ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 44886.1—2024

网络安全技术　网络安全产品互联互通　第1部分：框架

Cybersecurity technology—Cybersecurity product interconnectivity—Part 1：Framework

2024-11-28 发布　　2025-06-01 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。

本文件是GB/T 44886《网络安全技术　网络安全产品互联互通》的第1部分。GB/T 44886已经发布了以下部分：

——第1部分：框架。

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专利的责任。

本文件由全国网络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、国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、中国科学院信息工程研究所、中国移动通信集团有限公司、北京大学、中国联合网络通信集团有限公司、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、赵新强、孙彦、许玉娜、刘蓓、李建强、陈韵然、姜政伟、邱勤、谢安明、王智明、王影新、严冬、孙凌、陈星、安高峰、何茂根、闫桂勋、卞建超、唐迪、孙可人、王西子、张卫博、姚叶鹏、李强、丁宇征。

引　言

近年来，国家网络安全相关法律法规、政策文件陆续出台，建立健全统一高效的网络安全风险监测、情报共享、研判处置机制，形成跨部门、跨行业高效联动的网络安全防护体系，已经成为筑牢国家网络安全屏障的工作重点。

网络安全产品互联互通是建设高效联动的网络安全防护能力的必要条件，标准化是实现网络安全产品互联互通的重要手段。GB/T 44886《网络安全技术　网络安全产品互联互通》是指导网络安全产品互联互通建设的基础性和通用性标准，拟由六个部分构成。

——第1部分：框架。目的在于明确网络安全产品互联互通应用场景，提出互通建设思路。

——第2部分：资产信息格式。目的在于提出网络安全产品互联互通时的资产描述。

——第3部分：告警信息格式。目的在于有效整合网络安全产品报送的告警信息，提高告警应急处置效率。

——第4部分：威胁信息格式。目的在于统一网络安全产品及各组织威胁信息共享格式。

——第5部分：行为信息格式。目的在于促进网络安全产品行为信息的分析利用。

——第6部分：功能接口。目的在于高效整合网络安全信息，促进网络安全产品功能协同。

网络安全技术　网络安全产品互联互通　第1部分：框架

1　范围

本文件确立了网络安全产品互联互通框架，给出了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　信息安全技术　信息安全产品类别与代码

3　术语和定义

GB/T 25066 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　cybersecurity product

专门用于保障网络安全的软件、硬件或其组合体。

3.2

网络安全产品互联互通　cybersecurity product interconnectivity

通过统一的网络安全信息描述和功能接口定义，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实现所提供数据的类型、结构和数据格式。

4　缩略语

下列缩略语适用于本文件。

APT：高级持续性威胁（Advanced Persistent Threat）

IP：互联网协议（Internet Protocol）

TCP：传输控制协议（Transmission Control Protocol）

WEB：万维网（World Wide Web）

5 互联互通框架

5.1 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，规范接口的接口协议、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，包括资产信息、脆弱性信息、威胁信息、行为信息、告警信息和事件信息。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接口实现示例。

