(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 103281288 A
(43)申请公布日 2013.09.04

(21)申请号 201210581118.9

(22)申请日 2013.02.05

(71)申请人 武汉安天信息技术有限责任公司
地址 430000 湖北省武汉市东湖开发区光谷创业街6栋2楼

(72)发明人 方华 潘宣辰 乔伟 马志远

(51)Int.Cl.
H04L 29/06(2006.01)
H04M 1/725(2006.01)

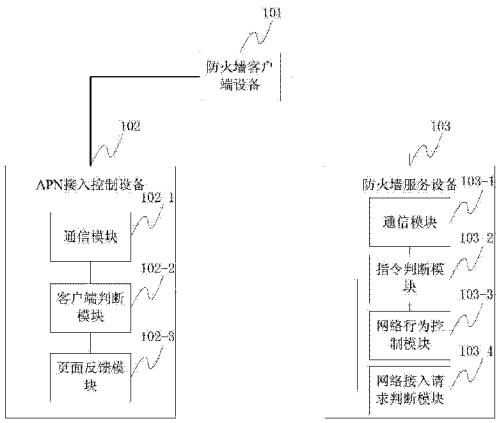
权利要求书3页 说明书8页 附图3页

(54)发明名称

一种手机防火墙系统及方法

(57)摘要

本发明提供了一种手机防火墙系统及方法，通过在移动终端的防火墙客户端修改移动终端的APN配置，使移动终端的网络接入请求发送到APN接入控制设备，APN接入控制设备将收到的网络访问请求转发给防火墙服务设备，防火墙服务设备对网络访问请求进行相关的检测，并将检测结果返回给APN接入控制设备。如果检测后需要经过用户控制，则用户将网络行为控制指令发送给防火墙，防火墙通知APN接入控制设备对网络接入请求放行或阻止。同时防火墙客户端设备还可以向防火墙服务器发送获取当前状态的信息和数据。通过本发明的方法，能够在不需要获得手机平台权限的情况下，对移动终端进行防火墙设置保护，适用于所有的移动终端平台。



CN 103281288 A

1. 一种手机防火墙系统，其特征在于，包括：

至少一台防火墙客户端设备，用于向 APN 接入控制设备发送网络接入请求，并接收 APN 接入控制设备返回的页面；或当接收到 APN 接入控制设备返回的用户控制页面后，向防火墙服务设备发送网络行为控制指令；

APN 接入控制设备，包括：通信模块，用于等待网络接入请求；

客户端判断模块，用于判断所述网络接入请求是否是防火墙客户端设备发送的请求，如果不是，则结束接入控制判断，否则将网络接入请求发送到防火墙服务设备，并接收防火墙服务设备返回的处理结果；

页面反馈模块，若处理结果为通过，则转发网络请求到目标服务器，并返回结果页面给客户端所在设备；若处理结果为不通过，则关闭所述网络接入请求，并将不通过详细信息页面返回给客户端所在设备；若处理结果为请求用户控制，则保留所述网络接入请求，并将用户控制页面返回给客户端所在设备；

防火墙服务设备，包括通信模块，用于接收服务请求指令；

指令判断模块，判断服务请求指令为网络行为控制指令或 APN 接入控制设备转发的网络接入请求指令；

网络行为控制模块，用于当判断为网络行为控制指令时，通过用户会话记录库确定所述网络行为控制指令所对应的防火墙客户端及 URL，判断所述网络行为控制指令类型，若网络行为控制指令为通过，则将通过信息发送给 APN 接入控制设备，若网络行为控制指令为不通过，则将不通过信息发送给 APN 接入控制设备；

网络接入请求判断模块，用于当判断为 APN 接入控制设备转发的网络接入请求指令时，检测所述网络接入请求是否为恶意，如果是，则返回给 APN 接入控制设备不通过信息；否则通过用户控制策略库匹配网络接入请求指令，若匹配到黑名单中，则返回给 APN 接入控制设备不通过信息；若匹配到白名单或直接放行名单中，则返回给 APN 接入控制设备通过信息；若匹配到要求用户控制名单中，则返回给 APN 接入控制设备请求用户控制信息。

2. 如权利要求 1 所述的系统，其特征在于，在防火墙客户端设备上配置 APN 接入点为接入到 APN 接入控制设备的地址及访问端口。

3. 如权利要求 1 所述的系统，其特征在于，所述的用户会话记录库中包括所有防火墙客户端设备的网络会话记录及对应的 URL 会话关系。

4. 如权利要求 1 所述的系统，其特征在于，所述的用户控制策略库为每个防火墙客户端设备的策略配置信息，所述配置信息中至少包括：客户端 ID、会话 ID、禁止接入网络的黑名单、允许接入网络的白名单及直接放行名单。

5. 如权利要求 1 所述的系统，其特征在于，所述的防火墙服务设备还包括，数据查询模块，用于接收用户使用状态数据查询指令，并通过用户使用管理记录库获取用户使用状态数据，并返回给客户端所在设备。

6. 如权利要求 1 所述的系统，其特征在于，防火墙服务设备检测所述网络接入请求是否为恶意具体为：通过恶意 URL 特征库中的恶意 URL 特征，判断所述网络接入请求是否包含恶意 URL 特征，如果是，则返回给 APN 接入控制设备不通过信息，否则通过恶意网络行为特征库，判断所述网络接入请求是否包含用户敏感信息，如果是，则返回给 APN 接入控制设备不通过信息，否则通过用户控制策略库匹配网络接入请求指令。

