(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 113179271 A
(43)申请公布日 2021.07.27

(21)申请号 202110465091.6

(22)申请日 2021.04.28

(71)申请人 深圳前海微众银行股份有限公司
地址 518027 广东省深圳市前海深港合作区前湾一路1号A栋201室

(72)发明人 刘俊豪 杨伟峰 史振辉

(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 邹雅莹

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)
H04L 9/32(2006.01)

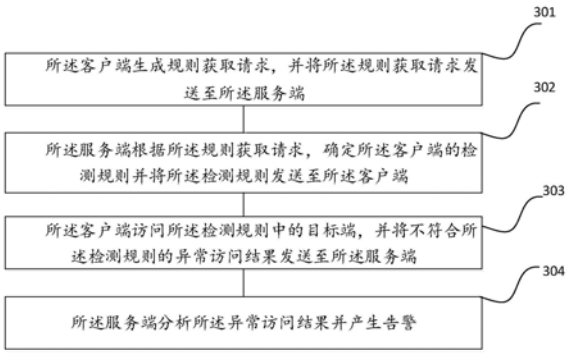
权利要求书3页 说明书12页 附图5页

(54)发明名称

一种内网安全策略检测方法及装置

(57)摘要

本发明实施例提供一种内网安全策略检测方法及装置，内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述方法包括：所述客户端生成规则获取请求，并将所述规则获取请求发送至所述服务端；所述服务端根据所述规则获取请求，确定所述客户端的检测规则并将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；所述客户端访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；所述服务端分析所述异常访问结果并产生告警。上述方法可以提高网络安全策略检测效率，自动更新检测规则。



CN 113179271 A

1.一种内网安全策略检测方法,其特征在于,内网安全策略检测系统中包含至少一个客户端和服务端,所述至少一个客户端分别属于内网中的至少一个网络区域,所述方法包括:

所述客户端生成规则获取请求,并将所述规则获取请求发送至所述服务端;

所述服务端根据所述规则获取请求,确定所述客户端的检测规则并将所述检测规则发送至所述客户端,所述检测规则用于指示客户端与目标端之间的访问权限;

所述客户端访问所述检测规则中的目标端,并将不符合所述检测规则的异常访问结果发送至所述服务端;

所述服务端分析所述异常访问结果并产生告警。

2.如权利要求1中所述的方法,其特征在于,所述服务端分析所述异常访问结果并产生告警,包括:

所述服务端确定所述异常访问结果是否符合白名单中的网络安全策略;

若不符合,则根据所述异常访问结果生成告警。

3.如权利要求2中所述的方法,其特征在于,所述服务端确定所述异常访问结果是否符合白名单中的网络安全策略,包括:

所述服务端确定所述异常访问结果中的源IP地址、目标IP地址和目标端口是否属于所述网络安全策略中的预设源IP地址、预设目标IP地址和预设目标端口;

若存在至少一项不符合,则确定所述异常访问结果不符合所述网络安全策略。

4.如权利要求1中所述的方法,其特征在于,所述规则获取请求包括所述客户端的IP地址及所述客户端生成的第一签名;

所述服务端根据所述规则获取请求,确定所述客户端的检测规则,包括:

所述服务端对所述规则获取请求中的第一签名进行验证,验证通过后根据所述客户端的IP地址确定所述客户端的检测规则。

5.如权利要求4中所述的方法,其特征在于,所述规则获取请求中还包括时间戳;

所述第一签名通过如下方式生成:

所述客户端将所述客户端的IP地址、所述时间戳和所述客户端的授权信息拼接得到有序拼接数据;

所述客户端通过预设的加密算法对所述有序拼接数据加密得到所述第一签名;

所述服务端对所述规则获取请求中的第一签名进行验证,包括:

所述服务端按照所述预设的加密算法,对所述规则获取请求中的所述客户端的IP地址、所述时间戳和服务端的授权信息进行加密,得到第二签名;所述客户端的授权信息与所述服务端的授权信息相同;

若所述服务端确定所述第一签名与所述第二签名相同,则通过验证,确定所述客户端为合法的。

6.如权利要求1-5中任一所述的方法,其特征在于,还包括:

所述服务端接收检测规则更新指令,根据所述检测规则更新指令分别对所述检测规则和/或所述网络安全策略进行更新。

7.一种内网安全策略检测方法,其特征在于,内网安全策略检测系统中包含至少一个客户端和服务端,所述至少一个客户端分别属于内网中的至少一个网络区域,所述方法包

括：

所述客户端生成规则获取请求，并将所述规则获取请求发送至所述服务端；

所述客户端接收所述服务端根据所述规则获取请求确定出的检测规则；所述检测规则用于指示客户端与目标端之间的访问权限；

所述客户端访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；所述异常访问结果用于所述服务端进行分析后产生告警。

8.一种内网安全策略检测方法，其特征在于，内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述方法包括：

所述服务端接收所述客户端发送的规则获取请求，并根据所述规则获取请求，确定所述客户端的检测规则；

所述服务端将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；

所述服务端接收所述客户端发送的异常访问结果，所述异常访问结果为所述客户端根据不符合所述检测规则的目标端确定的；

所述服务端分析所述异常访问结果并产生告警。

9.一种内网安全策略检测装置，其特征在于，内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述装置包括：

收发模块，用于生成规则获取请求，并将所述规则获取请求发送至所述服务端；

所述收发模块还用于，根据所述规则获取请求，确定所述客户端的检测规则并将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；

检测模块，用于访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；

告警模块，用于分析所述异常访问结果并产生告警。

10.一种内网安全策略检测装置，其特征在于，内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述装置包括：

收发模块，用于生成规则获取请求，并将所述规则获取请求发送至所述服务端；

所述收发模块还用于，接收所述服务端根据所述规则获取请求确定出的检测规则；所述检测规则用于指示客户端与目标端之间的访问权限；

检测模块，用于访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；所述异常访问结果用于所述服务端进行分析后产生告警。

11.一种内网安全策略检测装置，其特征在于，内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述装置包括：

收发模块，用于接收所述客户端发送的规则获取请求，并根据所述规则获取请求，确定所述客户端的检测规则；

所述收发模块还用于，将所述检测规则发送至所述客户端，所述检测规则用于指示客

户端与目标端之间的访问权限;接收所述客户端发送的异常访问结果,所述异常访问结果为所述客户端根据不符合所述检测规则的目标端确定的;

告警模块,用于分析所述异常访问结果并产生告警。

12.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有程序,当所述程序在计算机上运行时,使得计算机实现执行权利要求1至8中任一项所述的方法。

13.一种计算机设备,其特征在于,包括:

存储器,用于存储计算机程序;

处理器,用于调用所述存储器中存储的计算机程序,按照获得的程序执行如权利要求1至8任一权利要求所述的方法。

一种内网安全策略检测方法及装置

技术领域

[0001] 本申请涉及金融科技(Fintech)的网络技术领域,尤其涉及一种内网安全策略检测方法及装置。

背景技术

[0002] 近年来,随着计算机技术的发展,越来越多的技术应用在金融领域,传统金融业正在逐步向金融科技(Fintech)转变,但由于金融行业的安全性、实时性要求,也对技术提出更高的要求。其中,由于计算机发展过程中呈现的网络的连接方式的多样性、终端分布广、网络的开放和互联等特征,致使网络易遭受恶意攻击,而金融行业对安全性有着极高的要求,所以网络的安全是一个至关重要的问题。因此,网络安全策略作为网络层的基础安全防护手段,对网络中的信息起着保护作用。

