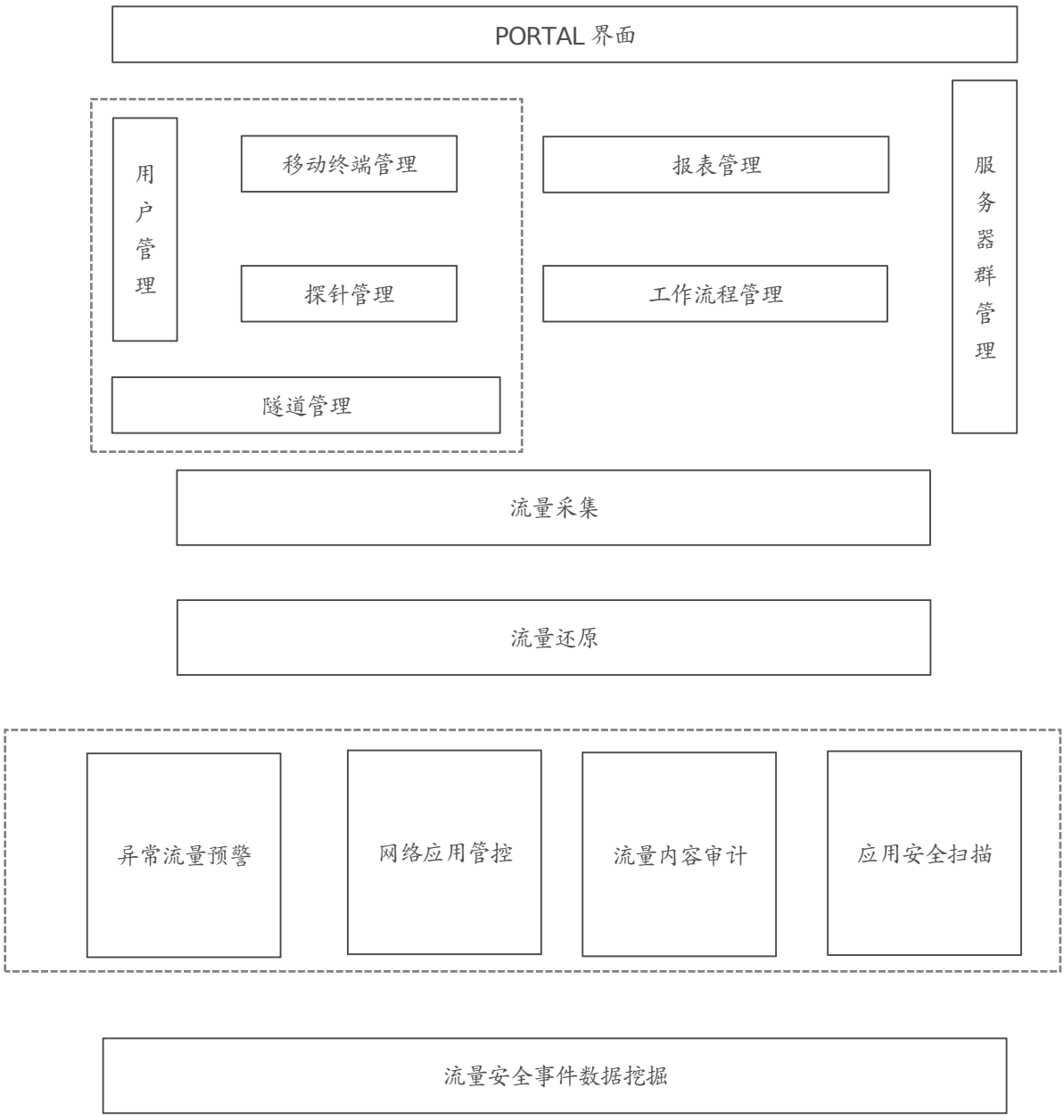
CFS 总体方案

目 录

1. CFSP 架构


PORTAL 界面
用户管理
移动终端管理
报表管理
服务器群管理
探针管理
工作流程管理
隧道管理
流量采集
流量还原
异常流量预警
网络应用管控
流量内容审计
应用安全扫描
流量安全事件数据挖掘

2. CFS 平台功能

1. 对用户提供 PORTAL 界面，包括：
   a) 最终用户的管理界面，包括平台试用界面，注册、登录和退出登录等的账号管理相关界面，用户自服务配置界面，检索查询界面，数据挖掘、报表相关界面。
   b) 平台管理员的管理界面
2. 用户管理相关功能，包括：
   a) 用户管理，包括用户注册、用户列表检索、用户信息管理、用户受平台管理的网络资产管理。
   b) 探针管理，管理每一个用户处部署的网络探针设备，包括探针配置，探针运行状态管理、探针故障告警。
   c) 移动终端管理，管理每一个用户处登记接受管理的移动终端，包括移动终端的信息管理、配置管理（通过 CFS 平台自定义的 CFS 管理协议接口）、运行状态管理、移动终端故障告警。
   d) 隧道管理，按照用户服务协议，管理平台和用户侧探针（CFS-Probe）和移动终端代理软件（CFS-MAgent）与平台侧之间的隧道，包括隧道的建立、拆除、状态监测。也包括，在服务器群管理模块的指令下，依据服务器负载均衡的算法，动态调整隧道的配置，包括但不限于：调整隧道的带宽参数、调整流量镜像策略以增加或减少镜像的流量、更换隧道平台侧的服务器节点以实现流量负载均衡。
3. 服务器群管理
   a) 管理维护平台服务器的列表，增加、拆除服务器，调整服务器的参数，以及相应的工作负载迁移。
   b) 监控服务器的运行状态，包括故障告警、负载情况等。
   c) 服务器群负载分担，针对服务器群中不同类型的服务器，采集不同的负载参数，根据负载均衡算法动态调整服务器的负载。包括对隧道管理模块下发指令，调整用户侧通过隧道上报信息对服务器群的压力冲击。

4. 报表管理

a) 平台管理员所需报表的管理，包括注册用户信息、状态的报表，平台、探针和移动终端软件运行状态报表，用户整体安全事件的汇总报表及数据挖掘报表的定制、生成和分发。

b) 用户所需报表的管理，包括用户自己的网络资产报表、用户流量分析报表、用户流量控制记录、用户流量内容信息安全报表、用户网络应用安全扫描报表以及以上历史记录信息的数据挖掘结果报表的定制、生成和分发。

5. 工作流程管理

是平台上所有业务工作流程的集中管理模块。读取来自用户配置的对流量的管理策略，根据服务器群管理模块采集到的服务器群运行状态，将用户流量的安全管控工作自动分配到服务器群的各类服务器上，以流水线的方式完成用户镜像的网络流量的各个处理环节。将最终的处理结果导向到数据库表予以记录，并提供给后续的数据挖掘和报表处理。

6. 流量采集

专用的服务器集群接入来自用户探针及移动终端代理软件的隧道，终结隧道，并从中提取出原始报文，或者是经过探针、移动终端软件代理软件处理并提取出来的流量信息。传递给后续的流量还原模块（服务器群）处理。

7. 流量还原

专用的服务器群接入来自流量采集前端服务器送来的原始报文流，进行 TCP / UDP 会话还原，提取出会话净荷，并对特定的应用予以进一步处理，提取出应用专有信息；或者是针对采集服务器送来的经过预处理提取出来的流量信息，再进行必要的更加深入的还原、精简处理。流量还原的结果将以格式化形式传递给后续的流量安全处理模块。

8. 流量安全处理模块，是对用户流量进行实际安全处理的系列模块，部署于专用或多功能共用的服务器中。包括：

a) 异常流量预警

b) 网络应用管控

c) 流量内容审计

d) 应用安全扫描

3. CFS 平台对外接口

3.1. CFSP 和 CFS 探针间接口

3.1.1. CFS Probe 的状态上报接口

接口名称：**CFSProbeStatus**

方向：**CFS Probe CFS 平台**

接口输入参数：

- 探针状态信息

接口输出参数：

接口相关处理流程：

3.1.2. CFS Probe 的配置接口

接口名称：**CFSProbeConfig**

方向：**CFS 平台 CFS Probe**

接口输入参数：

- 探针配置信息

接口输出参数：

- 探针配置结果

接口相关处理流程：

3.2. CFSP 和移动终端间接口

3.2.1. CFS MAgent 的状态上报接口

接口名称：**CFSMAgentStatus**

方向：**CFS MAgent　CFS 平台**

接口输入参数：

- 移动终端代理软件状态信息

接口输出参数：

接口相关处理流程：

3.2.2. CFS MAgent 的配置接口

接口名称：**CFSMAgentConfig**

方向：**CFS 平台　CFS MAgent**

接口输入参数：

- 移动终端软件代理配置信息

接口输出参数：

- 移动终端软件代理配置结果

接口相关处理流程：

4. 隧道管理

4.1. CFSP 和 CFS Probe 间的隧道

4.1.1. 管理隧道

SDN 建立管理隧道+自定义管理协议？直接使用自定义扩展 SDN 协议？

4.1.2. 流量镜像隧道

平台侧隧道管理模块自动建立探针和平台间的流量镜像隧道，隧道的相关参数遵从平台下发的探针配置策略。

平台侧隧道管理模块要实时监测每一个探针设备的流量镜像隧道，状态可被平台管理员检索，状态要被记录，历史记录也可以被检索。

在流量镜像隧道发生故障时，隧道管理模块要通过 SDN 协议予以处理以恢复正常。

4.1.1. 负载均衡

4.2. CFSP 和 CFS MAgent 间的隧道

4.2.1. 管理隧道

4.2.2. 流量镜像隧道