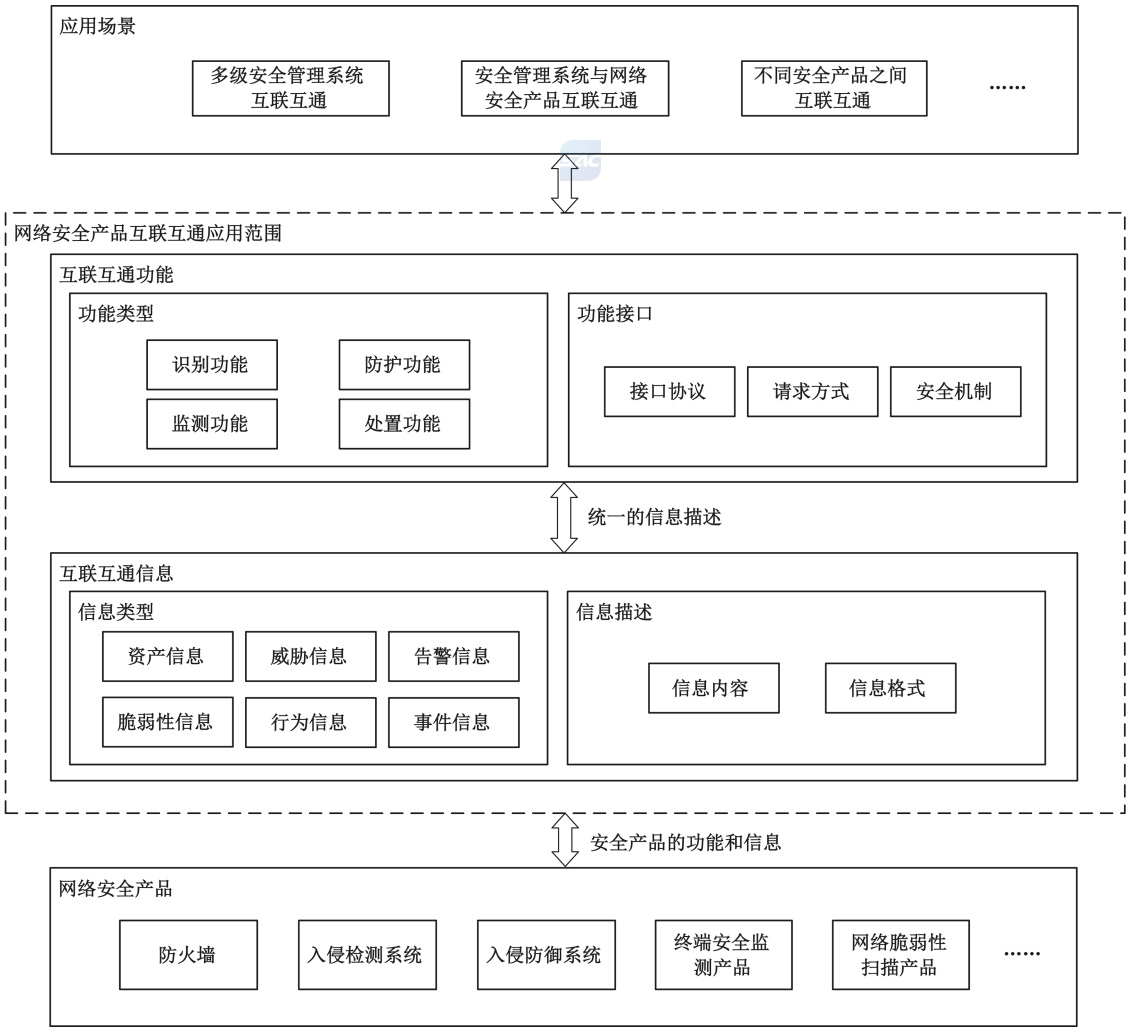


图1 网络安全产品互联互通框架

5.2 互联互通功能

5.2.1 功能类型

5.2.1.1 识别功能

识别功能通过对软硬件、网络流量等信息的采集与分析，形成资产信息、脆弱性信息、威胁信息、行为信息等。识别功能主要包括：

a） 资产识别：检查、发现网络、软硬件等资产，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） 行为识别：通过流量镜像、日志采集等方式，获取并记录网络、终端的行为，形成行为信息。

5.2.1.2 防护功能

防护功能通过实施防护措施，防范网络安全风险，形成行为信息、告警信息等。防护功能主要包括：

a） 身份管理与鉴别：标识和鉴别软硬件、网络等访问者身份的合法性，形成行为信息、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放行，形成行为信息、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、带宽限速等操作，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地址验证等方式，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：通过特征匹配、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、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理和控制，形成行为信息、告警信息；
l） 终端入侵防护：通过获取终端行为、系统日志等信息，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） 数据泄露防护：通过对终端和网络的监测，发现敏感信息非授权泄露，形成告警信息。

5.2.1.3 监测功能

监测功能通过持续监测目标网络与系统，发现网络安全风险，形成行为信息、告警信息。监测功能主要包括：

a） 入侵检测：通过采集网络流量、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；

b） 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，形成行为信息、告警信息；

c） 域名解析安全监测：对域名系统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；

d） 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；

注：实体是指网络中的各种硬件和软件，如服务器、数据库、应用程序等。

e） 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；

f） 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，形成行为信息、告警信息。

5.2.1.4 处置功能

处置功能是针对网络安全预警、网络安全事件等，采取相应的处置措施，应对潜在的网络安全风险，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：通过漏洞修复和安全加固、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） 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；

e） 通报预警：按照组织策略，就网络安全预警和网络安全事件进行通告。

5.2.2 功能接口

功能接口从接口协议、请求方式和安全机制等方面指导互联互通功能的实现。典型的接口协议包括Syslog、Kafka、HTTP（S）、FTP（SFTP）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。

