KD-LJ01-003

版本号: Version number:

1/2

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.>.

Version number:



三级文件 网络配置授权书 Network Configuration Authorization

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.>.

KD-LJ01-003

C/2

版 本 号: Version number:

三級文件 网络配置投权 + ument Network Configuration Authorization Nass 3 Document 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 王建勋 刘劲松 更换 log 及公司名称 黄伟 B/4 Liu Change log and company 2018/7/25 Wang Huang Wei Jianxun Jinsong name 更新网络拓扑图, F1000 防 刘劲松 火墙策略 王建勋 黄伟 2、3 B/5 Update the network 2018/12/20 Liu Wang Huang Wei F1000 topology and Jianxun Jinsong firewall policy 更新 F1000 防火墙策略 王建勋 刘劲松 黄伟 Update F1000 firewall 3 B/6 2019/01/22 Wang Liu Huang Wei policy Jianxun Jinsong 更新网络拓扑图 Update network topology 更新 F1000 防火墙策略 王建勋 刘劲松 黄伟 Update F1000 firewall 2, 3, 4 B/7 2019/09/18 Wang Liu Huang Wei policy Jianxun Jinsong 更新 F100 防火墙策略 Update F100 firewall policy 更新网络拓扑图 黄伟 王建勋 刘劲松 2, 3, 4 2019/11/06 B/8

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。

Update network topology

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.>.

Wang

Liu

Huang Wei

KD-LJ01-003

三级文件 网络配置授权书 San Document 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 更新 F1000 防火墙策略 Update network topology 更新 F1000 防火墙策略 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 五式 F100 F10 F10 F10 F10 F10 F10 F10 F10 F1			Update F1000 firewall policy			Jianxun	Jinsong
更新 F100 防火墙策略 Update F100 firewall policy 更新 MS F100 防火墙策略 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 2、3、4 B/9 E建勋 刘劲松 Huang Wei Jianxun Jinsong			policy				
更新 F100 防火墙策略 Update F100 firewall policy 更新 M9 E新 F100 防火墙策略 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy E							
Update F100 firewall policy 更新网络拓扑图 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 黄伟 Wang Liu Jianxun Jinsong			更新 F100 防火墙策略				
policy 更新网络拓扑图 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 型							
更新网络拓扑图 Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 2、3、4 B/9 E 建勋 刘劲松 Huang Wei Jianxun Jinsong			Update F100 firewall				
Update network topology 更新 F1000 防火墙策略 Update F1000 firewall policy 2、3、4 B/9 Update F1000 firewall policy 2019/11/19 Huang Wei Jianxun Jinsong			policy				
更新 F1000 防火墙策略 Update F1000 firewall policy B/9 E新 F1000 防火墙策略 T 建勋 刘	, I		更新网络拓扑图				
Update F1000 firewall 2、3、4 B/9 Update F1000 firewall policy jianxun Jinsong			Update network topology				
Update F1000 firewall 2019/11/19 黄伟 Wang Liu policy Jianxun Jinsong			更新 F1000 防火墙策略			工净品) 기자사
policy Huang Wei Jianxun Jinsong	2 2 4	D/0	Update F1000 firewall	2010/11/10	黄伟		
	2, 3, 4	В/9	policy	2019/11/19	Huang Wei	_	
果新 F100 防火墙策略			更新 F100 防火墙策略			Jianxun	Jinsong
Update F100 firewall			Update F100 firewall				
policy			policy				
更新网络拓扑图			更新网络拓扑图				
Update network topology			Update network topology				
更新 F1000 防火墙策略 王建勋 刘劲松			更新 F1000 防火墙策略			工建品	ᆌᄼᆀᄽ
Update F1000 firewall 2020.1.1 黄伟 Wang Liu	2 3 4	C/0	Update F1000 firewall	2020 1 1	黄伟		
policy Huang Wei Jianxun Jinsong	2, 3, 4	C/0	policy	2020.1.1	Huang Wei	_	
更新 F100 防火墙策略			更新 F100 防火墙策略			Jianxun	Jinsong
Update F100 firewall			Update F100 firewall				
policy			policy				
更新网络拓扑图			更新网络拓扑图				
Update network topology 王建勋 刘劲松			Update network topology			工建 勋	刘孙松
更新 F1000 防火墙策略	2. 3. 4	C/1	更新 F1000 防火墙策略	2020 1 17	黄伟		
Update F1000 firewall Huang Wei Jianxun Jinsong	2\ J, T	C/ 1	Update F1000 firewall	2020.1.11	Huang Wei	_	
policy			policy			Jianaun	amoong
更新 F100 防火墙策略			更新 F100 防火墙策略				

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. >.



