



## (12)发明专利

(10)授权公告号 CN 104380686 B

(45)授权公告日 2018.08.21

(21)申请号 201480001549.0

(22)申请日 2014.04.03

(65)同一申请的已公布的文献号

申请公布号 CN 104380686 A

(43)申请公布日 2015.02.25

(30)优先权数据

IN5037/CHE/2013 2013.11.07 IN

(85)PCT国际申请进入国家阶段日

2014.12.19

(86)PCT国际申请的申请数据

PCT/CN2014/074744 2014.04.03

(87)PCT国际申请的公布数据

WO2015/066996 EN 2015.05.14

(73)专利权人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 山贾·库马尔·纳维

德布塔·纳亚克 章驰

(51)Int.Cl.

H04L 29/06(2006.01)

(56)对比文件

CN 101444119 A, 2009.05.27,

CN 1798436 A, 2006.07.05,

US 2007192847 A1, 2007.08.16,

US 2012304244 A1, 2012.11.29,

CN 101729531 A, 2010.06.09,

CN 102045320 A, 2011.05.04,

US 2011321150 A1, 2011.12.29,

周安娜.应用防火墙应用与研究.《科技广场》.2009,(第07(2009)期),全文.

胡波.下一代防火墙技术探析.《保密科学技术》.2012,(第02(2012)期),正文第2-3节,表1.

审查员 李星星

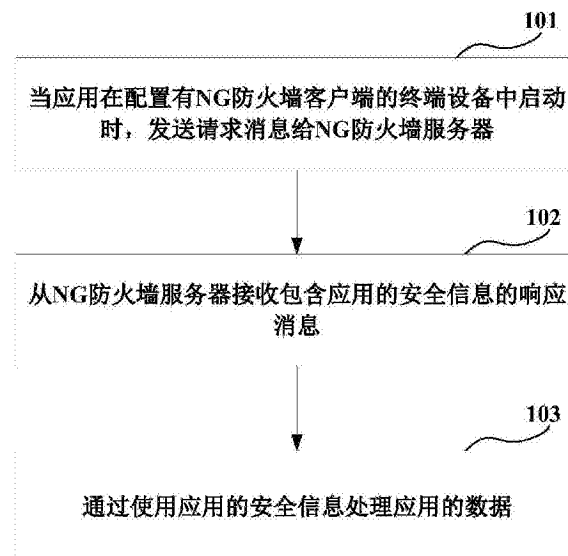
权利要求书4页 说明书18页 附图14页

### (54)发明名称

用于实施NG防火墙的方法和系统、NG防火墙客户端和NG防火墙服务器

### (57)摘要

本发明的实施例提供用于实施NG防火墙的方法和系统、NG防火墙客户端以及NG防火墙服务器。所述方法包括：当应用在配置有所述NG防火墙客户端的终端设备中被启动时，发送用于请求应用的安全信息的请求消息；接收包含所述应用的所述安全信息的响应消息；通过使用所述应用的所述安全信息处理所述应用的接收或发送数据。在本发明中，可以实现动态加载攻击防范，从而终端设备所需的软件占用空间可以减少，并且安装在终端设备上的应用的性能可以得到提高。



1. 一种用于实施NG防火墙(下一代防火墙)的方法,其特征在于,所述方法包括:

当应用在终端设备中被启动时,向NG防火墙服务器发送用于请求所述应用相对应的安全信息的请求消息;

从所述NG防火墙服务器接收包含所述应用的所述安全信息的响应消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;

通过使用所述应用的所述安全信息处理所述应用的数据。

2. 根据权利要求1所述的方法,其特征在于,所述请求消息包含所述应用的识别信息,以及所述应用的所述识别信息用于所述NG防火墙服务器确定所述应用的所述安全信息。

3. 根据权利要求1所述的方法,其特征在于,所述方法进一步包括:

当所述应用在所述终端设备中被关闭时,清除所述应用的所述安全信息。

4. 根据权利要求1至3任一项权利要求所述的方法,其特征在于,所述响应消息还包括用于维护所述应用的部分或全部安全信息的一个或多个定时器值;以及

所述方法进一步包括:当对应于所述应用的所述部分安全信息的所述一个或多个定时器值中的一个或多个定时器超时时,重新请求所述应用的所述部分安全信息,或

当对应于所述应用的所述全部安全信息的所述一个或多个定时器值中的一个或多个定时器超时时,重新请求所述应用的所述全部安全信息。

5. 根据权利要求4所述的方法,其特征在于,所述方法进一步包括:

当对应于所述应用的所述部分安全信息的所述一个或多个定时器值中的一个或多个定时器超时时,清除所述应用的所述部分安全信息,或

当对应于所述应用的所述全部安全信息的所述一个或多个定时器值中的一个或多个定时器超时时,清除所述应用的所述全部安全信息。

6. 根据权利要求1至3任一项权利要求所述的方法,其特征在于,所述应用的所述安全信息包括以下信息的任意一项或组合:

所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

7. 根据权利要求6所述的方法,其特征在于,存在不同的定时器值用于保存以下信息的任意一项或组合:所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息;或

存在相同的定时器值用于保存以下信息的任意一项或组合:所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

8. 根据权利要求6所述的方法,其特征在于,通过使用所述应用的所述安全信息处理所述应用的数据包括:

通过使用所述应用的所述报文签名信息处理所述应用的所述数据,或

通过使用所述应用的所述接入控制列表信息处理所述应用的所述数据,或

通过使用所述应用的所述畸形攻击信息处理所述应用的所述数据,或

通过使用所述应用的所述状态防火墙库信息处理所述应用的所述数据,或

通过使用所述应用的所述报文限速策略信息处理所述应用的所述数据。

9. 一种用于实施NG防火墙的方法,其特征在于,所述方法包括:

从终端设备接收用于请求应用相对应的安全信息的请求消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;

根据所述请求消息确定所述应用的所述安全信息;

向所述终端设备发送包含所述应用的所述安全信息的响应消息。

10. 根据权利要求9所述的方法,其特征在于,所述请求消息包括所述应用的识别信息;以及

所述根据所述请求消息确定所述应用的所述安全信息包括:根据所述请求消息中包含的所述应用的所述识别信息从数据库中获取所述应用的所述安全信息。

11. 根据权利要求9或10所述的方法,其特征在于,在向所述终端设备发送包含所述应用的所述安全信息的响应消息之前,所述方法进一步包括:

认证所述请求消息是否有效;

当所述请求消息有效时,执行向所述终端设备发送所述包含所述应用的所述安全信息的响应消息的过程。

12. 根据权利要求9或10所述的方法,其特征在于,所述方法进一步包括:

确定用于维护所述应用的部分或全部安全信息的一个或多个定时器值;

所述向所述终端设备发送包含所述应用的所述安全信息的响应消息包括:向所述终端设备发送包含所述应用的所述安全信息的响应消息,以及用于维护所述应用的部分或全部安全信息的一个或多个定时器值。

13. 根据权利要求9至10任一项权利要求所述的方法,其特征在于,所述应用的所述安全信息包括以下信息的任意一项或组合:所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

14. 一种NG防火墙客户端,其特征在于,包括:

发送单元,用于当应用在配置有NG防火墙客户端的终端设备中被启动时,向NG防火墙服务器发送用于请求所述应用相对应的安全信息的请求消息;

接收单元,用于从所述NG防火墙服务器接收包含所述应用的所述安全信息的响应消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;

处理单元,用于通过使用所述应用的所述安全信息处理所述应用的数据。

15. 根据权利要求14所述的NG防火墙客户端,其特征在于,所述发送单元具体用于,当应用在配置有所述NG防火墙客户端的终端设备中被启动时,向所述NG防火墙服务器发送用于请求所述应用的所述安全信息的所述请求消息;其中所述请求消息包含所述应用的识别信息,以及所述应用的所述识别信息用于所述NG防火墙服务器确定所述应用的所述安全信息。

16. 根据权利要求14所述的NG防火墙客户端,其特征在于,所述NG防火墙客户端进一步包括:

清除单元,用于当所述应用在所述终端设备中被关闭时,清除所述应用的所述安全信息。

17. 根据权利要求14至16任一项权利要求所述的NG防火墙客户端,其特征在于,所述响

应消息进一步包括用于维护所述应用的部分或全部安全信息的一个或多个定时器值;以及  
所述发送单元进一步用于,当对应于所述应用的所述部分安全信息的所述一个或多个定时器值中的一个或多个定时器超时,重新请求所述应用的所述部分安全信息,或当对应于所述应用的所述全部安全信息的所述一个或多个定时器值中的一个或多个定时器超时,重新请求所述应用的所述全部安全信息。

18.根据权利要求17所述的NG防火墙客户端,其特征在于,

所述NG防火墙客户端进一步包括:

清除单元,用于当所述应用在所述终端设备中被关闭时,清除所述应用的所述安全信息;

所述清除单元进一步用于,当对应于所述应用的所述部分安全信息的所述一个或多个定时器值中的一个或多个定时器超时,清除所述应用的所述部分安全信息,或当对应于所述应用的所述全部安全信息的所述一个或多个定时器值中的一个或多个定时器超时,清除所述应用的所述全部安全信息。

19.根据权利要求14至16任一项权利要求所述的NG防火墙客户端,其特征在于,所述应用的所述安全信息包括以下信息的任意一项或组合:所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

20.根据权利要求19所述的NG防火墙客户端,其特征在于,所述处理单元具体用于:

通过使用所述应用的所述报文签名信息处理所述应用的所述数据,或

通过使用所述应用的所述接入控制列表信息处理所述应用的所述数据,或

通过使用所述应用的所述畸形攻击信息处理所述应用的所述数据,或

通过使用所述应用的所述状态防火墙库信息处理所述应用的所述数据,或

通过使用所述应用的所述报文限速策略信息处理所述应用的所述数据。

21.一种NG防火墙服务器,其特征在于,包括:

接收单元,用于从终端设备接收用于请求应用相对应的安全信息的请求消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;

第一确定单元,用于根据所述请求消息确定所述应用的所述安全信息;

发送单元,用于向所述终端设备发送包含所述应用的所述安全信息的响应消息。

22.根据权利要求21所述的NG防火墙服务器,其特征在于,所述请求消息包括所述应用的识别信息;以及

所述第一确定单元具体用于根据所述请求消息中包含的所述应用的所述识别信息从数据库中获取所述应用的所述安全信息。

23.根据权利要求21或22所述的NG防火墙服务器,其特征在于,所述NG防火墙服务器进一步包括:

认证单元,用于认证所述请求消息是否有效;以及

所述发送单元具体用于,当所述请求消息有效时,发送包含所述应用的所述安全信息的所述响应消息给所述终端设备。

24.根据权利要求21或22所述的NG防火墙服务器,其特征在于,所述NG防火墙服务器进一步包括:

第二确定单元,用于确定用于维护所述应用的部分或全部安全信息的一个或多个定时器值;

所述发送单元具体用于发送包含所述应用的所述安全信息的响应消息,以及用于维护所述应用的部分或全部安全信息的一个或多个定时器值给所述终端设备。

25.根据权利要求21至22任一项权利要求所述的NG防火墙服务器,其特征在于,所述应用的所述安全信息包括以下信息的任意一项或组合:所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

26.一种终端设备,其特征在于,包括:

处理器和耦合至所述处理器的存储器;

其中所述处理器用于:

当应用在所述终端设备中被启动时,向NG防火墙服务器发送用于请求所述应用相对应的安全信息的请求消息;

从所述NG防火墙服务器接收包含所述应用的所述安全信息的响应消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;

通过使用所述应用的所述安全信息处理所述应用的数据。

27.一种NG防火墙服务器,其特征在于,包括:

处理器和耦合至所述处理器的存储器;

其中所述处理器用于:

从终端设备接收用于请求应用相对应的安全信息的请求消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;

根据所述请求消息确定所述应用的所述安全信息;

向所述终端设备发送包含所述应用的所述安全信息的响应消息。

28.一种用于实施NG防火墙的系统,其特征在于,所述系统包括:

如权利要求26所述的一个或多个终端设备;以及

如权利要求27所述的NG防火墙服务器。

## 用于实施NG防火墙的方法和系统、NG防火墙客户端和NG防火墙服务器

### 技术领域

[0001] 本发明涉及通信技术,尤其涉及一种用于实施NG防火墙的方法和系统、一种NG防火墙客户端以及一种NG防火墙服务器。

### 背景技术

[0002] NG防火墙(NG-FW,下一代防火墙)将安全服务统一到单一引擎中并改变接入控制和安全策略的设计。NG防火墙扩展了应用和业务流的管理。NG防火墙的功能包括:允许、拦截、记录、监控以及带宽控制等。

[0003] NG防火墙结合了第一代防火墙,例如,状态和无状态网络防火墙、应用防火墙、NAT-ALG(网络地址转换应用层网关)、IPS(入侵防御系统)/IDS(入侵检测系统)、反X恶意软件扫描。这种结合增加了NG防火墙的复杂性。NG防火墙的基础是对关联先前接收报文的传入和传出报文进行深度报文检测。

[0004] 另一方面,智能手机是旅行中BYOD(携带自己的设备办公)、个人银行、社交网站和娱乐的关键推动因素。这样增加了对消费者隐私的安全威胁以及个人和商业数据的泄漏。

