(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 113709135 A
(43)申请公布日 2021.11.26

(21)申请号 202110977301.X

(22)申请日 2021.08.24

(71)申请人 杭州迪普科技股份有限公司
地址 310051 浙江省杭州市滨江区通和路68号中财大厦6楼

(72)发明人 汪庆权 魏方征

(74)专利代理机构 北京金讯知识产权代理事务所(特殊普通合伙) 11554
代理人 黄剑飞

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

权利要求书3页 说明书9页 附图3页

(54)发明名称

SSL流量审计采集系统与方法

(57)摘要

本公开涉及一种SSL流量审计采集系统及其方法，该系统包括：FPGA器件，其接收报文，从接收到的报文内容中提取报文的会话五元组，根据所述会话五元组查找会话，并根据查找结果来确定建立会话、丢弃会话和上送会话；以及中央处理器(CPU)，其从FPGA器件接收报文，从所接收到的报文内容中提取报文的会话五元组，根据所述会话五元组查找会话，根据查找结果来确定建立会话、进行深度报文检测以生成流量审计日志，并构造会话丢包消息发送给FPGA器件进行处理，其中所述会话丢包信息包含所述会话五元组以及丢包动作，并且FPGA器件接收所述中央处理器的所述会话丢包消息，并根据会话丢包消息设置会话转发状态。报文通过FPGA器件辅助处理，后续会话流量就不用上送CPU进行处理，从而减轻CPU处理SSL流量审计的负担。

CN 113709135 A

1.一种SSL流量审计采集系统,该SSL流量审计采集系统包括:

FPGA器件,其接收报文,从接收到的报文内容中提取报文的会话五元组,根据所述会话五元组查找会话,并根据查找结果来确定建立会话、丢弃会话和上送会话;以及

中央处理器,其从所述FPGA器件接收报文,从所接收到的报文内容中提取报文的会话五元组,根据所述会话五元组查找会话,根据查找结果来确定建立会话、进行深度报文检测以生成流量审计日志,并构造会话丢包消息发送给所述FPGA器件进行处理,

其中所述会话丢包信息包含所述会话五元组以及丢包动作,并且

所述FPGA器件接收所述中央处理器的所述会话丢包消息,并根据会话丢包消息设置会话转发状态。

2.根据权利要求1所述的SSL流量审计采集系统,其中如果所述FPGA器件查找不到包含所述会话五元组的会话,则根据所述会话五元组建立会话,而如果所述FPGA器件查找到包含所述会话五元组的会话,则查找会话中的丢包标志位,以检查是否需要丢弃该报文,如果需要丢弃报文,那么直接丢弃,否则将该报文上送给所述中央处理器。

3.根据权利要求1所述的SSL流量审计采集系统,其中如果所述中央处理器找不到包含所述会话五元组的会话,根据会话五元组建立会话,而如果查找到包含所述会话五元组的会话,则进行深度报文检测,并且如果经过深度报文检测发现是SSL协议报文,则在会话上设置审计标志位,其表示后续此条会话报文均要进入SSL流量审计采集以提取安全访问网站的必要信息,来生成流量审计日志。

4.根据权利要求1所述的SSL流量审计采集系统,还包括:

网络控制器,其联接在所述FPGA器件与所述中央处理器之间,所述FPGA器件通过其向所述中央处理器上送报文,而所述中央处理器通过其发送报文;以及

交换器件,其包括以太网卡和以太网接口,所述以太网卡从Web网上接收报文,并且当系统处于收包方向时所述FPGA器件通过以太网口与该交换器件相联以接收报文,而当系统处于发包方向时所述中央处理器通过网络控制器和交换器件的以太网口相联以发送报文。

5.根据权利要求1所述的SSL流量审计采集系统,其中所述FPGA器件包括:

FPGA会话管理单元,其接收报文,从报文内容中提取报文的会话五元组,根据报文的会话五元组查询会话,如果找不到包含所述会话五元组的会话,则根据会话五元组建立会话,而如果找到包含所述会话五元组的会话,则查找会话中的丢包标志位,以检查是否需要丢弃该报文,如果需要丢弃报文,那么直接丢弃,否则将报文上送到所述中央处理器进行处理;以及

FPGA消息管理单元,其接收所述中央处理器的消息报文,解析报文以发现会话丢包消息,并在发现会话丢包消息后,根据会话丢包消息设置会话转发状态。

6.根据权利要求1所述的SSL流量审计采集系统,其中所述中央处理器包括:

CPU会话管理单元,其接收报文,然后从所接收到的报文内容中提取该报文的会话五元组,根据报文的会话五元组查询会话,如果找不到包含所述会话五元组的会话,则根据会话五元组建立会话;

深度报文检测单元,其在所述CPU会话管理单元找到包含所述会话五元组的会话时,对从所述CPU会话管理单元所接收的报文基于会话维度进行深度报文检测分析以检测报文所属于的类型,如果经过深度报文检测发现是SSL协议报文,则在会话上设置审计标志位,其

表示后续此条会话报文均要进入SSL流量审计采集；

SSL流量审计采集单元，其判断从所述深度报文检测单元所接收到的会话上是否有审计标志位，并对有审计标志位的会话进行SSL流量审计采集以提取安全访问网站的必要信息，来生成流量审计日志；

