[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 29/08 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200410070804.5

[43] 公开日 2006 年 1 月 25 日

[11] 公开号 CN 1725702A

[22] 申请日 2004.7.20
[21] 申请号 200410070804.5
[71] 申请人 联想网御科技（北京）有限公司
地址 100086 北京市海淀区中关村南大街 6 号中电信息大厦 801 – 810 室
[72] 发明人 刘春梅 刘永锋 王 刚 宋春雨 王 伟

[74] 专利代理机构 北京集佳知识产权代理有限公司
代理人 王学强

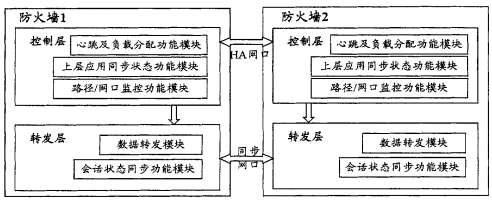
权利要求书 5 页 说明书 19 页 附图 3 页

[54] 发明名称

一种网络安全设备及其组成的实现高可用性的系统及方法

[57] 摘要

本发明公开了一种网络安全设备，用于组成具有高可用性的集群系统，该网络安全设备包含控制层和转发层。 本发明还公开了一种实现网络安全设备高可用性的系统，包括一个以上作为集群系统中集群节点的网络安全设备，每个网络安全设备包含控制层和转发层。 本发明还公开了一种实现网络安全设备高可用性的方法，该方法包括：控制层监控集群状态变化，根据集群状态信息进行负载分配，并将集群状态信息和负载分配信息下发给转发层；转发层根据控制层下发的集群状态信息和负载分配信息对数据包进行处理，并发送会话状态信息同步给同一集群系统的其它集群节点。 本发明提供的系统和方法可以实现网络安全设备的高可用性，并适应多种网络拓扑要求。



1、一种网络安全设备，用于组成具有高可用性的集群系统；其特征在于，该网络安全设备包含控制层和转发层；

所述控制层用于监控集群状态变化，进行节点配置信息的同步，根据集群状态变化进行负载分配，并将集群状态变化信息和负载分配信息下发给转发层；

所述转发层用于根据控制层下发的信息对数据包进行处理，更新会话状态信息，并进行会话状态信息的同步。

2、根据权利要求 1 所述的设备，其特征在于，所述控制层包括：心跳及负载分配功能模块和路径/网口监视功能模块；

所述路径/网口监视功能模块用于监视网络安全设备节点的状态变化，并将包含节点状态变化的信号发送给心跳及负载分配功能模块；

所述心跳及负载分配功能模块用于发送和接收心跳信号以监控集群状态变化，进行节点配置信息的同步，接收路径/网口监视功能模块发送来的包含节点状态变化的信号，根据集群状态变化和节点状态进行负载分配，并将负载分配信息下发给转发层。

3、根据权利要求 2 所述的设备，其特征在于，所述控制层进一步包括用于同步上层应用会话状态信息的上层应用同步状态功能模块。

4、根据权利要求 1、2 或 3 所述的设备，其特征在于，所述转发层包含：会话同步功能模块和数据转发模块；

所述数据转发模块用于接收控制层下发的负载分配信息，根据数据包信息和负载分配信息对数据包进行处理，并将会话状态信息发送给会话同步功能模块；

所述会话同步功能模块用于接收数据转发模块发送来的会话状态信息，并将包含会话状态信息的会话状态同步信号发送出去。

5、根据权利要求 1、2 或 3 所述的设备，其特征在于，所述控制层包含

专用的 HA 网口。

6、根据权利要求 1 所述的设备，其特征在于，所述转发层包含用于转发数据包的普通数据网口和用于同步状态信息的同步网口，同步网口为专用同步网口或普通数据网口。

7、一种实现网络安全设备高可用性的系统，包括一个以上作为集群系统中集群节点的网络安全设备；

其特征在于，每个网络安全设备包含控制层和转发层；

所述控制层用于监控集群状态变化，根据集群状态变化进行负载分配，并将集群状态变化信息和负载分配信息下发给转发层；

所述转发层用于根据控制层下发的信息对数据包进行处理，并更新会话状态信息；

所述每个网络安全设备的控制层之间通过彼此发送和接收心跳信号进行心跳通信，进行节点配置信息的同步；所述每个网络安全设备的转发层之间通过彼此发送和接收会话状态同步信号进行会话状态同步。

8、根据权利要求 7 所述的系统，其特征在于，所述网络安全设备的控制层包括：心跳及负载分配功能模块和路径/网口监视功能模块；

所述路径/网口监视功能模块用于监视网络安全设备节点的状态变化，并将包含节点状态变化的信号发送给心跳及负载分配功能模块；

所述心跳及负载分配功能模块用于发送和接收心跳信号以监控集群状态变化，进行节点配置信息的同步，接收路径/网口监视功能模块发送来的包含节点状态变化的信号，根据集群状态变化和节点状态进行负载分配，并将负载分配信息下发给转发层。

9、根据权利要求 8 所述的系统，其特征在于，所述网络安全设备的控制层进一步包括用于同步上层应用会话状态信息的上层应用同步状态功能模块。

10、根据权利要求 7、8 或 9 所述的系统，其特征在于，所述网络安全设备的转发层包含：会话同步功能模块和数据转发模块；

所述数据转发模块用于接收控制层下发的负载分配信息，根据数据包信息和负载分配信息对数据包进行处理，并将会话状态信息发送给会话同步功能模块；

所述会话同步功能模块用于接收数据转发模块发送来的会话状态信息，并将包含会话状态信息的会话状态同步信号发送出去。

11、根据权利要求 7、8 或 9 所述的系统，其特征在于，所述网络安全设备的控制层之间通过设定的专用 HA 网口相连。

12、根据权利要求 7 所述的系统，其特征在于，所述网络安全设备的转发层之间通过设定的专用同步网口或普通数据网口相连。

13、根据权利要求 7、8、9 或 12 所述的系统，其特征在于，所述网络安全设备为防火墙。

14、一种实现网络安全设备高可用性的方法，适用于由一个以上网络安全设备作为集群节点组成的集群系统，集群系统中包含一个主节点和至少一个从节点，每个集群节点包含控制层和转发层；其特征在于，该方法包括：

控制层监控集群状态变化，根据集群状态信息进行负载分配，并将集群状态信息和负载分配信息下发给转发层；

转发层根据控制层下发的集群状态信息和负载分配信息对数据包进行处理，并将会话状态信息发送给同一集群系统的其它集群节点以进行会话状态同步。

15、根据权利要求 14 所述的方法，其特征在于，所述控制层监控集群状态变化并进行负载分配的过程包括以下步骤：

A. 根据集群状态变化确定集群系统当前的主节点、节点的个数以及集群节点的工作状态；

B. 主节点根据集群工作模式和集群节点信息分配负载，将分配的负载信息通知给从节点，并更新集群节点信息。

16、根据权利要求 15 所述的方法，其特征在于，所述步骤 A 包括：

判断集群网络拓扑变化是节点加入还是节点退出，如果是节点加入，则判断当前加入节点是否检测到心跳信号，如果不是，则将把当前加入节点设置为主节点，然后执行所述步骤 B，否则将把当前加入节点设置为从节点，然后执行所述步骤 B;

如果是节点退出，则判断当前离开的节点是否是主节点，如果是，则将优先级最高的从节点设置为主节点后，然后执行所述步骤 B；否则直接执行所述步骤 B。

17、根据权利要求 15 或 16 所述的方法，其特征在于，步骤 B 中，所述主节点根据集群工作模式分配负载包括:

集群工作模式为负载均衡模式时，如果集群系统中仅包含主节点，则主节点将全部负载的 hash 值范围分配给自身，如果集群系统中包含主从节点，则主节点按照预先设定的负载分配算法分配负载 hash 值范围;

集群工作模式为双机热备模式时，将全部负载的 hash 值范围分配给主节点;

集群工作模式为链路冗余模式时，将全部负载的 hash 值范围分配给每个节点。

18、根据权利要求 14 所述的方法，其特征在于，所述转发层对收到的数据包进行处理的过程包括以下步骤:

a. 判断节点的状态是否为工作状态，如果不是，则将收到的数据包丢掉，否则执行步骤 b;

b. 转发层根据收到的数据包的信息计算数据包的 hash 值，并判断该数据包 hash 值是否落在本节点处理的 hash 值范围内，如果不是，则将该数据包丢掉；否则对数据包继续进行处理。

19、根据权利要求 18 所述的方法，其特征在于，在所述步骤 a 之前，该方法进一步包括：确定集群系统当前的集群工作模式，如果当前的集群工作模式为负载均衡模式，则直接执行步骤 b；如果当前集群工作模式为双机

热备模式，则继续执行步骤 a；如果当前集群工作模式为链路冗余模式，则对数据包继续进行处理。

20、根据权利要求 18 或 19 所述的方法，其特征在于，步骤 b 中，所述对数据包继续进行处理为：对数据包进行安全规则匹配或转发数据包。

一种网络安全设备及其组成的实现高可用性的系统及方法

技术领域

本发明涉及网络安全技术领域，特别涉及一种网络安全设备及其组成的实现高可用性的系统及方法。

背景技术

随着当今网络应用的迅猛增长，保证持续稳定的系统运行时间变得越来越重要，而防火墙作为网络安全体系的基础和保护企业网内部安全的核心控制设备，也日渐成为限制网络带宽的瓶颈和单一故障点，并极大地制约了网络的实际应用，因此，提高防火墙的高可用性和处理性能越来越受到人们的重视。

高可用性（HA）技术是指利用冗余网络设备、冗余电源、冗余协议等构建的具有高可用性的网络设备集群系统。该集群系统中的设备能自动检测网络中的故障节点或失效节点，并且当集群系统中的设备自动检测到网络中的故障节点或失效节点时，集群系统能够自动适当地重新进行配置，使集群系统中的其它节点能够自动承担故障或失效节点承载的服务，实现服务的不中断。另外，高可用性技术还可以利用集群的并行处理方法提高网络的处理性能。

防火墙常见的集群模式有三种：双机热备模式、负载均衡模式和链路冗余模式。在双机热备模式中，多个防火墙中有一个为主防火墙，其余防火墙为从防火墙，只有其中的主防火墙处于活动状态，对收到的数据包进行处理。在负载均衡模式中，多个防火墙中有一个为主防火墙，其余防火墙为从防火墙，主从防火墙都处于活动状态，共同分担网络流量。在链路冗余模式下，可以不区分主从防火墙，各防火墙都能够收到数据包并进行处理，但每个防

火墙收到的数据包并不相同，即单一数据包在同一时刻只发送给一台防火墙。

现有技术主要是在双机热备模式下实现防火墙高可用性的。该模式下，集群系统包含两台配置完全相同的防火墙，分别为主防火墙和从防火墙，主防火墙处于工作状态，从防火墙处于备份状态。当主防火墙失效时，从防火墙可以接管主防火墙的业务，保证网络连接的不间断。虽然现有技术可以采用双机热备模式实现网络业务的不中断，但无法实现多机动态负载均衡等方式，也不能适应多样的高可用性的网络拓扑的要求。另外，现有技术在实现防火墙等网络安全设备高可用性的硬件架构上尚未提出具体的实现方案。

发明内容

有鉴于此，本发明的主要目的在于提供一种实现集群系统高可用性的网络安全设备，使其能组成具有高可用性的集群系统。

本发明的另一目的在于提供一种实现网络安全设备高可用性的系统，使其能灵活设置硬件结构，实现网络安全设备的高可用性，并适应多种网络拓扑要求。

本发明进一步的目的在于提供一种实现网络安全设备高可用性的方法，使其能实现网络安全设备的高可用性，并适应多种网络拓扑要求。

为达到上述目的，本发明的技术方案是这样实现的：

本发明公开了一种网络安全设备，用于组成具有高可用性的集群系统；该网络安全设备包含控制层和转发层；

所述控制层用于监控集群状态变化，进行节点配置信息的同步，根据集群状态变化进行负载分配，并将集群状态变化信息和负载分配信息下发给转发层；

所述转发层用于根据控制层下发的信息对数据包进行处理，更新会话状态信息，并进行会话状态信息的同步。

其中，所述控制层包括：心跳及负载分配功能模块和路径/网口监视功能

模块；所述路径/网口监视功能模块用于监视网络安全设备节点的状态变化，并将包含节点状态变化的信号发送给心跳及负载分配功能模块；所述心跳及负载分配功能模块用于发送和接收心跳信号以监控集群状态变化，进行节点配置信息的同步，接收路径/网口监视功能模块发送来的包含节点状态变化的信号，根据集群状态变化和节点状态进行负载分配，并将负载分配信息下发给转发层。

所述控制层可以进一步包括用于同步上层应用会话状态信息的上层应用同步状态功能模块。

上述方案中，所述转发层包含：会话同步功能模块和数据转发模块；所述数据转发模块用于接收控制层下发的负载分配信息，根据数据包信息和负载分配信息对数据包进行处理，并将会话状态信息发送给会话同步功能模块；所述会话同步功能模块用于接收数据转发模块发送来的会话状态信息，并将包含会话状态信息的会话状态同步信号发送出去。

其中，所述控制层包含专用的 HA 网口。所述转发层包含用于转发数据包的普通数据网口和用于同步状态信息的同步网口，同步网口为专用同步网口或普通数据网口。

本发明还公开了一种实现网络安全设备高可用性的系统，包括一个以上作为集群系统中集群节点的网络安全设备；每个网络安全设备包含控制层和转发层；

所述控制层用于监控集群状态变化，根据集群状态变化进行负载分配，并将集群状态变化信息和负载分配信息下发给转发层；

所述转发层用于根据控制层下发的信息对数据包进行处理，并更新会话状态信息；

所述每个网络安全设备的控制层之间通过彼此发送和接收心跳信号进行心跳通信，进行节点配置信息的同步；所述每个网络安全设备的转发层之间通过彼此发送和接收会话状态同步信号进行会话状态同步。

其中，所述网络安全设备的控制层包括：心跳及负载分配功能模块和路径

/网口监视功能模块；所述路径/网口监视功能模块用于监视网络安全设备节点的状态变化，并将包含节点状态变化的信号发送给心跳及负载分配功能模块；所述心跳及负载分配功能模块用于发送和接收心跳信号以监控集群状态变化，进行节点配置信息的同步，接收路径/网口监视功能模块发送来的包含节点状态变化的信号，根据集群状态变化和节点状态进行负载分配，并将负载分配信息下发给转发层。