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

KD-LJ01-003

版本号: Version number:

C/2

目 录

Contents

1	网络配置	授权	z书 N	letwor	k Con	fig	uratior	ı Aut	tho	orizatio	n				7
2	网络拓扑	图 (见附	件1)	Net	W01	rk Top	olog	y (Annex	κI)				9
3 F	H3C F100	0-E-	SI 防	火墙的	安全策	略	(见附	件 2)	Н3С І	F1000)-E-S	I Fire	wall	Security
Po	licy (Ann	ex II	(9
4]	H3C F10	0-S-	G 防シ	人墙安	全策	略	(见附	件 3)	Н3С	F100)-SG	Firev	vall	Security
Po	licy (Ann	ex II	(II)			• • • • •									9

KD-LJ01-003

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 infor	mation
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.>.

Position: Chief Information Security Officer

签名:

Signature:

日期:

Date:



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)

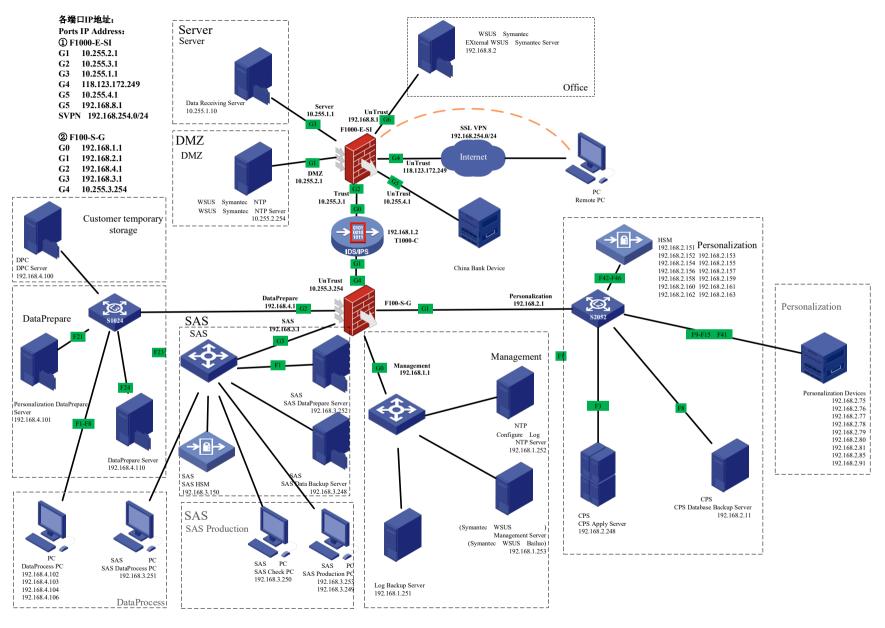
4 H3C F100-S-G 防火墙安全策略(见附件3)

H3C F100-SG Firewall Security Policy (Annex III)

