## H3C SecPath U200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**

**SecPath U系列统一威胁管理产品**是H3C公司自主研发的、面向企业级用户开发的新一代专业UTM设备。 SecPath U 系列统一威胁管理产品除了具有传统的防火墙功能外，还支持虚拟设备、安全区域、入侵检测和防御、网关防病毒、防垃圾邮件、P2P 流量控制、URL 过滤等功能，且支持特征库动态更新，能够有效地保证网络安全；采用 ASPF 技术，可以对连接过程和非法操作进行监测，并协同 ACL 完成动态包过滤；支持多种 VPN 业务，提供丰富的路由能力。

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：

|  |  |  |  |
| --- | --- | --- | --- |
| **SecPath U200业务特性** | **特性说明** | **中神通UTMWALL v1.8****功能项** | **页码** |
| Web 概述  | 对防火墙功能的 Web 网管进行了整体的介绍 | B快速安装指南2.4 gui菜单界面 | 954 |
| 设备概览  | 设备概览模块可以帮助用户了解设备的状态和概要信息，如系统资源状态、设备接口信息等。  | * 1. dashboard系统概要/仪表盘

1.5 nic网卡状态 | 1725 |
| 防火墙策略配置向导  | 提供了对虚拟设备的防火墙策略的快速配置功能，可以帮助用户完成域间策略相关参数的配置。  | 2.2 quickset初始设置2.3 guide任务向导 | 4952 |
| IPSec VPN 配置向导  | IPSec VPN 策略配置向导提供了对 IPSec VPN 的快速配置功能，可以帮助用户完成 IPSec VPN 相关参数的配置。  配置中心节点  配置分支节点  配置对等节点  | 2.3 guide任务向导 IPSEC | 52 |
| 设备基本配置向导  | 设备基本配置向导可以帮助用户快速完成如下信息的配置： 基本信息  服务管理  接口 IP 地址 NAT  | 2.2 quickset初始设置 | 49 |
| 基本配置  | 基本配置模块包括如下两个功能：  设备基本信息  Web 管理  | 3.7 dnsDNS解析2.4 gui菜单界面 | 8054 |
| 日期和时间  | 时间设置特性用于在 Web 网管上显示和设置系统时间。  配置日期和时间  | 2.5 systime本地时间 | 56 |
| 接口管理  | 接口管理特性用于在 Web 网管上管理设备所有的物理接口和几种逻辑接口。  查看接口信息和接口统计信息  新建接口  修改接口信息  关闭和开启接口  | 3.1 nic网卡设置 | 67 |
| 安全域  | 安全域是一个抽象的概念，它有两种划分方式：1.按照接口划分。它可以包含三层普通物理接口和逻辑接口，也可以包括二层物理 Trunk 接口+VLAN，划分到同一个安全区域中的接口通常在安全策略控制中具有一致的安全需求。2.按照IP地址划分。根据 IP 地址划分不同的安全域，以实现按业务报文的源 IP 地址或目的 IP 地址进行安全策略控制。引入安全区域的概念之后，安全管理员将安全需求相同的接口或 IP 地址进行分类（划分到不同的区域），能够实现策略的分层管理。  创建安全域  配置安全域的成员  | 3.1 nic网卡设置5.7 firewall总控策略 缺省阻拦 | 67105 |
| 虚拟设备管理  | 虚拟设备的引入主要是为了将一个物理设备划分为多个逻辑设备来使用。创建逻辑上的虚拟设备，能够提供设备的出租业务。 创建虚拟设备  转移接口成员到虚拟设备  转移 VLAN 成员到虚拟设备  选择虚拟设备  | 使用UTMWALL-VM产品 |  |
| TR-069  | TR-069 主要应用于 DSL 接入网络环境。在 DSL 接入网络中，由于用户设备数量繁多、部署分散，并通常存在于用户侧，不易进行设备的管理和维护。TR-069 提出通过 ACS（Auto-Configuration Server，自动配置服务器）对 CPE （Customer Premise Equipment，用户设备）进行远程集中管理，解决 CPE 设备的管理困难，节约维护成本，提高问题解决效率。  | 本版本暂无 | 45 |
| 配置管理  | 配置维护功能是指用户管理设备配置，包括保存当前配置到设备上的配置文件，备份配置文件到 TFTP 服务器、从 TFTP 服务器下载配置文件到设备进行配置恢复。  配置保存  配置备份  配置恢复  | 2.6 backup配置管理 | 58 |
| 服务管理  | 服务管理模块提供了 FTP、Telnet、SSH、SFTP、HTTP 和 HTTPS 服务的使能管理功能，可以使用户只在需要使用相应的服务时使能服务，否则关闭服务。这样，可以提高系统的性能和设备的安全性，实现对设备的安全管理。  | 3.1 nic网卡设置 管理选项 | 67 |