所述网络安全设备的控制层可以进一步包括用于同步上层应用会话状态信息的上层应用同步状态功能模块。

上述方案中，所述网络安全设备的转发层包含：会话同步功能模块和数据转发模块；所述数据转发模块用于接收控制层下发的负载分配信息，根据数据包信息和负载分配信息对数据包进行处理，并将会话状态信息发送给会话同步功能模块；所述会话同步功能模块用于接收数据转发模块发送来的会话状态信息，并将包含会话状态信息的会话状态同步信号发送出去。

其中，所述网络安全设备的控制层之间可以通过设定的专用 HA 网口相连。所述网络安全设备的转发层之间可以通过设定的专用同步网口或普通数据网口相连。所述网络安全设备可以为防火墙。

相应地，本发明进一步公开了一种实现网络安全设备高可用性的方法，适用于由一个以上网络安全设备作为集群节点组成的集群系统，集群系统中包含一个主节点和至少一个从节点，每个集群节点包含控制层和转发层；其特征在于，该方法包括：

控制层监控集群状态变化，根据集群状态信息进行负载分配，并将集群状态信息和负载分配信息下发给转发层；

转发层根据控制层下发的集群状态信息和负载分配信息对数据包进行处理，并将会话状态信息发送给同一集群系统的其它集群节点以进行会话状态同步。

其中，所述控制层监控集群状态变化并进行负载分配的过程可以包括以

下步骤:

A. 根据集群状态变化确定集群系统当前的主节点、节点的个数以及集群节点的工作状态;

B. 主节点根据集群工作模式和集群节点信息分配负载，将分配的负载信息通知给从节点，并更新集群节点信息。

其中，所述步骤 A 可以包括：判断集群网络拓扑变化是节点加入还是节点退出，如果是节点加入，则判断当前加入节点是否检测到心跳信号，如果不是，则将把当前加入节点设置为主节点，然后执行所述步骤 B，否则将把当前加入节点设置为从节点，然后执行所述步骤 B;

如果是节点退出，则判断当前离开的节点是否是主节点，如果是，则将优先级最高的从节点设置为主节点后，然后执行所述步骤 B；否则直接执行所述步骤 B。

步骤 B 中，所述主节点根据集群工作模式分配负载可以包括:

集群工作模式为负载均衡模式时，如果集群系统中仅包含主节点，则主节点将全部负载的 hash 值范围分配给自身，如果集群系统中包含主从节点，则主节点按照预先设定的负载分配算法分配负载 hash 值范围；集群工作模式为双机热备模式时，将全部负载的 hash 值范围分配给主节点；集群工作模式为链路冗余模式时，将全部负载的 hash 值范围分配给每个节点。

上述方案中，所述转发层对收到的数据包进行处理的过程包括以下步骤:

a. 判断节点的状态是否为工作状态，如果不是，则将收到的数据包丢掉，否则执行步骤 b;

b. 转发层根据收到的数据包的信息计算数据包的 hash 值，并判断该数据包 hash 值是否落在本节点处理的 hash 值范围内，如果不是，则将该数据包丢掉；否则对数据包继续进行处理。

其中，在所述步骤 a 之前，该方法可以进一步包括：确定集群系统当前

的集群工作模式，如果当前的集群工作模式为负载均衡模式，则直接执行步骤 b；如果当前集群工作模式为双机热备模式，则继续执行步骤 a；如果当前集群工作模式为链路冗余模式，则对数据包继续进行处理。其中，所述对数据包继续进行处理可以为：对数据包进行安全规则匹配或转发数据包。

由上述方案可以看出，本发明的关键在于：本发明提供的系统由多个集群节点组成，每个集群节点均包含控制层和转发层；控制层负责监控集群状态，向转发层通告集群状态的变化。转发层负责根据控制层下发的信息对收到的数据包进行处理，并同步节点会话状态。本发明提供的方法包括控制层根据网络拓扑变化进行负载分配的过程和转发层对收到的数据包进行处理的过程。

因此，本发明所提供的这种实现集群系统高可用性的网络安全设备以其组成的高可用性的系统及方法，在系统硬件设计上灵活多变，控制层与转发层可以灵活设置，并且分层处理可以使各层的任务单一，每层可以独立处理自己的专项任务，保证数据包的转发速度。本发明还可以构建高可用性的负载均衡集群，双机热备集群，链路冗余集群，扩大了 HA 拓扑环境的工作模式。集群中的网络安全设备可以全部处于工作状态，进行动态的负载分摊，也可以分别处于工作和备份的状态。通过选择负载均衡的集群工作模式，本发明提供的防火墙集群不但可以在各防火墙节点之间均衡用户负载，还可以消除防火墙作为网络设备可能出现的单点故障，即在防火墙上进行无缝式切换和动态负载均衡。这样，当一台防火墙出现故障后，集群系统中其它防火墙会接管出现故障防火墙的所有网络会话，网络会话不会被中断。

附图说明

图 1 为本发明实现防火墙高可用性的系统结构示意图；

图 2 为本发明根据网络拓扑变化进行负载均衡的方法实现流程图；

图 3 为本发明转发层对数据包进行处理的方法实现流程图；

图 4 为负载均衡模式下的防火墙高可用性系统结构示意图；

图 5 为双机热备模式下的防火墙高可用性系统结构示意图；

图 6 为链路冗余模式下的防火墙高可用性系统结构示意图。

具体实施方式

下面结合附图及具体实施例对本发明再作进一步详细的说明。

本发明提供的实现集群系统高可用性的网络安全设备包含控制层和转发层。基于这样的网络安全设备，本发明提供的系统是一个由多个上述网络安全设备组成的集群系统，该系统的每个集群节点就是一个网络安全设备，每个网络安全设备均包含控制层和转发层。其中，控制层负责监控集群状态，向转发层通告集群状态的变化。转发层负责根据控制层下发的信息对收到的数据包进行处理，并同步节点会话状态。相应地，本发明提供的方法包括控制层根据网络拓扑变化进行负载均衡的过程和转发层对收到的数据包进行处理的过程。

下面以网络安全设备是防火墙为例说明本发明。本实施例中，防火墙就是集群系统中的集群节点，所组成的集群系统可以称为防火墙集群。

本发明实现防火墙高可用性的系统可以应用于多种工作模式下，包括负载均衡模式、双机热备模式和链路冗余模式。下面以负载均衡模式为例详细说明本发明实现防火墙高可用性的系统。

图 1 为本发明负载均衡模式下实现防火墙高可用性的系统结构示意图，包括两个防火墙，防火墙 1 和防火墙 2，每个防火墙均包含控制层和转发层。其中，控制层用于监控整个防火墙集群的状态，并将集群状态的变化等信息下发给转发层；控制层还用于根据集群的状态等信息进行动态负载 hash 值分配，并将获得的 hash 值分配范围下发给转发层；控制层之间发送和接收心跳信号，进行节点配置同步和状态同步。转发层用于接收控制层下发的集群状态变化等信息，并根据收到的信息对收到的数据包进行处理或丢弃；转发层之间进行会话状态同步。控制层可以与转发层置于同一个硬件板上，也可以分开单独置于不同的硬件板上，甚至可以用一台单独的计算机来实现。

本实施例中，控制层之间可以通过专用的HA网口进行信息交互，即集群中的各防火墙节点通过HA网口进行心跳通信，实时监测各防火墙节点的状态。另外，控制层之间进行心跳通信的HA网口也用于控制层之间的集群状态信息的同步。转发层之间通过同步网口进行信息交互，同步网口可以采用专用的网口，也可以采用普通的数据网口。