日志管理单元，对审计日志进行维护管理；以及

CPU消息管理单元，其根据业务要求，对所述FPGA器件提交的消息进行业务处理。

7.根据权利要求6所述的SSL流量审计采集系统，其中所述业务处理包括生成基于会话的会话丢包消息，以通知所述FPGA器件后续报文不用上送所述中央处理器。

8.根据权利要求1-6之一所述的SSL流量审计采集系统，其中所述会话转发状态包括会话丢包标志位以便丢弃后续会话报文，从而控制报文上送所述中央处理器。

9.根据权利要求1-6之一所述的SSL流量审计采集系统，其中所述会话五元组包括报文的源IP、目的IP、协议号、源端口、目的端口。

10.一种用于SSL流量审计采集系统的流量审计采集方法，该SSL流量审计采集系统包括FPGA器件，其接收报文，从接收到的报文内容中提取报文的会话五元组，根据所述会话五元组查找会话，并根据查找结果来确定建立会话、丢弃会话和上送会话；以及中央处理器，其从所述FPGA器件接收报文，从所接收到的报文内容中提取报文的会话五元组，根据所述会话五元组查找会话，根据查找结果来确定建立会话、进行深度报文检测以生成流量审计日志，并构造会话丢包消息发送给所述FPGA器件进行处理，该流量审计采集方法包括以下步骤：

所述FPGA器件接收报文并从报文内容中提取报文的会话五元组，根据会话五元组查找会话，如果所述FPGA器件找不到包含所述会话五元组的会话，则根据会话五元组建立会话，而如果能找到包含所述会话五元组的会话，则查找会话丢包标志位，以检查是否需要丢弃报文，如果需要丢弃报文，那么直接丢弃，否则将报文上送到所述中央处理器进行处理；

所述中央处理器接收报文，从报文内容中提取报文的会话五元组，根据会话五元组查找会话，并且如果所述中央处理器找不到包含所述会话五元组的会话，则根据会话五元组建立会话；

如果所述中央处理器找到了会话，则对所接收的报文基于会话维度进行深度报文检测分析以检测报文所属于的类型，如果经过深度报文检测发现是SSL协议报文，则在会话上设置审计标志位，其表示后续此条会话报文均要进入SSL流量审计采集；

对有审计标志位的会话进行SSL流量审计采集以提取安全访问网站的信息，来生成流量审计日志并对审计日志进行维护管理；

根据业务要求，对FPGA器件提交的消息进行业务处理；并且

所述FPGA器件接收所述中央处理器的消息报文，解析报文以发现会话丢包消息，并在发现会话丢包消息后，根据会话丢包消息设置会话转发状态。

11.根据权利要求10所述的流量审计采集方法，其中所述业务处理包括生成基于会话的会话丢包消息，以通知所述FPGA器件后续报文不用上送所述中央处理器。

12.根据权利要求10所述的流量审计采集方法，其中所述会话转发状态包括会话丢包标志位以便丢弃后续会话报文，从而控制报文上送所述中央处理器。

13.根据权利要求10所述的流量审计采集方法，其中所述会话五元组包括报文的源IP、

目的IP、协议号、源端口、目的端口。

SSL流量审计采集系统与方法

技术领域

[0001] 本公开涉及流量SSL流量审计采集系统和方法，尤其涉及通过由网站访问信息生成的流量审计日志来提升SSL流量审计性能的SSL流量审计采集系统和方法。

背景技术

[0002] 过去，在大部分WEB应用中，浏览器通常利用超文本传输协议HTTP协议与服务器进行数据传输。然而，HTTP是超文本传输协议，信息是明文传输。在超文本传输协议HTTP协议下，出于信息安全考虑，诸如电子商务或在线财务账户之类的安全敏感信息必须在加密后才能在浏览器与服务器之前进行传输。

[0003] 为了提高数据传输的安全性，在1990年代中期定义所谓安全超文本传输协议HTTPS来满足进行安全通信的需求。在这种安全超文本传输协议HTTPS下，人们访问带有以HTTPS://开头的统一资源定位器(URL)的网页，当要将信息回送给服务器时，浏览器的HTTPS层会对其进行加密，而且从服务器处收到的确认回单也会以加密形式进行传输，到达时带有HTTPS://的统一资源定位器，它会通过浏览器的HTTPS子层对送达的信息进行解密。

[0004] 经过多年的发展，目前大部分浏览器与WEB服务器之间的数据传输已经采用了安全超文本传输协议HTTPS。HTTPS作为具有安全性的SSL加密传输协议，其安全基础便是SSL，加密操作需要SSL协助完成。SSL协议及其继任者TLS协议，是为网络安全提供安全性及数据完整性的一种安全协议。SSL/TLS协议位于TCP/IP协议和应用层协议之间，可为各种应用层协议(例如FTP、TELNET协议等)提供安全性保证。SSL/TLS协议也是目前最广泛应用的HTTP协议安全。

[0005] SSL/TLS协议包括两层：记录层协议和握手协议。记录协议为高层握手协议提供基本的安全服务，保证数据完整性，具体包括压缩解压缩、加解密、计算和校验MAC等。握手层协议包括握手协议、密码参数修改协议、告警协议和应用数据协议，用于通信双方认证、协商加密算法和生成私钥等。

[0006] 由SSL/TLS协议保护的高层协议在客户端与服务器之间传输的是密文数据，流量审计分析业务需要从SSL加密流量中提取访问网站、证书、加密套件等信息。然而，随着用户对安全及隐私的重视以及5G的发展，网络中的SSL流量越来越大，对流量审计系统性能带来了越来越大的挑战，需要流量审计系统越来越多，硬件成本越来越高，同时对能源及机房空间的需求也同步提升，投资越来越大。

[0007] 图1示出了一种典型的流量审计系统。如图1所示，该流量审计系统100包括中央处理器(CPU)130和网络控制器(网卡)120。数据流量经过网络控制器(网卡)120进入CPU 130进行处理。数据流量上送CPU 130后，CPU 130根据会话五元组(源IP、目的IP、源端口、目的端口、协议)建立会话；基于会话进行SSL流量审计采集；从SSL握手协商报文里面提取访问网站、证书、加密套件等信息；提取完成后，交给日志管理单元进行处理，一般发送到日志采集平台，对于同一条会话的后续报文一般予以丢弃，以节约性能。

