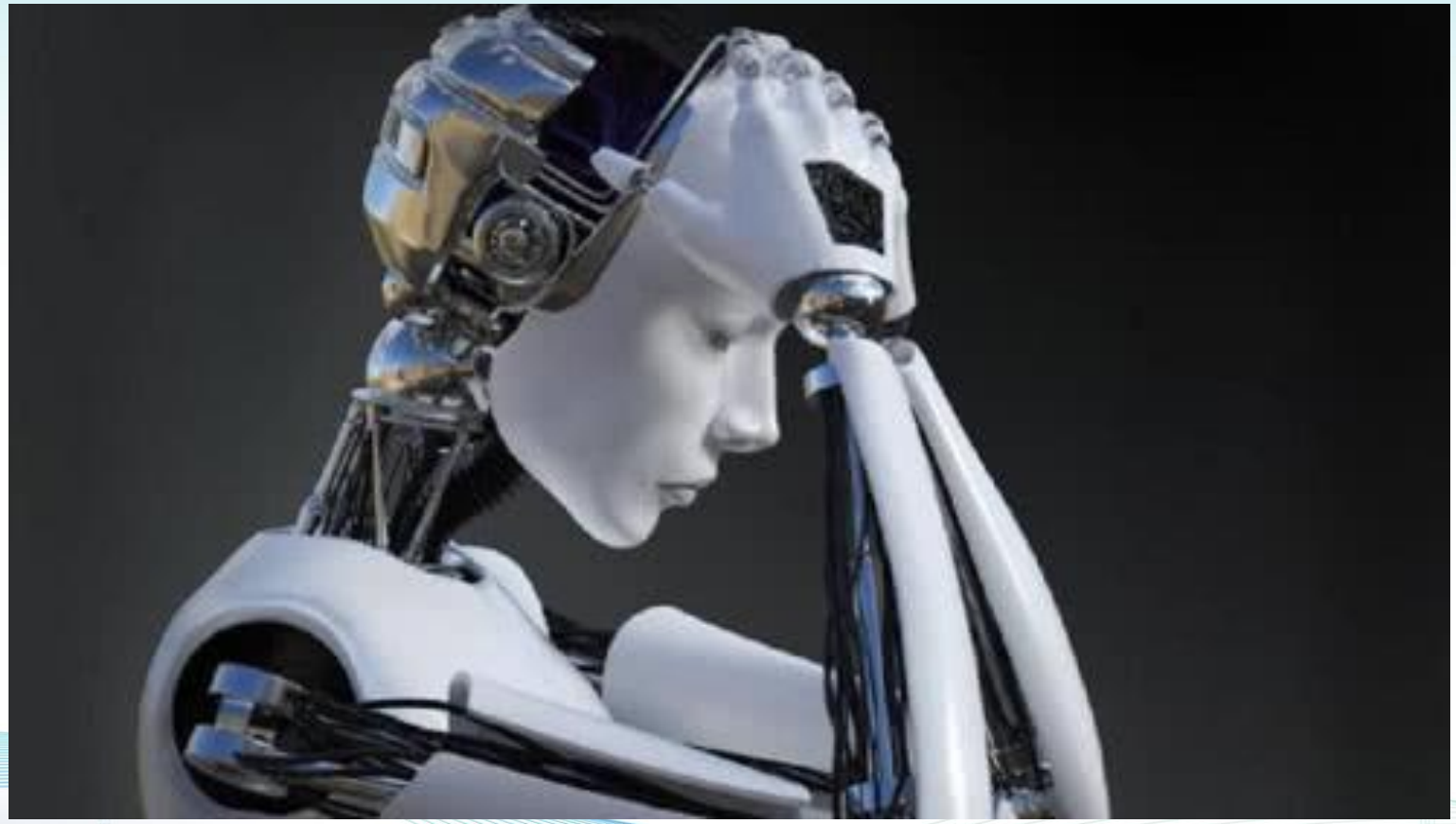
2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

《基于开源软件的网络纵深防御系统》

主讲人：吴志祥

困境



CONTENTS
目 录

研究背景

IBM 公司在1960年开发出了虚拟化技术以来，虚拟化技术已经变的越来越流行。随后VMWare公司推出了ESX Server 以及 Microsoft 公司的Hyper-V技术的虚拟化产品，当越来越多虚拟化技术的应用被提出后，我们开始思考如何将其运用在网络安全防护架构部署上并解决我们遇到的实际问题。本研究提出的是一个基于虚拟化技术的网络安全纵深防御架构解决方案，可以有效的降低企业在部署网络安全防御系统上的成本以及通过纵深防御架构来提高黑客入侵的时间成本。另外本研究也将针对传统纵深防御架构、整合威胁管理系统及本研究提出的虚拟化纵深防御架构做一综合性的深入研究并比较其优缺点，另外也针对上述架构进行网络性能测试、分析与探讨，冀望本研究能对网络安全相关研究以及企业内部的纵深防御部署提供有益的解决思路。

研究背景

目前一套包含威胁分析系统，DDOS流量清洗系统和防病毒网关的IDC网络安全防护系统价格在百万元左右。在建设资金趋紧的大环境下，市县一级的IDC中心和机房很多不具备购买商用网络安全防御工具的条件。

黑客攻击

嗅探，网络监听，非法入侵，信息窃取

恶意软件

病毒，蠕虫，木马，恶意代码，漏洞攻击脚本等

安全管理

缺乏告警监控手段，被动防御为主

业务演进

业务需求更新快，软件更新迭代快

研究背景

虚拟化部署

基于虚拟化技术搭建，便于快速部署和减少硬件投资。

使用开源软件

为降低整个系统的费用，使用开源软件来搭建。在现今的网络环境下，部分开源软件的性能不低于传统商用软件。

纵深防御机制

构筑纵深防御的网络防护架构，是网络防护方案的核心原则。当纵深防御被运用在网络安全上时则意味著以多层安全技术减轻网络安全风险。

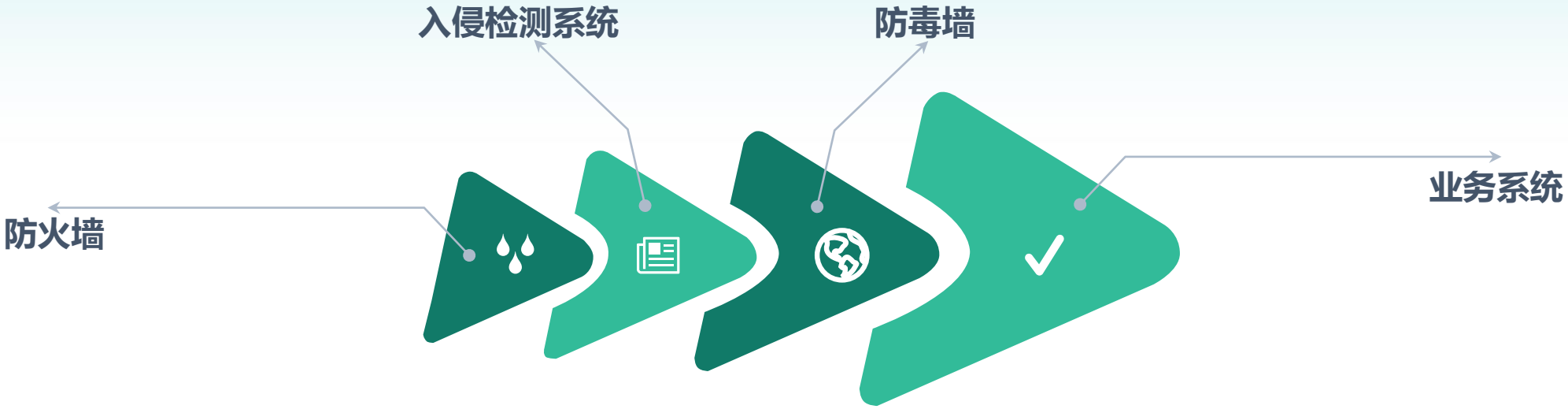
整体式威胁管理

整体式威胁管理是一个全面的解决方案，它能够执行多种安全功能。其优点在于管理多个防护系统，主要优点除了管理方便外，还有就是封包只需要解开一次。

相关研究


防火墙
阻挡非法的连接，允许合法的连接进入企业内部
虚拟专用网
在公共信道上建立安全虚拟专用网络
入侵检测系统
对网络进行即时监视，在发现可疑时发出警报或者采取主动反应措施
加密技术
信息交换加密
防毒墙
对病毒和恶意程序进行过滤的网络安全设备

