(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 104243591 B
(45)授权公告日 2018.02.09

(21)申请号 201410491545.7

(22)申请日 2014.09.24

(65)同一申请的已公布的文献号
申请公布号 CN 104243591 A

(43)申请公布日 2014.12.24

(73)专利权人 新华三技术有限公司
地址 310052 浙江省杭州市滨江区长河路466号

(72)发明人 韩小平 孙松儿

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 衣淑凤 宋志强

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

(56)对比文件
CN 1722664 A,2006.01.18,
CN 101414277 A,2009.04.22,
CN 102685163 A,2012.09.19,
CN 103973573 A,2014.08.06,
WO 2014066161 A2,2014.05.01,
WO 2010000146 A1,2010.01.07,

审查员 陈晨

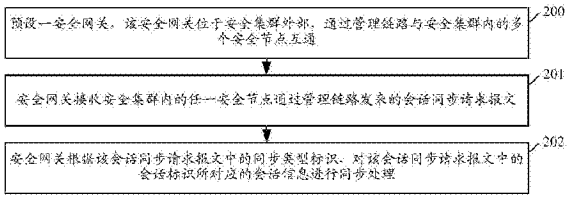
权利要求书3页 说明书8页 附图3页

(54)发明名称

同步安全集群会话信息的方法及装置

(57)摘要

本申请提出同步安全集群会话信息的方法及装置。方法包括:预设一安全网关,该安全网关位于安全集群外部,通过管理链路与安全集群内的多个安全节点互通,所述安全网关接收所述安全集群内的任一安全节点通过管理链路发来的会话同步请求报文,根据该会话同步请求报文中的同步类型标识,对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理。本申请提高了安全集群的会话性能。



CN 104243591 B

1.一种同步安全集群会话信息的方法，其特征在于，预设一安全网关，该安全网关位于安全集群外部，通过管理链路与安全集群内的多个安全节点互通，该方法包括：

所述安全网关接收所述安全集群内的任一安全节点通过所述管理链路发来的会话同步请求报文；

所述安全网关根据该会话同步请求报文中的同步类型标识，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理。

2.根据权利要求1所述的方法，其特征在于，当所述同步类型标识为创建同步标识时，

所述会话同步请求报文进一步携带在所述安全节点上创建成功的会话信息；

所述对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

所述安全网关保存该会话同步请求报文中携带的所述会话信息。

3.根据权利要求1所述的方法，其特征在于，当所述同步类型标识为更新同步标识时，

所述会话同步请求报文进一步携带在所述安全节点上创建成功的会话的更新会话信息；

所述对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

所述安全网关根据该会话同步请求报文携带的会话标识，在自身查找到对应的会话信息，根据该会话同步请求报文携带的所述更新会话信息对查找到的会话信息进行更新。

4.根据权利要求2或3所述的方法，其特征在于，所述会话同步请求报文携带多个会话的会话信息或更新会话信息，

且，所述对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理进一步包括：

所述安全网关向所述安全节点返回会话同步响应报文，该会话同步响应报文中携带同步成功的会话数目，以使得：所述安全节点在接收到所述会话同步响应报文后，判断该会话同步响应报文携带的同步成功的会话数目是否与本安全节点发出的会话同步请求报文携带的会话信息的数目一致，若不一致，则重新向所述安全网关发出所述会话同步请求报文。

5.根据权利要求1所述的方法，其特征在于，当所述同步类型标识为获取同步标识时，

所述会话同步请求报文中进一步携带请求获取的会话数目；

所述对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

所述安全网关根据该会话同步请求报文中携带的会话标识，在自身保存的所有会话信息中查找到对应的会话信息，将查找到的会话信息及返回的会话数目携带在会话同步响应报文中返回给所述安全节点，以使得：所述安全节点在接收到所述会话同步响应报文后，判断该会话同步响应报文携带的会话数目是否与本安全节点发出的会话同步请求报文携带的会话信息的数目一致，若不一致，则比较所述会话同步请求报文中携带的会话标识与所述会话同步响应报文中携带的会话标识，得知未被返回的会话标识，在本地创建对应的会话信息。

6.根据权利要求2所述的方法，其特征在于，当所述同步类型标识为删除同步标识时，

所述对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

所述安全网关根据该会话同步请求报文中携带的会话标识，在自身保存的所有会话信息中查找到对应的会话信息，删除查找到的会话信息。

7.根据权利要求2或6所述的方法，其特征在于，所述安全网关保存该会话同步请求报

文中携带的所述会话信息进一步包括：

所述安全网关为保存的每条会话信息设置一个老化定时器，所述老化定时器的定时时长大于对应会话信息的更新时长，

且，对于保存的每条会话信息，若在对应的老化定时器超时前，接收到所述安全节点发来的针对该会话信息的同步类型标识为更新同步标识的会话同步请求报文，则重启该老化定时器；对于保存的每条会话信息，在对应的老化定时器超时时，删除该会话信息。

8.一种同步安全集群会话信息的装置，位于安全网关上，其特征在于，该安全网关位于安全集群外部，通过管理链路与安全集群内的多个安全节点互通，该装置包括：

会话同步请求接收模块：接收所述安全集群内的任一安全节点通过所述管理链路发来的会话同步请求报文；

会话信息同步处理模块：根据所述会话同步请求报文中的同步类型标识，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理。

