

防火墙基础技术

www.huawei.com

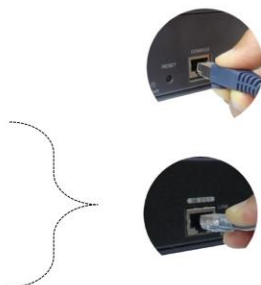
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.



防火墙设备管理概述

- 设备登录管理

- Console登录
- Web登录
- telnet登录
- SSH登录



- 设备文件管理

- 配置文件管理
- 系统文件管理（软件升级）
- License管理



- 设备登录管理

Console:通过RS-232配置线连接到设备上，使用Console方式登录到设备上，进行配置。

Telnet: 通过PC终端连接到网络上，使用Telnet方式登录到设备上，进行配置。

Web: 在客户端通过Web浏览器访问设备，进行控制和管理。

SSH: 提供安全的信息保障和强大认证功能，保护设备系统不受IP欺骗等攻击。

- 设备文件管理

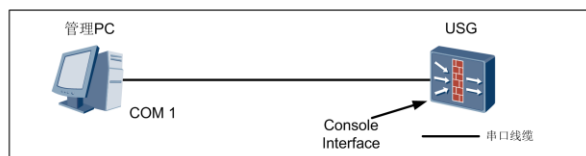
配置文件是设备启动时要加载的配置项。用户可以对配置文件进行保存、更改和清除、选择设备启动时加载的配置文件等操作。系统文件包括USG设备的软件版本，特征库文件等。一般软件升级需要管理系统文件。

系统软件升级。上传系统软件到设备可通过TFTP方式和FTP方式上传系统软件到设备上。升级系统软件 配置设备下次启动时使用的软件系统。

License是设备供应商对产品特性的使用范围、期限等进行授权的一种合约形式，License可以动态控制产品的某些特性是否可用。

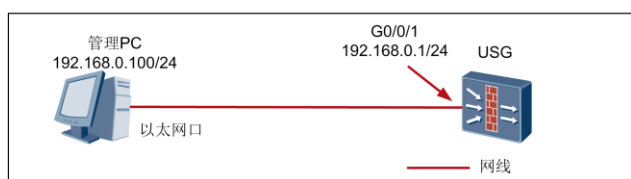
设备登录管理

- 设备登录管理组网- Console



- 设备登录管理组网- Web / SSH / Telnet

- 直接相连（通过局域网）
- 远程连接（通过广域网）



- 通过Console口登录：

使用PC终端通过连接设备的Console口来登录设备，进行第一次上电和配置。当用户无法进行远程访问设备时，可通过Console进行本地登录；当设备系统无法启动时，可通过console口进行诊断或进入BootRom进行系统升级。

- 通过Telnet登录：

通过PC终端连接到网络上，使用Telnet方式登录到设备上，进行本地或远程的配置，目标设备根据配置的登录参数对用户进行验证。Telnet登录方式方便对设备进行远程管理和维护。

- 通过SSH登录：

提供安全的信息保障和强大认证功能，保护设备系统不受IP欺骗等攻击。SSH登录能更大限度的保证数据信息交换的安全。

- 通过Web登录：

在客户端通过Web浏览器访问设备，进行控制和管理。适用于配置终端PC通过Web方式登录。

注意：PC和USG以太网口的IP地址必须在同一网段或PC和USG之间有可达路由。

通过Console口登录设备

- USG配置口登录的缺省用户名为admin，缺省用户密码为Admin@123。其中，用户名不区分大小写，密码要区分大小写。



如果使用PC进行配置，需要在PC上运行终端仿真程序（如Windows3.1的Terminal，Windows98/Windows2000/Windows XP的超级终端），建立新的连接。如图所示，键入新连接的名称，单击“确定”。

在串口的属性对话框中设置波特率为9600，数据位为8，奇偶校验为无，停止位为1，流量控制为无，单击“确定”，返回超级终端窗口。

打开设备电源开关。设备上电后，检查设备前面板上的指示灯显示是否正常。

通过Web方式登录设备

- 设备缺省可以通过GigabitEthernet0/0/0接口来登录Web界面。
 - 将管理员PC的网络连接的IP地址获取方式设置为“自动获取IP地址”。
 - 将PC的以太网口与设备的缺省管理接口直接相连，或者通过交换机中转相连。
 - 在PC的浏览器中访问http://192.168.0.1，进入Web界面的登录页面。
 - 缺省用户名为**admin**，密码为**Admin@123**



