ICS 35.030
CCS L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 网络安全产品互联互通框架

Information security technology—
Framework of network security product interconnect

（征求意见稿）

（本草案完成时间：2023 年 7 月 12 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：北京赛西科技发展有限责任公司、国家信息中心、国家互联网应急中心、中国电子技术标准化研究院、中国科学院信息工程研究所、中国移动通信集团、北京大学、联通数字科技有限公司、天翼安全科技有限公司、沈阳东软系统集成工程有限公司、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、北京升鑫网络科技有限公司、安天科技集团股份有限公司、广电计量检测集团股份有限公司、华为技术有限公司、奇安信科技集团股份有限公司。

本文件主要起草人：杨建军、姚相振、孙彦、许玉娜、刘蓓、李建强、陈韵然、姜政伟、邱勤、谢安明、王智明、马晨、严冬、孙凌、陈星、安高峰、何茂根、闫桂勋、卞建超、唐迪、孙可人、赵新强、张卫博、姚叶鹏、李强、丁宇征。

信息安全技术 网络安全产品互联互通框架

1 范围

本文件给出了网络安全产品互联互通框架，包括互联互通功能和互联互通信息。

本文件适用于指导网络安全产品互联互通的设计、开发和应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南

GB/T 25066-2020 信息安全技术 信息安全产品类别与代码

GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

GB/T 25066-2020界定的以及下列术语和定义适用于本文件。

3.1

网络安全产品 network security product

专门用于保障网络安全的软件、硬件或其组合体。

[来源：GB/T 25066-2020 3.1，有修改]

3.2

网络安全产品互联互通 network security product interconnect

通过统一的网络安全信息描述和安全功能实现，有效共享网络安全产品感知或产生的信息，协同不同网络安全产品的功能，支撑监测预警、信息共享、应急响应、态势感知等应用，提升网络安全防护能力和网络安全事件处置效率的一种机制。

