(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 101931625 A
(43)申请公布日 2010.12.29

(21)申请号 201010255367.X

(22)申请日 2010.08.13

(71)申请人 杭州迪普科技有限公司
地址 310053 浙江省杭州市滨江区火炬大道581号三维大厦B座9层

(72)发明人 李晶楠 张晓东 杨光 田海燕

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 吴贵明

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 12/24(2006.01)
H04L 12/26(2006.01)

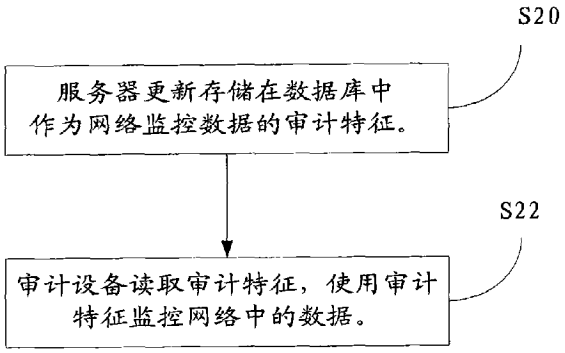
权利要求书 1 页 说明书 5 页 附图 3 页

(54)发明名称

网络监控数据的升级方法和装置

(57)摘要

本发明提供了一种网络监控数据的升级方法和装置，本发明的方法包括：更新存储在数据库中作为所述网络监控数据的审计特征；审计装置读取所述审计特征，监控网络中的数据。本发明还可加密数据库或数据库中的审计特征，防止被修改；在升级过程中备份数据库，如果升级失败，还可恢复并不影响其审计功能。由于将固化在审计装置中的特征库存在可执行修改、升级的数据库中，所以克服了由于修改固化在审计装置内的审计特征，并重新编译版本，升级过程时间较长的问题，节省升级时间，提高审计装置的工作效率。



CN 101931625 A

1. 一种网络监控数据的升级方法，包括数据库和审计装置，其特征在于包括以下步骤：

更新存储在所述数据库中作为所述网络监控数据的审计特征；

通过所述审计装置读取所述审计特征；以及

按照所述审计特征监控网络中的数据。

2. 根据权利要求 1 所述的方法，其特征在于，在所述更新步骤之前备份所述数据库中的所述审计特征。

3. 根据权利要求 2 所述的方法，其特征在于，在所述更新步骤之后将所述数据库加密成审计特征库。

4. 根据权利要求 3 所述的方法，其特征在于，所述读取所述审计特征的步骤包括：

通过所述审计装置解密所述审计特征库成所述数据库；

读取所述数据库中的所述审计特征；以及

如果读取失败，则读取备份的所述数据库的审计特征。

5. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于所述审计装置为路由器、交换机、或代理服务器。

6. 根据权利要求 5 所述的方法，其特征在于所述数据库或所述审计特征库安装在一个服务器中，所述服务器连接至所述审计装置。

7. 一种网络监控数据的升级装置，包括数据库和审计装置，其特征在于包括：

更新模块，用于更新存储在所述数据库中作为所述网络监控数据的审计特征；

获取模块，用于通过所述审计装置获取所述审计特征；以及

监控模块，用于响应所述审计特征监控网络中的数据。

8. 根据权利要求 7 所述的装置，其特征在于还包括备份模块，用于在所述更新模块执行所述更新操作之前，备份所述数据库的审计特征。

9. 根据权利要求 8 所述的装置，其特征在于还包括加密模块，用于在所述更新模块执行所述更新操作之后，将所述数据库加密成审计特征库。

10. 根据权利要求 9 所述的装置，其特征在于所述获取模块包括：

解密模块，用于将所述审计特征库解密成所述数据库；

读取模块，用于读取所述数据库中的所述审计特征；如果读取失败，则读取所述备份模块中备份的所述数据库的所述审计特征；

审计模块，用于通过所述读取模块读取的所述审计特征监控网络中的数据。

11. 根据权利要求 7 至 10 中任一项所述的装置，其特征在于所述审计装置为路由器、交换机、或代理服务器。

网络监控数据的升级方法和装置

技术领域

[0001] 本发明涉及计算机网络技术领域，更具体地，涉及一种网络监控数据的升级方法和装置。

背景技术

[0002] 随着网络的发展，网络信息安全关系着公司的很多方面利益，很多公司对内部计算机访问外部网络有严格的监控。这种监控系统又称为用户行为审计系统。

[0003] 目前，公司内部网络的用户行为审计系统对用户的网络操作进行监视，其基本处理流程是以将应用识别引擎集成在 IPS 内，IPS 为具有审计功能的审计装置，如统一接入网关 (UAG，Unified AccessGateway) 路由器、具备路由功能的交换机等。

