(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 7 月 31 日 (31.07.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/114232 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2014/071101

(22) 国际申请日: 2014 年 1 月 22 日 (22.01.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310023542.6 2013 年 1 月 22 日 (22.01.2013) CN

(71) 申请人: **横河电机株式会社 (YOKOGAWA ELECTRIC CORPORATION)** [JP/JP]; 日本东京都武藏野市中町 2 丁目 9 番地 32 号, Tokyo 180-8750 (JP)。

(72) 发明人; 及
(71) 申请人 (仅对加纳): **杨磊 (YANG, Lei)** [CN/JP]; 日本东京都武藏野市中町 2 丁目 9 番地 32 号, Tokyo 180-8750 (JP)。

(72) 发明人: **杨剑楠 (YANG, Jiannan)**; 日本东京都武藏野市中町 2 丁目 9 番地 32 号, Tokyo 180-8750 (JP)。
赵岳云 (ZHAO, Yueyun); 日本东京都武藏野市中町 2 丁目 9 番地 32 号, Tokyo 180-8750 (JP)。

(74) 代理人: **北京天昊联合知识产权代理有限公司 (TEE&HOWE INTELLECTUAL PROPERTY ATTORNEYS)**; 中国北京市东城区建国门内大街 28 号民生金融中心 D 座 10 层陈源, Beijing 100005 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: ISOLATION PROTECTION SYSTEM AND METHOD THEREOF FOR PERFORMING BIDIRECTIONAL DATA PACKET FILTRATION INSPECTION

(54) **发明名称** : 隔离保护系统及其执行双向数据包过滤检查的方法

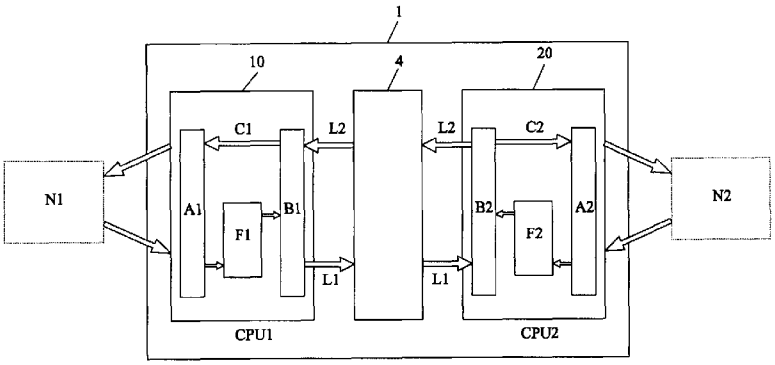

图 2 /Fig.2

(57) **Abstract**: Disclosed are an isolation protection system and a method thereof for performing bidirectional data packet filtration inspection. The isolation protection system is arranged in a communication line to subject the communication facilities of two communication parties to isolation protection, and comprises: a first protective device and a second protective device, which are used for respectively connecting to the communication facility of one of the communication parties; and a bidirectional data transmission module, which is arranged between the first protective device and the second protective device, and is used for connecting the first protective device and the second protective device, transmitting data output by the first protective device to the second protective device according to a proprietary communication protocol, and transmitting data output by the second protective device to the first protective device. The system is characterized in that: the first protective device and the second protective device have completely independent hardware structures and respectively operate in independent central processing units.

(57) **摘要**:

[见续页]

WO 2014/114232 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种隔离保护系统及其执行双向数据包过滤检查的方法，该隔离保护系统设置在通信线路中对通信双方的通信设施进行隔离保护，它包括：第一保护装置和第二保护装置，用于分别与所述通信方之一的通信设施连接；双向数据传输模块，设置在所述第一保护装置和所述第二保护装置之间，用于连接所述第一保护装置和所述第二保护装置，而且根据专有通信协议将所述第一保护装置输出的数据传送到所述第二保护装置，以及将所述第二保护装置输出的数据传送到所述第一保护装置；其特征在于：所述第一保护装置和所述第二保护装置具有完全独立的硬件结构并分别运行于独立的中央处理器。

隔离保护系统及其执行双向数据包过滤检查的方法

技术领域

本发明涉使用在通信线路上的隔离保护系统及其执行双向数据包过滤检查的方法，设置在通信路径中（例如通信网络之间、网关路径中以及不同的通信终端之间），实现网络安全保障、通信双方的设施的隔离保护、及其双向数据包过滤检查。尤其适用于工业现场的信息网络和控制网络。

背景技术

现有工业现场的信息网络和控制网络之间部署的安全性产品多采用防火墙或者网关产品。

现有防火墙技术存在的不足是对工业通信协议支持不够充分。例如工业现场应用 OPC 工业协议时，需要使用 1024 到 65535 的动态端口，所以防火墙必须开放上述范围内的所有端口，这样做显著增加了网络的安全性风险。另外，防火墙实现了 IP 层的读取控制，但是不支持对数据的读取控制。防火墙支持对一般网络的数据链路层、网络层、传输层进行检查，但是对应用层的检查功能存在一定的不足，尤其是对工业协议的检查功能有所欠缺。

网关技术首先从控制系统网络的服务器采集数据，网关代理了控制系统网络的服务器的功能，MES/ERP 层的客户端再通过网关采集数据，以此达到防护控制系统网络的服务器的目的。网关技术存在的不足在于网关产品有自己的 IP 地址，即使已经配置好的控制系统网络，其 MES/ERP 层的客户端仍然需要重新设定（更改服务器的 IP 以及服务器名等、注册网关服务器）。另外，网关的防火墙功能不足，由于网关产品有 IP 地址，可能会被攻击。当网关产品被入侵时，控制系统中设备的风险增加了。

作为保护网络安全、尤其是保护工业现场应用网络的现有技术可以参见例如中国专利公开 CN101014048（申请日 2007 年 02 月 12、申请号 200710063822.4、发明名称：分布式防火墙系统及实现防火墙内容检测的方法），以及多芬诺（TOFINO）工业网络安全保护技术（可通过链接

http://www.doc88.com/p-649582721525.html 来查看）。上述已有技术作为背景技术结合在本申请中作为参考。

可以将上述的已有技术用图 1 的框图来概括：在通信的双方（N1，N2）的通信线路中设置有安全防护装置 100，其中的过滤模块 F0 对于“来往”的数据包进行过滤。上述已有技术的缺陷在于，现有技术中的防火墙安全过滤检查模块都运行于单个中央处理器（CPU）上。在这种情况下，当防火墙在从一通信方向另一通信方传输数据时被攻击，则由于整个防火墙运行于单个中央处理器上，则整个安全防火墙将被损坏而无法使用。而且，上述已有技术中的安全防火墙技术并不对于数据包进行深度检查，例如对包体内容的深度检查，从而使得深入隐藏在包体内的病毒数据有可能破坏通信设施（N1，N2）的操作。