[0008] 流量审计系统100还可以包括交换器件110，在这种情况下，数据流量先经过交换

器件110的交换芯片,然后经过网络控制器(网卡)120进入CPU 130进行处理。

[0009] 在这种现有技术方案中,存在至少两个不足。其一是所有网络流量都上送到CPU进行处理,但由于SSL后续流量是加密的,上送CPU进行处理后基本上都会进行丢弃,这会大大加重CPU处理负担及业务复杂性,影响系统性能。其二也是所有网络流量都上送到CPU进行处理,从而影响系统性能,导致流量审计系统越来越多,因而造成硬件成本越来越高,同时对能源及机房空间的需求也同步提升,投资越来越大,也不绿色环保。

[0010] 因此,需要一种能够不用将数据流量上送到CPU进行处理就可以实现对SSL流量进行采集审计的系统和方法。

发明内容

[0011] 本公开为了解决上述现有技术问题而提出一种不仅能实现对SSL流量进行采集审计,而且能够大大减轻CPU处理SSL流量的负担的系统及其方法。

[0012] 根据本公开的一个方面,提供一种SSL流量审计采集系统,该SSL流量审计采集系统可以包括:FPGA器件,其接收报文,从接收到的报文内容中提取报文的会话五元组,根据所述会话五元组查找会话,并根据查找结果来确定建立会话、丢弃会话和上送会话;以及中央处理器,其从所述FPGA器件接收报文,从所接收到的报文内容中提取报文的会话五元组,根据所述会话五元组查找会话,根据查找结果来确定建立会话、进行深度报文检测以生成流量审计日志,并构造会话丢包消息发送给所述FPGA器件进行处理,其中所述会话丢包信息包含所述会话五元组以及丢包动作,并且所述FPGA器件接收所述中央处理器的所述会话丢包消息,并根据会话丢包消息设置会话转发状态。

[0013] 根据本公开的一个实施例,如果所述FPGA器件查找不到包含所述会话五元组的会话,则根据所述会话五元组建立会话,而如果所述FPGA器件查找到包含所述会话五元组的会话,则查找会话中的丢包标志位,以检查是否需要丢弃该报文,如果需要丢弃报文,那么直接丢弃,否则将该报文上送给所述中央处理器。

[0014] 根据本公开的一个实施例,如果所述中央处理器找不到包含所述会话五元组的会话,根据会话五元组建立会话,而如果查找到包含所述会话五元组的会话,则进行深度报文检测,并且如果经过深度报文检测发现是SSL协议报文,则在会话上设置审计标志位,其表示后续此条会话报文均要进入SSL流量审计采集以提取安全访问网站的必要信息,来生成流量审计日志。

[0015] 根据本公开的一个实施例,所述SSL流量审计采集系统还包括:网络控制器,其联接在所述FPGA器件与所述中央处理器之间,所述FPGA器件通过其向所述中央处理器上送报文,而所述中央处理器通过其发送报文;以及交换器件,其包括以太网卡和以太网接口,所述以太网卡从Web网上接收报文,并且当系统处于收包方向时所述FPGA器件通过以太网口与该交换器件相联以接收报文,而当系统处于发包方向时所述中央处理器通过网络控制器和交换器件的以太网口相联以发送报文。

[0016] 根据本公开的一个实施例,所述FPGA器件包括:FPGA会话管理单元,其接收报文,从报文内容中提取报文的会话五元组,根据报文的会话五元组查询会话,如果找不到包含所述会话五元组的会话,则根据会话五元组建立会话,而如果找到包含所述会话五元组的会话,则查找会话中的丢包标志位,以检查是否需要丢弃该报文,如果需要丢弃报文,那么

直接丢弃，否则将报文上送到所述中央处理器进行处理；以及FPGA消息管理单元，其接收所述中央处理器的消息报文，解析报文以发现会话丢包消息，并在发现会话丢包消息后，根据会话丢包消息设置会话转发状态。

[0017] 根据本公开的一个实施例，所述中央处理器包括：CPU会话管理单元，其接收报文，然后从所接收到的报文内容中提取该报文的会话五元组，根据报文的会话五元组查询会话，如果找不到包含所述会话五元组的会话，则根据会话五元组建立会话；深度报文检测单元，其在所述CPU会话管理单元找到包含所述会话五元组的会话时，对从所述CPU会话管理单元所接收的报文基于会话维度进行深度报文检测分析以检测报文所属于的类型，如果经过深度报文检测发现是SSL协议报文，则在会话上设置审计标志位，其表示后续此条会话报文均要进入SSL流量审计采集；SSL流量审计采集单元，其判断从所述深度报文检测单元所接收到的会话上是否有审计标志位，并对有审计标志位的会话进行SSL流量审计采集以提取安全访问网站的必要信息，来生成流量审计日志；日志管理单元，对审计日志进行维护管理；以及CPU消息管理单元，其根据业务要求，对所述FPGA器件提交的消息进行业务处理。

[0018] 根据本公开的一个方面，提供一种用于SSL流量审计采集系统的流量审计采集方法，该SSL流量审计采集系统包括FPGA器件，其接收报文，从接收到的报文内容中提取报文的会话五元组，根据所述会话五元组查找会话，并根据查找结果来确定建立会话、丢弃会话和上送会话；以及中央处理器，其从所述FPGA器件接收报文，从所接收到的报文内容中提取报文的会话五元组，根据所述会话五元组查找会话，根据查找结果来确定建立会话、进行深度报文检测以生成流量审计日志，并构造会话丢包消息发送给所述FPGA器件进行处理，该流量审计采集方法包括以下步骤：所述FPGA器件接收报文并从报文内容中提取报文的会话五元组，根据会话五元组查找会话，如果所述FPGA器件找不到包含所述会话五元组的会话，则根据会话五元组建立会话，而如果能找到包含所述会话五元组的会话，则查找会话丢包标志位，以检查是否需要丢弃报文，如果需要丢弃报文，那么直接丢弃，否则将报文上送到所述中央处理器进行处理；所述中央处理器接收报文，从报文内容中提取报文的会话五元组，根据会话五元组查找会话，并且如果所述中央处理器找不到包含所述会话五元组的会话，则根据会话五元组建立会话；如果所述中央处理器找到了会话，则对所接收的报文基于会话维度进行深度报文检测分析以检测报文所属于的类型，如果经过深度报文检测发现是SSL协议报文，则在会话上设置审计标志位，其表示后续此条会话报文均要进入SSL流量审计采集；对有审计标志位的会话进行SSL流量审计采集以提取安全访问网站的信息，来生成流量审计日志并对审计日志进行维护管理；根据业务要求，对FPGA器件提交的消息进行业务处理；并且所述FPGA器件接收所述中央处理器的消息报文，解析报文以发现会话丢包消息，并在发现会话丢包消息后，根据会话丢包消息设置会话转发状态。

