## 华为USG6000系列至中神通UTMWALL的功能迁移手册

* **更多产品迁移说明：http://www.trustcomputing.com.cn/utmwall-rom/migration**

**华为USG6000系列安全网关/NGFW**面向SOHO企业、连锁机构、营业网点、中小企业、企业的分支机构，提供高性能，全方位的下一代安全防护。该系列产品集防火墙、IPS、AV、VPN、上网行为管理等功能于一体，提供安全、灵活、便捷的一体化组网和接入解决方案。

武汉中神通信息技术有限公司历经15年的开发和用户使用形成了**中神通UTMWALL®**系列产品，有硬件整机、OS软件、虚拟化云网关等三种产品形式，OS由50多个不断增长的功能APP、32种内置日志和5种特征库组成，每个APP都有配套的在线帮助、任务向导、视频演示和状态统计，可以担当安全网关、防火墙、UTM、NGFW等角色，胜任局域网接入、服务器接入、远程VPN接入、流控审计、行为管理、安全防护等重任，具备稳定、易用、全面、节能、自主性高、扩展性好、性价比优的特点，是**云计算时代的网络安全产品**。

以下是两者之间的功能对比迁移表：

|  |  |  |  |
| --- | --- | --- | --- |
| **华为USG6000系列功能项** | **页码** | **中神通UTMWALL v1.8功能项** | **页码** |
| **一、特性变更与支持** |  | A功能简介 | 8 |
| **二、从这里开始** |  | <见下> |  |
| **下一代防火墙简介**  介绍下一代防火墙产品产生的背景与重要概念。 |  | 相似内容，可参考 |  |
| **部署场景**  设备的部署位置和部署模式影响到整网拓扑、IP地址分配以及特性选择，需要提前做好规划。 |  | 2.2 quickset初始设置 | 49 |
| **登录Web界面**  缺省情况下，设备允许管理员通过HTTPS方式登录NGFW的Web界面。 |  | B快速安装指南 | 9 |
| **熟悉Web界面的基本使用**  熟悉Web界面的一些常见元素和基本使用方法，可以帮助您更快地掌握Web界面其他功能的配置。 |  | 2.4 gui菜单界面 及帮助内容  2.8 password帐号口令  2.9 help帮助功能 | 54  62  64 |
| **场景A（三层路由网关）初始化**  在确定设备的部署场景并完成设备安装后，可以执行一系列初始化配置来使设备可以在网络中正常工作。 |  | 2.2 quickset初始设置 运行方式为NAT | 49 |
| **场景B（二层透明桥接）初始化**  通过将三层接口切换到二层模式，可以实现将设备透明植入现有网络中。 |  | 2.2 quickset初始设置 运行方式为透明网桥 | 49 |
| **场景C（双机热备）初始化**  通过两台设备进行备份，实现在一台设备故障时，另外一台设备能够迅速接替故障设备的工作，保证业务流量不中断。 |  | 3.5 failover双机热备 | 76 |
| **注册及激活License**  在线注册并激活License，获取更多功能的使用权限。 |  | 2.1 license许可证 2.7 update升级管理 | 47 60 |
| **升级特征库**  在配置内容安全功能之前，请先升级特征库。获取最新的特征库可以识别更多的应用、病毒和威胁，提高系统的安全防护能力。 |  | 2.1 license许可证 2.7 update升级管理 | 47 60 |
| **配置安全业务**  通过配置安全业务可以全面提升网络安全性，并可有效控制流量转发。 |  | **选择安全业务场景**  2.2 quickset初始设置  **配置安全区域、配置安全策略**  5.7 firewall总控策略  **管理内网用户**  8.3 usergroup用户组  **配置NAT策略**  5.6 natNAT策略 | 49  105  183  103 |
| **高级配置**  在完成基础的网络和安全业务部署之后，可以根据需要选配其他的特性。 |  | **配置策略路由**  5.7 firewall总控策略 策略路由  **通过VPN实现网络安全互联**  9 拨号接入  10 IPSEC VPN  **配置带宽策略**  5.5 qos_objQoS对象  5.4 session_obj会话对象 | 105  191  199  101  99 |
