证联网入网安全管理规范

证联网管理办公室

2018.05

第一章 总则

第一条 为保障证联网安全稳定运行，加强证联网信息安全管理工作，根据《中华人民共和国网络安全法》《证券期货业信息安全保障管理办法》《证券期货业信息系统运维管理规范》《证券期货业信息系统安全等级保护基本要求》《证券期货业信息系统审计指南》等相关法律法规、规章制度，制定本规范。

第二条 本规范适用于证联网接入安全管理与保障等相关工作。

第三条 证联网信息安全管理工作实行“谁运行、谁负责，谁使用、谁负责”和“安全优先、保障发展”的原则。

第四条 证券期货业信息化工作领导小组办公室（以下简称证信办）负责证联网信息安全管理工作的指导、监督和检查。证联网管理办公室是证信办领导下的证联网议事机构，负责制定证联网信息安全工作的总体方针、安全策略和管理制度。

第五条 证联网运管中心（以下简称运管中心）负责证联网信息安全的整体监测、协调等工作。证联网各承建单位（以下简称承建单位）负责各自节点的信息安全监测和保障工作，并承担本节点的安全运行责任。

第六条 证联网接入机构（以下简称接入机构）负责本机构网络的安全管理，并负责本机构业务系统的安全保障。

第二章 基本要求

第七条 接入机构应充分考虑国家和监管部门的信息安全相关要求，同步配套健全相关信息安全管理制度和设施。

第八条 接入机构应加强与运管中心、承建单位的沟通协作，共同保障证联网安全。

第九条 接入机构应按照所属行业信息安全等级保护第三级的要求，做好直连证联网生产网设备的安全防护。

第十条 接入机构应当确保接入证联网的设备符合国家和金融行业的安全标准、技术规范和质量要求。

第三章 接入机构职责

第十一条 接入机构应根据国家、行业信息安全和应急管理相关规定以及本规范的要求，制定网络和信息安全应急预案，并定期演练。

第十二条 接入机构应当配合运管中心和承建单位进行配置检查、应急演练和应急处置等工作。

第十三条 接入机构应当按照证联网要求的网络接入方式接入，并按要求为接入路由器、服务器、终端等设备分配 IP 地址并进行网络配置。

第十四条 接入机构负责自身网络和业务系统的安全保障，应当采取足够的安全防护措施，有效防范其他接入机构的安全隐患波及自身安全。发现其他接入机构存在安全隐患时，应及时告知相关机构，并向运管中心报告。

第十五条 接入机构负有保护证联网安全的共同义务，应在网络边界处部署设备或采取相应的技术措施，按照权限最小化原则进行双向访问控制，检查并阻止非授权的、非法的流量进入证联网，防止非授权用户、病毒、恶意程序和黑客通过接入机构的网络、系统或终端

攻击证联网。

第十六条 接入机构应做好网络隔离和安全防护措施，实现机构内网、证联网与互联网的有效隔离，禁止接入证联网的服务器、终端等设备访问互联网。

第十七条 接入机构自身业务系统不得设置恶意程序，发现自身设备、系统存在安全缺陷、漏洞等风险时，应当立即采取补救措施。如可能对证联网造成安全隐患，应及时向运管中心报告。

第十八条 接入机构负责自身接入证联网终端的安全管理，接入证联网的终端设备必须按照国家及行业发布的相关法律、法规、规定做好安全加固及防护工作。此外，接入机构还应该采取必要的技术措施，对接入证联网的终端进行主机监控、移动介质管理、非授权外连管理等。

第十九条 接入机构应当充分了解并评估证联网的安全保密条件是否满足自身业务的需求，如果业务有更高的安全保密要求，接入机构应当自行采用数据加密等安全措施，保障数据安全。

第二十条 接入机构应当充分了解评估证联网的传输能力、备份能力和容错能力能否满足自身业务的连续性要求，如果业务需要更高的保障条件，接入机构应当自行采取额外的线路备份、系统备份和业务备份等措施，切实保证自身业务的连续性。

第二十一条 接入机构不得在证联网上传播威胁国家安全，危害公民隐私等法律、法规禁止传输的信息。

第四章 自查与监督

第二十二条 本规范中的相关要求纳入《证券期货行业信息系统审计指南》，证券期货行业接入机构应严格按照相关要求进行自我检查和评价，做好证联网信息安全管理工作。其它行业接入机构参照执行。

第二十三条 运管中心和承建单位发现接入机构在证联网传播法律、法规禁止传输的信息，或者对证联网进行网络攻击、网络侵入、传播计算机病毒等危害网络安全的行为，应立即通知接入机构停止违规行为，并报告证信办。机构拒不执行的，运管中心和承建单位有权暂停其接入证联网。

第五章 附则

第二十四条 本规范由证信办负责发布和解释。

第二十五条 本规范自发布之日起施行。

附件 1：

生产网网络及安全配置指引

一、网络及安全配置要求

1. 网络要求

（1）接入机构根据机房所在位置就近接入证联网生产网，接入线路原则上应采用主备方式，具备两地三中心机房条件的接入机构可以申请第三条线接入。原则上银行、证券、基金类机构主用生产网 A 组节点（BJ-1、SH-1、SZ-1、SH-3、ZZ-1、DL-1），期货类机构主用 B 组节点（BJ-2、SH-2、SZ-2、SH-4、ZZ-2、DL-2）。

（2）证联网生产网支持运营商专线接入和交易所托管机房接入两种方式，机构根据自身情况自行选择。采用运营商专线接入时，应选择不同运营商的线路实现链路冗余。

（3）证联网运管中心负责为接入机构统一分配网络互联 IP 地址和业务 IP 地址，原则上业务 IP 地址只能用于接入机构服务器或终端设备，不能用于接入机构内部网络设备互联。接入机构应配置 NAT，隐藏内部主机的实际 IP 地址。服务器 IP 地址应在 41.x.x.1-41.x.x.223 和 41.x.x.240-41.x.x.254 内规划，终端设备 IP 地址应在 41.x.x.224-41.x.x.239 内规划。