9.根据权利要求8所述的装置，其特征在于，当所述会话同步请求接收模块接收到的会话同步请求报文中的同步类型标识为创建同步标识时，

所述会话同步请求报文进一步携带在所述安全节点上创建成功的会话信息；

所述会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

保存该会话同步请求报文中携带的所述会话信息。

10.根据权利要求8所述的装置，其特征在于，当所述会话同步请求接收模块接收到的会话同步请求报文中的同步类型标识为更新同步标识时，

所述会话同步请求报文进一步携带在所述安全节点上创建成功的会话的更新会话信息；

所述会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

根据该会话同步请求报文携带的会话标识，在自身查找到对应的会话信息，根据该会话同步请求报文携带的所述更新会话信息对查找到的会话信息进行更新。

11.根据权利要求9或10所述的装置，其特征在于，所述会话同步请求接收模块接收到的会话同步请求报文携带多个会话的会话信息或更新会话信息，

且，所述会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理进一步包括：向所述安全节点返回会话同步响应报文，该会话同步响应报文中携带同步成功的会话数目，以使得：所述安全节点在接收到所述会话同步响应报文后，判断该会话同步响应报文携带的同步成功的会话数目是否与本安全节点发出的会话同步请求报文携带的会话信息的数目一致，若不一致，则重新向所述安全网关发出所述会话同步请求报文。

12.根据权利要求8所述的装置，其特征在于，当所述会话同步请求接收模块接收到的会话同步请求报文中的同步类型标识为获取同步标识时，

所述会话同步请求报文中进一步携带请求获取的会话数目；

所述会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

根据该会话同步请求报文中携带的会话标识，在自身保存的所有会话信息中查找到对应的会话信息，将查找到的会话信息及返回的会话数目携带在会话同步响应报文中返回给所述安全节点，以使得：所述安全节点在接收到所述会话同步响应报文后，判断该会话同步响应报文携带的会话数目是否与本节点发出的会话同步请求报文携带的会话信息的数目一致，若不一致，则比较所述会话同步请求报文中携带的会话标识与所述会话同步响应报文中携带的会话标识，得知未被返回的会话标识，在本地创建对应的会话信息。

13.根据权利要求9所述的装置，其特征在于，当所述会话同步请求接收模块接收到的会话同步请求报文中的同步类型标识为删除同步标识时，

所述会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

根据该会话同步请求报文中携带的会话标识，在自身保存的所有会话信息中查找到对应的会话信息，删除查找到的会话信息。

14.根据权利要求9或13所述的装置，其特征在于，所述会话信息同步处理模块保存该会话同步请求报文中携带的所述会话信息进一步包括：

为保存的每条会话信息设置一个老化定时器，所述老化定时器的定时时长大于对应会话信息的更新时长，

且，对于保存的每条会话信息，若在对应的老化定时器超时前，接收到所述安全节点发来的针对该会话信息的同步类型标识为更新同步的会话同步请求报文，则重启该老化定时器；对于保存的每条会话信息，在对应的老化定时器超时时，删除该会话信息。

同步安全集群会话信息的方法及装置

技术领域

[0001] 本申请涉及安全集群技术领域，尤其涉及同步安全集群会话信息的方法及装置。

背景技术

[0002] 安全设备指的是在网络中专门执行安全策略如：防火墙设备。云计算、大数据等新兴技术的崛起在网络中产生了更多的数据，对于安全设备的性能要求也是成级数增长。受限于单台物理安全设备的性能限制，如何在平滑扩展安全设备性能的同时而不带来管理部署的复杂度成为安全设备急需解决的问题。安全集群是一种多虚一的虚拟化技术，可以有效解决上述问题。

[0003] 现有安全集群的组网形态与网络设备类似，安全集群内的安全设备的部署位置通常旁挂汇聚或核心交换机，以防火墙设备为例，简化后的安全集群组网形态如图1所示，其中，防火墙设备FW1～FW4构成一个安全集群，FW1～FW4通过聚合链路与核心交换机连接，核心交换机将来自下挂主机1～n的流量通过预设的负载分担算法分担到FW1～FW4上，FW1～FW4根据自身配置的安全策略确定对核心交换机发来的流量进行转发还是丢弃。

[0004] 为了实现集群处理的可靠性，现有安全集群处理机制通过手工指定或者自动建立配置备份关系，集群中的任何一个节点的会话必须备份到其它节点，从而实现宿主节点故障后，已经建立的数据流不中断。

发明内容

[0005] 本申请提供同步安全集群会话信息的方法及装置，以提高安全集群的会话性能。

[0006] 本申请的技术方案是这样实现的：

[0007] 一种同步安全集群会话信息的方法，预设一安全网关，该安全网关位于安全集群外部，通过管理链路与安全集群内的多个安全节点互通，该方法包括：

[0008] 所述安全网关接收所述安全集群内的任一安全节点通过所述管理链路发来的会话同步请求报文；

[0009] 所述安全网关根据该会话同步请求报文中的同步类型标识，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理。

[0010] 一种同步安全集群会话信息的装置，位于安全网关上，该安全网关位于安全集群外部，通过管理链路与安全集群内的多个安全节点互通，该装置包括：

[0011] 会话同步请求接收模块：接收所述安全集群内的任一安全节点通过所述管理链路发来的会话同步请求报文；

[0012] 会话信息同步处理模块：根据所述会话同步请求报文中的同步类型标识，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理。

[0013] 可见，本申请中，通过在安全集群外设置一安全网关，在安全集群内的各安全节点上创建的会话信息都同步到该安全网关上，安全节点之间无需相互备份会话信息，从而减轻了安全集群的处理负担，提高了安全集群的会话性能。

附图说明

[0014] 图1为现有的安全集群组网形态示意图；

[0015] 图2为本申请一实施例提供的同步安全集群会话信息的方法流程图；

[0016] 图3为本申请实施例提供的同步安全集群会话信息的组网示意图；

[0017] 图4为本申请另一实施例提供的同步安全集群会话信息的方法流程图；

[0018] 图5为本申请实施例提供的包含同步安全集群会话信息的装置的安全网关的硬件结构示意图；

[0019] 图6为本申请实施例提供的同步安全集群会话信息的装置的组成示意图。

具体实施方式

[0020] 申请人对现有安全集群处理机制进行分析发现：集群内的安全节点之间的会话备份占用了节点自身的会话资源，导致集群的会话性能无法线性增加，以1:1的备份为例，最差的情况下，集群整体的会话规格为单个节点规格之和的1/2。

