TOPSEC 解决方案

天融信公司技术服务部

对本稿的任何疑问、建议、意见欢迎跟 陈爱锋 联系，以便修正

010-62304680-261

chenaifeng@sohu.com

chenaifeng@ccert.com.cn

提 纲

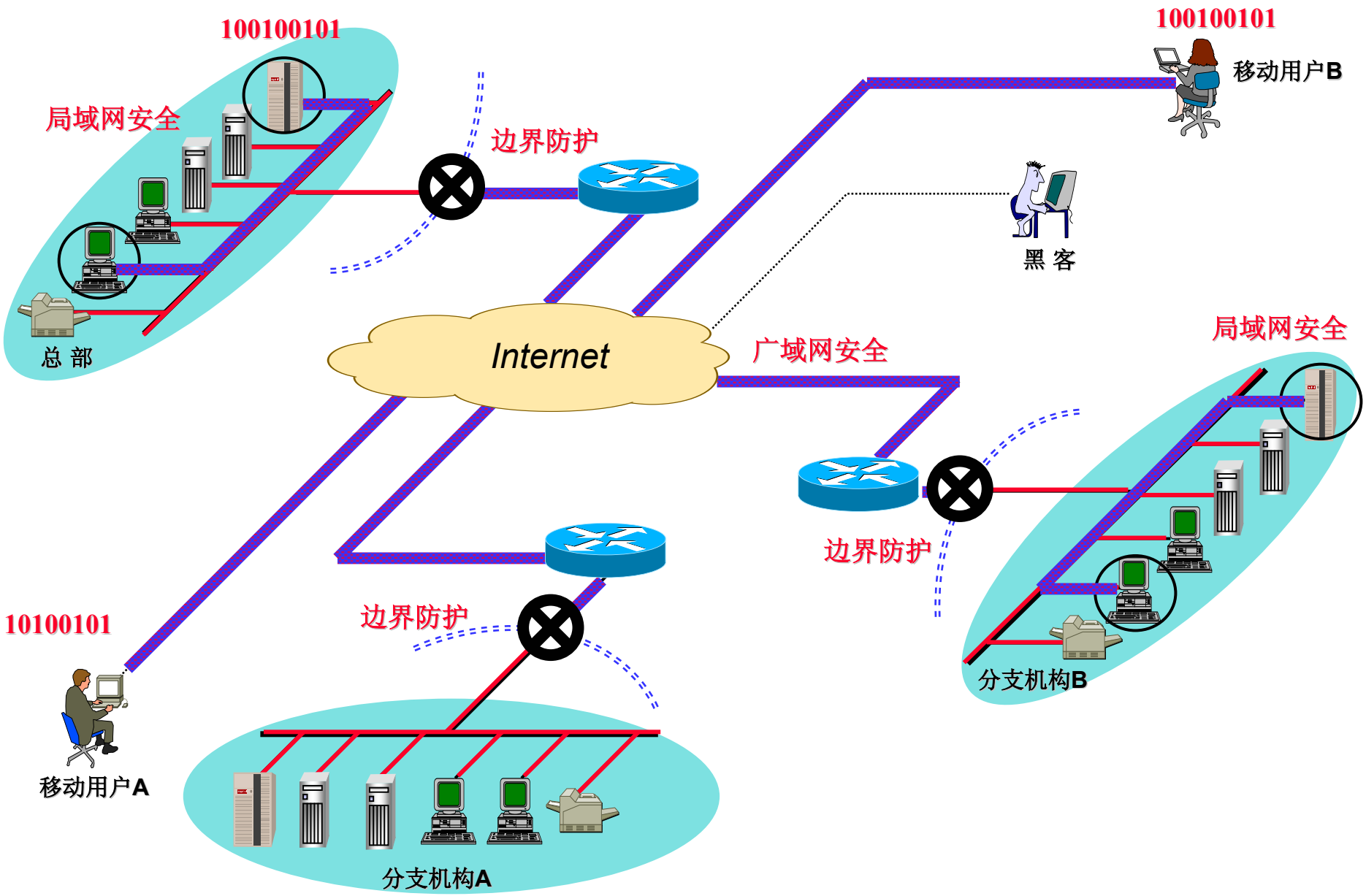
为什么需要 Topsec

Topsec 技术剖析

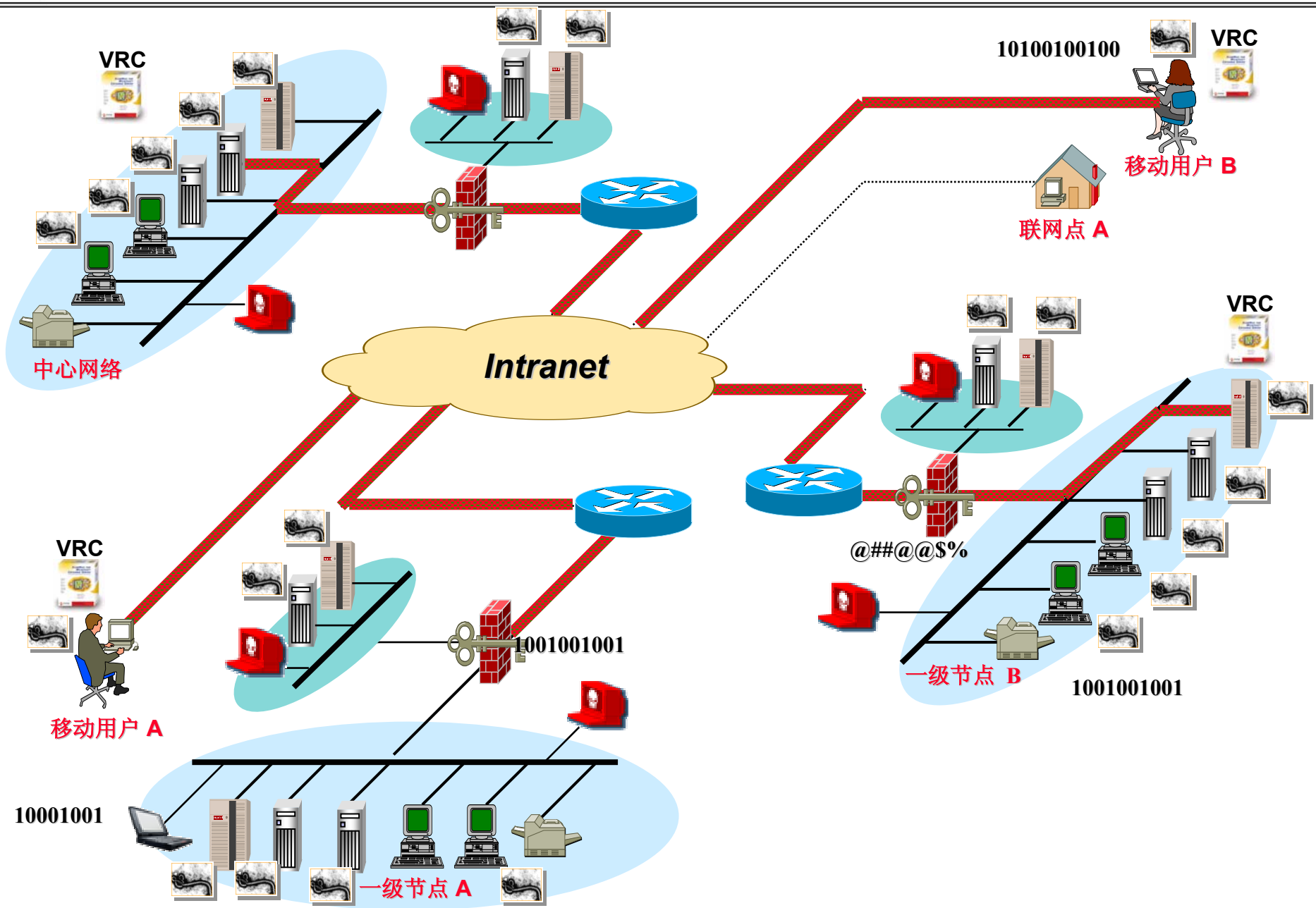
Topsec 的优势

Topsec 带来的实惠

网络面临的安全问题


100100101
局域网安全
总 部
边界防护
Internet
100100101
移动用户B
黑 客
广域网安全
局域网安全
边界防护
分支机构B
10100101
移动用户A
边界防护
分支机构A

