

360 入侵检测系统 白皮书

目录

1. 产品概述	1
1.1 现今网络面临的难题.....	1
1.2 采用的主流入侵检测技术.....	2
1.3 系统核心引擎运行流程	4
2. 产品特色	5
2.1 强大的分析检测能力.....	5
2.2 全面的检测范围.....	5
2.3 超低的误报率和漏报率	5
2.4 更直观的策略管理结构	6
2.5 细致详尽的全方位安全可视化.....	6
2.6 基于全局理念的安全指导指数.....	6
3. 技术优势	6
3.1 硬件加速包截获技术.....	6
3.2 基于状态的协议分析技术	7
3.3 应用层协议分析.....	7
3.4 成熟的流检测技术，提升性能和准确性	7
3.5 深度数据分析	8
4. 典型应用	8
5. 客户价值	9

1.产品概述

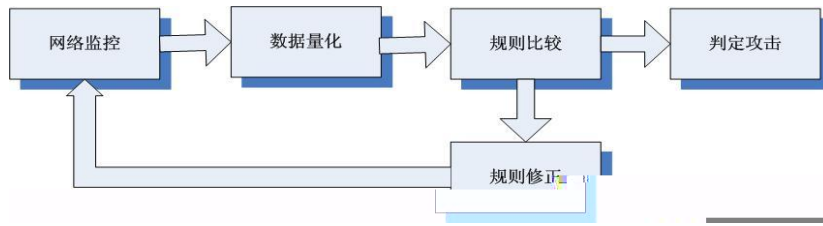
G

1.1 现今网络面临的难题

0

1.2 采用的主流入侵检测技术

-
-
-



●

●

●

●

●

●

G

G

G

G

G

1.3 系统核心引擎运行流程