[0021] 图2为本申请一实施例提供的同步安全集群会话信息的方法流程图，其具体步骤如下：

[0022] 步骤200：预设一安全网关，该安全网关位于安全集群外部，通过管理链路与安全集群内的多个安全节点互通。

[0023] 安全网关可以为物理安全网关，也可以是位于物理服务器上的虚拟安全网关。

[0024] 本申请实施例中的“管理链路”专用于安全网关与安全节点之间交互本申请实施例中提到的会话同步相关报文，由于安全网关与安全节点之间的交互要经过安全集群旁挂的核心/汇聚交换机，因此需要预先通过核心/汇聚交换机在安全网关与各安全节点之间建立物理链路作为管理链路，并为安全网关以及核心/汇聚交换机以及各安全节点在管理链路上的端口分配IP地址，需要预先将安全网关的IP地址配置到安全集群中的各安全节点上。

[0025] 图3给出了本申请实施例提供的同步安全集群会话信息的组网示意图，其中，安全集群内的各安全节点通过管理链路与安全网关互通，该管理链路路经安全集群旁挂的核心/汇聚交换机，即安全节点与安全网关之间的管理链路是要经过安全集群旁挂的核心/汇聚交换机的。

[0026] 步骤201：安全网关接收安全集群内的任一安全节点通过管理链路发来的会话同步请求报文。

[0027] 步骤202：安全网关根据该会话同步请求报文中的同步类型标识，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理。

[0028] 优选地，当同步类型标识为创建同步标识时，会话同步请求报文进一步携带在所述安全节点上创建成功的会话信息，且，步骤202中，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

[0029] 安全网关保存该会话同步请求报文中携带的所述会话信息。

[0030] 优选地，当同步类型标识为更新同步标识时，会话同步请求报文进一步携带在所述安全节点上创建成功的会话的更新会话信息，且，步骤202中，对该会话同步请求报文中

的会话标识所对应的会话信息进行同步处理包括：

[0031] 安全网关根据该会话同步请求报文携带的会话标识，在自身查找到对应的会话信息，根据该会话同步请求报文携带的所述更新会话信息对查找到的会话信息进行更新。

[0032] 优选地，会话同步请求报文携带多个会话的会话信息或更新会话信息，且，安全网关对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理进一步包括：

[0033] 安全网关向安全节点返回会话同步响应报文，该会话同步响应报文中携带同步成功的会话数目，以使得：安全节点在接收到会话同步响应报文后，判断该会话同步响应报文携带的同步成功的会话数目是否与本安全节点发出的会话同步请求报文携带的会话信息的数目一致，若不一致，则重新向安全网关发出上述会话同步请求报文。

[0034] 优选地，当同步类型标识为获取同步标识时，会话同步请求报文中进一步携带请求获取的会话数目；且，步骤202中，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

[0035] 安全网关根据该会话同步请求报文中携带的会话标识，在自身保存的所有会话信息中查找到对应的会话信息，将查找到的会话信息及返回的会话数目返回给所述安全节点，以使得：所述安全节点在接收到所述会话同步响应报文后，判断该会话同步响应报文携带的会话数目是否与本安全节点发出的会话同步请求报文携带的会话信息的数目一致，若不一致，则比较所述会话同步请求报文中携带的会话标识与所述会话同步响应报文中携带的会话标识，得知未被返回的会话标识，在本地创建对应的会话信息。

[0036] 优选地，当同步类型标识为删除同步标识时，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

[0037] 安全网关根据该会话同步请求报文中携带的会话标识，在自身保存的所有会话信息中查找到对应的会话信息，删除查找到的会话信息。

[0038] 优选地，安全网关保存该会话同步请求报文中携带的所述会话信息进一步包括：为保存的每条会话信息设置一个老化定时器，老化定时器的定时时长大于对应会话信息的更新时长，且，对于保存的每条会话信息，若在对应的老化定时器超时前，接收到安全节点发来的针对该会话信息的同步类型标识为更新同步标识的会话同步请求报文，则重启该老化定时器；对于保存的每条会话信息，在对应的老化定时器超时时，删除该会话信息。

[0039] 从本申请实施例可以看出：通过在安全集群外设置一安全网关，在安全集群内的各安全节点上创建的会话信息都同步到该安全网关上，这样，安全节点之间无需相互备份会话信息，从而减轻了安全集群的处理负担，提高了安全集群的会话性能。

[0040] 图4为本申请另一实施例提供的同步安全集群会话信息的方法流程图，其具体步骤如下：

[0041] 步骤400：预设一虚拟安全网关，该虚拟安全网关位于安全集群外部，安全集群中的每个安全节点分别通过管理链路与该虚拟安全网关互通。

[0042] 对于安全集群内的所有安全节点来说，虚拟安全网关为外置设备。虚拟安全网关的典型形态为外置服务器上的软件形态网关。

[0043] 虚拟安全网关不处理实际业务，仅用于备份安全集群监控的会话信息以及响应安全节点的会话信息获取请求。

[0044] 安全集群内所有节点的管理链路在同一管理VLAN(Virtual Local Area

Network，虚拟局域网)中。

[0045] 步骤401：对于安全集群内的任一安全节点，当该安全节点监控到两个主机之间的连接时，创建对应的会话，并将该会话信息携带在会话创建同步请求报文中发送给虚拟安全网关。

