ICS 35.040
CCS L 80

团　体　标　准

T/CESA 1165—2021

零信任系统技术规范

Technical specification for zero trust system

2021-06-30 发布　　2021-07-01 实施

中国电子工业标准化技术协会　发布

目　　次

前 言

本文件按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由深圳市腾讯计算机系统有限公司提出。

本文件由中国电子工业标准化技术协会归口。

本文件起草单位：深圳市腾讯计算机系统有限公司、完美世界控股集团有限公司、北京天融信网络安全技术有限公司、公安部第三研究所、绿盟科技集团股份有限公司、北京蔷薇灵动科技有限公司、中国移动通信集团设计院有限公司、任子行网络技术股份有限公司、上海观安信息技术股份有限公司、中孚信息股份有限公司、深圳市网安计算机安全检测技术有限公司、国家计算机网络应急技术处理协调中心、北京芯盾时代科技有限公司、深圳市联软科技股份有限公司、腾讯云计算(北京)有限责任公司、腾讯科技(深圳)有限公司。

本文件主要起草人：蔡东赟、何艺、李春鹏、龙凡、刘治平、陈妍、谢江、王龑、刘弘利、杜雪涛、张晨、赵蓓、齐聪、杨文宏、王文磊、孟昭宇、陈曦、程建明、黄超、刘海涛、王旭、宋爱元、谢仪頔。

零信任系统技术规范

1 范围

本文件规定了用户访问资源、服务之间调用两种场景下零信任系统在逻辑架构、认证、访问授权管理、传输安全、安全审计、自身安全等方面的功能、性能技术要求和相应的测试方法。

本文件适用于零信任系统的设计、技术开发和测试。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

访问主体 access subject

访问客体的主动实体。

注：访问主体例如用户、终端设备、物联网设备等

[来源：GB/T 29242—2012，3.7，有修改]

3.2

访问客体 access object

被访问的目标资源。

注：访问客体例如服务器、数据库、打印服务、网络等。

3.3

零信任技术 zero trust technology

旨在降低访问过程安全风险的持续动态安全访问控制技术。

注：零信任技术基于安全和信任状态对访问主体进行安全授权，并持续性的监测整个访问过程的安全。

3.4

零信任系统 zero trust system

基于零信任技术的相关产品和服务，或者是产品和服务的组合。

4 缩略语

下列缩略语适用于本文件。

API 应用程序接口（Application Programming Interface）

OIDC 开放 ID 连接（OpenID Connect）

RADIUS 远程用户拨号认证系统（Remote Authentication Dial In User Service）

RDP 远程桌面协议（Remote Desktop Protocol）

SAML 安全断言标记语言（Security Assertion Markup Language)

SDK 软件开发工具包（Software Development Kit）

SSH 安全外壳协议（Secure Shell）

TCP 传输控制协议（Transmission Control Protocol）

UDP 用户数据报协议（User Datagram Protocol）

URI 统一资源标识符（Uniform Resource Identifier）

5 零信任概述

5.1 理念

零信任是一种网络安全防护理念，并非指某种单一的安全技术或产品，其目标是为了降低资源访问过程中的安全风险，防止在未经授权情况下的资源访问，其关键是打破信任和网络位置的默认绑定关系。

在零信任理念下，网络位置不再决定访问权限，在访问被允许之前，所有访问主体都需要经过身份认证和授权。身份认证不再仅仅针对用户，还将对终端设备、应用软件等多种身份进行多维度、关联性的识别和认证，并且在访问过程中可以根据需要多次发起身份认证。授权决策不再仅仅基于网络位置、用户角色或属性等传统静态访问控制模型，而是通过持续的安全监测和信任评估，进行动态、细粒度的授权。安全监测和信任评估结论是基于尽可能多的数据源计算出来的。

5.2 基本假设

零信任理念的基本假设：

a) 内部威胁不可避免；

b) 从空间上，资源访问的过程中涉及到的所有对象（用户、终端设备、应用、网络、资源等）默认都不信任，其安全不再由网络位置决定；

c) 从时间上，每个对象的安全性是动态变化的（非全时段不变的）。

5.3 基本原则

零信任理念的基本原则如下：

a) 任何访问主体（人/设备/应用等），在访问被允许之前，都要经过身份认证和授权，避免过度的信任；

b) 访问主体对资源的访问权限是动态的（非静止不变的）；

c) 分配访问权限时遵循最小权限原则；

d) 宜减少资源非必要的网络暴露，以减少攻击面；

e) 宜确保所有的访问主体、资源、通信链路处于最安全状态；

f) 宜多的和及时的获取可能影响授权的所有信息，并根据这些信息进行持续的信任评估和安全响应。

5.4 应用场景

零信任在所有需要对资源访问进行安全防护的场景都可以使用，主要场景分为两类，一类是站在发起方，用户访问资源的场景，指的是用户访问内部资源时，如何验证用户是可信的，如何确保访问来源终端可信，如何确认拥有访问资源权限。另外一类是站在服务方，即服务资源之间如何安全的互相访问。但是否采用，应根据企业可接受的安全风险水平和投入综合考虑决定。

6 用户访问资源场景技术要求

6.1 逻辑架构

6.1.1 概述

用户访问资源场景下，系统逻辑架构见图 1，主要包括四个逻辑组件：访问主体，零信任网关，零信任控制中心和访问客体。其中访问主体为资源访问发起方，零信任网关提供对来访请求的转发和拦截功能，零信任控制中心提供对来访请求的认证和持续访问控制功能，访问客体提供被访问的资源。另外系统还可以通过联动接口和身份认证、安全分析和入侵检测方面的其他系统进行对接。其他系统不在本规范中定义，具体信息详见附录 A。

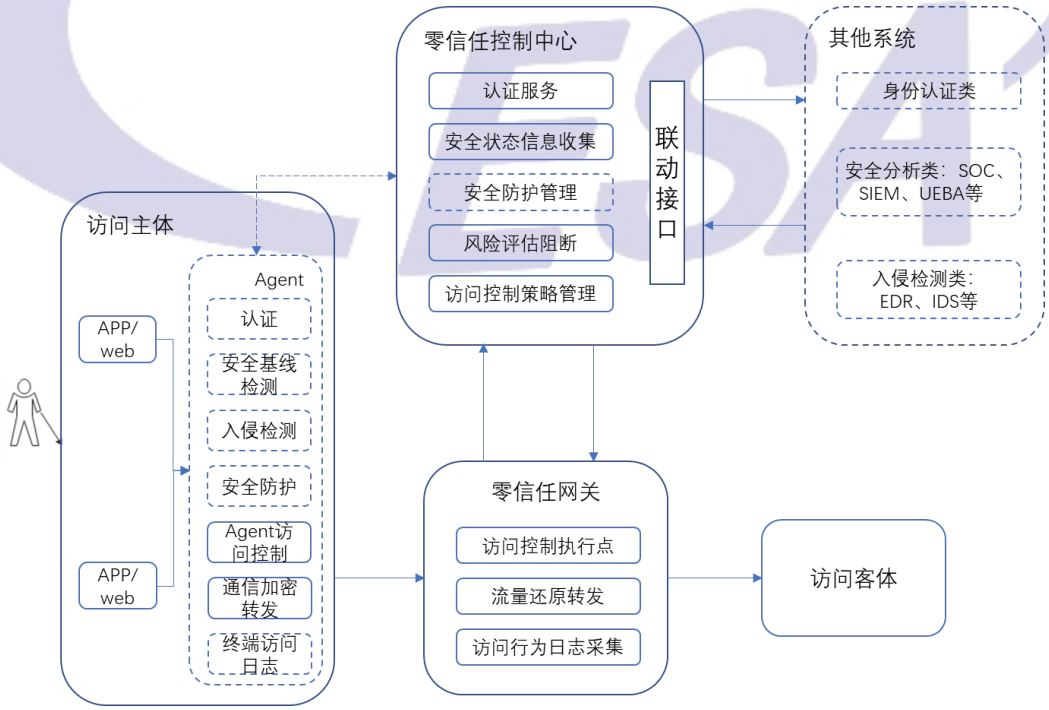

图 1 逻辑架构图（用户访问资源场景）

6.1.2 访问主体

访问主体发起资源访问，可提供终端认证、访问授权、流量加密、安全检测、安全防护等功能。

6.1.3 零信任网关

零信任网关是暴露在外部可被用户直接访问的系统，功能包括：

a）转发：对来访未经授权的请求进行认证授权转发，对已正确授权的请求进行资源访问转发；

b）拦截：对禁止访问的请求进行拦截阻断，阻止向后访问。网关包括全流量网关、web 网关、支持 SSH\RDP 协议的网关。流量网关应符合附录 B 规定。

6.1.4 零信任控制中心

零信任控制中心作为控制端的角色，功能包括：对用户、终端身份进行认证和授权以及持续访问控制，持续访问控制含：

a）访问控制策略：访问控制策略包含访问过程的关键对象、访问权限、环境安全状态因素，可以进行灵活的配置，方便在访问建立、访问中可以根据访问策略做风险判断，进行授权访问或者实时阻断；

b）动态安全检测：决策中心对鉴权和安全状态的检验应该是持续动态的过程，即每次对资源对访问应该都重新进行鉴权和检验；同时需要获取访问过程中关键对象、关键环境的安全状态，判定访问过程是否有风险；

