(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 102255909 B
(45)授权公告日 2014.07.02

(21)申请号 201110192688.4
(22)申请日 2011.07.11
(73)专利权人 北京星网锐捷网络技术有限公司
地址 100036 北京市海淀区复兴路33号翠微大厦东1106
(72)发明人 陈平平
(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)
H04L 12/70(2013.01)

(56)对比文件
CN 101958842 A,2011.01.26, 全文.
CN 1697443 A,2005.11.16, 全文.
US 6154775 A,2000.11.28, 全文.

审查员 杨凯鹏

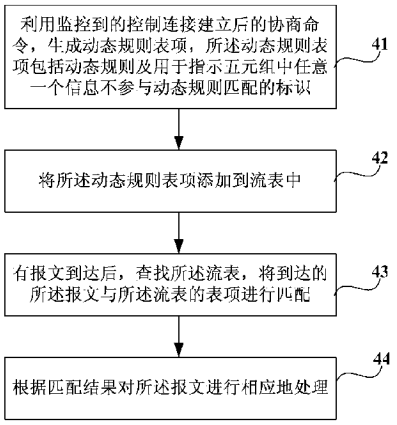
权利要求书1页 说明书6页 附图3页

(54)发明名称

监控会话流的方法及装置

(57)摘要

本发明涉及一种监控会话流的方法及装置，方法包括：利用监控到的控制连接建立后的协商命令，生成动态规则表项，所述动态规则表项包括动态规则及用于指示五元组中任意一个信息不参与动态规则匹配的标识；将所述动态规则表项添加到流表中；有报文到达后，查找所述流表，将到达的所述报文与所述流表的表项进行匹配；根据匹配结果对所述报文进行相应地处理。通过将特殊协议的动态规则与流表共用存储数据结构即动态规则表与流表合并在一起，节约了报文匹配时间，提升了网络安全设备的数据处理性能。



CN 102255909 B

1. 一种监控会话流的方法，其特征在于，包括：

利用监控到的控制连接建立后的协商命令，生成动态规则表项，所述动态规则表项包括动态规则及用于指示五元组中任意一个信息不参与动态规则匹配的标识，其中五元组包括：源 IP 地址、目的 IP 地址、协议号、源端口号、目的端口号；

将所述动态规则表项添加到流表中；

有报文到达后，查找所述流表，将到达的所述报文与所述流表的表项进行匹配；

根据匹配结果对所述报文进行相应地处理。

2. 根据权利要求 1 所述的监控会话流的方法，其特征在于，根据匹配结果对所述报文进行相应地处理的过程，包括：

若所述报文与所述动态规则表项匹配成功，则正常转发所述报文。

3. 根据权利要求 2 所述的监控会话流的方法，其特征在于，所述报文与所述动态规则表项匹配成功后，正常转发所述报文之前还包括：

根据所述报文在所述流表中创建新的流表项。

4. 根据权利要求 1 所述的监控会话流的方法，其特征在于，根据匹配结果对所述报文进行相应地处理的过程，包括：

若所述报文既与所述动态规则表项匹配成功，又与所述流表中的流表项匹配成功，则按照最长匹配结果优先原则，正常转发所述报文。

5. 根据权利要求 1-4 任一项所述的监控会话流的方法，其特征在于，所述标识通过掩码实现。

6. 一种监控会话流的装置，其特征在于，包括：

动态表项生成模块，用于利用监控到的控制连接建立后的协商命令，生成动态规则表项，所述动态规则表项包括动态规则及用于指示五元组中任意一个信息不参与动态规则匹配的标识，其中五元组包括：源 IP 地址、目的 IP 地址、协议号、源端口号、目的端口号；

