信息安全概念及规范

HUAWEI

前言

- 随着互联网的普及，众多的企业、组织、政府部门与机构都在组建和发展自己的网络，大量建设的各种信息系统已经成为国家和政府的关键基础设施。整个国家和社会对网络也越来越依赖，网络已经成为社会和经济发展的强大推动力，其地位越来越重要。正因为如此，网络安全和信息安全的保障也愈发重要和关键。在数据通信的过程中，各种不安全因素将会导致信息泄密、信息不完整和信息不可用等问题，影响巨大。本课程描述了信息安全的基本概念和发展历程，以及安全行业和技术的未来发展趋势，为后续安全相关的课程提供铺垫。
- 网络安全标准对各行业建立网络安全管理体系起着指导、牵引和监督的作用，本课程描述了国内和国际网络安全标准，以及这些标准的认证过程。

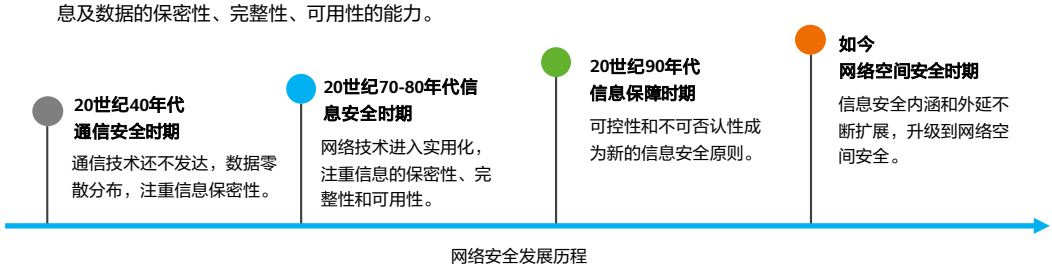
目标

- 学完本课程后，您将能够：
  - 描述网络安全的定义和特点
  - 描述网络安全的发展历程和趋势
  - 描述ISO 27001信息安全管理体系
  - 描述网络安全等级保护2.0标准

目录

网络安全

- 网络安全包括广义的网络安全和狭义的网络安全。
  - 广义的网络安全是指Cyber Security，也就是网络空间安全，网络空间由独立且互相依存的信息基础设施和网络组成，包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统等，是国家层面的。
  - 狭义的网络安全是指Network Security，也就是我们常说的网络安全，是指通过采取必要的措施，防范对网络及网络中传递的信息的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，保障网络中信息及数据的保密性、完整性、可用性的能力。



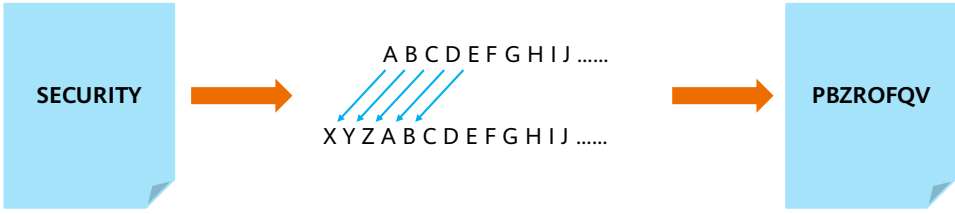
网络安全发展历程

HUAWEI

- 广义的网络安全，主要由国家从法律、制度、规章和流程等方面指导各政府机构、组织、各行各业乃至个人，共同构建国家层面的网络安全。
- 狭义的网络安全，包括网络安全厂商针对各类行业客户推出的网络安全设备及方案，主要用于保障各类网络如企业网络的安全运行。通过华为HCIA-Security认证后，您能够具备协助设计、部署和运维中小型企业网络安全架构的能力。
- 本课程主要讲解在狭义的网络安全中涉及到的安全技术及方案。

通信安全时期

- 20世纪40年代，通信技术还不发达，数据只是零散地位于不同的地点，信息系统的安全仅限于保证信息的物理安全以及通过密码（主要是序列密码）解决通信安全的保密问题。例如，将信息安置在相对安全的地点，不容许非授权用户接近，使用密码技术保障电话、电报和传真等信息交换过程的安全，从而确保数据的安全性。该时期侧重于保证数据在两个地点传输过程中的安全性。
- 信息系统安全仅限于保证信息的物理安全以及解决通信安全的保密问题。



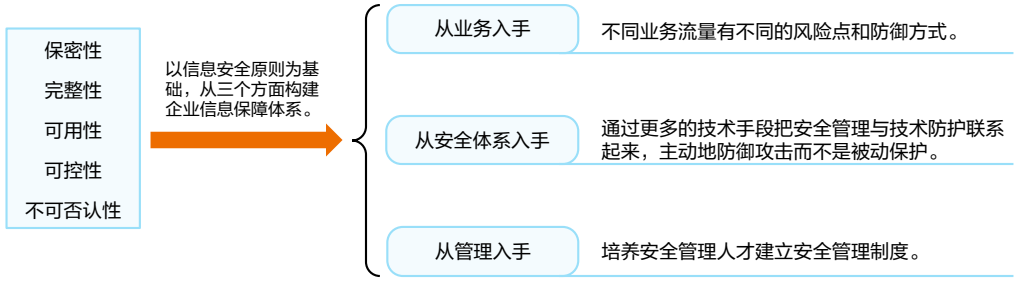
信息安全时期

- 计算机和网络技术的应用进入实用化和规模化，数据传输已经可以通过电脑网络完成。
- 信息安全的主要目标是确保信息的完整性、可用性和保密性。

完整性	可用性	保密性
• 确保信息在传输过程中不被篡改。如果被篡改，信息的接收方则可以识别到。	• 确保被授权人员在需要时可以获取和使用相关的信息资产。	• 确保信息只能由被授权的人员获取及使用。数据即使被攻击者窃取，也不能读出正确的信息。

信息保障时期

- 可控性和不可否认性成为保密性、完整性和可用性三个原则外，新的信息安全焦点。
- 从业务、安全体系和管理三个方面构建企业信息保障体系。

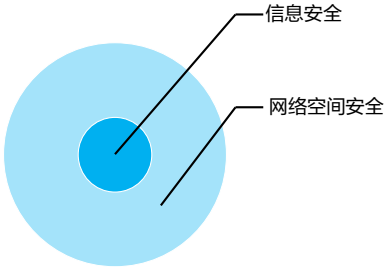


HUAWEI

- 20世纪90年代开始，互联网技术的飞速发展使信息安全问题跨越了时间和空间，可控性和不可否认性成为传统的保密性、完整性和可用性三个原则外，新的信息安全焦点。
  - 可用性：确保被授权人员在需要时可以获取和使用相关的信息资产；
  - 保密性：确保信息只能由被授权的人员获取及使用；
  - 完整性：确保信息在传输过程中不被篡改；
  - 可控性：对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统；
  - 不可否认性：防止信息源用户对他发送的信息事后不承认，或者用户接收到信息之后不认帐。

网络空间安全时期

- 信息安全的内涵和外延不断扩大，升级为网络空间安全，其目标是包含设施、数据、用户和操作在内整个网络空间的系统安全。
- 国家出台网络安全等级保护等相关标准和规范，引导企业建立信息安全管理体系。



建设网络安全的意义

重要性

网络安全对国家安全至关重要。

- 网络安全成为经济繁荣、社会稳定和国家发展的基础。
- 各国地缘政治博弈已经超越了实体空间限制，延伸到了网络空间。

合规性

企业信息安全管理体系建设需要符合网络安全政策要求。

- 我国在政策、法规和标准等多方面完善信息安全政策体系建设。
- 政府机关，企业网络需要符合等保规范。

效益性

企业建设网络安全可以减少遭受网络攻击后造成的损失。

- 网络攻击逐渐成为一种服务，企业面临更多网络风险。
- 企业因网络攻击导致应用系统瘫痪以及用户信息泄露，将遭受巨大损失。

目录

网络安全威胁

黑客往往是信息安全事件的发起者，通过攻击网络，获得有益的信息或者丰厚的报酬，通常伴随着犯罪行为。

漏洞是一切安全问题的根源。新增漏洞数量快速上涨，且漏洞挖掘从应用层面深入到底层组件甚至架构层面，影响不断增大。

勒索攻击数量继续增长，攻击门槛降低，多重勒索策略或将成为主流。勒索赎金整体走高，钓鱼和远程桌面协议是勒索攻击的主要媒介。

信息泄露是当今网络最常见的信息安全事件，通过在用户设备植入木马，安装窃听设备等方式，黑客可以对收集的信息进行数据挖掘，从照片、电子邮件、视频会议和社交资料各类信息中分析个人的联系方式与行为。

DDoS攻击正在逐渐演变为一种服务，成为攻击者获利的新手段。攻击者通过出售网络犯罪工具包和服务获取经济利益，网络犯罪日益增长。

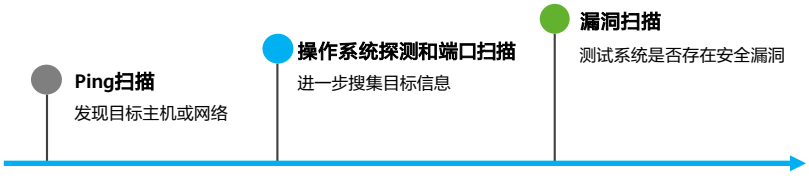
针对**供应链的威胁和攻击**不断增加，因为供应链所涉及的下游企业及用户众多，攻击成功后，往往会造成广泛的影响。

黑客

- 黑客（Hacker）是指对软件设计、编程和计算机科学等方面有深入理解的人。
  - 在计算机软件方面，“黑客”是对计算机及计算机网络系统特别感兴趣并且有深入理解的一群人；
  - 在业余计算机技术方面，“黑客”是指研究如何修改计算机相关产品的业余爱好者；
  - 在信息安全方面，“黑客”指研究如何智取计算机安全系统的人员。他们利用公共通讯网路，如电话系统和互联网，在非正规的情况下登录对方系统，掌握操控系统之权力。

漏洞

- 漏洞也称为脆弱性，是指计算机系统在硬件、软件和协议的具体事项或系统安全策略上存在缺陷和不足。
- 通过漏洞，信息系统可能会发生权限绕过、权限提升、执行非授权指令、数据泄露和拒绝服务攻击等信息安全事件。
- 现网中，工程师通过漏洞扫描来检测目标网络或主机的脆弱性，可用于模拟攻击实验和安全审计。

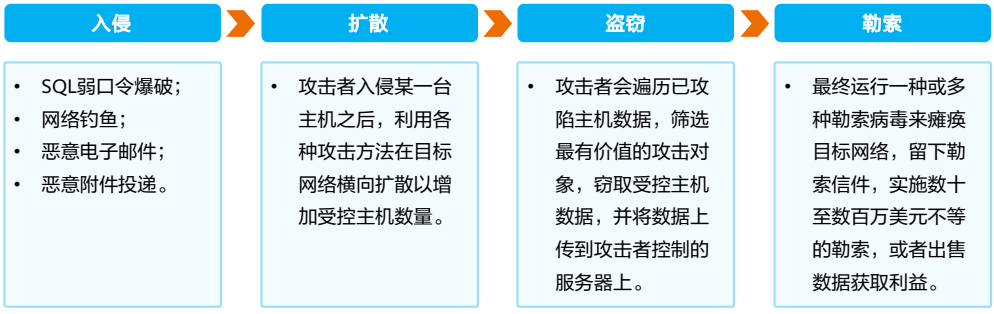


HUAWEI

- 漏洞对网络系统的安全威胁有：
  - 权限绕过和权限提升主要是为了获得期望的数据操作能力，如普通用户权限提升，获取管理员权限等；
  - 拒绝服务攻击是获得对系统某些服务的控制权限，导致服务被停止；
  - 数据泄露主要是黑客能够访问未授权的数据或保密信息，如读取受限文件，服务器信息泄露等；
  - 执行非授权指令主要是让程序将输入的内容作为代码来执行，从而获得远程系统的访问权限或本地系统的更高权限，如SQL注入和缓冲区溢出等。
- 漏洞扫描过程：Ping扫描确定目标主机地址，端口扫描确定目标主机开放的端口，然后基于端口扫描的结果，进行操作系统探测，最后根据掌握的信息进行漏洞扫描。

勒索攻击

- 某成品油管道运营商遭到勒索软件的网络攻击，影响了管理管道的计算机相关设备，导致部分燃料供应系统被迫下线。此次事件是对关键基础设施进行的极具破坏性的网络攻击。
- 勒索攻击过程如下所示：

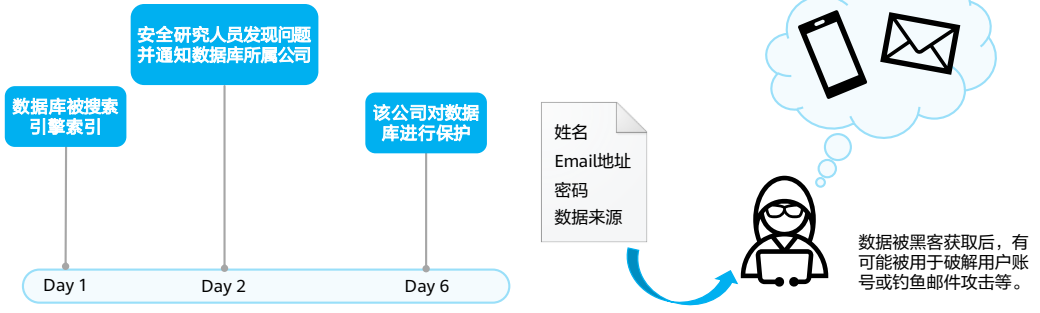


HUAWEI

- 攻击过程：
  - 勒索软件的上游开发者编写完整的勒索软件，授权给其下游隶属攻击组织使用，期间可能收取租金或授权费用；
  - 下游隶属组织可能维护一个钓鱼网站，上传勒索软件并诱使受害者访问；
  - 下游隶属组织可能通过钓鱼邮件或其他渠道发送钓鱼网站链接给受害者；
  - 受害者访问包含勒索软件的钓鱼链接；
  - 受害者根据钓鱼链接主动下载勒索软件或遭受远程代码执行攻击而被动下载勒索软件到本地；
  - 受害者在本地主动运行勒索软件，或遭受远程代码执行攻击而静默运行勒索软件，勒索软件加密本地磁盘文件以及搜索到的共享网络文件，在受害者计算机上留下勒索信，指引受害者缴纳赎金；
  - 受害者根据勒索信的指引，缴纳赎金给下游代理机构；
  - 勒索软件下游代理机构清洗赎金以掩盖上游开发者与下游隶属攻击组织；
  - 勒索软件下游隶属攻击组织发送解密程序给受害者，由受害者恢复加密文件。

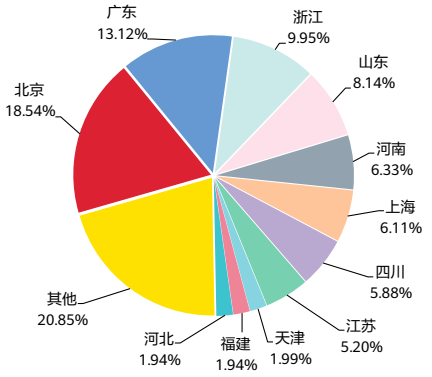
信息泄露

- 某安全研究人员发现网络中存在一个未受保护的数据库，该数据库采集了约50亿条数据，并且无需身份验证即可访问。研究人员通知了该数据库所属公司，三天后该公司保护了此数据库，但可能已造成了数据泄露。



DDoS攻击

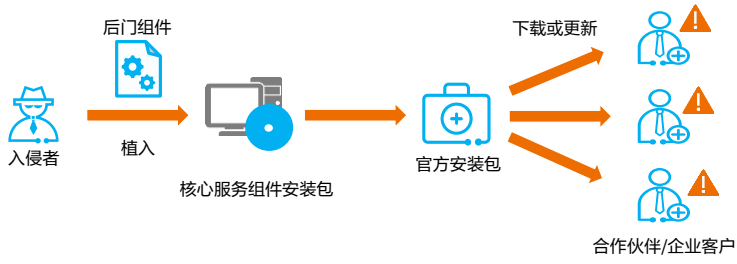
- 黑客个人或组织利用DDoS（Distributed Denial of Service）攻击，使目标服务器的网络或系统资源耗尽，使其服务暂时中断或停止，导致正常的用户无法访问。
- 随着物联网的兴起，越来越多的IoT（Internet of Things）设备接入网络，黑客利用设备硬件或管理漏洞就可以迅速发起一次大规模的DDoS攻击。黑客利用DDoS攻击资源对外提供能力租赁服务，缺乏技术能力的攻击者可以根据需要定制攻击，这逐渐成为掌握DDoS攻击能力的黑客组织获利的主流方式。



CNCERT《2018年网站攻击态势及“攻击团伙”挖掘分析报告》
境内受到网站攻击的服务器IP数量按省份分布图

供应链攻击

- 供应链攻击是针对供应链发起的网络攻击，并通过供应链将攻击延伸至相关的合作伙伴和企业客户。
- 某著名信息系统管理和网络监控软件开发公司的相关产品遭到供应链攻击事件被披露，引发全球关注。该公司遭到APT组织发动的供应链攻击，所属平台软件的安装包被植入后门，使用该软件的客户均存在被入侵的风险。该软件是一个针对网络设备提供实时监测和分析的管理平台软件，客户主要包括政府、军事、教育等重要机构和国际知名企业。



HUAWEI

- 供应链攻击的曝光，凸显出软件行业联系程度不足、生态系统脆弱、制度设计中充满假设、下游方简单地从已知“受信”供应商处接收更新等关键问题。
- 供应链攻击手段：
  - 盗取合法开发者账号替换正规应用，发布相似名称应用或添加恶意代码；
  - 通过第三方下载站点、社区、软件联盟以及黑产组织中去投放恶意应用或代码；
  - SaaS化上游服务污染，开源软件仓库投毒，伪装知名软件、域名、网站以及入侵合法网站替换下载链接；
  - 劫持正式更新下载地址的域名，DNS解析投毒，下载节点、CDN和P2P缓存投毒；
  - 入侵官方更新升级系统，入侵软件、硬件开发公司并植入恶意代码；
  - 仓储、物流链路劫持，盗取供应商预留的远程控制能力和超级权限账号；
  - 编译环境、开发工具、应用运行环境和应用组件环境污染，被植入后门。

目录

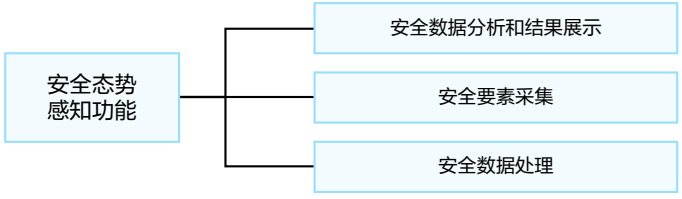
Gartner八大安全和风险趋势

序号	安全和风险趋势
1	网络安全网格：网络安全网格作为一种现代安全架构概念，可应对未来的网络安全威胁，能够使分布式企业在最需要的地方部署和扩展安全性。
2	精通网络安全的董事会成员：企业越来越关注网络安全，倾向于使用具有安全经验的高层管理者。
3	安全产品供应商整合：供应商整合和集成度更高的安全产品可以提高运维效率，降低企业成本。
4	身份优先：随着攻击者将目光聚焦到获得身份和访问管理功能权限上，身份优先安全变得更加急迫了。
5	管理机器身份正成为一项重要的安全能力：现代应用程序中的非人类实体数量呈爆炸式增长，管理机器身份已成为安全操作的重要组成部分。
6	“远程办公”兴起：未来社会实现远程办公，需要企业重新制定安全策略和工具以更好地降低安全风险。
7	善用攻防演练：攻防演练作为一个新兴市场，可以帮助企业检验其安全状况，提升其安全防御能力。
8	隐私增强计算技术：可以在不受信任环境中，实现安全的数据处理、共享、跨境传输和分析。

- Gartner是一家世界领先的研究与顾问公司，从全球化视野出发，针对企业所有重大业务职能领域，提供深入的业务与技术洞察。
- 上表为Gartner公司2021年针对安全领域的网络风险与客户业务需求提出的安全趋势。
- 安全设备厂商根据业界的发展趋势推出不同的网络安全解决方案，以应对客户现网中各类日新月异的威胁，如网络安全态势感知、零信任等。

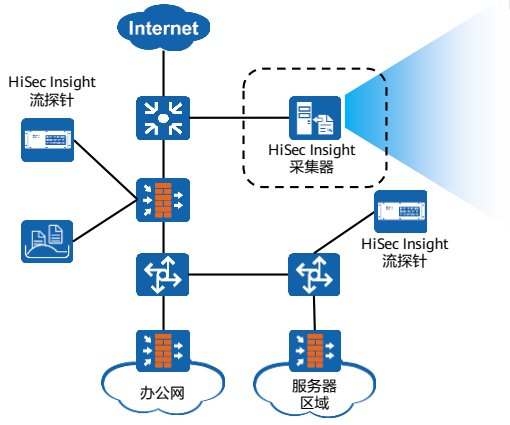
网络安全态势感知（1）

- 随着企业网络规模扩大，安全架构日趋复杂，各种类型的安全设备、安全数据越来越多，企业的安全运维压力不断加大。
- 当前企业网络环境中部署的各类安全设备主要实现单点检测，这种独立分割的安全防护体系已经很难应对以APT为代表的新型网络威胁。
- 网络安全态势感知是一种基于环境动态地、整体地洞悉安全风险的能力，它利用数据融合、数据挖掘、智能分析和可视化等技术，直观显示网络环境的实时安全状况，为网络安全保障提供技术支撑。



- 安全数据分析和结果展示：利用数据挖掘及智能分析等技术，提取系统安全特征和指标，发现网络安全风险，汇总成有价值的情报，并将网络安全风险通过可视化技术直观地展示出来。
- 安全要素采集：采集各类安全设备的海量数据，包括流量数据、各类日志、漏洞、木马和病毒样本等。
- 安全数据处理：对采集到的安全要素数据进行清洗、分类、标准化、关联补齐和添加标签等操作，将标准数据加载到数据存储中。

网络安全态势感知（2）

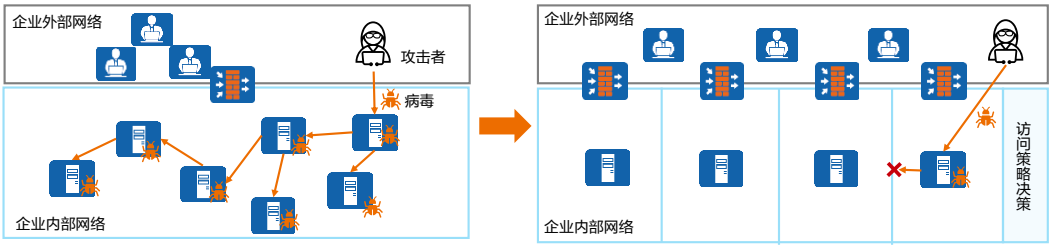


企业网络中部署HiSec Insight，通过流探针采集网络中的流量、设备日志等网络基础数据，通过大数据分析，结合机器学习技术、专家信誉和情报驱动，有效地发现网络中的潜在威胁和高级威胁，实现企业内部的全网安全态势感知，分析结果在可视化界面集中展示。

HUAWEI

零信任安全

- 零信任是一组不断发展的网络安全范式，该范式将网络防御从基于网络的静态边界转移到关注用户，资产和资源。零信任架构ZTA是基于零信任原则的企业网络安全战略，旨在防止数据泄露和限制内部横向移动。
- 零信任的核心思想是，默认情况下不应该信任网络内部和外部的任何人、设备和系统，需要基于认证、授权和重构访问控制的信任基础，即永不信任，始终验证。

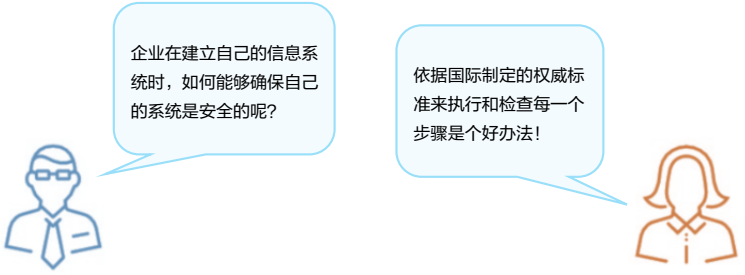


- 网络中心化：基于网络位置的可信控制模型，认为内部网络是可信的，外部网络是不可信的，内外网边界通过防火墙等设备进行防护。存在信任过度问题，无法防御从内部网络发起的内部攻击。
- 身份中心化：不管内部或是外部网络，任何一个用户，任何一台设备，发起的任何一次连接，申请的任何一次服务，在通过访问策略判决前均认为是不可信的。以身份为中心对资源进行细粒度的和自适应的访问控制。

目录

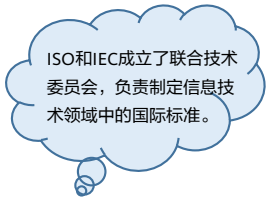
信息安全标准的意义

- 信息安全标准是规范性文件之一，其定义是：为了在一定的范围内获得最佳秩序，经协商一致并由公认机构批准，制定的一种规范性文件。
- 信息安全标准化是国家网络安全保障体系建设的重要组成部分。



信息安全标准组织

- 在国际上，与信息安全标准化有关的组织主要有以下2个：
  - International Organization for Standardization（ISO）国际标准化组织
  - International Electrotechnical Commission（IEC）国际电工委员会
- 国内的安全标准组织主要有：
  - 全国信息安全标准化技术委员会（TC260）
  - 中国通信标准化协会（CCSA）下辖的网络与信息安全技术工作委员会
- 其它一些制定标准的组织：
  - International Telecommunication Union（ITU）国际电信联盟
  - The Internet Engineering Task Force（IETF）Internet工程任务组
  - National Institute of Standards and Technology（NIST）美国国家标准与技术研究院



HUAWEI

- 国际上信息安全标准化工作兴起于20世纪70年代中期，80年代有了较快的发展，90年代引起了世界各国的普遍关注。目前世界上有近300个国际和区域性组织制定标准或技术规则。
- ISO是一个全球性的非政府组织，是国际标准化领域中一个十分重要的组织。ISO负责目前绝大部分领域（包括军工、石油和船舶等垄断行业）的标准化活动。
- IEC是世界上成立最早的国际性电工标准化机构，负责有关电气工程和电子工程领域中的国际标准化工作。
- ITU国际电联是主管信息通信技术事务的联合国机构，负责分配和管理全球无线电频谱与卫星轨道资源，制定全球电信标准，向发展中国家提供电信援助，促进全球电信发展。
- IETF是一个公开性质的大型民间国际团体，汇集了与互联网架构和互联网顺利运作相关的网络设计者、运营者、投资人和研究人员。

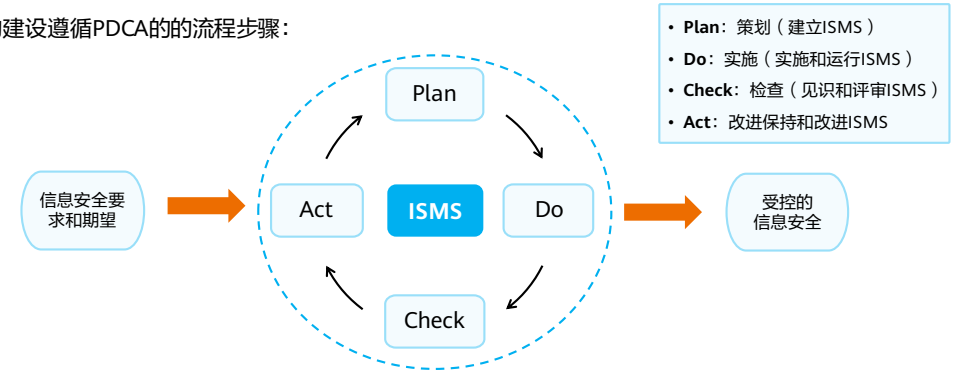
常见信息安全标准与规范

标准与规范	定义
网络安全等级保护制度	对信息和信息载体按照重要性等级分级别进行保护的一种制度。
ISO 27001	信息安全管理体系的国际标准。可以帮助企业建立与优化自身的信息安全管理体系，并对其进行评估。
美国标准TCSEC	Trusted Computer System Evaluation Criteria，可信计算机系统评价标准。1970年由美国国防科学委员会提出，1985年12月由美国国防部公布。是计算机系统安全评估的第一个正式标准。
欧盟标准ITSEC	Information Technology Security Evaluation Criteria，欧洲的安全评价标准，是英国、法国、德国和荷兰制定的IT安全评估准则，较美国军方制定的TCSEC准则在功能的灵活性和有关的评估技术方面均有很大的进步。应用领域为军队、政府和商业。

目录

信息安全管理体系

- 信息安全管理体系（Information Security Management System，简称ISMS）是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系。ISMS概念最初来源于英国标准学会制定的BS 7799标准, 随着其作为国际标准的发布和普及而被广泛地接受。
- ISMS的建设遵循PDCA的的流程步骤：

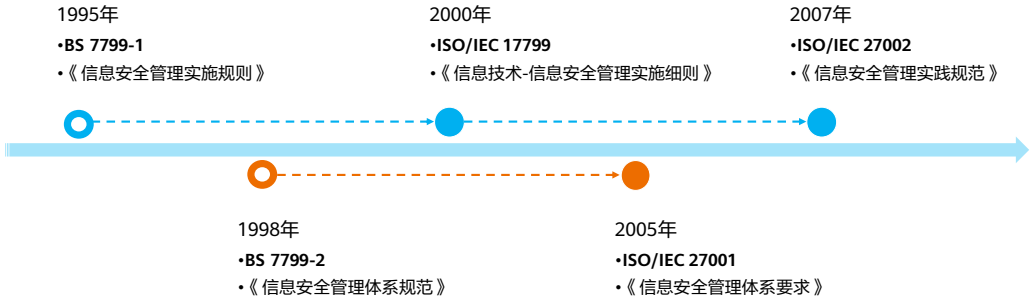


HUAWEI

- Plan：信息安全管理体系的策划与准备。根据组织的整体方针和目标，建立安全策略、目标以及与管理风险和改进信息安全相关的过程和程序，以获得结果。ISO 27002帮助组织建立ISMS。
- Do：信息安全管理体系文件的编制。实施和运行安全策略、控制、过程和程序。ISO 27003为实施者提供建立ISMS的参考方法。
- Check：信息安全管理体系运行。适用时，根据安全策略、目标和惯有经验评估以及测量过程业绩，向管理层报告结果，进行评审。ISO 27004为管理者提供度量方法和指标。
- Act：信息安全管理体系审核、评审和持续改进。根据内部ISMS审核和管理评审或其他信息，采取纠正和预防措施，以实现ISMS的持续改进。ISO 27005风险管理方法，贯穿整个风险识别、监控、评估和处置过程。

ISO 27000演变历程

- BS 7799标准后来被国际标准化组织ISO吸纳，成为了正式的国际标准。
- 目前正在适用的ISO/IEC 27001及ISO/IEC 27002均为2013发布的版本。



ISMS与ISO/IEC 27000

- ISO/IEC 27001是信息安全管理体系（ISMS）的国际规范性标准。
- ISO 27001认证要求组织通过一系列的过程，如确定信息安全管理体系范围、指定信息安全方针和策略、明确管理职责、以风险评估为基础选择控制目标和控制措施等，使组织达到动态的、系统的、全员参与的和制度化的，以预防为主的信息安全管理方式。
- ISO/IEC 27002从14个方面提出35个控制目标和113个控制措施，这些控制目标和措施是信息安全管理的最佳实践。

- ISMS是信息安全管理体系，任何公司都可以实施这个体系，但是怎么实施呢？要达到哪些要求呢？ISO 27000就给出了详细的要求或标准。组织可以依据ISO 27001的详细标准或要求去建立ISMS体系。
- ISO 27001的理念是基于风险评估的信息安全风险管理，采用PDCA过程方法，全面、系统和持续地改进组织的信息安全管理。可用于组织的信息安全管理体系建立和实施，保障组织的信息安全。
- ISO 27001是一个总的指导思想，依据是“PDCA”（PLAN、DO、CHECK、ACTION）的“戴明环”管理思想，是一个整体的信息安全管理框架，强调的是建立一个持续循环的长效管理机制；而ISO 27002就是具体的信息安全管理流程，是在ISO 27001整体框架指导下具体的信息安全细节。

构建信息安全管理体系的具体内容

- ISO 27002中的14个控制域为：

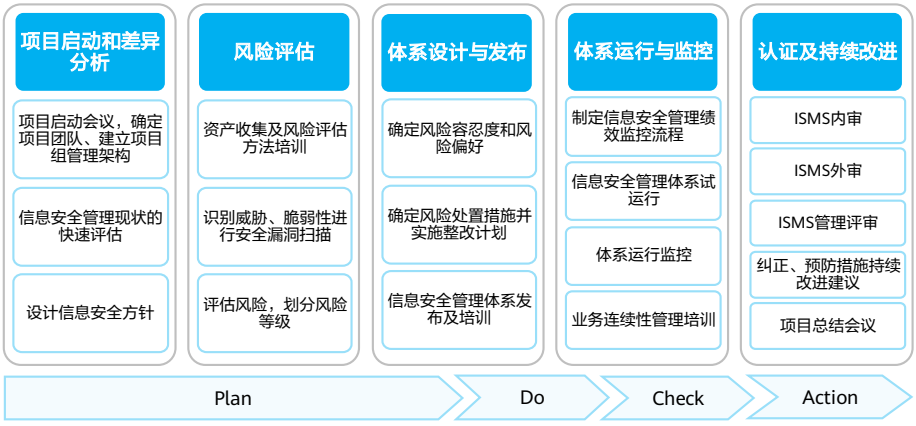
ISO 27000信息安全管理体系家族

- 除了ISO/IEC 27001和ISO/IEC 27002，ISO 27000系列标准还包括认证与审核指南相关的标准以及行业的相关标准。整个ISO 27000系列标准致力于帮助不同类型、大小的企业及组织建立并运行ISMS。

HUAWEI

- 只有ISO/IEC 27001是可以被认证的，其余的标准都是为这个认证所服务的具体条款和操作指导。

ISO 27001项目实施方法论及步骤



目录

等级保护定义

- 等级保护：对信息和信息载体按照重要性等级分级别进行保护的一种工作。
- 网络安全等级保护制度成为了国家网络安全领域的基本国策、基本制度和基本方法。等保是安全建设的一个“必过标杆”。

中华人民共和国网络安全法

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

- 信息安全等级保护是指对国家重要信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。
- 等级保护的法律责任：如果相关企业部门没有开展等级保护测评，将被按照相关规定进行不同程度的整改。如果其行为违反了正式实施的《 中华人民共和国网络安全法 》等相关规定，将被依据相关法律法规进行处罚。

等级保护的意义

合法合规

满足合法合规要求，落实网络安全保护义务，合理规避风险。

安全体系化

明确组织整体目标，改变以往单点防御方式，让安全建设更加体系化。

安全意识提升

提高人员安全意识，树立等级化防护思想，合理分配网络安全投资。

业务安全需求

以等保为契机，加强网络安全建设，源于等保，不止于等保，满足自身业务安全需求。

等级保护发展历程

- 等保经历了20多年的发展，大概经历了四个阶段，国家等级保护制定也从1.0版本发展到了2.0版本。

HUAWEI

- 等级保护发展时间轴：
  - 1994年2月18日中华人民共和国国务院令147号发布《中华人民共和国计算机信息系统安全保护条例》；
  - 2003年9月中共中央办公厅和国务院办公厅颁发《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）；
  - 2004年11月公安部、国家保密局、国家密码管理局和国务院信息化工作办公室联合发布《关于印发<关于信息安全等级保护工作的实施意见>的通知》（公通字[2004]66号）；
  - 2005年9月国信办文件《电子政务信息安全等级保护实施指南（试行）》（国信办[2004]25号）；
  - 2005年底，公安部和国务院信息化工作办公室联合下发《关于开展信息系统安全等级保护基础调查工作的通知》（**公信安**[2005]1431号）；
  - 2006年1月公安部、国家保密局、国家密码管理局和国家信息化工作办公室联合发布《关于印发<信息安全等级保护管理办法（试行）>的通知》（公通字[2006]7号）；
  - 2007年6月公安部、国家保密局、国家密码管理局和国家信息化工作办公室联合发布《信息安全等级保护管理办法》（公通字［2007］43号）；
  - 2008年发布GB/T 22239—2008《信息系统安全等级保护基本要求》，GB/T 22240—2008《信息系统安全等级保护定级指南》；

- 2009年中华人民共和国公安部发文《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）；
- 2010年3月公安部发文《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[303]号）；
- 2017年，《中华人民共和国网络安全法》正式实施，标志着等级保护2.0的正式启动。

等级保护对象

- 等级保护对象是指网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换和处理的系统，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网、工业控制系统和采用移动互联网技术的系统等。

等级保护系统定级

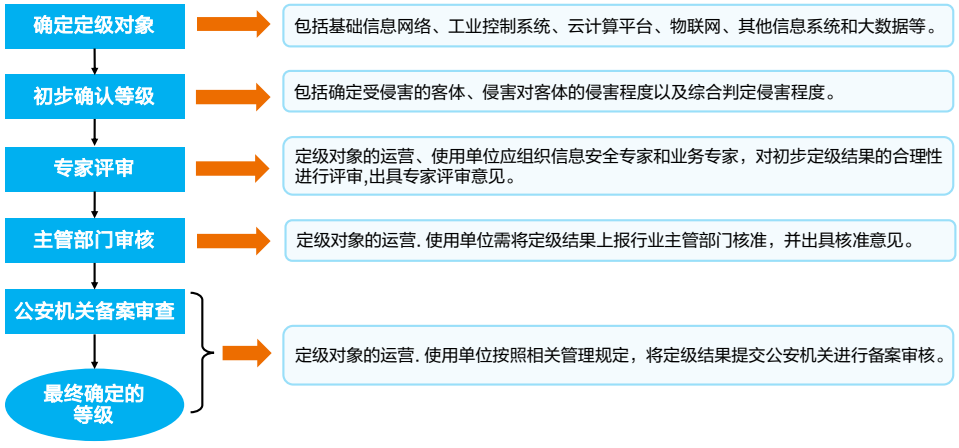
- 等级保护对象根据其在国家安全，经济建设和社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为五个安全保护等级。

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序 公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

定级要素与安全保护等级的关系

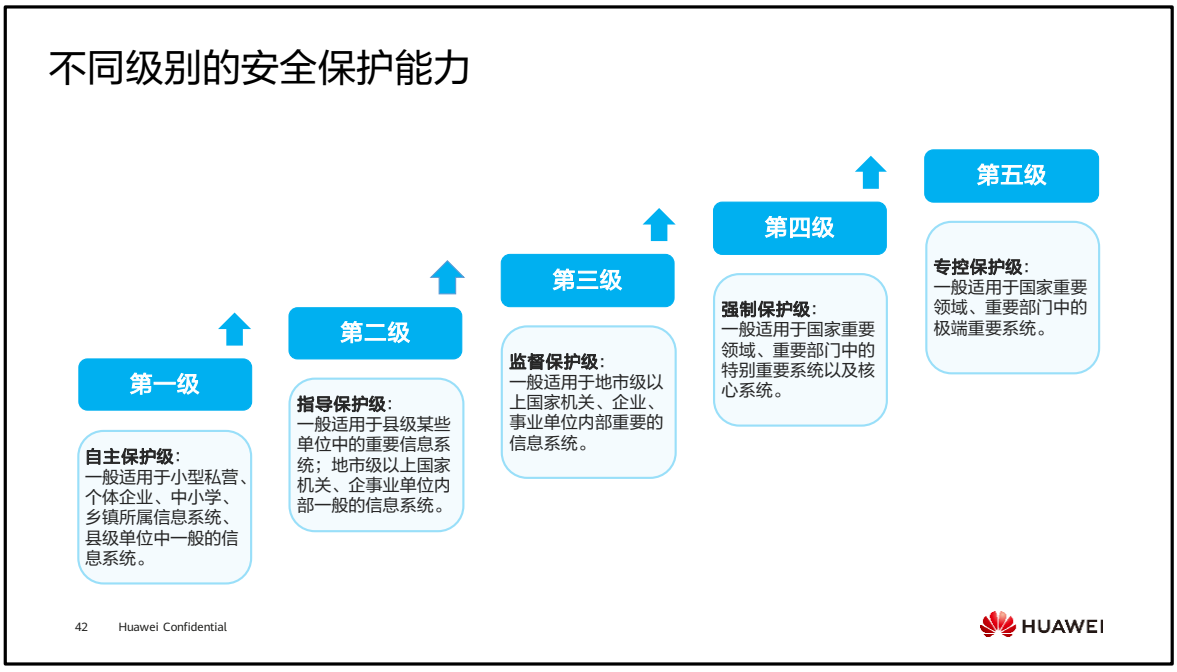
- 第一级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
- 第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
- 第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。
- 第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
- 第五级：信息系统受到破坏后，会对国家安全造成特别严重损害。

等级保护系统定级流程



HUAWEI

- 安全保护等级初步确定为第二级及以上的等级保护对象。其网络运营者依据本标准组织进行专家评审，主管部门核准和备案审核，最终确定其安全保护等级。
- 安全保护等级初步确定为第一级的等级保护对象，其网络运营者可依据本标准自行确定最终安全保护等级，可不进行专家评审，主管部门核准和备案审核。



- 第一级：自主保护级。能够防护拥有很少资源的威胁源发起的攻击、一般的自然灾害，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能。
- 第二级：指导保护级。能够防护外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。
- 第三级：监督保护级。能够在统一安全策略下防护来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。
- 第四级：强制保护级。能够在统一安全策略下防护来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾，以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。
- 第五级：专控保护级。能够在统一安全策略下，在实施专用的安全保护的基础上，通过可验证设计增强系统的安全性，使其具有抗渗透能力，使数据信息免遭非授权的泄露和破坏，保证最高安全的系统服务。

等级保护安全要求

- 等保2.0安全要求分为安全通用要求和安全扩展要求，以实现对不同级别和不同形态等级保护对象的共性化和个性化保护。
- 安全通用要求和扩展要求都分为技术要求和管理要求两方面，不同安全等级对应的要求具体内容不同，安全等级越高，要求内容越严格。

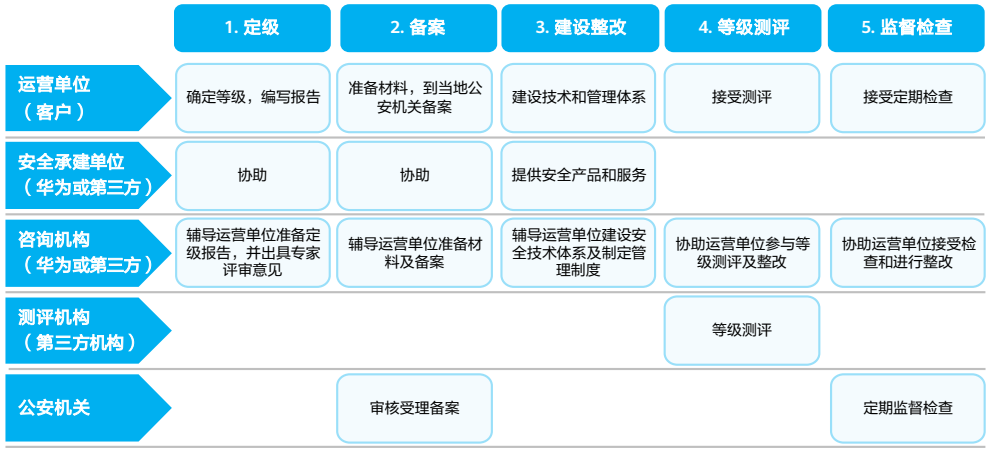
	等保2.0安全要求
	安全通用要求
安全扩展要求	云计算安全扩展要求
	移动互联安全扩展要求
	物联网安全扩展要求
	工业控制系统安全扩展要求

技术要求	管理要求
安全物理环境	安全管理制度
安全通信网络	安全管理机构
安全计算环境	安全管理人员
安全区域边界	安全建设管理
安全管理中心	安全运维管理

等保2.0标准体系

- 等保2.0标准体系除了明确网络安全等级保护基本要求的GB/T 22239-2019外，还有其他一系列标准用于指导等保2.0的定级、实施、测评等工作。

等级保护的工作流程



HUAWEI

- 安全保护等级初步确定为第一级的等级保护对象，其网络运营者可依据定级标准自行确定最终安全保护等级，可不进行专家评审，主管部门核准和备案审核。安全保护等级初步确定为第二级及以上的等级保护对象，其网络运营者需依据定级标准组织进行专家评审，主管部门核准和备案审核，最终确定其安全保护等级。
- 企业或组织有行业主管（监管）部门的，除出具专家评审意见外，还需将定级结果报请行业主管（监管）部门核准，并出具核准意见。

思考题

1. （单选题）等保2.0中定级对象初步定级为哪一级别，则其网络运营者可自行确定最终安全保护等级？（　　）

   A. 第一级

   B. 第二级

   C. 第三级

   D. 第四级

2. （判断题）ISO 27002标准可以对企业信息安全体系进行认证。（　　）

   A. 正确

   B. 错误

1. A
2. B

本章总结

- 本课程简要介绍了信息安全经历的四个发展时期，通信安全、信息安全、信息保障和网络空间安全，并描述了网络安全态势感知、零信任安全等安全理念和方案。讲解了各种信息安全国际标准和国家标准的制定，如ISO 27001，等保2.0等。这些标准规范促进了企业信息安全管理体系的建设。通过本课程的学习，您能够对信息安全的概念及规范有一定的了解。

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

缩略语表（1）

缩略语	英文全称	解释
APT	Advanced Persistent Threat	高级持续性威胁
BS	British Standard	英国国家标准
CCSA	China Communications Standards Association	中国通信标准化协会
CDN	Content Delivery Network	内容分发网络
DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
GB	China National Standards	国标
IEC	International Electrotechnical Commission	国际电工委员会
IETF	Internet Engineering Task Force	Internet工程任务组
IoT	Internet of Things	物联网
ISMS	Information Security Management System	信息安全管理体系
ISO	International Organization for Standardization	国际标准化组织

缩略语表 (2)

缩略语	英文全称	解释
ITSEC	Information Technology Security Evaluation Criteria	欧洲的IT安全评估准则
ITU	International Telecommunication Union	国际电信联盟
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
P2P	Peer to Peer	对等网络
PDCA	Plan–Do–Check–Action	PDCA循环
SaaS	Software as a Service	软件即服务
SQL	Structured Query Language	结构化查询语言
TC260	National Information Security Standardization Technical Committee	国家安全标准委员会
TCSEC	Trusted Computer System Evaluation Criteria	美国可信计算机系统评价标准
ZTA	Zero Trust Architecture	零信任架构

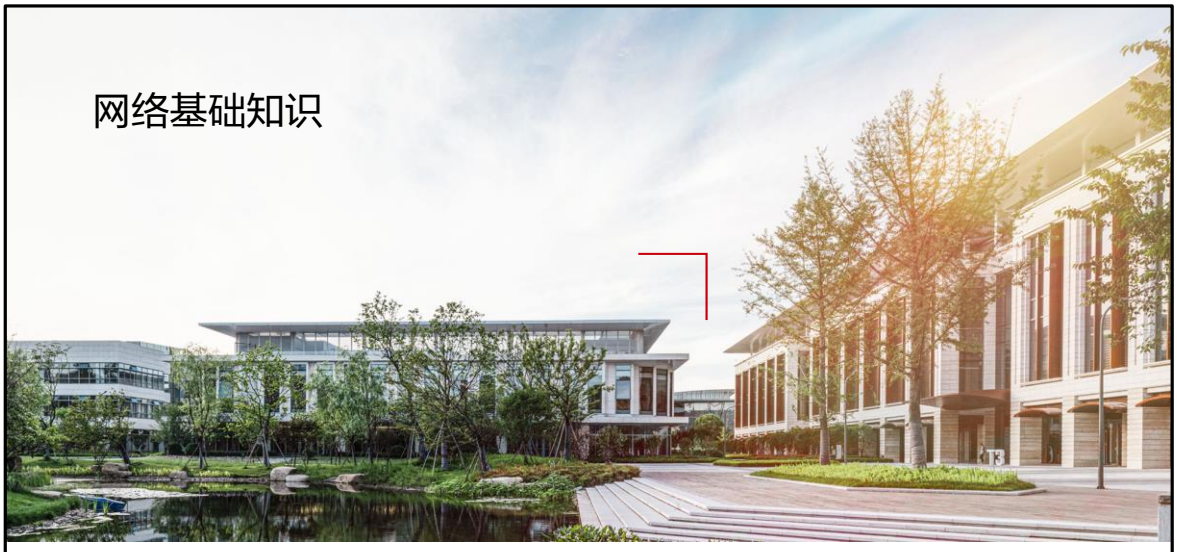
Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

网络基础知识



HUAWEI

前言

- 随着互联网的发展，各种网络攻击不断出现，网络安全的重要性愈加凸显。安全技术应用于数据通信的过程中，是数据通信技术的一种延伸和扩展。在学习安全技术之前，了解网络的基本概念，如网络的基本通信原理，网络的组成和常见的网络协议等，有助于更好地理解各种安全技术的工作原理和应用场景。
- 本课程将介绍企业网络的典型组网架构、常见的网络设备和它们的工作原理，并讲解防火墙的命令行和图形化界面两种配置方式。

目标

- 学完本课程后，您将能够：
  - 理解数据的定义及传递过程
  - 描述TCP/IP协议栈的工作原理
  - 描述常见协议的工作原理
  - 描述常见网络设备及工作原理

目录

应用与数据

- 在用户的眼中，应用的存在，是为了满足人们的各种需求，比如访问网页、在线游戏、在线视频等。伴随着应用会有信息的产生，比如文本、图片、视频等都是信息的不同呈现方式。
- 在网络工程师的眼中，应用会产生数据。数据是各种信息的载体，是对客观事物的性质、状态以及相互关系等进行记载的物理符号或这些物理符号的组合。数据可以是符号、文字、数字、语音、图像和视频等。
- 大部分应用所产生数据需要在不同的设备之间传输。对于一名网络工程师来说，更需要关注数据的端到端传输的过程。

- 计算机只能识别0和1组成的电子数据（digital data）。它不具备读取各种信息的能力，所以信息需要通过一定的规则翻译成数据。
- 而对人来说，我们不具备读取电子数据的能力，所以在读取信息的时候，需要将数据转成人能理解的信息。

OSI参考模型

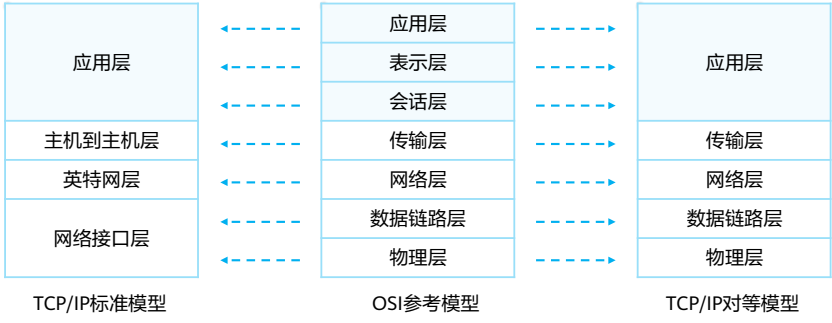
- OSI参考模型（Open Systems Interconnection Reference Model），是由国际标准化组织ISO于1984年发布的用于开放网络互联的模型，它由七个层级构成。

层级	作用
应用层	为应用程序提供接口。
表示层	进行数据格式的转换，以确保一个系统生成的应用层数据能够被另一个系统的应用层所识别和理解。
会话层	在通信双方之间建立、管理和终止会话。
传输层	建立、维护和取消一次端到端的数据传输过程。控制传输节奏的快慢，调整数据的排序等。
网络层	定义逻辑地址，实现数据从源到目的地的转发。
数据链路层	将分组数据封装成帧，在数据链路上实现数据的点到点、或点到多点方式的直接通信以及差错检测。
物理层	在媒介上传输比特流，提供机械的和电气的规约。

- OSI参考模型（Open Systems Interconnection Reference Model），由国际化标准组织ISO（The International Organization for Standardization）收录在ISO 7489标准中并于1984年发布。
- OSI参考模型又被称为七层模型，由上至下依次为：
  - 应用层：OSI参考模型中最靠近用户的一层，为应用程序提供相关服务；
  - 表示层：提供各种用于应用层数据的编码和转换功能，确保一个系统的应用层发送的数据能被另一个系统的应用层识别；
  - 会话层：负责建立、管理和终止表示层实体之间的通信会话。该层的通信由不同设备中的应用程序之间的服务请求和响应组成；
  - 传输层：提供面向连接或非面向连接的数据传递以及数据的差错检测功能；
  - 网络层：定义逻辑地址，供路由器确定路径，负责将数据从源网络传输到目的网络；
  - 数据链路层：将比特组合成字节，再将字节组合成帧，使用链路层地址（以太网使用MAC地址）来访问介质，并进行差错检测；
  - 物理层：在设备之间传输比特流，规定了电平、速度和电缆针脚等物理特性。

TCP/IP参考模型

- OSI参考模型较为复杂，且TCP和IP两大协议在业界被广泛使用，所以TCP/IP参考模型成为了互联网的实际参考模型。



HUAWEI

- TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）模型的开放性和易用性，以致在实践中得到了广泛应用。
- TCP/IP模型在结构上与OSI模型类似，采用分层架构，同时层与层之间联系紧密。不同点在于TCP/IP把表示层和会话层都归入应用层，所以TCP/IP模型从下至上分为四层：网络接口层，网络层，传输层和应用层。
- TCP/IP标准参考模型将OSI中的数据链路层和物理层合并为网络接口层，实际应用中，往往是对数据链路层和物理层分开处理的，故融合了TCP/IP标准模型和OSI参考模型的TCP/IP对等模型被提出，后面的讲解也都将基于这种模型。

TCP/IP协议栈常见协议

- TCP/IP协议栈定义了一系列的标准协议。

<table>
<tr><td rowspan="2">应用层</td><td>Telnet</td><td>FTP</td><td>TFTP</td><td>SNMP</td></tr>
<tr><td>HTTP</td><td>SMTP</td><td>DNS</td><td>DHCP</td></tr>
<tr><td>传输层</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td rowspan="2">网络层</td><td colspan="2">ICMP</td><td colspan="2">IGMP</td></tr>
<tr><td colspan="4">IP</td></tr>
<tr><td rowspan="2">数据链路层</td><td colspan="4">PPPoE</td></tr>
<tr><td colspan="2">Ethernet</td><td colspan="2">PPP</td></tr>
<tr><td>物理层</td><td colspan="4">.....</td></tr>
</table>

HUAWEI

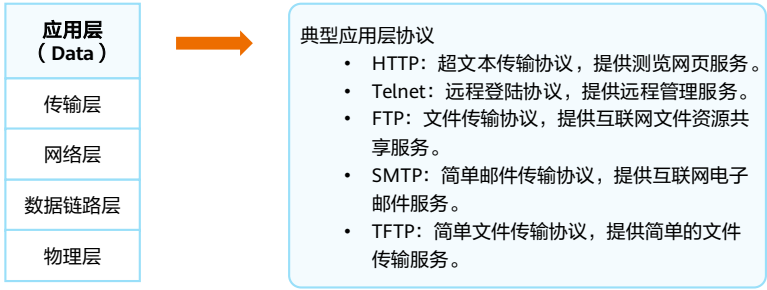
- 应用层：提供应用程序网络接口。
  - HTTP（Hypertext Transfer Protocol，超文本传输协议）：用来访问在网页服务器上的各种页面；
  - FTP（File Transfer Protocol，文件传输协议）：为文件传输提供了途径，它允许数据从一台主机传送到另一台主机上；
  - DNS（Domain Name Service，域名称解析服务）：用于实现从主机域名到IP地址之间的转换。
- 传输层：建立端到端连接。
  - TCP（Transmission Control Protocol，传输控制协议）：为应用程序提供可靠的面向连接的通信服务。目前，许多流行的应用程序都使用TCP；
  - UDP（User Datagram Protocol，用户数据报协议）：提供了无连接通信，且不对传送数据包进行可靠性的保证。
- 网络层：寻址和路由选择。
  - IP（Internet Protocol，互联网协议）：将传输层的数据封装成数据包并完成源站点到目的站点的转发，提供无连接的、不可靠的服务；
  - IGMP（Internet Group Management Protocol，因特网组管理协议）：负责IP组播成员管理的协议。它用来在IP主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系；

    - ICMP（Internet Control Message Protocol，网际报文控制协议）：基于IP协议在网络中发送控制消息，对于通信环境中可能发生的各种问题提供监测和反馈。通过这些信息，使管理者可以对所发生的问题作出诊断，然后采取适当的措施解决。
- 数据链路层：封装数据帧，向网络层提供“段内通信”。
    - PPP（Point-to-Point Protocol，点对点协议）：一种点对点模式的数据链路层协议，多用于广域网；
    - Ethernet（以太网协议）：一种多路访问广播型数据链路层协议，是当前应用最为广泛的局域网技术；
    - PPPoE（Point-to-Point Protocol over Ethernet，以太网承载PPP协议）：PPPoE提供通过简单桥接访问设备（接入设备）把一个网络的多个主机连接到远程访问集中器的功能。常见的应用有家庭宽带拨号上网。
- 物理层：负责比特流在介质上的传输。

目录

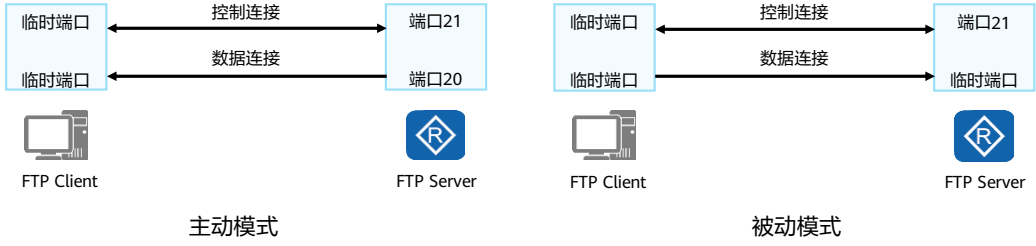
应用层

- 应用层为应用软件提供接口，使应用程序能够使用网络服务。应用程序会基于某一种传输协议，以及定义传输层所使用的端口号。



FTP

- FTP（File Transfer Protocol）是一个用于从一台主机传送文件到另一台主机的协议，用于文件的“下载”和“上传”，它采用C/S（Client/Server）结构。使用FTP传输数据时，需要在服务器和客户机之间建立控制连接和数据连接。
- FTP连接的建立分为主动模式和被动模式，两者的区别在于数据连接是由服务器发起还是由客户端发起。缺省情况下采用主动模式，用户可以通过命令切换。

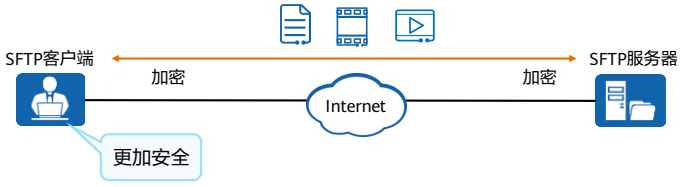


HUAWEI

- 主动模式下，当客户端存在防火墙时，由于数据连接是由服务器发起，数据连接可能会发生问题。被动模式下，这个问题得到了解决。主动模式有利于对FTP服务器的管理，不利于对客户端的管理；被动模式则相反。
- 缺省情况下，服务器的端口21用于传输控制命令，端口20用于传输数据。
- FTP连接主动模式建立过程：
  - 服务器打开端口21，启动监听，等待连接；
  - 客户端发起控制连接的建立请求，服务器响应；
  - 客户端通过控制连接发送PORT命令，将客户端数据连接的临时口号告诉服务器；
  - 服务器的20端口与客户建立起数据连接。
- FTP连接被动模式建立过程：
  - 服务器打开端口21，启动监听，等待连接；
  - 客户端发起控制连接的建立请求，服务器响应；
  - 客户端通过控制连接发送命令字PASV，告知服务器处于被动模式；
  - 服务器回应，将数据连接的临时端口号告诉客户；
  - 客户端与服务器的临时口建立起数据连接。

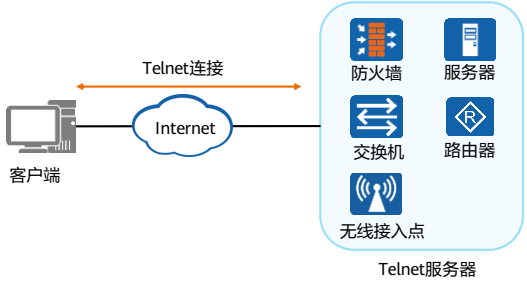
SFTP

- SFTP（Secure File Transfer Protocol，安全文件传输协议）是一种基于SSH（Secure Shell）提供文件安全传输的网络协议。
- FTP是明文传输的，并不安全。而SFTP对传输的认证信息和数据进行加密，相对于FTP极大提升了安全性。
- SFTP是一个单通道协议，目的端口号默认为22，通过客户端和服务器之间的SSH协议安全连接来传输文件，而FTP是一个双通道协议，包括控制通道和数据通道。



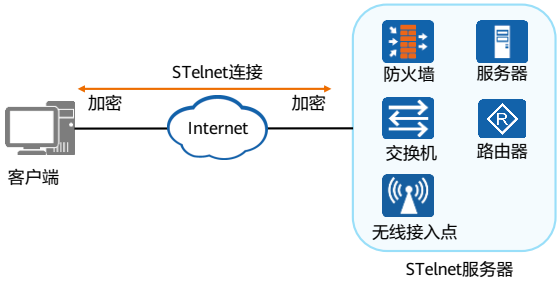
Telnet

- Telnet是数据网络中提供远程登录的标准协议。
- Telnet可以为用户实现在本地计算机上操作远程设备。
- 用户通过Telnet客户端程序连接到Telnet服务器。用户在Telnet客户端中输入命令，这些命令会在服务器端运行，就像直接在服务端的控制台上输入一样。



STelnet

- STelnet（Secure Telnet）是一种安全的Telnet服务，使用户可以从远端安全登录到设备，所有交互数据均经过加密，实现安全的会话连接。Telnet是明文传输的，并不安全，使用STelnet可以极大提升安全性。
- STelnet通过SSH协议实现，目的端口号默认为22。STelnet服务端与客户端的协商过程包括以下五个阶段：
  - 版本协商
  - 算法协商
  - 密钥交换
  - 用户认证
  - 会话交互

