(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114978890 B
(45)授权公告日 2024.01.23

(21)申请号 202210526920.1

(22)申请日 2022.05.16

(65)同一申请的已公布的文献号
申请公布号 CN 114978890 A

(43)申请公布日 2022.08.30

(73)专利权人 南京信息职业技术学院
地址 210023 江苏省南京市栖霞区仙林大学城文澜路99号

(72)发明人 刘新娥

(74)专利代理机构 南京纵横知识产权代理有限公司 32224
专利代理师 孙永生

(51)Int.Cl.
H04L 41/0803(2022.01)
H04L 67/63(2022.01)

(56)对比文件
CN 105991789 A,2016.10.05
CN 103516820 A,2014.01.15
CN 101605154 A,2009.12.16
CN 102148879 A,2011.08.10
US 2013058256 A1,2013.03.07
傅丰;徐洪章.端口映射的分析与应用.天中学刊.2006,(第02期),全文.
王新宇;胡华海.发布网络内部服务器及内网建站的方法.科技信息.2009,(第01期),全文.

审查员 高婷婷

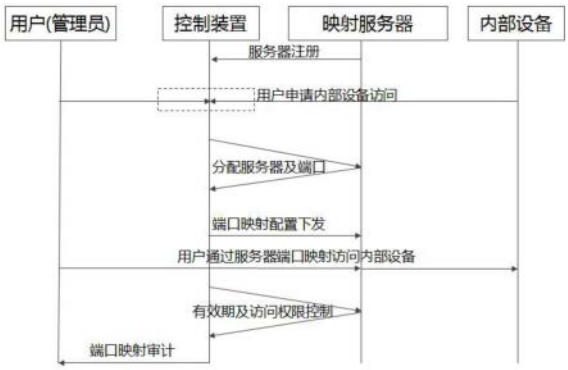
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种端口映射系统及其映射方法

(57)摘要

本发明公开了一种端口映射系统及其映射方法,映射系统包括控制装置、内部网络设备和若干端口映射服务器;所述控制装置用于登记端口映射服务器支持的内部网络设备及外部网络设备地址、可用端口和端口转发性能;用于,在接收到用户的访问内部网络设备的请求后,对访问请求进行分析,查找已配置的端口映射数据库,若未查找到,则根据已登记的端口映射服务器信息选择空闲的端口映射服务器端口,为相应内部网络设备配置端口映射关系,以及下发至所选择的端口映射服务器;控制装置根据新配置的端口映射关系数据,将内部网络设备对应的外部网络地址及端口返回给用户。本发明能够实现对端口映射服务器的机制控制管理,降低企业网络的维护成本和技术难度。



CN 114978890 B

1.一种端口映射系统,其特征在于:包括控制装置、内部网络设备和若干端口映射服务器;

所述端口映射服务器用于根据端口映射配置将外部网络的端口映射至对应的内部网络端口;所述端口映射配置记录有外部网络端口与内部网络端口的映射关系;

所述控制装置用于登记端口映射服务器支持的内部网络设备及外部网络设备地址、可用端口和端口转发性能;还用于,在接收到用户的访问内部网络设备的请求后,对访问请求进行分析,查找已配置的端口映射数据库,得到为相应内部网络设备配置的外部网络地址和端口,返回给用户,使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器;

所述控制装置查找已配置的端口映射数据库时,若未查找到为该内部网络设备配置的外部网络地址和端口,则根据已登记的端口映射服务器信息选择空闲的端口映射服务器端口,为相应内部网络设备配置端口映射关系,并将所配置的端口映射关系数据更新至端口映射数据库,以及下发至所选择的端口映射服务器;控制装置根据新配置的端口映射关系数据,将内部网络设备对应的外部网络地址及端口返回给用户;

控制装置存储端口映射数据,映射方法包括以下步骤:

控制装置对若干端口映射服务器支持的内部网络设备及外部网络设备地址、可用端口和端口转发性能进行登记;

控制装置接收用户提交访问内部网络设备的请求,并对用户的访问请求进行分析;

当用户的访问请求通过时,控制装置查找已配置的端口映射数据库,得到为相应内部网络设备配置的外部网络地址和端口,并返回给用户,使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器,再通过端口映射服务器将外部网络的端口映射至对应的内部网络端口;