动态表项添加模块，用于将所述动态规则表项添加到流表中；

查表模块，用于有报文到达后，查找所述流表，将到达的所述报文与所述流表的表项进行匹配；

处理模块，用于根据匹配结果对所述报文进行相应地处理。

7. 根据权利要求 6 所述的监控会话流的装置，其特征在于，所述处理模块具体用于若所述报文与所述动态规则表项匹配成功，则正常转发所述报文。

8. 根据权利要求 7 所述的监控会话流的装置，其特征在于，还包括：

流表项建立模块，用于所述报文与所述动态规则表项匹配成功后，所述处理模块正常转发所述报文之前，根据所述报文在所述流表中创建新的流表项。

9. 根据权利要求 6 所述的监控会话流的装置，其特征在于，所述处理模块具体用于若所述报文既与所述动态规则表项匹配成功，又与所述流表中的流表项匹配成功，则按照最长匹配结果优先原则，正常转发所述报文。

10. 根据权利要求 6-9 任一项所述的监控会话流的装置，其特征在于，所述动态表项生成模块建立的动态规则表项中，所述标识为掩码。

11. 根据权利要求 6-9 任一项所述的监控会话流的装置，其特征在于，所述监控会话流的装置为网络安全设备。

监控会话流的方法及装置

技术领域

[0001] 本发明涉及会话流监控技术，尤其涉及一种监控会话流的方法及装置。

背景技术

[0002] 在网络安全设备如防火墙中，普遍采用会话流状态跟踪技术来实现对经过网络安全设备的会话流进行监控管理，达到对特定非可信的会话流进行识别及阻断的目的。

[0003] 会话流即端到端的数据连接及通过端到端的数据连接传输的信息。在传输控制协议(Transmission Control Protocol，TCP)/因特网协议(Internet，Protocol，IP)协议里面，通常使用 5 元组信息：源 IP 地址、目的 IP 地址、协议号、TCP/ 用户数据报协议(User Data Protocol，UDP)源端口号、TCP/UDP 目的端口号来识别一个会话流。

[0004] 网络安全设备内通常使用一张会话流状态跟踪表(以下简称流表)来管理众多的会话流，并存储有该会话流的处理策略如阻断、通过或者其他附加处理操作。

[0005] 在上述会话流状态跟踪技术框架下，一个会话流的处理过程如图 1 所示。该会话流的首个报文到达时，建立一个新的会话流表项，添加到流表中；对该会话流进行安全策略匹配、审核，并将处理策略结果更新到新建立的会话流表项中。当该会话流的后续报文即非首个报文到达时，由于流表已经存有该会话流的信息，因此直接查找流表；按照对应会话流表项即新建立的会话流表项中的处理策略对该会话流进行处理。

[0006] 然而，某些特殊协议存在两个或多个相互关联的会话流，通常其中一个会话流为主控制连接会话流，其它会话流为该主控制连接所生成的附属连接会话流，建立过程如下：首先是客户端向服务器发起控制连接请求，以与服务器建立连接。连接建立后，客户端与服务器协商出附属连接的端口号，并发起建立相应的附属连接的操作。

[0007] 以文件传输协议(File Transfer Protocol，FTP)协议中的主动模式为例，一个完整的 FTP 传输需要建立两个 TCP 连接：控制连接、数据连接。控制连接为初始主连接，数据连接为协商生成的附属连接。假设服务器端 IP 地址为 10.0.0.1，监听 FTP 控制连接 TCP 端口号为 21 的端口，设客户端 IP 地址为 10.1.0.2。建立 FTP 传输时，客户端使用内部随机分配的端口(假设端口号为 12345)，向服务器端口号为 21 的端口发起控制连接请求。经过 TCP 三次握手，建立起该控制连接，即 TCP 连接：10.1.0.2:12345<->10.0.0.1:21。然后，

[0008] 客户端通过协商命令，向服务器端发起数据传输请求命令，内容包含：客户端 IP 地址及客户端的端口号(假设为 12346)。服务器端收到数据传输请求后，以端口号为 20 的端口为源端口，主动发起向客户端端口 12346(即端口号为 12346 的端口)的 TCP 连接请求，通过三次握手，成功建立起数据连接，即 TCP 连接：10.0.0.1:20<->10.1.0.2:12346。此后，双方通过数据连接传递文件数据内容。