相关研究

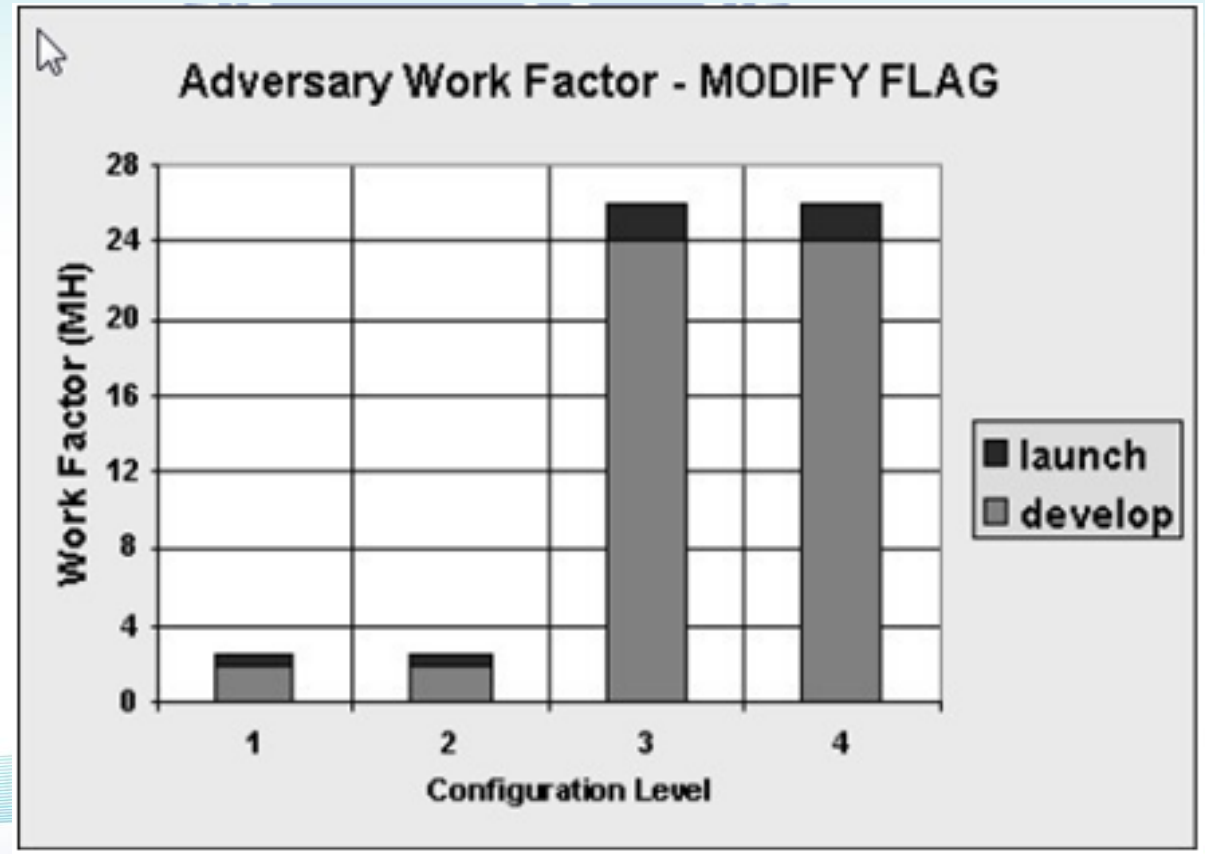


纵深防御原意是一种军事战略，有时也称作弹性防御或是深层防御，是以全面深入的防御去延迟前进中的敌人，通过放弃空间来换取时间与给予敌人额外的伤亡。当纵深防御被运用在网络安全上时则意味著以多层网络安全技术减轻网络安全风险。

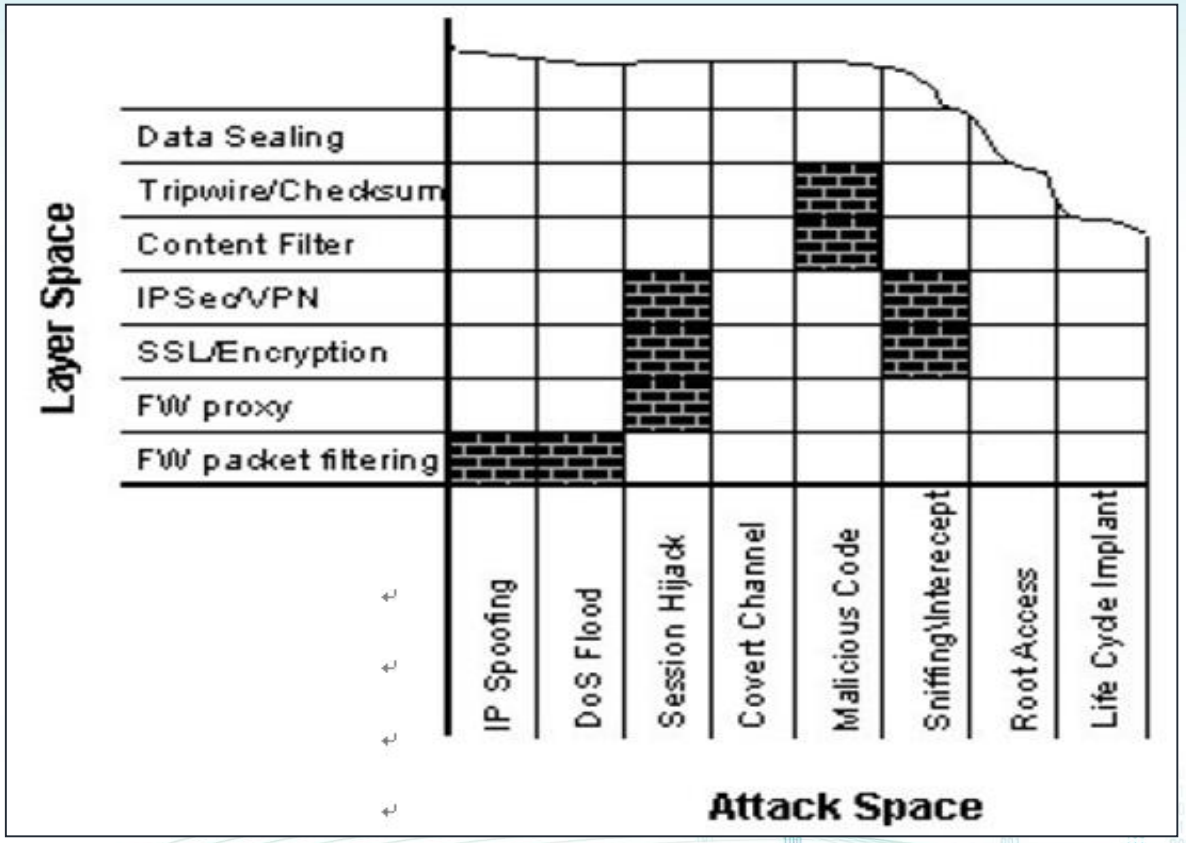
相关研究

网络安全纵深防御不能只著重在单一攻击行为上，还要针对广度防御进行部署考虑，且在考虑部署安全防御机制时，要考虑布署的层数不可太多，因为这样反而会导致防御产品太多造成维护过于复杂，而增加被黑客入侵的风险。

