ICS 35.030
CCS L 80

T/CCIA

中 国 网 络 安 全 产 业 联 盟 技 术 规 范

T/CCIA XXX—XXXX

网络安全技术 网络型防火墙互联互通接口内容和格式

Cybersecurity technology—Network-based firewall interface contents and format for interconnectivity

（征求意见稿）

2024/9/24

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国网络安全产业联盟　　发 布

单击或点击此处输入文字。

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。

本文件由中国网络安全产业联盟提出。

本文件由中国网络安全产业联盟归口。

本文件起草单位：北京天融信网络安全技术有限公司、北京赛西科技发展有限责任公司、国家信息中心、中国电子技术标准化研究院、中国科学院信息工程研究所、深信服科技股份有限公司、北京神州绿盟科技有限公司、杭州安恒信息技术股份有限公司、华为技术有限公司、启明星辰信息技术集团股份有限公司、北京升鑫网络科技有限公司、安天科技集团股份有限公司、北京山石网科信息技术有限公司、杭州迪普科技股份有限公司、新华三技术有限公司、中电科网络安全科技股份有限公司、长扬科技（北京）股份有限公司、天翼安全科技有限公司、南京众智维信息科技有限公司

本文件主要起草人：唐宁、许玉娜、安高峰、姜威、范鸿雷、黄雅静、晏尉、吴摇摇、赵新强、陈韵然、雷晓锋、王龑、张晓欣、隋鹤、李彦峰、闫桂勋、姚叶鹏、孙凌、王彦磊、何茂根、陈星、田丽丹、颜磊、胡月、蒋发群、卞建超、张宁、付巍、徐强、万晓兰、邹大均、赵华、康和、车洵、冯冲等。

网络安全技术 网络型防火墙互联互通接口内容和格式

1 范围

本文件规定了网络型防火墙产品实现互联互通的接口内容和格式。

本文件适用于指导网络型防火墙产品互联互通的设计、开发、应用和测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 20281-2020 信息安全技术 防火墙安全技术要求和测试评价方法

GB/T 25069-2022 信息安全技术 术语

GB/T AAAAA.1-20XX 网络安全技术 网络安全产品互联互通 第1部分：框架

GB/T AAAAA.2-20XX 网络安全技术 网络安全产品互联互通 第2部分：资产信息格式

GB/T AAAAA.3-20XX 网络安全技术 网络安全产品互联互通 第3部分：告警信息格式

3 术语和定义

GB/T 20281和GB/T 25069-2022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。

3.2

防火墙 firewall

对经过的数据流进行解析，并实现访问控制及安全防护功能的网络安全产品。

[来源：GB/T 20281-2020，3.1]

3.3

网络型防火墙 network-based firewall

部署于不同安全域之间，对经过的数据流进行解析，具备网络层、应用层访问控制及安全防护功能的网络安全产品。

[来源：GB/T 20281-2020，3.2]

4 概述

网络型防火墙产品可以通过与安全管理系统互联互通，实现安全信息的及时上报和安全功能的灵活调度，提升安全自动化响应与处置效能。

在划定的安全域中，网络型防火墙作为部署在网络边界侧的网络安全访问控制产品，可以与漏洞扫描器、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，通过调整防火墙访问控制策略，实现对网络攻击的及时处置。