[0009] 假设网络安全设备如图 2 所示，处于客户端与服务器端口之间，需要在二者之间做安全策略检查，服务器端监听的是 FTP 控制连接端口号为 21 的端口，为使上述 FTP 访问能正常进行，通常需要配置安全策略规则，允许指定的客户端用户可以访问上述指定服务器的 TCP 端口号为 21 的端口。但是，上述 FTP 的数据连接即附属连接，其端口号是客户端

与服务器端动态协商确定的，且是从服务器端口主动向客户端发起的连接请求，通常不能符合预设的安全策略，从而导致数据连接不能建立，也就无法完成 FTP 传输。

[0010] 为解决上述问题，通常在上述控制连接建立后，跟踪扫描控制连接的协商命令，抽取协商确定的客户端 / 服务器的 IP 地址端口号信息，动态生成一个安全策略规则，使得后续的数据连接请求能命中该动态安全策略规则，并被允许通过。具体如图 3 所示，网络安全设备构造了一个额外的动态规则表，若新的报文到达，但是未匹配到已存在的会话流，在执行安全策略匹配审核之前，先进行动态规则的匹配。若动态规则匹配成功，则略过安全策略匹配审核，直接设置安全策略匹配审核通过。

[0011] 如生成的动态规则为 :RULE :协议号 =TCP，源 IP=10.0.0.1，源端口 = 任意，目的 IP=10.1.0.2，目的端口 =12346 ;则当服务器端使用端口号为 20 的端口向客户端端口号为 12346 的端口主动发起数据连接时，显然会命中上述动态规则，从而直接通过安全采路匹配审核，不再进行普通安全策略的匹配审核，使得 FTP 数据传输得以正常进行。

[0012] 现有技术存在的缺陷在于 :建立会话流过程中增加了一个动态规则匹配的操作。当大量用户同时使用 FTP 或其他需要特殊处理的协议时，会生成数量巨大的动态规则，严重影响系统性能。

发明内容

[0013] 本发明提出一种监控会话流的方法及装置，以减少查表操作，提升网络安全设备的处理性能。

[0014] 本发明提供了一种监控会话流的方法，包括 :

[0015] 利用监控到的控制连接建立后的协商命令，生成动态规则表项，所述动态规则表项包括动态规则及用于指示五元组中任意一个信息不参与动态规则匹配的标识，其中五元组包括 :源 IP 地址、目的 IP 地址、协议号、源端口号、目的端口号 ;

[0016] 将所述动态规则表项添加到流表中 ;

[0017] 有报文到达后，查找所述流表，将到达的所述报文与所述流表的表项进行匹配 ;

[0018] 根据匹配结果对所述报文进行相应地处理。

[0019] 本发明还提供了一种监控会话流的装置，包括 :

[0020] 动态表项生成模块，用于利用监控到的控制连接建立后的协商命令，生成动态规则表项，所述动态规则表项包括动态规则及用于指示五元组中任意一个信息不参与动态规则匹配的标识，其中五元组包括 :源 IP 地址、目的 IP 地址、协议号、源端口号、目的端口号 ;

[0021] 动态表项添加模块，用于将所述动态规则表项添加到流表中 ;

[0022] 查表模块，用于有报文到达后，查找所述流表，将到达的所述报文与所述流表的表项进行匹配 ;

[0023] 处理模块，用于根据匹配结果对所述报文进行相应地处理。

[0024] 本发明提供的监控会话流的方法及装置通过将特殊协议的动态规则与流表共用存储数据结构即动态规则表与流表合并在一起，避免了单独为动态规则构建一张表，并将动态规则匹配过程合并到流表项查找过程，使得建立会话流过程省略了动态规则匹配的单独查表操作，将流表项的匹配所产生的查表操作及动态规则匹配所产生的查表操作合并为一次查表操作，节约了报文匹配时间，提升了网络安全设备的数据处理性能。

附图说明

[0025] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0026] 图 1 为现有技术中的会话流的处理过程示意图；