7. 如权利要求 6 所述的系统，其特征在于，所述的恶意 URL 特征至少包括 URL 域名、URL 完整连接或 URL 规则通配符。

8. 一种手机防火墙方法，其特征在于，包括 ：

防火墙客户端设备向 APN 接入控制设备发送网络接入请求，并接收 APN 接入控制设备返回的页面 ；或当接收到 APN 接入控制设备返回的用户控制页面后，向防火墙服务设备发送网络行为控制指令 ；

APN 接入控制设备等待网络接入请求，并判断所述网络接入请求是否是防火墙客户端设备发送的请求，如果不是，则结束接入控制判断，否则将网络接入请求发送到防火墙服务设备，并接收防火墙服务设备返回的处理结果，返回对应页面到客户端所在设备 ；若处理结果为通过，则转发网络请求到目标服务器，并返回结果页面给客户端所在设备 ；若处理结果为不通过，则关闭所述网络接入请求，并将不通过详细信息页面返回给客户端所在设备 ；若处理结果为请求用户控制，则保留所述网络接入请求，并将用户控制页面返回给客户端所在设备 ；

防火墙服务设备接收服务请求指令，并判断服务请求指令为网络行为控制指令或 APN 接入控制设备转发的网络接入请求指令 ；

若为网络行为控制指令，则通过用户会话记录库确定所述网络行为控制指令所对应的防火墙客户端及 URL，判断所述网络行为控制指令类型，若网络行为控制指令为通过，则将通过信息发送给 APN 接入控制设备，若网络行为控制指令为不通过，则将不通过信息发送给 APN 接入控制设备 ；

若为 APN 接入控制设备转发的网络接入请求指令，则检测所述网络接入请求是否为恶意，如果是，则返回给 APN 接入控制设备不通过信息 ；否则通过用户控制策略库匹配网络接入请求指令，若匹配到黑名单中，则返回给 APN 接入控制设备不通过信息 ；若匹配到白名单或直接放行名单中，则返回给 APN 接入控制设备通过信息 ；若匹配到要求用户控制名单中，则返回给 APN 接入控制设备请求用户控制信息。

9. 如权利要求 8 所述的方法，其特征在于，在防火墙客户端设备上配置 APN 接入点为接入到 APN 接入控制设备的地址及访问端口。

10. 如权利要求 8 所述的方法，其特征在于，所述的用户会话记录库中包括所有防火墙客户端设备的网络会话记录及对应的 URL 会话关系。

11. 如权利要求 8 所述的方法，其特征在于，所述的用户控制策略库为每个防火墙客户端设备的策略配置信息，所述配置信息中至少包括 ：客户端 ID、会话 ID、禁止接入网络的黑名单、允许接入网络的白名单及直接放行名单。

12. 如权利要求 8 所述的方法，其特征在于，所述的防火墙服务设备还包括，接收用户使用状态数据查询指令，并通过用户使用管理记录库获取用户使用状态数据，并返回给客户端所在设备。

13. 如权利要求 8 所述的方法，其特征在于，防火墙服务设备检测所述网络接入请求是否为恶意具体为 ：通过恶意 URL 特征库中的恶意 URL 特征，判断所述网络接入请求是否包含恶意 URL 特征，如果是，则返回给 APN 接入控制设备不通过信息，否则通过恶意网络行为特征库，判断所述网络接入请求是否包含用户敏感信息，如果是，则返回给 APN 接入控制设备不通过信息，否则通过用户控制策略库匹配网络接入请求指令。

14. 如权利要求 13 所述的方法，其特征在于，所述的恶意 URL 特征至少包括 URL 域名、URL 完整连接或 URL 规则通配符。

一种手机防火墙系统及方法

技术领域

[0001] 本发明涉及移动终端恶意代码检测领域，特别涉及一种手机防火墙系统及方法。

背景技术

[0002] 随着移动互联网的快速发展，普通用户使用手机来访问互联网资源已经成了一个非常普遍的现象。而互联网上存在着大量的不良信息，垃圾网站，钓鱼网站和恶意网站，对用户的手机使用安全造成较大的影响。现有的移动终端恶意代码检测方法，通常是在恶意行为已经发生后，根据所产生的行为来判断是否为恶意代码，而并不能在恶意行为发生前对其进行预防。相对来说，不同的手机平台都有不同的研发环境和开发方式，程序也无法通用。同时，许多系统并没有提供比较好的开发支持来实现防火墙功能。比如 Android 系统上，在不提权的情况下是无法实现完整的防火墙拦截和控制功能的，在 Symbian，Winphone，iPhoneOS 等各种手机系统上都存在类似的问题，导致无法在手机操作系统上实现比较好的网络行为控制和安全检查的防火墙功能。

发明内容

[0003] 本发明提供一种手机防火墙系统及方法，解决了现有技术中无法提权的情况下无法实现防火墙控制的问题，具有更准确的检测效果。

[0004] 一种手机防火墙系统，包括：

[0005] 至少一台防火墙客户端设备，用于向 APN 接入控制设备发送网络接入请求，并接收 APN 接入控制设备返回的页面；或当接收到 APN 接入控制设备返回的用户控制页面后，向防火墙服务设备发送网络行为控制指令；

