(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 105656927 A
(43)申请公布日 2016.06.08

(21)申请号 201610099561.0

(22)申请日 2016.02.23

(71)申请人 浙江宇视科技有限公司
地址 310051 浙江省杭州市滨江区西兴街道江陵路88号10幢南座1-11层

(72)发明人 周迪 赵晖

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 29/06(2006.01)
H04N 7/18(2006.01)

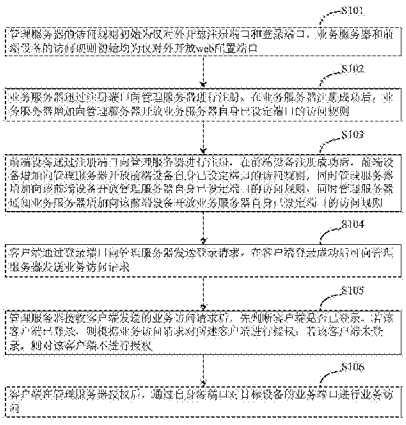
权利要求书2页 说明书13页 附图1页

(54)发明名称

一种安全访问方法及系统

(57)摘要

本申请提供一种安全访问方法及系统，该方法包括：业务服务器及前端设备均通过注册端口向管理服务器进行注册，在注册成功前，仅对外开放web配置端口，在注册成功后，业务服务器、前端设备及管理服务器更新各自的访问规则；客户端通过登录端口向管理服务器发送登录请求，在登录成功后可向管理服务器请求业务；客户端向管理服务器发送携带有目标设备、业务端口及自身源端口的业务访问请求，并在管理服务器授权后，通过自身源端口对该业务端口进行业务访问。本发明通过管理服务器对监控系统中的客户端、前端设备和业务服务器进行集中授权，仅允许经过授权的客户端、前端设备、业务服务器对监控设备进行访问，有效阻止入侵者对监控设备的扫描入侵。



CN 105656927 A

1.一种安全访问方法,其特征在于,所述安全访问方法包括:

管理服务器的访问规则初始为仅对外开放注册端口和登录端口,业务服务器和前端设备的访问规则初始均为仅对外开放web配置端口;

业务服务器通过所述注册端口向管理服务器进行注册,在业务服务器注册成功后,业务服务器增加向管理服务器开放业务服务器自身已设定端口的访问规则;

前端设备通过所述注册端口向管理服务器进行注册,在前端设备注册成功后,前端设备增加向管理服务器开放前端设备自身已设定端口的访问规则,同时管理服务器增加向该前端设备开放管理服务器自身已设定端口的访问规则,同时管理服务器通知业务服务器增加向该前端设备开放业务服务器自身已设定端口的访问规则;

客户端通过所述登录端口向管理服务器发送登录请求,在客户端登录成功后可向管理服务器发送业务访问请求,所述业务访问请求携带的信息至少包括:目标设备、业务端口及自身源端口,所述目标设备是管理服务器或业务服务器或前端设备;

管理服务器接收所述业务访问请求后,先判断客户端是否已登录,若该客户端已登录,则根据所述业务访问请求对所述客户端进行授权;若该客户端未登录,则对该客户端不进行授权;

客户端在管理服务器授权后,通过自身源端口对所述业务端口进行业务访问。

2.如权利要求1所述的安全访问方法,其特征在于,所述根据所述业务访问请求对所述客户端进行授权,具体包括:确定目标设备,当目标设备是管理服务器时,对该客户端进行授权;当目标设备是业务服务器或前端设备时,通知目标设备向该客户端开放所述业务端口,且在得到目标设备发送的已向该客户端开放所述业务端口的响应后,对该客户端进行授权。

3.如权利要求1所述的安全访问方法,其特征在于,所述根据所述业务访问请求对所述客户端进行授权,具体包括:确定目标设备,当目标设备是管理服务器时,对该客户端进行授权;当目标设备是业务服务器或前端设备时,通知目标设备向该客户端开放所述业务端口,并对该客户端进行授权。

4.如权利要求1所述的安全访问方法,其特征在于,所述安全访问方法还包括:

当管理服务器或业务服务器或前端设备的访问规则达到对应的预设阈值时,根据与预设阈值对应的控制粒度调整访问规则。

5.如权利要求1所述的安全访问方法,其特征在于,所述安全访问方法还包括:前端设备通过所述注册端口向管理服务器进行注册时发送的注册报文中携带的信息,至少包括:前端设备的IP地址和mask掩码地址,管理服务器根据前端设备的IP地址和mask掩码地址调整访问规则。

6.一种安全访问系统,其特征在于,所述安全访问系统包括管理服务器、业务服务器、前端设备和客户端;其中,管理服务器的访问规则初始为仅对外开放注册端口和登录端口,业务服务器和前端设备的访问规则初始均为仅对外开放web配置端口;

业务服务器通过所述注册端口向管理服务器进行注册,在业务服务器注册成功后,业务服务器增加向管理服务器开放业务服务器自身已设定端口的访问规则;

