(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108780481 B
(45)授权公告日 2023.08.25

(21)申请号 201780019053.X
(22)申请日 2017.03.20
(65)同一申请的已公布的文献号
申请公布号 CN 108780481 A
(43)申请公布日 2018.11.09
(30)优先权数据
15/079,849 2016.03.24 US
(85)PCT国际申请进入国家阶段日
2018.09.21
(86)PCT国际申请的申请数据
PCT/US2017/023196 2017.03.20
(87)PCT国际申请的公布数据
WO2017/165288 EN 2017.09.28
(73)专利权人 斯诺弗雷克公司
地址 美国蒙大拿州
(72)发明人 詹姆斯·卡尔文·阿姆斯特朗
乔纳森·克雷柏
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
专利代理师 周靖 杨明钊
(51)Int.Cl.
G06F 21/50(2006.01)
(56)对比文件
CN 1874223 A,2006.12.06
US 2010333177 A1,2010.12.30
CN CN101981557 Y,2011.02.23
US 2003154399 A1,2003.08.14
CN 108229133 A,2018.06.29
审查员 穆小川

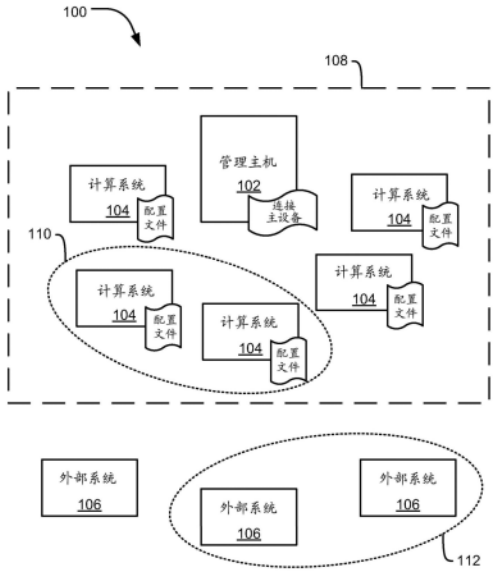
权利要求书4页 说明书11页 附图5页

(54)发明名称

用于安全管理网络连接的系统、方法和设备

(57)摘要

本公开总体上涉及用于管理网络连接的方法、系统和装置。用于管理网络连接的系统包括存储组件、解码组件、规则管理器组件和通知组件。存储组件被配置为存储对于多个联网机器的预期连接列表，其中预期连接列表中的每个连接定义对于该连接的起点和终点。解码组件被配置为对来自多个联网机器的指示对于对应机器的一个或更多个连接的消息解码。规则管理器组件被配置为基于预期连接列表来识别在多个网络机器中的至少一个上的连接的意外存在或不存在。通知组件被配置为提供意外存在或不存在的通知或指示。



CN 108780481 B

1.一种用于管理网络连接的系统,所述系统包括:

用于通过与多个联网机器通信的管理主机存储连接主文件的装置,所述连接主文件包括对于所述多个联网机器的预期连接列表,其中在所述连接主文件中的每个连接定义:

针对所述多个联网机器中的第一机器的第一端点连接;和

针对所述多个联网机器中的第二机器的第二端点连接;

用于从所述多个联网机器中的一个或更多个接收指示到相应机器的连接的通知的装置;