[0006] APN 接入控制设备，包括：通信模块，用于等待网络接入请求；

[0007] 客户端判断模块，用于判断所述网络接入请求是否是防火墙客户端设备发送的请求，如果不是，则结束接入控制判断，否则将网络接入请求发送到防火墙服务设备，并接收防火墙服务设备返回的处理结果；

[0008] 页面反馈模块，若处理结果为通过，则转发网络请求到目标服务器，并返回结果页面给客户端所在设备；若处理结果为不通过，则关闭所述网络接入请求，并将不通过详细信息页面返回给客户端所在设备；若处理结果为请求用户控制，则保留所述网络接入请求，并将用户控制页面返回给客户端所在设备；

[0009] 防火墙服务设备，包括通信模块，用于接收服务请求指令；

[0010] 指令判断模块，判断服务请求指令为网络行为控制指令或 APN 接入控制设备转发的网络接入请求指令；

[0011] 网络行为控制模块，用于当判断为网络行为控制指令时，通过用户会话记录库确定所述网络行为控制指令所对应的防火墙客户端及 URL，判断所述网络行为控制指令类型，若网络行为控制指令为通过，则将通过信息发送给 APN 接入控制设备，若网络行为控制指令为不通过，则将不通过信息发送给 APN 接入控制设备；

[0012] 网络接入请求判断模块，用于当判断为 APN 接入控制设备转发的网络接入请求指令时，检测所述网络接入请求是否为恶意，如果是，则返回给 APN 接入控制设备不通过信息；否则通过用户控制策略库匹配网络接入请求指令，若匹配到黑名单中，则返回给 APN 接入控制设备不通过信息；若匹配到白名单或直接放行名单中，则返回给 APN 接入控制设备通过信息；若匹配到要求用户控制名单中，则返回给 APN 接入控制设备请求用户控制信息。

[0013] 所述的系统中，在防火墙客户端上配置 APN 接入点为接入到 APN 接入控制设备的地址及访问端口。

[0014] 所述的系统，中，所述的用户会话记录库中包括所有客户端的网络会话记录及对应的 URL 会话关系。

[0015] 所述的系统中，所述的用户控制策略库为每个防火墙客户端设备的策略配置信息，所述配置信息中至少包括：客户端 ID、会话 ID、禁止接入网络的黑名单、允许接入网络的白名单及直接放行名单。

[0016] 所述的系统中，所述的防火墙服务设备还包括，数据查询模块，用于接收用户使用状态数据查询指令，并通过用户使用管理记录库获取用户使用状态数据，并返回给客户端所在设备。

[0017] 所述的系统中，防火墙服务设备检测所述网络接入请求是否为恶意具体为：通过恶意 URL 特征库中的恶意 URL 特征，判断所述网络接入请求是否包含恶意 URL 特征，如果是，则返回给 APN 接入控制设备不通过信息，否则通过恶意网络行为特征库，判断所述网络接入请求是否包含用户敏感信息，如果是，则返回给 APN 接入控制设备不通过信息，否则通过用户控制策略库匹配网络接入请求指令。

[0018] 所述的系统中，所述的恶意 URL 特征至少包括 URL 域名、URL 完整连接或 URL 规则通配符。

[0019] 一种手机防火墙方法，包括：

[0020] 防火墙客户端设备向 APN 接入控制设备发送网络接入请求，并接收 APN 接入控制设备返回的页面；或当接收到 APN 接入控制设备返回的用户控制页面后，向防火墙服务设备发送网络行为控制指令；

[0021] APN 接入控制设备等待网络接入请求，并判断所述网络接入请求是否是防火墙客户端设备发送的请求，如果不是，则结束接入控制判断，否则将网络接入请求发送到防火墙服务设备，并接收防火墙服务设备返回的处理结果，返回对应页面到客户端所在设备；若处理结果为通过，则转发网络请求到目标服务器，并返回结果页面给客户端所在设备；若处理结果为不通过，则关闭所述网络接入请求，并将不通过详细信息页面返回给客户端所在设备；若处理结果为请求用户控制，则保留所述网络接入请求，并将用户控制页面返回给客户端所在设备；

[0022] 防火墙服务设备接收服务请求指令，并判断服务请求指令为网络行为控制指令或 APN 接入控制设备转发的网络接入请求指令；

[0023] 若为网络行为控制指令，则通过用户会话记录库确定所述网络行为控制指令所对应的防火墙客户端及 URL，判断所述网络行为控制指令类型，若网络行为控制指令为通过，则将通过信息发送给 APN 接入控制设备，若网络行为控制指令为不通过，则将不通过信息发送给 APN 接入控制设备；

[0024] 若为 APN 接入控制设备转发的网络接入请求指令，则检测所述网络接入请求是否为恶意，如果是，则返回给 APN 接入控制设备不通过信息；否则通过用户控制策略库匹配网络接入请求指令，若匹配到黑名单中，则返回给 APN 接入控制设备不通过信息；若匹配到白名单或直接放行名单中，则返回给 APN 接入控制设备通过信息；若匹配到要求用户控制名单中，则返回给 APN 接入控制设备请求用户控制信息。