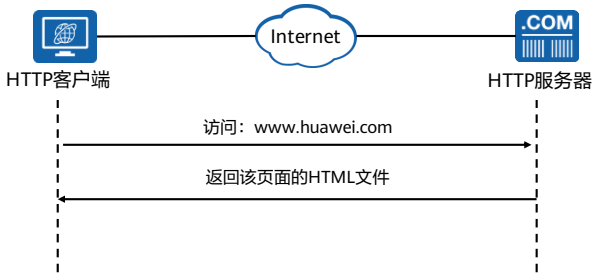


HUAWEI

- 版本协商阶段：SSH目前包括SSHv1和SSHv2两个版本，双方通过版本协商确定使用的版本。
- 算法协商阶段：SSH支持多种加密算法，双方根据本端和对端支持的算法，协商出最终使用的加密算法。
- 密钥交换阶段：通过密钥交换算法生成会话密钥，此后双方的会话均通过会话密钥加密。
- 用户认证阶段：SSH客户端向服务器端发起认证请求，服务器端对客户端进行认证。
- 会话交互阶段：认证通过后，服务器端和客户端进行信息的交互。

HTTP

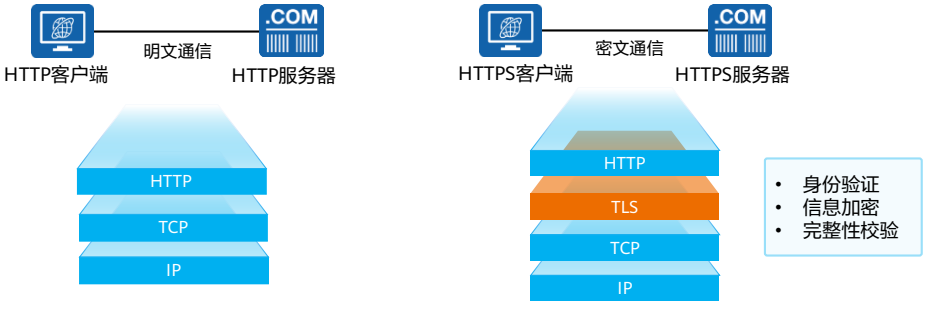
- HTTP（Hyper Text Transfer Protocol）是互联网上应用最为广泛的一种网络协议。设计HTTP最初的目的是为了提供一种发布和接收HTML页面的方法。



- WWW是World Wide Web的缩写，又称为3W或Web，中文译为“万维网”。它作为Internet上的新一代用户界面，摒弃了以往纯文本方式的信息交互手段，采用超文本（hypertext）方式。超文本是一种全局性的信息结构，它将文档中的不同部分通过关键字建立链接，使信息以交互方式进行传输。随着多媒体技术的兴起和发展，超文本技术的管理对象从纯文本扩展到多媒体，为强调管理对象的变化，就产生了超媒体。
- Internet采用超文本和超媒体的组合方式，将信息的链接扩展至整个Internet上。Web就是一种超文本信息系统，它使得文本不再固定在某一个位置，而是可以从一个位置跳转到另外的位置，正是这种多链接性，才把它称为Web。

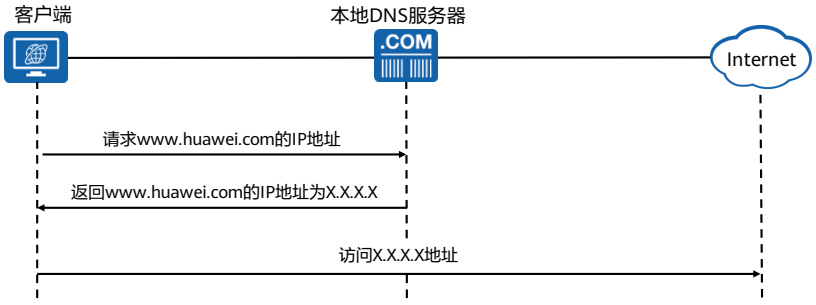
HTTPS

- HTTPS（Hypertext Transfer Protocol Secure，超文本传输安全协议），是以安全为目标的HTTP通道。
- HTTPS在HTTP的基础上加入TLS（Transport Layer Security）协议，为数据传输提供身份验证、加密及完整性校验。HTTPS的目的端口默认为443，HTTP的目的端口默认为80。目前大部分网站都提供HTTPS安全传输。



DNS

- 在浏览网页时，我们输入网址这个字符串，但计算机去访问这个网址时，真正需要知道的是网址对应域名的IP地址，这时就需要由专门的域名解析系统（Domain Name System，简称DNS）来完成。
- 域名解析分为动态域名解析和静态域名解析。在解析域名时，首先采用静态域名解析的方法，如果静态解析不成功，再采用动态域名解析的方法。



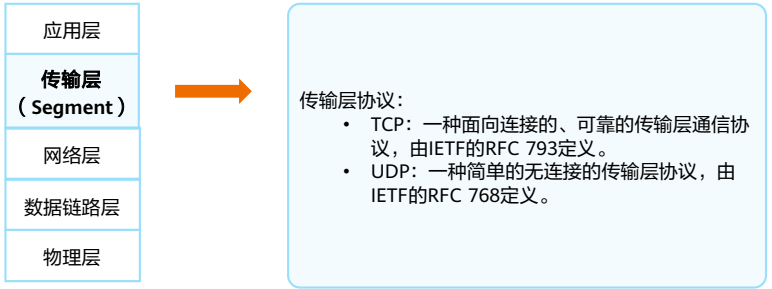
HUAWEI

- IPv4静态域名解析是通过静态域名解析表进行的，即手动建立域名和IPv4地址之间的对应关系表，该表的作用类似于Windows操作系统下的hosts文件，可以将一些常用的域名放入表中。当DNS客户端需要域名所对应的IPv4地址时，即到静态域名解析表中去查找指定的域名，从而获得所对应的IP地址，提高域名解析的效率。
- 动态域名解析需要专用的域名解析服务器（DNS Server）运行域名解析服务器程序，提供从域名到IP地址的映射关系，负责处理客户端提出的域名解析请求。

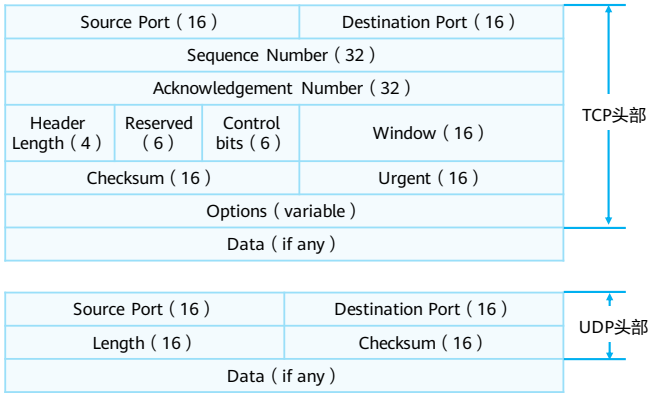
目录

传输层

- 传输层协议接收来自应用层协议的数据，封装上相应的传输层头部，帮助其建立“端到端”的连接。



TCP和UDP - 报文格式



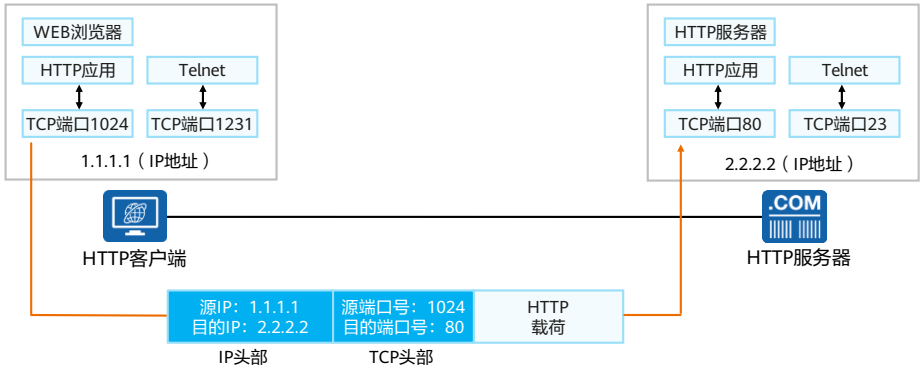
HUAWEI

- TCP报文头部：
  - Source Port：源端口，标识哪个应用程序发送。长度为16比特；
  - Destination Port：目的端口，标识哪个应用程序接收。长度为16比特；
  - Sequence Number：序号字段，TCP连接中传输的数据流每个字节都编上一个序号。序号字段的值指的是本报文段所发送数据的第一个字节的序号。长度为32比特；
  - Acknowledgment Number：确认序列号，是期望收到对方下一个报文段数据的第1个字节的序号，即上次已成功接收到的数据段的最后一个字节数据的序号加1。只有ACK标识为1，此字段有效。长度为32比特；
  - Header Length：头部长度，指出TCP报文头部长度，以32比特（4字节）为计算单位。若Option字段无内容，则该字段为5，即头部为20字节；
  - Reserved：保留，必须填0。长度为6比特；
  - Control bits：控制位，包含FIN、ACK、SYN等标志位，代表不同状态下的TCP数据段；
  - Window：窗口TCP的流量控制，这个值表明当前接收端可接受的最大的数据总数（以字节为单位）。窗口最大为65535字节。长度为16比特；
  - Checksum：校验字段，是一个强制性的字段，由发端计算和存储，并由收端进行验证。在计算检验和时，要包括TCP头部和TCP数据，同时在TCP报文段的前面加上12字节的伪头部。长度为16比特；

    - Urgent：紧急指针，只有当Urgent标志置1时紧急指针才有效。TCP的紧急方式是发送端向另一端发送紧急数据的一种方式。紧急指针指出在本报文段中紧急数据共有多少个字节（紧急数据放在本报文段数据的最前面）。长度为16比特；
    - Options：选项字段（可选），长度为0-40字节。
- UDP报文头部：
    - Source Port：源端口，标识哪个应用程序发送。长度为16比特；
    - Destination Port：目的端口，标识哪个应用程序接收。长度为16比特；
    - Length：该字段指定UDP报头和数据总共占用的长度。可能的最小长度是8字节，因为UDP报头已经占用了8字节。由于这个字段的存在，UDP报文总长不可能超过65535字节（包括8字节的报头，和65527字节的数据）；
    - Checksum：覆盖UDP头部和UDP数据的校验和，长度为16比特。

TCP和UDP - 端口号

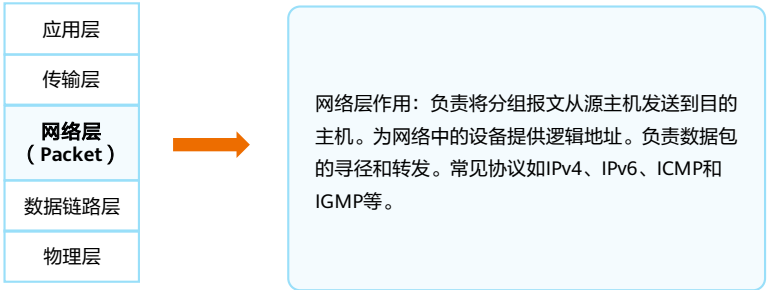
- TCP和UDP使用端口号来区分不同的服务。客户端使用的源端口一般随机分配，目标端口则由服务器的应用指定。源端口号一般为系统中未使用的，且大于1023的端口。目的端口号为服务端开启的应用（服务）所侦听的端口，如HTTP缺省使用80。



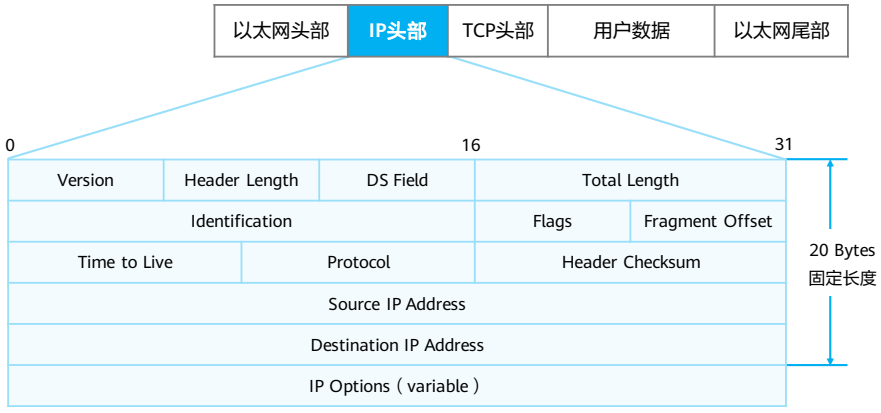
目录

网络层

- 传输层负责建立主机之间进程与进程之间的连接，而网络层则负责数据从一台主机到另外一台主机之间的传递。



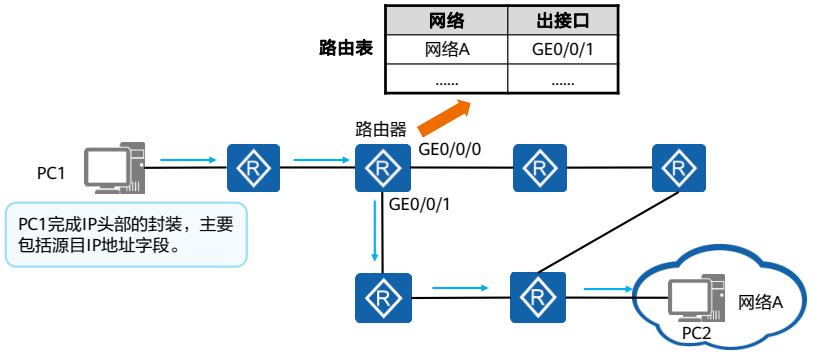
IP报文头部



HUAWEI

IP报文转发

- 源设备发出的报文会在其网络层头部携带源及目的设备的网络层地址。具备路由功能的网络设备（例如路由器等）会维护路由表。当这些网络设备收到报文时，会读取其网络层携带的目的地址，并在其路由表中查询该地址，找到匹配项后，按照该表项的指示转发数据。

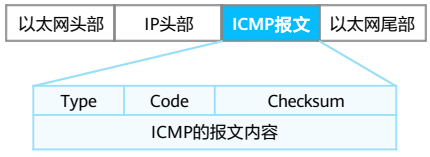


HUAWEI

- 当采用IP作为网络层协议时，通信的双方都会被分配到一个“独一无二”的IP地址来标识自己。IP地址可被写成32位的二进制整数值形式，但为了方便人们阅读和分析，它通常被写成点分十进制的形式，即四个字节被分开用十进制表示，中间用点分隔，比如192.168.1.1。
- IP数据包的封装与转发：
  - 网络层收到上层（如传输层）协议传来的数据时候，会封装一个IP报文头部，并且把源和目的IP地址都添加到该头部中；
  - 中间经过的网络设备（如路由器），会维护一张指导IP报文转发的“地图”——路由表，通过读取IP数据包的目的地址，查找本地路由表后转发IP数据包；
  - IP数据包最终到达目的主机，目的主机通过读取目的IP地址确定是否接受并做下一步处理。
- IP协议工作时，需要如OSPF、IS-IS、BGP等各种路由协议帮助路由器建立路由表，ICMP帮忙进行网络的控制和状态诊断。

ICMP协议

- Internet控制消息协议ICMP（Internet Control Message Protocol）是IP协议的辅助协议。
- ICMP协议用来在网络设备间传递各种差错和控制信息，对于收集各种网络信息、诊断和排除各种网络故障等方面起着至关重要的作用。



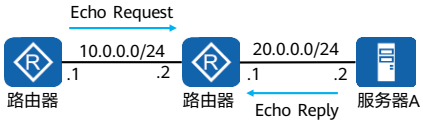
Type	Code	描述
0	0	Echo Reply
3	0	网络不可达
3	1	主机不可达
3	2	协议不可达
3	3	端口不可达
5	0	重定向
8	0	Echo Request

HUAWEI

- 为了更有效地转发IP数据报文和提高数据报文交互成功的机会，在网络层使用ICMP协议。ICMP允许主机或设备报告差错情况和提供有关异常情况的报告。
- ICMP消息封装在IP报文中，IP报文头部Protocol值为1时表示ICMP协议。
- ICMP字段解析：
  - ICMP消息的格式取决于Type和Code字段，其中Type字段为消息类型，Code字段包含该消息类型的具体参数。
  - Checksum校验和字段用于检查消息是否完整。
  - ICMP消息中包含32 bit的可变参数，这个字段一般不使用，通常设置为0。
    - 在ICMP重定向消息中，这个字段用来指定网关IP地址，主机根据这个地址将报文重定向到指定网关；
    - 在Echo请求消息中，这个字段包含标识符和序号，源端根据这两个参数将收到的回复消息与本端发送的Echo请求消息进行关联。尤其是当源端向目的端发送了多个Echo请求消息时，需要根据标识符和序号将Echo请求和回复消息进行一一对应。

ICMP差错检测

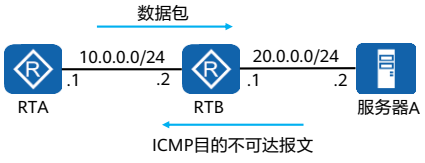
- ICMP Echo Request和ICMP Echo Reply消息常用于诊断源和目的地之间的网络连通性，同时还可以提供其他信息，如报文往返时间等。
- ICMP的一个典型应用是Ping。Ping是检测网络连通性的常用工具，同时也能够收集其他相关信息。用户可以在Ping命令中指定不同参数，如ICMP报文长度、发送的ICMP报文个数和等待回复响应的超时时间等，设备根据配置的参数来构造并发送ICMP报文，进行Ping测试。




```
[RTA] ping 20.0.0.2
  PING 20.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 20.0.0.2: bytes=56 Sequence=1  ttl=254 time=70 ms
    Reply from 20.0.0.2: bytes=56 Sequence=2  ttl=254 time=30 ms
    Reply from 20.0.0.2: bytes=56 Sequence=3  ttl=254 time=30 ms
    Reply from 20.0.0.2: bytes=56 Sequence=4  ttl=254 time=40 ms
    Reply from 20.0.0.2: bytes=56 Sequence=5  ttl=254 time=30 ms
  --- 20.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/40/70 ms
```

ICMP错误报告

- ICMP定义了各种错误消息，用于诊断网络连接性问题；根据这些错误消息，源设备可以判断出数据传输失败的原因。如当网络设备无法访问目标网络时，会自动发送ICMP目的不可达报文到发送端设备。
- Tracert基于报文头中的TTL值来逐跳跟踪报文的转发路径。Tracert是检测网络丢包和时延的有效手段，同时可以帮助管理员发现网络中的路由环路。



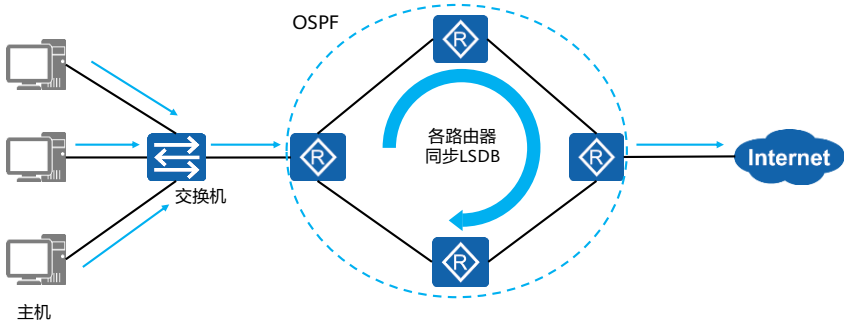

```
[RTA] tracert 20.0.0.2

traceroute to  20.0.0.2(20.0.0.2), max hops: 30,packet length:
40,press CTRL_C to break

1 10.0.0.2          80 ms    10 ms    10 ms

2 20.0.0.2          30 ms    30 ms    20 ms
```


HUAWEI

- ICMP定义了各种错误消息，用于诊断网络连接性问题；根据这些错误消息，源设备可以判断出数据传输失败的原因。
  - 如果网络中发生了环路，导致报文在网络中循环，且最终TTL超时，这种情况下网络设备会发送TTL超时消息给发送端设备；
  - 如果目的地不可达，则中间的网络设备会发送目的不可达消息给发送端设备。目的不可达的情况有多种，如果是网络设备无法找到目的网络，则发送目的网络不可达消息；如果网络设备无法找到目的网络中的目的主机，则发送目的主机不可达消息。
- ICMP的另一个典型应用是Tracert。Tracert基于报文头中的TTL值来逐跳跟踪报文的转发路径。为了跟踪到达某特定目的地址的路径，源端首先将报文的TTL值设置为1。该报文到达第一个节点后，TTL超时，于是该节点向源端发送TTL超时消息，消息中携带时间戳。然后源端将报文的TTL值设置为2，报文到达第二个节点后超时，该节点同样返回TTL超时消息，以此类推，直到报文到达目的地。这样，源端根据返回的报文中的信息可以跟踪到报文经过的每一个节点，并根据时间戳信息计算往返时间。

OSPF协议

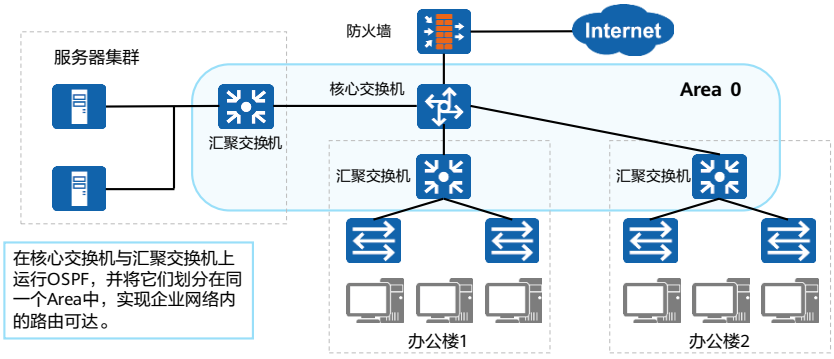
- 不同网络间的互通，需要通过路由实现。路由的获取方式有直连路由、静态路由、动态路由。动态路由因灵活性高、可靠性好、易扩展等特点被广泛应用于网络中。
- OSPF是企业网络中应用最广的动态路由协议。



- LSDB（Link State Database, 链路状态数据库），OSPF设备之间会同步链路状态信息，用于计算路由，保存这些信息的数据库就是LSDB。

OSPF区域

- OSPF Area用于标识一个OSPF的区域。
- 区域是从逻辑上将设备划分为不同的组，每个组用区域号（Area ID）来标识。
- 企业网络可以根据规模和需求规划为单区域或多区域组网。



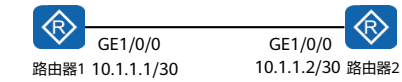
HUAWEI

- OSPF区域可以划分为骨干区域和非骨干区域。骨干区域为Area0，其他区域为非骨干区域。
- 大型企业网络中可以进行分层次的OSPF区域规划，如可以将出口设备和核心设备间规划为骨干区域Area0，核心设备和汇聚设备之间规划为非骨干区域，如Area10，Area20。

OSPF路由表

- 对于OSPF的路由表，需要了解：
  - OSPF路由表包含Destination、Cost和NextHop等指导转发的信息；
  - 使用命令display ospf routing查看OSPF路由表。

[R1]display ospf routing

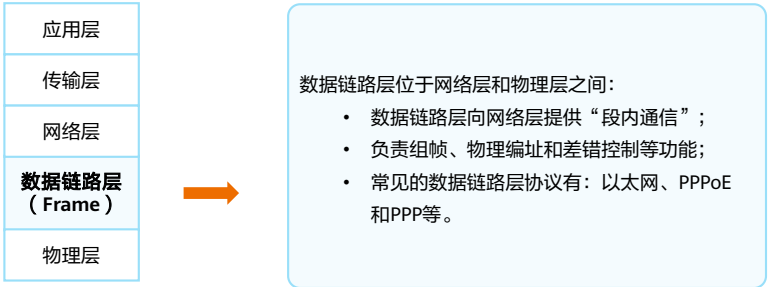



```
<R1> display ospf routing
OSPF Process 1 with Router ID 1.1.1.1
Routing Tables
Routing for Network
Destination        Cost  Type       NextHop         AdvRouter       Area
1.1.1.1/32         0     stub       1.1.1.1         1.1.1.1         0.0.0.0
10.1.1.0/20        1     Transit    10.1.1.1        1.1.1.1         0.0.0.0
2.2.2.2/32         1     stub       10.1.1.2        2.2.2.2         0.0.0.0

Total Nets: 3
Intra Area: 3  Inter Area: 0  ASE: 0  NSSA: 0
```

目录

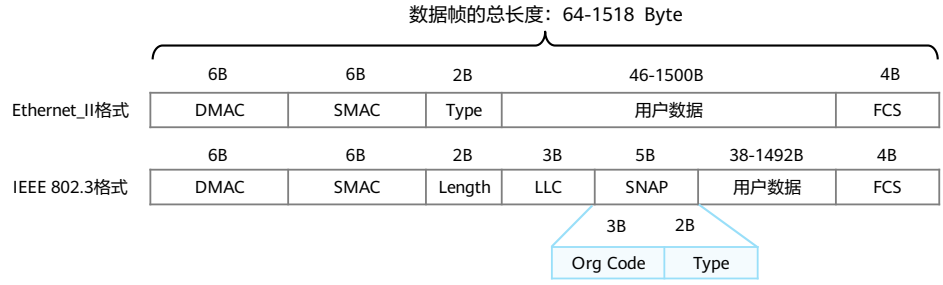
数据链路层

- 数据链路层位于网络层和物理层之间，可以向网络层的IP和IPv6等协议提供服务。
- 以太网（Ethernet）是最常见的数据链路层协议。



以太网帧结构

- 以太网技术所使用的帧为以太网帧（Ethernet Frame）。以太帧有Ethernet II格式和IEEE 802.3格式两个标准。
- MAC（Media Access Control）地址在网络中唯一标识一个网卡。MAC地址有48 bit，如00-1E-10-DD-DD-02。MAC地址用于同网段内的通信。



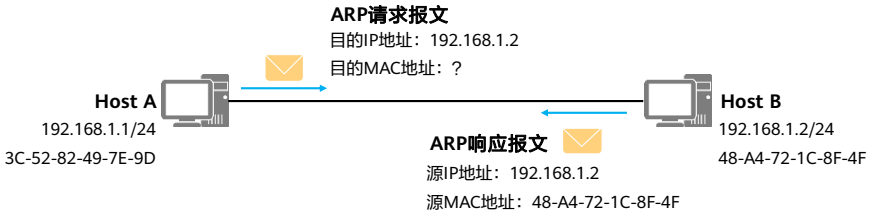
HUAWEI

- Ethernet II以太帧：
  - DMAC：6字节，目的MAC地址，该字段标识帧的接收者；
  - SMAC：6字节，源MAC地址，该字段标识帧的发送者；
  - Type：2字节，协议类型。常见值：
    - 0x0800：Internet Protocol Version 4（IPv4）；
    - 0x0806：Address Resolution Protocol（ARP）。
- IEEE 802.3 LLC以太帧：
  - SNAP：Sub-network Access Protocol，子网访问协议。SNAP由机构代码（Organization Code）和类型（Type）字段组成。
  - FCS：Frame Check Sequence，帧校验序列，这是一个32位的循环冗余校验码，主要用于校验二层数据帧在传输过程中是否发生差错
  - 逻辑链路控制LLC（Logical Link Control）由目的服务访问点DSAP（Destination Service Access Point）、源服务访问点SSAP（Source Service Access Point）和Control字段组成。
    - DSAP：1字节，目的服务访问点，若后面类型为IP，该字段值设为0x06。服务访问点的功能类似于Ethernet II帧中的Type字段或TCP/UDP传输协议中的端口号；
    - SSAP：1字节，源服务访问点，若后面类型为IP，该字段值设为0x06；

- Ctrl：1字节，该字段值通常设为0x03，表示无连接服务的IEEE 802.2无编号数据格式。

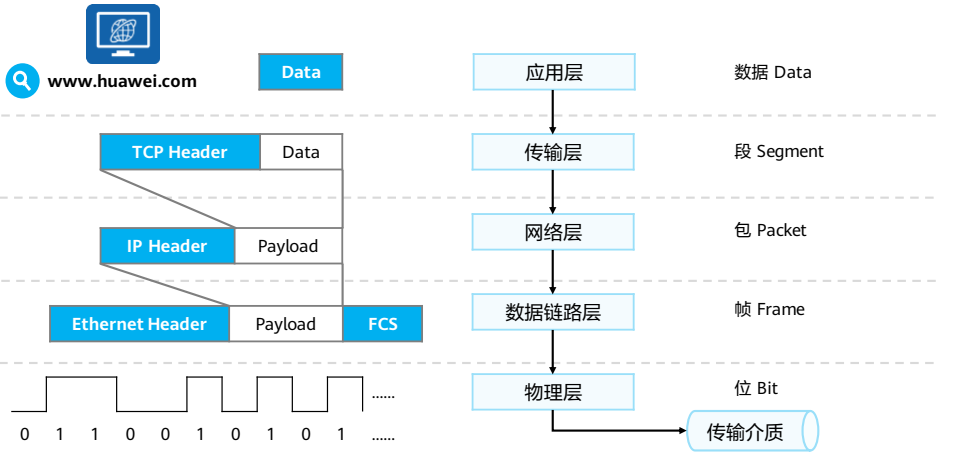
地址解析协议（ARP）

- 要使IP报文能够正常转发，还需要知道目的地址或者网关的MAC地址，这是就需要用到ARP（ Address Resolution Protocol ）地址解析协议：根据已知的IP地址解析获得其对应的MAC地址。



- ARP（ Address Resolution Protocol，地址解析协议 ）是根据IP地址获取数据链路层地址的一个TCP/IP协议。
- ARP是IPv4中必不可少的一种协议，它的主要功能是：
  - 将IP地址解析为MAC地址；
  - 维护IP地址与MAC地址的映射关系的缓存，即ARP表项；
  - 实现网段内重复IP地址的检测。

发送方数据封装

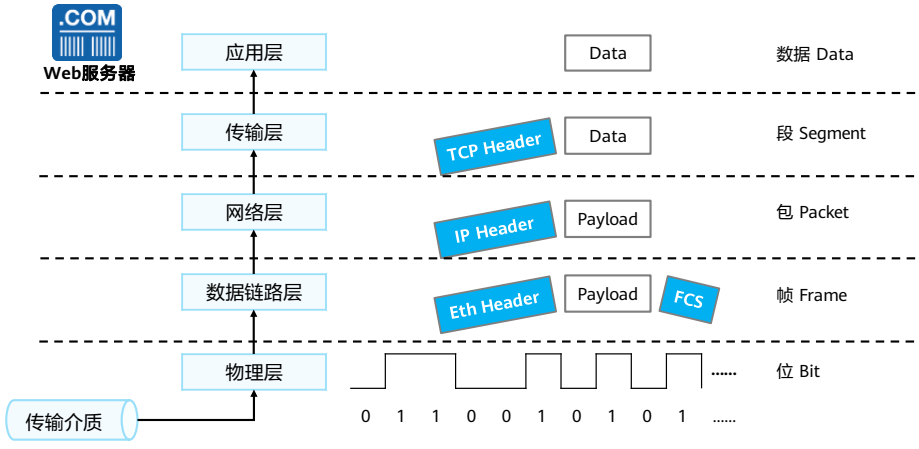


HUAWEI

- 假设你正在通过网页浏览器访问华为官网，当你输入完网址，敲下回车后，计算机内部会发生下列事情：
  - IE浏览器（应用程序）调用HTTP（应用层协议），完成应用层数据的封装（图中Data还应包括HTTP头部，此处省略）；
  - HTTP依靠传输层的TCP进行数据的可靠性传输，将封装好的数据传递到TCP模块；
  - TCP模块给应用层传递下来的Data添加上相应的TCP头部信息（源端口、目的端口等）。此时的PDU被称作Segment（段）；
  - 在IPv4网络中，TCP模块会将封装好的Segment传递给网络层的IPv4模块（若在IPv6环境，会交给IPv6模块进行处理）；
  - IPv4模块在收到TCP模块传递来的Segment之后，完成IPv4头部的封装，此时的PDU被称为Packet（包）；
  - 由于使用了Ethernet作为数据链路层协议，故在IPv4模块完成封装之后，会将Packet交由数据链路层的Ethernet模块（例如以太网卡）处理；
  - Ethernet模块在收到IPv4模块传递来的Packet之后，添加上相应的Ethernet头部信息和FCS帧尾，此时的PDU被称为Frame（帧）；
  - 在Ethernet模块封装完毕之后，会将数据传递到物理层；

- 根据物理介质的不同，物理层负责将数字信号转换成电信号，光信号，电磁波（无线）信号等；
- 转换完成的信号在网络中开始传递。

接收方数据解封装



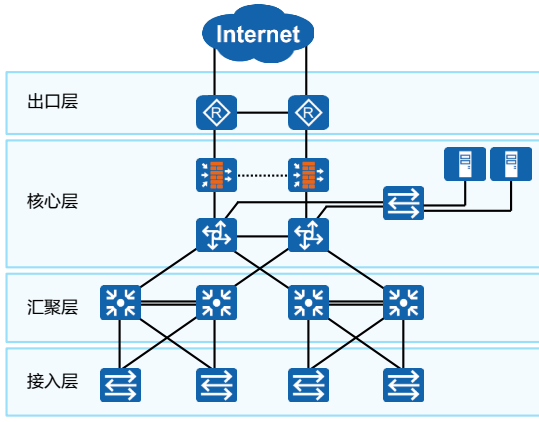
HUAWEI

- 经过网络传递之后，数据最终到达目的服务器。根据不同的协议头部的信息，数据将被一层层的解封装并做相应的处理和传递，最终交由Web服务器上的应用程序进行处理。

目录

企业园区网络典型架构

- 以下典型的企业园区网络组网，由交换机、路由器、防火墙和服务器组成。

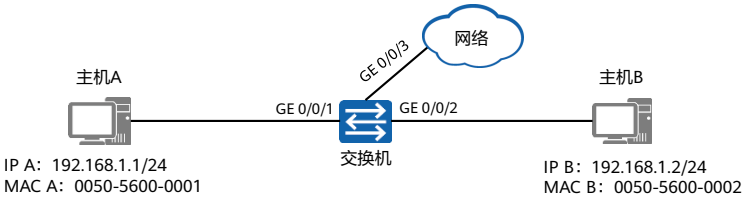


HUAWEI

- 一个典型的园区数据网络由路由器、交换机、防火墙等设备构成，通常会采用多层架构，包括：接入层、汇聚层、核心层和出口层。
- 交换机：同网段或跨网段通信设备。
- 路由器：跨网段通信设备。
- 防火墙：可部署在网络出口处进行防护。

交换机

- 交换机是距离终端用户最近的设备，用于终端接入网络，并且可以使数据帧在同一网段内转发。
- 交换机工作在数据链路层，根据MAC地址表转发数据帧。MAC地址表中存放了MAC地址与交换机端口之间的映射关系。



主机A发出的数据帧

源地址	目的地址
源MAC：MAC A	目的MAC：MAC B
源IP：IP A	目的IP：IP B

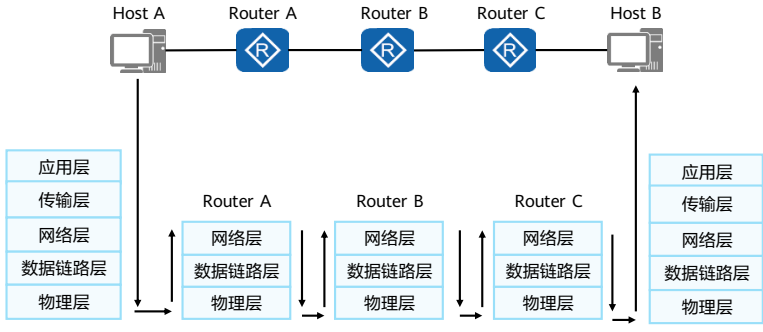
交换机的MAC地址表

MAC地址	Port
MAC A	GE0/0/1
MAC B	GE0/0/2
...	...

- 二层交换机工作在数据链路层，它对数据帧的转发是建立在MAC地址基础之上的。交换机不同的接口发送和接收数据是独立的，各接口属于不同的冲突域，因此有效地隔离了网络中的冲突域。
- 二层交换设备通过学习以太网数据帧的源MAC地址来维护MAC地址与接口的对应关系（保存MAC与接口对应关系的表称为MAC地址表），通过其目的MAC地址来查找MAC地址表决定向哪个接口转发。

路由器

- 路由器工作在网络层，使报文能够在不同网络间转发。

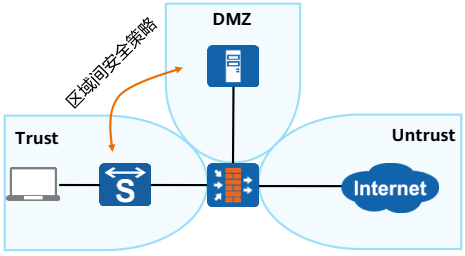


HUAWEI

- 路由器是网络层设备，其主要功能是实现报文在不同网络之间的转发。如图所示，位于不同网络（即不同链路）上的Host A和Host B之间相互通信。与Host A在同一网络（即同一链路）上的路由器接口接收到Host A发出的数据帧，路由器的链路层分析帧头确定为发给自己的帧之后，发送给网络层处理，网络层根据网络层报文头以决定目的地址所在网段，然后通过查表从相应的接口转发给下一跳，直到到达报文的目的地Host B。

防火墙

- 防火墙是对网络的访问行为进行控制的一种设备，安全防护是其核心特性，主要部署在网络边界。
- 防火墙认为在同一安全区域内部发生的数据流动是不存在安全风险的，不需要实施任何安全策略。只有当不同安全区域之间发生数据流动时，才会触发设备的安全检查，并实施相应的安全策略。

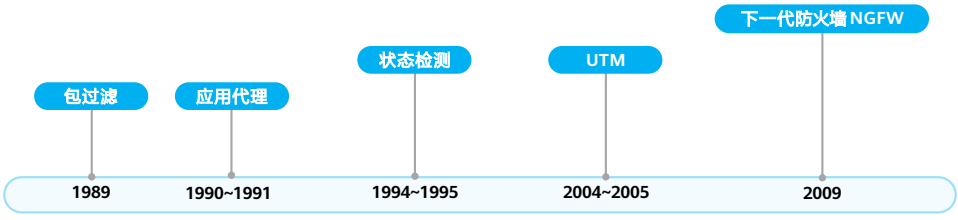


区域名称	默认安全优先级
非受信区域（Untrust）	低安全级别区域，优先级为5。
非军事化区域（DMZ）	中等安全级别区域，优先级为50。
受信区域（Trust）	较高安全级别区域，优先级为85。
本地区域（Local）	Local区域定义的是设备本身，例如设备的接口。Local区域是最高安全级别区域，优先级为100。

- 防火墙技术是计算机网络安全中不可或缺的一种技术，能够为计算机网络安全提供有效保护，对于一些应用范围较大的网络使用环境，将防火墙技术运用到计算机网络系统中，能够对累积的数据信息进行有效保护。硬件防火墙用来集中解决网络安全问题，可以适合各种场合，同时能够提供高效率的“过滤”。同时它可以提供包括访问控制、身份验证、数据加密、VPN技术、地址转换等安全特性，用户可以根据自己的网络环境的需要配置复杂的安全策略，阻止一些非法的访问，保护自己的网络安全。

防火墙的发展历史

- 随着科技的进步，防火墙的发展历史经历了从低级到高级、从功能简单到功能复杂的过程。网络技术的不断发展和越来越多的需求不断推动着防火墙的更新。
- 根据发展历史可以将防火墙分为：
  - 包过滤防火墙
  - 状态检测防火墙
  - 下一代防火墙



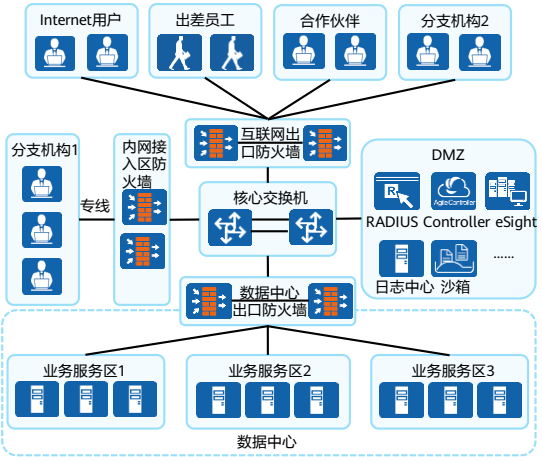
HUAWEI

- 最早的防火墙可以追溯到20世纪80年代，在这二十年多年间，防火墙的发展过程大致划分为以下3个时期：
  - 第一时期（1989年至1994年）：1989年产生了包过滤防火墙，能实现简单的访问控制，我们称之为第一代防火墙。随后出现了代理防火墙，在应用层代理内部网络和外部网络之间的通信，属于二代防火墙。1994 年 CheckPoint公司发布了基于状态检测技术的防火墙,通过动态分析报文的状态来决定对报文采取的动作，不需要为每个应用程序都进行代理，处理速度快而且安全性高。状态检测防火墙被称为第三代防火墙。
  - 第二时期（1995年至2004年）：防火墙开始增加一些其他功能，如VPN功能。同时出现了专门保护Web服务器安全的WAF（Web Application Firewall，Web应用防火墙）设备。2004年业界提出了UTM（United Threat Management，统一威胁管理）的概念，将传统防火墙、入侵检测、防病毒、URL过滤、应用程序控制、邮件过滤等功能融合到一台防火墙上，实现全面的安全防护。

- 第三时期（2005年至今）：2004年后，UTM市场得到了快速的发展，UTM产品如雨后春笋般涌现，但面临新的问题。首先是对应用层信息的检测程度受到限制，此时就需要更高级的检测手段，这使得DPI（Deep Packet Inspection，深度报文检测）技术得到广泛应用。其次是性能问题，多个功能同时运行，UTM设备的处理性能将会严重下降。2008年业界发布了下一代防火墙，解决了多个功能同时运行时性能下降的问题。同时，还可以基于用户、应用和内容来进行管控。2009年业界对下一代防火墙进行了定义，明确下一代防火墙应具备的功能特性。随后各个安全厂商也推出了各自的下一代防火墙产品，防火墙进入了一个新的时代。

防火墙功能

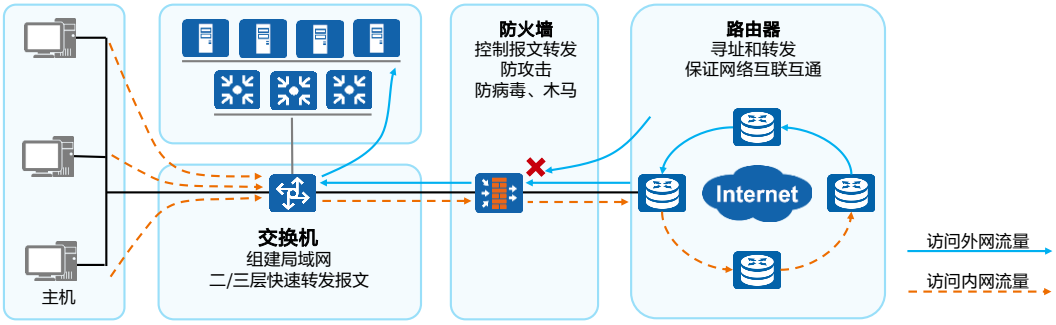
- 防火墙主要用于保护一个网络免受来自另一个网络的攻击和入侵。因其隔离、防守的属性，防火墙灵活应用于企业网络出口、大型网络内部子网隔离和数据中心边界等场景。
- 防火墙可以实现的功能如下：
  - 隔离不同安全级别的网络；
  - 实现不同安全级别网络之间的访问控制（安全策略）；
  - 用户身份认证；
  - 实现远程接入功能；
  - 实现数据加密及虚拟专用网业务；
  - 执行网络地址转换；
  - 其他安全功能。



HUAWEI

防火墙与交换机、路由器的对比

- 交换机通常用来组建局域网，路由器用来连接不同的网络，而防火墙主要部署在网络边界。
- 路由器与交换机的本质是转发，防火墙的本质是控制。



HUAWEI

- 防火墙与路由器、交换机的区别：
  - 路由器与交换机本质是转发，而防火墙的本质是控制；
  - 路由器用来连接不同的网络，通过路由协议保证互联互通，确保将报文转发到目的地；
  - 交换机通常用来组建局域网，作为局域网通信的重要枢纽，通过二层/三层交换快速转发报文；
  - 防火墙主要部署在网络边界，对进出网络的访问行为进行控制，安全防护是其核心特性。

网络设备登录和配置

- 不管是部署、操作或是维护网络设备，都会涉及到对网络设备的配置。配置之前，需要先登录设备。
- 管理员对网络设备的配置，有命令行和Web界面两种方式。

Console登录 **Telnet登录** **SSH登录**

```
Username: admin
Password: Admin@123
Info: The max number of VTY users is 21, the number of
current VTY users online is 0, and total number of terminal
users online is 1.
<FW> display this
#
sysname FW
#
 command-privilege level 0 view system interface
#
 Return
```

Web登录

HUAWEI

- 防火墙默认登录接口GigabitEthernet0/0/0，也称为MGMT接口。
- Web登录
  - 缺省网址：https://192.168.0.1:8443（或http://192.168.0.1）；
  - 缺省用户名：admin；
  - 缺省密码：Admin@123。

基本配置命令（1）

- 配置接口IP地址

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1] ip address 10.102.0.1 255.255.255.0
```

用来给设备上的物理或逻辑接口配置IP地址。

- 查看当前运行的配置

```
<FW> display current-configuration
```

- 配置文件保存

```
<FW> save
```

- 查看保存的配置

```
<FW> display saved-configuration
```


- 要在接口运行IP服务，必须为接口配置一个IP地址。一个接口一般只需要一个IP地址，如果接口配置了新的主IP地址，那么新的主IP地址就替代了原来的主IP地址。
- 用户可以利用命令ip address *ip-address* { *mask* | *mask-length* } [sub]为接口配置IP地址，这个命令中，mask代表子网掩码，如255.255.255.0，mask-length 代表的是掩码长度，如24。这两者任取其一均可。
- Loopback接口是一个逻辑接口，可用来虚拟一个网络或者一个IP主机。在运行多种协议的时候，由于Loopback接口稳定可靠，所以也可以用来做管理接口。
- 在给物理接口配置IP地址时，需要关注该接口的物理状态。默认情况下，华为路由器和交换机的接口状态为up；如果该接口曾被手动关闭，则在配置完IP地址后，应使用undo shutdown命令打开该接口。

基本配置命令 (2)

- 清除已保存的配置

```
<FW> reset saved-configuration
```

- 查看系统启动配置参数

```
<FW> display startup
```

用来查看设备本次及下次启动相关的系统软件、备份系统软件、配置文件、License文件、补丁文件以及语音文件。

- 配置系统下次启动时使用的配置文件

```
<FW> startup saved-configuration configuration-file
```

设备升级时，可以通过此命令让设备下次启动时加载指定的配置文件。

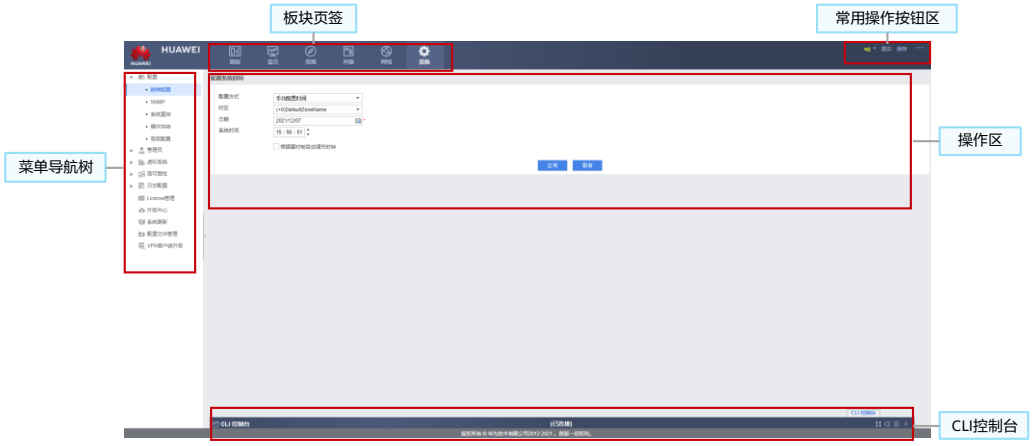
- 配置设备重启

