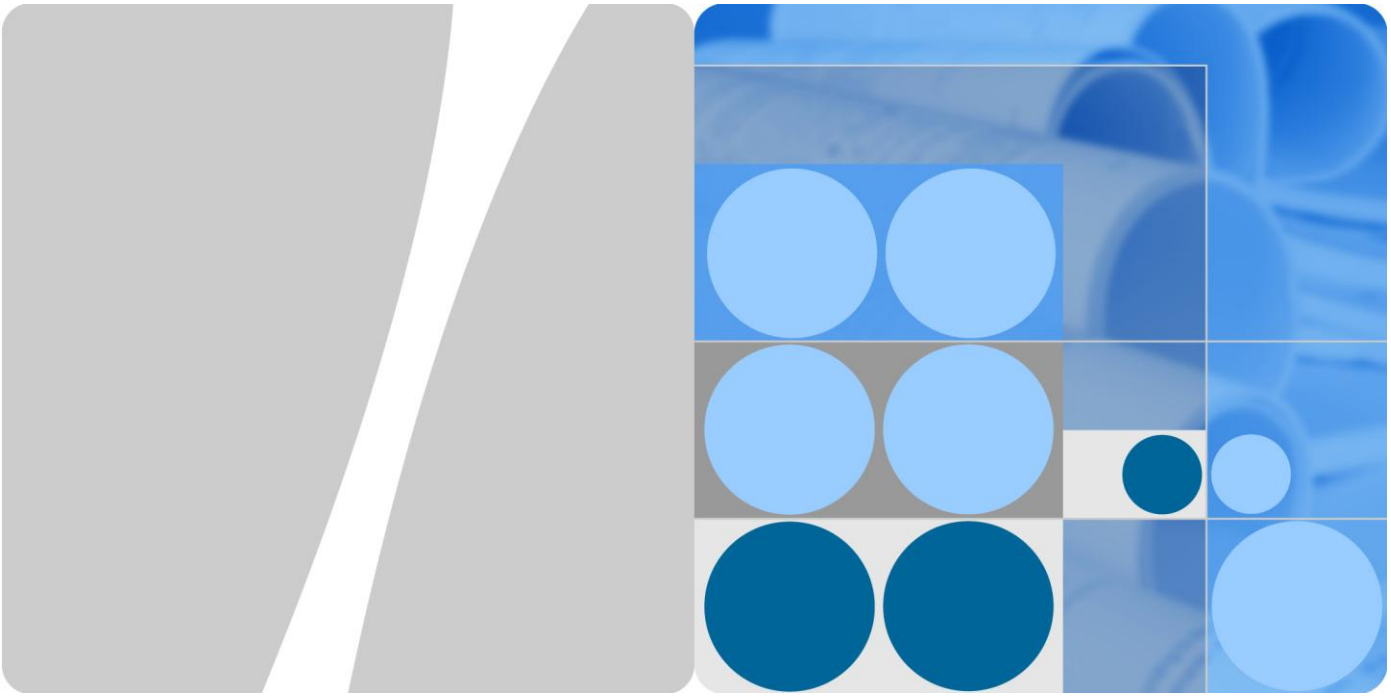


USG2200/5100/5500 统一安全网关
产品概述

文档版本 01

发布日期 2012-05-23

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

1 前言

产品版本

与本文档相对应的产品版本如下所示。

产品名称	产品版本
Secoway USG2200/5100/5500	V300R001

读者对象

本文档介绍 Secoway USG 的定位、功能特性、软硬件结构、典型组网方式和应用场景、遵循标准和技术指标。

通过本文档可以快速了解 USG 产品全貌。

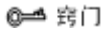
本文档主要适用于以下工程师：

- 网络规划工程师
- 数据配置工程师
- 系统维护工程师
- 网管管理员

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	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。

符号	说明
	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。
	表示能帮助您解决某个问题或节省您的时间。
	表示是正文的附加信息，是对正文的强调和补充。

修订记录

文档版本 01 (2012-05-23)

第一次正式发布。

2 产品定位

USG5500 系列

USG5500 系列产品是华为技术有限公司（以下简称华为）面向大中型企业和下一代数据中心推出的新一代电信级统一安全网关设备。可广泛应用于运营商、企业、政府、金融、能源、学校等领域的网络边界。

USG5500 系列包含 USG5530S、USG5530、USG5550、USG5560，其中 USG5530S、USG5530、USG5550 只有交流型号，USG5560 有交流和直流两种型号。

USG5500 系列产品有 1U 标准机箱和 3U 标准机箱两种硬件形态，提供多个固定千兆以太网口，并拥有丰富的接口扩展能力，支持多种接口卡其中包括万兆以太网接口卡。

该系列产品采用全新的万兆多核硬件平台，面对企业海量业务处理零延迟，打造更高速的网络；融合 Symantec 先进的入侵防御和反病毒技术，全新演绎专业内容安全防御，营造更安全的网络；集成业界领先的 DPI（深度包检测）识别技术，精细管理超千种应用程序，创建更高效的网络。为大型企业和数据中心打造“更高速、更高效、更安全”的高性价比网络体验。USG 可广泛应用于运营商、企业、政府、金融、能源、学校等领域的网络边界。

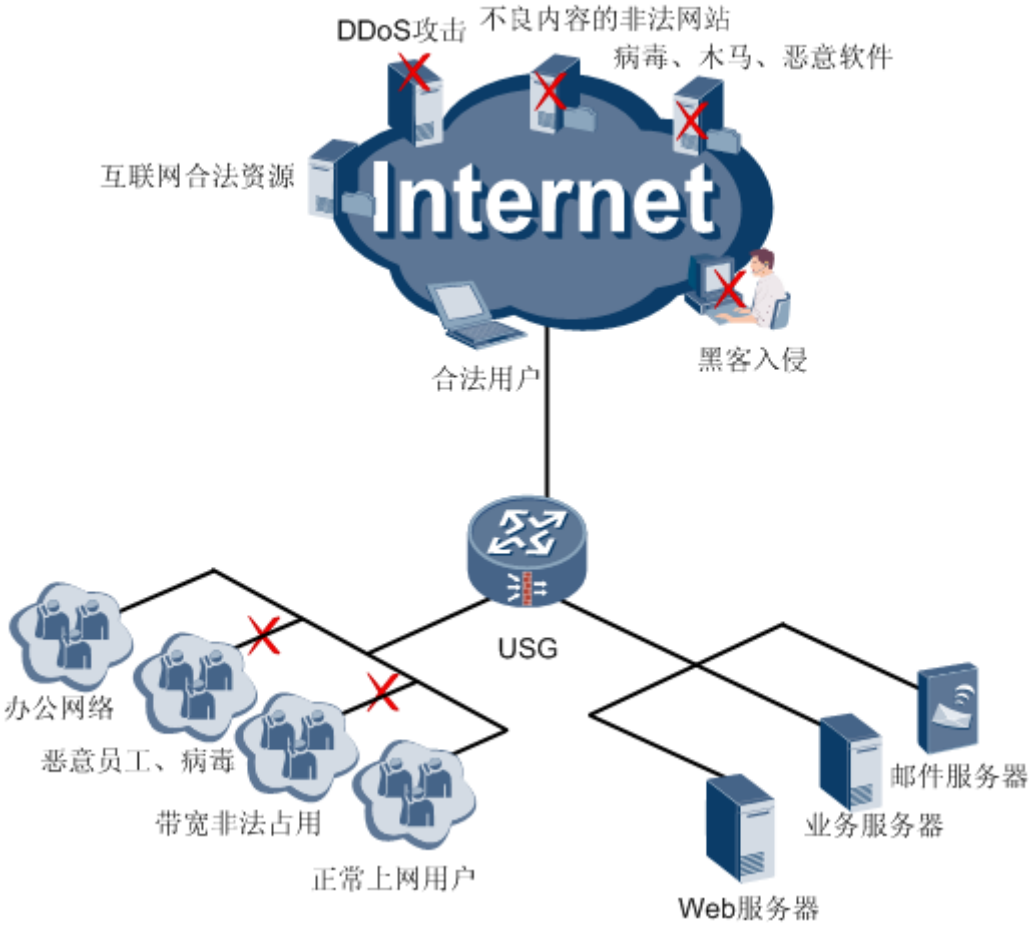
USG5500 在基本防火墙功能基础上还支持丰富的路由协议，可节省用户投资，降低组网成本。

支持 IPv4 和 IPv6 双协议栈工作方式，提供完整的 IPv6 特性和 IPv4 网络向 IPv6 网络平滑迁移的解决方案。

提供了完备的 UTM（Unified Threat Management）功能，致力于内容安全防护、上网行为管理等方面，为用户提供全方位的安全防护。

如图 2-1 所示，USG 部署于网络出口处，有效阻止 Internet 上的黑客入侵、DDoS 攻击，阻止内网用户访问非法网站，限制带宽，为内部网络提供一个安全可靠的网络环境。

图2-1 USG5500 系列典型应用



USG2200/5100 系列

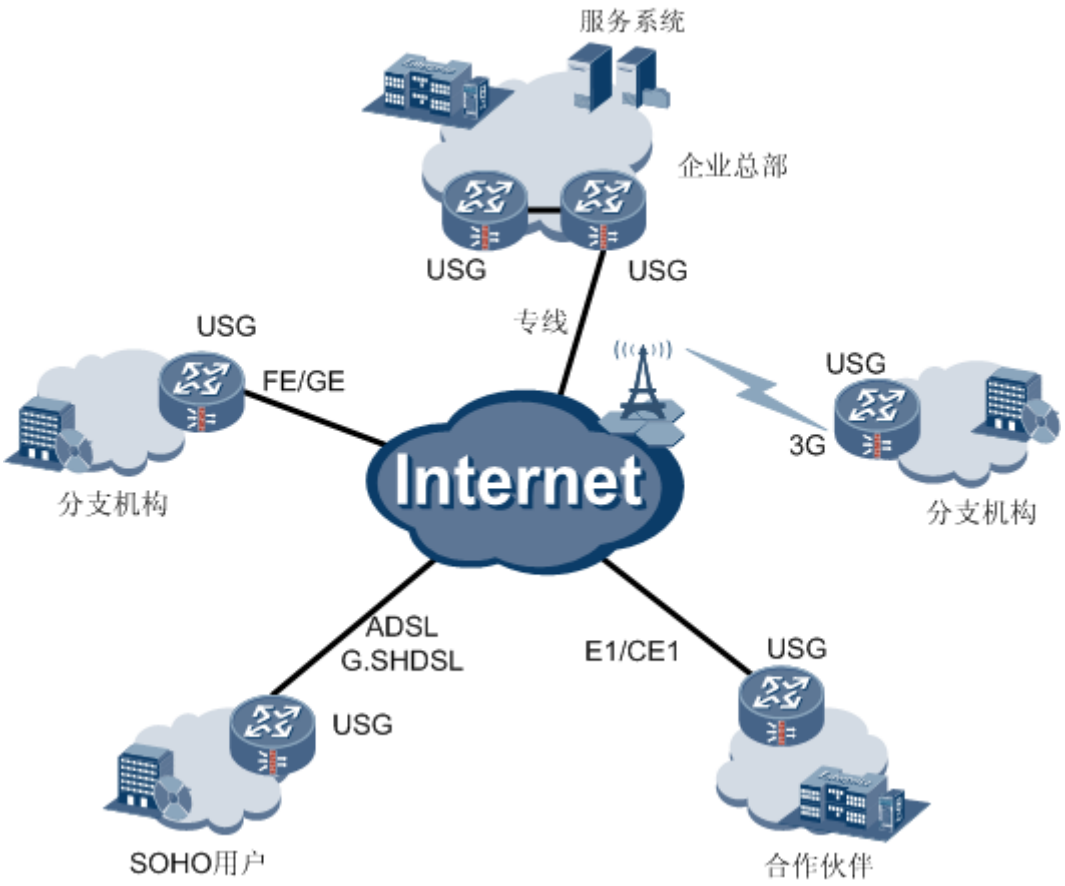
USG2200/5100 系列是华为公司针对中小型企业的需求推出的新一代产品。可广泛应用于中小企业、大型企业分支机构、SOHO 办公类用户以及网吧出口网关等。典型应用如图 2-2 所示。

USG2200/5100 采用模块化设计，集安全、路由、交换、无线（WiFi、3G）等特性于一体，接口类型丰富，性能领先。能为中小企业、大型企业分支机构、SOHO 办公类用户、以及网吧出口网关提供安全防护，并能提供集成的网络出口安全与互联解决方案，降低企业总所有成本，提升企业的效率，是中小型企业网络的理想安全防护设备。

USG2200/5100 将多种业务部署在同一节点，在可靠性、处理能力、模块化端口、业务能力等方面均有突出表现，极大地降低了企业网络建设的初期投资与长期运维成本。

- USG2200 系列包含 USG2210、USG2220、USG2230、USG2250、USG2260，其中 USG2250 和 USG2260 有交直流两种型号。
- USG5100 包含 USG5120、USG5150 和 USG5160。只有 USG5120 有交直流两种型号。USG5150 只有一个型号，但是支持交直流两种可更换的电源模块。USG5160 只有交流型号。

图2-2 USG2200/5100 系列典型应用



3 产品特点

USG5500 具备万兆多核全新硬件平台，为用户打造更高速的网络

- 性能优异，实现海量业务处理。
- 高密度万兆接口，适应不同应用场景需求，为提前跨入万兆时代的用户提供不同组网情况下的安全防护，方便用户细分安全区域。
- 关键部件冗余配置，成熟的链路转换机制，支持光电两类内置 Bypass 插卡，为用户提供超长无故障硬件保障打造永久的办公环境。

多业务集成

- 全面融合了安全、路由、交换、VPN 和无线等多种业务功能，极大地提高了产品的多业务集成能力。
- 真正实现了对以太网交换机的彻底融合。
- USG2200/5100 提供以太网、ADSL2+、SHDSL、E1/CE1、串口和 3G 等多种方式接入因特网，同时提供 WLAN（Wireless Local Area Network）功能。
- 用户可以轻松地使用路由器、防火墙、交换机、VPN 和无线设备的所有特性。

超千种应用程序的精细管理，为用户创建更高效的网络

- 广泛的应用协议识别，让用户对企业带宽应用一目了然。
- 海量网站分类，屏蔽挂马、钓鱼等恶意网站，防范员工不当操作危害内网安全；隔离赌博色情等不良网站，营造绿色上网环境。
- 基于时间、应用、用户、带宽、连接数的多方位调控手段，可有效保障关键业务带宽，提升带宽利用率，提升员工工作效率。

专业内容安全防御技术的重新演绎，为用户提供更安全的网络

- 基于 Symantec 多年积累的反病毒技术，采用文件级内容扫描的 AV 引擎，结合全球领先的仿真环境虚拟执行技术，提供高达 99%的精准检出率。
- 专业漏洞补丁技术，让“变形”无所遁形：传统的基于攻击代码的防护方式，因为攻击种类的频繁变形，需要维护更新庞大签名库，使得 IPS 引擎不堪重负，检测性能低下，误报漏报率较高。USG 采用 Symantec 领先的漏洞防护技术，针对漏洞（而非攻击代码）提供“虚拟补丁”， 让各种攻击变形无所遁形。

- 专业团队实时更新，持续追踪最新、最热门、最高危的系统漏洞和软件漏洞，以最快速的应对方案为用户提供更安全的办公网络。

一键式配置，将您从繁复的策略调优中彻底解放出来

- 基于 Web 界面对设备进行配置管理，更直观，更简单。
- 重点业务提供配置向导，引导管理员轻松完成配置。
- 一键开启 IPS 和 AV，减轻维护工作量，将管理员从费时、费力、繁复的策略配置中解放出来，真正实现快速部署，即插即用。

基于用户身份识别的内网控制及策略一体化

- 提供多种用户认证机制：本地用户数据库认证、Web Portal 用户认证页面、第三方认证服务器的无缝导入、对接、透明认证。
- 安全策略一体化，在精确识别用户(组)、应用协议分类的基础上，提供对流量进行分用户(组)、应用协议分类、时间段、IP 网段、端口等的精确控制。将包过滤、UTM、应用识别控制等策略配置过程集中展现，一次性配置完成。

灵活的扩展能力

USG 采用自主研发的软件平台和具有自主知识产权的安全操作系统。数据平面和管理平面完全分离，这种无依赖性提高了系统安全性。具有很强的可伸缩性、可配置性，并且接口开放，是一个可不断丰富和持续发展的系统平台。

U 盘、CF 卡、Micro-SD 卡等多种新型存储介质的应用提供了对设备存储介质的扩展能力。

USG 系列提供丰富的接口种类，包括 FE、GE、Console、USB、3G、WLAN、Micro-SD 卡接口和可选配的 MIC、DMIC、FIC 和 DFIC 扩展插槽。模块化的设计保证了用户投入的扩展能力，极强的硬件可扩展性为用户以多种方式接入和日后的网络升级提供最大程度的投资保护。

4 产品架构

关于本章

4.1 硬件结构

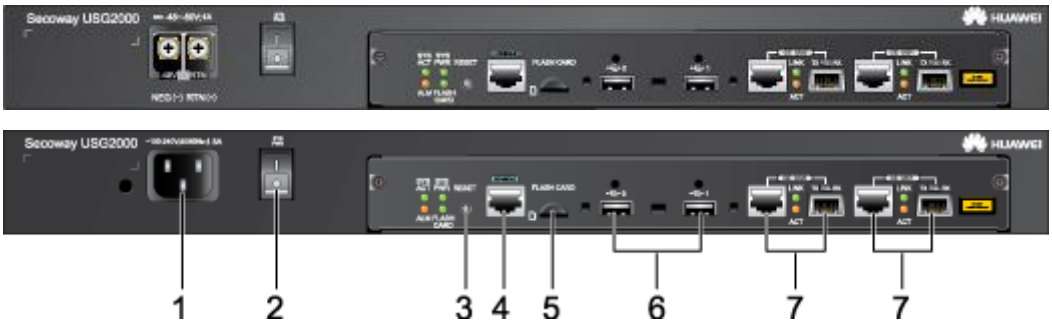
4.1.1 USG2200 系列产品外观

前面板

USG2200 系列产品包含 USG2210、USG2220、USG2230、USG2250 和 USG2260，均由一体化机箱、扩展接口卡组成，都支持交流电源，其中 USG2250/2260 还有支持直流电源的机型。都提供了 4 个 MIC 槽位和 2 个 FIC 槽位，为 1U 高设备。电源和风扇固定在设备中，不支持热插拔。

USG2200 的前面板如图 4-1 所示。

图4-1 USG2200 产品前面板



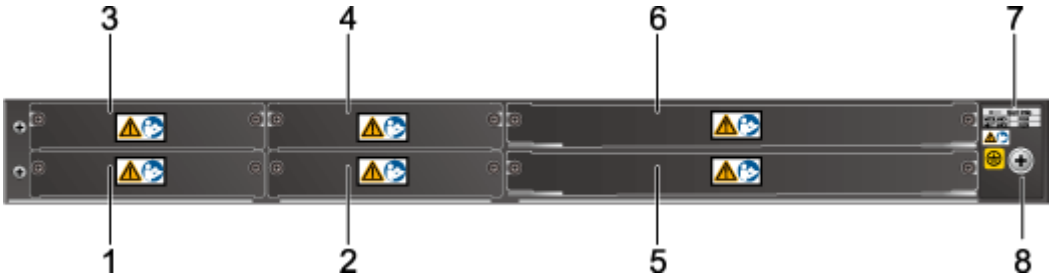
1. 交流/直流电源插座
2. 交流/直流电源开关
3. 系统复位键
4. Console 接口
5. Micro-SD 卡插槽
6. USB 接口

7. GE Combo 接口

后面板

USG2200 后面板如图 4-2 所示。

图4-2 USG2200 系列产品后面板



1. MIC1/DMIC1 插槽
2. MIC2/DMIC2 插槽
3. MIC3 插槽
4. MIC4 插槽
5. FIC5/DFIC5 插槽
6. FIC6 插槽
7. 槽位标识
8. 接地端子

USG2210 分为普通配置和交流基本配置，普通配置为整机无扩展接口卡，交流基本配置为整机标配 2 个 5FSW 接口卡，后面板如图 4-3 所示。

USG2220/2230/2250/2260 分为普通配置和交流基本配置，普通配置为整机无扩展接口卡，交流基本配置为整机标配 2 个 1GE 接口卡，后面板如图 4-4 所示。

图4-3 USG2210 基本配置型产品后面板

图4-4 USG2220/2230/2250/2260 基本配置型产品后面板

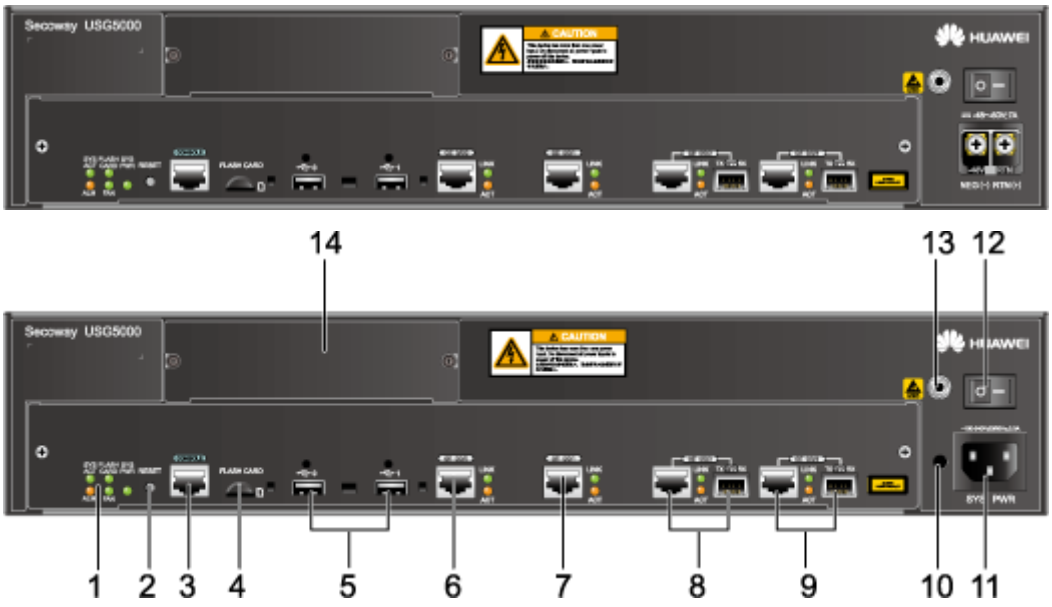
4.1.2 USG5100 系列产品外观

USG5100 系列产品包含 USG5120、USG5150 以及 USG5160。均由一体化机箱、扩展接口卡组成。

- USG5120 有交流和直流两种机型。提供了 4 个 MIC 和 4 个 FIC 槽位，为 2U 高设备。USG5120 电源和风扇固定在设备中，不支持热插拔。
- USG5150 电源可使用两个直流模块或两个交流模块，形成电源的负载分担。提供了 4 个 MIC 槽位和 6 个 FIC 槽位，为 3U 高设备。USG5150 的电源和风扇均支持热插拔。
- USG5160 只有交流机型，可使用两个交流模块，形成电源的负载分担。提供了 4 个 MIC 槽位和 6 个 FIC 槽位，为 3U 高设备。USG5160 的电源和风扇均支持热插拔。

