(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 110677396 A
(43)申请公布日 2020.01.10

(21)申请号 201910869707.9

(22)申请日 2019.09.16

(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 叶一聪 吴庆 王树太

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 陈蕾

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

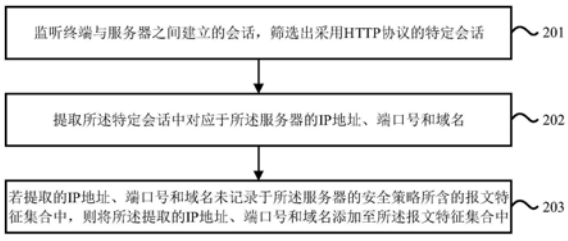
权利要求书2页 说明书9页 附图4页

(54)发明名称

一种安全策略配置方法和装置

(57)摘要

本申请提供一种安全策略配置方法和装置，应用于网络安全设备，通过监听终端与服务器之间建立的会话，筛选出采用HTTP协议的特定会话；提取所述特定会话中对应于所述服务器的IP地址、端口号和域名；若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中，则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中。通过本申请的技术方案，可以对服务器的安全策略所含的报文特征集合进行自动更新，保证了安全策略覆盖所有的Web服务，为服务器提供全面地安全防护。




CN 110677396 A

1.一种安全策略配置方法,其特征在于,包括:

通过监听终端与服务器之间建立的会话,筛选出采用HTTP协议的特定会话;

提取所述特定会话中对应于所述服务器的IP地址、端口号和域名;

若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中,则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中。

2.根据权利要求1所述的方法,其特征在于,所述筛选出采用HTTP协议的特定会话,包括:

提取监听到的任一会话中对应于所述服务器的IP地址和端口号;

将提取的IP地址和端口号与预设的检测状态表进行匹配,所述检测状态表记录了终端与服务器之间已建立的所有会话的IP地址、端口号与相应会话是否采用HTTP协议的映射关系;

根据匹配结果确定所述任一会话是否采用HTTP协议。

3.根据权利要求1所述的方法,其特征在于,所述筛选出采用HTTP协议的特定会话,包括:

对监听到的任一会话中传输的请求报文和响应报文进行格式分析,以确定是否与HTTP协议报文格式匹配;

若所述请求报文和所述响应报文均匹配于所述HTTP协议报文格式,则判定所述任一会话采用HTTP协议。

4.根据权利要求1所述的方法,其特征在于,所述若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中,则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中,包括:

将提取的任一特定会话的IP地址、端口号和域名与预设的检测结果表进行匹配,所述检测结果表记录了已添加至所述报文特征集合的所有IP地址、端口号与相应域名的映射关系;

当匹配结果表明所述检测结果表未包含所述任一特定会话的IP地址、端口号和域名时,将所述任一特定会话的IP地址、端口号和域名添加至所述检测结果表中;

根据所述检测结果表对所述报文特征集合进行同步,以将所述任一特定会话的IP地址、端口号和域名添加至所述报文特征集合中。

5.根据权利要求1所述的方法,其特征在于,所述若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中,则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中,包括:

将提取的任一特定会话的IP地址、端口号和域名与所述报文特征集合进行匹配;

当匹配结果表明所述报文特征集合未包含所述任一特定会话的IP地址、端口号和域名时,将所述任一特定会话的IP地址、端口号和域名添加至所述报文特征集合中。

6.一种安全策略配置装置,其特征在于,包括:

筛选单元,用于通过监听终端与服务器之间建立的会话,筛选出采用HTTP协议的特定会话;

提取单元,用于提取所述特定会话中对应于所述服务器的IP地址、端口号和域名;

添加单元,用于在提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含

的报文特征集合的情况下，将所述提取的IP地址、端口号和域名添加至所述报文特征集合中。

7.根据权利要求6所述的装置，其特征在于，所述筛选单元具体用于：

提取监听到的任一会话中对应于所述服务器的IP地址和端口号；

将提取的IP地址和端口号与预设的检测状态表进行匹配，所述检测状态表记录了终端与服务器之间已建立的所有会话的IP地址、端口号与相应会话是否使用HTTP协议的映射关系；

根据匹配结果确定所述任一会话是否采用HTTP协议。

8.根据权利要求6所述的装置，其特征在于，所述筛选单元具体用于：

对监听到的任一会话中传输的请求报文和响应报文进行格式分析，以确定是否与HTTP协议报文格式匹配；

若所述请求报文和所述响应报文均匹配于所述HTTP协议报文格式，则判定所述任一会话采用HTTP协议。

9.根据权利要求6所述的装置，其特征在于，所述添加单元具体用于：

将提取的任一特定会话的IP地址、端口号和域名与预设的检测结果表进行匹配，所述检测结果表记录了已添加至所述报文特征集合的所有IP地址、端口号与相应域名的映射关系；

当匹配结果表明所述检测结果表未包含所述任一特定会话的IP地址、端口号和域名时，将所述任一特定会话的IP地址、端口号和域名添加至所述检测结果表中；

根据所述检测结果表对所述报文特征集合进行同步，以将所述任一特定会话的IP地址、端口号和域名添加至所述报文特征集合中。

10.根据权利要求6所述的装置，其特征在于，所述添加单元具体用于：

将提取的任一特定会话的IP地址、端口号和域名与所述报文特征集合进行匹配；

当匹配结果表明所述报文特征集合未包含所述任一特定会话的IP地址、端口号和域名时，将所述任一特定会话的IP地址、端口号和域名添加至所述报文特征集合中。

11.一种电子设备，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如权利要求1-5中任一项所述的方法。

