(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109962903 A
(43)申请公布日 2019.07.02

(21)申请号 201711435195.2

(22)申请日 2017.12.26

(71)申请人 中移(杭州)信息技术有限公司
地址 311100 浙江省杭州市余杭区文一西路998号海创园18幢6层
申请人 中国移动通信集团公司

(72)发明人 黄一鸣

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 郭润湘

(51)Int.Cl.
H04L 29/06(2006.01)

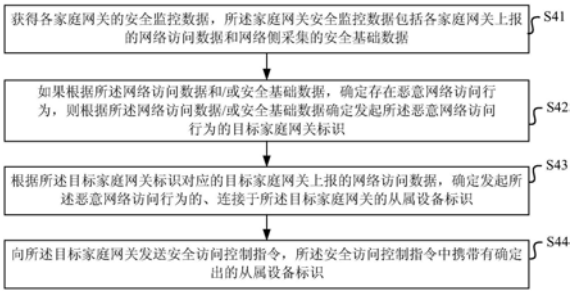
权利要求书4页 说明书18页 附图6页

(54)发明名称

一种家庭网关安全监控方法、装置、系统和介质

(57)摘要

本发明公开了一种家庭网关安全监控方法、装置、系统和介质，用以提高家庭网关安全监控的精确性。所述家庭网关安全监控方法，包括：获得各家庭网关的安全监控数据，家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据；如果根据网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识；并根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识；向目标家庭网关发送安全访问控制指令，其中携带有确定出的从属设备标识。



CN 109962903 A

1.一种家庭网关安全监控方法,其特征在于,包括:

获得各家庭网关的安全监控数据,所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据;

如果根据所述网络访问数据和/或安全基础数据,确定存在恶意网络访问行为,则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识;并

根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据,确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识;

向所述目标家庭网关发送安全访问控制指令,所述安全访问控制指令中携带有确定出的从属设备标识。

2.如权利要求1所述方法,其特征在于,所述网络访问数据包括以下至少一项:域名系统DNS解析请求数据和统一资源定位符URL访问数据;所述安全基础数据包括以下至少一项:网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

3.如权利要求2所述的方法,其特征在于,所述恶意网络访问行为包括异常流量攻击行为;以及

根据所述Netflow流量数据,按照以下流程判断是否存在异常流量攻击行为:

针对采集的Netflow流量数据中包含的目的互联网协议IP地址,统计在预设时长内去向该目的IP地址的第一网络流量;

如果所述第一网络流量超过动态流量阈值,则以所述预设时长为单位持续统计多个时段的第二网络流量;

如果各个统计时段的第二网络流量与所述第一网络流量的差值绝对值不超过预设流量阈值且持续时长超过预设时长阈值且持续时长超过预设时长阈值,则确定存在异常流量攻击行为,否则,确定不存在异常流量攻击行为。

4.如权利要求3所述的方法,其特征在于,如果确定存在异常流量攻击行为,则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识,具体包括:

根据存在异常流量攻击行为对应的目的IP地址,从采集的Netflow流量数据中查找该目的IP地址对应的源IP地址;

确定查找到的源IP地址为发起所述异常流量攻击行为的目标家庭网关标识;以及

根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据,确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识,具体包括:

根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据,确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

5.如权利要求2所述的方法,其特征在于,所述恶意网络访问行为包括恶意URL访问行为,所述威胁情报数据中包含有恶意URL列表;以及

根据所述URL访问数据,按照以下流程判断是否存在恶意URL访问行为:

查询各家庭网关上报的URL访问数据包含的URL是否存在于所述URL列表中;

如果是,则确定存在恶意URL访问行为,否则,确定不存在恶意URL访问行为。

6.如权利要求5所述的方法，其特征在于，如果确定存在恶意URL访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识，具体包括：

从存在恶意URL访问行为的家庭网关上报的DNS解析请求数据和URL访问数据中，查找发起请求的家庭网关IP地址和请求时间；

根据采集的NAT日志数据，确定发起恶意URL访问行为的实际IP地址；

根据所述RADIUS日志数据，确定所述实际IP地址的登录时间和退出时间；

如果发起请求的家庭网关IP地址与所述实际IP地址相同且所述请求时间位于所述登录时间和退出时间之间，则确定所述RADIUS日志数据对应的用户账号对应的家庭网关介质访问控制MAC地址为发起所述恶意网络访问行为的目标家庭网关标识；以及

根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识，具体包括：

根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

7.如权利要求1～6任一权利要求所述的方法，其特征在于，所述安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

8.一种家庭网关安全监控方法，其特征在于，包括：

向安全监控平台上报网络访问数据；

接收所述安全监控平台下发的安全访问控制指令，所述安全访问控制指令中携带有控制网络访问的从属设备标识，其中，所述安全访问控制指令为所述安全监控平台根据所述网络访问数据和/或采集的安全基础数据确定出存在恶意网络访问行为时下发的；

根据所述安全访问控制指令，对所述从属设备标识对应的从属设备的网络访问操作进行控制。

9.如权利要求8所述的方法，其特征在于，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一资源定位符URL访问数据；所述安全基础数据包括以下至少一项：网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

10.如权利要球8或9所述的方法，其特征在于，所述安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

11.一种家庭网关安全监控装置，其特征在于，包括：

获得单元，用于获得各家庭网关的安全监控数据，所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据；

第一确定单元，用于如果根据所述网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识；

第二确定单元，用于根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识；

发送单元，用于向所述目标家庭网关发送安全访问控制指令，所述安全访问控制指令

中携带有确定出的从属设备标识。

12.如权利要求11所述的装置，其特征在于，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一资源定位符URL访问数据；所述安全基础数据包括以下至少一项：网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

13.如权利要求12所述的装置，其特征在于，所述恶意网络访问行为包括异常流量攻击行为；以及

所述装置，还包括：

第三确定单元，用于针对采集的Netflow流量数据中包含的目的互联网协议IP地址，统计在预设时长内去向该目的IP地址的第一网络流量；如果所述第一网络流量超过动态流量阈值，则以所述预设时长为单位持续统计多个时段的第二网络流量；如果各个统计时段的第二网络流量与所述第一网络流量的差值绝对值均不超过预设流量阈值，则确定存在异常流量攻击行为，否则，确定不存在异常流量攻击行为。

14.如权利要求13所述的装置，其特征在于，

所述第一确定单元，具体用于根据存在异常流量攻击行为对应的目的IP地址，从采集的Netflow流量数据中查找该目的IP地址对应的源IP地址；确定查找到的源IP地址为发起所述异常流量攻击行为的目标家庭网关标识；

所述第二确定单元，具体用于根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

15.如权利要求12所述的装置，其特征在于，所述恶意网络访问行为包括恶意URL访问行为，所述威胁情报数据中包含有恶意URL列表；以及

所述装置，还包括：

第四确定单元，用于查询各家庭网关上报的URL访问数据包含的URL是否存在于所述URL列表中；如果是，则确定存在恶意URL访问行为，否则，确定不存在恶意URL访问行为。

16.如权利要求15所述的装置，其特征在于，

所述第一确定单元，具体用于从存在恶意URL访问行为的家庭网关上报的DNS解析请求数据和URL访问数据中，查找发起请求的家庭网关IP地址和请求时间；根据采集的NAT日志数据，确定发起恶意URL访问行为的实际IP地址；根据所述RADIUS日志数据，确定所述实际IP地址的登录时间和退出时间；如果发起请求的家庭网关IP地址与所述实际IP地址相同且所述请求时间位于所述登录时间和退出时间之间，则确定所述RADIUS日志数据对应的用户账号对应的家庭网关介质访问控制MAC地址为发起所述恶意网络访问行为的目标家庭网关标识；

所述第二确定单元，具体用于根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

17.如权利要求11～16任一权利要求所述的装置，其特征在于，所述安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

18.一种家庭网关安全监控装置,其特征在于,包括:

上报单元,用于向安全监控平台上报网络访问数据;

接收单元,用于接收所述安全监控平台下发的安全访问控制指令,所述安全访问控制指令中携带有控制网络访问的从属设备标识,其中,所述安全访问控制指令为所述安全监控平台根据所述网络访问数据和/或采集的安全基础数据确定出存在恶意网络访问行为时下发的;

控制单元,用于根据所述安全访问控制指令,对所述从属设备标识对应的从属设备的网络访问操作进行控制。

19.如权利要求18所述的装置,其特征在于,所述网络访问数据包括以下至少一项:域名系统DNS解析请求数据和统一资源定位符URL访问数据;所述安全基础数据包括以下至少一项:网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

20.如权利要求18或19所述的装置,其特征在于,所述安全访问控制指令包括以下任一项:网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

21.一种家庭网关安全监控系统,其特征在于,包括家庭网关和安全监控平台,其中所述家庭网关中设置有权利要求18、19或20所述的家庭网关安全监控装置;所述安全监控平台中设置有权利要求11～17任一权利要求所述的家庭网关安全监控装置。

22.一种计算装置,包括至少一个处理单元、以及至少一个存储单元,其中,所述存储单元存储有计算机程序,当所述程序被所述处理单元执行时,使得所述处理单元执行权利要求1～10任一权利要求所述方法的步骤。

23.一种计算机可读介质,其存储有可由计算装置执行的计算机程序,当所述程序在计算装置上运行时,使得所述计算装置执行权利要求1～10任一所述方法的步骤。

一种家庭网关安全监控方法、装置、系统和介质

技术领域

[0001] 本发明涉及计算机网络技术领域，尤其涉及一种家庭网关安全监控方法、装置、系统和介质。

背景技术

[0002] 本部分旨在为权利要求书中陈述的本发明的实施方式提供背景或上下文。此处的描述不因为包括在本部分中就承认是现有技术。

[0003] 目前，家庭宽带业务正逐步向智能化、物联网化方向发展，以智能家庭网关为核心，通过物联网技术将家中的各种设备连接，提供家电控制、防盗报警、环境监测等多种功能，并通过与云端业务系统的紧密结合，建立起人、家庭设备与网络的家庭物联生态。家庭宽带网络的发展带来了便捷的服务和应用，但同时伴随而来的还有日益严峻的网络安全形势：多层面的网络安全威胁和安全风险不断增加，网络病毒、Dos(拒绝服务攻击)/DDos(分布式拒绝服务攻击)攻击等构成的威胁和损失越来越大，网络攻击行为向着分布化、规模化、复杂化等趋势发展，曾经爆发的miria攻击导致北美网络瘫痪的安全事件，更是引起了全球范围内对物联网设备安全的广泛担忧，作为物联网生态中的重要一环，针对家庭宽带网络的安全防护也格外重要。