[0046] 例如：当两个主机之间采用TCP(Transmission Control Protocol，传输控制协议)通信时，两个主机通过TCP三次握手过程建立TCP连接，则，当安全节点发现两个主机之间的TCP三次握手成功时，确定TCP连接建立成功，将该TCP连接对应的会话信息携带在会话创建同步请求报文中发送给虚拟安全网关；

[0047] 当两个主机之间采用UDP(User Datagram Protocol，用户数据报协议)通信时，由于UDP属于无连接协议，则，当安全节点发现一个主机向另一主机第一次发起UDP报文，且另一主机也返回了UDP报文时，认为UDP连接建立成功，将该UDP连接对应的会话信息携带在会话创建同步请求报文中发送给虚拟安全网关。

[0048] 同步到虚拟安全网关的会话信息必须包括会话标识，如：五元组(包括：源地址、源端口号、目的地址、目的端口号和协议版本类型)，还可以包括：会话状态统计信息、NAT(Network Address Translation，网络地址转换)信息等，会话状态统计信息如：正、反向传递字节数等。

[0049] 步骤402：虚拟安全网关接收该会话创建同步请求报文，保存该会话创建同步请求报文中的会话信息，并向该安全节点返回会话创建同步响应报文。

[0050] 需要说明的是，安全节点可以将多个新建的会话的信息放在同一个会话创建同步请求报文中。

[0051] 本实施例中，安全节点与虚拟安全网关之间交互的会话同步报文的格式可如表1所示：

[0052]

序列号（Sequence Num）	Version（版本）	Code（类型码）	Count（数目）
会话信息 1			
会话信息 2			
…			

[0053]

会话信息 N

[0054] 表1本实施例中的会话同步报文格式

[0055] 如表1所示，其中：

[0056] 1)Sequence Num：用于唯一地标识一次会话同步，一次会话同步包括：安全节点向虚拟安全网关发出一个会话同步请求报文，然后，虚拟安全网关向该安全节点返回一个会话同步响应报文，该会话同步请求报文和该会话同步响应报文中的Sequence Num相同。

[0057] 本实施例中，会话同步请求报文主要包括：会话创建同步请求报文、会话删除同步请求报文、会话更新同步请求报文、会话信息获取请求报文。

[0058] 2)Version:表示会话同步报文中包含的会话信息采用的协议版本类型,主要包括IPv4和IPv6,对应的Version值可分别为0x4、0x6。

[0059] 当会话信息采用的协议版本类型不同时,会话信息中的各部分的长度是不同的。例如:当两条会话信息分别采用IPv4、IPv6时,它们包含的源地址和目的地址(分别为IPv4地址、IPv6地址)的长度是不同的。因此,为了使得虚拟安全网关或安全节点能够准确地解析会话同步报文中的会话信息的各部分内容,必须在会话同步报文中包含Version字段。

[0060] 3)Code:表示会话同步报文的类型,本实施例中,会话同步报文主要分为如表2所示的5种:

[0061]

Code	说明
0x1	会话创建同步请求报文(安全节点发出)
0x2	会话删除同步请求报文(安全节点发出)
0x3	会话更新同步请求报文(安全节点发出)
0x4	会话信息获取请求报文(安全节点发出)
0x5	会话同步响应报文(虚拟安全网关发出)

[0062] 表2本实施例中的会话同步报文的类型

[0063] 4)Count:

[0064] a、当Code值为0x1、0x3时,Count值表示本报文中包含的同步会话个数,同时在响应报文(Code值为0x5)中,Count值表示同步成功的会话个数。

[0065] 如果安全节点发现会话同步响应报文中的count值与本节点发出的对应会话同步请求报文中的count值不一致,则认为同步不成功,则重新向安全网关发出会话同步请求报文;若一致,则认为同步成功,不作进一步处理。

[0066] b、当Code值为0x2时,Count值表示本报文中包含的同步会话个数。

[0067] 当虚拟安全网关接收到会话删除同步请求报文时,只需根据会话删除同步请求报文中的会话信息删除本地保存的会话信息即可,无论是否删除成功都可不返回响应报文。因为:虚拟安全网关可分别为自身保存的每条会话信息维护一个老化定时器,该老化定时器随着会话信息的创建而创建,随着会话信息的更新而重启,该老化定时器的定时时长要大于对应会话信息的更新时长,当该老化定时器的定时时长到达时,若仍未收到针对该会话信息的会话更新同步请求报文,则删除该会话信息。

[0068] c、当Code值为0x4时,Count值表示本报文中包含的请求会话个数,同时在响应报文(Code值为0x5)中表示请求成功的会话个数。对于请求不成功的会话,安全节点会直接创建该会话。

[0069] 步骤403:安全节点周期性地向虚拟安全网关发送会话更新同步请求报文,该会话更新同步请求报文中携带自身保存的最新会话信息。

[0070] 步骤404:当虚拟安全网关接收到该会话更新同步请求报文时,根据该会话更新同步请求报文携带的会话信息中的会话标识在本地保存的会话信息中查找到对应的会话信息,以该会话更新同步请求报文携带的会话信息更新查找到的会话信息。

[0071] 步骤405:当该安全节点监控到两个主机间的连接删除时,删除自身保存的对应会话信息,并将该会话标识(如:五元组)携带在会话删除同步请求报文中发送给虚拟安全网

关。

[0072] 步骤406：当虚拟安全网关接收到该会话删除同步请求报文时，根据该会话删除同步请求报文中的会话标识在本地保存的会话信息中查找到对应的会话信息，删除查找到的会话信息。

[0073] 步骤407：当该安全节点需要向虚拟安全网关获取会话信息时，将该会话标识携带在会话信息获取请求报文中发送给虚拟安全网关。

[0074] 会话信息获取请求报文中可携带多个会话标识，报文中的Count字段值表示请求的会话数目。

[0075] 步骤408：虚拟安全网关接收到该会话信息获取请求报文，根据该会话信息获取请求报文中的会话标识查找到本地保存的对应会话信息，将查找到的会话信息携带在会话信息获取响应报文中返回给该安全节点。