12.一种计算机可读存储介质，其上存储有计算机指令，其特征在于，该指令被处理器执行时实现如权利要求1-5中任一项所述方法的步骤。

# 一种安全策略配置方法和装置

## 技术领域

[0001] 本申请涉及通信技术领域,特别涉及一种安全策略配置方法和装置。

## 背景技术

[0002] 随着网络技术的迅速发展,给社会提供便捷的同时也带来了威胁,Web服务器安全问题就是其中之一。用户通过终端设备在浏览器中输入Web服务对应的IP地址、域名或者端口与Web服务器进行信息交流,而对应的Web服务器采用HTTP/HTTPS协议提供给终端网上信息浏览服务。

[0003] 网络安全设备一般部署在Web服务器前端,为相应的Web服务器配置安全策略来为Web服务提供保护。目前,安全策略的配置往往需要网络管理员收集服务器对外提供的Web服务信息,然后手动将对应的IP地址、端口号和域名加入到网络安全设备的安全策略中,从而实现对服务器的防护。

[0004] 由于Web服务对应的IP地址、域名和端口具有多样性和可变性,网络管理员手动为Web服务配置安全策略,往往无法全面覆盖所有的Web服务,导致Web服务器容易被攻击。

## 发明内容

[0005] 有鉴于此,本申请提供了安全策略配置方法和装置,以实现自动为Web服务配置安全策略,全面地为服务器提供防护。

[0006] 具体地,本申请是通过如下技术方案实现的:

[0007] 根据本申请的第一方面,提供了一种安全策略配置方法,该方法应用于网络安全设备,包括:

[0008] 通过监听终端与服务器之间建立的会话,筛选出采用HTTP协议的特定会话;

[0009] 提取所述特定会话中对应于所述服务器的IP地址、端口号和域名;

[0010] 若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中,则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中。

[0011] 根据本申请的第二方面,提供了一种安全策略配置装置,该装置应用于网络安全设备,包括:

[0012] 筛选单元,用于通过监听终端与服务器之间建立的会话,筛选出采用HTTP协议的特定会话;

[0013] 提取单元,用于提取所述特定会话中对应于所述服务器的IP地址、端口号和域名;

[0014] 添加单元,用于在提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合的情况下,将所述提取的IP地址、端口号和域名添加至所述报文特征集合中。

[0015] 根据本申请的第三方面,提供一种电子设备。所述电子设备包括:

[0016] 处理器;

[0017] 用于存储处理器可执行指令的存储器;

[0018] 其中,所述处理器通过运行所述可执行指令以实现上述的安全策略配置方法。

[0019] 根据本申请的第四方面,提供一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现上述的安全策略配置方法。

[0020] 本申请基于上述技术方案,通过监听终端与服务器之间建立的会话,可以及时对服务器的安全策略所含的报文特征集合进行自动更新,保证了安全策略覆盖所有的Web服务,为服务器提供全面地安全防护。

## 附图说明

[0021] 图1是网络安全设备配置安全策略的示意图。

[0022] 图2是本申请示出的一种安全策略配置方法的流程图。

[0023] 图3是本申请一示例性实施例示出的一种安全策略配置方法的流程图。

[0024] 图4是本申请一示例性实施例示出的另一种安全策略配置方法的流程图。

[0025] 图5是本申请一示例性实施例示出的一种电子设备的结构示意图。

[0026] 图6是本申请一示例性实施例示出的一种安全策略配置装置的框图。

## 具体实施方式

[0027] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0028] 在本申请使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0029] 应当理解,尽管在本申请可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本申请范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0030] 图1是网络安全设备配置安全策略的示意图。如图1所示,用户的终端设备与服务器之间通过建立会话来进行信息传递,网络安全设备部署在网络服务器前端,监听客户端与服务器之间建立的会话。本申请实施例中的网络安全设备中配置有针对服务器的安全策略,所述安全策略中所含的报文特征集合记录有服务器提供不同的Web服务对应的IP地址、端口号和域名,网络安全设备可以为报文特征集合开启预定义的安全策略。其中,预定义的安全策略可以是IP地址拦截或者端口拦截等,而IP地址、端口号和域名可以统称为报文特征。所述终端设备是指具有信息浏览功能的设备,可以包括用户设备、无线终端设备、移动终端设备等,例如,可以包括移动电话,便携式、手持式或者车载的信息浏览装置,本申请并不具体限定。

[0031] 在服务器提供Web服务的过程中,服务器对应的IP地址、端口号和域名具有多样性

和多变性，在相关技术中，网络安全设备中的安全策略所含的报文特征集合依赖于网络管理员手动配置，容易导致安全策略所含的报文特征集合不能及时和全面地覆盖Web服务，容易导致服务器被攻击。

[0032] 因此，本申请通过改进服务器的安全策略所含报文特征集合的更新方式以解决相关技术中存在的上述技术问题。下面结合实施例进行详细说明。

[0033] 图2是本申请示出的一种安全策略配置方法的流程图。如图2所示，该方法应用于网络安全设备；可以包括以下步骤：

[0034] 步骤201，监听终端与服务器之间建立的会话，筛选出采用HTTP协议的特定会话。

[0035] 在一个实施例中，网络安全设备对监听到的会话中的请求报文和响应报文进行格式分析，从而确定该会话是否采用HTTP协议。其中，将监听到的采用HTTP协议的会话称为特定会话。