[0019] 根据本公开的一个实施例，所述业务处理包括生成基于会话的会话丢包消息，以通知所述FPGA器件后续报文不用上送所述中央处理器。

[0020] 根据本公开的一个实施例，所述会话转发状态包括会话丢包标志位以便丢弃后续会话报文，从而控制报文上送所述中央处理器。

[0021] 根据本公开的一个实施例，所述会话五元组包括报文的源IP、目的IP、协议号、源端口、目的端口。

[0022] 利用上述技术方案，系统或方法一旦提取到访问网站、证书、加密套件等信息后，

就将审计日志交付给日志管理单元处理，后续会话流量不用上送CPU进行处理，从而大大减轻CPU处理SSL流量的负担，提升了SSL流量审计采集系统性能，减少了硬件投资成本，降低了对能源及机房空间的需求，绿色环保。

附图说明

[0023] 通过参照附图详细描述其示例实施例，本公开的上述和其它目标、特征及优点将变得更加显而易见。下面描述的附图仅仅是本公开的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0024] 图1示出了一种典型的流量审计系统；

[0025] 图2示出了根据本公开的一个实施例的SSL流量审计采集系统；

[0026] 图3示出了根据本公开的一个实施例的FPGA器件的框图；

[0027] 图4示出了根据本公开的一个实施例的CPU的框图；以及

[0028] 图5是根据本公开的用于SSL流量审计采集系统的流量审计采集方法的流程图。

具体实施方式

[0029] 现在将参考附图更全面地描述示例实施例。然而，示例实施例能够以多种形式实施，且不应被理解为限于在此阐述的实施例；相反，提供这些实施例使得本公开将全面和完整，并将示例实施例的构思全面地传达给本领域的技术人员。在图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。

[0030] 此外，所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施例中。在下面的描述中，提供许多具体细节从而给出对本公开的实施例的充分理解。然而，本领域技术人员将意识到，可以实践本公开的技术方案而没有特定细节中的一个或更多，或者可以采用其它的方法、组元、装置、步骤等。在其它情况下，不详细示出或描述公知方法、装置、实现或者操作以避免模糊本公开的各方面。

[0031] 附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

[0032] 附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

[0033] 应理解，虽然本文中可能使用术语第一、第二、第三等来描述各种组件，但这些组件不应受这些术语限制。这些术语乃用以区分一组件与另一组件。因此，下文论述的第一组件可称为第二组件而不偏离本公开概念的教示。如本文中所使用，术语“及/或”包括相关联的列出项目中的任一个及一或多者的所有组合。

[0034] 本领域技术人员可以理解，附图只是示例实施例的示意图，附图中的模块或流程并不一定是实施本公开所必须的，因此不能用于限制本公开的保护范围。

[0035] 以下将描述本公开的具体实施方式，需要指出的是，在这些实施方式的具体描述过程中，为了进行简明扼要的描述，本说明书不可能对实际的实施方式的所有特征均作详尽的描述。应当可以理解的是，在任意一种实施方式的实际实施过程中，正如在任意一个工

程项目或者设计项目的过程中，为了实现开发者的具体目标，为了满足系统相关的或者商业相关的限制，常常会做出各种各样的具体决策，而这也会从一种实施方式到另一种实施方式之间发生改变。此外，还可以理解的是，虽然这种开发过程中所作出的努力可能是复杂并且冗长的，然而对于与本公开公开的内容相关的本领域的普通技术人员而言，在本公开揭露的技术内容的基础上进行的一些设计，制造或者生产等变更只是常规的技术手段，不应当理解为本公开的内容不充分。

[0036] 除非另作定义，权利要求书和说明书中使用的技术术语或者科学术语应当为本公开所属技术领域内具有一般技能的人士所理解的通常意义。本公开专利申请说明书以及权利要求书中使用的“第一”、“第二”以及类似的词语并不表示任何顺序、数量或者重要性，而只是用来区分不同的组成部分。“一个”或者“一”等类似词语并不表示数量限制，而是表示存在至少一个。“包括”或者“包含”等类似的词语意指出现在“包括”或者“包含”前面的元件或者物件涵盖出现在“包括”或者“包含”后面列举的元件或者物件及其等同元件，并不排除其他元件或者物件。“联接”或者“相联”等类似的词语并非限定于物理的或者机械的联接，也不限于是直接的还是间接的联接。

[0037] 本公开提供了新颖的SSL流量审计采集系统和方法，其通过在现有技术的SSL流量审计采集系统和方法的基础上，增加一个FPGA芯片作为以太网卡，来提取到访问网站、证书、加密套件等信息，并根据所提取到的信息直接生成流量审计日志并交付给日志管理单元处理，因此后续会话流量不用上送CPU进行处理，从而不仅能实现对SSL流量进行采集审计，还大大减轻CPU处理SSL流量的负担，提升了整个SSL流量审计采集系统性能，减少了硬件投资成本，降低了对能源及机房空间的需求，绿色环保。

[0038] 本公开新增添的FPGA芯片是一种现场可编程门阵列(Field Programmable Gate Array)，它是在PAL、GAL、CPLD等可编程器件的基础上进一步发展的产物，作为专用集成电路(ASIC)领域中的一种半定制电路而出现。

