中神通 UTMWALL-OS 与华为 USG 防火墙的技术对比

项目	中神通 UTMWALL-OS	华为 USG 防火墙	说明
基础知识			
安全区域	没有安全区域的定义操作，一个网卡（包括 VLAN 网卡、VPN 网卡 ）就是一个安全区域，无需事先定义，直接在总控策略中使用网卡作为安全策略的一部分	需要事先定义，成员是接口/网卡	华为 USG 两块或多块网卡同属一个安全域，相当于中神通 UTMWALL-OS 的网桥
默认安全区域	1、默认允许所有发自防火墙自身/内部的流量 2、外部发到防火墙 IP 的流量，由管理员主机 IP 控制是否允许来源 IP 登录 WEBAdmin，由网卡设置是否允许 ping 及 WEBAdmin 3、初始设置：第一块网卡 G1 为外网网卡，第二块网卡 G2 为内网网卡，第三块网卡 G3 为 DMZ 网卡 4、总控策略：缺省全不通，根据需要添加允许的策略	Trust （内网）、DMZ、Untrust（外网）和 Local	中神通 UTMWALL-OS 的安全策略由总控策略决定，不需要配置安全区域、安全级别
安全级别	没有安全级别的定义操作，任何一块网卡连接的网络都可以连接其它网卡之后的网络，只要总控策略允许，方向是流入还是流出指的是数据包进出防火墙的方向	1、每个安全区域都必须有一个安全级别，该安全级别是唯一的，用 1～100 的数字表示，数字越大，则代表该区域内的网络越可信 2、Local 区域是 100，Trust 区域是 85，DMZ 是 50，Untrust 是 5	中神通 UTMWALL-OS 的安全策略由总控策略决定，不需要配置安全区域、安全级别

		3、报文从低级别的安全区域向高级别的安全区域流动时为入方向(Inbound)，反之为出方向(Outbound)	
状态检测	1、需要看到完整的流量并比对总控策略才能建立会话 2、会话对象的超时设置 3、每条总控策略可以设置不同的会话对象，可以有不同的超时，停用某条总控策略的状态检测不影响其它总控策略使用状态检测功能	1、需要看到完整的报文并比对安全策略才能建立会话 2、老化时间、长连接设置 3、整体开启、关闭状态检测功能	
会话表	1、会话状态中可以查看、查询、终止会话 2、ARP 状态中查看主机的 IP、MAC 地址 3、实时监控中可以显示每个报文及其对应的总控策略序号，是允许还是拒绝（丢包），用于调试排错总控策略	1、查看全部会话表 2、丢包信息查询	中神通 UTMWALL-OS 的实时监控和在线主机功能，可以更深入、细致、全面、方便地查看、分析、统计实时流量
模拟器	中神通 UTMWALL-VM 虚拟机	eNSP 模拟器	中神通 UTMWALL-VM 可以在 PC 或生产环境中使用，不仅仅是模拟器
安全策略			
基本概念	1、网卡+五元组 2、可以设置匹配顺序，缺省是 Last match 3、缺省包过滤策略是拒绝，即“除非允许否则拒绝” 4、方向是流入还是	1、安全区域+五元组 2、匹配顺序只有 First Match 3、缺省包过滤策略是拒绝	1、华为 USG 安全策略的复杂度是 n^2，需要确定来源、目的安全区域及流向，当有几十个 VLAN 接口时，安全策略将变得十分复杂