相关研究



纵深防御层数及攻击执行成功所花费的时间比较



深度防御 vs 广度防御

系统实现

虚拟化网络安全纵深防御架构

实体层

实际的硬件资源，如 CPU、内存、网卡、硬盘等

监督层

虚拟机器管理员在 Guest 操作系统及硬件层之间设置的抽象层，这个抽象层允许任何操作系统在硬件上执行

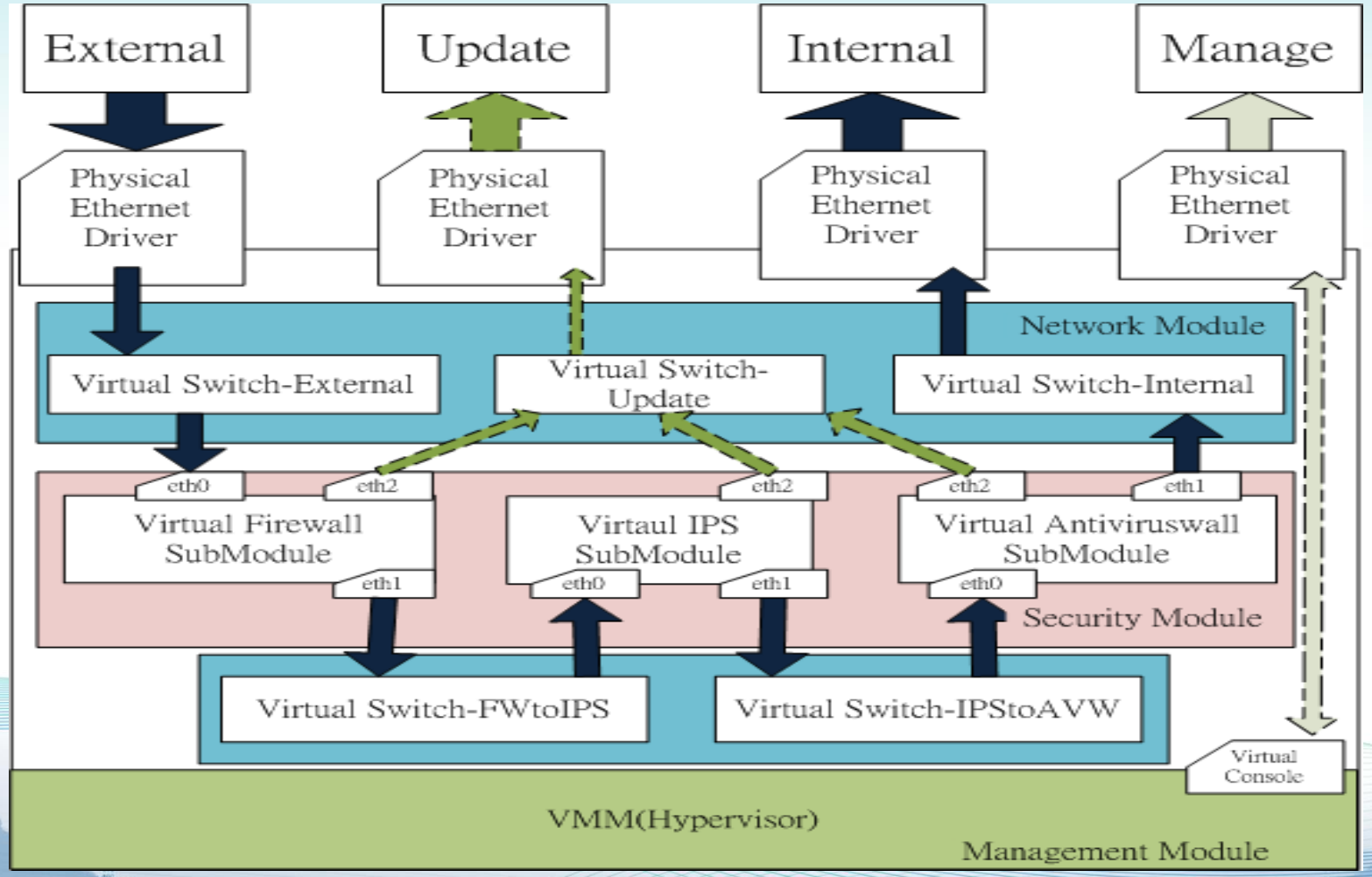
虚拟网络层

网络模组，主要作用是模拟虚拟交换机及调整虚拟机器网络架构

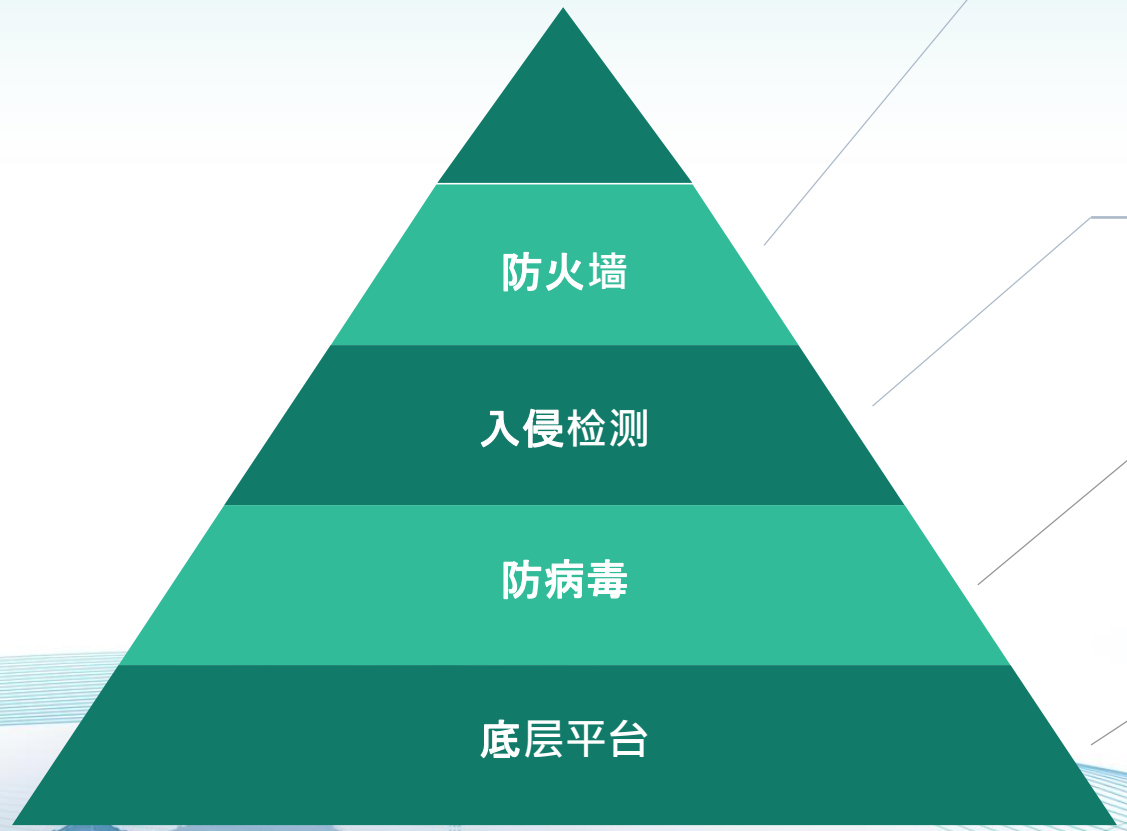
安全层

安全模组，主要作用是对网络流入流出的数据包进行检测

系统实现


External
Update
Internal
Manage
Physical Ethernet Driver
Physical Ethernet Driver
Physical Ethernet Driver
Physical Ethernet Driver
Network Module
Virtual Switch-External
Virtual Switch-Update
Virtual Switch-Internal
eth0
eth2
eth2
eth2
eth1
Virtual Firewall SubModule
Virtaul IPS SubModule
Virtual Antiviruswall SubModule
eth1
eth0
eth1
eth0
Security Module
Virtual Switch-FWtoIPS
Virtual Switch-IPStoAVW
Virtual Console
VMM(Hypervisor)
Management Module