[0004] 现有针对家庭宽带网络的安全防护手段，仍采用传统单一的网络安全检测和防护技术。在网络接入侧部署防火墙设备，保障安全域的划分及隔离；使用入侵检测系统，对家庭宽带网络中的攻击行为进行监测；使用防病毒系统，做到对家庭宽带网络中的僵木蠕等恶意程序的及时发现。除了传统的安全防护手段外，也采用拨测或设备认证的方式对网关设备及相关网元做全面的资产核查，确保在网设备资产清晰、配置合规、无可利用的漏洞等；使用异常流量监测系统及异常流量清洗设备，对家庭宽带网络中存在的恶意攻击流量进行有效的发现和清洗，保证家庭宽带网络性能稳定，正常流量不受影响。上述现有的安全防护措施，多为家庭宽带网络运营商在网络侧部署的安全防护系统，实现了对家庭宽带网络层面的有效防护。

[0005] 在家庭宽带网络侧部署的安全防护手段，保障了家庭宽带网络的基本安全需求，但在安全事件监控及安全事件处置上仍存在一定的不足。例如，家庭宽带网络侧只能够监控到智能网关一级，对于智能网关下挂的各类智能家居设备无法监控，因此在发现安全事件并定位到某个网关时，只能对整个网关的整体流量及行为进行处置，而真正的威胁实际存在于某个下挂设备从而导致的攻击，其他设备及网关本身并未受到威胁，因此一刀切的处置方式，也会影响到网关及其他下挂设备的正常使用，需要一个更加细粒度的监控和处置手段。

[0006] 因此，如何提高家庭网关安全监控的精确性成为现有技术中亟待解决的技术问题之一。

发明内容

[0007] 本发明实施例提供一种家庭网关安全监控方法、装置、系统和介质，用以提高家庭网关安全监控的精确性。

[0008] 第一方面，提供一种家庭网关安全监控方法，包括：

[0009] 获得各家庭网关的安全监控数据，所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据；

[0010] 如果根据所述网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识；并

[0011] 根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识；

[0012] 向所述目标家庭网关发送安全访问控制指令，所述安全访问控制指令中携带有确定出的从属设备标识。

[0013] 可选地，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一资源定位符URL访问数据；所述安全基础数据包括以下至少一项：网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

[0014] 可选地，所述恶意网络访问行为包括异常流量攻击行为；以及

[0015] 根据所述Netflow流量数据，按照以下流程判断是否存在异常流量攻击行为：

[0016] 针对采集的Netflow流量数据中包含的目的互联网协议IP地址，统计在预设时长内去向该目的IP地址的第一网络流量；

[0017] 如果所述第一网络流量超过动态流量阈值，则以所述预设时长为单位持续统计多个时段的第二网络流量；

[0018] 如果各个统计时段的第二网络流量与所述第一网络流量的差值绝对值不超过预设流量阈值且持续时长超过预设时长阈值，则确定存在异常流量攻击行为，否则，确定不存在异常流量攻击行为。

[0019] 可选地，如果确定存在异常流量攻击行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识，具体包括：

[0020] 根据存在异常流量攻击行为对应的目的IP地址，从采集的Netflow流量数据中查找该目的IP地址对应的源IP地址；

[0021] 确定查找到的源IP地址为发起所述异常流量攻击行为的目标家庭网关标识；以及

[0022] 根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识，具体包括：

[0023] 根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

[0024] 可选地，所述恶意网络访问行为包括恶意URL访问行为，所述威胁情报数据中包含有恶意URL列表；以及

[0025] 根据所述URL访问数据，按照以下流程判断是否存在恶意URL访问行为：

[0026] 查询各家庭网关上报的URL访问数据包含的URL是否存在于所述URL列表中；

[0027] 如果是，则确定存在恶意URL访问行为，否则，确定不存在恶意URL访问行为。

[0028] 可选地，如果确定存在恶意URL访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识，具体包括：

[0029] 从存在恶意URL访问行为的家庭网关上报的DNS解析请求数据和URL访问数据中，查找发起请求的家庭网关IP地址和请求时间；

[0030] 根据采集的NAT日志数据，确定发起恶意URL访问行为的实际IP地址；

[0031] 根据所述RADIUS日志数据，确定所述实际IP地址的登录时间和退出时间；

[0032] 如果发起请求的家庭网关IP地址与所述实际IP地址相同且所述请求时间位于所述登录时间和退出时间之间，则确定所述RADIUS日志数据对应的用户账号对应的家庭网关介质访问控制MAC地址为发起所述恶意网络访问行为的目标家庭网关标识；以及

[0033] 根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识，具体包括：

[0034] 根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

[0035] 可选地，所述安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

[0036] 第二方面，提供一种家庭网关安全监控方法，包括：

[0037] 向安全监控平台上报网络访问数据；

[0038] 接收所述安全监控平台下发的安全访问控制指令，所述安全访问控制指令中携带有控制网络访问的从属设备标识，其中，所述安全访问控制指令为所述安全监控平台根据所述网络访问数据和/或采集的安全基础数据确定出存在恶意网络访问行为时下发的；

[0039] 根据所述安全访问控制指令，对所述从属设备标识对应的从属设备的网络访问操作进行控制。

[0040] 可选地，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一资源定位符URL访问数据；所述安全基础数据包括以下至少一项：网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

[0041] 可选地，所述安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

[0042] 第三方面，提供一种家庭网关安全监控装置，包括：

[0043] 获得单元，用于获得各家庭网关的安全监控数据，所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据；

[0044] 第一确定单元，用于如果根据所述网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识；

[0045] 第二确定单元，用于根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识；

[0046] 发送单元，用于向所述目标家庭网关发送安全访问控制指令，所述安全访问控制指令中携带有确定出的从属设备标识。

[0047] 可选地，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一

资源定位符URL访问数据;所述安全基础数据包括以下至少一项:网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

[0048] 可选地,所述恶意网络访问行为包括异常流量攻击行为;以及

[0049] 所述装置,还包括:

[0050] 第三确定单元,用于针对采集的Netflow流量数据中包含的目的互联网协议IP地址,统计在预设时长内去向该目的IP地址的第一网络流量;如果所述第一网络流量超过动态流量阈值,则以所述预设时长为单位持续统计多个时段的第二网络流量;如果各个统计时段的第二网络流量与所述第一网络流量的差值绝对值均不超过预设流量阈值,则确定存在异常流量攻击行为,否则,确定不存在异常流量攻击行为。

[0051] 可选地,所述第一确定单元,具体用于根据存在异常流量攻击行为对应的目的IP地址,从采集的Netflow流量数据中查找该目的IP地址对应的源IP地址;确定查找到的源IP地址为发起所述异常流量攻击行为的目标家庭网关标识;

[0052] 所述第二确定单元,具体用于根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据,确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

[0053] 可选地,所述恶意网络访问行为包括恶意URL访问行为,所述威胁情报数据中包含有恶意URL列表;以及

[0054] 所述装置,还包括:

[0055] 第四确定单元,用于查询各家庭网关上报的URL访问数据包含的URL是否存在于所述URL列表中;如果是,则确定存在恶意URL访问行为,否则,确定不存在恶意URL访问行为。

[0056] 可选地,所述第一确定单元,具体用于从存在恶意URL访问行为的家庭网关上报的DNS解析请求数据和URL访问数据中,查找发起请求的家庭网关IP地址和请求时间;根据采集的NAT日志数据,确定发起恶意URL访问行为的实际IP地址;根据所述RADIUS日志数据,确定所述实际IP地址的登录时间和退出时间;如果发起请求的家庭网关IP地址与所述实际IP地址相同且所述请求时间位于所述登录时间和退出时间之间,则确定所述RADIUS日志数据对应的用户账号对应的家庭网关介质访问控制MAC地址为发起所述恶意网络访问行为的目标家庭网关标识;

[0057] 所述第二确定单元,具体用于根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据,确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

[0058] 可选地,所述安全访问控制指令包括以下任一项:网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

[0059] 第四方面,提供一种家庭网关安全监控装置,包括:

[0060] 上报单元,用于向安全监控平台上报网络访问数据;

[0061] 接收单元,用于接收所述安全监控平台下发的安全访问控制指令,所述安全访问控制指令中携带有控制网络访问的从属设备标识,其中,所述安全访问控制指令为所述安全监控平台根据所述网络访问数据和/或采集的安全基础数据确定出存在恶意网络访问行为时下发的;

[0062] 控制单元，用于根据所述安全访问控制指令，对所述从属设备标识对应的从属设备的网络访问操作进行控制。

[0063] 可选地，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一资源定位符URL访问数据；所述安全基础数据包括以下至少一项：网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

[0064] 可选地，所述安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

[0065] 第五方面，提供一种家庭网关安全监控系统，包括家庭网关和安全监控平台，其中所述家庭网关中设置有上述第四方面中所述的家庭网关安全监控装置；所述安全监控平台中设置有上述第三方面中所述的家庭网关安全监控装置。

[0066] 第六方面，提供一种计算装置，包括至少一个处理单元、以及至少一个存储单元，其中，所述存储单元存储有计算机程序，当所述程序被所述处理单元执行时，使得所述处理单元执行上述任一权利要求所述的步骤。

[0067] 第七方面，提供一种计算机可读介质，其存储有可由计算装置执行的计算机程序，当所述程序在计算装置上运行时，使得所述计算装置执行上述任一权利要求所述的步骤。

[0068] 本发明实施例提供的家庭网关安全监控方法、装置、系统和介质，网络侧的安全监控平台获得各家庭网关上报的网络访问数据和自身采集的安全基础数据；通过对各家庭网关上报的网络访问数据和自身采集的安全基础数据进行分析，最终溯源至家庭网关下挂的从属设备，从而实现了对家庭网关下挂从属设备网络行为的进一步精准监控，将攻击威胁监测及处置进一步下沉，避免因为处置网关攻击导致下挂从属设备无法进行网络访问，极大的提高了威胁处置粒度，从而提高了家庭网关安全监控的精确性。

[0069] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0070] 此处所说明的附图用来提供对本发明的进一步理解，构成本发明的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0071] 图1为根据本发明实施方式的网关安全插件的部署示意图；

