(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 114070585 A
(43)申请公布日 2022.02.18

(21)申请号 202111209232.4

(22)申请日 2021.10.18

(71)申请人 北京天融信网络安全技术有限公司
地址 100085 北京市海淀区上地东路1号院3号楼四层
申请人 北京天融信科技有限公司
北京天融信软件有限公司

(72)发明人 王耀杰

(74)专利代理机构 工业和信息化部电子专利中心 11010
代理人 焉明涛

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 12/66(2006.01)

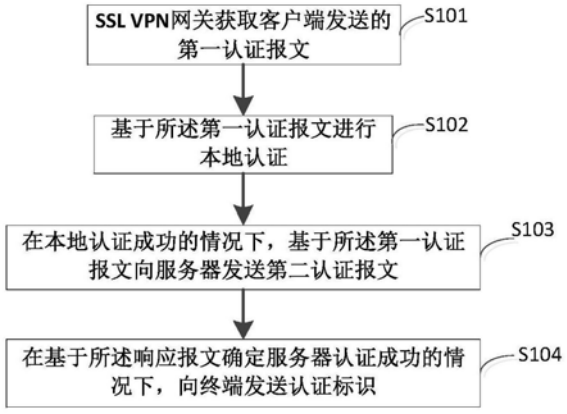
权利要求书1页 说明书5页 附图1页

(54)发明名称

一种SSL VPN认证方法、装置及网关

(57)摘要

本公开提出了一种SSL VPN认证方法、装置及网关，其中SSL VPN认证方法，包括：获取客户端发送的第一认证报文；基于所述第一认证报文进行本地认证；在本地认证成功的情况下，基于所述第一认证报文向服务器发送第二认证报文，所述第二认证报文可直接被服务器解析；接收服务器发送的响应报文，在基于所述响应报文确定服务器认证成功的情况下，向客户端发送认证标识，以供客户端基于所述认证标识实现业务数据传输。本实施例基于一套认证报文即可完成本地认证和服务器认证，实现了用户无需额外购买AAA服务器，有效减少用户投入成本。



CN 114070585 A

1.一种SSL VPN认证方法,其特征在于,包括:

获取客户端发送的第一认证报文;

基于所述第一认证报文进行本地认证;

在本地认证成功的情况下,基于所述第一认证报文向服务器发送第二认证报文,所述第二认证报文可直接被所述服务器解析;

接收所述服务器发送的响应报文,在基于所述响应报文确定服务器认证成功的情况下,向客户端发送认证标识,以供客户端基于所述认证标识实现业务数据传输。

2.如权利要求1所述的SSL VPN认证方法,其特征在于,基于所述第一认证报文进行本地认证之前,所述SSL VPN认证方法还包括:

获取用户成功登陆服务器的数据,并解析出目标报文格式和登陆成功的标识信息;

基于所述目标报文格式和登陆成功的标识信息配置服务器。

3.如权利要求2所述的SSL VPN认证方法,其特征在于,所述第二认证报文是按照所述目标报文格式拼接所述第一认证报文中的目标参数获得的。

4.如权利要求2所述的SSL VPN认证方法,其特征在于,基于所述响应报文确定服务器认证成功包括:

在从所述响应报文中解析获得预先配置的对应的登陆成功的标识信息的情况下,确定服务器认证成功。

5.如权利要求1所述的SSL VPN认证方法,其特征在于,在本地维护有用户认证信息,且本地维护的用户认证信息与服务器维护的用户认证信息相对应。

6.如权利要求1所述的SSL VPN认证方法,其特征在于,在本地认证失败的情况下,结束认证流程。

7.如权利要求1所述的SSL VPN认证方法,其特征在于,基于所述第一认证报文进行本地认证的方式包括:口令认证,和/或,证书认证。

8.一种SSL VPN认证装置,其特征在于,包括:

接口,被配置为获取客户端发送的第一认证报文;

处理器,被配置为:

基于所述第一认证报文进行本地认证;

在本地认证成功的情况下,基于所述第一认证报文向服务器发送第二认证报文,所述第二认证报文可直接被服务器解析;