如图1所示，网络型防火墙与安全管理系统及其它网络安全产品互联互通的信息主要包括告警信息，互联互通的功能包括网络访问控制策略和基础资源对象配置策略。

网络型防火墙产品互联互通的通信接口见附录A。

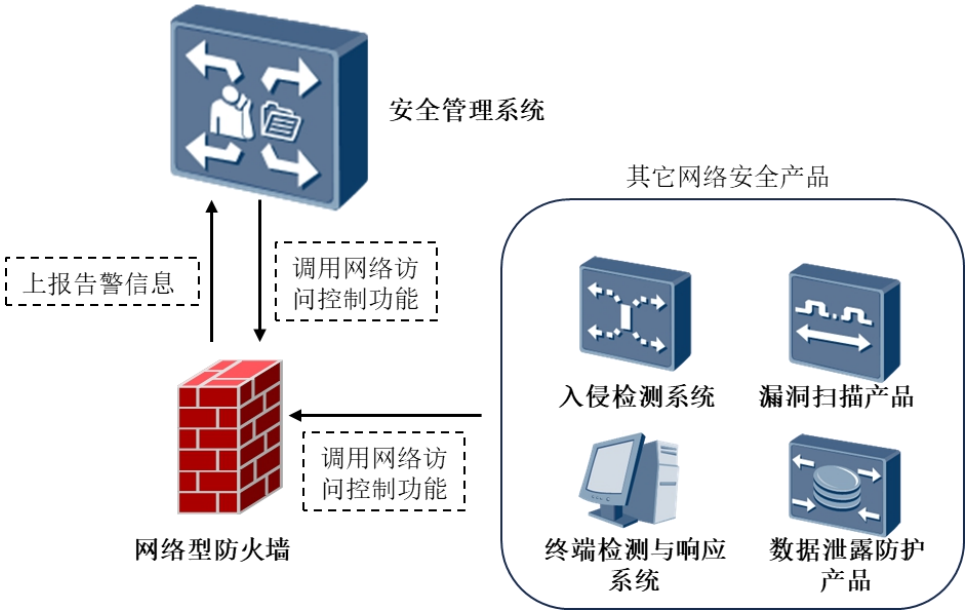

图 1 网络型防火墙产品互联互通示意图

5 字段类型取值

数据类型的取值见表1。

表 1 数据类型的取值

字段类型	说明
字符型	以字符包括字母、数字、汉字和其他字符形式表达的数据元值的类型。
整型	以任意实数表达的数据元值的类型。
日期时间型	以格式为“yyyy-mm-dd hh:mm:ss”的形式表达的数据元值的类型。
枚举	预定义列出所有的值，该类型取值只限于列举出来的值

6 网络型防火墙报送的信息内容和格式

6.1 告警信息

6.1.1 告警通用信息

告警通用信息见表2。

表 2 告警通用信息

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	告警时间	alarmTime	告警发生时间	日期时间型	是
2	告警等级	alarmLevel	1-低危 2-中危 3-高危	整型	是
3	告警名称	alarmName	告警信息名称	字符型	是
4	告警描述	alarmDesc	对告警的详细描述、说明	字符型	是
5	告警类型	alarmCategory	1-恶意程序告警，2-网络攻击告警，3-数据安全告警，4-异常行为告警，5-其他告警	整型	是
6	告警子类	alarmSubCategory	告警子类，参考 GB/T AAAAA.3-20XX 附录 B	字符型	是
7	产品类型	devType	网络安全产品类型参考 GB/T AAAAA.3-20XX 附录 C	字符型	是
8	产品地址	devIp	网络安全产品 IP 地址	字符型	是
9	受害对象 IP	victimIP	受害对象的 IP 地址，支持 ipv4、ipv6 格式，可对应防火墙安全策略中的目的 IP	字符型	是
10	受害对象端口	victimPort	受害对象的端口 对应防火墙安全策略中的目的端口	字符型	是
11	是否加密	encryption	告警所采集的网络安全信息是否加密，1-非加密，2-加密	整型	否
12	产品型号	devID	网络安全产品硬件型号	字符型	否
13	产品版本	devVer	网络安全产品软件版本	字符型	否
14	产品厂商	devVenodor	网络安全产品厂家名称	字符型	否
15	告警所属网络	alarmArea	告警所属的网络区域，如互联网、内网等	字符型	否
16	源 IP	sourceIP	对受害对象发起攻击或访问的 IP 地址，支持 ipv4、ipv6 格式	字符型	否
17	源端口	sourcePort	对受害对象发起攻击或访问的的端口	字符型	否
18	协议	protocol	承载的传输层协议或应用层协议	字符型	否
19	状态	state	攻击是否成功的状态，1-失败,2-成功,3-尝试，4-未知	字符型	否
20	是否上报	report	告警信息是否需要上报有关主管部门，1-需要,2-不需要	字符型	否
21	操作	oper	动作描述；中文：允许、阻断；英文：accept、deny	字符型	是
22	扩展字段	external	在完整告警信息之后可增加自定义扩展字段	字符型	否