[0005] 然而,申请人发现:NG防火墙安装在具有高计算能力的专用服务器上。然而,NG防火墙还没有在智能手机等终端设备上实施。因此终端设备所需的软件占用空间没有减少,而且安装在终端设备上的应用的性能没有得到提高。

### 发明内容

[0006] 本发明的实施例涉及提供一种实施NG防火墙的方法和系统、一种NG防火墙客户端以及一种NG防火墙服务器,以在不影响应用层防攻击的情况下,减少终端设备上NF防火墙NG防火墙的软件占用空间。

[0007] 根据本发明的实施例的一方面,提供了一种用于实施NG防火墙(下一代防火墙)的方法,所述方法包括:

[0008] 当应用在终端设备中被启动时,向NG防火墙服务器发送用于请求所述应用的安全信息的请求消息;

[0009] 从所述NG防火墙服务器接收包含所述应用的所述安全信息的响应消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;

[0010] 通过使用所述应用的所述安全信息处理所述应用的数据。

[0011] 根据本发明的实施例的另一方面,所述请求消息包含所述应用的识别信息,以及所述应用的所述识别信息用于所述NG防火墙服务器确定所述应用的所述安全信息。

[0012] 根据本发明的实施例的另一方面,所述方法进一步包括:

[0013] 当所述应用在所述终端设备中被关闭时,清除所述应用的所述安全信息。

[0014] 根据本发明的实施例的另一方面,所述响应消息进一步包括用于维护所述应用的部分或全部安全信息的一个或多个定时器值;以及

[0015] 所述方法进一步包括：当对应于所述应用的所述部分安全信息的所述一个或多个定时器值中的一个或多个定时器超时，重新请求所述应用的所述部分安全信息，或

[0016] 当对应于所述应用的所述全部安全信息的所述一个或多个定时器值中的一个或多个定时器超时，重新请求所述应用的所述全部安全信息。

[0017] 根据本发明的实施例的另一方面，所述方法进一步包括：

[0018] 当对应于所述应用的所述部分安全信息的所述一个或多个定时器值中的一个或多个定时器超时，清除所述应用的所述部分安全信息，或

[0019] 当对应于所述应用的所述全部安全信息的所述一个或多个定时器值中的一个或多个定时器超时，清除所述应用的所述全部安全信息。

[0020] 根据本发明的实施例的另一方面，所述应用的所述安全信息包括以下信息的任意一项或组合：所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

[0021] 根据本发明的实施例的另一方面，存在不同的定时器值用于保存以下信息的任意一项或组合：所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息；或

[0022] 存在相同的定时器值用于保存以下信息的任意一项或组合：所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

[0023] 根据本发明的实施例的另一方面，通过使用所述应用的所述安全信息处理所述应用的数据包括：

[0024] 通过使用所述应用的所述报文签名信息处理所述应用的所述数据，或

[0025] 通过使用所述应用的所述接入控制列表信息处理所述应用的所述数据，或

[0026] 通过使用所述应用的所述畸形攻击信息处理所述应用的所述数据，或

[0027] 通过使用所述应用的所述状态防火墙库信息处理所述应用的所述数据，或

[0028] 通过使用所述应用的所述报文限速策略信息处理所述应用的所述数据。

[0029] 根据本发明的实施例的另一方面，提供了一种用于实施NG防火墙的方法，所述方法包括：

[0030] 从终端设备接收用于请求应用的安全信息的请求消息，其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息；

[0031] 根据所述请求消息确定所述应用的所述安全信息；

[0032] 向所述终端设备发送包含所述应用的所述安全信息的响应消息。

[0033] 根据本发明的实施例的另一方面，所述请求消息包括所述应用的识别信息；以及

[0034] 根据所述请求消息确定所述应用的所述安全信息包括：根据所述请求消息中包含的所述应用的所述识别信息从数据库中获取所述应用的所述安全信息。

[0035] 根据本发明的实施例的另一方面，在向所述终端设备发送包含所述应用的所述安全信息的响应消息之前，所述方法进一步包括：

[0036] 认证所述请求消息是否有效；

[0037] 当所述请求消息有效时，执行向所述终端设备发送所述包含所述应用的所述安全信息的响应消息的过程。

[0038] 根据本发明的实施例的另一方面,所述方法进一步包括:

[0039] 确定用于维护所述应用的部分或全部安全信息的一个或多个定时器值;

[0040] 所述向所述终端设备发送包含所述应用的所述安全信息的响应消息包括:发送包含所述应用的所述安全信息的响应消息,以及用于维护所述应用的部分或全部安全信息的一个或多个定时器值给所述终端设备。

[0041] 根据本发明的实施例的另一方面,所述应用的所述安全信息包括以下信息的任意一项或组合:所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

[0042] 根据本发明的实施例的另一方面,提供了一种NG防火墙客户端,包括:

[0043] 发送单元,用于当应用在配置有NG防火墙客户端的终端设备中被启动时,向NG防火墙服务器发送用于请求所述应用的安全信息的请求消息;

[0044] 接收单元,用于从所述NG防火墙服务器接收包含所述应用的所述安全信息的响应消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;

[0045] 处理单元,用于通过使用所述应用的所述安全信息处理所述应用的数据。

[0046] 根据本发明的实施例的另一方面,所述发送单元具体用于,当应用在配置有所述NG防火墙客户端的终端设备中被启动时,向所述NG防火墙服务器发送用于请求所述应用的所述安全信息的所述请求消息;其中所述请求消息包含所述应用的识别信息,以及所述应用的所述识别信息用于所述NG防火墙服务器确定所述应用的所述安全信息。

[0047] 根据本发明的实施例的另一方面,所述NG防火墙客户端进一步包括:

[0048] 清除单元,用于当所述应用在所述终端设备中被关闭时,清除所述应用的所述安全信息。

[0049] 根据本发明的实施例的另一方面,所述响应消息进一步包括用于维护所述应用的部分或全部安全信息的一个或多个定时器值;以及

[0050] 所述发送单元进一步用于,当对应于所述应用的所述部分安全信息的所述一个或多个定时器值中的一个或多个定时器超时时,重新请求所述应用的所述部分安全信息,或当对应于所述应用的所述全部安全信息的所述一个或多个定时器值中的一个或多个定时器超时时,重新请求所述应用的所述全部安全信息。

[0051] 根据本发明的实施例的另一方面,所述清除单元进一步用于,当对应于所述应用的所述部分安全信息的所述一个或多个定时器值中的一个或多个定时器超时时,清除所述应用的所述部分安全信息,或当对应于所述应用的所述全部安全信息的所述一个或多个定时器值中的一个或多个定时器超时时,清除所述应用的所述全部安全信息。

[0052] 根据本发明的实施例的另一方面,所述应用的所述安全信息包括以下信息的任意一项或组合:所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。

[0053] 根据本发明的实施例的另一方面,所述处理单元具体用于:

[0054] 通过使用所述应用的所述报文签名信息处理所述应用的所述数据,或

[0055] 通过使用所述应用的所述接入控制列表信息处理所述应用的所述数据,或

[0056] 通过使用所述应用的所述畸形攻击信息处理所述应用的所述数据,或

- [0057] 通过使用所述应用的所述状态防火墙库信息处理所述应用的所述数据,或
- [0058] 通过使用所述应用的所述报文限速策略信息处理所述应用的所述数据。
- [0059] 根据本发明的实施例的另一方面,提供了一种NG防火墙服务器,包括:
- [0060] 接收单元,用于从终端设备接收用于请求应用的安全信息的请求消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;
- [0061] 第一确定单元,用于根据所述请求消息确定所述应用的所述安全信息;
- [0062] 发送单元,用于向所述终端设备发送包含所述应用的所述安全信息的响应消息。
- [0063] 根据本发明的实施例的另一方面,所述请求消息包括所述应用的识别信息;以及
- [0064] 所述第一确定单元具体用于根据所述请求消息中包含的所述应用的所述识别信息从数据库中获取所述应用的所述安全信息。
- [0065] 根据本发明的实施例的另一方面,所述NG防火墙服务器进一步包括:
- [0066] 认证单元,用于认证所述请求消息是否有效;以及
- [0067] 所述发送单元具体用于,当所述请求消息有效时,发送包含所述应用的所述安全信息的所述响应消息给所述终端设备。
- [0068] 根据本发明的实施例的另一方面,所述NG防火墙服务器进一步包括:
- [0069] 第二确定单元,用于确定用于维护所述应用的部分或全部安全信息的一个或多个定时器值;
- [0070] 所述发送单元具体用于发送包含所述应用的所述安全信息的响应消息,以及用于维护所述应用的部分或全部安全信息的一个或多个定时器值给所述终端设备。
- [0071] 根据本发明的实施例的另一方面,所述应用的所述安全信息包括以下信息的任意一项或组合:所述应用的报文签名信息、所述应用的接入控制列表信息、所述应用的畸形报文攻击信息、所述应用的有状态防火墙库信息以及所述应用的报文限速策略信息。
- [0072] 根据本发明的实施例的另一方面,提供一种终端设备,包括:
- [0073] 处理器和耦合至所述处理器的存储器;
- [0074] 其中所述处理器用于:
- [0075] 当应用在所述终端设备中被启动时,向NG防火墙服务器发送用于请求所述应用的安全信息的请求消息;
- [0076] 从所述NG防火墙服务器接收包含所述应用的所述安全信息的响应消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;
- [0077] 通过使用所述应用的所述安全信息处理所述应用的数据。
- [0078] 根据本发明的实施例的另一方面,提供了一种NG防火墙服务器,包括:
- [0079] 处理器和耦合至所述处理器的存储器;
- [0080] 其中所述处理器用于:
- [0081] 从终端设备接收用于请求应用的安全信息的请求消息,其中所述应用的所述安全信息表示对所述终端设备中启动的所述应用作安全保护的信息;
- [0082] 根据所述请求消息确定所述应用的所述安全信息;
- [0083] 向所述终端设备发送包含所述应用的所述安全信息的响应消息。
- [0084] 根据本发明的实施例的另一方面,提供了一种用于实施NG防火墙的系统,包括:
- [0085] 如上所述的一个或多个终端设备;以及

[0086] 如上所述的NG防火墙服务器。

[0087] 本发明的实施例的有益效果在于：当应用在终端设备中被启动时，NG防火墙客户端向NG防火墙服务器请求所述应用的安全信息。因此，本发明的实施例可以实现动态加载攻击防范，从而终端设备所需的软件占用空间可以减少，并且安装在终端设备上的应用的性能可以得到提高。

[0088] 此外，终端设备将受到保护，免遭来自新应用或服务的新攻击。由于攻击防范的数量直接依赖于用户正在使用的应用的数量，所以信令报文将减少，这样有助于延长移动终端的电池寿命。

[0089] 参考以下描述和附图，本发明的这些和其他方面以及特征将显而易见。在描述和附图中，详细揭示了本发明的特定实施例，以指示出本发明的原理可以采用的一些方式，但应理解，本发明并不限于对应的范围。相反，本发明包括所附权利要求书的精神和项内的所有变化、修改以及等效物。

[0090] 参考一项实施例描述和/或说明的特征可以采用相同方式或类似方式用于一项或多项其他实施例，和/或与其他实施例的特征结合使用或替代这些特征。

[0091] 应强调的是，本说明书中所用的术语“包括”用于说明存在所述特征、整体、步骤或部件，但并不排除存在或添加一个或多个其他特征、整体、步骤、部件或上述项的组合。

[0092] 参考以下附图可以更好地理解本发明的许多方面。附图中的部件不必按比例绘制，而是将重点放在清晰地说明本发明的原理上。为了有助于说明并描述本发明的一些部分，可以将附图中对应部分的尺寸放大，例如，相对于其他部分而言，使其比根据本发明实际制作的示例性装置大。本发明的一个附图或实施例中描绘的元件和特征可以与一个或多个额外附图或实施例中描绘的元件和特征相结合。此外，在附图中，相同参考编号指代若干视图中的对应部分，并且可以用来指代一项以上实施例中的相同或类似部分。

## 附图说明

[0093] 附图被包括在内以提供对本发明的进一步理解，附图构成本说明书的一部分，说明本发明的优选实施例，并且与描述内容一起用于阐明本发明的原理。附图中相同的参考编号始终表示相同的元件。

[0094] 在附图中：

[0095] 图1为根据本发明的实施例的用于实施NG防火墙的方法的流程示意图；

[0096] 图2为图示关于终端设备和NG防火墙服务器的结构示意图；

[0097] 图3为根据本发明的实施例的用于实施NG防火墙的方法的流程示意图；

[0098] 图4为根据本发明的实施例的用于实施NG防火墙的方法的另一流程示意图；

[0099] 图5为根据本发明的实施例的步骤402的流程示意图；

[0100] 图6为根据本发明的实施例的步骤403的流程示意图；

[0101] 图7为根据本发明的实施例的步骤405的流程示意图；

[0102] 图8为根据本发明的实施例的步骤406的流程示意图；

[0103] 图9为根据本发明的实施例的步骤407的流程示意图；

[0104] 图10为根据本发明的实施例的用于实施NG防火墙的方法的流程示意图；

[0105] 图11为根据本发明的实施例的用于实施NG防火墙的方法的另一流程示意图；

- [0106] 图12为根据本发明的实施例的终端设备的结构示意图；
- [0107] 图13为根据本发明的实施例的终端设备的结构示意图；
- [0108] 图14为根据本发明的实施例的NG防火墙服务器的结构示意图；
- [0109] 图15为根据本发明的实施例的NG防火墙服务器的另一结构示意图；
- [0110] 图16为根据本发明的实施例的终端设备的结构示意图；
- [0111] 图17为根据本发明的实施例的NG防火墙服务器的结构示意图；
- [0112] 图18为根据本发明的实施例的用于实施NG防火墙的系统的结构示意图。