[0076] 步骤409：安全节点接收该会话信息获取响应报文，保存该会话信息获取响应报文中的会话信息，根据该会话信息执行安全处理。

[0077] 会话信息获取响应报文中携带了返回的会话信息的数目，该数目携带在Count字段中，安全节点接收到该响应报文中，若发现有会话信息未被虚拟安全网关返回，则直接在本地创建对应的会话信息。

[0078] 以图3为例，设安全节点1故障，主机1发往主机2的TCP流量原来被核心交换机分配到安全节点1上，安全节点1故障后，主机1发往主机2的TCP流量被核心交换机分配到安全节点2上，当安全节点2第一次接收到主机1发往主机2的TCP流量时，发现本地未保存对应的TCP会话信息，则向虚拟安全网关发送携带五元组的会话信息获取请求报文，若之后虚拟安全网关返回的会话信息获取响应报文中携带了对应的TCP会话信息，则安全节点2保存该TCP会话信息，并根据该会话信息及自身配置的安全策略进行安全处理(转发或丢弃)；若虚拟安全网关返回的会话信息获取响应报文中未携带对应的TCP会话信息，则安全节点2丢弃该TCP流量，且在之后主机1与主机2通过TCP三次握手过程重新建立了TCP连接后，在本地保存该会话信息，并将该会话信息携带在会话创建同步请求报文中发送给虚拟安全网关。

[0079] 需要说明的是，为了提高安全网关的可靠性，也可设置多个安全网关，以实现安全网关的主备备份，具体实现如下：

[0080] 01：该多个安全网关具有共用的公共IP地址和相互独立的独立IP地址，在同一时刻只有其中一个安全网关为主安全网关，其它的都作为备安全网关；各安全网关之间通过独立IP地址进行通信，将安全网关的公共IP地址配置在安全集群内的所有安全节点上，公共IP地址只在主安全网关上生效，以使得：各安全节点只会与主安全网关进行通信。

[0081] 02：初始时，各安全网关之间根据预设选举原则，选举出主安全网关，主安全网关使能公共IP地址。

[0082] 03：主安全网关将安全节点同步来的所有会话信息实时或定期同步到所有备安全网关上。

[0083] 04：各安全网关之间周期性进行保活，若发现主安全网关故障，则剩余的正常备安全网关重新选举出新的主安全网关。

[0084] 本申请实施例提供的安全网关是可以软硬件结合的可编程设备，从硬件层面而言，安全网关的硬件架构示意图具体可以参见图5。图5为本申请实施例提供的包含同步安

全集群会话信息的装置的安全网关的硬件结构示意图。该安全网关中包括：非易失性存储器、CPU、内存和其它硬件，其中：

[0085] 非易失性存储器：存储指令代码；所述指令代码被CPU执行时完成的操作主要为内存中的同步安全集群会话信息的装置完成的功能。

[0086] CPU：与非易失性存储器通信，读取和执行非易失性存储器中存储的所述指令代码，完成上述同步安全集群会话信息的装置完成的功能。

[0087] 内存，当非易失性存储器中的所述指令代码被执行时完成的操作主要为内存中的同步安全集群会话信息的装置完成的功能。

[0088] 从软件层面而言，如图6所示，应用于安全网关中的同步安全集群会话信息的装置主要包括以下模块：会话同步请求接收模块和会话信息同步处理模块，其中：

[0089] 会话同步请求接收模块：接收安全集群内的任一安全节点通过管理链路发来的会话同步请求报文，将该会话同步请求报文转发给会话信息同步处理模块。

[0090] 会话信息同步处理模块：接收会话同步请求接收模块发来的会话同步请求报文，根据该会话同步请求报文中的同步类型标识，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理。

[0091] 优选地，当会话同步请求接收模块接收到的会话同步请求报文中的同步类型标识为创建同步标识时，会话同步请求报文进一步携带在安全节点上创建成功的会话信息；且，会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

[0092] 保存该会话同步请求报文中携带的所述会话信息。

[0093] 优选地，当会话同步请求接收模块接收到的会话同步请求报文中的同步类型标识为更新同步标识时，会话同步请求报文进一步携带在所述安全节点上创建成功的会话的更新会话信息；且，会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

[0094] 根据该会话同步请求报文携带的会话标识，在自身查找到对应的会话信息，根据该会话同步请求报文携带的所述更新会话信息对查找到的会话信息进行更新。

[0095] 优选地，会话同步请求接收模块接收到的会话同步请求报文携带多个会话的会话信息或更新会话信息；且，会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理进一步包括：向安全节点返回会话同步响应报文，该会话同步响应报文中携带同步成功的会话数目，以使得：安全节点在接收到该会话同步响应报文后，判断该会话同步响应报文携带的同步成功的会话数目是否与本安全节点发出的会话同步请求报文携带的会话信息的数目一致，若不一致，则重新向安全网关发出上述会话同步请求报文。

[0096] 优选地，当会话同步请求接收模块接收到的会话同步请求报文中的同步类型标识为获取同步标识时，会话同步请求报文中进一步携带请求获取的会话数目；且，会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

[0097] 根据该会话同步请求报文中携带的会话标识，在自身保存的所有会话信息中查找到对应的会话信息，将查找到的会话信息及返回的会话数目携带在会话同步响应报文中返回给所述安全节点，以使得：安全节点在接收到该会话同步响应报文后，判断该会话同步响

