## 天融信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**

**天融信NGFW下一代防火墙产品**采用高度集成的一体化智能过滤引擎技术。其能够在一次数据拆包过程中，对数据进行并行深度检测，从而保证了协议深度识别的高效性。另外，天融信NGFW下一代防火墙产品基于八元组高级访问控制设计，除传统的五元组控制以外，实现了用户身份信息、应用程序指纹及内容特征的识别与控制，充分体现了下一代防火墙“基于用户防护”与“面向应用安全”的设计理念。

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：

|  |  |  |  |
| --- | --- | --- | --- |
| **天融信NGFW v3.3功能项** | **页码** | **中神通UTMWALL v1.8功能项** | **页码** |
| **1 前言** | 7  | A功能简介 | 8 |
| **2 网络卫士防火墙简介** | 10  | A功能简介 | 8 |
| 2.1 功能和特点 | 10  | A功能简介 | 8 |
| 2.2 工作原理 | 11  | A功能简介 | 8 |
| 2.3 工作模式 | 16  | A功能简介2.2 quickset初始设置 | 849 |
| 2.4 虚系统 | 18  | 使用UTMWALL-VM虚拟机 |  |
| **3 防火墙初始配置和管理方式** | 20  | B快速安装指南 | 9 |
| 3.1 出厂配置 | 20  | C缺省配置 | 13 |
| 3.2 工作状态 | 22  | B快速安装指南 | 9 |
| 3.3 管理方式 | 22  | B快速安装指南 | 9 |
| 3.4 通过浏览器登录防火墙 | 28  | B快速安装指南 | 9 |
| 3.5 初始配置向导 | 28  | 2.2 quickset初始设置 | 49 |
| **4 系统管理**  | 41 | 2系统管理 | 47 |
| 4.1 基本信息 | 41  | 1.1 dashboard系统概要/仪表盘 | 17 |
| 4.2 配置 | 47  | <见下> |  |
| 4.2.1 设置系统参数 | 47  | 3.7 dnsDNS解析 | 80 |
| 4.2.2 开放服务 | 49  | 3.1 nic网卡设置 | 67 |
| 4.2.3 设置系统时间 | 53  | 2.5 systime本地时间 | 56 |
| 4.2.4 SNMP  | 54  | 4.6 snmpSNMP服务 | 91 |
| 4.2.5 邮件设置 | 58  | 2.1 license许可证 | 47 |
| 4.2.6 短信设置 | 59  | 2.1 license许可证 | 47 |
| 4.2.7 WEB管理 | 61  | 2.8 password帐号口令 | 62 |
| 4.2.8 TP注册 | 62  | 本版本暂无，天融信自有产品 |  |
| 4.3 维护 | 64  | <见下> |  |
| 4.3.1 配置维护 | 64  | 2.6 backup配置管理 | 58 |
| 4.3.2 升级 | 68  | 2.7 update升级管理 | 60 |
| 4.3.3 重启 | 71  | 1.2 func功能统计 重启关闭 | 19 |
| 4.3.4 健康记录 | 71  | 1.1 dashboard系统概要 下载zst文件 | 17 |
| 4.3.5 诊断 | 72  | 1.13 nettool测试工具 | 41 |
| 4.3.6 安全服务 | 73  | 2.1 license许可证 特征库升级 | 47 |
| 4.4 配置系统管理员 | 81  | 2.8 password帐号口令 | 62 |
| **5 系统监视**  | 87 | <见下> |  |
| 5.1 连接信息 | 87  | 1.11 session_status会话状态 | 37 |
| 5.2 接口流量 | 88  | 1.5 nic网卡状态 | 25 |
| 5.3 攻击统计 | 90  | 7.6 logIDS日志 | 172 |
| 5.4 攻击排名 | 91  | 7.6 logIDS日志统计 | 172 |
| 5.5 应用统计 | 93  | 1.9 specapp_state应用状态1.8 traffic_stat流量统计 | 3331 |
| 5.6 应用排名 | 100  | 1.9 specapp_state应用状态1.10 active_host在线主机 | 3335 |
| 5.7 病毒统计 | 103  | 6.24 antivirus防病毒引擎 日志统计 | 155 |
| 5.8 病毒排名 | 105  | 6.24 antivirus防病毒引擎 日志统计 | 155 |
| **6 网络管理** | 108 | <见下> |  |
| 6.1 网络规划 | 108  | 3.1 nic网卡设置 | 67 |
| 6.2 接口设置 | 110  | 3.1 nic网卡设置3.3 vlanVLAN | 6772 |
| 6.3 二层网络 | 117  | <见下> |  |
