于故障检修和调试。

总览

显示 NAV10V2-WF 网关的各项监控状态的总览信息，包括：



- 资源状态：包括 CPU 使用率、内存使用率和运行时间。
- 接口状态：包括已连接 / 未连接的接口数，以及各个接口的基本信息（IP 地址、接口类型、描述和连接状态）。
- 防火墙状态：包括拒绝的攻击数、防火墙日志。
- VPN 状态：包括 IPSec 已连接数， Quick VPN Account 启用 / 未启用， Full Tunnel SSL VPN Account 启用 / 未启用。
- 日志：包括总日志条数、严重日志条数、警告日志条数和提示日志条数。

- 自动刷新：点击“自动刷新”，则每隔 60 秒钟刷新监视信息。
- 停用刷新：点击“停用刷新”，则停止监视信息刷新。

接口状态

接口状态栏分别显示各个接口的工作模式、速率、连接状态、收到和发送的数据包、收到和发送的字节、收到的错误包，丢失接收的包以及 bit/ 秒等信息。

- 自动刷新：点击“自动刷新”，则每隔 60 秒钟刷新接口信息。
- 停用刷新：点击“停用刷新”，则停止刷新接口信息。
- 复位：将当前接口的信息恢复到初始状态。
- 复位所有：将所有接口的信息恢复到初始状态。

防火墙状态

防火墙状态栏显示 NAV10V2-WF 网关的所有防火墙策略配置，用户可查看全部的防火墙策略，或分别查看出方向访问控制策略和入方向访问控制策略。如果防火墙策略较多，可跳转或修改每页显示的策略条数。

- 自动刷新：点击“自动刷新”，则每隔 60 秒钟刷新防火墙策略信息。
- 停用刷新：点击“停用刷新”，则停止刷新防火墙策略信息。
- 出方向访问控制：允许所有通信从任一 LAN 到任一 WAN。
- 入方向访问控制：拒绝所有通信从任一 WAN 到任一 LAN。

VPN 状态

如果 NAV10V2-WF 网关禁用了 VPN 功能， VPN 状态栏将显示 VPN 当前为禁用状态。如果 NAV10V2-WF 网关启用 VPN 功能，可监视站点到站点 VPN、 Quick VPN Account 和 Full Tunnel SSL VPN Account 的状态。

- 自动刷新：点击“自动刷新”，则每隔 60 秒钟刷新 VPN 信息。
- 停用刷新：点击“停用刷新”，则停止刷新 VPN 信息。
- 站点到站点 VPN：列出 NAV10V2-WF 网关创建的所有站点到站点 VPN 通道信息，包括策略名、接口、远程对端主机、本地网络的 IP 地址以及子网掩码，远程 IP 地址和子网掩码一级状态等信息。
- Quick VPN Account：显示 Quick VPN Account 及其状态。

- Full Tunnel SSL VPN Account：显示 Full Tunnel SSL VPN Account 及其状态。

路由状态

路由状态栏可查看 NAV10V2-WF 网关当前的路由表信息，路由信息包括目的地址、掩码、网关、标志、路径成本以及路由接口等。

- 自动刷新：点击“自动刷新”，则每隔 60 秒钟刷新路由表信息。
- 停用刷新：点击“停用刷新”，则停止刷新路由表信息。

记录日志

如果您未启用日志功能（“配置” -> “其他任务” -> “设备属性” -> “日志”），记录日志栏将显示“系统日志服务状态为停用”。如果您启用了日志功能，记录日志栏将显示所有被记录的系统日志信息。

系统日志显示日志等级、日志记录的事件发生时间和日志详细信息等。

- 系统日志服务状态：启用或未启用。
- 选择备份日期：选择查看某一日期内的全部日志信息。
- 自动刷新：点击“自动刷新”，则每隔 60 秒钟刷新系统日志信息。
- 停用刷新：点击“停用刷新”，则停止刷新系统日志信息。
- 储存日志：点击“储存日志”，所有系统日志内容被保存到名为 syslog[x].txt 的文件内，您也可以选择将该日志文件保存到本地（“文件” -> “另存为”）。
- 删除选取备份日志：从日志列表中选择一条日志，点击该按钮删除。
- 删除全部日志：点击该按钮删除当前全部的系统日志信息。