（4）接入机构应在与生产网直连的接入设备上配置 BFD（双向转发检测）功能，监测网络的连通性，同时配置静态路由与 BFD 联动机制实现主、备线路自动切换。

（5）机构内部网络应采取技术措施（IP SLA、NQA、VRRP/HSRP、

浮动路由等）确保主用线路中断时，能够实现自动切换，保证业务不中断。

（6）接入机构应将生产网接入线路纳入本单位的监控系统，实时监控接入线路状态，并定期评估带宽使用率，以满足业务需求。

2. 安全要求

（1）接入机构应按照信息安全等级保护三级要求，部署防火墙、安全网关等设备，将自身网络分成逻辑安全区域，对每个区域进行安全防护，保障证联网生产网网络和业务系统安全。

（2）接入机构应按照权限最小化原则进行双向访问控制，出方向按照实际访问需求，配置访问控制策略，访问控制规则必须包括源IP、目的IP、目的端口、协议；入方向应按照对外提供的服务需求，配置访问控制策略，访问控制规则必须包括源IP、目的IP、目的端口、协议。

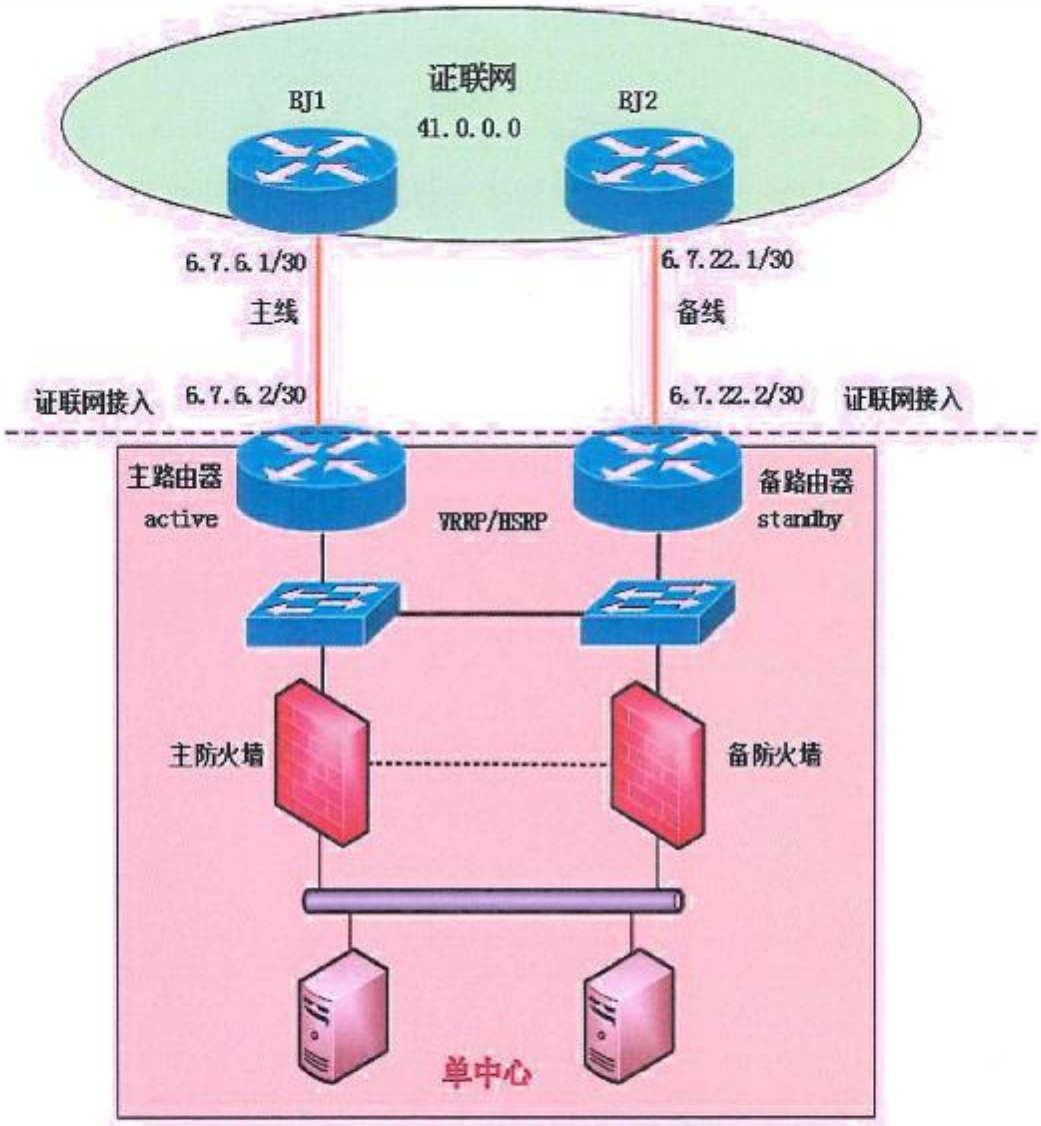
（3）接入生产网的服务器和终端必须参照《证券期货业信息系统运维管理规范》、《证券期货业信息系统安全等级保护基本要求》、《证券期货业信息系统审计指南》的要求，做好安全管理。此外，接入机构还应该采取必要的技术措施，对接入证联网的终端进行主机监控、移动介质管理、非授权外连管理等。

二、接入模式及配置参考

1. 接入模式一：单中心接入

接入机构在某城市只有单中心的，应申请两条线路，接入证联网同一对接入节点，两条线路互为备份，使用相同的业务IP地址。

（1）接入示意图：



注：图中所有IP地址均为示例IP，设备配置请根据实际分配IP地址为准：
证联网互联IP段：6.7.6.0/30 6.7.22.0/30
证联网分配的业务IP：41.13.0.0/24
内网业务IP：10.1.100.0/24

