

★完全公开

网神 SecGate 3600 防火墙 快速上线部署手册 V1.0



网络安全服务热线：95015

公司网址：<https://www.qianxin.com/>

联系地址：北京市西城区西直门外南路 26 号院 1 号楼

邮编：100044

● 版权声明

奇安信集团，保留所有权利。

奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。

对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（“**本声明**”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“**本产品**”）。如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。您有责任定期检查免责声明部分的内容，以了解是否发生了变更。如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**
2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。
3. 您明确理解并同意，您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：**1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5)政府管制、网络故障、国家政策变化、法律法规之变化等。**如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。
4. 对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。
5. 对于从非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的**本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛

伊木马程序或者黑客软件。使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。

6. 上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。
 7. 奇安信集团保留在不发布通知的情况下随时采取以下行动的权利：在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。
 8. 本声明受中华人民共和国法律的约束并依据其解释。
 9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。
-

数据安全分级标注说明

■ 数据分级	公开数据 (Y)	内部数据 ()	普通商秘 ()	核心商秘 ()
<p>*数据分级标注及说明：</p> <p>1、文档编写前，应标注数据安全级别，默认为内部；</p> <p>2、请根据文档内容评估数据安全级别，在对应数据级别 () 中填写 (Y) ；</p> <p>3、分级 TIPS:</p> <p>【核心商秘】：限于个别人、小范围共享和使用的信息，例如薪酬数据、未公开的产生严重危害的样本等。如泄露将导致法律风险或者影响到社会公众利益或者严重的恶意竞争等；</p> <p>【普通商秘】：限于特定人群、特定范围内共享和使用的信息，例如公司组织架构、产品样本集等。如泄露存在合规风险或者可能影响社会公众个人利益或者存在一般恶意竞争的风险等；</p> <p>【内部数据】：限于在公司范围内按需使用，除去公开数据、核心商秘、普通商秘，都为内部数据。如泄露不存在法律合规风险或不存在影响社会公众个人利益的风险，但会产生轻微的恶意竞争风险等；</p> <p>【公开数据】：对任何方面都无危害的、不会被任何方面进行利用的信息，例如官网上的产品简介等。如泄露对任何方面都无影响。</p> <p>更多分级 Tips 参考链接: https://sec.qianxin-inc.cn/data-security/data-classification-tips</p>				

目录

1 手册概述.....	9
1.1 手册简介	9
1.2 适用产品	9
1.3 读者对象	9
1.4 配套手册	9
1.5 符号约定	9
1.6 修订记录	10
2 设备上架.....	11
2.1 产品简介	11
2.1.1 面板示意图	11
2.1.2 指示灯	11
2.1.3 技术指标.....	12
2.2 安装前准备.....	13
2.2.1 工具准备.....	13
2.2.2 安装环境确认	14
2.3 设备上架	15
2.4 确定配置方式.....	17
2.4.1 确定接口部署模式	18
2.4.2 确定双机热备模式	20
3 购买产品许可证.....	23
4 通过管理口管理防火墙	24
4.1 防火墙登录相关说明	24
4.1.1 防火墙管理口和默认 IP	24
4.1.2 防火墙默认账号	24
4.2 准备工作	24
4.2.1 IP 规划	24
4.2.2 物理连接.....	24
4.3 登录防火墙 web 页面	25
4.4 使用部署向导快速配置.....	27
4.4.1 透明模式.....	28
4.4.2 路由模式.....	29
4.4.3 旁路镜像.....	31

4.5 重点功能配置	32
4.6 软件维护	32
5 通过智慧管理分析系统管理防火墙	33
5.1 在防火墙上配置集中管理	33
5.1.1 登录防火墙 web 页面.....	33
5.1.2 配置集中管理	33
5.2 使用智慧管理分析系统配置防火墙	34
5.2.1 登录智慧管理分析系统	34
5.2.2 配置防火墙	34
6 重点功能配置	35
6.1 HA 相关配置	35
6.1.1 主备模式.....	35
6.1.2 主主模式.....	37
6.2 配置安全策略与高级功能	39
6.2.1 配置高级功能	39
6.2.2 配置安全策略	39
6.3 配置攻击防护	40
6.4 配置流量编排	41
6.4.1 接口工作模式设置	41
6.4.2 添加网元组	41
6.4.3 添加服务链	43
6.4.4 添加引流策略	44
6.5 配置 SSL 解密.....	45
7 软件维护.....	48
7.1 导入许可证.....	48
7.2 系统和库升级	48
7.2.1 系统升级和打补丁	48
7.2.2 特征库升级	49
7.2.3 威胁情报库升级	50
7.3 双机场景下配置同步	51
7.3.1 执行配置对比操作	51
7.3.1 手动配置同步	52
7.4 常用操作	52
7.4.1 保存当前配置	52

7.4.2 查看告警详情	52
7.4.3 查看 License 状态提示信息	52
7.4.4 切换虚拟系统	52
7.4.5 账号相关操作	53
7.4.6 导入导出配置文件	53

1 手册概述

1.1 手册简介

本手册是《网神 SecGate 3600 防火墙 快速上线部署手册》，主要用于指导用户快速上线网神 SecGate 3600 防火墙，能够快速联网和快速部署重点功能。

1.2 适用产品

本手册适用于网神 SecGate 3600 防火墙产品。

与本文档相对应的产品版本如下所示。

产品名称	产品版本
网神 SecGate 3600 防火墙	V3.6.6.0(-6.1.15.170368&6.90.15.170368&6.91.15.170368)

1.3 读者对象

本文档主要适用于负责配置和维护防火墙的安全管理员。

本手册默认用户掌握 TCP/IP 协议、IP 地址及子网掩码等基本知识。




1.4 配套手册


《网神 SecGate 3600 防火墙 用户手册》为首次安装、使用提供指导。同时列举管理产品的基本操作方法。

《网神 SecGate 3600 防火墙 配置指南》以案例的形式为用户提供配置指导，并列举常见问题解决方法。

1.5 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号名称	说明
 警告	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤亡。
 注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

符号名称	说明
 窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

1.6 修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 V1.0（发布日期 2023-11-22）

第一次正式发布。

2 设备上架

2.1 产品简介

2.1.1 面板示意图

本小节主要介绍防火墙前面板指示灯及其相应状态，图中所示的接口数仅为示例，与用户实际购买使用的设备可能不符，请用户以实际购买为准。

网神 SecGate3600 防火墙系统允许通过专门的管理口（MGT 接口）或不带 MGT 接口，第一个业务接口（GE1）登录防火墙 Web 配置页面。

图 2-1 和图 2-2 所示为设备面板示意图。不同型号的面板不同，但上面的指示灯功能基本相同，部分产品具备▽/△指示灯。具体面板请以实际产品为准。

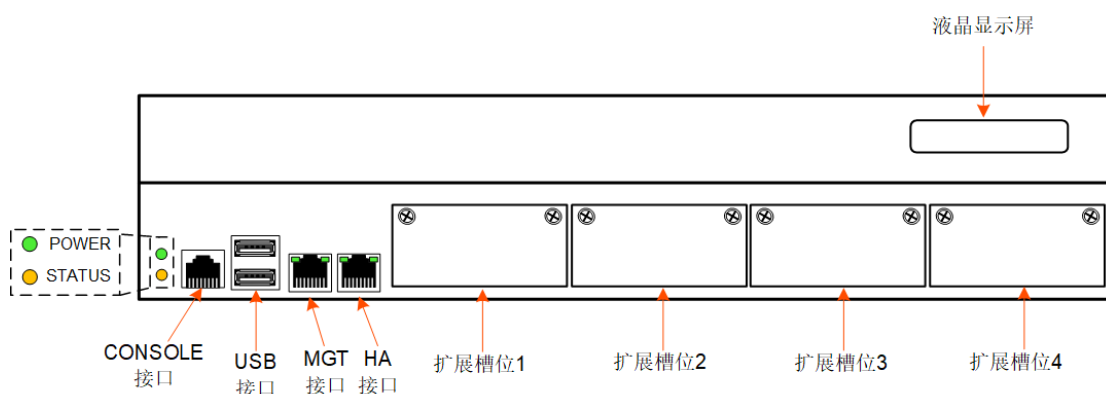


图 2-1 面板示意图（带 MGT）

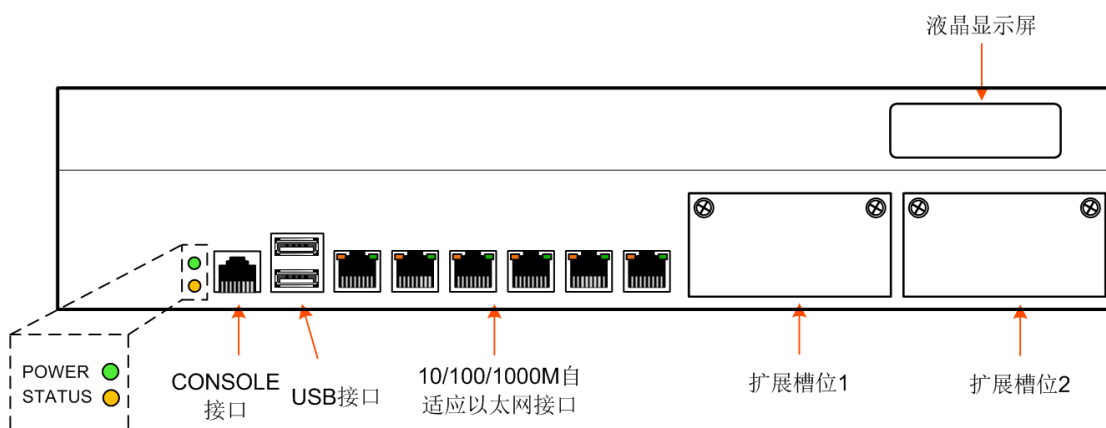


图 2-2 面板示意图（不带 MGT）

2.1.2 指示灯

防火墙面板指示灯的含义如表 2-1 所示。

表 2-1 面板指示灯

指示灯名称	颜色	描述
POWER	绿色	电源工作状态指示灯 ● 亮：表示电源供电正常 ● 灭：表示电源电压不稳，供电不正常
STATUS	橙色	系统工作指示灯 ● 闪烁：表示系统硬盘正在读写，或者系统正在启动过程中 ● 灭：表示系统正常，无硬盘读写操作
LNK/ACT (RJ45 接口左侧灯)	橙色	GE 接口和串口工作状态指示灯 ● 亮：表示接口连接正常，但无数据传输 ● 闪烁：表示接口连接正常，且正在进行数据传输 ● 灭：表示接口连接不正常
SPEED (RJ45 接口右侧灯)	橙色	GE 接口和串口工作速率指示灯 ● 亮：表示接口的工作速率为 1000M ● 灭：表示接口工作速率为 100M/10M 或者接口工作不正常
LINK/ACT (业务接口左侧灯)	绿色	SFP 光接口工作状态指示灯 ● 亮：表示接口连接正常，但无数据传输 ● 闪烁：表示接口连接正常，且正在进行数据传输 ● 灭：表示接口连接不正常
SPEED (业务接口右侧灯)	绿色	接口工作速率指示灯 ● 亮：表示千兆业务接口工作速率为 1000M；万兆业务接口工作速率为 10G ● 灭：表示千兆业务接口工作速率为 100M 或者接口连接不正常；万兆业务接口工作速率为 1000M 或者接口工作不正常
▽/△ (光接口底座上， ▽对应下方光口， △对应上方光口)	绿色	SFP/SFP+光接口工作状态指示灯 ● 亮：表示接口连接正常，但无数据传输 ● 闪烁：表示接口连接正常，且正在进行数据传输 ● 灭：表示接口连接不正常