接收服务器发送的响应报文,在基于所述响应报文确定服务器认证成功的情况下,向客户端发送认证标识,以供客户端基于所述认证标识实现业务数据传输。

9.一种SSL VPN网关,其特征在于,所述SSL VPN网关包括处理器和存储器,所述存储器上存储有计算机程序,所述计算机程序被处理器执行时实现如权利要求1至7中任一项所述的SSL VPN认证方法的步骤。

一种SSL VPN认证方法、装置及网关

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种SSL VPN认证方法、装置及网关。

背景技术

[0002] 虚拟专用网络(Virtual Private Network)：通过公用网络建立一个临时的、安全的链接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网络是对企业内部局域网的扩展。虚拟专用网络可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部局域网建立可信的安全连接，并保证数据的安全传输。虚拟专用网络可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全外联网虚拟专用网。

[0003] 虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部局域网建立可信的安全连接，并保证数据的安全传输。通过将数据流转移到低成本的网络上，一个企业的虚拟专用网解决方案将大幅度地减少用户花费在城域网和远程网络连接上的费用。同时这也将简化网络的设计和管理。

[0004] SSL VPN提供安全、可代理连接，只有经过认证的用户才能对资源进行访问。SSL VPN能对加密隧道进行细分，从而使得客户端用户能够同时接入Internet和访问内部企业网资源，也就是说它具备可控功能。另外，SSL VPN还能细化接入控制功能，易于将不同访问权限赋予不同用户。

[0005] 现有的认证方法用户需要另外购买短信授权或者采购AAA服务器。同时现有的方案设备间交互频繁，认证流程复杂。

发明内容

[0006] 本发明实施例提供一种SSL VPN认证方法、装置及网关，实现无需额外购买AAA服务器，同时提高认证效率。

[0007] 本公开提出一种SSL VPN认证方法，包括：

[0008] 获取客户端发送的第一认证报文；

[0009] 基于所述第一认证报文进行本地认证；

[0010] 在本地认证成功的情况下，基于所述第一认证报文向服务器发送第二认证报文，所述第二认证报文可直接被服务器解析；

[0011] 接收服务器发送的响应报文，在基于所述响应报文确定服务器认证成功的情况下，向客户端发送认证标识，以供客户端基于所述认证标识实现业务数据传输。

[0012] 在一些实施例中，基于所述第一认证报文进行本地认证之前，所述SSL VPN认证方法还包括：

[0013] 获取用户成功登陆服务器的数据，并解析出目标报文格式和登陆成功的标识信息；

[0014] 基于所述目标报文格式和登陆成功的标识信息配置服务器。

[0015] 在一些实施例中，所述第二认证报文是按照所述目标报文格式拼接所述第一认证报文中的目标参数获得的。

[0016] 在一些实施例中，基于所述响应报文确定服务器认证成功包括：

[0017] 在从所述响应报文中解析获得预先配置的对应的登陆成功的标识信息的情况下，确定服务器认证成功。

[0018] 在一些实施例中，在本地维护有用户认证信息，且本地维护的用户认证信息与服务器维护的用户认证信息相对应。

[0019] 在一些实施例中，在本地认证失败的情况下，结束认证流程。

[0020] 在一些实施例中，基于所述第一认证报文进行本地认证的方式包括：口令认证，和/或，证书认证。

[0021] 本公开还提出一种SSL VPN认证装置，包括：

[0022] 接口，被配置为获取客户端发送的第一认证报文；

[0023] 处理器，被配置为：

[0024] 基于所述第一认证报文进行本地认证；

[0025] 在本地认证成功的情况下，基于所述第一认证报文向服务器发送第二认证报文，所述第二认证报文可直接被服务器解析；

[0026] 接收服务器发送的响应报文，在基于所述响应报文确定服务器认证成功的情况下，向客户端发送认证标识，以供客户端基于所述认证标识实现业务数据传输。

[0027] 本公开还提出一种SSL VPN网关，所述SSL VPN网关包括处理器和存储器，所述存储器上存储有计算机程序，所述计算机程序被处理器执行时实现本公开各实施例所述的SSL VPN认证方法的步骤。

[0028] 本发明实施例基于一套认证报文即可完成本地认证和服务器认证从而实现了用户无需额外购买AAA服务器，有效减少用户投入成本。

[0029] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0030] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0031] 图1为本公开的SSL VPN认证方法的基本流程图；