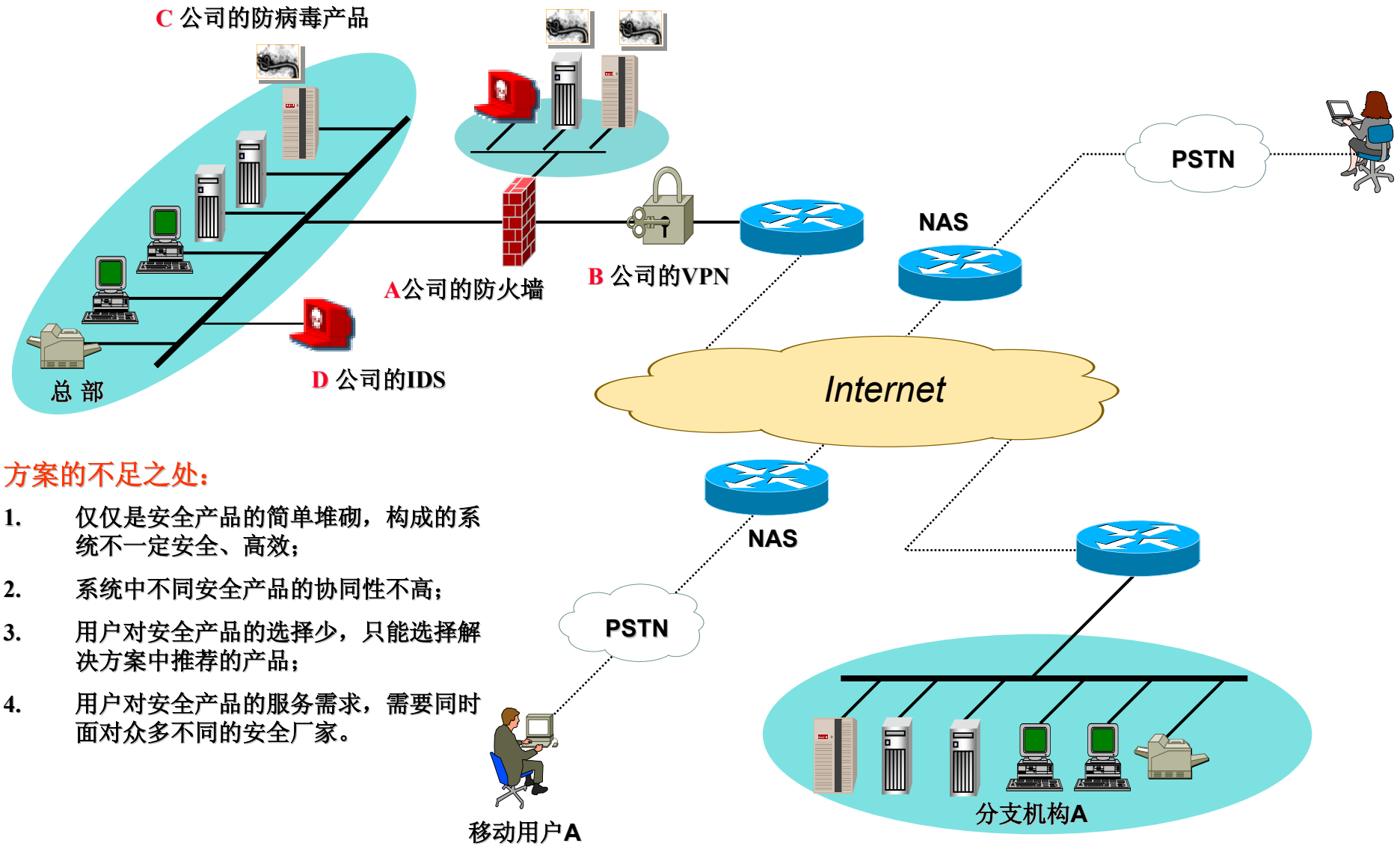
针对上述问题的解决方案



安全集成的几种手段

1. 安全集成方法之一：
   - 自己的安全产品+第三方的安全产品=整体解决方案
   - A公司的防火墙+B公司的IDS+C公司的防病毒+D公司的VPN=整体解决方案
2. 安全集成方法之二：
   - 全部使用自己的安全产品=整体解决方案
   - A公司的防火墙+A公司的IDS+A公司的防病毒+A公司的VPN=整体解决方案
3. 安全集成方法之三：
   - 自己的安全产品+标准TOPSEC协议+第三方的安全产品=整体解决方案
   - A公司的支持TOPSEC协议的防火墙+B公司支持TOPSEC协议的IDS+C公司支持TOPSEC协议的防病毒+D公司支持TOPSEC协议的VPN=整体解决方案

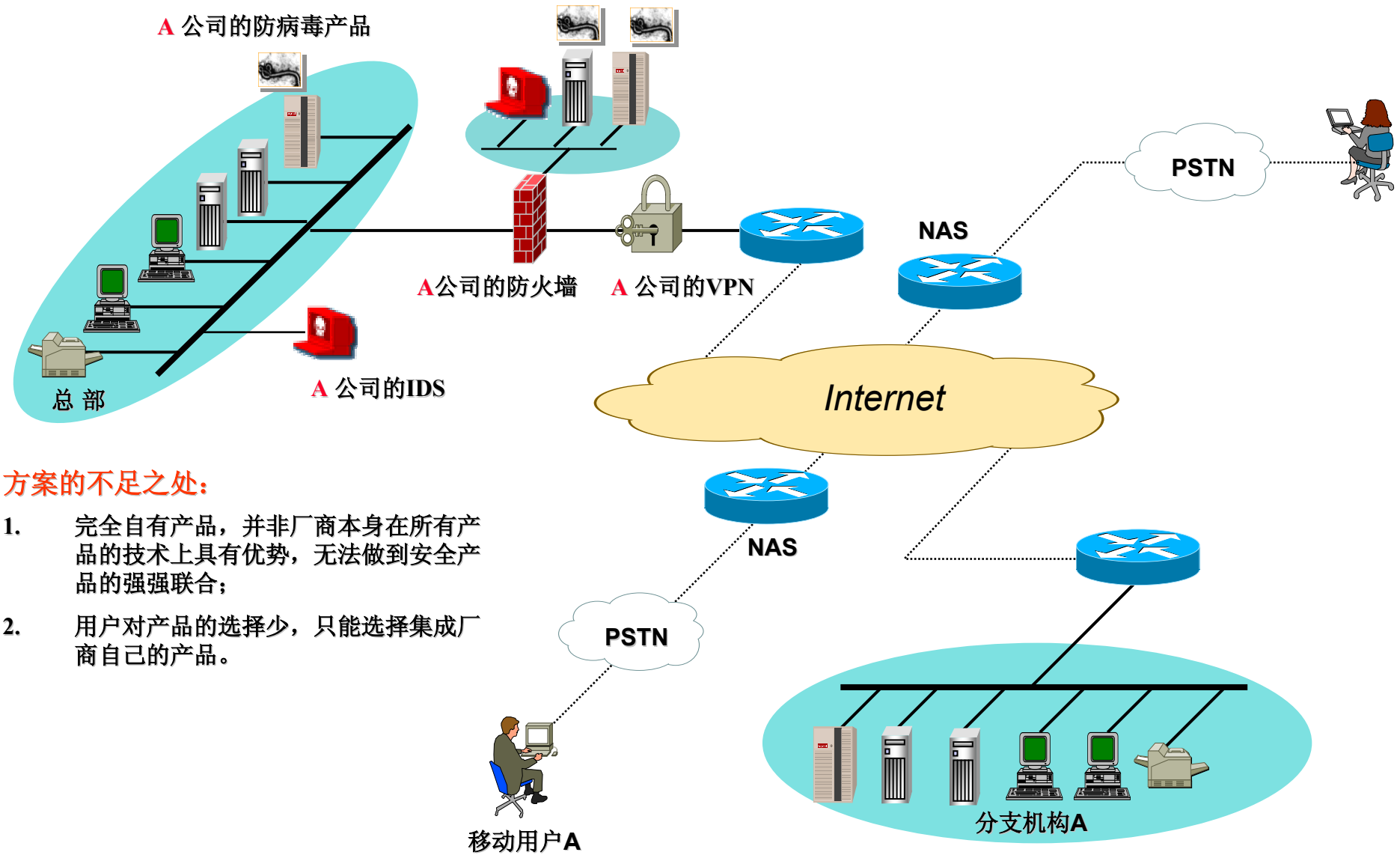
第一种安全集成方案



方案的不足之处：

1. 仅仅是安全产品的简单堆砌，构成的系统不一定安全、高效；
2. 系统中不同安全产品的协同性不高；
3. 用户对安全产品的选择少，只能选择解决方案中推荐的产品；
4. 用户对安全产品的服务需求，需要同时面对众多不同的安全厂家。