2.1.3 技术指标

产品整机指标如表 2-2 所示。

表 2-2 产品整机指标

分类	技术指标	说明
尺寸	整机尺寸	<ul style="list-style-type: none"> ● NSG2000 系列 <ul style="list-style-type: none"> 1U: 440mm (宽) × 330mm (深) × 45mm (高) 2U: 440mm (宽) × 500mm (深) × 89mm (高) ● NSG3000 系列 <ul style="list-style-type: none"> 桌面型: 200mm (宽) × 310mm (深) × 44mm (高) 1U: 426mm (宽) × 330mm (深) × 44mm (高) 2U: 440mm (宽) × 520mm (深) × 89mm (高) ● NSG4000 系列 <ul style="list-style-type: none"> 1U: 440mm (宽) × 330mm (深) × 45mm (高) 2U: 440mm (宽) × 500mm (深) × 89mm (高) ● NSG5000 系列 <ul style="list-style-type: none"> 440mm (宽) × 560mm (深) × 89mm (高) ● NSG5900 系列 <ul style="list-style-type: none"> 440mm (宽) × 560mm (深) × 89mm (高) ● NSG6000 系列 <ul style="list-style-type: none"> 1U: 442mm (宽) × 560mm (深) × 44.2mm (高) 2U: 442mm (宽) × 560mm (深) × 88.4mm (高) ● NSG7000 系列 <ul style="list-style-type: none"> 440mm (宽) × 560mm (深) × 89mm (高) ● NSG8000 系列 <ul style="list-style-type: none"> 440mm (宽) × 560mm (深) × 89mm (高) ● NSG9000 系列 <ul style="list-style-type: none"> 3U: 440mm (宽) × 600mm (深) × 133mm (高)
电源参数	额定输入电压	100V AC~240V AC, 50Hz/60Hz
环境参数	工作温度	0℃~+40℃
	工作湿度 (RH)	5%~90%, 无凝结
	储存温度	-25℃~+70℃



说明

设备尺寸不计面板螺钉、挂耳等突出部件。

2.2 安装前准备

2.2.1 工具准备

工具	数量	用途
Console 线缆	1	用于连接设备的 Console 接口，初始化和调试设备使用。

工具	数量	用途
网线	若干	用于连接设备的以太网接口和其他设备，例如连接 PC 用来调试设备。或连接其他设备用于检查设备是否配置正确。
十字型螺丝刀	1	PH2×75 或 PH2×100 规格，批头为强磁批头。
标记笔	1	彩色标记笔，用于在机柜上安装导轨时，标记导轨的位置。
其他	-	安装设备前，需要提前与用户沟通，明确安装条件，缺少的辅材需要提前准备。

2.2.2 安装环境确认

防火墙设备必须在室内使用，为保证设备的正常工作和延长使用寿命，在设备的安装和使用过程中，特提出如下安全建议：

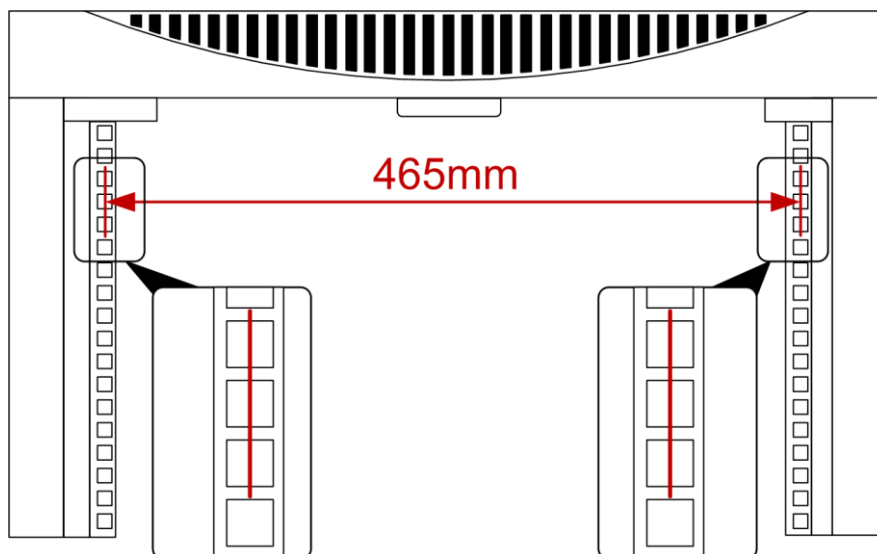
- 请将设备放置在远离潮湿或远离热源的地方。
- 请确认设备已经正确接地。

保护地线的正常连接是设备防雷、抗干扰的重要保障，所以用户在安装、使用设备时必须首先正确接好保护地线。

- 请在安装维护过程中预防静电。
- 建议用户使用 UPS（Uninterrupted Power Supply，不间断电源）。

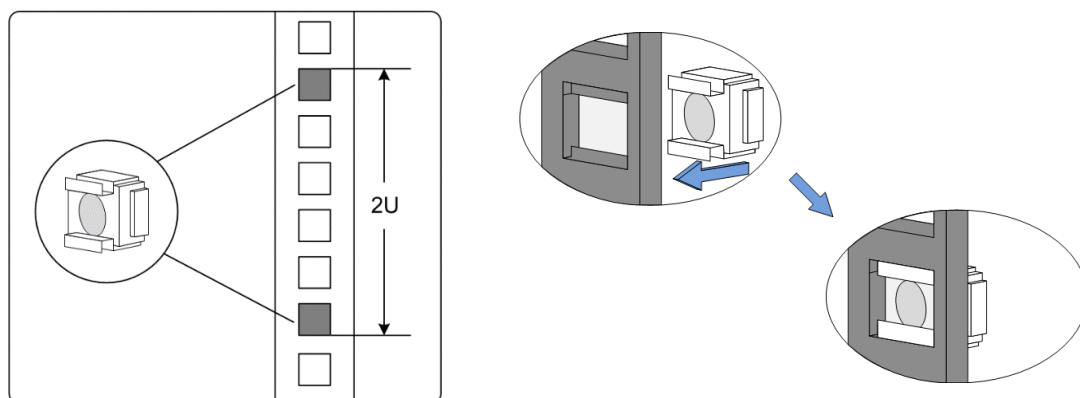
桌面型设备可以直接放在平台上；机架型设备可以放在机架上或直接放置于平台上，设备四周要留出散热空间，并且不要在设备上面放置重物。

- 用户安装设备的机柜应该为 19 英寸标准机柜，机柜深度大于 800mm，两个方孔条安装孔之间的距离为 465mm。
- 设备为前后维护方式，不能靠墙安装，需保证维护过道空间大于 760mm。



2.3 设备上架

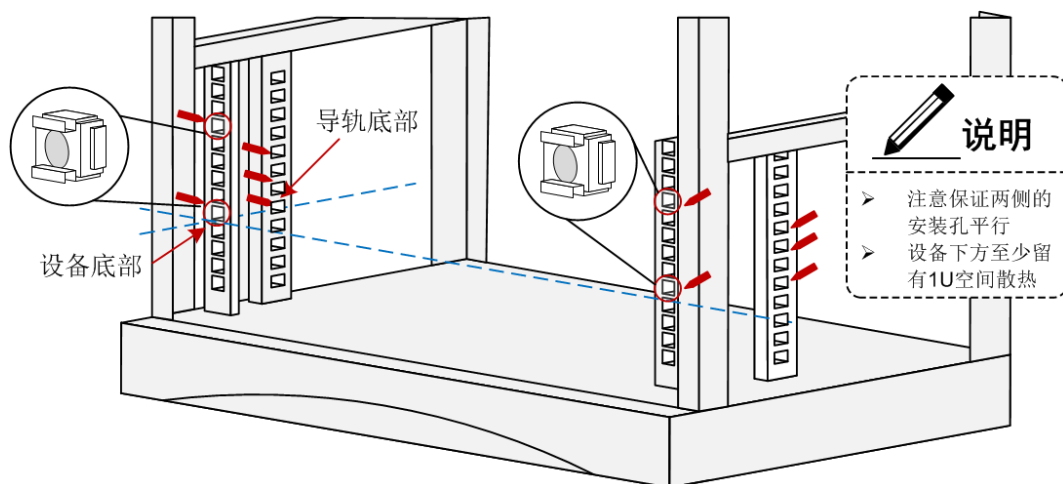
步骤1 确定设备的安装位置。设备通过两侧的挂耳固定在机柜中。首选需要明确设备的安装位置，并在机柜两侧的方形孔条上安装浮动螺母。



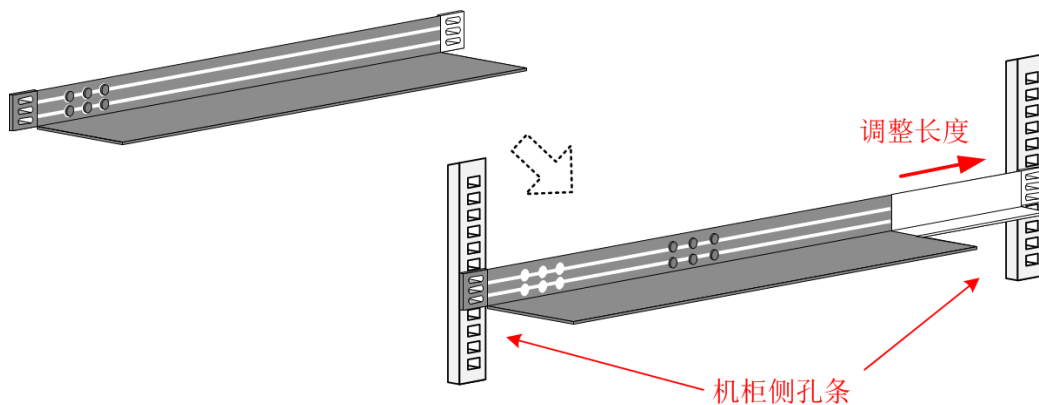
步骤2 标记导轨的安装位置。先根据设备安装孔的下边沿向内找出导轨安装孔的位置，并用标记笔标记。然后在机柜侧面孔条上的标记处安装浮动螺母。

