(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101764742 B
(45)授权公告日 2015.09.23

(21)申请号 200910215820.1
(22)申请日 2009.12.30
(73)专利权人 福建星网锐捷网络有限公司
地址 350002 福建省福州市仓山区金山大道618号桔园州工业园19#楼
(72)发明人 吴晶晶
(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 黄志华
(51)Int.Cl.
H04L 12/70(2013.01)
H04L 29/06(2006.01)

(56)对比文件
CN 101163336 A,2008.04.16,
CN 101039213 A,2007.09.19,
CN 101552784 A,2009.10.07,
CN 101425903 A,2009.05.06,

审查员 高静

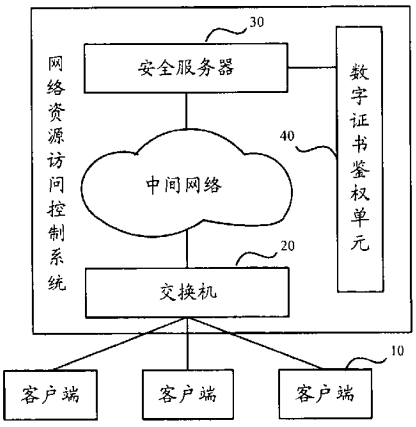
权利要求书3页 说明书9页 附图3页

(54)发明名称

一种网络资源访问控制系统及方法

(57)摘要

本发明涉及信息安全领域，具体涉及一种网络资源访问控制系统及方法，该系统包括：交换机，接收客户端请求访问网络资源时发起的登录认证请求并转发，根据接收的针对所述登录认证请求的访问控制信息，对发起所述登录认证请求的客户端进行网络资源访问控制；安全服务器，接收所述交换机转发的登录认证请求，对所述登录认证请求所包括的身份认证信息进行认证，认证通过后根据预先设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，向交换机下发针对该登录认证请求的访问控制信息。本发明是针对用户而非计算机来进行网络资源访问控制，避免了现有ACL策略基于IP地址进行网络资源访问控制所存在的各种缺陷。



CN 101764742 B

1. 一种网络资源访问控制系统，其特征在于，包括：

交换机，接收客户端请求访问网络资源时发起的登录认证请求并转发，根据接收的针对所述登录认证请求的访问控制信息，对发起所述登录认证请求的客户端进行网络资源访问控制；

安全服务器，接收所述交换机转发的登录认证请求，对所述登录认证请求所包括的身份认证信息进行认证，认证通过后根据预先设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，向所述交换机下发针对该登录认证请求的访问控制信息，其中，所述身份认证信息为用户的身份认证信息；

其中，所述登录认证请求还包括请求访问的安全域，所述安全服务器包括：

安全域确定单元，用于根据接收的登陆认证请求确定请求访问的安全域；

安全域访问控制单元，用于确定所述登录认证请求中的身份认证信息对请求访问的安全域的访问权限，向所述交换机下发访问控制信息进行请求访问安全域的访问控制；

所述安全服务器还包括：

访问记录获取单元，用于获取不同身份认证信息正在访问的安全域信息；

所述安全域访问控制单元，还用于根据所述访问记录获取单元获取的信息确定该身份认证信息有正在访问的其它安全域时，向交换机下发针对该身份认证信息的删除其它安全域下网络资源列表的隔离指令；

所述交换机在接收到所述隔离指令时，删除针对该身份认证信息的其它安全域下网络资源列表。

2. 如权利要求 1 所述的系统，其特征在于，所述安全服务器包括：

认证方式确定单元，用于确定所接收的登录认证请求所采用的认证方式；

认证单元，用于以所述确定的认证方式，对所述登录认证请求所包括的身份认证信息进行认证；

权限查询单元，用于在认证通过后，查询根据不同认证方式对应不同级别的网络资源访问权限，所设置的采用不同认证方式认证时，不同身份认证信息对应可访问的安全域及安全域下网络资源列表。

3. 如权利要求 2 所述的系统，其特征在于，

该系统还包括：

数字证书鉴权单元，用于在所述认证方式确定单元所确定的认证方式为数字证书方式时，对数字证书形式的身份认证信息进行鉴权，并将鉴权结果返回给所述认证单元；

所述认证单元在接收到鉴权通过的鉴权结果后，对所述数字证书形式的身份认证信息进行认证。

4. 如权利要求 1 所述的系统，其特征在于，

所述交换机包括：

访问权限获取单元，用于根据所述访问控制信息获取发起所述登录认证请求的客户端可访问的安全域及安全域下的网络资源列表；

访问控制单元，用于允许发起所述登陆请求的客户端访问属于所述安全域及安全域下的网络资源列表中网络资源。

5. 如权利要求 4 所述的系统，其特征在于，

所述交换机还包括权限反馈单元，用于将所述安全域列表及安全域下的网络资源列表，发送到发起所述登录认证请求的客户端。

6. 如权利要求 1 所述的系统，其特征在于，

所述交换机还用于接收客户端发起的退出认证请求并转发，根据接收的卸载指令，将所述卸载指令所针对的访问控制信息删除；

所述安全服务器还用于接收所述交换机转发的退出认证请求，根据所述退出认证请求所包括的身份认证信息，确定与包括该身份认证信息的登陆认证请求对应的访问控制信息，向所述交换机下发针对所述确定的访问控制信息的卸载指令。

7. 一种网络资源访问控制方法，其特征在于，包括：

交换机接收客户端请求访问网络资源时发起的登录认证请求并转发；

安全服务器接收所述交换机转发的登录认证请求，对所述登录认证请求所包括的身份认证信息进行认证，其中，所述身份认证信息为用户的身份认证信息；

认证通过后根据预先设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，向交换机下发针对该登录认证请求的访问控制信息；

所述交换机根据所述安全服务器下发的访问控制信息，对发起所述登录认证请求的客户端进行网络资源访问控制；

其中，所述登录认证请求还包括请求访问的安全域，所述安全服务器根据接收的登陆认证请求确定请求访问的安全域；

确定所述登录认证请求中的身份认证信息对请求访问的安全域的访问权限，向所述交换机下发访问控制信息进行请求访问安全域的访问控制；

该方法，还包括获取不同身份认证信息正在访问的安全域信息的步骤；

所述安全服务器还根据所述访问记录获取单元获取的信息确定该身份认证信息有正在访问的其它安全域时，向交换机下发针对该身份认证信息的删除其它安全域下网络资源列表的隔离指令；