第二种安全集成方案



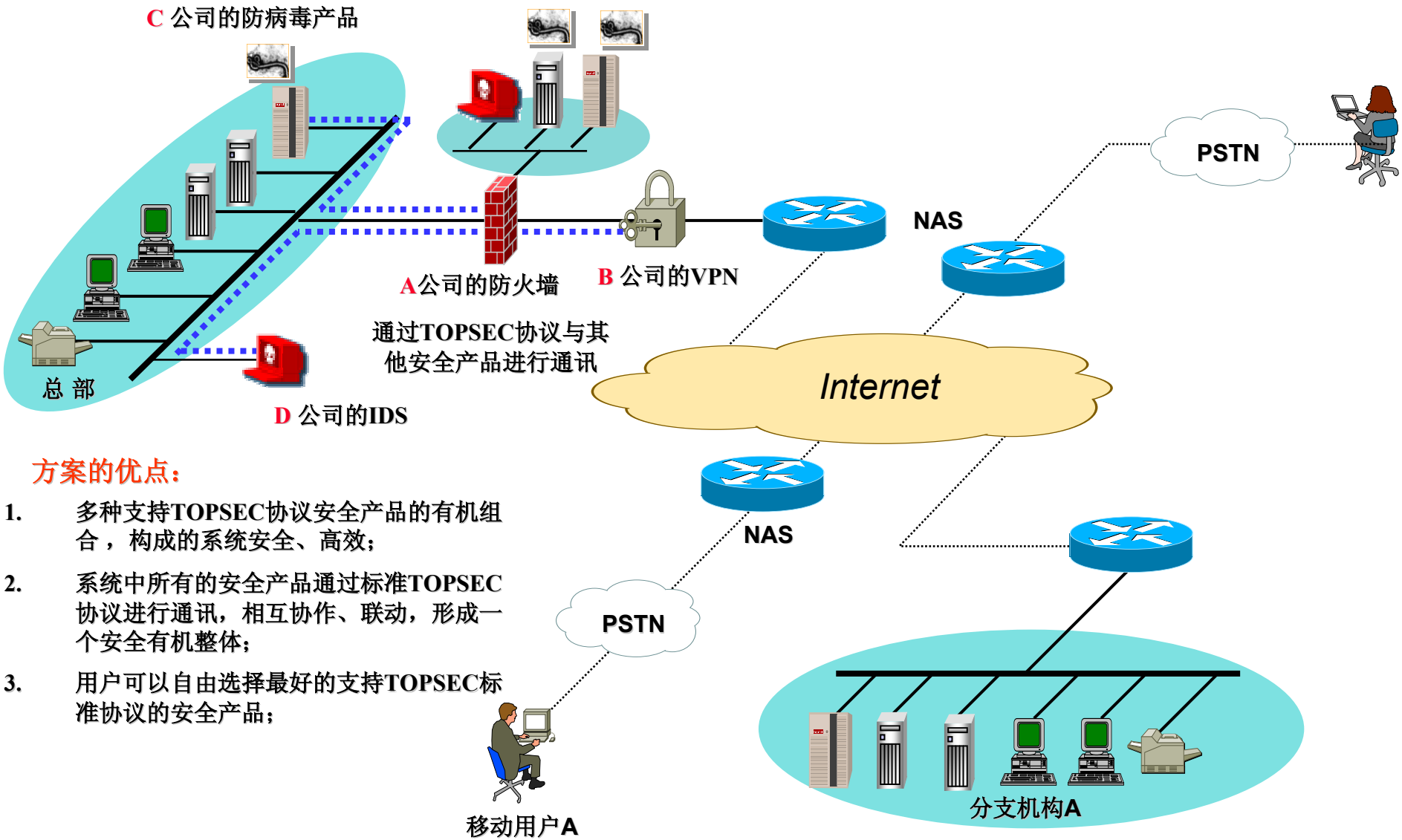
方案的不足之处：

1. 完全自有产品，并非厂商本身在所有产品的技术上具有优势，无法做到安全产品的强强联合；
2. 用户对产品的选择少，只能选择集成厂商自己的产品。

1. 使用不同厂家的安全产品所提供的安全解决方案具有不足之处；
2. 使用同一家厂商的安全产品所提供的安全解决方案也有自己的弱点；

那一个好的安全解决方案应该用什么样的安全产品来构建呢？

第三种安全集成方案

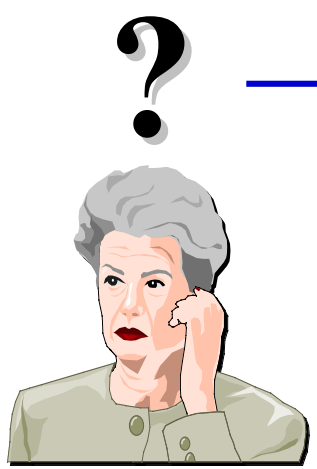


方案的优点：

1. 多种支持TOPSEC协议安全产品的有机组合，构成的系统安全、高效；
2. 系统中所有的安全产品通过标准TOPSEC协议进行通讯，相互协作、联动，形成一个安全有机整体；
3. 用户可以自由选择最好的支持TOPSEC标准协议的安全产品；

小 结

- TOPSEC解决方案能让不同品牌的安全产品相互联动、协同工作
- TOPSEC解决方案让用户可以自由选择性价比最好的安全产品
- TOPSEC解决方案能让合作伙伴、最终用户都从中获益



那么什么是TOPSEC 呢？

为什么需要 Topsec

Topsec 技术剖析

Topsec 的优势

Topsec 带来的实惠

TOPSEC解决方案的基本架构

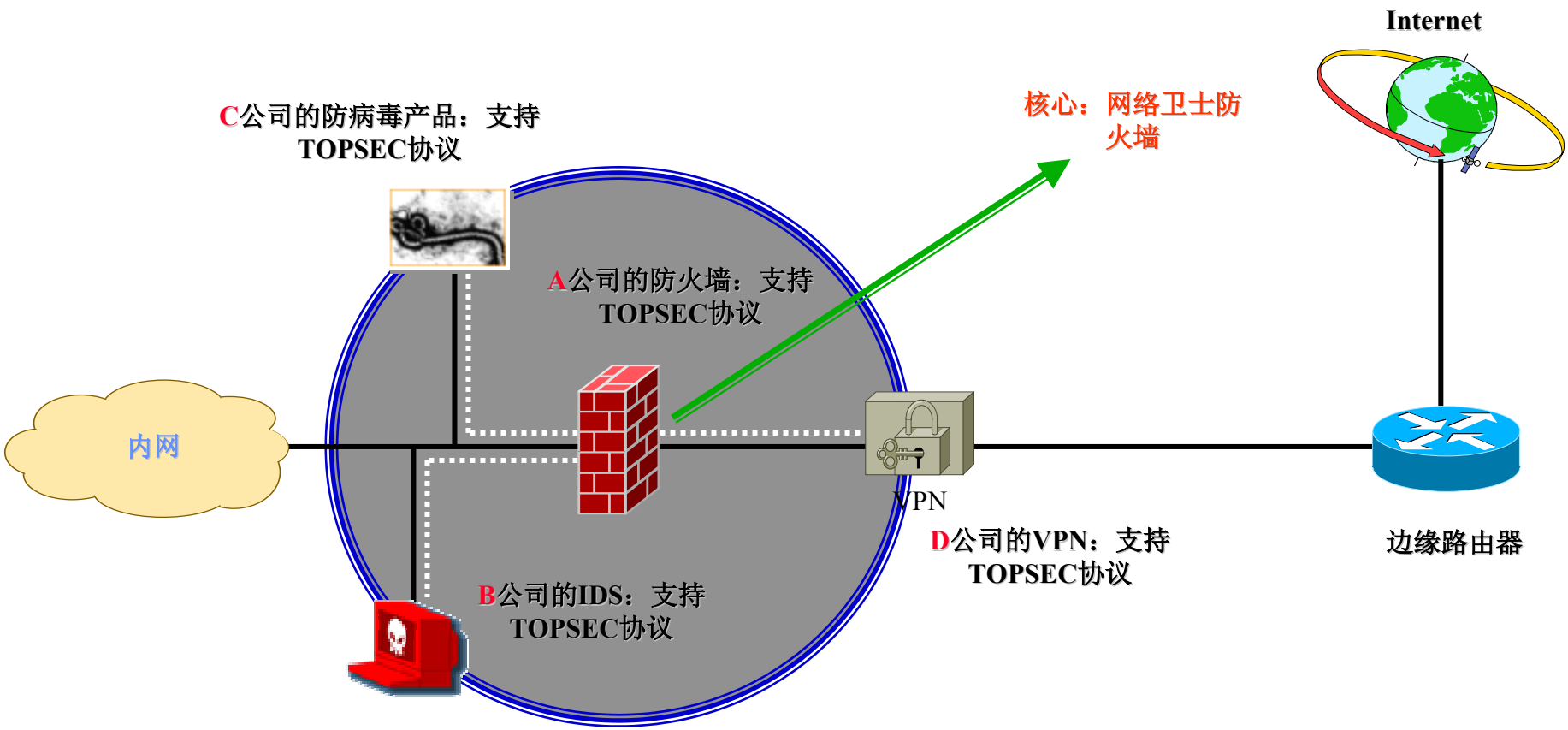
- **Talent Open Platform for Security**
  - 以网络卫士（NGFW）系列防火墙为核心
  - 以自主设计的TOPSEC协议为基础框架
  - 以PKI/CA体系为支撑平台
  - 集成/联动各类网络安全技术和产品
  - 构造一个统一的、可扩展的安全体系平台

