一、SDN&NFV

> 本文包括：
>
> 1、SDN
>
> 2、SDN 解决方案介绍
>
> 3、NFV
>
> 4、NFV 生态系统
>
> 5、NFV 关键能力

1、SDN

引言

1. 计算机从大型机到我们的家用电脑有共同的架构：
    - 专业硬件包含 CPU 主板，内存，硬盘等
    - 在硬件之上有操作系统，再有应用软件
    - 另一方面用 PC 生态系统作比较，支撑 PC 生态系统快速革新的三个因素是 Hardware、Substrate、硬件底层化

    > PC 工业已经找到了一个简单通用的硬件底层: x86 指令集、Software-definition

2. ICT 发展启示
    - 大型机、个人电脑、手机都采用三层架构 ---- **硬件、操作系统、应用软件。**
    - NICK认为网络生态效仿PC生态，采用三层架构，就可以蓬勃发展
    - 支撑 SDN 的关键是找到一个合适的 Hardware Substrate, 就有了 OpenFlow。
3. OpenFlow
    - OpenFlow描述了对网络设备的一种抽象，其基本编程载体是 flow, 定义 flow、操作 flow、缓存 flow 等，这个协议是网络世界的 flow 指令集。
    - flow 指令集可以作为硬件架构和软件定义的一个桥梁，协议本身可以不断演进，下层的硬件架构可以跟着持续演进，上层的网络软件可以保持兼容
4. IP 网络面临的问题
    - 唯一路径 网络利用率低，IP网络既聪明又笨重
    - 协议复杂 维护故障定位困难
    - 缺少全局视图 不能全局最优

SDN 介绍

1. SDN 核心思想
    - 控制和转发分离，软件应用灵活、可编程 ---- 这是源于 PC 和手机领域的变革
2. SDN 的价值
    - 技术驱动 网络架构的变革
    - 网络 构架构建一个集中的大脑，实现全局流量和整体最优 -关键价值 简化运维、自动化调度、提高网络利用率、网络开放
3. SDN 定义
    - Software define Network 即软件定义网络，由斯坦福大学 clean slate 研究组提出的，是一种新型网络创新架构。

- 核心技术：通过将**网络设备控制面与数据面分离开来**，从而实现了**网络流量的灵活控制**，为核心网络及应用的创新提供了良好的平台。
- 在网络中的表现：控制和转发是分开的，而且转发设备不再是专用设备。

4. SDN 网络与传统 IP 网络的区别？
   - SDN 利用控制转发相互分离从架构上解决根本问题：让网络敏捷起来，更快的部署新业务与快速定位故障点。采用资源集中和统一调度、能力开放的策略；让软件来干硬件的活；
5. SDN 的三个架构层
   - SDN 应用
   - SDN 控制器
   - 物理网络
6. NFV（Network Function Virtualization）：网络功能虚拟化，采用虚拟化技术，将传统电信设备的软件与硬件解耦，基于通用计算、存储、网络设备实现电信网络功能，提升管理和维护效率，增强系统灵活性
7. SDN 与 NFV 的本质区别与联系
   - SDN 的关键特征
     - 集中控制、优化全局效率
     - 开放接口、加快业务上线
     - 网络抽象、屏蔽底层差异
   - NFV 关键特征
     - 上层业务云化，底层硬件标准化
     - 分层运营加快业务上线与创新

2、SDN 解决方案介绍

DCI

- 什么是 DCI？
  - DCI：Data center interconnect， 指的是用于数据中心之间互联的网络，实现以数据中心为中心组网的基础承载网。
  - 未来超过 80% 的业务将部署在云上 我们云数据中心需要基于用户体验进行层次化布局，而网络则需要以数据中心为中心组网进行重构，在这样的大背景下，DCI 网络孕育而生。
- 为什么需要新建 DCI 网络？
  - 云数据中心的要求：高扩展性、低成本、资源丰富、温度适宜等条件，使得云数据中心建设位置要求
    - 比如：某运营商新建大型云数据中心与传统骨干网位置不重合
  - 云业务对网络要求
    - 云计算对时延有非常严格的要求，如跨 DC 同步计算、虚拟机热迁移等业务要求都在 10ms 以下
    - DC 间流量具有突发性和不均衡性，需采用 SDN 计数进行实时智能调控，而现有网络复杂。新技术难部署。------ 很难重用现有骨干网，需要新建 DCI 网络。
- 基于 SDN 的 DCI 方案总览
  - 顶层端到端协同，实现包含 DC 云与 DC 承载网的云网资源的一站式提供和端到端业务自动化协同发放。总的来说在多地区 多运营商部署多个数据中心的方式 目前已经成为了互联网行业普遍认可的最有效的解决用户覆盖提高用户业务体验的方案，建设并运营一张安全可靠、可灵活调度的多数据中心互联网络（DCI 网络），也成为了各大互联网公司在基础架构方面的工作之重，DCI 建成后 可以为宽带 4/3G 用户提供更好的访问体验外另一方面可以为互联网公司政府企业客户的云提供给更好的承载服务。
  - 现在 DCI 面临的实际问题：网络不灵活难以跟住业务快速迭代的步伐、链路利用率较低 以及居高不下的 OPEX 压力等。
  - 华为 SDN DCI 整体解决方案可以支撑云数据中心业务的端到端的运营，整体架构包括**承载层和控制层**，需要在网络基础承载层上引入部署 SDN 的控制层，控制层是网络的业务发放管理平台和网络智能控制中心，该层主要功能部件为：
    1. 业务发放平台：提供业务自动化入口实现租户业务自助发放以及网络资源状态的可视个运维管理入口
    2. 业务协同平台：DCI 业务需求分解和 DC 和 IDC 的协同实现端到端的跨控制器资源的协同和分解

