(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 102065021 B
(45)授权公告日 2012.12.26

(21)申请号 201110031342.6
(22)申请日 2011.01.28
(73)专利权人 北京交通大学
地址 100044 北京市海淀区上园村 3 号
(72)发明人 周华春 洪毅清 张宏科 易李 刘颖 汤春玲 任飞
(74)专利代理机构 北京正理专利代理有限公司 11257
代理人 张雪梅
(51)Int.Cl.
H04L 12/56(2006.01)
H04L 12/46(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 101222512 A,2008.07.16,
US 2003018889 A1,2003.01.23,
US 2005289311 A1,2005.12.29,
WO 03007524 A2,2003.01.23,
易李等．在 Click 平台上实现 IPSec/ESP 隧道通信．《铁路计算机应用》.2010, 第 19 卷（第 11 期）,38-41.
审查员 高静

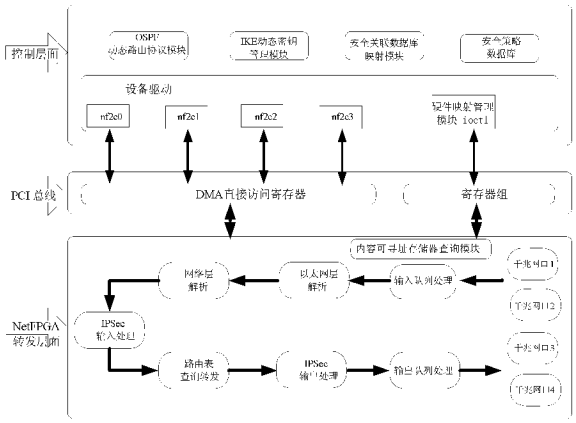
权利要求书 3 页 说明书 7 页 附图 2 页

(54)发明名称

基于 NetFPGA 的 IPSecVPN 实现系统及方法

(57)摘要

本发明涉及一种基于 NetFPGA 的 IPSec VPN 实现系统及方法，本发明在路由器的控制层面添加 IKE 模块，安全关联数据库映射模块和安全策略数据库，密钥管理模块，用于动态管理密钥、安全关联和安全策略；在转发层面充分利用 NetFPGA 开发板的模块化可重用思想，在原有 NetFPGA 的标准路由器架构中，增加了两个独立设计的 IPSec 输入和输出处理模块。该方案既能硬件实现数据流的路由转发功能，又能硬件实现 IPSec VPN 所要求的大部分计算功能，例如安全解封装载荷和完整性认证，能够有效地兼顾数据流的转发性能和 IPSec 协议处理性能。



CN 102065021 B

1. 一种基于 NetFPGA 的 IPSec VPN 实现系统，其特征在于：该系统包括控制层面和转发层面，所述的控制层面和转发层面之间通过 PCI 总线进行连接；

所述的控制层面包括：

OSPF 动态路由协议模块：用于运行管理 OSPF 动态路由协议，完成对路由表的实时动态地更新，并调用硬件映射模块将路由表映射进 NetFPGA 硬件平台的内容可寻址存储器；

IKE 动态密钥管理模块：用于完成路由器间的安全关联的动态管理，处理通信实体的配置信息，协商相关的安全关联和安全策略，并输出至安全策略数据库和安全关联数据库映射模块；为 IKE 两个阶段的交换生成伪随机序列和密钥交换载荷的 Diffie-Hellman 密钥材料；根据 IKE 模块协商好的安全关联，获取安全封装载荷或完整性认证信息中加密算法、认证算法的信息，调用密钥生成子模块生成密钥，调用硬件映射模块映射到密钥的内容可寻址存储器；

安全策略数据库和安全关联数据库映射模块：用于更新安全策略数据库和安全关联数据库，调用硬件映射模块，将安全策略数据库和安全关联数据库镜像映射入在 NetFPGA 硬件平台相应的内容可寻址存储器；

硬件映射管理模块：调用设备 I/O 管理函数 ioctl 的读寄存器函数 readReg() 和写寄存器函数 writeReg()，将用户控制平台的路由表、安全关联数据库、安全策略数据库、密钥库映射入 NetFPGA 硬件平台的内容可寻址存储器；

所述的转发层面包括：

内容可寻址存储器查询模块：定义并分配内容可寻址存储器用于存储路由表、安全关联数据库、安全策略数据库、密钥库，实现对各个模块的接口；

输入队列处理模块：完成对多个网口的接收队列进行调度，轮询处理数据包；

IPSec 输入处理模块：完成对来自对端子网的已经经过 IPSec 安全封装载荷封装认证处理的数据包进行 IPSec 的安全封装载荷的解封装或完整性验证操作；

路由表查询转发模块：完成对数据包的转发路由的查询，获取下一跳的 IP 地址和输出端口信息；

IPSec 输出处理模块：完成对来自本地子网尚未进行 IPSec 封装处理的数据包进行安全封装载荷封装或完整性认证 IPSec 处理操作；

输出队列处理模块：完成将输入的数据包存储进静态随机存储器，实现一个轮询机制来为数据的输出提供调度服务。

2. 如权利要求 1 所述的一种基于 NetFPGA 的 IPSec VPN 实现系统，其特征在于：所述的 PCI 总线包含有 DMA 直接访问寄存器和寄存器组。