TOPSEC的组成部分之一：防火墙

- 网络卫士系列防火墙
  - 是TOPSEC网络安全体系平台的核心，不仅拥有目前主流防火墙的所有核心功能，并具有极高的速率；
  - 支持大量的并发连接/协议还原/状态检测；
  - 动态过滤/包过滤代理；
  - 地址转换（NAT）/地址映射（MAP）；
  - ……

网络卫士系列：防火墙

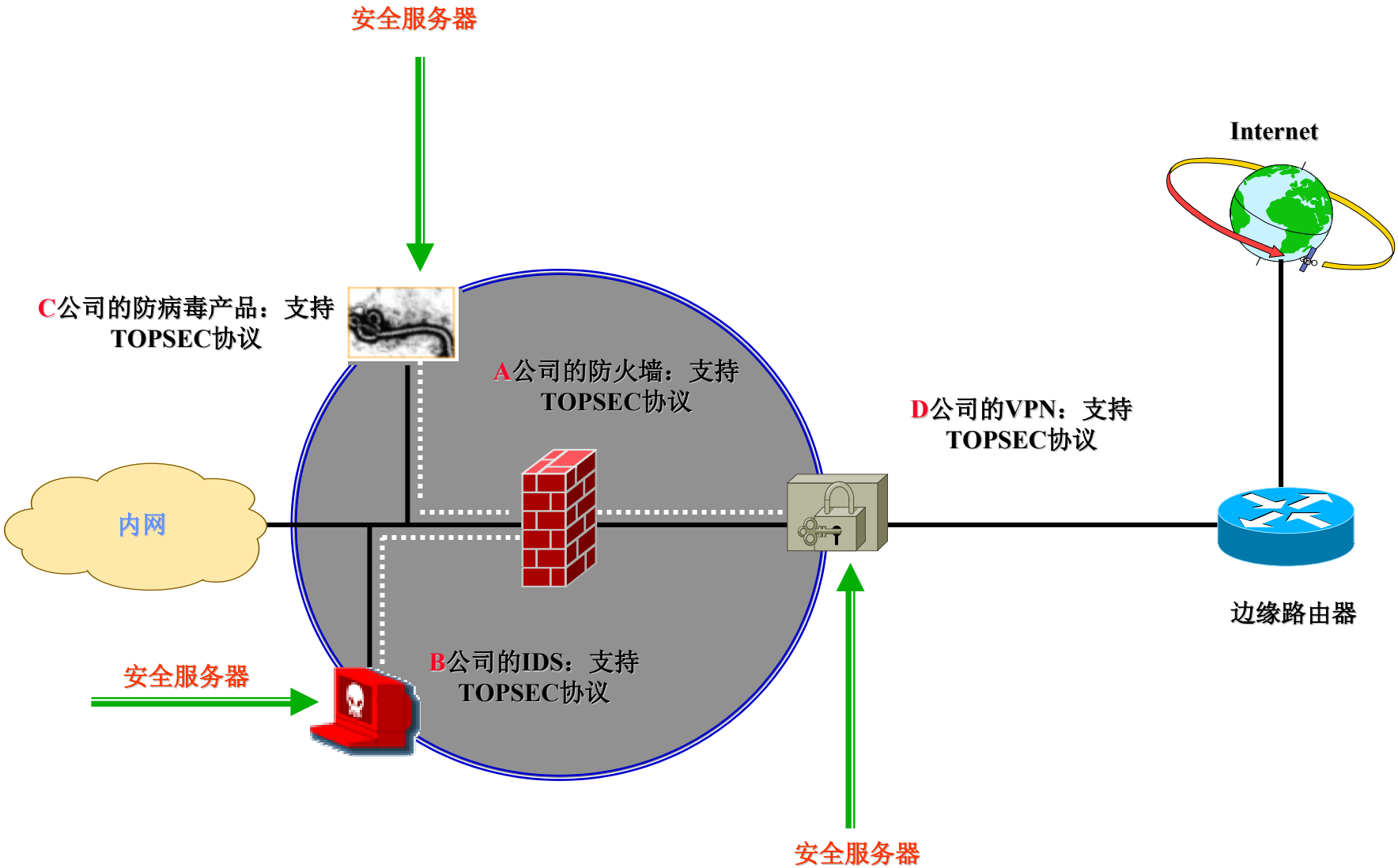
网络卫士防火墙在这里主要完成核心功能，周围的安全服务器将分担防火墙的负载，共同组成一个有机的安全整体



TOPSEC的组成部分二：TSS

- TOPSEC安全服务器（TSS）
  - 分布在网络卫士防火墙的外围支持各类TOPSEC协议的网络安全产品和系统，统称为TOPSEC安全服务器（Talent Security Server）包括：
  - 入侵检测产品（IDS）
  - 防病毒产品
  - 安全审计系统
  - 认证系统
  - 加密设备
  - PKI/CA系统
  - ……

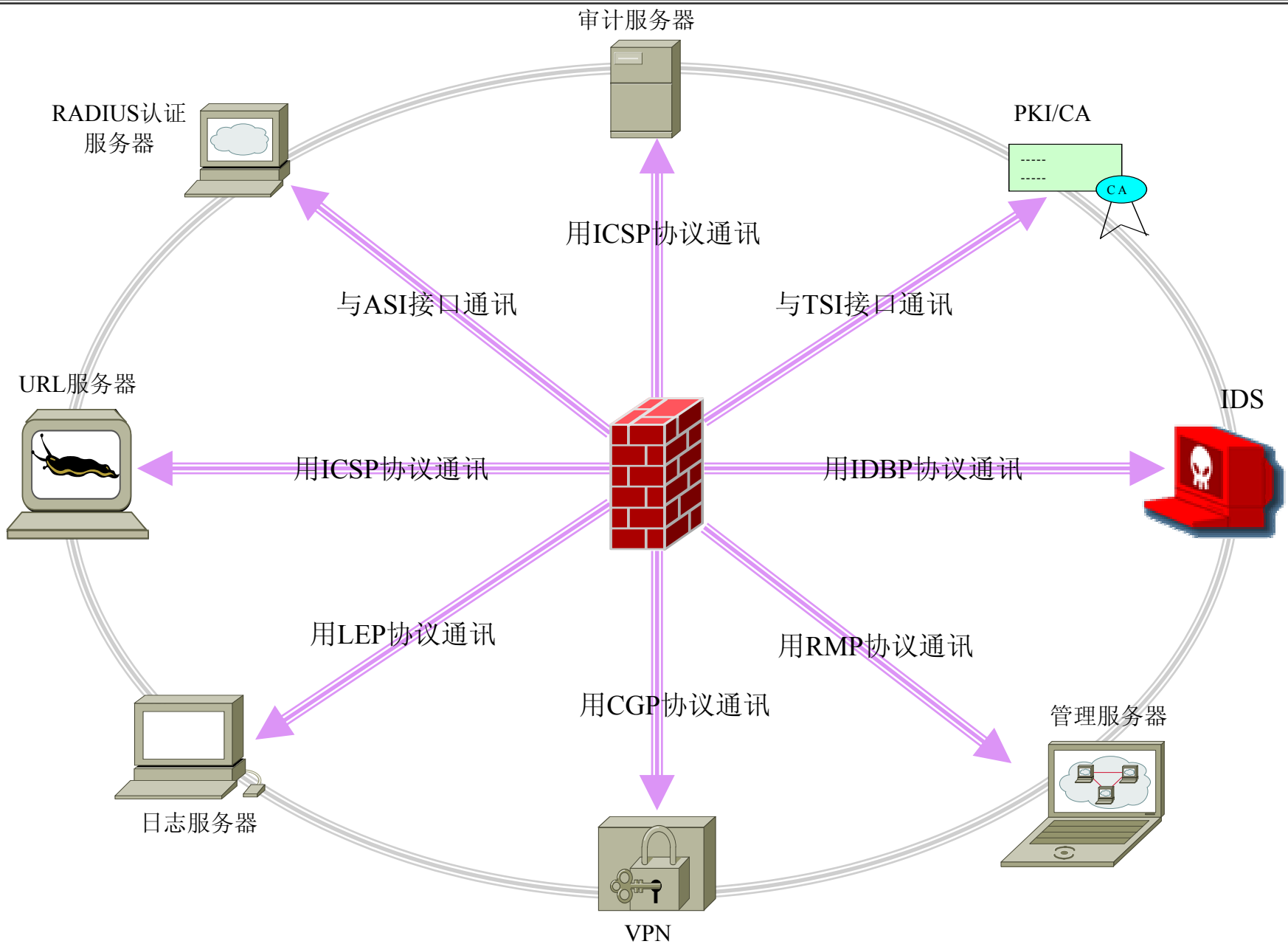
安全服务器（TSS）


安全服务器
Internet
C公司的防病毒产品：支持
TOPSEC协议
A公司的防火墙：支持
TOPSEC协议
D公司的VPN：支持
TOPSEC协议
内网
边缘路由器
安全服务器
B公司的IDS：支持
TOPSEC协议
安全服务器