[0003] 在企业的信息化建设过程中,信息安全问题逐步凸显,通过划分不同的网络区域进行隔离保护,在不同的网络区域之间甚至同个网络区域的不同端口之间需要进行网络访问控制,这导致网络安全策略数量越来越多且难以有效整理,这可能造成防火墙或其他网络安全设备出现性能瓶颈,从上层应用的角度,也难以清晰地描绘出不同业务应用之间的调用关系,难以在出现问题时从网络调用关系上迅速地进行问题定位。

[0004] 为了解决上述问题,现有技术中,通过在客户端中设置端口扫描器和对应的检测规则,以获取该客户端端口与其他端口的连接信息,根据该连接信息分析网络安全策略是否有效。但该方法各端口扫描器之间不能互相联动,因此需要人工获取各端口扫描器中的连接信息并分析,且一旦检测规则发生变更,则需要到各客户端的端口扫描器中重新部署。因此,导致该安全策略检测效率低,检测规则变更难度大。

[0005] 因此,现在亟需一种内网安全策略检测方法及装置,用于提高网络安全策略检测效率,自动更新检测规则。

发明内容

[0006] 本发明实施例提供一种内网安全策略检测方法及装置,用于提高网络安全策略检测效率,自动更新检测规则。

[0007] 第一方面,本发明实施例提供一种内网安全策略检测方法,该方法包括:

[0008] 内网安全策略检测系统中包含至少一个客户端和服务端,所述至少一个客户端分别属于内网中的至少一个网络区域,所述方法包括:所述客户端生成规则获取请求,并将所述规则获取请求发送至所述服务端;所述服务端根据所述规则获取请求,确定所述客户端的检测规则并将所述检测规则发送至所述客户端,所述检测规则用于指示客户端与目标端之间的访问权限;所述客户端访问所述检测规则中的目标端,并将不符合所述检测规则的异常访问结果发送至所述服务端;所述服务端分析所述异常访问结果并产生告警。

[0009] 上述方法中,一般来说,同一个网络区域中的网络安全策略相同,因此,可以针对一个网络区域选定一个客户端(若是网络资源允许,也可以选定多个客户端,这里只是一种

最优实现方法)，作为用于检测网络安全策略的客户端；多个网络区域对应多个客户端，这多个客户端可以与服务端通信。如此，客户端通过规则获取请求，可以从服务端获取检测规则，实现自动更新检测规则，降低检测规则变更难度。客户端还可以将检测得到的异常访问结果发送至服务端，使得服务端可以对各客户端上报的异常访问结果进行分析，确定对应网络区域的网络安全策略是否有效。

[0010] 可选的，所述服务端分析所述异常访问结果并产生告警，包括：所述服务端确定所述异常访问结果是否符合白名单中的网络安全策略；若不符合，则根据所述异常访问结果生成告警。

[0011] 上述方法中，白名单是指：一个网络区域内各客户端的检测规则相同，但是该网络区域中有一个例外的客户端，该客户端有一部分检测规则和该网络区域中其它客户端不太一样。例如，该网络区域中的各客户端均不允许其它网络区域的客户端访问端口8080，但是这个例外的客户端允许其它网络区域的客户端访问端口8080。但又不至于在一个网络区域中设置两个客户端获取不同的检测规则，浪费资源，所以设置这个例外的客户端的检测规则在白名单里，若是其它网络区域的客户端连通到例外的客户端的8080端口，是正常的，则将这个异常访问结果的记录删除，不用产生告警。如此，既节约网络资源，又可以提高网络安全策略的针对性。服务端接收客户端上报的异常访问结果进行分析并告警，相比于现有技术中使用端口扫描器等开源工具(如，nmap(Network Mapper，网络安全审计工具)等)检测网络安全策略，需要人工参与将不同网络区域之间的异常访问结果整合分析来说，本申请可以通过服务端接收的各客户端的异常访问结果进行分析告警，提高检测效率。

[0012] 可选的，所述服务端确定所述异常访问结果是否符合白名单中的网络安全策略，包括：所述服务端确定所述异常访问结果中的源IP地址、目标IP地址和目标端口是否属于所述网络安全策略中的预设源IP地址、预设目标IP地址和预设目标端口；若存在至少一项不符合，则确定所述异常访问结果不符合所述网络安全策略。

[0013] 上述方法中，根据异常访问结果中的源IP地址、目标IP地址和目标端口可以确定客户端的访问信息，网络安全策略中的预设源IP地址、预设目标IP地址和预设目标端口为检测规则中的规则信息。如此，若客户端的实际访问信息与规则信息不同，则网络安全策略大概率产生纰漏，因此后续由服务端产生告警，可以使得相关开发人员可以得知网络安全策略异常，并可以根据访问信息快速定位异常及其根因。

[0014] 可选的，所述规则获取请求包括所述客户端的IP地址及所述客户端生成的第一签名；所述服务端根据所述规则获取请求，确定所述客户端的检测规则，包括：所述服务端对所述规则获取请求中的第一签名进行验证，验证通过后根据所述客户端的IP地址确定所述客户端的检测规则。

[0015] 上述方法中，服务单对规则获取请求中的第一签名进行验证。提高检测的安全性，防止非法人员获取检测规则，根据检测规则对网络区域攻击。

[0016] 可选的，所述规则获取请求中还包括时间戳；所述第一签名通过如下方式生成：所述客户端将所述客户端的IP地址、所述时间戳和所述客户端的授权信息拼接得到有序拼接数据；所述客户端通过预设的加密算法对所述有序拼接数据加密得到所述第一签名；所述服务端对所述规则获取请求中的第一签名进行验证，包括：所述服务端按照所述预设的加密算法，对所述规则获取请求中的所述客户端的IP地址、所述时间戳和服务端的授权信息

进行加密，得到第二签名；所述客户端的授权信息与所述服务端的授权信息相同；若所述服务端确定所述第一签名与所述第二签名相同，则通过验证，确定所述客户端为合法的。

[0017] 上述方法中，将客户端的授权信息设置为与服务端的授权信息相同的授权信息，保证后续生成的用于验证的第一签名相同，使得服务端和客户端拥有通信‘许可’，使得服务端可以根据与客户端相同的授权信息对客户端进行验证，若授权信息相同，则得到的第一签名和第二签名相同，则可以认定该客户端合法，可以为该客户端提供检测规则。提高服务端与客户端交互的安全性。

[0018] 可选的，还包括：所述服务端接收检测规则更新指令，根据所述检测规则更新指令分别对所述检测规则和/或所述网络安全策略进行更新。

[0019] 上述方法中，服务器可以通过检测规则更新指令更新检测规则，进一步使得客户端获取最新的检测规则。相比于现有技术中将检测规则分别部署在端口扫描器等开源工具(如，nmap(Network Mapper，网络安全审计工具)等)等开源工具上来说，本申请可以只在服务端部署检测规则以及更新检测规则，就可以使得客户端主动下载最新检测规则，既降低了检测规则更新的复杂度，又提高了检测规则更新的及时性，进一步提高了网络安全策略检测的准确性。

[0020] 第二方面，本发明实施例提供一种内网安全策略检测方法，该方法包括：

[0021] 内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述方法包括：所述客户端生成规则获取请求，并将所述规则获取请求发送至所述服务端；所述客户端接收所述服务端根据所述规则获取请求确定出的检测规则；所述检测规则用于指示客户端与目标端之间的访问权限；所述客户端访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；所述异常访问结果用于所述服务端进行分析后产生告警。