```
<FW> reboot
```


- reset saved-configuration命令用来清除配置文件或配置文件中的内容。执行该命令后，如果不使用命令startup saved-configuration *configuration-file*重新指定设备下次启动时使用的配置文件，也不使用save命令保存当前配置，则设备下次启动时会采用缺省的配置参数进行初始化。
- display startup命令用来查看设备本次及下次启动相关的系统软件、备份系统软件、配置文件、License文件、补丁文件以及语音文件。
- startup saved-configuration *configuration-file*命令用来指定系统下次启动时使用的配置文件，*configuration-file*参数为系统启动配置文件的名称。
- reboot命令用来重启设备，重启前提示用户是否保存配置。

图形化界面（1）

- 防火墙图形化界面分为以下几部分：板块页签、菜单导航树、操作区、常用操作按钮区及CLI控制台。



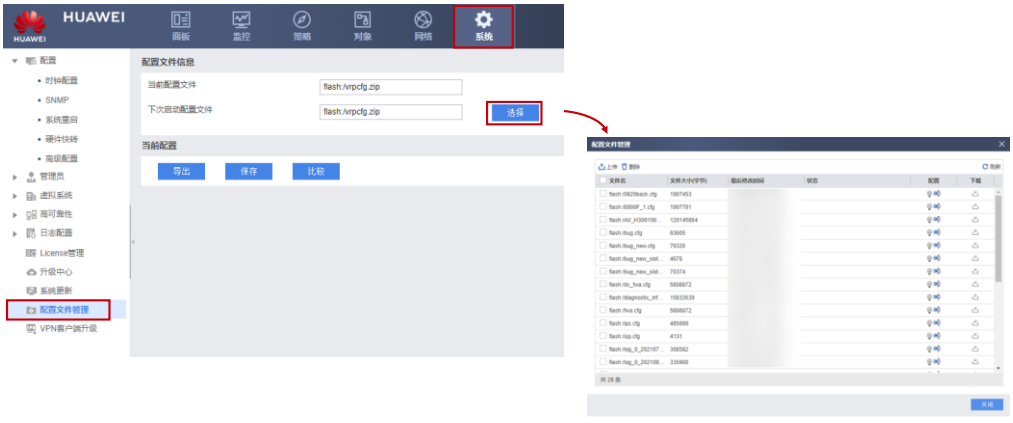
图形化界面（2）

- 图形化界面中的板块页签对防火墙的各种功能进行了分类显示，是通过Web界面配置防火墙时经常要用到的部分。

板块	说明
面板	直观、快速查看设备的常用状态信息，监测系统是否正常运行。
监控	查看日志信息、查看统计信息、诊断设备故障，提供全方位的运维手段。
策略	配置安全策略、带宽策略等各种业务策略，控制流量转发，防范网络威胁。
对象	配置地址对象、服务对象等被各种业务策略引用的公共元素，简化业务配置。
网络	配置接口、路由、VPN等网络互通功能，是设备接入网络的基础。
系统	配置管理员、时钟、SNMP、系统升级等设备管理功能，是系统正常工作的基础。

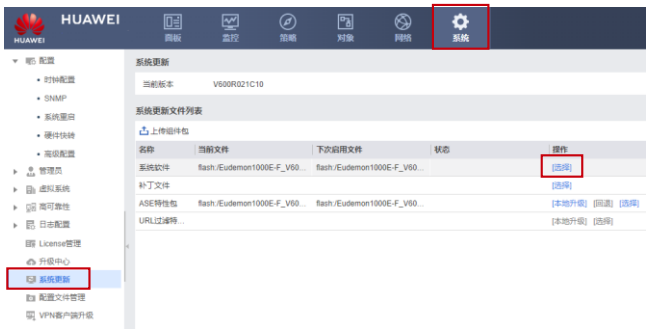
配置文件管理

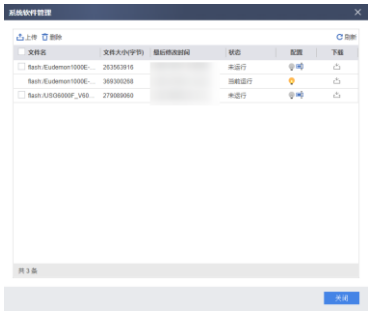
- 在“系统 > 配置文件管理”，可以查看当前配置文件，以及设置下一次启动配置文件。



版本升级

- 在“系统 > 系统更新”，可以对防火墙的系统软件、补丁文件、特性包进行升级。





思考题

1. （多选题）以下哪些选项属于应用层的协议？（　　）
   A. HTTP
   B. DNS
   C. FTP
   D. OSPF
2. （判断题）FTP主动模式下的数据连接由客户端发起。（　　）
   A. 正确
   B. 错误

1. ABC
2. B

本章总结

- 本课程简要介绍了TCP/IP参考模型的五层结构，包括应用层、传输层、网络层、数据链路层、物理层。每一层为其上一层提供服务，各层次都有对应的协议。并描述了一些常见的协议，如ARP、ICMP、FTP以及HTTPS等。
- 本课程描述了典型企业网络架构，对常见的网络设备，如交换机、路由器、防火墙进行了介绍。并讲解了防火墙的命令行和Web界面两种配置方式。

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

缩略语表（1）

缩略语	英文全称	解释
ACK	Acknowledge	应答消息
ARP	Address Resolution Protocol	地址解析协议
C/S	Client/Server	客户服务器模型
CLI	Command Line Interface	命令行视图
FIN	Finish	结束消息
FTP	File Transfer Protocol	文件传输协议
HTTP	Hyper Text Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure	加密的超文本传输协议
ICMP	Internet Control Message Protocol	互联网控制消息协议
IGMP	Internet Group Management Protocol	因特网组管理协议
IP	Internet Protocol	网际互连协议

缩略语表 (2)

缩略语	英文全称	解释
IS-IS	Intermediate System to Intermediate System	中间系统到中间系统协议
MAC	Media Access Control	媒体介入控制
OSI	Open Systems Interconnection	开放系统互联
PPP	Point-to-Point Protocol	点对点协议
PPPoE	Point-to-Point Protocol over Ethernet	以太网承载PPP协议
SFTP	Secure File Transfer Protocol	安全文件传输协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SSH	Secure Shell Protocol	安全外壳协议
STelnet	Secure Telnet	安全Telnet
SYN	Synchronize Sequence Numbers	同步序列编号
TCP	Transmission Control Protocol	传输控制协议

缩略语表 (3)

缩略语	英文全称	解释
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TLS	Transport Layer Security	传输层安全性协议
TTL	Time To Live	生存时间
UDP	User Datagram Protocol	用户数据包协议
URL	Universal Resource Locator	统一资源定位符
UTM	United Threat Management	统一威胁管理
VPN	Virtual Private Network	虚拟专用网
WAF	Web Application Firewall	Web应用防火墙
WWW	World Wide Web	万维网
OSPF	Open Shortest Path First	开放式最短路径优先
LSDB	Link State Database	链路状态数据库

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

常见网络安全威胁及防范

HUAWEI

前言

- 随着互联网技术的发展，网络攻击类型与频率也不断增长。信息及信息系统由于具备脆弱性、敏感性和机密性等多种特性，易遭受到来自不同手段的威胁或攻击，比如DDoS攻击、网络入侵、数据泄露和中间人攻击等。只有了解各种威胁来源及其应对方式，才能更好地保障信息系统的安全。
- 企业网络实现了企业内部的数据传输及企业内部与外部的数据交互。企业网络的安全性对保证企业的安全生产至关重要。本章将以企业网络为场景介绍常见的网络安全威胁及应对方式。

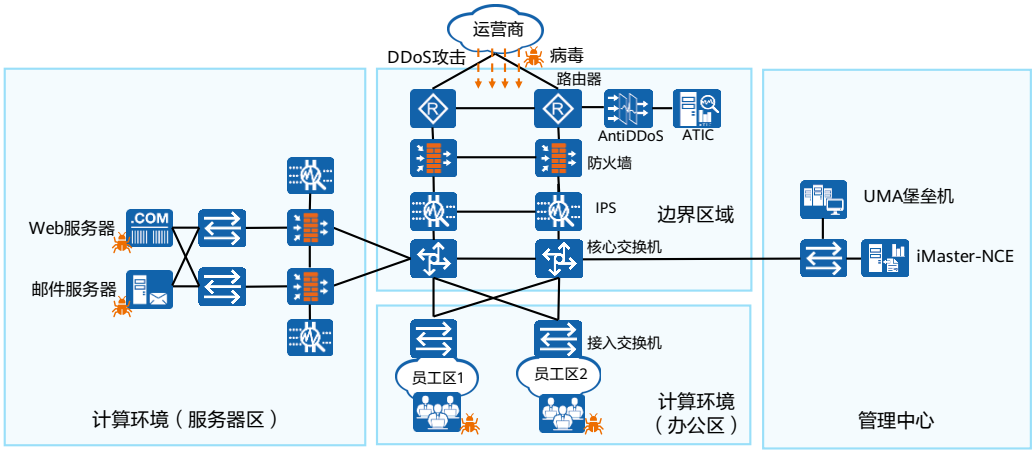
目标

- 学完本课程后，您将能够：
  - 描述企业网络受到的常见网络安全威胁
  - 描述常见网络安全威胁的应对方式

目录

企业网络安全威胁概览（1）

- 企业存在来自内部和外部的安全威胁，下图是一张典型的企业网络架构图：

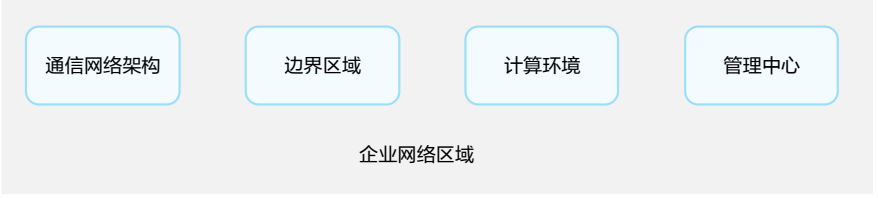


HUAWEI

- 企业网络的安全威胁来源大致可以分为以下几部分：
  - 外部威胁：来自企业网络外部的安全威胁，如DDoS攻击，病毒、木马、蠕虫等网络入侵，网络扫描，垃圾邮件，钓鱼邮件，针对Web服务器的攻击等；
  - 内部威胁：网络结构不可靠，网络未隔离，终端存在漏洞，员工行为不受控，信息安全违规操作，信息泄露，恶意员工，权限管理混乱，非法接入等。

企业网络安全威胁概览（2）

- 企业通常采取管理和技术两方面的措施规避安全风险，在管理上，通常制定各类安全制度、运维要求或应急流程，以提升员工的安全意识。
- 安全意识是一切防御手段的基础，针对全体员工定期展开安全意识培训，明确安全制度与规则，可以帮助企业避免大部分由于误操作引起的信息泄露或其他信息安全事件。
- 为了有针对性地防范企业网络安全威胁，企业工程师会根据威胁来源将网络划分为不同区域：



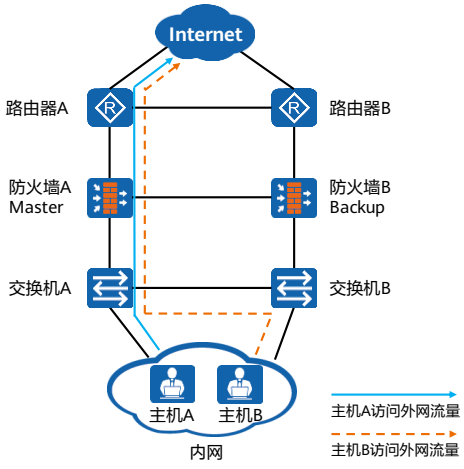
- 企业网络不同区域的安全威胁及防范措施：
  - 通信网络架构：具备高可靠性保障业务的正常运行；部署VPN等措施保障数据传输的机密性与完整性；
  - 边界区域：部署AntiDDoS方案应对DoS攻击；部署防火墙设备起到网络隔离及流量控制的目的；IPS设备则用于防范外网的病毒、入侵等威胁；
  - 计算环境：对终端进行安全加固，防范漏洞带来的威胁；部署IPS设备应对外网的入侵行为；部署终端IPS或杀毒软件应对病毒入侵；
  - 管理中心：通过堡垒机管控管理员的权限，降低恶意操作带来的影响，监控运维操作，做到运维过程可回溯；iMaster-NCE管控员工权限，降低信息泄露的风险，同时防范非法接入。
- 上述网络方案中部署了如下网络设备：
  - 路由器：同网段或跨网段通信设备，用于转发流量，构成网络的基础设备，我们将在《网络基础知识》章节中详细介绍路由器；
  - 交换机：同网段通信设备，用于转发流量，构成网络的基础设备，我们将在《网络基础知识》章节中详细介绍交换机；
  - 防火墙：最常见的安全设备，通常部署在企业出口处用于网络隔离或流量控制，我们将在《网络基础知识》章节中详细介绍防火墙设备；

- IPS设备：专业的入侵防御设备，通常部署在出口区域防火墙的后端，用于防范去往内网的安全威胁，在中大型企业中较为常见；
- AntiDDoS设备：专业的DDoS防御设备，主要用于大型企业，如银行、互联网公司等DDoS重灾区，价格昂贵；
- UMA堡垒机：专业的运维审计设备，主要用于管控管理员的操作权限及监控操作过程，企业通常根据需要部署；
- iMaster-NCE：企业中常见的准入控制设备，常与交换机/防火墙组成准入控制方案，对员工进行身份认证、授权访问资源及审计上网行为。

目录

需求1 - 网络架构可靠性

- 从第三级等级保护（监督保护级）开始，安全通信网络部分中网络架构要求：应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
- 防火墙作为企业出口区域的关键设备，应该具备高可靠性，不仅是线路的高可靠性，也需要保障设备的高可靠性。右图所示为防火墙高可靠组网方式。

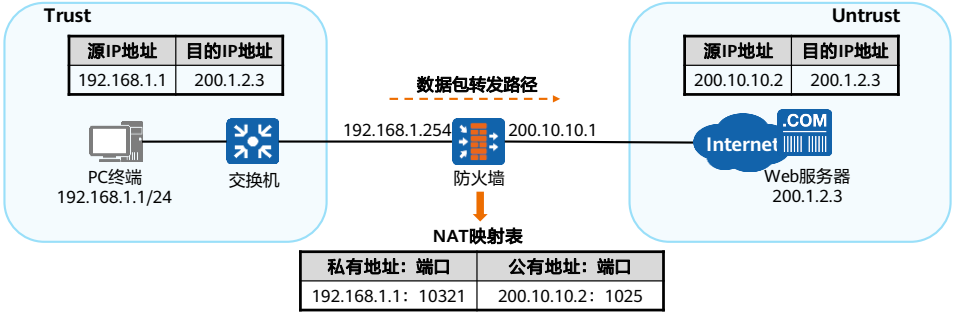


HUAWEI

- 防火墙双机热备的情况下，流量如何转发，业务的高可靠性如何保障？我们将在《防火墙双机热备技术》里详细介绍。

需求2 – 区域隔离

- 企业网络资源不能直接暴露在公网中，以免遭受来自互联网的猛烈攻击。此外，互联网中的不法份子可能通过IP地址扫描或其他方式探测企业网络，便于进行下一步的攻击。
- 通常在出口处部署防火墙，防火墙通过将所连接的不同网络分隔在不同安全区域隔离内外网，而通过在防火墙上部署地址转换技术，可以在一定程度上隐藏内网IP地址，保护内部网络。

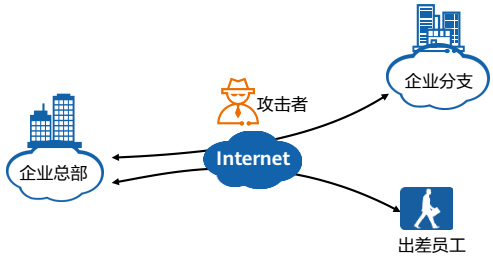


HUAWEI

- 安全区域：防火墙的基本机制，不同安全区域不能直接通信，以此起到隔离网络的作用，若要放通不同区域的流量，则需要配置安全策略，有关安全区域和安全策略的原理将在《防火墙安全策略》章节中具体阐述。
- 地址转换技术：通过将多个内网地址转换为1个或多个公网地址，对公网用户来说，只能看到发送方或接收方的公网地址，以此起到隐藏内网结构的作用。有关地址转换技术的原理，将在《防火墙网络地址转换技术》章节中具体阐述。

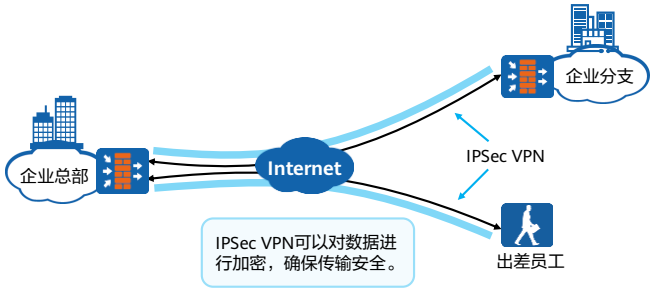
需求3 - 信息保密性

- 企业有出差员工，或者大型企业有多个分支机构。出差员工和企业总部，企业分支和企业总部之间在不安全的Internet上进行数据传输时，可能存在数据被窃取或篡改的风险，原因在于：
  - 企业数据传输本身未加密或加密程度不够；
  - 中间人攻击（Man-in-the-Middle Attack）：指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。在中间人攻击中，攻击者可以拦截通讯双方的通话并插入新的内容。



信息保密性安全方案

- 由于Internet的开放性，导致企业和其分支机构在Internet上传输数据的安全性无法保证，可以使用VPN技术在Internet上构建安全可靠的传输隧道。对于有经济实力和有高安全高可靠性要求的企业，还可以通过向运营商购买专线的方式，满足总部与分支机构之间的互联需求。
- 对于出差员工，可以使用L2TP over IPSec，SSL VPN等方式安全地接入公司网络。



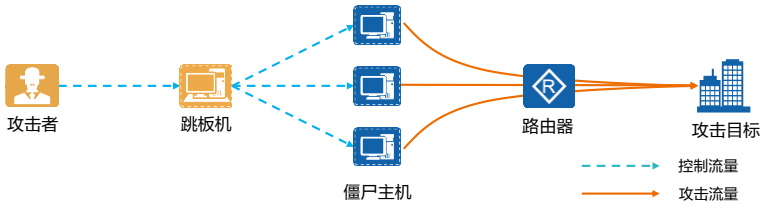
HUAWEI

- VPN技术的原理与配置将在《加密技术应用》中详细介绍。

目录

威胁1 - DDoS攻击

- DDoS攻击是指攻击者通过控制大量僵尸主机，向攻击目标发送大量攻击报文，导致被攻击目标所在网络的链路拥塞，系统资源耗尽，从而无法向正常用户提供服务。
- 有些恶意竞争对手会使用DDoS攻击，对正常合法企业造成较大经济损失。如在购物节期间对网上购物平台发动的DDoS攻击。



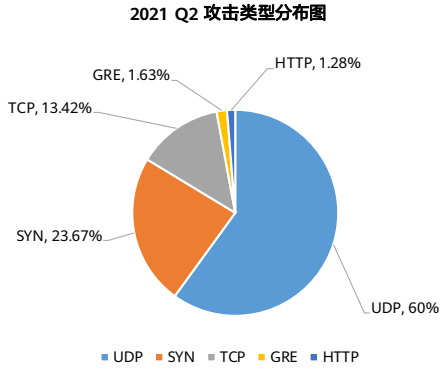
HUAWEI

- 随着越来越多的IoT设备接入网络，黑客利用设备硬件或管理漏洞就可以迅速发起一次大规模的DDoS攻击。而且，一些攻击开始呈现出揣摩人们行为习惯的趋势，而这样的攻击效果就越来越显著。

DDoS攻击种类

- 根据攻击报文类型的不同，可以分为TCP Flood、UDP Flood、ICMP Flood、HTTP Flood和GRE Flood等。

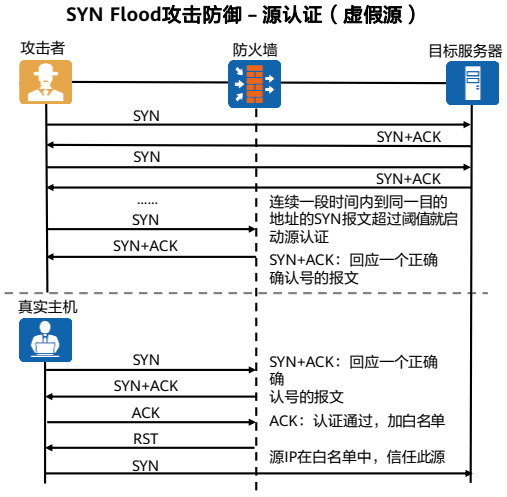
攻击类型	描述
TCP Flood	利用TCP协议发起的DDoS攻击，常见的攻击有SYN Flood，SYN+ACK Flood，ACK Flood，FIN/RST Flood等。
UDP Flood	使用UDP协议发起的攻击，常见攻击有UDP Flood，UDP分片攻击等。
ICMP Flood	利用ICMP协议在短时间内发送大量的ICMP报文导致网络瘫痪，或采用超大报文攻击导致网络链路拥塞。
HTTP Flood	利用HTTP协议交互，发动HTTP Flood，或者HTTP慢速攻击等。
GRE Flood	利用GRE报文发动的DDoS攻击，利用GRE报文的解封装消耗攻击目标的计算资源。



源自《kaspersky securelist-DDoS attacks in Q2 2021》

DDoS攻击安全防范

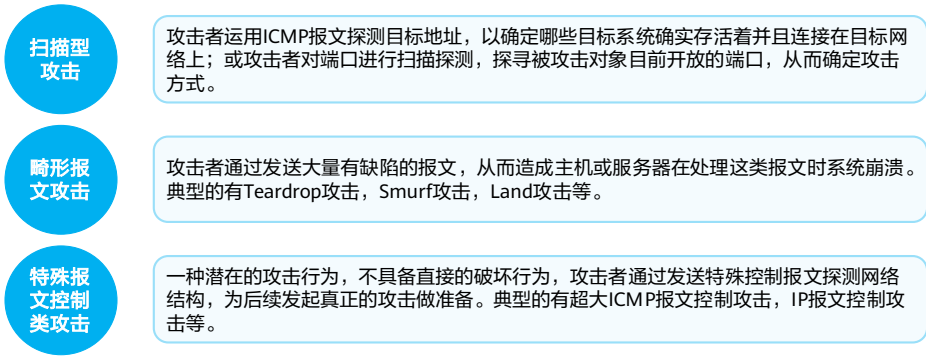
- 对于不同类型的DDoS攻击，AntiDDoS设备有源认证、限流等不同的防御方式，右图描述SYN Flood源认证防御的工作原理。
- SYN Flood攻击是通过伪造一个源地址的SYN报文，发送给受害主机，受害主机回复SYN+ACK报文给这些地址后，不会收到ACK报文，导致受害主机保持了大量的半连接，直到超时。这些半连接可以耗尽主机资源，使受害主机无法建立正常TCP连接，从而达到攻击的目的。



- 通过在企业网络出口部署防火墙或者专业AntiDDoS设备，阻断来自外部的DDoS攻击。对于需要防范大流量DDoS攻击的场景，也可以选择专业的AntiDDoS设备。
- 防火墙和AntiDDoS设备同时部署时，DDoS设备要部署在防火墙之前，有些防火墙虽然具有AntiDDoS功能，但是面对大流量DDoS攻击，有可能导致防火墙性能消耗很大，产生宕机等异常。
- 在TCP/IP协议中，TCP协议提供可靠的连接服务，采用三次握手建立一个连接。而SYN Flood攻击则是攻击者通过伪造大量的SYN发送给受害者， 且不会完成三次握手。
- SYN flood攻击是虚假源攻击的典型代表，此类攻击的最显著特点就是发送海量变源或变源端口的报文到受害主机，耗尽受害主机资源或网络资源。AntiDDoS设备通过对报文源的真实性检查来防御SYN Flood攻击。

威胁2 - 单包攻击

- 单包攻击不像DDoS攻击通过使网络拥塞，或消耗系统资源的方式进行攻击，而是通过发送有缺陷的报文，使主机或服务器在处理这类报文时系统崩溃，或发送特殊控制报文、扫描类报文探测网络结构，为真正的攻击做准备。



HUAWEI

- 扫描型攻击
  - IP Scan：利用IP地址扫描工具探测目标地址，确定目标系统是否存活。
- 畸形报文攻击
  - Smurf攻击：发送ICMP请求，该请求包的目标地址设置为受害网络的广播地址，源地址为服务器地址。该网络的所有主机都回应此ICMP请求，回应报文全部发往服务器，导致服务器不能正常提供服务。
- 特殊报文控制类攻击：
  - Tracert报文攻击：攻击者利用TTL为0时返回的ICMP超时报文，和到达目的地址时返回的ICMP端口不可达报文来发现报文到达目的地所经过的路径，它可以窥探网络的结构。
- 单包攻击与DDoS都属于DoS攻击。

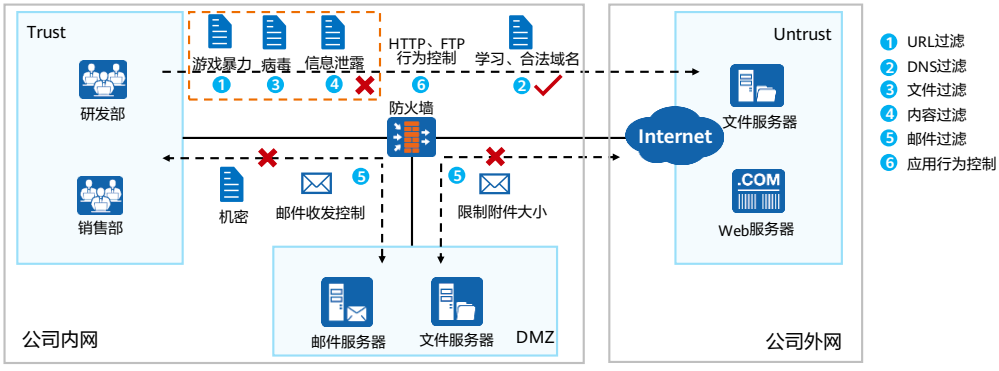
单包攻击安全防范

- 防火墙具有单包攻击防范功能，可以对扫描类攻击、畸形报文攻击和特殊报文控制类攻击进行有效防范。
- 不同单包攻击的原理不同，防火墙采用的防范原理也不同。以下对地址扫描攻击原理和其防范原理进行介绍。

- Rate：同一源IP每秒发往不同目的地址的ICMP报文数量。

威胁3 – 用户行为不受控

- 70%的信息安全事件是由于内部员工误操作或安全意识不够引起的。在加强员工安全意识的同时，企业也需要在技术层面管控员工访问外网的行为，不仅可以通过iMaster-NCE管控用户的访问权限，还可以通过防火墙的内容过滤功能管控用户的上网行为。



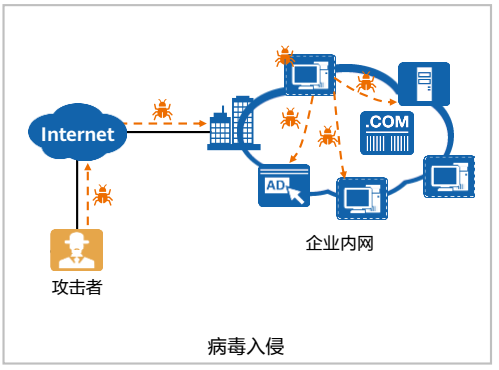
HUAWEI

- 企业也需要在技术层面管控员工访问外网的行为，比如不允许访问黄赌毒网站，防止对企业带来不良影响；上班时间不能访问语音娱乐网站，提高工作效率；又比如通过技术手段防范员工无意泄露个人或公司重要信息的行为。
- 内容安全过滤：
  - URL（Uniform Resource Locator）过滤可以对员工访问的URL进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的；
  - DNS过滤在域名解析阶段进行控制，防止员工随意访问非法或恶意的网站，带来病毒、木马和蠕虫等威胁攻击；
  - 文件过滤通过阻断特定类型的文件传输，可以降低内部网络执行恶意代码和感染病毒的风险，还可以防止员工将公司机密文件泄漏到互联网；
  - 内容过滤包括文件内容过滤和应用内容过滤。文件内容过滤是对用户上传和下载的文件内容中包含的关键字进行过滤。管理员可以控制对哪些应用传输的文件以及哪种类型的文件进行文件内容过滤。应用内容过滤是对应用协议中包含的关键字进行过滤。针对不同应用，设备过滤的内容不同；
  - 邮件过滤：通过检查发件人和收件人的邮箱地址、附件大小和附件个数来实现过滤；
  - 应用行为控制功能用来对用户的HTTP行为和FTP行为（如上传、下载）进行精确的控制。

威胁4 - 外部网络入侵行为

- 只要企业内网与外部网络有连接就有可能受到外部攻击者的入侵，如病毒、SQL注入和DDoS攻击等。

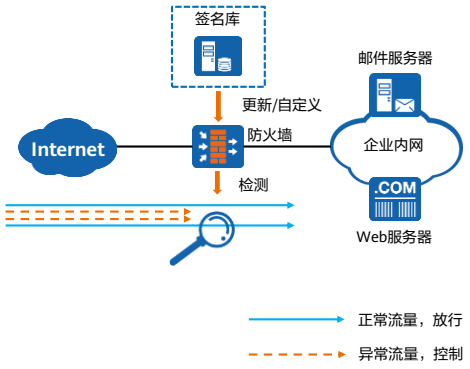
入侵类型	描述
病毒	一种可感染或附着在应用程序或文件中的恶意代码，一般通过邮件或文件共享等协议进行传播，威胁用户主机和网络的安全。病毒能够自我复制，但需要通过打开受感染的文件，启用宏等手动操作才能激活。
SQL注入	SQL注入攻击指的是通过构建特殊的输入作为参数传入Web应用程序，而这些输入大都是SQL语法里的一些组合，通过破坏SQL语句的原始逻辑，进而执行攻击者所希望的操作。SQL注入漏洞属于高危型Web漏洞。
DDoS攻击	DDoS攻击通过发出海量数据包，造成目标设备负载过高，最终导致网络带宽或是设备资源耗尽。



- 企业内部网络主机感染病毒后，攻击者会利用被感染主机入侵其他终端设备，扩大攻击成果，最终造成内网大量主机感染病毒。

入侵防御安全防范

- 防火墙的入侵防御功能对所有通过的报文进行检测分析，并实时决定允许通过或阻断。也可使用IPS设备对网络入侵行为进行防御。
- 防火墙/IPS设备通常部署在网络出口处，抵挡来自互联网的威胁。
- 防火墙/IPS设备上具备入侵防御功能模块，该模块通过将流经防火墙/IPS设备的流量与加载的签名库做对比并根据危险程度进行相应处理，签名库是签名的集合。
- 签名：用来描述网络中存在的该入侵行为的特征，及设备需要对其采取的动作。



HUAWEI

- 更多入侵防御原理将在《防火墙入侵防御》中详细介绍。

目录

终端软件漏洞

- 企业内网终端软件存在漏洞，往往给攻击者可乘之机，不管是从外网或是内网进行的网络攻击，内网终端感染病毒后，借助内网设备之间的信任关系，病毒通过横向扩散，最终往往造成内网大量终端设备感染。
- CVE（Common Vulnerabilities and Exposures）是一个披露漏洞的平台，它会提供编号作为漏洞对应的字符串式特征。

著名的WannaCry勒索病毒，就是利用Windows操作系统漏洞永恒之蓝发起攻击。由于很多受害者没有及时安装补丁，导致被病毒攻击，计算机中的文件被加密。

MSHTML的一个已知漏洞被某勒索软件团伙利用，与恶意广告一起感染受害者，并加密他们的设备。也有攻击者利用该漏洞，向Windows用户发送恶意的WinWord附件。

近期披露的某虚拟机软件漏洞可能被用于破坏虚拟机管理程序并处罚拒绝服务掉件。该漏洞很容易被高权限攻击者利用，一旦夺取了权限，可能导致虚拟机环境挂起或频繁崩溃。

终端软件漏洞应对方式

- 对企业网络终端设备的系统软件和应用软件及时打补丁，并且安装防病毒软件。
- 使用NAC（Network Admission Control）方案，对企业网络自有的终端和外来接入的终端进行安全性检查，阻止不符合要求的终端接入网络。
- 使用漏洞扫描工具扫描企业网络，对信息安全进行风险评估。检测网络中的设备存在的漏洞并及时进行修复。
- 进行渗透测试，使用专业人士对企业网络系统安全性进行评估，并给出针对性的改进措施。

渗透测试一般流程

目录

需求1 – 管理员权限管控

- 某些情况下，企业员工因为利益或不满，会实施危害企业信息安全的行为。比如盗取企业机密数据，破坏企业网络基础实施等。

某公司员工受虚拟货币利益驱使，偷偷使用公司服务器计算资源进行挖矿活动，获利数十万元，最后行为败露，受到法律制裁。但期间公司的服务器资源遭到侵占，影响正常业务的运行。

某公司员工因个人精神、生活等原因对公司线上生产环境进行了恶意的破坏。导致生产环境和数据遭受严重破坏，公司和客户利益收到严重损害。最终该员工也受到法律制裁。

某公司员工受利益驱使，离职前通过拍照、邮件外发等方式，盗窃公司机密信息。事发后受到法律制裁。

管理员权限管控安全方案

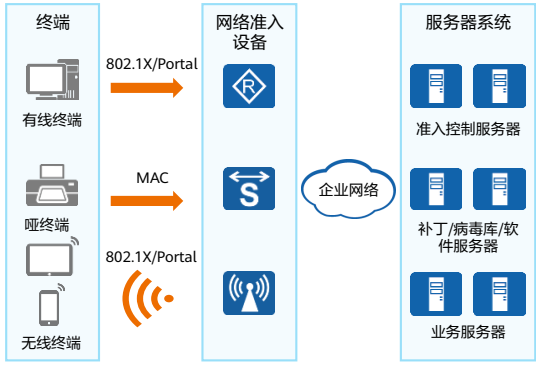
- 对于可能发生的企业员工的信息安全风险行为，可以从技术和管理两方面进行应对。
- 技术方面
  - 更严密的权限管理：对不同级别的企业员工设置不同权限的账号，特别是对运维的权限要遵循最小授权的原则，比如使用UMA统一运维审计对管理员的运维权限进行管控，并监控管理员行为；
  - 更可靠的备份机制：对于已经造成生产环境和数据破坏的情况，可以快速恢复，尽量减少损失。
- 管理方面
  - 在企业内部经常进行信息安全案例宣传，提高员工安全意识；
  - 对于高安全需求的区域，可以使用门禁系统；
  - 关注员工工作生活状态，及时进行心理辅导，防止员工因心理问题造成的信息安全风险行为。

需求2 - 上网权限管控

- 除了从企业外部网络带来的安全风险，企业内网安全隐患也日益增加。企业内可能会有外来人员，如果出现非法接入和非授权访问时，也会存在导致业务系统遭受破坏、关键信息资产泄露的风险。
  - 恶意人员接入网络之后，会进行破坏，或盗取信息的活动；
  - 接入网络的终端，如果携带有病毒，有可能导致病毒在企业内网传播。
- 应对非法接入，可以从技术和管理两方面入手：
  - 使用网络准入控制方案；
  - 对于出入企业的人员进行严格的行政管理。

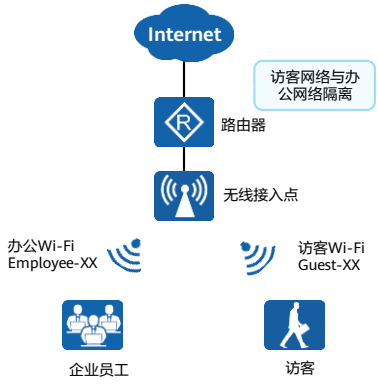
上网权限管控方案（1）

- 对于非法接入的应对措施，华为提供NAC方案，可以对接入用户进行安全控制，实现只有合法的用户、安全的终端才可以接入网络。
- NAC具有以下功能：
  - 身份认证：对接入网络的用户身份进行合法性认证，只有合法的用户才能接入企业网络；
  - 访问控制：根据用户身份、接入时间、接入地点、终端类型、接入方式精细匹配用户，控制用户能够访问的资源；
  - 对终端进行安全性检查，只有“健康的、安全的”用户终端才可以接入网络。



上网权限管控方案（2）

- 可以通过管理手段，规范员工进入企业内部，严格控制外来人员的进入。
  - 外来访问人员必须要提前登记，并出示有效证件才能进入；
  - 使用安保人员和设备控制外来人员及车辆的进入；
  - 对企业内部重要区域，可使用门禁系统，限制不符合权限的人员进入；
  - 禁止在计算机等设备上私自插入U盘等存储设备。
- 创建访客网络供外来访问人员进行接入，与企业办公网络隔离，消除安全风险。



思考题

1. （单选题）以下哪一内容过滤功能可防止员工将自己的身份信息泄露到外网？（　　）

   A. 邮件过滤

   B. 文件过滤

   C. URL过滤

   D. 内容过滤

2. （判断题）即使在经过源认证过滤非法流量后，访问目标服务器的流量依然很大，此时可以采用限流的方式保护目标服务器。（　　）

   A. 正确

   B. 错误

1. D
2. A

本章总结

- 本课程简要介绍了常见信息安全威胁的种类以及其威胁来源，详细描述了不同攻击的原理和影响，分别概述了不同威胁的应对方式和解决方案。
- 通过本课程的学习，您将能够对整个安全威胁的内容有一定的了解，为下一步深入学习打下基础。

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

缩略语表

缩略语	英文全称	解释
AntiDDoS	Anti Distributed Denial of Service	防御分布式拒绝服务
ATIC	Abnormal Traffic Inspection & Control System	异常流量监管系统
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
DMZ	Demilitarized Zone	半信任区
DoS	Denial of Service	拒绝服务
GRE	Generic Routing Encapsulation	通用路由封装
IPS	Intrusion Prevention System	入侵防御系统
IPSec	Internet Protocol Security	因特网协议安全协议
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
NAC	Network Admission Control	网络准入控制
SSL	Secure Sockets Layer	安全套接层
UMA	Unified Maintenance Audit	统一运维审计系统

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

防火墙安全策略

HUAWEI

前言

- 在人类社会的起源和发展过程中，通信就一直伴随着我们。随着信息技术的快速发展，特别是各类新技术、新业态、新应用不断涌现，给社会发展、百姓生活带来了极大的“红利”，但另一方面，也给网络安全带来了新的挑战。作为网络安全防护的第一道防线，防火墙扮演着非常重要的角色。
- 本课程主要介绍防火墙安全策略的原理以及在网络中的应用场景。

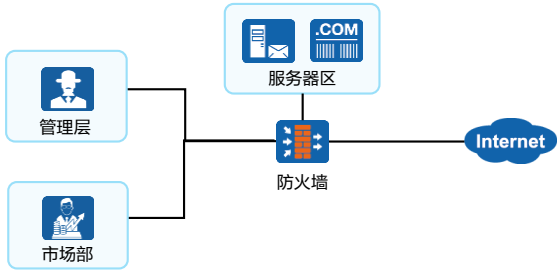
目标

- 学完本课程后，您将能够：
  - 描述防火墙安全区域
  - 描述防火墙的状态检测和会话机制
  - 描述防火墙在网络中的应用场景

目录

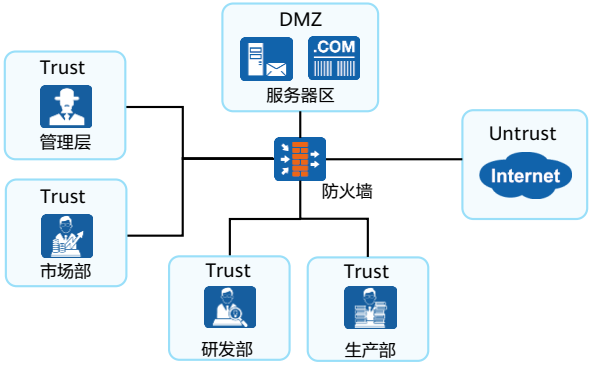
防火墙安全区域产生背景

- 防火墙不仅只是一个“入口的屏障”，而应该是多个网络的接入控制点。所有进出内网的数据流都应该首先经过防火墙，形成一个信息进出的关口。
- 如图所示，防火墙作为企业网络的重要组成部分，连接着企业网络管理层网络、市场部网络与服务器网络。防火墙一般部署在企业网络出口，与Internet连接。



防火墙安全区域基本概念

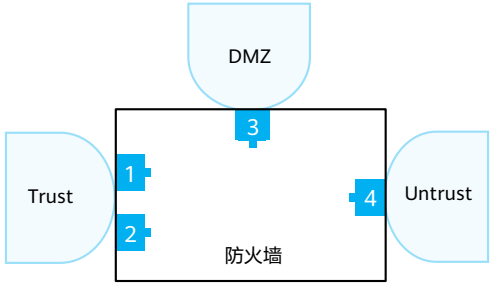
- 安全区域（Security Zone）：它是一个或多个接口的集合，是防火墙区别于路由器的主要特性。防火墙通过安全区域来划分网络、标识报文流动的“路线”，当报文在不同的安全区域之间流动时，才会触发安全检查。



- 在每一个被防火墙分割的网络内部中，所有的计算机之间是被认为“可信任的”，它们之间的通信不受防火墙的干涉。而在各个被防火墙分割的网络之间，必须按照防火墙规定的“策略”进行访问。

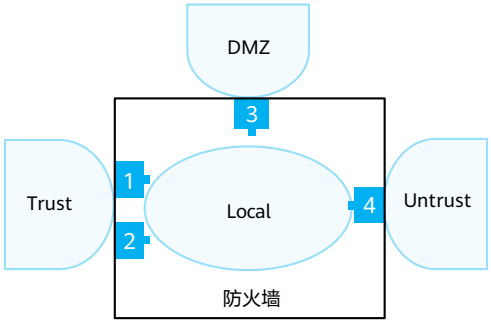
默认安全区域

- 华为防火墙产品默认提供了Trust、DMZ和Untrust三个可配置的安全区域。
  - Trust区域
    - 网络的受信任程度高；
    - 通常用来定义内部用户所在的网络。
  - DMZ区域
    - 网络的受信任程度中等；
    - 通常用来定义内部服务器所在的网络。
  - Untrust区域
    - 网络的受信任程度低；
    - 通常用来定义Internet等不安全的网络。



Local安全区域

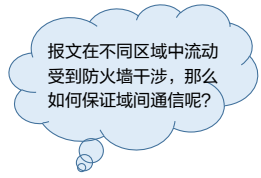
- 防火墙上提供的Local区域，代表防火墙本身。
- 凡是由防火墙主动发出的报文均可认为是从Local区域中发出，凡是需要防火墙响应并处理（而不是转发）的报文均可认为是由Local区域接收。
- Local区域中不能添加任何接口，但防火墙上所有业务接口本身都属于Local区域。
- 由于Local区域的特殊性，在很多需要设备本身进行报文收发的应用中，需要开放对端所在安全区域与Local区域之间的安全策略。例如Telnet登录、网页登录、接入SNMP网管等。



安全区域、受信任程度与优先级

- 不同的网络受信任程度不同，在防火墙上用安全区域表示网络后，如何来判断一个安全区域的受信任程度呢?
- 在华为防火墙上，每个安全区域都有一个唯一的优先级，用1至100的数字表示，数字越大，则代表该区域内的网络越可信。
  - 默认安全区域受信任程度：Local > Trust > DMZ > Untrust；
  - 用户可以根据实际组网需要，自行创建安全区域并定义其优先级。

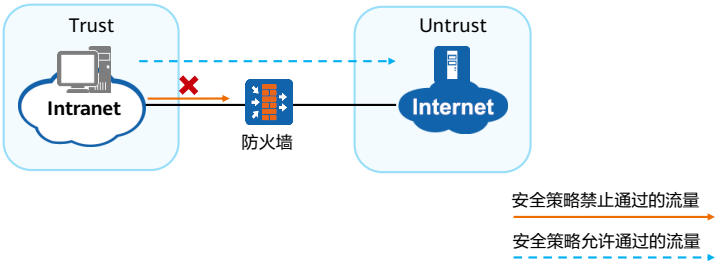
安全区域	优先级	说明
Local	100	设备本身，包括设备的各接口本身。
Trust	85	通常用于定义内网终端用户所在区域。
DMZ	50	通常用于定义内网服务器所在区域。
Untrust	5	通常用于定义Internet等不安全的网络。



目录

域间通信 - 安全策略

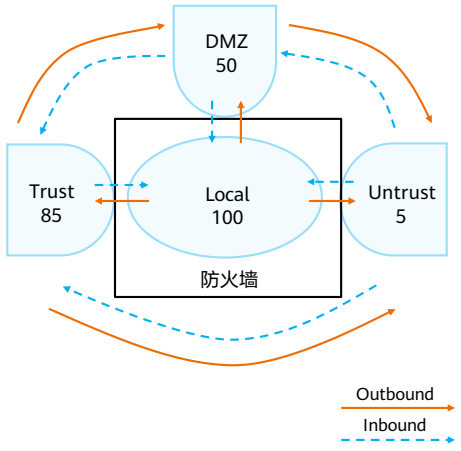
- 防火墙的基本作用是对进出网络的访问行为进行控制，保护特定网络免受“不信任”网络的攻击，但同时还必须允许两个网络之间可以进行合法的通信。防火墙一般通过安全策略实现以上功能。
- 安全策略是由匹配条件（五元组、用户、时间段等）和动作组成的控制规则，防火墙收到流量后，对流量的属性（五元组、用户、时间段等）进行识别，并将流量的属性与安全策略的匹配条件进行匹配。



- 安全策略是由匹配条件（例如五元组、用户、时间段等）和动作组成的控制规则，防火墙收到流量后，对流量的属性（五元组、用户、时间段等）进行识别，并将流量的属性与安全策略的匹配条件进行匹配。如果所有条件都匹配，则此流量成功匹配安全策略。流量匹配安全策略后，设备将会执行安全策略的动作：
  - 如果动作为“允许”，且没有配置内容安全检测，则允许流量通过；
  - 如果动作为“允许”，且配置了内容安全检测，则根据内容安全检测的结论来判断是否对流量进行放行；
  - 如果动作为“禁止”，则禁止流量通过。

安全域间、安全策略与报文流动方向

- 安全域间是用来描述流量的传输通道，它是两个“区域”之间的唯一“道路”。如果希望对经过这条通道的流量进行检测，就必须在通道上设立“关卡”，如防火墙安全策略。
  - 任意两个安全区域都构成一个安全域间（Interzone），并具有单独的安全域间视图；
  - 安全域间的数据流动具有方向性，包括入方向（Inbound）和出方向（Outbound）。



安全策略的匹配过程

- 防火墙最基本的设计原则一般是**没有明确允许的流量默认都会被禁止**，这样能够确保防火墙一旦接入网络就能保护网络的安全。
- 如果想要允许某流量通过，可以创建安全策略。一般针对不同的业务流量，设备上会配置多条安全策略。
- 安全策略匹配过程如下：

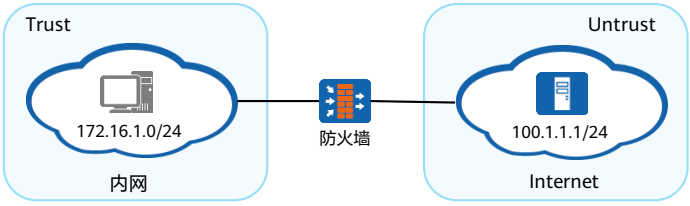
匹配顺序

策略编号	匹配条件				动作
Policy 1:	匹配条件1	匹配条件2	.....	匹配条件N	动作（允许/禁止）
Policy 2:	匹配条件1	匹配条件2	.....	匹配条件N	动作（允许/禁止）
.....					
Policy N:	匹配条件1	匹配条件2	.....	匹配条件N	动作（允许/禁止）
Default:	匹配条件均为any				动作（禁止）

- 同一安全区域内的流量和不同安全区域间的流量受缺省安全策略控制的情况分别为：
  - 对于不同安全区域间的流量（包括但不限于从防火墙发出的流量、防火墙接收的流量、不同安全区域间传输的流量），受缺省安全策略控制；
  - 对于同一安全区域内的流量，默认不受缺省安全策略控制，缺省转发动作为允许。如果希望同域流量受缺省安全策略控制，则需要开启缺省安全策略控制同一安全区域内流量的开关。开启后，缺省安全策略的配置将对同一安全区域内的流量生效，包括缺省安全策略的动作、日志记录功能等。
- 缺省安全策略可以修改默认动作、日志记录功能（包括策略命中日志、会话日志和流量日志）。

安全策略配置举例（1）

- 需求描述：
  - 某公司在网络边界处部署了防火墙作为安全网关。为了使私网中172.16.1.0/24网段的用户可以正常访问Internet，需要在防火墙上配置相应安全策略；
  - 在此网络中172.16.1.1、172.16.1.2和172.16.1.3的3台PC对安全性要求较高，不允许上网。

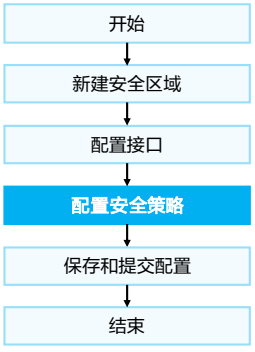


HUAWEI

- 网络中可能存在多种业务流量，针对不同的业务流量，设备上会配置多条安全策略。为了保证安全策略配置的正确性，管理员需要在配置安全策略前，完成安全策略的规划。安全策略的规划思路如下：
  - 了解企业的信息资产和服务，评估可能的风险；
  - 了解企业的业务，识别需要保护的信息资产，包括该资产可能面临的威胁。例如，如果一家科技公司，知识产权是该公司最宝贵的资产，该资产面临的最大威胁之一就是源代码被盗；
  - 使用安全区域划分网络，简化管理。管理员应首先明确需要划分哪几个安全区域，接口如何连接，分别加入哪些安全区域。流量不能在安全区域之间流动，除非存在动作为允许的安全策略，防止攻击者进入网络。通过部署基于安全区域、用户和应用的安全策略能阻止攻击者横向移动，即定义细粒度的区域，该区域仅允许特定的用户访问特定的应用和资源；
  - 识别业务和应用，确定业务黑白灰名单：
    - 识别出允许访问的应用白名单，并根据业务进行分类，以便应用到不同的策略中；
    - 识别出禁止访问的应用黑名单，应用到不同的策略中；
    - 灰名单是未知的，用于发现在企业运作的过程中遗漏的其它合法应用。例如，使用非知名端口的应用、企业自己开发的应用等。

安全策略配置举例（2）

- 配置思路：
  - 管理员应首先明确需要划分哪几个安全区域，接口如何连接，分别加入哪些安全区域；
  - 管理员选择可以根据“源地址”或“用户”来区分企业员工；
  - 如果想允许某种网络访问，则配置安全策略的动作为“允许”；如果想禁止某些地址访问，则配置安全策略的动作为“禁止”；
  - 将以上步骤规划出的安全策略的参数一一列出，并将所有安全策略按照先精确（条件细化的、特殊的策略）再宽泛（条件为大范围的策略）的顺序排序。在配置安全策略时需要按照此顺序进行配置。



安全策略配置举例（3）

- 先创建拒绝特殊的3个IP地址访问Internet的安全策略规则。（先精确）

```
[FW] security-policy
[FW-policy-security] rule name policy1
[FW-policy-security-rule-policy1] source-zone trust
[FW-policy-security-rule-policy1] destination-zone untrust
[FW-policy-security-rule-policy1] source-address 172.16.1.1 32
[FW-policy-security-rule-policy1] source-address 172.16.1.2 32
[FW-policy-security-rule-policy1] source-address 172.16.1.3 32
[FW-policy-security-rule-policy1] action deny
```

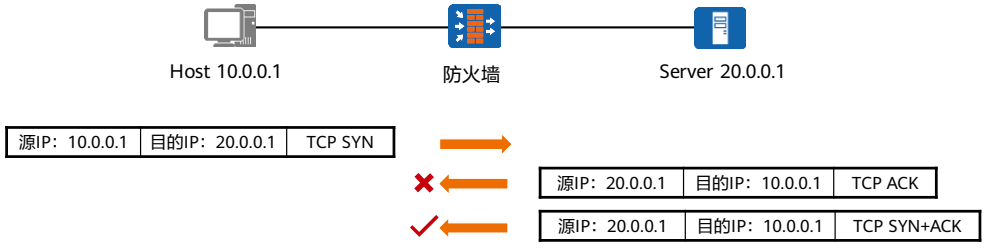
- 再创建允许172.16.1.0/24网段访问Internet的安全策略规则。（再宽泛）

```
[FW] security-policy
[FW-policy-security] rule name policy2
[FW-policy-security-rule-policy2] source-zone trust
[FW-policy-security-rule-policy2] destination-zone untrust
[FW-policy-security-rule-policy2] source-address 172.16.1.0 24
[FW-policy-security-rule-policy2] action permit
```

目录

状态检测机制

- 状态检测防火墙使用基于连接状态的检测机制，将通信双方之间交互的属于同一连接的所有报文都作为整个数据流来对待。在状态检测防火墙看来，同一个数据流内的报文不再是孤立的个体，而是存在联系的。
- 状态检测机制开启状态下，只有首包通过设备才能建立会话表项，后续包直接匹配会话表项进行转发。

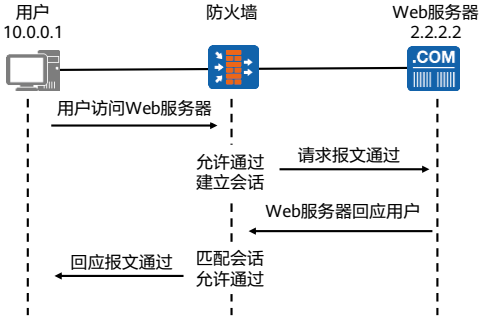


HUAWEI

- 状态检测机制关闭状态下，即使首包没有经过设备，后续包只要通过设备也可以生成会话表项。
- 在报文来回路径不一致的组网环境中，防火墙可能只会收到通信过程中的后续报文。在这种情况下，为了保证业务正常，就需要关闭防火墙的状态检测功能。当关闭状态检测功能后，可以通过后续报文建立会话，保证业务的正常运行。

会话机制

- 防火墙会将属于同一连接的所有报文作为一个整体的数据流（会话）来对待。会话表是用来记录TCP、UDP、ICMP等协议连接状态的表项，是防火墙转发报文的重要依据。



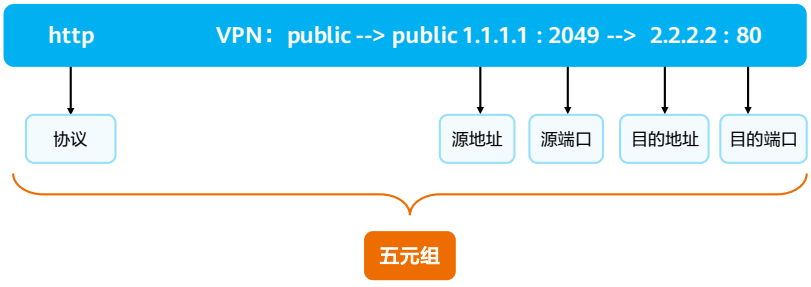
会话ID	源地址	源端口	目的地址	目的端口	动作
1	10.0.0.1	*	2.2.2.2	80	允许通过

HUAWEI

- 防火墙采用了基于“状态”的报文控制机制：只对首包或者少量报文进行检测就确定一条连接的状态，大量报文直接根据所属连接的状态进行控制。这种状态检测机制迅速提高了防火墙的检测和转发效率。会话表就是为了记录连接的状态而存在的。设备在转发TCP、UDP和ICMP报文时都需要查询会话表，来判断该报文所属的连接并采取相应的处理措施。

会话表项中的五元组信息

- 会话是通信双方的连接在防火墙上的具体体现，代表两者的连接状态，一条会话就表示通信双方的一个连接。
  - 通过会话中的五元组信息可以唯一确定通信双方的一条连接；
  - 防火墙将要删除会话的时间称为会话的老化时间；
  - 一条会话表示通信双方的一个连接，多条会话的集合叫做会话表。



HUAWEI

- 防火墙为各种协议设定了会话老化机制。当一条会话在老化时间内没有被任何报文匹配，则会被从会话表中删除。这种机制可以避免防火墙的设备资源被大量无用、陈旧的会话表项消耗。但是对于某些特殊业务中，一条会话的两个连续报文可能间隔时间很长。例如：
  - 用户通过FTP下载大文件，需要间隔很长时间才会在控制通道继续发送控制报文；
  - 用户需要查询数据库服务器上的数据，这些查询操作的时间间隔远大于TCP的会话老化时间。
- 在以上的场景中，如果会话表项被删除，则对应的业务就会中断。长连接（Long Link）机制可以给部分连接设定超长的老化时间，有效解决这个问题。

会话表项中的其他信息

- 在防火墙上通过display firewall session table命令可以看到正常建立的会话。

```
<FW> display firewall session table
Current Total Sessions : 1
telnet VPN:public --> public 192.168.3.1:2855-->192.168.3.2:23
```

- 在防火墙上通过display firewall session table verbose可以显示会话表详细信息。由于使用了verbose参数，可以看到除了五元组信息之外的其他信息。

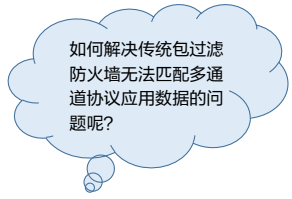
```
<FW> display firewall session table verbose
  Current Total Sessions : 1
  icmp  VPN:public --> public  ID: a58f3fe91023015aa15344e75b
  Zone: local--> trust  TTL: 00:00:20  Left: 00:00:09*
  Interface: GigabitEthernet0/0/0  NextHop: 10.1.2.2  MAC: 4437-e697-78fe
  <--packets:3 bytes:252    -->packets:3 bytes:252
  10.1.1.1:43982[1.1.1.1:2107]-->10.1.2.2:2048
```


- display firewall session table命令输出信息描述：
  - current total sessions：当前会话表数统计；
  - telnet：协议名称，举例中为telnet；
  - VPN:public-->public： VPN实例名称，表示方式为：源方向-->目的方向；
  - 192.168.3.1:2855-->192.168.3.2:23：会话表信息。
- display firewall session table verbose命令输出信息描述：
  - Current Total Sessions：当前会话表数统计；
  - Icmp：协议名称，举例中为icmp；
  - VPN:public-->public： VPN实例名称，表示方式为：源方向-->目的方向；
  - ID：当前会话ID；
  - Zone: local--> trust：会话的安全区域，表示方式为：源安全区域-->目的安全区域；
  - TTL：该会话表项总的生存时间；
  - Left：该会话表项剩余生存时间；
  - Interface：正向报文的出接口；
  - NextHop：正向报文的下一跳IP地址。

目录

ASPF技术产生背景

- 在TCP/IP模型中，应用层提供常见的网络应用服务，如Telnet、HTTP、FTP等协议。而应用层协议根据占用的端口数量可以分为单通道应用层协议与多通道应用层协议。
  - 单通道应用层协议：通信过程中只需占用一个端口的协议。例如： Telnet只需占用23端口，HTTP只需占用80端口；
  - 多通道应用层协议：通信过程中需占用两个或两个以上端口的协议。例如：FTP被动模式下需要占用21号端口以及一个随机端口。
- 传统包过滤防火墙针对多通道应用层协议访问控制的不足：
  - 传统的包过滤防火墙只能实现简单的访问控制；
  - 传统的包过滤防火墙只能阻止一些使用固定端口的单通道协议的应用数据。

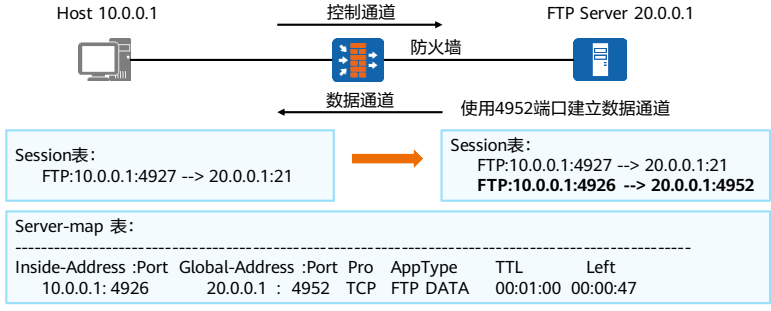


HUAWEI

- 多通道协议的应用需要先在控制通道中协商后续数据通道的地址和端口，然后根据协商结果建立数据通道连接。由于数据通道的地址和端口是动态协商的，管理员无法预知，因此无法制定完善精确的安全策略。为了保证数据通道的顺利建立，只能放开所有端口，这样显然会给服务器或客户端带来被攻击的风险。

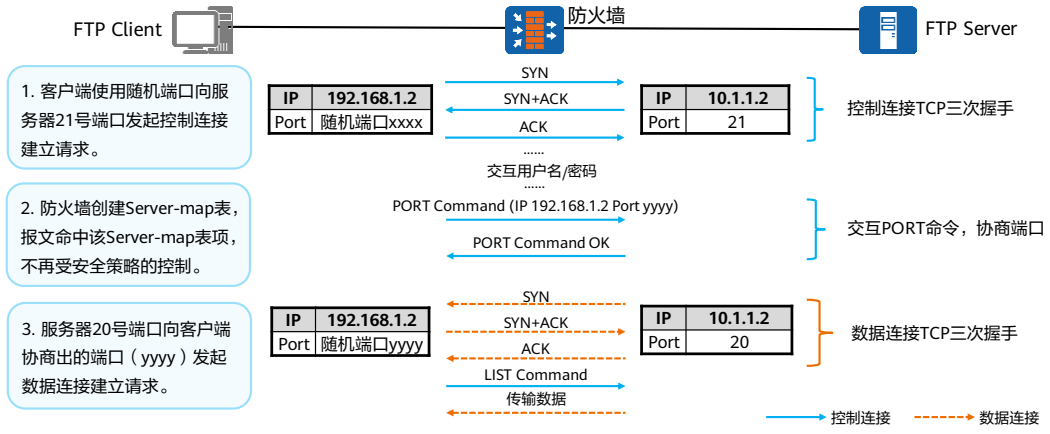
ASPF在多通道应用协议的应用

- ASPF（Application Specific Packet Filter）是针对应用层的包过滤。
  - 通过检测协商报文的应用层携带的地址和端口信息，自动生成相应的Server-map表，当数据通道的首包经过防火墙时，防火墙根据Server-map生成一条session，用于放行后续数据通道的报文，相当于自动创建了一条精细的“安全策略”。对于特定应用协议的所有连接，每一个连接状态信息都将被ASPF维护并用于动态的决定数据包是否被允许通过防火墙或丢弃。



FTP主动模式的ASPF

- Server-map表是通过ASPF功能自动生成的精细安全策略，是防火墙上的“隐形通道”。

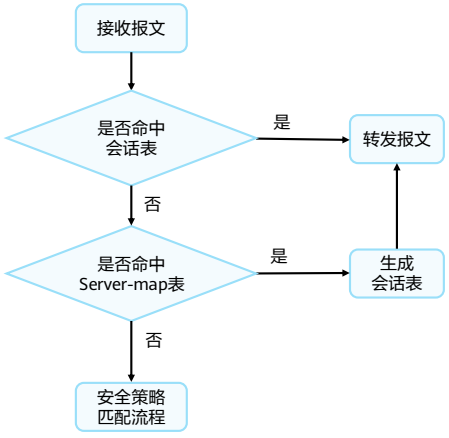


HUAWEI

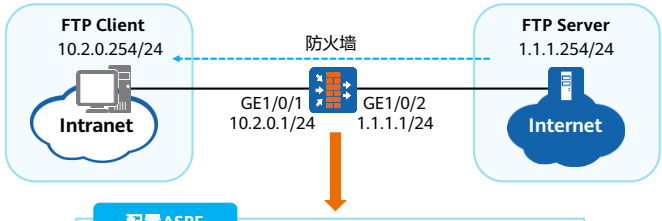
- FTP主动模式下，客户端使用随机端口xxxx向服务器的21端口发起连接请求建立控制通道，然后使用PORT命令协商两者建立数据通道的端口号，协商得出的端口是yyyy。然后服务器主动向客户端的yyyy端口发起连接请求，建立数据通道。数据通道建立成功后再进行数据传输。
- 在配置安全策略时，如果只配置了允许客户端访问服务器的21端口的安全策略，即控制连接能成功建立。但是当服务器访问客户端yyyy端口的报文到达防火墙后，对于防火墙来说，这个报文不是前一条连接的后续报文，而是代表着一条新的连接。要想使这个报文顺利到达FTP客户端，防火墙上就必须配置了安全策略允许其通过，如果没有配置服务器到客户端这个方向上的安全策略，该报文无法通过防火墙，导致数据通道建立失败。结果是用户能访问服务器，但无法请求数据。
- 由于PORT命令的应用层信息中携带了客户端的IP地址和向服务器随机开放的端口，防火墙通过分析PORT命令的应用层信息，提前预测到后续报文的行为方式，根据应用层信息中的IP和端口创建Server-map表。服务器向客户端发起数据连接的报文到达防火墙后命中该Server-map表项，不再受安全策略的控制。

Server-map表与会话表的关系

- Server-map表与会话表的关系如下：
  - Server-map表记录了应用层数据中的关键信息，报文命中该表后，不再受安全策略的控制；
  - 会话表是通信双方连接状态的具体体现；
  - Server-map表不是当前的连接信息，而是防火墙对当前连接分析后得到的即将到来报文的预测。
- 防火墙接收报文的处理过程如图所示：
  - 防火墙收到报文先检查是否命中会话表；
  - 如果没有命中则检查是否命中Server-map表；
  - 命中Server-map表的报文不受安全策略控制；
  - 防火墙最后为命中Server-map表的数据创建会话表。



Server-map表配置举例



配置ASPF

```
[FW] firewall interzone trust dmz
[FW-interzone-trust-dmz] detect ftp
```

自动生成Server-map表项

```
<FW> display firewall server-map
 Type: ASPF,  1.1.1.254 -> 10.2.0.254:2097,  Zone:---
 Protocol: tcp(Appro: ftp-data),  Left-Time:00:00:10
 Vpn: public -> public
```

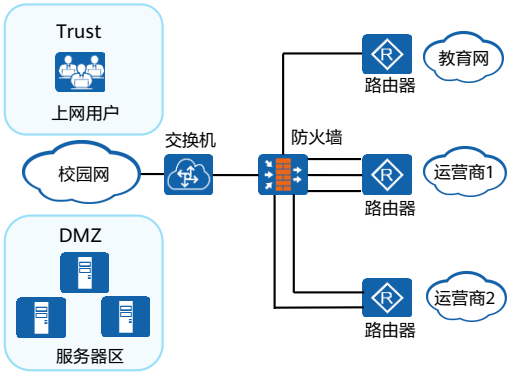
后续报文匹配会话表转发