前端设备通过所述注册端口向管理服务器进行注册,在前端设备注册成功后,前端设备增加向管理服务器开放前端设备自身已设定端口的访问规则,同时管理服务器增加向该

前端设备开放管理服务器自身已设定端口的访问规则，同时管理服务器通知业务服务器增加向该前端设备开放业务服务器自身已设定端口的访问规则；

客户端通过所述登录端口向管理服务器发送登录请求，在客户端登录成功后可向管理服务器发送业务访问请求，所述业务访问请求携带的信息至少包括：目标设备、业务端口及自身源端口，所述目标设备是管理服务器或业务服务器或前端设备；

管理服务器接收所述业务访问请求后，先判断客户端是否已登录，若该客户端已登录，则根据所述业务访问请求对所述客户端进行授权；若该客户端未登录，则对该客户端不进行授权；

客户端在管理服务器授权后，通过自身源端口对所述业务端口进行业务访问。

7.如权利要求6所述的安全访问系统，其特征在于，管理服务器根据所述业务访问请求对所述客户端进行授权，具体包括：确定目标设备，当目标设备是管理服务器时，对该客户端进行授权；当目标设备是业务服务器或前端设备时，通知目标设备向该客户端开放所述业务端口，且在得到目标设备发送的已向该客户端开放所述业务端口的响应后，对该客户端进行授权。

8.如权利要求6所述的安全访问系统，其特征在于，管理服务器根据所述业务访问请求对所述客户端进行授权，具体包括：确定目标设备，当目标设备是管理服务器时，对该客户端进行授权；当目标设备是业务服务器或前端设备时，通知目标设备向该客户端开放所述业务端口，并对该客户端进行授权。

9.如权利要求6所述的安全访问系统，其特征在于，当管理服务器或业务服务器或前端设备的访问规则达到对应的预设阈值时，根据与预设阈值对应的控制粒度调整访问规则。

10.如权利要求6所述的安全访问系统，其特征在于，所述前端设备通过所述注册端口向管理服务器进行注册时发送的注册报文中携带的信息，至少包括：前端设备的IP地址和mask掩码地址，管理服务器根据前端设备的IP地址和mask掩码地址调整访问规则。

一种安全访问方法及系统

技术领域

[0001] 本申请涉及视频监控领域，尤其涉及一种安全访问方法及系统。

背景技术

[0002] 随着IP视频监控业务的发展，视频监控系统的安全防护变得日益重要。通常入侵者首先会使用漏洞扫描工具对目标设备进行端口扫描，端口扫描一般向目标设备的各个知名端口及部分常用服务端口范围连接消息，根据接收到的消息回应类型判断设备是否在使用该端口，然后通过分析提供服务端口漏洞，进一步发起入侵攻击。然而目前视频监控系统中，前端设备(如IPC网络摄像机、EC编码器)、管理服务器(如VM，Video Management Server视频管理服务器)、业务服务器(如DM，Data Manager Server数据管理服务器)等监控设备的各知名端口及常用服务端口，甚至全部端口均是开放的，容易被入侵者非法入侵攻击。漏洞会不断被发现或新出现，通过升级监控软件版本来解决漏洞和防护攻击，在时间上有一定的迟滞，而且在网设备的升级工作量巨大，故迫切需要一种有效阻止攻击者访问监控设备的方案一劳永逸的消除安全隐患。

发明内容

[0003] 有鉴于此，本申请提供一种安全访问方法及系统，可以有效阻止入侵者对监控设备的扫描入侵。

[0004] 具体地，本申请是通过如下技术方案实现的：

[0005] 根据本发明实施例的第一方面，提供一种安全访问方法，该方法包括：

[0006] 管理服务器的访问规则初始为仅对外开放注册端口和登录端口，业务服务器和前端设备的访问规则初始均为仅对外开放web配置端口；

[0007] 业务服务器通过所述注册端口向管理服务器进行注册，在业务服务器注册成功后，业务服务器增加向管理服务器开放业务服务器自身已设定端口的访问规则；

[0008] 前端设备通过所述注册端口向管理服务器进行注册，在前端设备注册成功后，前端设备增加向管理服务器开放前端设备自身已设定端口的访问规则，同时管理服务器增加向该前端设备开放管理服务器自身已设定端口的访问规则，同时管理服务器通知业务服务器增加向该前端设备开放业务服务器自身已设定端口的访问规则；

[0009] 客户端通过所述登录端口向管理服务器发送登录请求，在客户端登录成功后可向管理服务器发送业务访问请求，所述业务访问请求携带的信息至少包括：目标设备、业务端口及自身源端口，所述目标设备是管理服务器或业务服务器或前端设备；

[0010] 管理服务器接收所述业务访问请求后，先判断客户端是否已登录，若该客户端已登录，则根据所述业务访问请求对所述客户端进行授权；若该客户端未登录，则对该客户端不进行授权；

[0011] 客户端在管理服务器授权后，通过自身源端口对所述业务端口进行业务访问。

[0012] 根据本发明实施例的第二方面，提供一种安全访问系统，所述安全访问系统包括

管理服务器、业务服务器、前端设备和客户端；其中，管理服务器的访问规则初始为仅对外开放注册端口和登录端口，业务服务器和前端设备的访问规则初始均为仅对外开放web配置端口；