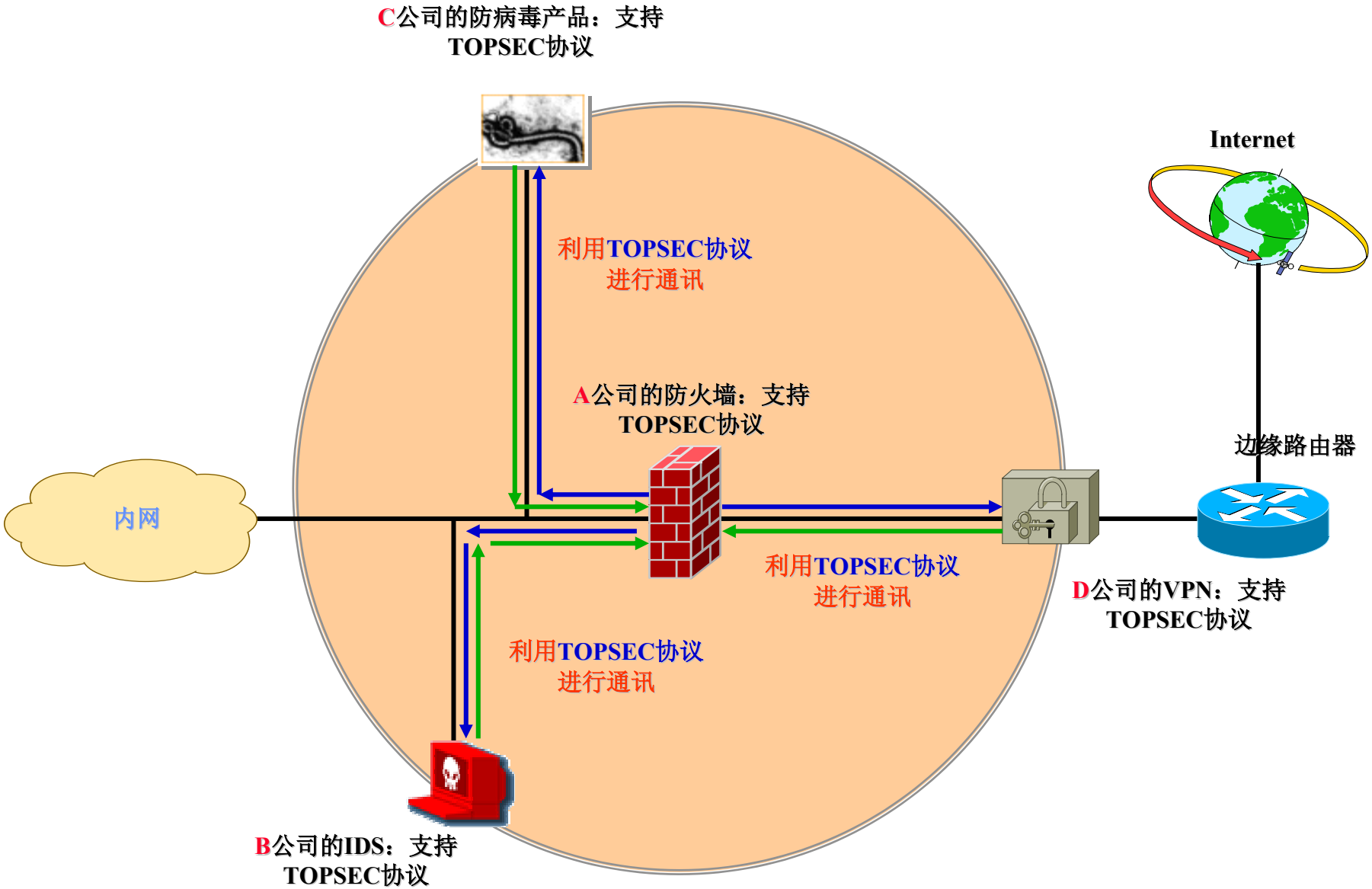
TOPSEC的组成部分三：TOPSEC协议

- **TOPSEC协议集**
  - TOPSEC协议是网络卫士系列防火墙与其外围服务器（TSS）进行通信和联动的基础，它由一系列的子协议组成，这些协议分别用于网络卫士系列防火墙与不同的TSS进行通信和联动，具体包括：
  - IDBP 入侵检测与阻断协议
  - ICSP 信息检查与过滤协议
  - ASI 鉴别服务接口
  - TSI 信任服务接口
  - LEP 日志输出协议
  - CGP 加密网关协议
  - HAP（LB/HS）高可用协议
  - RMP 远程管理协议
  - ……