```
<FW> display firewall session table
 ftp  VPN: public --> public  10.2.0.254:2095 --> 1.1.1.254:21
 ftp-data  VPN: public --> public  1.1.1.254:20 --> 10.2.0.254:2097
```

目录

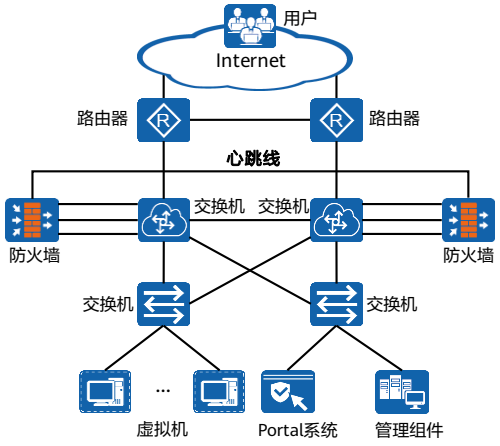
防火墙在校园出口安全方案中的应用场景

- 校园网从网络层到应用层的各个层面都面临着不同的安全威胁：
  - 网络边界防护
  - 内容安全防护
- 如图所示，防火墙作为安全网关部署在校园网出口：
  - 提供内、外网互访的安全隔离和防护。例如：提供传统的基于IP地址的安全策略制定和网络访问控制；
  - 同时提供基于用户的访问控制和行为溯源。



防火墙在云计算网络中的应用

- 随着云计算的迅猛发展，企业可以便捷地接入云计算网络，获取服务器、存储、应用等资源，减少构建IT基础设施的投资成本，大大加快了信息化进程。
- 如图所示，云计算网络中部署防火墙可以实现：
  - 不同的外网企业用户访问虚拟机时，相互之间不能影响，业务隔离；
  - 外网企业用户能够通过公网地址访问企业内部虚拟机和Portal系统；
  - 提高业务可靠性，不能因为一台设备出现故障而导致业务中断。



本章总结

- 本课程系统介绍了防火墙的基本概念与发展历史，同时介绍了防火墙安全区域、安全策略以及相应的控制原理。
- 通过本课程的学习，搭配基于实际环境的练习，您将能独立完成华为防火墙安全策略的配置方法，并掌握防火墙在网络安全方案的部署场景。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

防火墙网络地址转换技术

HUAWEI

前言

- 随着Internet的发展和网络应用的增多，有限的IPv4公有地址已经成为制约网络发展的瓶颈。尽管IPv6可以从根本上解决IPv4地址空间不足的问题，但目前众多网络设备和网络应用大多是基于IPv4地址。因此在IPv6广泛应用之前，NAT（Network Address Translation，网络地址转换）技术应需而生。
- NAT作为减缓IPv4地址枯竭的一种过渡方案，通过地址复用的方法来满足IP地址的需求，可以在一定程度上缓解IPv4地址空间枯竭的压力。
- 本章节您将了解NAT的技术背景，学习不同类型NAT的技术原理及应用场景。

目标

- 学完本课程后，您将能够：
  - 描述NAT的技术背景
  - 说明NAT的分类和技术原理
  - 区分NAT技术的应用场景

目录

NAT产生背景

- 随着网络设备的数量不断增长，对IPv4地址的需求也不断增加，导致可用的公网IPv4地址空间已经耗尽。解决IPv4地址枯竭问题的权宜之计是分配可重复使用的各类私有地址段给企业内部或家庭使用。
- 公有地址与私有地址的区别：
  - 公有地址：由专门的机构管理、分配，可以在Internet上直接通信的IP地址；
  - 私有地址：组织和个人可以任意使用，无法在Internet上直接通信，只能在内网使用的IP地址。
- A、B、C类地址中各预留了一些地址专门作为私有IP地址：
  - A类：10.0.0.0 ~ 10.255.255.255
  - B类：172.16.0.0 ~ 172.31.255.255
  - C类：192.168.0.0 ~ 192.168.255.255

防火墙NAT的实现 – NAT策略

- 防火墙的NAT功能可以通过配置NAT策略实现。
- NAT策略由转换后的地址（地址池地址或者出接口地址）、匹配条件和动作三部分组成。
  - 地址池类型包括源地址池和目的地址池。根据NAT转换方式的不同，可以选择不同类型的地址池或者出接口方式；
  - 匹配条件包括源/目的地址、源/目的安全区域、出接口、服务和时间段等。根据不同的需求配置不同的匹配条件，对匹配上条件的流量进行NAT转换；
  - 动作包括源地址转换或者目的地址转换。无论源地址转换或者目的地址转换，都可以对匹配上条件的流量进行选择NAT转换或者不转换两种方式。

- 如果防火墙创建了多条NAT策略，设备会从上到下依次进行匹配。如果流量匹配了某个NAT策略，进行NAT转换后，将不再进行下一个NAT策略的匹配。
- 双向NAT策略和目的NAT策略会在源NAT策略的前面，双向NAT策略和目的NAT策略之间按配置先后顺序排列，源NAT策略也按配置先后顺序排列。新增的策略和被修改NAT动作的策略都会被调整到同类NAT策略的最后面。
- NAT策略的匹配顺序可根据需要进行调整，但是源NAT策略不允许调整到双向NAT策略和目的NAT策略之前。

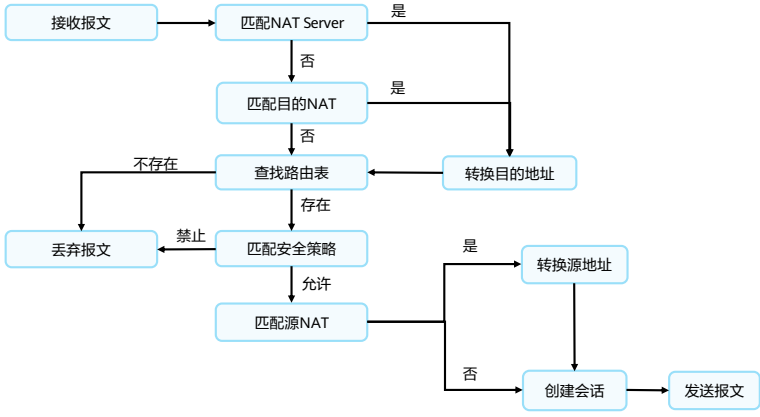
NAT分类与优缺点

- 根据应用场景的不同，NAT可以分为以下三类：
  - 源NAT（Source NAT）：适用于用户通过私网地址访问Internet的场景；
  - 目的NAT（Destination NAT）： 适用于用户通过公网地址访问私网服务器的场景；
  - 双向NAT（Bidirectional NAT）：适用于通信双方访问对方的时候目的地址都不是真实的地址，而是NAT转换后的地址的场景。
- NAT的优点：
  - 实现IP地址复用，节约宝贵的地址资源；
  - 有效避免来自外网的攻击，对内网用户提供隐私保护，可以很大程度上提高网络安全性。
- NAT的缺点：
  - 网络监控难度加大；
  - 限制某些具体应用。

- NAT技术除了可以实现地址复用，节约宝贵IP地址资源的优点外，还有其他一些优点，NAT技术的发展，也不断吸收先进的理念。
- NAT的优点：
  - 可以使一个局域网中的多台主机使用少数的合法地址访问外部的资源，也可以设定内部的FTP、Telnet等服务提供给外部网络使用，解决了IP地址日益短缺的问题；
  - 对于内外网络用户，感觉不到IP地址转换的过程，整个过程对于用户来说是透明的；
  - 对内网用户提供隐私保护，外网用户不能直接获得内网用户的IP地址、服务等信息，具有一定的安全性；
  - 通过配置多个相同的内部服务器的方式可以减小单个服务器在大流量时承担的压力，实现服务器负载均衡。
- NAT的不足：
  - 由于需要对数据报文进行IP地址的转换，涉及IP地址的数据报文的报头不能被加密。在应用协议中，如果报文中有地址或端口需要转换，则报文不能被加密。例如，不能使用加密的FTP连接，否则FTP的port命令不能被正确转换；
  - 网络监管变得更加困难。例如，如果一个黑客从内网攻击公网上的一台服务器，那么要想追踪这个攻击者很难。因为在报文经过NAT转换设备的时候，地址经过了转换，不能确定哪台才是黑客的主机。

NAT处理流程

- 防火墙上针对不同的NAT类型会采用不同的NAT策略，具体处理流程如下：



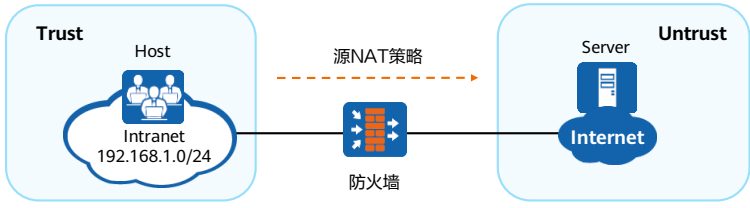
HUAWEI

- NAT处理流程简述如下：
  - 步骤1：防火墙收到报文后，查找NAT Server生成的Server-Map表，如果报文匹配到Server-Map表，则根据表项转换报文的目的地址，然后进行步骤3处理；如果报文没有匹配到Server-Map表，则进行步骤2处理；
  - 步骤2：查找NAT策略中目的NAT，如果报文符合匹配条件，则转换报文的目的地址后进行路由处理；如果报文不符合目的NAT的匹配条件，则直接进行路由处理；
  - 步骤3：根据报文当前的信息查找路由（包括策略路由），如果找到路由，则进入步骤4处理；如果没有找到路由，则丢弃报文；
  - 步骤4：查找安全策略，如果安全策略允许报文通过且之前并未匹配过NAT策略（目的NAT或者双向NAT），则进行步骤5处理；如果安全策略允许报文通过且之前匹配过双向NAT，则直接进行源地址转换，然后创建会话并进入步骤6处理；如果安全策略允许报文通过且之前匹配过目的NAT，则直接创建会话，然后进行步骤6处理；如果安全策略不允许报文通过，则丢弃报文；
  - 步骤5：查找NAT策略中源NAT，如果报文符合源NAT的匹配条件，则转换报文的源地址，然后创建会话；如果报文不符合源NAT的匹配条件，则直接创建会话；
  - 步骤6：防火墙发送报文。

目录

源NAT技术概述

- 背景：企业或家庭所使用的网络为私有网络，使用的是私有地址；运营商维护的网络为公共网络，使用的是公有地址。私有地址不能在公网中通信。
- 解决方案：多个用户共享少量公网地址访问Internet的时候，可以使用源NAT技术来实现。
  - 源NAT技术只对报文的源地址进行转换；
  - 源NAT技术可以分为NAT No-PAT、NAPT、Easy IP和三元组NAT等。

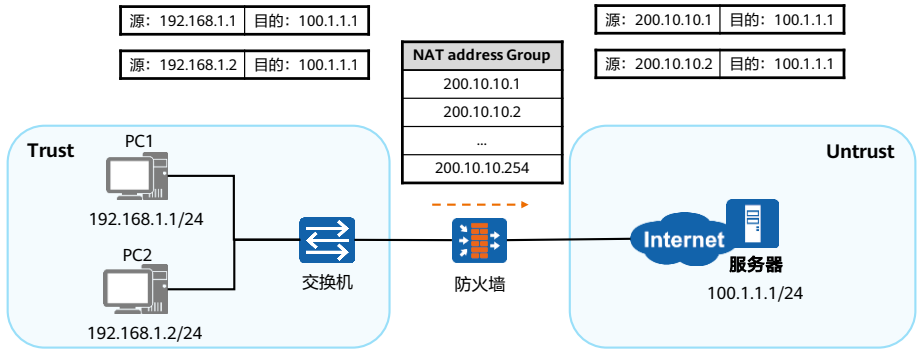


HUAWEI

- 在学校、公司中经常会有多个用户共享少量公网地址访问Internet的需求，通常情况下可以使用源NAT技术来实现。源NAT技术只对报文的源地址进行转换。通过源NAT策略对IPv4报文头中的源地址进行转换，可以实现私网用户通过公网IP地址访问Internet的目的。
- 如图所示，防火墙部署在网络边界处，通过部署源NAT策略，可以将私有网络用户访问Internet的报文的源地址转换为公网地址，从而实现私网用户接入Internet的目的。

NAT No-PAT原理

- NAT No-PAT（No-Port Address Translation，非端口地址转换）是一种只转换地址，不转换端口，实现私网地址与公网地址一对一的地址转换方式。NAT No-PAT无法提高公有地址利用率。
- NAT No-PAT适用于上网用户较少且公网地址数与同时上网的用户数量相同的场景。

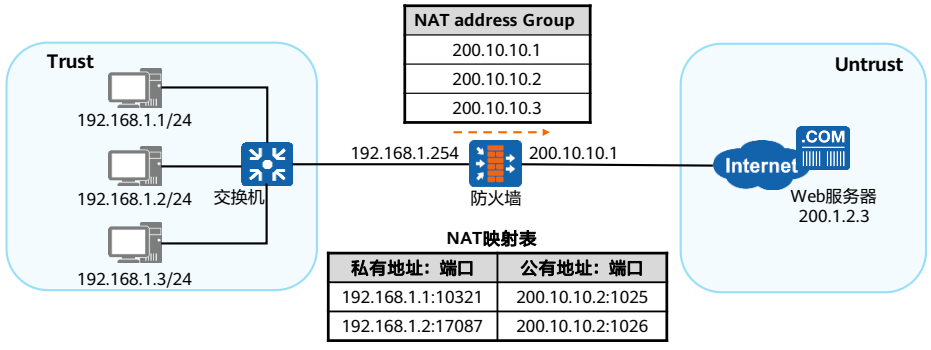


HUAWEI

- 当内部PC1和PC2需要与公网中的目的主机通信时，防火墙会从配置的公网地址池中选择一个未使用的公网地址与之做映射。每台主机都会分配到地址池中的一个唯一地址。当网关收到回复报文后，会根据之前的映射再次进行转换之后转发给对应主机。当不需要此连接时，对应的地址映射将会被删除，公网地址也会被恢复到地址池中待用。
- 动态NAT地址池中的地址用尽以后，只能等待被占用的公用IP地址被释放后，其他主机才能使用它来访问公网。
- 在使用NAT功能时，如果配置了No-PAT参数，那么设备会对内网IP和外网IP进行一对一的映射，而不进行端口转换。此时，内网IP的所有端口号都可以被映射为外网地址的对应端口，外网用户也就可以向内网用户的任意端口主动发起连接。所以配置NAT No-PAT后，设备会为有实际流量的数据流建立Server-map表，用于存放内网IP地址与外网IP地址的映射关系。设备根据这种映射关系对报文的地址进行转换，然后进行转发。

NAPT原理

- NAPT（Network Address and Port Translation，网络地址端口转换）是一种同时转换地址和端口，实现多个私网地址共用一个或多个公网地址的地址转换方式。NAPT可以有效地提高公有地址利用率。
- NAPT适用于公网地址数量少，需要上网的私网用户数量大的场景。



NAT映射表

私有地址：端口	公有地址：端口
192.168.1.1:10321	200.10.10.2:1025
192.168.1.2:17087	200.10.10.2:1026

HUAWEI

- NAPT借助端口可以实现一个公有地址同时对应多个私有地址。该模式同时对IP地址和端口号进行转换，实现不同私有地址（不同的私有地址，不同的源端口）映射到同一个公有地址（相同的公有地址，不同的源端口）。

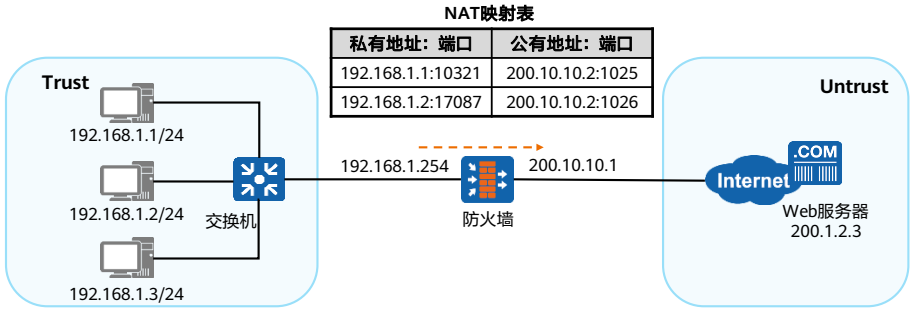
源NAT的两种转换方式的区别

- 源NAT有多种转换方式，这里只介绍其中的两种：
  - 不带端口转换的地址池方式（No-PAT）
  - 带端口转换的地址池方式（NAPT）

源NAT转换方式	实现方式	场景	公有地址使用率
NAT No-PAT	只转换地址，不转换端口	需要上网的私网用户数量少，公网IP地址数量与同时上网的最大私网用户数量基本相同。	1：1
NAPT	同时转换地址和端口	公网IP地址数量少，需要上网的私网用户数量大。	1：N

Easy IP

- Easy IP：实现原理和NAPT相同，同时转换IP地址和传输层端口，区别在于Easy IP没有地址池的概念，使用出接口的公网IP地址作为NAT转后的地址。
- Easy IP适用于不具备固定公网IP地址的场景。例如：拨号上网（PPPoE）。

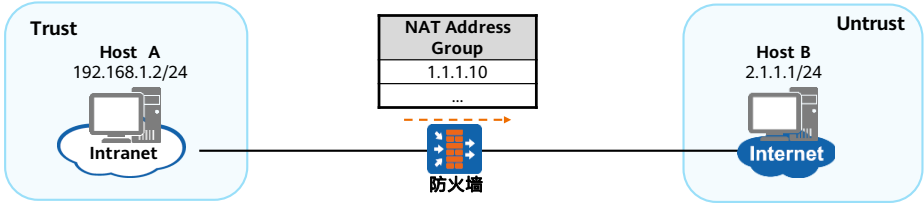


HUAWEI

- PPPoE（PPP over Ethernet）是在以太网链路上运行PPP协议，在小区组网等一系列应用中被广泛采用。

三元组NAT

- 三元组NAT是一种转换时同时转换地址和端口，实现多个私网地址共用一个或多个公网地址的地址转换方式。
- 三元组NAT允许Internet上的用户能主动访问私网用户，如文件共享、语音通信和视频传输等。



Server-Map Table				
Direction	Protocol	S-IP	D-IP:D-Port[New-D-IP:New-D-Port]	Zone
Destination	UDP	Any	1.1.1.10:2296 [192.168.1.2:6363]	Untrust
Direction	Protocol	S-IP:S-Port[New-S-IP:New-S-Port]	D-IP	Zone
Source	UDP	192.168.1.2:6363 [192.168.1.2:6363]	Any	Untrust

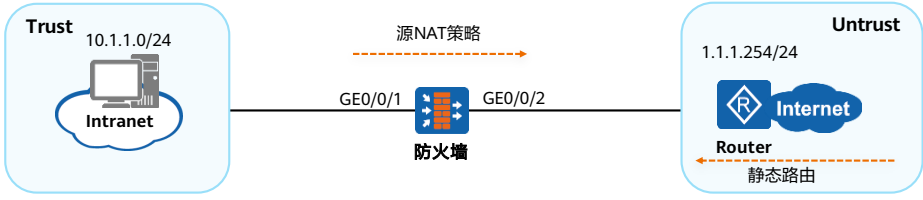
Session Table		
Protocol	S-IP:S-Port[New-S-IP:New-S-Port]	D-IP:D-Port
UDP	192.168.1.2:6363[1.1.1.10:2296]	1.1.1.10:80

HUAWEI

- 当Host A访问Host B时，防火墙的处理流程如下：
  - 防火墙收到Host A发送的报文后，根据目的IP地址判断报文需要在Trust区域和Untrust区域之间流动，通过域间安全策略检查后继而查找域间NAT策略，发现需要对报文进行地址转换。
  - 防火墙从NAT地址池中选择一个公网IP地址，替换报文的源IP地址为1.1.1.10，替换报文的端口号2296，并建立会话表和Server-map表，然后将报文发送至Host B。
  - 防火墙收到Host B响应Host A的报文后，通过查找会话表匹配到之前建立的表项，将报文的目的IP地址替换为192.168.1.2，端口号替换为6363，然后将报文发送至Host A。
- 防火墙上生成的Server-map表中存放Host的私网IP地址与公网IP地址的映射关系。
  - 正向Server-map表项保证内部PC转换后的地址和端口不变；
  - 反向Server-map表项允许外部设备可以主动访问内部PC。

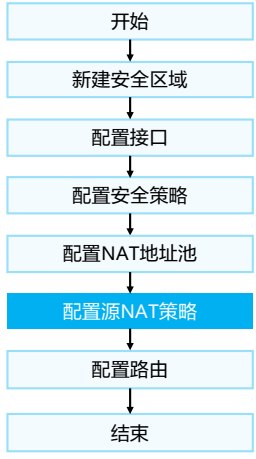
源NAT策略配置举例（1）

- 需求描述：
  - 某公司在网络边界处部署了防火墙作为安全网关。为了使私网中10.1.1.0/24网段的用户可以正常访问Internet，需要在防火墙上配置源NAT策略；
  - 除公网接口IP地址之外，公司还向运营商申请了6个IP地址（1.1.1.10 ~ 1.1.1.15）作为私网地址转换后的公网地址。如图所示，其中Router是运营商提供的接入网关。



源NAT策略配置举例（2）

- 配置思路：
  - 配置接口IP地址和安全区域，完成网络基本参数配置；
  - 配置安全策略，允许私网指定网段与Internet进行报文交互；
  - 配置NAT地址池，配置时开启允许端口转换，以实现公网地址复用；
  - 配置源NAT策略，实现私网指定网段访问Internet时自动进行源地址转换；
  - 在防火墙上配置缺省路由，使私网与运营商路由器流量可以正常互通。



源NAT策略配置举例（3）

- 将防火墙接口加入相应的安全区域。

```
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet 0/0/1
[FW-zone-trust] quit
[FW] firewall zone untrust
[FW-zone-untrust] add interface GigabitEthernet 0/0/2
[FW-zone-untrust] quit
```

- 配置安全策略，允许私网指定网段与Internet进行报文交互。

```
[FW] security-policy
[FW-policy-security] rule name policy1
[FW-policy-security-rule-policy1] source-zone trust
[FW-policy-security-rule-policy1] destination-zone untrust
[FW-policy-security-rule-policy1] source-address 10.1.1.0 24
[FW-policy-security-rule-policy1] action permit
[FW-policy-security-rule-policy1] quit
```

源NAT策略配置举例（4）

- 配置NAT地址池，配置时开启允许端口地址转换，实现公网地址复用。

```
[FW] nat address-group group1
[FW-address-group-addressgroup1] mode pat
[FW-address-group-addressgroup1] section 0 1.1.1.10 1.1.1.15
[FW-address-group-addressgroup1] route enable
```

- 配置源NAT策略，实现私网指定网段访问Internet时自动进行源地址转换。

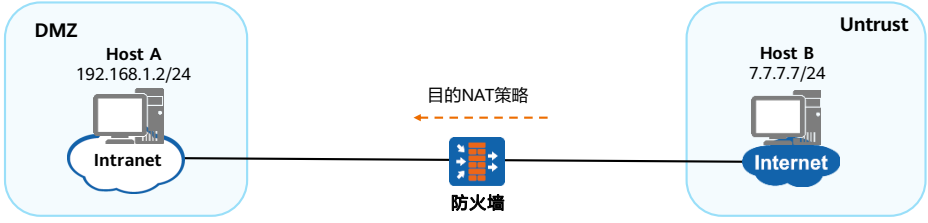
```
[FW] nat-policy
[FW-policy-nat] rule name policy1
[FW-policy-nat-rule-policy1] source-zone trust
[FW-policy-nat-rule-policy1] destination-zone untrust
[FW-policy-nat-rule-policy1] source-address 10.1.1.0 24
[FW-policy-nat-rule-policy1] action source-nat address-group group1
```


- 在防火墙上配置缺省路由，使私网流量可以正常转发至运营商的路由器。
- 在私网主机上配置缺省网关，使私网主机访问Internet时，将流量发往防火墙。

目录

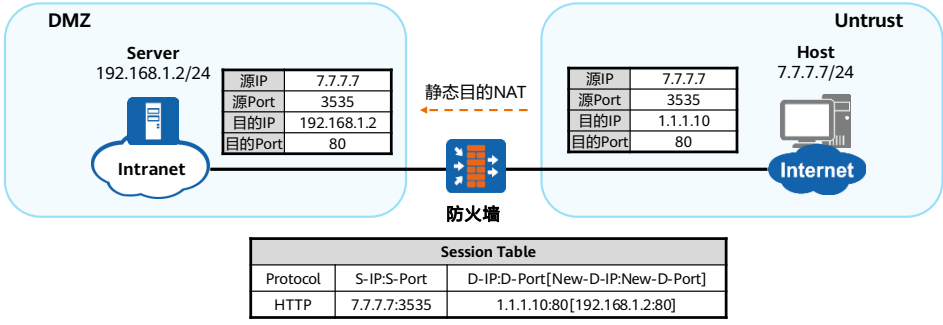
目的NAT概述

- 目的NAT是指对报文中的目的地址和端口进行转换。通过目的NAT技术将公网IP地址转换成私网IP地址，使公网用户可以利用公网地址访问内部Server。
- 当外网用户访问内部Server时，防火墙的处理过程如下：
  - 当外网用户访问内网Server的报文到达防火墙时，防火墙将报文的目的IP地址由公网地址转换为私网地址；
  - 当回程报文返回至防火墙时，防火墙再将报文的源地址由私网地址转换为公网地址。
- 根据转换后的目的地址是否固定，目的NAT分为静态目的NAT和动态目的NAT。



静态目的NAT

- 静态目的NAT是一种转换报文目的IP地址的方式，且转换前后的地址存在一种固定的映射关系。
- 通常情况下，出于安全的考虑，不允许外部网络主动访问内部网络。但是在某些情况下，还是希望能够为外部网络访问内部网络提供一种途径。例如，公司需要将内部网络中的资源提供给外部网络中的客户和出差员工访问。



Session Table		
Protocol	S-IP:S-Port	D-IP:D-Port[New-D-IP:New-D-Port]
HTTP	7.7.7.7:3535	1.1.1.10:80[192.168.1.2:80]

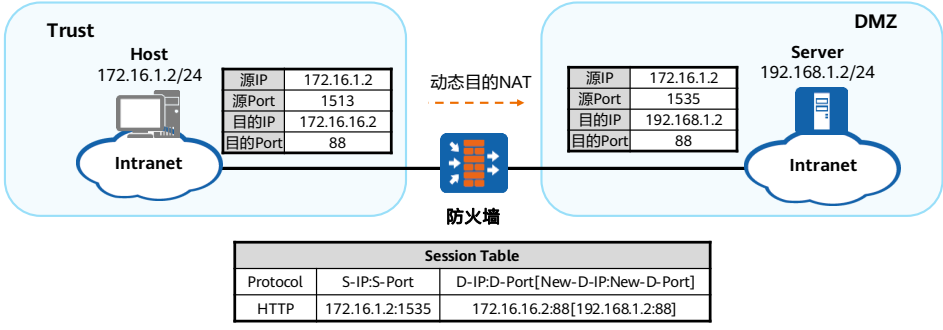
HUAWEI

当Host访问Server时，防火墙的处理过程如下：

1. 防火墙收到Internet上用户访问1.1.1.10（Server对外发布的公网IP地址）的报文的首包后，将匹配NAT策略的报文的目的地址进行转换。
2. 防火墙选择一个私网IP地址，替换报文的目的地址，同时可以选择使用新的端口替换目的端口号或者端口号保持不变。公网地址与私网地址一对一进行映射的场景下，公网地址与目的地址池地址按顺序一对一进行映射，防火墙从地址池中依次取出私网IP地址，替换报文的目的地址。
3. 报文通过安全策略后，防火墙建立会话表，然后将报文发送至内网服务器。
4. 防火墙收到Server响应Host的报文后，通过查找会话表匹配到步骤3中建立的表项，用原Host报文的目的地址（1.1.1.10）替换Server的IP地址（192.168.1.2），然后将报文发送至Host。
5. 后续Host继续发送给Server的报文，防火墙都会直接根据会话表项的记录对其进行转换。

动态目的NAT

- 动态目的NAT是一种动态转换报文目的IP地址的方式，转换前后的地址不存在一种固定的映射关系。
- 通常情况下，静态目的NAT可以满足大部分目的地址转换的场景。但是在某些情况下，希望转换后的地址不固定。例如，移动终端通过转换目的地址访问无线网络。



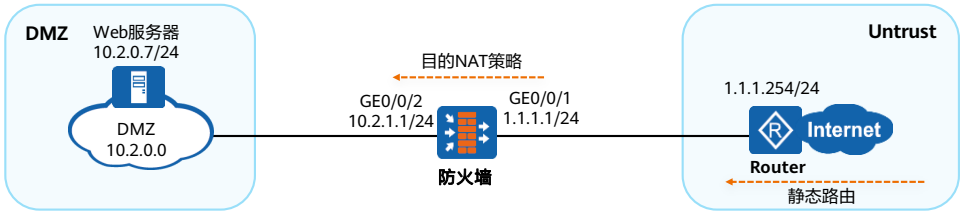
Session Table		
Protocol	S-IP:S-Port	D-IP:D-Port[New-D-IP:New-D-Port]
HTTP	172.16.1.2:1535	172.16.16.2:88[192.168.1.2:88]

HUAWEI

- 当Host访问Server时，防火墙的处理过程如下：
  - 防火墙收到Host发送的报文后，将匹配NAT策略的报文进行目的地址转换，从地址池中随机选择一个地址作为转换后的地址，将报文的目的IP地址由172.16.16.2转换为192.168.1.2；
  - 防火墙通过域间安全策略检查后建立会话表，然后将报文发送至Server；
  - 防火墙收到Server响应Host的报文后，通过查找会话表匹配到相应的表项，将报文的源地址替换为172.16.16.2，然后将报文发送至Host。

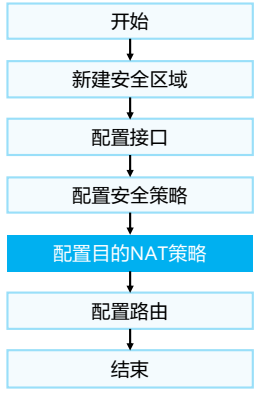
目的NAT策略配置举例（1）

- 需求描述：
  - 某公司在网络边界处部署了防火墙作为安全网关。为了使私网Web服务器能够对外提供服务，需要在防火墙上配置目的NAT；
  - 除了公网接口的IP地址外，公司还向运营商申请了IP地址（1.1.10.10）作为内网服务器对外提供服务的地址。网络环境如图所示，其中Router是运营商提供的接入网关。



目的NAT策略配置举例（2）

- 配置思路：
  - 配置接口IP地址和安全区域，完成网络基本参数配置；
  - 配置安全策略，允许外部网络用户访问内部服务器；
  - 通过目的NAT，使得外网用户能够访问内部服务器时，防火墙将流量能够送给内网的服务器；
  - 在防火墙和Router上配置缺省路由，使内网服务器与运营商路由器流量可以正常互通。



目的NAT策略配置举例（3）

- 将防火墙接口加入相应的安全区域。

```
[FW] firewall zone DMZ
[FW-zone-dmz] add interface GigabitEthernet 0/0/2
[FW-zone-dmz] quit
[FW] firewall zone untrust
[FW-zone-untrust] add interface GigabitEthernet 0/0/1
[FW-zone-untrust] quit
```

- 配置安全策略，允许外部网络用户访问内部服务器。

```
[FW] security-policy
[FW-policy-security] rule name policy1
[FW-policy-security-rule-policy1] source-zone untrust
[FW-policy-security-rule-policy1] destination-zone dmz
[FW-policy-security-rule-policy1] destination-address 10.2.0.0 24
[FW-policy-security-rule-policy1] action permit
[FW-policy-security-rule-policy1] quit
```

目的NAT策略配置举例（4）

- 配置目的NAT地址池，配置时开启允许端口地址转换，实现公网地址复用。

```
[FW1]destination-nat  address-group  group1
[FW1-dnat-address-group-group1]section  10.2.0.7  10.2.0.8
[FW-address-group-group1]  quit
```

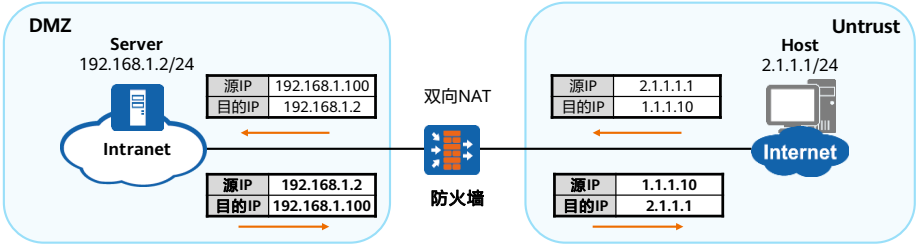
- 配置目的NAT策略，使得外网用户能够访问内部服务器时，防火墙将流量能够送给内网的服务器。

```
[FW]  nat-policy
[FW-policy-nat]  rule name policy1
[FW-policy-nat-rule-policy1]  source-zone  untrust
[FW-policy-nat-rule-policy1]  destination-address 1.1.10.10  1.1.10.11
[FW-policy-nat-rule-policy1]  service http
[FW-policy-nat-rule-policy1]  action destination-nat static address-to-address  address-group  group1
[FW-policy-nat-rule-policy1]  quit
```

目录

双向NAT

- 双向NAT指的是在转换过程中同时转换报文的源/目的IP地址。双向NAT不是一个单独的功能，而是源NAT和目的NAT的组合。
- 双向NAT是针对同一条流，在其经过防火墙时同时转换报文的源地址和目的地址。



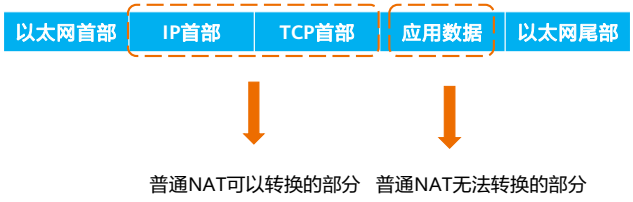
Session Table		
Protocol	D-IP:D-Port[New-D-IP:New-D-Port]	D-IP:D-Port[New-D-IP:New-D-Port]
HTTP	2.1.1.1:1535[192.168.1.100:2048]	1.1.1.10:80[192.168.1.2:80]

- 双向NAT主要应用在以下两个场景：
  - 外网用户访问内部服务器；
  - 私网用户访问内部服务器。
- 当外部网络中的用户访问内部服务器时，使用该双向NAT功能同时转换该报文的源和目的地址可以避免在内部服务器上设置网关，简化配置。
- 如图所示，当Host访问Server时，防火墙的处理过程如下：
  - 防火墙对匹配双向NAT处理的策略的报文进行地址转换；
  - 防火墙从目的NAT地址池中选择一个私网IP地址替换报文的目的IP地址，同时使用新的端口号替换报文的目的端口号；
  - 判断是否满足安全策略的要求，通过安全策略后从源NAT地址池中选择一个私网IP地址替换报文的源IP地址，同时使用新的端口号替换报文的源端口号，并建立会话表，然后将报文发送至Intranet；
  - 防火墙收到Server响应Host的报文后，通过查找会话表匹配到建立的表项，将报文的源地址和目的地址替换为原先的IP地址，将报文源和目的端口号替换为原始的端口号，然后将报文发送至Internet。

目录

NAT ALG概述

- 在防火墙基础中我们提到ASPF可以匹配多通道应用协议的数据，根据应用层信息中的IP地址和端口创建Server-map表。NAT ALG（Application Level Gateway，应用级网关）特定的应用协议的转换代理，可以完成应用层数据中携带的IP地址及端口号的转换。两者区别如下：
  - ASPF功能的主要目的是通过对应用层协议的报文分析，为其开放相应的包过滤规则；
  - NAT ALG（Application Level Gateway，应用级网关）的主要目的是为其开放相应的NAT规则；
  - 由于两者通常都是结合使用的，所以使用同一条命令就可以将两者同时开启。

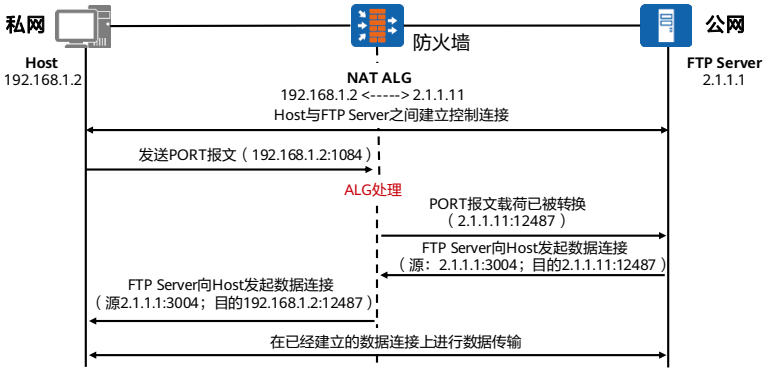


HUAWEI

- 在以太网数据帧结构中，IP首部包含32位的源IP地址和32位的目的IP地址，TCP首部包含16位的源端口号和16位的目的端口号。
- 但是很多协议会通过IP报文的数据载荷进行新端口甚至新IP地址的协商。协商完成之后，通信双方会根据协商结果建立新的连接进行后续报文的传输。而这些协商出来的端口和IP地址往往是随机的，管理员并不能为其提前配置好相应的NAT规则，这些协议在NAT转换过程中就会出现问题。
- 普通NAT实现了对UDP或TCP报文头中的的IP地址及端口转换功能，但对应用层数据载荷中的字段无能为力，在许多应用层协议中，比如多媒体协议（H.323、SIP等）、FTP、STelnet等，TCP/UDP载荷中带有地址或者端口信息，这些内容不能被NAT进行有效的转换，就可能导致问题。而NAT ALG（Application Level Gateway，应用层网关）技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的IP地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。
- 例如，FTP应用就由数据连接和控制连接共同完成，而且数据连接的建立动态地由控制连接中的载荷字段信息决定，这就需要ALG来完成载荷字段信息的转换，以保证后续数据连接的正确建立。
- 为了实现应用层协议的转发策略而提出了ASPF功能。ASPF功能的主要目的是通过对应用层协议的报文分析，为其开放相应的包过滤规则，而NAT ALG的主要目的，是为其开放相应的NAT规则。由于两者通常都是结合使用的，所以使用同一条命令就可以将两者同时开启。

NAT ALG实现原理

- 私网侧的主机要访问公网的FTP服务器。NAT设备上配置了私网地址192.168.1.2到公网地址2.1.1.11的映射，实现地址的NAT转换，以支持私网主机对公网的访问。组网中，若没有ALG对报文载荷的处理，私网主机发送的PORT报文到达服务器端后，服务器无法根据私网地址进行寻址，也就无法建立正确的数据连接。

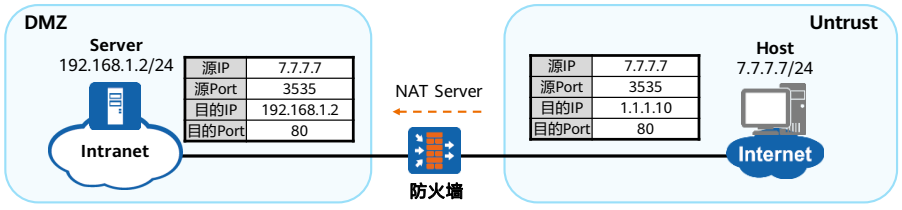


HUAWEI

- 整个通信过程包括如下四个阶段：
  - 私网主机和公网FTP服务器之间通过TCP三次握手成功建立控制连接；
  - 控制连接建立后，私网主机向FTP服务器发送PORT报文，报文中携带私网主机指定的数据连接的目的地址和端口，用于通知服务器使用该地址和端口和自己进行数据连接；
  - PORT报文在经过支持ALG特性的NAT设备时，报文载荷中的私网地址和端口会被转换成对应的公网地址和端口。即设备将收到的PORT报文载荷中的私网地址192.168.1.2转换成公网地址2.1.1.11，端口1084转换成12487；
  - 公网的FTP服务器收到PORT报文后，解析其内容，并向私网主机发起数据连接，该数据连接的目的地址为2.1.1.11，目的端口为12487（注意：一般情况下，该报文源端口为20，但由于FTP协议没有严格规定，有的服务器发出的数据连接源端口为大于1024的随机端口，如本例采用的是FTP服务器，采用的源端口为3004）。由于该目的地址是一个公网地址，因此后续的数据连接就能够成功建立，从而实现私网主机对公网服务器的访问。

NAT Server

- NAT Server也称静态映射，是一种转换报文目的IP地址的方式，它提供了公网地址和私网地址的映射关系，实现外部网络用户通过公网地址访问私网内部服务器的需求。



Server-Map Table			
Direction	Protocol	S-IP	D-IP:D-Port[New-D-IP:New-D-Port]
Obverse	TCP	Any	1.1.1.10:80[192.168.1.2:80]

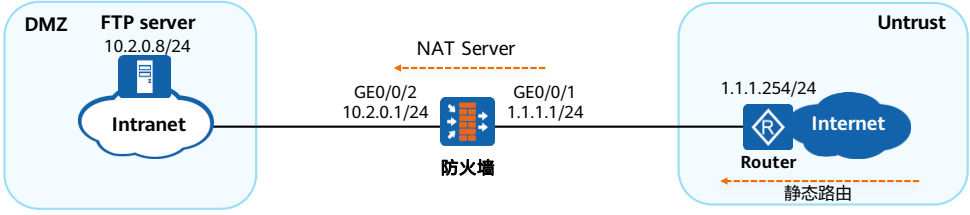
Session Table		
Protocol	S-IP:S-Port	D-IP:D-Port[New-D-IP:New-D-Port]
HTTP	7.7.7.7:3535	1.1.1.10:80[192.168.1.2:80]

HUAWEI

- NAT Server也称静态映射，是一种转换报文目的IP地址的方式，它提供了公网地址和私网地址的映射关系，将报文中的公网地址转换为与之对应的私网地址。
- 在使用NAT Server功能时，外网的用户向内部服务器主动发起访问请求，该用户的IP地址和端口号都是不确定的，唯一可以确定的是内部服务器的IP地址和所提供服务的端口号。所以在配置NAT Server成功后，设备会自动生成Server-map表项，用于存放Global地址与Inside地址的映射关系。设备根据这种映射关系对报文的地址进行转换并转发。
- 如图所示，当Host访问Server时，防火墙的处理过程如下：
  - 防火墙收到Internet上用户访问1.1.1.10的报文的首包后，查找并匹配到Server-Map表项，将报文的目的IP地址转换为192.168.1.2；
  - 防火墙根据目的IP地址判断报文需要在Untrust区域和DMZ区域之间流动，通过域间安全策略检查后建立会话表，然后将报文发送至Intranet；
  - 防火墙收到Server响应Host的报文后，通过查找会话表匹配到上一步骤中建立的表项，将报文的源地址替换为1.1.1.10，然后将报文发送至Internet；
  - 后续Host继续发送给Server的报文，防火墙都会直接根据会话表项的记录对其进行转换，而不会再去查找Server-map表项。
- 另外，防火墙在进行地址映射的过程中还可以选择是否允许端口转换，是否允许服务器采用公网地址上网，以满足不同场景的需求。

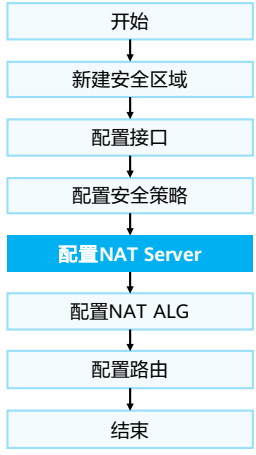
NAT Server配置举例（1）

- 需求描述：
  - 某公司在网络边界处部署了防火墙作为安全网关。为了使FTP服务器能够对外提供服务，需要在防火墙上配置NAT Server功能。
  - 除了公网接口的IP地址外，公司还向运营商申请了一个IP地址（1.1.1.10）作为内网服务器对外提供服务的地址。网络环境如图所示，其中Router是运营商提供的接入网关。



NAT Server配置举例（2）

- 配置思路：
  - 配置接口IP地址和安全区域，完成网络基本参数配置；
  - 配置安全策略，允许外部网络用户访问内部服务器；
  - 通过配置NAT Server，分别映射FTP服务器；
  - 通过开启FTP协议的NAT ALG功能，完成应用层数据中携带的地址及端口号信息的转换；
  - 在防火墙跟Router上配置缺省路由，使内网服务器与运营商路由器流量可以正常互通。



NAT Server配置举例（3）

- 将防火墙接口加入相应的安全区域。

```
[FW] firewall zone dmz
[FW-zone-dmz] add interface GigabitEthernet 0/0/2
[FW-zone-dmz] quit
[FW] firewall zone untrust
[FW-zone-untrust] add interface GigabitEthernet 0/0/1
[FW-zone-untrust] quit
```

- 配置安全策略，允许外部网络用户访问内部服务器。

```
[FW] security-policy
[FW-policy-security] rule name policy1
[FW-policy-security-rule-policy1] source-zone untrust
[FW-policy-security-rule-policy1] destination-zone dmz
[FW-policy-security-rule-policy1] destination-address 10.2.0.0 24
[FW-policy-security-rule-policy1] action permit
[FW-policy-security-rule-policy1] quit
```

NAT Server配置举例（4）

- 配置NAT Server功能。

```
[FW] nat server policy_ftp protocol tcp global 1.1.1.10 ftp inside 10.2.0.8 ftp unr-route
```

- 开启FTP协议的NAT ALG功能。

```
[FW] firewall interzone dmz untrust
[FW-interzone-dmz-untrust] detect ftp
[FW-interzone-dmz-untrust] quit
```

- 配置缺省路由，使内网服务器对外提供的服务流量可以正常转发至运营商的路由器。

```
[FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```


- 当NAT Server的global地址与公网接口地址不在同一网段时，必须配置黑洞路由；
- 当NAT Server的global地址与公网接口地址在同一网段时，建议配置黑洞路由；
- 当NAT Server的global地址与公网接口地址一致时，不会产生路由环路，不需要配置黑洞路由。

思考题

1. (简答题)哪种NAT转换允许私网服务器既能被内部访问又能被外部访问?
2. (简答题)NAPT相比较于NAT No-PAT有哪些优点?

1. 通过NAT Server配置，将公网地址与一个私网服务器地址绑定，在地址转换后，外网主机便可以通过公有地址访问内网服务器。同时，私网地址用户可以通过服务器的私网地址访问内网服务器。
2. NAPT支持多个私有地址转换为一个共同的公有地址，公有地址利用率更高。

本章总结

- 本课程系统介绍了NAT相关原理详解， NAT分为源NAT、目的NAT、双向NAT等技术。同时还介绍了NAT ALG与NAT Server。
- 通过本课程的学习，搭配基于实际环境的练习，您将能独立完成华为NAT策略配置，并掌握NAT技术的各种应用场景。

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

缩略语表

缩略语	英文全称	解释
ALG	Application Layer Gateway	应用层网关
NAPT	Network Address and Port Translation	网络地址端口转换
NAT	Network Address Translation	网络地址转换
NO-PAT	No-Port Address Translation	非端口地址转换

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

防火墙双机热备技术

HUAWEI

前言

- 随着移动办公、网上购物、即时通讯、互联网金融和互联网教育等业务蓬勃发展，网络承载的业务越来越多，越来越重要。所以如何保证网络的不间断传输成为网络发展过程中急需解决的一个问题。
- 双机热备份技术的出现改变了可靠性难以保证的尴尬局面，它通过在网络出口位置部署两台防火墙，保证了内部网络与外部网络之间的通讯可靠性。

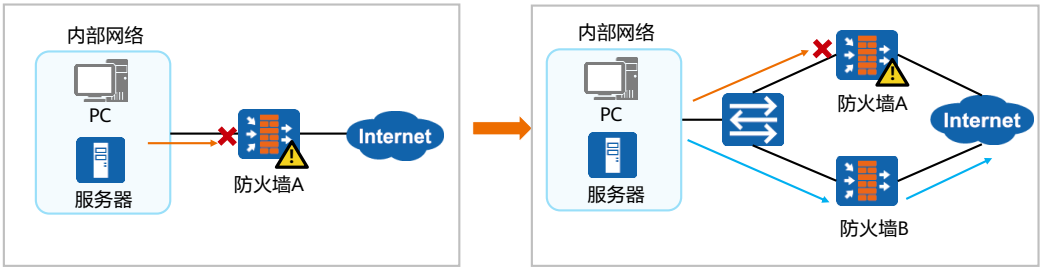
目标

- 学完本课程后，您将能够:
  - 掌握双机热备技术原理
  - 掌握双机热备基础配置

目录

双机热备技术产生的背景

- 传统的组网方式如下左图所示，内部用户和外部用户的交互报文全部通过防火墙A。如果防火墙A出现故障，内部网络中所有以防火墙A作为默认网关的主机与外部网络之间的通讯将中断，通讯可靠性无法保证。
- 防火墙作为安全设备，一般会部署在需要保护的网络和不受保护的网络之间，即位于网络边界上。在网络边界上，如果仅仅使用一台防火墙设备，无论其可靠性多高，系统都可能会承受因为单点故障而导致网络中断的风险。为了防止一台设备出现意外故障而导致网络业务中断，可以采用两台防火墙形成双机备份。

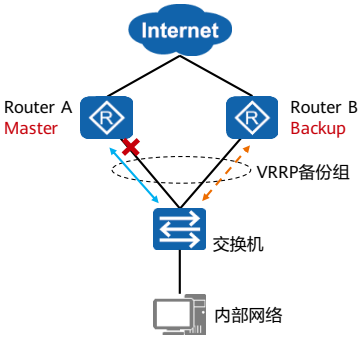


HUAWEI

- 在双机热备组网中，一台防火墙转发流量，一台防火墙作为备份，这时需要VRRP协议帮助两台设备协同工作。VRRP协议最初使用在路由器可靠性组网上。

基于VRRP的路由器冗余部署方案

- VRRP（Virtual Router Redundancy Protocol）是一种容错协议，它保证当主机的下一跳路由器（默认网关）出现故障时，由备份路由器自动代替出现故障的路由器完成报文转发任务，从而保持网络通信的连续性和可靠性。同一VRRP备份组内的路由器有两种角色：Master设备（活动状态）、Backup设备（备份状态）。



- 主设备Router A正常时：
  - Router A作为VRRP备份组的Master设备，负责转发数据流量。
- 主设备Router A故障时：
  - Router B感知到VRRP心跳超时，从而被选举为新的主设备；
  - Router B发送免费ARP，交换机收到后刷新MAC地址表；
  - Router B响应用户的ARP请求，并负责流量转发。

HUAWEI

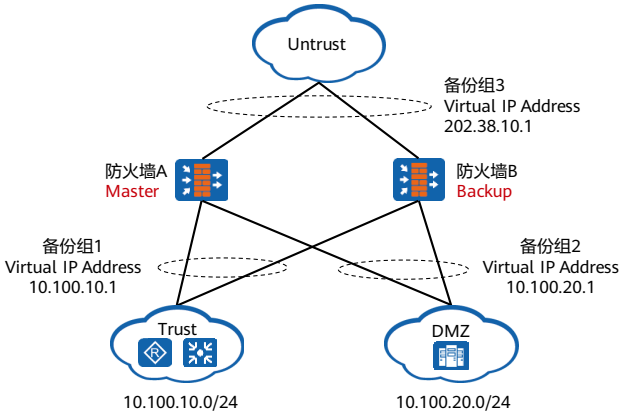
- 备份组：同一个广播域的一组路由器组织成一个虚拟路由器，备份组中的所有路由器一起，共同提供一个虚拟IP地址，作为内部网络的网关地址，实现网关的备份。
- 当Master设备正常工作时，网络内主机通过Master设备与外部网络通信。当Master设备出现故障时，Backup设备会成为新的Master设备，接替原Master设备的报文转发工作，保证网络不中断。
  - Master：活动状态。VRRP备份组状态为Master的设备被称为Master设备。Master设备拥有VRRP备份组的虚拟IP地址和虚拟MAC地址。Master设备收到目的IP地址是虚拟IP地址的ARP请求时，会响应这个ARP请求。在同一个备份组中的多个路由器中，只有一台处于活动状态，只有主路由器能转发以虚拟IP地址作为下一跳的报文；
  - Backup：备份状态。VRRP备份组状态为Backup的设备被称为Backup设备。Backup设备不会响应目的IP地址为虚拟IP地址的ARP请求。在同一个备份组中的多个路由器中，除主路由器外，其他路由器均为备份路由器，处于备份状态。当Master设备出现故障时，剩下的Backup设备中将会选举出新的Master设备；
  - Master设备选举规则：首先比较优先级的大小，优先级的范围为0-255，优先级高者当选为Master设备，其次比较接口IP地址大小，接口IP地址较大的设备当选为Master设备。成为Master的设备运行优先级自动变为255；
  - 主路由器通过组播方式定期向备份路由器发送通告报文（Hello报文），备份路由器则负责监听通告报文，以此来确定其状态。由于VRRP Hello报文为组播报文，所以要求备份组中的各路由器通过二层设备相连。

- 图中Router A正常时流量转发流程如下：
  - Router A发送免费ARP：免费ARP包含VRRP虚拟IP地址与VRRP虚拟MAC地址；
  - 交换机刷新MAC地址表：MAC地址表将虚拟MAC地址与接收免费ARP的接口映射；
  - 内部网络用户发送ARP请求询问网关地址：网关地址即虚拟IP地址；
  - Router A应答ARP请求：Router A将虚拟MAC地址回应给内部网络用户；
  - 内部网络用户的流量发向网关Router A：内部网络用户将流量发送给虚拟MAC地址，交换机根据MAC地址映射表将流量转发给Router A。
- Router A故障时流量转发流程如下：
  - Router B三个报文周期没有收到主设备Router A发送的VRRP报文，自动切换成为新的Master；
  - Router B发送免费ARP：免费ARP包含VRRP虚拟IP地址与VRRP虚拟MAC地址；
  - 交换机刷新MAC地址表：MAC地址表将虚拟MAC地址与接收免费ARP的接口映射；
  - 内部网络用户发送ARP请求询问网关地址：网关地址即虚拟IP地址；
  - Router B应答ARP请求：Router B将虚拟MAC地址回应给内部网络用户；
  - 内部网络用户的流量发向网关Router B：内部网络用户将流量发送给虚拟MAC

地址，交换机根据MAC地址映射表将流量转发给Router B。

VRRP在多区域防火墙组网中的应用

- 为防火墙上多个区域提供双机备份功能时，需要在每一台防火墙上配置多个VRRP备份组。

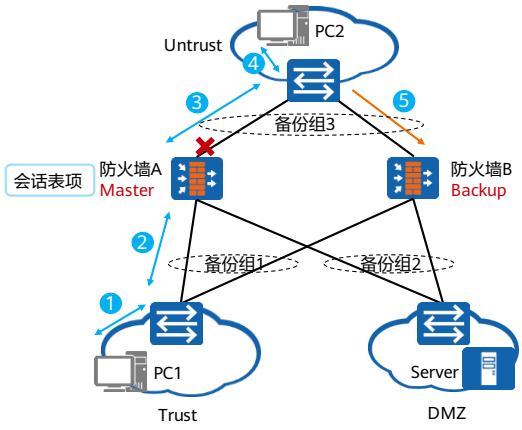


HUAWEI

- 当防火墙上多个区域需要提供双机备份功能时，需要在一台防火墙上配置多个VRRP备份组。
- 由于USG防火墙是状态防火墙，它要求报文的来回路径通过同一台防火墙。为了满足这个限制条件，就要求在同一台防火墙上的所有VRRP备份组状态保持一致，即需要保证在主防火墙上所有VRRP备份组都是主状态，这样所有报文都将从此防火墙上通过，而另外一台防火墙则充当备份设备。

VRRP在防火墙应用中存在的缺陷

- 传统VRRP方式无法实现主、备用防火墙状态信息和多组VRRP状态的一致性。



- 当防火墙A和防火墙B的VRRP状态一致：
  - Trust区域的PC1访问Untrust区域的PC2，报文来回路径一致，防火墙A状态检测机制检测通过，通信正常。
- 当防火墙A和防火墙B的VRRP状态不一致：
  - 防火墙A上游链路发生故障，防火墙B成为备份组3新的Master；
  - Trust区域的PC1访问Untrust区域的PC2，报文来回路径不一致，防火墙B状态检测机制检测不通过，报文丢失。

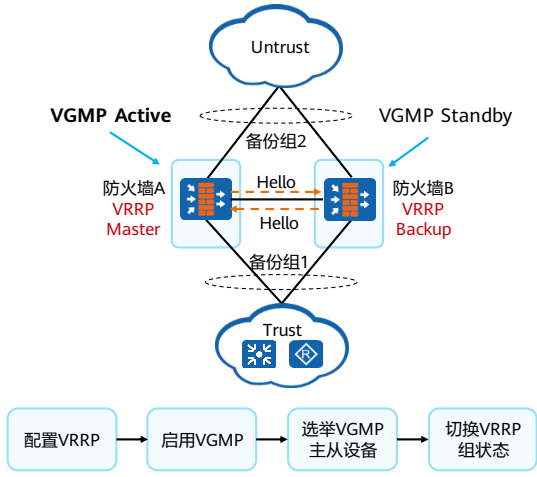
HUAWEI

- 如图所示，假设防火墙A和防火墙B的VRRP状态一致，即防火墙A的所有接口均为主用状态，防火墙B的所有接口均为备用状态。
  - 此时，Trust区域的PC1访问Untrust区域的PC2，报文的转发路线为(1)-(2)-(3)-(4)。防火墙A转发访问报文时，动态生成会话表项。当PC2的返回报文经过(4)-(3)到达防火墙A时，由于能够命中会话表项，才能再经过(2)-(1)到达PC1，顺利返回。同理，当PC2和DMZ区域的Server也能互访。
  - 假设防火墙A和防火墙B的VRRP状态不一致，例如，当防火墙B与Trust区域相连的接口为备用状态，但与Untrust区域的接口为主用状态，则PC1的报文通过防火墙A设备到达PC2后，在防火墙A上动态生成会话表项。PC2的返回报文通过路线(5)返回。此时由于防火墙B上没有相应数据流的会话表项，在没有其他报文过滤规则允许通过的情况下，防火墙B将丢弃该报文，导致会话中断。
- 问题产生的原因：报文的转发机制不同。
  - 路由器：每个报文都会查路由表，当匹配上后才进行转发。链路切换后，后续报文不会受到影响，继续进行转发。
  - 状态检测防火墙：如果首包允许通过会建立一条五元组的会话连接，只有命中该会话表项的后续报文（包括返回报文）才能够通过防火墙；如果链路切换后，后续报文找不到正确的表项，会导致业务中断。
- 如要保障防火墙双机热备的顺利运行，VRRP在防火墙中应用还需满足以下条件：VRRP状态的一致性和防火墙状态信息的一致性。

目录

VGMP基本原理（1）

- 为了保证所有VRRP备份组切换的一致性，在VRRP的基础上进行了扩展，推出了VGMP（VRRP组管理协议）来弥补此局限。将同一台防火墙上的多个VRRP备份组都加入到一个VGMP管理组，由管理组统一管理所有VRRP备份组的状态，来保证管理组内的所有VRRP备份组状态都是一致的。
  - 防火墙VGMP组状态分为三类：Load-balance、Active、Standby；
  - 防火墙VGMP组通过发送VGMP报文通告自身运行状态，从而根据Hello优先级决定主备设备，主设备VGMP组的状态为Active，备设备VGMP组的状态为Standby；
  - 当防火墙上的VGMP组为Active/Standby状态时，组内所有VRRP备份组的状态统一为Active/Standby状态。
- VGMP组选举主从设备工作流程如图所示。



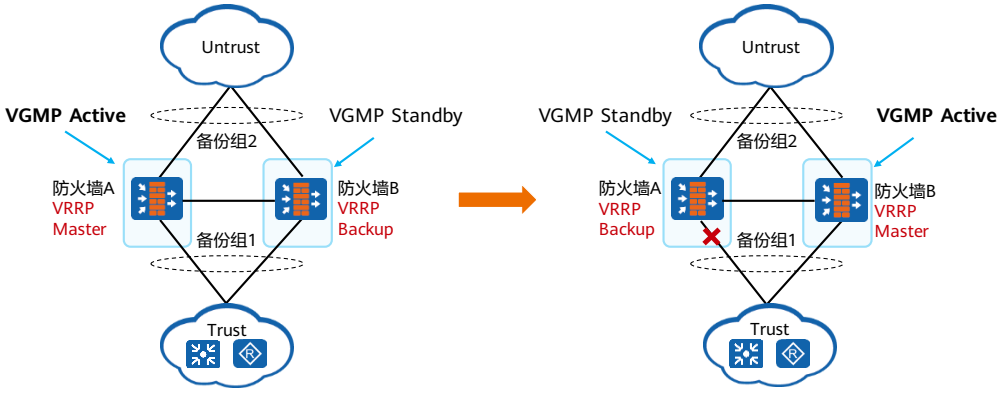
HUAWEI

- VGMP（VRRP Group Management Protocol）是VRRP组管理协议，该协议定义了VGMP组，防火墙基于VGMP组实现设备主备状态管理。
- VGMP状态：
  - Initialize是初始化状态，设备未启用双机热备功能时，VGMP组处于这个状态；
  - 设备自身的VGMP组优先级等于对端设备的VGMP组优先级时，设备的VGMP组状态为Load-balance；
  - 设备自身的VGMP组优先级大于对端设备的VGMP组优先级时，设备的VGMP组状态为Active；
  - 设备自身的VGMP组优先级小于对端设备的VGMP组优先级时，设备的VGMP组状态为Standby；
  - 设备没有接收到对端设备的VGMP报文，无法了解到对端VGMP组优先级时，设备的VGMP组状态为Active；
  - 当防火墙上的VGMP为Active状态时，它保证组内所有VRRP备份组的状态统一为Active状态，这样所有报文都将从该防火墙上通过，该防火墙成为主用防火墙。此时另外一台防火墙上对应的VGMP为备状态，该防火墙成为备用防火墙。
- VGMP报文：VGMP报文包含VGMP Hello报文、HRP Hello报文以及HRP数据报文。
  - VGMP报文发送周期缺省为1秒，通过心跳口发送；

    - VGMP Hello报文用于协商防火墙主备状态，主备防火墙VGMP组定期向对端发送VGMP Hello报文，通知对端本身的运行状态（优先级、设备状态等），事件触发时也会发送VGMP报文（如VGMP开启，优先级改变）；
    - HRP Hello报文用于探测对端的VGMP组是否处于工作状态，主备防火墙VGMP组定期向对端发送HRP Hello报文，当Standby端五个报文周期没有收到对端发送的HRP Hello报文时，会认为对端出现故障，从而将自己切换到Active状态。
- VGMP组选举主设备工作流程如下：
    - 配置VRRP：配置VRRP备份组1和VRRP备份组2，备份组1和备份组2指定防火墙A为Master设备，防火墙B为Backup设备；
    - 启用防火墙VGMP功能：备份组1和备份组2被防火墙A和防火墙B的VGMP组纳管；
    - 选举VGMP主设备：启用VGMP功能后，VRRP备份组的优先级失效，VRRP Master设备由VGMP优先级指定。防火墙A和防火墙B相互发送VGMP Hello报文，默认情况下，两台防火墙VGMP组的优先级相同，优先级为45000（不同防火墙型号和版本有所区别），此时根据VRRP的配置决定防火墙VGMP组的状态；
    - 切换VRRP组状态：根据配置，防火墙A成为主设备，状态为Active；防火墙B为备设备，状态为Standby。此时备份组1和备份组2皆以防火墙A为Master设备，由防火墙A转发流量。

VGMP基本原理（2）

- 当故障发生时，VGMP统一切换VRRP备份组1与VRRP备份组2的状态。当VGMP组状态为Active时，VRRP备份组的状态都是Master；当VGMP组状态为Standby时，VRRP备份组的状态都是Backup；



- 防火墙正常时工作原理如左图，在防火墙A上将VRRP备份组1和VRRP备份组2都加入状态为Active的VGMP组，在防火墙B上将VRRP备份组1和VRRP备份组2都加入状态为Standby的VGMP组。由于VGMP组的状态决定了组内VRRP备份组的状态，所以防火墙A上VRRP备份组1和2的状态都为Master，防火墙B上VRRP备份组1和2的状态都为Backup。这样防火墙A就是VRRP备份组1和VRRP备份组2中的Master设备（也就是两台防火墙中的主用设备），而防火墙B就是他们的Backup设备（也就是两台防火墙中的备用设备），所以上下行的业务流量都会被引导到主用设备防火墙A转发。
- 防火墙故障时工作原理如右图，当防火墙A的接口故障时，VGMP组控制VRRP备份组状态统一切换的过程如下：
  - 当防火墙A的下联接口故障时，防火墙A上的VRRP备份组1发生状态切换（由Master切换成Initialize）；
  - 防火墙A的VGMP组感知到这一故障后，会降低自身的优先级，然后与防火墙B的VGMP组比较优先级，重新协商主备状态；
  - 协商后，防火墙A的VGMP组状态由Active切换成Standby，防火墙B的VGMP组状态由Standby切换成Active；
  - 同时，由于VGMP组的状态决定了组内VRRP备份组的状态，所以防火墙A的VGMP组会强制组内的VRRP备份组2由Master切换成Backup状态，防火墙B的VGMP组也会强制组内的VRRP备份组1和2由Backup切换成Master状态。这样防火墙B就成为了VRRP备份组1和VRRP备份组2中的Master设备，也就成了为两台防火墙中的主用设备；而防火墙A则成为了VRRP备份组1和VRRP备份组2中的Backup设备，也就成为了两台防火墙中的备用设备；

    - 防火墙B会分别向Trust和Untrust区域发送免费ARP，更新他们的MAC转发表，使Trust访问Untrust的上行报文和回程报文都转发到防火墙B。这样就完成了VRRP备份组状态的统一切换，并且保证业务流量不会中断。
- 如下故障会引发防火墙VGMP状态切换，不同故障降低的优先级数值不同：
    - VGMP组监控的接口故障；
    - VGMP监控的链路故障；
    - 接口板故障；
    - 业务板故障；
    - 交换网板故障。

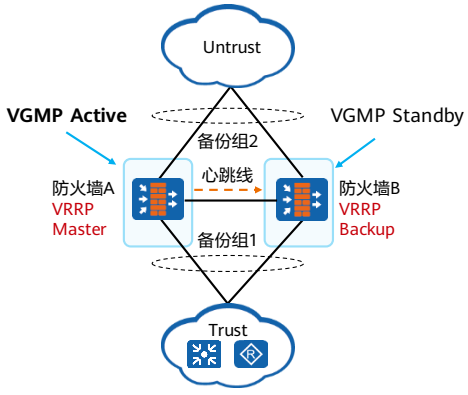
VGMP组管理

- 状态一致性管理
  - VGMP管理组控制所有的VRRP备份组统一切换，VRRP备份组加入到管理组后状态不能单独切换。
- 抢占管理
  - 当原来出现故障的主设备故障恢复时，其VGMP管理组优先级也会恢复，此时可以重新将自己的VGMP管理组状态抢占为主；
  - 当VRRP备份组加入到VGMP管理组后，备份组上原来的抢占功能将失效，抢占行为发生与否必须由VGMP管理组统一决定。
- 通道管理
  - 所谓通道管理，就是为了确定双机热备的两台防火墙之间有哪些接口是可用的，VGMP、HRP模块将自动选用可用的接口来发送VGMP、HRP报文。

目录

HRP基本概念

- HRP（Huawei Redundancy Protocol）协议，用来实现防火墙双机之间状态信息和关键配置命令的动态备份。
- 备份方向
  - 支持备份的配置命令默认只能在配置主设备上执行，这些命令会自动备份到备设备上。例如，安全策略配置命令、NAT策略配置命令等；
  - 主备备份组网中，只有主设备会处理业务，主设备上生成业务表项，并向备设备备份。负载分担组网中，两台防火墙都会处理业务，都会生成业务表项并向对端设备备份。
- 备份通道
  - 配置和状态数据需要网络管理员指定备份通道接口进行备份。一般情况下，在两台设备上直连的端口作为备份通道，有时也称为“心跳线”（VGMP也通过该通道进行通信）。



配置备份与状态信息备份

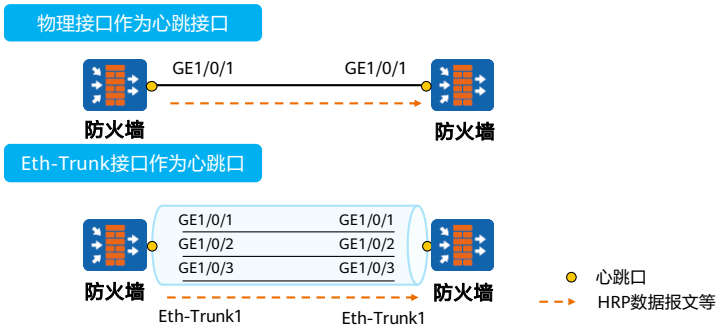
- 为了让两台设备故障切换时业务能平滑切换，两台设备间需要备份配置和状态信息。

备份方式	备份内容
• 自动备份：缺省为开启状态，能够自动实时备份配置命令和周期性地备份状态信息，适用于各种双机热备组网。 • 手工批量备份：需要管理员手工触发，每执行一次手工批量备份命令，主用设备就会立即同步一次配置命令和状态信息到备用设备。 • 设备重启主备防火墙的配置自动同步：重启成功的设备会自动从当前承载业务的防火墙上进行一次配置同步。 • 会话快速备份：会话快速备份功能，适用于负载分担的工作方式，以应对报文来回路径不一致的场景。	• 设备配置： ▫ 策略：安全策略、NAT策略、认证策略、攻击防范和ASPF等； ▫ 对象：地址、地区、服务、应用、用户、认证服务器、时间段、地址池、URL分类、关键字组、邮件地址组、签名和安全配置文件等； ▫ 网络：新建逻辑接口、安全区域、DNS、静态路由（配置hrp auto-sync config static-route后才可以备份）、IPSec和SSL VPN等； ▫ 系统：管理员、虚拟系统、日志配置等。 • 状态信息：会话表、Sever-map表、黑白名单、地址映射表、MAC表、用户表、IPSec安全联盟和隧道等。

- 开启会话快速备份功能后：
  - 到设备自身和从设备发出的报文产生的会话不会备份；
  - 对于ICMP协议，设备收到ICMP ECHO-REQUEST报文，生成会话后就立即备份会话；
  - 对于TCP协议，设备收到SYN报文，生成会话后就立即备份会话；
  - 对于UDP协议，设备收到正向的首个报文，生成会话后就立即备份会话。

HRP心跳线

- 双机热备组网中，心跳线是两台防火墙交互消息了解对端状态、备份配置命令和各种表项的通道。
  - 心跳线两端的接口通常被称之为“心跳接口”；
  - 心跳接口可以是一个物理接口（GE接口），或者多个物理接口捆绑成的一个逻辑接口（Eth-Trunk）。

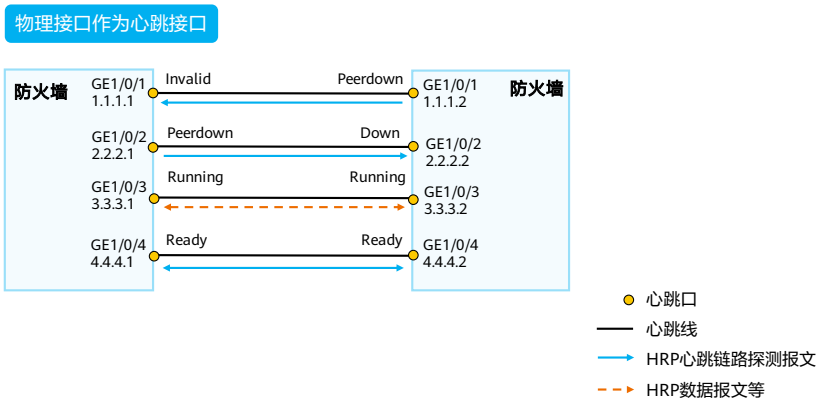


HUAWEI

- 心跳线主要传递如下消息：
  - HRP Hello报文：两台防火墙通过定期（默认周期为1秒）互相发送心跳报文检测对端设备是否存活，也称为HRP心跳报文；
  - VGMP Hello报文：了解对端设备的VGMP组的状态，确定本端和对端设备当前状态是否稳定，是否要进行故障切换；
  - HRP数据报文：用于两台防火墙同步配置命令和状态信息；
  - 心跳链路探测报文：用于检测对端设备的心跳口能否正常接收本端设备的报文，确定是否有心跳接口可以使用；
  - 配置一致性检查报文：用于检测两台防火墙的关键配置是否一致，如安全策略、NAT等；
  - 上述报文均不受防火墙的安全策略控制。因此，不需要针对这些报文配置安全策略。
- 通常情况下，备份数据流量约为业务流量的20%～30%，请根据备份数据量的大小选择捆绑物理接口的数量。