3.3

互联互通功能 interconnect function

网络安全产品实现互联互通所应用的安全功能及其实现方式。

3.4

互联互通信息 interconnect information

网络安全产品支撑互联互通功能实现所提供数据的类型、结构和数据格式。

4 互联互通框架

4.1 概述

网络安全产品互联互通框架包括网络安全产品的互联互通功能和互联互通信息，具体见图1。

互联互通功能的功能类型主要分为4类，包括识别功能、防护功能、监测功能和处置功能。功能接口支撑各类功能实现，规范接口的通信协议、请求方式以及应满足的安全机制。

互联互通信息的信息类型主要分为6类，包括行为信息、告警信息、资产信息、脆弱性信息、威胁信息和事件信息。信息描述规范互联互通信息的信息内容和信息格式。

附录A给出了网络安全产品互联互通典型应用场景。附录B给出了互联互通功能使用的互联互通信息。

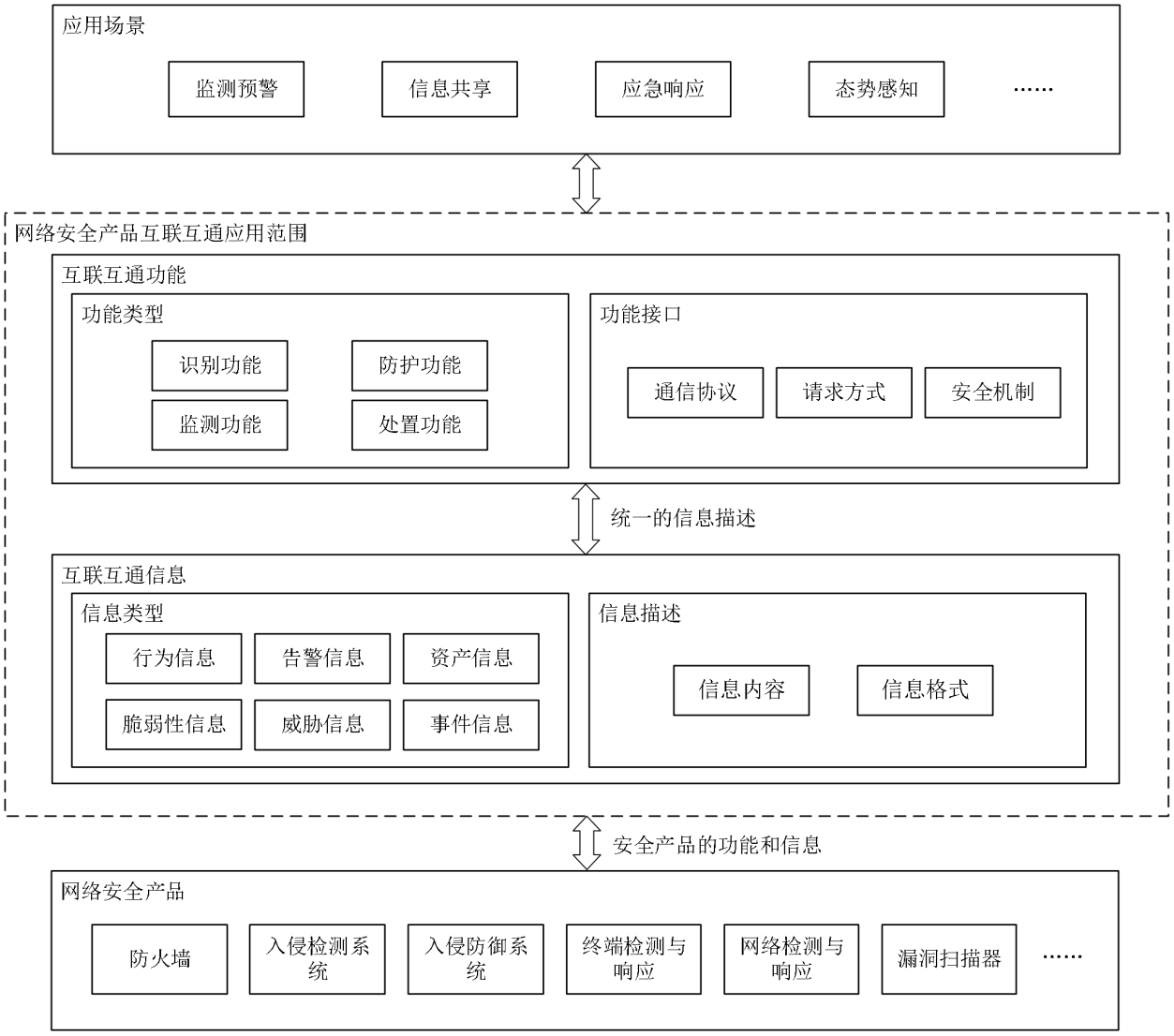

图 1　网络安全产品互联互通框架

4.2　互联互通功能

4.2.1　功能类型

4.2.1.1　识别功能

识别功能通过对软硬件、数据、网络等信息的采集与分析，识别潜在的网络安全风险。识别功能主要包括：

a)　资产识别：检查、发现网络、软硬件和数据等资产，形成资产信息；

b)　脆弱性识别：发现已识别资产中可能存在的脆弱性，包括漏洞扫描、代码审计、配置核查等，形成脆弱性信息；

c)　威胁识别：通过分析网络流量、安全日志、威胁情报等，识别威胁，形成威胁信息；

d) 网络流量采集：通过流量镜像等方式，获取并记录网络行为，形成行为信息；
e) 终端信息采集：对终端进程、流量特征、文件等信息进行采集，获取并记录终端行为，形成行为信息。