说明

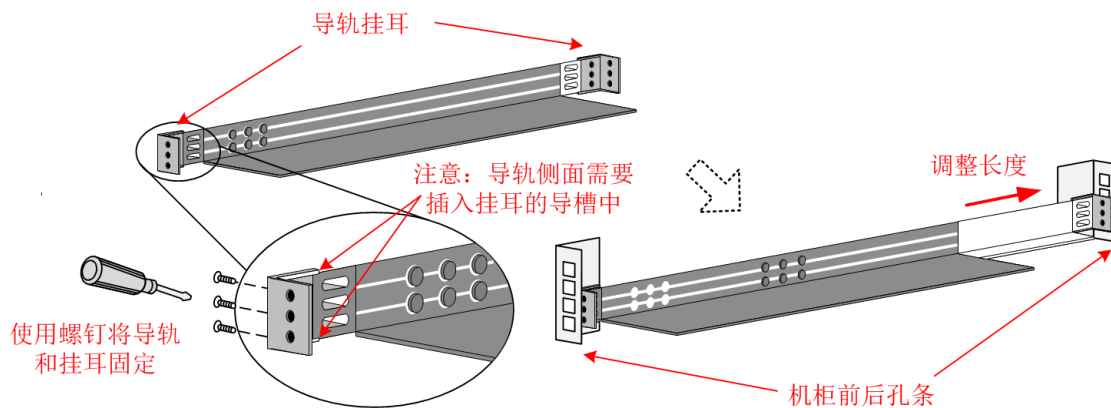
注意保证两侧安装孔平行，可以根据机柜两侧孔条上标记的数字来协助对齐。



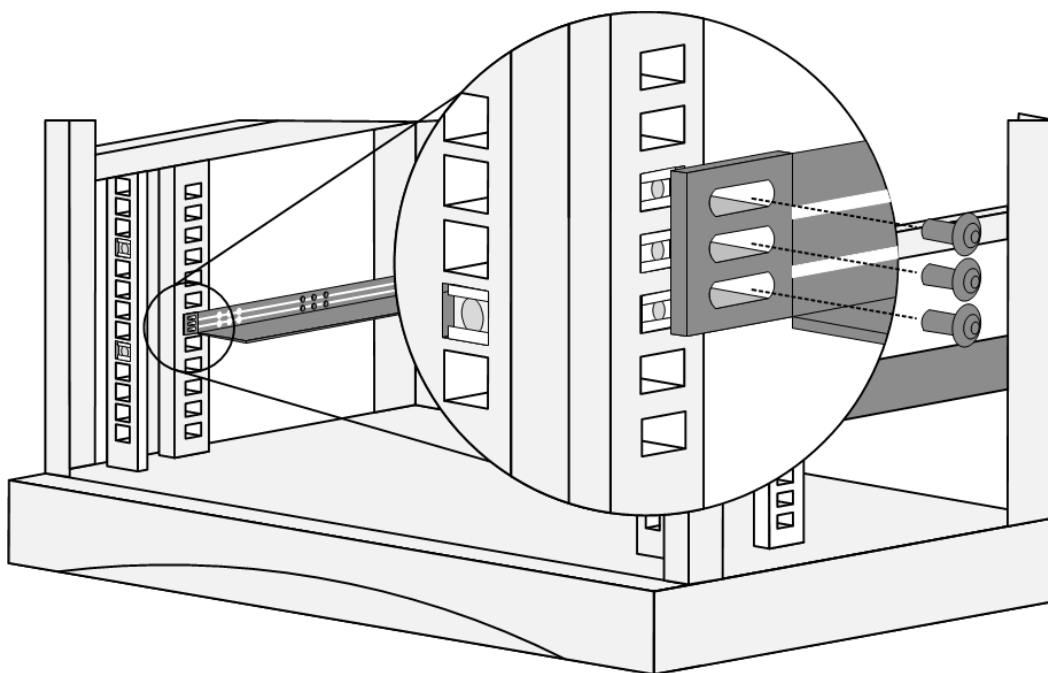
步骤3 设备附带的导轨为两段式，长度可调导轨。当机柜为标准机柜，包含侧孔条时，可以将导轨安装在侧孔条上。安装前需要首先调整导轨的长度，保证导轨的长度与机柜的侧面前后两个孔条的距离一致。



步骤4 在没有侧孔条的非标准机柜或机架上安装时，需要首先在导轨上安装挂耳，然后将导轨安装在机柜的前后孔条上。



步骤5 使用螺钉将导轨固定在机柜上。



步骤6 将防火墙抬起，平稳缓慢地放在导轨上。沿着导轨轻轻地将设备推入机柜，直到防火墙的挂耳贴合在机柜前方的孔条上为止。推入设备时请注意设备的角度，不要让设备撞击到机柜后面的立柱。

说明

设备较重，建议搬运时至少 2 人一起协助完成。安装过程中需小心被砸伤或挤伤。

步骤7 使用螺钉将防火墙固定在机柜上。

2.4 确定配置方式

配置方式需要确定防火墙接口的部署模式，是否双机部署，以及是否采用集中

管理系统或第三方服务器进行管理。

- 通过防火墙管理口进行配置，请参见“4 通过管理口管理防火墙”。
- 通过智慧管理分析系统管理防火墙，请参见“5 通过智慧管理分析系统管理防火墙”。
- 通过 API Restful 北向接口进行管理，请参见《网神 SecGate3600 防火墙 RESTful API 使用指南》。

2.4.1 确定接口部署模式

2.4.1.1 路由模式

路由模式下，防火墙接口工作在三层，接口需要配置 IP 地址。典型组网如图 2-3 所示。

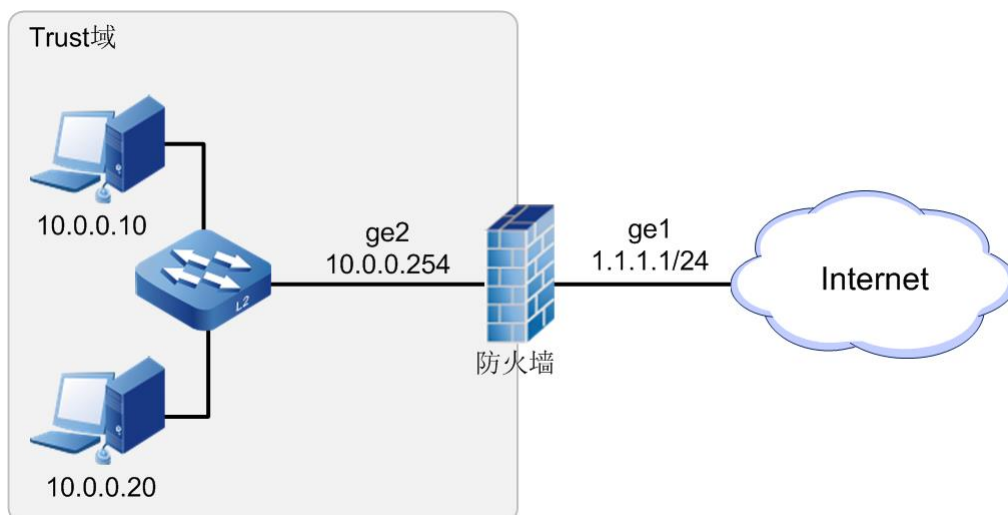


图 2-3 路由模式

在路由模式下，防火墙作为用户内网访问外网的网关，承担着路由交换、IP 分配、NAT 等功能。防火墙能对网络中的流量进行检测，并对包含威胁的流量进行阻断或重置。

2.4.1.2 透明模式

交换模式下，防火墙接口工作在二层，不需要配置 IP 地址。防火墙透明接入汇聚交换机和出口网关之间。透明模式接入支持 VLAN 接入、桥接入。

2.4.1.2.1 VLAN 接入场景

基于接口来划分 VLAN 时，需要绑定 VLAN 和接口。用户主机被划分到其连接接口绑定的 VLAN 下。

接入 VLAN 场景，接口的交换模式支持 Access 和 Trunk。

- 模式为 Access

链路类型为 Access 的接口只能属于某一个 VLAN，接收和发送本 VLAN 内的报文。一般用于连接终端 PC。

- 模式为 Trunk

链路类型为 Trunk 的接口可以接收和发送多个 VLAN 的报文。一般与交换设备的 trunk 接口对接。

2.4.1.2.2 透明桥接场景

桥（Bridge）模式下，用户将 2 个或 2 个以上物理接口绑定同一个桥，桥透明接入用户网络。桥可以通过绑定桥接口配置 IP 地址，管理员可以通过桥接口管理防火墙。

如图 2-4 所示，防火墙通过桥方式透明接入用户网络，保护 VLAN10 和 VLAN20 的子网。PC1 或 PC2 可以通过同网段桥接口 IP 管理防火墙。

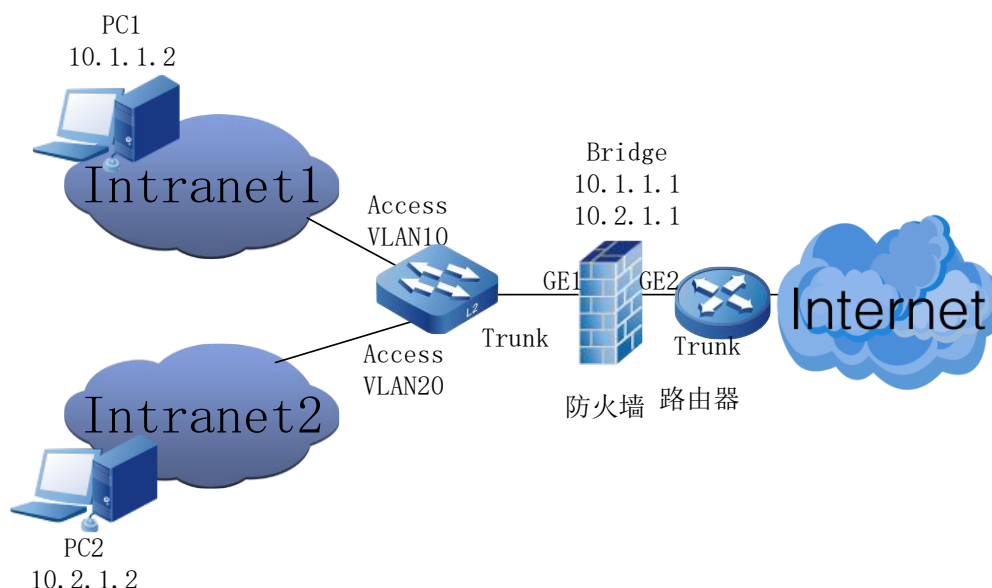


图 2-4 通过桥透明接入

2.4.1.2.3 虚拟线路桥接场景

虚拟线路桥只能绑定两个物理接口，且不能绑定桥接口。通过虚拟线路桥转发的报文只能从虚拟线路桥的一个物理接口进入，从另一个物理接口转发出去。即虚拟线路桥进行报文转发无需查看 MAC 表和路由表直接转发。

如图 2-5 所示，内网用户可以通过虚拟线路桥直接访问内网服务器。

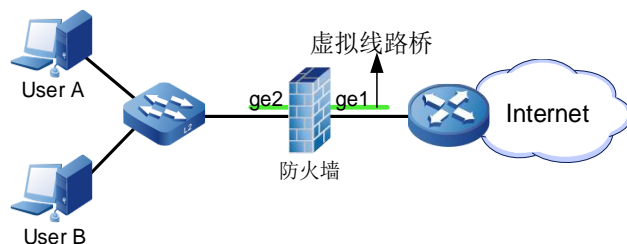


图 2-5 通过虚拟线路桥透明接入

当上下行设备都配置了聚合接口时，防火墙可以配置虚拟线路桥，通过桥透传报文，无需参与聚合协商。

2.4.1.3 旁路模式

当防火墙接口处于旁路模式时，防火墙将检测由交换机镜像而来的 IP 数据包。防火墙的作用更像是处于网络外的威胁检测器，防火墙不会对原有网络造成任何影响。

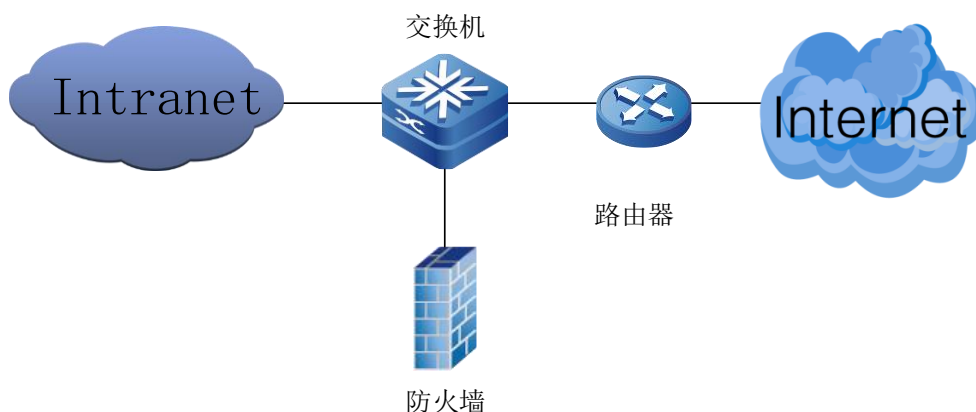


图 2-6 旁路模式

2.4.1.4 服务链模式

防火墙使用智能流量编排功能时，接口需要工作在服务链模式下。此时防火墙可以作为流量编排器，支持将其它安全设备作为 PNF 安全网元加入不同的串接或旁路服务链，根据引流策略将业务流量引导到不同服务链的安全网元处理。且加密流量可以在防火墙上进行一次 SSL 解密后根据流量策略引流到相应设备进行精细化处理。