3. 云平台：接受业务发放平台的业务分解，进行 DC 运业务分解和协同，实现 DC 的内存储、算和网络的协同
4. DC 控制器：接受 OpenStack 业务分解同一控制 DC 的 NVE 和 VxLAN GW 实现 DC 内网络自动部署和控制
5. DCI 控制器：接受业务协同平台资源的分解，实现 Underlay 网络部署的自动化和网络流量的智能优化
6. 流量采集工具、调优策略的输入、流量采集组件可以基于端口 TE 隧道进行流量采集和分析并提供网络流量可视化界面

- DCI 骨干网解决方案承载层是租户业务的承载实体，负责跨 DC 网络的连接以及业务宽带和 SLA 保证
- 骨干网支持 VxLAN 技术提供了大二层组网的能力，能够跨越广域网和多个物理 DC 构建 vDC 网络, 实现跨区域的资源节点的互备和虚机动态迁移，有效提升了 DC 云资源的利用效率
- 骨干网部署业界广泛使用的 MPLS TE 流量工程技术为租户业务提供端到端的宽带保证，提升了网络资源的利用效率，特别是提供了基于租户和业务的差异化的服务能力
- 网络承载支持采用 Overlay 技术，Overlay 业务网络基于云业务驱动支持快速的业务开通
- Underlay 物理网络按需提供网络资源，实现端到端的 SLA 保障和智能流量的优化
- 目前 IP Core 网络中存在如下一些流量调整需求：
  - 实现 IGW 出口、DC 出口的流量均衡
  - 降低不同 ISP 网间费用的结算，将流量分配到费用较低的链路上
  - 提升 VIP 用户体验
  - 针对这些需求，当前主要依赖于手工调整 BGP 路由策略 ：
    1. 监控链路带宽利用率
    2. 识别出需要调整的流
    3. 基于流制作 BGP 策略下发给设别
    4. 循环操作，直到流量符合期望目标的要求
- 智能流量调优方案：RR + 方案
  - 手工方法不能实时调整，耗时长、配置和维护复杂问题，RR + 方案用于解决这问题。
  - RR + 方案在 IP core 现网中加入 SDN Controller，实现集中控制，智能化调优
- RR + 可以带来什么？

1. 最大化 IGW 带宽利用率均衡链路间流量的分布，降低网间结算费用，不同客户提供不同 SLA 服务
2. 自动调整流量，取代复杂的手工操作
3. 基于标准 BGP 通讯，可以和现网设备平滑兼容。

PCE+方案

- 什么是 PCE + 方案
  - 路由转发用最短路径算法不考虑带宽，存在利用率低的问题， PCE + 正是为了解决这一问题而诞生的
  - PCE + 通过在网络中不部署 PCE server（就是 SDN Controller），使用 StatefulPCE 技术，为 MPLS TE LSP 集中算路。使网络带宽资源使用尽量达到最优。
  - 该架构方案中需要新部署的网元是 PCE Server，转发设备为 PCE Client。
  - PCE Client 需要计算 LSP 时会向 PCE Server 发出路径计算请求，server 计算后结果反馈给 client，client 然后进行 LSP 隧道建立。
- 思考：什么是 DCI? DCI 即 Data center interconnect 指的是用于数据中心之间互联的网络 DCI 网络正是实现 “以数据为中心的中心组网” 的基础承载网。

test

```
) SDN 云数据中心场景使用 VXLAN 作为转发隧道，对于 BUM 报文设备会向所有的 VXLAN 隧道泛洪。B

  A 对
  B 错

VXLAN 集中式网关适合大型的数据中心。B

  A 对
  B 错

VXLAN 隧道不支持跨数据中心建立。B
```

```
   A  对
   B  错

在 SDN 云网一体化场景中，AC 控制器通过什么协议和 OpenStack 的 Neutron 实现对接？B

   A  Netconf
   B  Restful
   C  SNMP
   D  OpenFlow

 在 SDN 云数据中心场景中，AC 控制器通过什么协议向 underlay 网络中的设备下发配置？A

   A  Netconf
   B  OpenFlow
   C  Restful
   D  SNMP
```

