## 深信服NGAF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**

**深信服下一代防火墙（Next-Generation Application Firewall）NGAF** 是面向应用层设计，能够精确识别用户、应用和内容，具备完整安全防护能力，能够全面替代传统防火墙，并具有强劲应用层处理能力的全新网络安全设备。NGAF 解决了传统安全设备在应用识别、访问控制、内容安全防护等方面的不足，同时开启所有功能后性能不会大幅下降。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：

|  |  |  |  |
| --- | --- | --- | --- |
| **深信服NGAF v5.0功能项** | **页码** | **中神通UTMWALL v1.8功能项** | **页码** |
| **第2章 控制台的使用** | 4 |  |  |
| 2.1. 登录 WebUI 配置界面 | 4 | B快速安装指南 | 9 |
| 2.2. 配置和使用  | 5 | B快速安装指南 | 9 |
| **第3章 功能说明** | 7 |  |  |
| **3.1. 运行状态** | 7 | 1状态统计 | 16 |
| 3.1.1. 系统状态 | 7 | 1.1 dashboard系统概要/仪表盘 | 17 |
| 3.1.2. 实时漏洞风险  | 16 | 7.6 logIDS日志 | 172 |
| 3.1.3. 最近安全事件 | 17 | 7.6 logIDS日志 | 172 |
| 3.1.4. 服务器安全事件 | 18 | 7.6 logIDS日志 | 172 |
| 3.1.5. 终端安全事件  | 18 | 7.6 logIDS日志 | 172 |
| 3.1.6. 最近攻击来源 | 19 | 7.6 logIDS日志 | 172 |
| 3.1.7. IP 流量排名 | 19 | 1.10 active_host在线主机 | 35 |
| 3.1.8. 用户流量排名  | 22 | 1.10 active_host在线主机 | 35 |
| 3.1.9. 应用流量排名  | 27 | 1.10 active_host在线主机1.8 traffic_stat流量统计 | 3531 |
| 3.1.10. 流量管理状态 | 28 | 1.1 dashboard仪表盘1.4 network_status网络状态 | 1723 |
| 3.1.11. DHCP 运行状态  | 30 | 4.3 dhcpDHCP服务 | 86 |
| 3.1.12. 在线用户管理 | 30 | 1.10 active_host在线主机1.11 session_status会话状态 | 3537 |
| 3.1.13. 联动封锁源 IP | 33 | 7.7 ips_statusIPS状态 | 174 |
| **3.2. 网络配置** | 34 | 3网络设置 | 67 |
| 3.2.1. 接口/区域  | 34 | 3.1 nic网卡设置 | 67 |
| 3.2.2. 路由 | 45 | 3.6 route路由设置 | 78 |
| 3.2.3. 虚拟网线  | 62 | 硬件设备BIOS设置 | 25 |
| 3.2.4. 高级网络配置 | 63 | 3.2 bonding链路聚合3.3 vlanVLAN | 7072 |
| 3.2.5. 光口 bypass 设置 | 69 | 硬件设备BIOS设置 | 67 |
| **3.3. 安全防护对象** | 70 | 7 入侵检测与防御 | 162 |
| 3.3.1. 漏洞特征识别库 | 70 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 3.3.2. WEB 应用防护特征库 | 72 | 7.5 idp_rulesIDP特征值规则6.4 wafWEB审计过滤 | 170115 |
| 3.3.3. 实时漏洞分析识别库  | 74 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 3.3.4. 数据泄密防护识别库  | 77 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 3.3.5. 僵尸网络识别规则库 | 80 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 3.3.6. 自定义规则库 | 81 | 7.5 idp_rulesIDP特征值规则 | 170 |
| **3.4. VPN** | 84 | 10 IPSEC VPN | 199 |
| 3.4.1. DLAN 运行状态  | 84 | 10.4 connectionIPSEC VPN连接 | 206 |
| 3.4.2. 基本设置  | 86 | 10.1 ipsec_vpn_basicIPSEC VPN总体设置 | 199 |