[0032] 图2为本公开的SSL VPN认证方法总流程图。

具体实施方式

[0033] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0034] 本公开提出一种SSL VPN认证方法，如图1所示，本公开的SSL VPN认证方法应用于SSL VPN网关一侧，包括如下步骤：

[0035] 在步骤S101中SSL VPN网关获取客户端发送的第一认证报文。本示例中客户端可以是诸如PC，智能设备等，用户可以使用浏览器登录SSL VPN网关，SSL VPN网关可以获取的第一认证报文例如可以是该用户的登录口令，证书等，在此不做一一限定。

[0036] 在步骤S102中基于所述第一认证报文进行本地认证。也即可以通过SSL VPN网关对用户的登录行为进行认证，用户的登录行为可以是例如用户输入的用户名、密码等信息，基于第一认证报在SSL VPN网关本地完成，在一些实施例中，基于所述第一认证报文进行本地认证的方式包括：口令认证，和/或，证书认证或者多种认证方式的结合，具体可以根据实际需要设定，在本地认证失败的情况下，判定本次认证请求失败，结束认证流程。

[0037] 在步骤S103中在本地认证成功的情况下，基于所述第一认证报文向服务器发送第二认证报文，所述第二认证报文可直接被服务器解析。本实例中在SSL VPN网关认证用户的登录行为成功之后，可以基于第一认证报文的参数拼接成服务器可以直接解析格式的第二认证报文，并将第二认证报文发送给服务器。服务器在接收到第二认证报文之后，基于认证结果向SSL VPN网关发送响应报文。

[0038] 在步骤S104中接收服务器发送的响应报文，在基于所述响应报文确定服务器认证成功的情况下，向客户端发送认证标识，以供客户端基于所述认证标识实现业务数据传输。例如响应报文中可以包含有服务器的认证结果，例如可以设置标识认证的字段成功则为1，失败则为0，或者配置一个标识信息，在响应报文中包含相应的标识信息则说明认证成功，否则确定服务器认证失败。认证失败则结束认证流程。

[0039] 通过这样的方式，本公开的方法能够基于一套认证报文即可完成本地认证和服务器认证从而实现了用户无需额外购买AAA服务器，有效减少用户投入成本。

[0040] 在一些实施例中，基于所述第一认证报文进行本地认证之前，所述SSL VPN认证方法还包括：

[0041] 获取用户成功登陆服务器的数据，并解析出目标报文格式和登陆成功的标识信息。例如可以使用抓包工具抓取成功登录服务器的交互数据包，并解析出请求报文格式(目标报文格式)并选取登陆成功的标识信息；

[0042] 基于所述目标报文格式和登陆成功的标识信息配置服务器。具体SSL VPN网关上可以配置服务器的IP地址，及服务器的请求报文拼接时所需要的一些参数等，并配置成功标识信息。在一些实施例中，SSL VPN网关在本地维护有用户认证信息，且本地维护的用户认证信息与服务器维护的用户认证信息相对应。也即SSL VPN网关上维护一套用户信息，该套用户信息所对应用户名口令与服务器所使用的用户名口令一致，从而SSL VPN网关、服务器能够统一使用一套用户信息，大大降低运维成本，易于管理、部署和维护。并且使用一套用户信息可以极大简化交互流程，降低开发和部署难度。

[0043] 在一些实施例中，基于所述响应报文确定服务器认证成功包括：在从所述响应报文中解析获得预先配置的对应的登陆成功的标识信息的情况下，确定服务器认证成功。基于所述目标报文格式和登陆成功的标识信息配置服务器，也即在配置完成后服务器可以解析目标报文格式的数据，并且服务器可以基于第二认证报文识别成功后，在响应消息中返回预先配置的成功标识信息即可。SSL VPN网关解析响应消息若响应消息中包含成功标识

信息则可以确定服务器认证成功。

[0044] 在一些实施例中,所述第二认证报文是按照所述目标报文格式拼接所述第一认证报文中的目标参数获得的。基于前述实施方式,基于所述目标报文格式和登陆成功的标识信息配置服务器,也即在配置完成后服务器可以解析目标报文格式的数据,由此SSL VPN网关在本地认证成功之后,可以将第一认证报文按照目标报文格式拼接从而得到第二认证报文,也可以拼接指定的部分参数,具体在此不做限定。