USG5120 产品前面板

图4-5 USG5120 产品交流和直流前面板



1. 指示灯	2. 系统复位键	3. Console 接口	4. Micro-SD 卡插槽
5. USB 接口	6. 10/100/1000M 以太网接口 0	7. 10/100/1000M 以太网接口 1	8. GE Combo 接口 2
9. GE Combo 接口 3	10. 卡扣插孔	11. 电源插座	12. 电源开关
13. 防静电手腕带插孔	14. 防尘面板		

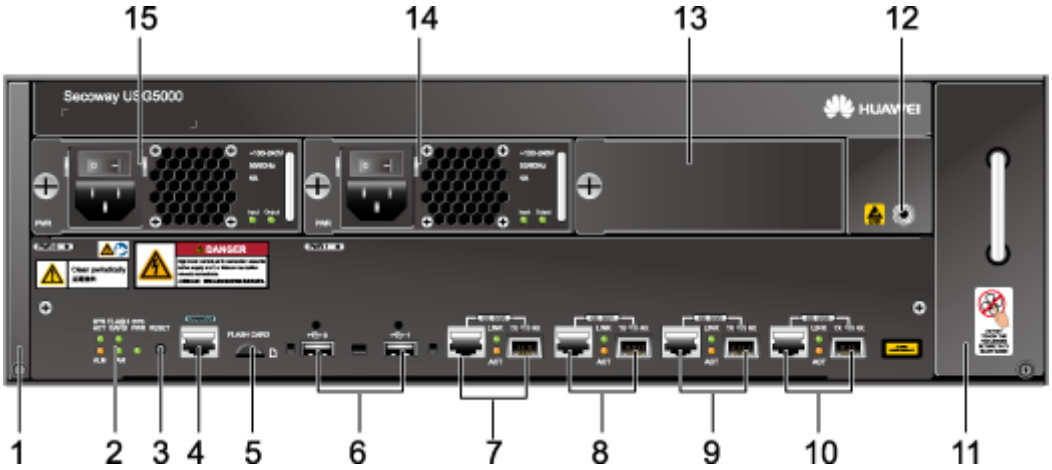
USG5120 产品后面板

图4-6 USG5120 产品后面板

1. MIC1/DMIC1 插槽
2. MIC2/DMIC2 插槽
3. MIC3 插槽
4. MIC4 插槽
5. FIC5/DFIC5 插槽
6. FIC6/DFIC6 插槽
7. FIC7/DFIC7 插槽
8. FIC8 插槽
9. 槽位标识
10. 接地端子

USG5150/5160 产品前面板（USG5160 无直流机型）

图4-7 USG5150/5160 产品前面板

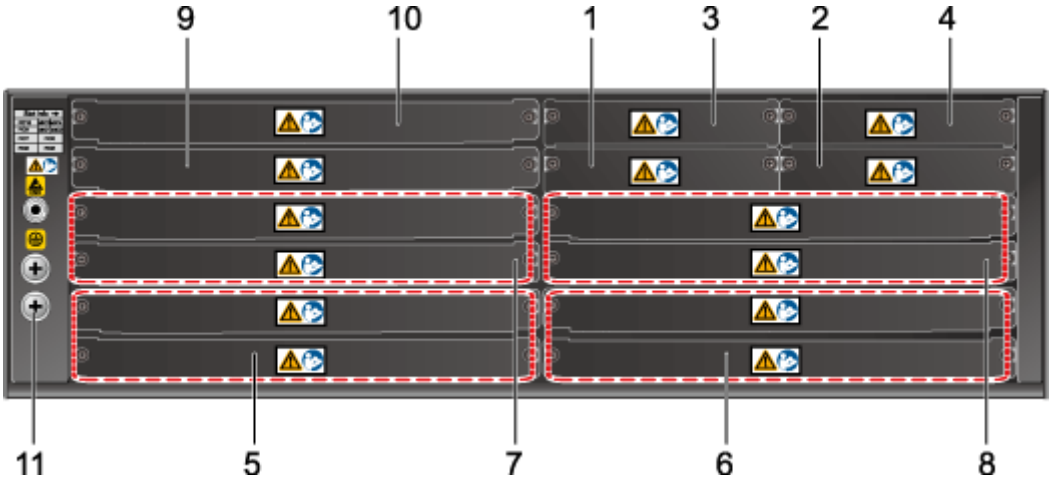


1 .防尘网	2. 指示灯	3. 系统复位键
4. Console 接口	5. 闪存接口	6. USB 接口
7. GE Combo 接口 0	8. GE Combo 接口 1	9. GE Combo 接口 2
10. GE Combo 接口 3	11. 风扇框	12. 防静电手腕带插孔

13. 防尘挡板	14. 电源模块 1	15. 电源模块 0

USG5150/5160 产品后面板

图4-8 USG5150/5160 产品后面板



1. MIC1/DMIC1 插槽	2. MIC2/DMIC2 插槽	3. MIC3 插槽	4. MIC4 插槽
5. FIC5/DFIC5 插槽	6. FIC6/DFIC6 插槽	7. FIC7/DFIC7 插槽	8. FIC8/DFIC8 插槽
9. FIC9 插槽	10. FIC10 插槽	11. 接地端子	

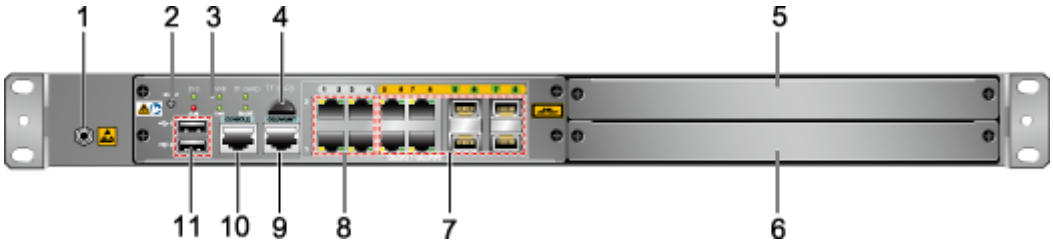
4.1.3 USG5500 系列产品外观

USG5500 系列包含 USG5530S、USG5530、USG5550、USG5560，均由一体化机箱、扩展接口卡组成。其中 USG5530S、USG5530 只有交流型号，USG5550、USG5560 有交流和直流两种型号。USG5500 系列包含 USG5530S、USG5530、USG5550、USG5560，其中 USG5530S、USG5530、USG5550 只有交流型号，USG5560 有交流和直流两种型号。电源可使用两个直流模块或两个交流模块，形成电源的负载分担。电源和风扇均支持热插拔。

USG5530S 前面板

USG5530S 前面板如图 4-9 所示。

图4-9 1U 设备前面板

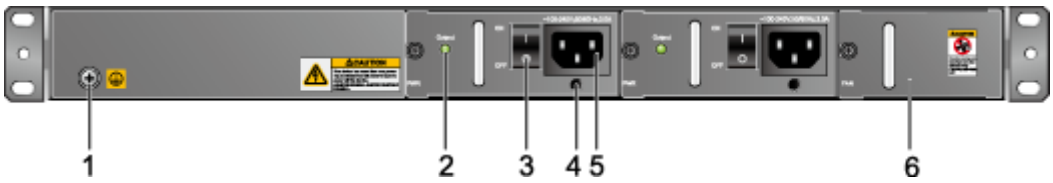


1.防静电手腕带插孔	2.系统复位键	3.指示灯
4.Micro-SD 卡插槽（暂不支持）	5.FIC2 插槽	6.FIC1/DFIC1 插槽
7.GE Comno 接口	8.10/100/1000M 以太网电接口	9.带外管理口
10.Console 接口	11.USB 2.0 接口	

USG5530S 后面板

USG5530S 的后面板如图 4-10 所示。

图4-10 1U 设备后面板

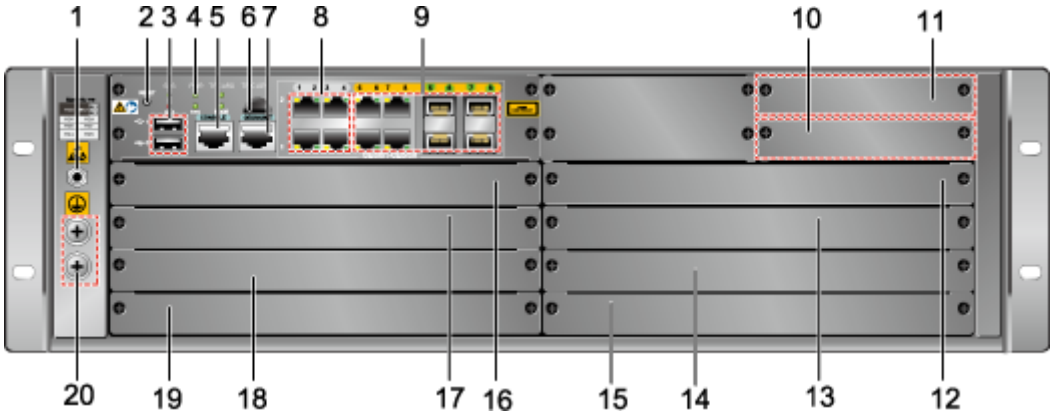


1.接地端子	2.电源指示灯	3.电源开关
4.交流电源线扎线孔	5.电源接口	6.风扇框

USG5530/5550/5560 前面板

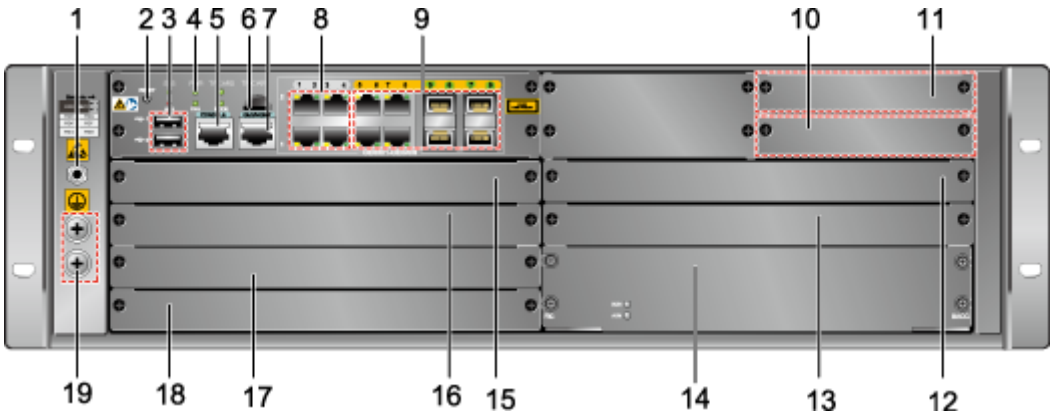
USG5530/5550/5560 前面板如图 4-11、图 4-12 和图 4-13 所示。

图4-11 USG5530 前面板



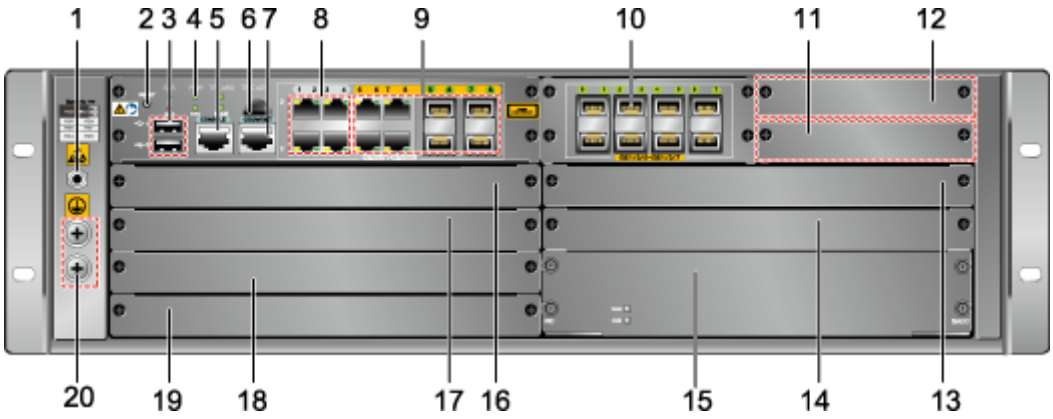
1. 防静电手腕带插孔	2. 系统复位键	3. USB 2.0 接口
4. 指示灯区域	5. Console 接口	6. Micro-SD 卡插槽（暂不支持）
7. 管理口	8. 10/100/1000M 自适应以太网电接口	9. GE Comno 接口
10. MIC2/DMIC2 插槽	11. MIC3 插槽	12. FIC9 插槽
13. FIC7/DFIC7 插槽	14. 假面板	15. FIC5/DFIC5 插槽
16. FIC8 插槽	17. FIC6/DFIC6 插槽	18. 假面板
19. FIC4/DFIC4 插槽	20. 接地端子	

图4-12 USG5550 前面板



1. 防静电手腕带插孔	2. 系统复位键	3. USB 2.0 接口
4. 指示灯区域	5. Console 接口	6. Micro-SD 卡插槽（暂不支持）
7. 管理口	8. 10/100/1000M 自适应以太网电接口	9. GE Comno 接口
10. MIC2/DMIC2 插槽	11. MIC3 插槽	12. FIC9 插槽
13. FIC7/DFIC7 插槽	14. FPGA 加速卡	15. FIC8 插槽
16. FIC6/DFIC6 插槽	17. 假面板	18. FIC4/DFIC4 插槽
19. 接地端子		

图4-13 USG5560 前面板



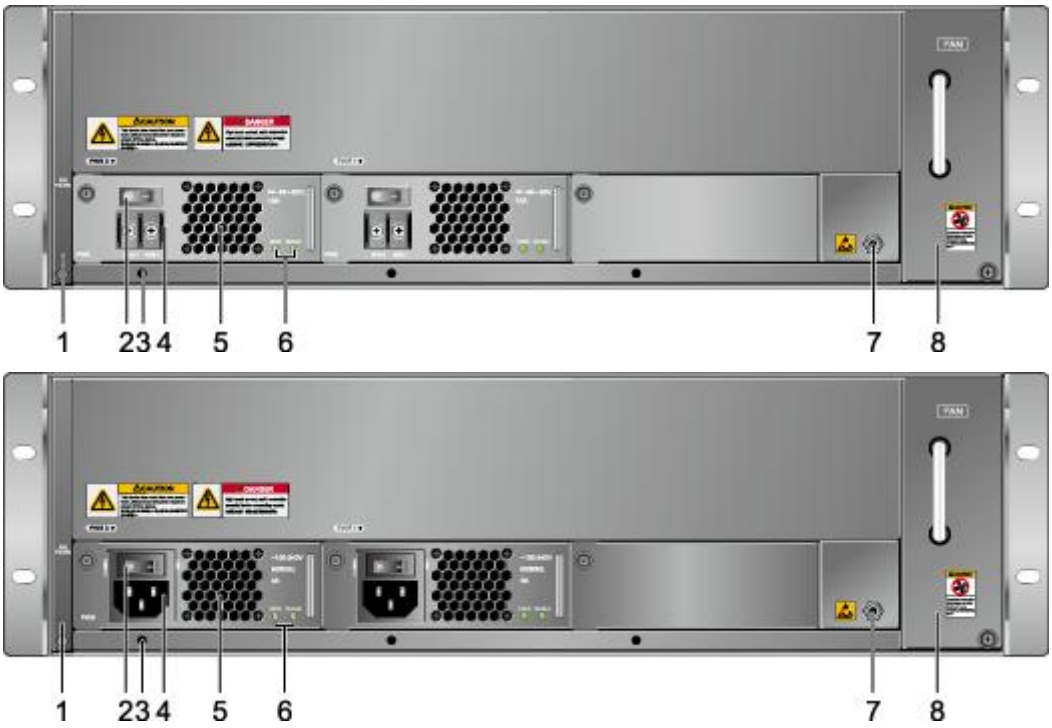
1. 防静电手腕带插孔	2. 系统复位键	3. USB 2.0 接口
4. 指示灯区域	5. Console 接口	6. Micro-SD 卡插槽（暂不支持）
7. 管理口	8. 10/100/1000M 自适应以太网电接口	9. GE Comno 接口
10. 100/1000M 以太网光接口	11. MIC2/DMIC2 插槽	12. MIC3 插槽
13. FIC9 插槽	14. FIC7/DFIC7 插槽	15. FPGA 加速卡
16. FIC8 插槽	17. FIC6/DFIC6 插槽	18. 假面板
19. FIC4/DFIC4 插槽	20. 接地端子	

USG5530/5550/5560 电源侧面板

USG5530/5550/5560 的后面板如图 4-14 所示。上图为直流机型，下图为交流机型。

说明
USG5530 和 USG5550 不支持直流电源。

图4-14 后面板



1.防尘网　2.电源开关　3.交流电源线扎线孔
4.电源接口　5.电源风扇网　6.电源指示灯
7.防静电手腕带插孔　8.风扇框

4.1.4 扩展接口卡和固定接口

USG 支持多种扩展接口卡，在丰富的固定接口的基础上提供了强大的接口扩展能力。具体如表 4-1、表 4-2、表 4-3 所示。

表4-1 固定接口

USG2210/2220/2230/2250/2260	USG5120	USG5150/5160	USG5530S/5530/5550	USG5560
• 2 个千兆 Combo 口（WAN 口）	• 2 个千兆电口（WAN 口）	• 2 个千兆电口（WAN 口）	• 1 个 Console 接口	• 1 个 Console 接口

USG2210/2220/2230/2250/2260	USG5120	USG5150/5160	USG5530S/5530/5550	USG5560
• 1 个 Console 口 • 2 个 USB 接口 • 1 个 Micro-SD 卡插槽	• 2 个千兆 Combo 口（WAN 口） • 1 个 Console 口 • 2 个 USB 接口 • 1 个 Micro-SD 卡插槽	• 4 个千兆 Combo 口（WAN 口） • 1 个 Console 口 • 2 个 USB 接口 • 1 个 Micro-SD 卡插槽	• 1 个 10/100/1000M 带外管理口 • 2 个 USB 接口 • 4 个 10/100/1000M 以太网电接口 • 4 个 GE Combo 口	• 1 个 10/100/1000M 带外管理口 • 2 个 USB 接口 • 4 个 10/100/1000M 以太网电接口 • 4 个 GE Combo 口 • 8 个 100/1000M 以太网光接口

表4-2 USG2200/5100 扩展接口卡

类型	接口卡	接口说明	备注
MIC	1E1 接口卡	1 个 E1 接口	-
MIC	1CE1 接口卡	1 个 CE1 接口	-
MIC	1ADSL2+接口卡	1 个 ADSL2+接口	主要应用于不对称速率传输。
MIC	1FE 接口卡	1 个 10/100M 以太网自协商电接口	-
MIC	5ESW 接口卡 5FSW 接口卡	5 个 10/100M 以太网自协商电接口	-
MIC	1SA 接口卡	1 个同异步串口	-
MIC	1G.SHDSL 接口卡	1 个 G.SHDSL 接口	-
MIC	2G.SHDSL 接口卡	2 个 G.SHDSL 接口	-
MIC	4G.SHDSL	4 个 G.SHDSL 接口	-

类型	接口卡	接口说明	备注
	接口卡		
MIC	1SA 接口卡	2 个同异步串口	-
MIC	MIC-3G-WCDMA 接口卡	提供支持 WCDMA 标准的 3G 接口，无连接线缆。	设备在同一时间只能使用 1 个 3G 接口卡（包括 USB-3G 接口卡和 MIC-3G 接口卡），请根据网络环境选购。
MIC	MIC-3G-CDMA2000 接口卡	提供支持 CDMA2000 标准的 3G 接口，无连接线缆。	
MIC	MIC-3G-TD-SCDMA 接口卡	提供支持 TD-SCDMA 标准的 3G 接口，无连接线缆。	
MIC	WiFi 接口卡	WLAN 接口，用户无线接入	-
DMIC	8FE+2GE 接口卡	8 个 10M/100M 以太网自协商电接口和 2 个 10M/100M/1000M 电接口	-
FIC	2E1 接口卡	2 个 E1 接口	-
FIC	2CE1 接口卡	2 个 CE1 接口	-
FIC	4E1 接口卡	4 个 E1 接口	-
FIC	4CE1 接口卡	4 个 CE1 接口	-
FIC	8E1 接口卡	8 个 E1 接口	-
FIC	8CE1 接口卡	8 个 CE1 接口	-
FIC	1GE 接口卡	1 个 10M/100M/1000M 自协商电接口	-
FIC	4GE 接口卡	4 个 10M/100M/1000M 自协商电接口	-
FIC	2FE+2FE Combo 接口卡	2 个 10M/100M 自协商电接口和 2 个 10M/100MGE Combo 口	-
FIC	电 Bypass 接口卡（USG2200 不支持该接口卡）	4 个 10/100/1000M 自适应以太网电接口	设备出现故障或下电时，流量可以绕过 USG5100 两端的设备实现直接对接。

