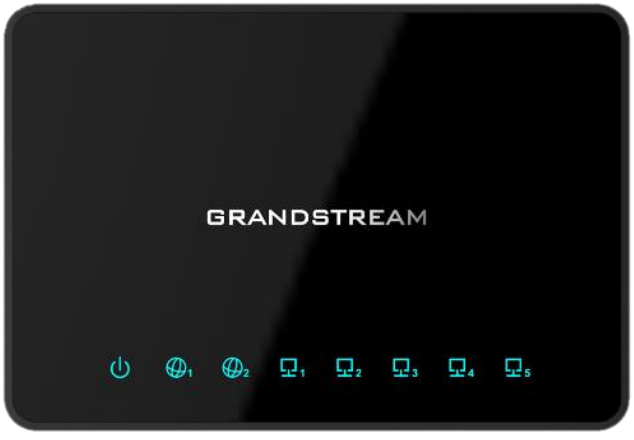
Grandstream Networks, Inc.

GWN7000

企业级多 WAN 口千兆 VPN 路由器

用户手册



版权

开源许可证

GWN7000 固件包含第三方开源软件。 潮流开源许可证可以从这里下载。

注意

未经潮流批准擅自修改本产品，或以用户手册以外的方式使用本产品，将会导致保修无效。

警告

请不要使用与设备不同的电源适配器，设备可能因此损坏，导致保修失效。

目录

文档目的 9

修订历史 11

固件版本 1.0.2.71 11

欢迎使用 12

产品概述 13

技术参数 13

安装 15

设备包装 15

连接 GWN7000 15

安全认证 16

保修 16

入门 17

LED 指示灯 17

使用 WEB 页面 17

访问 Web 页面 17

Web 页面语言 19

Web 页面配置 20

概览页面 21

保存和应用 22

路由器配置 23

状态 23

端口 23
WAN 端口配置 *23*
隧道 *25*
全局设置 *26*
端口镜像 *26*
静态路由 26
QoS 28
DDNS 30
建立无线网络 31
发现和匹配 GWN76xx 接入点 31
网络组 33
创建 SSID *38*
相同网络组下的额外 SSID *39*
客户端配置 41
客户端 41
状态 *41*
编辑 IP 和名称 *42*
阻止客户端 *43*
VPN（虚拟私有网络） 44
概览 44
OpenVPN ®服务器配置 44
生成 CA 证书 *44*
生成服务器/客户端证书 *47*
创建 OpenVPN®服务器 *52*
OpenVPN®客户端配置 54
L2TP/IPsec 配置 57
GWN7000 L2TP/IPsec 客户端配置 *57*
PPTP 配置 59
GWN7000 客户端配置 *60*
防火墙 62

基本 62
一般设置 *62*
端口转发 *62*
DMZ *63*
组内流量转发 *64*
UPnP *65*
流量规则设定 65
防火墙高级设置 67
一般设置 *67*
SNAT *67*
DNAT *68*
维护和调试 70
维护 70
调试 71
抓包 *71*
Ping/路由跟踪 *72*
Syslog *73*
NAT Table *74*
文件共享 75
SNMP（待定） 77
升级和配置 79
升级固件 79
通过 WEB 页面升级 *79*
配置和备份 80
下载配置 *80*
配置服务器 *80*
重置和重启 80
体验 GWN7000 企业级路由器 82

表目录

表 1: GWN7000 技术参数 13
表 2: GWN7000 设备包装 15
表 3: LED 指示状态 17
表 4 : 概览 21
表 5: GWN7000 WEB 页面 -> 路由器 ->Port -> WAN 端口(1,2) 24
表 6: 6in4 隧道 25
表 7: 6rd 隧道 25
表 8: aiccu 隧道 25
表 9: GWN7000 WEB 页面->路由器->端口->全局设置 26
表 10:端口镜像 26
表 11: IPv4 静态路由 27
表 12: IPv6 静态路由 27
表 13: QoS 基本 28
表 14: 上游 QoS 28
表 14: QoS 策略 29
表 16: 设备配置 32
表 17: 基本 34
表 18: Wi-Fi 35
表 19: CA 证书 45
表 20:服务器证书 48
表 21:客户端证书 51
表 22: OpenVPN®服务器 53
表 22: OpenVPN®客户端 55
表 24: L2TP 配置 58
表 25: PPTP 配置 61
表 26: 端口转发 63
表 27: 端口转发 63
表 28: UPnP 设置 65
表 29: 防火墙流量规则 66
表 30: 防火墙-一般设置 67
表 31: SNAT 68
表 32: DNAT 69
表 33: 维护 70
表 33: 调试-抓包 72
表 35: 新建文件共享 76
表 36: SNMP 基本页面 77
表 37: SNMP 高级页面 78
表 38: 网络升级配置 79

图目录

图 1: GWN7000 前视图 15
图 2: GWN7000 后视图 16
图 3: GWN7000 Web 页面登录页面 18
图 4: 首次登录修改密码 19
图 5: 设置向导 19
图 6: GWN7000 Web 页面 语言 20
图 7: GWN7000 Web 页面 语言 20
图 8: 概览页面 21
图 9: 保存更改 22
图 10: 路由器状态 23
图 11: QoS 28
图 12: 发现 AP 31
图 13: 发现的设备 31
图 14: GWN7610 在线 32
图 15: 网络组 33
图 16: 新建网络组 34
图 17: 设备管理 37
图 18: 接入点页面添加 AP 至网络组 38
图 19: 创建 SSID 39
图 20:额外 SSID 40
图 21:额外 SSID 创建 40
图 22: 客户端 41
图 23: 客户端状态 42
图 24: 客户端配置 43
图 25: 阻塞客户端 43
图 26: 取消禁用客户端 43
图 27: 创建 CA 证书 45
图 28: CA 证书 46
图 29: 创建服务器证书 47
图 30: 用户管理 49
图 31: 客户端证书 50
图 32: 创建 OpenVPN®服务器 52
图 33: OpenVPN® 54
图 34: OpenVPN®客户端 55
图 35: OpenVPN®客户端 57
图 36: L2TP 客户端配置 58
图 37: L2TP 客户端 59
图 38:PPTP 客户端配置 60

图 39:PPTP 客户端 61
图 40:基本->一般设置 62
图 41:端口转发 63
图 42:DMZ 63
图 43:组内流量转发 64
图 44:启用组内流量转发 64
图 45:流量规则设置 66
图 46:抓包文件 72
图 47:IP Ping 73
图 48:路由跟踪 73
图 49:Syslog 74
图 50:NAT Table 75
图 51:新建文件共享 76
图 52:文件共享激活 76
图 53:访问文件共享 77

文档目的

本文档介绍了如何通过 CLI 或 WEB 页面配置 GWN7000 并充分使用。本文档主要针对网络管理员。

下载最新版本“GWN7000 用户手册”，请访问潮流网络技术有限公司网站：

http://www.grandstream.com/support.

文档主要包含以下几点：

- 产品概述
- 安装
- 入门
- 路由器配置
- 建立无线网络
- 客户端配置
- VPN
- 防火墙
- 维护和诊断
- 体验 GWN7000 企业级路由器

修订历史

这部分记录了上次用户手册以来的重要改变，仅列出主要功能升级和文档修订，细小的修正和改变不包括在修订记录内。

固件版本 1.0.2.71

- 初始版本.

欢迎使用

感谢您购买潮流 GWN7000 企业级多 WAN 口千兆 VPN 路由器。

GWN7000 是一款功能强大的企业级多 WAN 口千兆 VPN 路由器。量身为中小企业定做，如：写字楼、零售商店、购物中心、酒店、医院、会展中心等，GWN7000 允许企业跨越多个不同的物理位置，建立全面的 Wi-Fi 或 VPN 网络。它具有高性能的路由和交换电源，以及一个硬件加速的 VPN 客户端/服务器，用于安全的局间连接。为了最大限度地提高网络可靠性，GWN7000 支持流量负载均衡和故障转移。 GWN7000 集成控制器和自动配置主站，可以配置和管理网络中多达 300 多个的 GWN 系列 Wi-Fi 接入点。这个功能可以通过产品的直观的 Web 界面轻松操作，它还提供了一个中央面板，以监控整个网络。

注意:

未经潮流批准擅自修改本产品，或以用户手册以外的方式使用本产品，将会导致保修无效。

警告:

请不要使用与设备不同的电源适配器，设备可能因此损坏，导致保修失效。

产品概述

技术参数

表 1: GWN7000 技术参数

网络接口	• 2 x 自适应 10/100/1000 Base-T WAN • 1 x 自适应 10/100/1000 Base-T 可配置为 LAN/WAN 或 VoIP 端口（pending） • 4 x 自适应 10/100/1000 Base-T LAN
WAN 功能	• DHCP • 静态 IP • PPPoE • 负载均衡 & 故障转移 • 路由规则
LAN 功能	• DHCP 服务器 • DNS 缓存 • 多区域 • VLAN
辅助接口	• 2 x USB 2.0 • 1 x Reset 针孔
路由效率	高达 1Mpps/每秒传输的数据包大小为 64bytes
USB	• 3G/4G/LTE as WAN （pending） • 打印机共享 • 文件共享
网络协议	• IPv4, IPv6 (pending), 802.1Q, 802.1p
VPN	• 协议: PPTP, L2TP/IPSec, OpenVPN® • Client，Server 或透传直通
LED	8 个绿色 LED 指示设备跟踪和状态显示
安装	支持挂壁,桌面安装
QoS	VLAN, TOS，支持多个流量类，按端口，IP 地址，DSCP 和策略进行过滤
防火墙	NAT, DMZ, Port Forwarding, SPI, UPnP
自动配置能力	集成配置主站，最大控制 300+GWN 系列 Wi-Fi 接入点
管理	Web, CLI
电源	• 802.3at PoE • 供应电源: 12V/2A • 最大功耗: 16W
环境	• 温度: 0°C to 40°C

	• 存储: -10°C to 60°C • 湿度: 10% to 90% 无冷凝
包装内容	• GWN7000 企业级路由器 • 12V/2A 电源适配器 • 快速安装手册 • GPL License
认证	FCC, CE, RCM, IC

安装

在部署和配置 GWN7000 之前，设备需要上电并连接网络。这部分将会详细讲述 GWN7000 的安装、连接和保修政策。 t

设备包装

表 2: GWN7000 设备包装

主设备	1 个
电源适配器	1 个
快速安装手册	1 个
GPL License	1 个

连接 GWN7000

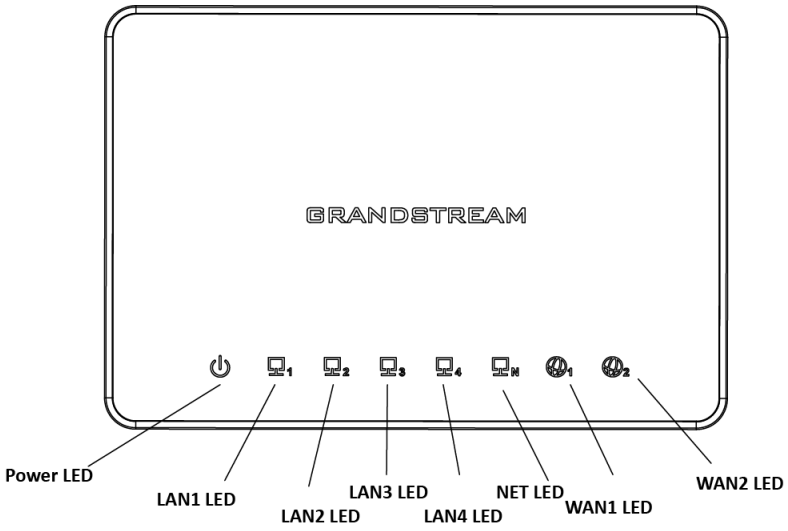


图 1: GWN7000 前视图

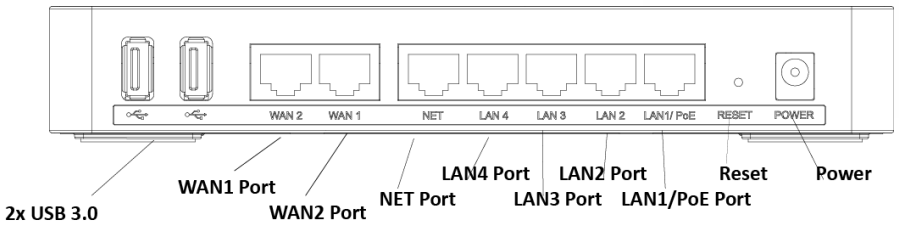


图 2: GWN7000 后视图

请按以下步骤设置 GWN7000：

1. 将RJ-45 网线的一端插入GWN的WAN1 或WAN2。
2. 将网线的另一端插入DSL调制解调器或路由器。
3. 将 12V直流电源适配器连接插入GWN7000 背面的电源插孔，将适配器的主插头插入电源插座。
4. 等待GWN7000 启动并连接到互联网/网络，在GWN7000 前面指示电源的绿色LED将会亮起，指示WAN口的绿色LED将闪烁。
5. 将一个 LAN口与您的电脑相连，连接端口的绿色LED将会闪烁。
6. (可选) 将设备的LAN口连接到GWN7610 接入点或其他设备，相关的LAN口绿色LED将会闪烁。

安全认证

GWN7000 企业级路由器符合FCC/CE和各种安全标准。GWN7000 的电源适配器服务UL标准。仅支持使用GWN包装中的通用电源适配器，制造商的保修范围不包括由使用不匹配电源适配器造成的损坏。

保修

如果您购买自经销商，请直接联系经销商更换，维修或退货。如果您直接购于潮流网络公司，请联系潮流技术支持团队，取得退货许可号码（RMA）后退货。潮流网络科技公司保留在不做预先通知的情况下修改售后服务细则的权利。

入门

GWN7000 为用户提供直观的 Web 页面配置界面，对设备所有配置选项进行配置管理。

本节提供说明分步读取 LED 灯的指示状态和使用 GWN7000 的 Web 页面。

LED 指示灯

GWN7000 的前面板有电源和接口活动的 LED 指示灯，下表描述了 LED 灯的指示状态。

表 3: LED 指示状态

LED	状态	描述
电源	关闭	电源关闭或设备电源不正常.
	绿灯	设备正常上电
WANs(1,2)	绿灯闪烁	GWN7000 作为客户端连接到其他网络，并且数据正在传输
	绿灯	GWN7000 作为客户端连接到其他网络，并且没有数据传输
LANs(1,2,3,4,5)	绿灯闪烁	一个设备连接到相应的 LAN 口，并且正在传输数据
	绿灯	一个设备连接到相应的 LAN 口，并且没有数据传输

使用 WEB 页面

访问 Web 页面

GWN7000 内嵌 Web服务器响应HTTPS GET/POST请求。内嵌HTML页面允许用户通过Web浏览器，如 Microsoft IE, Mozilla Firefox, Google Chrome等配置设备。

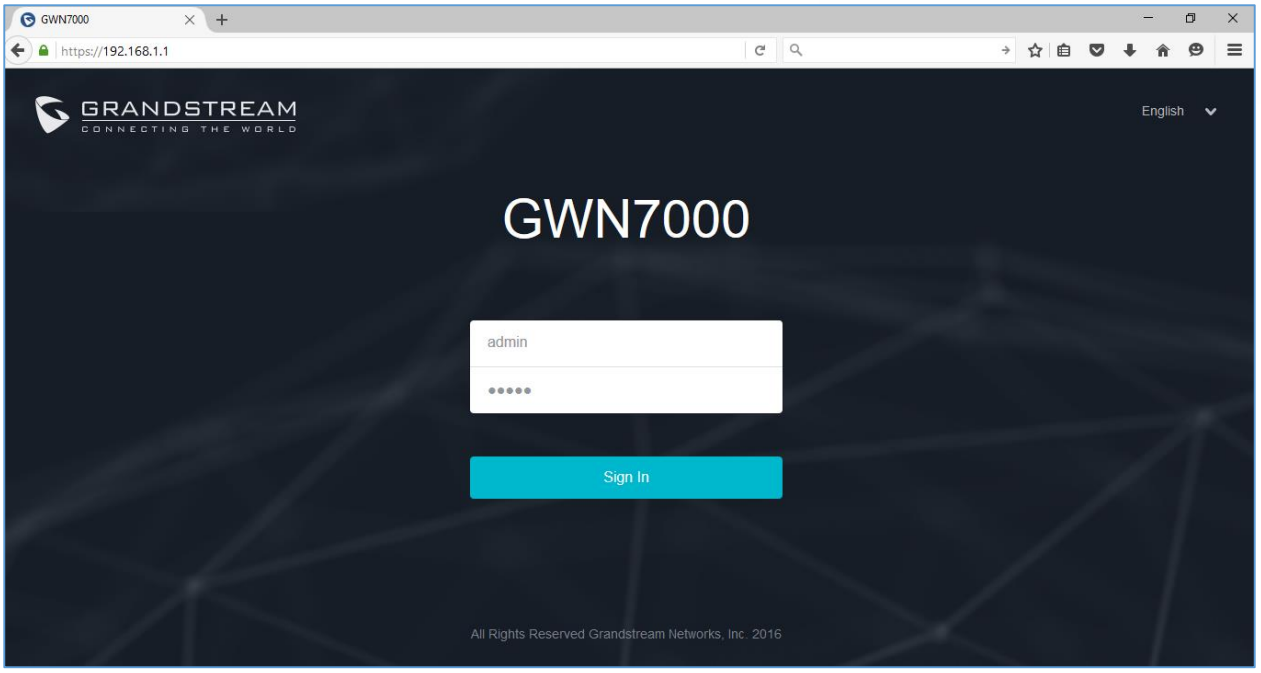


图 3: GWN7000 Web 页面登录页面

访问 Web页面:

1. 将电脑连到GWN7000 的一个LAN口上。
2. 确保设备已经上电，并且指示电源、LAN口的LED是亮的。
3. 打开Web浏览器，并以以下形式输入Web页面 https://192.168.1.1（默认的IP地址）。
4. 输入管理员的账号和密码登录WEB配置页面，默认的管理员账号和密码均为“admin”。强烈建议第一次登录后修改默认密码。