4.2.1.2 防护功能

防护功能通过实施防护措施，防范网络安全风险。防护功能主要包括：
a) 身份管理与鉴别：标识和鉴别软硬件、数据、网络等访问者身份合法性的过程，形成行为信息，对于存在非授权访问的情况，还应形成告警信息；
b) 网络访问控制：按照网络访问控制策略对访问行为进行阻断或授权，形成行为信息，当发生阻断时，还应形成告警信息；
c) 网络入侵防御：通过协议解码、内容检测、规则匹配及威胁情报分析等技术手段，检测和阻断网络入侵行为，形成行为信息、告警信息；
d) 网络隔离交换：通过终止网络连接、分离网络协议等方式，将数据以专有数据块的形式在不同网络间进行摆渡，实现网络隔离环境下数据交换的过程，形成行为信息、告警信息；
e) 网络行为控制：通过行为模式识别、规则匹配等方式分析网络行为，进行隔离、过滤、放行等操作，形成行为信息、告警信息；
f) 网络流量控制：基于流量控制策略对网络流量进行监测、分类、整形、带宽限速、带宽保障等操作，优化带宽资源使用，避免网络拥塞，形成行为信息、告警信息；
g) 拒绝服务攻击防护：通过 TCP 代理、源 IP 验证等方式，发现网络流量的拒绝服务攻击行为，对匹配抗拒绝服务策略的网络流量进行阻断，形成行为信息、告警信息；
h) 数据库防护：通过数据库审计等方式，发现并阻断针对数据库系统的攻击，形成行为信息、告警信息；
i) 恶意代码防范：通过漏洞扫描、注册表查找等方式，检测发现僵尸、木马、蠕虫等恶意代码，并对其进行清除或隔离等操作，形成行为信息、告警信息；
j) 应用安全防护：分析 Web 应用、主机设备等的访问流量，实现 Web 应用攻击防护、非授权访问防护、恶意代码防护、邮件安全防护、网页防篡改等功能，形成行为信息、告警信息；
k) 终端访问控制：通过终端访问控制规则对终端操作和访问行为进行管控，形成行为信息、告警信息。终端操作和访问行为包括且不限于网络访问、文件访问、系统指令访问、进程创建、移动存储介质访问、办公设备访问等；
l) 终端入侵防护：通过获取终端行为、系统日志或其他终端上的信息，发现违反安全策略的行为并加以阻断，形成行为信息、告警信息；
m) 终端防病毒：在终端设备上实现的恶意代码防范功能，形成行为信息、告警信息；
n) 终端行为控制：依据访问控制规则对终端操作和访问行为进行控制，终端操作和访问行为包括但不限于网络访问、文件访问、系统指令访问、进程创建、移动存储介质访问、办公设备访问等，形成行为信息、告警信息。

4.2.1.3 监测功能

监测功能通过持续监测目标网络与系统，发现网络安全事件并触发预警或响应。监测功能主要包括：
a) 入侵检测：通过嗅探网络流量、行为、安全日志及其他相关信息，分析计算终端和网络资源的恶意使用行为，包括但不限于入侵行为、非授权访问等，形成行为信息、告警信息，处理后形成事件信息；

b) 高级持续性威胁（APT）检测：通过技术手段检测或监视高级持续性威胁，包括但不限于未知恶意代码检测、嵌套式攻击检测、木马蠕虫病毒检测、隐蔽信道检测等，形成行为信息、告警信息，处理后形成事件信息；
c) 终端安全检测：对受保护终端的终端进程、流量特征、文件、系统性能等进行监测，发现安全风险，形成行为信息、告警信息，处理后形成事件信息；
d) 域名解析安全监测：对域名系统（Domain Name System，DNS）节点上的流量进行监测，发现因拒绝服务攻击等造成的域名异常，形成行为信息、告警信息，处理后形成事件信息；
e) 用户与实体行为监测：采用规则匹配、安全基线、机器学习等方式，监测、分析用户与实体的异常行为，形成行为信息、告警信息，处理后形成事件信息；
f) 网络行为监测：监控网络流量，采用深度检测等技术发现因拒绝服务攻击、恶意程序等造成的网络异常行为，形成行为信息或告警信息，处理后形成事件信息；
g) 互联网信息监测：通过互联网信息采集技术、智能处理技术等对互联网信息进行汇集、分类、整合、筛选，实现对互联网信息收集与整理。形成行为信息、告警信息，处理后形成事件信息；
h) 安全审计：记录并存储网络、软硬件及其组件的活动，产生各类审计日志，包括但不限于主机审计日志、网络审计日志、数据库审计日志、应用审计日志、运维审计日志等，形成行为信息、告警信息、威胁信息，处理后形成事件信息。

4.2.1.4 处置功能

处置功能是发现网络安全事件、安全威胁等情况时，通过相应的响应手段应对网络安全风险，减缓网络安全事件带来的影响。处置功能主要包括：

a) 事件自动化处置：通过漏洞加固、封堵 IP、自动化编排等方式，对安全分析结果进行自动化应用、联动处置；
b) 攻击抑制：采用病毒查杀、进程终止、蜜罐诱捕等方式，对攻击流量和可疑行为进行阻断、限制；
c) 备份恢复：基于已备份的信息，实现对业务系统数据和功能的恢复；
d) 通报预警：对监测过程中获取的行为信息、脆弱性信息、事件信息、威胁信息等在一定范围内进行预警或告知，形成告警信息和威胁信息；
e) 攻击溯源：通过对攻击信息片段进行综合分析和场景还原，重构攻击者的攻击路径、攻击手法、攻击意图等，形成事件信息。

