

H3C SecPath F100-X-G5[F1000-X-G5]系列 防火墙

快速开局一本通

Copyright © 2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介	1
2 设备外观介绍	1
2.1 F100-C-G5、F100-S-G5、F100-M-G5 设备前视图	1
2.2 F100-A-G5 设备前视图	1
2.3 F100-E-G5、F1000-C-G5、F1000-C-G5-LI 设备前视图	2
2.4 F1000-S-G5、F1000-A-G5 设备前视图	3
2.5 F1000-E-G5、F1000-H-G5 设备前视图	3
3 防火墙的工作原理	4
3.1 防火墙的基本概念	4
3.2 接口与安全域	4
3.3 安全策略	5
4 完成防火墙的初始配置	5
4.1 设备出厂配置	5
4.2 应用场景组网	6
4.3 登录设备 Web 管理页面	7
4.4 路由模式接入 Internet	12
4.4.1 指定 IP 方式接入	12
4.4.2 DHCP 方式接入	17
4.4.3 PPPoE 方式接入	23
4.5 透明模式接入 Internet	28
4.6 配置特征库升级	31
4.6.1 定时升级特征库	32
4.6.2 立即升级特征库	37
4.6.3 本地升级特征库	41
4.7 License 首次激活和安装	41
4.8 配置基础安全策略	42
4.9 配置恢复出厂设置	44
4.9.1 特性简介	44
4.10 软件升级	46
4.11 设备维护和诊断	47
5 高级功能	47
5.1 NAT 功能	47

5.1.1 应用场景	47
5.1.2 配置方法	48
5.2 远程办公接入之 IPsec 方式	48
5.2.1 应用场景	48
5.2.2 配置方法	48
5.3 远程办公接入之 SSL VPN 方式	49
5.3.1 应用场景	49
5.3.2 配置方法	49
5.4 双机热备功能	49
5.4.1 应用场景	49
5.4.2 配置方法	50
6 更多参考信息	51

1 简介

本手册可帮助您对防火墙的使用过程有初步的认识，并完成防火墙的基本配置，如防火墙的常见组网方式，如何将防火墙快速接入 Internet，如何快速实现企业网络的安全防护和常用的设备运维操作等。如果您想深入了解和使用防火墙其他更多、更丰富的安全防护功能，具体查阅对应产品的手册。



说明

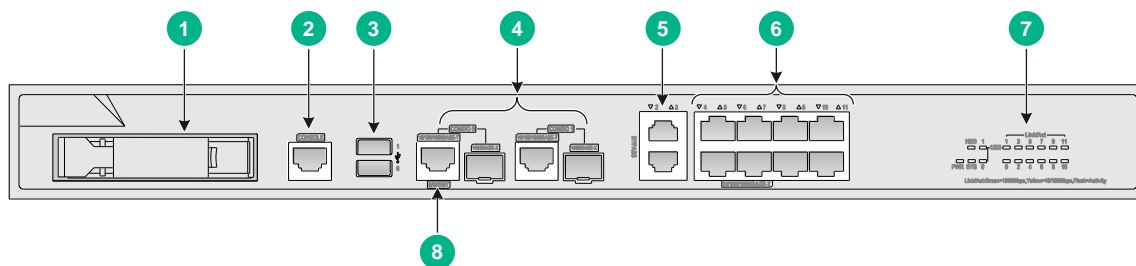
本手册的配置步骤是以 F1000-H-G5 举例，具体以设备的实际情况为准。

2 设备外观介绍

2.1 F100-C-G5、F100-S-G5、F100-M-G5设备前视图

设备前面板上有 8 个 10/100/1000BASE-T 自适应以太网电口、2 个 COMBO 接口（含 1 个管理以太网口）、2 个 BYPASS 口、2 个 USB 接口、1 个 CONSOLE 接口和 1 个硬盘扩展插槽，具体结构如下图所示。

图2-1 设备前视图

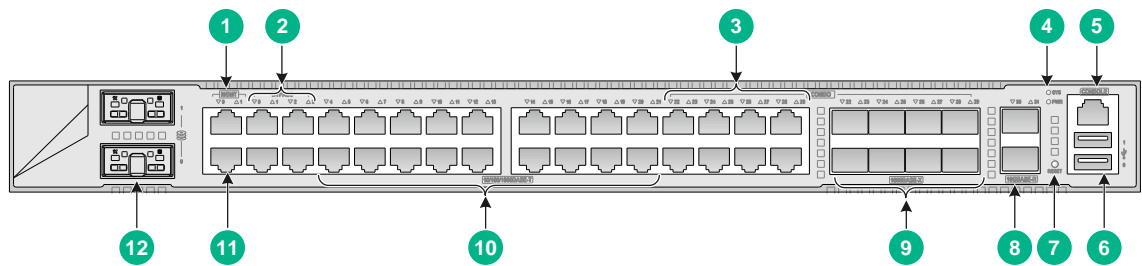


1: 硬盘扩展插槽	2: CONSOLE 口
3: USB 口 (Host 模式, A 类型接口)	4: COMBO 口
5: BYPASS 口	6: 10/100/1000BASE-T 以太网电口
7: 设备指示灯	8: 管理以太网口 (0/MGMT)

2.2 F100-A-G5设备前视图

设备前面板上有 18 个 10/100/1000BASE-T 自适应以太网电口、2 个 10GBASE-R 以太网光口、2 个管理以太网口、4 个 BYPASS 口、8 个 COMBO 口、1 个 CONSOLE 口、2 个 USB 口、1 个 RESET 按键以及 2 个硬盘扩展插槽。具体结构如下图所示。

图2-2 设备前视图



1: 管理以太网口 (1/MGMT)	2: BYPASS口
3: 10/100/1000BASE-T以太网电口 (COMBO口)	4: 设备指示灯
5: CONSOLE口	6: USB口
7: RESET按键 (重启设备)	8: 10GBASE-R以太网光口
9: 1000BASE-X以太网光口 (COMBO口)	10: 10/100/1000BASE-T以太网电口
11:管理以太网口 (0/MGMT)	12: 硬盘扩展插槽

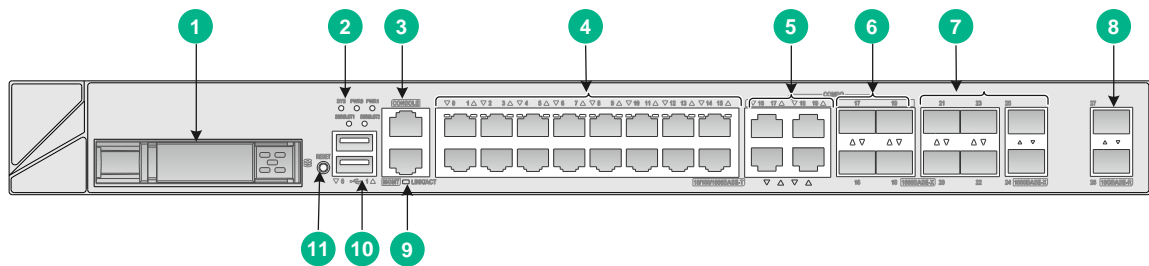


RESET 按键：用于重启设备，不会恢复默认出厂配置。

2.3 F100-E-G5、F1000-C-G5、F1000-C-G5-LI设备前视图

设备前面板上有 16 个 10/100/1000BASE-T 自适应以太网电口、4 个 COMBO 口、6 个 1000BASE-X 以太网光口、2 个 10GBASE-R 口、2 个 USB 接口、1 个 CONSOLE 接口、1 个硬盘扩展插槽以及 1 个管理以太网口。具体结构如下图所示。

图2-3 设备前视图

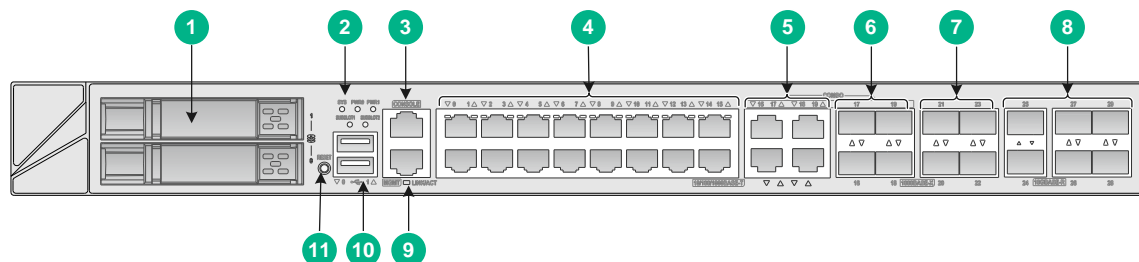


1: 硬盘扩展插槽	2: 设备指示灯
3: CONSOLE口	4: 10/100/1000BASE-T以太网电口
5: 10/100/1000BASE-T以太网电口 (COMBO口)	6: 1000BASE-X以太网光口 (COMBO口)
7: 1000BASE-X以太网光口	8: 10GBASE-R以太网光口
9: 管理以太网口 (MGMT)	10: USB口 (Host模式, A类型接口)
11: RESET按键	

2.4 F1000-S-G5、F1000-A-G5设备前视图

设备前面板上有 16 个 10/100/1000BASE-T 自适应以太网电口、4 个 COMBO 口、4 个 1000BASE-X 以太网光口、6 个 10GBASE-R 以太网光口、2 个 USB 接口和 1 个 CONSOLE 接口、2 个硬盘扩展插槽以及 1 个管理以太网口。具体结构如下图所示。

图2-4 设备前视图

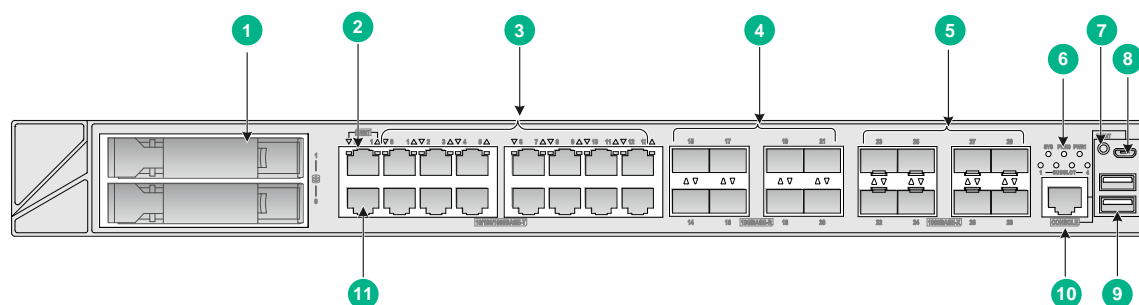


1: 硬盘扩展插槽	2: 设备指示灯
3: CONSOLE 口	4: 10/100/1000BASE-T以太网电口
5: 10/100/1000BASE-T以太网电口 (COMBO口)	6: 1000BASE-X以太网光口 (COMBO口)
7: 1000BASE-X以太网光口	8: 10GBASE-R以太网光口
9: 管理以太网口	10: USB口 (Host模式, A类型接口)
11: RESET按键	

2.5 F1000-E-G5、F1000-H-G5设备前视图

设备前面板上有 14 个 10/100/1000BASE-T 自适应以太网电口、8 个 1000BASE-X 以太网光口、8 个 10GBASE-R 以太网光口、2 个 USB 接口、1 个 CONSOLE 接口、1 个 Micro USB 接口、2 个硬盘扩展插槽以及 2 个管理以太网口。具体结构如下图所示。

图2-5 设备前视图



1: 硬盘扩展插槽	2: 管理以太网口 (1/MGMT)
3: 10/100/1000BASE-T以太网电口	4: 10GBASE-R以太网光口
5: 1000BASE-X以太网光口	6: 设备指示灯
7: RESET按键	8: Micro USB口
9: USB口	10: CONSOLE口
11: 管理以太网口 (0/MGMT)	

3 防火墙的工作原理

3.1 防火墙的基本概念

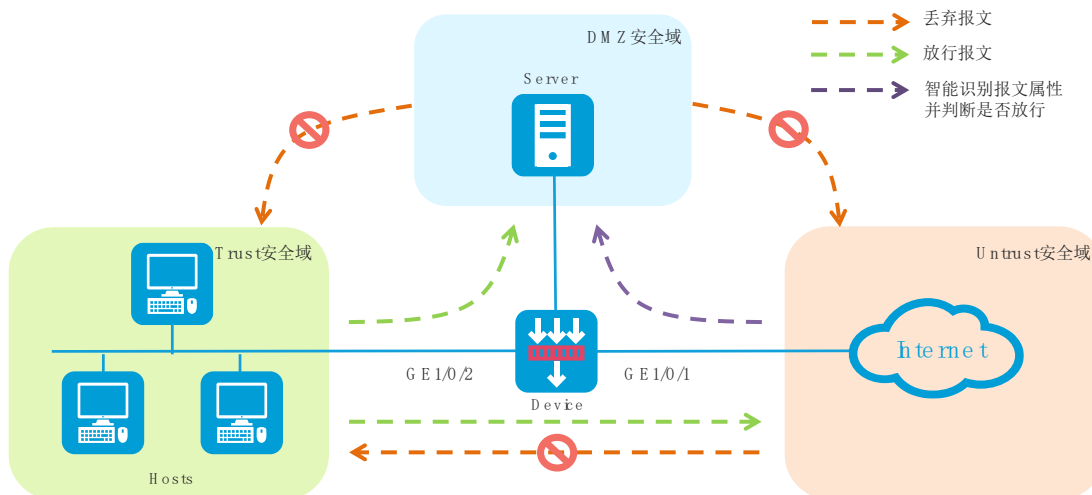
防火墙是一种网络安全设备，通常位于网络边界，用于隔离不同安全级别的网络，保护一个网络免受来自另一个网络的攻击和入侵。这种隔离是有控制地隔离，允许合法流量通过防火墙，禁止非法流量通过防火墙。