版本号: C/2

Annex I: Production Network Topology

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

				IP IP	Olicy lo		LCWall High. Ogg	<i>y</i> • EE
Source	rection Destination	P/D	Source	IF	Destination	2	Port/service	Reason
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31842-318 43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。
				0.0.0.0		0.0.0.0		拒绝访问Internet。
Server	UnTrust	Deny	Any		Any		Any	Deny access to the Internet.
								仅允许数据接收服务器通过Ping, WSUS, NTP服务访问WSUS服务器
Server	DMZ	Permit	10.255.1.10	0.0.0.0	10.255.2.254	0.0.0.0	Ping,WSUS,NTP	Permit access of data receiving server to WSUS servers only through Ping, WSUS and NTP
								services.
Convor	DMZ	Deny	Any		Anv		Any	拒绝访问到DMZ区。
Server	DIVIZ	Deny	Any		Any		Any	Deny access to the DMZ
								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
Server	Trust	Permit	10.255.1.10	0.0.0.0	192.168.1.253	0.0.0.0	Bailuo,Symantec,Ping	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。
OTTTUSE	JCI VCI	1 CITIIL	132.100.234.0	0.0.0.200	10.233.1.10	0.0.0.0		仅允许卫计委通过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	Permit access of National Health and Family Planning Commission of the People's Republic of
								China to data receiving server only through FTP service.
								仅允许卫计委通过FTP服务访问数据接收服务器。
UnTrust	Server	Permit	182.150.13.131	0.0.0.0	10.255.1.10	0.0.0.0	FTP	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。
OTTTTGGE	001401	1 OIIIIIC	10.00.7.10	0.0.0.0	10.200.1.10	0.0.0.0		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. 仅允许天府通通过FTP服务访问数据接收服务器。
UnTrust	Server	Permit	182.140.133.54	0.0.0.0	10.255.1.10	0.0.0.0	FTP	1X.允许大府通通过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.
								仅允许银联通过FTP服务访问数据接收服务器。
UnTrust	Server	Permit	31.0.0.50	0.0.0.0	10.15.132.2	0.0.0.0	FTP	Permit access of Yinlian Tong to data receiving server only through FTP service.
		n .	101 000 100	0.000	10.15.100.0		FT0	仅允许银联通过FTP服务访问数据接收服务器。
UnTrust	Server	Permit	101.230.4.30	0.0.0.0	10.15.132.2	0.0.0.0	FTP	Permit access of Yinlian Tong to data receiving server only through FTP service.
								仅允许省中行设备通过FTP服务访问数据接收服务器。
UnTrust	Server	Permit	10.255.4.0	0.0.0.255	10.255.1.10	0.0.0.0	FTP	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。
01111400	00.70.	. 01111110	100.2001200.20	0.0.0.200	20.200.2.20	0.0.0.0		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. 拒绝访问到Server区。
UnTrust	Server	Deny	Any		Any		Any	TE绝명미화JServer区。 Deny access to the Server.
								仅允许WSUS外部服务器通过Symantec, WSUS, Ping服务访问WSUS服务器。
UnTrust	DMZ	Permit	192.168.8.2	0.0.0.0	10.255.2.254	0.0.0.0	Symantec,WSUS,Ping	permit access of the WSUS External server to WSUS server through Symantec, WSUS and Ping
OTTTASE	DIVIZ	1 GIIIIIC	102.100.0.2	0.0.0.0	10.200.2.201	0.0.0.0	dymanted, wood, mg	service.
								拒绝访问到DMZ区。
UnTrust	DMZ	Deny	Any		Any		Any	Deny access to the DMZ.
11. =			Δ.				^	拒绝访问到内部网络。
UnTrust	Trust	Deny	Any		Any		Any	Deny access to internal network.
UnTrust	Local	Permit	Λm.		118.123.172.249	0.0.0.0	HTTD9 Ding	仅允许远端PC连接SSL-VPN
Unitust	LOCAL	Permit	Any		110.123.172.249	0.0.0.0	HTTPS,Ping	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

			B DI BOOG		Olicy 10		LCWall 出级。 0级) o L
	irection	P/D		IP			Port/service	Reason
Source	Destination	.,-	Source		Destination	1		
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P。 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 Yikahul 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:

第2页,共3页 Page 2 of 3 文件编号:KD-LJ01-003 Rev:C/2 Document No.:KD-LJ01-003 Rev:C/2

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

				2	9			V		
	Direction	P/D	IP				Port/service	Reason		
Source	Destination	P/D	Source		Destinatio	n	POIT/Service	Reason		
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。		