[0013] 业务服务器通过所述注册端口向管理服务器进行注册，在业务服务器注册成功后，业务服务器增加向管理服务器开放业务服务器自身已设定端口的访问规则；

[0014] 前端设备通过所述注册端口向管理服务器进行注册，在前端设备注册成功后，前端设备增加向管理服务器开放前端设备自身已设定端口的访问规则，同时管理服务器增加向该前端设备开放管理服务器自身已设定端口的访问规则，同时管理服务器通知业务服务器增加向该前端设备开放业务服务器自身已设定端口的访问规则；

[0015] 客户端通过所述登录端口向管理服务器发送登录请求，在客户端登录成功后可向管理服务器发送业务访问请求，所述业务访问请求携带的信息至少包括：目标设备、业务端口及自身源端口，所述目标设备是管理服务器或业务服务器或前端设备；

[0016] 管理服务器接收所述业务访问请求后，先判断客户端是否已登录，若该客户端已登录，则根据所述业务访问请求对所述客户端进行授权；若该客户端未登录，则对该客户端不进行授权；

[0017] 客户端在管理服务器授权后，通过自身源端口对所述业务端口进行业务访问。

[0018] 本发明通过管理服务器对监控系统中的客户端、前端设备和业务服务器进行集中授权，仅允许经过授权的客户端、前端设备、业务服务器对监控系统中的管理服务器或业务服务器或前端设备等监控设备进行访问，而入侵者无法访问监控系统中的任何监控设备的端口，即使监控设备版本有新增漏洞或暂未解决的漏洞，攻击者由于不能访问监控设备而无法利用版本漏洞，有效保障监控系统中各设备安全，有效阻止入侵者对监控设备的扫描入侵。

附图说明

[0019] 图1是本申请一示例性实施例示出的一种安全访问方法的流程图。

具体实施方式

[0020] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的方法和系统的例子。

[0021] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0022] 应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在.....时”或

“当.....时”或“响应于确定”。

[0023] 请参见图1，图1为本发明实施例提供的一种安全访问方法的流程示意图。该安全访问方法包括：

[0024] S101、管理服务器的访问规则初始为仅对外开放注册端口和登录端口，业务服务器和前端设备的访问规则初始均为仅对外开放web配置端口。

[0025] 本发明实施例中，管理服务器为VM视频管理服务器，统一管理监控系统中的前端设备(比如IPC网络摄像机、EC编码器)、业务服务器(比如DM数据管理服务器)和客户端。为方便描述，下文将管理服务器、前端设备和业务服务器统一称为监控设备。

[0026] 管理服务器初始访问规则为：仅对外开放注册端口和登录端口，即除注册端口和登录端口外，管理服务器不对外开放其他端口。允许任何设备通过注册端口向管理服务器进行注册，允许客户端以用户名及密码鉴权形式通过登录端口向管理服务器进行登录。业务服务器和前端设备的初始访问规则均为：仅对外开放web配置端口，即除web配置端口外，业务服务器和前端设备不对外开放其他端口。允许用户以用户名及密码鉴权形式通过web配置端口登录业务服务器或前端设备的web页面进行配置，配置管理服务器的注册信息后主动向管理服务器进行注册。作为一个例子，管理服务器的注册端口可以为5060，登录端口可以为80，管理服务器的初始访问规则可以如表1所示的访问规则。

[0027] 表1

[0028]

本设备目的端口	源设备	控制行为
5060、80	所有	允许“源设备”访问“本设备目的端口”

[0029] 作为一个例子，前端设备或业务服务器的web配置端口可以为81，前端设备或业务服务器的初始访问规则可以如表2所示的访问规则。

[0030] 表2

[0031]

本设备目的端口	源设备	控制行为
81	所有	允许“源设备”访问“本设备目的端口”

[0032] S102、业务服务器通过注册端口向管理服务器进行注册，在业务服务器注册成功后，业务服务器增加向管理服务器开放业务服务器自身已设定端口的访问规则。

[0033] 业务服务器注册成功后，向管理服务器开放其自身已设定端口的访问规则，业务服务器自身已设定端口包括所有业务类端口及信令交互端口。业务服务器注册成功后，可以向管理服务器开放其自身所有已设定端口，也可以根据实际场景向管理服务器开放其自身部分已设定端口。优选地，在本实施例中，业务服务器注册成功后，向管理服务器开放其所有已设定端口，允许管理服务器访问其所有设定端口，便于后续与管理服务器的通信。

[0034] 作为一个例子，假设管理服务器IP为192.168.1.11，业务服务器IP为192.168.1.12。业务服务器通过5060端口向管理服务器进行注册，注册成功后，业务服务器新增一条访问规则为：允许IP地址为192.168.1.11的管理服务器访问业务服务器所有已设定端口(为方便描述，以下简称为所有端口)，更新后的访问规则如表3所示。

[0035] 表3

[0036]

本设备目的端口	源设备	控制行为

[0037]

81	所有	允许“源设备”访问“本设备目的端口”
所有	192.168.1.11	只允许“源设备”中的 IP 访问“本设备目的端口”