防火墙控制网络流量的实现主要依托于安全域和安全策略，下文详细介绍。

3.2 接口与安全域

如图 3-1 所示，管理员将安全需求相同的接口进行分类，并划分到不同的安全域（Security Zone），能够实现域间策略的统一管理。安全域，是一个逻辑概念。

图3-1 安全域的划分图



设备上缺省存在 Local、Management、Trust、DMZ 和 Untrust 安全域。缺省安全域不能被删除。各缺省安全域的作用及应用场景说明如下：

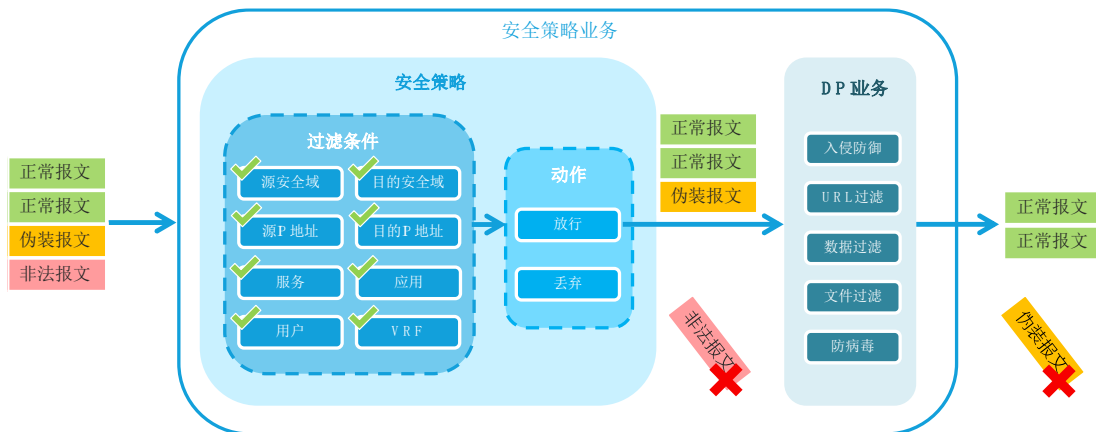
- **Local:** 指设备本身，且不能向 Local 安全域添加接口成员。非 Management 安全域与设备本身之间相互通信时，需要配置放行相应安全域与 Local 安全域之间报文的安全策略。
- **Management:** 指用于管理设备的区域，该安全域与设备本身通信的报文默认放行，即 Management 与 Local 之间的报文默认放行，无需配置安全策略。缺省情况下，设备管理口属于 Management 安全域，用于通过 PC 登录设备进行配置。
- **Trust:** 指可信任的网络区域。通常会将设备连接内网的接口添加至 Trust 安全域，并通过配置安全策略，对其他安全域发往 Trust 的报文进行威胁检测，保护内网主机，对 Trust 发往其他安全域的报文进行严格管理和控制，避免机密数据外泄。
- **DMZ:** Demilitarized Zone，隔离区。通常会将设备连接各类公共服务或资源（如 Web server、FTP server 等）的接口添加至 DMZ 安全域，并通过配置安全策略，对其他安全域发往 DMZ 的报文进行审计，避免服务器被攻击或机密数据被非法窃取。

- **Untrust:** 指不信任的网络区域。通常会将设备连接 Internet 的接口添加至 Untrust 安全域，并通过配置安全策略，对 Untrust 发往其他安全域的报文进行严格检测，阻断外来攻击和病毒等威胁。

3.3 安全策略

如图 3-2 所示，安全策略通过指定源/目的安全域、源 IP/MAC 地址、目的 IP 地址、服务、应用、终端、用户和时间段等过滤条件匹配出特定的报文，并根据预先设定的策略动作对此报文进行处理；若报文未匹配上任何策略，则丢弃该报文。当安全策略中未配置过滤条件时，则该策略将匹配所有报文。

图3-2 安全策略的报文处理流程图



4 完成防火墙的初始配置

4.1 设备出厂配置

防火墙设备出厂配置如下表，用户也可通过设备上的铭牌获取到设备的缺省用户名和密码等信息。

表4-1 防火墙出厂配置

登录信息项	默认配置	备注
用户名	admin	-
密码	admin	-
登录类型	<ul style="list-style-type: none"> • 通过 Web 界面登录设备 • 通过 Console 口登录设备 	其他登录类型需要自行配置

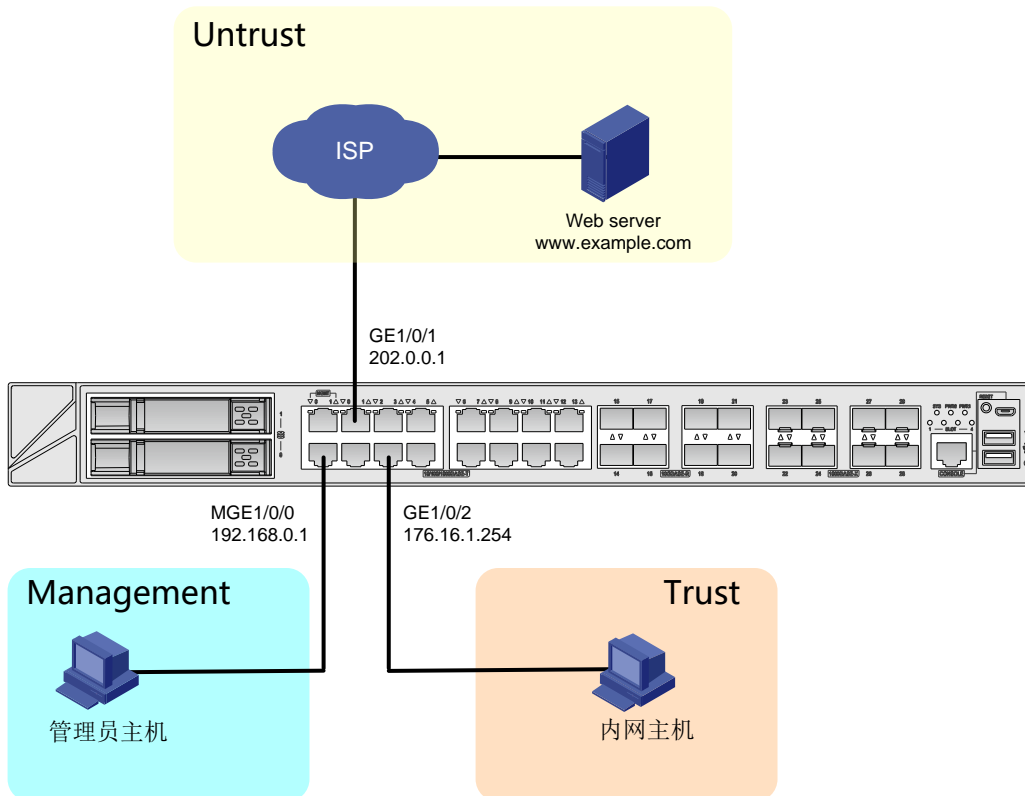
登录信息项	默认配置	备注
以太网管理口的 IP地址	<ul style="list-style-type: none"> 接口号: GigabitEthernet1/0/0 或 M-GigabitEthernet1/0/0 IP 地址: 192.168.0.1/24 	不同设备的管理网口编号存在差异, 具体可查阅对应的产品资料或者查看设备的铭牌

4.2 应用场景组网

如图 4-1 所示, 按照图中的拓扑连接设备的管理网口、内网口 GE1/0/2 和外网口 GE1/0/1。管理网口和管理员主机连接, 用于登录 Web 界面。内网口作为 LAN 口, 一般加入 Trust 安全域, 用于连接公司内网主机等。外网口作为 WAN 口, 一般加入 Untrust 安全域, 用于连接运营商网络与外部进行通信。

如果使用命令行配置设备, 在首次登录设备, 请使用 Console 配置线连接管理 PC 的串口和设备的 Console 口。

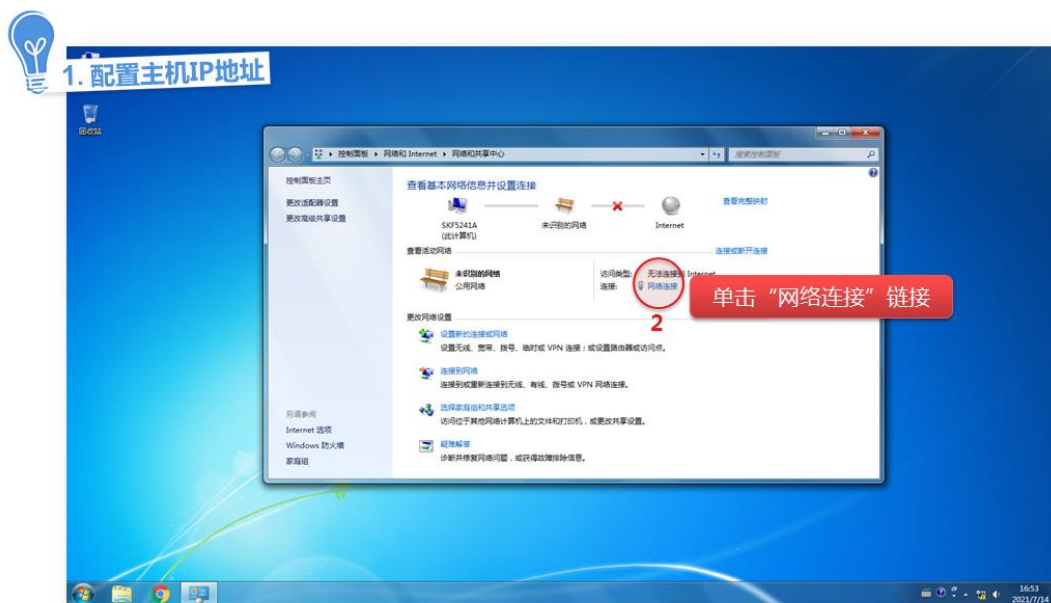
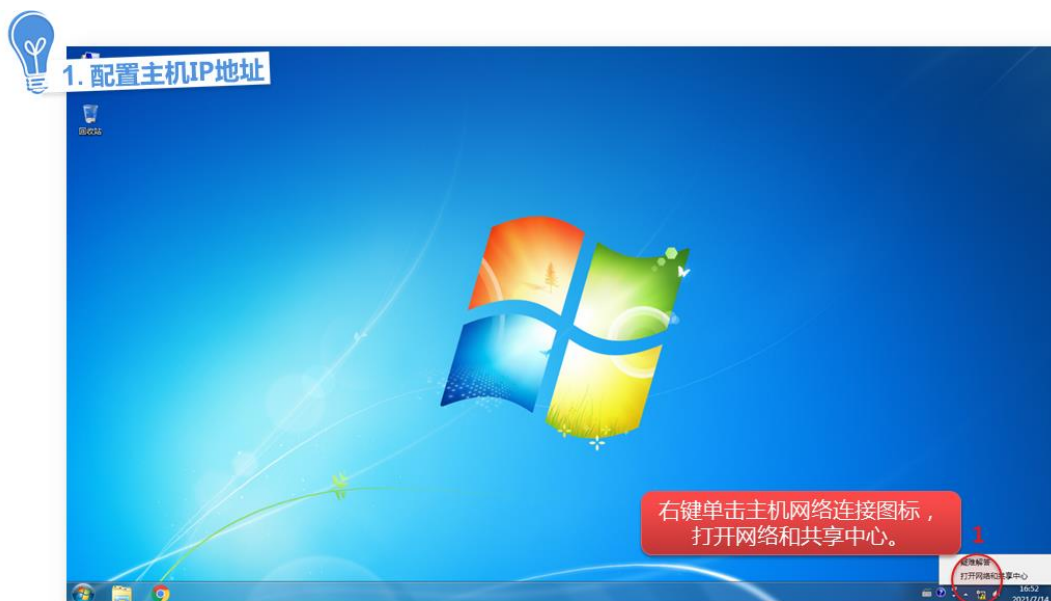
图4-1 连接线缆图



4.3 登录设备Web管理页面

说明

- 建议使用以下浏览器访问 Web 管理页面：Chrome 40 及以上版本、Firefox 19 及以上版本、Internet Explorer 10 及以上版本。
- 使用的浏览器必须要设置能接受第一方 Cookie（即来自站点的 Cookie），并启用活动脚本（或 JavaScript），才能正常访问 Web。以上功能在不同浏览器中的名称及设置方法可能不同，请以实际情况为准。
- 使用 Internet Explorer 浏览器时，还必须启用以下两个功能，才能正常访问 Web：对标记为可安全执行脚本的 ActiveX 控件执行脚本、运行 ActiveX 控件和插件。
- 更改设备的软件版本后，建议在登录 Web 页面之前先清除浏览器的缓存，以便正确地显示 Web 页面。

