网络安全认证概述

HUAWEI

前言

- 在学习HCIP-Security课程之前，我们需要了解课程的定位以及课程的大纲。
- 工信部发布了关于安全岗位的《网络安全产业人才岗位能力要求》，对网络安全工程师的种类和职责进行了统一规范。对标《网络安全产业人才岗位能力要求》，HCIP-Security认证主要面向安全实施工程师与安全运维工程师。
- 本章节我们将学习网络安全工程师的种类和职责、安全实施工程师与安全运维工程师的能力模型以及HCIP-Security的课程大纲。

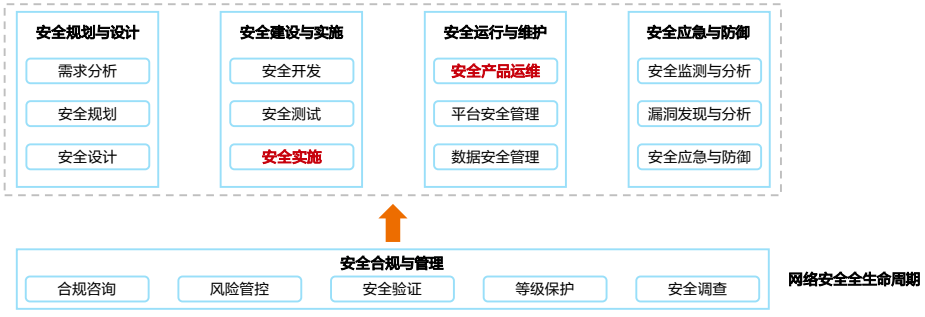
目标

- 学完本课程后，您将能够：
  - 描述网络安全工程师的岗位分类与职责
  - 描述安全实施工程师的能力模型
  - 描述安全运维工程师的能力模型
  - 了解HCIP-Security的课程大纲

目录

网络安全主要方向及岗位

- 网络安全工程师通过在规划与设计、建设与实施、运行与维护、应急与防御等各个阶段采用安全技术、产品和服务，并进行全生命周期的安全合规和管理，以保障信息、信息系统、信息基础设施和网络不因无意的、偶然的或恶意的原因而遭受到破坏、更改、泄露、泛用，以确保其保密性、完整性、可用性。
- 下图为网络安全全生命周期及网络安全工程师对应的岗位方向：



HUAWEI

- 本课程主要面向安全实施工程师与安全运维工程师。
- 该章节根据工信部发布的《网络安全产业人才岗位能力要求》撰写。
- 根据网络安全生命周期保障体系，网络安全产业大致将主要岗位分为5个方向：安全规划与设计、安全建设与实施、安全运行与维护、安全应急与防御、安全合规与管理。
  - 安全规划与设计是整个网络安全生命周期的基础环节，是指根据产品和业务安全需求，从整体上规划和设计网络系统的安全保障体系。主要包括：安全需求分析、安全战略规划及安全架构设计等。
  - 安全建设与实施是整个网络安全生命周期的关键环节，主要是指根据安全需求进行安全开发、测试和实施。主要包括：安全产品开发、安全基础测试和安全现场实施等。
  - 安全运行与维护是整个网络安全生命周期的重要环节，是指在信息、信息系统、信息基础设施和网络交付使用以后，以安全框架为基础、以安全策略为指导，依托成熟的运维管理体系，配备安全运维人员和工具，以有效和高效的技术手段，对保障信息、信息系统、信息基础设施和网络进行运行监测和安全维护，以确保其安全。主要包括：安全产品运维、平台安全管理和数据安全管理等。

- 安全应急与防御是整个网络安全生命周期的重要保障，是指通过安全监测、漏洞分析、防御技术等，识别、分析、处置信息、信息系统、信息基础设施和网络存在的安全威胁，收集网络安全情报， 并进行安全分析，主动通过渗透攻击和攻防演练等方式评估安全防御措施的有效性，持续完善安全防御措施，并在安全事件发生时快速完成应急响应。主要包括：安全监测与分析、漏洞发现与分析、安全防御和应急响应等。
- 安全合规与管理贯穿整个网络安全生命周期，是指依据相关法律法规、标准要求，结合实际安全需求，提供安全合规咨询，进行风险分析，提供解决方案，进行合规监管、风险管控及安全评估。主要包括：安全合规咨询、风险管控、安全评估、网络安全等级保护和网络安全调查等。

网络安全产业人才岗位能力要素

- 在介绍安全实施工程师与安全运维工程师能力模型前，我们需要了解安全岗位人才标准的能力要素。
- 网络安全产业人才岗位在综合能力、专业知识、技术技能和工程实践四个方面提出了能力要求。

综合能力	专业知识	技术技能	工程实践
• 相应岗位人才为完成工作任务所应具备的行为特征和综合素质，包括学习追踪、沟通协调、需求与趋势分析、熟悉业务场景等技能。	• 相应岗位人才为完成工作任务所必备的知识，主要为基本理论、相关标准规范、有关法律法规，以及与具体岗位要求相适应的理论知识、技术要求和操作规程等。	• 相应岗位人才为完成工作任务所应具备的对专业知识应用的水平以及对专业工具使用的掌握。	• 相应岗位人才在实际工程与项目推进中应当具备的经验。

- 本课程将聚焦于专业知识、技术技能的培养。

安全实施工程师能力模型

- 安全实施工程师与安全运维工程师主要工作在安全运行与维护阶段。
- 安全实施工程师主要负责安全实施方案中的规划与设计、工程实施，以及验收方案、培训方案、交付文档的制定与编写。安全实施工程师对专业知识与技术技能的要求如下：

专业知识

- 掌握现行网络安全服务相关标准内容；
- 熟悉网络安全服务体系中安全攻防、渗透测试、安全咨询、代码审计、应急响应等的技术规范与实施流程；
- 掌握安全服务规则与建设，针对复杂的业务环境提供集成的、先进的安全解决方案；
- 熟悉网络安全服务相关基础知识，熟悉主流安全厂家设备产品的原理、部署和安全评估方法。

技术技能

- 掌握如端口、漏洞分析检测、权限管理、入侵和攻击分析追踪、网站渗透、病毒木马防范等技能；
- 熟悉网络安全设备配置；
- 操作系统的基本命令/工具、常规服务等；
- 熟悉系统及应用安全防护，熟悉漏洞扫描工作原理，熟悉网络安全技术；
- 熟悉网络基本原理，熟悉TCP/IP协议，理解TCP/IP、HTTP、FTP、SNMP等常用协议，熟悉交换机、路由器日常维护操作。

- 根据正文所述，专业知识与技术技能主要在如下方面对实施工程师提出要求：
  - 安全标准：如ISO27001、等级保护制度等，可参考HCIA-Security认证；
  - 安全建设规则与解决方案：实施工程师需要充分了解安全方案的实施细节；
  - 网络原理与网络安全设备配置：网络安全设备部署与功能配置为实施工程师需要具备的基本素质，也是HCIA/HCIP-Security重点讲解部分；
  - 系统与应用安全：业务承载在服务器与操作系统上，系统与应用安全是安全实施的重点考虑部分；
  - 安全攻防、应急响应等技术与流程：安全方案部署时需要考虑日常运维的可行性。

安全运维工程师能力模型

- 安全运维工程师负责对服务器、网络设备、安全产品、网络信息系统等进行安全维护、安全巡检、策略维护管理、配置变更、故障处置与安全分析等，消除所发现的威胁，降低企业的安全风险。
- 安全运维工程师对专业知识与技术技能的要求如下：

专业知识

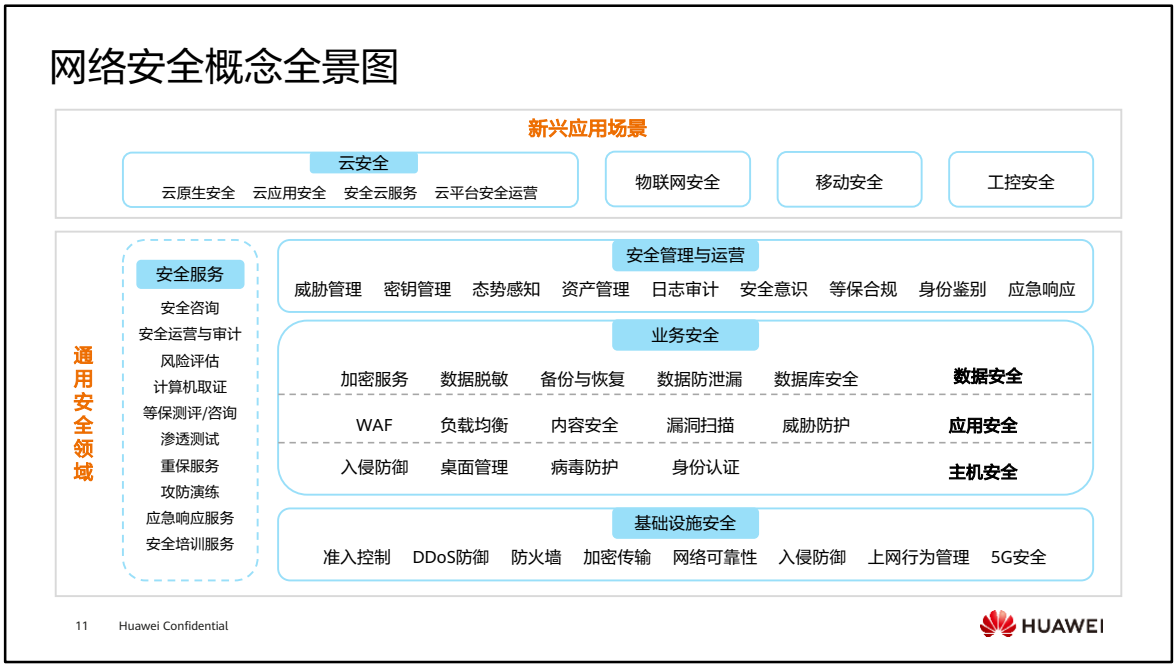
- 掌握安全运维相关技术指南及标准规范；
- 掌握常见操作系统及网络设备的操作命令；
- 熟悉常见安全漏洞的攻击原理；
- 熟悉安全运维的安全监控、安全研判、风险处置、应急响应等的流程及方法。

技术技能

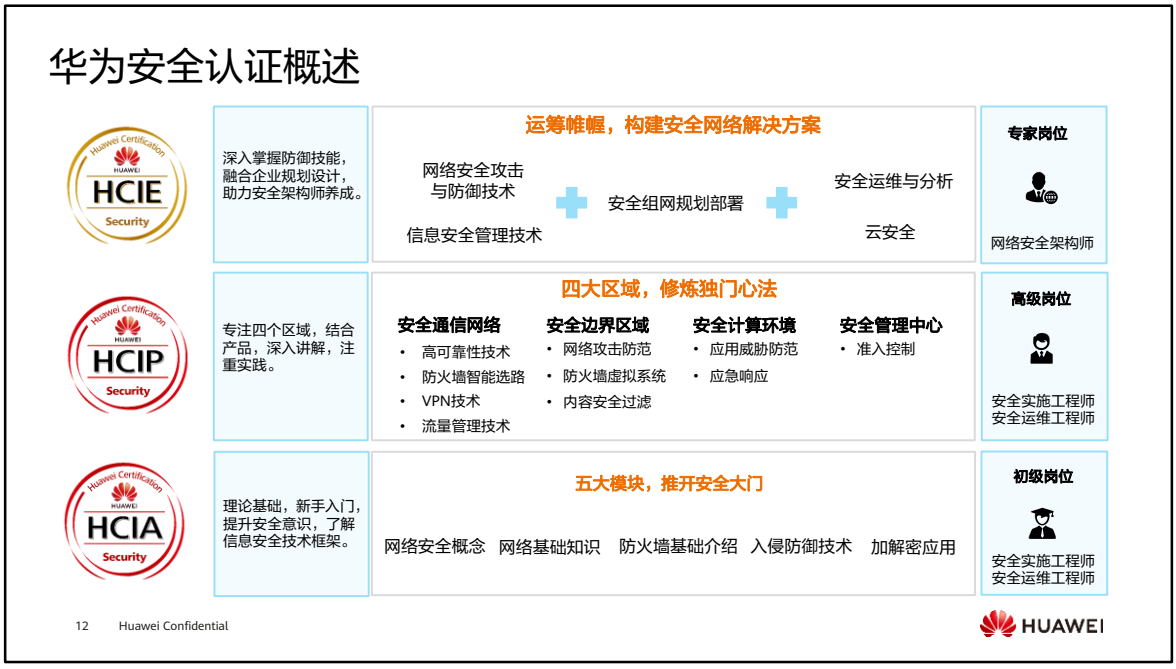
- 掌握常见网络安全产品，如防火墙、IDS/IPS、日志审计等的运维操作；
- 掌握TCP/IP网络协议等网络运行协议；
- 掌握常见应用程序和操作系统安全漏洞，如SQL注入、XSS、提权漏洞等的检测与防护原理，并修复；
- 熟练操作linux、windows操作系统与Oracle、MySQL等数据库语言的使用；
- 熟悉常用网络监控方法。

- 安全运维工程师与安全实施工程师在专业知识和技术技能上的要求范围大致相同。安全实施工程师侧重安全方案、安全设备与功能的部署，运维工程师则在故障排除、威胁识别与应急响应上能力要求更高。
- 对标网络实施工程师与网络运维工程师的专业知识与技术技能要求，安全认证聚焦于网络安全方案规划与设计、实施与建设、运维与优化。

目录



- 上图呈现了常见网络安全概念，以通用安全领域和新兴应用场景展开：
  - 通用安全领域：任何一个网络都会涉及到的安全技术领域，通常会包含基础设施安全、业务安全和安全管理与运营，有时会涉及安全服务。
    - 基础设施安全：通过采用安全设备及其上的功能来保障整体网络的安全性，包括对内网业务的保护和对网络架构及设施本身的保护。
    - 业务安全：保障业务及其承载设备的安全性，包括对主机的保护，主机上的应用保护以及后台数据的保护。
    - 安全管理与运营：任何网络都需要安全管理，包括行政管理制度和技术管理方法，如安全意识的培养、安全态势的感知。
    - 安全服务：安全服务商向企业提供安全服务，比如风险评估、攻防演练等。
  - 新兴应用场景：基于通用安全领域技术，根据业务的独特性，增加特性保护，比如云安全场景，在通用安全领域技术的基础上，还需要保护云应用的安全等。
- 本课程聚焦网络安全实施工程师与运维工程师，着重介绍基础设施安全，对业务安全、安全管理与运营也有部分涉及。



- HCIA-Security认证聚焦安全实施工程师与安全运维工程师，适用于学生、新员工等即将从事相关领域的从业工作者或爱好者。通过该认证后，证明考生已掌握中小型网络信息安全基础知识与相关技术（华为防火墙技术、加解密技术、PKI证书体系等），具备搭建中小型企业信息安全网络的能力，实现中小企业网络和应用的安全保障。
- HCIP-Security认证聚焦安全实施工程师与安全运维工程师。通过该认证后，证明考生已掌握华为网络安全技术（包括网络架构安全、边界安全、应用安全、终端安全等），具备大中型企业网络安全的架构设计、部署和运维能力，能够识别风险并及时响应，保障企业信息资产安全。
- HCIE-Security认证聚焦网络安全架构师，培养与认证具备企业信息安全解决方案整体的设计、部署和运维综合能力的安全专家。通用该认证后，证明考生已掌握最新安全体系架构和安全标准最佳实践，具备大中型企业信息安全解决方案整体的设计、部署和运维等综合能力，满足企业不断发展的网络安全需求，应对日益多样的网络安全挑战。

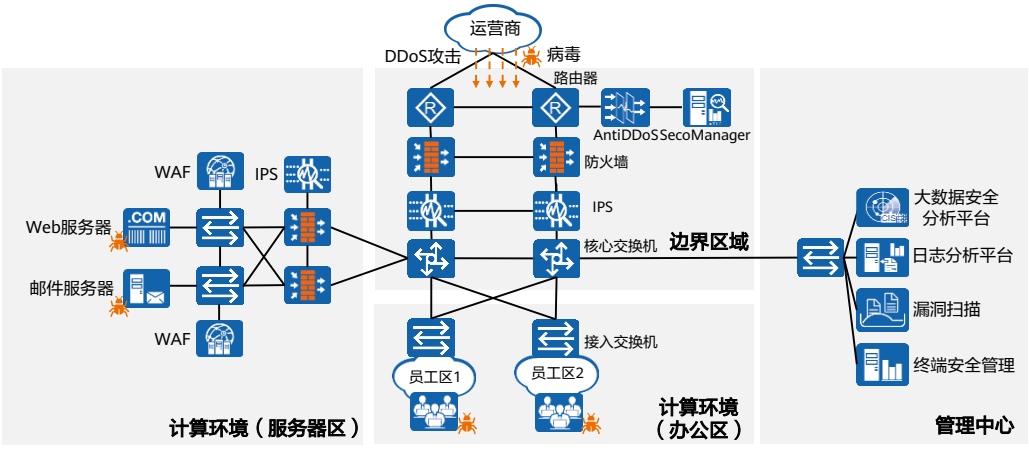
目录

HCIP-Security课程架构

- 《网络安全等级保护基本要求》中将安全通用要求细分为技术要求和管理要求。其中技术要求包括“安全物理环境”、“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心”；管理要求包括“安全管理制度”、“安全管理机构”、“安全管理人员”、“安全建设管理”和“安全运维管理”。
- 本课程首先通过《网络安全认证概述》阐述HCIP-Security的定位与课程框架。
- 在具体课程内容上，又将华为网络安全解决方案的高阶知识点分为安全通信网络、安全区域边界、安全计算环境和安全管理中心四个方面。结合HCIA-Security的初级知识点，完整地呈现华为网络安全解决方案的具体技术细节。
- 最后，通过华为网络安全具体案例，系统地讲解安全实施工程师如何部署安全方案，以及安全运维工程师如何进行日常运维。

企业网络安全威胁概览

- 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：

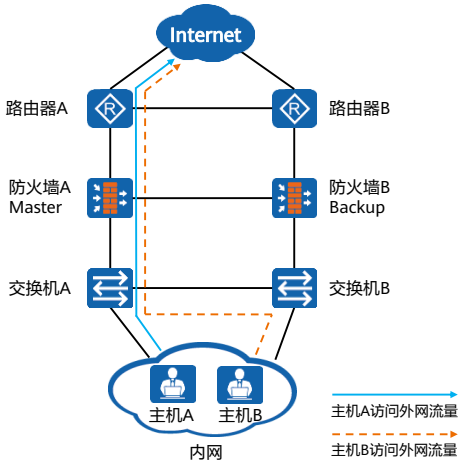


HUAWEI

- 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，Web漏洞攻击等；
  - 内部威胁：网络结构不可靠，网络未隔离，终端漏洞，员工行为不受控，信息安全违规操作，信息泄露，权限管理混乱，非法接入等。
- 安全威胁层出不穷，意味着将对企业提出越来越多的安全挑战，企业安全需求也随之增长。

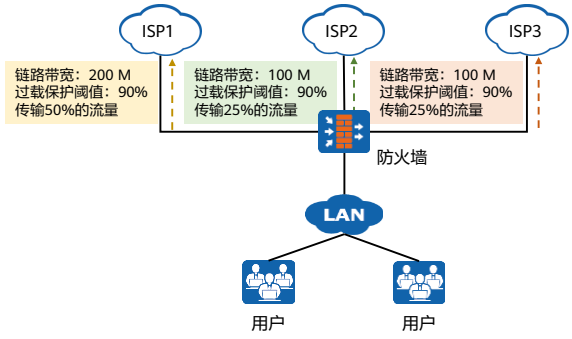
通信网络安全需求 - 设备冗余

- 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。包括且不限于路由器、交换机等转发设备，也包括防火墙、IPS和AntiDDoS等安全设备。
- 安全认证以防火墙高可靠性为例，在HCIA-Security课程中，详细介绍了防火墙双机热备的运行原理与业务转发机制，HCIP-Security课程将继续介绍更多防火墙双机热备的组网与常规运维操作。



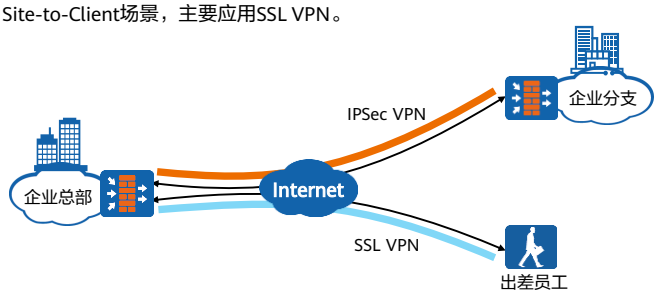
通信网络安全需求 - 线路冗余

- 大中型企业通常具备多条出口线路，而防火墙也是常见的网络出口设备。出口设备通常根据路由选择最优路径或根据等价路由中随机选择一条链路转发流量。然而不同的链路，存在质量、带宽、开销等区别，企业需要根据自身需求动态选择最优路径，或将流量按照不同比例合理地分配到各条链路上，提高链路资源的利用率和用户体验。



通信网络安全需求 - 加密传输

- 保障企业信息在传输过程中不被窃取，主要有两种方式，一种是专线传输，一种是VPN加密传输。专线传输适用于不同机构之间通信，且成本较高，故现网中VPN加密传输的使用较为常见。
  - Site-to-Site场景，主要应用IPSec VPN；
  - Site-to-Client场景，主要应用SSL VPN。

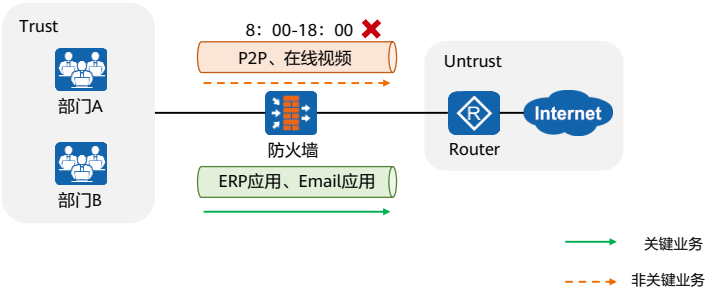


IPSec VPN可以对数据进行加密，确保传输安全。

SSL VPN在保障数据保密性的同时，能够验证用户的身份。

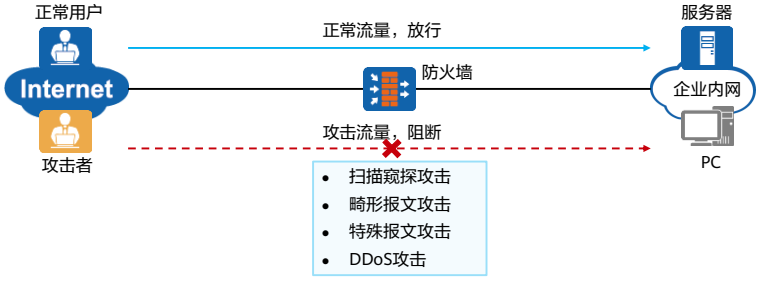
通信网络安全需求 - 带宽管理

- 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：应保证网络各个部分的带宽满足业务高峰期需要。在防火墙上部署带宽管理，可以保障关键业务的流量带宽，同时可以在防火墙上部署配额控制策略，控制用户的上网流量与上网时间，提供员工工作效率。



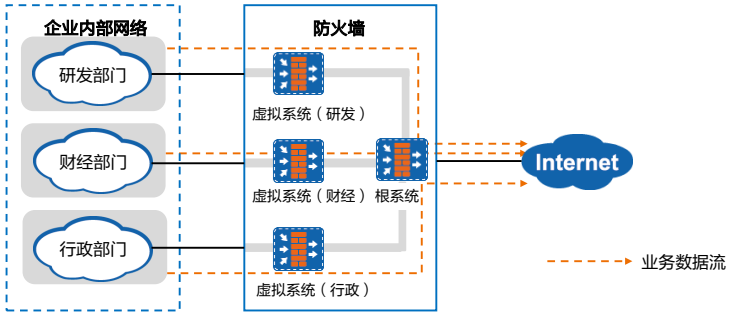
边界区域安全威胁 - 网络攻击防范

- 通常情况下，防火墙部署在企业内网出口，开启攻击防御功能后，防火墙能够区分出正常流量和攻击流量。对正常流量进行放行，对于攻击流量进行阻断，从而有效保障了企业内网服务器和PC的正常运行，使服务器能够响应正常用户的业务需求，内网用户的PC能够正常工作。



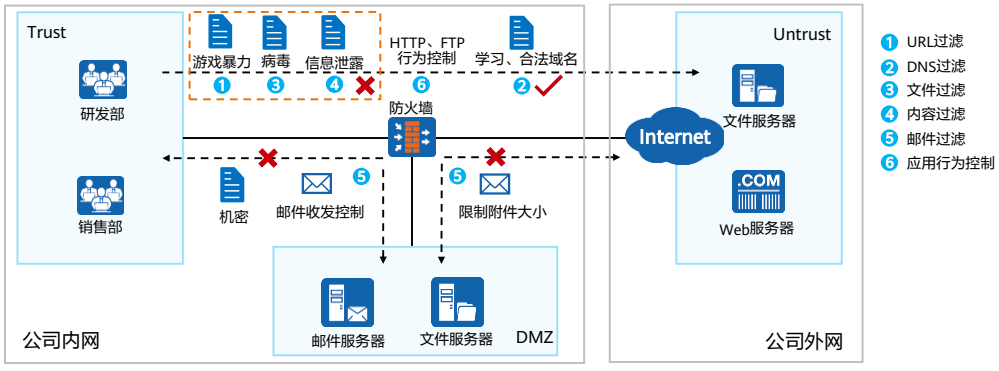
边界区域安全需求 - 网络隔离

- 通常大中型企业组织架构复杂，网络设备数量众多，网络环境复杂。随着企业业务规模的不断增大，各业务部门都会有不同的安全需求。如果将业务需求都部署在一台防火墙上，会导致防火墙的配置异常复杂，管理员操作容易出错。通过防火墙的虚拟化技术，可以在实现网络隔离的基础上，使得业务管理更加清晰和简便。



边界区域安全需求 - 应用内容安全

- 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。无论是从合规性角度还是从业务需求角度，企业都需要实现对员工行为、对应用内容的控制，保障员工行为不违规、企业机密不外泄、内网安全受保障。

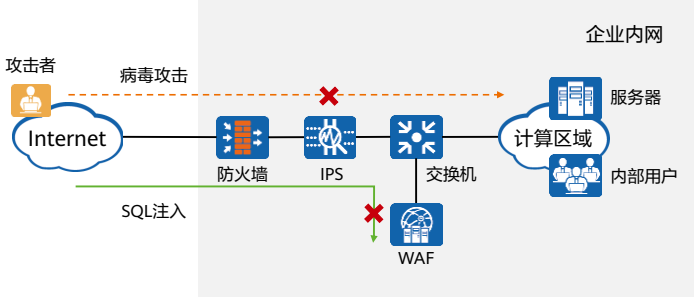


HUAWEI

- 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。

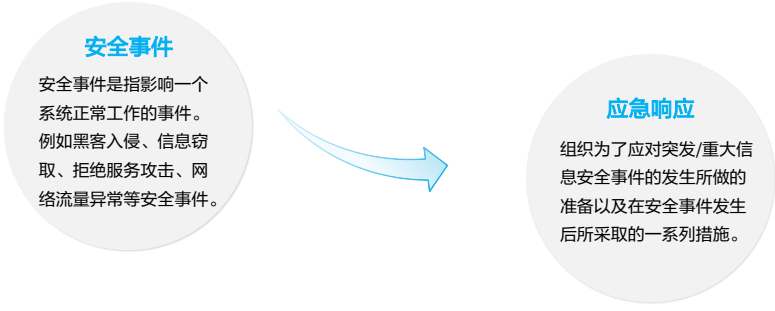
计算环境安全威胁 - 应用威胁

- 内部网络计算区域包含办公电脑、服务器和移动终端等硬件设备及其承载的系统、应用和数据。当内部网络出现漏洞时，极易受到病毒、入侵等多种应用威胁。安全实施工程师通常部署安全设备保护计算区域，安全运维工程师也在日常工作中通过漏洞扫描及时发现漏洞，打上补丁，有时会进行渗透测试，预防网络可能遭受的威胁。



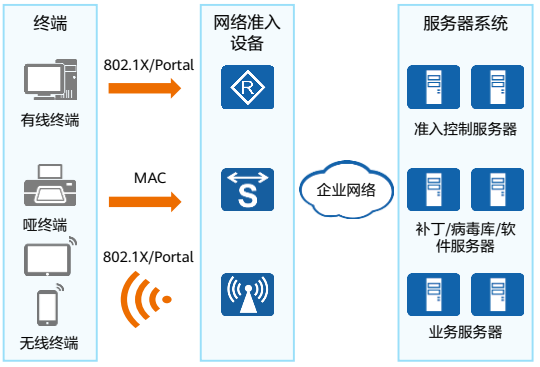
管理中心安全需求 - 应急响应

- 安全运维工程师需要了解网络的安全态势，以便及时识别安全风险，预防或及时响应安全威胁。
- 应急响应（Incident Response/Emergency Response）通常是指一个组织为了应对突发、重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。
- 应急响应能够降低企业受到的损失，减少信息安全事件带来的负面影响。



管理中心安全需求 - 准入控制

- 当员工的权限范围过大时，如果出现误操作，业务系统的安全风险将会增大，如误删数据库等；
- 另一方面，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。
- 此时需要对接入用户的身份进行认证，对授权进行管控。准入控制是每个园区网络都必需的。



准入控制示意图

思考题

1. （多选题）下列哪些项不属于基础设施安全的范畴？（　　）
   A. 加密传输
   B. 漏洞扫描
   C. 态势感知
   D. 网络可靠性
2. （判断题）防火墙可靠性属于边界区域的安全措施。（　　）
   A. T
   B. F

1. BC
2. B

本章总结

- 本章节介绍了网络安全工程师的分类与职责，并描述了安全实施与安全运维工程师的能力模型，以及针对能力模型，华为安全认证课程的覆盖范围。
- 通过本章节的学习，您将能够描述安全工程师的分类以及相关岗位的人才要求，了解HCIP-Security的课程大纲。

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
5G	5th Generation	第五代
AntiDDoS	Anti Distributed Denial of Service	异常流量监管系统
DNS	Domain Name Server	域名服务器
DDoS	Distributed Denial of Service	分布式拒绝服务
ERP	Enterprise Resource Planning	企业资源计划
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
IDS	Intrusion Detection System	入侵检测系统
IPS	Intrusion Prevention System	入侵防御系统
ISP	Internet Service Provider	互联网服务提供商
IPSec	Internet Protocol Security	因特网协议安全协议
SNMP	Simple Network Management Protocol	简单网络管理协议

缩略语表 (2)

缩略语	英文全称	解释
SQL	Structured Query Language	结构化查询语言
SSL	Universal Serial Bus	通用串行总线
TCP/IP	Transmission Control Protocol/Internet Protocol	传输控制协议/互联网协议
URL	Uniform Resource Locator	统一资源定位符
WAF	Web Application Firewall	Web应用防火墙
XSS	Cross-Site Scripting	跨站点脚本

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.

防火墙高可靠性技术

HUAWEI

前言

- 防火墙通常部署在整个企业网络的边界，或者企业内网不同区域之间，属于网络中的关键网元。为保障企业网络稳定可靠的运行，需要应用多种提高防火墙高可靠性的技术。
- 防火墙高可靠性技术一般通过设备冗余和链路冗余来实现，本章主要介绍防火墙高可靠性技术的原理及应用场景。

目标

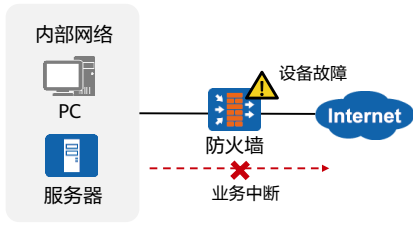
- 学完本课程后，您将能够：
  - 描述防火墙高可靠性技术的原理
  - 了解防火墙高可靠组网方式
  - 描述防火墙高可靠性技术的应用场景
  - 配置防火墙高可靠性技术

目录

防火墙高可靠性技术背景

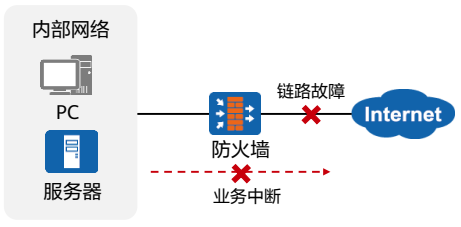
- 网络架构中硬件的不可靠主要源自于设备不可靠与链路不可靠两方面，以防火墙为例：

设备不可靠



- 设备故障：当防火墙出现硬件或业务功能故障时，所有以防火墙作为默认网关的主机与外部网络之间的通讯将中断。

链路不可靠



- 链路故障：当防火墙唯一的出口链路发生故障时，所有以防火墙作为默认网关的主机与外部网络之间的通讯将中断。

防火墙高可靠性技术概览

- 防火墙高可靠性技术分为两类：设备高可靠性和链路高可靠性。

设备高可靠性技术

双机热备	跨数据中心集群	硬件Bypass
两台防火墙组成双机热备，当一台防火墙发生故障时，另一台防火墙接替工作，保障业务的连续性。	当某一个数据中心防火墙发生故障或灾难的情况下，其他数据中心防火墙可以对其业务实现接管，达到互为备份的效果。	当防火墙工作失效时，会导致网络中断，而硬件Bypass则能让防火墙在工作失效后，对流量不作任何处理，直接转发。

链路高可靠性技术

Eth-Trunk	IP-Link	BFD	Link-Group	健康检查
绑定多个物理接口为一个逻辑接口，提高链路的可靠性。	周期性发送ARP或ICMP报文，检测链路的可用性。	周期性发送BFD控制报文，检测设备或系统之间链路的可用性。	Link-Group功能是将多个接口的状态相互绑定，组成一个逻辑组。	防火墙上的功能，对服务可用性、链路可用性或链路时延等进行探测，目前与防火墙智能选路特性结合使用。

目录

双机热备工作原理

- HRP协议：即Huawei Redundancy Protocol，主要用于实现防火墙双机之间关键配置命令和状态化信息的备份，状态化信息主要包括会话表、Servermap表、黑白名单、NAT映射表等。
- VGMP协议：即VRRP Group Management Protocol，主要用于实现对VRRP备份组的统一管理，保证多个VRRP备份组状态的一致性，同时VGMP的状态也会影响路由协议的开销。
- 备份通道：也称为“心跳线”，用于HRP协议和VGMP协议的通信。

HUAWEI

- VGMP状态：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。

双机热备工作模式

- 防火墙支持主备备份和负载分担两种工作模式。

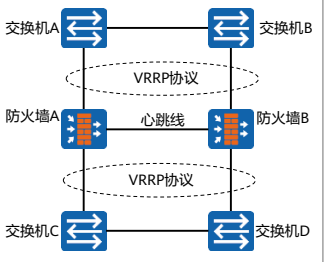
主备备份模式	负载分担模式
• 两台设备一主一备。正常情况下业务流量由主用设备处理。当主用设备故障时，备用设备接替主用设备处理业务流量，保证业务不中断。 • 流量由单台设备处理，相较于负载分担模式，路由规划和故障定位相对简单。 • 主备备份模式中，备用设备不承载任何业务流量，资源利用率不高。	• 两台设备互为主备。正常情况下两台设备共同分担整网的业务流量。当其中一台设备故障时，另外一台设备会承担其业务，保证原本通过该设备转发的业务不中断。 • 相较于主备备份模式，组网方案和配置相对复杂。 • 负载分担模式组网中流量由两台设备共同处理，可以提高防火墙整体的业务吞吐量。 • 负载分担模式组网中设备发生故障时，只有一半的业务需要切换，故障切换的速度更快。

- 不同模式中备份的注意事项：
  - 在主备备份组网下，配置命令和状态信息都由主用设备备份到备用设备。
  - 而在负载分担组网下，两台防火墙都是主用设备。因此如果允许两台主用设备之间能够相互备份命令，那么可能就会造成两台设备命令相互覆盖或冲突的问题。所以为了方便管理员对两台防火墙配置的统一管理，避免混乱，我们引入配置主和配置从设备的概念。
  - 负载分担组网下，发送备份配置命令的防火墙称为配置主设备（命令行提示符前有HRP_M前缀），接收备份配置命令的防火墙称为配置从设备（命令行提示符前有HRP_S前缀）。配置命令只能由“配置主设备”备份到“配置从设备”。状态信息则是两台设备相互备份。

双机热备场景介绍

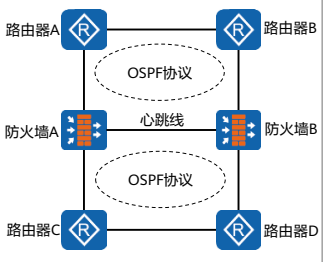
- 根据防火墙组网方式不同，可将双机热备分为以下场景，每种场景均支持主备备份/负载分担模式。

基于VRRP的双机热备



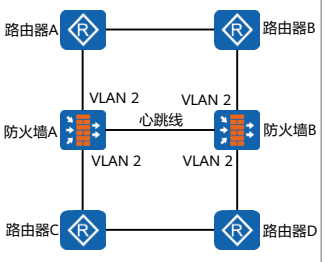
- 防火墙的业务接口工作在三层模式，上下行与交换机互联，运行VRRP协议。

基于路由协议的双机热备



- 防火墙的业务接口工作在三层模式，上下行与路由器互联，运行OSPF协议。

透明模式的双机热备

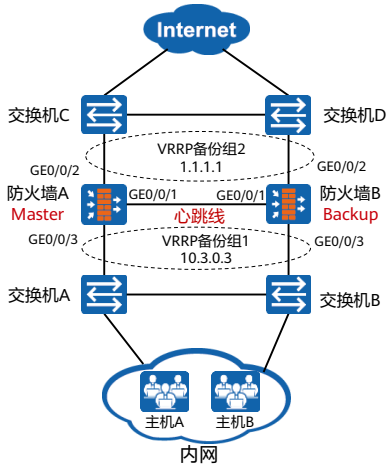


- 防火墙的业务接口工作在二层模式，上下行与路由器/交换机互联。

目录

主备备份模式的应用场景

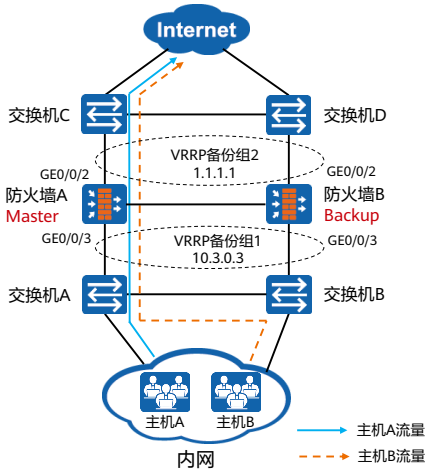
- 组网描述：
  - 如图所示，对于可靠性要求较高的场景，可在企业网络出口部署两台防火墙组成双机热备。
- 组网分析：
  - 防火墙VGMP状态：防火墙A为Master，VGMP状态为Active；防火墙B为Backup，VGMP状态为Standby；
  - VRRP备份组：防火墙下游配置VRRP备份组1 ，防火墙上游配置VRRP备份组2；防火墙A的VRRP备份组1和2设置为Master，防火墙B的VRRP备份组1和2设置为Backup；
  - 备份接口：两台防火墙的GE0/0/1接口为心跳口，对应的心跳线作为备份链路。



HUAWEI

主备备份模式的流量转发过程

- 流量转发过程：
  - 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。
  - 返回流量的转发过程类似，不再赘述。

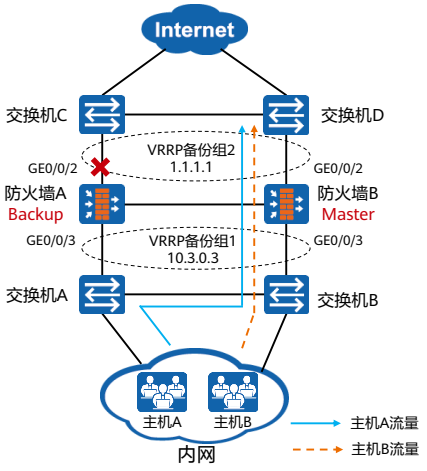


HUAWEI

- 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。

主备备份模式的故障切换 (1)

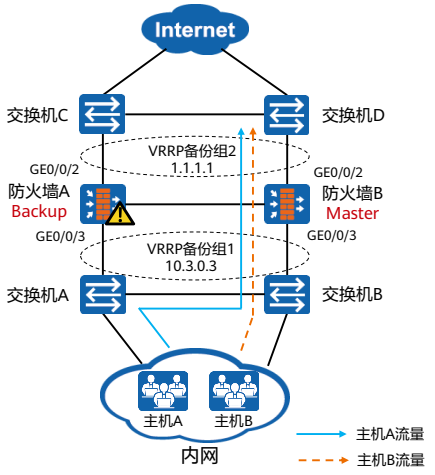
- 防火墙业务接口/业务线路故障，触发主备切换：
  - 如图所示，当防火墙A的GE0/0/2接口出现故障时，防火墙A的VGMP组优先级降低，发送VGMP请求报文；
  - 防火墙B收到对端发送的VGMP请求报文后，与自己的VGMP组优先级进行比较，发送VGMP应答报文；
  - 防火墙A收到回应报文，将VGMP组状态切换为Standby，防火墙A上的VRRP备份组1和备份组2则切换状态为Backup；
  - 防火墙B将VGMP组状态切换为Active，防火墙B上的VRRP备份组1和备份组2则切换状态为Master；
  - 防火墙B向交换机B和D发送免费ARP报文，刷新交换机的MAC地址表，业务流量切换至防火墙B。



HUAWEI

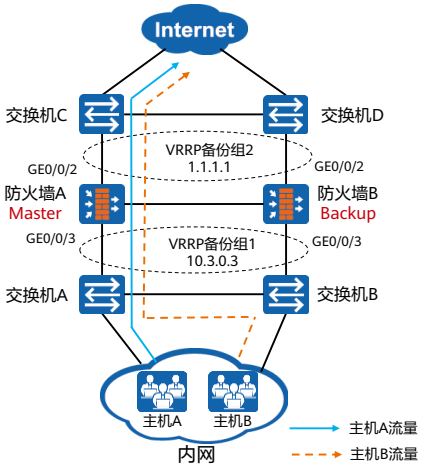
主备备份模式的故障切换 (2)

- 防火墙整机故障，触发主备切换：
  - 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B向交换机B和D发送免费ARP报文，刷新交换机的MAC地址表，业务流量切换至防火墙B。



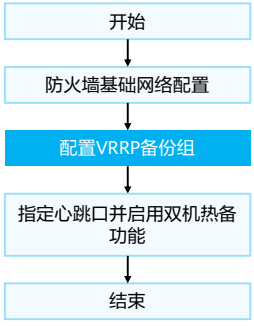
主备备份模式的回切过程

- 故障恢复，触发主备回切流程：
  - 防火墙A故障恢复后，此时VGMP组优先级恢复，缺省情况下，等待60秒后，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；
  - 防火墙A向交换机A和C发送免费ARP报文，刷新交换机的MAC地址表，业务流量回切至防火墙A。



主备备份模式的配置思路

- 配置思路：



- 关键配置：
  - 在防火墙A的上下行业务接口上配置VRRP备份组，并设置VRRP组状态为Active。

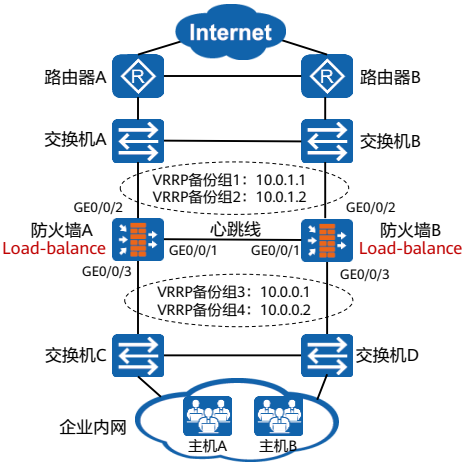
```
[FW_A] interface GE0/0/2
[FW_A-GE0/0/2] vrrp vrid 1 virtual-ip 1.1.1.1 active
[FW_A-GE0/0/2] quit
[FW_A] interface GE0/0/3
[FW_A-GE0/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 active
[FW_A-GE0/0/3] quit
```

  - 在防火墙B的上下行业务接口上配置VRRP备份组，并设置VRRP组状态为Standby。

```
[FW_B] interface GE0/0/2
[FW_B-GE0/0/2] vrrp vrid 1 virtual-ip 1.1.1.1 standby
[FW_B-GE0/0/2] quit
[FW_B] interface GE0/0/3
[FW_B-GE0/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 standby
[FW_B-GE0/0/3] quit
```

负载分担模式的应用场景

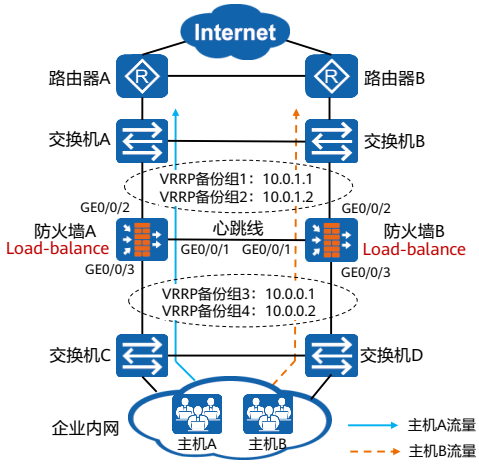
- 组网描述：
  - 如图所示，防火墙的上下行业务接口工作在三层，两台防火墙同时工作为用户转发流量，同时互为备份，增加网络的可靠性。
- 组网分析：
  - 如果两台防火墙工作在负载分担模式，两台防火墙上均要存在状态为Master的VRRP备份组；
  - 防火墙A的VRRP1和VRRP3状态为Master，VRRP2和VRRP4状态为Backup；
  - 防火墙B的VRRP1和VRRP3状态为Backup ，VRRP2和VRRP4状态为Master；
  - 两台设备的VGMP组状态都是Load-balance。



HUAWEI

负载分担模式的流量转发过程

- 流量转发过程：
  - 企业内网中部分主机的网关被设置成VRRP3的虚拟IP地址10.0.0.1。这些主机在访问外部网络时，会发送ARP请求报文，请求10.0.0.1的MAC地址。防火墙A的VRRP3状态为Master，会响应内网主机的ARP请求。防火墙B的VRRP3状态为Backup，不会响应内网主机的ARP请求。防火墙A响应的ARP报文会刷新交换机的MAC地址表和主机的ARP缓存表，使这部分主机发往外部网络的流量都被引导到防火墙A上处理。
  - 另一部分主机的网关被设置成VRRP4的虚拟IP地址10.0.0.2。这些主机在访问外部网络时，会发送ARP请求报文，请求10.0.0.2的MAC地址。此时，只有防火墙B会响应这个ARP请求。因此，这部分主机的流量都被引导到防火墙B上转发。

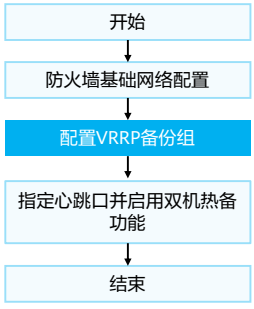


HUAWEI

- 同理，路由器A到内部网络路由的下一跳地址被设置成了VRRP备份组1的虚拟IP地址10.0.1.1，路由器A发往内部网络的流量会被引导到防火墙A上处理。路由器B到内部网络路由的下一跳被设置成了VRRP备份组2的虚拟IP地址10.0.1.2，路由器B发往内部网络的流量会被引导到防火墙B上处理。

负载分担模式的配置思路

- 配置思路：



- 关键配置：
  - 在防火墙上分别配置两个VRRP备份组。

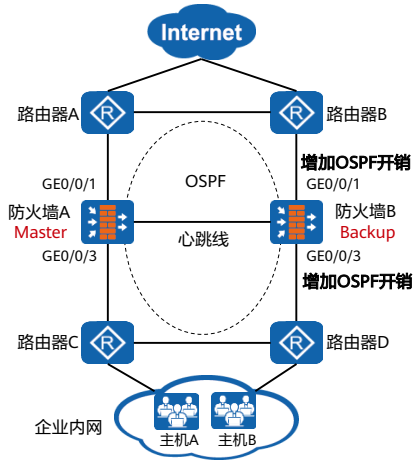
```
[FW_A] interface GigabitEthernet 0/0/2
[FW_A-GE0/0/2] vrrp vrid 1 virtual-ip 10.0.1.1 active
[FW_A-GE0/0/2] vrrp vrid 2 virtual-ip 10.0.1.2 standby
[FW_A] interface GigabitEthernet 0/0/3
[FW_A-GE0/0/3] vrrp vrid 3 virtual-ip 10.0.0.1 active
[FW_A-GE0/0/3] vrrp vrid 4 virtual-ip 10.0.0.2 standby

[FW_B] interface GigabitEthernet 0/0/2
[FW_B-GE0/0/2] vrrp vrid 1 virtual-ip 10.0.1.1 standby
[FW_B-GE0/0/2] vrrp vrid 2 virtual-ip 10.0.1.2 active
[FW_B] interface GigabitEthernet 0/0/3
[FW_B-GE0/0/3] vrrp vrid 3 virtual-ip 10.0.0.1 standby
[FW_B-GE0/0/3] vrrp vrid 4 virtual-ip 10.0.0.2 active
```

目录

主备备份模式的应用场景

- 组网描述：
  - 如图所示，防火墙的上下行业务接口工作在三层，与路由器直连。防火墙与路由器之间运行OSPF协议。
- 组网分析：
  - 防火墙A为Master，VGMP状态为Active。防火墙B为Backup，VGMP状态为Standby。
  - 启用双机热备功能后，防火墙能根据VGMP组状态动态调整OSPF协议的路径开销。Master防火墙的VGMP组状态为Active，防火墙按照OSPF路由的配置正常发布路由，不修改开销；Backup防火墙的VGMP组状态为Standby，防火墙会增加OSPF路由的开销，使得Backup防火墙发布出去的OSPF路由成为备用路由。

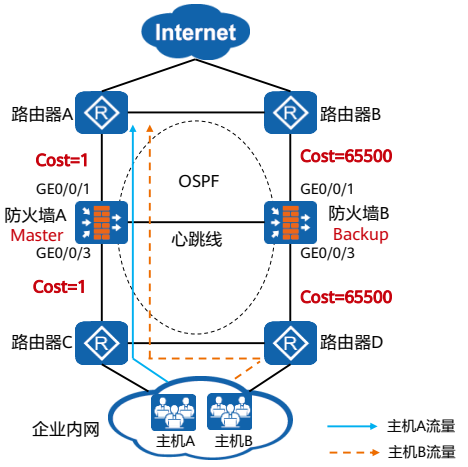


HUAWEI

- 上下行连接三层设备，无法配置VRRP组，无法通过VRRP确定主备设备，也无法通过VRRP监控防火墙直连业务口。
- hrp adjust enable命令用来启动路由开销调整功能，防火墙会根据主备状态动态调整OSPF等路由协议的开销。

主备备份模式的流量转发过程

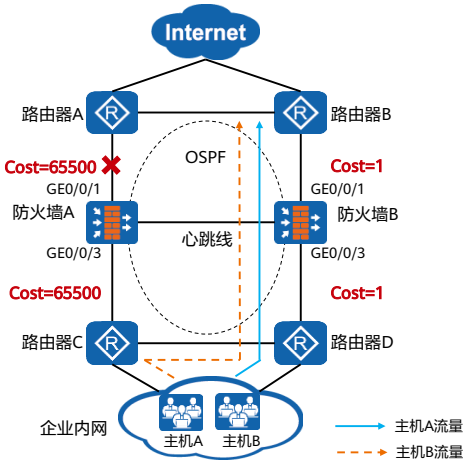
- 流量转发过程：
  - 正常工作时，防火墙A按照OSPF配置正常发布路由，而防火墙B发布的OSPF路由的Cost值则被调整为65500。防火墙A所在链路的开销值将远小于防火墙B所在链路的开销值。路由器在转发流量时会选择开销更小的路径，因此内外部网络之间的流量都被引导到防火墙A上转发。
  - 图中防火墙A的接口带宽为1000 Mbps，所以OSPF的Cost开销为1。



HUAWEI

主备备份模式的故障切换

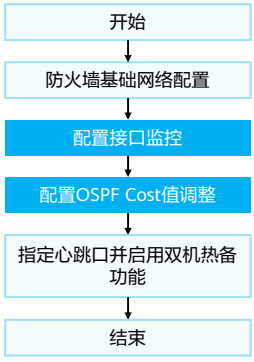
- 主备切换过程：
  - 当防火墙A的上行业务接口故障。防火墙A的VGMP组状态变为Standby，防火墙B的VGMP组状态变为Active。
  - 防火墙A、B根据VGMP组状态对OSPF开销进行调整：
    - 防火墙A发布的OSPF路由开销值被调整为65500；
    - 防火墙B发布的OSPF路由开销值被调整为1。
  - OSPF路由完成收敛后，内外部网络之间的流量都被引导至防火墙B进行转发。



HUAWEI

主备备份模式的配置思路

- 配置思路：



- 关键配置：
  - 在防火墙A、B上分别配置HRP Track Interface，监控上下行业务口。

```
[FW_A] hrp track interface GE0/0/1
[FW_A] hrp track interface GE0/0/3
[FW_B] hrp track interface GE0/0/1
[FW_B] hrp track interface GE0/0/3
```

  - 在防火墙A和防火墙B上配置Cost值调整命令。

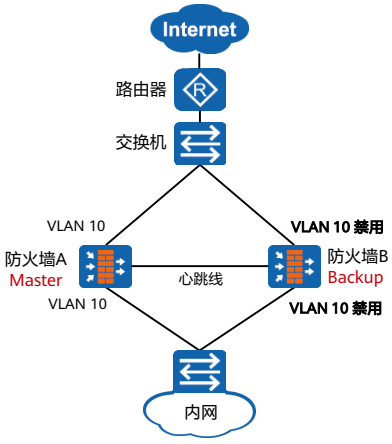
```
[FW_A] hrp adjust ospf-cost enable
[FW_B] hrp adjust ospf-cost enable
```

说明：防火墙发布OSPF路由时，如果是主用设备，防火墙把学习到的OSPF路由直接发布出去；如果是备用设备，防火墙发布slave-cost值为65500的OSPF路由。

目录

主备备份模式的应用场景

- 组网描述：
  - 如图所示，防火墙的上下行业务口工作在二层，与二层交换机直连。每台防火墙的上下行业务接口加入到相同VLAN。要求防火墙能够监测业务口的可用性。
- 组网分析：
  - 防火墙A为Master，VGMP状态为Active，防火墙B为Backup，VGMP状态为Standby。
  - 启用双机热备后，防火墙能根据VGMP组状态启用或禁用VLAN（需配置VLAN监控）。
    - VGMP组状态为**Active**时，防火墙将VGMP组监控的VLAN状态调整为启用状态，该VLAN可以转发报文。
    - VGMP组状态为**Standby**时，防火墙将VGMP组监控的VLAN状态调整为禁用状态，该VLAN不能转发报文。

