(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 1578215 B
(45)授权公告日 2010.05.12

(21)申请号 200410063279.4

(22)申请日 2004.06.30

(30)优先权数据
10/608,334 2003.06.30 US

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 D·B·贝哈拉诺

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 钱静芳

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 29/06(2006.01)

(56)对比文件
US 2002/0157019 A1,2002.10.24, 全文.
CN 1350382 A,2002.05.22, 全文.
CN 1416245 A,2003.05.07, 全文.
US 5828893 A,1998.10.27, 说明书第2栏第15行至第4栏第51行、附图1-3.

审查员 杨威明

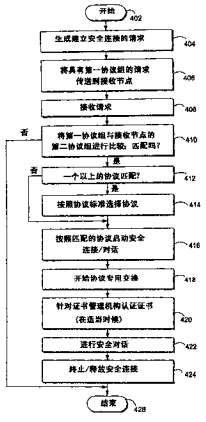
权利要求书 2 页 说明书 5 页 附图 4 页

(54)发明名称

安全协议的自动协商系统和方法

(57)摘要

允许位于支持安全性的域之外的计算机或其它节点与服务器或在该域内的其它节点协商支持的安全协议的协议协商平台。现用目录™(AD)、Kerberos和其它网络技术允许在域中的代理或节点利用默认协议和秘钥、证书或其它认证技术相互安全地通信。然而,过去的外部代理没有透明的方法进入该域,需要手工选择用于跨域边界的协议。根据本发明,外部代理和内部代理中的任一个都可启动建立跨域边界的安全对话的尝试,将包括一组支持的协议的请求传送到接收机器。接着,协商引擎可对在在对话两端中任一端的代理、节点上或机器上的可用协议进行比较,并在发现时,选择一兼容的协议。该内部和外部代理也可以用秘钥、证书或其它机构进行相互认证。



CN 1578215 B

1. 一种自动协商安全协议的方法，其特征在于，包括：

由接收节点接收在具有与其相关联的第一协议组的内部节点和具有与其相关联的第二协议组的外部节点之间建立安全连接的安全授权请求，其中所述内部节点在支持安全性的域内，而所述外部节点在所述支持安全性的域外，其中所述接收节点是所述内部节点和所述外部节点中的一个，并且其中，所述安全授权请求包含指示与所述内部节点和所述外部节点中的另一个相关联的协议组的数据字段；

由所述接收节点将与所述内部节点相关联的第一协议组同与所述外部节点相关联的第二协议组相比较；

由所述接收节点确定所述内部节点和所述外部节点包含共有的两种或更多种安全协议；

按协议标准或网络标准从所述两种或更多种安全协议中选择一优选协议；以及

基于所述优选协议，在所述外部节点和所述内部节点之间自动建立安全连接。

2. 如权利要求 1 所述的方法，其特征在于，所述外部节点包括计算机和支持网络的无线装置中的至少一个。

3. 如权利要求 1 所述的方法，其特征在于，所述内部节点包括客户机计算机和服务器中的至少一个。

4. 如权利要求 1 所述的方法，其特征在于，所述支持安全性的域包括一分布式目录域。

5. 如权利要求 1 所述的方法，其特征在于，所述支持安全性的域包括一基于证书的域。

6. 如权利要求 5 所述的方法，其特征在于，所述基于证书的域包括一支持 Kerberos 的域。

7. 如权利要求 6 所述的方法，其特征在于，所述共有的两种或更多种安全协议包括一 X.509 证书。

8. 如权利要求 1 所述的方法，其特征在于，所述安全授权请求是由所述另一个节点生成的。

9. 如权利要求 1 所述的方法，其特征在于，还包括当所述外部节点和所述内部节点之间的对话完成时终止所述安全连接的步骤。

10. 如权利要求 1 所述的方法，其特征在于，还包括当在所述第一协议组和所述第二协议组之间没有发现匹配时终止连接处理的步骤。

11. 如权利要求 1 所述的方法，其特征在于，还包括认证所述内部节点和所述外部节点中的至少一个的步骤。

12. 如权利要求 15 所述的方法，其特征在于，所述认证的步骤还包括将证书传送到证书管理机构的步骤。

13. 一种自动协商安全协议的系统，其特征在于，包括：

内部节点，所述内部节点位于支持安全性的域的内部，所述内部节点被配置成存储第一协议组，所述第一协议组包括所述内部节点所支持的安全协议；协商引擎，所述协商引擎被配置成：

(1) 接收在具有所述第一协议组的内部节点和在所述支持安全性的域的外部的外部节点之间建立安全连接的安全授权请求，所述外部节点被配置成存储第二协议组，所述第二协议组包括所述外部节点所支持的安全协议，所述安全授权请求包含指示所述第二协议组