[0027] 图 2 为网络安全设备的位置示意图；

[0028] 图 3 为现有技术中 FTP 会话流的监控流程图；

[0029] 图 4 为本发明实施例提供的一种监控会话流的方法的流程图；

[0030] 图 5 为本发明实施例提供的另一种监控会话流的方法流程图；

[0031] 图 6 为本发明实施例提供的监控会话流的装置的结构示意图。

具体实施方式

[0032] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0033] 图 4 为本发明实施例提供的一种监控会话流的方法的流程图。如图 4 所示，包括：

[0034] 步骤 41、利用监控到的控制连接建立后的协商命令，生成动态规则表项，所述动态规则表项包括动态规则及用于指示五元组中任意一个信息不参与动态规则匹配的标识。

[0035] 如生成动态规则：RULE：协议号 =TCP，源 IP=10.0.0.1，源端口 = 任意，目的 IP=10.1.0.2，目的端口 =12346；

[0036] 则建立的动态规则表项包含上述动态规则，此外还包含一个用于指示源端口不参与动态规则匹配的标识。此标识的实现方式可以是掩码方式，也可以采取其他方式。若采用掩码方式实现，则建立的动态规则表项如下：

[0037] KEY：协议号 =TCP，源 IP=10.0.0.1，源端口 = 任意，目的 IP=10.1.0.2，目的端口 =12346

[0038] MASK：协议号 =0xFF，源 IP=0xFFFFFFFF，源端口 =0x0000，目的 IP=0xFFFFFFFF，目的端口 =0xFFFF

[0039] MASK 的位图中，为 1 表示参与匹配，为 0 表示不参与匹配。从上述“MASK”内容可知：源端口不参与动态规则匹配。

[0040] 建立的动态规则表项中，标识可以用来指示五元组中的任何一个信息不参与匹配。如对于 FTP 连接的被动模式，目的端口不参与动态规则匹配，则建立的动态规则表项中可包含一个用于指示目的端口不参与动态规则匹配的标识；再如视频连接中，一个客户端需要同多个视频服务器建立连接，这样目的 IP 不参与动态规则匹配，则建立的动态规则表项中包含一个用于指示目的 IP 不参与动态规则匹配的标识。标识同样可采用上述掩码的方式实现。

[0041] 步骤 42、将所述动态规则表项添加到流表中；

[0042] 步骤 43、有报文到达后，查找所述流表，将到达的所述报文与所述流表的表项进行匹配；

[0043] 步骤 44、根据匹配结果对所述报文进行相应地处理。

[0044] 上述步骤 41- 步骤 44 均可由网络安全设备执行。

[0045] 步骤 44 中，具体地，若所述报文与所述动态规则表项匹配成功，则所述报文可能为与所述控制连接相关的会话流的第一个报文即建立所述控制连接的附属连接的数据连接请求，正常转发所述第一个报文。

[0046] 所述报文也可能为数据连接建立后传输的报文。所述报文与所述动态规则表项匹配成功后，正常转发所述报文之前还可包括：

[0047] 根据所述报文在所述流表中创建新的流表项。

[0048] 对后续到达的报文再次查找所述流表，按照最长匹配结果优先原则将所述后续到达的报文与所述流表中的表项进行匹配。由于流表中还有动态规则表项，因此，匹配时采用最长匹配结果优先原则，即当一个报文同时匹配到一个动态规则表项和一个流表项时，优先选择流表项的匹配结果。由于流表项的匹配关键字由五元组构成，包括源 IP、目的 IP、协议号、源端口、目的端口，且执行的是精确的关键字匹配，而动态规则表项的关键字虽然与流表项的关键字相同，但是，动态规则匹配执行的是模糊匹配，即上述五个关键字某些关键字允许是任意值，只要剩余关键字匹配成功，则认为动态规则匹配成功，因此，流表项的匹配结果长度大于动态规则表项的匹配结果。通过新建立的流表项，可以对一个控制连接的多个数据连接上的会话流分别进行监控。

[0049] 当到达网络安全设备的报文为数据连接建立后在建立的数据连接上传输的报文时，步骤 44 可包括：若所述报文既与所述动态规则表项匹配成功，又与所述流表中的流表项匹配成功，则按照最长匹配结果优先原则，正常转发所述报文。