如图1所示，控制层之间通过HA网口发送和接收心跳信号来监测整个防火墙集群的状态和网络拓扑的变化，根据集群的状态、集群节点的状态信息和预先配置的负载均衡算法重新分配各节点处理的负载 hash 值范围，并向转发层下发集群的状态信息和节点处理的负载 hash 值范围等信息；转发层根据控制层下发的集群系统的状态信息和节点处理的负载 hash 值范围等信息对数据包进行处理，并通过同步网口发送会话状态同步信息给同一集群的其它节点的转发层。

其中，当设备刚启动时，控制层向转发层下发的信息包括：机群 ID、节点 ID、节点优先级、集群工作模式、本节点的工作状态、网络拓扑变化的序号、本节点处理数据包的hash值范围和用于转发层同步的网口。其中，机群ID用于标识该节点所在的集群，节点ID用于标识该集群中的节点。节点优先级由启动顺序决定，优先级最高的节点为主节点。集群工作模式包括负载均衡模式、双机热备模式和链路冗余模式。本节点的工作状态为工作状态或备份状态。网络拓扑变化的序号在集群刚启动时为1，集群拓扑每变化一次，网络拓扑变化的序号加1，集群节点个数、各集群节点的优先级以及各集群节点的资源使用情况都可能引起网络拓扑的变化。本节点处理数据包的 hash 值范围由控制层根据集群工作模式与节点信息进行分配。用于转发层同步的网口是由管理员配置的，转发层根据该设置将会话同步信息通过该网口转发给其它节点的转发层。上述信息中，机群ID、节点ID、节点优先级、集群工作模式、集群节点的工作状态和网络拓扑变化信息均可称为集群状态信息。

当有节点离线或新的节点加入时，控制层监测到网络拓扑的变化后，就会修改已存入转发层的信息。修改的信息包括：节点优先级、本节点的工作状态、网络拓扑变化的序号以及由控制层重新分配的本节点处理数据包 hash 值范围。

转发层对收到的数据包进行处理的具体过程为：如果当前的集群工作模式为负载均衡模式或链路冗余模式，则转发层根据收到的数据包的信息计算数据包的 hash 值，并判断计算得到的数据包的 hash 值是否落在本节点处理的范围内，如果没有落在本节点 hash 值范围内，则把该数据包丢掉，如果落在本节点 hash 值范围内，则继续处理。继续处理可以包括安全规则匹配和数据转发等。如果当前集群工作模式为双机热备模式，则转发层判断本节点的工作状态是否为有效处理状态，如果处于备份状态，则把数据包丢掉，如果是工作状态，则根据收到的数据包的信息计算数据包的 hash 值，并判断计算得到的数据包的 hash 值是否落在本节点处理的范围内，如果没有落在本节点 hash 值范围内，则把该数据包丢掉，如果落在本节点 hash 值范围内，则继续处理。

转发层还根据收到的网络拓扑变化的序号判断网络状态是否改变，如果网络拓扑变化的序号发生改变，则说明网络状态发生改变，比如新节点加入，或节点离线，这时，转发层之间就会通过控制层下发的用于转发层同步的网口进行状态同步。

下面以负载均衡模式为例详细说明控制层和转发层所包含的各个功能模块。

控制层包含心跳及负载分配功能模块和路径/网口监视功能模块。其中，节点控制层心跳及负载分配功能模块通过 HA 网口发送和接收心跳信号，并根据是否收到心跳信号来判断节点是否在线或离线。

在负载均衡模式下，整个集群包含一个主节点和至少一个从节点。所有节点都包含在集群节点状态表中，优先级最高，比如优先级为 1 的节点为主

节点，负责控管整个集群系统。主节点周期性地将自己的心跳 alive 信号传播给各从节点，从节点也周期性地将自己的心跳 alive 信号传播给主节点。

如果主节点在规定时间没有收到某一从节点的心跳 alive 信号，则认为该从节点已经离线，主节点会从集群节点状态表中删除该节点，同时更新节点状态表中各节点的信息，比如节点优先级等，然后将该信息通过同步节点状态表信号发送给从节点。如果主节点离线了，优先级为 2 的从节点在规定时间内没有收到主节点的心跳 alive 信号，认为主节点已经离线，该节点会自动升为主节点来控管整个集群，删除自身集群节点状态表中原来的主节点。同样地，主节点更新集群节点状态表，并将集群节点状态表同步给从节点。

每次有节点加入集群或离开集群，主节点都会重新调整集群中各节点的网络负载。主节点控制层心跳及负载分配功能模块根据当前集群中的节点个数，节点优先级、节点资源等信息，以及预先配置的负载均衡算法分配各节点处理数据包的 hash 值范围。主节点通过 HA 网口向从节点发送同步负载信号将各节点处理的 hash 值范围通知给从节点。从节点收到同步负载信号后，将获得的 hash 值范围下发给各自对应的转发层。

集群节点控制层心跳及负载分配功能模块还通过发送同步配置信号保证各节点的配置信息相同。在一组实施相同的整体安全策略并且共享相同配置的防火墙集群系统中，当一台防火墙节点新加入集群系统时，集群中的主防火墙节点会向该新加入的防火墙节点发送同步配置信号对其进行自动配置同步。如果在集群正常运转中，管理员对主防火墙节点配置进行了更改，主防火墙节点也会将发生的任何更改通过同步配置信号同步给其它所有从防火墙节点。同样地，如果管理员对从防火墙节点的配置进行了更改，从防火墙节点也会将发生的任何更改通过同步配置信号同步给其它节点，包括主节点。这样保证了集群系统中的各防火墙节点保持相同的配置信息。其中，配置信息包括节点的 IP 地址、采用的安全规则等。

另外，集群中的主节点控制层的心跳及负载分配功能模块周期性地广播自身的系统时间给集群中的从节点，从节点收到同步时间信号后更新自身的系统时间。上述的同步配置信号、同步负载信号、同步时间信号均可作为心跳信号的一部分，通过 HA 网口进行传递。

控制层路径/网口监视功能模块用于监视集群节点是否失效或复活，并将失效或复活信息发送给心跳及负载分配功能模块。心跳及负载分配功能模块将失效或复活信息通过心跳信号发送向外广播给其它集群节点。其它集群节点收到包含失效或复活信息的心跳信号后，主动更新节点状态表，并由主节点调节各节点的网络负载，通知其它节点接管重新分配的网络负载。其中，节点失效可以作为节点退出的一种形式，节点复活可以作为节点加入的一种形式。

控制层路径/网口监视功能模块用于监控节点的状态变化，即节点的失效和复活，具体包括：对链路层的网口的监控和对网络层的周边设备 IP 的监控。链路层的网口监控主要是检查防火墙设备的物理网口是否处于活动状态并连接到周边网络设备。防火墙管理员可以定义需要监控的网口，网口的状态会根据网口是否处于活动状态并连接到周边网络设备而成为 Link Down 状态和 Link Up 状态，这样，就可以根据网口的状态判断该防火墙节点是有效状态还是失效状态。如果网口的监控结果是 Link Down 状态，则该防火墙节点将进入失效状态；如果网口的监控结果是 Link Up 状态，则该防火墙节点将从失效状态重新转变为有效状态。

网络层的周边设备 IP 监控主要是向指定的 IP 地址以固定的间隔发送 ARP 请求，监控周边设备是否响应，并根据 IP 监控总故障数判断该防火墙节点是否失效或有效。如果一个防火墙节点的 IP 监控总故障数超过预先设置的该节点的故障切换临界值，则该防火墙节点将进入失效状态。如果监控 IP 总故障数不再超过故障切换临界值，则该防火墙节点将失效状态重新转变为有效状态。节点从失效状态转变为有效状态就是节点的复活。