3、NFV

- CT 当前面临的结构性挑战
  - 增收方面：用户饱和，传统业务下滑
  - 节流方面：CT 投入成本下降，IT 部分的投入从 2002 年 6% 增加到 2013 年 13%，
  - 创新方面：CT 界 5 个/年， IT 界 160000 个/年 ，是32000 多倍
  - 商用速度：CT 每个月 6 个上市， IT 每小时 12 个
- 什么是 NFV?
  - NFV (Network Function Virtualization) 网络功能虚拟化，ETSI 组织下组建的。
  - NFV 是 IT 与 CT 结合的产物
  - 希望通过采用通用服务器、交换机和存储设备实现传统电信网络的功能。
  - 通过 IT 的虚拟化技术，许多类型的网络设备可以合并到工业界标准中，如 servers 、switchs 和 storages 。
  - 需要用软件实现网络功能并能在一系列工业标准服务器硬件上运行，可以根据需要迁移，实例化部署在网络的不同位置而不需要部署新设备
  - 关键诉求：需要大容量 Server 存储，大容量以太网，不同应用以软件形式远程自动部署在统一的基础设施上。
  - 三个关键点：软硬件解耦 开放 自动化
- NFV 将 IP 基因融入电信网络
  - 传统电信网软硬件绑定，更新困难，管理维护困难。
  - 采用虚拟化技术和云计算的网络，硬件采用标准的服务器、存储设备和交换机
  - 虚拟化之后 ，上层业务通过软件形式运行在统一的标准的硬件基础之上 。
  - 虚拟化后的网络好处：易于更新、硬件通用化 支持异构，资源归一 简化管理与运维
- NFV 正走向成熟
  - 2012年开始上升
  - 2013到2014年下降
  - 2015~2016 年稳步爬升 趋于成熟

4、NFV 生态系统

1. NNFV 生态系统：
   - ETSI 在 2012 年成立了 NFV ISG 来研究网络功能虚拟化
   - 随后，涌现了一批 NFV 的开源组织，比如 OPNFV，OpenStack
   - NFV 产业联盟，秉承开发、创新、协同、落地的宗旨，集多长家和合作伙伴进行联合创新，成为开放联盟的引领者。
2. NFV 框架
   - NFV 框架主要包括 3 大组件：NFVI、VNF、和 MANO 解释：
   - 框架中最底层的是硬件，包括计算、存储、和网络资源
   - 往上是云操作系统，完成虚拟化和云化的相关的功能，硬件和云操作系统成为 NFVI。I 指的是 instruction，设施的意思，这些设都是有 VIM 来管理。
   - 再往上是虚拟网网络功能，比如 vIMS 提供 IMS 的语音业务，vEPC 提供 4G 的数据网络功能。虚拟网络功能由 VNFM 来管理，提供 VNF 的生命周期管理。

- 再往上是网络管理层及网管，网管可以配套 NFVO 进行网络业务生命周期的管理

3. NFV 三大组件的关键要求

   - 组件 MANO：包括 NFVO、VNFM 和 VIM，
     - 要求 VNFM 适配不同厂商 NFVO 和 VIM；并且 MANO 系统应该尽量减少对现有的 OSS/BSS 的冲击。比如要求 MANO 支持和现有传统平台（如 U2000）的对接
   - 组件 VNF(虚拟化网络功能)：
     - 要求它可以运行在不同厂商的 NFVI；
     - 对应传统的电信业务网络，每个物理网元映射为一个虚拟网元 VNF。
   - 组件 NFVI - 云操作系统
     - 要求优选基于 OpenStack 的云操作系统
     - 将物理计算 / 存储 / 交换网络资源通过虚拟化计算转换为虚拟的计算 / 存储 / 交换资源池
   - 组件 NFVI - 硬件
     - 要求它优选具有虚拟化辅助功能的芯片的 COTS
     - 同时具备高 IOPS 与高可靠性的磁阵
     - 低 RAID 等级的磁阵建议冗余组网

5、NFV 关键能力

1. 开放 ---- 广泛兼容，性能稳定，支持异构；

   - 开放的能力是指虚拟化网络功能运行在多厂商云平台；
   - NFV 支持异构：在硬件基础上，可以支持厂商 B 的 VNFM 和厂商 A 的 NFVO，并且可以在和现网的传统平台如 U2000 OSS 进行异构系统的集成；
   - NFV 可以广泛兼容不同厂商的硬件以及云化的操作系统

2. 云化架构（虚拟化！= 云化）

   - 云化架构是弹性和可靠性的基础。
   - 传统平台软件和硬件是绑定的；
   - 虚拟化阶段：软件和硬件进行了解耦，软件可以运行在标准的硬件基础上，但是业务逻辑和业务数据还是绑定的
   - 云化架构阶段: 软件和硬件继续解耦，同时业务逻辑和业务数据进行解耦，会话转发层和业务逻辑进行解耦。
   - 业界主要厂商当前能力和华为当前能力区别：程序与数据分离，转发与数据分离；支持水平扩容，内存分布式数据。

3. 弹性

   - 分钟级的弹性扩容和秒级弹性缩容。
   - 当业务量需要增加的时候，由主 RDB 生成新的虚拟机来支持更多的业务处理，RDB 中就保留了动态数据（用户签约数据、链路局向配置数据、稳态呼叫会话数据），因此用动态数据可以生成新的 VM 来支持业务需要；
   - 当业务量下降时，将业务迁移到其他虚拟机，对相应的虚拟机设备下电，减少虚拟机设备的运行，而稳态话务可以立即在其他模块中重建。

4. 高可靠性

   - 应用层、云操作系统层、硬件层都有相应的冗余机制。
   - 应用层高可靠性可以通过主备和负荷分担方式实现主备 VM 之间的冗余。主备冗余与无状态N+M。确保应用层会话 0 中断，99.999% 的可用性。
   - 云操作系统的可靠性可以通过虚拟机快速重建冗余机制来实现。
   - 硬件层高可靠性主要通过族化以及物料冗余机制来实现计算、存储、网络等硬件设备的冗余
   - 硬件层、VM 层、业务层各层可靠性各自独立，高度互补确保整体可用性。

