	四川科道芯国智能技术股份有限公司 Sichuan Keydom Smart Technology Co., Ltd.	文件编号: Document No. :	KD-LJ01-003
	Class 3 Document 三级文件 网络配置授权书 Network Configuration Authorization	版本号: Version number:	C/2

网络配置授权书

Network Configuration Authorization

文 件 编 号: KD-LJ01-003

Doc. No.:

编 制:安全策略部

Prepared by: Security Policy Department

审 核:

Reviewed by:

批 准:

Approved by:

版本 /修订状态: C2

Rev./Revision status:

受 控 状 态:

Controlled status:

2020-3-2 发布

2020-3-2 实施

Issued on 3/ 2 /2020

Implemented on 3/ 2 /2020

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可, 任何人不得对此机密档的全部或部分进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

文件种类: 管制文件 File Type: controlled document


修订历史记录 Document Changes

修改条款 Modified terms	修订状态 Revision Status	修改内容 Description	修改日期 Date	修改人 Changed by	审核人 Reviewed by	批准人 Approved By
/	A/0	初次发行 Initial release	2015/09/22	韩德均 Han Dejun	刘劲松 Liu Jinsong	李永量 Li Yongliang
2、3、4	B/0	1.更新网络拓扑图 1. Update network topology 2.变更防火墙配置命令为安全策略列表 2. Modification from the firewall configuration commands to security policy list	2016/03/11	曹良攀 Cao Liangpan	刘劲松 Liu Jinsong	李永量 Li Yongliang
2、3、4	B/1	1.更新防火墙策略 1. Update firewall policy	2017/03/03	徐锐 Xu Rui	刘劲松 Liu Jinsong	崔云峰 Cui Yunfeng
2、3、4	B/2	1.更新网络拓扑图 1. Update network topology 2.更新防火墙策略 2. Update firewall policy	2017/08/23	王建勋 Wang Jianxun	王建勋 Wang Jianxun	刘劲松 Liu Jinsong
2、3、4	B/3	更新 F1000-E-SI 防火墙策略 Update F1000-E-SI firewall policy	2018/04/28	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可，任何人不得对此机密档的全部或部分进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

文件种类：管制文件 File Type: controlled document


		四川科道芯国智能技术股份有限公司 Sichuan Keydom Smart Technology Co., Ltd.	文件编号: Document No. :	KD-LJ01-003
Class 3 Document	三级文件	网络配置授权书	版本号: Version number:	C/2

		更新 F100-S-G 防火墙策略 Update F100-SG firewall policy 修订网络拓扑图版本号 Version Number of the revised network topology				
/	B/4	更换 log 及公司名称 Change log and company name	2018/7/25	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong
2、3	B/5	更新网络拓扑图, F1000 防火墙策略 Update the network topology and F1000 firewall policy	2018/12/20	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong
3	B/6	更新 F1000 防火墙策略 Update F1000 firewall policy	2019/01/22	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong
2、3、4	B/7	更新网络拓扑图 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 更新 F100 防火墙策略 Update F100 firewall policy	2019/09/18	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong
2、3、4	B/8	更新网络拓扑图 Update network topology	2019/11/06	黄伟 Huang Wei	王建勋 Wang	刘劲松 Liu

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可, 任何人不得对此机密档的全部或部份进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

文件种类: 管制文件 File Type: controlled document


		四川科道芯国智能技术股份有限公司 Sichuan Keydom Smart Technology Co., Ltd.	文件编号: Document No. :	KD-LJ01-003
Class 3	Document	三级文件 Network Configuration Authorization	版本号: Version number:	C/2

		更新 F1000 防火墙策略 Update F1000 firewall policy 更新 F100 防火墙策略 Update F100 firewall policy			Jianxun	Jinsong
2、3、4	B/9	更新网络拓扑图 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 更新 F100 防火墙策略 Update F100 firewall policy	2019/11/19	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong
2、3、4	C/0	更新网络拓扑图 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 更新 F100 防火墙策略 Update F100 firewall policy	2020.1.1	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong
2、3、4	C/1	更新网络拓扑图 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 更新 F100 防火墙策略 Update F100 firewall policy	2020.1.17	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可，任何人不得对此机密档的全部或部分进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

文件种类：管制文件 File Type: controlled document


		四川科道芯国智能技术股份有限公司 Sichuan Keydom Smart Technology Co., Ltd.	文件编号: Document No. :	KD-LJ01-003
Class 3	Document	三级文件 Network Configuration Authorization	版本号: Version number:	C/2

		Update F100 firewall policy				
3	C/2	更新 F1000 防火墙策略。 Update F1000 firewall policy	2020 . 3 . 2	黄伟 Huang Wei	王建勋 Wang Jianxun	刘劲松 Liu Jinsong

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可，任何人不得对此机密档的全部或部份进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