所述控制装置查找已配置的端口映射数据库时,若未查找到为该内部网络设备配置的外部网络地址和端口,控制装置根据已登记的端口映射服务器信息选择空闲的端口映射服务器端口,获取映射内部网络设备的空闲端口,生成外部网络设备地址、端口和内部网络设备地址、端口的表项,并将表项转换成工具支持的配置格式,且更新至端口映射数据库,以及下发至所选择的端口映射服务器;控制装置根据新配置的端口映射关系数据,将内部网络设备对应的外部网络地址及端口返回给用户;使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器,再通过端口映射服务器将外部网络的端口映射至对应的内部网络端口。

2.根据权利要求1所述的一种端口映射系统,其特征在于,访问请求包括:内部网络设备地址及端口、有效期和访问协议。

3.根据权利要求2所述的一种端口映射系统,其特征在于,还包括:当用户访问内部网络设备的有效期到期时,控制装置删除为相应内部网络设备配置端口映射关系。

4.根据权利要求1所述的一种端口映射系统,其特征在于:登记的若干端口映射服务器分别与外部网络和内部网络联通,且安装有端口映射软件。

5.根据权利要求4所述的一种端口映射系统,其特征在于:所述端口映射软件包括Rinetd和Portmap。

6.根据权利要求1所述的一种端口映射系统,其特征在于:分配空闲端口映射服务器端

口时,控制装置至少配置一个端口映射服务器,或者采用映射服务器的负载均衡策略。

7.根据权利要求1所述的一种端口映射系统,其特征在于,还包括:用户在访问内部设备时,控制装置对用户提供端口的审计、权限和安全控制。

一种端口映射系统及其映射方法

技术领域

[0001] 本发明属于网络通信技术领域,涉及一种端口映射系统及其映射方法。

背景技术

[0002] 很多企业都搭建了内部局域网,同时需要将内部局域网接入外部网络,比如因特网。随着因特网的迅速发展,IP地址短缺是一个十分突出的问题,企业的服务资源不可能每个都有一个IP地址,端口映射是一个内外网络互通的解决方案。

[0003] 端口映射就是将内网主机的一个端口映射为外网主机的一个端口,当用户访问外网IP的某个端口时,服务器自动将用户请求映射到内网主机的端口上,这样既可以解决内外网络互通的问题,也节省了IP地址空间,对企业而言就是几个外网IP地址就可以满足企业的大量的内部需求。

[0004] 端口映射可以通过一些软件比如Rinetd,Portmap等来实现,只要在服务器上安装这些软件,就可以在这个服务器上实现端口映射。

[0005] 端口映射方法解决了企业外部网络和内部隔离网络的互通问题,但也增加了企业的运维成本,尤其存在大量互通业务时,配置工作量大,配置效率低。如果出现配置错误或端口重复被映射,导致业务不通或者阻塞,故障排查困难,排查技术要求高,人力工作量大。

发明内容

[0006] 本发明的目的在于克服现有技术中的不足,提供一种端口映射系统及其映射方法,能够实现对端口映射服务器的机制控制管理,降低企业网络的维护成本和技术难度。

[0007] 为达到上述目的,本发明是采用下述技术方案实现的:

[0008] 一方面,本发明提供一种端口映射系统,包括控制装置、内部网络设备和若干端口映射服务器;

[0009] 所述端口映射服务器用于根据端口映射配置将外部网络的端口映射至对应的内部网络端口;所述端口映射配置记录有外部网络端口与内部网络端口的映射关系;

[0010] 所述控制装置用于登记端口映射服务器支持的内部网络设备及外部网络设备地址、可用端口和端口转发性能;还用于,在接收到用户的访问内部网络设备的请求后,对访问请求进行分析,查找已配置的端口映射数据库,得到为相应内部网络设备配置的外部网络地址和端口,返回给用户,使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器;

[0011] 所述控制装置查找已配置的端口映射数据库时,若未查找到为该内部网络设备配置的外部网络地址和端口,则根据已登记的端口映射服务器信息选择空闲的端口映射服务器端口,为相应内部网络设备配置端口映射关系,并将所配置的端口映射关系数据更新至端口映射数据库,以及下发至所选择的端口映射服务器;控制装置根据新配置的端口映射关系数据,将内部网络设备对应的外部网络地址及端口返回给用户。