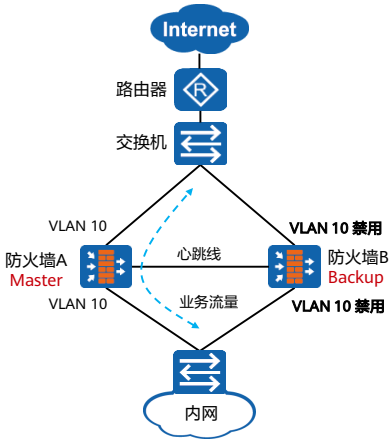


HUAWEI

- 在此组网中，防火墙透明接入到原有交换机网络，不改变网络拓扑。

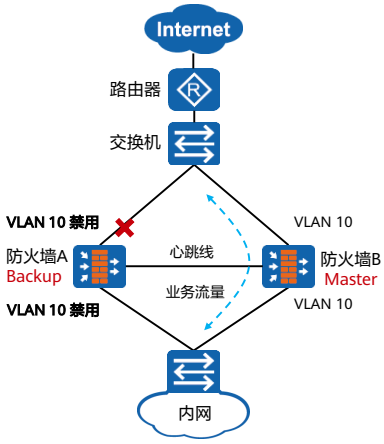
主备备份模式的流量转发过程

- 流量转发流程：
  - 当两台防火墙都正常工作时，因为防火墙B为备用防火墙，VLAN 10处于禁用状态。防火墙A的VLAN 10处于启用状态。上下行交换机只能从连接防火墙A的接口上学习到MAC地址，流量都被引导到防火墙A上处理。



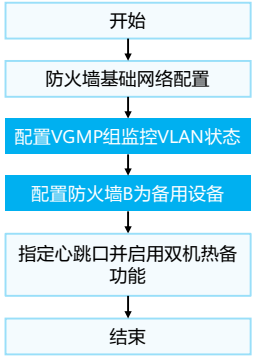
主备备份模式的故障切换

- 故障切换流程：
  - 防火墙A的上行业务接口故障。防火墙A的VGMP组状态变为Standby，防火墙B的VGMP组状态变为Active。
  - 防火墙A、B根据VGMP组状态调整VLAN状态：防火墙A的VLAN 10被禁用，防火墙B的VLAN 10被启用。
  - 同时，防火墙A上所有加入VLAN 10的接口都会变为Down状态，以此触发上下行交换机删除MAC地址表。
  - 当报文到达交换机时，由于匹配不到MAC地址，报文会在VLAN 10内泛洪。之后，上下行交换机从连接防火墙B的接口学习到MAC地址表，后续流量被引导到防火墙B上处理。



主备备份模式的配置思路

- 配置思路：



- 关键配置：
  - 在防火墙A、B上配置VGMP组监控VLAN状态，监控上下行业务接口对应的VLAN。

```
[FW_A] hrp track vlan 10
[FW_B] hrp track vlan 10
```

  - 配置防火墙B为备用设备。

```
[FW_B] hrp standby-device
```

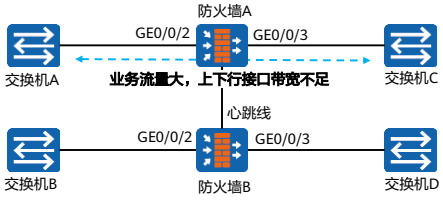

HUAWEI

- 配置VGMP组监控VLAN状态：
  - 应用场景：防火墙工作在二层时，为了让VGMP管理组能够监控二层业务接口的状态，需要将上下行业务接口加入同一个VLAN，并配置hrp track vlan。
  - 作用：配置hrp track vlan后，VLAN中每个接口故障，VGMP管理组优先级降低2。备用设备上配置hrp track vlan后，该VLAN就不能转发报文。
  - 配置命令：hrp track vlan vlan-id。

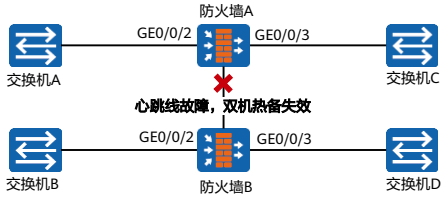
目录

Eth-Trunk技术背景

- 防火墙通常是企业网络中较为关键的网络设备，双机热备技术虽然可以明显提高设备的可靠性，但是从网络整体来看，依然可能存在以下问题：
  - 若发生双机热备频繁切换事件，会造成网络不稳定；
  - 业务流量较大的场景中，链路带宽可能存在瓶颈，无法满足业务需求（特别是突发业务流量）；
  - “心跳线”出现故障后，导致HRP/VGMP协议无法通信，双机热备失效，影响业务。



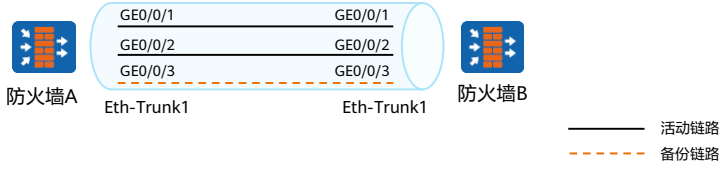
接口带宽存在瓶颈



心跳线故障

Eth-Trunk技术介绍

- Eth-Trunk技术简称链路聚合，可以将多条以太网物理链路捆绑在一起成为一条逻辑链路，可实现增加带宽、提高链路可靠性的作用。
- Eth-Trunk主要功能如下：
  - 增加带宽：链路聚合接口的最大带宽可以达到各成员接口带宽之和。
  - 流量负载分担：在一个链路聚合组内，可以实现业务流量的负载分担。
  - 提高可靠性：当某条链路出现故障时，流量可以切换到其他可用链路上，从而提高链路聚合接口的可靠性。



HUAWEI

- 链路聚合组和链路聚合接口：
  - 链路聚合组LAG（Link Aggregation Group）是指将若干条以太链路捆绑在一起所形成的逻辑链路。
  - 每个聚合组唯一对应着一个逻辑接口，这个逻辑接口称之为链路聚合接口或Eth-Trunk接口。
- 活动接口和非活动接口：链路聚合组的成员接口存在活动接口和非活动接口两种。转发数据的接口称为活动接口，不转发数据的接口称为非活动接口。
- 活动链路和非活动链路：活动接口对应的链路称为活动链路，非活动接口对应的链路称为非活动链路。
- Eth-Trunk的链路聚合模式：
  - 手工模式：Eth-Trunk接口的创建、成员接口的加入由手工配置。手工模式下，所有链路都是活动链路，如果有链路断连，则其他活动链路自动分担流量。
  - LACP模式：Eth-Trunk接口的创建、成员接口的加入由手工配置。链路状态协商由LACP协议控制，可以动态监控链路的状态，推荐使用此方式。关于LACP的详细内容，请查阅华为相关产品文档。

Eth-Trunk配置命令

- 创建链路聚合组。

  [FW] **interface eth-trunk** *trunk-id*

- 将以太网物理接口加入链路聚合组中（以太网接口视图）。

  [FW] interface GigabitEthernet 0/0/1
  [FW-GigabitEthernet0/0/1] **eth-trunk** *trunk-id*
  [FW] interface GigabitEthernet 0/0/2
  [FW-GigabitEthernet0/0/2] **eth-trunk** *trunk-id*

- 配置链路聚合接口的IP地址。

  [FW-Eth-Trunk *trunk-id*] **ip address** *x.x.x.x*

查看Eth-Trunk接口状态

- 查看Eth-Trunk接口的配置信息及接口状态。

```
<FW> display eth-trunk
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to flow
Least Active-linknumber: 2  Max Bandwidth-affected-linknumber: 8        Operate status: up
Number Of Up Port  In Trunk: 2
--------------------------------------------------------------------------------
PortName Status weight
GigabitEthernet0/0/1 Up 1
GigabitEthernet0/0/2 Up 1
```

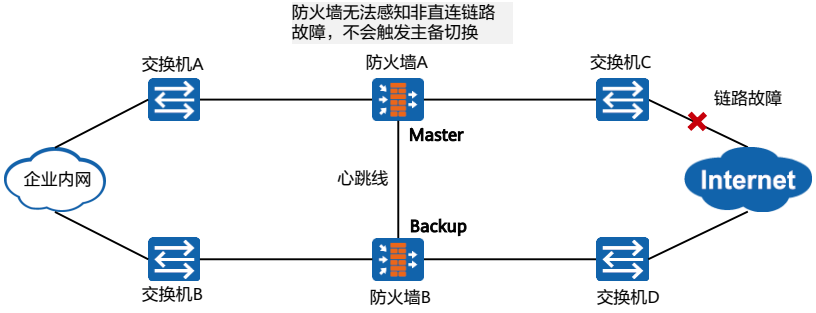

HUAWEI

- WorkingMode代表Eth-Trunk接口的工作模式，有以下几种状态：
  - NORMAL：表示手工负载分担模式；
  - STATIC：表示静态LACP模式；
  - BACKUP：表示手工1：1主备模式。
- Hash arithmetic代表为Eth-Trunk接口负载分担模式，有以下几种状态：
  - According to flow：Eth-Trunk接口根据流进行负载分担；
  - According to packet all：Eth-Trunk接口根据所有包进行负载分担。
- Least Active-linknumber代表状态为Up的Eth-Trunk接口成员链路数的下限阈值。如果Eth-Trunk接口中状态为Up的成员口数小于下限阈值，会导致Eth-Trunk接口状态为Down。
- Max Bandwidth-affected-linknumber代表影响二层Eth-Trunk有效带宽的链路数的上限阈值。
- Operate status代表Eth-Trunk接口的状态：
  - UP：接口处于UP状态，能够正常转发流量；
  - DOWN：接口处于DOWN状态，不能转发流量。
- Number Of Up Port In Trunk代表Eth-Trunk接口中处于Up状态的成员接口数。

目录

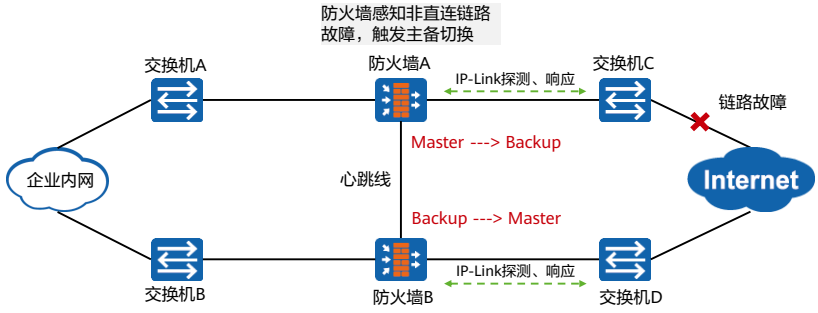
传统双机热备存在的不足

- 传统的双机热备通常只监控防火墙的直连接口，当主用防火墙的直连接口状态由UP转为DOWN时，防火墙触发主备切换。但是对于非直连链路的故障，防火墙无法感知，不会进行主备切换，导致业务中断。



IP-Link探测技术

- IP-Link探测技术是指防火墙通过向指定的目的IP周期性地发送探测报文并等待应答，来判断链路是否发生故障。IP-Link可以检测到非直连链路的故障，与双机热备技术结合使用，提高网络可靠性。

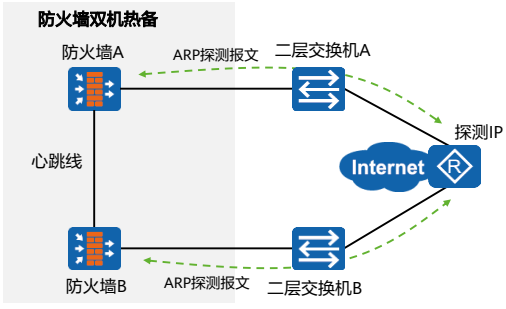


- 防火墙发送探测报文后，在三个探测周期（默认为15s）内未收到响应报文，则认为当前链路发生故障，IP-Link的状态变为DOWN。
- 当链路从故障中恢复，若防火墙能连续地收到3个响应报文，则认为链路故障已经消除，IP-Link的状态变为UP。也就是说，链路故障恢复后，IP-Link的状态并不会立即变为UP，而是要等三个探测周期（默认为15s）才会变为UP。

IP-Link探测模式

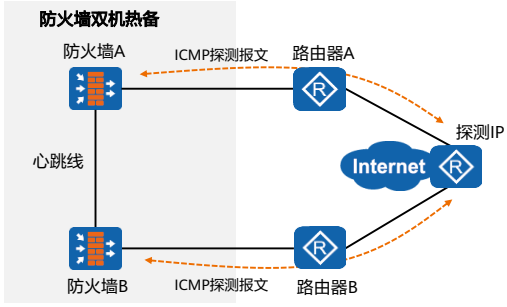
- IP-Link技术根据探测报文的不同，可以分为以下两种探测模式：

ARP探测模式



ARP探测模式仅能用于探测二层网络的连通性。

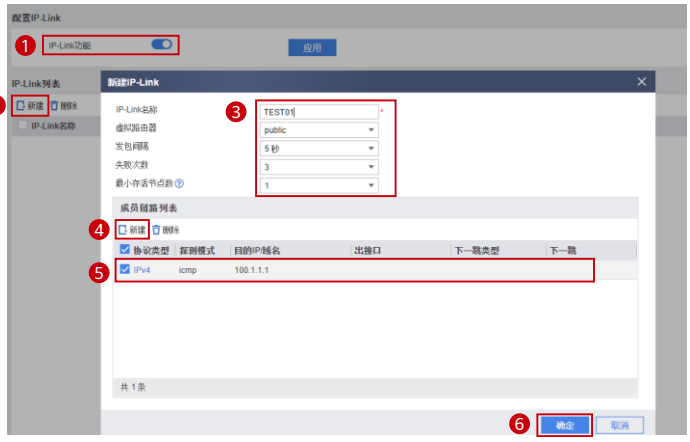
ICMP探测模式



ICMP探测模式适用于探测二层/三层网络的连通性。

IP-Link配置 - Web (1)

- 使用Web方式登陆防火墙，点击“系统 > 高可靠性 > IP-Link”，按照以下顺序配置：
  1. 启用IP-Link功能；
  2. 新建“IP-Link”；
  3. 配置“IP-Link”名称及参数；
  4. 新建“成员链路”；
  5. 配置链路的探测参数；
  6. 点击“确定”。



IP-Link配置 - Web (2)

- 在双机热备中应用IP-Link。
  - 点击“系统 > 高可靠性 > 双机热备 > 配置”，按照如下进行配置：

HUAWEI

IP-Link配置 - CLI

- 配置IP-Link。

```
[FW] ip-link check enable
[FW] ip-link name test
[FW-iplink-test] destination 100.1.1.1 interface GigabitEthernet 0/0/3
```

- 在双机热备中应用IP-Link，当网络故障时，IP-Link状态变为DOWN，VGMP组优先级降低2。

```
[FW] hrp track ip-link test
```

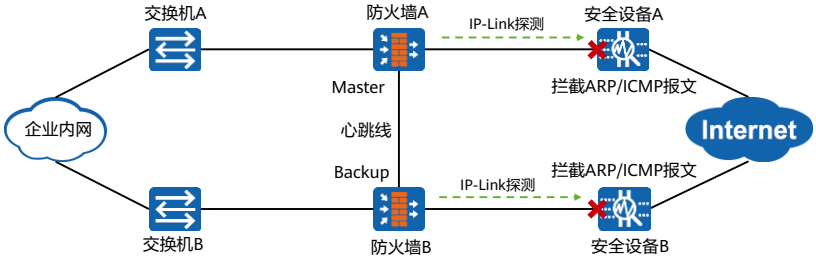
- 查看IP-Link的信息。

```
[FW] display ip-link
Current Total Ip-link Number :1
Name    Member    State  Up/Down/Init
test      1         up     1    0      0
```

目录

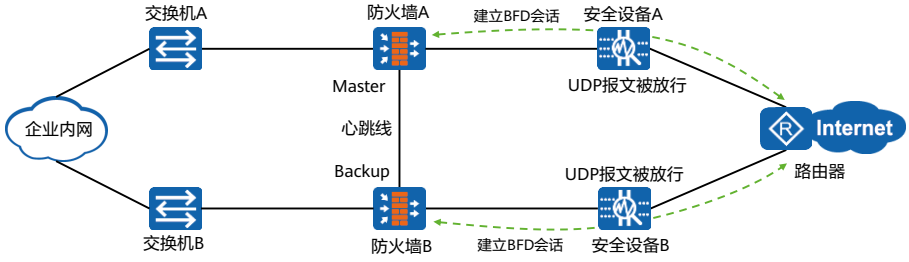
IP-Link探测技术的不足

- IP-Link探测基于ARP或ICMP协议实现，若探测路径上存在某些安全设备，对ARP/ICMP报文进行了过滤，则会导致IP-Link探测失效。



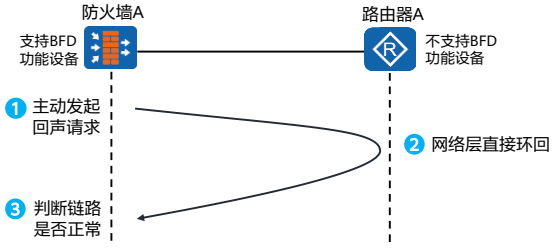
BFD探测技术介绍

- BFD（Bidirectional Forwarding Detection，双向转发检测）用于快速检测设备之间的通信故障，并在出现故障时通知上层协议。
- BFD技术基于UDP报文进行探测，目的端口号为3784。
- 需要在防火墙和被探测设备（如路由器）之间建立BFD会话，需要会话两端设备支持BFD协议。



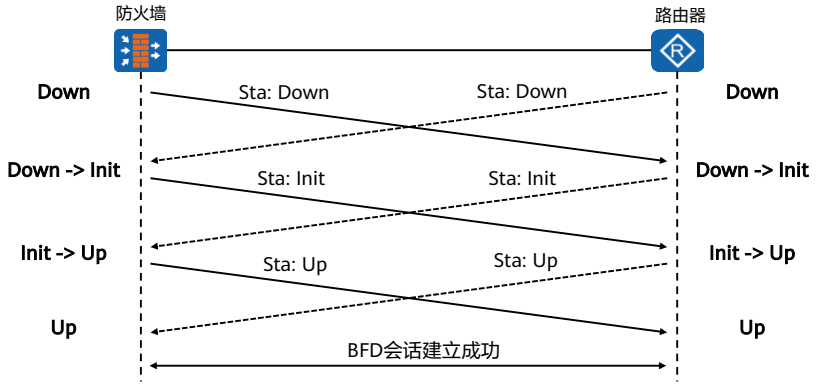
基于单跳会话的BFD Echo功能

- 如果对端设备不支持BFD功能，则无法正常建立会话。此时可以使用基于单跳会话的BFD Echo功能来检测链路。
- BFD Echo功能也称为BFD回声功能，是由本地发送BFD Echo报文，远端系统将报文环回的一种检测机制。
- 为了能够快速的检测这两台设备之间的故障，可以在支持BFD功能的设备上创建单臂回声功能的BFD会话。支持BFD功能的设备主动发起回声请求功能，不支持BFD功能的设备接收到该报文后直接将其环回，从而实现转发链路的连通性检测功能。



BFD会话建立过程

- BFD通过控制报文中的本地标识符和远端标识符区分不同的会话。
- BFD会话有四种状态：Down、Init、Up和AdminDown，BFD会话建立过程如下：

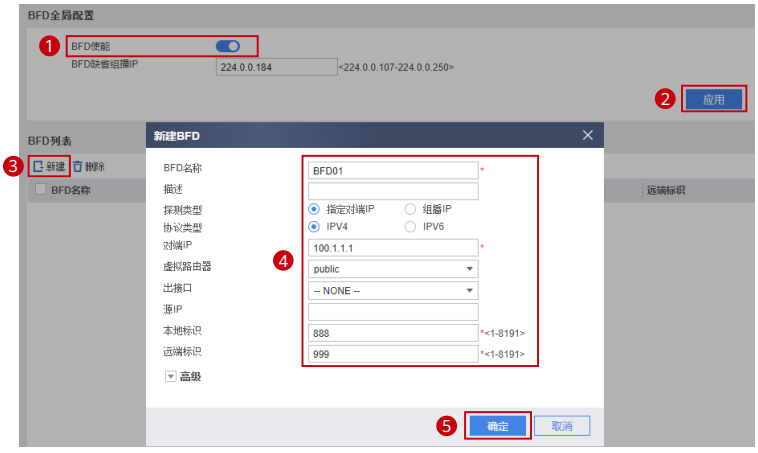


HUAWEI

- 发送方在发送BFD控制报文时会在Sta字段填入本地当前的会话状态，接收方根据收到的BFD控制报文的Sta字段以及本端当前会话状态来进行状态机的迁移。
- BFD会话建立过程如下：
  - 防火墙和路由器的BFD模块收到上层应用的通知后，发送状态为Down的BFD控制报文。
  - 防火墙收到状态为Down的BFD控制报文后，本地状态切换至Init，并发送状态为Init的BFD控制报文。路由器的BFD状态变化同防火墙。
  - 防火墙收到状态为Init的BFD控制报文后，本地状态切换至Up，并发送状态为Up的BFD控制报文。路由器的BFD状态变化同防火墙。
  - 防火墙和路由器双方状态都为Up，会话成功建立并开始检测链路状态。

BFD配置 - Web

- 使用Web方式登陆防火墙，点击“系统 > 高可靠性 > BFD”，按照以下顺序配置：



HUAWEI

BFD配置 - CLI

- 开启全局BFD功能并进入BFD全局视图。

```
[FW] bfd
```

- 通过指定对端IP地址方式创建静态BFD会话。

```
[FW] bfd cfg-name bind peer-ip peer-ip [ vpn-instance vpn-instance-name ] [ interface interface-type interface-number [ nexthop { nexthop-address | dhcp } ] ] [ source-ip source-ip ]
```

此条命令是针对有IP地址的三层接口。

- 配置标识符。

```
[FW-bfd-session-name] discriminator local local-discr-value
```

配置本地标识符。

```
[FW-bfd-session-name] discriminator remote remote-discr-value
```

配置远端标识符。

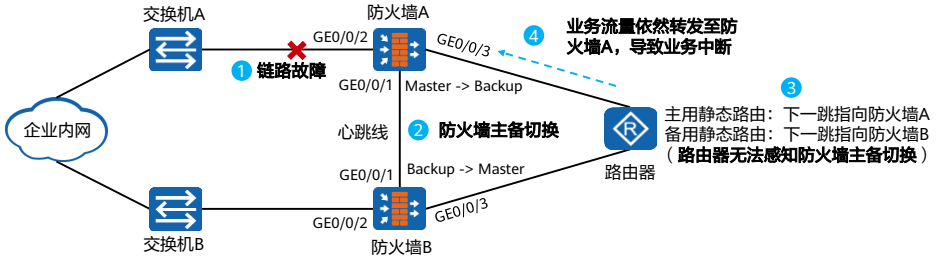
- 提交配置。

```
[FW-bfd-session-name] commit
```

目录

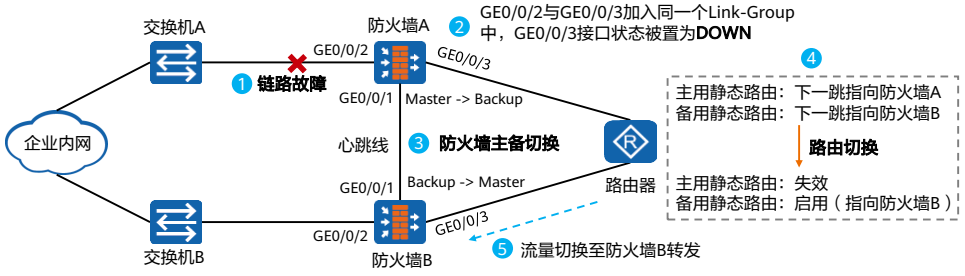
静态路由场景中双机热备存在的问题

- 如下场景中，防火墙A为主用，防火墙B为备用，均与路由器直连，路由器配置了两条静态路由用于访问企业内网，其中主用静态路由指向防火墙A，备用静态路由指向防火墙B，数据流量由防火墙A进行转发。
- 当防火墙A的GE0/0/2接口链路发生故障时，触发防火墙主备切换，防火墙B切换为主用，但是路由器无法感知防火墙发生了主备切换，依然会将业务流量转发至防火墙A，导致业务中断。



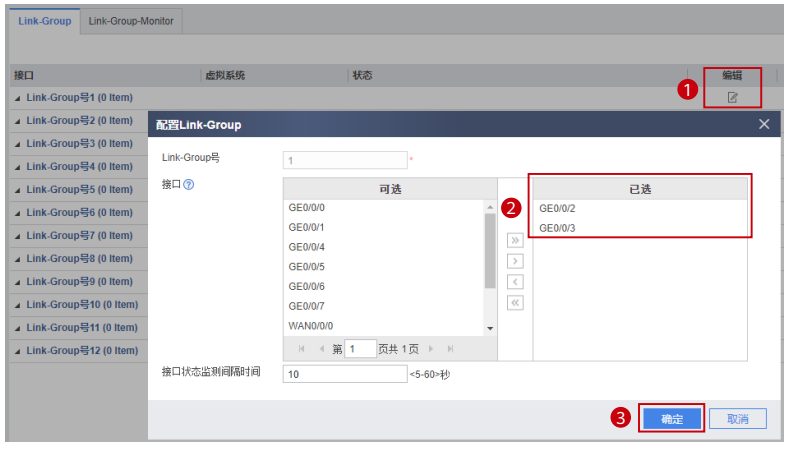
Link-Group原理简介

- Link-Group功能可以将防火墙的多个接口组成一个逻辑组，组内接口始终保持相同的状态（UP/DOWN）。
  - 若组内任一接口出现故障，系统将组内所有接口的状态置为DOWN；
  - 组内所有接口均恢复正常后，系统才会将组内接口的状态置为UP。
- 配置Link-Group功能，使防火墙直联的网络设备可以感知到主备发生切换，从而切换路由，恢复业务。



Link-Group配置 - Web

- 使用Web方式登陆防火墙，点击“系统 > 高可靠性 > Link-Group”，按照以下顺序配置：



Link-Group配置 - CLI

- 配置防火墙接口加入Link-Group。

```
<FW> system-view
[FW] interface GigabitEthernet 0/0/2
[FW-GigabitEthernet0/0/2] link-group 1
[FW] interface GigabitEthernet 0/0/3
[FW-GigabitEthernet0/0/3] link-group 1
```

- 查看Link-Group成员接口状态。

```
[FW] display link-group 1
link group 1, total 2, fault 0
GigabitEthernet0/0/2 : up
GigabitEthernet0/0/3 : up
```

目录

双机热备系统版本升级概述

- 双机热备系统版本升级是现网中常见的运维操作之一，系统升级主要有以下原因：

当前现网软件版本出现Bug，需要升级版本修复Bug。	当前现网软件版本不支持某些特性，需要新增设备特性。	设备现网软件版本不统一，需要进行全网版本规范整改。

- 本章节仅介绍双机热备系统版本升级的一般思路，具体的一些操作，包括设备运行信息的查看、业务运行信息的查看、配置文件的备份与比对、License上传、内容安全组件包上传、验证升级结果等需要根据具体现网情况及需求调整。
- 需要注意的是：版本升级对升级前的设备型号和版本是有要求的，详见华为官网的《 升级指导书 》。

升级前准备 (1)

- 确定升级方式：Web升级或者命令行方式升级。
- 准备升级环境：配置防火墙作为Web server或FTP server。
- 准备升级工具：登录工具及配置文件比较工具。
- 获取升级所需的文件：如系统软件，以.bin为后缀名；内容安全组件包；特征库本地升级包等。
- 查看设备当前运行情况：
  - 查询当前版本软件的信息。

```
<FW> display version
```

  - 确认当前License的使用情况。

```
<FW> display license
```

  - 查看设备当前硬件运行状态。

```
<FW> display device
```


- Web升级和命令行升级都适用于设备处于正常运行的状态下，已经承载了业务流量的情况。
- 各类升级场景都支持这两种升级方案。一般推荐命令行方式升级。
- 查看设备的配置、运行情况和业务的运行情况，便于升级完成后对比，确认业务连续性不受影响。

升级前准备 (2)

- 查询设备当前配置文件。

```
<FW> display startup
```

- 查看设备接口信息。

```
<FW> display interface brief
```

- 查看设备双机状态。

```
<FW> display hrp state
<FW> display vrrp
```

- 查询业务运行情况：
  - 查看设备路由表。

```
<FW> display ip routing-table
```

  - 查看设备MAC表。

```
<FW> display mac-address
```

升级前准备 (3)

- 查看设备会话表。

```
<FW> display firewall session table
```

- 查看和备份重要数据：
  - 备份系统软件。
  - 保存配置并备份配置文件。

```
<FW> save
```

```
ftp> get remote-filename [ local-filename ]
```

- 检查剩余空间：

```
<FW> dir hda1:
```

升级前准备 (4)

- 上传待升级版本软件，并设置为下次启动时使用的软件版本：

```
ftp> put local-filename [ remote-filename ]
```

```
<FW> startup system-software filename
```

版本升级 (1)

- 为保障升级过程中业务的连续性，系统升级通常选择在业务运行较少的时段，如非工作时间段；此外，升级需要遵循的主要原则是Active设备和Standby设备分别升级，先升级Standby设备，然后再升级Active设备，在升级过程中HRP备份通道（心跳线）必须断开。
- 备机升级：
  1. Shutdown备机的业务接口；
  2. Shutdown备机的心跳接口；
  3. 升级备机的系统软件版本；
  4. Undo shutdown备机的心跳接口；
  5. 等待主备防火墙同步会话表等表项；
  6. Undo shutdown备机的业务接口；
  7. 验证备机的升级结果：版本信息、License信息、设备运行状态、接口信息、配置对比、路由表、会话表等；
  8. 保存配置。

- 必须是先shutdown业务接口，再shutdown心跳接口，否则可能会形成双主现象。
- 当系统升级后业务异常时，需要进行版本回退。

版本升级 (2)

- 主机升级：
  1. Shutdown主机的业务接口；
  2. Shutdown主机的心跳接口；
  3. 升级主机的系统软件版本；
  4. Undo shutdown主机的心跳接口；
  5. 等待主备防火墙同步会话表等表项；
  6. Undo shutdown主机的业务接口；
  7. 验证主机的升级结果：版本信息、License信息、设备运行状态、接口信息、配置对比、路由表、会话表等；
  8. 保存配置。

- 当系统升级后业务异常时，需要进行版本回退。
- 需要注意的是：当HRP协议格式发生变更时，两种不同的系统版本不能兼容，无法形成双机热备，可能会形成双主现象。此时，应该先shutdown主机的心跳接口，再undo shutdown备机的心跳接口，依靠VRRP优先级完成业务流量转变。

升级后验证

- 使用**display hrp state**命令可以查看防火墙的业务主备状态。
- 使用**Ping**命令测试业务是否正常。
- 测试双机倒换：
  - 在内网的PC上长Ping公网的IP地址，然后将主用防火墙的上行或下行接口shutdown，观察防火墙状态切换及Ping包丢包情况。如果切换正常，备用防火墙会立即切换为主机承载业务。备用防火墙命令行提示符前的前缀由HRP_S变为HRP_M，主用防火墙命令行提示符前的前缀由HRP_M变为HRP_S。Ping测试观察是否存在丢包情况；
  - 再将主用防火墙的上行或下行接口恢复，观察防火墙状态切换及Ping包丢包情况。如果切换正常，在抢占延迟时间到达（缺省是60s）后，主用防火墙会重新切换为主机承载业务。主用防火墙命令行提示符前的前缀由HRP_S变为HRP_M，备用防火墙命令行提示符前的前缀由HRP_M变为HRP_S。Ping测试观察存在丢包情况。

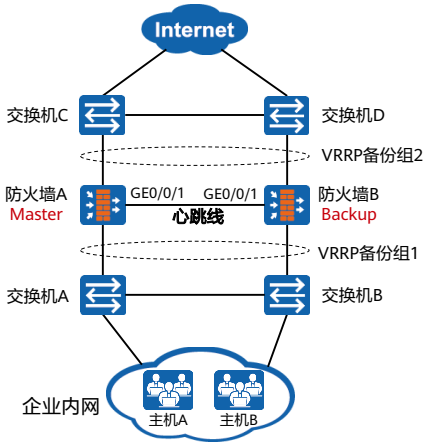
目录

故障一：HRP协议状态异常

- 故障现象：防火墙主备备份组网场景中，在防火墙A查看HRP运行状态，对端状态显示为“unknown”，如下：

```
HRP_M[NGFW] display hrp state
Role: active, peer: unknown (should be "active-standby")
Running priority: 47004, peer: unknown
Core state: abnormal(active), peer: unknown
Backup channel usage: 0%
Stable time: 0 days, 3 hours, 48 minutes
```

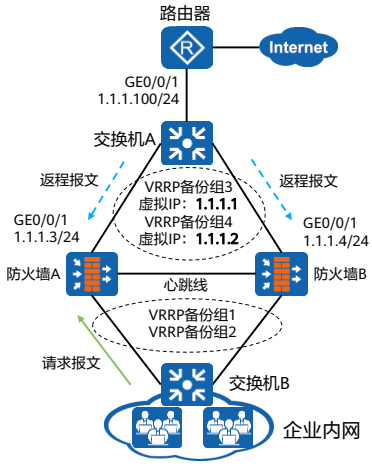
- 故障原因分析：
  - 对端设备没有开启双机热备功能。
  - 当前没有可用的备份通道。
- 解决措施：
  - 启用对端防火墙的双机热备功能。
  - 使用命令“display hrp interface”检查备份通道并修复。



HUAWEI

故障二：NAT场景中流量转发路径异常 (1)

- 组网描述：防火墙负载分担组网场景中，上下行链路均采用VRRP协议。
  - VRRP备份组1和备份组3中，防火墙A为Master，防火墙B为Backup；
  - VRRP备份组2和备份组4中，防火墙A为Backup，防火墙B为Master；
  - 防火墙A的NAT地址池为：1.1.1.5~1.1.1.10；
  - 防火墙B的NAT地址池为：1.1.1.11~1.1.1.15。
- 故障现象：路由器发送的返程报文时而到达防火墙A，时而达到防火墙B，影响业务的正常运行。



HUAWEI

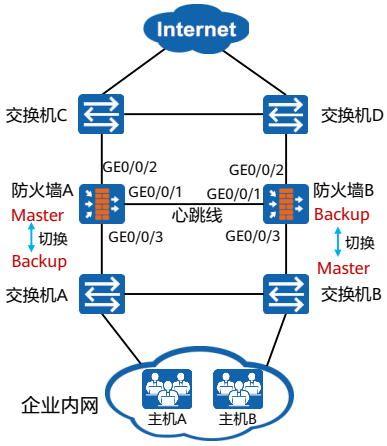
故障二： NAT场景中流量转发路径异常 (2)

- 故障原因分析：
  - 以VRRP备份组1为例，内网用户访问Internet的流量到达防火墙A后，源IP地址被NAT策略修改为公网地址（假设为1.1.1.5）；
  - 防火墙A会将NAT策略和NAT映射信息同步至防火墙B；
  - 路由器发送返程报文时，会发送ARP请求1.1.1.5的MAC地址，防火墙A、B均会响应，导致返程流量路径异常。
- 解决措施：
  - 需要在防火墙上将NAT地址池与VRRP备份组进行绑定：防火墙A的NAT地址池与VRRP备份组3绑定，防火墙B的NAT地址池与VRRP备份组4绑定。
  - 绑定后，仅有主用防火墙A会响应ARP请求，且响应的MAC地址为VRRP备份组3对应的虚拟MAC地址，所有返程流量只会转发至防火墙A。

- 由于系统会自动将处于同一地址网段的NAT地址池与VRID最小的VRRP备份组绑定，所以在主备备份方式下，一般不需要我们手工配置VRRP备份组与NAT地址池绑定。

故障三：防火墙主备切换频繁

- 故障现象：防火墙主备备份组网场景中，防火墙双机热备的状态反复切换，导致流量异常。
- 故障原因分析：
  - 防火墙业务接口状态异常，频繁UP/DOWN，导致主备切换频繁；
  - 主备防火墙的心跳报文发送间隔不一致。
- 解决措施：
  - 检查业务接口配置是否错误；
  - 若业务接口为光接口，检查光模块是否存在异常；
  - 检查防火墙心跳报文的发送间隔，并配置一致。



思考题

1. （判断题）防火墙心跳接口的连线方式可以是直连，也可以通过交换机或路由器连接。（　　）
   A. 正确
   B. 错误
2. （多选题）以下有关防火墙双机热备系统版本升级的描述，哪些选项是错误的？（　　）
   A. 系统升级通常在业务运行较少的时段进行
   B. 双机热备升级通常先升级Active设备，再升级Standby设备
   C. 双机热备升级前需要备份重要数据，如配置文件等
   D. 双机热备升级前不需要记录业务运行情况，因为业务每时每刻都不尽相同

1. A
2. BD

本章总结

- 本章节主要介绍了防火墙高可靠性技术，包括双机热备和链路高可靠性技术。其中链路高可靠性技术介绍了Eth-Trunk、IP-Link、BFD、Link-Group等。
- 此外还介绍了各类高可靠性技术常见的运维操作，如双机热备版本升级与常见故障排除。
- 通过本章课程的学习，您将进一步掌握对防火墙高可靠性技术的部署及运维操作，能够应对大中型企业网络的高可靠性需求。

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
ARP	Address Resolution Protocol	地址解析协议
BFD	Bidirectional Forwarding Detection	双向转发检测
HRP	Huawei Redundancy Protocol	华为冗余协议
ICMP	Internet Control Message Protocol	互联网控制报文协议
LACP	Link Aggregation Control Protocol	链路聚合控制协议
LAG	Link Aggregation Group	链路聚合组
MAC	Media Access Control	媒体接入控制
NO-PAT	No-port Address Translation	非端口地址转换
OSPF	Open Shortest Path First	开放式最短路径优先
PAT	Port Address Translation	端口地址转换

缩略语表 (2)

缩略语	英文全称	解释
POS	Packet Over SDH/SONET	基于SDH/SONET的包封装
USG	Unified Security Gateway	统一安全网关
VLAN	Virtual Local Area Network	虚拟局域网
VGMP	VRRP Group Management Protocol	VRRP组管理协议
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议
VPN	Virtual Private Network	虚拟专用网

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.

防火墙流量管理

HUAWEI

前言

- 传统网络业务在飞速发展，但是网络带宽不可能无限扩展。所以必要时管理员需要对带宽占用进行管理，保证高优先级的业务优先转发，降低低优先级业务的带宽占用。传统流量管理由于流量分类不够精细，无法对流量进行多层级管理，无法满足当前用户的需求。
- 华为防火墙流量管理技术，分为带宽管理和配额控制策略，能对业务流量进行精确识别和管理，同时提供多层级的带宽策略，适用于多种组织架构的部署。本课程将详细介绍流量管理技术。

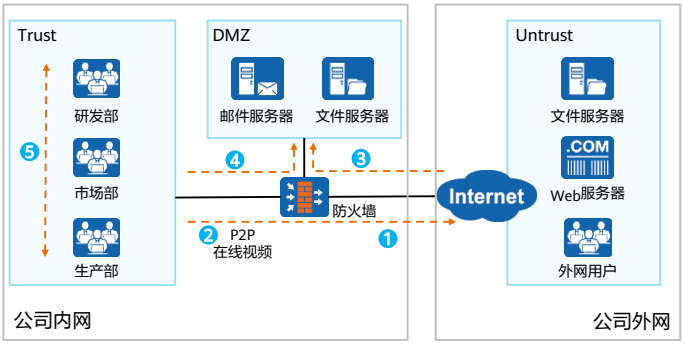
目标

- 学完本课程后，您将能够：
  - 描述带宽管理的应用场景
  - 描述带宽管理的基本原理
  - 描述配额控制策略的应用场景
  - 描述配额控制策略的基本原理
  - 掌握防火墙流量管理的配置

目录

带宽管理技术背景

- 防火墙作为大中型企业的出口网关，部署在网络边界处，对于出入的流量起到限制的作用。如果不合理的流量占用了大量的带宽，会给企业带来一系列问题。比如：无法访问服务器、工作效率低和导致服务器性能降低等情况。



1. 内网用户访问Internet时，需要大量带宽；
2. P2P类型的业务流量消耗了绝大部分的带宽资源；
3. 大量Internet用户访问内网服务器，导致服务器性能降低；
4. 大量的针对服务器的访问需求导致服务器无法正常工作；
5. 不同用户/部门之间无限制占用带宽资源，降低网络质量。

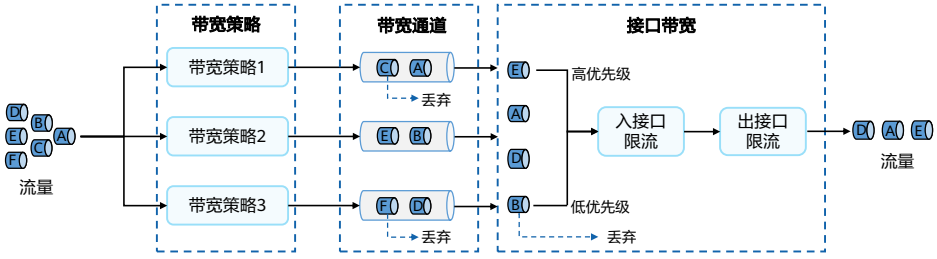
带宽管理简介

- 针对企业用户流量，防火墙提供了带宽管理功能，基于出/入接口、源/目的安全区域、源/目的地址、时间段和报文DSCP优先级等信息，对通过自身的流量进行管理和控制。
- 带宽管理提供带宽限制、带宽保证和连接数限制功能，可以提高带宽利用率，避免带宽耗尽。

带宽限制	带宽保证	连接数限制
• 限制网络中非关键业务占用的带宽，避免此类业务消耗大量带宽资源，影响其他业务。	• 保证网络中关键业务所需的带宽，当线路繁忙时，确保此类业务不受影响。	• 限制业务的连接数，有利于降低该业务占用的带宽，还可以节省设备的会话资源。

带宽管理处理流程

- 防火墙通过带宽策略、带宽通道和接口带宽来实现带宽管理功能。
  - 带宽策略：带宽策略定义了被管理的对象和动作，并引用带宽通道。
  - 带宽通道：带宽通道定义了被管理的对象所能够使用的带宽资源。
  - 接口带宽：接口带宽定义了接口入方向和出方向的实际带宽，出方向上的流量发生拥塞时，启用队列调度机制。

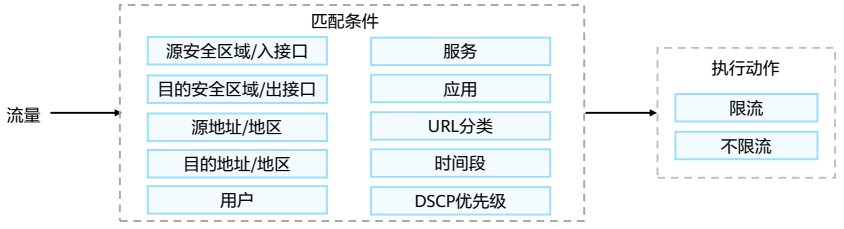


HUAWEI

- 带宽管理的整体处理流程如下：
  - 流量匹配带宽策略，经过带宽策略的分流后，进入相应的带宽通道进行处理。带宽通道的处理包括：
    - 丢弃超过了预先定义的最大带宽的流量。
    - 限制业务的连接数。
    - 标记流量的优先级，作为后续队列调度的依据。
  - 受入接口带宽的限制，如果流量大于入接口带宽，将根据带宽通道中设置的转发优先级对流量进行队列调度，保证高优先级的报文被优先发送。
  - 流量最终从出接口发送时，受出接口带宽的限制。如果流量大于出接口带宽，将根据转发优先级对流量进行队列调度，保证高优先级的报文被优先发送。

带宽策略规则

- 带宽策略决定了对网络中的哪些流量进行带宽管理，以及如何进行带宽管理。
- 带宽策略是多个带宽策略规则的集合，带宽策略规则由条件和动作组成：
  - 条件：防火墙匹配报文的依据。
  - 动作：防火墙对报文采取的处理方式，主要包括：
    - 限流：对符合条件的流量进行管理。当动作为限流时，需在带宽策略中引用带宽通道，对流量的具体管理措施由该带宽通道决定。
    - 不限流：对符合条件的流量不进行管理。

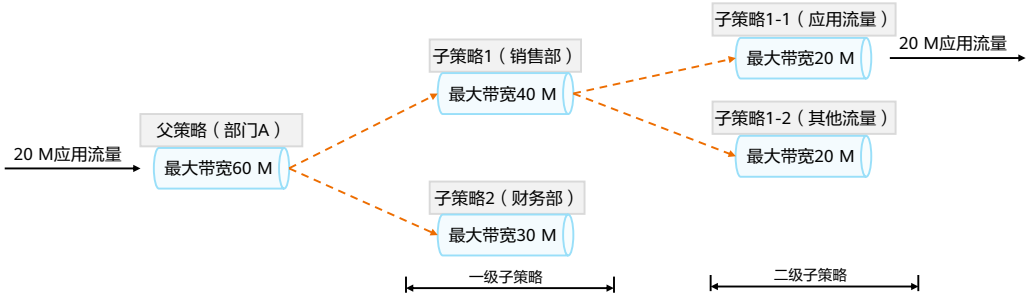


HUAWEI

- 默认情况下，防火墙上存在一条缺省的带宽策略，所有匹配条件均为任意（any），动作为不限流。若所有规则都没有匹配到，则按照缺省的带宽策略进行处理。

带宽策略类型

- 防火墙可配置多条带宽策略，主要分为同级策略和多级策略两种类型。
  - 同级策略：多条带宽策略之间相互独立。流量匹配多条同级策略是按照从上往下的顺序依次匹配，一旦匹配上一条策略的所有条件，会立即执行带宽通道的动作，不在继续匹配剩下的规则。
  - 多级策略：又称为父子策略，即一条带宽策略下可以配置多条带宽子策略。流量匹配多级策略时，先匹配父策略，再匹配子策略，直到匹配到最后一级可以匹配到的子策略为止。华为防火墙最多支持四级父子策略。



- 防火墙进行带宽限制时，配置多级策略能达到更好的带宽复用效果。（目前V6R7C20版本防火墙支持四级）
- 上图是一个20 M的应用流量匹配带宽策略时，过程如下：
  - 首先匹配父策略，发现小于父策略的最大带宽60 M，则继续匹配一级子策略；
  - 匹配一级子策略时，发现小于子策略1的最大带宽40 M，则继续匹配二级子策略；
  - 匹配二级子策略时，发现小于子策略1-1最大带宽20M，则流量全部通过，若应用流量大于20 M时，则将限速20 M。

带宽通道

- 流量匹配带宽策略后进入带宽通道，带宽通道定义了具体的带宽资源，是进行带宽管理的基础。
- 通过带宽通道，可以将物理的带宽资源从逻辑上划分为多个虚拟的带宽资源。带宽通道通过以下方面来对带宽资源进行限制，包括整体的保证带宽和最大带宽、每IP/每用户的最大带宽、连接数限制和DSCP优先级重标记等。此外，带宽通道还可以实现带宽资源的闲时复用。

- 整体的保证带宽和最大带宽：进入带宽通道的流量可获得的最小带宽资源和最大带宽资源。
- 每IP/每用户的保证带宽和最大带宽：在带宽通道中针对IP或用户设置的最小带宽和最大带宽，实现粒度更加细化的带宽限制。
- 连接数限制：防火墙通过限制自身生成的会话数量，来实现连接数限制功能。
- 上下行带宽独立控制和整体控制：在上面提到的最大带宽、保证带宽和连接数限制均支持上下行分别配置。在带宽通道中，上下行代表的含义跟带宽策略本身有关。
  - 流量传输方向与带宽策略同向时，定义为上行；
  - 与带宽策略反向时，定义为下行。
- DSCP优先级重标记：DSCP字段也称为DSCP优先级，是网络设备进行流量分类的依据。防火墙可以在带宽通道中对符合条件的报文修改其DSCP字段值，进而对不同DSCP优先级的流量采取差异化的处理。
- 带宽复用：多条流量进入同一个带宽通道后，带宽通道内的带宽资源可以实现动态分配。
- 流量转发优先级：防火墙支持为带宽通道配置流量转发优先级，不同的优先级对应着流量监管和流量整形两种不同的带宽限制方式。

带宽通道参数设置

- 带宽设置可以包含以下重要参数：
  - 整体的保证带宽和最大带宽；
  - 连每IP/每用户的保证带宽和最大带宽；
  - 上下行带宽独立控制和整体控制；
  - 连接数限制（并发连接总数限制和新建连接速率限制）。

HUAWEI

- 整体的保证带宽是指进入带宽通道的流量可获得的最小带宽资源，整体的最大带宽是指进入带宽通道的流量可获得的最大带宽资源。流量进入带宽通道后，防火墙将当前流量与带宽通道中设置的保证带宽/最大带宽进行比较，采取不同的处理方式：
  - 如果流量小于保证带宽，这部分流量在出接口发送环节能够确保被转发。
  - 如果流量大于最大带宽，则直接丢弃超出最大带宽的流量。
  - 超出保证带宽的流量，在出接口发送环节将会与其它带宽通道中同类型的流量自由竞争带宽资源。带宽通道的优先级越高，就会更优先获得剩余带宽资源。获得带宽资源后发送流量，否则丢弃流量。
- 每IP/每用户的保证带宽和最大带宽：除了设置整体的保证带宽和最大带宽之外，还可以在带宽通道中定义针对IP或用户的保证带宽和最大带宽，实现粒度更加细化的带宽限制。
  - 当带宽通道被带宽策略引用后，防火墙会基于IP地址或用户，对符合带宽策略匹配条件的流量进行统计，每IP/每用户的保证带宽和最大带宽的作用与整体带宽类似，只是作用范围细化至每IP/用户范围。
  - 防火墙还提供了基于整体最大带宽和在线IP/用户数量，为每一个IP/用户实现带宽动态均分的控制方式，充分利用闲置带宽的同时，还保证了带宽使用的公平性。

- 连接数限制：通信双方建立的连接在防火墙上体现为会话，一条会话对应一个连接。防火墙通过限制自身生成的会话数量，来实现连接数限制功能，主要作用包括：
    - P2P业务会产生大量的连接，限制其连接数有利于减少P2P业务的流量，降低带宽占用。
    - 在部署了内网服务器的场景中，连接数限制功能可以辅助防火墙防范针对内网服务器的DDoS（Distributed Denial Of Service）攻击。
    - 节省防火墙上的会话资源。
- 带宽通道中可以配置整体的最大连接数，也可以配置针对源IP或用户的最大连接数，实现更加细化的连接数限制。
- 上下行带宽独立控制和整体控制：在上面提到的最大带宽、保证带宽和连接数限制均支持上下行分别配置。在带宽通道中，上下行代表的含义跟带宽策略本身有关：流量传输方向与带宽策略同向时，定义为上行；与带宽策略反向时，定义为下行。换言之，流量命中带宽策略，定义为上行流量；将带宽策略中的源和目的互换进行反向查询，命中的流量定义为下行流量。
- 例如，如果需要限制Trust到Untrust的流量，可以有以下两种方式：
    - 带宽策略的源区域为Trust，目的区域为Untrust，带宽通道中配置对上行带宽进行管控（与带宽策略同向）。
    - 带宽策略的源区域为Untrust，目的区域为Trust，带宽通道中配置对下行带宽进行管控（与带宽策略反向）。
- 此外，除了上下行带宽独立控制这种细粒度的管控方式，防火墙还提供了基于上行和下行流量之和的带宽管控方式，大大增加了管理的灵活度。

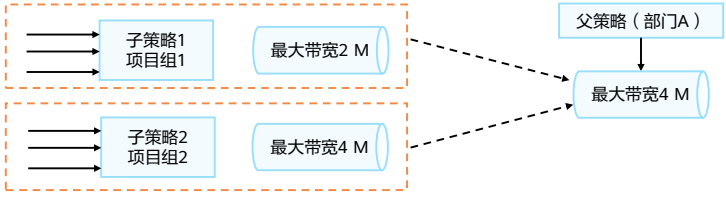
工作方式

- 带宽通道被带宽策略引用后，整体最大带宽、整体保证带宽和整体最大连接数就会在带宽策略中起作用，其工作方式包括两种：

策略独占	策略共享
• 每一个引用带宽通道的带宽策略都独自受到该带宽通道的约束，即符合该带宽策略匹配条件的流量，独享最大带宽资源。	• 所有引用带宽通道的带宽策略都共同受到该带宽通道的约束，即符合多条带宽策略匹配条件的流量，共享最大带宽资源。

带宽复用

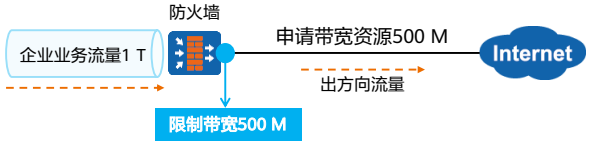
- 带宽复用是带宽通道的重要特征，指的是多条流量进入同一个带宽通道后，带宽通道内带宽资源的动态分配方式。当带宽通道中某一条流量没有使用带宽资源时，该空闲的带宽资源可以借给其它流量使用；如果有流量需要使用带宽资源时，可以压缩其它流量的带宽，从而将带宽资源抢占回来。
- 带宽复用包括下面几种情况：
  - 多条流量匹配到了同一个带宽策略，多条流量之间可以实现带宽复用。
  - 多个带宽策略以策略共享的方式引用带宽通道，则匹配了带宽策略的多条流量之间可以实现带宽复用。
  - 匹配了父子策略中的多个子策略的多条流量之间可以实现带宽复用。



- 在进行带宽限制时使用多级策略，与使用独立的带宽策略相比，可以达到更好的带宽复用效果。
- 例如，部门A中包括两个项目组：项目组1和项目组2，使用父策略限制部门A的最大带宽，同时使用两条子策略限制两个项目组的最大带宽。假设项目组2（子策略2）只有2 M流量，项目组1（子策略1）就可以复用部门A（父策略）中剩余的2 M带宽资源。如果不使用多级策略，而使用两条引用了不同带宽通道的独立的带宽策略，这两条带宽策略之间无法共用带宽通道，两个项目组之间也就无法实现带宽资源的复用。

接口带宽原理

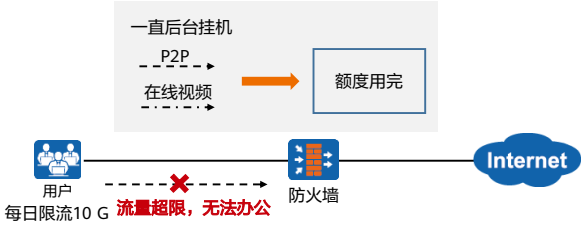
- 防火墙作为大中型企业的出口网关时，企业向运营商申请的带宽资源一般都小于防火墙出接口的物理带宽。如果防火墙无法感知出接口上所能够使用的最大带宽资源，导致发出去的流量到达对端设备后产生拥塞，严重的话将会造成丢包。
- 通过配置接口出方向上的带宽限制功能，可以使出接口的实际带宽与运营商所提供的带宽资源相匹配。当流量超过接口可以使用的实际带宽时，防火墙可以感知拥塞，触发队列调度机制，优先转发关键业务的流量。此外，也可以配置接口入方向上的实际带宽，当防火墙接收其它设备发送的流量时，限制进入接口的流量，防止内部服务器压力过大导致性能降低。



目录

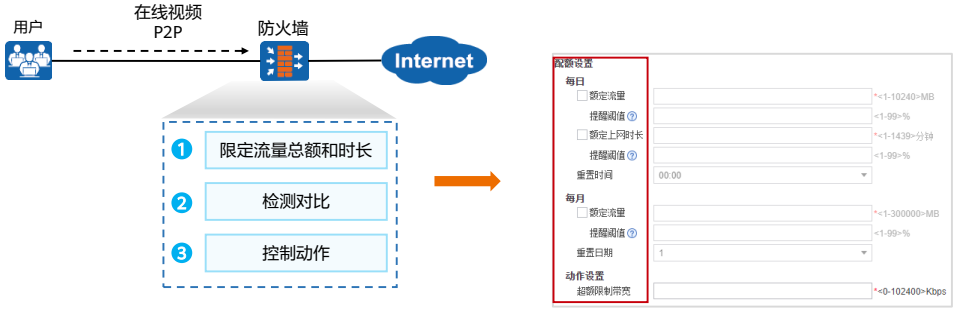
配额控制策略概述

- 带宽管理配置可以解决前面提到的绝大数问题，但是针对娱乐流量依然会存在以下问题：
  - 由于P2P下载、在线视频等应用的存在，使得少数员工占用了企业几乎全部的带宽资源，导致关键业务无法开展。
  - 对于某些通过流量与ISP结算费用的企业来说，P2P下载、在线视频这些应用，采用传统限制带宽的方式，已经无法应对长时间挂机下载、缓冲等逃避方案。
  - 另外员工利用互联网，长时间进行一些娱乐活动，也严重影响了工作效率。



配额控制策略原理

- 配额控制策略用于控制用户的上网流量和上网时间，可以有效防止带宽滥用、上网时间过长影响工作效率等问题。其中，配额控制策略包括检测和控制两部分。
  - 检测：实时检测上网流量和时长，并与用户的上网配额进行比较，比较结果会作为控制的依据。
  - 控制：包括直接阻断和限制最大带宽。



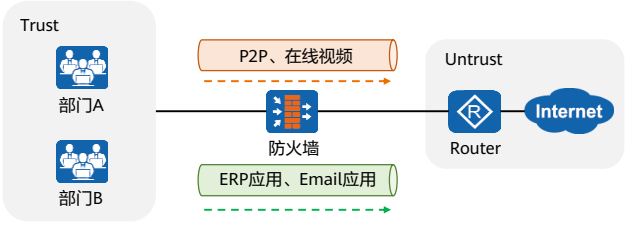
HUAWEI

- 管理员可以为用户提供三种配额分配方式，方便多元化管理。
  - 每日流量配额：限定用户每日上网流量总额；
  - 每月流量配额：限定用户每月上网流量总额；
  - 每日上网时长配额：限定用户每日的上网时长总额。

目录

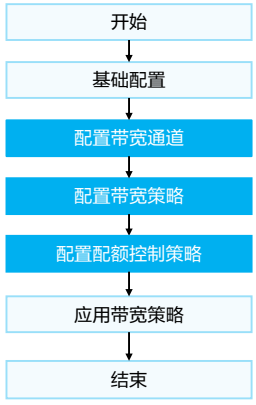
流量管理配置举例 (1)

- 需求描述：
  - 企业在ISP处购买了100 M带宽，要求部门A的下行最大带宽不超过60 M，部门B的下行最大带宽不超过40 M；
  - 部门A和部门B的P2P下行最大带宽不超过30 M，要计算到各自部门的总带宽中；为了更好的控制P2P、在线视频流量，可以通过限制连接数的方式，限制最大连接数不超过10000；同时为了提高员工工作效率，每位用户P2P、在线视频每月流量累计最高15 G；
  - 为了让Email、ERP等应用在正常工作时间内不受到影响，此类流量可获得的最小带宽不少于30 M，要计算到各自部门的总流量中。



流量管理配置举例 (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；
  - 配置基于公司要求，限制各个部门下行的最大带宽；
  - 配置基于P2P、在线视频应用的带宽策略，并引用整体最大带宽为30 Mbps、整体最大连接数为10000的带宽通道；
  - 配置Email、ERP应用的带宽，设置保证带宽；
  - 配置配额控制策略，限制用户每月P2P流量。



部门带宽限制 - 配置带宽通道

- 为部门A配置带宽通道：选择“策略 > 带宽管理 > 带宽通道”，单击“新建”，按如图参数配置。

HUAWEI

- 同理，需要为部门B配置带宽通道。

部门带宽限制 - 配置带宽策略

- 针对部门A进行带宽管理：选择“策略 > 带宽管理 > 带宽策略”，单击“新建”，按如图参数配置。

HUAWEI

- 同理，也需要为部门B配置带宽策略。

P2P带宽限制 - 配置带宽通道

- 为部门A和部门B的P2P应用配置带宽通道：选择“策略 > 带宽管理 > 带宽通道”，单击“新建”，按如图参数配置。

P2P带宽限制 - 配置带宽策略

- 针对部门A的P2P应用进行带宽管理：选择“策略 > 带宽管理 > 带宽策略”，单击“新建”，按如下参数配置。

HUAWEI

- 同理，也需要为部门B配置针对P2P应用的带宽策略。
- 说明：此处统一用了基于P2P的应用作为例子，具体配置时请根据实际需求指定应用。

Email、ERP应用带宽限制 - 配置带宽通道

- 为Email、ERP应用配置时间段。
- 为Email、ERP应用配置相应的带宽通道： 选择“策略 > 带宽管理 > 带宽通道”；单击“新建”，按如图参数配置。

Email、ERP应用带宽限制 - 配置带宽策略

- 针对Email、ERP应用进行带宽管理：选择“策略 > 带宽管理 > 带宽策略”，单击“新建”，按如图参数配置。

HUAWEI

- 说明：此处仅给出了Outlook Web Access、LotusNotes两种应用作为例子，具体配置时请根据实际需求指定应用。

配额控制策略

- 针对用户组的所有用户配置配额控制策略：选择“策略 > 配额控制策略”，单击“新建”，按如图参数配置。

思考题

1. （判断题）带宽管理中保证带宽可以大于最大带宽。（　　）
   A. 对
   B. 错
2. （多选题）带宽策略规则由条件和动作组成，以下哪些属于带宽策略规则的匹配条件？（　　）
   A. 源安全区域/入接口
   B. 用户
   C. 服务
   D. 时间段

1. B
2. ABCD

本章总结

- 本章内容主要介绍了带宽管理的基本概念和处理流程，包括带宽策略、带宽通道和接口带宽。然而在特殊场景下，带宽管理可能无法满足企业的需求，可以使用配额控制策略进行用户流量限制。
- 通过本课程的学习，您将掌握防火墙流量管理的基本配置，帮助用户更加精准的识别业务和进行流量管理。

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
DDoS	Distributed Denial of Service	分布式拒绝服务
DMZ	Demilitarized Zone	半信任区
DSCP	Differentiated Services Code Point	区分服务编码点
ERP	Enterprise Resource Planning	企业资源计划
IP	Internet Protocol	互联网协议
ISP	Internet service provider	网络服务供应商
P2P	Peer to Peer	点对点
URL	Uniform Resource Locator	统一资源定位符

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.