[0036] 网络安全设备先对会话中正向传输的请求报文进行格式分析，判断其是否采用HTTP协议。如果请求报文不满足采用HTTP协议请求报文的格式内容，则判定该会话不采用HTTP协议，不需要对响应报文进行格式分析；如果请求报文满足采用HTTP协议请求报文的格式内容，则继续对响应报文的格式内容进行分析。当会话的请求报文和响应报文都匹配于相应的格式内容，则可以判定该会话为采用HTTP协议的会话。

[0037] 在另一实施例中，网络安全设备可以提取监听到的会话中的IP地址和端口号，并在预设的检测状态表中进行查询，从而判断该会话是否采用HTTP协议。

[0038] 在网络安全设备中预先设置有检测状态表，记录了终端与服务器之间已经建立的所有会话的IP地址、端口号以及相应会话是否采用HTTP协议的映射关系。网络安全设备根据监听到的会话的IP地址和端口号在检测状态表中进行查询，可以快速获得该会话是否采用HTTP协议。如果未在检测状态表中查询到，则需要根据该会话中的请求报文和响应报文进行格式分析，从而判断其是否采用HTTP协议。

[0039] 步骤202，提取所述特定会话中对应于所述服务器的IP地址、端口号和域名。

[0040] 网络安全设备对监听到的采用HTTP协议的会话，提取该会话对应服务器的IP地址、端口号和域名。其中，IP地址、端口号和域名可以统称为报文特征。

[0041] 步骤203，若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中，则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中。

[0042] 在一个实施例中，网络安全设备将提取的IP地址、端口号和域名在对应的针对服务器的安全策略所含的报文特征集合中查询，如果某一会话的IP地址、端口号和域名在所述的报文特征集合中查询到，则不将其添加至所述报文特征集合中；如果某一会话的IP地址、端口号和域名未在所述的报文特征集合中查询到，则将其添加至所述报文特征集合中。

[0043] 在另一实施例中，网络安全设备将提取的IP地址、端口号和域名在预设的检测结果表中进行查询，从而判断是否将所述提取的IP地址、端口号和域名添加至检测结果表中。在网络安全设备中预先设置有检测结果表，记录了已经添加至安全策略所含的报文特征集合中的所有IP地址、端口号和域名的映射关系。如果提取到的IP地址、端口号和域名在检测结果表中查询到，则不将其添加至所述检测结果表中；如果提取到的IP地址、端口号和域名在检测结果表中未查询到，则将其添加至所述检测结果表中。然后将检测结果表与服务器的安全策略所含的报文特征集合进行匹配，将记录在检测结果表中而未记录在报文特征集

合中的IP地址、端口号和域名添加至报文特征集合中。

[0044] 由上述技术方案可见，本申请通过监听终端与服务器之间建立的会话并且提取会话中对应服务器的报文特征，可以根据提取到的报文特征将针对服务器的安全策略所含的报文特征集合进行自动更新，可以实现服务器的安全策略覆盖所有的Web服务，以使得服务器获得全面的防护。

[0045] 为了便于理解，下面结合附图对本申请的技术方案进行进一步说明。请参见图3，图3是本申请一示例性实施例一种安全策略配置方法的流程图。如图3所示，该方法应用于网络安全设备；可以包括以下步骤：

[0046] 步骤301，监听终端与服务器之间建立的会话。

[0047] 步骤302，判断是否采用HTTP协议。

[0048] 对监听到的会话中的请求报文和响应报文进行格式分析，从而判断该会话是否采用HTTP协议。其中，将监听到的采用HTTP协议的会话称为特定会话。

[0049] 网络安全设备对会话中正向传输的请求报文进行格式分析，从而判断其是否采用HTTP协议。其中，采用HTTP协议的请求报文的格式要求为：第一行以一个方法符号开始，以空格分开，后面为请求的URI(Uniform ResourceIdentifier，统一资源标识符)，再以空格分开，后面为协议的版本号，最后以回车换行结尾，接着以“名字+冒号(:)+空格+值+回车换行”的格式重复，最后以回车换行为单独一行结尾。

[0050] 如果请求报文不满足上述格式内容，则判定该会话不采用HTTP协议，不需要对响应报文进行格式分析。

[0051] 如果请求报文满足上述格式内容，则继续对响应报文进行格式分析。采用HTTP协议的响应报文的格式要求为：第一行以服务器HTTP协议的版本开始，以空格分开，后面为服务器发回的响应状态代码，再以空格分开，后面为状态代码的文本描述，最后以回车换行为单独一行结尾。

[0052] 如果请求报文和响应报文均匹配于HTTP协议格式内容，则判定该会话为采用HTTP协议的特定会话。

[0053] 步骤303，提取特定会话中对应于所述服务器的报文特征。

[0054] 提取特定会话中的对应于所述服务器的报文特征可以包括，提取满足HTTP协议的会话中对应于所述服务器的IP地址、端口号和域名。IP地址、端口号和域名可以统称为报文特征。

[0055] 步骤304，将报文特征与安全策略的报文特征集合进行匹配。

[0056] 将提取的特定会话的IP地址、端口号和域名在针对服务器的安全策略所含的报文特征集合中进行查询。若特定会话的IP地址、端口号和域名在所述报文特征集合中查询到时，不将该IP地址、端口号和域名添加至所述报文特征集合中，保持报文特征集合不变。