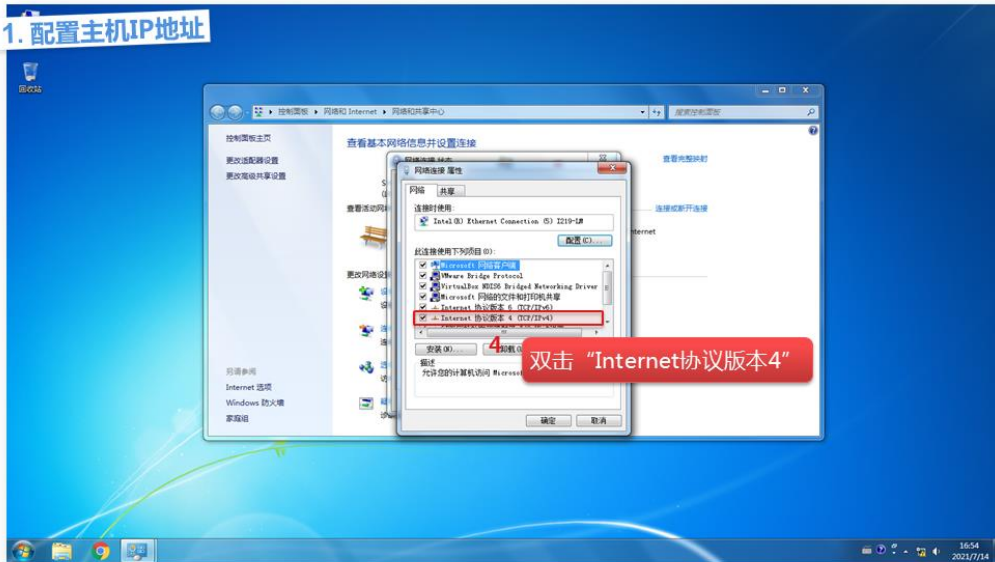




1. 配置主机IP地址

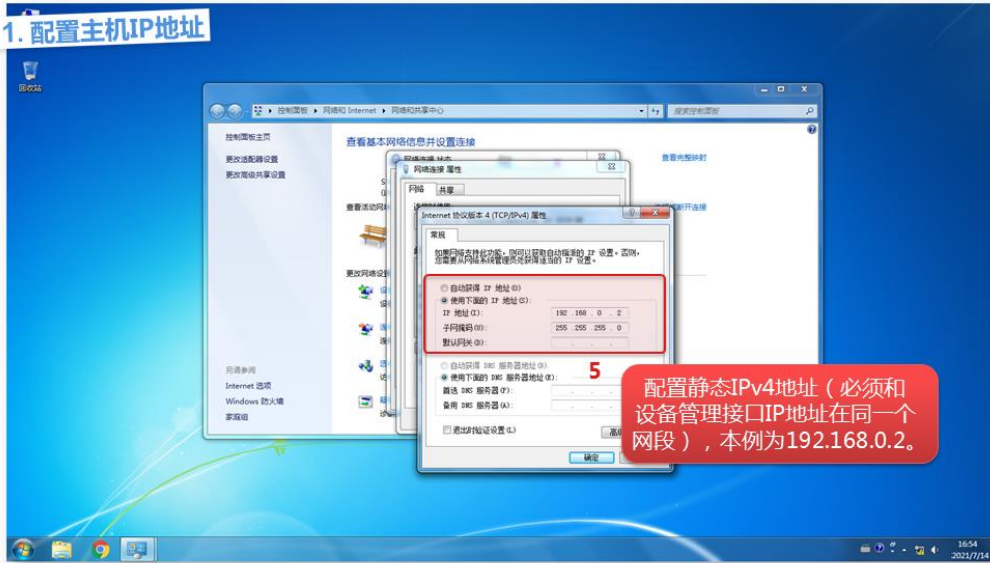


1. 配置主机IP地址

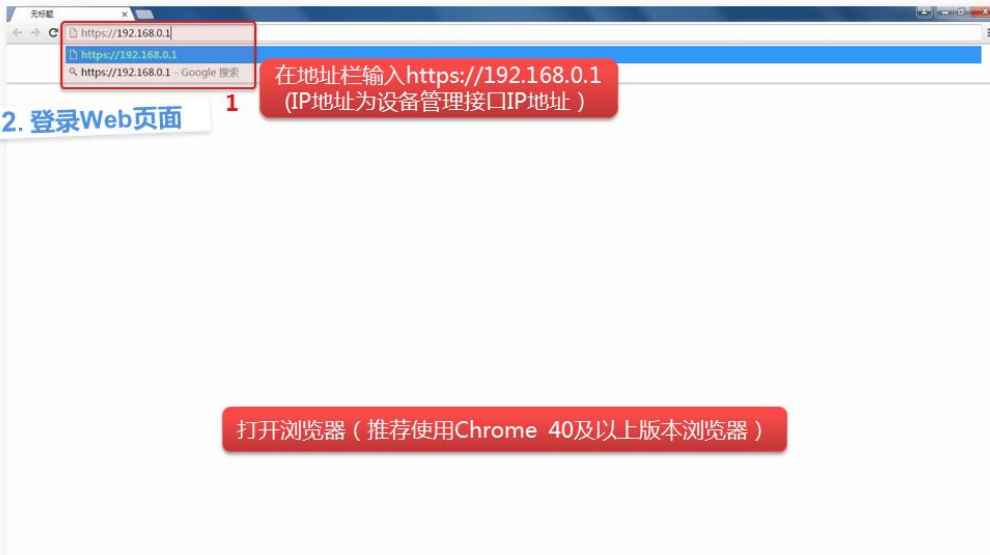




1. 配置主机IP地址



2. 登录Web页面





2. 登录Web页面



2. 登录Web页面





2. 登录Web页面

设备状态图

内存使用率 37% CPU使用率 3% Flash使用率 44%

系统流量统计

速率统计

系统日志

时间	级别	详细信息
2021-07-19 14:46:40	Error	Physical state on the interface SSLVPN-AC1 changed to up.

系统信息

设备名称	1060	[设置]
设备型号	SecPath F1060	[设置]
软件版本	7.1.064.Feature 9360P13	[设置]
序列号	210235A1PVH14A000003	[设置]
集群模式	集群模式	[设置]
IRF成员状态	Slot1 主	[设置]
系统时间	2021-07-19 15:28:42	[设置]

系统会话统计

最近一个小时 (个)

系统新建速率统计

最近一个小时 (个/秒)

登录成功, 进入Web配置页面

Copyright © 2004-2021 新华三技术有限公司 版权所有, 保留一切权利



3. 保存配置

单击“保存”图标

设备状态图

内存使用率 37% CPU使用率 3% Flash使用率 44%

系统流量统计

速率统计

系统日志

时间	级别	详细信息
2021-07-19 14:46:40	Error	Physical state on the interface SSLVPN-AC1 changed to up.

系统信息

设备名称	1060	[设置]
设备型号	SecPath F1060	[设置]
软件版本	7.1.064.Feature 9360P13	[设置]
序列号	210235A1PVH14A000003	[设置]
集群模式	集群模式	[设置]
IRF成员状态	Slot1 主	[设置]
系统时间	2021-07-19 15:28:42	[设置]

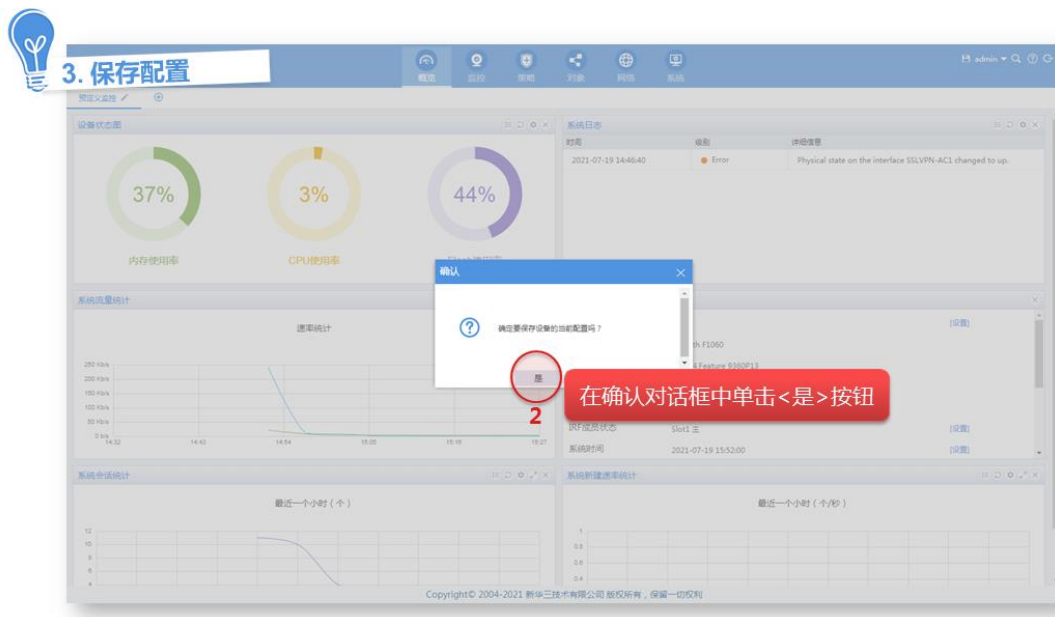
系统会话统计

最近一个小时 (个)

系统新建速率统计

最近一个小时 (个/秒)

Copyright © 2004-2021 新华三技术有限公司 版权所有, 保留一切权利



4.4 路由模式接入Internet

路由模式接入是指设备以三层模式（即设备的上下行业务接口工作在三层模式）部署在网络中，此模式下设备一般作为企业的网关连接内网和互联网，对网络流量进行安全监测和安全控制。此模式下设备可支持丰富的路由功能和安全功能。为适应不同的网络环境，设备提供如下三种方式快速接入 Internet。

- 指定 IP 方式接入：是从运营商获取一个固定的公网 IP 地址，用户内网需通过该公网 IP 地址接入 Internet。
- DHCP 方式接入：是设备通过运营商提供的 DHCP 服务动态获取一个公网 IP 地址即可接入 Internet。
- PPPoE 方式接入：用户从运营商处获取一个 PPPoE 接入认证账户，可通过该帐户接入 Internet。

4.4.1 指定 IP 方式接入

指定 IP 地址方式是从运营商获取一个固定的公网 IP 地址，用户内网需通过该公网地址接入 Internet。具体配置方法如下。



1. 配置快速接入

1. 系统

2. 快速接入Internet

3. 路由模式 (使用防火墙的路由功能)

4. 开始配置

选择“路由模式”接入Internet



1. 配置快速接入

5. 选择WAN口为GE 1/0/1 接入方式为“指定IP地址”

6. 配置WAN口IP地址、掩码、默认路由及DNS服务地址

接口	GE1/0/1	
接入方式	指定IP地址 DHCP PPPoE	
IP地址/掩码长度	202.0.0.1	255.255.255.0
默认路由	202.0.0.254	
网关		
首选DNS服务器	219.141.136.102	
备用DNS服务器	219.141.140.10	

7. 下一步



1. 配置快速接入

8. 选择LAN口为GE 1/0/2

9. 配置LAN口IP地址，开启内网DHCP服务

接口	GE1/0/2	
IP地址/掩码长度	172.16.1.254	255.255.255.0
DHCP	开启	
地址池名称	GuideSecDHCPool (1-63字符)	
动态分配的地址段	172.16.1.0	255.255.255.0

10. 下一步



1. 配置快速接入

接入模式

- 路由模式 (使用防火墙网关的路由功能)
- 透明模式 (不改变原有的网络结构)

开始配置

路由模式

- WAN口配置
- LAN口配置
- DMZ口配置
- 安全配置
- 广域网加速
- 一键流控
- 连接安全云
- 核对配置信息

DMZ口配置、安全配置和广域网加速 无需配置，点击下一步即可

11



1. 配置快速接入

接入模式

- 路由模式 (使用防火墙网关的路由功能)
- 透明模式 (不改变原有的网络结构)

开始配置

路由模式

- WAN口配置
- LAN口配置
- DMZ口配置
- 安全配置
- 广域网加速
- 一键流控
- 连接安全云
- 核对配置信息

期望带宽 10000 Mbps (1-100000)

配置“期望带宽”

12

13



1. 配置快速接入

接入模式

- 路由模式 (使用防火墙网关的路由功能)
- 透明模式 (不改变原有的网络结构)

开始配置

路由模式

- WAN口配置
- LAN口配置
- DMZ口配置
- 安全配置
- 广域网加速
- 一键流控
- 连接安全云
- 核对配置信息

14



1. 配置快速接入

路由模式

- 路由模式 (使用防火墙网关的路由功能)
- 透明模式 (不改变原有的网络结构)

开始配置

路由模式

1 WAN口配置

2 LAN口配置

3 DMZ口配置

4 安全配置

5 广域网加速

6 一键流控

7 连接安全云

8 快速配置向导

WAN口配置

接口: GE1/0/1

接入方式: 指定IP地址

IP地址/掩码长度: 202.0.0.1/255.255.255.0

默认路由: 202.0.0.254

首选DNS服务器: 219.241.136.102

备用DNS服务器: 219.241.140.10

LAN口配置

接口: GE1/0/0

IP地址/掩码长度: 172.16.1.254/255.255.255.0

DHCP服务: 开启

DHCP地址池名称: GuideSecPool

DHCP地址池地址: 172.16.1.1/24

操作: 上一步 完成 取消

15



2. 配置安全策略

策略

安全策略配置向导之第 1 步: 如要立即生效, 请点击 **立即生效** 按钮。内容安全配置向导之第 1 步: 如要立即生效, 请点击 **提交** 按钮。时效性提示: (灰色: 已失效, 红色: 一天内失效, 橙色: 一周内失效, 黄色: 30天内失效, 绿色: 生效)

允许配置的最大策略总数为: 10000, 且每种类型策略数不允许大于5000。

名称	源安全域	目的安全域	类型	ID	描述	源地址	目标地址	服务	策略	用户	动作	内容...	命中...	流量	统计	剩余...	会话数	策略	编辑
GuideSecPolicy	Trust	DMZ	IP4	0		Any	Any	Any	Any	Any	允许					0			编辑