	流出指的是数据包进出防火墙的方向		2、中神通 UTMWALL-OS 安全策略的复杂度是 n，只需要确定网卡，即数据包接触防火墙的第一块网卡，方向是流入，之后由路由和“五元组”状态检测自动判断流向，相当于“发射后不管”
一体化安全策略	1、对允许的流量，再做时间控制、用户认证、MAC 地址过滤、内容审计、特殊应用过滤、QQ 账号过滤、WEB 协议过滤、WEB 内容关键词过滤、IDS/IPS、反病毒、反垃圾邮件过滤 2、功能统计中展示来源 IP 对象和包含该对象的各类安全策略的二维透视表	五元组信息 + Application（应用）、Content（内容）、Time（时间）、User（用户）、Attack（威胁）、Location（位置）6 个维度	中神通 UTMWALL-OS 可以对 VPN 隧道里的流量进行一体化安全策略过滤
ASPF（Application Specific Packet Filter）	支持 FTP、TFTP、TELNET、SQL、SIP、H.323、VOIP 等	支持 FTP、TFTP、SIP、H.323、MGCP、QQ、MSN 等	
故障排除	1、实时监控 2、会话状态 3、流量统计（按总控策略号统计流量和会话）	1、丢包统计 2、安全策略匹配统计	中神通 UTMWALL-OS 可以精确定位、查询每个数据包对应的总控策略号及允许、拒绝状态，方便故障排除
配置思路	1、“除非允许否则拒绝”，只需添加允许的策略，实现最	首先配置缺省包过滤的动作为允许通过，对业务进行调测，保证业务正常运	华为 USG 的配置思路有点绕弯，需要两次操作

	小特权 2、一般而言，允许的策略相互不矛盾，无所谓匹配顺序，方便配置总控策略 3、只需要确定流入的网卡，不需要确定来源和目的安全区域，“发射后不管”，方便配置总控策略	行；然后查看会话表，以会话表中记录的信息为匹配条件配置安全策略；最后恢复缺省包过滤的配置,再次对业务进行调测，验证安全策略是否正确	
带宽管理	QoS 对象	带宽管理	
攻击防范			
单包攻击	1、畸形报文攻击 2、扫描类攻击 3、特殊控制报文攻击	1、畸形报文攻击 2、扫描类攻击 3、特殊控制报文攻击	
SYN-flood 洪水攻击	SYN 代理	TCP 代理	
UDP 洪水攻击	1、会话对象 2、IDS/IPS	1、基于流量入接口的限流 2、基于目的 IP 的限流 3、基于目的安全区域的限流 4、基于指纹学习	
HTTP Flood 攻击	1、WEB 审计过滤（WAF） 2、WEB 代理协议过滤	HTTP 源探测	
NAT			
类型	1、来源 NAT SNAT 2、目的 NAT DNAT 3、DNS 代理	1、源 NAT 2、NAT Server 3、双向 NAT（NAT Inbound 不需要服务器设置网关） 4、域内 NAT 5、NAT 黑洞	1、服务器不设置默认网关的做法不安全 2、NAT 地址池和网卡 IP 不是一个网段不常见
匹配顺序	First match	First match	
其它特性	1、支持 NAT 地址池 2、基于来源 IP 分配不同的外网 NAT 地址 3、支持多 WAN	1、支持 NAT 地址池 2、基于来源 IP 分配不同的外网 NAT 地址 3、支持多出口 4、NAT ALG	

	4、NAT ALG 5、自动生成相应的总控策略		
其它功能			
VPN 种类	PPTP VPN IPSEC VPN SSLVPN 大地云控支持： L2TP VPN GRE VPN IKEv2 VPN OCSERV VPN SoftEther VPN SSTP VPN VPN 客户端	L2TP VPN GRE VPN IPSEC VPN IKEv2 VPN DSVPN SSLVPN	
双机热备	1、VRRP 网关热备 2、类型：主主热备、主从热备 3、基于 VLAN 的双机热备 4、配置管理 5、不需要心跳线	1、VRRP、VGMP 网关热备 2、主备备份 3、负载分担 4、配置备份 5、心跳线	
出口选路	1、多 WAN 口 SNAT 及 DNAT 2、策略路由 3、服务器负载均衡 SLB 4、链路质量探测	1、就近选路 2、策略路由 3、智能选路 4、透明 DNS 选路 5、旁挂出口选路 6、链路质量探测	
设备类型及报文处理流程	1、兼容 X86 硬件，性能由 CPU、主板、网卡、存储器等共同决定 2、参见图 8 数据包过滤流程示意图	1、对于集中式低端防火墙 USG2000/3000/5000/6000 来说，报文会被上送至一个集中的 CPU 模块（可能由多个 CPU 组成）进行处理。 2、集中式防火墙一般为盒式设备，可以插接多种扩展接口卡，但设备的总机性能恒定，即取决于该设备配置的 CPU 模块处理能力。	