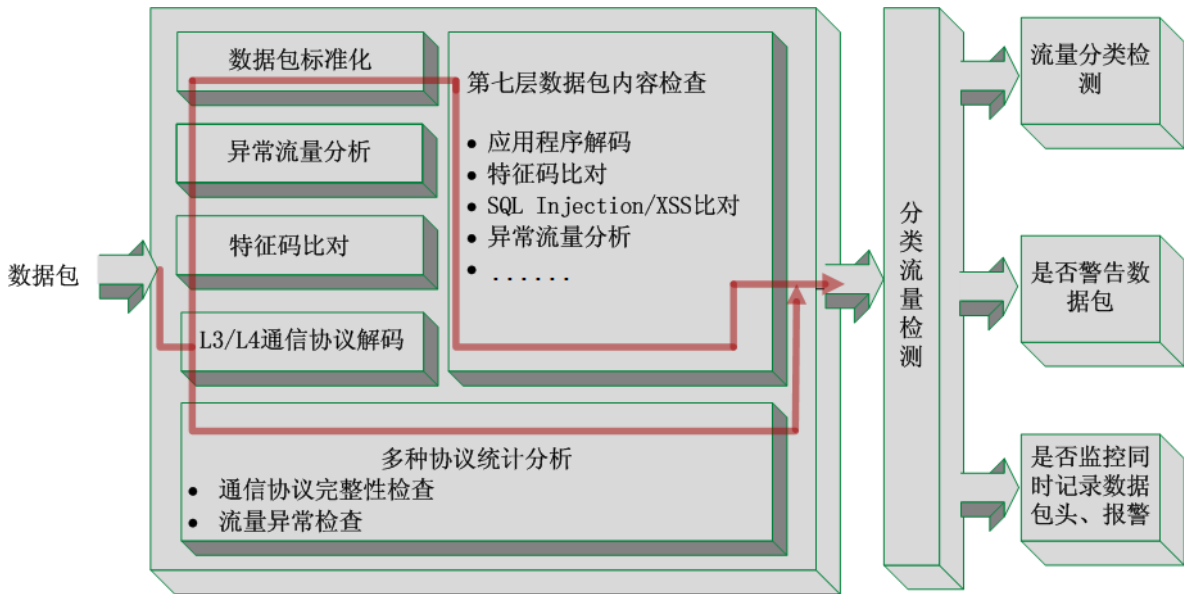
14

14

14

14

14



14

2. 产品特色

2.1 强大的分析检测能力

14

2.2 全面的检测范围

14

gle

0

AEG

GG

n0n G

2.3 超低的误报率和漏报率

A G

G

2.4 更直观的策略管理结构

14

2.5 细致详尽的全方位安全可视化

14

14 ca

14

n0n

G

G

G

G

/

G

G

mn/

C g

me

2.6 基于全局理念的安全指导指数

14

3.技术优势

3.1 硬件加速包截获技术

14

3.2 基于状态的协议分析技术

14

DA

14

G

14

c lcr D F

G

G

3.3 应用层协议分析

A G

14

3.4 成熟的流检测技术，提升性能和准确性

14

A

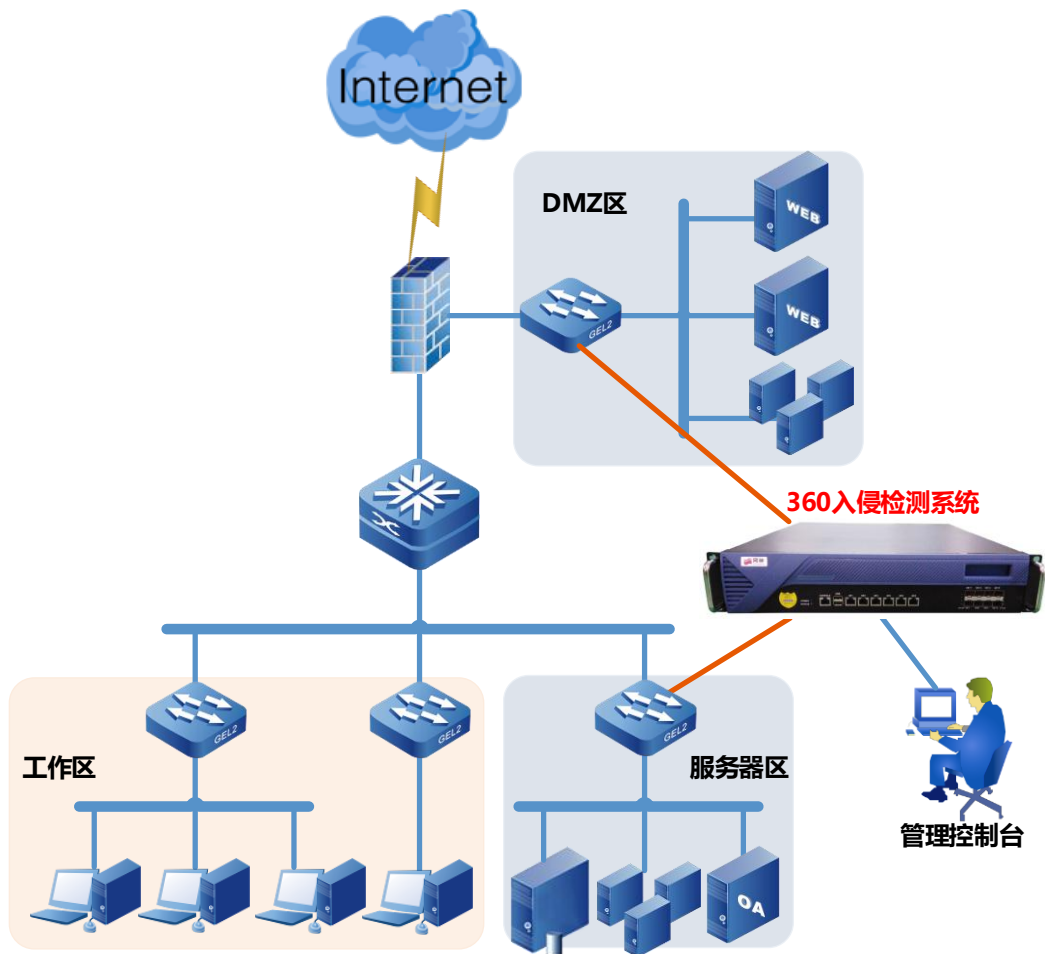
G

3.5 深度数据分析

14

4.典型应用

14



5.客户价值

me

14