[0004] 计算机的报文经过审计装置时，审计装置识别出报文所属的网络协议，在协议识别之后的基础上再对协议载荷进行审计特征识别，协议载荷为此协议的报文所封装的内容数据，如网页、聊天、邮件等数据内容。审计特征为所监控数据的关键词，通过判断出不同的协议后，按照此协议需要监控的关键词，判断协议载荷中是否存在这些关键词，例如，判断报文属于邮件协议或即时消息的协议后，截取里面的收件人邮箱或聊天内容等；判断报文属于 XML 协议后，判断报文中是否含有非法网站地址这类关键词。

[0005] 对于不同的协议报文，对应有不同的审计特征，调用此协议报文相对应的处理函数进行审计，提取报文中的关键词判断是否合法，即判断报文中是否含有与审计特征相同或相近似的关键词，判断出非法的关键词作为审计结果以日志的形式存储到数据库中，也可将审计日志发送到远程主机，远程主机通过解析日志文件将结果显示给管理员。

[0006] 目前的用户行为审计系统所支持业务的审计特征都是固化在审计装置中并预先定义好的，当编译后的系统版本运行在装置上就可以对支持的业务进行审计。当系统版本需要升级，比如要对审计装置中的审计特征进行修改、删除等操作，或是新增审计特征，需要修改审计装置中的平台代码，并重新编译系统版本，将编译后的系统版本更新到审计装置完成升级操作。

[0007] 由于用户需要频繁改变被审计的网络协议和审计业务，审计装置内则需要重新启动、下载新的审计特征，修改固化在内部相应审计特征，并重新编译版本，频繁的重启、升级过程花费较长时间，降低了审计装置的工作效率。

发明内容

[0008] 本发明旨在提供一种网络监控数据的升级方法和装置，其能够解决审计装置升级的过程中，由于修改固化在审计装置内的审计特征，并重新编译版本，重启、升级过程时间较长的问题。

[0009] 根据本发明的一个方面，提供了一种网络监控数据的升级方法，包括更新存储在数据库中作为网络监控数据的审计特征，通过审计装置获取审计特征，按照审计特征监控网络中的数据。

[0010] 进一步地，更新操作之前，还包括备份数据库中的审计特征。

[0011] 进一步地，更新操作之后，还包括将数据库加密成审计特征库。

[0012] 进一步地，通过审计装置获取审计特征的步骤包括将审计特征库解密成数据库并读取数据库中的审计特征；在读取失败的情况下，读取备份的数据库的审计特征。

[0013] 进一步地，数据库或审计特征库安装在一个与审计装置连接的服务器中。

[0014] 根据本发明的另一个方面，还提供一种网络监控数据的升级装置，包括更新模块，用于更新存储在数据库中作为网络监控数据的审计特征；获取模块，用于通过审计装置获取审计特征；以及监控模块，用于响应审计特征监控网络中的数据。

[0015] 进一步地，升级装置还包括备份模块，用于在更新模块执行更新操作之前，备份数据库的审计特征。

[0016] 进一步地，升级装置还包括加密模块，用于在更新模块执行更新操作之后，将数据库加密成审计特征库。

[0017] 进一步地，监控模块包括解密模块，用于将审计特征库解密成数据库；读取模块，用于读取数据库中的审计特征；如果读取失败，则读取备份模块中备份的数据库中的审计特征；以及审计模块，用于通知读取模块读取的审计特征，监控网络中的数据。

[0018] 进一步地，以上所述审计装置为路由器、交换机、或代理服务器。

[0019] 因为本发明采用了将固化在审计装置中的特征库存在可升级并修改的数据库中且不需要编译、重新启动，所以克服了审计装置重启、升级的过程中，由于修改固化在审计装置内的审计特征，并重新编译版本，升级过程时间较长的问题，进而达到了节省升级时间，提高审计装置的工作效率的效果。

附图说明

[0020] 附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0021] 图 1 示出了根据本发明一个实施例的网络装置结构框图；