发明内容

本发明所要解决的技术问题是提供一种设置在通信线路中对通信双方的通信设施进行隔离保护的隔离保护系统及其执行双向数据包过滤检查的方法，该隔离保护系统集成有分别针对通信双方的运行于独立的中央处理器上的两个保护装置以及按照专有通信协议在两个保护装置之间进行双向数据通信的一个双向数据传输模块，以在确保在通信双方之间的数据包传输的安全性的同时避免由于针对一通信方的中央处理器受到攻击而被破坏时整个隔离保护系统都受到损坏而无法使用。

为此，本发明提供了一种隔离保护系统，设置在通信线路中对通信双方的通信设施进行隔离保护，它包括：

第一保护装置和第二保护装置，用于分别与所述通信方之一的通信设施连接；

双向数据传输模块，设置在所述第一保护装置和所述第二保护装置之间，用于连接所述第一保护装置和所述第二保护装置，而且根据专有通信协议将所述第一保护装置输出的数据传送到所述第二保护装置，以及将所述第二保护装置输出的数据传送到所述第一保护装置；其特征在于：

所述第一保护装置和所述第二保护装置具有完全独立的硬件结构并分别运行于独立的中央处理器，其中所述第一保护装置和所述第二保护装

置的每一个包括：

第一接口，用于分别从所连接的通信方的通信设施接收数据流的数据包并将来自另一通信方的数据输出到所连接的通信设施；

过滤模块，用于对从所述第一接口接收的数据流执行过滤检查，并输出符合安全性要求的数据；

第二接口，用于接收所述的符合安全性要求的数据，并将该符合安全性要求的数据传送到所述双向数据传输模块；以及

传输通道，用于将来自所述第二接口的数据传送到所述第一接口。

本发明的上述隔离保护系统采用了本发明的“2+1”的结构，即采用了包括具有完全独立的硬件结构并分别运行于独立的中央处理器的第一保护装置和第二保护装置以及连接在第一保护装置和第二保护装置之间使通信双方根据专有通信协议进行通信的双向数据传输模块的结构，来在通信双方之间实现安全的双向数据通信。由于两个保护装置运行于独立的中央处理器上，因此当其中的一个保护装置受到攻击或者物理损坏时，另一个保护装置不会受其影响；由于构成隔离保护系统的两个保护装置运行于独立的中央处理器上，因此在硬件实现上可以以分立的方式构建每个保护装置，这样当其中一个保护装置受到攻击或者物理损坏时，可以方便地进行替换和有针对性地修复和维护；另外，由于构成隔离保护系统的两个保护装置的硬件结构完全独立，因此在制造上可以分开制造硬件结构完全独立控制的保护装置，然后根据各保护装置所连接的通信方或目的通信方的安全性需求对其硬件结构进行程序化，与现有技术中的运行于单个中央处理器上的防火墙安全过滤检查模块相比，本发明的这种配置可以在整体上简化硬件制造工艺的同时，提供对于通信双方设施的分别保护。另外，根据本发明的隔离保护系统中所包括的设置于两个保护装置之间的双向数据通信模块按照专有通信协议在针对通信双方的两个保护装置之间架构通信链路，也就是说，通过了一个保护装置的数据流的数据包必须满足专有通信协议才能够进入另一个保护装置，因此双向数据传输模块在两个保护装置之间（也就是在通信双方之间）设置了另一道保护屏障。由于根据本发明的隔离保护系统是通过保护装置中的过滤模块和双向数据传输模块在通信双方之间实现安全的双向数据传输，因此本发明的隔离保护系

统克服了现有网关技术中存在的网关产品必须有自己的 IP 地址的问题，也就是说，在通信双方采用根据本发明的隔离保护系统建立通信时，不需要对已经配置好的各个网络端进行重新设置，这样，由于没有 IP 地址，被攻击的可能性得到了进一步降低。

其中，所述的通信方的通信设施可以是计算机、服务器或其它网络信息的输入/输出装置。

优选地，所述数据过滤模块可以包括分别用于对传输的数据流的数据包执行基本防火墙检查的内置防火墙模块和用于执行数据包深度过滤的数据包过滤模块。

其中，所述内置防火墙模块可以对数据流的数据包执行包头内容检查，而所述数据包过滤模块可以对数据流的数据包执行包体内容检查。

其中，所述包头内容涉及 IP 地址、MAC 地址、协议类型信息、端口信息，而所述包体内容涉及通信目标、通信源、通信目的、通信类型和通信内容。

本发明的隔离保护系统的每个保护装置中包括的内置防火墙模块和数据包过滤模块对流经的数据流的数据包先后进行两道过滤检查，其中内置防火墙模块对所流经的数据流的数据包的包头执行基本防火墙检查，而数据包过滤模块对数据流的数据包执行数据包深度过滤检查。进一步地，执行基本防火墙检查可以包括对数据流的数据包执行包头内容检查，而对数据流的数据包执行数据包深度过滤检查可以包括对数据流的数据包执行包体内容检查。在一个保护装置内相继对数据包进行两道过滤处理，确保了流经的数据包的安全性。另外，由于在两个保护装置之间还设置了双向数据传输模块，该双向数据传输模块根据专有通信协议在两个保护装置之间进行进一步的防护。因此，即使在一个保护装置中通过了内置防火墙模块和数据包过滤模块所进行的两道过滤检查处理的不安全数据包在不满足专有通信协议的情况下也无法通过双向数据传输模块而进入另一个保护装置，换句话说，通过了内置防火墙模块和数据包过滤模块之后，不安全数据包的进一步传输也会被双向数据通信模块阻断，这进一步增加了通信双方数据传输的安全性。

优选地，所述数据包过滤模块中分别内置有支持工业通信协议的过

滤列表。

在本发明的隔离保护系统中，由于各个保护装置中的数据包过滤模块能够检查工业协议的应用数据，因此本发明的网络隔离保护系统能够充分支持工业通信协议，增强了对应用层的检查功能，能够容易地应用于工业现场信息网络和控制网络之间。

本发明还提供了采用上述隔离保护系统执行双向数据包过滤检查的方法，其特征在于包括步骤：

在通信线路中设置具有完全独立的硬件结构并且分别运行于独立的中央处理器的第一保护装置和第二保护装置分别用于通信双方的通信设施；以及

利用设置在第一保护装置和第二保护装置中的过滤模块对传输的数据流的数据包执行过滤检查。

其中，所述的过滤检查包括：

对传输的数据流的数据包执行基本防火墙检查，以及

对传输的数据流的数据包执行深度过滤。

其中，所述对传输的数据流的数据包执行基本防火墙检查包括对数据流的数据包执行包头内容检查，而所述对传输的数据流的数据包执行深度过滤包括对数据流的数据包执行包体内容检查。