c）动态防护响应：如果判定有风险的相关访问，应该可以及时采取降权、阻断等防护策略。

6.1.5 访问客体

访问客体提供被访问的资源，如服务器、数据库、打印服务、网络等。

6.2 功能要求

6.2.1 认证功能

6.2.1.1 本地账户管理

本地账户管理功能应符合以下要求：

a） 提供本地账户的创建、批量导入、批量导出（加密导出/明文导出）、修改、删除；

b） 提供分组管理（按组织架构）能力；

c） 提供角色管理（按业务职能）能力；

d） 提供针对分组管理和角色管理的授权能力。

6.2.1.2 其他系统账户管理对接

其他系统账户管理对接功能要求如下：

a） 应支持与其他系统认证体系（Radius、LDAP、AD 域等）对接；

b） 应支持同步其他系统认证体系对应的账户、组织架构信息等；

c） 终端认证可由其他认证系统完成。

6.2.1.3 多因素认证

多因素认证功能应支持数字证书、动态令牌、短信、扫码、token、人脸识别等的一种或几种。

6.2.1.4 单点登录授权

单点登录授权功能应支持 SAML2.0 或 Oauth2 协议。

6.2.2 安全基线检测能力要求

安全基线检测能力应支持如下终端安全信息收集：

a） 杀毒防护组件检查；

b） 弱密码检查；

c） 高危漏洞检查；

d） 违规进程、应用软件检查；

e） 违规服务检查；

f） 操作系统版本检查。

6.2.3 访问授权功能管理

6.2.3.1 服务资源管理

服务资源管理功能要求如下：

a） 应支持目标资源录入、修改和归类；

b） 应支持录入格式域名或者 ip 端口；

c） 应支持七层网络协议配置；

d） 可支持 tcp、udp 四层协议目的资源配置。

6.2.3.2 访问授权管理

访问授权管理功能应支持配置指定身份\身份组，访问指定的目的资源。

6.2.3.3 安全属性授权访问

安全属性授权访问功能要求应支持根据配置安全基线状态情况、以及其他存在安全风险的特征属性变化，对关联访问连接进行阻断。

6.2.3.4 终端应用可信管理

终端应用可信管理功能要求如下：

a） 可提供可信进程的基础库做访问控制；

b） 可收集终端发起网络访问的进程的特征，提供进程、签名、操作系统、厂商、其他病毒查询结果报表，并提供给管理员操作转入可信应用；

c） 可自动收集应用信息，并通过其他系统病毒特征查询自动检查放行；

d）在自动检查判定可信应用的功能基础上，需要支持黑名单机制完善管理场景。

6.2.3.5 可信硬件授权访问

可信硬件授权访问应符合如下功能要求：

a）支持适配公司的资产库，只有公司允许的硬件字长才可以进行内部资源的访问；

b）这次只有满足某种安全的可信硬件设备标准检查结果的设备，才可以进行公司内部的访问。

6.2.3.6 可信操作系统管理访问授权

可信操作系统管理访问授权功能应符合可信操作系统管理安全标准，对方公司信任的操作系统才可以访问，可以针对性做配置。

6.2.3.7 终端应用沙箱授权访问

终端应用沙箱授权访问功能应支持基于终端应用沙箱或应用容器，授权可信的沙箱或容器应用访问后端资源。

6.2.4 网关管理

6.2.4.1 网关管理信息管理

网关管理信息管理功能应支持管理网关地址，增删改查，提供给终端访问。

6.2.4.2 业务访问网关路由编排

业务访问网关路由编排功能可支持不同的业务流量，配置使用不同的网关加密传输通道。

6.2.5 通信传输安全

6.2.5.1 控制通道传输加密

控制通信传输加密功能应支持客户端 agent 与控制中心通信应采用双向加密，相互验证，防止伪造的服务器或者终端，如双向加密传输等。

6.2.5.2 数据通道传输加密

数据通道传输加密功能应支持客户端代理可以把任意流量加密，再转发到网关再鉴权解密到目的系统，防止终端到网关的网络存在中间人劫持，如 https 等。

6.2.6 安全审计日志

对安全审计日志应符合如下功能要求：

a）对于访问行为日志，支持如下访问连接行为信息的采集：用户身份、设备身份、终端应用进程、IP、目的 IP、源端口、目的端口、协议、域名、uri、时间、状态；

b）对于终端认证日志，支持如下信息收集：认证时间、认证身份、来源设备信息、网络信息、认证结果；

c）对于审计日志，支持收集后台管理系统管理员操作行为。

6.2.7 联动接口对接要求

联动接口对接应符合如下功能要求：

a）支持通过常见认证协议，如 LDAP，OAuth2.0、RADIUS、OIDC、SAML 等对接其他认证系统；

b）支持提供给其他安全系统调用的接口，当出现安全风险的时候，支持阻断身份、应用、终端设备标示对应的所有访问连接；

c）支持安全状态信息收集接口，接收其他系统安全状态信息，用来角色判断用户访问策略，提供安全状态信息接收接口。接口要求描述关键访问过程的对象，如身份、设备、网络连接、资源的等对象的安全状态，必须为确切状态方便多系统间协作；

d）支持访问行为日志对外输出，可以提供给其他安全分析系统针对本系统获取到的日志，如认证、访问日志等。

6.2.8 设备安全增强功能

6.2.8.1 终端设备安全防护

终端设备安全防护可符合如下功能要求：

a）支持设备操作系统基础病毒防护；

b）支持终端系统漏洞修复；

c）支持终端系统硬件设备管控。

6.2.8.2 入侵检测

入侵检测可符合如下功能要求：

a）支持动态检测终端设备的入侵行为，并输出告警，并能够联动阻断访问；

b）支持对外可以提供行为日志溯源搜索检测能力。

6.2.9 运维监控

运维监控应符合如下功能要求：

a）组件集中化监控看板，知道组件特别是网关的运行状态，cpu、内存、磁盘利用率、服务可用性等；

b）告警信息看板，展示产生运维过程监控告警。

6.3 系统自身安全要求

6.3.1 身份、凭据防盗

身份、凭据防盗功能应支持身份凭据、授权访问凭据防盗用功能，避免通过客户端存储、简单逆向、接口交互等突途径盗取身份或者访问凭据。

6.3.2 权限分离

权限分离功能应支持管理员、审计员、策略员控制台访问操作权限分离。

6.3.3 安全审计

安全审计功能应支持管理员行为审计，对任意管理员控制台涉及到删除修改的业务的动作，都要能够记录和追溯。

6.3.4 系统加固

系统加固功能要求如下：

a）应支持系统所在服务器自身加固功能，包括：管理员操作日志审计、控制台管理端 web 平台防护、所在服务器基础防御加固，系统防火墙、SSHD\RDP 等服务加固、具备 DDoS 防护能力；

b）应支持终端安全文件目录自保护、自身进程异常中断保护；

c）可支持系统安全加固：系统密码复杂度加固、屏幕保护设置、共享、高危服务关闭、终端高危端口屏蔽、终端系统审计日志开启。

6.4 性能要求

网关单台并发情况下，网关配置如下：cpu：8core 内存：16G 磁盘网卡流量：500G。测试指标满足以下要求：每秒静态页面鉴权访问并发数量：2000 请求数/秒～8000 请求数/秒。

6.5 部署要求

6.5.1 访问主体部署方式

访问主体部署功能要求应选择如下中的一种方式：

a）支持有 agent 支持的部署，设备操作系统类型：windows、macosx、linux、android、ios；

b）支持无 agent 部署模式，支持各类标准浏览器访问。

6.5.2 控制中心部署

控制中心部署应符合如下要求：

a）支持单机、集群、多级部署模式。集群模式具备扩展性，实现服务的弹性伸缩，集群内避免异构部署模式；多级模式下，控制中心独立部署、互相隔离，仅通过服务总线实现跨控制中心服务调用；

b）支持高并发机制，确保单节点并发处理能力满足并发处理要求，对高频访问数据采用高速分布式缓存，确保服务达到响应时间要求；

c）支持数据库的分布式部署，建设分布式数据库集群，隶属于控制中心的数据库仅支持本控制中心垂直访问；

d）支持可运维性，统计和展示服务调用量、异常量、最高并发量等运行情况，支持系统的安装、配置、部署、升级操作；

e）支持授权、保护等策略管理，包括制定、修改、删除、审核与发布等。

6.5.3 零信任网关部署

零信任网关部署功能要求如下：

a）应支持集群部署，集群架构具备扩展性，实现服务的弹性伸缩，集群内避免异构部署模式；

b）应支持加速和动态分发，采用负载均衡技术，实现接入的均衡分布。

6.6 容灾要求

6.6.1 容灾架构

容灾架构示意图见图 2。

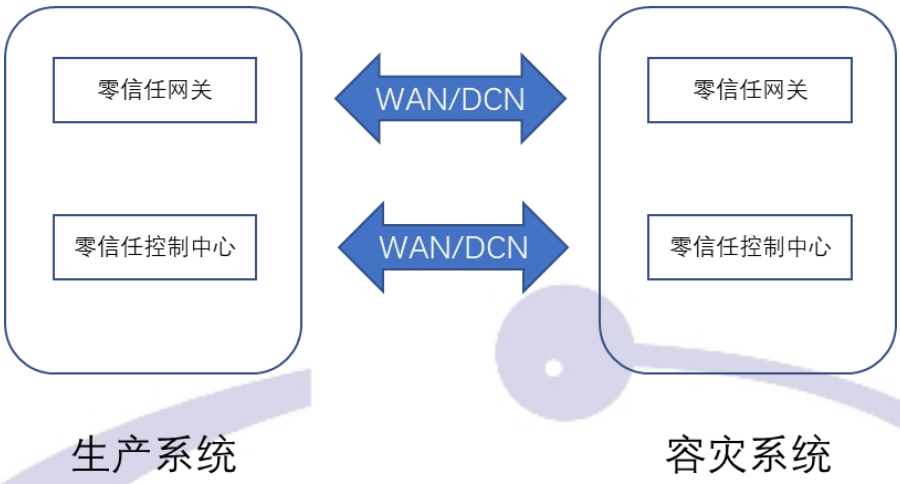

图 2 容灾示意图

注： WAN：外网，公网，DCN：数据通信网络。

6.6.2 控制中心容灾

控制中心容灾示意图见图 2，应符合以下要求：

a）支持基础设施高可靠，支持备份、容错、冗余机制；

b）支持数据冷热分离部署；

c）支持数据存储高可靠，数据存储能够进行增量、全量的备份和恢复操作，支持分布式存储和存储容量冗余设计；

d）支持内存数据库数据持久化，便于故障恢复；

e）支持系统软件高可靠，增强系统稳定性；

f）支持 7×24 h 无故障运行能力，包括系统可靠性和数据可靠性；

g）支持故障管理，包括告警、上报等。

6.6.3 网关容灾

网关容灾应符合以下要求：

a）保证网关服务可用性；

b）支持 7×24 h 无故障运行能力，包括网关可靠性和数据可靠性；

c）支持故障管理，包括告警、上报等。

7 服务之间访问场景技术要求

7.1 逻辑架构

7.1.1 概述

服务之间访问场景下，系统逻辑架构图见图 3，主要包含两个逻辑组件：策略控制点和策略执行点。策略控制点负责鉴权和授权判断，并提供业务流的可视化能力；策略执行点用于执行访问控制决策，允许/拒绝通信或进行协商加密；有时也会将工作负载的相关信息同步给安全控制中心，从而辅助其进行决策。策略执行点有两种形态：一是部署在工作负载上的服务端代理，另一种是运行在网络上的网关。