[0022] 图 2 示出了根据本发明方法的一个实施例的流程图；

[0023] 图 3 示出了根据本发明第二和第三个实施例的网络装置结构框图；

[0024] 图 4 示出了根据本发明方法第二个实施例的流程图；

[0025] 图 5 示出了根据本发明方法第三个实施例的流程图；以及

[0026] 图 6 示出了根据本发明第四个实施例的结构框图。

具体实施方式

[0027] 下面将参考附图并结合实施例，来详细说明本发明。

[0028] 本发明将固化在审计装置 10 中审计特征，以数据库 12 的形式保存，数据库可集成在审计装置 10 中，也可以单独集成在与审计装置 10 连接的服务器 16 中。从而在对审计特征进行升级时，可直接修改数据库 12 中的审计特征，不必修改、编译固化在审计装置 10 内的审计特征，从而节省了时间，提高了审计装置 10 的工作效率。

[0029] 本发明的实现方式有多种形式，下面详细描述各个实施例中审计特征的升级过程。

[0030] 下面结合附图详细说明根据本发明的第一个实施例，该实施例中，存储审计特征的数据库 12 集成在服务器 16 内，如图 1 所示的网络装置的结构示意图，审计装置 10 连接服务器 16，并从服务器 16 中的数据库 12 读取审计特征。审计装置 10 连接远程监控中心的客户端 14，由用户通过客户端 14 修改审计装置 10 的数据库 12 中的审计特征，审计装置 10 连接装置 1 至装置 N，审计各个装置发送或接收到的数据。根据本发明的方法应用在图 1 所示的网络装置中，下面通过本发明所应用的网络环境装置并结合图 2 所示的流程图详细说明实施例一，实施例一包括以下步骤：

[0031] S20：服务器 16 更新存储在数据库 12 中作为网络监控数据的审计特征。

[0032] 优选地，服务器 16 接收管理员输入的修改信息，并根据修改信息来更新存储在数据库 12 中作为网络监控数据的审计特征。管理员可通过服务器 16 连接的远程管理中心的客户端 14，由管理员通过客户端 14 修改数据库 12 中审计特征，这些审计特征包括：需要审计的报文协议，如 TCP/IP 协议报文、XML 协议报文、邮件传输协议报文等，以及每种协议所对应的要审计的关键词，如网址、即时消息、邮件中的收件人等审计特征。在更新操作完成之后，即可实现审计特征的升级，这些审计特征作为后续的监控数据。

[0033] S22：审计装置 10 读取审计特征，使用审计特征监控网络中的数据。

[0034] 审计装置 10 读取数据库 12 中的审计特征，并监控网络中的数据。审计装置 10 可以是路由器、交换机、或代理服务器等，可按照 IP 地址或 MAC 地址监控每个地址所对应审计装置 10 的收发的数据，这些审计装置 10 与审计装置 10 连接，包括装置 1 至装置 N，通过审计装置 10 收发数据，审计装置 10 从收发的数据中监控相应的审计特征，并将监控的审计特征以日志形式发送至连接的远程监控中心的客户端 14，还可以同时保存在存储审计特征的数据库内。

[0035] 上面详细描述了根据本发明的实施例一，在该实施例中，可以通过数据库升级审计特征，审计装置 10 直接读取数据库 12 中更新后的审计特征，并使用读取的审计特征监控数据。由于避免了更新、编译固化在审计装置 10 内的审计特征，可有效节省升级时间，提高审计装置 10 的工作效率。

[0036] 当然，存储审计特征的数据库 12 还可以集成在审计装置 10 内部，如图 3 所示，用户通过审计装置 10 连接的 I/O 装置 20 对数据库中的审计特征进行修改。为便于审计特征不被任意修改、或泄密，还可对审计特征进行加密，并使用加密后的审计特征进行升级。下面通过图 4 所示的第二个实施例说明此流程，该流程包括以下步骤：

[0037] S40：审计装置 10 对审计特征或数据库进行加密。审计装置 10 加密用于升级的审计特征或存储审计特征的数据库，加密后的数据库 12 也可定义为审计特征库 18。

[0038] S42：更新审计装置 10 内的审计特征库 18。用户可通过外部存储器连接审计装置 10，如 U 盘或读卡器等，由审计装置 10 自动更新连接的 U 盘或读卡器中存储卡的审计特征库 18，或通过审计装置 10 连接的 I/O 装置 20，修改审计特征库 18 内的审计特征。