| 软件升级  | 软件升级功能是指用户从 TFTP 服务器下载软件到设备，进行设备的软件升级。  配置软件升级  | 2.7 update升级管理 | 60 |
| 设备重启  | 设备重启功能是指用户通过 Web 网管重新启动设备。  配置设备重启  | 1.2 func功能统计 重启关闭系统 | 19 |
| 地址资源  | 地址资源分为 IP 地址资源、IP 地址组资源、MAC 地址资源和 MAC 地址组资源四种，可以被域间策略等模块所引用，作为报文匹配的条件。  配置主机地址资源  配置范围地址资源  配置子网地址资源  配置 IP 地址组资源  配置 MAC 地址资源  配置 MAC 地址组资源  导出和导入配置  | 5.1 ip_obj地址对象4.1 ipmacARP服务 | 9382 |
| 服务资源  | 服务资源定义了 IP 承载的协议类型和协议的特性（如 TCP 或 UDP 的源端口/目的端口、ICMP 协议的消息类型/消息码等），可以被域间策略等模块所引用，作为报文匹配的条件。  查看预定义服务资源  配置自定义服务资源  配置服务组资源  导出和导入配置  | 5.7 firewall总控策略  | 105 |
| 时间段资源  | 时间段资源用来定义时间段信息，并可以被 ACL（Access Control List，访问控制列表）、域间策略等模块所引用，来设置该访问控制列表中的某条规则在指定时间段定义的范围内有效。  配置时间段资源  | 5.2 shedule_obj时间对象 | 95 |
| VLAN  | VLAN 技术可以把一个 LAN 划分成多个逻辑的 LAN（即 VLAN），每个 VLAN 是一个广播域，VLAN 间不能直接互通，广播报文被限制在一个 VLAN 内。  新建 VLAN  修改 VLAN 中的端口  修改端口所属的 VLAN  | 3.3 vlanVLAN | 72 |
| MAC 地址表  | 为了转发报文，设备需要维护 MAC 地址表。MAC 地址表的表项包含了与该设备相连的设备的 MAC 地址、与此设备相连的设备的接口号以及所属的 VLAN ID。  增加 MAC 地址表项  设置 MAC 地址表项的老化时间  | 4.1 ipmacARP服务 | 82 |
| MSTP  | MSTP 可以弥补 STP 和 RSTP 的缺陷，它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。  配置 MSTP 域  配置 MSTP 全局  配置 MSTP 端口  | 本版本暂无 |  |
| INLINE 转发  | 高端设备支持二层 INLINE 转发，二层 INLINE 转发分为转发类型（Forward）、反射类型（Reflect）、黑洞类型（Blackhole）三种。  配置 INLINE 转发  | 本版本暂无 |  |
| PPPoE  | PPPoE 利用以太网将大量主机组成网络，通过一个远端接入设备连入因特网，并对接入的每个主机实现控制、计费功能。  配置 PPPoE Client  | 3.1 nic网卡设置 PPPOE方式 | 67 |
| DHCP  | DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。  配置 DHCP 服务器  配置 DHCP 中继  | 4.3 dhcpDHCP服务3.1 nic网卡设置 DHCP方式 | 8667 |
| DNS  | 域名系统（DNS，Domain Name System）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。  静态域名解析配置  动态域名解析配置  | 3.7 dnsDNS解析6.5 dnsfilterDNS代理过滤4.4 ddnsDDNS服务 | 8011788 |
| 路由信息  |  路由信息  | 3.6 route路由设置  | 78 |
| 静态路由  | 静态路由是一种特殊的路由，它由管理员手工配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。恰当地设置和使用静态路由可以改进网络的性能，并可为重要的网络应用保证带宽。  静态路由配置  | 3.6 route路由设置  | 78 |
| RIP  | RIP（Routing Information Protocol，路由信息协议）是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络中。  配置 RIP  | 3.6 route路由设置  | 78 |
| OSPF  | OSPF（Open Shortest Path First，开放最短路径优先）是 IETF 组织开发的一个基于链路状态的内部网关协议。  OSPF 配置  | 3.6 route路由设置  | 78 |