所述交换机在接收到所述隔离指令时，删除针对该身份认证信息的其它安全域下网络资源列表。

8. 如权利要求 7 所述的方法，其特征在于，

所述交换机所接收的登陆认证请求采用多种认证方式中的一种；

所述预先设置的不同认证信息对应可访问的安全域及安全域下的网络资源列表，具体通过如下方式设置：

对采用不同认证方式的登陆认证请求，分配不同级别的网络资源访问权限；

根据所分配的网络资源访问权限级别，设置采用不同认证方式认证时，不同认证信息对应可访问的安全域及安全域下的网络资源列表。

9. 如权利要求 7 所述的方法，其特征在于，

所述交换机接收的访问控制信息为发起所述登录认证请求的客户端可访问的安全域及安全域下的网络资源列表；

所述交换机进行网络资源访问控制具体为，允许发起所述登陆请求的客户端访问属于所述安全域及安全域下的网络资源列表中网络资源。

10. 如权利要求 7 所述的方法，其特征在于，

所述交换机在接收客户端发起的退出认证请求时，将该退出认证请求转发到安全服务器；

所述安全服务器根据该退出认证请求所包括的身份认证信息，确定与包括该身份认证信息的登陆认证请求对应的访问控制信息，并将针对所述确定的访问控制信息的卸载指令发送到交换机；

所述交换机在接收到安全服务下发的卸载指令后，将卸载指令所针对的访问控制信息删除。

一种网络资源访问控制系统及方法

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种保证网络资源访问安全的网络资源访问控制系统及方法。

背景技术

[0002] 随着信息化发展的逐步深入，我们对信息系统的依赖越来越强，国家信息基础设施和重要信息系统能否安全正常地运行直接关系到国家安全和社会秩序。但是大型信息系统的安全保障体系建设是一个极为复杂的工作，为大型信息系统建立一套完整和有效的安全保障体系一直是个世界性的难题。一些行业性机构或大型企业的信息系统应用众多、结构复杂、覆盖地域广阔、涉及的行政部门和人员众多，因此信息系统面临着各种性质的安全威胁，如间谍、黑客、病毒蠕虫、木后门、非法的合作伙伴等。信息系统安全保障要求的内容极为广泛，从物理安全、网络安全、系统安全、应用安全到安全管理、安全组织建设等等，凡是涉及到影响正常运行和业务连续性的都可以认为是信息安全问题。

[0003] 对于如何解决信息系统的信息安全问题，美国及西方发达国家为了抵御信息网络的脆弱性和安全威胁，制定了一系列强化信息网络安全建设的政策和标准，其中一个很重要思想就是按照安全保护强度划分不同的安全等级，以指导不同领域的信息安全工作。

[0004] 经过我国信息安全领域有关部门和专家学者的多年研究，在借鉴国外先进经验和结合我国国情的基础上，提出了分等级保护的策略来解决我国信息网络安全问题，即针对信息系统建设和使用单位，根据其使用单位的重要程度、信息系统承载业务的重要程度、信息内容的重要程度、系统遭到攻击破坏后造成的危害程度等安全需求以及安全成本等因素，依据国家规定的等级划分标准，设定其保护等级，自主进行信息系统安全建设和安全管理，提高安全保护的科学性、整体性、实用性。

[0005] 等级保护中，将由实施共同安全策略的主体和客体组成的集合定义为安全域。安全域可以理解为同一信息系统内根据信息的性质、使用主体、安全目标和策略等元素的不同来划分的不同逻辑子网或网络。

[0006] 依据等级保护的规定，在政务内网划分不同部门、机关的物理安全域，不同的部门、机关应该各自隶属不同的安全域，安全域之间需要通过专用安全硬件（防火墙等）实施隔离，严格限制互访；依据分级保护的规定，在同一安全域内的各种应用，依据密级不同需要划分高密、低密等不同的权限等级，不同的终端接入用户对不同密级的应用的访问权限不同，如高权限的用户允许访问高密、低密应用；低权限的用户仅允许访问低密应用。同一用户所拥有的权限由管理员指定。

[0007] 为了保证信息系统的信息安全，目前最常用的方法是通过部署防火墙设备来实现安全域间的隔离及同一安全域下不同权限等级用户的权限限制，防火墙的原理为基于IP地址来对终端接入用户和信息系统进行分别标识，在防火墙设备上配置访问控制表(Access Control List,ACL)策略来达到终端接入用户访问权限的控制，ACL使用包过滤技术，在路由器上或交换机上读取报文头中的信息如源地址、目的地址、源端口、目的端口等，

根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。因此可以通过手动配置防火墙设备上的 ACL 来隔离不同的安全域，及设定终端接入用户拥有哪些信息系统的访问权限。

[0008] 通过在防火墙设备上配置 ACL 策略来保证信息系统的信息安全具有以下缺陷 ：1) 因为 ACL 策略是基于 IP 地址来对终端接入用户和信息系统进行标识，在防火墙设备上配置 ACL 策略来达到访问权限的控制，当出现 IP 地址变更时（如终端接入用户的 IP 变更等），需要手动进行配置调整，难于使用 ；2) 通过手动配置 ACL 策略，策略直接同终端接入计算机的 IP 关联，同一个用户想要访问不同权限的系统，需要跑到不同的计算机上去访问，不符合现实中的权限分配模式 ；3) 因为手动配置 ACL 策略，策略直接同终端接入计算机的 IP 关联，这样终端接入计算机可以通过修改 IP 的方式来使得防火墙的控制失效 ；4) 虽然安全域间互相隔离，但是终端接入用户可以同时访问多个安全域，这样会导致中间人攻击，例如没有安全域 A 访问权限的用户，可以通过控制有安全域 A 访问权限的计算机，来达到对安全域 A 中网络资源的访问，造成了安全隐患。

