## 网康NGFW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**

**网康下一代防火墙（NGFW）**是一款可以全面应对应用层威胁的高性能防火墙。通过深入洞察网络流量中的用户、应用和内容，并借助全新的高性能单路径异构并行处理引擎，NGFW能够为用户提供有效的应用层一体化安全防护，帮助用户安全地开展业务并简化用户的网络安全架构。应该是防火墙+IDP组合的产品。

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：

|  |  |  |  |
| --- | --- | --- | --- |
| **网康NGFW v1.0功能项** | **页码** | **中神通UTMWALL v1.8功能项** | **页码** |
| **2. 系统工作环境** | 7  | B快速安装指南 | 9 |
| 2-1 虚拟线模式 | 7  | 硬件设备BIOS设置 | 9 |
| 2-2 Vlan模式  | 7 | 3.3 vlanVLAN | 72 |
| 2-3 网关模式 | 8  | B快速安装指南2.2 quickset初始设置 | 99 |
| 2-4 NAT模式  | 8 | B快速安装指南2.2 quickset初始设置 | 99 |
| 2-5 镜像模式 | 8  | B快速安装指南2.2 quickset初始设置 | 99 |
| **3. 系统登陆**  | 10 | B快速安装指南 | 9 |
| 3-1-1 界面登录 | 10  | B快速安装指南 | 9 |
| 3-1-2 受限shell登录 | 12  | B快速安装指南 | 9 |
| 3-2 系统功能简介  | 15 | A功能简介 | 8 |
| 3-1-1 系统监控 | 15  | 1.1 dashboard系统概要/仪表盘 | 17 |
| 3-1-2 应用分析 | 15  | 1.9 specapp_state应用状态 | 33 |
| 3-1-3 数据中心 | 15  | 1.15 log_stat日志统计 | 45 |
| 3-1-4 策略配置 | 16  | 5.7 firewall总控策略 | 105 |
| 3-1-5 网络配置 | 16  | 3.1 nic网卡设置3.3 vlanVLAN | 6772 |
| 3-1-6 用户管理 | 16  | 8.2 user用户8.3 usergroup用户组 | 181183 |
| 3-1-7 系统管理 | 16  | 2.5 systime本地时间 | 56 |
| **4. 系统监控**  | 17 | 1状态统计 | 16 |
| 4-1 应用监控 | 18  | 1.9 specapp_state应用状态 | 33 |
| 4-1-1 应用风险系数  | 18 | 1.9 specapp_state应用状态 | 33 |
| 4-1-2 Top应用 | 19  | 1.1 dashboard仪表盘 热门应用统计 | 17 |
| 4-1-3 Top高风险应用  | 20 | 1.1 dashboard仪表盘 热门应用统计 | 17 |
| 4-1-4 设备接口吞吐  | 21 | 1.5 nic网卡状态 | 25 |
| 4-1-5 接口监控 | 22  | 1.4 network_status网络状态 | 23 |
| 4-1-6 IP流量排名  | 22 | 1.10 active_host在线主机 | 35 |
| 4-2 系统监控 | 23  | 1.3 system_status系统状态 | 21 |
| 4-2-1 基本信息 | 23  | 1.1 dashboard系统概要/仪表盘 | 17 |
| 4-2-2 系统资源 | 24  | 1.1 dashboard系统概要/仪表盘 | 17 |
| 4-3 日志  | 25 | 1.14 log日志操作 | 43 |
| 4-3-1 威胁日志 | 25  | 7.6 logIDS日志 | 172 |
| 4-3-2 URL日志 | 25  | 6.4 wafWEB审计过滤 WEB审计日志 | 115 |
| 4-3-3 告警日志 | 26  | 1.14 log系统日志 | 43 |
| **5. 应用分析ACC** | 28  | 1.9 specapp_state应用状态 | 33 |
| 5-1 应用排名 | 28  | 1.9 specapp_state应用状态 | 33 |
| 5-2 网址排名 | 29  | 6.4 wafWEB审计过滤 WEB审计日志统计 | 115 |
| 5-3 威胁排名 | 30  | 7.6 logIDS日志 | 172 |
| 5-4 数据的钻取 | 31  | 1.15 log_stat日志统计 | 45 |
| 5-5 设置过滤条件  | 32 | 1.15 log_stat日志统计 | 45 |
| 5-6 界面工具条的使用 | 33  | 1.15 log_stat日志统计 | 45 |
| 5-7 应用系数 | 33  | 1.9 specapp_state应用状态 | 33 |
| 5-8 与日志的关联  | 33 | 1.15 log_stat日志统计 | 45 |
| **6. 数据中心**  | 35 | 1.15 log_stat日志统计 | 45 |
| 6-1 统计  | 35 |
| 6-1-1 汇总概览 | 35  |
| 6-1-2 应用对比统计  | 38 |
| 6-1-3 应用趋势统计  | 39 |
| 6-1-4 威胁排名统计  | 42 |
| 6-1-5 IP对比统计  | 44 |
| 6-1-6 IP趋势统计  | 46 |
| 6-1-7 IP威胁统计  | 47 |
| 6-2 日志  | 49 |
| 6-2-1 流量日志 | 49  |
| 6-2-2 网址过滤日志  | 53 |
| 6-2-3 威胁日志 | 55  |
| 6-2-4 配置日志 | 58  |
| 6-2-5 告警日志 | 60  |
| 6-2-6 系统日志： | 63  |
| 6-2-7 用户上下线日志  | 65 |
| 6-3 监控  | 67 | 1状态统计 | 16 |
| 6-3-1 会话连接 | 67  | 1.11 session_status会话状态 | 37 |
| 6-3-2 流量通道 | 68  | 1.6 qos_statusQoS状态 | 27 |