[0039] 图2示出了根据本公开的一个实施例的SSL流量审计采集系统。如图2所示，该SSL流量审计采集系统200包括中央处理器(CPU)230、网络控制器220、交换器件210以及FPGA器件240。

[0040] 交换器件210包括多个入接口(在图2中示出为附图标记eth0～ethN)和以太网口(在图2中示出为附图标记ieth)。这里的入接口和以太网口个数是示意性而非限制性的，在根据本公开的其他实施例中，以太网口的个数也可以是多个，而入接口的个数可以是一个。

[0041] 在SSL流量审计采集系统收包时，交换器件210将入接口(eth0～ethN)收到的报文通过以太网口(ieth)发送给FPGA器件240。

[0042] 交换器件210的其他方面与现有技术的SSL流量审计采集系统的交换器件相似，因此将不在此赘述。

[0043] 还需要说明的是，流量审计系统200与现有技术的SSL流量审计采集系统一样，也可以不包括交换器件210。在这种情况下，数据流量直接被发送给FPGA器件240进行后续处理。

[0044] 图2中的网络控制器220与现有技术的SSL流量审计采集系统的网络控制器具有相似的结构和功能，因此也不在此赘述。

[0045] 该FPGA器件240包括FPGA芯片作为以太网卡。由于FPGA芯片可以扩展以太网接口，

所以收包方向FPGA器件240和交换器件210通过以太网口相联以接收报文，而发包方向CPU 230则通过网络控制器220和交换器件210的以太网口相联以发送报文。

[0046] FPGA器件240从交换器件210收到报文后，从报文内容中提取报文的会话五元组(源IP、目的IP、协议号、源端口、目的端口)，根据会话五元组查找会话，如果找不到包含所述会话五元组的会话，根据会话五元组建立会话。如果能找到包含所述会话五元组的会话，则查找会话中的丢包标志位，以检查是否需要丢弃该报文。如果需要丢弃报文，那么直接丢弃，否则将报文通过网络控制器220上送到CPU 230进行处理。

[0047] FPGA器件240还从CPU 230接收消息并对该消息进行解析，以发现会话丢包消息。在发现会话丢包消息后，FPGA器件240设置会话丢包标志位，此条会话后续报文直接丢弃，不用上送CPU 230进行处理，从而大大减轻了CPU 230处理SSL流量的负担。

[0048] 该CPU 230通过PCIE总线访问并管理FPGA器件240。CPU 230从FPGA器件240收到报文后，从报文内容中提取报文的会话五元组(源IP、目的IP、协议号、源端口、目的端口)，并根据会话五元组查找会话。如果找不到包含所述会话五元组的会话，根据会话五元组建立会话。如果能找到包含所述会话五元组的会话，则进行深度报文检测，而如果经过深度报文检测发现是SSL协议报文，在会话上设置审计标志位，后续此条会话报文均要进入SSL流量审计采集，以提取访问网站、证书、加密套件等信息，待提取信息完成后，生成流量审计日志。

[0049] 在此同时，该CPU 230还构造会话丢包消息发送给FPGA器件240进行处理，会话丢包信息包含会话五元组以及丢包动作。

[0050] 以下将对FPGA器件240和CPU 230的结构和功能进一步详细描述。

[0051] 图3示出了根据本公开的一个实施例的FPGA器件240的框图。如图3所示，该FPGA器件240包括FPGA会话管理单元310和FPGA消息管理单元320。

[0052] FPGA会话管理单元310收到报文，从报文内容中提取报文的会话五元组(源IP、目的IP、协议号、源端口、目的端口)，根据报文的会话五元组(源IP、目的IP、协议号、源端口、目的端口)查询会话，并且如果找不到包含所述会话五元组的会话，则根据会话五元组建立会话，而如果找到包含所述会话五元组的会话，则查找会话中的丢包标志位，以检查是否需要丢弃该报文。如果需要丢弃报文，那么直接丢弃，否则将报文通过网络控制器220(如图2所示)上送到CPU 230进行处理。

[0053] FPGA消息管理单元320负责接收CPU 230的消息报文，支持解析报文，以发现会话丢包消息。在发现会话丢包消息后，根据会话丢包消息设置会话转发状态，如通过设置会话丢包标志位丢弃后续会话报文，从而控制报文是否上送CPU 230。

[0054] 图4示出了根据本公开的一个实施例的CPU 230的框图。如图4所示，该CPU 230主要包含CPU会话管理单元410、深度报文检测单元420、SSL流量审计单元430、日志管理单元440、CPU消息管理单元450。

[0055] CPU会话管理单元410具有与图3中所示的FPGA会话管理单元310相似的结构和功能，但CPU会话管理单元410不是从图2所示的交换器件210而是从图3所示的网络控制器220接收报文，然后从所接收到的报文内容中提取该报文的会话五元组(源IP、目的IP、协议号、源端口、目的端口)，根据报文的会话五元组(源IP、目的IP、协议号、源端口、目的端口)查询会话，并且如果找不到包含所述会话五元组的会话，则根据会话五元组建立会话，而如果找

到包含所述会话五元组的会话，则将其交给深度报文检测单元420进行深度报文检测分析。

[0056] 深度报文检测单元420对从CPU会话管理单元410所接收的报文基于会话维度进行深度报文检测分析，以检测报文所属于的应用层协议、病毒、攻击等。如果经过深度报文检测发现是SSL协议报文，则在会话上设置审计标志位，以表示后续此条会话报文均要进入SSL流量审计采集，以提取访问网站、证书、加密套件等信息，待提取信息完成后，生成流量审计日志。

[0057] SSL流量审计采集单元430判断从深度报文检测单元420接收到的会话上是否有深度报文检测单元420设置的审计标志位，并对有审计标志位的会话进行SSL流量审计采集以提取访问网站、证书、加密套件等信息，并待提取信息完成后，生成流量审计日志。