发明内容

[0009] 本发明提供一种网络资源访问控制系统及方法，用以解决现有技术中基于 IP 建立的 ACL 控制策略进行网络资源访问权限设置所存在的问题。

[0010] 本发明提供一种网络资源访问控制系统，包括 ：

[0011] 交换机，接收客户端请求访问网络资源时发起的登录认证请求并转发，根据接收的针对所述登录认证请求的访问控制信息，对发起所述登录认证请求的客户端进行网络资源访问控制 ；

[0012] 安全服务器，接收所述交换机转发的登录认证请求，对所述登录认证请求所包括的身份认证信息进行认证，认证通过后根据预先设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，向所述交换机下发针对该登录认证请求的访问控制信息，其中，所述身份认证信息为用户的身份认证信息 ；

[0013] 其中，所述登录认证请求还包括请求访问的安全域，所述安全服务器包括 ：

[0014] 安全域确定单元，用于根据接收的登陆认证请求确定请求访问的安全域 ；

[0015] 安全域访问控制单元，用于确定所述登录认证请求中的身份认证信息对请求访问的安全域的访问权限，向所述交换机下发访问控制信息进行请求访问安全域的访问控制 ；

[0016] 所述安全还服务器包括 ：

[0017] 访问记录获取单元，用于获取不同身份认证信息正在访问的安全域信息 ；

[0018] 所述安全域访问控制单元，还用于根据所述访问记录获取单元获取的信息确定该身份认证信息有正在访问的其它安全域时，向交换机下发针对该身份认证信息的删除其它安全域下网络资源列表的隔离指令 ；

[0019] 所述交换机在接收到所述隔离指令时，删除针对该身份认证信息的其它安全域下网络资源列表。

[0020] 本发明还提供了一种网络资源访问控制方法，包括 ：

[0021] 交换机接收客户端请求访问网络资源时发起的登录认证请求并转发 ；

[0022] 所述安全服务器接收所述交换机转发的登录认证请求，对所述登录认证请求所包

括的身份认证信息进行认证，其中，所述身份认证信息为用户的身份认证信息；

[0023] 认证通过后根据预先设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，向交换机下发针对该登录认证请求的访问控制信息；

[0024] 所述交换机根据所述安全服务器下发的访问控制信息，对发起所述登录认证请求的客户端进行网络资源访问控制；

[0025] 其中，所述登录认证请求还包括请求访问的安全域，所述安全服务器根据接收的登陆认证请求确定请求访问的安全域；

[0026] 确定所述登录认证请求中的身份认证信息对请求访问的安全域的访问权限，向所述交换机下发访问控制信息进行请求访问安全域的访问控制；

[0027] 该方法，还包括获取不同身份认证信息正在访问的安全域信息的步骤；

[0028] 所述安全服务器还根据所述访问记录获取单元获取的信息确定该身份认证信息有正在访问的其它安全域时，向交换机下发针对该身份认证信息的删除其它安全域下网络资源列表的隔离指令；

[0029] 所述交换机在接收到所述隔离指令时，删除针对该身份认证信息的其它安全域下网络资源列表。

[0030] 利用本发明提供的网络资源访问控制系统及方法，具有以下有益效果：

[0031] 由于采用发起登录认证请求，及根据预先设置的不同身份认证信息对应可访问的网络资源的方式进行网络资源访问限制，因此是针对用户而非计算机来进行网络资源访问控制，避免了现有 ACL 策略基于 IP 地址进行网络资源访问控制所存在的各种缺陷。

附图说明

[0032] 图 1 为本发明实施例中网络资源访问控制系统结构框图；

[0033] 图 2 为本发明网络资源访问控制方法的流程图；

[0034] 图 3 为本发明实施例中采用用户名和密码认证时的网络资源访问控制方法流程图；

[0035] 图 4 为本发明实施例中采用数字证书认证时对应的网络资源访问控制方法流程图。

具体实施方式

[0036] 下面结合附图和实施例对本发明提供的网络资源访问控制系统及方法进行更详细的说明。

[0037] 如图 1 所示，本发明提供的网络资源访问控制系统包括：

[0038] 交换机 20，接收客户端 10 请求访问网络资源时发起的登录认证请求，并将其转发给安全服务器 30，根据所述安全服务器 30 下发的针对该登录认证请求的访问控制信息，对发起所述登录认证请求的客户端 10 进行网络资源访问控制。因此，用户在个人计算机上利用登录认证的方式进行上网；

[0039] 所述安全服务器 30，接收所述交换机 20 转发的登录认证请求，对所述登录认证请求所包括的身份认证信息进行认证，认证通过后根据预先设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，向所述交换机 20 下发针对该登录认证请求的

访问控制信息。

[0040] 本发明在原有交换机功能的基础上，增加了安全管理服务器及交换机同安全管理服务器交互的一些功能。在本发明中，所述交换机包括：访问权限获取单元，用于根据所述访问控制信息获取发起所述登录认证请求的客户端可访问的安全域及安全域下的网络资源列表；访问控制单元，用于允许发起所述登陆请求的客户端访问属于所述安全域及安全域下的网络资源列表中网络资源，因此，交换机根据安全管理服务器下发的访问控制信息，可以生成发起认证登录请求的客户端可以访问的安全域及安全域下的网络资源列表，进而获得 ACL 列表，所生成的 ACL 是与认证登录请求对应，而不是像现有技术那样与 IP 地址对应的。针对用户而非计算机来进行安全域控制，符合日常应用中的权限分配方式。

[0041] 安全管理服务器作为整个访问控制的核心服务器，在本发明中，它通过预先设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，可以控制采用认证方式上网的 PC 能够访问的网络权限；能够指定不同身份认证信息对应用户拥有哪些安全域下哪些网络资源（具体为信息系统）的访问权限，用户在个人 PC 上的使用客户端进行认证上网，选择认证方式以及要访问的安全域后认证上网，安全管理服务器通过下发访问控制信息给交换机，能够保证用户通过认证后只能接入有权限访问的网络。