用于确定所述第一端点连接是否连接到所述第一机器并且所述第二端点连接是否连接到所述第二机器的装置;以及

用于响应于确定所述第一端点连接连接到所述第一机器并且所述第二端点连接连接到所述第二机器而创建在所述第一端点连接和所述第二端点连接处的必要许可的装置。

2.根据权利要求1所述的系统,其中,用于存储包括所述预期连接列表的所述连接主文件的装置包括用于基于数据序列化标准来存储所述预期连接列表的装置。

3.根据权利要求1所述的系统,其中,用于存储所述连接主文件的装置包括用于以YAML文件格式存储所述预期连接列表的装置。

4.根据权利要求1所述的系统,其中,用于存储包括所述预期连接列表的所述连接主文件的装置包括用于所述预期连接列表的版本跟踪和控制的装置。

5.根据权利要求1所述的系统,其中,所述连接主文件中的每个连接还包括对于对应连接的协议、端口号或端口号范围中的一个或更多个。

6.根据权利要求1所述的系统,其中,在所述预期连接列表中针对所述第一机器的所述第一端点连接或针对所述第二机器的所述第二端点连接中的一个或更多个包括组。

7.根据权利要求1所述的系统,其中,用于接收所述通知的装置包括用于接收包括对于所述相应机器的当前连接或配置的连接中的一个或更多个的消息的装置。

8.根据权利要求1所述的系统,其中,所述通知包括用于机器的路由表,其中所述连接主文件包括主路由表。

9.根据权利要求1所述的系统,还包括用于确定在所述连接主文件中存在匹配条目的装置。

10.根据权利要求1所述的系统,还包括基于对应机器在所述连接主文件中没有匹配条目来确定连接是意外。

11.根据权利要求1所述的系统,还包括基于所述连接主文件中的条目在对于对应机器的一个或更多个连接中没有匹配连接来确定连接意外地不存在。

12.根据权利要求1所述的系统,其中,用于提供所述通知的装置包括用于将警告保存到日志文件或用户界面的通知区域的装置。

13.根据权利要求1所述的系统,其中,用于提供所述通知的装置包括用于在消息中向管理员提供所述通知的装置。

14.根据权利要求1所述的系统,其中,用于提供所述通知的装置包括用于标记在所述连接主文件中的条目以反映所述连接的意外存在或不存在的装置。

15.根据权利要求1所述的系统,还包括用于确定所述预期连接列表和在所述多个联网机器上的实际连接或配置之间的差异的数量的装置。

16.根据权利要求1所述的系统，还包括用于基于所述连接主文件来修改所述多个联网机器上的连接配置的装置。

17.一种用于管理网络连接的方法，所述方法包括：

通过与多个联网机器通信的管理主机存储连接主文件，所述连接主文件包括对于所述多个联网机器的预期连接列表，其中在所述连接主文件中的每个连接定义：

针对所述多个联网机器中的第一机器的第一端点连接；和

针对所述多个联网机器中的第二机器的第二端点连接；

从所述多个联网机器中的一个或更多个接收指示到相应机器的连接的通知；

确定所述第一端点连接是否连接到所述第一机器并且所述第二端点连接是否连接到所述第二机器；以及

响应于确定所述第一端点连接连接到所述第一机器并且所述第二端点连接连接到所述第二机器而创建在所述第一端点连接和所述第二端点连接处的必要许可。

18.根据权利要求17所述的方法，其中，所述连接主文件包括基于数据序列化标准而存储的列表。

19.根据权利要求17所述的方法，其中，所述连接主文件包括以YAML文件格式存储的列表。

20.根据权利要求17所述的方法，还包括提供所述连接主文件的版本跟踪和控制。

21.根据权利要求17所述的方法，其中，所述连接主文件中的连接还包括对于对应连接的协议、端口号或端口号范围中的一个或更多个。

22.根据权利要求17所述的方法，其中，对于所述连接主文件中的连接的所述第一端点连接或所述第二端点连接中的一个或更多个包括组。

23.根据权利要求17所述的方法，其中，所述通知包括对于所述相应机器的当前连接或配置的连接中的一个或更多个。

24.根据权利要求17所述的方法，其中，所述通知中的至少一个通知包括用于机器的路由表，其中所述连接主文件包括主路由表。

25.根据权利要求17所述的方法，其中，确定对于所述相应机器的所述连接是预期的，包括确定在所述连接主文件中存在匹配条目。

26.根据权利要求17所述的方法，其中，确定对于所述相应机器的所述连接意外地存在，包括确定对于所述相应机器的所述连接不包括在所述连接主文件中的匹配条目。

27.根据权利要求17所述的方法，其中，确定对于所述相应机器的所述连接意外地不存在，包括确定所述连接主文件中的条目不包括对于所述相应机器的匹配连接。

28.根据权利要求17所述的方法，其中，提供所述通知包括向日志文件或用户界面的通知区域提供警告。

29.根据权利要求17所述的方法，其中，提供所述通知包括在消息中向管理员提供所述通知。

30.根据权利要求17所述的方法，其中，提供所述通知包括标记所述连接主文件中的条目以反映所述连接的意外存在或不存在。

31.根据权利要求17所述的方法，还包括确定在所述连接主文件和所述多个联网机器上的实际连接或配置之间的差异的数量。

32.根据权利要求17所述的方法，还包括基于所述连接主文件来添加或删除所述多个联网机器上的连接配置。

33.一种用于管理网络连接的系统，所述系统包括：

存储组件，其被配置为通过与多个联网机器通信的管理主机存储连接主文件，所述连接主文件包括对于所述多个联网机器的预期连接列表，其中所述连接主文件中的每个连接定义：

针对所述多个联网机器中的第一机器的第一端点连接；和

针对所述多个联网机器中的第二机器的第二端点连接；

解码组件，其被配置为对来自所述多个联网机器的指示到对应机器的连接的消息解码；

规则管理器组件，其被配置为确定所述第一端点连接是否连接到所述第一机器并且所述第二端点连接是否连接到所述第二机器；以及

通知组件，其被配置为响应于确定所述第一端点连接连接到所述第一机器并且所述第二端点连接连接到所述第二机器而创建在所述第一端点连接和所述第二端点连接处的必要许可。

34.根据权利要求33所述的系统，其中，所述连接主文件包括以YAML文件格式存储的列表。

35.根据权利要求33所述的系统，其中，所述存储组件被配置为提供所述连接主文件的版本跟踪和控制。

36.根据权利要求33所述的系统，其中，每个连接还包括对于所述连接的协议、端口号或端口号范围中的一个或更多个。

37.根据权利要求33所述的系统，其中，对于所述连接主文件中的连接的所述第一端点连接或所述第二端点连接中的一个或更多个包括组。

38.根据权利要求33所述的系统，其中，所述消息包括对于所述对应机器的当前连接或配置的连接中的一个或更多个。

39.根据权利要求33所述的系统，其中，所述消息中的至少一个消息包括用于机器的路由表，其中所述连接主文件包括主路由表。

40.根据权利要求33所述的系统，其中，所述规则管理器组件被配置为在所述连接主文件中存在匹配条目时确定对于所述对应机器的所述连接是预期的。

41.根据权利要求33所述的系统，其中，所述规则管理器组件被配置为基于对于所述对应机器的所述连接在所述连接主文件中没有匹配条目来识别所述连接的意外存在。

42.根据权利要求33所述的系统，其中，所述规则管理器组件被配置为基于所述连接主文件中的条目对于所述对应机器没有匹配连接来识别所述连接的意外不存在。

43.根据权利要求33所述的系统，其中，所述通知组件被配置为向日志文件或用户界面的通知区域提供警告。

44.根据权利要求33所述的系统，其中，所述通知组件被配置为在消息中向管理员提供所述通知。

45.根据权利要求33所述的系统，其中，所述通知组件被配置为标记所述连接主文件中的条目，以反映所述连接的意外存在或不存在。

46.根据权利要求33所述的系统，其中，所述通知组件被配置为确定在所述连接主文件和所述多个联网机器上的实际连接或配置之间的差异的数量。

47.根据权利要求33所述的系统，还包括被配置为基于所述连接主文件来添加或删除所述多个联网机器上的连接配置的推送组件。

用于安全管理网络连接的系统、方法和设备

技术领域

[0001] 本公开总体上涉及用于安全管理网络连接的方法、系统和装置。

[0002] 背景

[0003] 计算设备常常通过网络进行通信，例如局域网(LAN)、广域网(WAN)、互联网等。因为计算系统常常用于控制重要的操作系统、存储或访问机密数据或者执行其他重要或敏感的功能，所以计算机系统的安全性非常重要。在一些情况下，可以通过限制或控制特定计算系统被允许通信的设备或系统来提高安全性。

[0004] 附图简述

[0005] 参考以下附图描述了本公开的非限制性和非详尽的实现，其中，除非以其它方式说明，在所有各个附图中相似的参考数字指相似的部分。本公开的优点将关于下面的描述和随附的附图变得更好理解，其中：

[0006] 图1是示出根据一个实现的对于管理主机的示例操作环境的示意性框图；

[0007] 图2是示出根据一个实现的管理主机的示例组件的示意性框图；

[0008] 图3是示出根据一个实现的用于管理在端点处的通信配置的方法的示意性信号图；

[0009] 图4是示出根据一个实现的用于管理网络连接的方法的示意性流程图；以及

[0010] 图5是描绘与本文所教导的计算机过程的启用公开一致的示例计算设备或系统的框图。

[0011] 详细描述

[0012] 目前保护系统的方法集中于保护或配置通信的端点。例如，IP表(在Linux™中用于保护系统安全的核心工具)可以允许特定系统基于端口和互联网协议(IP)地址块来拒绝对系统的访问。Amazon Web Services™(AWS)通过指定来往于可包括多于一个机器或地址的其他安全组的被允许的连接来提供安全组。

[0013] 申请人已经认识到，当前的技术没有提供确认被允许的连接是完整和正确的有效方法。在软件产品中，需要在两台或更多台机器上的两个端点的专用服务之间可能存在内部连接。因为现有技术是在单个端点的基础上配置的，所以这种方法冒失配的配置的风险。例如，一台机器可能允许连接，而另一台不允许。Amazon提供了用于创建安全组的工具CloudFormation™，但是它明确地需要单端方法。当需要两个安全组来进行通信时，管理员需要在模板中输入两个规则，如在http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-security-group.html：找到的对AWS CloudFormation™的下面的引用中所陈述的：

[0014] 如果你想要在那些安全组的入口和出口规则中交叉引用两个安全组，使用AWS::EC2::SecurityGroupEgress和AWS::EC2::SecurityGroupIngress资源来定义你的规则。不要使用在AWS::EC2::SecurityGroup中的所嵌入的入口和出口规则。如果你使用，则它引起AWS CloudFormation所不允许的循环依赖。

[0015] 基于上述限制，申请人开发了改进网络连接管理的系统、方法和设备。申请人认识

到，在至少一个实施例中，从两个端点一起的视角管理网络通信许可而不是分开地管理端点导致更大的控制和效率。

[0016] 在一个实施例中，用于管理网络连接的系统可以存储对于多个被管理的机器、设备或计算系统的预期连接列表。例如，可以使用标记语言或数据序列化标准(例如YAML)来存储预期连接列表。YAML代表YAML不是标记语言，且目的在于是许多或所有编程语言的人类可读标准。在一个实施例中，在预期连接列表中的每个连接都被定义有起点、终点、IP协议和端口号或端口号的范围。如果端点映射到多台机器，则管理系统还可以包括检查和创建在两个端点处的必要许可的工具、验证这些连接的工具和/或指定映射的工具。这些工具中的一个或更多个可用于将远程机器上的连接信息聚集到单个机器(例如管理系统)以及将配置从单个机器推送到远程机器的能力。

[0017] 在一个实施例中，预期连接列表(例如描述连接的YAML文件)可以作为源代码工件来管理(使用任何数量的源代码版本控制系统)。然后，最新版本可用于对照在列表中定义的配置或连接来验证现有配置或连接。在一个实施例中，可以对照预期的配置检查在实时配置中所做的改变，并且如果配置不同步，则生成警报。

[0018] 在一个实施例中，用于管理网络连接的系统包括存储组件、解码组件、规则管理器组件和通知组件。存储组件被配置为存储对于多个联网机器的预期连接列表。预期连接列表中的每个连接定义对于该连接的起点和终点。解码组件被配置为对来自多个联网机器的指示对应机器的一个或更多个连接的消息解码。规则管理器组件被配置为基于预期连接列表来识别在多个联网机器中的至少一个上的连接的意外存在或不存在。通知组件被配置为提供意外存在或不存在的通知或指示。