[0039] S44：审计装置 10 解密审计特征库 18，读取解密后的数据库 12 中的审计特征。在审计装置 10 更新审计特征库 18 以后，解密审计特征库 18，恢复数据库 12，读取数据库 12 中的审计特征。

[0040] S46：审计装置 10 使用读取的审计特征，监控网络中的数据。在上述第二实施例中，通过加密审计特征或数据库 12，在升级的同时，还可有效防止审计特征随意被改动，避

免被修改的审计特征导致审计装置 10 监控失效。

[0041] 在审计特征升级的过程中，如果将数据库 12 或审计特征库 18 直接覆盖升级前的数据库 12 或审计特征库 18，有时会出现升级失败的情况，从而导致升级后的审计装置 10 无法实现审计功能，为避免这种情况，可在升级操作前，备份数据库 12 或审计特征库 18，下面通过实施例三说明，参见图 5 和图 3，其包括以下步骤：

[0042] S500：审计装置 10 执行审计功能。审计装置 10 响应审计特征对网络中的数据进行审计。

[0043] S502：为审计装置 10 选择用于升级的审计特征库 18。用户通过审计装置 10 连接的 I/O 装置 20 为审计装置 10 选择用于升级的审计特征库 18。

[0044] S504：审计装置 10 停止当前的审计功能。

[0045] S506：审计装置 10 备份当前的审计特征库 18。在审计装置 10 停止操作后，审计装置 10 备份当前使用的审计特征库 18 或数据库 12。

[0046] S508：审计装置 10 更新审计特征库 18。审计装置 10 按照 S502 选择的审计特征库 18 更新。当然，如果审计特征存储在第一实施例中与审计装置 10 连接的服务器 16 上，可由服务器 16 升级审计特征库 18 或数据库 12，

[0047] S510：审计装置 10 读取审计特征库 18 并解密，恢复数据库 12。

[0048] S512：审计装置 10 获得数据库 12 中的审计特征，并判断是否可用，如果是，则执行 S500，审计装置 10 按照审计特征对网络中的数据进行审计。如果否，则执行 S514。

[0049] S514：审计装置 10 还原备份的审计特征库 18，并执行 S508。

[0050] 经过上述的步骤，当审计装置 10 在升级过程中，如果出现了升级失败的情况，可选择备份的审计特征库 18 或数据库 12 继续使用。从而即使出现因升级失败导致的审计装置 10 失效，审计装置 10 还可恢复并继续使用。

[0051] 在上述的实施例三中，审计装置 10 还可能初始化，如执行 S506a，在 S506a 的步骤之后，执行 S508 等步骤以执行审计操作。

[0052] 上面详细说明了根据本发明方法的实施例，根据本发明的方法可以采用各种装置的形式集成在审计装置 10 中，如集成在代理服务器、路由器、交换机、网关等装置中，还可集成在与审计装置 10 连接的服务器 16 中，均不影响本发明的实现。下面通过实施例四描述根据本发明的优选升级装置，参见图 6，该升级装置包括更新模块 60，用于更新存储在数据库 12 中作为网络监控数据的审计特征；监控模块 62，用于控制审计装置 10 读取审计特征，并响应审计特征监控网络中的数据。

[0053] 优选地，该升级装置还包括备份模块 64，用于在更新模块 60 执行更新操作之前，响应相连接的更新模块 60，备份数据库 12 的审计特征。以便于后续的恢复过程中，由连接的读取模块 622 读取备份模块 64 中的备份的数据库 12 的审计特征。

[0054] 优选地，该升级装置还包括加密模块 66，用于在所述更新模块 60 执行所述更新操作之后，响应更新模块 60，将数据库 12 加密成审计特征库 18。

[0055] 优选地，监控模块 62 包括解密模块 620，用于将所述审计特征库 18 解密成数据库 12；读取模块 622，用于读取解密模块 620 所解密出的数据库 12 中的审计特征；如果读取失败，则读取备份模块 64 中备份的数据库 12 的审计特征；审计模块 624，用于通知读取模块 622 读取的审计特征，监控网络中的数据。

[0056] 优选地，所述审计装置 10 为路由器、交换机、或代理服务器。本发明的装置可集成在审计装置 10 内部，也可集成在存储器中，可插拔连接审计装置 10，便于用户使用。