2.4.2 确定双机热备模式

确认是否采用双机热备，并确认双机热备的部署模式。防火墙支持主备双机热备和双主双机热备。

2.4.2.1 主备模式

两台防火墙以主备备份方式工作。正常情况下，所有流量均由防火墙 A 转

发。当防火墙 A 出现故障时，所有流量切换到防火墙 B，保证业务不中断。

防火墙可以工作在二层，也可以工作在三层。上下行设备可以是二层设备，也可以是三层设备。当上下行都是三层路由设备时，上下行路由器之间运行 OSPF 协议，防火墙作为二层设备透传 OSPF 协议报文，不参与路由协议计算。

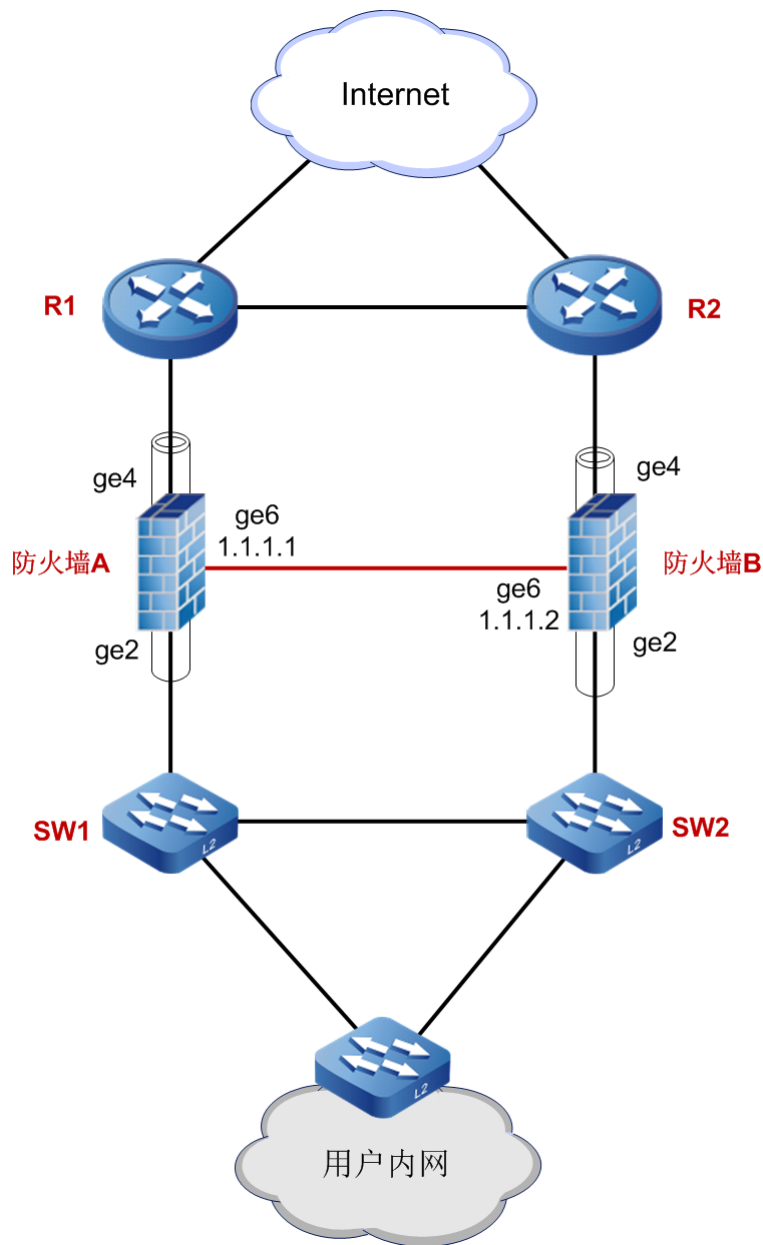


图 2-7 主备模式

2.4.2.2 主主模式

两台防火墙以主主模式工作。正常情况下：子网 1 的流量由防火墙 A 转发，子网 2 的流量由防火墙 B 转发。当其中一台防火墙出现故障时，另外一台防火墙转发全部业务，保证业务不中断。

防火墙可以工作在二层，也可以工作在三层。上下行设备可以是二层设备，也可以是三层设备。当上下行都是三层路由设备时，上下行路由器之间运行 OSPF 协议，防火墙作为二层设备透传 OSPF 协议报文，不参与路由协议计算。

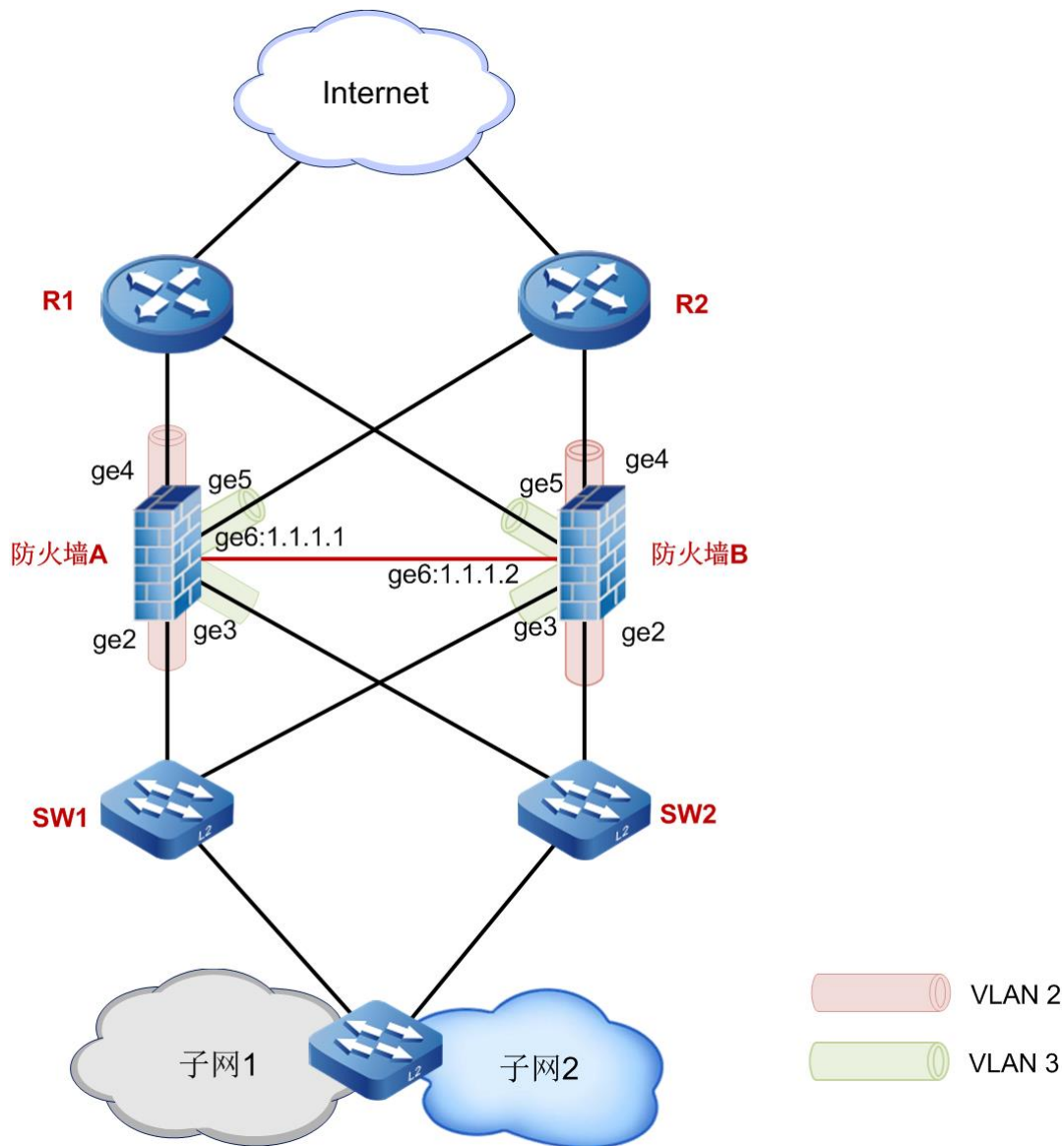


图 2-8 主主模式

3 购买产品许可证

感谢您购买防火墙系统，如果您购买了产品相应的模块或者特征库升级等服务，需要申请产品许可证导入防火墙之后才能正常使用。

产品许可证申请需要您与客户服务中心联系，热线电话 **95015**，在您与客服联系之前，需要您提前准备以下信息：

- 购买产品模块及特征库升级等服务的订单号，这在您的购买合同上可以查到。
- 代理商名称，如果您是从代理商处购买则需要。
- 您的单位名称、姓名、联系方式。
- 设备 SN 信息，这是非常重要的信息，您可以在设备的机身产品标签查到 SN 信息。

4 通过管理口管理防火墙

4.1 防火墙登录相关说明

4.1.1 防火墙管理口和默认 IP

网神 SecGate3600 防火墙系统采用管理数据与业务数据分离的结构，部分产品提供专门的 MGT 管理口，根据产品是否存在 MGT 接口，登录接口分为两种情况：

- 防火墙有专门的 MGT 管理口。
只能通过 MGT 管理口登录。
- 防火墙没有专门的 MGT 管理口。
只能通过防火墙第一个业务接口登录。防火墙第一个业务接口一般默认为 GE1 接口。

管理口或首个业务接口 IP 地址默认为 10.0.0.1，子网掩码为 255.255.255.0。

首次通过 Web 登录防火墙必须使用 HTTPS。

防火墙默认开启可信主机，可信主机的 IP 地址为 10.0.0.44（登录管理防火墙的电脑 IP 配置为 10.0.0.44），子网掩码为 255.255.255.0。

4.1.2 防火墙默认账号

SecGate3600 防火墙系统默认存在一个管理员账号：admin 缺省密码为：!1fw@2soc#3vpn



说明

首次登录设备，必须强制修改密码，管理员密码必须定期修改以保证管理员账号的安全。

4.2 准备工作

4.2.1 IP 规划

规划好防火墙接入网络的位置和 IP 地址等信息。

4.2.2 物理连接

4.2.2.1 路由模式

步骤1 使用一根网线，连接管理主机的网口和防火墙的 MGT 口。

步骤2 使用一根网线，将防火墙规划好的内网接口连接汇聚交换机的接口。

也可以配置完成后再连接汇聚交换机。

步骤3 使用一根网线，连接防火墙规划好的外网网口和出口交换机接口。

步骤4 （可选）双机热备时，同样方式连接另一台防火墙的内外网接口和交换机的接口。同时连接防火墙之间的心跳接口。

4.2.2.2 透明模式

步骤1 使用一根网线，连接管理主机的网口和防火墙的 MGT 口。

步骤2 使用一根网线，连接防火墙规划好的内网网口和汇聚交换机的接口。

步骤3 使用一根网线，连接防火墙规划好的外网网口和出口网关的接口。

步骤4 （可选）双机热备时，同样方式连接另一台防火墙的内外网接口和交换机的接口。同时连接防火墙之间的心跳接口。

4.2.2.3 旁路模式

步骤1 使用一根网线，连接管理主机的网口和防火墙的 MGT 口。

步骤2 使用一根网线，连接防火墙规划好的接口与交换机的镜像接口。

4.3 登录防火墙 web 页面

步骤1 将管理主机的 IP 地址配置为 10.0.0.44（防火墙默认可信主机的地址），子网掩码为 255.255.255.0，默认网关可以不填写或者配置为 10.0.0.1。