[0050] 本实施例，在基于会话流状态跟踪技术的网络安全设备中，通过将特殊协议的动态规则与流表共用存储数据结构即动态规则表与流表合并在一起，避免了单独为动态规则构建一张表，并将动态规则匹配过程合并到流表项查找过程，使得建立会话流过程省略了动态规则匹配的单独查表操作，将流表项的匹配所产生的查表操作及动态规则匹配所产生的查表操作合并为一次查表操作，节约了报文匹配时间，提升了网络安全设备的数据处理性能。

[0051] 图 5 为本发明实施例提供的另一种监控会话流的方法流程图。本实施例中对图 2 所示的 FTP 传输的会话流进行监控，如图 5 所示，监控会话流的具体过程如下：

[0052] 步骤 51、查找流表以对传输的报文进行匹配。

[0053] 流表中包含动态规则表项和流表项。其中，动态规则表项在 FTP 控制连接建立后，利用客户端发送的协商命令即向服务器端发起的数据传输请求命令生成，如：

[0054] KEY：协议号 =TCP，源 IP=10.0.0.1，源端口 = 任意，目的 IP=10.1.0.2，目的端口 =12346

[0055] MASK：协议号 =0xFF，源 IP=0xFFFFFFFF，源端口 =0x0000，目的 IP=0xFFFFFFFF，目的端口 =0xFFFF

[0056] 并添加到流表中。

[0057] 服务器端收到协商命令后，服务端端口号为 20 的源端口，主动发起向客户端端口

号为 12346 的端口的 TCP 连接请求，通过三次握手，成功建立起数据连接，即 TCP 连接 ：

[0058] 协议号 =TCP，源 IP=10.0.0.1，源端口 =20，目的 IP=10.1.0.2，目的端口 =12346。

[0059] 此后，服务器端与客户端的数据交换，使用的就是与新建的流表项对应的会话流。

[0060] 其中，TCP 连接请求即新的会话流的第一个报文，网络安全设备如防火墙在接收到服务器端发起的 TCP 连接请求即数据连接请求后，查找流表，进行表项匹配。此时，该第一个报文仅与动态规则表项匹配成功。

[0061] 后续报文到达时，再次进行流表查找，按最长匹配优先原则，与新建的流表项成功匹配，然后报文被正常转发。换句话说，会话流的第一个报文命中动态规则表项后，根据当前报文的精确 5 元组信息，立即构造出一条精确匹配的流表项，此后该会话流的报文都会命中流表项，而走正常的报文转发。

[0062] 步骤 52、判断匹配是否成功。由于流表中包含动态规则表项及流表项，因此，匹配也包括动态规则匹配与流表项匹配两种匹配。相应地，匹配成功包括流表项匹配成功、动态规则匹配成功或流表项及动态规则匹配成功。如果仅流表项匹配成功，说明到达的报文所属的会话流与其他会话流没有关联，执行步骤 54 ；若仅动态规则匹配成功，说明到达的报文所属的会话流在流表中尚未建立流表项，或者动态规则表项的附属连接仅有一条，因为附属连接只有一条的话，可不用建立流表项，执行步骤 55 ；若流表项及动态规则匹配成功，说明到达的报文所属的会话流所使用的数据连接为一个控制连接的附属连接，流表中相应的动态规则表项及流表项均已建立，按图 4 所示实施例中采用的采用最长匹配结果优先原则，判定为流表项匹配成功，则直接设置安全策略匹配审核为通过，略过安全策略匹配审核过程，执行步骤 54。若匹配失败，说明到达的报文为某一会话流的第一个报文，且该会话流与其他会话流不相关，执行步骤 53。

