四川科道芯国智能技术股份有限公司

关键设备审查记录表（设备）

审查日期: _____ 检查人：_____ 审核人：_____

设备名称及IP地址	所在区域	编号	检查信息	结果	备注
F1000 （10.255.3.1）	服务器机柜	1	安全策略：检查每一项防火墙规则设置的合理性，是否有达到其作用（见后附策略表）	是否正常：☐是☐否	
		2	配置文件：当前配置文件是否保存，配置文件是否有及时备份，配置文件是否存在未授权篡改	是否正常：☐是☐否	
		3	CPU，内存占用情况	CPU使用率：_____% 内存使用率：_____%	
		4	系统时钟：是否与系统时钟同步	是否正常：☐是☐否	
		5	日志：系统操作日志是否对应符合表单记录，系统运行日志是否正常，安全策略日志是否正常	是否正常：☐是☐否	
		6	路由：是否已禁止源路由，其他路由信息是否满足连接访问需求	是否正常：☐是☐否	
		7	SSL-VPN：用户登录情况，用户分配情况（权限信息检查），界面、访问站点配置，证书配置	是否正常：☐是☐否	
		8	标记标示清晰，网络接口正常，显示正常	是否正常：☐是☐否	
		9	系统访问验证、测试	是否正常：☐是☐否	
F100 （192.168.1.1）	服务器机柜	1	安全策略：检查每一项防火墙规则设置的合理性，是否有达到其作用（见后附策略表）	是否正常：☐是☐否	
		2	配置文件：当前配置文件是否保存，配置文件是否有及时备份，配置文件是否存在未授权篡改	是否正常：☐是☐否	
		3	CPU，内存占用情况	CPU使用率：_____% 内存使用率：_____%	
		4	系统时钟：是否与系统时钟同步	是否正常：☐是☐否	
		5	日志：系统操作日志是否对应符合表单记录，系统运行日志是否正常，安全策略日志是否正常	是否正常：☐是☐否	
		6	路由：是否已禁止源路由，其他路由信息是否满足连接访问需求	是否正常：☐是☐否	
		7	标记标示清晰，网络接口正常，显示正常	是否正常：☐是☐否	
		8	系统访问验证、测试	是否正常：☐是☐否	

关键设备审查记录表（设备）

设备名称及IP地址	所在区域	编号	检查信息	结果	备注
数据接收服务器（10.255.1.10）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间，登录日志，权限信息	是否正常：☐是☐否	
		2	软件：是否存在未授权软件，软件更新情况，运行情况	是否正常：☐是☐否	
		3	安全配置：本地防火墙，密码规则，锁定规则，远程配置	是否正常：☐是☐否	
		4	更新：windows更新，symantec更新	是否正常：☐是☐否	
		5	CPU，内存占用情况	CPU使用率：_____% 内存使用率：_____%	
		6	磁盘占用情况	C盘共 100GB，可用_____ D盘共 0.99TB，可用_____	
		7	系统时钟：ntp同步是否正常	是否正常：☐是☐否	
		8	Serv-U：用户分配情况（权限信息），登录日志，日志备份情况	是否正常：☐是☐否	
		9	标记标示清晰，网络接口正常，显示正常	是否正常：☐是☐否	
		10	系统访问验证、测试	是否正常：☐是☐否	
数据准备服务器（192.168.4.110）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间，登录日志，权限信息	是否正常：☐是☐否	
		2	软件：是否存在未授权软件，软件更新情况，运行情况	是否正常：☐是☐否	
		3	安全配置：本地防火墙，密码规则，锁定规则，远程配置	是否正常：☐是☐否	
		4	更新：windows更新，symantec更新	是否正常：☐是☐否	
		5	CPU，内存占用情况	CPU使用率：_____% 内存使用率：_____%	
		6	磁盘占用情况	C盘共 292GB，可用_____ D盘共 732GB，可用_____ E盘共 837GB，可用_____	
		7	系统时钟：ntp同步是否正常	是否正常：☐是☐否	
		8	Serv-U：用户分配情况（权限信息），登录日志，日志备份情况	是否正常：☐是☐否	
		9	标记标示清晰，网络接口正常，显示正常	是否正常：☐是☐否	
		10	系统访问验证、测试	是否正常：☐是☐否	

关键设备审查记录表（设备）

设备名称及IP地址	所在区域	编号	检查信息	结果	备注
WSUS服务器 （10.255.2.254）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间，登录日志，权限信息	是否正常：☐是☐否	
		2	软件：是否存在未授权软件，软件更新情况，运行情况	是否正常：☐是☐否	
		3	安全配置：本地防火墙，密码规则，锁定规则，远程配置	是否正常：☐是☐否	
		4	更新：windows更新，symantec更新	是否正常：☐是☐否	
		5	CPU，内存占用情况	CPU使用率：_____% 内存使用率：_____%	
		6	磁盘占用情况	C盘共 0.99TB，可用_____ D盘共 838GB，可用_____	
		7	系统时钟：ntp同步是否正常	是否正常：☐是☐否	
		8	标记标示清晰，网络接口正常，显示正常	是否正常：☐是☐否	
		9	系统访问验证、测试	是否正常：☐是☐否	
IDS （192.168.0.1）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间	是否正常：☐是☐否	
		2	日志:系统操作日志是否对应符合表单记录,系统运行日志是否正常,入侵检查防御日志,URL过滤日志	是否正常：☐是☐否	
		3	CPU，内存占用情况	CPU使用率：_____% 内存使用率：_____%	
		4	系统时钟：ntp同步是否正常	是否正常：☐是☐否	
		5	标记标示清晰，网络接口正常，显示正常	是否正常：☐是☐否	
		6	系统访问验证、测试	是否正常：☐是☐否	
日志服务器 （192.168.1.252）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间	是否正常：☐是☐否	
		2	软件：是否存在未授权软件，软件更新情况，运行情况	是否正常：☐是☐否	
		3	系统：是否符合安装标准	是否正常：☐是☐否	
		4	日志:系统操作日志是否对应符合表单记录,系统运行日志是否正常,入侵检查防御日志,URL过滤日志	是否正常：☐是☐否	
		5	CPU，内存占用情况	CPU使用率：_____% 内存使用率：_____%	
		6	磁盘占用情况	C盘共 100GB，可用_____	