[0072] 图2为本发明实施例中，安全监控平台采集安全监控数据的示意图；

[0073] 图3为本发明实施例中，家庭网关安全监控系统的结构示意图；

[0074] 图4为本发明实施例中，安全监控平台侧实施的家庭网关安全监控方法的实施流程示意图；

[0075] 图5为本发明实施例中，异常流量攻击行为检测流程示意图；

[0076] 图6为本发明实施例中，恶意URL访问行为检测流程示意图；

[0077] 图7为本发明实施例中，家庭网关侧实施的家庭网关安全监控方法的实施流程示意图；

[0078] 图8为本发明实施例中，安全监控平台侧实施的家庭网关安全监控装置的结构示

意图；

[0079] 图9为本发明实施例中，家庭网关侧实施的家庭网关安全监控装置的结构示意图；

[0080] 图10为根据本发明实施方式的计算装置的结构示意图。

具体实施方式

[0081] 为了提高家庭网关安全监控的精确性，本发明实施例提供了一种家庭网关安全监控方法、装置、系统和介质。

[0082] 发明人发现，在家庭宽带网络侧部署的安全防护手段，保障了家庭宽带网络的基本安全需求，但在安全事件监控及安全事件处置上仍存在一定的不足。例如，家庭宽带网络侧资产核查只能够监控到智能网关一级，对于智能网关下挂的各类智能家居设备无法监控，因此在发现安全事件并定位到某个网关时，只能对整个网关的整体流量及行为进行处置，而真正的威胁实际存在于某个下挂设备从而导致的攻击，其他设备及网关本身并未受到威胁，因此一刀切的处置方式，也会影响到网关及其他下挂设备的正常使用，需要一个更加细粒度的监控和处置手段。传统的入侵检测及防病毒系统，只能够对家庭宽带网络中海量的上网行为进行监控，从中发现恶意行为，而由于网关请求在经过家庭宽带网络并从出口路由出网时经过了多次地址转换，因此即使发现了恶意行为也无法在网络侧定位到具体用户，因此定位溯源手段的缺失，导致在发现恶意行为后，在网络侧也无法针对威胁用户进行安全处置。对于利用智能网关及下挂设备发起的针对某个特定目标的DDoS攻击，家庭宽带网络侧配置有流量检测设备及流量清洗设备，然而同样是无法定位具体网关的原因，流量清洗只能使用针对去往攻击目标的异常流量清洗方式，对全量的访问流量进行清洗，一方面该处置流程较为复杂，需要网络侧多个网元进行配合，成本较高，另一方面清洗流量的手段过于集中，且对所以去往目标地址的流量进行清洗，对于性能影响较大，效果并非最佳。家庭宽带网络中的安全防护设备及手段相互独立、功能单一，无法发现对于做了有效隐蔽手段的安全攻击，同时在安全事件发生时，也无法做到有效的功能联动，对安全事件进行及时的处置。

[0083] 有鉴于此，本发明实施例提供了一种家庭网关安全监控方法，充分利用网关侧安全数据及网络侧流量及日志数据，针对上述传统安全防护手段中的不足，设计了一套有针对性的解决智能家庭网关安全威胁的安全监控及处置系统，主要解决的问题包括：

[0084] 1、利用智能网关安全插件，实现对网关本身及下挂设备的信息获取，同时对流经网关的所有网络访问行为进行监控，可详细的获取网关及下挂设备的网络访问记录，为细粒度访问控制建立数据基础。

[0085] 2、统一收集家庭宽带网络侧Radius认证数据、NAT地址转换日志，结合发现的安全威胁网关地址，实现对安全事件发生网关的精准溯源，并还原网关对应的用户信息，从而可及时定位受害用户并发送通知提醒。

[0086] 3、结合多协议异常流量分析及网关精确溯源，不仅实现对DDoS攻击流量的追踪以及对发起攻击网关甚至下挂设备的精准定位，同时结合智能网关安全插件，对发起DDoS攻击的网关及下挂设备进行针对性的阻断及限速，通过处置能力下沉，实现DDoS攻击威胁在家庭宽带网络中的精确处置。

[0087] 4、通过多级设备进行联动，在终端和网络侧多个环节对发现的安全威胁进行拦截

处置,有效加强安全威胁处置力度,提高安全威胁处置效率。

[0088] 以下结合说明书附图对本发明的优选实施例进行说明,应当理解,此处所描述的优选实施例仅用于说明和解释本发明,并不用于限定本发明,并且在不冲突的情况下,本发明中的实施例及实施例中的特征可以相互组合。

[0089] 家庭网关安全监控系统主要包括家庭网关和安全监控平台,其中,家庭网关中设置有家庭网关安全监控装置,其可以以网关安全插件方式部署于家庭网关中,网关安全插件和安全监控平台分别收集家庭网关侧的安全数据并进行综合分写,并使用自身及联动各类设备对安全威胁进行处置。

[0090] 目前,主流的智能家庭网关多采用嵌入式的Linux操作系统,且在系统上层部署OSGI(Open Service Gateway Initiative,开放服务网关协议)框架容器作为上层应用的服务中间件,通过OSGI容器,上层插件应用可获取到很多家庭网关设备信息及行为信息,同时提供控制网关设备的命令接口,网关安全插件便是使用OSGI框架提供的信息查询及指令接口,实现其网关信息采集及威胁处置的功能。如图1所示,其为网关安全插件的部署示意图。

[0091] 具体实施时,网关安全插件主要功能包括:

[0092] (1)网络访问数据收集

[0093] 网关安全插件主要通过两个OSGI开放的接口进行数据的采集:

[0094] 一、数据流镜像服务类(TrafficMirrorService)接口

[0095] 通过该接口,网关安全插件能够以镜像报文的方式获得家庭网关及所有下挂从属设备的DNS(域名系统)解析请求数据,采集到的参数可以但不限于包括:

[0096] 请求解析时间(Timestamp);

[0097] 网关内网IP地址(Gateway IP);

[0098] 网关MAC(Gateway MAC);

[0099] 下挂的从属设备内网IP地址(Subdevice IP);

[0100] 下挂的从属设备MAC地址(Subdevice MAC);

[0101] 请求解析DNS地址的域名(Dns);

[0102] DNS解析出的IP地址(Dst IP)。

[0103] 每条信息的报文格式如表1所示:

[0104] 表1

[0105]

Timestamp	Gateway IP	Gateway MAC	Subdevice IP	Subdevice MAC	Dns	Dst IP

[0106] 二、数据流精细处理服务类(TrafficDetailProcessService)接口

[0107] 通过该接口,可获得网关及所属下挂设备的URL访问数据,网关将抓取的内容通过系统消息通知到网关安全插件,能过采集到的参数可以但不限于包括:

[0108] 请求解析时间(Timestamp);

[0109] 访问URL的具体请求信息(Url);

[0110] URL对应的域名信息(Referer);

[0111] 响应状态(StatusCode)。

[0112] 每条消息的报文格式如表2所示：

[0113] 表2

[0114]

Timestamp	URL	Referer	StatusCode

[0115] 通过这两个osgi采集到的网络访问数据，即可关联分析出在具体时间，具体的网关及下挂设备发起的针对指定URL(统一资源定位符)及域名的访问请求，从而做到准确的上网行为数据定位。由于网关安全插件性能有限，关联分析工作不在插件上进行，这两部分信息，统一由网关通过UDP(用户数据包)包的方式，上传到安全监控平台进行接收、整理及关联分析，最终得出不同网关的上网行为。

[0116] 安全监控平台部署在云端，通过收集家庭网关侧上传的网络访问数据及在网络侧的流量及日志数据，实现对安全威胁的实时判定及准确溯源，同时对具备威胁特性的家庭网关及下挂的从属设备进行处置。

[0117] 其中，安全监控平台主要收集4类现网产生的数据，并引入外部情报数据：

[0118] 1)网关上网行为数据：主要收集上述提到的网关DNS解析数据及网关URL访问数据。

[0119] 2)Netflow流量数据：从BRAS(Broadband Remote Access Server，宽带远程接入服务器)接入设备或上层核心路由设备中抽样采集Netflow流量数据，能够根据每条Netflow日志分析出流量的源、目的走向及相关信息，具体信息主要包括：

[0120] 流量起始时间(Start Time)；

[0121] 源IP(Src IP)；

[0122] 源端口(Src Port)；

[0123] 目的IP(Dst IP)；

[0124] 目的端口(Dst Port)；

[0125] 协议类型(Proto)；

[0126] 传输包大小(Bytes Sent)。

[0127] Netflow流量日志格式如表3所示：

[0128] 表3

[0129]

Start Time	Src IP	Src Port	Dst Ip	Dst Port	Proto	Bytes Sent

[0130] 3)RADIUS日志数据：用户在宽带网络上线后，RADIUS会认证其账号登录信息，并在其通过认证后为该家庭网关分配内网地址，公网地址及可使用的端口段，家庭网关向外的访问会话都会通过该公网IP及随机端口与远端目的平台进行通信。安全监控平台采集该部分数据，从而可以实现对用户账号的精确溯源，RADIUS日志数据如表3所示。

[0131] 表3

[0132]

时间	账号	MAC	用户 IP	Online/ Offline	BAS_IP	AAA_server	NAT 公网 IP	开始端口	结束端口
20150417 15001	138XXX XXXXX	—	10.230.9 .142	Online	211.143. 228.46	192.168. 210.133	112.24. 194.172	47392	48399
20150417 150001	139XXX XXXXX	—	10.230.2 06.232	Offline	211.143. 228.46	192.168. 210.133	112.24. 194.29	27232	28239

[0133] 4)NAT地址转换日志数据:在家庭网关对外访问的上网行为时,每个会话都会基于网关的公网地址以及从端口段中为其分配一个随机端口,目的平台接收到访问请求后也会根据该公网地址及端口响应访问信息。整个过程为NAT地址转换,地址转换的日志会被保存,安全监控平台通过采集这部分数据实现对内网网关的分析溯源。

[0134] NAT转换关系如表4所示:

[0135] 表4

[0136]

私网 IP	私网端口	源公网 IP	源公网端口	目的 IP	目的端口	时间	未使用字段	持续时间
172.27.162.39	45863	118.212.213.110	29666	110.75.114. 7	80	2015-6-11 14:48:55	0	60
172.16.51.188	50905	118.212.215.245	23733	163.177.89 .180	8080	2015-6-11 14:48:55	0	60
172.22.45.33	47556	118.212.219.92	9067	220.248.19 2.13	53	2015-6-11 14:48:55	0	60