防火墙虚拟系统

HUAWEI

前言

- 随着网络规模的扩大，企业的网络环境越来越复杂。对于有业务和应用隔离需求的用户来说，传统的物理网络隔离方案已经无法满足需求，比如：管理分散、安全策略部署难以及无法提供统一的应用服务等。因此，为了满足业务和应用隔离需求的同时又节约投资成本，提出使用单个网关作为多个网关的概念，此时虚拟系统技术应运而生。
- 本章将介绍防火墙虚拟化技术的相关应用及基本原理。

目标

- 学完本课程后，您将能够：
  - 描述虚拟系统的应用场景
  - 描述虚拟系统的基本概念
  - 掌握防火墙虚拟系统的配置

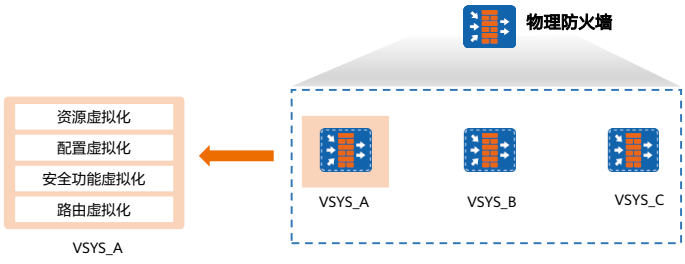
目录

虚拟化概述

- 虚拟化（Virtualization）的含义很广泛。将任何一种形式的资源抽象成另一种形式，都可以称为虚拟化。虚拟化是资源的逻辑表示，使资源的分配不受物理限制。
- 虚拟化使得在一台物理的服务器上可以跑多台虚拟机，虚拟机共享物理机的CPU、内存、I/O硬件资源，但逻辑上虚拟机之间是相互隔离的。虚拟化可以达到节省硬件成本、能耗和空间的目的。

防火墙虚拟系统

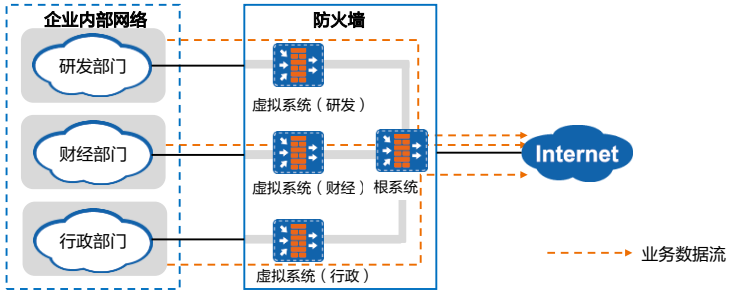
- 防火墙虚拟系统是指将一台物理防火墙设备从逻辑上划分为多个虚拟系统。虚拟系统之间相互独立，有自己的接口、地址集、用户/用户组、路由表项以及策略，并可通过虚拟系统的管理员进行配置和管理。



- 为了实现每个虚拟系统的业务都能够做到正确转发、独立管理和相互隔离，防火墙主要实现了以下方面的虚拟化：
  - 资源虚拟化：每个虚拟系统都有独享的资源，包括接口、VLAN、策略和会话等。根系统管理员分配给每个虚拟系统，由各个虚拟系统自行管理和使用。
  - 配置虚拟化：每个虚拟系统都拥有独立的虚拟系统管理员和配置界面，每个虚拟系统管理员只能管理自己所属的虚拟系统。
  - 安全功能虚拟化：每个虚拟系统都可以配置独立的安全策略及其他安全功能，只有属于该虚拟系统的报文才会受到这些配置的影响。
  - 路由虚拟化：每个虚拟系统都拥有各自的路由表，相互独立隔离。目前仅支持静态路由的虚拟化。
- 通过以上几个方面的虚拟化，当创建虚拟系统之后，一台物理防火墙上划分出多台相互独立的逻辑设备，每个虚拟系统的管理员都像在使用一台独占的设备。

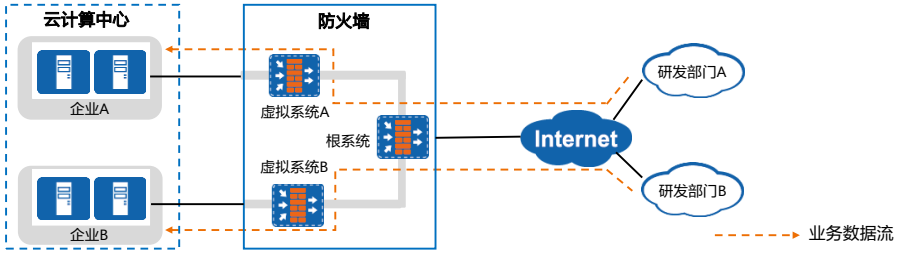
防火墙虚拟系统应用场景 - 大中型企业网络隔离

- 通常大中型企业中网络设备的数量众多，网络环境复杂。随着企业业务规模的不断增大，各业务部门的职能和权责划分也越来越清晰，每个部门都会有不同的安全需求。这将导致防火墙的配置异常复杂，管理员操作容易出错。通过防火墙的虚拟化技术，可以在实现网络隔离的基础上，使得业务管理更加清晰和简便。
- 如图所示，企业内部网络通过防火墙的虚拟系统将网络隔离为研发部门、财经部门和行政部门。不同部门的管理员权限区分明确，各部门之间可以根据权限互相访问。



防火墙虚拟系统应用场景 - 云计算的安全网关

- 新兴的云计算技术，其核心理念是将网络资源和计算能力存放于网络云端。网络用户只需通过终端接入公有网络，就可以访问相应的网络资源。在这个过程中，不同用户之间的流量隔离、安全防护和资源分配是非常重要的一环。通过配置虚拟系统，就可以让部署在云计算中心出口的防火墙具备云计算网关的能力，对用户流量进行隔离的同时提供强大的安全防护能力。
- 如图所示，企业A和企业B分别在云计算中心放置了服务器。防火墙作为云计算中心出口的安全网关，能够隔离不同企业的网络及流量，并根据需求进行安全防护。



目录

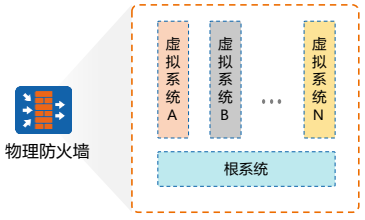
虚拟系统特点

- 防火墙实现将资源、配置、安全功能和路由方面虚拟化后，使虚拟系统的业务能够正确转发，相互隔离。因此，虚拟系统具备以下特点：

管理独立	资源分配	流量隔离	配置独立
• 每个虚拟系统由独立的管理员进行管理，使得多个虚拟系统的管理更加清晰简单，所以非常适合大规模的组网环境。	• 可以为每个虚拟系统分配固定的系统资源，保证不会因为一个虚拟系统的业务繁忙而影响其他虚拟系统。	• 虚拟系统之间的流量相互隔离，更加安全。在需要的时候，虚拟系统之间也可以进行安全互访。	• 每个虚拟系统拥有独立的配置及路由表项，这使得虚拟系统下的局域网即使使用了相同的地址范围，仍然可以正常进行通信。

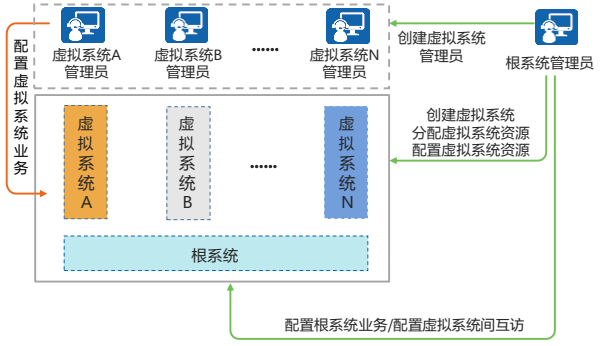
虚拟系统类型

- 防火墙上存在根系统和虚拟系统两种类型的虚拟系统。
  - 根系统（Public）
    - 根系统是防火墙上缺省存在的一个特殊的虚拟系统。即使虚拟系统功能未启用，根系统也依然存在。此时，管理员对防火墙进行配置等同于对根系统进行配置。启用虚拟系统功能后，根系统会继承先前防火墙上的配置。
    - 在虚拟系统这个特性中，根系统的作用是管理其他虚拟系统，并为虚拟系统间的通信提供服务。
  - 虚拟系统（VSYS）
    - 虚拟系统是在防火墙上划分出来的、独立运行的逻辑设备。



虚拟系统管理

- 虚拟系统的管理和配置是相互独立的，所对应的管理员也是不同的。根据虚拟系统的类型，管理员分为根系统管理员和虚拟系统管理员。两类管理员的作用范围和功能都不相同。



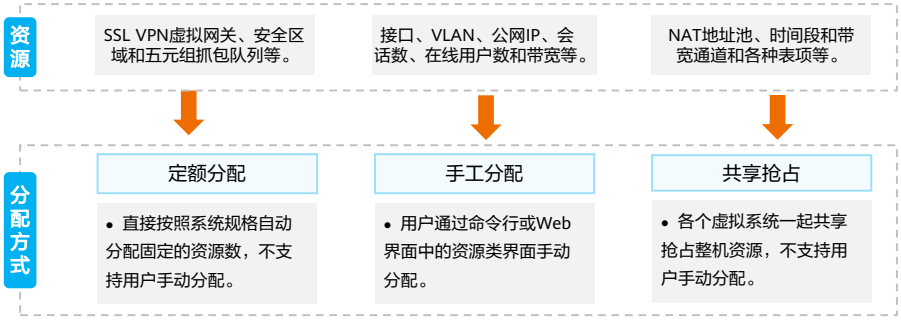
HUAWEI

- 根系统管理员
  - 启用虚拟系统功能后，设备上已有的管理员将成为根系统的管理员。管理员的登录方式、管理权限、认证方式等均保持不变。根系统管理员负责管理和维护设备、配置根系统的业务。
  - 只有具有虚拟系统管理权限的根系统管理员（本章节后续内容中提及的根系统管理员都是指此类管理员）才可以进行虚拟系统相关的配置，如创建、删除虚拟系统，为虚拟系统分配资源等。
- 虚拟系统管理员
  - 创建虚拟系统后，根系统管理员可以为虚拟系统创建一个或多个管理员。虚拟系统管理员的作用范围与根系统管理员有所不同：虚拟系统管理员只能进入其所属的虚拟系统的配置界面，能配置和查看的业务也仅限于该虚拟系统；根系统管理员可以进入所有虚拟系统的配置界面，如有需要，可以配置任何一个虚拟系统的业务。
  - 为了正确识别各个管理员所属的虚拟系统，虚拟系统管理员用户名格式统一为“管理员名@@虚拟系统名”。

目录

资源分配

- 合理地分配资源可以对单个虚拟系统的资源进行约束，避免因某个虚拟系统占用过多的资源，导致其他虚拟系统无法获取资源或业务无法正常运行。
- 防火墙实现虚拟系统业务的基础资源支持定额分配和手工分配；此外，其他资源使用共享抢占方式进行资源分配。不同资源采用不同的分配方式。

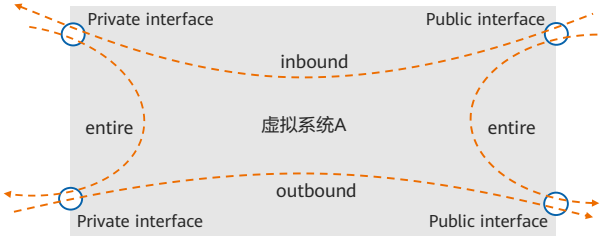


HUAWEI

- 管理员为虚拟系统手工分配资源时，首先需要配置资源类，并在资源类中指定各个资源项的保证值和最大值，然后将资源类与虚拟系统绑定。虚拟系统可以使用的资源数量受资源类中配置的保证值和最大值控制。
  - 保证值：虚拟系统可使用某项资源的最小数量。这部分资源一旦分配给虚拟系统，就被该虚拟系统独占。
  - 最大值：虚拟系统可使用某项资源的最大数量。虚拟系统可使用的资源能否达到最大值视其他虚拟系统对该项资源的使用情况而定。
- 如果虚拟系统不绑定资源类，则虚拟系统的资源不受限制，虚拟系统和根系统以及其他未绑定资源类的虚拟系统一起共同抢占整机的剩余资源。
- 如果虚拟系统绑定的资源类对某些资源项未指定最大值和保证值，则虚拟系统的这些资源项不受限制，虚拟系统和根系统以及其他未限定该资源项的虚拟系统一起共同抢占整机的剩余资源。
- 分配公网IP地址时，需要遵循以下几项原则：
  - 在exclusive模式下，一个公网IP地址只能被分配给一个虚拟系统；在free模式下，一个公网IP地址可以被分配给多个虚拟系统；
  - 公网IP地址不能与根系统上的NAT Server功能中的Global地址冲突；
  - 公网IP地址不能与根系统上的NAT地址池冲突。

手工分配 – 带宽资源

- 带宽资源主要是指网络中关键业务所需的带宽。在防火墙中可通过手工分配的方式设置，避免线路繁忙时，关键业务受影响。
- 带宽资源分为入方向带宽、出方向带宽和整体带宽三类。一条数据流是受哪类带宽资源限制与流量的出接口或入接口有关。



HUAWEI

- 如图所示，虚拟系统A有两个公网接口和两个私网接口。虚拟系统A入方向流量、出方向流量和整体流量如下：
  - 入方向（inbound）流量：从公网接口流向私网接口的流量，受入方向带宽的限制。
  - 出方向（outbound）流量：从私网接口流向公网接口的流量，受出方向带宽的限制。
  - 整体（entire）流量：虚拟系统的全部流量 = 入方向流量 + 出方向流量 + 私网接口到私网接口的流量 + 公网接口到公网接口的流量。整体流量受整体带宽的限制。
- 此处的公网接口并不是特指防火墙连接Internet的接口。而是指接口下配置了set public-interface命令的接口。私网接口则是指未配置set public-interface的接口。
- 在跨虚拟系统转发的场景中，Virtual-if接口默认为公网接口。

目录

虚拟系统的分流

- 报文进入防火墙后，先确定报文与虚拟系统的归属关系，若防火墙配置了虚拟系统，则报文仅根据虚拟系统内的策略和表项对报文进行处理；若未配置虚拟系统，则直接根据根系统的策略和表项处理。
- 分流是指确定报文与虚拟系统归属关系的过程。防火墙通过分流将进入设备的报文送入正确的虚拟系统处理，分流方式有以下三种：

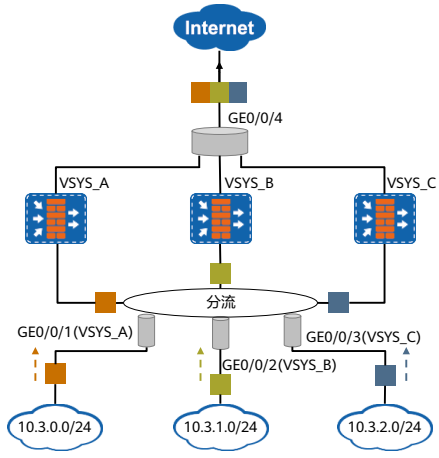
基于接口	接口工作在三层时，采用基于接口的分流方式。
基于VLAN	接口工作在二层时，采用基于VLAN的分流方式。
基于VNI	虚拟系统和VXLAN结合使用时，采用基于VNI的分流方式。

- 本文对基于VNI的分流方式不做详细介绍。

基于接口的虚拟系统分流

- 将接口与虚拟系统绑定后，该接口接收到的报文将根据虚拟系统配置进行处理。
- 如图所示，将防火墙的接口按照下列表格和虚拟系统绑定后，虚拟系统从各自绑定的接口收到报文会分别送入对应的系统中进行路由查找和策略处理。

接口	虚拟系统
GE0/0/1	VSYS_A
GE0/0/2	VSYS_B
GE0/0/3	VSYS_C



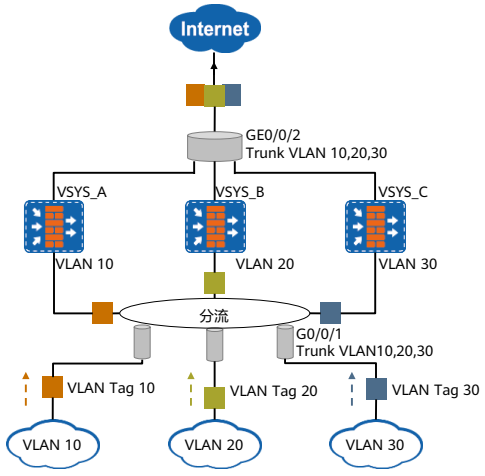
HUAWEI

- 注意：设备管理口GE0/0/0无法作为业务口，分配给虚拟系统。

基于VLAN的虚拟系统分流

- 将VLAN与虚拟系统绑定后，该VLAN内的报文都将被送入与其绑定的虚拟系统进行处理。
- 如图所示，将防火墙的VLAN和对应的虚拟系统绑定后，流量可以根据所属的VLAN判断属于哪个虚拟系统。然后再根据该虚拟系统的MAC地址表查询出接口，确定报文出入接口的域间关系，最后查找域间策略对报文进行转发或丢弃。

VLAN	虚拟系统
VLAN 10	VSYS_A
VLAN 20	VSYS_B
VLAN 30	VSYS_C



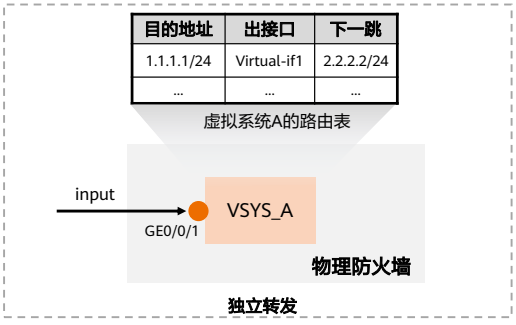
HUAWEI

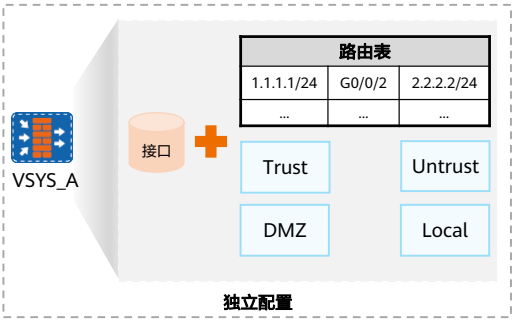
- 接口可以通过不同VLAN的流量，而不同流量又属于不同的虚拟系统，因此基于VLAN的分流时，二层接口不属于任何虚拟系统。

目录

虚拟系统的独立配置

- 将虚拟系统视为一台真实的防火墙，这台防火墙不仅有着独立的管理员账号，还有着独立的配置界面。将虚拟系统和物理防火墙的接口绑定后，从划分的接口接收的流量会按照虚拟系统的配置以及独立的路由表项进行数据转发。
- 使用**switch vsys *vsys-name***命令，用来从根系统的系统视图切换到指定的虚拟系统的用户视图。





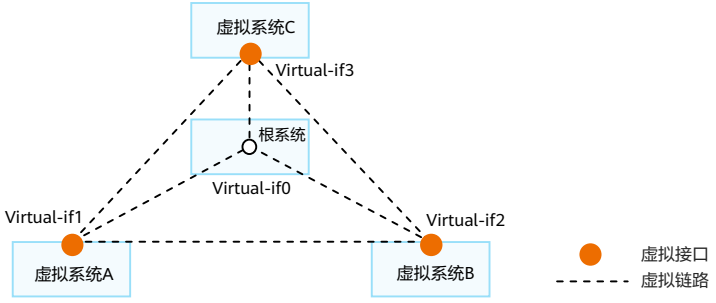
HUAWEI

- 虚拟系统同样可以有各自的安全区域、路由表和不同的接口。

目录

虚拟接口

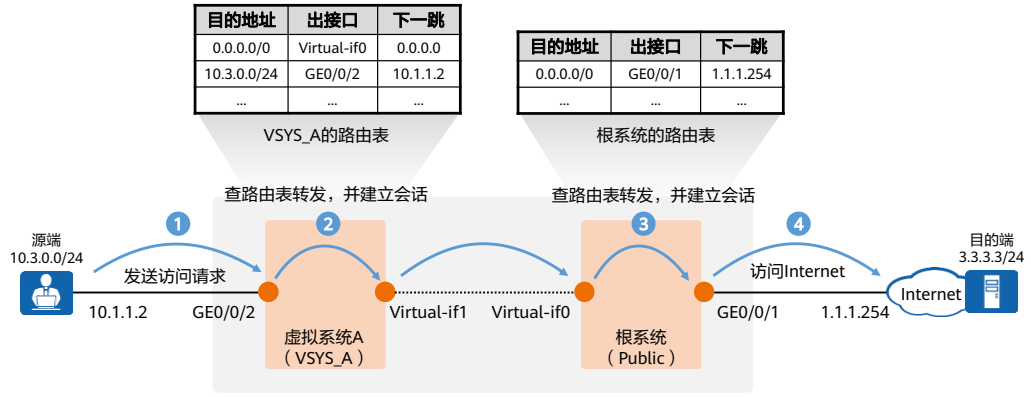
- 虚拟系统之间通过虚拟接口实现互访。虚拟接口是创建虚拟系统时系统自动为其创建的一个逻辑接口，作为虚拟系统自身与其他虚拟系统之间通信的接口。
- 虚拟接口名的格式为“Virtual-if + 接口号”，根系统的虚拟接口名为Virtual-if0，其他虚拟系统的Virtual-if接口号从1开始，根据系统中接口号占用情况自动分配。



- 虚拟接口的链路层和协议层始终是UP的。在虚拟系统互访场景下，虚拟接口必须配置IP地址并加入安全区域，否则无法正常工作。
- 各个虚拟系统以及根系统的虚拟接口之间默认通过一条“虚拟链路”连接。如果将虚拟系统、根系统都视为独立的设备，将虚拟接口视为设备之间通信的接口，通过将虚拟接口加入安全区域并按照配置一般设备间互访的思路配置路由和策略，就能实现虚拟系统和根系统的互访、虚拟系统之间的互访。

虚拟系统与根系统互访 - 虚拟系统访问根系统

- 虚拟系统与根系统互访有两种场景：虚拟系统访问根系统、根系统访问虚拟系统。这两种场景下，报文转发的流程略有不同。如图所示，该场景是虚拟系统访问根系统的流程。



HUAWEI

- 虚拟系统A下10.3.0.0/24网段的用户通过根系统的公网接口GE0/0/1访问Internet服务器3.3.3.3，详细流程如下：
  - 客户端向服务器发起连接。
  - 首包到达防火墙后，基于接口分流，被送入虚拟系统A。虚拟系统A按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等。如果虚拟系统A不允许转发报文，则丢弃报文，流程结束；如果虚拟系统A允许转发报文，则将报文送入根系统中处理。同时，虚拟系统A会为这条连接建立会话。
  - 根系统的虚拟接口Virtual-if0收到报文后，根系统按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等。如果根系统不允许转发报文，则丢弃报文，流程结束；如果根系统允许转发报文，则将报文发往服务器。同时，根系统会为这条连接建立会话。
  - 报文经过路由转发后，到达目的服务器。
- 需要注意的是因为虚拟系统和根系统都需要按照防火墙转发流程对报文进行处理，所以虚拟系统和根系统中要分别完成策略、路由等配置。

虚拟系统访问根系统的路由配置

- 虚拟系统配置：
  - 配置去程路由，即到Internet的路由。

    ```
    [FW-VSYS_A] ip route-static 0.0.0.0 0.0.0.0 public
    ```

    因为报文要经过根系统发送到Internet，所以要配置虚拟系统到根系统的路由。虚拟系统到根系统的路由只能是静态路由。和一般的静态路由不同，这条静态路由不需要配置下一跳或者出接口，而是要指定目的虚拟系统为根系统。
  - 配置回程路由，即到内网的路由。可以是动态路由（如OSPF），也可以是静态路由。

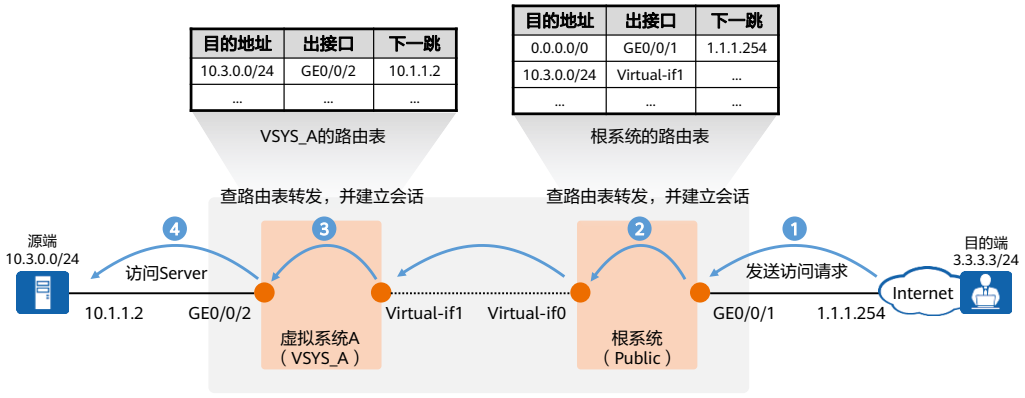
    ```
    [FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.2
    ```
- 根系统配置：
  - 配置去程路由，即到Internet的路由。可以是动态路由（如OSPF），也可以是静态路由。

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

    需要注意的是根系统中不需要针对服务器回应的报文配置回程路由。服务器回应的报文在根系统中匹配会话表后，直接发送到虚拟系统中处理。这点和同虚拟系统内转发场景下路由的配置有所不同。

虚拟系统与根系统互访 - 根系统访问虚拟系统

- 如图所示，该场景是公网用户通过根系统的公网接口GE0/0/1访问虚拟系统VSYS_A下的服务器。报文先进入根系统处理，然后再进入虚拟系统处理。



HUAWEI

- 公网用户通过根系统的公网接口GE0/0/1访问虚拟系统A下的服务器，详细流程如下：
  - 客户端向服务器发起连接。
  - 首包到达防火墙后，防火墙按照转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等。如果根系统不允许转发报文，则丢弃报文，流程结束；如果根系统允许转发报文，则根据路由表对应的出接口转发给虚拟系统A。同时，根系统会为这条连接建立会话。
  - 虚拟系统的虚拟接口Virtual-if1收到报文后，虚拟系统按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等。如果虚拟系统A不允许转发报文，则丢弃报文，流程结束；如果虚拟系统A允许转发报文，则将报文发往服务器。同时，虚拟系统会为这条连接建立会话。
  - 报文经过路由转发后，到达目的服务器。

根系统访问虚拟系统的路由配置

- 根系统系统配置：
  - 配置去程路由，即到内网服务器的路由。

    ```
    [FW] ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
    ```

    因为报文要经过虚拟系统发送到服务器，所以要配置根系统到虚拟系统的路由。根系统到虚拟系统的路由只能是静态路由。和一般的静态路由不同，这条静态路由不需要配置下一跳或者出接口，而是要指定目的虚拟系统为服务器所在虚拟系统。
  - 配置回程路由，即到Internet的路由。可以是动态路由（如OSPF），也可以是静态路由。

    ```
    [FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
    ```
- 虚拟系统配置：
  - 配置去程路由，即到Internet的路由。可以是动态路由（如OSPF），也可以是静态路由。

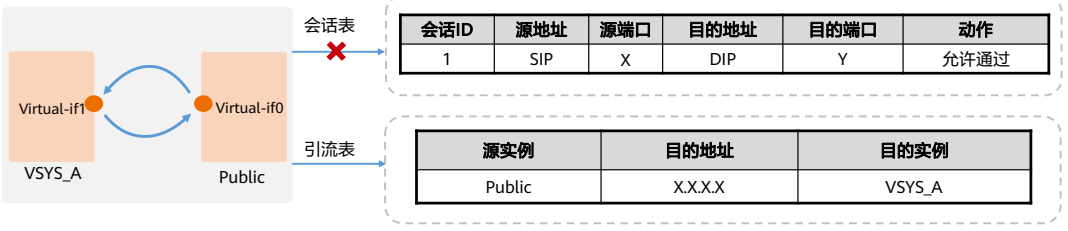
    ```
    [FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.2
    ```

    需要注意的是虚拟系统中不需要针对服务器回应的报文配置回程路由。服务器回应的报文在虚拟系统中匹配会话表后，直接发送到根系统中处理。这点和同虚拟系统内转发场景下路由的配置有所不同。

- 需要注意的是为了让公网用户能够访问私网的服务器，必须在VSYS_A或根系统中配置NAT Server，进行公网地址和私网地址的转换。
  - 如果在根系统中配置NAT Server，根系统先将报文的目的地址由公网地址转换为私网地址，然后再查路由。因此，根系统中配置路由时，目的地址应配置为服务器的私网地址。
  - 如果在虚拟系统中配置NAT Server，根系统将报文转发给虚拟系统，虚拟系统将报文的目的地址由公网地址转换为私网地址。因此，根系统中配置路由时，目的地址应配置为服务器的公网地址。

引流表概述

- 在虚拟系统和根系统互访的场景中，虚拟系统和根系统都会按照防火墙转发流程对报文进行处理。针对互访的业务，虚拟系统和根系统都要配置策略和建立会话。这样，一方面增加了配置的复杂性，另一方面，每条连接都需要两条会话，业务量大时，会造成整机的会话资源紧张。
- 当配置引流表时，引流表中记录的是IP地址和虚拟系统的归属关系。若报文命中引流表，根系统无需建立会话，直接按照路由表或引流表转发报文，从而避免以上问题。



会话ID	源地址	源端口	目的地址	目的端口	动作
1	SIP	X	DIP	Y	允许通过

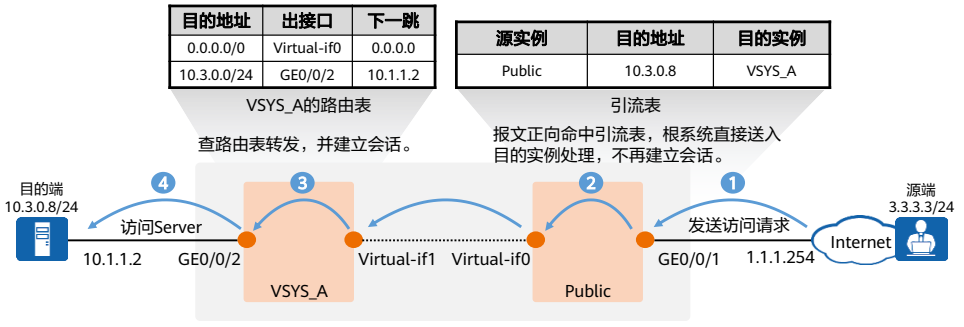
源实例	目的地址	目的实例
Public	X.X.X.X	VSYS_A

HUAWEI

- 引流表包括源虚拟系统、目的地址、目的虚拟系统。

引流表 - 正向命中

- 报文命中引流表分为正向命中和反向命中两种情况。
- 正向命中：根系统发往虚拟系统的报文，**目的地址**匹配引流表中的“Destination Address”，则报文正向命中引流表。报文正向命中引流表时，根系统按引流表转发报文，将报文送入命中的表项对应的“Destination Instance”中处理。

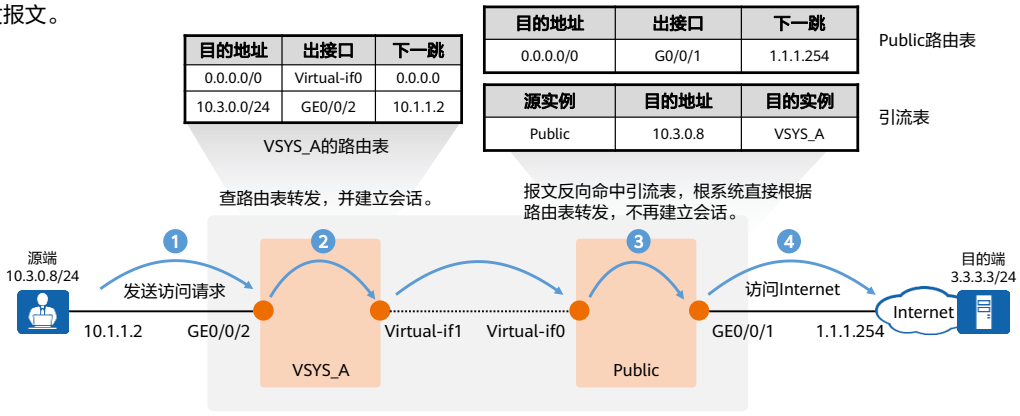


HUAWEI

- 公网用户通过根系统的公网接口GE0/0/1访问虚拟系统VSYS_A下的服务器，详细流程如下：
  - 客户端向服务器发起连接。
  - 报文达到根系统后命中引流表，将报文送入命中的表项对应的“Destination Instance”中处理，发送给VSYS_A。
  - 虚拟系统的虚拟接口Virtual-if1收到报文后，虚拟系统按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等等。如果虚拟系统不允许转发报文，则丢弃报文，流程结束；如果虚拟系统允许转发报文，则将报文发往服务器。同时，虚拟系统会为这条连接建立会话。
  - 报文经过路由转发后，到达目的服务器。

引流表 - 反向命中

- 反向命中：虚拟系统发往根系统的报文，**源地址**匹配引流表中的“Destination Address”，源虚拟系统匹配引流表中的“Destination Instance”，则报文反向命中引流表。报文反向命中引流表时，根系统按路由表转发报文。



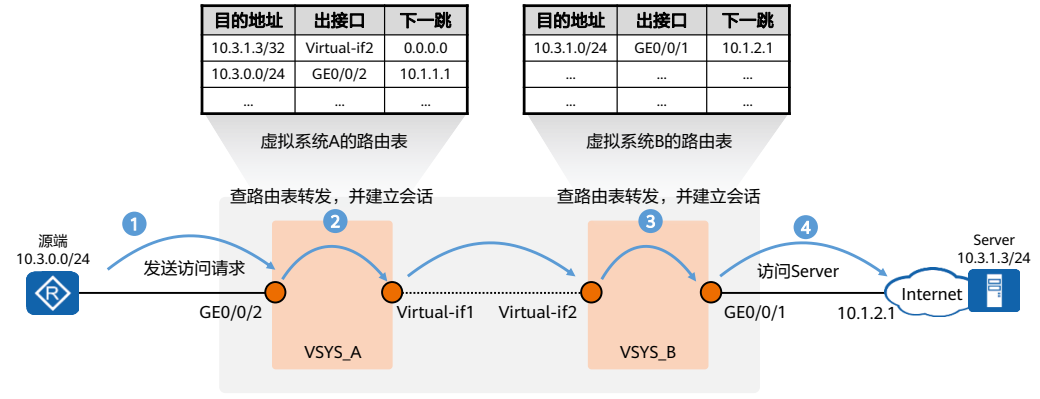
HUAWEI

- 虚拟系统A下10.3.0.0/24网段的用户通过根系统的公网接口GE0/0/1访问Internet服务器3.3.3.3，详细流程如下：
  - 客户端向服务器发起连接。
  - 首包到达防火墙后，基于接口分流，被送入VSYS_A。VSYS_A按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等等。如果VSYS_A不允许转发报文，则丢弃报文，流程结束；如果VSYS_A允许转发报文，则将报文送入根系统中处理。同时，VSYS_A会为这条连接建立会话。
  - 根系统的虚拟接口Virtual-if0收到报文后，根系统根据报文的源地址和引流表中的“Destination Address”进行匹配，匹配成功则查找路由表转发。
  - 报文经过路由转发后，到达目的服务器。

目录

虚拟系统之间互访

- 防火墙的虚拟系统之间默认是互相隔离的，不同虚拟系统下的主机不能通信。如果两个虚拟系统下主机有通信的需求，就需要配置策略和路由，使不同虚拟系统能够互访。



HUAWEI

- 该场景是虚拟系统VSYS_A向虚拟系统VSYS_B发起访问。报文先进入虚拟系统VSYS_A，虚拟系统VSYS_A按照防火墙转发流程对报文进行处理。然后报文进入虚拟系统VSYS_B，虚拟系统VSYS_B再次按照防火墙转发流程对报文进行处理。具体过程如下：
  - 客户端向服务器发起连接。
  - 首包到达防火墙后，基于接口分流，被送入虚拟系统VSYS_A。VSYS_A按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等等。如果VSYS_A不允许转发报文，则丢弃报文，流程结束；如果VSYS_A允许转发报文，则将报文送入VSYS_B中处理。同时，VSYS_A会为这条连接建立如下会话。
  - VSYS_B的虚拟接口Virtual-if2收到报文后，VSYS_B按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等等。如果VSYS_B不允许转发报文，则丢弃报文，流程结束；如果VSYS_B允许转发报文，则将报文发往服务器。同时，VSYS_B会为这条连接建立如下会话。
  - 报文经过路由转发后，到达目的服务器。
- 因为两个虚拟系统都需要按照防火墙转发流程对报文进行处理，所以两个虚拟系统中要分别完成策略、路由等配置。

虚拟系统互访的路由配置

- VSYS_A配置：
  - 配置去程路由，即到服务器的路由。

    ```
    [FW-VSYS_A] ip route-static vpn-instance vsysa 10.3.1.3 255.255.255.0 vpn-instance vsysb
    ```

    因为报文要经过VSYS_A发送到服务器，所以要配置VSYS_A到VSYS_B的路由。跨虚拟系统的路由只能是静态路由。和一般的静态路由不同，这条静态路由不需要配置下一跳或者出接口，而是要指定目的虚拟系统为服务器所在虚拟系统。
  - 配置回程路由，即到达客户端的路由。可以通过动态路由（如OSPF）或静态路由配置，本例采用静态路由配置。

    ```
    [FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.1
    ```
- VSYS_B配置：
  - 配置去程路由，即到服务器的路由。可以通过动态路由（如OSPF）或静态路由配置，本例采用静态路由配置。

    ```
    [FW-VSYS_B] ip route-static 10.3.1.0 255.255.255.0 10.1.2.1
    ```

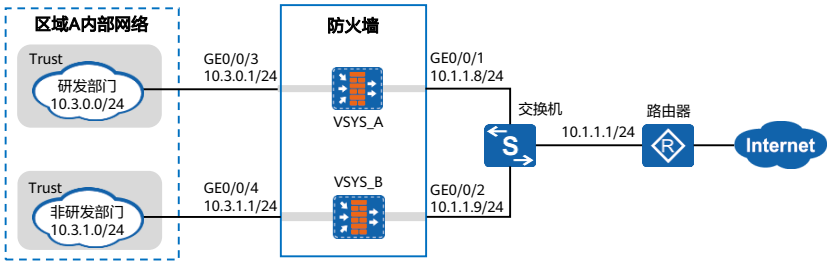
    VSYS_B中不需要针对服务器回应的报文配置回程路由。服务器回应的报文在VSYS_B中匹配会话表后，直接发送到VSYS_A中处理。

- 按上述方法配置，只能实现VSYS_A到VSYS_B的单向通信，即只能是VSYS_A中主机主动向VSYS_B中主机发起访问，VSYS_B中主机不能主动向VSYS_A中主机发起访问。
- 如果VSYS_B中主机有主动访问VSYS_A中主机的需求，则需要配置VSYS_B到VSYS_A的路由。比如VSYS_B中主机访问VSYS_A中IP地址为10.3.0.3的主机，路由配置命令为ip route-static vpn-instance vsysb 10.3.0.3 255.255.255.255 vpn-instance vsysa。同时，也需要配置策略。策略的源和目的安全区域与VSYS_A访问VSYS_B时相反。

目录

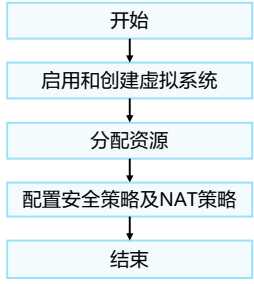
组网需求

- 某大型企业园区的区域A中，部署了一台防火墙作为接入网关。根据权限不同，区域A内网络划分为研发部门和非研发部门，且这两个部门的网络访问权限不同，具体需求如下：
  - 研发部门只有10.3.0.2-10.3.0.10地址段可以访问Internet，非研发部门的全部员工都可以访问Internet。
  - 研发部门和非研发部门之间相互隔离，不能互访。
  - 研发部门和非研发部门的业务量差不多，所以为它们分配相同的虚拟系统资源。



配置思路

- 启用虚拟系统。
- 根系统管理员分别创建虚拟系统VSYS_A、虚拟系统VSYS_B，并为每个虚拟系统分配资源。
- 根系统管理员为虚拟系统VSYS_A配置IP地址、路由和安全策略和NAT策略。
- 根系统管理员为虚拟系统VSYS_B配置IP地址、路由和安全策略和NAT策略。



数据规划

虚拟系统VSYS_A的参数信息：

虚拟系统名称	公网接口/地址	公网安全区域	私网接口/IP地址	私网安全区域	允许访问公网的地址范围
vsysa	GE0/0/1 (10.1.1.8/24)	Untrust	GE0/0/3 (10.3.0.1/24)	Trust	10.3.0.2/24-10.3.0.10/24

虚拟系统VSYS_B的参数信息：

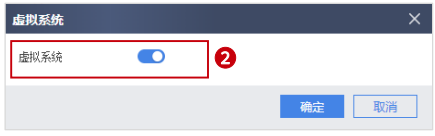
虚拟系统名称	公网接口/地址	公网安全区域	私网接口/IP地址	私网安全区域	私网地址范围
vsysb	GE0/0/2 (10.1.1.9/24)	Untrust	GE0/0/4 (10.3.1.1/24)	Trust	10.3.1.0/24

资源类的参数信息：

名称	会话保证值/最大值	用户数	用户组	策略数	出方向带宽
r1	10000/50000	300	10	300	20 M

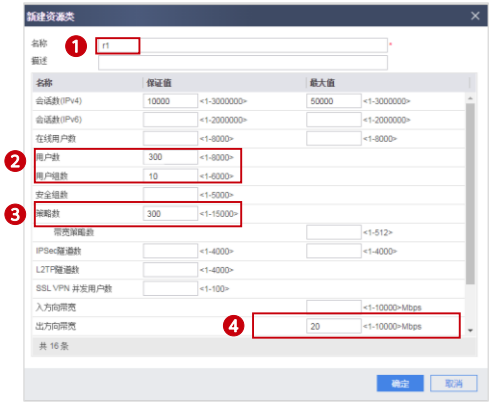
启动虚拟系统

- 进入“面板”，在“设备信息”窗格中，单击“虚拟系统”所在行的“配置”，启用虚拟系统功能。



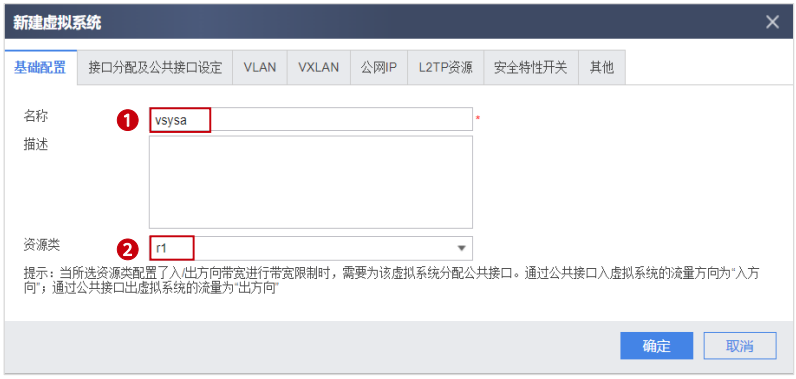
配置资源类

- 选择“系统 > 虚拟系统 > 资源类”。单击“新建”，按如图参数配置资源类名称、会话数保证值及最大值、用户数、用户组数、策略书以及整体带宽。



创建虚拟系统并分配资源类

- 选择“系统 > 虚拟系统 > 虚拟系统”。单击“新建”，选择“基础配置”页签，为虚拟系统A分配资源类为r1，点击确定。

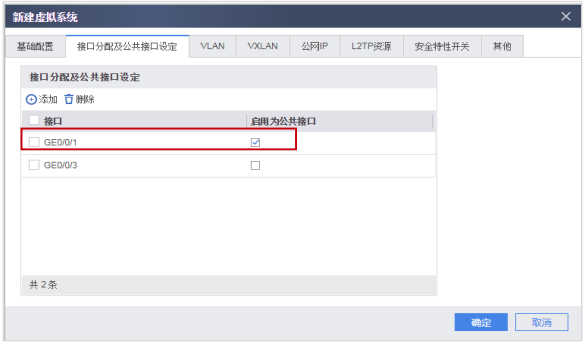


接口分配

- 选择“接口分配及公共接口设定”页签，为虚拟系统分配接口，将GE0/0/1和GE0/0/3分配给虚拟系统A，并点击确定。

公共接口设定

- 将GE0/0/1接口设置为公共接口。只有配置了公共接口，资源类中的带宽资源配置才会生效。
- 参考上述步骤，创建虚拟系统B并为其分配资源r1、分配接口GE0/0/2和GE0/0/4，公共接口为GE0/0/2口设置为公共接口。因其配置过程与虚拟系统A基本相同，此处省略。



HUAWEI

虚拟系统IP地址配置

- 在虚拟系统A中配置接口相关参数。
  - 在界面右上角的“虚拟系统”下拉菜单中选择“vsysa”，进入虚拟系统A。

  - 选择“网络 > 接口”，按如图参数进行配置。

HUAWEI

- 参考上述步骤，为虚拟系统B进行接口参数配置。

虚拟系统路由配置

- 在虚拟系统A中配置路由，使其访问Internet。
  - 选择“网络 > 路由 > 静态路由”。
  - 选择“新建”，配置一条缺省静态路由，使其可以访问Internet。配置参数如下：

HUAWEI

安全策略配置

- 在虚拟系统A中配置安全策略，允许特定网段的研发员工访问Internet。
  - 选择“对象 > 地址”；
  - 单击新建，如图参数建立一个地址段；
  - 再选择“策略 > 安全策略 > 安全策略”；
  - 单击“新建 > 新建安全策略”，配置实现ipaddress1可以访问Internet。

HUAWEI

- 除放行网段的其他员工访问Internet时，报文会匹配到default安全策略，即被deny掉。

NAT策略配置

- 在虚拟系统A中配置NAT策略。选择“策略 > NAT策略 > NAT策略”，单击“新建”，按如下参数配置NAT策略。

HUAWEI

- 根系统管理员为虚拟系统B配置IP地址、路由、安全策略和NAT策略。 具体配置过程与研发部门类似，主要有以下几点区别：
  - 内网接口的IP地址不同；
  - 非研发部门无需创建地址范围，直接配置一条允许所有地址范围访问Internet的安全策略、一条允许员工互访的安全策略即可；
  - NAT策略的出接口配置为GE0/0/2，源地址为any。

思考题

1. （判断题）防火墙的管理接口不可以分配给虚拟系统。（　　）
   A. 对
   B. 错
2. （多选题）虚拟防火墙支持以下哪些分流方式？（　　）
   A. 基于接口的分流
   B. 基于VLAN的分流
   C. 基于VNI的分流
   D. 基于协议的分流

1. A
2. ABC

本章总结

- 本章课程主要介绍了虚拟系统的基本概念，通过配置防火墙虚拟系统可以实现业务和路由隔离。在不同应用场景中，虚拟系统的相关路由配置也有所不同。通过配置虚拟系统可以满足多场景多业务隔离需求，节省了企业硬件成本和减轻管理员的运维压力。
- 通过本课程的学习，您将能够了解虚拟系统的基本概念，独立完成虚拟系统的配置。

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

缩略语	英文全称	解释
DMZ	Demilitarized Zone	半信任区
CPU	Central Processing Unit	中央处理单元
I/O	Input/Output	输入输出
NAT	Network Address Translation	网络地址转换
OSPF	Open Shortest Path First	开放最短路径优先
SSL	Secure Sockets Layer	安全套接层
VLAN	Virtual Local Area Network	虚拟局域网
VNI	VXLAN Network Identifier	VXLAN网络标识
VPN	Virtual Private Network	虚拟专用网络
VSYS	Virtual System	虚拟系统
VXLAN	Virtual Extensible Local Area Network	虚拟扩展局域网

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.