| BGP  | BGP（Border Gateway Protocol，边界网关协议）是一种用于AS（Autonomous System，自治系统）之间的动态路由协议。AS 是拥有同一选路策略，在同一技术管理部门下运行的一组路由器。  BGP 配置  | 3.6 route路由设置  | 78 |
| 组播路由  | 组播路由表由一组（S，G）表项组成，其中（S，G）表示由源 S 向组播组 G 发送组播数据的路由信息。如果路由器支持多种组播路由协议，则其组播路由表中将包括由多种协议生成的组播路由。路由器根据组播路由策略，从组播路由表中选出最优的组播路由。  配置组播路由  | 本版本暂无 |  |
| 策略路由  | 策略路由是一种依据用户制定的策略进行路由选择的机制。  创建策略路由  应用策略路由  | 5.7 firewall总控策略 策略路由 | 105 |
| IGMP  | IGMP 是 Internet Group Management Protocol（互联网组管理协议）的简称。它是 TCP/IP 协议族中负责 IP 组播成员管理的协议，用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。  配置 IGMP  | 系统内置 |  |
| PIM  | PIM 是 Protocol Independent Multicast（协议无关组播）的简称，表示可以利用静态路由或者任意单播路由协议（包括 RIP、 OSPF、IS-IS、BGP 等）所生成的单播路由表为 IP 组播提供路由。组播路由与所采用的单播路由协议无关，只要能够通过单播路由协议产生相应的组播路由表项即可。  配置 PIM  | 本版本暂无 |  |
| 主机业务流量统计  | 主机业务流量统计模块提供了在局域网中，监控主机使用各种网络服务的流量，并将流量统计结果以 Syslog 的格式上报给指定的日志主机的功能。管理员通过查看这些日志信息就可以清楚地了解局域网中每台主机使用指定网络服务的收发报文数和报文字节数。  配置主机业务流量统计  | 1.8 traffic_stat流量统计 | 31 |
| 二层转发报文统计  | 二层转发报文统计模块提供了显示设备上所有二层接口的转发统计信息的功能。  | 1.5 nic网卡状态 | 25 |
| 本地用户  | 所谓本地用户，是指在 NAS（即 UTM 设备）上设置的一组用户的集合。该集合以用户名为用户的唯一标识。  配置本地用户  | 8.2 user用户 | 181 |
| 在线用户  | 在线用户是指通过 AAA 认证后连接上线的用户。  查看在线用户  | 8.6 user_status用户状态1.10 active_host在线主机 | 18935 |
| RADIUS  | RADIUS 是一种分布式的、客户机/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰。  配置 RADIUS 服务器信息  配置 RADIUS 参数  | 8.1 auth认证方法 | 179 |
| HWTACACS  | HWTACACS 安全协议是在 TACACS 基础上进行了功能增强的一种安全协议。该协议是一种用于实现 AAA 的协议。  创建 HWTACACS 系统方案  配置 HWTACACS 服务器信息  配置 HWTACACS 参数  | 本版本暂无 |  |
| 域间策略  | 域间策略是基于 ACL（Access Control List，访问控制列表），在安全域之间实现流识别功能的。  新建域间策略规则  导出和导入配置  调整规则的匹配顺序  查看策略匹配统计信息  | 5.7 firewall总控策略  | 105 |
| NAT  | NAT是将IP数据报报头中的IP地址转换为另一个IP地址的过程。  配置地址池  配置动态地址转换  配置静态地址映射  配置接口静态地址转换  配置内部服务器  配置 DNS mapping  | 5.6 natNAT策略 | 103 |
| 应用层协议检测  | 应用层协议检测，即 ALG（Application Level Gateway，应用层网关），主要完成对应用层报文的处理。  配置应用层协议检测  | 5.6 natNAT策略 | 103 |
| ACL  | ACL即是通过配置对报文的匹配规则和处理操作来实现包过滤的功能。  新建 ACL  配置基本 ACL 规则  配置高级 ACL 规则  配置二层 ACL 规则  | 5.7 firewall总控策略  | 105 |
| ARP  | ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。目前 ARP 攻击和 ARP 病毒已经成为局域网安全的一大威胁，为了避免各种攻击带来的危害，设备提供了多种技术对攻击进行检测和解决。  免费 ARP 定时发送功能  ARP 自动扫描功能  ARP 固化功能  | 4.1 ipmacARP服务 | 82 |