TOPSEC安全体系平台结构示意图



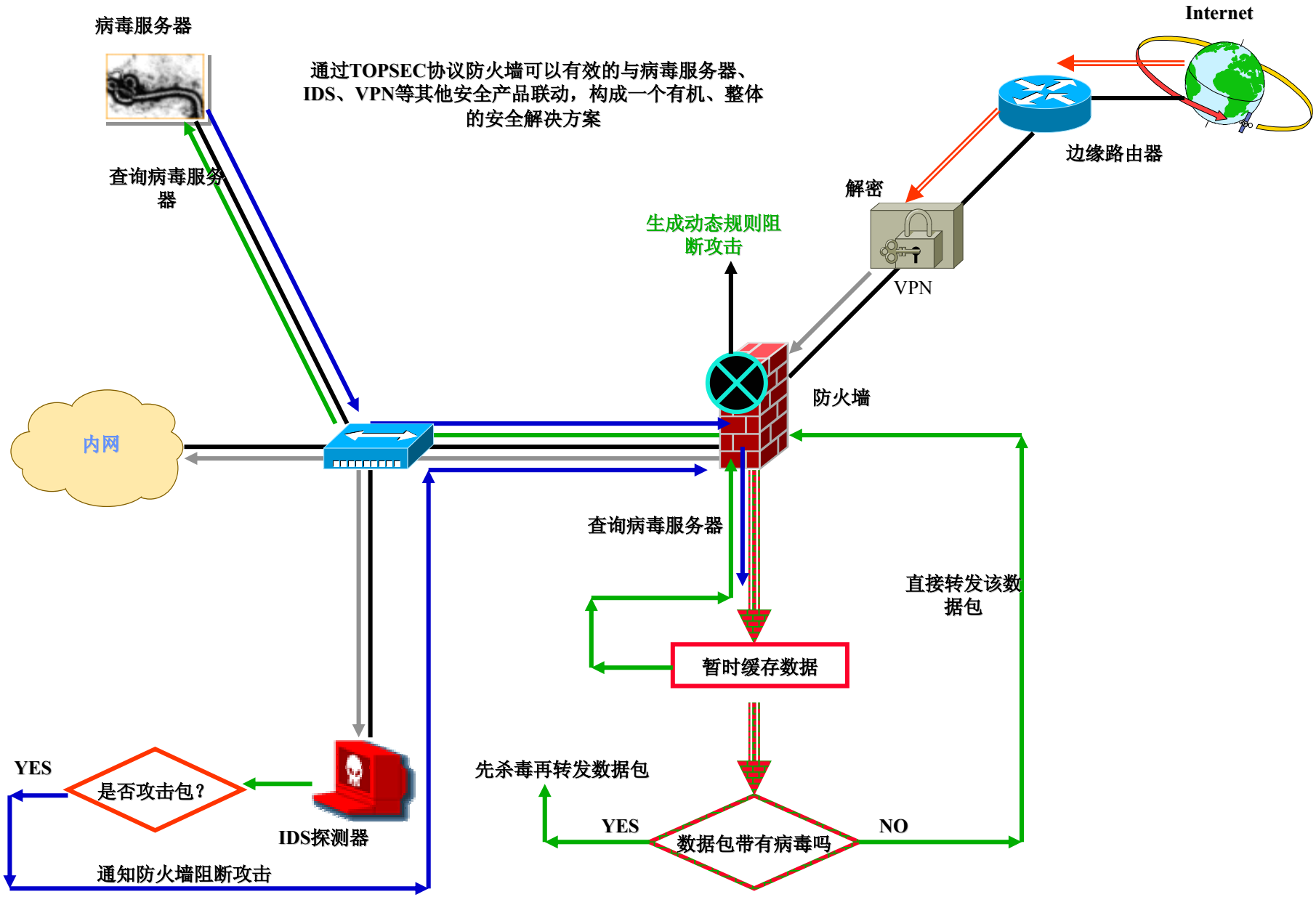
TOPSEC协议


C公司的防病毒产品：支持
TOPSEC协议
Internet
利用TOPSEC协议
进行通讯
A公司的防火墙：支持
TOPSEC协议
边缘路由器
内网
利用TOPSEC协议
进行通讯
D公司的VPN：支持
TOPSEC协议
利用TOPSEC协议
进行通讯
B公司的IDS：支持
TOPSEC协议

TOPSEC安全平台的总体特点

1. 网络卫士防火墙是整个安全平台的核心
2. 它通过TOPSEC协议接口与外围的TSS密切交互
3. 这种与TSS的交互使原本孤立的安全产品和系统与网络卫士防火墙有机联动和协同工作
4. 从而构成一个完整的、积极防御的安全体系平台，实现动态的、自适应的调整安全策略
5. 通过配置动态规则实现动态过滤，从而大大提高整个系统的安全性。

