声明

服务修订：

- 本公司保留不预先通知客户而修改本文档所含内容的权利。

有限责任：

- 本公司仅就产品信息预先说明的范围承担责任，除此以外，无论明示或默示，不作其它任何担保，包括（但不限于）本手册中推荐使用产品的适用性和安全性、产品的适销性和适合某特定用途的担保。
- 本公司对于您的使用或不能使用本产品而发生的任何损害不负任何赔偿责任，包括（但不限于）直接的、间接的、附加的个人损害或商业损失或任何其它损失。

网御神州科技（北京）有限公司

目 录

一、概述

SecGate 3600-G10 防火墙缺省支持两种管理方式：

（1） CONSOLE 口命令行方式

（2） 通过专用管理口（MNG）或者普通网络接口进行的 WEB（https）管理

CONSOLE 口命令行方式适用于对防火墙操作命令比较熟悉的用户。WEB 方式直观方便，为保证安全，连接之前需要对管理员身份进行认证。要快速配置使用防火墙，推荐采用 CONSOLE 口命令行方式；日常管理监控防火墙时，WEB 方式则是更方便的选择。

安装防火墙之前，请您阅读本指南的“二、三”两节。如果希望使用 CONSOLE 口命令行方式管理防火墙，请您仔细阅读本指南的第四节；如果希望使用 WEB 方式管理防火墙，请您仔细阅读本指南的第五节。

防火墙主要以两种方式接入网络：路由方式和混合方式。在路由方式下，配置完防火墙后您还能还需要把受保护区域内主机的网关指向防火墙；混合方式时，由防火墙自动判定具体报文应该通过路由方式还是透明桥方式转发，如果为透明桥方式，则不用修改已有网络配置。

二、防火墙硬件描述

SecGate 3600-G10 防火墙前面板示意图如下图所示，SecGate 3600-G10 接口排列分

为两层，上层为 NP 网络接口，下层为专用控制接口。以 G10-218 配置为例，上层从左到右依次排列一个千兆电口（带千兆 VPN 功能）、两个千兆 GBIC 光口模块、8 个百兆电口模块，以及公司标识。下层从左到右依次排列有专用管理口（MNG）、HA 专用口（HA）、AUX 口、CONSOLE 口、电源指示灯和系统状态指示灯。

说明如下：

文字项	说　明
百兆网络接口	8 个百兆网络接口分两层，上层从左至右依次为：fe1、fe3、fe5、fe7，下层从左至右依次为：fe2、fe4、fe6、fe8。 该接口支持 10M/100M 自适应，自动识别线序，采用 5 类双绞线，RJ-45 头连接。 可在WEB管理界面“网络配置>>网络接口”中配置相关属性；或者，在命令行界面使用interface命令配置相关属性。
千兆网络接口	从左至右依次为：ge1、ge2、ge3。 ge1 为千兆电口，ge2、ge3 为千兆光模块 GBIC，支持热插拔，可接单模或多模光纤。 可在 WEB 管理界面“网络配置>>网络接口”中配置相关属性；或者，在命令行界面使用 interface 命令配置相关属性。 GBIC 的工作电压：＋3.3V 请注意使用与网络设备（交换机、路由器）相匹配的 GBIC。
MNG 管理接口	专用管理口，支持 10M/100M 自适应，采用 5 类双绞线，RJ-45 头连接。 注意：如果 PC 直接和管理口相连，需要使用交叉网线。
HA 专用接口	如果使用了 HA 功能，则需要使用交叉网线把两台防火墙的 HA 口连接起来。
CONSOLE 接口	系统管理串行接口，波特率为9600。管理员可用随机专用串口线连接终端和防火墙来管理系统。
电源指示灯	面板上标识为 POWER，加电以后一直为绿色
状态指示灯	面板上标识为SYSTEM，系统正常运行时黄灯一直闪烁。停止闪烁表示系统出现故障。