| 6-3-3 上线用户 | 69  | 1.10 active_host在线主机 | 35 |
| **7. 安全策略**  | 71 | 10.3 gatewayIPSEC VPN网关 | 204 |
| 7-1 策略配置 | 71  | 5基础策略 | 93 |
| 7-1-1 安全策略 | 71  | 5.7 firewall总控策略 | 105 |
| 7-1-2 地址转换 | 75  | 5.6 natNAT策略 | 103 |
| 7-1-3 DOS防护 | 79  | 5.4 session_obj会话对象5.7 firewall总控策略 | 99105 |
| 7-1-4 流量管理 | 84  | 5.5 qos_objQoS对象 | 101 |
| 7-2 对象配置 | 91  | 5基础策略 | 93 |
| 7-2-1 地址对象 | 91  | 5.1 ip_obj地址对象 | 93 |
| 7-2-2 地址组对象 | 93  |
| 7-2-3 服务对象 | 94  | 5.7 firewall总控策略 | 105 |
| 7-2-4 服务组对象 | 96  |
| 7-2-5 自定义应用对象  | 97 |
| 7-2-6 应用过滤对象  | 102 | 6.1 specapp_basic特殊应用总体设置6.2 netgame特殊应用功能设置 | 109111 |
| 7-2-7 应用组对象 | 105  |
| 7-2-8 时间调度对象  | 108 | 5.2 shedule_obj时间对象 | 95 |
| 7-2-9 运营商地址对象  | 113 | 5.1 ip_obj地址对象 | 93 |
| 7-3 动作配置 | 115  | 6应用过滤 | 109 |
| 7-3-1 防病毒配置 | 116  | 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 | 155128136140142 |
| 7-3-2 入侵防御配置  | 118 | 5.7 firewall总控策略 日志项7.1 idp_basicIDP总体设置 | 105162 |
| 7-3-3 网址过滤配置  | 121 | 6.3 netaudit网络审计6.4 wafWEB审计过滤 | 113115 |
| 7-3-4 DOS防护配置  | 124 | 5.4 session_obj会话对象5.7 firewall总控策略 | 99105 |
| 7-3-5 攻击防护配置  | 126 | 5.7 firewall总控策略 | 105 |
| **8. 网络配置**  | 129 |  |  |
| 8-1 接口与区域 | 129  | 3.1 nic网卡设置 | 67 |
| 8-1-1 接口配置 | 129  | 3.1 nic网卡设置 | 67 |
| 8-2 路由  | 138 | 3.6 route路由设置 | 78 |
| 8-2-1 静态路由 | 138  |
| 8-2-2 Ospf路由 | 139  |
| 8-2-3 路由信息 | 145  |
| 8-3 高级网络 | 146  | <见下> |  |
| 8-3-1 静态ARP | 146  | 4.1 ipmacARP服务 | 82 |
| 8-3-1 ARP代理 | 147  | 4.1 ipmacARP服务 | 82 |
| 8-3-2 DHCP服务 | 147 | 4.3 dhcpDHCP服务 | 86 |
| 8-4 虚拟专用网络（VPN） | 149  | 10.1 ipsec_vpn_basicIPSEC VPN总体设置10.2 certificatIPSEC VPN本机设置10.3 gatewayIPSEC VPN网关10.4 connectionIPSEC VPN连接 | 199202204206 |
| 8-4-1 基本ipsec节点互连配置(共享密钥方式) | 149  |
| 8-4-2 数字证书方式的ipsec节点互连配置  | 152 |
| 8-4-3 一端为动态IP方式和DNS域名方式的IPSec节点互连配置 | 154  |
| 8-4-4 穿NAT方式的Ipsec节点互连配置  | 155 |
| 8-4-5 多节点方式的Ipsec节点互连配置  | 156 |
| 8-4-5 配置实例 | 156  |
| SSLVPN |  | 11.1 sslSSL接入11.2 sslvpnSSLVPN总体设置 | 208210 |
| **9. 用户管理**  | 158 | 8.1 auth认证方法8.2 user用户8.3 usergroup用户组 | 179181183 |
| 9-1 对象设置 | 158  |
| 9-1-1 位置对象  | 158 |
| 9-1-2 工具对象 | 160  |
| 9-2 用户导入 | 160  |
| 9-2-1 IP 导入  | 160 |
| 9-2-2 LDAP导入 | 165  |
| 9-2-3 网康自定义 | 178  |
| 9-3 组织管理 | 180  |
| 9-3-1 账户管理 | 180  |
| 9-4 认证管理 | 192  |
| 9-4-1 登录界面 | 192  |
| 9-4-2 第三方服务器  | 195 |
| 9-4-3 认证配置 | 199  |
| 9-4-4 认证策略 | 211  |
| **10. 系统管理**  | 215 | 2系统管理 | 47 |
| 10-1 系统配置 | 215  | 2系统管理 | 47 |
| 10-1-1 基本配置 | 215  | 2.2 quickset初始设置3.1 nic网卡设置 | 4967 |
| 10-1-2 权限配置 | 221  | 2.8 password帐号口令 | 62 |
| 10-1-3 授权与更新 | 223  | 2.1 license许可证 | 47 |
| 10-1-4 高级配置 | 230  | 硬件设备BIOS设置 |  |
| 10-2 系统维护 | 231  | 2.6 backup配置管理1.2 func功能统计 重启关闭系统 | 5819 |
| 10-2-1 系统配置维护  | 231 |

**参考文件：**

1. 网康下一代防火墙 v1.0 用户手册

http://wenku.baidu.com/view/bd11f7ceaa00b52acfc7caed.html

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