系统实现



防火墙系统

使用 Netfilter/Iptables开源防火墙

入侵监测系统

入侵防御系统使用Snort开源入侵检测系统
搭配Iptables Queue模块

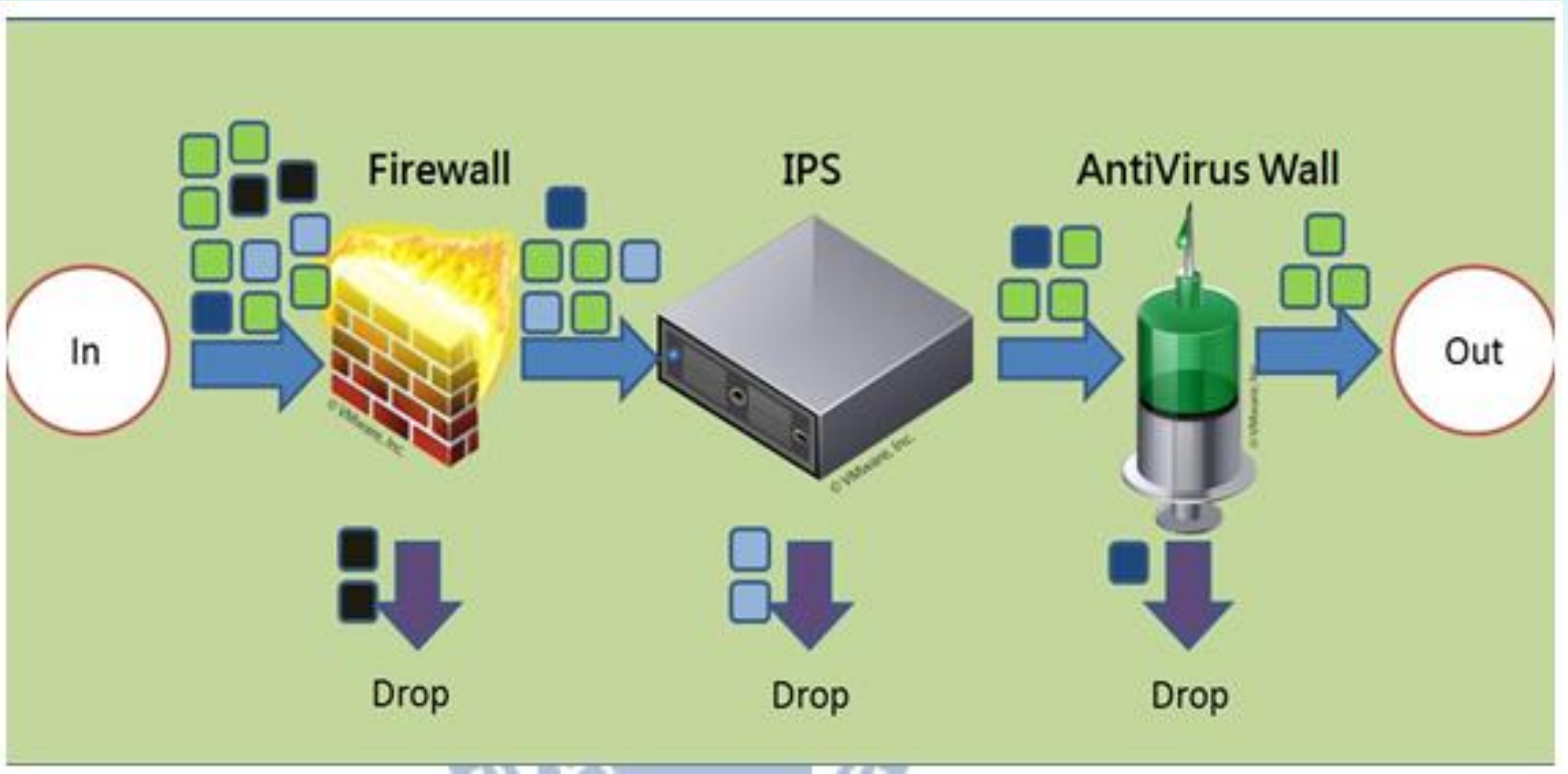
防病毒网关

使用基于Linux下的ClamAV 加上 HTTP
Anti-Virus Proxy(HAVP)做为病毒库服务器

虚拟化平台