| 3.4.3. 用户管理 | 88 | 10.3 gatewayIPSEC VPN网关 | 204 |
| 3.4.4. 连接管理 | 100 | 10.4 connectionIPSEC VPN连接 | 206 |
| 3.4.5. 虚拟 IP 池 | 103 | 10.4 connectionIPSEC VPN连接 | 206 |
| 3.4.6. 外网接口设置 | 108 | 10.3 gatewayIPSEC VPN网关 | 204 |
| 3.4.7. 内网接口设置 | 109 | 10.3 gatewayIPSEC VPN网关 | 204 |
| 3.4.8. 多线路选路策略 | 110 | 5.7 firewall总控策略 | 105 |
| 3.4.9. 本地子网列表 | 112 | 10.4 connectionIPSEC VPN连接 | 206 |
| 3.4.10. 隧道间路由设置 | 113 | 3.6 route路由设置 | 78 |
| 3.4.11. 第三方对接 | 116 | 10.1 ipsec_vpn_basicIPSEC VPN总体设置 | 199 |
| 3.4.12. 通用设置 | 122 | 10.1 ipsec_vpn_basicIPSEC VPN总体设置 | 199 |
| 3.4.13. 高级设置 | 124 | 10.1 ipsec_vpn_basicIPSEC VPN总体设置 | 199 |
| SSLVPN |  | 11.1 sslSSL接入11.2 sslvpnSSLVPN总体设置 | 208210 |
| **3.5. 对象定义** | 133 | 2.2 quickset初始设置 | 49 |
| 3.5.1. ISP 地址库 | 133 | 5.1 ip_obj地址对象 | 93 |
| 3.5.2. 应用特征识别库  | 134 | 6.2 netgame特殊应用功能设置 | 111 |
| 3.5.3. 应用智能识别库 | 138 | 6.2 netgame特殊应用功能设置 | 111 |
| 3.5.4. 自定义应用 | 141 | 5.7 firewall总控策略 | 105 |
| 3.5.5. URL 分类库 | 144 | 6.6 dns_url_dbDNS&URL库 | 119 |
| 3.5.6. 服务 | 148 | 5.7 firewall总控策略 | 105 |
| 3.5.7. IP 组 | 151 | 5.1 ip_obj地址对象 | 93 |
| 3.5.8. 时间计划 | 154 | 5.2 shedule_obj时间对象 | 95 |
| 3.5.9. 文件类型组 | 157 | 6.4 wafWEB审计过滤6.9 webproxy_rulesWEB代理过滤规则 | 115126 |
| 3.5.10. 信任的证书颁发机构 | 158 | 6.8 webproxyWEB代理过滤6.9 webproxy_rulesWEB代理过滤规则 | 124126 |
| **3.6. 认证系统** | 159 | 8用户认证 | 179 |
| 3.6.1. 用户管理  | 159 | 8.2 user用户8.3 usergroup用户组 | 181183 |
| 3.6.2. 用户认证 | 203 | 8.1 auth认证方法5.7 firewall总控策略 | 179105 |
| **3.7. 防火墙** | 258 | 5.7 firewall总控策略 | 105 |
| 3.7.1. 地址转换  | 258 | 5.6 natNAT策略 | 103 |
| 3.7.2. 连接数控制 | 279 | 5.4 session_obj会话对象5.7 firewall总控策略 | 99105 |
| 3.7.3. DoS/DDoS 防护 | 281 | 5.4 session_obj会话对象5.7 firewall总控策略 | 99105 |
| 3.7.4. ARP 欺骗防御 | 291 | 4.1 ipmacARP服务 | 82 |
| **3.8. 内容安全** | 292 | 10.1 ipsec_vpn_basicIPSEC VPN总体设置 | 199 |
| 3.8.1. 应用控制策略  | 292 | 6.1 specapp_basic特殊应用总体设置 | 109 |
| 3.8.2. 病毒防御策略  | 294 | 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 |
| 3.8.3. APT 检测  | 296 | 5.3 traffic_obj流量对象 | 97 |
| 3.8.4. WEB 过滤 | 299 | 6.4 wafWEB审计过滤6.9 webproxy_rulesWEB代理过滤规则6.10 webfilterWEB内容过滤 | 115126128 |
| **3.9. IPS** | 303 | 7.1 idp_basicIDP总体设置 | 162 |