| **下一步干什么**  下一步您可以根据需要选择使用更多功能，或者通过帮助、网站、技术支持中心获得更多与本产品有关的知识。 |  | **升级系统软件**  2.7 update升级管理  **设置其他管理员**  **更多安全措施**  5.7 firewall总控策略 SYN代理  5.4 session_obj会话对象  7.7 ips_statusIPS状态  4.1 ipmacARP服务  **阅读丰富的日志与报表**  1.15 log_stat日志统计  **获取帮助**  2.9 help帮助功能 | 69  内置  105  99  174  82  45  64 |
| **三、向导**  介绍快速向导的使用方法。通过快速向导您可以快速完成设备基础配置并连接到互联网。 |  | 2.3 guide任务向导 | 52 |
| **快速向导**  快速向导将帮助您完成设备基础配置并连接到互联网。本节将分别介绍每个步骤的参数和向导的操作方法。 |  | 2.3 guide任务向导 | 52 |
| **四、面板**  通过面板可以直观、快速地查看设备的状态信息，分析设备当前的运行情况。 |  | 1.1 dashboard系统概要/仪表盘 | 17 |
| **设置状态窗口**  在面板界面有多个状态窗口，可以进行自定义设置。 |  | 1.1 dashboard系统概要/仪表盘 | 17 |
| **设备状态图**  在本窗口可以查看设备上接口和指示灯的状态信息。 |  | 1.5 nic网卡状态 | 25 |
| **设备资源信息**  在本窗口通过资源图可以查看CPU、内存、CF卡和硬盘的资源使用情况。 |  | 1.3 system_status系统状态 | 21 |
| **系统信息**  在本窗口可以查看设备的序列号、系统软件版本和设备工作状态等信息。 |  | 1.1 dashboard系统概要 | 17 |
| **接口流量统计信息**  在本窗口通过折线图展示在过去一段时间内通过接口的数据流量信息。 |  | 1.4 network_status网络状态 | 23 |
| **License信息**  在本窗口可以查看License的激活状态以及受License控制的资源的可用数量。 |  | 2.1 license许可证 | 47 |
| **告警信息**  在本窗口可以查看设备产生的告警信息。所有告警信息按产生时间顺序排列，最新的排在最上方。 |  | 1.14 log系统日志  上面框架中的滚动窗口实时显示 | 43 |
| **系统日志信息**  在本窗口可以查看设备最新产生的系统日志信息。所有系统日志信息按产生时间顺序排列，最新的排在最上方。 |  | 1.14 log系统日志 | 43 |
| **威胁日志信息**  在本窗口可以查看设备最新产生的威胁日志信息。所有威胁日志信息按产生时间顺序排列，最新的排在最上方。 |  | 7.6 logIDS日志及统计 | 172 |
| **日志系统业务存储情况**  在本窗口可以查看每类系统业务日志和报表占用硬盘的容量大小以及占用硬盘容量与总容量的比例。 |  | 1.15 log_stat日志统计 | 45 |
| **可视化管理中心**  介绍可视化管理中心的使用方法。 |  | 1.1 dashboard系统概要 | 17 |
| **五、系统**  介绍设备各种基本功能的配置，以及升级和维护的配置。 |  |  |  |
| **首次登录设备**  介绍管理员如何通过Console口和Web首次登录一台NGFW的管理员界面。 |  | B快速安装指南  2.8 password帐号口令 | 9  62 |
| **管理员**  介绍管理员、管理员界面以及管理员服务的配置方法。 |  | WEBAdmin及Console管理员  2.2 quickset初始设置 管理主机 | 49 |
| **系统时钟**  为了保证与其他设备协调工作，需要准确设置系统的时钟。 |  | 2.5 systime本地时间 | 56 |
| **License管理**  介绍申请、激活、检查、调试License的内容。 |  | 2.1 license许可证 2.7 update升级管理 | 47 60 |
| **SNMP**  简单网络管理协议SNMP是广泛用于TCP/IP网络的网络管理标准协议。SNMP提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站网管）来管理网元的方法。SNMP有SNMPv1、SNMPv2c和SNMPv3三个版本，用户可以根据情况选择同时配置一个或多个版本。 |  | 4.6 snmpSNMP服务 | 91 |