[0025] 所述的方法中，在防火墙客户端上配置 APN 接入点为接入到 APN 接入控制设备的地址及访问端口。

[0026] 所述的方法中，所述的用户会话记录库中包括所有客户端的网络会话记录及对应的 URL 会话关系。

[0027] 所述的方法中，所述的用户控制策略库为每个防火墙客户端设备的策略配置信息，所述配置信息中至少包括：客户端 ID、会话 ID、禁止接入网络的黑名单、允许接入网络的白名单及直接放行名单。

[0028] 所述的方法中，所述的防火墙服务设备还包括，接收用户使用状态数据查询指令，并通过用户使用管理记录库获取用户使用状态数据，并返回给客户端所在设备。

[0029] 所述的方法中，防火墙服务设备检测所述网络接入请求是否为恶意具体为：通过恶意 URL 特征库中的恶意 URL 特征，判断所述网络接入请求是否包含恶意 URL 特征，如果是，则返回给 APN 接入控制设备不通过信息，否则通过恶意网络行为特征库，判断所述网络接入请求是否包含用户敏感信息，如果是，则返回给 APN 接入控制设备不通过信息，否则通过用户控制策略库匹配网络接入请求指令。

[0030] 所述的方法中，所述的恶意 URL 特征至少包括 URL 域名、URL 完整连接或 URL 规则通配符。

[0031] 本发明的方法及系统，利用手机系统的网络访问的功能配置策略，手机系统在接入网络时，需要根据运营商提供的不同的网络接入服务来进行不同的 APN 配置，通过配置不同的 APN 可以通过不同的方式来使用移动运营商提供的网络接入服务，使手机可以访问互联网上的数据。因此本发明利用了 APN 的配置特点提供了一种可以适用于所有平台的手机防火墙系统，能够以极低的成本实现手机操作系统的网络行为控制，对移动终端的网络行为发生前，将网络行为获取到 APN 接入控制设备进行判断和拦截。不需要获得移动终端平台控制权限，即能够实现防火墙的拦截和控制功能。

[0032] 本发明提供了一种手机防火墙系统及方法，通过在移动终端的防火墙客户端修改移动终端的 APN 配置，使移动终端的网络接入请求发送到 APN 接入控制设备，APN 接入控制设备将收到的网络访问请求转发给防火墙服务设备，防火墙服务设备对网络访问请求进行相关的检测，并将检测结果返回给 APN 接入控制设备。如果检测后需要经过用户控制，则用户将网络行为控制指令发送给防火墙，防火墙通知 APN 接入控制设备对网络接入请求放行或阻止。同时防火墙客户端设备还可以向防火墙服务器发送获取当前状态的信息和数据。通过本发明的方法，能够在不需要获得手机平台权限的情况下，对移动终端进行防火墙设置保护，适用于所有的移动终端平台。

附图说明

[0033] 为了更清楚地说明本发明或现有技术中的技术方案，下面将对实施例或现有技术

描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0034] 图 1 为一种手机防火墙系统结构示意图；

[0035] 图 2 为一种手机防火墙方法中防火墙客户端设备流程图；

[0036] 图 3 为一种手机防火墙方法中 APN 接入控制设备流程图；

[0037] 图 4 为一种手机防火墙方法中防火墙服务器设备流程图。

具体实施方式

[0038] 为了使本技术领域的人员更好地理解本发明实施例中的技术方案，并使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图对本发明中技术方案作进一步详细的说明。

[0039] 本发明提供一种手机防火墙系统及方法，解决了现有技术中无法提权的情况下无法实现防火墙控制的问题，具有更准确的检测效果。

[0040] 一种手机防火墙系统，如图 1 所示，包括：

[0041] 至少一台防火墙客户端设备 101，用于向 APN 接入控制设备发送网络接入请求，并接收 APN 接入控制设备返回的页面；或当接收到 APN 接入控制设备返回的用户控制页面后，向防火墙服务设备发送网络行为控制指令；

[0042] APN 接入控制设备 102，包括：通信模块 102-1，用于等待网络接入请求；

[0043] 客户端判断模块 102-2，用于判断所述网络接入请求是否是防火墙客户端设备发送的请求，如果不是，则结束接入控制判断，否则将网络接入请求发送到防火墙服务设备，并接收防火墙服务设备返回的处理结果；

[0044] 页面反馈模块 102-3，若处理结果为通过，则转发网络请求到目标服务器，并返回结果页面给客户端所在设备；若处理结果为不通过，则关闭所述网络接入请求，并将不通过详细信息页面返回给客户端所在设备；若处理结果为请求用户控制，则保留所述网络接入请求，并将用户控制页面返回给客户端所在设备；

[0045] 防火墙服务设备 103，包括通信模块 103-1，用于接收服务请求指令；

[0046] 指令判断模块 103-2，判断服务请求指令为网络行为控制指令或 APN 接入控制设备转发的网络接入请求指令；

[0047] 网络行为控制模块 103-3，用于当判断为网络行为控制指令时，通过用户会话记录库确定所述网络行为控制指令所对应的防火墙客户端及 URL，判断所述网络行为控制指令类型，若网络行为控制指令为通过，则将通过信息发送给 APN 接入控制设备，若网络行为控制指令为不通过，则将不通过信息发送给 APN 接入控制设备；

[0048] 网络接入请求判断模块 103-4，用于当判断为 APN 接入控制设备转发的网络接入请求指令时，检测所述网络接入请求是否为恶意，如果是，则返回给 APN 接入控制设备不通过信息；否则通过用户控制策略库匹配网络接入请求指令，若匹配到黑名单中，则返回给 APN 接入控制设备不通过信息；若匹配到白名单或直接放行名单中，则返回给 APN 接入控制设备通过信息；若匹配到要求用户控制名单中，则返回给 APN 接入控制设备请求用户控制信息。