关键设备审查记录表（设备）

设备名称及IP地址	所在区域	编号	检查信息	结果	备注
日志服务器 （192.168.1.252）	服务器机柜	6	磁盘占用情况	G盘共 0.99TB，可用_____	
		7	系统时钟：ntp同步是否正常	是否正常：☐是☐否	
		8	标记标示清晰，网络接口正常，显示正常	是否正常：☐是☐否	
		9	系统访问验证、测试	是否正常：☐是☐否	
加密机 （SafeNet）	服务器机柜	1	系统时间与硬件时间同步是否正常	是否正常：☐是☐否	
		2	运行灯是否正常亮起	是否正常：☐是☐否	
		3	设备是否有异常报警声	是否正常：☐是☐否	
SAS数据准备服务器 （192.168.3.252）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间，登录日志，权限信息	是否正常：☐是☐否	
		2	软件：是否存在未授权软件，软件更新情况，运行情况	是否正常：☐是☐否	
		3	安全配置：本地防火墙，密码规则，锁定规则，远程配置	是否正常：☐是☐否	
		4	更新：windows更新，symantec更新	是否正常：☐是☐否	
		5	CPU，内存占用情况	CPU使用率：_____% 内存使用率：_____%	
		6	磁盘占用情况	C盘共 199GB，可用_____ D盘共 781GB，可用_____ E盘共 880GB，可用_____	
		7	系统时钟：ntp同步是否正常	是否正常：☐是☐否	
		8	Serv-U：用户分配情况（权限信息），登录日志，日志备份情况	是否正常：☐是☐否	
		9	标记标示清晰，网络接口正常，显示正常	是否正常：☐是☐否	
		10	系统访问验证、测试	是否正常：☐是☐否	
SAS数据备份服务器 （192.168.3.248）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间，登录日志，权限信息	是否正常：☐是☐否	
		2	软件：是否存在未授权软件，软件更新情况，运行情况	是否正常：☐是☐否	
		3	安全配置：本地防火墙，密码规则，锁定规则，远程配置	是否正常：☐是☐否	
		4	更新：windows更新，symantec更新	是否正常：☐是☐否	

关键设备审查记录表（设备）

设备名称及IP地址	所在区域	编号	检查信息	结果	备注
SAS数据备份服务器 （192.168.3.248）	服务器机柜	5	CPU，内存占用情况	CPU使用率：_____ % 内存使用率：_____ %	
		6	磁盘占用情况	C盘共 199GB，可用_____ D盘共 781GB，可用_____ E盘共 880GB，可用_____	
		7	系统时钟：ntp同步是否正常	是否正常：□ 是 □ 否	
		8	Serv-U：用户分配情况（权限信息），登录日志，日志备份情况	是否正常：□ 是 □ 否	
		9	标记标示清晰，网络接口正常，显示正常	是否正常：□ 是 □ 否	
		10	系统访问验证、测试	是否正常：□ 是 □ 否	
日志备份服务器 （192.168.1.251）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间	是否正常：□ 是 □ 否	
		2	软件：是否存在未授权软件，软件更新情况，运行情况	是否正常：□ 是 □ 否	
		3	系统：是否符合安装标准	是否正常：□ 是 □ 否	
		4	日志是否正常备份	是否正常：□ 是 □ 否	
		5	CPU，内存占用情况	CPU使用率：_____ % 内存使用率：_____ %	
		6	磁盘占用情况	C盘共 300GB，可用_____ G盘共 1.70TB，可用_____	
		7	系统时钟：ntp同步是否正常	是否正常：□ 是 □ 否	
		8	标记标示清晰，网络接口正常，显示正常	是否正常：□ 是 □ 否	
		9	系统访问验证、测试	是否正常：□ 是 □ 否	
管理服务器 （192.168.1.253）	服务器机柜	1	用户：是否存在未授权用户，用户名密码过期时间	是否正常：□ 是 □ 否	
		2	软件：是否存在未授权软件，软件更新情况，运行情况	是否正常：□ 是 □ 否	
		3	系统：是否符合安装标准	是否正常：□ 是 □ 否	
		5	CPU，内存占用情况	CPU使用率：_____ % 内存使用率：_____ %	
		6	磁盘占用情况	C盘共 199GB，可用_____ D盘共 200GB，可用_____ E盘共 1.70TB，可用_____	
		7	系统时钟：ntp同步是否正常	是否正常：□ 是 □ 否	
		8	标记标示清晰，网络接口正常，显示正常	是否正常：□ 是 □ 否	