中神通 UTMWALL-OS WEBAdmin 管理界面图例：

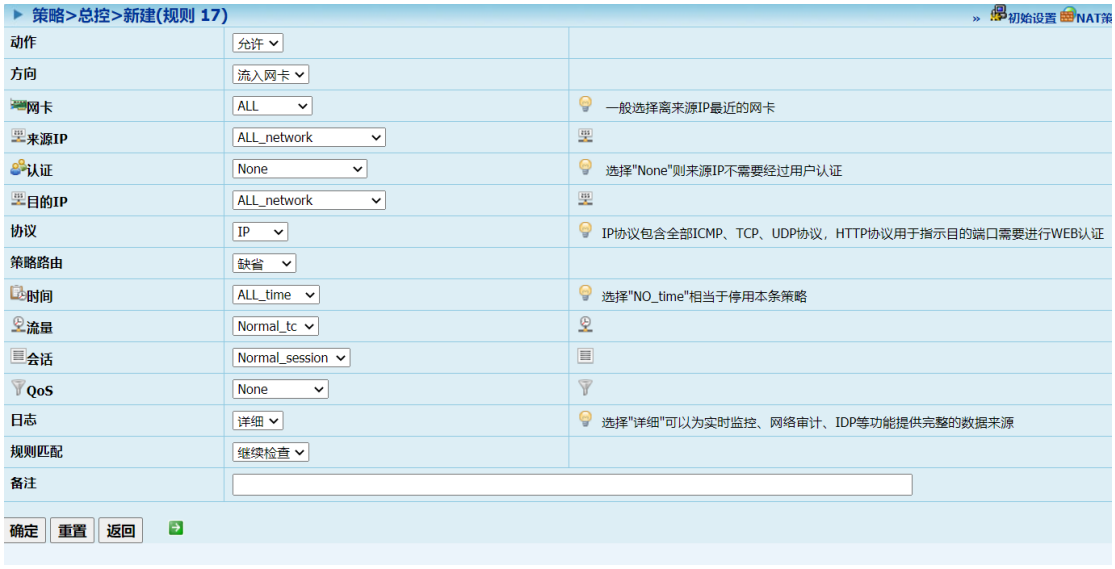
策略>总控

总共有15个记录 总控策略状态: 有效 总控功能状态: 有效

序号	动作	网卡	来源	认证	目的	协议	端口	时间	流量	会话	QoS	日志	状态	修
	丢弃	ALL	ALL_network		ALL_network	IP		ALL_time				简单		
1	允许	»G2:	USER_ip		ALL_network	IP		ALL_time	Normal_tc	Normal_session		详细	MSTH	
2	允许↑	»ALL	SUPERUSER_ip		ALL_network	IP		ALL_time	Normal_tc	Normal_session		简单	MSTH	
3	允许	»ALL	USER_ip		ALL_network	IP		ALL_time	IP_tc	IP_session		简单	MSTH	
4	允许	»G2:	USER_ip		ALL_network	TCP	1~65535	ALL_time	TCP_tc	TCP_session	TCP_qos	详细	MSTH	
5	允许	»G2:	USER_ip		ALL_network	UDP	1~65535	ALL_time	UDP_tc	UDP_session	UDP_qos	简单	MSTH	
6	允许↑	»G2:	USER_ip		ALL_network	ICMP		ALL_time	Normal_tc	ICMP_session		简单	MSTH	
7	允许	»G2:	USER_ip		ALL_network	UDP	53	ALL_time	Normal_tc	DNS_session		详细	MSTH	
8	允许	»G2:	USER_ip		ALL_network	HTTP	80	ALL_time	WEB_tc	HTTP_session		详细	MSTH	
9	允许	»G2:	USER_ip		ALL_network	TCP	443	ALL_time	SSL_tc	HTTPS_session		详细	MSTH	
10	允许	»G2:	USER_ip		FAKE80_Server	TCP	80~8081	ALL_time	FAKE80_tc	FAKE80_session	FAKE80_qos	无	MSTH	