步骤2 打开浏览器，在地址栏中输入 <https://10.0.0.1>，回车。

步骤3 在防火墙登录页面输入防火墙用户名、密码、验证码后登录防火墙。

登录前请仔细阅读《用户许可协议》和《隐私协议》，必须同意这两个协议才可以登录。



步骤4 修改管理员密码。

为保证防火墙系统的安全性，首次登录防火墙，系统会要求用户修改密码。设置的密码必须符合复杂度要求。

4.4 使用部署向导快速配置

防火墙提供部署向导的功能，帮助用户快速配置防火墙基本功能。

选择“系统配置 > 部署向导”。

根据使用场景选择防火墙的工作模式。

- 防火墙作为二层设备使用，不改变原有网络结构，选择“透明模式”。
- 防火墙作为三层设备使用，部署于网络边界，选择“路由模式”。
- 防火墙旁路镜像部署，只做流量监测，选择“旁路镜像”。

4.4.1 透明模式

4.4.1.1 配置接口

步骤1 配置业务接口。

选择 **WAN** 接口和 **LAN** 接口。**WAN** 口指定防火墙连接外网的接口，**LAN** 指定防火墙连接内网的接口。

步骤2 （可选）配置静态路由。

根据需求指定目的地址/掩码和下一跳网关。

步骤3 （可选）配置管理接口。

不选择管理接口时，首次登录默认带 **MGT** 口的设备使用 **MGT** 口，不带 **MGT** 口的设备使用 **GE1** 口作为管理接口。

选中“配置管理口”复选框后配置管理口参数，包括选择管理接口、配置接口的 IP 地址/掩码、配置管理方式。



说明

部署向导中仅支持选择路由模式物理接口（即三层物理接口）和 **MGT** 口作为管理接口。**MGT** 口作为管理接口时，需要事先保证管理路由可达，否则配置向导无法成功配置。

接口支持 **HTTPS**、**SSH**、**Ping** 管理方式。

- **HTTPS** 表示允许通过该接口以 **HTTPS** 连接登录 Web 管理页面。
- **SSH** 表示允许通过该接口以 **SSH** 连接登录 CLI 界面。
- **Ping** 表示该接口会响应 ping 请求。

选中一个或多个方式后，用户可以通过该方式打开接口 IP 地址管理防火墙。

步骤4 （可选）配置 **DNS**。

DNS 用于解析用户访问的域名和防火墙升级使用的域名。

步骤5 配置完成后，单击“下一步”。

配置可信主机

可信主机功能用于设置可以登录防火墙的主机 IP 地址和可以使用的管理服务。

防火墙默认的可信主机 IP 地址为 **10.0.0.44**。首次登录防火墙时，用户必须将管理主机的 IP 地址配置为 **10.0.0.44**。

单击“添加可信主机”，添加防火墙信任的可信主机以及可信主机可以使用的服务。配置完成后，单击“下一步”。

配置安全策略

配置向导中仅支持配置全通安全策略，即源和目的都为 **any**，允许任何流量通过。默认开启全通策略。用户仅需配置策略的名称。配置完成后，单击“下一步”。

检查许可证

许可证用于对受控的功能进行授权。请检查需要的功能最大连接数是否够用，存在有效期的功能剩余天数是否充足，授权状态是否正常。已经到期或未授权的许可将影响功能的正常使用。

若无异常，请单击“下一步”，否则请联系客服更换许可证。

确认配置

完成以上配置后，请再次检查配置项是否正确。若配置无误，请单击“应用”，否则，请单击“上一步”，修改配置。

4.4.2 路由模式

配置接口

步骤1 指定业务接口。

选择 **WAN** 接口和 **LAN** 接口，并指定接口的静态 IP 地址和掩码。
WAN 口指定防火墙连接外网的接口，**LAN** 指定防火墙连接内网的接口。

IP 地址支持 IPv4 和 IPv6 地址。

步骤2 （可选）配置静态路由。

根据需求指定目的地址/掩码和下一跳网关。

步骤3 （可选）配置管理接口。

不选择管理接口时，首次登录默认带 **MGT** 口的设备使用 **MGT** 口，不带 **MGT** 口的设备使用 **GE1** 口作为管理接口。

选中“配置管理口”复选框后配置管理口参数，包括选择管理接口、配置接口的 IP 地址/掩码、配置管理方式。



部署向导中仅支持选择路由模式物理接口（即三层物理接口）和 MGT 口作为管理接口。

接口支持 HTTPS、SSH、Ping 管理方式。

- HTTPS 表示允许通过该接口以 HTTPS 连接登录 Web 管理页面。
- SSH 表示允许通过该接口以 SSH 连接登录 CLI 界面。
- Ping 表示该接口会响应 ping 请求。

选中一个或多个方式后，用户可以通过该方式打开接口 IP 地址管理防火墙。

步骤4 （可选）配置 DNS。

DNS 用于解析用户访问的域名和防火墙升级使用的域名。

步骤5 配置完成后，单击“下一步”。

配置可信主机

可信主机功能用于设置可以登录防火墙的主机 IP 地址和可以使用的管理服务。

防火墙默认的可信主机 IP 地址为 10.0.0.44。首次登录防火墙时，用户必须将管理主机的 IP 地址配置为 10.0.0.44。

单击“添加可信主机”，添加防火墙信任的可信主机以及可信主机可以使用的服务。配置完成后，单击“下一步”。

配置安全策略

配置向导中仅支持配置全通安全策略，即源和目的都为 any，允许任何流量通过。默认开启全通策略。用户仅需配置策略的名称。配置完成后，单击“下一步”。

检查许可证

许可证用于对受控的功能进行授权。请检查需要的功能最大连接数是否够用，存在有效期的功能剩余天数是否充足，授权状态是否正常。已经到期或未授权的许可将影响功能的正常使用。

若无异常，请单击“下一步”，否则请联系客服更换许可证。

确认配置

完成以上配置后，请再次检查配置项是否正确。若配置无误，请单击“应用”，否则，请单击“上一步”，修改配置。

4.4.3 旁路镜像

4.4.3.1 配置接口

步骤1 配置监听接口。

从可选接口列表中选择加入已选接口列表。

步骤2 （可选）配置静态路由。

根据需求指定目的地址/掩码和下一跳网关。

步骤3 （可选）配置管理接口。

不选择管理接口时，首次登录默认带 MGT 口的设备使用 MGT 口，不带 MGT 口的设备使用 GE1 口作为管理接口。

选中“配置管理口”复选框后配置管理口参数，选择管理接口、配置接口的 IP 地址/掩码、配置管理方式。



说明

部署向导中仅支持选择路由模式物理接口（即三层物理接口）和 MGT 口作为管理接口。

接口支持 HTTPS、SSH、Ping 和 SNMP 管理方式。

- HTTPS 表示允许通过该接口以 HTTPS 连接登录 Web 管理页面。
- SSH 表示允许通过该接口以 SSH 连接登录 CLI 界面。
- Ping 表示该接口会响应 ping 请求。

选中一个或多个方式后，用户可以通过该方式打开接口 IP 地址管理防火墙。出于安全性的考虑，推荐使用 HTTPS 和 SSH。

步骤4 （可选）配置 DNS。

DNS 用于解析用户访问的域名和防火墙升级使用的域名。

步骤5 配置完成后，单击“下一步”。

4.4.3.2 配置可信主机

可信主机功能用于设置可以登录防火墙的主机 IP 地址和可以使用的管理服务。

防火墙默认的可信主机 IP 地址为 10.0.0.44。首次登录防火墙时，用户必须将管理主机的 IP 地址配置为 10.0.0.44。

单击“添加可信主机”，添加防火墙信任的可信主机以及可信主机可以使用的服务。配置完成后，单击“下一步”。

配置安全策略

配置向导中仅支持配置全通安全策略，即源和目的都为 **any**，允许任何流量通过。默认开启全通策略。用户仅需配置策略的名称。配置完成后，单击“下一步”。

检查许可证

许可证用于对受控的功能进行授权。请检查需要的功能最大连接数是否够用，存在有效期的功能剩余天数是否充足，授权状态是否正常。已经到期或未授权的许可将影响功能的正常使用。

若无异常，请单击“下一步”，否则请联系客服更换许可证。

确认配置

完成以上配置后，请再次检查配置项是否正确。若配置无误，请单击“应用”，否则，请单击“上一步”，修改配置。

4.5 重点功能配置

重点功能配置请参见“6 重点功能配置”。

4.6 软件维护

软件维护的内容请参见“7 软件维护”。

5 通过智慧管理分析系统管理防火墙

5.1 在防火墙上配置集中管理

5.1.1 登录防火墙 web 页面

请参见 4.3 登录防火墙 web 页面。

5.1.2 配置集中管理

步骤1 选择【系统配置】>【集中管理】>【集中管理】。

步骤2 指定集中管理服务器地址和通信端口。

参数	说明
集中管理服务器地址	输入管理分析系统的 IP 地址。支持 IPv4 和 IPv6 地址。
端口	输入管理分析系统使用的端口，端口号必须为 3601。管理分析系统使用 HTTPS 协议 3601 端口与防火墙通信。 智慧管理分析系统通过 HTTPS 协议向防火墙进行配置下发。防火墙使用随机端口主动连接管理分析系统提供的端口。

步骤3 配置高级参数。

参数	说明
IPSec VPN 隧道监控信息上报	选中该复选框后开启 IPSec VPN 隧道监控信息上报。防火墙将定期向集中管理系统上传 IPSec VPN 隧道监控信息。IPSec VPN 隧道监控信息包括 IPSec 自动隧道和 IPSec 手工隧道监控页面记录的所有信息。
上报周期	上报周期默认为 60 秒。上报周期可以根据实际情况进行修改，其取值范围为 3~86400 秒。
上报集中管理侧端口	配置集中管理系统接收 IPSec VPN 隧道监控信息的端口。端口默认为 3605，取值范围为 1000~65535。
本地接口	选择防火墙与管理分析平台通信的接口。
本地地址	选择防火墙与管理分析平台通信的 IP 地址。

步骤4 选中【启用】，开启集中管理功能。

步骤5 配置完成后，单击【应用】。

- 连接状态为“在线”说明防火墙跟管理分析系统连接正常。
- 连接状态为“离线”说明防火墙与管理分析系统连接不正常。

5.2 使用智慧管理分析系统配置防火墙

5.2.1 登录智慧管理分析系统

步骤1 打开浏览器，在地址栏中输入业务接口的 IP 地址（缺省为 <https://10.0.0.1>），打开 vSMAC 的 Web 登录界面。登录界面，如图 5-1 所示。