[0042] 所述登录认证请求还包括请求访问的安全域，优选地，该安全服务器还包括：安全域确定单元，用于根据接收的登陆认证请求确定请求访问的安全域；安全域访问控制单元，用于确定所述登录认证请求中的身份认证信息对请求访问的安全域的访问权限，向所述交换机下发访问控制信息进行请求访问安全域的访问控制。这样可以实现用户针对某个安全域发出的登录认证请求进行请求安全域的访问控制，只允许用户访问其请求的那个安全域。

[0043] 进一步地，为了实现用户在同一时刻只能访问一个安全域，实现对于同一用户对不同安全域之间的隔离，所述安全还服务器包括：

[0044] 访问记录获取单元，用于获取不同身份认证信息正在访问的安全域信息，如针对某个身份认证信息，若之前向交换机下发过某个安全域下的网络资源列表时，表示该身份认证信息对应用户正在访问该安全域，若之前没有向交换机下发过某个安全域下的网络资源列表，或是向交换机下发过某个安全域下的网络资源列表后又向交换机下发删除针对该身份认证信息的该安全域下的网络资源列表时，表示该用户没有正在访问该安全域；

[0045] 所述安全域访问控制单元，在确定所述身份认证信息对请求访问的安全域具有访问权限时，向交换机下发请求访问的安全域下的网络资源列，且根据所述访问记录获取单元获取的信息确定该身份认证信息有正在访问的其它安全域时，向交换机下发针对该身份认证信息的删除其它安全域下网络资源列表的隔离指令；

[0046] 所述交换机在接收到所述隔离指令时，删除针对该身份认证信息的其它安全域下网络资源列表。从而实现用户只能访问其请求访问的安全域而与其它安全域隔离。

[0047] 认证作为一种准入网络的控制方式，用户只有认证通过后才能访问网络，未认证或认证未通过时无法访问网络。本发明可以采用现有的各种认证方式。如可以采用用户名加密码的认证方式，也可以采用数字证书认证方式。优选地，该系统还包括：认证方式确定单元，用于确定所接收的登录认证请求所采用的认证方式；认证单元，用于以所述确定的认证方式，对所述登录认证请求所包括的身份认证信息进行认证；权限查询单元，用于在认证

通过后，查询根据不同认证方式对应不同级别的网络资源访问权限，所设置的采用不同认证方式认证时，不同身份认证信息对应可访问的安全域及安全域下网络资源列表。该系统还包括：数字证书鉴权单元，用于在所述认证方式确定单元所确定的认证方式为数字证书方式时，对数字证书形式的身份认证信息进行鉴权，并将鉴权结果返回给所述认证单元；所述认证单元在接收到鉴权通过的鉴权结果后，对所述数字证书形式的身份认证信息进行认证。

[0048] 公钥基础设施(Public Key Infrastructure,PKI)是利用公开密钥理论和技术建立的提供安全服务的在线基础设施。公钥系统中的用户都有一对相关的密钥，其中一个密钥加密的信息只能被相应的另一个密钥解密。用户保存其中一个密钥作为私钥，而把另一个密钥与拥有者的信息捆绑后公开发布为公钥。这样，可以用别人的公钥加密信息，而只有私钥持有者才能读懂该信息；还可以用自己的私钥签名信息，其他人利用公钥就可鉴别信息发送者的身份。公钥加密需要解决一个问题：加密信息的发送者需要认定公钥确实是接收者的，如果他用第三者的公钥去加密，他希望的接收者无法解密该信息，而拥有私钥的第三者却可以做到。这实际上就涉及到应用公钥技术的关键：如何确认某个人真正拥有的公钥。

[0049] 在PKI中，为了确保用户的身份及他所持有密钥的正确匹配，公开密钥系统需要一个值得信赖而且独立的第三方机构充当认证中心(Certification Authority,CA)，来确认声称拥有公开密钥的人的真正身份。认证中心发放一个叫数字证书的身份证明。这个数字证书包含了用户身份的部分信息及用户所持有的公开密钥。认证中心利用本身的私钥为数字证书加盖上数字签名。

[0050] 任何想发放自己公钥的用户，可以去认证中心申请自己的数字证书。认证中心在鉴定该用户的真实身份后，颁发包含用户公钥的数字证书。其他用户只要能验证数字证书是真实的，并且信任颁发证书的认证中心，就可以确认用户的公钥。

[0051] 鉴于此，所述交换机20所接收的登陆认证请求采用多种认证方式中的一种，如采用用户加密码的认证方式，或采用数字证书认证方式；所述安全服务器30对采用不同认证方式的登陆认证请求，分配不同级别的网络资源访问权限，如可以为不需要认证的用户能够访问最低密的网络资源，使用用户名加密码认证的用户能够访问较为低密的网络资源，使用数字证书认证的用户可以访问高密的网络资源。安全服务器根据所分配的网络资源访问权限级别，设置采用不同认证方式认证时，不同身份认证信息对应可访问的安全域及安全域下网络资源列表。

[0052] 登陆认证请求采用的认证方式为数字证书认证方式时，所述登陆认证请求所包括的身份认证信息采用数字证书方式，该系统还包括：

[0053] 数字证书鉴权单元40，用于对所述安全服务器30接收的数字证书方式的身份认证信息进行鉴权，并将鉴权结果返回给所述安全服务器30。安全服务器30对经鉴权有效的数字证书所包括的身份认证信息进行认证。即数字证书中所包括的身份认证信息经客户端的私钥加密，经数字证书鉴权单元40鉴权后，得出公钥是客户端的公钥，因此，安全服务器30利用客户端的公钥解密得到身份认证信息并进行认证。

[0054] 本实施例中的数字证书鉴权单元40作为CA基础设施，包括了RA(Register Authority)、CA(Certificate Authority)、LDAP(Lightweight Directory Access

Protocol）服务器等设施，数字证书鉴权单元 40 通过公钥密码体制中用户私钥的机密性来提供用户身份的唯一性验证，并通过公钥数字证书的方式为每个合法用户的公钥提供一个合法性的证明，从而建立了从用户公钥到数字证书 ID 号之间的唯一映射关系。