防火墙智能选路

HUAWEI

前言

- 在实际组网中，企业出于带宽和可靠性的要求，往往会租用多条运营商链路，以规避单运营商链路故障带来的风险并解决带宽不足的问题。由于出口设备在转发流量时一般是随机选择一条链路，且不考虑各条链路的实际带宽或链路的实时状态，这样会导致链路空闲或链路拥塞等新问题。
- 在出口防火墙上部署智能选路功能可解决上述问题。防火墙通过不同的智能选路方式，动态选择最优链路，以此提高链路资源的利用率和用户体验。
- 本章课程将详细介绍智能选路的原理和应用。

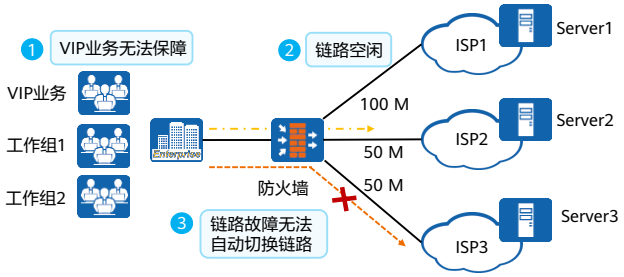
目标

- 学完本课程后，您将能够：
  - 描述智能选路的基本概念
  - 描述智能选路的使用场景
  - 掌握智能选路的配置步骤

目录

智能选路产生背景 (1)

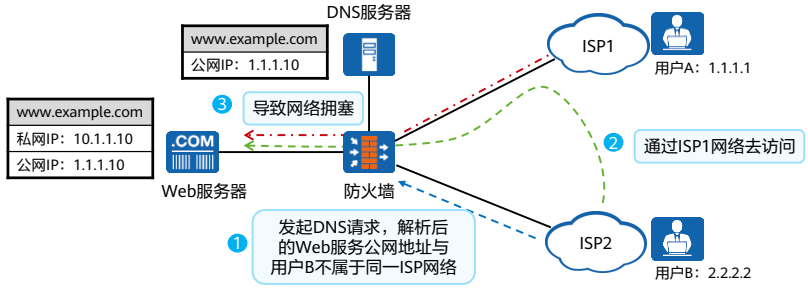
- 中大型企业通常会在网络出口部署多条链路，提高出口链路的带宽和可靠性。面对多出口场景，传统方法采用等价路由，但是等价路由会造成大量的跨运营商访问，效率低下。此外，防火墙转发报文时不考虑各条链路的实际带宽或实时状态，在实际应用中会存在链路拥塞、用户体验感差等诸多问题。



多出口出站场景

智能选路产生背景 (2)

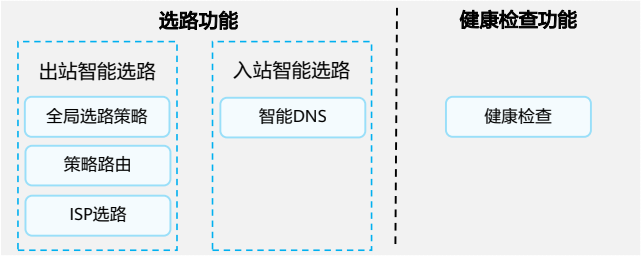
- 企业内网同时部署了DNS和Web服务器的场景下，当外网用户通过域名访问企业内网Web服务器时，由于DNS解析后的地址可能与用户地址属于不同的ISP网络，会导致访问延迟、额外产生ISP间的流量成本或链路拥塞等问题。



多出口入站场景

智能选路概述

- 智能选路是指到达目的网络有多条链路可选时，防火墙通过不同的智能选路方式，动态选择最优链路，并根据各链路实时状态动态调整分配结果，以此提高链路资源的利用率和用户体验。
- 智能选路的功能主要分为以下两部分：
  - 选路功能：可根据入站和出站场景分类，对应着不同的智能选路技术，满足多场景应用；
  - 健康检查：可对服务可用性、链路可用性或链路时延进行探测，并根据探测结果调整业务流量的分配，为网络服务质量提供必要保障。



HUAWEI

- 出站智能选路和入站智能选路的实现方式有所不同：
  - 出站智能选路：当内网用户访问外网时，如果到达目的网络有多条链路可选，防火墙进行智能选路。
    - 全局选路策略：当到达目的网络有多条等价路由或者缺省路由时，防火墙通过不同的智能选路方式动态选择最优链路。
    - 策略路由：当网络中配置了策略路由，并且流量命中配置的策略路由时，如果到达目的网络有多条链路可选，防火墙通过不同的智能选路方式动态选择最优链路。
    - ISP选路：当防火墙作为出口网关设备连接多个ISP网络时，通过批量生成ISP路由，使访问特定ISP网络的流量从相应出接口转发出去，保证流量转发使用最短路径。
  - 入站智能选路：当外网用户访问内网时，如果到达目的网络有多条链路可选，防火墙进行智能选路。
    - 智能DNS：当外网用户通过域名访问内网服务器时，向企业内网DNS服务器发起DNS请求，DNS服务器返回解析后地址给外网用户，防火墙可以将DNS回应报文中的解析地址进行智能修改，使用户能够获得最合适的解析地址，避免链路拥塞或者跨运营商访问。
- 健康检查一般不会独立使用，与智能选路结合使用才有实际作用。当前健康检查功能只支持与出站智能选路功能结合使用。

目录

全局选路 策略路由选路 ISP选路

出站智能选路 - 全局选路策略

- 在多出口场景下，全局选路策略可根据不同的智能选路方式选择出接口，并根据各条链路的实时状态动态调整分配结果，以此实现链路资源的合理利用，提升用户体验。
- 用户还可根据具体需求设置链路的过载保护阈值，当某条链路承载的流量超过用户所设置的阈值时，过载保护会将超出的流量在未超出阈值的链路间负载分担。

智能选路方式

链路带宽负载分担	链路质量负载分担	链路权重负载分担	链路优先级主备备份
• 防火墙按照带宽比例将流量分配到各链路上。	• 防火墙优先使用链路质量高的链路转发流量。	• 防火墙按照权重的比例将流量分配到各条链路上。	• 防火墙优先使用主接口转发流量。

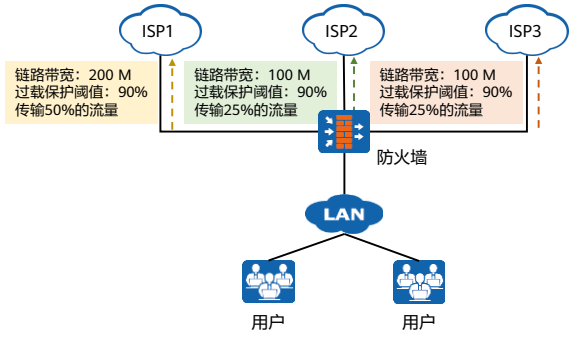
HUAWEI

- 在多出口且存在等价路由的场景下，防火墙默认按照逐流负载分担模式进行转发，使用源IP地址和目的IP地址进行HASH计算选择出接口，即由报文的源IP和目的IP决定选择哪条路，不会考虑各条链路的实际带宽或链路的实时状态。当转发流量较大时，很可能出现一部分链路拥塞、另一部分链路闲置的情况，造成链路资源的浪费。当某些链路的传输质量比较差时，可能造成访问失败，影响用户的体验。

全局选路 策略路由选路 ISP选路

全局选路策略 - 链路带宽负载分担

- 当企业从不同ISP处获得多条带宽不等的链路时，为了充分利用各链路的带宽，提高链路的利用率，可以选择链路带宽负载分担方式，该方式也是默认的智能选路方式。
- 防火墙在部署时，需要在各条链路的出接口上配置入方向和出方向的带宽，管理员根据实际链路带宽设置合理的带宽值。



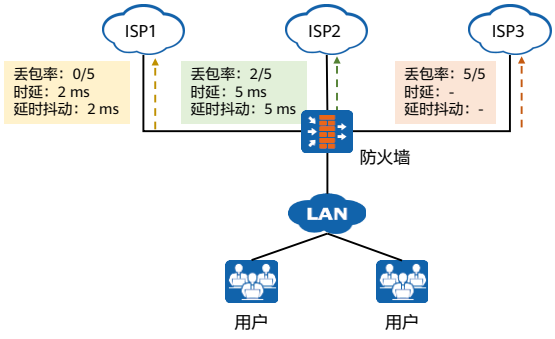
HUAWEI

- 如图所示，防火墙有3条出接口链路，其中与ISP1相连的链路带宽为200 M，与ISP2和ISP3相连的链路带宽均为100 M，所以带宽比例为**2:1:1**。当防火墙转发一段时间流量后，各链路上累计传输的流量将分别占到总流量的50%、25%、25%，即各链路传输流量的比例和带宽的比例成正比。
- 为了保证链路不会过载，管理员设置了过载保护阈值，各链路均为90%。当某条链路的带宽使用率达到90%时，已建立会话的流量仍从该链路转发，但是后续新建立会话的流量不再通过此链路转发，防火墙会在未过载的链路中智能选路，后续流量按照未过载链路之间的带宽比例进行负载分担。如果所有链路都已过载，那么防火墙将继续按照各链路的带宽比例分配流量。

全局选路 策略路由选路 ISP选路

全局选路策略 - 链路质量负载分担

- 当企业从不同ISP处获得多条链路时，为了使用户获得最佳的访问体验，需要防火墙能够根据各链路的实时传输质量动态调整流量的分配，此时可以选择链路质量负载分担方式。
- 丢包率、时延和时延抖动是防火墙衡量链路质量的三个参数，管理员可以根据实际需要选择其中的一个或多个参数判断链路质量。



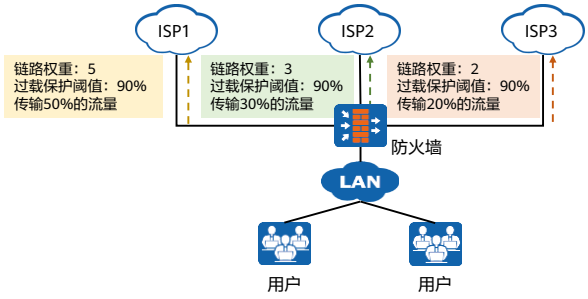
HUAWEI

- 如图所示，防火墙拥有3条出接口链路，分别属于不同的ISP。防火墙向各个ISP内的指定设备发送5个探测报文，其中ISP1链路没有丢包，ISP2链路丢了2个包，ISP3链路没有收到回应报文。所以防火墙判定ISP1的质量最高，将优先使用ISP1链路转发流量，只要探测表项没有老化，防火墙就一直使用ISP1转发流量，不会使用ISP2链路和ISP3链路。
- 如果管理员还为各链路设置了过载保护阈值，那么当ISP1链路的带宽利用率达到阈值时，ISP1链路将不再参与智能选路，防火墙会选择其他链路中质量最高的ISP2链路转发后续流量。
- 三个质量参数中，丢包率是最重要的参数，如果两条链路的丢包率、时延、时延抖动各不相同，那么防火墙判定丢包率小的链路质量高。

全局选路 策略路由选路 ISP选路

全局选路策略 - 链路权重负载分担

- 当企业从不同ISP处获得多条性能不等的链路时，为了优先使用转发性能最优的链路，保证大多数用户的访问体验，且不浪费其它性能稍差的链路，可以选择链路权重负载分担方式。
- 管理员在防火墙上为各个接口指定权重时，需要综合考虑各链路的带宽、转发时延、链路租借费用等因素。



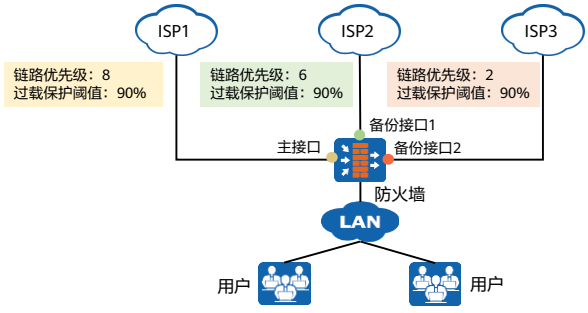
HUAWEI

- 如图所示，防火墙拥有3条出接口链路属于不同的ISP。其中，ISP1的链路权重为5，ISP2的链路权重为3，ISP3的链路权重为2，所以权重比例为5:3:2。当防火墙转发一段时间流量后，各链路上累计传输的流量将分别占到总流量的50%、30%、20%，即各链路传输流量的比例和权重的比例成正比。
- 为了保证链路不会过载，管理员还设置了过载保护阈值，各链路均为90%。当某条链路的带宽使用率达到90%时，此链路将不再被分配流量，防火墙会在未过载的链路中智能选路，后续流量按照未过载链路之间的权重比例进行负载分担。如果所有链路都已过载，那么防火墙将继续按照各链路的权重比例分配流量。
- “转发性能最优的链路”指的是最符合企业利益的链路，而不是单指转发速度最快的链路，所以管理员需要根据实际情况设置合理的权重。

全局选路 策略路由选路 ISP选路

全局选路策略 - 链路优先级主备备份

- 当企业从不同ISP处获得多条链路时，若各链路的带宽、转发时延等因素差异较大时，可调大某些链路的优先级使之为主接口并优先传输流量，其他链路作为备份链路或负载分担链路，提高业务的可靠性。该方式为链路优先级主备备份方式，分为两种场景：主备备份场景和负载分担场景。



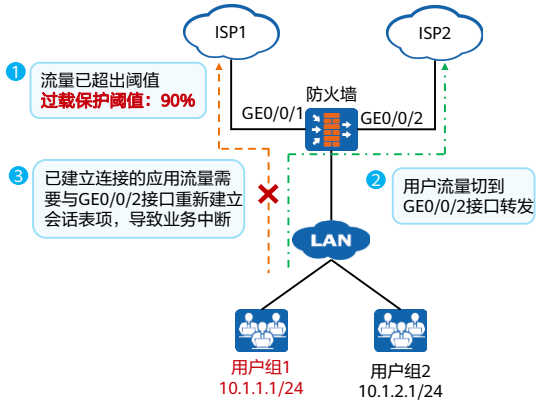
链路优先级主备备份场景

HUAWEI

- 该智能选路方式分为两种场景：
  - 主备备份场景：防火墙优先使用主接口转发流量。如果没有为主接口链路指定过载保护阈值，那么即使链路过载，防火墙也不会使用其他链路传输流量。只有当主接口链路发生故障后，优先级次高的备份接口才被启用以替代主接口，而其他优先级更低的备份接口则仍未启用。
  - 负载分担场景：为了提高传输的可靠性和负载能力，可以为各接口链路设置过载保护阈值。当主接口链路过载时，防火墙会使用优先级次高的备份接口和主接口一起分担流量。当主接口和优先级次高的备份接口都过载后，余下的备份接口中优先级最高的接口才被启用进行流量分担。
- 主备备份场景如图所示，防火墙有3条出接口链路属于不同的ISP。其中，ISP1，ISP2和ISP3的链路优先级分别为8，6和2。ISP1的链路优先级最高，防火墙优先使用ISP1链路转发流量。
- 上图管理员设置了过载保护阈值，各链路均为90%。防火墙优先使用ISP1链路转发流量，当ISP1链路的带宽利用率达到90%后，启用ISP2链路和ISP1链路一起分担流量。当ISP1链路和ISP2链路都过载时，启用ISP3链路和ISP1、ISP2链路一起分担流量。当3条链路都过载时，防火墙将按照各链路带宽的比例分配流量，不再根据链路优先级来分配。

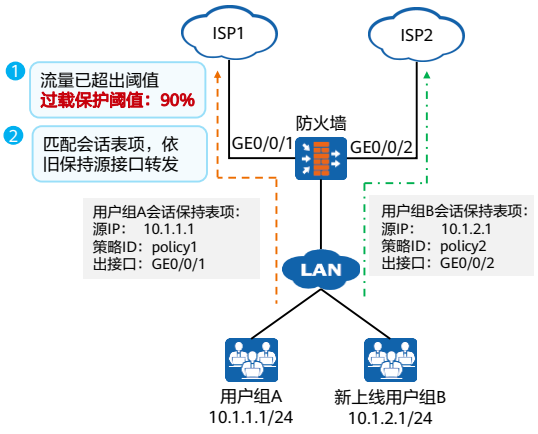
过载保护存在的问题

- 智能选路接口可以配置过载保护阈值，当接口链路的带宽利用率达到过载保护阈值时，防火墙对新流量进行智能选路时将排除该过载链路，在其他未过载的链路中进行选路。
- 这样可能会导致用户上网流量在接口链路过载前选择了该接口链路，而新建会话流量（如打开新网页）因为原接口链路过载而被防火墙从其他接口转发出去，从而出现已经登录的网站在刷新后需要重新登录或者网络游戏在链路切换后掉线，甚至某些网上银行业务因检测到IP地址变化而拒绝用户访问等现象。



会话保持

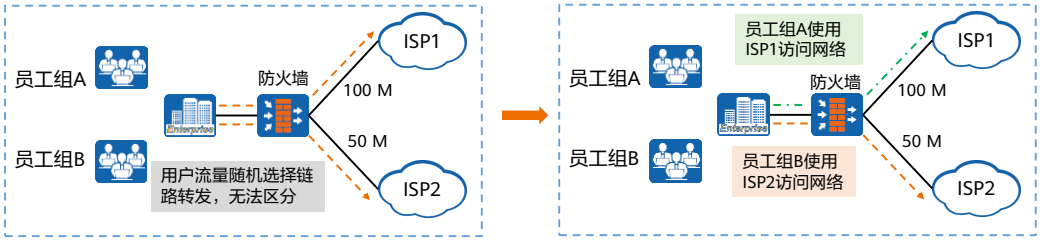
- 为了解决上述问题，可以开启智能选路会话保持功能。用户A的上网流量进行首次智能选路后，会生成一个会话保持表项，其中包含了源IP地址、匹配的智能选路策略ID和首次选路的出接口。当该用户再次发起连接时，防火墙会根据新流量中的源IP和匹配的智能选路策略ID查找相应的会话保持表项，并直接使用会话保持表项中记录的出接口转发该流量，这样就保证了此用户的流量始终使用同一出接口转发。新上线的内网用户，则会选择别的接口，并生成会话保持表。
- 可以使用**display session persistence table**命令查看会话保持表项。



- 华为USG6000E系列防火墙支持在四种智能选路方式中配置会话保持功能。

出站智能选路 - 策略路由

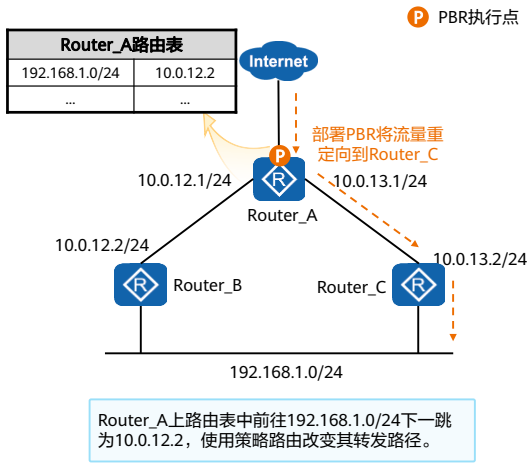
- 全局选路策略是基于链路参数来影响选路，无法提供有差别的服务。若用户指定路径转发流量时，可通过策略路由选路方式实现。因策略路由优先于路由表生效，从更多的维度（入接口、源安全区域、源/目的IP地址、用户、服务、应用等）制定策略来决定报文的转发路径，可增加报文转发控制上的灵活度。
- 如图所示，在双ISP接入场景中，某企业的员工组A权限高，需享受快速网络，即选择链路ISP1（100 M）访问互联网；而员工组B权限低，通过链路ISP2（50 M）访问互联网。该需求无法通过传统的路由技术实现，可通过策略路由实现。



- 策略路由并没有替代路由表机制，而是优先于路由表生效，为某些特殊业务指定转发方向。

策略路由基本概念

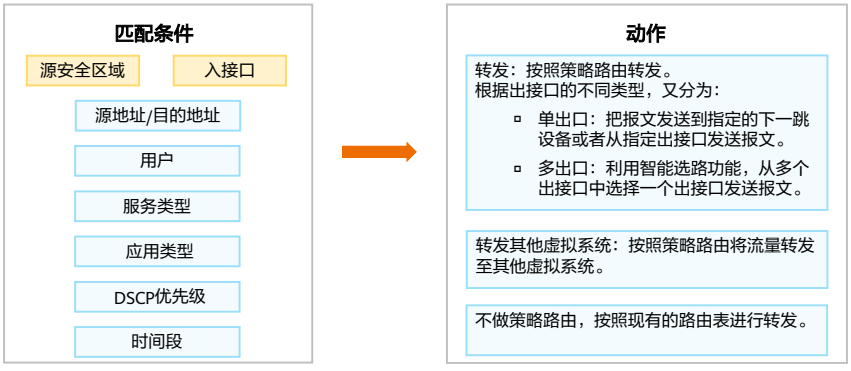
- PBR（Policy-Based Routing，策略路由）使得网络设备不仅能够基于报文的目的IP地址进行数据转发，更能基于其他元素进行数据转发，例如源IP地址、源目MAC地址和源目端口号等。
- 用户还可以使用ACL匹配特定的报文，然后针对该ACL进行PBR部署。
- 若设备部署了PBR，则被匹配的报文优先根据PBR的策略进行转发，即PBR策略的优先级高于传统路由表。



Router_A上路由表中前往192.168.1.0/24下一跳为10.0.12.2，使用策略路由改变其转发路径。

策略路由匹配规则 (1)

- 策略路由由多个节点组成，每个节点由匹配条件和执行动作两部分组成。
  - 匹配条件可以将要做策略路由的流量区分开来。其中，源安全区域和入接口是互斥的必选项，二者必须配置其中一项。
  - 如果策略路由配置的所有匹配条件都匹配，则此流量成功匹配该策略路由规则，并执行策略路由的动作。



- 服务类型、应用类型、用户作为匹配条件时，可以同时指定多个服务/服务组、应用/应用组、用户/用户组，只要与其中一个相同，就算满足该匹配条件。

策略路由匹配规则 (2)

- 防火墙收到流量后，对流量的属性进行识别，并将流量的属性与策略路由的匹配条件进行匹配。如果所有条件都匹配，则此流量成功匹配策略路由。流量匹配策略路由后，设备将会执行策略路由的动作。
  - 单条策略路由中包含多个匹配条件，各个匹配条件之间是“与”的关系，报文的属性与各个条件必须全部匹配，才认为该报文匹配这条规则。
  - 多条策略路由是“或”的关系，按照策略列表的顺序执行的，即从策略列表顶端开始逐条向下匹配，如果流量匹配了某个策略路由，将不再进行下一个策略的匹配。

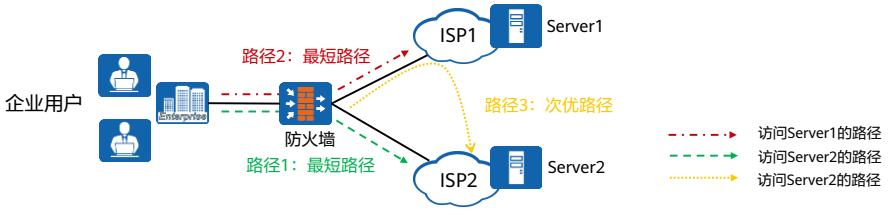
匹配顺序

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
Policy 2:	匹配条件1	匹配条件2	.....	匹配条件N	动作
.....					
Policy N:	匹配条件1	匹配条件2	.....	匹配条件N	动作
Default:	匹配条件均为any				动作（不做策略路由）

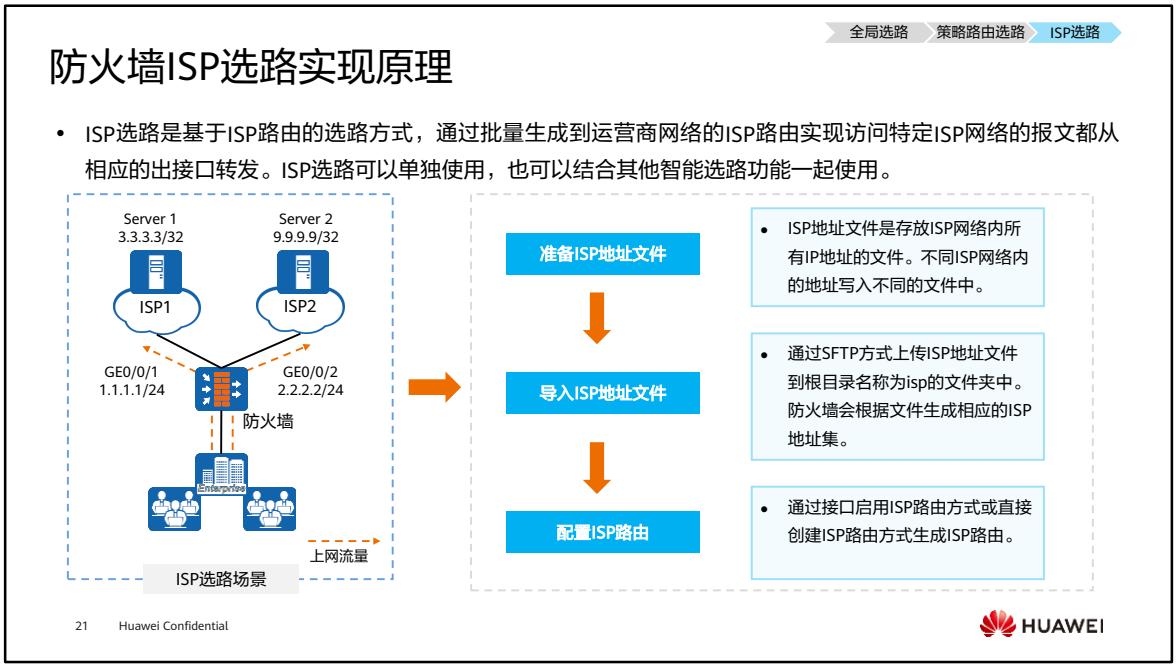
- 当配置多条策略路由规则时，策略路由列表默认是按照配置顺序排列的，越先配置的策略路由规则位置越靠前，优先级越高。策略路由的匹配就是按照策略列表的顺序执行的，即从策略列表顶端开始逐条向下匹配，如果流量匹配了某个策略路由，将不再进行下一个策略的匹配。所以策略路由的配置顺序很重要，需要先配置条件精确的策略，再配置宽泛的策略。如果某条具体的策略路由放在通用的策略路由之后，可能永远不会被命中。
- 此外，系统默认存在一条缺省策略路由default，缺省策略路由位于策略列表的最底部，优先级最低，所有匹配条件均为any，动作为不做策略路由，即按照现有的路由表进行转发。如果所有配置的策略都未匹配，则将匹配缺省策略路由default。

出站智能选路 - ISP选路

- ISP选路功能也称为运营商地址库选路功能，当防火墙作为出口网关设备连接多个ISP网络时，通过ISP选路功能可以使访问特定ISP网络的流量从相应出接口转发出去，保证流量转发使用最短路径。
- 配置ISP选路功能后，当内网用户访问Server1或Server2时，防火墙会根据目的地址所在ISP网络选择相应的出接口，从而使访问流量通过最短路径到达服务器，避免次优路径产生。



- 如图所示，防火墙拥有两条属于不同ISP网络的出口链路。当内网用户访问ISP2中的Server2时，如果防火墙上存在等价路由，则防火墙可以通过多条不同的路径到达Server2。其中，路径3显然不是最优路径，路径1才是用户所期望的路径。



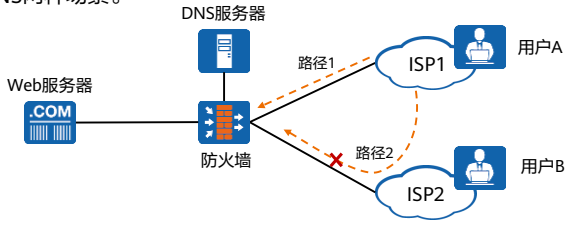
- 如图所示，防火墙作为安全网关部署在网络出口，企业分别从ISP1和ISP2租用一条链路。
  - 需求：
    - 企业希望访问Server 1的报文从ISP1链路转发，访问Server 2的报文从ISP2链路转发。
    - 当其中一条链路故障时，后续流量可以通过另一条链路转发，保证传输的可靠性。
  - 实现原理：
    - 分别为ISP1和ISP2链路配置健康检查，检测链路状态。
    - 制作isp1.csv和isp2.csv两个ISP地址文件，将Server 1的IP地址3.3.3.3写入isp1.csv文件中；将Server 2的IP地址9.9.9.9写入isp2.csv文件中，并上传到防火墙上。
    - 配置ISP选路功能，使访问Server 1的报文从ISP1链路转发，访问Server 2的报文从ISP2链路转发。
    - 配置基本的安全策略，允许企业内部用户访问外网资源。
- 目前ISP地址文件有如下两种获取方式：
  - 方式一：登录安全中心平台（isecurity.huawei.com）进入“特征库升级”，选择相应的型号和版本后，切换到“因特网服务提供方库”页签下载最新的ISP地址文件，可以根据现网实际情况进行相应修改；

    - 方式二：在Web配置界面，进入“新建运营商”中下载地址库文件模板，并在本地编辑。
- 导入ISP地址文件：
    - 上传ISP地址文件到防火墙，可以使用SFTP方式进行传输，也可以直接通过Web界面直接上传，导入的ISP地址文件固定存放在根目录下名称为isp的文件夹内。
- 配置ISP路由的方法有：
    - 方式一：接口启用ISP路由，通过在接口中指定ISP地址集生成ISP路由，对于同一接口只能指定一个ISP地址集。
    - 方式二：直接创建ISP路由，直接创建ISP路由，可以为同一接口指定多个ISP地址集。
- 防火墙出厂时已经预置下列运营商的ISP地址文件：中国移动：china-mobile.csv；中国联通：china-unicom.csv；中国电信：china-telecom.csv；中国教育网：china-educationnet.csv。
- 地址库文件注意事项：
    - 该文件必须为csv格式。
    - 防火墙预置的地址库文件可以直接使用，但不能确保该地址库文件中的IP地址信息完全准确，应用时请根据现网实际情况进行相应调整。
    - 预置和导入的ISP地址文件固定存放在根目录下名称为isp的文件夹内。导入ISP地址文件后，管理员需要为每个文件创建一个名称，一般是以该ISP代表的运营商名称命名。成功导入文件后，每个地址库文件会自动生成一个ISP地址集（也称为运营商地址集），其中包含了地址库文件中的所有IP地址，该地址集可以被策略路由引用作为源地址或目的地址。
- ISP路由在路由表中显示的协议类型为UNR（User Network Route，用户网络路由），路由优先级为70。
- 为了提高流量转发的可靠性，ISP选路功能可以配合健康检查功能一起使用，保证流量不被转发到故障链路上。当健康检查的结果显示链路故障时，对应的ISP路由表项将被删除，所以流量不会命中该条路由，也就避免被转发到故障链路上。当链路状态恢复正常时，对应的ISP路由表项将重新生成，流量即可按此路由进行转发。

目录

入站智能选路 - 智能DNS

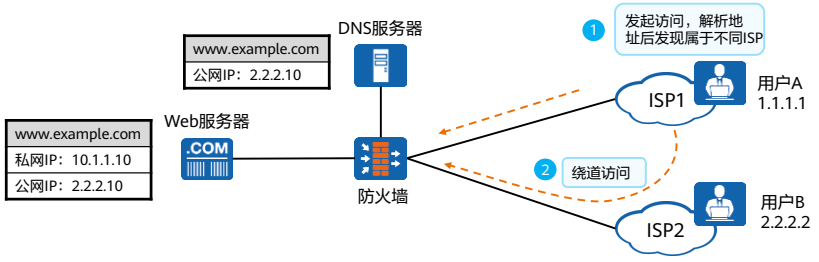
- 企业内网部署DNS服务器，存放服务器域名与IP地址的映射关系，当外网用户通过域名访问企业内网服务器时，存在多条访问路径，此时需要智能DNS技术选择最优路径。
- 如图所示，当外网用户A通过域名访问内网服务器时，向企业内网DNS服务器发起DNS请求。DNS服务器返回解析后地址给外网用户，防火墙可以将DNS回应报文中的解析地址进行智能的修改，确保和用户A在同一个ISP网络，避免用户A跨运营商访问，这种入站智能选路解析方式称为智能DNS。
- 智能DNS实现方式有出接口方式、简单轮询方式或加权轮询方式。根据服务器数量可以分为单服务器智能DNS和多服务器智能DNS两种场景。



- 出接口方式：防火墙通过智能DNS映射表，将DNS回应报文中的IP地址修改为与用户同属一个ISP公网地址，从而避免流量绕行。
- 简单轮询或加权轮询方式：防火墙通过简单轮询或加权轮询算法按照一定的权重比例给用户分配不同的解析地址。将用户访问的目的地址按比例修改为不同的地址，使流量通过不同的链路到达Web服务器，从而实现链路负载均衡。

单服务器智能DNS场景

- 单服务器智能DNS：当企业内网只部署一台Web服务器，即企业内网的DNS服务器上Web服务器的域名与一个Web服务器的IP地址对应时，需要配置单服务器智能DNS。
- 单服务器场景下用户访问路径如图所示，存在次优路径、链路拥塞等问题。为了解决上述问题，可以为ISP1用户配置出接口方式的单服务器智能DNS功能。

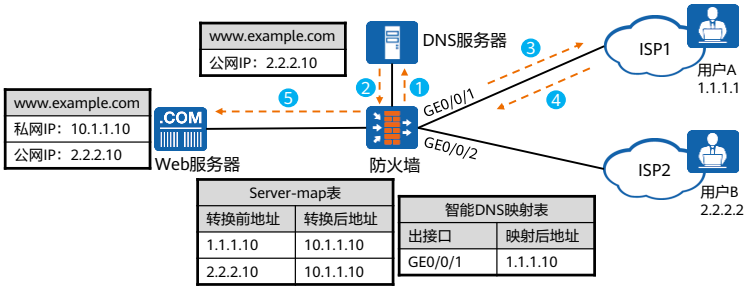


HUAWEI

- 如图所示：企业或数据中心通过多条链路连接到多个ISP网络，Web服务器的私网地址是10.1.1.10，公网地址是2.2.2.10，内网DNS服务器上只有Web服务域名（www.example.com）和公网地址（2.2.2.10）的对应关系。ISP1的用户通过域名www.example.com访问企业的Web服务时，解析后的地址是2.2.2.10，防火墙再利用NAT Server功能将报文的目的地址由2.2.2.10转换为服务器的私网地址10.1.1.10。
- 如果没有配置智能DNS功能，当其他ISP的用户（例如ISP1用户）通过域名www.example.com访问企业的Web服务时，解析后的地址2.2.2.10与用户地址（ISP1用户地址1.1.1.1）属于不同ISP网络，这样就会导致ISP1用户需要绕道ISP2网络才能到达服务器，从而增加了业务访问延迟和ISP间流量的结算成本。而且所有外网用户访问企业Web服务时都通过ISP2网络转发，这很可能导致防火墙连接ISP2网络的链路拥塞，而连接其他ISP网络的链路（ISP1链路）闲置。

单服务器智能DNS - 出接口方式

- 配置出接口方式的单服务器智能DNS功能后，防火墙会将返回给ISP1用户的服务器地址修改为ISP1网络的地址（例如从ISP1网络申请到的地址1.1.1.10），这样ISP1用户直接从ISP1网络就可以访问Web服务器，无需绕道ISP2网络。
- 如图所示，假设防火墙上为ISP1用户配置了出接口方式的智能DNS，将出接口为GigabitEthernet 0/0/1的DNS回应报文中的解析地址映射为1.1.1.10，ISP1用户访问Web服务器的流程如下：

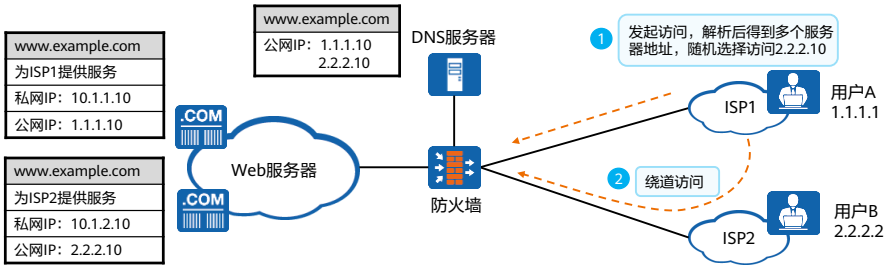


HUAWEI

- 步骤解析：
  1. ISP1用户通过域名www.example.com访问企业的Web服务器，发起DNS请求。
  2. DNS服务器返回解析后的IP地址2.2.2.10。
  3. 防火墙根据智能DNS映射表将DNS回应报文中的IP地址修改为1.1.1.10（与ISP1用户属于同一ISP），映射表中记录了出接口GigabitEthernet 0/0/1对应映射后的地址1.1.1.10。
  4. ISP1用户以返回的IP地址1.1.1.10为目的进行访问，通过ISP1网络到达防火墙。
  5. 防火墙利用NAT Server功能将报文的目的地址由1.1.1.10转换为Web服务器的私网地址10.1.1.10。
- 对于ISP2网络的用户来说，防火墙不会修改DNS服务器返回的地址仍为2.2.2.10，防火墙再利用NAT Server功能将报文的目的地址由2.2.2.10转换为服务器的私网地址10.1.1.10，ISP2网络用户直接通过ISP2网络即可访问Web服务器。这样就不会造成ISP1链路闲置、ISP2链路拥堵的情况，同时也提升了用户的访问速度和用户体验。

多DNS服务器场景问题

- 多服务器智能DNS：当企业内网部署多台Web服务器，即企业内网的DNS服务器上Web服务器的域名与多个Web服务器的IP地址对应时，需要配置多服务器智能DNS。
- 多服务器场景下用户访问路径如下图所示，存在次优路径和额外结算成本等问题。为了解决上述问题，可以为ISP1用户配置出接口方式的多服务器智能DNS功能。

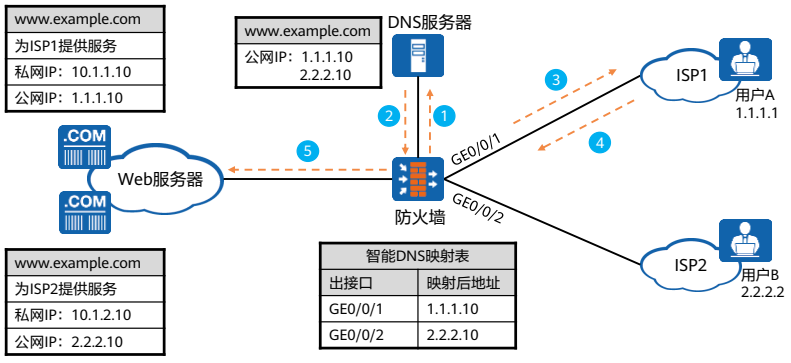


HUAWEI

- 如图所示：大型企业或数据中心在对外提供Web服务（例如网页访问）时，一般都会公布多个服务器的地址（例如1.1.1.10和2.2.2.10），用来供给不同ISP的用户访问。企业或数据中心的DNS服务器上存在Web服务的域名与多个服务器地址的对应关系。
- 如果没有配置智能DNS功能，当其中一个ISP（例如ISP1）的用户通过域名访问Web服务（例如www.example.com）时，会向企业内的DNS服务器发起DNS请求。DNS服务器会解析并返回多个服务器地址（1.1.1.10和2.2.2.10）给该用户。ISP1用户会随机选择其中一个服务器地址进行访问，所以这个服务器地址很可能属于另外一个ISP（例如ISP1用户随机选择了ISP2服务器地址2.2.2.10）。这样就会导致ISP1用户需要绕道ISP2网络才能到达服务器，从而增加了业务访问延迟和ISP间流量的结算成本。

多服务器智能DNS - 出接口方式

- 配置出接口方式的智能DNS功能后，防火墙只会返回一个服务器的地址给每个用户，且这个服务器的地址与用户的地址属于同一个ISP网络，这样用户就不用绕道其他ISP网络访问Web服务器了。



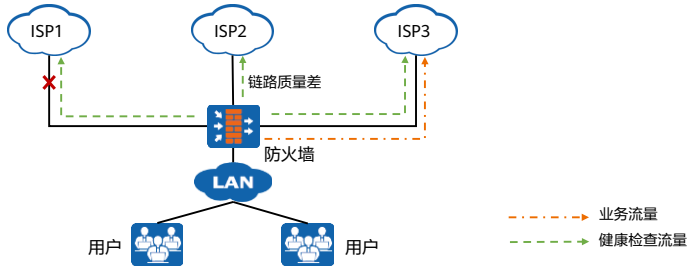
HUAWEI

- 步骤解析：
  1. ISP1用户通过域名www.example.com访问企业的Web服务器，发起DNS请求。
  2. DNS服务器返回解析后的IP地址1.1.1.10和2.2.2.10。
  3. 防火墙根据智能DNS映射表将DNS回应报文中的IP地址修改为1.1.1.10，映射表中记录了出接口GigabitEthernet 0/0/1对应映射后的地址1.1.1.10。
  4. ISP1用户以返回的IP地址1.1.1.10为目的进行访问到达防火墙，这样就保证ISP1用户访问时直接从ISP1网络就可以到达防火墙，无需绕道ISP2网络，从而提升了用户的访问速度和用户体验。
  5. 防火墙利用NAT Server功能将报文的目的地址由1.1.1.10转换为Web服务器的私网地址10.1.1.10。
- 上图中假设防火墙上为ISP1用户配置了出接口方式的智能DNS，将出接口为GigabitEthernet 0/0/1的DNS回应报文中的解析地址映射为1.1.1.10，将出接口为GigabitEthernet 0/0/2的DNS回应报文中的解析地址映射为2.2.2.10，以ISP1用户访问Web服务器为例说明用户访问Web服务器的流程如上介绍。
- 同理，ISP2用户通过域名www.example.com访问Web服务器时，防火墙根据智能DNS映射表将DNS回应报文中的IP地址修改为2.2.2.10，ISP2用户以2.2.2.10为目的进行访问，防火墙再利用NAT Server功能将报文的目的地址由2.2.2.10转换为Web服务器的私网地址10.1.2.10。

目录

健康检查概述

- 健康检查可以对服务可用性、链路可用性或链路时延等进行探测，并根据探测结果调整业务流量的分配，为网络服务质量提供必要保障。
- 防火墙通过健康检查结果实时感知到网络中发生的变化，并立即作出相应地调整，保证所使用的服务器或链路是可用的。当多个服务器或链路可用时，防火墙可以根据服务类型选择性能最优的服务器处理业务流量，或根据链路时延、抖动、丢包率选择最符合需求的链路传输业务流量，从而提高用户的使用体验。



健康检查协议类型和原理

- 防火墙分别向各ISP网络中的指定设备发送探测报文。如果出接口链路可用，那么可以收到被探测设备的响应报文，否则收不到响应报文。为了防止被探测设备自身故障导致误判，可以通过一个出接口同时向多个指定设备发送探测报文，当防火墙收到指定个数的响应报文时，才判定该接口链路可用。
- 防火墙可以根据不同类型的目的设备发送相应协议的探测报文，通过分析应答报文即可判断链路的可用性。

探测协议	探测原理
DNS	使用DNS协议向指定设备发起请求，如果应答报文中的标识字段与请求报文一致，即认为该链路可用。
HTTP	完成TCP三次握手后，使用HTTP协议向指定设备发送获取指定目的根目录的请求，收到HTTP应答报文即认为该链路可用，随后防火墙会发送RST报文终止此TCP连接。
ICMP	向指定设备发送ICMP请求报文，如果ICMP应答报文中的标识符和序列号字段与请求报文的一致，即认为该段链路可用。
RADIUS	使用RADIUS协议向指定服务器发起认证请求，用户名为“guest”，密码为空，如果应答报文中的标识符与发送报文一致，即认为该服务可用。
TCP	使用TCP协议向指定设备发送TCP连接请求，如果连接建立成功，即认为该链路可用，随后防火墙会发送RST报文终止此TCP连接。
TCP（简单探测）	使用TCP报文检查网络的连通性。只要目的设备回应第一个探测报文，即认为链路是可用的，无需完成三次握手。

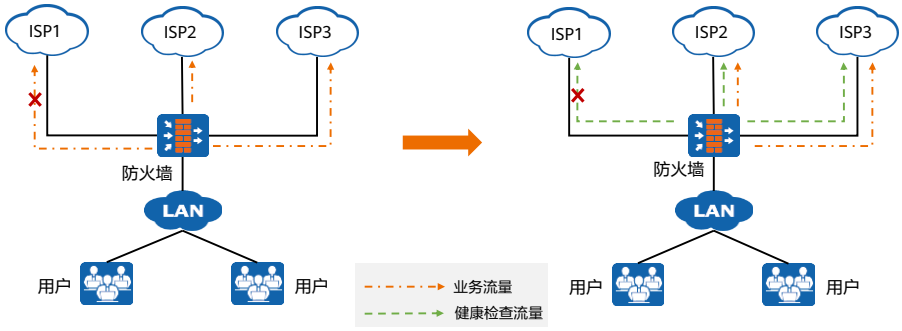
链路质量参数

- 链路质量参数包括：丢包率、时延和抖动。其中丢包率是最重要的参数，如果两条链路的丢包率、时延、抖动各不相同，那么防火墙判定丢包率小的链路质量高。

链路质量参数	计算方法
时延	回应报文的接收时间减去探测报文的发送时间即为时延。防火墙发送N个探测报文后，将分别计算每次探测的时延，并取N次探测的平均值作为最终结果。
抖动	相邻两次探测的时延之差取绝对值即为抖动。防火墙发送N个探测报文后，将分别计算相邻两次探测的时延之差并取绝对值，然后取所有抖动的平均值作为最终结果。
丢包率	防火墙发送若干个探测报文后，将统计丢包的个数，并计算丢包率。丢包率等于丢包个数除以探测报文个数。

健康检查应用场景

- 为提高流量转发的可靠性，智能选路功能可以配合健康检查功能一起使用，保证流量不被转发到故障链路上。
  - 当健康检查的结果显示链路故障时，对应的接口链路将不再参与智能选路，流量也就避免被转发到故障链路上。
  - 当链路状态恢复正常时，对应的接口链路重新参与智能选路，并转发分配到的流量。



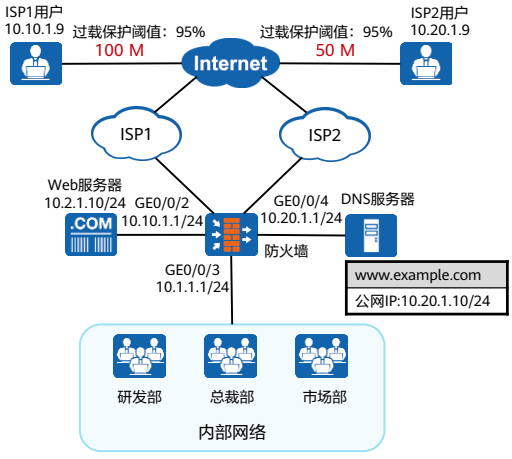
HUAWEI

- 如图所示，在全局选路场景中：
  - 未使用健康检查功能前，由于不能感知到ISP1链路发生故障，所以当选路结果为ISP1链路时，流量将从ISP1链路转发，导致访问失败。
  - 使用健康检查功能后，防火墙探测到ISP1链路故障，当流量触发智能选路时，ISP1链路不再参与智能选路，防火墙将从ISP2链路和ISP3链路中选择一条进行流量转发。

目录

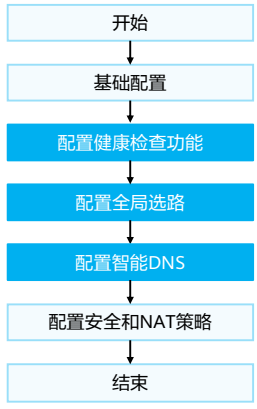
智能选路配置举例 (1)

- 需求描述：
  - 某企业分别从ISP1和ISP2租用了一条链路，ISP1链路的带宽为100 M，ISP2链路的带宽为50 M。
  - 流量需按照带宽比例分担到ISP1和ISP2链路上，保证带宽资源得到充分利用。
  - 当其中一条ISP链路过载时，后续流量将通过另一条ISP链路传输，提高访问的可靠性。
  - ISP1用户从ISP1链路访问企业Web服务器，ISP2用户从ISP2链路访问企业Web服务器，防止次优路径。



智能选路配置举例 (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；
  - 配置健康检查功能，检测链路状态；
  - 配置全局选路策略，根据链路带宽实现负载分担；
  - 配置智能DNS，使外网用户按最优路径访问服务器；
  - 配置安全和NAT策略，让内网用户成功访问Internet。

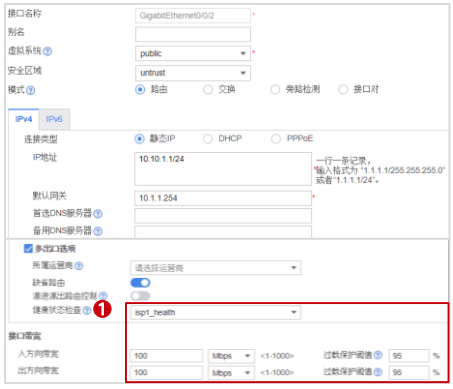


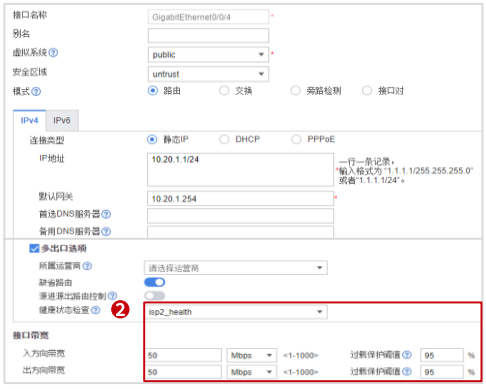
配置健康检查功能

- 选择“对象 > 健康检查”，在“健康检查列表”区域单击“新建”，按如下参数分别为ISP1和ISP2新建健康检查。

配置接口

- 选择“网络 > 接口”，按如下参数为防火墙连接ISP的接口设置链路带宽和过载保护阈值，并绑定对应的健康检查。





配置链路带宽负载分担

- 选择“网络 > 路由 > 智能选路”，在“全局选路策略列表”区域，单击“配置”，按如下参数配置链路带宽负载分担。

HUAWEI

配置出接口智能DNS

- 选择“网络 > DNS > 智能DNS”。启用“智能DNS”后，单击“应用”。
  - 在“智能DNS列表”中，单击“新建”。按如下参数配置单服务器智能DNS，将回应给ISP1用户的地址由10.20.1.10修改为10.10.1.10（从ISP1申请）。

思考题

1. （多选题）全局选路策略中的负载分担方式有哪些？（　　）
   A. 根据链路带宽负载分担
   B. 根据链路质量负载分担
   C. 根据链路权重负载分担
   D. 根据链路优先级主备备份
2. （多选题）策略路由匹配条件中，防火墙支持以下哪些类型的匹配条件？（　　）
   A. 入接口
   B. 服务类型
   C. 应用类型
   D. 用户

1. ABCD
2. ABCD

本章总结

- 本章主要介绍了华为防火墙智能选路功能。通过智能选路功能，可以给企业用户分配合理的链路访问资源，实现链路负载分担，提高网络利用率。
- 通过本课程的学习，您将对防火墙智能选路的原理有一定的了解，掌握智能选路的相关配置。

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

缩略语	英文全称	解释
ACL	Access Control List	访问控制列表
DNS	Domain Name Service	网域名称解析服务
HTTP	Hypertext Transfer Protocol	超文本传输协议
ICMP	Internet Control Message Protocol	网际报文控制协议
ISP	Internet service provider	互联网服务提供商
NAT	Network Address Translation	网络地址转换
PBR	Policy-Based Routing	策略路由
RADIUS	Remote Authentication Dial-In User Service	远程身份验证拨号用户服务
TCP	Transmission Control Protocol	传输控制协议
SFTP	Secure File Transfer Protocol	安全文件传输协议

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.