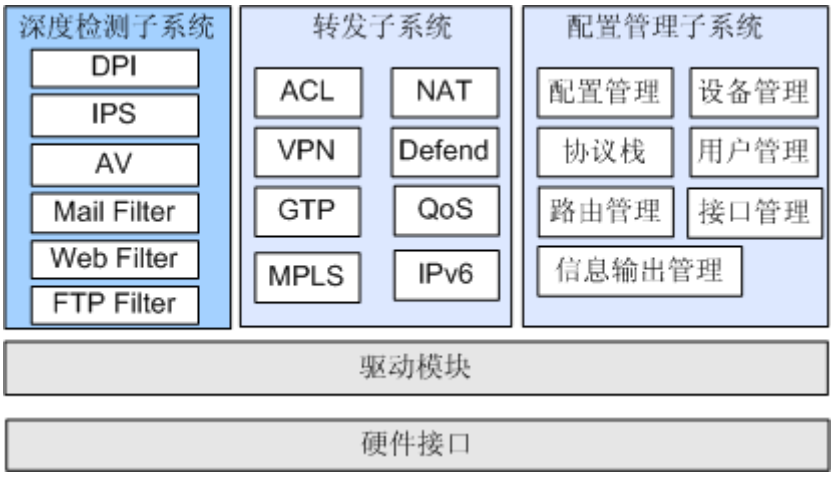
类型	接口卡	接口说明	备注
FIC	加密卡	-	不提供接口，为 IPSec VPN 提供高性能协议处理能力
DFIC	18FE+2SFP 接口卡	16 个 10/100/1000M 自适应以太网电接口和 4 个千兆以太网光接口	二层卡。
DFIC	16GE+4SFP 接口卡	18 个 10/100M 自适应以太网电接口和 2 个千兆以太网光接口	二层卡。
USB	USB-3G-E180 卡	-	制式：WCDMA
USB	USB-3G-EC169/EC169C 卡	-	制式：CDMA2000
USB	USB-3G-ET128/ET128-2 卡	-	制式：TD-SCDMA

表4-3 USG5500 扩展接口卡

接口卡类型	接口卡	接口	说明
FIC	2×10GE 光接口卡	2 个万兆光接口	-
FIC	2×10GE 光口+8GE 电口接口卡	8 个 10/100/1000M 自适应以太网电接口和 2 个万兆以太网光接口	-
FIC	8×GE 电接口卡	8 个 10/100/1000M 自适应以太网电接口	-
FIC	4×GE 电 BYPASS 接口卡	4 个 10/100/1000M 以太网电接口	设备出现故障或下电时，流量可以绕过 USG5500，使得 USG5500 两端的设备实现直接对接。
FIC	光 BYPASS 接口卡	一块光 Bypass 接口卡含 2 个 Bypass 链路插卡，一个 Bypass 链路插卡上有 4 个光接口	Bypass 链路插卡可处于工作回路和保护回路两种状态。处于工作回路状态时，将上行设备的流量引到 USG5500 处理，处理完成后再将流

接口卡类型	接口卡	接口	说明
			量引到下行设备；当处于保护回路状态时，将USG5500的上下行设备直接连接。
FIC	8×GE光接口卡	8个千兆光接口	-
FIC	加密卡	-	不提供接口，为IPSec VPN提供高性能协议处理能力
DFIC	16×GE电口+4×GE光接口卡	16个10/100/1000M自适应以太网电接口和4个千兆以太网光接口	二层卡。
DFIC	18×FE电口+2×GE光接口卡	18个10/100M自适应以太网电接口和2个千兆以太网光接口	二层卡。
DFIC	FPGA加速卡	-	加速报文转发，非首包的部分报文无需经过CPU处理，直接由FPGA加速卡转发。 说明 USG5530S/5530不支持FPGA加速卡，USG5550/5560支持且标配。
DMIC	2×10GE光接口卡	2个万兆光接口	说明 DMIC接口卡只能插放在MIC2/DMIC2插槽，同时需要将MIC3插槽的假面板取下。
USB	USB-3G-E180卡	-	制式：WCDMA
USB	USB-3G-EC169/EC169C卡	-	制式：CDMA2000
USB	USB-3G-ET128/ET128-2卡	-	制式：TD-SCDMA

4.2 软件结构



深度检测子系统

深度检测子系统对报文进行深入分析及检测，对应用层攻击进行检测并防御。实现的主要功能是：DPI 检测的应用层协议控制、IPS 入侵防御、AV 反病毒、邮件过滤、Web 过滤、FTP 过滤。

转发子系统

转发子系统主要是完成对报文的转发处理，实现的主要功能有：黑名单、ACL（Access Control List）对报文进行访问控制、NAT（Network Address Translation）、VPN（Virtual Private Network）、攻击防范、分片处理、GTP、MPLS、IPv6。

配置管理子系统

实现配置管理子系统对整个系统进行支撑并与用户进行交互。提供了配置、测试、维护等接口。实现了配置管理、设备管理、文件系统管理、信息中心对日志和告警的管理、软件补丁管理、License 管理、路由管理。

驱动模块和硬件接口

提供软件和硬件进行连接的基本支撑。

5 业务特性

关于本章

5.1 产品功能列表

USG2200/5100/5500 系列产品支持的特性如表 5-1 所示。

表5-1 USG2200/5100/5500 系列产品支持的特性

分类	说明		USG2200	USG5100	USG5500
防火墙功能	ACL 和安全策略	• 支持一体化的安全策略 • 支持基本 ACL 和高级 ACL。	Y	Y	Y

分类	说明		USG2200	USG5100	USG5500
		• 支持基于时间段的 ACL。 • 支持基于 MAC 地址的 ACL。 • 支持硬件包过滤 ACL。 • 支持动态维护 ACL 规则。 • 支持黑名单、IP 和 MAC 地址绑定。 • 支持应用层过滤、提供状态检测。 • 提供端口映射机制。			
	NAT	• 地址转换（NAT 和 PAT）。 • 提供内部服务器。 • 端口级 NAT 服务器。 • 支持多种 NAT ALG。	Y	Y	Y
	攻击防范	• 防范多种 DoS 和 DDoS 攻击：SYN Flood、ICMP Flood、UDP Flood、HTTP Flood、SIP Flood、WinNuke、ICMP 重定向和不可达报文、Land、Smurf、Fraggle、IP Spoofing 等。 • 防范扫描窥探：包括地址扫描、端口扫描、IP 源站选路选项、IP 路由记录选项、时间戳、刺探路由。 • 畸形报文攻击：畸形 IP 分片报文、畸形 TCP 报文、超大 ICMP 报文、TearDrop、Ping Of Death。	Y	Y	Y
	TSM 联动	• 支持对终端用户的接入进行控制。 • 支持多种特权用户方式。 • 支持在设备上强制在线用户下线。 • 支持逃生功能。	Y	Y	Y
	支持虚拟防火墙		Y	Y	Y

分类	说明		USG2200	USG5100	USG5500
	支持 IDS 联动		Y	Y	Y
UTM	反病毒	• 支持对用 HTTP/SMTP/POP3 协议传输的文件进行病毒扫描。 • 支持病毒库升级，包括在线升级和本地升级。 • 支持病毒库版本回退。 • 支持全局病毒扫描开关和对不同协议的策略配置。	Y	Y	Y
	入侵防御	• 支持深度检测。 • 支持 IPS 签名库升级，包括在线升级和本地升级。 • 支持 IPS 签名库版本回退。 • 支持 IPS 策略定制。	Y	Y	Y
	Web 过滤	• 支持 Web 内容过滤 • 支持搜索引擎关键字过滤 • 支持对 HTTP 请求的 URL 过滤，达到精确管理上网行为。 • 支持配置黑白名单、预定义分类和自定义分类对 URL 过滤。 • 支持记录配置扩展名资源的 HTTP 访问日志。	Y	Y	Y
	邮件过滤	• 支持反垃圾邮件 • 支持邮件内容过滤	Y	Y	Y
	FTP 过滤	• 支持主动模式与被动模式 • 支持 FTP 命令过滤 • 支持 FTP 文件过滤 • 支持文件大小过滤 • 支持 FTP 审计	Y	Y	Y
	应用控制（DPI）	• 支持查询 DPI 知识库，知识库中包含丰富的协议特征。 • 支持对 DPI 知识库进行在线升级和本地升级。	Y	Y	Y

分类	说明		USG2200	USG5100	USG5500
		• 支持基于时间的控制策略，例如上班期间不允许使用 MSN、QQ 等，而下班时间可以使用。 • 支持按协议进行流量限制、连接数限制，有效实现游戏、股票、P2P 流量、IM 流量、VoIP 流量控制。			
MPLS&VPN	• 支持 BGP/MPLS IP VPN • 支持 L2TP VPN • 支持 IPSec VPN • 支持 GRE VPN • 支持 SSL VPN • 支持 CA 证书		Y	Y	Y
用户与认证	管理上网用户	• 支持用户分层分组管理。 • 支持用户认证范围控制。 • 支持本地认证、RADIUS 服务器认证、LDAP 服务器认证、AD 服务器认证、单点登录。	Y	Y	Y
	管理接入用户	• 支持 RADIUS 协议，提供 PAP 和 CHAP 验证方式。 • 支持提供 PPP、Login 登录用户认证。 • 支持本地认证。 • 支持多 ISP。	Y	Y	Y
接入	Ethernet	• 支持二层、三层以太网接口 • 支持二层、三层以太网接口之间互相切换 • 支持三层以太网子接口	Y	Y	Y
	Eth-Trunk	• 支持二层、三层 Eth-Trunk 接口 • 支持三层 Eth-Trunk 子接口	Y	Y	Y
	VLAN	• 支持 Vlanif 接口转发 • 支持 Access 端口	Y	Y	Y

分类	说明		USG2200	USG5100	USG5500
		• 支持 Trunk 端口 • 支持 Hybrid 端口			
	PPPoE	• PPPoE Client • PPPoE Server	Y	Y	Y
	链路聚合		Y	Y	Y
	DCC		Y	Y	Y
	HDLC		Y	Y	N
	端口隔离		Y	Y	Y
	MSTP		Y	Y	Y
	3G		Y	Y	Y
	WLAN		Y	Y	N
	SA		Y	Y	N
	E1/CE1		Y	Y	N
	ADSL2+		Y	Y	N
	SHDSL		Y	Y	N
	PPP/MP		Y	Y	不支持MP
IP 业务	ARP	• 静态 ARP • 动态 ARP • ARP 代理 • 免费 ARP	Y	Y	Y
	DNS	• 支持本地静态域名 • 支持 DNS Client • 支持 DNS 代理 • 支持 DDNS 动态域名服务	Y	Y	Y
	DHCP	• 支持 DHCP Server • 支持 DHCP Client • 支持 DHCP 中继 • 支持 DHCP Snooping	Y	Y	Y
	IP 单播策略路由		Y	Y	Y
	IPV6	• 支持 IPv6 PPPoE • 支持 IPv6 DNS	Y	Y	Y

分类	说明		USG2200	USG5100	USG5500
		• 支持 DHCPv6 • 支持 IPv6 over IPv4 隧道 • 支持 IPv4 over IPv6 隧道 • 支持 NAT64 • 支持 IPv6 ACL • 支持 IPv6 ASPF • 支持 IPv6 URPF • 支持 IPv6 QoS			
路由	IPv4 路由	• 支持静态路由 • 支持 RIP、OSPF、BGP、ISIS 等动态路由 • 支持路由策略和路由叠代	Y	Y	Y
	IPv6 路由	• 支持静态路由 • 支持 RIPng、OSPFv3、BGP4+、ISISv6 等动态路由 • 支持路由策略和路由叠代	Y	Y	Y
IP 组播	• 支持 IGMP、IGMP Snooping、PIM-DM、PIM-SM、MSDP • 支持静态组播		Y	Y	Y
维护和可靠性	多种维护手段和可靠性特性	• 支持端口镜像 • 支持远程抓包 • 支持双机热备份 • 支持负载均衡 • 支持 Link-Group • 支持电源 1+1 备份 • 支持硬件 Bypass 卡	Y（不支持硬件 Bypass 卡）	Y	Y
	多种升级方式	• FTP 方式升级 • TFTP 方式升级 • Web 方式升级 • BootROM 方式升级 • U 盘方式升级	Y	Y	Y
QoS 和流量限制	• 支持流量监管 • 支持流量整形 • 支持接口限速		Y	Y	Y

分类	说明		USG2200	USG5100	USG5500
	• 支持拥塞管理 • 支持拥塞避免 • 支持 HQoS（分层 QoS） • 支持基于 IP 的限流，包括每 IP 和所有 IP 整体限流，并支持保证带宽和闲时复用。				
系统管理	信息中心	• 对日志信息进行管理和输出 • 对告警信息进行管理和输出 • 对 Debug 信息进行管理和输出	Y	Y	Y
	SNMP	• 支持 Snmp v1 • 支持 Snmp v2c • 支持 Snmp v3	Y	Y	Y
	Web 管理	• 支持通过 HTTP 协议对设备进行 Web 管理 • 支持通过 HTTPS 协议对设备进行 Web 管理	Y	Y	Y
	NTP	• 支持 NTP 客户端/服务器服务方式 • 支持时钟对等体服务方式 • 支持 NTP 局域网广播服务方式 • 支持 NTP 组播服务方式 • 支持 NTP v3 协议，兼容 v2 和 v1 协议	Y	Y	Y
	Netstream		Y	Y	Y
	NQA		Y	Y	Y
	CWMP（TR-069）		Y	Y	N

5.2 防火墙特性

NAT

NAT 是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程。

- 地址转换

  主要用于实现内部网络（私有 IP 地址）访问外部网络（公有 IP 地址）的功能。通过应用 NAT，能够使多数的私有 IP 地址转换为少数的公有 IP 地址，减缓可用 IP 地址空间枯竭的速度。

  地址转换包括五种形式：

  - 支持基于地址池的 IP 地址转换。
  - 支持根据不同地址实施不同策略的地址转换。
  - 支持结合地址和端口（TCP/UDP 协议的端口信息）进行 PAT 转换（Port Address Translation）。
  - 支持根据 ACL 规则进行地址转换。
  - 支持端口级地址转换。

- NAT 内部服务器

  NAT 隐藏了内部网络的结构，具有“屏蔽”内部主机的作用，但是在实际应用中，可能需要提供给外部一个访问内部主机的机会，如提供给外部一台 WWW 的服务器，或是一台 FTP 服务器。使用 NAT 可以灵活地添加内部服务器。

  USG 系列的 NAT 能够为外部网络用户提供访问的内部服务器。外部用户访问内部服务器时，有如下两部分操作：

  - USG 系列将外部用户的请求报文的目的地址转换成内部服务器的私有地址。
  - USG 系列将内部服务器的回应报文的源地址（私网地址）转换成公网地址。

  USG 系列支持为外部用户提供多台同样的服务器，例如，提供多台 Web 服务器。

- 多种 NAT ALG

  对于一些特殊协议，例如 ICMP、FTP 等，它们报文的数据部分可能包含 IP 地址或端口信息，这些内容如果不能被 NAT 有效的转换，就可能导致问题。

  NAT 采用“注册”方式支持多种 NAT ALG（Application Level Gateway），包括：

  - 支持 FTP 协议的 NAT ALG。
  - 支持 H.323（包括 T.120、RAS、Q.931 和 H.245 等）协议的 NAT ALG。
  - 支持 ICQ 协议的 NAT ALG。
  - 支持 ILS(Internet Locator Service)协议的 NAT ALG。
  - 支持 RTSP（Real-Time Streaming Protocol）协议的 NAT ALG。
  - 支持 MGCP（Media Gateway Control Protocol）协议的 NAT ALG。
  - 支持 MMS（Multimedia Messaging Service）协议的 NAT ALG。
  - 支持 Microsoft 公司提供的 MSN 聊天会话的 NAT ALG。
  - 支持 PPTP（Point to Point Tunneling Protocol）协议的 NAT ALG。
  - 支持对腾讯公司的 QQ 聊天会话的 NAT ALG。
  - 支持 NBT（NetBIOS over TCP）协议的 NAT ALG。

- 支持 SIP（Session Initiation Protocol）协议的 NAT ALG。
- 支持 SQL.NET 协议的 NAT ALG。
- 支持自定义的 NAT ALG。

通过“注册”方式支持特殊协议，使软件有良好的扩充性，无需更改软件构架，很容易支持新的协议。

多种 ACL

ACL 是设备实现数据控制的重要手段，它可以应用到包过滤、NAT（Network Address Translation）、IPSec、QoS（Qulity of Service）、路由策略等功能中。路由设备为了过滤数据包，需要配置一系列的规则，以决定什么样的数据包能够通过，这些规则就是通过访问控制列表 ACL（Access Control List）定义的。

访问控制列表是由 permit/deny 语句组成的一系列有顺序的规则，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL 通过这些规则对数据包进行分类，这些规则应用到路由设备接口上，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

- 基本 ACL 可以根据源 IP 地址对报文进行访问控制。
- 高级 ACL 可以根据源 IP 地址、目的 IP 地址、源端口、目的端口、协议报文进行访问控制。
- 基于 MAC 的 ACL 可以根据源 MAC 地址、目的 MAC 地址、数据帧的类型和优先级对报文或二层以太网帧进行访问控制。

设备采用的快速流分类算法使系统在进行上万条 ACL 规则的查找时，性能基本不受影响，处理速度保持不变。

ASPF

ASPF（Application Specific Packet Filter）是针对应用层的包过滤，即基于状态的报文过滤，以便于实施内部网络的安全策略。ASPF 能够检测试图通过 USG 的应用层协议会话信息，阻止不符合规则的数据报文穿过。并提供对有害 Java Applets、有害 ActiveX 的阻断。

状态检测功能

状态检测是一种高级通信过滤。它检查应用层协议信息并且监控基于连接的应用层协议状态。对于所有连接，每一个连接状态信息都被监控并用于动态地决定数据包是否被允许通过设备或丢弃。

状态检测技术在网络层实现所有需要的安全能力，它既有包过滤机制的速度和灵活，也有代理型防火墙安全的优点。USG 利用最新的状态检测技术提供高速的安全防范和报文处理能力。

虚拟防火墙

USG 针对小型私有网络的特点，提出多实例解决方案。即将一台 USG 从逻辑上划分为多台虚拟防火墙，分别为多个小型私有网络提供独立的安全保障。对于网络运营商，可使用 USG 向外出租网络安全保障服务。

VPN 实例为虚拟防火墙提供相互隔离的 VPN 路由，VPN 实例与虚拟防火墙是一一对应的。目前，USG 支持 IPSec 多实例、L2TP 多实例、NAT 多实例、安全区域多实例、ACL 多实例、Session 多实例、黑名单多实例和路由多实例。

黑名单过滤恶意主机

USG 可以提供丢弃黑名单用户的所有报文来为用户提供安全保证。当 USG 根据报文的行为特征察觉到特定 IP 地址的用户的攻击企图后，主动将其加入黑名单表项，过滤从该 IP 地址发送的报文，从而保障网络安全。

USG 可以手工添加黑名单，可以动态地添加或删除黑名单，还可以将黑名单与 ACL 关联，即报文命中黑名单后，查找黑名单关联的 ACL 策略，如果命中 ACL 策略并且策略允许通过，则报文可以通过，否则报文被过滤丢弃。

黑名单仅对 IP 地址进行匹配，可以以很高的速度实现黑名单表项匹配，从而快速有效地屏蔽特定 IP 地址的用户。

IP 和 MAC 地址绑定

IP 地址和 MAC 地址绑定是避免 IP 地址假冒攻击的一种有效手段。

USG 可以配置 IP 地址和 MAC（Media Access Control）绑定，根据用户的配置，USG 在 IP 地址和 MAC 地址之间形成关联关系。

- 对于源 IP 地址与源 MAC 地址不匹配指定的关联关系的报文，将予以丢弃。
- 对于匹配目的 IP 地址的报文，USG 将该报文发送到关联关系中该 IP 地址对应的 MAC 地址。

强大的攻击防范能力

- 防范多种 DDoS 攻击

  USG 可以有效地检测出这些类攻击报文，通过丢弃这些报文等处理措施避免攻击行为，同时将这些攻击行为记录在日志中。目前，USG 可以防范多种 DDoS 攻击，主要包括：SYN Flood 攻击、ICMP Flood 攻击、SIP Flood 攻击、UDP Flood 攻击、tcp-illegal-session 攻击、HTTP Flood 攻击、Land 攻击、Smurf 攻击、Fraggle 攻击、WinNuke 攻击、ICMP 重定向或不可达报文、TCP 报文标志位（如 ACK、SYN、FIN 等）不合法、Ping of Death 攻击、Tear Drop 攻击等。

- 防范扫描窥探攻击

  攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。USG 通过比较分析，可以灵活高效地检测出这类扫描窥探报文，从而预先避免后续的攻击行为。

- 防范其它攻击

  USG 除了可以有效防范多种 DDoS 攻击和扫描窥探外，还可以有效防范 IP Spoofing 攻击、带源路由选项的 IP 报文攻击、带路由记录选项的 IP 报文攻击、利用 tracert 工具窥探网络结构等其他攻击，确保系统访问权的安全。

GTP

USG 基于 UDP（User Datagram Protocol）协议实现 GTP 功能。USG 在 GPRS 网络中，可以部署在 Gn、Gp 和 Gi 接口上。

USG 主要有以下几种应用：

- 工作在 Gn 接口，过滤掉恶意报文，保证同一个 PLMN 内网元的安全。
- 工作在 Gp 接口，当一个 PLMN 网络与其他 PLMN 网络相连时，过滤掉来自其他 PLMN 网络的恶意报文，保证 PLMN 网络内网元的安全。
- 工作在 Gi 接口，当 PLMN 网络与外部 IP 网络相连时，过滤掉来自外部 IP 网络的恶意报文，保证 PLMN 网络内网元的安全。
- 对 GTP 计费溢出攻击进行防范。

5.3 UTM 功能

华为提供强大的安全服务中心，为 IPS 签名库、病毒库的在线升级提供了便利的方式。丰富的 IPS 签名库和病毒库使得 USG 能够有效的识别各种网络应用中存在威胁与漏洞，用户不必再担心含有恶意代码的网站、携带病毒的邮件、木马、后门、内部员工访问非法网站等问题，对用户机构中面临的各种网络安全威胁实现有效的保护。

AV 反病毒

USG 对最有可能携带病毒的 Web 访问流量、电子邮件流量进行全面扫描，经扫描确认无病毒后再转发。对多种压缩格式的压缩文件、加壳文件以及 email 中的附件都能进行全面的扫描，防止病毒传播。

