## NetScreen防火墙至中神通UTMWALL的功能迁移手册

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

**Netscreen防火墙**是一种高性能的硬件防火墙，与其它的硬件防火墙相比有本质的区别。其它的硬件防火墙实际上是运行在PC平台上的一个软件防火墙，而Netscreen防火墙则是由ASIC芯片来执行防火墙的策略和数据加解密，因此速度比其它防火墙要快得多。从软件特性上看Netscreen防火墙是状态检测与应用代理混合的防火墙。2008年起已经停止销售，原有设备的售后维护也将于2013年起停止。

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：

|  |  |  |  |
| --- | --- | --- | --- |
| **NetScreen防火墙功能项** | **页码** | **中神通UTMWALL v1.8功能项** | **页码** |
| **第 1 卷: 概述** | | A功能简介 | 8 |
| **第 2 卷: 基本原理** | | A功能简介 | 8 |
| 第 1 章 ScreenOS 体系结构 | 1 | A功能简介 | 8 |
| 第 2 章 区段 | 23 | 3.1 nic网卡设置 3.3 vlanVLAN | 67 72 |
| 第 3 章 接口 | 31 | <见下> |  |
| 接口类型 | 32 | 3.1 nic网卡设置 3.3 vlanVLAN | 67 72 |
| 查看接口 | 38 | 1.5 nic网卡状态 | 25 |
| 配置安全区段接口 | 39 | 3.1 nic网卡设置 | 67 |
| 创建二级 IP 地址 | 45 | 4.1 ipmacARP服务 ARP代理 | 82 |
| 回传接口 | 52 | 内置 |  |
| 接口状态更改 | 55 | 1.14 log系统日志 | 43 |
| 第 4 章 接口模式 | 73 | <见下> |  |
| 透明模式 | 74 | 2.2 quickset初始设置 透明网桥模式  2.3 guide任务向导 透明网桥接入 | 49 |
| NAT 模式 | 85 | 2.2 quickset初始设置 NAT模式  2.3 guide任务向导 NAT接入 | 49 |
| 路由模式 | 90 | 2.2 quickset初始设置 路由模式  2.3 guide任务向导 路由接入 | 49 |
| 第 5 章 为策略构建块 | 95 | <见下> |  |
| 地址 | 95 | 5.1 ip_obj地址对象 | 93 |
| 服务 | 100 | 5.7 firewall总控策略 | 105 |
| 动态 IP 池 | 128 | 5.6 natNAT策略 | 103 |
| 设置循环时间表 | 142 | 5.2 shedule_obj时间对象 | 95 |
| 第 6 章 策略 | 145 | 5.7 firewall总控策略 | 105 |
| 第 7 章 信息流整形 | 175 | 5.5 qos_objQoS对象 1.6 qos_statusQoS状态 | 101 27 |
| 第 8 章 系统参数 | 197 | <见下> |  |
| 域名系统支持 | 197 | 3.7 dnsDNS解析  4.4 ddnsDDNS服务 | 80  88 |
| 动态主机配置协议 | 205 | 4.3 dhcpDHCP服务 3.1 nic网卡设置 DHCP方式 | 86 67 |
| 以太网点对点协议 | 222 | 9.3 pppoePPPOE总体设置 | 195 |
| 许可密钥 | 229 | 2.1 license许可证 2.7 update升级管理 | 47 60 |
| 预定服务的注册与激活 | 230 | 2.1 license许可证 2.7 update升级管理 | 47 60 |
| 系统时钟 | 232 | 2.5 systime本地时间 | 56 |
| **第 3 卷: 管理** | | <见下> |  |
| 第 1 章 管理 | 1 | <见下> |  |
| 通过 Web 用户界面进行管理 | 2 | B快速安装指南 | 9 |
| 通过命令行界面进行管理 | 9 | B快速安装指南 | 9 |
| 通过 NetScreen-Security Manager 进行管理 | 20 | URL调用 |  |
| 控制管理性流量 | 25 | 3.1 nic网卡设置 | 67 |
| 管理的级别 | 29 | 系统内置 |  |
| 定义 Admin 用户 | 31 | 系统内置 |  |
| 保证管理流量的安全 | 33 | 2.8 password帐号口令 | 62 |
| 密码策略 | 46 | 2.8 password帐号口令 | 62 |
| 创建登录标题 | 48 | 2.4 gui菜单界面 | 54 |
| 第 2 章 监控安全设备 | 49 | <见下> |  |
| 储存日志信息 | 50 | 1.15 log_stat日志统计 | 45 |
| 事件日志 | 51 | 1.14 log系统日志 | 43 |
| 流量日志 | 54 | 5.3 traffic_obj流量对象 流量日志 | 97 |
| Self 日志 | 59 | 5.7 firewall总控策略 包过滤日志 | 105 |