缺省情况下，设备开启HTTP；建议开启HTTPS，提高安全性。用户可以通过用户名/密码：admin/Admin@123登录，为保证系统安全，登录后请修改密码。

只有GigabitEthernet 0/0/0接口加入Trust域并提供缺省IP地址（192.168.0.1/24），并开放Trust域到Local域的缺省包过滤，方便初始登录设备。

缺省情况下开放Local域到其他任意安全区域的缺省包过滤，方便设备自身的对外访问。

其他接口都没有加安全区域，并且其他域间的缺省包过滤关闭。要想设备转发流量必须将接口加入安全区域，并配置域间安全策略或开放缺省包过滤。

Web登录配置管理

- 配置USG的IP地址。(略)
- 配置USG接口Web设备管理。
[USG-GigabitEthernet0/0/1] service-manage enable
[USG-GigabitEthernet0/0/1] service-manage http permit
- 启动Web管理功能。
[USG] web-manager security enable port 2000
- 配置Web用户。
[USG] aaa
[USG-aaa] local-user webuser password cipher Admin@123
[USG-aaa] local-user webuser service-type web
[USG-aaa] local-user webuser level 3

- 开启HTTP

执行命令system-view，进入系统视图。

执行命令web-manager enable [port port-number]，开启HTTP。

此时在Web浏览器中应该通过http://格式的地址登录设备。默认端口号是80。

- 开启HTTPS（默认证书）

执行命令system-view，进入系统视图。

执行命令web-manager security enable port port-number，开启HTTPS。

此时在Web浏览器中应该通过https://格式的地址登录设备。

- local-user level命令用来配置本地用户的优先级。

Level 3：管理级

VRP命令行级别

参观级	网络诊断工具命令（ping、tracert）、从本设备出发访问外部设备的命令（包括：Telnet客户端、SSH、Rlogin）等，该级别命令不允许进行配置文件保存的操作。
监控级	用于系统维护、业务故障诊断等，包括display、debugging命令，该级别命令不允许进行配置文件保存的操作。
配置级	业务配置命令，包括路由、各个网络层次的命令，这些用于向用户提供直接网络服务。
管理级	关系到系统基本运行，系统支撑模块的命令，这些命令对业务提供支撑作用

VRP系统命令采用分级保护方式，命令被划分为参观级、监控级、配置级、管理级4个级别。

参观级：网络诊断工具命令（ping、tracert）、从本设备出发访问外部设备的命令（包括：Telnet客户端、SSH、Rlogin）等，该级别命令不允许进行配置文件保存的操作。

监控级：用于系统维护、业务故障诊断等，包括display、debugging命令，该级别命令不允许进行配置文件保存的操作。

配置级：业务配置命令，包括路由、各个网络层次的命令，这些用于向用户提供直接网络服务。

管理级：关系到系统基本运行，系统支撑模块的命令，这些命令对业务提供支撑作用，包括文件系统、FTP、TFTP、Xmodem下载、配置文件切换命令、备板控制命令、用户管理命令、命令级别设置命令、系统内部参数设置命令等。

系统对登录用户也划分为4级，分别与命令级别对应，即不同级别的用户登录后，只能使用等于或低于自己级别的命令。当用户从低级别用户切换到高级别用户时，需要使用命令：super password [level user-level] { simple | cipher } password 切换。

VRP命令视图

- 系统将命令行接口划分为若干个命令视图，系统的所有命令都注册在某个（或某些）命令视图下，只有在相应的视图下才能执行该视图下的命令。
- 命令视图的分类：
 - 用户视图
 - <USG>
 - 系统视图
 - [USG]
 - 接口视图
 - [USG -Ethernet0/0/1]
 - 协议视图
 - [USG -rip]
 -

系统将命令行接口划分为若干个命令视图，系统的所有命令都注册在某个（或某些）命令视图下，只有在相应的视图下才能执行该视图下的命令。

与防火墙建立连接即进入用户视图，它只完成查看运行状态和统计信息的简单功能，再键入system-view进入系统视图，在系统视图下，可以再键入不同的配置命令进入相应的协议、接口等视图。

VRP在线帮助

- 键入一命令，后接以空格分隔的“?”，如果该位置为关键字，则列出全部关键字及其简单描述。

<USG 5000> display ?