TOPSEC整体联动演示图



为什么需要 Topsec

Topsec 技术剖析

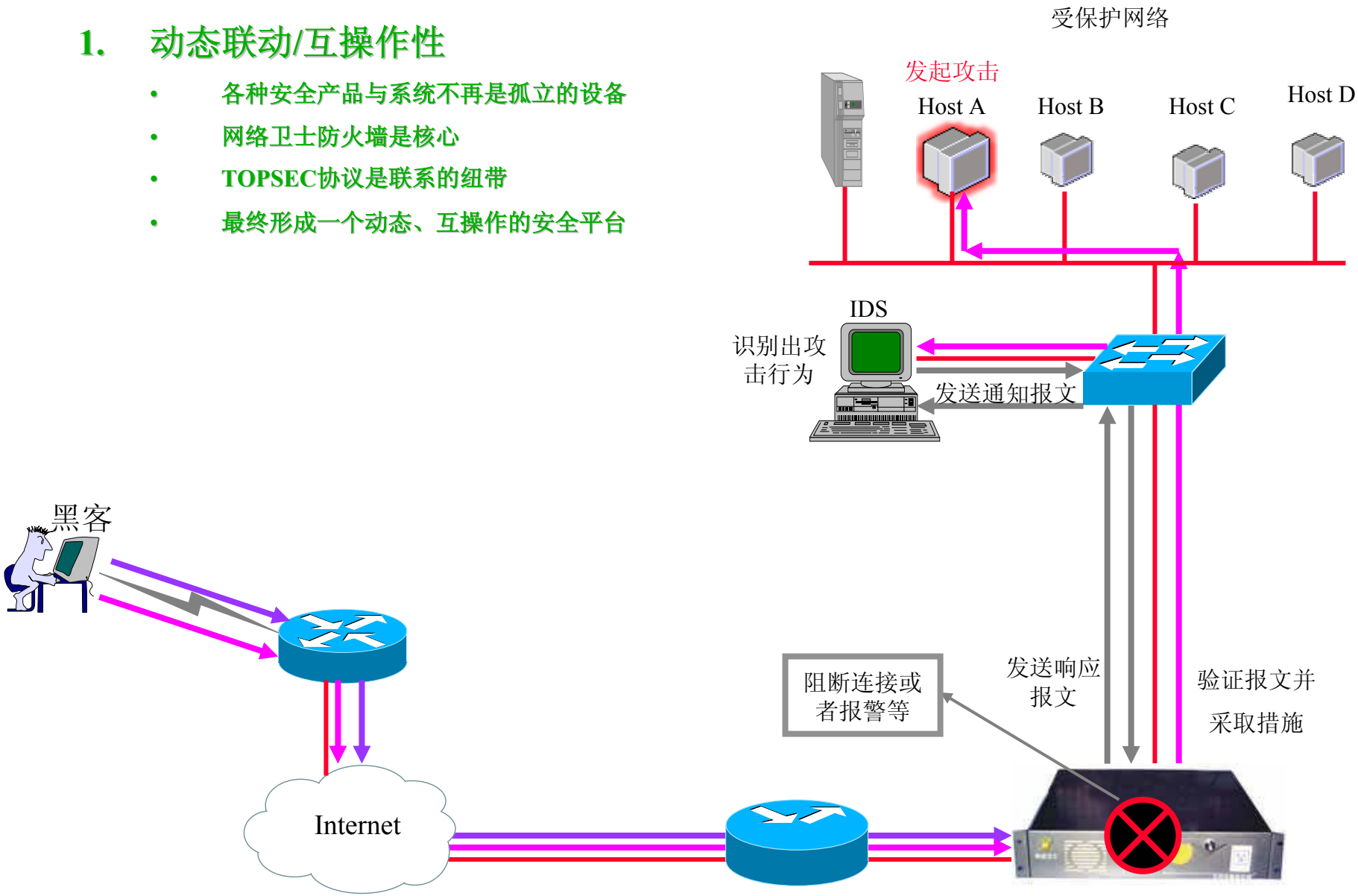
Topsec 的优势

Topsec 带来的实惠

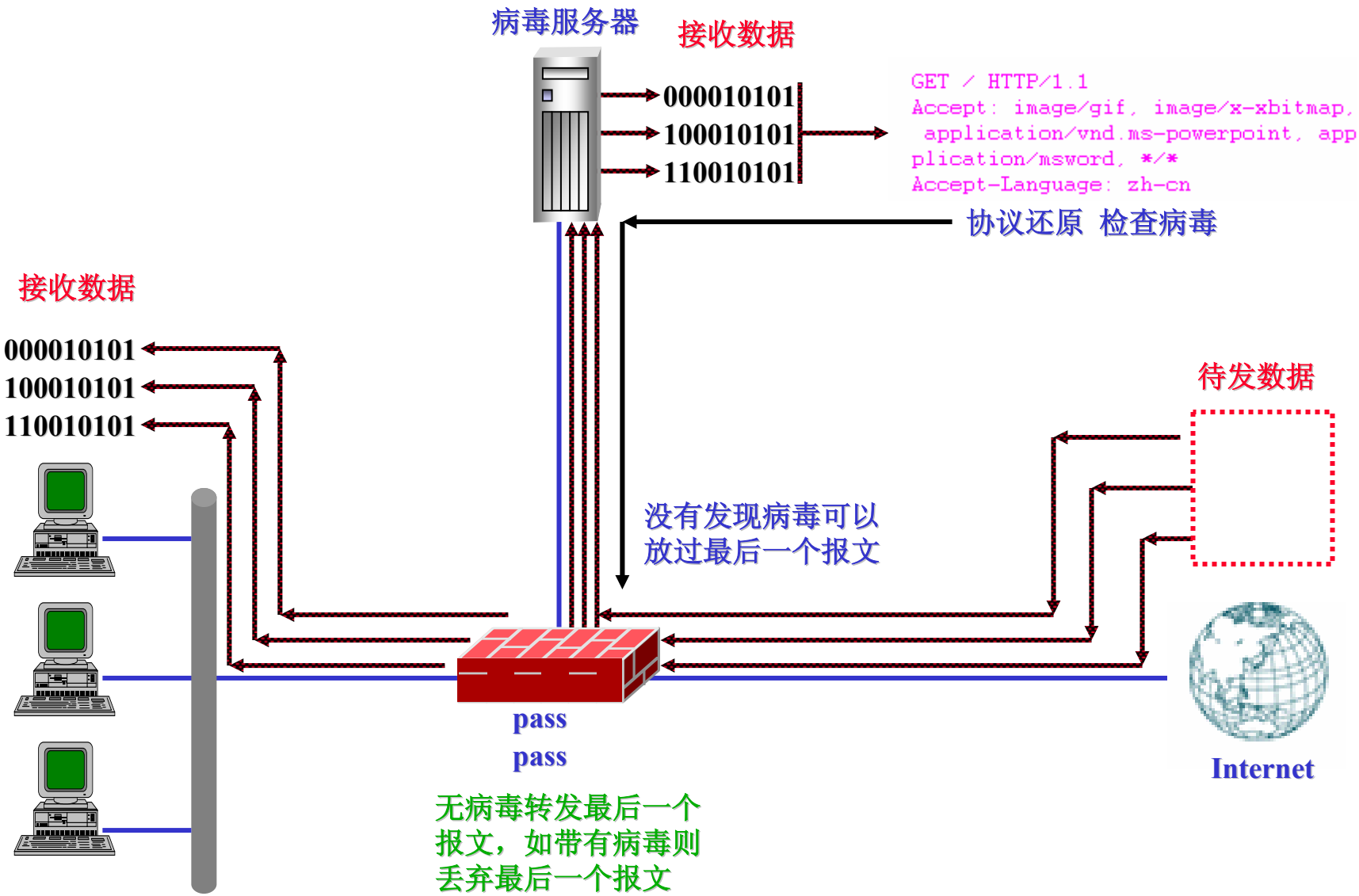
TOPSEC优势之一：与IDS的联动

1. 动态联动/互操作性

- 各种安全产品与系统不再是孤立的设备
- 网络卫士防火墙是核心
- TOPSEC协议是联系的纽带
- 最终形成一个动态、互操作的安全平台



与病毒服务器的安全联动



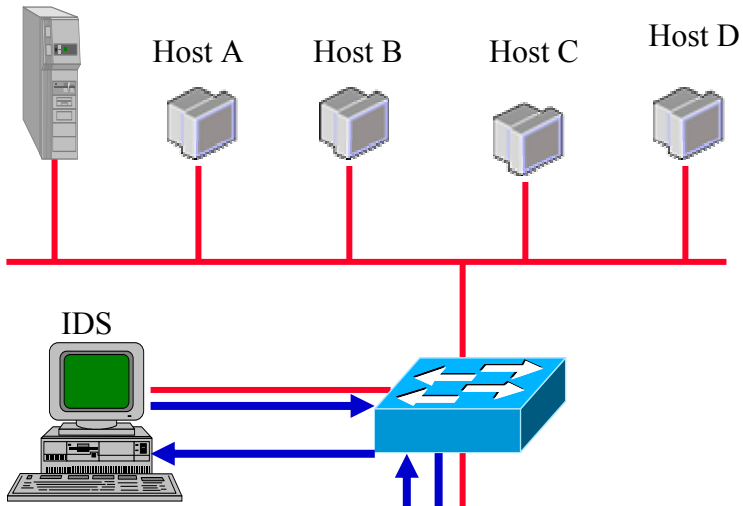
TOPSEC优势之二:安全性

2. 安全性

- 安全产品不再是简单的叠加集成
- 不同安全产品能有效的协同工作
- 不同的安全技术能优势互补
- 所以整个系统的安全性应该是1+1>2

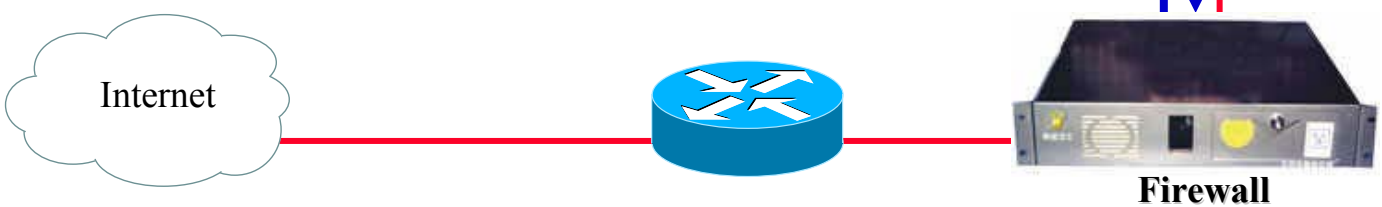
孤立的IDS ＋ 孤立的防火墙 =2

联动的IDS ＋ 联动的防火墙 >2



通过TOPSEC协议将两种不同功能的安全产品有机的组合起来

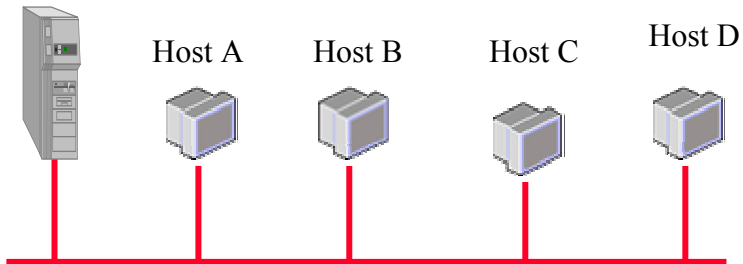
所以TOPSEC解决方案让你的系统更安全



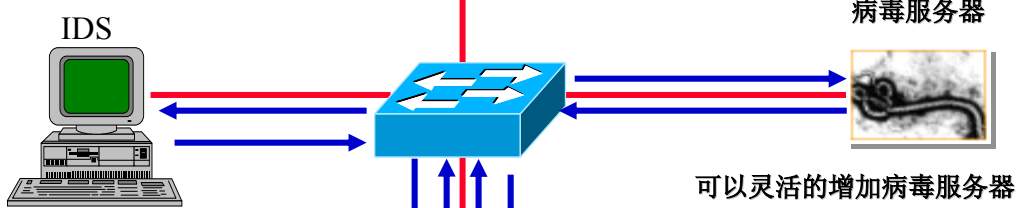
TOPSEC优势之三:可伸缩性

3. 可伸缩性

- 各种安全功能合理地分布在NGFW和TSS上实现
- 根据不同的安全需求和成本组合不同的功能模块
- 防火墙和TSS专注于自己的核心功能
- 整个系统将有更好的综合性能