4.2.2 功能接口

功能接口从通信协议、请求方式和安全机制等方面指导互联互通功能的实现。通信协议主要包括Syslog、Kafka、Http(s)等。请求方式主要包括请求参数格式、请求报文结构、响应参数数据格式等。安全机制主要包括认证过程、认证参数、加密方式等。

4.3 互联互通信息

4.3.1 信息类型

4.3.1.1 行为信息

行为信息通过直接记录原始数据或采用审计日志的方式，描述安全域内终端、网络环境中的各类行为活动的信息。行为信息主要包括：

a) 终端行为信息：包括但不限于系统日志、第三方终端监控日志；

b) 网络行为信息：包括但不限于各类网络协议日志。

4.3.1.2 告警信息

告警信息是网络安全产品依据设定的规则或模型，对采集到的网络安全信息自动进行规则匹配、归并、分析等活动后产生的风险警示信息。告警信息主要包括：

a) 恶意程序告警信息：包括但不限于计算机病毒告警、网络蠕虫告警、特洛伊木马告警、僵尸网络告警、恶意代码内嵌网页告警、勒索软件告警和挖矿软件告警等信息；
b) 网络攻击告警信息：包括但不限于网络扫描探测告警、网络钓鱼告警、漏洞利用告警、后门利用告警、凭据攻击告警、拒绝服务告警、网页篡改告警、失陷主机告警和 APT 告警等信息；
c) 数据安全告警信息：包括但不限于数据篡改告警、数据泄露告警等信息；
d) 异常行为告警信息：包括但不限于访问异常告警、流量异常告警等信息；
e) 其他不能归为以上 4 类的网络安全告警信息。

4.3.1.3 资产信息

资产信息是实现网络安全产品互联互通时所使用的资产信息，包括但不限于硬件设备、业务系统、操作系统、数据库、中间件、应用软件等。

4.3.1.4 脆弱性信息

脆弱性信息是描述可能被一个或多个威胁利用的资产或控制弱点的信息。脆弱性信息主要涉及系统软件、应用中间件、应用系统等，按照GB/T 30279-2020 第5章进行分类，包括但不限于代码问题信息、配置错误信息等。

4.3.1.5 威胁信息

威胁信息是一种基于证据的知识,用于描述现有或可能出现的威胁,从而实现对威胁的响应和预防。威胁信息可分为域名类、IP类和文件类，威胁信息的要素包括但不限于网络安全事件、攻击指标、攻击方法、攻击活动等。

4.3.1.6 事件信息

事件信息是由于自然或人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的描述。事件信息按照GB/T 20986-2023的5.2进行分类。

4.3.2 信息描述

信息描述对互联互通信息内容和信息格式进行规范。互联互通信息内容包括各类信息的通用内容和扩展内容，信息格式包括字段名称、字段类型、字段取值、字段说明等。

附 录 A
（资料性）
网络安全产品互联互通典型应用场景

A.1 概述

互联互通应用场景包括两类。

一是安全管理系统（如网络安全态势感知平台、安全编排自动化与响应平台、安全信息和事件管理平台和安全运营中心等）与网络安全产品互联互通，是目前互联互通的主要应用场景。这类场景中，不同网络安全产品通过与安全管理平台的信息交互，支撑安全管理平台开展网络安全事件的分析和处置。