的数据字段，

(2) 将与所述内部节点相关联的第一协议组同与所述外部节点相关联的第二协议组相比较，

(3) 确定所述第一协议组和所述第二协议组包含共有的两种或更多种安全协议，

(4) 按协议标准或网络标准从所述两种或更多种安全协议中选择一优选协议，以及

(5) 基于所述优选协议在所述外部节点和所述内部节点之间建立安全连接。

14. 如权利要求 13 所述的系统，其特征在于，所述外部节点包括计算机和支持网络的无线装置中的至少一个。

15. 如权利要求 13 所述的系统，其特征在于，所述内部节点包括客户机计算机和服务器中的至少一个。

16. 如权利要求 13 所述的系统，其特征在于，所述支持安全性的域包括一分布式目录域。

17. 如权利要求 13 所述的系统，其特征在于，所述支持安全性的域包括一基于证书的域。

18. 如权利要求 17 所述的系统，其特征在于，所述基于证书的域包括一支持 Kerberos 的域。

19. 如权利要求 18 所述的系统，其特征在于，所述共有的两种或更多种安全协议包括一 X.509 证书。

20. 如权利要求 13 所述的系统，其特征在于，所述安全授权请求是由外部节点生成的。

21. 如权利要求 13 所述的系统，其特征在于，当所述外部节点和所述内部节点之间的对话完成时，所述协商引擎终止所述安全连接。

22. 如权利要求 13 所述的系统，其特征在于，当在所述第一协议组和所述第二协议组之间没有发现匹配时，所述协商引擎终止连接处理。

23. 如权利要求 13 所述的系统，其特征在于，所述内部节点和所述外部节点中的至少一个认证另一个。

24. 如权利要求 23 所述的系统，其特征在于，所述认证包括将证书传送到证书管理机构。

安全协议的自动协商系统和方法

(1) 技术领域

[0001] 本发明涉及联网计算机领域，特别涉及支持安全性的域和一个或多个外部节点之间的安全协议的自动协商。

(2) 背景技术

[0002] 网络技术的发展使网络管理员和其它人能对他们的网络和其它配置保持更大，更完善的安全控制。例如：微软视窗™NT，2000 和相关产品允许管理员用现用目录™(AD) 结构布署支持安全性的网络域。公知的 Kerberos 网络标准同样允许网络中的节点用秘钥 / 认证平台互相进行认证。有了这些操作技术，网络管理员能，例如：在安全的基础上，向个人工作站和其它客户机推行规则、应用程序、插入码、驱动器和其它来自网络服务器的资源，用于统一安装。在支持安全性的域中的所有机器也许能明显地识别和认证那些和其它类型的数据的传送。

[0003] 然而，当节点在支持安全性的域外时，将规则、应用程序或其它资源的传递到工作站和从工作站传送规则、应用程序或其它资源的能力变得更加困难。例如：一公司可能有一组在局域网 (LAN) 上的计算机，但它们也与不在现用目录™或其它支持安全性的域的一部分的远程位置上的计算机相互作用。跨安全域边界的通信变得更加复杂，部分是因为在域内部的机器和域外部的机器之间建立连接需要在相互支持的安全协议上达成一致。

[0004] 因此，在对话发生之前，强制系统管理员和其它人尝试通过识别一个可在内部和外部机器之间兼容的协议，来作出将外部代理或节点输入到支持安全性的域的安排。例如：外部节点可配置成通过传输层 (TLS) 安全协议、基于 Kerberos 的协议、加密套接字协议层 (SSL) 或其它协议与在支持安全性的域中的管理服务器通信。该机器可依次在它的默认协议中指示一协议故障，请求切换该协议，或对外部节点和代理作出其它反应。因此，可能需要安全、传输和其它协议的手工设置或调整，它一种费时又易出错的过程。还存在其它问题。

(3) 发明内容

[0005] 本发明解决在一方面涉及安全协议的自动协商的系统和方法的领域的这些和其它问题，其中，可以在不需要管理员的干预的自动的基础上，建立与外部代理或节点的安全通信并认证身份。根据本发明的一个方面，网络管理器或其它在支持安全性的域中的代理或节点可启动建立与外部代理或节点的安全连接的尝试。该请求可包括指示一组可供管理器使用的安全协议的数据字段。所述外部代理可接收该请求并将可用于外部代理或管理器的协议与由外部代理支持的一组协议相比较。如果发现可用协议之间的匹配，就可以在选定的协议的基础上继续通信。在实施例中，每个外部代理和内部代理都通过一个秘钥、证书或其它认证机构相互认证。