基于Vmware虚拟化平台，搭建Linux操作系统

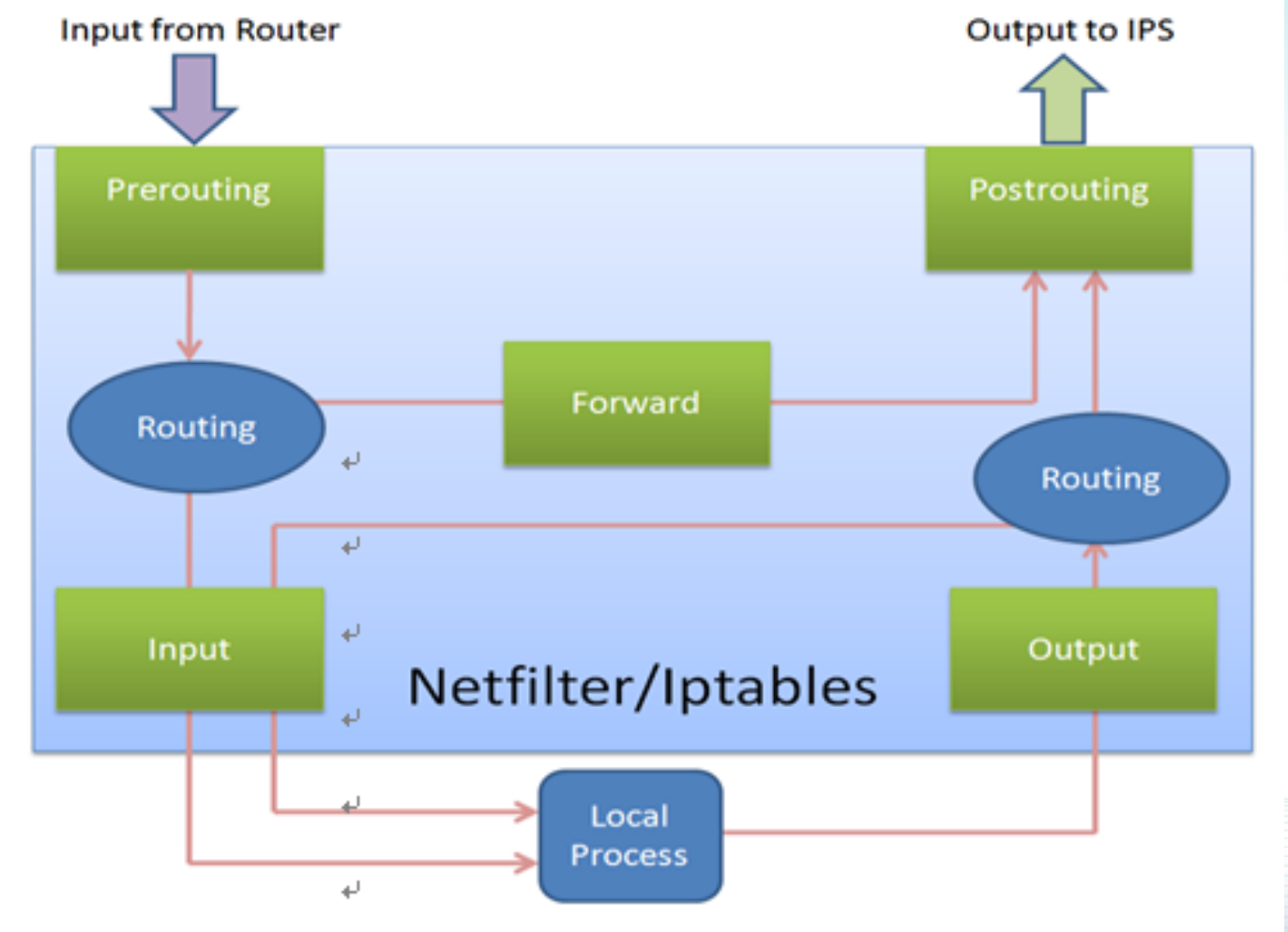
系统实现



虚拟化纵深防御网络封包流程

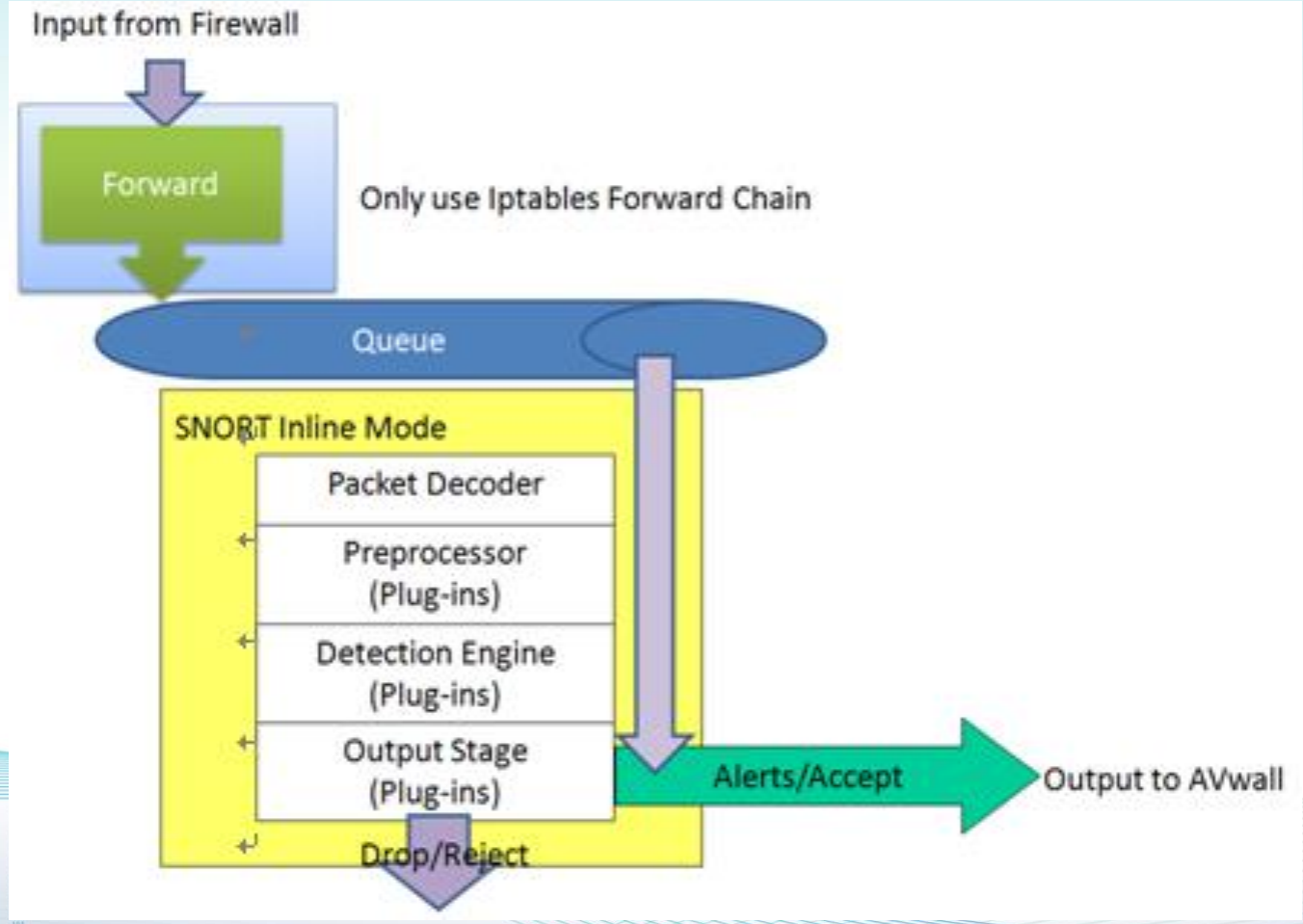
虚拟化网络安全纵深防御架构在安全模组中，本研究设计了三套针对不同防御性质的子功能模组，并且利用网络模组将其数据包传递路径定义清楚，主要分为：(1)管理模组。(2)网络模组。(3)安全模组