5. 高性能

   - NFV 业界最权威的评估公司 SPECvirt。华为的 FusionSphere 性能得分为 4.6，排第一。
   - 呼叫处理方面华为的 FusionSphere 比第二名的 Vmware 高 17%。
   - 高性能技术的关键技术：NUMA 亲和性、CPU 绑定、DPDK、透明巨页、虚拟中断优化等

6. NFV 存在的问题

   - （1）标准不成熟，技术架构实现上有分歧；
   - （2）多供应商、集成复杂。
   - （3）部件兼容性风险大,NFV 只定义架构，都是开源组织自行定制。
   - （4）NFV 工程难度大，多厂家多方面。
   - （5）网络功能虚拟化技术滞后
   - （6）虚拟化可靠性不足。传统电信要求 99.999% 可靠性，所以需要完善

test

```
NFV 即 Network Functions Virtualization（网络功能虚拟化），就是将传统的 CT 业务部署到云平台上（云平台是指将物理硬件虚拟化所形成的虚拟机平台，能够

   A 对
   B 错

VNF Descriptor (VNFD): 属于 TOSCA 标准的 YMAL 格式配置模板，主要描述了实例化一个 VNF 所需要的资源信息以及操作行为，主要用于 VNF 实例化以及生命周

   A 对
   B 错

 在 NFV 架构下，KVM 是基于 windows 内核特性，可借助于硬件辅助虚拟化技术，结合 Qemu 完成对 I/O 的模拟和操作，共同支撑多个 Guest OS 在同一套硬件上运

   A 对
   B 错

以下哪一项描述了 NFV 的本质？D

   A 性能更好，速度更快
   B 网络架构扁平化
   C 万物互联
   D 网络设备的 IT 化和云化

在 NFV 架构下，以下哪些是 IMS 切新平台及虚拟化的价值？BCD

   A 增加 IMS 系统新特性
   B 推动 TTM 大幅下降
   C 降低 CAPEX/OPEX
   D 提升网络灵活性和开放性
```

二、大数据与安全

> 本文包括：
>
> 1、大数据概述
>
> 2、电信大数据应用
>
> 3、安全
>
> 4、防火墙技术描述
>
> 5、信息安全框架
>
> 6、信息安全审计
>
> 7、信息安全标准
>
> 8、信息安全现状分析
>
> 9、信息安全发展趋势
>
> 10、云安全框架
>
> 11、网络安全攻防

1、大数据概述

- 大数据产生背景
  - 1996 年，SGI 公司首席科学家 John Mashey 第一次提出大数据的概念。

    - 2001 年，Gartner 分析师 Doug Laney 首先定义了大数据的三个维度：数据容量、速度和种类（3V）。
    - 业界把 3V 扩展到了 11V，但主要包括 Volume、Velocity、Variety、Value 等
- 大数据定义
    - 指无法在可承受的时间内用软硬件进行捕捉、管理和处理的数据集合，需要新处理模式才能使该数据集合成为具有更强的决策力、洞察力和流程优化等能力的海量、多样化的信息资产。
- 海量数据的来源
    - 海量数据的组成：由 25% 的结构化数据和 75% 的非结构和半结构化数据构成。
    - 数据类型分为：
        - 结构化数据：指可以存储在数据库里，可以用二维表结构来逻辑表达实现的数据。
        - 非结构化数据：不方便用数据库二维逻辑表来表现的数据，包括所有格式的办公文档，文本、图片，XML，HTML，各类报表图像和音频，视频信息等等
        - 半结构化数据：介于结构化数据和非结构化数据之间的数据。HTML 文档就属于半结构化数据。
- 大数据的价值
    - 对于企业组织，大数据在竞争能力构建、决策分析和成本控制等领域有广泛的应用前景；
    - 对于事业组织，大数据在科学探索、知识服务和社会安全等领域也有强烈的需求。
    - 例如：
        1. 在卫星测绘领域能海量存储数据。
        2. 在金融领域能盘活归档数据，深挖存量数据价值。
        3. 在能源勘探领域能进行潜力分析，降低的勘探成本。
        4. 在媒体娱乐中能进行高清制播
- 大数据基本特征（4V）
    - 量大（Volume）：存储大、计算量大
    - 样多（Variety）：来源多、格式多
    - 快速（Velocity）：处理快，生成速度快、处理速度要求快
    - 价值（Value）：价值第，价值密度的高低和数据总量的大小成反比，即有价值的数据比重小。
- 大数据带来的挑战：
    - 网络架构：传统网络架构支持南北向网络流量，不适配大数据应用对东西流量的需求。（从垂直访问到水平访问）
    - 数据中心：数据中心将面临巨大压力，同时访问子系统压力大。
    - 数据仓库：支持结构化数据，但不适应非结构化数据和半结构化数据在数据处理上的需求。
- 大数据与云计算的关系：
    - 云计算是底层平台，大数据是应用。
    - 云计算作为底层平台，整合了计算、存储、网络等资源。同时提供基础架构资源弹性伸缩能力。
    - 大数据在云计算平台的支撑下，调度下层资源进行数据源加载，计算和最终结构输出等动作。
- 如何面对大数据
    - 各类组织在管理方法、技术工具、基础架构、思维方式
    - 渴望变革
    - 主动挖掘数据价值