编辑自动创建的安全策略

3



2. 配置安全策略

增加源(Local)和目的(Local、Trust)安全域

5



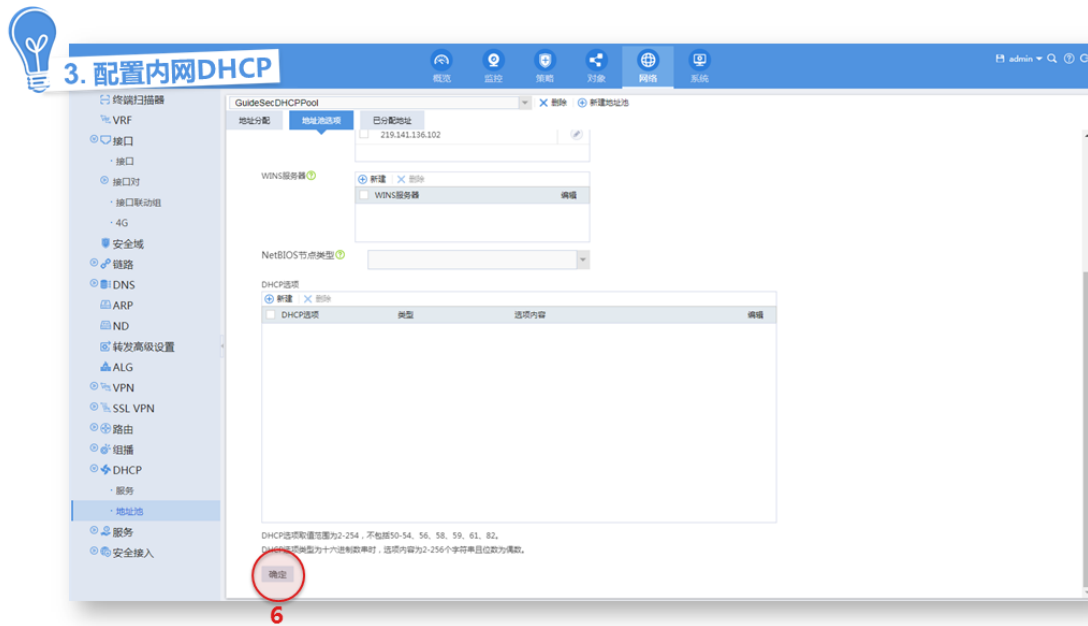
3. 配置内网DHCP

1

3

4 新建内网地址池网关

5 新建DNS服务器地址



4.4.2 DHCP 方式接入

DHCP 方式接入 Internet 方式是设备通过运营商提供的 DHCP 服务动态获取一个公网 IP 地址即可接入 Internet。具体配置方法如下。



1. 配置快速接入

1 系统

2 快速接入Internet

3 路由模式 (使用防火墙网关的路由功能)

4 开始配置

选择“路由模式”接入Internet



1. 配置快速接入

5 选择WAN口为GE 1/0/1

6 选择“DHCP”接入方式

7 下一步



1. 配置快速接入

The screenshot shows the '快速接入Internet' (Quickly Access Internet) configuration wizard. The '路由模式' (Routing Mode) is set to '路由模式' (Routing Mode). The 'LAN口配置' (LAN Port Configuration) step is active, showing the following configuration:

- 接口: GE10/2
- IP地址/掩码长度: 172.16.1.254 / 255.255.255.0
- DHCP: 开启
- 地址池名称: GuideSecDHCPPool
- 动态分配的地址段: 172.16.1.0 / 255.255.255.0

Annotations:

- 8: 选择LAN口为GE 1/0/2
- 9: 配置LAN口IP地址，开启内网DHCP服务
- 10: 下一步



1. 配置快速接入

The screenshot shows the '快速接入Internet' (Quickly Access Internet) configuration wizard. The '路由模式' (Routing Mode) is set to '路由模式' (Routing Mode). The 'DMZ口配置' (DMZ Port Configuration) step is active, showing the following configuration:

- 接口: [Empty]
- IP地址/掩码长度: [Empty]

Annotations:

- 11: DMZ口配置、安全配置和广域网加速无需配置，点击下一步即可



1. 配置快速接入

The screenshot shows the '快速接入Internet' (Quick Internet Access) configuration wizard. The '路由模式' (Routing Mode) dialog box is open, and the 'WAN口配置' (WAN Port Configuration) step is active. The interface includes a sidebar with navigation options like '高可靠性', '日志设置', '报表设置', '会话设置', '升级中心', 'License配置', '高级虚拟化', '管理员', '维护', '诊断中心', and '配置向导'. The main area shows '接入模式' (Access Mode) with options for '路由模式' and '透明模式'. The '路由模式' dialog has a list of steps: 1. WAN口配置, 2. LAN口配置, 3. DMZ口配置, 4. 安全配置, 5. 广域网加速, 6. 一键流控, 7. 连接安全云, 8. 核对配置信息. In step 1, the '接口' (Interface) is set to 'GE1/0/1', and the '期望带宽' (Expected Bandwidth) is set to '10000' Mbps. A red circle highlights the '期望带宽' field, and a red arrow points to it with the text '配置“期望带宽”'. The '下一步' (Next) button is also circled in red with the number '13' below it.



1. 配置快速接入

The screenshot shows the same '快速接入Internet' configuration wizard. The '路由模式' dialog box is open, and the '连接安全云' (Connect to Security Cloud) step is active. The 'WAN口配置' step is now completed. The '连接安全云' step has a checkbox labeled '连接安全云' which is checked. The '下一步' (Next) button is circled in red with the number '14' below it.



2. 配置安全策略

修改安全策略

名称: GuideSecPolicy

源安全域: Trust, Local

目的安全域: Untrust, DMZ, Local, Trust

动作: 允许

源IP/MAC地址: Any

目的IP地址: Any

服务: Any

应用: Any

协议/端口: Any

确定

4 增加源(Local)和目的(Local、Trust)安全域

5



3. 配置内网DHCP

配置内网DHCP

租约有效期: 1 天 0 小时 0 分 0 秒

网关: 172.16.1.254

DNS服务器: 219.141.136.102

WINS服务器

NetBIOS节点类型

DHCP选项

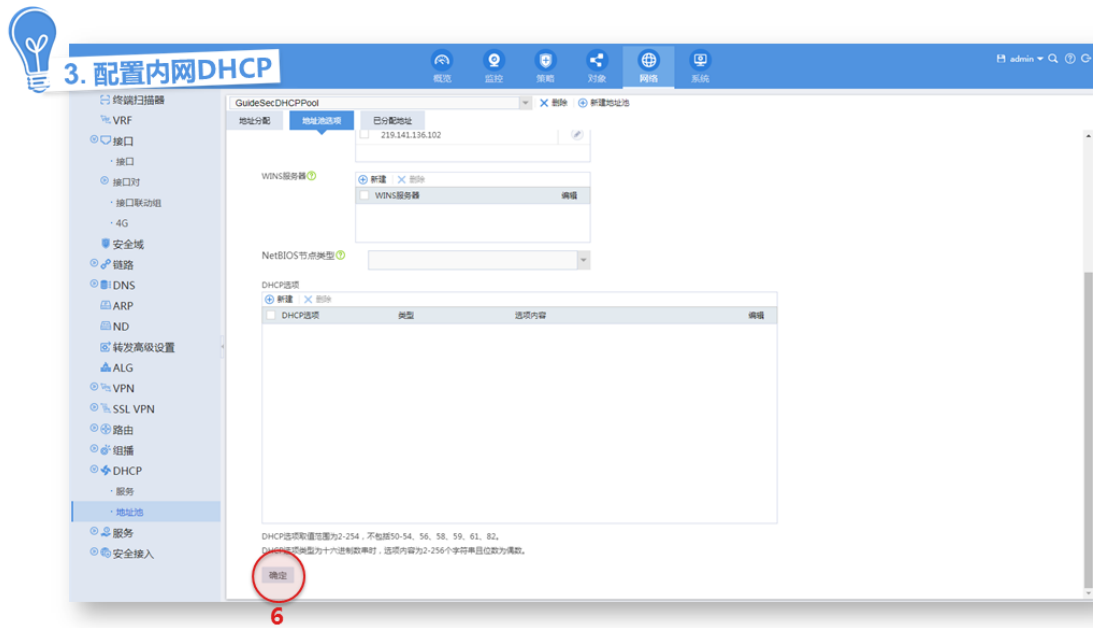
2

1

3

4 新建内网地址池网关

5 新建DNS服务器地址



4.4.3 PPPoE 方式接入

用户从运营商处获取一个 PPPoE 接入认证账户，可通过该帐户接入 Internet。具体配置方法如下。



1. 配置快速接入

1 系统

2 快速接入Internet

3 路由模式 (使用防火墙网关的路由功能)

4 开始配置

选择“路由模式”接入Internet



1. 配置快速接入

5 选择WAN口为GE 1/0/1

6 选择“PPPoE”接入方式

7 输入PPPoE用户名及密码

8 下一步

1 WAN口配置

接口 GE1/0/1

接入方式 指定IP地址 DHCP **PPPoE**

用户名 ppoeuser1

密码

在线方式 **永久在线**

自动获取IP地址

使用指定的IP地址

IP地址/掩码长度



1. 配置快速接入

9 选择LAN口为GE 1/0/2

10 配置LAN口IP地址，开启内网DHCP服务

11 下一步

2 LAN口配置

接口 GE1/0/2

IP地址/掩码长度 172.16.1.254 / 255.255.255.0

DHCP 开启

地址池名称 GuideSecDHCPool (1-43字符)

动态分配的地址段 172.16.1.0 / 255.255.255.0



1. 配置快速接入

接入模式

- 路由模式 (使用防火墙网关的路由功能)
- 透明模式 (不改变原有的网络结构)

开始配置

路由模式

- WAN口配置
- LAN口配置
- DMZ口配置
- 安全配置
- 广域网加速
- 一键流控
- 连接安全云
- 核对配置信息

DMZ口配置、安全配置和广域网加速 无需配置，点击下一步即可

12



1. 配置快速接入

接入模式

- 路由模式 (使用防火墙网关的路由功能)
- 透明模式 (不改变原有的网络结构)

开始配置

路由模式

- WAN口配置
- LAN口配置
- DMZ口配置
- 安全配置
- 广域网加速
- 一键流控
- 连接安全云
- 核对配置信息

配置“期望带宽”

13



1. 配置快速接入

接入模式

- 路由模式 (使用防火墙网关的路由功能)
- 透明模式 (不改变原有的网络结构)

开始配置

路由模式

- WAN口配置
- LAN口配置
- DMZ口配置
- 安全配置
- 广域网加速
- 一键流控
- 连接安全云
- 核对配置信息

15



1. 配置快速接入

路由模式

- 路由模式 (使用防火墙网关的路由功能)
- 透明模式 (不改变原有的网络结构)

开始配置

路由模式

1 WAN口配置

2 LAN口配置

3 DMZ口配置

4 安全配置

5 广域网加速

6 一键流控

7 连接安全云

8 成对配置向导

WAN口配置

接口: GE1/0/1

接入方式: PPPoE

网关: pppoeuser1

用户名: user

密码: 永久连接

LAN口配置

接口: GE1/0/2

IP地址/掩码长度: 172.16.1.254/255.255.255.0

DHCP服务: 开启

DHCP地址池名称: GuideSecPolicyPool

DHCP地址池网段: 172.16.1.254/255.255.255.0

操作: 上一步 完成 取消

16



2. 配置安全策略

策略

新建 插入 删除 复制 粘贴 统计 取消统计 应用 禁用 清空统计数据 清除过滤条件

安全策略配置变更之后，如需立即生效，请点击 立即加载。内容安全配置变更之后，如需立即生效，请点击 提交。时效提示：(灰色：已失效，红色：一天内失效，黄色：30天内失效，绿色：生效)

允许配置的最大策略总数为：10000，且每种类型策略数不允许大于5000。

名称	源安全域	目的安全域	类型	ID	描述	源地址	目的地址	服务	规则	用户	动作	内容...	命中...	流量	统计	删除...	会话查看	策略
GuideSecPolicy	Trust	Untr...	DMZ	0		IPv4	Any	Any	Any	Any	允许					0	查看	编辑