[0049] 所述的系统中，在防火墙客户端设备上配置 APN 接入点为接入到 APN 接入控制设备的地址及访问端口。本步骤的目的在于将手机上所有的网络行为的访问都转发给 APN 接入控制设备。

[0050] 所述的系统中，所述的用户会话记录库中包括所有客户端的网络会话记录及对应的 URL 会话关系。

[0051] 所述的系统中，所述的用户控制策略库中为每个防火墙客户端设备的策略配置信息，所述配置信息至少包括：客户端 ID、会话 ID、禁止接入网络的黑名单、允许接入网络的白名单及直接放行名单。

[0052] 所述的系统中，所述的防火墙服务设备还包括，数据查询模块，用于接收用户使用状态数据查询指令，并通过用户使用管理记录库获取用户使用状态数据，并返回给客户端所在设备。

[0053] 所述的系统中，防火墙服务设备检测所述网络接入请求是否为恶意具体为：通过恶意 URL 特征库中的恶意 URL 特征，判断所述网络接入请求是否包含恶意 URL 特征，如果是，则返回给 APN 接入控制设备不通过信息，否则通过恶意网络行为特征库，判断所述网络接入请求是否包含用户敏感信息，如果是，则返回给 APN 接入控制设备不通过信息，否则通过用户控制策略库匹配网络接入请求指令。

[0054] 所述的系统中，所述的恶意 URL 特征至少包括 URL 域名、URL 完整连接或 URL 规则通配符。

[0055] 一种手机防火墙方法，包括：

[0056] 防火墙客户端设备方法流程如图 2 所示：

[0057] S201：向 APN 接入控制设备发送网络接入请求；

[0058] 或 S202：当接收到 APN 接入控制设备返回的用户控制页面后，向防火墙服务设备发送网络行为控制指令；

[0059] S203：接收 APN 接入控制设备返回的页面。

[0060] APN 接入控制设备方法流程图如图 3 所示：

[0061] S301：等待网络接入请求；

[0062] S302：判断所述网络接入请求是否是防火墙客户端设备发送的请求，如果不是，则结束接入控制判断，否则执行 S303；

[0063] S303：将网络接入请求发送到防火墙服务设备，并接收防火墙服务设备返回的处理结果；若处理结果为通过，则执行 S304；若处理结果为不通过，则执行 S305；若处理结果为请求用户控制，则执行 S306；

[0064] S304：转发网络请求到目标服务器，并返回结果页面给客户端所在设备；

[0065] S305：关闭所述网络接入请求，并将不通过详细信息页面返回给客户端所在设备；

[0066] S306：保留所述网络接入请求，并将用户控制页面返回给客户端所在设备。

[0067] 防火墙服务设备方法流程图如图 4 所示：

[0068] S401：接收服务请求指令；

[0069] S402 判断服务请求指令为网络行为控制指令或 APN 接入控制设备转发的网络接入请求指令；

[0070] 若为网络行为控制指令，则执行 S403 ；若为 APN 接入控制设备转发的网络接入请求指令，则执行 S406 ；

[0071] S403 ：通过用户会话记录库确定所述网络行为控制指令所对应的防火墙客户端及 URL，判断所述网络行为控制指令类型，若网络行为控制指令为通过，则执行 S404 ；若网络行为控制指令为不通过，则执行 S405 ；

[0072] S404 ：将通过信息发送给 APN 接入控制设备 ；

[0073] S405 ：将不通过信息发送给 APN 接入控制设备 ；

[0074] S406 ：检测所述网络接入请求是否为恶意，如果是，则执行 S405 ；否则执行 S407 ；

[0075] S407 ：通过用户控制策略库匹配网络接入请求指令，若匹配到黑名单中，则执行 S405 ；若匹配到白名单或直接放行名单中，则执行 S404 ；若匹配到要求用户控制名单中，则执行 S408 ；

[0076] S408 ：返回给 APN 接入控制设备请求用户控制信息。

[0077] 所述的方法中，在防火墙客户端上配置 APN 接入点为接入到 APN 接入控制设备的地址及访问端口。本步骤的目的在于将手机上所有的网络行为的访问都转发给 APN 接入控制设备。

[0078] 所述的方法中，所述的用户会话记录库中包括所有客户端的网络会话记录及对应的 URL 会话关系。

[0079] 所述的方法中，所述的用户控制策略库中为每个防火墙客户端设备的策略配置信息，所述配置信息至少包括 ：客户端 ID、会话 ID、禁止接入网络的黑名单、允许接入网络的白名单及直接放行名单。

[0080] 所述的方法中，所述的防火墙服务设备还包括，接收用户使用状态数据查询指令，并通过用户使用管理记录库获取用户使用状态数据，并返回给客户端所在设备。

[0081] 所述的方法中，防火墙服务设备检测所述网络接入请求是否为恶意具体为 ：通过恶意 URL 特征库中的恶意 URL 特征，判断所述网络接入请求是否包含恶意 URL 特征，如果是，则返回给 APN 接入控制设备不通过信息，否则通过恶意网络行为特征库，判断所述网络接入请求是否包含用户敏感信息，如果是，则返回给 APN 接入控制设备不通过信息，否则通过用户控制策略库匹配网络接入请求指令。