文件种类：管制文件 File Type: controlled document

	四川科道芯国智能技术股份有限公司 Sichuan Keydom Smart Technology Co., Ltd.		文件编号: Document No. :	KD-LJ01-003
	Class 3 Document	三级文件 网络配置授权书 Network Configuration Authorization	版本号: Version number:	C/2

目 录


Contents

1 网络配置授权书 Network Configuration Authorization	7
2 网络拓扑图（见附件 1） Network Topology (Annex I).....	9
3 H3C F1000-E-SI 防火墙安全策略（见附件 2） H3C F1000-E-SI Firewall Security Policy (Annex II).....	9
4 H3C F100-S-G 防火墙安全策略（见附件 3） H3C F100-SG Firewall Security Policy (Annex III)	9

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可，任何人不得对此机密档的全部或部份进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

文件种类：管制文件 File Type: controlled document

	四川科道芯国智能技术股份有限公司 Sichuan Keydom Smart Technology Co., Ltd.	文件编号: Document No. :	KD-LJ01-003
	Class 3 Document 三级文件 网络配置授权书 Network Configuration Authorization	版本号: Version number:	C/2

1 网络配置授权书

Network Configuration Authorization

四川科道芯国智能技术股份有限公司智能卡及数据生产中心网络配置，此网络配置经授权后生效，逻辑安全管理员应根据本授权配置更改或检查网络和设备。

The network configuration of Intelligent Card and Data Production Center of Sichuan KEYDOM Intelligent Technology Co., Ltd. shall be effective upon authorization. The Logical security administrator shall change or check the network and devices according to this authorized configuration.

本授权包括以下内容：

This authorization is as following:

- 生产网络拓扑图
Production network topology
- F1000-E-SI 防火墙配置
F1000-E-SI firewall configuration
- F100-S-G 防火墙配置
F100-SG firewall configuration

授权信息

Authorization information

姓名: _____

Name: _____

职位: 首席信息安全官

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可，任何人不得对此机密档的全部或部份进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

文件种类：管制文件 File Type: controlled document

	四川科道芯国智能技术股份有限公司 Sichuan Keydom Smart Technology Co., Ltd.	文件编号: Document No. :	KD-LJ01-003
KEYDOM	Class 3 Document 三级文件 网络配置授权书 Network Configuration Authorization	版本号: Version number:	C/2

Position: Chief Information Security Officer

签名:

Signature:



日期:

Date:

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可，任何人不得对此机密档的全部或部份进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

文件种类：管制文件 File Type: controlled document

	四川科道芯国智能技术股份有限公司 Sichuan Keydom Smart Technology Co., Ltd.	文件编号: Document No. :	KD-LJ01-003
	Class 3 Document 三级文件 网络配置授权书 Network Configuration Authorization	版本号: Version number:	C/2

2 网络拓扑图（见附件 1）

Network Topology (Annex I)

3 H3C F1000-E-SI 防火墙安全策略（见附件 2）

H3C F1000-E-SI Firewall Security Policy (Annex II)

4 H3C F100-S-G 防火墙安全策略（见附件 3）

H3C F100-SG Firewall Security Policy (Annex III)

本文所包含内容所有权归属<四川科道芯国智能技术股份有限公司>。未经<四川科道芯国智能技术股份有限公司>书面许可，任何人不得对此机密档的全部或部分进行复制、出版或交第三方使用。

All ownership included in this article belongs to <Sichuan KEYDOM Intelligent Technology Co., Ltd. >. No part of this confidential document may be copied, published or used by third parties without the written permission of <Sichuan KEYDOM Intelligent Technology Co., Ltd.>.