2、电信大数据应用

1. 大数据给电信行业的机会与挑战
    1. 电信行业生产圈的信息产业遇到了革命性的变化。运营商相关业务的发展更加依赖数据，如传统的语音 窄宽 带宽数据以及超宽带 数字经济等相关业务的数据数据量越来越大。
    2. OTT 虚拟运营商的介入。使得运营商竞争环境更加的复杂和激烈
    3. 客户消费模式的改变。需要大数据分析深入洞察用户的需求，进行定制化的服务，改善客户体验
    4. 提升精细化的管理水平。以数据为中心的运营支撑一体化、精细化成为必然趋势，数据将成为企业的核心资产。
2. 电信行业大数据典型商业需求
    - 大数据的总体目标是构建统一的数据采集与整合能力，大数据分析处理能力，计算及数据服务能力，大数据应用能力和互联网化的数据开放能力，支撑业务创新与商业成功。
        1. 延长用户生命周期 ---- 大数据建模支撑用户全生命周期的营销和维系
        2. 提升业务使用量 ---- 基于大数据的营销体系有效运作、支撑多批次、小群体、高成功率、多用户触点的营销

3. 对外价值变现 ---- 实现对外合作、MR 数字轨迹形成商业价值

3. 常见应用场景

    1. 潜在离网用户维挽场景
        - 通过大数据的用户管理，对潜在的离网用户进行数据分析。通过大数据实现用户管理、营销策划、营销实施和闭环反馈的拉通。
        - 当海量用户数据来了之后，用大数据平台对所有用户进行分类、识别和管理。
        - 用户识别之后，根据用户大数据分析结果触发营销策略。
        - 对用户在内部进行渠道选择，匹配相应的资源套餐，通过用户的选择来进行效果的反馈。
    2. 综合网管分析平台—基站关联分析场景
        - 根据离网用户的位置轨迹，用户的业务行为，基站地图以及基站网络质量 KPI 获得数据源，然后进行大数据的建模分析，判断离网用户是否与其常出没的基站存在关联，进而输出质差基站列表、基站供需平衡度、经常出没已识别质差以及基站的未离网用户列表。最后确定可服务的商用场景。
    3. 数据变现场景：户外数字媒体 / 非数字媒体价值评估场景
        - 户外媒体行业缺乏受众测量方法
        - 户外数字媒体 / 非数字媒体价值评估场景 ---- 需求分析、相关数据分析、广告屏分析得出结果输出
    4. 电信运营商大数据应用方向
        - 以前电信运营商的主要收入来源：语音、短信业务，现在：流量接入收入，未来：数字化服务收入时代
        - 需要建设大数据平台支撑：（1）自有业务收入提升（2）非通信价值变现，进而使运营商的业务数字化。

test

HDFS 的是基于流数据模式访问和处理超大文件的需求而开发的，具有高容错、高可靠性、高可扩展性、高吞吐率等特征，适合的读写任务是一次写入，多次读写。A

A 对
B 错

聚类是指将物理或抽象对象的集合分组成为由类似的对象组成的多个类的过程。A

A 对
B 错

下列选项中，哪一项属于大数据的核心？B

A 规模化
B 预测
C 匿名化
D 告知与许可

当前大数据技术的基础是由下列哪家公司提出的？C

A 阿里巴巴
B 微软
C 谷歌
D 百度

某超市研究销售纪录数据后发现，买啤酒的人很大概率也会购买尿布，这种情况属于数据挖掘的哪类问题？A

A 关联规则发现
B 分类
C 自然语言处理
D 聚类

3、安全

防火墙产品概述

- Eudemon8000E 防火墙产品介绍（一道门）
- Eudemon8000E 产品的硬件架构和单板类型
- 主流的产品信号

- X3
  - 直流电源机箱4U，交流电源机箱5U
  - 3*LPU 1~3槽位
  - 主控板在4 5 槽位，1:1备份方式
- X8
  - 8*LPU 1~8 槽位
  - 主控槽位9 10
  - SFU板在11槽位，可以看成3块SFU，2+1备份的方式工作
- X16
  - 16*LPU 板 1~16 槽位
  - MPU 主控板在 17 18 槽位， 1：1 备份方式
  - 4*SFU 板在 19~22 槽位， 3+1 备份方式，，正常4块同时工作，当一块坏了，其他3块接替它的业务

- Eudemon8000E 应用场景
  - 大型IDC出口
    - 可以保证高可靠性
    - 防火墙的分布式接口，可以适应扩容，适应组网情况
  - 可以用在高速的校园网边界
    - 不同的运营商，内部网络限流
    - 支持NAT，可以将私网地址转为公网地址
  - 政府机构

4、防火墙技术描述

- 防火墙技术
  - 报文过滤（包过滤）
  - 报文过滤：防火墙通过域来表示不同的网络，通过将接口加入域并在安全区域之间启动安全检查（称为**安全策略**），从而对流经不同安全区域的信息流进行安全过滤。
- 默认的四个安全区域：
  - 本地区域（Local）：100
  - 受信区 （Trust）：85
  - 非军事区 （DMZ）：50
  - 非受信区：5