系统实现



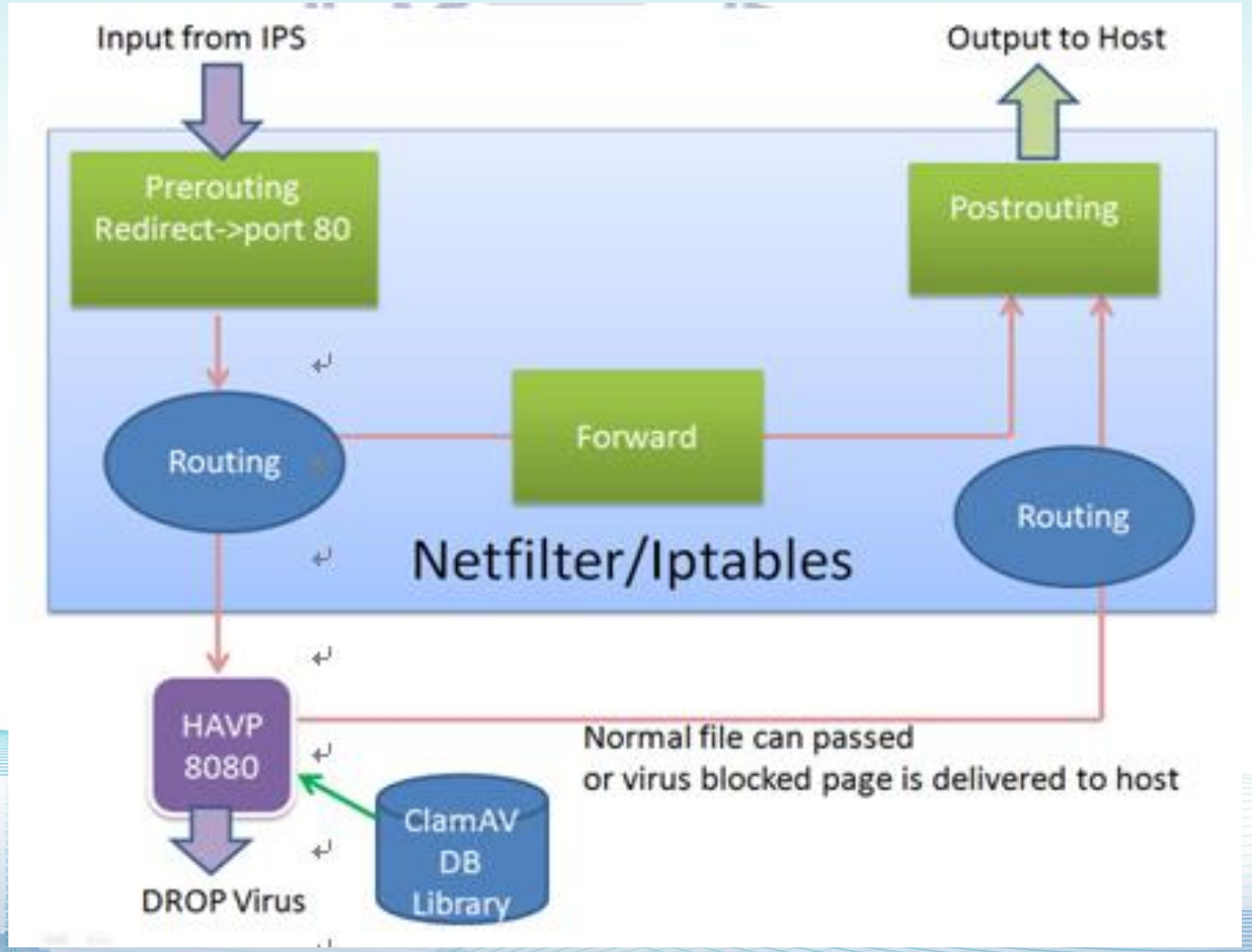
防火墙内部运行流程图

系统实现



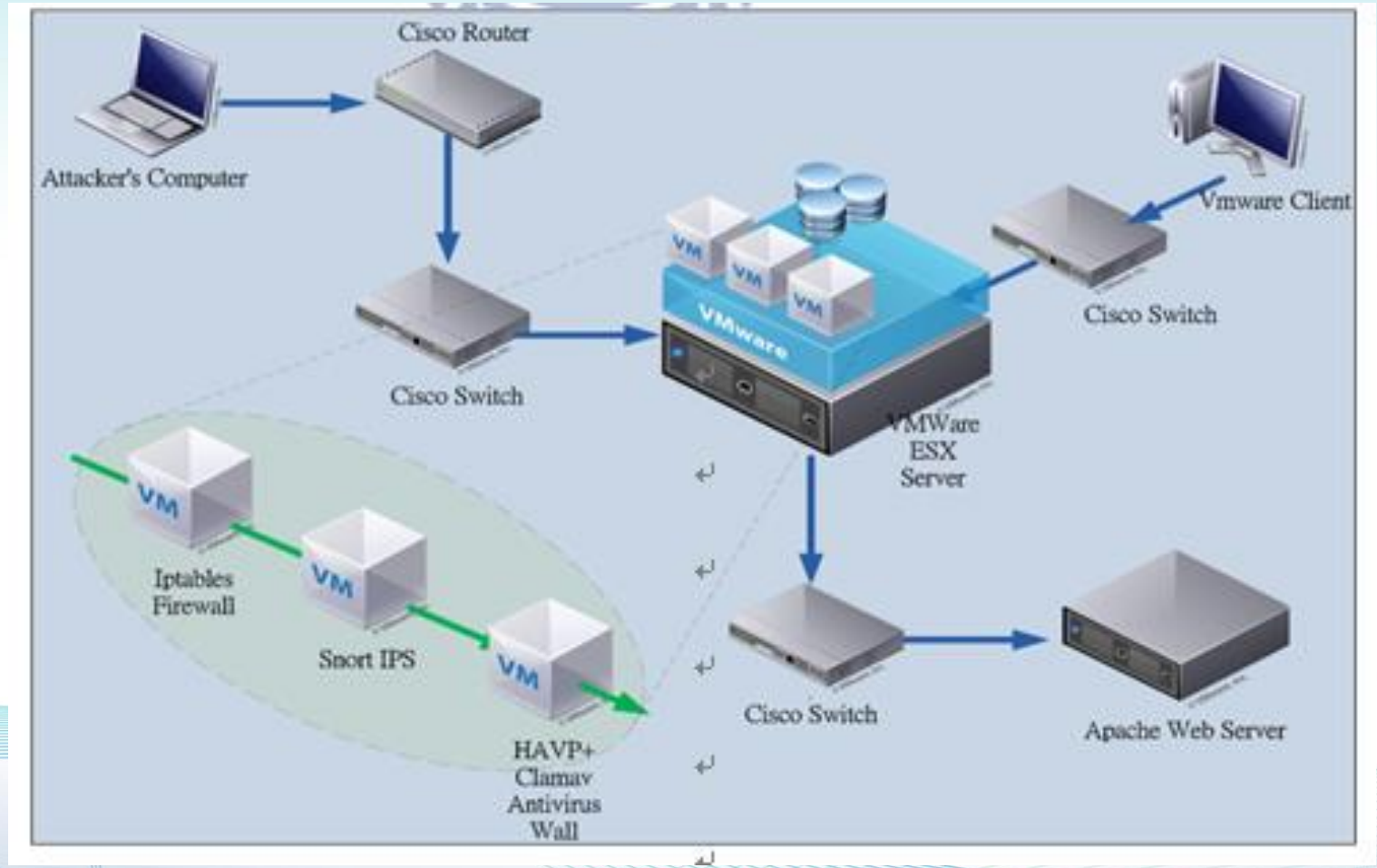
入侵防御系统内部运行流程图

系统实现



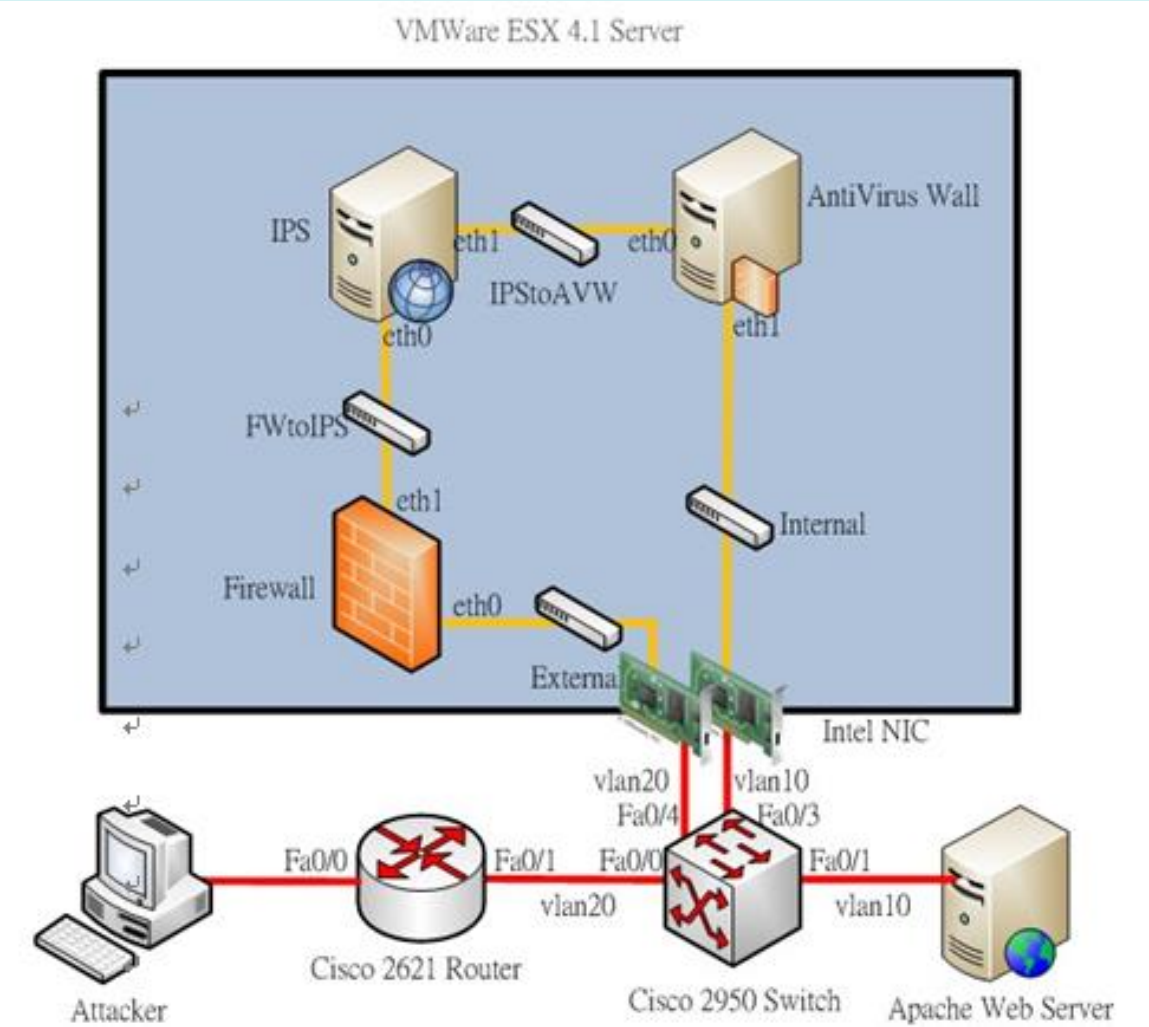
防毒墙内部运行流程图

系统实现



实验环境配置图

系统实现



虚拟化网络安全纵深防御网络架构示意图

性能分析

防火墙功能测试

使用Putty连接网页服务器器的Telnet端口