[0137] 5)威胁情报数据:从外部引入恶意IP、恶意域名的威胁情报库,安全监控平台通过与用户访问行为中的域名及IP进行对比,从而发现网关用户是否有访问恶意域名,从而判断是否有感染恶意程序的风险。

[0138] 安全监控平台通过对以上五类信息的采集分析处理,从而在网络中监测两类主要安全威胁:

[0139] 1)异常流量攻击溯源检测:通过对netflow流量日志中时间、地址、及包大小等信息,可检测出异常的流量特征,并结合NAT日志根据发起源从而定位具体的流量发起网关,从而全流程还原出异常流量的变化。

[0140] 2)恶意程序感染溯源检测:通过将用户上网行为中的域名及IP与威胁情报库中的恶意域名与IP进行比对,从而发现恶意的访问行为,并确定是否已经感染恶意程序,同时结合RADIUS及NAT日志,实现对感染网关及用户的准确溯源及定位。

[0141] 具体实施时,安全监控平台可以按照预设的采集周期分别采集Netflow流量数据、RADIUS(远程用户拨号认证系统)日志数据、NAT(网络地址转换)地址转换日志数据和威胁情报数据等,各类数据的采集周期可以相同,也可以不同,本发明实施例对此不进行限定。

[0142] 如图2所示,其为安全监控平台采集安全监控数据的示意图。

[0143] 安全监控平台对发现的威胁行为，定位到具体的网关及下挂从属设备进行处置指令的下发，网关安全插件收到处置指令之后，对网关及下挂从属设备进行相关限速、限制等操作。

[0144] 本发明实施例中，通过部署于家庭网关中的网关安全插件和安全监控平台的联动，实现了威胁信息的采集分析以及家庭网关及其下挂从属设备的联动处置，如图3所示，其为本发明实施例提供的家庭网关安全监控系统的结构示意图，包括安全监控平台31和部署了网关安全插件的家庭网关31。

[0145] 基于图3所示的家庭网关安全监控系统，本发明实施例提供了一种安全监控平台实施的家庭网关安全监控方法，如图4所示，可以包括以下步骤：

[0146] S41、获得各家庭网关的安全监控数据，所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据。

[0147] 具体实施时，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一资源定位符URL访问数据；所述安全基础数据包括以下至少一项：网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

[0148] S42、如果根据所述网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识。

[0149] S43、根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

[0150] S44、向所述目标家庭网关发送安全访问控制指令，所述安全访问控制指令中携带有确定出的从属设备标识。

[0151] 其中，恶意网络访问行为包括异常流量攻击行为和恶意URL访问行为。

[0152] 针对异常流量攻击行为，本发明实施例中，可以按照图5所示的流程进行异常流量攻击行为的检测及处置，包括以下步骤：

[0153] S51、采集Netflow流量数据。

[0154] 例如，安全监控平台在核心路由设备上采集$[t_n, t_{n+1}]$(n＝0,1,2,3……)时刻内的Netflow流量数据。

[0155] S52、针对采集的Netflow流量数据中包含的目的互联网协议IP地址，统计在预设时长内去向该目的IP地址的第一网络流量。

[0156] 本步骤中，安全监控平台对采集的Netflow流浪数据进行如下分析：安全监控平台以预设时长做维度进行流量大小统计，其中，预设时长可以根据实际需要进行设置，例如，预设时长可以设置为1分钟，安全监控平台以Netflow流量数据中包含的目的IP地址为索引，对所有去向该目的IP地址的流量进行统计，得到该目的IP地址在当前时段的访问流量，为了便于描述，记为C。

[0157] S53、判断第一网络流量是否超过动态流量阈值，如果是，执行步骤S54，如果否，执行步骤S511。

[0158] 具体实施时，可以按照以下方式确定动态流量阈值：针对该目的IP，统计历史上相同时间的访问流量均值，为了便于描述，记为A，动态流量阈值可以设置为统计得到的访问

流量均值的N倍，N为大于等于1的整数。例如，N为2，则本步骤中可以判断C是否大于等于2A。

[0159] 具体实施时，可以统计过去R天相同时间的访问流量平均值作为动态流量阈值，其中，R为正整数。

[0160] S54、以所述预设时长为单位持续统计多个时段的第二网络流量。

[0161] 本步骤中，如果判断出该目的IP当前访问流量超过动态流量阈值，则监控该目的IP当前持续访问流量。具体地，可以以分钟为单位分别记录该目的IP在每一时间单位内的网络访问流量C1，C2，C3……。

[0162] S55、判断各个统计时段的第二网络流量与所述第一网络流量的差值绝对值不超过预设流量阈值且持续时长超过预设时长阈值，如果是，执行步骤S55，否则，执行步骤S511。

[0163] 本步骤中，如果C1、C2、C3……与C的差值绝对值在很小范围内，且持续时长超过预设时长阈值，例如，持续尺长超过5分钟，则执行步骤S55。如果C1、C2、C3……与C的差值绝对值在很小范围内，但持续时长不超过预设时长阈值，则执行步骤S511，即只有同时满足这两个条件时将执行步骤S55。

[0164] S56、确定存在异常流量攻击行为。

[0165] S57、根据存在异常流量攻击行为对应的目的IP地址，从采集的Netflow流量数据中查找该目的IP地址对应的源IP地址。

[0166] 本步骤中，可以从采集的Netflow流量数据中溯源发起异常流量攻击的源IP地址，以确定相应的家庭网关。

[0167] S58、确定查找到的源IP地址为发起所述异常流量攻击行为的目标家庭网关标识。

[0168] S59、根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起异常流量攻击行为的、连接于所述目标家庭网关的从属设备标识。

[0169] 本步骤中，根据溯源出的发起异常流量攻击行为的家庭网关标识，根据相应网关上报的DNS解析数据和URL访问数据，确定发起异常流量攻击行为的从属设备标识。

[0170] S510、安全平台根据确定出的目标家庭网关标识，向相应的家庭网关发送安全访问控制指令，流程结束。

[0171] 在发送的安全访问控制指令中，携带有步骤S57中确定出的从属设备标识，使得部署于家庭网关中的网关安全插件对发起异常流量攻击行为的从属设备进行网络访问控制。

[0172] 其中，安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令，以对相应从属设备进行流量限速或者阻断处理，降低异常攻击流量。

[0173] S511、确定为正常流量。

[0174] 本发明实施例中，根据历史流量信息，构建动态异常流量分析模型，通过当前流量与历史流量的比较，当前异常流量的持续时间等检测特征，判定当前的流量是否出现异常。当判定为异常流量时，对去往该目标IP的源网关进行溯源，并连接网关安全插件去发现发起流量攻击的下挂设备，并对这些设备进行流量限制处置。

[0175] 针对恶意URL访问行为，安全监控平台可以根据采集的威胁情报数据中包含的恶意URL列表判断是否存在恶意URL访问，本发明实施例中，可以按照图6所示的流程进行检测及处置，包括以下步骤：

[0176] S61、查询各家庭网关上报的URL访问数据包含的URL是否存在于所述URL列表中，如果是，执行步骤S62，如果否，执行步骤S69。

[0177] 本步骤中，安全监控平台根据$[t_n,t_{n+1}]$(n＝0,1,2,3……)时刻内获得的URL访问数据，查找所述URL访问数据包含的URL是否存在于所述URL列表中，如果是，则确定监控到恶意URL访问行为，否则，确定不存在恶意URL访问行为。

[0178] S62、从存在恶意URL访问行为的家庭网关上报的DNS解析请求数据和URL访问数据中，查找发起请求的家庭网关IP地址和请求时间。

[0179] 本步骤中，安全监控平台根据各家庭网关在$[t_n,t_{n+1}]$(n＝0,1,2,3……)时刻内上报的DNS解析请求数据和URL访问数据，查找发起请求的家庭网关IP地址和请求时间。

[0180] S63、根据采集的NAT日志数据，确定发起恶意URL访问行为的实际IP地址。

[0181] 本步骤中，安全监控平台根据在$[t_n,t_{n+1}]$(n＝0,1,2,3……)时刻内采集的NAT日志数据，确定发起URL访问行为的实际IP地址。

[0182] S64、根据采集的RADIUS日志数据，确定所述实际IP地址的登录时间和退出时间。

[0183] 本步骤中，安全监控平台根据在$[t_n,t_{n+1}]$(n＝0,1,2,3……)时刻内采集的RADIUS日志数据，确定所述实际IP地址的登录时间和退出时间。

[0184] 需要说明的是，步骤S62、步骤S63和步骤S64没有一定的先后执行顺序，三个步骤可以同时执行，也可以分别执行，本发明实施例对此不进行限定。

[0185] S65、判断发起请求的家庭网关IP地址与所述实际IP地址相同且所述请求时间位于所述登录时间和退出时间之间，如果是，执行步骤S66，如果否，执行步骤S69。

[0186] S66、确定所述RADIUS日志数据对应的用户账号对应的家庭网关介质访问控制MAC地址为发起所述恶意网络访问行为的目标家庭网关标识。

[0187] 本步骤中，可以输出所有符合步骤S65中的两个条件的Radius日志中的用户帐号与所用家庭网关MAC地址。

[0188] S67、根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起所述恶意URL访问行为的、连接于所述目标家庭网关的从属设备标识。

[0189] S68、安全平台根据确定出的目标家庭网关标识，向相应的家庭网关发送安全访问控制指令，流程结束。

[0190] 在发送的安全访问控制指令中，携带有步骤S57中确定出的从属设备标识，使得部署于家庭网关中的网关安全插件对发起异常流量攻击行为的从属设备进行网络访问控制。

[0191] S69、确定不存在恶意URL访问行为。

[0192] 本发明实施例中，针对恶意URL访问行为，安全监控平台从网关安全插件上报的上网URL访问数据中，分析是否存在恶意的URL信息，若是存在，则查询发起该访问行为的网关IP及相应时间，同时根据NAT日志及RADIUS日志查找该IP的上下线时间，若时间对应关系一致，则认定该家庭网关发起了恶意URL的访问请求，实现了该网关的溯源，并根据控制策略，对网关及相关用户进行提醒及处置。

[0193] 相应地，本发明实施例还提供了一种家庭网关侧实施的家庭网关安全监控方法，如图7所示，可以包括以下步骤：

[0194] S71、向安全监控平台上报网络访问数据。

[0195] 具体实施时，家庭网关可以按照预设的上报周期向安全监控平台上报自身采集的网络访问数据。具体地，部署于家庭网关中的网关安全插件可以通过两个OSGI开放的接口进行数据的采集：