可对使用 HTTP、SMTP、POP3、FTP 协议传输的文件进行病毒扫描。用户可根据网络部署特点，针对不同的协议，灵活配置不同的病毒扫描策略，如使能反病毒开关、配置响应方式、限制扫描文件大小、根据文件类型进行扫描等。发现病毒后能采用邮件宣告说明，Web 页面推送等手段有效通知用户。可将策略应用到特定的域间，减小全局扫描带来的性能消耗。

病毒库可以在线升级，用户可让 USG 在设定的时间点自主连接安全服务中心对病毒库进行自动升级，也可手动实时升级病毒库。对于 USG 无法连接到互联网上的安全服务中心的情况，用户可从安全服务中心获得病毒库的升级包，将升级包下载到 USG，再进行本地脱机升级。此外，病毒库还支持版本回退。

IPS 入侵防御

IPS 对网络上的流量进行状态监视，以深度分析报文的方式更准确全面地发现入侵，并根据策略对入侵进行响应。

对于承载在应用层中的数据，传统的防火墙功能并没有进行深入全面的检测。比如在网络应用中，HTTP 是应用广泛的协议，这类数据流占据了网络数据中很大的比例，同时也隐藏了许多的安全威胁，传统的防火墙功能很难做到非常有效的深入检查。IPS 实现了对这些数据的深入检测。可根据用户的设置，实现对入侵的及时阻断，有效保护内网的安全。同时 IPS 提供了事后审计功能，对入侵事件实时记录相关信息。

USG 的 IPS 功能可根据用户不同的应用场景定制使用不同的 IPS 策略，策略内容丰富，用户可根据所保护的网络的实际情况定制。

IPS 支持对 IP 报文碎片重组及 TCP 流重组功能，防止躲避 IPS 检测的攻击行为。对于运行在非知名端口的应用协议，IPS 能够有效识别，同时对这些数据进行相应的检测，提高了入侵的检测率。IPS 还支持协议异常分析，特征检测等，实现对蠕虫、木马、扫描及间谍软件等攻击行为的检测。用户还可以通过命令行和 Web 页面查看签名库所支持的检测攻击行为，查询到每一个攻击签名对应的攻击描述，对网络的影响程度等。

当 USG 串行部署在网络上时，IPS 功能也可以支持防护和告警两种工作模式。在防护模式下，签名的阻断动作才可以生效；告警模式下，签名的阻断动作无效，但会产生日志告警，可以在不对网络流量产生任何影响的情况下，协助用户分析网络流量中的入侵状态。

USG 的 IPS 对新发现的攻击响应迅速。IPS 签名库可以在线升级，用户可让 USG 在设定的时间点自主连接安全服务中心对 IPS 签名库进行自动升级，也可手动实时升级签名库。对于 USG 无法连接到互联网上的安全服务中心的情况，用户可从安全服务中心获得 IPS 签名库的升级包，将升级包下载到 USG，再进行本地脱机升级。此外，IPS 签名库还支持版本回退。

邮件过滤

- 反垃圾邮件（RBL 过滤）

  RBL 过滤通过本地黑白名单或第三方组织提供的动态更新的黑名单库，对垃圾邮件进行过滤。RBL 过滤只根据 SMTP 连接的源 IP 地址过滤 SMTP 传输的邮件。

- 邮件内容过滤

  邮件内容过滤在内网用户通过 Webmail 或 SMTP/POP3 客户端收发电子邮件时，对邮件地址、主题、正文、附件大小、附件名或附件类型等进行监控，防止数据泄漏或敏感信息传输。

Web 过滤

Web 过滤包括 URL 过滤、搜索引擎关键字过滤、Web 内容过滤。

- URL 过滤

  员工随意不受控地访问非法网站，不仅严重影响工作效率而且威胁企业网络安全。URL 过滤对用户的 URL 请求进行访问控制，允许或禁止用户访问某些网络资源，可以达到规范上网行为的目的。

  主要功能如下：

  - 支持本地 URL 黑白名单过滤，用户可自定义需要控制的 URL 列表。
  - 支持基于 URL 分类对 URL 进行过滤。先向安全服务中心进行分类查询，然后根据过滤策略进行过滤。
  - 支持细粒度的 URL 过滤策略设置，用户可按时间、IP 地址分类制定灵活的过滤策略。
  - 提供 URL 过滤的豁免 IP 列表，可以指定某些 IP 可以不进行 URL 过滤，直接放行，满足部分特权用户的需求。
  - 支持 URL 分类、用户组、时间对象绑定访问策略，对 URL 请求进行访问控制。

- 阻断 URL 时，支持页面推送，用户可自定义该通知页面。
- 支持对 URL 访问请求进行审计，即记录原始的 URL 请求、记录访问者 IP 地址、访问时间。USG 在 elog 日志服务器上进行审计，并对审计内容进行分析，能够查看到经过设备访问最多的 TOP N 的网站，以及访问频繁的 TOP N 用户等。

- 搜索引擎关键字过滤

  对指定搜索引擎中的关键字进行过滤，目前支撑的搜索引擎有 Google、Yahoo、Bing、百度。当内网用户在这些搜索引擎上搜索 Internet 上的内容时，管理员通过在 USG 上配置关键字过滤功能，防止用户访问匹配这些关键字的内容。

- Web 内容过滤

  Web 内容过滤可以对 HTTP 协议传输的 Web 页面内容进行控制，可以控制的项目包括：

  - Web 页面关键字过滤：过滤 Web 页面上的文本。
  - 论坛发贴内容关键字过滤：过滤内网用户在 BBS、论坛发贴文本。
  - Web 页面中包含文件（如图形、视频等）的文件名过滤：过滤上传或下载文件的名称。
  - Web 页面中包含文件（如图形、视频等）的文件类型过滤：过滤上传或下载文件的扩展名。
  - 文件大小过滤：对基于 HTTP 协议的上传或下载的文件大小过滤。

FTP 过滤

FTP 文件传输是网络信息共享非常重要的内容，如果 FTP 操作和通过 FTP 上传/下载的文件不受控，那么内网会存在较多的不可控威胁，通过 FTP 过滤，可以对 FTP 操作（上传、下载、删除）、上传/下载的文件名、文件类型、文件大小进行控制。

深度检测过载保护

USG 可以通过开启或关闭深度检测过载保护功能实现业务优先和安全优先。开启时，当经过 UTM 模块的流量超过其处理能力时，这些流量不经 UTM 处理就放行。关闭后，当经过 UTM 模块的流量超过其处理能力，超过处理能力的流量被丢弃，最大限度保证了安全。

应用控制（DPI）

USG 通过 DPI（Deep Packet Inspection）技术对数据流进行深度检测，识别出应用层协议，并对指定类型的数据流量进行控制。USG 通过分析收到的数据包并和 DPI 特征库进行比对，对游戏、股票、P2P、IM、VoIP 等类型的网络数据流量进行分类，并对不同类型的协议进行相应的控制。

- 支持查询 DPI 知识库，知识库中包含丰富的协议特征。
- 支持对 DPI 知识库进行在线升级和本地升级。
- 支持基于时间的控制策略，例如工作期间不允许使用 MSN、QQ 等，而下班时间可以使用。
- 游戏、股票、P2P 流量、IM 流量、VoIP 流量控制。

- 支持用户自定义规则实现对特定 IP 的游戏、股票、P2P 访问权限的控制（允许或禁止）。

5.4 MPLS 与 VPN 特性

L2TP

USG 系列支持使用 L2TP（Layer Two Tunneling Protocol）协议构建 VPDN（Virtual Private Dial Network），利用公共网络（如 ISDN 和 PSTN）的拨号功能及接入网来实现虚拟专用网，为企业、小型 ISP、移动办公人员提供接入服务。

USG 系列支持作为 LNS（L2TP Network Server）和 LAC（L2TP Access Concentrator）设备。

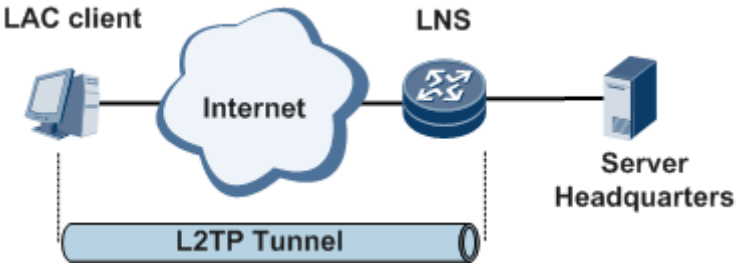
USG 支持使用 L2TP（Layer Two Tunneling Protocol）协议构建 VPDN（Virtual Private Dial Network），利用公共网络（如 ISDN 和 PSTN）的拨号功能及接入网来实现虚拟专用网，为企业、小型 ISP、移动办公人员提供接入服务。

USG 支持作为 LNS 和 LAC 设备，支持以下三种典型的隧道模式：

图5-1 NAS-Initialized 方式的 L2TP 隧道示意图

如图 5-1 所示，远端系统通过 PSTN/ISDN 拨入 LAC，由 LAC（NAS）通过 Internet 向 LNS 发起建立隧道连接请求。由 LNS 为拨号用户分配私有 IP 地址，对远程拨号用户的验证既可由 LAC 侧的代理完成，也可在 LNS 完成。

图5-2 Client-Initialized 方式的 L2TP 隧道示意图



如图 5-2 所示，LAC 客户可直接向 LNS 发起隧道连接请求，无需再经过一个单独的 LAC 设备。在 LNS 设备上收到了 LAC 客户的请求之后，根据用户名、密码进行验证，并且为 LAC 客户分配私有 IP 地址。

LAC 自主拨号方式：用户通过配置命令触发建立 LAC 与 LNS 之间的永久性 L2TP 会话。LAC 使用存储在本地的用户名通过虚模板接口和 LNS 建立一个永久存在的 L2TP 隧道，此时的 L2TP 隧道就想当于一个物理连接，出接口是虚模板接口。用户与 LAC 之间的连接就不受限于 PPP 连接，而只要是一个 IP 连接即可，这样 LAC 能够将用户的 IP 报文转发到 LNS。

IPSec

IPSec 协议族是 IETF 制定的一系列协议，它为 IP 报文提供了高质量的、可互操作的、基于密码学的安全保护机制。特定的通信双方在 IP 层通过加密与数据源验证等方式，保证报文在网络中传输时的私有性、完整性、真实性和防重放。

USG 可以通过硬件加密提供 IPSec 安全机制，为通信双方提供访问控制、完整性、数据来源认证、防重放、加密以及对数据流分类加密等服务。通过 AH（Authentication Header）和 ESP（Encapsulating Security Payload）这两个安全协议来实现对 IP 数据报或上层协议的保护，支持传输和隧道两种封装模式，如图 5-3 所示。

图5-3 IPSec 隧道示意图

USG 还支持使用 IKEv2 协议进行 IPSec 隧道协商。IKEv2 协议保留了 IKE 的基本功能，并针对 IKE 研究过程中发现的问题进行修订。同时兼顾简洁性、高效性、安全性和健壮性的需要，整合了 IKE 的相关文档，由 RFC 4306 单个文档替代。通过核心功能和默认密码算法的最小化规定，新协议极大地提高了不同 IPSec VPN 系统的互操作性。

IKEv2 与传统 IKE 相比有以下优点：

- 用 4 条消息就可以完成一个 IKE SA 和一对 IPSec SA 的协商建立，提高了协商效率。
- 删除了原有协议中的 DOI、SIT 以及域名标识符、提交位这些功能不强且难以理解、容易混淆的数据结构。
- 修复了多处公认的密码学方面的安全漏洞，提高了安全性能。
- 定义了独立的通讯量选择载荷，分担了原有 ID 载荷的部分功能，增加了协议灵活性。
- 加入对 EAP 身份认证方式的支持，提高了认证方式的灵活性和可扩展性。

USG 的 IPSec 支持 CA 证书。

USG 不仅可以通过 IPSec 为用户提供高可靠的安全传输通道，而且还支持 IPSec 结合 L2TP 和 GRE 构建多种 VPN 应用：

- L2TP over IPSec VPN
- GRE over IPSec VPN

GRE

USG 系列支持使用通用路由封装 GRE（Generic Routing Encapsulation）协议对某些网络层协议的数据报进行封装，使这些被封装的报文能够在另一网络层协议中传输。

GRE 可以作为 VPN 的第三层隧道协议，在协议层之间采用了 Tunnel 技术。Tunnel 是一个虚拟的点对点的连接，在实际中可以看成仅支持点对点连接的虚拟接口，这个接口提供了一条通路使封装的数据报能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报进行封装及解封装。

USG 支持使用通用路由封装 GRE（Generic Routing Encapsulation）协议对某些网络层协议的数据报进行封装，使这些被封装的报文能够在另一网络层协议中传输。

SSL VPN

- 虚拟网关

  在 USG 系列中，SSL VPN 功能模块建立的通道称为虚拟网关。USG 系列通过虚拟网关为用户提供 SSL VPN 服务。USG 系列作为一个物理实体，可以通过虚拟网关技术虚拟为多个逻辑上独立的网关，各虚拟网关的配置和提供的服务互相独立，以提供给多个企业或者一个企业的多个部门使用。

  比如，某个大型企业有多个部门，每个部门有各自的员工，部门间能够访问的资源和服务也各不相同，每个部门有自己的访问控制规则。在这种情况下，可以为每个部门分配一个虚拟网关，每个虚拟网关都是独立可管理的，可以配置各自的用户、资源和策略规则，形成独立的访问体系。而每个部门的感觉就像各自在使用一个独立的网关一样高效、安全。

  虚拟网关按照 IP 地址和域名的分配情况分为独占型和共享型。独占型虚拟网关独占一个或多个 IP 地址和域名；多个共享型虚拟网关共享同一个 IP 地址，具有相同的父域名，通过子域名来区分各虚拟网关。

- Web 代理

  Web 代理提供外部客户端和内部局域网 Web 服务器通信中转功能，避免局域网 Web 服务器直接暴露给外网攻击者，为局域网 Web 服务器提供理想的安全保护。

  Web 代理是指通过 USG 系列可以安全的访问内网 Web 资源，包括 Webmail 和 Web 服务器，它将来自远端浏览器的页面请求（采用 HTTPS 协议）转发给内网 Web 服务器，然后将服务器的响应回传给终端用户。

  用户只要在 USG 系列的虚拟网关客户端 Web 页面上安装控件后即可访问 Web 资源。

- 网络扩展

  网络扩展功能通过建立 SSL（Secure Socket Layer）隧道，实现了对所有基于 IP 的内网业务的全面访问。用户远程访问内网资源就像访问本地局域网一样方便，适用于各种复杂的业务功能。

  网络扩展提供了两种使用方式，用户可以通过登录 USG 系列客户端页面，安装 ActiveX 控件启用网络扩展服务，或者下载安装独立的网络扩展客户端软件。

  网络扩展支持三种访问模式：

  - 全路由模式

    用户只与 USG 系列建立网络连接，只能对企业内网进行访问。

  - 分离模式

用户不仅能够经过 USG 系列安全远程访问企业内网，同时也可以访问本地子网。

- 手动模式

  用户不仅能访问企业内网的特定资源、本地子网，还能访问 Internet 的各种资源。

- 端口转发

  端口转发业务是提供基于 TCP 的应用程序的安全接入，是一种非 Web 的应用方式。

  使用端口转发时，通过在客户端安装 ActiveX 控件来监听用户发起的 TCP 服务请求，控件将截获的数据流经 SSL 加密后传送给 USG 系列，由 USG 系列解密并解析后传送给相应的应用服务器。端口转发在应用层对用户访问进行控制，控制是否提供各种应用的服务，如：Telnet、远程桌面、FTP（File Transfer Protocol）、Email 等服务。

  USG 系列支持：

  - 单端口单服务器应用，如 MS RDP、Telnet、SSH、VNC（Virtual Network Computing）
  - 单端口多服务器应用，如 Lotus Notes
  - 动态端口应用，如 FTP、Oracle
  - 多端口应用，如 Email

- 文件共享

  文件共享的主要功能是将不同的文件服务器（如支持 SMB 协议的 Windows 系统、支持 NFS 协议的 Linux 系统）的共享资源以网页的形式提供给用户访问。

  用户直接通过浏览器就能在内网文件系统上创建和浏览目录，进行下载、上传、改名、删除等文件操作，就像对本机文件系统进行操作一样方便安全。

MPLS

MPLS 是一种结合了 IP 技术信令简单和 ATM 交换引擎高效的优势的新技术。MPLS VPN 可以将现有的 IP 网络分解成逻辑上隔离的虚拟网络，在 VPN、TE、QoS 等方面具有广泛的应用。

MPLS 域中参与 MPLS 转发的设备都需要配置 MPLS 基本能力。并且，只有配置了 MPLS 基本能力后，才能进行 MPLS 其他特性的配置。静态 LSP（Label Switched Path）不能使用标签发布协议动态建立，需要由管理员手工配置。配置静态 LSP 时，管理员需要为各 LSR 手工分配标签，需要遵循的原则是：前一节点出标签的值等于下一个节点入标签的值。

静态 LSP 上的各 LSR 之间不能相互感知整条 LSP 的情况，因此静态 LSP 是一个本地概念。

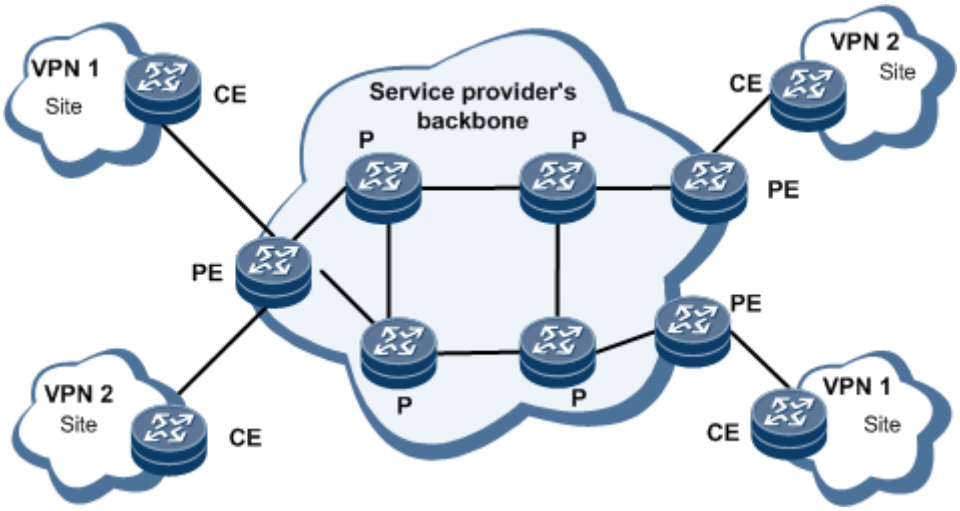
LDP 协议是创建动态 LSP 的一种方法。当不需要严格控制 LSP 建立的过程，且不需要在 MPLS 网络中部署流量工程时，建议采用 LDP 协议来创建 LSP。

BGP MPLS IP VPN

BGP/MPLS IP VPN 是提供商 VPN 解决方案 PPVPN（Provider Provisioned VPN）中一种基于 PE 的 L3VPN 技术。它使用 BGP 在服务提供商骨干网上发布 VPN 路由，使用 MPLS 在服务提供商骨干网上转发 VPN 报文。

BGP/MPLS IP VPN 组网方式灵活、可扩展性好，并能够方便地支持 MPLS QoS，因此得到越来越多的应用。

图5-4 L3VPN 隧道示意图



BGP/MPLS IP VPN 模型由三部分组成：CE、PE 和 P。

- CE（Customer Edge）：用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是 USG 或交换机，也可以是一台主机。通常情况下，CE“感知”不到 VPN 的存在，也不需要支持 MPLS。
- PE（Provider Edge）：服务提供商边缘设备，是服务提供商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。
- P（Provider）：服务提供商网络中的骨干设备，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。
- Site：指相互之间具备 IP 连通性的一组 IP 系统，并且这组 IP 系统的 IP 连通性不需通过服务提供商网络实现。Site 通过 CE 连接到服务提供商网络，一个 Site 可以包含多个 CE，但一个 CE 只属于一个 Site。

5.5 用户管理特性

上网用户管理

“上网用户”指通过 USG 设备访问资源的用户，包括内网主动发起上网行为的对象，如内网 PC，和从外网经 USG 访问内网资源的对象，如公司出差员工等 。

上网用户管理需要首先对公司的组织结构进行层级划分，将公司员工（用户）加入用户组，然后针对用户或用户组进行网络行为控制和审计，根据用户或用户组进行策略的可视化制定，提高策略制定的易用性，报表中体现用户信息，对用户进行上网行为分析，以达到对用户（而非单纯的 IP 地址）行为的追踪审计，解决现网应用中同一用户对应 IP 经常变化带来的应用行为策略控制难题。

上网用户管理功能支持用户或用户组的新建、删除、移动、修改、查询、导入导出、IP/MAC 帐号绑定、帐号有效期设置、别名、描述信息、状态设置等操作。

支持基于网段进行免认证、密码认证（本地或第三方服务器）和单点登录三种认证方式。免认证可以是 IP/MAC 绑定免认证，也可以是 IP 段自动创建临时用户。第三方服务器包括 RADIUS 服务器认证、LADP 服务器认证、AD 服务器，单点登录认证只支持 AD 服务器认证。

支持 AD 单点登录、Web 事前或会话认证、认证成功自动跳转、支持跳转到上次访问页面 支持 HTTP 和 HTTPS 两种认证方式、支持用户认证失败次数和失败锁定时间可配置、 支持在线用户老化时间可配置

管理员可对在线用户进行查看、激活、强制注销、冻结、解冻等操作。

接入用户管理

“接入用户”指 PPP 或隧道建立过程中使用的用户。USG 对这些用户提供本地认证、RADIUS 认证、HWTACACS 认证，可验证用户身份的合法性并为合法用户进行授权，防止非法用户进行访问。

管理员用户

“管理员用户”指通过 Telnet、SSH、web、FTP 等协议或通过 Console 接口访问设备并对设备进行配置或操作的用户。设备出厂时为 Telnet、web 和 Console 接口三种访问设备的方式提供默认管理员用户帐号 admin，密码 Admin@123。

