**基于SDN的电力仿真平台**

**动态防护方案说明**

目录

[1 总体说明 3](#_Toc3463330)

[1.1 系统功能结构框图 3](#_Toc3463331)

[1.2 系统功能组件定义 3](#_Toc3463332)

[2 动态防护流程描述 6](#_Toc3463333)

[2.1 病毒攻击防护流程 6](#_Toc3463334)

[2.2 DDos拒绝服务攻击防护流程 9](#_Toc3463335)

[2.3 攻击检测简要流程 12](#_Toc3463336)

[3 功能实现动态描述 13](#_Toc3463337)

[3.1 网络拓扑管理 13](#_Toc3463338)

[3.2 网络流量监控 14](#_Toc3463339)

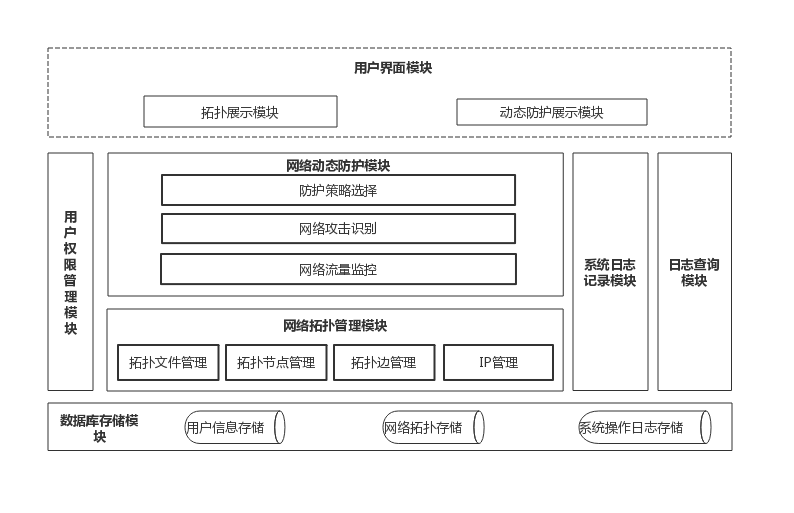
[3.3 网络攻击识别 15](#_Toc3463340)

[3.4 防护策略选择 16](#_Toc3463341)

[3.5 基于攻击的动态防护整体描述 17](#_Toc3463342)

# 总体说明

## 系统功能结构框图

****

基于SDN的动态防护平台由用户界面模块、用户管理模块、网络拓扑管理模块、网络动态防护模块、日志查询模块、系统日志记录模块、数据存储模块组成。

用户登录系统之后，用户管理监控模块（仅管理员可进入）根据当前用户是否具有查看拓扑、开启攻击识别和动态防护、查询日志的权限在分用户界面模块限制用户的相关操作。用户选择不同的网络拓扑文件，网络拓扑管理模块读取拓扑信息后在前端实现网络拓扑的可视化，然后用户可以选择修改网络拓扑结构，例如对于网络节点或者连接的添加和删除；网络动态防护模块内可以设置是否开启网络攻击识别和动态防护，开启动态防护之后平台在后台执行入侵检测算法，根据检测到的网络入侵选择适当防护策略进行动态防护，并且能够在前端实时展示防护过程中的信息流动或者网络分区变化；日志查询模块选择查询时间区间，读取系统操作日志并将查询结果在前端展示；系统日志记录模块就是记录当前用户的操作，例如登陆、修改拓扑、开启网络动态防护、注销等；数据存储模块完成平台相关信息的数据库存取。

## 系统功能组件定义

**（1）网络拓扑管理模块**

定义：该模块主要负责网络拓扑的构建、选择、修改和标记拓扑节点的功能标记，实现网络拓扑结构的搭建以及可视化展示。

功能：用户选择不同的网络拓扑文件时，模块能够在拓扑展示界面进行不同拓扑的切换，并且可以在已有的网络拓扑基础上完成增加、删除拓扑节点或者连接（边）。并且能够在拓扑展示界面标记不同的功能节点，例如web服务器节点等。

**（2）网络动态防护模块**

定义：该模块主要负责网络拓扑中攻击的识别以及动态防护，并且实时展示防护过程。

功能：该模块中用户可以选择开启或者关闭入侵检测和网络动态防护以了解动态防护对于网络拓扑系统的保护效果，可以完成对网络拓扑中网络攻击的识别也就是系统入侵检测以及针对于入侵选择合适的防护策略以完成动态防护，并且实时展示防护过程中的信息流向或者网络分区变化。

设计理念：模块基于mininet完成网络拓扑的动态展示，后端连接ONOS控制器，在ONOS网络流表基础上设计入侵检测算法完成对网络攻击的识别，根据网络攻击类型适当防护策略，初步防护策略包括多分区网络隔离和网络动态配置等，再利用mininet和ONOS相关组件API完成前端的动态可视化展示。

**（3）日志查询模块**

定义：该模块查询时间区间内系统的操作日志记录，以列表的形式进行展示。

功能：时间区间的选择在用户界面确定，通过查看系统日志，显示具体用户的操作等。

**（4）系统日志记录模块**

定义：该模块用于记录用户的各种操作及发生时间，例如登入、登出、修改拓扑、查询流表等。

功能：本模块为日志查询模块服务，提供系统运行状态的记录以备查。

设计理念：根据Spring AOP面向切面编程的思想来编写操作日志记录模块，定义控制层为切面，用户提交请求给控制层执行相关操作时，自动触发完成操作日志的记录。

**（5）用户管理监控模块**

定义：该模块仅限管理员进入，管理员可进行用户的增加、删除，修改用户的密码及权限，限制用户是否具有查看拓扑、修改拓扑、查看日志等功能。

功能：通过权限管理，能够限制用户的操作范围，避免用户的一些过失操作对平台造成的破坏。

设计理念：通过过滤器Servlet Filter来实现请求资源或者从资源返回信息的过滤操作，通过读取session的attribute属性来判断当前用户是否登陆、身份（是否为管理员）以及是否具备相应操作的权限，完成页面的跳转。

