华为工烟安全运维解决方案与中软中烟安全信息运维管理平台互通测试报告

编号：HWEBGOPLAB01C131116004

1 互通测试简介

1.1 测试背景

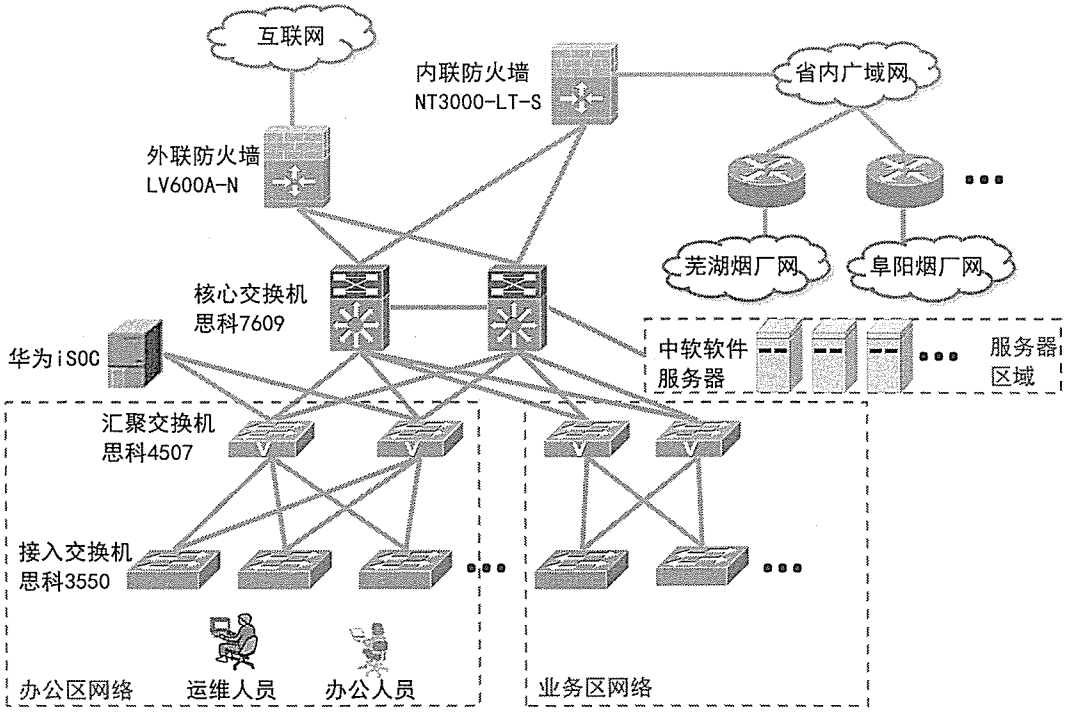
华为工烟安全运维解决方案旨在统一烟草公司的服务流程和运维入口、降低信息泄露和安全事故风险、提升烟草公司的运维效率、降低运维成本。方案与中软中烟安全信息运维管理平台系统互联互通以共同满足以上需求。

中软国际是中国大型综合性软件与信息服务企业，提供从咨询、解决方案、外包服务到IT人才培养的“端到端”软件及信息服务，目前已经覆盖政府与大型企业、制造与流通、金融与银行、保险证券、电信、高科技、公共服务、能源等多个行业。

本次测试的目的是验证中软中烟安全信息运维管理平台系统能够获取华为统一安全管控中心（iSOC）数据库中统计记录的被监控网络设备及服务器的告警及风险信息，从而满足统一运维入口，降低安全风险，提高运维效率的需求。

1.2 测试组网

下图为合肥中烟现场互通测试组网图，主要包括华为iSOC、中软中烟安全信息运维管理平台及被监控设备。被监控设备包括网络设备及服务器：网络设备包括思科防火墙5520、思科交换机6509、7609系列；服务器为IBM3650、P7系列。



2 主要互通设备及软件信息

公司名称	设备及软件名称	型号	软件版本
华为	统一安全管控中心	iSOC 3000E	V200R001C00SPC200
中软	统一运维软件	中软中烟安全信息运维管理平台	CSI-ITSM2.0