| **跨三层MAC识别**  当NGFW与内网之间通过三层网络设备相连时，配置跨三层MAC识别功能可使NGFW获取到内网PC的MAC地址。 |  | 4.2 mac3layerSNMP监控 | 84 |
| **推送信息配置**  介绍如何配置推送信息。 |  | 6.10 webfilterWEB内容过滤 内置提示  6.5 dnsfilterDNS代理过滤 | 128  117 |
| **邮件服务设置**  通过设置SMTP邮件服务器，设备可以将信息发送到指定邮箱中。 |  | 内置账号，可通过许可证设置 |  |
| **日志/告警/调试信息的输出**  介绍日志/告警/调试信息的内容和配置方法。 |  | 1.14 log系统日志 | 43 |
| **文件系统**  介绍对NGFW的文件系统进行管理的操作，以及NGFW与其他设备之间进行文件传输的配置。 |  | 1.15 log_stat日志统计  内置日志留存管理机制 | 45 |
| **NTP**  介绍NTP的基本概念、原理、配置以及应用。 |  | 2.5 systime本地时间 | 56 |
| **升级中心**  介绍如何在升级中心将特征库升级到指定版本。及时更新特征库的版本，可以提高网络安全设备的动态安全防御能力。 |  | 2.7 update升级管理 | 60 |
| **系统更新**  介绍升级系统软件和补丁软件。 |  | 2.7 update升级管理 | 60 |
| **配置文件管理**  介绍如何使用、保存、备份、清除、比较以及查看配置文件。 |  | 2.6 backup配置管理 | 58 |
| **重启系统**  在系统升级或修改设备重大配置后，通常需要重新启动系统，以便最新配置生效。 |  | 1.2 func功能统计 重启关闭 | 19 |
| **NQA**  介绍了NQA的基本原理、多种测试情况和通用参数，并提供了配置举例。 |  | 1.13 nettool测试工具 | 41 |
| **LLDP**  LLDP提供了一种链路层网络的发现方式，用于跟踪和快速掌握二层网络的拓扑变化。 |  | <本版本暂无>  可用ping、snmp等代替 |  |
| **PMTU**  通过探测PMTU，找到从源端到目的端路径上使报文不分片的所有接口中的最小MTU值。 |  | <本版本暂无>  可用第三方工具软件代替 |  |
| **NetStream**  介绍NetStream的基本概念、原理以及如何实现和应用。 |  | <本版本暂无>  与4.5 netflowNetflow探针类似 | 89 |
| **敏捷网络**  介绍敏捷网络的基本概念、NGFW在敏捷网络中的配置方法和使用限制。 |  | <本版本暂无>  可通过2.6 backup配置管理保存配置并上传到新设备上，再恢复配置 | 58 |
| **六、高可靠性**  介绍了如何利用设备提升网络可靠性，以及双机热备、Bypass、Link-group、IP-link及BFD的配置方法。 |  | <见下> |  |
| **双机热备**  双机热备功能可以保证网络中主用设备出现故障时，备用设备能够平衡地接替主用设备的工作，从而实现业务的不间断运行。 |  | 3.5 failover双机热备 | 76 |
| **Bypass**  通过配置电口Bypass可以避免设备故障引起的网络通信中断，提高网络的可靠性。Bypass功能需要Bypass接口卡的支持。 |  | 需硬件主板支持 |  |
| **Link-group**  Link-group是指将多个物理接口绑定在一个逻辑组中，保证组内物理接口的状态一致性。 |  | 3.5 failover双机热备 | 76 |
| **IP-link**  IP-Link主要用于业务链路正常与否的自动侦测，可以检测到与设备不直接相连的链路状态。 |  | 3.1 nic网卡设置 网关IP探测  5.6 natNAT策略 服务器IP探测 | 67  103 |
| **BFD**  BFD是一种独立的Hello协议，可以实现轻负荷的快速故障探测功能。通过与上层协议的联动，可以让上层协议快速发现故障并进行恢复。 |  | <本版本暂无> |  |
| **七、虚拟系统**  介绍虚拟系统的配置方法。 |  | <本版本暂无>  因UTMWALL OS中每块网卡均具备全部功能，所以可以达到同样的效果，或者用虚拟云防火墙产品代替 |  |
| **八、网络**  介绍网络相关特性的内容和配置方法。 |  | 3网络设置 | 67 |
| **接口和接口对**  介绍接口和接口对的基本概念、配置过程和配置举例。 |  | 3.1 nic网卡设置 | 67 |