[0045] 与现有技术相比,本公开的方法用户不需要另外购买短信授权或者采购AAA服务器,即可实现SSL VPN的多因子认证,减少了用户投入成本。本公开所涉及到的主要组件(SSL VPN网关和服务器)共用一套用户信息即可,大大降低了运维成本,易于管理、部署和维护。本公开的方法交互流程简单,开发和部署难度小。

[0046] 本公开还提出一种SSL VPN认证方法的实施案例,如图2所示,本示例中以服务器为WEB服务器为例进行举例说明,包括如下步骤:

[0047] 使用抓包工具抓取成功登录WEB服务器的交互数据包,解析出请求报文格式并选取成功标识信息;

[0048] SSL VPN网关上配置WEB服务器IP地址,及请求报文拼接时所需要的一些参数等,并配置成功标识信息。

[0049] 在SSL VPN网关上维护同一套用户信息,该套用户信息所对应用户名口令与WEB服务器所使用的用户名口令一致。

[0050] 用户使用浏览器/终端上的客户端登录SSL VPN网关,SSL VPN网关先依据登录的请求信息进行本地认证(包括但不限于口令、证书认证),若认证失败则判定本次认证请求失败。

[0051] 若本地认证成功,将按照指定格式拼接好的认证请求报文发送至WEB服务器,等待并接收WEB服务器的响应报文。

[0052] 接收并解析WEB服务器发送来的响应报文,若从响应报文中解析出SSL VPN网关上预先配置的成功标识信息,则判定认证成功并生成session id(认证标识),下发给浏览器/终端的客户端;浏览器/终端使用收到的session id请求建立SSL隧道,即可建立数据传输隧道,并进行资源下发等操作,从而实现业务数据的安全传输。

[0053] 本公开的方法用户不需要另外购买短信授权或者采购AAA服务器,只需要用户内网环境一台正常可用的WEB服务器(包括但不限于OA、邮箱系统),即可实现一种SSL VPN多因子认证,减少了用户投入成本。

[0054] 本公开还提出一种SSL VPN认证装置,包括:

[0055] 接口,被配置为获取客户端发送的第一认证报文;

[0056] 处理器,被配置为:

[0057] 基于所述第一认证报文进行本地认证;

[0058] 在本地认证成功的情况下,基于所述第一认证报文向服务器发送第二认证报文,所述第二认证报文可直接被服务器解析;

[0059] 接收服务器发送的响应报文,在基于所述响应报文确定服务器认证成功的情况下,向客户端发送认证标识,以供客户端基于所述认证标识实现业务数据传输。

[0060] 本公开还提出一种SSL VPN网关,所述SSL VPN网关包括处理器和存储器,所述存

储器上存储有计算机程序，所述计算机程序被处理器执行时实现本公开各实施例所述的SSL VPN认证方法的步骤。

[0061] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0062] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0063] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0064] 上面结合附图对本发明的实施例进行了描述，但是本发明并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本发明的启示下，在不脱离本发明宗旨和权利要求所保护的范围情况下，还可做出很多形式，这些均属于本发明的保护之内。

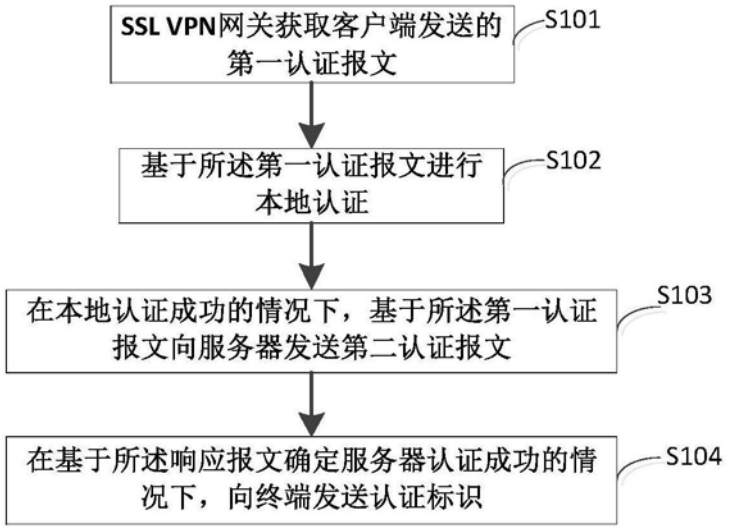

SSL VPN网关获取客户端发送的第一认证报文
S101
基于所述第一认证报文进行本地认证
S102
在本地认证成功的情况下，基于所述第一认证报文向服务器发送第二认证报文
S103
在基于所述响应报文确定服务器认证成功的情况下，向终端发送认证标识
S104