[0055] 本发明提供的网络资源访问控制系统中由安全管理服务器下发给安全交换机来达到对安全交换机下接入用户的访问控制，提供了一种简便、灵活的访问控制方法，进行网络资源如信息系统的安全域划分和管理，整个安全域访问控制过程自动完成，即使客户端的 IP 发生更改也无需管理员手动管理；可以针对用户来进行安全域及安全域下网络资源设置，而不再是使用计算机来进行设置，有效的解决了通过手动修改计算机的一些配置（如 IP 地址）来绕开控制的问题。

[0056] 本发明可以进行细粒度的安全域设置，对于一个用户，通过安全服务器的预先设置，可以拥有多个安全域的权限。在同一个安全域中的各个信息系统，又可以依据密级不同划分成高密、低密等不同的权限等级，不同的用户对不同密级的应用的访问权限不同。

[0057] 本实施例中所述访问控制信息具体为发起所述登录认证请求的客户端可访问的安全域及安全域下的网络资源列表，所述交换机进行网络资源访问控制具体为，允许发起所述登陆请求的客户端访问属于所述安全域及安全域下的网络资源列表中网络资源。交换机还用于将所述安全域列表及安全域下的网络资源列表，发送到发起所述登录认证请求的客户端。这样用户在客户端可以直接获取到该用户本身可以访问的安全域列表及安全域下的网络资源列表，从而有针对性访问这些网络资源，提高了访问的效率。另外，由于用户同一时刻只能访问一个安全域，这样可以避免网内其它安全域的用户通过访问这台计算机来操作这个安全域中信息系统的安全问题，有效的避免了中间人攻击，保障了信息系统的安全。

[0058] 本实施例中所述交换机还用于接收客户端发起的退出认证请求，并将该退出认证请求转发到安全服务器，在接收到安全服务下发的卸载指令后，将卸载指令所针对的访问控制信息删除；所述安全服务器还用于根据交换机转发的退出认证请求所包括的身份认证信息，确定与包括该身份认证信息的登陆认证请求对应的访问控制信息及对应的记录，将所述对应的记录删除，并将针对所述确定的访问控制信息的卸载指令发送到交换机。

[0059] 如图 2 所示，本发明提供的网络资源访问控制方法包括步骤：

[0060] S201，交换机接收客户端请求访问网络资源时发起的登录认证请求，并将其转发给安全服务器；S202，所述安全服务器接收所述交换机转发的登录认证请求，对所述登录认证请求所包括的身份认证信息进行认证；S203，认证通过后，安全服务器根据预先设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，向交换机下发针对该登录认证请求的访问控制信息；S204，所述交换机根据所述安全服务器下发的针对该登录认证请求的访问控制信息，对发起所述登录认证请求的客户端进行网络资源访问控制。

[0061] 依照本发明的实施例中，步骤 S201 中交换机所接收的登陆认证请求采用多种认证方式中的一种，登陆认证请求优选包括请求访问的安全域、身份认证信息等；步骤 S203 中预先设置的不同认证信息对应可访问的安全域及安全域下的网络资源列表，采用如下方式设置：对采用不同认证方式的登陆认证请求，分配不同级别的网络资源访问权限；根据所分配的网络资源访问权限级别，设置采用不同认证方式认证时，不同认证信息对应可访问的安全域及安全域下的网络资源列表。另外，所述登录认证请求还包括请求访问的安全

域，为了实现对请求访问的安全域的访问控制，所述安全服务器根据接收的登陆认证请求确定请求访问的安全域；根据所述请求访问的安全域，确定请求访问安全域的访问权限，向所述交换机下发访问控制信息进行请求访问安全域的访问控制。这样实现了用户只能访问其请求的那个安全域。

[0062] 为了实现同一时刻只允许用户访问一个安全域的目的，该方法还包括获取不同身份认证信息正在访问的安全域信息的步骤；所述安全服务器在确定具有对所请求访问的安全域的访问权限时，向交换机下发请求访问的安全域下的网络资源列，且根据确定获取不同身份认证信息正在访问的安全域信息确定有正在访问的其它安全域时，还用于向交换机下发删除所述其它安全域下网络资源列表的隔离指令；所述交换机在接收到所述隔离指令时，删除其它安全域下网络资源列表。

[0063] 下面给出以用户名和密码的认证方式，及以数字证书的认证方式进行网络资源访问控制的详细过程。

[0064] 管理员在安全服务器上为用户开户，支持用户名、密码认证和数字证书认证两种认证方式，对这两种认证方式对应以下两种不同的开户方式：

[0065] A. 用户名、密码认证：在安全管理服务器上直接开户，开户内容包括用户名和密码等，将用户名、密码信息告知用户；

[0066] B. 在CA中心申请数字证书，将其分发给用户（可以采用USB-KEY作为存储介质）。

[0067] 如图3所示，用于以用户名、密码的认证方式在客户端登录时，网络资源访问控制具体过程为：

[0068] S301，用户在客户端输入用户名和密码发送登录认证请求，以请求接入网络资源；优选地，客户端还具有认证方式选择列表，用户可以选择使用用户名、密码或是数字证书认证的方式来认证上网；安全域选择列表，用户认证前可以选择要访问的安全域进行认证；

[0069] S302，交换机接收客户端请求访问网络资源时发起的登录认证请求，并将其转发给安全服务器；

[0070] S303，安全服务器接收所述交换机转发的登录认证请求，对所述登录认证请求所包括的用户名和密码进行认证，若认证通过，根据预先设置的不同用户名和密码对应可访问的安全域及安全域下的网络资源列表，向交换机下发针对该登录认证请求的网络资源列表，若登录认证请求包括请求访问的安全域，在确定请求访问的安全域有访问权限时，向交换机下发请求访问的安全域下的网络资源列表，同时确定该登录认证请求的身份认证信息是否正在访问其它安全域，若是，则向交换机下发针对该身份认证信息的删除其它安全域下网络资源的隔离指令。

[0071] 管理员在安全管理服务器上针对需要进行访问控制的网络资源，按现有标准划分不同的安全域，不同安全域之间的网络资源在网络中是被严格隔离的；并配置安全域中的网络资源，本实施例中具体为信息系统。安全管理服务器将安全域和信息系统存储到数据库表中；数据库表结构如下：

[0072] 表1安全域表

[0073]