应报文携带的会话数目是否与本安全节点发出的会话同步请求报文携带的会话信息的数目一致，若不一致，则比较会话同步请求报文中携带的会话标识与会话同步响应报文中携带的会话标识，得知未被返回的会话标识，在本地创建对应的会话信息。

[0098] 优选地，当会话同步请求接收模块接收到的会话同步请求报文中的同步类型标识为删除同步标识时，会话信息同步处理模块对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理包括：

[0099] 根据该会话同步请求报文中携带的会话标识，在自身保存的所有会话信息中查找到对应的会话信息，删除查找到的会话信息。

[0100] 优选地，会话信息同步处理模块保存该会话同步请求报文中携带的所述会话信息进一步包括：为保存的每条会话信息设置一个老化定时器，老化定时器的定时时长大于对应会话信息的更新时长，且，对于保存的每条会话信息，若在对应的老化定时器超时前，接收到安全节点发来的针对该会话信息的同步类型标识为更新同步的会话同步请求报文，则重启该老化定时器；对于保存的每条会话信息，在对应的老化定时器超时时，删除该会话信息。

[0101] 上述的同步安全集群会话信息的装置作为一个逻辑意义上的装置，其是通过CPU将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。当对应的计算机程序指令被执行时，形成的同步安全集群会话信息的装置用于按照上述实施例中的同步安全集群会话信息的方法执行相应操作。

[0102] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

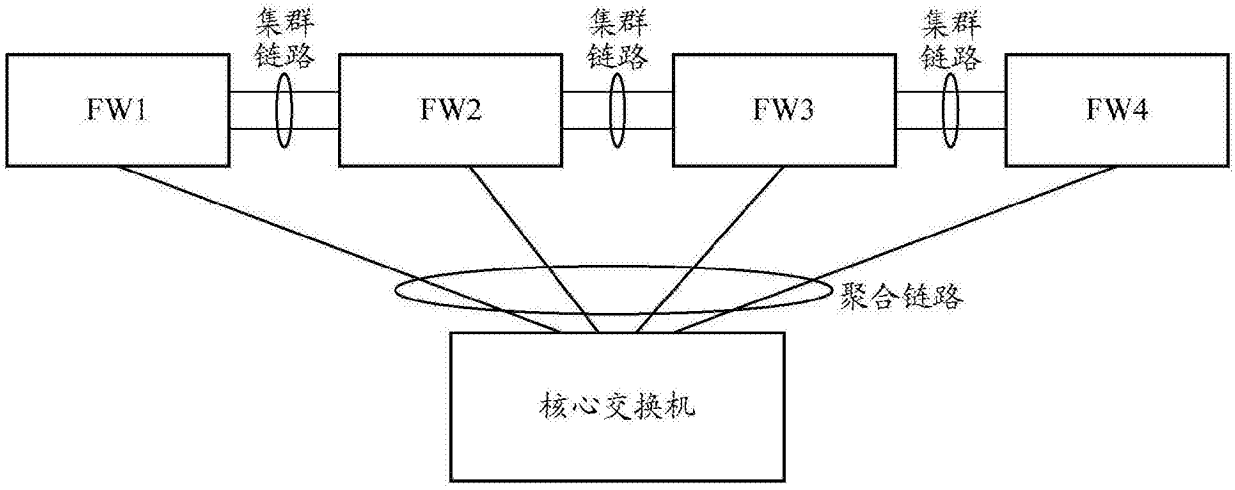

集群链路
集群链路
集群链路
FW1
FW2
FW3
FW4
聚合链路
核心交换机

图1

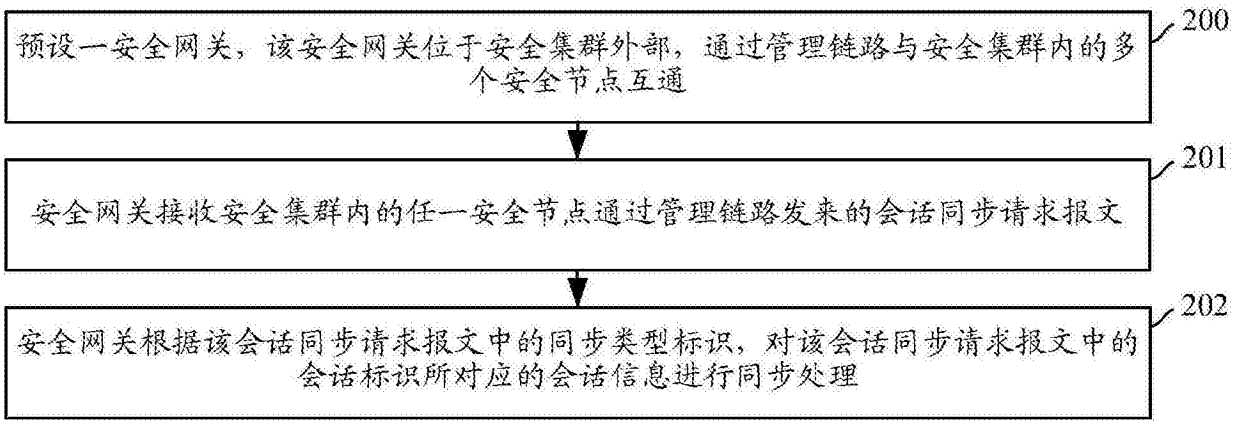

预设一安全网关，该安全网关位于安全集群外部，通过管理链路与安全集群内的多个安全节点互通
200
安全网关接收安全集群内的任一安全节点通过管理链路发来的会话同步请求报文
201
安全网关根据该会话同步请求报文中的同步类型标识，对该会话同步请求报文中的会话标识所对应的会话信息进行同步处理
202