   注意：首次登录或恢复出厂设置后，用户将被要求更改默认管理员和用户密码，然后才能访问GWN7000 Web界面。

   密码字段区分大小写，最大长度为 32 个字符。 为安全起见，建议使用强密码，包括字母，数字和特殊字符。

图 4: 首次登录修改密码

首次登录后，用户可以使用安装向导工具进行配置，或退出以进行手动配置。 安装向导可以随时通过在 Web 界面上单击  来访问。

图 5: 设置向导

Web 页面语言

当前GWN7000 系列Web页面支持英语和简体中文。

用户可以在登录之前或之后在WEB用户登录界面的右上角选择显示的语言。

图 6: GWN7000 Web 页面 语言

图 7: GWN7000 Web 页面 语言

Web 页面配置

在web用户界面有 6 个主要部分，以查看链接状态，配置和管理路由器

- **概览:** 提供以仪表板样式显示的GWN7000 信息的总体视图，便于监控。
- **路由器:** 显示设备状态，用于配置WAN端口的IP配置，负载均衡，故障切换，静态路由，端口镜像，QoS和DDNS等端口设置。
- **接入点:** 增加、匹配和管理已经发现的接入点。
- **客户端**: 显示通过LAN连接到GWN7000 的客户端列表和通过无线接入点连入的无线客户端。
- **VPN:** 配置 OpenVPN的客户端和服务器，PPTP和L2TP的客户端通道。
- **防火墙:** 基本和高级防火墙配置，以安全地管理路由器的入站/出站流量。

- **网络组：**通过使用VLAN配对的接入点添加和管理无线网络组。
- **系统设置：**用于维护和调试功能，以及生成证书和文件共享。

概览页面

用户成功登录 GWN7000 后首先看到的是概览页面。它以仪表板样式显示 GWN7000 信息的总体视图，便于监控。

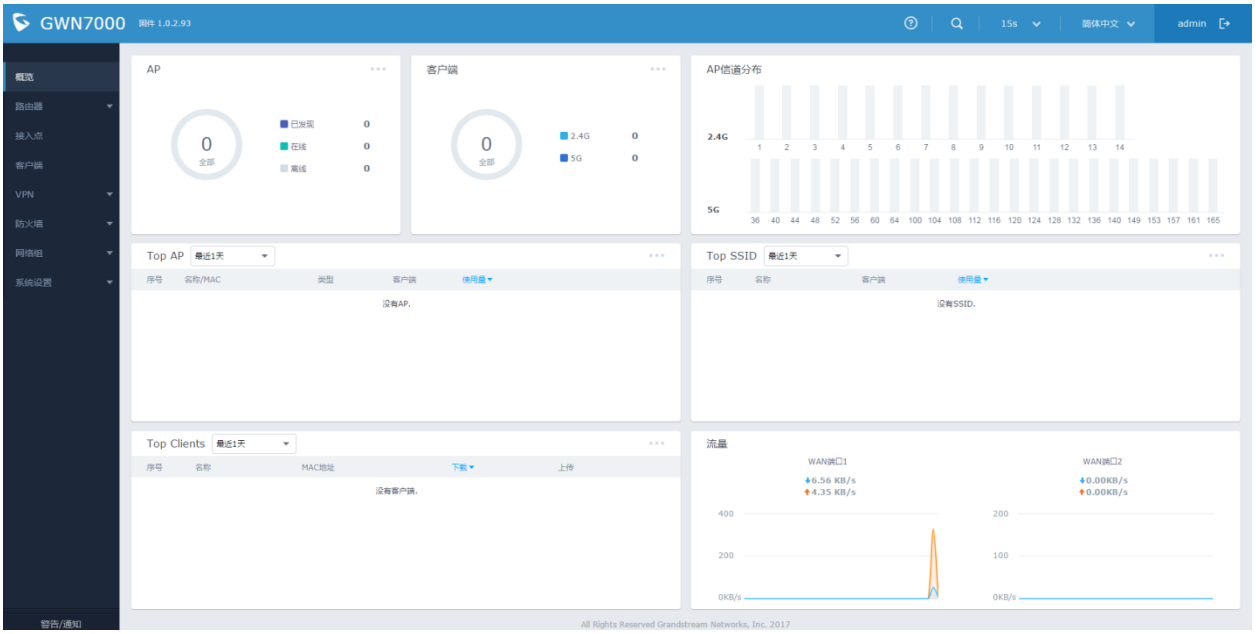


图 8: 概览页面

用户可以快速查看 GWN7000 各项状态，请参照下表查看

表 4：概览

AP	显示已发现，配对（在线）和离线的接入点数。 用户可以点击 ••• 进入接入点的页面查看 AP 基本和高级的置选项
客户端	显示连接的客户端的总数，以及连接到每个通道的客户端的计数。 用户可以点击 ••• 进入客户端面了解更多选项。
AP 信道分布	显示所有与 AP 匹配的信道。
Top AP	显示顶部 AP 列表，用户可以通过连接到每个 AP 的客户端的数目或者数据使用量分类列表。用户可以点击 ••• 进入接入点页面以获得 AP 的基本和高级配置选项。
Top SSID	显示顶部 SSID 列表，用户可以通过连接到每个 SSID 的客户端数量或结合上传和下载的数据使用来分类列表。 用户可以点击 ••• 进入网络组页面了解更多选项。

Top clients	显示热门客户端列表，用户可以通过上传或下载来分类客户端列表。 用户可以点击 进入客户页面了解更多选项。
流量	显示两个 WAN 端口上发送/接收的流量数据速度。

概览页面每过 5s/15s/1min/2min 和 5min 进行刷新，或者点击页面上部的菜单 (默认的刷新时间是 5s)。

保存和应用

在Web页面配置或改变任意选项之后，请点击“保存”按钮。提醒更改数目的消息将会出现在菜单的上部(详见图 9)。

图 9: 保存更改

点击 应用 应用修改 ， 点击 撤销 撤销修改。

路由器配置

本节包括网络 WAN 端口，静态路由，QoS 和 DDNS 的配置页面，并显示路由器状态。

状态

状态页面用于显示**设备状态**，以检查 GWN7000 及其 WAN 端口的 MAC 地址，部件号，固件相关信息和正常运行时间。

用户还可以检查 WAN 状态，显示常规信息，如正常运行时间，当前吞吐量，总体使用情况和 IP 地址。

路由器状态可以通过 **Web 页面->路由器->状态**访问。

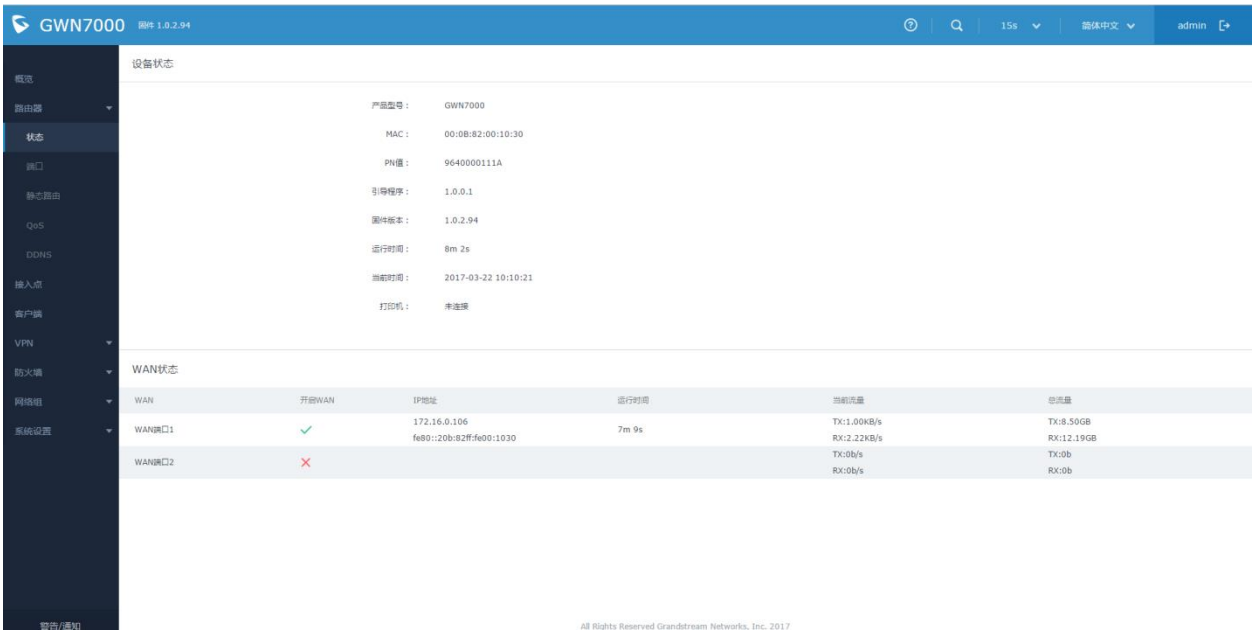


图 10: 路由器状态

端口

将电脑连接到GWN7000 的LAN端口访问Web页面页面，进入**路由器->端口** 页面配置进行端口。

WAN 端口配置

默认情况下，GWN7000 有 2 个WAN端口配置为DHCP客户端。 每个端口都可以连接DSL调制解调器或路由器。

用户还可以设置静态IPv4 / IPv6 地址，并为每个WAN端口配置PPPoE。

GWN7000 WAN口上的基本网络配置参数请参考下表。

表 5: GWN7000 WEB 页面 -> 路由器 ->Port -> WAN 端口(1,2)

启用	选择是否启用 WAN 端口
WAN 地址类型	选择 WAN 端口的工作模式 "DHCP", "静态" 或 "PPPoE"， 默认设置为 "DHCP". • **DHCP** 设备自动从 DHCP 服务器获取地址 • **静态** 用户需要设置静态的 IPv4 地址、子网掩码和网关或设置 IPv6 地址、前/后缀长度 • **PPPoE** 用户需设置 PPPoE 账号和密码、维持时间、Inter-key 超时时间
首选 DNS	输入首选 DNS 地址，一旦设置，改地址会被优先使用
备用 DNS	输入备用 DNS 地址，当首选 DNS 出现问题时使用
Native IPv6	用于启用将 IPv6 地址分配给 GWN7000。 一旦启用，用户将能够配置以下字段：“IPv6 地址分配”，“首选 IPv6 DNS”，“次选 IPv6 DNS”和“IPv6 Relay to LAN”。
IPv6 地址分配	当启用“Native IPv6”选项时，会出现此选项。 选择“自动”从 DHCP 服务器获取 IPv6 地址，或选择“静态”手动配置 IPv6 地址。 如果设置为“静态”，用户应设置以下字段： • **IPv6 地址/Prefix Length** 用于在使用静态 IPv6 选项时设置 IPv6 地址/前缀长度。 例如：fec0：470：28：5b2 :: 1/64 • **IPv6 网关** 设置 IPv6 网关地址。 • **IPv6 前缀/前缀长度** 输入 IPv6 前缀和 IPv6 前缀长度。 示例：:: 1/64
IPv6 首选 DNS	仅当启用“本机 IPv6”选项时，才会显示此选项。 它用于设置首选 DNS 服务器地址（IPv6 地址）。 如果设置了首选 DNS，GWN7000 将优先使用。
IPv6 次选 DNS	仅当启用“本机 IPv6”选项时，才会显示此选项。 它用于设置备用 DNS 服务器地址（IPv6 地址）。 如果设置了首选 DNS，当首选 DNS 失效时，GWN7000 将使用它。
IPv6 Relay to LAN	仅当启用“本机 IPv6”选项时，才会显示此选项。 启用后，GWN7000 将中继 IPv6 地址到 LAN 客户端。
VLAN Tagging	用于启用 VLAN 标记。 如果设置为“0”，VLAN 标记将被禁用， 否则设置 VLAN 间介于 5 到 4093 之间。缺省值为 0。

隧道

隧道页面用于通过 IPv6 隧道代理服务提供商在 WAN 端口上设置 IPv6 隧道，用于通过 IPv4 网络传输 IPv6 数据包。 用户可以创建 6in4,6rd 和 aiccu 隧道。 每种隧道类型请参考下表。

表 6: 6in4 隧道

WAN 接口	选择要设置 6in4 隧道的 WAN 端口。
MTU	设置最大传输单位值。 有效范围是 64-9000。 默认值为 1500。
6in4 IPv4 peer 地址	输入对端的 IPv4 地址。
6in4 隧道终端 IPv6 地址	本端的 IPv6 地址（由隧道提供者分配的） 例如：2001：db8：2222 :: 2/64
6in4 路由前缀	设置隧道提供商给出的可路由前缀，以允许 LAN 客户端从该前缀获取地址。
隧道 ID	设置隧道 ID。
用户名	设置用于登录隧道代理的用户名。
密码	设置用于登录隧道代理的密码。
更新密钥	HE.net 更新密钥，重置密码（终端更新时用）。

表 7: 6rd 隧道

WAN 接口	选择要设置 6rd 隧道的 WAN 端口。
MTU	设置最大传输单位值。 有效范围是 64-9000。 默认值为 1500。
6rd IPv4 peer 地址	输入对端的 IPv4 地址。
6rd IPv6 地址前缀	本端的 IPv6 地址（由隧道提供者分配的） 例如：2001：db8：2222 :: 2/64
IPv6 前缀长度	设置 IPv6 前缀长度（有效值 1-128） 例如：128
IPv4 前缀长度	设置 IPv4 传输地址前缀长度。 （有效值 1-32）

表 8: aiccu 隧道

WAN 接口	选择要设置 6rd 隧道的 WAN 端口。
用户名	输入用户名（通过注册 SixXS Tunnel Broker 提供）
密码	输入密码

全局设置

本节指定multi-WAN的运行模式 ，用于启用/禁用WAN端口的故障切换和负载均衡。
下表说明 Multi-WAN 的详细设置参数 。

表 9: GWN7000 WEB 页面->路由器->端口->全局设置

多 WAN	3 项可选: • 禁用 • 故障切换 • 负载均衡+故障切换
禁用	禁用多 WAN 功能
故障转移	如果选择启用故障转移，管理员需要指定被使用的 WAN 端口。 选择后，用户可以在 WAN 端口上设置多 WAN 参数。
负载均衡 +故障转移	除了故障切换，负载均衡将所有端口的资源进行优化。请注意，此工作模式下，WAN 端口应该连接到不同的网络。 选择后，用户可以在 WAN 端口上设置多 WAN 参数。
禁止的客户端 MAC	设置要禁止的无线客户端的 MAC 地址，可以通过点击 添加或点击 删除。
MAC 重写地址	MAC 重写功能用于向 GWN7000 提供虚拟 MAC 地址，以便任何连接到路由器的客户端都将可以使用输入的 MAC 地址。 注意：在较小的情况下，请确保输入覆盖 MAC 地址。

端口镜像

启用端口镜像后，GWN7000 会将一个 LAN 端口上看到的所有网络数据包的副本发送到另一个端口，从而可以对数据包进行分析。 有关配置选项，请参阅下表。

表 10:端口镜像

开启输出镜像	选择是否启用 LAN 端口的输出镜像。 默认为“禁用”。
开启输入镜像	选择是否启用 LAN 端口的输入镜像。 默认为“禁用”。
镜像端口	选择流量镜像的 LAN 端口，默认为“禁用”。
被镜像端口	选择被镜像的 LAN 端口，默认为禁用。

静态路由

GWN7000 支持手动设置静态 IPv4 和 IPv6 路由，并显示路由表项。
用户可以从 GWN7000 **WebGUI->路由器->静态路由**配置静态路由。

有三个选项卡可用：

- **路由**查看路由表条目。

- **IPv4** 创建，编辑或删除静态IPv4 静态路由。

- **IPv6** 创建，编辑或删除静态IPv6 静态路由。

IPv4 和 **IPv6** 选项卡中均包含以下操作：

- 点击 

添加静态路由
- 点击  编辑静态路由。
- 点击  删除静态路由

请参考下表，创建 IPv4/IPv6 静态路由。

表 11: IPv4 静态路由

名字	输入静态路由的名称。
开启	选择启用/禁用该静态路由。
组	选择使用改静态路由的 LAN 口网络组。
目标网络/主机	输入要将数据路由到的网络/主机 IP 地址。 示例：192.168.5.0
子网掩码	输入目标网络/主机子网掩码。 例如：255.255.255.0
网关	输入网关 IP 地址。 如：192.168.5.1
Metric	设置度量值。有效范围为 0-255。 默认值为 1。

表 12: IPv6 静态路由

名字	输入静态路由的名称。
开启	选择启用/禁用该静态路由。
组	选择使用改静态路由的 LAN 口网络组。
目标网络/主机	输入要将数据路由到的网络/主机 IP 地址。 例如：2001:db8:3c4d:4::/64
网关	输入网关 IP 地址。 如：fec0:470:28:5b2::1/64
Metric	设置度量值。有效范围为 0-255。 默认值为 1。

QoS

GWN7000 提供了在 WAN 和 LAN 端口配置 QoS 的可能性，帮助管理员更深入的对不同的服务如数据、声音、视频进行网络流量管理。

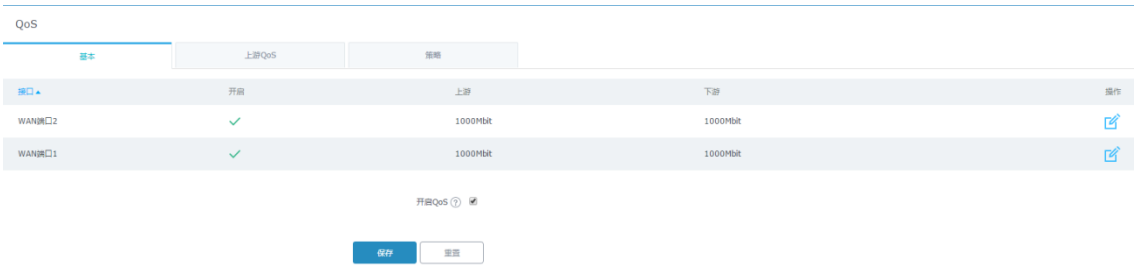


图 11: QoS

要激活 QoS，请选中“开启 QoS”。 有三个选项卡可供配置：

- 基本：用户可以在 WAN 接口上设置下载和上传带宽限制。
- 上游 QoS：用户可以创建流量类来优先处理特定资源的流量网络；这将保证至少一个类别具有配置的上行带宽。
- 策略：用户可以为特定目标创建规则，以设置优先级和流量速率，以允许 GWN7000 在达到配置的最大速率时丢弃超出的流量。

请参照下表对各选项卡进行配置：

表 13: QoS 基本

开启	选择是否启用所选 WAN 接口的上游和下游限制规则。
上游	为指定的接口设置上行带宽限制，如果设置值指“位”单位，则该值应以 Mbit，Kbit 或无单位结束。 示例：1000Mbit 100Kbit 500
下游	为指定的接口设置下行带宽限制，如果设置值指“位”单位，则该值应以 Mbit，Kbit 或无单位结束。 示例：1000Mbit 100Kbit 500