字段	属性	长度	是否可为空	描述

securityDomainIndex	bigint	16	No	索引,唯一主键
securityDomainName	varchar	32	No	安全域名称
securityDomainDesc	varchar	256	Yes	安全域描述

[0074] 表 2 信息系统表

[0075]

字段	属性	长度	是否可为空	描述
infoSystemIndex	bigint		No	索引,唯一主键
infoSystemName	varchar	64	No	信息系统名称
ip	varchar	15	No	信息系统的 IP 地址
url	varchar	256	No	信息系统的访问 URL 地址

[0076]

securityDomianIndex	bigint		No	标识信息系统属于哪个安全域

[0077] 经过以上设置后,为开户的用户分配拥有哪些安全域下的哪些信息系统的访问权限,得到经过认证的用户可访问的安全域及安全域下网络资源列表。

[0078] 优选地,在用户发起的登录认证请求包含请求访问的安全域时,也可以只下发该安全域下的网络资源列表,上述客户端发送的登录认证请求和后续退出认证请求还优选包括客户端 IP、介质访问控制 MAC 地址等信息。安全服务器对用户认证后向交换机下发打开端口的通知,并获取用户登录的安全域下有访问权限的信息系统,根据用户 IP、用户 MAC、信息系统 IP,生成对应的 ACL,并向这个用户所接入的交换机端口下发这个 ACL,以限制用户只能访问这些有权限的信息系统。

[0079] S304,交换机接收的安全服务器下发的发起所述登录认证请求的客户端可访问的安全域及安全域下的网络资源列表,进行发起所述登录认证请求的客户端网络资源访问控制 :允许发起所述登陆请求的客户端访问属于所述安全域及安全域下的网络资源列表中网络资源 ;交换机在接收到所述隔离指令时,删除其它安全域下网络资源列表

[0080] S305,若在步骤 S303 中,安全服务器只下发了用户请求登录的安全域下的网络资源列表,在该步骤,优选地,安全服务器还将用户对应可以访问的安全域列表及安全下网络资源列表下发给交换机,由交换机将其下发给发起登录认证请求的客户端,这样可以在客户端将用户可以访问的安全域及安全域下网络资源列表展示给用户。

[0081] S306,客户端在访问结束后发出退出认证请求,该退出认证请求中也携带身份认证信息 ;

[0082] S307,所述交换机在接收客户端发起的退出认证请求时,将该退出认证请求转发到安全服务器 ;

[0083] S308,安全服务器根据该退出认证请求所包括的身份认证信息,确定与包括该身

份认证信息的登陆认证请求对应的网络资源列表，删除与该身份认证信息对应的正在访问某个安全域的记录，并将针对所述确定的网络资源列表的卸载指令发送到交换机；

[0084] S309，交换机在接收到安全服务下发的卸载指令后，将卸载指令所针对的网络资源列表删除。

[0085] 如图 4 所示为以数字证书的认证方式进行网络资源访问控制的详细过程，与采用用户名加密码不同的是，增加了步骤 S403，安全服务器需要将接收的登录认证请求中的数字认证发送到数字证书鉴权单元进行鉴权，在鉴权通过后执行步骤 S404。

[0086] 本实施例中安全管理服务器向客户端发送用户当前有权限访问的安全域列表（包括安全域名称）和信息系统列表（包括信息系统名称和访问 URL 地址）；认证客户端将立即将信息系统列表展示给用户，用户通过点击列表上的链接可以直接访问信息系统；用户退出认证后，再次认证时，将只能选择自己有访问权限的安全域来认证。

[0087] 用户通过客户端退出认证时，客户端会将用户名上报给安全管理服务器，安全管理服务器向接入安全交换机下发关闭端口的通知，并向接入安全交换机下发删除这个用户所有相关 ACL 的命令，交换机将会删除将相应的 ACL。

[0088] 具体实施时，按照图 1 结构搭建网络，在网络中的任意位置搭建安全管理服务器，在个人 PC 上安装认证客户端，个人 PC 直接连接到安全接入交换机。优选地，本实施例中在安全管理服务器上，配置未认证上网的 PC 机可以访问哪些网络资源，即有些用户在不需要认证的情况下也可以访问一些密级较低的网络资源。配置访问控制模板，只允许计算机访问某台指定的修复服务器；配置访问控制策略，指定刚才配置的访问控制模板在哪些交换机上生效；在安全管理服务器上，按照等分级保护的要求，配置安全域；在安全管理服务器上，配置信息系统，并为信息系统指派安全域；在安全管理服务器上，为用户分配安全域和信息系统的访问权限。

[0089] 举例说明，用户可以登录行政司和财务司两个安全域，并且拥有行政司下日志系统和财务司下工资查询系统的访问权限，没有其它系统的访问权限；经过以上配置，当用户未认证上网时，只能访问指定的那台修复服务器资源，当用户认证上网时，选择登录行政司后认证，将弹出可以访问的信息系统列表（这里只有日志系统的链接），用户点击日志系统的链接，可以访问日志系统；用户这时候只能访问这个信息系统，访问不了其它信息系统。

[0090] 经过以上配置，当用户认证上网时，选择登录财务司后认证，将弹出可以访问的信息系统列表（这里只有工资查询系统的链接），用户点击工资查询系统的链接，可以访问工资查询系统；用户这时候只能访问这个信息系统，访问不了其它信息系统；用户退出认证后，将无法访问任何网络。