关键设备审查记录表（防火墙）

F100-S-G防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求	安全要求
Source	Destination		Source		Destination					
UnTrust	DataPrepare	Deny	Any		Any		Any	拒绝来自外部网络的任何访问。 Deny any access from external network.		
UnTrust	SAS	Deny	Any		Any		Any	拒绝来自外部网络的任何访问。 Deny any access from external network.		
UnTrust	Personalization	Deny	Any		Any		Any	拒绝来自外部网络的任何访问。 Deny any access from external network.		
UnTrust	Management	Permit	10.255.1.10	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,Ping	仅允许数据接收服务器通过百络网警,Symantec,Ping服务访问管理服务器。 Only allow the data receiving server to access the management server through BaiLuo, Symantec, and Ping service.		
UnTrust	Management	Permit	10.255.2.254	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许WSUS服务器通过百络网警,Symantec,WSUS,Ping服务访问管理服务器。 Permit access of WSUS servers to the management server only through Bailuo,Symantec, WSUS and Ping services.		
UnTrust	Management	Permit	10.255.1.10	0.0.0.0	192.168.1.252	0.0.0.0	Log	仅允许数据接收服务器通过Log服务访问日志服务器。 Permit access of data receiving server to log server only through Log service.		
UnTrust	Management	Permit	10.255.2.254	0.0.0.0	192.168.1.252	0.0.0.0	Log	仅允许WSUS服务器通过Log服务访问日志服务器。 Permit access of WSUS servers to the log server only via Log service.		
UnTrust	Management	Permit	10.255.3.1	0.0.0.0	192.168.1.252	0.0.0.0	Syslog	仅允许F1000防火墙通过Syslog服务访问日志服务器。 Permit access of F1000 firewall to the log server only via Syslog service.		
UnTrust	Management	Deny	Any		Any		Any	拒绝来自外部网络的任何访问。 Deny any access from external network.		
UnTrust	Local	Deny	Any		Any		Any	拒绝外部登录防火墙。 Deny external login to the firewall.		
DataPrepare	SAS	Deny	Any		Any		Any	拒绝数据准备区到SAS区的任何访问。 Deny any access from the data staging area to the SAS area.		
DataPrepare	Personalization	Permit	192.168.4.102-104, 106	0.0.0.0	192.168.2.11	0.0.0.0	FTP,MySQL	仅允许数据处理PC通过FTP，MySQL服务访问CPS数据库备份服务器 Only allow the data processing PC to access the CPS database backup server through FTP and MySQL service		
DataPrepare	Personalization	Permit	192.168.4.104	0.0.0.0	192.168.2.154	0.0.0.0	Ping,8	允许数据主管PC访问154加密机 Allow data supervisor PC to access 154 encryptor		
DataPrepare	Personalization	Permit	192.168.4.100	0.0.0.0	192.168.2.161	0.0.0.0	Ping,8	允许DPC数据准备服务器访问DPC加密机 Allow DPC data preparation server to access DPC encryptor		
DataPrepare	Personalization	Permit	192.168.4.100	0.0.0.0	192.168.2.75-81, 85，91	0.0.0.0	Any	允许DPC数据准备服务器访问个人化设备 Allow DPC data preparation server to access personalization device		
DataPrepare	Personalization	Permit	192.168.4.102-104, 106	0.0.0.0	192.168.2.248	0.0.0.0	MySQL	仅允许数据处理PC通过MySQL服务访问CPS应用服务器 Only allow data processing PC to access CPS application server through MySQL service		
DataPrepare	Personalization	Deny	Any		Any		Any	拒绝数据准备区到个人化区的任何访问。 Deny any access from the data staging area to the personalization area.		
DataPrepare	Management	Permit	192.168.4.110	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	仅允许数据准备服务器通过通过百络网警,Symantec,WSUS,Ping服务访问管理服务器。 Only allow the data preparation server to access the management server through BaiLuo, Symantec, WSUS, and Ping service.		
DataPrepare	Management	Permit	192.168.4.101	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	仅允许个人化数据准备服务器通过通过百络网警,IMC,Symantec,WSUS,Ping服务访问管理服务器。 Only allow the personalization data preparation server to access the management server through BaiLuo, Symantec, WSUS, and Ping service.		
DataPrepare	Management	Permit	192.168.4.102-104, 106	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	仅允许数据数据处理PC通过通过百络网警,Symantec,WSUS,Ping服务访问管理服务器。 Only allow the data processing PC to access the management server through BaiLuo , Symantec, WSUS and Ping service.		
DataPrepare	Management	Permit	192.168.4.110	0.0.0.0	192.168.1.252	0.0.0.0	NTP,Log	仅允许数据准备服务器、数据处理PC通过通过NTP,Log服务访问日志服务器。 Only allow the data preparation server and data processing PC to access the log server through NTP and Log service.		