编辑自动创建的安全策略

3



2. 配置安全策略

修改安全策略

名称: GuideSecPolicy

源安全域: Trust, Local

目的安全域: Untrust, DMZ, Local, Trust

动作: 允许

目的IP地址: Any

确定

4 增加源(Local)和目的(Local、Trust)安全域

5



3. 配置内网DHCP

配置内网DHCP

租约有效期: 1 天 0 小时 0 分 0 秒

网关: 172.16.1.254

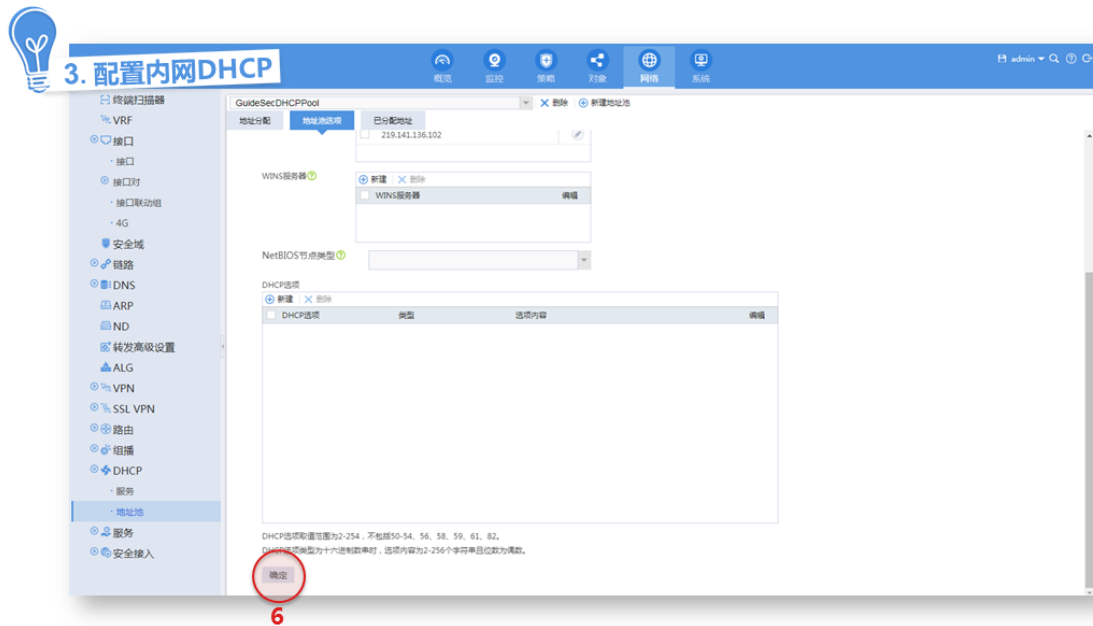
DNS服务器: 219.141.136.102

新建内网地址池网关

新建DNS服务器地址

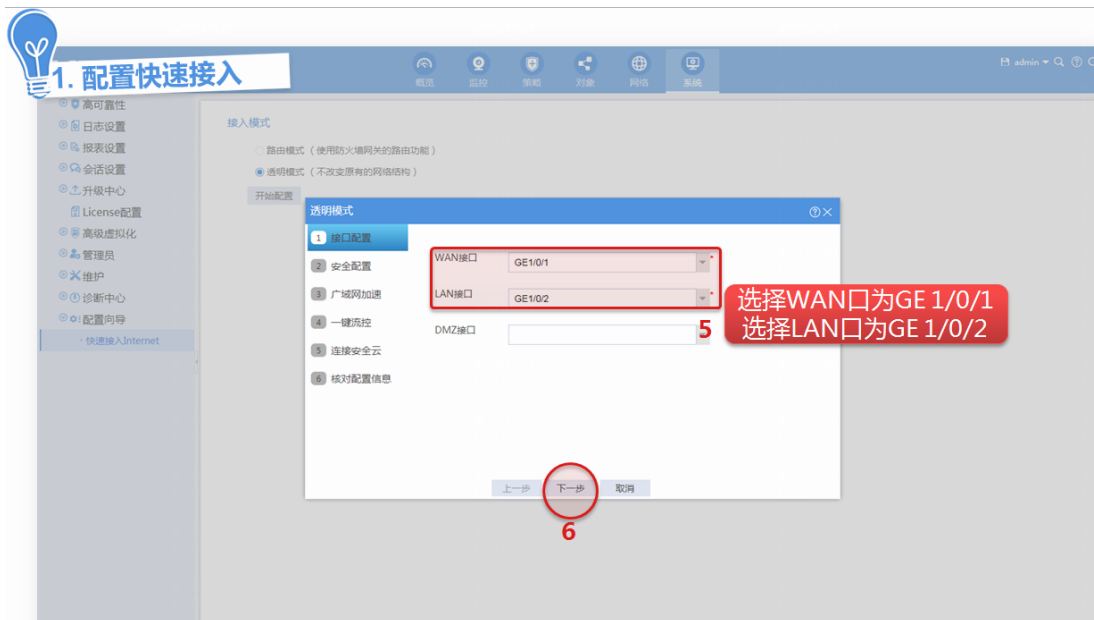
4

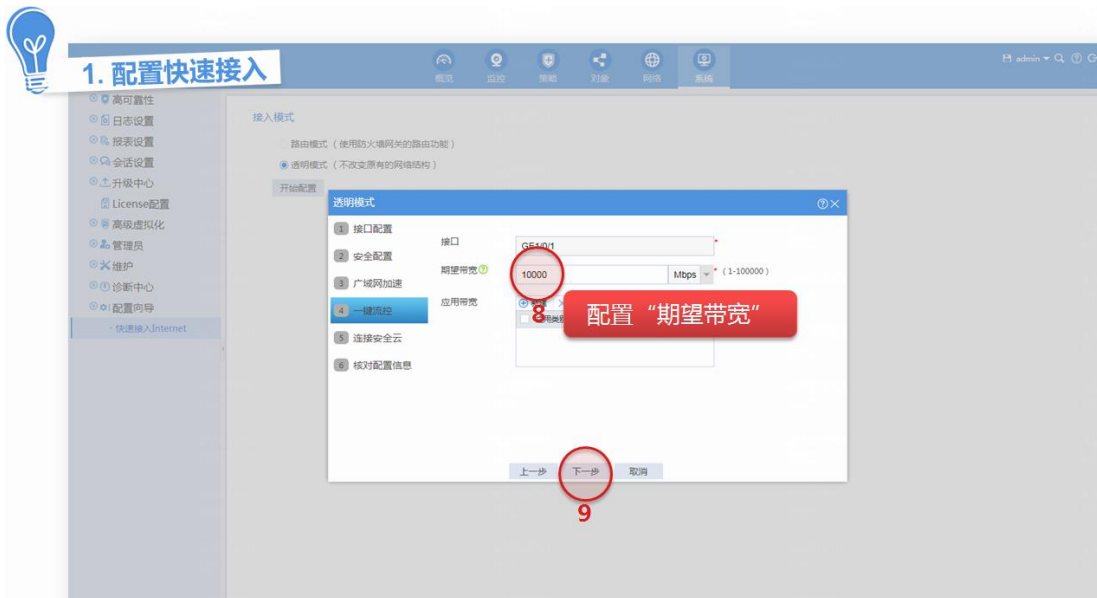
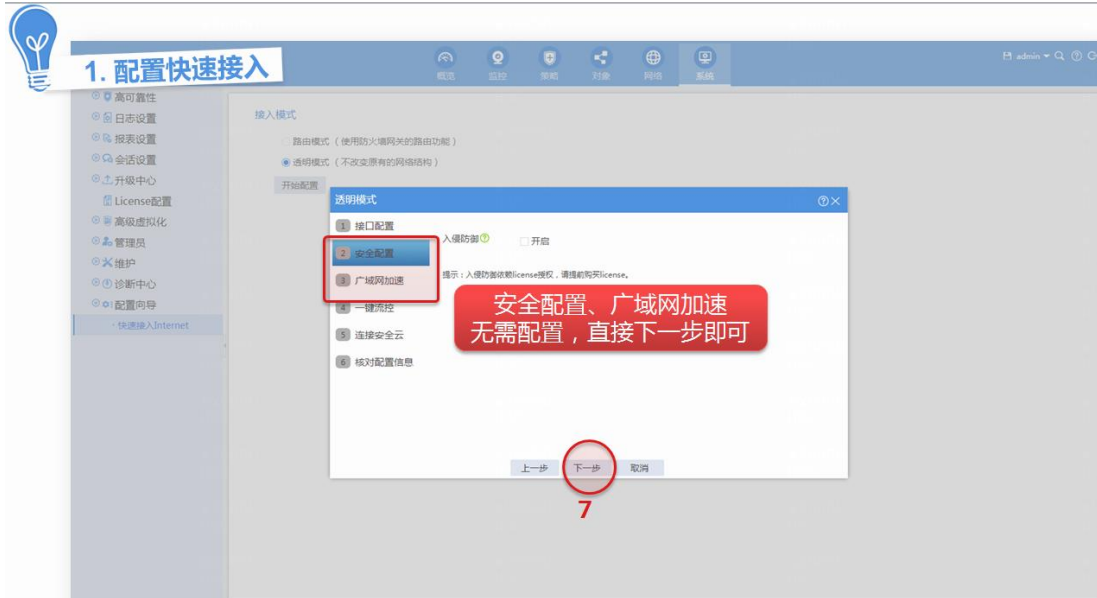
5

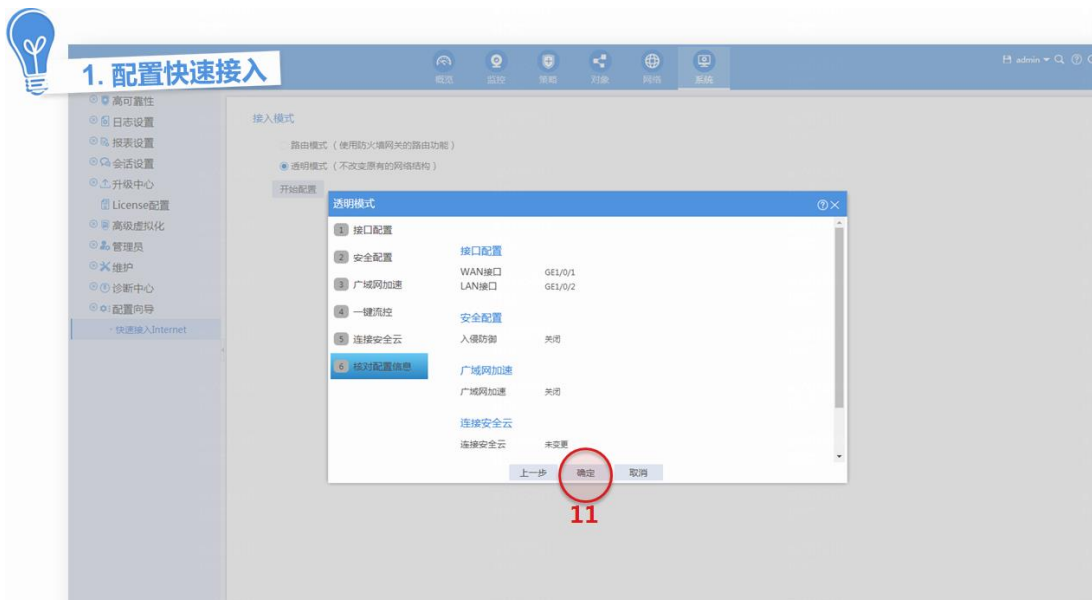
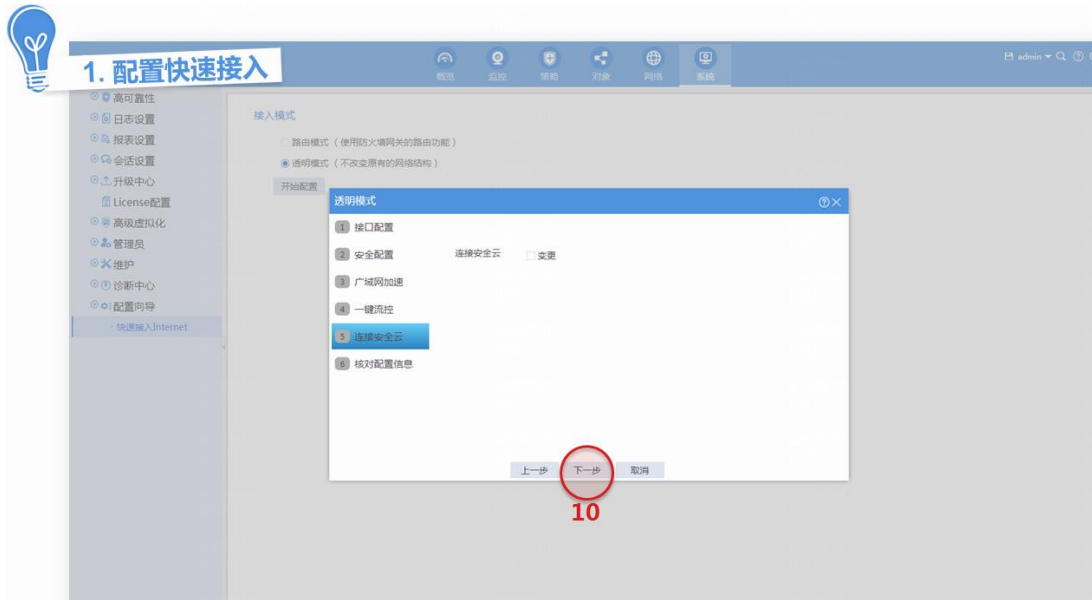


4.5 透明模式接入Internet

不同于路由模式，透明模式采用二层模式（即设备的上下行业务接口工作在二层模式）部署在网络中，此模式下设备一般部署在企业网关内侧，不直接与互联网连接，但可以对网络流量进行安全监测和安全控制。此模式无需路由及 NAT，不改变网络结构，可快速部署设备，上线安全业务。具体配置方法如下。







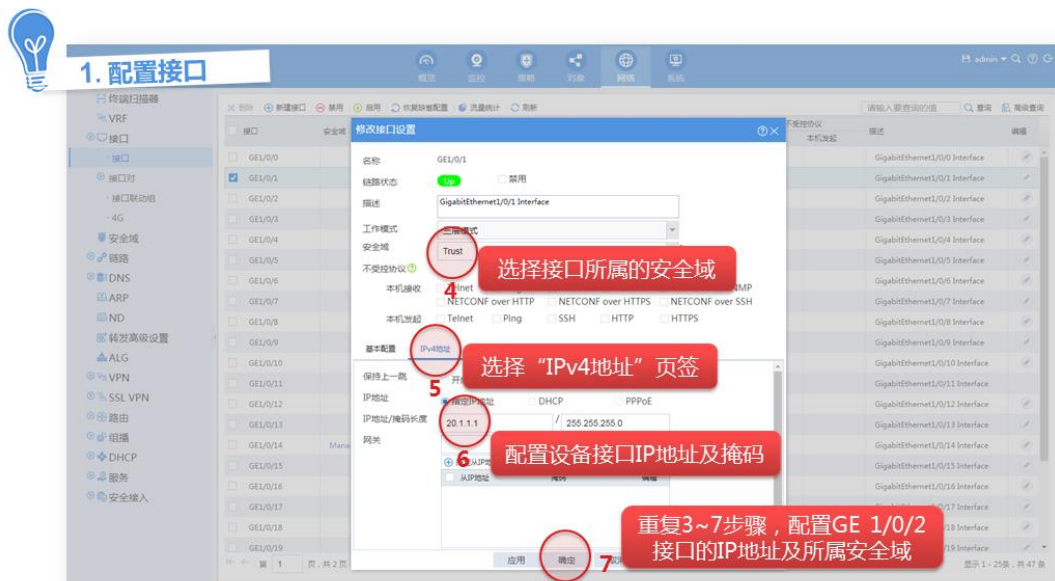
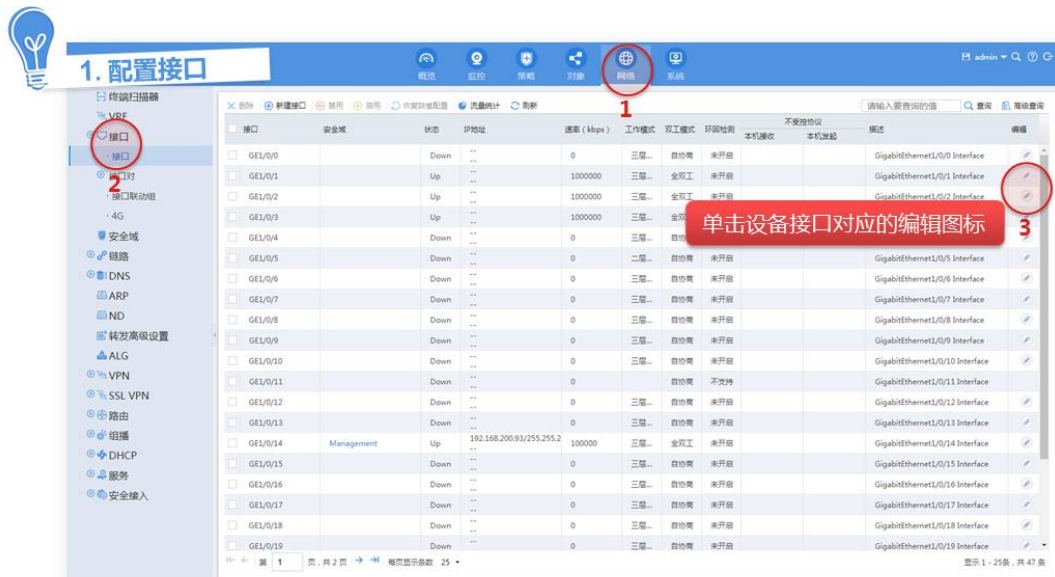
4.6 配置特征库升级