第3页,共3页 Page 3 of 3 文件编号:KD-LJ01-003 Rev:C/2 Document No.:KD-LJ01-003 Rev:C/2

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

Direc					P		二 齿蚁:3蚁 小田	-
Source	Destination	P/D	Source		Destination	1	Port/service	Reason
UnTrust	DataPrepare	Deny	Any		Any		Any	拒绝来自外部网络的任何访问。
OTTTUSE	Datai repaire	Derity	7 (11)		7 (11y		7 1119	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.
								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。
UnTrust	Management	Permit	10.255.1.10	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,Ping	Only allow the data receiving server to access the management server through BaiLuo, Symantec, and
Onridat	Wanagement	1 GITTIE	10.200.1.10	0.0.0.0	102.100.1.200	0.0.0.0	bailea0,0ymaneo,i mg	Ping service.
								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。
UnTrust	Management	Permit	10.255.2.254	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping	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。
01111400	management		20120012120	0.0.0.0	102.1200.11.202	0.0.0.0	239	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. 仅允许F1000防火墙通过Syslog服务访问日志服务器。
UnTrust	Management	Permit	10.255.3.1	0.0.0.0	192.168.1.252	0.0.0.0	Syslog	Permit access of F1000 firewall to the log server only via Syslog service.
								拒绝来自外部网络的任何访问。
UnTrust	Management	Deny	Any		Any		Any	Deny any access from external network.
		-						拒绝外部登录防火墙。
UnTrust	Local	Deny	Any		Any		Any	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。
Datai repare	3/13	Derity	Ally		Ally		Ally	Deny any access from the data staging area to the SAS area.
			192.168.4.102-104,					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
DataPrepare	Personalization	Permit	106	0.0.0.0	192.168.2.11	0.0.0.0	FTP,MySQL	Only allow the data processing PC to access the CPS database backup server through FTP and MySQL
								service 允许数据主管PC访问154加密机
DataPrepare	Personalization	Permit	192.168.4.104	0.0.0.0	192.168.2.154	0.0.0.0	Ping,8	元计数据主管PC切向154加密机 Allow data supervisor PC to access 154 encryptor
								允许DPC数据准备服务器访问DPC加密机
DataPrepare	Personalization	Permit	192.168.4.100	0.0.0.0	192.168.2.161	0.0.0.0	Ping,8	Allow DPC data preparation server to access DPC encryptor
D . D	D 11 11	Б :	100 100 1100	0000	192.168.2.75-81,	0.000	^	允许DPC数据准备服务器访问个人化设备
DataPrepare	Personalization	Permit	192.168.4.100	0.0.0.0	85, 91	0.0.0.0	Any	Allow DPC data preparation server to access personalization device
DataPrepare	Personalization	Permit	192.168.4.102-104,	0.0.0.0	192.168.2.248	0.0.0.0	MySOL	仅允许数据处理PC通过MySQL服务访问CPS应用服务器
Datai repare	T ersonalization	1 GIIIIIL	106	0.0.0.0	132.100.2.240	0.0.0.0	IVIYSQL	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.
DataBassass	Management	D '+	100 100 4 110	0000	100 100 1 050	0.0.0.0	Dailous Comanda a MICHIC Disas A D	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。
DataPrepare	Management	Permit	192.168.4.110	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	Only allow the data preparation server to access the management server through BaiLuo, Symantec, WSUS, and Ping service.
								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。
DataPrepare	Management	Permit	192.168.4.101	0.0.0.0	192.168.1.253	0.0.0.0	BaiLuo,Symantec,WSUS,Ping,AD	Only allow the personalization data preparation server to access the management server through
_ ata opa10	ariagomone	. 5111116		0.0.0.0	102,100,1,100	0.0.0.0		BaiLuo, Symantec, WSUS, and Ping service.
			400 400 4400 404					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。
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	Only allow the data processing PC to access the management server through BaiLuo , Symantec, WSUS
			100					and Ping service.
								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。
DataPrepare	Management	Permit	192.168.4.110	0.0.0.0	192.168.1.252	0.0.0.0	NTP,Log	Only allow the data preparation server and data processing PC to access the log server through NTP
								and Log service.

批准: Approved by:

第1页, 共4页 Page 1 of 4 文件编号: KD-LJ01-003 Rev: C/2 Document No.: KD-LJ01-003 Rev: C/2

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

Direc				1			TI 苗級: 5級 小陆	Descrip
Source	Destination	P/D	Source		Destination		Port/service	Reason
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

批准: Approved by:

第2页, 共4页 Page 2 of 4 文件编号: KD-LJ01-003 Rev: C/2 Document No.: KD-LJ01-003 Rev: C/2

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

	1. 1100		bootifuj	1011		II Owa		
Source Direct	Destination	P/D	Source	I	P Destination	1	Port/service	Reason
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.

批准: Approved by:

第3页, 共4页 Page 3 of 4 文件编号: KD-LJ01-003 Rev: C/2 Document No.: KD-LJ01-003 Rev: C/2

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

Direc	ction	P/D		I	Р		Port/service	Reason
Source	Destination	P/D	Source		Destination		FOIT/Service	Reason
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Symantes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.

文件编号: KD-LJ01-003 Rev: C/2 Document No.: KD-LJ01-003 Rev: C/2