二是不同安全产品（不包括安全管理系统）之间的互联互通，此类场景在实际应用中相对较少，典型应用如防火墙与相关网络安全产品互联互通。

A.2 安全管理系统与网络安全产品互联互通

安全管理系统和网络安全产品互联互通可以实现互联互通功能的灵活调度，提升安全自动化响应与处置效能，见图A.1。

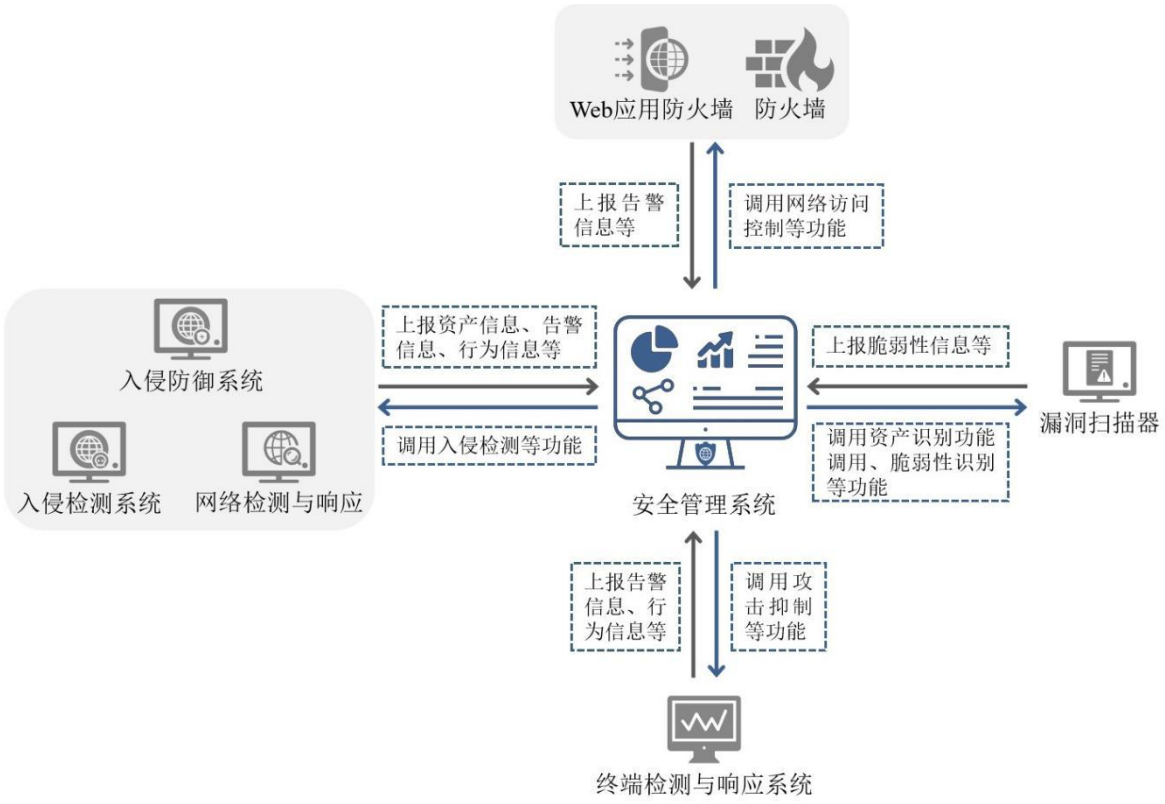

图 A.1 安全管理系统与网络安全产品互联互通示意图

a) 数据采集场景。安全管理系统与网络安全产品通过数据接口进行数据采集，主要包括资产信息、告警信息、脆弱性信息、行为信息等，具体如下：

1) 资产信息可通过入侵检测系统、入侵防御系统、网络检测与响应等获取，上报的资产信息内容包括但不限于资产标识、资产名称等；

2) 告警信息可通过 Web 应用防火墙、防火墙、入侵检测系统、入侵防御系统、网络检测与响应、终端检测与响应系统等获取，上报的告警信息内容包括但不限于告警时间、告警等级等；
3) 脆弱性信息可通过漏洞扫描器获取，上报的脆弱性信息内容包括但不限于代码问题信息、配置错误信息等。
4) 行为信息可通过入侵检测系统、入侵防御系统、网络检测与响应、终端检测与响应系统获取，上报的行为信息内容包括但不限于系统日志等。

b) 联动处置场景。以安全管理系统为中心，通过联动处置接口，可实现防火墙网络访问控制等功能调用，漏洞扫描器的资产识别、脆弱性识别等功能调用，终端检测与响应系统的攻击抑制等功能调用，入侵检测系统、入侵防御系统、网络检测与响应等安全监测产品的入侵检测等功能调用。