关键设备审查记录表（防火墙）

F100-S-G防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求	安全要求
Source	Destination		Source		Destination					
DataPrepare	Management	Permit	192.168.4.101	0.0.0.0	192.168.1.252	0.0.0.0	NTP,Log	仅允许个人化数据准备服务器、数据处理PC通过通过NTP,Log服务访问日志服务器。 Only allow the personalization data preparation server and data processing PC to access the log server through NTP and Log service.		
DataPrepare	Management	Permit	192.168.4.102-104, 106	0.0.0.0	192.168.1.252	0.0.0.0	NTP,Log	仅允许数据处理PC通过通过NTP,Log服务访问日志服务器。 Only allow the data processing PC to access the log server through NTP and Log service.		
DataPrepare	Management	Deny	Any		Any		Any	拒绝数据准备区到管理区的任何访问。 Deny any access from the data staging area to the management area.		
DataPrepare	UnTrust	Permit	192.168.4.104	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许数据主管的PC通过FTP服务访问数据接收服务器。 Only allow the data supervisor PC to access the data receiving server through the FTP service.		
DataPrepare	UnTrust	Deny	Any		Any		Any	拒绝任何计算机访问到外部网络。 Deny any computer access to the external network.		
DataPrepare	Local	Deny	Any		Any		Any	拒绝任何计算机登录防火墙。 Deny any computer login to the firewall.		
SAS	UnTrust	Permit	192.168.3.251	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许SAS数据处理PC通过FTP服务访问数据接收服务器。 Only allow the SAS data processing PC to access the data receiving server through the FTP service.		
SAS	UnTrust	Deny	Any		Any		Any	拒绝访问到外部网络。 Deny access to the external network.		
SAS	Personalization	Deny	Any		Any		Any	拒绝访问到个人化区。 Deny access to the personalization area.		
SAS	Management	Permit	192.168.3.248-253	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	仅允许SAS数据准备服务器通过百络网警,Symantec,WSUS,Ping服务访问管理服务器。 Only allow the SAS data preparation server to access the management server through BaiLuo, Symantec, WSUS and Ping service.		
SAS	Management	Permit	192.168.3.248-253	0.0.0.0	192.168.1.252	0.0.0.0	NTP,Log	仅允许SAS设备通过NTP,Log服务访问日志服务器。 Only allow the SAS devices to access the log server through NTP and Log service.		
SAS	Management	Deny	Any		Any		Any	拒绝访问到管理区 Deny access to the management area		
SAS	DataPrepare	Deny	Any		Any		Any	拒绝访问到数据准备区 Deny access to the data staging area		
SAS	Local	Deny	Any		Any		Any	拒绝登录防火墙。 Deny log to the firewall.		
Management	SAS	Permit	192.168.1.253	0.0.0.0	192.168.3.248-253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping服务访问到SAS区。 Only allow the management server to access the SAS area through BaiLuo, Symantec, WSUS and Ping service.		
Management	SAS	Permit	192.168.1.252	0.0.0.0	192.168.3.248-253	0.0.0.0	Log	仅允许日志服务器通过Log服务访问SAS设备。 Only allow the log server to access the SAS devices through Log service.		
Management	SAS	Deny	Any		Any		Any	拒绝访问SAS区。 Deny access to the SAS area.		
Management	DataPrepare	Permit	192.168.1.253	0.0.0.0	192.168.4.102-104, 106	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping服务访问到数据处理PC Only allow the management server to access the data processing PC through BaiLuo, Symantec, WSUS and Ping service.		
Management	DataPrepare	Permit	192.168.1.253	0.0.0.0	192.168.4.110	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping服务访问到数据准备服务器 Only allow the management server to access the data preparation server through BaiLuo, Symantec, WSUS and Ping service.		
Management	DataPrepare	Permit	192.168.1.253	0.0.0.0	192.168.4.101	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping服务访问到个人化数据准备服务器 Only allow the management server to access the personalization data preparation server through BaiLuo, Symantec, WSUS and Ping service.		
Management	DataPrepare	Permit	192.168.1.252	0.0.0.0	192.168.4.101-104,106,110	0.0.0.0	Log	仅允许日志服务器通过Log服务访问数据区设备。 Only allow the log server to access the DataPrepare devices through Log service.		
Management	DataPrepare	Deny	Any		Any		Any	拒绝访问到数据准备区 Deny access to the data staging area		

关键设备审查记录表（防火墙）

F100-S-G防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求	安全要求
Source	Destination		Source		Destination					
Management	UnTrust	Permit	192.168.1.253	0.0.0.0	10.255.1.10	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping服务访问数据接收服务器 Only allow the management server to access the data receiving server through BaiLuo, Symantec, WSUS and Ping service.		
Management	UnTrust	Permit	192.168.1.253	0.0.0.0	10.255.2.254	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping服务访问WSUS服务器 Only allow the management server to access the WSUS server through BaiLuo, Symantec, WSUS and Ping service.		
Management	UnTrust	Permit	192.168.1.253	0.0.0.0	10.255.3.1	0.0.0.0	0_firewall_manage	仅允许管理服务器登录到F1000防火墙。 Only allow the management server to login to the F1000 firewall.		
Management	UnTrust	Permit	192.168.1.252	0.0.0.0	10.255.2.254	0.0.0.0	NTP、Symantec	仅允许日志服务器通过NTP,Symantec服务访问WSUS服务器 Only allow the log server to access the WSUS server through NTP and Symantec service.		
Management	UnTrust	Permit	192.168.1.252	0.0.0.0	10.255.2.254	0.0.0.0	Log	仅允许日志服务器通过Log服务访问WSUS服务器。 Only allow the log server to access the WSUS server through Log service.		
Management	UnTrust	Permit	192.168.1.252	0.0.0.0	10.2551.10	0.0.0.0	Log	仅允许日志服务器通过Log服务访问数据接收服务器。 Only allow the log server to accessthe data receiving server through Log service.		
Management	UnTrust	Deny	Any		Any		Any	拒绝访问外部网络。 Deny access to the external network.		
Management	Personalization	Permit	192.168.1.253	0.0.0.0	192.168.2.75-81, 85，91	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping服务访问到个人化设备。 Only allow the management server to access the personalization device through BaiLuo, Symantec, WSUS and Ping service.		
Management	Personalization	Permit	192.168.1.253	0.0.0.0	192.168.2.11	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping服务访问到CPS数据库备份服务器。 Only allow the management server to access the CPS database backup server through BaiLuo, Symantec, WSUS and Ping service.		
Management	Personalization	Permit	192.168.1.253	0.0.0.0	192.168.2.248	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping,服务访问CPS应用服务器 Only allow the management server to access the CPS application server through BaiLuo, Symantec, WSUS, Ping service.		
Management	Personalization	Permit	192.168.1.252	0.0.0.0	192.168.2.75-81, 85，91，11，248	0.0.0.0	Log	仅允许日志服务器通过Log服务访问个人化设备。 Only allow the log server to access the Personalization devices through Log service.		
Management	Personalization	Deny	Any		Any		Any	拒绝访问到个人化区。 Deny access to the personalization area.		
Management	Local	Permit	192.168.1.253	0.0.0.0	192.168.1.1	0.0.0.0	0_firewall_manage	仅允许管理服务器登录到F100防火墙。 Only allow the management server to login to the F100 firewall.		
Management	Local	Deny	Any		Any		Any	拒绝登录防火墙。 Deny log to the firewall.		
Personalization	SAS	Deny	Any		Any		Any	拒绝访问SAS区。 Deny access to the SAS area.		
Personalization	Management	Permit	192.168.2.75-81, 85，91	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许个人化设备通过百络网警,Symantec,WSUS,Ping服务访问管理服务器。 Only allow the personalization device to access the management server through BaiLuo, Symantec, WSUS and Ping service.		
Personalization	Management	Permit	192.168.2.248	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许CPS应用服务器通过百络网警,Symantec,WSUS,Ping服务访问管理服务器。 Only allow the CPS application server to access the management server through BaiLuo, Symantec, WSUS and Ping service.		
Personalization	Management	Permit	192.168.2.75-81, 85，91	0.0.0.0	192.168.1.252	0.0.0.0	NTP,Log	仅允许个人化设备通过NTP,Log服务访问日志服务器。 Only allow the personalization device to access the log server through NTP and Log service.		
Personalization	Management	Permit	192.168.2.248	0.0.0.0	192.168.1.252	0.0.0.0	NTP,Log	仅允许CPS应用服务器通过NTP.Log服务访问日志服务器。 Only allow the CPS application server to access the log server through NTP and Log service.		
Personalization	Management	Permit	192.168.2.11	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	仅允许CPS数据库备份服务器通过百络网警,Symantec,WSUS,Ping服务访问管理服务器。 Only allow the CPS database backup server to access the management server through BaiLuo, Symantec, WSUS and Ping service.		
Personalization	Management	Permit	192.168.2.11	0.0.0.0	192.168.1.252	0.0.0.0	NTP,Log	仅允许CPS数据库备份服务器通过NTP.Log服务访问日志服务器。 Only allow the CPS database backup server to access the log server through NTP and Log service.		