[0038] S103、前端设备通过注册端口向管理服务器进行注册，在前端设备注册成功后，前端设备增加向管理服务器开放前端设备自身已设定端口的访问规则，同时管理服务器增加向该前端设备开放管理服务器自身已设定端口的访问规则，同时管理服务器通知业务服务器增加向该前端设备开放业务服务器自身已设定端口的访问规则。

[0039] 前端设备注册成功后，向管理服务器开放其自身已设定端口的访问规则，前端设备自身已设定端口包括所有业务类端口及信令交互端口。前端设备注册成功后，可以向管理服务器开放其自身所有已设定端口，也可以根据实际场景向管理服务器开放其自身部分已设定端口。优选地，在本实施例中，前端设备注册成功后，向管理服务器开放其所有已设定端口，允许管理服务器访问其所有设定端口。同时，管理服务器增加向该前端设备开放其所有已设定端口的访问规则，同时管理服务器通知业务服务器增加向该前端设备开放业务服务器自身所有已设定端口的访问规则，便于后续通信。比如该前端设备在注册成功后，可以在业务服务器或管理服务器上进行存储、升级等业务，本发明不对具体业务类型进行限定。

[0040] 优选地，前端设备通过所述注册端口向管理服务器进行注册时发送的注册报文中携带的信息，至少包括：前端设备的IP地址和mask掩码地址，管理服务器根据前端设备的IP地址和mask掩码地址调整访问规则。

[0041] 作为一个例子，假设前端设备IP地址为192.168.2.20，mask掩码地址为255.255.255.0，管理服务器IP为192.168.1.11，业务服务器IP为192.168.1.12。前端设备通过5060端口向管理服务器进行注册，发送的注册报文中携带有IP地址192.168.2.20和mask掩码地址255.255.255.0，前端设备的mask掩码地址被管理服务器记录，用于后续调整访问规则(访问规则的调整方式不在此说明，在下文中描述)。前端设备注册成功后，管理服务器在表1所示的访问规则基础上新增一条访问规则，新增的访问规则为：允许IP地址为192.168.2.20，mask掩码地址为255.255.255.0的前端设备访问管理服务器的所有端口，更新后的访问规则如表4所示；前端设备也在表2所示的访问规则基础上新增一条访问规则，新增的访问规则为：允许IP地址为192.168.1.11的管理服务器访问前端设备的所有端口，更新后的访问规则如表3所示。同时，管理服务器通知业务服务器向该前端设备放开所有端口，故业务服务器在表3所示的访问规则基础上新增一条访问规则，新增的访问规则为：允许IP地址为192.168.2.20的前端设备访问业务服务器的所有端口，更新后的访问规则如表5所示。

[0042] 表4

[0043]

本设备目的端口	源设备	控制行为
5060、80	所有	允许“源设备”访问“本设备目的端口”
所有	IP：192.168.2.20 mask:255.255.255.0	只允许“源设备”中的IP访问“本设备目的端口”

[0044] 表5

[0045]

本设备目的端口	源设备	控制行为
81	所有	允许“源设备”访问“本设备目的端口”
所有	192.168.1.11	只允许“源设备”中的IP访问“本设备目的端口”
所有	IP：192.168.2.20	只允许“源设备”中的IP访问“本设备目的端口”

[0046] S104、客户端通过登录端口向管理服务器发送登录请求，在客户端登录成功后可向管理服务器发送业务访问请求。

[0047] 在本实施例中，该业务访问请求携带的信息至少包括：目标设备、业务端口及自身源端口，该目标设备是管理服务器或业务服务器或前端设备。

[0048] 客户端以用户名及密码鉴权形式通过登录端口向管理服务器发送登录请求，登录成功后，可向管理服务器请求管理服务器或业务服务器或前端设备所提供的业务，需要管理服务器对客户端进行授权。

[0049] S105、管理服务器接收客户端发送的业务访问请求后，先判断客户端是否已登录，若该客户端已登录，则根据该业务访问请求对该客户端进行授权；若该客户端未登录，则对该客户端不进行授权。

[0050] 可选地，当客户端已登录时，管理服务器进一步确定目标设备，当目标设备是管理服务器时，对该客户端进行授权；当目标设备是业务服务器或前端设备时，通知目标设备向该客户端开放业务端口，且在得到目标设备发送的已向该客户端开放业务端口的响应后，对该客户端进行授权。

[0051] 可选地，当客户端已登录时，管理服务器进一步确定目标设备，当目标设备是管理服务器时，对该客户端进行授权；当目标设备是业务服务器或前端设备时，通知目标设备向该客户端开放业务端口，并对该客户端进行授权。