3. 一种基于 NetFPGA 的 IPSec VPN 实现方法，其特征在于：该方法包括下面几个阶段：

阶段一：建立安全关联和安全策略的动态管理阶段，在控制层面调用系统的 IKE 协议进程来实现安全关联的动态管理，完成安全关联数据库和安全策略数据库的动态更新；根据安全关联的参数信息，生成符合要求的密钥，进而更新密钥数据库；

阶段二：建立硬件镜像映射实现阶段，调用设备 I/O 管理函数 ioctl，实现将安全关联数据库和安全策略数据库映射进在 NetFPGA 上相应的内容可寻址存储器和随机存储器寄存器里；

阶段三：建立 IPSec 数据包输入处理阶段，数据包在转发层面实现硬件访问安全策略

数据库、安全关联数据库和密钥的内容可寻址存储器，对已经实施 IPSec 保护的数据流，进行解封装、数据完整性认证操作；

阶段四：建立 IPSec 数据包输出处理阶段，数据包在转发层面实现硬件访问安全策略数据库、安全关联数据库和密钥的内容可寻址存储器，进行 IPSec 协议的处理。

4. 如权利要求 3 所述的一种基于 NetFPGA 的 IPSec VPN 实现方法，其特征在于：所述的阶段一实现的具体步骤如下：

步骤 1：在控制层面调用 IKE 协议进程，完成 IKE 第一阶段的交换，在路由器间协商建立 ISAKMP 安全关联；

步骤 2：在第一阶段建立的 ISAKMP 安全关联的安全保护下，通过快速模式完成 IKE 第二阶段的交换，通信对等实体协商 IPSec 安全关联的各项特征，并为其生成密钥，动态更新安全关联数据库、安全策略数据库和密钥库。

5. 如权利要求 3 所述的一种基于 NetFPGA 的 IPSec VPN 实现方法，其特征在于：所述的阶段二实现的具体步骤如下：

步骤 1 在 NetFPGA 上定义并开辟安全关联寄存器组，分配安全关联寄存器组的地址空间，调用设备 I/O 管理函数 ioctl 的读寄存器函数 readReg() 读取安全关联寄存器组的内容，将存储于主机内存的安全关联数据库映射到安全关联寄存器组；

步骤 2 在 NetFPGA 上定义开辟安全策略寄存器组，分配安全策略寄存器组的地址空间，调用设备 I/O 管理函数 ioctl 的读寄存器函数 readReg() 读取安全策略寄存器组的内容，将存储于主机内存的安全策略映射到安全策略寄存器组；

步骤 3 在 NetFPGA 上定义开辟密钥寄存器组，分配密钥寄存器组的地址空间，调用设备 I/O 管理函数 ioctl 的读寄存器函数 readReg() 读取密钥寄存器组的内容，将存储于主机内存的密钥库映射到密钥寄存器组。

6. 如权利要求 3 所述的一种基于 NetFPGA 的 IPSec VPN 实现方法，其特征在于：所述的阶段三实现的具体步骤如下：

步骤 1 调用数据包协议分析模块进行判断：将 UDP 类型、端口号 500 的 IKE 更新包和 TCP 类型、端口号 89 的 OSPF 更新包转送给主机系统的协议进程处理；将包含 IPSec 首部的数据流，进入步骤 2 的 IPSec 输入处理模块；其他的 IP 数据流，跳过阶段三的处理，进入阶段四的处理；

步骤 2 调用 IPSec 输入处理模块，提取出目的 IP 地址、协议类型、安全参数索引，查询安全策略数据库获取安全策略，若存在，获取该安全策略所对应的安全关联在内容可寻址存储器的存储地址；若不存在相应的安全策略，则直接跳过 IPSec 输入处理阶段，进入输出端口；

步骤 3 根据步骤 2 获取的安全关联的存储地址，查询安全关联数据库，获取相应的安全关联信息，读取 IPSec 协议模式、安全封装载荷和完整性认证信息及安全关联参数；

步骤 4 根据安全封装载荷和完整性认证信息及安全关联参数，获取解密算法和认证算法、密钥、初始值参数信息；硬件访问密钥内容可寻址存储器寄存器获取对应的密钥；

步骤 5 根据步骤 4 所获得的信息，从安全封装载荷中分离出加密载荷，调用解密集成模块，处理密文字段，获取相应的明文；

步骤 6 调用认证算法模块，对步骤 5 的输出的明文状态的数据，进行数据完整性的验

证；

步骤 7IP 数据包重构，传输模式下，修正原有 IP 首部的相关字段；隧道模式下，移除 IPSec 添加的 IP 首部和安全封装载荷首部或完整性认证首部，还原加密载荷的 IP 首部。

7. 如权利要求 3 所述的一种基于 NetFPGA 的 IPSec VPN 实现方法，其特征在于：所述的阶段四实现的具体步骤如下：

步骤 1 调用 IPSec 输出处理模块，获取目的 IP 地址和协议，检索安全策略数据库，获得安全关联在内容可寻址存储器的存储地址；若未存在安全关联，则调用 IKE 协议进程建立安全关联；

步骤 2 根据步骤 1 获取的安全关联的存储地址，查询安全关联数据库，获取相应的安全关联信息，读取 IPSec 协议模式、安全封装载荷和完整性认证信息及安全关联参数；

步骤 3 根据安全封装载荷和完整性认证信息及安全关联参数，获取加密算法和认证算法、密钥、初始值参数信息；硬件访问密钥的内容可寻址存储器获取对应的密钥；

步骤 4 调用加密集成模块，根据步骤 3 所获得的信息，传输模式下，对 IP 数据包的传输层及以上数据进行加密；隧道模式下，对 IP 数据包的网络层及传输层和应用层的数据进行加密；