**（6）数据存储模块**

定义：以数据库的形式存储平台的关键数据，包括用户信息、网络拓扑、系统操作日志、网络数据流信息等。

功能：作为底层模块，为日志查询模块、网络动态防护模块等模块提供数据查询服务。

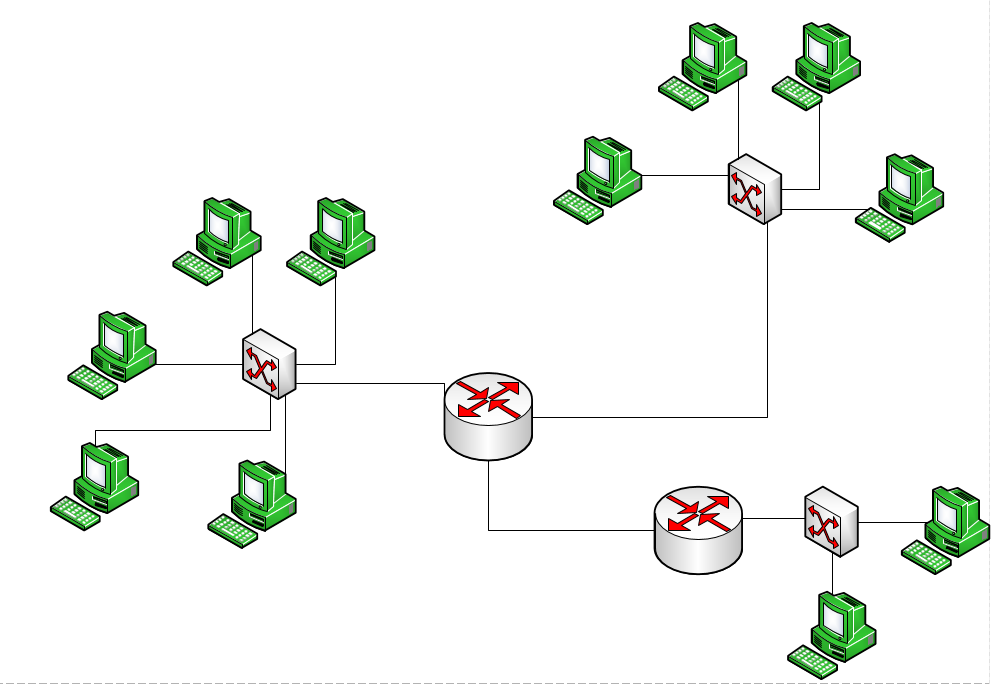
设计理念：通过对象关系映射框架hibernate对JDBC进行轻量级的对象封装，将POJO与数据库表建立映射关系，hibernate是一个全自动的orm框架，可以自动生成SQL语句并自动执行，使用对象编程思维来操纵数据库。