(4) 附图说明

[0006] 图 1 示出可操作本发明的实施例的网络构造。

[0007] 图 2 示出根据本发明的实施例，在内部节点和外部节点之间进行的协议过程。

[0008] 图 3 示出根据本发明的实施例的协议表间的对比。

[0009] 图 4 示出根据本发明的实施例示出全部协议协商过程。

(5) 具体实施方式

[0010] 图 1 示出其中根据本发明的实施例的协议协商平台和方法可运行的构造。如图所示，在示出的实施中，一组客户机、服务器、代理或其它节点或机器可以在支持安全性的域 102 操作。可以在实施例中的支持安全性的域是或包括，例如：微软视窗™NT 现用目录™(AD)，Kerberos 或其它以证书为基础或以秘钥为基础的域，或其它关闭的或安全分布式的目录或其它环境。在支持安全性的域中说明性地示出的是一内部管理器 104，在实施例中可以是或包括一服务器或其它节点和一组内部代理 106（由 A1，A2...AN 示出，N 为任何值）。

[0011] 在实施例中，该组内部代理可由附加服务器，工作站或其它客户机，或其它在支持安全性的域 102 中操作的内部代理或节点组成，或包括它们，并与内部管理器 104 通信。在实施例中，内容管理器 104 可以确定时间或执行网络定理功能，例如：将网络规则或其它数据传送或“推行”到所述内部代理组 106，例如：存储的操作方针（例如：冗余阵列磁盘机方针，故障结束标准、存储器限制）、带宽实用程序或其它规则或数据。在传送这些或其它类型的数据时，内部管理器 104 或内部代理组 106 可利用支持安全性的域的安全资源来保证网络的安整性或规则及其它数据的分布。

[0012] 如图所示，在实施例中，支持安全性的域 102 可提供认证服务，例如：使用诸如证书 108 的证书，它在实施例中可以是或包括根据 X.509 或其它标准或格式配置的证书。在实施例中，秘钥或其它机构同样可被使用。如图所示，证书 108 可以与内部管理器的认证数据结合或提供内部管理器的认证数据。为了验证，内部代理组 106 组中的任何一个都可以通过将证书 108 传送到证书管理机构 110 来认证规则、指令或其它从内部管理器 104 接收的数据。证书管理机构自己也可位于支持安全性的域 102 中，或按照示出的位于支持安全性的域 102 的外面。

[0013] 在实施例中，证书管理机构 110 可以是或包括一服务器，或配置成读取并解码证书 108 的其它节点或其它认证机构，并将结果返回给内部代理组 106 或其它节点。内部代理组 106 中的每个节点也可与证书，秘钥或其它与支持安全性的域 102 兼容的认证数据相结合。内部代理组 106 中的节点也可以利用证书或其它机构相互通信及相互认证。

[0014] 在图 1 所示的实施中，外部代理 114 也可以配置成通过通信网络 112 与内部管理器 104 通信。该外部代理 114 也可以是或包括服务器、工作站或其它节点或资源。为了认证，该外部代理 114 也可以与识别外部代理 114 的证书 116 相结合。通过通信网络 112，外部代理 114 可与内部管理器 104 或实施例中的其它节点通信。通信网络 112 可以是，包括或连接到诸如：因特网、企业内部网、局域网 (LAN)、广域网 (WAN)、城域网 (MAN)、存储区网络 (SAN)、帧中继连接、高级智能网络 (AIN) 连接、同步光网 (SONET) 连接，数字 T1，T3，E1 或 E3 线路，数字数据服务 (DDS) 连接、ATM（异步传输模式）连接、FDDI（光纤分布式的数据界面）、CDDI（铜分布式的数据界面）或其它有线的、无线的或光连接。在实施例中外部代理 114 可以是或包含工作站、服务器、支持无线网络的装置、或其它节点、为联网的通信配置的

代理或平台。

[0015] 不同于跨域通信的已有实施，根据本发明的实施例，外部代理可启动与内部管理器 104 的联系，在相互兼容协议的基础上，以自动且透明的形式，用手工选择一兼容协议来建立安全连接。如图 2 所示，在外部代理 114 上执行的外部应用程序 130 可通过外部协商引擎 126 启动与内部管理器 104 的联系。外部应用程序 130 可以是或包括系统实用程序、生产力或其它应用程序，例如 :数据备份调度程序、防火墙、防病毒或其它应用程序。例如 :外部应用程序 130 可能需要用户简档、更新或其它数据来执行各种任务，并因此启动与内部管理器 104 的这种通信。