[0058] 日志管理单元440对审计日志进行维护管理，如支持以TLV、JSON、XML、SYSLOG等格式进行发送。

[0059] CPU消息管理单元450根据业务要求，对如图2所示的FPGA器件240提交的消息进行业务处理，如生成基于会话的丢包消息，以通知FPGA器件240的FPGA消息管理单元320(如图3所示)，后续报文不用上送CPU 230。

[0060] 图5是根据本公开的用于SSL流量审计采集系统的流量审计采集方法的流程图。在图5的步骤S510中，在FPGA器件收到报文后，从报文内容中提取报文的会话五元组(源IP、目的IP、协议号、源端口、目的端口)，根据会话五元组查找会话，如果找不到包含所述会话五元组的会话，则根据会话五元组建立会话。如果能找到包含所述会话五元组的会话，则查找会话丢包标志位，以检查是否需要丢弃报文，如果需要丢弃报文，那么直接丢弃，否则将报文通过网络控制器上送到CPU进行处理。

[0061] 接下来，在步骤S520中，CPU接收到报文后，从报文内容中提取报文的会话五元组(源IP、目的IP、协议号、源端口、目的端口)，根据会话五元组查找会话，并且如果找不到包含所述会话五元组的会话，则根据会话五元组建立会话。

[0062] 如果在步骤S520中找到了会话，则在步骤S530中对所接收的报文基于会话维度进行深度报文检测分析，以检测报文所属于的应用层协议、病毒、攻击等。如果经过深度报文检测发现是SSL协议报文，在会话上设置审计标志位，后续此条会话报文均要进入SSL流量审计采集，以提取访问网站、证书、加密套件等信息，待提取信息完成后，生成流量审计日志。

[0063] 在步骤S540中，对有审计标志位的会话进行SSL流量审计采集以提取访问网站、证书、加密套件等信息，并待提取信息完成后，生成流量审计日志。

[0064] 在步骤S550中，对审计日志进行维护管理，如支持以TLV、JSON、XML、SYSLOG等格式进行发送。

[0065] 在步骤S560中，根据业务要求，对FPGA器件提交的消息进行业务处理，如生成基于会话的丢包消息，以通知FPGA器件后续报文不用上送CPU。

[0066] 最后，在步骤S570中，FPGA器件接收CPU的消息报文，支持解析报文，以发现会话丢包消息。在发现会话丢包消息后，根据会话丢包消息设置会话转发状态，如通过设置会话丢包标志位丢弃后续会话报文，从而控制报文是否上送CPU 230。

[0067] 本公开根据上述技术方案，不仅能实现对SSL流量进行审计，而且一旦提取到访问网站、证书、加密套件等信息后，通过生成流量审计日志，将审计日志交付给日志管理单元

440(如图所示)处理,后续会话流量就不用上送CPU 230(如图2所示)进行处理,从而大大减轻CPU 230处理SSL流量审计的负担,提升了SSL流量审计采集系统性能,减少了硬件投资成本,降低了对能源及机房空间的需求,绿色环保。

[0068] 概括而言,硬件上需要增加一个FPGA芯片通过PCIE与CPU互联。设备在硬件设计中除了CPU、网络控制器、交换芯片(Switch)等关键器件外,还需要增加一个FPGA芯片作为以太网卡,CPU通过PCIE总线访问管理FPGA芯片。由于FPGA芯片可以扩展以太网接口,所以收包方向FPGA芯片和交换芯片(Switch)通过以太网口相连,而发包方向CPU则通过网络控制器和交换芯片(Switch)以太网口相连。在收包时,交换芯片(Switch)将入接口(Eth0～EthN)收到的报文通过与FPGA芯片相连的以太网口(上图侧ieth接口)发送给FPGA芯片。FPGA芯片收到报文后,从报文内容中提取报文的五元组(源IP、目的IP、协议号、源Port、目的Port),根据五元组查找会话,如果找不到会话,根据五元组建立会话。如果能找到会话,查找会话丢包标志位,检查是否需要丢弃报文,如果需要丢弃报文,那么直接丢弃,否则将报文通过网络控制器上送到CPU进行处理。CPU收到报文后,从报文内容中提取报文的五元组(源IP、目的IP、协议号、源Port、目的Port),根据五元组查找会话,如果找不到会话,根据五元组建立会话。如果能找到会话,进行DPI深度业务分析,经过DPI分析,如果发现是SSL协议报文,在会话上设置审计标志位,后续此条会话报文均要进入SSL流量审计模块进行处理,以提取访问网站、证书、加密套件等信息,待提取信息完成后,构造审计日志发到日志处理模块进行处理;同时构造会话丢包消息发送给FPGA进行处理,会话丢包信息包含会话五元组以及丢包动作,FPGA消息处理模块收到消息后,对消息进行解析,发现是会话丢包消息后,设置会话丢包标志位,此条会话后续报文直接丢弃,不用上送CPU进行处理,从而大大减轻了CPU处理SSL流量的负担。

[0069] 本公开的FPGA会话管理单元负责根据报文五元组(源IP、目的IP、协议号、源Port、目的Port)建立会话、老化会话,以及根据查询条件会话查询等功能。本公开的FPGA消息管理单元负责接收CPU消息报文,支持解析报文,根据消息消息设置会话转发状态,如通过设置会话报文丢弃标志位丢弃后续会话报文,从而控制报文是否上送CPU。本公开的CPU会话管理单元同FPGA会话管理单元。本公开的DPI深度包检测单元对接收的报文基于会话维度进行DPI深度包检测,以检测报文所属于的应用层协议、病毒、攻击等。本公开的CPU SSL流量审计单元对SSL流量进行审计,以提取访问网站、证书、加密套件等信息。本公开的CPU日志管理单元对审计日志进行管理,如支持TLV、JSON、XML、SYSLOG等格式进行发送。本公开的CPU消息管理单元根据业务模块生成和FPGA通信的消息,以进行业务处理,如生成基于会话的丢包消息,通知FPGA后续报文不上送CPU。