表 14: 上游 QoS

流量类	
名称	定义流量类别的名称

优先级	设置流量类的优先级，值越小，优先级越高。 有效范围介于 1 到 64 之间。
接口	选择要从中分类流量的 WAN 接口，确保从基本中已启用所需的接口。
上游	为指定的接口设置上行带宽限制，如果设置值指“位”单位，则该值应以 Mbit，Kbit 或无单位结束。 示例：1000Mbit 100Kbit 500
流量过滤	
类	从已经创建好的流量类别中选择一个类别
名称	为流量过滤规则定义名称
DSCP	从下拉菜单中选择不同的服务代码点 (DSCP)，默认为 0.
IP 源地址	指定将应用流量过滤规则的源 IP 地址。
IP 目标地址	指定要应用流量过滤规则的目标 IP 地址。
TCP 源端口	指定要应用流量过滤规则的 TCP 源端口。
TCP 目标端口	指定要应用流量过滤规则的 TCP 目标端口。
UDP 源端口	指定要应用流量过滤规则的 UDP 源端口。
UDP 目标端口	指定要应用流量过滤规则的 UDP 目标端口。
组源	选择指定的源 IP 地址的 LAN 组。如果未定义源 IP 地址，则该规则将应用于该 LAN 组的所有成员。

表 15: QoS 策略

名称	定义 QoS 策略规则的名称。
接口	选择要监管流量的接口，确保从 QoS 基本中已启用所需的接口。
优先级	设置流量类的优先级，值越小，优先级越高。有效范围介于 1 到 64 之间。
速率	在应用策略规则时，设置要应用的限制值。
DSCP	从下拉列表中选择差分服务代码（DSCP）值。默认为 0。
IP 源地址	指定将应用 QoS 规则的源 IP 地址。
IP 目标地址	指定将应用 QoS 规则的目标 IP 地址。
TCP 源端口	指定将应用 QoS 规则的 TCP 源端口。
TCP 目标端口	指定将应用 QoS 规则的 TCP 目标端口。
UDP 源端口	指定将应用 QoS 规则的 UDP 源端口。
UDP 目标端口	指定要应用 QoS 规则的 UDP 目标端口。
组源	选择指定的源 IP 地址的 LAN 组。如果未定义源 IP 地址，则该规则将应用于该 LAN 组的所有成员。

DDNS

DDNS 允许用户通过域名而不是 IP 地址访问 GWN7000，GWN7000 支持以下 DDNS 供应商：

- Dyndns.org
- Changeip.com
- Zoneedit.com
- Free.editdns.net
- Freedns.afraid.org
- He.Net
- Dnsomatic.Com
- No-ip.pl
- Myonlineportal.net

在 GWN7000 上配置 DDNS 设置之前，用户首先需要通过支持的提供商创建和确认其 DDNS 账号。
请根据以下步骤配置 DDNS：
1.访问 GWN7000 Web GUI，并导航到**路由器-> DDNS**，并启用 DDNS 服务。
2.在域名字段下填写 DDNS 提供商创建的域名。
3.在“用户名”和“密码”字段下输入您的帐户用户名和密码。
4.在“网络接口”字段下指定应用 DDNS 的 WAN 接口。
5.（可选）对于高级配置，用户还可以登录到 Syslog 并修改刷新字段的值，以便定期检查更新的 IP 地址。

建立无线网络

GWN7000 企业级路由器提供用户通过添加GWN76xx系列接入点创建无线网络的能力，连接工作在最常见的无线标准下(802.11b/g/n)，范围在 2.4GHz至 5GHz之间。
GWN7000 集成了多种安全协议，包括基于IEEE 802.1x端口认证协议，有线等效保密协议（WEP），Wi-Fi保护访问协议（WPA和WPA2）、防火墙协议和VPN隧道协议。
本章节将会介绍如何添加GWN76xx接入点，创建和管理Wi-Fi。
更多GWN76xx系列详细信息，请查阅以下链接：
http://www.grandstream.com/products/networking-solutions/wifi-access-points

发现和匹配 GWN76xx 接入点

GWN76xx 是一款强大的接入点，与 GWN7000 完全兼容，可以轻松直观地一键添加，配置和管理。 一旦 GWN76xx 成功连接并且从 GWN7000 路由器获取到 IP，则用户可以将其与 GWN7000 配对并将其与网络组相关联。
要将连接到 LAN 客户端的 GWN76xx 接入点与 GWN7000 配对，请按照以下步骤操作：

1.访问 GWN7000 Web GUI 进入**接入点**页面

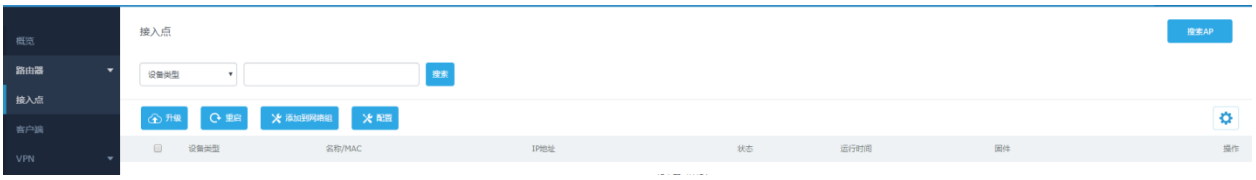


图 12: 发现 AP

2.点击 搜索AP 发现已经连接到 GWN7000 网络中的接入点，以下界面将会出现。

图 13: 发现的设备

3.点击“操作”下的，将接入点和 GWN7000 进行匹配。

4.已经匹配的 GWN76xx 将会显示在线，用户可以点击 取消匹配。

图 14: GWN7610 在线

5. 用户可以点击，检查设备配置的状态，连接到它的用户和配置，或从同一型号选择多个 GWN76xx AP，然后单击 配置 在所选单元上应用相同的配置。

请参照下表进行设备配置。

表 16: 设备配置

状态	显示设备的配置信息如：固件版本、IP 地址、运行时间、平均负荷、连接速度等
用户	显示通过 GWN76xx 接入点接入的用户
配置	• **设备名称:** 设置 GWN76xx 名称，以及其 MAC 地址 • **固定 IP:** 用于为 GWN76xx 设置静态 IP，如果检查用户需要设置以下内容： -IPv4 地址：输入要设置为静态的 IPv4 地址 -IPv4 子网掩码：输入子网掩码。 -IPv4 网关：输入网关的 IPv4 地址。 • **频段:** 设置 GWN76xx 频段，可选 2.4GHz, 5GHz 或双频。 • **开启频段切换：** 设置是否能使用频谱导航功能，若开启，系统将自动调整 2.4G/5G 用户双频段用户接入比例。 • **模式:** 通常情况下，为获得最佳性能及兼容性，2.4G 频段请选择 802.11n；5G 频段请选择 802.11ac。 • **信道带宽:** 请选择工作信道带宽，注意工作信道带宽能提高速率，实际应用和周边无线环境密切相关，请根据实际情况选择合适的工作信道带宽。 • **40MHz 通道位置:** 在频道宽度中使用 20MHz / 40MHz/80MHz 时，可以配置 40MHz 频道的位置，用户可将其设置为“次信道低于主信道”、“主信道低于次信道”或“自动”。 • **信道:** 选择“自动”或特定信道。 默认为“自动”。请注意，建议的信道取决于**系统设置->维护**下的国家/地区设置。 • **启用短间隔:** 非多径环境下，使能“短间隔保护”，有利于提高无线连接速率。 • **激活空间流:** 自定义选择空间流数，如自动、1、2、3（仅限 GWN7610） • **无线电传送功率:** 设置无线电功率，低、中、高可选，射频功率太高将增加设备间干扰，请根据实际情况选择射频功率。

注意:

如果GWN76xx未配对，或配对图标为灰色，请确保该设备未与另一台作为主控制器的GWN7000路由器或

GWN76xx接入点配对，如果是，则用户首先需要取消配对，或者恢复出厂使其可用于配对。

网络组

用户可以创建由 VLAN 分隔的不同网络组，并添加配对的 GWN76xx 接入点。

登录 GWN7000 Web GUI，访问**网络组->网络组**。

图 15: 网络组

GWN7000 具有名为 group0 的默认网络组，单击  编辑它，或单击 

添加新的网络组。

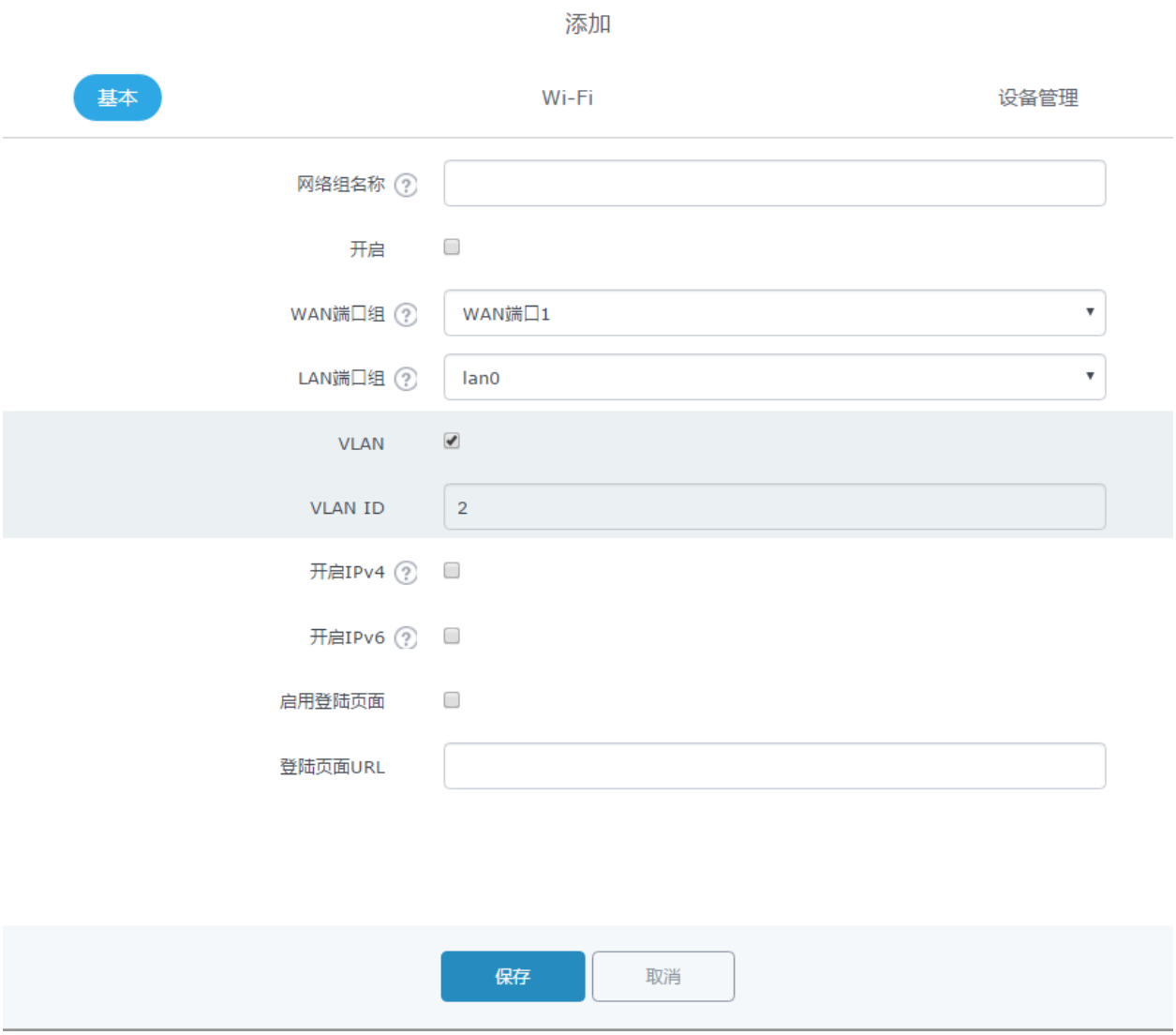


图 16: 新建网络组

编辑或添加新的网络组时，用户将有三个选项卡进行配置：

- **基本：**用于命名网络组，如果添加新网络组，则设置 VLAN ID，并对每个字段进行寻址，请参见下表。

表 17: 基本

网络组名称	指定网络组名称。
WAN 端口组	选择 WAN 端口成员资格。 如果在**“路由器”->“端口”->“全局设置”**下启用，则可以从“多 WAN”选项中受益。
LAN 端口组	选择 LAN 端口成员。
VLAN	启用 VLAN。只有当拥有多个网络组时，该字段才会出现。
VLAN ID	设置 VLAN ID，有效值从 2 到 4093。
开启 IPv4	选择是否在该网络组启用 IPv4 地址。

IPv4 静态地址	设置一个静态 IPv4 地址。
IPv4 子网掩码	设置 IPv4 子网掩码。
开启 IPv4 DHCP	选择是否启用 IPv4 DHCP 服务。这将允许连接到该网络组的客户端从作为 DHCP 服务器的 GWN7000 自动获取 IPv4 地址。
DHCP 开始地址	设置 DHCP 的起始地址，地址会被分配给连接到该网络组的用户。
DHCP 结束地址	设置 DHCP 的结束地址，地址会被分配给连接到该网络组的用户。
DHCP 租约时间	设置 DHCP 租约时间，默认为 12h
DHCP 选项	设置 DHCP 选项。点击添加其他选项，点击删除选项。 示例：44,192.168.2.50 的 DHCP 选项 44 和 192.168.2.50 是 WINS 服务器的地址。 有关 DHCP 选项语法，请参阅以下链接： https://wiki.openwrt.org/doc/howto/dhcp.dnsmasq
开启 DHCPv4 Relay	如果您希望 GWN7000 将来自客户端的 DHCP 请求中继到另一个 DHCP 服务器，请启用此选项。点击添加另一个 DHCPv4 中继目标，点击删除一个 DHCPv4 中继目标。
开启 IPv6	选择是否使用 IPv6 地址。
IPv6 Relay from WAN	检查以允许 GWN7000 将 IPv6 DHCP 请求从网络组的客户端中继到 WAN 端口。
开启 IPv6 DHCP	选择是否启用 IPv6 DHCP 服务。
IPv6 分配前缀	设置要分配给网络组的前缀长度。有效范围介于 1 到 64 之间。 示例：64 将分配/ 64 前缀。
IPv6 子网提示	设置子网掩码值。
IPv6 Uplink	选择 WAN 端口。
启用登录页面	启用后在连接到此网络组的 Wi-Fi 时启用登录页面。这将允许用户设置登录网址，用户将自动重定向到配置的网址。
登录页面 URL	连接到网络组的 Wi-Fi 后，设置客户端将被重定向到的目标网页地址。

- **Wi-Fi：**参照下表区域 Wi-Fi 设置选项。

表 18: Wi-Fi

启用 Wi-Fi	选择是否在该网络组启用 Wi-Fi。
SSID	设置或修改 SSID 名称。
隐藏 SSID	选择隐藏 SSID。

	扫描 Wi-Fi 时，SSID 不可见，将设备连接到隐藏的 SSID，用户需要手动指定 SSID 名称和身份验证密码。
安全模式	设置加密的安全模式，有 5 个选项可用： ● WEP 64 位：使用静态 WEP 密钥。 字符只能为 0-9 或长度为 10 的 A-F，或长度为 5 的可打印 ASCII 字符。 ● WEP 128 位：使用静态 WEP 密钥。 字符只能为 0-9 或长度为 26 的 A-F，或长度为 13 的可打印 ASCII 字符。 ● WPA / WPA2：使用“PSK”或“802.1x”作为 WPA 密钥模式，使用“AES”或“AES / TKIP”加密类型。 ● WPA2：使用“PSK”或“802.1x”作为 WPA 密钥模式，使用“AES”或“AES / TKIP”加密类型。 建议用于认证的配置。 ● 打开：不需要密码。 用户将被连接而不进行身份验证。 不推荐出于安全考虑。
使用 MAC 过滤	选择黑/白名单指定要排除/包含连接到区域的 Wi-Fi MAC 地址。默认为禁用。
客户端隔离	客户端隔离功能通过 GWN76xx WiFi 接入点阻止连接的无线客户端之间的任何 TCP/IP 连接。客户端隔离有助于增强访客网络/公共 Wi-Fi 的安全性。 如果启用，则必须在“网关 MAC 地址”字段下指定默认的 LAN 网关的 MAC 地址。 客户端无法发现，ping 或访问连接到 GWN7000 网络组的其他无线设备，并且只能访问默认网关。 如果禁用，客户端将可以完全访问连接到网络的任何设备，包括网络组中的无线客户端。默认为“禁用”。
MAC 白名单/黑名单	添加客户端隔离的设备的黑白名单 MAC 地址
开启 RSSI	启用 RSSI 功能， AP 在最小 RSSI（dBm）情况下将断开低于配置阈值的用户。
最小 RSSI（dBm）	输入最小 RSSI 值，单位：dBm。 如果信号值低于配置的最小值，客户端将被断开。 输入范围为“-94”或“-1”。