SecGate 3600-G10 防火墙硬件的后面板示意图如下图所示：

说明如下：

冗余电源	两个拉手分别对应两个电源模块，便于更换电源模块。 两个电源接口（交流 220V）分别对应两个电源模块。 指示灯用于指示电源模块运行状态，绿色指示灯亮表示电源模块在运行。
主控板固定螺栓	两个主控板螺栓用于固定主控板。请勿拆卸！

三、防火墙安装

1. 安全使用注意事项

本章列出各条安全使用注意事项，请仔细阅读并在使用 SecGate 3600-G10 防火墙过程中严格执行。这将有助于您更安全地使用和维护您的防火墙。

（1）您使用的 SecGate 3600-G10 防火墙采用 220V 交流电源，请确认工作电压并且务必使用三芯带接地电源插头和插座。良好地接地是您的防火墙正常工作的重要保证。

（2）为使防火墙正常工作，请不要将其放置于高温或者潮湿的地方。

（3）请不要将防火墙放在不稳定的桌面上，万一跌落，会对防火墙造成严重损害。

（4）请保持室内通风良好并保持防火墙通气孔畅通。

（5）为减少受电击的危险，在防火墙工作时不要打开外壳，即使在不带电的情况下，也不要随意打开防火墙机壳。

（6）清洁防火墙前，请先将防火墙电源插头拔出。不要用湿润的布料擦拭防火墙，不能用液体清洗防火墙。

2. 检查安装场所

SecGate 3600-G10防火墙必须在室内使用，无论您将防火墙安装在机柜内还是直接放在工作台上，都需要保证以下条件：

（1）确认防火墙的入风口及通风口处留有空间，以利于防火墙机箱的散热。

（2）确认机柜和工作台自身有良好的通风散热系统。

（3）确认机柜和工作台足够牢固，能够支撑防火墙及其安装附件的重量。

（4）确认机柜和工作台的良好接地。

为保证防火墙正常工作和延长使用寿命，安装场所还应该满足下列要求。

2.1 温度／湿度要求

为保证SecGate 3600-G10防火墙正常工作和使用寿命，机房内需维持一定的温度和湿度。若机房内长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，有时也易发生材料机械性能变化、金属部件锈蚀等现象；若相对湿度过低，绝缘垫片会干缩而引起紧固螺丝松动，同时在干燥的气候环境下，易产生静电，危害防火墙的电路。温度过高则危害更大，长期高温将加速绝缘材料的老化过程，使防火墙的可靠性大大降低，严重影响其寿命。

2.2 洁净度要求

灰尘对防火墙的运行安全是一大危害。室内灰尘落在机体上，可以造成静电吸附，使金属接插件或金属接点接触不良。尤其是在室内相对湿度偏低的情况下，更易造成静电吸附，不但会影响设备寿命，而且容易造成通信故障。除灰尘外，机房内应防止有害气体（如SO_2、H_2S、NH_3、Cl_2 等）的侵入。这些有害气体会加速金属的腐蚀和某些部件的老化过程。同时防火墙机房对空气中所含的盐、酸、硫化物也有严格的要求。

2.3 抗干扰要求

防火墙在使用中可能受到来自系统外部的干扰，这些干扰通过电容/电感耦合，电磁波辐射，公共阻抗（包括接地系统）耦合和导线（电源线、信号线和输出线等）的传导方式对设备产生影响。为此应注意以下条件：

（1）交流供电系统为TN系统，交流电源插座应采用有保护地线（PE）的单相三线电源插座，使设备上滤波电路能有效的滤除电网干扰。

（2）防火墙工作地点远离强功率无线电发射台、雷达发射台、高频大电流设备。

（3）电缆要求在室内走线，禁止户外走线，以防止因雷电产生的过电压、过电流将设备信号口损坏。

3. 安装

SecGate 3600-G10 防火墙可以放置在桌面上，也可以放在标准的 19 英寸机架上。安放在桌面上不需要特别的操作，安放在机架上时需要自备螺丝刀，螺钉在包装箱中。