> 数字为优先级，数值越大，级别越大

- 允许 Trust 到非 Trust 区域，但反过来需要定义严格的安全策略。
- 数据流方向定义：高优先级到低为出方向 低到高为入方向
- 包过滤：根据源 / 目的 IP 或 MAC 地址、协议、端口号、报文优先级、服务类型
- 动作：允许（Permit）与拒绝（Deny）
  - 进来的报文先匹配策略，进行动作，允许进入
  - 拒绝丢弃
- 为了提高效率，进行首包检查机制：对于一个数据流（源/目的IP 源/目的端口号 协议都相同的流）只对第一个报文进行检查不检查后续报文，后续报文不需要安全检查，可以直接通过防火墙
- 会话表机制：
  - 对源/目的 IP 地址，源/目的端口号，协议号进行记录 返回来的流量如果命中会话表记录，则不进行安全策略检查。
  - 如果外网主动请求访问内网，如果没有命中会话表则进行检查，不通过则不允许访问。
- ASPF（Application Specific Packet Filter）：基于状态的报文过滤
  - 引进原因：有些软件如 QQ、 FTP 服务器等，由于机制问题，客户端发起的端口号和服务器返回端口号不一致，如FTP 发起21号端口，返

回则20号端口。所以要用 ASPF
    - 解决措施：统计常用端口号
- 现网为了防止防火墙故障，一般会部署两个，一个备用。
    - 平时出入数据流通过主防火墙，主防火墙有会话表，但是备用防火墙没有会话表，
    - 如果主防火墙损坏，则没有数据流穿越备防火墙，但备防火墙没有会话表，所以会丢失数据流
    - 所以用 HRP（Huawei Redundancy Protocol）协议对会话表进行备份，主防火墙将会话表备份到备用防火墙。

test

公钥密码体制算法用一个密钥进行加密，而用另一个不同但是有关的密钥进行解密。A

A 对
B 错

在设计一个安全的网络系统时，应当具有以下哪些特点？BCD

A 保证网络在任何时刻都有很高的传输速度
B 保证合法访问者的访问和接受正常的服务
C 保护各种数据的机密
D 保护所有信息、数据及系统中各种程序的完整性和准确性

5、信息安全框架

信息与信息安全

- 信息：数据 / 信息流
- 信息安全：
    - 保密性（Confidentiality）：只有授权用户可以获取信息
    - 完整性（Integrity）：信息在输入和传输过程中不被非法授权、修改和破坏，保证数据的一致性。
    - 可用性（Availability）：保证合法用户对信息和资源的使用不会被不正当的拒绝。
    - 上述三个基本安全属性称为 CIA
- 安全漏洞的影响
    1. 声誉损失
    2. 财务损失
    3. 知识产权损失
    4. 失去客户的信任
    5. 业务中断
    6. 这所有最终会造成信誉损失。
- 信息安全
    - 信息安全是 “组织问题” 不是 “IT 问题”
    - 超过 70% 的威胁是内部
    - 超过 60% 的罪魁祸首是初次欺诈和讹骗活动。
    - 最大的风险和资产都是人。
    - 社会工程是重大威胁
- IATF——深度防御保障模型
    - IATF 阐述了系统工程、系统采购、风险管理、认证和鉴定、以及生命周期、支持等过程。
- 信息安全管理的作用
    - 技术措施需要配合正确的使用才能发挥作用。
    - 根本上说，信息安全是个管理的过程，而不是技术过程，技术不高但管理良好的系统远比技术高但管理混乱的系统安全。
    - 3分技术，7分管理
- 信息安全管理体系（ISMS）
    - 是一种常见的对组织信息安全进行全面、系统管理的方法。
    - ISMS 是由 ISO27000 定义的一种有关信息安全的管理体系，是一种典型的基于风险管理与过程方法的管理体系。

- ISMS 规定的四个必要活动，能确保 ISMS 进入良性循环，持续自我改进。
  - 周期性的风险评估
  - 内部审核
  - 有效性测量
  - 管理评审

6、信息安全审计

- 风险、信息安全风险的概念
  - 风险：指事态的概率及其结果的组合
  - 信息安全风险：指人为或自然的威胁，利用信息系统及其管理体系中存在的脆弱性导致安全事件的发送及其组织造成的影响。（例如：棱镜门事件）
- 风险的构成（5个方面）
  - 起源（威胁源）
  - 方式（威胁行为）
  - 途径（脆弱性）
  - 受体（资产）
  - 后果（影响）

