1安全产品

01防火墙产品描述

1. Eudemon8000E防火墙产品介绍

华为提出的，电信级防火墙设备。目前主流的Eudemon8000E设备形态主要有Eudemon8000E\_X3\Eudemon8000E\_X8\Eudemon8000E\_X16

Eudemon8000E\_X16设备支持16块LPU板-业务处理板，分布在1-16号槽位；17、18是主控板槽位，主控板是以1比1备份的方式，主用主控故障了启动备用主控；19-22是SFU板-交换网板，以3+1的方式备份，正常下四块同时工作，一个故障，其他三个替代。

Eudemon8000E\_X8设备支持8块LPU板-业务处理板，分布在1-8号槽位；9和10槽位是主控板槽位（SRU）是以1比1备份的方式工作的；11槽位是SFU板，由于X8设备的主控板同时集成了交换网板的功能，因此也可以看做是3块sfu板，以2+1备份的方式工作。

Eudemon8000E\_X3设备，直流电源机箱高4U，交流电源机箱高5U，三种设备都支持直流和交流电源。X3支持3块LPU板-业务处理板，分布在1-3号槽位；4、5MPU-主控板，1比1备份的方式，没有交换网板，他的3块LPU板是以全连接的方式来进行报文和数据的转发。

1. 应用场景
2. 大型IDC中心出口，Eudemon8000E产品的双机热备（？？？）的特性以及可靠性。防火墙设备的分布式接口可以根据业务的扩容来实现板卡的扩展适应组网的情况
3. 高速的校园网的网络边界，可以实现内部用户通过不同的运营商访问不同的网络，可以对内部用户进行限流，防火墙设备支持NET，可以借助端口将多个私网的IP地址转化为有限的公网地址；
4. 政府或大型企业的网络边界，可以提供政府或大型企业分支机构的灵活接入，可以通过配置多种参数例如IP地址、端口号，通过配置策略实现总部内部资源的访问控制。

02防火墙技术描述

1. 功能：攻击防范、报文过滤
2. 如何实现报文过滤：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。

防火墙安全区域：（1）本地区域（Local）100-优先级，最高；（2）受信区85；（3）非军事区（DMZ）50；非受信区（Untrust）5；

1. 如何配置防火墙策略

(1)数据流方向：低优先级区域到高优先级区域的入方向；高优先级区域到低优先级区域称为出方向；

(2) 报文区分（源、目的IP地址；源、目的MAC地址、协议、端口号、报文优先级、服务类型）对应的处理方式只有Permit和Deny（允许和不允许）

(3)对于进来的报文首先匹配报文的策略，是否允许；

(4)为了提高报文转发效率---首包检查机制，对一个数据流只对第一个包进行安全检查。

从untrust到trust需要定义一个严格的安全策略

(5)会话表机制。对内网用户发起一个数据包访问某公网的服务器，防火墙会对数据包进行策略检查，记录数据包的源IP、目的IP、源端口号、目的端口号、协议号。

从外网服务器返回后，对已有的会话进行匹配，若返回流量命中了会话表不进行安全策略检查直接返回内网；但是外网服务器或用户主动发起访问内网用户的时候，若没有会话表，安全策略检测不通过，是不允许发送数据包到内网，访问内网的。

QQ和FTP服务器，客户端发起所使用的端口号和服务器回应所使用的端口号是不一样的 。FTP客户端发起使用的是21号端口，服务器吧数据流发给客户端用的是20号端口，如果防火墙没有20号端口对应的会话表，服务器是没办法发送的。，就需要借助ASPF机制。

ASPF（Application Specific Packer Filter：基于状态的报文过滤），对常用的端口号进行统计。

(6)为了防止现网防火墙故障会布置两台防火墙，采用一主一备的方式。

备用的防火墙是不能通过安全策略检查的，就需要一个备份的协议，HRP（Huawei Redundancy Protocol）是承载在VGMP报文上进行传输的，用于在主用设备和备用设备之间备份关键配置命令和会话表状态信息。

2信息安全

01 信息安全框架

1. 信息与信息安全

信息：数据、信息流

信息安全包括（CIA）：保密性（Confidentiality）----只有授权用户可以获取信息

完整性（Integrity）----输入和传输过程中 数据一致性

可用性（Availability）----保证合法用户对信息资源的使用不会被不正当的拒绝。

1. 安全漏洞的危害

信息作为一种资源，具有普遍性、共享性、增值性、可处理性和多效应性。

安全漏洞会导致：声誉损失、财务损失、知识产权损失、失去客户的信任、业务中断、信誉损失

信息安全是“组织问题”而不是“IT问题”；超过70%的威胁是内部；最大风险和最大资产都是人；社会工程师重大威胁；

1. 信息保障技术框架（IATF）

代表理论为深度防御，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。

1. 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。

从根本上说，信息安全是个管理过程，而不是技术过程；

技术不高但管理良好的系统远比技术高超但管理混乱的系统安全；

3分技术，7分管理；

1. 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。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和过程方法的管理体系。四个必要活动：风险评估、内部审核、有效性测量、管理评审。