[0022] 上述方法中，客户端可以生成规则获取请求，主动从服务端获取该客户端的检测规则，客户端可以根据获取的检测规则进行网络安全策略检测。如此，实现客户端检测规则的自动更新，相比于现有技术中客户端需要人工更新检测规则来说，本申请能够提高检测规则更新的及时性，降低更新检测规则的成本。其中，检测规则中包含用于指示客户端与目标端之间的访问权限。如此，当客户端访问检测规则中的目标端时，可以获取该过程中的访问信息，以确定该检测信息中客户端与目标端之间的访问，是否符合检测规则中的客户端与目标端之间的访问权限。

[0023] 第三方面，本发明实施例提供一种内网安全策略检测方法，该方法包括：

[0024] 内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述方法包括：所述服务端接收所述客户端发送的规则获取请求，并根据所述规则获取请求，确定所述客户端的检测规则；所述服务端将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；所述服务端接收所述客户端发送的异常访问结果，所述异常访问结果为所述客户端根据不符合所述检测规则的目标端确定的；所述服务端分析所述异常访问结果并产生告警。

[0025] 上述方法中，服务端可以根据客户端发送的规则获取请求向客户端发送对应的检测规则，实现检测规则自动更新，提高检测规则更新效率。且服务器可以根据客户端发送的异常方问结果进行分析，产生告警，便于开发人员定位异常根因，提高定位异常的准确度和

运维效率。

[0026] 第四方面，本发明实施例提供一种内网安全策略检测装置，该装置包括：内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述装置包括：收发模块，用于生成规则获取请求，并将所述规则获取请求发送至所述服务端；所述收发模块还用于，根据所述规则获取请求，确定所述客户端的检测规则并将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；检测模块，用于访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；告警模块，用于分析所述异常访问结果并产生告警。

[0027] 第五方面，本发明实施例提供一种内网安全策略检测装置，该装置包括：内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述装置包括：收发模块，用于生成规则获取请求，并将所述规则获取请求发送至所述服务端；所述收发模块还用于，接收所述服务端根据所述规则获取请求确定出的检测规则；所述检测规则用于指示客户端与目标端之间的访问权限；检测模块，用于访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；所述异常访问结果用于所述服务端进行分析后产生告警。

[0028] 第六方面，本发明实施例提供一种内网安全策略检测装置，该装置包括：内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述装置包括：收发模块，用于接收所述客户端发送的规则获取请求，并根据所述规则获取请求，确定所述客户端的检测规则；所述收发模块还用于，将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；接收所述客户端发送的异常访问结果，所述异常访问结果为所述客户端根据不符合所述检测规则的目标端确定的；告警模块，用于分析所述异常访问结果并产生告警。

[0029] 第七方面，本申请实施例还提供一种计算设备，包括：存储器，用于存储程序；处理器，用于调用所述存储器中存储的程序，按照获得的程序执行如第一方面、第二方面、第三方面的各种可能的设计中所述的方法。

[0030] 第八方面，本申请实施例还提供一种计算机可读非易失性存储介质，包括计算机可读程序，当计算机读取并执行所述计算机可读程序时，使得计算机执行如第一方面、第二方面、第三方面的各种可能的设计中所述的方法。

[0031] 本申请的这些实现方式或其他实现方式在以下实施例的描述中会更加简明易懂。

附图说明

[0032] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0033] 图1为本发明实施例提供的一种内网安全策略检测的架构示意图；

[0034] 图2a为本发明实施例提供的一种客户端；

[0035] 图2b为本发明实施例提供的一种服务端；

[0036] 图3为本发明实施例提供的一种内网安全策略检测方法的流程示意图；

[0037] 图4为本发明实施例提供的一种白名单和异常访问结果匹配方法的流程示意图；

[0038] 图5为本发明实施例提供的一种内网安全策略检测方法的流程示意图；

[0039] 图6为本发明实施例提供的一种内网安全策略检测的装置示意图；

[0040] 图7为本发明实施例提供的一种内网安全策略检测的装置示意图；

[0041] 图8为本发明实施例提供的一种内网安全策略检测的装置示意图。

具体实施方式

[0042] 为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

[0043] 图1为本发明实施例提供的一种内网安全策略检测的系统架构，该系统架构可以应用到任何企业或机构等组织中的内网网络安全检测中。内网中可以包括网络区域1、网络区域2…网络区域n等多个网络区域，各网络区域中可以设置相应的网络安全策略，这里也可以存在不设置网络安全策略的网络区域(不设置网络安全策略的网络区域无需进行网络安全策略检测)，具体设置方案不做限定。以每个网络区域中设置网络安全策略为例，分别在网络区域1、网络区域2…网络区域n中确定一个客户端(一般来说，同一个网络区域中的各客户端的网络安全策略相同，为了节省网络资源，可以针对每个网络区域选择一个客户端进行网络安全策略检测；若网络资源充裕，也可以针对一个网络区域设置多个客户端，或者根据网络区域的网络安全策略的布置情况，以及根据需求在网络区域中确定一个或多个客户端)。开发人员可以在服务端1中的前端页面配置检测规则和白名单等，进而，客户端将生成的规则获取请求发送至服务端1，服务端1根据客户端发送的规则获取请求确定该客户端对应的检测规则，并将该检测规则发送至该客户端。该客户端根据检测规则分别访问该检测规则中的目标端，获取访问各目标端的访问信息，并将不符合该检测规则的异常访问结果发送至服务端1。服务端1接收异常访问结果并根据白名单对该异常访问结果进行分析，将与白名单对应的异常访问结果删除后，根据剩余的异常访问结果产生告警，可以将该告警通过邮件或短信等方式通知开发人员，使得开发人员及时发现网络安全策略的异常，加快异常根因定位，提高运维效率。

[0044] 基于上述图1中的系统架构，如图2a所示，本申请实施例提供了一种客户端，该客户端中包含规则获取模块和检测模块；规则获取模块用于生成规则获取请求，并将规则获取请求发送至服务端1。接收服务端1返回的检测规则后，通过检测模块分别访问检测规则中的目标端，获取异常访问结果，并通过检测模块将异常访问结果发送至服务端1。

[0045] 基于上述图1中的系统架构，如图2b所示，本申请实施例提供了一种服务端，该服务端1中包含检测规则模块、结果处理模块和告警模块；其中，检测规则模块用于根据检测规则更新指令或白名单更新指令分别对检测规则和/或网络安全策略，以及白名单进行更新；并根据接收的客户端的规则获取请求确定对应的检测规则，将该检测规则发送至该客户端。结果处理模块用于接收客户端的异常访问结果，并根据白名单删除该白名单对应的异常访问结果，通过告警模块根据剩余的异常访问结果产生告警。这里需要说明的是，上述内网安全策略检测的系统架构、客户端和服务端只是本申请的一种示例，并不对本申请中

的具体实施所基于的系统和设备做限定。

[0046] 基于上述系统架构和设备，本申请实施例提供了一种内网安全策略检测方法流程，如图3所示，包括：

[0047] 步骤301、所述客户端生成规则获取请求，并将所述规则获取请求发送至所述服务端；

[0048] 此处，客户端可以是个人计算机、服务器主机等设备，这里对具体设备种类不做限定。

[0049] 步骤302、所述服务端根据所述规则获取请求，确定所述客户端的检测规则并将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；

[0050] 此处，访问权限可以是客户端是否应该与目标端实现通信。

[0051] 步骤303、所述客户端访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；

[0052] 此处，例如，检测规则中客户端与目标端访问权限是不应连通，但是客户端与目标端在访问中实现连通，则可以确定该客户端所在的网络区域的网络安全策略有漏洞，则生成异常访问结果。