[0016] 外部协商引擎 126 可以处理并管理外部应用程序 130 请求的通信，以与支持安全性的域 102 中的内部管理器 104 建立可相互兼容的通信链路。如示出的，在实施例中，作为公知的简单且防护的 GSS-API 协商 (SPNEGO) 协议的实施，外部协商引擎 126 可以启动并管理协商模块 118。也可以用其它协议。在实施例中，可以通过外部代理 114 的操作系统，例如 :通过应用编程界面 (API) 或其它机构来访问、启动或生成协商模块 118。

[0017] 外部协商引擎 126 也可包括或生成外部传输指定器 120，指示以消息为基础的或可能被外部代理 114 用于执行协议协商过程的其它信道。例如 :在实施例中，外部传输指定器 120 可将安全支持供应者界面 (SSPI) 协议指定为微软 NET 构造的一部分，允许外部应用程序 130 或其它软件或模块来存取，例如 :动态链接库或支持标准密码的或其它编码方案的其它资源。可以在外部传输指定器 120 中使用或指定其它协议。因此，如图 2 所示，该外部协商引擎 126 可传送表示那个或其它数据的数据报，至与内部管理器 104 相关联的内部协商引擎 128。

[0018] 内部协商引擎 128 也可包括或连接到协商模块 122 和内部传输指定器 124。接着，内部协商引擎 128 可与在内部管理器 104 上执行或由内部管理器存取的内部应用程序 132 通信。例如 :内部应用程序 132 可以是或包括系统管理、生产力或其它应用程序。当接到与内部管理器 104 建立通信的请求时，内部协商引擎 128 可以通过内部传输指定器 124 与外部代理 114 建立以消息为基础的或其它的信道，例如 :确认信道用 SSPI 协议的信道通信。

[0019] 外部协商引擎 126 和外部协商引擎 128 可以用外部代理 114 和内部管理器 104 之间建立的初始信道启动协议协商和减少。在实施例中，外部代理 114 可以将图 3 所示的外部协议表 134 传送给内部管理器 104。外部协议表 134 可指定外部代理 114 可配置使用哪些协议。在外部协议表 134 被内部管理器 104 接收到时，可以将它与内部协议表 136 相比较，指示出一组可供内部管理器 104 使用的安全协议。外部协议表 134 和内部协议表 134 的任何一个可包括指示，例如 :传输层安全 (TLS)、加密套接字协议层 (SSL)、Kerberos、安全 IP(IPSec) 或其它可用的协议或标准的字段。如图 3 所示，与内部管理器 104 相关联的协商引擎 128 可识别出外部代理 114 和内部管理器 104 相互支持的一个或多个协议。

[0020] 协商引擎 128 在实施例中也可将内部协议表 136 传送到与外部代理 114 相关联的协商引擎 126，用于类似的协议比较。因此，协商引擎 126 和协商引擎 128 可协商相互可用的协议的选择，以建立跨支持安全性的域的安全通信。例如 :如果只有一单个的普通协议既能供外部代理使用，也可供内部管理器 104 使用，114 和内部管理器 104 可能会同意使用一个使用那个协议 (例如 :TLS 或其它协议) 的对话。如果协商引擎 126 和协商引擎 128 同意没有发现共同的协议，终止建立跨域通信的尝试。相反地，如协商引擎 126 和协商引擎 128

识别出多个共有的协议，可以按照网络标准（例如：传送速度、秘钥的位深度或其它安全机构，或其它因素）的选择协议。

[0021] 有了相互兼容的协议，可以在外部代理 114 和内容管理器 104 之间建立安全对话。在实施例中，为了增加安全，外部代理 114 和内容管理器 104 中的每一个可同样地执行认证步骤来验证相对节点的身份、特权等级或其它安全细节。如图 1 所示，这可以用证书或其它安全机构执行。外部代理 114 可通过将证书 108 传送到证书管理机构 110 来认证内部管理器 104。反过来，内部管理器 104 可通过将证书 116 传送到证书管理机构 110 来认证外部代理 114。还可使用其它安全机构。

[0022] 在外部代理 114 和内部管理器 104 之间交换的数据类型和内容在实施例中取决于两个节点间的相互认证。例如：可以为仅指示存取特权的给定等级的内部或外部节点保留对网络管理规则或参数的存取。可以使用其它认证规则或标准。在建立了操作的安全协议且任何认证过程都结束之后，外部代理 114 和内部管理器 104 可以交换数据、应用程序、规则或其它信息。当传输完成后，协商引擎 126 和协商引擎 128 可释放或终止该通信链路。