[0057] 步骤305，若报文特征在所述报文特征集合中未查询到时，将该报文特征添加至所述报文特征集合中。

[0058] 若提取的特定会话的IP地址、端口号和域名在所述报文特征集合中未查询到时，将该特定会话的IP地址、端口号和域名添加至所述报文特征集合中，实现对报文特征集合的更新。

[0059] 由上述技术方案可见，本申请通过监听终端与服务器之间建立的会话并且提取会

话中对应服务器的报文特征，可以根据提取到的报文特征将针对服务器的安全策略所含的报文特征集合进行自动更新，可以实现服务器的安全策略覆盖所有的Web服务，以使得服务器获得全面的防护。

[0060] 图4是本申请一示例性实施例示出的另一种安全策略配置方法的流程图。如图4所示，该方法应用于网络安全设备，可以包括以下步骤：

[0061] 步骤401，监听终端与服务器之间建立的会话。

[0062] 步骤402，提取IP地址和端口号，判断是否记录在检测状态表中。

[0063] 提取监听到的终端与服务器之间建立的会话中对应服务器的IP地址和端口号，判断该IP地址和端口号是否记录在检测状态表中。

[0064] 在网络安全设备中预先设置有检测状态表，如下表1所示，记录了终端与服务器之间已经建立的所有会话的IP地址、端口号以及相应会话是否采用HTTP协议的映射关系。

[0065] 表1

[0066]

| IP地址 | 端口号 | 是/否采用HTTP协议 |
|---|---|---|
| 192.168.0.1 | 80 | 是 |
| 192.168.0.2 | 8081 | 是 |
| 192.168.0.3 | 8080 | 否 |
| …… | …… | …… |

[0067] 根据提取的会话中的IP地址和端口号，在检测状态表中进行查询，可以快速得到该IP地址和端口号对应的会话是否采用HTTP协议。

[0068] 步骤403，在检测状态表查询是否采用HTTP协议。

[0069] 如果提取的IP地址和端口号在检测状态表中查询到，则直接根据检测状态表的记录可以快速获得该会话是否采用HTTP协议。通过在检测状态表中对IP地址和端口号的查询，可以快速判断该会话是否采用HTTP协议，避免了每次都需要对会话中的请求报文和响应报文进行格式分析。

[0070] 如果查询到该会话采用HTTP协议则转入步骤405；如果查询到该会话没有采用HTTP协议，则不需要对该会话进行处理。

[0071] 步骤404，判断是否采用HTTP协议。

[0072] 如果提取的IP地址和端口号在检测状态表中未查询到，对该会话中的请求报文和响应报文进行格式分析，判断该会话是否采用HTTP协议，与步骤302相同，这里不再赘述，判断结束后需要将该会话的IP地址、端口号和是否采用HTTP协议的映射关系添加至检测状态表中。

[0073] 步骤405，提取特定会话中的域名。

[0074] 根据采用HTTP协议的会话中的报文格式，解析请求报文，提取其中为Host的值，该值的内容即为域名，以及前面提取到的特定会话中对应于服务器的IP地址和端口号，可以得到该满足HTTP协议的会话中的IP地址、端口号和域名。

[0075] 步骤406，判断IP地址、端口号和域名是否在检测结果表中。

[0076] 根据提取到的特定会话中对应服务器的IP地址、端口号和域名，可以判断该IP地址、端口号和域名是否记录在检测结果表中。

[0077] 在网络安全设备中预先设置有检测结果表，如下表2所示，记录有已经添加至安全

策略的报文特征集合中的所有IP地址、端口号和域名。此外，如下表2所示，相同的IP地址和端口号可能对应不同的域名。

[0078] 如果特定会话的IP地址、端口号和域名在检测结果表中查询到，则保持检测结果表不变。

[0079] 表2

[0080]

| IP地址 | 端口号 | 域名 |
|---|---|---|
| 192.168.0.1 | 80 | abc01.com |
| 192.168.0.2 | 8081 | abc02.com |
| 192.168.0.2 | 8081 | abc03.com |
| …… | …… | …… |

[0081] 步骤407，将IP地址、端口号和域名添加到检测结果表中。

[0082] 如果特定会话的IP地址、端口号和域名在检测结果表中未查询到，将该IP地址、端口号和域名添加至检测结果表中。

[0083] 步骤408，根据检测结果表对报文特征集合进行同步。

[0084] 将检测结果表与服务器的安全策略所含的报文特征集合进行匹配，如果检测结果表中记录的IP地址、端口号和域名在报文特征集合中不存在，则将该IP地址、端口号和域名添加至所述安全策略所含的报文特征集合中；如果检测结果表中记录的IP地址、端口号和域名在安全策略所含的报文特征集合中存在，则保持所述安全策略的报文特征集合不变。通过检测结果表对报文特征集合进行同步，可以避免频繁使用报文特征集合进行查询匹配，可以避免影响安全策略配置的速率。

[0085] 举例而言，假定用户A通过用户的终端设备登录网络，访问某一网站，网络安全设备提取服务器的IP地址为192.168.0.1，端口号为80。假定另一用户B通过用户终端登录网络，访问另一网站，网络安全设备提取到服务器的IP地址为192.168.0.4，端口号为8080。

[0086] 根据上述表1，可以快速查询到用户A与服务器建立的会话在上述表1中有记录，并且该IP地址和端口号对应的会话采用HTTP协议；而用户B与服务器建立的会话中对应的IP地址192.168.0.4和端口号8080在表1中未查询到，因此，需要对该会话中的请求报文和响应报文进行格式分析，来判断该会话是否采用HTTP协议，假定判断结果为该会话采用HTTP协议，将对应的IP地址、端口号和是否采用HTTP协议的映射关系添加至上述表1中，得到结果如下表3所示。实际上，无论该会话是否采用HTTP协议都需要将该会话的IP地址、端口号和是否采用HTTP协议的映射关系添加至上述表1中。