6.1.2 访问控制告警信息

访问控制告警信息见表3。

表3 访问控制告警信息

序号	信息项	字段名称	字段说明	数据类型	是否必选
1	策略 ID	policyId	命中的访问控制策略 ID	字符型	否
2	策略名称	policyName	命中的访问控制策略名	字符型	是
3	传输层协议	proto4	传输层协议，取值如：ICMP，IGMP，GGP，IP in IP，TCP，UDP，HMP，RDP，RSVP，GRE，ESP，AH，NARP，IPv6-ICMP，IPv6-NoNxt，IPv6-Opts，OSPF，VRRP，L2TP,ISIS,CRTP,CRUDP,SCTP,UDPLite,MPLS-in-IP,Other；	字符型	是
4	应用层协议	proto7	应用协议名称	字符型	否

表3 访问控制告警信息（续）

序号	信息项	字段名称	字段说明	数据类型	是否必选
5	账号	account	用户名	字符型	否

7 网络型防火墙接收的功能内容和格式

7.1 内容概述

网络型防火墙互联互通的功能主要包括基础资源对象配置策略（地址策略、服务策略、区域策略），见表6至表12，和访问控制策略，见表13。

其中，访问控制策略中的部分字段依赖于基础资源对象。

7.2 基础资源对象配置策略

7.2.1 地址策略

表6 主机地址策略

序号	信息项	字段名称	字段描述和要求	数据类型	是否必选
1	对象名	name	对象名称	字符型	是
2	IP 地址	ipAddr	支持 IPV4 IPV6，示例如下： IPV4：x.x.x.x 或 IPV6：xx:xx:xx:xx:xx:xx:xx:xx	字符型	否

表7 地址范围策略

序号	信息项	字段名称	字段说明描述和要求	数据类型	是否必选
1	对象名	name	对象名称	字符型	是
2	第一个 IP 地址	ip1	支持 IPV4 IPV6，格式如下 IPV4：x.x.x.x 或 IPV6：xx:xx:xx:xx:xx:xx:xx:xx	字符型	否
3	最后一个 IP 地址	ip2	支持 IPV4 IPV6，格式如下 IPV4：x.x.x.x 或 IPV6：xx:xx:xx:xx:xx:xx:xx:xx	字符型	否
4	要排除的地址	except	支持 IPV4 IPV6，格式如下 IPV4：x.x.x.x 或 IPV6：xx:xx:xx:xx:xx:xx:xx:xx	字符型	否

表8 子网地址策略

序号	信息项	字段名称	字段说明描述和要求	数据类型	是否必选
1	对象名	name	对象名称	字符型	是
2	IP 地址	ipAddr	支持 IPV4 IPV6，格式如下 IPV4：x.x.x.x/x 或 IPV6：xxxx::xxxx/x”	字符型	否
3	要排除的地址	except	支持 IPV4 IPV6，格式如下 IPV4：x.x.x.x 或 IPV6：xx:xx:xx:xx:xx:xx:xx:xx	字符型	否

表9 MAC地址策略

序号	信息项	字段名称	字段说明描述和要求	数据类型	是否必选
1	对象名	name	对象名称	字符型	是
2	mac 地址	macAddr	例 AA:BB:CC:DD:EE:FF	字符型	否