[0019] 现在参考附图，图1示出了为管理主机102提供操作环境的示例系统100。系统100包括多个被管理的计算系统104和多个外部系统106。管理主机102和计算系统104可以包括计算设备，例如服务器、虚拟机或构成网络计算系统108的一部分的任何其他计算设备。网络计算系统108的管理主机102和计算系统104可以物理地位于同一数据中心或服务器农场内，或者可以彼此远离地定位，并且可以由管理主机102共同管理。外部系统106表示不由管理主机102管理的系统，并且可以包括位于同一数据中心内或远离管理主机102的计算系统。管理主机102、计算系统104和外部系统106中的每一个可以连接到允许它们彼此通信的一个或更多个网络或联网设备。例如，管理主机102、计算系统104和外部系统106可以通过因特网、通过专用网络或任何类型的网络彼此通信。

[0020] 内部或被管理的计算系统104的每一个可以例如在配置文件中为自己存储连接配置。连接配置可以存储在路由表、IP表、防火墙或任何其他格式或程序中。连接配置可以指示被允许与计算系统104通信的其他设备、地址或安全组。连接配置可以指定对于特定连接的通信方向(例如，入站或出站)、地址、端口号(或端口号的范围)、安全组标识符等。安全组标识符可以包括对应于多个机器或地址的名称、号码或其他标识符。例如，第一安全组110包括两个被管理的计算系统104，以及第二安全组112包括两个外部系统106。因此，在特定计算系统104的配置文件中的连接条目可以指示计算系统被允许与在第一安全组110或第二安全组112中的任何系统通信(入站或出站)，而无需明确地标识安全组中的机器。在一个实施例中，每个计算系统104仅为自己存储配置。

[0021] 管理主机102存储连接主文件，其包括对于所有被管理的计算系统104的主信息。

例如,连接主文件可以包括对于在网络计算系统108中所有被管理的计算系统104的预期连接列表。因此,在一个实施例中,列表存储每个计算系统104的连接信息,使得用于计算系统104的所有配置存储在连接主文件中。可以基于任何文件格式(例如标记语言或数据序列化标准)来存储连接主文件。根据一个实施例,连接主文件包括YAML文件。

[0022] 利用由管理主机102存储的连接主文件,管理主机然后可以监控计算系统104的实际配置(例如,基于配置文件)。在一个实施例中,计算系统104的每一个可以周期性地或者响应于请求而向管理主机102发送它的配置文件。当管理主机102已经接收到配置文件时,管理主机102可以将配置文件与连接主文件进行比较以检测任何差异。在一个实施例中,差异可以包括在计算系统处的配置文件中的意外连接的存在。例如,在配置文件中的连接条目可能没有在连接主文件中的相应的条目。在一个实施例中,差异可以包括在计算系统处的配置文件中的预期连接的不存在。例如,在连接主文件中的连接条目可能没有在对于正确的一个或更多个计算系统104的配置文件中的相应的条目。

[0023] 由管理主机102识别的差异可以指示对一个或更多个计算系统104的连接主文件或配置文件存在错误/遗漏。例如,如果在配置文件中存在意外连接(关于连接主文件),则可能是连接主文件不正确地被配置,并且意外连接实际上应该在连接主文件中。另一方面,意外连接可以反映计算系统104的配置文件不正确,并且对于计算系统存在安全风险或操作风险。

[0024] 在一个实施例中,管理主机102及其功能和特征可以提供优于其他可用技术的显著益处。例如,都基于单个端点的现有技术没有容易的机制来对照预期的配置监控现有配置。因为管理主机102提供了在连接基础上而不是在单个端点基础上监控和管理连接的简单且快速的方式,所以管理主机102提高了安全性并降低了在监控中的成本。此外,这些监控方面可以充当对各种安全认证(包括例如服务组织控制2(SOC2)认证和健康保险责任法案(HIPAA)认证和合规)的有效控制。

[0025] 在一个实施例中,管理主机102和连接主文件可用于管理在现有云服务中(例如在Amazon的AWSTM账户中)的安全组配置。在一个示例中,根据需要,AWS安全组可以与外部子网一起在端点处被使用。连接主文件(例如YAML文件)可能注意到某个服务或机器需要与另一个服务或机器通信。运行规则管理器,管理主机102可以确保规则存在于端点处。规则管理器还可以检查安全组中的规则,并删除那些不被期望的规则。在一个实施例中,规则管理器可以作为验证器操作(例如,响应于当启动规则管理器时的标记),以提供在预期规则集(例如,在连接主文件中)和现有规则(例如,在配置文件中)之间的差异的计数。

[0026] 为了说明的目的,示例规则可能是允许外部负载平衡器在单个端口上对全局服务(GS)实例讲话的规则。管理员可以为弹性负载平衡器定义安全组prod_elb,为全局服务定义prod_gs,它们标识属于每个组或服务的机器、地址、标识符等。规则可以如下存储在YAML文件中:

[0027] source:prod_elb

[0028] destination:prod_gs

[0029] protocol:tcp

[0030] service:snowflake_elb

[0031] 上述规则告诉规则管理器(例如,管理主机102或在管理主机102上运行的服务)预

期被定义为snowflake_elb(例如,具有值8084)的端口用具有在prod_elb上到prod_gs的出站规则和在prod_gs上来自prod_elb的入站规则的传输控制协议(TCP)打开。第二映射文件可用于定义哪些机器(例如地址、标识符等)有全球服务(GS)的角色以包括prod_gs作为安全组,以及有负载平衡器的角色以包括prod_elb。GS的示例代码可以如下:

[0032] role:GS

[0033] groups:

[0034] -group:prod_gs

[0035] -group:prod_core

[0036] 在一个实施例中,对于在所有实例当中共享的规则,GS的角色与prod_gs组和第二组prod_core包括在一起。例如,一个角色可能属于多于一个安全组(Amazon AWSTM允许在每个实例上多达五个安全组)。在一个实施例中,管理主机可以执行验证程序以确认所有GS实例都与两个安全组一起运行。

[0037] 上面的示例仅仅是说明性的,并且包括可以扩展以适用于任何多端点配置的教导和原理。在一个实施例中,管理主机102然后可以将配置推送到(或者被管理的计算系统104可以将配置拉到)端点。在一个实施例中,在端点(例如,被管理的计算系统104)处的实际配置可以由管理主机102请求和/或发送到管理主机102。此外,对于端点的各种文件格式类型或通信配置被设想在本公开的范围内。例如,端点可以各自具有路由表,并且可以由在管理主机102上的单个路由表管理器管理。

[0038] 图2是示出管理主机102的示例组件的框图。在所描绘的实施例中,管理主机102包括存储组件202、解码组件204、规则管理器组件206、通知组件208和推送组件210。组件202-210仅作为示例被给出,并且可能没有全被包括在所有实施例中。事实上,一些实施例可以仅包括组件202-210中的一个或者两个或更多个的任何组合而没有限制。一些组件202-210可以位于在不同系统或机器上的管理主机102的外部,或者管理主机102可以包括多个不同的机器或系统,这些机器或系统包括组件202-212的一个或更多个。

[0039] 存储组件202被配置为存储用于多个联网机器(例如图1的被管理的计算系统104)的预期连接列表。在一个实施例中,在预期连接列表中的每个连接定义了该连接的起点和终点。预期连接列表可以被存储为YAML文件的一部分或者任何其他格式或类型的文件。预期连接列表可以包括定义对于连接的行动的关键字,例如连接仅仅是外部的还是内部的(它是否允许未被管理的设备或系统使用该连接来进行连接)。在一个实施例中,预期连接列表可存储在源控件中以提供对于列表的版本跟踪。

[0040] 列表中的每个条目可以包括对于连接的多个附加要求,例如对于对应连接或通信的协议、端口号和端口号范围。在一个实施例中,对于在预期连接列表中的连接的起点和/或终点包括诸如安全组的组。组的使用可以允许该组的任何成员参与通信(根据通信或连接要求),而成员没有被特别识别。