- **设备管理**：用于添加或删除配对网络组中的接入点。

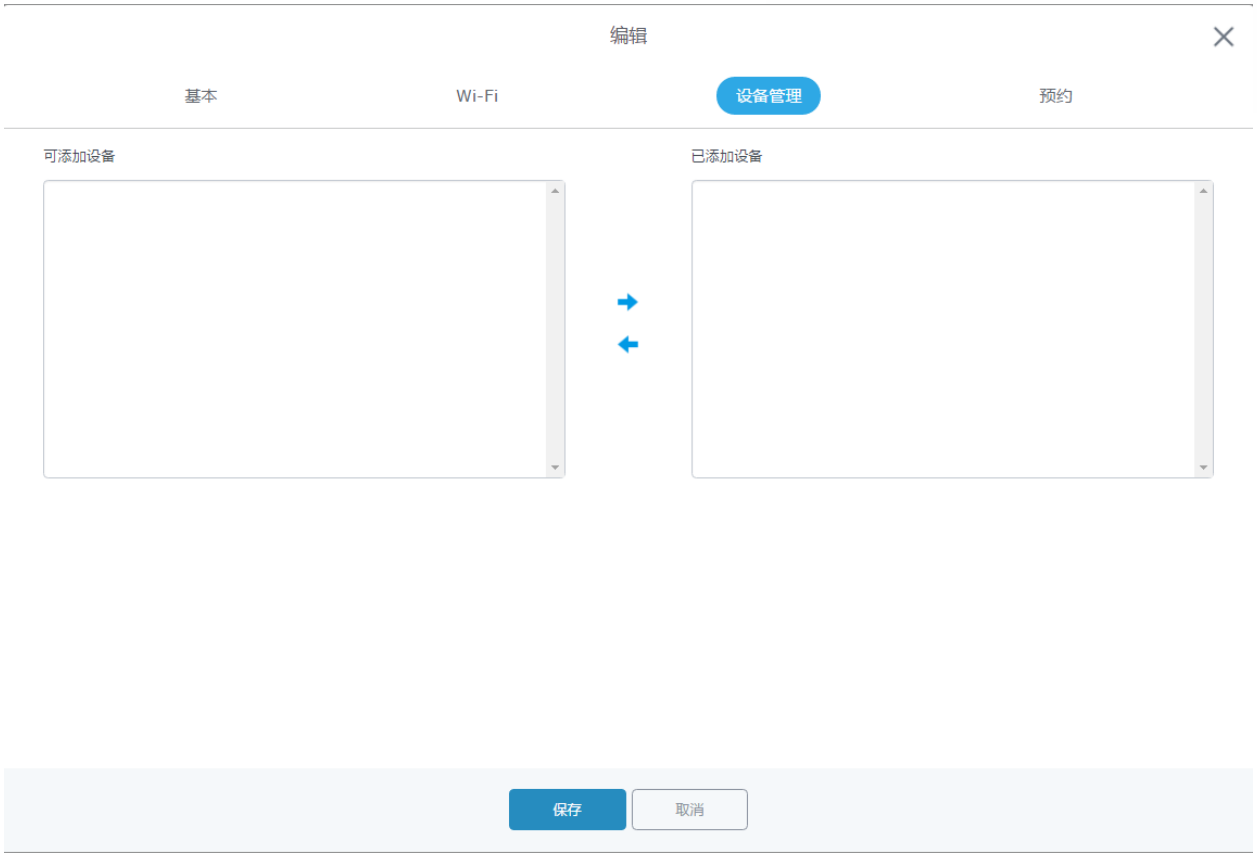


图 17: 设备管理

点击 添加 GWN76xx 至网络组，点击 移除。

用户也可以在接入点页面添加设备至网络组：

-选择想要添加到网络组的 AP，点击 添加到网络组

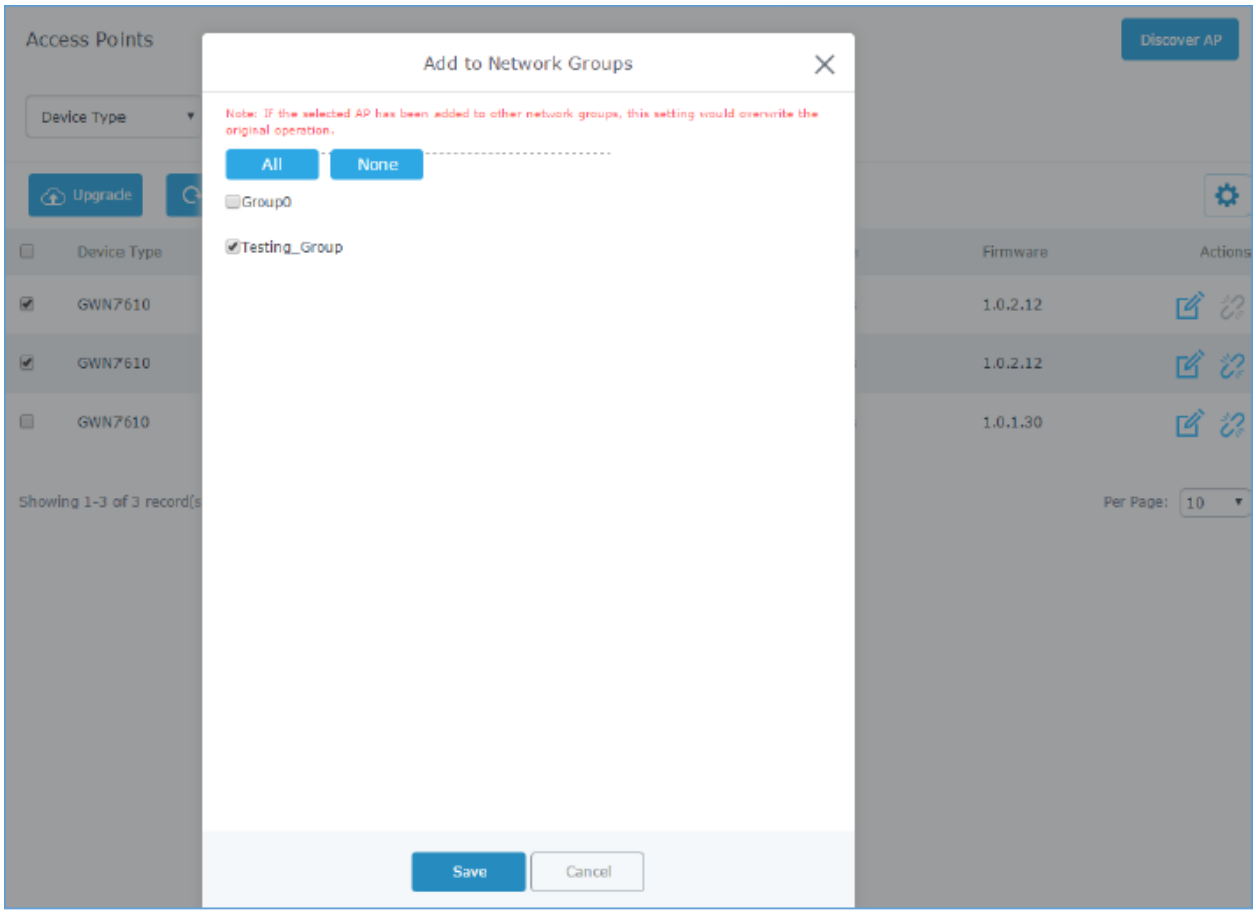


图 18: 接入点页面添加 AP 至网络组

选择所需的网络，其中将添加所选的 AP，如上图所示。

创建 SSID

在网络组页面下，单击以编辑网络组或创建新的网络组，然后转到 Wi-Fi 选项卡。

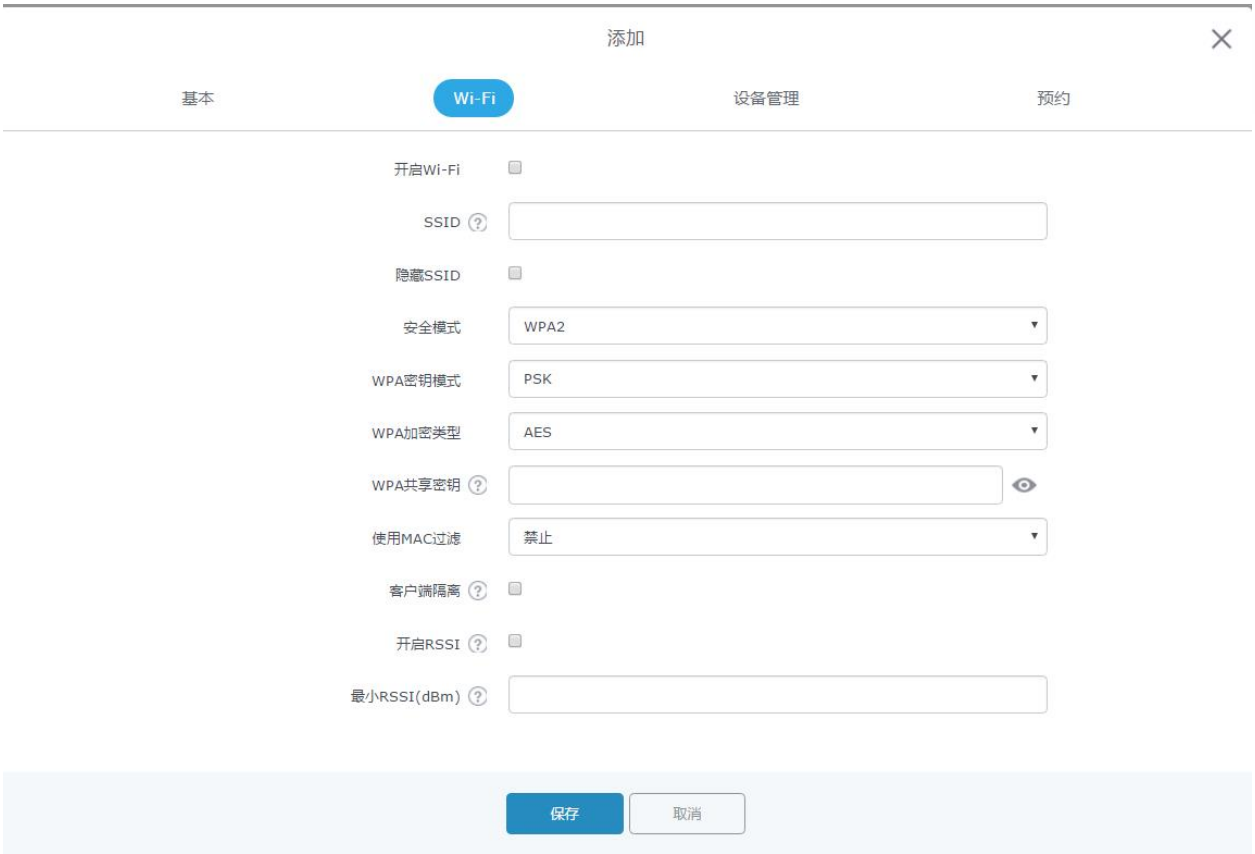


图 19: 创建 SSID

有关 Wi-Fi 选项，请参阅[表 18：Wi-Fi]。

相同网络组下的额外 SSID

用户还可以在同一组下创建一个额外 SSID。
要创建额外 SSID，请转到**网络组->额外 SSID**。

图 20:额外 SSID

从“网络组成员资格”下拉菜单中选择一个可用的网络组；这将创建一个附加的 SSID，并在创建主网络组时配置相同的设备成员。

图 21:额外 SSID 创建

点击 删除额外 SSID，点击 进行编辑。

客户端配置

客户端

客户连接到不同区域均可以显示和管理。管理员可以在 GWN7000 的 **Web 页面 -> 客户端**访问客户列表执行不同的操作。

GWN7000 企业级路由器内嵌 DHCP 服务器，启用 LAN 端口级别，会自动分配 IP 地址给设备如电脑或 GWN76xx 接入点和已经连接到 GWN76xx 的无线客户端。

图 22: 客户端

点击 查看客户端状态或修改其配置。

状态

图 23: 客户端状态

编辑 IP 和名称

用户可以为客户端设置名字或静态 IP

图 24: 客户端配置

阻止客户端

点击 将阻塞一个客户端，完成该操作后被阻塞的客户端将自动添加到**路由器->端口->全局设置**，禁止的客户端列表中。

图 25: 阻塞客户端

要取消禁用客户端，请转到**路由器->端口->全局设置**。 点击 将其从禁止列表中删除。

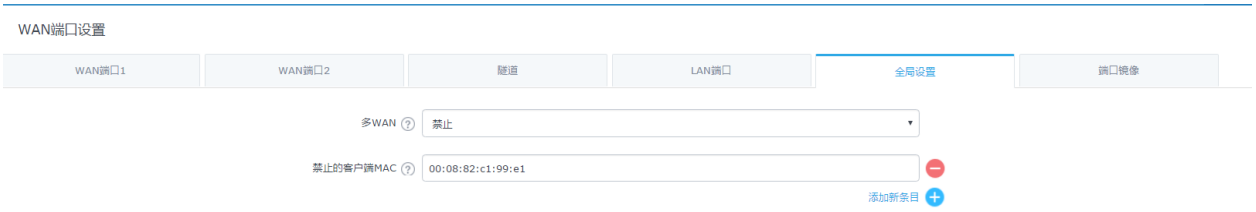


图 26: 取消禁用客户端

VPN（虚拟私有网络）

概览

VPN 允许GWN7000 连接到一个远程VPN服务器（使用PPTP, L2TP and OpenVPN协议），用户可以在GWN7000 **Web页面** -> **VPN**访问VPN页面。

OpenVPN ®服务器配置

要使用 GWN7000 作为 OpenVPN®服务器，用户需要创建 OpenVPN®证书和客户端证书。在生成服务器/客户端证书之前，用户应首先生成 CA 证书，这将有助于发布服务器/客户端证书。
GWN7000 证书可以从 **WebGUI - >系统设置 - >证书管理**进行管理。

生成 CA 证书

证书颁发机构（CA）是一个值得信赖的实体，它发布电子文档用于验证互联网上的数字实体身份。电子文件（a.k.a.数字证书）是安全通信的重要组成部分，并在公钥基础设施（PKI）中发挥重要作用。
要创建证书颁发机构（CA），请执行以下步骤：

1. 登录 GWN7000 Web 页面导航至**系统设置->证书管理->CAs**。
2. 点击 

按钮，将出现一个提示窗口。
3. 根据您的需要输入 CA 值，包括 CN，密钥长度和摘要算法等。
   参见下图配置示例，下表显示了所有可用的选项及其各自的描述。

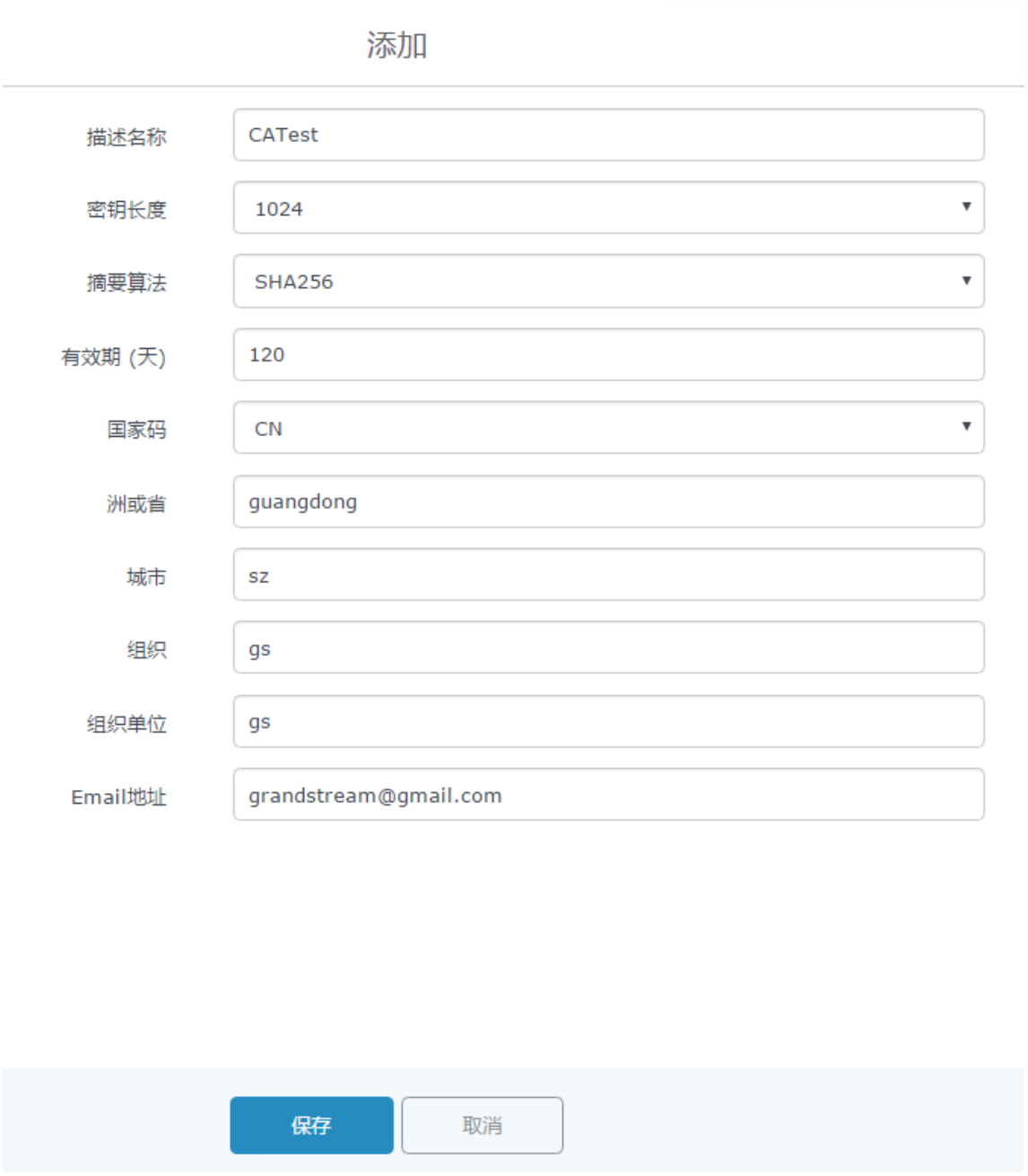


图 27: 创建 CA 证书

表 19: CA 证书

选项	描述
描述名称	输入 CA 的名称。 它可以是识别此证书的任何名称。 例如：“CATest”。

密钥长度	选择生成 CA 证书的密钥长度。 以下值可用： ● 1024：1024 位的密钥不再足以防止攻击。 ● 2048：2048 位密钥是一个很好的最小值（推荐）。 ● 4096：几乎所有 RSA 系统都接受 4096 位的密钥。 使用 4096 位密钥将显着增加 TLS 操作的生成时间，TLS 握手延迟和 CPU 使用情况。
摘要算法	选择摘要算法： ● SHA1：该摘要算法提供基于任意长度输入的 160 位输出。 ● SHA-256：该摘要算法生成一个几乎唯一的，固定大小的 256 位（32 字节）散列。 哈希是单向函数 - 它不能被解密。
有效期（天）	输入 CA 证书的有效期，以天为单位，默认为 120 天。
国家码	从下拉菜单中选择国家代码，如：“MA”。
洲或省	输入洲名称或省名称。 如：“guangdong”。
城市	输入城市名称。 如：“sz”。
组织	输入组织名称。 如：“gs”。
组织单位	输入组织单位。 如“gs”。
Email 地址	输入 email 地址。 如：grandstream@gmail.com。