| 下载资源恢复日志 | 61 | 2.6 backup配置管理 | 58 |
| 流量报警 | 61 | 5.3 traffic_obj流量对象 流量日志 | 97 |
| 系统日志 | 64 | 1.14 log系统日志 | 43 |
| 简单网络管理协议 | 66 | 4.6 snmpSNMP服务 | 91 |
| 用于自行生成的信息流的 VPN 通道 | 69 | 10 IPSEC VPN | 199 |
| 查看屏幕计数器 | 83 | 1.5 nic网卡状态  1.3 system_status系统状态  1.4 network_status网络状态 | 25  21  23 |
| **第 4 卷: 攻击检测和防御机制** | | <见下> |  |
| 第 1 章 保护网络 | 1 | <见下> |  |
| 攻击阶段 | 2 | 内容可参考 |  |
| 检测和防御机制 | 2 | 内容可参考 |  |
| 攻击监视 | 5 | 1.12 realtime_monitor实时监控  7.8 honeypot蜜罐检测 | 39  176 |
| 第 2 章 侦查威慑 | 7 | <见下> |  |
| IP 地址扫描 | 8 | 5.7 firewall总控策略 缺省拒绝策略 | 105 |
| 端口扫描 | 9 | 5.7 firewall总控策略 缺省拒绝策略 | 105 |
| 使用 IP 选项的网络侦查 | 10 | 5.7 firewall总控策略 缺省拒绝策略 | 105 |
| 操作系统探查 | 12 | 5.7 firewall总控策略 缺省拒绝策略 | 105 |
| 逃避技术 | 14 | 5.7 firewall总控策略 缺省拒绝策略 | 105 |
| 第 3 章 拒绝服务攻击防御 | 25 | <见下> |  |
| 防火墙 DoS 攻击 | 26 | 5.7 firewall总控策略 缺省拒绝策略 | 105 |
| 会话表泛滥 | 26 | 5.7 firewall总控策略 5.4 session_obj会话对象 | 105 99 |
| SYN-ACK-ACK 代理泛滥 | 30 | 5.7 firewall总控策略 SYN代理 | 105 |
| 网络 DoS 攻击 | 32 | 5.7 firewall总控策略 SYN代理  5.4 session_obj会话对象 | 105  99 |
| 与操作系统相关的 DoS 攻击 | 45 | 系统内置 |  |
| 第 4 章 内容监控和过滤 | 49 | <见下> |  |
| 碎片重组 | 50 | 5.7 firewall总控策略 | 105 |
| 防病毒扫描 | 53 | 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 |
| 反垃圾邮件过滤 | 81 | 6.26 antispam防垃圾邮件引擎 6.16 pop3filterPOP3代理过滤 6.17 smtpfilterSMTP代理过滤 | 159 140 142 |
| Web 过滤 | 84 | 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 |
| 第 5 章 深入检查 | 101 | <见下> |  |
| 概述 | 102 | 7 入侵检测与防御 | 162 |
| 攻击对象数据库服务器 | 105 | 7.5 idp_rulesIDP特征值规则  2.1 license许可证 | 170  47 |
| 攻击对象和组 | 111 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 攻击操作 | 120 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 攻击记录 | 131 | 7.1 idp_basicIDP总体设置 | 162 |
| 将定制服务映射到应用程序 | 133 | 7.4 idp_varIDP变量 | 168 |
| 定制的攻击对象和组 | 137 | 7.3 idp_ip_expIDP IP白名单 | 166 |
| HTTP 组件的点状封锁 | 148 | 6.4 wafWEB审计过滤 6.9 webproxy_rulesWEB代理过滤规则 | 115 126 |
| 第 6 章 入侵检测和防护 | 151 | <见下> |  |
| 有 IDP 功能的安全设备 | 152 | Netcreen专有产品 |  |
| 有 IDP 功能的设备上的信息流 | 153 | Netcreen专有做法 |  |
| 配置入侵检测和防护 | 154 | 7.1 idp_basicIDP总体设置 | 162 |
| 配置安全策略 | 161 | 5.7 firewall总控策略 | 105 |
| 使用 IDP 规则库 | 162 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 在防火墙规则中启用 IDP | 164 | 5.7 firewall总控策略 日志详细 | 105 |
| 配置 IDP 规则 | 165 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 配置免除规则 | 177 | 7.3 idp_ip_expIDP IP白名单 | 166 |