注：被监控设备主要为思科和 IBM 设备，无互通关系，这里不做列举。

3 互通主要功能测试

3.1 测试结果汇总

测试类别	测试项目	测试结果
iSOC防火墙类日志收集分析和事件告警	防火墙ARP中毒攻击事件告警	■passed □passed partly □failed □not test □block
	防火墙IP碎片攻击事件告警	■passed □passed partly □failed □not test □block
	防火墙IRP攻击失败事件告警	■passed □passed partly □failed □not test □block
	黑名单IP尝试非法访问事件告警	■passed □passed partly □failed □not test □block
	防火墙网络端口扫描事件告警	■passed □passed partly □failed □not test □block
	防火墙疑似Dos攻击事件告警	■passed □passed partly □failed □not test □block
	防火墙违反ACL策略事件告警	■passed □passed partly □failed □not test □block
iSOC交换机路由器类日志收集分析和事件告警	CGI计数程序缓存溢出事件告警	■passed □passed partly □failed □not test □block
	DNS服务器收到过大的NXT资源事件告警	■passed □passed partly □failed □not test □block
	IP碎片太小，疑似DOS攻击事件告警	■passed □passed partly □failed □not test □block
	Land攻击，目的地址和源地址相同事件告警	■passed □passed partly □failed □not test □block
	Statd缓存区溢出事件告警	■passed □passed partly □failed □not test □block
	尝试非法访问-试图通过tfp客户端或服务器更改安全策略事件告警	■passed □passed partly □failed □not test □block
	非法访问被禁止的网站事件告警	■passed □passed partly □failed □not test □block
	拒绝服务攻击-试图通过HTTP运行newdsn事件告警	■passed □passed partly □failed □not test □block
	可能的安全漏洞攻击-通过TFTP	■passed □passed partly □failed □not test □block

	传输密码文件事件告警	
	目标渗透攻击-非法用户发送邮件或发送邮件给无效的接收者事件告警	■passed □passed partly □failed □not test □block
	认证失败-主机EOU认证失败事件告警	■passed □passed partly □failed □not test □block
	设置了SYN和FIN标志的单一零散TCP数据包被发送到一个特定的主机事件告警	■passed □passed partly □failed □not test □block
iSOC服务器类日志收集分析和事件告警	登陆失败事件告警	■passed □passed partly □failed □not test □block
	密码猜解事件告警	■passed □passed partly □failed □not test □block
	SU切换事件告警	■passed □passed partly □failed □not test □block
iSOC自身主机日志收集分析和事件告警	PMCCPU利用率超过阈值事件告警	■passed □passed partly □failed □not test □block
	PMC硬盘利用率超过阈值事件告警	■passed □passed partly □failed □not test □block
中软系统获取iSOC数据库告警记录	中软读取iSOC防火墙告警记录	■passed □passed partly □failed □not test □block
	中软读取iSOC路由交换机告警记录	■passed □passed partly □failed □not test □block
	中软读取iSOC服务器告警记录	■passed □passed partly □failed □not test □block
iSOC设备风险值及风险级别计算	iSOC风险脆弱关联配置	■passed □passed partly □failed □not test □block
	iSOC设备风险识别配置	■passed □passed partly □failed □not test □block
	iSOC设备风险值和风险级别计算	■passed □passed partly □failed □not test □block
中软获取iSOC设备风险信息并计算系统风险	中软获取iSOC数据库中关于设备风险信息	■passed □passed partly □failed □not test □block
	中软计算总系统风险并保存在中软数据库中	■passed □passed partly □failed □not test □block
	中软按照地域或系统计算系统风险并保存在中软数据库中	■passed □passed partly □failed □not test □block
备注: Passed—通过 passed partly—部分通过 failed—不通过 not test—未测试 block—未实现该功能		

4 结论

本次互通测试验证了中软中烟安全信息运维管理平台系统能够获取华为统一安全管控中心（iSOC）数据库中统计记录的被监控网络设备和服务器的告警及风险信息。基本功能对接测试通过，能够满足工烟安全运维解决方案的应用需求。

公司名称：华为技术有限公司

测试人员（签字）：

公司盖章：

日期：2013.11.18

公司名称：中软国际有限公司

测试人员（签字）：

公司盖章：

日期：2013.11.18