02信息安全审计

1. 风险、信息安全风险的概念

风险指时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生及其对组织造成的影响。

风险的构成：起源（威胁源）、方式（威胁行为）、途径（脆弱性）、受体（资产）、后果（影响）；

1. 相关术语

资产是任何对组织有价值的东西，是要保护的对象；资产以多种形式存在（多种分类方法）；

威胁是指可能导致对系统或组织危害的不希望事故潜在起因；引起风险的外因；威胁源采取恰当的威胁方式才可能引发危险。（操作失误，滥用授权，行为抵赖，身份假冒）

脆弱性是可能被危险所利用的资产或若干资产的薄弱环节；造成风险的内因；脆弱性本身并不对资产构成危害，会被危险源利用，从而对信息资产造成危害。

（系统程序代码缺陷、系统设备安全配置错误）

可能性是某件事发生的机会；威胁源利用脆弱性造成不良后果的机会。

风险就是威胁源采用威胁方式，利用脆弱性造成不良后果的可能性。

风险是这个事件

1. 信息安全审计

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。

03 信息安全标准

1. 大部分信息安全问题的发生是因为：

员工缺乏信息安全意识；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

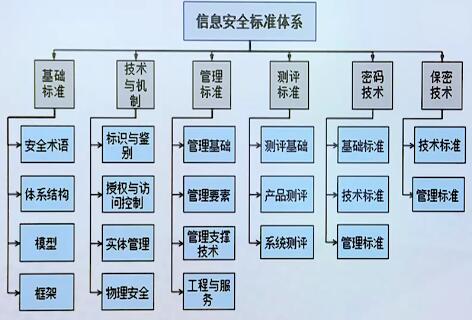
国际标准化组织（ISO）、国家标准（GB）

1. 信息安全标准体系

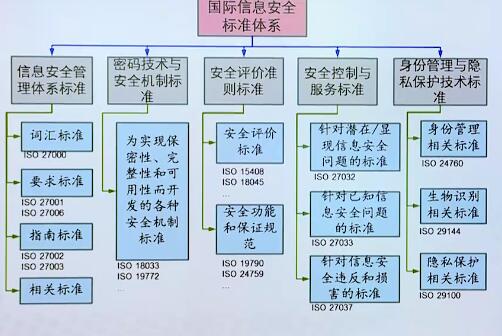
由信息安全领域具有内在联系的标准组成科学有机整体；

编制信息安全标准制定、修订的重要依据。

我国信息安全标准体系



国际信息安全标准体系框架



04 信息安全现状分析

1. 常见信息安全问题

计算机病毒、系统漏洞、黑客入侵

1. 信息安全问题产生根源

内因：信息系统自身存在脆弱性（过程复杂、结构复杂、应用复杂）

外因：威胁与破坏（人为和环境）

1. 信息安全发展阶段

COMSEC—通信安全；COMPUSEC—计算机安全；

INFOSEC—信息系统安全；IA—信息安全保障；

CS/IA—网络空间安全、信息安全保障

1. 信息安全

（1）通信安全20世纪，40-70年代

核心思想：通过密码技术解决通信保密，保证数据保密性和完整性，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

（2）计算机安全

20世纪，70-90年代

核心思想：预防、检测减小计算机系统（包括软件和硬件）执行的未授权活动所造成的后果；主要关注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

安全措施：通过操作系统的访问控制技术来防止非授权用户的访问

（3）信息系统安全

20世纪，90年代后

核心思想：综合通信安全和计算机安全；重点在于保护比“数据”更精练得“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、转移或破坏；

安全威胁：网络入侵、病毒破坏、信息对抗

安全措施：防火墙、防病毒、漏洞扫描、入侵检测、PKI、VPN等

1. 信息安全保障

核心思想：信息安全从技术扩展到管理、从静态到动态；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、自然灾害、电力中断

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

2011年美国发布《网络空间国际战略》，明确了针对网络攻击的指导原则

05 信息安全发展趋势

1. 发展趋势

云计算和软件开源逐步成为新的标准

云服务：随着越来越多企业和个人开始将自己的有价值数据保存在云环境当中，恶意人士当然也会找到可行途径利用计算基础设施以访问这些数据。

存在现象：勒索软件、钓鱼式攻击、

1. 已知的安全隐患

（1）开源运动使得很多现成的软件系统受到追捧。整合这些软件将比内部开发软件具有更高的性价比。公众已知的安全隐患往往是IT部门面临的最大威胁之一。

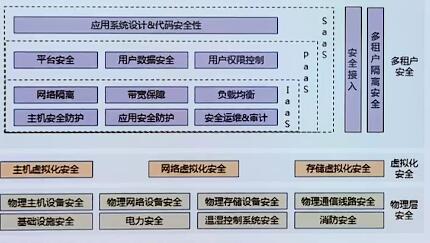
（2）物联网

物联网代表了另一种潜在的威胁。当连接性扩展到我们的生活和企业中的每一个角落，企业确保数据入口和数据流的安全将变得越来越有挑战性。

06 云安全框架

1. 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

1. 云安全聚焦

（1）应用安全

在云环境下，应用安全将会聚焦在：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

1. 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。

07 网络安全攻防介绍

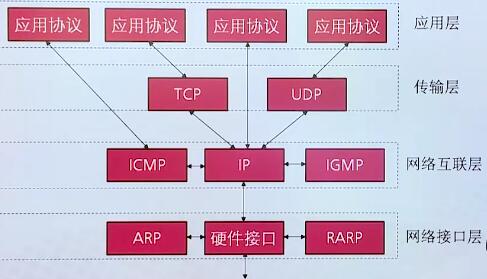
1. OSI安全体系结构

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；

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

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。

1. 网络协议安全问题



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；

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

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

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

1. 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）

1. 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

防火墙功能：

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

1. 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。

1. 网络架构安全

网络是新系统的基础支撑环境，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方式，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