其中，所述包头内容涉及 IP 地址、MAC 地址、协议类型信息、端口信息，而所述包体内容涉及通信目标、通信源、通信目的、通信类型和通信内容。

根据本发明的设置在通信线路中对通信双方的通信设施进行隔离保护的隔离保护系统及其执行双向数据包过滤检查的方法，不仅能够通过保护装置中的内置防火墙模块在数据链路层、网络层、传输层上对数据包进行过滤检查以及能够通过保护装置中的数据包过滤模块对数据包进行深度过滤检查来在通信双方之间建立双向数据通信，从而使得本发明的隔离保护系统及其执行双向数据包过滤检查的方法能够实现通信双方的双向数据传输的安全性；而且由于根据本发明的隔离保护系统所包括的针对通信双方的第一保护装置和第二保护装置运行于彼此独立的中央处理器上，因此当其中的一个保护装置受到攻击或者物理损坏时，另一个保护装置不

会受其影响。

附图说明

通过结合附图的以下描述，将会更容易地理解本发明并且更容易地理解其伴随的优点和特征，其中：

图 1 示出了现有技术的安全防火墙产品的原理示意图；

图 2 示出了根据本发明的第一实施例的隔离保护系统的框图；

图 3 示出了根据本发明的第二实施例的隔离保护系统的框图；

图 4 示出了利用根据本发明的第二实施例的隔离保护系统从客户端向服务器端传输数据时所执行的数据包过滤检查的方法的流程图；以及

图 5 示出了利用根据本发明的第二实施例的隔离保护系统从服务端向客户端传输数据时所执行的数据包过滤检查的方法的流程图。

具体实施方式

为了使本发明的内容更加清楚和易于理解，下面结合附图对本发明的具体实施例进行详细描述。在本发明中，以示例方式，对本发明提出的隔离保护系统及其执行双向数据包过滤检查的方法进行了说明，但是本发明不限于所公开的优选实施例的具体形式。所属领域的技术人员可以根据本发明公开的内容对本发明进行修改和变型，这些修改和变型也应当属于由权利要求限定的本发明保护的范围。

本发明针对现有工业现场的信息网络和控制网络之间部署的安全性产品多采用防火墙或者网关产品以及现有技术中只能通过运行于单个中央处理器上的防火墙产品来实现双向数据传输的安全性的问题，提出了一种隔离保护系统及其执行双向数据包过滤检查的方法。为了在通信双方之间实现安全的双向数据传输，本发明所提供的设置在通信线路中对通信双方的通信设施进行隔离保护的隔离保护系统采用了本发明的“2+1”结构（即，针对通信双方的分别运行于彼此独立的两个中央处理器上的两个保护装置和连接在两个保护装置之间利用专有通信协议控制两个保护装置之间数据传输的一个双向数据传输模块）来在通信双方之间建立安全的双向数据传输。其中，针对通信双方的两个保护装置分别运行于独立的中央

处理器上，因此当针对一通信方的保护装置受到攻击或者物理损坏时，针对另一通信方的保护装置不会受其影响；由于构成隔离保护系统的两个保护装置运行于独立的中央处理器上，因此在硬件实现上可以以分立的方式构建每个保护装置，这样当其中一个保护装置受到攻击或者物理损坏时，可以方便地进行拆卸替换；另外，由于构成隔离保护系统的两个保护装置的硬件结构完全独立，因此在硬件实现上可以分开制造硬件结构完全独立控制的保护装置，然后根据各保护装置所连接的通信方或目的通信方的安全性需求对其硬件结构进行程序化（这其中主要涉及对通信协议的配置），与现有技术中的运行于单个中央处理器上的防火墙安全过滤检查模块相比，本发明的这种配置可以在整体上简化硬件制造工艺的同时，提供对于通信双方设施的分别保护。另外，隔离保护系统中的双向数据通信模块利用专有通信协议在针对通信双方的两个保护装置之间架构通信链路，也就是说，通过了一个保护装置的数据流必须满足专有通信协议才能够进入另一个保护装置，因此双向数据传输模块在两个保护装置之间（也就是在通信双方之间）设置了另一道保护屏障。这同时也克服了现有网关技术中存在的网关产品必须有自己的 IP 地址的问题，也就是说，在网络之间采用根据本发明的隔离保护系统建立数据通信时，不需要对已经配置好的各个网络端进行重新设置，这样，由于没有 IP 地址，被攻击的可能性得到了进一步降低。

下面参照附图对本发明的隔离保护系统进行描述。

图 2 示出了根据本发明的第一实施例的隔离保护系统 1 的框图。根据本发明的隔离保护系统 1 可以设置在第一通信方 N1 和第二通信方 N2 之间，以在第一通信方 N1 和第二通信方 N2 之间实现安全的双向数据通信。其中，第一通信方 N1 和第二通信方 N2 的通信设施可以是计算机、服务器或其它网络信息的输入/输出装置。如图 2 所示，隔离保护系统 1 可以包括第一保护装置 10、第二保护装置 20 和双向数据传输模块 4，即本发明的“2+1”结构。第一保护装置 10 和第二保护装置 20 通过双向数据传输模块 4 进行双向数据通信。双向数据传输模块 4 中内置有专有通信协议，其可以为专有通信协议硬件或者专有通信协议软件或二者结合，用以在第一保护装置 10 和第二保护装置 20 之间建立安全的屏障，使得符合

该专有通信协议的数据包通过，而不符合该专有通信协议的数据包被拦截阻断，从而可以确保第一保护装置 10 和第二保护装置 20 之间的安全的数据交互。

如图 2 所示，第一保护装置 10 包括与第一通信方 N1 进行双向数据通信的第一接口 A1 以及与双线数据通信模块 4 进行双向通信的第二接口 B1。在第一保护装置 10 中还包括过滤模块 F1 和将来自第二接口 B1 的数据包传送到第一接口 A1 的传输通道 C1。过滤模块 F1 设置在第一接口 A1 和第二接口 B1 之间，用于对从第一接口 A1 接收到的要从第一通信方 N1 传输到第二通信方 N2 的数据包执行过滤检查，并且将符合该过滤模块 F1 内置的作为安全性要求的通信协议的数据包输出到第二接口 B1。第二接口 B1 将通过了过滤模块 F1 的过滤检查的数据包输出到双向数据传输模块 4，而双向数据传输模块 4 根据专有通信协议将第一保护装置 10 通过第二接口 A2 输出的数据传送到第二保护装置 20。