[0082] 对恶意 URL 特征库举例如下 ：

[0083]

```
struct
{
    char* malurlsig;
    char* maldescription;
}MalURL;
struct
{
    MalURL* iMalURLList;
    int          iMalURLCnt;
}MalURLDatabase;
```

[0084]

[0085] 其中 MalURLDatabase 为恶意 URL 特征库，由 MalURL 数组组成，malurlsig 为恶意 URL 的特征，maldescription 为对该特征的描述。

[0086] 所述的方法中，所述的恶意 URL 特征至少包括 URL 域名、URL 完整连接或 URL 规则通配符。

[0087] 本发明的方法及系统，利用手机系统的网络访问的功能配置策略，手机系统在接入网络时，需要根据运营商提供的不同的网络接入服务来进行不同的 APN 配置，通过配置不同的 APN 可以通过不同的方式来使用移动运营商提供的网络接入服务，使手机可以访问互联网上的数据。因此本发明利用了 APN 的配置特点提供了一种可以适用于所有平台的手机防火墙系统，能够以极低的成本实现手机操作系统的网络行为控制，对移动终端的网络行为发生前，将网络行为获取到 APN 接入控制设备进行判断和拦截。

[0088] 不需要获得移动终端平台控制权限，即能够实现防火墙的拦截和控制功能。

[0089] 本发明提供了一种手机防火墙系统及方法，通过在移动终端的防火墙客户端修改移动终端的 APN 配置，使移动终端的网络接入请求发送到 APN 接入控制设备，APN 接入控制设备将收到的网络访问请求转发给防火墙服务设备，防火墙服务设备对网络访问请求进行相关的检测，并将检测结果返回给 APN 接入控制设备。如果检测后需要经过用户控制，则用户将网络行为控制指令发送给防火墙，防火墙通知 APN 接入控制设备对网络接入请求放行或阻止。同时防火墙客户端设备还可以向防火墙服务器发送获取当前状态的信息和数据。通过本发明的方法，能够在不需要获得手机平台权限的情况下，对移动终端进行防火墙设置保护，适用于所有的移动终端平台。

[0090] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0091] 本发明可用于众多通用或专用的计算系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶

盒、可编程的消费电子设备、网络 PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

[0092] 本发明可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本发明，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0093] 虽然通过实施例描绘了本发明，本领域普通技术人员知道，本发明有许多变形和变化而不脱离本发明的精神，希望所附的权利要求包括这些变形和变化而不脱离本发明的精神。

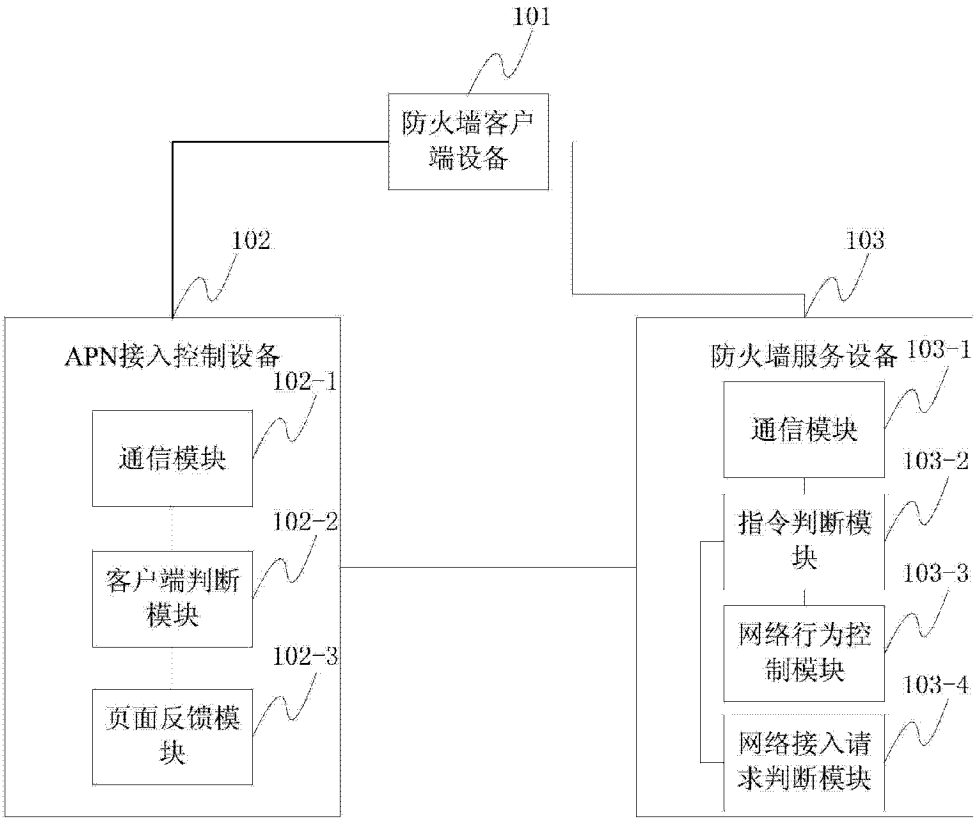

101
防火墙客户端设备
102
APN接入控制设备
102-1
通信模块
102-2
客户端判断模块
102-3
页面反馈模块
103
防火墙服务设备
103-1
通信模块
103-2
指令判断模块
103-3
网络行为控制模块
103-4
网络接入请求判断模块