心跳接口的状态

- HRP心跳接口共有五种状态：Invalid、Down、Peerdown、Ready、Running。



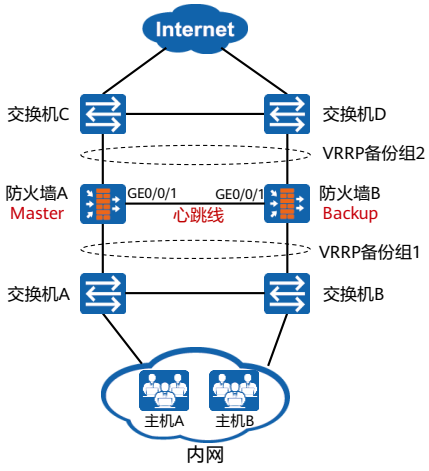
HUAWEI

- Invalid：当本端防火墙上的心跳口配置错误时显示此状态（物理状态up，协议状态down），例如指定的心跳口为二层接口或未配置心跳接口的IP地址。
- Down：当本端防火墙上的心跳口的物理与协议状态均为down时，则会显示此状态。
- Peerdown：当本端防火墙上的心跳口的物理与协议状态均为up时，则心跳口会向对端对应的心跳口发送心跳链路探测报文。如果收不到对端响应的报文，那么防火墙会设置心跳接口状态为Peerdown。但是心跳口还会不断发送心跳链路探测报文，以便当对端的对应心跳口up后，该心跳链路能处于连通状态。
- Ready：当本端防火墙上的心跳口的物理与协议状态均为up时，则心跳口会向对端对应的心跳口发送心跳链路探测报文。如果对端心跳口能够响应此报文（也发送心跳链路探测报文），那么防火墙会设置本端心跳接口状态为ready，随时准备发送和接受心跳报文。这时心跳口依旧会不断发送心跳链路探测报文，以保证心跳链路的状态正常。
- Running：当本端防火墙有多个处于ready状态的心跳口时，防火墙会选择最先配置的心跳口形成心跳链路，并设置此心跳口的状态为Running。如果只有一个处于Ready状态的心跳口，那么它自然会成为状态为Running的心跳口。状态为Running的接口负责发送HRP心跳报文、HRP数据报文、HRP链路探测报文、VGMP报文和一致性检查报文。这时其余处Ready状态的心跳口处于备份状态，当处于Running状态的心跳口或心跳链路故障时，其余处于Ready状态的心跳口依次（按配置先后顺序）接替当前心跳口处理业务。

目录

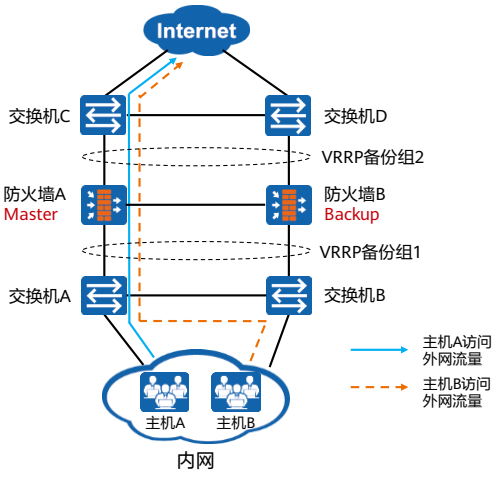
防火墙双机热备主备备份应用场景

- 应用场景
  - 主要应用于对可靠性要求较高场景，如企业办公场景，为提升网络可靠性，可在企业网络出口部署两台防火墙构成双机热备的组网。综合考虑业务需求，双机热备采用主备模式。
- 配置分析
  - 防火墙VGMP状态：防火墙A为主设备，VGMP状态为Active；防火墙B为备设备，VGMP状态为Standby；
  - VRRP 备份组：防火墙下游配置VRRP备份组1 ，防火墙上游配置VRRP备份组2；VRRP备份组1和2设置防火墙A为Master，VRRP备份组1和2设置防火墙B为Backup；
  - 备份方式：默认情况下，双机热备采用自动备份方式；
  - 备份接口：防火墙GE0/0/1接口为心跳口，所连接的线路为心跳线；
  - 抢占：默认开启，默认抢占时延为60s。



防火墙双机热备主备备份工作流程

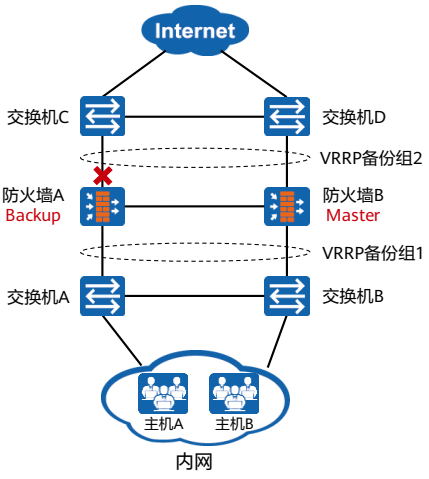
- 防火墙主备状态：防火墙A为主设备，VGMP状态为Active，VRRP备份组1和2状态为Matser；防火墙B为备设备，VGMP状态为Standby，VRRP备份组1和2状态为Backup；
- 配置与状态备份：防火墙A的配置与状态信息通过心跳线实时备份到防火墙B；
- 流量转发路径：防火墙A向交换机A和交换机C发送免费ARP报文，刷新交换机的MAC地址表。当主机A访问Internet时，首先通过ARP查询网关MAC地址（即查询VRRP Virtual IP的MAC地址），防火墙A回应VRRP Virtual MAC，主机A向交换机A发送业务报文，交换机A根据MAC表转发流量到防火墙A，防火墙A再转发到Internet。返程同理。



HUAWEI

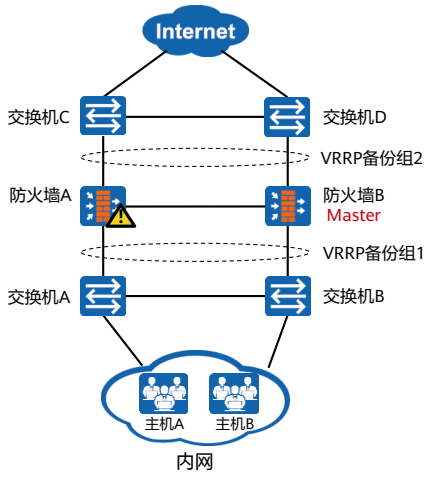
防火墙双机热备主备切换（1）

- 业务口/业务线路故障
  - 如图所示，防火墙A的业务口/所连业务线出现故障时，防火墙A的VGMP组优先级降低，发送VGMP请求报文；
  - 防火墙B收到对端发送的VGMP请求报文后，与自己的VGMP组优先级进行比较，发送VGMP应答报文；
  - 防火墙A收到回应报文，将VGMP组状态切换为Standby，防火墙A上的VRRP备份组1和备份组2则切换状态为Backup；
  - 防火墙B将VGMP组状态切换为Active，防火墙B上的VRRP备份组1和备份组2则切换状态为Master。由防火墙B向交换机B和D发送免费ARP报文。



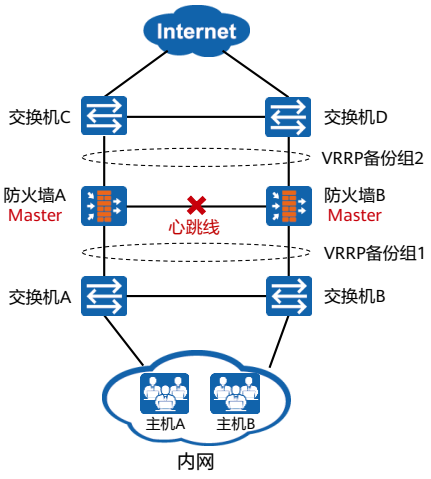
防火墙双机热备主备切换（2）

- 整机故障
  - 防火墙A出现整机故障，不再发送HRP Hello报文，防火墙B五个报文周期没有收到对端发送的HRP Hello报文，则防火墙B切换为主设备，VGMP状态为Active，防火墙B上的VRRP备份组1和备份组2则切换状态为Master。



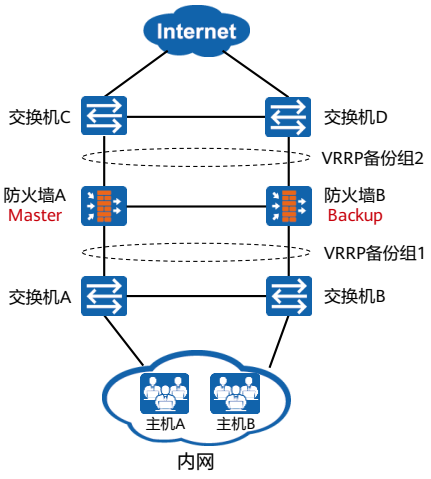
防火墙双机热备主备切换（3）

- 心跳线故障
  - 心跳线出现故障，防火墙B五个报文周期没有收到对端发送的HRP Hello报文，则防火墙B切换为主设备，VGMP状态为Active，防火墙B上的VRRP备份组1和备份组2则切换状态为Master。此时出现双主现象。



防火墙双机热备主备切回切

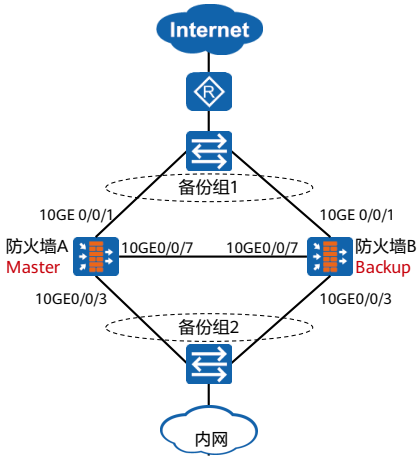
- 防火墙A故障恢复后，此时VGMP组优先级恢复，在等待60s后，发送VGMP请求报文；
- 防火墙B收到VGMP请求报文后，与自己的VGMP组优先级进行比较，发现对端的优先级较高或相等（相等时查看VGMP的配置），则回应VGMP应答报文，同时将自己的VGMP组状态切换为Standby，VRRP备份组1和2状态切换为Backup；
- 防火墙A收到回应报文后，将自己的VGMP状态切换为Active，VRRP备份组1和2状态切换为Master。



目录

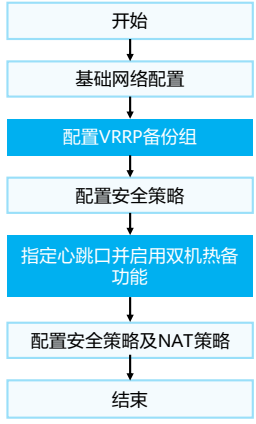
防火墙主备备份双机热备配置举例（1）

- 需求描述：
  - 防火墙A和防火墙B的业务接口都工作在三层，上下行分别连接二层交换机。上行交换机连接运营商的接入点，运营商为企业分配的IP地址为1.1.1.1 。现在希望防火墙A和防火墙B以主备备份方式工作。正常情况下，流量通过防火墙A转发；当防火墙A出现故障时，流量通过防火墙B转发，保证业务不中断；
  - VRRP备份组1的虚拟IP：1.1.1.1/24；
  - VRRP备份组2的虚拟IP：10.3.0.3/24；
  - 防火墙A心跳接口10GE0/0/7地址：10.10.0.1/24；
  - 防火墙B心跳接口10GE0/0/7地址：10.10.0.2/24。



防火墙主备备份双机热备配置举例（2）

- 配置思路：
  - 完成基本网络配置：包括配置防火墙各接口的IP地址，将防火墙各接口加入相应的安全区域及缺省路由配置；
  - 配置VRRP备份组：在两台防火墙上完成VRRP备份组配置；
  - 配置安全策略，允许心跳口之间交互HRP报文；
  - 指定心跳接口，配置认证密钥，并启用双机热备功能；
  - 配置安全策略，允许内网用户访问Internet；
  - 配置NAT策略，让内网用户成功访问Internet。



防火墙主备备份双机热备配置举例（3）

- 在防火墙A上行业务接口10GE0/0/1上配置VRRP备份组1，并设置其状态为Active。

```
[FWA] interface 10ge0/0/1
[FWA-10GE0/0/1] vrrp vrid 1 virtual-ip 1.1.1.1 active
[FWA-10GE0/0/1] quit

[FWA] interface 10ge0/0/3
[FWA-10GE0/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 active
[FWA-10GE0/0/3] quit
```

- 在防火墙B上行业务接口10GE0/0/1上配置VRRP备份组1，并设置其状态为Standby。

```
[FWB] interface 10ge0/0/1
[FWB-10GE0/0/1] vrrp vrid 1 virtual-ip 1.1.1.1 standby
[FWB-10GE0/0/1] quit

[FWB] interface 10ge0/0/3
[FWB-10GE0/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 standby
[FWB-10GE0/0/3] quit
```

防火墙主备备份双机热备配置举例（4）

- 在防火墙A指定心跳接口，配置认证密钥，并启用双机热备功能。

```
[FWA] hrp interface 10ge0/0/7 remote 10.10.0.2
[FWA] hrp authentication-key Admin@123
[FWA] hrp enable
```

- 在防火墙B指定心跳接口，配置认证密钥，并启用双机热备功能。

```
[FWB] hrp interface 10ge0/0/7 remote 10.10.0.1
[FWB] hrp authentication-key Admin@123
[FWB] hrp enable
```

思考题

1. （判断题）HRP技术可以实现备防火墙不需要配置任何信息，所有配置信息均由主防火墙通过HRP同步至备防火墙，且重启后配置信息不丢失。（　　）

   A. 正确

   B. 错误

2. （判断题）防火墙会话快速备份适用于负载均衡场景。（　　）

   A. 正确

   B. 错误

1. B
2. A

本章总结

- 本课程简要介绍了双机热备的应用场景、实现技术原理、报文转发流程以及主备倒换时的切换逻辑，同时介绍了双机热备不同组网的关键配置和配置流程。
- 通过本课程的学习，您将能够对双机热备使用场景有一定的了解，搭配基于实际环境的实验，能独立完成华为防火墙双机热备的配置，并掌握防火墙在双机热备场景中的部署方法。

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

缩略语表

缩略语	英文全称	解释
GE	Gigabit Ethernet	千兆以太网
HRP	Huawei Redundancy Protocol	华为冗余协议
USG	Universal Service Gateway	通用业务网关
VGMP	VRRP Group Management Protocol	VRRP组管理协议
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

防火墙入侵防御

HUAWEI

前言

- 在目前出现的各种安全威胁当中，恶意程序类别占有很高的比例，灰色软件的影响也逐渐扩大，而与恶意代码有关的安全威胁已经成为网络安全的重要影响因素。
- 目前用户面临的不再是传统的病毒攻击，“网络威胁”经常是融合了病毒、黑客入侵、木马、僵尸和间谍等危害于一身的混合体，因此单靠以往的防病毒或者单一的安全技术往往难以抵御。
- 本章节主要对入侵的概念以及华为防火墙产品入侵防御功能进行介绍。

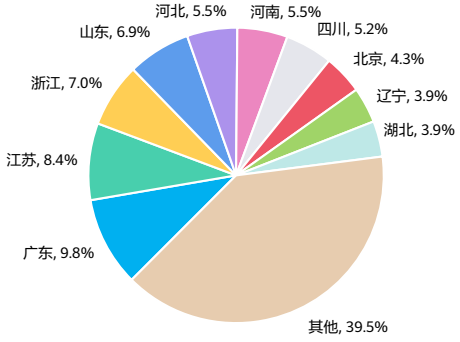
目标

- 学完本课程后，您将能够：
  - 描述入侵防御的种类
  - 描述入侵防御基本原理
  - 应用网络反病毒策略

目录

网络威胁现状

- 根据CNCERT发布的《2021年上半年我国互联网网络安全监测数据分析报告》，我国上半年境内受计算机恶意程序攻击的IP分布情况如下图。



HUAWEI

- 2021年上半年，捕获恶意程序样本数量约2307万个，日均传播次数达582万余次，涉及恶意程序家族约20.8万个。境内来源主要来自河南省、广东省和浙江省等。按照攻击目标IP地址统计，我国境内受恶意程序攻击的IP地址近3048万个，约占我国IP地址总数的7.8%。按照传播来源统计，主要来源境外，这些受攻击的IP地址主要集中在广东省、江苏省以及浙江省等地区。

网络安全事件举例

- 现在大多数病毒等网络威胁不再单纯地攻击电脑系统，而是被黑客攻击和不法分子利用，成为他们获取利益的工具。因此，传统的电脑病毒等网络威胁，正在向由利益驱动的、全面的网络威胁发展变化。

案例一

黑客攻击了某国最大的成品油管道运营商，迫使该运营商一度关闭整个能源供应网络，极大影响了国家燃油能源供应，同时导致了该国家首次因网络攻击而进入国家紧急状态。

案例二

某国公共部门的互联网服务提供商遭到大规模分布式拒绝服务（DDoS）攻击，导致政府的内部系统与面向公众的网站全部离线，政府许多网站和服务被迫下线。

案例三

某计算机巨头遭到了勒索软件攻击，勒索软件团伙成功入侵该巨头的系统，并公布了部分该公司的财务电子表格及银行对账单，索要的赎金达到5000万美元，是迄今为止已知数额最大的一笔赎金。

- 在目前出现的各种安全威胁当中，恶意程序（病毒与蠕虫、Bot、Rootkit、特洛依木马与后门程序、弱点攻击程序以及行动装置恶意程序等）类别占有很高的比例，灰色软件（间谍/广告软件）的影响也逐渐扩大，而与犯罪程序有关的安全威胁已经成为威胁网络安全的重要因素。

入侵概述

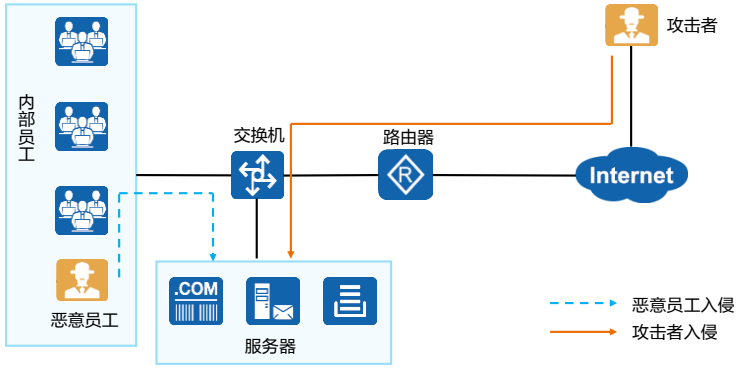
- 入侵是指未经授权而尝试访问信息系统资源、篡改信息系统中的数据，使信息系统不可靠或不能使用的行为。
- 入侵企图破坏信息系统的完整性、机密性、可用性以及可控性。
- 常见入侵手段有：
  - 利用系统及软件的漏洞
  - DDoS攻击
  - 病毒及恶意软件安全威胁

威胁 / 特征	未经授权访问	未经授权篡改	未经授权破坏
系统及软件漏洞	✓	✓	✓
DDoS攻击威胁	✓		✓
病毒及恶意软件	✓	✓	✓

- 典型的入侵行为有：
  - 篡改Web网页；
  - 破解系统密码；
  - 复制/查看敏感数据；
  - 使用网络嗅探工具获取用户密码；
  - 访问未经允许的服务器；
  - 其他特殊硬件获得原始网络包；
  - 向主机植入特洛伊木马程序。

漏洞威胁

- 网络攻击者、企业内部恶意员工利用系统及软件的漏洞入侵服务器，严重威胁企业关键业务数据的安全。

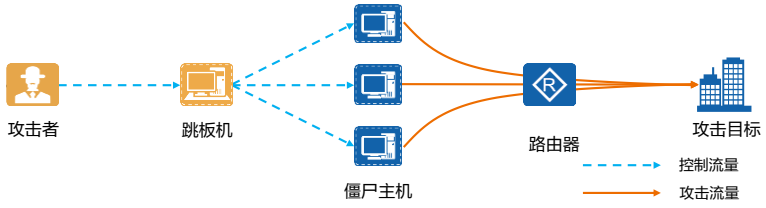


HUAWEI

- 漏洞给企业造成严重的安全威胁：
  - 企业内网中许多应用软件可能存在漏洞；
  - 互联网使应用软件的漏洞迅速传播；
  - 蠕虫利用应用软件漏洞大肆传播，消耗网络带宽，破坏重要数据；
  - 黑客、恶意员工利用漏洞攻击或入侵企业服务器，业务机密被篡改、破坏和偷窃。

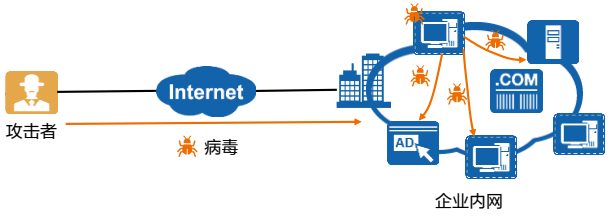
DDoS攻击

- DDoS（Distributed Denial of Service）即分布式拒绝服务。DDoS攻击是指攻击者通过控制大量的僵尸主机，向被攻击目标发送大量精心构造的攻击报文，造成被攻击者所在网络的链路拥塞、系统资源耗尽，从而使被攻击者产生拒绝向正常用户提供服务的效果。
- 目前，互联网中存在着大量的僵尸主机和僵尸网络，在商业利益的驱使下，DDoS攻击已经成为互联网面临的重要安全威胁。遭受DDoS攻击时，网络带宽被大量占用，网络陷于瘫痪；受攻击服务器资源被耗尽无法响应正常用户请求，严重时会造成系统死机，企业业务无法正常运行。



恶意代码入侵威胁

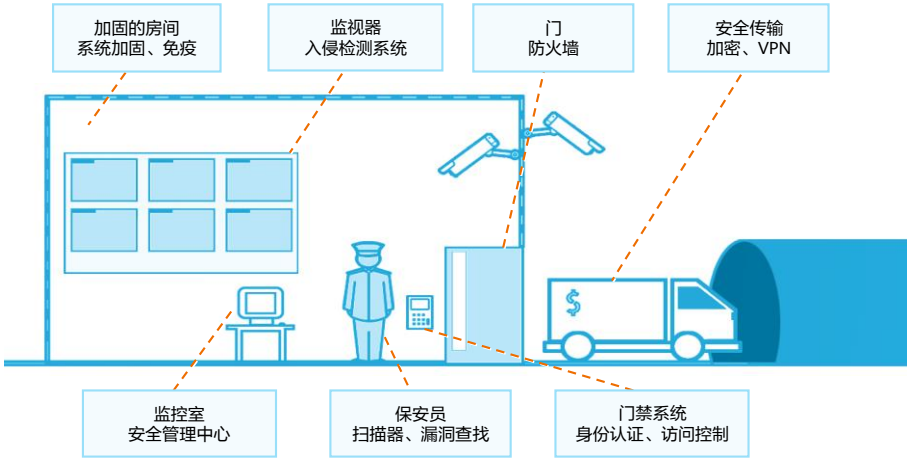
- 恶意代码包含病毒、木马和间谍软件等。恶意代码可感染或附着在应用程序或文件中，一般通过邮件或文件共享等方式进行传播，威胁用户主机和网络的安全。恶意代码入侵威胁包括以下特点：
  - 浏览网页和邮件传输是病毒、木马、间谍软件进入内网的主要途径；
  - 病毒能够破坏计算机系统，篡改、损坏业务数据；
  - 木马使攻击者不仅可以窃取计算机上的重要信息，还可以对内网计算机破坏；
  - 间谍软件搜集、使用并散播企业员工的敏感信息，严重干扰企业的正常业务；
  - 桌面型反病毒软件难以从全局上防止恶意代码泛滥。



- 当前的反病毒软件可防范恶意代码。

目录

安全设备在安全体系中的位置

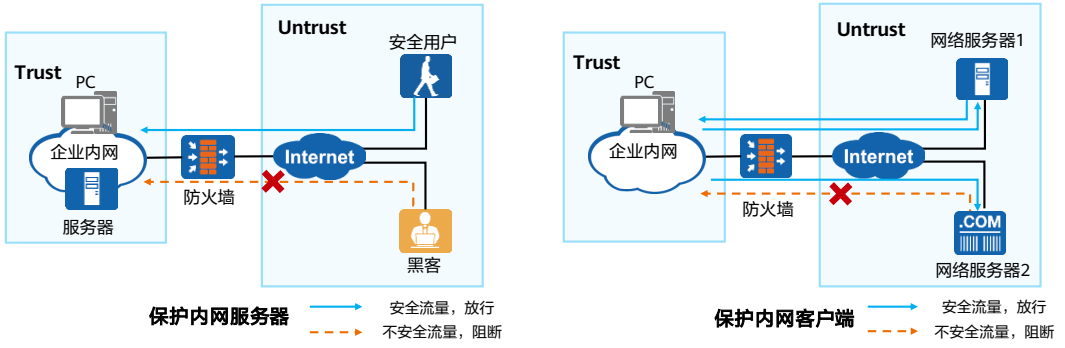


HUAWEI

- 入侵检测（ID，Intrusion Detection）通过监视各种操作，分析、审计各种数据和现象来实时检测入侵行为的过程，是一种积极的和动态的安全防御技术。入侵检测的内容涵盖了授权的和非授权的各种入侵行为。
- 入侵检测系统（IDS，Intrusion Detection System）能在发现有违反安全策略的行为或系统存在被攻击的痕迹时，立即启动有关安全机制进行应对。
- 在信息安全建设中，入侵检测系统扮演着监视器的角色，通过监控信息系统关键节点的流量，对其进行深入分析，发掘正在发生的安全事件。一个形象的比喻就是：IDS就像安全监控体系中的摄像头，通过IDS，系统管理员能够捕获关键节点的流量并做智能的分析，从中发现异常、可疑的网络行为，并向管理员报告。

入侵防御概述

- 入侵防御是一种安全机制。通过分析网络流量，检测入侵（包括缓冲区溢出攻击、木马、蠕虫等），并通过一定的响应方式，实时地中止入侵行为，保护企业信息系统和网络架构免受侵害。
- 入侵防御功能通常用于防护来自内部或外部网络对内网服务器和客户端的入侵。

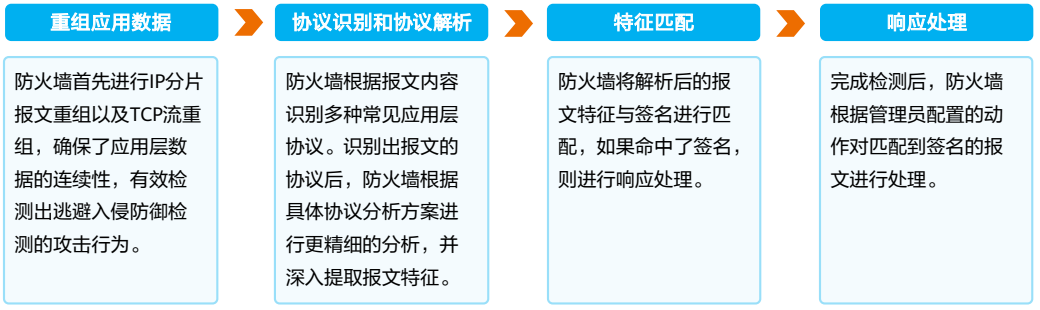


HUAWEI

- 入侵防御是一种既能发现又能阻止入侵行为的新安全防御技术。通过检测发现网络入侵后，能自动丢弃入侵报文或者阻断攻击源，从根本上避免攻击行为。
- 入侵防御的主要优势有如下几点：
  - 实时阻断攻击：设备直路部署在网络中，能够实时对入侵活动和攻击性网络流量进行拦截，将对网络的影响降到最低。
  - 深层防护：新型的攻击都隐藏在TCP/IP协议的应用层里，入侵防御不但能检测报文应用层的内容，还可以对网络数据流重组进行协议分析和检测，并根据攻击类型、策略等确定应该被拦截的流量。
  - 全方位防护：入侵防御可以提供针对蠕虫、病毒、木马、僵尸网络、间谍软件、广告软件、CGI（Common Gateway Interface）攻击、跨站脚本攻击、注入攻击、目录遍历、信息泄露、远程文件包含攻击、溢出攻击、代码执行、拒绝服务、扫描工具等多种攻击的防护措施，全方位保护网络安全。
  - 内外兼防：入侵防御不但可以防止来自于企业外部的攻击，还可以防止来自于企业内部的攻击。设备对经过的流量都可以检测，既可以对服务器进行防护，也可以对客户端进行防护。
  - 精准防护：入侵防御特征库持续更新，使设备拥有最新的入侵防御能力。您可以从云端安全中心定期升级设备的特征库，以保持入侵防御的持续有效性。

入侵防御实现机制

- 入侵防御的基本实现机制包括以下四块内容：



签名

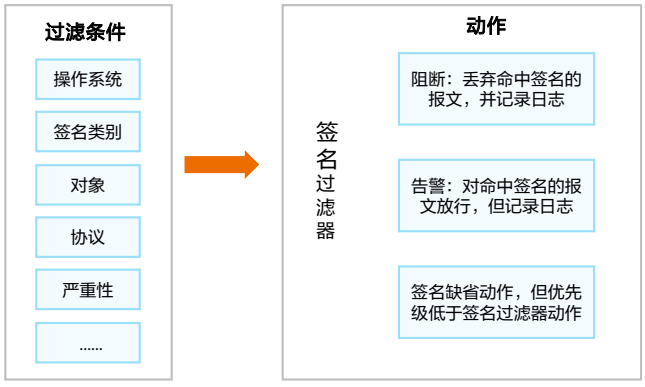
- 入侵防御签名用来描述网络中攻击行为的特征，防火墙通过将数据流和入侵防御签名进行比较来检测和防范攻击。

预定义签名	自定义签名
• 预定义签名是入侵防御特征库中包含的签名。预定义签名的内容是固定的，不能创建、修改或删除。 • 每个预定义签名都有缺省的动作，分别为： ▫ 放行：指对命中签名的报文放行，不记录日志； ▫ 告警：指对命中签名的报文放行，但记录日志； ▫ 阻断：指丢弃命中签名的报文，阻断该报文所在的数据流，并记录日志。	• 自定义签名是指管理员通过自定义规则创建的签名。 • 新的攻击出现后，其对应的攻击签名通常都会晚一点才会出现。当用户自身对这些新的攻击比较了解时，可以自行创建自定义签名以便实时地防御这些攻击。 • 自定义签名创建后，系统会自动对自定义规则的合法性进行检查，避免低效签名浪费系统资源。 • 自定义签名的动作分为阻断和告警，可以在创建自定义签名时配置签名的响应动作。

- 建议只在非常了解攻击特征的情况下才配置自定义签名。因为自定义签名设置错误可能会导致配置无效，甚至导致报文误丢弃或业务中断等问题。

签名过滤器

- 由于设备升级签名库后会存在大量签名，而这些签名是没有进行分类的，且有些签名所包含的特征本网络中不存在，需要设置签名过滤器对其进行管理，并过滤掉。签名过滤器是满足指定过滤条件的集合。



HUAWEI

- 签名过滤器的过滤条件包括：签名的类别、对象、协议、严重性、操作系统等。只有同时满足所有过滤条件的签名才能加入签名过滤器中。一个过滤条件中如果配置多个值，多个值之间是“或”的关系，只要匹配任意一个值，就认为匹配了这个条件。
- 签名过滤器的动作分为阻断、告警和采用签名的缺省动作。签名过滤器的动作优先级高于签名缺省动作，当签名过滤器的动作不采用签名缺省动作时，以签名过滤器设置的动作为准。
- 各签名过滤器之间存在优先关系（按照配置顺序，先配置的优先）。如果一个安全配置文件中的两个签名过滤器包含同一个签名，当报文命中此签名后，设备将根据优先级高的签名过滤器的动作对报文进行处理。

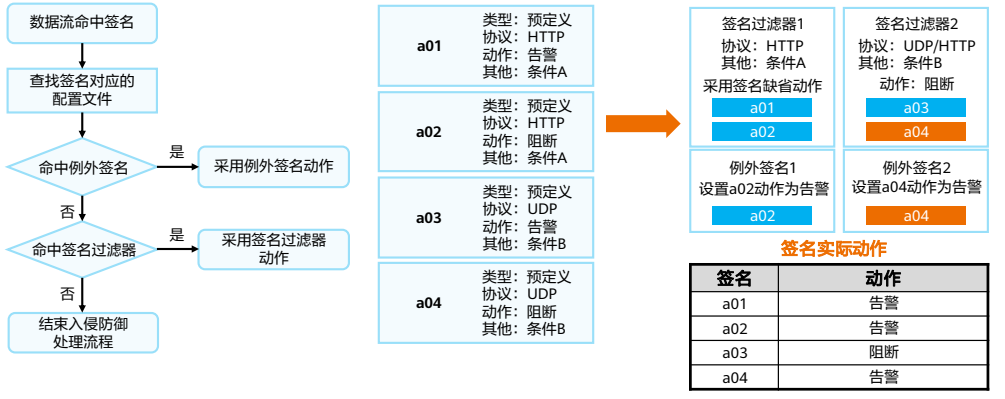
例外签名

- 由于签名过滤器会批量过滤出签名，且通常为了方便管理会设置为统一的动作。如果管理员需要将某些签名设置为与签名过滤器不同的动作时，可将这些签名引入到例外签名中，并单独配置动作。
- 例外签名的动作分为：
  - 阻断：丢弃命中签名的报文并记录日志；
  - 告警：对命中签名的报文放行，但记录日志；
  - 放行：对命中签名的报文放行，且不记录日志；
  - 添加黑名单：是指丢弃命中签名的报文，阻断报文所在的数据流，记录日志，并可将报文的源地址或目的地址添加至黑名单。
- 例外签名的动作优先级高于签名过滤器。如果一个签名同时命中例外签名和签名过滤器，则以例外签名的动作为准。

- 例如，签名过滤器中过滤出一批符合条件的签名，且动作统一设置为阻断。但是员工经常使用的某款自研软件也被拦截了。观察日志发现，用户经常使用的该款自研软件命中了签名过滤器中某个签名，被误阻断了。此时管理员可将此签名引入到例外签名中，并修改动作为放行。

入侵防御对数据流的处理

- 当数据流命中的攻击防御模板中包含入侵防御模板时，设备将数据流送到入侵防御模块，并依次匹配入侵防御模板引用的签名。

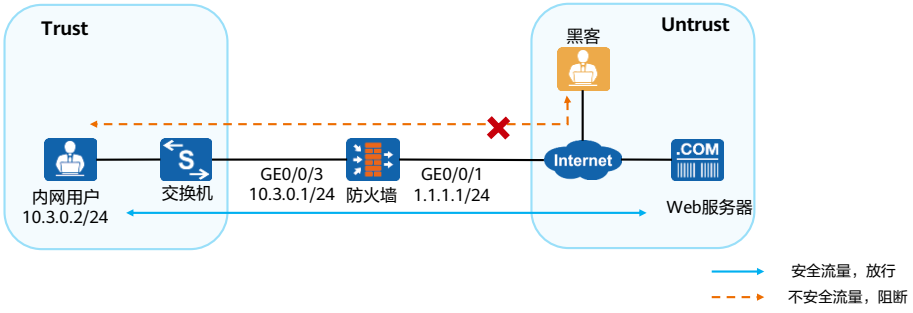


- 当数据流命中多个签名，对该数据流的处理方式如下：
  - 如果这些签名的实际动作都为告警时，最终动作为告警；
  - 如果这些签名中至少有一个签名的实际动作为阻断时，最终动作为阻断。
- 当数据流命中了多个签名过滤器时，设备会按照优先级最高的签名过滤器的动作来处理。

目录

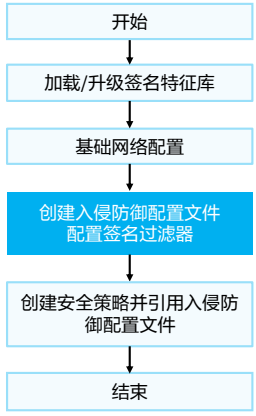
入侵防御配置举例（1）

- 需求描述：
  - 某企业在网络边界处部署了防火墙作为安全网关。在该组网中，内网用户可以访问Internet的Web服务器。
  - 该企业需要在防火墙上配置入侵防御功能，用于防范内网用户访问Internet的Web服务器时受到攻击。例如，含有恶意代码的网站对内网用户发起攻击。



入侵防御配置举例（2）

- 配置思路：
  - 配置定时升级签名特征库，可以最大限度降低误报和漏报概率；
  - 配置接口IP地址和安全区域，完成网络基本参数的配置；
  - 创建入侵防御配置文件，配置签名过滤器；
  - 配置安全策略，并将入侵防御配置文件应用到安全策略中。

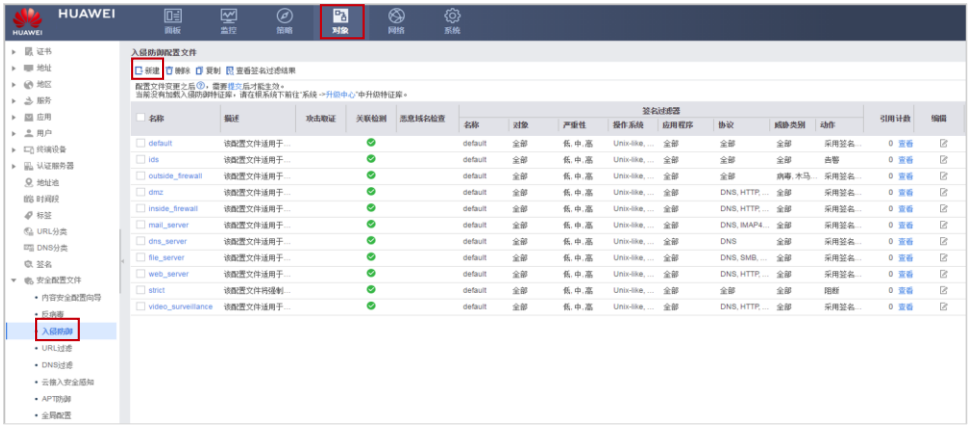


HUAWEI

- 入侵防御特征库的升级服务受入侵防御License控制项控制。License控制项未激活时，设备不会自动加载预置的特征库，也无法手动加载或者升级特征库。License控制项激活后，可以进行特征库加载和升级的相关操作。License控制项到期后，无法手动加载或者升级特征库，入侵防御功能可用，但特征库无法保证最新，入侵检测和防御能力有限。

入侵防御配置举例（3）

- 创建入侵防御配置文件，选择“对象 > 安全配置文件 > 入侵防御 > 新建”。



入侵防御配置举例 (4)

- 在“入侵防御配置文件”中，单击“新建”后，按如下参数配置。该配置将被从Trust区域到Untrust区域的安全策略引用。配置后单击“确定”，完成入侵防御配置文件的配置。

查看入侵及防御行为

- 查看威胁日志，选择“日志 > 威胁日志”。

HUAWEI

- 入侵日志信息：虚拟系统/命中的安全策略/源目地址/源目端口/源目安全域/用户/协议/应用/命中的入侵安全配置文件/签名名称/签名序号/事件计数/入侵目标/入侵严重性/操作系统/签名分类/签名动作，其中重点关注信息如下：
  - 配置文件：命中的入侵安全配置文件。
  - 威胁名称：入侵防御签名用来描述网络中存在的攻击行为的特征，通过将数据流和入侵防御签名进行比较来检测和防范攻击。
  - 事件计数：日志归并引入字段，是否归并需根据归并频率及日志归并条件来确定，不发生归并则为1。
  - 入侵目标：签名所检测的报文所攻击对象。具体情况如下：
    - server：攻击对象为服务端；
    - client：攻击对象为客户端；
    - both：攻击对象为服务端和客户端。
  - 入侵严重性：签名所检测的报文所造成攻击的严重性。具体情况如下：
    - information：表示严重性为提示；
    - low：表示严重性为低；
    - medium：表示严重性为中；
    - high：表示严重性为高。

    - 操作系统：签名所检测的报文所攻击的操作系统。具体情况如下：
        - all：表示所有系统；
        - android：表示安卓系统；
        - ios：表示苹果系统；
        - unix-like：表示Unix系统；
        - windows：表示Windows系统；
        - other：表示其他系统。
    - 签名分类：签名检测到的报文攻击特征所属的威胁分类。
- 签名动作：签名动作。具体情况如下：
    - alert：签名动作为告警；
    - block：签名动作为阻断。

目录

计算机病毒

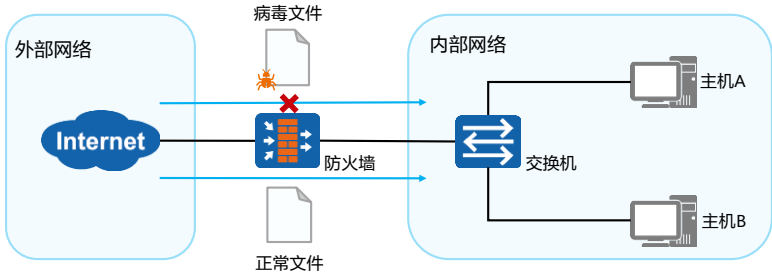
- 计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。
- 计算机病毒具有传染性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。广义的计算机病毒定义中常见的计算机病毒类型有三种，分别是病毒、蠕虫和木马。

项目	病毒	蠕虫	木马
存在形式	寄生在文件和引导中	独立个体	植入在文件或者应用中
复制机制	复制自身代码	复制自身代码	不自我复制
传染性	宿主程序运行	依靠网络和系统漏洞	依据应用或者传输载体
传染目标	针对计算机本地	针对网络上其它计算机	针对下载植入木马应用或者文件的计算机
触发机制	通过特定的条件触发	程序自身	用户执行
影响重点	文件系统、硬件	网络性能、系统性能	信息窃取或拒绝服务
防治措施	从宿主程序中摘除	使用补丁程序（Patch）对系统加固	防止木马植入

- 计算机病毒常见的传染途径：可移动媒体、网络共享、网络扫描、电子邮件和P2P网络。
- 常见的感染对象：操作系统、应用程序和设备硬件（如某病毒针对BIOS攻击）。
- 常见的计算机病毒携带者：可执行文件、脚本、宏和引导区。

反病毒产生背景

- 随着网络的不断发展和应用程序的日新月异，企业用户越来越频繁地开始在网络上传输和共享文件，随之而来的病毒威胁也越来越大。企业只有拒病毒于网络之外，才能保证数据的安全和系统的稳定。因此，保证计算机和网络系统免受病毒的侵害，让系统正常运行便成为企业所面临的一个重要问题。
- 反病毒是一种安全机制，它可以通过识别和处理病毒文件来保证网络安全，避免由病毒文件引起的数据破坏、权限更改和系统崩溃等情况发生。



HUAWEI

- 在以下场合中，通常利用反病毒功能来保证网络安全：
  - 内网用户可以访问外网，且经常需要从外网下载文件；
  - 内网部署的服务器经常接收外网用户上传的文件。
- 如图所示，防火墙作为网关设备隔离内、外网，内网包括用户PC和服务器。内网用户可以从外网下载文件，外网用户可以上传文件到内网服务器。为了保证内网用户和服务器接收文件的安全，需要在防火墙上配置反病毒功能。

自适应安全引擎检测（1）

- 反病毒的处理流程主要包括自适应安全引擎检测和反病毒处理两部分。
- 自适应安全引擎检测步骤如下：

1. 流量深层分析

- 智能感知引擎对流量进行深层分析，识别出流量对应的协议类型和文件传输的方向。

2. 判断文件传输所使用的协议和文件传输的方向是否支持病毒检测

- 防火墙支持对使用以下协议传输的文件进行病毒检测：
  - FTP、HTTP、POP3、SMTP、IMAP、NFS、SMB。
- 防火墙支持对不同传输方向上的文件进行病毒检测：
  - 上传：指客户端向服务器发送文件；
  - 下载：指服务器向客户端发送文件。

自适应安全引擎检测（2）

3. 判断文件是否命中白名单

- 命中白名单后，防火墙将不对文件做病毒检测。
  - 白名单由白名单规则组成，管理员可以为信任的域名、URL、IP地址或IP地址段配置白名单规则，以此提高反病毒的检测效率；
  - 白名单规则的生效范围仅限于所在的反病毒配置文件，每个反病毒配置文件都拥有自己的白名单。

4. 病毒检测

- 智能感知引擎对符合病毒检测的文件进行特征提取，提取后的特征与病毒特征库中的特征进行匹配。
  - 如果匹配，则认为该文件为病毒文件，并按照模板中的响应动作进行处理；
  - 如果不匹配，则允许该文件通过。

- 病毒特征库是由华为公司通过分析各种常见病毒特征而形成的。该特征库对各种常见的病毒特征进行了定义，同时为每种病毒特征都分配了一个唯一的病毒ID。当设备加载病毒特征库后，即可识别出特征库里已经定义过的病毒。同时，为了能够及时识别出最新的病毒，设备上的病毒特征库需要不断地从升级中心进行升级。

反病毒处理（1）

- 当防火墙检测出传输文件为病毒文件时，需要进行如下处理：

1. 判断该病毒文件是否命中病毒例外

- 当用户认为已检测到的某个病毒为误报时，可以将该对应的病毒ID添加到病毒例外。
- 如果检测结果命中了病毒例外，则该文件的响应动作为放行。

2. 判断该病毒文件是否命中应用例外

- 如果不是病毒例外，则判断该病毒文件是否命中应用例外。如果是应用例外，则按照应用例外的响应动作（放行、告警和阻断）进行处理。
- 在配置响应动作时：
  - 如果只配置协议的响应动作，则协议上承载的所有应用都继承协议的响应动作；
  - 如果协议和应用都配置了响应动作，则以应用的响应动作为准。

反病毒处理（2）

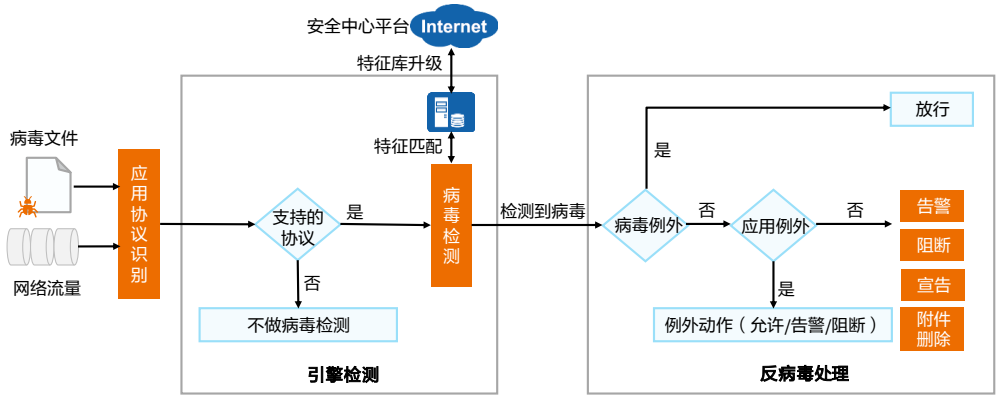
3. 按照配置文件中配置的协议和传输方向对应的响应动作进行处理

- 如果病毒文件既没命中病毒例外，也没命中应用例外，则按照配置文件中配置的协议和传输方向对应的响应动作进行处理。
- 防火墙对不同协议在不同的文件传输方向上支持不同的响应动作。

协议	传输方向	响应动作	说明
HTTP	上传/下载	告警/阻断	告警：允许病毒文件通过，同时生成病毒日志。 阻断：禁止病毒文件通过，同时生成病毒日志。 宣告：对携带病毒的邮件文件，允许该文件通过，但会在邮件正文中添加检测到病毒的提示信息，同时生成病毒日志。 删除附件：对携带病毒的邮件文件，允许该文件通过，但设备会删除邮件中的附件内容并在邮件正文中添加宣告，同时生成病毒日志。
FTP	上传/下载	告警/阻断	
NFS	上传/下载	告警	
SMB	上传/下载	告警/阻断	
SMTP	上传	告警/宣告/删除附件	
POP3	下载	告警/宣告/删除附件	
IMAP	上传/下载	告警/宣告/删除附件	

反病毒工作流程

- 防火墙利用专业的智能感知引擎和不断更新的病毒特征库实现对病毒文件的检测和处理。

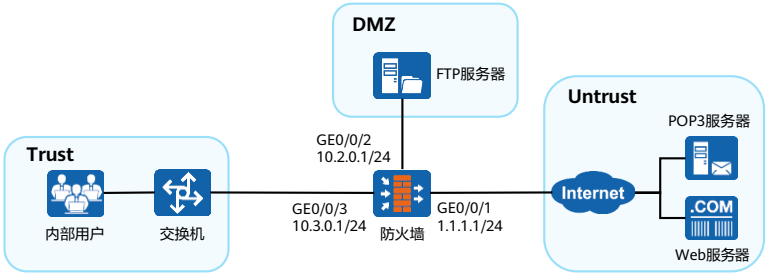


HUAWEI

目录

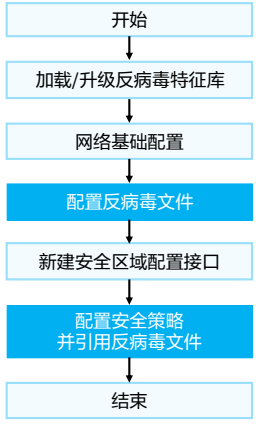
防火墙反病毒配置举例（1）

- 需求描述：
  - 某公司在网络边界处部署了防火墙作为安全网关。内网用户需要通过Web服务器和POP3服务器下载文件和邮件，内网FTP服务器需要接收外网用户上传的文件；
  - 公司利用防火墙提供的反病毒功能阻止病毒文件进入到受保护的网络，保障内网用户和服务器的安全。



防火墙反病毒配置举例（2）

- 配置思路：
  - 配置定时升级反病毒特征库，可以最大限度降低误报和漏报概率；
  - 配置接口IP地址和安全区域，完成网络基本参数配置；
  - 配置两个反病毒文件，一个反病毒配置文件针对HTTP和POP3协议设置匹配条件和响应动作，另外一个反病毒配置文件针对FTP协议设置匹配条件和响应动作；
  - 配置安全策略，在Trust到Untrust和DMZ到Untrust方向分别引用反病毒配置文件，实现组网需求。



HUAWEI

- 反病毒特征库的升级服务受反病毒License控制项控制。License控制项未激活时，设备不会自动加载预置的特征库，也无法手动加载或者升级特征库。License控制项激活后，可以进行特征库加载和升级的相关操作。License控制项到期后，无法手动加载或者升级特征库，反病毒功能可用，但特征库无法保证最新，病毒检测和防御能力有限。

防火墙反病毒配置举例（3）

- 配置反病毒文件，选择“对象 > 安全配置文件 > 反病毒”。

防火墙反病毒配置举例（4）

- 单击“新建”后，按下图完成针对HTTP和POP3协议的配置。

防火墙反病毒配置举例（5）

- 参考上述步骤按如下参数完成针对FTP协议的配置。

本章总结

- 本课程简要介绍了入侵的概念、典型的入侵手段及病毒的概念，详细介绍了入侵防御和反病毒的技术原理、检测和阻断流程，以及防火墙在入侵防御和反病毒中的相关配置方法。
- 通过本课程的学习，您能够对入侵防御使用场景有一定的了解，搭配基于实际环境的练习，学员将能独立完成华为防火墙入侵防御的配置，并掌握防火墙在入侵防御场景中的部署方法。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

防火墙用户管理技术

HUAWEI

前言

- 信息安全事件频繁发生，大多数是由于内部用户和管理员安全意识薄弱或误操作导致，而权限管理不当使得安全事件的影响范围扩大、系统损害加深。
- 在企业网应用场景中，用户是访问网络资源的主体，为了保证网络资源的安全性，应该对用户进行适当的认证和合理的授权。
- 用户管理技术使管理员有能力控制用户对网络资源的访问。对于任何网络，用户管理都是最基本的安全管理要求之一。

目标

- 学完本课程后，您将能够:
  - 描述AAA的原理
  - 描述用户认证技术
  - 实现用户认证相关配置

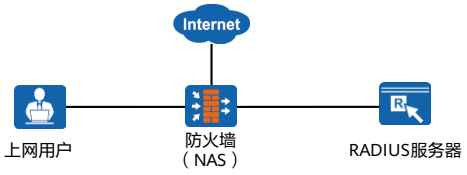
目录

AAA简介

- AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称，是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。
  - 认证：验证用户是否可以获得访问权，确定哪些用户可以访问网络；
  - 授权：授权用户可以使用哪些服务；
  - 计费：记录用户使用网络资源的情况。

AAA常见应用场景

通过RADIUS服务器实现用户上网管理



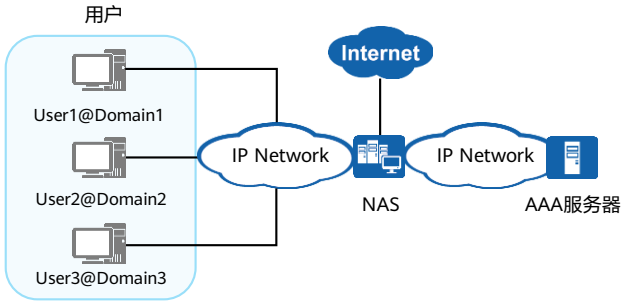
- 通过在NAS上配置AAA方案，实现NAS与RADIUS服务器的对接。
- 用户在客户端上输入用户名和密码后，NAS可以将这些信息发送至RADIUS服务器进行认证。
- 如果认证通过，则授予用户访问Internet的权限。
- 在用户访问过程中，RADIUS服务器还可以记录用户使用网络资源的情况。

通过本地认证实现网络管理员权限控制

- 在防火墙上配置本地AAA方案后，当网络管理员登录防火墙时，防火墙将网络管理员的的用户名密码等信息，与本地配置的用户名信息进行比对认证。
- 认证通过后，防火墙将授予网络管理员一定的管理员权限。

AAA的基本架构

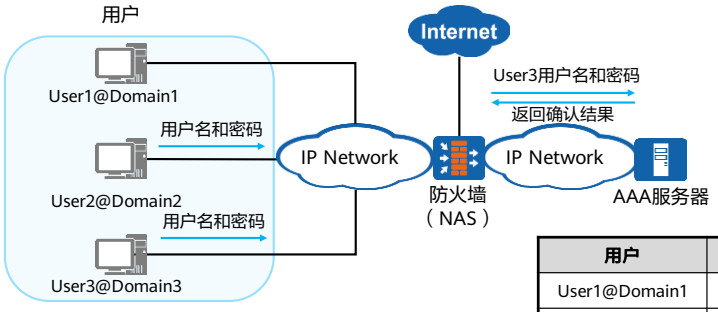
- AAA的基本架构中包括用户、NAS、AAA服务器。
  - NAS负责集中收集和管理用户的访问请求，现网常见的NAS设备有交换机、防火墙等；
  - AAA服务器负责集中管理用户信息。



- NAS基于域来对用户进行管理，每个域都可以配置不同的认证、授权和计费方案，用于对该域下的用户进行认证、授权和计费。
  - 每个用户都属于某一个域。用户属于哪个域是由用户名中的域名分隔符@后的字符串决定。例如，如果用户名是User1@Domain1，则用户属于Domain1域。如果用户名后不带有@，则用户属于系统缺省域；
  - 在NAS上会创建多个域来管理用户，不同的域可以关联不同的AAA方案；当收到用户接入网络的请求时，NAS会根据用户名来判断用户所在的域，根据该域对应的AAA方案对用户进行管控。
- 用户域即用户所在的区域，域名为该区域的名字，一般情况下用户名@域名则表明用户属于这个区域。

认证

- 防火墙支持的认证方式有：不认证，本地认证，远端认证。

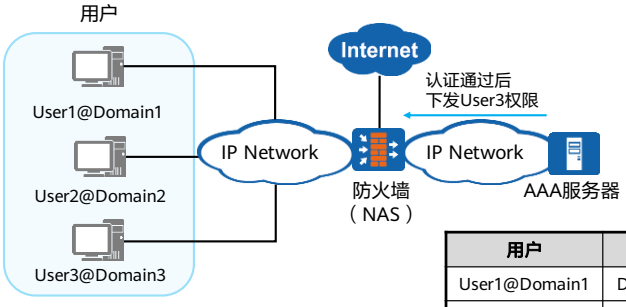


用户	域	认证方式
User1@Domain1	Domain1	不认证
User2@Domain2	Domain2	本地认证
User3@Domain3	Domain3	远端认证

- 防火墙支持的三种认证方式：
  - 不认证：完全信任用户，不对用户身份进行合法性检查。鉴于安全考虑，这种认证方式很少被采用。
  - 本地认证：将本地用户信息（包括用户名、密码和各种属性）配置在NAS上，此时NAS就是AAA Server。本地认证的优点是处理速度快、运营成本低；缺点是存储信息量受设备硬件条件限制。这种认证方式常用于对用户登录设备进行管理，如Telnet，FTP等。
  - 远端认证：将用户信息（包括用户名、密码和各种属性）配置在认证服务器上。支持通过RADIUS协议进行远端认证。NAS作为客户端，与RADIUS服务器服务器进行通信。

授权

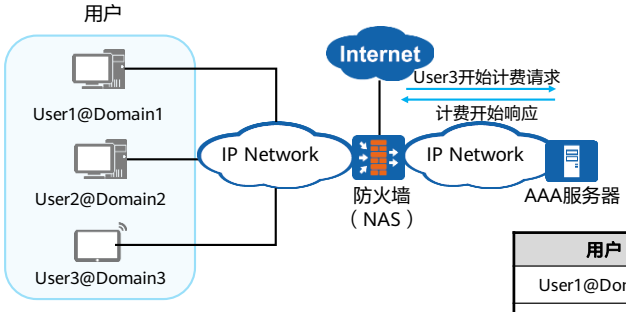
- 授权表示用户可以使用哪些业务，如公共业务以及敏感业务等。
- 防火墙支持的授权方式有：不授权、本地授权、远端授权。授权内容包括：用户组、VLAN、ACL编号等。



用户	域	授权方式	授权内容
User1@Domain1	Domain1	不授权	无
User2@Domain2	Domain2	NAS本地授权	可以访问Internet
User3@Domain3	Domain3	远端授权	由远端服务器授权

计费

- 防火墙支持的AAA计费方式有：不计费，远端计费。
- 计费功能用于监控授权用户的网络行为和网络资源的使用情况。



用户	域	计费方式
User1@Domain1	Domain1	不计费
User2@Domain2	Domain2	不计费
User3@Domain3	Domain3	远端计费

HUAWEI

- 计费主要的含义有三个：
  - 用户用多长时间；
  - 用户花了多少钱；
  - 用户做了哪些操作。

AAA常用技术方案

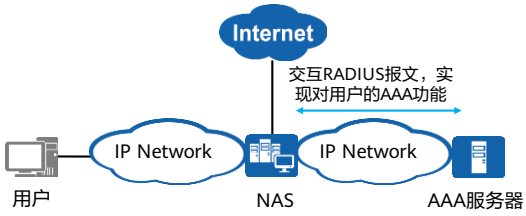
- 目前华为设备支持基于RADIUS、HWTACACS、LDAP或AD来实现AAA，在实际应用中，RADIUS最为常用。

技术方案	交互协议	认证	授权	计费
RADIUS	UDP	✓	✓	✓
HWTACACS	TCP	✓	✓	✓
LDAP	TCP	✓	✓	✗
AD	TCP	✓	✓	✗
本地认证授权	/	✓	✓	✗

- 华为终端访问控制器控制系统协议HWTACACS是在TACACS（RFC 1492）基础上进行了功能增强的安全协议。HWTACACS是一种集中式的、客户端/服务器结构的信息交互协议，使用TCP协议传输，端口号为49。HWTACACS提供的认证、授权和计费服务相互独立，能够在不同的服务器上实现。HWTACACS协议主要用于采用点对点协议PPP（Point-to-Point Protocol）或虚拟私有拨号网络VPDN（Virtual Private Dial-up Network）方式接入Internet的接入用户以及对设备进行操作的管理用户的认证、授权和计费。
- LDAP认证中，LDAP客户端是通过明文方式发送用户的密码到LDAP服务器，存在安全风险。为此，可将Kerberos协议集成到LDAP认证过程中，利用Kerberos协议的对称密钥体制来提高密码传输的安全性，防止在LDAP认证过程中泄露用户的密码，这种集成了Kerberos协议的认证方式称为AD认证。

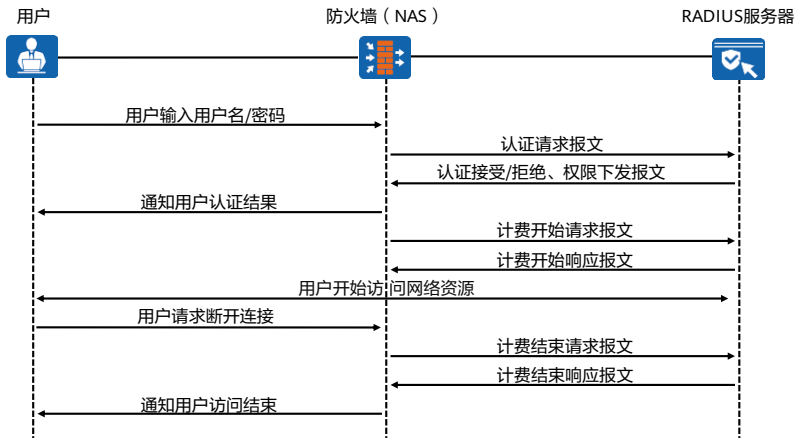
RADIUS协议概述

- AAA可以通过多种协议来实现，在实际应用中，最常使用RADIUS协议。
- RADIUS是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求有较高安全性、又允许远程用户访问的各种网络环境中。
- 该协议定义了基于UDP（User Datagram Protocol）的RADIUS报文格式及其传输机制，并规定UDP端口1812、1813分别作为默认的认证、计费端口。
- RADIUS协议的主要特征如下：
  - 客户端/服务器模式
  - 安全的消息交互机制
  - 良好的扩展性