11	允许	»G2:	USER_ip		ALL_network	TCP	110	ALL_time	Normal_tc	POP3_session		详细	MSTH	
12	允许	»G2:	USER_ip		ALL_network	TCP	25	ALL_time	Normal_tc	SMTP_session		详细	MSTH	
13	允许	»G2:	USER_ip		ALL_network	TCP	21	ALL_time	Normal_tc	FTP_session		详细	MSTH	
14	拒绝	»ALL	Blocked_Client		ALL_network	IP		ALL_time				简单		
15	拒绝	»ALL	USER_ip		Blocked_Server	IP		ALL_time				简单		

新建 删除 拷贝 粘贴 直编 全选 重置 流量统计

图 1-1 总控策略列表



策略>总控>新建(规则 17)

动作	允许	
方向	流入网卡	
网卡	ALL	一般选择离来源IP最近的网卡
来源IP	ALL_network	
认证	None	选择"None"则来源IP不需要经过用户认证
目的IP	ALL_network	
协议	IP	IP协议包含全部ICMP、TCP、UDP协议，HTTP协议用于指示目的端口需要进行WEB认证
策略路由	缺省	
时间	ALL_time	选择"NO_time"相当于停用本条策略
流量	Normal_tc	
会话	Normal_session	
QoS	None	
日志	详细	选择"详细"可以为实时监控、网络审计、IDP等功能提供完整的数据来源
规则匹配	继续检查	
备注		

确定 重置 返回

图 1-2 新建总控策略

策略>NAT

总共有2个记录 NAT策略状态: 有效 NAT功能状态: 有效

序号	转换类型	网卡	来源地址	目的地址	协议	目的端口	转换后地址	转换后端口	相关代理	时间策略	总控策略	修改
1 ↑	来源(SNAT)	G1:	USER_ip*	ALL_network	IP		G1:_ip			ALL_time	查看	
2 ↑	外网目的(DNAT)	G1:	ALL_network	G1:_ip*	TCP	80	Server1	80		ALL_time	查看	