| **安全区域**  介绍安全区域的基本概念和配置过程。 |  | 3.1 nic网卡设置 | 67 |
| **DNS**  介绍DNS、DDNS、DNS透明代理和智能DNS的基本概念、配置过程和配置举例。 |  | 3.7 dnsDNS解析  6.5 dnsfilterDNS代理过滤 | 80  117 |
| **DHCP**  介绍DHCP的基本概念、配置过程和配置举例。 |  | 4.3 dhcpDHCP服务 3.1 nic网卡设置 DHCP方式 | 86 67 |
| **DHCPv6**  介绍DHCPv6的基本概念、配置过程和配置举例。 |  | <本版本暂无> |  |
| **链路聚合**  介绍链路聚合的基本概念、配置过程和配置举例。 |  | 3.2 bonding链路聚合 | 70 |
| **PPP**  介绍PPP的基本概念和配置过程。 |  | 9 拨号接入 | 191 |
| **PPPoE**  介绍PPPoE的基本概念、配置过程和配置举例。 |  | 9.3 pppoePPPOE总体设置 | 195 |
| **MAC地址表**  介绍MAC地址表的基本概念、配置过程和配置举例。 |  | 4.1 ipmacARP服务 | 82 |
| **ARP**  介绍ARP的基本概念、配置过程和配置举例。 |  | 4.1 ipmacARP服务 | 82 |
| **VLAN**  介绍VLAN的基本概念、配置过程和配置举例。 |  | 3.3 vlanVLAN | 72 |
| **DHCP Snooping**  介绍DHCP Snooping的基本概念、配置过程和配置举例。 |  | <本版本暂无>  4.3 dhcpDHCP服务 DHCP中继 |  |
| **IPv6邻居发现**  介绍IPv6邻居发现和安全邻居发现的基本概念、配置过程和配置举例。 |  | <本版本暂无> |  |
| **IP性能**  介绍IP性能的基本概念和配置过程。 |  | 系统内置 |  |
| **九、智能选路**  当NGFW拥有多条出口链路时，智能选路功能可以动态地选择出接口，保证链路资源得到充分利用，提升用户的上网体验。 |  | 3.1 nic网卡设置 网关IP探测  3.6 route路由设置  5.1 ip_obj地址对象 ISP地址  5.7 firewall总控策略 策略路由 | 67  78  93  105 |
| **十、IP路由**  介绍IP路由的内容和配置方法。 |  | <见下> |  |
| **路由基础**  NGFW根据IP路由协议生成路由表，并根据路由表转发数据包。 |  | <参考相关描述> |  |
| **静态路由**  静态路由适用于网络拓扑结构简单的网络环境。 |  | 3.6 route路由设置 | 78 |
| **RIP**  介绍RIP的基本概念、配置过程和配置举例。 |  | 3.6 route路由设置 RIP | 78 |
| **OSPF**  介绍OSPF的基本概念、配置过程和配置举例。 |  | 3.6 route路由设置 OSPF | 78 |
| **BGP**  BGP是一种基于距离矢量的外部网关协议，着眼点在于控制路由的传播和选择最佳路由。 |  | 3.6 route路由设置 BGP | 78 |
| **IS-IS**  IS-IS协议在运营商中得到广泛的应用，是直接运行在链路层的内部网关路由协议，具有收敛速度快，分层结构清晰的特点，非常适合大规模网络。 |  | <本版本暂无> |  |
| **路由策略**  路由策略可以对发布、接收、引入的路由信息进行筛选，或者修改路由信息的属性。 |  | <参考相关描述> |  |
| **RIPng**  介绍RIPng的基本概念、配置过程和配置举例。 |  | <本版本暂无> |  |
| **OSPFv3**  介绍OSPFv3的基本概念、配置过程和配置举例。 |  | <本版本暂无> |  |
| **BGP4+**  BGP4+协议是BGP协议的扩展，提供了对IPv6网络的支持。与BGP一样，BGP4+也是用于在AS之间传递路由信息的外部网关路由协议。 |  | <本版本暂无> |  |
| **MPLS**  MPLS支持多层标签和面向连接特性。MPLS LDP协议提供了环路检测机制，可以预防LSP环路的出现。如果管理员不需要严格控制LSP建立的过程，则推荐采用LDP协议来创建LSP。 |  | <本版本暂无> |  |