（2）路由器接口配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
ip address 6.7.6.2 255.255.255.252	ip address 6.7.6.2 255.255.255.252	与证联网互联接口
undo shutdown	no shutdown	激活接口

interface GigabitEthernet0/1	interface GigabitEthernet0/1	
ip address 10.1.1.253 255.255.255.0	ip address 10.1.1.253 255.255.255.0	内网接口
undo shutdown	no shutdown	激活接口
用户路由器 R2 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
ip address 6.7.22.2 255.255.255.252	ip address 6.7.22.2 255.255.255.252	与证联网互联接口
undo shutdown	no shutdown	激活接口
interface GigabitEthernet0/1	interface GigabitEthernet0/1	
ip address 10.1.1.252 255.255.255.0	ip address 10.1.1.252 255.255.255.0	内网接口
undo shutdown	no shutdown	激活接口

（3）VRRP/HSRP 配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
interface GigabitEthernet0/1	interface GigabitEthernet0/1	
vrrp vrid 1 virtual-ip 10.1.1.254	standby 1 ip 10.1.1.254	虚拟网关
vrrp vrid 1 priority 120	standby 1 priority 120	优先级
vrrp vrid 1 preempt	standby 1 preempt	开启抢占
（适用于托管机房）		
vrrp vrid 1 track 1 priority reduced 50	standby 1 track 1 G0/0 50	Track 与接口联动（适用于托管机房）
track 1 interface GigabitEthernet0/0	track 1 interface GigabitEthernet0/0 ip routing	开启 Track（适用于托管机房）
（适用于运营商专线）		
interface GigabitEthernet0/1	interface GigabitEthernet0/1	
vrrp vrid 1 track 2 priority reduced 50	standby 1 track 2 decrement 50	Track 与接口联动（适用于运营商专线）
nqa entry admin test1 type icmp-echo destination ip 6.7.6.1 source ip 6.7.6.2 frequency 500 reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only	ip sla 1 icmp-echo 6.7.6.1 source-ip 6.7.6.2	监控上联 IP 地址可达性（适用于运营商专线）

nqa schedule admin test1 start-time now lifetime forever	ip sla schedule 1 life forever start-time now	开启探测（适用于运营商专线）
track 2 nqa entry admin test1 reaction 1	track 2 ip sla 1 reachability	Track 与 sla/nqa 联动（适用于运营商专线）
用户路由器 R2 配置		
interface GigabitEthernet0/1	interface GigabitEthernet0/1	
ip address 10.1.1.252 255.255.255.0	ip address 10.1.1.252 255.255.255.0	内网接口
vrrp vrid 1 virtual-ip 10.1.1.254	standby 1 ip 10.1.1.254	虚拟网关
注：接入机构通过运营商专线接入证联网时，应通过 Track 与 SLA（NQA）联动机制检测线路状态，实现 VRRP/HSRP 虚拟网关自动切换，保证业务不中断。当主线路恢复后，通过配置抢占功能，将 VRRP/HSRP 虚拟网关自动切换回主路由器。		

（4）BFD 配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
bfd min-receive-interval 500	bfd interval 500 min_rx 500 multiplier 3	BFD 检测参数配置（接受间隔）
bfd min-transmit-interval 500		BFD 检测参数配置（发送间隔）
bfd detect-multiplier 3		BFD 检测参数配置（检测次数）
用户路由器 R2 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
bfd min-receive-interval 500	bfd interval 500 min_rx 500 multiplier 3	BFD 检测参数配置（接受间隔）
bfd min-transmit-interval 500		BFD 检测参数配置（发送间隔）
bfd detect-multiplier 3		BFD 检测参数配置（检测次数）

（5）路由配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
ip route-static 41.0.0.0 255.0.0.0 GigabitEthernet0/0 6.7.6.1 bfd control-packet preference 1	ip route static bfd G0/0 6.7.6.1 ip route 41.0.0.0 255.0.0.0 G0/0 6.7.6.1	配置去往证联网路由
ip route-static 41.13.0.0 255.255.255.0	ip route 41.13.0.0 255.255.255.0	配置去往内部路由

GigabitEthernet0/1 10.1.1.10	G0/1 10.1.1.10	
用户路由器 R2 配置		
ip route-static 41.0.0.0 255.0.0.0 GigabitEthernet0/0 6.7.22.1 bfd control-packet preference 1	ip route static bfd G0/0 6.7.22.1 ip route 41.0.0.0 255.0.0.0 G0/0 6.7.22.1	配置去往证联网路由
ip route-static 41.13.0.0 255.255.255.0 GigabitEthernet0/1 10.1.1.10	ip route 41.13.0.0 255.255.255.0 G0/1 10.1.1.10	配置去往内部路由

（6）禁用病毒端口参考

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
acl advanced name Denyport rule deny tcp destination-port range 135 139 rule deny tcp destination-port eq 445 rule deny udp destination-port eq 445 rule permit ip	ip access-list extended Denyport deny tcp any any range msrpc 139 deny tcp any any eq 445 deny udp any any eq 445 permit ip any any	访问控制策略
interface GigabitEthernet0/0 packet-filter name Denyport inbound packet-filter name Denyport outbound	interface GigabitEthernet0/0 ip access-group Denyport in ip access-group Denyport out	调用访问控制策略
用户路由器 R2 配置		
acl advanced name Denyport rule deny tcp destination-port range 135 139 rule deny tcp destination-port eq 445 rule deny udp destination-port eq 445 rule permit ip	ip access-list extended Denyport deny tcp any any range msrpc 139 deny tcp any any eq 445 deny udp any any eq 445 permit ip any any	访问控制策略策略
interface GigabitEthernet0/0 packet-filter name Denyport inbound packet-filter name Denyport outbound	interface GigabitEthernet0/0 ip access-group Denyport in ip access-group Denyport out	调用访问控制策略

（7）防火墙 NAT 配置

H3C 配置	Cisco 配置（v9.5）	配置说明
动态 NAT 配置（客户端使用）		
nat address-group 1 41.13.0.X 41.13.0.X	object network Inside-to-Outside-POOL range 41.13.0.x 41.13.0.x	配置动态 NAT 池
acl number 2xxx rule permit source 10.1.100.0 0.0.0.255 rule deny	object network Inside-Network-NAT-Outside subnet 10.1.100.x 255.255.255.x nat (inside,outside) dynamic	动态 PAT 转换

interface gigabitethernet x/x nat outbound 2xxx address-group 1	pat-pool Inside-to-Outside-POOL round-robin	
静态 NAT 配置（服务器使用）		
nat static 10.1.100.X 41.13.0.X interface gigabitethernet x/x nat outbound static	object network Inside-Server host 10.1.100.x nat (inside,outside) static 41.13.0.x	静态 NAT