5.6 可靠性特性

VRRP

USG 系列支持 VRRP（Virtual Router Redundancy Protocol）协议，基于虚拟 IP 地址形成备份组，网络内的主机把这个虚拟 IP 地址作为网关地址与其它网络进行通信。

双机热备份

USG 系列支持 HRP（Huawei Redundancy Protocol），此时一个备份组内包括一个主用设备和一个备用设备。HRP 协议负责在主/备 USG 设备之间备份关键配置命令和会话表、IPSec 协商 SA 状态信息等，从而确保主用 USG 出现故障时能由备份 USG 平滑地接替工作。

负载均衡

当一台服务器无法处理多个用户的访问时，可使用多台服务器分担网络流量。此时可以将 USG 系列部署在服务器所在网络的出口，用户只需访问一个 IP 地址，USG 系列按照配置的算法，将访问流量分配到不同的服务器上。这样不但可以分别利用各个服务器的处理能力，达到流量分担的目的，而且保障了服务器的可用性，得到最佳的网络扩展性。

USG 系列同时支持对服务器的健康性检查功能。

Link-Group

Link-group 的功能是将多个物理接口的状态相互绑定，组成一个逻辑组。如果组内任意接口因故障而状态变为 fault，系统将组内其它接口状态设置为 Down。当组内所有接口恢复正常后，整个组内的接口状态才重新被设置为 Up。

Bypass

USG5100、USG5500 支持专门设计的 Bypass 接口卡，在设备故障的时候或掉电的情况下，一对 Bypass 接口自动切换成直连，可以保证两个接口之间的业务正常进行。

5.7 完备的 QoS 机制

传统的网络服务采用尽力而为（Best-Effort）策略，无区分的处理所有报文，对分组转发的延迟、抖动、丢包率和可靠性等需求不提供任何承诺和保证。

随着网络技术的飞速发展和业务的逐渐多样化，新业务对网络的服务能力提出了更高的要求。这些新业务有一个共同特点，即对带宽、延迟、延迟抖动等传输性能有着特殊的需求。比如电视会议、视频点播需要高带宽、低延迟和低延迟抖动的保证。事务处理、Telnet 等关键任务虽然不一定要求高带宽，但非常注重低延迟，在拥塞发生时要求优先获得处理。新业务的不断涌现对 IP 网络的服务能力提出了更高的要求，用户已不再满足于能够简单地将报文送达目的地，而是还希望在投递过程中得到更好的服务，诸如支持为用户提供专用带宽、减少报文的丢失率、管理和避免网络拥塞、调控网络的流量、设置报文的优先级等。所有这些，都要求网络具备更为完善的服务能力。QoS 技术应运而生。

QoS 提供的主要的流量管理技术如下：

- 流量监管

  通过设置特定数据流的规格，对超出监管流量的数据包进行丢弃，防止突发大量数据流引发网络拥塞。

- 流量整形

  通过设置特定数据流的规格，对超出限制流量的数据包进行缓存，使这一流量的报文以比较均匀的速度向外发送。避免下游设备因为转发能力较差造成数据包丢失。

- 拥塞避免

  支持通过尾丢弃或 WRED 丢弃算法丢弃队列中的报文，防止队列溢出。

- 拥塞管理

提供 FIFO、CQ、PQ、WFQ 等队列调度算法，即可以保证调度的公平，又能确保高优先级的业务能够优先得到服务,可以满足多种业务组合的需求。完善的 QoS 机制满足未来对区分服务的建设要求。对不同的业务保证不同的延迟、抖动、带宽和丢包率，保证数据、语音等多种业务的开展，适应多业务承载 IP 网的发展要求。

- 接口限速

  接口限速采用令牌桶进行流量控制。如果在设备的某个端口上配置了端口限速功能，所有经由该端口发送的报文首先要经过 LR 的令牌桶进行处理。如果令牌桶中有足够的令牌，则报文可以发送；否则，报文将进入 QoS 队列进行拥塞管理。

- HQoS

  HQoS 是一种既能控制用户的流量，又能同时根据用户业务优先级进行调度的 QoS 技术。HQoS 弥补了传统 QoS 无法对接口上多个用户的多种业务流量进行多级区分服务的不足，在区分了用户的同时，还对用户的流量进行了业务区分。既提供了精细化的服务质量保证，又可以从整体上节约网络运维成本。

设备还支持基于 IP 地址的带宽和连接数限制功能，在域间对流量进行控制。起到优化网络流量、保证用户的正常访问速率、防范网络攻击的作用。

- 每 IP 限流

  对符合匹配条件的每个 IP 地址发起或接收的带宽、连接数进行限制。

- 整体 IP 限流

  对符合匹配条件的所有 IP 地址发起或接收的带宽总和或连接数总和进行整体限制。

5.8 IP 业务

ARP

ARP（Address Resolution Protocol）就是将一个 IP 地址映射到正确的 MAC 地址的地址解析机制。

局域网中每台主机或路由设备都有一个 32 位的 IP 地址，这个地址用于该主机的所有通信中。IP 地址的分配是独立于机器的硬件地址的。

而在以太网中，主机或路由设备是根据 48 位的 MAC（Medium Access Control）地址来发送、接收以太网数据帧的，这个 MAC 地址又称为物理地址或硬件地址，是制造设备时分配到以太网接口中的。因而，在实际的网络互联中，需要一种地址解析的机制来为这两种不同的地址形式提供映射。

IP 单播策略路由

IP 单播策略路由是一种依据用户制定的策略进行路由选择的机制。与单纯依照 IP 报文的目的地址查找路由表进行转发不同，USG 系列的策略路由支持基于到达报文的源地址、报文长度、用户(组)、应用协议分类等信息灵活地指定路由，可应用于安全、负载均衡等需求。支持 IPv4 和 IPv6 两种协议。

DHCP

DHCP 采用客户/服务器通信模式，由客户端向服务器提出配置申请（包括分配的 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回相应配置信息。

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复杂，经常出现计算机位置变化（如便携机或无线网络）和计算机数量超过可分配的 IP 地址的情况。动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）就是为满足这些需求而发展起来的。

USG 支持 DHCP 服务器、代理、客户端功能。通过配置 DHCP，与 USG 相连的计算机可快速、动态地获取它所需要的 IP 地址和所有配置信息，而不需要管理员手动为每台计算机指定。

DNS

TCP/IP 不仅提供了 IP 地址来确定设备，而且还专门设计了一种字符串形式的主机命名机制，这就是所谓的域名系统 DNS（Domain Name System）。此系统使用一种有层次的命名方式，为网上的设备指定一个有意义的名字，并且在网络上设置域名解析服务器，建立域名与 IP 地址的对应关系。

域名解析分为动态 DNS 解析和静态 DNS 解析。在解析域名时，可以首先采用静态解析的方法，如果静态解析不成功，再采用动态解析的方法。可以将一些常用的域名放入静态域名解析表中，这样可以提高域名解析效率。

USG 支持做 DNS Client 和 DNS Proxy。

DNS 仅仅提供了域名和 IP 地址之间的静态对应关系，当节点的 IP 地址发生变化时，DNS 无法动态地更新域名和 IP 地址的对应关系。此时，如果仍然使用域名访问该节点，通过域名解析得到的 IP 地址是错误的，从而导致访问失败。DDNS（Dynamic Domain Name System）用来动态更新 DNS 服务器上域名和 IP 地址之间的对应关系，保证通过域名解析到正确的 IP 地址。

NAT64

IPv4 网络在向 IPv6 网络迁移的过程中，NAT64 作为一种过渡技术，能够实现 IPv6 网络与 IPv4 网络的共存以及数据交互。

NAT64 的地址转换是 IPv6 传输地址（IPv6 地址与端口，简称 IPv6 传输地址）与 IPv4 传输地址（IPv4 地址与端口，简称 IPv4 传输地址）的转换。

NAT64 的协议转换机制包括对 IPv6 报文头与 IPv4 报文头的转换，也包括对 TCP、UDP、ICMP 的协议转换。

IPv6 over IPv4

在 IPv4 网络上用于连接 IPv6 孤岛的隧道，称为 IPv6 over IPv4 隧道。

在 IPv4 Internet 向 IPv6 Internet 过渡的初期，IPv4 网络已被大量部署，而 IPv6 网络只是散布在世界各地的一些孤岛。采用专用的线路将这些孤岛互连起来，显然是不经济的，通常的做法是采用隧道技术。利用隧道技术可在 IPv4 网络上创建隧道，从而实现 IPv6 孤岛的互连。这类似于在 IP 网络上利用隧道技术部署 VPN 的情况。

在 IPv4 网络上用于连接 IPv6 孤岛的隧道，称为 IPv6 over IPv4 隧道。为了实现 IPv6 over IPv4 隧道，需要在 IPv4 网络与 IPv6 网络交界的边界路由设备上启动 IPv4/IPv6 双协议栈。

IPv4 over IPv6

在 IPv6 网络上用于连接 IPv4 孤岛的隧道，称为 IPv4 over IPv6 隧道。

在 IPv4 Internet 向 IPv6 Internet 过渡的后期，IPv6 网络已被大量部署，此时可能出现 IPv4 孤岛。利用隧道技术可在 IPv6 网络上创建隧道，从而实现 IPv4 孤岛的互连。这类似于在 IP 网络上利用隧道技术部署 VPN。在 IPv6 网络上用于连接 IPv4 孤岛的隧道，称为 IPv4 over IPv6 隧道。

5.9 IPv4 与 IPv6 路由

静态路由

USG 系列支持用户手工配置到某一特定目的地的静态路由。

当网络结构比较简单时，只配置静态路由就可以使网络正常工作。设置和使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

静态路由的缺点在于：当网络发生故障或者拓扑发生变化后，静态路由不会自动改变，必须由管理员进行重新手工配置。

IPv6 静态路由与 IPv4 静态路由类似，也需要管理员手工配置，适合于一些结构比较简单的 IPv6 网络。

它们之间的主要区别是目的地址和下一跳地址有所不同，IPv6 静态路由是使用 IPv6 地址为下一跳，而 IPv4 静态路由则使用 IPv4 地址为下一跳。另外，目前仅 IPv4 静态路由支持 VPN 实例。

RIP

USG 系列支持配置 RIP（Routing Information Protocol）动态路由协议，指导报文的转发。

RIP 是一种较为简单的内部网关协议，基于距离矢量算法，通过 UDP 报文进行路由信息的交换，使用的端口号为 520。

RIP 使用跳数（Hop Count）来衡量到达目的地址的距离，称为度量值。在 RIP 中，路由器到与它直接相连的网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。

为限制收敛时间，RIP 规定度量值取 0～15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得 RIP 不可能在大型网络中得到应用。

为提高性能，RIP 支持设置报文的发送间隔和发送报文的最大数量；为防止产生路由循环，RIP 支持水平分割（Split Horizon）和毒性反转（Poison Reverse）功能。

RIP 实现较为简单，在配置和维护管理方面也远比 OSPF（Open Shortest Path First）和 IS-IS（Intermediate system to intermediate system）容易，因此在实际组网中仍有广泛的应用。用户可以根据实际的组网需求选择配置 RIP 来发现和生成路由信息。

RIPng

RIPng 又称为下一代 RIP 协议（RIP next generation），它是为了在 IPv6 网络应用 RIP 而对原来的 IPv4 网络中 RIP-2 协议的扩展和修改。大多数 RIP 的概念都可以用于 RIPng。

RIPng 协议是基于 D-V（Distance Vector，距离矢量）算法的路由协议。它通过 UDP 报文交换路由信息，使用的端口号为 521。RIPng 协议用跳数来衡量到达目的主机的距离，也称为度量值或开销。在 RIPng 协议中，从一个路由器到其直连网络的跳数为 0，而通过另一台路由器到达一个网络的跳数为 1，如此类推。当跳数大于或等于 16 时，目的网络或主机就被定义为不可达。

OSPF

OSPF 是 IETF（The Internet Engineering Task Force）组织开发的一个基于链路状态的内部网关协议。

OSPF 路由协议有如下几个特点：

- 适应范围广，支持各种规模的网络，最多可支持几百台设备。
- 快速收敛，在网络的拓扑结构发生变化后立即发送更新报文，将更新后的网络拓扑在自治系统中同步。
- 无自环，由于 OSPF 根据收集到的链路状态采用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分，允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。
- 等价路由，支持到同一目的地址的多条等价路由。
- 路由分级，使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。
- 支持验证，支持基于接口的报文验证，以保证报文交互的安全性。
- 组播发送，在某些类型的链路上以组播地址发送协议报文，减少对其他设备的干扰。

OSPF 适合于大中型网络。

OSPFv3

OSPFv3 是 OSPF 版本 3 的简称，主要提供对 IPv6 的支持，遵循的标准为 RFC2740（OSPF for IPv6）。大多数 OSPF 的概念都可以用于 OSPFv3。

OSPFv3 和 OSPFv2 在很多方面相同：

- Router ID，Area ID，LSA Link State ID 仍然是 32 位的。
- 相同类型的报文：Hello 报文、DD 报文、LSR 报文、LSU 报文和 LSAck 报文。
- 相同的邻居发现机制和邻接（Adjacency）形成机制。

- 相同的 LSA 扩散（Flooding）机制和老化（Aging）机制。
- 基本相同的 LSA 类型。

OSPFv3 和 OSPFv2 的不同包括：

- OSPFv3 是基于链路（Link）运行，OSPFv2 是基于网段（Network）运行。
- OSPFv3 在同一条链路上可以运行多个实例。
- OSPFv3 的拓扑关系和 IPv6 地址前缀没有关系。
- 使用 IPv6 的链路本地（Link-local）地址标识邻接的邻居。
- 新增的 3 种不同的 LSA 扩散范围。

BGP

BGP（Border Gateway Protocol）是一种自治系统间的动态路由发现协议，它的基本功能是在自治系统间自动交换无环路的路由信息，通过交换带有自治系统号（AS）序列属性的路径可达信息，来构造自治区域的拓扑图，从而消除路由环路并实施用户配置的路由策略。

与 OSPF 和 RIP 等在自治区域内部运行的协议对应，BGP 是一类 EGP（Exterior Gateway Protocol）协议，而 OSPF 和 RIP 等为 IGP（Interior Gateway Protocol）协议。BGP 协议经常用于 ISP 之间。

BGP 是一种外部路由协议，与 OSPF、RIP 等的内部路由协议不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最好的路由。

通过携带 AS 路径信息，可以彻底解决路由循环问题。

为控制路由的传播和路由选择，它为路由附带属性信息。

BGP4+

BGP4+是一种用于自治系统 AS（Autonomous System）之间的动态路由协议，它是对 BGP 的扩展。

传统的 BGP4 只能管理 IPv4 的路由信息，对于使用其它网络层协议（如 IPv6 等）的应用，在跨自治系统传播路由信息时就受到一定限制。

为了提供对多种网络层协议的支持，IETF 对 BGP4 进行了扩展，形成 BGP4+，目前的 BGP4+标准是 RFC2858（Multiprotocol Extensions for BGP-4，BGP-4 多协议扩展）。

为了实现对 IPv6 协议的支持，BGP4+需要将 IPv6 协议的信息反映到 NLRI（Network Layer Reachable Information）属性及 Next_Hop 属性中。

BGP4+中引入的两个 NLRI 属性分别是：

- MP_REACH_NLRI：Multiprotocol Reachable NLRI，多协议可达 NLRI。用于发布可达路由及下一跳信息。
- MP_UNREACH_NLRI：Multiprotocol Unreachable NLRI，多协议不可达 NLRI。用于撤销不可达路由。

BGP4+中的 Next_Hop 属性用 IPv6 地址来表示，可以是 IPv6 全球单播地址或者下一跳的链路本地地址。

在 BGP4+中，BGP 协议原有的消息机制和路由机制并没有改变。

IS-IS

IS-IS 最初是国际标准化组织 ISO（the International Organization for Standardization）为它的无连接网络协议 CLNP（ConnectionLess Network Protocol）设计的一种动态路由协议。

为了提供对 IP 的路由支持，IETF 在 RFC1195 中对 IS-IS 进行了扩充和修改，使它能够同时应用在 TCP/IP 和 OSI 环境中，称为集成化 IS-IS（Integrated IS-IS 或 Dual IS-IS）。

IS-IS 属于内部网关协议 IGP（Interior Gateway Protocol），用于自治系统内部。IS-IS 是一种链路状态协议，使用最短路径优先 SPF（Shortest Path First）算法进行路由计算，与 OSPF 协议有很多相似之处。

IETF 的 draft-ietf-isis-ipv6-05.txt 中规定了 IS-IS 为支持 IPv6 所新增的内容。主要是新添加的支持 IPv6 路由信息的两个 TLVs（Type-Length-Values）和一个新的 NLPID（Network Layer Protocol Identifier）。IS-IS 与 RIP 和 OSPF 不同，这两个协议 RIP 和 OSPF 有单独的版本 RIPng 和 OSPFv3 支持 IPv6。

TLV 是在 LSP（Link State PDUs）中的一个可变长字段值。新增的两个 TLV 分别是：

- IPv6 Reachability：

  类型为 236（0xEC），通过定义路由信息前缀、度量值等信息来说明网络的可达性。

- IPv6 Interface Address：

  类型为 232（0xE8），它相当于 IPv4 中的“IP Interface Address”TLV，只不过把原来的 32 比特的 IPv4 地址改为 128 比特的 IPv6 地址。

NLPID 是标识网络层协议报文的一个 8 比特字段，IPv6 的 NLPID 值为 142（0x8E）。如果 IS-IS 路由器支持 IPv6，那么向外发布 IPv6 路由时必须携带 NLPID 值。

路由策略

路由策略是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。

USG 系列在发布与接收路由信息时，可以实施一些策略，用来对路由信息进行过滤，例如只接收或发布满足一定条件的路由信息。另外，一种路由协议可能需要引入其它的路由协议发现的路由信息，同时引入的路由信息必须满足一定的条件，并对所引入的路由信息的某些属性进行设置，以使其满足本协议的要求。

在 USG 中，提供了访问控制列表、地址前缀列表、AS 路径过滤器、团体属性过滤器、扩展团体属性过滤器、RD 属性过滤器和 Route-Policy 等七种过滤器供路由协议引用。

5.10 IP 组播特性

IGMP

IGMP（Internet Group Management Protocol）因特网组管理协议，是 TCP/IP 协议族中负责 IPv4 组播成员管理的协议，用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

通过在接收者主机和与其直连的组播路由器上配置 IGMP，可以实现主机动态加入组播组和组播路由器对本地网络组成员信息的管理。

到目前为止，IGMP 有三个版本：IGMPv1 版本（RFC1112）、IGMPv2 版本（RFC2236）和 IGMPv3 版本（RFC3376）。所有 IGMP 版本都支持 ASM（Any-Source Multicast）模型。IGMPv3 可以直接应用于 SSM（Source-Specific Multicast）模型，而 IGMPv1 和 IGMPv2 则需要通过 SSM-Mapping 技术来支持 SSM 模型。

要使组播报文最终能够到达接收者，需要将接收者主机接入 IP 组播网络，并加入到相应的组播组中。IGMP 通过在主机侧和路由器侧交互 IGMP 报文实现组成员管理功能。IGMP 协议可以记录接口下主机的加入和离开等信息，以确保组播数据能够正确地转发到该接口。

IGMP Snooping

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束机制，用于管理和控制组播组。

当没有运行 IGMP Snooping 时，组播数据在二层被广播；当运行 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。

应用 IGMP Snooping 的优势主要有以下方面：

- 节约网络带宽，方便对主机单独计费。
- 各个 VLAN 独立转发，提高信息安全性。
- 快速响应链路故障，增强可靠性。

PIM-DM

PIM（Protocol Independent Multicast）称为协议无关组播，表示为 IP 组播提供路由信息的可以是静态路由、RIP、OSPF、IS-IS、BGP 等任何一种单播路由协议。组播路由和单播路由协议无关，只要通过单播路由协议能够产生相应组播路由表项即可。

PIM-DM（Protocol Independent Multicast Dense Mode）称为协议无关组播－密集模式，属于密集模式的组播路由协议，适用于组成员分布相对密集的小型网络。

PIM-DM 的基本原理如下：

- PIM-DM 假设网络中的每个子网都存在至少一个组播组成员，因此组播数据将被扩散（Flooding）到网络中的所有节点。然后，PIM-DM 对没有组播数据转发的分支进行剪枝（Prune），只保留包含接收者的分支。这种“扩散—剪枝”现象周期性地发生，被剪枝的分支也可以周期性地恢复成转发状态。

- 当被剪枝分支的节点上出现了组播组的成员时，为了减少该节点恢复成转发状态所需的时间，PIM-DM 使用嫁接（Graft）机制主动恢复其对组播数据的转发。

一般说来，密集模式下数据包的转发路径是有源树（Source Tree，即以组播源为“根”、组播组成员为“枝叶”的一棵转发树）。由于有源树使用的是从组播源到接收者的最短路径，因此也称为最短路径树（Shortest Path Tree，SPT）。路由器收到组播数据的接口称为上游，转发组播数据的接口称为下游。

PIM-SM

PIM-SM（Protocol Independent Multicast-Sparse Mode）称为协议无关组播－稀疏模式，属于稀疏模式的组播路由协议，适用于组成员分布相对分散、范围较广、大规模的网络。

PIM-SM 的基本原理如下：

- PIM-SM 假设所有主机都不需要接收组播数据，只向明确提出需要组播数据的主机转发。PIM-SM 实现组播转发的核心任务就是构造并维护 RPT（Rendezvous Point Tree，共享树或汇集树），RPT 选择 PIM 域中某台路由器作为公用的根节点 RP（Rendezvous Point，汇集点），组播数据通过 RP 沿着 RPT 转发给接收者。
- 连接接收者的路由器向某组播组对应的 RP 发送加入消息（Join Message），该报文被逐跳送达 RP，所经过的路径就形成了 RPT 的分支。
- 组播源如果要向某组播组发送组播数据，首先由组播源侧 DR（Designated Router，指定路由器）负责向 RP 进行注册，把注册消息（Register Message）通过单播方式发送给 RP，该报文到达 RP 后触发建立 SPT。之后组播源把组播数据沿着 SPT 发向 RP，当组播数据到达 RP 后，被复制并沿着 RPT 发送给接收者。