| QoS  | QoS（Quality of Service，服务质量）是各种存在服务供需关系的场合中普遍存在的概念，它评估服务方满足客户服务需求的能力。  新建类  配置分类规则  新建流行为  配置流行为中的动作  新建策略  配置策略中类和流行为的对应关系  应用策略到接口  在端口上配置端口限速  配置端口带宽限制  | 5.5 qos_objQoS对象 | 101 |
| 流量监管  | 流量监管是指对进入设备的特定流量的规格进行监管，通常作用在接口入方向。当流量超出规格时，可以采取限制或惩罚措施，以保护运营商的商业利益和网络资源不受损害。  新建 CAR 列表  应用 CAR 列表到接口  | 5.3 traffic_obj流量对象1.4 network_status网络状态 | 9723 |
| 会话管理  | 会话管理是为了实现 NAT、ASPF、攻击防范等基于会话进行处理的业务而抽象出来的公共功能。  配置会话基本设置  查看会话列表  查看会话全局统计信息  配置会话统计使能状态  查看 IP 统计信息  查看安全区域统计信息  | 5.4 session_obj会话对象1.11 session_status会话状态 中断会话1.8 traffic_stat流量统计 | 993731 |
| 黑名单  | 黑名单是根据报文的源 IP 地址进行过滤的一种攻击防范方式。  启用黑名单过滤功能  手动新建黑名单表项  查看黑名单  | 5.1 ip_obj地址对象 Blocked\_Client及Blocked\_Server7.7 ips_statusIPS状态 | 93174 |
| 报文异常检测  | 报文异常检测是指设备分析通过的网络报文的特征（即报文特有的标识，如端口号、报文内容中包含的特殊字段等），若报文具有攻击性，则输出告警日志并且阻断报文通过。  配置报文异常检测  | 5.7 firewall总控策略 内置 | 105 |
| 流量异常检测  | 设备通过检测网络流量，分析异常流量的特征，能成功检测出各种泛洪攻击和网络扫描攻击，具体功能包括：ICMP Flood攻击检测、UDP Flood 攻击检测、SYN Flood 攻击检测、连接数限制和扫描攻击检测。  配置 ICMP Flood 攻击检测  配置 UDP Flood 攻击检测  配置 SYN Flood 攻击检测  配置连接数限制  配置扫描攻击检测  | 5.7 firewall总控策略 SYN代理5.4 session_obj会话对象 | 10599 |
| URPF 检查  | URPF 检查是用于防止基于源地址欺骗的网络攻击行为  配置 URPF 检查  | 5.7 firewall总控策略 内置 | 105 |
| TCP Proxy  | TCP Proxy 功能用来防止服务器受到 SYN Flood 攻击。  配置 TCP Proxy 全局参数  使能 TCP Proxy 功能  新建静态受保护 IP 表项  查看受保护 IP 表项及统计信息  | 5.7 firewall总控策略 SYN代理 | 105 |
| IDS 联动  | IDS 联动功能用来实现设备与 IDS 设备的联动  启用 IDS 联动  | 7.7 ips_statusIPS状态 调用阻拦URL | 174 |
| 入侵检测统计  | 入侵检测统计是指对报文异常检测和流量异常检测功能所检测到的攻击次数和丢包个数进行统计，以帮助用户对入侵的类型和数量进行详细的分析，制定更好的防火墙策略。  查看入侵检测统计  | 7.6 logIDS日志统计 | 172 |
| IPS AV 应用控制  | 设备除了能提供 VPN、防火墙等基本的安全功能，还实现了防火墙与 IPS（Intrusion Prevention System，入侵防御系统）、 AV（Anti-Virus，防病毒）等应用的融合及协调工作的功能。  快速配置 IPS 策略  快速配置 AV 策略  新建深度安全策略  配置应用安全策略  | 7 入侵检测与防御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 | 162155128136140142 |
| 内容过滤  | 目前设备所支持的内容过滤功能，可以阻止内部用户访问非法的网址，以及对网页内的 Java 或 ActiveX 程序进行阻断。  配置内容过滤  | 6.4 wafWEB审计过滤6.9 webproxy_rulesWEB代理过滤规则 | 115126 |
| IKE  | IKE 为 IPSec 提供了自动协商交换密钥、建立 SA 的服务，能够简化 IPSec 的使用和管理，大大简化 IPSec 的配置和维护工作。  配置 IKE 全局参数  配置 IKE 安全提议  配置 IKE DPD  配置 IKE 对等体  查看 IKE 安全联盟  | 10.1 ipsec_vpn_basicIPSEC VPN总体设置 | 199 |