# 动态防护流程描述

## 病毒攻击防护流程

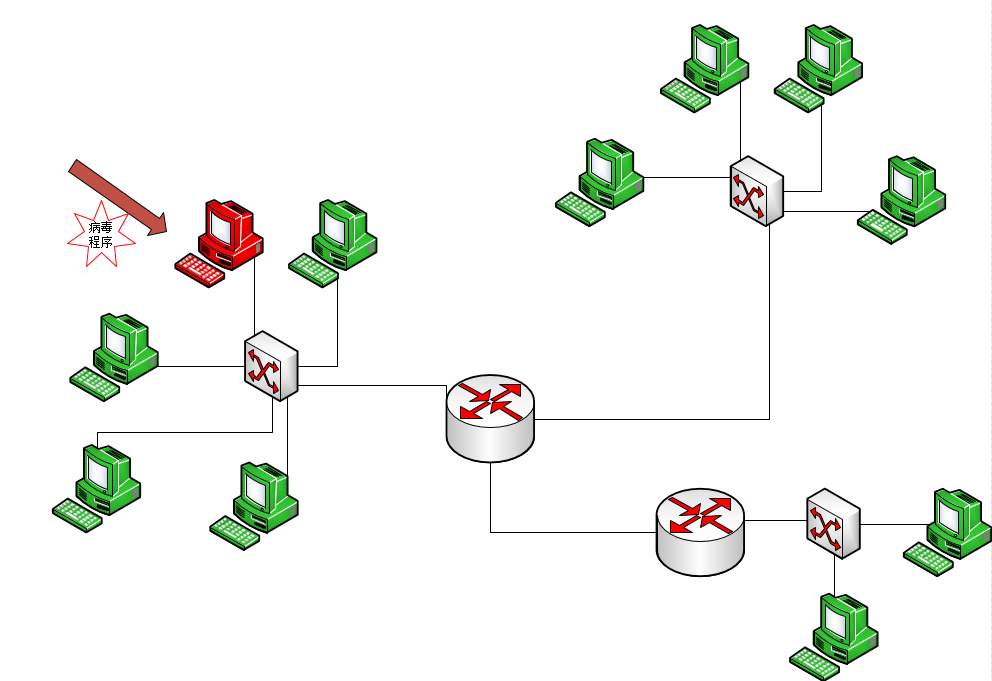
（1）**安全环境下的网络拓扑：**

（PC为绿色代表处于可信环境中，未受攻击）



（2）**某台计算机受到外部网络中的病毒程序攻击：**

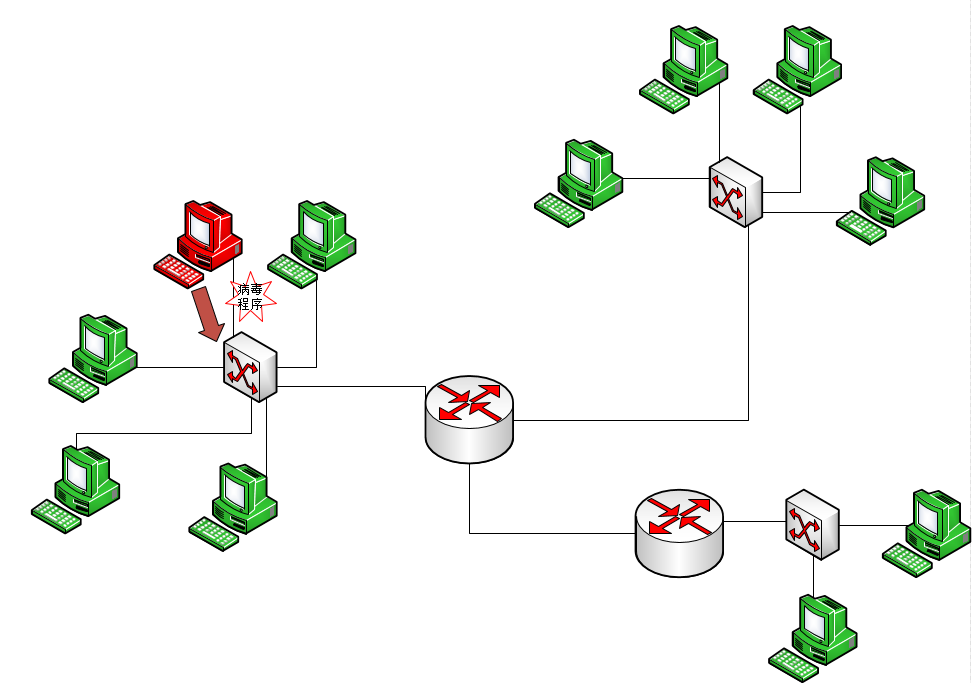
（PC为红色代表受到病毒程序攻击）



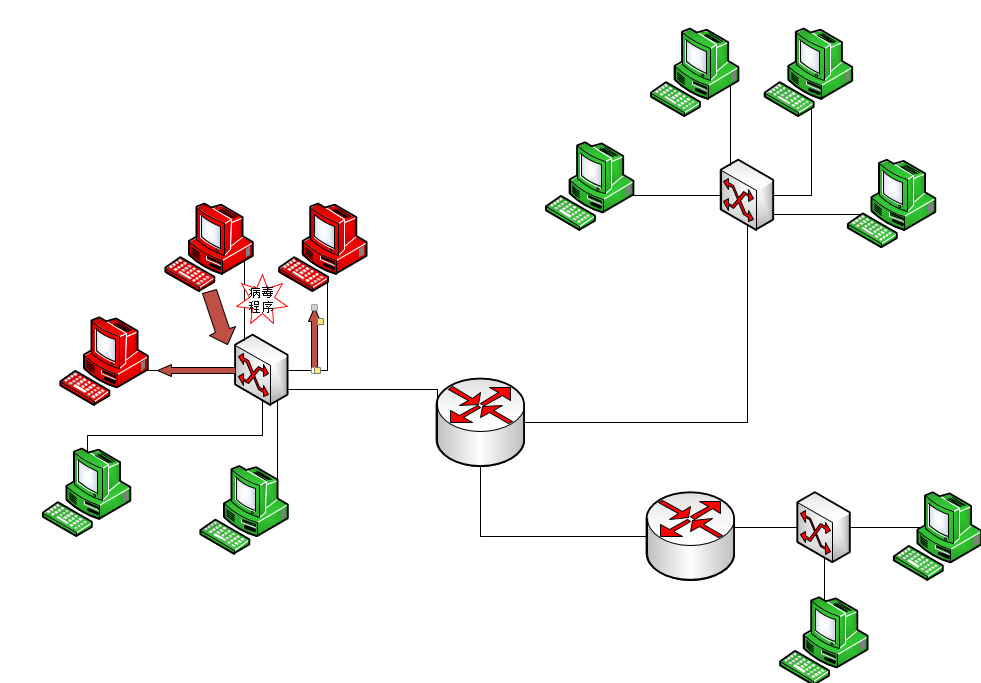
**（3）病毒程序通过局域网或者互联网中的网络设备传播到其他网络环境中：**

受到病毒攻击的主机向外传播病毒，通过网络设备使得更多的主机受到病毒攻击，导致网络中主机大范围出现被病毒程序攻击的情况。

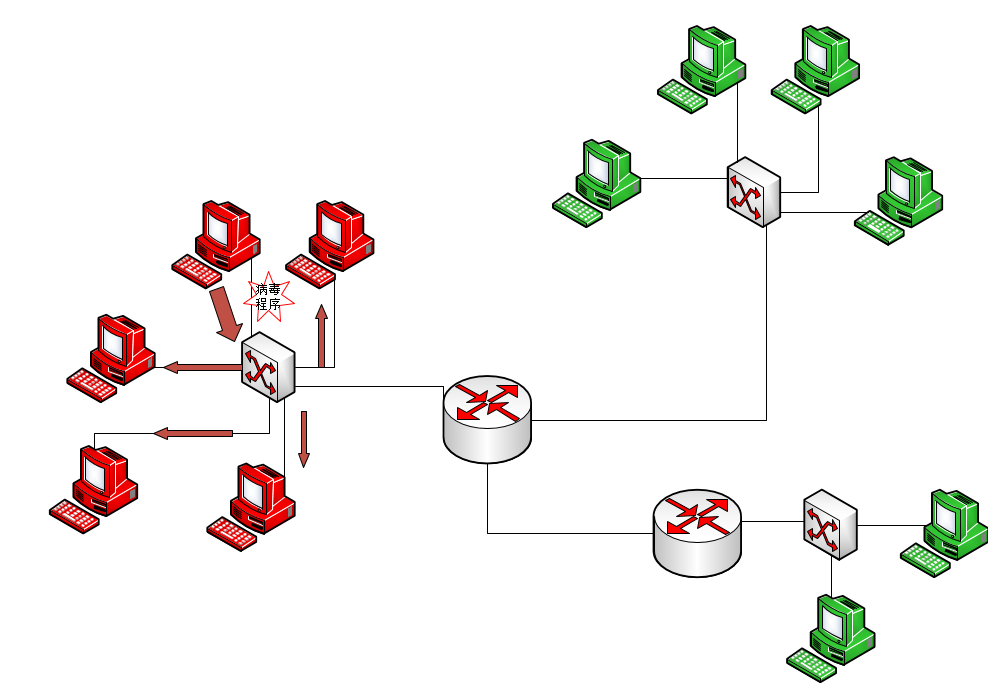
①



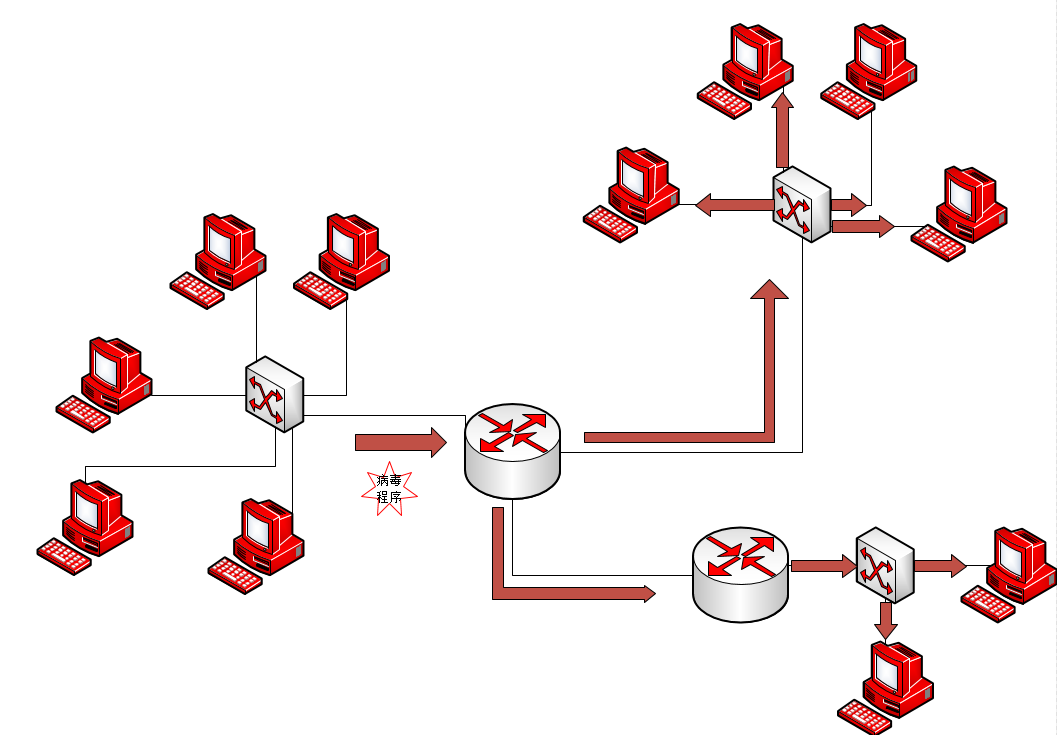
②



③



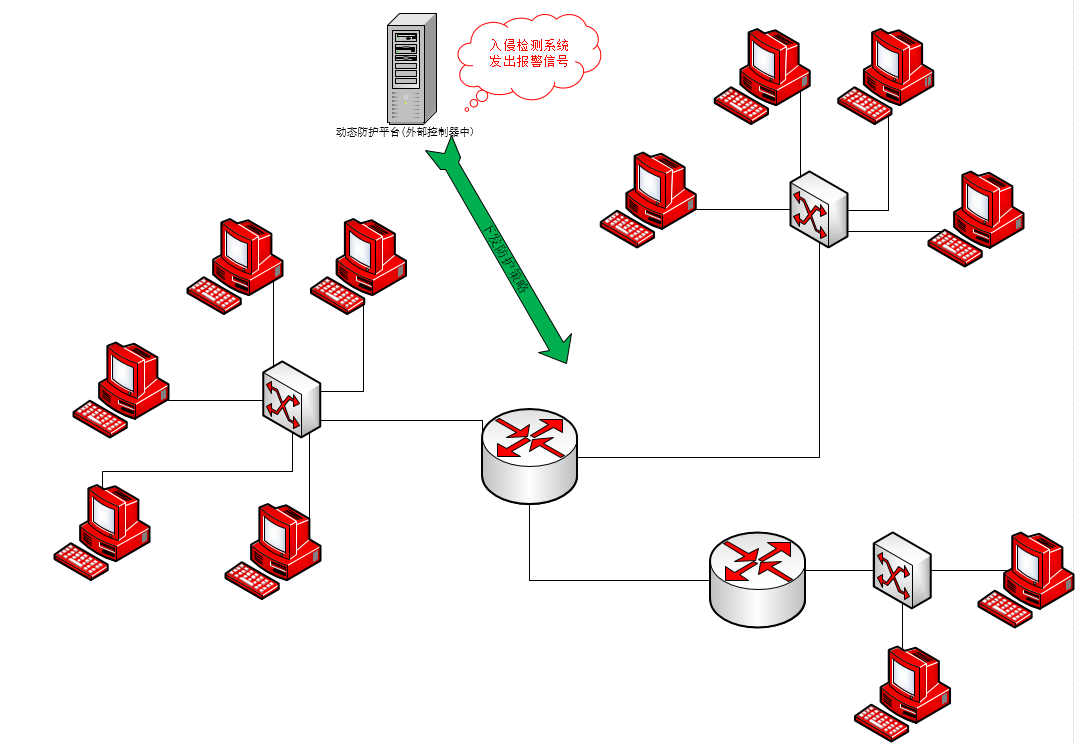
④



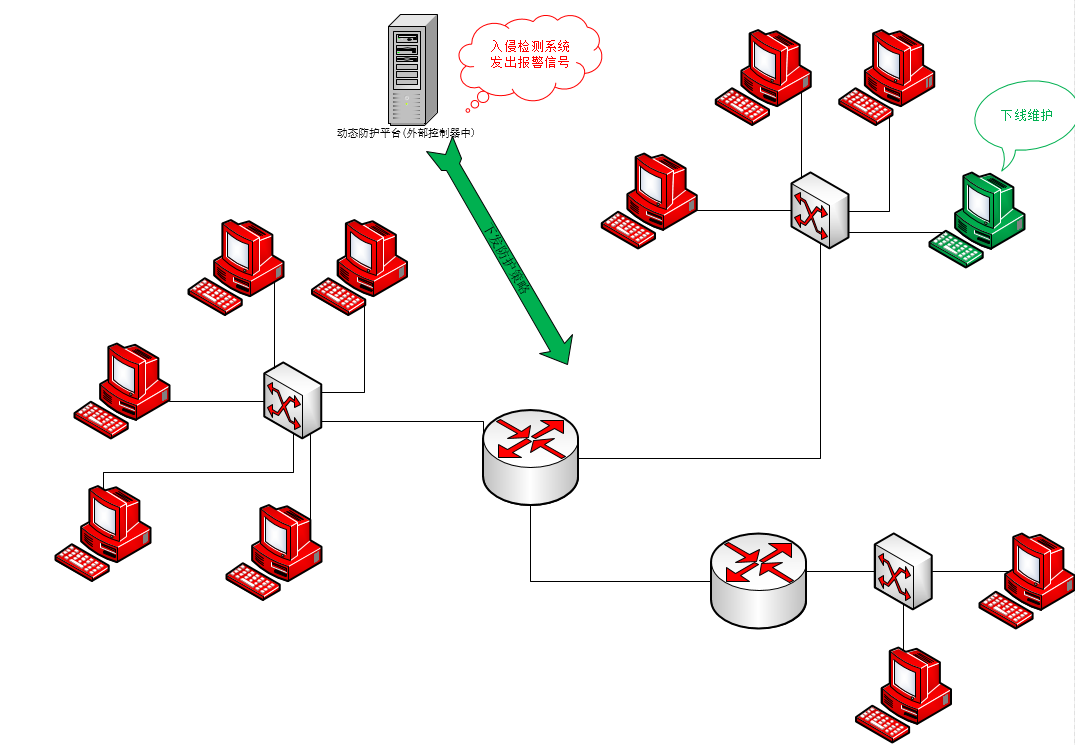
**（4）防护平台执行入侵检测后发出报警信号并向网络下发防护策略进行动态防护**：

位于网络外部控制器上的防护平台在执行攻击检测算法过程中发现受攻击主机节点，发出警报并报告受攻击节点，随后下发防护策略，如主机下线维护清除病毒程序。待主机维护完成之后，重新上线。所有主机维护完成后，防护平台警报清除。

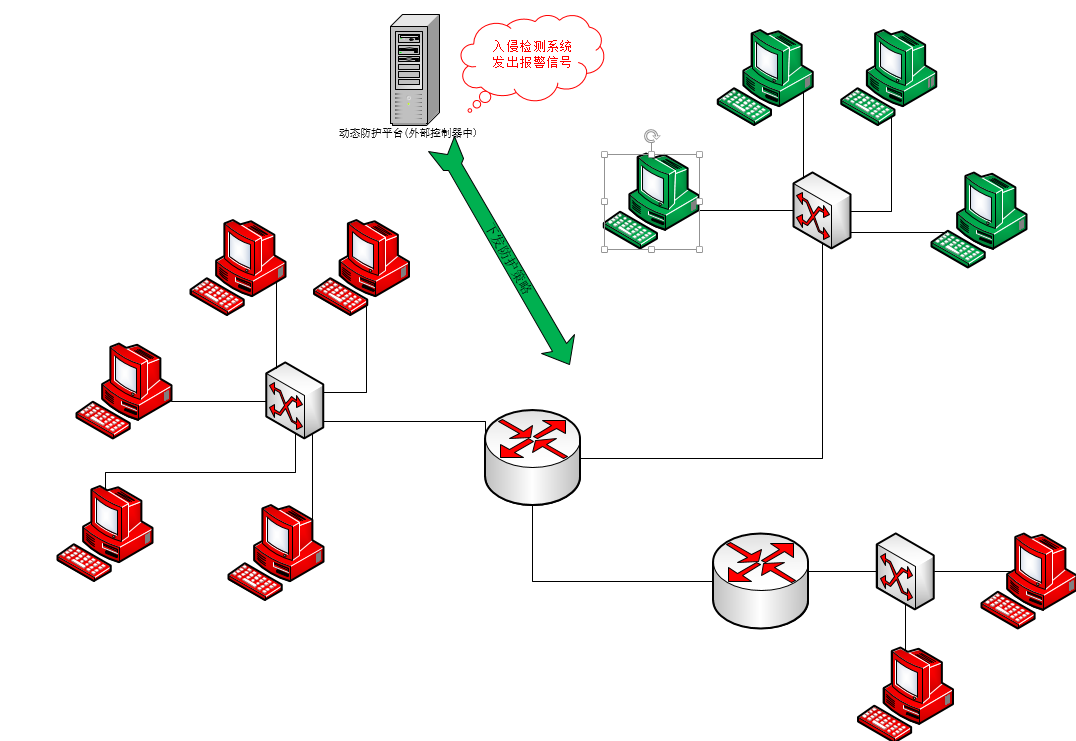
①



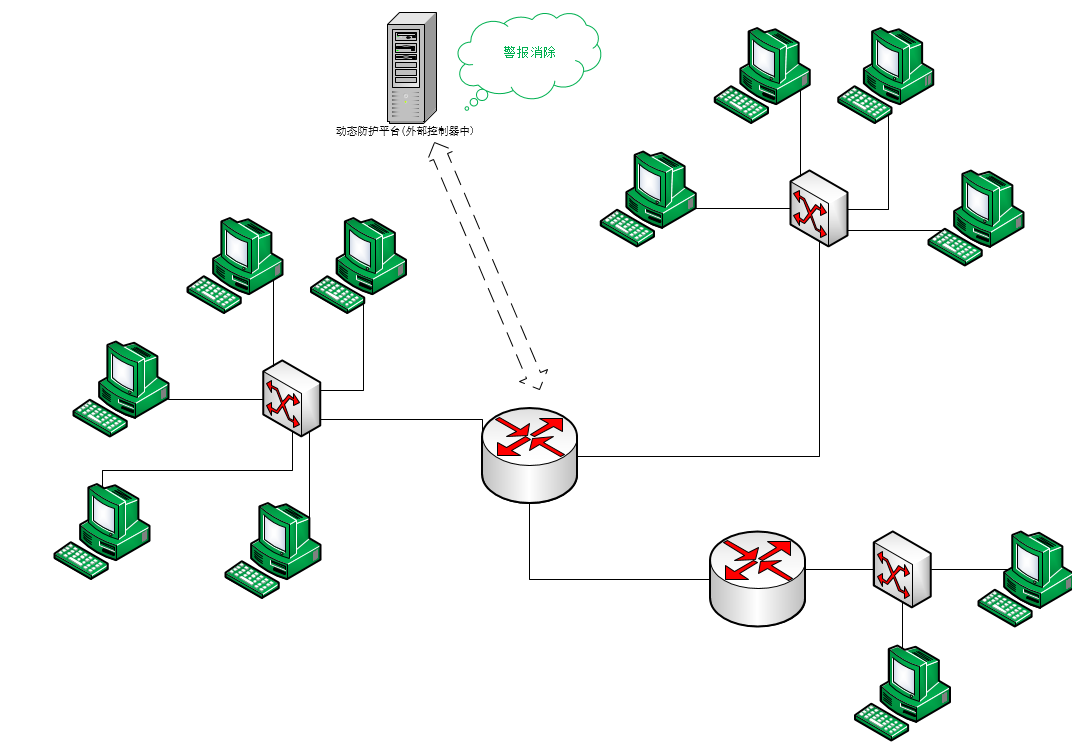
②



③



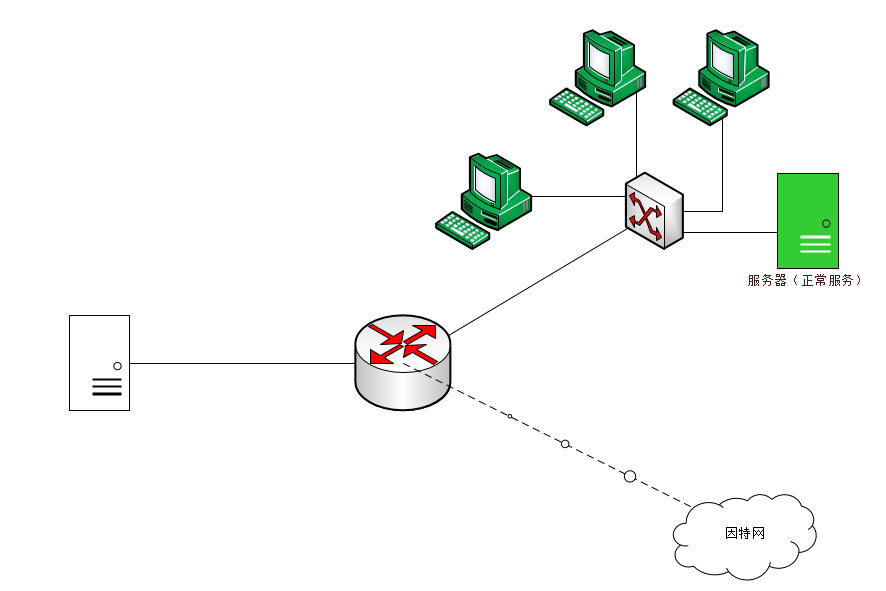
④



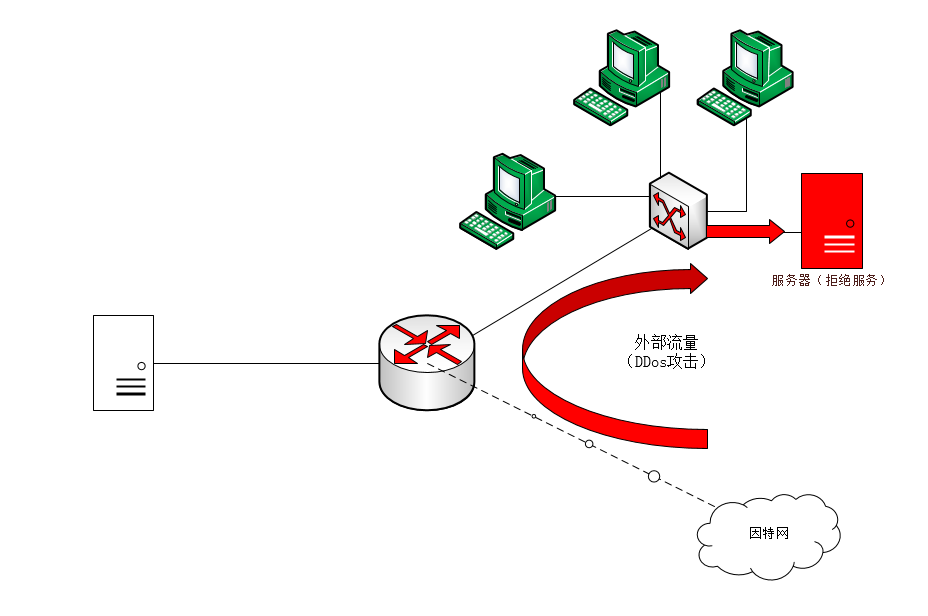
## DDos拒绝服务攻击防护流程

**（1）网络中服务器提供某服务处于正常状态中：**

局域网或者通过路由器连接至因特网中的主机可以通过网络连接访问该服务器上的服务。

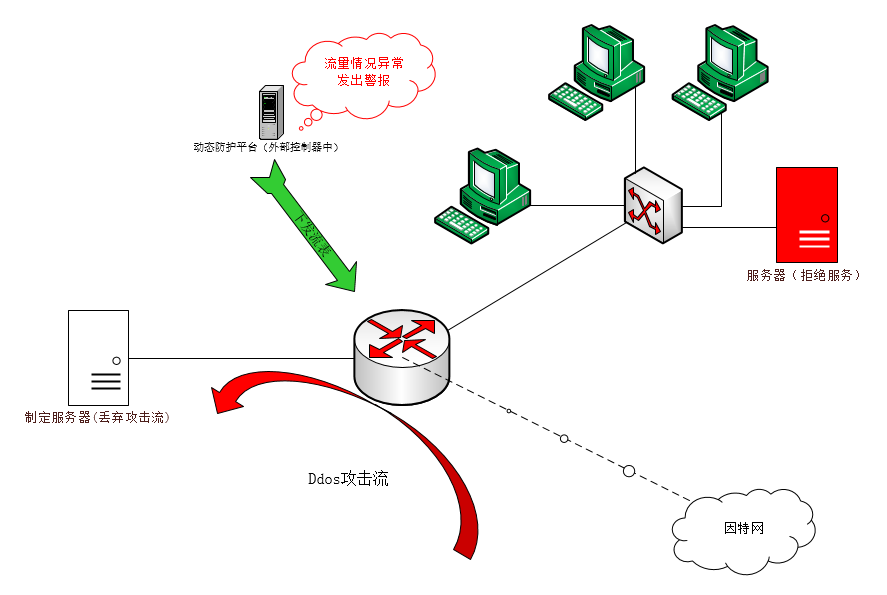


**（2）服务器受到因特网中DDos攻击导致服务资源被占用，拒绝服务：**

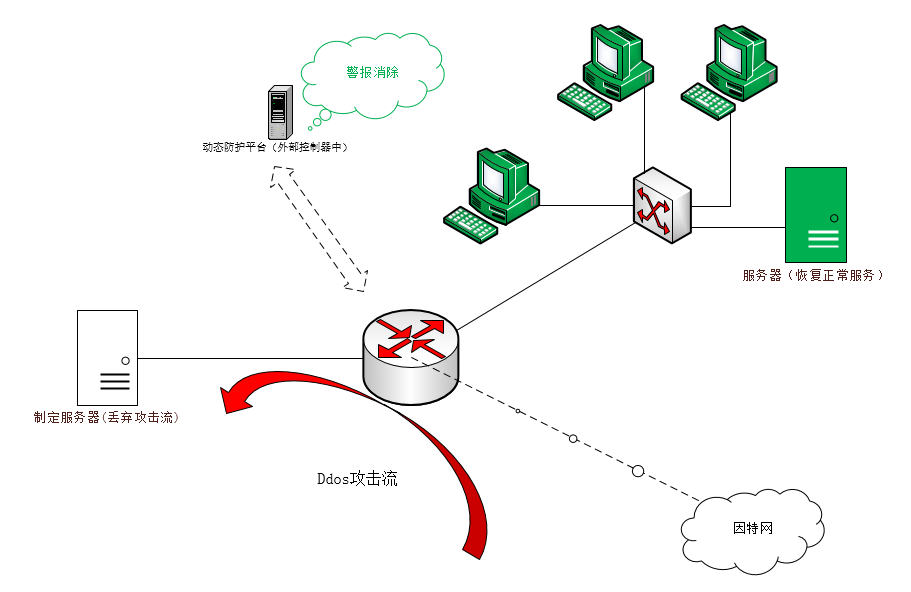


**（3）动态防护平台通过流量检测发现服务器流量异常，发出警报：**

防护平台经过流量统计监控发现该服务器流量异常，发出警报并报告攻击节点。然后通过下发流表等方式将来自外部网络的DDos攻击流导向网络中特定服务器处理，使得服务能够正常进行。



**（4）服务器恢复正常服务之后，防护平台警报消除：**



**服务器流量随时间变化图：**

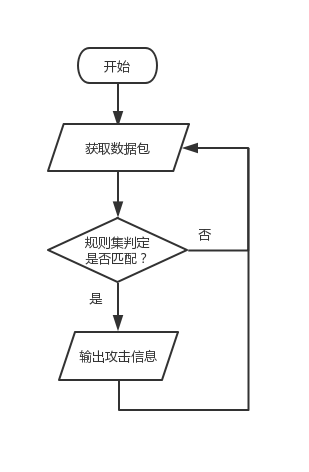
时间

Ddos攻击

开始

我们可以从此示意图中看到服务器流量在受到DDos攻击时呈一个突然上升趋势，当防护平台检测到受到攻击后下发流表将攻击流导向至特定服务器节点后受攻击服务器流量开始下降最后趋于稳定。

## 攻击检测简要流程

****

对于病毒攻击检测的初步构思为基于数据包检测的实时分析：运行一个监听进程，获取发送至主机的所有数据包。我们实现根据攻击定义一个规则集，包含一些预定义的规则，例如在一个连续时间内，收到一定频率以上的SYN或者FIN请求（TCP），我们就可以认为检测到了SYN/FIN扫描攻击，对于其他攻击也类似。通过一个匹配算法，将收到的数据包与规则集中的规则进行匹配，进而确定属于哪种攻击类型，然后输出攻击信息。

# 功能实现动态描述

## 网络拓扑管理



功能描述：用户在下拉框中选择不同拓扑文件，对应的网络拓扑展示区域实现网络拓扑图的实时切换；用户可以对网络拓扑图进行修改，包括添加、删除拓扑节点或者边，以及修改网络元素的属性。

流程描述：chooseTopology()提交用户所查看的拓扑文件名称，拓扑展示模块实现拓扑可视化的展示。addNetworkElement()添加网络拓扑元素，传递参数包括元素类型——节点和边。deleteNetworkElemet()删除网络拓扑元素，传递一个要删除的拓扑元素对象。modifyNetworkElement()修改网络拓扑元素属性，传递参数包括拓扑元素对象、要修改的属性以及属性的值。

## 网络流量监控



功能描述：用户开启网络动态防护功能之后，攻击识别子模块获取网络流量时控制网络流量监控子模块开始网络流量监控。

流程描述：是用户选择开启动态防护后攻击识别子模块通过getNetworkTraffic()来获取网络流量信息，此时网络流量监控子模块自调用trafficMonitor()统计流量信息。

## 网络攻击识别



功能描述：防护策略选择子模块在选择防护策略时需要调用攻击识别子模块以获取网络所受攻击的信息。由网络流量监控子模块统计得到的流量信息传递给攻击识别子模块，攻击识别子模块自调用模块内的入侵检测函数对流量信息进行检测以识别网络中的攻击并得到攻击信息包括受攻击节点以及攻击类别。

流程描述：防护策略选择子模块调用getAttackInfo()获取攻击信息时，调用攻击识别子模块通过detectIntrusion()检测网络攻击得到攻击信息包括受攻击节点以及攻击类别，。

## 防护策略选择



功能描述：网络系统中有网络攻击发生时，攻击识别子模块得到攻击信息（受攻击节点以及攻击类别）后，将这些信息发送给防护策略选择子模块，该模块针对具体攻击类别选择合适的防护策略并由攻击防护展示模块在网络拓扑中执行此防护策略

流程描述： 防护策略选择子模块getProtectionStrategy()获取防护策略时，调用防护策略中的selectProtectionStrategy()方法根据具体攻击的信息选择（包括入侵的类型、攻击节点）选择合适防护策略。进而由攻击防护展示模块调用runSafeProtection()执行安全防护并在网络拓扑图中展示具体防护过程以直观呈现。

## 基于攻击的动态防护整体描述



整体顺序图就是将以上各场景合并描述整个动态防护过程的场景是如何在各模块间依次执行的，过程介绍可参考3.2至3.4描述。