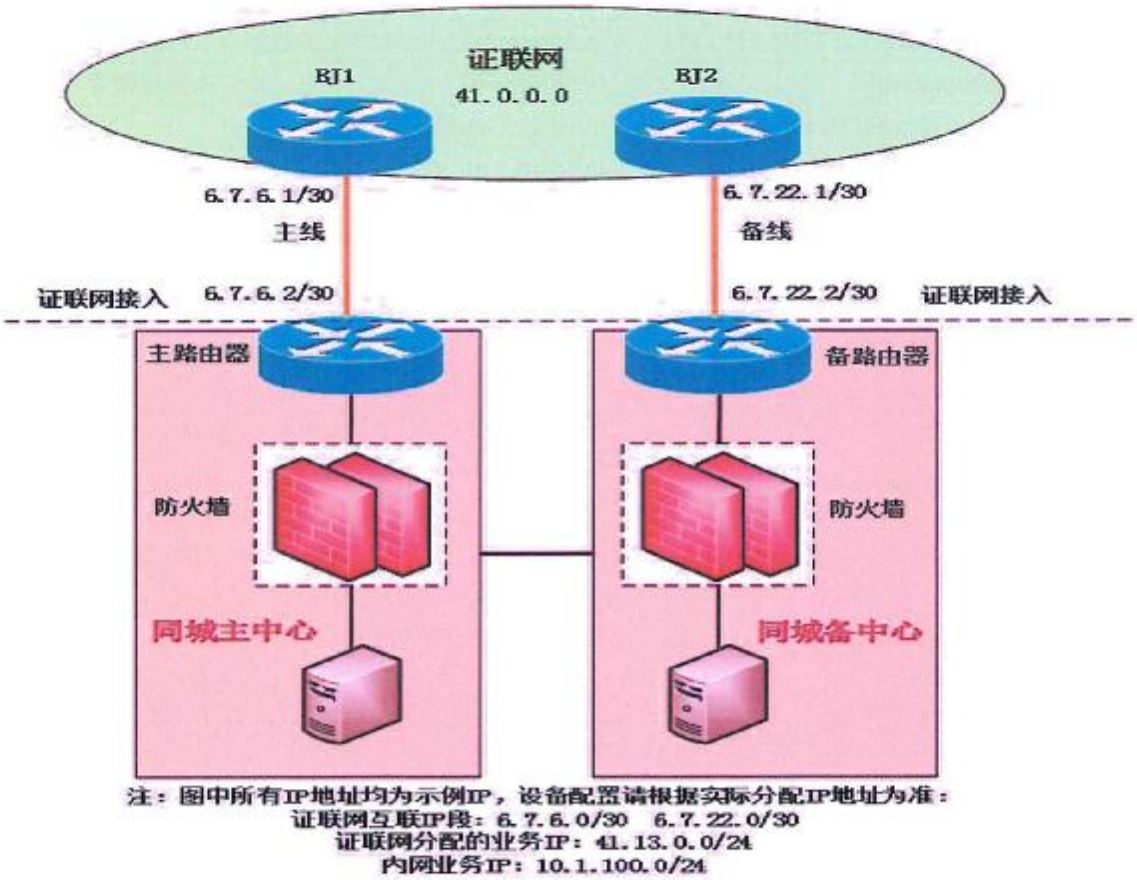
（8）防火墙访问控制策略配置

H3C 配置	Cisco 配置（v9.5）	配置说明
acl number 3xxx rule 0 permit icmp source 41.x.x.x 0 destination 10.1.100.x 0 rule 5 permit tcp source 41.x.x.x 0 destination 10.1.100.x 0 destination-port eq ftp rule 10 permit tcp source 41.x.x.x 0 destination 10.1.100.x 0 destination-port eq www rule 15 deny ip logging	access-list Outside_access_Inside extended permit icmp host 41.X.X.X host 10.1.100.X access-list Outside_access_Inside extended permit tcp host 41.X.X.X host 10.1.100.X eq ftp access-list Outside_access_Inside extended permit tcp host 41.X.X.X host 10.1.100.X eq www access-list Outside_access_Inside extended deny ip any any log notifications	按照权限最小化原则配置防火墙入方向访问控制策略
acl number 3yyy rule 0 permit icmp source 10.1.100.x 0 destination 41.x.x.x 0 rule 5 permit tcp source 10.1.100.x 0 destination 41.x.x.x 0 destination-port eq www rule 10 permit tcp source 10.1.100.x 0 destination 41.x.x.x 0 destination-port eq ftp rule 15 deny ip logging	access-list Inside_access_Outside extended permit icmp host 10.1.100.X host 41.X.X.X access-list Inside_access_Outside extended permit tcp host 10.1.100.X host 41.X.X.X eq ftp access-list Inside_access_Outside extended permit tcp host 10.1.100.X host 41.X.X.X eq www access-list Inside_access_Outside extended deny ip any any log notifications	按照权限最小化原则配置防火墙出方向访问控制策略
interzone source outside destination inside rule acl 3xxx rule acl enable	access-group Outside_access_Inside in interface Outside	调用入方向策略
interzone source inside destination outside rule acl 3yyy rule acl enable	access-group Inside_access_Outside in interface Inside	调用出方向策略

2. 接入模式二：同城主、备双中心接入

接入机构在同一城市有主、备双中心的，双中心之间网络应保证互通，同城主、备中心应分别申请一条线路，接入证联网同一对接入节点，两条线路互为备份，使用相同的业务 IP 地址。

（1）接入示意图：



（2）路由器接口配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
ip address 6.7.6.2 255.255.255.252	ip address 6.7.6.2 255.255.255.252	与证联网互联接口
undo shutdown	no shutdown	激活接口
interface GigabitEthernet0/1	interface GigabitEthernet0/1	
ip address 10.1.1.253 255.255.255.0	ip address 10.1.1.253 255.255.255.0	内网接口
undo shutdown	no shutdown	激活接口

interface GigabitEthernet0/2	interface GigabitEthernet0/2	
ip address 10.1.2.1 255.255.255.252	ip address 10.1.2.1 255.255.255.252	R1 与 R2 互联地址
undo shutdown	no shutdown	激活接口
用户路由器 R2 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
ip address 6.7.22.2 255.255.255.252	ip address 6.7.22.2 255.255.255.252	与证联网互联接口
undo shutdown	no shutdown	激活接口
interface GigabitEthernet0/1	interface GigabitEthernet0/1	
ip address 10.2.1.252 255.255.255.0	ip address 10.2.1.252 255.255.255.0	内网接口
undo shutdown	no shutdown	激活接口
interface GigabitEthernet0/2	interface GigabitEthernet0/2	
ip address 10.1.2.2 255.255.255.252	ip address 10.1.2.2 255.255.255.252	R1 与 R2 互联地址
undo shutdown	no shutdown	激活接口

（3）BFD 配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
bfd min-receive-interval 500	bfd interval 500 min_rx 500 multiplier 3	BFD 检测参数配置（接受间隔）
bfd min-transmit-interval 500		BFD 检测参数配置（发送间隔）
bfd detect-multiplier 3		BFD 检测参数配置（检测次数）
用户路由器 R2 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
bfd min-receive-interval 500	bfd interval 500 min_rx 500 multiplier 3	BFD 检测参数配置（接受间隔）
bfd min-transmit-interval 500		BFD 检测参数配置（发送间隔）
bfd detect-multiplier 3		BFD 检测参数配置（检测次数）

（4）路由配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
ip route-static 41.0.0.0 255.0.0.0 GigabitEthernet0/0 6.7.6.1 bfd control-packet preference 1	ip route static bfd G0/0 6.7.6.1 ip route 41.0.0.0 255.0.0.0 G0/0 6.7.6.1	配置去往证联网路由
ip route-static 41.13.0.0 255.255.255.0 GigabitEthernet0/1 10.1.1.10 preference 1	ip route 41.13.0.0 255.255.255.0 G0/1 10.1.1.10	配置去往内部路由

用户路由器 R2 配置		
ip route-static 41.0.0.0 255.0.0.0 GigabitEthernet0/0 6.7.22.1 bfd control-packet preference 1	ip route static bfd G0/0 6.7.22.1 ip route 41.0.0.0 255.0.0.0 G0/0 6.7.22.1	配置去往证联网路由
ip route-static 41.13.0.0 255.255.255.0 GigabitEthernet0/1 10.2.1.10 preference 1	ip route 41.13.0.0 255.255.255.0 G0/1 10.2.1.10	配置去往内部路由
注：接入机构应根据各自内部网络实际情况配置路由协议，实现当主线路中断后能够切换至备线，保证业务正常运行。		

（5）禁用病毒端口参考

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
acl advanced name Denyport rule deny tcp destination-port range 135 139 rule deny tcp destination-port eq 445 rule deny udp destination-port eq 445 rule permit ip	ip access-list extended Denyport deny tcp any any range msrpc 139 deny tcp any any eq 445 deny udp any any eq 445 permit ip any any	访问控制策略
interface GigabitEthernet0/0 packet-filter name Denyport inbound packet-filter name Denyport outbound	interface GigabitEthernet0/0 ip access-group Denyport in ip access-group Denyport out	调用访问控制策略
用户路由器 R2 配置		
acl advanced name Denyport rule deny tcp destination-port range 135 139 rule deny tcp destination-port eq 445 rule deny udp destination-port eq 445 rule permit ip	ip access-list extended Denyport deny tcp any any range msrpc 139 deny tcp any any eq 445 deny udp any any eq 445 permit ip any any	访问控制策略
interface GigabitEthernet0/0 packet-filter name Denyport inbound packet-filter name Denyport outbound	interface GigabitEthernet0/0 ip access-group Denyport in ip access-group Denyport out	调用访问控制策略

（6）防火墙 NAT 配置

H3C 配置	Cisco 配置（v9.5）	配置说明
动态 NAT 配置（客户端使用）		
nat address-group 1 41.13.0.X 41.13.0.X	object network Inside-to-Outside-POOL range 41.13.0.x 41.13.0.x	配置动态 NAT 池
acl number 2xxx rule permit source 10.1.100.0	object network Inside-Network-NAT-Outside	动态 PAT 转换

0.0.0.255 rule deny	subnet 10.1.100.x 255.255.255.x nat (inside,outside) dynamic	
interface gigabitethernet x/x nat outbound 2xxx address-group 1	pat-pool Inside-to-Outside-POOL round-robin	
静态 NAT 配置（服务器使用）		
nat static 10.1.100.X 41.13.0.X interface gigabitethernet x/x nat outbound static	object network Inside-Server host 10.1.100.x nat (inside,outside) static 41.13.0.x	静态 NAT

（7）防火墙访问控制策略配置

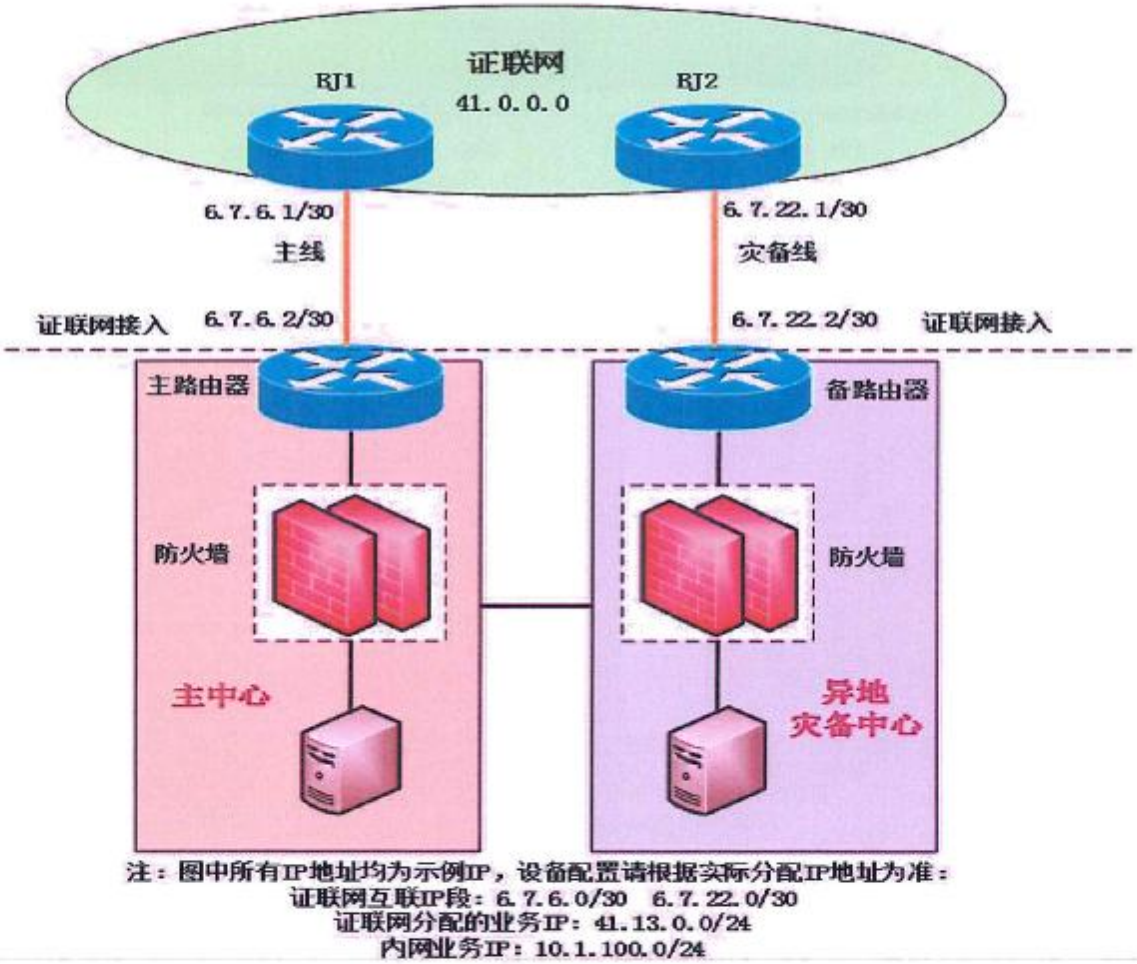
H3C 配置	Cisco 配置（v9.5）	配置说明
acl number 3xxx rule 0 permit icmp source 41.x.x.x 0 destination 10.1.100.x 0 rule 5 permit tcp source 41.x.x.x 0 destination 10.1.100.x 0 destination-port eq ftp rule 10 permit tcp source 41.x.x.x 0 destination 10.1.100.x 0 destination-port eq www rule 15 deny ip logging	access-list Outside_access_Inside extended permit icmp host 41.X.X.X host 10.1.100.X access-list Outside_access_Inside extended permit tcp host 41.X.X.X host 10.1.100.X eq ftp access-list Outside_access_Inside extended permit tcp host 41.X.X.X host 10.1.100.X eq www access-list Outside_access_Inside extended deny ip any any log notifications	按照权限最小化原则配置防火墙入方向访问控制策略
acl number 3yyy rule 0 permit icmp source 10.1.100.x 0 destination 41.x.x.x 0 rule 5 permit tcp source 10.1.100.x 0 destination 41.x.x.x 0 destination-port eq www rule 10 permit tcp source 10.1.100.x 0 destination 41.x.x.x 0 destination-port eq ftp rule 15 deny ip logging	access-list Inside_access_Outside extended permit icmp host 10.1.100.X host 41.X.X.X access-list Inside_access_Outside extended permit tcp host 10.1.100.X host 41.X.X.X eq ftp access-list Inside_access_Outside extended permit tcp host 10.1.100.X host 41.X.X.X eq www access-list Inside_access_Outside extended deny ip any any log notifications	按照权限最小化原则配置防火墙出方向访问控制策略
interzone source outside destination inside rule acl 3xxx rule acl enable	access-group Outside_access_Inside in interface Outside	调用入方向策略

interzone source inside destination outside rule acl 3yyy rule acl enable	access-group Inside_access_Outside in interface Inside	调用出方向策略

3. 接入模式三：主中心、异地灾备双中心接入

接入机构在某城市有主中心，在另一城市有异地灾备中心的，主中心、异地灾备中心之间应保证互通，分别申请一条线路，接入证联网同一对接入节点，两条线路互为备份，使用相同的业务 IP 地址段。

（1）接入示意图:

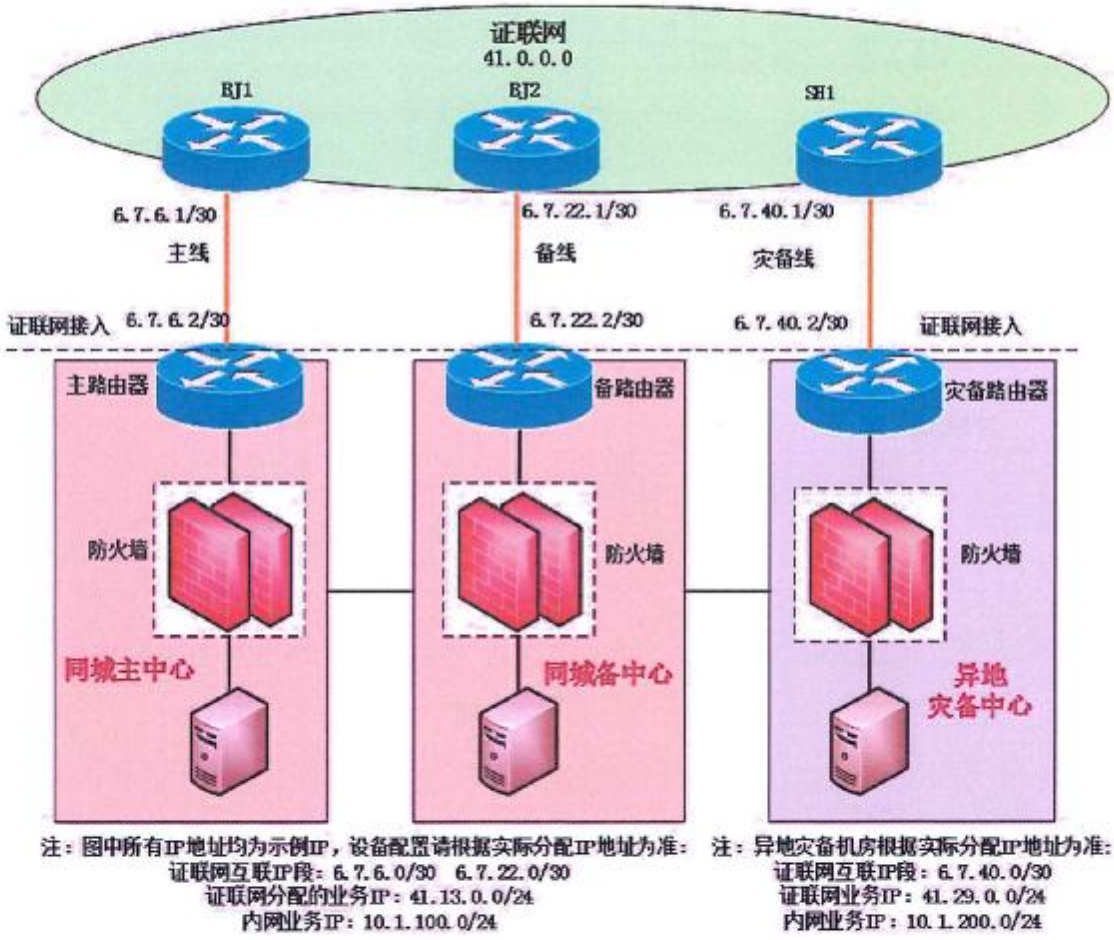


（2）具体配置参考接入模式二。

4. 接入模式四：两地三中心接入

接入机构在某城市有主、备中心，在另一城市有异地灾备中心的，主、备中心应分别申请一条线路，接入证联网同一对接入节点，两条线路互为备份，主、备中心使用一段业务 IP 地址；异地灾备中心再申请一条线路，接入证联网异地节点，异地灾备中心使用另一段业务 IP 地址。

（1）接入示意图：



（2）具体配置参考接入模式二。

附件 2：

测试网网络及安全配置指引

一、网络及安全配置要求

1. 网络要求

（1）接入机构根据机房所在位置就近接入证联网测试网，接入线路原则上应采用单线接入。

（2）证联网测试网支持运营商专线接入和交易所托管机房接入两种方式，机构根据自身情况自行选择。

（3）证联网运管中心负责为接入机构统一分配网络互联 IP 地址和业务 IP 地址，原则上业务 IP 地址只能用于接入机构服务器或终端设备，不能用于接入机构内部网络设备互联。接入机构应配置 NAT，隐藏内部主机的实际 IP 地址。服务器 IP 地址应在 42.x.x.1-42.x.x.223 和 42.x.x.240-42.x.x.254 内规划，终端设备 IP 地址应在 42.x.x.224-42.x.x.239 内规划。

（4）接入机构应在与测试网直连的接入设备上配置 BFD（双向转发检测）功能，监测网络的连通性。

（5）接入机构应将测试网接入线路纳入本单位的监控系统，实时监控接入线路状态，并定期评估带宽使用率，以满足业务需求。

2. 安全要求

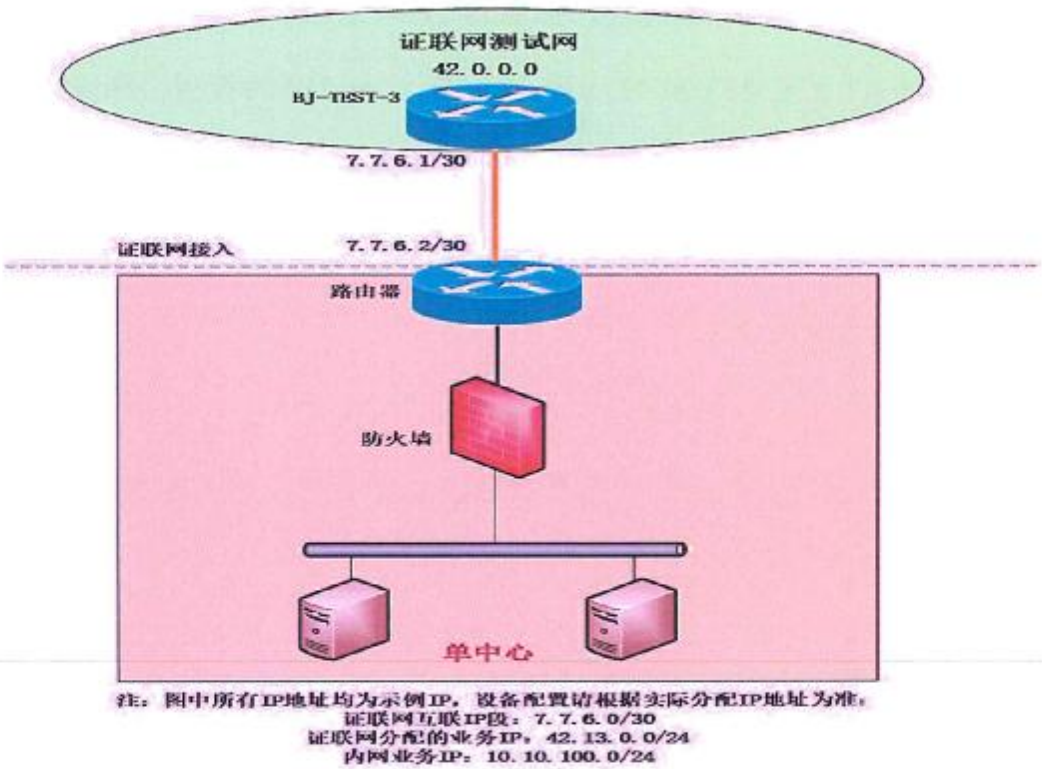
（1）接入机构应在网络边界上部署防火墙、安全网关等设备，将自身网络分成逻辑安全区域，对每个区域进行安全防护，保障证联网测试网网络和业务系统安全。

（2）接入机构应按照权限最小化原则进行双向访问控制，出方向按照实际访问需求，配置访问控制策略，访问控制规则必须包括源IP、目的IP、目的端口、协议；入方向应按照对外提供的服务需求，配置访问控制策略，访问控制规则必须包括源IP、目的IP、目的端口、协议。

（3）接入测试网的服务器和终端必须参照《证券期货业信息系统运维管理规范》、《证券期货业信息系统安全等级保护基本要求》、《证券期货业信息系统审计指南》的要求，做好安全管理。此外，接入机构还应该采取必要的技术措施，对接入证联网的终端进行主机监控、移动介质管理、非授权外连管理等。

二、接入模式及配置参考

1. 接入示意图：



注：图中所有IP地址均为示例IP，设备配置请根据实际分配IP地址为准。
证联网互联IP段：7.7.6.0/30
证联网分配的业务IP：42.13.0.0/24
内网业务IP：10.10.100.0/24

2. 路由器接口配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
ip address 7.7.6.2 255.255.255.252	ip address 7.7.6.2 255.255.255.252	与证联网互联接口
undo shutdown	no shutdown	激活接口
interface GigabitEthernet0/1	interface GigabitEthernet0/1	
ip address 10.10.1.254 255.255.255.0	ip address 10.10.1.254 255.255.255.0	内网接口
undo shutdown	no shutdown	激活接口

3. BFD 配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
interface GigabitEthernet0/0	interface GigabitEthernet0/0	
bfd min-receive-interval 500	bfd interval 500 min_rx 500 multiplier 3	BFD 检测参数配置（接受间隔）
bfd min-transmit-interval 500		BFD 检测参数配置（发送间隔）
bfd detect-multiplier 3		BFD 检测参数配置（检测次数）

4. 路由配置

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
ip route-static 42.0.0.0 255.0.0.0 GigabitEthernet0/0 7.7.6.1 bfd control-packet preference 1	ip route static bfd G0/0 7.7.6.1 ip route 42.0.0.0 255.0.0.0 G0/0 7.7.6.1	配置去往证联网路由
ip route-static 42.13.0.0 255.255.255.0 GigabitEthernet0/1 10.10.1.10	ip route 42.13.0.0 255.255.255.0 G0/1 10.10.1.10	配置去往内部路由

5. 禁用病毒端口参考

H3C 配置（v7 版本）	Cisco 配置	配置说明
用户路由器 R1 配置		
acl advanced name Denyport rule deny tcp destination-port range 135 139 rule deny tcp destination-port eq 445 rule deny udp destination-port eq 445 rule permit ip	ip access-list extended Denyport deny tcp any any range msrpc 139 deny tcp any any eq 445 deny udp any any eq 445 permit ip any any	访问控制策略
interface GigabitEthernet0/0	interface GigabitEthernet0/0	调用访问控制策

packet-filter name Denyport inbound packet-filter name Denyport outbound	ip access-group Denyport in ip access-group Denyport out	略

6. 防火墙 NAT 配置

H3C 配置	Cisco 配置（v9.5）	配置说明
动态 NAT 配置（客户端使用）		
nat address-group 1 42.13.0.X 41.13.0.X	object network Inside-to-Outside-POOL range 42.13.0.x 41.13.0.x	配置动态 NAT 池
acl number 2xxx rule permit source 10.10.100.0 0.0.0.255 rule deny interface gigabitethernet x/x nat outbound 2xxx address-group 1	object network Inside-Network-NAT-Outside subnet 10.10.100.x 255.255.255.x nat (inside,outside) dynamic pat-pool Inside-to-Outside-POOL round-robin	动态 PAT 转换
静态 NAT 配置（服务器使用）		
nat static 10.10.100.X 42.13.0.X interface gigabitethernet x/x nat outbound static	object network Inside-Server host 10.10.100.x nat (inside,outside) static 42.13.0.x	静态 NAT

7. 防火墙访问控制策略配置

H3C 配置	Cisco 配置（v9.5）	配置说明
acl number 3xxx rule 0 permit icmp source 42.x.x.x 0 destination 10.10.100.x 0 rule 5 permit tcp source 42.x.x.x 0 destination 10.10.100.x 0 destination-port eq ftp rule 10 permit tcp source 42.x.x.x 0 destination 10.10.100.x 0 destination-port eq www rule 15 deny ip logging	access-list Outside_access_Inside extended permit icmp host 42.X.X.X host 10.10.100.X access-list Outside_access_Inside extended permit tcp host 42.X.X.X host 10.10.100.X eq ftp access-list Outside_access_Inside extended permit tcp host 42.X.X.X host 10.10.100.X eq www access-list Outside_access_Inside extended deny ip any any log notifications	按照权限最小化原则配置防火墙入方向访问控制策略
acl number 3yyy rule 0 permit icmp source 10.10.100.x 0 destination 42.x.x.x 0 rule 5 permit tcp source 10.10.100.x 0 destination 42.x.x.x 0 destination-port eq www rule 10 permit tcp source 10.10.100.x	access-list Inside_access_Outside extended permit icmp host 10.10.100.X host 42.X.X.X access-list Inside_access_Outside extended permit tcp host 10.10.100.X host 42.X.X.X eq ftp access-list Inside_access_Outside	按照权限最小化原则配置防火墙出方向访问控制策略

0 destination 42.x.x.x 0 destination-port eq ftp rule 15 deny ip logging	extended permit tcp host 10.10.100.X host 42.X.X.X eq www access-list Inside_access_Outside extended deny ip any any log notifications	
interzone source outside destination inside rule acl 3xxx rule acl enable	access-group Outside_access_Inside in interface Outside	调用入方向策略
interzone source inside destination outside rule acl 3yyy rule acl enable	access-group Inside_access_Outside in interface Inside	调用出方向策略