A.3 防火墙与相关网络安全产品互联互通

在划定的安全域中，防火墙作为部署在网络边界侧的网络安全访问控制产品，可接收不同类型网络安全设备上报的行为信息和告警信息，通过调整防火墙的访问控制策略，及时处置网络攻击。

防火墙可与漏洞扫描器、终端检测与响应系统、数据泄露防护系统和入侵检测系统等网络安全产品互联互通，获取资产信息、脆弱性信息、行为信息、告警信息等信息，及时调整防火墙访问控制策略，实现对网络攻击的阻断。见图A.2。

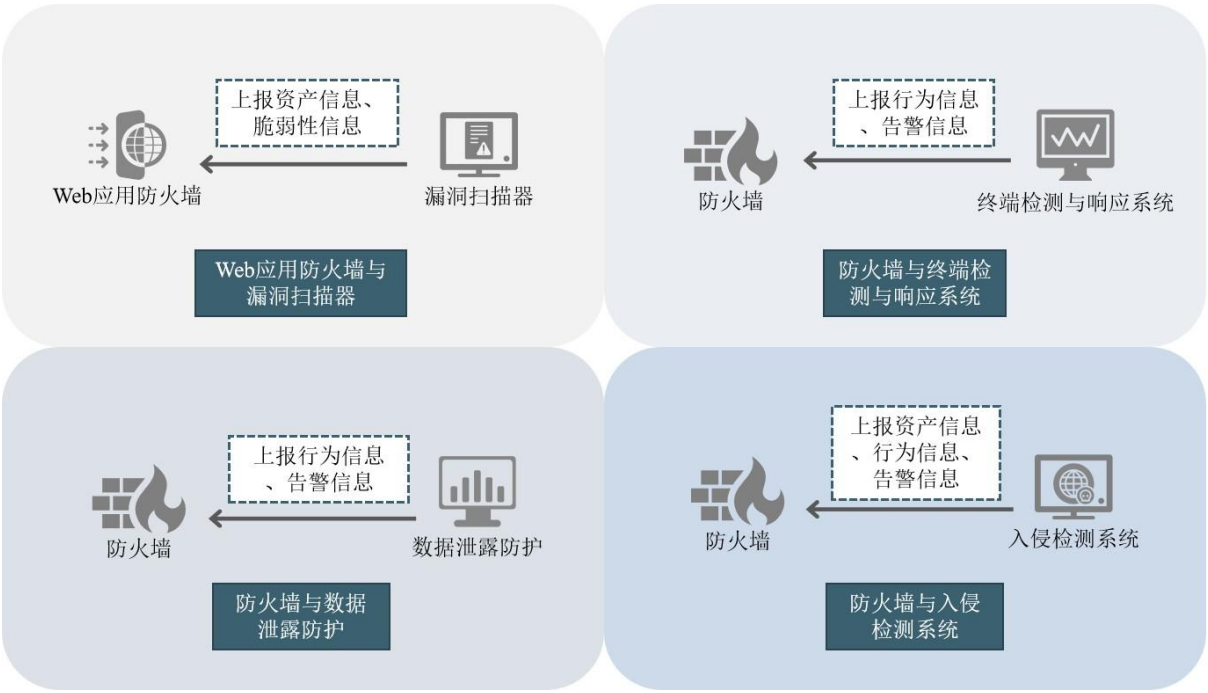

图 A.2 防火墙与相关网络安全产品互联互通示意图

a) Web 应用防火墙与漏洞扫描器产品互联互通场景。漏洞扫描器对目标资产进行脆弱性扫描，并将扫描结果反馈给 Web 应用防火墙。Web 应用防火墙根据获取的资产信息和脆弱性信息，更新并应用新的访问控制策略；
b) 防火墙与终端检测与响应系统互联互通场景。防火墙从终端检测与响应系统获取终端的安全状态，并根据接收到的行为信息和告警信息调整防火墙的访问控制策略，控制存在安全风险的终端网络访问行为；

c) 防火墙与数据防泄露系统互联互通场景。数据防泄露系统识别敏感数据异常访问行为，将需要阻断的数据访问行为生成行为信息和告警信息上报给防火墙；防火墙根据数据防泄露系统上报的信息，更新访问控制策略，并阻断相应数据访问行为；

d) 防火墙与入侵检测系统互联互通场景。入侵检测系统检测到网络攻击行为时，收集网络攻击相关的资产信息、行为信息和告警信息，并将相关信息上报给部署在网络出入口处的防火墙，由防火墙根据上报信息生成对应的网络访问控制规则，从而实现对网络攻击事件的及时阻断或限流。