图 1

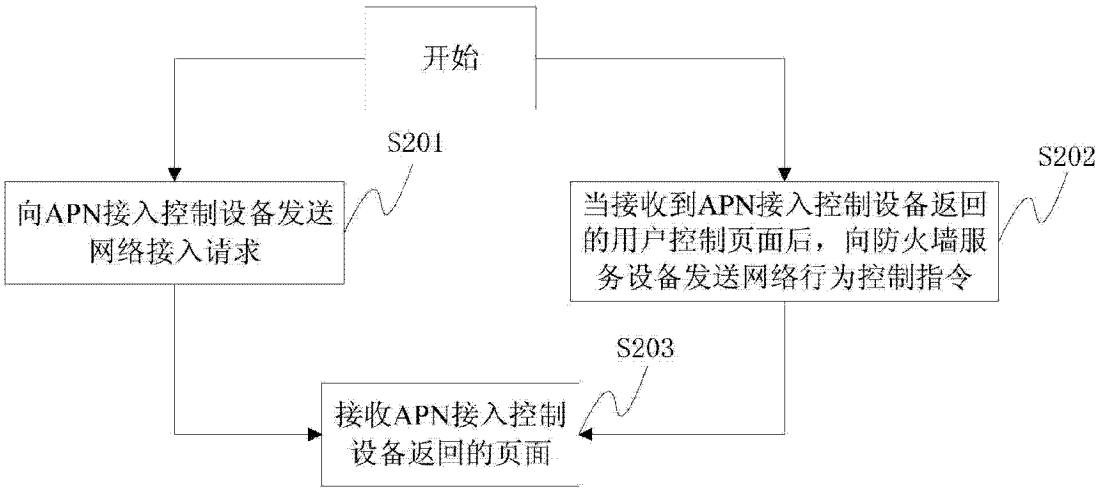

开始
S201
向APN接入控制设备发送网络接入请求
S202
当接收到APN接入控制设备返回的用户控制页面后，向防火墙服务设备发送网络行为控制指令
S203
接收APN接入控制设备返回的页面

图 2

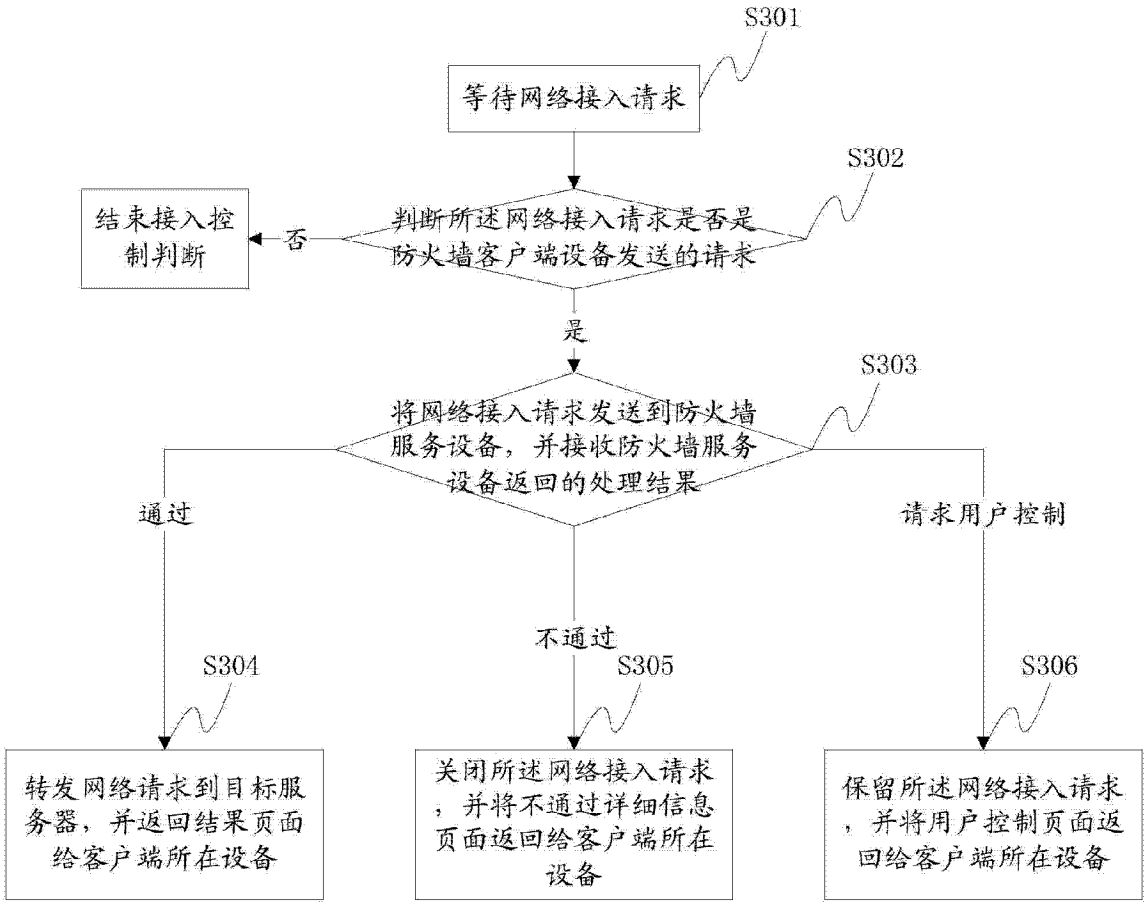

S301
等待网络接入请求
S302
判断所述网络接入请求是否是防火墙客户端设备发送的请求
否
结束接入控制判断
是
S303
将网络接入请求发送到防火墙服务设备，并接收防火墙服务设备返回的处理结果
通过
不通过
请求用户控制
S304
转发网络请求到目标服务器，并返回结果页面给客户端所在设备
S305
关闭所述网络接入请求，并将不通过详细信息页面返回给客户端所在设备
S306
保留所述网络接入请求，并将用户控制页面返回给客户端所在设备