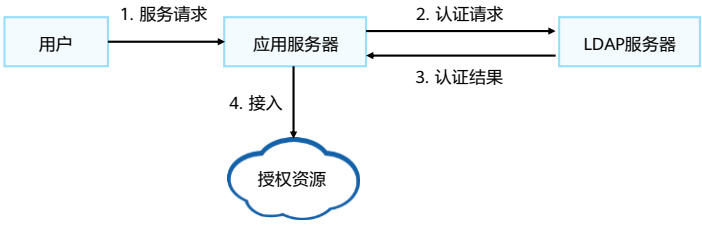
- RADIUS有时也会使用1645、1646分别作为默认的认证、计费端口。

AAA实现协议 - RADIUS认证流程



LDAP简介

- LDAP是轻量级目录访问协议的简称，LDAP基于C/S架构。
- LDAP服务器负责对来自应用服务器的请求进行认证，同时还指定用户访问的资源范围等。
- LDAP定义了多种操作来实现LDAP的各种功能，其中可以利用LDAP的绑定和查询操作来实现用户的认证和授权功能。

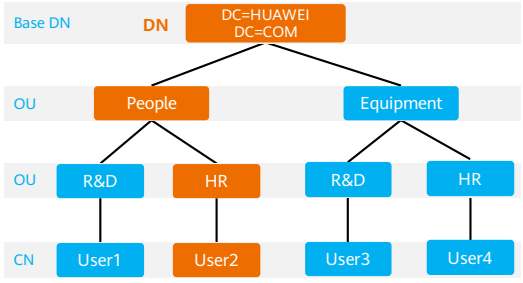


HUAWEI

- 应用场景：网络接入设备和LDAP服务器对接，利用LDAP的绑定和查询操作来实现用户的认证和授权功能。

LDAP目录

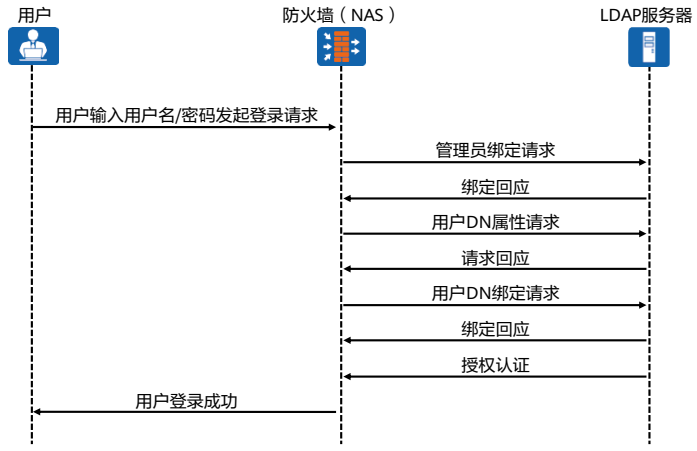
- 目录是一组具有类似属性、以一定逻辑和层次组合的信息。LDAP协议中目录是按照树型结构组织，目录由条目（Entry）组成，条目是具有区别名DN的属性集合。属性由类型和多个值组成。



LDAP目录树

- CN（Common Name，通用名称）：表示对象名称。
- DC（Domain Controller，域控制器）：表示对象所属的区域，一般一台LDAP服务器即为一个域控制器。
- DN（Distinguished Name，区别名）：对象的位置，从对象开始逐层描述到根区别名，例如User1的DN为“CN=User1，OU=HR，OU=People，DC=HUAWEI，DC=COM”。
- Base DN：根区别名。
- OU（Organization Unit，组织单元）：表示对象所属的组织。

LDAP认证流程



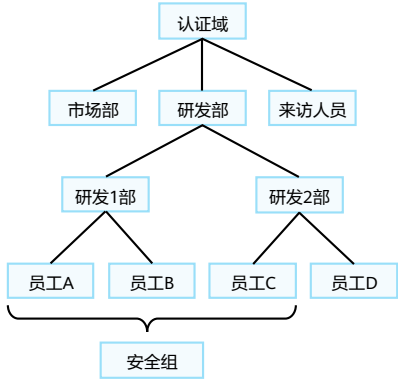
HUAWEI

- 认证流程描述如下：
  - 用户输入用户名/密码发起登录请求，防火墙和LDAP服务器建立TCP连接；
  - 防火墙以管理员DN和密码向LDAP服务器发送绑定请求报文用以获得查询权限；
  - 绑定成功后，LDAP服务器向防火墙发送绑定回应报文；
  - 防火墙使用用户输入的用户名向LDAP服务器发送用户DN查询请求报文；
  - LDAP服务器根据用户DN进行查找，如果查询成功测发送查询回应报文；
  - 防火墙使用查询到的用户DN和用户输入的密码向LDAP服务器发送用户DN绑定请求报文，LDAP服务器查询用户密码是否正确；
  - 绑定成功后，LDAP服务器发送绑定回应报文；
  - 授权成功后，防火墙通知用户登录成功。

目录

用户组织架构及管理

- 用户是网络访问的主体，是防火墙进行网络行为控制和网络权限分配的基本单元。用户组织架构中涉及三个概念：
  - 认证域：用户组织结构的容器，防火墙缺省存在default认证域，用户可以根据需求新建认证域；
  - 用户组/用户：用户按树形结构组织，用户隶属于组（部门）。管理员可以根据企业的组织结构来创建部门和用户；
  - 安全组：横向组织结构的跨部门群组。当需要基于部门以外的维度对用户进行管理可以创建跨部门的安全组。例如企业中跨部门成立的群组。
- 系统默认有一个缺省认证域，每个用户组可以包括多个用户和用户组。每个用户组只能属于一个父用户组，每个用户至少属于一个用户组，也可以属于多个用户组。



HUAWEI

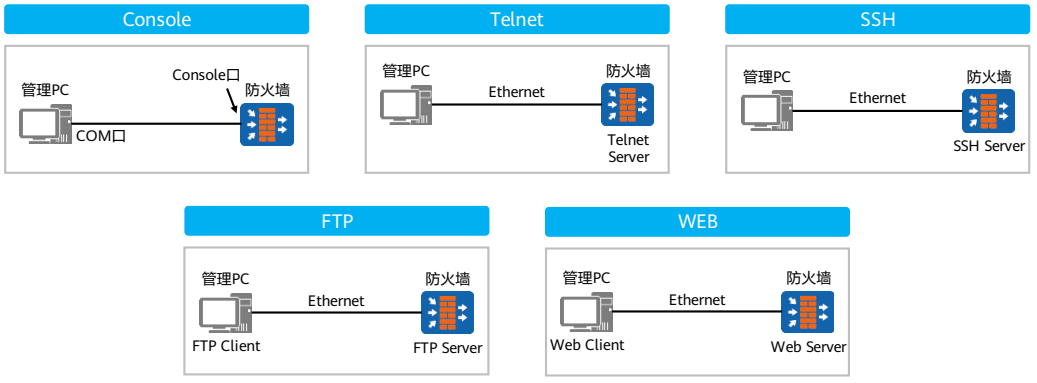
- 认证域：
  - 认证域是认证流程中的重要环节，认证域上的配置决定了对用户的认证方式以及用户的组织结构；
  - 对于不同认证方式的用户，认证域的作用不尽相同。
- 防火墙通过识别用户名中包含的认证域，将所有待认证的用户“分流”到对应的认证域中，根据认证域上的配置来对用户进行认证。
- 为了给不同的用户或部门进行差异化管理，分配不同的权限，需要对组织结构进行规划和管理。防火墙支持创建树型的组织结构，这种结构和通常的行政架构比较类似，非常方便规划和管理。
- 每个用户/用户组可以被安全策略、限流策略、认证策略等引用，从而实现基于用户的权限和带宽资源控制。
- 如果管理员使用缺省的default认证域对用户进行认证，用户登录时只需要输入用户名；如果管理员使用新创建的认证域对用户进行认证，则用户登录时需要输入“用户名@认证域名”。

用户分类

- 管理员
  - 管理员用户指通过Telnet、SSH、Web、FTP等协议或通过Console接口访问设备并对设备进行配置或操作的用户。
- 上网用户
  - 上网用户是网络访问的标识主体，是设备进行网络权限管理的基本单元；
  - 设备通过对访问网络的用户进行身份认证，从而获取用户身份，并针对用户的身份进行相应的策略控制。
- 接入用户
  - 外部网络中访问网络资源的主体，如企业的分支机构员工和出差员工；
  - 接入用户需要先通过SSL VPN、L2TP VPN、IPSec VPN或PPPoE方式接入到防火墙，然后才能访问企业总部的网络资源。

目录

管理员认证登录方式

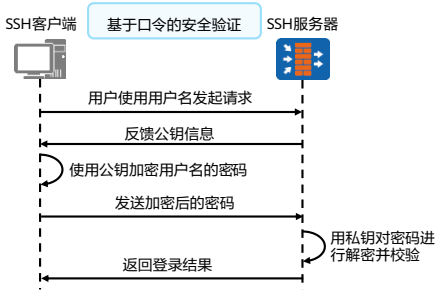


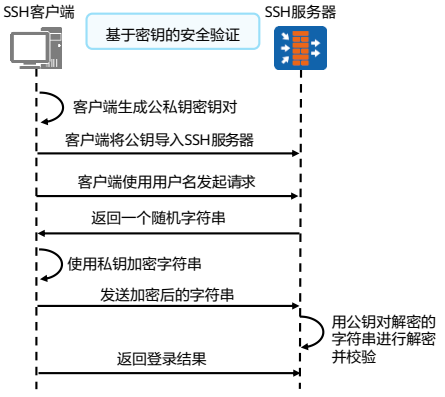
HUAWEI

- 管理员主要为了实现对设备的管理、配置和维护，登录方式可以分为：
  - Console：Console接口提供命令行方式对设备进行管理，通常用于设备的第一次配置，或者设备配置文件丢失，没有任何配置。当设备系统无法启动时，可通过Console口进行诊断或进入BootRom进行升级；
  - Web：终端通过HTTP/HTTPS方式登录到设备进行远程配置和管理；
  - Telnet：Telnet是一种传统的登录方式，通常用于通过命令行方式对设备进行配置和管理；
  - FTP：FTP管理员主要对设备存储空间里的文件进行上传和下载；
  - SSH：SSH提供安全的信息保障和强大的认证功能，在不安全的网络上提供一个安全的“通道”，此时，设备作为SSH服务器。

管理员认证方式 - SSH

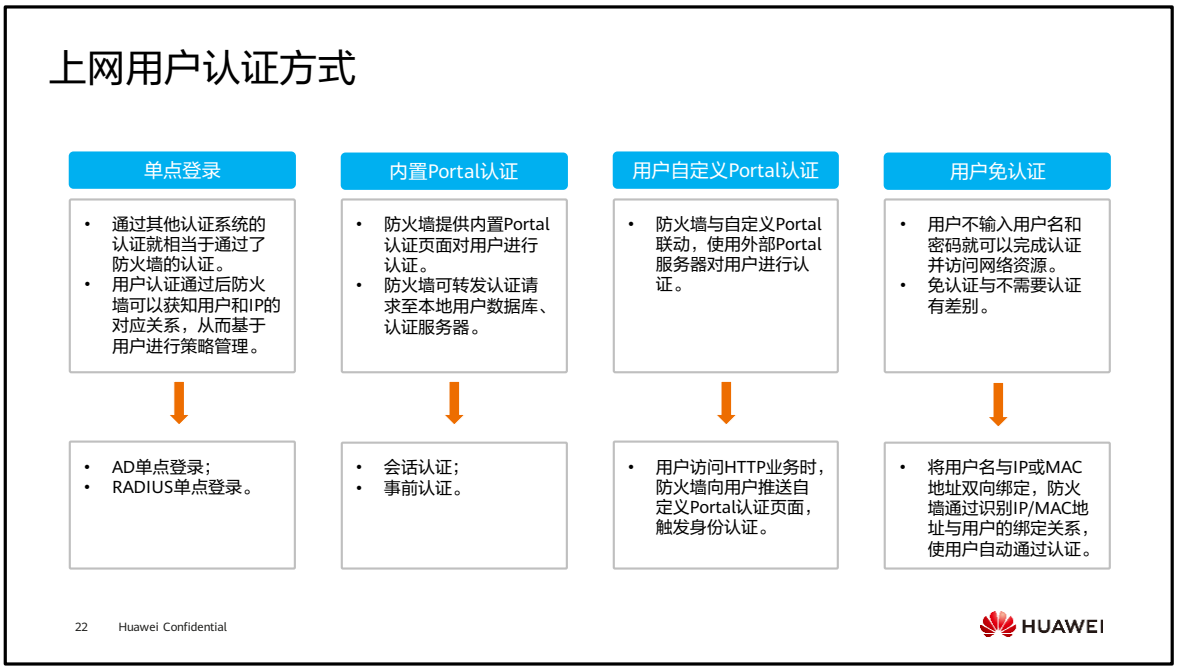
- SSH（Secure Shell）安全外壳协议是建立在应用层基础上的安全协议，避免数据的明文传输。SSH可靠性高，是专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。
- SSH安全验证方式：
  - 基于口令的安全验证
  - 基于密钥的安全验证





HUAWEI

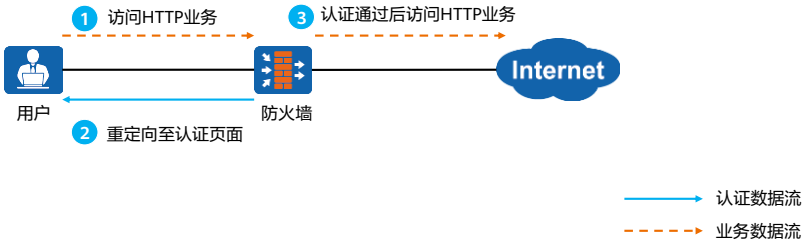
- 简单说，SSH是一种网络协议，用于计算机之间的加密登录。如果一个用户从本地计算机，使用SSH协议登录另一台远程计算机，我们就可以认为，这种登录是安全的，即使被中途截获，密码也不会泄露。
- SSH基于口令的安全验证登录步骤：
  - 用户发起登陆请求；
  - 远程主机将自己的公钥返回给请求主机；
  - 请求主机使用公钥对用户输入的密码进行加密；
  - 请求主机将加密后的密码发送给远程主机；
  - 远程主机使用私钥对密码进行解密；
  - 最后，远程主机判断解密后的密码是否与用户密码一致，一致则登录成功。
- SSH基于密钥的安全验证登录步骤：
  - 用户主机生成密钥对，并将公钥导入远程主机；
  - 用户发起登陆请求；
  - 远程主机向用户返回一个随机串；
  - 用户所在主机使用私钥对这个随机串进行加密，并将加密的随机串返回至远程主机；
  - 远程主机使用导入进来的公钥对加密随机串进行解密；如果解密成功，就证明用户的登陆信息是正确的，则允许登陆。



- 单点登录：此种方式适用于部署防火墙用户认证功能之前已经部署认证系统的场景。
- 内置Portal认证：此种方式适用于通过防火墙对用户进行认证的场景。
- 用户自定义Portal认证：目前存在两种类型的自定义Portal认证，具体请参见自定义Portal认证。
- 用户免认证：免认证是指用户无需输入用户名、密码，但是防火墙可以获取用户和IP的对应关系，从而实现用户管理。
- 下文针对内置Portal认证详细讲解上网用户认证流程。

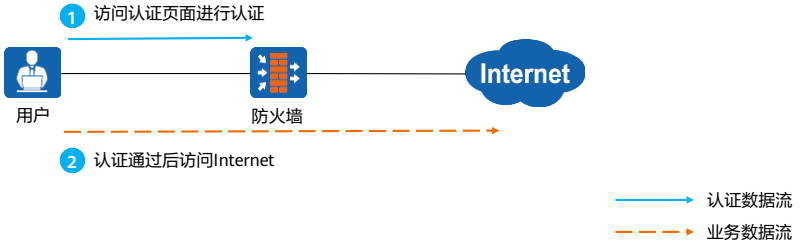
内置Portal认证 - 会话认证

- 会话认证是用户不主动进行身份认证，先进行HTTP业务访问，在访问过程中进行认证。认证通过后，再进行业务访问。
- 当防火墙收到用户的第一条HTTP业务访问数据流时，将HTTP请求重定向到认证页面，触发访问者身份认证。认证通过后，就可以访问HTTP业务以及其他业务。



内置Portal认证 - 事前认证

- 事前认证是指访问者在访问网络资源之前，先主动进行身份认证，认证通过后，再访问网络资源。
- 用户主动向防火墙提供的认证页面发起认证请求。防火墙收到认证请求后，对其进行身份认证。认证通过后，就可以访问Internet。



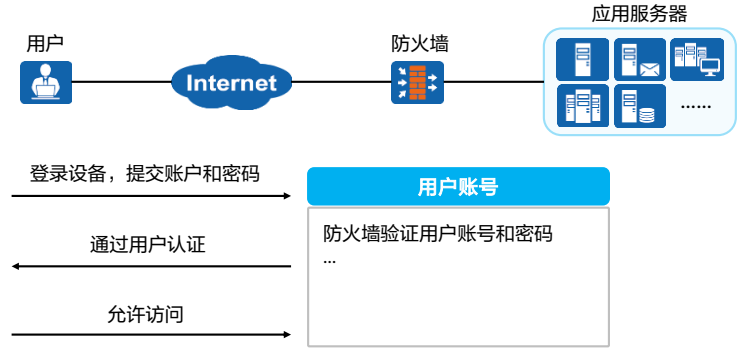
接入用户认证方式

- 接入用户认证指的是对各类VPN接入用户进行认证。

SSL VPN	L2TP VPN	IPSec VPN	PPPoE
• 访问者登录SSL VPN模块提供的认证页面来触发认证过程，认证完成后，SSL VPN接入用户可以访问总部的网络资源。 • SSL VPN作为新型的轻量级远程接入方案，移动的办公用户可以不安装客户端。	• L2TP（Layer 2 Tunneling Protocol）VPN是一种隧道技术，该技术主要应用在远程办公场景中，为出差员工提供企业内网资源接入服务。 • 无论出差员工是通过传统的的拨号方式接入Internet，还是通过以太网方式接入Internet，L2TP VPN都可以向其提供远程接入服务。	• IPSec是一组开放的网络安全协议。是一系列为IP网络提供安全性协议和服务的集合，包括AH和ESP两个安全协议，以及密钥交换和用于验证及加密的一些算法等。 • 通过这些协议，在两个设备之间建立一条IPSec隧道。数据通过IPSec隧道进行转发，实现数据安全传输。	• PPPoE（PPP over Ethernet）协议是一种把PPP帧封装到以太网帧中的链路层协议。PPPoE可以使以太网网络中的多台主机连接到远端的宽带接入服务器。

SSL VPN

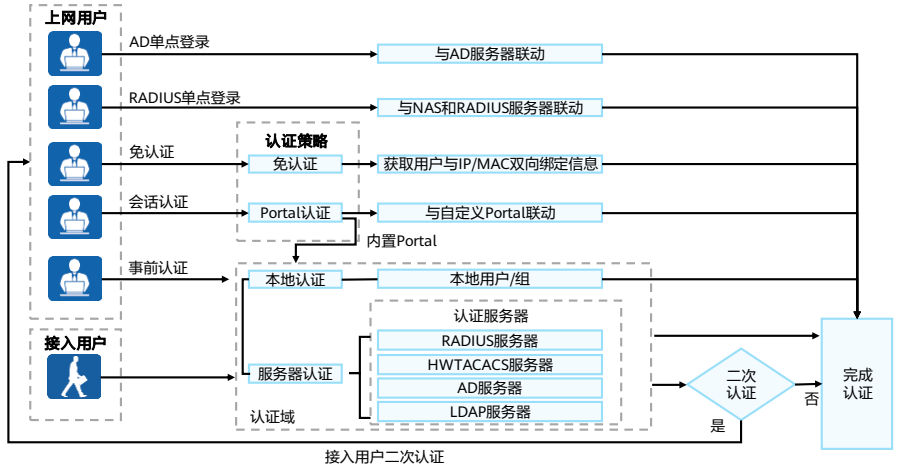
- 用户在外网通过SSL VPN拨入防火墙，实现访问内网资源的需求。



HUAWEI

- SSL VPN是以HTTPS为基础的VPN技术，工作在传输层和应用层之间，在Internet基础上提供机密性的安全协议。主要提供业务有Web代理、网络扩展、文件共享和端口转发。
- SSL协议通信的握手步骤如下：
  - SSL客户端向SSL服务器发起连接，并要求服务器验证自身的身份；
  - 服务器通过发送自身的数字证书证明身份；
  - 服务器发出一个请求，对客户端的证书进行验证；
  - 验证通过后，协商用于加密的消息加密算法和用于完整性检查的哈希函数。通常由客户端提供它支持的所有算法列表，然后由服务器选择最强大的加密算法；
  - 客户端和服务器通过以下步骤生成会话密钥：
    - 客户端生成一个随机数，并使用服务器的公钥（从服务器证书中获取）对它加密，以送到服务器上；
    - 服务器用随机数据（客户端的密钥可用时则使用客户端密钥，否则以明文方式发送数据）响应；
    - 使用哈希函数从随机数据中生成密钥。
- 如上图所示，某企业在网络边界处部署了防火墙作为VPN接入网关，连接内部网络与Internet。出差员工通过SSL VPN接入到防火墙后，使用网络扩展业务访问网络资源。

认证流程总结



HUAWEI

目录

认证策略

- 认证策略用于决定防火墙需要对哪些数据流进行认证，匹配认证策略的数据流必须经过防火墙的身份认证才能通过。缺省情况下，防火墙不对经过自身的数据流进行认证，仅认证匹配认证策略的数据流。如果经过防火墙的流量匹配了认证策略将触发如下动作：
  - 会话认证：用户访问HTTP业务时，如果数据流匹配了认证策略，防火墙会推送认证页面要求访问者进行认证；
  - 事前认证：用户访问非HTTP业务时必须主动访问认证页面进行认证，否则匹配认证策略的业务数据流将被防火墙禁止；
  - 免认证：用户访问业务时，如果匹配了免认证的认证策略，则无需输入用户名、密码直接访问网络资源。防火墙根据用户与IP/MAC的绑定关系来识别用户；
  - 单点登录：单点登录用户上线不受认证策略控制，只有当用户业务流量匹配认证策略才进行策略管控。

- 以下流量即使匹配了认证策略也不会触发认证：
  - 访问设备或设备发起的流量；
  - DHCP、BGP、OSPF、LDP报文；
  - 触发认证的第一条HTTP业务数据流对应的DNS报文不受认证策略控制，用户认证通过上线后的DNS报文受认证策略控制。

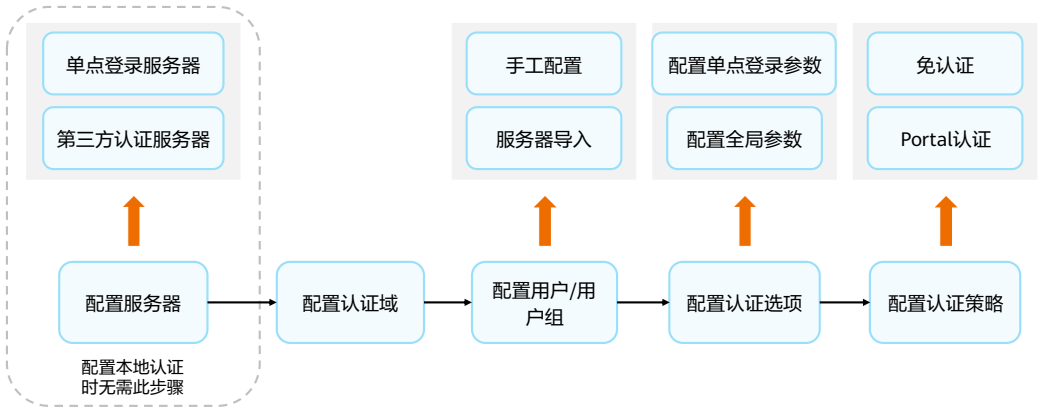
认证策略组成信息

- 认证策略是多个规则的集合。认证策略规则由条件和动作组成，条件指的是防火墙匹配报文的依据，包括：
  - 源/目的安全区域
  - 源地址/地区
  - 目的地址/地区
- 动作指的是防火墙对匹配到的数据流采取的处理方式，包括：
  - Portal认证
  - 短信认证
  - 免认证
  - 不认证

- Portal认证：对符合条件的数据流进行Portal认证。
- 短信认证：对符合条件的数据流进行短信认证，要求用户输入短信验证码。
- 免认证：对符合条件的数据流进行免认证，防火墙通过其他手段识别用户身份。主要应用于以下情况：
  - 对于企业的高级管理者来说，一方面他们希望省略认证过程；另一方面，他们可以访问机密数据，对安全要求又更加严格。为此，管理员可将这类用户与IP/MAC地址双向绑定，对这类数据流进行免认证，但是要求其只能使用指定的IP或者MAC地址访问网络资源。防火墙通过用户与IP/MAC地址的绑定关系来识别该数据流所属的用户；
  - 在AD/RADIUS单点登录的场景中，防火墙已经从其他认证系统中获取到用户信息，对单点登录用户的业务流量进行免认证。
- 不认证：对符合条件的数据流不进行认证，主要应用于以下情况：
  - 不需要经过防火墙认证的数据流，例如内网之间互访的数据流；
  - 在AD/RADIUS单点登录的场景中，如果待认证的访问者与认证服务器之间交互的数据流经过防火墙，则要求不对这类数据流进行认证。
- 防火墙上存在一条缺省的认证策略，所有匹配条件均为任意（any），动作为不认证。

目录

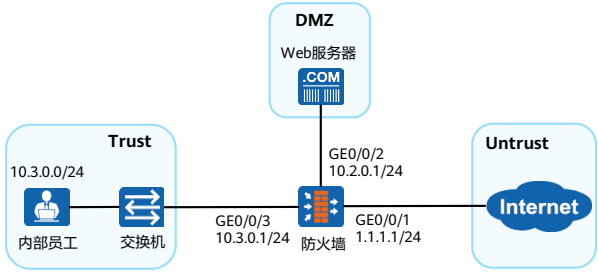
上网用户认证 - 配置流程



- 配置用户/用户组：设备实施基于用户/用户组的管理之前，必须先创建用户/用户组。设备支持管理员手动配置、本地导入和服务器导入多种创建方式。
- 手动配置组/用户：
  - 防火墙上默认存在default认证域，可以在其下级创建用户/组，如果需要规划其他认证域的组织结构请先配置认证域；
  - 当需要根据企业组织结构创建用户组时，并基于用户组进行网络权限分配等管理时，该步骤必选；
  - 当对用户进行本地密码认证时，必须要在本地创建用户，并配置本地密码信息。
- 本地导入：
  - 支持将CSV格式的文件导入设备。
- 服务器导入：
  - 网络中，使用第三方认证服务器的情况非常多，很多公司的网络都存在认证服务器，认证服务器上存放着所有用户和用户组信息。从认证服务器上批量导入用户是指通过服务器导入策略，将认证服务器上用户信息导入到设备上。
- 配置认证选项包含全局参数、单点登录及定制认证页面三部分内容的配置。

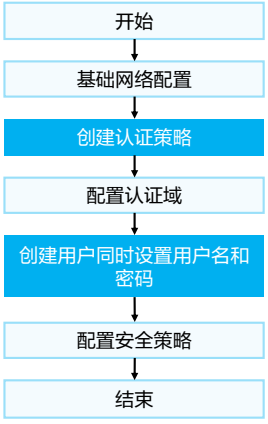
上网用户认证配置举例（1）

- 需求描述：
  - 某企业在网络边界处部署了防火墙作为出口网关，连接内部网络与Internet。企业内部网络中的员工均动态获取IP地址。内部员工访问网络资源之前必须通过防火墙的认证；
  - 内部员工使用浏览器访问某个Web页面，防火墙会将浏览器重定向到认证页面。认证通过后，浏览器的界面会自动跳转到先前访问的Web页面。



上网用户认证配置举例（2）

- 配置思路：
  - 完成基本网络配置：包括配置防火墙各接口的IP地址，将防火墙各接口加入相应的安全区域及缺省路由配置；
  - 创建认证策略：设置匹配条件以及认证动作；
  - 配置认证域：场景选择“上网行为管理”，用户所在位置选择“本地”；
  - 在本地域中新建用户组及用户名密码，提供给内部员工认证时使用；
  - 配置安全策略：让内部员工认证时可以访问认证页面，完成认证并上网。



- 此处配置流程中的安全策略作用是允许访问者访问认证页面，其他业务相关安全策略请根据实际情况设置。

上网用户认证配置举例（3）

- 创建认证策略，选择“对象 > 用户 > 认证策略 > 新建”。

上网用户认证配置举例（4）

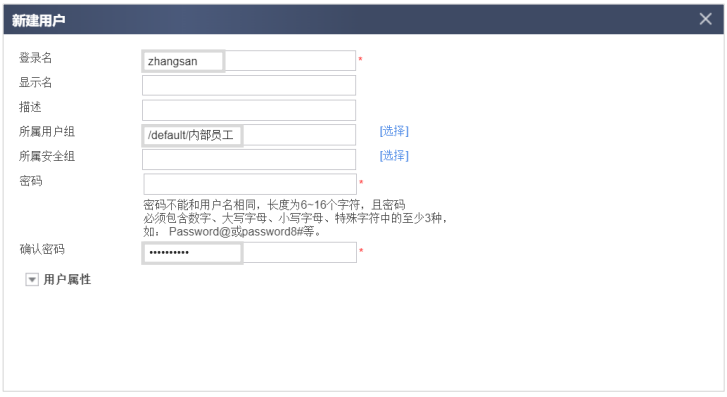
- 配置本地认证，选择“对象 > 用户 > default”。

上网用户认证配置举例（5）

- 创建用户组，选择“对象> 用户 > default > 新建”。

上网用户认证配置举例（6）

- 创建用户，选择“对象 > 用户 > default > 新建”。



本章总结

- 本课程简要介绍了用户管理的架构、用户认证的具体方案和认证流程，阐述了用户的具体类型和对应用户认证的配置方式。
- 通过本课程的学习，您能够对用户分类、用户认证协议有一定的了解，学员将能独立完成华为防火墙用户管理的配置，并掌握防火墙在认证场景中的部署方法。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

加解密技术原理

HUAWEI

前言

- 互联网把全世界连接在一起，走向互联网就意味着走向了世界，这对无数企业而言无疑是梦寐以求的好事。但TCP/IP协议簇设计之初没有重点关注安全问题，这使得在互联网上进行文件传输、电子邮件等数据传递时，存在许多不安全因素。使用加密算法对数据加密是提升数据通信安全性的常用手段。
- 本课程主要介绍了加解密的发展历程，对称加密算法、非对称加解算法、散列算法等常见算法的工作原理及过程。

目标

- 学完本课程后，您将能够：
  - 描述加解密的发展历程
  - 描述不同加解密的过程
  - 描述加解密算法的原理

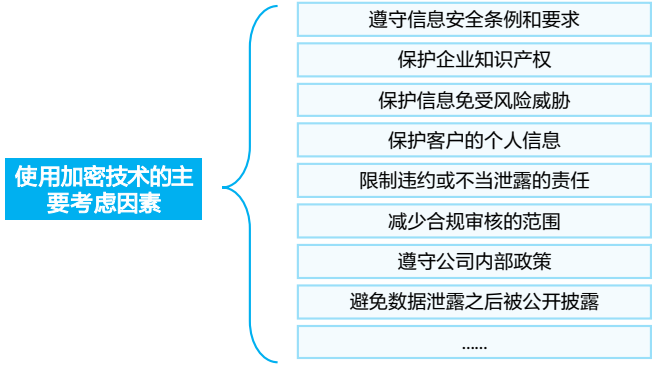
目录

加解密定义

- 数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，通过这样的途径来达到保护数据不被非法人员窃取、阅读的目的。
- 数据解密的过程就是对密文使用相应的算法和密钥进行解密处理，将密文解密成明文的过程。

- 加密的安全性取决于：
  - 密钥的生成，管理，存储；
  - 加密算法的安全性；
  - 加解密的环境。

加密产生背景



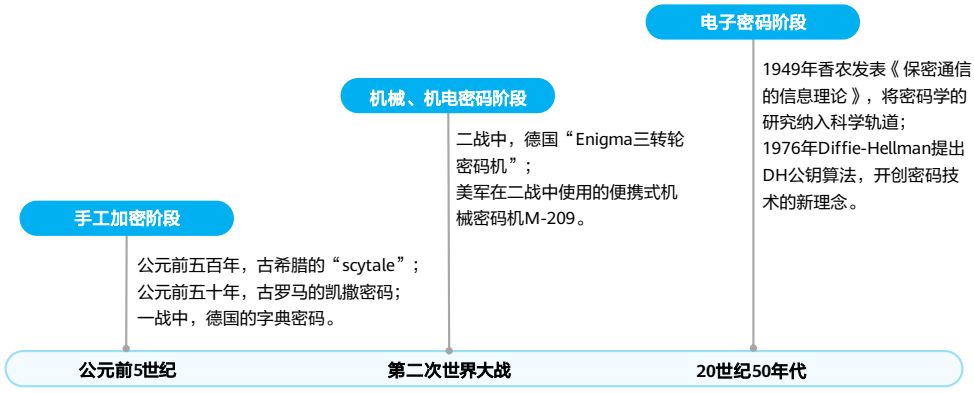
加密的目的

- 通过加密可保证信息的机密性、完整性、鉴别性和不可否认性。

机密性	完整性	鉴别性	不可否认性
• 通过数据加密实现； • 提供只允许特定用户访问和阅读信息，任何非授权用户对信息都不可理解的服务。	• 通过数据加密、散列或数字签名来实现； • 提供确保数据在存储和传输过程中不被未授权修改的服务。	• 通过数据加密、数据散列或数字签名来实现； • 提供与数据和身份识别有关的服务，即认证数据发送和接收者的身份。	• 通过对称加密或非对称加密，以及数字签名等，并借助可信的注册机构或证书机构的辅助来实现； • 提供阻止用户否认先前的言论或行为的抗抵赖服务。

- 加密是一个过程，它使信息只对正确的接收者可读，其他用户看到的是杂乱无序的信息，使其只能在使用相应的密钥解密之后才能显示出本来内容。
- 加密在网络上的作用就是防止私有化信息在网络上被拦截和窃取。通过加密可保证信息的机密性、完整性、鉴别性和不可否认性。

加密技术的发展史

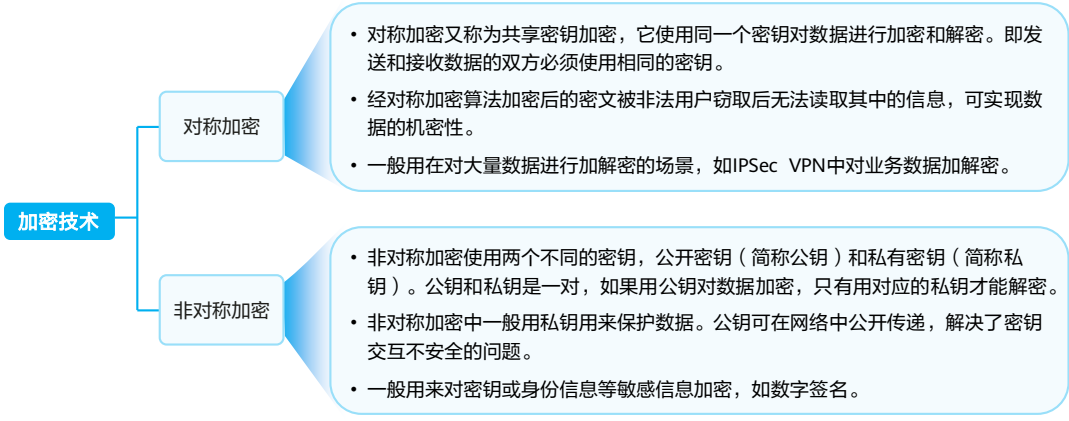


HUAWEI

- 加密作为保障信息安全的一种方式，它不是现代才有的，它产生的历史相当久远，可以追溯到人类刚刚出现，并且尝试去学习如何通信的时候。他们不得不去寻找方法确保他们的通信的机密。
- 但是最先有意识地使用一些技术方法来加密信息的可能是公元前五百年的古希腊人。他们使用的是一根叫scytale的棍子，送信人先绕棍子卷一张纸条，然后把要加密的信息写在上面，接着打开纸送给收信人。如果不知道棍子的宽度（这里作为密钥）是不可能解密信里面内容的。
- 大约在公元前5世纪，古罗马的统治者凯撒发明了一种战争时用于传递加密信息的方法，后来称之为“凯撒密码”。它的原理就是：将26个字母按自然顺序排列，并且首尾相连，明文中的每个字母都用其后的第三个字母代替，例如HuaweiSymantec通过加密之后就变成KxdzhlvBPdqwhf。
- 在第一次世界大战中，德国人曾依靠字典编写密码，比如：10-4-2，就是某字典第10页，第4段的第2个单词。
- 在二次世界大战中，最广为人知的编码机器是德国人的Enigma三转轮密码机，在二次世界大战中德国人利用它加密信息。
- 电子密码阶段有两个里程碑：
  - 1949年香农发表《保密通信的信息理论》，将密码学的研究纳入科学轨道；
  - 1976年Diffie-Hellman提出DH公钥算法，开创密码技术的新理念。

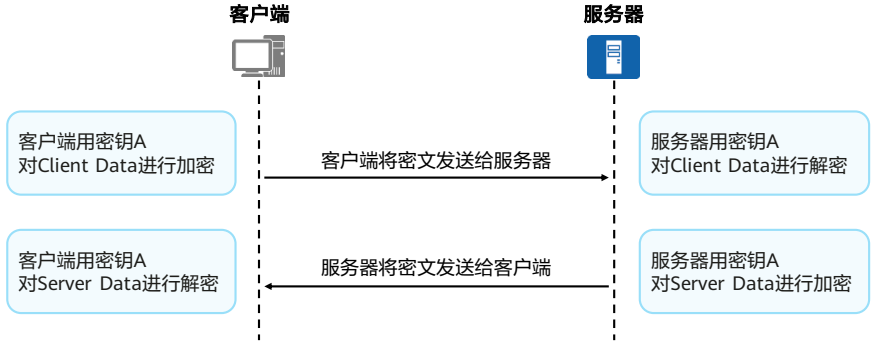
目录

加密技术分类



对称加密算法

- 对称加密算法的加密和解密都是用**同一个密钥**。
- 如图所示，客户端与服务器进行数据交互，采用对称加密算法。客户端与服务器事先协商好对称密钥A，具体加解密过程如下：

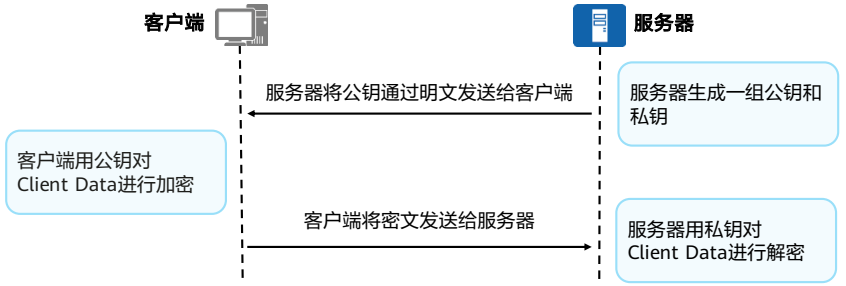


HUAWEI

- 如果通信双方都各自持有同一个密钥，且没有别人知道，则两方的通信安全是可以被保证的（除非密钥被破解）。然而，最大的问题就是这个密钥怎么让传输的双方知晓，同时不被别人知道。如果由服务器生成一个密钥并传输给浏览器，这个传输过程中密钥被别人劫持，之后他就能用密钥解开双方传输的任何内容。如果浏览器内部预存了网站A的密钥，且可以确保除了浏览器和网站A，不会有任何外人知道该密钥，那理论上用对称加密是可以的。这样，浏览器只要预存好世界上所有HTTPS网站的密钥就可以了。显然，这样做是不现实的。为了解决这个问题，我们就需要非对称加密。

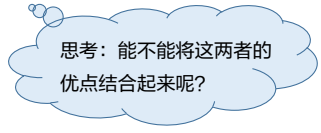
非对称加密算法

- 非对称加密算法需要**一组密钥对**，分别是**公钥**和**私钥**，这两个密钥是成对出现的。
- 非对称加密解决了对称密钥的发布和管理问题，一个用于加密信息，另一个则用于解密信息，通信双方无需事先交换密钥就可进行保密通信。通常以公钥作为加密密钥，以私钥作为解密密钥。
- 如图所示，客户端与服务器进行数据交互，采用非对称加密算法，具体加解密过程如下：



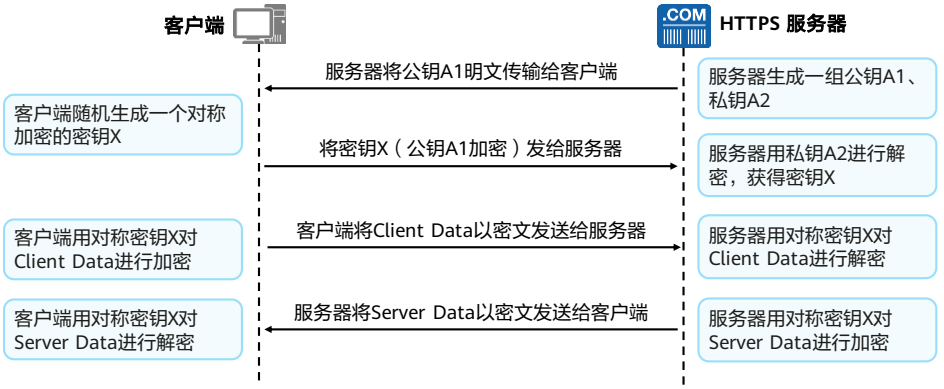
对称和非对称加密比较

加密算法	优点	缺点	使用场景
对称加密	效率高，算法简单，系统开销小，适合加密大量数据。	实现困难，扩展性差。	对大量数据进行加解密。
非对称加密	无法从一个密钥推导出另一个密钥；公钥加密的信息只能用私钥进行解密。	算法非常复杂，导致加密大量数据所用的时间较长，而且加密后的报文较长，不利于网络传输。	对密钥或身份信息等敏感信息加密。



非对称加密与对称加密结合

- 采用非对称加密与对称加密结合的方式，可以减少非对称加密的次数，HTTPS就是采用了这种方案。首先通过非对称加密交换对称加密密钥，然后使用对称加密算法加密业务数据，具体交互流程如下：



目录

常见的对称加解密算法

算法	描述
DES	Data Encryption Standard，即数据加密标准。DES算法是以64位为块，在加密端把数据分成多块，对每块数据进行加密，生成密文；在解密端则把64位密文转换为64位明文。各个块之间建立一定的联系，DES使用16个迭代块来完成迭代。其中，加密和解密使用56位密钥。
3DES	Triple DES，即三重数据加密标准。
AES	Advanced Encryption Standard，即高级加密标准。AES支持多种变长密钥，如128位、192位、256位以及384位等。
SM1	SM1加密强度与AES相当。该算法不公开，调用该算法时，需要通过加密芯片的接口进行调用。
SM4	SM4 无线局域网标准的分组数据算法。对称加密，密钥长度和分组长度均为128位。
其他	IDEA等。

- DES是由美国国家标准与技术研究院开发的。DES算法是第一个得到广泛应用的密码算法，使用相同的密钥来加密和解密。DES是一种分组加密算法，输入的明文为64位，密钥为56位，生成的密文为64位（把数据加密成64位的block）。因密码容量只有56位，因此针对其不具备足够安全性的弱点，后来又提出了3DES。
- 3DES使用了128位密钥。信息首先使用56位的密钥加密，然后用另一个56位的密钥译码，最后再用原始的56位密钥加密，这样3DES使用了有效的128位长度的密钥。3DES最大的优点就是可以使用已存在的软件和硬件，并且在DES加密算法上的技术可以轻松地实施3DES。
- AES采用128位的分组长度，支持长度为128位、192位、256位和384位的密钥长度，并可支持不同的平台。128位的密钥长度能够提供足够的安全性，且相比更长的密钥需要较少的处理时间。到目前为止，AES还没有出现任何致命缺陷。但由于快速DES芯片的大量生产，使得DES仍能继续使用。但AES取代DES和3DES以增强安全性和效率已是大势所趋。
- 国密算法是由国家密码管理局编制的一种商用密码分组标准对称算法，国密算法的分组长度和密钥长度都为128位。在安全级别要求较高的情况下，使用SM1或SM4国密算法可以充分满足加密需求。
- IDEA（International Data Encryption Algorithm）是对称分组密码算法，输入明文为64位，密钥为128位，生成的密文为64位。应用方面有很多，其中SSL就将IDEA包含在其加密算法库中。

常见的非对称加解密算法

算法	描述
DH	DH（Diffie-Hellman）算法在IPSec中尤其重要，用于解决秘钥交换问题。因为不可能长期使用同一个秘钥，为了保证足够的安全，所以需要动态的在两端获得秘钥。
RSA	名称由RSA三个提出者（Ron Rivest、Adi Shamir和Leonard Adleman）的姓氏首字母组合而成，这种算法的可靠性由对极大整数做因数分解的难度决定。RSA既能实现数字签名，又能实现加解密。
DSA	DSA（Digital Signature Algorithm）即数字签名算法，又称DSS（Digital Signature Standard，数字签名标准）。DSA仅能实现数字签名，不能用于加解密。

- 非对称加密算法此处有两个作用：
  - 根据算法自动生成一对公私钥；
  - 按照非对称加密算法的交互数据。
- 目前比较常用的非对称加密算法，主要包含DH、RSA和DSA算法。
  - DH算法一般用于双方协商出一个对称加密的密钥，即加密解密都是同一个密钥。实质是双方共享一些参数，然后各自生成密钥，然后根据数学原理，各自生成的密钥是相同的，这个密钥不会涉及到在链路中传播，但是之前的参数的交互会涉及链路传输；
  - RSA公钥加密算法是1977年由Ron Rivest、Adi Shamir和LenAdleman在（美国麻省理工学院）开发的。RSA取名来自开发他们三者的名字。RSA是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的所有密码攻击，已被ISO推荐为公钥数据加密标准。是第一个能同时用于加密和数字签名的算法；
  - DSA在保证数据的完整性、不可抵赖性等方面起着非常重要的作用。DSA是基于整数有限域离散对数难题的，其安全性与RSA相比差不多。在DSA数字签名和认证中，发送者使用自己的私钥对文件或消息进行签名，接受者收到消息后使用发送者的公钥来验证签名的真实性。DSA只是一种算法，和RSA不同之处在于它不能用作加密和解密，也不能进行密钥交换，只用于签名，它比RSA要快很多。

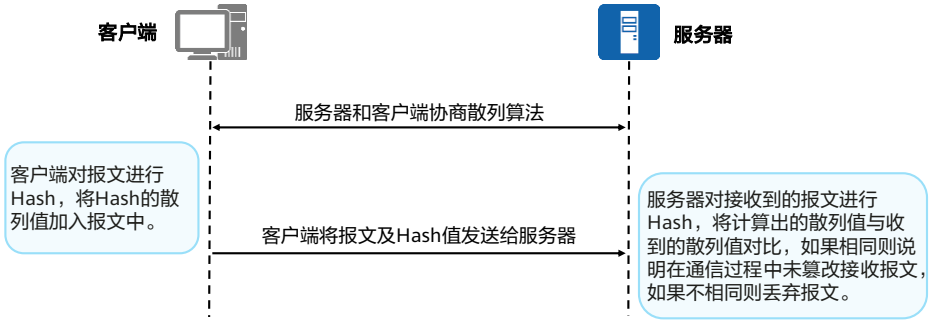
目录

散列算法简介

- 在通信过程中，使用加密技术实现了数据的机密性，但对安全级别需求较高的用户来说，仅对数据加密是不够的，数据仍能够被非法破解并修改。使用散列算法可检查出数据在通信过程中是否被篡改，从而实现数据完整性校验。
- 散列算法就是把任意长度的数据作为输入，然后通过Hash得到一个固定长度的输出值，该输出值就是散列值，它是一种数据压缩映射关系。简单来说就是将任意长度的消息转换到某一固定长度的消息摘要的函数。散列算法具有正向快速、不可逆、输入敏感、抗碰撞的特点。
  - 正向快速：给定明文和Hash算法，在有限时间和有限资源内计算Hash值；
  - 不可逆性：给定任意的Hash值，在有限时间内很难逆推出明文；
  - 输入敏感：如果输入的数据信息被轻微修改，输出的Hash值也会有很明显的变化；
  - 抗碰撞性：任意输入不同的数据，其输出的Hash值不可能相同。对于一个给定的数据块，找到和它hash值相同的数据块极为困难。

散列算法应用

- 在数据通信过程中发送方对报文进行Hash，并将报文和Hash值发送给接收方。接收方采用相同的算法对报文进行Hash，然后通过对比两个Hash值，来判断通信过程中报文是否受到篡改，从而实现完整性校验。
- 如图所示，客户端与服务器进行数据交互，采用散列算法，具体交互流程如下：



常见散列算法

算法	描述
MD5	MD5（Message Digest Algorithm 5）是RSA数据安全公司提出的一种单向散列算法，具有稳定且运算速度快、输出长度固定、运算不可逆以及高度离散等特点。
SHA	SHA（Secure Hash Algorithm）可以对任意长度的数据运算生成一个160位的字符串。
SM3	SM3是国家密码管理局编制的商用算法，用于密码应用中的数字签名和验证、消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。
其他	HMAC等。

- MD5（消息摘要算法第五版）是计算机安全领域广泛使用的一种散列函数，用以提供消息的完整性保护。将数据（如汉字）运算为另一固定长度值。
- SHA（安全散列算法）是由NIST开发的散列算法，和MD5一样，都可以作为数字签名标准（DSS）里面定义的数字签名算法（DSA）来使用。
  - SHA-0：NIST最早载明的算法，在发布后很快被撤回，取而代之的是SHA-1；
  - SHA-1：数据块通过SHA-1算法能够产生160位的消息摘要。SHA-1比MD5要慢，但是更安全。因为它的签名比较长，具有更强大的抗碰撞能力，并可以更有效地发现共享的密钥；
  - SHA-2：SHA-2是SHA-1的加强版本，SHA-2算法相对于SHA-1加密数据长度有所上升，安全性能要远远高于SHA-1。SHA-2算法包括SHA2-256、SHA2-384和SHA2-512，密钥长度分别为256位、384位和512位。
- SM3属于国密即国家密码局认定的国产密码算法。
- HMAC：密钥相关的哈希运算消息认证码，在IPSec、SSL中广泛应用。
- 以上几种算法各有特点，MD5算法的计算速度比SHA-1算法快，而SHA-1算法的安全强度比MD5算法高，SHA-2、SM3算法相对于SHA-1来说，加密数据位数的上升增加了破解的难度，使得安全性能要远远高于SHA-1。

思考题

1. （多选题）以下哪些算法属于对称加密算法？（　　）
   A. MD5
   B. RSA
   C. DES
   D. AES

1. CD

本章总结

- 本课程简要介绍了不同加密技术的应用场景，系统介绍了数据加解密的概念、加密技术的发展历程以及对称加密技术和非对称加密技术的原理和区别，同时介绍了常见的加解密算法和散列算法。
- 通过本课程的学习，您能够对加密技术的知识有一定的了解。

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

缩略语表

缩略语	英文全称	解释
AES	Advanced Encryption Standard	高级加密标准
DES	Data Encryption Standard	数据加密标准
DH	Diffie-Hellman	密钥交换算法
DSA	Digital Signature Algorithm	数字签名算法
DSS	Digital Signature Standard	数字签名标准
3DES	Triple Data Encryption Standard	三重数据加密标准
HMAC	Hash-based Message Authentication Code	散列信息认证码
IDEA	International Data Encryption Algorithm	国际数据加密算法
MD5	Message Digest Algorithm 5	消息摘要算法第五版
RSA	Ron Rivest, Adi Shamir, Leonard Adleman	RSA算法
SHA	Secure Hash Algorithm	安全哈希算法
SM	Shang Mi	国密

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

PKI证书体系

HUAWEI

前言

- 随着网络技术和信息技术的发展，电子商务已逐步被人们所接受，并得到不断普及。但通过网络进行电子商务交易时，存在如下问题：交易双方并不现场交易，无法确认双方的合法身份；通过网络传输时信息易被窃取和篡改，无法保证信息的安全性；交易双方发生纠纷时没有凭证可依，无法提供仲裁。
- 为了解决上述问题，PKI技术应运而生，其利用公钥技术保证在交易过程中能够实现身份认证、保密、数据完整性和不可否认性。因而在网络通信和网络交易中，特别是电子政务和电子商务业务，PKI技术得到了广泛的应用。
- 本课程主要介绍了数据安全通信过程，PKI证书体系架构及PKI工作机制。

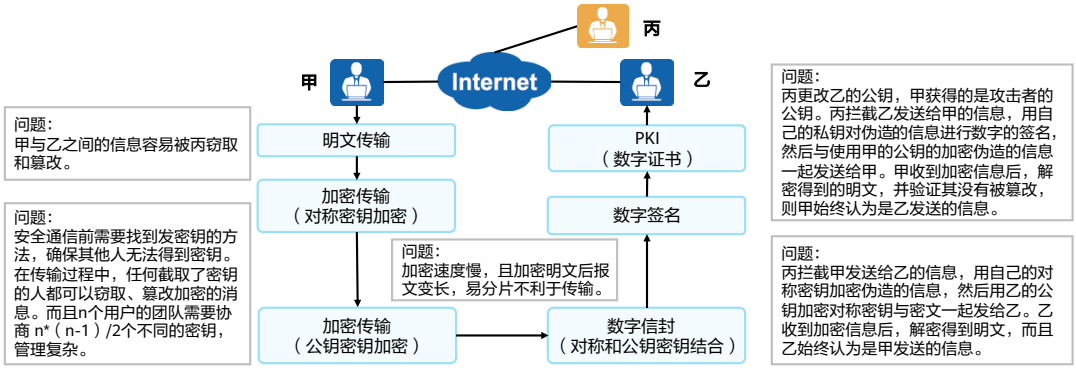
目标

- 学完本课程后，您将能够：
  - 描述数据安全通信技术
  - 描述PKI证书体系架构
  - 描述PKI工作机制

目录

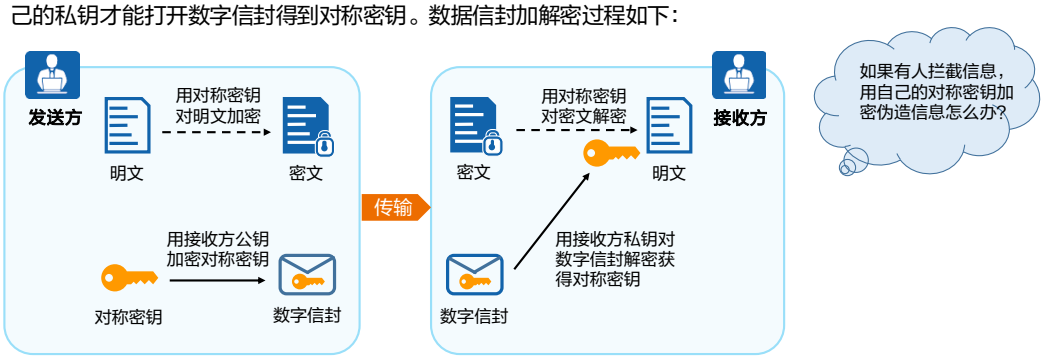
数据安全通信技术演进过程

- PKI的核心技术就围绕着数字证书的申请、颁发和使用等整个生命周期进行展开，而在这整个生命周期过程中，PKI会使用到对称密钥加密、公钥加密、数字信封和数字签名技术。
- 下图介绍这些技术的演进过程。甲和乙通过Internet进行通信，丙（模拟攻击者）专门破坏甲和乙间的通信。



数字信封

- 在现实生活中我们可以把信件装进信封，这样信件的内容就不会被他人窥探，而数据通信中也可以把通信的数据装在数字信封中。
- 数字信封是指发送方采用接收方的公钥来加密对称密钥后所得的数据。采用数字信封时，接收方需要使用自己的私钥才能打开数字信封得到对称密钥。数据信封加解密过程如下：

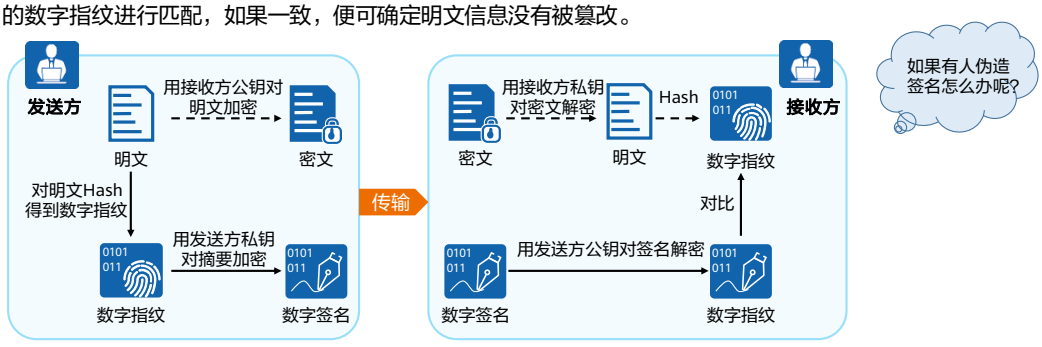


HUAWEI

- 发送方事先获得接收方的公钥，具体加解密过程如下：
  - 发送方使用对称密钥对明文进行加密，生成密文信息；
  - 发送方使用接收方的公钥加密对称密钥，生成数字信封；
  - 发送方将数字信封和密文信息一起发送给接收方；
  - 接收方接收到发送方的加密信息后，使用自己的私钥打开数字信封，得到对称密钥；
  - 接收方使用对称密钥对密文信息进行解密，得到最初的明文。
- 从加解密过程中，可以看出，数字信封技术结合了对称密钥加密和公钥加密的优点，解决了对称密钥的发布和公钥加密速度慢等问题，提高了安全性、扩展性和效率等。
- 但是，数字信封技术还有个问题，如果攻击者拦截发送方的信息，用自己的对称密钥加密伪造信息，并用接收方的公钥加密自己的对称密钥，然后发送给接收方。接收方收到加密信息后，解密得到的明文，而且接收方始终认为是发送方发送的信息。此时，需要一种方法确保接收方收到的信息就是指定的发送方发送的。

数字签名

- 数字签名是指发送方用自己的私钥对数字指纹进行加密后所得的数据。
- 数字指纹又称为信息摘要，它是指发送方通过Hash算法对明文信息计算后得出的数据。采用数字指纹时，发送方会将数字指纹和明文一起发送给接收方，接收方用同样的Hash算法对明文计算生成的数据指纹，与收到的数字指纹进行匹配，如果一致，便可确定明文信息没有被篡改。

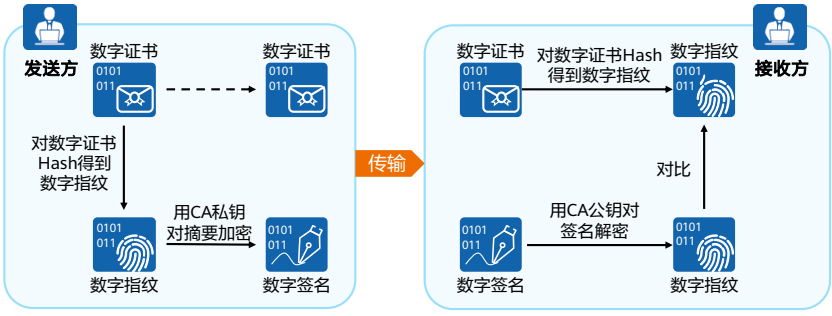


HUAWEI

- 发送方事先获得接收方的公钥，具体加解密过程如下：
  - 发送方使用接收方的公钥对明文进行加密，生成密文信息；
  - 发送方使用Hash算法对明文进行Hash运算，生成数字指纹；
  - 发送方使用自己的私钥对数字指纹进行加密，生成数字签名；
  - 发送方将密文信息和数字签名一起发送给接收方；
  - 接收方使用发送方的公钥对数字签名进行解密，得到数字指纹；
  - 接收方接收到发送方的加密信息后，使用自己的私钥对密文信息进行解密，得到最初的明文；
  - 接收方使用Hash算法对明文进行Hash运算，生成数字指纹；
  - 接收方将生成的数字指纹与得到的数字指纹进行比较。如果一致，接收方接受明文；如果不一致，接收方丢弃明文。
- 从加解密过程中，可以看出，数字签名技术不但证明了信息未被篡改，还证明了发送方的身份。数字签名和数字信封技术也可以组合使用。
- 但是，数字签名技术还有个问题，如果攻击者更改接收方的公钥，发送方获得的是攻击者的公钥，攻击者拦截接收方发送给发送方的信息，用自己的私钥对伪造的信息进行数字签名，然后与使用发送方的公钥加密的伪造信息一起发送给发送方。发送方收到加密信息后，解密得到的明文，并验证明文没有被篡改，则发送方始终认为是接收方发送的信息。此时，需要一种方法确保一个特定的公钥属于一个特定的拥有者。

数字证书

- 数字证书简称证书，它是一个经证书授权中心（即在PKI中的证书认证机构CA）数字签名的文件，包含拥有者的公钥及相关身份信息。数字证书技术解决了数字签名技术中无法确定公钥是指定拥有者的问题。
- 数字证书可以说是Internet上的安全护照或身份证。当人们到其他国家旅行时，用护照可以证实其身份，并被获准进入这个国家。数字证书提供的是网络上的身份证明。

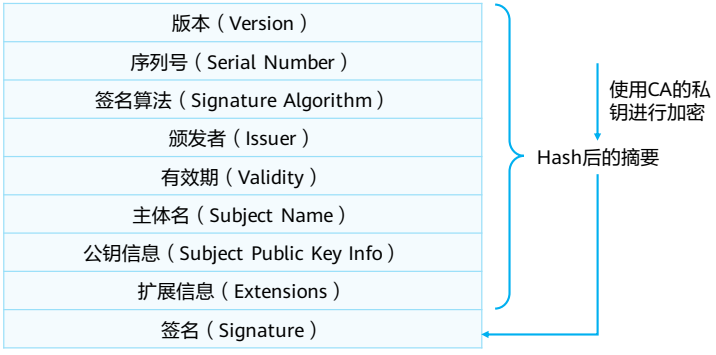


HUAWEI

- 数字证书的生成：CA收到数字证书申请并认证申请者的真实身份后，把申请者的公钥、身份信息、数字证书的有效期等信息作为消息明文，进行Hash生成摘要，并用CA的私钥加密进行签名；数字签名与证书拥有者的公钥、身份信息、证书有效期等其他信息共同组成数字证书。简单地来说，把上面的明文换成公钥、身份信息、有效期等其他信息，就是数字证书的生成和验证过程。
- 使用CA公钥进行签名和解密，可以证明证书确实是由CA发布的。
- 两份摘要的对比结果，可以证明证书内容是否在传输过程中被改动。如果消息明文中的公钥和身份信息是CA的，则是CA自签名的过程。
- 数字证书的最初目的是建立公钥与用户之间的对应关系。
    - 由于公钥是随机产生的，从公钥无法直接判断属于哪个用户。为解决公钥与用户映射关系问题，PKI引入数字证书，用于建立公钥与用户之间的对应关系；
    - 由于数字证书中包含用户身份信息和公钥信息，根据数字证书就可以直接判断该公钥属于哪个用户；
    - 由于数字证书中不包含秘密信息，因此数字证书可公开发布。