5.3 互联互通信息

5.3.1 信息类型

5.3.1.1 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资产的基本信息、位置信息、网络信息和扩展信息，资产包括但不限于硬件设备、操作系统、数据库、中间件、应用软件、业务系统等。

5.3.1.2 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的弱点的信息，包括但不限于代码问题信息、配置错误信息等。

5.3.1.3 威胁信息

威胁信息是描述现有或可能出现的威胁的信息。威胁信息可分为域名类、IP类和文件类等，威胁信息的要素包括但不限于攻击指标、安全事件、攻击活动、威胁主体、攻击目标等。

5.3.1.4 行为信息

行为信息是从原始日志或审计日志中获取的，描述安全域内终端、网络环境中的各类行为活动的信息。行为信息主要包括终端行为信息、网络行为信息等。

5.3.1.5 告警信息

告警信息是描述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警示的信息。告警主要包括：

a） 恶意程序告警：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；

b） 网络攻击告警：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；

c） 数据安全告警：包括但不限于数据篡改告警、数据泄露告警等；

d） 异常行为告警：包括但不限于访问异常告警、流量异常告警等；

e） 其他不能归为以上4类的网络安全告警。

5.3.1.6 事件信息

事件信息是描述由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障等因素，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件的信息。事件类别应按GB/T 20986—2023的5.2划分，事件信息的要素包括但不限于事件类别、事件级别、事件时间、攻击者、受害者等。

5.3.2 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部分和专有部分，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

互联互通应用场景主要包括3类。

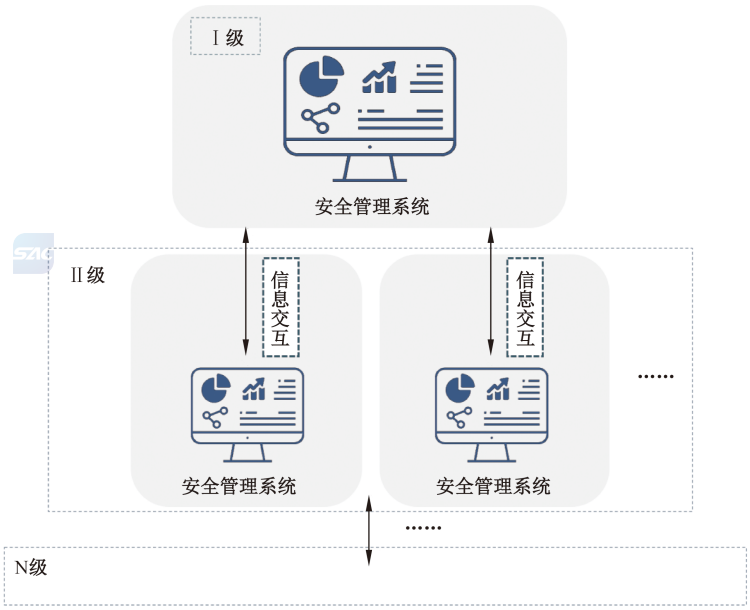
一是多级安全管理系统的互联互通。这类场景中，多级安全管理系统通过信息交互实现多级安全管理系统间的监测预警、应急响应、态势感知等应用。

二是安全管理系统（如网络安全态势感知产品、安全编排自动化与响应平台、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系统的信息交互，支撑安全管理系统开展网络安全事件的分析和处置。

三是不同网络安全产品（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　多级安全管理系统互联互通

多级安全管理系统互联互通可实现监测预警、应急响应、态势感知等应用场景。实现方法主要是上级安全管理系统向下级管理系统下发功能指令，下级安全管理系统根据接收到的指令，向上级管理系统上报资产信息、脆弱性信息、告警信息、事件信息等，见图A.1。