由此可见，TOPSEC解决方案让您可以灵活的分步实施自己的安全规划



起先没有购买安全产品

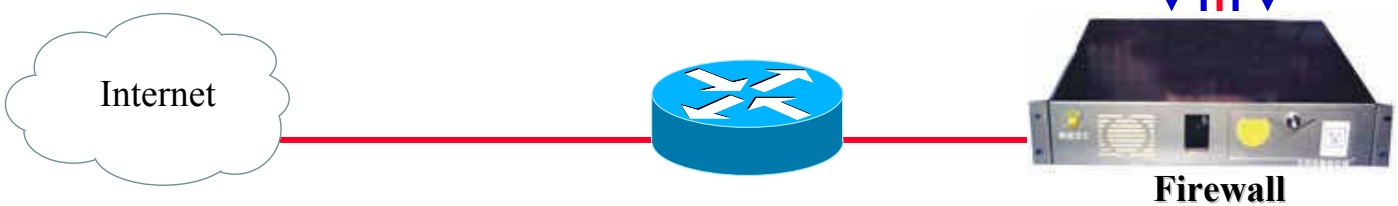
可以灵活的增加IDS

可以灵活的增加病毒服务器

一期增加一个支持TOPSEC协议的防火墙

二期增加一个支持TOPSEC协议的IDS

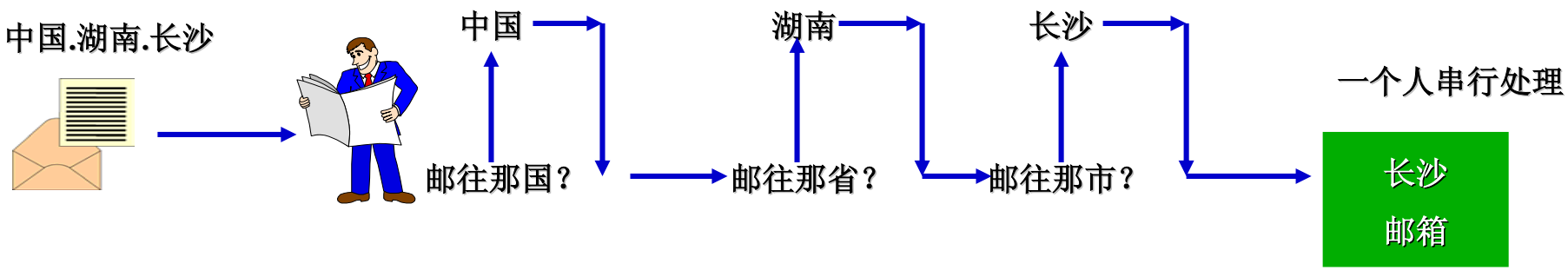
三期增加一个支持TOPSEC协议的病毒服务器

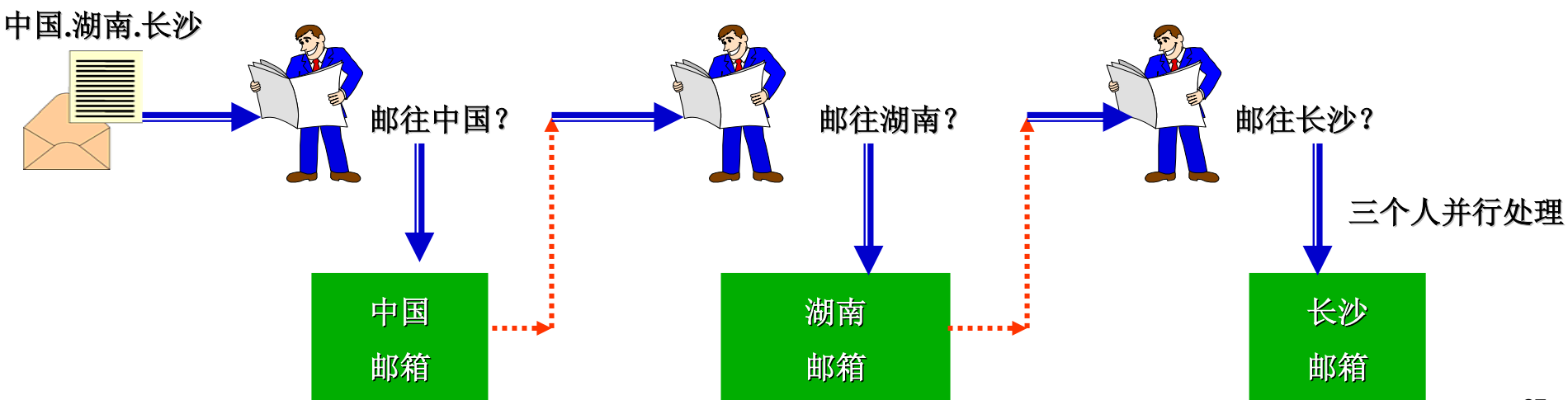


TOPSEC优势之四:高性能

4. 高性能

- 诚然，在防火墙上实现TOPSEC协议将会有一定的系统开销
- 但对防火墙的核心功能影响很小
- 安全功能/任务的合理分发，使各种安全产品专注于自己的核心功能
- 防火墙可以调度多个TSS同时处理同一数据（串行处理到并行处理的转变）
- 故系统的整体性能将明显提高





TOPSEC优势之五:开放性

5. 开放性/可扩展性

- TOPSEC协议对第三方厂商公开
- 其他厂商可以基于公开的TOPSEC协议开发与网络卫士防火墙联动的产品

TOPSEC优势之六:易用性

6. 易用性/可管理性

- 由于TOPSEC安全体系平台是一个开放的平台，可以实现与现有各种安全设备之间的互通与联动，对于新出现的安全技术和产品也保留了开放的扩展接口。
- 由于TOPSEC安全体系平台具有一定程度的智能性，通过NGFW与TSS之间的有机联动，用户不必再手工地配置和调整每个安全设备上的安全策略和规则。同时，整个TOPSEC安全体系平台可以通过统一的基于SNMP的网络安全管理平台来进行集中管理和监控，具有更好的可管理性。

为什么需要 Topsec

Topsec 技术剖析

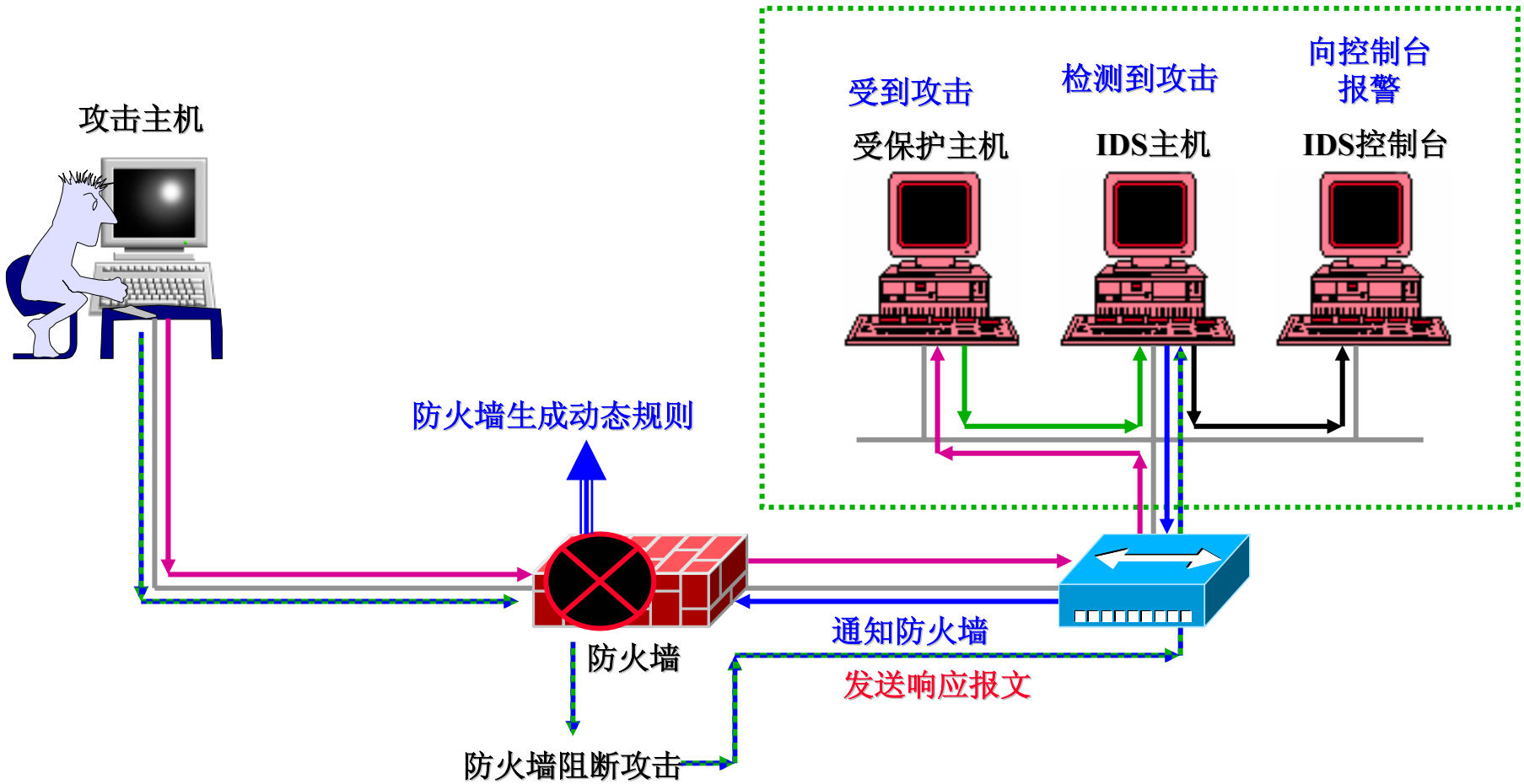
Topsec 的优势

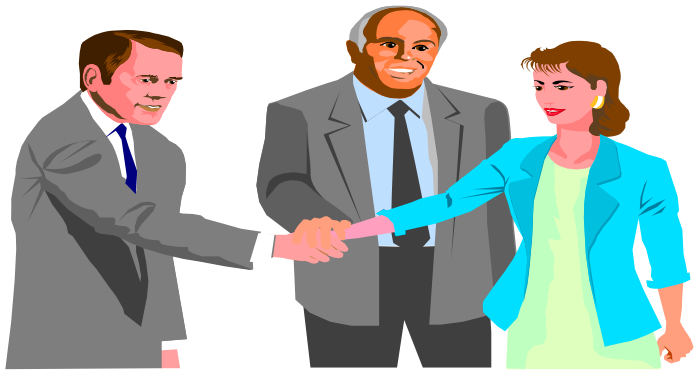
Topsec 带来的实惠

TOPSEC的实惠

1. 对于合作伙伴
   1. 支持TOPSEC协议可以提高其产品在市场上的竞争力
   2. 同时也能够提供最好的、满足用户安全需求的安全解决方案
2. 对于最终用户
   1. 选择TOPSEC平台就等于选择了安全产业内专业厂商提供的最优秀的技术、产品和服务，以及他们之间的最佳组合。
   2. 用户得到的不止是最好的产品，而且拥有更大的选择空间，从而获得更优质的安全服务。

防火墙与IDS联动实验原理图





谢谢！