入侵检测功能测试

使用N-Stalke的网页测试工具对Snort进行触发警报测试

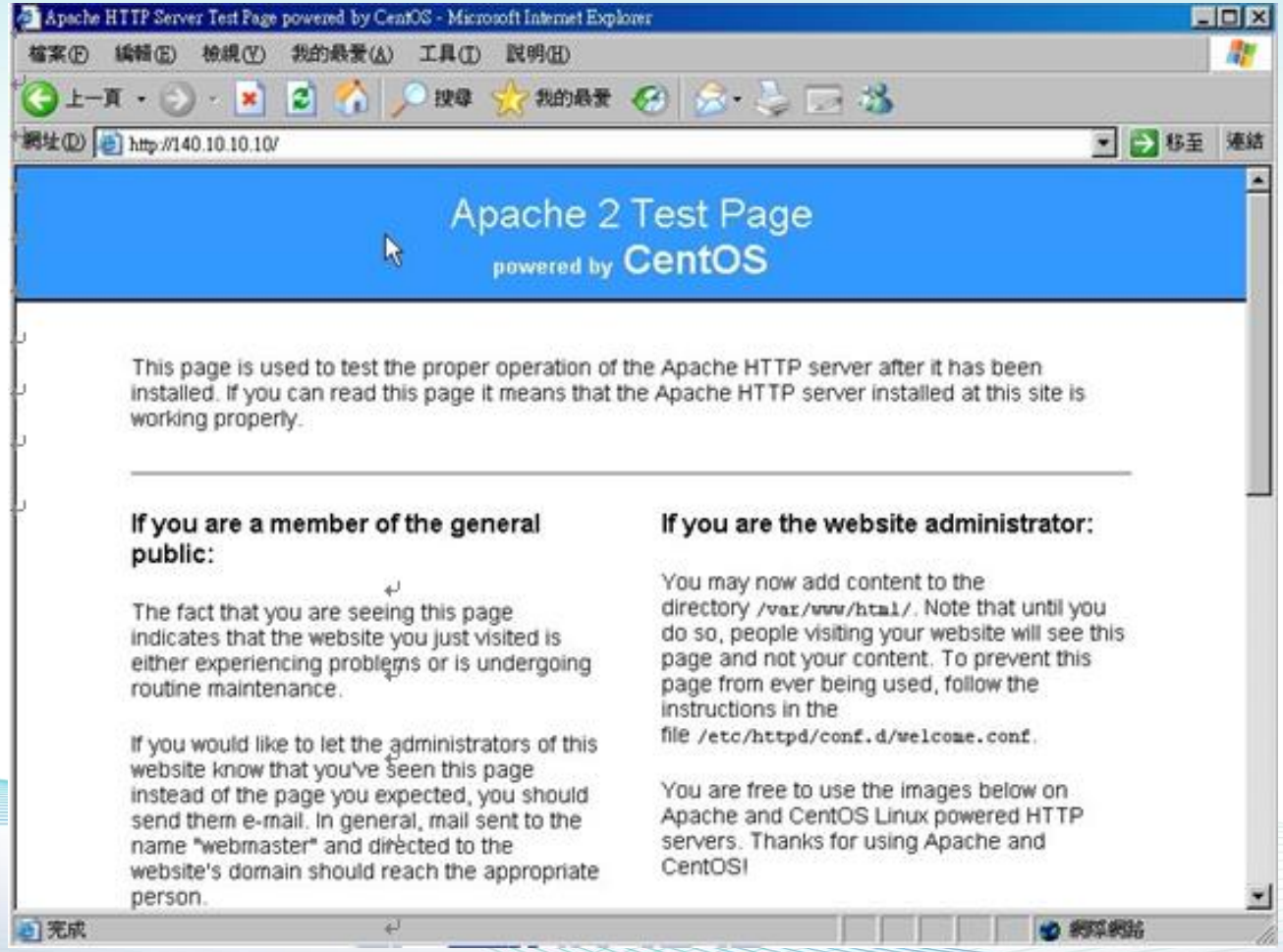
防病毒网关功能测试

从eicar网站上抓取病毒样本放置在攻击者的网页上，然后由内部网络连接下载，测试防病毒网关是否能正常工作

压力测试

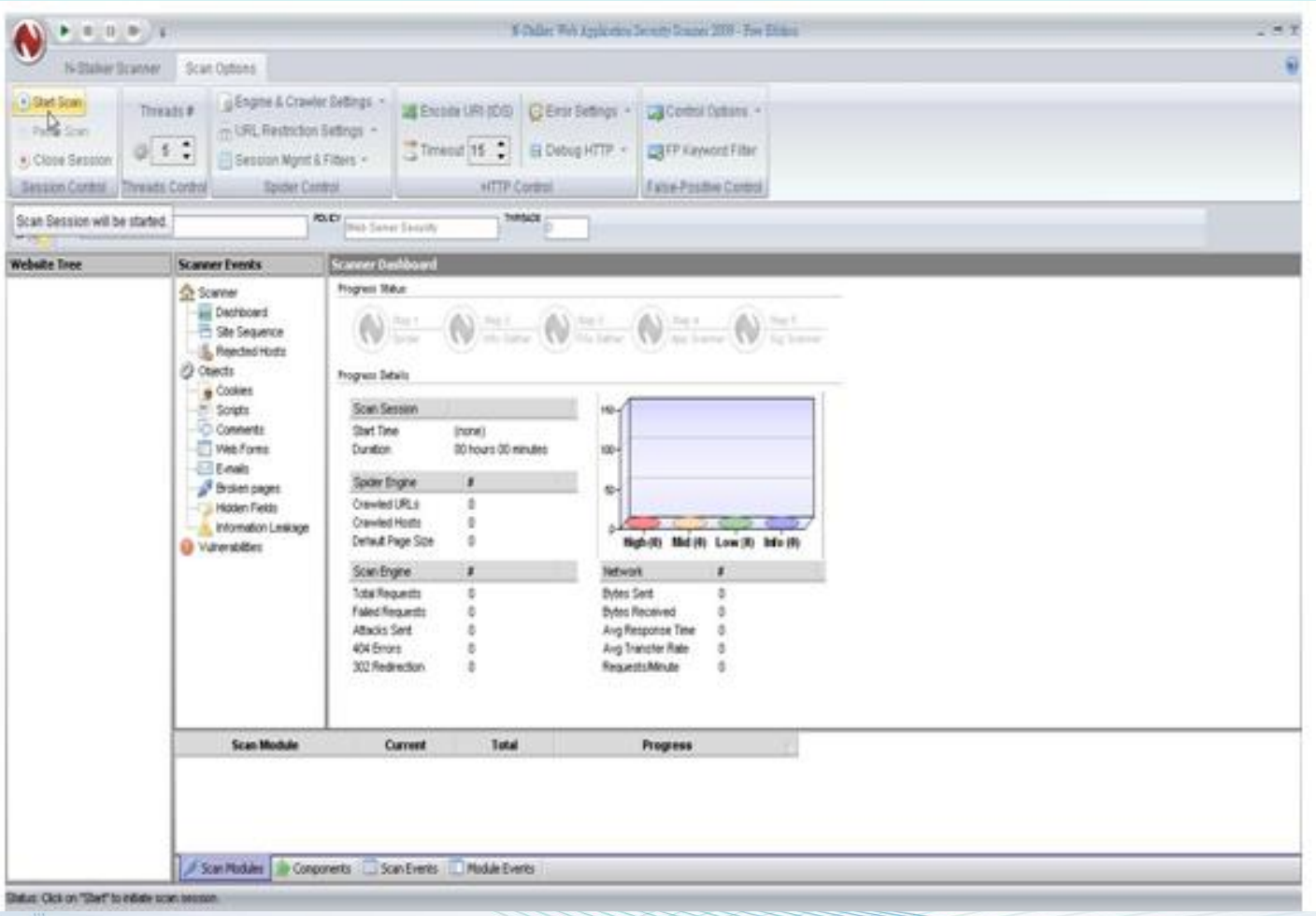
使用Iperf 和Httperf 进行压力测试

性能分析



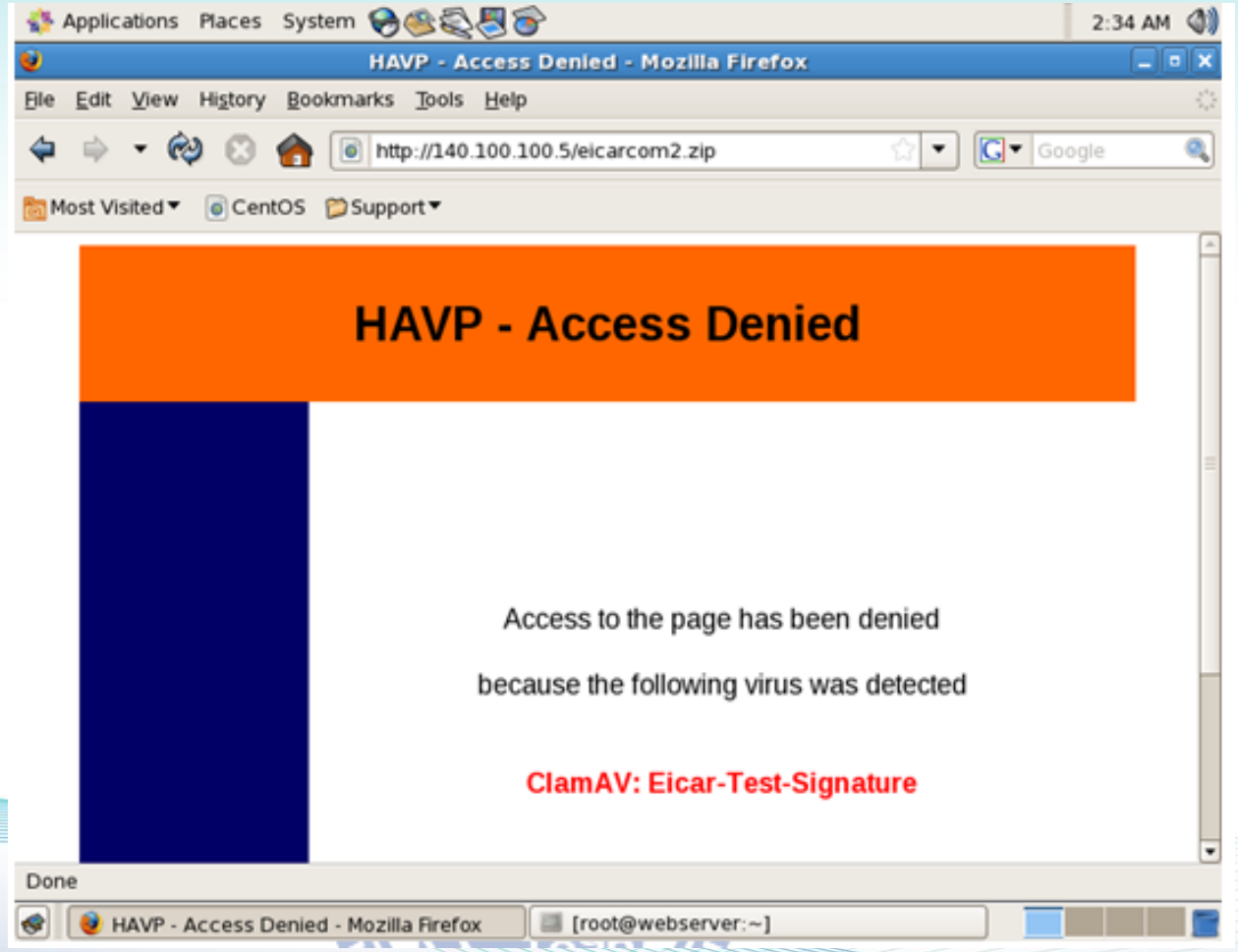
防火墙系统功能测试

性能分析



N-Stalker执行画面

性能分析



HAVP回应用户病毒被阻挡的信息页面

性能分析

本研究结合了网络安全纵深防御机制及虚拟化技术，可以有效降低营运成本以及减少运算资源的浪费，利用纵深防御的概念强化企业网络安全架构可提高安全性。基于开源软件的网络纵深防御系统，包括软件防火墙，入侵检测系统，防病毒网关等模块，通过此系统的应用可以满足小规模IDC机房或中小ISP对于网络安全防御的业务需求。

THANK YOU

谢　　谢　　观　　看