图A.1　多级安全管理系统互联互通示意图

A.3　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.2。

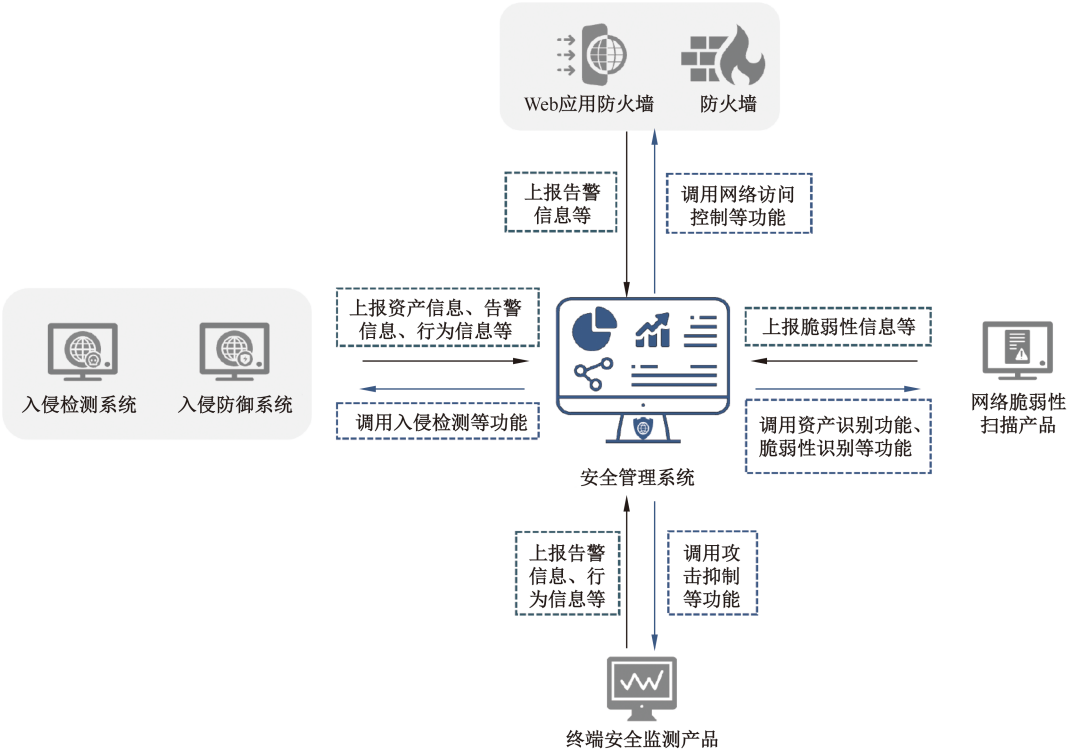


图 A.2　安全管理系统与网络安全产品互联互通示意图

主要应用场景包括如下场景。

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、终端安全监测产品等获取，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） 脆弱性信息可通过网络脆弱性扫描产品获取，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） 行为信息可通过终端安全监测产品等获取，上报的行为信息内容包括但不限于网络行为信息、终端行为信息等。

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，网络脆弱性扫描产品的资产识别、脆弱性识别等功能调用，终端安全监测产品的攻击抑制等功能调用，入侵防御系统等安全监测产品的入侵检测等功能调用。

A.4　不同网络安全产品之间互联互通

以防火墙为例，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产品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。

防火墙可与网络脆弱性扫描产品、终端安全监测产品、数据泄露防护产品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，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.3。