附 录 B
（资料性）
互联互通功能使用的互联互通信息

网络安全产品互联互通功能输入/输出的互联互通信息内容见表B.1。

表 B.1 互联互通功能使用的互联互通信息

互联互通功能类型	互联互通功能子类	输入信息类型	输出信息类型
识别功能	资产识别	行为信息	资产信息
	脆弱性识别	行为信息、威胁信息	脆弱性信息
	威胁识别	资产信息、行为信息、告警信息、威胁信息、事件信息、脆弱性信息	威胁信息
	网络流量采集	—	行为信息
	终端信息采集	—	行为信息
防护功能	身份管理与鉴别	资产信息、行为信息	行为信息、告警信息
	网络访问控制	行为信息、告警信息、脆弱性信息、威胁信息、事件信息	行为信息、告警信息
	网络入侵防御	行为信息、告警信息、脆弱性信息、威胁信息、事件信息	行为信息、告警信息
	网络隔离交换	行为信息、告警信息、脆弱性信息、威胁信息、事件信息	行为信息、告警信息
	网络行为控制	行为信息、告警信息、脆弱性信息、威胁信息、事件信息	行为信息、告警信息
	网络流量控制	行为信息、告警信息、威胁信息、事件信息	行为信息、告警信息
	拒绝服务攻击防护	行为信息、告警信息、威胁信息、事件信息	行为信息、告警信息
	数据库防护	资产信息、行为信息、脆弱性信息、威胁信息、事件信息	行为信息、告警信息
	恶意代码防范	告警信息、威胁信息、事件信息	行为信息、告警信息
	应用安全防护	行为信息、告警信息、脆弱性信息、威胁信息、事件信息	行为信息、告警信息
	终端访问控制	行为信息、告警信息、威胁信息、事件信息	行为信息、告警信息
	终端入侵防护	行为信息、告警信息、威胁信息、事件信息	行为信息、告警信息
	终端防病毒	行为信息、告警信息、威胁信息、事件信息	行为信息、告警信息
	终端行为控制	行为信息、告警信息、威胁信息、事件信息	行为信息、告警信息
监测功能	入侵检测	行为信息、威胁信息、资产信息、事件信息	行为信息、告警信息、事件信息
	高级持续性威胁检测	行为信息、威胁信息、资产信息、事件信息	行为信息、告警信息、事件信息
	终端安全检测	行为信息、威胁信息、资产信息、事件信息	行为信息、告警信息、事件信息
	域名解析安全监测	行为信息、威胁信息、资产信息、事件信息	行为信息、告警信息、事件信息
	用户与实体行为监测	行为信息、威胁信息、资产信息、事件信息	行为信息、告警信息、事件信息
	网络行为监测	行为信息、威胁信息、资产信息、事件信息	行为信息、告警信息、事件信息
	互联网信息监测	行为信息、威胁信息、资产信息、事件信息	行为信息、告警信息、事件信息
	安全审计	行为信息、威胁信息、资产信息、事件信息	行为信息、告警信息、威胁信息、事件信息

表B.1　互联互通功能使用的互联互通信息（续）

互联互通功能类别	互联互通功能子类	输入信息类别	输出信息类别
处置功能	事件自动化处置	行为信息、告警信息、威胁信息、事件信息	—
	攻击抑制	行为信息、告警信息、威胁信息、事件信息	—
	备份恢复	行为信息、告警信息、威胁信息、事件信息	—
	通报预警	行为信息、脆弱性信息、威胁信息、事件信息	告警信息、威胁信息
	攻击溯源	行为信息、告警信息、威胁信息	事件信息

参 考 文 献

[1] GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范
[2] GB/T 28517-2012 网络安全事件描述和交换格式
[3] GB/T 36643-2018 信息安全技术 网络安全威胁信息格式规范
[4] GB/T 37027-2018 信息安全技术 网络攻击定义及描述规范