图 5-1 登录界面

步骤2 输入缺省的用户名、密码和验证码，单击“登录”，进入客户端界面。缺省的用户名是 `admin`，密码为 `!1fw@2soc#3vpn`。

5.2.2 配置防火墙

配置的重点功能可参考“6 重点功能配置”，但使用防火墙配置与集中配置方式配置有些差异。具体配置请参见智慧管理分析系统的用户手册和配置指南。

6 重点功能配置

6.1 HA 相关配置

6.1.1 主备模式

6.1.1.1 配置主防火墙

步骤1 选择【网络配置】>【接口联动】，单击【添加】，配置接口联动组。将防火墙上下行接口进行联动，保证当联动组内一侧链路失效时，另一侧可以同步失效，用来触发链路切换。

接口	接口联动	操作
ge1	<input type="checkbox"/>	<input type="checkbox"/>
ge2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ge3	<input type="checkbox"/>	<input type="checkbox"/>
ge4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ge5	<input type="checkbox"/>	<input type="checkbox"/>

共 5 条

(最多绑定8个接口)

步骤2 选择【系统配置】>【高可用性】，选择【高可用性】页签页签，配置 HA。

- 选中【启用 HA】、【配置同步】和【动态信息同步】。
- 配置 HA 通信接口、HA 通信端口、本地接口 IP 地址和对端接口 IP 地址。支持 HA 口的设备还可以指定 HA 辅助通信接口、HA 辅助通信端口、本地辅助通信接口 IP 和对端辅助通信接口 IP。
- 配置 HA 组抢占模式和优先级。

HA设置 | 接口监控 | 链路探测 | BFD监控 | 网元监控 | 配置对比

启用HA ☒

配置同步 ☒ 手动同步

动态信息同步 ☒

负载均衡模式 ☐

HA通信接口(心跳口) ge6

HA通信端口 6260 * (范围: 1-6260和6600-65535)

本地接口IP 1.1.1.2

对端接口IP 1.1.1.1

HA辅助通信接口

HA组

+ 添加 - 删除

HA组ID	抢占模式	抢占延时(秒)	优先级	当前优先级	通告间隔(秒)	管理状态	转发状态	同步配置	同步动态信息	操作
0	非抢占	0	100	100	1	INIT	INIT	INIT	INIT	✎ ⌂

(HA组优先级数字越大, 优先级越高)

应用 取消

步骤3 选择【系统配置】>【高可用性】，选择【接口监控】页签，单击【添加】，分别配置 GE2 和 GE4 的接口监控功能。

添加HA接口监控

HA组ID 0 * (被接口引用生效)

接口 ge2 *

权重 255 * (1-255, 数字越大, 权重等级越高)

确定 取消

添加HA接口监控

HA组ID 0 * (被接口引用生效)

接口 ge4 *

权重 255 * (1-255, 数字越大, 权重等级越高)

确定 取消

确定主墙的网络连通性。使用常用测试 ping, telnet, http, ftp 等方法，测试网络是否连通。

6.1.1.2 配置备防火墙

步骤1 进入 Web 配置界面，选择【系统配置】>【高可用性】，选择【高可用性】页签，配置 HA。

- 选中【启用 HA】、【配置同步】和【动态信息同步】。
- 配置心跳接口、心跳端口、本地接口 IP 地址和对端接口 IP 地址。支持 HA 口的设备还可以指定 HA 辅助通信接口、HA 辅助通信端口、本地辅助通信接口 IP 和对端辅助通信接口 IP。

➤ 配置 HA 组抢占模式和优先级。

步骤2 HA 启动后，等待主墙给同步过来配置即可。同步配置成功之后，备墙状态切换为 BACKUP。

查看防火墙 B 的配置，应该与防火墙 A 一致。

6.1.2 主主模式

6.1.2.1 配置防火墙 A

步骤1 进入 Web 配置界面，选择【系统配置】>【高可用性】，选择【HA 设置】页签，在【HA 组】中单击【添加】，添加 HA 组 1。

双机热备组

HA组ID	1	(被接口引用生效)
优先级	50	* (1-255)
通告间隔(秒)	1	* (1-60)
抢占模式	<input type="radio"/> 非抢占 <input checked="" type="radio"/> 抢占	
抢占延时(秒)	0	* (0-60)

确定 取消

步骤2 配置内外网接口时，分别将一对接口加入 HA0，一对接口加入 HA1。

编辑物理接口

虚MAC地址: 00:00:00:10:10:00

安全域: any

工作模式: ☒ 路由模式 ☐ 交换模式 ☐ 旁路模式 ☐ 服务链模式

HA组: 0

Netflow配置: ☐ 启用

外网接口: ☐ 启用

本地地址列表: IPv4 IPv6

☒ 静态地址 ☐ DHCP

+ 添加 - 删除

本地地址	子网掩码	类型	操作
<input type="checkbox"/> 172.24.230.75	255.255.255.0	float	<input checked="" type="checkbox"/>

确定 取消

步骤3 选择【系统配置】>【高可用性】，选择【HA 设置】页签，配置 HA。

- 选中【启用 HA】、【配置同步】和【动态信息同步】可选框。
- 选中【非对称模式】可选框。
- 配置心跳接口、心跳端口、本地接口 IP 地址和对端接口 IP 地址。支持 HA 口的设备还可以指定 HA 辅助通信接口、HA 辅助通信端口、本地辅助通信接口 IP 和对端辅助通信接口 IP。
- 配置 HA 组抢占模式和优先级。

HA组ID	抢占模式	抢占延时(秒)	优先级	当前优先级	通告间隔(秒)	管理状态	转发状态	同步配置	同步动态信息	操作
0	非抢占	0	100	100	1	INIT	INIT	INIT	INIT	✕ ○
1	非抢占	0	120	120	1	-	INIT	INIT	INIT	✕ ○

(HA组优先级数字越大,优先级越高)

步骤4 选择【系统配置】>【高可用性】，选择【接口监控】页签，单击【添加】，分别配置 2 对内网外接口的接口监控功能。

HA组ID	接口	权重	虚拟系统	状态	操作
0	ge4	255	root-vsys	INIT	✕
0	ge2	255	root-vsys	INIT	✕
1	ge3	255	root-vsys	INIT	✕
1	ge5	255	root-vsys	INIT	✕

步骤5 确定防火墙 A 的网络连通性。使用常用测试 ping, telnet, http, ftp 等方法，测试网络是否连通。

6.1.2.2 配置防火墙 B

步骤1 进入 Web 配置界面，选择【系统配置】>【高可用性】，选择【HA 设置】页签，配置 HA。

- 勾选【启用 HA】、【配置同步】和【动态信息同步】可选框。
- 勾选【负载分担模式】可选框。

- 配置心跳接口、心跳端口、本地接口 IP 地址和对端接口 IP 地址。支持 HA 口的设备还可以指定 HA 辅助通信接口、HA 辅助通信端口、本地辅助通信接口 IP 和对端辅助通信接口 IP。
- 配置 HA 组抢占模式和优先级。

步骤2 HA 启动后，等待主墙给同步过来配置即可。同步配置成功之后，备墙状态切换为 **BACKUP**。

步骤3 测试防火墙 B 的网络连通性。使用常用测试 ping, telnet, http, ftp 等方法测试网络是否连通。

查看防火墙 B 的配置，应该与防火墙 A 一致。

6.2 配置安全策略与高级功能

6.2.1 配置高级功能

防火墙支持漏洞防护、间谍软件防护、Web 攻击防护、防病毒、文件过滤、内容过滤、邮件过滤、行为管控、联动终端管控等高级安全业务功能。请根据使用场景选择配置。

入侵防护是防火墙的核心功能之一，访问外网的安全策略建议引用漏洞防护、防间谍软件、web 攻击防护等高级功能配置文件，确保 Web 服务、数据库服务以及其他应用的安全。

反病毒配置文件可以配置对 SMTP、POP3、IMAP、FTP、SMB、HTTP、IPTUX 协议进行病毒防护。

需要对文件进行保护时建议开启文件过滤、内容过滤、邮件过滤。

需要对用户行为或物联网协议行为进行管控时，建议开启行为管控。

选择【对象配置】>【安全配置文件】，找到要配置的功能，添加相应高级功能配置文件，并进行参数配置后，单击【确定】。

当同时使用多个高级安全功能时，可以创建安全配置文件组，将多个安全配置文件绑定同一个安全配置文件组。

6.2.2 配置安全策略

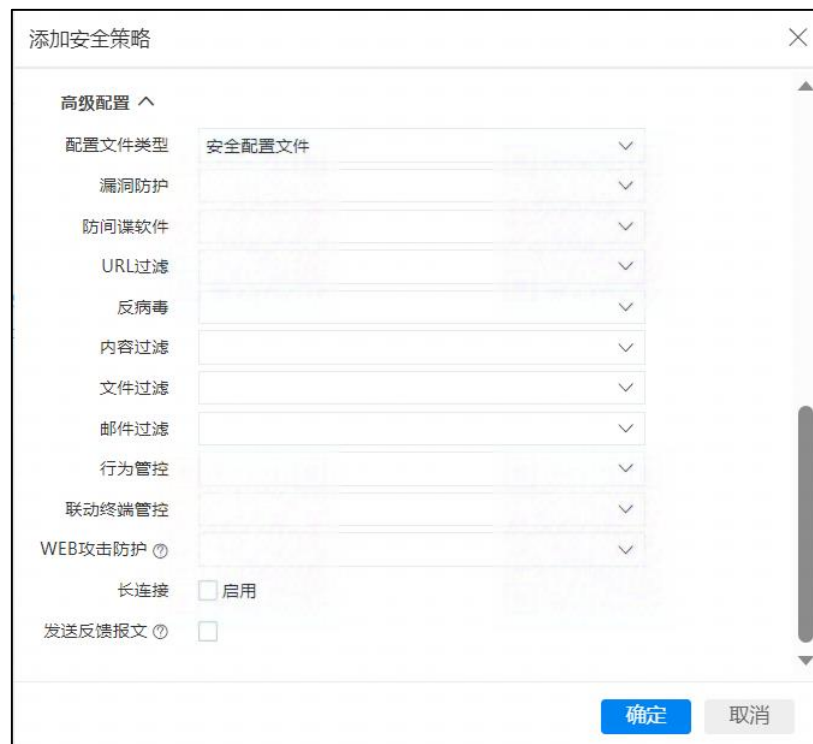
防火墙通过安全策略对流量进行控制。在安全策略中可以通过引用安全配置文件或安全配置文件组对流量执行安全配置文件定义的内容安全检测。

步骤1 选择“策略配置 > 安全策略”，单击“添加”。

步骤2 配置安全策略的基本参数。

步骤3 高级配置下引用配置好的安全配置文件或安全配置文件组。

引用配置好的漏洞防护、防间谍软件、防病毒、文件过滤、内容过滤、邮件过滤、URL 过滤、网络行为管理、Web 攻击防护等配置文件。



步骤4 单击“确定”。

6.3 配置攻击防护

选择【策略配置】>【安全防护】>【攻击防护】，单击【添加】，配置添加一个攻击防护策略。防火墙的攻击防护是基于安全域的攻击防护。管理员可以为每一个安全域配置单独的攻击防护策略。

加入攻击防护白名单的地址，流量不进行攻击防护检测，直接放行。

攻击防护策略中支持配置传输层和应用层 Flood、恶意扫描、欺骗防护、异常包攻击、ICMP 管控、ICMPv6 管控、IPv6 扩展头防护等的攻击防护。根据需求选择要配置的项，配置完成后，单击【确定】。