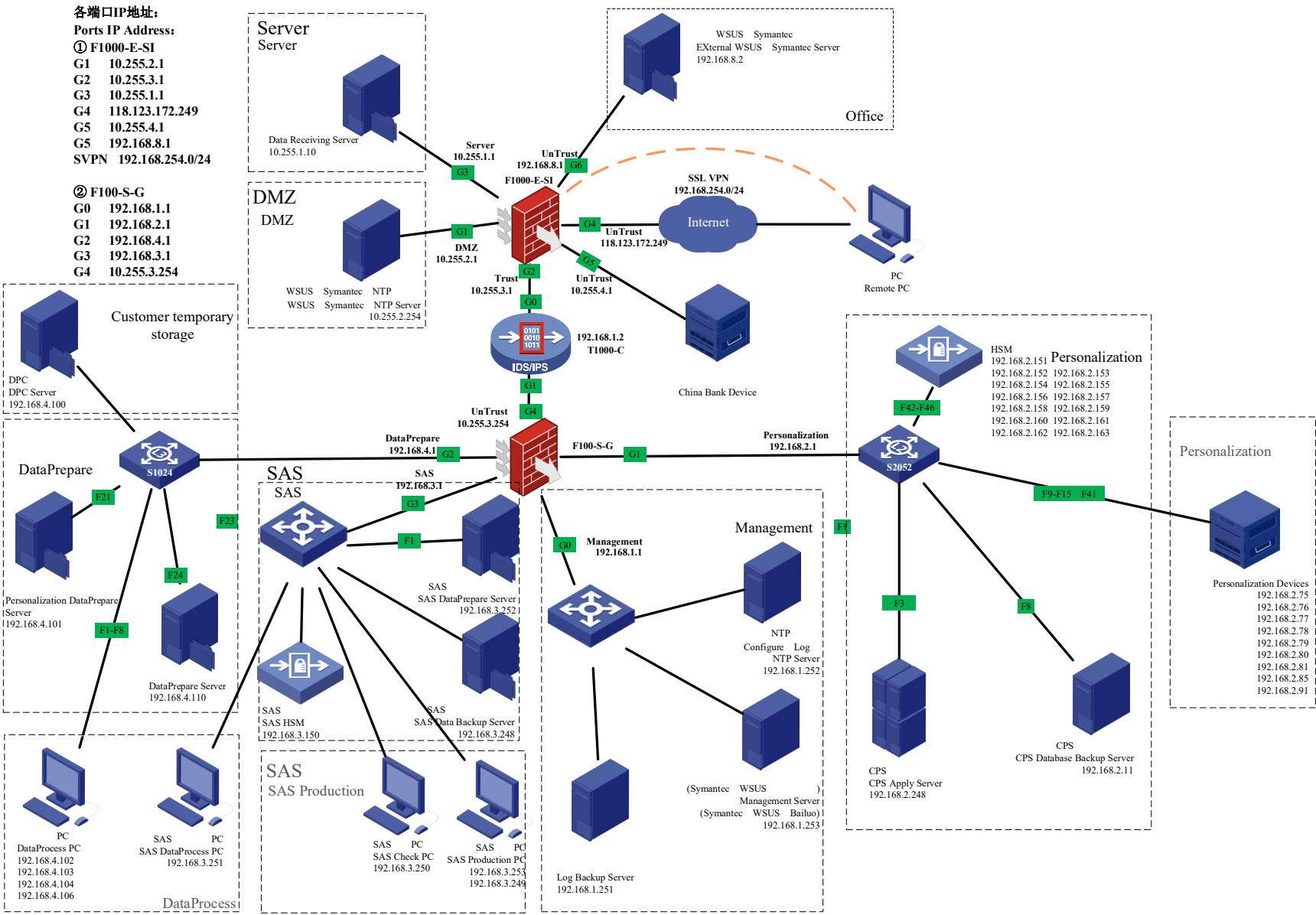
文件种类：管制文件 File Type: controlled document

附件一：生产网络拓扑图

Annex I: Production Network Topology

版本号：C/2

Version number: C/2 密级：3 级 机密



批准：
Approved by:

附件二：F1000-E-SI 防火墙安全策略

Annex II: F1000-E-SI Security Policy for Firewall 密级：3级 机密

Direction		P/D	IP				Port/service	Reason
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。
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.

批准：
Approved by:

附件二：F1000-E-SI 防火墙安全策略

Annex II: F1000-E-SI Security Policy for Firewall 密级：3级 机密

Direction		P/D	IP				Port/service	Reason
Source	Destination		Source		Destination			
UnTrust	Local	Permit	192.168.0.88	0.0.0.0	118.123.172.249	0.0.0.0	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	0.0.0.0	118.123.172.249	0.0.0.0	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	0.0.0.0	118.123.172.249	0.0.0.0	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	0.0.0.0	118.123.172.249	0.0.0.0	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	0.0.0.0	118.123.172.249	0.0.0.0	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	0.0.0.0	118.123.172.249	0.0.0.0	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	0.0.0.0	118.123.172.249	0.0.0.0	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。
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.
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.

批准：
Approved by:

附件二：F1000-E-SI 防火墙安全策略

Annex II：F1000-E-SI Security Policy for Firewall 密级：3级 机密

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

批准：
Approved by:

附件三：F100-S-G 防火墙安全策略

Annex III: F100-S-G Security Policy for Firewall 密级: 3级 机密

Direction		P/D	IP				Port/service	Reason
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.

批准：

Approved by:

附件三：F100-S-G 防火墙安全策略

Annex III: F100-S-G Security Policy for Firewall 密级: 3级 机密

Direction		P/D	IP				Port/service	Reason
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

附件三：F100-S-G 防火墙安全策略

Annex III: F100-S-G Security Policy for Firewall 密级：3级 机密

Direction		P/D	IP				Port/service	Reason
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.

附件三：F100-S-G 防火墙安全策略

Annex III: F100-S-G Security Policy for Firewall 密级: 3级 机密

Direction		P/D	IP				Port/service	Reason
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.