[0063] 步骤 53、利用到达的报文在流表中生成新的流表项，并对该会话流进行安全策略匹配审核。

[0064] 步骤 54、正常转发到达的报文。

[0065] 步骤 55、利用到达的报文在流表中生成新的流表项，并直接设置安全策略匹配审核为通过，略过安全策略匹配审核过程，直接执行步骤 54。

[0066] 可以看出本实施例相对现有技术方案，在建立会话流过程中，减少了单独用于动态规则匹配的一次查表操作，使得网络安全设备的负荷减少，从而提升了网络安全设备的处理性能。

[0067] 本领域普通技术人员可以理解 ：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤 ；而前述的存储介质包括 ：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0068] 图 6 为本发明实施例提供的监控会话流的装置的结构示意图。如图 6 所示，监控会话流的装置可为网络安全设备，具体包括 ：动态表项生成模块 61、动态表项添加模块 62、查表模块 63 及处理模块 64。

[0069] 动态表项生成模块 61 用于利用监控到的控制连接建立后的协商命令，生成动态规则表项，所述动态规则表项包括动态规则及用于指示五元组中任意一个信息不参与动态规则匹配的标识 ；所述标识可为掩码，详见上述方法实施例中的说明。

[0070] 动态表项添加模块 62 用于将所述动态规则表项添加到流表中；查表模块 63 用于有报文到达后，查找所述流表，将到达的所述报文与所述流表的表项进行匹配；处理模块 64 用于根据匹配结果对所述报文进行相应地处理。如所述处理模块具体用于若所述报文与所述动态规则表项匹配成功，则正常转发所述报文；或者如所述处理模块具体用于若所述报文既与所述动态规则表项匹配成功，又与所述流表中的流表项匹配成功，则按照最长匹配结果优先原则，正常转发所述报文。详见上述方法实施例中的说明。

[0071] 本发明实施例提供的监控会话流的装置还可包括：流表项建立模块，用于所述报文与所述动态规则表项匹配成功后，所述处理模块正常转发所述报文之前，根据所述报文在所述流表中创建新的流表项。

[0072] 所述查表模块还用于对后续到达的报文再次查找所述流表，按照最长匹配结果优先原则将所述后续到达的报文与所述流表中的表项进行匹配。

[0073] 本实施例中，监控会话流的装置如在基于会话流状态跟踪技术的网络安全设备中，将特殊协议的动态规则匹配过程合并到流查找过程，使得建立会话流过程省略了单独用于动态规则的匹配操作的查表操作，降低了网络安全设备的负荷，提升了网络安全设备的处理性能。