第二保护装置 20 在硬件结构上与第一保护装置 10 完全独立。第二保护装置 20 包括与第二通信方 N2 进行双向数据通信的第一接口 A2 以及与双线数据通信模块 4 进行双向通信的第二接口 B2。在第二保护装置 20 中还包括过滤模块 F2 和将来自第二接口 B2 的数据包传送到第一接口 A2 的传输通道 C2。过滤模块 F2 设置在第一接口 A2 和第二接口 B2 之间，用于对从第一接口 A2 接收到的要从第二通信方 N2 传输到第一通信方 N1 的数据包执行过滤检查，并且将符合该过滤模块 F2 内置的作为安全性要求的通信协议的数据包输出到第二接口 B2。第二接口 B2 将通过了过滤模块 F2 的过滤检查的数据包输出到双向数据传输模块 4，而双向数据传输模块 4 根据专有通信协议将第二保护装置 20 通过第二接口 B2 输出的数据包传送到第一保护装置 10。

根据本发明的隔离保护系统 1 中的第一保护装置 10 和第二保护装置 20 分别运行于彼此独立（即，独立进行操作和运算）的中央处理器 CPU1 和中央处理器 CPU2 上，其中，每个中央处理器对应一个内存。这样的构造确保了当其中一台中央处理器受到病毒侵害或者物理损坏时，另一台中央处理器不会受到影响。这两个独立运行于各自中央处理器上的第一保护装置 10 和第二保护装置 20 按照专有通信协议通过双向数据传输模块 4 进

行双向数据传输。

从以上可以看出，根据本发明的第一实施例的隔离保护系统 1 利用其所包括的运行于独立的中央处理器上的保护装置中所设置的过滤模块和两个保护装置之间设置的双向数据传输模块在通信双方进行数据传输，因此利用根据本发明的第一实施例的隔离保护系统 1 在网络之间交互数据时，不需要如现有网关产品一样，要对客户端和服务器端的 IP 地址进行设置，因此对已有网络无任何影响。

由于根据本发明的隔离保护系统 1 的安全策略是通过对保护装置所包括的过滤模块进行设置来实现的，因此可以根据通信双方的安全性需求设置适当的安全策略。

利用根据本发明的第一实施例的隔离保护系统 1，当要从第一通信方 N1 向第二通信方 N2 传输数据包时，数据包流向如图 2 中的路径 L1 所示。具体地讲，来自第一通信方 N1 的数据由第一保护装置 10 的第一接口 A1 进入第一保护装置 10；在第一保护装置 10 内部，该数据包通过过滤模块 F1 进行过滤检查；符合安全性要求的数据包通过过滤模块 F1，并且经由第一保护装置 10 的第二接口 A2 进入双向数据传输模块 4；如果该数据包不符合双向数据传输模块 4 内置的专有通信协议，则数据包将被阻断而无法进入第二保护装置 20，如果该数据包符合专有通信协议，则其可以通过中间通信模块 4 进入第二保护装置 20；在第二保护装置 20 内部，该数据包由第二接口 B2 通过传输通道 C2 直接传输到第一接口 A2，从而完成从第一通信方 N1 向第二通信方 N2 的数据包传输。在从第一通信方 N1 向第二通信方 N2 传输数据包的过程中，数据包首先通过了第一保护装置 10 中设置的过滤模块 F1 的过滤检查，然后根据专有通信协议从第一保护装置 10 进入第二保护装置 20，这样的配置能够确保从第一通信方 N1 传输到第二通信方 N2 的数据安全性。从第二通信方 N2 向第一通信方 N1 的数据包传输流向如图 2 中的路径 L2 所示，其类似于路径 L1，在此将省略其描述。

与图 1 所示的现有技术的防火墙相比，根据本发明的隔离保护系统 1 采用了本发明的“2+1”结构：即，针对通信双方的运行于彼此独立的两个中央处理器上且在硬件结构上完全独立的两个保护装置 10、20 和设置

在两个保护装置 10、20 之间且根据专有通信协议在两个保护装置 10、20 之间进行安全数据交互的双向数据通信模块 4，来在通信双方之间实现双向数据通信。两个保护装置中均包含有对数据包进行过滤检查的过滤模块，这样可以根据通信双方的安全性要求对过滤模块的作为安全性要求的通信协议进行设置，以满足通信双方的安全性要求。在根据本发明的第一实施例的隔离保护系统 1 中，第一保护装置 10 和第二保护装置 20 分别运行于独立的中央处理器上，因此可以实现硬件上彼此完全独立的两个保护装置；双向数据传输模块 4 设置在第一保护装置 10 和第二保护装置 20 之间且利用专有通信协议实现第一保护装置 10 和第二保护装置 20 之间的安全通信，本发明的这种“2+1”结构在硬件实现上可以带来很多优点。例如，可以将第一保护装置 10 和第二保护装置 20 制造成两个彼此独立的主机，该主机包括中央处理器，而每个中央处理器可以具有相对应的内存。对于每个主机，可以采用以 Bootloader 作为引导加载程序的专用嵌入式 Linux 操作系统。这样，两个保护装置之间不会因为一个被攻击或者物理损坏而影响另一个保护装置的性能。又例如，可以将第一保护装置 10 和第二保护装置 20 制造成插件形式的装置，即制造成可拆卸形式的装置，而将双向数据传输模块 4 制造成内置有专有通信协议的背板，这样，当两个保护装置插入背板时，就形成了根据本发明的对通信双方的通信设施进行隔离保护的隔离保护系统。在这种情况下，当其中一个保护装置破坏时，可以容易地进行更换和维护，而另一个保护装置不会受到任何影响。

下面参照图 3 描述根据本发明第二实施例的隔离保护系统 2。图 3 所示的第二实施例中与图 2 所示的第一实施例中相同的标号表示相同的部件，在此不再重复描述。

与本发明第一实施例的隔离保护系统 1 不同的是，在根据本发明第二实施例的隔离保护系统 2 中，第一保护装置 10 中的过滤模块 F1 包括内置防火墙模块 K1 和数据包过滤模块 S1，而第二保护装置 20 中的过滤模块 F2 包括内置防火墙模块 K2 和数据包过滤模块 S2，如图 3 所示。内置防火墙模块 K1 可以对要从第一通信方 N1 传输到第二通信方 N2 的从第一接口 A1 接收的数据包执行防火墙过滤检查，防火墙过滤检查可以是基本的防火墙检查，以确保一般性的网络攻击难以奏效。基本的防火墙技术通