关键设备审查记录表（防火墙）

F100-S-G防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求	安全要求
Source	Destination		Source		Destination					
Personalization	Management	Deny	Any		Any		Any	拒绝访问到管理区 Deny access to the management area		
Personalization	DataPrepare	Permit	192.168.2.75-81, 85, 91	0.0.0.0	192.168.4.110	0.0.0.0	SQLServer,FTP	仅允许个人化设备通过FTP服务访问数据准备服务器。 Only allow the personalization device to access the data preparation server through the FTP service.		
Personalization	DataPrepare	Permit	192.168.2.75-81, 85, 91	0.0.0.0	192.168.4.100	0.0.0.0	Any	仅允许个人化设备访问DPC数据准备服务器。 Only allow the personalization device to access the DPC data preparation server.		
Personalization	DataPrepare	Deny	Any		Any		Any	拒绝访问到数据准备区 Deny access to the data staging area		
Personalization	UnTrust	Permit	192.168.2.75-81, 85, 91	0.0.0.0	10.255.2.254	0.0.0.0	Symantec	仅允许个人化设备通过Symantec服务访问WSUS服务器。 Only allow the personalization device to access the WSUS server through the Symantec service.		
Personalization	UnTrust	Permit	192.168.2.11	0.0.0.0	10.255.2.254	0.0.0.0	Symantec	仅允许CPS数据库备份服务器通过Symantec服务访问WSUS服务器。 Only allow the CPS database backup server to access the WSUS server through the Symantec service.		
Personalization	UnTrust	Permit	192.168.2.248	0.0.0.0	10.255.2.254	0.0.0.0	Symantec	仅允许CPS应用服务器通过Symantec服务访问WSUS服务器。 Only allow the CPS application server to access the WSUS server through the Symantec service.		
Personalization	UnTrust	Deny	Any		Any		Any	拒绝访问到UnTrust区。 Deny access to the UnTrust area		
Personalization	Local	Deny	Any		Any		Any	拒绝登录防火墙。 Deny log to the firewall.		