## 具体实施方式

[0113] 各实施例的许多特征和优点在详细说明书中显而易见，因此，所附权利要求书意图涵盖属于其真实精神和范围内的实施例的所有此类特征和优点。此外，由于所属领域的技术人员将容易想到多种修改和变化，因而并不希望将发明性实施例限于所说明并描述的确切构造和操作，因此，可以采取的所有适当修改和等效物均属于相应范围内。

[0114] 下文参考附图来描述本发明的实施例。

### [0115] 实施例1

[0116] 本发明的该实施例提供一种用于实施NG防火墙的方法，该方法应用在NG防火墙客户端中。

[0117] 图1是根据本发明的实施例1的用于实施NG防火墙的方法的流程示意图。如图1所示，所述方法包括：

[0118] 步骤101，当应用在配置有NG防火墙客户端的终端设备中被启动时，NG防火墙客户端发送请求消息给NG防火墙服务器，其中，请求消息用于请求应用的安全信息。

[0119] 步骤102，NG防火墙客户端从NG防火墙服务器接收响应消息；其中应用的安全消息包含在响应消息中；应用的安全信息表示在终端设备中启动的应用的安全保护的信息。

[0120] 步骤103，NG防火墙客户端通过使用应用的安全信息处理应用的数据。

[0121] 在该实施例中，NG防火墙客户端可以配置在终端设备中，终端设备可以是固定设备或无线设备，例如，智能手机、平板电脑。应用可以是社交软件（例如，Skype、youtube），并且可能已经安装在终端设备中。然而，并不限于此，可根据实际需要来确定特定实施方式。

[0122] 在该实施例中，NG防火墙服务器具有一个含有NG防火墙的数据或信息的NG-FW数据库。关于NG-FW数据库的详情，请参考现有技术。NG防火墙服务器可以通过终端设备（例如智能手机）的任意接口，例如，蓝牙、USB端口或任何空中接口进行连接。

[0123] 在该实施例中，应用的安全信息可包括：应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。然而，并不限于此，可根据实际需要来确定特定实施方式。

[0124] 图2为图示关于终端设备和NG防火墙服务器的结构的示例的示意图。应注意的是该图仅是示例性的，其他类型的结构可用于补充或替换此结构。

[0125] 如图2所示，配置有NG-FW客户端的终端设备中存在一些应用；同时配置有数据库的NG-FW服务器中存在这些应用的安全信息（例如应用的攻击防范数据）。

[0126] 例如，存储应用的安全信息的数据库可以配置在NG-FW服务器中；换句话说，数据库是NG-FW服务器的本地数据库。在另一示例中，存储应用的安全信息的数据库可以单独配

置;NG-GW服务器可以通过通信接口访问该数据库。然而,并不限于此。

[0127] 在该实施例中,NG-FW是终端设备(智能手机等)的强制要求之一以实现BYOD,获得个人理财和战略业务信息以及安全个人信息。智能手机是电池操作设备,还具有有限的计算资源。

[0128] 随着移动VAS(增值业务)的数量呈指数级增长,攻击的数量也将呈指数级增长,因此NG-FW的软件占用空间以及使用复杂应用框架处理每种类型的攻击将会很昂贵。显然,移动用户同时将使用数量非常有限的应用。

[0129] 在该实施例中,例如,基于NG-FW的穷尽攻击防范可以安装在集中式实体上,例如,在环境中的分组核心网、辅助存储器,或服务器中。当智能手机用户启动任何应用时,攻击防范请求将被发送到NG-FW数据库。智能手机将安装应用特定攻击防范、接入控制列表以及应用签名。任何Rx/Tx报文将检查新安装的攻击防范,这样入口和出口应用的接入控制就可以在智能手机上实现。

[0130] 从上述实施例可以看出:当应用在配置有NG防火墙客户端的终端设备中被启动时,NG防火墙客户端向NG防火墙服务器请求应用的安全信息。因此,本发明的实施例可以实现动态加载攻击防范,从而终端设备所需的软件占用空间可以减少,并且安装在终端设备上的应用的性能可以得到提高。

[0131] 实施例2

[0132] 基于实施例1,本发明的该实施例提供一种用于实施NG防火墙的方法;相同内容将不再予以描述。

[0133] 图3为根据本发明的实施例的用于实施NG防火墙的方法的流程示意图。如图3所示,该方法包括:

[0134] 步骤301,当应用在配置有NG防火墙客户端的终端设备中被启动时,NG防火墙客户端发送请求消息给NG防火墙服务器,其中该请求消息用于请求所述应用的安全信息。

[0135] 在该实施例中,请求消息可包括应用的识别信息,例如,应用的标识符或应用的种类;应用的识别信息由NG防火墙服务器用来确定应用的安全信息。然而,并不限于此,可根据实际需要来确定特定实施方式。

[0136] 步骤302,NG防火墙从NG防火墙服务器接收包含应用的安全信息的响应消息。

[0137] 步骤303,NG防火墙客户端通过使用应用的安全信息处理应用的数据。

[0138] 如图3所示,该方法可进一步包括:

[0139] 步骤304,当应用在终端设备中关闭时,NG防火墙客户端清除应用的安全信息。

[0140] 在该实施例中,一旦智能手机结束或关闭应用(例如Skype),应用的安全信息(例如,所有安装和下载的数据、应用接入列表和签名)被清空。

[0141] 图4是根据本发明的实施例的用于实施NG防火墙的方法的另一流程示意图。终端设备配置有NG-FW客户端。如图4所示,该方法可包括:

[0142] 步骤401,在终端设备中启用NG防火墙功能。

[0143] 步骤402,在终端设备中配置NG防火墙服务器的IP地址和端口号。

[0144] 在该步骤中,终端设备可基于NG防火墙服务器的IP地址和端口号生成请求消息。

[0145] 步骤403,当应用在终端设备中被启动时,终端设备发送请求消息给NG防火墙服务器;其中请求消息用于请求应用的安全信息并包括应用的识别信息。

[0146] 步骤404,NG防火墙服务器在接收请求消息之后根据请求消息中包含的应用的识别信息确定应用的安全信息。

[0147] 在该实施例中,NG-FW服务器可发送响应消息给终端设备;应用的安全信息包含在响应消息中。

[0148] 此外,用于保存应用的部分或全部安全信息的一个或多个定时器值可包含在响应消息中。

[0149] 例如,响应消息中存在一个定时器值,用于应用的所有安全信息;或存在一个定时器值,用于应用的报文签名信息;另一定时器值,用于应用的接入控制列表信息;以及另一定时器值,用于应用的畸形攻击信息。然而,并不限于此,可根据实际需要来确定特定实施方式。

[0150] 步骤405,NG防火墙从NG防火墙服务器接收包含应用的安全信息的响应消息。

[0151] 步骤406,NG防火墙客户端通过使用应用的安全信息处理应用的数据。

[0152] 在该实施例中,当对应于应用的部分安全信息的一个或多个定时器值中的一个或多个定时器超时,终端设备可重新请求应用的部分安全信息。

[0153] 或者,当对应于应用的全部安全信息的一个或多个定时器值中的一个或多个定时器超时,终端设备可重新请求应用的全部安全信息。

[0154] 例如,如果响应消息中存在用于应用的全部安全信息的定时器值A,则当对应于定时器值A的定时器超时,终端设备可重新请求应用的全部安全信息。

[0155] 又例如,如果响应消息中有三个定时器值:用于应用的报文签名信息的定时器值B、用于应用的接入控制列表信息的定时器值C以及用于应用的畸形攻击信息的定时器值D,则当对应于定时器值B的定时器超时,终端设备可重新请求应用的报文签名信息;或当对应于定时器值C的定时器超时,终端设备可重新请求应用的接入控制列表信息;或当对应于定时器值D的定时器超时,终端设备可重新请求应用的畸形攻击信息。

[0156] 如图4所示,该方法可进一步包括:

[0157] 步骤407,当应用在终端设备中关闭时,终端设备清除应用的安全信息。

[0158] 在该步骤中,终端设备还可基于定时器清除应用的安全信息。终端设备将在定时器超时清除应用的安全信息。

[0159] 例如,当对应于应用的部分安全信息的一个或多个定时器值中的一个或多个定时器超时,终端设备可清除应用的部分安全信息。或者,当对应于应用的全部安全信息的一个或多个定时器值中的一个或多个定时器超时,终端设备可清除应用的全部安全信息。

[0160] 在步骤401中,在终端设备上启用NG-FW客户端(其具有NG防火强功能)。可以允许每个应用来选择终端设备用户是否想要启用NG-FW攻击应用。默认所有的应用都不允许从NG-FW服务器上下载。

[0161] 在步骤402中,NG防火墙服务器信息,例如NG防火墙服务器的端口号和IP地址,可由用户在终端设备中配置。此外,用于保存应用的安全信息的定时器值可由用户在终端设备中配置。

[0162] 在该实施例中,应用的安全信息可包括以下信息的任意一项或组合:应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。

[0163] 其中存在不同的定时器值用于保存以下信息的任意一项或组合：应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。

[0164] 或者，存在相同的定时器值用于保存以下信息的任意一项或组合：应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。

[0165] 在该实施例中，通过使用应用的安全信息处理应用的数据的过程可包括：通过使用应用的报文签名信息处理应用的数据，或通过使用应用的接入控制列表信息处理应用的数据，或通过使用应用的畸形攻击信息处理应用的数据，或通过使用应用的状态防火墙库信息处理应用的数据，或通过使用应用的报文限速策略信息处理应用的数据。

[0166] 图5为根据本发明的实施例的步骤402的流程示意图。如图5所示，终端设备判断现有策略中是否存在任何变化；例如，判断安全配置是否是默认配置（步骤501）。

[0167] 当配置不是默认配置时，在终端设备中配置端口号和IP地址（步骤502）。此外，可以配置用于保存应用的安全信息的定时器。

[0168] 在步骤403中，例如，终端设备的用户启动“Skype”等应用进行社交活动。事件将被发送给在终端设备上运行的NG-FW客户端。终端设备将生成请求消息以请求应用的安全信息。该请求消息可以基于任何传送机制。

[0169] 在实施中，应用的安全信息可包括：应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击、应用的状态防火墙库信息以及应用的报文限速策略信息等。

[0170] 图6为根据本发明的实施例的步骤403的流程示意图。如图6所示，终端设备可判断安全信息是否是默认配置（步骤601）。当配置不是默认配置时，终端设备可触发事件（步骤602），例如发送消息给在终端设备中配置的NG-FW客户端。

[0171] 随后，终端设备可判断NG-FW数据库是否退出应用（步骤603）。当NG-FW数据库未退出应用时，终端设备发送请求应用的安全信息的请求消息（步骤604）。

[0172] 如图6所示，终端设备可判断是否发生超时或是否接收到确认消息（步骤605）；如果否，终端设备将继续下载应用的安全信息和更新现有策略（步骤606）。随后，使用现有应用策略和安全机制（即，攻击防范机制）（步骤607）。

[0173] 在步骤403中，请求消息可基于作为传送协议的UDP（用户数据报协议）生成。请求消息的格式如下所示。

[0174]

智能手机请求消息



[0175] 在步骤405中,NG防火墙服务器发送应用的安全信息,例如,所有攻击防范策略、NG-FW应用和签名。

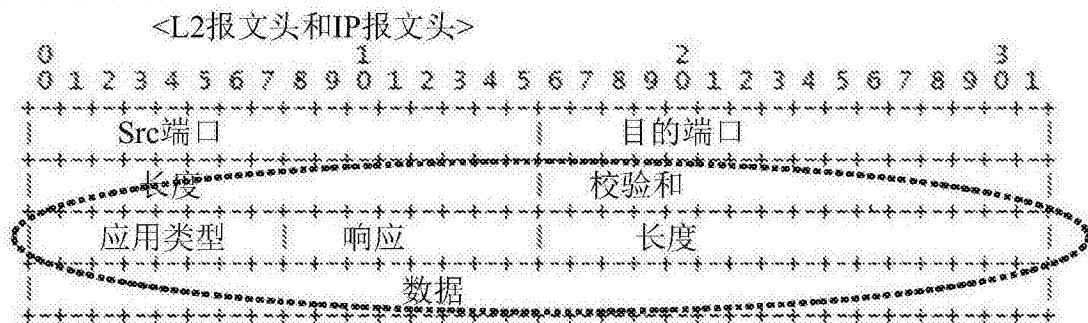
[0176] 图7为根据本发明的实施例的步骤405的流程示意图。如图7所示,NG防火墙服务器从终端设备接收请求消息(步骤701)。随后,NG防火墙服务器可判断是否对终端设备进行认证(步骤702)。