[0057] 本发明的技术效果在于，因为本发明采用了将固化在审计装置中的审计特征库存在可升级并修改的数据库中、且不需要编译，所以克服了审计装置升级的过程中，由于修改固化在审计装置内的审计特征，并重新编译版本，升级过程时间较长的问题，进而达到了节省升级时间，提高审计装置的工作效率的效果。

[0058] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0059] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

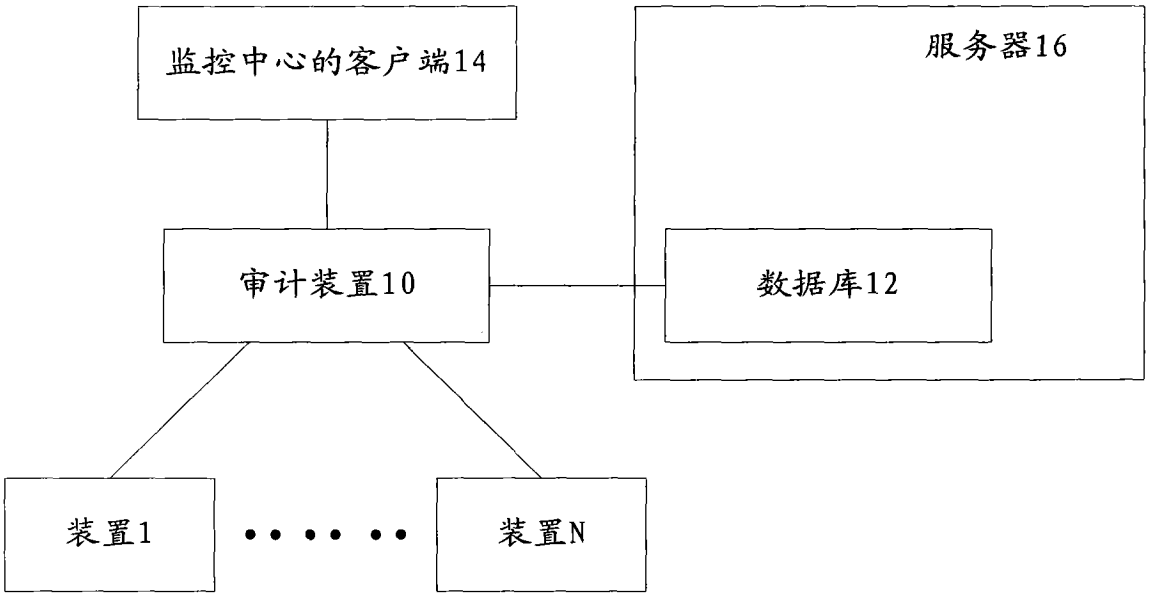

监控中心的客户端14
服务器16
审计装置10
数据库12
装置1
装置N