入侵防御状态

仅高级安全型号的 NAV10V2-WF 网关（型号名 NAV10V2-WF-ADVSEC）支持入侵防护功能监视功能。

查看入侵防御报告

如果您启用了入侵防御相关功能（“配置” -> “入侵防御” -> “IPS” -> “IPS 设置”）和反病毒功能（“配置” -> “入侵防御” -> “IPS” -> “反病毒设置”），入侵防御栏将显示最近 24 小时的流量和事件分析图表，以及各个接口的前 5 位攻击和前 10 位攻击事件的类型以及 IPS 阻绝端口等信息。用户也可以查看入侵防御的原始数据。

注意　须先启用日志缓冲区功能，才能监视入侵防御状态。

1. 打开 “监视” -> “入侵防御状态” -> “报告”，查看入侵防御报告。
   - 自动刷新：点击 “自动刷新”，则每隔 60 秒钟刷新入侵防御信息。
   - 停用刷新：点击 “停用刷新”，则停止刷新入侵防御信息。
   - 删除记录：删除所有入侵防御信息。
2. 用户可分别查看入侵防御和反病毒功能的状态：启用或停用。
3. 查看最近 24 小时的流量和事件图 ：通过流量和事件对比图显示最近 24 小时内监测到的流量和攻击事件图。
4. 前 5 位攻击：可选择查看全部接口 （WAN 接口和 VLAN 接口）或单个接口的前 5 位的攻击信息，包括攻击频率和来源 IP 地址。
5. 前 10 位事件类别：可选择查看全部接口 （WAN 接口和 VLAN 接口）或单个接口的前 10 位的攻击事件类别，包括攻击类型和攻击频率。
6. IPS 阻绝端口：查看各个 LAN 端口是否被阻隔。

查看入侵防御原始数据

打开 “监视” -> “入侵防御状态” -> “原始数据”，查看入侵防御的原始数据。

- 自动刷新：点击 “自动刷新”，则每隔 60 秒钟刷新入侵防御的数据。
- 停用刷新：点击 “停用刷新”，则停止刷新入侵防御的数据。
- 删除记录：删除所有入侵防御信息。

无线状态

无线状态栏可查看 NAV10V2-WF 网关的无线网络状态，包括无线模式、无线频道以及各个无线网络的基本信息和连接信息等。

- 自动刷新：点击 “自动刷新”，则每隔 60 秒钟刷新无线网络信息。
- 停用刷新：点击 “停用刷新”，则停止刷新无线网络信息。
- 模式：显示 NAV10V2-WF 网关采用的无线网络工作模式。
- 无线频道：显示 NAV10V2-WF 网关当前采用的无线信道。

- 无线网络基本信息：分别显示 NAV10V2-WF 网关的无线网络的基本信息，包括 SSID、MAC 地址、无线网络名称、安全模式、SSID 广播、WMM 和接入的终端数目。
- 无线网络连接信息：分别显示 NAV10V2-WF 网关的各个无线网络的连接状态，包括 SSID、连接状态、收到 / 发送的数据包、收到 / 发送的字节、收到的错误包和丢失接收的包等。点击 “复位所有” 或 “复位” 可复位无线网络的连接状态。

服务质量

服务质量栏查看 NAV10V2-WF 网关的 QoS 策略信息，包括带宽控制策略和通信规则等。

- 自动刷新：点击 “自动刷新”，则每隔 60 秒钟刷新 QoS 策略信息。
- 停用刷新：点击 “停用刷新”，则停止刷新 QoS 策略信息。
- 带宽控制：显示当前带宽控制的 QoS 策略。
- 通信规则：显示 NAV10V2-WF 网关当前采用的通信规则及其详细设置。