[0196] 一、数据流镜像服务类(TrafficMirrorService)接口

[0197] 通过该接口，网关安全插件能够以镜像报文的方式获得家庭网关及所有下挂从属设备的DNS(域名系统)解析请求数据，采集到的参数可以但不限于包括：

[0198] 请求解析时间(Timestamp)；

[0199] 网关内网IP地址(Gateway IP)；

[0200] 网关MAC(Gateway MAC)；

[0201] 下挂的从属设备内网IP地址(Subdevice IP)；

[0202] 下挂的从属设备MAC地址(Subdevice MAC)；

[0203] 请求解析DNS地址的域名(Dns)；

[0204] DNS解析出的IP地址(Dst IP)。

[0205] 二、数据流精细处理服务类(TrafficDetailProcessService)接口

[0206] 通过该接口，可获得网关及所属下挂设备的URL访问数据，网关将抓取的内容通过系统消息通知到网关安全插件，能过采集到的参数可以但不限于包括：

[0207] 请求解析时间(Timestamp)；

[0208] 访问URL的具体请求信息(Url)；

[0209] URL对应的域名信息(Referer)；

[0210] 响应状态(StatusCode)。

[0211] S72、接收所述安全监控平台下发的安全访问控制指令。

[0212] 其中，所述安全访问控制指令中携带有控制网络访问的从属设备标识，所述安全访问控制指令为所述安全监控平台根据所述网络访问数据和/或采集的安全基础数据确定出存在恶意网络访问行为时下发的。

[0213] 可选地，所述网络访问数据包括以下至少一项:DNS解析请求数据和URL访问数据；所述安全基础数据包括以下至少一项:Netflow流量数据、RADIUS日志数据、NAT地址转换日志数据和威胁情报数据。

[0214] S73、根据所述安全访问控制指令，对所述从属设备标识对应的从属设备的网络访问操作进行控制。

[0215] 其中，所述安全访问控制指令包括以下任一项:网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。本发明实施例提供的家庭网关安全监控方法中，以网关安全插件为突破，配合安全监控平台的流量、日志实时采集分析，解决了传统家庭宽带安全防护方式只能够监测到网关一级，且防护手段手段集中，无法进一步下沉的难点问题，实现了对网关及下挂设备发起威胁风险的精准监控及溯源，同时将处置手段下沉至智能网关侧，将安全风险在网关侧既予以拦截及阻断，避免了网络攻击对家庭宽带网络造成的冲击，在保障家庭宽带用户网关安全的同时，提供了一个安全稳定的家庭宽带网络。

[0216] 本发明实施提供的家庭网关安全监控方法相比于传统的针对网关一级的网络行为安全监控，通过网关安全插件及网络侧RADIUS及NAT日志的采集分析，实现了对网关下挂设备网络行为的进一步精准监控，从而将攻击威胁监测及处置进一步下沉，避免因为处置

网关攻击威胁导致正常设备不能上网，极大的提高了威胁处置粒度。

[0217] 与传统的家庭宽带侧异常流量检测及处置手段相比，通过核心网络出口侧的netflow采集，配合网络侧RADIUS及NAT日志的精准溯源能力以及网关安全插件的网络行为上报，能够及时的发现异常流量攻击行为，并溯源定位发起攻击的网关及其下挂设备，极大的提高了检测精准度。同时与在网络侧用专用设备进行流量清洗相比，使用网关安全插件在网关上对发起攻击的下挂设备进行流量限速及处置，有效减少了网络流量清洗时网元间互相调度的工作路径，降低了对正常网络流量的影响，避免了对家庭宽带网络稳定性的干扰，通过底层设备的分布式流量控制，从而使更大规模的异常流量防护体系成为可能。

[0218] 基于同一发明构思，本发明实施例中还分别提供了安全监控平台和家庭网关侧实施的家庭网关安全监控装置，由于上述装置解决问题的原理与分别与上述的安全监控平台和家庭网关侧实施的家庭网关安全监控方法相似，因此上述装置的实施可以参见方法的实施，重复之处不再赘述。

[0219] 如图8所示，其为安全监控平台侧实施的家庭网关安全监控装置的结构示意图，可以包括：

[0220] 获得单元81，用于获得各家庭网关的安全监控数据，所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据；

[0221] 第一确定单元82，用于如果根据所述网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识；

[0222] 第二确定单元83，用于根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识；

[0223] 发送单元84，用于向所述目标家庭网关发送安全访问控制指令，所述安全访问控制指令中携带有确定出的从属设备标识。

[0224] 可选地，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一资源定位符URL访问数据；所述安全基础数据包括以下至少一项：网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

[0225] 可选地，所述恶意网络访问行为包括异常流量攻击行为；以及

[0226] 所述装置，还包括：

[0227] 第三确定单元，用于针对采集的Netflow流量数据中包含的目的互联网协议IP地址，统计在预设时长内去向该目的IP地址的第一网络流量；如果所述第一网络流量超过动态流量阈值，则以所述预设时长为单位持续统计多个时段的第二网络流量；如果各个统计时段的第二网络流量与所述第一网络流量的差值绝对值均不超过预设流量阈值，则确定存在异常流量攻击行为，否则，确定不存在异常流量攻击行为。

[0228] 可选地，所述第一确定单元，具体用于根据存在异常流量攻击行为对应的目的IP地址，从采集的Netflow流量数据中查找该目的IP地址对应的源IP地址；确定查找到的源IP地址为发起所述异常流量攻击行为的目标家庭网关标识；

[0229] 所述第二确定单元，具体用于根据所述目标家庭网关标识对应的目标家庭网关上

报的DNS解析请求数据和URL访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

[0230] 可选地，所述恶意网络访问行为包括恶意URL访问行为，所述威胁情报数据中包含有恶意URL列表；以及

[0231] 所述装置，还包括：

[0232] 第四确定单元，用于查询各家庭网关上报的URL访问数据包含的URL是否存在于所述URL列表中；如果是，则确定存在恶意URL访问行为，否则，确定不存在恶意URL访问行为。

[0233] 可选地，所述第一确定单元，具体用于从存在恶意URL访问行为的家庭网关上报的DNS解析请求数据和URL访问数据中，查找发起请求的家庭网关IP地址和请求时间；根据采集的NAT日志数据，确定发起恶意URL访问行为的实际IP地址；根据所述RADIUS日志数据，确定所述实际IP地址的登录时间和退出时间；如果发起请求的家庭网关IP地址与所述实际IP地址相同且所述请求时间位于所述登录时间和退出时间之间，则确定所述RADIUS日志数据对应的用户账号对应的家庭网关介质访问控制MAC地址为发起所述恶意网络访问行为的目标家庭网关标识；

[0234] 所述第二确定单元，具体用于根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识。

[0235] 可选地，所述安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

[0236] 如图9所示，其为家庭网关侧实施的家庭网关安全监控装置的结构示意图，包括：

[0237] 上报单元91，用于向安全监控平台上报网络访问数据；

[0238] 接收单元92，用于接收所述安全监控平台下发的安全访问控制指令，所述安全访问控制指令中携带有控制网络访问的从属设备标识，其中，所述安全访问控制指令为所述安全监控平台根据所述网络访问数据和/或采集的安全基础数据确定出存在恶意网络访问行为时下发的；

[0239] 控制单元93，用于根据所述安全访问控制指令，对所述从属设备标识对应的从属设备的网络访问操作进行控制。

[0240] 可选地，所述网络访问数据包括以下至少一项：域名系统DNS解析请求数据和统一资源定位符URL访问数据；所述安全基础数据包括以下至少一项：网络流Netflow流量数据、远程用户拨号认证系统RADIUS日志数据、网络地址转换NAT地址转换日志数据和威胁情报数据。

[0241] 可选地，所述安全访问控制指令包括以下任一项：网络访问限速控制指令、禁止网络访问控制指令和URL/IP地址过滤控制指令。

[0242] 为了描述的方便，以上各部分按照功能划分为各模块(或单元)分别描述。当然，在实施本发明时可以把各模块(或单元)的功能在同一个或多个软件或硬件中实现。

[0243] 具体实施时，本发明实施例提供的家庭网关安全监控系统，包括家庭网关和安全监控平台，其中所述家庭网关中设置有上述家庭网关侧实施的家庭网关安全监控装置；所述安全监控平台中设置有上述安全监控平台侧实施的家庭网关安全监控装置。

[0244] 在介绍了本发明示例性实施方式的家庭网关安全监控方法和装置之后，接下来，

介绍根据本发明的另一示例性实施方式的计算装置。

[0245] 所属技术领域的技术人员能够理解，本发明的各个方面可以实现为系统、方法或程序产品。因此，本发明的各个方面可以具体实现为以下形式，即：完全的硬件实施方式、完全的软件实施方式(包括固件、微代码等)，或硬件和软件方面结合的实施方式，这里可以统称为“电路”、“模块”或“系统”。

[0246] 在一些可能的实施方式中，根据本发明的计算装置可以至少包括至少一个处理单元、以及至少一个存储单元。其中，所述存储单元存储有程序代码，当所述程序代码被所述处理单元执行时，使得所述处理单元执行本说明书上述描述的根据本发明各种示例性实施方式的家庭网关安全监控方法中的步骤。例如，所述处理单元可以执行如图4中所示的步骤S41、获得各家庭网关的安全监控数据，所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据，步骤S42、如果根据所述网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识；步骤S43、根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识；以及步骤S44、向所述目标家庭网关发送安全访问控制指令，所述安全访问控制指令中携带有确定出的从属设备标识；或者执行如图7中所示的步骤S71、向安全监控平台上报网络访问数据，步骤S72、接收所述安全监控平台下发的安全访问控制指令；步骤S73、根据所述安全访问控制指令，对所述从属设备标识对应的从属设备的网络访问操作进行控制。

[0247] 下面参照图10来描述根据本发明的这种实施方式的计算装置100。图10显示的计算装置100仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0248] 如图10所示，计算装置100以通用计算设备的形式表现。计算装置100的组件可以包括但不限于：上述至少一个处理单元101、上述至少一个存储单元102、连接不同系统组件(包括存储单元102和处理单元101)的总线103。

[0249] 总线103表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器、外围总线、处理器或者使用多种总线结构中的任意总线结构的局域总线。

[0250] 存储单元102可以包括易失性存储器形式的可读介质，例如随机存取存储器(RAM)1021和/或高速缓存存储器1022，还可以进一步包括只读存储器(ROM)1023。