图 1

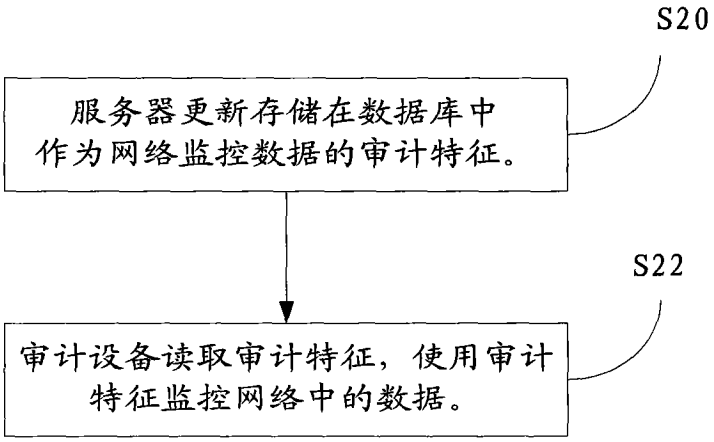

S20
服务器更新存储在数据库中
作为网络监控数据的审计特征。
S22
审计设备读取审计特征，使用审计
特征监控网络中的数据。

图 2

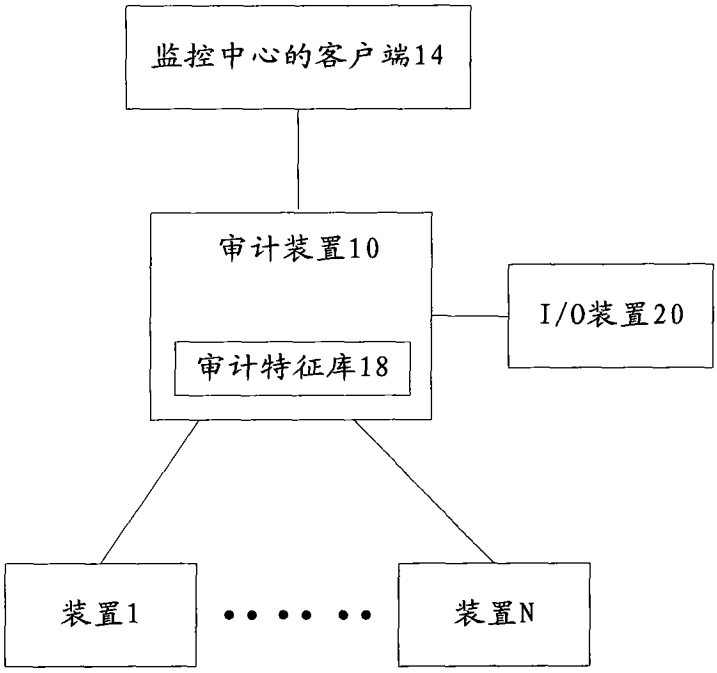

监控中心的客户端14
审计装置10
审计特征库18
I/O装置20
装置1
装置N

图 3

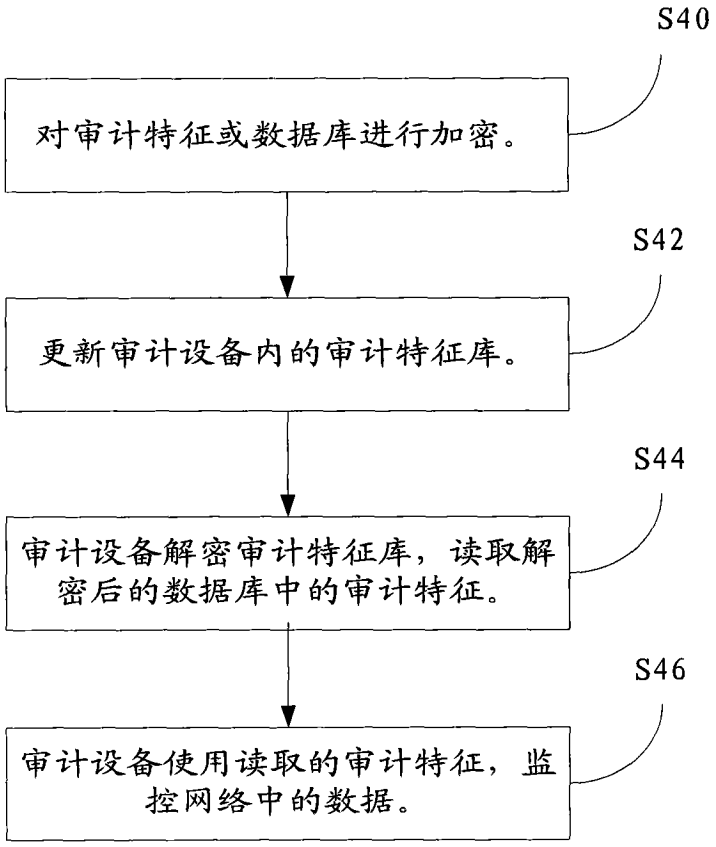

S40
对审计特征或数据库进行加密。
S42
更新审计设备内的审计特征库。
S44
审计设备解密审计特征库，读取解密后的数据库中的审计特征。
S46
审计设备使用读取的审计特征，监控网络中的数据。

