(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114499976 B
(45)授权公告日 2022.11.04

(21)申请号 202111626510.6
(22)申请日 2021.12.28
(65)同一申请的已公布的文献号
申请公布号 CN 114499976 A
(43)申请公布日 2022.05.13
(73)专利权人 航天科工智慧产业发展有限公司
地址 100044 北京市西城区高梁桥路6号5号楼A区(T4)06A1(德胜园区)
专利权人 北京计算机技术及应用研究所
(72)发明人 贾炜 白翔宇 樊杰龙 任思路 郭旭东
(74)专利代理机构 北京市盛峰律师事务所 11337
专利代理师 席小东
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/1095(2022.01)

(56)对比文件
CN 101447862 A,2009.06.03
CN 113452653 A,2021.09.28
CN 109117313 A,2019.01.01
CN 110855634 A,2020.02.28
CN 109005179 A,2018.12.14
CN 101635704 A,2010.01.27
CN 101277308 A,2008.10.01
CN 106789755 A,2017.05.31
CN 103139058 A,2013.06.05
CN 111526100 A,2020.08.11
CN 112261067 A,2021.01.22
CN 110213318 A,2019.09.06
王进.跨网络信息流转的安全防护设计.《电子技术与软件工程》.2021,

审查员 李国鑫

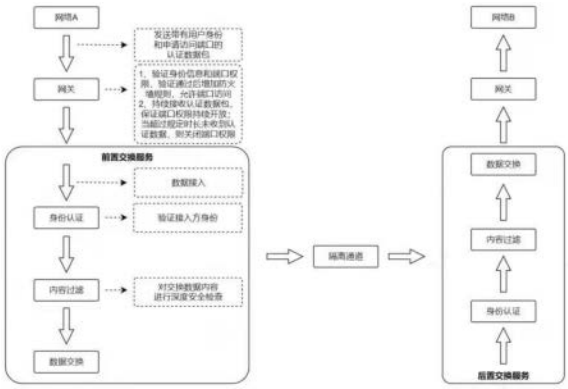
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种实现跨网交换的数据交换方法

(57)摘要

本发明提供一种实现跨网交换的数据交换方法,包括以下步骤:步骤1,构建网络架构;所述网络架构包括:第一网络、第一网关、前置交换服务平台、通信隔离通道、后置交换服务平台、第二网关和第二网络;所述第一网络,依次通过所述第一网关和所述前置交换服务平台,连接到所述通信隔离通道的一端;所述通信隔离通道的另一端,依次通过所述后置交换服务平台和所述第二网关,连接到所述第二网络,由此实现所述第一网络和所述第二网络的通信连接。本发明提供的一种实现跨网交换的数据交换方法具有以下优点:本发明提供的一种实现跨网交换的数据交换方法,可有效提高跨网数据交换的安全性,满足跨网数据交换的通信需求。



CN 114499976 B

1.一种实现跨网交换的数据交换方法,其特征在于,包括以下步骤:

步骤1,构建网络架构;所述网络架构包括:第一网络、第一网关、前置交换服务平台、通信隔离通道、后置交换服务平台、第二网关和第二网络;

所述第一网络,依次通过所述第一网关和所述前置交换服务平台,连接到所述通信隔离通道的一端;所述通信隔离通道的另一端,依次通过所述后置交换服务平台和所述第二网关,连接到所述第二网络,由此实现所述第一网络和所述第二网络的通信连接;

步骤2,所述第一网关配置多个网络端口,在默认状态下,所有网络端口均为隐藏且关闭状态,对所述第一网络不可见;

当第一网络需要向第二网络通信时,所述第一网络与所述第一网关协商,确定可向所述第一网络短时间开放的网络端口,表示为网络端口P;

所述第一网关向所述第一网络开放网络端口P,其他网络端口保持关闭状态;

步骤3,所述第一网络向所述第一网关发送带有用户身份和申请访问端口M的认证数据包;