[0053] 步骤304、所述服务端分析所述异常访问结果并产生告警。

[0054] 上述方法中，一般来说，同一个网络区域中的网络安全策略相同。因此，可以针对一个网络区域选定一个客户端(若是网络资源允许，也可以选定多个客户端，这里只是一种最优实现方法)，作为用于检测网络安全策略的客户端；多个网络区域对应多个客户端，这多个客户端可以与服务端通信。如此，客户端通过规则获取请求，可以从服务端获取检测规则，实现自动更新检测规则，降低检测规则变更难度。客户端还可以将检测得到的异常访问结果发送至服务端，使得服务端可以对各客户端上报的异常访问结果进行分析，确定对应网络区域的网络安全策略是否有效。

[0055] 本申请实施例提供了一种异常访问结果分析方法，所述服务端分析所述异常访问结果并产生告警，包括：所述服务端确定所述异常访问结果是否符合白名单中的网络安全策略；若不符合，则根据所述异常访问结果生成告警。也就是说，服务端中包含白名单，若异常访问结果中存在于白名单中相匹配的信息，即，确定该异常访问结果不属于网络安全策略异常的结果，而属于白名单中的网络安全策略，则将该匹配的异常访问结果删除，不必生成告警。并根据不符合白名单的异常访问结果生成告警。

[0056] 本申请实施例提供了一种异常访问结果分析方法，所述服务端确定所述异常访问结果是否符合白名单中的网络安全策略，包括：所述服务端确定所述异常访问结果中的源IP地址、目标IP地址和目标端口是否属于所述网络安全策略中的预设源IP地址、预设目标IP地址和预设目标端口；若存在至少一项不符合，则确定所述异常访问结果不符合所述网络安全策略。

[0057] 也就是说，客户端根据检测规则访问检测规则中的目标端，获取的访问信息中包含客户端IP地址，即源IP地址，还包括目标端的目标IP地址和目标端口。若该访问信息异常，则将该访问信息记录为异常访问结果发送至服务端。服务端中的白名单中包含网络安全策略，该网络安全策略中包含预设源IP地址、预设目标IP地址和预设目标端口。若是异常访问结果中的源IP地址、目标IP地址和目标端口与网络安全策略中包含预设源IP地址、预

设目标IP地址和预设目标端口完全匹配，则可以认为该异常访问结果的实质是非异常的，将该异常访问结果删除。

[0058] 在一种示例中，网络区域1的IP地址段为192.168.124.0/24、客户端的IP地址为192.168.124.20、网络区域2的IP地址段为192.168.125.0/24、服务端的白名单中的网络安全策略中包含预设源IP地址为该内网中的所有IP地址0.0.0.0/0、预设目标IP地址192.168.125.20和预设目标端口8080。网络区域1中的客户端获取到的检测规则为：该内网中的所有IP地址可以访问IP地址段为192.168.125.0/24的80、443端口，其他的端口不允许访问。即，当客户端向服务端发送规则获取请求时，获取服务端返回的数据为：

[0059] {“rules”:{

[0060] “id”:”1”,--(检测规则标识,1)

[0061] ”src_ip”:”0.0.0.0/0”,--(源IP地址为该内网中的所有IP地址)

[0062] ”dst_ip”:”192.168.125.0/24”,--(目标IP地址为网络区域2中的所有IP地址)

[0063] ”open_ports”:”80,443”,--(网络区域2中的所有设备的开放端口为,80,443)

[0064] }}.

[0065] 即，网络安全策略是：网络区域2的设备不能被其他网络区域的设备访问到除了80和443以外的端口，而网络区域2中有一台申请了例外的设备，该设备IP地址为：192.168.125.20需要被其他网络区域的设备访问到8080端口。

[0066] 客户端根据获取的上述检测规则1确定自身的IP地址是否存在于检测规则1中的源IP地址中；若不存在，可以认为客户端需要检测默认的65535个端口，即，所有端口(若客户端的自身IP地址不存在于检测规则1的源IP地址中，则网络安全策略是不允许客户端访问网络区域2中的任何一个端口；因此，客户端需要分别与网络区域2中的所有端口尝试连接，以达到检测的目的；若客户端可以与网络区域2中的不可连通的端口实现连通，则该网络区域1和/或网络区域2中的网络安全策略出现异常，需要生成异常访问结果)。若客户端确定自身的IP地址存在于检测规则1中的源IP地址中，则将端口列表中的网络区域2中端口80和443删除(在一种可能中，客户端可以连通的端口无需尝试连接)，尝试与端口列表中剩余的除80和443以外的65533个端口连接，以达到检测网络安全策略的目的。若客户端与网络区域2中IP地址192.168.125.20中的端口90和8080建立连接成功，则生成包含：源IP地址192.168.124.20、目标IP地址192.168.125.20、目标端口90，和源IP地址192.168.124.20、目标IP地址192.168.125.20、目标端口8080两条异常访问结果。客户端将该异常访问结果发送至服务端，服务端接收该异常访问结果后，分别将该两条异常访问结果与白名单匹配，确定源IP地址192.168.124.20、目标IP地址192.168.125.20、目标端口8080的异常访问结果符合白名单的网络安全策略中包含预设源IP地址为该内网中的所有IP地址0.0.0.0/0、预设目标IP地址192.168.125.20和预设目标端口8080，则将该条异常访问结果删除，根据剩余的异常访问结果产生告警。

[0067] 这里本申请实施例提供一种异常访问结果与白名单匹配方法：

[0068] 所述服务端确定所述异常访问结果中的源IP地址是否属于所述网络安全策略中的预设源IP地址，若不属于，则获取下一条异常访问结果；

[0069] 若属于，则所述服务端确定所述异常访问结果中的目的IP地址是否属于所述网络安全策略中的预设目的IP地址，若不属于，则获取下一条异常访问结果；

[0070] 若属于，则所述服务端确定所述异常访问结果中的目的端口是否属于所述网络安全策略中的预设目的端口，若不属于，则获取下一条异常访问结果；

[0071] 若属于，则删除该条异常访问结果；最终获取剩余异常访问结果，针对每条剩余异常访问结果产生告警。其中，服务端可以以接收异常访问结果的时间为匹配异常访问结果顺序，先接收的异常访问结果先进行匹配，这里确定匹配异常访问结果顺序的方式只是一种可能的设计，并不对具体匹配顺序的方式做限定。

[0072] 基于上述示例和方法，这里本申请实施例提供一种异常访问结果与白名单匹配方法流程示例，如图4所示：步骤401、获取异常访问结果，依次遍历白名单列表，获取相应的白名单数据。如上述示例，获取源IP地址192.168.124.20、目标IP地址192.168.125.20、目标端口8080的异常访问结果。第一条白名单：{“white_list_src_ip”:”0.0.0.0/0”,”white_list_dst_ip”:”192.168.125.20”,”open_ports”:”8080”}；

[0073] 步骤402、判断异常访问结果的源IP地址src_ip是否在白名单中的源IP地址white_list_src_ip之中；如果不在则返回步骤401继续获取白名单中下一条白名单数据。如果在则执行步骤403继续往下判断。

[0074] 步骤403、判断dst_ip与white_list_dst_ip是否相等；如果不相等则回到步骤401获取下一条白名单数据。如果相等则执行步骤404继续往下判断。