> *威胁源 采取 威胁行为 利用 脆弱性 对 资产 造成 后果*

- 资产：任何对组织有价值的东西，是要保护的对象，以多种形式存在（多种分类方法）：
  - 物理：计算设备、网络设备和存储介质等
  - 逻辑：体系结构、通信协议、计算程序和数据文件等
  - 硬件和软件
  - 有形、无形：品牌、名誉等
  - 静态：设施、规程等，动态：人员和过程
  - 技术和管理等。
- 威胁：可能导致对系统或组织危害的不希望事故潜在起因
  - 是引起风险的外因。
  - 威胁源采取适当的威胁方式才可能引发风险。
  - 常见的威胁源：操作失误、滥用授权、行为抵赖、身份假冒、口令攻击、密钥分析、漏洞利用、拒绝服务、窃取数据、物理破坏、社会工程等。
- 脆弱性：可能被威胁所利用的资产或若干资产的薄弱环节
  - 是造成风险的内因。
  - 脆弱性本身不对资产构成危害，会被威胁源利用，从而对信息资产造成危害
  - 比如：系统程序代码缺陷、系统安全配置错误、系统操作流程有缺陷、维护人员安全意识不足。
- 可能性：某件事发生的机会
  - 代表威胁源利用脆弱性造成不良后果的机会
- 风险：威胁源采用某种威胁方式利用脆弱性造成不良后果的可能性
  - 即威胁源采取威胁方式利用脆弱性造成风险。
- 信息安全审计
  - 是依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。
  - 是揭示信息安全风险的最佳手段，改进信息安全现状的有效途径，满足信息安全合规要求的有效方式。

7、信息安全标准

- 大部分信息安全问题的发生原因：
  - 员工缺乏信心安全意识
  - 没有建立必要的信息安全管理机制
  - 没有严格执行信息安全管理制度
  - 缺乏必要的信息安全技术控制措施

- 标准和标准化相关的基本概念
- 标准：是为了在一定范围内获得的最佳秩序，经协商一致制定并由公认机构批准，共同使用和重复使用的规范性文件。
- 国际标准化组织（ISO）：是一个全球性的非政府性组织，是国际标准化领域中一个十分重要的组织。
- 国际标准：是指国际标准化组织或国际标准组织通过并公开发布的标准。
- 国家标准（GB）：是指国家标准机构通过并公开发布的标准。
- 信息安全标准体系
    - 是由信息安全领域内具有内在联系的标准组成的科学有机整体
    - 是编制信息安全标准制定 / 修订计划的重要依据。
- 我国信息安全标准体系（截图）
- 国际信息安全标准体系框架（截图）
    - 最著名的是信息安全管理体系标准：ISO 27000
    - 国际认可，广泛采用

8、信息安全现状分析

- 常见信息安全问题
    - 计算机病毒：编制者在计算机程序中插入的破化计算机功能或数据的代码，能影响计算机使用，能自我复制的一组计算机指令或程序代码。
    - 系统漏洞：应用软件或操作系统软件在逻辑设计上的错误或缺陷。
    - 黑客：热心于计算机技术、水平高超的闯入计算机系统或者网络系统者，热衷于从事恶意破解商业软件、恶意入侵别人网站等事务。
- 信息安全问题产生根源
    - 内因：信息系统本身存在脆弱性，主要在于过程复杂、结果复杂、应用复杂。
    - 外因：威胁与破坏，主要因为人为因素和环境因素。
- 信息安全发展阶段
    1. 通信安全：信息和保密性。诞生于 20 世纪 40~70 年代。
        - 核心思想是：通过密码技术解决通信保密，保证数据的保密性和完整性，主要关注传输过程中的数据保护。
        - 安全威胁：搭线窃听、密码学分析。
        - 安全措施：加密技术，如凯撒密码，对称密码，在古罗马就使用了
    2. 计算机安全：随着计算机的出现，安全就聚焦在如何保护计算安全。诞生于 20 世纪 70~90 年代。
        - 核心思想是：预防、检测和减小计算机系统（包括软件和硬件）执行未授权活动所造成的后果，主要关注与数据处理和存储时的数据保护。
        - 安全威胁：非法访问、恶意代码、脆弱口令等
        - 安全措施：通过操作系统的访问控制技术来防止非收取用户的访问。
    3. 信息系统安全：随着信息化的不断深入，互联网的出现需要用到信息系统，主要涉及到保密性、完整性、可用性等。诞生于 20 世纪 90 年代后。
        - 核心思想是：综合通信安全和计算机安全。重点在于保护比 “数据” 更精炼的 “信息”，确保信息在存储、处理和传输过程中免受偶然或恶意的非法泄密、转移或破化。
        - 安全威胁：网络入侵、病毒破化、信息对抗等。
        - 安全措施：防火墙、防病毒、漏洞扫描、入侵检测、PKI、VPN 等
    4. 信息安全保障：提升到一个可以可靠的、有利的保障企业安全运作、国家安全。
        - 核心思想是：信息安全从技术扩展到管理，从静态扩展到动态，通过技术、管理和工程等措施的综合融合，形成对信息、信息系统乃至业务使命的保障。
        - 安全威胁：黑客、恐怖分子、信息战、自然灾难、电力中断等
        - 安全措施：技术安全保障体系、安全管理体系、人员意识培训教育

9、信息安全发展趋势

- 云服务

    - 随着越来越多的企业和个人开始将自己的数据保存到云环境
    - 恶意分子当然也会找到利用漏洞攻击
- 勒索软件
    - 通过加密重要文件，使得数据无法被访问，直到支付赎金
    - 勒索软件带来的影响越来越大
- 钓鱼式攻击
    - 越来越复杂
    - 搭建足以以假乱真的信息和网站，或者装作看上去来自可信来源的通信，以获取用户数据
- 开源软件安全
    - 公众已知的安全隐患往往也能造成重大影响
- 物联网
    - 代表了另一种潜在的威胁
    - 敏感数据应该被加密，访问必须被加密、必须被监督