[0012] 另一方面,本发明提供第一方面所述的端口映射系统的映射方法,控制装置存储

端口映射数据,映射方法包括以下步骤:

[0013] 控制装置对若干端口映射服务器支持的内部网络设备及外部网络设备地址、可用端口和端口转发性能进行登记;

[0014] 控制装置接收用户提交访问内部网络设备的请求,并对用户的访问请求进行分析;

[0015] 当用户的访问请求通过时,控制装置查找已配置的端口映射数据库,得到为相应内部网络设备配置的外部网络地址和端口,并返回给用户,使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器,再通过端口映射服务器将外部网络的端口映射至对应的内部网络端口;

[0016] 所述控制装置查找已配置的端口映射数据库时,若未查找到为该内部网络设备配置的外部网络地址和端口,控制装置根据已登记的端口映射服务器信息选择空闲的端口映射服务器端口,获取映射内部网络设备的空闲端口,生成外部网络设备地址、端口和内部网络设备地址、端口的表项,并将表项转换成工具支持的配置格式,且更新至端口映射数据库,以及下发至所选择的端口映射服务器;控制装置根据新配置的端口映射关系数据,将内部网络设备对应的外部网络地址及端口返回给用户;使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器,再通过端口映射服务器将外部网络的端口映射至对应的内部网络端口。

[0017] 可选的,访问请求包括:内部网络设备地址及端口、有效期和访问协议。

[0018] 可选的,还包括:当用户访问内部网络设备的有效期到期时,控制装置删除为相应内部网络设备配置端口映射关系。

[0019] 可选的,登记的若干端口映射服务器分别与外部网络和内部网络联通,且安装有端口映射软件。

[0020] 可选的,所述端口映射软件包括Rinetd和Portmap。

[0021] 可选的,分配空闲端口时,控制装置至少配置一个端口映射服务器,或者采用映射服务器的负载均衡策略。

[0022] 可选的,用户在访问内部设备时,控制装置对用户提供端口的审计、权限和安全控制。

[0023] 与现有技术相比,本发明所达到的有益效果:

[0024] 本发明提供的端口映射方法能够实现对端口映射服务器的机制控制管理,提高配置效率,避免出现配置错误或端口重复被映射时,业务不通或者阻塞,故障排查困难的问题;并且映射服务器的管理对用户是透明的,降低企业网络的维护成本和技术难度。

附图说明

[0025] 图1所示为本发明端口映射的交互流程图;

[0026] 图2所示为本发明端口映射的结构图。

具体实施方式

[0027] 下面结合附图对本发明作进一步描述。以下实施例仅用于更加清楚地说明本发明的技术方案,而不能以此来限制本发明的保护范围。

[0028] 在本发明的描述中,需要理解的是,术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作,因此不能理解为对本发明的限制。此外,术语“第一”、“第二”等仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”等的特征可以明示或者隐含地包括一个或者更多个该特征。在本发明的描述中,除非另有说明,“多个”的含义是两个或两个以上。

[0029] 在本发明的描述中,需要说明的是,除非另有明确的规定和限定,术语“安装”、“相连”、“连接”应做广义理解,例如,可以是固定连接,也可以是可拆卸连接,或一体地连接;可以是机械连接,也可以是电连接;可以是直接相连,也可以通过中间媒介间接相连,可以是两个元件内部的连通。对于本领域的普通技术人员而言,可以通过具体情况理解上述术语在本发明中的具体含义。

[0030] 实施例一:

[0031] 如图1和图2所示,一种端口映射系统,包括控制装置、内部网络设备和若干端口映射服务器;

[0032] 所述端口映射服务器用于根据端口映射配置将外部网络的端口映射至对应的内部网络端口;所述端口映射配置记录有外部网络端口与内部网络端口的映射关系;

[0033] 所述控制装置用于登记端口映射服务器支持的内部网络设备及外部网络设备地址、可用端口和端口转发性能;还用于,在接收到用户的访问内部网络设备的请求后,对访问请求进行分析,查找已配置的端口映射数据库,得到为相应内部网络设备配置的外部网络地址和端口,返回给用户,使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器;