步骤4,所述第一网关在向第一网络开放网络端口P后,判断是否在设定时间内接收到所述第一网络发送的认证数据包,如果没有接收到,则关闭网络端口P,结束流程;如果接收到,则执行步骤5;

步骤5,所述第一网关从所述认证数据包中解析出用户身份和申请访问端口M的请求,一方面,对所述用户身份进行验证,另一方面,验证申请访问端口M是否与网络端口P相同,如果相同,则表示端口权限验证通过;

如果用户身份和端口权限中存在任意一项没有验证通过,则所述第一网关关闭网络端口P,结束流程;

如果用户身份和端口权限均验证通过后,所述第一网关增加防火墙规则,向此用户身份的客户端开放网络端口P;允许所述第一网络中的此用户身份的客户端访问所述第一网关的网络端口P;

在所述第一网关向用户身份的客户端开放网络端口P后,所述第一网关持续监测是否每隔设定时间间隔接收到此用户身份的客户端发送的认证数据包,如果接收到,则保证网络端口P的权限持续向此用户身份的客户端开放,并执行步骤6;否则,则关闭网络端口P对此用户身份的客户端的访问权限,结束流程;

步骤6,所述第一网关接收来自于所述第一网络的此用户身份的客户端发送的通信数据包,并发送给所述前置交换服务平台;

步骤7,所述前置交换服务平台,依次对所述通信数据包进行身份认证、日志记录和内容过滤处理后,得到第一处理后的通信数据包;

步骤8,所述前置交换服务平台,将所述第一处理后的通信数据包,发送给所述通信隔离通道,经所述通信隔离通道进行传输,传输到所述后置交换服务平台;

步骤9,所述后置交换服务平台,依次对所述第一处理后的通信数据包进行身份认证和内容过滤处理后,得到第二处理后的通信数据包,并将所述第二处理后的通信数据包发送给所述第二网关;

步骤10,所述第二网关将接收到的所述第二处理后的通信数据包,发送给所述第二网络。

2.根据权利要求1所述的一种实现跨网交换的数据交换方法,其特征在于,所述通信隔离通道采用网闸实现双向数据隔离传输,或者,采用单向光闸实现单向数据隔离传输。

一种实现跨网交换的数据交换方法

技术领域

[0001] 本发明属于计算机科学技术领域，具体涉及一种实现跨网交换的数据交换方法。

背景技术

[0002] 计算机信息化和大数据技术的蓬勃发展，使得系统间数据的互通互联、数据共享变得尤为重要。此外，为防止核心数据泄露，互联网与局域网之间无法实现直接连通，如何实现一种安全的跨网交换方法也成为各公司需要考虑的问题。

[0003] 绝大多数公司对数据安全的要求比较高，所以不能将公司内部局域网与互联网进行直接互通。然而，公司系统常常具有在互联网和公司内部局域网进行数据通信的需求，进而实现运行期间业务数据的关联，以及数据的互相传递，因此，如何保证跨网交换时数据通信的安全性，是目前急需解决的事情。

发明内容

[0004] 针对现有技术存在的缺陷，本发明提供一种实现跨网交换的数据交换方法，可有效解决上述问题。

[0005] 本发明采用的技术方案如下：

[0006] 本发明提供一种实现跨网交换的数据交换方法，包括以下步骤：

[0007] 步骤1，构建网络架构；所述网络架构包括：第一网络、第一网关、前置交换服务平台、通信隔离通道、后置交换服务平台、第二网关和第二网络；

[0008] 所述第一网络，依次通过所述第一网关和所述前置交换服务平台，连接到所述通信隔离通道的一端；所述通信隔离通道的另一端，依次通过所述后置交换服务平台和所述第二网关，连接到所述第二网络，由此实现所述第一网络和所述第二网络的通信连接；