| IPSec  | 是 IETF 制定的三层隧道加密协议，它为 Internet 上传输的数据提供了高质量的、可互操作的、基于密码学的安全保证。  配置 IPSec 安全提议  配置安全策略模板  配置安全策略  应用安全策略组  | 10 IPSEC VPN | 199 |
| PKI  | 公钥基础设施，通过使用公开密钥技术和数字证书来确保系统信息安全，并负责验证数字证书持有者身份的一种体系。  新建 PKI 实体  新建 PKI 域  生成 RSA 密钥对  销毁 RSA 密钥对  获取证书  申请本地证书  获取和查看 CRL  | 10.2 certificatIPSEC VPN本机设置 | 202 |
| L2TP  | L2TP（Layer 2 Tunneling Protocol，二层隧道协议）是 VPDN（Virtual Private Dial-up Network，虚拟私有拨号网）隧道协议中使用最广泛的一种协议。  启用 L2TP 功能  新建 L2TP 用户组  | 本版本暂无，可用PPTP VPN代替 |  |
| GRE  | GRE（Generic Routing Encapsulation，通用路由封装）协议是对某些网络层协议（如 IP 和 IPX）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议（如 IP）中传输。GRE 采用了 Tunnel（隧道）技术，是 VPN（Virtual Private Network）的第三层隧道协议。  配置概述  新建 GRE 隧道  | 本版本暂无，可用PPTP VPN代替 |  |
| SSLVPN |  | 11.1 sslSSL接入11.2 sslvpnSSLVPN总体设置 | 208210 |
| VRRP  | VRRP 是一种容错协议，在提高可靠性的同时，简化了主机的配置。  新建 VRRP 备份组  配置 VRRP 备份组的具体属性  | 3.5 failover双机热备 | 76 |
| 双机热备  |  双机热备概述  配置双机热备  | 3.5 failover双机热备 | 76 |
| 接口组联动  |  接口组联动概述  配置接口组联动  | 3.5 failover双机热备 | 76 |
| 日志管理  | 日志管理模块能够将系统消息或包过滤的动作产生的日志等存入缓冲区或定向发送到日志主机上。  会话日志  日志报表  | 1.15 log_stat日志统计 | 45 |
| 负载均衡  | 负载均衡将特定的业务（网络服务、网络流量等）分担给多台网络设备（包括服务器、防火墙等）或多条链路，从而提高了业务处理能力，保证了业务的高可靠性。  配置链路负载均衡  | 5.6 natDNAT策略3.1 nic网卡设置 监控缺省路由5.1 ip_obj地址对象 ISP1.4 network_status网络状态 | 103679323 |
| 内容监控  | 内容监控特性能够对用户的上网行为，如 Web 网页访问、IM（Instant Messaging，即时消息服务）应用、远程交互应用和数据库应用进行过滤或监控，并产生相应的监控日志。  | 6.3 netaudit网络审计6.18 msnMSN审计过滤6.19 qqQQ审计过滤 | 11314446 |
| 带宽管理  | 网络流量按照其用途的不同划分成不同的服务类型，例如E-Mail 服务、VoIP 服务等，对不同的服务类型实施不同的管理控制行为，称为带宽管理。  配置带宽管理  配置 BWC  | 5.5 qos_objQoS对象 | 101 |
| 协议审计  | 协议内容审计主要包括如下几个协议的审计：  HTTP 协议的审计  SMTP/POP3 协议审计  FTP 协议审计  | 6.3 netaudit网络审计 | 113 |
| 反垃圾邮件  | 反垃圾邮件检测实现对去往内网的电子邮件进行检测，并根据需要对检测到的垃圾邮件进行修改标题、丢弃、记录日志等处理，以防止垃圾邮件占用内网资源。  配置反垃圾邮件检测基本功能  配置日志输出参数  创建并应用反垃圾邮件策略  | 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 |
| 分层 QoS  | 分层 QoS 技术根据不同的段、用户、应用或业务分层次的划分出多条不同的通道，对这些通道分别进行带宽控制。每条通道上需要配置分类规则和控制策略。  新建通道  新建子通道  | 5.5 qos_objQoS对象 | 101 |

**参考文件：**

1. H3C SecPath U系列统一威胁管理产品 用户手册-5PW103

http://www.h3c.com.cn/Service/Document\_Center/IP\_Security/TYWX/SecPath\_U200/Configure/User\_Manual/H3C\_SecPath\_U\_UM-5PW103/

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