| **十一、用户与认证**  介绍用户与认证的内容和配置方法。 |  | 8.2 user用户  8.1 auth认证方法  8.3 usergroup用户组  5.7 firewall总控策略 用户认证  userWEB用户门户 | 181  179  183  105 |
| **十二、对象**  介绍对象的内容和配置方法。 |  |  |  |
| **地址和地址组**  介绍地址和地址组的定义和配置方法。 |  | 5.1 ip_obj地址对象 | 93 |
| **域名组**  域名组是域名的集合，管理员可以在带宽策略中引用域名组实现基于域名的带宽策略控制。 |  | 5.1 ip_obj地址对象  事先解析域名 | 93 |
| **地区和地区组**  地区和地区组是基于地理位置划分的IP地址集合，管理员可以在策略中引用地区或地区组实现基于地区的策略控制。 |  | 5.1 ip_obj地址对象  事先收集整理 | 93 |
| **服务和服务组**  介绍服务和服务组的定义和配置方法。 |  | 5.7 firewall总控策略  直接填写目的IP及端口 | 105 |
| **应用和应用组**  NGFW上的应用识别模块能够很好的识别各种常见的应用，并对各种应用进行了详细的标识。您可以基于应用去创建策略，为不同的应用指定不同策略，实现不同应用差异化、精细化管理的目的。 |  | 6.1 specapp_basic特殊应用总体设置  6.2 netgame特殊应用功能设置 | 109  111 |
| **证书**  证书也称为数字证书，由CA（认证中心）颁发，为网络上通信的实体提供加解密、身份验证及防止抵赖等功能。 |  | 10.2 certificatIPSEC VPN本机设置  userWEB用户门户 下载证书 | 202 |
| **时间段**  介绍时间段的定义和配置方法。 |  | 5.2 shedule_obj时间对象 | 95 |
| **ACL**  介绍ACL的定义、工作机制以及配置方法。 |  | 5.7 firewall总控策略  3.4 bridge网桥设置 MAC过滤 | 105  74 |
| **IPv6 ACL**  本章介绍IPv6 ACL的定义、工作机制以及配置方法。 |  | <本版本暂无> |  |
| **十三、安全策略与配置文件**  介绍安全策略与配置文件的内容和配置方法。 |  | <见下> |  |
| **安全策略**  安全策略负责防火墙流量的转发和内容安全的一体化检测及处理。 |  | 5.7 firewall总控策略 | 105 |
| **反病毒**  反病毒特性用于保护内网的用户和服务器免受病毒威胁。 |  | 6.24 antivirus防病毒引擎 6.10 webfilterWEB内容过滤 6.14 webfilter_av_exp防病毒例外 6.16 pop3filterPOP3代理过滤 6.17 smtpfilterSMTP代理过滤 | 155 128 136 140 142 |
| **入侵防御**  入侵防御是一种安全机制。设备通过分析网络流量来检测入侵，并通过一定的响应方式实时地中止入侵行为。 |  | 7 入侵检测与防御 | 162 |
| **URL过滤**  URL（Uniform Resource Locator）过滤可以对用户访问的URL进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的。 |  | 6.4 wafWEB审计过滤 6.9 webproxy_rulesWEB代理过滤规则  6.6 dns_url_dbDNS&URL库 | 115 126  119 |
| **文件过滤**  文件过滤通过阻断特定类型的文件传输，可以降低内部网络执行恶意代码和感染病毒的风险，还可以防止员工将公司机密文件泄漏到互联网。 |  | 6.4 wafWEB审计过滤 6.9 webproxy_rulesWEB代理过滤规则 | 115 126 |
| **内容过滤**  内容过滤可以防止机密信息的泄露及违规信息的传输。 |  | 6.12 keywords_rules关键词规则  6.13 keywords_exp关键词例外 | 132  134 |
| **应用行为控制**  应用行为控制功能可以对常见的HTTP行为和FTP行为进行精细化控制。 |  | 6.4 wafWEB审计过滤 6.9 webproxy_rulesWEB代理过滤规则  6.15 ftpfilterFTP代理过滤 | 115 126  138 |
| **邮件过滤**  邮件过滤是指对邮件收发行为进行管控，包括防止垃圾邮件和匿名邮件泛滥，控制违规收发等。 |  | 6.16 pop3filterPOP3代理过滤 6.17 smtpfilterSMTP代理过滤 | 140 142 |