关键设备审查记录表（防火墙）

F1000-E-SI防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求	安全要求
Source	Destination		Source		Destination					
Server	UnTrust	Permit	10.15.132.2	0.0.0.0	31.0.0.50	0.0.0.0	31842-31843	仅允许数据接收服务器通过31842-31843端口访问银联服务器。		
Server	UnTrust	Permit	10.15.132.2	0.0.0.0	101.230.4.30	0.0.0.0	31842-31843	仅允许数据接收服务器通过31842-31843端口访问银联服务器。		
Server	UnTrust	Deny	Any		Any		Any	拒绝访问Internet。 Deny access to the Internet.		
Server	DMZ	Permit	10.255.1.10	0.0.0.0	10.255.2.254	0.0.0.0	Ping,WSUS,NTP	仅允许数据接收服务器通过Ping，WSUS，NTP服务访问WSUS服务器 Permit access of data receiving server to WSUS servers only through Ping，WSUS and NTP services.		
Server	DMZ	Deny	Any		Any		Any	拒绝访问到DMZ区。 Deny access to the DMZ.		
Server	Trust	Permit	10.255.1.10	0.0.0.0	192.168.1.253	0.0.0.0	Bailuo,Symantec,Ping	仅允许数据接收服务器通过百络网警,Symantec,Ping服务访问管理服务器 Permit access of data receiving server to the management server only through Bailuo，Symantec and Ping services.		
Server	Trust	Permit	10.255.1.10	0.0.0.0	192.168.1.252	0.0.0.0	Log,Ping	仅允许数据接收服务器通过Syslog服务访问日志服务器。 Permit access of data receiving server to log server only through Syslog service.		
Server	Trust	Deny	Any		Any		Any	拒绝访问到Trust区。 Deny access to the Trust.		
UnTrust	Server	Permit	192.168.254.0	0.0.0.255	10.255.1.10	0.0.0.0	FTP	仅允许SSL-VPN用户通过FTP服务访问数据接收服务器。 Permit access of SSL-VPN users to data receiving server through FTP service.		
UnTrust	Server	Permit	192.168.0.88	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许卫计委通过FTP服务访问数据接收服务器。 Permit access of National Health and Family Planning Commission of the People's Republic of China to data receiving server only through FTP service.		
UnTrust	Server	Permit	182.150.13.131	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许卫计委通过FTP服务访问数据接收服务器。 Permit access of National Health and Family Planning Commission of the People's Republic of China to data receiving server only through FTP service.		
UnTrust	Server	Permit	10.50.7.45	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许天府通通过FTP服务访问数据接收服务器。 Permit access of Tianfu Tong to data receiving server only through FTP service.		
UnTrust	Server	Permit	172.16.2.15	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许天府通通过FTP服务访问数据接收服务器。 Permit access of Tianfu Tong to data receiving server only through FTP service.		
UnTrust	Server	Permit	182.140.133.54	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许天府通通过FTP服务访问数据接收服务器。 Permit access of Tianfu Tong to data receiving server only through FTP service.		
UnTrust	Server	Permit	31.0.0.50	0.0.0.0	10.15.132.2	0.0.0.0	FTP	仅允许银联通过FTP服务访问数据接收服务器。 Permit access of Yinlian Tong to data receiving server only through FTP service.		
UnTrust	Server	Permit	101.230.4.30	0.0.0.0	10.15.132.2	0.0.0.0	FTP	仅允许银联通过FTP服务访问数据接收服务器。 Permit access of Yinlian Tong to data receiving server only through FTP service.		
UnTrust	Server	Permit	10.255.4.0	0.0.0.255	10.255.1.10	0.0.0.0	FTP	仅允许省中行设备通过FTP服务访问数据接收服务器。 permit access of the provincial branch of the People's Bank of China to data receiving server only through FTP service.		
UnTrust	Server	Permit	103.209.139.29	0.0.0.255	10.255.1.10	0.0.0.0	FTP	仅允许壹卡会通过FTP服务访问数据接收服务器。 permit access of the Yikahui to data receiving server only through FTP service.		
UnTrust	Server	Permit	21.64.188.0	0.0.1.255	10.255.1.10	0.0.0.0	FTP	仅允许壹卡会通过FTP服务访问数据接收服务器。 permit access of the Yikahui to data receiving server only through FTP service.		
UnTrust	Server	Deny	Any		Any		Any	拒绝访问到Server区。 Deny access to the Server.		
UnTrust	DMZ	Permit	192.168.8.2	0.0.0.0	10.255.2.254	0.0.0.0	Symantec,WSUS,Ping	仅允许WSUS外部服务器通过Symantec，WSUS，Ping服务访问WSUS服务器。 permit access of the WSUS External server to WSUS server through Symantec,WSUS and Ping service.		
UnTrust	DMZ	Deny	Any		Any		Any	拒绝访问到DMZ区。 Deny access to the DMZ.		
UnTrust	Trust	Deny	Any		Any		Any	拒绝访问到内部网络。 Deny access to internal network.		