| 配置后门规则 | 181 | 7.5 idp_rulesIDP特征值规则 | 170 |
| 将设备配置为独立的 IDP 设备 | 200 | 7.1 idp_basicIDP总体设置 | 162 |
| 管理 IDP | 203 | 7.6 logIDS日志 | 172 |
| 第 7 章 可疑封包属性 | 207 | 5.7 firewall总控策略 内置 | 105 |
| **第 5 卷: 虚拟专用网** | | <见下> |  |
| 第 1 章 互联网协议安全性 | 1 | 内容可参考 |  |
| 第 2 章 公开密钥密码术 | 17 | 内容可参考 |  |
| 第 3 章 虚拟专用网准则 | 43 | 内容可参考 |  |
| 第 4 章 站点到站点的虚拟专用网 | 71 | 10 IPSEC VPN | 199 |
| 第 5 章 拨号虚拟专用网 | 147 | 9.1 pptp_vpnPPTP总体设置 | 191 |
| 第 6 章 第 2 层通道协议 | 189 | 本版本暂无，可以借鉴PPTP VPN |  |
| 第 7 章 高级虚拟专用网功能 | 213 | 10 IPSEC VPN | 199 |
| 第 8 章 自动连接虚拟专用网 | 297 | 10 IPSEC VPN | 199 |
| SSLVPN |  | 11.1 sslSSL接入  11.2 sslvpnSSLVPN总体设置 | 208  210 |
| **第 6 卷: IP 语音协议** | |  |  |
| 第 1 章 H.323 应用程序层网关 | 1 | 6.20 h323proxyH323代理  6.21 h323gwH.323网守 | 147  149 |
| 第 2 章 会话启动协议应用程序层网关 | 13 | 本版本暂无 |  |
| 第 3 章 媒体网关控制协议应用层网关 | 61 | 本版本暂无 |  |
| 第 4 章 瘦客户端控制协议应用层网关 | 75 | 本版本暂无 |  |
| **第 7 卷: 路由** | | <见下> |  |
| 第 1 章 静态路由 | 1 | 3.6 route路由设置 | 78 |
| 第 2 章 路由 | 13 | 3.6 route路由设置 | 78 |
| 第 3 章 开放最短路径优先 | 43 | 3.6 route路由设置 | 78 |
| 第 4 章 路由信息协议 | 69 | 3.6 route路由设置 | 78 |
| 第 5 章 边界网关协议 | 97 | 3.6 route路由设置 | 78 |
| 第 6 章 基于策略的路由 | 123 | 5.7 firewall总控策略 策略路由 | 105 |
| 第 7 章 组播路由 | 139 | 内置 |  |
| 第 8 章 互联网组管理协议 | 147 | 本版本暂无 |  |
| 第 9 章 协议无关组播 | 171 | 本版本暂无 |  |
| 第 10 章 ICMP 路由器发现协议 | 203 | 本版本暂无 |  |
| **第 8 卷: 地址转换** | 1 | 5.6 natNAT策略 | 103 |
| **第 9 卷: 用户认证** | | <见下> |  |
| 第 1 章 认证 | 1 | 8用户认证 | 179 |
| 第 2 章 认证服务器 | 11 | 8.1 auth认证方法 | 179 |
| 第 3 章 Infranet 认证 | 37 | 5.7 firewall总控策略 认证选项 | 105 |
| 第 4 章 认证用户 | 41 | 8.2 user用户  8.3 usergroup用户组 | 181  183 |
| 第 5 章 IKE、 XAuth 和 L2TP 用户 | 61 | 10.3 gatewayIPSEC VPN网关 | 204 |
| 第 6 章 无线接口和以太网接口的可扩展认证 | 83 | 3.1 nic网卡设置 WLAN方式 | 67 |
| **第 10 卷 : 虚拟系统** | | 使用UTMWALL-VM产品 |  |
| **第 11 卷 : 高可用性** | | 3.5 failover双机热备 | 76 |
| **第 12 卷 : WAN、 DSL、拨号和无线** | | <见下> |  |
| 第 1 章 广域网 | 1 | 本版本暂无，可使用第三方设备 |  |
| 第 2 章 数字用户线 | 61 | 3.1 nic网卡设置 PPPoE方式 | 67 |
| 第 3 章 ISP 故障切换和拨号恢复 | 103 | 3.1 nic网卡设置 监控缺省路由 | 67 |
| 第 4 章 无线局域网 | 109 | 3.1 nic网卡设置 WLAN方式 | 67 |
| **第 13 卷 : 通用分组无线业务** | | 本版本暂无 |  |
| **第 14 卷 : IPv6 双栈体系结构** | | 本版本暂无 |  |

**参考文件：**

1. 概念与范例 ScreenOS 参考指南全卷合订

http://www.juniper.net/techpubs/software/screenos/screenos6.0.0/translated/

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