图2

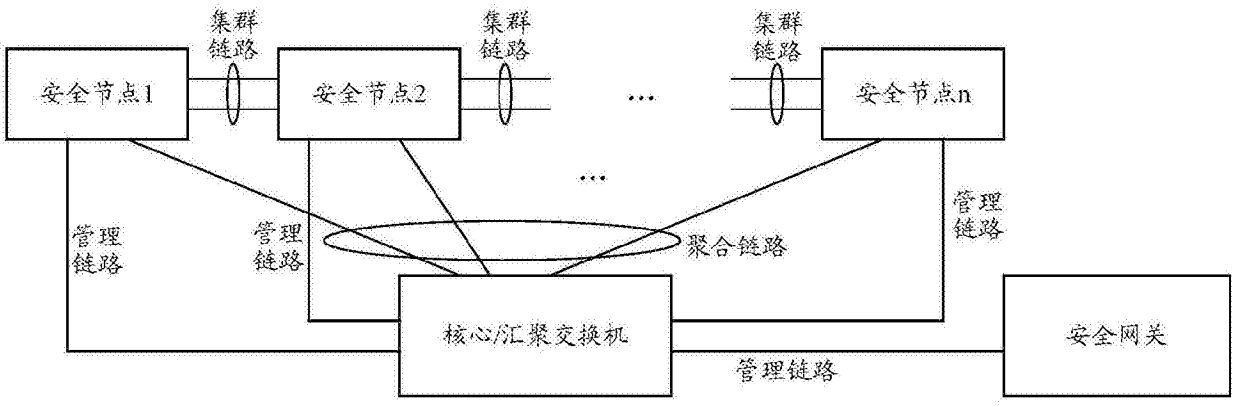

集群链路
集群链路
集群链路
安全节点1
安全节点2
安全节点n
管理链路
管理链路
聚合链路
管理链路
核心/汇聚交换机
安全网关
管理链路

图3

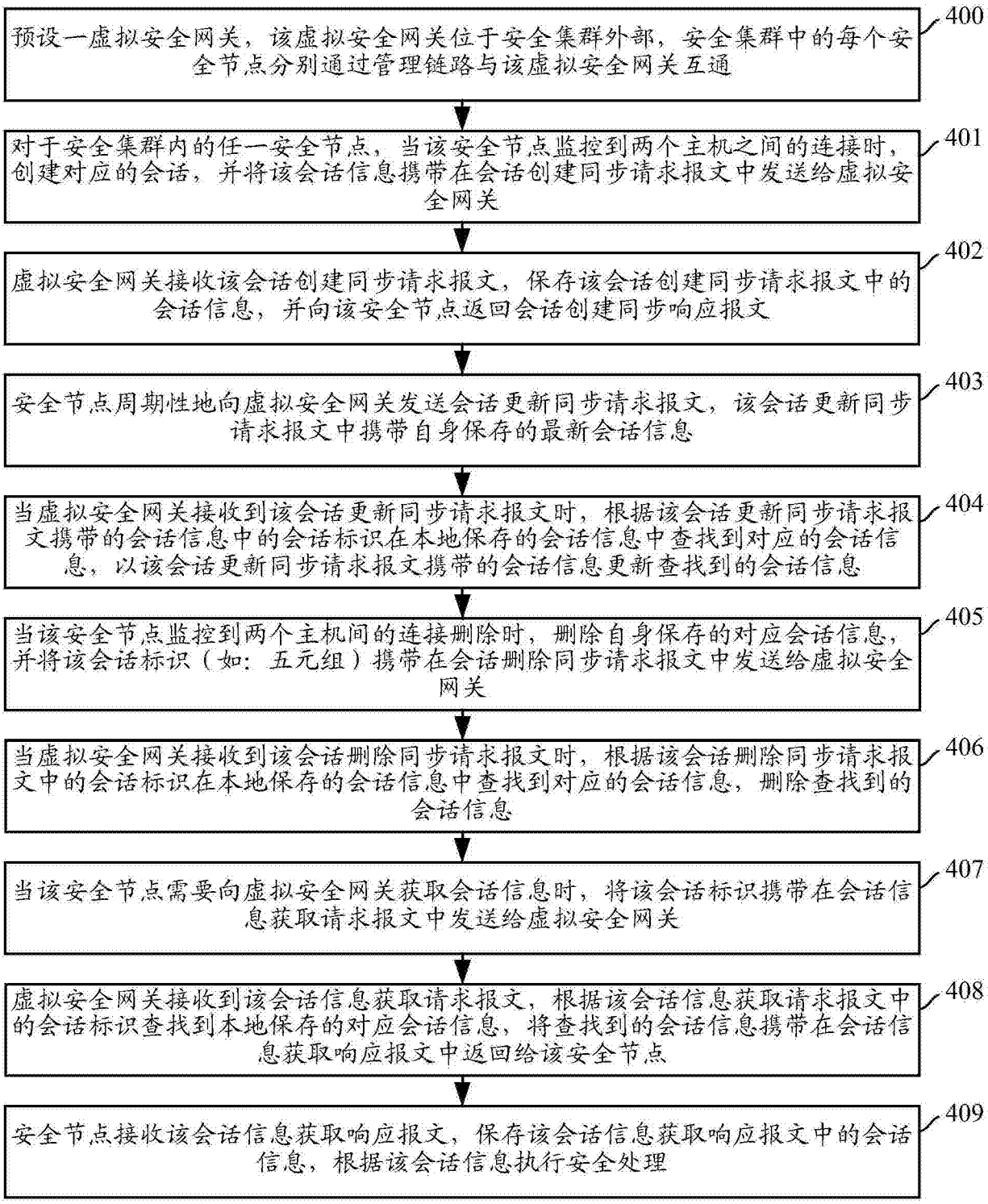

预设一虚拟安全网关，该虚拟安全网关位于安全集群外部，安全集群中的每个安全节点分别通过管理链路与该虚拟安全网关互通
400
对于安全集群内的任一安全节点，当该安全节点监控到两个主机之间的连接时，创建对应的会话，并将该会话信息携带在会话创建同步请求报文中发送给虚拟安全网关
401
虚拟安全网关接收该会话创建同步请求报文，保存该会话创建同步请求报文中的会话信息，并向该安全节点返回会话创建同步响应报文
402
安全节点周期性地向虚拟安全网关发送会话更新同步请求报文，该会话更新同步请求报文中携带自身保存的最新会话信息
403
当虚拟安全网关接收到该会话更新同步请求报文时，根据该会话更新同步请求报文携带的会话信息中的会话标识在本地保存的会话信息中查找到对应的会话信息，以该会话更新同步请求报文携带的会话信息更新查找到的会话信息
404