[0034] 所述控制装置查找已配置的端口映射数据库时,若未查找到为该内部网络设备配置的外部网络地址和端口,则根据已登记的端口映射服务器信息选择空闲的端口映射服务器端口,为相应内部网络设备配置端口映射关系,并将所配置的端口映射关系数据更新至端口映射数据库,以及下发至所选择的端口映射服务器;控制装置根据新配置的端口映射关系数据,将内部网络设备对应的外部网络地址及端口返回给用户。

[0035] 实施例二:

[0036] 如图1和图2所示,基于实施例一所述的一种端口映射系统,本实施例提供一种端口映射系统的映射方法,控制装置存储端口映射数据,映射方法包括以下步骤:

[0037] S1,控制装置对若干端口映射服务器支持的内部网络设备及外部网络设备地址、可用端口和端口转发性能进行登记,登记的若干端口映射服务器安装有端口映射软件,端口映射软件包括Rinetd和Portmap;

[0038] S2,控制装置接收用户提交访问内部网络设备地址及端口、有效期和访问协议的请求,并对用户的访问请求进行分析;

[0039] S3,控制装置查找已配置的端口映射数据库,得到为相应内部网络设备配置的外部网络地址和端口,返回给用户,使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器;

[0040] S3,控制装置查找已配置的端口映射数据库时,若未查找到为该内部网络设备配置的外部网络地址和端口,控制装置根据已登记的端口映射服务器信息选择空闲的端口映射服务器端口,为相应内部网络设备配置端口映射关系,配置的端口映射关系是根据端口映射软件类型,控制装置获取映射设备的空闲端口,生成外部网络设备地址、端口和内部网络设备地址、端口的表项,根据端口映射设备类型将表项转换成工具支持的配置格式,并将所配置的端口映射关系数据更新至端口映射数据库,以及下发至所选择的两个端口映射服务器中的一个,多个端口映射服务器可实现端口备份及高可用性,或者采用映射服务器的负载均衡策略提升网络性能;控制装置根据新配置的端口映射关系数据,将内部网络设备对应的外部网络地址及端口返回给用户,使得用户能够通过所述外部网络地址和端口访问对应的端口映射服务器, 再通过端口映射服务器将外部网络的端口映射至对应的内部网络端口;用户在访问内部设备时,控制装置对用户提供端口的审计、权限和安全控制。

[0041] S4,当用户访问内部网络设备的有效期到期时,控制装置删除为相应内部网络设备配置端口映射关系。

[0042] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明技术原理的前提下,还可以做出若干改进和变形,这些改进和变形也应视为本发明的保护范围。