另外，控制层还包含上层应用的状态同步模块，其中的状态同步主要是针对动态协议。比如，客户机每次进行视频会议或访问 FTP 服务之前，需要动态地协商每次连接所采用的端口。协商后的连接端口在控制层获得，并由处理的节点通过 HA 网口同步给其它节点。

转发层包含会话同步功能模块和数据转发模块。其中，会话同步功能模块用于进行会话的同步。防火墙节点在处理网络会话时，会建立相应的会话状态表来维护和处理该网络会话的所有数据帧。为了防止集群中离线或失效的防火墙节点正在处理的网络会话全部丢失，节点之间需要进行高效率的链路层实时会话同步。也就是说，一旦集群系统中任何节点有新的网络会话建立，该节点会将新的网络会话状态同步到集群系统中其它节点；一旦集群系统中任何节点有网络会话消失，该节点会将消失的网络会话同步到集群系统中其它节点。

各设备的转发层根据会话进行的程度以及通信的协议类型和集群的工作模式来确定会话状态信息的同步时机，并在该同步时机将会话状态信息同步到其它节点，以确保会话在节点间迁移时不中断。同步的会话状态表内容主要包括源 IP、源端口、目的 IP、目的端口、协议、当前连接的状态以及其它信息，比如，作地址转换时转换后的 IP 地址。本实施例中，会话同步可以由数据流驱动，通过广播的形式将节点会话状态同步到其它节点，这样可以避免瞬时对设备处理能力的大量占用，同时又能最大限度地保证状态的同步。

数据转发模块用于接收控制层下发的本节点处理数据包的hash值范围，并根据收到的数据包的信息计算数据包的 hash 值，将该本节点处理数据包的 hash 值范围与计算得到的 hash 值进行比较，然后根据比较结果将数据包丢弃或继续处理。比如，数据转发模块首先根据收到的数据包的五元组信息计算数据包的 hash 值，然后判断该 hash 值是否落在控制层分配的本节点处理的 hash 值范围内，如果是，则继续处理该数据包，否则将该数据包丢弃。

其中，数据包的五元组信息包括数据包的源 IP 地址、目的 IP 地址、源端口、目的端口和传输协议。

与负载均衡模式相比，双机热备模式和链路冗余模式下，控制层的集群状态监控功能和转发层的会话状态同步功能与负载均衡模式是类似的，但对于双机热备模式，网络负载全部由主节点承担，从节点的退出或加入不影响网络负载的分配，当主节点退出时，从节点变成新的主节点接管全部网络流量即可；对于链路冗余模式，可以不区分主节点和从节点，也可以将首先加入集群的节点作为主节点，其次加入集群的节点作为从节点，该模式下所有的节点均处理流经自身的网络流量。

或者也可以这样认为：对于双机热备模式，控制层将全部网络流量的 hash 值范围下发给主节点的转发层，不向从节点的转发层下发 hash 值范围或者下发的 hash 值范围为空；对于链路冗余模式，控制层将全部网络流量的 hash 值范围下发给每个节点的转发层。

基于上述实现网络安全设备高可用性的系统，本发明实现网络安全设备高可用性的方法包括：

控制层之间发送和接收心跳信号来监测整个防火墙集群的状态和网络拓扑的变化，根据集群的状态、集群节点的状态信息和预先配置的负载均衡算法重新分配负载 hash 值范围，并将集群的状态信息和节点处理的负载 hash 值范围等信息下发给转发层；

转发层根据控制层下发的集群系统的状态信息和节点处理的负载 hash 值范围等信息对数据包进行处理，并发送会话状态同步信息给同一集群的其它节点的转发层。

上述方法具体可以包括：图 2 所示的控制层根据网络拓扑变化进行负载均衡的过程和图 3 所示的转发层对收到的数据包的处理过程。

如图 2 所示，控制层根据网络拓扑变化进行负载均衡的过程包括以下步骤：

步骤 201、判断网络拓扑变化是节点加入还是节点退出，如果节点加入，则继续执行步骤 204；如果节点退出，则继续执行步骤 202；

步骤 202～203、判断当前退出的节点是否是主节点，如果是，则优先级最高的从节点成为新的主节点，并继续执行步骤 207，否则直接执行步骤 207。

步骤 204～206、当前加入的节点判断是否检测到其它设备的心跳信号，如果不是，则把自己设置成主设备，并接管网络全部流量，更新集群节点状态表信息；否则把自己设置成从设备，执行步骤 207。

步骤 207、主节点重新分配负载，将分配的负载信息通知给从节点，并更新集群节点信息。集群节点状态表信息包括：节点 ID、节点个数、节点优先级等。

上述方案中，不同的集群工作模式在具体处理时并不完全相同。负载均衡模式下，其处理过程与上述过程基本相同。在节点退出时，如果是双机热备模式，则判断当前退出的节点是否是主节点，如果是，则优先级最高的从节点成为主节点，并接管网络全部流量，否则更新集群节点状态表信息。如果是链路冗余模式，则直接更新集群节点状态表信息。

在节点加入时，如果是双机热备模式，则当前加入的节点判断是否检测到其它设备的心跳信号，如果不是，则把自己设置成主设备，并接管网络全部流量；否则把自己设置成从设备，并更新集群节点状态表信息。如果是链路冗余模式，则节点更新集群节点状态表信息，并主动处理流经自身的流量，这是由于该模式下的网络环境包含具有负载均衡功能的路由器或交换机，该模式下各节点所处理的负载范围已经由路由器或交换机分配好了。

如图 3 所示，转发层对接收到的数据包的处理过程包括以下步骤：

步骤 301～302、判断当前的集群工作模式是哪种工作模式：负载均衡模式、双机热备模式或链路冗余模式，如果是负载均衡模式，则执行步骤 304；如果是双机热备模式，则转发层判断本节点的工作状态是否为有效处

理状态，如果是处于备份状态，则执行步骤303，如果是处于工作状态，则继续执行步骤304；如果是链路冗余模式，则继续执行步骤306；

步骤303、将该数据包丢掉，结束流程；

步骤304～305、转发层根据收到的数据包的信息计算数据包的hash值，并判断计算得到的数据包的hash值是否落在本节点处理的hash值范围内，如果没有落在本节点处理的hash值范围内，则执行步骤303，如果落在本节点处理的hash值范围内，则继续执行步骤306；

步骤306、对数据包继续进行处理。其中，对数据包继续进行处理可以包括对数据包进行安全规则匹配和将数据包转发等。

下面分别以负载均衡模式、双机热备模式和链路冗余模式三种集群工作模式为例具体说明本发明系统及方法的工作原理。

一、负载均衡模式：

在负载均衡模式下，集群中所有节点的任意对应的业务网口IP和MAC地址都分别相同，各节点协同工作，对用户的负载进行均衡，不需要额外的负载均衡器。其中，优先级为1的防火墙是主节点，处于工作状态，根据负载均衡算法处理部分网络流量以及整个集群的控管；其它防火墙节点为从节点，也处于工作状态，与主节点一起分担网络流量。一旦某一防火墙节点发生故障后，其负载可以根据负载均衡算法迅速切换到集群中其它防火墙上，保证网络正常通信。

如图4所示，在负载均衡模式下，本发明实现防火墙高可用性的系统包括两个防火墙，分别为防火墙1和防火墙2。其中，外部Internet网络通过路由器和外部交换机与防火墙相连，受防火墙保护的内部网络信任区段通过内部交换机与防火墙相连。受防火墙保护的内部网络通常会包含几个信任区段，信任区段内包含若干个主机。不同的信任区段可以与同一内部交换机相连，也可以与不同内部交换机相连。路由器之间通过虚拟路由冗余协议（VRRP）进行信息交互，交换机之间通过Trunk口相连，防火墙之间通过

心跳线相连。

本发明实现防火墙高可用性的方法包括:

1、防火墙管理员预先对集群设备分别进行配置，将集群工作模式配置为负载均衡模式，并重新启动集群设备。

2、当第一台设备启动时，第一台设备的控制层检测不到其它设备的心跳信号，则将把自身设置成主设备，接管全部的网络流量，并将该信息下发给转发层，让它处理全部流量。

3、当第二台设备启动时，第二台设备的控制层检测到主设备的心跳信号，则将自身设置成从设备，同时主设备控制层也检测到从设备的心跳信号，就重新进行负载分配，将自己承担的负载分一半给从设备，并通过同步负载信号通知从设备接管分得的流量。两台设备的控制层分别把负载变化后的本节点处理的 hash 值范围下发给各自的转发层，转发层分别根据计算得到的数据包的 hash 值和本节点处理的 hash 值范围内对数据包进行处理。转发层之间通过同步网口互相同步自己的会话状态。

如果有第三台设备加入，同样地，如果第三台设备的控制层检测到主设备的心跳信号，则将自身设置为从设备，同时主设备控制层也检测到第三台设备的存在，则主设备重新进行负载分配，把自己承担的负载的三分之一和第二台设备承担的负载的三分之一分配给第三台设备，并通过同步负载信号通知第二台设备按照新的负载分配范围承载负载，通知第三台设备接管分得的流量。同时，每台设备把自己承载的负载范围的变化情况下发给各自的转发层，转发层分别根据计算得到的数据包的 hash 值和本节点处理的 hash 值范围内对数据包进行处理。转发层之间同步各自处理的会话状态。如果有更多的集群设备加入，其工作原理与上述过程是类似的。

4、当有一台集群设备失效或退出时，如果该集群设备是从设备，则主设备重新进行负载分配，自动把失效设备的负载重新分配给工作中的设备。如果失效的设备是主设备，则优先级最高的从设备升为主设备。新的主设备

进行负载分配，把失效主设备的负载重新分配给剩下的设备。每台设备的控制层各自向自身对应的转发层下发重新分配的本节点处理的 hash 值范围，转发层分别根据计算得到的数据包的 hash 值和本节点处理的 hash 值范围内对数据包进行处理。类似地，转发层进行会话状态同步。

可见，每台网络中的设备只处理一部分数据，进行动态的负载分摊，不需要额外的负载均衡器。

二、双机热备模式：

在双机热备模式下，集群中所有节点的任意对应的业务网口 IP 和 MAC 地址都分别相同。其中优先级为 1 的防火墙为主节点，处于工作状态，负责处理所有的网络数据流以及整个集群的控管；其它防火墙节点为从节点，处于热备份状态，不处理网络数据，但处理主节点广播发出的同步状态表信号。一旦主节点发生故障，优先级次之的从节点升为主节点，接管原来主节点的工作，保证网络正常通信。

如图 5 所示，在双机热备模式下，本发明实现防火墙高可用性的系统包括两个防火墙，分别为防火墙 1 和防火墙 2。其中，外部 Internet 网络的数据包通过路由器到达交换机，交换机将数据包发送给防火墙，进行处理后再发送回交换机，交换机将数据包发送给受防火墙保护的内部网络信任区段的用户。防火墙之间通过心跳线相连。本发明实现防火墙高可用性的方法包括：

1、防火墙管理员预先对集群设备分别进行配置，将集群工作模式配置为双机热备模式，并重新启动集群设备。

2、当第一台设备启动时，第一台设备的控制层检测不到其它设备的心跳信号，则把自己设置成主设备，将全部的网络流量分配给自身，并通知转发层自己为主设备，让它处理全部流量。转发层处理全部流量，并把自己处理的会话的状态同步出去。

3、当第二台设备启动时，第二台设备控制层检测到主设备的心跳信号，则把自己设置成从设备，将自身设置为备份状态，并通知转发层自己为从设

备。第二台设备的转发层不处理网络流量，并将主设备发送来的会话状态保存在自己的会话状态表中。

4、当有一台集群设备失效时，如果该集群设备是从设备，则不影响主设备对数据包的处理；如果该集群设备是主设备，则从设备变为主设备，接管所有的网络流量。由于会话状态已事先同步，所以会话可以不间断地迁移。

三、链路冗余模式：

链路冗余模式主要应用在已经具有负载均衡功能的路由器或交换机的网络环境中，或者应用在通过生成树协议（STP）、开放最短路径优先协议（OSPF）或增强内部网关路由协议（EIGRP）等协议自动选择路径的网络环境中。集群中所有节点都处于工作状态，负责处理流经自身节点的网络数据流。一旦链路冗余模式下的任何一条链路的防火墙节点发生故障，另外一条链路的防火墙节点会接管失效链路的会话，保证网络正常通信。

如图 6 所示，在链路冗余模式下，本发明实现防火墙高可用性的系统包括两个防火墙，分别为防火墙 1 和防火墙 2，防火墙之间通过心跳线相连。网络本身通过 EIGRP 协议自动选择网络链路或通过路由的设定选路，网络中任何一个设备的失效都不会导致连接的中断。

本发明实现防火墙高可用性的工作的方法包括：

1、防火墙管理员预先对集群设备分别进行配置，将集群工作模式配置为链路冗余模式，并重新启动集群设备。

2、两台集群设备启动之后分别把自身设置成工作状态，两台集群设备的控制层分别把本节点的状态信息和集群工作模式下发给转发层，转发层对收到的所有数据包进行处理。转发层之间互相同步会话状态。

3、当一台集群设备失效后，选路协议会自动选择另外一条路径，由于另外一条路径的防火墙上有失效路径防火墙上的全部状态信息，所以连接可以不间断地迁移。

本发明提供的实现网络安全设备高可用性的系统及方法还可用于 VPN，

交换机，路由器，服务器集群等其它需要高可用性的设备集群中，其工作原理与防火墙高可用性的实现原理是类似的。

总之，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，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。

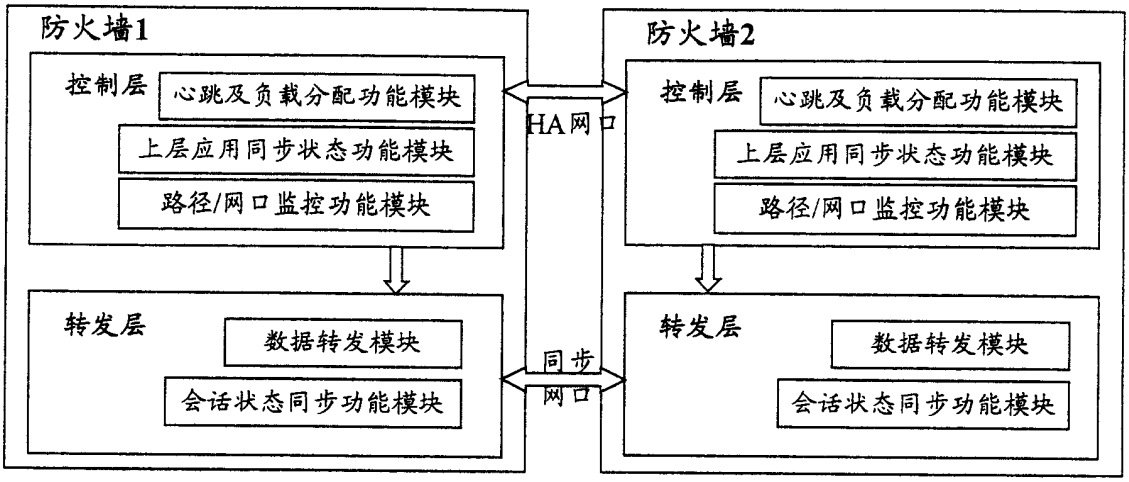

防火墙1
控制层
心跳及负载分配功能模块
上层应用同步状态功能模块
路径/网口监控功能模块
转发层
数据转发模块
会话状态同步功能模块
HA网口
同步网口
防火墙2
控制层
心跳及负载分配功能模块
上层应用同步状态功能模块
路径/网口监控功能模块
转发层
数据转发模块
会话状态同步功能模块

图 1

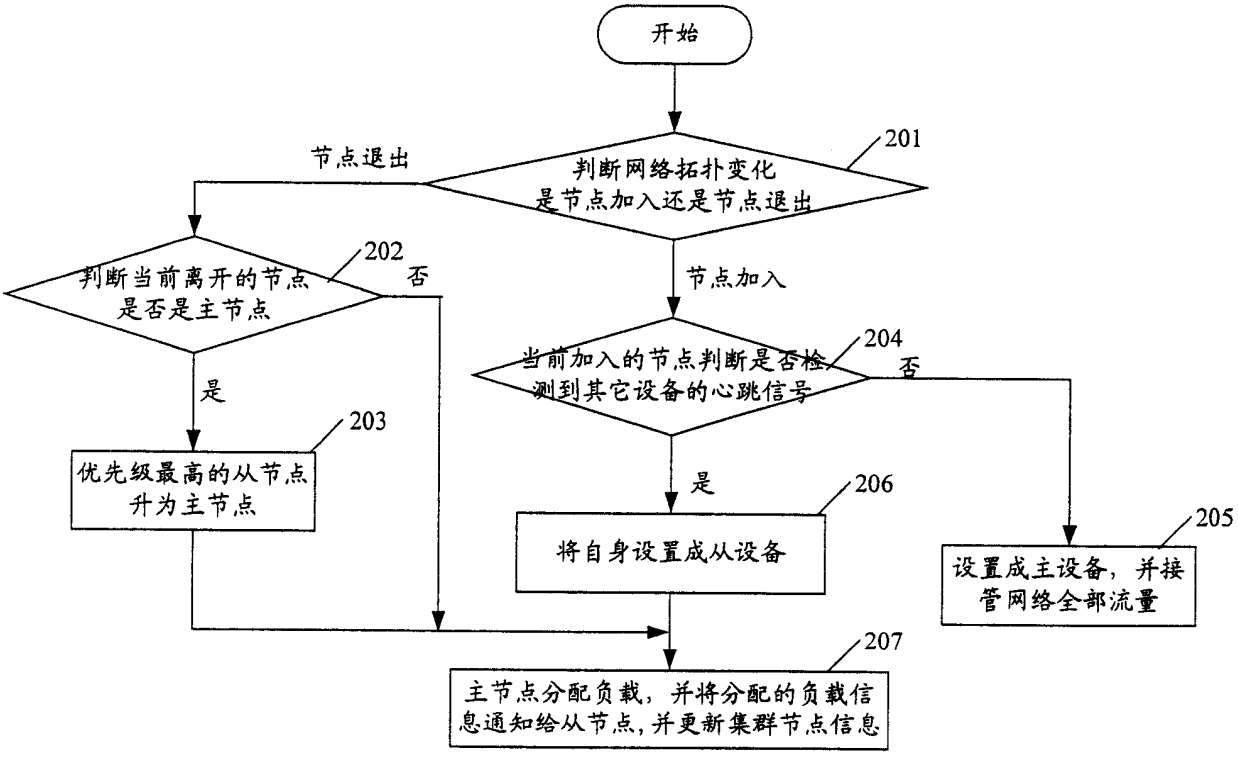

开始
判断网络拓扑变化
是节点加入还是节点退出
201
节点退出
节点加入
判断当前离开的节点
是否是主节点
202
否
是
优先级最高的从节点
升为主节点
203
当前加入的节点判断是否检
测到其它设备的心跳信号
204
否
是
将自身设置成从设备
206
设置成主设备，并接
管网络全部流量
205
主节点分配负载，并将分配的负载信
息通知给从节点，并更新集群节点信息
207

图 2

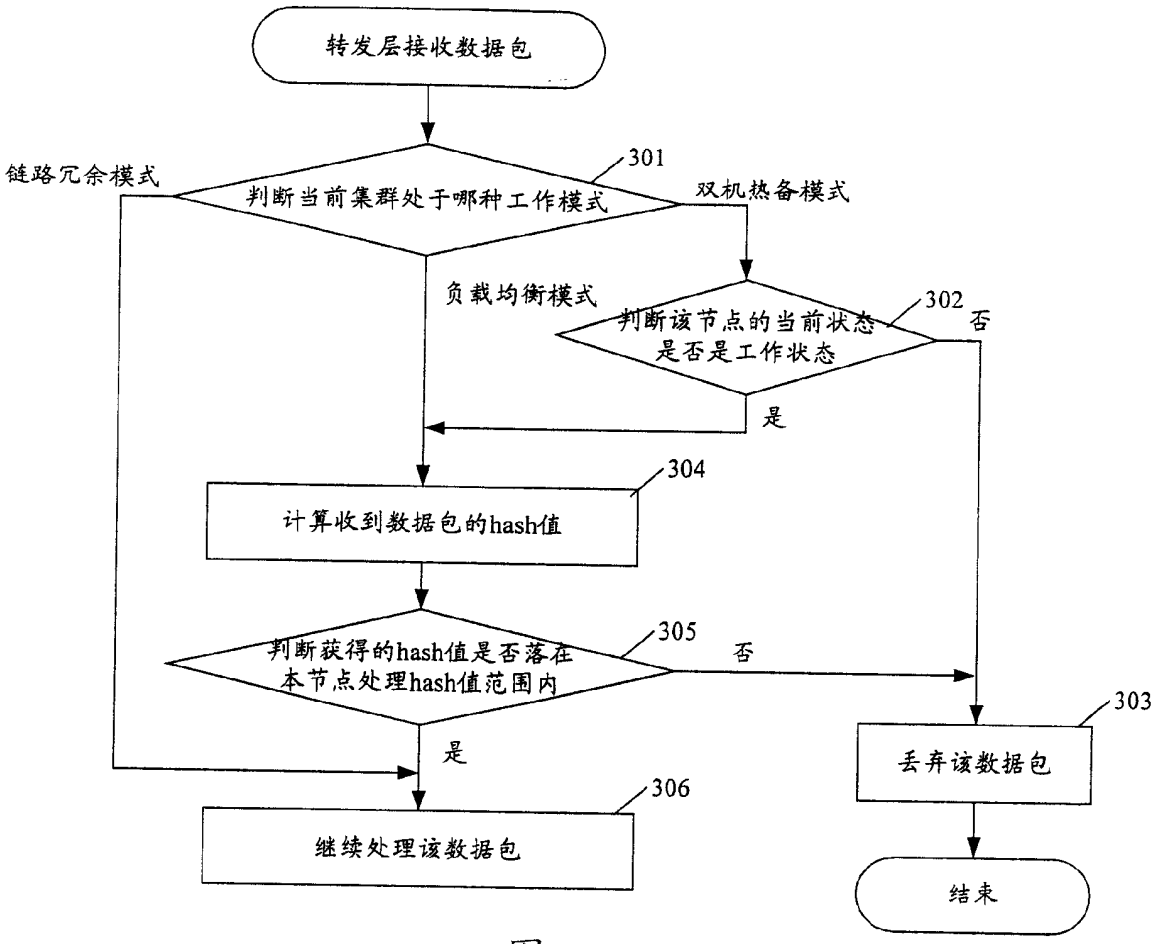

转发层接收数据包
301
判断当前集群处于哪种工作模式
链路冗余模式
双机热备模式
负载均衡模式
302
判断该节点的当前状态是否是工作状态
否
是
304
计算收到数据包的hash值
305
判断获得的hash值是否落在本节点处理hash值范围内
否
是
303
丢弃该数据包
306
继续处理该数据包
结束

图 3

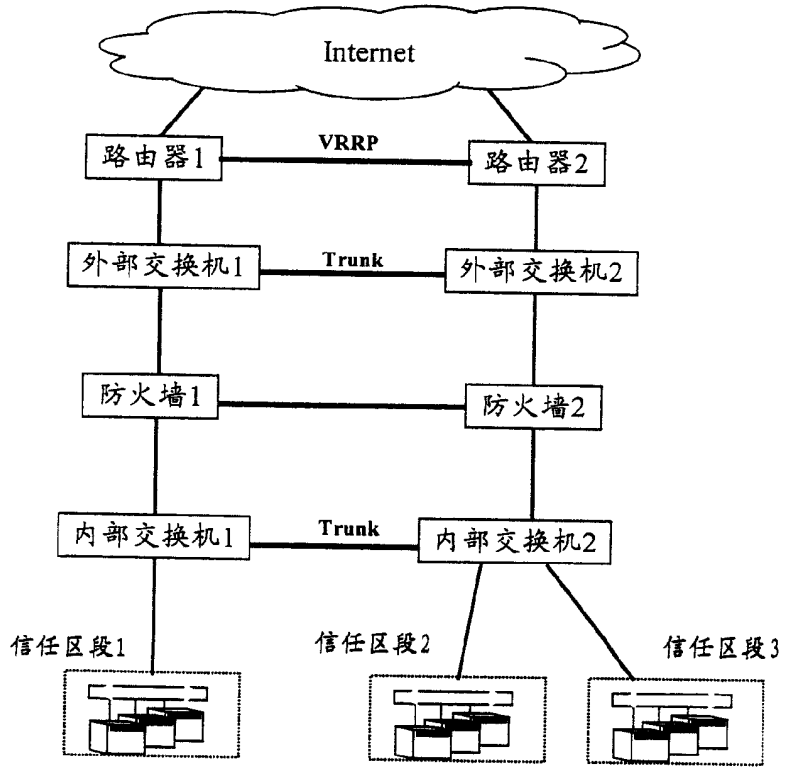

Internet
路由器1
VRRP
路由器2
外部交换机1
Trunk
外部交换机2
防火墙1
防火墙2
内部交换机1
Trunk
内部交换机2
信任区段1
信任区段2
信任区段3

图 4

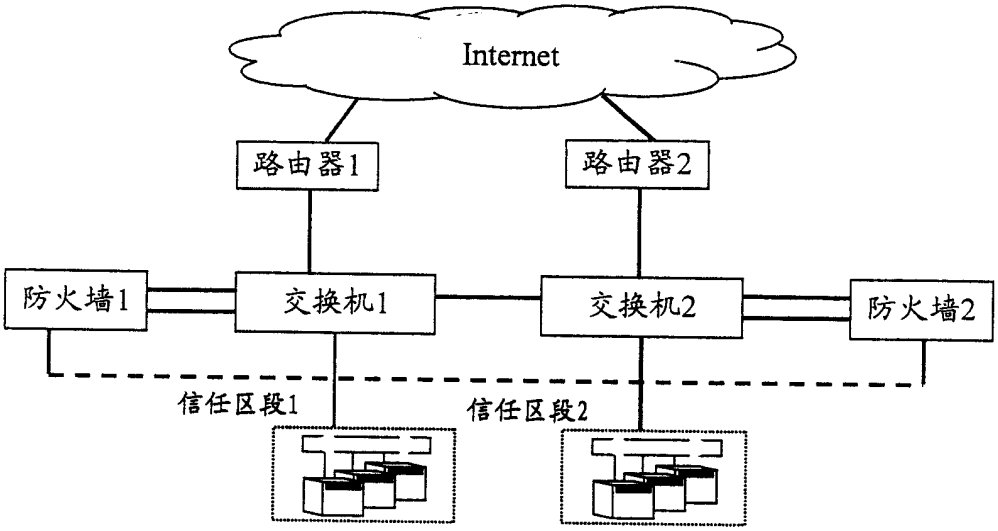

Internet
路由器1
路由器2
防火墙1
交换机1
交换机2
防火墙2
信任区段1
信任区段2

图 5

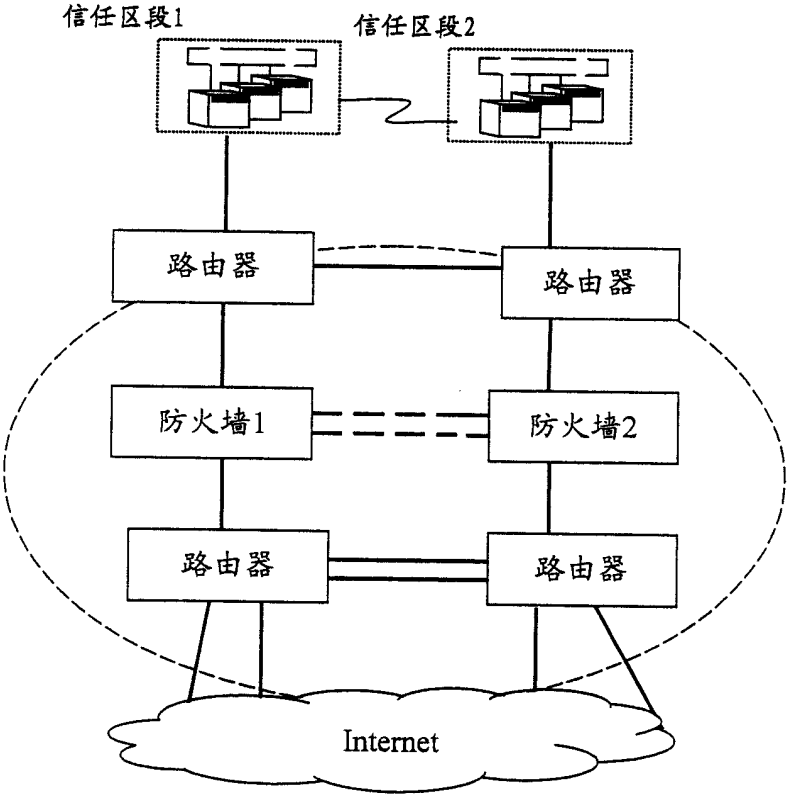

信任区段1
信任区段2
路由器
路由器
防火墙1
防火墙2
路由器
路由器
Internet

图 6