[0251] 存储单元102还可以包括具有一组(至少一个)程序模块1024的程序/实用工具1025，这样的程序模块1024包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0252] 计算装置100也可以与一个或多个外部设备104(例如键盘、指向设备等)通信，还可与一个或者多个使得用户能与计算装置100交互的设备通信，和/或与使得该计算装置100能与一个或多个其它计算设备进行通信的任何设备(例如路由器、调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口105进行。并且，计算装置100还可以通过网络适配器106与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图所示，网络适配器106通过总线103与用于计算装置100的其它模块通信。应当理解，尽管图中未示出，可以结合计算装置100使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数

据备份存储系统等。

[0253] 在一些可能的实施方式中，本发明提供的家庭网关安全监控方法的各个方面还可以实现为一种程序产品的形式，其包括程序代码，当所述程序产品在计算机设备上运行时，所述程序代码用于使所述计算机设备执行本说明书上述描述的根据本发明各种示例性实施方式的家庭网关安全监控方法中的步骤，例如，所述计算机设备可以执行如图4中所示的步骤S41、获得各家庭网关的安全监控数据，所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据，步骤S42、如果根据所述网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识；步骤S43、根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识；以及步骤S44、向所述目标家庭网关发送安全访问控制指令，所述安全访问控制指令中携带有确定出的从属设备标识；或者执行如图7中所示的步骤S71、向安全监控平台上报网络访问数据，步骤S72、接收所述安全监控平台下发的安全访问控制指令；步骤S73、根据所述安全访问控制指令，对所述从属设备标识对应的从属设备的网络访问操作进行控制。

[0254] 所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0255] 本发明的实施方式的用于家庭网关安全监控的程序产品可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在计算设备上运行。然而，本发明的程序产品不限于此，在本文件中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0256] 可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括——但不限于——电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0257] 可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于——无线、有线、光缆、RF等等，或者上述的任意合适的组合。

[0258] 可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算设备，或者，可以连接到外部计算设备(例如利用因特网服务

提供商来通过因特网连接)。

[0259] 应当注意,尽管在上文详细描述中提及了装置的若干单元或子单元,但是这种划分仅仅是示例性的并非强制性的。实际上,根据本发明的实施方式,上文描述的两个或更多单元的特征和功能可以在一个单元中具体化。反之,上文描述的一个单元的特征和功能可以进一步划分为由多个单元来具体化。

[0260] 此外,尽管在附图中以特定顺序描述了本发明方法的操作,但是,这并非要求或者暗示必须按照该特定顺序来执行这些操作,或是必须执行全部所示的操作才能实现期望的结果。附加地或备选地,可以省略某些步骤,将多个步骤合并为一个步骤执行,和/或将一个步骤分解为多个步骤执行。

[0261] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0262] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0263] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0264] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0265] 尽管已描述了本发明的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例做出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0266] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

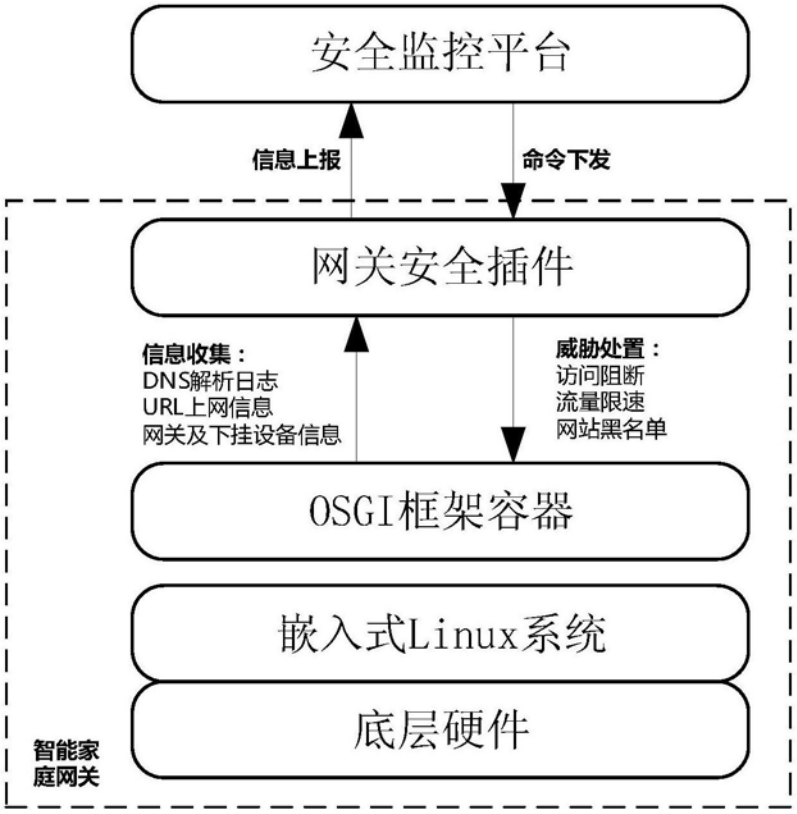

安全监控平台
信息上报
命令下发
网关安全插件
信息收集：
DNS解析日志
URL上网信息
网关及下挂设备信息
威胁处置：
访问阻断
流量限速
网站黑名单
OSGI框架容器
嵌入式Linux系统
底层硬件
智能家
庭网关

图1

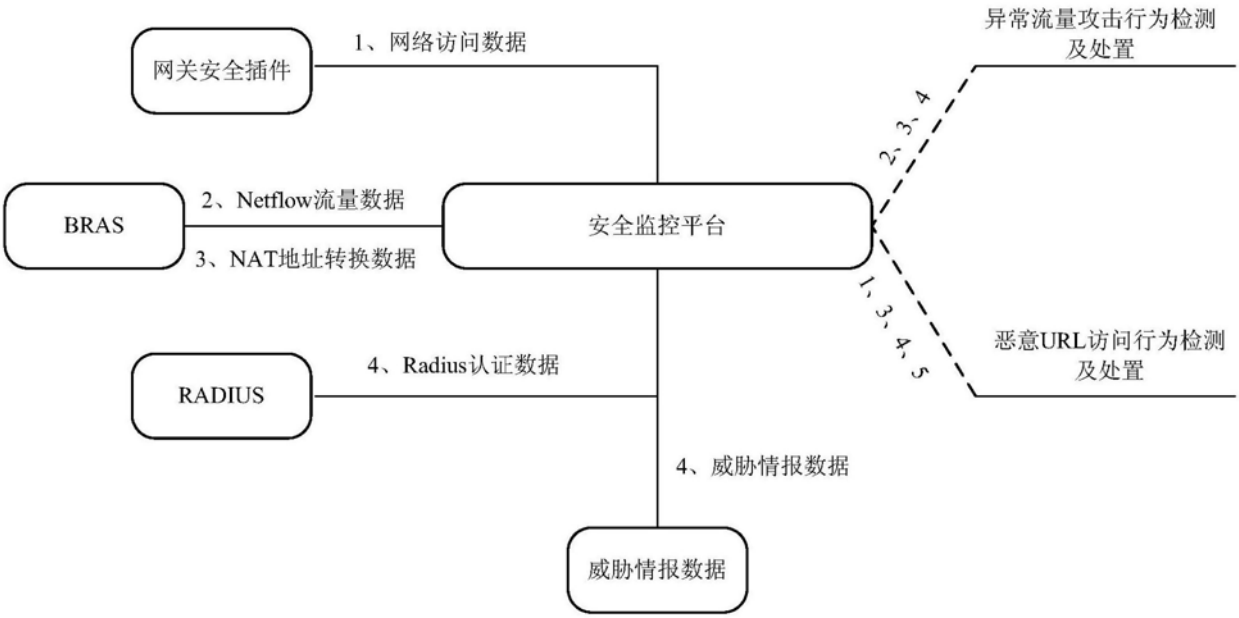

网关安全插件
1、网络访问数据
BRAS
2、Netflow流量数据
3、NAT地址转换数据
安全监控平台
RADIUS
4、Radius认证数据
4、威胁情报数据
威胁情报数据
异常流量攻击行为检测
及处置
2、3、4
1、3、4、5
恶意URL访问行为检测
及处置

图2

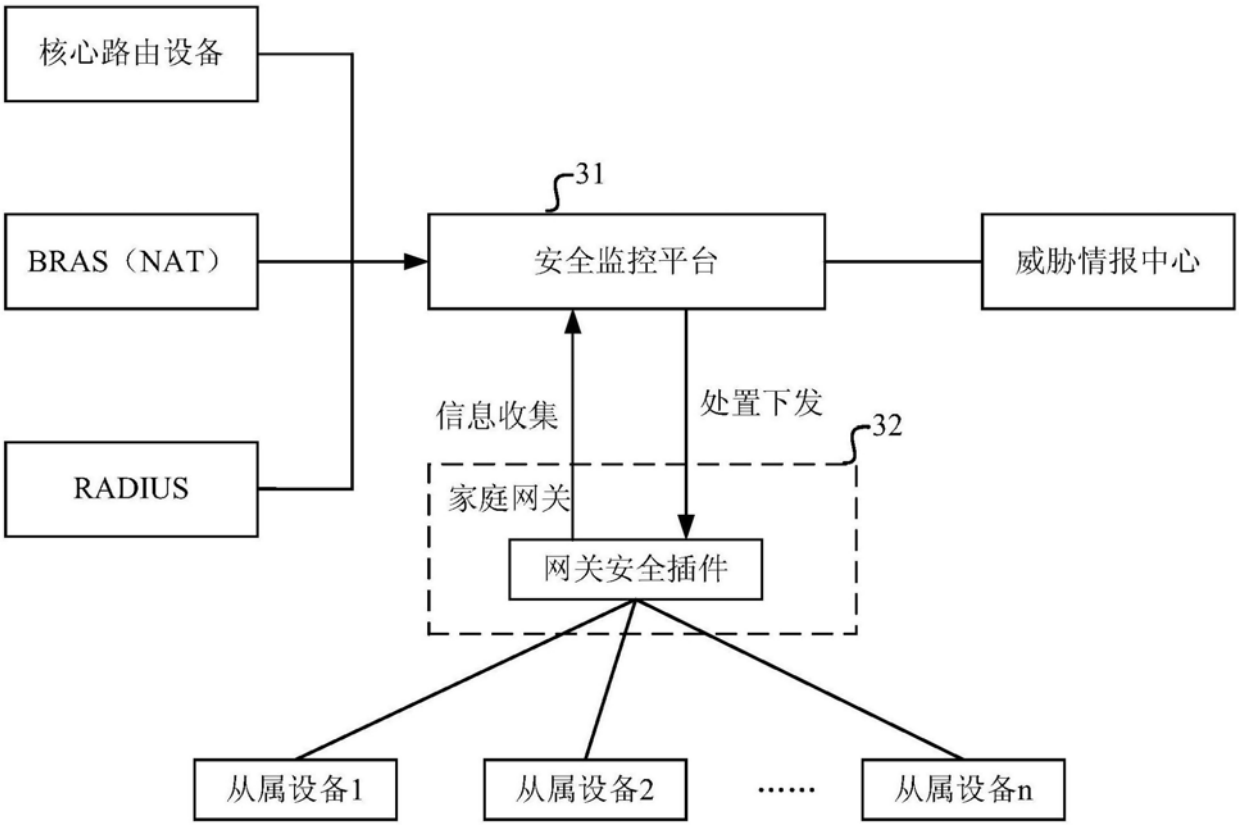

核心路由设备
BRAS（NAT）
RADIUS
31
安全监控平台
威胁情报中心
信息收集
处置下发
32
家庭网关
网关安全插件
从属设备1
从属设备2
……
从属设备n