[0075] 步骤404、判断port是否在open_ports之中；如果不在则回到步骤401获取下一条白名单数据。如果在则代表该条异常访问结果在白名单之中，删除该条异常访问结果，并回到步骤401继续获取下一条异常访问结果数据。该示例中，该异常访问结果在白名单之中，删除该条异常访问结果。步骤401、若还存在未匹配的异常访问结果，则获取异常访问结果，依次遍历白名单列表，获取相应的白名单数据。如上述示例，获取源IP地址192.168.124.20、目标IP地址192.168.125.20、目标端口90的异常访问结果。第一条白名单：{“white_list_src_ip”:”0.0.0.0/0”,”white_list_dst_ip”:”192.168.125.20”,”open_ports”:”8080”}；

[0076] 步骤402、判断异常访问结果的源IP地址src_ip是否在白名单中的源IP地址white_list_src_ip之中；如果不在则返回步骤401继续获取白名单中下一条白名单数据。如果在则执行步骤403继续往下判断。

[0077] 步骤403、判断dst_ip与white_list_dst_ip是否相等；如果不相等则回到步骤401获取下一条白名单数据。如果相等则执行步骤404继续往下判断。

[0078] 步骤404、判断port是否在open_ports之中；如果不在则回到步骤401获取下一条白名单数据。如果在则代表该条异常访问结果在白名单之中，删除该条异常访问结果，并回到步骤401继续获取下一条异常访问结果数据。该示例中，该异常访问结果不在白名单之中，保留该条异常访问结果。

[0079] 步骤405、遍历完所有的异常访问结果后，剩余的异常访问结果即为要告警的数据，服务端根据剩余的异常访问结果产生告警。在上述示例中，两条异常访问结果中的目标端口为90的异常访问结果与白名单中的网络安全策略不匹配，遍历完所有的异常访问结果后，最后的列表中剩余异常访问结果：源IP地址192.168.124.20、目标IP地址192.168.125.20、目标端口90；针对该异常访问结果产生告警。这里需要说明的是，上述异常访问结果与白名单中的源IP地址、目的IP地址、目的端口分别与预设源IP地址、预设目的

IP地址、预设目的端口的匹配顺序，可以以白名单中的预设源IP地址、预设目的IP地址、预设目的端口的排序进行匹配，也可以按照异常访问结果中源IP地址、目的IP地址、目的端口进行匹配，这里异常访问结果和白名单中的数据匹配顺序可以根据需要设置，具体不做限定。

[0080] 本申请实施例提供了一种规则获取请求验证方法，所述规则获取请求包括所述客户端的IP地址及所述客户端生成的第一签名；所述服务端根据所述规则获取请求，确定所述客户端的检测规则，包括：所述服务端对所述规则获取请求中的第一签名进行验证，验证通过后根据所述客户端的IP地址确定所述客户端的检测规则。也就是说，规则获取请求中可以包含第一签名，使得服务端获取第一签名后，对该第一签名进行验证，若第一签名为合法的，则认为发送该规则获取请求的客户端是合法客户端。

[0081] 本申请实施例提供了一种规则获取请求验证方法，所述规则获取请求中还包括时间戳；所述第一签名通过如下方式生成：所述客户端将所述客户端的IP地址、所述时间戳和所述客户端的授权信息拼接得到有序拼接数据；所述客户端通过预设的加密算法对所述有序拼接数据加密得到所述第一签名；所述服务端对所述规则获取请求中的第一签名进行验证，包括：所述服务端按照所述预设的加密算法，对所述规则获取请求中的所述客户端的IP地址、所述时间戳和服务端的授权信息进行加密，得到第二签名；所述客户端的授权信息与所述服务端的授权信息相同；若所述服务端确定所述第一签名与所述第二签名相同，则通过验证，确定所述客户端为合法的。其中，客户端将客户端的IP地址、时间戳和客户端的授权信息拼接得到有序拼接数据，则进一步通过预设的加密算法将该有序拼接数据进行加密得到第一签名，如，预设的加密算法可以是MD5信息摘要算法或哈希算法等。若客户端的授权信息和服务端的授权信息相同，则客户端的第一签名和服务端的第二签名都是通过客户端的IP地址、时间戳和客户端的授权信息拼接后，再通过预设的加密算法进行加密得到的，则第一签名和第二签名相同，验证通过，客户端为合法客户端。相应的，若客户端的授权信息和服务端的授权信息不相同，则第一签名和第二签名不同，验证不通过，客户端为非法客户端。

[0082] 本申请实施例提供了一种规则更新方法包括：所述服务端接收检测规则更新指令，根据所述检测规则更新指令分别对所述检测规则和/或所述网络安全策略进行更新。也就是说，服务端可以提供前端页面等向外接口，使得开发人员可以在对应位置输入检测规则和网络安全策略、白名单等相关配置信息，服务端根据开发人员输入的配置信息生成检测规则更新指令，将该检测规则、网络安全策略、白名单对应更新。

[0083] 基于图1的系统架构、图2a、图2b、图3的客户端和服务端、包括图4的方法流程，本申请实施例提供了一种内网安全策略检测方法流程，如图5所示，包括：

[0084] 步骤501、服务端接收检测规则更新指令，根据检测规则更新指令分别对检测规则和/或网络安全策略和/或白名单进行更新。在一种示例中，用户可通过服务端的前端页面进行配置，根据企业的网络架构配置相应的检测规则、网络安全策略规则和白名单，服务端根据用户在前端页面输入的配置信息生成检测规则更新指令对检测规则和/或网络安全策略和/或白名单进行更新。在上述示例中，服务端更新后的检测规则1为：网络区域2中的设备允许该企业内网中其他网络区域的设备访问80、443端口，网络区域2中其他的端口不允许访问。即，源IP地址："0.0.0.0/0"；目的IP地址："192.168.125.0/24"；开放的端口："80、

443”。服务端更新后的白名单中的网络安全策略为:包含预设源IP地址为该内网中的所有IP地址0.0.0.0/0、预设目标IP地址192.168.125.20和预设目标端口8080。这里需要说明的是,网络安全策略包括各内网中各网络区域部署的网络安全策略和白名单中预设的网络安全策略,此处只以对白名单中预设的网络安全策略进行更新为示例,但不对各内网中各网络区域部署的网络安全策略具体更新过程做限制,即,客户端也可以通过相同的方法通过请求从服务端获取对应网络区域的网络安全策略。

[0085] 步骤502、客户端将自身IP地址、当前时间戳以及授权信息拼接,通过预设的加密算法生成第一签名,进一步生成包含自身IP地址、当前时间戳和第一签名的规则获取请求。这里授权信息可以是确定客户端加入到该网络区域时,为该客户端配置的;授权信息可以是key值;预设的加密算法可以是MD5算法。

[0086] 步骤503、客户端将规则获取请求发送至服务端。

[0087] 步骤504、服务端获取规则获取请求后,提取规则获取请求中的客户端IP地址和当前时间戳,并获取自身的授权信息,将客户端IP地址、当前时间戳、自身的授权信息拼接,通过预设的加密算法生成第二签名,将第一签名和第二签名进行比较,若第一签名和第二签名相同,则该规则获取请求对应的客户端是合法的。这里服务端的预设的加密算法和客户端的预设的加密算法相同。

[0088] 步骤505、服务端从规则获取请求中获取客户端的IP地址,生成相应的查询语句从数据库中获取检测规则。

[0089] 步骤506、服务端将检测规则返回至发起规则获取请求的客户端。

[0090] 步骤507、客户端接收检测规则,并根据检测规则生成检测列表,依次与检测列表中的目标端口建链socket连接。在上述示例中,根据检测规则1生成的检测列表为:

[0091] {192.168.125.1:1,

[0092] 192.168.125.1:2,

[0093] …

[0094] 192.168.125.24:65535}。其中不包含端口80和端口443。

[0095] 步骤508、客户端根据不符合检测规则的访问信息生成异常访问结果。在上述示例中,客户端与网络区域2中IP地址192.168.125.20中的端口90和8080建立连接成功,生成包含:源IP地址192.168.124.20、目标IP地址192.168.125.20、目标端口90,和源IP地址192.168.124.20、目标IP地址192.168.125.20、目标端口8080两条异常访问结果。

[0096] 步骤509、客户端将异常访问结果发送至服务端。

[0097] 步骤510、服务端根据白名单确定不符合白名单的异常访问结果。在上述示例中,将该两条异常访问结果分别与白名单中的白名单数据:预设源IP地址所有IP地址0.0.0.0/0、预设目标IP地址192.168.125.20和预设目标端口8080进行匹配。

[0098] 步骤511、服务端根据不符合白名单的异常访问结果产生告警。

[0099] 这里需要说明的是,上述方法流程并不唯一,如步骤502可以在步骤501之前执行。

[0100] 基于同样的构思,本发明实施例提供一种内网安全策略检测的装置,图6为本申请实施例提供的一种内网安全策略检测的装置示意图,如图6示,包括:

[0101] 内网安全策略检测系统中包含至少一个客户端和服务端,所述至少一个客户端分别属于内网中的至少一个网络区域,所述装置包括:

[0102] 收发模块601，用于生成规则获取请求，并将所述规则获取请求发送至所述服务端；

[0103] 所述收发模块601还用于，根据所述规则获取请求，确定所述客户端的检测规则并将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；

[0104] 处理模块602，用于访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；

[0105] 所述处理模块602还用于，分析所述异常访问结果并产生告警。

[0106] 可选的，所述处理模块602具体用于：确定所述异常访问结果是否符合白名单中的网络安全策略；若不符合，则根据所述异常访问结果生成告警。

[0107] 可选的，所述处理模块602具体用于：确定所述异常访问结果中的源IP地址、目标IP地址和目标端口是否属于所述网络安全策略中的预设源IP地址、预设目标IP地址和预设目标端口；若存在至少一项不符合，则确定所述异常访问结果不符合所述网络安全策略。

[0108] 可选的，所述规则获取请求包括所述客户端的IP地址及所述客户端生成的第一签名；所述收发模块601具体用于：对所述规则获取请求中的第一签名进行验证，验证通过后根据所述客户端的IP地址确定所述客户端的检测规则。

[0109] 可选的，所述规则获取请求中还包括时间戳；所述第一签名通过如下方式生成：所述收发模块601具体用于：将所述客户端的IP地址、所述时间戳和所述客户端的授权信息拼接得到有序拼接数据；

[0110] 所述客户端通过预设的加密算法对所述有序拼接数据加密得到所述第一签名；所述收发模块601具体用于：按照所述预设的加密算法，对所述规则获取请求中的所述客户端的IP地址、所述时间戳和服务端的授权信息进行加密，得到第二签名；所述客户端的授权信息与所述服务端的授权信息相同；若确定所述第一签名与所述第二签名相同，则通过验证，确定所述客户端为合法的。

[0111] 可选的，所述处理模块602还用于：接收检测规则更新指令，根据所述检测规则更新指令分别对所述检测规则和/或所述网络安全策略进行更新。

[0112] 基于同样的构思，本发明实施例提供一种内网安全策略检测的装置，图7为本申请实施例提供的一种内网安全策略检测的装置示意图，如图7示，包括：

[0113] 内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分别属于内网中的至少一个网络区域，所述装置包括：

[0114] 收发模块701，用于生成规则获取请求，并将所述规则获取请求发送至所述服务端；

[0115] 所述收发模块701还用于，接收所述服务端根据所述规则获取请求确定出的检测规则；所述检测规则用于指示客户端与目标端之间的访问权限；

[0116] 检测模块702，用于访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端；所述异常访问结果用于所述服务端进行分析后产生告警。

[0117] 基于同样的构思，本发明实施例提供一种内网安全策略检测的装置，图8为本申请实施例提供的一种内网安全策略检测的装置示意图，如图8示，包括：

[0118] 内网安全策略检测系统中包含至少一个客户端和服务端，所述至少一个客户端分

别属于内网中的至少一个网络区域，所述装置包括：

[0119] 收发模块801，用于接收所述客户端发送的规则获取请求，并根据所述规则获取请求，确定所述客户端的检测规则；

[0120] 所述收发模块801还用于，将所述检测规则发送至所述客户端，所述检测规则用于指示客户端与目标端之间的访问权限；接收所述客户端发送的异常访问结果，所述异常访问结果为所述客户端根据不符合所述检测规则的目标端确定的；

[0121] 告警模块802，用于分析所述异常访问结果并产生告警。

[0122] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0123] 本申请是参照根据本申请的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0124] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0125] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0126] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