[0177] 如图7所示,当终端设备认证为有效用户时,NG防火墙服务器将确定应用的安全信息(步骤703),例如最新的攻击防范策略和库。随后,NG防火墙服务器可判断NG-FW数据库是否退出应用(步骤704)。当NG-FW数据库未退出应用时,NG防火墙服务器将发送应用的安全信息(例如,应用特定攻击防范和更新的现有策略)给终端设备(步骤705)。随后,NG防火墙服务器可发送确认消息(步骤706)。

[0178] 在步骤405中,包含应用的安全信息的响应消息可基于作为传送协议的UDP生成。响应消息的格式如下所示。

[0179]

智能手机请求消息



[0180] 在步骤406中,终端设备下载NG-FW应用并在数据平面中安装应用接入列表和签名。来自/到达终端设备的应用的任意接收/发送的报文将由应用的安全信息处理。

[0181] 图8为根据本发明的实施例的步骤406的流程示意图。如图8所示,终端设备从NG-FW服务器接收应用的安全信息(步骤801),例如应用特定攻击防范。随后,终端设备判断是否对NG防火墙服务器进行认证(步骤802)。当NG防火墙服务器被认证时,终端设备下载应用的所有安全信息,例如所有攻击防范机制。

[0182] 在步骤407中,一旦终端设备的用户结束或关闭应用(例如Skype),应用的安全信息(包括所有安装和下载的应用接入列表和签名)将被清空。

[0183] 图9为根据本发明的实施例的步骤407的流程示意图。如图9所示,终端设备可进一步判断其是否超时(步骤901);当其超时,终端设备发送消息以清除下载的数据(步骤902)。

[0184] 从上述实施例可以看出:当应用在配置有NG防火墙客户端的终端设备中被启动时,NG防火墙客户端向NG防火墙服务器请求应用的安全信息。因此,本发明的实施例可以实现动态加载攻击防范,从而终端设备所需的软件占用空间可以减少,并且安装在终端设备上的应用的性能可以得到提高。

[0185] 此外,终端设备将受到保护,免遭来自新应用或服务的新攻击。由于攻击防范的数量直接依赖于用户正在使用的应用的数量,所以信令报文将减少,这样有助于延长移动终端的电池寿命。

[0186] 实施例3

[0187] 本发明的该实施例提供一种用于实施NG防火墙的方法,该方法应用在NG防火墙服务器中。该实施例对应于上述实施例1或2,并且相同内容将不再予以描述。

[0188] 图10是根据本发明的实施例的用于实施NG防火墙的方法的流程示意图。如图10所示,该方法包括:

[0189] 步骤1001,NG防火墙服务器从终端设备接收请求消息,其中请求消息用于请求应用的安全信息;应用的安全信息表示在终端设备中启动的应用的安全保护的信息。

[0190] 步骤1002,NG防火墙服务器根据请求消息确定应用的安全信息。

[0191] 步骤1003,NG防火墙服务器发送包含应用的安全信息的响应消息给终端设备。

[0192] 在该实施例中,应用的安全信息包括:应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。然而,并不限于此,可根据实际需要来确定特定实施方式。

[0193] 图11是根据本发明的实施例的用于实施NG防火墙的方法的另一流程示意图。如图11所示,所述方法包括:

[0194] 步骤1101,NG防火墙服务器从终端设备接收请求消息,其中请求消息用于请求应用的安全信息;应用的安全信息表示在终端设备中启动的应用的安全保护的信息。

[0195] 步骤1103,NG防火墙服务器根据请求消息确定应用的安全信息。

[0196] 在该实施例中,根据请求消息确定应用的安全信息的过程可包括:根据请求消息中包含的应用的识别信息从数据库中获取应用的安全信息。

[0197] 例如,存储应用的安全信息的数据库可以配置在NG-FW服务器中;换句话说,数据库是NG-FW服务器的本地数据库。在另一示例中,存储应用的安全信息的数据库可以单独配置;NG-GW服务器可以通过通信接口访问该数据库。然而,并不限于此。

[0198] 步骤1104,NG防火墙服务器发送包含应用的安全信息的响应消息给终端设备。

[0199] 如图11所示,该方法可进一步包括:

[0200] 步骤1102,NG防火墙服务器认证请求消息是否有效。当请求消息有效时,执行发送包含应用的安全信息的响应消息给终端设备的过程。

[0201] 在该实施例中,用于保存应用的部分或全部安全信息的一个或多个定时器值可包含在响应消息中。

[0202] 该方法可进一步包括:确定用于保存应用的部分或全部安全信息的一个或多个定时器值;发送包含应用的安全信息的响应消息给终端设备(步骤1104)可包括:发送包含应用的安全信息的响应消息,以及用于保存应用的部分或全部安全信息的一个或多个定时器值给终端设备。

[0203] 应注意,在上述网络环境中,由NG-FW服务器发回的应用的安全信息对于终端设备的不同应用可能有所不同。或者,NG-FW服务器可发回不同的安全信息用于终端设备的不同请求消息。然而,并不限于此,可根据实际需要来确定特定实施方式。

[0204] 从上述实施例可以看出:当应用在配置有NG防火墙客户端的终端设备中被启动时,NG防火墙客户端向NG防火墙服务器请求应用的安全信息。因此,本发明的实施例可以实现动态加载攻击防范,从而终端设备所需的软件占用空间可以减少,并且安装在终端设备上的应用的性能可以得到提高。

#### [0205] 实施例4

[0206] 本发明的该实施例进一步提供在终端设备中配置的NG防火墙客户端。该实施例对应于上述实施例1的方法,并且相同内容将不再予以描述。

[0207] 图12为根据本发明的实施例的NG防火墙客户端的结构示意图。如图12所示,NG防火墙客户端1200包括:发送单元1201、接收单元1202以及处理单元1203。NG防火墙客户端的其他部件可以参考现有技术并且在本发明中不再予以描述。然而,并不限于此,可根据实际需要来确定特定实施方式。

[0208] 其中发送单元1201用于,当应用在配置有NG防火墙客户端的终端设备中被启动时,发送请求消息以请求应用的安全信息;接收单元1202用于接收包含应用的安全信息的响应消息;处理单元1203用于通过使用应用的安全信息处理应用的数据。

[0209] 在该实施例中,发送单元1201可具体用于,当应用在配置有NG防火墙客户端的终端设备中被启动时,发送用于请求应用的安全信息的请求消息给NG防火墙服务器;其中请求消息包含应用的识别信息,以及应用的识别信息由NG防火墙服务器用来确定应用的安全信息。

[0210] 从上述实施例可以看出:当应用在配置有NG防火墙客户端的终端设备中被启动时,NG防火墙客户端向NG防火墙服务器请求应用的安全信息。因此,本发明的实施例可以实现动态加载攻击防范,从而终端设备所需的软件占用空间可以减少,并且安装在终端设备上的应用的性能可以得到提高。

#### [0211] 实施例5

[0212] 本发明的该实施例进一步提供在终端设备中配置的NG防火墙客户端。该实施例对应于上述实施例2的方法,并且相同内容将不再予以描述。

[0213] 图13为根据本发明的实施例的NG防火墙客户端的结构示意图。如图13所示,NG防火墙客户端1300包括:发送单元1201、接收单元1202以及处理单元1203,如上述实施例4所述。

[0214] 如图13所示,NG防火墙客户端1300可进一步包括:清除单元1304。清除单元1304用于,当应用在终端设备中关闭时,清除应用的安全信息。

[0215] 如图13所示,NG防火墙客户端1300可进一步包括:开启单元1305、配置单元1306以及生成单元1307。其中,开启单元1305用于启用NG防火墙功能;配置单元1306用于配置NG防火墙服务器的IP地址和端口号;生成单元1307用于生成请求消息。

[0216] 在该实施例中,响应消息可进一步包括用于保存应用的部分或全部安全信息的一个或多个定时器值;以及发送单元进一步用于,当对应于应用的部分安全信息的一个或多个定时器值中的一个或多个定时器超时,重新请求应用的部分安全信息,或当对应于应用的全部安全信息的一个或多个定时器值中的一个或多个定时器超时,重新请求应用的全部安全信息。

[0217] 在该实施例中,清除单元可进一步用于,当对应于应用的部分安全信息的一个或多个定时器值中的一个或多个定时器超时,清除应用的部分安全信息,或当对应于应用的全部安全信息的一个或多个定时器值中的一个或多个定时器超时,清除应用的全部安全信息。

[0218] 在该实施例中,应用的安全信息可包括以下信息的任意一项或组合:应用的报文

签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。

[0219] 其中处理单元1203可具体用于：通过使用应用的报文签名信息处理应用的数据，或通过使用应用的接入控制列表信息处理应用的数据，或通过使用应用的畸形攻击信息处理应用的数据，或通过使用应用的状态防火墙库信息处理应用的数据，或通过使用应用的报文限速策略信息处理应用的数据。

[0220] 从上述实施例可以看出：当应用在配置有NG防火墙客户端的终端设备中被启动时，NG防火墙客户端向NG防火墙服务器请求应用的安全信息。因此，本发明的实施例可以实现动态加载攻击防范，从而终端设备所需的软件占用空间可以减少，并且安装在终端设备上的应用的性能可以得到提高。

[0221] 此外，终端设备将受到保护，免遭来自新应用或服务的新攻击。由于攻击防范的数量直接依赖于用户正在使用的应用的数量，所以信令报文将减少，这样有助于延长移动终端的电池寿命。

[0222] 实施例6

[0223] 本发明的该实施例进一步提供NG防火墙服务器。该实施例对应于上述实施例3的方法，并且相同内容将不再予以描述。

[0224] 图14为根据本发明的实施例的NG防火墙服务器的结构示意图。如图14所示，终端设备1400包括：接收单元1401、第一确定单元1402以及发送单元1403。NG防火墙客户端的其他部件可以参考现有技术并且在本发明中不再予以描述。然而，并不限于此，可根据实际需要来确定特定实施方式。

[0225] 其中，接收单元1401用于从终端设备接收请求消息以请求应用的安全信息；第一确定单元1402用于根据请求消息确定应用的安全信息；发送单元1403用于发送包含应用的安全信息的响应消息给终端设备。

[0226] 图15为根据本发明的实施例的NG防火墙服务器的另一示意图。如图15所示，NG防火墙服务器1500包括：接收单元1401、第一确定单元1402以及发送单元1403，如上述实施例所述。

[0227] 在该实施例中，请求消息可包括应用的识别信息；以及第一确定单元1402具体用于根据请求消息中包含的应用的识别信息从数据库中获取应用的安全信息。

[0228] 如图15所示，NG防火墙服务器1500可进一步包括：认证单元1503；认证单元1503用于认证请求消息是否有效。发送单元1403具体用于，当请求消息有效时，发送包含应用的安全信息的响应消息给终端设备。

[0229] 在此实施例中，NG防火墙服务器1500可以进一步包括：第二确定单元1504，用于确定用于保存应用的部分或全部安全信息的一个或多个定时器值。

[0230] 发送单元1403具体用于发送包含应用的安全信息的响应消息，以及用于保存应用的部分或全部安全信息的一个或多个定时器值给终端设备。

[0231] 在该实施例中，应用的安全信息可包括以下信息的任意一项或组合：应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。

[0232] 从上述实施例可以看出：当应用在配置有NG防火墙客户端的终端设备中被启动

时,NG防火墙客户端向NG防火墙服务器请求应用的安全信息。因此,本发明的实施例可以实现动态加载攻击防范,从而终端设备所需的软件占用空间可以减少,并且安装在终端设备上的应用的性能可以得到提高。

[0233] 此外,终端设备将受到保护,免遭来自新应用或服务的新攻击。由于攻击防范的数量直接依赖于用户正在使用的应用的数量,所以信令报文将减少,这样有助于延长移动终端的电池寿命。

[0234] 实施例7

[0235] 本发明的该实施例进一步提供配置有NG-FW客户端的终端设备。该实施例对应于上述实施例1-2的方法,并且相同内容将不再予以描述。

[0236] 在该实施例中,终端设备包括处理器和耦合至处理器的存储器。

[0237] 图16为根据本发明的实施例的终端设备的示意结构图。如图16所示,存在处理器41和耦合至处理器41的存储器42。

[0238] 存储器42用于存储程序。具体而言,程序可以包括程序代码,而程序代码包括计算机操作指令。

[0239] 处理器41用于:当应用在终端设备中被启动时,发送用于请求应用的安全信息的请求消息给NG防火墙服务器;从NG防火墙服务器接收包含应用的安全信息的响应消息;通过使用应用的安全信息处理应用的数据。

[0240] 存储器42可包括高速RAM和非易失性存储器。处理器41可以是中央处理单元(CPU),或可以是专用集成电路(ASIC),或可以用于一个或多个ASIC。

[0241] 根据上述终端设备,请求消息包含应用的识别信息,而应用的识别信息由NG防火墙服务器用来确定应用的安全信息。

[0242] 根据上述终端设备,处理器41进一步用于:当应用在终端设备中关闭时,清除应用的安全信息。

[0243] 根据上述终端设备,响应消息进一步包括用于保存应用的部分或全部安全信息的一个或多个定时器值。

[0244] 处理器41进一步用于:当对应于应用的部分安全信息的一个或多个定时器值中的一个或多个定时器超时,重新请求应用的部分安全信息,或当对应于应用的全部安全信息的一个或多个定时器值中的一个或多个定时器超时,重新请求应用的全部安全信息。