4．加电启动

防火墙启动步骤如下：

（1）请将防火墙安装在机架上或放在一个水平面上。

（2）确认防火墙电源是关闭的。

（3）连接电源线。

（4）防火墙可以通过网口用网线连接管理主机，也可通过串口线连接管理主机进而用超级终端管理防火墙。

（5）接通电源，按下防火墙上的电源开关，置于 ON 状态，防火墙加电启动。

（6）听到“嘀嘀嘀”三声，且橙黄色的状态灯开始闪烁，表示启动成功。

防火墙启动成功以后，请通过 CONSOLE 口命令行或者 WEB 浏览器方式管理防火墙，具体方法请参考以下相关章节。

如果防火墙未正常启动，请按以上步骤进行检查，如仍无法解决问题，请您联系供应商相关技术支持人员。

四、通过 CONSOLE 口命令行进行管理

基本步骤：连接串口线 —> 配置超级终端 —> 开始配置管理

1．选用管理主机

要求该主机具备：

（1）空闲的 RS232 串口

（2）有超级终端软件。比如 Windows 系统中的“超级终端”连接程序。

2. 连接防火墙

利用随机附带的串口线连接管理主机的串口和防火墙串口 CONSOLE，启动超级终端工具，以 Windows 自带“超级终端”为例：点击“开始 --> 所有程序 --> 附件 --> 通讯 --> 超级终端”，选择用于连接的串口设备，定制通讯参数：