[0023] 图 4 示出根据本发明的实施例的全部网络协议处理。在步骤 402 中，处理可开始。在步骤 404 中，在外部代理 114、内部管理器 104 或其它客户机、代理或节点的任何一个中生成建立跨支持安全性的网络 102 的安全连接的请求。在步骤 406 中，可以将该建立安全连接的请求传送到接收节点（不论它是内部管理器 104、外部代理 114 或其它客户机、代理或节点），该请求合并了与传送节点兼容的第一协议组。在步骤 408 中，可由接收节点接收该请求。在步骤 410 中，该接收节点（不论它是内部管理器 104、外部代理 114 或其它客户机、代理或节点），都可比较第一协议组和接收节点的第二协议组，以确定是否可以在可用的协议中发现匹配。

[0024] 如在第一协议组和第二协议组之间发现了匹配，则处理进入步骤 412，步骤 412 确定是否发现了一个以上的匹配的协议。如果发现了一个以上的匹配的协议组，处理进入步骤 414，在步骤 414 中，可以按协议标准（例如：传送速度、秘钥的位深度或其它安全机构，或其它因素）选用匹配的协议中的一个。随后处理可进入步骤 416，在步骤 416 中，可以根据选定的协议启动外部代理 114 和内部管理器 104 之间的安全连接或对话。同样地，如果在步骤 412 中仅发现一个匹配的协议，处理进入到步骤 416，在步骤 416 中可以启动一安全连接或对话。例如：在实施例中，可以在 TCP/IP 或其它通信或其它协议下打开指定的端口。

[0025] 在步骤 418 中，可用信号交换和其它根据运用的匹配协议进行的步骤在外部代理 114 和内部管理器 104 之间启动协议专用交换。在步骤 420 中，外部代理 114 和内部管理器 104 中的任一个或它们两个都可通过适当地将相应的证书 116（外部代理 114 的）或证书 108（内部管理器的）传送到证书管理机构 108 来认证相应的其它结点。在实施例中，证书 116 或证书 108 或其它安全数据可以是或包括与 X.509 标准，或其它标准或格式相符的证书对象。当合适的认证完成时，处理进入到步骤 422，在步骤 422 中，可以在外部代理 114 和内部管理器 104 之间进行安全连接或对话。例如：为了系统管理或其它目的，可以在两个节点之间传送网络或其它规则。

[0026] 在完成安全对话时，处理可进入到步骤 424，在步骤 424，可终止或释放外部代理 114 和内部管理器 104 之间的安全连接。在步骤 426 中，处理可终止，重复，返回到前面的处理点或采取其它动作。同样地，如果在步骤 410 的确定中没有识别出匹配的协议，处理可进

入到步骤 426，以终止，重复，返回到前面的处理点或采取其它动作。

[0027] 以上对本发明的描述是示例的，对本技术领域的技术人员来说，可对配置和实施进行修改。例如：尽管本发明是按照单个外部代理 114 描述的，但在实施例中，可以将多个外部代理或节点配置成与在支持安全性的域 102 中的内部管理器 104 或其它客户机或节点自动协商一个匹配的协议。同样地，尽管认证机构通常被描述成由使用 X.509 或其它标准的单个认证实体 110 支持，但在实施例中，也可使用多个认证实体或其它认证或认证平台。可以在实施例中分布其它硬件、软件或其它描述成唯一的资源，并同样在实施例中，可结合描述成分布式的资源。

[0028] 另外，尽管在几次启动安全协议时描述了在支持安全性的域 102 之外的一个或其它节点或代理，将理解任何根据本发明配置的节点和代理，在域的外部或内部，能启动协议处理。同样地，内部和外部代理中的任一个或它们俩都能启动相对代理或节点的认证。因此，本发明的范围仅由以下权利要求书限定。