MSDP

MSDP 是 Multicast Source Discovery Protocol（组播源发现协议）的简称，是为了解决多个 PIM-SM（Protocol Independent Multicast Sparse Mode，协议无关组播—稀疏模式）域之间的互连而开发的一种域间组播解决方案，用来发现其它 PIM-SM 域内的组播源信息。

在基本的 PIM-SM 模式下，组播源只向本 PIM-SM 域内的 RP 注册，且各域的组播源信息是相互隔离的，因此 RP 仅知道本域内的组播源信息，只能在本域内建立组播分发树，将本域内组播源发出的组播数据分发给本地用户。

如果能够有一种机制，将其它域内的组播源信息传递给本域内的 RP，则本域内的 RP 就可以向其它域内的组播源发起加入过程并建立组播分发树，实现组播数据跨域传输，从而使本域内的组成员主机接收到其他域的组播源发出的数据。

基于这一设想，MSDP 通过在网络中选取适当的路由器建立 MSDP 对等体关系，以连通各 PIM-SM 域的 RP。通过在各 MSDP 对等体之间交互 SA（Source Active，信源有效）消息来共享组播源信息。

MSDP 对等体之间使用 TCP 连接，对接收到的 SA 消息执行 RPF 检查。

5.11 接入特性

以太网

通过二层接口 USG 系列可实现二层高速交换，方便实现二层接入。

目前 USG 支持的 LAN 接口为以太网接口，包括如下三种：

- 传统以太网接口：符合 10Base-T 物理层规范，工作速率为 10Mbit/s，有半双工和全双工两种工作方式。
- 快速以太网（Fast Ethernet）接口：符合 100Base-TX 物理层规范，兼容 10Base-T 物理层规范，可以在 10Mbit/s、100Mbit/s 两种速率下工作，有半双工和全双工两种工作方式。它具有自动协商模式，可以与其他网络设备协商确定工作方式和速率，自动选择最合适的工作方式和速率，从而可以简化系统的配置和管理。
- 千兆以太网（Gigabit Ethernet）接口：符合 1000Base-T 物理层规范，可以工作在全双工工作方式下，速率可达 1000Mbit/s。千兆以太网接口能够工作在自动协商模式下，可以用于协商流控。

Eth-Trunk

为了提高链路的传输能力，需要将多个以太网端口捆绑为一个 Eth-Trunk 接口，Eth-Trunk 接口的总带宽是各成员带宽之和，通过这种方式，可以增加接口的带宽。

通过 Eth-Trunk 接口可以实现负载分担。Eth-Trunk 接口将流量分配到不同的链路上，最后到达同一目的地。这样可以避免流量仅在一条链路中传输而造成流量阻塞。

Eth-Trunk 接口还可以提高链路的可靠性。在 Eth-Trunk 接口中，如果某个成员端口状态为 Down，流量还能通过其他的端口进行传输。

NULL 和 Loopback

Loopback 是一种纯软件性质的逻辑接口。任何送到该接口的网络数据报文都会被认为是送往 USG 自身。

Loopback 接口也称为环回接口，与普通接口使用同样的 IP 地址配置原则，用户可以根据需要在系统启动后动态创建和删除该类型的接口。

由于创建后一直保持 Up 状态，并具有回环的特性，Loopback 接口也常用来提高配置的可靠性。

Null 接口也是一种纯软件性质的逻辑接口，与 Loopback 接口不同，Null 接口更类似于一些操作系统中支持的空设备（Null devices），任何送到该接口的网络数据报文都会被丢弃。有些应用（比如配置 SNA 的 local peer）需要在不影响物理接口配置的情况下，配置一个带有指定 IP 地址的本地接口，并且需要将这个接口上的地址通过路由协议发布出去。

VLAN

用户可以根据实际组网需要在 USG 系列上划分 VLAN，实现以下功能：

- 控制广播域的范围。将局域网内的广播报文限制在一个 VLAN 内，节省带宽，提高网络处理能力。
- 增强局域网的安全性。由于报文在数据链路层被 VLAN 划分的广播域所隔离，因此各个 VLAN 内的主机间不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。
- 灵活创建虚拟工作组。使用 VLAN 可以创建跨物理网络范围的虚拟工作组。
- 相同 VLAN 下的用户互访不受访问策略的控制。
- 不同 VLAN 之间的用户互访受到访问策略的控制。

端口隔离

用户将需要进行控制的端口加入到端口隔离组中，实现隔离组内端口间二层、三层数据报文的隔离。端口隔离功能在增强了网络安全的同时，也为用户提供了更为灵活的组网方案。

MAC 地址表

USG 系列通过维护 MAC 地址表，实现报文快速转发。MAC 地址表项包括静态 MAC 地址表项、动态 MAC 地址表项和黑洞 MAC 地址表项。

E1 和 CE1

E-载波是国际电信联盟-电信标准部 ITU-T（International Telecommunication Union-Telecommunication Standardization Sector）建议的一种数字通信体系。它开始于 E1，应用于北美以外地区。

E1/CE1 接口有如下特点：

- 当工作在净通道模式下时，也称为非成帧模式。它相当于一个不分时隙、数据带宽为 2.048Mbit/s 的接口，其逻辑特性与同步串口相同。它支持 PPP、HDLC 链路层协议，支持 IP 等网络协议。
- 当工作在非通道化模式下时，也称为成帧模式。此时可以对接口进行时隙绑定，但是只能进行一次捆绑，绑定出一个通道。比如，捆绑时隙 1 和时隙 2 形成一个带宽为 128K 的串口，则剩下的时隙不能再被捆绑。即，不管一次捆绑几个时隙，只能捆绑一次，绑定成一个串口。其逻辑特性与同步串口相同，支持 PPP、HDLC 等链路层协议，支持 IP 等网络协议。
- 当工作在通道化模式下时，也称为成帧模式。它在物理上分为 32 个时隙，对应编号为 0～31。可任意捆绑为 N×64Kbit/s 的逻辑通道。其中时隙 0 用于传送帧同步信号，不能被捆绑。其余的 31 个时隙可以被任意地分成若干组（channel-set），每组时隙捆绑以后作为一个接口使用，其逻辑特性与同步串口相同。它支持 PPP、HDLC 链路层协议，支持 IP 等网络协议。

串口

串口是最常用的广域网接口之一，分为同步串口和异步串口。

同步串口特性：

- 可以工作在 DTE（Data Terminal Equipment）和 DCE（Data Circuit-terminal Equipment）两种方式。一般情况下，同步串口作为 DTE 设备，接受 DCE 设备提供的时钟。
- 同步串口可以外接多种类型电缆，如 V.24、V.35、X.21、RS449、RS530 等。USG 可以自动检测同步串口外接电缆类型，并完成电气特性的选择。一般情况下，无需手工配置。
- 同步串口支持的链路层协议类型包括 PPP（Peer-Peer Protocol）、HDLC（High Level Data Link Control）。
- 支持 IP 网络层协议。

异步串口可以工作在协议模式和流模式下。异步串口外接 Modem 或 ISDN TA（Terminal Adapter，终端适配器）时可以作为拨号接口使用。协议模式下，链路层协议可以为 PPP，网络层协议可以为 IP 和 IPX 等。

WLAN（WIFI）

无线局域网（WLAN）是指以无线信道作传输媒介的计算机局域网，是有线联网方式的重要补充和延伸，并逐渐成为计算机网络中一个至关重要的组成部分，广泛适用于需要可移动数据处理或无法进行物理传输介质布线的领域。

作为新型的宽带接入方式，WLAN 越来越受到人们的宠爱，并得到迅猛的发展，由此涌现出多种 WLAN 的标准：

- 802.11
- Bluetooth
- HiperLAN2（High Performance Radio LAN 2）
- HomeRF（Home Radio Frequency）

其中，802.11 因技术简单、通信质量稳定、传输带宽较高而成为了构建 WLAN 的常用标准。

3G

3G（The Third Generation）是第三代移动通信系统，相对于第一代模拟制式系统（1G）和第二代 GSM 数字系统（2G），是指将无线通信与因特网等多媒体通信结合的新一代移动通信系统。3G 能够处理图像、音乐、视频流等多种媒体形式，提供包括网页浏览、电话会议、电子商务等在内的多种信息服务。ITU（International Telecommunication Union）在 2000 年 5 月确定 WCDMA、CDMA2000 和 TD-SCDMA 三大主流无线接口标准，写入 3G 技术指导性文件《2000 年国际移动通讯计划》。

USG 可以插入多种 3G 数据卡，局域网用户可以通过 3G 数据卡上行接入网络。通过插入不同的 3G 数据卡，USG 系列可支持 WCDMA、CDMA2000 和 TD-SCDMA 三种制式。

PPP

PPP（Point-to-Point protocol）是在点到点链路上承载网络层数据包的一种链路层协议，提供用户验证功能，支持同 / 异步。

PPP（Point-to-Point Protocol）定义了一整套的协议，其中包括：

- 链路控制协议 LCP（Link Control Protocol）：用于建立、拆除和监控数据链路。
- 网络层控制协议 NCP（Network Control Protocol）：用于协商数据链路上传输的数据包的格式与类型。
- 验证协议 PAP（Password Authentication Protocol）、CHAP（Challenge Handshake Authentication Protocol）：用于验证网络安全。

MP

MP 是出于增加带宽的考虑，将多个 PPP 链路捆绑使用的技术。可以在支持 PPP 的接口（如通道化出的 Serial 接口或低速 POS 接口）上应用。

MP 允许将报文分片，分片报文通过 MP 的多条 PPP 链路送往同一目的地。

MP 的协商包括 LCP 协商和 NCP 协商两个过程：

- LCP 协商：两端首先进行 LCP 协商，除了协商一般的 LCP 参数外，还要验证对端接口是否也工作在 MP 方式下。如果两端工作方式不同，LCP 协商不成功。
- NCP 协商：根据 MP-Group 接口的各项 NCP 参数（如 IP 地址等）进行 NCP 协商，物理接口配置的 NCP 参数不起作用。

NCP 协商通过后，即可建立 MP 链路。

HDLC

HDLC（High-level Data Link Control procedure）最大的特点是不需要规定数据必须是字符集，对任何一种比特流，均可以实现透明的传输。

标准 HDLC 协议族中的协议运行于同步串行线路之上，如 DDN（Digital Data Network）。

HDLC 的地址字段和控制字段均是 8 比特，用来实现 HDLC 协议的各种控制信息，并标识是否是数据。

MSTP

MSTP（Multiple Spanning Tree Protocol）兼容 STP（Spanning Tree Protocol）和 RSTP（Rapid Spanning Tree Protocol），并弥补 STP 和 RSTP 的缺陷。STP 选择性地阻塞网络冗余链路，将网络修剪成树状，达到消除环路的目的，同时具备链路备份功能。MSTP 既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供良好的负载分担机制。

PPPoE

PPPoE（Point-to-Point Protocol over Ethernet）利用以太网将大量主机组成网络，通过一个远端接入设备连入因特网。

通过配置 PPPoE，可以实现与远端设备建立 PPP 会话，实现接入控制和计费。

USG 可以作为 PPPoE（PPP over Ethernet）Server 端，用于在以太网环境中接入不同类型的 PPPoE Client 用户。

USG 可以作为 PPPoE Client 设备，实现 PPPoE 的客户端拨号功能。

ADSL

ADSL 技术是提供高带宽接入的技术之一，主要应用于不对称速率传输。ADSL 利用现有的用户电话线传送高速数据，为用户提供诸如高速 Internet 接入、视频点播 VOD（Video on Demand）、可视电话等多种业务。

ADSL2+是 2003 年 1 月举行的 ITU 会议上通过的新一代 ADSL 标准，是在 ADSL2 和无分离器的 ADSL2 基础上进一步扩展的 ADSL 标准。

USG 可以插入 ADSL2+接口模块，从而支持 ADSL2+特性。

G.SHDSL

SHDSL 是由 ITU-T 定义的，在单对双绞线上提供传输双向对称带宽数据业务的一种技术，符合国际电联 G.991.2 推荐标准，又称 G.SHDSL。SHDSL 属于对称 DSL 技术，传输距离是所有 DSL 技术中最远的。

USG 的 MIC 插槽可以插入 G.SHDSL 接口模块，从而支持 SHDSL 特性。

5.12 系统管理

信息中心

信息中心通过接收处理日志信息、调试信息和告警信息，为网络管理员和开发人员监控网络运行和诊断网络故障提供支持。

SNMP

目前，计算机网络中用得最广泛的网络管理协议是简单网络管理协议 SNMP（Simple Network Management Protocol），它是被广泛接受并投入使用的工业标准。

SNMP 的作用是保证管理信息在任意两点间传送，便于网络管理员在网络上的任何节点检索信息，进行修改，寻找故障，完成故障诊断，容量规划和报告生成。

SNMP 采用轮询机制，提供最基本的功能集。适合小型、快速和低价格的环境使用。它只要求无连接的传输层协议 UDP，受到许多产品的广泛支持。

设备支持 SNMP v3 版本，并兼容 SNMP v1 版本和 SNMP v2c 版本。

LLDP

LLDP（Link Layer Discovery Protocol）是 IEEE 802.1AB 中定义的第二层网络发现协议。通过采用 LLDP 技术，在网络规模迅速扩大时，网络管理系统可以快速掌握网络的拓扑信息和拓扑变化信息。

LLDP 提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit）中发布给与自己直连的邻居，邻居收到这些信息后将它以标准 MIB（Management Information Base）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

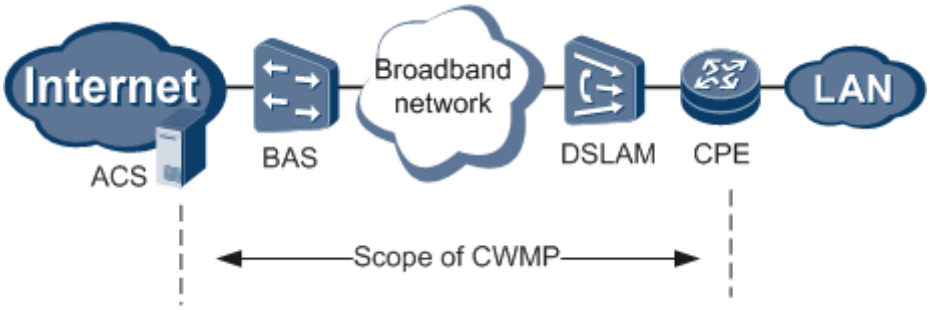
CWMP（TR-069）

CWMP 是一种广域网管理协议，可实现 ACS 对 CPE 的集中管理,主要功能为配置管理、版本管理、远程监控和诊断功能。

CWMP（CPE WAN Management Protocol，CPE 广域网管理协议）是由 DSL（Digital Subscriber's Line，数字用户线路）论坛发起开发的技术规范之一。它提供了对下一代网络中家庭网络设备进行管理配置的通用框架、消息规范、管理方法和数据模型。CWMP 主要应用于 DSL 接入网络环境中。在 DSL 接入网络中，由于用户设备数量繁多、部署分散，通常位于用户侧，不易进行设备的管理和维护，CWMP 提出通过 ACS（Auto-Configuration Server，自动配置服务器）对 CPE（Customer Premises Equipment，用户侧设备）进行远程的集中式管理，解决 CPE 设备的管理问题，节约维护的成本，提高问题解决的效率。

CWMP 典型组网如图 5-5 所示。通常，用户侧设备（例如网关、机顶盒）种类繁多，部署分散。当需要配置变更或者故障处理时，通常只有运营商的维护人员上门处理，管理非常不便。CWMP 的出现解决这样一个难题。它提供了对用户终端设备进行管理配置的通用框架和协议，实现了从网络侧对用户侧设备进行远程集中管理。通过部署 CWMP，用户侧相关设备的配置、诊断、升级等工作，均可以由 ACS 来完成，大大节省了维护成本。

图5-5 CWMP(TR-069)典型应用



NetStream

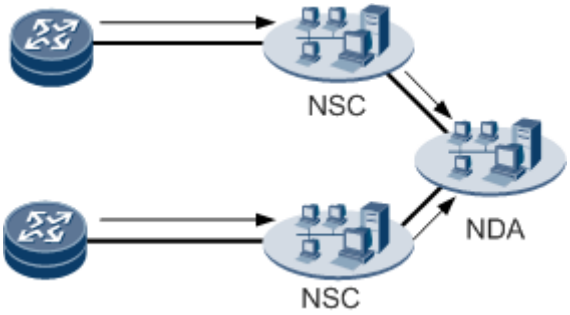
NestStream 对网络流量进行统计，并定期向 NSC 发送统计数据。这些数据可用于计费、网络管理和规划等。

随着网络支持的业务和应用日渐增多，用户对流量统计分析提出了更高的要求，NetStream 特性提供了一种解决途径。NetStream 给网络管理人员提供了从他们的数据网络访问“详细记录”信息的方法。输出的 NetStream 数据可以有多种用途，包括网络管理和规划、企业记帐和分部门的计费、ISP 编制帐单、数据储备以及用于商业目的的数据采集。

在网络中，由于 IP 网络的非面向连接特性，网络中不同类型业务的通信可能是任意一台终端设备向另一台终端设备发送的一组 IP 数据包，这组数据包实际上就构成了网络中某种业务的一个数据流。绝大部分的数据流量都是短暂、阵发的双向数据流。NetStream 主要根据一个报文的目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、ToS（Type of Service）、输入/输出接口组成的 7 元组来区分不同的流，针对这些流做独立的数据统计。路由设备把采集到的关于流的详细信息输出给 NSC（NetStream

Collector），NSC 收集和存储 NDE 发来的流量统计数据信息，并进行过滤和聚合后，输出给 NDA，NDA 对数据进一步的聚合、排序并将各种数据以图形的形式显示出来。通过对 NDA 输出的结果进行分析，为网络计费，网络规划，网络监控，应用监控、分析和故障定位等提供依据。

图5-6 NetStream 典型应用



设备把采集到的关于流的详细信息输出给 NSC，由 NSC 进行初步的处理输出给 NDA，然后由后续的 NDA 进行分析。

NTP

NTP 的目的是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致，从而使设备能够提供基于统一时间的多种应用。对于运行 NTP 的本地系统，既可以接受来自其他时钟源的同步，也可以作为时钟源去同步别的时钟，并且可以通过交换 NTP 报文互相同步。

NTP 基于 UDP 传输，使用端口号 123。

NQA

NQA 提供对网络上运行的各种协议的性能进行测试的功能。同时，NQA 也是网络故障诊断和定位的有效工具。

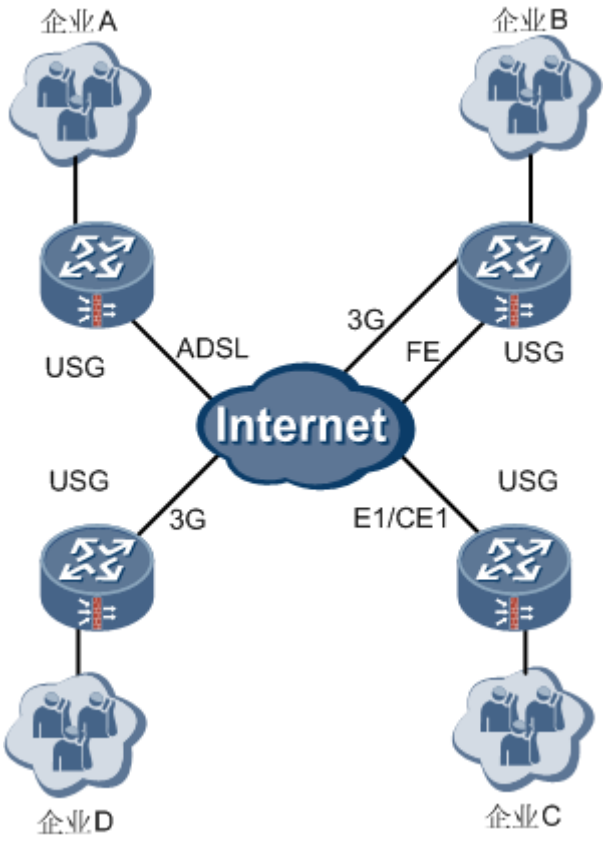
NQA 是对 Ping 功能的扩展和增强，它可以探测 TCP、UDP、DHCP、FTP、HTTP、SNMP 服务是否打开，以及测试各种服务的响应时间。

6 应用场景

关于本章

6.1 综合接入解决方案

图6-1 多种方式接入因特网

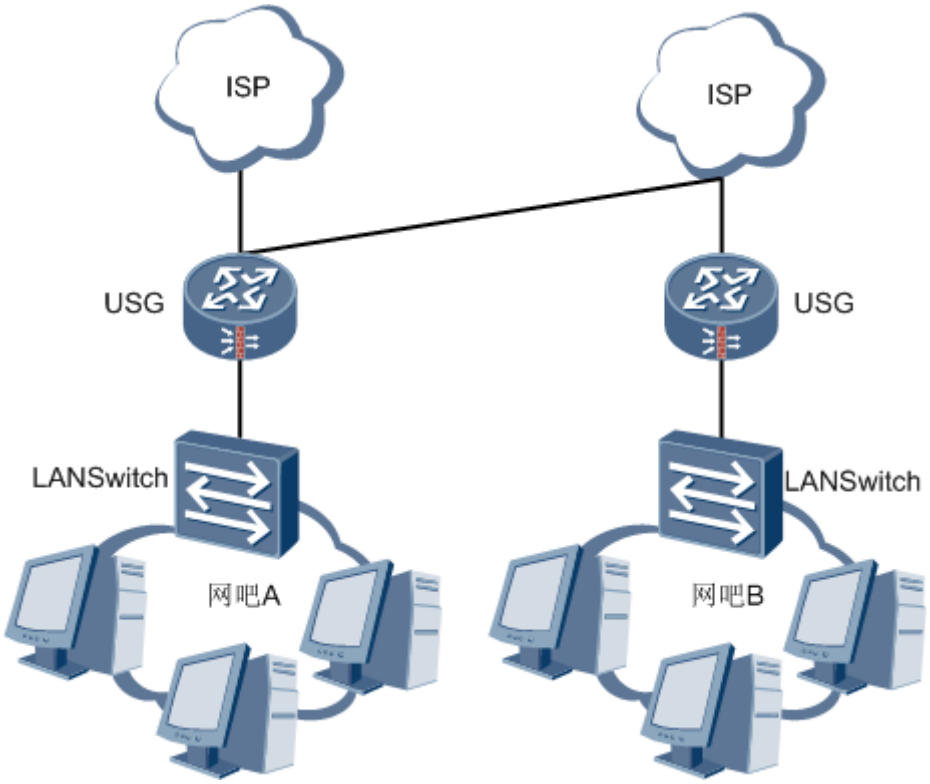


根据运营商提供的网络环境，用户可以选择采用 E1/CE1、FE、GE、3G、WLAN、ADSL2+、G.SHDSL 或者 SA 的接入方式。USG 系列可以提供双上行链路，保证上网业务的可靠性。