[0070] 以上结合具体实施例描述了本公开的基本原理,但是需要指出的是,对本领域的普通技术人员而言,能够理解本公开的方法和系统的全部或者任何步骤或者部件,可以在任何计算装置(包括处理器、存储介质等)或者计算装置的网络中,以硬件、固件、软件或者它们的组合加以实现,这是本领域普通技术人员在阅读了本公开的说明的情况下运用他们的基本编程技能就能实现的。

[0071] 因此,本公开的目的还可以通过在任何计算装置上运行一个程序或者一组程序来实现。所述计算装置可以是公知的通用装置。因此,本公开的目的也可以仅仅通过提供包含实现所述方法或者系统的程序代码的程序产品来实现。也就是说,这样的程序产品也构成

本公开，并且存储有这样的程序产品的存储介质也构成本公开。显然，所述存储介质可以是任何公知的存储介质或者将来所开发出来的任何存储介质。

[0072] 还需要指出的是，在本公开的系统和方法中，显然，各部件或各步骤是可以分解和/或重新组合的。这些分解和/或重新组合应视为本公开的等效方案。并且，执行上述系列处理的步骤可以自然地按照说明的顺序按时间顺序执行，但是并不需要一定按照时间顺序执行。某些步骤可以并行或彼此独立地执行。

[0073] 上述具体实施方式，并不构成对本公开保护范围的限制。本领域技术人员应该明白的是，取决于设计要求和其他因素，可以发生各种各样的修改、组合、子组合和替代。任何在本公开的精神和原则之内所作的修改、等同替换和改进等，均应包含在本公开保护范围之内。

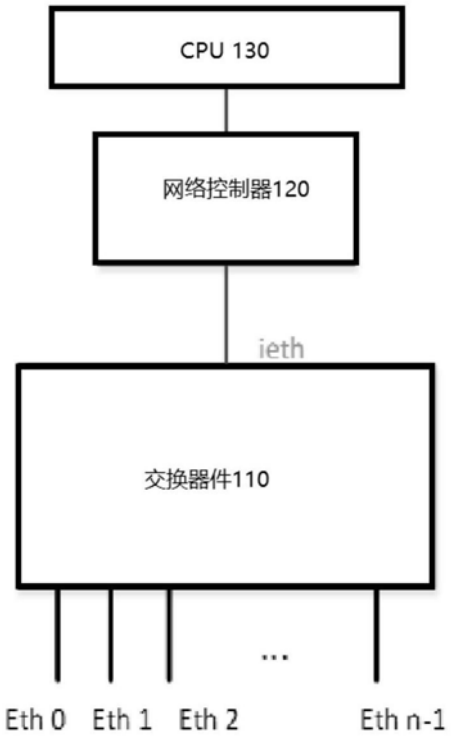
CPU 130
网络控制器120
ieth
交换器件110
...
Eth 0
Eth 1
Eth 2
Eth n-1

图1

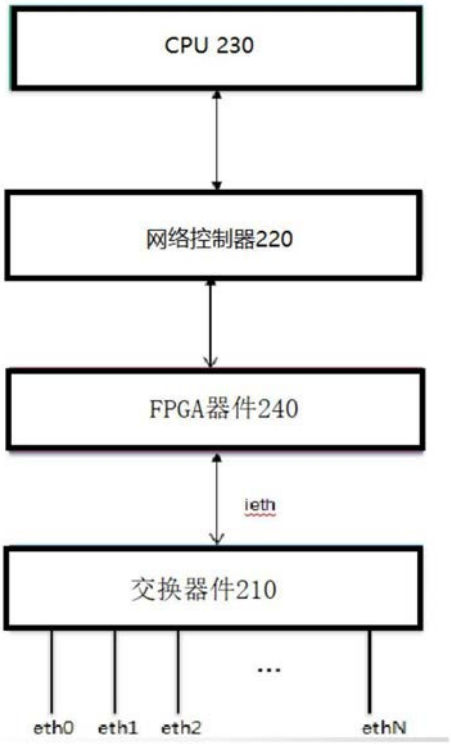
CPU 230
网络控制器220
FPGA器件240
ieth
交换器件210
...
eth0
eth1
eth2
ethN

图2

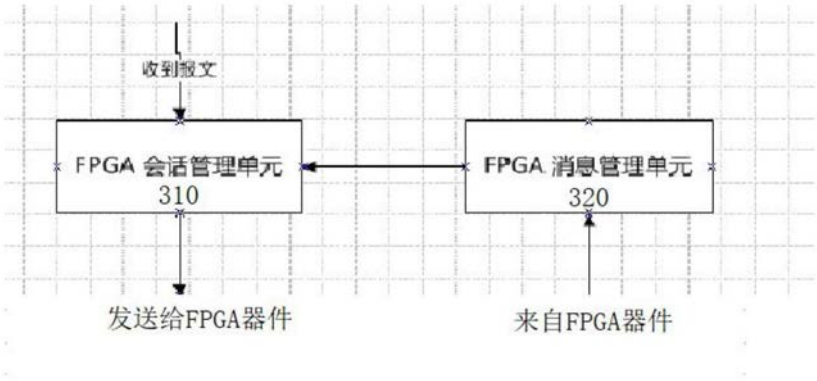
收到报文
FPGA 会话管理单元
310
FPGA 消息管理单元
320
发送给FPGA器件
来自FPGA器件