各业务的特征库升级功能需要安装 License 才能使用。License 过期后，各业务可以采用设备中已有的特征库正常工作，但无法升级特征库。

设备支持如下几种升级方式，可根据实际需求选择升级方式：

- 定时升级：设备根据管理员设置的时间定期自动更新本地的特征库。
- 立即升级：管理员手工触发设备立即更新本地的特征库。
- 本地升级：当设备无法自动获取特征库时，需要管理员先手动获取最新的特征库，再更新设备本地的特征库。

4.6.1 定时升级特征库

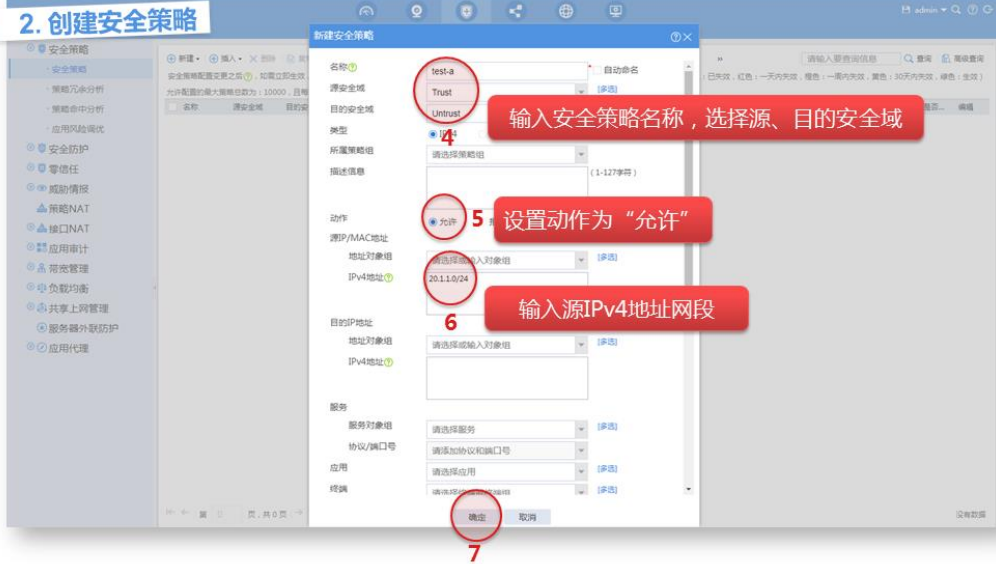




2. 创建安全策略



2. 创建安全策略





2. 配置路由

配置目的IP地址、掩码长度以及下一跳地址，其他配置项使用缺省值



3. 配置DNS服务器地址

域名服务器地址以 10.72.66.36为例

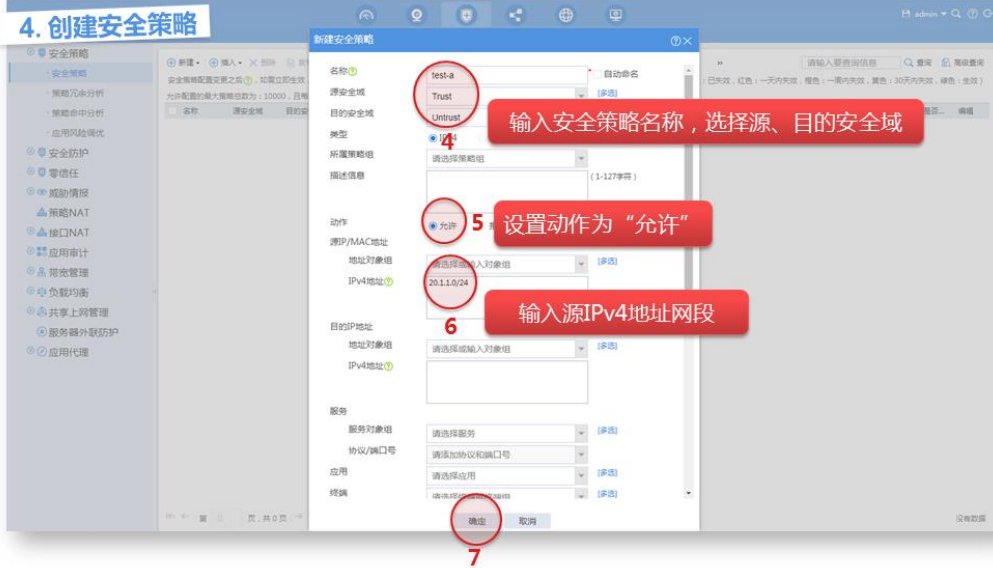
点击<添加>按钮完成添加



4. 创建安全策略



4. 创建安全策略





5. 定时升级特征库

1 勾选需要升级的特征库

2 配置

3

4 确定

设置定时时间

定时升级配置存在抖动时间（即实际自动升级开始时间的偏差范围），取值为指定的定时升级时间的前后一小时

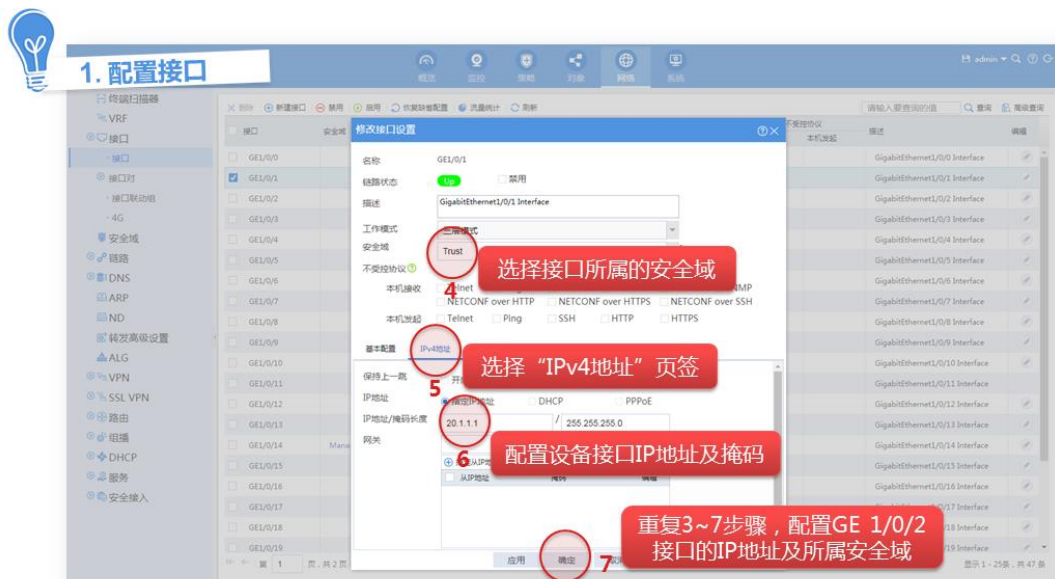
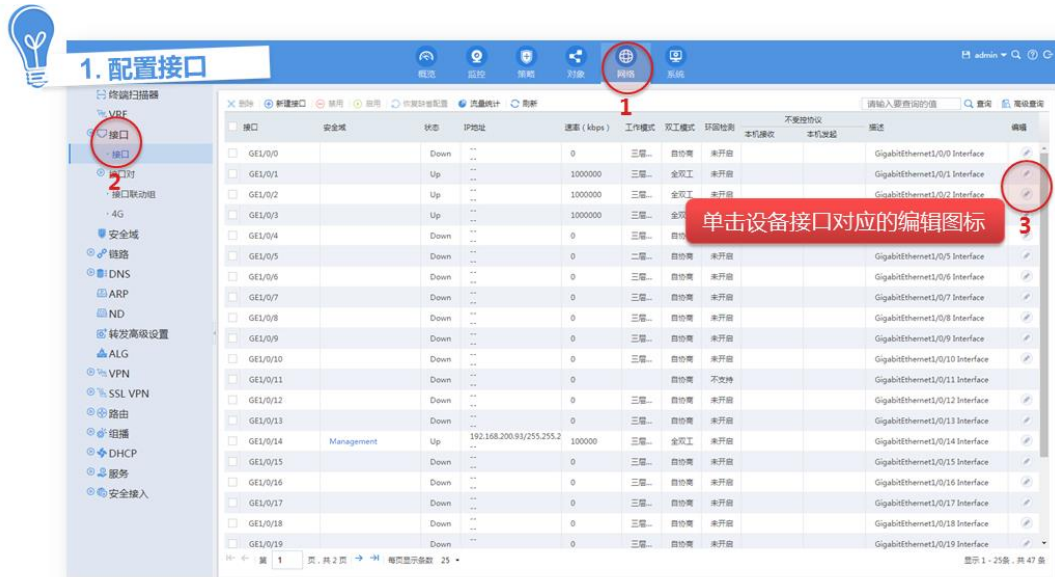
特征库名称	当前版本	版本发布日期	定时升级时间	操作
人眼检测特征库	-	-	每周六 3:00 (默认)	升级
人脸检测特征库	-	-	-	升级
车牌识别特征库	1.0.0	-	-	升级
人脸检测特征库	1.0.0	-	-	升级
人脸检测特征库	-	-	-	升级
人脸检测特征库	-	-	-	升级
人脸检测特征库	-	-	-	升级
人脸检测特征库	-	-	-	升级
人脸检测特征库	-	-	-	升级
人脸检测特征库	-	-	-	升级

人眼检测特征库定时升级配置

定时升级时间: 每周六 3:00 (默认)