[0041] 存储组件202可以将预期连接列表存储在管理主机102本地的连接主文件中,或者可以将该列表存储在网络可访问的存储位置上。

[0042] 解码组件204被配置为从由管理主机102管理的一个或更多个机器接收消息和/或对消息解码。例如,解码组件204可以包括网络接口卡(NIC)、路由组件或其他硬件或软件,以接收、解码、解析或以其他方式处理来自被管理的设备的消息。消息可以包括指示对于对

应机器的一个或更多个连接的信息。例如，消息可以包括对于对应机器的当前连接或配置的连接中的一个或更多个。例如，消息可以包括配置文件中的信息，或者可以包括反映特定机器在特定时间处的实际当前通信连接的信息。在一个实施例中，消息可以包括用于机器的路由表、用于防火墙的配置或关于哪些连接被特定机器或系统允许或不允许的其他信息。

[0043] 规则管理器组件206被配置为确定在端点(例如计算系统104)处的连接或配置是否符合预期连接列表。在一个实施例中，规则管理器组件206被配置为基于预期连接列表来识别在多个联网机器中的至少一个上的连接的意外存在或不存在。在一个实施例中，规则管理器组件206被配置为在预期连接列表中存在匹配条目时确定对于对应机器的一个或更多个连接中的连接是预期的。在一个实施例中，规则管理器组件206被配置为基于在预期连接列表中没有匹配条目的连接来识别意外连接的存在。在一个实施例中，规则管理器组件206被配置为基于预期连接列表中的条目在对于对应机器的一个或更多个连接中没有匹配连接来识别连接的意外不存在。

[0044] 在一个实施例中，规则管理器组件206被配置为验证通信配置的完整性和/或准确性。例如，规则管理器组件206可以对在预期连接列表和被管理的系统的实际配置之间的差异的数量计数。如果差异的数量是非零，这可能意味着预期连接列表不准确，或者端点不正确地被配置。在一个实施例中，管理员可以被通知是否存在差异，并且管理员将确定是否需要对意外连接的列表进行更改。由规则管理器组件206执行的验证角色可以允许确定配置是否匹配预期配置以及使管理员识别任何差异在哪里变得容易。例如，可以容易地确定所有端点都是根据在连接主文件内的预期连接列表来配置的。

[0045] 在一个实施例中，规则管理器组件206被配置为实施在预期连接列表中的预期连接。例如，规则管理器组件206可以基于预期连接列表来将配置向下推送到每个端点。规则管理器组件206可以将列表中的条目翻译成对于每个被管理的端节点的特定规则。例如，规则管理器组件206可以将在YAML文件中的规则转换成配置文件的格式。此外，在YAML文件中的规则可以从整个连接规则(或通信的两端)转换成单个端点规则，用于由特定的端点机器存储。已经被向下推送或发送到端点的这些配置(例如，使用推送组件210)可能导致在端点上的规则的删除或添加，或者可能导致在端点处的所有连接规则的更换。

[0046] 在一个实施例中，规则管理器组件206通常可以作为验证器操作，且然后响应于来自管理员的输入而在端点上实施预期连接。例如，规则管理器组件206可以周期性地或响应于命令而在端点处执行配置的验证。如果存在差异，则规则管理器组件206可以使消息被发送给管理员(例如，使用通知组件208)。然后，管理员可以复查差异，以确定是否需要对预期连接列表进行任何更改。如果不需要更改，则管理员可以使规则管理器组件206将更改推送到或实施到与预期连接列表所要求的不同地配置的任何端点上。如果需要更改，则管理员可以接着对预期连接列表进行更改，并发起另一个验证过程和/或经修订列表的实施。

[0047] 通知组件208被配置为向管理员、管理系统或通知系统提供通知。在一个实施例中，通知组件208可以提供包括意外连接的存在或不存在的指示的通知。例如，通知可以识别从特定系统的配置中缺少的在预期连接列表中的连接。作为另一个例子，通知可以识别不在由管理主机存储的预期连接列表中的在特定系统的配置中的连接。在一个实施例中，通知可以包括用于在预期连接列表和多个机器上的实际连接或配置之间的差异的数量的

指示符。

[0048] 在一个实施例中，通知可以被提供给日志文件、用户界面的通知区域、电子邮件地址、文本消息中的一个或更多个，或者作为另一消息的一部分。作为一个例子，通知组件208可以向监控系统提供通知。Nagios™是可用于递送通知的监控系统的一个示例。通知可以被发送给管理员，使得管理员被告知差异，并且可以采取复查和/或纠正差异的步骤。在一个实施例中，通知组件208被配置为标记在预期连接列表中或在端点的配置文件中的条目，以反映连接的意外存在或不存在。

[0049] 推送组件210被配置为基于由存储组件202存储的预期连接列表来向端点提供连接规则。例如，管理员可能能够建立和/或复查预期连接列表，且然后基于预期连接列表来为每个端点创建规则。在一个实施例中，推送组件210被配置为基于预期连接列表来添加或删除在多个机器上的连接配置。例如，推送组件210可以向缺少对应于预期连接列表中的条目的规则的端点添加规则。作为另一个例子，推送组件210可以删除端点上的规则，基于预期连接列表，该规则不应该在那里。

[0050] 图3是示出用于管理网络连接的方法300的示意性信号图。方法300可以由管理主机102和一个或更多个被管理的计算系统104执行。

[0051] 管理主机102在302处将主连接列表存储在YAML文件中。例如，主连接列表可以包括预期连接列表和/或主连接文件，如在本文所讨论的。管理主机102可以将YAML文件存储在版本跟踪和控制系统中，该版本跟踪和控制系统跟踪对文件的更改，并且可以被有效地监控和跟踪。管理主机102在304处请求来自被管理的计算系统104的当前连接的报告。例如，管理主机102可以周期性地发送对当前连接的请求，以监控如何配置被管理的端点。在一个实施例中，该请求可以包括对端点的连接配置和/或实际当前连接的请求。

[0052] 管理主机102在306处接收指示在计算系统104处的当前连接的一个或更多个消息。例如，被管理的计算系统104可以发送指示当前连接配置或当前通信连接的消息。消息可以根据一种或更多种不同格式(例如以iptable格式、AWS™格式或任何其他格式)指示当前连接。尽管方法300示出了在306处响应于来自管理主机102的请求而接收消息，但是计算系统104(或其他端点)可以自主地或者在不需要管理主机102发送请求的情况下周期性地提供关于当前连接的信息。

[0053] 响应于在306处接收到消息，管理主机102在308处检测在YAML文件和计算系统104的当前配置或连接之间的差异。例如，管理主机102可以检查在YAML文件中的每个条目是否在对应的端点中具有对应的条目，并且检查在端点配置中的每个条目是否在YAML文件中具有对应的条目。管理主机102可以对检测到的差异的数量计数和/或标记差异中的每一个。管理主机102可以在310处发送指示差异的通知(例如，在YAML文件中或在端点配置中的差异的数量和/或所标记的条目)。可以在310处将通知发送到接口或管理员设备314，其中管理员或自动化服务可以确定如何处理差异。例如，管理员可能能够逐一复查每个差异，并选择是否排除YAML文件版本、端点配置版本，和/或为YAML文件或端点定义新规则。例如，管理员可能认识到端点适当地被配置，但是YAML文件丢失或不正确。另一方面，管理员可以确认YAML文件是正确的，且端点不正确或不适当地被配置。一旦管理员确定了如何处理差异，管理员就可以指示YAML文件是最终的(或者特定的差异被接受或拒绝)。接口或管理员设备314在312处向管理主机102提供所接受的或拒绝的差异。例如，由接口或管理员设备314发