表10 地址组策略

序号	信息项	字段名称	字段说明描述和要求	数据类型	是否必选
1	对象名	name	对象名称	字符型	是
2	对象地址组	member	主机、子网或者范围对象地址组	字符型	否

7.2.2 服务策略

表11 服务策略

序号	信息项	字段名称	字段说明描述和要求	数据类型	是否必选
1	服务名	name	服务名称	字符型	是
2	协议号	protocol	支持三层协议，例如 TCP、UDP、ICMP 或者填写协议号	字符型	是
3	端口范围	ports	ICMP 协议仅支持单端口配置，且配置端口范围 0-18，示例：3-0，其中 3 为类型值，0 为代码值； 其他协议均支持多端口配置，且配置端口范围 0-65535，示例：0-1023 或 80。	字符型	否

7.2.3 区域策略

表12 区域策略

序号	信息项	字段名称	字段说明描述和要求	数据类型	是否必选
1	区域名	name	区域名称	字符型	是
2	接口	interface	区域对象接口	字符型	否

7.3 网络访问控制策略

表13 网络访问控制策略

序号	信息项	字段名称	字段说明	字段类型	是否必填
1	策略名字	name	策略名称	字符型	是
2	策略描述	comment	对策略的描述	字符型	否
3	动作	action	策略的动作，选项为 accept|deny，分别标识允许|阻断	枚举	是
4	生效开关	enable	生效开关，默认为开，选项为 yes|no，分别标识开、关	枚举	是
5	日志开关	log	日志开关，默认为关，选项为 on|off，分别标识开、关	枚举	是
6	源 ip 对象标识	srcIp	源 ip 对象标识	字符型	否
7	目的 ip 地址对象标识	dstIp	目的 ip 地址对象标识	字符型	否
8	源端口对象标识	srcPort	源端口对象标识	字符型	否
9	服务对象标识	service	服务对象标识	字符型	否
10	源区域对象标识	srcArea	源区域对象标识	字符型	否
11	目的区域对象标识	dstArea	目的区域对象标识	字符型	否
12	地址转换前的目标地址对象标识	origDst	地址转换前的目标地址对象标识	字符型	否

附录 A
（规范性）
防火墙互联互通通信接口

A.1 防火墙互联互通上报信息通信接口

防火墙产品应支持通过接口上报互联互通信息。

A.2 防火墙互联互通下发功能通信接口

防火墙产品应通过接口接收互联互通的功能。

A.2.1 通信协议

防火墙产品通信接口和数据传输应采用统一的加密协议。当使用HTTPS协议时，应通过POST/GET/PUT/DELETE方式进行数据请求，编码格式统一为UTF-8，说明如下：

POST方法：新建操作时使用；

GET方法：查询及批量查询时使用；

PUT方法：修改及更新操作时使用；

DELETE方法：删除操作时使用。

本协议规约不改变现有HTTP标准的定义，实现者可以充分利用开发语言的HTTP工具包进行扩充。

A.2.2 请求 URL 结构

请求URL通信规约结构定义见下图。

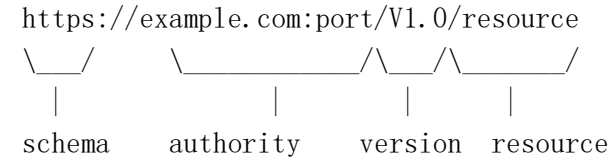

图 A.1 请求 URL 通信规约结构定义图

请求URL字段定义见下表。

表A.1 请求URL字段定义表

字段	说明
schema	本文件规定 schema 采用 https
authority	提供 API 服务的主机名称（或 ip）以及端口
version	版本号
resource	操作的资源路径

参考文献

[1] GB/T 13000-2010 信息技术 通用多八位编码字符集（UCS）
[2] RFC 2616 超文本传输协议1.1（Hypertext Transfer Protocol--HTTP/1.1 ）
[3] RFC 4627 JSON应用与媒体类型[The application/json Media Type for JavaScript Object Notation (JSON]