[0052] 当客户端已登录且目标设备是业务服务器或前端设备时，管理服务器通知目标设备向该客户端开放业务端口，可以在目标设备返回的已向该客户端开放业务端口的响应

后，再对该客户端进行授权，也可以不等待响应，直接对该客户端进行授权。本发明对此不作限定。

[0053] 本发明实施例中，当客户端发送的业务访问请求所携带的目标设备为管理服务器时，管理服务器直接对客户端进行授权，并更新访问规则，即在原访问规则基础上新增一条访问规则，允许该客户端访问管理服务器的该业务端口。当客户端发送的业务访问请求所携带的目标设备为业务服务器时，管理服务器接收该业务访问请求后，先向业务服务器发送携带有客户端IP地址、客户端源端口和业务端口的业务准备通知；业务服务器在接收到业务准备通知时，更新自身的访问规则，并向管理服务器发送允许该客户端访问该业务端口的准备就绪响应；管理服务器在接收到准备就绪响应后，对客户端进行授权。当客户端发送的业务访问请求所携带的目标设备为前端设备时，管理服务器接收该业务访问请求后，先向前端设备发送携带有客户端IP地址、客户端源端口和业务端口的业务准备通知；前端设备在接收到业务准备通知时，更新自身的访问规则，并向管理服务器发送允许该客户端访问该业务端口的准备就绪响应；管理服务器在接收到准备就绪响应后，对客户端进行授权。

[0054] 本发明实施例中，管理服务器可提供升级业务，业务端口为21；业务服务器可提供回放业务，业务端口为554；前端设备可提供实况业务，业务端口为554。管理服务器、业务服务器及前端设备所支持的业务类型还可以包括其他业务，本发明在此不进行一一举例。

[0055] 作为一个例子，假设前端设备IP为192.168.2.20，mask掩码地址为255.255.255.0，管理服务器IP为192.168.1.11，业务服务器IP为192.168.1.12，客户端IP为192.168.3.10。

[0056] 当客户端请求管理服务器提供的升级业务时，向管理服务器发送携带有自身源端口10000的业务访问请求，请求访问管理服务器的业务端口21，由于客户端已登录成功，则管理服务器直接对该客户端进行授权，同时在表4所示的访问规则基础上新增一条访问规则，新增的访问规则为：允许IP地址为192.168.3.10和源端口为10000的客户端访问管理服务器的业务端口21，更新后的访问规则如表6所示。

[0057] 表6

[0058]

本设备目的端口	源设备	控制行为
5060、80	所有	允许“源设备”访问“本设备目的端口”
所有	IP：192.168.2.20 MASK:255.255.255.0	只允许“源设备”中的IP访问“本设备目的端口”
21	IP：192.168.3.10 源端口：10000	只允许“源设备”中的IP和端口访问“本设备目的端口”

[0059] 当客户端请求业务服务器提供的回放业务时，向管理服务器发送携带有自身源端口10003的业务访问请求，请求访问业务服务器的业务端口554，由于客户端已登录成功，管

理服务器通知业务服务器向IP地址为192.168.3.10,源端口为10003的客户端开发其554端口,业务服务器在接收到该业务准备通知后,在表5所示的访问规则基础上新增一条访问规则,新增的访问规则为:允许IP地址为192.168.3.10和源端口为10003的客户端访问业务服务器的业务端口554,更新后的访问规则如表7所示。

[0060] 表7

[0061]

本设备目的端口	源设备	控制行为
81	所有	允许“源设备”访问“本设备目的端口”
所有	192.168.1.11	只允许“源设备”中的 IP 访问“本设备目的端口”
所有	IP：192.168.2.20	只允许“源设备”中的 IP 访问“本设备目的端口”
554	IP：192.168.3.10 源端口：10003	只允许“源设备”中的 IP 和端口访问“本设备目的端口”

[0062] 当客户端请求前端设备提供的实况业务时,向管理服务器发送携带有自身源端口10005的业务访问请求,请求访问前端设备的业务端口554,由于客户端已登录成功,管理服务器通知前端设备向IP地址为192.168.3.10,源端口为10005的客户端开发其554端口,前端设备在接收到该业务准备通知后,在表3所示的访问规则基础上新增一条访问规则,新增的访问规则为:允许IP地址为192.168.3.10和源端口为10005的客户端访问前端设备的业务端口554,更新后的访问规则如表8所示。

[0063] 表8

[0064]

本设备目的端口	源设备	控制行为
81	所有	允许“源设备”访问“本设备目的端口”
所有	192.168.1.11	只允许“源设备”中的 IP 访问“本设备目的端口”

[0065]

554	IP：192.168.3.10 源端口：10005	只允许“源设备”中的 IP 和端口访问“本设备目的端口”

[0066] S106、客户端在管理服务器授权后,通过自身源端口对目标设备的业务端口进行

业务访问。

[0067] 只有经过管理服务器授权的客户端，可通过自身源端口对目标设备提供服务的业务端口进行访问。其他未经过管理服务器授权的客户端或其他设备，均无法访问目标设备。

[0068] 从上述方法实施例可看出，本发明通过管理服务器对监控系统中的客户端、前端设备和业务服务器进行集中授权，仅允许经过授权的客户端、前端设备、业务服务器对监控设备进行访问，而入侵者无法访问任何监控设备的端口，即使监控设备版本有新增漏洞或暂未解决的漏洞，攻击者由于不能访问监控设备而无法利用版本漏洞，有效保障监控系统中各设备安全，有效阻止入侵者对监控设备的扫描入侵。

[0069] 优选地，当管理服务器或业务服务器或前端设备的访问规则达到对应的预设阈值时，根据与预设阈值对应的控制粒度调整访问规则。

[0070] 本发明实施例中，当管理服务器存储在本地的访问规则数量达到第一阈值时，根据第一控制粒度调整访问规则；当业务服务器存储在本地的访问规则数量达到第二阈值时，根据第二控制粒度调整访问规则；当业务服务器存储在本地的访问规则数量达到第三阈值时，根据第三控制粒度调整访问规则；当前端设备存储在本地的访问规则数量达到第四阈值时，根据第二控制粒度调整访问规则；当业务服务器存储在本地的访问规则数量达到第五阈值时，根据第三控制粒度调整访问规则。

[0071] 可选地，第三阈值比第二阈值的数值大，第五阈值比第四阈值的数值大；根据第一控制粒度、第二控制粒度、第三控制粒度调整访问规则后的访问规则数量较调整前少。

[0072] 本发明实施例中，管理服务器、前端设备、业务服务器的访问规则自动生成，无需人工配置，安全部署方便快捷。为避免访问规则数量过多影响设备性能，访问规则的控制粒度随访问量的变化而动态调整，控制的粒度随着访问量变大而逐步变粗，从而减少规则数量。

[0073] 本发明实施例中，当有前端设备注册成功时，管理服务器存储在本地的访问规则根据初始控制粒度添加新规则，初始控制粒度为“服务端口号+前端设备IP地址”。当有大量前端设备注册时，管理服务器的访问规则数量达到预设的第一阈值(比如5000条)时，将控制粒度变粗，降低为第一控制粒度，第一控制粒度为“服务端口号+前端设备IP网段”，并根据第一控制粒度调整访问规则。

[0074] 作为一个例子，比如管理服务器的访问规则数量达到第一阈值时的访问规则如表9所示，则根据第一控制粒度调整后的访问规则如表10所示。对比表9和表10可看出，根据第一控制粒度调整后的访问规则数量较调整前少。

[0075] 表9

[0076]

本设备目的端口	源设备	控制行为
5060、80	所有	允许“源设备”访问“本设备目的端口”
所有	IP：192.168.2.20 MASK:255.255.255.0	只允许“源设备”中的 IP 访问“本设备目的端口”
21	IP：192.168.3.10 源端口：10000	只允许“源设备”中的 IP 和端口访问“本设备目的端口”
所有	IP：192.168.2.30 MASK:255.255.255.0	只允许“源设备”中的 IP 访问“本设备目的端口”
所有	IP：192.168.4.20 MASK:255.255.255.0	只允许“源设备”中的 IP 访问“本设备目的端口”
所有	IP：192.168.4.30 MASK:255.255.255.0	只允许“源设备”中的 IP 访问“本设备目的端口”

[0077] 表10

[0078]

本设备目的端口	源设备	控制行为
5060、80	所有	允许“源设备”访问“本设备目的端口”
所有	IP：192.168.2.0 MASK:255.255.255.0	只允许“源设备”中的 IP 访问“本设备目的端口”
21	IP：192.168.3.10 源端口：10000	只允许“源设备”中的 IP 和端口访问“本设备目的端口”
所有	IP：192.168.4.0 MASK:255.255.255.0	只允许“源设备”中的 IP 访问“本设备目的端口”

[0079] 本发明实施例中，当有客户端请求访问业务服务器的业务端口时，业务服务器存储在本地的访问规则根据初始控制粒度添加新规则，初始控制粒度为“服务端口号+客户端IP地址+客户端源端口号”。随着访问目标设备的客户端增加，当访问规则数量达到达到预

设的第二阈值(比如600条)时,将控制粒度变粗,降低为第二控制粒度,第二控制粒度为“服务端口号+客户端IP地址”,并根据第二控制粒度调整访问规则;当访问规则数量达到达到预设的第三阈值(比如1000条)时,将控制粒度变粗,降低为第三控制粒度,第三控制粒度为“服务端口号”,并根据第三控制粒度调整访问规则。

[0080] 作为一个例子,比如业务服务器的访问规则数量达到第二阈值时的访问规则如表11所示,则根据第二控制粒度调整后的访问规则如表12所示。对比表11和表12可看出,根据第二控制粒度调整后的访问规则数量较调整前少。

[0081] 表11

[0082]

本设备目的端口	源设备	控制行为
81	所有	允许“源设备”访问“本设备目的端口”
所有	192.168.1.11	只允许“源设备”中的 IP 访问“本设备目的端口”

[0083]

所有	IP：192.168.2.20	只允许“源设备”中的 IP 访问“本设备目的端口”
554	IP：192.168.3.10 源端口：10003	只允许“源设备”中的 IP 和端口访问“本设备目的端口”
21	IP：192.168.3.10 源端口：10007	只允许“源设备”中的 IP 和端口访问“本设备目的端口”
554	IP：192.168.3.11 源端口：10009	只允许“源设备”中的 IP 和端口访问“本设备目的端口”
21	IP：192.168.3.11 源端口：10011	只允许“源设备”中的 IP 和端口访问“本设备目的端口”

[0084] 表12

[0085]

本设备目的端口	源设备	控制行为
81	所有	允许“源设备”访问“本设备目的端口”
所有	192.168.1.11	只允许“源设备”中的 IP 访问“本设备目的端口”
所有	IP：192.168.2.20	只允许“源设备”中的 IP 访问“本设备目的端口”
554、21	IP：192.168.3.10	只允许“源设备”中的 IP 访问“本设备目的端口”
554、21	IP：192.168.3.11	只允许“源设备”中的 IP 访问“本设备目的端口”

[0086] 作为一个例子，比如业务服务器的访问规则数量达到第三阈值时的访问规则如表12所示，则根据第三控制粒度调整后的访问规则如表13所示。对比表12和表13可看出，根据第三控制粒度调整后的访问规则数量较调整前少。

[0087] 表13

[0088]

本设备目的端口	源设备	控制行为
81	所有	允许“源设备”访问“本设备目的端口”
所有	192.168.1.11	只允许“源设备”中的 IP 访问“本设备目的端口”
所有	IP：192.168.2.20	只允许“源设备”中的 IP 访问“本设备目的端口”
554、21	所有	只允许“源设备”中的 IP 访问“本设备目的端口”

[0089] 本发明实施例中，当有客户端请求访问前端设备的业务端口时，前端设备存储在本地的访问规则根据初始控制粒度添加新规则，初始控制粒度为“服务端口号+客户端IP地址+客户端源端口号”。随着访问目标设备的客户端增加，当访问规则数量达到达到预设的第四阈值(比如300条)时，将控制粒度变粗，降低为第二控制粒度，第二控制粒度为“服务端口号+客户端IP地址”，并根据第二控制粒度调整访问规则；当访问规则数量达到达到预设

的第五阈值(比如500条)时,将控制粒度变粗,降低为第三控制粒度,第三控制粒度为“服务端口号”,并根据第三控制粒度调整访问规则。前端设备对访问规则的调整方式同业务服务器,本发明在此不再举例说明。

[0090] 从上述方法实施例可看出,本发明通过管理服务器对监控系统中的客户端、前端设备和业务服务器进行集中授权,仅允许经过授权的客户端、前端设备、业务服务器对监控设备进行访问,而入侵者无法访问任何监控设备的端口,即使监控设备版本有新增漏洞或暂未解决的漏洞,攻击者由于不能访问监控设备而无法利用版本漏洞,有效保障监控系统中各设备安全,有效阻止入侵者对监控设备的扫描入侵。本发明中,管理服务器、前端设备、业务服务器的访问规则自动生成,无需人工配置,安全部署方便快捷,并且访问规则的控制粒度随访问量的变化而动态调整,控制的粒度随着访问量变大而逐步变粗,从而减少规则数量,避免出现因访问规则数量过多而影响设备性能的情况。

[0091] 与前述一种安全访问方法的实施例相对应,本申请还提供了一种安全访问系统的实施例。

[0092] 该安全访问系统包括管理服务器、业务服务器、前端设备和客户端;其中,管理服务器的访问规则初始为仅对外开放注册端口和登录端口,业务服务器和前端设备的访问规则初始均为仅对外开放web配置端口;

[0093] 业务服务器通过所述注册端口向管理服务器进行注册,在业务服务器注册成功后,业务服务器增加向管理服务器开放业务服务器自身已设定端口的访问规则;

[0094] 前端设备通过所述注册端口向管理服务器进行注册,在前端设备注册成功后,前端设备增加向管理服务器开放前端设备自身已设定端口的访问规则,同时管理服务器增加向该前端设备开放管理服务器自身已设定端口的访问规则,同时管理服务器通知业务服务器增加向该前端设备开放业务服务器自身已设定端口的访问规则;

[0095] 客户端通过所述登录端口向管理服务器发送登录请求,在客户端登录成功后可向管理服务器发送业务访问请求,该业务访问请求携带的信息至少包括:目标设备、业务端口及自身源端口,目标设备是管理服务器或业务服务器或前端设备;

[0096] 管理服务器接收业务访问请求后,先判断客户端是否已登录,若该客户端已登录,则根据该业务访问请求对所述客户端进行授权;若该客户端未登录,则对该客户端不进行授权;

[0097] 客户端在管理服务器授权后,通过自身源端口对该业务端口进行业务访问。

[0098] 优选地,管理服务器根据业务访问请求对客户端进行授权,具体包括:确定目标设备,当目标设备是管理服务器时,对该客户端进行授权;当目标设备是业务服务器或前端设备时,通知目标设备向该客户端开放业务端口,且在得到目标设备发送的已向该客户端开放业务端口的响应后,对该客户端进行授权。

[0099] 优选地,管理服务器根据业务访问请求对客户端进行授权,具体包括:确定目标设备,当目标设备是管理服务器时,对该客户端进行授权;当目标设备是业务服务器或前端设备时,通知目标设备向该客户端开放业务端口,并对该客户端进行授权。

[0100] 优选地,当管理服务器或业务服务器或前端设备的访问规则达到对应的预设阈值时,根据与预设阈值对应的控制粒度调整访问规则。

[0101] 优选地,前端设备通过注册端口向管理服务器进行注册时发送的注册报文中携带

的信息，至少包括：前端设备的IP地址和mask掩码地址，管理服务器根据前端设备的IP地址和mask掩码地址调整访问规则。

[0102] 上述系统中各个设备的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0103] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