5

系统管理

软件升级

警告

软件更新过程可能需要几分钟，请勿关闭或复位 NAV10V2-WF 网关。

要升级软件，请将最新的软件安装包解压到电脑后执行以下步骤：

1. 选择 “系统管理” -〉“软件升级”，打开软件升级界面。
2. 点击 “浏览”，找到用来更新的软件包。
3. 点击 “更新”按钮，按照界面上的提示对固件进行升级。

注释

软件更新前，建议将 NAV10V2-WF 网关的配置信息保存到本地。软件更新完毕后，建议先将 NAV10V2-WF 网关的设置恢复到出厂默认设置，然后导入备份的配置信息，并重启 NAV10V2-WF 网关。

配置管理

此功能可用来保存或恢复 NAV10V2-WF 网关的配置文件。 NAV10V2-WF 网关的配置文件为二进制格式，因此无法通过编辑配置文件来更改。

1. 选择 “系统管理” -〉“配置管理”，打开配置管理界面。
2. 要保存配置，请先选择配置保存位置，然后点击 “保存”按钮。
   - 选择 “到 PC”，可将配置文件保存到本地主机上。
   - 在 NAV10V2-WF 网关 USB 端口插入用来备份配置信息的 USB 设备，然后选择 “到 USB”，可将配置保存到该 USB 设备。
3. 要恢复配置，请在相应栏中输入配置文件的路径和文件名，或点击 “浏览”按钮，从本地主机或 USB 设备上找到配置文件，然后点击 “载入”按钮。

重置为默认值

1. 选择 “系统管理” -〉“重置为默认值”，打开恢复出厂设置界面。
2. 点击 “恢复出厂默认值”按钮， NAV10V2-WF 网关将重新启动并恢复到出厂默认设置。

注释 按下后面板的复位按钮 3 秒钟以上也可以将 NAV10V2-WF 网关的配置复位为出厂默认值。

重新启动

选择 “系统管理” -〉“重新启动”，打开重启设置界面。点击 “重启”按钮可重新启动设备。

6

工具

Ping

1. 选择 “工具” -〉“Ping”。
2. 分别输入以下参数：
   - IP 或 URL 地址：输入 NAV10V2-WF 网关要 ping 的 IP 地址或 URL 地址。
   - 包大小：输入 NAV10V2-WF 网关将采用的数据包的大小。
   - Ping 次数：选择 NAV10V2-WF 网关将要发送的 ping 命令次数。
3. 点击 “开始 Ping” 按钮发送 ping 数据包。消息框中将显示 ping 的结果。

路由追踪

1. 选择 “工具” -〉“路由追踪”，打开路由追踪设置界面。
2. 分别输入以下参数：
   - IP 或 URL 地址：输入 IP 地址或 URL 地址以执行路由追踪测试。
   - 最大跳数：选择路由追踪测试的最大跳数。
3. 点击 “开始 Traceroute” 按钮执行路由追踪测试。消息框中将显示路由追踪的结果。

DNS 查询

1. 选择 “工具” -〉“DNS 查询”，打开 DNS 查询设置界面。
2. 输入 IP 地址或 URL 地址以执行 DNS 查询。
3. 点击 “开始 Query”，开始查询指定 IP 或 URL 的 DNS 服务器 IP 地址。消息框中将显示 DNS 查询结果。

HTTPGet

注释 HTTPGet 不支持启用 Proxy 服务器的局域网络 。

HTTP-GET 方法可取回由 Request-URI 标识的信息。

1. 选择 “工具” -〉“HTTPGet”，打开 HTTPGet 设置界面。
2. 分别设置以下参数：
   - IP 或 URL 地址：输入 IP 地址或 URL 地址以执行 HTTPGET 操作。
   - 账号和密码：输入用户名和密码。
   - 再试次数：输入 HTTPGET 的尝试次数。
3. 点击 “开始”按钮，执行 HTTPGET 操作，返回的信息显示在下方。