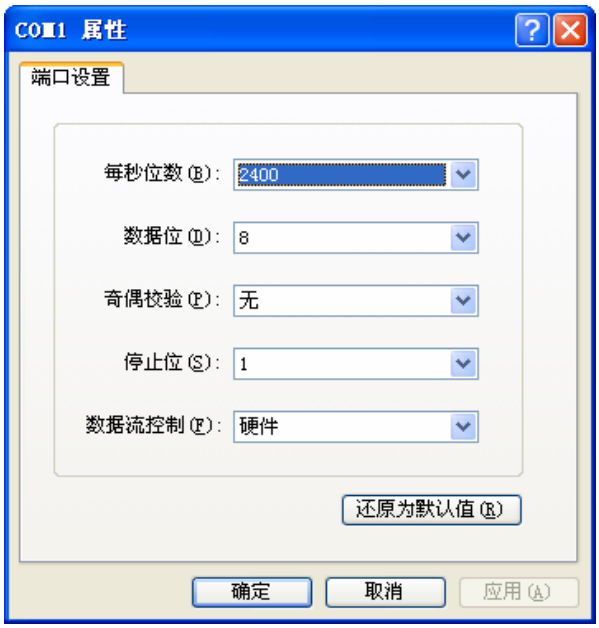
（1）每秒位数：9600；

（2）数据位：8；

（3）奇偶校验：无；

（4）停止位：1；

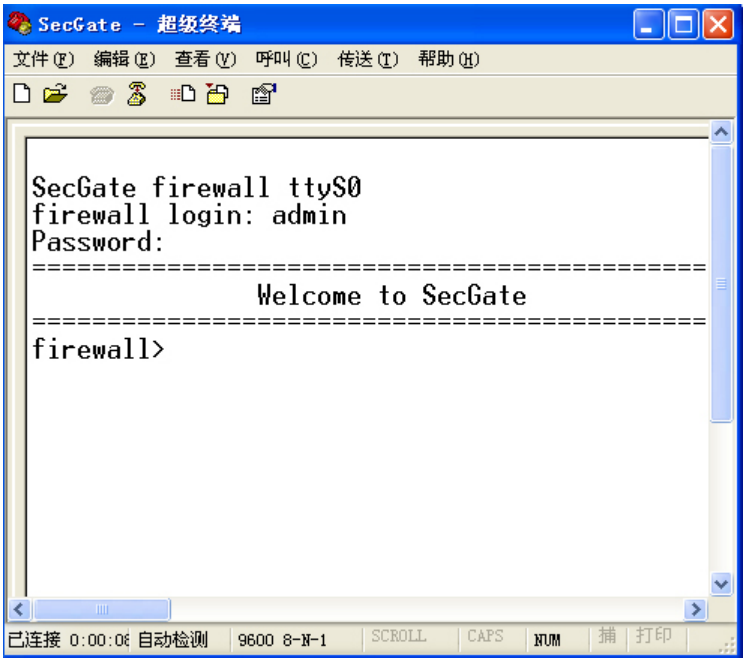
（5）数据流控制：无；



提示：对于 Windows 自带“超级终端”，选择“还原默认值”即可。

3．登录 CLI 界面

连接成功以后，提示输入管理员账号和口令时，输入出厂默认账号“admin”和口令“firewall”即可进入登录界面，注意所有的字母都是小写的。



五、通过 WEB 界面进行管理

基本过程：配置管理主机 —>配置管理主机 —> 安装 usb 电子钥匙驱动—>认证管理员身份—>开始配置管理

1．选用管理主机

要求具有以太网卡、USB 接口和光驱，操作系统可以为 Window98/2000/XP 中的任

意一种，管理主机 IE 建议为 5.0 以上版本、文字大小为中等，屏幕显示建议设置为 1024×768。

2. 安装认证驱动程序

在第一次使用电子钥匙前，需要先按照电子钥匙的认证驱动程序。插入随机附带的驱动光盘，进入光盘\\Ikey Driver\目录，双击运行 INSTDRV 程序，选择“开始安装”，随后出现安装成功的提示，选择“退出”，重新插锁。

切记：安装驱动前不要插入 usb 电子钥匙。

3. 安装 USB 电子钥匙

在管理主机上插入 usb 电子钥匙，系统提示找到新硬件，稍后提示完全消失，说明电子钥匙已经可以使用了。如果您在安装驱动前插了一次电子钥匙，此时系统会弹出“欢迎使用找到新硬件向导”对话框。直接选择“下一步”并耐心等待，约半分钟后系统将提示驱动程序没有经过 windows 兼容性测试，选择“仍然继续”即可，如长时间（如约 3 分钟）无反映，请拔下 usb 电子钥匙，重启系统后再试一次，如仍无法解决，请您联系技术支持人员。

4. 连接管理主机与防火墙

利用随机附带的网线直接连接管理主机网口和防火墙 FE1 网口（初始配置，只能将管理主机连接在防火墙的第一个网口上），把管理主机 IP 设置为 10.50.10.44，掩码为 255.255.255.0。在管理主机运行 ping 10.50.10.45 验证是否真正连通，如不能连通，请检查管理主机的 IP（10.50.10.44）是否设置在与防火墙相连的网络接口上。

强烈建议该网口不要绑定其他 IP，并且使用交叉线直接连接防火墙。

5．认证管理员身份

第一、插入电子钥匙。

第二、运行\\Admin Auth\目录中的 ikeyc 程序，提示输入用户 pin，输入 12345678 即可。此时电子钥匙中存储的默认防火墙 IP 地址为 10.50.10.45，认证端口为 9999。如果认证成功，将弹出对话框提示“通过认证”。说明管理员已经通过了身份认证，可以对防火墙进行配置管理了。如果出现其他错误，请检查网络连接、pin 码是否输入错误等。

6．登录防火墙 WEB 界面

运行 IE 浏览器，在地址栏输入 https://10.50.10.45:8888，等待约 20 秒钟会弹出一个对话框提示接受证书，选择确认即可。系统提示输入管理员帐号和口令。缺省情况下，管理员帐号是 admin，密码是：firewall。