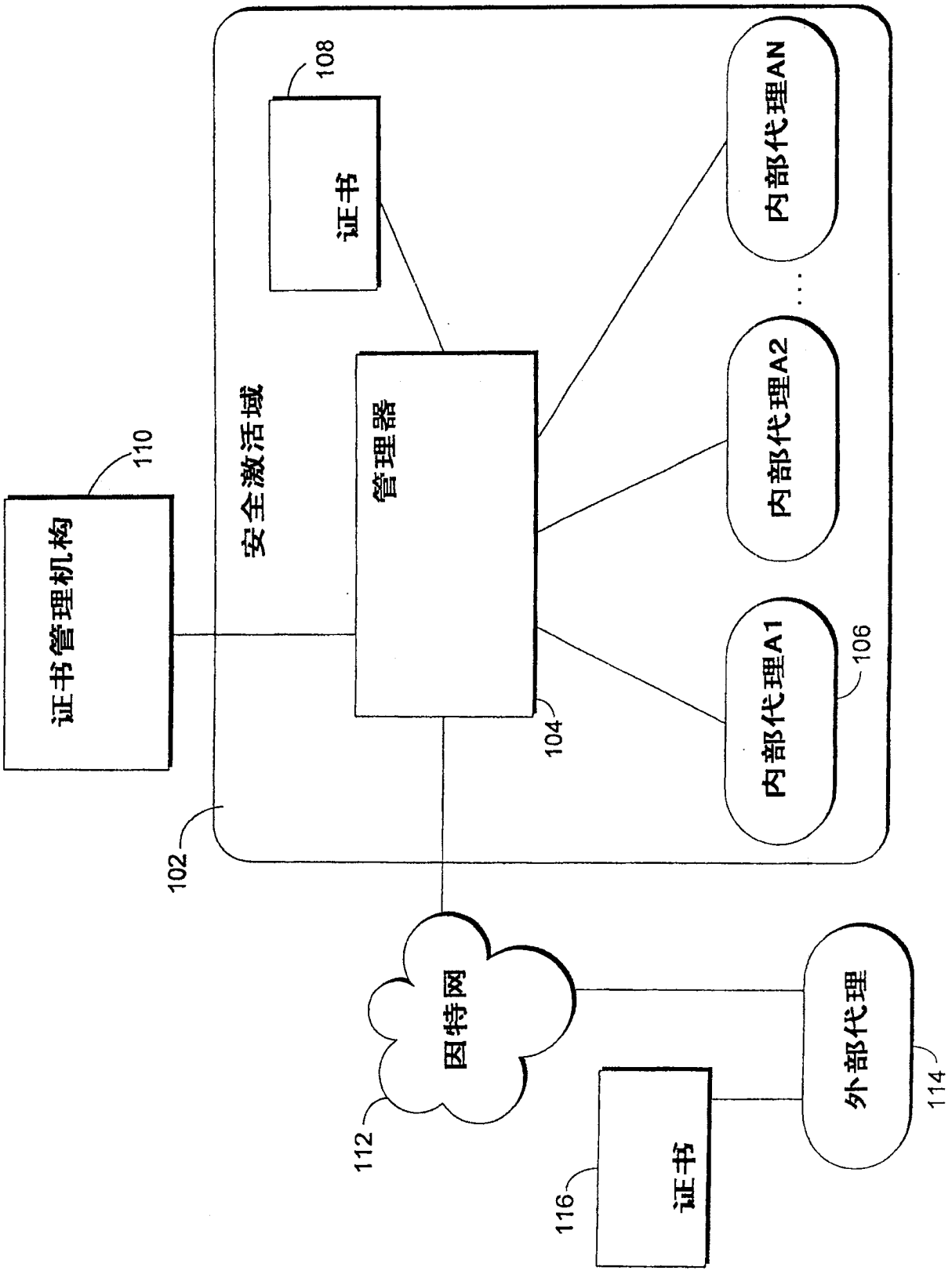

证书管理机构
110
安全激活域
证书
108
管理器
104
内部代理AN
内部代理A2
内部代理A1
106
102
因特网
112
外部代理
114
证书
116