[0091] 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。

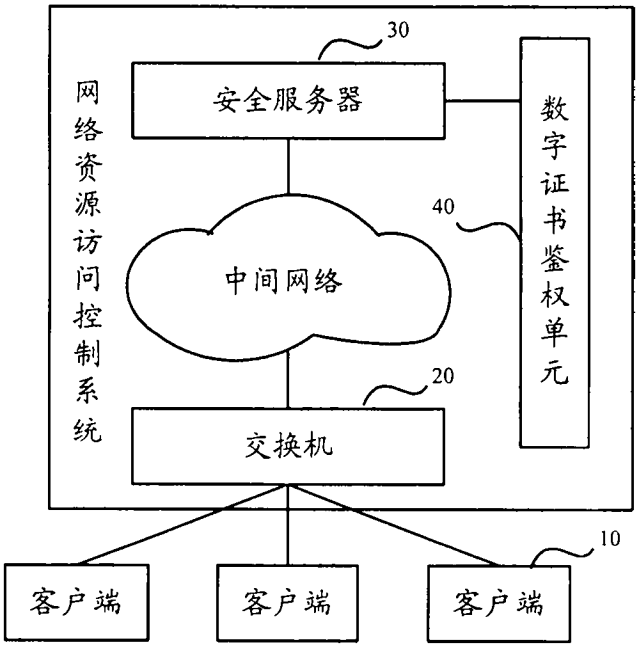

网络资源访问控制系统
30
安全服务器
数字证书鉴权单元
40
中间网络
20
交换机
10
客户端
客户端
客户端

图 1

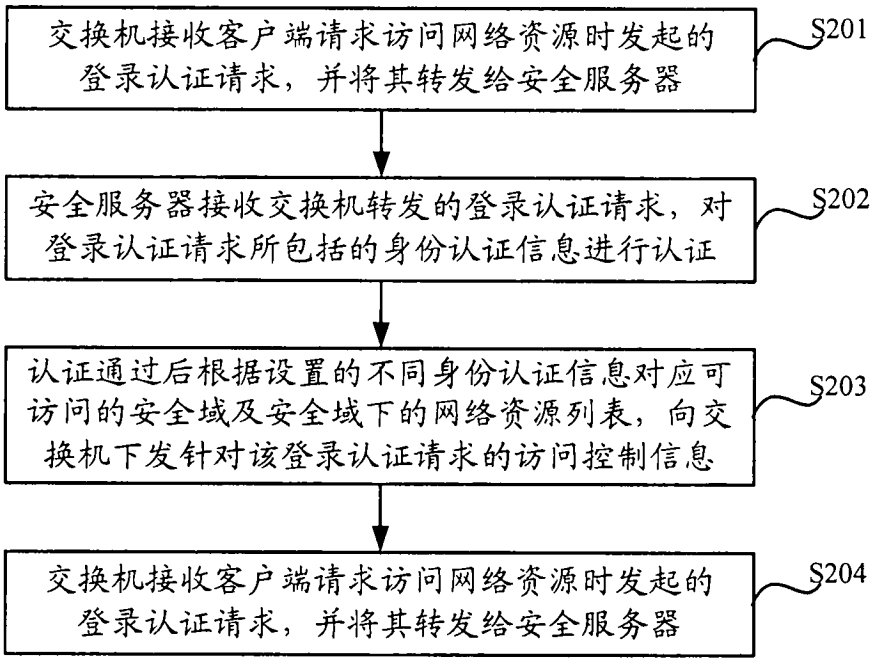

交换机接收客户端请求访问网络资源时发起的登录认证请求，并将其转发给安全服务器
S201
安全服务器接收交换机转发的登录认证请求，对登录认证请求所包括的身份认证信息进行认证
S202
认证通过后根据设置的不同身份认证信息对应可访问的安全域及安全域下的网络资源列表，向交换机下发针对该登录认证请求的访问控制信息
S203
交换机接收客户端请求访问网络资源时发起的登录认证请求，并将其转发给安全服务器
S204