[0245] 根据上述终端设备,处理器41进一步用于:当对应于应用的部分安全信息的一个或多个定时器值中的一个或多个定时器超时,清除应用的部分安全信息,或当对应于应用的全部安全信息的一个或多个定时器值中的一个或多个定时器超时,清除应用的全部安全信息。

[0246] 根据上述终端设备,应用的安全信息包括以下信息的任意一项或组合:应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。

[0247] 根据上述终端设备,存在不同的定时器值用于保存以下信息的任意一项或组合:应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息;或者,存在相同的定时器值用于保存以下信息的任意一项或组合:应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应

用的状态防火墙库信息以及应用的报文限速策略信息。

[0248] 根据上述终端设备,在通过使用应用的安全信息处理应用的数据的步骤中,处理器41进一步用于:通过使用应用的报文签名信息处理应用的数据,或通过使用应用的接入控制列表信息处理应用的数据,或通过使用应用的畸形攻击信息处理应用的数据,或通过使用应用的状态防火墙库信息处理应用的数据,或通过使用应用的报文限速策略信息处理应用的数据。

[0249] 此外,如图16所示,还可存在通信接口43,用于完成终端设备和NG防火墙服务器或其他设备之间的通信。

[0250] 如图16所示,终端设备还可包括磁盘44,用于存储待测试的程序和待测试程序的过程的状态信息。

[0251] 或者,在特定实施方式中,如果存储器42、处理器41、通信接口43以及磁盘44可以单独实施,则存储器42、处理器41、通信接口43以及磁盘44可以通过BUS进行通信连接。BUS可以是工业标准结构 (ISA) BUS、外围部件互连标准 (PCI) BUS或扩充工业标准体系结构 (EISA) BUS等等。BUS可以划分成地址BUS、数据BUS和控制BUS等等。为了便于表示,BUS仅由单根粗线表示,但不意味这仅存在一个BUS或一类BUS。

[0252] 或者,在特定实施方式中,如果存储器42、处理器41、通信接口43以及磁盘44可以集成在单个芯片中,则存储器42、处理器41、通信接口43以及磁盘44可以通过内部接口进行通信连接。

[0253] 本发明的实施例的有益效果在于:当应用在终端设备中被启动时,终端设备向NG防火墙服务器请求应用的安全信息。因此,本发明的实施例可以实现动态加载攻击防范,从而终端设备所需的软件占用空间可以减少,并且安装在终端设备上的应用的性能可以得到提高。

[0254] 此外,终端设备将受到保护,免遭来自新应用或服务的新攻击。由于攻击防范的数量直接依赖于用户正在使用的应用的数量,所以信令报文将减少,这样有助于延长移动终端的电池寿命。

[0255] 本发明还提供了一种非瞬时计算机可读存储介质,包含计算机程序代码,当计算机处理器执行计算机程序代码时,致使计算机处理器根据本发明的实施例执行用于实施NG防火墙的方法。

[0256] 通过上面描述的实施例,所属领域的技术人员可清楚地明白本发明可由软件和必要的通用硬件实施。具体而言,本发明还可仅由硬件实施。然而,前者是优选的实施模式。根据这样的理解,本发明的技术解决方案的本质或对现有技术做出贡献的本发明的部分技术解决方案可采用软件产品的形式实施。计算机软件产品存储在可读存储介质,例如,计算机软盘、硬盘或光盘中,并包括多个使计算机设备(其可以是个人计算机、服务器或网络设备)执行本发明的实施例中描述的方法。

[0257] 实施例8

[0258] 本发明的该实施例提供NG-FW服务器。该实施例对应于上述实施例3的方法,并且相同内容将不再予以描述。

[0259] 在该实施例中,NG-FW服务器包括:处理器和耦合至处理器的存储器。

[0260] 图17为根据本发明的实施例的NG-FW服务器的示意结构图。如图17所示,存在处理

器51和耦合至处理器51的存储器52。

[0261] 存储器52用于存储程序。具体而言,程序可以包括程序代码,而程序代码包括计算机操作指令。

[0262] 处理器51用于:从终端设备接收用于请求应用的安全信息的请求消息,其中应用的安全信息表示在终端设备中启动的应用的安全保护的信息;根据请求消息确定应用的安全信息;发送包含应用的安全信息的响应消息给终端设备。

[0263] 存储器52可包括高速RAM和非易失性存储器。处理器51可以是中央处理单元(CPU),或可以是专用集成电路(ASIC),或可以用于一个或多个ASIC。

[0264] 根据上述NG-FW服务器,请求消息包括应用的识别信息;在根据请求消息确定应用的安全信息的步骤中,处理器51进一步用于:根据请求消息中包含的应用的识别信息从数据库中获取应用的安全信息。

[0265] 根据上述NG-FW服务器,处理器51进一步用于:认证请求消息是否有效;当请求消息有效时,执行发送包含应用的安全信息的响应消息给终端设备的过程。

[0266] 根据上述NG-FW服务器,处理器51进一步用于:确定用于保存应用的部分或全部安全信息的一个或多个定时器值;以及在发送响应消息的步骤中,处理器51进一步用于:发送包含应用的安全信息的响应消息,以及用于保存应用的部分或全部安全信息的一个或多个定时器值给终端设备。

[0267] 根据上述NG-FW服务器,应用的安全信息包括以下信息的任意一项或组合:应用的报文签名信息、应用的接入控制列表信息、应用的畸形攻击信息、应用的状态防火墙库信息以及应用的报文限速策略信息。

[0268] 此外,如图17所示,还可存在通信接口53,用于完成NG-FW服务器和终端设备或其他设备之间的通信。

[0269] 如图17所示,NG-FW服务器还可包括磁盘54,用于存储待测试的程序和待测试程序的过程的状态信息。

[0270] 或者,在特定实施方式中,如果存储器52、处理器51、通信接口53以及磁盘54可以单独实施,则存储器52、处理器51、通信接口53以及磁盘54可以通过BUS进行通信连接。BUS可以是工业标准结构(ISA) BUS、外围部件互连标准BUS或扩充工业标准体系结构(EISA) BUS等等。BUS可以划分成地址BUS、数据BUS和控制BUS等等。为了便于表示,BUS仅由单根粗线表示,但不意味这仅存在一个BUS或一类BUS。

[0271] 或者,在特定实施方式中,如果存储器52、处理器51、通信接口53以及磁盘54可以集成在单个芯片中,则存储器52、处理器51、通信接口53以及磁盘54可以通过内部接口进行通信连接。

[0272] 本发明的实施例的有益效果在于:当应用在终端设备中被启动时,终端设备向NG防火墙服务器请求应用的安全信息。因此,本发明的实施例可以实现动态加载攻击防范,从而终端设备所需的软件占用空间可以减少,并且安装在终端设备上的应用的性能可以得到提高。

[0273] 此外,终端设备将受到保护,免遭来自新应用或服务的新攻击。由于攻击防范的数量直接依赖于用户正在使用的应用的数量,所以信令报文将减少,这样有助于延长移动终端的电池寿命。

[0274] 本发明还提供了一种非瞬时计算机可读存储介质,包含计算机程序代码,当计算机处理器执行计算机程序代码时,致使计算机处理器根据本发明的实施例执行用于实施NG防火墙的方法。

[0275] 实施例9

[0276] 本发明的该实施例提供一种用于实施NG防火墙的系统。该实施例对应于上述实施例7和8,并且相同内容将不再予以描述。

[0277] 在该实施例中,用于实施NG防火墙的系统包括:如实施例7中描述的一个或多个终端设备以及如实施例8中描述的NG防火墙服务器。

[0278] 图18为根据本发明的实施例的用于实施NG防火墙的系统的示意结构图。如图18所示,在用于实施NG防火墙1800的系统中至少存在一个配置有NG-FW客户端1802的终端设备1801以及一个NG-FW服务器1803。

[0279] 本发明的实施例的有益效果在于:当应用在终端设备中被启动时,终端设备向NG防火墙服务器请求应用的安全信息。因此,本发明的实施例可以实现动态加载攻击防范,从而终端设备所需的软件占用空间可以减少,并且安装在终端设备上的应用的性能可以得到提高。

[0280] 此外,终端设备将受到保护,免遭来自新应用或服务的新攻击。由于攻击防范的数量直接依赖于用户正在使用的应用的数量,所以信令报文将减少,这样有助于延长移动终端的电池寿命。

[0281] 通过上面描述的实施例,所属领域的技术人员可清楚地明白本发明可由软件和必要的通用硬件实施。具体而言,本发明还可仅由硬件实施。然而,前者是优选的实施模式。根据这样的理解,本发明的技术解决方案的本质或对现有技术做出贡献的本发明的部分技术解决方案可采用软件产品的形式实施。计算机软件产品存储在可读存储介质,例如,计算机软盘、硬盘或光盘中,并包括多个使计算机设备(其可以是个人计算机、服务器或网络设备)执行本发明的实施例中描述的方法。

[0282] 从上述实施例可以看出:可以实现实施例的有益效果和优点:

[0283] (1) 减少针对终端设备(例如智能手机和其他终端设备)的NG防火墙软件的占用空间;

[0284] (2) 如果是一个不常用的应用,NG防火墙不会响应控制消息,这样终端不用处理,可以延长电池寿命;

[0285] (3) 减少应用特定接入列表(例如白名单或黑名单)的大小,这样可以实现更好的性能;

[0286] (4) 当关键业务应用启动时,将强制使用终端设备(例如智能手机)上的NG防火墙服务。

[0287] (5) 通过使用其他接口(例如,蓝牙、USB端口等等)控制关键信息;

[0288] (6) 在运行应用时将使用安全应用、数据以及应用接入控制。

[0289] 应理解,本发明的各部分可以由硬件、软件、固件或其组合来实施。在上述实施例中,多个步骤或方法可以由存储在存储器中的软件或固件来实现,并且由合适的指令执行系统来执行。例如,如果由硬件来实现,那么可以像在另一实施例中一样由所属领域已知的以下技术中的任一技术或其组合来实现:具有逻辑门电路的用于实现数据信号的逻辑功能

的离散逻辑电路、具有适当的组合逻辑门电路的专用集成电路、可编程门阵列 (PGA), 以及现场可编程门阵列 (FPGA) 等等。

[0290] 流程示意图中的描述或块或者采用其他形式的任何进程或方法应被理解成表明包括一个或多个模块、片段或部分, 以用于实现特定逻辑功能或进程中步骤的可执行指令的代码, 而且本发明的优选实施例的范围包括其他实施方案, 其中这些功能可以采用与所示或所述那些不同的方式来执行, 包括根据相关功能以基本上同步的方式或以相反的顺序来执行这些功能, 本发明相关领域的技术人员应理解上述内容。

[0291] 例如, 流程示意图中图示或本文以其他方式描述的逻辑和/或步骤应被理解为用于实现逻辑功能的可执行指令的顺序表, 它可以在任何计算机可读媒体中实施, 以供指令执行系统、设备或装置 (例如, 包括计算机的系统、包括处理器的系统, 或能够从指令执行系统、设备或装置中提取指令并执行这些指令的其他系统) 使用, 或者与指令执行系统、设备或装置结合使用。

[0292] 上述文字描述和附图示出了本发明的各种特征。应理解, 所属领域的技术人员可以准备合适的计算机代码, 以执行上文所述且附图所示的每个步骤和进程。还应理解, 所有的终端、计算机、服务器以及网络可以是任何类型的, 并且可以根据本发明来准备计算机代码, 以通过使用相应设备来实施本发明。

[0293] 本文中揭示了本发明的特定实施例。所属领域的技术人员将容易认识到, 本发明可以应用于其他环境。实际上, 存在许多实施例和实施方案。所附权利要求书并非意图将本发明的范围限于上述特定实施例。此外, 任何对“用于……的设备”的引用都是在解释设备加功能, 以描述元件和权利要求, 而且并不希望将任何未引用“用于……的设备”的元件理解为设备加功能的元件, 即使权利要求中包括词语“设备”也是如此。

[0294] 虽然已经示出了一项特定的实施例并且已经描述了本发明, 但很明显所属领域的技术人员在阅读并理解上述描述和附图后可以想到等效修改和变型。特别是对于由上述元件 (部分、组件、设备以及组成等等) 执行的各种功能而言, 除非另有规定, 否则希望描述这些元件的术语 (包括对“设备”的引用) 对应于执行这些元件的特定功能的任何元件 (即, 功能等效物), 即使该元件不同于执行本发明就相关结构所说明的一项或多项示例性实施例的功能的元件。此外, 尽管仅参考所述实施例中的一项或多项来描述本发明的特定特征, 但是此类特征可以根据需要并鉴于任何给定或特定应用的有利方面而与其他实施例的一个或多个其他特征相结合。