| 6.3.1 ARP  | 118 | 4.1 ipmacARP服务 | 82 |
| 6.3.2 VLAN | 119  | 3.3 vlanVLAN | 72 |
| 6.3.3 MAC  | 123  | 4.1 ipmacARP服务 | 82 |
| 6.4 路由 | 125  | 3.6 route路由设置5.6 natNAT策略5.7 firewall总控策略 策略路由 | 78103105 |
| 6.5 接入 | 160  | <见下> |  |
| 6.5.1 ADSL | 160  | 3.1 nic网卡设置 | 67 |
| 6.5.2 虚拟线 | 163  | 硬件设备 BIOS设置 |  |
| 6.5.3 链路聚合 | 164  | 3.2 bonding链路聚合 | 70 |
| 6.5.4 802.1X认证 | 167  | 本版本暂无 |  |
| 6.5.5 VLAN-VPN | 168  | 3.3 vlanVLAN | 72 |
| 6.6 DHCP  | 169 | 4.3 dhcpDHCP服务 | 86 |
| 6.7 流量管理 | 177  | <见下> |  |
| 6.7.1 QoS | 177  | 5.5 qos_objQoS对象 | 101 |
| 6.7.2 地址统计 | 181  | 1.8 traffic_stat流量统计 | 31 |
| 6.7.3 常用端口流量统计 | 184  | 1.8 traffic_stat流量统计 | 31 |
| 6.7.4 IP连接统计 | 186  | 1.10 active_host在线主机 | 35 |
| 6.8 IP探测 | 187  | 3.1 nic网卡设置 监控缺省路由 | 67 |
| 6.9 域名解析 | 189  | 3.7 dnsDNS解析6.5 dnsfilterDNS代理过滤 | 80117 |
| **7 资源管理** | 190  | <见下> |  |
| 7.1 设置地址资源 | 190  | 5.1 ip_obj地址对象 | 93 |
| 7.2 设置属性资源 | 197  | 3.1 nic网卡设置 | 67 |
| 7.3 设置区域资源 | 200  | 3.1 nic网卡设置 | 67 |
| 7.4 设置时间资源 | 201  | 5.2 shedule_obj时间对象 | 95 |
| 7.5 设置服务资源 | 204  | 5.7 firewall总控策略 | 105 |
| 7.6 设置域名对象 | 207  | 6.7 domain_rules自定义域名规则6.4 wafWEB审计过滤 | 122115 |
| **8 用户认证** | 209  | 8用户认证 | 179 |
| 8.1 用户管理 | 210  | 8.2 user用户8.6 user_status用户状态 | 181189 |
| 8.2 用户角色设置 | 217  | 8.3 usergroup用户组 | 183 |
| 8.3 外部认证 | 222  | 8.1 auth认证方法 | 179 |
| 8.4 认证设置 | 227  | 5.7 firewall总控策略 认证选项 | 105 |
| 8.5 可信接入 | 232  | 8.3 usergroup用户组 NAC | 183 |
| **9 防火墙** | 240  | <见下> |  |
| 9.1 阻断策略 | 240  | 5.7 firewall总控策略  | 105 |
| 9.2 访问控制规则 | 243  | 5.7 firewall总控策略 1.8 traffic_stat流量统计 | 10531 |
| 9.3 访问记录 | 257  | 5.7 firewall总控策略 包过滤日志 | 105 |
| 9.4 地址转换 | 259  | 5.6 natNAT策略 | 103 |
| 9.5 IP/MAC地址绑定 | 266  | 4.1 ipmacARP服务 | 82 |
| 9.6 内容安全策略 | 269  | 6.4 wafWEB审计过滤6.8 webproxyWEB代理过滤6.15 ftpfilterFTP代理过滤6.6 dns_url_dbDNS&URL库6.16 pop3filterPOP3代理过滤6.17 smtpfilterSMTP代理过滤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6.2 netgame特殊应用功能设置 | 115124138119140142155128136111 |
| **10 内容过滤** | 282  | <见下> |  |
| 10.1 邮件过滤 | 282  | 6.16 pop3filterPOP3代理过滤6.17 smtpfilterSMTP代理过滤 | 140142 |
| 10.2 HTTP过滤 | 285  | <见下> |  |
| 10.2.1 URL过滤 | 285  | 6.4 wafWEB审计过滤6.8 webproxyWEB代理过滤6.6 dns_url_dbDNS&URL库 | 115124119 |