图3

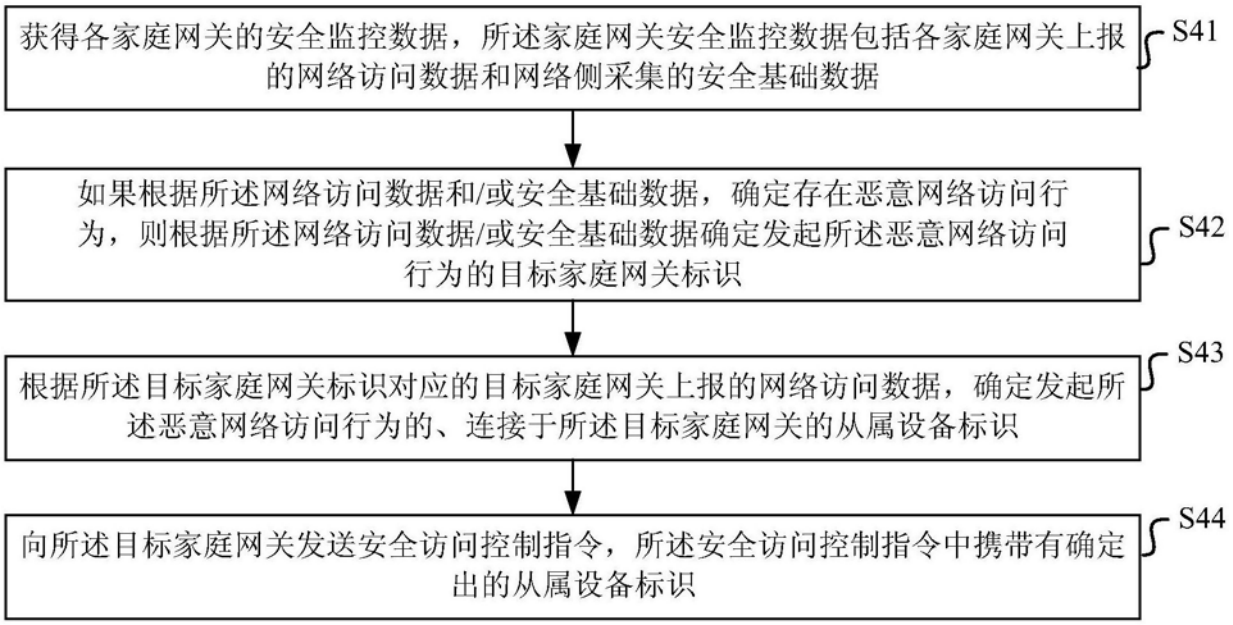

获得各家庭网关的安全监控数据，所述家庭网关安全监控数据包括各家庭网关上报的网络访问数据和网络侧采集的安全基础数据
S41
如果根据所述网络访问数据和/或安全基础数据，确定存在恶意网络访问行为，则根据所述网络访问数据/或安全基础数据确定发起所述恶意网络访问行为的目标家庭网关标识
S42
根据所述目标家庭网关标识对应的目标家庭网关上报的网络访问数据，确定发起所述恶意网络访问行为的、连接于所述目标家庭网关的从属设备标识
S43
向所述目标家庭网关发送安全访问控制指令，所述安全访问控制指令中携带有确定出的从属设备标识
S44

图4

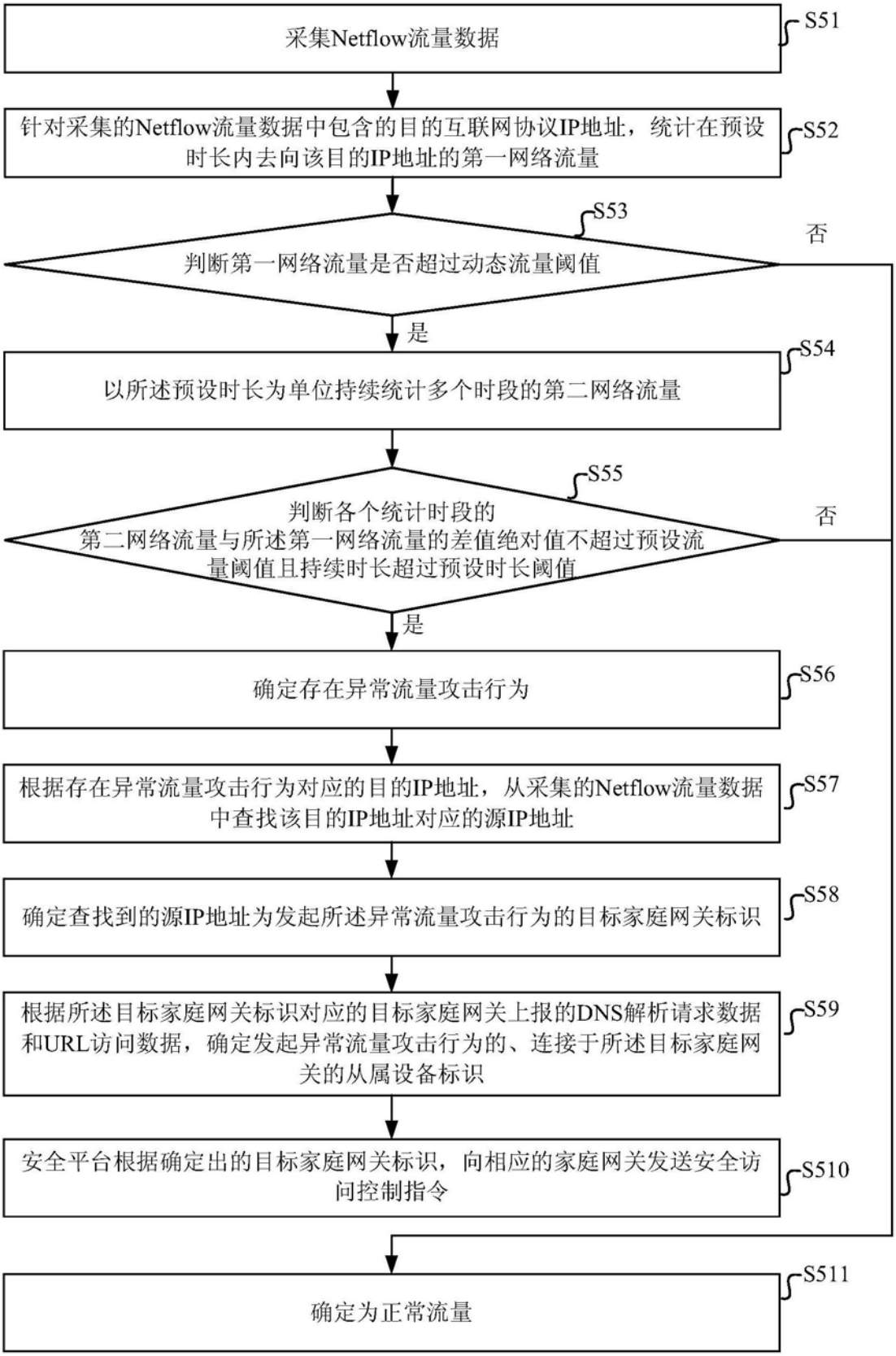

采集Netflow流量数据
S51
针对采集的Netflow流量数据中包含的目的互联网协议IP地址，统计在预设时长内去向该目的IP地址的第一网络流量
S52
S53
判断第一网络流量是否超过动态流量阈值
否
是
以所述预设时长为单位持续统计多个时段的第二网络流量
S54
S55
判断各个统计时段的第二网络流量与所述第一网络流量的差值绝对值不超过预设流量阈值且持续时长超过预设时长阈值
否
是
确定存在异常流量攻击行为
S56
根据存在异常流量攻击行为对应的目的IP地址，从采集的Netflow流量数据中查找该目的IP地址对应的源IP地址
S57
确定查找到的源IP地址为发起所述异常流量攻击行为的目标家庭网关标识
S58
根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起异常流量攻击行为的、连接于所述目标家庭网关的从属设备标识
S59
安全平台根据确定出的目标家庭网关标识，向相应的家庭网关发送安全访问控制指令
S510
确定为正常流量
S511