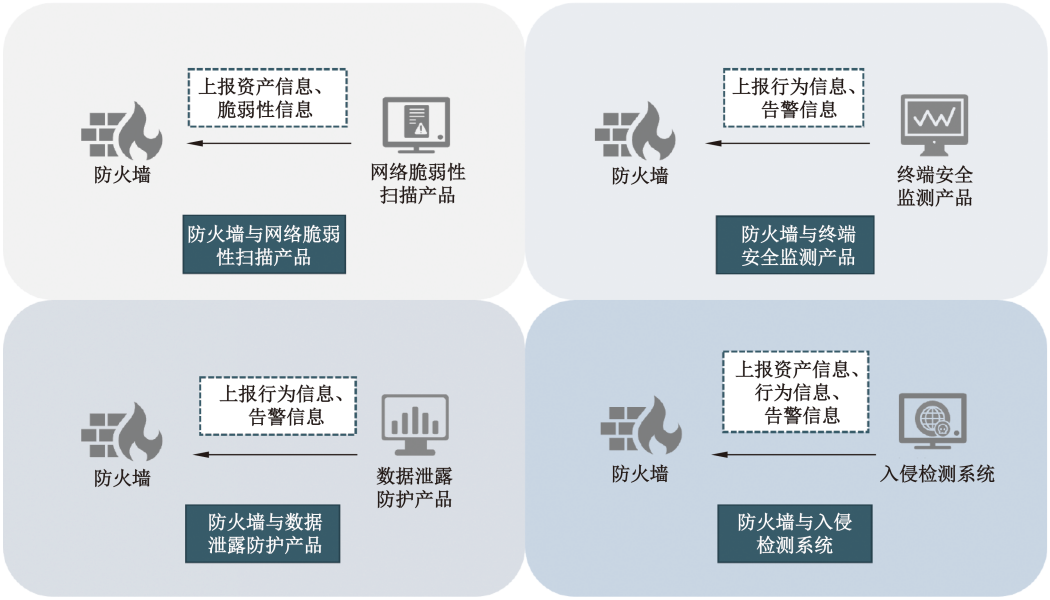


图 A.3　防火墙与相关网络安全产品互联互通示意图

主要应用场景包括如下场景。

a）防火墙与网络脆弱性扫描产品互联互通场景。网络脆弱性扫描产品对目标资产进行脆弱性扫描，并将扫描结果反馈给防火墙。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）防火墙与终端安全监测产品互联互通场景。防火墙从终端安全监测产品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）防火墙与数据泄露防护产品互联互通场景。数据泄露防护产品识别敏感数据的异常访问行为，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；防火墙根据数据泄露防护产品上报的信息，更新访问控制策略，并阻断相应的访问行为。

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策略，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）
互联互通功能接口实现示例

功能接口从接口协议、请求方式和安全机制等方面指导互联互通功能的实现。本附录给出了一种采用HTTP协议实现互联互通功能接口的典型方式，数据请求使用HTTP POST方式，编码格式为UTF-8，数据传输采用HTTPS加密协议，HTTP的请求报文体中约定互联互通功能的行为（action）、目标（target）和参数（args），参数属于可选项，根据不同的互联互通功能进行确定。表B.1针对互联互通功能类型给出了行为和目标及实现示例（JSON格式），不同互联互通功能接口的实现由行为和目标的组合完成。

表B.1 互联互通功能接口实现示例

序号	互联互通功能类型		行为	目标	示例
1	识别功能	资产识别	扫描：scan 状态查询：query	网络地址类：email_addr、uri、ipv4_net、ipv6_net 域名类：domain_name、idn_domain_name 设备类：device、mac_addr、interface	扫描ipv4地址识别资产： {"action": "scan", "target":{"ipv4_net":"198.2.3.4/24"}, "args":{"duration": 500}}
2		脆弱性识别	扫描：scan 状态查询：query	网络地址类：email_addr、uri、ipv4_net、ipv6_net 域名类：domain_name、idn_domain_name 设备类：device、mac_addr、interface	扫描域名识别脆弱性： {"action": "scan", "target":{"domain_name":"www.abcd.com"}, "args":{"vulnerability_library_template":vul_lib_tem001}}

表 B.1　互联互通功能接口实现示例（续）

序号	互联互通功能类型		行为	目标	示例
3	识别功能	威胁识别	扫描：scan 状态查询：query	网络地址类：email_addr、uri、ipv4_net、ipv6_net 域名类：domain_name、idn_domain_name 设备类：device、mac_addr、interface 网络连接类：ipv4_connection、ipv6_connection、sess_app、sess_tcp、sess_tcp_new、sess_tcp_num、sess_udp、sess_udp_new、sess_udp_num、vlan_id 文件、进程类：file、process、properties	扫描文件识别病毒威胁： {"action": "scan", "target":{"file":"filedirectory/filename.aaa"}, "args":{"threat_name": "Trojan/Generic.aiddi"}}
4		行为识别	扫描：scan 状态查询：query	网络地址类：email_addr、uri、ipv4_net、ipv6_net 网络连接类：ipv4_connection、ipv6_connection、sess_app、sess_tcp、sess_tcp_new、sess_tcp_num、sess_udp、sess_udp_new、sess_udp_num、vlan_id 域名类：domain_name、idn_domain_name 设备类：device、mac_addr、interface 文件、进程类：file、process、properties	扫描IPv4连接识别网络行为： {"action":"scan", "target":{"ipv4_connection":"198.2.3.4/24","198.2.4.5/24"}, "args":{"duration": 500}}