[0009] 步骤2，所述第一网关配置多个网络端口，在默认状态下，所有网络端口均为隐藏且关闭状态，对所述第一网络不可见；

[0010] 当第一网络需要向第二网络通信时，所述第一网络与所述第一网关协商，确定可向所述第一网络短时间开放的网络端口，表示为网络端口P；

[0011] 所述第一网关向所述第一网络开放网络端口P，其他网络端口保持关闭状态；

[0012] 步骤3，所述第一网络向所述第一网关发送带有用户身份和申请访问端口M的认证数据包；

[0013] 步骤4，所述第一网关在向第一网络开放网络端口P后，判断是否在设定时间内接收到所述第一网络发送的认证数据包，如果没有接收到，则关闭网络端口P，结束流程；如果接收到，则执行步骤5；

[0014] 步骤5，所述第一网关从所述认证数据包中解析出用户身份和申请访问端口M的请求，一方面，对所述用户身份进行验证，另一方面，验证申请访问端口M是否与网络端口P相同，如果相同，则表示端口权限验证通过；

[0015] 如果用户身份和端口权限中存在任意一项没有验证通过，则所述第一网关关闭网

络端口P,结束流程;

[0016] 如果用户身份和端口权限均验证通过后,所述第一网关增加防火墙规则,向此用户身份的客户端开放网络端口P;允许所述第一网络中的此用户身份的客户端访问所述第一网关的网络端口P;

[0017] 在所述第一网关向用户身份的客户端开放网络端口P后,所述第一网关持续监测是否每隔设定时间间隔接收到此用户身份的客户端发送的认证数据包,如果接收到,则保证网络端口P的权限持续向此用户身份的客户端开放,并执行步骤6;否则,则关闭网络端口P对此用户身份的客户端的访问权限,结束流程;

[0018] 步骤6,所述第一网关接收来自于所述第一网络的此用户身份的客户端发送的通信数据包,并发送给所述前置交换服务平台;

[0019] 步骤7,所述前置交换服务平台,依次对所述通信数据包进行身份认证、日志记录和内容过滤处理后,得到第一处理后的通信数据包;

[0020] 步骤8,所述前置交换服务平台,将所述第一处理后的通信数据包,发送给所述通信隔离通道,经所述通信隔离通道进行传输,传输到所述后置交换服务平台;

[0021] 步骤9,所述后置交换服务平台,依次对所述第一处理后的通信数据包进行身份认证和内容过滤处理后,得到第二处理后的通信数据包,并将所述第二处理后的通信数据包发送给所述第二网关;

[0022] 步骤10,所述第二网关将接收到的所述第二处理后的通信数据包,发送给所述第二网络。

[0023] 优选的,所述通信隔离通道采用网闸实现双向数据隔离传输,或者,采用单向光闸实现单向数据隔离传输。

[0024] 本发明提供的一种实现跨网交换的数据交换方法具有以下优点:

[0025] 本发明提供的一种实现跨网交换的数据交换方法,可有效提高跨网数据交换的安全性,满足跨网数据交换的通信需求。

附图说明

[0026] 图1为本发明提供的一种实现跨网交换的数据交换方法的流程示意图。

具体实施方式

[0027] 为了使本发明所解决的技术问题、技术方案及有益效果更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明。

[0028] 本发明提供一种实现跨网交换的数据交换方法,参考图1,包括以下步骤:

[0029] 步骤1,构建网络架构;所述网络架构包括:第一网络、第一网关、前置交换服务平台、通信隔离通道、后置交换服务平台、第二网关和第二网络;

[0030] 本发明中,第一网络,可以为局域网或互联网;第二网络可以为局域网或互联网。

[0031] 所述第一网络,依次通过所述第一网关和所述前置交换服务平台,连接到所述通信隔离通道的一端;所述通信隔离通道的另一端,依次通过所述后置交换服务平台和所述第二网关,连接到所述第二网络,由此实现所述第一网络和所述第二网络的通信连接;

[0032] 步骤2,所述第一网关配置多个网络端口,在默认状态下,所有网络端口均为隐藏且关闭状态,对所述第一网络不可见;

[0033] 当第一网络需要向第二网络通信时,所述第一网络与所述第一网关协商,确定可向所述第一网络短时间开放的网络端口,表示为网络端口P;