当该安全节点监控到两个主机间的连接删除时，删除自身保存的对应会话信息，并将该会话标识（如：五元组）携带在会话删除同步请求报文中发送给虚拟安全网关
405
当虚拟安全网关接收到该会话删除同步请求报文时，根据该会话删除同步请求报文中的会话标识在本地保存的会话信息中查找到对应的会话信息，删除查找到的会话信息
406
当该安全节点需要向虚拟安全网关获取会话信息时，将该会话标识携带在会话信息获取请求报文中发送给虚拟安全网关
407
虚拟安全网关接收到该会话信息获取请求报文，根据该会话信息获取请求报文中的会话标识查找到本地保存的对应会话信息，将查找到的会话信息携带在会话信息获取响应报文中返回给该安全节点
408
安全节点接收该会话信息获取响应报文，保存该会话信息获取响应报文中的会话信息，根据该会话信息执行安全处理
409

图4

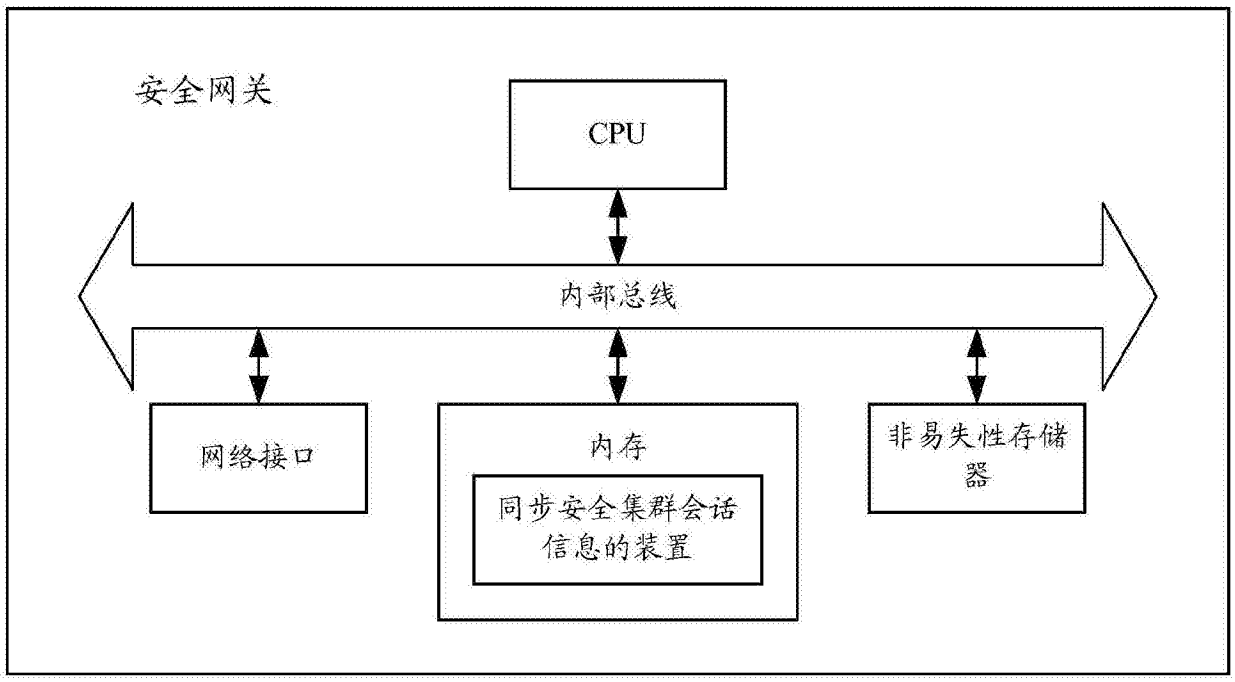

安全网关
CPU
内部总线
网络接口
内存
同步安全集群会话信息的装置
非易失性存储器

图5

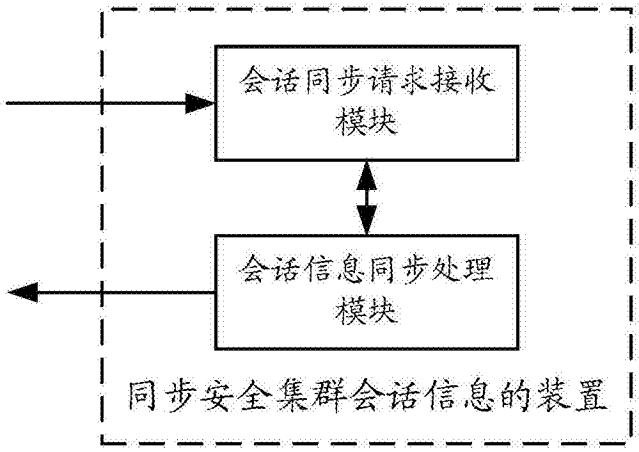

会话同步请求接收模块
会话信息同步处理模块
同步安全集群会话信息的装置

图6