图1

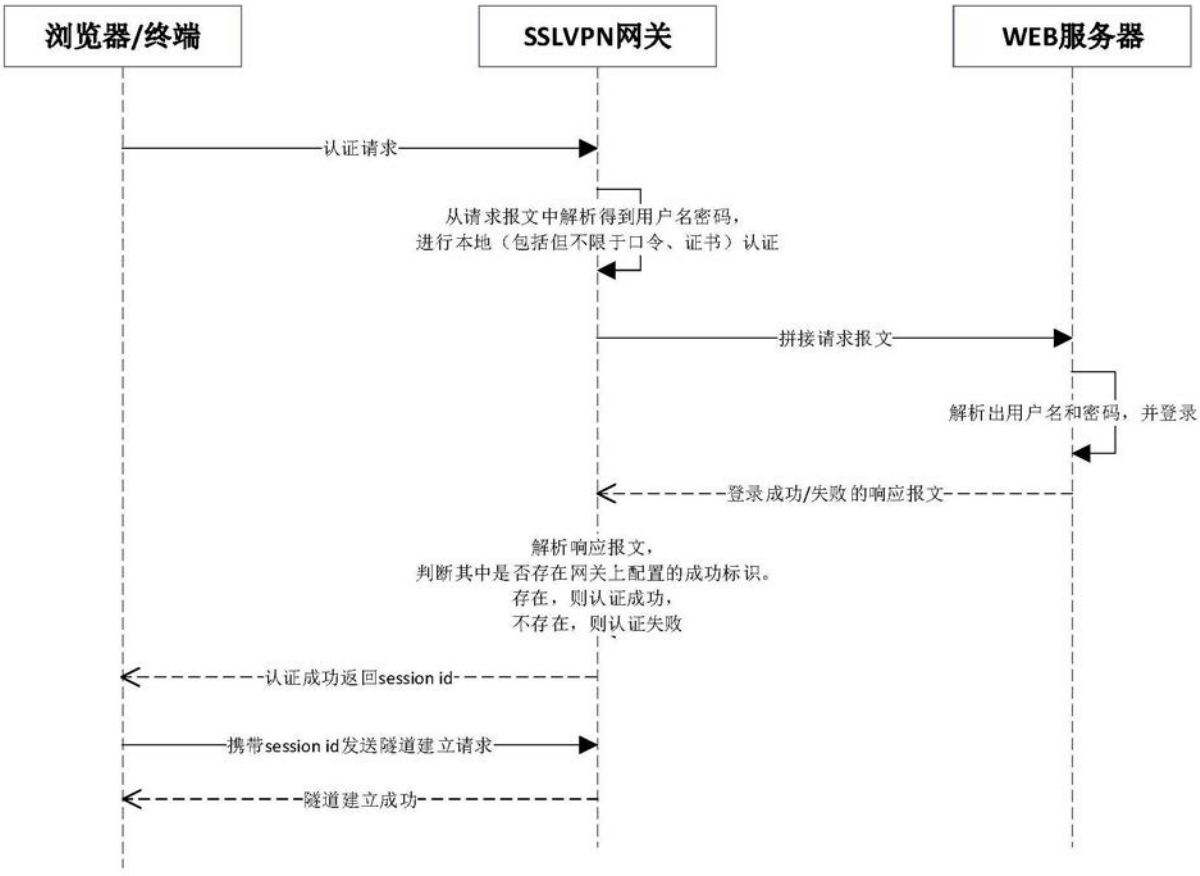

浏览器/终端
SSLVPN网关
WEB服务器
认证请求
从请求报文中解析得到用户名密码，
进行本地（包括但不限于口令、证书）认证
拼接请求报文
解析出用户名和密码，并登录
登录成功/失败的响应报文
解析响应报文，
判断其中是否存在网关上配置的成功标识。
存在，则认证成功，
不存在，则认证失败
认证成功返回session id
携带session id发送隧道建立请求
隧道建立成功

图2