六、常见问题解答 FAQ

1．如何用远程 SSH 方式登录防火墙？

答：（1）选中“远程 SSH 管理”，如下图：

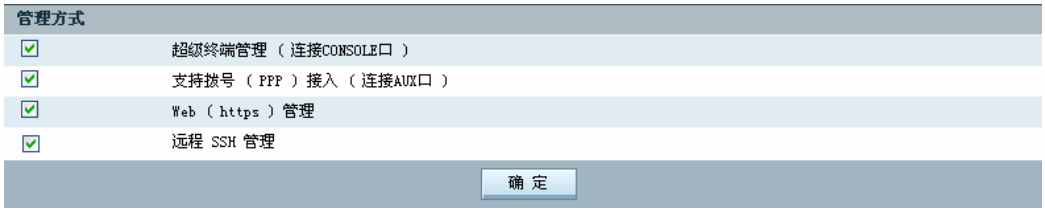


图 1

（2）确认防火墙已设置可管理的 IP 地址及管理主机 IP 地址；

（3）在管理主机上使用 SSH 客户端连接防火墙，建立连接后会出现登录提示符，此时即可输入管理员帐户名和密码进入防火墙命令行管理方式。

以 putty 作为客户端为例，如下图所示：

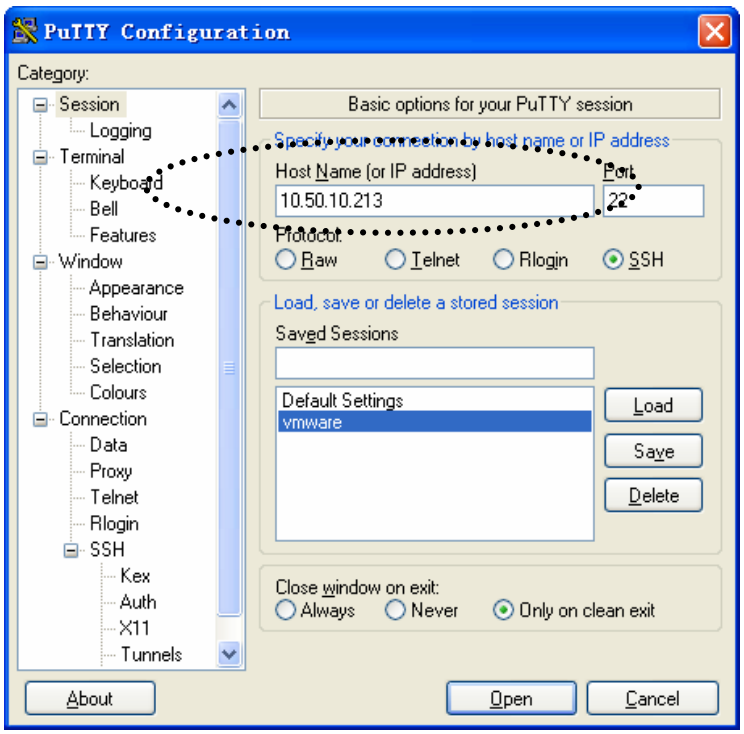


图 2

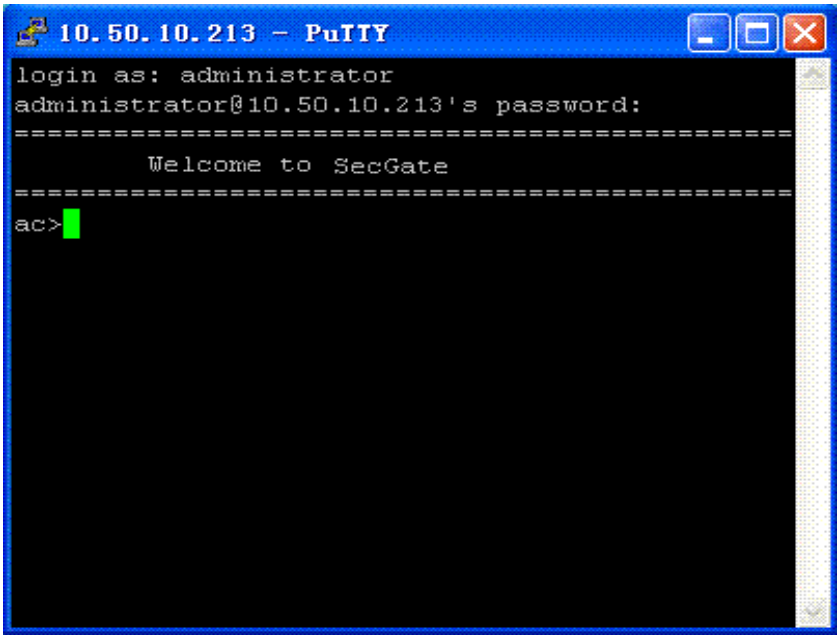


图 3

2．为什么删除不掉超级管理员？

答：因为本防火墙设置超级管理员是不能被删除的。

3．可以多个管理员同时在线管理防火墙吗？

答：可以。

（1）进入“管理配置>>管理员账号”

（2）选中“允许多个管理员管理同时管理”。

（3）在弹出的对话框中点击“确认”按钮即可。

4．防火墙能抵抗那些恶意攻击？应如何配置使防火墙能抵抗这些恶意攻击？

答：防火墙能抵抗以下的恶意攻击： SYN Flood 攻击；ICMP Flood 攻击；Ping of Death 攻击；UDP Flood 攻击；PING SWEEP 攻击；TCP 端口扫描；UDP 端口扫描；松散源路由攻击；严格源路由攻击；WinNuke 攻击；smuef 攻击；TCP 无标记攻击；圣诞树攻

击；SYN&FIN 攻击；无确认 FIN 攻击；IP 安全选项攻击；IP 记录路由攻击；IP 流攻击；IP 时间戳攻击；Land 攻击；tear drop 攻击。

（1）进入“安全策略>>抗攻击”。

（2）点击相应网络接口的  ，启动该网络接口的抗攻击功能。

（3）配置相应网络接口的抗攻击参数。

5．如何补全命令行中的关键字？

答：输入关键字的第一个字母，按 Tab 键就可以补全关键字。