防火墙支持对 SYN Flood、ICMP Flood、UDP Flood、IP Flood、Frag Flood、Tracert、IP 扫描、端口扫描、IP 欺骗、异常包攻击、HTTP Flood、DNS Request Flood、DNS Reply Flood、HTTP Flood、NTP Request Flood、NTP Reply Flood、SIP Flood 等进行攻击防护。用户通过启用并配置攻击防护模块，有效的过滤并采取相应的措施阻止非正常报文或攻击报文流入用户内网。

6.4 配置流量编排

6.4.1 接口工作模式设置

步骤1 选择【网络配置】>【接口】。

步骤2 编辑或添加接口，配置接口模式为“服务链模式”。

物理接口、物理子接口、聚合接口、聚合子接口、虚拟系统接口、隧道接口都支持配置为“服务链模式”。

步骤3 单击“确定”。

6.4.2 添加网元组

步骤1 选择【策略配置】>【流量编排】>【网元管理】。

步骤2 在【网元管理】页面，单击【添加】。

步骤3 配置网元组名称和工作模式。

网元组名称支持大小写字母、数字、汉字和@。网元组名称必须唯一。

工作模式支持“旁路”和“串联”。旁路部署的网元工作模式选择“旁路”，直接接入网络中的网元工作模式选择“串联”。

步骤4 选择网元组类型。

网元组类型支持“IPS”、“IDS”、“WAF”、“NGFW”、“探针”、“数据库审计”、“上网行为管理”、“日志审计”、“数据库防火墙”、“蜜罐”和“其他”。

由老版本升级上来的网元类型为“其他”，新添加的网元组类型默认为“IPS”。

步骤5 选择组负载均衡算法。

负载均衡算法支持“源地址哈希”、“加权源地址哈希”、“源目的地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”，默认设置为“源地址哈希”。加入该网元组的网元之间采用选定的算法进行负载均衡。

步骤6 在【网元组】区域框中，单击【添加】，添加网元。

步骤7 配置网元参数。

➤ 串联网元组添加网元



➤ 旁路网元组添加网元



自定义网元名称，选择网元接口。串联网元需要选择内网接口和外网接口；旁路网元选择镜像接口，旁路网元的接口可以选择绑定 GRE 隧道的 tunnel 口。

配置权重，权重用于配置负载均衡算法中的权重值。

选择【链路健康检查】对象对网元监控进行检测。若需要添加新的【链路健康检查】对象，在【链路健康检查】下拉菜单中单击【添加】，配置链路健康检查。

串联网元可以开启【回环检测】，以便快速发现回环问题快速解决。

步骤8 配置完成后，单击【确定】，返回【添加网元组】页面。

步骤9 单击【确定】。

步骤10 添加后的网元组在【网元管理】页面显示，可以对网元进行编辑、删除、网元组流量 bypass 等操作。

6.4.3 添加服务链

步骤1 选择【策略配置】>【流量编排】>【服务链管理】。

步骤2 在【服务链管理】页面，单击【添加】。

步骤3 配置服务链名称。

服务链的名称用于唯一标识一个服务链，取值范围为 1~63 个字符。字符可以是数字、大小写字母、汉字和@。

步骤4 配置串接链。

在【串接链】区域框中，单击【添加】，选择加入串接链的网元组，并设置网元组在串接链中的位置。串接链中只能选择工作模式为“串联”的网元。设置完成后，单击【确定】。多个网元可以连接成一个串接链。

方向支持设置为“置顶”、“之前”、“之后”和“末尾”，当方向为“之前”和“之后”时，需要选择目的位置，即选择目的网元。



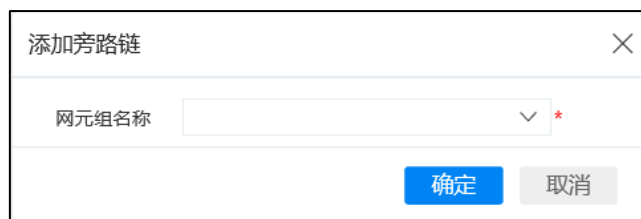
添加串接链对话框，包含以下字段：

- 网元组名称：下拉菜单，带红色星号。
- 方向：下拉菜单，当前显示“末尾”，带红色星号。
- 目的位置：下拉菜单，带红色星号。
- 底部有“确定”和“取消”按钮。

步骤5 配置旁路链。

在【旁路链】区域框中，单击【添加】，选择加入旁路链的网元组。

旁路链中的所有网元逻辑上都是直接旁挂在防火墙上，由防火墙直接引流到旁路链中的网元。



添加旁路链对话框，包含以下字段：

- 网元组名称：下拉菜单，带红色星号。
- 底部有“确定”和“取消”按钮。

步骤6 配置完成后，单击【确定】。

6.4.4 添加引流策略

步骤1 选择【策略配置】>【流量编排】。

步骤2 单击【引流策略】。

步骤3 单击【添加】。

步骤4 配置引流策略参数。

参数	说明
名称	配置引流策略的名称。
描述	为引流策略添加说明。
启用	引流策略必须启用后才能生效。
源安全域	选择入接口所属的安全域。
目的安全域	选择出接口所属的安全域。
源用户	选择发送流量的认证服务器和用户或用户组。多个源用户之间通过英文逗号(,)分隔。
源地址	<p>选择流量的源地址。源地址支持地址对象和地址组。请根据场景配置宽松或严格的源地址。</p> <p>单击【源地址】的文本框，选择要添加的地址。默认显示所有地址和地址组。可以在下拉框中选择只显示地址、地址组、预定义区域或自定义区域。</p> <p>若引用的地址对象或地址组中的地址对象下包含域名，其中的域名会下发生成域名组，支持对流量进行基于域名组的匹配。</p> <p>单击【添加】按钮，可以添加新的地址对象、地址组和地区。对选中的地址或地区，可以通过【删除】按钮进行删除。</p>
目的地址	<p>选择流量的目的地址。</p> <p>选择的方法与选择源地址相同。</p>
服务	<p>服务用于设置流量的服务类型。默认显示所有服务。在文本框中输入关键字可以进行搜索。选中服务前的复选框后，单击【引流策略】页面的任意位置，返回引流策略页面，服务被添加到对应文本框中。</p> <p>通过指定服务可以对流量进行针对服务的引流限制。</p>

参数	说明
应用	<p>用于设置流量的应用类型。默认显示所有应用。在下拉框中根据类型筛选应用。选中应用前的复选框后，单击【引流策略】页面的任意位置，返回引流策略页面，应用被添加到对应文本框中。</p> <p>通过指定应用可以对流量进行针对应用的引流限制。</p>
VLAN	当防火墙工作在透明模式时，可以对不同 VLAN 的流量进行限制。
服务链	在下拉菜单中选择配置好的服务链。流量将按照服务链的逻辑关系进行引流。
流量方向	<p>指定流量方向，三种参数说明如下：</p> <ul style="list-style-type: none"> ● 默认 <p>默认时，引流方向由入接口、出接口的内外口标记，是否开启了 snat 和 dnat 决定。</p> <ul style="list-style-type: none"> ■ 1、接口标记了【外网接口】，则该接口为外网接口，否则接口为“内网接口”。流量方向根据接口是出接口还是入接口，以及接口是内网口还是外网口来确定。比如接口是出接口，接口为外网口，则有内网到外网；接口是出接口，接口为内网口，则有外网到内网。 ■ 2、配置了 snat，引流方向由内网到外网。 ■ 3、配置了 dnat，引流方向由外网到内网。 ■ 4、接口没有标记内外网，接口内外网由接口网卡的 index 决定，index 小的为内网口，index 大的为外网口。 ● 内网到外网 ● 外网到内网 <p>流量方向的优先级为明确指定“内网到外网”、“外网到内网”优先级高于“默认”；“默认”时，接口标记了内外网 > snat > dnat > 通过接口网卡 index 决定。</p>

步骤5 配置完成后，单击【确定】。

6.5 配置 SSL 解密

防火墙支持 SSL 代理解密与入站检查解密，通常采用 SSL 代理解密。防火墙作为 SSL 代理分别与客户端和服务端建立 SSL 连接。防火墙将客户端发送的 SSL 加密流量进行解密后，对流量进行内容安全检测。检测完成后，防火墙会对流量再次进行加密并发送到服务器端。

步骤1 选择【策略配置】>【SSL 解密策略】。

步骤2 单击【添加】。

步骤3 配置 SSL 解密策略的参数。

参数	说明
名称	配置 SSL 解密策略的名称。字符串形式，取值为 1~63 个字符。
启用	选中【启用】后，开启该条 SSL 解密策略。
源安全域	指定 SSL 解密策略的源安全域。
目的安全域	指定 SSL 解密策略的目的安全域。
源地址	<p>选择流量的源地址。源地址支持地址对象和地址组。请根据场景配置宽松或严格的源地址。</p> <p>单击【源地址】的文本框，选择要添加的地址。默认显示全部地址和地址组。可以在下拉框中选择只显示地址、地址组。</p> <p>若引用的地址对象或地址组中的地址对象下包含域名，其中的域名会下发生成域名组，支持对流量进行基于域名组的匹配。</p> <p>单击【添加】按钮，可以添加新的地址对象、地址组。对选中的地址，可以通过【删除】按钮进行删除。</p>
目的地址	<p>选择流量的目的地址。</p> <p>选择的方法与选择源地址相同。</p>
SSL 协议的服务	配置 SSL 协议的服务。默认下拉列表支持“HTTPS”、“SMTPS”、“PoP3S”、“IMAPS”、“POP3”、“IMAP”、“SMTP”。
解密日志	选中【记录日志】前的复选框，开启记录解密日志功能。默认情况下未开启。
解密证书自学习	选中【解密证书自学习】复选框，开启解密证书自学习功能。开启解密证书自学习时，不需要用户导入解密证书，系统会自动获取解密证书。
动作	解密策略的处理动作，分为解密、不解密两种。
解密类型	解密类型选择“SSL 代理”。

参数	说明
SSL 服务器证书	选择 SSL 服务器证书名称。SSL 服务器证书配置文件需要在“对象 > 解密配置文件 > SSL 服务器证书”下配置。
检查解密对象	选择 SSL 检查解密对象。 当 SSL 解密策略的解密类型为“SSL 代理”时，可以引用检查解密对象配置。
证书自动签发	仅解密类型为“SSL 代理”且引用了 SSL 服务器证书时才可以配置。 选中【证书自动签发】复选框，开启证书自动签发功能。 当引用的 SSL 服务器证书与真实服务器证书不匹配时，自动签发服务器证书。
镜像接口	防火墙支持将解密后的明文流量镜像到其他设备进行分析统计。此时需要开启镜像功能，并指定镜像接口。
镜像目的接口	在下拉菜单中选择镜像目的接口。