| **3.10. 服务器保护** | 306 | 5.7 firewall总控策略 | 105 |
| 3.10.1. WEB 应用防护 | 306 | 6.4 wafWEB审计过滤6.9 webproxy_rulesWEB代理过滤规则6.10 webfilterWEB内容过滤 | 115126128 |
| 3.10.2. 网站篡改防护 | 327 | 1.13 nettool测试工具第三方网站篡改防护软件 | 41 |
| **3.11. 风险发现和防护** | 332 | 第三方漏洞扫描工具 |  |
| 3.11.1. 风险分析  | 332 | 第三方漏洞扫描工具 |  |
| 3.11.2. WEB 扫描 | 338 | 1.13 nettool测试工具第三方漏洞扫描工具 | 41 |
| 3.11.3. 实时漏洞分析 | 348 | 第三方漏洞扫描工具 |  |
| **3.12. 流量管理** | 350 | 5.5 qos_objQoS对象5.7 firewall总控策略 | 101105 |
| 3.12.1. 概述 | 350 | 5.5 qos_objQoS对象 | 101 |
| 3.12.2. 流量通道匹配及优先级 | 351 | 5.5 qos_objQoS对象 | 101 |
| 3.12.3. 通道配置 | 351 | 5.5 qos_objQoS对象 | 101 |
| 3.12.4. 虚拟线路配置 | 368 | 5.5 qos_objQoS对象 | 101 |
| **3.13. 系统** | 370 | 2系统管理 | 47 |
| 3.13.1. 系统配置 | 370 | 2.6 backup配置管理 | 58 |
| 3.13.2. 管理员账号 | 376 | 2.8 password帐号口令 | 62 |
| 3.13.3. 高可用性  | 378 | 3.5 failover双机热备 | 76 |
| 3.13.4. 日志设置 | 382 | 1.15 log_stat日志统计 | 45 |
| 3.13.5. 邮件服务器 | 385 | 2.1 license许可证 | 47 |
| 3.13.6. 邮件告警  | 385 | 2.1 license许可证 | 47 |
| 3.13.7. 短信告警  | 387 | 2.1 license许可证 | 47 |
| 3.13.8. 全局排除地址 | 387 | 5.1 ip_obj地址对象 | 93 |
| 3.13.9. 页面定制 | 389 | 2.4 gui菜单界面 | 54 |
| 3.13.10. 集中管理 | 390 | 2.4 gui菜单界面 | 54 |
| **3.14. 系统维护** | 391 | 2系统管理 | 47 |
| 3.14.1. 系统更新 | 391 | 2.7 update升级管理 | 60 |
| 3.14.2. 备份与恢复 | 393 | 2.6 backup配置管理 | 58 |
| 3.14.3. 系统故障日志  | 394 | 1.14 log日志操作 | 43 |
| 3.14.4. 命令行控制台 | 396 | 1.13 nettool测试工具 | 43 |
| 3.14.5. 数据包拦截日志与直通  | 396 | 1.12 realtime_monitor实时监控 | 39 |
| 3.14.6. 远程技术支持  | 398 | QQ远程协助 |  |
| 3.14.7. 重启网关/服务 | 398 | 1.2 func功能统计 | 19 |
| **3.15. 配置向导** | 399 | 2.3 guide任务向导 | 52 |
| 3.15.1. 设备作为网关（路由模式） | 399 | 2.2 quickset初始设置2.3 guide任务向导 | 4952 |
| 3.15.2. 数据镜像（旁路模式） | 400 | 2.2 quickset初始设置  | 49 |
| 3.15.3. 不改变原有网络（网桥透明模式） | 400 | 2.2 quickset初始设置2.3 guide任务向导 | 4952 |
| 3.15.4. 用户认证 | 401 | 2.3 guide任务向导 | 52 |
| 3.15.5. 保护服务器 | 401 | 2.3 guide任务向导 | 52 |
| 3.15.6. 保护内网用户上网安全  | 402 | 2.3 guide任务向导 | 52 |
| 3.15.7. 保护内网用户上网带宽 | 403 | 2.3 guide任务向导 | 52 |

**参考文件：**

1. 深信服NGAF v5.0 用户手册（564页）

http://www.sangfor.com/product\_doc/manual/SANGFOR\_NGAF\_v5.0\_Manual\_CN\_20140120.pdf.7z

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