数字证书结构

- 最简单的证书包含一个公钥、名称以及证书授权中心的数字签名。
- 一般情况下证书中还包括密钥的有效期，颁发者（证书授权中心）的名称，该证书的序列号等信息。证书的结构遵循X.509 v3版本的规范。



HUAWEI

- 证书内容中各字段含义如下：
  - 版本：即使用X.509的版本，目前普遍使用的是v3版本（0x2）；
  - 序列号：颁发者分配给证书的一个正整数，同一颁发者颁发的证书序列号各不相同，可用与颁发者名称一起作为证书唯一标识；
  - 签名算法：颁发者颁发证书使用的签名算法；
  - 颁发者：颁发该证书的设备名称，必须与颁发者证书中的主体名一致。通常为CA服务器的名称；
  - 有效期：包含有效的起、止日期，不在有效期范围的证书为无效证书；
  - 主体名：证书拥有者的名称，如果与颁发者相同则说明该证书是一个自签名证书；
  - 公钥信息：用户对外公开的公钥以及公钥算法信息；
  - 扩展信息：通常包含了证书的用法、CRL的发布地址等可选字段；
  - 签名：颁发者用私钥对证书信息的签名。

数字证书分类

- 数字证书有三种类型：CA证书、本地证书及自签名证书。

CA证书	本地证书	自签名证书
• CA自身的证书。 • PKI系统中没有多层级CA，CA证书就是自签名证书。 • PKI系统中有多层级CA，则会形成一个CA层次结构，最上层的CA是根CA，它拥有一个CA“自签名”的证书。 • 申请者通过验证CA的数字签名从而信任CA，任何申请者都可以得到CA的证书（含公钥），用以验证它所颁发的本地证书。	• CA颁发给申请者的证书。 • 本地证书就是通常意义上的证书，由用户向CA发起申请，CA审核通过后颁发给用户使用的证书。	• 自签名证书是设备为自己颁发的证书，由设备的预置CA进行签名。 • 通过设备生成自签名证书和不带签名的证书，可以实现简单证书颁发功能。

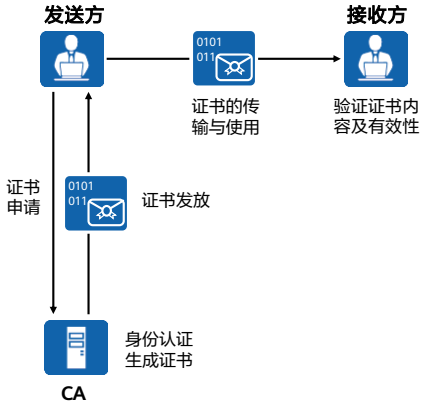
数字证书格式

- 数字证书支持三种文件格式保存。

格式	描述
PKCS#12	以二进制格式保存证书，可以包含私钥，也可以不包含私钥。常用的后缀有：.P12和.PFX。
DER	以二进制格式保存证书，不包含私钥。常用的后缀有：.DER、.CER和.CRT。
PEM	以ASCII码格式保存证书，可以包含私钥，也可以不包含私钥。常用的后缀有：.PEM、.CER和.CRT。

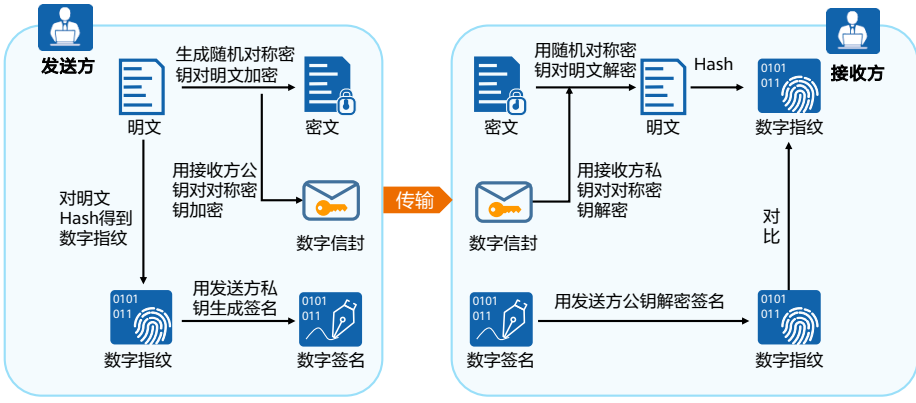
数据通信全过程（1）

- 数字证书提供了一种发布公钥的简便途径，大家通过向CA申请认证发布自己的公钥，通过向CA验证来确认自己获得了别人的公钥。
- 数字证书的申请、发布及使用具体流程如下：
  - 发送方先向CA发起数字证书申请；
  - CA对发送方进行身份认证，认证通过后生成数字证书；
  - CA将生成的数字证书发放给发送方；
  - 接收方下载发送方的数字证书；
  - 接收方收到数字证书后，使用CA公钥对数字签名解密生成消息摘要，对证书内容进行hash生成摘要，两份摘要进行比对可证明证书内容的完整性与真实性。



数据通信全过程（2）

- 下图展示了通信双方互相获得公钥完成身份认证后的通信过程。



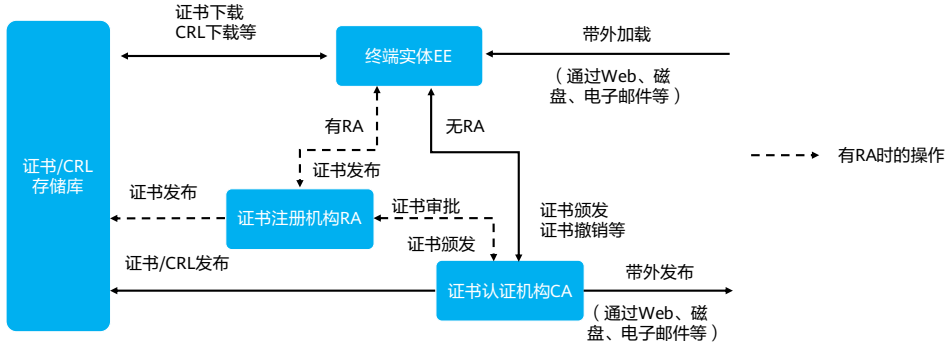
HUAWEI

- 发送方处理过程：
  - 发送方对要传输消息明文进行Hash，生成数字指纹，再用发送方的私钥生成数字签名；
  - 发送方随机生成对称秘钥，对明文加密，生成密文；
  - 发送方用接收方公钥加密对称秘钥；
  - 将加密后的对称秘钥、数字签名与密文一同发送给接收方。
- 接收方处理过程：
  - 接收方收到消息后，用自己的私钥解密对称秘钥；
  - 用对称秘钥解密密文，得到明文；
  - 对明文Hash得到数字指纹，用发送方的公钥解密签名得到数字指纹，对比两份数字指纹，如果相同接收消息，如果不同丢弃。
- 非对称加密安全性高，但计算量大效率低，因此使用对称秘钥对通信的主要内容进行加密。对称秘钥每次使用随机生成，用完即丢弃，降低风险。
- 用接收方公钥加密对称秘钥，保证了只有接收方才能对密文进行解密。用发送方私钥进行签名，使得接收方可以验证消息的发送方和消息是否被修改过，保证了信息的完整性和抗否认性。

目录

PKI体系架构

- PKI是Public Key Infrastructure的缩写，是通过使用公钥技术和数字证书来提供系统信息安全服务，并负责验证数字证书持有者身份的一种体系。PKI的本质是把非对称密钥管理标准化。
- 一个PKI体系由终端实体、证书认证机构、证书注册机构和证书/CRL存储库四部分共同组成。



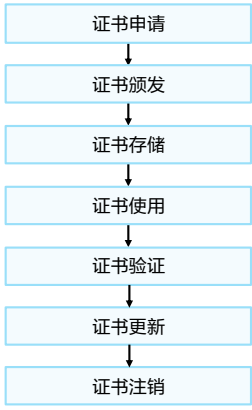
HUAWEI

- 终端实体EE（End Entity）：也称为PKI实体，它是PKI产品或服务的最终使用者，可以是个人、组织、设备（如路由器、防火墙）或计算机中运行的进程。
- 证书认证机构CA：CA是PKI的信任基础，是一个用于颁发并管理数字证书的可信实体。它是一种权威性、可信任性和公正性的第三方机构，通常由服务器充当。
  - CA通常采用多层次的分级结构，根据证书颁发机构的层次，可以划分为根CA和从属CA；
    - 根CA是公钥体系中第一个证书颁发机构，它是信任的起源。根CA可以为其它CA颁发证书，也可以为其它计算机、用户、服务颁发证书。对大多数基于证书的应用程序来说，使用证书的认证都可以通过证书链追溯到根CA。根CA通常持有一个自签名证书；
    - 从属CA必须从上级CA处获取证书。上级CA可以是根CA或者是一个已由根CA授权可颁发从属CA证书的从属CA。上级CA负责签发和管理下级CA的证书，最下一级的CA直接面向用户。例如，CA2和CA3是从属CA，持有CA1发行的CA证书；CA4、CA5和CA6是从属CA，持有CA2发行的CA证书。
  - 当某个PKI实体信任一个CA，则可以通过证书链来传递信任，证书链就是从用户的证书到根证书所经过的一系列证书的集合。当通信的PKI实体收到待验证的证书时，会沿着证书链依次验证其颁发者的合法性；
  - CA的核心功能就是发放和管理数字证书，包括：证书的颁发、证书的更新、证书的撤销、证书的查询、证书的归档、证书废除列表CRL的发布等。

- 证书注册机构RA（Registration Authority）：是数字证书注册审批机构，RA是CA面对用户的窗口，是CA的证书发放、管理功能的延伸，它负责接受用户的证书注册和撤销申请，对用户的身份信息进行审查，并决定是否向CA提交签发或撤销数字证书的申请。RA作为CA功能的一部分，实际应用中，通常RA并不一定独立存在，而是和CA合并在一起。RA也可以独立出来，分担CA的一部分功能，减轻CA的压力，增强CA系统的安全性。
- 证书/CRL存储库：由于用户名称的改变、私钥泄漏或业务中止等原因，需要存在一种方法将现行的证书吊销，即撤消公钥及相关的PKI实体身份信息的绑定关系。在PKI中，所使用的这种方法为证书废除列表CRL。任何一个证书被撤消以后，CA就要发布CRL来声明该证书是无效的，并列出所有被废除的证书的序列号。因此，CRL提供了一种检验证书有效性的方式。证书/CRL存储库用于对证书和CRL等信息进行存储和管理，并提供查询功能。构建证书/CRL存储库可以采用LDAP（Lightweight Directory Access Protocol）服务器、FTP（File Transfer Protocol）服务器、HTTP（Hypertext Transfer Protocol）服务器或者数据库等。其中，LDAP规范简化了笨重的X.500目录访问协议，支持TCP/IP，已经在PKI体系中被广泛应用于证书信息发布、CRL信息发布、CA政策以及与信息发布相关的各个方面。如果证书规模不是太大，也可以选择架设HTTP、FTP等服务器来储存证书，并为用户提供下载服务。

PKI证书申请流程

- PKI的核心技术就围绕着本地证书的申请、颁发、存储、下载、安装、验证、更新和撤销的整个生命周期进行展开。



HUAWEI

- 证书申请：证书申请即证书注册，就是一个PKI实体向CA自我介绍并获取证书的过程。
- 证书颁发：PKI实体向CA申请本地证书时，如果有RA，则先由RA审核PKI实体的身份信息，审核通过后，RA将申请信息发送给CA。CA再根据PKI实体的公钥和身份信息生成本地证书，并将本地证书信息发送给RA。如果没有RA，则直接由CA审核PKI实体身份信息。
- 证书存储：CA生成本地证书后，CA/RA会将本地证书发布到证书/CRL存储库中，为用户提供下载服务和目录浏览服务。
- 证书下载：PKI实体通过SCEP或CMPv2协议向CA服务器下载已颁发的证书，或者通过LDAP、HTTP或者带外方式，下载已颁发的证书。该证书可以是自己的本地证书，也可以是CA/RA证书或者其他PKI实体的本地证书。
- 证书安装：PKI实体下载证书后，还需安装证书，即将证书导入到设备的内存中，否则证书不生效。该证书可以是自己的本地证书，也可以是CA/RA证书，或其他PKI实体的本地证书。通过SCEP协议申请证书时，PKI实体先获取CA证书并将CA证书自动导入设备内存中，然后获取本地证书并将本地证书自动导入设备内存中。
- 证书验证：PKI实体获取对端实体的证书后，当需要使用对端实体的证书时，例如与对端建立安全隧道或安全连接，通常需要验证对端实体的本地证书和CA的合法性（证书是否有效或者是否属于同一个CA颁发等）。如果证书颁发者的证书无效，则由该CA颁发的所有证书都不再有效。但在CA证书过期前，设备会自动更新CA证书，异常情况下才会出现CA证书过期现象。

- 证书更新：当证书过期、密钥泄漏时，PKI实体必须更换证书，可以通过重新申请来达到更新的目的，也可以使用SCEP或CMPv2协议自动进行更新。
- 证书撤销：由于用户身份、用户信息或者用户公钥的改变、用户业务中止等原因，用户需要将自己的数字证书撤消，即撤消公钥与用户身份信息的绑定关系。在PKI中，CA主要采用CRL或OCSP协议撤销证书，而PKI实体撤销自己的证书是通过带外方式申请。

PKI证书申请流程

- PKI证书申请流程如下：
  - 用户申请：用户获取CA的数字证书（根证书），与安全服务器建立连接，同时生成自己的公钥和私钥，将公钥和自己的身份信息提交给安全服务器。安全服务器将用户的申请信息传送给RA服务器。
  - RA审核：RA收到用户的申请，用户向RA证明自己的身份，RA进行核对。如果RA同意用户申请证书的请求，则对证书申请信息做数字签名，否则拒绝用户的申请。
  - CA发行证书：RA将用户申请和RA签名传输给CA，CA对RA数字签名做认证，如果验证通过，则同意用户请求，颁发证书，然后将证书输出。如果验证不通过，则拒绝证书申请。
  - RA转发证书：RA从CA得到新的证书，首先将证书输出到LDAP服务器以提供目录浏览，再通知用户证书发行成功，告知证书序列号，到指定的网址去下载证书。
  - 用户证书获取：用户使用证书序列号去指定网址下载自己的数字证书，只有持有与申请时提交的公钥配对的私钥才能下载成功。

证书申请方式

- PKI实体向CA申请本地证书有以下几种方式：

方式	描述
SCEP	SCEP（Simple Certificate Enrollment Protocol）主要用于在线申请，是VPN设备PKI证书申请的工业标准，使用HTTP协议被绝大多数VPN和CA厂商支持，为VPN设备（VPN最终用户）提供了简单而功能强大的证书申请方式。
CMPv2	CMPv2（Certificate Management Protocol version 2）协议向CA发送证书注册请求消息来申请本地证书。
File-based	File-based主要用于离线证书申请，PKI实体使用PKCS#10格式打印出本地的证书注册请求消息并保存到文件中，然后通过带外方式（如Web、磁盘、电子邮件等）将文件发送给CA进行证书申请。

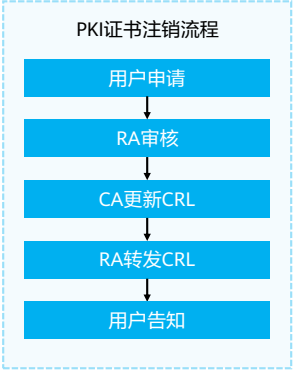
PKI证书验证

- PKI实体获取对端实体的证书后，当需要使用对端实体的证书时，通常需要验证对端实体的本地证书和CA的合法性。通常检查证书状态的方式有三种：CRL方式、OCSP方式、None方式。
  - CRL方式
    - PKI实体可以通过SCEP、HTTP、LDAP和LDAPv3模板方式下载CRL。
    - 当PKI实体验证本地证书时，先查找本地内存的CRL，如果本地内存没有CRL，则需下载CRL并安装到本地内存中，如果对端实体的本地证书在CRL中，表示此证书已被撤销。
  - OCSP方式
    - 在IPSec场景中，PKI实体间使用证书方式进行IPSec协商时，可以通过OCSP方式实时检查对端实体的证书状态。
    - OCSP克服了CRL的主要缺陷：PKI实体必须经常下载CRL以确保列表的更新。当PKI实体访问OCSP服务器时，会发送一个对于证书状态信息的请求。OCSP服务器会回复一个“有效”、“过期”或“未知”的响应。
  - None方式
    - 如果PKI实体没有可用的CRL和OCSP服务器，或者不需要检查PKI实体的本地证书状态，可以采用None方式，即不检查证书是否被撤销。

- OCSP方式中，服务器的响应消息：
  - 有效表示证书没有被撤销；
  - 过期表示证书已被撤销；
  - 未知表示OCSP服务器不能判断请求的证书状态。

PKI证书注销流程

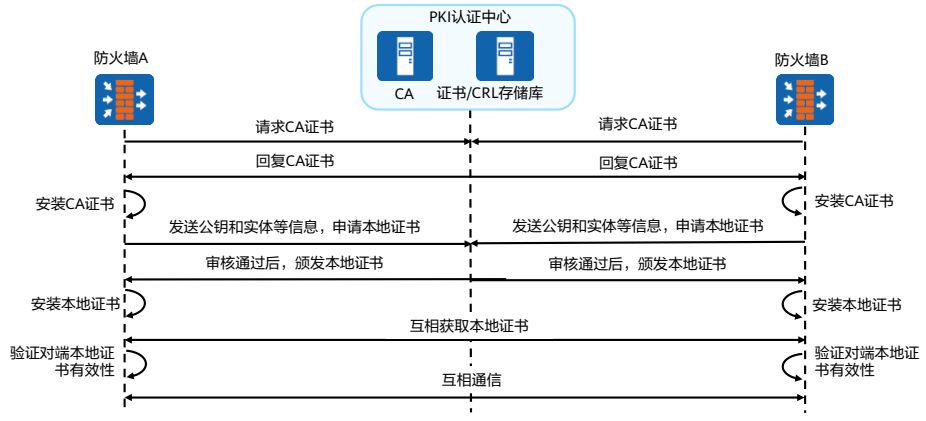
- 证书撤销流程如下：
  - 用户申请：用户向RA发送一封签名加密邮件，申请撤销证书；
  - RA审核：注册机构同意证书撤销，并对申请签名；
  - CA更新CRL：CA验证证书撤销请求的RA签名，如果正确，则同意申请，更新CRL，并输出；
  - RA转发CRL：注册中心收到CRL，以多种方式将CRL公布（包括LDAP服务器）；
  - 用户告知：用户访问LDAP服务器，下载或浏览CRL。



目录

PKI工作机制

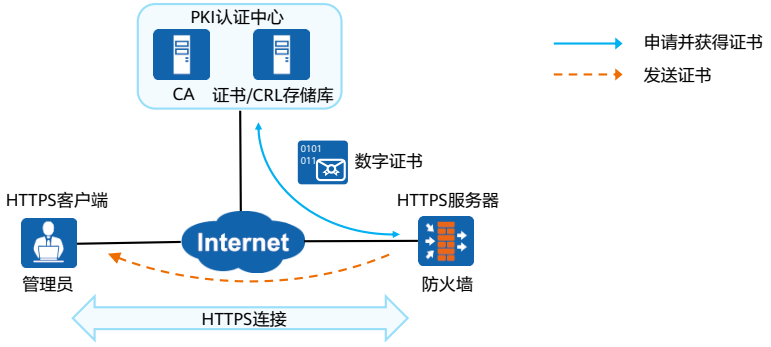
- 针对一个使用PKI的网络，配置PKI的目的就是为指定的PKI实体向CA申请一个本地证书，并由设备对证书的有效性进行验证。PKI具体工作过程如下：



- PKI实体向CA请求CA证书，即CA服务器证书。
- CA收到PKI实体的CA证书请求时，将自己的CA证书回复给PKI实体。
- PKI实体收到CA证书后，安装CA证书。
  - 当PKI实体通过SCEP协议申请本地证书时，PKI实体会用配置的Hash算法对CA证书进行运算得到数字指纹，与提前配置的CA服务器的数字指纹进行比较，如果一致，则PKI实体接受CA证书，否则PKI实体丢弃CA证书。
- PKI实体向CA发送证书注册请求消息（包括配置的密钥对中的公钥和PKI实体信息）。
  - 当PKI实体通过SCEP协议申请本地证书时，PKI实体对证书注册请求消息使用CA证书的公钥进行加密和自己的私钥进行数字签名。如果CA要求验证挑战密码，则证书注册请求消息必须携带挑战密码（与CA的挑战密码一致）；
  - 当PKI实体通过CMPv2协议申请本地证书时，PKI实体可以使用额外证书（其他CA颁发的本地证书）或者消息认证码方式进行身份认证。
    - 额外证书方式：PKI实体对证书注册请求消息使用CA证书的公钥进行加密和PKI实体的额外证书相对应的私钥进行数字签名；
    - 消息认证码方式：PKI实体对证书注册请求消息使用CA证书的公钥进行加密，而且证书注册请求消息必须包含消息认证码的参考值和秘密值（与CA的消息认证码的参考值和秘密值一致）。

PKI证书应用场景 - 通过HTTPS登录Web

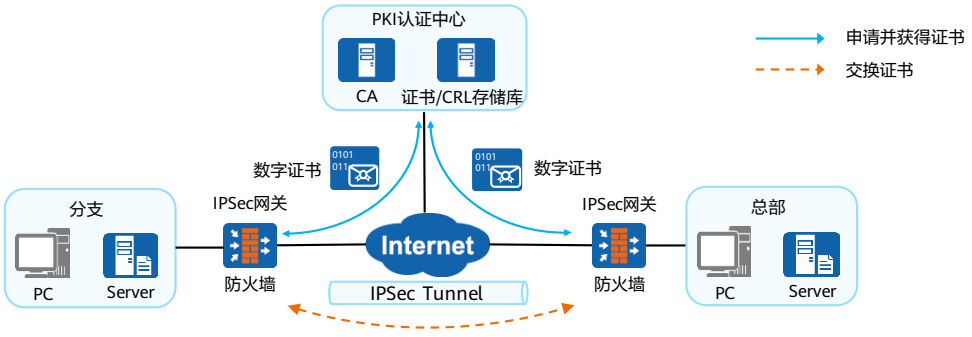
- 在设备上为HTTPS客户端指定由Web浏览器信任的CA颁发的本地证书。这样，Web浏览器可以验证本地证书的合法性，避免了可能存在的主动攻击，保证了管理员的安全登录。



- 在SSL连接建立的过程中，HTTPS客户端和HTTPS服务器之间的主要交互流程如下：
  - HTTPS服务器向PKI认证中心申请本地证书；
  - PKI认证中心向HTTPS服务器颁发本地证书；
  - HTTPS服务器将携带自己公钥信息的数字证书发送给HTTPS客户端；
  - HTTPS客户端验证HTTPS服务器的本地证书合法后，利用证书中的公钥加密HTTPS客户端随机生成的密钥，并发送给HTTPS服务器；
  - HTTPS客户端和HTTPS服务器通过协商，最终确定所使用的密钥和加密套件；
  - 后续传输的数据，双方都会使用该密钥和加密套件进行加密处理。

PKI证书应用场景 - IPSec VPN

- IPSec采用基于PKI的证书进行身份认证后，在进行IKE协商过程中交换密钥时，会对通信双方进行身份认证，保证了密钥交换的安全。

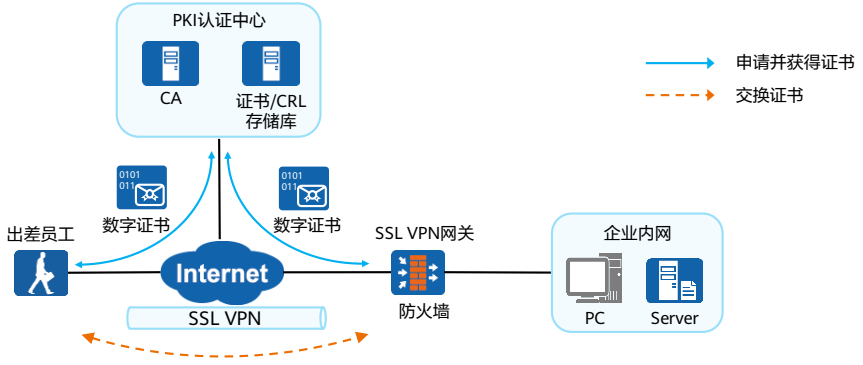


HUAWEI

- 因为公网是不安全的网络，为了保护数据的安全性，设备采用IPSec技术，与对端设备建立IPSec隧道。通常情况下，IPSec采用预共享密钥方式协商IPSec。但是，在大型网络中IPSec采用预共享密钥方式时存在密钥交换不安全和配置工作量大的问题。为了解决上述问题，设备之间可以采用基于PKI的证书进行身份认证来完成IPSec隧道的建立。
- 采用基于PKI的证书进行身份认证后，IPSec在进行IKE协商过程中交换密钥时，会对通信双方进行身份认证，保证了密钥交换的安全。而且，证书可以为IPSec提供集中的密钥管理机制，并增强整个IPSec网络的可扩展性。同时，在采用证书认证的IPSec网络中，每台设备都拥有PKI认证中心颁发的本地证书。有新设备加入时，只需要为新增加的设备申请一个证书，新设备就可以与其它设备进行安全通讯，而不需要对其他设备的配置进行修改，这大大减少了配置工作量。

PKI证书应用场景 - SSL VPN

- SSL VPN可以为出差员工提供方便的接入功能，使其在出差期间也可以正常访问内部网络。为了提高出差员工访问内部网络的安全性，设备可以采用PKI的证书方式来对用户进行认证。



- 在SSL VPN应用中，SSL VPN客户端可以通过证书验证SSL VPN网关的身份；SSL VPN网关也可以通过证书来验证客户端的身份。

本章总结

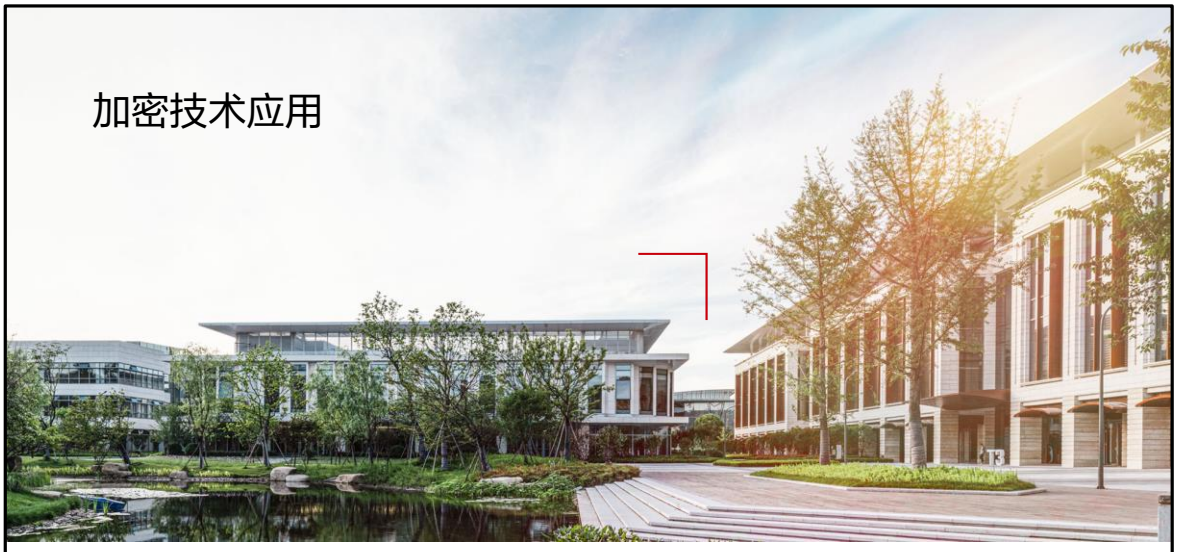
- 本课程简要介绍了数字信封、数字签名及数字证书的基本概念及工作原理，系统介绍了PKI体系架构组成及PKI工作机制，描述了常见的数字证书应用场景。
- 通过本课程的学习，您会对PKI体系架构有更深理解、提升了对数字证书灵活应用能力。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

加密技术应用



HUAWEI

前言

- 通过加密技术，可以保证网络中数据传输的安全性，数据不会被篡改和窥探；通过签名技术，可以保证数据的完整性，证明了数据发送方的身份；通过PKI证书认证技术，可以验证公钥的合法性，从而保证用户接入到安全、合法的网络中。
- 通过使用这些技术，企业可以防止非法用户接入企业网络中。企业分支之间可以建立安全通道，保证企业数据的安全性。

目标

- 学完本课程后，您将能够：
  - 描述加密技术的应用场景
  - 使用不同VPN技术的配置方法

目录

加密学的应用（1）

- 在信息安全领域，主要使用数字信封、数字签名和数字证书等密码技术。

信息安全要素	应付的威胁	使用的密码技术
机密性	窃听 敏感信息泄露	数字信封 对称加密和非对称加密
完整性	篡改 破坏	数字签名 哈希函数
可鉴别性	伪装 仿冒	数字证书和数字签名 口令和共享秘密
不可否认性	否认已送到资料 否认已收到资料	数字证书和数字签名 证据存储
授权及访问控制	越权访问 非法存取资料	访问控制 属性证书

- 数字信封：结合对称和非对称加密，从而保证数据传输的机密性。
- 数字签名：采用散列算法，从而保证数据传输的完整性。
- 数字证书：通过第三方机构（CA）对公钥进行公证，从而保证数据传输的不可否认性。

加密学的应用 (2)

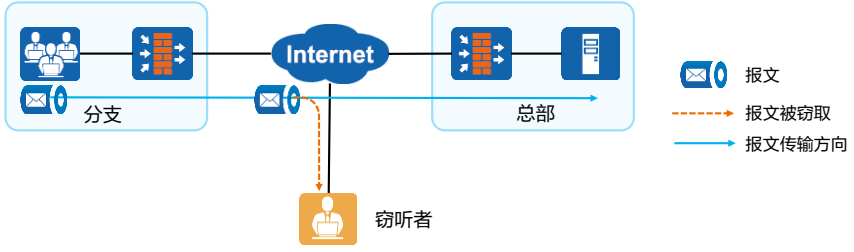
- 结合到实际的网络应用场景，数字信封、数字签名和数字证书可以用于以下场景：
  - VPN：很多VPN技术需要采用加解密技术来保证数据的机密性，如IPSec VPN、SSL VPN。
  - IPv6：为了防止设备被攻击者冒充，可以在设备上配置SEND（Secure Neighbor Discovery）路由器授权功能。通过数字证书技术选用合法网关设备。
  - HTTPS登录设备：管理员可以通过HTTPS方式安全地登录HTTPS服务器的Web界面，并通过Web界面对设备进行管理。为了提高双方建立SSL连接时的安全性，在设备上为HTTPS客户端指定由Web浏览器信任的CA颁发的本地证书。这样，Web浏览器可以验证本地证书的合法性，避免了可能存在的主动攻击，保证了管理员的安全登录。
  - 设备系统登录授权：将用户密码先进行摘要算法之后存放，用户登录时比对授权。

- 在各种应用场景中，其中最主要的应用场景就是在VPN上的应用。
- 本课程主要介绍几种加密VPN及一些其他常用的VPN技术。

目录

VPN产生背景

- 在VPN（Virtual Private Network）出现之前，跨越Internet的数据传输只能依靠现有物理网络，具有很多的不安全因素。
- 如下图所示，某企业的总部和分支机构位于不同区域（如位于不同的国家或城市），当分支机构员工需访问总部服务器的时候，数据传输要经过Internet。由于Internet中存在多种不安全因素，则当分支机构的员工向总部服务器发送访问请求时，报文容易被网络中的黑客窃取或篡改，最终造成数据泄密、重要数据被破坏等后果。



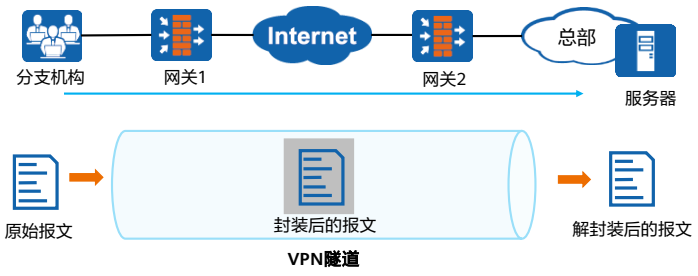
VPN定义

- VPN即虚拟专用网，用于在公用网络上构建私人专用虚拟网络，并在此虚拟网络中传输私网流量。VPN把现有的物理网络分解成逻辑上隔离的网络，在不改变网络现状的情况下实现安全、可靠的连接。
- VPN具有以下两个基本特征：
  - 专用（Private）：VPN网络是专门供VPN用户使用的网络，对于VPN用户，使用VPN与使用传统专网没有区别。VPN能够提供足够的安全保证，确保VPN内部信息不受外部侵扰。VPN与底层承载网络（一般为IP网络）之间保持资源独立，即VPN资源不被网络中非该VPN的用户所使用；
  - 虚拟（Virtual）：VPN用户内部的通信是通过公共网络进行的，而这个公共网络同时也可以被其他非VPN用户使用，VPN用户获得的只是一个逻辑意义上的专网。这个公共网络称为VPN骨干网（VPN Backbone）。
- VPN对数据进行封装和加密，即使网络黑客窃取到数据也无法破解，确保了数据的安全性，且搭建VPN不需改变现有网络拓扑，没有额外费用。

- VPN和传统的数据专网相比具有如下优势：
  - 安全：远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的连接，保证数据传输的安全性。这对于实现电子商务或金融网络与通讯网络的融合特别重要；
  - 廉价：利用公共网络进行信息通讯，企业可以用更低的成本连接远程办事机构、出差人员和业务伙伴；
  - 支持移动业务：支持驻外VPN用户在任何时间、任何地点的移动接入，能够满足不断增长的移动业务需求；
  - 可扩展性：由于VPN为逻辑上的网络，物理网络中增加或修改节点，不影响VPN的部署；
  - VPN在保证网络的安全性、可靠性、可管理性的同时提供更强的扩展性和灵活性。在全球任何一个角落，只要能够接入到Internet，即可使用VPN。

VPN封装原理

- VPN的基本原理是利用隧道（Tunnel）技术，对传输报文进行封装，利用VPN骨干网建立专用数据传输通道，实现报文的安全传输。
- 隧道技术使用一种协议封装另外一种协议报文（通常是IP报文），而封装后的报文也可以再次被其他封装协议所封装。对用户来说，隧道是其所在网络的逻辑延伸，在使用效果上与实际物理链路相同。



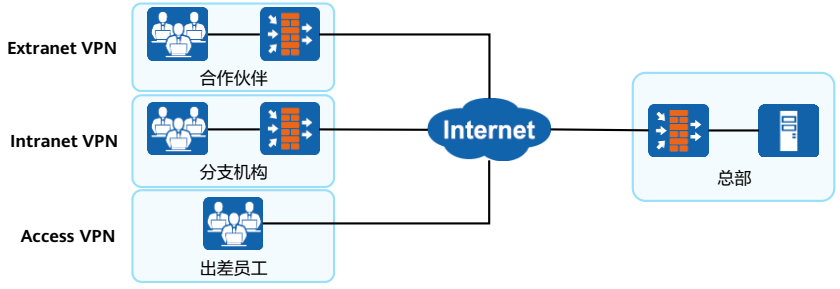
VPN分类：根据应用场景

- VPN现在广泛应用于企业网络分支机构和出差员工连接总部网络的场景，以下是VPN常见的几种分类方式。
- 根据应用场景不同分类：
  - Client-to-Site VPN：即客户端与企业内网之间通过VPN隧道建立连接，客户端可以是一台防火墙、路由器，也可以是个人计算机。此场景可以使用以下几种VPN技术实现：SSL、IPSec、L2TP和L2TP over IPSec；
  - Site-to-Site VPN：即两个局域网之间通过VPN隧道建立连接，部署的设备通常为路由器或者防火墙。此场景可以使用以下几种VPN技术实现：IPSec、L2TP、L2TP over IPSec、GRE over IPSec和IPSec over GRE。

- Client-to-Site VPN：又称Remote Access VPN适用于出差员工VPN拨号接入的场景。员工可以在任何能接入Internet的地方，通过远程拨号接入企业内网，从而访问内网资源。
- Site-to-Site VPN：适用于公司两个异地机构的局域网互连。

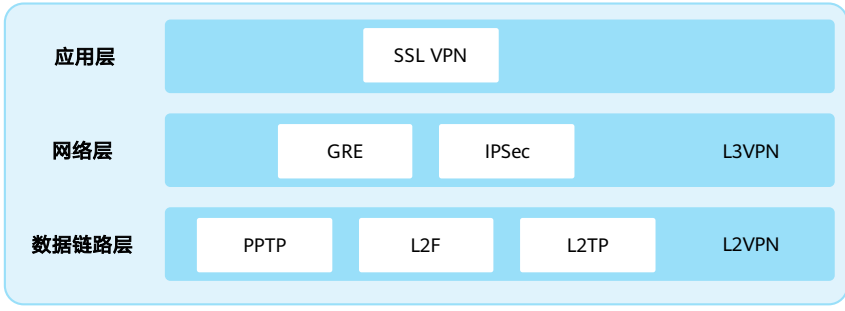
VPN分类：根据应用对象

- 根据应用对象不同分类：
  - Extranet VPN： 利用VPN将企业网延伸至合作伙伴处，使不同企业间通过Internet来构筑VPN；
  - Intranet VPN：通过公用网络进行企业内部各个网络的互连；
  - Access VPN：面向出差员工，允许出差员工跨越公用网络远程接入公司内部网络。



VPN分类：根据VPN实现层次

- 根据VPN技术实现的网络层次分类：

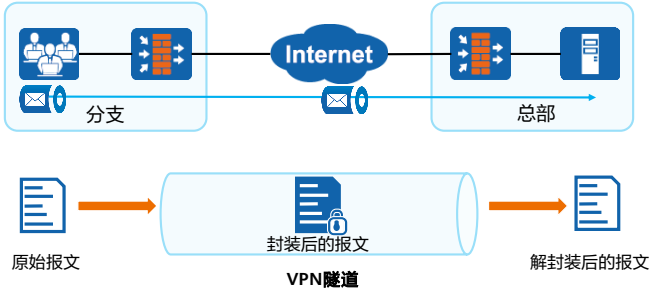


HUAWEI

- L3VPN
  - 三层VPN主要是指VPN技术工作在协议栈的网络层。以IPSec VPN技术为例，IPSec报头与IP报头工作在同一层次，封装报文时是以IP in IP的方式进行封装，或者是IPSec报头与IP报头同时对数据载荷进行封装；
  - 除IPSec VPN技术外，主要的三层VPN技术还有GRE VPN。GRE VPN产生的时间比较早，实现的机制也比较简单。GRE VPN可以实现任意一种网络协议在另一种网络协议上的封装。与IPSec相比，安全性没有得到保证，只能提供有限的简单的安全机制。
- L2VPN
  - 与三层VPN类似，二层VPN则是指VPN技术工作在协议栈的数据链路层。二层VPN主要包括的协议有点到点隧道协议（PPTP，Point-to-Point Tunneling Protocol）、二层转发协议（L2F，Layer 2 Forwarding）以及二层隧道协议（L2TP，Layer 2 Tunneling Protocol）。

VPN的关键技术：隧道技术

- VPN的基本原理是利用隧道（Tunnel）技术，对传输报文进行封装，利用VPN骨干网建立专用数据传输通道，实现报文的安全传输。
- 隧道技术使用一种协议封装另外一种协议报文（通常是IP报文），而封装后的报文也可以再次被其他封装协议所封装。对用户来说，隧道是其所在网络的逻辑延伸，在使用效果上与实际物理链路相同。



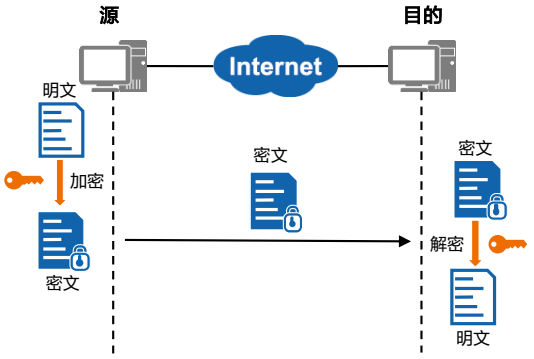
- 隧道技术是VPN的基本技术，类似于点对点连接技术。如图所示，分支VPN网关收到原始报文后，将报文封装，然后通过Internet传输到总部VPN网关。总部VPN网关再对报文进行解封装，最后得到原始报文。
- “封装/解封装”过程本身就可以为原始报文提供安全防护功能，所有被封装的报文在Internet上传输时所经过的逻辑路径被称为“隧道”。

VPN的关键技术：身份认证技术

- 身份认证技术，其主要用于移动办公用户远程接入的情况。总部的VPN网关对用户的身份进行认证，确保接入内部网络的用户是合法用户，而非恶意用户。不同的VPN技术能提供的用户身份认证方法不同：
  - GRE：不支持针对用户的身份认证技术；
  - L2TP：依赖PPP提供的认证。对接入用户进行认证时候，可以使用本地认证方式也可以使用第三方RADIUS服务器来认证，认证通过以后会给用户分配内部的IP地址，通过此IP地址对用户进行授权和管理；
  - IPSec：使用IKEv2时，支持对用户进行EAP认证。认证方式同L2TP一样，认证通过后分配IP地址，通过此IP地址可以对用户进行授权和管理；
  - SSL VPN：对接入用户进行认证时，支持本地认证、证书认证和服务器认证，另外，接入用户也可以对SSL VPN服务器进行身份认证，确认SSL VPN服务器的合法性。

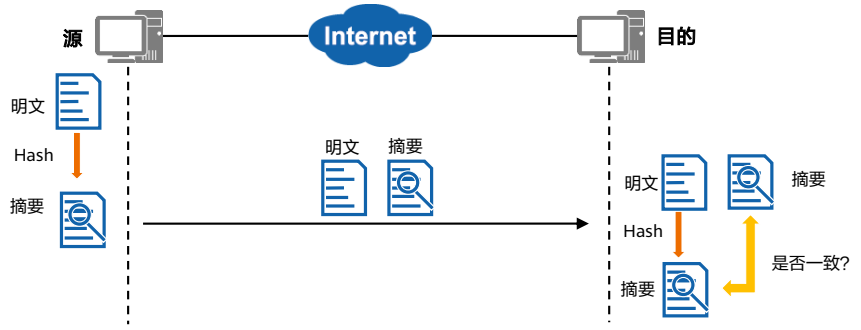
VPN的关键技术：加密技术

- 加密技术就是把明文加密成密文的过程，这样即便黑客截获了报文也无法知道其真实含义。加密对象有数据报文和协议报文之分，能够实现协议报文和数据报文都加密的协议安全系数更高。
- GRE和L2TP协议本身不提供加密技术，所以通常结合IPSec协议一起使用，依赖IPSec的加密技术。
- IPSec：支持对数据报文和协议报文进行加密。
- SSL VPN：支持对数据报文和协议报文加密。



VPN的关键技术：数据验证技术

- 数据验证技术就是对报文的真伪进行检查，丢弃伪造的、被篡改的报文。那么验证是如何实现的呢？它采用一种称为“摘要”的技术。
- “摘要”技术主要采用Hash函数将一段长的报文通过函数变换，映射为一段短的报文。在收发两端都对报文进行验证，只有摘要一致的报文才被接受。



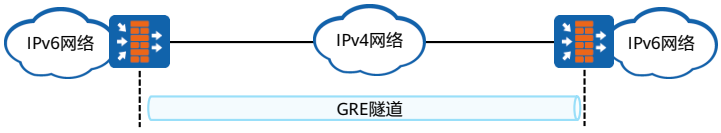
VPN技术对比

技术	保护范围	适用场景	身份认证	加密和验证
GRE	IP及以上数据	Intranet VPN	不支持	支持简单的关键字验证、校验和验证
IPSec	IP及以上数据	Access VPN Intranet VPN Extranet VPN	支持预共享密钥或证书认证； 支持IKEv2的EAP认证	支持
L2TP	IP及以上数据	Access VPN Extranet VPN	支持基于PPP的CHAP、PAP、EAP认证	不支持
SSL VPN	应用层特定数据	Access VPN	支持用户名/密码或证书认证	支持

目录

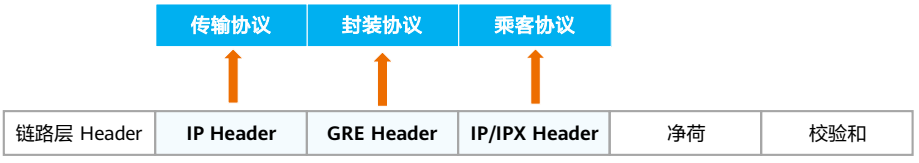
GRE VPN简介

- Generic Routing Encapsulation，简称GRE，是一种三层VPN封装技术。GRE可以对某些网络层协议（如IPX、Apple Talk、IP等）的报文进行封装，使封装后的报文能够在另一种网络中（如IPv4）传输，从而解决了跨越异种网络的报文传输问题。
- 异种报文传输的通道称为Tunnel（隧道）。
- 通常通过在IPv4网络上建立GRE隧道，解决两个IPv6网络的通信问题。



GRE协议栈

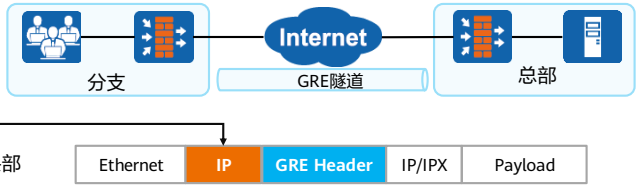
- 网络封装技术，其基本的构成要素都可以分为三个部分：乘客协议、封装协议、传输协议。GRE也不例外，为了方便理解，我们用邮政系统打个比方：
  - 乘客协议就是我们自己写的信，信的语言可以是汉语、英语、法语等，具体的内容由写信人、读信人自己负责；
  - 封装协议可以理解为信封，可以是平信、挂号或者EMS，不同的信封就对应于多种封装协议；
  - 运输协议就是信的运输方式，可以是陆运、海运或者空运，不同的运输方式就对应于多种运输协议。



- GRE封装报文时，封装前的报文称为净荷，封装前的报文协议称为乘客协议，然后GRE会封装GRE头部，GRE成为封装协议，也叫运载协议，最后负责对封装后的报文进行转发的协议称为传输协议。

GRE封装

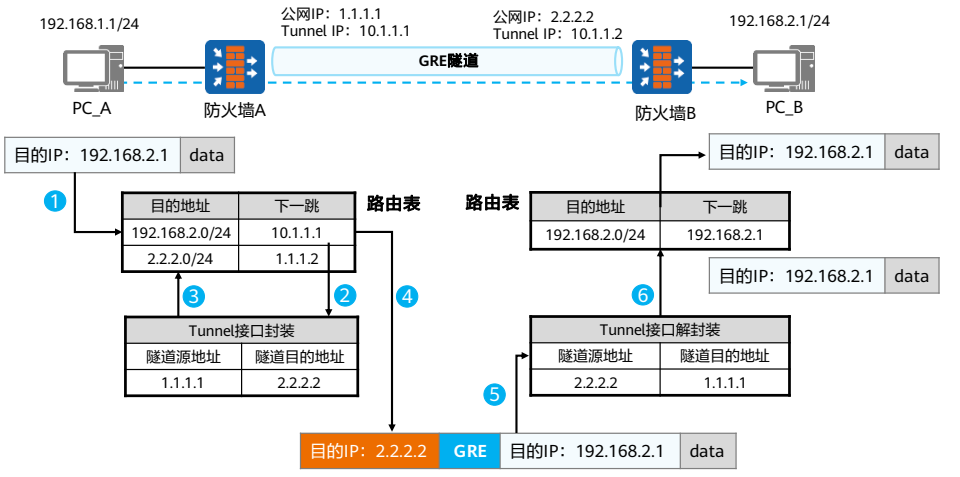
- GRE是按照协议栈对报文进行逐层封装。封装过程可以分成两步：
  - 第一步是为原始报文添加GRE头；
  - 第二步是在GRE头前面再加上新的IP头。
- GRE的封装操作是通过逻辑接口Tunnel完成的，Tunnel接口是一个通用的隧道接口，所以GRE协议在使用这个接口的时候，会将接口的封装协议设置为GRE协议。



HUAWEI

- GRE封装和解封装报文的过程如下：
  - 设备从连接私网的接口接收到报文后，检查报文头中的目的IP地址字段，在路由表查找出接口，如果发现出接口是隧道接口，则将报文发送给隧道模块进行处理；
  - 隧道模块接收到报文后首先根据乘客协议的类型和当前GRE隧道配置的校验参数，对报文进行GRE封装，即添加GRE报文头；
  - 然后，设备给报文添加传输协议报文头，即IP报文头。该IP报文头的源地址就是隧道源地址，目的地址就是隧道目的地址；
  - 最后，设备根据新添加的IP报文头目的地址，在路由表中查找相应的出接口，并发送报文。之后，封装后的报文将在公网中传输。
  - 接收端设备从连接公网的接口收到报文后，首先分析IP报文头，如果发现协议类型字段的值为47，表示协议为GRE，于是出接口将报文交给GRE模块处理。GRE模块去掉IP报文头和GRE报文头，并根据GRE报文头的协议类型字段，发现此报文的乘客协议为私网中运行的协议，于是将报文交给该协议处理。

GRE报文处理过程

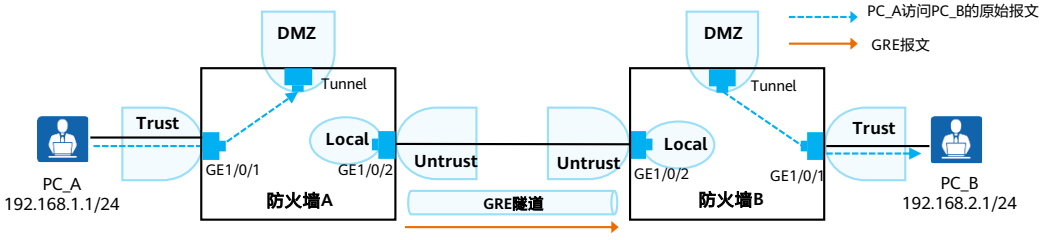


HUAWEI

- PC_A通过GRE隧道访问PC_B时，防火墙A和防火墙B上的报文转发过程如下：
  - PC_A访问PC_B的原始报文进入防火墙A后，首先匹配路由表；
  - 根据路由查找结果，防火墙A将报文送到Tunnel接口进行GRE封装，增加GRE头，外层加新IP头；
  - 防火墙A根据GRE报文的新IP头的目的地址（2.2.2.2），再次查找路由表；
  - 防火墙A根据路由查找结果将报文发送至防火墙B，图中假设防火墙A查找到的去往防火墙B的下一跳地址是1.1.1.2；
  - 防火墙B收到GRE报文后，首先判断这个报文是不是GRE报文。封装后的GRE报文会有个新的IP头，这个新的IP头中有个Protocol字段，字段中标识了内层协议类型，如果这个Protocol字段值是47，就表示这个报文是GRE报文。如果是GRE报文，防火墙B则将该报文送到Tunnel接口解封装，去掉新的IP头和GRE头，恢复为原始报文；如果不是，则报文按照普通报文进行处理；
  - 防火墙B根据原始报文的目的地址再次查找路由表，然后根据路由匹配结果将报文发送至PC_B。

GRE安全策略

- PC_A发出的原始报文进入Tunnel接口这个过程中，报文经过的安全域间是Trust > DMZ；原始报文被GRE封装后，防火墙A在转发这个报文时，报文经过的安全域间是Local > Untrust。
- 当报文到达防火墙B时，防火墙B会进行解封装。在此过程中，报文经过的安全域间是Untrust > Local；GRE报文被解封装后，防火墙B在转发原始报文时，报文经过的安全域间是DMZ > Trust。

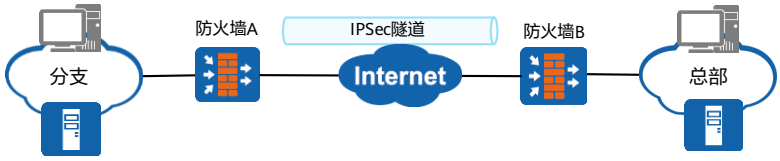


HUAWEI

目录

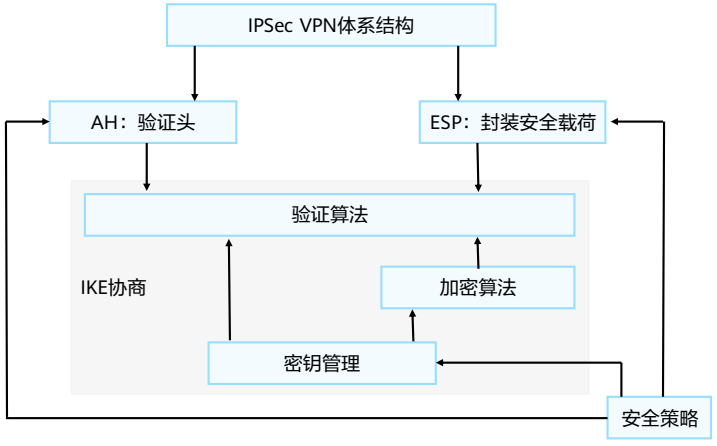
IPSec VPN简介

- IPSec（IP Security）协议族是IETF制定的一系列安全协议，它为端到端IP报文交互提供了基于密码学的、可互操作的、高质量的安全保护机制。IPSec VPN是利用IPSec隧道建立的网络层VPN。
- 对于L2TP VPN和GRE VPN，数据都是明文传输的，用户或企业的安全性得不到保证。若在网络中部署IPSec，便可对传输的数据进行保护处理，降低信息泄漏的风险。



- IPSec通过加密与验证等方式，从以下几个方面保障了用户业务数据在Internet中的安全传输：
  - 数据来源验证：接收方验证发送方身份是否合法；
  - 数据加密：发送方对数据进行加密，以密文的形式在Internet上传送，接收方对接收的加密数据进行解密后处理或直接转发；
  - 数据完整性：接收方对接收的数据进行验证，以判定报文是否被篡改；
  - 抗重放：接收方拒绝旧的或重复的数据包，防止恶意用户通过重复发送捕获到的数据包所进行的攻击。

IPSec VPN体系结构

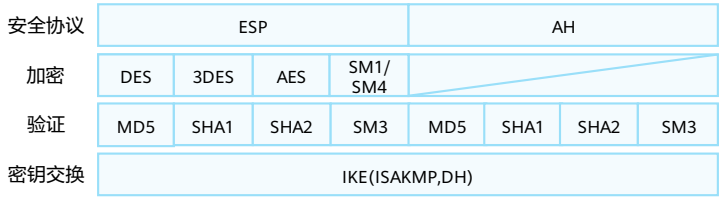


HUAWEI

- IPSec VPN体系结构主要由AH、ESP和IKE协议套件组成。IPSec通过ESP来保障IP数据传输过程的机密性，使用AH/ESP提供数据完整性、数据源验证和抗报文重放功能。ESP和AH定义了协议和载荷头的格式及所提供的服务，但却没有定义实现以上能力所需的具体转码方式，转码方式包括对数据转换方式，如算法、密钥长度等。为简化IPSec的使用和管理，IPSec还可以通过IKE进行自动协商交换密钥、建立和维护安全联盟的服务。具体介绍如下：
  - AH协议：AH是报文头验证协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放功能。然而，AH并不加密所保护的数据报；
  - ESP协议：ESP是封装安全载荷协议。它除提供AH协议的所有功能外（但其数据完整性校验不包括IP头），还可提供对IP报文的加密功能；
  - IKE协议：IKE协议用于自动协商AH和ESP所使用的密码算法。

IPSec协议体系

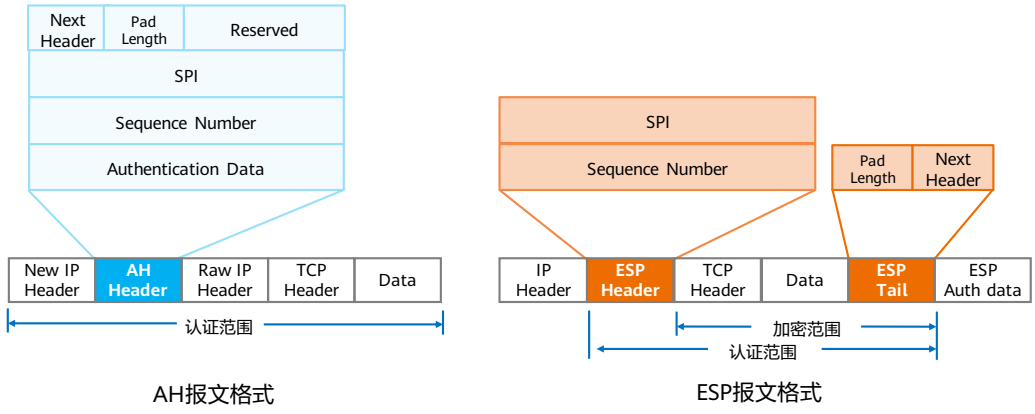
- IPSec通过验证头AH（Authentication Header）和封装安全载荷ESP（Encapsulating Security Payload）两个安全协议实现IP报文的安全保护。
  - AH是报文头验证协议，主要提供数据源验证、数据完整性验证和防报文重放功能，不提供加密功能；
  - ESP是封装安全载荷协议，主要提供加密、数据源验证、数据完整性验证和防报文重放功能。



HUAWEI

- AH和ESP协议提供的安全功能依赖于协议采用的验证、加密算法。
- IPSec加密和验证算法所使用的密钥可以手工配置，也可以通过因特网密钥交换IKE（Internet Key Exchange）协议动态协商。
- 本课程主要讲解手工方式的IPSec隧道建立。

AH和ESP报文格式对比



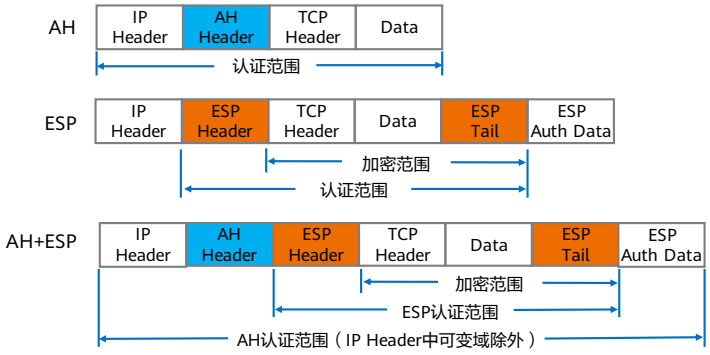
AH报文格式　　ESP报文格式

HUAWEI

- AH报文头字段含义如下：
  - Next Header（下一头部）：8比特，标识AH报文头后面的负载类型。传输模式下，是被保护的上层协议（TCP或UDP）或ESP协议的编号；隧道模式下，是IP协议或ESP协议的编号；
  - Pad Length（负载长度）：8比特，表示以32比特为单位的AH头部长度减2，缺省为4；
  - Reserved（保留字段）：16比特，保留将来使用，缺省为0；
  - SPI（安全参数索引）：32比特，用于唯一标识IPSec安全联盟；
  - Sequence Number（序列号）：32比特，是一个从1开始的单项递增的计数器，唯一地标识每一个数据包，用于防止重放攻击；
  - Authentication Data（认证数据）：一个变长字段，长度为32比特的整数倍，通常为96比特。该字段包含数据完整性校验值ICV（Integrity Check Value），用于接收方进行完整性校验。可选择的认证算法有MD5（Message Digest）、SHA-1（Secure Hash Algorithm）、SHA-2、SM3。前三个认证算法的安全性由低到高依次排列，安全性高的认证算法实现机制复杂，运算速度慢。SM3密码杂凑算法是中国国家密码管理局规定的IPSec协议规范。

封装模式 - 传输模式

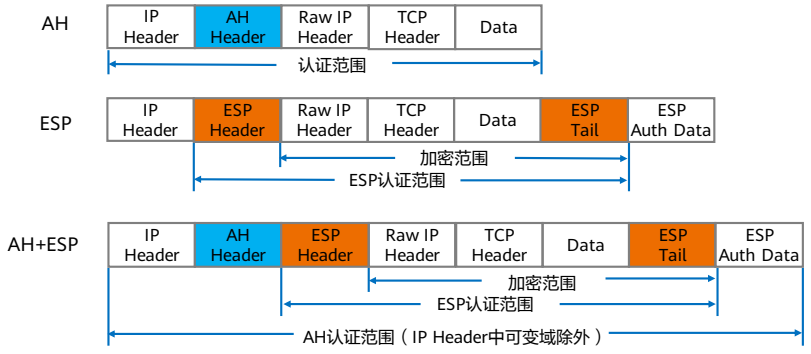
- 在传输模式中，AH头或ESP头被插入到IP头与传输层协议头之间，保护TCP/UDP/ICMP负载。以TCP报文为例，原始报文经过传输模式封装后，报文格式如图所示。



- 传输模式不改变报文头，故隧道的源和目的地址必须与IP报文头中的源和目的地址一致，所以只适合两台主机或一台主机和一台VPN网关之间通信。

封装模式 - 隧道模式

- 在隧道模式下，AH头或ESP头被插到原始IP头之前，另外生成一个新的报文头放到AH头或ESP头之前，保护IP头和负载。以TCP报文为例，原始报文经隧道模式封装后的报文结构如图所示。