步骤 5 调用认证算法模块，对步骤 4 的输出数据进行数据完整性的验证；

步骤 6IP 数据包重构，传输模式下，修正原有 IP 首部的相关字段；隧道模式下，重新生成各个 IP 首部字段，重新构建 IP 首部。

基于 NetFPGA 的 IPSec VPN 实现系统及方法

技术领域

[0001] 本发明涉及基于 NetFPGA 的 IPSec VPN 实现系统及方法。

背景技术

[0002] IPSec 协议是因特网安全工程组 IETF1998 年着手制定的一套开放标准网络安全协议，将密码技术应用在网络层，以提供发送、接收端的数据的认证、完整性、存取控制、以及机密性等安全服务。高层的应用协议也可以直接或间接地使用这些安全服务。因此，IPSec 协议常常配置在路由器、防火墙、主机和通信链路上，以实现 VPN 网络中的安全隧道功能，从而实现安全防护的功能。

[0003] IPSec 协议可在终端主机、网关 / 路由器或者两者间同时进行实施和配置 :主机实施 IPSec 主要用于确保传输层的通信安全 ;路由器上实施 IPSec，主要用于确保网络层的通信安全。

[0004] 主机实施的实现方式有集成方式、" 堆栈中的块" 方式。

[0005] (1) 集成方式 :把 IPSec 集成到 IP 协议的原始实现，需要处理系统内核，IPSec 层需要网络层的服务构建 IP 首部，适用于在主机和安全网关上实现。

[0006] (2)" 堆栈中的块" 方式 :把 IPSec 作为一个" 契子" 插入在协议堆栈的网络层与数据链路层之间实施，不需要处理 IP 源码，使用于对原有系统的升级，通常在主机上实现。

[0007] 路由器实施的实现方式有原始方式、" 线缆中的块" 方式。

[0008] (1) 原始实施 :它等同于在主机上进行的操作系统集成实施方案，在这种情况下，IPSec 是集成在路由器软件中实现的。

[0009] (2)" 线缆中的块" 方式 :该方式是在特定硬件设备中实现 IPSec，然后将这个设备接入路由器或者主机中实现 IPSec 功能。一般这个设备直接接入路由器的物理接口，不运行路由算法，只是附着在路由器设备上用来保障数据包的安全。

[0010] 在路由器上实施 IPSec 协议，对路由器的数据包转发能力有着严重的依赖关系。路由器通常能够以尽可能快的速度转发 IP 数据包。而目前在路由器上实施 IPSec 的这两种方案，均存在各自的问题。原始方式由于使用路由软件来实现 IPSec 进行加解密操作等一系列复杂操作时，会耗费大量的系统资源 ;影响数据包的转发处理速度，对于较大流量的网络，容易造成网络堵塞，转发慢等问题。" 线缆中的块" 方式虽然能够较快地利用硬件完成 IPSec 复杂的操作，但是" 线缆中的块" 方式不能作为一种长期方案来使用，因为不可能让一个设备连接路由器的每个接口，若要完成完整的保护，则配备与路由器接口等量的" 线缆中的块" 方式的设备，将会大幅度增加路由器的功耗和成本。

发明内容

[0011] 本发明的目的在于，针对现有在路由器上通过原始方式或者" 线缆中的块" 方式实现的 IPSec VPN 导致的数据包转发效率低，处理速度慢的不足，提出了一种基于

NetFPGA(Net Field Programmable GateArray,网络可编程门阵列）的 IPSec VPN 实现系统及方法。本发明依据 RFC3746(L.Yang,R.Dantu,T.Anderson,R.Gopal.Forwarding and Control ElementSeparation(ForCES)Framework,IETF rfc,April,2004) 的描述,在路由器的控制层面添加 IKE 动态密钥管理模块,安全关联数据库映射模块和安全策略数据库,用于动态管理密钥、安全关联和安全策略;在转发层面充分利用 NetFPGA 开发板的模块化可重用思想,在原有 NetFPGA 的标准路由器架构中,增加了两个独立设计的 IPSec 输入和输出处理模块。该方案既能硬件实现数据流的路由转发功能,又能硬件实现 IPSec VPN 所要求的大部分计算功能,例如安全（解）封装载荷和完整性认证,能够有效地兼顾数据流的转发性能和 IPSec 协议处理性能。

[0012] 本发明的技术方案如下：

[0013] 一种基于 NetFPGA 的 IPSec VPN 实现系统,该系统包括控制层面和转发层面,所述的控制层面和转发层面之间通过 PCI 总线进行连接。

[0014] 所述的控制层面包括：

[0015] OSPF 动态路由协议模块:用于运行管理 OSPF 动态路由协议,完成对路由表的实时动态地更新,并调用硬件映射模块将路由表映射进 NetFPGA 硬件平台的内容可寻址存储器；

[0016] IKE 动态密钥管理模块:用于完成路由器间的安全关联的动态管理,处理通信实体的配置信息,协商相应的安全关联和安全策略,并输出至安全策略数据库和安全关联数据库映射模块;为 IKE 两个阶段的交换生成伪随机序列和密钥交换载荷的 Diffie-Hellman 密钥材料;根据 IKE 模块协商好的安全关联,获取安全封装载荷或完整性认证信息中加密算法、认证算法的信息,调用密钥生成子模块生成密钥,调用硬件映射模块映射到密钥的内容可寻址存储器；

[0017] 安全策略数据库和安全关联数据库映射模块:用于更新安全策略数据库和安全关联数据库,调用硬件映射模块,将安全策略数据库和安全关联数据库镜像映射入在 NetFPGA 硬件平台相应的内容可寻址存储器；

[0018] 硬件映射管理模块:调用设备 I/O 管理函数 ioctl 的读寄存器函数 readReg() 和写寄存器函数 writeReg(),将用户控制平台的路由表、安全关联数据库、安全策略数据库、密钥库映射入 NetFPGA 硬件平台的内容可寻址存储器；

[0019] 所述的转发层面包括：

[0020] 内容可寻址存储器查询模块:定义并分配内容可寻址存储器寄存器用于存储路由表、安全关联数据库、安全策略数据库、密钥库,实现对各个模块的接口；

[0021] 输入队列处理模块:完成对多个网口的接收队列进行调度,轮询处理数据包；

[0022] IPSec 输入处理模块:完成对来自对端子网的已经经过 IPSec 安全封装载荷封装认证处理的数据包进行 IPSec 的安全封装载荷的解封装或完整性验证等操作；

[0023] 路由表查询转发模块:完成对数据包的转发路由的查询,获取下一跳的 IP 地址和输出端口等信息；

[0024] IPSec 输出处理模块:完成对来自本地子网尚未进行 IPSec 封装处理的数据包进行安全封装载荷封装或完整性认证等 IPSec 处理操作；

[0025] 输出队列处理模块:完成将输入的数据包存储进静态随机存储器,实现一个轮询

机制来为数据的输出提供调度服务。

[0026] 进一步，所述的 PCI 总线包含有 DMA 直接访问寄存器和寄存器组。

[0027] 一种基于 NetFPGA 的 IPSec VPN 实现方法，该方法包括下面几个阶段：

[0028] 阶段一：建立安全关联和安全策略的动态管理阶段，在控制层面调用系统的 IKE 协议进程来实现安全关联的动态管理，完成安全关联数据库和安全策略数据库的动态更新；根据安全关联的相应信息，生成符合要求的密钥，进而更新密钥数据库；

[0029] 阶段二：建立硬件镜像映射实现阶段，调用设备 I/O 管理函数 ioctl，实现将安全关联数据库和安全策略数据库映射进 NetFPGA 上相应的内容可寻址存储器和随机存储器寄存器里；

[0030] 阶段三：建立 IPSec 数据包输入处理阶段，数据包在转发层面实现硬件访问安全策略数据库、安全关联数据库和密钥的内容可寻址存储器，对已经实施 IPSec 保护的数据流，进行解封装、数据完整性认证等操作；

[0031] 阶段四：建立 IPSec 数据包输出处理阶段，数据包在转发层面实现硬件访问安全策略数据库、安全关联数据库和密钥的内容可寻址存储器，进行 IPSec 协议的处理。

[0032] 进一步，所述的阶段一实现的具体步骤如下：

[0033] 步骤 1 在控制层面调用 IKE 协议进程，完成 IKE 第一阶段的交换，在路由器间协商建立 ISAKMP 安全关联；

[0034] 步骤 2 在第一阶段建立的 ISAKMP 安全关联的安全保护下，通过快速模式完成 IKE 第二阶段的交换，通信对等实体协商 IPSec 安全关联的各项特征，并为其生成密钥，动态更新安全关联数据库、安全策略数据库和密钥库。

[0035] 进一步，所述的阶段二实现的具体步骤如下：

[0036] 步骤 1 在 NetFPGA 上定义并开辟安全关联寄存器组，分配安全关联寄存器组的地址空间，调用设备 I/O 管理函数 ioctl 的读寄存器函数 readReg() 读取安全关联寄存器组的内容，将存储于主机内存的安全关联数据库映射到安全关联寄存器组；

[0037] 步骤 2 在 NetFPGA 上定义开辟安全策略寄存器组，分配安全策略寄存器组的地址空间，调用设备 I/O 管理函数 ioctl 的读寄存器函数 readReg() 读取安全策略寄存器组的内容，将存储于主机内存的安全策略映射到安全策略寄存器组；

[0038] 步骤 3 在 NetFPGA 上定义开辟密钥寄存器组，分配密钥寄存器组的地址空间，调用设备 I/O 管理函数 ioctl 的读寄存器函数 readReg() 读取密钥寄存器组的内容，将存储于主机内存的密钥库映射到密钥寄存器组。

[0039] 进一步，所述的阶段三实现的具体步骤如下：

[0040] 步骤 1 调用数据包协议分析模块进行判断：将 UDP 类型、端口号 500 的 IKE 更新包和 TCP 类型、端口号 89 的 OSPF 更新包转送给主机的协议进程处理；将包含 IPSec 首部的数据流，进入步骤 2 的 IPSec 输入处理模块；其他类型的 IP 数据流，跳过阶段三的处理，进入阶段四的处理；

[0041] 步骤 2 调用 IPSec 输入处理模块，提取出目的 IP 地址、协议类型、安全参数索引，查询安全策略数据库获取安全策略，若存在，获取该安全策略所对应的安全关联在内容可寻址存储器的存储地址；若不存在相应的安全策略，则直接跳过 IPSec 输入处理阶段，进入输出端口；

[0042] 步骤 3 根据步骤 2 获取的安全关联的存储地址，查询安全关联数据库，获取相应的安全关联信息，读取 IPSec 协议模式、安全封装载荷和完整性认证信息及安全关联参数；

[0043] 步骤 4 根据安全封装载荷和完整性认证信息及安全关联参数，获取诸如解密算法和认证算法、密钥、初始值等参数信息；硬件访问密钥内容可寻址存储器寄存器获取对应的密钥；

[0044] 步骤 5 根据步骤 4 所获得的信息，从安全封装载荷中分离出加密载荷，调用解密集成模块，处理密文字段，获取相应的明文；

[0045] 步骤 6 调用认证算法模块，对步骤 5 的输出的明文状态的数据，进行数据完整性的验证；

[0046] 步骤 7IP 数据包重构，传输模式下，修正原有 IP 首部的相关字段；隧道模式下，移除 IPSec 添加的 IP 首部和安全封装载荷首部或完整性认证首部，还原加密载荷的 IP 首部。

[0047] 进一步，所述的阶段四实现的具体步骤如下：

[0048] 步骤 1 调用 IPSec 输出处理模块，获取目的 IP 地址和协议，检索安全策略数据库，获得安全关联在内容可寻址存储器的存储地址；若未存在安全关联，则调用 IKE 协议进程建立安全关联；

[0049] 步骤 2 根据步骤 2 获取的安全关联的存储地址，查询安全关联数据库，获取相应的安全关联信息，读取 IPSec 协议模式、安全封装载荷和完整性认证信息及安全关联参数；

[0050] 步骤 3 根据安全封装载荷和完整性认证信息及安全关联参数，获取诸如加密算法和认证算法、密钥、初始值等参数信息；硬件访问密钥的内容可寻址存储器获取对应的密钥；

[0051] 步骤 4 调用加密集成模块，根据步骤 3 所获得的信息，传输模式下，对 IP 数据包的传输层及以上数据进行加密；隧道模式下，对 IP 数据包的网络层及以上的数据进行加密；

[0052] 步骤 5 调用认证算法模块，对步骤 4 的输出数据进行数据完整性的验证；

[0053] 步骤 6IP 数据包重构，传输模式下，修正原有 IP 首部的相关字段；隧道模式下，重新生成各个 IP 首部字段，重新构建 IP 首部。

[0054] 本发明的有益效果如下：提供一种在基于 NetFPGA 的路由器上实现 IPSec VPN 的方法，优先地将 IPSec VPN 的输入处理和输出处理从主机系统中移至 NetFPGA 上实现，并实现了转发功能，能够很好的提高数据包的 IPSec 处理速度和路由转发速度。

[0055] 该方法结合 IPSec VPN 技术，充分利用 NetFPGA 的硬件模块化可重用特点，实现了 IPSec 在基于 NetFPGA 的路由器上的运用，提高了 IPSec VPN 实施的灵活性和高速性，能够使得路由器实施 IPSec VPN 更加高速，更加高效的加密、认证等安全保障。

附图说明

[0056] 图 1：本发明在网络中部署的拓扑图；

[0057] 图 2：本发明的系统架构示意图；

[0058] 图 3：本发明的数据包处理流程图。

具体实施方式

[0059] 下面结合附图和具体的实施方案对本发明作进一步的详细描述：

[0060] 如图1为本发明在网络中部署的拓扑图，实施例在如图1所示的拓扑中，进行基于NetFPGA的IPSec VPN实施方案，本实施方案是在对应于两个通信子网的路由器间，建立一条高效、高速的IPSec-VPN隧道，以保护两个通信子网间的通信。

[0061] 图2为本发明的系统架构示意图，在具体实施中，设计了如图2的系统架构来实现IPSec VPN的保护。路由器上的IPSec VPN实施包括控制层面的软件部署和基于NetFPGA的转发层面的硬件模块部署。本发明利用集成于NetFPGA的四个千兆网卡进行数据包的发送与接收；将接收到的IP数据包，送入队列缓存中，添加相关的控制信息，等待输入判定器的轮询调用；进入IPSec输入处理模块，对于已有IPSec首部的数据包进行处理，其他的数据包查询安全策略数据库选择丢弃或者绕过此模块的处理；进入路由表查询模块，获取数据包的转发输出端口；进入IPSec输出处理模块，查询安全策略数据库选择丢弃、绕过IPSec服务或者应用IPSec服务；进入输出缓存队列模块，对数据包进行控制信息的移除等处理，送入网卡模块并发送至以太网。利用控制层面的软件实现安全关联动态管理、路由表的动态更新，并映射入NetFPGA相应的内容可寻址存储器，主要包括的模块：硬件映射管理模块、OSPF路由协议模块、安全策略数据库和安全关联数据库映射模块、IKE动态密钥管理模块。

[0062] 控制层面各模块功能如下：

[0063] IKE模块：完成路由器间的安全关联的动态管理，处理通信实体的配置信息，协商相关的安全关联和安全策略，并输出至安全策略数据库和安全关联数据库映射模块；

[0064] 安全策略数据库和安全关联数据库映射模块：更新安全策略数据库和安全关联数据库，调用硬件映射模块，将安全策略数据库和安全关联数据库镜像映射入在NetFPGA硬件平台相应的内容可寻址存储器；

[0065] 密钥管理模块：为IKE两个阶段的交换生成伪随机序列和密钥交换载荷作为Diffie-Hellman密钥材料；根据IKE模块协商好的安全关联，获取安全封装载荷或完整性认证信息中加密算法、认证算法的信息，调用密钥生成子模块生成密钥，调用硬件映射模块映射到密钥的内容可寻址存储器；

[0066] OSPF路由协议模块：运行管理OSPF动态路由协议，完成对路由表的实时更新，并调用硬件映射模块将路由表映射进NetFPGA硬件平台的内容可寻址存储器；

[0067] 硬件映射管理模块：调用设备I/O管理函数ioctl的读寄存器函数readReg()和写寄存器函数writeReg()，将用户控制平台的路由表、安全关联数据库、安全策略数据库、密钥库映射入NetFPGA硬件平台的内容可寻址存储器。

[0068] 利用NetFPGA硬件平台实现转发层面的数据包路由转发和IPSec输入输出处理等操作，主要包括的模块有内容可寻址存储器查询模块、输入队列处理模块、IPSec输入处理模块、路由表查询转发模块、IPSec输出处理模块和输出队列处理模块。

[0069] NetFPGA硬件平台各模块功能如下：

[0070] 内容可寻址存储器查询模块：定义并分配内容可寻址存储器寄存器用于存储路由表、安全关联数据库、安全策略数据库、密钥库，实现对各个模块的接口；

[0071] 输入队列处理模块：完成对多个网口的接收队列进行调度，轮询处理数据包；

[0072] IPSec输入处理模块：完成对来自对端子网已经经过IPSec封装认证处理的数据包进行IPSec的安全封装载荷的解封装或完整性验证等操作；

[0073] 路由表查询转发模块：完成对数据包的转发路由的查询，获取下一跳地址和输出端口等信息；

[0074] IPSec 输出处理模块：完成对来自本地子网的尚未进行 IPSec 封装处理的数据包进行安全封装载荷封装或完整性认证等 IPSec 处理操作；

[0075] 输出队列处理模块：完成将输入的数据包存储进静态随机存储器，实现一个轮询机制来为数据的输出提供调度服务。

[0076] 图 3 为本发明的数据包处理流程图，本发明的数据包处理流程如下：

[0077] (1) 通过 NetFPGA 硬件平台的 4 个千兆网卡获得的数据包，首先在队列缓存中进行帧重组，送入输入判定器，执行轮询机制从各个网口读入数据包。

[0078] (2) 首先对经输入判断器读入的数据包，进行协议的简单分析。

[0079] 如果是 UDP 类型、端口号 500 的 IKE 更新包和 TCP 类型、端口号 89 的 OSPF 更新包，直接通过 PCI 总线的直接存取存储器 DMA，转送到用户控制平台，进行安全关联的动态管理和 OSPF 动态路由表的更新，并调用硬件映射管理模块，将更新后的数据库，诸如 OSPF 路由表、安全关联数据库、安全策略数据库和密钥库，映射入 NetFPGA 硬件平台的内容可寻址存储器和随机存储器；

[0080] 如果是如 ICMP 数据包及其他类型 IP 包，则继续在 NetFPGA 上进行处理。

[0081] (3) 判断 IP 首部的协议字段。

[0082] 若协议号不等于 0x32 或 0x33，则直接跳至 (7)，进入路由表查询转发模块；

[0083] 若协议号等于 0x32 则 IPSec 类型为安全封装载荷，或者协议号等于 0x33 则 IPSec 类型为完整性认证，说明存在 IPSec 首部，则进入 IPSec 输入处理模块。提取目的 IP 地址、协议号和安全参数索引，构建选择符，查询安全关联数据库对应的内容可寻址存储器。若存在相应的安全策略，若为丢弃，则放弃对此数据包的处理；若为绕过，则直接跳至 (7)，进入路由表查询转发模块。

[0084] 若策略为应用，则根据提供的存储地址，查询安全关联数据库对应的内容可寻址存储器，获取相应的安全关联；得到安全关联的 IPSec 协议模式，包括隧道模式和传输模式；得到安全封装载荷信息，如加密算法、密钥、初始值、密钥生存周期等参数；完整性认证信息，如认证算法、密钥、初始值、密钥生存周期等参数。

[0085] (4) 采用的是安全封装载荷协议封装：首先验证安全封装载荷头的完整性，若完整性错误，直接丢弃此包；若正确，则根据 (3) 获取的安全封装载荷信息，查询密钥对应的内容可寻址存储器得到密钥，调用密码模块，对安全封装载荷进行解密，获得包含有填充数据的伪明文；而后，根据填充长度字段，将伪明文的填充部分去除，获得明文。

[0086] (5) 采用的是完整性认证协议：计算整个 IP 首部的完整值，并与完整性认证首部的认证数据进行比较，若错误，直接丢弃此包；若正确，则去除完整性认证首部，修正 IP 首部的协议字段和校验和等字段。

[0087] (6) 若 IPSec 协议模式为传输模式，修正原有 IP 首部的相关字段；若为隧道模式，移除 IPSec 添加的 IP 首部和安全封装载荷首部或完整性认证首部，还原加密载荷的 IP 首部。

[0088] (7) 进入路由查询转发模块。根据进入的 IP 数据包的目的 IP 地址查询路由表对应的内容可寻址存储器，获取并输出该数据包的下一跳 IP 地址和输出端口，供输出队列使

用。

[0089] (8) 将路由查询转发模块处理的数据包送入 IPSec 输出处理模块处理。

[0090] 获取目的 IP 地址和协议，查询安全策略数据库对应的内容可寻址存储器，获得安全关联的存储地址，再根据此存储地址查询安全关联数据库对应的内容可寻址存储器，获取安全关联；若未存在安全关联，则调用 IKE 协议进程为这类连接创建安全关联；

[0091] 获取相应的安全关联信息，读取 IPSec 协议模式、安全封装载荷和完整性认证信息等相关的安全关联参数；

[0092] 根据安全封装载荷和完整性认证信息及相关安全参数索引，获取诸如加密算法和认证算法、密钥、初始值等参数信息；硬件访问密钥对应的可寻址存储器来获取对应的密钥；根据选择的密钥特性，设置填充字段和填充长度字段，然后调用密钥模块，进行加密操作；

[0093] 若选择的 IPSec 协议模式为传输模式，对 IP 数据包的传输层及以上数据进行加密或认证；若为隧道模式，对 IP 数据包的网络层及以上的数据进行加密或认证；

[0094] 调用完整性校验算法模块，对经完整性认证或安全封装载荷的输出数据进行数据完整值的计算；

[0095] 利用相关的参数值完成 IP 数据包的重构：传输模式下，修正原有 IP 首部的相关字段；隧道模式下，重新生成各个 IP 首部字段，重新构建 IP 首部。

[0096] (9) 调用输出队列模块，将输入的数据包存储进静态随机存储器，实现一个轮询机制来为数据包进行存储，去除相关的控制首部，修正 IP 首部的相关字段值，送入输出缓冲队列，等待送到指定的输出网口。

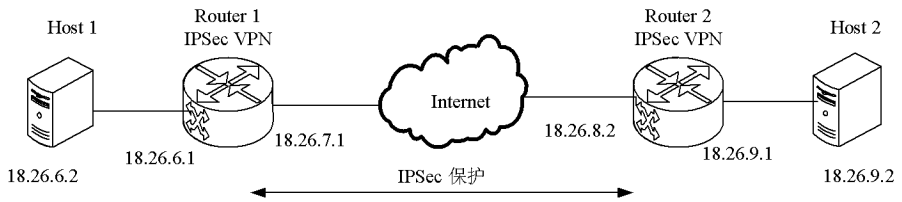

Host 1
Router 1
IPSec VPN
Internet
Router 2
IPSec VPN
Host 2
18.26.6.2
18.26.6.1
18.26.7.1
18.26.8.2
18.26.9.1
18.26.9.2
IPSec 保护

图 1

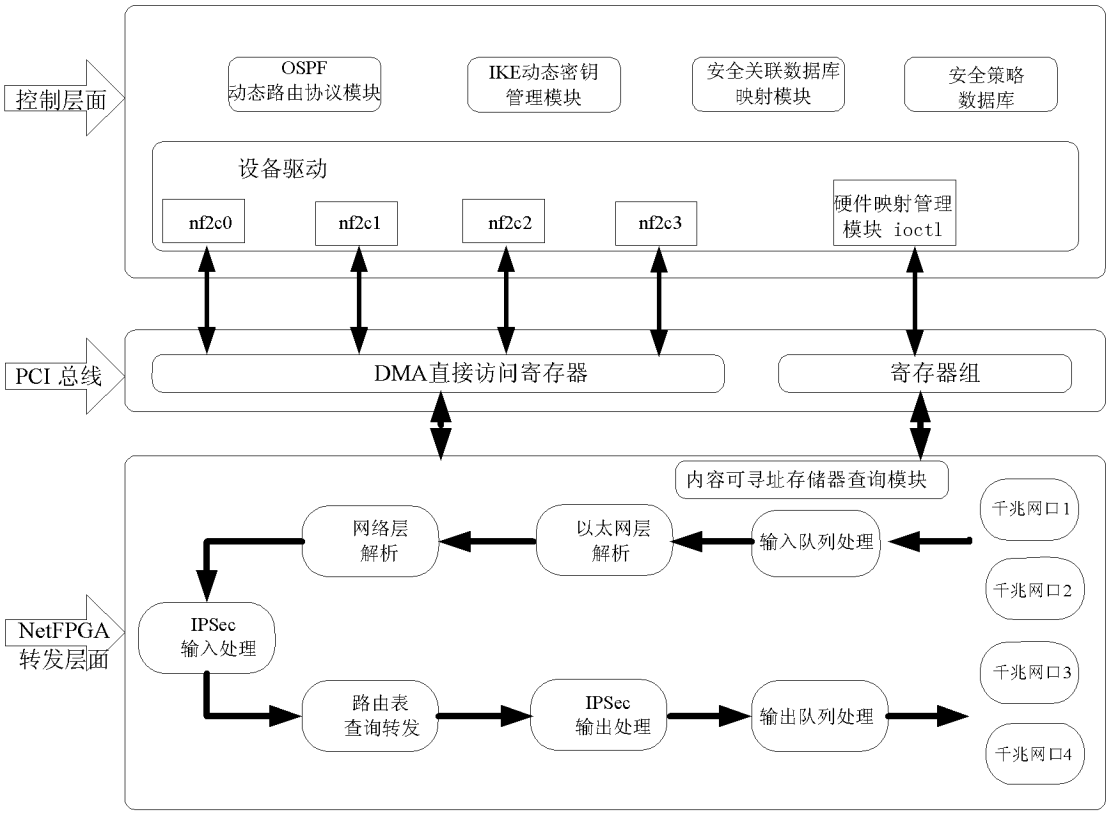

控制层面
OSPF
动态路由协议模块
IKE动态密钥
管理模块
安全关联数据库
映射模块
安全策略
数据库
设备驱动
nf2c0
nf2c1
nf2c2
nf2c3
硬件映射管理
模块 ioctl
PCI 总线
DMA直接访问寄存器
寄存器组
内容可寻址存储器查询模块
千兆网口1
网络层
解析
以太网层
解析
输入队列处理
千兆网口2
NetFPGA
转发层面
IPSec
输入处理
千兆网口3
路由表
查询转发
IPSec
输出处理
输出队列处理
千兆网口4

图 2

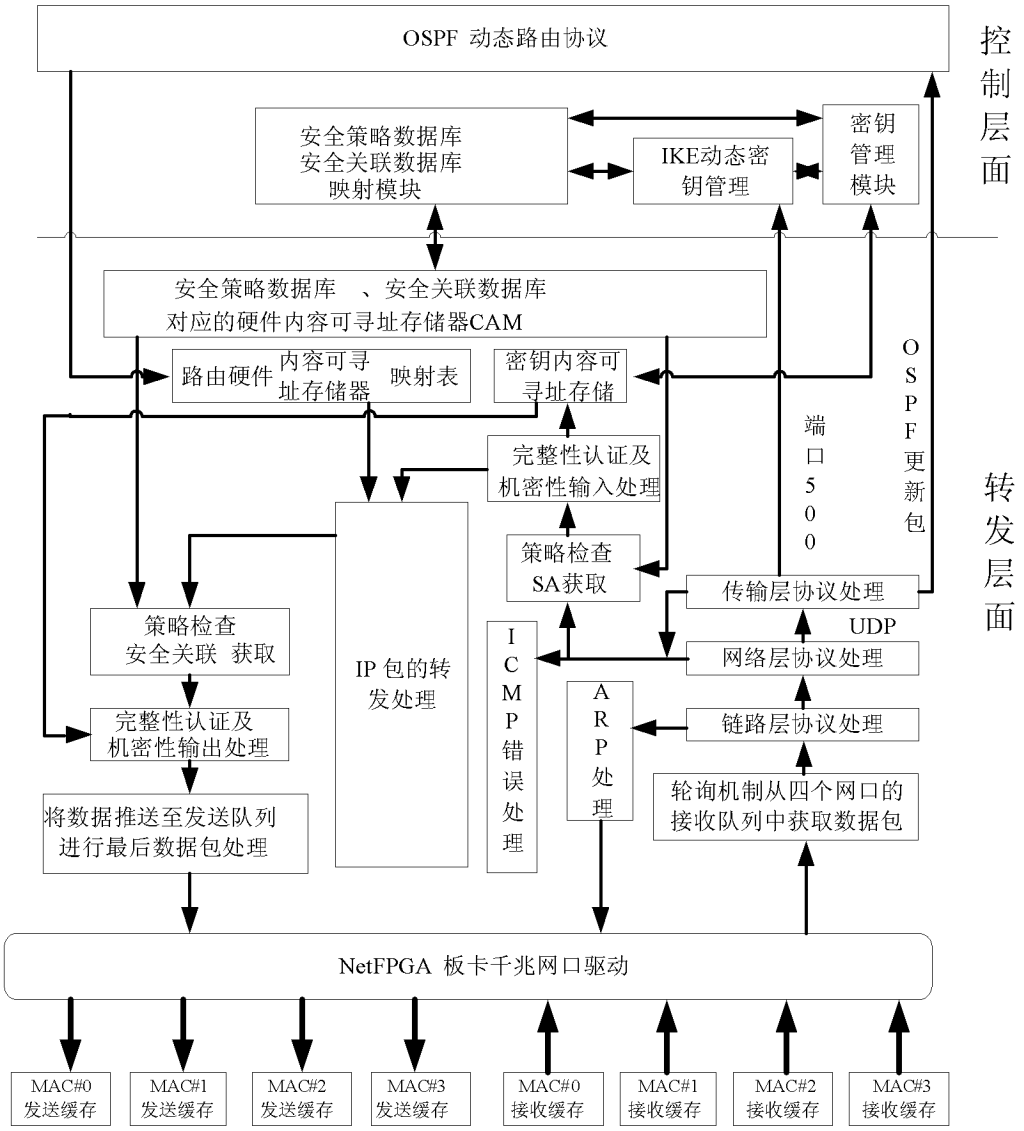

OSPF 动态路由协议
控制层面
安全策略数据库
安全关联数据库
映射模块
IKE动态密钥管理
密钥管理模块
安全策略数据库 、安全关联数据库
对应的硬件内容可寻址存储器CAM
路由硬件 内容可寻址存储器 映射表
密钥内容可寻址存储
OSPF更新包
端口500
完整性认证及机密性输入处理
转发层面
策略检查 SA获取
传输层协议处理
UDP
策略检查 安全关联 获取
IP 包的转发处理
ICMP错误处理
网络层协议处理
ARP处理
链路层协议处理
完整性认证及机密性输出处理
轮询机制从四个网口的接收队列中获取数据包
将数据推送至发送队列进行最后数据包处理
NetFPGA 板卡千兆网口驱动
MAC#0 发送缓存
MAC#1 发送缓存
MAC#2 发送缓存
MAC#3 发送缓存
MAC#0 接收缓存
MAC#1 接收缓存
MAC#2 接收缓存
MAC#3 接收缓存

图 3