IPSec VPN技术与应用

HUAWEI

前言

- 在Internet的传输中，绝大部分数据的内容都是明文传输的，这样就会存在很多潜在的危险，比如：密码、银行帐户的信息被窃取、篡改，用户的身份被冒充，遭受网络恶意攻击等。
- 在企业分支与总部通信等场景部署IPSec VPN后，可对分支与总部之间传输的数据进行保护处理，降低信息泄漏的风险。
- 本章节我们将详细介绍IPSec的基本原理、应用场景、高可靠性及排错思路。

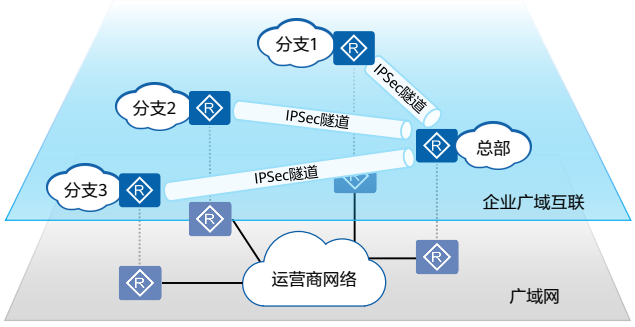
目标

- 学完本课程后，您将能够：
  - 掌握IPSec VPN的基本原理
  - 了解IPSec VPN典型应用场景
  - 掌握高可靠的IPSec VPN配置方法
  - 掌握IPSec VPN的故障排除方法

目录

IPSec VPN的产生背景

- 企业分支之间经常有互联的需求，企业互联的方式很多，可以使用广域网专线或者Internet线路。
- 部分企业从成本和需求的考虑点出发会选择使用Internet进行互联，但是存在信息泄露等安全风险，因此保障数据在传输时不会被窃取或者被篡改成为了重点关注因素。可以在各分支与总部之间建立IPSec隧道，通过将数据报文进行加密传输，达到保障企业安全互联的目的。

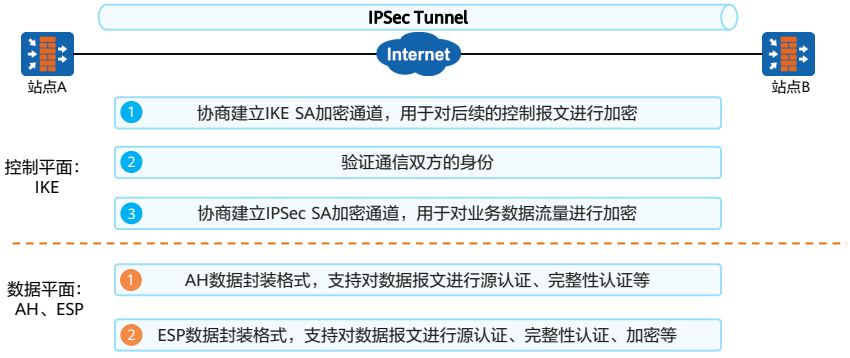


HUAWEI

- 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，以密文的形式在开放网络上传送，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。

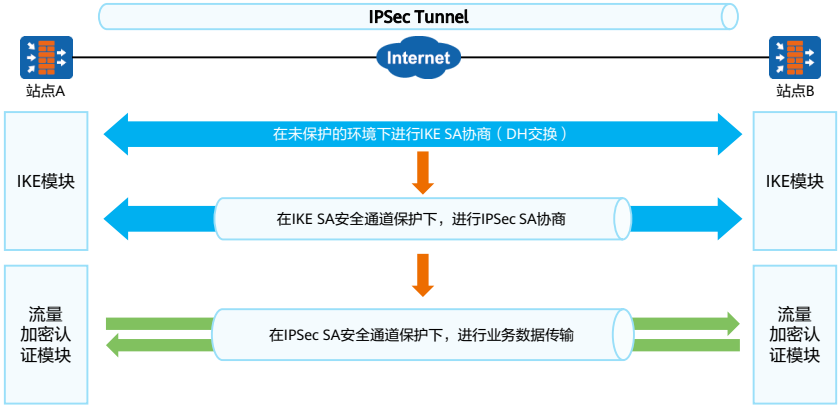
IPSec协议框架

- IPSec（Internet Protocol Security，因特网协议安全协议）是IETF制定的一组开放的网络安全协议。它并不是一个单独的协议，而是一系列为IP网络提供安全性的协议和服务的集合。
- IPSec协议框架主要包含三个标准协议：IKE、AH、ESP。其主要作用如下所示：



IKE SA与IPSec SA

- IPSec对等体需要先后协商两种类型的SA：IKE SA与IPSec SA，协商顺序如下所示。



HUAWEI

- 一个典型的IPSec通信模型中，需要建立一个IKE SA和两个IPSec SA。
- IKE SA与IPSec SA的关系如上图所示，对等体之间建立一个IKE SA完成身份验证和密钥信息交换后，在IKE SA的保护下，根据配置的AH/ESP安全协议等参数协商出一对IPSec SA。此后，对等体间的业务数据将在IPSec SA隧道中加密传输。

IKE SA关键参数

- IKE有两个版本：IKEv1和IKEv2，IPSec对等体在协商建立IKE SA安全通道的过程中，协商参数如下表所示。
- IPSec对等体之间仅需建立一个IKE SA，即可实现数据双向传输。

参数	IKEv1	IKEv2	参数说明
IKE工作模式	主模式 or 野蛮模式	/	IKEv1第一阶段有两种工作模式
DH组	组编号：14、15、16、18、19、20、21、22等		DH算法用于协商对称密钥
加密算法	DES、3DES、AES、SM4	DES、3DES、AES	用于IKE SA的报文加密
认证算法	MD5、SHA1、SHA2、SM3	MD5、SHA1、SHA2	用于IKE SA的报文认证
认证方式	预共享密钥、RSA签名、RSA数字信封、国密数字信封		用于IPSec对等体身份验证
超时时间	缺省为86400秒		IKE SA的生存周期
PRF算法	/	MD5、SHA1、SHA2等	IKEv2伪随机数产生算法

- IKEv2通过初试交换建立IKE SA，不涉及工作模式。
- DH是一种公共密钥交换方法，它用于产生密钥材料，并通过ISAKMP消息在发送和接收设备之间进行密钥材料交换。然后，两端设备各自计算出完全相同的对称密钥。该对称密钥用于计算加密和验证的密钥。
- 加密算法：DES和3DES加密算法不安全，建议使用AES或SM4算法。SM4是国密加密算法。
- 认证算法：MD5和SHA1认证算法不安全，建议使用SHA2-256、SHA2-384、SHA2-512、SM3算法。SM3是国密认证算法。
- PRF算法是IKEv2协商时所使用的伪随机数产生函数的算法，缺省为HMAC-SHA2-256算法。

IPSec SA关键参数

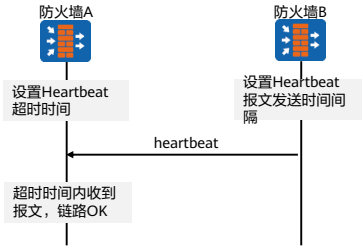
- IPSec SA用于对业务数据进行加密，其协商过程受到IKE SA加密安全通道的保护，协商参数如下表所示。
- IPSec对等体之间至少需要建立两个IPSec SA，才能实现数据双向加密传输（IPSec SA是单向的）。

参数	AH	ESP	参数说明
待保护流量	仅支持认证，不支持加密	支持认证及加密	协商需要保护哪些数据流
封装模式	传输模式、隧道模式		传输模式：不添加新的IP报文头 隧道模式：增加新的IP报文头
加密算法	/	DES、3DES、AES、GMAC、GCM、SM4等	用于IPSec SA的报文加密
认证算法	MD5、SHA1、SHA2、SM3等		用于IPSec SA的报文认证
PFS	是否进行额外的DH交换，协商IPSec SA的对称密钥		PFS可增强IPSec SA的安全性
超时时间	基于时间：缺省为3600秒；基于流量：缺省为5242880KB		IPSec SA的生存周期

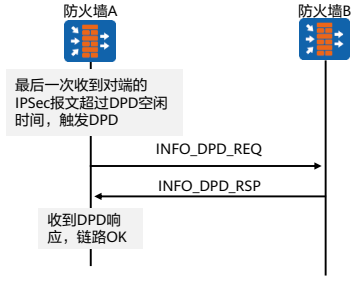
- PFS（Perfect Forward Secrecy，完美前向保密）指的是用于IPSec SA的对称密钥通过单独的一次DH交换产生，并不依赖于IKE SA。这样，即使IKE SA的密钥被破解，也不会影响IPSec SA的安全性。

IKE SA状态检测机制

- 由于IKE协议自身未提供对等体状态监测机制，当其中一端对等体不可达时，另一端无法感知，导致转发至对端的数据流量被丢弃。为快速检测对等体状态，设备提供Heartbeat和DPD两种IKE对等体状态检测机制。
  - Heartbeat检测：本端定时地向对端发送Heartbeat报文来告知对端自己处于活动状态。
  - DPD检测：当一定时间间隔内没有收到对端发来的IPSec流量时，发送DPD报文探测对端的状态。



heartbeat检测机制

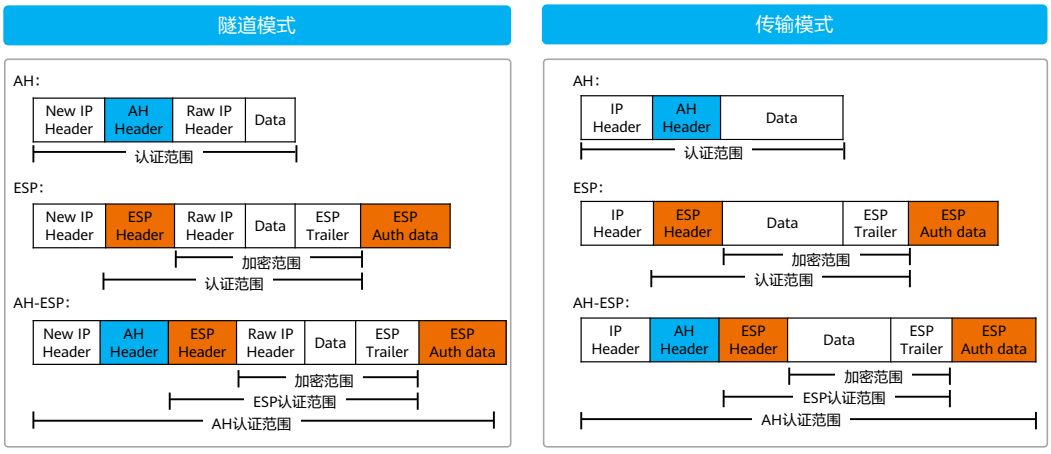


DPD检测机制

HUAWEI

- DPD有如下两种检测模式：
  - 按需型：当本端需要向对端发送IPSec报文时，判断当前距离最后一次收到对端的IPSec报文超过DPD空闲时间，则本端主动向对端发送DPD请求报文。
  - 周期型：如果当前距离最后一次收到对端的IPSec报文或DPD请求报文的时长已超过DPD空闲时间，则本端主动向对端发送DPD请求报文。

IPSec数据封装方式



HUAWEI

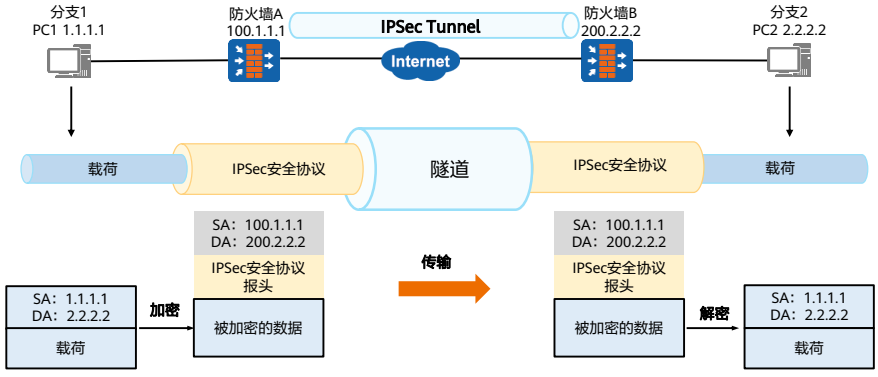
- 传输模式：AH头或ESP头被插入到IP头与传输层协议头之间，保护TCP/UDP/ICMP负载。由于传输模式未添加额外的IP头，所以原始报文中的IP地址在加密后报文的IP头中可见。
- 隧道模式：AH头或ESP头被插到原始IP头之前，另外生成一个新的报文头放到AH头或ESP头之前，保护IP头和负载。
- 在隧道模式下，AH协议的完整性验证范围为包括新增IP头在内的整个IP报文。ESP协议验证报文的完整性检查部分包括ESP头、原IP头、传输层协议头、数据和ESP报尾，但不包括新IP头，因此ESP协议无法保证新IP头的安全。ESP的加密部分包括原IP头、传输层协议头、数据和ESP报尾。

AH和ESP协议对比

安全协议	AH	ESP
协议号	51	50
数据完整性校验	支持（验证整个IP报文）	支持（不验证IP头）
数据源验证	支持	支持
数据加密	不支持	支持
防报文重放攻击	支持	支持
NAT穿越	不支持	支持

IPSec VPN

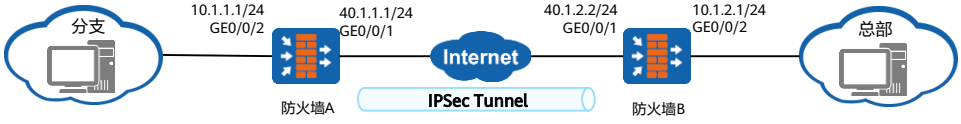
- IPSec的数据封装方式分为传输模式和隧道模式两种，当使用隧道模式时，除保护数据流量外，还能够实现VPN的功能，称为IPSec VPN。下图是分支1与分支2之间使用IPSec VPN加密通信的典型应用场景。



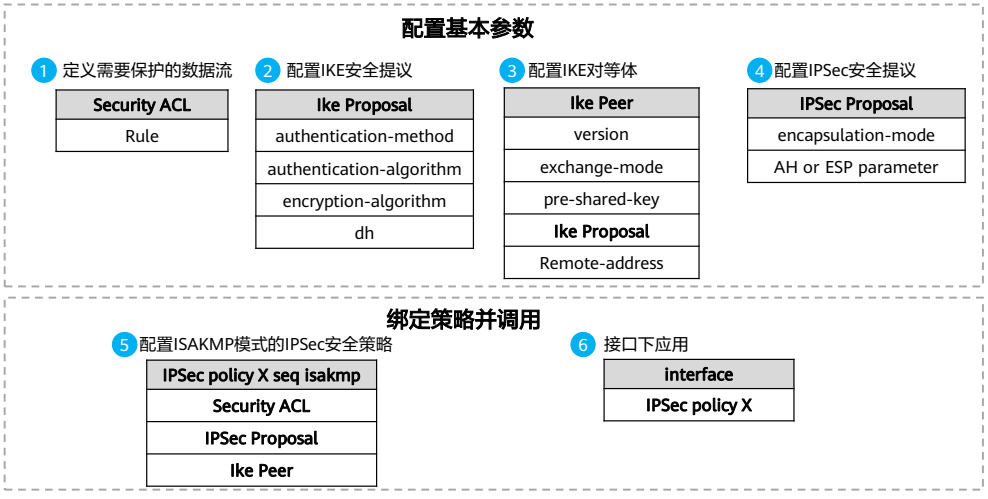
目录

IPSec VPN点到点应用场景

- 点到点IPSec VPN也称为局域网到局域网IPSec VPN或网关到网关IPSec VPN，主要用于两个网关之间建立IPSec隧道，从而实现局域网之间安全地互访。
- 点到点IPSec VPN两端网关必须提供固定的IP地址或固定的域名，通信双方都可以主动发起连接。



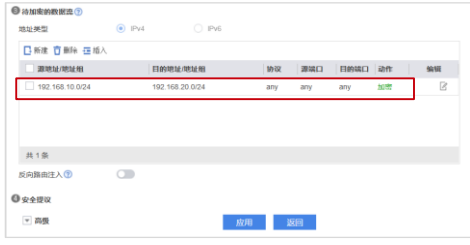
配置思路



- 以介绍IPSec IKEv1的配置流程为例，IKEv2中的ike Peer没有exchange-mode，安全策略相关配置请参考配置手册。

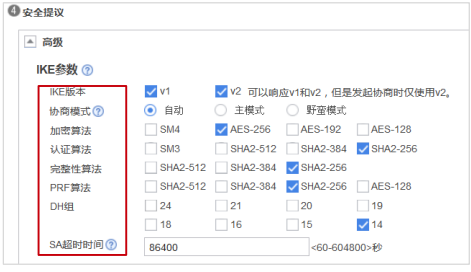
关键配置（1）

- 选择“网络 > IPSec > IPSec”，单击“新建”，建立一条ISAKMP方式（即点到点场景）的IPSec策略。



关键配置 (2)

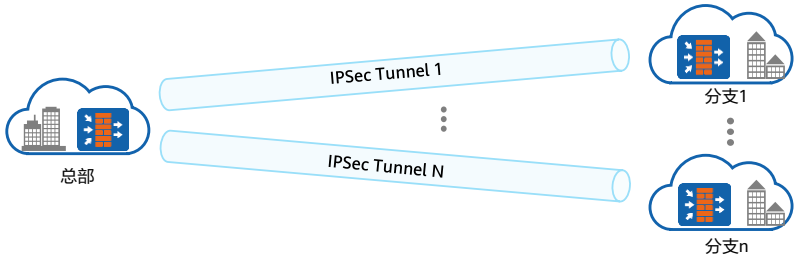
- 配置IPSec策略，选择IKE、IPSec相关参数。



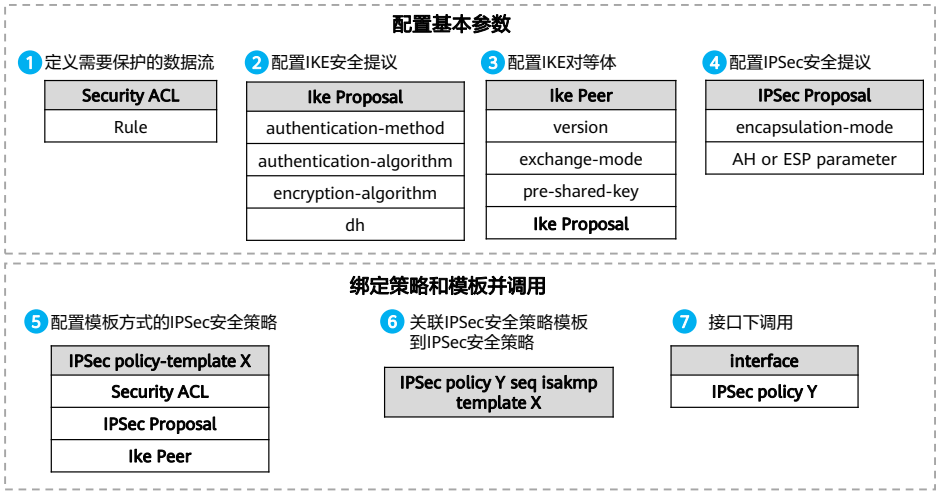
目录

IPSec VPN点到多点应用场景

- 点到多点多用于一个总部与多个分支建立IPSec VPN的场景。在实际的应用中，经常使用Hub-Spoke类型的组网，即一个总部到多个分支机构的组网，分支节点建立到总部的IPSec隧道，各个分支机构之间的通信由总部节点转发和控制。



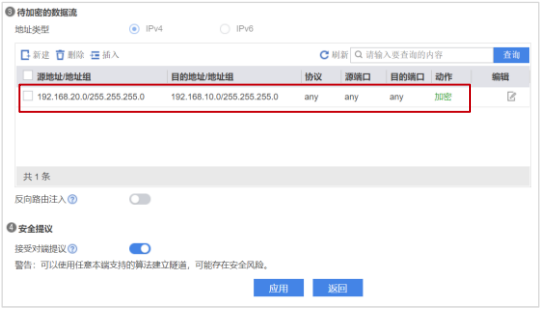
配置思路 - 模板方式



- 采用点到点IPSec VPN传统配置方式时要求指定对端IP地址，很多场景下建立IPSec VPN的一端（比如较小的分支机构、门店）并无公网IP或固定IP。当分支机构众多时，总部需要为每个分支机构单独维护一份配置，总部的配置量无疑将会非常臃肿。此时可以采用IPSec模板方式配置，可以有效的解决以上问题。
- IPSec模板：不限制对端IP地址，可以严格指定对端IP地址（单个IP），可以宽泛指定对端IP地址（IP地址段），也可以干脆不指定对端IP（意味着对端IP可以是任意IP）。
- 本文仅介绍IPSec配置流程，安全策略相关配置请参考配置手册。

关键配置

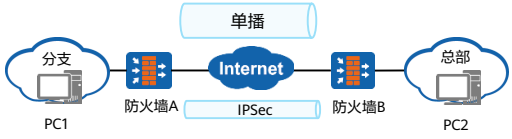
- 选择“网络 > IPSec > IPSec”，单击“新建”，建立模板方式（即点到多点场景）的IPSec策略。



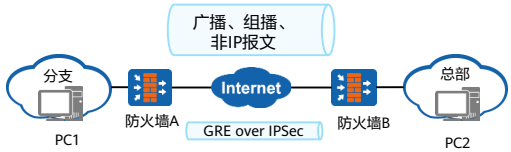
目录

GRE over IPSec应用场景

- IPSec VPN本端设备无法感知对端有几个设备，本端共用一个IPSec SA。报文封装中没有对端设备的下一跳，所以无法传输组播、广播和非IP报文，比如OSPF协议，导致分支与总部的内部网络之间无法使用OSPF路由。
- GRE over IPSec可利用GRE和IPSec的优势，通过GRE将组播、广播和非IP报文封装成普通的IP报文，通过IPSec为封装后的IP报文提供安全地通信，进而可以提供在总部和分支之间安全地传送广播、组播的业务。



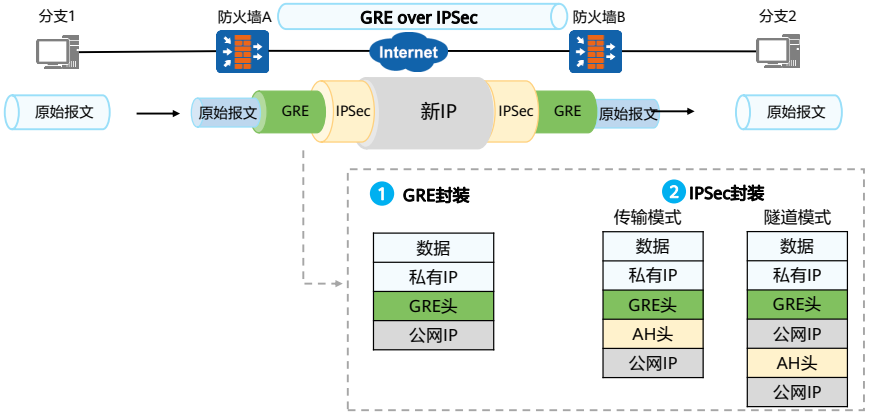
IPSec VPN场景



GRE over IPSec场景

GRE over IPSec报文封装

- 当网关之间采用GRE over IPSec连接时，先进行GRE封装，再进行IPSec封装。GRE over IPSec使用的封装模式为可以是隧道模式也可以是传输模式。采用AH协议的GRE over IPSec报文封装过程如下：



HUAWEI

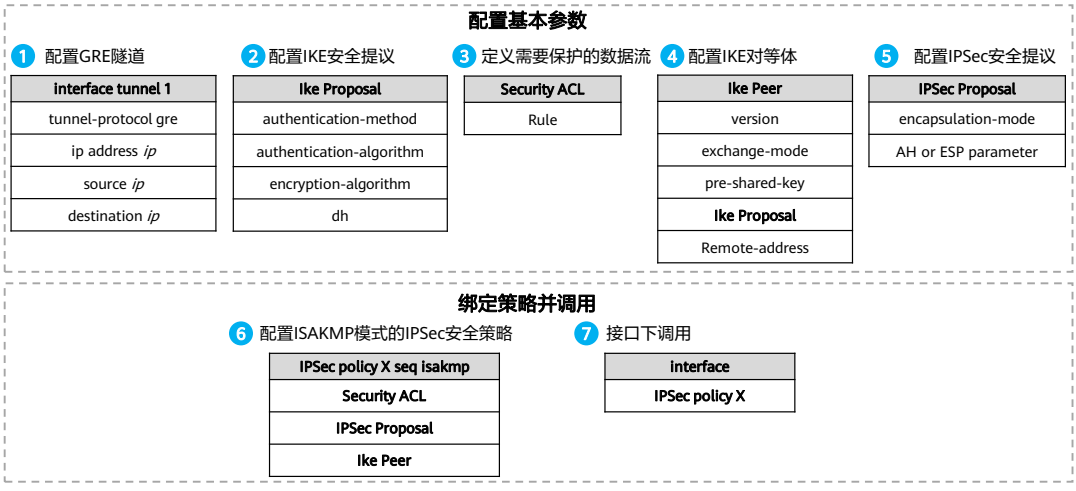
- GRE over IPSec报文封装过程：
  - GRE协议能够支持非IP单播报文，比如IPX报文、组播报文等，原始报文被封装在GRE隧道中。
  - GRE隧道封装包被封装在IPSec隧道封装包中。

GRE over IPSec的优势

特性	GRE是否支持	IPSec是否支持	GRE over IPSec是否支持
支持组播	Y	N	Y
对动态路由协议的支持	Y	N	Y
对丰富的网络层协议的支持	Y	支持有限	Y
机密性	N	Y	Y
完整性	N	Y	Y
数据源验证	N	Y	Y

- 组播：组播类型的报文；
- 动态路由协议：如OSPF、IS-IS等，动态路由协议报文有些是组播或者广播报文；
- 丰富的网络层协议：支持网络层协议，IP协议、IPX协议、ARP协议和ICMP协议等；
- 机密性：支持对报文进行加密；
- 完整性：支持对收到的报文进行校验，检查报文是否完整，是否被改动；
- 数据源认证：对收到数据的源进行认证。

GRE over IPSec的配置思路

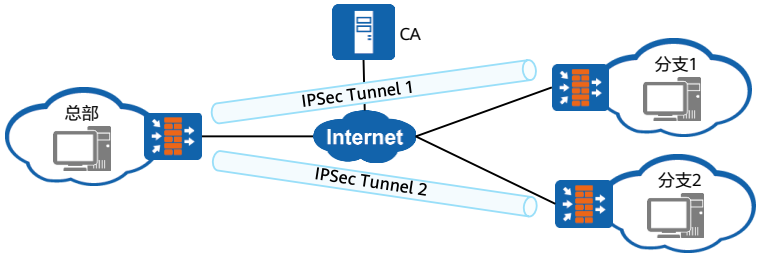


- 以ISAKMP模式的IPSec VPN为例，按照GRE和IPSec点到点配置思路配置即可。

目录

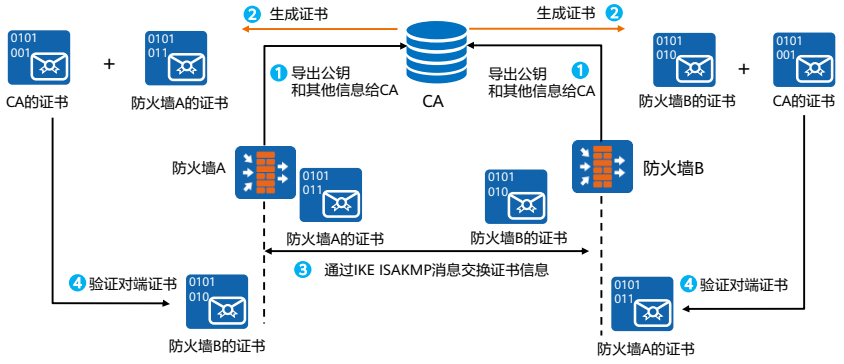
IPSec VPN证书认证场景

- IPSec VPN点到多点场景中，进行身份认证时如果使用预共享密钥方式，总部和每个分部之间形成的对等体都要配置预共享密钥。如果所有对等体都使用同一个密钥，存在安全风险；而每个对等体都使用不同的密钥，又不便于管理和维护。
- 为了解决上述问题，可以使用证书认证。IKE通过借用了PKI中的证书机制来进行对等体的身份认证，不必再为每个对等体配置单独的密钥，降低管理成本。



证书在IPSec VPN中的应用

- 使用证书进行身份认证需要经历两个步骤：
  - 证书导入：使用设备的密钥及必要信息到CA颁发证书，并将成对的证书导入到设备；
  - 证书认证：IPSec身份认证时，各自将导入的本地证书发送给对端验证身份。



HUAWEI

- 使用证书进行身份认证流程如下：
  - 防火墙生成公钥和私钥对并将公钥和实体信息一同发送给CA；
  - CA通过防火墙发送的信息生成CA证书和防火墙的证书，再由防火墙通过在线或者离线的方式进行申请获得；
  - 防火墙通过ISAKMP消息交换证书；
  - 防火墙使用CA证书校验对方的身份。

关键配置 – 防火墙申请本地证书

- 创建公私密钥对。创建一个2048位的RSA密钥对rsa，并设置为可以从设备上导出。

```
[FW] pki rsa local-key-pair create rsakey exportable
```

- 配置PKI实体信息。

```
[FW] pki entity user01
[FW-pki-entity-user01] common-name devicea
[FW-pki-entity-user01] country cn
[FW-pki-entity-user01] ip-address 10.1.61.11
[FW-pki-entity-user01] state Hangzhou
[FW-pki-entity-user01] organization huawei
[FW-pki-entity-user01] organization-unit Training
[FW-pki-entity-user01] quit
```

- 配置为PKI实体离线申请本地证书。申请本地证书时，申请文件中的IP地址需要配置为防火墙建立IPSec隧道时所使用的IP地址。

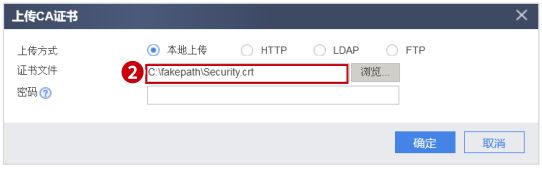
```
[FW] pki realm abc
[FW-pki-realm-abc] entity user01
[FW-pki-realm-abc] rsa local-key-pair rsakey
[FW-pki-realm-abc] quit
[FW] pki enroll-certificate realm abc pkcs10 filename cer_req
```


- 配置RSA密钥对，申请本地证书时，需先配置RSA密钥对生成公钥和私钥。公钥由PKI实体发送给CA，可以被对端用来加密明文；私钥由PKI实体保留，可以被用来数字签名和解密对端发送过来的密文。
- 完成配置后，可执行命令display pki cert-req查看证书请求文件的内容。
- 本地证书注册成功后，可以通过带外方式下载本地证书。下载后，可以通过文件传输协议导入到设备的存储介质中。

关键配置 - 导入本地及CA证书

- 证书申请好之后，在“对象 > 证书 > 本地证书”中导入本地证书：

- 在“对象 > 证书 > CA证书”中导入CA认证：



HUAWEI

关键配置 - 采用RSA签名认证

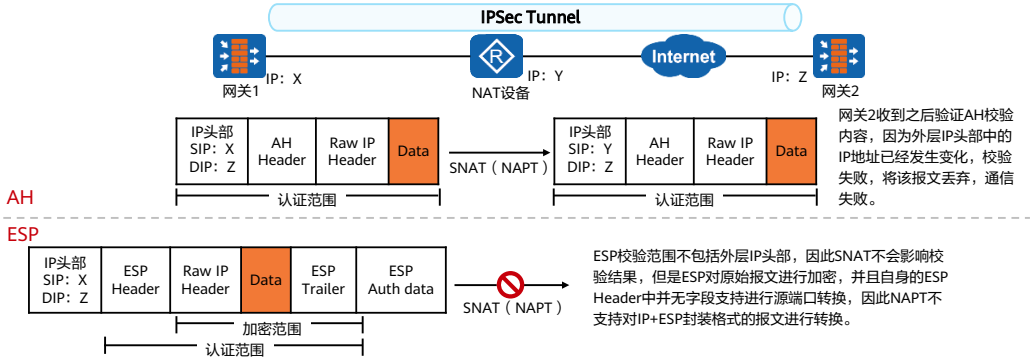
- 选择“网络 > IPSec > IPSec”，在“IPSec策略列表”下单击“新建”。
- 按如下参数配置“基本配置”：
  - 认证方式选择“RSA签名”；
  - 选择已导入的证书进行验证，本端ID和对端ID需要与申请证书时填写的一致。

- 如果此处选择“RSA数字信封”模式，除了导入本端证书，还需要导入对端证书，此证书中的部分信息将会在隧道建立过程中发给对端，供双方验证对端的合法性。

目录

IPSec VPN在NAT场景中存在的问题

- 默认情况下，IPSec VPN传输数据时外层IP头部之上为ESP header或者AH header，传输模式和隧道模式在传输路径中存在源NAT设备时都会遇到问题。
- 下图以隧道模式为例介绍：

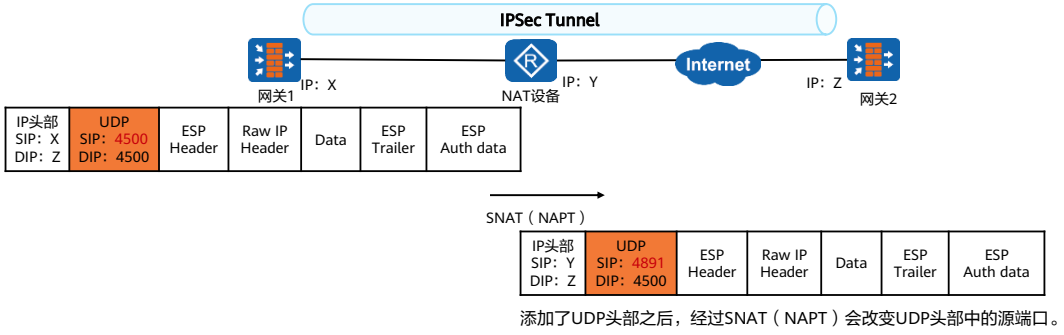


HUAWEI

- 采用AH安全协议完全不支持NAT穿越场景，ESP安全协议受限于端口，需要用额外端口实现。

NAT穿越功能简介

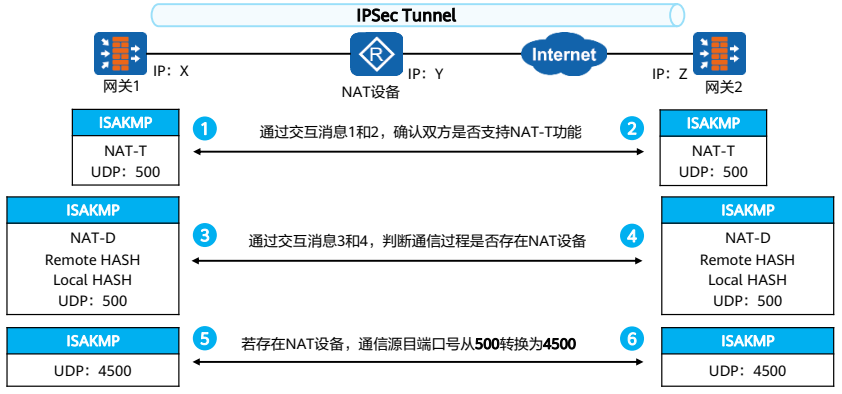
- 为解决上述问题，必须在建立IPSec隧道的两个网关上开启NAT穿越功能（ NAT Traversal ）。
- 开启NAT穿越之后，当检测到（ IKE协商过程中进行检测 ）两台网关中间存在NAT设备，ESP报文会被封装在一个UDP头部中，源目端口号4500，以此支持NAT转换。



添加了UDP头部之后，经过SNAT（ NAPT ）会改变UDP头部中的源端口。

NAT穿越检测原理

- 以IKEv1主模式为例，介绍NAT穿越检测原理。

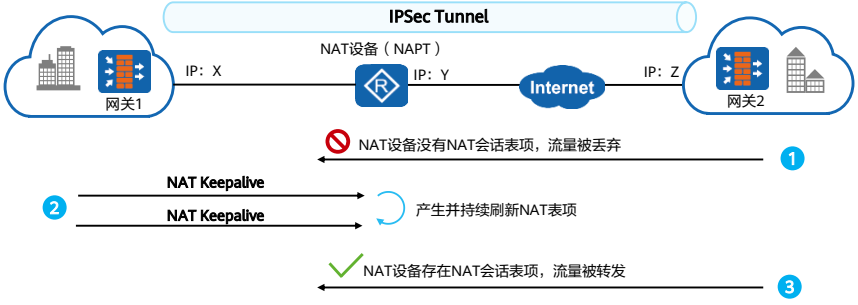


HUAWEI

- 开启NAT穿越时，IKEv1协商第一阶段的前两个消息会发送标识NAT穿越（NAT Traversal，简称NAT-T）能力的Vendor ID载荷（主模式和野蛮模式都是）。用于检查通信双方是否支持NAT-T，当双方都在各自的消息中包含了该载荷时，才会进行相关的NAT-T协商。
- 主模式消息3和消息4中发送NAT-D（NAT Discovery）载荷。NAT-D载荷用于探测两个要建立IPSec隧道的网关之间是否存在NAT设备以及NAT设备的位置。
  - Remote HASH：指将发送报文中的目的IP地址和端口号进行HASH运算后的数值。
  - Local HASH：指将发送报文中的源IP地址和端口号进行HASH运算后的数值。
  - 通过对比Remote HASH和Local HASH值，可以判断网关之间是否存在NAT设备以及NAT网关的位置。
- 发现NAT设备后，后续ISAKMP消息（主模式从消息5开始）的端口号转换为4500。

NAT穿越会话保活机制

- 如图所示为NAPT场景，网关1处在NAT设备之后。若网关1未主动发起访问，则NAT设备不存在NAT会话表项，此时网关2无法访问网关1。
- 为解决以上问题，需要网关1开启NAT会话保活功能。开启后，网关1会定期发送NAT Keepalive报文，使NAT设备上产生并维持NAT表项，使得网关2可以主动访问网关1。

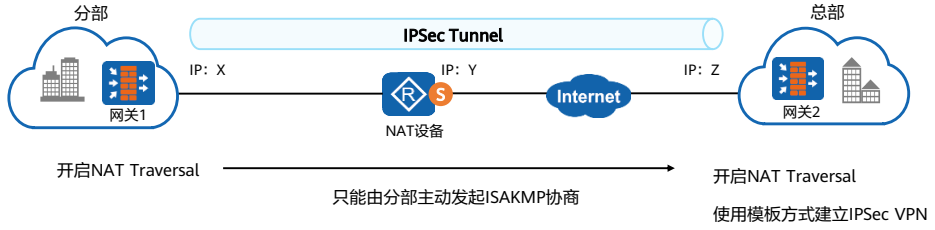


HUAWEI

- NAT Keepalive报文格式非常简单，在UDP头部之后为两个十六进制F，用于刷新NAT设备会话表项。
- 华为防火墙检测出IPSec VPN处于NAT穿越场景后，NAT设备内侧设备（发起方网关1）会定期发送NAT Keepalive报文，保证中间NAT设备上的源NAT会话不老化。

NAT穿越场景 (1)

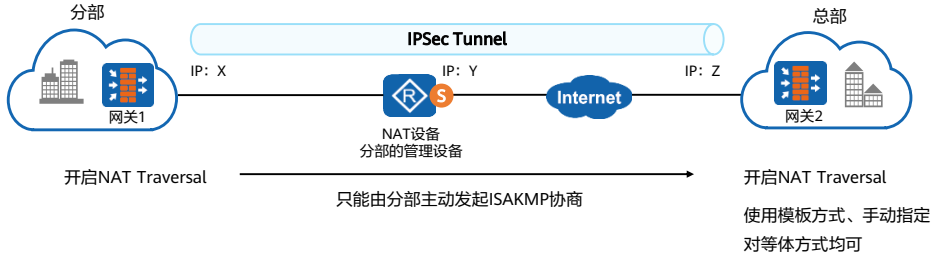
- 该场景中，NAT设备位于分部网络之外，分部网关1出接口的私网IP地址X，经过NAT设备转换后变为公网IP地址Y。由于总部无从获知经过NAT设备转换后的分部公网IP地址，也就无法在总部网关2上明确指定对端的公网地址。因此，总部网关2必须使用模板方式来配置IPSec，同时总部和分布的网关都要开启NAT穿越功能。
- 总部既然使用了模板方式，那就无法主动访问分部，只能由分部主动向总部发起ISAKMP协商。



- 该场景中，分部网关为防火墙，NAT设备的公网地址对总部不可见，所以需要使用模板方式建立IPSec，此时虽然分部与总部之间存在NAT设备，但是防火墙的安全策略相关配置与非NAT穿越场景一致。
- 网关1与网关2的安全区域划分规则，连接内部网络的区域为trust区域，连接外部网络的区域为untrust区域，设备本身地址为local区域，安全策略配置如下：
  - 网关1安全策略：
    - local -> untrust，网关1的IP地址：X -> 网关2的IP地址：Z；
    - trust -> untrust，分部内网地址 -> 总部内网地址；
    - untrust -> local，网关2的IP地址：Z -> 网关1的IP地址：X。
  - 网关2安全策略：
    - local -> untrust，网关2的IP地址：Z -> any；
    - trust -> untrust，总部内网地址 -> 分部内网地址；
    - untrust -> local，any -> 网关2的IP地址：Z。

NAT穿越场景 (2)

- 该场景中，NAT设备位于分部网络之外，分部网关1出接口的私网IP地址X，经过NAT设备转换后变为公网IP地址Y。NAT转换设备为分部自己管理设备，并且公网IP地址固定，此时转换后的公网地址可知。因此，总部可以使用模板方式或者手动指定对等体的方式配置IPSec VPN。
- 由于NAT设备只进行源地址转换，所以依旧只能由分部主动发起ISAKMP协商。

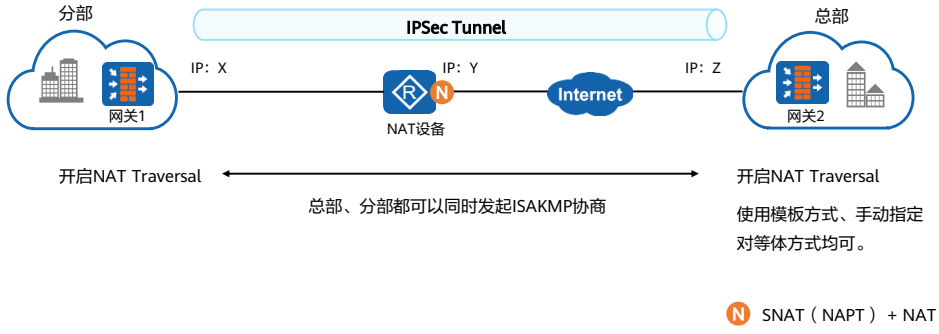


HUAWEI

- 该场景中，分部网关为防火墙，NAT设备的公网地址固定，总部对NAT设备的公网地址可知，所以可以使用模板方式或者手动指定对等体的方式配置IPSec，此时由于分部与总部之间存在NAT设备，所以防火墙的安全策略相关配置与非NAT穿越场景有差别。
- 网关1与网关2的安全区域划分规则，连接内部网络的区域为trust区域，连接外部网络的区域为untrust区域，设备本身地址为local区域，安全策略配置如下：
  - 网关1安全策略：
    - local -> untrust，网关1的IP：X -> 网关2的IP：Z；
    - trust -> untrust，分部内网地址 -> 总部内网地址；
    - untrust -> local，网关2的IP：Z -> 网关1的IP：X。
  - 网关2安全策略：
    - local -> untrust，网关2的IP：Z -> NAT设备的IP：Y；
    - trust -> untrust，总部内网地址 -> 分部内网地址；
    - untrust -> local，NAT设备的IP：Y -> 网关2的IP：Z。

NAT穿越场景 (3)

- 该场景中，NAT设备为分部管理设备，提供NAT Server功能，映射网关的接口地址，总部上使用手动指定对等体方式配置IPSec，此时可以实现总部主动发起ISAKMP协商以及流量访问。



HUAWEI

- 该场景中，分部网关为防火墙，NAT设备的公网地址固定，总部对NAT设备的公网地址可知，所以可以使用模板方式或者手动指定对等体的方式配置IPSec；由于NAT设备配置了NAT Server将网关1的IP：X映射到公网，所以此时总部也可以主动向分部发起ISAKMP协商。
- 网关1与网关2的安全区域划分规则，连接内部网络的区域为trust区域，连接外部网络的区域为untrust区域，设备本身地址为local区域，安全策略配置如下：
  - 网关1安全策略：
    - local -> untrust，网关1的IP：X -> 网关2的IP：Z；
    - trust -> untrust，分部内网地址 -> 总部内网地址；
    - untrust -> local，网关2的IP：Z -> 网关1的IP：X。
  - 网关2安全策略：
    - local -> untrust，网关2的IP：Z -> NAT设备的IP：Y；
    - trust -> untrust，总部内网地址 -> 分部内网地址；
    - untrust -> local，NAT设备的IP：Y -> 网关2的IP：Z。

NAT穿越场景关键配置

- 开启NAT穿越功能命令。

```
<sysname> system-view
[sysname] ike Peer Peer1
[sysname-ike-Peer-Peer1] nat traversal
```

- 配置NAT穿越功能时，使用的IPSec安全提议ipsec proposal只能选择ESP安全协议。

```
<sysname> system-view
[sysname] ipsec proposal newprop1
[sysname-ipsec-proposal-newprop1] transform esp
```

- 配置IPSec NAT穿越的UDP端口号（默认端口号为UDP 4500），可以执行命令ipsec nat-traversal source-port进行配置。

```
<sysname> system-view
[sysname] ipsec nat-traversal source-port 4510
```

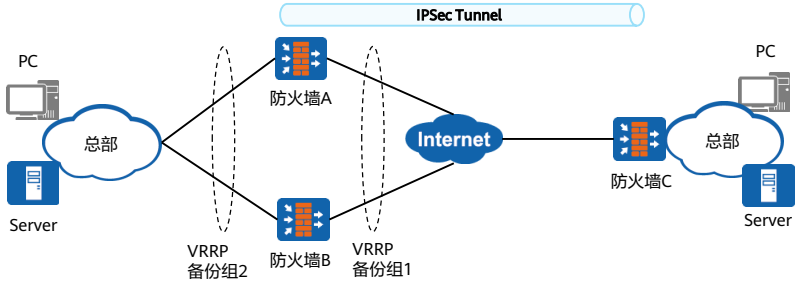
- 当对等体间存在NAT网关，为防止NAT表项老化，NAT网关内网侧的设备会以一定的时间间隔向对端发送NAT Keepalive报文，以维持NAT会话的存活。

```
<sysname> system-view
[sysname] ike nat-keepalive-timer interval 30
```

目录

IPSec双机热备

- 总部分支场景下，防火墙A和防火墙B对外配置VRRP备份组1，并在VRRP备份组1和分支网关防火墙C的物理接口之间建立IPSec隧道。当主用防火墙A物理接口、链路或主机故障时，流量被引导到备用防火墙B进行IPSec和转发处理。这种情况下，原有的IPSec隧道并不会被拆除，切换速度更具优势。

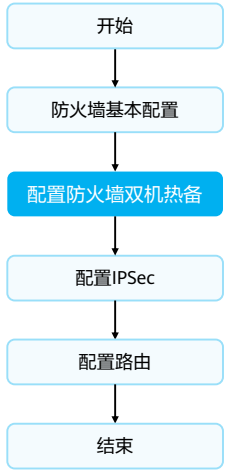


HUAWEI

- 防火墙支持主备方式和负载分担方式两种双机热备，需根据实际组网情况进行选择。上文主要介绍的是主备方式，负载分担方式可自行参考华为防火墙产品手册进行学习。

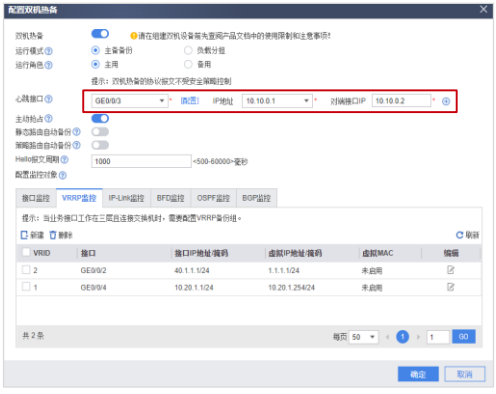
配置思路

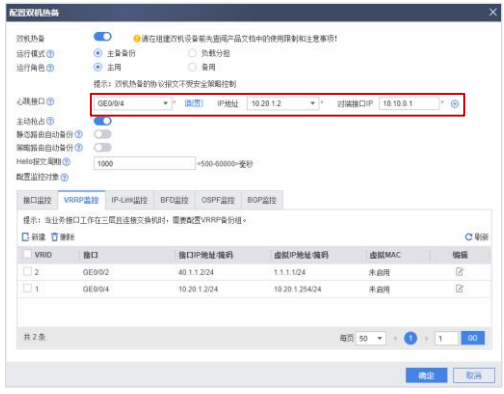
- 完成防火墙基本配置，比如接口添加安全区域和相关策略等；
- 配置防火墙双机热备，采用主备方式；
- 配置IPSec基本参数，包括对端和本段信息、选择感兴趣数据流和安全提议等；
- 配置路由保证互联互通。



关键配置（1）

- 假设两台防火墙的心跳接口为GE0/0/3，上下行接口为GE0/0/2、GE0/0/4，双机热备关键配置如下：





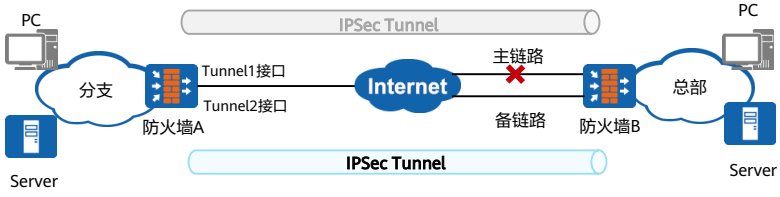
关键配置 (2)

- 假设两台防火墙连接Internet接口为GE0/0/2，这两个接口组成VRRP冗余备份组2，总部IPSec关键配置如下：

目录

IPSec主备链路冗余备份

- 为提高网络可靠性，企业分支通过两条链路与企业总部建立IPSec连接，形成两条主备链路。当主链路故障时，启用备份链路建立IPSec隧道，旧的IPSec隧道被拆除，流量切换也随之完成。
- 如下图所示，防火墙A通过两条主备链路连接防火墙B，正常情况下，流量通过由主链路和Tunnel1接口建立的IPSec隧道传输；当主链路故障时，防火墙A感知变化，采用Tunnel2接口与防火墙B的备份链路建立IPSec隧道。



HUAWEI

- 在防火墙A上创建两个Tunnel接口，借用同一个物理接口的IP地址，分别应用不同的IPSec安全策略，在防火墙B的两个物理接口上也分别应用不同的IPSec安全策略，这样就可以创建主备两条IPSec隧道。

关键配置 (1)

- 总部防火墙的主用出口为GE0/0/1，备用出口为GE0/0/2，需要创建两套IPSec安全策略。

```
[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 b
[FW_B-ipsec-policy-isakmp-map1-10] quit
```

```
[FW_B] ipsec policy map2 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 b
[FW_B-ipsec-policy-isakmp-map1-10] quit
```

- 分别调用在两个出接口中。

```
[FW_B] interface GigabitEthernet 0/0/1
[FW_B-GigabitEthernet0/0/1] ipsec policy map1
[FW_B-GigabitEthernet0/0/1] quit
[FW_B] interface GigabitEthernet 0/0/2
[FW_B-GigabitEthernet0/0/2] ipsec policy map2
[FW_B-GigabitEthernet0/0/2] quit
```

关键配置 (2)

- 分支防火墙上创建两个Tunnel接口，借用同一个物理接口的IP地址，分别应用不同的IPSec安全策略。

```
[FW_A] interface tunnel 1
[FW_A-Tunnel1] ip address unnumbered interface GigabitEthernet 0/0/1
[FW_A-Tunnel1] tunnel-protocol ipsec
[FW_A-Tunnel1] quit
```

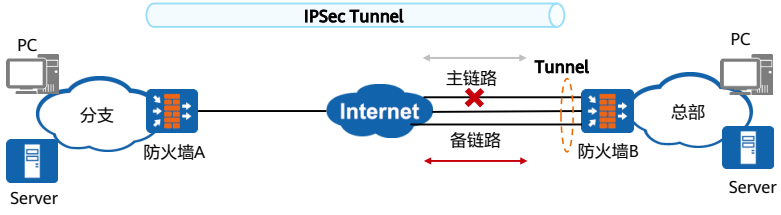
```
[FW_A] interface tunnel 2
[FW_A-Tunnel1] ip address unnumbered interface GigabitEthernet 0/0/1
[FW_A-Tunnel1] tunnel-protocol ipsec
[FW_A-Tunnel1] quit
```

- 分别调用在两个出接口中。

```
[FW_A] interface tunnel 1
[FW_A-Tunnel1] ipsec policy map1
[FW_A-Tunnel1] quit
[FW_A] interface tunnel 2
[FW_A-Tunnel2] ipsec policy map2
[FW_A-Tunnel2] quit
```

IPSec多链路冗余备份

- 为提高网络可靠性，企业分支通过两条或多条链路与企业总部建立IPSec连接。当主物理链路失效时，其路由变为不可达，流量切换到备用链路。IPSec隧道不需要进行重协商，可快速完成流量切换。
- 如下图所示，防火墙A通过两条主备链路连接防火墙B，系统在防火墙A的物理接口与防火墙B的Tunnel接口之间建立一个IPSec隧道，流量通过Tunnel接口进行IPSec处理，然后通过路由表选择物理接口发送。当主物理链路失效时，其路由变为不可达，流量自然切换到备用链路。



HUAWEI

- 通过Tunnel接口进行链路冗余备份可以实现多条链路的冗余备份，而且与主备链路冗余备份相比，配置更简单，流量切换速度更快。

关键配置

- 在总部设备上创建隧道接口与分部建立IPSec VPN，当主链路故障时，主链路路由失效，流量切换到备链路传输，并且主备链路切换时，保证IPSec流量不中断。

```
[FW_B] interface tunnel 0
[FW_B-tunnel0] tunnel-protocol ipsec
[FW_B-tunnel0] ip address 1.1.0.2 24
[FW_B-tunnel0] ipsec policy map1
[FW_B-tunnel0] quit
```

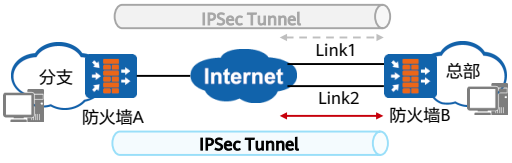
- 配置到分部的静态路由，此处假设分部的地址为10.4.0.0/24。

```
[FW_B] ip route-static 10.4.0.0 255.255.255.0 tunnel 0
```

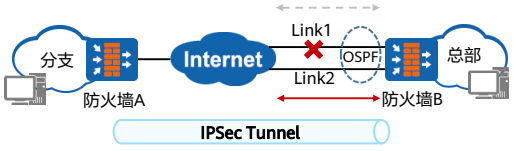
目录

智能选路

- 防火墙作为分支的网关时，可以通过配置IPSec智能选路功能实现多条IPSec隧道动态切换。按照链路切换机制的不同可以分为两种不同场景：基于链路质量探测结果和基于路由状态变化。
  - 基于链路质量探测结果：防火墙实时检测当前IPSec隧道的时延或丢包率，在时延或丢包率高于设定的阈值时，动态切换到备用链路上重新建立IPSec隧道。
  - 基于路由状态变化：根据路由状态建立IPSec隧道，当链路出现故障后，路由不可达，基于路由变化自动将IPSec隧道切换到备链路。