- 提供路由、安全、交换、VPN 和无线功能，为报文的安全、快速、可靠转发提供保障。
- 提供攻击防范功能，对来自外部网络和内部网络的各种攻击进行防范。
- 提供拥塞管理和 CAR（Committed Access Rate）限流，为用户上网提供带宽保证。
- 提供 NAT 功能。

6.2 网吧出口网关

图6-2 网吧出口网关

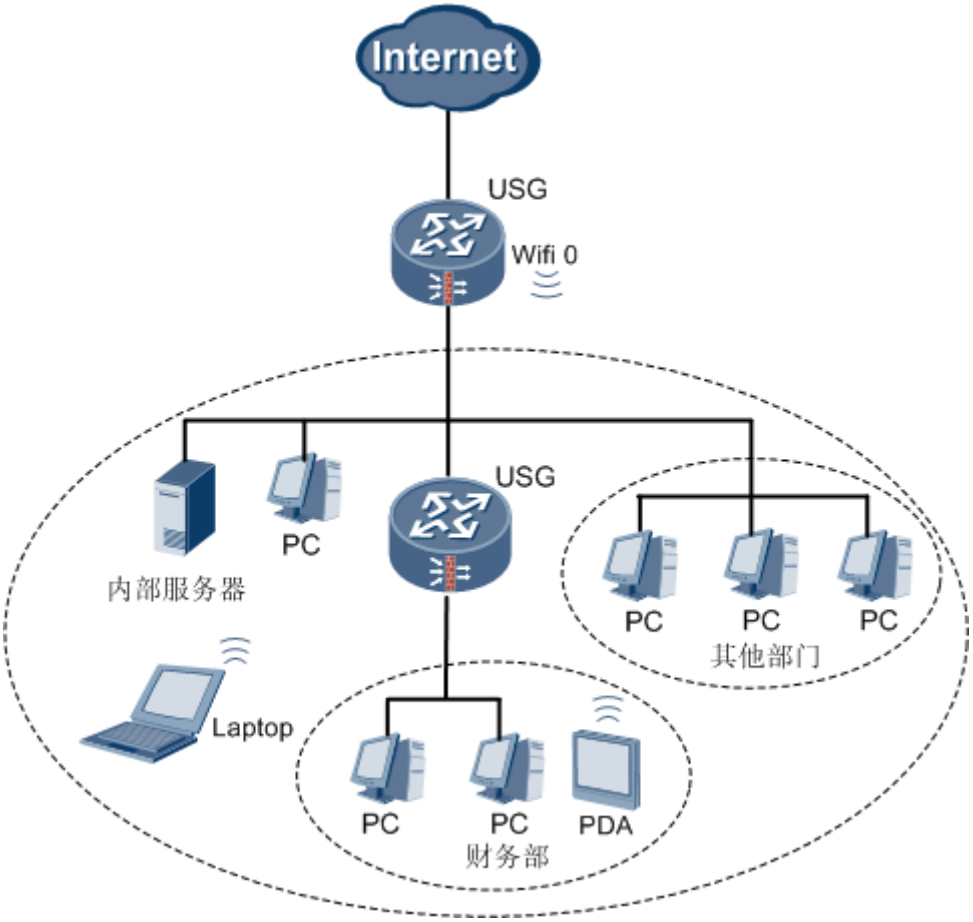


对于大型网吧，USG 可以作为出口网关，为网吧用户提供 Internet 接入：

- 提供丰富的路由功能，为报文的快速正确转发提供支持。
- 提供安全防范功能，对来自外网和内网的各种攻击进行防范。
- 提供拥塞管理和 CAR 限流，为用户上网提供带宽保证。
- 提供双上行链路，保证上网用户的业务的可靠性。
- 保证大流量上网线路稳定性。

6.3 保护内部局域网

图6-3 保护内部局域网

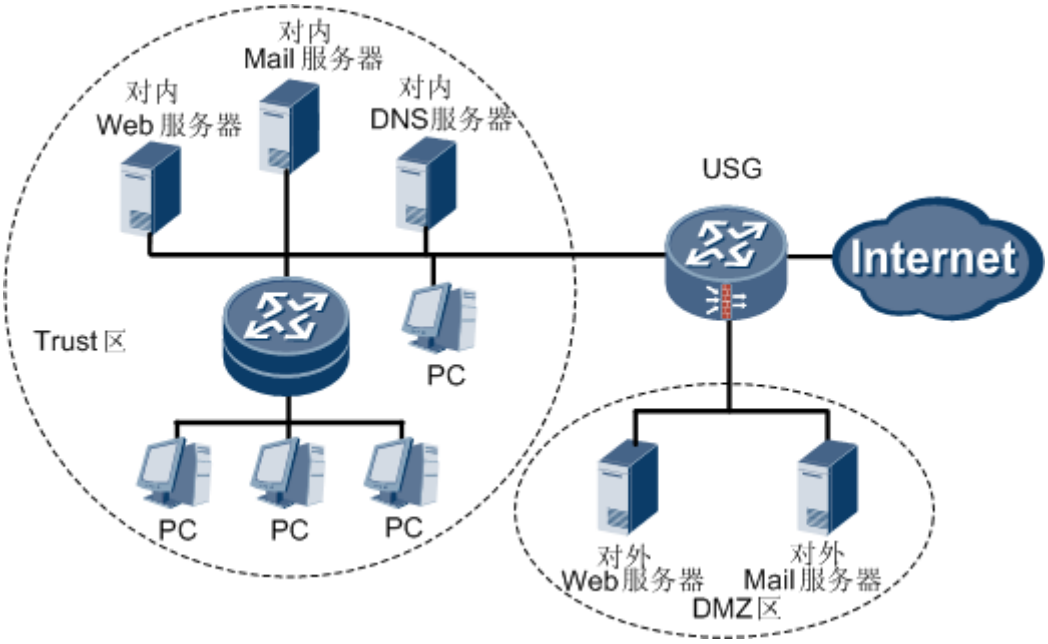


USG 系列可以部署在企业内部网与外部网的接口处，也可以部署在企业局域网内部的各个关键位置，以保护重点资源的信息安全。

如图 6-3 所示，企业局域网与因特网在接口处通过 USG 系列相连，限制因特网用户访问企业局域网。如果企业局域网用户需要访问因特网资源，可以在进行上网用户认证后，经过 NAT（Network Address Translation）转换之后向外发起访问。关键部门（财务部）本身组成一个小的局域网，通过 USG 系列进行保护，以防止非法内部用户访问关键资源。

6.4 安全地开放内网服务器

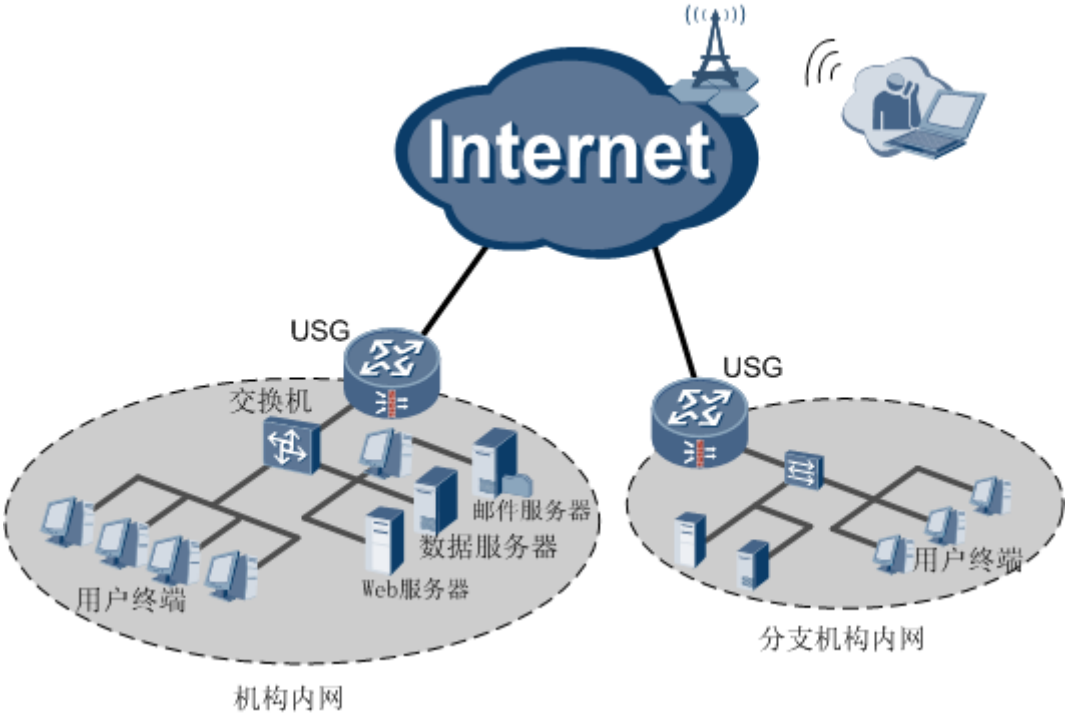
图6-4 安全地开放内网服务器



对于数据中心、ISP（Internet Service Provider）、小区、学校和政府等单位，有对外提供 Web、Email 等服务的需求，可以通过 USG 系列来过滤报文，如只允许外部访问所开放服务器特定端口的报文通过，检测并防止各类攻击。

6.5 内网用户管理

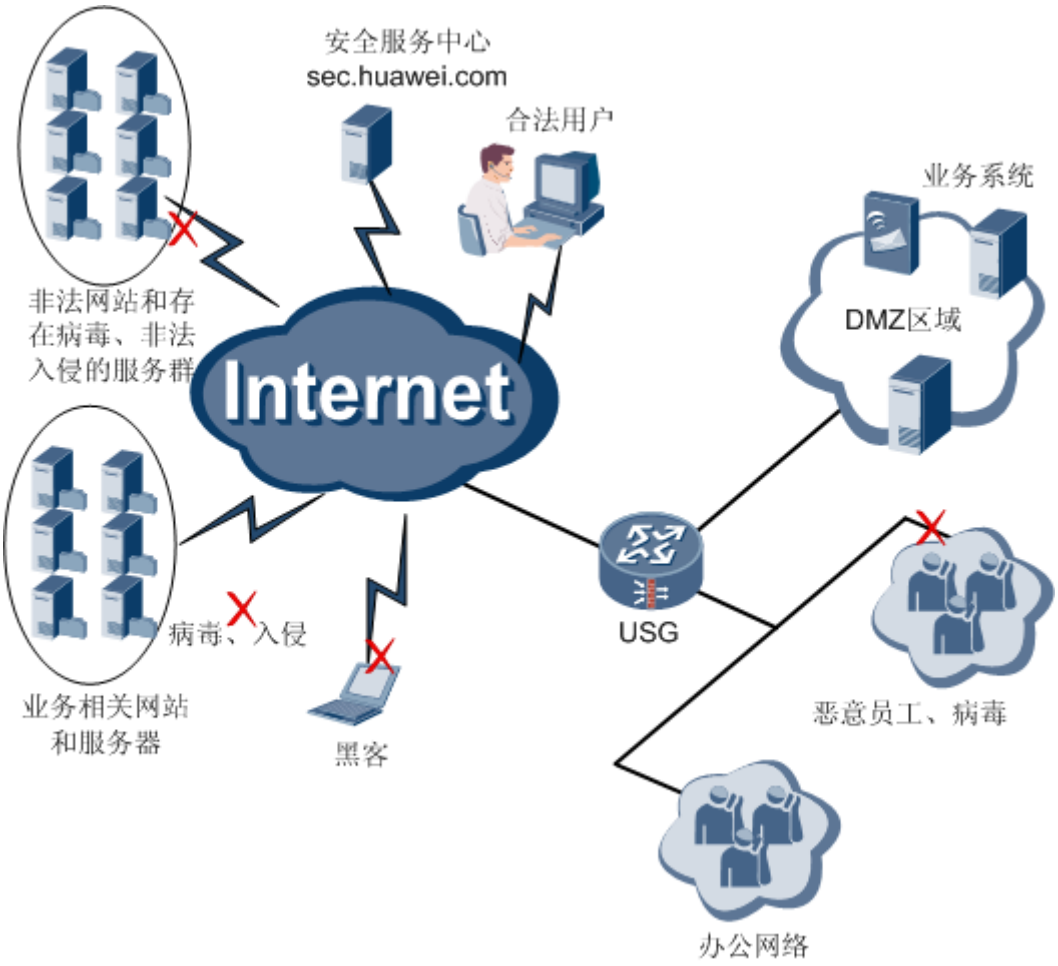
图6-5 内网用户管理



- 配置上网用户管理对企业内网用户的上网权限进行认证。
- 通过策略一体化引用应用控制策略、限流策略，精确识别各类应用，配置每 IP 限流、整体限流策略，还可以配置最大带宽与保证带宽，限制非业务应用对带宽的占用的同时，保证业务应用的带宽需求，使公司有限的带宽资源能最大限度的发挥作用。

6.6 企业或政府机构安全防护应用

图6-6 安全防护应用

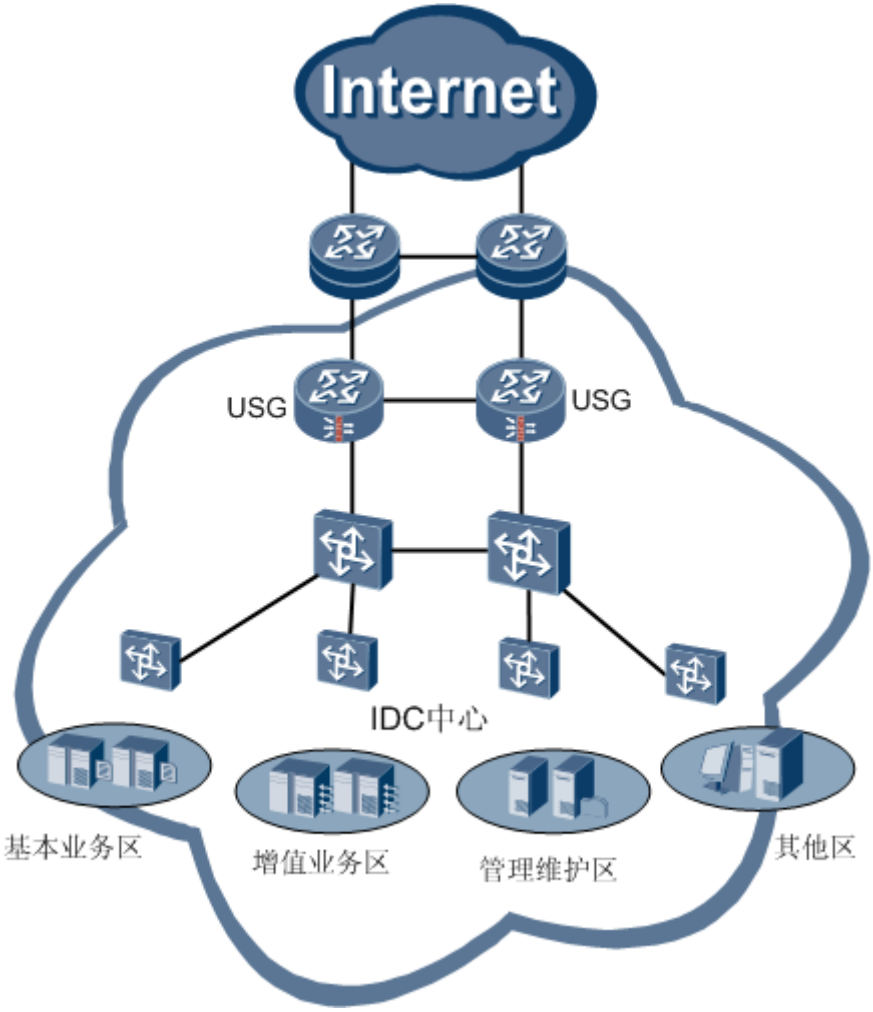


- 通过如下功能保护内网关键业务
  - 攻击防范
  - IPS
  - AV
  - 邮件过滤
- 网络访问
  - 提供 NAT 功能供内网用户访问 Internet，NAT Server 功能使企业对外开放邮件、Web 等内部服务器。
  - 提供 IPSec/L2TP/SSL 等 VPN 功能，使分支机构和出差员工安全的访问总部资源。
- 控制内网用户上网行为
  - P2P 限流
  - IM 阻断

- URL 过滤

6.7 IDC 安全防护应用

图6-7 IDC 安全防护组网图



两台 USG 部署在数据中心的出口处，配置基本的路由功能、防火墙功能、入侵防御功能、反病毒攻击功能和 URL 过滤功能。

入侵防御功能可以深度感知并检测流经的数据流量，发现攻击后能及时阻断，对应用层攻击的防御效果显著。

反病毒功能实现对使用 HTTP、SMTP、POP3 协议传输的文件进行病毒扫描，并根据 AV 策略对带病毒文件进行处理。

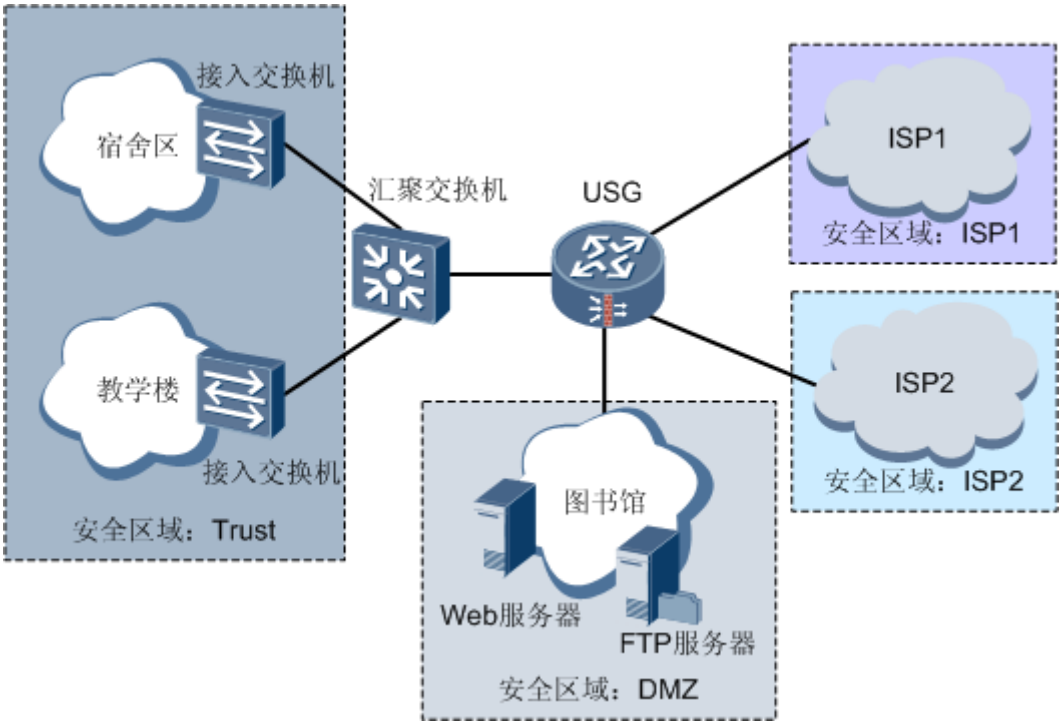
URL 过滤对上网行为进行管理，有效实现对终端应用的审计监控，对于可能增加内部安全威胁或影响正常业务的应用进行限制。

Internet 上的安全服务中心能够给 USG 提供 IPS 签名库和病毒库在线升级，可保证 USG 上时刻保持最新的 IPS 签名库和病毒库，使入侵防御和反病毒功能更有效。

6.8 校园网应用

校园网的应用如图 6-8 所示。

图6-8 校园网应用组网图



- 为了实现校园网用户使用有限公网 IP 地址接入 Internet，需要配置 NAPT 方式的 NAT，借助端口将大量私网 IP 地址转换为有限的公网 IP 地址。

  由于校园网连接两个运营商，因此需要分别进行地址转换，将私网地址转换为公网地址。即创建两个安全区域 ISP1 和 ISP2（安全优先级低于 DMZ 区域），并分别在 Trust 与 ISP1 域间、Trust 与 ISP2 域间配置 NAT outbound。
- 为了实现去往不同运营商的流量由对应接口转发，需要收集 ISP1 和 ISP2 所属网段的信息，并配置到这些网段的静态路由。使去往 ISP1 的流量通过连接 ISP1 的接口转发，去往 ISP2 的流量通过连接 ISP2 的接口转发。