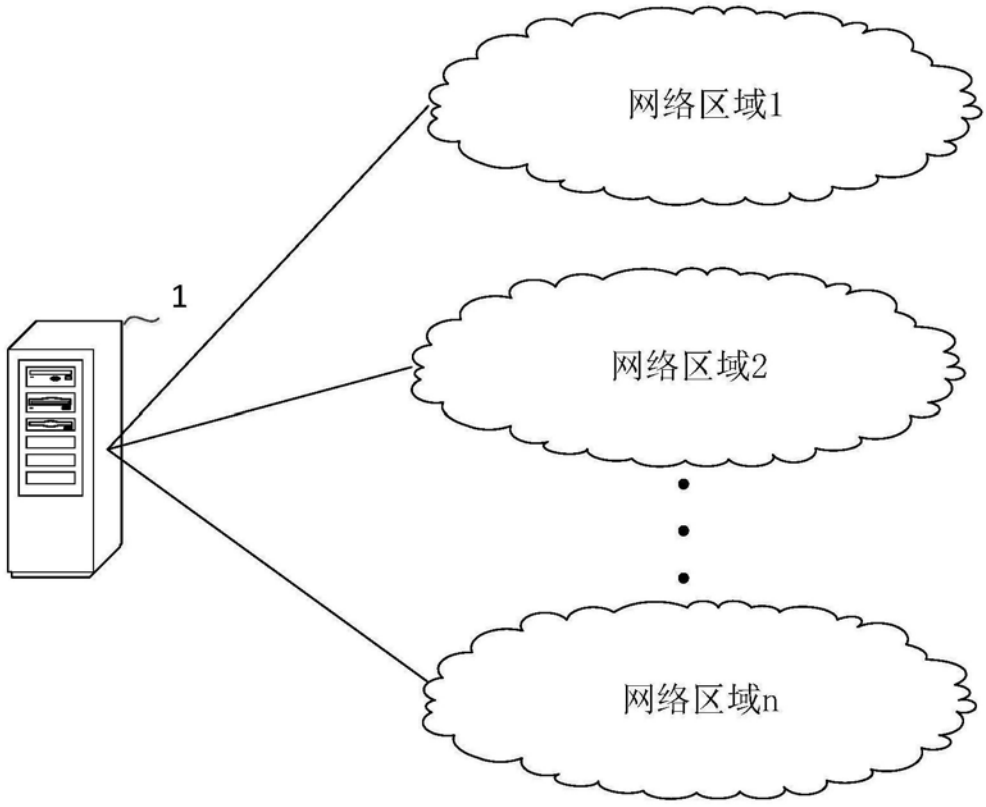


图1

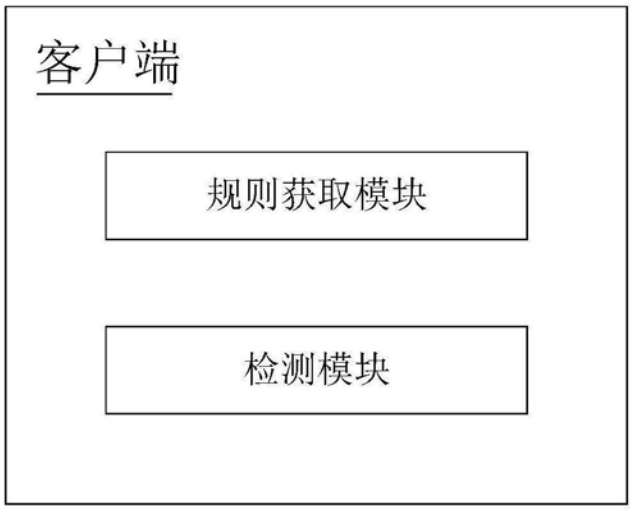


图2a

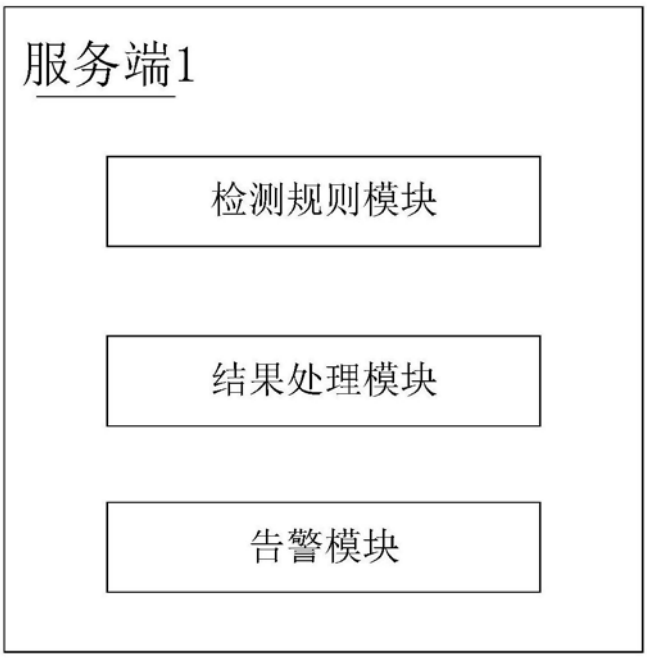

服务端1
检测规则模块
结果处理模块
告警模块

图2b

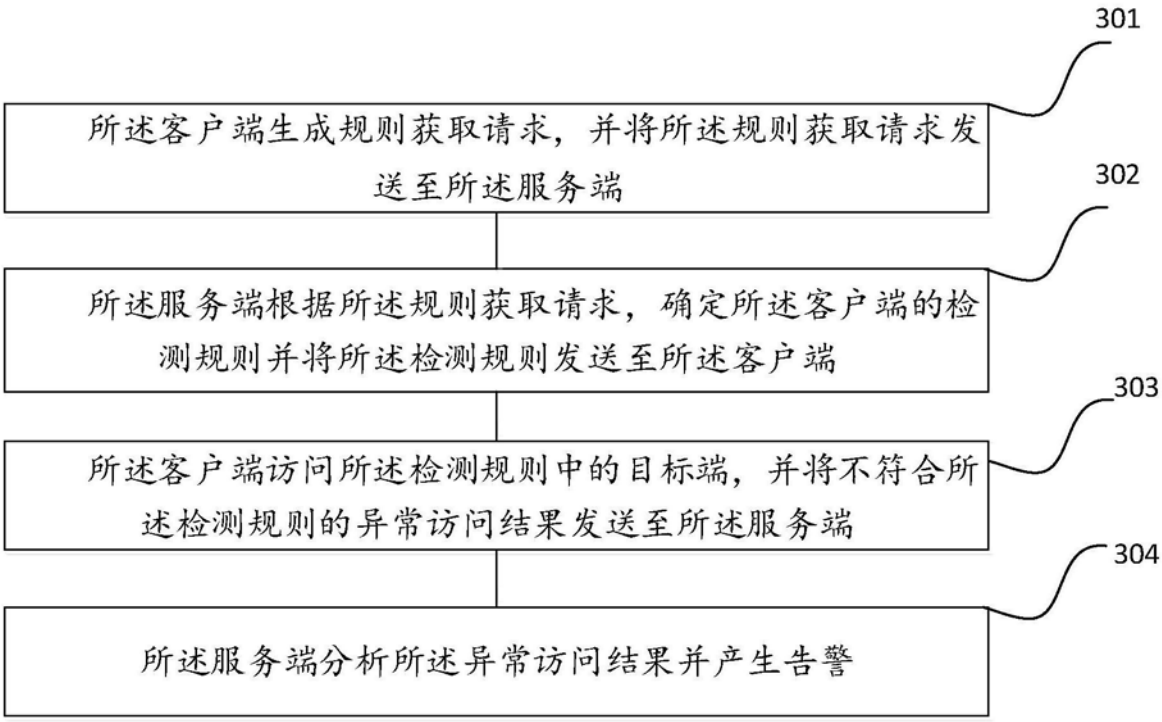

301
所述客户端生成规则获取请求，并将所述规则获取请求发送至所述服务端
302
所述服务端根据所述规则获取请求，确定所述客户端的检测规则并将所述检测规则发送至所述客户端
303
所述客户端访问所述检测规则中的目标端，并将不符合所述检测规则的异常访问结果发送至所述服务端
304
所述服务端分析所述异常访问结果并产生告警