图 2

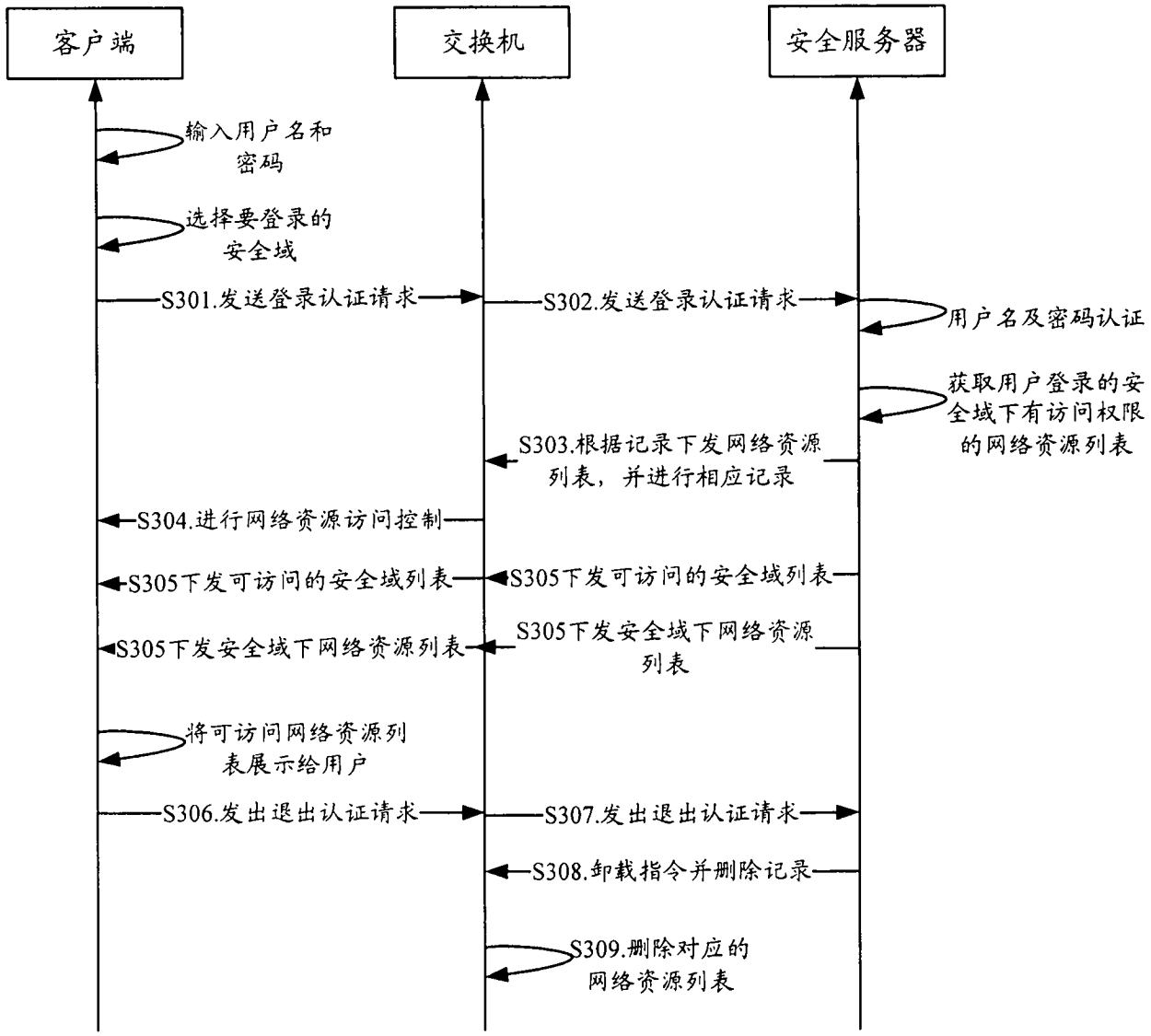

客户端
交换机
安全服务器
输入用户名和密码
选择要登录的安全域
S301.发送登录认证请求
S302.发送登录认证请求
用户名及密码认证
获取用户登录的安全域下有访问权限的网络资源列表
S303.根据记录下发网络资源列表，并进行相应记录
S304.进行网络资源访问控制
S305下发可访问的安全域列表
S305下发可访问的安全域列表
S305下发安全域下网络资源列表
S305下发安全域下网络资源列表
将可访问网络资源列表展示给用户
S306.发出退出认证请求
S307.发出退出认证请求
S308.卸载指令并删除记录
S309.删除对应的网络资源列表

图 3

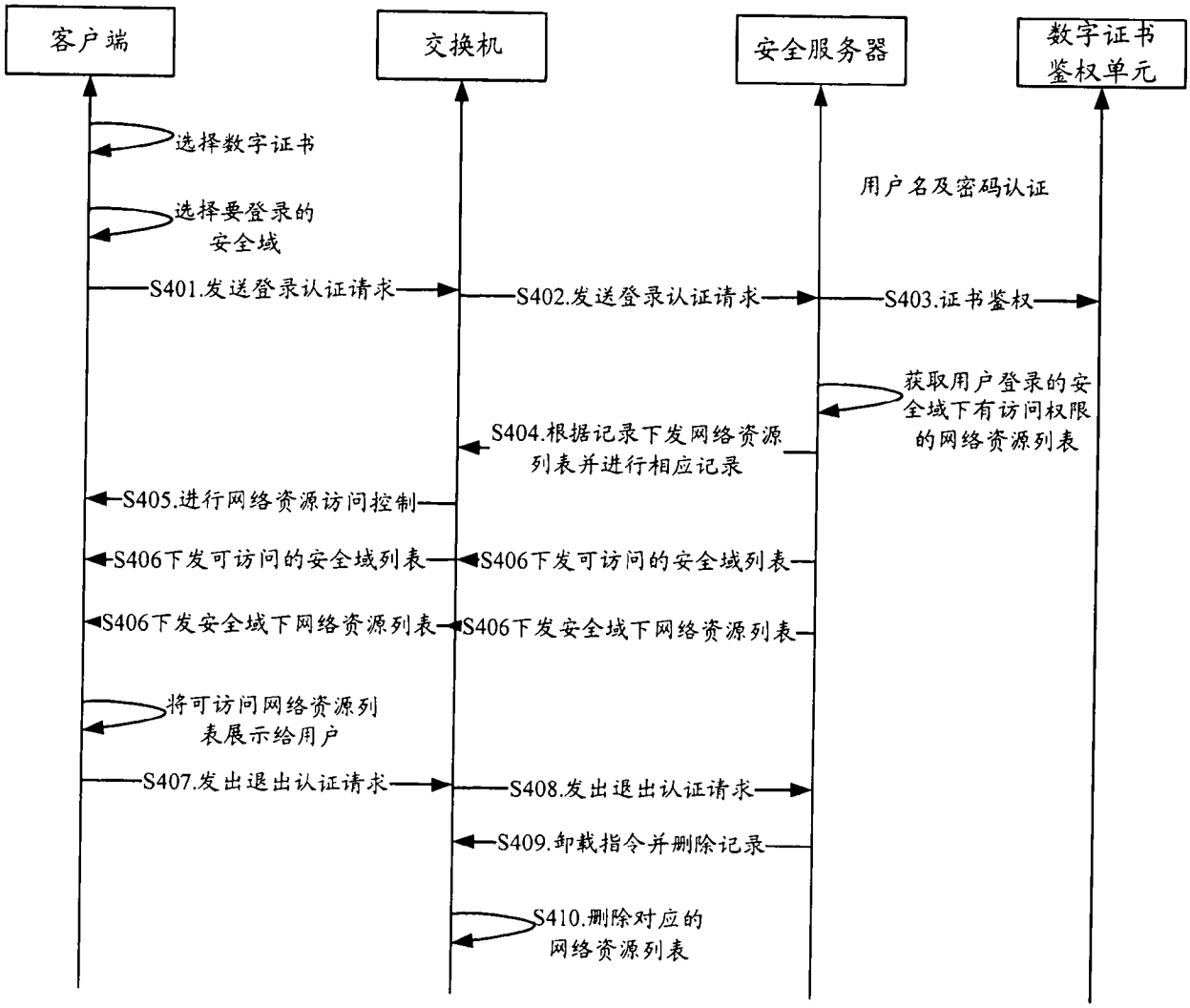

客户端
交换机
安全服务器
数字证书鉴权单元
选择数字证书
选择要登录的安全域
用户名及密码认证
S401.发送登录认证请求
S402.发送登录认证请求
S403.证书鉴权
获取用户登录的安全域下有访问权限的网络资源列表
S404.根据记录下发网络资源列表并进行相应记录
S405.进行网络资源访问控制
S406下发可访问的安全域列表
S406下发可访问的安全域列表
S406下发安全域下网络资源列表
S406下发安全域下网络资源列表
将可访问网络资源列表展示给用户
S407.发出退出认证请求
S408.发出退出认证请求
S409.卸载指令并删除记录
S410.删除对应的网络资源列表

图 4