送的所接受或拒绝的差异可以包括来自管理员的指示如何处理差异(例如,从计算系统104删除规则或将规则添加到YAML文件中的列表)的输入。

[0054] 管理主机102根据需要基于在312处接收到的所接受或拒绝的差异来在316处更新在YAML文件中的连接列表。对应于更新316连接列表的框以虚线边缘示出,以指示基于从管理员接收的输入,可能不需要对YAML文件中的连接列表的更改。例如,仅当在312处接收到的所接受或拒绝的差异指示规则需要从YAML文件中被添加或删除时,才可以更新主连接列表。管理主机102根据需要在318处将主配置推送到端点。例如,由管理员接受或拒绝的更改可能不需要对端点配置的更改,或者可能需要对一个或更多个端点的任何组合的更改。

[0055] 现在参考图4,示出了用于管理通信配置的方法400的示意性流程图。方法400可以由管理主机(例如图1、图2或图3的管理主机102)执行。

[0056] 方法400开始,且在402处,解码组件204从多个联网机器接收指示对于对应机器的一个或更多个连接的消息。规则管理器组件206在404处基于预期连接列表来识别在多个联网机器中的至少一个上的连接的意外存在或不存在。例如,可以将连接主列表与端点的当前配置进行比较,以确定是否存在意外的连接规则或者是否有从当前配置中缺少的规则。

[0057] 通知组件208在406处提供连接规则的意外存在或不存在的通知或指示。通知可以被发送到机器或接口用于由管理员复查。管理员然后可以采取纠正在端点上或在连接主列表或预期连接列表中的配置的步骤。

[0058] 图5是描绘示例计算设备500的框图。在一些实施例中,计算设备500用于实现本文讨论的一个或多个系统和组件。例如,计算设备500可以允许用户或管理员访问管理主机102;或者管理主机102、计算系统104和/或外部计算系统106可以被实现为具有作为计算机可读代码存储在计算机可读存储介质中的组件或模块的计算设备500。此外,计算设备500可以与本文描述的任何系统和组件交互。因此,计算设备500可以用于执行各种过程和任务,例如在本文中所讨论的过程和任务。计算设备500可以起服务器、客户端或任何其他计算实体的作用。计算设备500可以是在各种计算设备(例如台式计算机、笔记本计算机、服务器计算机、手持计算机、平板计算机等)中的任一个。

[0059] 计算设备500包括都耦合到总线512的一个或更多个处理器502、一个或更多个存储器设备504、一个或更多个接口506、一个或更多个大容量储存设备508以及一个或更多个输入/输出(I/O)设备510。处理器502包括执行在存储器设备504和/或大容量储存设备508中存储的指令的一个或更多个处理器或控制器。处理器502还可以包括各种类型的计算机可读介质,诸如,高速缓冲存储器。

[0060] 存储器设备504包括各种计算机可读介质,例如易失性存储器(例如随机存取存储器(RAM))和/或非易失性存储器(例如只读存储器(ROM))。存储器设备504还可以包括可重写ROM,诸如,闪速存储器。

[0061] 大容量储存设备508包括各种计算机可读介质,例如磁带、磁盘、光盘、固态存储器(例如闪速存储器)等。在大容量储存设备508中还可以包括各种驱动器,以便能够读取和/或写入各种计算机可读介质。大容量储存设备508包括可移动介质和/或不可移动介质。

[0062] I/O设备510包括允许将数据和/或其他信息输入到计算设备500或从计算设备500取出数据和/或其他信息的各种设备。示例I/O设备510包括光标控制设备、键盘、小键盘、麦克风、监视器或其他显示设备、扬声器、打印机、网络接口卡、调制解调器、镜头或其他图像

捕获设备等。

[0063] 接口506包括允许计算设备500与其他系统、设备或计算环境交互的各种接口。示例接口506包括任何数量的不同的网络接口，例如到局域网(LAN)、广域网(WAN)、无线网络和互联网的接口。

[0064] 总线512允许处理器502、存储器设备504、接口506、大容量储存设备508、以及I/O设备510彼此通信、以及与耦合到总线512的其他设备或组件通信。总线512表示在几种类型的总线结构中的一种或更多种，诸如系统总线、PCI总线、IEEE 1394总线、USB总线等等。

[0065] 为了说明的目的，程序和其他可执行程序组件在本文中被示出为分立的块，但是应当理解，这种程序和组件可以在不同时间处驻留在计算设备500的不同储存组件中，并且由处理器502执行。可选地，在本文中描述的系统和过程可以以硬件的方式、或以硬件、软件和/或固件的组合的方式来实现。例如，一个或更多个专用集成电路(ASIC)可经编程来执行本文所描述的系统和过程中的一个或更多个。如本文所使用的，为了执行本文所公开的全部或部分操作的目的，术语“模块”或“组件”意欲传达用于例如通过硬件或硬件、软件和/或固件的组合来实现过程的实现装置。

[0066] 示例

[0067] 以下示例涉及另外的实施例。

[0068] 示例1是一种用于管理网络连接的系统，其包括存储组件、解码组件、规则管理器和通知组件。存储组件被配置为存储对于多个联网机器的预期连接列表，其中在预期连接列表中的每个连接定义对于该连接的起点和终点。解码组件被配置为对来自多个联网机器的指示对于对应机器的一个或更多个连接的消息解码。规则管理器组件被配置为基于预期连接列表来识别在多个联网机器中的至少一个上的连接的意外存在或不存在。通知组件被配置为提供意外存在或不存在的通知或指示。

[0069] 在示例2中，示例1中的预期连接列表包括以YAML文件格式存储的列表。

[0070] 在示例3中，示例1-2中的任何一个中的存储组件被配置为提供对预期连接列表的版本跟踪和控制。

[0071] 在示例4中，示例1-3中的任何一个中的预期连接列表中的连接还包括对于对应连接的协议、端口号和端口号范围中的一个或更多个。

[0072] 在示例5中，示例1-4中的任何一个中的预期连接列表中的连接的起点和终点中的一个或更多个包括诸如安全组的组。

[0073] 在示例6中，示例1-5中的任何一个中的消息包括对于对应机器的当前连接或配置的连接中的一个或更多个。

[0074] 在示例7中，示例1-6中的任何一个中的消息的至少一个消息包括用于机器的路由表，其中预期连接列表包括主路由表。

[0075] 在示例8中，示例1-7中的任何一个中的规则管理器组件被配置为在预期连接列表中存在匹配条目时确定对于对应机器的一个或更多个连接中的连接是预期的。

[0076] 在示例9中，示例1-8中的任何一个中的规则管理器组件被配置为基于对于对应机器的一个或更多个连接中的连接在预期连接列表中没有匹配条目来识别连接的意外存在。

[0077] 在示例10中，示例1-9中的任何一个中的规则管理器组件被配置为基于预期连接列表中的条目在对于对应机器的一个或更多个连接中没有匹配连接来识别连接的意外不

存在。

[0078] 在示例11中,示例1-10中的任何一个中的通知组件被配置为向日志文件或用户界面的通知区域提供警告。

[0079] 在示例12中,示例1-11中的任何一个中的通知组件被配置为在消息中向管理员提供通知。

[0080] 在示例13中,示例1-12中的任何一个中的通知组件被配置为标记在预期连接列表中的条目,以反映该连接的意外存在或不存在。

[0081] 在示例14中,示例1-13中的任何一个中的通知组件被配置为确定在预期连接列表和多个机器上的实际连接或配置之间的差异的数量。

[0082] 在示例15中,示例1-14中的任何一个中的系统还包括被配置为基于预期连接列表来添加或删除在多个机器上的连接配置的推送组件。

[0083] 示例16是一种用于管理网络连接的方法。该方法包括存储对于多个联网机器的预期连接列表,其中预期连接列表中的每个连接定义对于该连接的起点和终点。该方法包括接收来自多个联网机器的指示对于相应机器的一个或更多个连接的指示。该方法包括基于预期连接列表来识别在多个联网机器中的至少一个上的连接的意外存在或不存在。该方法还包括提供意外存在或不存在的通知或指示。