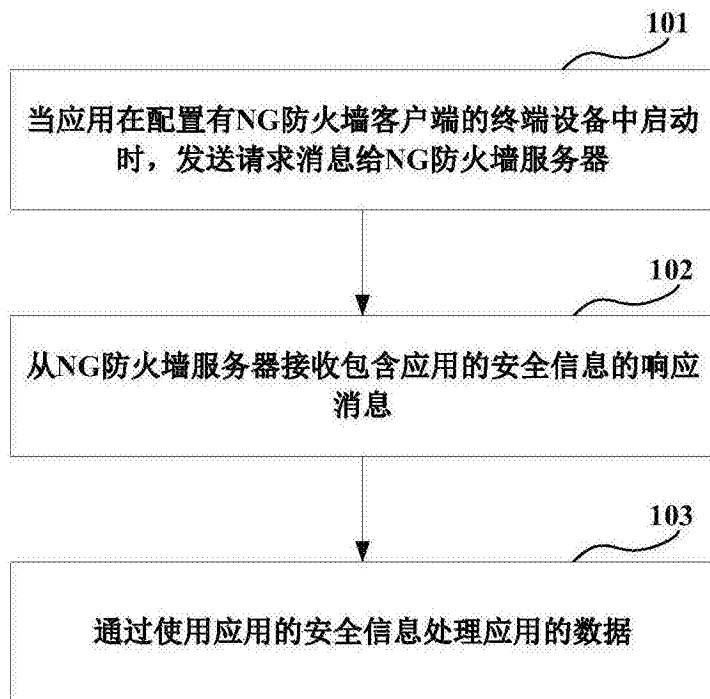


图1

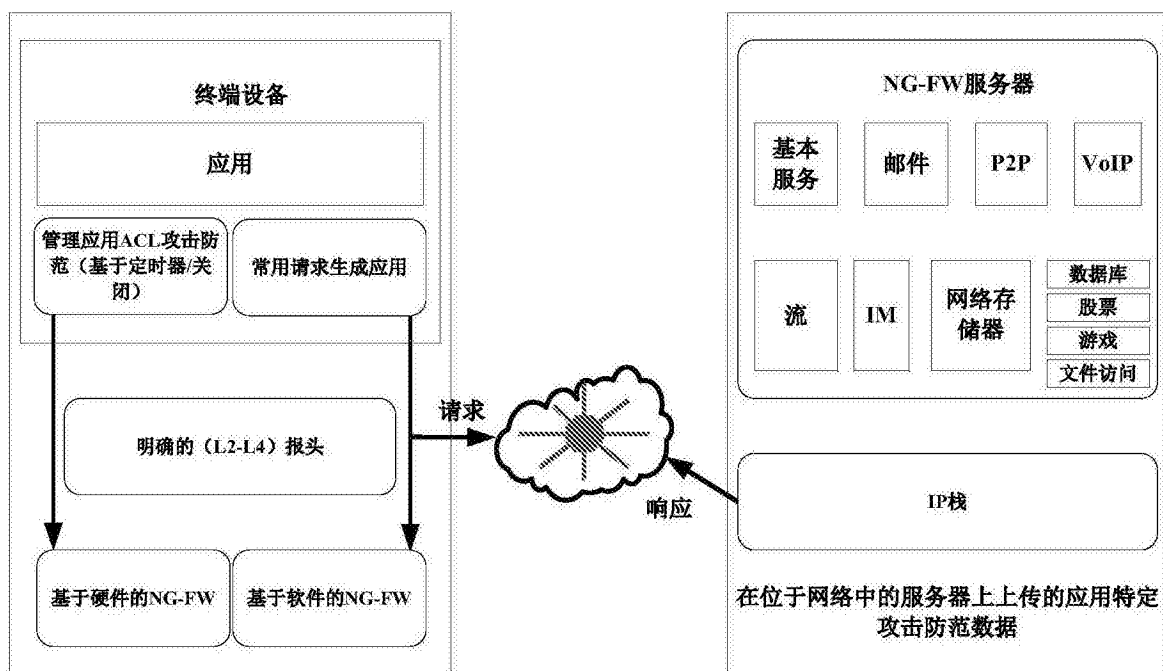


图2

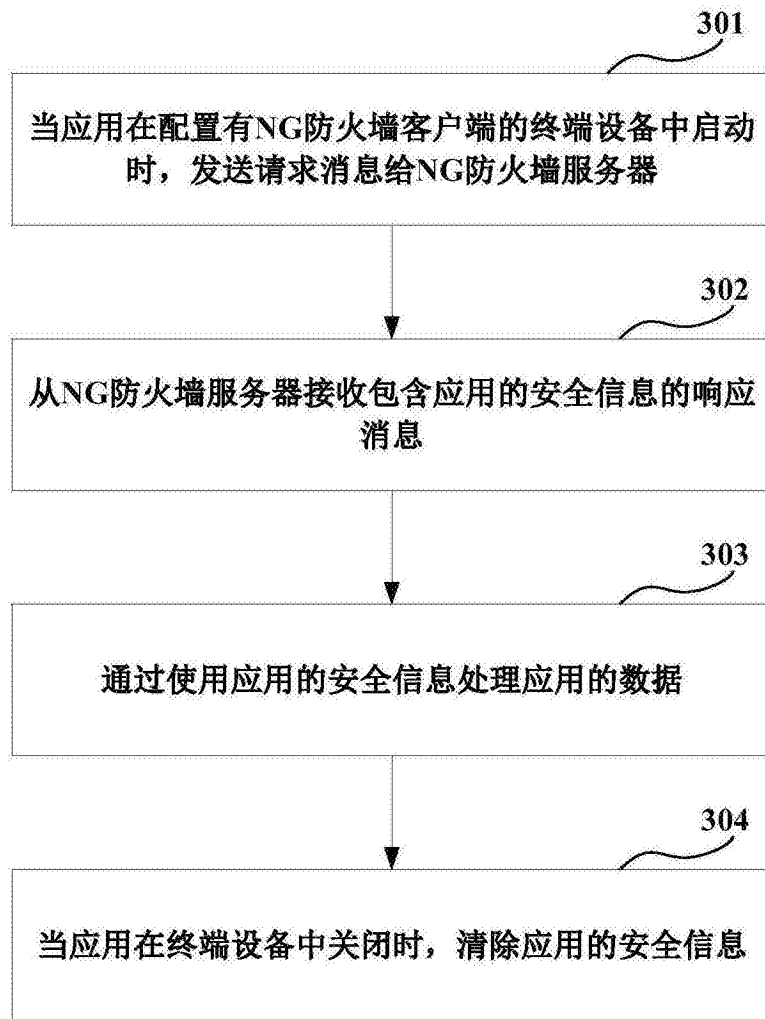


图3

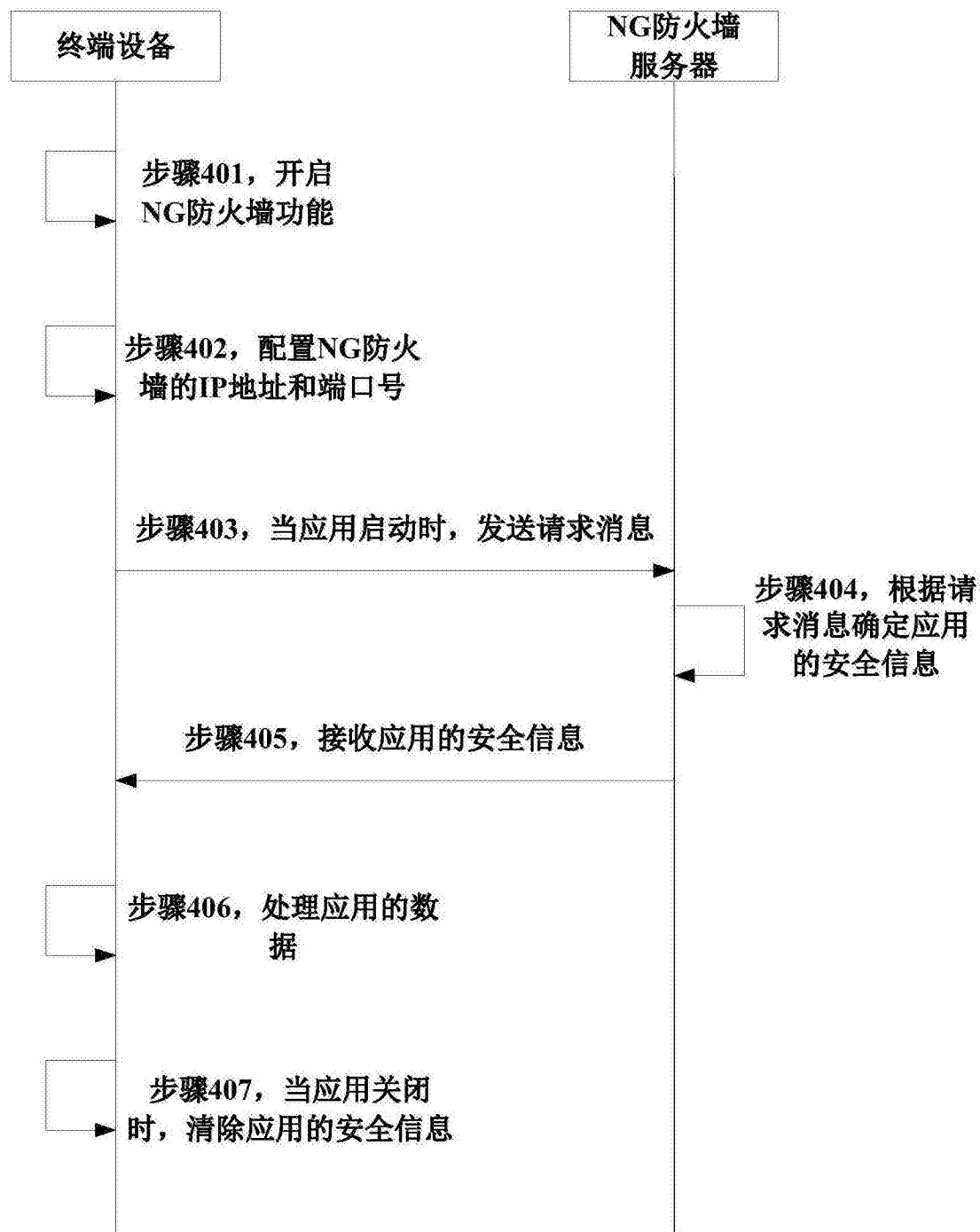


图4

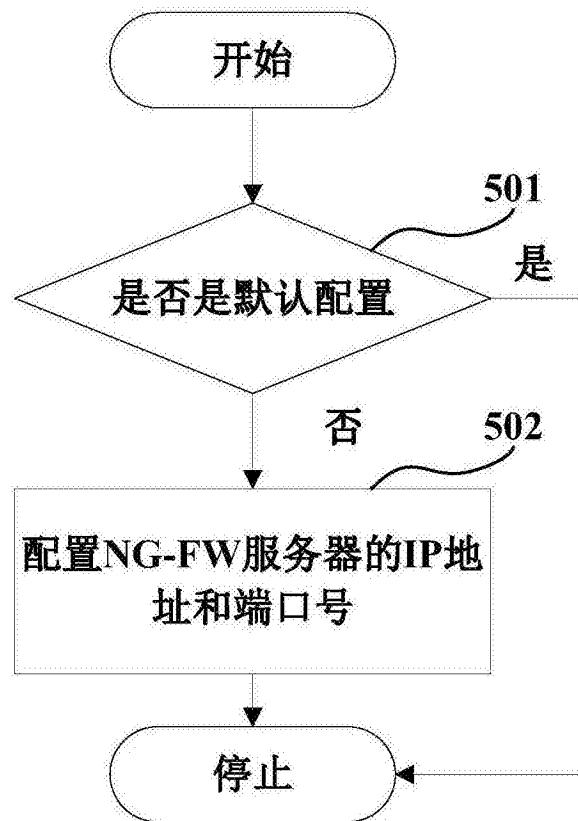


图5

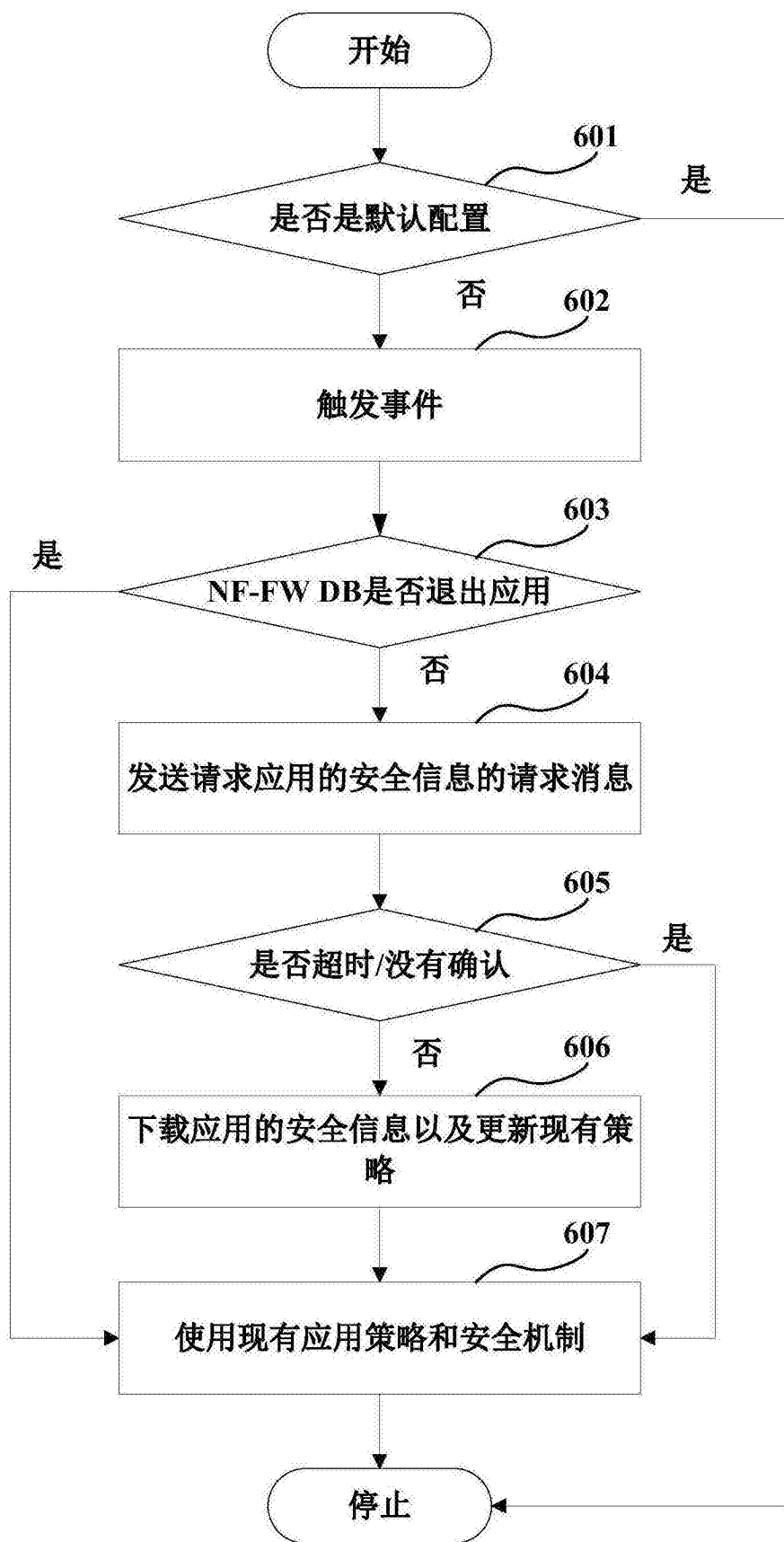


图6