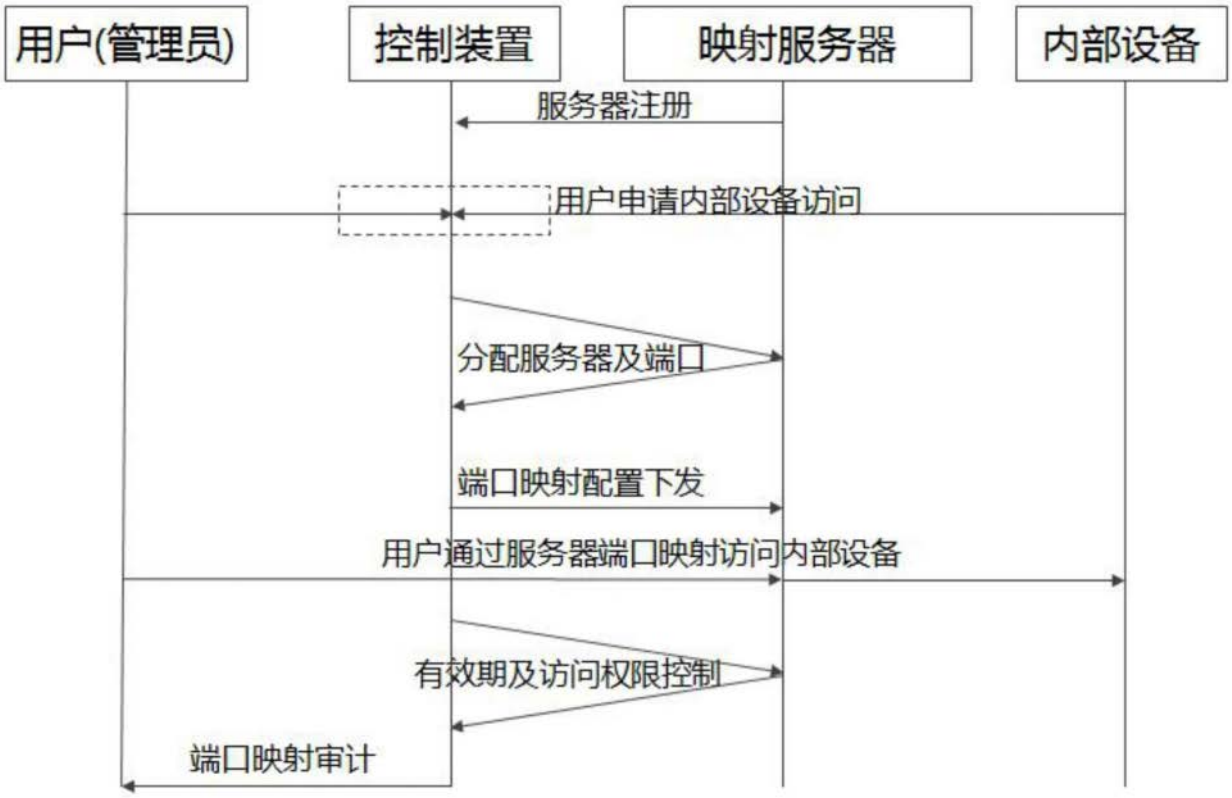

用户(管理员)
控制装置
映射服务器
内部设备
服务器注册
用户申请内部设备访问
分配服务器及端口
端口映射配置下发
用户通过服务器端口映射访问内部设备
有效期及访问权限控制
端口映射审计

图1

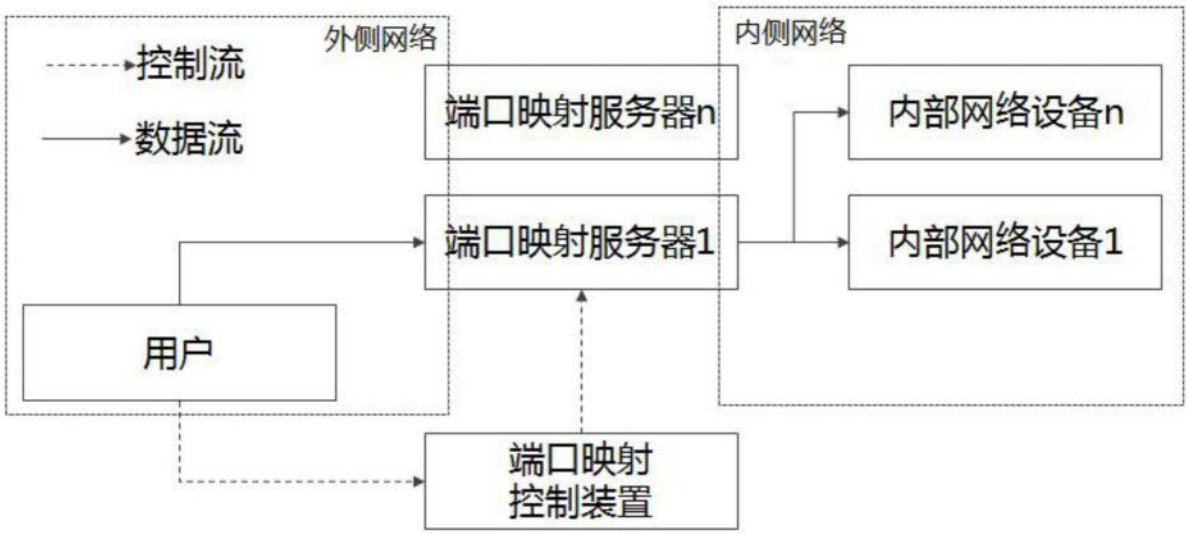

外侧网络
内侧网络
控制流
数据流
端口映射服务器n
内部网络设备n
端口映射服务器1
内部网络设备1
用户
端口映射
控制装置

图2