图 3

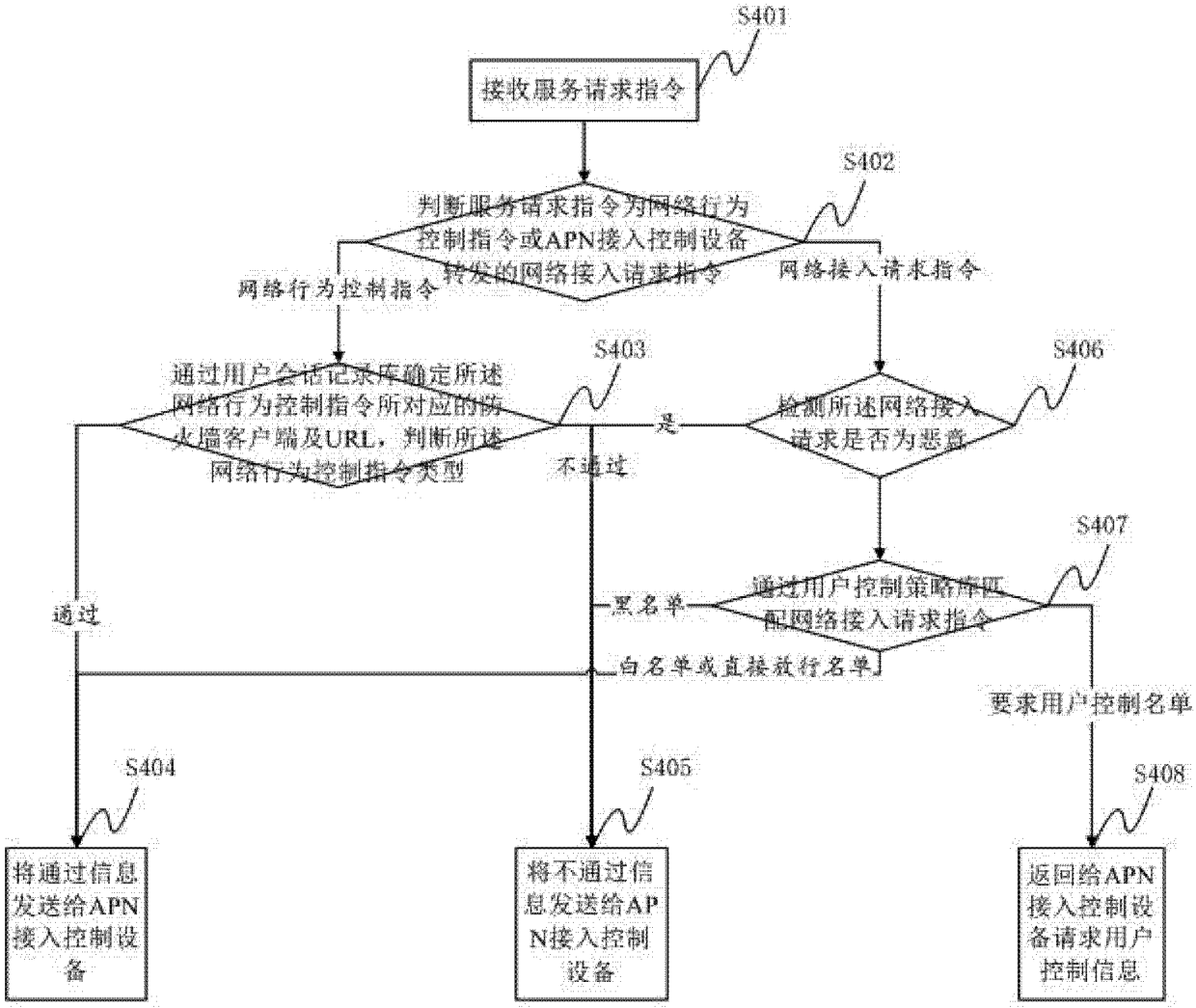

S401
接收服务请求指令
S402
判断服务请求指令为网络行为控制指令或APN接入控制设备转发的网络接入请求指令
网络行为控制指令
网络接入请求指令
S403
通过用户会话记录库确定所述网络行为控制指令所对应的防火墙客户端及URL，判断所述网络行为控制指令类型
是
不通过
S406
检测所述网络接入请求是否为恶意
S407
通过用户控制策略库匹配网络接入请求指令
通过
黑名单
白名单或直接放行名单
要求用户控制名单
S404
S405
S408
将通过信息发送给APN接入控制设备
将不通过信息发送给APN接入控制设备
返回给APN接入控制设备请求用户控制信息

图 4