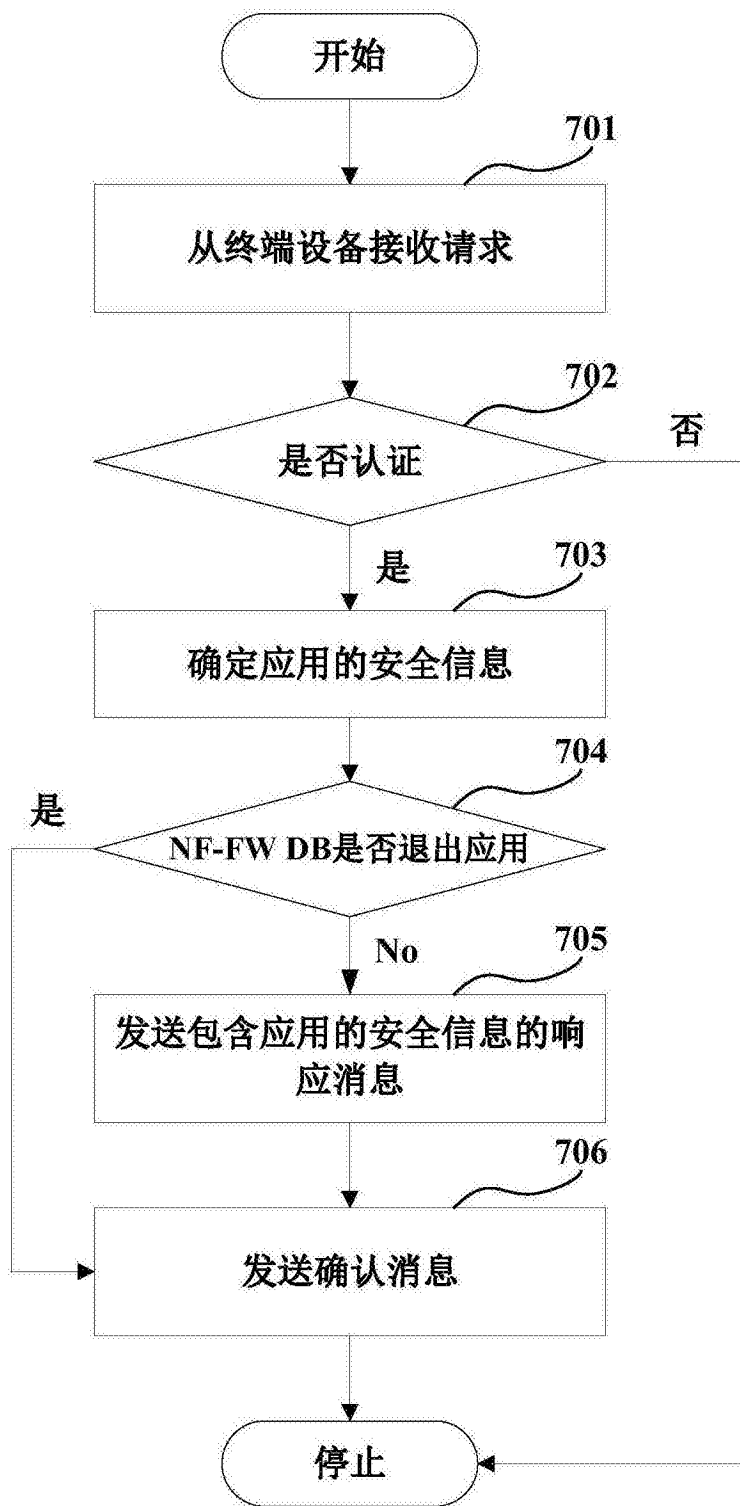


图7

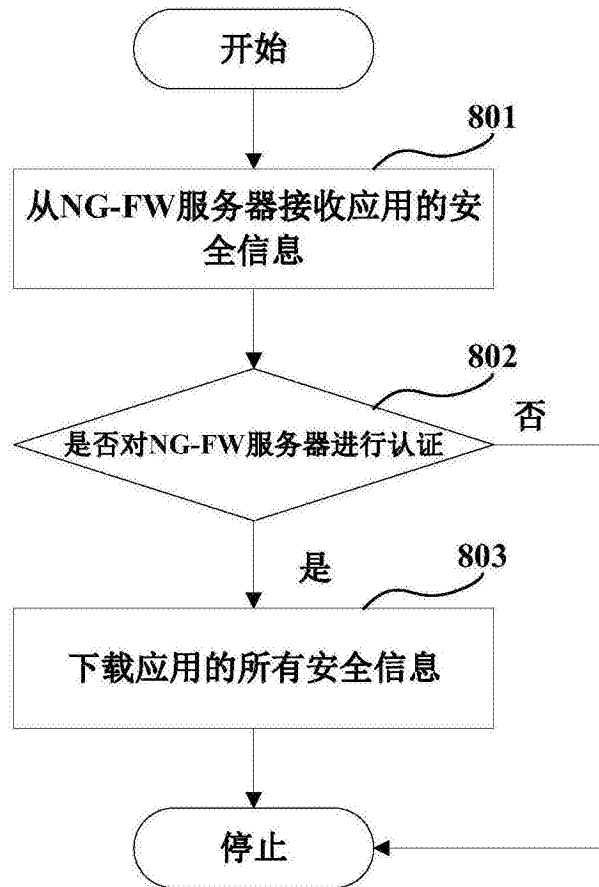


图8

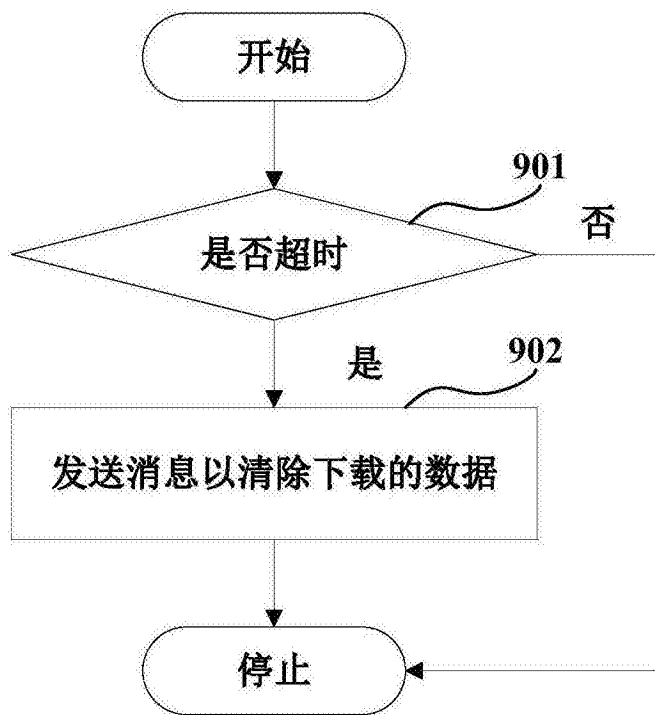


图9

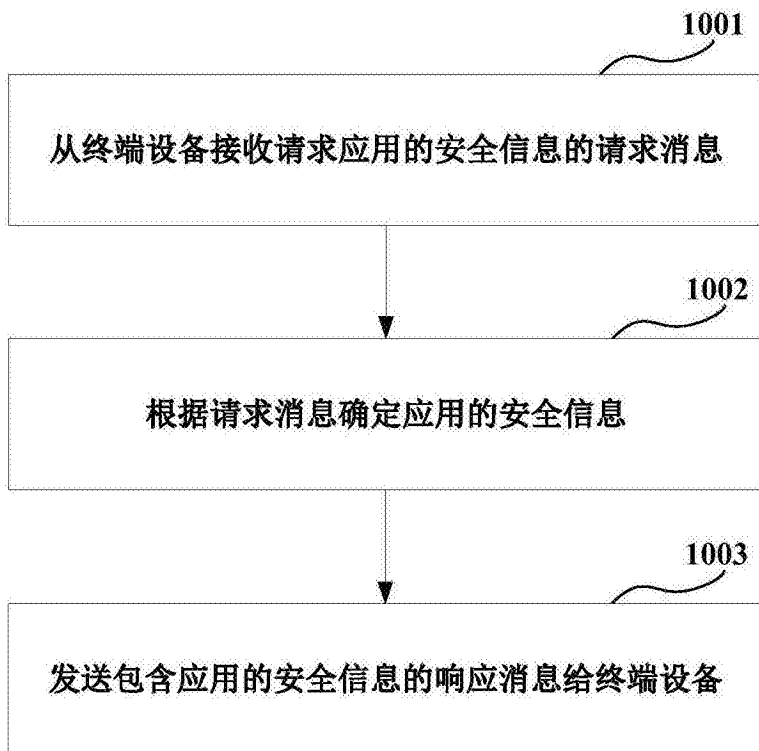


图10

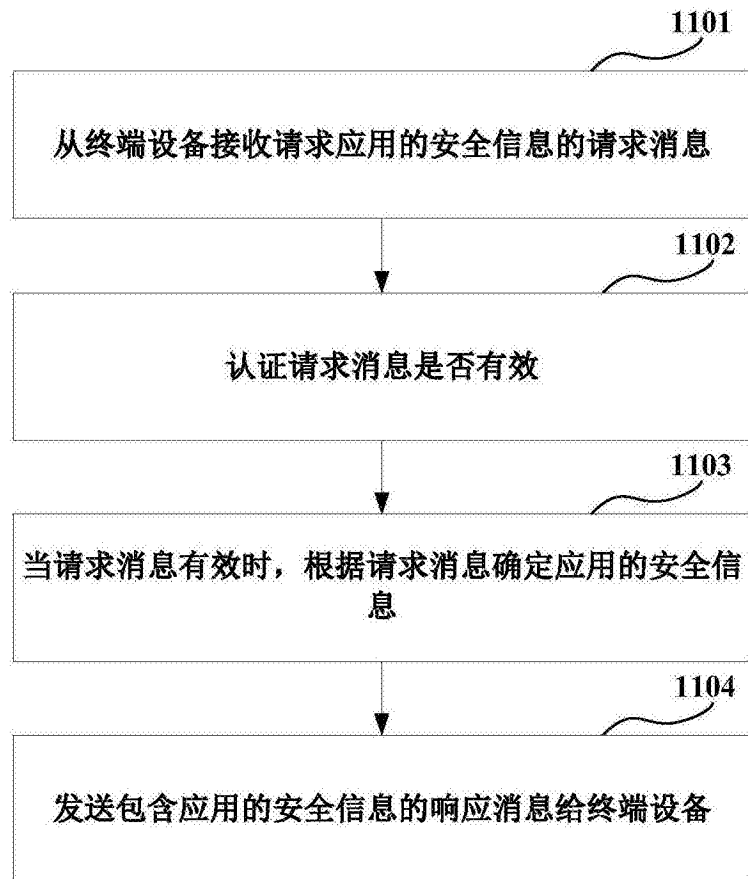


图11

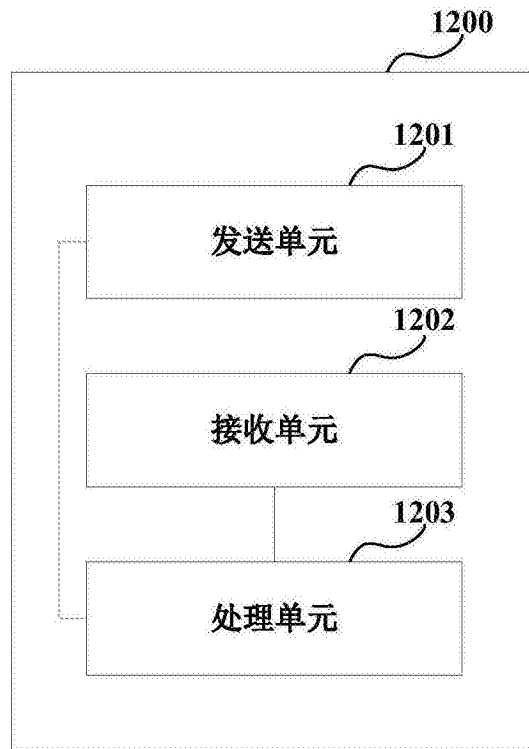


图12