过设定协议、端口、IP 等的通信规则实现防御功能，即可以在数据链路层、网络层、传输层上对流经数据包进行检查，这其中主要涉及到对数据包执行包头内容检查，不满足该通信规则的数据包将被拦截。数据包过滤模块 S1 用于对经过内置防火墙模块 K1 过滤后的数据包进行数据包过滤检查，数据包过滤检查不同于防火墙过滤检查，其可以是基于应用层上数据包的深度过滤检查、协议分析，其主要涉及对数据流的数据包执行包体内容检查。在根据本发明的隔离保护系统 2 部署在工业现场的信息网络和控制网络之间作为工业网络安全隔离系统时，数据包过滤模块 S1 中可以内置工业通信协议，以检查符合工业通信协议的应用数据。所述包头内容涉及 IP 地址、MAC 地址、协议类型信息、端口信息，而所述包体内容涉及通信目标、通信源、通信目的、通信类型和通信内容。第二保护装置 20 中的过滤模块 F2 包括内置防火墙模块 K2 和数据包过滤模块 S2。内置防火墙模块 K2 用于对要从第二通信方 N2 传输到第一通信方 N1 的从第一接口 A2 输入的数据包进行防火墙过滤检查，防火墙过滤检查可以是基本的防火墙检查，来确保一般性的网络攻击难以奏效，基本的防火墙技术通过设定协议、端口、IP 等的通信规则实现防御功能，即可以在数据链路层、网络层、传输层上对流经数据进行检查，这其中主要涉及到对数据包的包头的检查，不满足该通信规则的数据包将被拦截。数据包过滤模块 S2 用于对经过内置防火墙模块 K2 过滤后的数据包进行数据包过滤检查，数据包过滤检查不同于防火墙过滤检查，其可以是基于应用层上数据包的深度过滤检查、协议分析，其主要涉及对数据流的数据包执行包体内容检查。在根据本发明的隔离保护系统 2 部署在工业现场的信息网络和控制网络之间作为工业网络安全隔离系统时，数据包过滤模块 S2 中可以内置工业通信协议，以检查符合工业通信协议的应用数据。所述包头内容涉及 IP 地址、MAC 地址、协议类型信息、端口信息，而所述包体内容涉及通信目标、通信源、通信目的、通信类型和通信内容。

从以上可以看出，第一保护装置 10 和第二保护装置 20 中均包含有相继对数据包进行过滤检查的内置防火墙模块和数据包过滤模块，这两道过滤检查可以针对数据流的数据包的不同部分进行过滤检查，例如内置防火墙模块支持对一般网络的数据链路层、网络层、传输层进行检查，即，

主要用于对数据包的包头进行过滤检查；而数据包过滤模块支持对应用层数据进行检查，即，主要对数据包内容进行过滤检查，因此可以在数据包过滤模块中内置多种工业通信协议，以用于检查符合工业协议的应用数据。由于根据本发明的隔离保护系统中所包含的每个保护装置均包含有相继对数据进行过滤检查的内置防火墙模块和数据包过滤模块，因此可以确保通过数据的安全性，并且可以通过在数据包过滤模块中预设期望的工业通信协议来使得本发明的网络安全保护系统能够充分地支持工业通信协议，以适应工业现场的信息网络和控制网络之间的安全需求。

在本发明中，内置防火墙模块 S1 和内置防火墙模块 S2 可以相同，即，提供相同的基本防火墙过滤检查。数据包过滤模块 S1 和数据包过滤模块 S2 可以相同，即，其中可以内置有相同的通信协议；也可以根据第一通信方 N1 和第二通信方 N2 的不同的安全性要求而内置有不同的通信协议，例如，在第一通信方 N1 作为数据包的发送方，而第二通信方 N2 作为数据包的接收方时，可以根据作为数据包接收方的第二通信方 N2 的安全性要求对第一保护装置 10 内的数据包过滤模块 S1 内置的通信协议进行设置；而当第一通信方 N1 作为数据包的接收方，而第二通信方 N2 作为数据包的发送方时，可以根据第一通信方 N1 的安全性要求对第二保护装置 20 内的数据包过滤模块 S2 内置的通信协议进行设置，从而满足通信双方的安全性需求。

由于第一保护装置 10 和第二保护装置 20 之间设置了内置有专有通信协议的双向数据传输模块 4，这样的话，要从一通信方传输到另一通信方的数据包即使通过了保护装置内的内置防火墙模块和数据包过滤模块的过滤检查，在其不满足双向数据传输模块 4 中内置的专有通信协议时也会被拦截阻断，而无法到达另一通信方，这进一步增加了通信双方通信线路上的数据传输的安全性。

根据本发明第二实施例的隔离保护系统 2 可以应用于工业现场信息网络和控制网路之间，对控制网路进行安全性防护。这主要是因为，在本发明的隔离保护系统 2 中，第一保护装置 10 和第二保护装置 20 中都包含有除了常规内置防火墙过滤检查之外的数据包过滤检查。在数据包过滤模块中可以内置多种自动化产品制造商的私有通信协议，以在客户端和服务

器端之间进行有效的 OPC、Modbus 等工业协议数据的通信，并且支持数据的读写控制。其他非工业数据全部被丢弃。

下面，将结合图 3 并且参照图 4 和图 5 来详细描述利用本发明的隔离保护系统 2 执行双向数据包过滤检查的方法。

为了描述的方便起见，图 4 和图 5 中以客户端和服务器端作为通信双方为例描述根据本发明的隔离保护系统 2 如何在客户端和服务器端实现数据的安全传输的方法。

图 4 示出了从客户端向服务器端传输数据的流程图。在步骤 S71，客户端发送数据包；在步骤 S72，数据包被发送至与客户端连接的 CPU（第一保护装置 10）；在步骤 S73，进行基本的防火墙检查，无效数据的数据包将被丢弃（步骤 S76），而有效数据进一步进行数据包过滤检查（步骤 S74）；经过步骤 S74 的数据包过滤检查的数据如果被认定为是无效数据，则数据包将被丢弃（步骤 S76），而被认定为有效的数据将被传送至与服务器端连接的 CPU（第二保护装置 20）（步骤 S75）；进一步，在步骤 S77，将接收到的数据包发送至服务器端。

图 5 示出了从服务器端向客户端传输数据的流程图。在步骤 S81，服务器端发送数据包；在步骤 S82，数据包被发送至与服务器端连接的 CPU（第二保护装置 20）；在步骤 S83，进行基本的防火墙检查，无效数据的数据包将被丢弃（步骤 S86），而有效数据进一步进行数据包过滤检查（步骤 S84）；经过步骤 S84 的数据包过滤检查的数据如果被认定为是无效数据，则数据包将被丢弃（步骤 S86），而被认定为有效的数据将被传送至与客户端连接的 CPU（第一保护装置 10）（步骤 S85）；进一步，在步骤 S87，将接收到的数据包发送至客户端。

以上示出了根据本发明的隔离保护系统及其执行双向数据包过滤检查的方法。本发明的隔离保护系统采用了本发明的“2+1”结构，即，能够分别与通信双方进行双向通信的第一保护装置和第二保护装置以及置于其间用于对第一保护装置和第二保护装置之间的数据交互进行控制的内置专有通信协议的双向数据传输模块，其特征在于本发明的隔离保护系统中的第一保护装置和第二保护装置分别运行于彼此独立的主机上，由彼此独立的 CPU 处理器进行控制，这样就确保了当其中一个主机出现故障或