6．如何获得命令的提示信息？

答：按 ？ 可以获得上下文相关的帮助信息。

7．我在命令行界面下，输入这样的备注 address1 address2 ，为什么会提示错误？

答：如果输入的备注信息中包含空格，必须使用双引号，正确的备注格式应该是“address1 address2”。

8．为何在网络连接正确时，不能“ping”通防火墙？

答：检查相应的网络接口是否启动 ping 功能。

9．从防火墙上 ping 其它的主机，发现网络不通，可能有哪些问题？

答：网线没连接好；路由不正确；对方机器不允许（如加载了个人防火墙）。

10．内网、DMZ 网段不能访问外网，可能有哪些问题？

答：网线没连接好；规则中未允许访问相应服务，如未允许 ICMP 包通过就 ping 不通；

NAT 或路由不正确；启动了“IP/MAC 绑定”或“用户认证功能”，但用户没登录或没在 IP/MAC 表中加入正确的绑定信息。

11．规则的执行顺序是怎么样的？

答：先执行优先级高的规则，规则的序号代表了规则的优先级，一般越先添加的规则，序号越小，优先级越高。但是，选中规则后，点击 

可以改变规则的优先级。

12．如何配置代理功能？

答：SecGate 3600 防火墙支持 HTTP 代理，FTP 代理，TELENT 代理，SMTP 代理，POP3 代理五种预定义代理和自定义代理。配置代理功能步骤如下：

（1）定义需要代理的服务对象。

（2）配置相应的代理。

（3）添加代理规则，

13．SecGate 3600 防火墙有几种工作模式？

答：SecGate 3600 防火墙有两种工作模式——路由模式和混合模式，可以使用命令“sysif set <interface> mode route/broute”来设置防火墙的工作模式。

14．SecGate 3600 防火墙没有发送报警邮件？

答：请确认“系统配置”>>“报警邮箱”页面内的各项内容设置正确，另外请设置域名服务器。