UnTrust	Local	Permit	Any		118.123.172.249	0.0.0.0	HTTPS,Ping	仅允许远端PC连接SSL-VPN Permit only remote PC connection to SSL-VPN.		

关键设备审查记录表（防火墙）

F1000-E-SI防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求	安全要求
Source	Destination		Source		Destination					
UnTrust	Local	Permit	192.168.0.88		118.123.172.249		ESP	仅允许卫计委通过ESP服务访问外部IP。 Permit access of Weijiwei to external IP only through ESP service.		
UnTrust	Local	Permit	182.150.13.131		118.123.172.249		ESP	仅允许卫计委通过ESP服务访问外部IP。 Permit access of Weijiwei to external IP only through ESP service.		
UnTrust	Local	Permit	31.0.0.50		118.123.172.249		UDP_500	仅允许银联通过UDP_500端口访问外部IP。 Permit access of Yinlian to external IP only through UDP_500 Ports.		
UnTrust	Local	Permit	101.230.4.30		118.123.172.249		UDP_500	仅允许银联通过UDP_500端口访问外部IP。 Permit access of Yinlian to external IP only through UDP_500 Ports.		
UnTrust	Local	Permit	10.50.7.45		118.123.172.249		ESP	仅允许天府通通过ESP服务访问外部IP。 Permit access of Tianfu Tong to external IP only through ESP service.		
UnTrust	Local	Permit	172.16.2.15		118.123.172.249		ESP	仅允许天府通通过ESP服务访问外部IP。 Permit access of Tianfu Tong to external IP only through ESP service.		
UnTrust	Local	Permit	182.140.133.54		118.123.172.249		ESP	仅允许天府通通过ESP服务访问外部IP。 Permit access of Tianfu Tong to external IP only through ESP service.		
UnTrust	Local	Permit	103.209.139.29	0.0.0.0	118.123.172.249	0.0.0.0	ESP	仅允许壹卡会通过ESP服务访问外部IP。 Permit access of Yikahui to external IP only through ESP service.		
UnTrust	Local	Permit	21.64.188.0	0.0.1.255	118.123.172.249	0.0.0.0	ESP	仅允许壹卡会通过ESP服务访问外部IP。 Permit access of Yikahui to external IP only through ESP service.		
UnTrust	Local	Deny	Any		Any		Any	拒绝访问到本地。 Deny access to the Local.		
DMZ	UnTrust	Permit	10.255.2.254	0.0.0.0	Any		Any	仅允许访问Internet以获取更新。 Access to the Internet is only allowed for updates.		
DMZ	UnTrust	Deny	Any		Any		Any	拒绝访问到Internet。 Deny access to the Internet.		
DMZ	Server	Permit	10.255.2.254	0.0.0.0	10.255.1.10	0.0.0.0	Ping,WSUS	仅允许WSUS服务器通过Ping，WSUS服务访问数据接收服务器。		
DMZ	Server	Deny	Any		Any		Any	拒绝访问数据接收服务器。 Deny access to the data receiving server.		
DMZ	Trust	Permit	10.255.2.254	0.0.0.0	192.168.1.253	0.0.0.0	Bailuo,Symantec,WSUS,Ping	仅允许WSUS服务器通过百络网警,Symantec,WSUS,Ping服务访问管理服务器。 Permit access of WSUS servers to the management server only through Bailuo, Symantec, WSUS and Ping services.		
DMZ	Trust	Permit	10.255.2.254	0.0.0.0	192.168.1.252	0.0.0.0	Log,Ping	仅允许WSUS服务器通过Syslog服务访问日志服务器。 Permit access of WSUS servers to the log server only via Syslog service.		
DMZ	Trust	Deny	Any		Any		Any	拒绝访问到内部网络。 Deny access to internal network.		
DMZ	Local	Deny	Any		Any		Any	拒绝登录防火墙。 Deny log to the firewall.		
Trust	Server	Permit	192.168.4.102	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许数据主管PC通过FTP服务访问数据接收服务器。 Permit access of data supervisor PC to data receiving server only via FTP service.		
Trust	Server	Permit	192.168.3.251	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许SAS生产PC通过FTP服务访问数据接收服务器。 Permit access of the SAS Production PC to data receiving server only through Bailuo, IMC, Symantec, WSUS and Ping services.		
Trust	Server	Permit	192.168.1.253	0.0.0.0	10.255.1.10	0.0.0.0	Bailuo,Symantec,Ping	仅允许管理服务器通过百络网警,Symantec,Ping服务访问数据接收服务器。 Permit access of the management server to data receiving server only through Bailuo, Symantec and Ping services.		
Trust	Server	Permit	192.168.1.252	0.0.0.0	10.255.1.10	0.0.0.0	FTP,Log	仅允许日志服务器通过FTP，Log服务访问数据接收服务器。 Permit access of the log server to data receiving server only through FTP and Log services.		
Trust	Server	Deny	Any		Any		Any	拒绝访问到Server区。 Deny access to the Server.		
Trust	DMZ	Permit	192.168.1.253	0.0.0.0	10.255.2.254	0.0.0.0	Bailuo,Symantec,WSUS,Ping	仅允许管理服务器通过百络网警,Symantec,WSUS,Ping,服务访问WSUS服务器。 Permit access of the management server to WSUS servers only through Bailuo, Symantec, WSUS and Ping services.		