端口检查

NAV10V2-WF 网关支持根据 IP 地址进行扫描，检查其开放的 TCP/UDP 端口状态。

1. 选择 “工具” -〉“端口检查”，打开端口检查设置界面。
2. 分别设置以下参数：
   - IP 或 URL 地址：输入执行端口扫描的目标 IP 地址或 URL 地址。
   - 端口：输入端口号，范围 1 到 65535。
   - 网络传输协议：选择基于 TCP 或 UDP 协议进行端口扫描。
3. 点击 “开始检查”按钮，执行端口扫描操作，扫描结果显示在下方。

A

附录

救援模式

注意　仅固件版本为 0.0.7 及其以上版本的 NAV10V2-WF 网关支持救援模式。

请依照下列步骤：

1. 当因软件发生问题导致系统无法开机，或先按重置按键再插入电源适配器直接进入救援模式时，Status LED 呈现黄灯并闪烁。
2. 此时， NAV10V2-WF 网关启动 TFTP 服务器，请利用 TFTP 客户端上传软件至 NAV10V2-WF 网关， TFTP 服务器的 IP 地址为 192.168.1.1。
3. 软件上传后， NAV10V2-WF 网关 将进行修复更新动作，可能需要几分钟的时间。
4. 更新完成后，系统会自动重新启动。重新开机后， Status LED 呈现绿灯恒亮。

USB 软件更新模式

请依照下列步骤：

1. 将用来更新的软件命名为 firmware.img，存入到备份 USB 的根目录下，并将备份 USB 插入 NAV10V2-WF 网关的 USB 接口，然后重新开机。
2. NAV10V2-WF 网关将自动进入 USB 软件更新模式，此时 Status LED 呈现闪烁。
3. 软件更新可能需要几分钟的时间。
4. 软件更新完成后，系统会自动重启。重新开机完成后， Status LED 呈现绿灯恒亮。

LED 运转状态

LED	颜色	动作	描述
Power	绿灯	关	电源关闭
		开	电源开启
Status	绿灯	开	系统已准备
		闪	开机
	黄灯	闪	进入救援模式
VPN	绿灯	关	无 VPN 通道
		开	VPN 通道已建立
		闪	尝试建立 VPN 通道
	黄灯	闪	SA/ 通道协商失败
IPS	绿灯	关	IPS 禁用
		开	IPS 启用
		闪	侦测到外部攻击
	黄灯	闪	侦测到内部攻击
FW	绿灯	关	防火墙未启用
		开	防火墙被启用
USB （用于备份 USB）	绿灯	关	备份 USB 未连接
		开	备份 USB 连接
		闪	传输 / 接收资料
Wireless	绿灯	关	无线功能已禁用
		开	有客户端连接但无资料流量
		闪	客户端连接且有资料流量
	黄灯	开	无线功能启用但是尚无客户端连接
		闪	有报文错误或缓冲区溢位

LED	颜色	动作	描述
Link/Act (LAN&WAN)	绿灯	关	以太网未连接
		开	以太网连接
		闪	传输 / 接收资料
1000 Mbps (LAN&WAN)	绿灯	关	10/100 Mbps 连接
		开	1000 Mbps 连接

B

声明

本手册中的技术规格和相关产品信息如有变化恕不另行通知。本手册中的所有声明、信息和建议都是真实可信的，但并不带有任何种类的明示或暗示保证。用户必须对其所有产品的应用负全部责任。

产品有限保证条款包含在产品一起发货的资料包中，并构成本附注的组成部分。如果未能找到产品有限保证条款，请与思科销售代表联系以获取其副本。

不考虑此处的其他保证，这些提供者的所有文档文件和软件连同其全部错误均按 “原样”提供。思科系统公司和上述提供者并未作出任何明示或暗示的保证，包括但不限于适销性、特定用途的适合性以及非侵权的保证、或交易过程、习惯、或贸易惯例所引发的保证。

在任何情况下，思科系统公司或其提供者对任何直接的、特殊的、因果性的、或偶然性的损害均不承担责任，包括但不限于由于使用或未能使用本手册所造成的利润损失或者数据损失或损害，即使思科系统公司或其提供者已被告知存在此类损害的可能性。