| 10.2.2 内容过滤 | 286  | 6.11 keywords_db关键词库6.12 keywords_rules关键词规则6.13 keywords_exp关键词例外 | 130132134 |
| 10.3 其他协议过滤 | 288  | <见下> |  |
| 10.3.1 关键字对象 | 288  | 7.5 idp_rulesIDP特征值规则 自定义 | 170 |
| 10.3.2 登录标题对象 | 290  | 6.15 ftpfilterFTP代理过滤6.16 pop3filterPOP3代理过滤6.17 smtpfilterSMTP代理过滤 | 138140142 |
| 10.4 应用端口绑定 | 291  | 6.3 netaudit网络审计5.6 natNAT策略 | 113103 |
| **11 应用识别** | 294  | <见下> |  |
| 11.1 账号过滤 | 294  | 6.18 msnMSN审计过滤6.19 qqQQ审计过滤 | 144146 |
| 11.2 自定义应用 | 296  | 5.7 firewall总控策略 7.5 idp_rulesIDP特征值规则 自定义 | 105170 |
| 11.3 主机流量分析 | 297  | 1.9 specapp_state应用状态1.10 active_host在线主机 | 3335 |
| 11.4 流量异常检测 | 297  | 5.3 traffic_obj流量对象1.10 active_host在线主机 | 9735 |
| **12 PKI设置** | 300  | <见下> |  |
| 12.1 本机证书 | 300  | 10.2 certificatIPSEC VPN本机设置 | 202 |
| 12.2 第三方CA证书 | 305  | 8.1 auth本地认证方法 | 179 |
| 12.3 本地CA策略 | 308  | 8.2 user用户 用户证书2.8 password帐号口令 管理员证书 | 18162 |
| 12.4 USB KEY  | 318  | 8.1 auth本地认证方法 | 179 |
| 12.5 远程证书认证 | 319  | 10.3 gatewayIPSEC VPN网关 | 204 |
| 12.6 证书请求 | 320  | 10.2 certificatIPSEC VPN本机设置 | 202 |
| 12.7 备份和恢复 | 325  | 2.6 backup配置管理  | 58 |
| **13 虚拟专网** | 326  | 五、远程接入篇 | 178 |
| 13.1 L2TP管理 | 326  | 本版本暂无 |  |
| 13.2 PPTP管理 | 329  | 9.1 pptp_vpnPPTP总体设置 | 191 |
| 13.3 GRE管理 | 332  | 9.1 pptp_vpnPPTP总体设置 | 191 |
| SSLVPN |  | 11.1 sslSSL接入11.2 sslvpnSSLVPN总体设置 | 208210 |
| **14 入侵防御** | 336  | 7 入侵检测与防御 | 162 |
| 14.1 主机防护 | 336  | 5.7 firewall总控策略  | 105 |
| 14.2 主机限制 | 339  | 5.4 session_obj会话对象 | 99 |
| 14.3 ANTI-DOS | 343  | 5.7 firewall总控策略 内置 | 105 |
| 14.4 防ARP欺骗 | 347  | 4.1 ipmacARP服务 | 82 |
| 14.5 防路由欺骗 | 348  | 5.7 firewall总控策略 内置 | 105 |
| 14.6 IDS联动  | 349 | 7.7 ips_statusIPS状态 调用阻拦URL | 174 |
| **15 反垃圾邮件** | 353  | 6.26 antispam防垃圾邮件引擎6.16 pop3filterPOP3代理过滤6.17 smtpfilterSMTP代理过滤 | 159140142 |
| **16 高可用性** | 360  | <见下> |  |
| 16.1 接口联动 | 360  | 3.5 failover双机热备 | 76 |
| 16.2 高可用性 | 362  | 3.5 failover双机热备 | 76 |
| 16.3 链路备份 | 372  | 3.1 nic网卡设置 监控缺省路由 | 67 |
| 16.4 服务器负载均衡 | 373  | 5.6 natDNAT策略 | 103 |
| **17 日志与报警** | 378  | <见下> |  |
| 17.1 日志设置 | 378  | 1.14 log日志操作 | 43 |
| 17.2 日志查看 | 380  | 1.15 log_stat日志统计 | 45 |
| 17.3 报警 | 383  | 1.14 log系统日志 | 43 |

**参考文件：**

1. 天融信NGFW管理手册——基础配置（416页）

ftp:// ftp.topsec.com.cn

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