[0084] 在示例17中,示例16中的预期连接列表包括以YAML文件格式存储的列表。

[0085] 在示例18中,示例16-17中的任何一个中的方法还包括提供对预期连接列表的版本跟踪和控制。

[0086] 在示例19中,示例16-18中的任何一个中的预期连接列表中的连接还包括对于对应连接的协议、端口号和端口号范围中的一个或更多个。

[0087] 在示例20中,示例16-19中的任何一个中的预期连接列表中的连接的起点和终点中的一个或更多个包括诸如安全组的组。

[0088] 在示例21中,示例16-20中的任何一个中的消息包括对于对应机器的当前连接或配置的连接中的一个或更多个。

[0089] 在示例22中,示例16-21中的任何一个中的消息中的至少一个消息包括用于机器的路由表,其中预期连接列表包括主路由表。

[0090] 在示例23中,在示例16-22中的任何一个中,确定对于对应机器的一个或更多个连接中的连接是预期的包括确定在预期连接列表中存在匹配条目。

[0091] 在示例24中,在示例16-23中的任何一个中确定对于对应机器的一个或更多个连接中的连接意外地存在包括确定对于对应机器的一个或更多个连接中的连接不包括在预期连接列表中的匹配条目。

[0092] 在示例25中,在示例16-24中的任何一个中,确定对于对应机器的一个或多个连接中的连接意外地不存在包括确定预期连接列表中的条目不包括在对于对应机器的一个或更多个连接中的匹配连接。

[0093] 在示例26中,在示例16-25中的任何一个中提供通知包括向日志文件或用户界面的通知区域提供警告。

[0094] 在示例27中,在示例16-26中的任何一个中提供通知包括在消息中向管理员提供通知。

[0095] 在示例28中，在示例16-27中的任何一个中提供通知包括标记在预期连接列表中的条目，以反映该连接的意外存在或不存在。

[0096] 在示例29中，在示例16-28中的任何一个中的方法还包括确定在预期连接列表和多个机器上的实际连接或配置之间的差异的数量。

[0097] 在示例30中，在示例16-29中的任何一个中的方法还包括基于预期连接列表来添加或删除在多个机器上的连接配置。

[0098] 示例31是一种包括用于实现如在示例1-30中的任一个中的方法或实行如在示例1-30中的任一个中的系统或装置的一个或多个装置的系统或设备。

[0099] 在上面的公开中，已经对形成公开的一部分的附图进行参考，并且其中作为例证示出本公开可被实践的特定实现。应理解的是，其他实施方式可被使用并且可在不脱离本公开的范围的情况下做出结构改变。在说明书中对“一个实施例”、“实施例”、“示例实施例”等的参考指示所描述的实施例可包括特定特征、结构或特性，但是每个实施例可以不必包括该特定特征、结构或特性。此外，这样的短语不一定是指同一实施例。此外，当描述与实施例有关的特定特征、结构或特性时，应建议，这是在本领域的技术人员的知识范围之内，用以实现与其它实施例有关的这种特征、结构或特性，无论是否明确地描述。

[0100] 本文所公开的系统、设备和方法的实现可包括或使用专用或通用计算机，其包括计算机硬件，诸如例如一个或更多个处理器和系统存储器，如本文所讨论的。本公开的范围内的实现还可以包括物理和其他计算机可读介质，以用于承载或存储计算机可执行指令和/或数据结构。该类计算机可读介质可以是任何可用的介质，其可由通用或专用计算机系统访问。存储计算机可读指令的计算机可读介质是计算机存储介质(设备)。承载计算机可执行指令的计算机可读介质为传输介质。因此，通过示例的方式且不为限制，本公开的实现可包括至少两个明显不同种类的计算机可读介质：计算机存储介质(设备)和传输介质。

[0101] 计算机存储介质(设备)包括RAM、ROM、EEPROM、CD-ROM、固态驱动(“SSD”)(例如，基于RAM)、闪存、相变存储器(“PCM”)、其他类型的存储器、其他光盘存储装备、磁盘存储装备或其他磁存储设备，或者可用于以计算机可执行指令或数据结构的形式存储所需程序代码装置并且可由通用或专用计算机访问的任何其他介质。

[0102] 本文公开的设备、系统和方法的实现可以通过计算机网络进行通信。“网络”被定义为一个或更多个数据链路，其实现计算机系统和/或模块和/或其他电子设备之间的电子数据的传输。当经由网络或另一个通信连接(硬接线、无线或者硬接线或无线的组合)将信息转移或提供到计算机时，计算机适当地将连接视为传输介质。传输介质可包括网络和/或数据链路，其可用于以计算机可执行指令或数据结构的形式承载所需程序代码装置，并且可由通用或专用计算机访问。上述的组合也应该被包括在计算机可读介质的范围内。

[0103] 例如，计算机可执行指令包括指令和数据，其中当在处理器处执行时，该指令和数据使通用计算机、专用计算机或专用处理设备实现某个功能或一组功能。例如，计算机可执行指令可以是二进制、中间格式指令(诸如汇编语言或甚至源代码)。尽管已经以特定于结构化特征和/或方法行为的语言描述了主题，应理解的是，随附权利要求中定义的主题不必需局限于所描述的特征或以上所描述的行为。相反，所描述的特征和行为被公开作为实施权利要求的示例形式。

[0104] 本领域中的技术人员将认识到，可在具有许多类型的计算机系统配置(包括个人

计算机、桌面型计算机、膝上型计算机、消息处理器、手持设备、多处理器系统、基于微处理器的或可编程的消费电子设备、网络PC、微型计算机、大型计算机、移动电话、PDA、平板电脑、传呼机、路由器、交换器、各种存储设备等)的网络计算环境中实践本发明。还可在分布式系统环境中实践本公开,其中经网络链接(通过硬接线数据链路、无线数据链路或通过硬接线和无线数据链路的组合)的本地和远程计算机系统都执行任务。在分布式系统环境中,程序模块可位于本地和远程存储器存储设备中。

[0105] 进一步地,在适当的情况下,可在以下中的一个或更多个中执行本文所描述的功能:硬件、软件、固件、数字组件或模拟组件。例如,一个或更多个专用集成电路(ASIC)可经编程来执行本文所描述的系统和过程中的一个或更多个。某些术语贯穿说明书和权利要求使用以指代特定系统组件。如本领域技术人员将认识到,可通过不同的名字来指代组件。本文档不旨在区分在名字上而不是功能上不同的组件。

[0106] 应该注意,上面讨论的实施例可以包括计算机硬件、软件、固件或其任何组合以执行它们的功能的至少一部分。例如,模块可以包括配置成在一个或更多个处理器中执行的计算机代码,并且可以包括由计算机代码控制的硬件逻辑/电路。这些示例设备在本文中为了说明的目的而被提供,并且没有被规定为限制性的。如相关领域的技术人员所知,本公开的实施例可以在其他类型的设备中实现。

[0107] 本公开的至少一些实施例目的在于包括存储在任何计算机可用介质上的这种逻辑(例如,以软件的形式)的计算机程序产品。当在一个或更多个数据处理设备中执行时,这种软件使得设备如本文所述的那样进行操作。

[0108] 虽然上面描述了本公开的各种实施例,但是应当理解,它们仅作为例子而不是限制被呈现。对于相关领域的技术人员明显的是,在不脱离本公开的精神和范围的情况下,可以在其中进行形式和细节上的各种改变。因此,本公开的广度和范围并不被上面描述的示例性实施例中的任一个限制,而应当仅仅根据接下来的权利要求以及它们的等同物来限定。上述描述已经被呈现用于说明和描述的目的。其不旨在为详尽本公开或将本公开限制为所公开的精确形式。鉴于以上教示,许多修改和变型是可能的。进一步地,应注意,前面提到的可选实现中的任一个和全部可在形成本公开的额外混合实现所需的任何组合中被使用。

[0109] 进一步地,尽管描述和示出了本公开的特定实现,本公开不限于如此描述和示出的部件的特定形式和布置。将通过此处所附的权利要求、在这里和在不同申请中提交的任何未来的权利要求以及它们的等同物来定义本公开的范围。