10、云安全框架

- 云安全与传统安全技术的关系
    - 云计算安全模式的划分与传统安全模式大体类似
    - 由于虚拟化的引入，需要纳入虚拟化的安全防护措施
    - 在基础层面上依然可依靠成熟的传统安全技术来提供安全防护
- 云安全主要聚焦于：
    1. 应用安全：
        - 应用安全架构
        - 软件开发生命周期；
        - 工具和服务；
        - 合规性；
        - 脆弱性
    2. 加密和密钥
        - 管理云用户和提供商需要避免数据丢失和被窃。
        - 加密提供了资源保护功能，同时密钥管理则提供了对受保护资源的访问控制。
        - 加密及秘钥管理是云计算系统保护数据的核心机制。
        - 加密和密钥管理聚焦在加密的机密性、完整性以及密钥管理
    3. 身份和访问管理
        - 管理身份和访问应用程序的控制仍然是当今的 IT 面临的最大挑战之一。
        - 从长远来说延伸企业身份管理服务到云计算确是实现按需计算服务战略的先导。
        - 安全有效的云身份和访问管理是企业部署云计算体系的前提。
        - 身份和访问管理聚焦在身份供应和取消供应、认证联盟、授权和用户配置文件管理。
        - 合规是整个过程的关键考虑因素
    4. 虚拟化
        - 虚拟化在云计算的应用中，提供了整个云计算平台。
        - 特别关注与系统和硬件虚拟化相关的安全问题
        - 聚焦于虚拟机管理程序
- 业务连续性和灾难恢复
    - 传统的物理安全、业务连续性计划（BCP）和灾难恢复（DR）等形式的专业知识与云计算仍然有紧密关系。

11、网络安全攻防

- OSI 安全体系结构

1. OSI 安全体系结构定义了系统应当提供的五类安全服务，以及提供这些服务的八类安全机制；
2. 五类安全服务是：鉴别、访问控制、数据机密性、数据完整性和抗抵赖性
3. 八类安全机制分别包括：加密、数字签名、访问控制、数据完整性、鉴别、流量填充、路由控制和公证。
4. 安全服务和安全机制的关系：某种安全机制可以提供一种或多种安全服务

- 网络协议安全问题

1. 网络接口层安全问题常见的有：自然灾害、误操作、传输线路电磁泄露、ARP 欺骗等；
2. 网络互连层安全问题常见的有：分片攻击、IP 地址欺骗、窃听和 IP 数据包伪造
3. 传输层安全问题常见的有：SYN 洪水攻击、TCP 会话劫持、数据包伪造等
4. 应用层安全问题常见的有：跨站点脚本、钓鱼攻击、数据泄露等

- 无线局域网安全问题

  - 安全问题：传输信道开放、容易接入、开放式认证系统、易于伪造的 SID、无保护任意接入
  - 认证机制：开放式认证系统、共享密钥认证（使用 WAP 进行保护，手动管理密钥存在重大隐患）

- 网络安全设备—防火墙

  - 防火墙是位于多个网络间，实施网络之间访问控制的一组组件集合
  - 防火墙作用：
    - 能在网络连接点上建立一个安全控制点，对进出网络数据进行限制，将需要保护的网络与不可信任的网络进行隔离，隐藏信息，并对进出进行安全防护，以及对进出数据进行安全检查、记录相关信息。
  - 防火墙的局限性：只实现了粗粒度的访问控制，不能防范病毒

- 网络安全设备——入侵检测系统

  - 作用：启示防火墙重要补充，构建网络安全防御体系重要环节，能够克服传统网络防御体系的限制。
  - 功能：
    - 检测并分析用户系统活动
    - 检测系统配置和漏洞
    - 对操作系统进行日志管理
    - 并识别违反安全策略的用户活动
    - 针对已发现的攻击行为作出适当的反应。
  - 局限性：配置操作和管理使用较为复杂，高虚报警域。

- 网络架构安全

  - 网络架构安全核心是保护网络和基础设施
  - 核心目的是通过增加系统的防御屏障或将各层之间的漏洞错开的方式防范差错发生，实现深度防御。
  - 即通过设置多次层次的安全防护系统而构成多道防线，即使某一防线失效也能被其他防线弥补或纠正。
  - 网络架构安全设计聚焦：在合理规划网络安全区域、规划 IP 地址和 VLAN 设计、安全配置路由以及交换设备、网络边界访问控制策略、安全冗余配置等

test

防火墙用于域间的通信报文安全过滤，对于防火墙不同端口之间，但属于一个域内的报文通信，防火墙不进行过滤。A

A 对
B 错

防火墙默认有 4 个安全区域，安全域优先级从高到低的是下面哪个？A

A Local、Trust、DMZ、Untrust
B Local、DMZ、Trust、Untrust
C Trust、Local、DMZ、Untrust
D Trust、Untrust、Local、DMZ

针对防火墙的安全功能描述正确的有哪些？BCD

A 防火墙默认域间缺省包过滤是 permit 的
B 要求域间配置严格的安全策略
C 一般将内网放入 Trust 域，服务器放入 DMZ 域，外网放入 Untrust 域
D 防火墙可以划分不同级别的安全策略，优先级从 1-100