| **十四、SSL解密**  介绍SSL解密功能的内容和配置方法。 |  | 11.1 sslSSL接入 | 208 |
| **十五、审计策略与审计配置文件**  通过配置审计策略与审计配置文件，可以对用户的上网行为进行记录，便于管理员后续对用户的上网行为进行审查和分析。 |  | 6.3 netaudit网络审计 | 113 |
| **十六、NAT策略**  介绍NAT策略的内容和配置方法。 |  | 5.6 natNAT策略 | 103 |
| **十七、策略路由**  与单纯按照IP报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行转发的机制。 |  | 3.1 nic网卡设置 网关IP探测  3.6 route路由设置  5.1 ip_obj地址对象 ISP地址  5.7 firewall总控策略 策略路由 | 67  78  93  105 |
| **十八、带宽管理**  介绍带宽管理的内容和配置方法。 |  | 5.5 qos_objQoS对象  5.4 session_obj会话对象  5.7 firewall总控策略 | 101  99  105 |
| **十九、配额控制策略**  介绍配额控制策略的内容和配置方法。 |  | 5.3 traffic_obj流量对象  5.7 firewall总控策略 | 97  105 |
| **二十、VPN**  VPN（Virtual Private Network）即虚拟专用网。介绍了VPN的基本概念以及几种VPN的配置方法。 |  | <见下> |  |
| **VPN总论**  介绍VPN的产生背景、封装原理、优势、应用场景及选择方法等，可通过本章来选择适合的VPN类型。 |  | 相似内容，可参考 |  |
| **IPSec**  通信双方在IP层通过隧道加密方式进行通信，其优点是能够保证数据报在网络上传输时的私有性、完整性、真实性。 |  | 10 IPSEC VPN | 199 |
| **L2TP**  L2TP是对PPP模型的扩展。待访问内网服务器的用户会向LAC或LNS发起PPP连接，LAC或LNS对用户进行认证，并由LNS给认证通过的用户分配内网地址。分配到地址的用户便可以自由访问服务器资源，如同处于内网一样。 |  | <本版本暂无>  可用PPTP VPN代替 |  |
| **L2TP over IPSec**  L2TP over IPSec，即先用L2TP封装报文后再用IPSec封装，这样可以综合两种VPN的优势，通过L2TP实现用户验证和地址分配，并利用IPSec保障安全性。 |  | <本版本暂无>  可用PPTP VPN代替 |  |
| **GRE**  GRE（General Routing Encapsulation，通用路由封装）是对某些网络层协议的报文进行封装，使这些被封装的报文能够在另一网络层协议中传输。 |  | <本版本暂无>  可用PPTP VPN代替 |  |
| **DSVPN**  DSVPN用于在Hub-Spoke组网方式下，为分支与分支之间建立动态的VPN隧道，实现分支用户之间的直接互访。 |  | <本版本暂无> |  |
| **BGP/MPLS IP VPN**  BGP/MPLS IP VPN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。 |  | <本版本暂无> |  |
| **二十一、SSL VPN**  介绍了SSL VPN（Secure Sockets Layer VPN）的内容和配置方法。 |  | 11.1 sslSSL接入  11.2 sslvpnSSLVPN总体设置 | 208  210 |
| **二十二、安全防护**  介绍安全防护的内容和配置方法。 |  | 5.7 firewall总控策略 帮助内容 | 105 |
| **攻击防范**  NGFW的攻击防范功能能够检测出多种类型的网络攻击，并能采取相应的措施保护内部网络免受恶意攻击，保证内部网络主机的正常运行。 |  | 5.7 firewall总控策略 内置 | 105 |
| **黑名单**  如果认为某个用户/IP地址不可信时，可以将该用户/IP地址加入黑名单，设备将丢弃来自或发往这些用户/IP地址的所有报文，从而达到保护网络安全的目的。 |  | 5.1 ip_obj地址对象  Blocked\_Client及Blocked\_Server 7.7 ips_statusIPS状态 | 93  174 |