关键设备审查记录表（防火墙）

F1000-E-SI防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求	安全要求
Source	Destination		Source		Destination					
Trust	DMZ	Permit	192.168.1.252	0.0.0.0	10.255.2.254	0.0.0.0	NTP,Log	仅允许日志服务器通过NTP,Log服务访问WSUS服务器 Permit access of the log server to WSUS servers only via NTP and Log services.		
Trust	DMZ	Deny	Any		Any		Any	拒绝访问到DMZ区。 Deny access to the DMZ.		
Trust	UnTrust	Deny	Any		Any		Any	拒绝访问Internet。 Deny access to the Internet.		
Trust	Local	Permit	192.168.1.253	0.0.0.0	10.255.3.1	0.0.0.0	FirewallManage	仅允许管理服务器登录F1000防火墙。 (0_firewall_manager) Permit only management server to log F1000 firewall. (0_firewall_manager)		
Trust	Local	Deny	Any		Any		Any	拒绝登录防火墙。 Deny log to the firewall.		

关键设备审查记录表（防火墙）

F100-S-G需要修改的项

Direction		P/D	IP				Port/service	Reason
Source	Destination		Source		Destination			

F100-S-G需要删除的项

Direction		P/D	IP				Port/service	Reason
Source	Destination		Source		Destination			

关键设备审查记录表（防火墙）

F1000-E-SI需要修改的项

Direction		P/D	IP				Port/service	Reason
Source	Destination		Source		Destination			

F1000-E-SI需要删除的项

Direction		P/D	IP				Port/service	Reason
Source	Destination		Source		Destination			

关键设备审查记录表（防火墙业务需求确认表）

F1000-E-SI防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求
Source	Destination		Source		Destination				
Server	UnTrust	Permit	10.15.132.2	0.0.0.0	31.0.0.50	0.0.0.0	31842-31843	仅允许数据接收服务器通过31842-31843端口访问银联服务器。	
Server	UnTrust	Permit	10.15.132.2	0.0.0.0	101.230.4.30	0.0.0.0	31842-31843	仅允许数据接收服务器通过31842-31843端口访问银联服务器。	
UnTrust	Server	Permit	192.168.254.0	0.0.0.255	10.255.1.10	0.0.0.0	FTP	仅允许SSL-VPN用户通过FTP服务访问数据接收服务器。 Permit access of SSL-VPN users to data receiving server through FTP service.	
UnTrust	Server	Permit	192.168.0.88	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许卫计委通过FTP服务访问数据接收服务器。 Permit access of National Health and Family Planning Commission of the People's Republic of China to data receiving server only through FTP service.	
UnTrust	Server	Permit	182.150.13.131	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许卫计委通过FTP服务访问数据接收服务器。 Permit access of National Health and Family Planning Commission of the People's Republic of China to data receiving server only through FTP service.	
UnTrust	Server	Permit	10.50.7.45	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许天府通通过FTP服务访问数据接收服务器。 Permit access of Tianfu Tong to data receiving server only through FTP service.	
UnTrust	Server	Permit	172.16.2.15	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许天府通通过FTP服务访问数据接收服务器。 Permit access of Tianfu Tong to data receiving server only through FTP service.	
UnTrust	Server	Permit	182.140.133.54	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许天府通通过FTP服务访问数据接收服务器。 Permit access of Tianfu Tong to data receiving server only through FTP service.	
UnTrust	Server	Permit	31.0.0.50	0.0.0.0	10.15.132.2	0.0.0.0	FTP	仅允许银联通过FTP服务访问数据接收服务器。 Permit access of Yinlian Tong to data receiving server only through FTP service.	
UnTrust	Server	Permit	101.230.4.30	0.0.0.0	10.15.132.2	0.0.0.0	FTP	仅允许银联通过FTP服务访问数据接收服务器。 Permit access of Yinlian Tong to data receiving server only through FTP service.	
UnTrust	Server	Permit	10.255.4.0	0.0.0.255	10.255.1.10	0.0.0.0	FTP	仅允许省中行设备通过FTP服务访问数据接收服务器。 permit access of the provincial branch of the People's Bank of China to data receiving server only through FTP service.	
UnTrust	Server	Permit	103.209.139.29	0.0.0.255	10.255.1.10	0.0.0.0	FTP	仅允许壹卡会通过FTP服务访问数据接收服务器。 permit access of the Yikahui to data receiving server only through FTP service.	
UnTrust	Server	Permit	21.64.188.0	0.0.1.255	10.255.1.10	0.0.0.0	FTP	仅允许壹卡会通过FTP服务访问数据接收服务器。 permit access of the Yikahui to data receiving server only through FTP service.	
UnTrust	Local	Permit	Any		118.123.172.249	0.0.0.0	HTTPS,Ping	仅允许远端PC连接SSL-VPN Permit only remote PC connection to SSL-VPN.	
UnTrust	Local	Permit	192.168.0.88		118.123.172.249		ESP	仅允许卫计委通过ESP服务访问外部IP。 Permit access of Weijiwei to external IP only through ESP service.	
UnTrust	Local	Permit	182.150.13.131		118.123.172.249		ESP	仅允许卫计委通过ESP服务访问外部IP。 Permit access of Weijiwei to external IP only through ESP service.	
UnTrust	Local	Permit	31.0.0.50		118.123.172.249		UDP_500	仅允许银联通过UDP_500端口访问外部IP。 Permit access of Yinlian to external IP only through UDP_500 Ports.	
UnTrust	Local	Permit	101.230.4.30		118.123.172.249		UDP_500	仅允许银联通过UDP_500端口访问外部IP。 Permit access of Yinlian to external IP only through UDP_500 Ports.	
UnTrust	Local	Permit	10.50.7.45		118.123.172.249		ESP	仅允许天府通通过ESP服务访问外部IP。 Permit access of Tianfu Tong to external IP only through ESP service.	
UnTrust	Local	Permit	172.16.2.15		118.123.172.249		ESP	仅允许天府通通过ESP服务访问外部IP。 Permit access of Tianfu Tong to external IP only through ESP service.	
UnTrust	Local	Permit	182.140.133.54		118.123.172.249		ESP	仅允许天府通通过ESP服务访问外部IP。 Permit access of Tianfu Tong to external IP only through ESP service.	
UnTrust	Local	Permit	103.209.139.29	0.0.0.0	118.123.172.249	0.0.0.0	ESP	仅允许壹卡会通过ESP服务访问外部IP。 Permit access of Yikahui to external IP only through ESP service.	
UnTrust	Local	Permit	21.64.188.0	0.0.1.255	118.123.172.249	0.0.0.0	ESP	仅允许壹卡会通过ESP服务访问外部IP。 Permit access of Yikahui to external IP only through ESP service.	
Trust	Server	Permit	192.168.4.102	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许数据主管PC通过FTP服务访问数据接收服务器。 Permit access of data supervisor PC to data receiving server only via FTP service.	
Trust	Server	Permit	192.168.3.251	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许SAS生产PC通过FTP服务访问数据接收服务器。 Permit access of the SAS Production PC to data receiving server only through Bailuo, IMC, Symantec, WSUS and Ping services.	

关键设备审查记录表（防火墙业务需求确认表）

F1000-E-SI防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求
Source	Destination		Source		Destination				
Trust	Server	Permit	192.168.1.252	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许日志服务器通过FTP服务访问数据接收服务器。 Permit access of the log server to data receiving server only through FTP services.	

F100-S-G防火墙策略

Direction		P/D	IP				Port/service	Reason	业务需求
Source	Destination		Source		Destination				
DataPrepare	Personalization	Permit	192.168.4.102-104, 106	0.0.0.0	192.168.2.11	0.0.0.0	FTP,MySQL	仅允许数据处理PC通过FTP，MySQL服务访问CPS数据库备份服务器 Only allow the data processing PC to access the CPS database backup server through FTP and MySQL service	
DataPrepare	Personalization	Permit	192.168.4.104	0.0.0.0	192.168.2.154	0.0.0.0	Ping,8	允许数据主管PC访问154加密机 Allow data supervisor PC to access 154 encryptor	
DataPrepare	Personalization	Permit	192.168.4.100	0.0.0.0	192.168.2.161	0.0.0.0	Ping,8	允许DPC数据准备服务器访问DPC加密机 Allow DPC data preparation server to access DPC encryptor	
DataPrepare	Personalization	Permit	192.168.4.100	0.0.0.0	192.168.2.75-81, 85，91	0.0.0.0	Any	允许DPC数据准备服务器访问个人化设备 Allow DPC data preparation server to access personalization device	
DataPrepare	Personalization	Permit	192.168.4.102-104, 106	0.0.0.0	192.168.2.248	0.0.0.0	MySQL	仅允许数据处理PC通过MySQL服务访问CPS应用服务器 Only allow data processing PC to access CPS application server through MySQL service	
DataPrepare	UnTrust	Permit	192.168.4.104	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许数据主管的PC通过FTP服务访问数据接收服务器。 Only allow the data supervisor PC to access the data receiving server through the FTP service.	
SAS	UnTrust	Permit	192.168.3.251	0.0.0.0	10.255.1.10	0.0.0.0	FTP	仅允许SAS数据处理PC通过FTP服务访问数据接收服务器。	
SAS	DataPrepare	Permit	192.168.3.253	0.0.0.0	192.168.4.101	0.0.0.0	FTP,SQLServer	仅允许SAS生产PC通过FTP,SQLServer服务访问个人化数据准备服务器。	
Personalization	DataPrepare	Permit	192.168.2.75-81,	0.0.0.0	192.168.4.110	0.0.0.0	SQLServer,FTP	仅允许个人化设备通过FTP服务访问数据准备服务器。	

审核

业务部门：	日期：	数据部门：	日期：	生产部门：	日期：

备注： 如有需要修改的，请在相应位置做出修改标记；