基于链路质量探测结果切换



基于路由状态变化切换

HUAWEI

- 基于链路质量探测结果切换：在防火墙B上配置IPSec智能选路功能后，防火墙B会选择一条链路建立IPSec隧道（Link1）。而后防火墙B通过发送ICMP报文检测IPSec隧道的时延或丢包率。当隧道的时延或丢包率高于设定的阈值时，防火墙B会拆除当前的IPSec隧道，并选择另一条链路建立IPSec隧道（Link2）。这样，就能确保分支和总部之间始终使用满足质量要求的IPSec隧道通信。
- 基于路由状态变化切换：从分支网关防火墙B到总部网关防火墙A之间有两条链路Link1和Link2，防火墙B与Internet之间运行动态路由协议（此处以OSPF为例）。在防火墙B上配置IPSec智能选路功能，可以实现分支和总部之间多条IPSec隧道动态切换。Link1和Link2链路状态都正常的情况下，防火墙B会选择一条链路建立IPSec隧道，例如选择Link1链路。当Link1链路出现故障时，通过Link1到达防火墙A的路由就会消失，于是防火墙B会根路由变化自动将IPSec隧道切换到Link2上。

目录

IPSec诊断 - Web

- 在使用IPSec时，如出现故障，可通过以下方式来对故障进行诊断。
  - 选择“监控 > 诊断中心”，单击“IPSec诊断”。
  - 配置IPSec诊断：诊断对象、IPSec策略名称、本端接口及策略名称。单击“诊断”，即可得到诊断信息。

IPSec诊断- CLI

- 查看IPSec处理报文的统计信息，如受安全保护的进出报文统计信息、加解密报文统计信息、被丢弃的受安全保护的详细统计信息以及IKE协商相关的报文统计信息等，这有助于IPSec故障诊断和维护。

```
<sysname> display ipsec statistics
```

- 查看IKE SA协商结果。
  - display ike sa命令可以查看到的信息包括：安全联盟的连接索引、安全联盟的对端IP地址、VPN实例名称、SA所属阶段、对端ID类型、对端ID、此安全联盟的状态。

```
<sysname> display ike sa
```

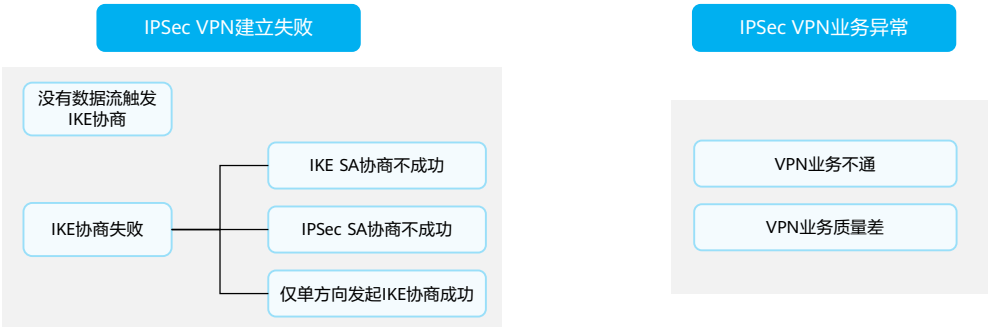
- 查看IPSec SA的配置信息。

```
<sysname> display ipsec sa
```


- display ipsec statistics命令输出信息描述
  - IPSec statistics information：PSec报文统计信息。
  - Number of IPSec tunnels：IPSec隧道数目。
  - Number of standby IPSec tunnels：业务板备份时，备用IPSec隧道数目。
  - the security packet statistics：受安全保护的报文统计信息。
    - input/output security packets：受安全保护的进出报文数。
    - input/output security bytes：受安全保护的进出字节数。
    - input/output dropped security packets：被丢弃的受安全保护的进出报文数。
    - the encrypt packet statistics：加密报文的统计信息。
    - the decrypt packet statistics：解密报文的统计信息。
    - dropped security packet detail：被丢弃的受安全保护报文的详细统计信息。
    - negotiate about packet statistics：IKE协商相关的报文统计信息。

IPSec VPN主要故障

- 从故障现象的维度进行划分，IPSec故障可分为如下两大类：
  - IPSec隧道建立失败（隧道协商失败）。
  - IPSec隧道建立成功后业务异常（加密数据流不通）。

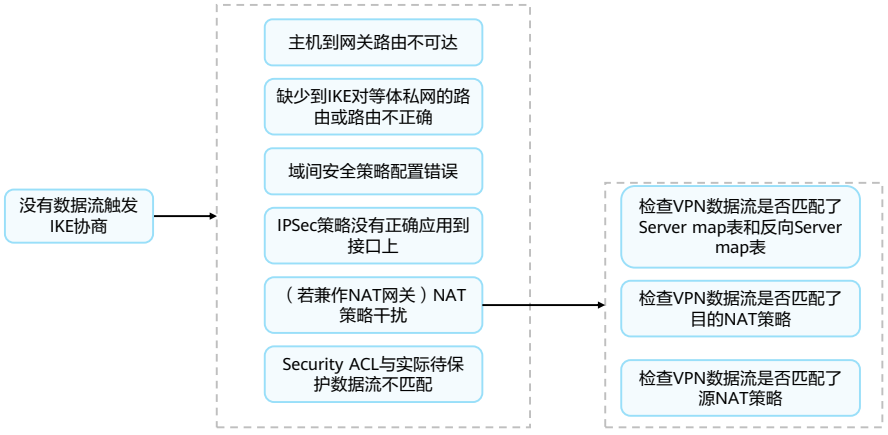


HUAWEI

- IPSec故障分析可以按照故障出现的先后顺序从以下几个现象入手：
  - 配置阶段：IPSec配置界面不可见。
  - 业务触发阶段：没有数据流触发IKE协商。
  - IKE协商阶段：IKE协商不成功（IKE SA、IPSec SA协商不成功）。
  - 数据传输阶段：IKE协商成功，但VPN业务异常（不通或质量不好）。
- 其中IKE协商不成功是IPSec故障的核心问题，可以结合IKE协商过程进行深入分析；其它故障仅表现为IPSec业务故障，多为防火墙基本特性的错误配置，如license、接口、链路、路由、安全区域、NAT等，需要结合具体场景来处理。

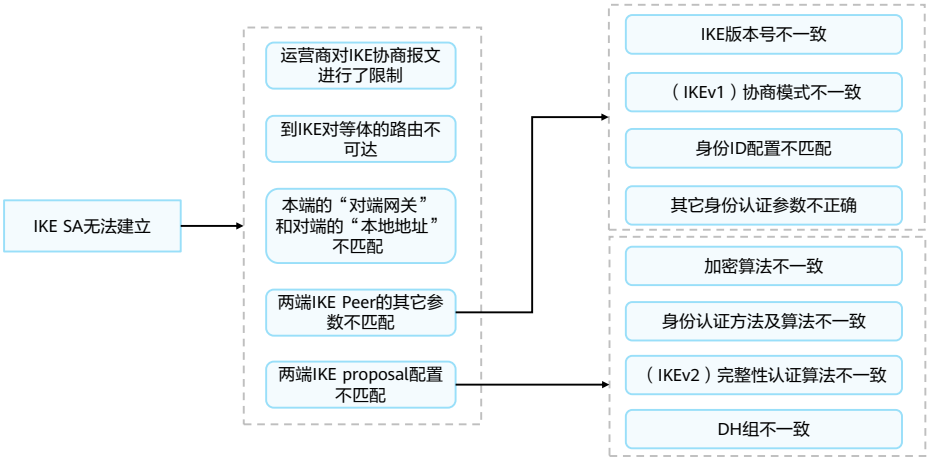
IPSec VPN故障处理思路 - 没有数据流触发IKE协商

- IKE没有建立成功，首先需要检查是否有数据流触发IKE协商，可能原因和检查措施如下：



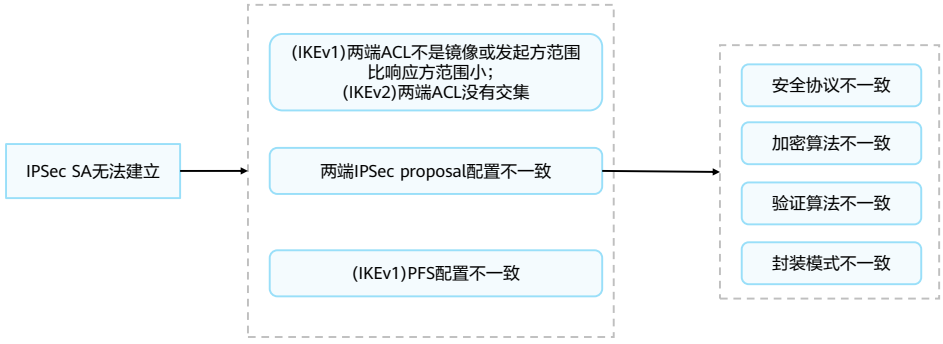
IPSec VPN故障处理思路 - IKE SA协商不成功

- 有数据流触发IKE协商，但是IKE协商失败，可能原因如下：



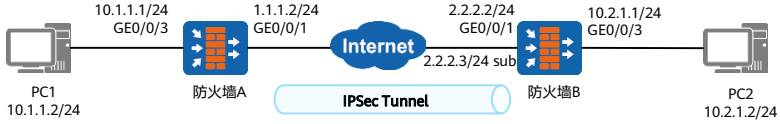
IPSec VPN故障处理思路 - IPSec SA协商不成功

- IKE协商成功后，IPSec SA无法建立，可能原因如下：



案例一：故障现象

- 在两台防火墙之间建立IPSec隧道。组网如图所示，在修改参数之前，隧道能够建立成功。当在防火墙B的公网接口增加了sub地址并修改了IPSec配置后，发现隧道建立不成功。经检查，两端IPSec和IKE参数配置均正确。路由、接口、安全策略等配置也正确。



- 有时为了使路由设备的一个接口能够与多个子网相连，可以在一个接口上配置多个IP地址，其中一个为主IP地址，其余为从IP地址。Sub地址就是接口的从IP地址。

案例一：故障分析

- 检查防火墙A上IKE SA是否存在，执行display ike sa命令，发现sa number已经变成0。

```
<FW_A> display ike sa
current ike sa number: 0
```

- 检查防火墙A上IKE对等体的配置信息，执行display ike peer命令，防火墙A的remote address为2.2.2.2。

```
[FW_A] display ike peer brief
current ike Peer number: 1
--------------------------------------------------------------------------------
 Peer Name    Version  Exchange-mode  Proposal  Id-type  RemoteAddr
--------------------------------------------------------------------------------
 b            v1v2     N/A            10        IP       2.2.2.2
```

- 在防火墙B上查询配置发现，防火墙A的remote address和防火墙B的local address不一致。

```
[FW_B-ipsec-policy-isakmp-map1-10]display this
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-Peer a
 proposal tran1
 local-address 2.2.2.3
```


- 主要从IKE对等体间路由、IKE Peer和IKE Proposal等方面进行分析。故障由防火墙B的公网接口增加sub地址引起，猜测可能是sub地址触发了IPSec协商，使IKE协商失败导致。

案例一：故障处理

- 已经得知是本端的“对端网关”和对端的“本地地址”不匹配导致IKE协商失败，故只要在防火墙A上修改IKE对等体的remote address即可。

```
[FW_A] ike Peer b
[FW_A-ike-Peer-b] remote-address 2.2.2.3
[FW_A-ike-Peer-b] quit
```

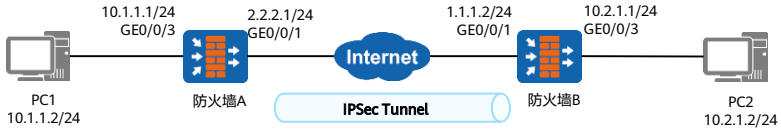
- 两端私网再次ping测试已通，查看IKE SA，发现已经重新建立。

```
[FW_A] display ike sa
current ike sa number: 2
---------------------------------------------------------------------
conn-id    Peer                 flag         phase   vpn
---------------------------------------------------------------------
40003      2.2.2.3              RD|ST         v2:2  public
3          2.2.2.3              RD|ST         v2:1  public
```

- 总结：在配置IPSec安全策略时，local-address命令为可选配置。当本端发起IPSec隧道协商的IP地址与实际应用IPSec策略的接口IP地址不同时，需要配置local-address为本端发起协商的IP地址，且该地址需要和对端使用remote-address命令设置的目的地址一致。

案例二：故障现象

- 在防火墙A与防火墙B之间建立点到点IPSec VPN，配置完成后，出现以下情况：
  - 从PC1 ping PC2，无法ping通，检查IPSec VPN未建立成功；
  - 从PC2 ping 防火墙A的GE0/0/3接口，可以ping通，并正常建立隧道；
  - 经检查，各PC的IP地址、网关等基本配置无误；防火墙A和防火墙B的IP地址、路由、安全域和域间策略等基本配置都无误。



案例二：故障分析 (1)

- 在PC2可以ping通PC1的情况下，执行display ike sa、 display ipsec sa命令，防火墙A和防火墙B的IKE SA、IPSec SA可以正常建立。

[FW_A] **display ike sa**
current ike sa number: 2

conn-id	Peer	flag	phase	vpn
40050	1.1.1.2	RD|ST	v1:2	public
40049	1.1.1.2	RD|ST	v1:1	public

[FW_B] **display ike sa**
current ike sa number: 2

conn-id	Peer	flag	phase	vpn
40050	2.2.2.1	RD|ST	v1:2	public
40049	2.2.2.1	RD|ST	v1:1	public

[FW_A] **display ipsec sa**
ipsec sa information:
Interface: GigabitEthernet0/0/1
IPSec policy name: "pc1"
Sequence number : 1
Acl group : 3000/IPv4
Acl rule : 5
Mode : isakmp
Connection ID : 67108879
Encapsulation mode: Tunnel
Failover state : Master

[FW_B] **display ipsec sa**
ipsec sa information:
Interface: GigabitEthernet0/0/1
IPSec policy name: "pc2"
Sequence number : 1
Acl group : 3000/IPv4
Acl rule : 5
Mode : isakmp
Connection ID : 67108879
Encapsulation mode: Tunnel
Failover state : Master

- 由于已经排除IP地址、路由、域间策略等基本设置无误，且执行display ike sa、display ipsec sa命令后，发现SA无异常，继续排查其他问题。

案例二：故障分析 (2)

- 执行display acl命令，发现ACL的规则范围有问题。

```
[FW_A] display acl 3000
Acl's step is 5
 rule 5 permit ip source 10.1.1.1 0.0.0.0 destination 10.2.1.0 0.255.255.255
```

```
[FW_B] display acl 3000
Acl's step is 5
 rule 5 permit ip source 10.2.1.0 0.255.255.255 destination 10.1.1.1 0.0.0.0
```

- 从IKE阶段一和阶段二的可能原因逐一排查，执行display acl命令后发现两端ACL规则未包含PC1的IP地址，可确定这是ACL未正确匹配兴趣流引起的问题。

案例二：故障处理与总结

- 由于防火墙A和防火墙B上配置的ACL规则没有包含PC1的IP地址，导致从PC1 ping PC2时业务不通。修改防火墙上的ACL规则后问题解决。

```
[FW_A-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.2.1.0 0.255.255.255
Warning: The rule already exists. Are you sure to update? [Y/N]:y
```

```
[FW_B-acl-adv-3000] rule 5 permit ip source 10.2.1.0 0.255.255.255 destination 10.1.1.0 0.0.0.255
Warning: The rule already exists. Are you sure to update? [Y/N]:y
```

- IPSec使用高级ACL定义需要保护的数据流，建议检查隧道两端的ACL规则是否完全包含需要保护的数据流，且保持隧道两端的ACL规则互为镜像。

- 隧道两端配成镜像并不是必要条件，IKEv1要求两端配置的ACL规则互为镜像或发起方配置的ACL规则为响应方的子集。IKEv2取双方ACL规则交集作为协商结果。
- 实际配置中建议将隧道两端的ACL规则配成互为镜像，既简单也不容易出错。

思考题

1. （多选题）根据对报文的封装形式，IPSec的封装模式可以分为以下哪几种？（　　）

   A. 传输模式

   B. 隧道模式

   C. 主模式

   D. 快速模式

1. AB

本章总结

- 本章主要介绍了IPSec VPN的产生背景、基本概念、关键协议、应用场景及其可靠性技术等。同时对IPSec基本配置思路、问题排查思路等关键知识点做了详细的阐述。
- 通过本章课程的学习，您可以深入了解IPSec VPN的应用，能够独立完成IPSec VPN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
3DES	Triple Data Encryption Standard	三重数据加密标准
ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	报文认证头协议
CA	Certification Authority	证书颁发中心
DES	Data Encryption Standard	数据加密标准
DH	Diffie-Hellman	密钥交换算法
DPD	Dead Peer Detection	失效对等体检测
ESP	Encapsulating Security Payload	封装安全载荷协议
GCM	Galois/Counter Mode	伽罗瓦计数器模式

缩略语表 (2)

缩略语	英文全称	解释
GMAC	Galois Message Authentication Code	伽罗瓦消息验证码
GRE	Generic Routing Encapsulation	通用路由封装协议
IKE	Internet Key Exchange	因特网密钥交换协议
IPSec	Internet Protocol Security	因特网协议安全协议
ISAKMP	Internet Security Association and Key Management Protocol	Internet安全联盟和密钥管理协议
IS-IS	Intermediate System-to-Intermediate System	中间系统到中间系统协议
MD5	Message Digest 5	消息摘要算法第五版
NAPT	Network Address and Port Translation	网络地址端口转换
NAT	Network Address Translation	网络地址转换
OSPF	Open Shortest Path First	开放最短通路优先协议

缩略语表 (3)

缩略语	英文全称	解释
PKI	Public Key Infrastructure	公钥基础设施
PRF	Pseudorandom Function	伪随机函数
RSA	Rivest, Shamir, and Adleman	RSA加密算法
SA	Security Association	安全联盟
SHA1	Secure Hash Algorithm 1	安全散列算法1
SHA2	Secure Hash Algorithm 2	安全散列算法2
SHA3	Secure Hash Algorithm 3	安全散列算法3
SNAT	Source Network Address Translation	源地址转换
VPN	Virtual Private Network	虚拟专用网
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.

SSL VPN技术与应用

HUAWEI

前言

- 随着时代的发展，远程居家办公已经渐渐成为一种趋势。这种办公方式也意味着企业需要依靠ISP提供的公网线路，建立专用通信隧道，为用户提供可靠安全的数据传输。移动办公人员使用SSL VPN技术远程接入网络办公的方式逐渐成为主流方式。移动办公人员使用SSL VPN可以安全、方便地接入企业内网，访问企业内网资源，提高工作效率。
- 本章节主要介绍SSL VPN的各种应用场景及SSL VPN故障处理思路。

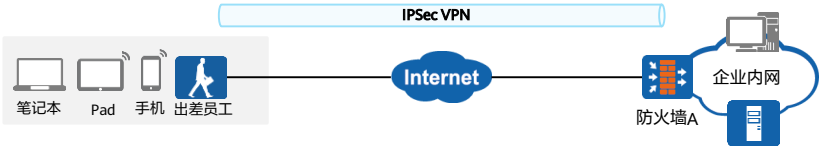
目标

- 学完本课程后，您将能够:
  - 了解SSL VPN的应用场景
  - 掌握SSL VPN的主要功能和实现原理
  - 熟悉SSL VPN的组网
  - 掌握SSL VPN的配置方法

目录

IPSec VPN的不足

- 随着时代的发展，企业的出差员工逐渐有访问公司内部网络的需求，出差场景下员工需要使用笔记本等设备安全地访问公司内部资源，IPSec VPN技术最早出现满足这一需求。

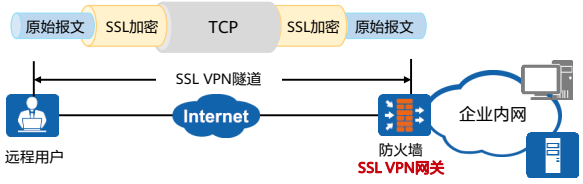


- 但是在使用过程中，逐渐发现IPSec VPN存在以下不足：

使用门槛较高	运维成本较高	访问权限管理粒度较粗	支持终端类型有限
普通用户初次使用客户端需要设置许多加密对接参数。	后续IPSec客户端软件的获取、安装、升级需要专业的技术人员负责。	基于五元组控制访问。	能够良好的支持PC，对于手机、Pad等新型设备兼容性有差异，支持不全面。

SSL VPN简介

- 对于IPSec VPN在实现远程接入方面存在的问题，SSL VPN可以很好地解决。
- SSL VPN是通过SSL/TLS协议实现远程安全接入的VPN技术，主要应用场景是保证远程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。

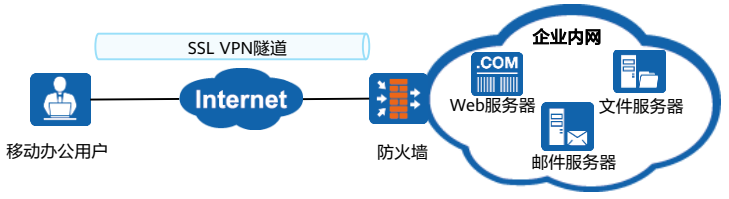


- 相较于IPSec VPN，SSL VPN存在如下特点：

使用方式简单便捷	运维简单	访问权限管理粒度精细	支持多种终端
用户仅需在浏览器打开网址并输入用户名密码即可访问内网资源或者自助下载客户端访问。	借助浏览器，用户可以自行下载和安装客户端，减轻网管维护客户端的压力。	解析应用层协议，关联用户角色，针对用户进行高细粒度地访问控制。	支持手机、PAD等多样化终端接入，适用于出差场景和远程办公场景。

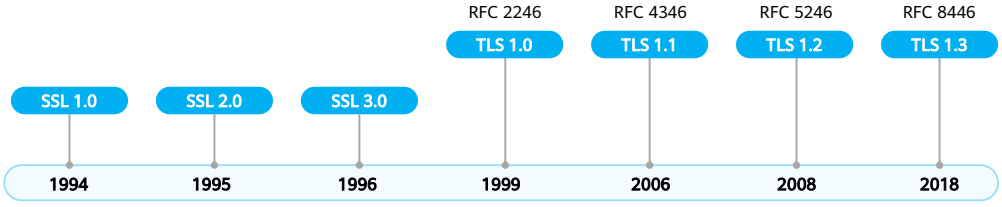
SSL VPN应用场景

- SSL VPN作为新型的轻量级远程接入方案，主要应用于企业员工出差期间需远程访问企业内部资源的场景，同时对用户可访问内网资源的权限做精细化控制。
- 防火墙作为企业出口网关连接至Internet，并向移动办公用户提供SSL VPN接入服务。移动办公用户使用终端（如便携机、智能手机等）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/TLS协议发展历史

- SSL（Secure Socket Layer，安全套接层）协议是网景公司（Netscape）在1994年首次推出的用以保护Web通信的网络安全协议，它工作在TCP协议之上，主要用来对HTTP协议进行加解密（即HTTPS）。
- 1999年，网景公司将SSL协议提交给IETF组织，IETF将SSL协议标准化后，将其称为TLS（Transport Layer Security，传输层安全）协议。TLS实现原理与SSL基本一致。
- SSL协议一共经历了三个版本，但是均存在较严重的安全漏洞，目前已经被大多数厂家所禁用、淘汰。而TLS协议逐渐成为加密HTTP流量的主流协议，已经经历多个版本的迭代。



HUAWEI

- 当前华为USG6000E系列防火墙SSL VPN功能支持TLS 1.0、TLS 1.1和TLS 1.2版本。

SSL VPN与IPSec VPN的比较

- 关于SSL VPN与IPSec VPN在各方面的对比如下表所示。

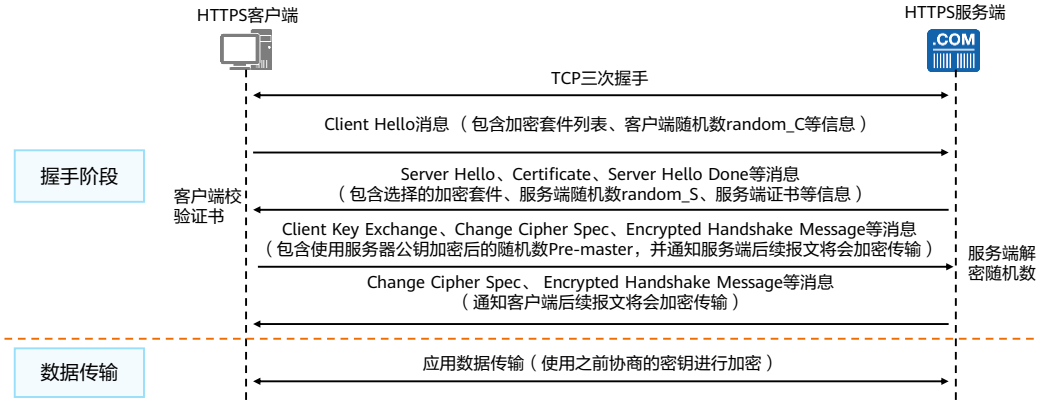
远程访问的需求		SSL VPN	IPSec VPN
安全性	传输加密	各种常见算法	各种常见算法
	身份认证	种类多，强度高	种类少，强度不高
	权限管理	粒度细	粒度粗
	防病毒入侵	可以实施	难以实施
接入	接入终端	支持的终端类型丰富	支持的终端类型少
使用	客户端安装	免安装或自动安装	预先安装
	客户端维护	自动配置运行	手工配置
身份认证集成与应用承载	身份认证集成	支持的认证种类多，与原有身份认证系统易于集成	支持的认证种类少，与原有身份认证系统较难集成
	应用承载	支持各种IP应用	不支持非IP单播应用

- 防病毒入侵：
  - SSL VPN安装ActiveX插件或客户端后可以基于用户检查终端安全，防止被病毒入侵的终端接入VPN，IPSec难以实现该功能。
- 身份认证集成：
  - IPSec VPN仅支持常规的算法认证，无法使用双因子认证或者借助AD域实现认证，假设企业内部系统原本存在AD域控，新建的IPSec VPN无法与原有的AD域控身份认证关联使用，造成资源浪费；
  - SSL VPN支持本地认证、服务器认证、证书匿名认证和证书挑战认证等，假设企业内部系统原本存在AD域控，新建的SSL VPN可以与原有的AD域控身份认证关联使用，易于集成。

目录

TLS协议加解密原理

- SSL VPN中对HTTP流量的加密是基于TLS协议实现的，TLS协议可以建立一条安全的数据传输通道，建立过程可以大致分为两个阶段：握手阶段和数据传输阶段。其工作原理如下所示：



HUAWEI

- 数据加密使用的密钥通过以下三个参数计算得出：客户端随机数random_C、服务端随机数random_S、随机数Pre-master。
- 随机数Pre-master由客户端生成，并使用服务器证书中的公钥加密后，发送至服务端，服务端使用私钥解密，得到随机数Pre-master。由于服务端的私钥是保密的，所以第三方中间人无法解密，从而保证了最终计算出的密钥是安全的。
- 应用数据的传输使用对称密钥加密算法，效率较高。

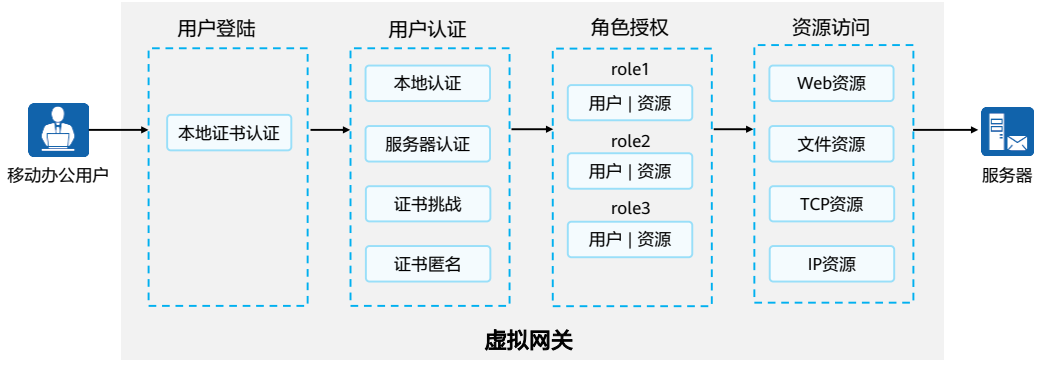
SSL VPN业务功能

- SSL VPN为了更精细化控制移动办公用户资源访问权限，将内网资源划分为Web资源、文件资源、端口资源和IP资源四种。每一类资源都有与之对应的访问方式，资源访问方式如下表所示。

SSL VPN业务	说明
Web代理	移动办公用户访问内网Web资源时使用Web代理业务。
文件共享	移动办公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。 移动办公用户直接通过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。
端口转发	移动办公用户访问内网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。
网络扩展	移动办公用户访问内网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此业务。

SSL VPN虚拟网关

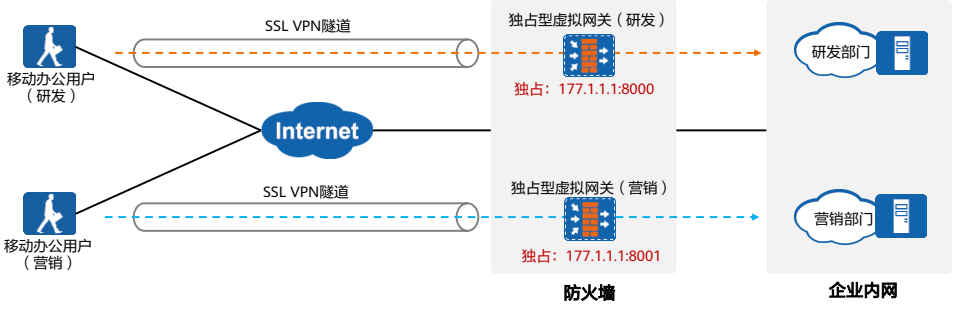
- 防火墙通过虚拟网关向移动办公用户提供SSL VPN接入服务，虚拟网关是移动办公用户访问企业内网资源的统一入口。下图是移动办公用户登录SSL VPN虚拟网关并访问企业内网资源的总体流程。



- 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。
- 一台防火墙设备可以创建多个虚拟网关，虚拟网关之间相互独立，互不影响。不同虚拟网关下可以配置各自的用户和资源，进行单独管理。虚拟网关本身无独立的管理员，所有虚拟网关的创建、配置、修改和删除等管理操作统一由防火墙的系统管理员完成。

虚拟网关类型 - 独占型

- 虚拟网关可分为独占型虚拟网关和共享型虚拟网关。
- 独占型虚拟网关指的是一个虚拟网关独自占有某个IP地址的某个端口，其他的虚拟网关无法再使用此IP的此端口（但是可以使用此IP的其他端口）。
- 根系统/虚拟系统中均可配置多个独占型虚拟网关，以隔离不同的业务需求，使用场景如下所示。

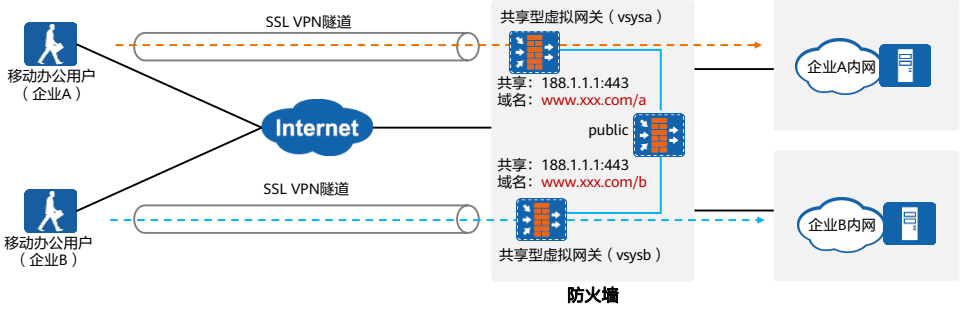


HUAWEI

- 上图以根系统的多个独占型网关为例进行说明，虚拟系统的独占型网关功能与之相似，不再赘述。

虚拟网关类型 - 共享型

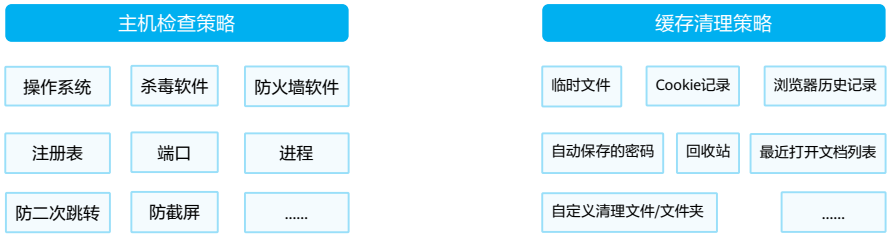
- 共享型虚拟网关常用于防火墙配置了多个虚拟系统的场景中，指的是多个虚拟系统中的虚拟网关共享防火墙的公共IP的某个端口向移动用户提供SSL VPN服务（公共IP及域名需要在防火墙根系统中提前配置）。
- 根系统的公共IP仅能配置一个，每个虚拟系统中仅能创建一个使用此公共IP的共享型虚拟网关。
- 共享型虚拟网关由于使用相同的IP和端口，所以需要使用不同的访问路径区分不同的内网资源，如下所示。



- 上图中的公共IP为188.1.1.1，对应的域名为www.xxx.com，此地址和域名需要在防火墙的根系统中提前配置。

终端安全

- 终端安全是SSL VPN中检查终端是否安全的一种手段，可以防止危险终端接入内网和预防内网资源信息被泄露等情况。终端安全包括用户接入虚拟网关时的主机检查和用户退出时的缓存清理两部分。
  - 在接入虚拟网关时，用户终端需要通过主机检查策略，用户才可以成功接入SSL VPN。
  - 用户主机在断开SSL VPN时，终端安全可以使用缓存清理策略清理用户访问内网过程中在终端留下的访问痕迹，防止内网信息泄露。

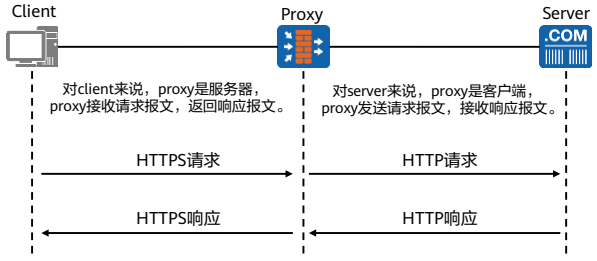


- 主机检查策略主要用于检查用户接入虚拟网关的主机是否符合安全要求，包括操作系统、端口、进程、杀毒软件、防火墙软件、注册表以及是否存在指定文件。另外还提供以下功能：
  - 防二次跳转，检查客户端是否开启远程共享程序，以防止客户端被其他PC远程控制；
  - 防截屏，检查客户端是否开启截屏程序，避免机密信息泄露。
- 缓存清理策略主要用于清理用户访问内网过程中在终端上留下的访问痕迹，包括：
  - 清除生成的临时文件、自动保存的密码、Cookie记录、浏览器历史记录、回收站以及最近打开文档列表；
  - 禁用IE浏览器的表单自动完成功能和地址栏自动完成功能；
  - 自定义清理特定的文件或文件夹等。

目录

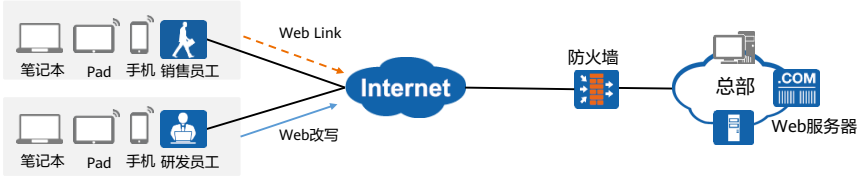
Web代理简介

- Web代理是SSL VPN的功能之一，用户可以通过防火墙做代理访问内网的Web服务器资源（即URL资源），如有需要也可以隐藏内网服务器真实的URL。
- Web代理依靠HTTP代理实现的，其核心思想是对请求做中转，如下图所示。Web代理功能按照实现方式不同分为Web改写和Web Link两种。



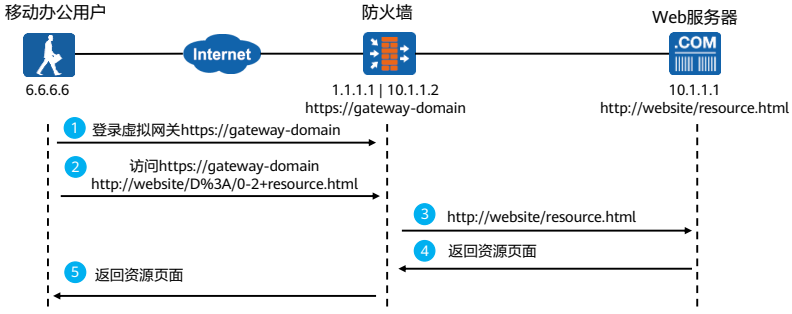
应用场景

- 通常大中型企业的网络架构复杂，需求差异化也很大，当员工在出差过程中访问企业总部的Web应用也存在不同需求。针对员工的不同需求，可以通过Web代理的两种方式实现。
- 如图所示：
  - 研发员工出差时需要使用开发的Web页面，企业出于安全考虑，需隐藏这些Web的具体路径，并且要适配员工的电脑。可以采用Web改写的方式，将访问Web页面的URL进行改写，达到加密链接和适配终端的需求；
  - 销售员工拜访客户时企业更关注销售员工打开Web链接时效率第一，不能出现图片错位、大小不一致或者不兼容等问题。可以采用Web Link的方式，直接“转发”销售员工的Web资源请求，不做任何处理，避免图片错位等问题。



Web代理业务交互流程

- Web代理功能的实现原理是将Internet用户访问Web Server的过程分成了两个阶段。
  - Internet用户与防火墙的虚拟网关之间建立HTTPS会话；
  - 防火墙的虚拟网关再与Web Server建立HTTP会话。
- 防火墙虚拟网关在Internet用户访问企业内网Web Server中起到了改写、转发Web请求的作用。

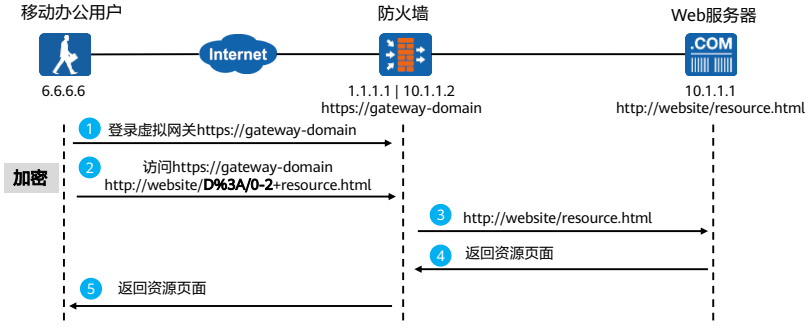


HUAWEI

- 如图所示是移动办公用户通过Web代理的方式来访问内网Web Server的一个业务交互流程，具体步骤如下：
  - 移动办公用户通过域名（https://gateway-domain）访问虚拟网关。
  - 登录虚拟网关成功后，移动办公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。防火墙再将内网资源（http://website/resource.html）呈现给移动办公用户时，会改写该资源的URL。移动办公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://gateway-domain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，经过HTTPS方式转发给移动办公用户。

Web改写

- Web改写中的“改写”包含两层含义：
  - 加密，即移动办公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；
  - 适配，不同的终端设备使用着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。虚拟网关对Web资源进行“改写”，使之能够适配这些不同的终端。

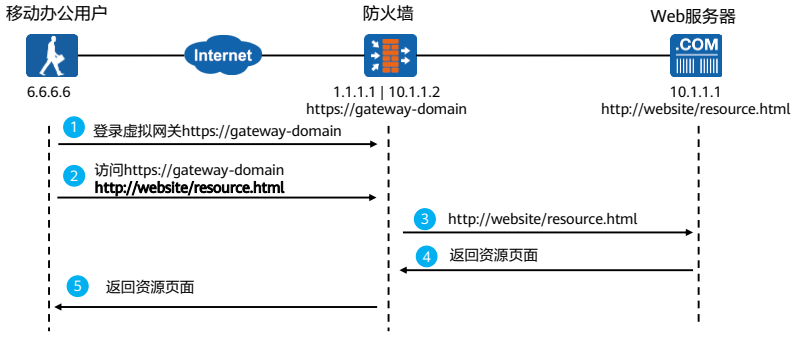


HUAWEI

- 加密：如图的第2步中，用户要访问的真实URL是http://website/resource.html，而经过Web改写以后URL可能会显示为http://website/D%3A/0-2+resource.html。通过Web改写，起到隐藏内网Web资源真实URL的目的，从而保护内网Web服务器的地址安全。在Web改写中，这种加密不仅体现于此，包括用户要访问的Web资源页面链接对象（例如Flash、PDF、Java Applet等）的URL也会被一并加密。
- 适配：启用Web代理功能以后，防火墙设备会自动对Web资源进行改写。对于个别HTML对象和ActiveX控件如果在启用Web代理以后，仍然出现显示异常的情况，则可以通过手动配置的方法进行精确改写，解决此问题。

Web Link

- Web Link不会对原始URL进行加密和适配，只会单纯“转发”移动办公用户的Web资源请求，如下图所示的第二步和第三步，用户访问的URL地址始终保持不变，所以业务处理效率较之Web改写要高。



HUAWEI

- 需要注意的是，Web Link只适合在用户使用Window操作系统 + IE浏览器的终端上使用。

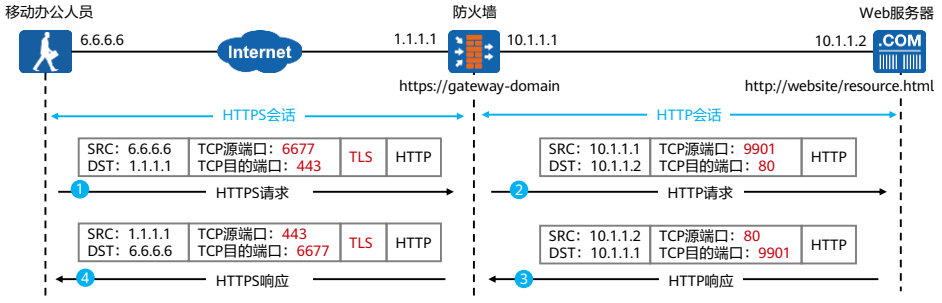
Web代理实现方式对比

- Web代理实现方式包括Web改写和Web Link，二者的差异请参见下表：

对比项	Web改写	Web Link
安全性	对真实的URL进行改写，隐藏内网服务器地址，安全性较高。	对URL不会进行改写，直接转发Web请求和响应，会暴露内网服务器的真实地址。
易用性	不依赖IE控件，在非IE环境的浏览器中可以正常使用。	依赖IE控件，在非IE环境中无法正常使用。
兼容性	由于Web技术发展非常迅速，防火墙对于各类URL资源的改写无法做到面面俱到，可能会出现图片错位，字体显示不正常等问题。	无需对资源进行改写，由防火墙直接对请求和响应进行转发，所以没有页面兼容性问题。
使用建议	优先推荐使用Web改写，因为这是最安全、最方便的一种访问方式。如果出现页面显示异常，再考虑Web Link方式。	Web Link作为Web改写的最佳替补，但由于依赖IE控件，必然在使用上存在局限性。而且没有对内网URL进行改写，存在安全风险。

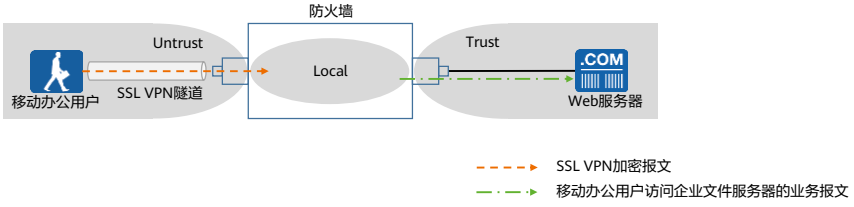
Web代理报文封装

- 如图所示是移动办公用户访问内网Web资源时的报文封装过程，从图中可以看出移动办公用户的访问过程本质上是由HTTPS和HTTP这两个会话衔接而成。
  - 移动办公用户与虚拟网关建立HTTPS会话时，使用的源端口为6677，这个源端口是一个随机端口，目的端口是443。
  - 虚拟网关与Web Server建立HTTP会话时，源端口是9901，这个源端口也是随机端口，目的端口为80。



Web代理中的关键安全策略

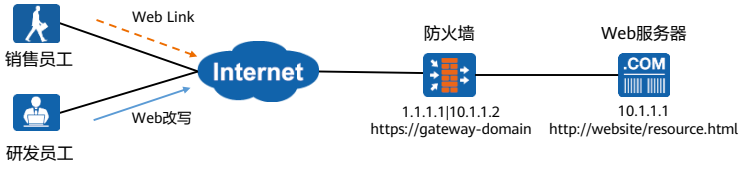
- 移动办公用户访问企业Web Server的过程中，经过防火墙的流量分为以下两类，为确保Web代理功能的正常使用，需要放行的安全策略如下：
  - 移动办公用户与防火墙间的SSL VPN加密报文。
    - SSL VPN加密报文会经过Untrust -> Local区域，放行Untrust -> Local的安全策略。
  - 移动办公用户访问企业Web Server的业务报文。
    - 解密后的业务报文经过的安全区域为Local -> Trust，放行Local -> Trust的安全策略。



- 后续文件共享和端口转发的安全策略和Web代理相同，不再介绍。
- 配置从Internet到防火墙的安全策略，允许出差员工登录SSL VPN网关。
  - 源安全区域：untrust，目的安全区域：local；
  - 源地址：any，源端口号：any；
  - 目的地址：SSL VPN网关地址，目的端口号：虚拟网关的端口号，如果改了https端口号，需要按照修改后的端口号放开；
  - 服务：https服务；
  - 动作：允许。
- 配置防火墙到内网的安全策略，允许出差员工访问总部资源。
  - 源安全区域：local，目的安全区域：trust；
  - 目的地址：内网文件服务器IP地址；
  - 动作：允许。

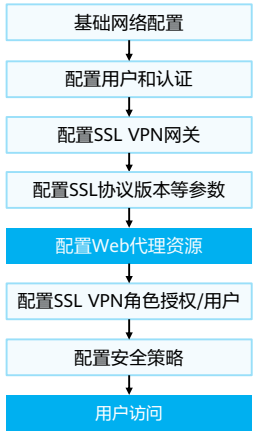
Web代理功能举例 (1)

- 如图所示，某科技公司的销售和研发员工频繁出差，都有访问企业内部Web网站的需求。现在该公司在网络边界部署了防火墙作为安全网关，管理员将使用防火墙SSL VPN的“Web代理”功能，通过Web Link和Web改写将内网的Web应用提供给出差员工使用。
- 具体需求如下：
  - 销售员工面向客户时需要展示官方网页，讲究效率第一；
  - 研发员工则需要使用开发的网站，出于安全考虑，需要隐藏这些开发Web网页的具体路径。



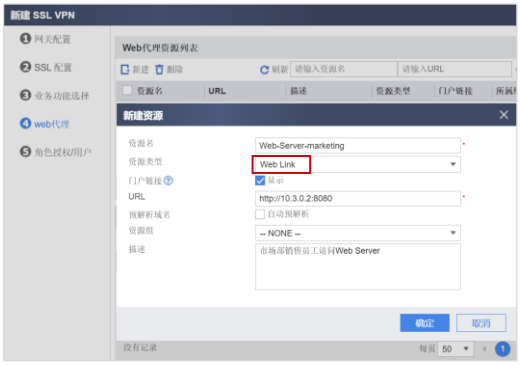
Web代理功能举例 (2)

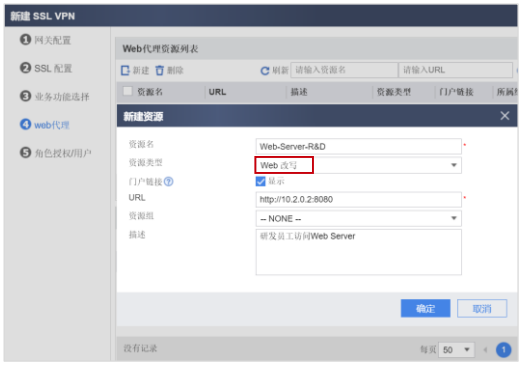
- 配置思路：
  - 完成基础网络配置，保证互联互通；
  - 配置SSL VPN接入的用户及认证方式；
  - 配置SSL VPN网关相关参数，包括类型、网关地址等；
  - 配置SSL基本参数，包括版本、算法、加密套件等；
  - 配置Web代理资源，包括资源名、资源类型和URL地址等；
  - 配置相关用户角色授权；
  - 配置安全策略，放行相关流量；
  - 实现用户访问。



配置Web代理资源

- 在“Web代理资源列表”中，单击“新建”，按如下配置新建Web代理资源。

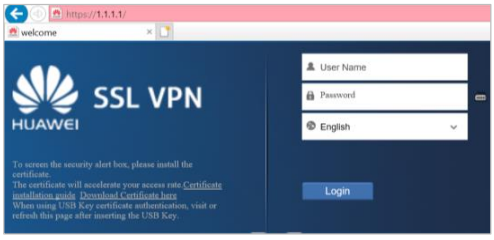




HUAWEI

用户访问验证配置结果 (1)

- 用户在PC浏览器中输入https://1.1.1.1:443，访问SSL VPN登录界面。（首次访问时，需要根据浏览器的提示信息安装控件。）



- 用户在登录界面中输入用户名/密码，单击“登录”。登录成功后，虚拟网关界面上显示Web资源链接。

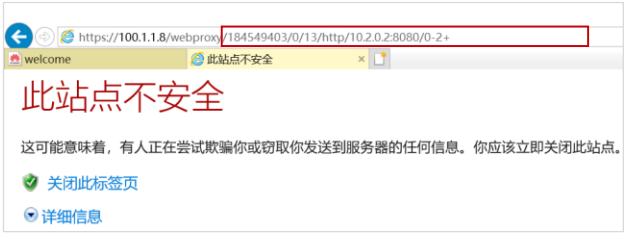
HUAWEI

- 本结果验证环节中，将Web代理中的资源链接集中展示，同一个用户可以看到市场部的资源，也可以看到研发部的资源。

用户访问验证配置结果 (2)

- 用户点击虚拟网关界面上显示Web资源链接，单击链接即可访问该资源。
  - Web-Server-marketing资源为Web-Link模式，点击发现URL如下所示。

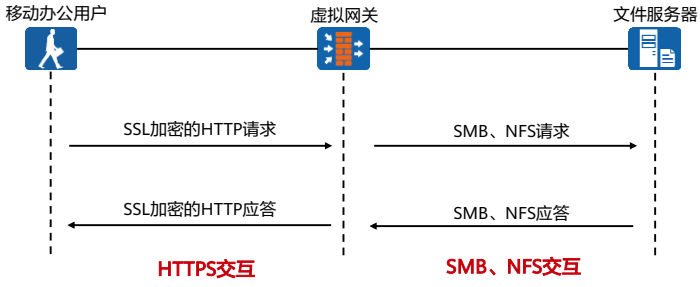
  - Web-Server-R&D资源为Web改写模式，虚拟网关会将真实的URL进行隐藏。



目录

文件共享简介

- 文件共享是SSL VPN的功能之一，通过将文件共享协议（SMB、NFS）转换成基于SSL的超文本传输协议（HTTPS），实现对内网文件服务器的Web方式访问。
- 它能够让远程接入用户直接通过浏览器安全地访问企业内部的文件服务器，而且支持新建、修改、上传、下载等常见的文件操作。

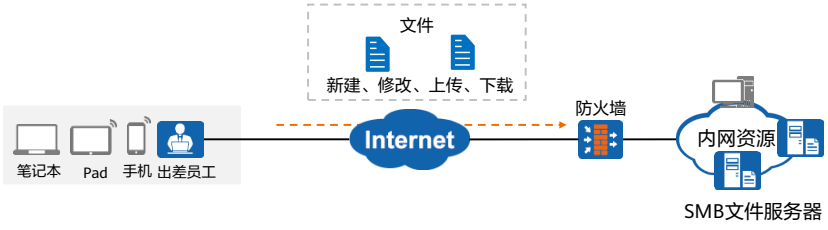


HUAWEI

- 目前，在企业中较为流行的文件共享协议包括SMB（Server Message Block）和NFS（Network File System），前者主要应用于Windows操作系统，后者主要应用在Linux操作系统。华为防火墙的SSL VPN支持这两种协议。
- 如图所示，可以将防火墙作为虚拟网关设备，与客户端之间的通信始终是通过安全HTTPS协议加密传输，当加密报文抵达防火墙后，防火墙对其解密后并进行协议转换，最终作为SMB客户端，向相应的SMB文件共享服务器发起请求，其中还包含了文件服务器认证的过程。从通信所使用协议的角度，以上过程可以概况为两个阶段：
  - 远程接入用户作为Web Client与防火墙Web Server之间的HTTPS交互；
  - 防火墙作为SMB Client与文件服务器SMB Server之间的SMB交互。

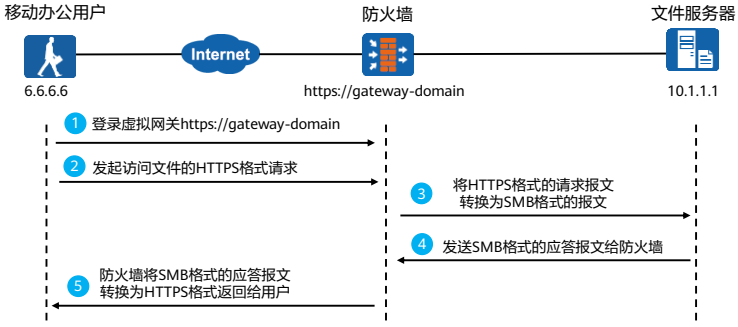
应用场景

- 在大中型企业，内部网络存在多台SMB文件服务器，每台文件服务器提供不同的文件资源。作为出差员工希望快捷地查看公司内部的文档资源，同时又能保证访问的安全性，通过文件共享功能即可实现该需求。
- 如图所示，通过使用文件共享功能，Web链接的形式将SMB Server的文件资源展现出来，实现员工访问内网文件资源的需求。出差用户访问内网文件服务器就像访问普通Web网页一样，不用安装文件共享客户端、不用记服务器的IP地址，只需要在Web网页中点击感兴趣的文件资源的链接访问即可。



文件共享业务交互流程

- 文件共享功能在移动办公用户访问内网的文件资源过程中起到了协议转换的作用，以访问内网Windows文件服务器为例，移动办公用户访问文件服务器的过程被分成了如下两个阶段：
  - HTTPS阶段：防火墙作为Web Server接收远程用户的文件访问请求，并翻译为SMB请求；
  - SMB阶段：防火墙作为SMB Client发起请求，接收应答并翻译给远程用户。