确定 取消

4.6.2 立即升级特征库

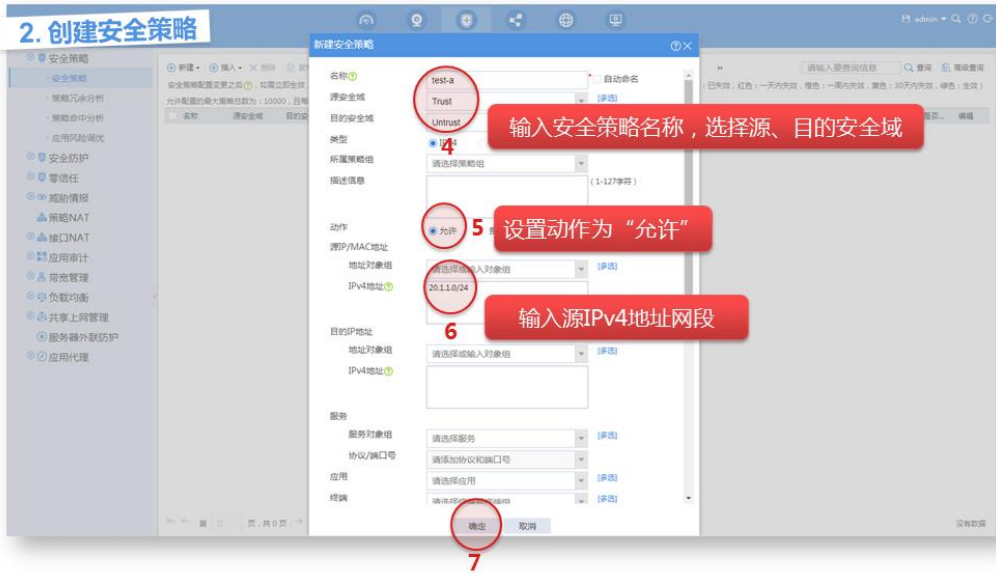




2. 创建安全策略



2. 创建安全策略





2. 配置路由

配置目的IP地址、掩码长度以及下一跳地址，其他配置项使用缺省值

1. 路由配置图标

2. 路由配置入口

3. 目的IP地址

4. 掩码长度

5. 下一跳地址



3. 配置DNS服务器地址

点击<添加>按钮完成添加

域名服务器地址以 10.72.66.36 为例

1. DNS配置图标

2. DNS配置入口

3. 服务器类型

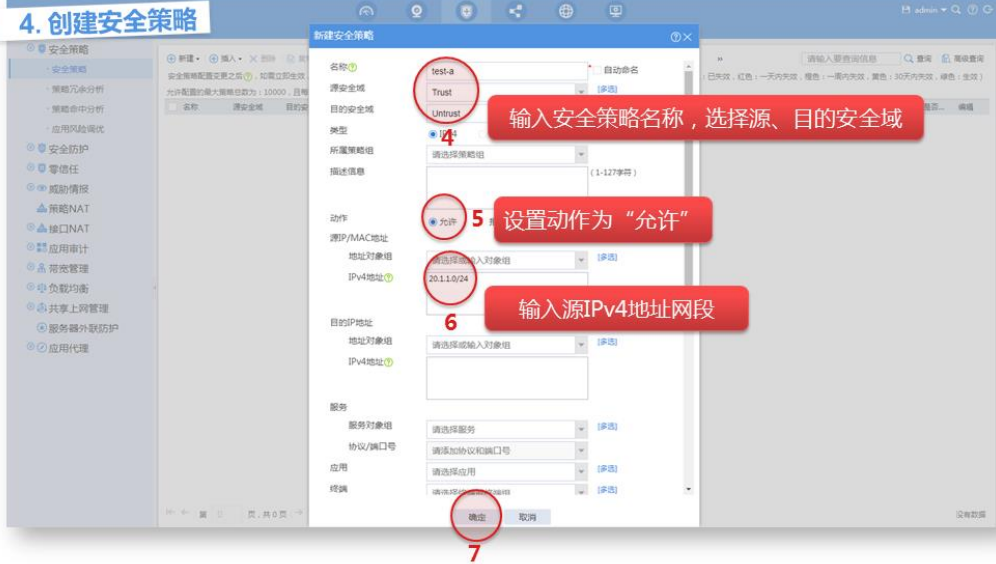
4. 域名服务器地址

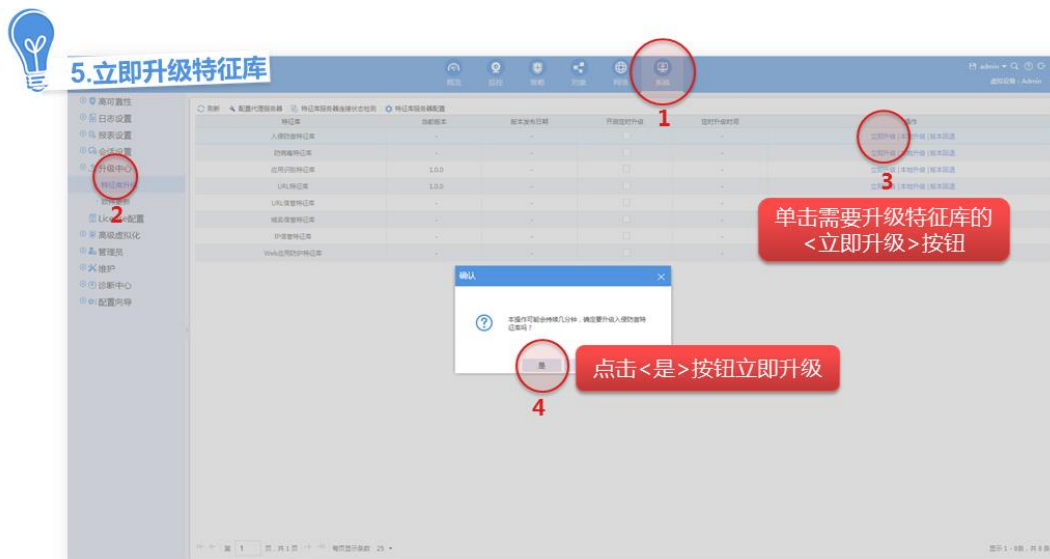


4. 创建安全策略



4. 创建安全策略





4.6.3 本地升级特征库



4.7 License首次激活和安装

设备的部分特性需要获取 License 授权后才能使用，因此为使这些特性能够使用，需要激活这些特性的 License。具体可观看《[H3C 安全产品 License 注册演示视频\(Comware V7\)](#)》完成 License 的激活和安装。

4.8 配置基础安全策略



1. 配置接口

1

2

3

单击设备接口对应的编辑图标

接口	安全域	状态	IP地址	速率 (kbps)	工作模式	双工模式	环回检测	本机接收	本机发起	描述	编辑
<input type="checkbox"/> GE1/0/0		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/0 Interface	
<input type="checkbox"/> GE1/0/1		Up	...	1000000	三层	全双工	未开启			GigabitEthernet1/0/1 Interface	
<input type="checkbox"/> GE1/0/2		Up	...	1000000	三层	全双工	未开启			GigabitEthernet1/0/2 Interface	
<input type="checkbox"/> GE1/0/3		Up	...	1000000	三层	全双工	未开启			GigabitEthernet1/0/3 Interface	
<input type="checkbox"/> GE1/0/4		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/4 Interface	
<input type="checkbox"/> GE1/0/5		Down	...	0	二层	自协商	未开启			GigabitEthernet1/0/5 Interface	
<input type="checkbox"/> GE1/0/6		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/6 Interface	
<input type="checkbox"/> GE1/0/7		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/7 Interface	
<input type="checkbox"/> GE1/0/8		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/8 Interface	
<input type="checkbox"/> GE1/0/9		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/9 Interface	
<input type="checkbox"/> GE1/0/10		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/10 Interface	
<input type="checkbox"/> GE1/0/11		Down	...	0	三层	自协商	不支持			GigabitEthernet1/0/11 Interface	
<input type="checkbox"/> GE1/0/12		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/12 Interface	
<input type="checkbox"/> GE1/0/13		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/13 Interface	
<input type="checkbox"/> GE1/0/14	Management	Up	192.168.200.93/255.255.2	1000000	三层	全双工	未开启			GigabitEthernet1/0/14 Interface	
<input type="checkbox"/> GE1/0/15		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/15 Interface	
<input type="checkbox"/> GE1/0/16		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/16 Interface	
<input type="checkbox"/> GE1/0/17		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/17 Interface	
<input type="checkbox"/> GE1/0/18		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/18 Interface	
<input type="checkbox"/> GE1/0/19		Down	...	0	三层	自协商	未开启			GigabitEthernet1/0/19 Interface	



1. 配置接口

4

5

6

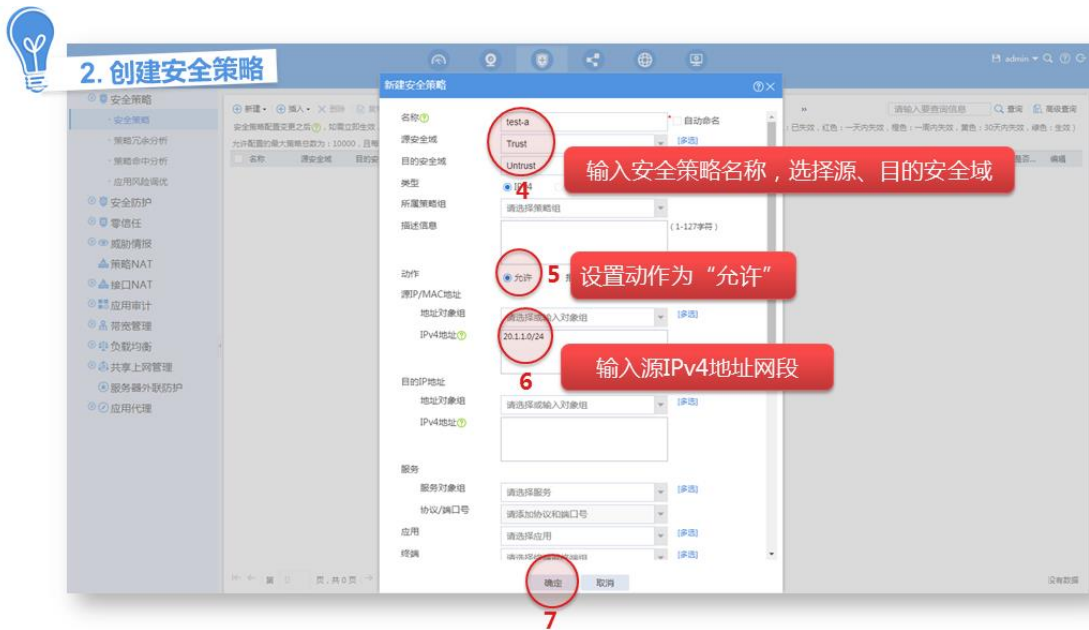
7

选择接口所属的安全域

选择“IPv4地址”页签

配置设备接口IP地址及掩码

重复3~7步骤，配置GE 1/0/2接口的IP地址及所属安全域



4.9 配置恢复出厂设置

4.9.1 特性简介



说明

恢复到出厂配置，将抹去除“.bin”和License文件以外的所有配置，请谨慎使用。



1. 备份至本地

1. 备份至本地

2. 配置文件

3. 备份至本地

4. 备份至本地

5. 确定

选择备份至本地的方式



1. 备份至服务器

1. 备份至服务器

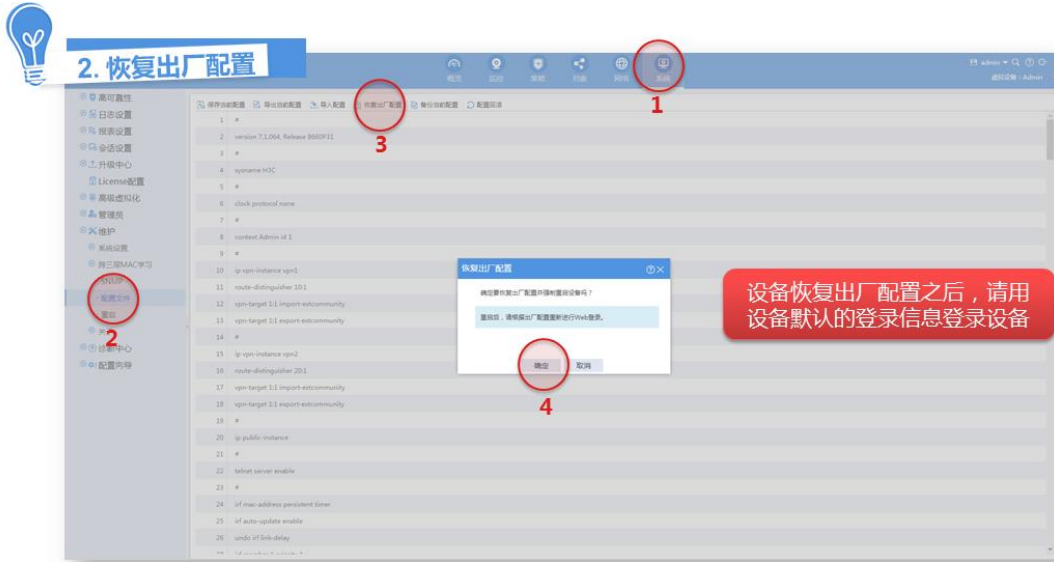
2. 配置文件

3. 备份至服务器

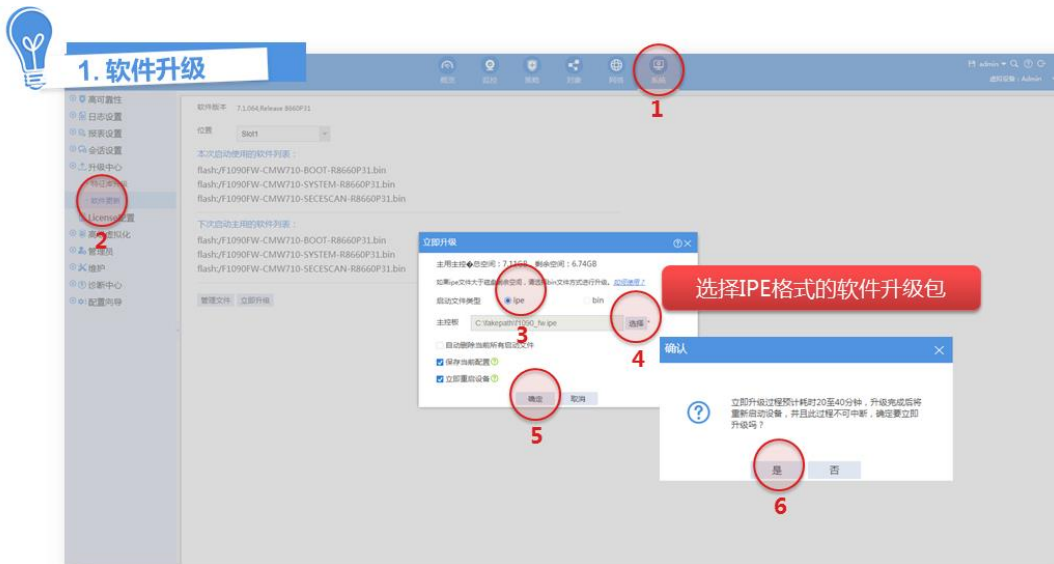
4. 备份至服务器

5. 确定

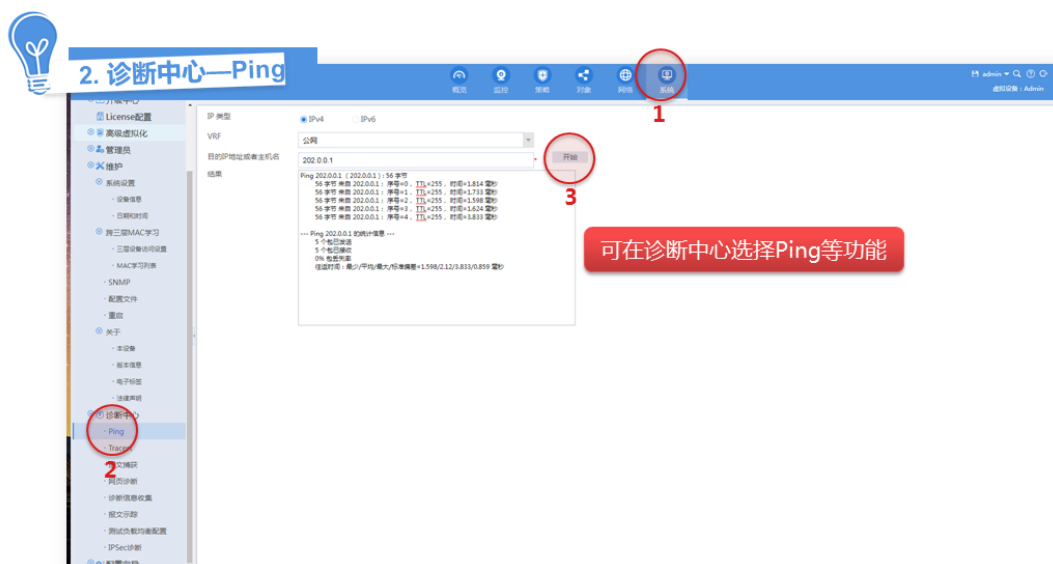
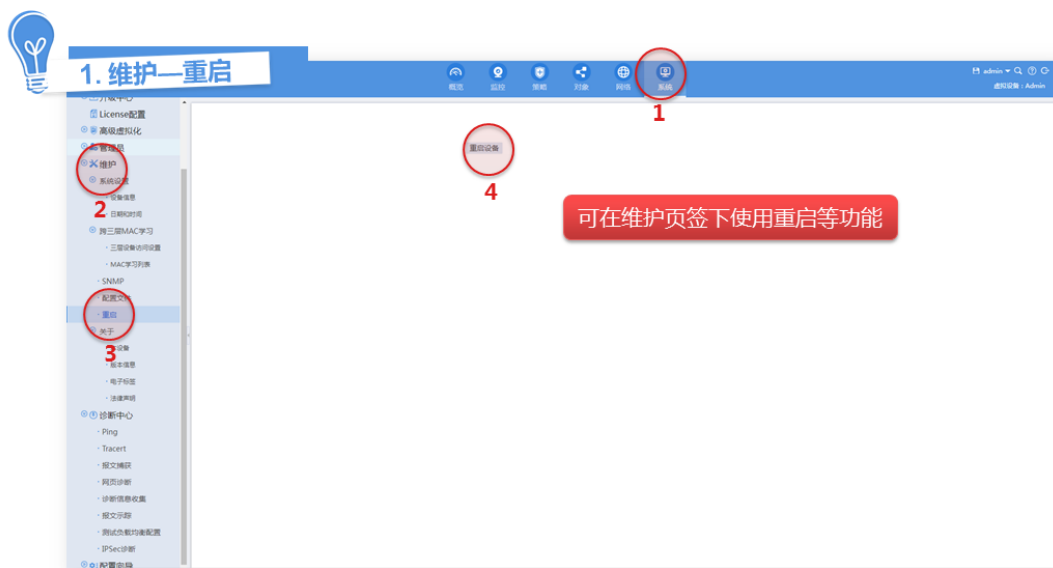
选择备份至服务器的方式