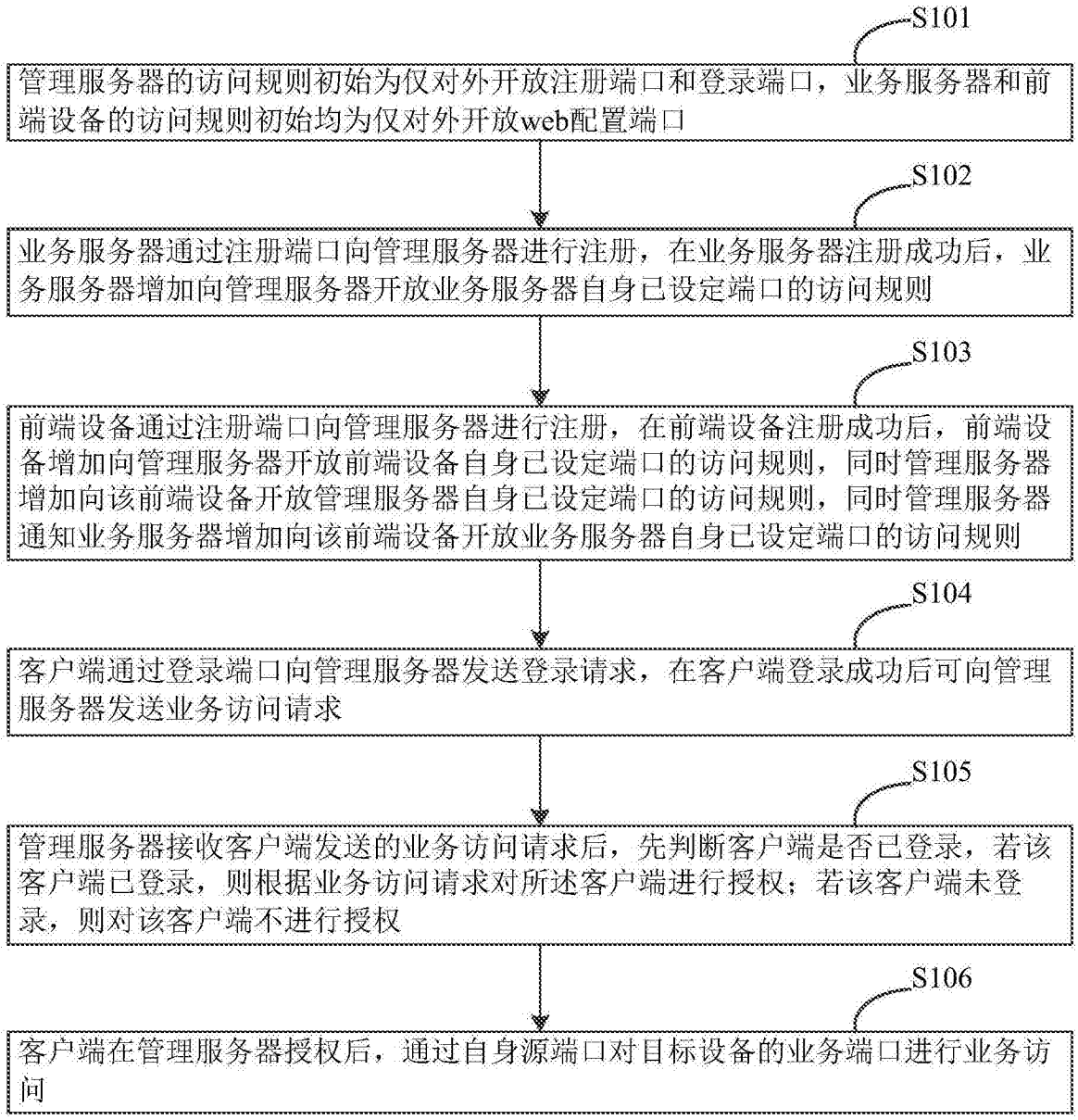

S101
管理服务器的访问规则初始为仅对外开放注册端口和登录端口，业务服务器和前端设备的访问规则初始均为仅对外开放web配置端口
S102
业务服务器通过注册端口向管理服务器进行注册，在业务服务器注册成功后，业务服务器增加向管理服务器开放业务服务器自身已设定端口的访问规则
S103
前端设备通过注册端口向管理服务器进行注册，在前端设备注册成功后，前端设备增加向管理服务器开放前端设备自身已设定端口的访问规则，同时管理服务器增加向该前端设备开放管理服务器自身已设定端口的访问规则，同时管理服务器通知业务服务器增加向该前端设备开放业务服务器自身已设定端口的访问规则
S104
客户端通过登录端口向管理服务器发送登录请求，在客户端登录成功后可向管理服务器发送业务访问请求
S105
管理服务器接收客户端发送的业务访问请求后，先判断客户端是否已登录，若该客户端已登录，则根据业务访问请求对所述客户端进行授权；若该客户端未登录，则对该客户端不进行授权
S106
客户端在管理服务器授权后，通过自身源端口对目标设备的业务端口进行业务访问

图1