图 4

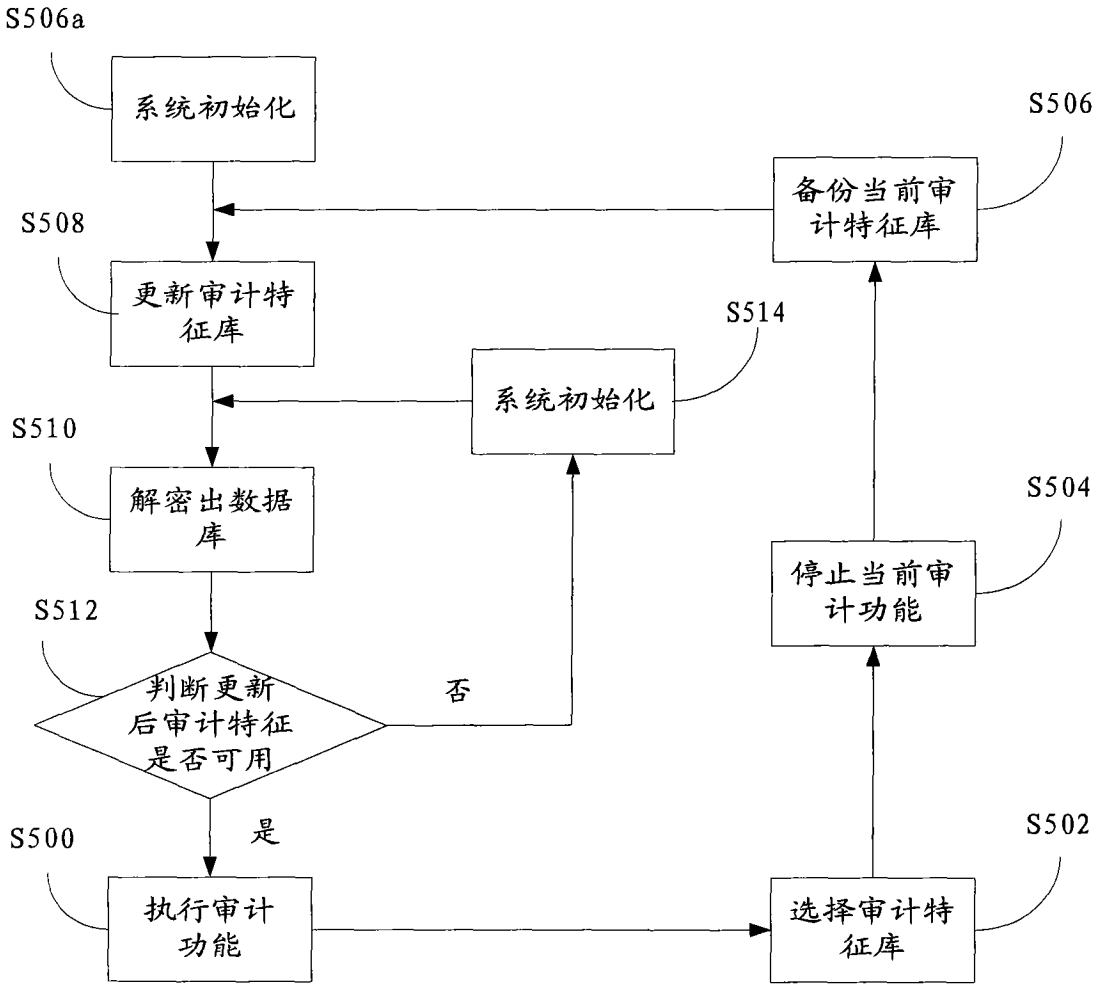

S506a
系统初始化
S506
备份当前审计特征库
S508
更新审计特征库
S514
系统初始化
S510
解密出数据库
S504
停止当前审计功能
S512
判断更新后审计特征是否可用
否
S500
是
S502
执行审计功能
选择审计特征库

图 5

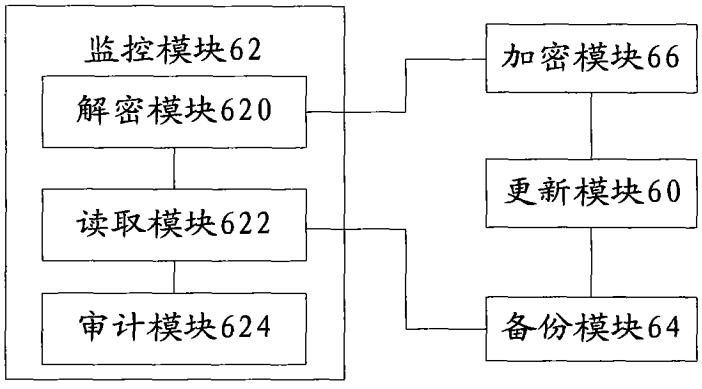

监控模块62
解密模块620
读取模块622
审计模块624
加密模块66
更新模块60
备份模块64

图 6