表 B.1　互联互通功能接口实现示例（续）

序号	互联互通功能类型		行为	目标	示例
5	防护功能	身份管理与鉴别	允许/阻断：allow、deny	设备类：device	对某一设备的下线： {"action": "deny", "target": {"device":{"device_ipv4": "10.1.1.2"}}
6		网络访问控制	允许/阻断：allow、deny 删除：delete	网络连接类：ipv4_connection、ipv6_connection 网络地址类：ipv4_net、ipv6_net、mac_addr、uri 域名类：domain_name、idn_domain_name	阻断某 ipv4 连接的网络访问： {"action": "deny", "target": {"ipv4_connection":{ "src_addr": "1.2.3.4/24", "dst_addr": "198.2.3.4", "src_port": 15943, "dst_port": 1521, "protocol": "tcp"}},"args": {"duration": 500,"direction": 0,"rule_id":"2738df11-7376-4f3b-a179-69b14f307 d25"}}
7		网络入侵防御	加入/删除白名单：create、delete	网络连接类：ipv4_connection、ipv6_connection 网络地址类：uri、rule_id	允许某一个白名单地址的访问： {"action": "ccreate", "target": {"ipv4_connection": {"src_addr": "1.2.3.4"}}, "args": {"duration": 5000, "rule_id": "2738df11-7376-4f3b-a179-69b14f307d25"}}
8		网络隔离交换	加入/删除白名单：create、delete	网络连接类：ipv4_connection、ipv6_connection	允许某一个白名单地址的访问： {"action": "create", "target":{"ipv4_connection": { "src_addr": "198.2.3.4", "src_port":1278, "dst_addr": "192.168.1.201", "dst_port": 80}}, "args":{"rule_id": "2738df11-7376-4f3b-a179-69b14f307d25"}}
9		网络行为控制	阻断/允许访问：deny、allow	网络连接类：ipv4_connection、ipv6_connection	阻断某一ipv4地址的访问行为： {"action":"deny", "target":{"ipv4_connection": {"src_addr": "1.2.3.4", "src_port":, "dst_addr":, "dst_port":}}}

表 B.1　互联互通功能接口实现示例（续）

序号	互联互通功能类型		行为	目标	示例
10	防护功能	网络流量控制	参数设置：set 行为管控： allow、deny、 redirect	网络连接类： sess_app、sess_tcp、 sess_udp、 sess_tcp_new、 sess_udp_new、 sess_tcp_num、 sess_udp_num 文件、进程类：artifact	设置TCP会话连接阈值： {"action": "set", "target":{"sess_tcp_num":"10000"}}
11		拒绝服务攻击防护	行为管控： allow、deny、 redirect	网络地址类：ipv4_net、 ipv6_net、uri 网络连接类： ipv4_connection、 ipv6_connection 规则类：rule	流量重定向： {"action": "redirect", "target":{"ipv4_net":"198.2.3.4/24"}}
12		数据库防护	行为管控： deny、allow 处置： investigate、 copy	网络地址类：ipv4_net、 ipv6_net、email_addr 网络连接类： ipv4_connection、 ipv6_connection 设备类：mobile db_object	风险告警： {"action": "investigate", "target":{"email_addr":"test@test.com"}}
13		恶意代码防范	状态查询： query 扫描：scan 行为管控： allow、deny 处置： remediate、 contain、 update、 detonate、 restore	网络地址类：ipv4_net、 ipv6_net、uri、 email_addr 网络连接： ipv4_connection、 ipv6_connection 域名类：domain_name 设备类：device、 features 文件、进程类：file、 properties	查询某IP的威胁IOC： {"action": "query", "target":{"ipv4_net":"198.2.3.4/24"}}
14		应用安全防护	行为管控： allow、deny、 redirect 处置： investigate、 restore、 contain、copy	网络地址类：ipv4_net、 ipv6_net、uri 网络连接类： ipv4_connection、 ipv6_connection 域名类：domain_name 设备类：device、artifact 文件、进程类：file	禁止某IP访问： {"action": "deny", "target": {"ipv4_net":"198.2.3.4/24"}}