- 键入一命令，后接以空格分隔的“?”，如果该位置为参数，则列出有关的参数描述。

[USG 5000] interface ethernet ?

<3-3> Slot number

- 键入一字符串，其后紧接“?”，列出以该字符串开头的所有命令。

<USG 5000> d?

debugging delete dir display

VRP平台提供十分方便的命令行在线帮助，只需要在有疑问的地方键入问号即可。

例如在系统视图下直接键入问号，系统便会列出在系统视图下可以配置的命令参数，或者在参数后键入空格，然后再键入问号，便可获得该参数后可以使用的参数列表，如果是键入一字符串，其后紧按键入问号，则系统会列出以该字符串开头的命令。

VRP在线帮助（续）

- 输入命令的某个关键字的前几个字母，按下<TAB>键，可以显示出完整的关键字
- 暂停显示时键入<Ctrl+C> 停止显示和命令执行
- 暂停显示时键入空格键 继续显示下一屏信息
- 暂停显示时键入回车键 继续显示下一行信息

输入命令的某个关键字的前几个字母，按下<tab>键，系统还可以显示出完整的关键字。

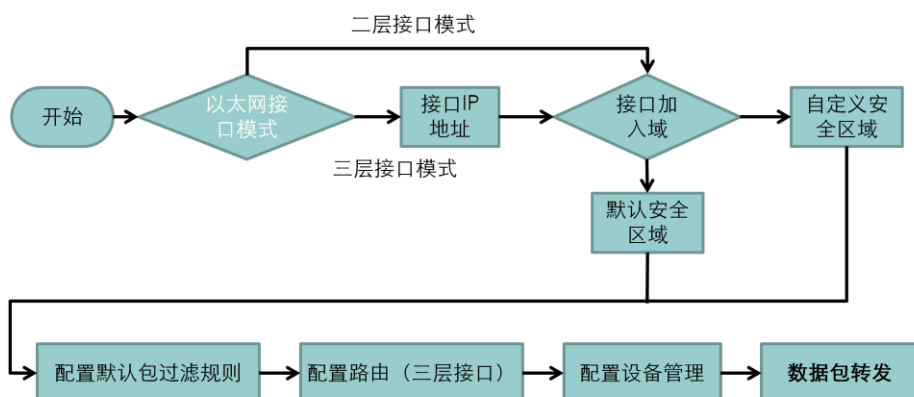
我们看到有的时候在一次显示信息有可能会超过一屏，此时系统提供了暂停功能，这时用户可以有三种选择：