[0087] 表3

[0088]

| IP地址 | 端口号 | 是/否采用HTTP协议 |
|---|---|---|
| 192.168.0.1 | 80 | 是 |
| 192.168.0.2 | 8081 | 是 |
| 192.168.0.3 | 8080 | 否 |
| …… | …… | …… |
| 192.168.0.4 | 8080 | 是 |

[0089] 接着，提取到用户A与服务器建立的会话中服务器的IP地址为192.168.0.1，端口号为80，域名为abc01.com。提取到用户B与服务器建立的会话中服务器的IP地址为

192.168.0.4,端口号8080,域名为abc04.com。

[0090] 根据上述表2进行查询,用户A与服务器建立的会话中提取到的IP地址、端口号和域名在表2中可以查询到,因此,保持表2不变。用户B与服务器建立的会话中提取到的IP地址、端口号和域名在表2中未查询到,因此,将对应的报文特征添加至表2中,得到结果如下表4所示。

[0091] 表4

[0092]

| IP地址 | 端口号 | 域名 |
|---|---|---|
| 192.168.0.1 | 80 | abc01.com |
| 192.168.0.2 | 8081 | abc02.com |
| 192.168.0.2 | 8081 | abc03.com |
| …… | …… | …… |
| 192.168.0.4 | 8080 | abc04.com |

[0093] 将表4的内容与安全策略所含的报文特征集合进行匹配,检测结果表中记录的IP地址、端口号和域名在所述报文特征集合中存在,则保持报文特征集合不变。

[0094] 由上述技术方案可见,本申请通过监听终端与服务器之间建立的会话并且提取会话中对应服务器的报文特征,可以根据提取到的报文特征将针对服务器的安全策略所含的报文特征集合进行自动更新,可以实现服务器的安全策略覆盖所有的Web服务,以使得服务器获得全面的防护。

[0095] 图5示出了根据本申请的一示例性实施例的电子设备的结构示意图。请参考图5,在硬件层面,该电子设备包括处理器501、内部总线502、网络接口503、内存504以及非易失性存储器505,当然还可能包括其他业务所需要的硬件。处理器501从非易失性存储器505中读取对应的计算机程序到内存504中然后运行,在逻辑层面上形成安全策略配置装置。当然,除了软件实现方式之外,本申请并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限定于各个逻辑单元,也可以是硬件或逻辑器件。

[0096] 请参考图6,在软件实施例中,该安全策略配置装置可以包括筛选单元601、提取单元602和添加单元603。其中:

[0097] 筛选单元601,通过监听终端与服务器之间建立的会话,筛选出采用HTTP协议的特定会话;

[0098] 提取单元602,提取所述特定会话中对应于所述服务器的IP地址、端口号和域名;

[0099] 添加单元603,在提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合的情况下,将所述提取的IP地址、端口号和域名添加至所述报文特征集合中。

[0100] 可选的,所述筛选单元可以提取监听到的任一会话中对应于所述服务器的IP地址和端口号,并将提取的IP地址和端口号与预设的检测状态表进行匹配,根据匹配结果确定所述任一会话是否采用HTTP协议。其中,所述检测状态表记录了终端与服务器之间已建立的所有会话的IP地址、端口号与相应会话是否使用HTTP协议的映射关系。

[0101] 可选的,所述筛选单元可以对监听到的任一会话中传输的请求报文和响应报文进行格式分析,以确定是否与HTTP协议报文格式匹配,若所述请求报文和所述响应报文均匹

配于所述HTTP协议报文格式，则判定所述任一会话采用HTTP协议。

[0102] 可选的，还包括：

[0103] 所述添加单元可以将提取的任一特定会话的IP地址、端口号和域名与预设的检测结果表进行匹配，当匹配结果表明所述检测结果表未包含所述任一特定会话的IP地址、端口号和域名时，将所述任一特定会话的IP地址、端口号和域名添加至所述检测结果表中，并根据所述检测结果表对所述报文特征集合进行同步，以将所述任一特定会话的IP地址、端口号和域名添加至所述报文特征集合中。其中，所述检测结果表记录了已添加至所述报文特征集合的所有IP地址、端口号与相应域名的映射关系。

[0104] 可选的，所述添加单元将提取的任一特定会话的IP地址、端口号和域名与所述报文特征集合进行匹配，当匹配结果表明所述报文特征集合未包含所述任一特定会话的IP地址、端口号和域名时，将所述任一特定会话的IP地址、端口号和域名添加至所述报文特征集合中。

[0105] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0106] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0107] 在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器，上述指令可由报文的发送装置的处理器执行以完成上述方法，该方法可以包括：

[0108] 通过监听终端与服务器之间建立的会话，筛选出采用HTTP协议的特定会话；

[0109] 提取所述特定会话中对应于所述服务器的IP地址、端口号和域名；

[0110] 若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中，则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中。

[0111] 可选的，所述筛选出采用HTTP协议的特定会话，包括：提取监听到的任一会话中对应于所述服务器的IP地址和端口号；

[0112] 将提取的IP地址和端口号与预设的检测状态表进行匹配，所述检测状态表记录了终端与服务器之间已建立的所有会话的IP地址、端口号与相应会话是否使用HTTP协议的映射关系；