[0074] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

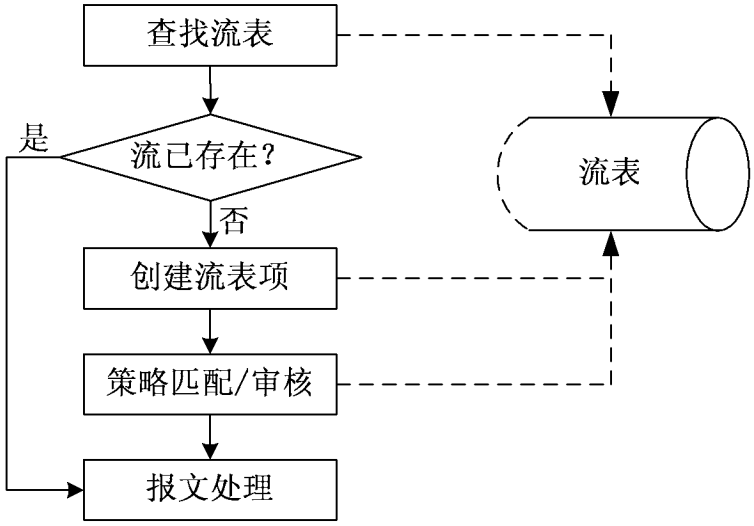


图 1

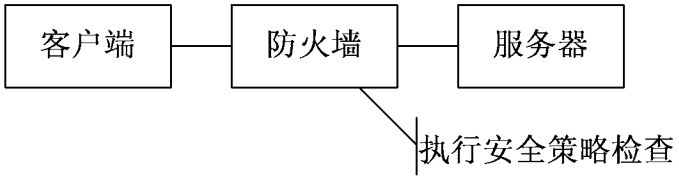


图 2

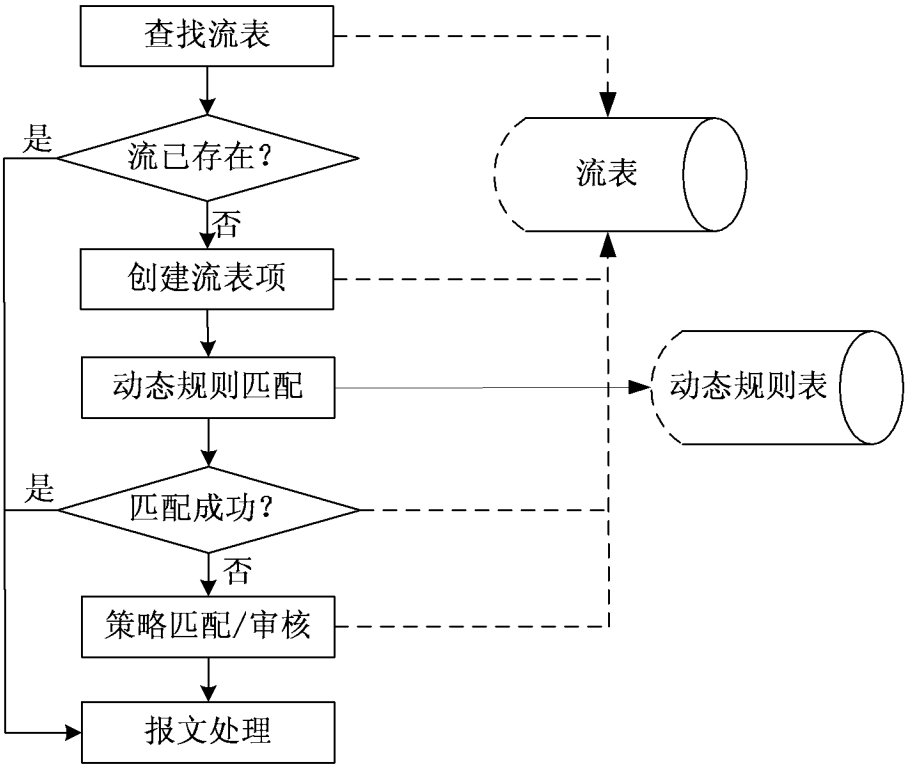

查找流表
流已存在？
是
否
流表
创建流表项
动态规则匹配
动态规则表
匹配成功？
是
否
策略匹配/审核
报文处理

图 3

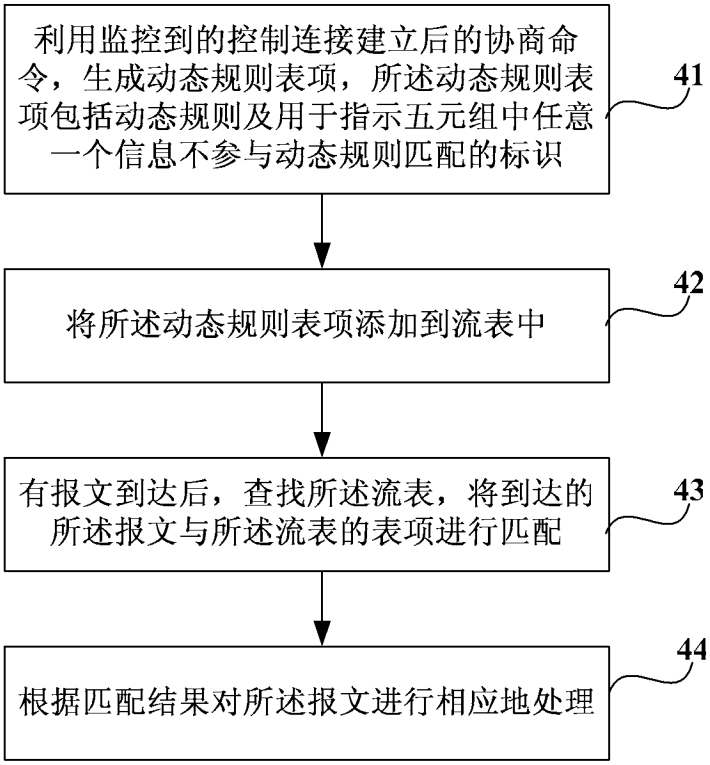