暂停显示时键入<Ctrl+C> 停止显示和命令执行

暂停显示时键入空格键 继续显示下一屏信息

暂停显示时键入回车键 继续显示下一行信息

防火墙基本配置流程



以上配置流程不等同于防火墙转发流程。

基本配置包括基本功能配置和设备管理配置。

配置接口模式

步骤 1 进入系统视图。

```
<USG>system-view
```

步骤 2 进入接口视图

```
[USG]interface interface-type interface-number
```

步骤 3 配置三层以太网接口或者二层以太网接口

配置三层以太网接口

```
ip address ip-address { mask | mask-length }, 。
```

或配置二层以太网接口

```
portswitch
```

在USG中，支持以下两种接口卡：

二层接口卡：所有接口均为二层以太网接口，不支持切换为三层接口。

三层接口卡：所有接口缺省为三层以太网接口，可以通过命令portswitch切换为二层以太网接口。

配置安全区域

步骤 1 执行命令**system-view**，进入系统视图。

步骤 2 执行命令**firewall zone [name] zone-name**，创建安全区域，并进入相应安全区域视图。

安全区域
已经存在

不必配置关键字name，直接进入安全区域视图

安全区域
不存在

需要配置关键字name，进入安全区域视图

步骤 3 执行命令**set priority security-priority**，配置安全区域的安全级别。

- 创建自定义安全区域。

步骤1 执行命令system-view，进入系统视图。

步骤2 执行命令firewall zone [name] zone-name，创建安全区域，并进入相应安全区域视图。

执行firewall zone命令时，存在如下两种情况：

安全区域已经存在：不必配置关键字name，直接进入安全区域视图。

安全区域不存在：需要配置关键字name，进入安全区域视图。

系统预定义了Local、Trust、DMZ、Untrust 共4个安全区域。在路由模式下，4个安全区域无需创建，也不能删除。防火墙最多支持16个安全区域

步骤3 执行命令set priority security-priority，配置安全区域的安全级别。

- 配置安全区域的安全级别时，需要遵循如下原则：

1. 只能为自定义的安全区域设定安全级别。
2. 安全级别一旦设定，不允许更改。
3. 同一系统中，两个安全区域不允许配置相同的安全级别。
4. 新建的安全区域，未设定其安全级别前，系统规定其安全级别为0。

将接口加入安全区域

步骤 1 执行命令**system-view**，进入系统视图。

步骤 2 执行命令**firewall zone [name] zone-name**，创建安全区域，并进入相应安全区域视图。

步骤 3 执行命令**add interface interface-type interface-number**，配置接口加入安全区域。

配置域间缺省包过滤规则

步骤 1 执行命令system-view，进入系统视图。

步骤 2 执行命令firewall packet-filter default { permit | deny } { { all | interzone zone1 zone2 } [direction { inbound | outbound }] }，配置域间缺省包过滤规则。



zone1与zone2有先后顺序吗???

没有先后顺序。因为Inbound和Outbound的方向只与域的优先级有关

- 配置域间包过滤规则

当数据流无法匹配防火墙中的ACL时，会按照域间缺省包过滤规则转发或丢弃该数据流的报文。配置域间缺省包过滤规则，需要进行如下操作。

步骤 1 执行命令system-view，进入系统视图。

步骤 2 执行命令firewall packet-filter default { permit | deny } { { all | interzone zone1 zone2 } [direction { inbound | outbound }] }，配置域间缺省包过滤规则。

参数说明：

permit：默认过滤规则为允许；deny：默认过滤规则为禁止；all：配置作用于所有安全区域间；interzone：配置作用于特定安全区域间；zone1：第一个安全区域的名字，可以是DMZ、Local、Trust、Untrust区域以及自定义区域；zone2：第二个安全区域的名字，可以是DMZ、Local、Trust、Untrust区域以及自定义区域；direction：配置过滤规则作用的方向；inbound：配置过滤规则作用于安全区域间入方向；outbound：配置过滤规则作用于安全区域间出方向。

配置路由

- 配置静态路由，需要进行如下操作。

步骤 1 执行命令**system-view**，进入系统视图。

步骤 2 执行命令**ip route-static ip-address { mask | mask-length } { interface-type interface-number | next-ip-address } [preference value]** 增加一条静态路由

- 配置缺省路由，需要进行如下操作。

步骤 1 执行命令**system-view**，进入系统视图。

步骤 2 执行命令**ip route-static 0.0.0.0 { 0.0.0.0 | 0 } { interface-type interface-number | next-ip-address } [preference value]**，配置缺省路由。

通过静态路由的配置可建立一个互通的网络，但这种配置问题在于：当一个网络故障发生后，静态路由不会自动发生改变，必须有管理员的介入。

缺省路由就是在没有找到匹配的路由表入口项时才使用的路由。即只有当没有合适的路由时，缺省路由才被使用。在路由表中，缺省路由以到网络0.0.0.0（掩码为0.0.0.0）的路由形式出现。如果报文的目的地址不能与路由表的任何入口项相匹配，那么该报文将选取缺省路由。如果没有缺省路由且报文的目的地址不在路由表中，那么该报文被丢弃的同时，将向源端返回一个ICMP 报文报告该目的地址或网络不可达。

Thank you

www.huawei.com

Copyright©2013 Huawei Technologies Co., Ltd. All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.