图3

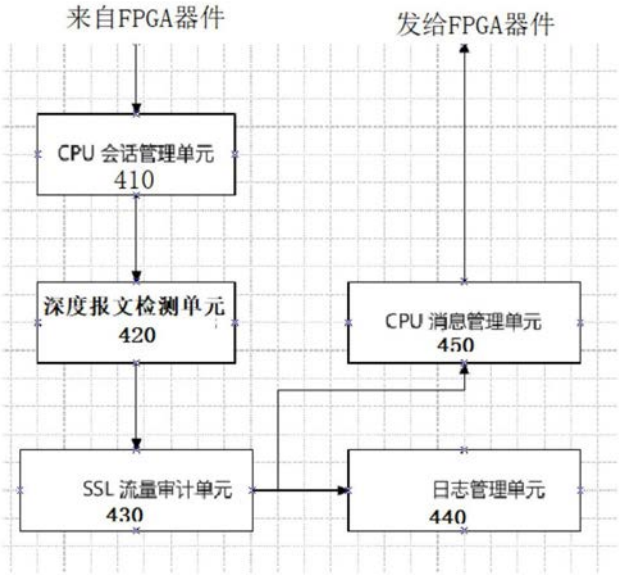
来自FPGA器件
发给FPGA器件
CPU 会话管理单元
410
深度报文检测单元
420
CPU 消息管理单元
450
SSL 流量审计单元
430
日志管理单元
440

图4

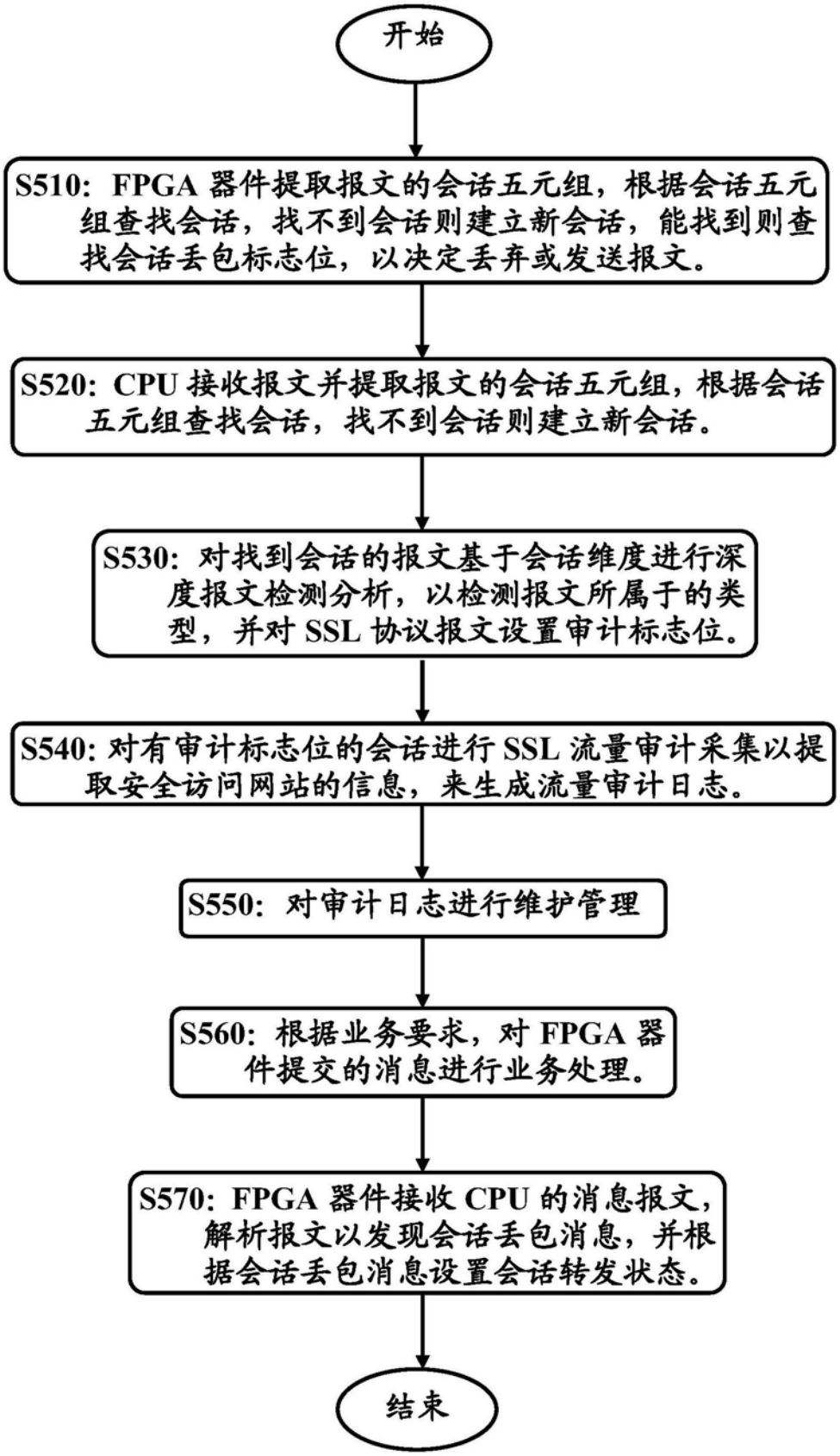
开始
S510: FPGA 器件提取报文的会话五元组，根据会话五元组查找会话，找不到会话则建立新会话，能找到则查找会话丢包标志位，以决定丢弃或发送报文。
S520: CPU 接收报文并提取报文的会话五元组，根据会话五元组查找会话，找不到会话则建立新会话。
S530: 对找到会话的报文基于会话维度进行深度报文检测分析，以检测报文所属于的类型，并对 SSL 协议报文设置审计标志位。
S540: 对有审计标志位的会话进行 SSL 流量审计采集以提取安全访问网站的信息，来生成流量审计日志。
S550: 对审计日志进行维护管理
S560: 根据业务要求，对 FPGA 器件提交的消息进行业务处理。
S570: FPGA 器件接收 CPU 的消息报文，解析报文以发现会话丢包消息，并根据会话丢包消息设置会话转发状态。
结束

图5