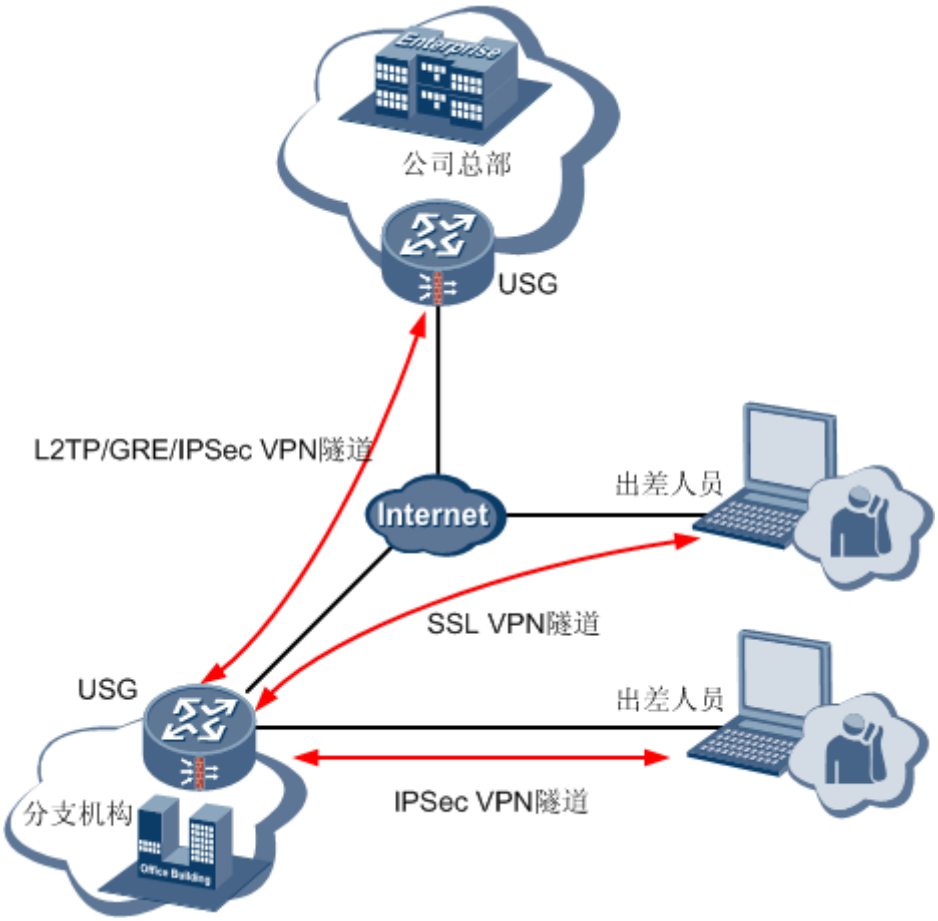
  为了提高链路可靠性，避免业务中断，需要配置两条缺省路由。当报文无法匹配静态路由时，通过缺省路由发送给下一跳。
- 由于图书馆的服务器部署在内网，其 IP 地址为私网 IP 地址。如果想对校外用户提供服务，就需要将服务器的私网 IP 地址转换为公网 IP 地址。即分别基于 ISP1、ISP2 区域配置 NAT Server。
- 由于运营商提供给该学校的带宽有限，为了保证其他业务不受影响，对 P2P 流量进行限制。

- 在 USG 上启用攻击防范功能，保护校园网内部网络。

6.9 VPN 组网应用

利用 VPN 功能，分布于各地的分支机构和出差员工使用 Internet，实现快速部署等特点使其更适合在任何时间，任何地点，任何设备的灵活安全接入场景。

图6-9 VPN 接入应用



如图 6-9 所示，公司总部通过 USG 与外部网（Internet）相连，总部服务器可以向包括分支机构以及出差员工在内的内部用户提供服务。分支机构也通过 USG 连接 Ineternet，并也可以向外提供服务，同时分支机构的用户需要访问总部服务器或总部局域网主机。此外，出差员工可通过 IPSec VPN 或 SSL VPN 访问企业内网资源。

为了将总部与分支机构以及出差员工共同组成企业 Intranet，可以在总部与分支机构之间建立 L2TP、GRE 或 IPSec 三种不同类型的 VPN 通道。出差员工通过建立 IPSec VPN 或 SSL VPN 通道，在经过服务器的认证之后可以进入公司内部网络。

7 操作和维护

关于本章

7.1 多种设备配置管理方式

Console

支持配置终端与 Console 口相连后，在配置终端上对设备进行配置和维护。

Telnet

只要有到设备路由可达的配置终端，设备支持用 Telnet 方式在终端上对设备进行配置和维护。

SSH

支持 SSH（Secure Shell）维护管理方式，实现在不能保证安全的网络上提供安全信息保障和强大认证功能，以避免受到 IP 地址欺诈、明文密码截取等攻击。

Web

Web 配置方式基于 sWeb 平台。

设备提供基于 GUI（Graphic User Interface）的 Web 管理界面，为用户提供友好的配置和管理界面。设备支持通过 HTTP（Hyper Text Transfer Protocol）和 HTTPS（Secure Hyper Text Transfer Protocol）协议访问 Web 管理界面。

在 Web 管理界面中，可以配置安全区域、ACL（Access Control List）、NAT（NetworkAddress Translation）、ASPF（Application Specific Packet Filter）、攻击防范、黑名单、VLAN、QoS、入侵防御系统、应用控制、VPN、策略路由、负载均衡等功能和各种统计参数。

基于 SNMP 的终端系统管理

设备支持 SNMP（Simple Network Management Protocol）（v1/v2c/v3）协议和 Client/Server 体系结构，接受 NMS（Network Management System）网管站的管理，如接受华为公司网管平台 U2000 的管理。

U 盘升级

通过 U 盘自动升级或手动升级，实现方便的版本升级、配置。

一键式恢复出厂默认配置

USG2200/5100 支持一键恢复，通过面板上的 Reset 键完成对设备一键恢复到设备的出厂缺省配置。

7.2 丰富的系统维护功能

- 远程抓包

  远程抓包功能是将经过 USG 的报文复制保存到内存中，然后将报文发送到特定的主机，以实现在远程主机上对 USG 的报文进行分析。

- 丢包统计

  USG 提供多种丢包统计的数据，有效提供了丢包分析。

- 多种升级方式

  对 DPI 知识库提供了在线自动升级、在线手动升级、离线升级方式。

  对病毒库、IPS 功能的签名库提供在线自动升级、在线手动升级、离线升级方式，还支持版本回退功能。

- 调试命令

  USG 提供业务运行的 Debug 功能，在线记录用户指定的业务运行时刻的关键事件、报文处理、报文解析、状态切换等信息；为用户在调测设备及组网方案提供了有利的支持；Debug 可以根据指定业务（如某一路由协议）、指定接口（如某一路由协议在特定接口上的信息）通过控制台打开或者关闭。USG 提供系统操作的 Trace 功能，在线记录系统的任务切换、中断、队列读写、系统异常等重要事件，系统发生故障重起后，可以读出 Trace 信息作为故障定位参考。Trace 功能可以通过控制台命令打开或关闭。

- 灾备还原配置

  通过事先指定一份配置文件作为灾备配置文件，并指定灾备配置文件作为下次启动的配置文件，则在配置文件不可恢复时，可以有效实现最初业务正常使用的目的。

- Web 界面诊断功能

sWeb 界面上提供 IPSec 协商诊断、3G 接入诊断、ADSL 接入诊断、针对网页无法打开的故障诊断功能，极大地方便了对故障进行定位与排查。

7.3 增强的日志管理

- 两种日志输出方式

  USG 不仅能通过文本方式输出 Syslog 日志，而且还针对流经 USG 的数据流量大和日志信息丰富等特点，创建基于流状态的信息表，并通过二进制方式输出高速流日志。

- 丰富的日志信息

  流量监控日志、黑名单日志、攻击防范日志、地址绑定日志、HTTP 访问日志、包过滤日志、反病毒日志、入侵检测日志、URL 过滤日志、NAT/ASPF 等会话日志。

- 与 eLog 联动

  eLog 日志管理系统是华为推出的设备日志管理系统。通过高效地采集设备的日志，用户能及时了解安全设备和网络设备的运行情况，跟踪网络用户的行为，迅速识别并消除安全威胁。

  USG 系列支持与 eLog 日志管理系统进行联动，实现日志信息的海量存储与快捷查询，有效帮助用户定位网络问题和设备运行的历史信息。

- 日志服务器容灾

  最多支持向 16 个日志服务器发送日志，日志发送方式支持轮询和并发两种。

7.4 安全性

数据系统安全性

系统采取以下措施保护数据的安全性：

- 备份恢复策略

  将系统某个时间点的数据（系统软件、配置文件、日志文件、数据库数据）保存到其他介质中，当系统出现异常情况时，可导入备份数据到系统中，将系统恢复到正常运行状态。

- 灾备还原配置

  通过事先指定一份配置文件作为灾备配置文件，并指定灾备配置文件作为下次启动的配置文件，则在配置文件不可恢复时，可以有效实现最初业务正常使用的目的。

操作维护安全性

USG 从设备管理、应用、日志等多个层面提供安全机制，构建操作维护的安全性：

- 管理员分权分域管理机制

USG 通过管理员组实现管理员分权分域管理机制。管理员组是操作权限的集合。不同的管理员组拥有不同的权限集。当为管理员指定所属的管理员组后，该管理员将拥有该管理员组的权限。管理员登录系统必须提供用户名和密码，登录后只能进行其权限内的操作。

- 访问通道控制

  USG 提供独立的带外管理接口，使业务和管理通道相分离。

  设备支持通过 ACL 和策略机制来保证对设备的访问控制的安全性。

  USG 与第三方网管系统之间使用安全协议进行数据通信。支持启用安全协议的服务，如 HTTPS。支持关闭不安全协议的相关服务，如 HTTP、Telnet。

- 安全日志功能

  系统对于重要操作，包括登录、退出等都提供了安全日志功能，可以供后续系统安全审计使用。

- 用户敏感信息保护机制

  提供密码和身份认证，采用高强度的数据加密算法对敏感的用户信息数据进行加密保存。系统为每个用户分配一个密码，在为用户提供各种服务时，系统对用户密码进行校验，以保护用户信息的安全性。管理员登陆设备时，系统强制要求修改缺省的密码，以加强安全管理。

  设备可以配置专门的审计级用户用以查看 UTM 特性的敏感日志，避免用户数据泄露。

- 防暴力破解机制

  为防止一些未授权用户试图通过猜测管理员的用户名和密码，使用反复尝试的手段非法登录设备。USG 提供了登录失败次数检测功能，当用户的登录失败次数超过限定值时，系统会将该用户的 IP 地址加入到隔离列表，不允许该用户在锁定期间内再次访问设备。

8 技术指标

关于本章

8.1 整机指标

表8-1 系统参数和整机指标

项目	USG2210/2220/2230/2250/2260	USG5120/5150/5160	USG5530S/USG5530/5550/5560
外形尺寸（宽×深×高）	442mm×414mm×43.6mm	• USG5120：442mm×414mm×86.1mm • USG5150/5160：442mm×414mm×130.5mm	• USG5530S：442mm×560mm×43.6mm • USG5530/5550/5560：442mm×414.1mm×130.5mm
重量	裸机5.4kg，满配8kg	• USG5120：裸机6.5kg，满配13.5kg • USG5150/5160：裸机8.3kg，满配17.5kg	• USG5530S：裸机8.24kg，满配8.9kg • USG5530：裸机15.8kg，满配17.9kg • USG5550：裸机16.5kg，满配18.3kg • USG5560：裸机16.6kg，满配18.4kg
CPU	MIPS多核处理	MIPS多核处理器，主频1GHz	MIPS多核处理器，主频950MHz

项目	USG2210/2220/2230/2250/2260	USG5120/5150/5160	USG5530S/USG5530/5550/5560
	器，主频 750MHz		
内存	2GB	2GB	4GB
NVRAM	512KB(Flash 中)	256KB	512KB
Flash Memory	64MB	64MB	64MB
CF 卡	不支持	不支持	2GB
Micro SD 卡	标配 2GB 容量 Micro SD 卡	标配 2GB 容量 Micro SD 卡	不支持
输入额定电压	AC：100V～240V（50/60Hz） DC：-48V～-60V	AC：100V～240V（50/60Hz） DC：-48V～-60V	AC：100V～240V （50/60Hz） DC：-48V～-60V
电源最大功率	100W	• USG5120：210W • USG5150/5160：300W	• USG5530S：150W • USG5530/5550/5560：300W

说明

- 内存是设备启动起来以后的运行环境，选取内存更大的设备可以获得更优越的性能。
- Flash 用于保存设备的启动文件及配置文件，一般容量较小，固定在设备内部。
- Micro SD 卡/CF 卡可用于保存设备的启动文件及配置文件，容量较大。可进行更换升级。

8.2 环境指标

表8-2 USG2200/5100/5500 的环境指标

项目	描述
海拔	≤2000m（长期工作温度在 0℃～45℃时）
气压	70kPa～106kPa
工作环境温度	长期：0℃～45℃ 短期：-5℃～55℃
存储环境温度	-40℃～70℃
环境相对湿度（工作和存储）	长期：10%RH～90%RH，非冷凝 短期：5%RH～95%RH，非冷凝

8.3 遵循的标准和协议

表8-3 ETS 相关标准

标准名	说明
ETS 300 019-2-2	Equipment Engineering; Environmental conditions and environmental tests for telecommunications equipment. part2-2: specification of environmental tests transportation
ETS 300 119-3	European telecommunication standard for equipment practice Part 3: Engineering requirements for miscellaneous racks and cabinets
EN 300 386 Version 1.2.1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements

表8-4 IEC 相关标准

标准名	说明
IEC 61000	Electromagnetic compatibility (EMC)

标准名	说明
IEC 61000-4-2	Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 2: Electrostatic discharge immunity test - Basic EMC publication
IEC 61000-4-3	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques; Radiated, radio-frequency, electromagnetic field immunity tes
IEC 61000-4-4	Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 4: Electrical fast transient/burst immunity test - Basic EMC publication
IEC 61000-4-5	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 5: Surge immunity test
IEC 61000-4-6	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 6: Immunity to conducted disturbances, induced by radio-frequency fields
IEC 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits; Limits for harmonic current emissions (equipment input current <kleiner =>16 A per phase)
IEC 61000-3-3	Electromagnetic compatibility (EMC) - Part 3: Limits; section 3: Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current <kleiner =>16 A
IEC 62151	Safety of equipment electrically connected to a telecommunication network

表8-5 ISO 相关标准

标准名	说明
ISO/IEC 11801	Information technology - Generic cabling for customer premises
ISO/IEC 15802-2	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 2: LAN/MAN management

表8-6 CISPR 相关标准

标准名	说明
CISPR 22	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement

表8-7 ITU-T 相关标准

标准名	说明
I.430	[I.430] Recommendation I.430 (11/95) - Basic user-network interface - Layer 1 specification
I.431	[I.431] Recommendation I.431 (03/93) - Primary rate user-network interface - Layer 1 specification

表8-8 IEEE 相关标准

标准名	说明
IEEE802.3	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification
IEEE802.3u	Media Access Control (MAC) parameters, physical Layer, medium attachment units, and repeater for 100 Mb/s operation, type 100Base-T
IEEE802.1D	Media Access Control (MAC) Bridges
IEEE802.3af	DTE Power via MDI

表8-9 国家相关标准

标准名	说明
YDN028-1997	SDH 光缆系统及设备的线性复用段保护——线性复用段、自愈环及其它类型结构
YDN 062-1997	PDH 通道、段和传输系统及 SDH 通道和复用段的故障检测和定位程序
GB/T 13543-92	数字通信设备环境试验方法
GB 2421-89	电工电子产品基本环境试验规程总则
GB 2423.1-89	电工电子产品基本环境试验规程试验 A：低温试验方法
GB 2423.2-89	电工电子产品基本环境试验规程试验 B：高温试验方法
GB/T 2423.3-93	电工电子产品基本环境试验规程试验 Ca：恒定湿热试验方法
GB/T 2423.5-1995	电工电子产品环境试验 第二部分：试验方法试验 Ea 和导则：冲击
GB/T 2423.6-1995	电工电子产品环境试验 第二部分：试验方法试验 Eb 和导则：碰撞
GB 2423.9-89	电工电子产品基本环境试验规程试验 Cb：设备用恒定湿热试验方法

标准名	说明
GB/T 2423.10-1995	电工电子产品环境试验 第二部分：试验方法试验 Fc 和导则：振动（正弦）
GB 2423.22-87	电工电子产品基本环境试验规程 试验 N：温度变化试验方法
GB 2423.43-1995	电工电子产品环境试验 第二部分：试验方法 元件、设备和其他产品在 冲击（Ea）、碰撞（Eb）、振动（Fc 和 Fd）和稳态加速度（Ga）等动力学试验中的安装要求和导则
GB2424.1-89	电工电子产品基本环境试验规程 高温低温试验导则
GB/T2424.2-93	电工电子产品基本环境试验规程 湿热试验导则
GB2424.13-81	电工电子产品基本环境试验规程 温度变化试验导则
SJ2170-82～ SJ2175-82	一般电子产品运输包装基本试验方法
SJ 3213-89～ SJ 3215-89	一般电子产品运输包装基本试验方法
SJ/Z 3216-89	电子产品防护、包装和装箱等级
GB 3873-83	通信设备产品包装通用技术条件
GB/T 4857.1-92	包装、运输包装件试验时各部位的标示方法
GB/T 14013-92	移动通信设备 运输包装
GB191-1990	包装储运图示标志
GB6388-1986	运输包装收发货标志
GB/T 13426-1992	数字通信设备的可靠性要求和试验方法

9 选购指南

关于本章

9.1 主机选购

USG5500 根据 CPU、内存、Flash 的大小、MIC/DMIC 和 FIC/DFIC 插槽数分为如表 9-1 所示的几种型号。

表9-1 USG5500 主机选购一览表

主机型号	CPU	内存	Flash	CF卡	MIC/DMIC 插槽	FIC/DFIC 插槽
USG5530S	950 MHz	4GB	64MB	2GB	0/0	2/1
USG5530	950 MHz	4GB	64MB	2GB	2/1	6/4
USG5550	950 MHz	4GB	64MB	2GB	2/1	5/3
USG5560	950 MHz	4GB	64MB	2GB	2/1	5/3

USG2200/5100 根据 CPU、内存、Flash 的大小、MIC 和 FIC 插槽数分为如表 9-2 所示的几种型号。

表9-2 USG2200/5100 主机选购一览表

主机型号	CPU	内存	Flash	SD卡	MIC/DMIC 插槽	FIC/DFIC 插槽
USG2200	750 MHz	2GB	64MB	2GB	4/2	2/1
USG5120	1GHz	2GB	64MB	2GB	4/2	4/3
USG5150	1GHz	2GB	64MB	2GB	4/2	6/4
USG5160	1GHz	2GB	64MB	2GB	4/2	6/4

9.2 接口卡选购

USG5500

USG5500 提供的接口卡，可以单独选购，独立于主机单独发货。

接口卡选购包括两个部分，首先是选择接口卡，其次是相应的电缆/光纤。电缆/光纤应根据线路特性及接口数量在外部成套电缆中进行选购，详细情况见表 9-3。

表9-3 USG5500 扩展接口卡和光模块选购一览表

类型	名称	线缆（选配）
FIC	2×10GE 光接口卡	多模光纤、单模光纤
FIC	8×GE 电接口卡	以太网电缆
FIC	2×10GE 光口+8×GE 电口接口卡	以太网电缆、多模光纤、单模光纤
FIC	4×GE 电 Bypass 接口卡	以太网电缆
FIC	光 BYPASS 接口卡（多模或单模）	多模光纤、单模光纤
FIC	8×GE 光接口卡	多模光纤、单模光纤
DFIC	16×GE 电口+4×GE 光接口卡	以太网电缆、多模光纤、单模光纤
DFIC	18×FE 电口+2×GE 光接口卡	以太网电缆、多模光纤、单模光纤
DFIC	2×10GE 光接口卡	多模光纤、单模光纤

类型	名称	线缆（选配）
USB	USB-3G-E180 卡	-
USB	USB-3G-EC169/EC169C 卡	-
USB	USB-3G-ET128/ET128-2 卡	-
SFP 光模块	多模光收发一体模块	多模光纤
SFP 光模块	单模光收发一体模块	单模光纤

USG2200/5100

用户在选购接口卡时可从以下几个方面进行考虑：

- 当用户需要下挂多个设备，使用 VLAN 等交换特性时，可以选购 5FE 接口卡。
- 当用户需要通过上行链路连接到运营商时，可以考虑选购 E1/CE1 接口卡、ADSL2+接口卡、G.SHDSL 接口卡、FE 接口卡、GE 接口卡、SA 接口卡、3G 数据卡。
- 当用户需要使用双上行链路提供链路备份时，可以考虑选购 E1/CE1 接口卡、ADSL2+接口卡、G.SHDSL 接口卡、FE 接口卡、GE 接口卡、SA 接口卡、3G 数据卡。

表9-4 USG2200/5100 扩展接口卡和光模块选购一览表

类型	接口卡	线缆（选配）
MIC	1E1 接口卡	• E1 75 欧姆非平衡同轴电缆 • E1 120 欧姆平衡双绞线电缆
MIC	1CE1 接口卡	
MIC	1ADSL2+接口卡	电话线
MIC	1FE 接口卡	以太网电缆
MIC	5ESW 接口卡 5FSW 接口卡	以太网电缆
MIC	1SA 接口卡	1 个同异步串口
MIC	1G.SHDSL 接口卡	电话线
MIC	2G.SHDSL 接口卡	
MIC	4G.SHDSL 接口卡	
MIC	1SA 接口卡	• V.24 （DTE/DCE）电缆 • V.35 （DTE/DCE）电缆 • X.21 （DTE/DCE）电缆 • RS449 （DTE/DCE）电缆

类型	接口卡	线缆（选配）
		• RS530 DTE 电缆
MIC	MIC-3G-WCDMA 接口卡	-
MIC	MIC-3G-CDMA2000 接口卡	-
MIC	MIC-3G-TD-SCDMA 接口卡	-
MIC	WiFi 接口卡	-
DMIC	8FE+2GE 接口卡	8 个 10M/100M 以太网自协商电接口和 2 个 10M/100M/1000M 以太网自协商电接口
FIC	2E1 接口卡	• E1 75 欧姆非平衡同轴电缆 • E1 120 欧姆平衡双绞线电缆
FIC	2CE1 接口卡	
FIC	4E1 接口卡	
FIC	4CE1 接口卡	
FIC	8E1 接口卡	
FIC	8CE1 接口卡	
FIC	1GE 接口卡	以太网电缆
FIC	4GE 接口卡	以太网电缆
FIC	2FE+2FE Combo 接口卡	以太网电缆、多模光纤、单模光纤
FIC	电 Bypass 接口卡	以太网电缆
DFIC	18FE+2SFP 接口卡	以太网电缆、多模光纤、单模光纤
DFIC	16GE+4SFP 接口卡	以太网电缆、多模光纤、单模光纤
USB	USB-3G-E180 卡	-
USB	USB-3G-EC169/EC169C 卡	-
USB	USB-3G-ET128/ET128-2 卡	-
SFP 光模块	多模光收发一体模块	多模光纤
SFP 光模块	单模光收发一体模块	单模光纤