表 B.1　互联互通功能接口实现示例（续）

序号	互联互通功能类型		行为	目标	示例
15	防护功能	终端访问控制	参数设置：set 行为管控：allow、deny	网络地址类：ipv4_net、ipv6_net、uri 网络连接类：ipv4_connection、ipv6_connection 设备类：mac_addr	禁止某IP访问： {"action": "deny", "target":{"ipv4_net":"198.2.3.4/24"}, "args": {"duration": 500}}
16		终端入侵防护	行为管控：allow、deny、redirect	文件、进程类：file、process 网络地址类：email_addr、uri、ipv4_net、ipv6_net、port 域名类：domain_name	结束指定终端上符合条件的进程： {"action":"deny", "target_count":1, "target":{"process":{"pid":512,"uuid":"","name":"example", "file":{…}}} "args":{"hostname":"1.1.1.1",} "actuator":{"hostname": "192.168.1.1","asset_id": ""}}
17		数据泄露防护	阻断/允许访问：deny、allow	网络连接类：ipv4_connection、ipv6_connection 网络地址类：ipv4_net、ipv6_net、uri 设备类：mac_addr	阻断某一ipv4地址的访问行为： {"action":"deny", "target":{"ipv4_connection": {"src_addr": "1.2.3.4", "src_port":, "dst_addr":, "dst_port":}}}
18	监测功能	入侵检测	开始检测：detect 停止检测：undetect	网络连接类：ipv4_connection、ipv6_connection 网络地址类：url 域名类：domain_name	检测ipv4网络连接： {"action":"detect", "target":{"ipv4_net":"192.168.1.0/24"}, "args":{"start_time":1534775460000, "duration":500 }}
19		终端安全检测	开始检测：detect 停止检测：undetect	网络连接类：ipv4_connection、ipv6_connection 文件、进程类：file、pcap_file、process	检测文件“3.txt”： {"action":"detect", "target":{"file":{"path":"ftp://192.168.0.8/3.txt"}},"args":{"start_time":1534775460000, "duration":500}}
20		域名解析安全监测	开始检测：detect 停止检测：undetect	网络地址类：ipv4_net、ipv6_net、url 域名类：domain_name	检测域名“www.explorer.com”： {"action": "detect", "target": {"domain_name ":"www.explorer.com"}}
21		用户与实体行为监测	开始检测：detect 停止检测：undetect	用户类：users 网络地址类：ipv4_net、ipv6_net、url 网络连接类：ipv4_connection、ipv6_connection	检测用户test01行为： {"action":"detect", "target":{"users":"test01"},"args":{"timeout": 500,"start_time":609434061000,"duration": 864000 }}

表 B.1　互联互通功能接口实现示例（续）

序号	互联互通功能类型		行为	目标	示例
22	监测功能	网络行为监测	开始检测： detect 停止检测： undetect	网络地址类：ipv4_net、 ipv6_net 网络连接类： ipv4_connection、 ipv6_connection 用户类：users	检测ipv4连接行为： {"action":"detect", "target":{"ipv4_net":"192.168.1.0/24"}, "args":{"start_time":1534775460000, "duration":500 }}
23		安全审计	开始检测： detect 停止检测： undetect	网络连接类： ipv4_connection、 ipv6_connection 用户类：users	审计ipv4连接： {"action": "detect", "target":{"ipv4_connection":"192.168.1.1:80"}, "args":{" start_time":1534775460000, "duration":500 }}
24	处置功能	事件自动化处置	处置： remediate、 deny、allow	网络地址类：ipv4_net、 ipv6_net、email_addr 设备类：mac_addr 网络连接类： ipv4_connection、 ipv6_connection	IP封堵： {"action": "deny", "target":{"ipv4_net":"198.2.3.4/24"}}
25		攻击抑制	处置：deny、 limit、 redirect、 allow、 unlimit、 unredirect、 restore	网络地址类：ipv4_net、 ipv6_net、uri 网络连接类： ipv4_connection、 ipv6_connection 文件、进程类：file、 process	攻击阻断： {"action": "deny", "target":{ipv4_connection: {"src_addr": "1.2.3.4/24"}}, "args":{"start_time":1534775460000,"duration": 500, "rule_id": "2738df11-7376-4f3b-a179-69b14f307d25"}}
26		备份恢复	处置：copy、 restore	文件、进程类： properties、file 设备类：device	快照恢复： {"action": "restore", "target":{"device": "22323-4343-323"}, "args":{"name":"22323-4343-323操作系统快照"}}
27		攻击溯源	处置：query、 copy	网络地址类： properties、ipv4_net、 ipv6_net 网络连接类： ipv4_connection、 ipv6_connection	攻击溯源： {"action":"query", "target":{"ipv4_net":"198.2.3.4"}}
28		通报预警	处置： investigate	文件、进程类： properties、artifact	通报下发： {"action":"investigate", "target":{"artifact":event_object}}

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 30279—2020 信息安全技术 网络安全漏洞分类分级指南
[4] GB/T 36643—2018 信息安全技术 网络安全威胁信息格式规范
[5] GB/T 37027—2018 信息安全技术 网络攻击定义及描述规范