图5

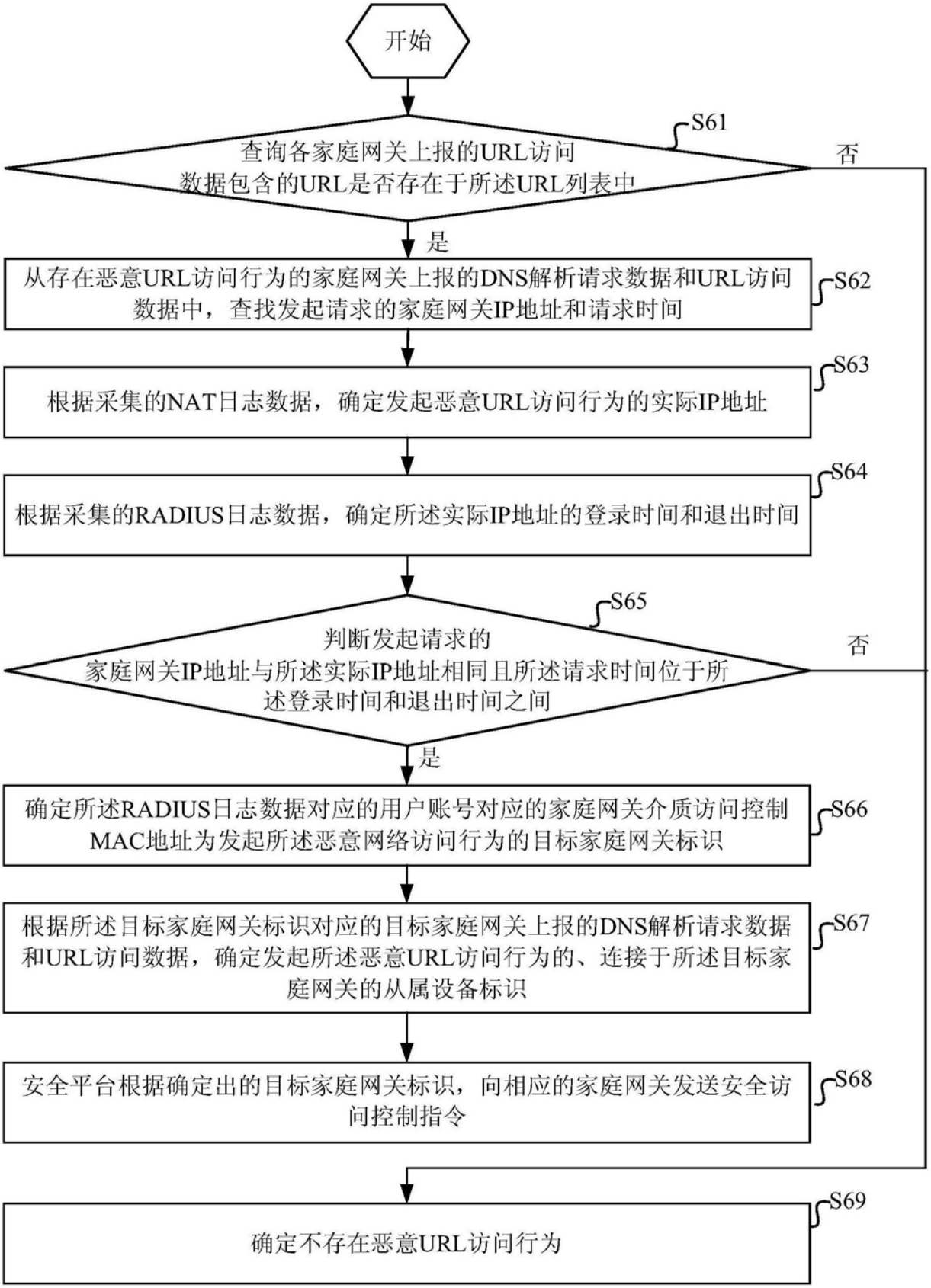

开始
S61
查询各家庭网关上报的URL访问数据包含的URL是否存在于所述URL列表中
否
是
从存在恶意URL访问行为的家庭网关上报的DNS解析请求数据和URL访问数据中，查找发起请求的家庭网关IP地址和请求时间
S62
根据采集的NAT日志数据，确定发起恶意URL访问行为的实际IP地址
S63
根据采集的RADIUS日志数据，确定所述实际IP地址的登录时间和退出时间
S64
S65
判断发起请求的家庭网关IP地址与所述实际IP地址相同且所述请求时间位于所述登录时间和退出时间之间
否
是
确定所述RADIUS日志数据对应的用户账号对应的家庭网关介质访问控制MAC地址为发起所述恶意网络访问行为的目标家庭网关标识
S66
根据所述目标家庭网关标识对应的目标家庭网关上报的DNS解析请求数据和URL访问数据，确定发起所述恶意URL访问行为的、连接于所述目标家庭网关的从属设备标识
S67
安全平台根据确定出的目标家庭网关标识，向相应的家庭网关发送安全访问控制指令
S68
确定不存在恶意URL访问行为
S69

图6

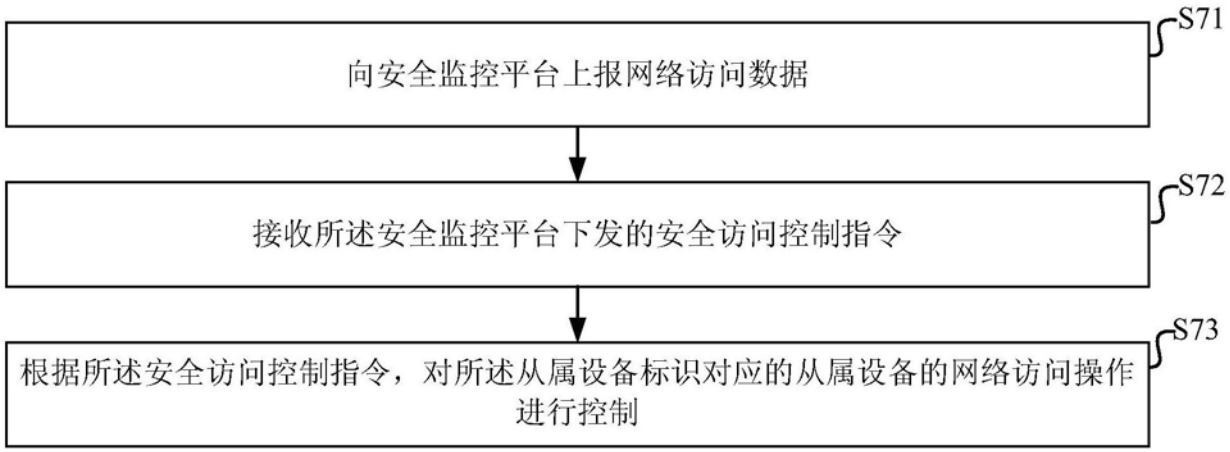

S71
向安全监控平台上报网络访问数据
S72
接收所述安全监控平台下发的安全访问控制指令
S73
根据所述安全访问控制指令，对所述从属设备标识对应的从属设备的网络访问操作进行控制

图7

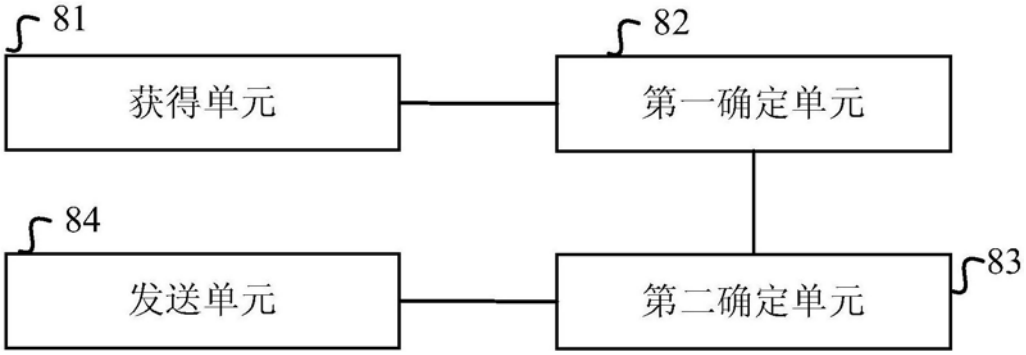

81
获得单元
82
第一确定单元
84
发送单元
83
第二确定单元

图8


91
上报单元
安全监控平台
92
接收单元
93
控制单元

图9

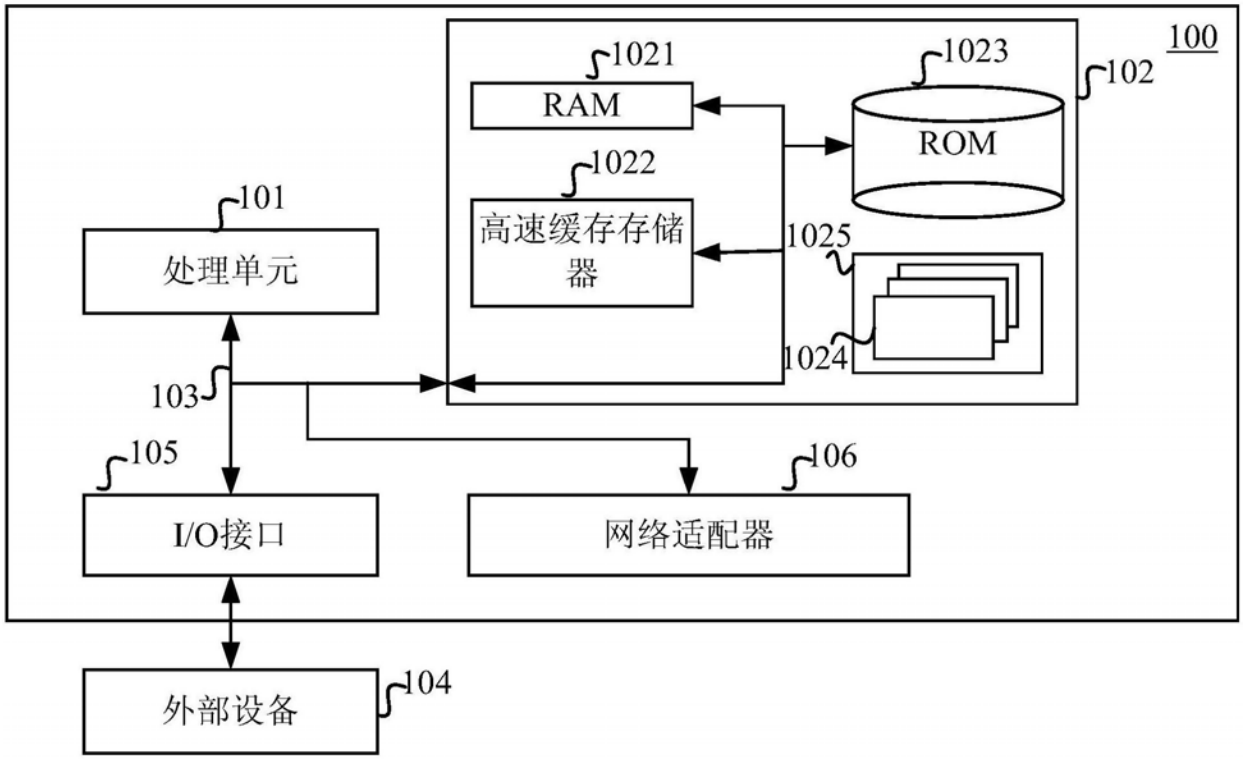

100
1021
RAM
1023
ROM
102
1022
高速缓存存储器
1025
1024
101
处理单元
103
105
I/O接口
106
网络适配器
外部设备
104

图10