受到病毒侵害时，另一个主机不会受到影响。另外，本发明的隔离保护系统中的第一保护装置和第二保护装置内的数据包过滤模块是针对应用层数据包的深度检查、协议分析，通过在其中内置多种专有工业通信协议，可以实现基于内置工业通讯协议的防护模式，在应用层上对数据包进行深度检查，为工业通讯提供独特的、工业级的专业隔离防护解决方案。因此，本发明的隔离保护系统尤其适于应用于工业现场信息网络和控制网络之间的数据的安全交互。

最后应说明的是：以上实施例仅用以说明本发明的技术方案而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或者等同替换，而不脱离本发明技术方案的精神和范围。

权 利 要 求 书

1. 一种隔离保护系统，设置在通信线路中对通信双方的通信设施进行隔离保护，它包括：

第一保护装置（10）和第二保护装置（20），用于分别与所述通信方之一的通信设施连接；

双向数据传输模块（4），设置在所述第一保护装置（10）和所述第二保护装置（20）之间，用于连接所述第一保护装置（10）和所述第二保护装置（20），而且根据专有通信协议将所述第一保护装置（10）输出的数据传送到所述第二保护装置（20），以及将所述第二保护装置（20）输出的数据传送到所述第一保护装置（10）；其特征在于：

所述第一保护装置（10）和所述第二保护装置（20）具有完全独立的硬件结构并分别运行于独立的中央处理器（CPU1，CPU2），其中所述第一保护装置（10）和所述第二保护装置（20）的每一个包括：

第一接口（A1，A2），用于从所连接的通信方的通信设施接收数据流的数据包并将来自另一通信方的数据输出到所连接的通信设施；

过滤模块（F1，F2），用于对从所述第一接口（A1，A2）接收的数据流执行过滤检查，并输出符合安全性要求的数据；

第二接口（B1，B2），用于接收所述的符合安全性要求的数据，并将该符合安全性要求的数据传送到所述双向数据传输模块（4）；以及

传输通道（C1，C2），用于将来自所述第二接口（B2，B1）的数据传送到所述第一接口（A1，A2）。

2. 根据权利要求 1 所述的隔离保护系统，其中所述的通信方的通信设施是计算机、服务器或其它网络信息的输入/输出装置。

3. 根据权利要求 1 所述的隔离保护系统，其中所述过滤模块（F1，F2）包括分别用于对传输的数据流的数据包执行基本防火墙检查的内置防火墙模块（K1，K2）和用于执行数据包深度过滤的数据包过滤模块（S1，S2）。

4. 根据权利要求 3 所述的隔离保护系统，其中所述内置防火墙模块（K1，K2）对数据流的数据包执行包头内容检查，而所述数据包过滤模块（S1，S2）对数据流的数据包执行包体内容检查。

5. 根据权利要求 4 所述的隔离保护系统，其中所述包头内容涉及 IP 地址、MAC 地址、协议类型信息、端口信息，而所述包体内容涉及通信目标、通信源、通信目的、通信类型和通信内容。

6. 根据权利要求 1 所述的隔离保护系统，其中所述数据包过滤模块（S1，S2）中分别内置有支持工业通信协议的过滤列表。

7. 采用根据权利要求 1 的隔离保护系统执行双向数据包过滤检查的方法，其特征在于包括步骤：

在通信线路中设置具有完全独立的硬件结构并且分别运行于独立的中央处理器（CPU1,CPU2）的第一保护装置（10）和第二保护装置（20）分别用于通信双方的通信设施；以及

利用设置在第一保护装置（10）和第二保护装置（20）中的过滤模块（F1，F2）对传输的数据流的数据包执行过滤检查。

8. 根据权利要求 7 所述的方法，其中所述的过滤检查包括：

对传输的数据流的数据包执行基本防火墙检查，以及

对传输的数据流的数据包执行数据包深度过滤。

9. 根据权利要求 8 所述的方法，其中

所述对传输的数据流的数据包执行基本防火墙检查包括对数据流的数据包执行包头内容检查，以及

所述对传输的数据流的数据包执行数据包深度过滤包括对数据流的数据包执行包体内容检查。

10. 根据权利要求 9 所述的方法，其中所述包头内容涉及 IP 地址、

MAC 地址、协议类型信息、端口信息，而所述包体内容涉及通信目标、通信源、通信目的、通信类型和通信内容。

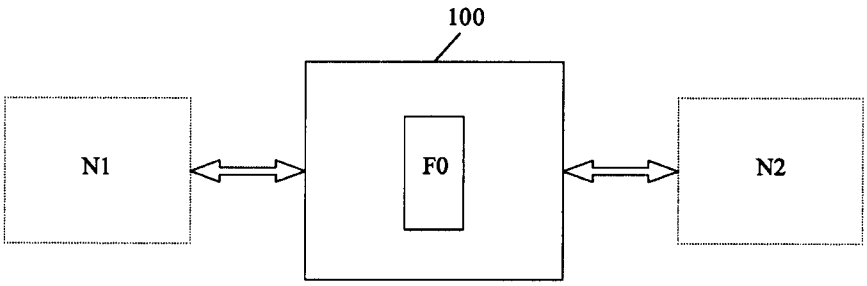
100
N1
F0
N2

图 1

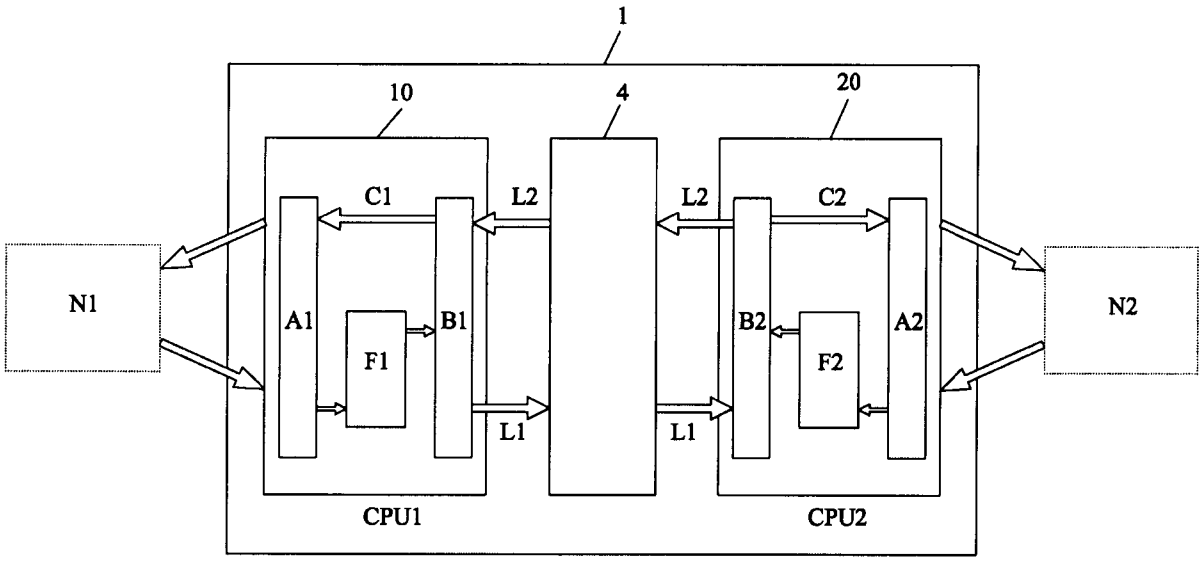
1
10
4
20
C1
L2
L2
C2
N1
A1
F1
B1
B2
F2
A2
N2
L1
L1
CPU1
CPU2