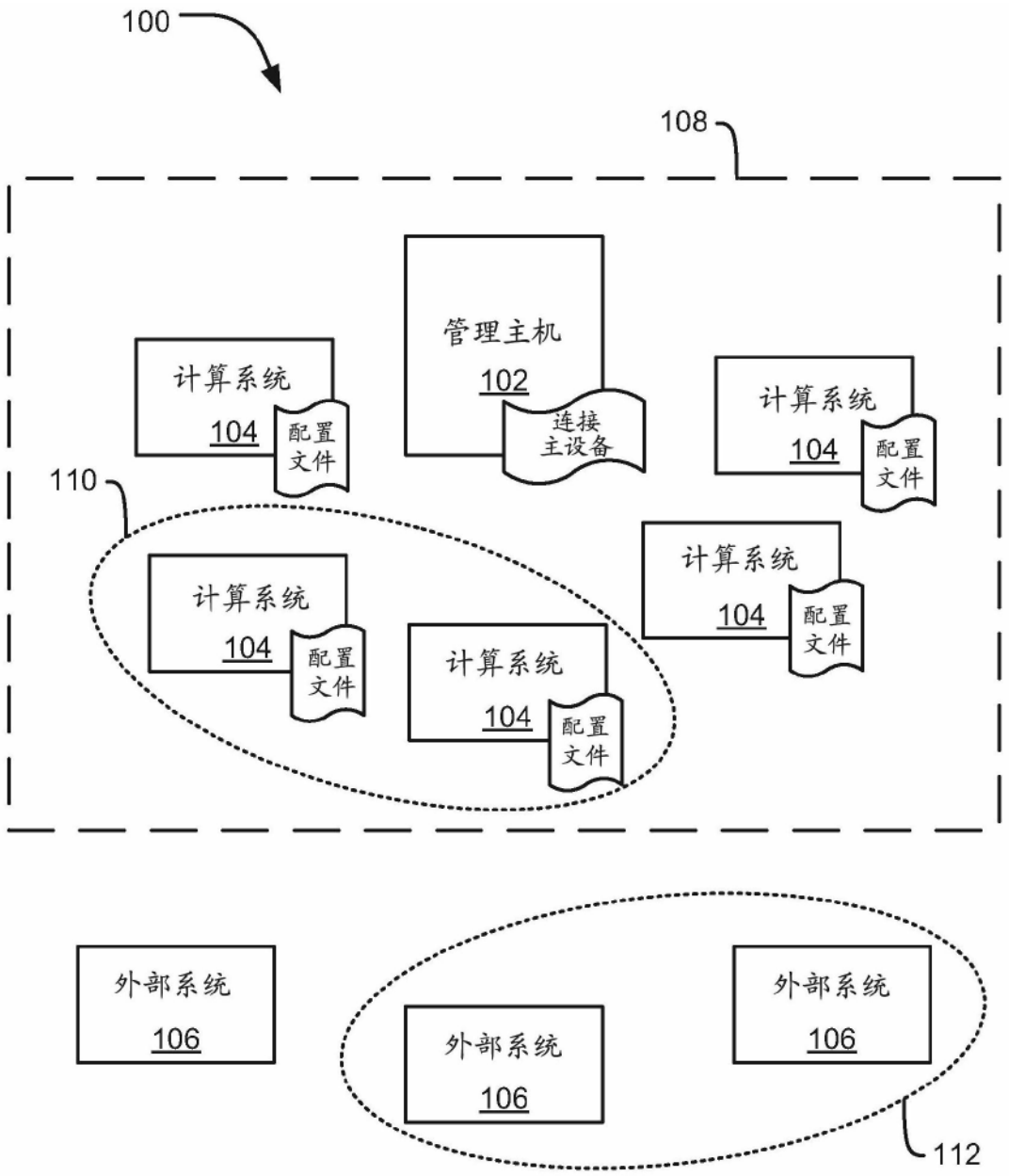


图1

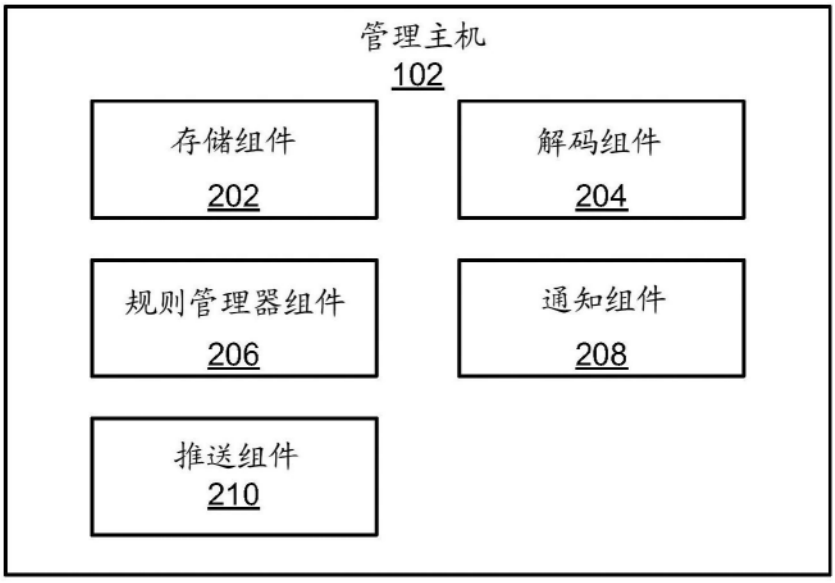


图2

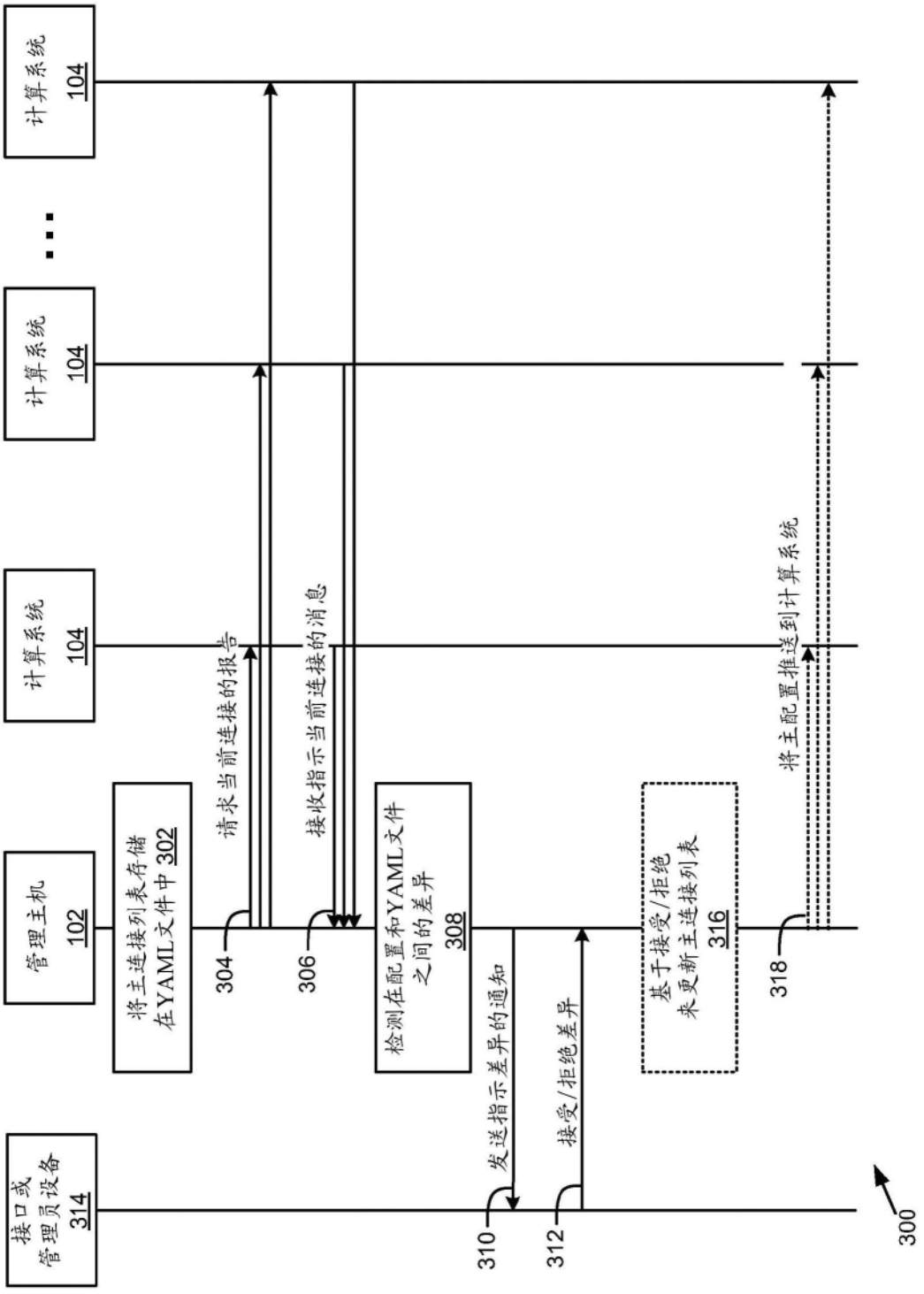

计算系统 104
计算系统 104
计算系统 104
管理主机 102
接口或管理员设备 314
将主连接列表存储在YAML文件中 302
请求当前连接的报告
304
接收指示当前连接的消息
306
检测在配置和YAML文件之间的差异 308