图3

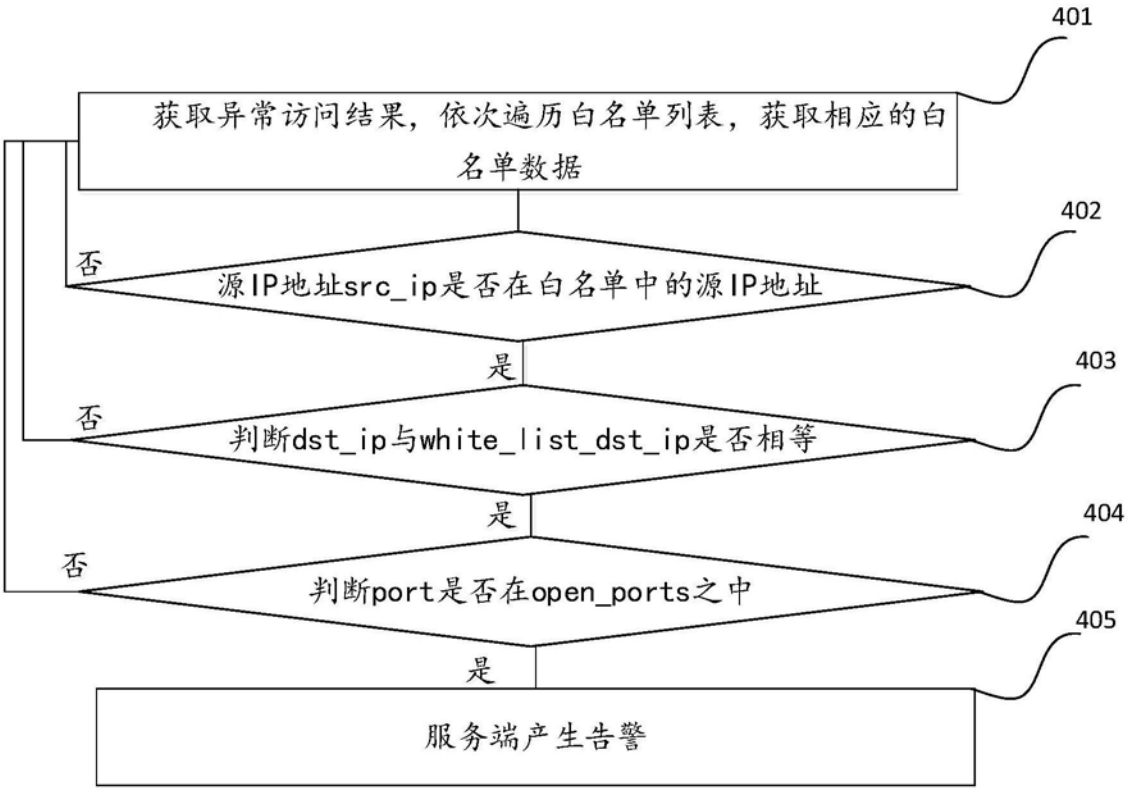

401
获取异常访问结果，依次遍历白名单列表，获取相应的白名单数据
402
否
源IP地址src_ip是否在白名单中的源IP地址
是
403
否
判断dst_ip与white_list_dst_ip是否相等
是
404
否
判断port是否在open_ports之中
是
405
服务端产生告警

图4

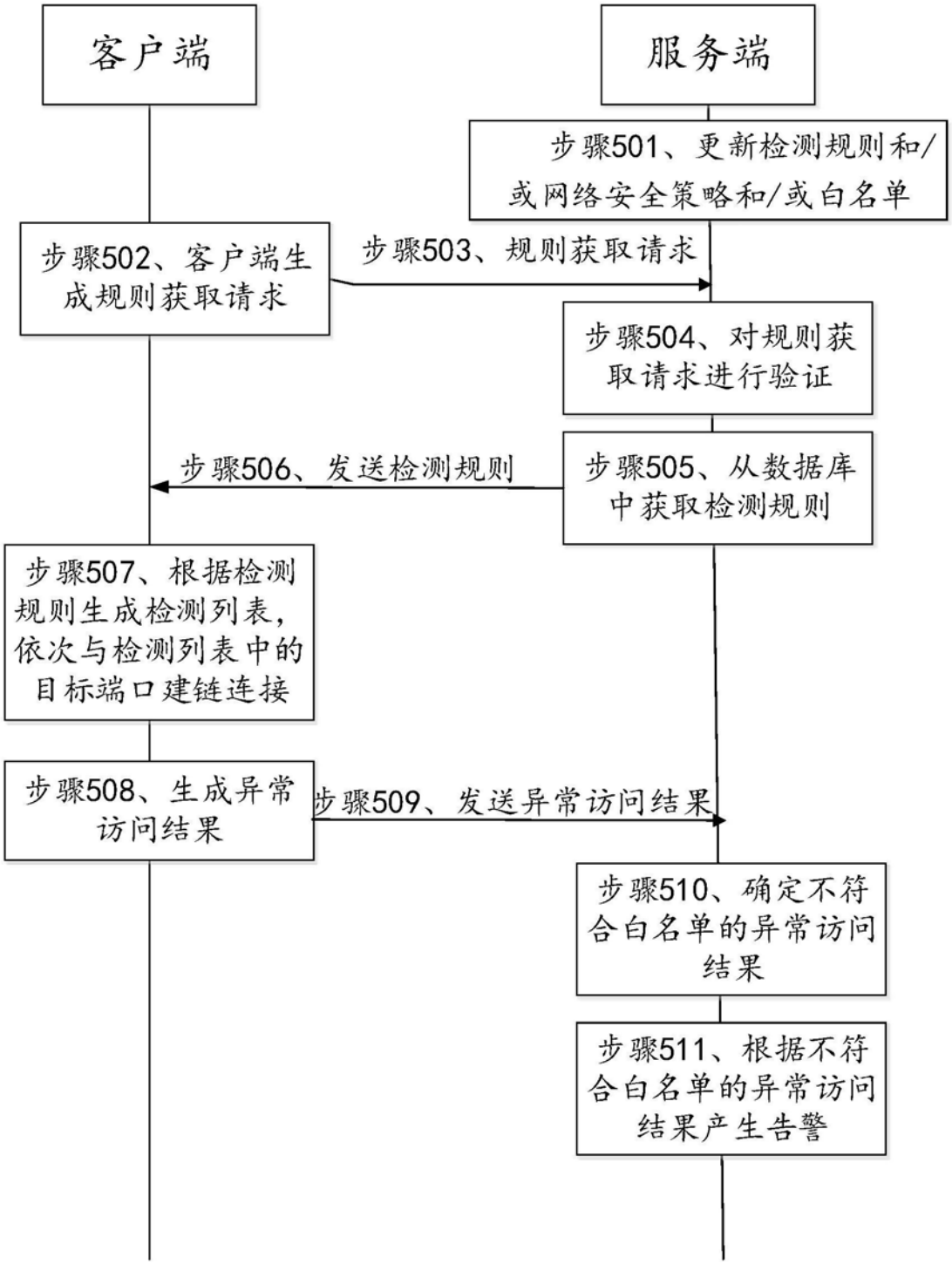

客户端
服务端
步骤501、更新检测规则和/或网络安全策略和/或白名单
步骤502、客户端生成规则获取请求
步骤503、规则获取请求
步骤504、对规则获取请求进行验证
步骤505、从数据库中获取检测规则
步骤506、发送检测规则
步骤507、根据检测规则生成检测列表，依次与检测列表中的目标端口建链连接
步骤508、生成异常访问结果
步骤509、发送异常访问结果
步骤510、确定不符合白名单的异常访问结果
步骤511、根据不符合白名单的异常访问结果产生告警

图5

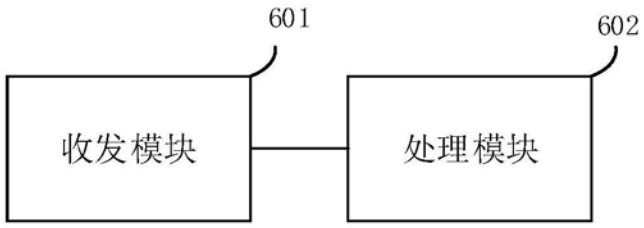


图6

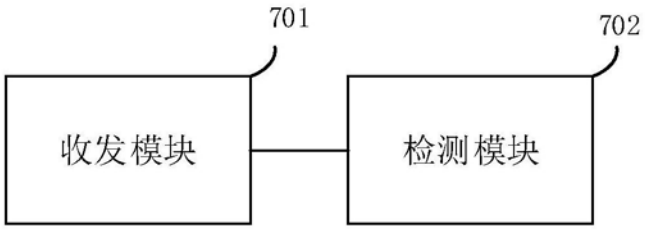


图7

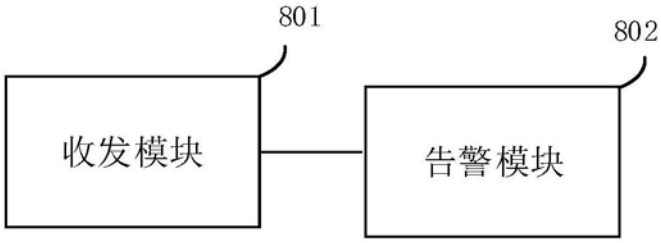


图8