利用监控到的控制连接建立后的协商命令，生成动态规则表项，所述动态规则表项包括动态规则及用于指示五元组中任意一个信息不参与动态规则匹配的标识
41
将所述动态规则表项添加到流表中
42
有报文到达后，查找所述流表，将到达的所述报文与所述流表的表项进行匹配
43
根据匹配结果对所述报文进行相应地处理
44

图 4

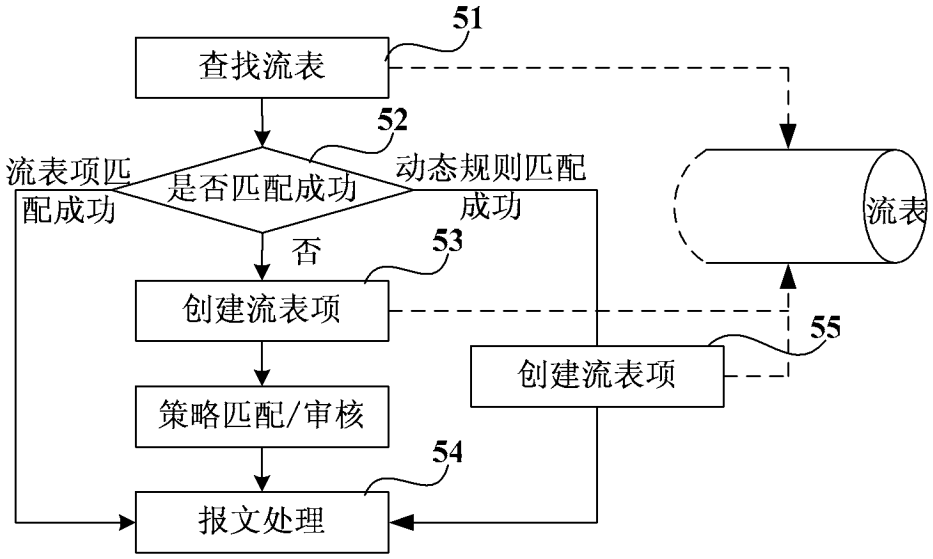

51
查找流表
52
流表项匹配成功
是否匹配成功
动态规则匹配成功
否
53
创建流表项
流表
55
创建流表项
策略匹配/审核
54
报文处理

图 5

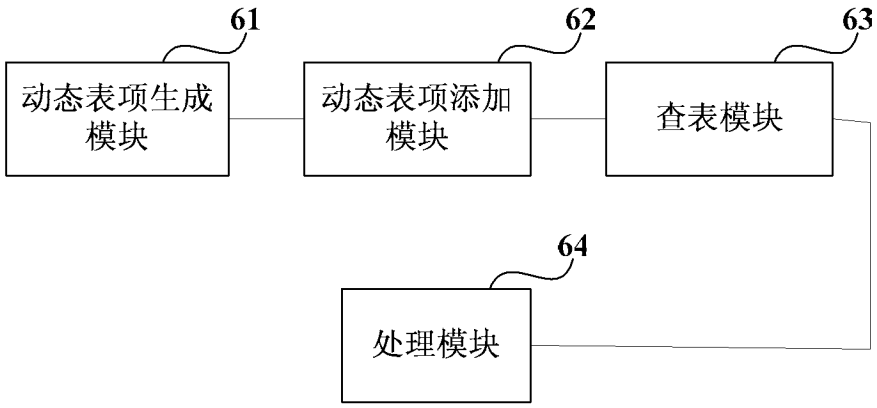

61
动态表项生成模块
62
动态表项添加模块
63
查表模块
64
处理模块

图 6