图 2

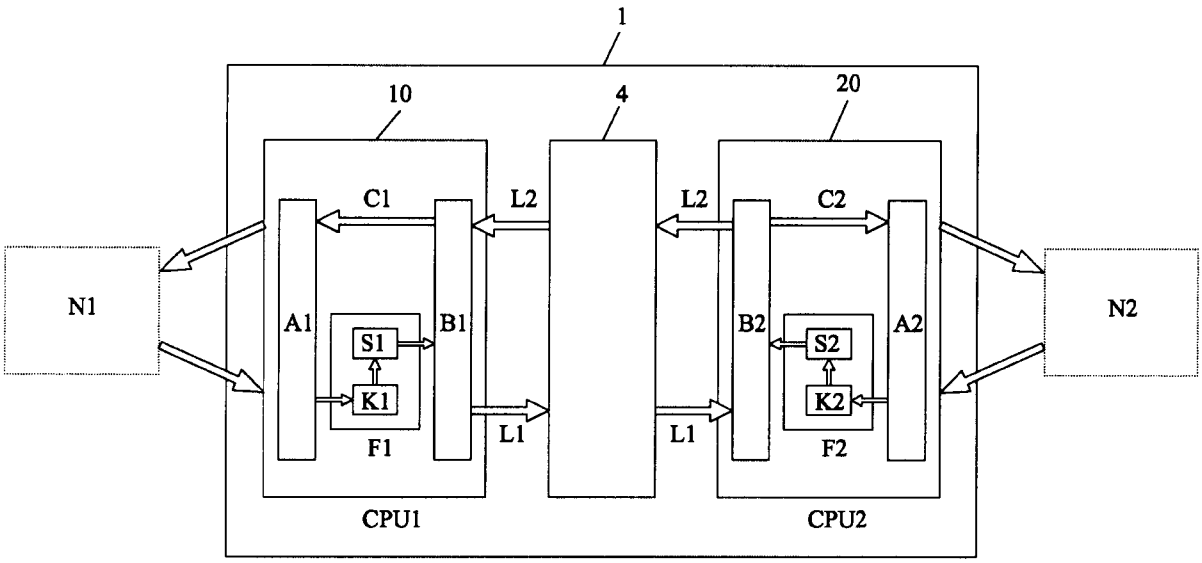
1
10
4
20
C1
L2
L2
C2
N1
A1
S1
K1
F1
B1
B2
S2
K2
F2
A2
N2
L1
L1
CPU1
CPU2

图 3

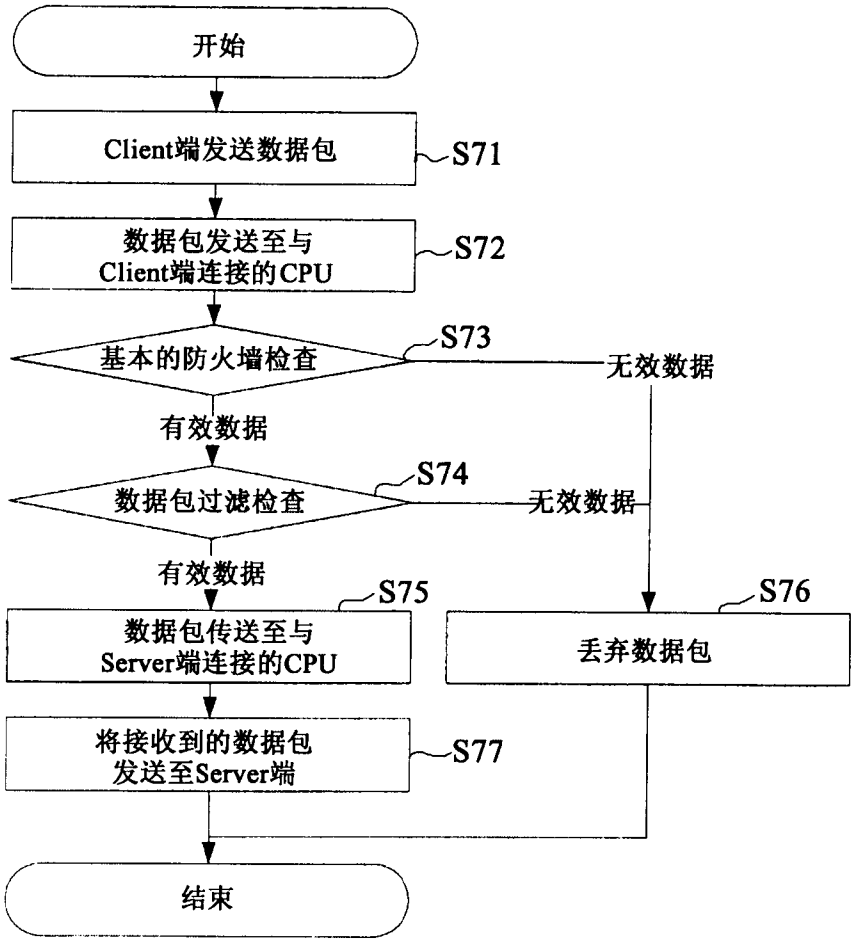
开始
Client端发送数据包
S71
数据包发送至与
Client端连接的CPU
S72
基本的防火墙检查
S73
无效数据
有效数据
数据包过滤检查
S74
无效数据
有效数据
数据包传送至与
Server端连接的CPU
S75
丢弃数据包
S76
将接收到的数据包
发送至Server端
S77
结束