图 1

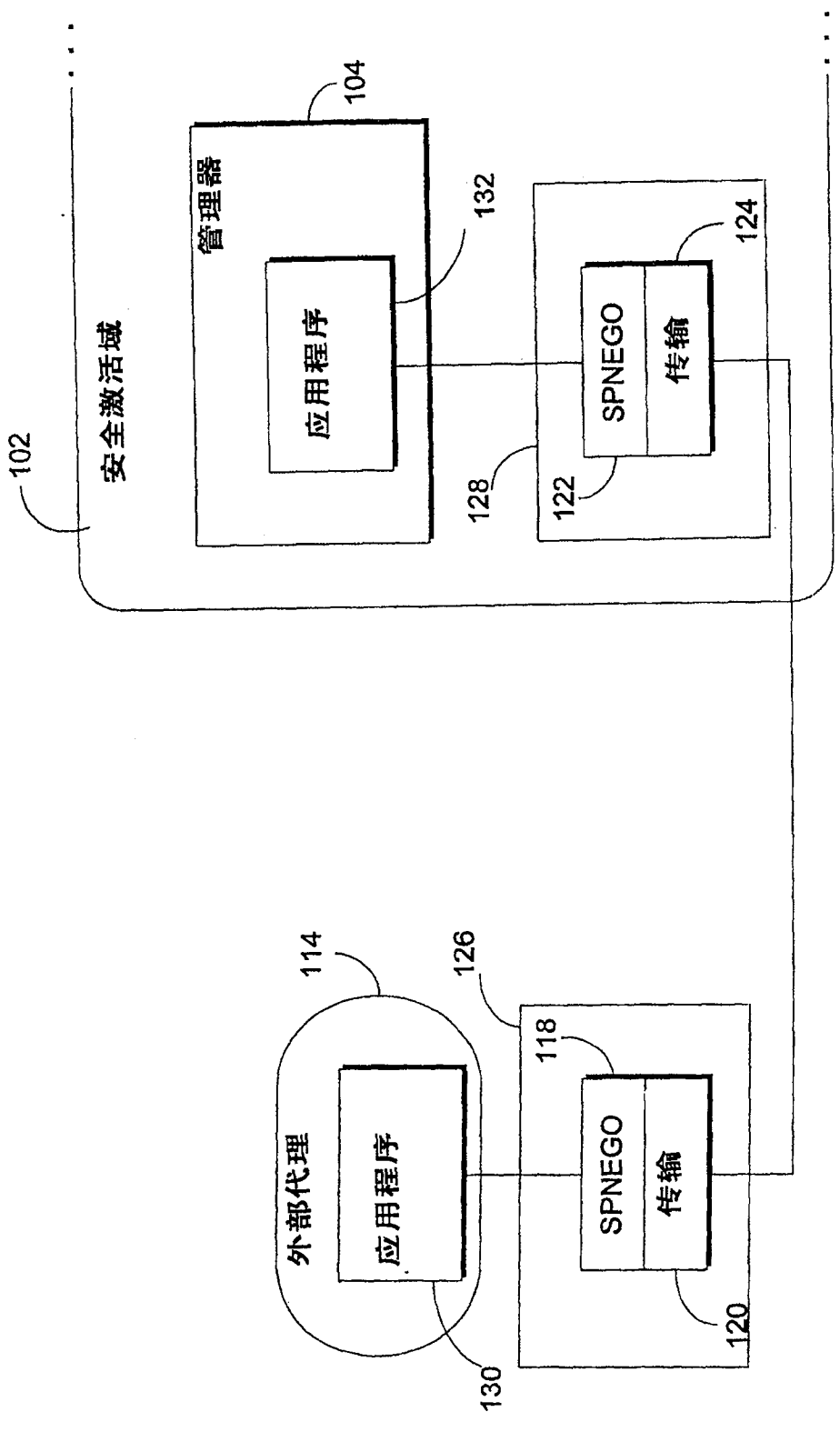

102
安全激活域
管理器
104
应用程序
132
SPNEGO
传输
124
128
122
外部代理
114
应用程序
126
118
SPNEGO
传输
120
130