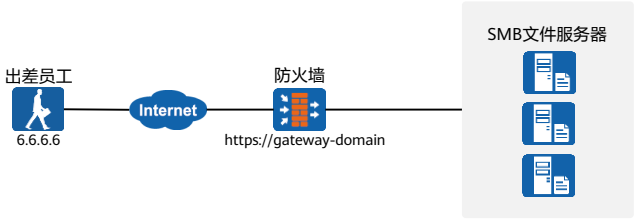


HUAWEI

- 图中所示是移动办公用户通过文件共享功能来访问内网文件服务器的一个业务交互流程，具体步骤如下：
  - 移动办公用户通过域名（ https://gateway-domain ）访问虚拟网关，进行SSL VPN登录认证；
  - 登录虚拟网关成功后，如果是用户首次访问文件共享资源，要先通过文件服务器的认证，这里所说的认证一定要和SSL VPN登录时的认证区分开，在登录阶段，接入用户首先要通过的是防火墙认证。而此时要访问文件共享资源，还要看文件服务器是否响应。在点击资源列表中的”Public_share“时会弹出认证页面。文件服务器认证成功后，移动办公用户会在虚拟网关中看到自己有权访问的文件资源列表，然后单击要访问的资源链接；
  - 防火墙收到上述HTTPS请求后，将HTTPS格式的请求报文转换为SMB格式的报文转发给文件服务器；
  - 文件服务器收到SMB格式的请求报文，会按照SMB格式回复给防火墙；
  - 防火墙收到SMB应答报文将SMB格式的应答报文转换为HTTPS格式返回给用户。

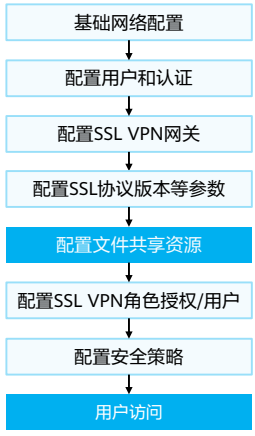
文件共享功能举例 (1)

- 某公司网络边界部署了防火墙作为安全网关，内部网络存在多台SMB文件服务器，文件服务器提供不同的文件资源。现在公司希望出差员工能够在Internet中安全、快捷地查看公司内部的文档资源。
- 具体需求如下：
  - 管理员使用SSL VPN的“文件共享”功能，满足出差员工的访问需求；
  - 隐藏内部文件的具体路径和位置。



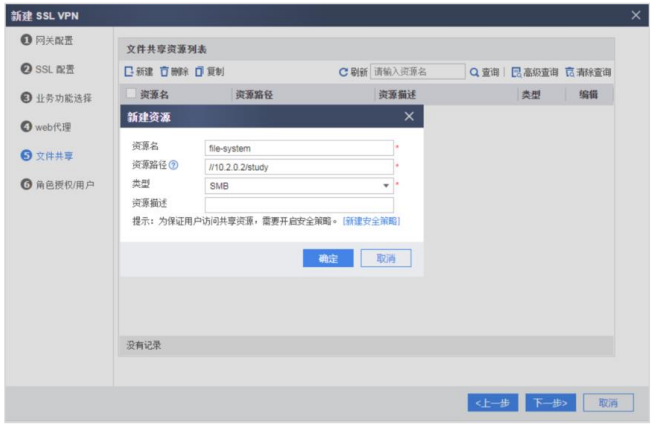
文件共享功能举例 (2)

- 配置思路：
  - 完成基础网络配置，保证互联互通；
  - 配置SSL VPN接入的用户及认证方式；
  - 配置SSL VPN网关相关参数，包括类型、网关地址等；
  - 配置SSL基本参数，包括版本、算法、加密套件等；
  - 配置文件共享资源，包括资源名、资源路径和类型等；
  - 配置相关用户角色授权；
  - 配置安全策略，放行相关流量；
  - 实现用户访问。



配置文件共享资源

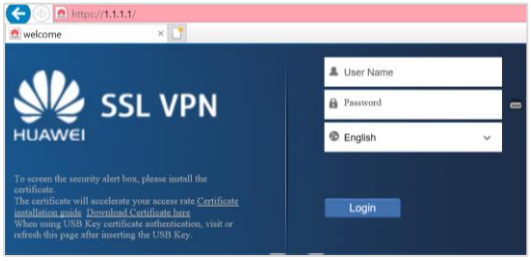
- 在“文件共享资源列表”中，单击“新建”，按如下配置新建文件资源。



HUAWEI

用户访问验证配置结果

- 用户在浏览器中输入https://1.1.1.1:443，访问SSL VPN登录界面。（首次访问时，需要根据浏览器的提示信息安装控件。）

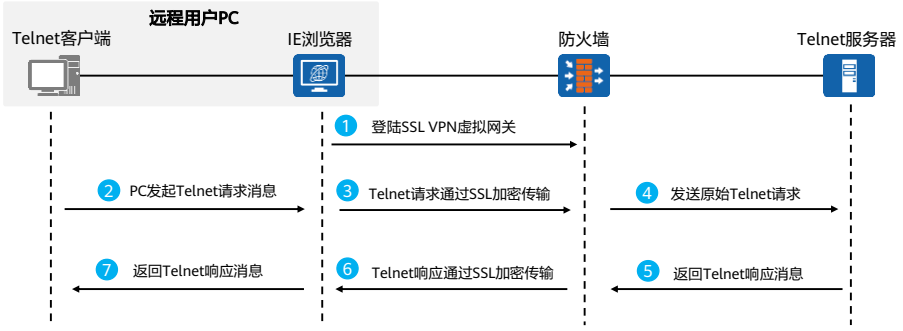


- 用户在登录界面中输入用户名/密码，单击“登录”。登录成功后，虚拟网关界面上会显示Web资源链接，单击链接即可访问该资源。

目录

端口转发简介

- 端口转发是通过在客户端上获取指定目的IP地址和端口的TCP报文，然后使用虚拟网关转发到内网，实现对内网指定TCP资源的访问。
- TCP资源是以TCP协议为基础的上层应用，例如Telnet、FTP、Email等。以Telnet方式登录服务器为例，端口转发流程如下所示。

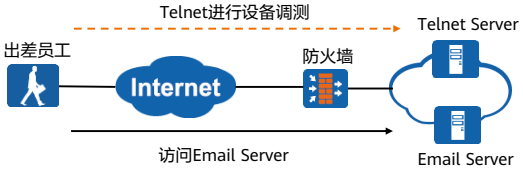


HUAWEI

- 上图中假设Telnet地址为10.1.1.1，详细过程如下：
  - 用户在客户端上Telnet 10.1.1.1发起请求；
  - IE浏览器安装的ActiveX插件识别前往10.1.1.1的数据，交由虚拟网卡转发到防火墙虚拟网关；
  - 防火墙虚拟网关收到SSL请求报文后，解密报文并将请求转发给Telnet服务器10.1.1.1，防火墙与Telnet服务器之间建立TCP连接，同时回复防火墙对应的Telnet登录信息；
  - 防火墙收到“Telnet登录信息”后，将这些信息封装在SSL报文中，转发给远程用户电脑；
  - 远程用户电脑收到防火墙虚拟网关的报文后，ActiveX控件会对收到的SSL加密报文进行解密，并返回“Telnet登录信息”给客户端。

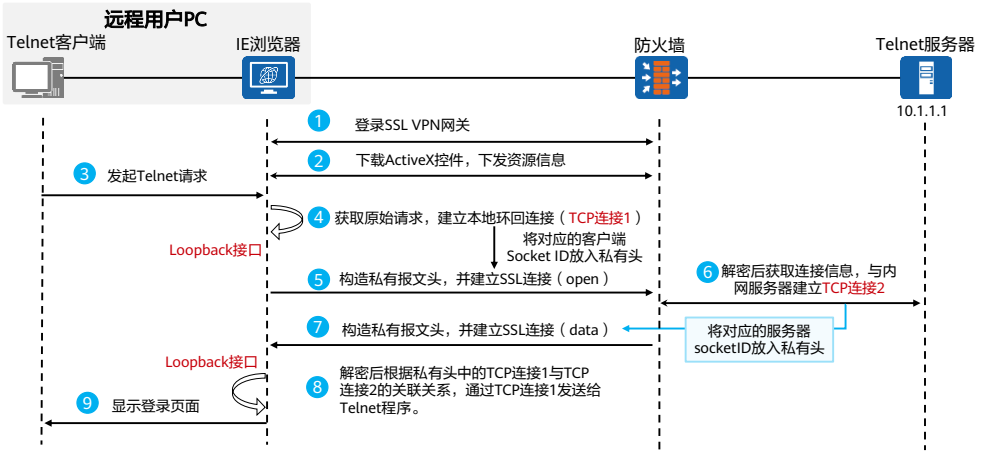
应用场景

- 在前文介绍的SSL VPN业务功能中，Web代理和文件共享都是常见的细粒度资源。但是企业中还存在基于TCP的非Web应用访问需求，此时企业可以通过SSL VPN的端口转发功能将Internet的请求转发到内网，安全有效的满足用户访问基于TCP协议的资源需求。
- 如图所示，出差员工希望远程Telnet企业内部的各种网络设备进行调测，同时也需要访问Email Sever。针对这些需求可以使用SSL VPN的端口转发功能，在满足需求的同时又能加密报文，保障报文交互的机密性。



端口转发业务交互流程

- 以移动办公用户通过Telnet客户端访问企业内网Telnet服务器为例，介绍端口转发业务的工作流程如下。

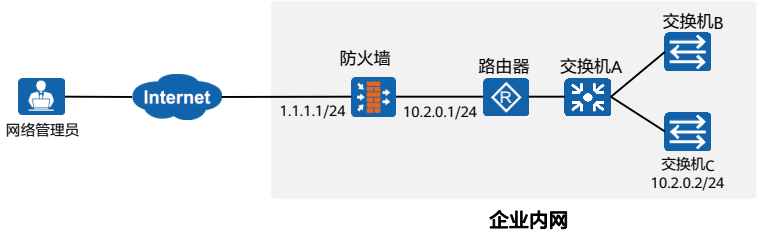


- 端口转发的关键的技术点在端口转发客户端，用户使用Windows系统的IE浏览器登录虚拟网关后，会在本地PC的IE浏览器上自动运行端口转发客户端（ActiveX控件）。这个客户端的作用是时刻监听其他程序的所有请求，并且会将远程用户发给内网服务器的请求拦截下来，然后再通过SSL连接发送给虚拟网关。对于监听到的请求，选择哪些请求进行拦截，是根据虚拟网关的配置来严格执行的。配置的端口转发资源，就是虚拟网关给端口转发客户端下发的指令：有用户要访问内网TCP资源，端口转发客户端协助用户完成访问任务。在端口转发功能中，下发的指令便是目的主机IP地址+目的端口，以上信息可以唯一确定远程用户要访问的应用信息。

- 图中所示是移动办公用户通过“端口转发”方式来访问内网Telnet Server的一个业务交互流程，具体步骤如下：
    - 打开浏览器，输入https://SSL VPN服务器的地址:端口或https://域名，发起连接；
    - 使用Windows系统的IE浏览器登录虚拟网关后，本地PC的IE浏览器上自动运行端口转发客户端（ActiveX控件），并且根据虚拟网关下发的资源信息“聆听”请求；
    - 端口转发客户端会随时“聆听”电脑的请求，当发现与虚拟网关下发的资源信息（目的IP+目的端口）匹配，会立刻将此TCP SYN报文“拦截”，使用本地Loopback口（127.0.0.1）作为接收方，模拟接收一次Telnet业务请求（TCP链接）；
    - 将TCP连接1的Socket ID放入构造的私有报文头，经过SSL加密发给虚拟网关；
    - 虚拟网关收到加密后的报文，对其进行解密，在“私有报文头”中获取到Telnet真实的目的IP地址和端口、命令字等信息，此时虚拟网关将作为Telnet客户端与内网服务器进行交互建立Telnet连接；
    - 虚拟网关收到内网服务器的响应报文（登录界面），在发给远程客户之前，虚拟网关依然会构造私有报文头，填写TCP连接2的socket ID（服务器socket ID），这样便可以与TCP连接1建立对应关系；
    - 虚拟网关把经过SSL加密后的私有报文头+数据发送给端口转发客户端；端口转发客户端根据私有头中客户端socket ID找到TCP连接1，再根据本地环回记录表找到Telnet客户端真实IP地址，最终返回真实的数据。

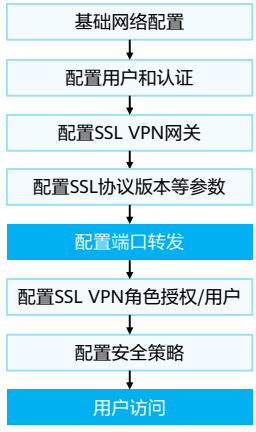
端口转发功能举例 (1)

- 某企业在网络边界部署了防火墙作为安全网关，企业内部有较多路由器、交换机和服务器等设备，现在网络管理员正在出差中，需要使用SSL VPN的端口转发功能，远程Telnet登录企业内网的网络设备（10.2.0.2/24）进行管理。



端口转发功能举例 (2)

- 配置思路：
  - 完成基础网络配置，保证互联互通；
  - 配置SSL VPN接入的用户及认证方式；
  - 配置SSL VPN网关相关参数，包括类型、网关地址等；
  - 配置SSL基本参数，包括版本、算法、加密套件等；
  - 配置端口转发功能，包括资源名、主机地址类型和端口等；
  - 配置相关用户角色授权；
  - 配置安全策略，放行相关流量；
  - 实现用户访问。



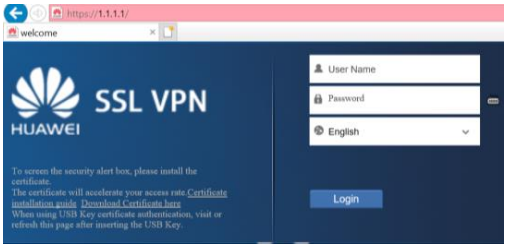
配置端口转发

- 在“端口转发”业务中，启用“客户端自动启用”，然后在“端口转发资源列表”中， 单击“新建”，按如下配置新建端口转发资源。

HUAWEI

用户访问验证配置结果

- 用户在PC浏览器中输入https://1.1.1.1:443，访问SSL VPN登录界面。（首次访问时，需要根据浏览器的提示信息安装控件。）

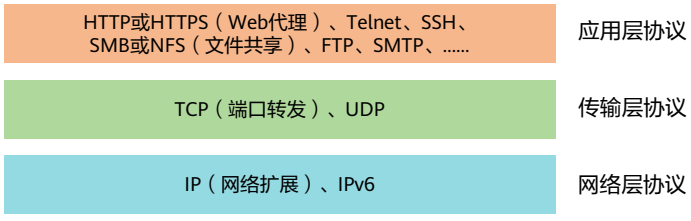


- 用户在登录界面中输入用户名/密码，单击“登录”。登录成功后，虚拟网关界面上会显示端口转发资源，单击链接即可访问该资源。

目录

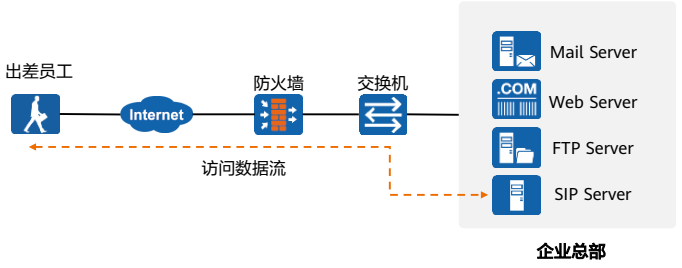
网络扩展简介

- 前文介绍的Web代理、文件共享和端口转发功能虽然解决了移动办公用户访问内部资源的问题，但是这些功能所支持的资源都存在一定的局限性，只支持特定的协议。如果用户需要访问内部语音服务器进行电话会议，由于电话语音业务一般是基于UDP，上述的功能均无法满足该需求。
- SSL VPN网络扩展功能支持建立网络层VPN隧道，帮助用户能够访问更加丰富的资源，实现移动办公用户对企业IP业务的全面访问。



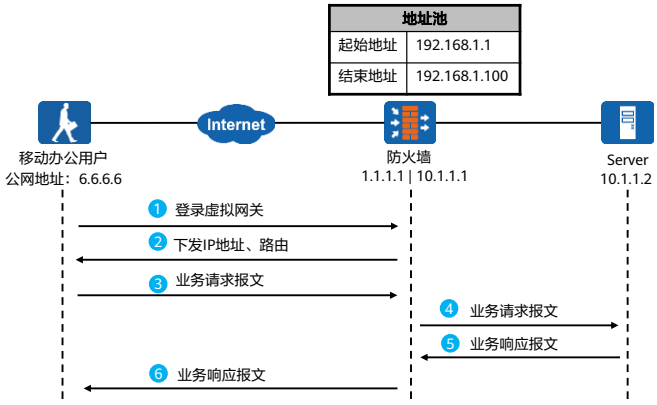
应用场景

- 大中型复杂的企业架构中，存在多种复杂的功能，比如常见的视频会议、财务系统等。面对此类需求，通过SSL VPN网络扩展功能实现远程用户访问。
- 如图所示，总部提供SIP语音服务，现需要使用某种技术保护出差员工与内网SIP Server之间的通信，同时也需要出差员工可以像在局域网内一样，访问企业内部的各种资源。此时，可以通过SSL VPN的网络扩展功能，满足该企业出差员工无差别访问企业总部资源的各种需求。



业务交互流程

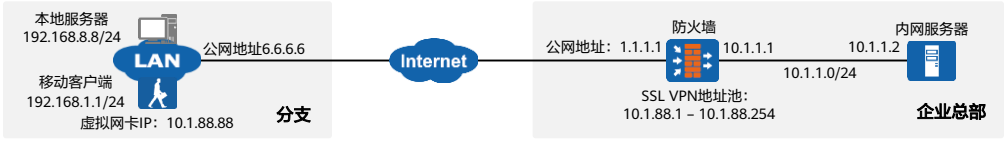
- 出差用户与虚拟网关建立SSL VPN，使用网络扩展功能访问内网资源，其内部交互流程如下。



HUAWEI

- 图中所示是移动办公用户通过网络扩展功能来访问服务器资源的一个业务交互流程，具体步骤如下：
  - 移动办公用户通过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，会触发以下动作：
    - 移动办公用户与虚拟网关之间会建立一条SSL VPN隧道；
    - 移动办公用户本地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，分配给移动办公用户的虚拟网卡，该地址作为移动办公用户与企业内网Server之间通信的地址。有了该私网IP地址，移动办公用户就如同企业内网用户一样可以方便访问内网IP资源；
    - 虚拟网关向移动办公用户下发到达企业内网Server的路由信息。虚拟网关会根据网络扩展业务中的配置，向移动办公用户下发不同的路由信息；
  - 移动办公用户向企业内网的Server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Server。
  - 内网Server响应移动办公用户的业务请求。
  - 响应报文到达虚拟网关后进入SSL VPN隧道。移动办公用户收到业务响应报文后进行解封装，取出其中的业务响应报文。

路由模式



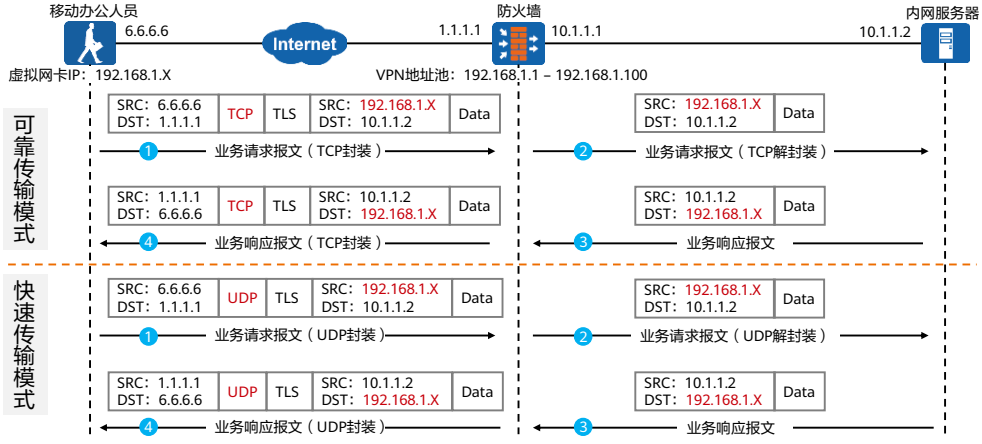
路由模式	目标网络	下一跳地址	Metric	说明
客户端原始路由（未使用SSL VPN）	0.0.0.0/0	192.168.1.254	10	移动客户端地址：192.168.1.1/24 移动客户端网关：192.168.1.254
	192.168.8.0/24	192.168.1.254	11	
手动路由模式	0.0.0.0/0	192.168.1.254	10	虚拟网关下发远端内网资源对应的路由10.1.1.0/24，引流至虚拟网卡；访问Internet和本地LAN的路由保持不变。
	192.168.8.0/24	192.168.1.254	11	
	10.1.1.0/24	**10.1.88.88（虚拟网卡）**	**1**	
分离路由模式	**0.0.0.0/0**	**10.1.88.88（虚拟网卡）**	**1**	虚拟网关下发默认路由，Metric为1，用户只能访问远端内网资源和本地LAN，不能访问Internet。
	192.168.8.0/24	192.168.1.254	11	
全路由模式	**0.0.0.0/0**	**10.1.88.88（虚拟网卡）**	**1**	虚拟网关下发默认路由和本地LAN路由，Metric为1，用户只能访问远端内网资源，无法访问Internet和本地LAN。
	192.168.8.0/24	192.168.1.254	11	
	192.168.8.0/24	**10.1.88.88（虚拟网卡）**	**1**	

HUAWEI

- 以上拓扑图说明如下：
  - 移动客户端位于分支机构，获取分支机构内网地址192.168.1.1/24，网关是192.168.1.254。
  - 分支机构的本地服务器地址为192.168.8.8/24，移动客户端存在一条路由192.168.8.0/24，下一跳指向网关地址192.168.1.254。
  - 移动客户端通过SSL VPN连接企业总部，成功后，虚拟网卡获取的地址为10.1.88.88。防火墙的SSL VPN虚拟网关的地址池取值范围是10.1.88.1-10.1.88.254。
  - 企业总部提供的内网资源地址段为10.1.1.0/24。

报文封装

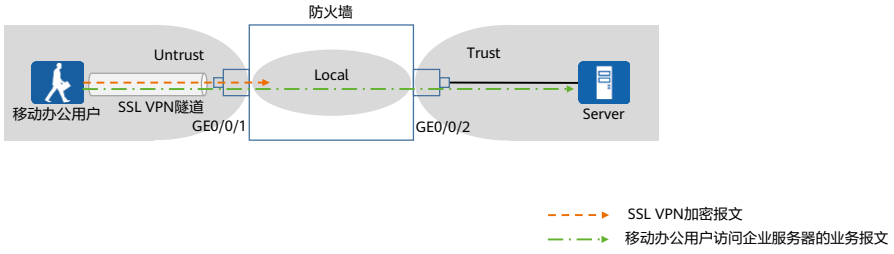
- 网络扩展功能的报文封装有两种方式：可靠传输模式（TCP封装）和快速传输模式（UDP封装），如下：



- 在网络环境不稳定的情况下推荐使用可靠性传输模式。网络环境比较稳定的情况下，推荐使用快速传输模式，这样数据传输的效率更高。

网络扩展中的关键安全策略

- 移动办公用户访问企业服务器过程中，经过防火墙的流量分为以下两类，对应流量的安全策略处理原则如下：
  - 移动办公用户与防火墙间的SSL VPN加密报文。
    - 加密报文会经过Untrust -> Local区域，放行Untrust -> Local的安全策略。
  - 移动办公用户访问企业Server的业务报文。
    - 解密后的业务报文经过的安全区域为Untrust -> Trust，放行Untrust -> Trust的安全策略。

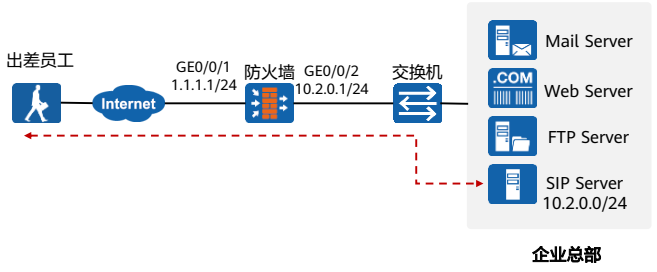


HUAWEI

- 对于移动办公用户访问企业Server的业务报文，解密以后的业务报文经过的目的安全区域为Trust，源安全区域是业务报文入接口所在安全区域。此处的业务报文入接口是GE0/0/1，安全区域为Untrust，则解密后的报文源安全区域就是Untrust。
- 配置从Internet到防火墙的安全策略，允许出差员工登录SSL VPN网关。
  - 源安全区域：untrust，目的安全区域：local；
  - 源地址：any，源端口号：any；
  - 目的地址：SSL VPN网关地址，目的端口号：虚拟网关的端口号，如果改了https端口号，需要按照修改后的端口号放开；
  - 服务：https服务；
  - 动作：允许。
- 配置移动办公用户到内网的安全策略，允许出差员工访问总部资源。
  - 源安全区域：untrust，目的安全区域：trust；
  - 源地址：移动办公用户获取到的IP地址网段，源端口号：any；
  - 目的地址：内网文件服务器IP地址；目的端口号：内网Web Server服务器的端口号；
  - 动作：允许。

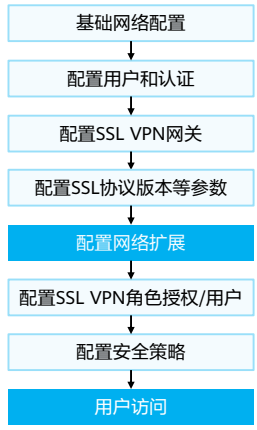
网络扩展功能举例 (1)

- 某企业在网络边界部署了防火墙作为安全网关，出差员工需要访问公司内网的各种服务器资源，同时出差员工和总部进行语音电话会议时，需要连接总部的SIP服务器，企业总部SIP服务器的地址在10.2.0.0/24网段，网络管理员使用SSL VPN的网络扩展功能实现该需求。



网络扩展功能举例 (2)

- 配置思路：
  - 完成基础网络配置，保证互联互通；
  - 配置SSL VPN接入的用户及认证方式；
  - 配置SSL VPN网关相关参数，包括类型、网关地址等；
  - 配置SSL基本参数，包括版本、算法、加密套件等；
  - 配置网络扩展功能，包括保持连接、可分配IP地址范围和路由模式等；
  - 配置相关用户角色授权；
  - 配置安全策略，放行相关流量；
  - 实现用户访问。



配置网络扩展

- 选择“网络 > SSL VPN > SSL VPN”，单击“新建”，按如下配置网络扩展资源。

HUAWEI

用户访问验证配置结果 (1)

- 用户在PC浏览器中输入https://1.1.1.1:443，访问SSL VPN登录界面。（首次访问时，需要根据浏览器的提示信息安装控件。）

- 用户在登录界面中输入用户名/密码，单击“登录”。登录成功后，点击“用户选项”下载并安装网络扩展客户端。

用户访问验证配置结果 (2)

- 使用安装好的客户端软件登录SSL VPN。

HUAWEI

用户访问验证配置结果 (3)

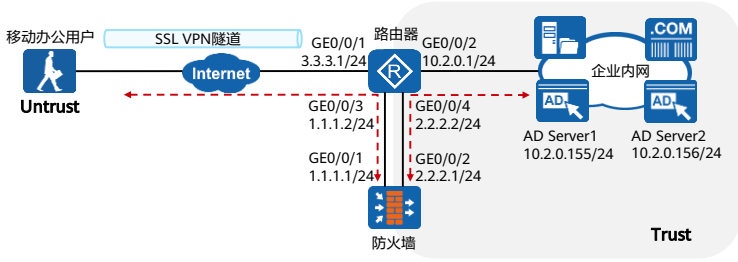
- 登录成功后可以访问内网资源。

HUAWEI

目录

SSL VPN配置举例 (1)

- 如图所示为某企业部分组网图，具体描述如下：
  - 路由器：作为企业内网服务器的网关和出口设备，GE0/0/1连接互联网；通过NAT Server转发移动办公用户与防火墙建立SSL VPN的请求、转发移动办公用户访问内网业务的数据；
  - 防火墙：旁路部署在路由器侧作为SSL VPN虚拟网关，负责将移动办公用户的访问转发到企业内网；
  - 服务器：AD服务器负责认证移动办公用户身份、授权移动办公用户访问资源，其他服务器负责提供业务应用。



SSL VPN配置举例 (2)

- 企业希望出差在外的移动办公用户能够通过SSL VPN访问公司总部的资源，并要求对接入用户进行身份认证。需求如下：
  - 普通员工出差或家庭办公时能够通过Web界面访问企业Web Mail和ERP系统；
  - 高级管理者出差或家庭办公时能够使用客户端拨入SSL VPN并获取到私网IP地址，就像在企业内部办公一样使用各种内网资源。还能够通过Web界面访问企业Web Mail和ERP系统；
  - 现网已经部署AD服务器，要求接入用户在身份认证后再访问内网资源；
  - 对接入企业内网的终端进行安全检查，如果未安装杀毒软件则禁止接入。
- 通过SSL VPN技术中的网络扩展和Web代理技术来满足以上需求：
  - 网络扩展：支持高级管理者在出差和居家办公场景下，无差别访问公司的内网资源；
  - Web代理：支持高级管理者和普通员工通过Web界面访问企业Web Mail和ERP系统。

SSL VPN配置举例 (3)

- 该网络中设备的接口IP地址以及SSL VPN涉及的参数如下表所示。

项目	数据
路由器接口	接口号：GigabitEthernet 0/0/1 IP地址：3.3.3.1/24
	接口号：GigabitEthernet 0/0/2 IP地址：10.2.0.1/24
	接口号：GigabitEthernet 0/0/3 IP地址：1.1.1.2/24
	接口号：GigabitEthernet 0/0/4 IP地址：2.2.2.2/24
防火墙接口	接口号：GigabitEthernet 0/0/1 IP地址：1.1.1.1/16 安全区域：untrust
	接口号：GigabitEthernet 0/0/2 IP地址：2.2.2.1/16 安全区域：trust
AD Server1地址	IP地址：10.2.0.155/24 网关：10.2.0.1/24
AD Server2地址	IP地址：10.2.0.156/24 网关：10.2.0.1/24

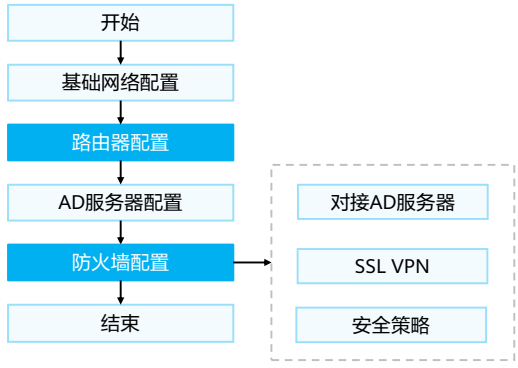
表1 IP地址规划

项目	数据
远程办公用户账号	**高级管理者** 用户名：user_0001 所属用户组：/cce.com/director
	普通员工 用户名：user_0002 所属用户组：/cce.com/employee
防火墙虚拟网关	名称：example 接口：GigabitEthernet 1/0/1 域名：example.huawei.com 最大用户数：150 最大在线用户数：100
AD服务器	主服务器：10.2.0.155 从服务器：10.2.0.156
Web代理资源	名称：Webmail，链接：http://10.2.0.10 名称：ERP，链接：http://10.2.0.11
网络扩展	网络扩展地址池：172.16.1.1-172.16.1.100 路由模式：手动 网络扩展用户可访问的内网网段：10.2.0.0/16

表2 SSL VPN参数规划

SSL VPN配置举例 (4)

- 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；
  - 配置路由器：包括NAT Server、策略路由以及缺省路由；
  - 完成AD服务器基本配置；
  - 配置防火墙：包括配置AD服务器对接参数、SSL VPN相关配置及必要的安全策略。



HUAWEI

- 各设备接口IP基础配置请按照上页规划配置，此处不做详细介绍。
- 第三步AD服务器配置，本章节不做详细介绍。

配置路由器

- 路由器配置
  - 配置NAT Server将移动办公用户建立SSL VPN的请求和访问企业内网的数据转发给防火墙。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat server protocol tcp global 3.3.3.1 443 inside 1.1.1.1 443
```

  - 配置策略路由，将服务器给移动办公用户回复的数据转发到防火墙处理。

```
[Router] acl number 3000
[Router-acl-adv-3000] rule permit ip source 10.2.0.0 0.0.0.255

[Router] traffic classifier internal
[Router-classifier-internal] if-match acl 3000
[Router] traffic behavior internal
[Router-behavior-internal] redirect ip-nexthop 2.2.2.1
[Router] traffic policy internal
[Router-trafficpolicy-internal] classifier internal behavior internal

[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-policy internal inbound
```

  - 配置去往Internet的缺省路由，转发经过防火墙加密的回复数据给移动办公用户。

```
[Router] ip route-static 0.0.0.0 0 3.3.3.2
```

配置防火墙 - 安全区域

- 防火墙的配置，主要涉及路由互通、SSL VPN的“Web代理”和“网络扩展”相关配置、安全策略配置等。
  - 选择“网络 > 接口”，编辑GE0/0/1接口，将GE0/0/1接口加入Untrust区域。同理将GE0/0/2接口加入Trust区域。

配置防火墙 - 缺省路由

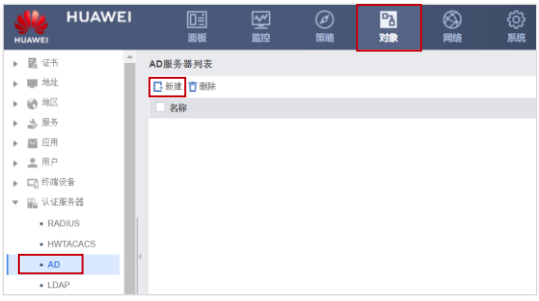
- 选择“网络 > 路由 > 静态路由”，新建防火墙到内网的路由。

- 选择“网络 > 路由 > 静态路由”，新建防火墙到外网的路由。

HUAWEI

配置防火墙 - AD对接参数

- 选择“对象 > 认证服务器 > AD”，配置防火墙和AD服务器的对接参数。



配置认证域

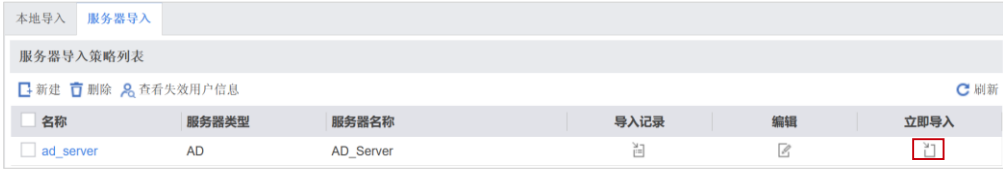
- 新建认证域，配置的认证域名称要和认证服务器上的域名保持一致。
  - 选择“对象 > 用户 > 认证域”，单击“新建”，创建认证域。

导入策略 (1)

- 在防火墙上配置服务器导入策略，为后续导入服务器上的用户和组织结构做准备。
  - 选择“对象 > 用户 > 用户导入 > 服务器导入”，单击“新建”，创建服务器导入策略。

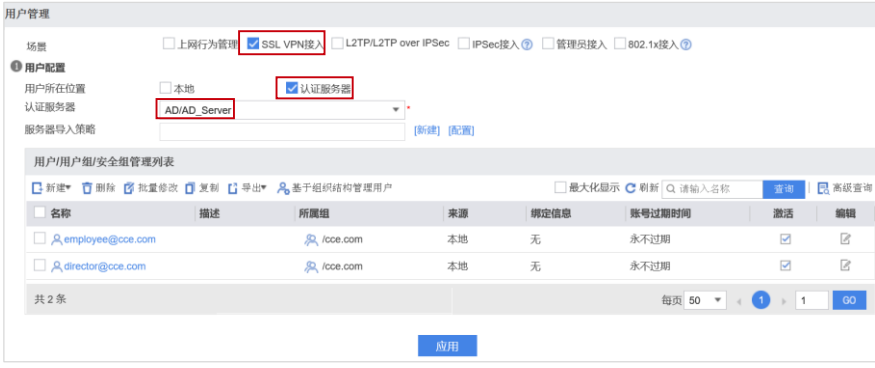
导入策略 (2)

- 导入AD认证服务器上的用户和组织结构，便于后续分组应用。
  - 服务器导入策略创建成功后，单击 ，导入认证服务器上的组织结构到防火墙上。导入成功后，在“对象 > 用户 > 用户/组”下可以看到导入的用户和组织结构信息。



配置SSL VPN接入方式

- 配置SSL VPN接入用户管理，指定用户认证服务器。
  - 选择“对象 > 用户”下的“cce.com”。
    - 选择“SSL VPN接入”场景并指定使用的AD服务器。



配置授权模式

- 配置授权模式为AD服务器授权。
  - 配置授权模式为AD服务器授权。由于Web界面无法配置授权模式，需要登录到CLI控制台配置授权模式，单击界面右下方的“CLI控制台”对话框中单击鼠标左键，连接设备CLI控制台，连接成功后，配置如下命令。

```
<FW> system-view
[FW] aaa
```

  - 创建授权方案ad，指定授权模式为AD授权。

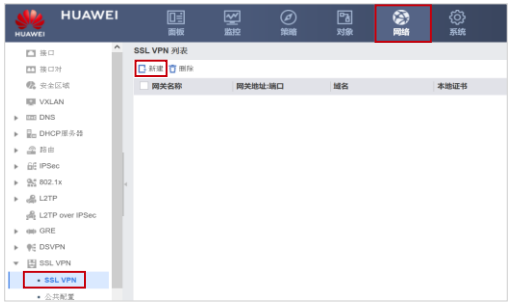
```
[FW-aaa] authorization-scheme ad
[FW-aaa-author-ad] authorization-mode ad
[FW-aaa-author-ad] quit
```

  - 在认证域中引用授权方案。