[0113] 根据匹配结果确定所述任一会话是否采用HTTP协议。

[0114] 可选的，所述筛选出采用HTTP协议的特定会话，包括：对监听到的任一会话中传输的请求报文和响应报文进行格式分析，以确定是否与HTTP协议报文格式匹配；

[0115] 若所述请求报文和所述响应报文均匹配于所述HTTP协议报文格式，则判定所述任一会话采用HTTP协议。

[0116] 可选的，还包括：

[0117] 所述若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文

特征集合中，则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中，包括：将提取的任一特定会话的IP地址、端口号和域名与预设的检测结果表进行匹配，所述检测结果表记录了已添加至所述报文特征集合的所有IP地址、端口号与相应域名的映射关系；

[0118] 当匹配结果表明所述检测结果表未包含所述任一特定会话的IP地址、端口号和域名时，将所述任一特定会话的IP地址、端口号和域名添加至所述检测结果表中；

[0119] 根据所述检测结果表对所述报文特征集合进行同步，以将所述任一特定会话的IP地址、端口号和域名添加至所述报文特征集合中。

[0120] 可选的，所述若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中，则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中，包括：将提取的任一特定会话的IP地址、端口号和域名与所述报文特征集合进行匹配；

[0121] 当匹配结果表明所述报文特征集合未包含所述任一特定会话的IP地址、端口号和域名时，将所述任一特定会话的IP地址、端口号和域名添加至所述报文特征集合中。

[0122] 其中，所述非临时性计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等，本申请并不对此进行限制。

[0123] 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。

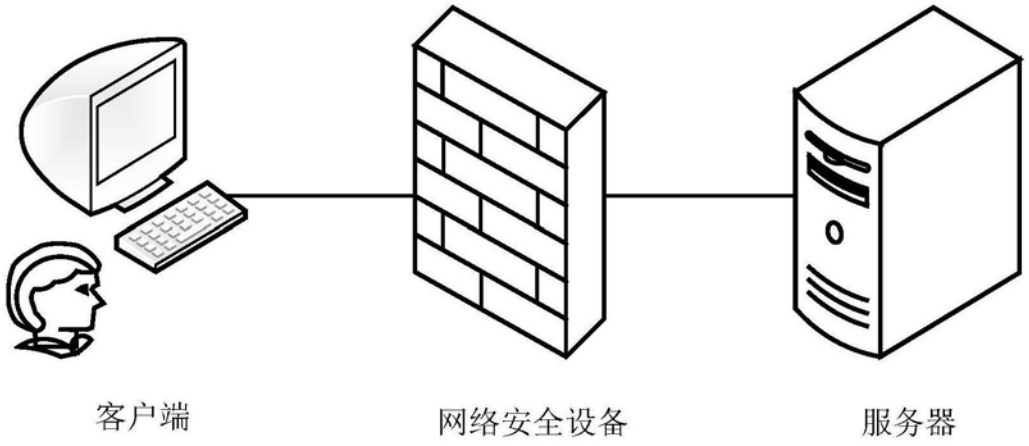

客户端
网络安全设备
服务器

图1

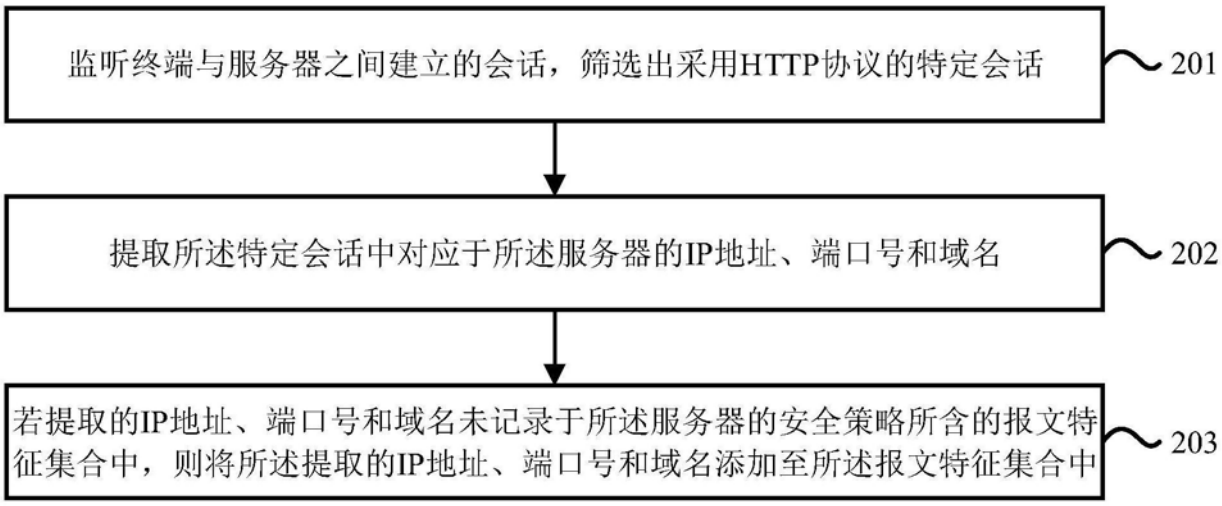

监听终端与服务器之间建立的会话，筛选出采用HTTP协议的特定会话
201
提取所述特定会话中对应于所述服务器的IP地址、端口号和域名
202
若提取的IP地址、端口号和域名未记录于所述服务器的安全策略所含的报文特征集合中，则将所述提取的IP地址、端口号和域名添加至所述报文特征集合中
203