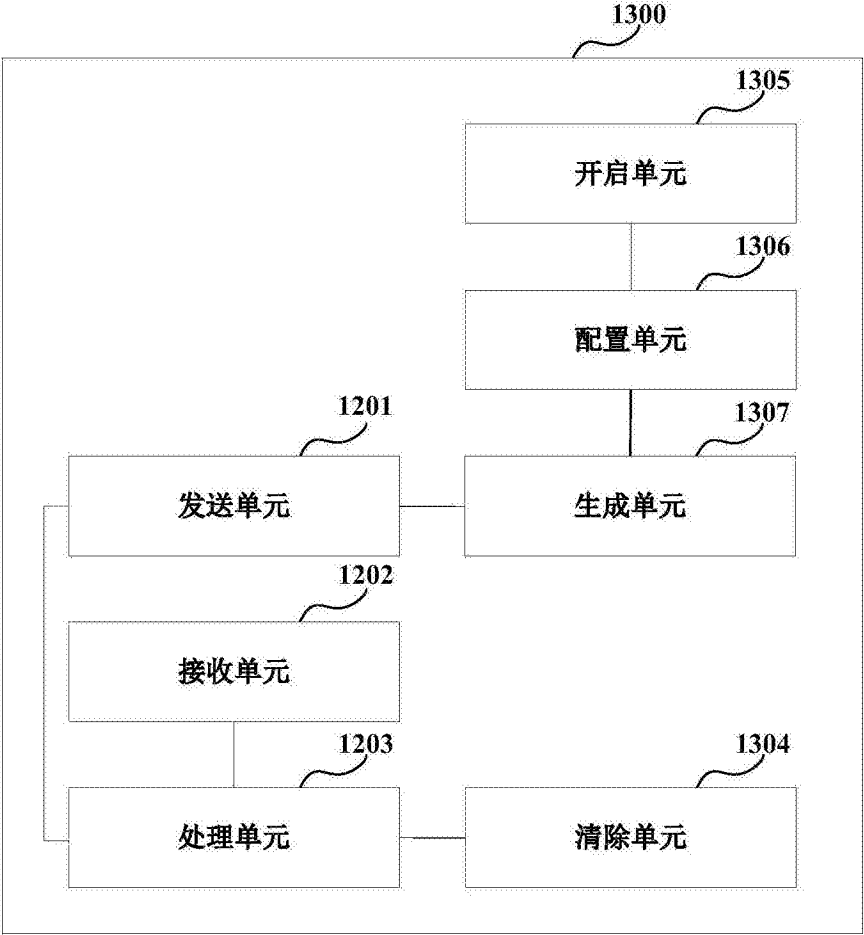


图13

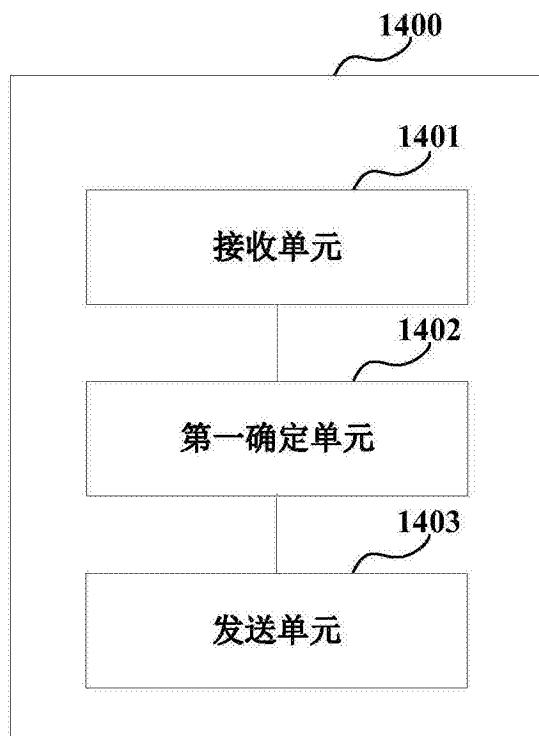


图14

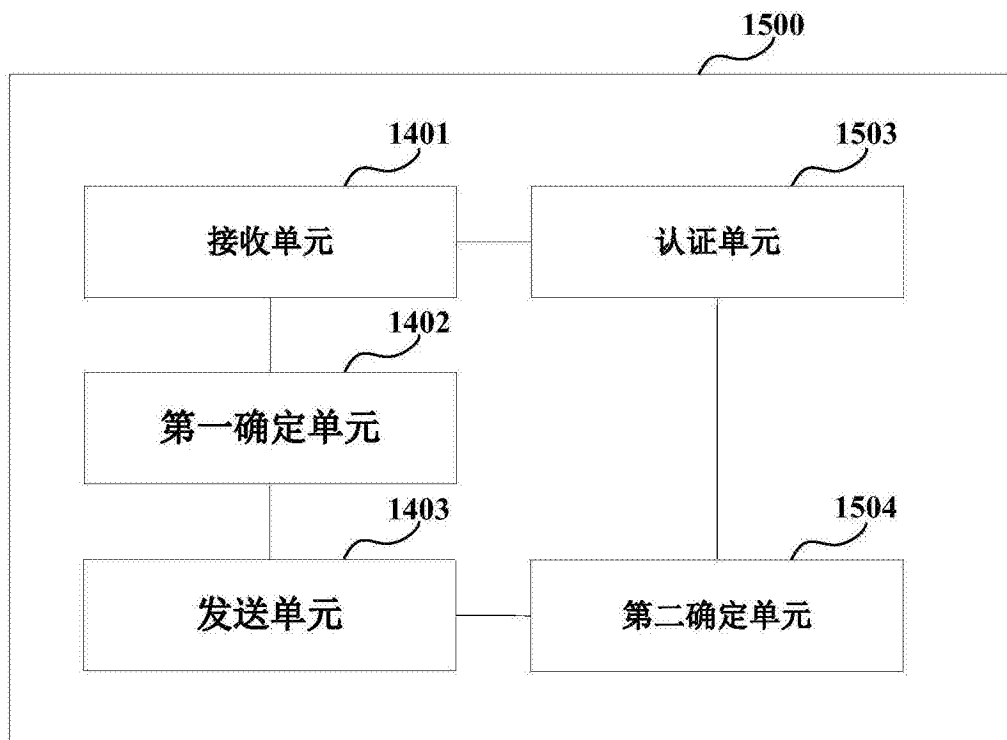


图15

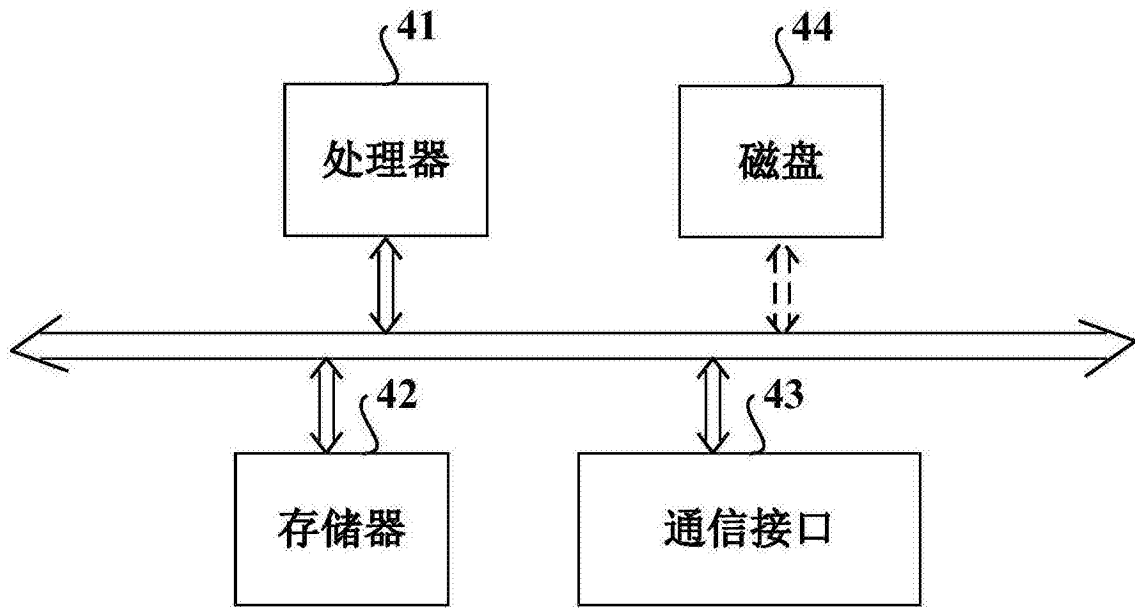


图16

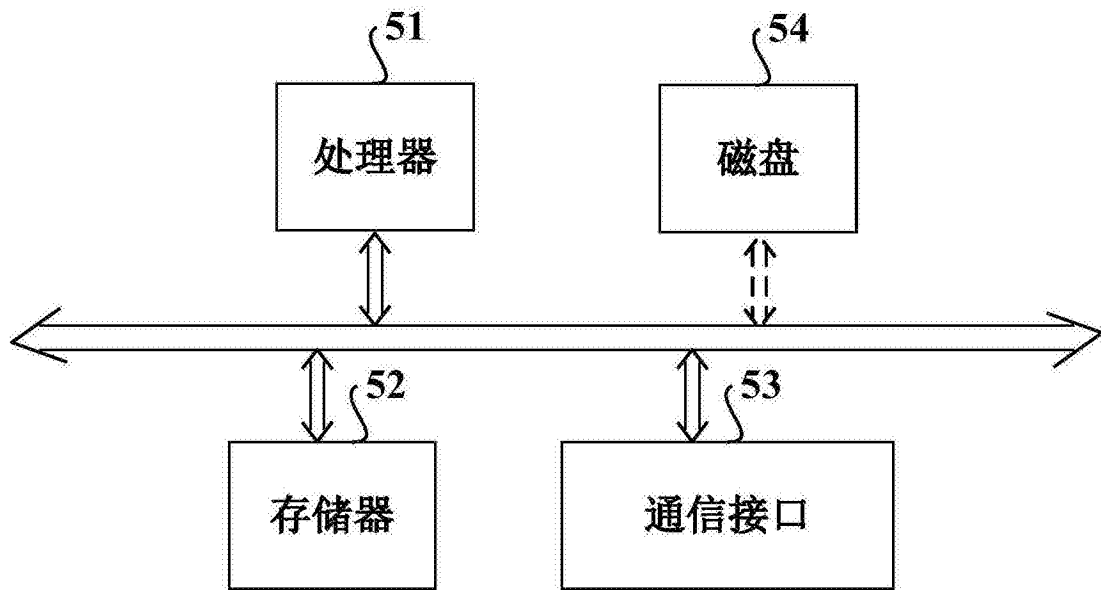


图17

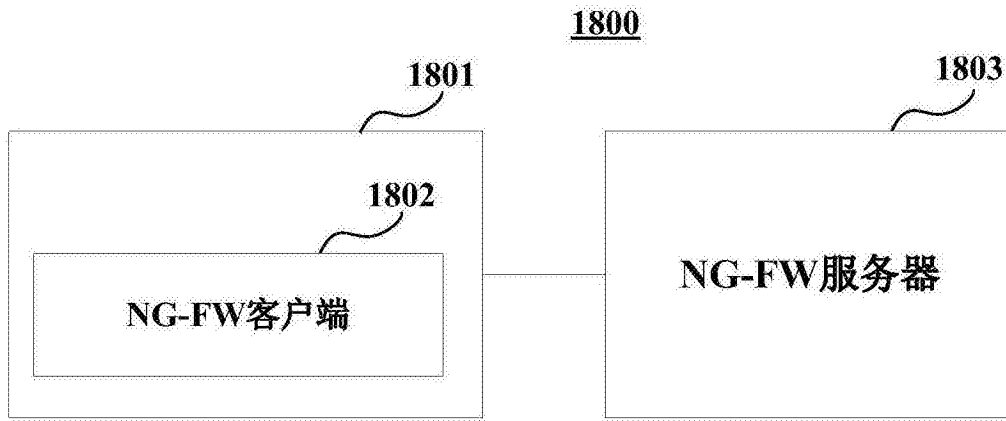


图18