[0034] 所述第一网关向所述第一网络开放网络端口P,其他网络端口保持关闭状态;

[0035] 步骤3,所述第一网络向所述第一网关发送带有用户身份和申请访问端口M的认证数据包;

[0036] 步骤4,所述第一网关在向第一网络开放网络端口P后,判断是否在设定时间内接收到所述第一网络发送的认证数据包,如果没有接收到,则关闭网络端口P,结束流程;如果接收到,则执行步骤5;

[0037] 步骤5,所述第一网关从所述认证数据包中解析出用户身份和申请访问端口M的请求,一方面,对所述用户身份进行验证,另一方面,验证申请访问端口M是否与网络端口P相同,如果相同,则表示端口权限验证通过;

[0038] 如果用户身份和端口权限中存在任意一项没有验证通过,则所述第一网关关闭网络端口P,结束流程;

[0039] 如果用户身份和端口权限均验证通过后,所述第一网关增加防火墙规则,向此用户身份的客户端开放网络端口P;允许所述第一网络中的此用户身份的客户端访问所述第一网关的网络端口P;

[0040] 在所述第一网关向用户身份的客户端开放网络端口P后,所述第一网关持续监测是否每隔设定时间间隔接收到此用户身份的客户端发送的认证数据包,如果接收到,则保证网络端口P的权限持续向此用户身份的客户端开放,并执行步骤6;否则,则关闭网络端口P对此用户身份的客户端的访问权限,结束流程;

[0041] 步骤6,所述第一网关接收来自于所述第一网络的此用户身份的客户端发送的通信数据包,并发送给所述前置交换服务平台;

[0042] 步骤7,所述前置交换服务平台,依次对所述通信数据包进行身份认证、日志记录和内容过滤处理后,得到第一处理后的通信数据包;

[0043] 步骤8,所述前置交换服务平台,将所述第一处理后的通信数据包,发送给所述通信隔离通道,经所述通信隔离通道进行传输,传输到所述后置交换服务平台;

[0044] 步骤9,所述后置交换服务平台,依次对所述第一处理后的通信数据包进行身份认证和内容过滤处理后,得到第二处理后的通信数据包,并将所述第二处理后的通信数据包发送给所述第二网关;

[0045] 步骤10,所述第二网关将接收到的所述第二处理后的通信数据包,发送给所述第二网络。

[0046] 下面对本发明主要特点进行介绍:

[0047] 1)数据接入内容

[0048] 本发明,第一网络和第二网络之间通信的通信包内容,可以为数据库内容、文件、音视频流、消息等各类格式,实现多种数据格式通信。

[0049] 2)第一网关

[0050] 为保证跨网交换的安全性,第一网关采用端口隐藏、按需授权的方式把控请求,从

而减少攻击方向，极大程度降低安全风险，保护关键资产和基础架构，从而阻止潜在的基于网络的攻击。

[0051] 第一网关允许预先审查控制所有连接，例如，预先设置第一网络中可接入的设备范围、服务范围、设施范围等，因此，提高数据接入的安全性。

[0052] 与传统的TCP/IP网络默认允许连接相比，本发明第一网关的端口默认为关闭状态，在没有经过身份验证和授权之前，对于网络终端用户是完全不可见的，从缺省信任变成绝不信任。

[0053] 另外，区别于传统网络只验证一次的验证方式，通过在第一网关实施实时的动态可信授权验证，可以实现对于连接授权的始终验证。

[0054] 3)前置交换服务平台

[0055] 前置交换服务平台提供身份认证、格式检查、日志记录、内容过滤、流量监控功能。其中，身份认证、格式检查和内容过滤功能，是为保证数据通信的安全性，实现“来源可证、流向可控、行为可查、内容可判、终点可知”。