图 2-1 NAT 策略列表

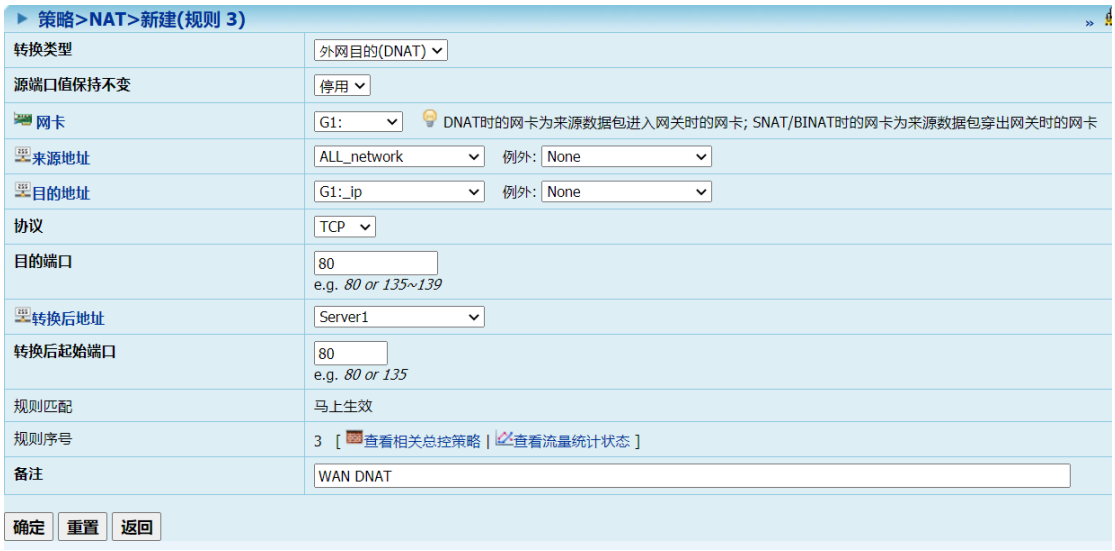


图 2-2 新建 NAT 策略

图 3 实时监控

图 4 会话状态

图 5 在线主机-流量明细

图 6-1 流量统计-流量明细

图 6-2 流量统计-规则汇总

图 7 功能统计-来源 IP 二维透视表

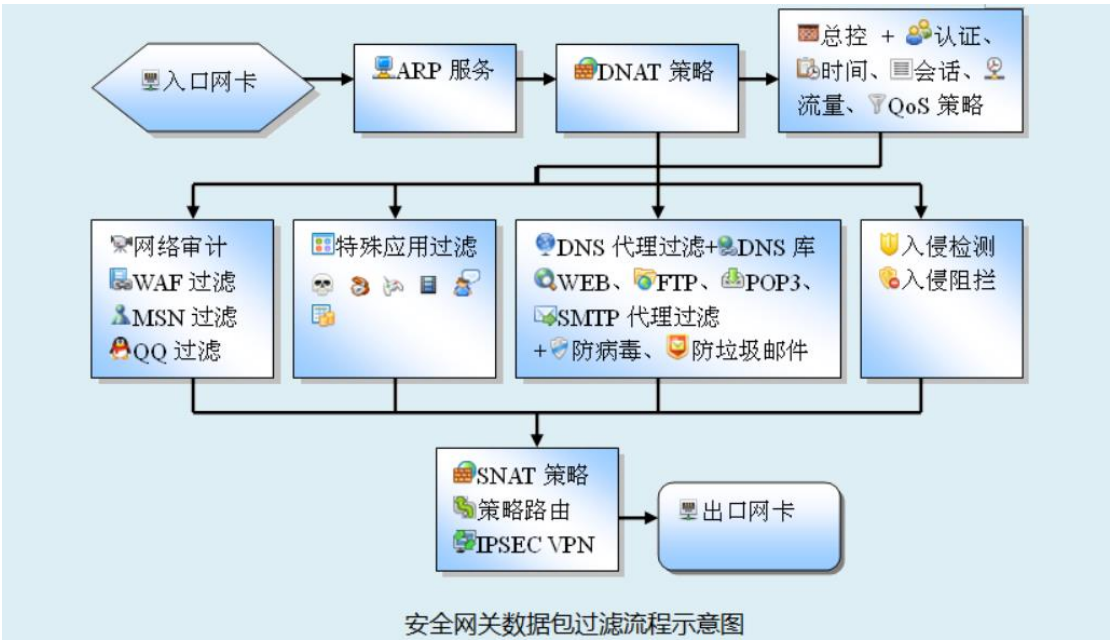


图 8 数据包过滤流程示意图

参考文件:

1、华为防火墙技术漫谈:

https://pan.baidu.com/s/1eSgQdLC

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

3、华为 USG6000 至中神通 UTMWALL 的功能迁移手册:

http://www.trustcomputing.com.cn/utmwall-rom/migration/Huawei_USG6000_UTMWALL_Migration.docx

4、华为 USG5000 至中神通 UTMWALL 的功能迁移手册：http://www.trustcomputing.com.cn/utmwall-rom/migration/Huawei_USG_UTMWALL_Migration.docx