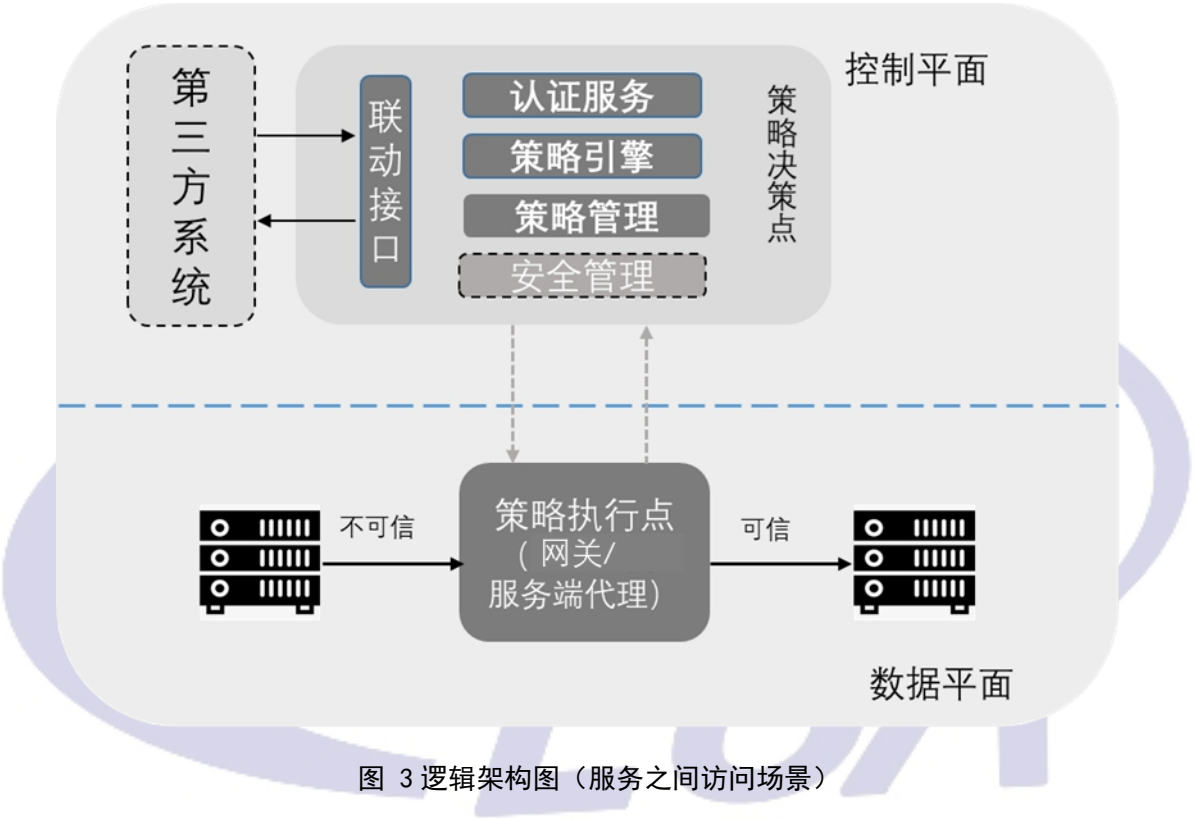

图 3 逻辑架构图（服务之间访问场景）

7.1.2 策略执行点——服务端代理

服务端代理对工作负载进行认证，接受并执行控制中心下发的策略，对工作负载进行访问授权，记录工作负载访问日志并加密上传至策略决策点，根据需要扩充安全检测、安全防护能力。

7.1.3 策略执行点——网关

网关组件通过底层平台对接等方式对工作负载进行认证，在网络层接受并执行控制中心下发的策略，对工作负载进行访问授权，记录工作负载访问日志并加密上传至控制中心，根据需要扩充安全检测、安全防护能力。

7.1.4 策略决策点

策略决策点作为控制端的角色，提供认证、访问授权、策略统一管理、策略动态调整、安全管理能力和其他系统联动管理等。

7.2 功能要求

7.2.1 认证功能

认证功能要求如下：

a）应支持自身具备或可从外部获取工作负载基本信息的功能，基本信息包括操作系统版本、网卡信息、服务信息、监听端口信息等；

b）应能够为每一台工作负载确定唯一标识的身份信息；

c）应支持当主机信息发生变化时，可上传至管理端；

d）应支持认证组件在策略决策点中负责主体的身份认证。认证组件可以自行完成，或提供与其他系统认证对接的接口。实现对工作负载的认证。

7.2.2 服务之间访问控制功能

服务端代理/网关组件要具备访问控制能力，具体要求如下：

a）应支持使用最小安全原则，即除非明确允许，否则就禁止；

b）应能实现基于源 IP 地址、目的 IP 地址和端口的访问控制；

c）应支持实现出站和入站的双向访问控制；

d）应支持接收并执行策略决策点下发的动态访问控制策略；

e）应支持记录违反策略规则的阻断日志，并上传至策略决策点；

f）可支持组件对 ipv6 网络流量进行访问控制；

g）可支持组件进行容器之间的访问控制；

h）可支持通过建立服务之间的加密隧道来实现访问控制。

7.2.3 服务之间流量识别

服务之间流量识别功能要求如下：

a）应能识别出站及入站的流量，包括流量的来源 IP，目的 IP，端口及服务信息等；

b）应支持策略决策点将学习到的流量信息统一进行呈现及搜索；

c）应支持以报表形式输出流量统计分析结果；

d）应支持记录异常访问日志，并支持输出到其他系统平台；

e）应支持通过策略执行点上传的流量，展示实时工作负载间流量关系拓扑，并标识流量与安全策略的匹配情况，包括匹配策略的流量和不匹配策略的流量；

f）应支持对策略执行点上传的阻断日志进行统一的查看，并支持基于时间、来源、目的、端口等维度的分析；

g）可支持识别 IPv6 的出站及入站的流量；

h）可支持能够识别容器之间的流量。

7.2.4 策略管理功能

策略管理功能要求如下：

a）应支持通过策略决策点的集中管理界面对分布式部署的策略执行点统一策略下发；

b）应支持配置任意两个工作负载之间的安全策略；

c）应支持接收策略控制点组件上传的工作负载策略状态变化信息；

d）可支持支持基于识别到的流量自动或半自动的方式生成安全策略；

e）可支持支持基于业务角色、主机属性等进行安全策略配置；

f）可支持应具备防护及非防护状态，尽可能减少策略配置对业务的影响。

7.2.5 动态授权功能

动态授权功能要求如下：

a）可支持在工作负载发生变化时，如虚拟机下线、IP 地址变化或虚拟机迁移时，动态调整访问控制策略；

b）可支持在工作负载认证信息发送变化时，动态调整访问控制策略。

7.2.6 接口对接功能

接口对接功能要求如下：

a）提供给其他安全系统调用的接口，出现安全风险的时候，支持阻断身份、应用、终端设备标示对应的所有访问连接。

b）提供给其他安全分析系统针对本系统获取到的日志，如认证、访问日志等。

7.2.7 安全防护管理

安全防护管理功能要求如下:

a）可支持工作负载操作系统基础病毒防护；

b）可支持工作负载漏洞修复；

c）可支持能够动态检测工作负载的入侵行为，并输出告警。

7.3 系统自身安全要求

7.3.1 标识与鉴别

标识与鉴别功能要求如下：

a）应维护每个用户的安全属性，属性可包括：用户标识、授权信息或用户组信息、其他安全属性等；

b）应保证任何用户都具有全局唯一的标识；

c）应要求每个用户在执行与系统安全相关的任何其他操作之前，都已被成功鉴别；

d）应支持服务端代理/网关组件能够对自身的运行状态进行感知，并上传至策略决策点。

7.3.2 鉴权失败处理

鉴权失败处理功能要求如下：

a）应能检测用户的不成功的鉴别尝试；

b）在达到或超过最大鉴别失败尝试次数阈值后，应采取措施阻止进一步的鉴别尝试，直至满足已定义的条件才允许进行重新鉴别；

c）应仅由授权管理员设置未成功鉴别尝试次数阈值。

7.3.3 通信传输保护

通信传输功能要求如下：

a）服务端代理/网关组件与策略决策点的通信应进行加密传输；

b）如支持用户通过 web 页面管理系统，应保证管理过程的数据采用加密方式传输；

c）如支持用户使用 API 接口对系统进行控制，应保证 API 需通过权限验证后才可使用。

7.3.4 安全审计

安全审计功能要求如下：

a）如果支持以下事件，应能为其产生审计记录：

1） 审计功能的启动和关闭；

2） 导出、另存和删除审计日志；

3） 设置鉴别尝试次数；

4） 鉴别机制的使用；

5） 用户的创建、修改、删除与授权；

6） 其他系统参数配置和管理安全功能行为的操作。

b）应在每个审计记录中至少记录下列信息：

1） 事件发生的日期和时间；

2） 事件类型；

3） 事件主体身份标识；

4） 事件描述及结果。

7.3.5 系统加固

系统加固功能要求如下：

a）策略决策点所在主机应开启系统防火墙并限定端口开放；

b）策略决策点所在主机应完成漏洞修复，策略决策点自身应无高危漏洞。

7.4 性能要求

服务端代理/网关组件应具备降级机制，对于 CPU、内存、硬盘中的一个或多个的占用设置限度。

7.5 部署要求

部署功能要求如下：

a）策略决策点应支持集群化部署，具备高可用性；

b）服务端代理/网关应能支持自动化部署。

8 用户访问资源场景测试

8.1 测试环境

测试环境典型示意图见图 4，其中：

a） 客户端操作系统：windows、macosx、linux（指定一个版本）、android、ios；

b） 服务器操作系统：linux(任意发行服务器版本)\windows server；

c） 目标业务系统：网页系统、SSHD\RDP 服务器；

d） 网络：千兆网络。

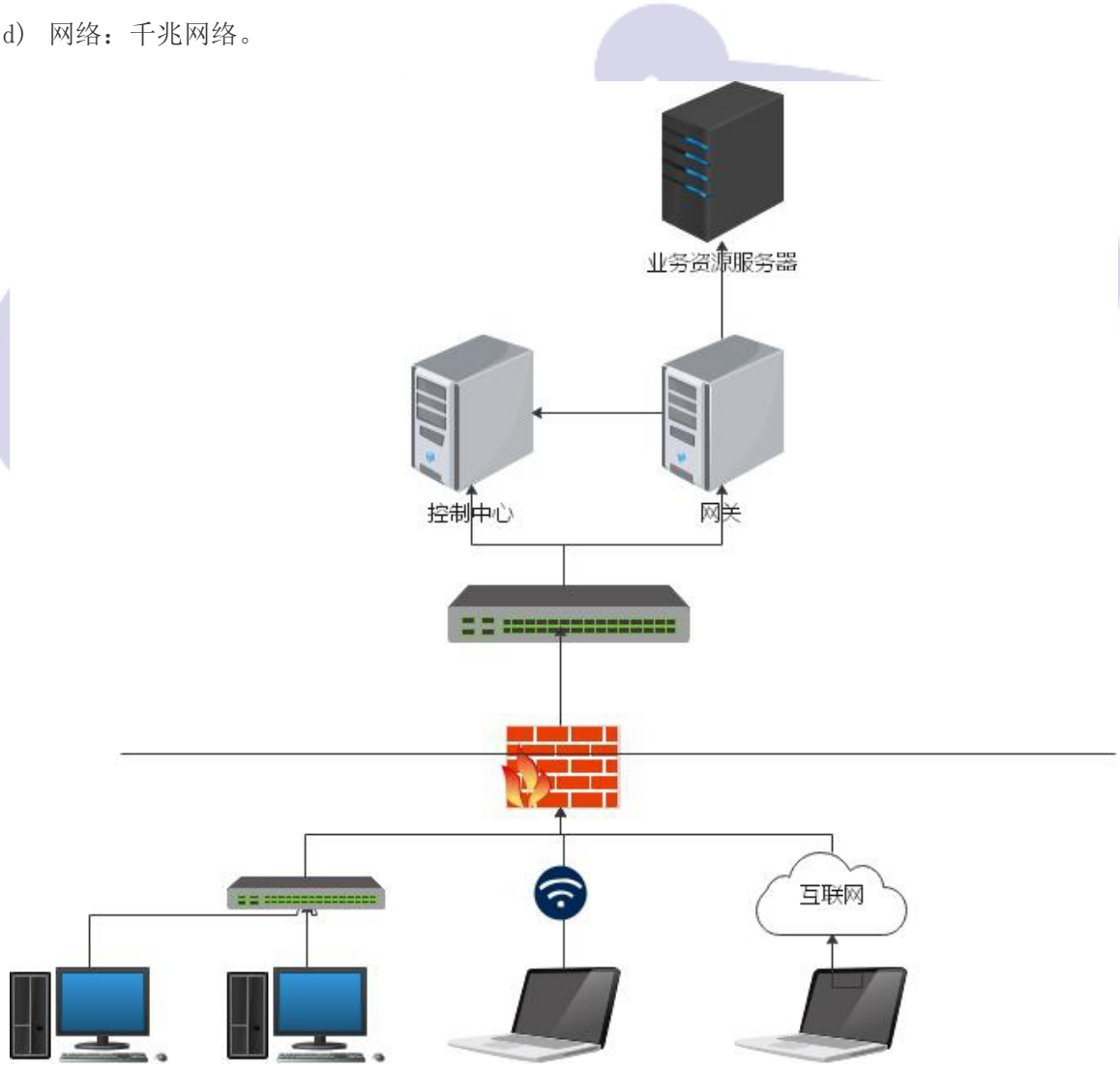

图 4 测试环境典型示意图

8.2 功能测试

8.2.1 认证功能测试

8.2.1.1 自建账户管理测试

8.2.1.1.1 测试方法

自建账户管理测试方法如下：

a） 控制中心管理端，新建账号、初始化密码，其次就是能够删除账户、重置密码；

b） 新建账户，有终端代理的场景，安装对应的客户端，启动终端登录新建的账号；

c） 新建账户，没有终端代理程序的场景，在客户端浏览器直接访问保护的目标域名，在跳转登录页面使用新建账号。

8.2.1.1.2 预期结果

自建账户管理测试预期结果如下：

a） 控制中心可以进行账号，新建、初始化密码、删除账户、重置密码；

b） 终端可以使用控制中心创建的账号密码，进行登录。

8.2.1.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.1.2 其他系统账户管理对接测试

8.2.1.2.1 测试方法

其他系统账户管理对接测试方法如下：

a） 在控制中心配置其他认证系统对接参数，后台可以导入对应的账户体系；

b） 终端认证账户密码等校验信息，可以转到其他认证系统完成认证；

c） 终端认证发起请求后，能够在其他认证系统看到认证记录。

8.2.1.2.2 预期结果

其他系统账户管理对接测试预期结果如下：

a） 在控制中心可以成功配置其他认证系统对接；

b） 控制中心可以同步其他认证系统的用户信息列表；

c） 终端发起认证后能够在其他认证系统认证并成功（口令认证通过/口令错误认证拒绝）。

8.2.1.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.1.3 多因素认证测试

8.2.1.3.1 测试方法

多因素认证测试方法如下：

a） 终端设备上面使用手机扫码认证；

b） 终端设备上面输入 token 账号和动态口令认证；

c） 后端可以对应录入或者对接对应的人脸和身份对应识别的库，终端设备上面必须有摄像头，开启扫脸认证，或者采用手机扫码并扫脸认证。

8.2.1.3.2 预期结果

符合校验信息的可以认证成功、非法用户认证失败。

8.2.1.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.1.4 单点登录授权测试

8.2.1.4.1 测试方法

单点登录授权测试方法如下：

a） 针对 BS 应用的：提供统一的认证授权系统的来源的页面，给到后台 bs 架构的系统认证集成，同时提供统一的登录态鉴权接口给其他业务系统查询身份凭据状态。提供对应的 demo 系统并测试；

b） cs 应用：终端认证 sdk 给到其他终端应用集成，控制中心提供统一的后台凭据校验查询的接口。提供继承好的 demo 系统并测试通过。

8.2.1.4.2 预期结果

能在系统登录认证之后，提供给终端设备统一的鉴权快速登录能力。

8.2.1.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.2 安全检测测试

8.2.2.1 测试方法

安全监测测试方法如下：

a） 配置检查策略：终端有没有安装杀毒防护的组件，组件是否运行。终端收到策略后执行检查，回传到控制中心结果；

b） 在控制中心配置密码检查策略，将测试终端所在的 PC 密码改为符合弱密码规则的密码，测试终端能否检测弱密码，并将结果回传至控制中心；

c） 在控制中心配置高危漏洞检查任务，测试终端能否在存在高危漏洞的系统功能中完成漏洞检

查，并将结果回传至控制中心；

d） 在控制中心可配置违规进程/软件检查策略，测试终端能否发现违规，并将结果回传至控制中心；

e） 在控制中心可配置违规服务检查策略，测试终端能否发现违规服务，并将结果回传至控制中心；

f） 测试终端能否正确检查操作系统版本，并将测试结果回传至控制中心，测试控制中心能否可以配置更新操作系统版本列表入口。

8.2.2.2 预期结果

安全监测测试预期结果如下：

a） 测试可以在控制中心看到检查结果；

b） 测试终端能够对弱密码进行检查，能够在控制中心配置检查策略，在控制中心可以看到检查结果；

c） 测试终端能够对高危漏洞进行检查，能够在控制中心配置检查策略，在控制中心可以看到检查结果；

d） 测试终端能够对违规进程/软件进行检查，能够在控制中心配置检查策略，在控制中心可以看到检查结果；

e） 测试终端能够对违规服务进行检查，能够在控制中心配置检查策略，在控制中心可以看到检查结果。

8.2.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.3 访问授权测试

8.2.3.1 服务资源管理测试

8.2.3.1.1 测试方法

服务资源管理测试方法如下：

a） 测试录入目标资源并对资源进行修改、归类；

b） 按照域名列表进行录入资源；

c） 按照 IP+端口列表进行录入资源；

d） 测试在控制中心配置网络七层协议并观察是否生效；

e） 测试在控制中心配置 TCP、UDP 四层协议网络控制列表。

8.2.3.1.2 预期结果

控制台能够编辑录入资源信息，并在访问控制策略侧可以对应。

8.2.3.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.3.2 访问授权管理测试

8.2.3.2.1 测试方法

访问授权管理测试方法如下：

a） 在控制中心配置基于用户身份和身份组策略，针对身份、访问资源的规则配置；

b） 能够配置可信应用列表，不在可信的范围内的应用、硬件资产、操作系统等不可以发起资源访问。

8.2.3.2.2 预期结果

访问授权管理预期结果如下：

a） 合法的身份并具备配置的策略的资源访问权限的，从终端可以发起访问并成功；不合法的身份无法访问任何配置资源；

b） 在合法身份访问权限的设备上面，如果同时存在不可信的应用、不可信的硬件资产、不可信操作系统不可以发起资源访问，只有具备所有配置要求项安全可信才可以访问资源。

8.2.3.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.3.3 终端应用可信管理测试

8.2.3.3.1 测试方法

终端应用可信管理测试方法如下：

a） 在控制中心查看可信进程基础库列表，点击添加、修改可信进程表；

b） 支持管理员确认应用可信的编辑操作，通过终端收集到的应用特征，管理员在管理员操作指定应用特征进入可信应用列表；

c） 在控制台开启自动收集应用，并通过其他系统自动检查判定是否可信放行，开启后自动收集终端应用签名、hash、厂商等信息，送检到其他系统病毒库检查；

d） 支持在自动放行其他系统检测可信的基础上面，支持添加黑名单机制，能够添加应用名、签名、hash、版本、发布厂商等信息对应到的应用，进行阻断访问。

8.2.3.3.2 预期结果

终端应用可信管理测试预期结果如下：

a） 在控制中心可查看可信进程基础库，管理员能够成功添加、修改可信进程库；

b） 在终端发起网络访问，可成功在控制中心查看到进程详情（包括但不限于进程、签名名、操作系统、厂商、其他系统病毒查询结果报表等），且管理员可成功将进程信息编辑添加至可信进程库；

c） 策略可以选择对应的可信用库，才允许资源访问，非这个库里面的特征不能够访问。也可以采用自动判定是否可行放行访问。

8.2.3.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.3.4 可信硬件管理测试

8.2.3.4.1 测试方法

可信硬件管理测试方法如下：

a） 控制台可以配置可信的硬件信息如设备 mac、bois sn 信息等信息，可以通过已有采集身份认证的形成基础库；

b） 可以采集送检到其他系统确认是否是公司资产，提供对应标准检查透传接口。

8.2.3.4.2 预期结果

能够建立企业资产库，可以用来做终端是否访问资源的一个控制项。

8.2.3.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.3.5 可信操作系统管理访问授权测试

8.2.3.5.1 测试方法

控制台可以收集终端操作系统信息，并可以配置指定操作系统授权访问。

8.2.3.5.2 预期结果

非指定可信操作系统无法进行资源访问。

8.2.3.5.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.3.6 基于安全属性变化的动态安全阻断测试

8.2.3.6.1 测试方法

基于安全属性变化的动态安全阻断测试方法如下：

a） 控制台可以联动使用基线的安全检查结果、配置对应条件如果如果基线不满足就阻断资源访问；

b） 控制台可以配置根据不同网络位置，切换不同的等级的访问资源。

8.2.3.6.2 预期结果

终端不同场景安全状态，可以对应资源访问不同，或者安全基线变化，访问阻断。

8.2.3.6.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.4 网关管理测试

8.2.4.1 网关管理信息管理测试

8.2.4.1.1 测试方法

网关管理信息管理测试方法如下：

a） 测试新增网关地址，适配终端访问；

b） 测试删除网关地址，测试终端是否无法访问；

c） 测试修改网关地址，适配终端访问；

d） 测试查询当前网关地址，且能看到查询结果。

8.2.4.1.2 预期结果

网关地址支持增删改查等管理操作。

8.2.4.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.4.2 业务访问网关路由编排测试

8.2.4.2.1 测试方法

控制台支持不同网关配置不同业务资源访问。

8.2.4.2.2 预期结果

终端可以根据不同资源的路由到不同的网关链路。

8.2.4.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.5 通信传输安全测试

8.2.5.1 测试方法

通信传输安全测试方法如下：

a） 终端在正常业务访问的时候，使用网络抓包工具，在终端进行抓包，无法破解出明文；

b） 使用流量录制工具，录制一份正常授权资源的的访问，在另外非法设备上面回放访问网关。

8.2.5.2 预期结果

通信传输安全测试预期结果如下：

a） 无法识别破解出明文；

b） 无法在另外机器回放访问服务器成功。

8.2.5.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.6 安全审计日志测试

8.2.6.1 测试方法

安全审计日志测试方法如下：

a) 终端合法身份登录，访问对应资源；

b) 后台登录管理员，下发、修改访问策略。

8.2.6.2 预期结果

安全审计日志测试方法如下：

a) 控制台应支持包含：用户身份、设备身份、终端应用进程、IP、目的 IP、源端口、目的端口、协议、域名、uri、时间、状态等信息对应的登录日志、访问行为日志的查看；