[0056] 身份认证：认证访问对象，确保访问对象的身份可信，通过技术手段固化主体责任；

[0057] 日志记录：详细记录数据通信过程中行为，用于审计；

[0058] 流量监控：进行业务级流量控制，针对每个业务可从频次、流量、时间、级别、线程维度进行流量控制，对超限业务进行熔断；

[0059] 内容过滤：对接入数据内容进行检查，包括数据完成性验证、数据格式验证、数据长度验证、数据敏感信息验证、非法数据验证，确保数据安全合法。

[0060] 4)通信隔离通道

[0061] 通信隔离通道通过网闸或者单向光闸实现，提供隔离传输能力。

[0062] 网闸技术是基于双向的，即通过配置，允许高安全网络和低安全网络之间双向数据交换。涉密网络与非涉密网络连接时，若非涉密网络与互联网物理隔离，则采用双向网闸隔离；若非涉密网络与互联网是逻辑隔离的，则采用单向网闸隔离，保证涉密数据不从高密级网络流向低密级网络。

[0063] 单向光闸集是一种基于光的单向性的单向隔离软硬件系统，用于对安全性要求极高的网络的数据交换场景，如涉密网络与非涉密网络之间，行业内网与公共网络之间。

[0064] 下面介绍一个具体实施例：

[0065] 步骤1：数据接入

[0066] 数据从第一网络传输方接入到第一网关中。支持多种格式数据，包括数据库、文件、音视频、消息。

[0067] 步骤2：网关安全认证

[0068] 构建第一网络的安全认证客户端，与第一网关的网关服务联合使用实现安全认证。

[0069] 当客户端进行请求时，第一网关开放一个同客户端协商好的端口，其他端口默认关闭，客户端发送包含用户身份和申请访问端口的认证数据包。第一网关收到认证数据包后，验证身份合法性和端口权限。验证通过则增加防火墙规则，允许此身份的IP访问开放端口。

[0070] 为保证安全性，本认证机制实现固定时长重新认证功能，如果用户超过规定时间未进行操作，端口权限会自动关闭，用户再次操作时，需重新进行认证。如果用户一直在操作，那么客户端会定期建立与网关的连接，继续认证，保证端口权限持续开放。

[0071] 步骤3：前置交换服务平台

[0072] (1)身份认证

[0073] 前置交换服务平台对接入的应用数据进行身份认证，通过IP/MAC认证、接口AK/SK认证、静态口令密码认证、证书认证，确保接入数据对象的身份安全。

[0074] (2)流量监控

[0075] 前置交换服务平台对流量进行控制，针对每个业务从频次、流量、时间、级别、线程多个维度进行流量监控，对于超过限制的业务进行熔断。

[0076] (3)内容过滤

[0077] 前置交换服务平台对接入数据内容进行检查，包括数据完成性验证、数据格式验证、数据长度验证、数据敏感信息验证、非法数据验证，确保数据安全合法。

[0078] (4)日志记录

[0079] 针对数据，前置交换服务平台记录数据的来源、流向、内容、操作进行记录，用于审计；

[0080] 步骤4：通信隔离通道

[0081] 通过网闸或者单向光闸提供数据隔离传输能力，实现数据从第一网络到第二网络的数据传输。

[0082] 步骤5：经通信隔离通道、后置交换服务平台和第二网关后，到达第二网络。

[0083] 本发明提供的实现跨网交换的数据交换方法，可适用以下场景：

[0084] 通过全量或增量的方式进行主流关系型数据库(第一网络中的数据库)以及非关系型数据库(第二网络中的数据库)之间的数据同步。

[0085] 通过设置同步定时任务，将第一网络中的全量数据周期性的从原始库拷贝到第二网络的目标库中。

[0086] 增量数据同步通过触发器、时间、快照、标记方式对增量数据进行同步。

[0087] (1)通过FTP、SFTP、NFS、CIFS、SMB协议进行源端与目标端的文件交换。支持增量文件同步和以目录为单位的全量文件同步。

[0088] (2)支持各类消息系统的读写，通过订阅的方式获取主体消息信息，实现消息交换。

[0089] 本发明提供的一种实现跨网交换的数据交换方法具有以下优点：

[0090] 本发明提供的一种实现跨网交换的数据交换方法，可有效提高跨网数据交换的安全性，满足跨网数据交换的通信需求。

[0091] 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，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视本发明的保护范围。