4. 在设置完所有 CA 的选项后点击 保存 。

5. 点击 导出 CA 证书至本地，CA 默认扩展名为“.crt”。

图 28: CA 证书

生成服务器/客户端证书

用户需要创建服务器和客户端证书，用于客户端和作为 OpenVPN®服务器的 GWN7000 之间的加密通信。

- **创建服务器证书**

  请按照一下步骤创建服务器证书：

  1. 导航至“**系统设置->证书管理->证书**”。
  2. 点击 

按钮，将出现一个提示窗口。

  参见下图配置示例，下表显示了所有可用的选项及其各自的描述。

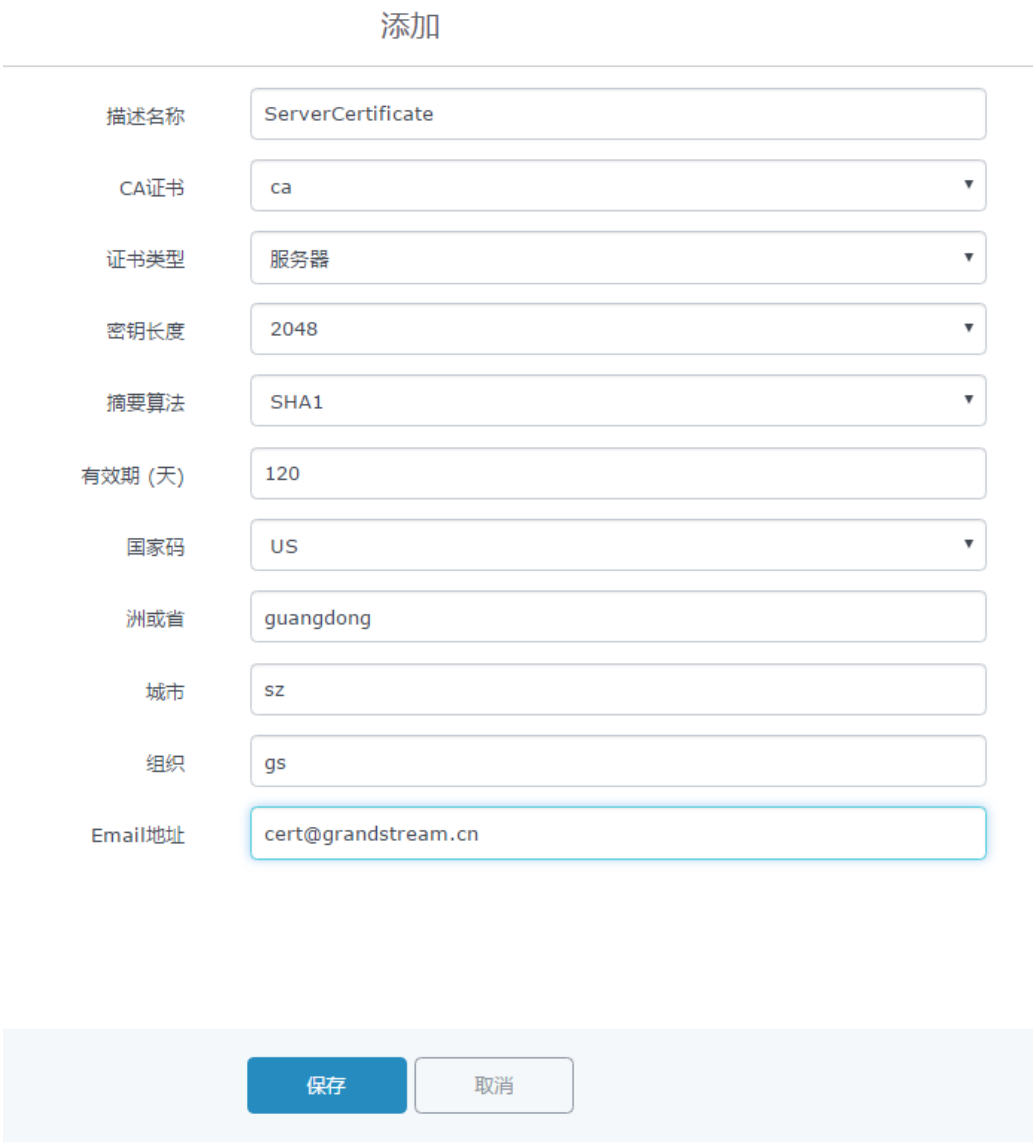


图 29: 创建服务器证书

表 20:服务器证书

选项	描述
描述名称	输入 CA 的名称。 它可以是识别此证书的任何名称。 例如：“CATest”。
CA 证书	从下拉列表中选择先前生成的 CA 证书。 例如：“CATest”。
证书类型	从下拉列表中选择证书类型。 它可以是客户端或服务器证书。 选择“服务器”生成服务器证书。
密钥长度	选择生成 CA 证书的密钥长度。 以下值可用： ● 1024：1024 位的密钥不再足以防止攻击。 ● 2048：2048 位密钥是一个很好的最小值（推荐）。 ● 4096：几乎所有 RSA 系统都接受 4096 位的密钥。 使用 4096 位密钥将显着增加 TLS 操作的生成时间，TLS 握手延迟和 CPU 使用情况。
摘要算法	选择摘要算法： ● SHA1：该摘要算法提供基于任意长度输入的 160 位输出。 ● SHA-256：该摘要算法生成一个几乎唯一的，固定大小的 256 位（32 字节）散列。 哈希是单向函数 - 它不能被解密。
有效期（天）	输入 CA 证书的有效期，以天为单位，默认为 120 天。
国家码	从下拉菜单中选择国家代码，如：“MA”。
洲或省	输入洲名称或省名称。 如：“guangdong”。
城市	输入城市名称。 如：“sz”。
组织	输入组织名称。 如：“gs”。
Email 地址	输入 email 地址。 如：cert@grandstream.cn。

3. 在设置完所有 CA 的选项后点击 保存。

点击 以“.crt”格式导出服务器证书文件。

点击 以“.key”格式导出服务器密钥。

如果不再需要，单击  按钮撤消服务器证书。

注意：

- GWN7000 作为服务器时，将使用服务器证书（.crt 和.key）。
- 服务器证书（.crt 和.key）可以导出并在其他 OpenVPN®服务器上使用。

◆ **创建客户端证书**

请按照以下步骤创建客户端证书：

1- 创建用户

a. 导航至“系统设置->用户管理”。

b. 点击 

将出现以下窗口。

图 30: 用户管理

c.输入用户信息如下表所示。

选项	描述
开启	选择是否使用该用户。
全称	输入全称用于识别该用户。
用户名	输入用户名用于识别客户端证书。
密码	设置用户密码。

IPsec 预共享密钥	输入预共享密钥以连接到 VPN 服务器。 当客户端使用预共享密钥时，将使用此字段。

d.为所有用户重复以上步骤。

2-创建客户端证书

a. 导航至“系统设置->证书管理->证书”。

b. 点击 

按钮，将弹出以下窗口。

c. 输入客户端证书信息如下表所示。

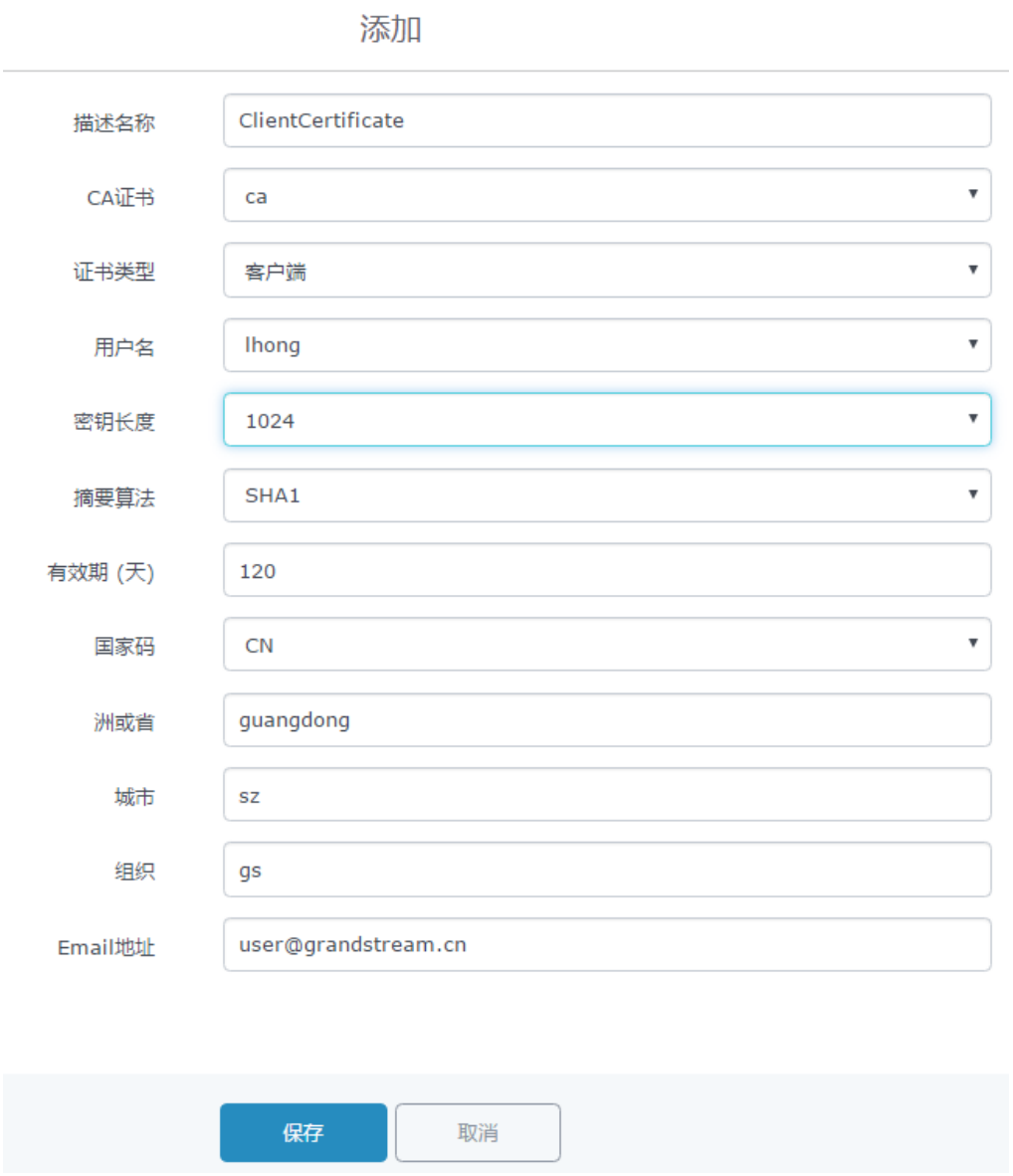


图 31: 客户端证书

表 21:客户端证书

选项	描述
描述名称	输入 CA 的名称。 它可以是识别此证书的任何名称。 例如：“ClientCertificate”。
CA 证书	从下拉列表中选择先前生成的 CA 证书。 例如：“CATest”。
证书类型	从下拉列表中选择证书类型。 它可以是客户端或服务器证书。 选择“客户端”生成客户端证书。
密钥长度	选择生成 CA 证书的密钥长度。 以下值可用： ● 1024：1024 位的密钥不再足以防止攻击。 ● 2048：2048 位密钥是一个很好的最小值（推荐）。 ● 4096：几乎所有 RSA 系统都接受 4096 位的密钥。 使用 4096 位密钥将显着增加 TLS 操作的生成时间，TLS 握手延迟和 CPU 使用情况。
摘要算法	选择摘要算法： ● SHA1：该摘要算法提供基于任意长度输入的 160 位输出。 ● SHA-256：该摘要算法生成一个几乎唯一的，固定大小的 256 位（32 字节）散列。 哈希是单向函数 - 它不能被解密。
有效期（天）	输入 CA 证书的有效期，以天为单位，默认为 120 天。
国家码	从下拉菜单中选择国家代码，如：“MA”。
洲或省	输入洲名称或省名称。 如：“guangdong”。
城市	输入城市名称。 如：“sz”。
组织	输入组织名称。 如：“gs”。
Email 地址	输入 email 地址。 如：user@grandstream.cn。

d.在设置完所有客户端的选项后点击 保存。

e.点击 以“.crt”格式导出客户端证书文件。

f.点击 以“.key”格式导出客户端密钥。

如果不再需要，单击按钮撤消客户端证书。

客户端证书（“.crt”和“.key”）将被连接到 GWN7000 的客户端使用，以建立 TLS 握手。

注意：

- 从 GWN7000 生成的客户端证书需要上传到客户端。
- 为了提高安全性，每个客户端都需要拥有自己的用户名和证书，即使用户受到威胁，其他用户也不会受到影响。

创建 OpenVPN®服务器

一旦成功创建客户端和服务器证书，用户可以创建一个新的服务器，以便客户端通过“VPN>OpenVPN®>服务器”导航来连接。

要创建一个新的 VPN 服务器，请按照下列步骤操作：

1. 点击 添加 将出现以下窗口。

图 32: 创建 OpenVPN®服务器

表 22: OpenVPN®服务器

选项	描述
开启	选择是否开启 OpenVPN 服务器功能。
VPN 名称	输入 OpenVPN 服务器名称
服务器模式	选择 OpenVPN 服务器模式，4 种模式可选： ● **PSK**：用于建立点对点 OpenVPN®配置。 将创建具有指定 IP 的服务器端点和指定 IP 的客户端端点的 VPN 隧道。 客户端和服务器之间的加密通信将通过 UDP 端口 1194（默认的 OpenVPN®）端口进行。 ● **SSL**：仅使用证书进行身份验证（无用户/通行验证）。 每个用户都有一个唯一的客户端配置，包括他们的个人证书和密钥。 如果客户端不被提示输入用户名和密码，它是非常有用的，但由于需要依赖用户所拥有的东西（TLS 密钥和证书），它相较于其他方式缺少安全性。 ● **用户认证**：认证仅使用 CA，用户和密码，无证书。 如果客户没有单独的证书，那么很有用。 较不安全，因为它依赖于共享的 TLS 密钥加上用户所知道的信息（用户名/密码）。 ● **SSL +用户认证**：需要证书和用户名/密码。 每个用户都有一个唯一的客户端配置，包括他们的个人证书和密钥。 最安全的，因为有多个身份验证因素（用户拥有的 TLS 密钥和证书）以及他们知道的用户名/密码。
协议	从下拉列表中选择传输协议，TCP 或 UDP。 默认协议是 UDP。
接口	选择 GWN7000 用于连接上游的接口，WAN1，WAN2 或 All。
本地端口	配置 OpenVPN®服务器的监听端口。 默认值为 1194。
加密算法	从下拉列表中选择加密算法，以便加密数据，以便接收方可以使用相同的算法进行解密。
摘要算法	从下拉列表中选择摘要算法，它将唯一标识数据以提供数据完整性，并确保接收器具有来自原始主机发送的数据的未修改数据。
TLS 身份验证	该选项使用静态预共享密钥（PSK），它必须提前生成并在所有对等体之间共享。此功能通过要求传入数据包具有使用 PSK 密钥生成的有效签名，为 TLS 通道增加了额外的保护。
TLS 预共享密钥	使用 TLS 验证时输入生成的 TLS 预共享密钥。
证书权威	从下拉菜单中选择生成的 CA 证书。

服务器证书	从下拉菜单中选择生成的服务器证书。
IPv4 隧道网络	输入 GWN7000 将从 OpenVPN®客户端提供的网络范围。 注意：网络格式应为 10.0.10.0/16。 掩码应至少为 16 位。
重定向网关	当使用重定向网关时，OpenVPN®客户端将通过 VPN 路由 DNS 查询，VPN 服务器将需要处理它们。
自动防火墙规则	启用自动防火墙规则
组内流量自动转发	如果启用，请选择要转发的组，否则，需要在防火墙设置下手动配置转发规则。
LZO 压缩	选择是否激活 LZO 压缩，如果设置为“自适应”，则服务器将决定是否启用此选项。
允许对端改变 IP	允许远程更改 IP 和/或端口，通常适用于远程 IP 地址频繁更改的情况。

2. 配置完所有选项后点击 保存 。
3. 点击页面上方“应用”应用修改。

图 33: OpenVPN®

OpenVPN®客户端配置

GWN7000 充当 OpenVPN®客户端和服务器，一旦创建了用户和客户端证书，请导航至“VPN>OpenVPN®>客户端”，并按照以下步骤操作：

1. 点击 添加 将会出现以下窗口。

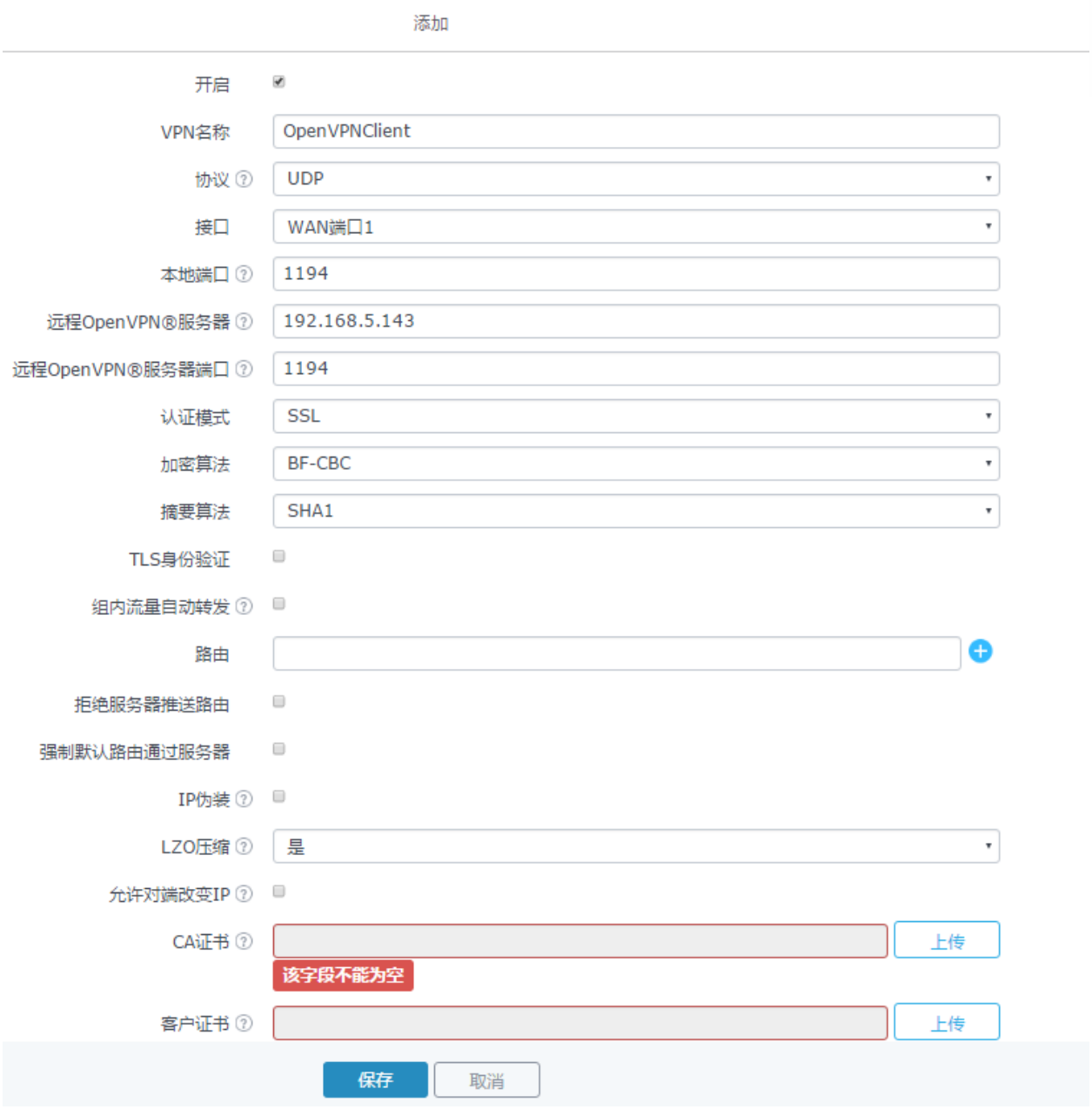


图 34: OpenVPN®客户端

表 23: OpenVPN®客户端

选项	描述
开启	选择是否开启 OpenVPN 服务器功能。
VPN 名称	输入 OpenVPN 服务器名称

协议	从下拉列表中选择传输协议，TCP 或 UDP。 默认协议是 UDP。
接口	选择 GWN7000 用于连接上游的接口，WAN1，WAN2 或 All。
本地端口	配置 OpenVPN®服务器的监听端口。 默认值为 1194。
远程 OpenVPN®服务器	配置远程 OpenVPN®服务器 IP 地址。
远程 OpenVPN®服务器端口	配置远程 OpenVPN®服务器端口。
认证模式	选择 OpenVPN 服务器模式，4 种模式可选： ● **PSK**：用于建立点对点 OpenVPN®配置。 将创建具有指定 IP 的服务器端点和指定 IP 的客户端端点的 VPN 隧道。 客户端和服务器之间的加密通信将通过 UDP 端口 1194（默认的 OpenVPN®）端口进行。 ● **SSL**：仅使用证书进行身份验证（无用户/通行验证）。 每个用户都有一个唯一的客户端配置，包括他们的个人证书和密钥。 如果客户端不被提示输入用户名和密码，它是非常有用的，但由于需要依赖用户所拥有的东西（TLS 密钥和证书），它相较于其他方式缺少安全性。 ● **用户认证**：认证仅使用 CA，用户和密码，无证书。 如果客户没有单独的证书，那么很有用。 较不安全，因为它依赖于共享的 TLS 密钥加上用户所知道的信息（用户名/密码）。 ● **SSL +用户认证**：需要证书和用户名/密码。 每个用户都有一个唯一的客户端配置，包括他们的个人证书和密钥。 最安全的，因为有多个身份验证因素（用户拥有的 TLS 密钥和证书）以及他们知道的用户名/密码。
加密算法	从下拉列表中选择加密算法，以便加密数据，以便接收方可以使用相同的算法进行解密。
摘要算法	从下拉列表中选择摘要算法，它将唯一标识数据以提供数据完整性，并确保接收器具有来自原始主机发送的数据的未修改数据。
TLS 身份验证	该选项使用静态预共享密钥（PSK），它必须提前生成并在所有对等体之间共享。此功能通过要求传入数据包具有使用 PSK 密钥生成的有效签名，为 TLS 通道增加了额外的保护。
TLS 预共享密钥	使用 TLS 验证时输入生成的 TLS 预共享密钥。
组内流量自动转发	如果启用，请选择要转发的组，否则，需要在防火墙设置下手动配置转发规则。
路由	添加您需要的路由。

拒绝服务器推送路由	若启用，客户端会忽略服务器推送的路由。
强制默认路由通过服务器	强制默认路由通过服务器。
IP 伪装	此功能是一种网络地址转换（NAT）形式，允许内部计算机在网络外部没有已知地址的情况与外部通信。 它允许一台机器代表其他机器。
LZO 压缩	选择是否激活 LZO 压缩，如果设置为“自适应”，则服务器将决定是否启用此选项。
允许对端改变 IP	允许远程更改 IP 和/或端口，通常适用于远程 IP 地址频繁更改的情况。
CA 证书	点击“上传”，然后选择以前在本设备中生成的“CA”证书。
客户端证书	点击“上传”，然后选择以前在本设备中生成的“客户端证书”。
客户端私钥	点击“上传”，然后选择以前在本设备中生成的“客户端私钥”。
客户端私钥密码	输入客户端私钥密码。

2. 配置完所有选项后点击 保存 。
3. 点击页面上用的“应用”应用修改。

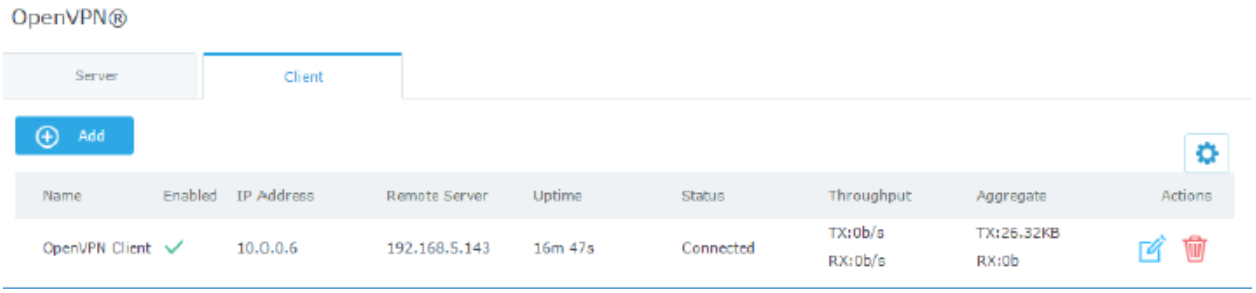


图 35: OpenVPN®客户端

L2TP/IPsec 配置

第二层隧道协议（L2TP）是用于支持虚拟专用网（VPN）或作为 ISP 提供服务的一部分的隧道协议。 它本身不提供任何加密或机密性。 相反，它依赖于它在隧道内通过的加密协议来提供隐私保护。

GWN7000 L2TP/IPsec 客户端配置

要在 GWN7000 上配置 L2TP 客户端，请导航至“VPN - > L2TP / IPSec”，并设置以下内容：

1- 点击 添加 ，将出现以下界面。

图 36: L2TP 客户端配置

表 24: L2TP 配置

选项	描述
开启	选择是否开启 L2TP 客户端功能。
VPN 名称	输入 L2TP 名称
WAN 端口	选择 GWN7000 用于连接上游的接口，WAN1 或 WAN2。
远程 L2TP 服务器	配置远程 L2TP 服务器。
用户名	输入用于 VPN 服务器认证的用户名。

密码	输入用户 VPN 服务器认证的密码。
连接方式	选择传输或隧道方式： ● 传输模式通常用于在网关被视为主机的清醒下，终端站之间或端站与网关之间的交互。 ● 隧道模式用于网关之间，或在终端站到网关，网关作为代理服务器后台的主机。
预共享密钥	输入 L2TP 预共享密钥。
组内流量自动转发	如果启用，请选择要转发的组，否则，需要在防火墙设置下手动配置转发规则。
对端子网范围	配置 VPN 的远程子网。 格式应为“IP /掩码”，其中 IP 可以是 IPv4 或 IPv6，掩码是 1 到 32 之间的数字。 例如：192.168.5.0/24
使用隧道作为默认路由	启用此选项，默认使用 L2TP / IPSec VPN 隧道。
IP 伪装	此功能是一种网络地址转换（NAT）形式，允许内部计算机在网络外部没有已知地址的情况与外部通信。 它允许一台机器代表其他机器。
使用服务器 DNS	选择是否使用服务器给定的 DNS。
尝试重新连接数	配置重新连接 L2TP 客户端的次数，如果超过该次数，客户端将与 L2TP / IP 服务器断开连接。
利用内置 IPv6 管理	选择是否启用 IPv6 管理。
端口转发规则	设置端口转发规则。
端口触发规则	设置端口触发规则。

2- 配置完成后点击 保存 。

3- 点击页面上方的 应用 应用修改。

图 37: L2TP 客户端

PPTP 配置

基于点对点协议（PPP）并由微软开发的用于广域网（WAN）的数据链路层协议，使得网络流量能够通过诸如因特网等不安全的公共网络进行封装和路由。 点对点隧道协议（PPTP）允许创建虚拟专用网络（VPN），通过互联网来传输 TCP / IP 数据。

GWN7000 客户端配置

要在 GWN7000 上配置 PPTP 客户端，请导航至“**VPN-> PPTP**”，并设置以下内容：

1- 点击 添加，将出现以下界面。

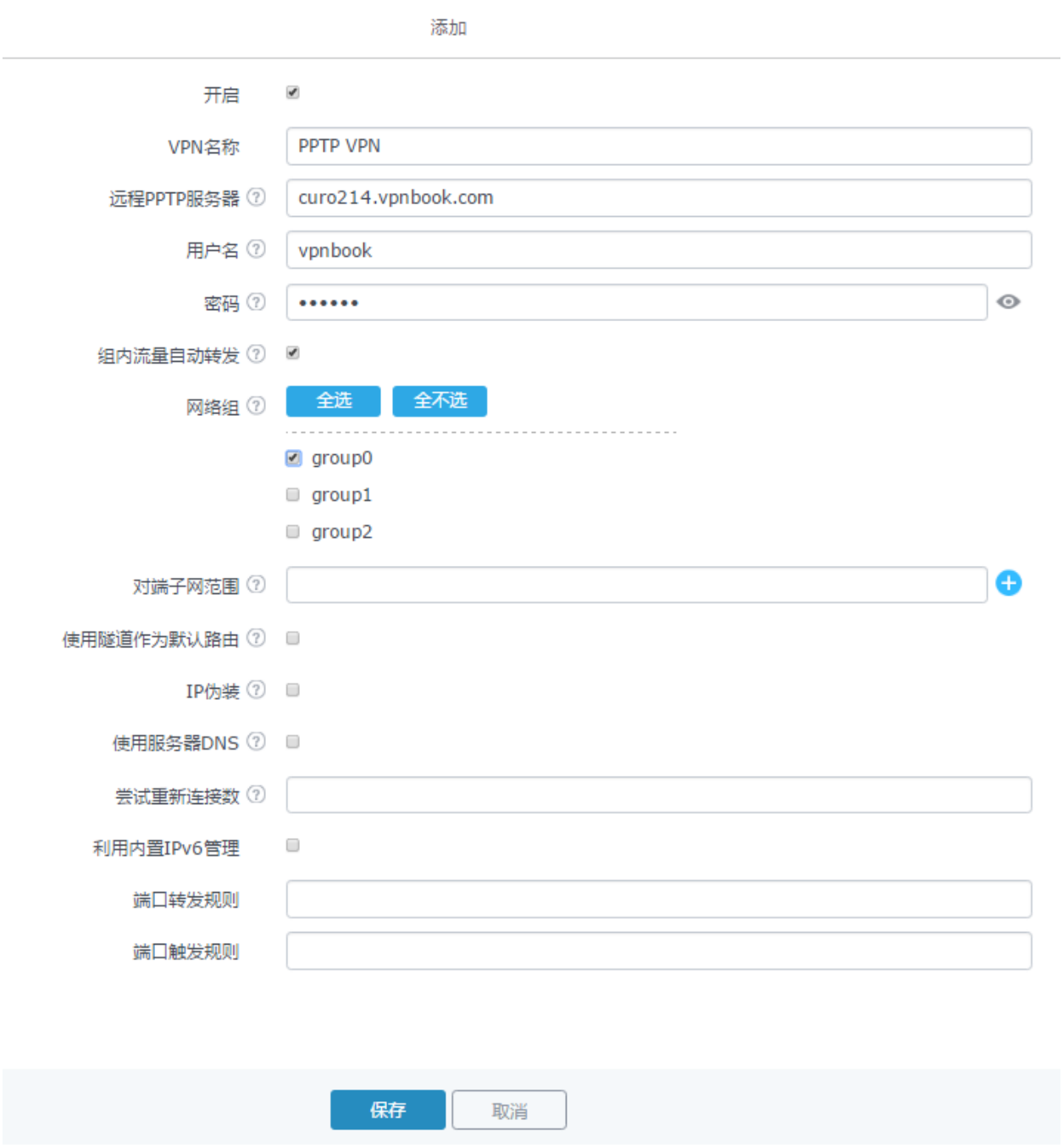


图 38:PPTP 客户端配置

表 25: PPTP 配置

选项	描述
开启	选择是否开启 PPTP 客户端功能。
VPN 名称	输入 PPTP 客户端名称
远程 PPTP 服务器	配置远程 PPTP 服务器。
用户名	输入用于 VPN 服务器认证的用户名。
密码	输入用户 VPN 服务器认证的密码。
组内流量自动转发	如果启用，请选择要转发的组，否则，需要在防火墙设置下手动配置转发规则。
对端子网范围	配置 VPN 的远程子网。 格式应为“IP /掩码”，其中 IP 可以是 IPv4 或 IPv6，掩码是 1 到 32 之间的数字。 例如：192.168.5.0/24
IP 伪装	此功能是一种网络地址转换（NAT）形式，允许内部计算机在网络外部没有已知地址的情况与外部通信。 它允许一台机器代表其他机器。
使用服务器 DNS	选择是否使用服务器给定的 DNS。
尝试重新连接数	配置重新连接 L2TP 客户端的次数，如果超过该次数，客户端将与 L2TP / IP 服务器断开连接。
利用内置 IPv6 管理	选择是否启用 IPv6 管理。
端口转发规则	设置端口转发规则。
端口触发规则	设置端口触发规则。

2- 配置完成后点击 保存 。

3- 点击页面上方的 应用 应用修改。

图 39:PPTP 客户端

防火墙

GWN7000 支持防火墙功能，通过限制或拒绝特定流量来控制进出流量，并通过防御网络攻击增强设备的安全性。

防火墙功能包括 3 个菜单：

- **基本：**用于启用SYN Flood，设置端口转发，DMZ，组间流量转发和UPnP。
- **流量规则：**用于在自定义的计划时间内控制进/出流量，并对指定的规则执行操作，如接受，拒绝和丢弃
- **高级：**用于设置SNAT和DNAT。

基本

一般设置

用户可以通过启用“SYN Flood 保护”来避免 DOS 攻击。

默认情况下，在 GWN7000 上启用 SYN Flood 保护功能，用户可以编辑 SYN Flood 攻击速率限制和 SYN Flood 爆炸极限，以及是否丢弃无效数据包，如下图所示

图 40:基本->一般设置

端口转发

用户可以为 LAN 客户端设置端口转发，允许将通信请求从一个地址和端口号组合重定向到另一个。

- 点击 

增加端口转发规则。
- 点击  编辑端口转发规则。
- 点击  删除端口转发规则。

图 41:端口转发

编辑或创建端口转发规则，请参阅下表：

表 26: 端口转发

名称	指定端口转发规则名称。
开启	选择是否使用此端口转发规则
协议	选择协议，用户可以选择 TCP,UDP 或 TCP/UDP。
源组	选择 WAN 端口。
源端口	设置源端口号。
目标组	选择 LAN 端口。
目标地址	设置目标 IP 地址。
目标端口	设置目标端口。

DMZ

GWN7000 支持 DMZ，用户可以 LAN 客户端置于 DMZ 上。

- 点击 

添加 IP 到 DMZ。
- 点击  编辑 DMZ。
- 点击  删除 DMZ。

图 42:DMZ

请参照下表设置 DMZ 选项：

表 27: 端口转发

名称	指定 DMZ 名称。
开启	选择是否使用此端口作为 DMZ 主机。

源组	选择 WAN 端口。
目标组	选择 LAN 端口。
目标地址	设置目标 IP 地址。

组内流量转发

GWN7000 提供了用户允许不同组和接口之间流量转发的可能性。
用户可以选择编辑源组，并向其中添加其他网络组和 WAN 接口，以允许所选成员之间的组间流量转发。

图 43:组内流量转发

单击 编辑源组，然后单击 以将组和接口添加到所选组，或单击 以从所选组中删除成员，如下图所示。

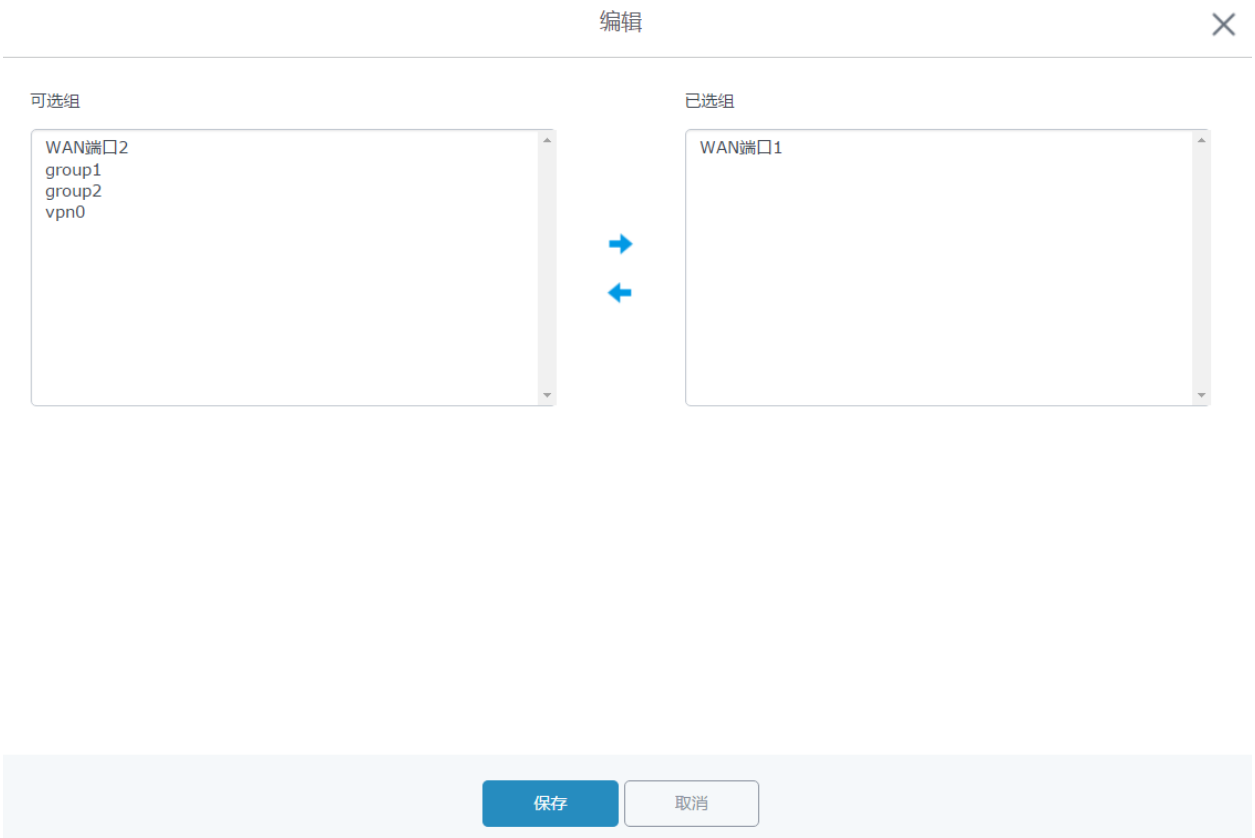


图 44:启用组内流量转发

UPnP

GWN7000 支持 UPnP，使主机上运行的程序可以自动配置端口转发。
UPnP 允许程序使 GWN7000 打开必要的端口，无需用户干预，而不进行任何检查。
用户可以从 GWN7000 **WebGUI->防火墙->基本-> UPnP** 设置中配置 UPnP 设置。
UPnP 设置请参见下表。

表 28: UPnP 设置

开启 UPnP 守护	选择是否开启 UPnP 守护。
外部接口	选择 WAN 接口以允许外部连接到启用 UPnP 的资源。
内部接口	选择使用 UPnP 的 LAN 端口网络组。
开启 UPnP	选择是否为所选网络组的 LAN 客户端开启 UPnP 功能。
开启 NAT-PMP	启用自动 NAT 端口映射（NAT-PMP）。
安全模式	选择是否在安全模式下激活 UPnP。
生成系统日志	选择是否生成 UPnP 系统日志。
下载速度	设置下载速度，以 KB/s 为单位，默认为 2048.
上传速度	设置上传速度，以 KB/s 为单位，默认为 1024.

流量规则设定

GWN7000 为用户提供了在定制安排的时间内完全控制不同协议的传入/传出流量的可能性，并为指定的规则采取措施如接受、拒绝和丢弃。
用户可以配置配置协议的输入，输出和转发规则。

- 点击 

添加流量规则。
- 点击  编辑规则。
- 点击  删除规则。

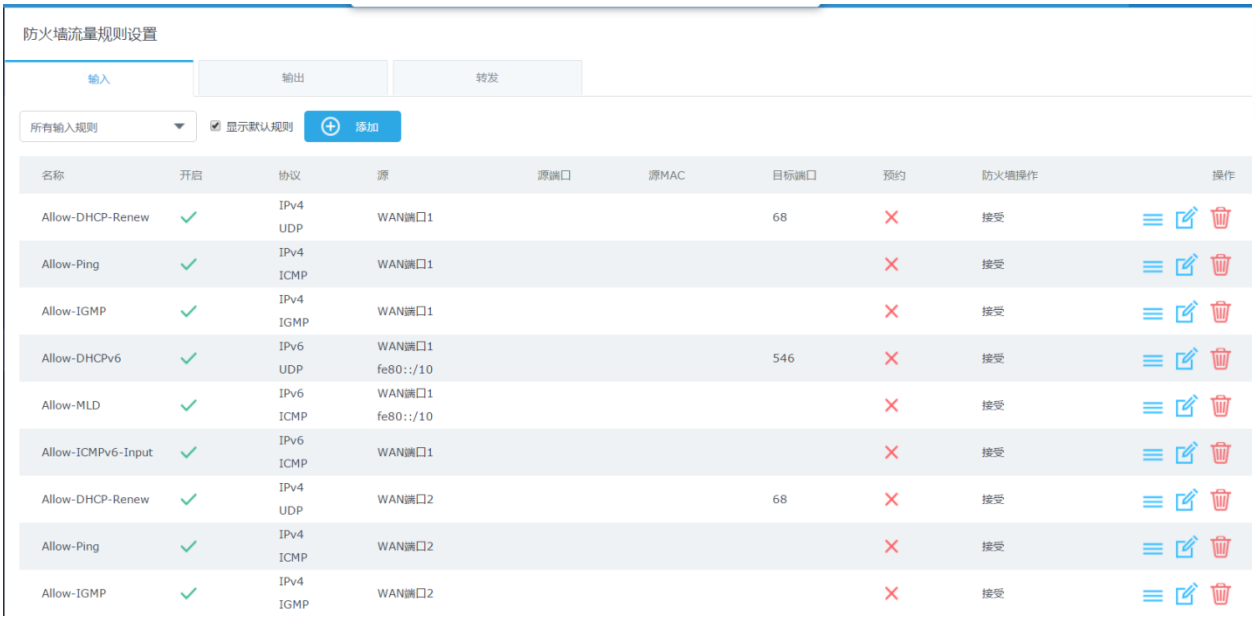


图 45:流量规则设置

请参照下表创建或编辑流量规则。

表 29: 防火墙流量规则

名称	指定流量规则名称。
开启	选择是否使用该规则。
IP 协议族	选择 IP 协议族，IPv4，IPv6 或 any
源组	为源组选择 WAN 接口或 LAN 组，用户还可以选择全部。
协议	从下拉列表或全部选择一个协议，可用选项有：UDP，TCP，TCP / UCP，UDP-Lite，ICMP，AH，SCTP，IGMP 和 All。
源 IP 地址	设置源 IP 地址，该地址可以 IPv4 或 IPv6 地址。
源端口	设置源端口号。
源 MAC 地址	设置源 MAC 地址。
目标端口	设置目标端口号。
预约开始日期	单击 图标以计划应用此规则的开始日期。
预约结束日期	单击 图标以计划应用此规则的结束日期。
预约开始时间	单击 图标以计划应用此规则的开始时间。
预约结束时间	单击 图标以计划应用此规则的结束时间。
工作日	选择要应用流量规则的日期，未选择的日期将忽略此规则。
月份日期	输入要应用流量规则的月份（以空格分隔）的日期。 示例：5 10 15

	这只适用于每月第 5，第 10 和第 15 天。
将时间值作为 UTC 而不是当地时间	检查使用 UTC 作为指定时间的时区，而不是使用 GWN7000 的本地时间。
防火墙操作	选择要针对给定流量规则执行的操作，有 3 个选项可用：接受，拒绝或丢弃。

防火墙高级设置

在此页面中，用户将能够为每个 WAN 接口和 LAN 组设置输入/输出策略；以及为静态和动态 NAT 设置配置。

一般设置

点击 WAN 接口或网络组旁边的  编辑其输入和输出策略。

请参照下表设置一般设置选项

表 30：防火墙-一般设置

输入策略	选择要应用于此接口/ LAN 组的所有输入流量的操作，可以使用 3 个操作：接受，拒绝和丢弃。
输出策略	选择要应用于此接口/ LAN 组的所有输出流量的操作，可以使用 3 个操作：接受，拒绝和丢弃。
IP 伪装	此功能是一种网络地址转换（NAT）形式，允许内部计算机在网络外部没有已知地址的情况与外部通信。 它允许一台机器代表其他机器。
MSS Clamping	检查以启用 MSS 夹紧。 这将提供一种在通信路径上的 MTU 值低于 MSS 值时防止分片的方法。
记录丢弃和拒绝流量到系统日志	检查发送所有被拒绝和丢弃的流量日志到配置的 Syslog 服务器。
丢弃和拒绝流量限度	指定丢弃和拒绝流量的限制。 值格式为 N / unit，其中 N 为数字，单位为秒，分，小时或天。

SNAT

用户可以在此页设置 SNAT。

- 点击  添加 SNAT 输入。
- 点击  编辑 SNAT 输入。
- 点击  删除 SNAT 规则。

请参照下表创建或编辑 SNAT 输入

表 31: SNAT

名称	指定 SNAT 输入名称。
开启	选择是否使用该 SNAT 输入。
IP 协议族	选择 IP 协议族，IPv4，IPv6 或 any
源组	为源组选择 WAN 接口或 LAN 组，用户还可以选择全部。
协议	从下拉列表或全部选择一个协议，可用选项有：UDP，TCP，TCP / UCP，UDP-Lite，ICMP，AH，SCTP，IGMP 和 All。
源 IP 地址	设置源 IP 地址，该地址可以 IPv4 或 IPv6 地址。
源端口	设置源端口号。
源 MAC 地址	设置源 MAC 地址。
目标端口	设置目标端口号。
预约开始日期	单击 图标以计划应用此规则的开始日期。
预约结束日期	单击 图标以计划应用此规则的结束日期。
预约开始时间	单击 图标以计划应用此规则的开始时间。
预约结束时间	单击 图标以计划应用此规则的结束时间。
工作日	选择要应用流量规则的日期，未选择的日期将忽略此规则。
月份日期	输入要应用流量规则的月份（以空格分隔）的日期。 示例：5 10 15 这只适用于每月第 5，第 10 和第 15 天。
将时间值作为 UTC 而不是当地时间	检查使用 UTC 作为指定时间的时区，而不是使用 GWN7000 的本地时间。

DNAT

用户可以在此页设置 DNAT。

- 点击 添加 添加 DNAT 输入。
- 点击 编辑 DNAT 输入。
- 点击 删除 DNAT 规则。

请参照下表创建或编辑 DNAT 输入

表 32: DNAT

名称	指定 SNAT 输入名称。
开启	选择是否使用该 SNAT 输入。
IP 协议族	选择 IP 协议族，IPv4，IPv6 或 any
源组	为源组选择 WAN 接口或 LAN 组，用户还可以选择全部。
协议	从下拉列表或全部选择一个协议，可用选项有：UDP，TCP，TCP / UCP，UDP-Lite，ICMP，AH，SCTP，IGMP 和 All。
源 IP 地址	设置源 IP 地址，该地址可以 IPv4 或 IPv6 地址。
源端口	设置源端口号。
源 MAC 地址	设置源 MAC 地址。
目标端口	设置目标端口号。
预约开始日期	单击 图标以计划应用此规则的开始日期。
预约结束日期	单击 图标以计划应用此规则的结束日期。
预约开始时间	单击 图标以计划应用此规则的开始时间。
预约结束时间	单击 图标以计划应用此规则的结束时间。
工作日	选择要应用流量规则的日期，未选择的日期将忽略此规则。
月份日期	输入要应用流量规则的月份（以空格分隔）的日期。 示例：5 10 15 这只适用于每月第 5，第 10 和第 15 天。
将时间值作为 UTC 而不是当地时间	检查使用 UTC 作为指定时间的时区，而不是使用 GWN7000 的本地时间。
开启 NAT 反射	检查以启用此 NAT 条目的 NAT 反射，以允许通过本地网络内的公共 IP 地址访问服务。

维护和调试

GWN7000 提供多种工具和选项进行维护和调试，帮助用户进一步对 GWN7000 资源进行故障排除和监控。

维护

用户可以从 GWN7000 WebGUI->系统设置 - >维护访问维护页面。
有关维护选项请参见下表。

表 33: 维护

基本	
国家	从下拉菜单中选择国家。
时区	为 GWN7000 配置时区，该选项需要重启生效。
NTP 服务器	配置 NTP 服务器的 IP 地址或 URL，GWN7000 将从该服务器获取日期和时间。
日期显示格式	更改日期显示格式，可以有三个选项 YYYY / MM / DD，MM / DD / YYYY 和 DD / MM / YYYY
升级	
认证配置文件	是否对配置文件进行验证，默认为否。
XML 配置文件密码	如果您使用 XML provision 方式进行配置文件更新，而且已经使用 Openssl 等加密工具对其进行了加密，该项将提供密码使得设备可以对下载的 XML 文件进行解密。
升级方式	指定固件和配置升级方式，3 中方式可选：HTTP,HTTPS 和 TFTP。
固件服务器	配置固件服务器的 IP 地址或 URL。
配置文件服务器	设置配置文件服务器的 IP 地址或 URL。
启动时检查/下载新固件	选择是否在重启后启用或禁用自动升级和配置。 默认为禁用。
自动更新	选择每隔一段时间/每天/每周自动升级，设备将根据配置时间自动请求升级。默认为“禁用”。
立即升级	单击升级，启动固件/配置文件配置。 请确保在点击升级之前保存并应用更改。
下载配置文件	点击下载设备当前配置。

上传配置文件	选择一个压缩配置文件包来恢复此配置，恢复成功后，设备将自动重启。
重启	点击重启按钮重启设备。
恢复出厂	将此设备和所有在线的 AP 都恢复出厂。
访问	
当前管理员密码	输入当前管理员密码。
管理员新密码	改变管理员密码。密码对大小写敏感，最大长度为 32 位。
确认管理员新密码	再次输入管理员新密码进行验证。
用户新密码	输入用户登录密码。密码对大小写敏感，最大长度为 32 位。
确认用户新密码	再次输入用户新密码进行验证。
系统日志	
系统日志服务器地址	系统日志服务器的 IP 地址或 URL。
系统日志级别	在下拉菜单中选择报告日志的级别。默认设置为 Debug。

调试

GWN7000 的 WebGUI 上的用户可以使用许多调试工具来检查状态并对 GWN7000 的服务和网络进行故障排除。

调试页面提供 4 个选项卡：抓包，Ping / 路由跟踪，Syslog 和 Nat Table。

抓包

该功能用于从 GWN7000 接口（WAN 端口和网络组）捕获数据包跟踪，以进行故障排除或监控。用户需要将 USB 设备插入 GWN7000 背面的其中一个 USB 端口。

点击 

启动抓包并将捕获的数据包存于连接到 GWN7000 USB 端口的存储设备。

点击 

停止抓包。

点击 

显示所选设备上的捕获文件，用户可以查看捕获文件的详细信息，点击 

删除所有文件，点击 
捕获文件旁边的文件将其下载到本地文件夹，或点击 
删除。

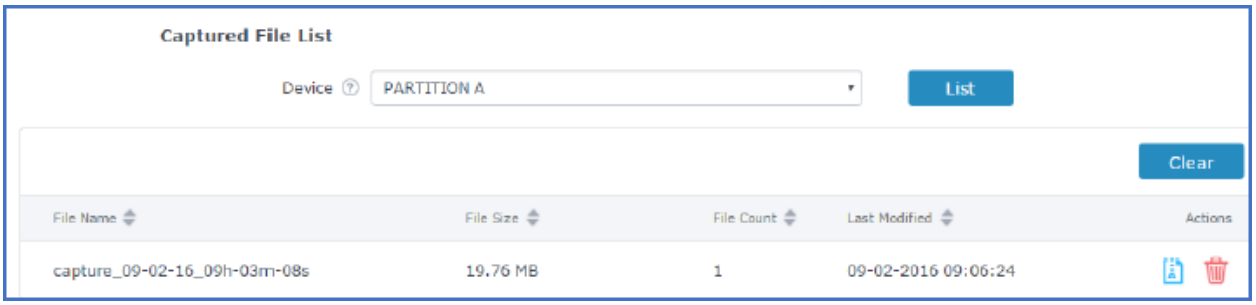


图 46:抓包文件

下表显示抓包的各个选项。

表 34: 调试-抓包

文件名	输入将要生成的抓包文件的名称。
接口	选择一个接口（WAN1 或 2 或网络组）开启抓包。
设备	选择一个接入到 USB 接口的设备存储抓包文件。
文件大小	设置抓包文件的大小（可选字段）。
循环次数	设置可创建的最大文件个数。
方向	设置要抓取的包的方向。
源端口	设置源端口以过滤捕获的数据。
目标端口	设置目标端口以过滤捕获的数据。
源地址	设置源地址以过滤捕获的数据。
目标地址	设置目标地址以过滤捕获的数据。
协议	选择所有或特定协议来捕获数据包（IP，ARP，RARP，TCP，UDP，ICMP，IPv6）

Ping/路由跟踪

Ping 和路由跟踪是有用的调试工具，用于验证网络（WAN 或 LAN）中的其他客户端的可达性。 GWN7000 提供了用于 IPv4 和 IPv6 协议的 Ping 和路由跟踪工具。

要使用这些工具，请转到 GWN7000 **WebGUI->系统设置->调试**，然后单击 **Ping / 路由跟踪**。

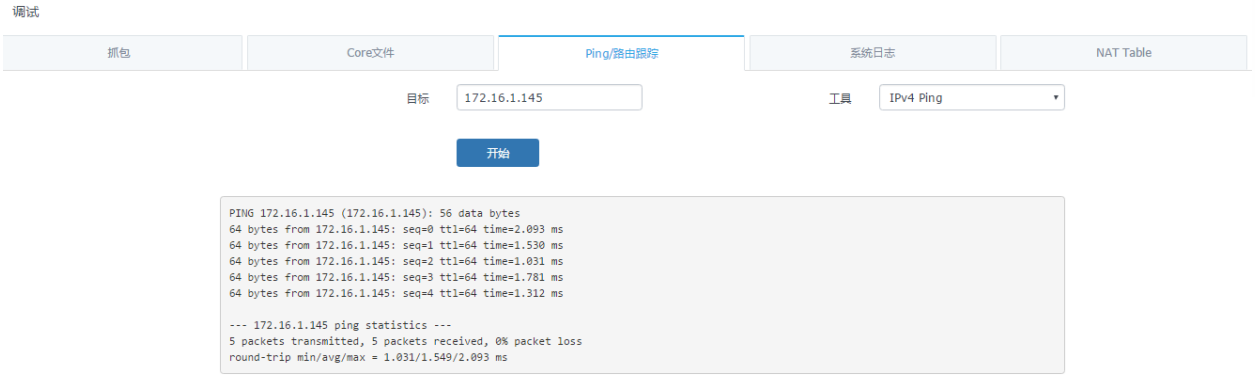


图 47:IP Ping

- 工具旁边从下拉菜单中选择：
  - IPv4 Ping 测试
  - IPv6 Ping 测试
  - IPv4 路由跟踪
  - IPv6 路由跟踪
- 在目标字段中键入目的地的 IP 地址/域名。
- 点击开始。

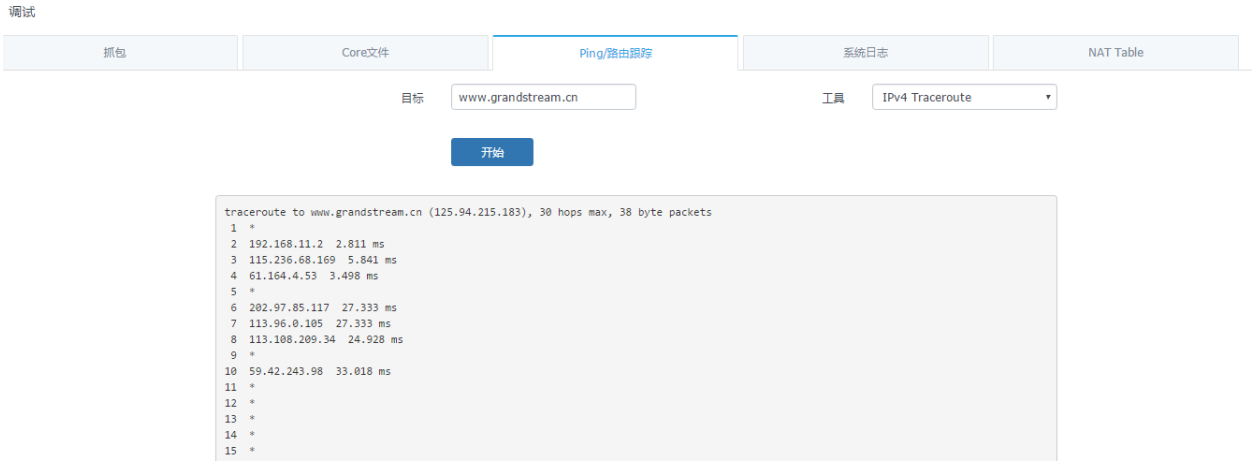


图 48:路由跟踪

Syslog

在 GWN7000 上，用户可以在 **Web GUI->系统设置->维护->系统日志**下将 syslog 信息转储到远程服务器。输入 syslog 服务器主机名或 IP 地址，并选择 syslog 信息的级别。 有五个级别的 syslog 可用：None，Debug，Info，Warning 和 Error。

系统日志消息也可以在 **Web GUI->系统设置->调试-> Syslog** 下实时显示。

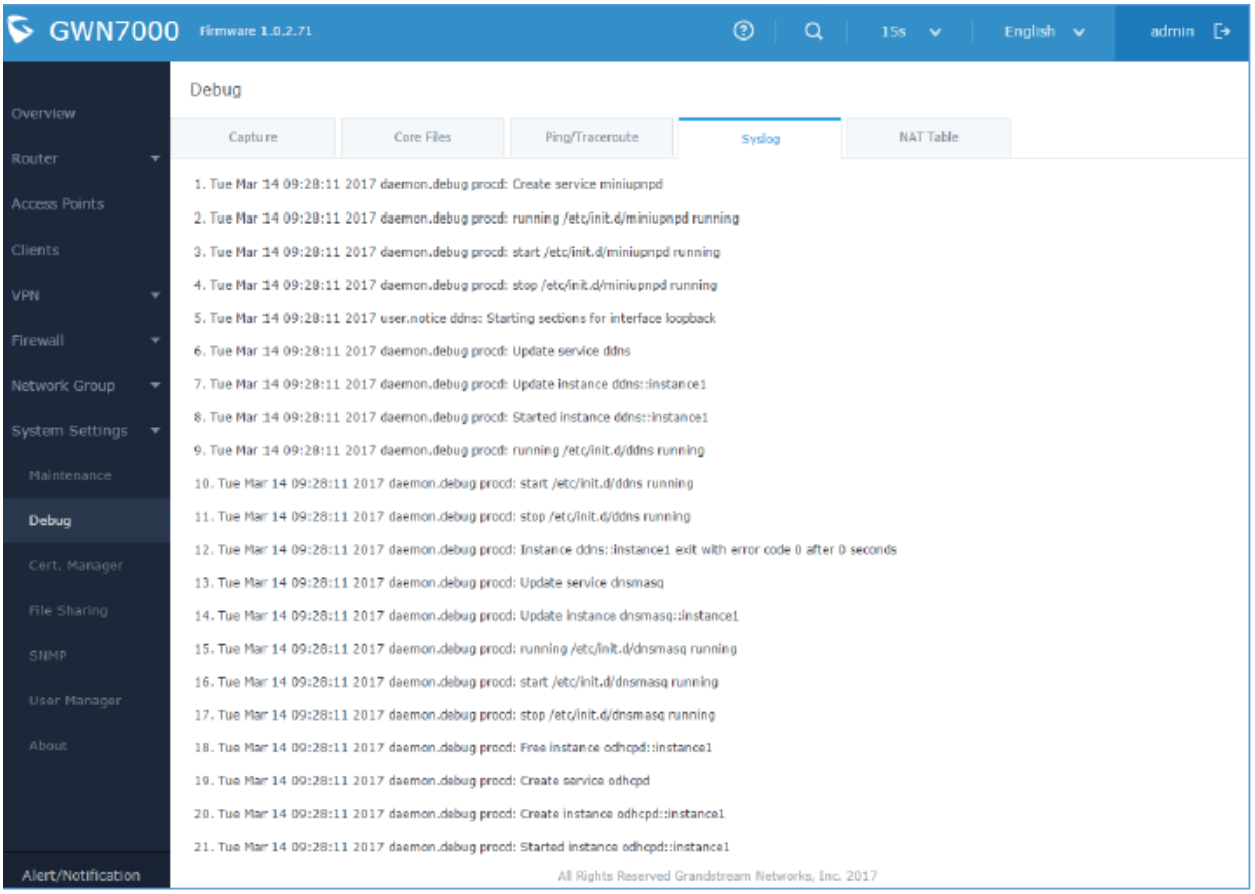


图 49:Syslog

NAT Table

NAT Table 在 GWN7000 的 WebGUI 上动态更新，检查 NAT Table 是否进入系统设置->调试-> NAT Table。

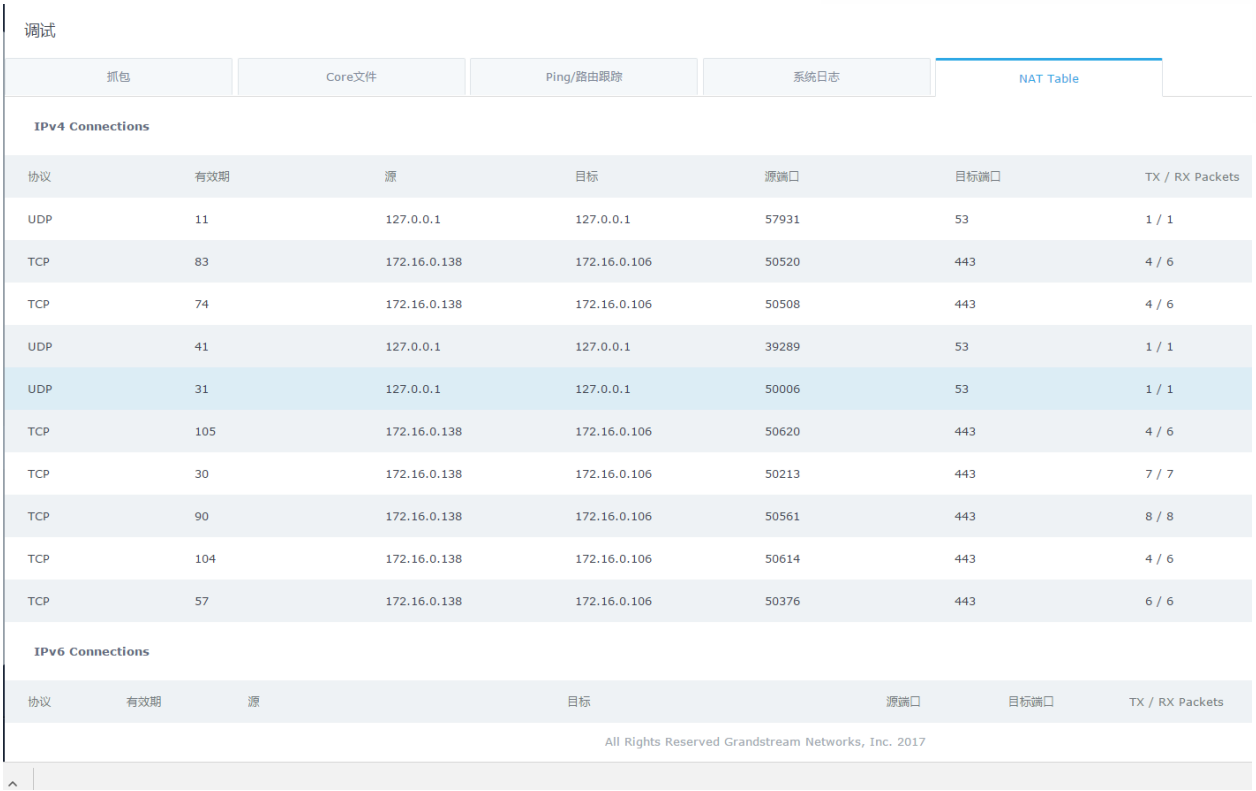


图 50:NAT Table

文件共享

GWN7000 具有 2 个 USB 端口，也可用于文件共享，可在 USB 端口上插入设备上进行文件共享，请转到路由器- >文件共享。

点击 

在与连接到 GWN7000 的其中一个 USB 端口的设备上共享一个目录及其内容，弹出下图。

图 51:新建文件共享

表 35: 新建文件共享

共享名称	输入共享文件名称。
共享路径	从下拉菜单中选择共享路径。
访问方式	选择是否允许用户读写/只读共享文件。
备注	添加对共享文件的备注。
允许共享网络组	选择是否允许所有 LAN 网络组访问共享路径，通过仅选择一些组（或无限制）来限制访问。

用户可以通过点击编辑共享文件夹，或点击删除共享文件。

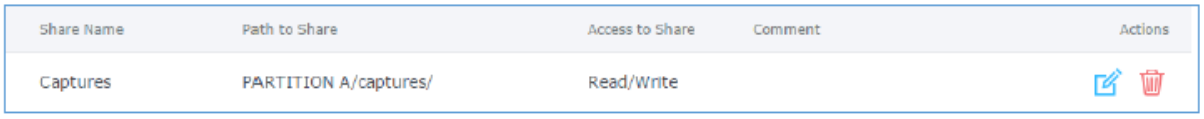


图 52:文件共享激活

连接到被允许访问共享文件的网络组的设备可以使用以下路径进行访问：\\ GWN_Address \ Share_Name \

其中 GWN_Address 是 GWN7000 IP 地址，Share_Name 是为文件共享创建的共享名称。 用户还可以在 Windows 上映射网络驱动器，或在 Linux 机器上使用 Samba 客户端。

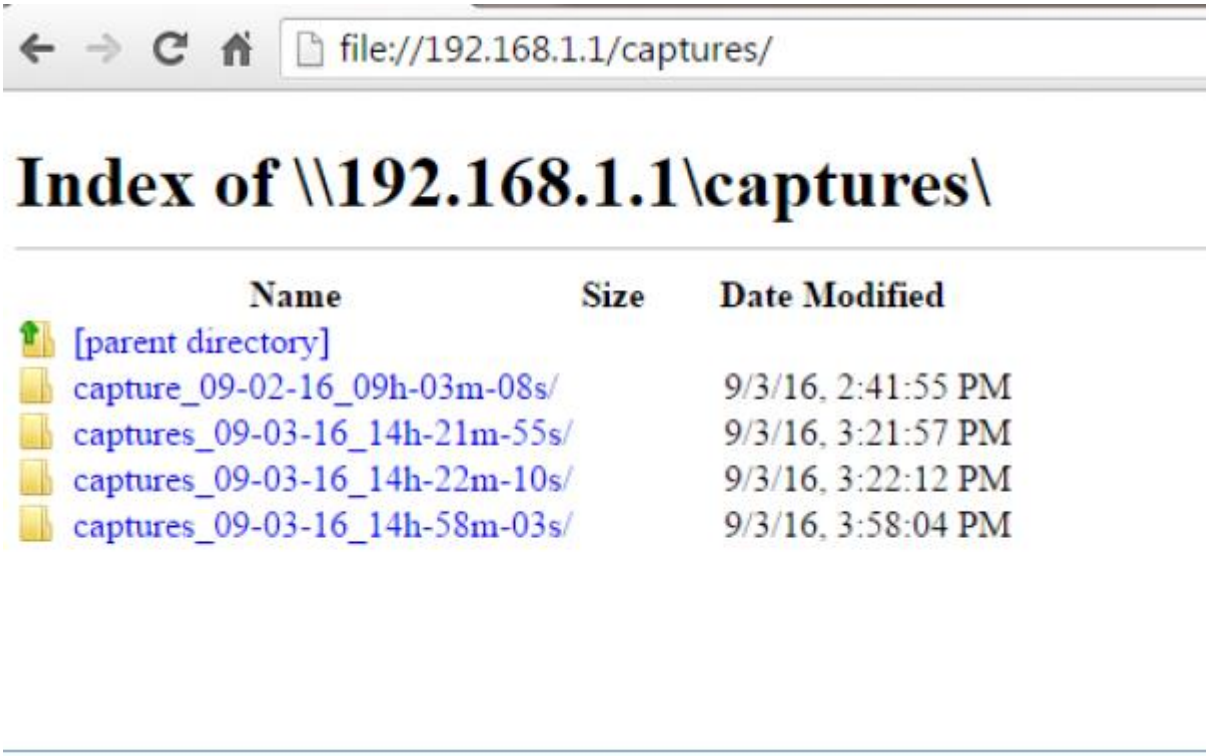


图 53:访问文件共享

SNMP（待定）

GWN7000 支持 SNMP（简单网络管理协议），广泛应用于网络监控网络管理，用于收集有关被监控设备的信息。

要配置 SNMP 设置，进入 GWN7000 Web GUI 中 - >系统设置 - > SNMP，此页面有两个标签：基本和高级，请参考以下表格。

表 36: SNMP 基本页面

系统位置	设置系统位置信息，例如：SNMP-Server Lobby GWN。
系统联系人	设置系统联系人信息，例如：通过 1000 分机连接 Supervisor_GWN。
系统名称	设置系统名称信息，例如：Supervisor_GWN。
IPv4 只读团体名	授予团体通过 IPv4 协议访问和只读管理信息库中的设备的权限。
IPv4 读写团体名	授予团体通过 IPv4 协议访问和读写管理信息库中的设备的权限。
IPv6 只读团体名	授予团体通过 IPv6 协议访问和只读管理信息库中的设备的权限。

IPv6 读写团体名	授予团体通过 IPv6 协议访问和读写管理信息库中的设备的权限。
陷阱类型	从下拉菜单中选择陷阱类型，有 4 个选项可用：无，SNMPv1，SNMPv2c 和 SNMPv2cInforms。
监控地址	输入监控主机的 IP /域名（网络管理系统“NMS”）。
监控端口	进入监控主机的端口（网管系统“NMS”）。
陷阱团体名	输入陷阱团体名字符串以对服务器进行身份验证。

表 37: SNMP 高级页面

SNMP 监听服务	点击  添加 SNMP 监听服务： ● 设置传输类型：UDPv4，UDPv6，TCPv4 或 TCPv6。 ● 选择 **IP 地址**从下拉菜单列表。 ● 设置 GWN7000 侦听的端口号。
SNMPv3 用户	点击  添加 SNMPv3 用户： ● 设置用户名进行身份验证。 ● 选择验证类型，有 2 个选项可用：SHA 和 MD5。 ● 从验证密码设置验证密码。 ● 再次输入密码以通过验证密码确认确认。 ● 选择隐私协议，有 3 个选项可用：无，DES 和 AES。 ● 设置隐私密码。 ● 在隐私密码确认字段中输入隐私密码。

升级和配置

升级固件

GWN7000 支持远程或本地固件升级。本节将讲述如何升级您的 GWN7000。

通过 WEB 页面升级

GWN7000 可以通过配置 TFTP/HTTP/HTTPS 服务器进行升级，用户可以自选其中一种。为 TFTP/HTTP/HTTPS 服务器配置有效的 URL，服务器的名字可以使 FQDN 或 IP 地址。

有效的 URLs:
firmware.grandstream.com/BETA
192.168.5.87

通过 **Web 页面->路由器->维护**，访问升级配置页面。.

表 38: 网络升级配置

升级方式	用户可以自助选择固件升级方式：TFTP, HTTP or HTTPS.
固件服务器	定义固件服务器路径
启动检查更新	允许设备在启动时检查是否有从固件服务器下发的固件
自动升级检查间隔(m)	设置自动升级的检查时间间隔
即刻升级	点击 Upgrade 开始升级。注意设备会在固件下载完成后重启

⚠ **注意:**

设备升级过程中，请确保电源保持畅通。

服务提供商应该有自己的固件升级服务器。没有 TFTP/HTTP/HTTPS 服务器的用户，以下是一些免费的 windows 版本的 TFTP 服务器可供下载：
http://www.solarwinds.com/products/freetools/free_tftp_server.aspx

http://tftpd32.jounin.net

请访问 http://www.grandstream.com/support/firmware 获取最新的固件。

通过TFTP进行本地固件升级：

1. 解压固件文件并把所有文件放在TFTP根目录下；
2. 将电脑和GWN7000 连接到同一个局域网中；
3. 打开 TFTP服务器，进入File menu->Configure->Security，把TFTP服务器的默认设置从"Receive Only" 改为 "Transmit Only"；
4. 启动TFTP服务器，并在GWN7000 web配置页面配置该服务器；
5. 将电脑的IP地址配置给固件服务器；
6. 更新修改并重启GWN7000

终端用户也可以从 http://httpd.apache.org/ 下载免费的HTTP服务器或使用 Microsoft IIS web服务器。

配置和备份

GWN7000 的配置可以通过本地或网络备份。备份文件可以在必要时用来恢复 GWN70000。

下载配置

用户可以下载GWN7000 的配置用来恢复， **Web页面->路由器-> 维护。**

点击 Download 下载本地配置文件。

配置服务器

管理员可以通过将配置文件放到TFTP/HTTP/HTTPS服务器，并为TFTP/HTTP/HTTPS设置配置服务器的方式下载和配置GWN7000。

重置和重启

管理员可以重启或将设备恢复出厂设置，通过 **Web页面->路由器->维护，** 点击 Reboot 按钮。

Reset 将会把在线的GWN7610 以及GWN7000 本身恢复出厂设置。

体验 GWN7000 企业级路由器

请访问我们的网站： http://www.grandstream.com 来获取最新的固件版本，新增的功能，FAQs，文档和新的产品特性。

我们鼓励您访问我们的 产品相关文档, FAQs 和 用户和开发人员论坛 来解答一些您常见的问题。 如果您通过经潮流认证的合作伙伴或经销商购买了我们的产品，请直接联系他们请求支持。

我们的技术支持人员可随时为您解答所有疑问。请联系我们的技术支持人员或 在线提交故障清单 来获取更深入的支持。

再次感谢您购买潮流 GWN7000 企业级路由器，确信它会为您的工作和生活带来便利和色彩。