b) 后台审计员可以查看到不同管理员的操作行为日志。

8.2.6.3 结果判断

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.7 接口对接测试

8.2.7.1 其他认证系统对接测试

8.2.7.1.1 测试方法

控制台可以配置对应的，同时需要找一个标准协议的认证系统进行测试，可以指定一种两种协议进行配置。

8.2.7.1.2 预期结果

配置后终端可以使用其他认证接口进行认证,并认证成功。

8.2.7.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.7.2 访问过程中阻断联动接口测试

8.2.7.2.1 测试方法

产品方提供调用样例脚本，修改对应身份、应用程序特征、终端设备特征，让后对控制台进行调用访问。

8.2.7.2.2 预期结果

控制台可以记录对应访问的动作信息，同时可以查询对应的身份、应用程序、设备相关的访问连接，进行访问阻断。

8.2.7.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.7.3 安全状态信息收集测试

8.2.7.3.1 测试方法

提供样例脚本，可以修改参数，对控制中心精心调用。

8.2.7.3.2 预期结果

控制台可以看到对应的对象、安全状态信息传递进来的日志。

8.2.7.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.7.4 访问行为日志对外输出测试

8.2.7.4.1 测试方法

控制台可以配置目标推送服务地址，进行传输适配。提供简单样例目标系统。

8.2.7.4.2 预期结果

外部样例系统可以打印对应的接收日志。

8.2.7.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.8 设备安全增强测试

8.2.8.1 终端设备安全防护管理测试

8.2.8.1.1 测试方法

终端设备安全防护管理测试方法如下：

a) 在终端所在设备上安装基础病毒样本，测试设备针对操作系统病毒防护；

b) 在未修复漏洞的系统上安装终端，测试针对漏洞的修复能力；

c) 插入未注册的U盘、鼠标等外设，测试设备对未知外设的管控能力。

8.2.8.1.2 预期结果

终端设备安全防护管理测试预期结果如下：

a) 可成功查杀系统病毒；

b) 可成功修复基础漏洞；

c) 可成功检测、发现、禁用未知设备。

8.2.8.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.8.2 数据保护测试

8.2.8.2.1 测试方法

数据保护测试方法如下：

a） 测试打开终端，能否出现屏幕水印；

b） 测试打印素材后，素材能否出现水印。

8.2.8.2.2 预期结果

数据保护测试预期结果如下：

a） 成功出现屏幕水印；

b） 素材打印后成功出现水印。

8.2.8.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.8.3 入侵检测测试

8.2.8.3.1 测试方法

入侵检测测试方法如下：

a） 测试终端设备发起入侵（包括扫描网络、账号爆破、远程注入等），测试控制中心能够检测，并能发起告警；

b） 测试测试终端设备发起入侵（包括但不限于 Sql 注入、暴力破解等），能够实现阻断访问；

c） 测试对外日志接口，按照相关信息可成功检索日志相关信息。

8.2.8.3.2 预期结果

入侵检测测试预期结果如下：

a） 终端能够发起入侵后能够被控制中心检测，并产生告警；

b） 测试终端发起入侵后能够成功被拦截阻断；

c） 测试对外日志接口可提供日志检索能力。

8.2.8.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.8.4 终端安全应用沙箱测试

8.2.8.4.1 测试方法

控制中心下发策略开启终端应用沙箱功能。

8.2.8.4.2 预期结果

终端安全应用沙箱测试预期结果如下：

a） 终端可以收集到应用的恶意行为并能够阻断可以程序的内部资源访问；

b） 控制中心可以查看到对应应用的恶意行为日志。

8.2.8.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2.9 运维监控测试

8.2.9.1 测试方法

打开控制中心运维看板。

8.2.9.2 预期结果

运维监控测试预期结果如下：

a） 可以看到所有组件的所在宿主的 cpu、内存、磁盘利用率、服务可用性的各类指标；

b） 可以查询对应到网关到每个配置的额访问资源的网络可用性。

8.2.9.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.3 系统自身安全测试

8.3.1 身份凭据盗用避免测试

8.3.1.1 测试方法

身份凭据盗用避免测试方法如下：

a） 人工分析检查；

b） 终端程序是否有加壳；

c） 日志是否可以会看到凭据；

d） 是否有地方存储凭据，复制到另外一台设备要不可用；

e） 流量录制，要无法被回放。

8.3.1.2 预期结果

身份凭据盗用避免测试预期结果如下：

a） 流量回放访问失败；

b） 无法行本地明文存储文件获取大对应访问的凭据；

c） 终端应用程序无法直接静态逆向。

8.3.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.3.2 管理员角色权限分离测试

8.3.2.1 测试方法

人工检查管理员、审计员、策略员控制台访问操作权限是否分离。

8.3.2.2 预期结果

管理员、审计员、策略员控制台访问操作权限分离。

8.3.3 管理员行为审计能力测试

8.3.3.1 测试方法

人工检查任意管理员控制台涉及到删除修改的业务的动作，是否能够记录和追溯。

8.3.3.2 预期结果

任意管理员控制台涉及到删除修改的业务的动作，都可以记录和追溯。

8.3.4 系统所在服务器自身加固测试

8.3.4.1 测试方法

系统所在服务器自身加固测试方法如下：

a) 测试终端对系统弱密码检测、对密码策略修改，对弱密码进行修改；

b) 测试终端可以检测系统活跃，自动开启屏幕保护；

c) 测试终端可以发现共享等高位服务并屏蔽端口；

d) 测试终端可以开启审计日志，并成功收集日志。

8.3.4.2 预期结果

系统所在服务器自身加固测试预期结果如下：

a) 终端可以对系统弱密码进行检测发现，对密码策略可成功修改，对弱密码可以成功修改；

b) 终端可以在系统不活跃时，成功开启屏幕保护；

c) 终端可以成功关闭高危端口；

d) 终端可以成功开启审计日志，并收集上报。

8.3.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.4 网关单台并发性能测试

8.4.1 测试方法

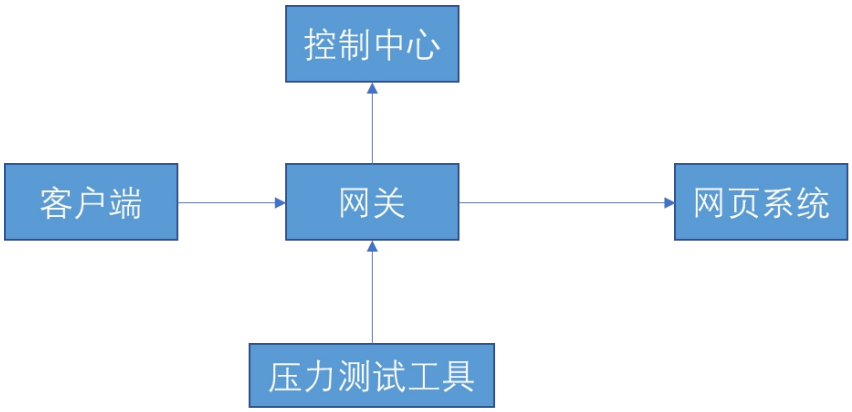

图 5 测试示意图

网关单台并发测试示意图见图 5，测试方法要求如下：

a) 提供客户端测试脚本或者测试工具，并且可以修改参数填入控制中心提供的有效授权；

b) 网页系统应提供一个优化系统，直接用 ab 或者 web 压力测试工具，直接用行业工具压力测试应超过 8000 请求数/秒；

c) 修改客户端提供对应的测试脚本或者工具参数，可以修改或者获取到控制中心一个有效授权的票据，可以直接发起网关请求，并到达网页系统。

8.4.2 预期结果

网关单台并发测试预期结果如下：

a) 可以请求成功页面系统、控制中心有对应的请求日志；

b) 压测可以达到每秒 2000 请求数/秒。

8.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.5 部署测试

8.5.1 终端部署测试

8.5.1.1 测试方法

在不同的操作系统和版本上进行客户端代理的安装。

8.5.1.2 预期结果

在不同的操作系统和版本上都能安装成功，并且运行连接成功控制中心。

8.5.2 控制中心部署测试

8.5.2.1 测试方法

控制中心部署测试方法如下：

a) 进行单机、集群、多级模式下的部署。集群模式下，增加服务器，测试服务总体的 qps。多级模式下，跨地域访问控制中心服务；

b) 进行压力测试，对比预期的并发请求数量，响应时间；

c) 跨地域访问控制中心的数据库；

d) 在展示平台查看控制中心的服务调用量、异常量、最高并发量等运行情况，进行服务器软件的安装、配置、部署、升级操作。

8.5.2.2 预期结果

控制中心部署测试预期结果如下：

a) 单机、集群、多级模式部署均能正常运行。集群模式下，增加服务器，服务的总体 qps 达到预期。多级模式下，可以实现跨地域访问控制中心服务；

b) 能达到预期并发能力，响应时间；

c) 无法跨地域访问控制中心的数据库；

d) 可以正常查看控制中心的服务调用量、异常量、最高并发量等运行情况，进行服务器软件的安装、配置、部署、升级操作。

8.5.2.3 结果判定

实际测试结果和预期结果一致，说明符合测试要求。

8.5.3 网关部署测试

8.5.3.1 测试方法

网关部署测试方法如下：

a) 增加服务器，测试服务总体的 qps；

b) 采用负载均衡技术，测试各个服务的响应时间。

8.5.3.2 预期结果

网关部署测试预期结果如下：

a) 增加服务器后，服务总体 qps 按预期提高；

b) 实现接入的均衡分布。

8.5.3.3 结果判定

实际测试结果和预期结果一致，说明符合测试要求。

8.6 容灾测试

8.6.1 控制中心容灾测试

8.6.1.1 测试方法

控制中心容灾测试方法如下：

a) 查看服务的备份、容错、冗余能力；

b) 进行控制中心数据库的数据冷热分离部署；

c) 进行数据库的增量、全量备份后测试恢复情况；

d) 利用内存数据库的持久化，查看数据恢复情况；

e) 测试 7×24 小时运行状态，期间系统状态和数据是否正常；

f) 测试控制中心的故障管理、控制能力。

8.6.1.2 预期结果

控制中心容灾预期结果如下：

a) 服务的备份、容错、冗余能力正常；

b) 数据冷热分离部署成功；

c) 数据恢复完整、速度符合预期；

d) 内存数据库能完全恢复数据；

e) 测试期间控制中心服务功能正常、数据可靠；

f) 故障情况下，控制中心可以进行告警、错误上报。

8.6.1.3 结果判定

实际测试结果和预期结果一致，说明符合测试要求。

8.6.2 网关容灾测试

8.6.2.1 测试方法

网关容灾测试方法如下：

a) 测试网关的功能；

b) 测试 7×24 h 运行的状态，期间系统状态和数据是否正常；

c) 测试网关的故障管理、控制能力。

8.6.2.2 预期结果

网关容灾测试预期结果如下：

a) 网关功能正常；

b) 测试期间网关功能正常、数据可靠；

c) 故障情况，网关可以进行告警、错误上报。

8.6.2.3 结果判定

实际测试结果和预期结果一致，说明符合测试要求。

9 服务之间调用场景测试

9.1 测试环境

功能及自身安全测评典型环境见图 6，物理服务器及虚拟机操作系统应涵盖主流 windows 及 Linux 系统，例如 windows server 2012、centos7、Ubuntu14 等；网络类型须包括 IPv4 及 IPv6。

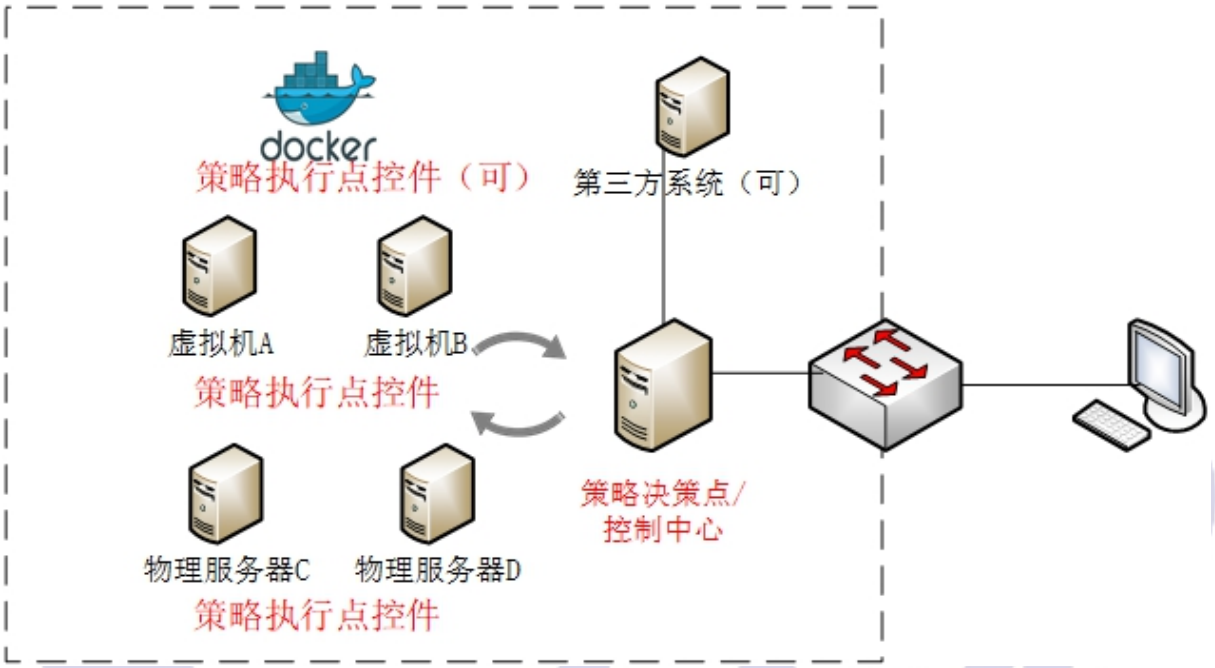

图 6 测试环境典型示意图

9.2 功能测试

9.2.1 工作负载信息识别测试

9.2.1.1 工作负载基本信息（含操作系统版本、网卡信息、服务信息、监听端口信息等）获取测试

9.2.1.1.1 测试方法

工作负载基本信息获取测试方法如下：

a) 审查系统说明文档，分析产品基本信息获取能力；

b) 在策略决策点中查看一台已管理的工作负载，查看是否识别或读取到工作负载的操作系统版本、网卡信息、服务信息、监听端口信息等；

c) 查看此信息与是否与工作负责实际情况一致。

9.2.1.1.2 预期结果

工作负载基本信息获取测试预期结果如下：

a) 能够显示工作负载的操作系统版本、网卡信息、服务信息、监听端口信息等；

b) 自动识别或读取到的信息与工作负载实际的信息一致。

9.2.1.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.1.2 工作负载唯一标识身份信息确定测试

9.2.1.2.1 测试方法

工作负载唯一标识身份信息确定测试方法如下：

a) 审查系统说明文档，分析系统标识身份信息能力；

b) 检查是否能够为每一台工作负载配置或生成身份信息；

c) 身份信息是否唯一。

9.2.1.2.2 预期结果

工作负载唯一标识身份信息确定测试预期结果如下：

a) 系统能够为每一台工作负载配置或生成身份信息；

b) 身份信息唯一。

9.2.1.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.1.3 主机信息状态变化上传至管理端测试

9.2.1.3.1 测试方法

主机信息状态变化上传至管理端测试方法如下：

a) 将某台管理范围内的工作负载的基本信息进行修改，例如 IP 信息、关机等；

b) 查看策略决策点是否识别出该变化。

9.2.1.3.2 预期结果

策略决策点能够识别主机信息变化。

9.2.1.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.1.4 其他认证体系对接支持测试

9.2.1.4.1 测试方法

其他认证体系对接支持测试方法如下：

a) 审查系统说明文档，分析系统与其他认证体系对接功能；

b) 查看系统是否具备与其他认证体系对接的接口；

c） 通过接口导入认证信息，系统是否可接收并显示信息。

9.2.1.4.2 预期结果

其他认证体系对接支持测试预期结果如下：

a） 系统具备与其他认证体系对接的接口；

b） 认证信息可成功导入系统，系统可接收且显示。

9.2.1.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.2 服务之间访问控制测试

9.2.2.1 服务端代理/网关组件使用最小安全原则测试

9.2.2.1.1 测试方法

服务端代理/网关组件使用最小安全原则测试方法如下：

a） 审查系统说明文档，分析系统的访问控制能力；

b） 配置服务之间的允许访问控制规则，查看符合规则的访问是否被放行；

c） 构建不符合规则的访问，查看是否被阻止。

9.2.2.1.2 预期结果

服务端代理/网关组件使用最小安全原则测试预期结果如下：

a） 系统可以配置允许的访问控制规则；

b） 符合规则的访问被放行，不符合规则的被禁止。

9.2.2.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.2.2 基于源 IP 地址、目的 IP 地址和端口的访问控制测试

9.2.2.2.1 测试方法

基于源 IP 地址、目的 IP 地址和端口的访问控制测试方法如下：

a） 审查系统说明文档，分析系统的访问控制能力；

b） 配置一条允许某 IP 访问另一 IP 地址特定端口的访问控制规则；

c） 验证是否符合规则的访问被放行。

9.2.2.2.2 预期结果

基于源 IP 地址、目的 IP 地址和端口的访问控制测试预期结果如下：

a） 系统可以配置基于源 IP、目的 IP 及端口的访问控制规则；

b） 符合规则的访问被放行。

9.2.2.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.2.3 出站和入站双向访问控制测试

9.2.2.3.1 测试方法

出站和入站双向访问控制测试方法如下：

a) 审查系统说明文档，分析系统的出站及入站控制功能；

b) 配置相关出站及入站规则；

c) 分别尝试执行符合规则出站、入站的访问，检查是否成功；

d) 分别尝试执行违反规则的出站、入站访问，检查是否成功。

9.2.2.3.2 预期结果

出站和入站双向访问控制测试预期结果如下：

a) 系统能够配置出站及入站规则；

b) 符合规则的访问被放行；

c) 违反规则的访问被阻止。

9.2.2.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.2.4 接收并执行控制中心组件下发动态访问控制策略测试

9.2.2.4.1 测试方法

接收并执行控制中心组件下发动态访问控制策略测试方法如下：

a) 审查系统说明文档，分析系统的策略同步机制；

b) 在策略决策点修改某工作负载的安全策略，在服务端代理/网关组件上查看查看是否接收到修改的安全策略并执行。

9.2.2.4.2 预期结果

服务端代理/网关组件可以准确接收并执行策略决策点下发的策略。

9.2.2.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.2.5 记录违反策略规则的阻断日志，并上传至控制中心测试

9.2.2.5.1 测试方法

记录违反策略规则的阻断日志，并上传至控制中心测试方法如下：

a) 审查系统说明文档，分析系统阻断日志能力；

b） 配置安全策略，并尝试执行违反安全策略的访问，查看策略决策点是否记录相应日志。

9.2.2.5.2 预期结果

系统可以记录相应阻断日志。

9.2.2.5.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.2.6 ipv6 网络流量访问控制测试

9.2.2.6.1 测试方法

ipv6 网络流量访问控制测试方法如下：

a） 审查系统说明文档，分析系统对于 IPv6 的支持能力；

b） 构建 IPv6 环境，基于 IPv6 地址配置安全策略；

c） 利用 IPv6 地址进行符合安全策略的网络访问，查看是否被放行；

d） 利用 IPv6 地址进行违反安全策略的网络访问，查看是否被阻止。

9.2.2.6.2 预期结果

ipv6 网络流量访问控制测试预期结果如下：

a） 系统可以配置 IPv6 的安全策略；

b） 符合安全策略的访问被放行，违反安全策略的访问被阻止。

9.2.2.6.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.2.7 容器之间访问控制测试

9.2.2.7.1 测试方法

容器之间访问控制测试方法如下：

a） 审查系统说明文档，分析系统对容器的支持能力；

b） 构建容器环境，配置容器之间的访问控制规则；

c） 容器之间进行符合安全策略的网络访问，查看是否被放行；

d） 容器之间进行违反安全策略的网络访问，查看是否被阻止。

9.2.2.7.2 预期结果

容器之间访问控制测试预期结果如下：

a） 系统能够配置容器之间的访问控制规则；

b） 符合安全策略的访问被放行；

c） 违反安全策略的访问被阻止。

9.2.2.7.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.2.8 建立服务之间的加密隧道来实现访问控制测试

9.2.2.8.1 测试方法

建立服务之间的加密隧道来实现访问控制测试方法如下：

a） 审查系统说明文档，分析系统加密功能；

b） 配置工作负载之间的基于加密方式访问控制策略；

c） 尝试进行符合安全策略的访问，查看是否被放行，并通过抓包工具抓取对应流量，查看是否加密；

d） 尝试进行违反安全策略的访问，查看是够被阻止。

9.2.2.8.2 预期结果

建立服务之间的加密隧道来实现访问控制测试预期结果如下：

a） 系统可以配置基于加密方式的访问控制策略；

b） 符合安全策略的被放行，且抓包工具抓取的流量为加密形式；

c） 违反安全策略的访问被阻止。

9.2.2.8.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.3 服务之间流量识别

9.2.3.1 识别出站及入站的网络流量测试

9.2.3.1.1 测试方法

识别出站及入站的网络流量测试方法如下：

a） 审查系统说明文档，分析系统出入站流量识别能力；

b） 构建工作负载出站及入站流量，查看系统是否识别到对应流量；

c） 查看是否识别到来源 IP、目的 IP、端口及服务信息。

9.2.3.1.2 预期结果

识别出站及入站的网络流量测试预期结果如下：

a） 系统能够识别工作负载的出站及入站流量；

b） 能够识别到流量的来源 IP，目的 IP，端口及服务。

9.2.3.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.3.2 学习到流量信息统一呈现及搜索测试

9.2.3.2.1 测试方法

学习到流量信息统一呈现及搜索测试方法如下：

a) 审查系统说明文档，分析系统流量呈现及搜索能力；

b) 查看系统策略决策点是否支持流量信息的统一查看；

c) 查看系统是否支持流量信息的搜索。

9.2.3.2.2 预期结果

学习到流量信息统一呈现及搜索测试预期结果如下：

a) 系统能够对流量进行统一呈现；

b) 系统支持流量信息的搜索。

9.2.3.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.3.3 报表形式输出流量统计分析结果测试

9.2.3.3.1 测试方法

报表形式输出流量统计分析结果测试方法如下：

a) 审查系统说明文档，分析系统流量日志导出能力；

b) 查看系统是否支持将流量信息通过报表形式进行导出。

9.2.3.3.2 预期结果

系统能够支持以报表形式导出流量信息。

9.2.3.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.3.4 支持记录异常访问日志，并支持输出到其他系统平台测试

9.2.3.4.1 测试方法

支持记录异常访问日志，并支持输出到其他系统平台测试方法如下：

a) 审查系统说明文档，分析系统异常访问日志功能；

b) 查看系统是否能够记录异常访问日志；

c) 查看系统是否具备接口将日志导出至其他系统，或允许其他系统读取。

9.2.3.4.2 预期结果

支持记录异常访问日志，并支持输出到其他系统平台测试预期结果如下：

a) 系统能够记录异常访问日志；

d） 系统具备接口将日志导出至其他系统，或允许其他系统读取。

9.2.3.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.3.5 实时工作负载间流量关系拓扑测试

9.2.3.5.1 测试方法

实时工作负载间流量关系拓扑测试方法如下：

a） 审查系统说明文档，分析系统流量拓扑能力；

b） 查看策略决策点是否能够以拓扑形式展示工作负载间流量；

c） 构建工作负载间符合策略与违反策略的访问，查看系统是否能够在拓扑图中进行明确的标识。

9.2.3.5.2 预期结果

实时工作负载间流量关系拓扑测试预期结果如下：

a） 系统能够以拓扑的形式展示工作负载间的流量；

b） 系统能够标识匹配策略与不匹配策略的流量。

9.2.3.5.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.3.6 组件上传阻断日志查看测试

9.2.3.6.1 测试方法

组件上传阻断日志查看测试方法如下：

a） 审查系统说明文档，分析阻断日志呈现与分析能力；

b） 构建工作负载之间的违反策略的访问，并形成阻断日志；

c） 查看系统是否能够统一对阻断日志进行查看，尝试基于时间、来源 IP、目的 IP、端口等维度搜索相应阻断日志。

9.2.3.6.2 预期结果

组件上传阻断日志查看测试预期结果如下：

a） 系统能够对阻断日志进行统一查看；

b） 系统支持基于时间、来源、目的、端口等维度对阻断日志进行分析。

9.2.3.6.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.3.7 IPv6 出站及入站流量识别测试

9.2.3.7.1 测试方法

IPV6 出站及入站流量识别测试方法如下：

a） 审查系统说明文档，分析系统 IPv6 流量识别能力；

b） 构建 IPv6 环境，并通过 IPv6 网络进行工作负载之间出站及入站的访问；

c） 查看系统是否识别到相应的访问流量。

9.2.3.7.2 预期结果

系统能够准确识别 IPv6 下的出站及入站访问。

9.2.3.7.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.3.8 容器之间流量识别测试

9.2.3.8.1 测试方法

容器之间流量识别测试方法如下：

a） 审查系统说明文档，分析系统容器流量识别能力；

b） 构建容器环境，并构建容器之间的流量；

c） 查看系统是否准确识别容器之间的流量。

9.2.3.8.2 预期结果

系统能够准确识别容器之间的流量。

9.2.3.8.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.4 策略管理能力

9.2.4.1 通过集中安全管理界面对分布式部署安全服务组件的统一策略下发的测试

9.2.4.1.1 测试方法

通过集中安全管理界面对分布式部署安全服务组件的统一策略下发的测试方法如下：

a） 审查系统说明文档，分析系统策略管理能力；

b） 通过策略决策点进行安全策略的配置，查看各策略执行组件（服务端代理/网关）是否接收并执行相应策略。

9.2.4.1.2 预期结果

通过集中安全管理界面对分布式部署安全服务组件的统一策略下发的测试预期结果如下：

a） 系统可以通过策略决策点统一配置安全策略；

b） 分布式组件能够正确获取并执行安全策略。

9.2.4.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.4.2 支持配置任意两个工作负载之间安全策略的测试

9.2.4.2.1 测试方法

支持配置任意两个工作负载之间安全策略的测试方法如下：

a） 审查系统说明文档，分析系统配置策略能力；

b） 构建两个不同环境，例如公有云和私有云，或者物理环境和虚拟化环境，选择不同环境的两台工作负载（网络互通），并查看是否能够正常配置安全策略。

9.2.4.2.2 预期结果

系统能够配置两台不同环境的工作负载。

9.2.4.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.4.3 接收策略控制点组件上传工作负载策略状态变化信息的测试

9.2.4.3.1 测试方法

接收策略控制点组件上传工作负载策略状态变化信息的测试方法如下：

a） 审查系统说明文档，分析系统相关能力说明；

b） 查看系统是否能够记录控制点组件（服务端代理/网关）策略修改、同步、篡改等变化日志。

9.2.4.3.2 预期结果

系统能够记录相关策略变化日志。

9.2.4.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.4.4 基于识别到的流量自动或半自动的方式生成安全策略的测试

9.2.4.4.1 测试方法

基于识别到的流量自动或半自动的方式生成安全策略的测试方法如下：

a） 审查系统说明文档，分析系统相关能力说明；

b） 构建工作负载间的访问流量，查看策略决策点是否能够基于流量快速配置策略。

9.2.4.4.2 预期结果

系统不是手动填写策略，而是可以通过系统相关功能快速生成安全策略。

9.2.4.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.4.5 基于业务角色、主机属性等进行安全策略配置的测试

9.2.4.5.1 测试方法

基于业务角色、主机属性等进行安全策略配置的测试方法如下：

a) 审查系统说明文档，查看系统相关功能说明；

b) 基于业务角色及主机属性配置两条安全策略；

c) 分别构建符合两条安全策略的访问，查看是否被放行；

d) 分别构建违反两条安全策略的访问，查看是否被阻止。

9.2.4.5.2 预期结果

基于业务角色、主机属性等进行安全策略配置的测试预期结果如下：

a) 系统具备基于工作负载业务角色、主机属性配置安全策略的能力；

b) 符合策略的访问放行，违反策略的访问被阻止。

9.2.4.5.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.4.6 具备防护及非防护状态的测试

9.2.4.6.1 测试方法

具备防护及非防护状态的测试方法如下：

a) 审查系统说明文档，查看系统相关功能说明；

b) 配置两个工作负载间的策略，当防护状态时，查看策略是否生效；

c) 切换防护状态到非防护状态，查看策略是否失效。

9.2.4.6.2 预期结果

具备防护及非防护状态的测试预期结果如下：

a) 防护状态下，策略生效；

b) 切换为非防护状态时，策略失效。

9.2.4.6.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.5 动态授权测试

9.2.5.1 工作负载发生变化时，访问控制策略动态调整测试

9.2.5.1.1 测试方法

工作负载发生变化时，访问控制策略动态调整测试方法如下：

a) 审查系统说明文档，分析系统动态授权功能；

b) 配置两台工作负载之间的安全策略；

c) 修改安全策略中来源工作负载的 IP，查看系统是否自动修改原安全策略；

d) 将安全策略中来源工作负载关机，并从策略决策点删除此台工作负载，查看系统是否能够自动修改原安全策略。

9.2.5.1.2 预期结果

工作负载发生变化时，访问控制策略动态调整测试预期结果如下：

a) 系统能够识别 IP 变化，并自动修改安全策略中的源 IP；

b) 系统能够自动删除安全策略中已下线的工作负载 IP。

9.2.5.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.5.2 工作负载认证信息发送变化时，访问控制策略动态调整测试

9.2.5.2.1 测试方法

工作负载认证信息发送变化时，访问控制策略动态调整测试方法如下：

a) 审查系统说明文档，分析相关功能说明；

b) 修改某工作负载的认证信息，查看系统是否动态调整安全策略。

9.2.5.2.2 预期结果

工作负载认证信息发送变化时，访问控制策略动态调整测试预期结果如下：

a) 系统能够识别到认证信息的修改；

b) 系统能够动态调整安全策略。

9.2.5.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.6 接口对接测试

9.2.6.1 阻断其他系统访问连接测试

9.2.6.1.1 测试方法

提供给其他安全系统调用的接口，出现安全风险的时候，阻断身份、应用、工作负载标示对应的所

有访问连接的测试方法如下：

a） 审查系统说明文档，分析相关接口文档；

b） 配置两台工作负载间的安全策略，通过接口向系统发送修改策略的指令，查看系统是否接收；

c） 查看安全策略是否被修改。

9.2.6.1.2 预期结果

提供给其他安全系统调用的接口，出现安全风险的时候，阻断身份、应用、工作负载标示对应的所有访问连接的测试预期结果如下：

a） 系统具备接受指令接口，并能正确接收指令；

b） 安全策略被修改。

9.2.6.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.6.2 提供给其他安全分析系统针对本系统获取到日志的测试

9.2.6.2.1 测试方法

提供给其他安全分析系统针对本系统获取到日志的测试方法如下：

a） 审查系统说明文档，查看相关接口文档；

b） 构造认证信息及访问日志等信息；

c） 通过接口读取系统相关日志信息，查看是否能够成功读取。

9.2.6.2.2 预期结果

系统能够被其他系统读取相关日志信息。

9.2.6.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.7 安全防护管理测试

9.2.7.1 工作负载操作系统基础病毒防护测试

9.2.7.1.1 测试方法

工作负载操作系统基础病毒防护测试方法如下：

a） 审查系统说明文档，分析相关病毒防护能力；

b） 查看系统是否具备病毒防护的功能；

c） 构建病毒文档发送至工作负载，查看系统是否识别到该病毒并进行处置。

9.2.7.1.2 预期结果

工作负载操作系统基础病毒防护测试预期结果如下：

a） 系统具备病毒防护功能；

b） 系统能够识别并防护病毒。

9.2.7.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.7.2 工作负载漏洞修复测试

9.2.7.2.1 测试方法

工作负载漏洞修复测试方法如下：

a） 审查系统说明文档，查看漏洞修复能力；

b） 通过系统对工作负载进行漏洞扫描，查看是否能够发现漏洞并提供解决办法。

9.2.7.2.2 预期结果

系统能够发现工作负载漏洞，并提供解决办法。

9.2.7.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.2.7.3 动态检测工作负载的入侵行为，并输出告警的测试

9.2.7.3.1 测试方法

动态检测工作负载的入侵行为，并输出告警的测试方法如下：

a） 审查系统说明文档，查看系统入侵检测功能；

b） 构造针对工作负载的恶意脚本攻击、暴力破解、或漏洞利用攻击等行为；

c） 查看系统是否对入侵行为进行检测，并输出告警。

9.2.7.3.2 预期结果

系统能够准确识别入侵行为，并进行告警。

9.2.7.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3 系统自身安全测试

9.3.1 标识与鉴别

9.3.1.1 维护用户安全属性（用户标识、授权信息或用户组信息、其他安全属性等）测试

9.3.1.1.1 测试方法

维护每个用户安全属性测试方法如下：

a） 查看产品是否为每一个用户保存其安全属性表，属性可包括：用户标识、授权信息或用户组信息、其他安全属性等；

b） 以不同的授权用户身份登录系统，执行其权限范围内的操作，检查该用户可执行的操作与其安全属性（如用户标识、授权信息等）的要求是否一致；

c） 修改用户的部分安全属性后，检查该用户可执行的操作与其被修改后的安全属性的要求是否一致。

9.3.1.1.2 预期结果

维护每个用户安全属性测试预期结果如下：

a） 产品支持为每一个用户定义及维护其安全属性表；

b） 用户可执行的操作与其安全属性（如用户标识、授权信息等）的要求一致；

c） 用户可执行的操作与其被修改后的安全属性（如授权信息等）的要求一致。

9.3.1.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.1.2 用户全局唯一标识测试

9.3.1.2.1 测试方法

任何用户均具有全局唯一标识的测试方法如下：

a） 以授权用户身份登录系统，查看用户信息；

b） 尝试新建一个相同用户标识的用户，检查操作是否能够成功。

9.3.1.2.2 预期结果

系统不能新建相同用户标识的用户。

9.3.1.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.1.3 用户成功鉴别测试

9.3.1.3.1 测试方法

每个用户在执行与系统安全相关的任何其他操作之前，都已被成功鉴别的测试方法如下：

a） 查看用户在未被成功鉴别前，是否被拒绝执行任何安全相关的操作；

b） 查看产品是否拒绝错误的鉴别信息的用户登录；

c） 以正确的鉴别信息登录并进行安全相关操作，验证产品是否允许登录，是否允许进行安全相关操作。

9.3.1.3.2 预期结果

每个用户在执行与系统安全相关的任何其他操作之前，都已被成功鉴别的测试预期结果如下：

a） 用户被成功鉴别前，不能执行任何与安全相关的操作；

b） 输入错误鉴别信息，产品不允许登录；

c） 输入正确的鉴别信息，能够成功登录，并执行安全相关操作

9.3.1.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.1.4 服务端代理/网关组件感知自身运行状态并上传至管理端的测试

9.3.1.4.1 测试方法

服务端代理/网关组件能够对自身的运行状态进行感知，并上传至管理端的测试方法如下：

a） 查看系统策略决策点是否能够显示各个服务端代理/网关组间的运行状态；

b） 修改某个服务端代理/网关的运行状态，查看策略决策点是否能够能够修改对应状态或记录相关日志。

9.3.1.4.2 预期结果

服务端代理/网关组件能够对自身的运行状态进行感知，并上传至管理端的测试预期结果如下：

a） 系统能够正确显示服务端代理/网关的运行状态；

b） 当状态改变时，系统能够记录对应状态或日志。

9.3.1.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.2 鉴权失败处理测试

9.3.2.1 测试方法

鉴权失败处理测试方法如下：

a） 系统应能检测用户不成功的鉴权尝试；

b） 在达到或超过最大连续鉴别失败尝试次数阈值后，系统应采取措施阻止进一步的鉴权尝试，直至满足已定义的条件才允许进行重新鉴权；

c） 应仅由授权管理员设置未成功鉴权尝试次数阈值。

9.3.2.2 预期结果

鉴权失败处理测试预期结果如下：

a） 以错误的鉴别信息尝试登录微隔离产品，检查是否被拒绝进入系统；

b） 继续进行一定次数的登录尝试，验证在达到允许的鉴别失败尝试次数后，微隔离产品是否使该用户账号或登录点失效；

c） 查看达到微隔离产品已定义的解锁条件后，失效的用户账号或登录点是否可以重新进行鉴别操作；

d） 检查未成功鉴别尝试次数阈值是否仅由授权管理员设置。

9.3.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.3 通信传输保护测试

9.3.3.1 服务端代理/网关组件与策略决策点通信加密测试

9.3.3.1.1 测试方法

在策略决策点修改服务端代理/网关的安全策略，或进行相关配置，同时使用抓包工具截取数据进行分析，查看数据是否不为明文。

9.3.3.1.2 预期结果

获取的数据不为明文。

9.3.3.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.3.2 web 页面管理系统管理过程数据加密测试

9.3.3.2.1 测试方法

通过 web 页面对策略决策点进行系统配置、修改安全策略等操作，同时使用抓包工具截取数据进行分析，查看数据是否不为明文。

9.3.3.2.2 预期结果

获取的数据不为明文。

9.3.3.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.3.3 API 接口权限验证测试

9.3.3.3.1 测试方法

API 权限验证测试方法如下：

a） 在无验证的情况下通过 api 接口对系统进行工作负载信息查看或系统配置，查看请求是否被阻止；

b） 在输入正确验证信息的情况下，通过 API 接口对系统进行工作负载信息查看或系统配置。

9.3.3.3.2 预期结果

API 权限验证测试预期结果如下：

a） 不进行权限验证，请求被阻止；

b） 进行权限验证的情况下，请求被允许，能够查看及修改相关信息。

9.3.3.3.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.4 安全审计测试

针对以下事件，产生审计记录：

a) 审计功能的启动和关闭；

b) 导出、另存和删除审计日志；

c) 设置鉴别尝试次数；

d) 鉴别机制的使用；

e) 用户的创建、修改、删除与授权；

f) 其他系统参数配置和管理安全功能行为的操作。

9.3.4.1 测试方法

安全审计测试方法如下：

a) 以授权用户身份登录系统执行检测要求上述相关的操作，查看审计记录，检查系统是否对操作进行了审计记录；

b) 查看审计记录内容中是否包括事件发生的日期和时间、事件类型、主体身份标识、事件描述及结果等信息。

9.3.4.2 预期结果

安全审计测试预期结果如下：

a) 产品对支持的事件发生产生了审计记录；

b) 审计记录内容中包括事件发生的日期和时间、事件类型、主体身份标识、事件描述及结果等信息。

9.3.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.5 系统加固测试

9.3.5.1 策略决策点所在主机防火墙开启并限定端口开放的测试

9.3.5.1.1 测试方法

策略决策点所在系统防火墙开启并限定端口开放测试方法如下：

a) 查看策略决策点所在主机的防火墙状态是否为开启；

b) 查看是否除必要开放的端口外，其他端口均已关闭。

9.3.5.1.2 预期结果

策略决策点所在系统防火墙为开启状态，且只开放了必要端口。

9.3.5.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.3.5.2 策略决策点所在主机应完成漏洞修复，策略决策点自身应无高危漏洞的测试

9.3.5.2.1 测试方法

对策略决策点所在主机进行漏洞扫描，查看是否存在高危漏洞。

9.3.5.2.2 预期结果

策略决策点及所在系统均不存在高危漏洞。

9.3.5.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.4 性能测试服务端代理/网关组件降级测试

9.4.1 测试方法

服务端代理/网关组件降级测试方法如下：

a) 查看系统文档，分析系统降级机制；

b) 根据系统设计的降级机制，构造 CPU、内存、硬盘中的一个或多个的占用达到设计的限度，查看系统组件是否能够自动暂停服务或控制占用不再增加。

9.4.2 预期结果

系统具备降级机制，当占用达到设计限度时，系统组件可以自动降级（暂停服务或控制占用不再增加）。

9.4.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.5 部署测试

9.5.1 策略决策点集群化部署测试

9.5.1.1 测试方法

策略决策点集群化部署测试方法如下：

a) 尝试是否能够成功采用多台物理服务器或虚拟机进行集群化部署系统策略决策点；

b) 在系统运行时，任意关闭一台策略决策点所在主机，查看系统是否仍正常运行。

9.5.1.2 预期结果

策略决策点集群化部署测试预期解雇如下：

a) 策略决策点可以集群化部署；

b) 任意关闭一台不影响系统运行。

9.5.1.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

9.5.2 服务端代理/网关组件自动化部署测试

9.5.2.1 测试方法

服务端代理/网关组件自动化部署测试方法如下：

a) 查看系统文档，分析系统组件自动化部署能力；

b) 通过自动化工具或系统提供的自动化部署方式，尝试自动化部署 5 个服务端代理/网关组件，查看是否成功部署。

9.5.2.2 预期结果

能够成功部署。

9.5.2.3 结果判定

实际测试结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

附录 A
（资料性）
其他系统

A.1 身份认证接口适配场景

A.1.1 场景

落地不同企业都有对接其他身份认证系统的需求。

A.1.2 接口要求

能够对接其他身份认证系统，支持常见认证协议，如 LDAP，OAuth2.0、RADIUS、OIDC、SAML2.0 等，支持认证协议的可扩展性。

A.2 访问过程中阻断联动接口场景

A.2.1 场景

访问过程中，一旦发现针对访问过程中关键对象的安全风险，要对关键对象的涉及到的资源访问进行阻断，最大程度降低企业数据泄漏或者入侵的风险。

提供访问控制阻断接口，供其他安全分析系统在发现有关键对象风险的时候，进行针对性阻断。

A.2.1 接口要求

支持身份、应用、终端设备等出现安全风险的时候调用阻断。

A.3 安全信息对接场景

A.3.1 场景

企业内部有多种多样的安全系统，需要收集和访问过程有关系的关键对象检测系统的检测结果。比如身份风险、恶意应用、设备风险等等，这些和访问过程中的关键对象的安全状态星系。

A.3.2 接口要求

接口要求涉及到：关键对象（因素）、身份、设备、网络连接、资源等，标示了风险程度，需尽量提供确切的结果，减少分析的复杂度。自动化过程期望确切的信息，不确切的，需要额外的分析系统去做做处理，可能会涉及到人员运营参与。

A.4 访问行为日志对外输出场景

A.4.1 场景

对外输出安全系统输出访问日志，其他系统做访问风险分析。

A.4.2 接口要求

传输方式：部署采集器，或者流方式队列对接 kafka、nsq、tcp-syslog（访问日志量大，建议采用流式队列的方案）。

数据格式：一层 key-value,少嵌套，json 或者其他兼容性更好的自描述格式，如 {Key:’value’,key2:123}、或者’ vendor="top" dev_type="3" dev_name="RJY-NGJMR"

dev_ip="172.21.6.244" time="2020-07-20 14:38:46" ‘（支持非机构化存储，非结构化便于扩展，自描述跨系统解析方便性，兼容更多分析存储平台）。

内容：使用网关的信息、【认证类型】、账户\身份，时间，设备信息，进程，连接信息（设备网络地址，目标地址），连接耗时，连接错误信息等。

数据关键点：

——网关 IP；

——网关端口；

——客户端帐号；

——设备唯一标志；

——访问时间；

——客户端 IP；

——进程名；

——目标地址；

——目标 IP；

——目标端口；

——耗时；

——错误信息。

附录 B
（规范性）
垂直流量网关功能要求

B.1 反向代理功能

反向代理应符合如下功能要求：

a） 具备通过 DNS 解析方式，将应用访问解析到网关上；

b） 对于接入的应用，在非授权状态下拦截访问请求；

c） 对请求身份可以基于用户身份和来源终端进行识别和判断。

B.2 应用层代理能力

B.2.1 Web 协议代理网关

Web 协议代理网关应符合以下要求：

a） 支持客户端流量解密，并还原到不同协议的业务系统；

b） 支持包头拆解终端身份鉴权权、访问系统权限鉴定；

c） 支持提供对外的阻断能力。

B.2.2 Web API 网关

Web API 网关应符合如下：

a） 支持访问来源参数鉴权，访问权限鉴定；

b） 支持 api 访问目的系统，编排自动路由能力；

c） 支持服务注册。

B.2.3 SSH 代理网关

SSH 网关应符合如下：

a） 支持来源终端鉴权；

b） 支持命令行信息收集审计；

c） 支持响应各种命令阻断能力；

d） 支持联动其他安全信息阻断。

B.3 全流量代理能力

全流量代理应符合如下：

a） 支持所有终端应用类型的协议；

b） 支持还原转发到所有原始系统的流量，支持 tcp、udp 以及各类应用层协议；

c） 访问日志上报。

参 考 文 献

[1] GB/T 25069－2010　信息安全技术　术语

[2] GB/T 29242—2012　信息安全技术　鉴别与授权安全断言标记语言

[3] ISO/IEC 24745:2011　Information technology—Security techniques—Biometric information protection