图2

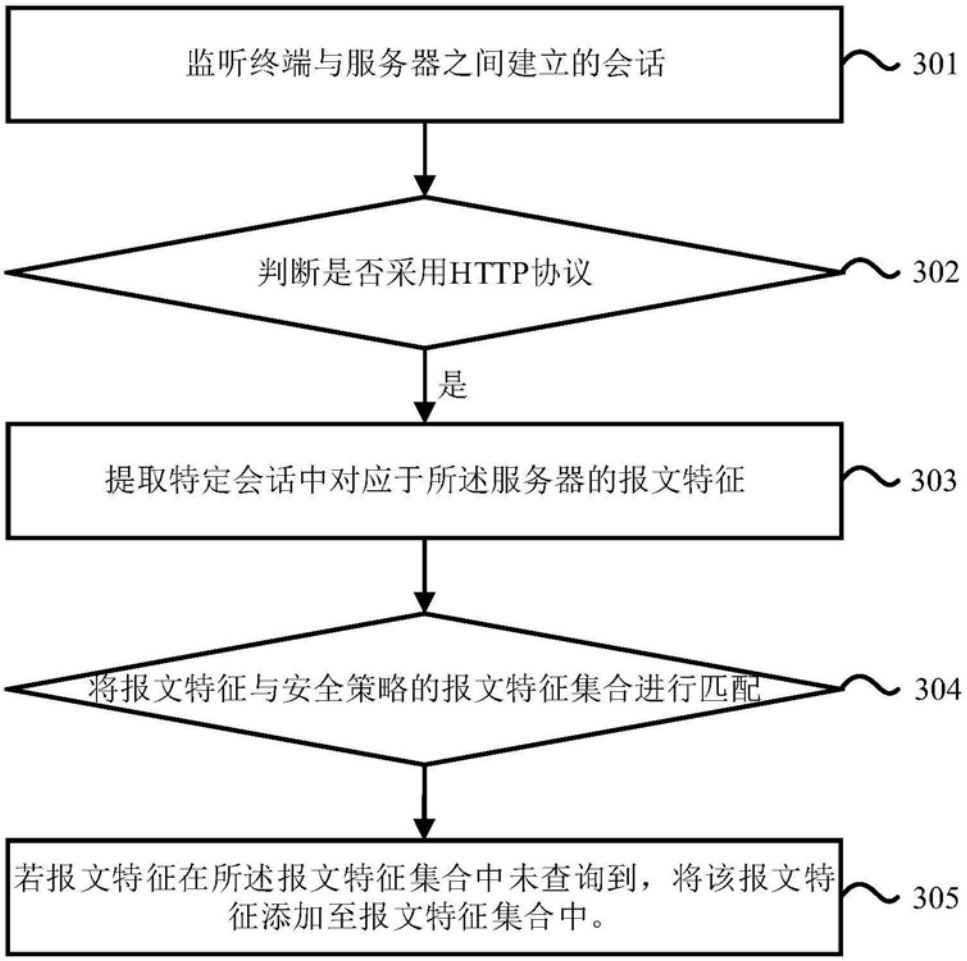

监听终端与服务器之间建立的会话
301
判断是否采用HTTP协议
302
是
提取特定会话中对应于所述服务器的报文特征
303
将报文特征与安全策略的报文特征集合进行匹配
304
若报文特征在所述报文特征集合中未查询到，将该报文特征添加至报文特征集合中。
305