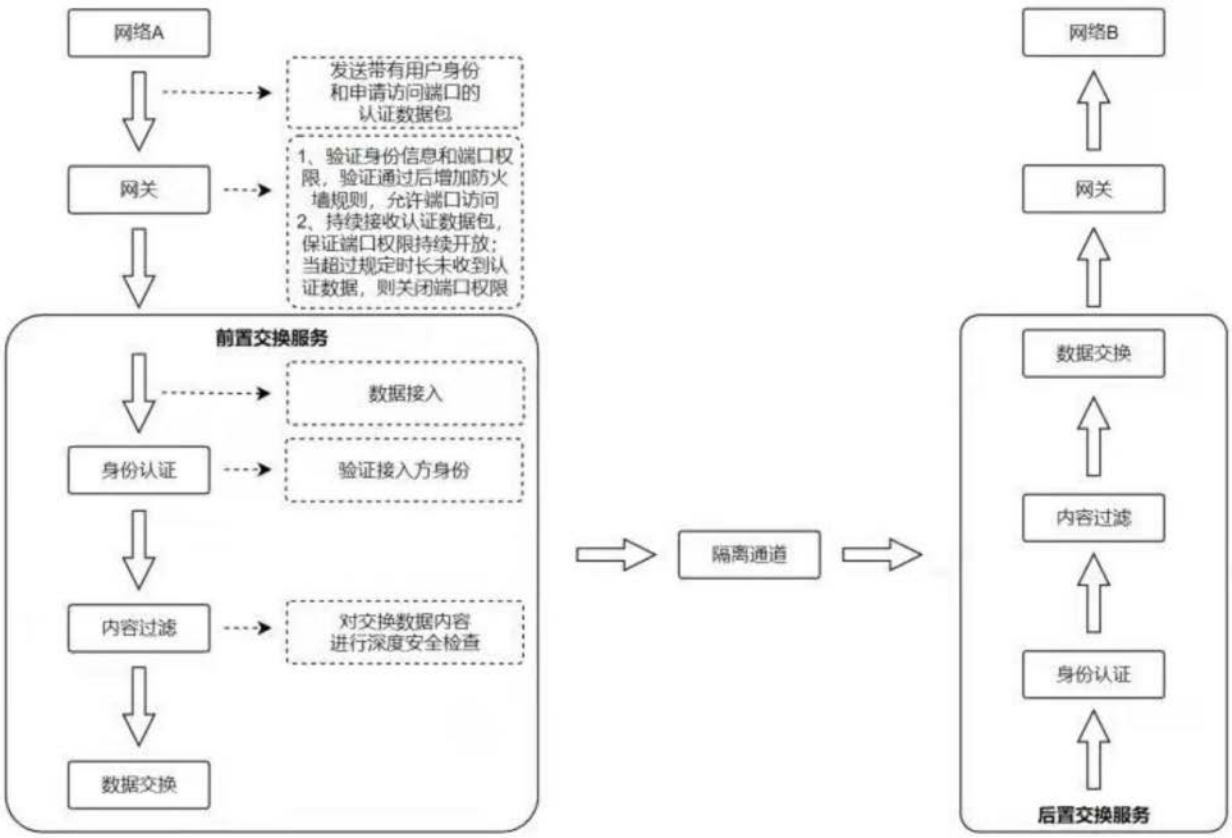

网络A
发送带有用户身份和申请访问端口的认证数据包
网关
1、验证身份信息和端口权限，验证通过后增加防火墙规则，允许端口访问
2、持续接收认证数据包，保证端口权限持续开放；当超过规定时长未收到认证数据，则关闭端口权限
前置交换服务
数据接入
身份认证
验证接入方身份
内容过滤
对交换数据内容进行深度安全检查
数据交换
隔离通道
网络B
网关
数据交换
内容过滤
身份认证
后置交换服务

图1