图 4

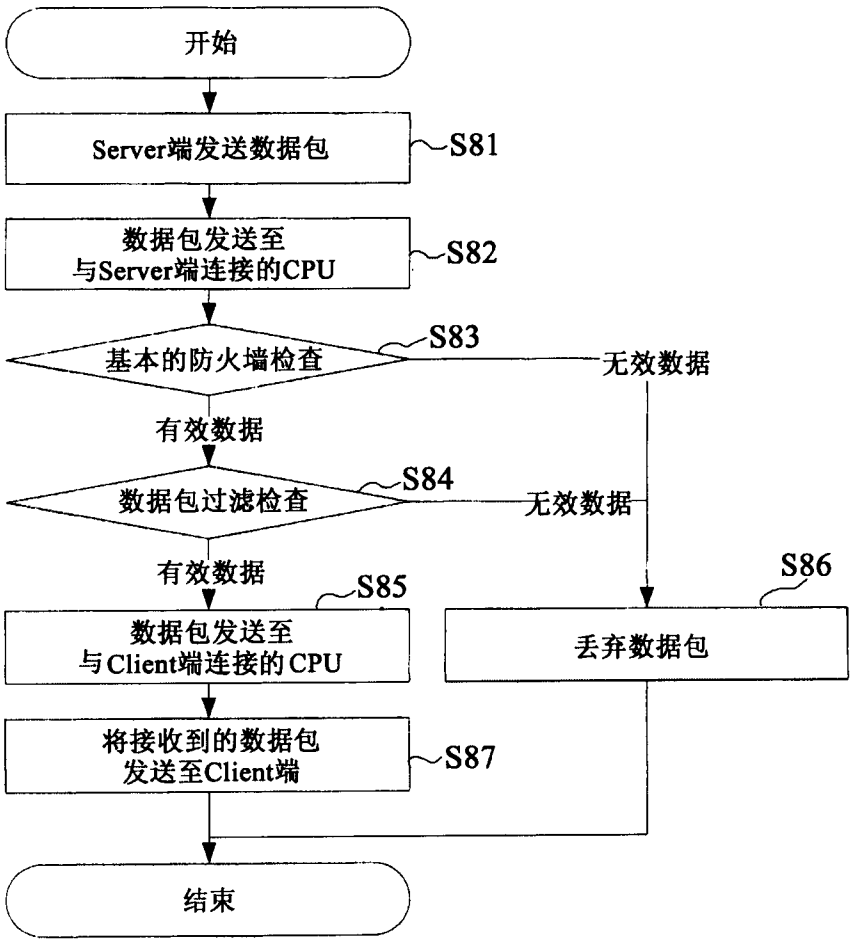
开始
Server端发送数据包
S81
数据包发送至
与Server端连接的CPU
S82
基本的防火墙检查
S83
无效数据
有效数据
数据包过滤检查
S84
无效数据
有效数据
S85
数据包发送至
与Client端连接的CPU
S86
丢弃数据包
将接收到的数据包
发送至Client端
S87
结束

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/071101

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L; H04W; H04Q; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, CNKI, VEN: isolat+, separat+, secur+, safe, safety, protect+, filter+, data packet, head, body, processor, CPU, independent, interface?, first, second, firewall, content, check+, examin+, inspect+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101540668 A (LENOVO GROUP BEIJING LTD.) 23 September 2009 (23.09.2009) description, page 3, line 4 to page 10, line 11 and figures 1 to 6	1-10
X	US 2012266230 A1 (LOCKHEED MARTIN CORPORATION) 18 October 2012 (18.10.2012) description, paragraphs [0017] to [0031] and figures 1A and 1B	1-10
A	CN 1173256 A (DIGITAL SECURED NETWORKS TECHNOLOGY INC.) 11 February 1998 (11.02.1998) the whole document	1-10
A	CN 102685119 A (SHANGHAI JIEZHINENG INFORMATION TECHNOLOGY CO., LTD.) 19 September 2012 (19.09.2012) the whole document	1-10
A	CN 101668002 A (INVENTEC CORP.) 10 March 2010 (10.03.2010) the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February 2014 (20.02.2014)	20 March 2014 (20.03.2014)
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer GONG, Mei Telephone No. (86-10) 62089571

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/071101

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101540668 A	23.09.2009	CN 101540668 B	22.06.2011
US 2012266230 A1	18.10.2012	None	
CN 1173256 A	11.02.1998	AU 7154896 A	28.04.1997
		US 5757924 A	26.05.1998
		EP 0872074 A1	21.10.1998
		US 6151679 A	21.11.2000
		WO 9713340 A1	10.04.1997
		IL 121416 A	13.09.2001
		CA 2211301 C	24.01.2006
		AU 725712 B2	19.10.2000
		SG 92687 A1	19.11.2002
		SG 96185 A1	23.05.2003
		IL 121416 D0	28.10.1999
CN 102685119 A	19.09.2012	None	
CN 101668002 A	10.03.2010	None	

国际检索报告

国际申请号
PCT/CN2014/071101

A. 主题的分类

H04L 29/06 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L, H04W, H04Q, G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CPRSABS; CNTXT; CNKI; VEN：隔离、保护、安全、过滤、数据包、包头、包体、处理器、独立、单独、接口、第一、第二、防火墙、内容、检测、检查、isolat+, separat+, secur+, safe, safety, protect+, filter+, data packet, head, body, processor, CPU, independent, interface?, first, second, firewall, content, check+ ,examin+, inspect+

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 101540668 A（联想（北京）有限公司）23.9 月 2009(23.09.2009) 说明书第 3 页第 4 行至第 10 页第 11 行，图 1-6	1-10
X	US 2012266230 A1 （LOCKHEED MARTIN CORPORATION） 18.10 月 2012(18.10.2012) 说明书第[0017]-[0031]段，图 1A，1B	1-10
A	CN 1173256 A（数字保证网络技术股份有限公司） 11.2 月 1998(11.02.1998) 全文	1-10
A	CN 102685119 A （上海杰之能信息科技有限公司） 19.9 月 2012(19.09.2012) 全文	1-10
A	CN 101668002 A （英业达股份有限公司）10.3 月 2010(10.03.2010) 全文	1-10

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
20.2 月 2014(20.02.2014)	**20.3 月 2014 (20.03.2014)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 龚玫 电话号码：(86-10) **62089571**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2014/071101

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 101540668 A	23.09.2009	CN 101540668 B	22.06.2011
US 2012266230 A1	18.10.2012	无	
CN 1173256 A	11.02.1998	AU 7154896 A	28.04.1997
		US 5757924 A	26.05.1998
		EP 0872074 A1	21.10.1998
		US 6151679 A	21.11.2000
		WO 9713340 A1	10.04.1997
		IL 121416 A	13.09.2001
		CA 2211301 C	24.01.2006
		AU 725712 B2	19.10.2000
		SG 92687 A1	19.11.2002
		SG 96185 A1	23.05.2003
		IL 121416 D0	28.10.1999
CN 102685119 A	19.09.2012	无	
CN 101668002 A	10.03.2010	无	