图3

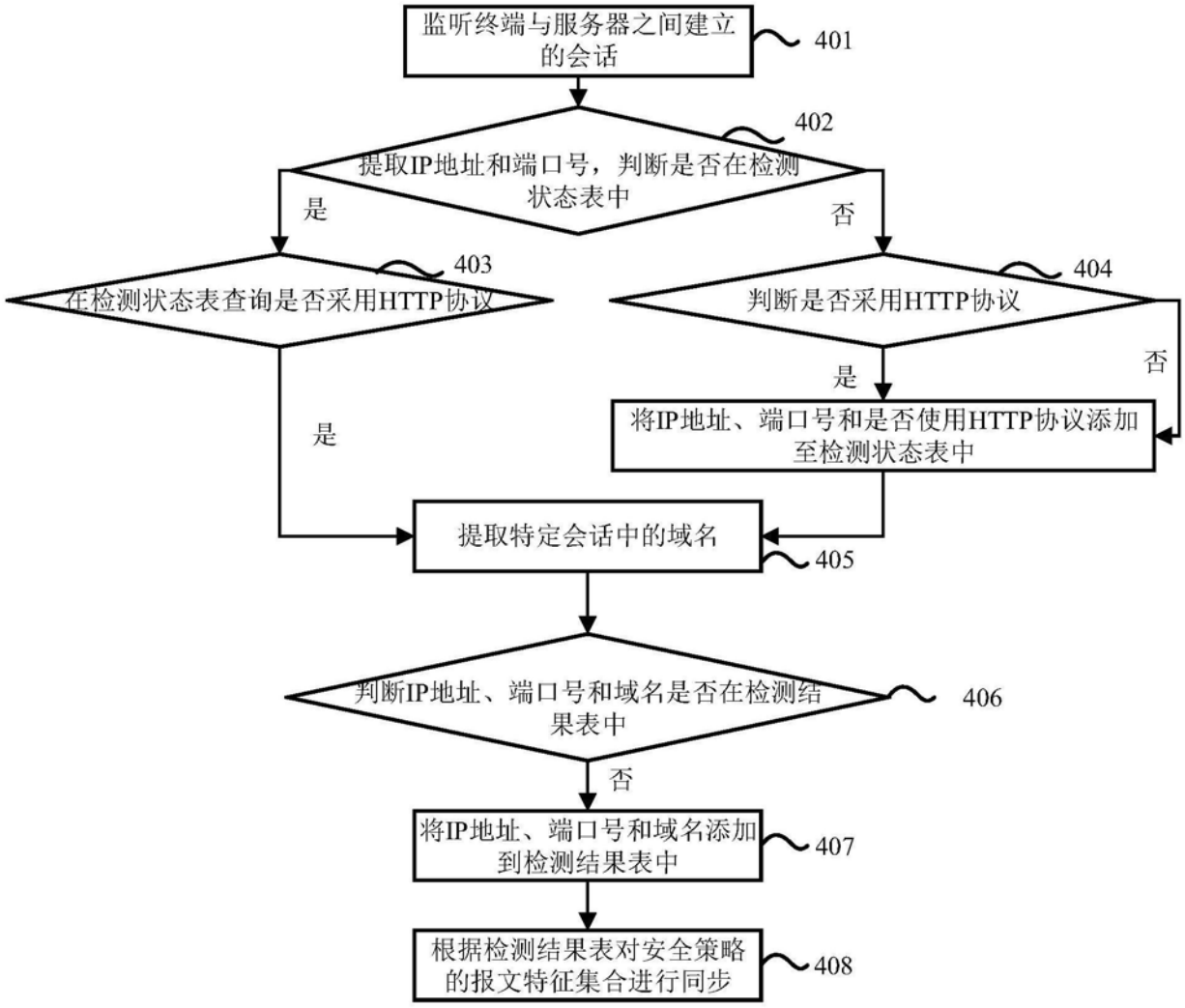

监听终端与服务器之间建立的会话
401
提取IP地址和端口号，判断是否在检测状态表中
402
是
否
在检测状态表查询是否采用HTTP协议
403
判断是否采用HTTP协议
404
是
否
是
将IP地址、端口号和是否使用HTTP协议添加至检测状态表中
提取特定会话中的域名
405
判断IP地址、端口号和域名是否在检测结果表中
406
否
将IP地址、端口号和域名添加到检测结果表中
407
根据检测结果表对安全策略的报文特征集合进行同步
408

图4

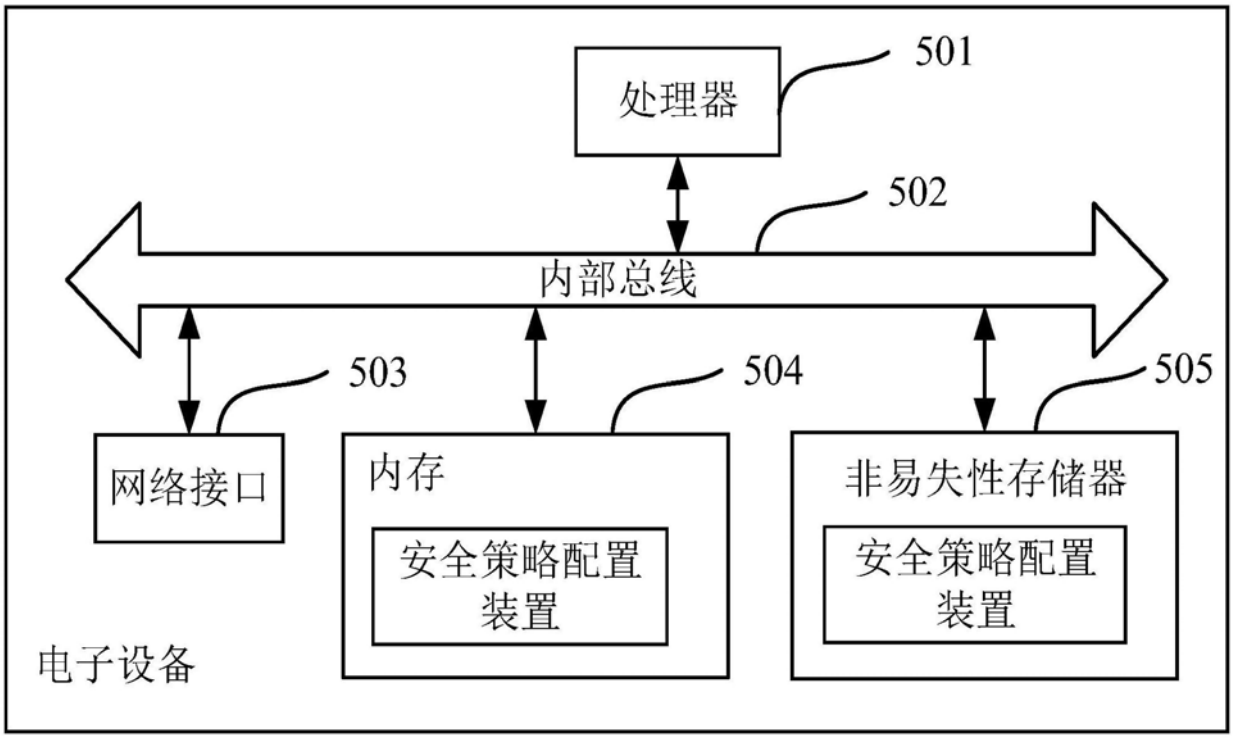



图5

安全策略配置装置


图6