步骤4 配置完成后，单击【确定】。

配置完成后的 SSL 解密策略在 SSL 解密策略列表中显示。可以查看策略的名称、源安全域、目的安全域、源地址、目的地址、服务、是否启用、动作等。

7 软件维护

7.1 导入许可证

防火墙必须导入有效的许可证后，需要许可证授权的功能才可以正常使用。

步骤1 选择“系统配置 > 许可证”。

步骤2 单击“导入”。

步骤3 单击“浏览”，选择许可证文件。

步骤4 导入许可证前可以单击“证书详情”下拉箭头，查询 License 内容。

检查 license 中的功能支持最大数、有效期、授权类型是否正确。

步骤5 单击“确定”。

导入成功，若提示是否重启设备。单击“确定”，重启设备，License 内容生效。若单击“取消”，则等下次重启设备后，License 内容生效。

步骤6 查看 License 列表中的参数是否已经更新。

7.2 系统和库升级

7.2.1 系统升级和打补丁

步骤1 选择“系统配置 > 升级管理 > 系统升级”。

步骤2 选择升级类型为“升级系统”或“升级包”。

步骤3 选择上传系统文件的配置类型。

配置类型可以选择“本地”、“FTP 服务器”和“TFTP 服务器”。本地方式要求将系统文件保存在管理防火墙的管理主机上。

FTP 服务器或 TFTP 服务器方式需要一台开启 FTP 服务器或 TFTP 服务器的客户端，并且将系统文件保存在 FTP 服务器或 TFTP 服务器上。

步骤4 设置上传系统文件的参数。

支持本地方式、FTP 服务器方式和 TFTP 服务器方式。本地方式请先将安装包保存在本地。

步骤5 配置完成后，单击“确定”。

步骤6 （可选）当系统中已经存在两个版本，会弹出提示。选择要删除的

文件，单击“确定”。

升级过程，请耐心等待。

步骤7 升级完成后，是否保存配置并重启设备。单击“确认”，重启设备。单击“取消”，则下次重启后，升级为新版本。



说明

通过“升级系统”或“hotfix”类型的升级包进行升级后不需要重启即生效。通过“patch”类型的升级包升级后必须重启系统后才能生效。

7.2.2 特征库升级

当特征库当前版本跟最新版本的版本号不一致时，可以将特征库升级到最新版本。只有处于升级服务有效期内的特征库才能升级。

步骤1 选择“系统配置 > 升级管理 > 特征库升级”。

步骤2 在“库升级设置”区域框中，设置库升级参数。

服务器支持才用公网服务器和私网服务器。

- 公网服务器

升级服务器默认采用 `ngfwup.sg.qianxin.com`。防火墙必须能够正常解析升级域名，才能够升级成功。

若防火墙无法连接默认的公网服务器，可以指定代理服务器。

- 私网服务器

可获取的最新的特征库放在私网服务器上进行特征库升级。支持 FTP 或 TFTP 服务器。

步骤3 配置完成后，单击“确定”。

步骤4 选中要自动升级的特征库，单击“启用自动升级”。

特征库将在设定的升级时间自动升级。若用户需要立刻升级，可以单击“立即升级”。

当防火墙无法通过升级服务器进行升级时，可以选择手动升级。手动升级需要将要升级到的特征库保存在本地。

步骤5 查看升级后的当前版本是否正确。

若当前版本为最新的特征库版本或指定的特征库版本，则升级成功。

7.2.3 威胁情报库升级

当防火墙上购买了威胁情报许可后，防火墙上支持本地检测。为了保证威胁情报本地检测结果，用户需要及时更新设备上的威胁情报库。

7.2.3.1 本地威胁情报库升级

步骤1 选择“系统配置 > 协同防护 > 云联防”。

The screenshot shows the '奇安信云情报平台' (Qianxin Cloud Intelligence Platform) settings page. Under '本地情报检测设置' (Local Threat Intelligence Detection Settings), the '开启' (Enable) checkbox is checked. Under '本地情报升级设置' (Local Threat Intelligence Upgrade Settings), the '当前情报库版本编号' (Current Threat Intelligence Library Version Number) and '最新情报库版本编号' (Latest Threat Intelligence Library Version Number) are both 2106111055. The '自动升级' (Automatic Upgrade) radio button is selected, with a dropdown menu set to '6小时' (6 hours). There are also '手动升级' (Manual Upgrade) and '立即升级' (Upgrade Immediately) buttons. At the bottom, there are '应用' (Apply) and '取消' (Cancel) buttons.

防火墙通过默认的升级服务器（ngfwup.sg.qianxin.com）进行升级。防火墙必须能够正常解析升级域名，才能够升级成功。

若防火墙无法连接默认的公网服务器，可以指定代理服务器。

威胁情况库支持自动升级、手动导入和立即升级。默认选择“自动升级”。

- 自动升级

自动升级按照配置的升级周期定期检测当前情报库版本编号和最新情报库版本编号是否一致。当最新情报库版本编号大于当前情报库版本编号时，自动进行升级。情报库默认 6 小时自动更新一次，用户可以修改为其他时间段。

- 立即升级

防火墙通过默认的升级服务器进行升级。用户不需要按升级周期升级，只需单击“立即升级”。确认要立即升级后，威胁情报库升至最新版本。

- 手动导入

单击“手动导入”，选择要导入的威胁情报库文件，单击“确定”。

7.3 双机场景下配置同步

7.3.1 执行配置对比操作

防火墙提供双机环境下两台防火墙设备的配置对比，并标识出差异性，帮助快速对比主备防火墙的配置差异。

步骤1 选择【系统配置】>【高可用性】。

步骤2 选择【配置对比】。

步骤3 选择虚拟系统。

默认取值为“root-vsys”，即根防火墙系统。配置了虚拟系统的情况下如需要对虚拟系统下的配置进行对比，需要选择对应的虚拟系统。

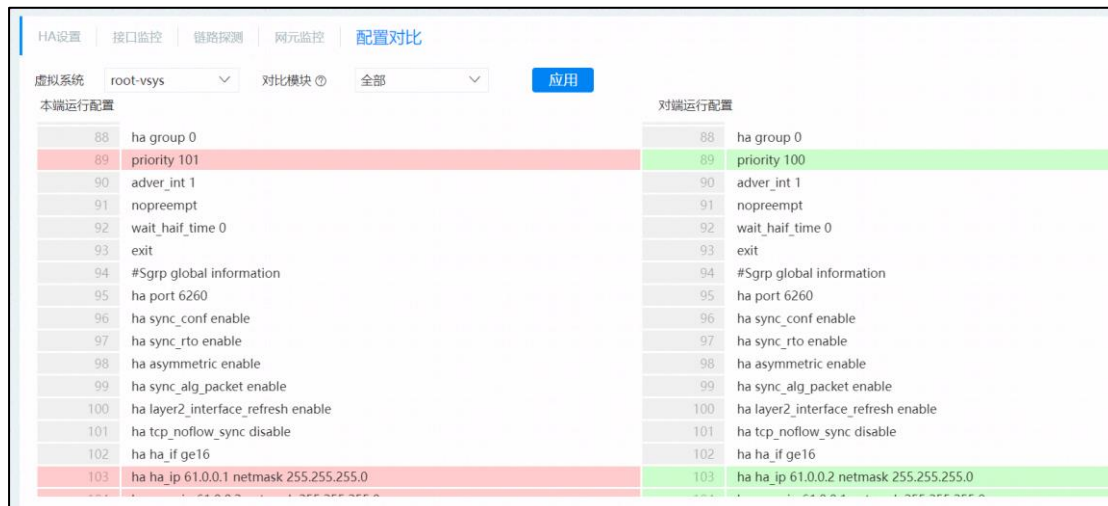
步骤4 选择对比模块。

防火墙支持对“全部功能”或“关键配置”进行对比。默认选择为“全部”，“全部”包括防火墙当前运行的所有配置。“关键配置”包括“安全策略”、“NAT 策略”、“策略路由”和“静态路由”的配置。

步骤5 单击【应用】，执行配置对比操作。

配置对比将执行几秒，请耐心等待。执行结果在【配置对比】页面显示，左侧为“本端运行配置”，右侧为“对端运行配置”。存在差异的配置通过红色和绿色进行标识，一目了然。

当配置文件过大时无法在防火墙本地显示，会弹出提示框，单击【导出】后，可以将配置对比文件导出到本地查看。




7.3.1 手动配置同步

主备防火墙配置存在差异时，可以在【HA 设置】页面单击【手动配置同步】进行配置同步。


主墙和备墙上都可以执行配置同步，但方向都是主墙的配置同步到备墙。

7.4 常用操作

7.4.1 保存当前配置

单击页面右上角的保存图标，保存系统当前配置。没有保存的配置，设备重启后会被丢失。

7.4.2 查看告警详情

当系统告警图标呈现红黄色交替闪现时，说明防火墙当前系统有告警信息。单击该图标，弹出“告警详情”页面。

7.4.3 查看 License 状态提示信息

当 License 存在过期等异常信息时，用户登录防火墙后，会在告警图标和“应急响应”提示框的下方弹出一个提示框进行提示。

单击“提示信息”，跳转到“许可证”页面。

7.4.4 切换虚拟系统

单击页面右上角的下拉框，在下拉列表中选择要管理的虚拟系统。对该虚拟系统的功能进行管理配置。

7.4.5 账号相关操作

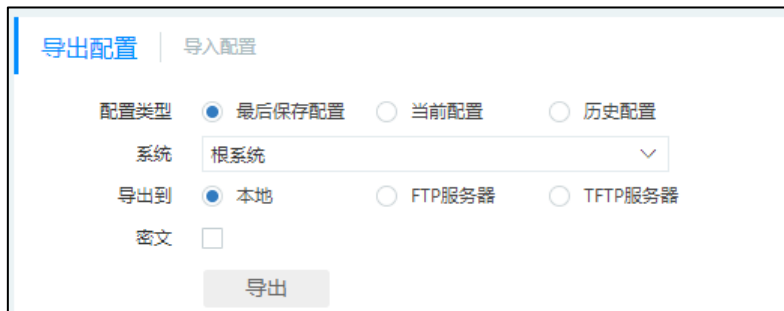
单击当前管理员下拉箭头，在下拉菜单中选择要执行的操作。

- 单击“关于”，查看防火墙版本号和序列号。
- 单击“帮助”，查看防火墙联机帮助。
- 单击“修改密码”，修改管理员密码。建议定期修改密码，保证密码安全。
- 单击“恢复出厂配置”，防火墙配置将恢复到出厂设置。请慎重执行该操作。
- 单击“重启”，重新启动防火墙。
- 单击“保存并重启”，保存配置并重新启动防火墙。该功能等同于保存和重启。
- 单击“退出”，退出当前登录账号。

7.4.6 导入导出配置文件

选择“系统配置 > 配置文件”可以执行导入或导出配置的操作。

图 7-1 导入导出配置



选择“系统配置 > 配置文件”可以执行导入配置的操作，配置导入之后需要重启设备。

图 7-2 导入配置

导出配置 | 导入配置 | 自动保存配置

配置类型 ☒ 本地 ☐ FTP服务器 ☐ TFTP服务器

名称 浏览...

密文 ☐

历史配置列表

☐ 删除

<input type="checkbox"/> 历史配置	配置类型	最后一次修改配置	操作
<input type="checkbox"/> 2024-09-10 17:03:38	自动保存	20240910_095509	<input checked="" type="radio"/>
<input type="checkbox"/> 2024-09-04 17:03:18	自动保存	20240904_103219	<input type="radio"/>
<input type="checkbox"/> 2024-09-02 16:37:51	手动保存	20240902_124309	<input type="radio"/>
<input type="checkbox"/> 2024-09-02 12:43:14	手动保存	20240902_124309	<input type="radio"/>
<input type="checkbox"/> 2024-08-28 19:39:28	自动保存	20240827_193918	<input type="radio"/>
<input type="checkbox"/> 2024-08-27 16:54:23	手动保存	20240827_141002	<input type="radio"/>
<input type="checkbox"/> 2024-08-24 10:16:41	自动保存	20240823_171315	<input type="radio"/>
<input type="checkbox"/> 2024-08-21 10:16:40	自动保存	20240820_173631	<input type="radio"/>
<input type="checkbox"/> 2024-08-17 10:16:40	自动保存	20240816_170041	<input type="radio"/>
<input type="checkbox"/> 2024-08-16 16:56:05	手动保存	20240816_165600	<input type="radio"/>
<input type="checkbox"/> 2024-08-15 10:16:40	自动保存	20240814_101631	<input type="radio"/>

共 20 条

导入