发送指示差异的通知
310
接受/拒绝差异
312
基于接受/拒绝来更新主连接列表 316
318
将主配置推送到计算系统
300

图3

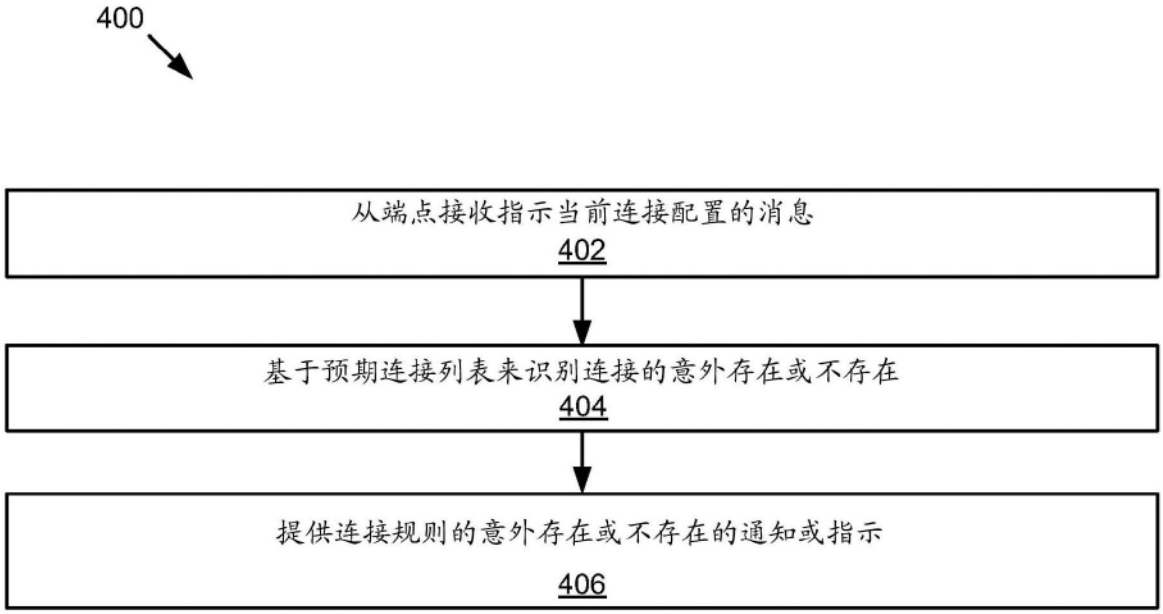

400
从端点接收指示当前连接配置的消息
402
基于预期连接列表来识别连接的意外存在或不存在
404
提供连接规则的意外存在或不存在的通知或指示
406

图4

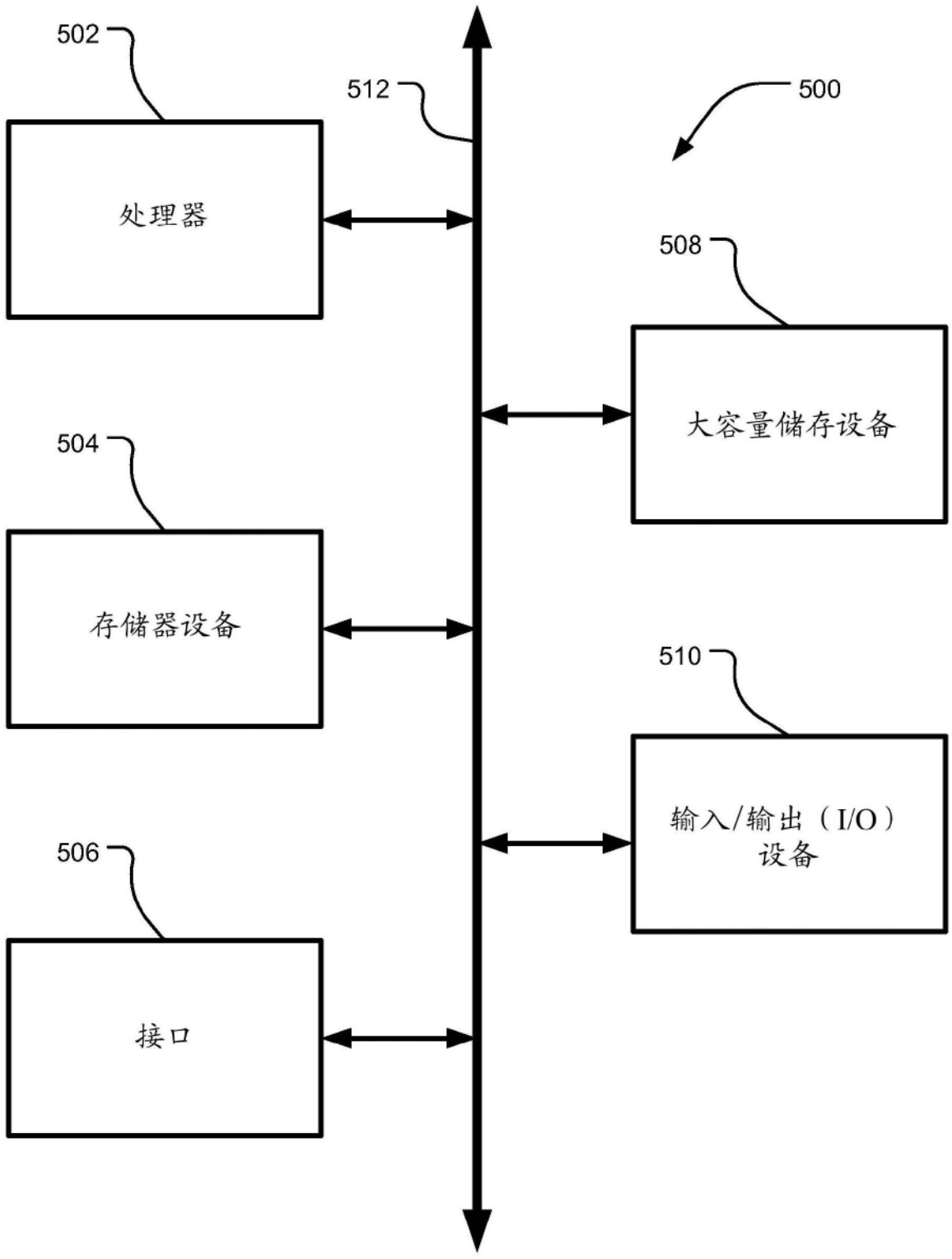


图5