4.10 软件升级



4.11 设备维护和诊断



5 高级功能

5.1 NAT功能

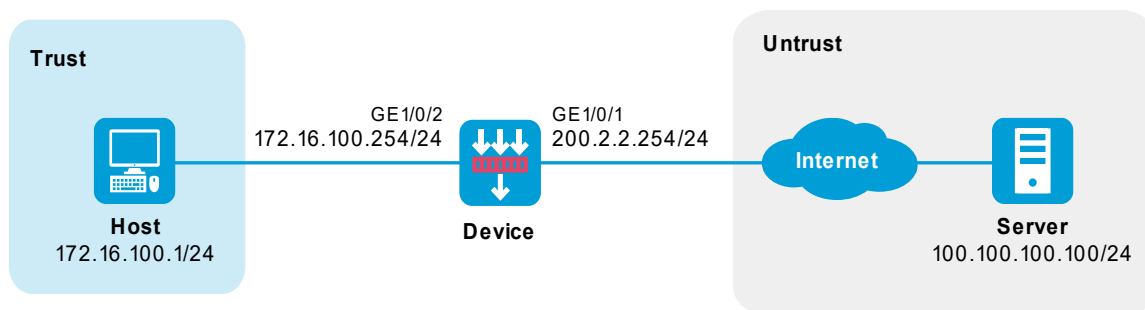
5.1.1 应用场景

NAT (Network Address Translation, 网络地址转换) 是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中, NAT 主要应用在连接两个网络的边缘设备上, 用于实现允许内

部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源（例如内部服务器）的目的。此功能需要在路由模式下使用。

初始配置中，路由模式的快速向导会自动生成了一条内网访问外网流量的 NAT 策略，保证内网可以访问外网。您可以直接使用此 NAT 策略，也可以根据不同网络的实际需求，配置不同的 NAT 策略。

图5-1 NAT 功能示意图



5.1.2 配置方法

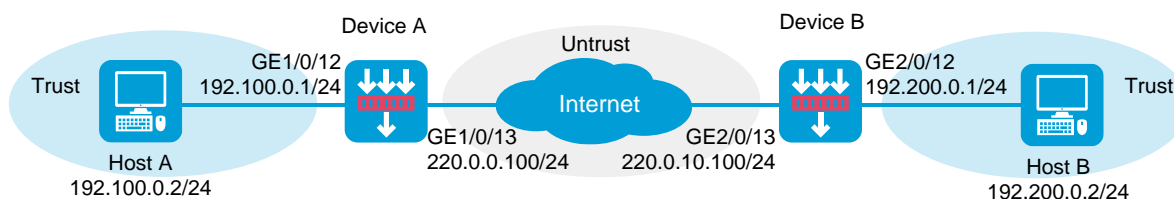
有关 NAT 相关功能的配置视频，请点击此链接 [《H3C SecPath 系列防火墙 Web 典型配置演示视频》](#) 观看《全局 NAT 目的地址转换典型配置举例演示视频》和《全局 NAT 源地址转换典型配置举例演示视频》。

5.2 远程办公接入之IPsec方式

5.2.1 应用场景

IPsec (IP Security, IP 安全) 是 IETF 制定的三层隧道加密协议，它为互联网上传输的数据提供了高质量的、基于密码学的安全保证，是一种传统的实现三层 VPN (Virtual Private Network, 虚拟专用网络) 远程办公的安全接入技术。IPsec 通过在特定通信方之间 (例如两个安全网关之间) 建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。

图5-2 IPsec 功能示意图



5.2.2 配置方法

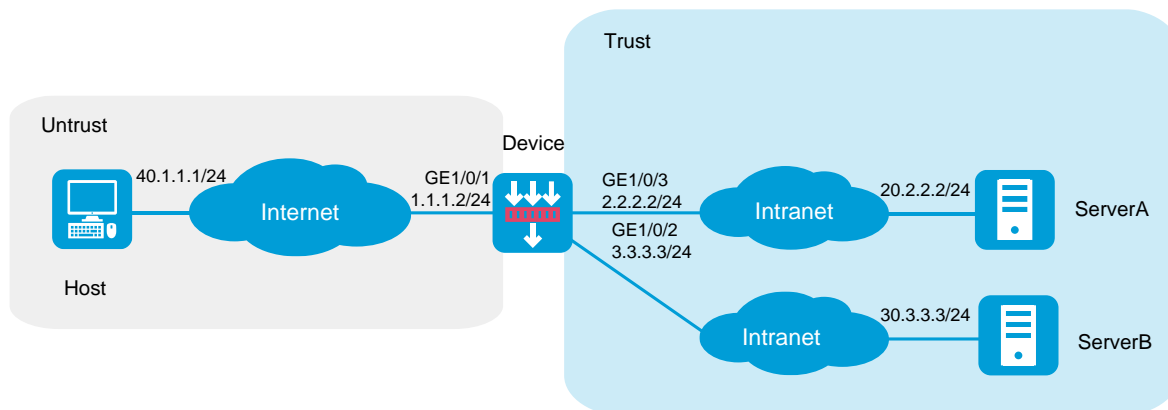
有关 IPsec 相关功能的配置视频，请点击此链接 [《H3C SecPath 系列防火墙 Web 典型配置演示视频》](#) 观看《IPsec 典型配置举例演示视频》。

5.3 远程办公接入之SSL VPN方式

5.3.1 应用场景

SSL VPN 以 SSL（Secure Sockets Layer，安全套接字层）为基础提供远程的安全连接服务。用户可通过互联网，使用内嵌 SSL 协议的浏览器与远端的 Web 服务器建立安全的连接，访问内部资源。企业或机构可通过 SSL VPN 来为移动用户或者外部客户提供访问内部资源的服务并保证安全性。

图5-3 SSL VPN 功能示意图



5.3.2 配置方法

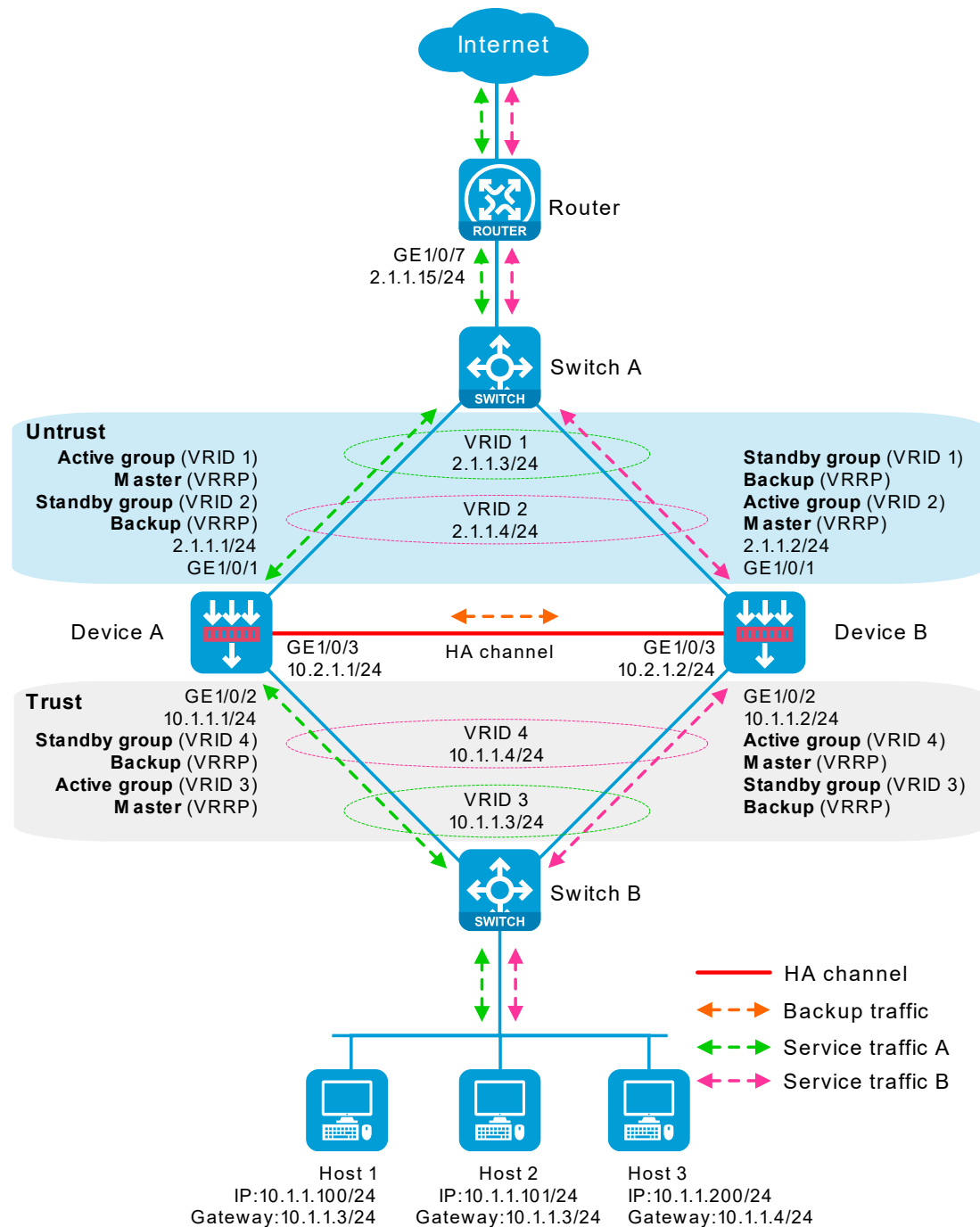
有关 SSL VPN 相关功能的配置视频，请点击此链接 [《H3C SecPath 系列防火墙 Web 典型配置演示视频》](#) 观看《SSL VPN IP 接入配置演示视频》。

5.4 双机热备功能

5.4.1 应用场景

双机热备是一种设备级的高可靠性（High Availability，简称 HA）的技术。此技术能够在通信线路或设备产生故障时提供备用方案，当其中一个网络节点发生故障时，另一个网络节点可以接替故障节点继续工作。双机热备通过我司私有的 RBM（Remote Backup Management，远端备份管理）协议来实现。

图5-4 双机热备功能示意图



5.4.2 配置方法

有关双机热备相关功能的配置视频，请点击此链接《[H3C SecPath 系列防火墙 Web 典型配置演示视频](#)》观看《HA 联动 VRRP 双主典型配置举例演示视频(IPv4)》、《HA 联动 VRRP 主备典型配置举例演示视频(IPv4)》、《HA 联动路由双主典型配置举例演示视频(IPv4)》和《HA 联动路由主备典型配置举例演示视频(IPv4)》。

6 更多参考信息

至此，您已了解和掌握了防火墙的基本功能和部分常用的高级功能。后续您可以登录 H3C 官网，访问“文档中心”或“知了社区”获取更多的产品知识。有个产品资料的具体使用方法请参考如下。

图6-1 产品资料获取方法示意图



按产品检索 → 选择 [安全]

各产品栏目中的资料根据款型系列划分，您可以在清单中直接点击进入具体产品的资料栏目。



快速检索 → 输入产品系列名称的关键字 → 从关键字匹配结果中选择其一

快速检索功能为您提供了在产品栏目中快速定位到具体产品资料入口的便捷操作。

快速检索



常见资料栏目

全部文档 | 显示本产品栏目下全部文档

文档合集 | 资料书架 CHM文档包

快速系列 | 快速安装 快速配置 产品FAQ

视频专区 | 安装视频 产品介绍视频 技术介绍视频 配置视频

了解产品 | 产品介绍 安全和兼容性手册

了解技术 | 技术白皮书 技术介绍

安装升级 | 安装指导 可插拔部件手册 升级指南 License指南 Visio模具

配置调测 | 配置指导 典型配置举例 高危操作手册 安全加固手册

参考指南 | 命令参考 日志参考 MIB参考

诊断维护 | 故障处理手册

二次开发 | 开发指南 API参考

工具 | 命令查询 日志查询 H3C个人资料库

说明：安全产品系列众多，针对不同产品系列配套的资料栏目和手册稍有差异，请以网站显示为准。