图 2

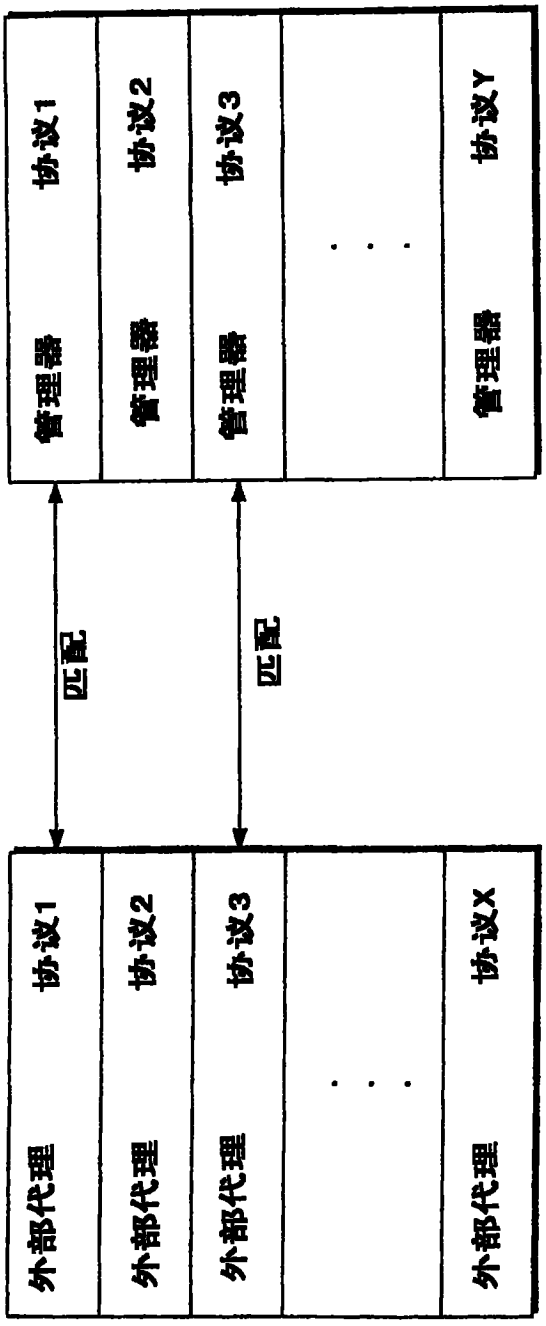

协议1
协议2
协议3
协议Y
管理器
管理器
管理器
管理器
匹配
匹配
协议1
协议2
协议3
协议X
外部代理
外部代理
外部代理
外部代理

图 3

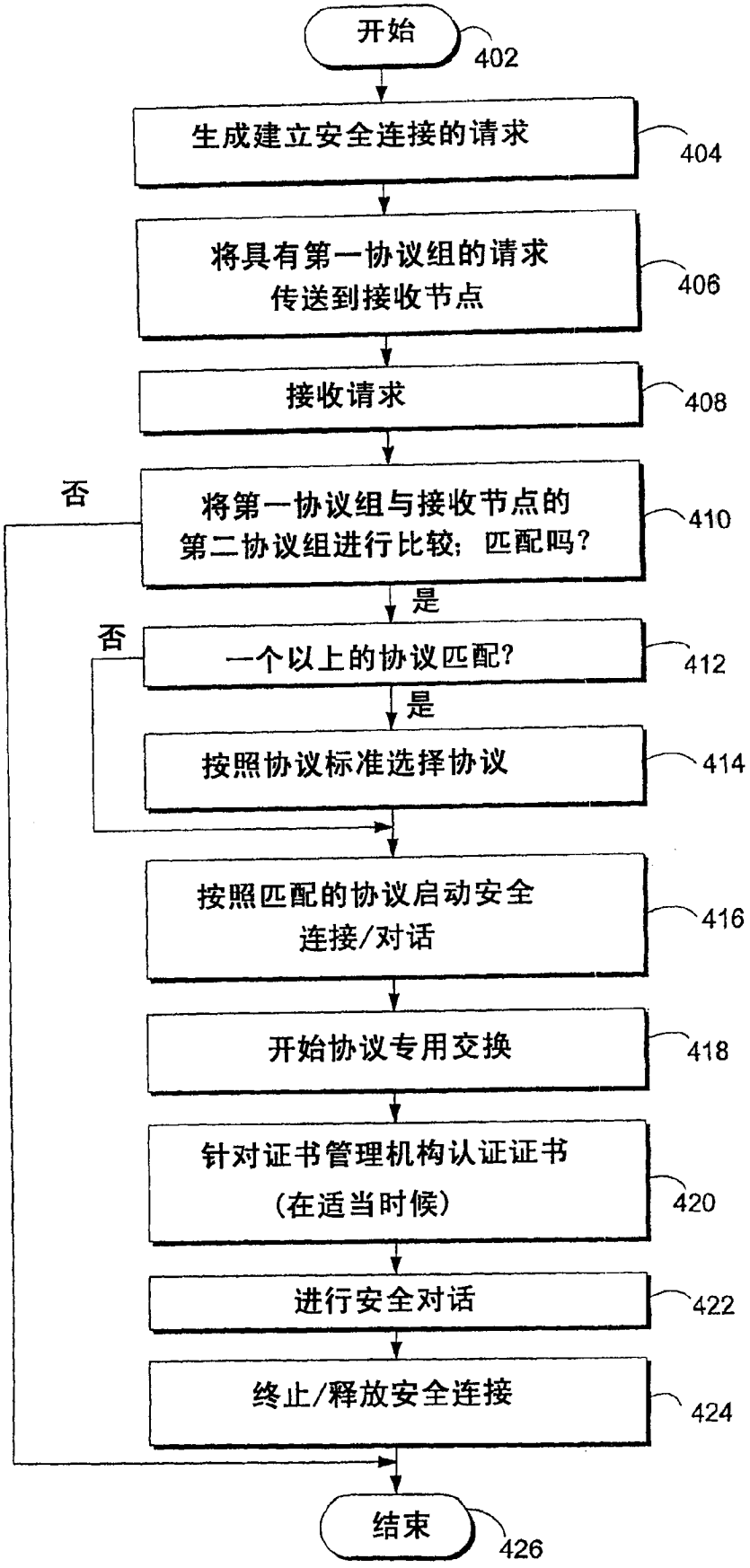

开始
402
生成建立安全连接的请求
404
将具有第一协议组的请求
传送到接收节点
406
接收请求
408
否
将第一协议组与接收节点的
第二协议组进行比较；匹配吗？
410
是
否
一个以上的协议匹配？
412
是
按照协议标准选择协议
414
按照匹配的协议启动安全
连接/对话
416
开始协议专用交换
418
针对证书管理机构认证证书
（在适当时候）
420
进行安全对话
422
终止/释放安全连接
424
结束
426

图 4