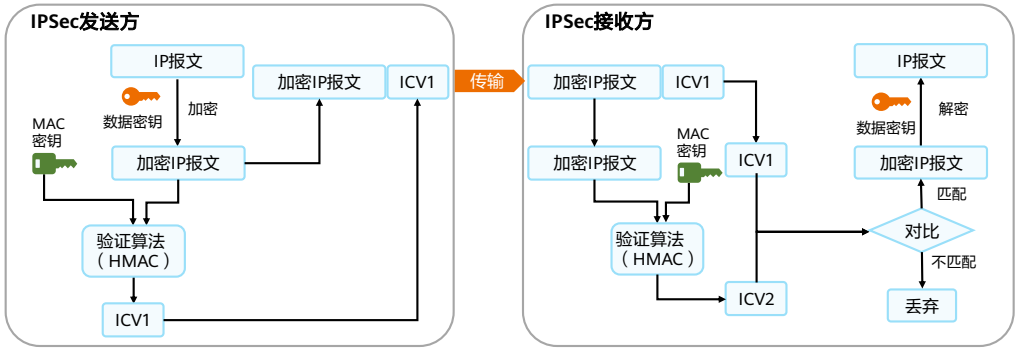


HUAWEI

- 隧道模式主要应用于两台VPN网关之间或一台主机与一台VPN网关之间的通信。
- 传输模式和隧道模式的区别在于：
  - 从安全性来讲，隧道模式优于传输模式，它可以完全地对原始IP数据报进行验证和加密，隐藏内部IP地址、协议类型和端口；
  - 从性能来讲，隧道模式因为有一个额外的IP头，所以它将比传输模式占用更多带宽。
- 当安全协议同时采用AH和ESP时，AH和ESP协议必须采用相同的封装模式。

IPSec数据加密及认证

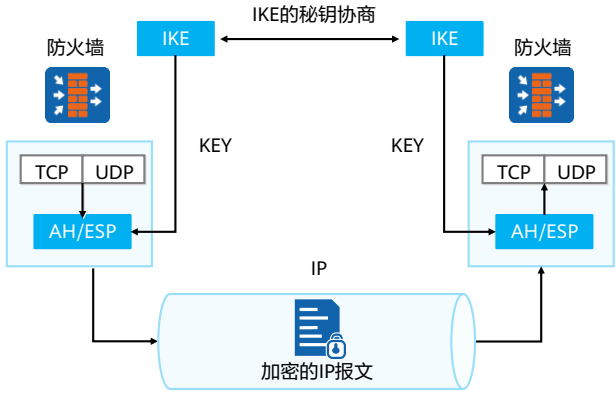
- IPSec提供了两种安全机制：加密和认证。
  - IPSec采用对称加密算法对数据进行加密和解密。数据发送方和接收方使用相同的密钥进行加密和解密；
  - IPSec采用HMAC（Hash-based Message Authentication Code）功能，比较数字签名进行数据完整性和真实性认证。



HUAWEI

- ICV(Integrity Check Value)用于接收方进行完整性校验。可选择的认证算法有MD5、SHA1、SHA2、SM3。
- MAC秘钥：Message Authentication Code秘钥，用于HMAC算法。
- IPSec常用的对称加密算法包括：数据加密标准DES（Data Encryption Standard）、3DES（Triple Data Encryption Standard）、先进加密标准AES（Advanced Encryption Standard）和国密算法（SM1和SM4）。其中，DES和3DES算法安全性低，存在安全风险，不推荐使用。
- IPSec常用的验证算法包括：消息摘要MD5（Message Digest 5）、安全散列算法SHA1（Secure Hash Algorithm 1）、SHA2和国密算法SM3（Senior Middle 3）。其中，MD5、SHA1算法安全性低，存在安全风险，不推荐使用。
- IPSec的加密功能，无法验证解密后的信息是否是原始发送的信息或完整。IPSec采用HMAC（Hash-based Message Authentication Code）功能，比较数字签名进行数据包完整性和真实性验证。通常情况下，加密和验证通常配合使用。如图所示，在IPSec发送方侧，加密后的报文通过验证算法和对称密钥生成完整性校验值ICV，将IP报文和完整性校验值ICV同时发给对端；在IPSec接收方侧，使用相同的验证算法和对称密钥对加密报文进行处理，同样得到完整性校验值ICV，然后比较完整性校验值ICV，进行数据完整性和真实性验证，验证不通过的报文直接丢弃，验证通过的报文再进行解密。

IKE与AH/ESP之间关系

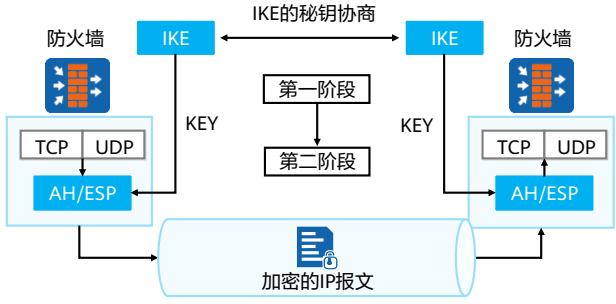


HUAWEI

- IKE是UDP之上的一个应用层协议，是IPSec的信令协议。IKE为IPSec协商生成密钥,供AH/ESP加解密和验证使用。AH协议和ESP协议有自己的协议号，分别是51和50。
- IKE协议有IKEv1和IKEv2两个版本。

IKE的交换阶段

- IKE使用了两个阶段为IPSec进行密钥协商并建立安全联盟。
  - 第一阶段：通信各方彼此间建立了一个已通过身份验证和安全保护的隧道，即IKE SA。协商模式包括主模式、野蛮模式。认证方式包括预共享密钥、数字签名方式、公钥加密；
  - 第二阶段：用在第一阶段建立的安全隧道为IPSec协商安全服务，建立IPSec SA。IPSec SA用于最终的IP数据安全传送。协商模式为快速模式。

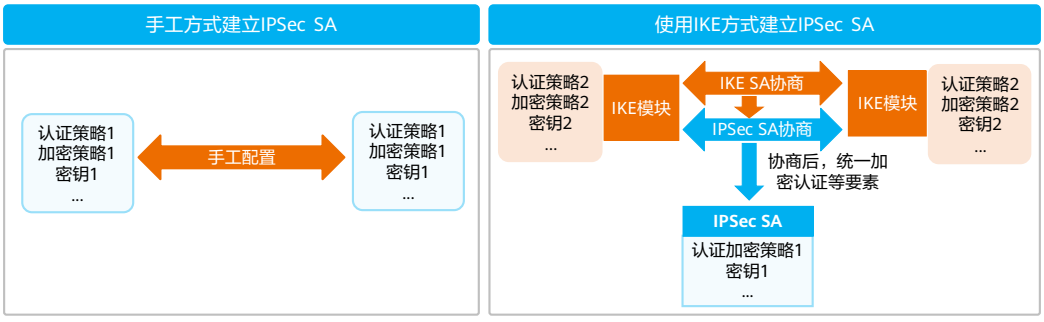


HUAWEI

- IKE使用了两个阶段的ISAKMP。第一阶段建立IKE安全联盟（IKE SA），第二阶段利用这个既定的安全联盟，为IPSec协商具体的安全联盟。
- 在RFC2409（The Internet Key Exchange）中规定，IKE 第一阶段的协商可以采用两种模式：主模式（Main Mode）和野蛮模式（Aggressive Mode）。这两种模式各自做着相同的事情：建立一个加密和验证无误的通信信道（IKE SA），以及生成验证过的密钥，为双方的IKE通信提供机密性、消息完整性以及消息源验证服务。IKE中定义的其他所有交换都要求一个验证过的IKE SA作为首要条件。所以无论主模式还是野蛮模式，第一阶段都必须在其他任何交换之前完成。
- IKE的工作流程如下：
  - 当一个报文从某接口外出时，如果此接口应用了IPSec，会进行安全策略的匹配；
  - 如果找到匹配的安全策略，会查找相应的安全联盟。如果安全联盟还没有建立，则触发IKE进行协商。IKE首先建立第一阶段的安全联盟，即IKE SA；
  - 在第一阶段安全联盟的保护下协商第二阶段的安全联盟，即IPSec SA；
  - 使用IPSec SA保护通讯数据。

IPSec SA

- IPSec安全传输数据的前提是在IPSec对等体（即运行IPSec协议的两个端点）之间成功建立安全联盟SA（Security Association）。SA可以帮助IPSec对特定要素进行约定，比如：加密算法使用DES，认证算法使用MD5，封装方式使用Tunnel等。
- 建立IPSec SA一般有两种方式：手工方式和IKE方式。

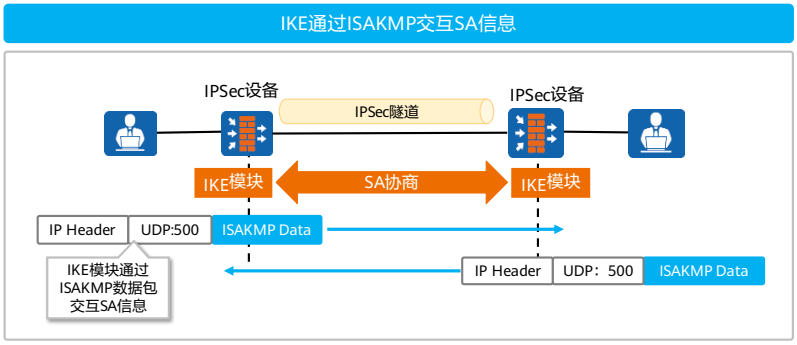


HUAWEI

- IPSec技术在数据加密，数据验证，数据封装等方面有多种实现方式或算法，两端的设备使用IPSec进行通信时需要保证一致的加密算法，验证算法等。因此需要一种机制帮助两端设备协商这些参数。
- 建立IPSec SA一般有两种方式：
  - 手工方式：手工方式建立IPSec SA管理成本很高，加密验证方式需要手工配置，手工刷新SA，且SA信息永久存在安全性较低，适用于小型网络；
  - IKE方式：IKE方式建立IPSec SA管理成本比较低，加密验证方式通过DH算法生成，SA信息有生成周期，且SA动态刷新，适用于小型，中大型网络。
- IPSec SA，由一个三元组来唯一标识，这个三元组包括安全参数索引SPI（Security Parameter Index）、目的IP地址和使用的安全协议号（AH或ESP）。
- IKE SA的主要作用是构建一条安全的通道，用于交互IPSec SA。

IKE SA

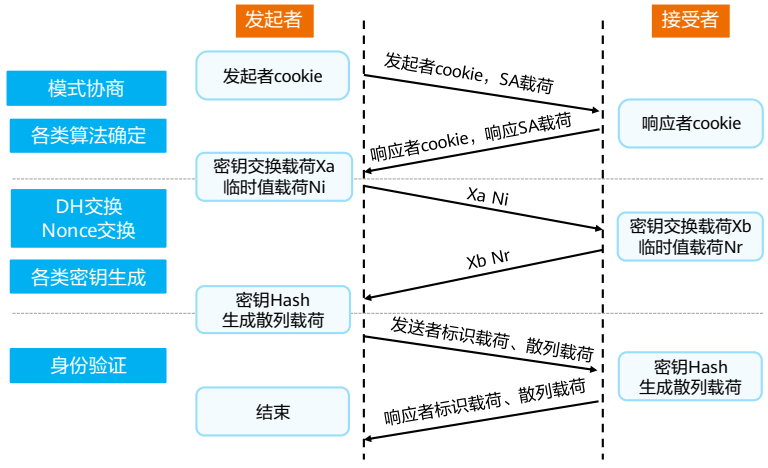
- 现网中交互对称密钥一般会使用密钥分发协议：IKE（Internet Key Exchange，因特网密钥交换）。
- IKE协议建立在ISAKMP（Internet安全联盟和密钥管理协议）定义的框架上，是基于UDP的应用层协议。它为IPSec提供了自动协商密钥、建立IPSec安全联盟的服务，能够简化IPSec的配置和维护工作。



HUAWEI

- IKE支持的认证算法有：MD5、SHA1、SHA2-256、SHA2-384、SHA2-512、SM3。
- IKE支持的加密算法有：DES、3DES、AES-128、AES-192、AES-256、SM1和SM4。
- ISAKMP由RFC2408定义，定义了协商、建立、修改和删除SA的过程和包格式。ISAKMP只是为SA的属性和协商、修改、删除SA的方法提供了一个通用的框架，并没有定义具体的SA格式。
- ISAKMP报文可以利用UDP或者TCP，端口都是500，一般情况下常用UDP协议。

IKEv1第一阶段协商 – 主模式预共享密钥协商过程



HUAWEI

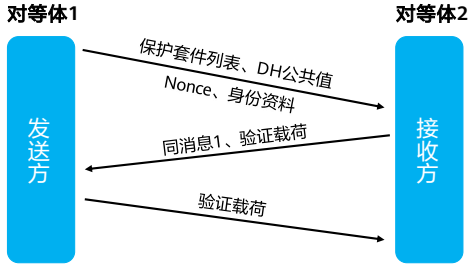
- IKE交换阶段第一阶段——主模式交换
  - 主模式被设计成将密钥交换信息与身份认证信息相分离的一种交换技术。这种分离保证了身份信息在传输过程中的安全性，这是因为交换的身份信息受到了加密保护；
  - 主模式总共需要经过三个步骤共6条消息来完成第一阶段的协商，最终建立IKE SA。这三个步骤分别是模式协商、Diffie-Hellman交换和nonce交换、以及对对方身份的验证；
  - 主模式的特点包括身份保护以及对ISAKMP协商能力的完全利用。其中，身份保护在对方希望隐藏自己的身份时显得尤为重要。在我们讨论野蛮模式时，协商能力的完全利用与否也会凸显出其重要性。若使用预共享密钥方法验证。在消息1、2发送之前，协商发起者和响应者必须计算产生自己的cookie，用于唯一标识每个单独的协商交换。cookie使用源/目的IP地址、随机数字、日期和时间进行MD5运算得出，并且放入消息1的ISAKMP中，用以标识单独的一个协商交换；
  - 在第一次交换中，需要交换双方的cookie和SA载荷，在SA载荷中携带需要协商的IKE SA的各项参数，主要包括IKE的散列类型、加密算法、认证算法和IKE SA的协商时间限制等；
  - 第一次交换后到第二次交换前，通信双方需要生成用于产生Diffie-Hellman共享密钥的DH值。生成方法是双方各自生成一个随机数字，通过DH算法对随机

数字进行运算，得出一个DH值Xa和Xb（Xa是发起方的DH值，Xb是响应者的DH值），然后双方再根据DH算法运算得出一个临时值Ni和Nr；

- 第二次交换中，双方交换各自的密钥交换载荷（即Diffie-Hellman交换）以及临时值载荷（即nonce交换）。其中密钥交换载荷包含了Xa和Xb，临时值交换包含了Ni和Nr；
- 双方交换了临时值载荷Ni和Nr之后，配合事先预置好的预共享密钥，再通过随机函数运算便可产生一个密钥SKEYID，这个密钥是后续所有密钥生成的基础。随后，通过自己算出来的DH值、交换得到的DH值以及SKEYID进行运算便可产生一个只有双方才知道的共享密钥SKEYID_d。此共享密钥并不进行传输，传输的只是是DH值以及临时值，因此即使第三方得到了这些材料也无法计算出共享密钥；
- 在第二次交换完成之后，双方所需的计算材料都已经交换完毕，此时，双方就可以将所有的密钥计算出来，并使用该密钥对随后的IKE消息提供安全保护。这些密钥包括：SKEYID_a以及SKEYID_e。SKEYID_a用来为IKE消息提供完整性以及数据源身份验证等安全服务；SKEYID_e则用于对IKE消息进行加密；
- 第三次交换是对标识载荷和散列载荷进行交换。标识载荷包含了发起者的标识信息、IP地址或主机名，散列载荷包含上一过程中产生的三组密钥进行Hash运算得出的值。这两个载荷通过SKEYID_e进行加密，如果双方的载荷相同，那么认证成功。IKE第一阶段主模式预共享密钥交换也就完成了。

IKEv1第一阶段协商 - 野蛮模式预共享密钥协商过程

- 野蛮模式一共需要交换3个消息：
  - 消息1交换SA载荷、密钥材料、和身份信息；
  - 消息2在交换消息1内容的同时增加了Hash认证载荷；
  - 消息3是响应方对发起方的认证。



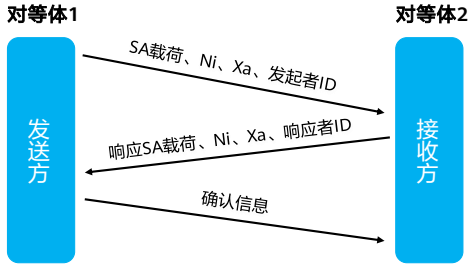
- IKE交换阶段第一阶段——野蛮模式交换
  - 从上述主模式协商的叙述中可以看到，在第二次交换之后便可生成会话密钥，会话密钥的生成材料中包含了预共享密钥。而当一个对等体同时与多个对等体进行协商SA时，则需要为每个对等体设置一个预共享密钥。为了对每个对等体正确地选择对应的预共享密钥，主模式需要根据前面交换信息中的IP地址来区分不同的对等体；
  - 但是当发起者的IP地址是动态分配获得时，由于发起者的IP地址不可能被响应者提前知道，而且双方都打算采用预共享密钥验证方法，此时响应者就无法根据IP地址选择对应的预共享密钥。野蛮模式就是被用于解决这个矛盾的；
  - 与主模式不同，野蛮模式仅用3条信息便完成了IKE SA的建立。由于对消息数进行了限制，野蛮模式同时也限制了它的协商能力，而且不会提供身份保护；
  - 在野蛮模式的协商过程中，发起者会提供一个保护套件列表、Diffie-Hellman公共值、nonce以及身份资料。所有这些信息都是随第一条信息进行交换的。作为响应者，则需要回应选择一个保护套件、Diffie-Hellman公共值、nonce、身份资料以及一个验证载荷。发起者将它的验证载荷在最后一条消息交换；
  - 野蛮模式由于在其第一条信息中就携带了身份信息，因此本身无法对身份信息进行加密保护，这就降低了协商的安全性，但也因此不依赖IP地址标识身份，在野蛮模式下也就有了更多灵活的应用。

IKEv1主模式和野蛮模式区别

- 交换的消息：
  - 主模式为6个，野蛮模式为3个。
- 身份保护：
  - 主模式的最后两条消息有加密，可以提供身份保护功能；而野蛮模式消息集成度过高，因此无身份保护功能。
- 对等体标识：
  - 主模式只能采用IP地址方式标识对等体；而野蛮模式可以采用IP地址方式或者Name方式标识对等体。

IKEv1第二阶段协商 - 快速模式协商过程

- 快速模式一共需要交换3个消息：
  - 消息1和消息2中，交换SA、KEY、Nonce和ID。用以协商算法、保证PFS以及提供“在场证据”；
  - 消息3是用于验证响应者是否可以通信，相当于确认信息。



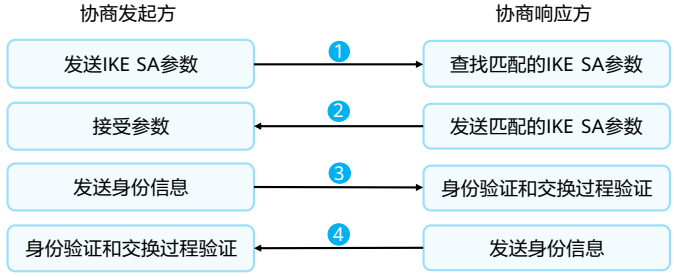
HUAWEI

- IKE交换阶段第二阶段——快速模式交换
  - 建立好IKE SA之后（无论通过主模式还是通过野蛮模式交换），便可用它为IPSec生成相应的SA。IPSec SA是通过快速模式交换来建立的，对快速模式交换来说，它是在已经建立好的IKE SA的保护下完成的；
  - 在一次快速交换模式中，通信双方需要协商拟定IPSec安全联盟的各项特征，并为其生成密钥。IKE SA保护快速模式交换的方法是：对其进行加密，并对消息进行验证。消息的验证是通过伪随机函数来进行的。来自IKE SA的SKEYID_a的值作为一个密钥，对快速模式交换的整个消息进行验证。这种验证除了能提供数据完整性保证之外，还能对数据源的身份进行验证。在消息接收到之后，我们知道它只有可能来自验证通过的实体，而且那条消息在传送过程并未发生改变。而通过加密（使用SKEYID_e），则可保障交换的机密性；
  - 快速模式需要从SKEYID_d状态中衍生出用于IPSec SA的密钥，这个密钥将在伪随机函数中使用，这样便可确保每个SA都有自己独一无二的密钥。每个SA都有一个不同的SPI，所以入方向SA的密钥也会与出方向SA不同。所有IPSec密钥都是根据相同的来源衍生的，所以相互间都有关联。假如一名攻击者能够根据IKE SA判断出SKEYID_d的值，那么就能非常容易地掌握自那个SKEYID_d衍生出来的IPSec SA的任何密钥。另外，还能继续掌握未来将要衍生的所有密钥，这显然是个大问题，所有这些密钥都不能保证所谓的“完美向前保密（PFS）”。快速模式为此专门提供了一个PFS选项，来满足这方面的需要，用户可根据自己地安全需要选择是否使用PFS；

- 为了在快速模式交换中实现PFS，需要执行一次额外的Diffie-Hellman交换，最终生成的共享密钥将在为IPSec生成密钥的过程中用到。显然，一旦交换完成，这个密钥便不复存在。一旦完成，它所驻留的那个内存位置必须清零和释放。从而保证了密钥之间地不相关性；
- 我们前面将快速模式描述成一种简单的请求 / 响应交换，但它的实际功用远不止于此。发起者可能需要一个“在场”证据，证明响应者在线，而且已经实际地处理了它的初始快速模式消息。为了达到这个要求，响应者需要在验证散列载荷中，加入交换的发起者nonce以及消息ID。这个摘要现在不仅能保障消息的完整性，也能为发起者提供源验证功能，另外还能提供在场证据；
- 响应者也需要一个在场证据，从发起者传来的可能是一条过期的消息，是由不怀好意的人重播的。这个人可能不知道消息的内容，但通过对通信的分析，能够知道它是一条快速模式消息。如果重播那条消息，响应者便不得不创建多余的SA。我们可将其想像成一种“服务否认”攻击，只是属于比较温和的那种，因为响应者会根据这条消息，增加不必要的内存及SA管理开销。想要防范此类攻击，需在快速模式交换中增加第三条消息。在这条消息中，发起者需要同时包括nonce和此次交换的消息ID，并把它们保存在一个验证散列载荷中。这样发起者便可向响应者证实：自己是此次交换的活动参与者；
- 在前两条消息中，发起者和响应者都发送了SA载荷，和主模式、野蛮模式一样，SA载荷是用来协商各种保护算法的。而Ni、Nr以及ID则是用来提供“在场证据”的。Xa以及Xb则是用来生成新的DH共享密钥，保证PFS的。Xa以及Xb将与IKE第一阶段生成的SKEYID_d、Ni、Nr以及SPI等信息共同生成最终用于IPSec加密的密钥；
- 最后发起者会发送一条确认信息，响应者收到该信息后就知道发起者已经收到了第二条消息。此时IKE第二阶段结束。

IKEv2协商 – 初始交换

- IKEv2定义了三种交换：初始交换（Initial Exchanges）、创建子SA交换（Create_Child_SA Exchange）以及通知交换（Informational Exchange）。
- 正常情况下，IKEv2通过初始交换就可以完成第一对IPSec SA的协商建立。IKEv2初始交换对应IKEv1的第一阶段，初始交换包含两次交换四条消息，如下图所示：



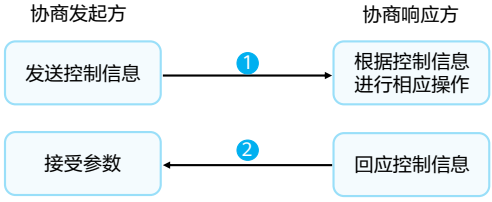
HUAWEI

- 采用IKEv2协商安全联盟比IKEv1协商过程要简化的多。要建立一对IPSec SA，IKEv1需要经历两个阶段：“主模式＋快速模式”或者“野蛮模式＋快速模式”，前者至少需要交换9条消息，后者也至少需要6条消息。而IKEv2正常情况使用2次交换共4条消息就可以完成一对IPSec SA的建立，如果要求建立的IPSec SA大于一对时，每一对IPSec SA只需额外增加1次创建子SA交换，也就是2条消息就可以完成。
- 初始交换过程：
  - 消息①和②属于第一次交换（称为IKE_SA_INIT交换），以明文方式完成IKE SA的参数协商，包括协商加密和验证算法、交换临时随机数和DH交换。IKE_SA_INIT交换后生成一个共享密钥材料，通过这个共享密钥材料可以衍生出IPSec SA的所有密钥；
  - 消息③和④属于第二次交换（称为IKE_AUTH交换），以加密方式完成身份认证、对前两条信息的认证和IPSec SA的参数协商。IKEv2支持RSA签名认证、预共享密钥认证以及扩展认证方法EAP（Extensible Authentication Protocol）。EAP认证是作为附加的IKE_AUTH交换在IKE中实现的，发起者通过在消息3中省去认证载荷来表明需要使用EAP认证。

- 创建子SA交换：
  - 当一个IKE SA需要创建多对IPSec SA时，需要使用创建子SA交换来协商多于一对的IPSec SA。另外，创建子SA交换还可以用于IKE SA的重协商；
  - 创建子SA交换包含一个交换两条消息，对应IKEv1协商阶段2，交换的发起者可以是初始交换的协商发起方，也可以是初始交换的协商响应方。创建子SA交换必须在初始交换完成后进行，交换消息由初始交换协商的密钥进行保护；
  - 类似于IKEv1，如果启用PFS，创建子SA交换需要额外进行一次DH交换，生成新的密钥材料。生成密钥材料后，子SA的所有密钥都从这个密钥材料衍生出来。

IKEv2协商 – 通知交换

- 运行IKE协商的两端有时会传递一些控制信息，例如错误信息或者通告信息，这些信息在IKEv2中是通过通知交换完成的，如图所示。
- 通知交换必须在IKE SA保护下进行，也就是说通知交换只能发生在初始交换之后。控制信息如果是IKE SA的，那么通知交换必须由该IKE SA来保护进行；控制信息如果是某子SA的，那么该通知交换必须由生成该子SA的IKE SA来保护进行。



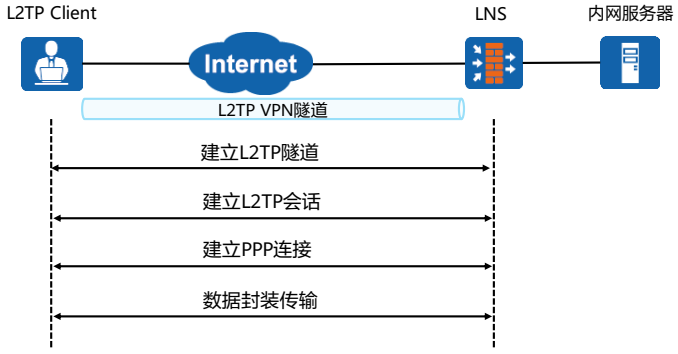
目录

L2TP VPN简介

- L2TP（Layer Two Tunneling Protocol）二层隧道协议是另一种常见VPN协议。
  - L2TP是虚拟私有拨号网VPDN（Virtual Private Dial-up Network）隧道协议的一种，它扩展了点到点协议PPP的应用，是一种在远程办公场景中为出差员工或企业分支远程访问企业内网资源提供接入服务的VPN。
- L2TP VPN主要有三种使用场景：
  - NAS-Initiated VPN：由远程拨号用户发起，远程系统通过PSTN/ISDN拨入LAC。由LAC通过Internet向LNS发起建立隧道连接请求，拨号用户地址则由LNS分配。对远程拨号用户的验证与计费既可由LAC侧的代理完成，也可在LNS完成；
  - Call-LNS：L2TP除了可以为出差员工提供远程接入服务以外，还可以进行企业分支与总部的内网互联，实现分支用户与总部用户的互访；
  - Client-Initialized：直接由LAC客户（指可在本地支持L2TP协议的用户）发起。客户需要知道LNS的IP地址。LAC客户可直接向LNS发起隧道连接请求，无需再经过一个单独的LAC设备。在LNS设备上收到了LAC客户的请求之后，根据用户名、密码进行验证，并且给LAC客户分配私有IP地址。

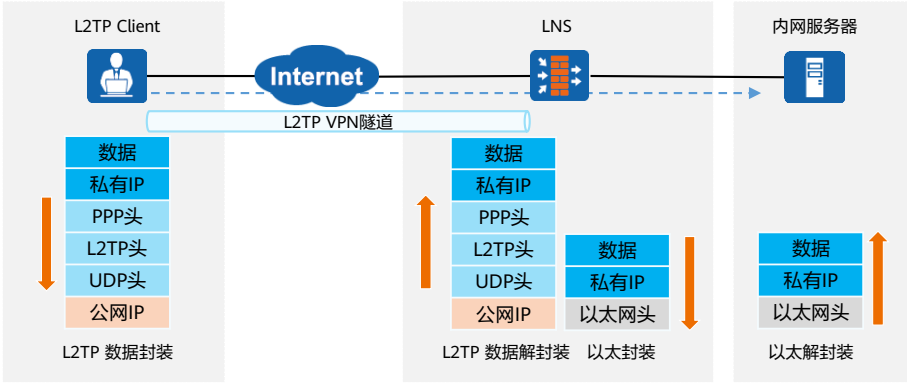
Client-Initiated场景中的L2TP VPN原理（1）

- 从隧道协商、报文封装、安全策略这3个方面介绍Client-Initiated场景中L2TP VPN的工作原理。
- 隧道协商：移动办公用户在访问企业总部服务器之前，需要先通过L2TP VPN软件与LNS建立L2TP VPN隧道。下图所示是移动办公用户与LNS协商建立L2TP VPN隧道，直至最后成功访问企业内网资源的完整过程。



Client-Initiated场景中的L2TP VPN原理（2）

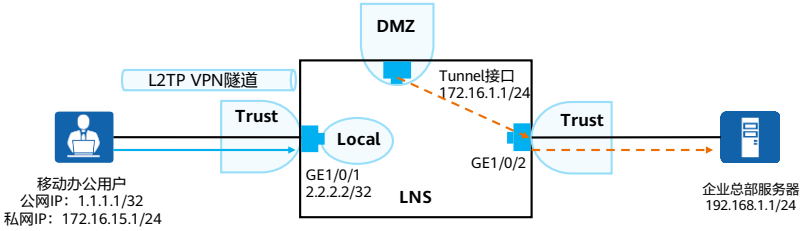
- 报文封装：报文的封装和解封装过程如图所示。



- L2TP Client发往内网服务器的报文的转发过程如下：
  - L2TP Client将原始报文用PPP头、L2TP头、UDP头、外层公网IP头层层封装，成为L2TP报文；
  - L2TP 报文穿过Internet到达LNS；
  - LNS收到报文后，在L2TP模块中完成了身份认证和报文的解封装，去掉PPP头、L2TP头、UDP头、外层公网IP头，还原成原始报文；
  - 原始报文只携带了内层私网IP头，内层私网IP头中的源地址是L2TP Client获取到的私网IP地址，目的地址是内网服务器的私网IP地址。LNS根据目的地址查找路由表，然后根据路由匹配结果转发报文。

Client-Initiated场景中的L2TP VPN原理（3）

- 安全策略：下图所示为LNS设备上报文所经过的安全域间，以及LNS的安全策略匹配条件。



业务方向	设备	源安全区域	目的安全区域	源地址	目的地址	应用
移动办公用户访问企业总部服务器	LNS	Untrust	Local	Any	2.2.2.2/32	L2TP
		DMZ	Trust	172.16.1.2/24～172.16.1.100/24（地址池地址）	192.168.1.0/24	/
企业总部服务器访问移动办公用户	LNS	Trust	DMZ	192.168.1.0/24	172.16.1.2～172.16.1.100/24（地址池地址）	/

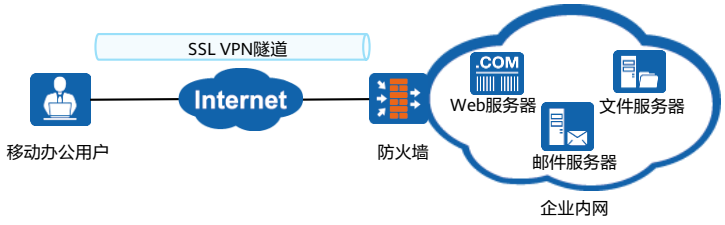
HUAWEI

- 移动办公用户访问企业总部服务器的过程中，经过LNS的流量分为以下2类，对应流量的安全策略处理原则如下。
  - 移动办公用户与LNS间的L2TP报文：此处的L2TP报文既包含移动办公用户与LNS建立隧道时的L2TP协商报文，也包含移动办公用户访问企业总部服务器被解封装前的业务报文，这些L2TP报文会经过Untrust > Local区域；
  - 移动办公用户访问企业总部内网服务器的业务报文：LNS通过VT接口将移动办公用户访问企业总部服务器的业务报文解封装以后，这些报文经过的安全域间为DMZ > Trust。DMZ区域为LNS上Tunnel接口所在的安全区域，Trust为LNS连接总部内网接口所在的安全区域。

目录

SSL VPN简介

- IPSec、L2TP等早期出现的VPN技术虽然可以支持远程接入这个应用场景，但这些VPN技术存在以下问题：
  - 移动办公用户需要安装指定的客户端软件；
  - 网络部署和维护都比较麻烦；
  - 无法对移动办公用户的访问权限做精细化控制。
- SSL VPN作为新型的轻量级远程接入方案，可以有效地解决上述问题。SSL VPN是通过SSL协议实现远程安全接入的VPN技术，保证移动办公用户能够在企业外部安全、高效地访问企业内部的网络资源。

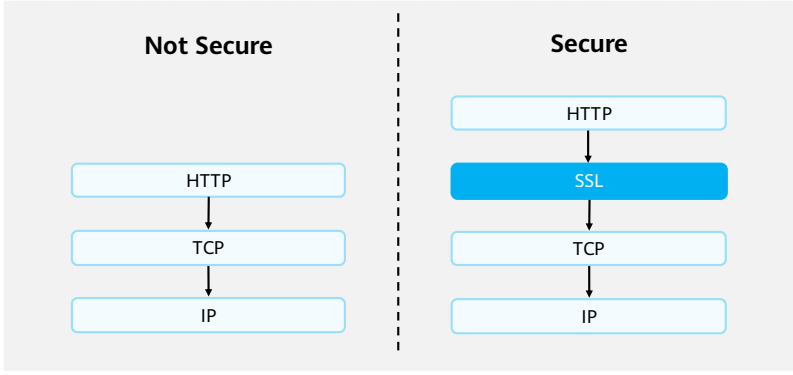


HUAWEI

- SSL VPN主要应用场景：企业出差员工，需要在外地远程办公，并期望能够通过Internet随时随地的远程访问企业内部资源。同时，企业为了保证内网资源的安全性，希望能对移动办公用户进行多种形式的身份认证，并对移动办公用户可访问内网资源的权限做精细化控制。
- 如上图所示，防火墙作为企业出口网关连接至Internet，并向移动办公用户（即出差员工）提供SSL VPN接入服务。移动办公用户使用终端（如便携机、PAD或智能手机）与防火墙建立SSL VPN隧道以后，就能通过SSL VPN隧道远程访问企业内网的Web服务器、文件服务器、邮件服务器等资源。

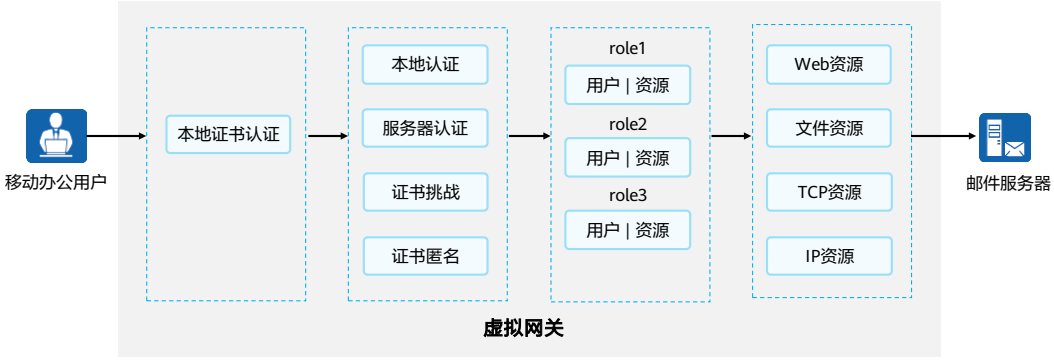
SSL VPN封装

- SSL封装位于传输层与各种应用层协议之间，为数据通讯提供安全支持，建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。



SSL VPN虚拟网关

- 防火墙通过虚拟网关向移动办公用户提供SSL VPN接入服务，虚拟网关是移动办公用户访问企业内网资源的统一入口。下图是移动办公用户登录SSL VPN虚拟网关并访问企业内网资源的总体流程。系统管理员在防火墙上创建SSL VPN虚拟网关，并通过虚拟网关对移动办公用户提供SSL VPN接入服务。

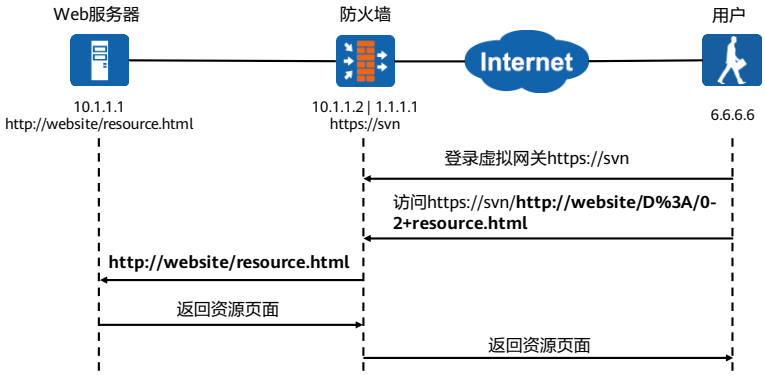


HUAWEI

- 移动办公用户登录SSL VPN虚拟网关并访问企业内网资源的过程如下：
  - 用户登录：移动办公用户在浏览器中输入SSL VPN虚拟网关的IP地址或域名，请求建立SSL连接。虚拟网关向远程用户发送自己的证书，远程用户对虚拟网关的证书进行身份认证。认证通过后，远程用户与虚拟网关成功建立SSL连接，进入SSL VPN虚拟网关的登录页面；
  - 用户认证：在登录页面输入用户名、密码后，虚拟网关将对该用户进行身份认证。虚拟网关验证用户身份的方式有很多种，包括本地认证、服务器认证、证书匿名认证、证书挑战认证等；
  - 角色授权：用户身份认证通过后，虚拟网关会查询该用户所属的角色信息，然后再将该角色所拥有的资源链接推送给用户。角色代表了一类用户的资源访问权限，例如企业中总经理这个角色的资源访问权限和普通员工这个角色的资源访问权限是不一样的；
  - 资源访问：用户点击虚拟网关资源列表中的链接就可以访问对应资源。

SSL VPN业务 – Web代理

- 移动办公用户访问内网Web资源时使用Web代理业务。
- Web代理按照实现方式的不同分为了Web改写和Web link两种。



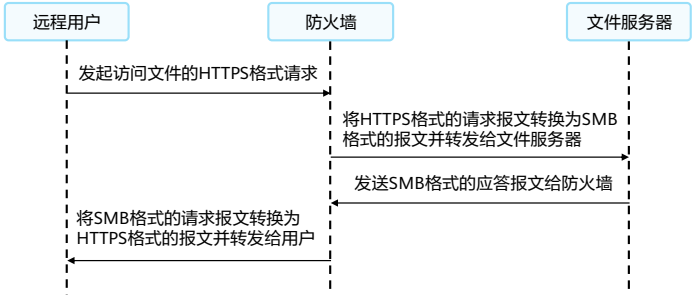
HUAWEI

- Web代理业务交互流程：
  - 远程用户通过域名（https://svn）来访问虚拟网关；
  - 登录虚拟网关成功后，远程用户会在虚拟网关中看到自己有权访问的Web资源列表，然后单击要访问的资源链接。防火墙在将内网资源（http://website/resource.html）呈现给远程用户时，会改写该资源的URL。远程用户点击资源链接后，发送给防火墙的HTTPS链接请求就是虚拟网关改写以后的URL，改写后的URL实质上是由https://svn和http://website/resource.html这两个URL拼接而成；
  - 防火墙收到上述URL后，会向Web Server重新发起一个HTTP请求，这个HTTP请求就是Web资源实际的URL（http://website/resource.html）；
  - Web Server以HTTP方式向防火墙返回资源页面；
  - 虚拟网关将Web Server返回的资源页面，再经过HTTPS方式转发给远程用户。
- Web改写：Web改写中的“改写”包含两层含义。第一层含义是加密，即远程用户在点击虚拟网关资源列表中的链接时，虚拟网关会将用户要访问的真实URL进行加密。第二层含义是适配。随着网络技术不断的发展，远程用户接入Internet的终端类型也变得丰富起来，如智能手机、PAD、便携机等越来越普及。这些不同的终端设备使用不同的操作系统和浏览器，这就使得它们在Web资源的支持上存在差异。为了解决终端类型差异对业务的影响，这就需要防火墙不仅能将内网Web资源转发给远程用户，而且还要对Web资源进行“改写”，使之能够适配这些不同的终端。

- Web link：Web Link不会进行加密和适配，只做单纯转发远程用户的Web资源请求。

SSL VPN业务 – 文件共享

- 远程用户访问内网文件服务器（如支持SMB协议的Windows系统、支持NFS协议的Linux系统）时使用文件共享业务。
- 远程用户直接通过Web浏览器就能在内网文件系统上创建和浏览目录，进行下载、上传、改名、删除等文件操作，就像对本机文件系统进行操作一样方便。

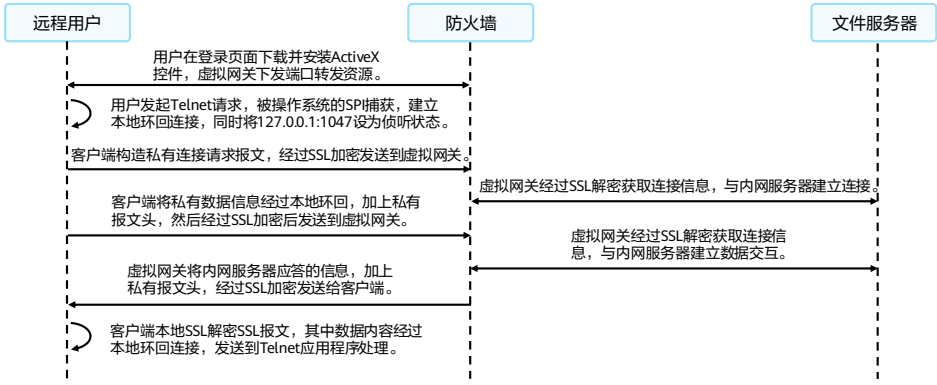


HUAWEI

- 在文件共享业务中防火墙起到了协议转换器的作用，以访问内网Windows文件服务器为例，具体实现过程如图所示。

SSL VPN业务 – 端口转发

- 远程用户访问内网TCP资源时使用端口转发业务。适用于TCP的应用服务包括Telnet、远程桌面、FTP、Email等。端口转发提供了一种端口级的安全访问内网资源的方式。

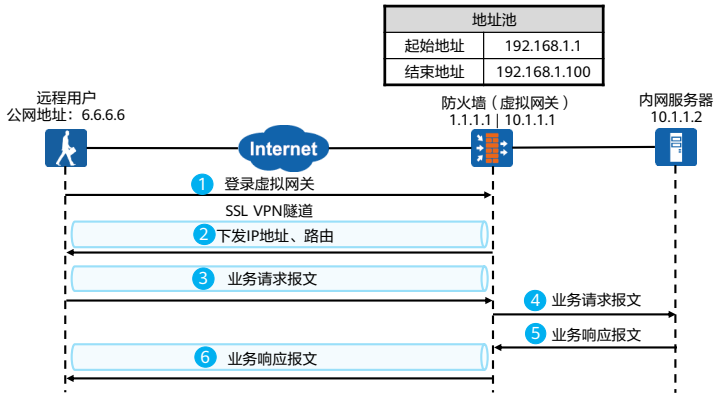


HUAWEI

- 端口转发需要在客户端上运行一个ActiveX控件作为端口转发器，用于侦听指定端口上的连接。以用户Telnet到内网服务器为例，端口转发的实现过程如图所示。

SSL VPN业务 – 网络扩展（1）

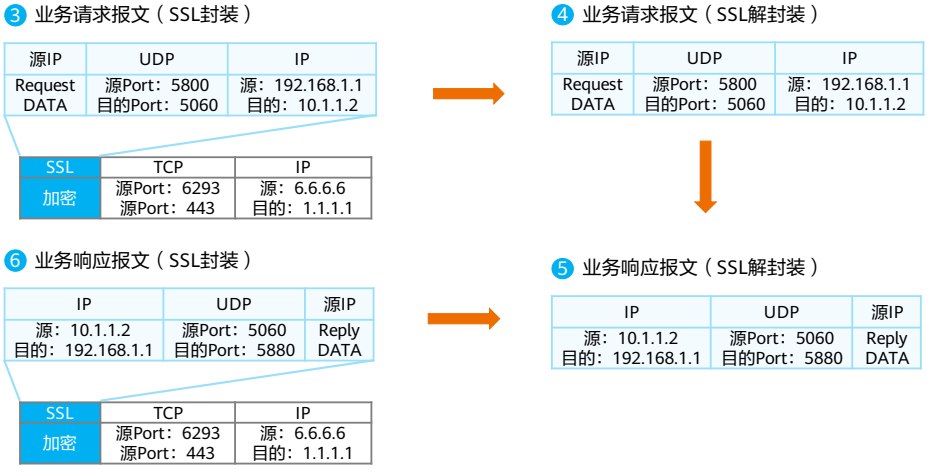
- 远程用户访问内网IP资源时使用网络扩展业务，Web资源、文件资源以及TCP资源都属于IP资源。
- 通常在不区分用户访问的资源类型时为对应用户开通网络扩展业务。



HUAWEI

- 远程用户通过Web浏览器登录虚拟网关。
- 成功登录虚拟网关后启动网络扩展功能。启动网络扩展功能，会触发以下几个动作：
  - 远程用户与虚拟网关之间会建立一条SSL VPN隧道；
  - 远程用户本地PC会自动生成一个虚拟网卡。虚拟网关从地址池中随机选择一个IP地址，分配给远程用户的虚拟网卡，该地址作为远程用户与企业内网Server之间通信之用。有了该私网IP地址，远程用户就如同企业内网用户一样可以方便访问内网IP资源；
  - 虚拟网关向远程用户下发到达企业内网服务器的路由信息。虚拟网关会根据网络扩展业务中的配置，向远程用户下发不同的路由信息。
- 远程用户向企业内网的服务器发送业务请求报文，该报文通过SSL VPN隧道到达虚拟网关。
- 虚拟网关收到报文后进行解封装，并将解封装后的业务请求报文发送给内网服务器。
- 内网服务器响应远程用户的业务请求。
- 响应报文到达虚拟网关后进入SSL VPN隧道。

SSL VPN业务 – 网络扩展 (2)



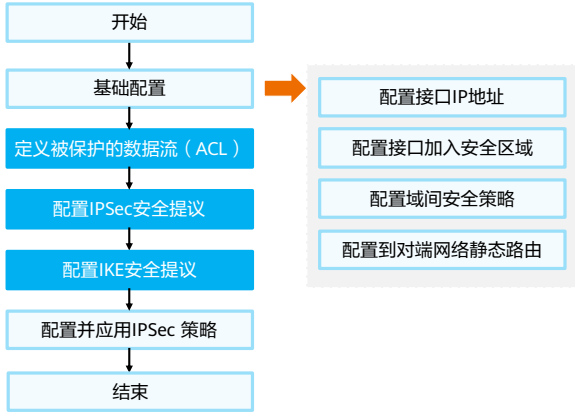
目录

IPSec VPN配置举例（1）

- 需求描述：
  - 两个网关之间通过IKE方式协商IPSec VPN隧道（采用预共享密钥认证），从而实现局域网之间安全地互访；
  - 网络A和网络B通过防火墙A和B之间建立的IPSec隧道互联互通；
  - 网络A属于10.1.1.0/24子网，通过接口GigabitEthernet 0/0/3与防火墙A连接；
  - 网络B属于10.1.2.0/24子网，通过接口GigabitEthernet 0/0/3与防火墙B连接；
  - 防火墙A和防火墙B路由可达。

IPSec VPN配置举例（2）

- 配置思路：
  - 完成接口基本配置；
  - 配置安全策略，允许私网指定网段进行报文交互；
  - 配置到对端内网的路由；
  - 配置IPSec策略，包括配置IPSec策略的基本信息、配置待加密的数据流、配置安全提议的协商参数。



IPSec VPN配置举例（3）

- 定义被保护的数据流。
  - 防火墙A：配置高级ACL 3000，允许10.1.1.0/24网段访问10.1.2.0/24网段。

```
[FW_A] acl 3000
[FW_A-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[FW_A-acl-adv-3000] quit
```

  - 防火墙B：配置高级ACL 3000，允许10.1.2.0/24网段访问10.1.1.0/24网段。

```
[FW_B] acl 3000
[FW_B-acl-adv-3000] rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[FW_B-acl-adv-3000] quit
```

IPSec VPN配置举例（4）

- 配置IPSec安全提议。（防火墙A与防火墙B配置相同，缺省参数可不配置）

```
[FW_A] IPSec proposal tran1
[FW_A-IPSec-proposal-tran1] esp authentication-algorithm sha2-256
[FW_A-IPSec-proposal-tran1] esp encryption-algorithm aes-256
[FW_A-IPSec-proposal-tran1] quit
```

- 配置IKE安全提议。（防火墙A与防火墙B配置相同）

```
[FW_A] ike proposal 10
[FW_A-ike-proposal-10] authentication-method pre-share
[FW_A-ike-proposal-10] prf hmac-sha2-256
[FW_A-ike-proposal-10] encryption-algorithm aes-256
[FW_A-ike-proposal-10] dh group14
[FW_A-ike-proposal-10] integrity-algorithm hmac-sha2-256
[FW_A-ike-proposal-10] quit
```

IPSec VPN配置举例（5）

- 配置IKE peer。

```
[FW_A] ike peer b
[FW_A-ike-peer-b] ike-proposal 10
[FW_A-ike-peer-b] remote-address 1.1.5.1
[FW_A-ike-peer-b] pre-shared-key Test!1234
[FW_A-ike-peer-b] quit
```

```
[FW_B] ike peer a
[FW_B-ike-peer-a] ike-proposal 10
[FW_B-ike-peer-a] remote-address 1.1.3.1
[FW_B-ike-peer-a] pre-shared-key Test!1234
[FW_B-ike-peer-a] quit
```

- 配置IPSec策略。

```
[FW_A] IPSec policy map1 10 isakmp
[FW_A-IPSec-policy-isakmp-map1-10] security acl 3000
[FW_A-IPSec-policy-isakmp-map1-10] proposal tran1
[FW_A-IPSec-policy-isakmp-map1-10] ike-peer b
[FW_A-IPSec-policy-isakmp-map1-10] quit
```

```
[FW_B] IPSec policy map1 10 isakmp
[FW_B-IPSec-policy-isakmp-map1-10] security acl 3000
[FW_B-IPSec-policy-isakmp-map1-10] proposal tran1
[FW_B-IPSec-policy-isakmp-map1-10] ike-peer a
[FW_B-IPSec-policy-isakmp-map1-10] quit
```

IPSec VPN配置举例（6）

- 引用IPSec策略。
  - 防火墙A：在接口GigabitEthernet 0/0/1上应用IPSec策略组map1。

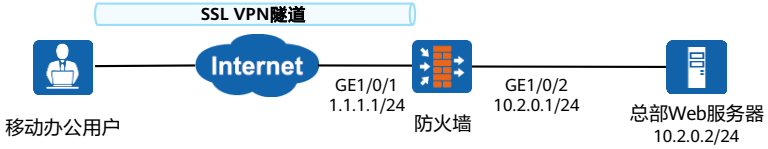
```
[FW_A] interface GigabitEthernet 0/0/1
[FW_A-GigabitEthernet0/0/1] IPSec policy map1
[FW_A-GigabitEthernet0/0/1] quit
```

  - 防火墙B：在接口GigabitEthernet 0/0/1上应用IPSec策略组map1。

```
[FW_B] interface GigabitEthernet 0/0/1
[FW_B-GigabitEthernet0/0/1] IPSec policy map1
[FW_B-GigabitEthernet0/0/1] quit
```

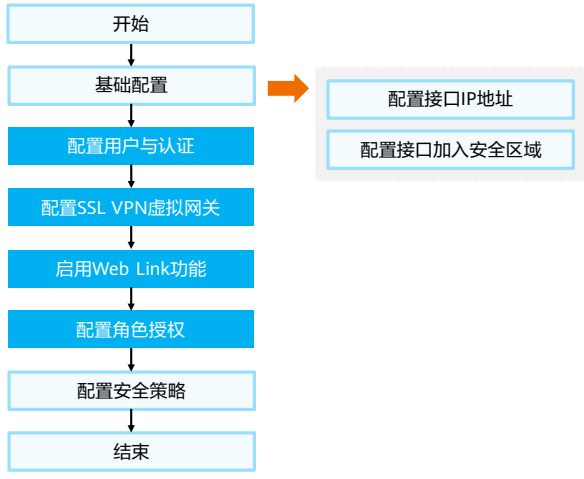
SSL VPN配置举例（1）

- 需求描述：
  - 企业网络如图所示，企业希望移动办公用户通过Web代理访问企业Web服务器（Web Link）；
  - 企业使用防火墙的本地认证对各部门的员工进行用户认证，通过认证的用户能够获得接入企业内部网络的权限。



SSL VPN配置举例（2）

- 配置思路：
  - 完成接口基本配置；
  - 配置用户和认证：配置认证域，创建用户组和用户；
  - 配置SSL VPN虚拟网关；
  - 配置Web Link功能：启用Web Link功能，配置Web Link资源；
  - 配置角色授权：将用户组添加到虚拟网关中，创建角色，将角色与用户组绑定，同时启用Web Link功能；
  - 配置安全策略，允许移动办公用户登录SSL VPN网关；允许出差员工访问Web代理资源。



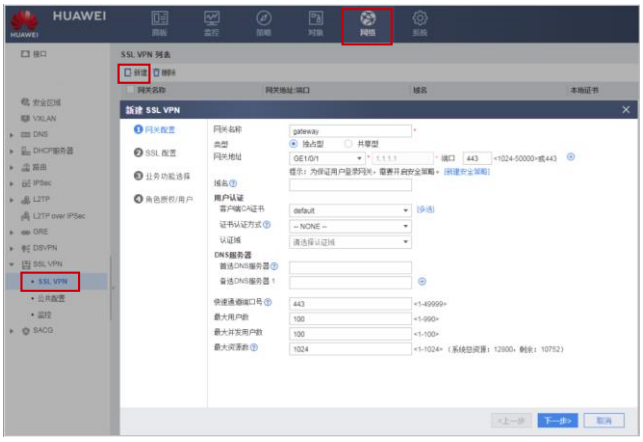
SSL VPN配置举例（3）

- 配置用户与认证。选择“对象 > 用户 > default”，按如下参数配置，然后单击“应用”。

- 用户user0001所属的用户组为“/default/group1”，认证类型为本地认证，密码为Password@123。需要注意，在新建用户user0001之前，应先新建用户组“/default/group1”，这样才能在新建用户时引用已创建好的用户组。
- 命令行配置如下：
  - [FW] aaa
  - [FW-aaa] domain default
  - [FW-aaa-domain-default] authentication-scheme default
  - [FW-aaa-domain-default] service-type ssl-vpn
  - [FW-aaa-domain-default] quit
  - [FW-aaa] quit
  - [FW] user-manage group /default/group1
  - [FW-usergroup-/default/group1] quit
  - [FW] user-manage user user0001 domain default
  - [FW-localuser-user0001] password Password@123
  - [FW-localuser-user0001] parent-group /default/group1
  - [FW-localuser-user0001] quit

SSL VPN配置举例（4）

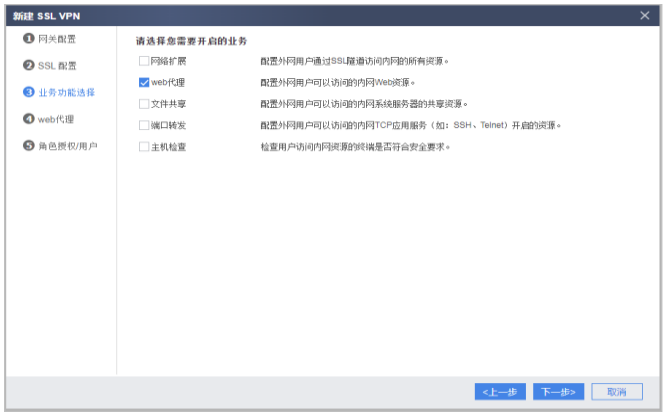
- 配置SSL VPN网关。选择“网络> SSL VPN > SSL VPN > 新建”，按如下参数配置。



- 命令行配置如下：
  - [FW] v-gateway gateway interface GigabitEthernet 0/0/1 private
  - [FW] v-gateway gateway udp-port 443
  - [FW] v-gateway gateway authentication-domain default

SSL VPN配置举例（5）

- 配置SSL协议的版本、加密套件、会话超时时间和生命周期。可直接使用默认值。选择“Web代理”业务，单击“下一步”。

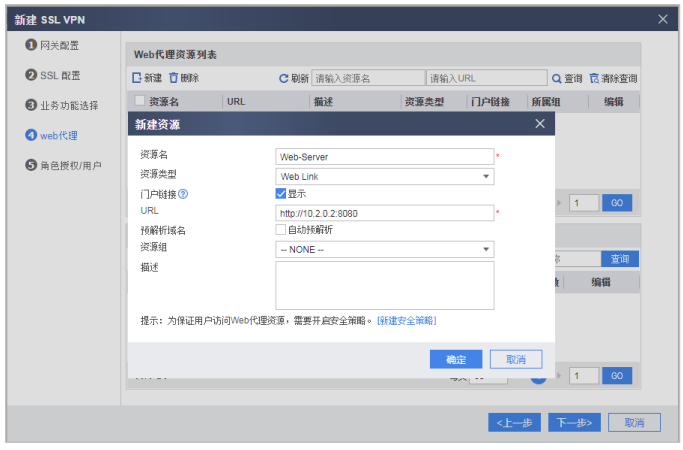


HUAWEI

- 命令行配置如下：
  - [FW] v-gateway gateway
  - [FW-gateway] service
  - [FW-gateway-service] web-proxy enable
  - [FW-gateway-service] web-proxy web-link enable

SSL VPN配置举例（6）

- 配置Web代理。选择“Web代理资源列表> 新建”，按如下配置新建Web代理资源。

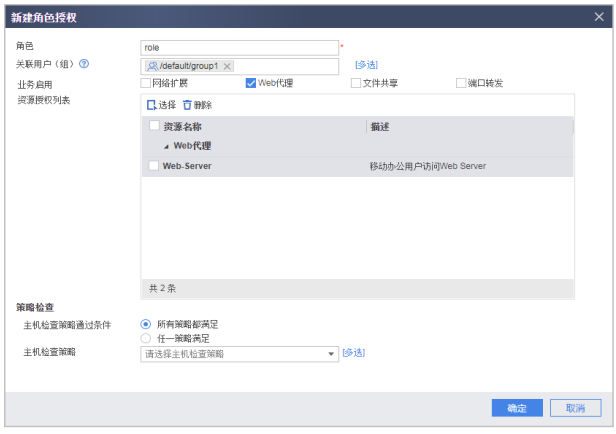


HUAWEI

- 命令行配置如下：
  - [FW-gateway-service] web-proxy link-resource Web-Server http://10.2.0.2:8080 show-link

SSL VPN配置举例（7）

- 配置SSL VPN的角色授权。选择“角色授权列表 > 新建”，按下图配置角色授权参数。



HUAWEI

- 命令行配置如下：
  - [FW-gateway] vpndb
  - [FW-gateway-vpndb] group /default/sslvpn
  - [FW-gateway-vpndb] quit
  - [FW-gateway] role
  - [FW-gateway-role] role role
  - [FW-gateway-role] role role group /default/sslvpn
  - [FW-gateway-role] role role web-proxy enable
  - [FW-gateway-role] role role web-proxy resource Web-Server
  - [FW-gateway-role] quit
  - [FW-gateway] quit

思考题

1. （判断题）IPSec采用的是非对称加密算法加密用户数据的方式来保证信息传递机密性的。（　　）

   A. 正确

   B. 错误

2. （多选题）以下哪些项属于防火墙SSL VPN的主要功能？（　　）

   A. 端口转发

   B. 网络扩展

   C. 文件共享

   D. Web代理

1. B
2. ABCD

本章总结

- 本课程简要介绍了不同加密技术的应用场景，系统介绍了VPN技术的产生背景、加解密的工作原理，以及不同VPN技术的配置方法和典型案例。
- 通过本课程的学习，搭配基于实际环境的练习，您将能独立完成IPSec VPN、SSL VPN等多种VPN技术的配置。

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

缩略语表（1）

缩略语	英文全称	解释
CHAP	Challenge Handshake Authentication Protocol	挑战握手认证协议
EAP	Extensible Authentication Protocol	可扩展的身份验证协议
EMS	Express Mail Service	邮政特快专递服务
ICV	Integrity Check Value	数据完整性校验值
IPv4	Internet Protocol Version 4	第四版因特网协议
IPv6	Internet Protocol Version 6	第六版因特网协议
IPX	Internetwork Packet Exchange Protocol	互联网分组交换协议
ISAKMP	Internet Security Association Key Management Protocol	因特网安全联盟和密钥管理协议
ISDN	Integrated Services Digital Network	综合业务数字网
L2F	Layer 2 Forwarding	二层转发协议

缩略语表 (2)

缩略语	英文全称	解释
LAC	L2TP Access Concentrator	L2TP访问集中器
LNS	L2TP Network Server	L2TP网络服务器
PAP	Password Authentication Protocol	密码认证协议
PFS	Perfect Forward Secrecy	完善的前向安全性
PPTP	Point-to-Point Tunneling Protocol	点到点隧道协议
PSTN	Public Switched Telephone Network	公共交换电话网络
SA	Security Association	安全联盟
SEND	Secure Neighbor Discovery	路由器授权功能
SPI	Security Parameter Index	安全参数索引

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI