IDF互联网情报威慑防御实验室

虚拟网络安全实验室构建

张世会 @IDF实验室

你在使用哪些虚拟机？（1）

个人版：

- Vmware Workstation
- KVM

企业版：

- Vmware vSphere
- Ctrix
- Hyper-v

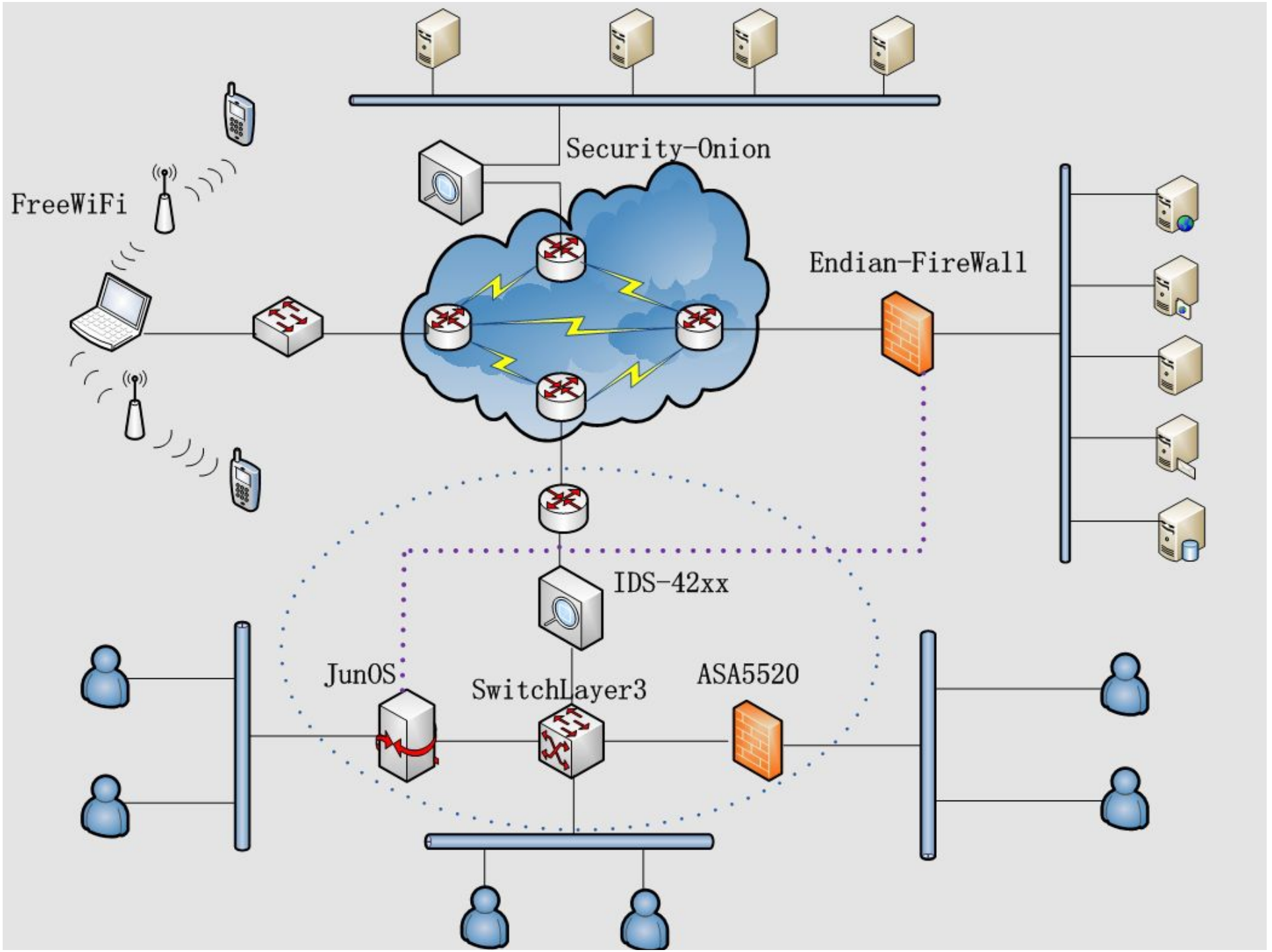
你在使用哪些虚拟机？（2）

开源：

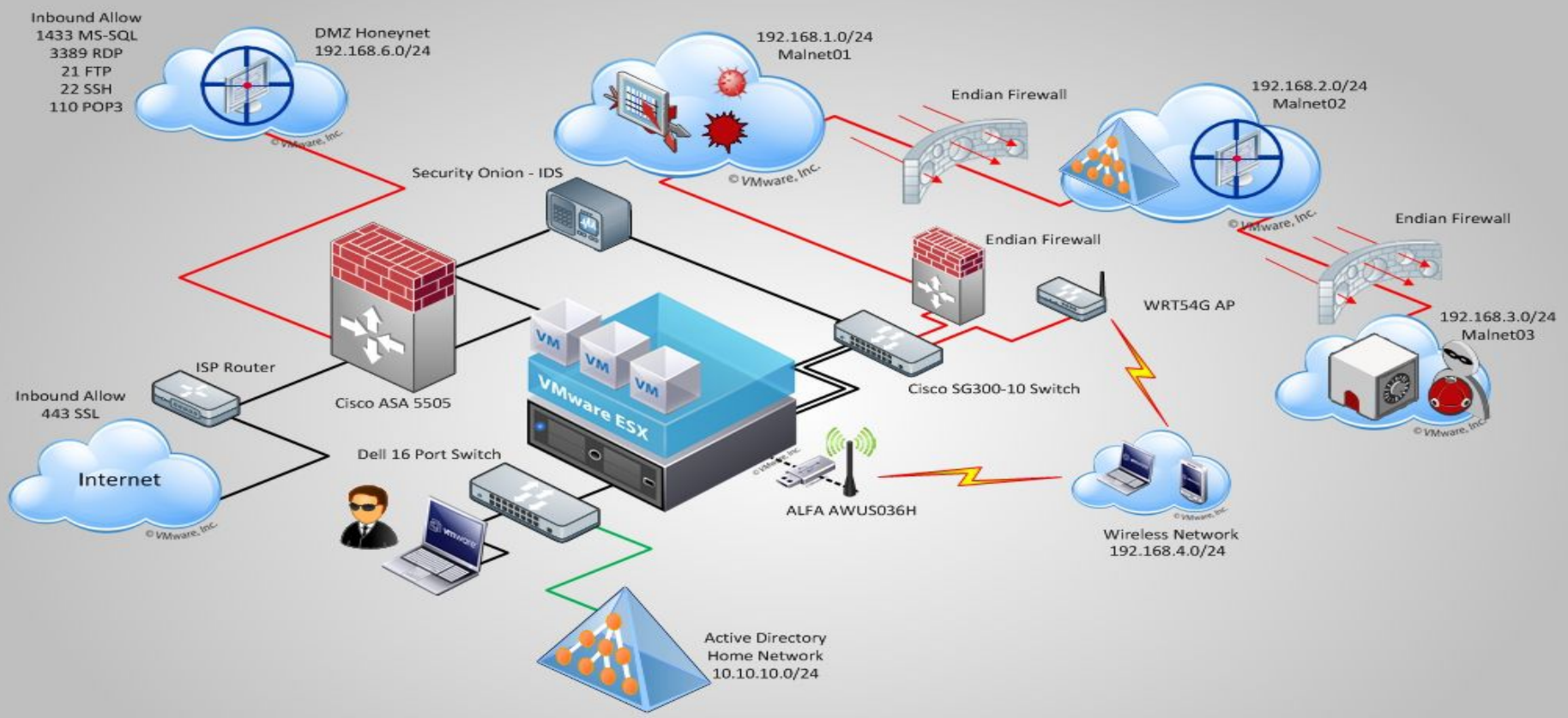
- VirtualBox
- Xen

云平台管理项目：

- Openstack/Cloudstack


Security-Onion
FreeWiFi
Endian-FireWall
IDS-42xx
JunOS
SwitchLayer3
ASA5520

参考 ESXi安全实验室：http://blog.idf.cn/2013/06/esxi-security-lab/



议题

一、Host环境

二、需要解决的一些问题（服务器单网卡）

- IP规划/路由
- 网络设备/镜像的选择

....

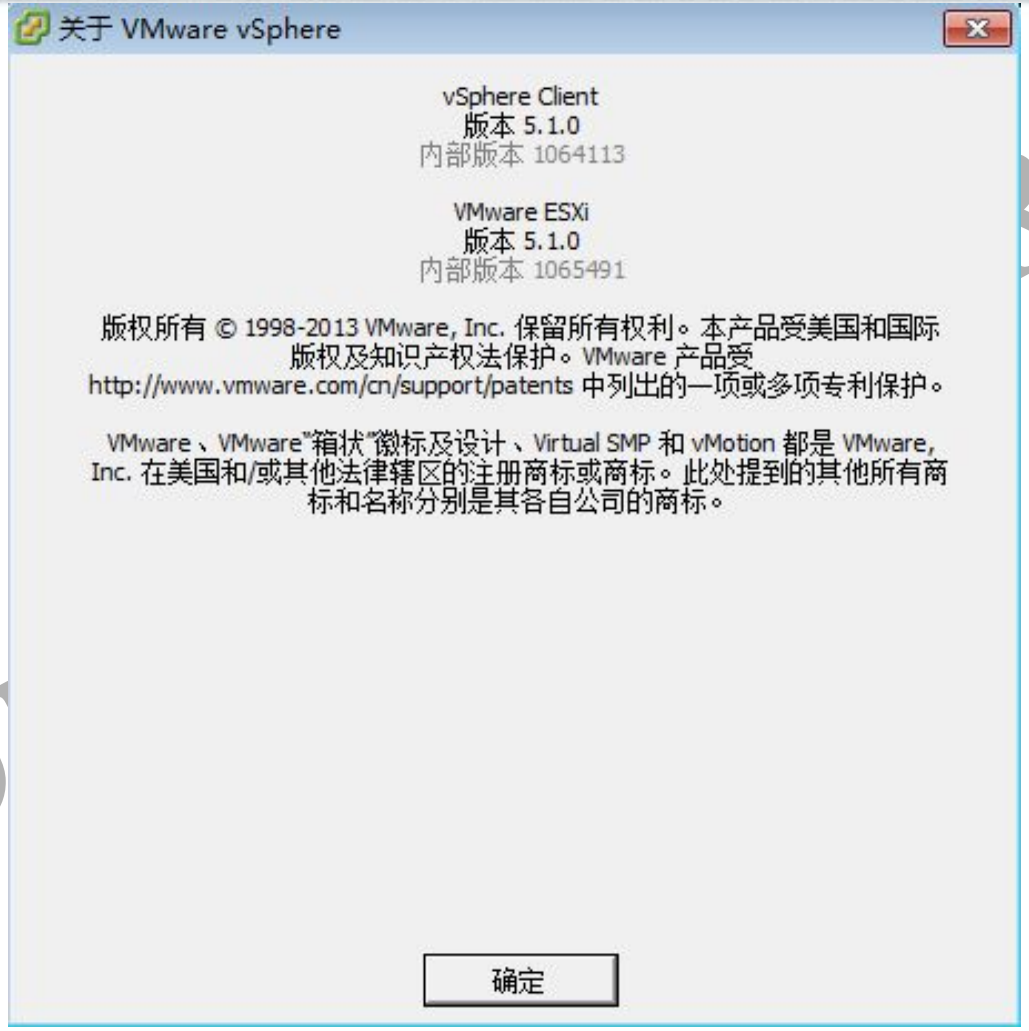
三、设备登录

四、小结、推荐资源

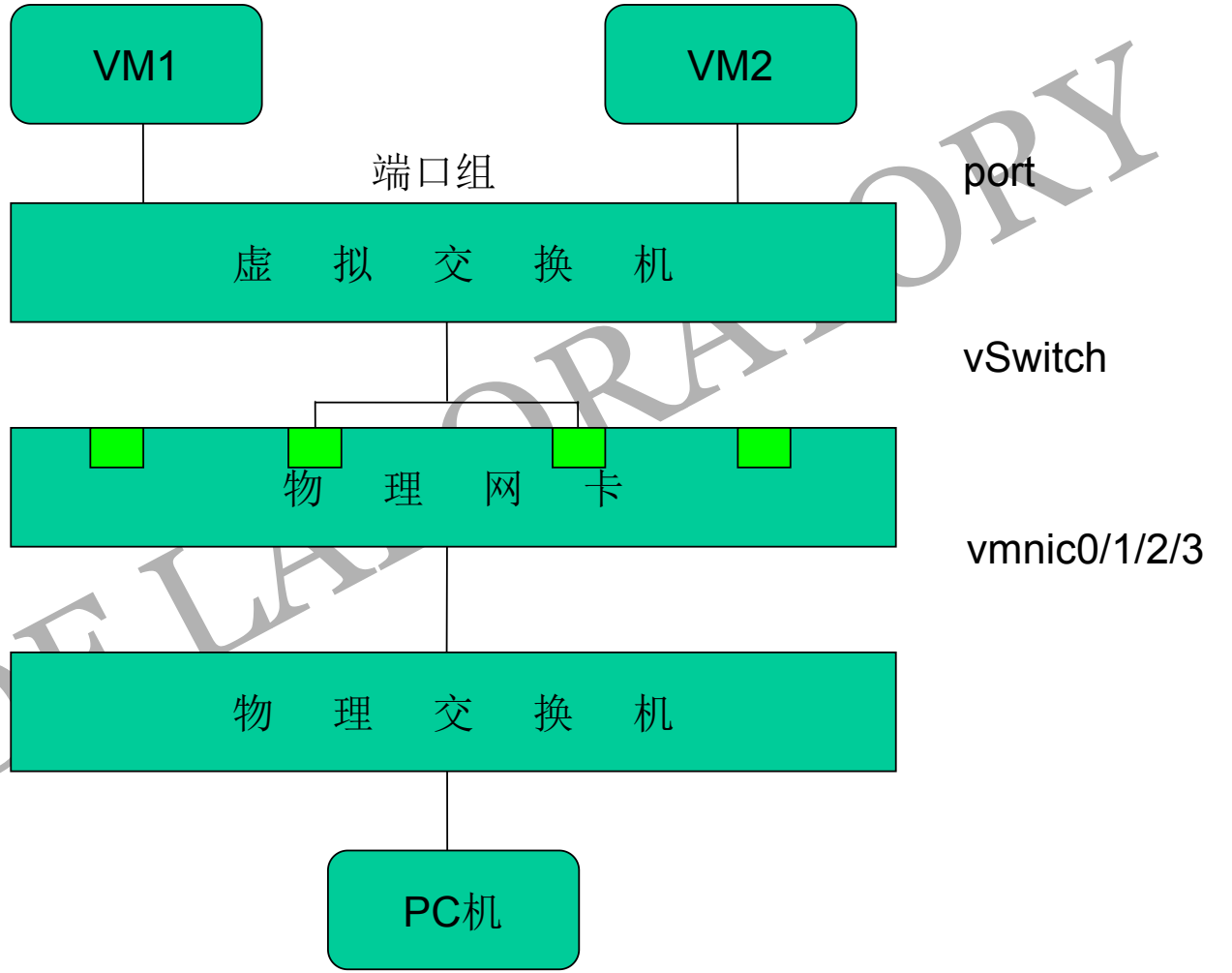
一、Host环境

- CPU：支持虚拟化
- 内存：至少4G
- 网卡：千兆

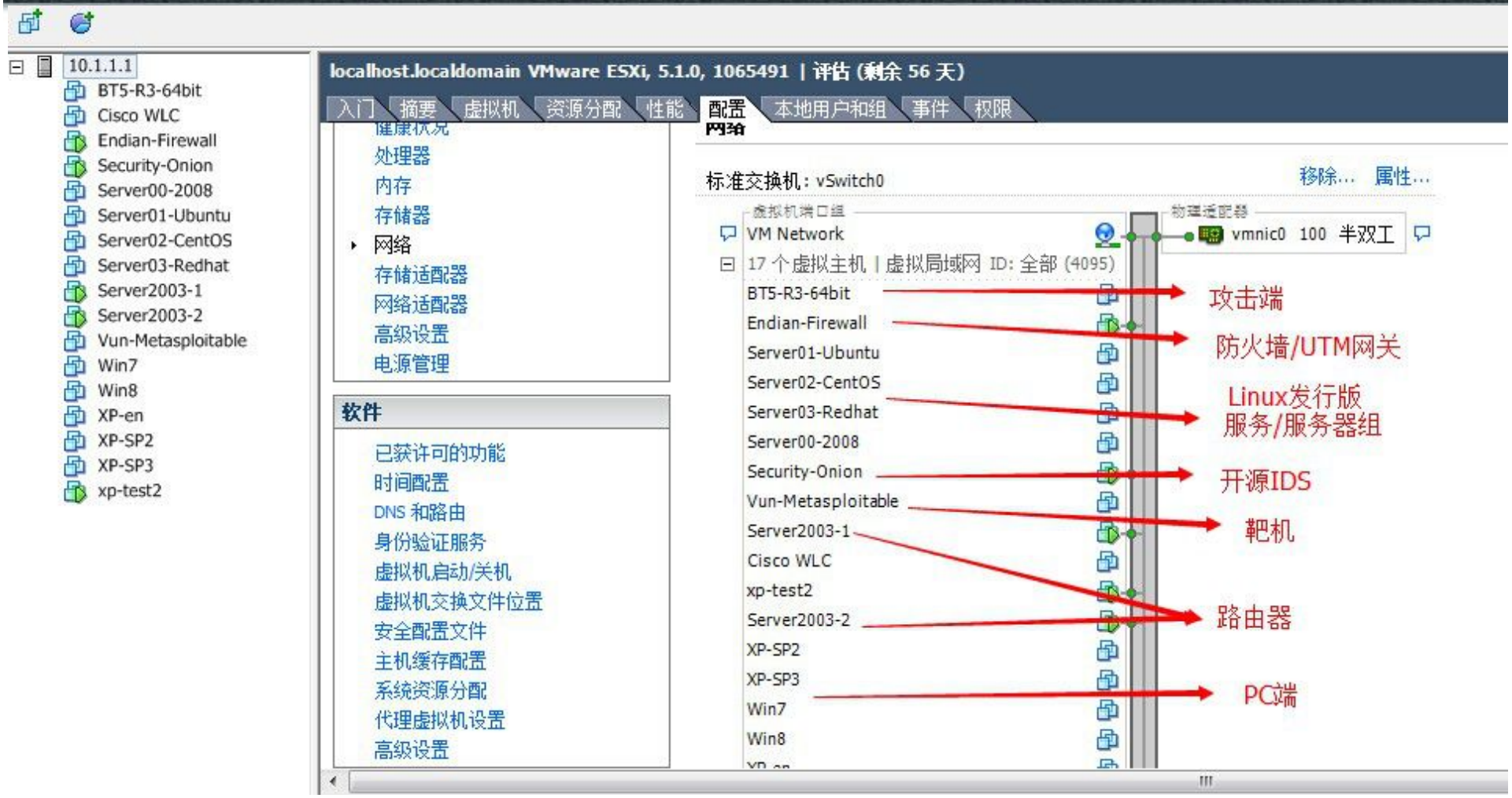
1，vSphere版本


关于 VMware vSphere
vSphere Client
版本 5.1.0
内部版本 1064113
VMware ESXi
版本 5.1.0
内部版本 1065491
版权所有 © 1998-2013 VMware, Inc. 保留所有权利。本产品受美国和国际版权及知识产权法保护。VMware 产品受 http://www.vmware.com/cn/support/patents 中列出的一项或多项专利保护。
VMware、VMware"箱状"徽标及设计、Virtual SMP 和 vMotion 都是 VMware, Inc. 在美国和/或其他法律辖区的注册商标或商标。此处提到的其他所有商标和名称分别是其各自公司的商标。
确定

2，vSwitch



3，设备清单


10.1.1.1
BT5-R3-64bit
Cisco WLC
Endian-Firewall
Security-Onion
Server00-2008
Server01-Ubuntu
Server02-CentOS
Server03-Redhat
Server2003-1
Server2003-2
Vun-Metasploitable
Win7
Win8
XP-en
XP-SP2
XP-SP3
xp-test2
localhost.localdomain VMware ESXi, 5.1.0, 1065491 | 评估 (剩余 56 天)
入门
摘要
虚拟机
资源分配
性能
配置
本地用户和组
事件
权限
处理器
内存
存储器
网络
存储适配器
网络适配器
高级设置
电源管理
软件
已获许可的功能
时间配置
DNS 和路由
身份验证服务
虚拟机启动/关机
虚拟机交换文件位置
安全配置文件
主机缓存配置
系统资源分配
代理虚拟机设置
高级设置
标准交换机：vSwitch0
移除...
属性...
VM Network
vmnic0 100 半双工
17 个虚拟主机 | 虚拟局域网 ID: 全部 (4095)
攻击端
防火墙/UTM网关
Linux发行版
服务/服务器组
开源IDS
靶机
路由器
PC端

二、需要解决的一些问题（1）

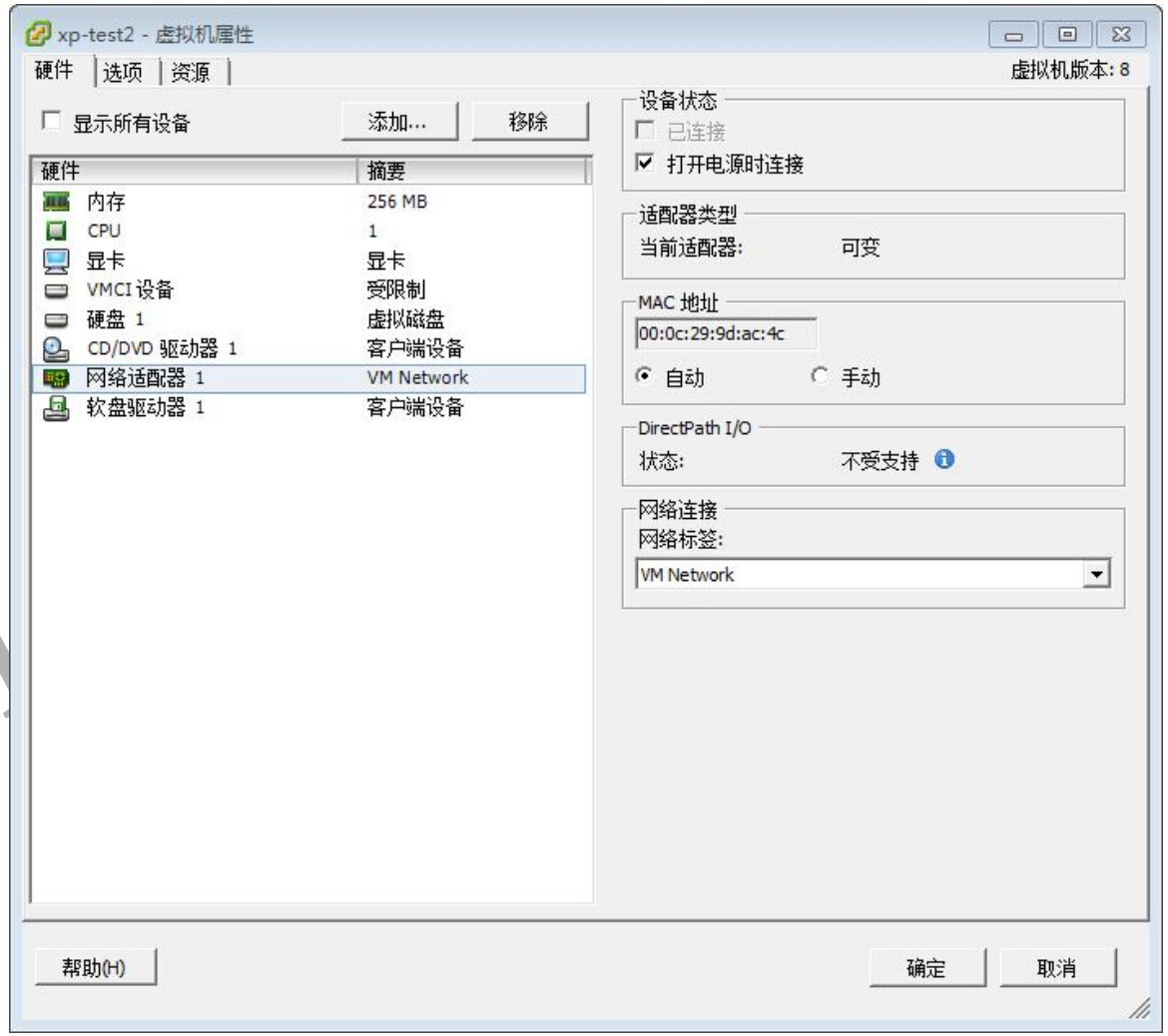
- IP/子网规划
- 路由（三层路由解决多个子网之间通信问题）

```
R1#show ip route
Gateway of last resort is not set
     34.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet1/0
C       12.12.12.0 is directly connected, Serial0/2
C       13.13.13.0 is directly connected, Serial0/3
C       14.14.14.0 is directly connected, Serial0/0
O       23.23.23.0 [110/128] via 13.13.13.3, 00:01:55, Serial0/3
O       34.34.34.0 [110/128] via 14.14.14.4, 00:01:52, Serial0/0
O       100.1.1.0 [110/65] via 12.12.12.2, 00:01:52, Serial0/2
O       200.1.1.0 [110/65] via 13.13.13.3, 00:01:54, Serial0/3
O       200.2.2.0 [110/65] via 14.14.14.4, 00:01:55, Serial0/0
C       1.1.1.1 is directly connected, Loopback0
O       2.2.2.2 [110/65] via 12.12.12.2, 00:01:52, Serial0/2
O       3.3.3.3 [110/65] via 13.13.13.3, 00:01:52, Serial0/3
O       4.4.4.4 [110/65] via 14.14.14.4, 00:01:52, Serial0/0
O       8.8.8.8 [110/65] via 14.14.14.4, 00:01:55, Serial0/0
```

需要解决的一些问题（2）

如何添加网卡

混杂模式



需要解决的一些问题（3）

- 镜像选择
- 设备激活：cisco 的ASA

三、设备登录

IOS
IDS/ASA
JunOS
Endian-FireWall
Security-Onion
Kali-MetaSploitable2
Linux发行版
Windows-xp、win7/win8、Server2003/2008/2012

1、创建一个虚拟机

- 使用客户端工具：vSphere-Client

- 创建虚拟主机的三种方法：
  1、创建新的虚拟机
  2、从VA Marketplace部署（联网）
  3、部署OVF模板

2、路由环境

- Cisco IOS（型号c3640/c3725）

  Router#show version

  Cisco IOS Software, 3600 Software (**C3640-JK9O3S-M**), Version 12.4(16a), RELEASE SOFTWARE (fc2)

- 宿主环境：server2003/ubuntu/centos（dynamips/qemu）
- 推荐GNS3
- 适用于单网卡服务器环境

3、入侵检测/防御设备

- IDS-42xx
- ASA5520：图形配置工具asdm
- JunOS

4、Snort/防火墙（1）

- Security-Onion

  Snorby：入侵检测

  sguil：安全日志分析前端

  squert

  ELSA

  Xplice

4、Snort/防火墙（2）

- Endian-Firewall

  防火墙

  IPS

  AV（FTP/HTTP/IMAP）

  反垃圾邮件

推荐资源：

- **UOS**
- **在线安全实验环境**

UOS优点：基于OpenStack，网络功能强大

缺点：不支持自定义镜像

https://www.ustack.com/

http://erange.heetian.com/

IDF实验室简介

- 全称**互联网情报威慑防御（之友）实验室**，是一个由信息安全从业人员、专家及信息安全爱好者组成的独立第三方民间机构。

- **发展历程**

  2004-2005年孕育于中国鹰派联盟网。

  2009年逐渐转为非营利组织（NGO）。

  2010年在北京组建实体机构。

- **使命愿景**

  普及信息安全知识、分析行业市场动态、评估安全行业产品

  致力安全人才培养、促进国际技术交流、推动黑客文化演绎

关注我们

- **IDF官网/论坛：**

  http://www.idf.cn

  http://bbs.idf.cn

- **邮箱联系：**

  idf.lab@gmail.com

- **关注微博**

  新浪微博：@IDF实验室

  腾讯微博：@NeteasyIDF