| **IP-MAC绑定**  将IP地址与MAC地址进行绑定是防范IP地址冒用以及ARP欺骗等攻击的重要手段。 |  | 4.1 ipmacARP服务 | 82 |
| **应用层包过滤（ASPF）**  由于某些特殊应用会在通信过程中临时协商端口号等信息，所以需要设备通过检测报文的应用层数据，自动获取相关信息并创建相应的会话表项，以保证这些应用的正常通信。这个功能称为ASPF（Application Specific Packet Filter）。 |  | 5.6 natNAT策略  ALG功能 | 103 |
| **配置基于MAC地址的包过滤**  基于MAC地址的包过滤用于控制接口收到的以太网帧。配置基于MAC地址的包过滤可以通过屏蔽主机MAC地址来防止ARP攻击，以及根据协议类型来控制报文的通过。 |  | 5.7 firewall总控策略  3.4 bridge网桥设置 MAC过滤 | 105  74 |
| **URPF**  使用单播逆向路径转发URPF（Unicast Reverse Path Forwarding）技术可以解决源地址欺骗造成的网络安全问题。 |  | 5.7 firewall总控策略  SYN代理 | 105 |
| **GTP**  GTP是用于GPRS网络中GSN节点之间的接口协议，通过GTP协议实现GPRS网络中分组数据的传输。通过在GPRS网络中部署NGFW设备，为GPRS网络中分组数据提供安全防护。 |  | <本版本暂无> |  |
| **IDS联动**  IDS联动能够增强网络的安全性，加强防火墙设备的入侵检测和分析能力。 |  | 7.7 ips_statusIPS状态  手工或程序调用添加、删除阻拦的IP | 174 |
| **终端安全管理（TSM联动）**  介绍终端安全管理的基本概念、配置过程和配置举例。 |  | 7.7 ips_statusIPS状态  手工或程序调用添加、删除阻拦的IP | 174 |
| **二十三、IP组播**  本章介绍了产品支持的组播特性和配置，包括IGMP、PIM、MSDP以及组播路由与转发的配置方法。 |  | 系统内置 |  |
| **二十四、IPv6过渡技术**  介绍IPv6过渡技术的内容和配置方法。 |  | <本版本暂无> |  |
| **二十五、监控**  介绍了监控的内容和配置方法。 |  | 1状态统计 | 16 |
| **日志和报表**  管理员可以通过查看日志和报表来获知当前使用网络的用户、应用、安全事件以及流经网络的通信流量特征，并根据日志详情和报表统计分析结果进行相应的防护控制。 |  | 1.15 log_stat日志统计 | 45 |
| **流量地图**  流量地图宏观展现流量在全球的分布态势，还可以具体查看流量排名、大小、走向、具体源/目的IP地址等信息，为管理员进一步采取措施提供依据。 |  | 1.10 active_host在线主机 | 35 |
| **威胁地图**  威胁地图宏观展现威胁分布态势，可以查看发起攻击和被攻击的地区分及布及详细攻击信息，为管理员进一步采取措施提供依据。 |  | 7.6 logIDS日志及统计 | 172 |
| **会话表与长连接**  会话表是一个记录TCP、UDP、ICMP等协议连接状态，实现报文正常转发的重要表项。长连接是保持部分特殊会话超长存活的手段。 |  | 1.11 session_status会话状态 | 37 |
| **Server-map表**  由于会话表对哪些报文属于同一条流量的标准过于严格，会导致一些特殊协议不能正确匹配会话表。Server-map表可以解决这一问题。 |  | 1.11 session_status会话状态 | 37 |
| **系统统计**  介绍了查看系统统计的Web和CLI配置方法。 |  | 1.1 dashboard系统概要 | 17 |
| **系统诊断**  介绍了系统诊断的内容和使用方法。 |  | 1.13 nettool测试工具 | 41 |

**参考文件：**

1. HUAWEI USG6000系列 & NGFW Module 产品文档 04 管理员指南

http://support.huawei.com/ehedex/hdx.do?docid=DOC1000054336&lang=zh

2. 中神通UTMWALL网关管理员手册  
http://www.trustcomputing.com.cn/utmwall-rom/UTMWALL\_v1.9\_Manual\_CN\_20150331.pdf