```
[FW-aaa] domain cce.com
[FW-aaa-domain-cce.com] authorization-scheme ad
```

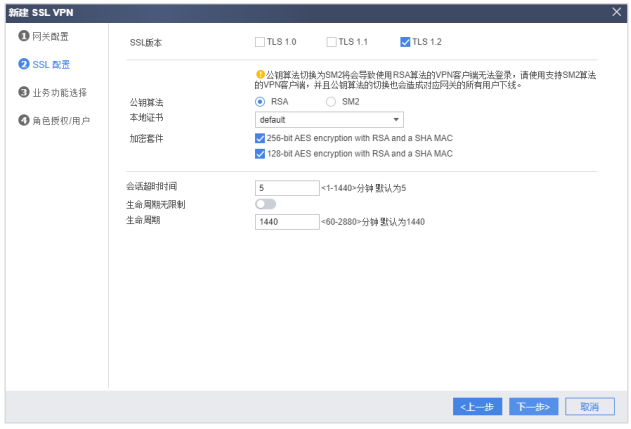
配置SSL VPN (1)

- 配置SSL VPN网关，包括：网关地址、用户认证、最大并发用户数。
  - 选择“网络 > SSL VPN > SSL VPN”，单击“新建”，按如下参数配置。



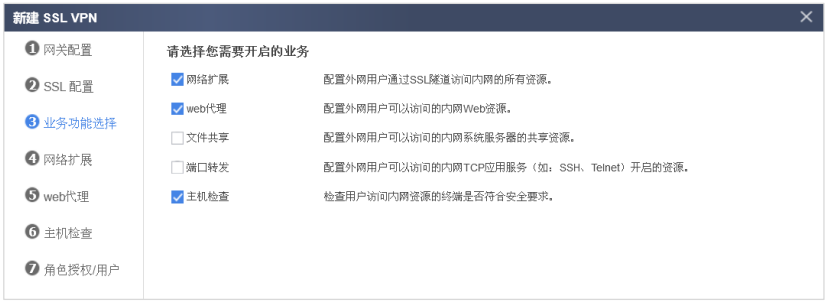
配置SSL VPN (2)

- 配置SSL参数，保持默认即可，单击下一步。



配置SSL VPN (3)

- 配置SSL业务功能参数。
  - 选择需要开启的业务“ Web代理”、“网络扩展”、“主机检查”。



配置SSL VPN (4)

- 配置网络扩展，按如下参数配置可分配IP地址池范围和可访问内网网段。

- 配置Web代理，添加资源Web mail和ERP，在“Web代理资源列表”中，单击“新建”。

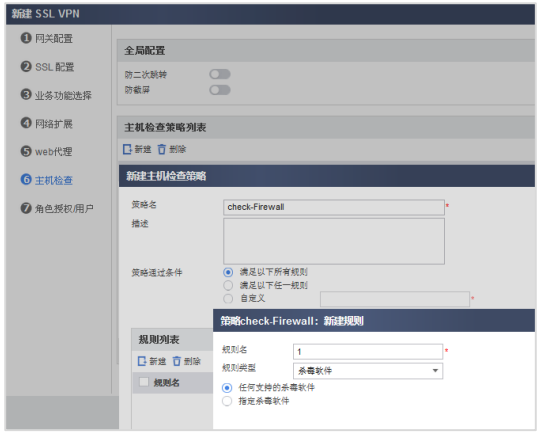
HUAWEI

配置SSL VPN (5)

- 配置Web代理，按如下参数添加Web代理资源Web mail和ERP。

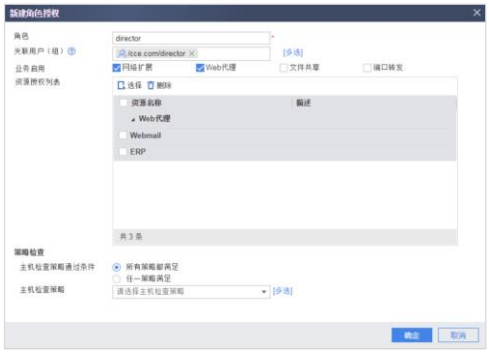
配置SSL VPN (6)

- 配置主机检查，按如下参数添加主机检查规则，主机安装任何支持的杀毒软件即可。



配置SSL VPN (7)

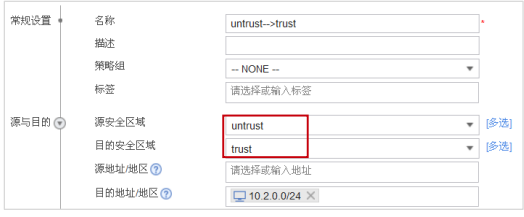
- 配置SSL VPN的角色授权/用户：将director组加入角色并关联相应权限。



- 配置SSL VPN的角色授权/用户：将employee组加入角色并关联相应权限。

配置安全策略 (1)

- 配置安全策略，允许移动办公用户登录虚拟网关，允许“网络扩展”模式中的移动办公用户访问内网资源。具体配置安全策略如下：
  - 放行Untrust -> Local区域，允许移动办公用户登录虚拟网关；
  - 放行Untrust -> Trust区域，允许移动办公用户访问企业内网。



HUAWEI

配置安全策略 (2)

- 配置安全策略，允许“Web代理”模式中的移动办公用户访问内网资源。具体安全策略如下：
  - 放行Local -> Trust区域，允许通过Web代理方式访问企业内网。

用户访问验证配置结果 (1)

- 用户在PC浏览器中输入https://3.3.3.1:443，访问SSL VPN登录界面。（首次访问时，需要根据浏览器的提示信息安装控件。）

- 高级管理者user_0001登录SSL VPN后，可以使用Web代理业务。单击“Webmail”和“ERP”可使用相应的业务。

用户访问验证配置结果 (2)

- 高级管理者在Web页面的“用户选项”中下载客户端软件并安装，设置SSL VPN的参数后可使用SSL VPN的“网络扩展”功能。自动安装虚拟网卡获取到虚拟IP地址，就像在局域网内一样能够使用各种业务。

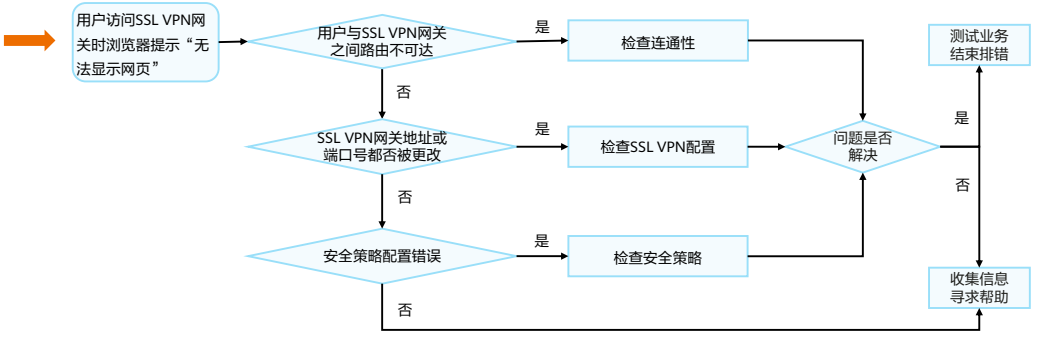
HUAWEI

用户访问验证配置结果 (3)

- 普通员工user_0002登录SSL VPN后，只能使用Web代理业务，单击“Webmail”和“ERP”使用相应的业务。

目录

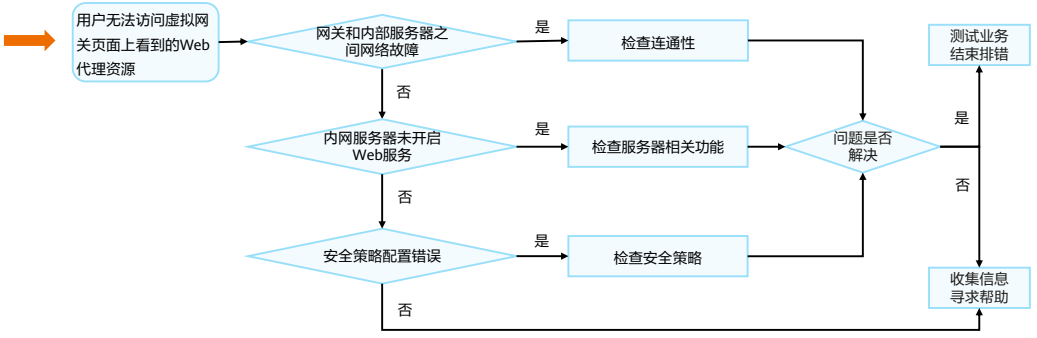
用户访问SSL VPN网关时浏览器提示“无法显示网页”



处理步骤

- 根据上述流程执行相关操作进行诊断：
  - 用户PC与SSL VPN网关路由不可达：
    - 在PC上使用Ping命令测试到达虚拟网关IP地址的连通性。如不能Ping通，表示路由不可达，请检查网络状况，并确保路由配置正确。
  - SSL VPN网关的地址或端口号已经被更改：
    - 请联系管理员获取正确的SSL VPN网关地址和端口号。
  - 安全策略配置错误：
    - 管理员登录防火墙的Web界面，在导航树上选择“策略 > 安全策略 > 安全策略”；
    - 检查安全策略的配置，看是否有哪条安全策略限制了该用户登录SSL VPN网关。如果有，则修改此策略的配置。

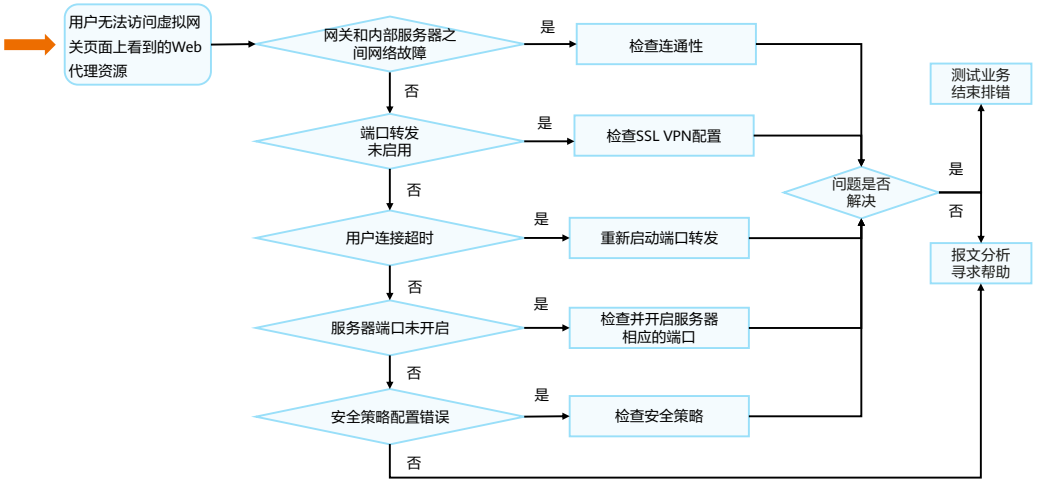
用户无法访问虚拟网关页面上看到的Web代理资源



处理步骤

- 根据上述流程执行相关操作进行诊断：
  - 网关和内网服务器之间的网络故障：
    - 管理员登录防火墙的Web界面，在导航树上选择“监控 > 诊断中心”。选择“Ping诊断”，在“目的主机的域名或IP地址”中输入内网服务器的IP地址。单击“Ping”，检查网络连接。
    - 如果不可以Ping通，则说明SSL VPN网关和内网服务器之间的网络存在问题，请检查网关和内网服务器之间的连线，若线路正常，请检查路由配置。
  - 内网服务器没有开启Web服务：
    - 在路由可达的情况下，在内网服务器的操作系统上选择“开始 > 运行”。在对话框中输入**cmd**，单击“确定”。
    - 在命令行窗口中执行**netstat -anp tcp**命令，查看Web服务的端口是否正在侦听（LISTENING）。如果正在侦听，表明Web服务端口开启。如果没有开启，请开启Web服务。
  - 安全策略配置错误：
    - 管理员登录防火墙的Web界面，在导航树上选择“策略 > 安全策略 > 安全策略”；
    - 检查安全策略的配置，看是否有哪条安全策略限制了该用户登录SSL VPN网关。如果有，则修改此策略的配置。

用户无法通过端口转发访问内网资源



处理步骤 (1)

- 根据上述流程执行相关操作进行诊断：
  - 网关和内网服务器之间的网络故障：
    - 管理员登录防火墙的Web界面，在导航树上选择“监控 > 诊断中心”。选择“Ping诊断”，在“目的主机的域名或IP地址”中输入内网服务器的IP地址。
    - 单击“Ping”，检查网络连接。如果不可以Ping通，则说明SSL VPN网关和内网服务器之间的网络存在问题，请检查网关和内网服务器之间的连线，若线路正常，请检查路由配置。
  - 端口转发未启用：
    - 用户登录SSL VPN网关界面后，如果“端口转发”栏下的按钮文字为“启动”，则表示未启动端口转发，请单击“启动”，启动端口转发。
  - 用户连接超时：
    - 用户连接超时后，“端口转发”栏下的按钮文字变为“启动”，请单击“启动”，重新启动端口转发。如果单击“启动”，界面跳回登录界面，请重新登录并启动端口转发。

处理步骤 (2)

- 内网服务器没有开启相应的端口：
  - 在路由可达的情况下，在内网服务器的操作系统上选择“开始 > 运行”。在对话框中输入**cmd**，单击“确定”。
  - 在命令行窗口中执行**netstat -anp tcp**命令，查看该服务的端口是否正在侦听（LISTENING）。如果正在侦听，表明服务端口开启。如果没有开启，请开启端口。
- 安全策略配置错误：
  - 管理员登录案例的Web界面，在导航树上选择“策略 > 安全策略 > 安全策略”。
  - 检查安全策略的配置，看是否有哪条安全策略限制了该用户对这条资源的访问。如果有，则修改此策略的配置。

思考题

1. （单选题）某企业出差用户希望访问企业内部文件服务器，且用户权限需要被精细化地控制，如普通员工仅可以访问一般性文件，以下哪一项SSL VPN功能可以满足以上需求？（　　）

   A. Web代理

   B. 文件共享

   C. 端口转发

   D. 网络扩展

1. B

本章总结

- 本课程介绍了SSL VPN的产生背景，系统介绍了SSL VPN的“Web代理”、“文件共享”、“端口转发”和“网络扩展”四大功能的原理及使用场景。列举了网络管理员在运维SSL VPN过程中可能遇到的一些问题及对应的排查思路。
- 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SSL VPN的配置方法，并掌握SSL VPN在网络安全方案中的部署方法。

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 (1)

缩略语	英文全称	解释
AD	Active Directory	活动目录
ERP	Enterprise Resource Planning system	企业资源规划系统
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure	加密的超文本传输协议
IPSec	Internet Protocol Security	互联网协议安全协议
ISP	Internet Service Provider	互联网服务提供商
NAT	Network Address Translation	网络地址转换
NFS	Network File System	网络文件系统
SIP	Session Initiation Protocol	会话发起协议

缩略语表 (2)

缩略语	英文全称	解释
SMB	Server Message Block	服务器消息块
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SSH	Secure Shell Protocol	安全外壳协议
SSL	Secure Sockets Layer	安全套接字层
TCP	Transmission Control Protocol	传输控制协议
telnet	Telecommunication Network Protocol	电信网络协议
TLS	Transport Layer Security	传输层安全性协议
UDP	User Datagram Protocol	用户数据报协议
URL	Uniform Resource Locator	统一资源定位符
VPN	Virtual Private Network	虚拟专用网

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.

网络攻击与防范

HUAWEI

前言

- 云计算、大数据、人工智能、物联网等技术与概念的落地，技术的变革伸向了网络空间和现实世界的各个角落。技术环境和产业环境在变，导致网络攻击的手段和强度在迭代更新，网络攻击从未缺席。
- 在多种网络攻击类型中，DDoS攻击具有隐蔽性高、破坏性大、难以防范的特点，是最为常见的攻击方式之一。此外，传统的单包攻击也会对网络和系统造成较大的破坏。
- 本章节我们将会介绍常见的网络攻击原理以及防范技术。

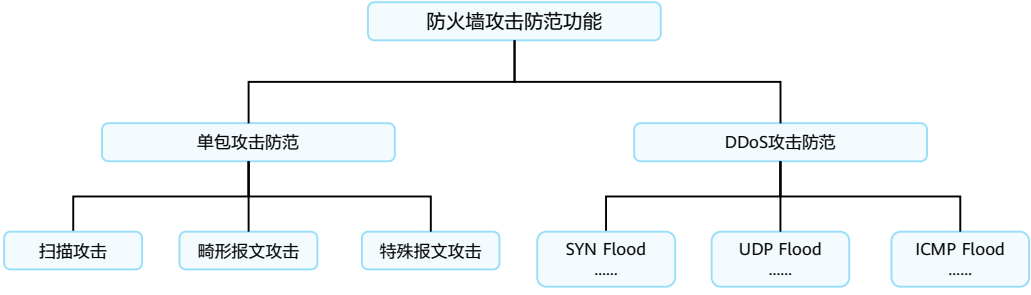
目标

- 学完本课程后，您将能够：
  - 描述常见单包攻击的原理
  - 描述常见DDoS攻击的原理
  - 描述针对单包攻击的防范原理
  - 描述针对DDoS攻击的防范原理
  - 描述AntiDDoS解决方案和防御原理

目录

攻击防范技术简介

- 防火墙的攻击防范功能能够检测出多种类型的网络攻击，并能采取相应的措施保护内部网络免受恶意攻击，保证内部网络主机的正常运行。
- 攻击防范功能可以抵御传统的单包攻击，也能够抵御各种常见的DDoS攻击。



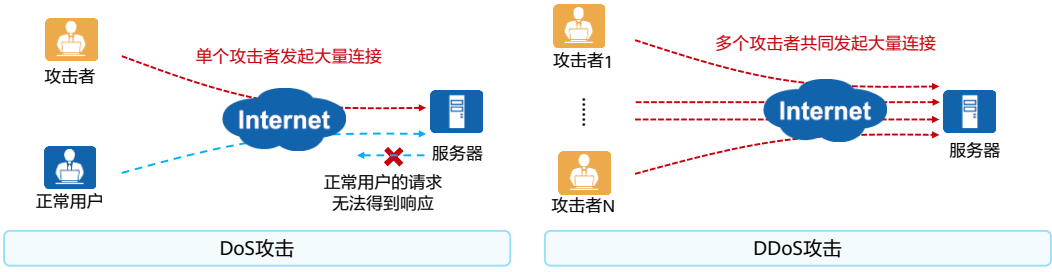
单包攻击

- 单包攻击主要包括扫描类攻击、畸形报文类攻击和特殊报文类攻击。

扫描类攻击	畸形报文类攻击	特殊报文类攻击
• 扫描型攻击是一种潜在的攻击行为，并不具有直接的破坏行为，通常是攻击者发动真正攻击前的网络探测行为。 • 例如：IP地址扫描攻击、端口扫描攻击等。	• 畸形报文攻击通常指攻击者发送大量有缺陷的报文，从而造成主机或服务器在处理这类报文时系统崩溃。 • 例如：Ping of Death攻击、Smurf攻击、Fraggle攻击、Land攻击等。	• 特殊控制报文攻击也是一种潜在的攻击行为，不具直接的破坏行为，攻击者通过发送特殊控制报文探测网络结构，为后续发送真正的攻击做准备。 • 例如：ICMP重定向攻击、Tracert攻击等。

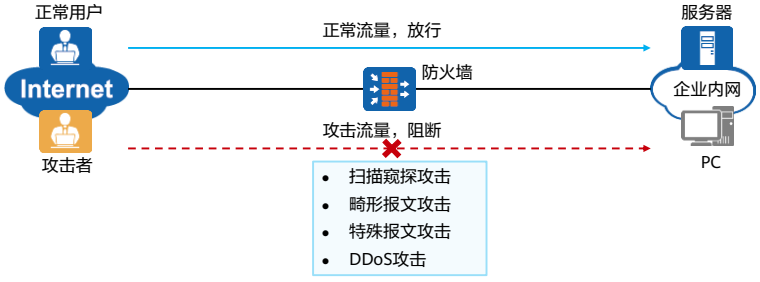
DDoS攻击

- DDoS攻击是一种分布式的DoS攻击。DoS即拒绝服务，其利用TCP/IP协议缺陷，通过占用协议栈资源或者发起大流量拥塞，达到消耗目标机器性能或者带宽资源的目的。不同于其他的留有木马后门或劫持数据的方式，DoS攻击并不威胁敏感数据，使合法用户不能获得应有的服务。
- DDoS即分布式拒绝服务，在DoS攻击的基础上，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力，使目标服务器无法提供正常服务。



攻击防范技术的应用场景

- 通常情况下，防火墙部署在企业内网出口，开启攻击防范功能后，防火墙能够区分出正常流量和攻击流量。对正常流量进行放行，对于攻击流量进行阻断，从而有效保障企业内网服务器和PC的正常运行，使服务器能够响应正常用户的业务需求，内网用户的PC能够正常工作。



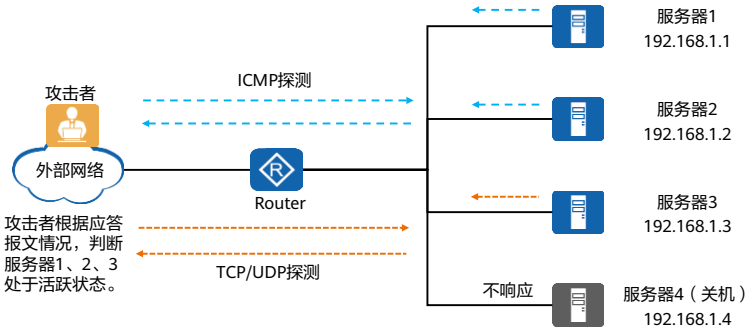
目录

常见的单包攻击

扫描攻击	畸形报文攻击	特殊报文攻击
地址扫描攻击	Smurf攻击	超大ICMP报文攻击
端口扫描攻击	Land攻击	ICMP重定向报文攻击
	Fraggle攻击	ICMP不可达报文
	IP分片报文攻击	Tracert报文攻击
	IP欺骗攻击	带源路由选项的IP报文攻击
	Ping of Death攻击	带路由记录项的IP报文攻击
	TCP报文标志位攻击	带时间戳选项的IP报文攻击
	Teardrop攻击	

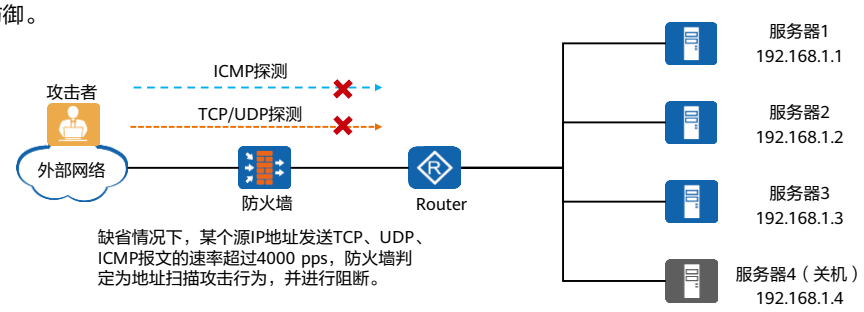
地址扫描攻击原理

- 攻击者运用ICMP报文（如Ping和Tracert命令）探测目标地址，或者使用TCP/UDP报文对目标地址发起连接（如TCP Ping），若能收到对应的响应报文，则表明目标主机处于活跃状态。



地址扫描攻击防范原理

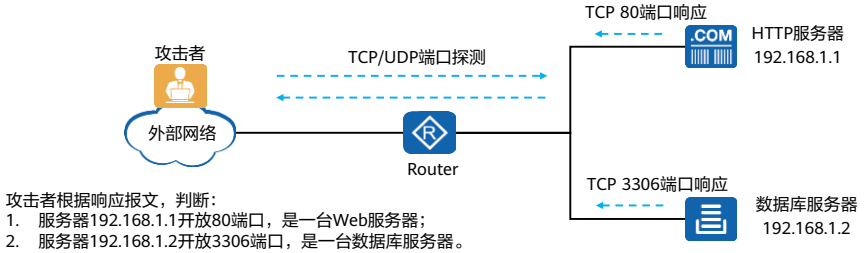
- 配置IP地址扫描攻击防范后，防火墙对接收的TCP、UDP、ICMP报文进行检测，若某个源IP地址每秒发往不同目的IP地址的报文数超过设定的阈值，就认为该源IP地址在进行IP地址扫描攻击，防火墙将该IP地址加入黑名单。
- IP地址扫描攻击防范功能按照IP报文的首包速率进行统计，如果源IP加入了白名单，则防火墙不再对此源IP进行防御。



缺省情况下，某个源IP地址发送TCP、UDP、ICMP报文的速率超过4000 pps，防火墙判定为地址扫描攻击行为，并进行阻断。

端口扫描攻击原理

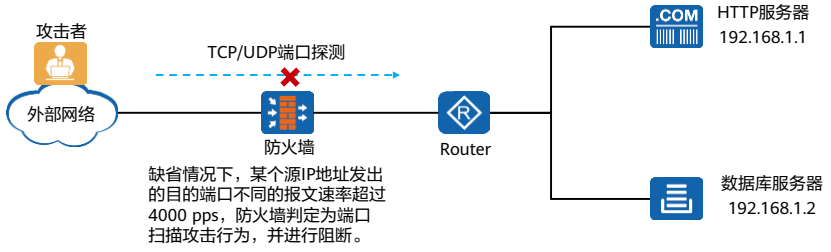
- 攻击者通过对端口进行扫描，探寻被攻击对象目前开放的端口，以确定攻击方式。在端口扫描攻击中，攻击者通常使用端口扫描攻击软件，发起一系列TCP/UDP连接，根据应答报文判断主机是否使用这些端口提供服务。



攻击者根据响应报文，判断：
1. 服务器192.168.1.1开放80端口，是一台Web服务器；
2. 服务器192.168.1.2开放3306端口，是一台数据库服务器。

端口扫描攻击防范原理

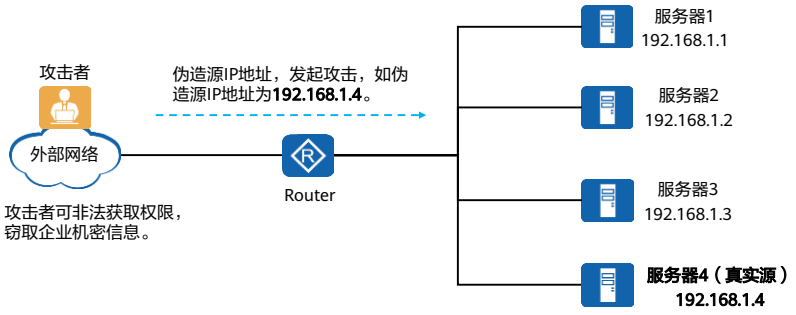
- 配置端口扫描攻击防范后，设备对接收的TCP、UDP报文进行检测，如果某个源IP地址每秒发出的报文中目的端口不同的报文数超过了设定的阈值时，就认为该源IP地址在进行端口扫描攻击，防火墙将该IP地址加入黑名单。
- 端口扫描攻击防范功能按照IP报文的首包速率进行统计，如果源IP加入了白名单，则防火墙不再对此源IP进行防御。



缺省情况下，某个源IP地址发出的目的端口不同的报文速率超过4000 pps，防火墙判定为端口扫描攻击行为，并进行阻断。

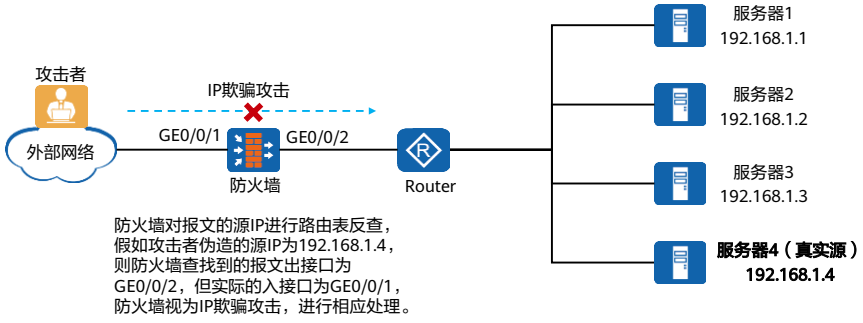
IP欺骗攻击原理

- IP欺骗攻击是一种常用的攻击方法，同时也是其他攻击方法的基础。攻击者通过向目标主机发送源IP地址伪造的报文，欺骗目标主机，从而获取更高的访问和控制权限。该攻击危害目标主机的资源，造成信息泄漏。



IP欺骗攻击防范原理

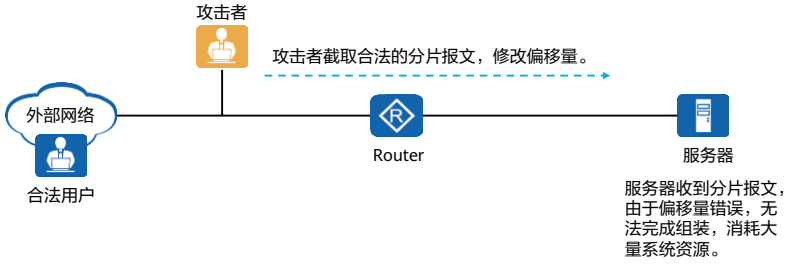
- 启用IP欺骗攻击防范后，设备对报文的源IP地址进行路由表反查，检查路由表中到源IP地址的出接口和报文的入接口是否一致。如果不一致，则视为IP欺骗攻击，并根据配置的动作处理该数据包。



防火墙对报文的源IP进行路由表反查，
假如攻击者伪造的源IP为192.168.1.4，
则防火墙查找到的报文出接口为
GE0/0/2，但实际的入接口为GE0/0/1，
防火墙视为IP欺骗攻击，进行相应处理。

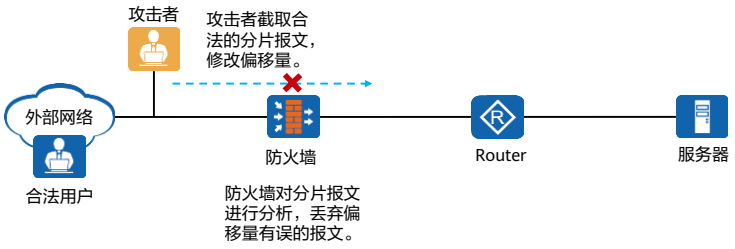
Teardrop攻击原理

- 为满足链路层MTU的要求，一些大的IP报文在传送过程中需要进行分片，被分片的报文在IP报头中会携带分片标志位和分片偏移量。如果攻击者截取分片报文后，对其中的偏移量进行修改，则数据接收端在收到分片报文后，无法组装为完成的数据包。接收端会不断进行尝试，消耗大量系统资源。



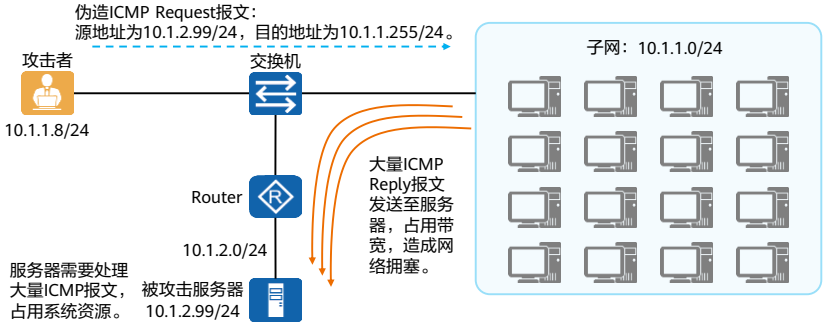
Teardrop攻击防范原理

- 启用Teardrop攻击防范后，设备会对接收到的分片报文进行分析，计算报文的偏移量是否有误。如果有误则直接丢弃该报文，并记录攻击日志。



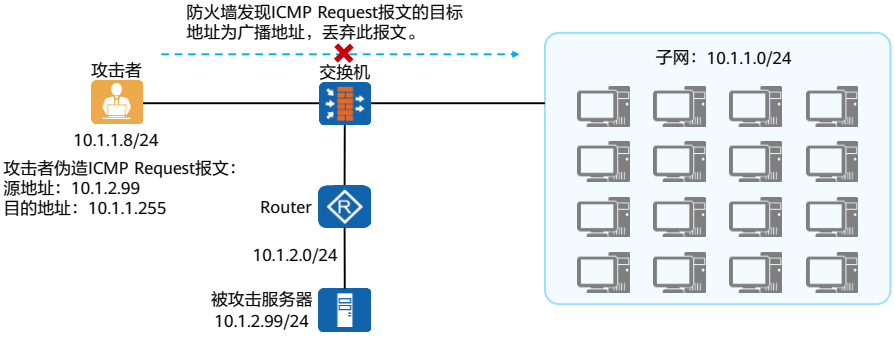
Smurf攻击原理

- 攻击者并不直接攻击目标服务器，而是通过伪造大量ICMP请求报文来实施网络攻击。伪造报文的源地址是被攻击服务器的地址，目的地址是某一个网络的广播地址，从而会造成大量主机向被攻击服务器发送ICMP应答报文，消耗网络带宽资源和服务器系统资源。此类攻击称为Smurf攻击。



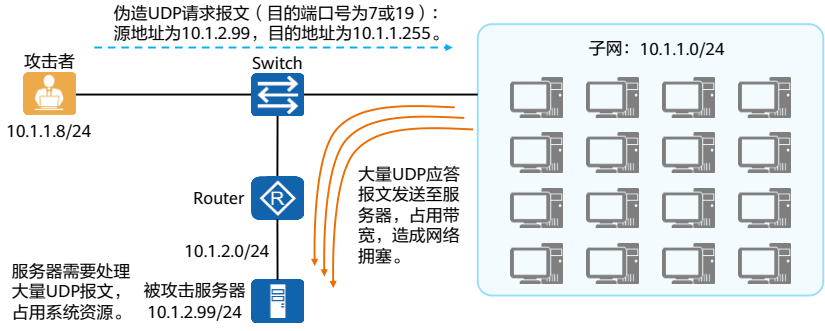
Smurf攻击防范原理

- 启用Smurf攻击防范后，防火墙会检查ICMP请求报文的目的地址是否为广播地址（即主机位全1）或网络地址（即主机位全0）。如果是则丢弃该报文，并记录攻击日志。



Fraggle攻击原理

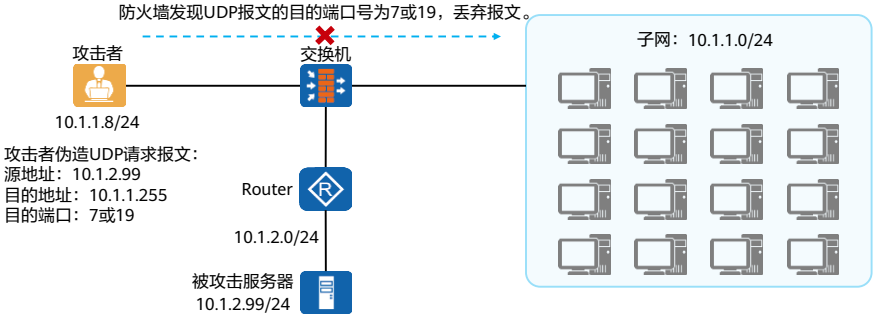
- 类似于Smurf攻击，攻击者通过伪造大量UDP请求报文（目的端口号为7或19）来实施网络攻击。伪造报文的源地址是被攻击服务器地址，目的地址是某一个网络的广播地址，从而会造成大量主机向被攻击服务器发送UDP应答报文，消耗网络带宽资源和服务器系统资源。此类攻击称为Fraggle攻击。



- UDP端口7是一个知名端口，对应的协议是Echo（回显）协议，主机收到一个UDP Echo请求报文，会回复相同的内容作为响应。
- UDP端口19是一个知名端口，对应的协议是Chargen（字符发生器）协议，主机收到一个UDP Chargen请求报文，会回复一串字符串作为响应。

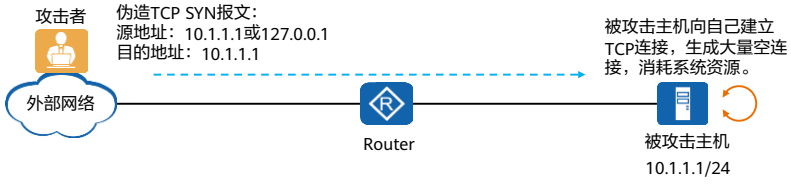
Fraggle攻击防范原理

- 启用Fraggle攻击防范后，设备会对收到的UDP报文进行检测。若目的端口号为7或19，设备拒绝该报文，并记录攻击日志。



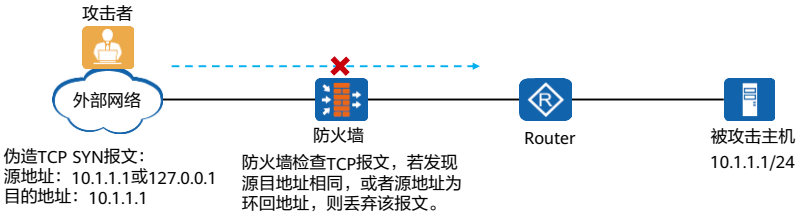
Land攻击原理

- 攻击者伪造TCP SYN数据包发送至被攻击主机，伪造报文的源地址和目的地址相同，或者源地址为环回地址（即127.0.0.0/8），导致被攻击主机向自己的地址发送SYN-ACK消息，产生大量的TCP空连接，消耗主机系统资源。此类攻击称为Land攻击，又称为环回攻击。



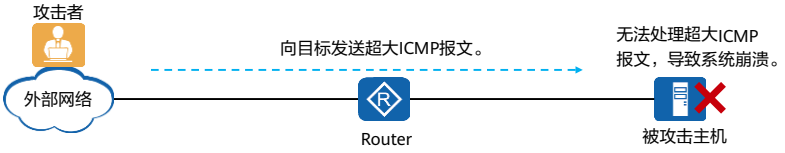
Land攻击防范原理

- 防火墙启用环回攻击防范后，设备会检查TCP报文的源地址和目的地址是否相同，或者TCP报文的源地址是否为环回地址。如果是则丢弃该报文，并记录攻击日志。



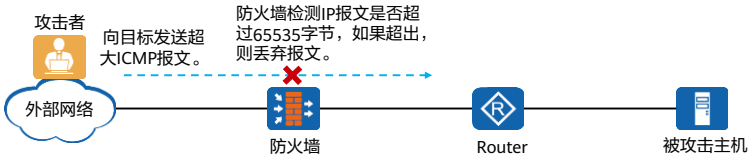
Ping of Death攻击原理

- IP报文的长度字段为16位，即IP报文的最大长度为65535字节。Ping of Death利用一些长度超大的ICMP报文对系统进行攻击。
- 对于某些网络设备或主机系统，在接收到超大ICMP报文后，由于处理不当，会造成系统崩溃、死机或重启。



Ping of Death攻击防范原理

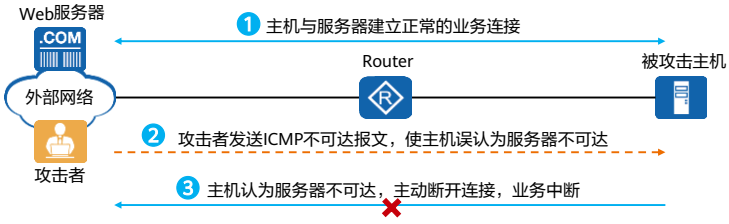
- 防火墙启用Ping of Death攻击防范后，设备会检测IP报文的大小是否大于65535字节，对大于65535字节的报文直接丢弃，并记录攻击日志。



- 防火墙还支持对未超过65535字节的超大ICMP报文攻击进行防御，用户可以根据实际网络需要，自行定义允许通过的ICMP报文的最大长度，如果防火墙检测发现实际的ICMP报文长度超过阈值，则认为发生了超大ICMP报文攻击，将丢弃该报文。

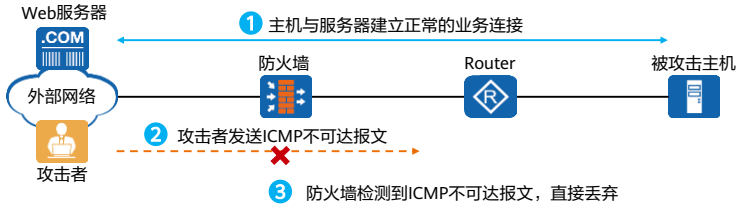
ICMP不可达报文攻击原理

- 不同的系统对ICMP不可达报文的处理方式不同，有的系统在收到网络或主机不可达的ICMP报文后，对后续发往此目的地址的报文直接认为不可达，从而断开正常的业务连接。攻击者利用这一点，伪造不可达ICMP报文，切断受害者与目的地的连接，造成攻击。



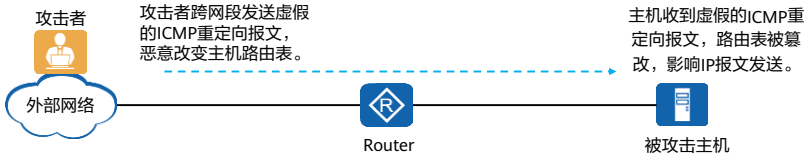
ICMP不可达报文攻击防范原理

- 防火墙启用ICMP不可达报文攻击防范后，设备将直接丢弃ICMP不可达报文，并记录攻击日志。



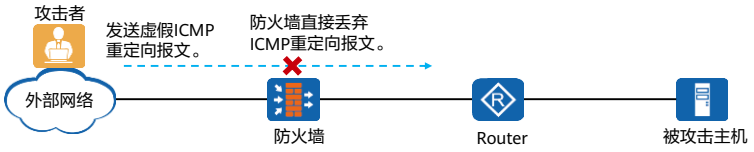
ICMP重定向报文攻击原理

- 网络设备通常通过向同一个子网的主机发送ICMP重定向报文来请求主机改变路由。一般情况下，设备仅向同一个子网的主机发送ICMP重定向报文，但一些恶意的攻击可能跨越网段向另外一个网络的主机发送虚假的重定向报文，以改变主机的路由表，干扰主机正常的IP报文发送。



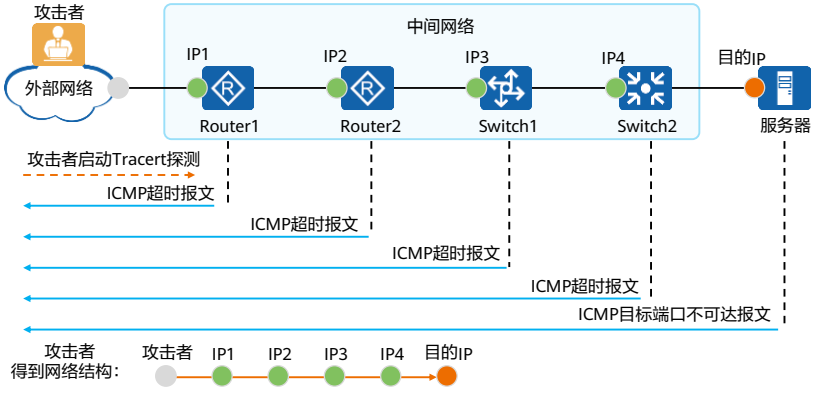
ICMP重定向报文攻击防范原理

- 启用ICMP重定向报文攻击防范后，防火墙将直接丢弃所有接收到的ICMP重定向报文，并记录攻击日志。



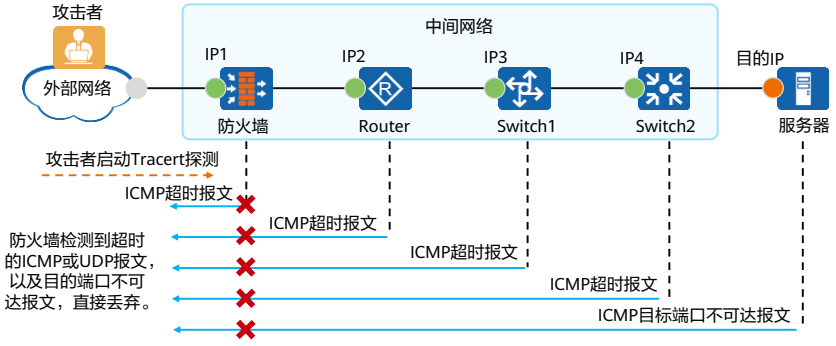
Tracert攻击原理

- Tracert攻击是攻击者利用TTL为0时返回的ICMP超时报文，以及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，主要用于窥探目标网络的结构。



Tracert攻击防范原理

- 启用Tracert攻击防范后，防火墙将检测到的超时的ICMP报文或UDP报文，或者目的端口不可达报文，直接丢弃，并记录攻击日志。



目录

地址扫描攻击防范配置

- 配置IP地址扫描攻击防范功能：
  - 开启IP地址扫描攻击防范功能；

```
[FW] firewall defend ip-sweep enable
```

  - 配置地址扫描速率阈值，当发现某台主机的地址扫描行为的速率超过了该阈值，判断其为攻击者；

```
[FW] firewall defend ip-sweep max-rate max-rate-number
```

  - 配置单包攻击的动作为discard；

```
[FW] firewall defend action discard
```

  - 开启黑名单功能，识别出攻击者后，将其加入黑名单。

```
[FW] firewall blacklist enable
[FW] firewall defend ip-sweep blacklist-timeout interval
```


- 配置IP地址扫描攻击防范后，设备对接收的TCP、UDP、ICMP报文进行检测，如果某个源IP地址每秒发往不同目的IP地址的报文数超过了设定的阈值时，就认为该源IP地址在进行IP地址扫描攻击，防火墙将对该IP地址做如下处理：
  - 若防火墙开启了黑名单功能，且配置了firewall defend action discard，则该IP地址被加入黑名单，系统丢弃从该IP地址发来的报文。
  - 若防火墙没有开启黑名单功能，但配置了firewall defend action discard，系统也会产生告警，并丢弃报文。
- 如果源IP加入了白名单，则IP地址扫描攻击防范不再对此源IP进行检查。

端口扫描攻击防范配置

- 配置端口扫描攻击防范功能：
  - 开启端口扫描攻击防范功能；

```
[FW] firewall defend port-scan enable
```

  - 配置端口扫描速率阈值。当发现某台主机的端口扫描行为的速率超过了该阈值，就会将其判断为攻击者；

```
[FW] firewall defend port-scan max-rate max-rate-number
```

  - 配置单包攻击的动作为discard；

```
[FW] firewall defend action discard
```

  - 开启黑名单功能，识别出攻击者后，将其加入黑名单。

```
[FW] firewall blacklist enable
[FW] firewall defend port-scan blacklist-timeout interval
```


- 配置端口扫描攻击防范后，设备对接收的TCP、UDP报文进行检测，如果某个源IP地址每秒发出的目的端口不同的报文数超过了设定的阈值时，就认为该源IP地址在进行端口扫描攻击，防火墙将对该IP地址做如下处理：
  - 若防火墙开启了黑名单功能，且配置了firewall defend action discard，则该IP地址被加入黑名单，系统丢弃从该IP地址发来的报文。
  - 若防火墙没有开启黑名单功能，但配置了firewall defend action discard，系统也会产生告警，并丢弃报文。
- 如果源IP加入了白名单，则端口扫描攻击不再对此源IP进行防范。

单包攻击防范配置 (1)

- 配置IP欺骗攻击防范功能：

```
[FW] firewall defend ip-spoofing enable
```

- 配置Teardrop攻击防范功能：

```
[FW] firewall defend teardrop enable
```

- 配置Smurf攻击防范功能：

```
[FW] firewall defend smurf enable
```

- 配置Land攻击防范功能：

```
[FW] firewall defend land enable
```

- 配置Fraggle攻击防范功能：

```
[FW] firewall defend fraggle enable
```

- 配置Ping of Death攻击防范功能：

```
[FW] firewall defend ping-of-death enable
```

单包攻击防范配置 (2)

- 配置超大ICMP报文攻击防范功能：

```
[FW] firewall defend large-icmp enable
[FW] firewall defend large-icmp max-length length
```

- 配置ICMP不可达报文攻击防范功能：

```
[FW] firewall defend icmp-unreachable enable
```

- 配置ICMP重定向报文攻击防范功能：

```
[FW] firewall defend icmp-redirect enable
```

- 配置Tracert报文攻击防范功能：

```
[FW] firewall defend tracert enable
```

目录

DDoS攻击防范技术介绍

防范技术	简易原理	可防范的攻击类型
源探测技术	设备对请求服务的报文的源IP地址进行探测，来自真实源IP地址的报文将被转发，来自虚假源IP地址的报文将被丢弃。	SYN Flood、HTTP Flood、HTTPS Flood、DNS Request Flood、DNS Reply Flood、SIP Flood
指纹技术	设备将攻击报文的一段显著特征学习为指纹，未匹配指纹的报文将被转发，匹配指纹的报文将被丢弃。	UDP Flood、UDP Fragment Flood
限流技术	设备直接丢弃超过速率上限的报文。	ICMP Flood、UDP Flood

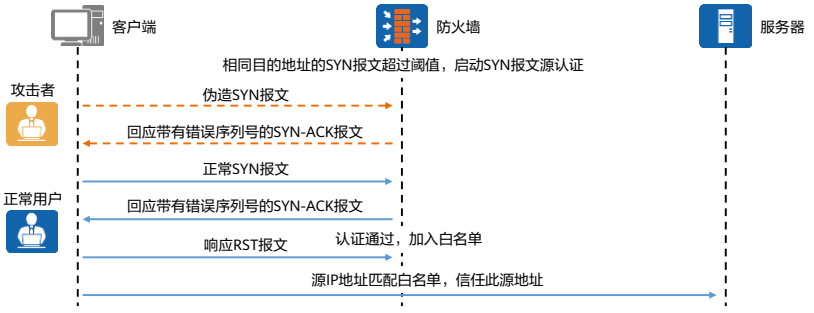
SYN Flood攻击原理

- 攻击者伪造大量的SYN请求报文发送给服务器，服务器每收到一个SYN就会响应一个SYN-ACK报文，但是攻击者并不会理会此SYN-ACK报文，所以服务器端会存在大量TCP半开连接，维护这些链接需要消耗大量的CPU及内存资源，最终导致服务器无暇处理正常的SYN请求，拒绝服务。此攻击称为SYN Flood攻击。

- 与SYN Flood攻击相似的攻击还有FIN Flood攻击、RST Flood攻击、ACK Flood攻击等，其攻击原理都是伪造带有特殊标志位的TCP报文，对目标服务器发起攻击，消耗其系统资源，最终导致服务器无法提供正常的服务，这类攻击本文不再赘述。

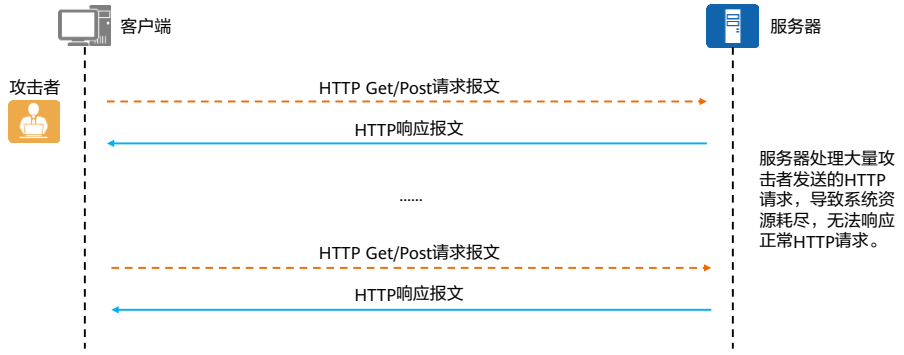
SYN Flood防范原理

- 在连续一段时间内，防火墙收到的具有相同目的地址的SYN报文数如果超过阈值，则启动SYN报文源认证。防火墙拦截SYN报文，并伪造一个带有错误序列号的SYN-ACK报文回应给客户端。
  - 如果客户端是虚假源，则不会对错误的SYN-ACK报文进行回应，认证失败，防火墙丢弃后续此源地址的SYN报文；
  - 如果客户端是真实源，则会响应一个RST报文，认证通过，防火墙把此源地址加入白名单，并放行后续的SYN报文。



HTTP Flood攻击原理

- 攻击者通过代理或僵尸主机向目标服务器发起大量的HTTP Get/Post请求报文，这些请求报文一般都会消耗大量的服务器系统资源（如请求数据库操作），最终导致服务器系统资源耗尽，无法响应正常请求。这类攻击称为HTTP Flood攻击。



HTTP Flood防范原理 (基本模式)

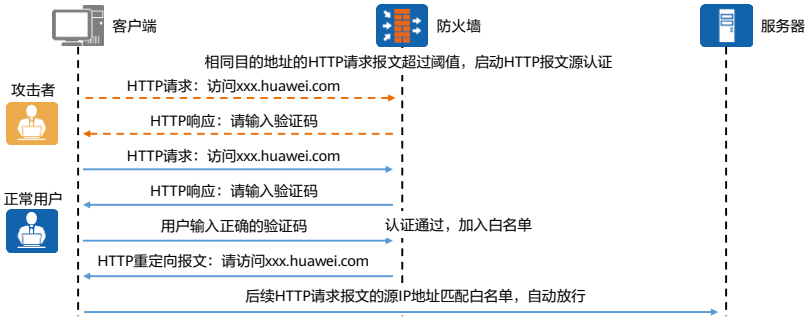
- 在连续一段时间内，防火墙收到具有相同目的地址的HTTP请求报文数如果超过阈值，则启动HTTP报文源认证。防火墙拦截HTTP请求报文，并返回一个HTTP重定向报文给客户端：
  - 如果是虚假源，不会对HTTP重定向报文进行相应，认证失败，防火墙丢弃后续此源地址的HTTP请求报文；
  - 如果是真实源，则会正常响应HTTP重定向报文，认证通过，源地址加入防火墙白名单，后续HTTP请求报文自动放行。

HUAWEI

- 基本模式中的重定向功能只能对整个网页进行重定向，不能针对网页中的内嵌资源（比如：图片）进行重定向。当用户请求的页面与页面内嵌资源不在同一个服务器上，内嵌资源所在服务器发生异常时，可以对嵌套资源服务器启动302重定向防御，探测访问源是否为真实浏览器。真实浏览器支持重定向功能，可以自动完成重定向过程，不会影响客户体验。

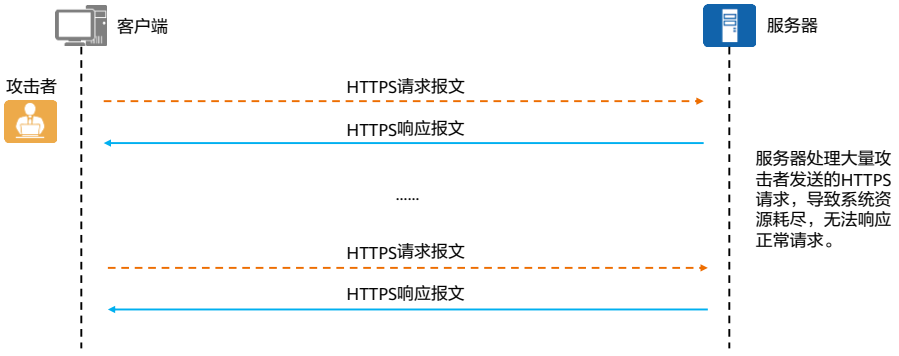
HTTP Flood防范原理 (增强模式)

- 在连续一段时间内，防火墙收到的具有相同目的地址的HTTP请求报文数如果超过阈值，则启动HTTP报文源认证。防火墙拦截HTTP请求报文，并返回一个HTTP页面给客户端，并请求用户输入页面中的验证码：
  - 如果是虚假源，不会输入验证码信息，认证失败，防火墙丢弃后续此源地址的HTTP请求报文；
  - 如果是真实源，输入正确的验证码信息，认证通过，源地址加入防火墙白名单，后续HTTP请求报文自动放行。



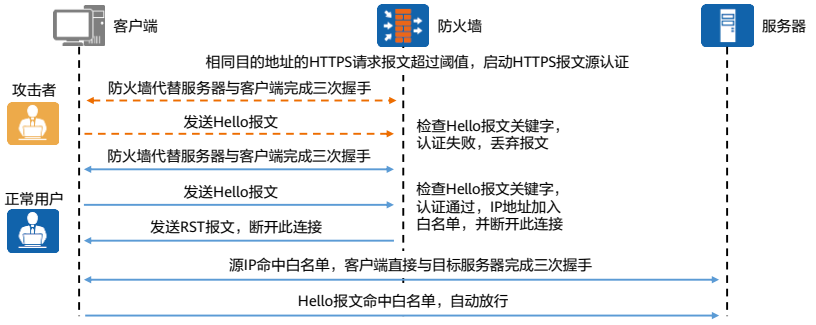
HTTPS Flood攻击原理

- 攻击者通过代理、僵尸主机或者直接向目标服务器发起大量的HTTPS连接，造成服务器资源耗尽，无法响应正常的请求。这类攻击称为HTTPS Flood攻击。



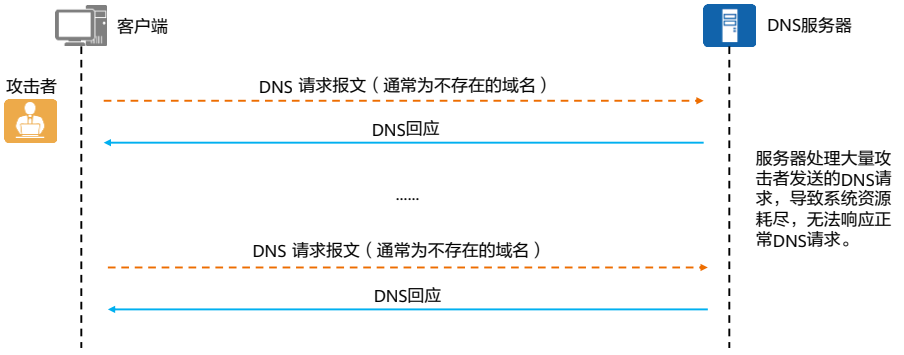
HTTPS Flood防范原理

- 防火墙基于目的地址对目的端口为443的HTTPS报文（不区分请求或响应报文）速率进行统计，当目的IP相同且目的端口为443的HTTPS报文速率达到阈值时，启动源认证防御。防火墙代替服务器与客户端完成三次握手，随后对客户端发送的Hello报文的关键字段进行检查，丢弃攻击者报文，放通正常用户报文（并加入白名单）。



DNS Request Flood攻击原理

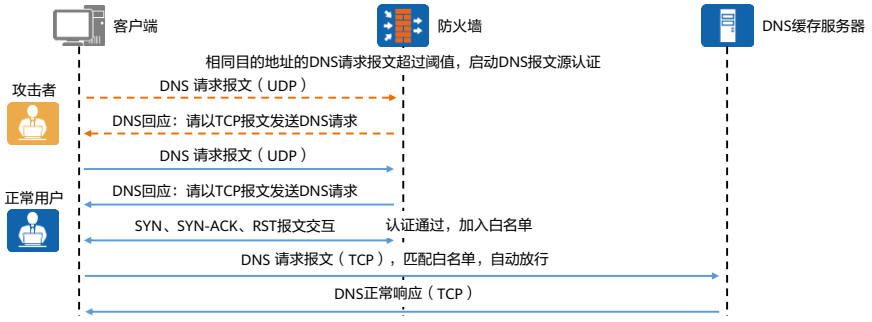
- 攻击者向DNS服务器发送大量的域名解析请求（通常都是不存在的域名解析请求），导致DNS缓存服务器/授权服务器消耗大量系统资源，最终导致服务器瘫痪，无法对正常DNS请求作出回应。这类攻击称为DNS Request Flood攻击。



源探测技术 指纹技术 限流技术

DNS Request Flood防范原理 (针对DNS缓存服务器)

- 针对DNS缓存服务器，在连续一段时间内，防火墙收到的具有相同目的地址的DNS请求报文数如果超过阈值，则启动DNS报文源认证。防火墙强制让客户端以TCP报文发送DNS请求：
  - 如果是虚假源，则客户端不会切换至TCP报文格式发送DNS请求，认证失败，防火墙拒绝后续DNS请求报文；
  - 如果是真实源，则客户端会以TCP报文发送DNS请求，认证通过，加入白名单，防火墙放行后续DNS请求报文。

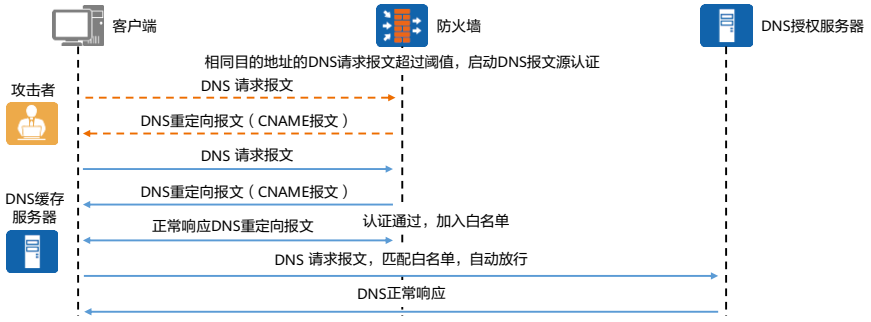


HUAWEI

- 在DNS源认证过程中，防火墙会触发客户端以TCP报文发送DNS请求，用以验证源IP的合法性，但在一定程度上会消耗DNS缓存服务器的TCP连接资源。
- 此方式可以很好的防御针对缓存服务器的DNS请求攻击，但是在现网使用过程中，并不是所有场景都适用。因为在源探测过程中，防火墙会要求客户端通过TCP方式发送DNS请求，但是并不是所有的客户端都支持以TCP方式发送DNS请求，所以这种方式在使用过程中也有限制。如果有正常客户端不支持以TCP方式发送DNS请求，使用此功能时，就会影响正常业务。

DNS Request Flood防范原理 (针对DNS授权服务器)

- 针对DNS授权服务器，在连续一段时间内，防火墙收到的具有相同目的地址的DNS请求报文数如果超过阈值，则启动DNS报文源认证。防火墙向客户端发送DNS重定向报文：
  - 如果是虚假源，则不会回应DNS重定向报文，认证失败，防火墙拒绝后续DNS请求报文；
  - 如果是真实源，则会正常响应DNS重定向报文，认证通过，加入白名单，防火墙放行后续DNS请求报文。

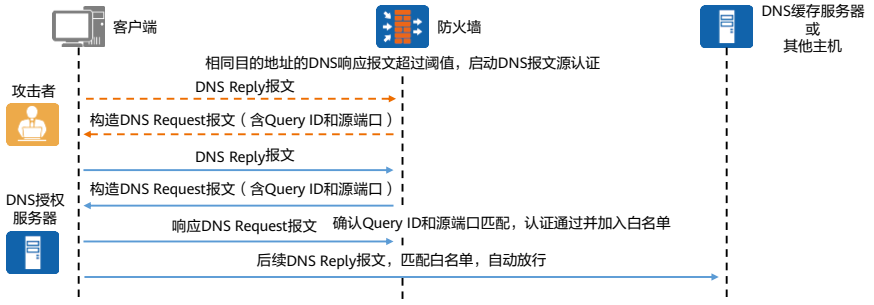


DNS Reply Flood攻击原理

- 攻击者向DNS服务器发送大量的DNS Reply报文，进而消耗服务器资源，此类攻击称为DNS Reply Flood攻击，攻击可能造成的影响有：
  - DNS Reply报文把正常域名指向恶意IP地址，影响正常的DNS解析功能。
  - 大量DNS Reply报文消耗带宽资源、服务器系统资源，导致DNS服务器瘫痪，无法提供正常服务。

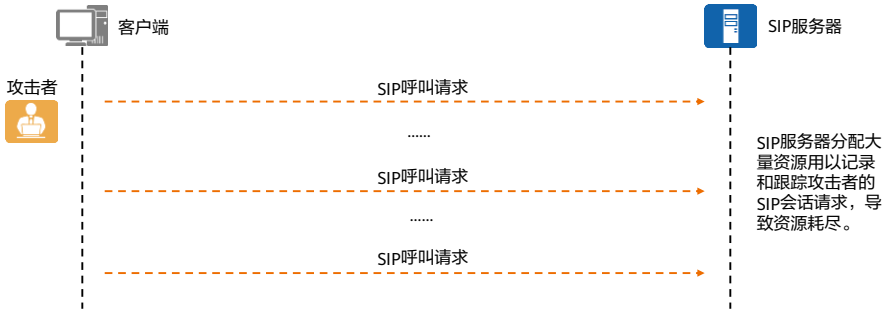
DNS Reply Flood防范原理

- 在连续一段时间内，防火墙收到的具有相同目的地址的DNS响应报文数如果超过阈值，则启动DNS报文源认证。防火墙构造新的DNS Request报文（包含Query ID和源端口）发送至源端：
  - 如果是虚假源，则不会回应此DNS Request报文，认证失败，防火墙拒绝DNS响应报文；
  - 如果是真实源，则会正常响应此DNS Request报文，认证通过，加入白名单，防火墙放行后续DNS响应报文。



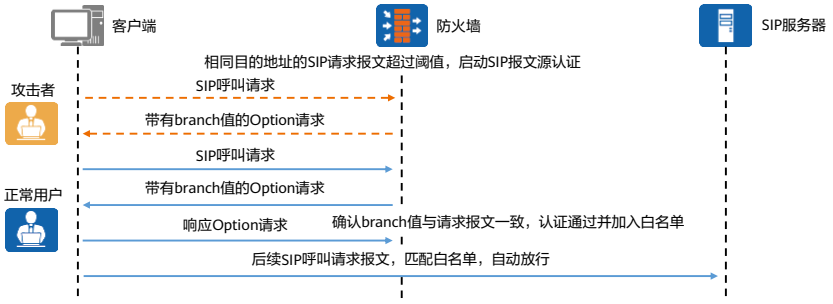
SIP Flood攻击原理

- 攻击者通过发送大量的SIP呼叫请求消息到SIP服务器，导致SIP服务器分配大量的资源用以记录和跟踪会话，最终资源耗尽而无法响应合法用户的呼叫请求。此类攻击称为SIP Flood攻击。



SIP Flood防范原理

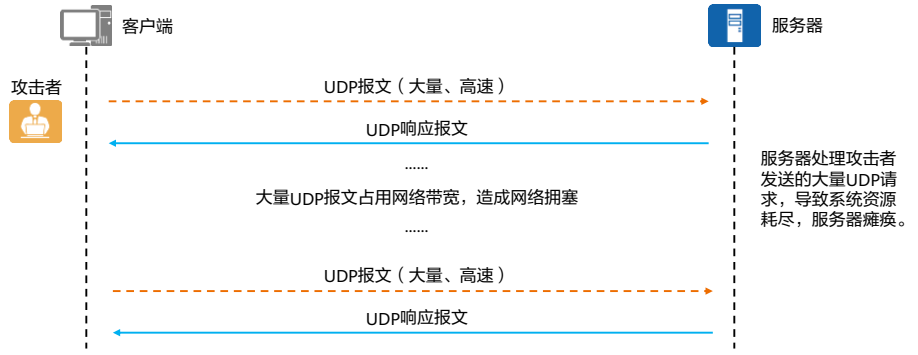
- 在连续一段时间内，防火墙收到的具有相同目的地址的SIP请求报文数如果超过阈值，则启动SIP报文源认证。防火墙发送带有branch值的Option请求报文至源端：
  - 如果是虚假源，则不会响应此Option请求，认证失败，防火墙拒绝SIP请求报文；
  - 如果是真实源，则会正常响应此Option请求，认证通过，加入白名单，防火墙放行后续SIP响应报文。



源探测技术 指纹技术 限流技术

UDP Flood攻击原理

- UDP协议是一种无连接的服务，攻击者向服务器发送大量UDP协议数据包，如发送大量UDP报文冲击DNS服务器、Radius认证服务器、流媒体视频服务器等，导致服务器带宽和系统资源耗尽，无法提供正常服务。此类攻击称为UDP Flood攻击。

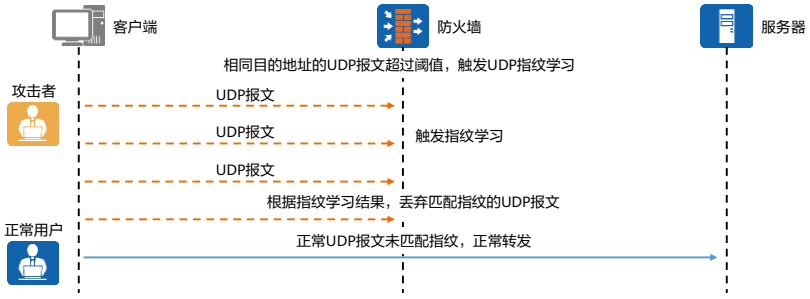


HUAWEI

- UDP Flood攻击包括小包和大包两种方式进行攻击：
  - 小包是指64字节大小的数据包，这是以太网上传输数据帧的最小值，在相同流量下，单包体积越小，数据包的数量就越多。由于交换机、路由器等网络设备需要对每一个数据包进行检查和校验，因此使用UDP小包攻击能够最有效的增大网络设备处理数据包的压力，造成处理速度的缓慢和传输延迟等拒绝服务攻击的效果。
  - 大包是指1500字节以上的数据包，其大小超过了以太网的最大传输单元，使用UDP大包攻击，能够有效的占用网络接口的传输宽带，并迫使被攻击目标在接收到UDP数据时进行分片重组，造成网络拥堵，服务器响应速度变慢。
- UDP Fragment Flood攻击原理与UDP Flood类似，不再赘述。

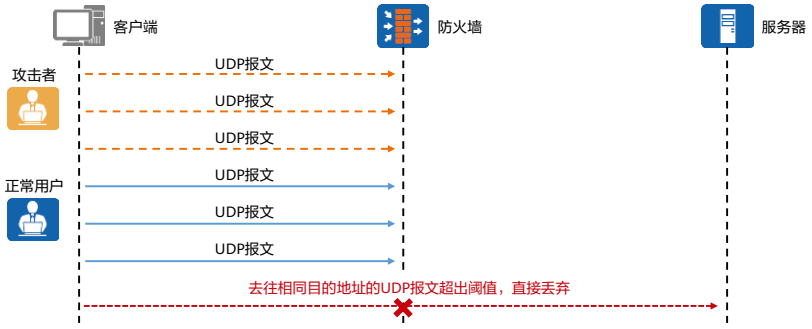
UDP Flood防范原理 (指纹学习)

- UDP Flood攻击报文具有一定的特点，这些攻击报文通常都拥有相同的特征字段，可以通过指纹学习的方式防御UDP Flood攻击。
- 在连续一段时间内，防火墙收到的具有相同目的地址的UDP报文数如果超过阈值，则触发指纹学习。防火墙将攻击报文的一段显著特征学习为指纹后，匹配指纹的报文会被丢弃。



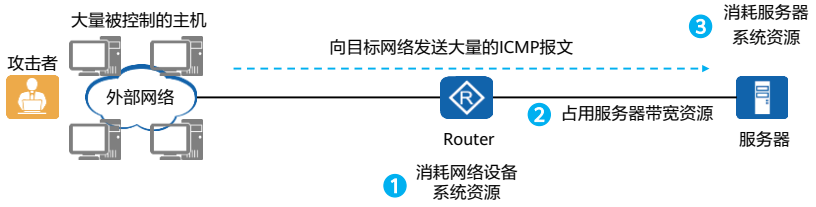
UDP Flood防范原理 (限流)

- 如果通过指纹学习方式仍然无法抵御UDP Flood攻击，可以采用限流技术防范UDP Flood攻击。限流技术将去往同一目的地址的UDP报文速率限制在一定阈值之内，直接丢弃超过阈值的UDP报文，以避免网络拥塞。
- 限流技术本身无法区分正常报文和攻击报文，使用时可能影响正常业务，推荐使用UDP指纹学习方式。



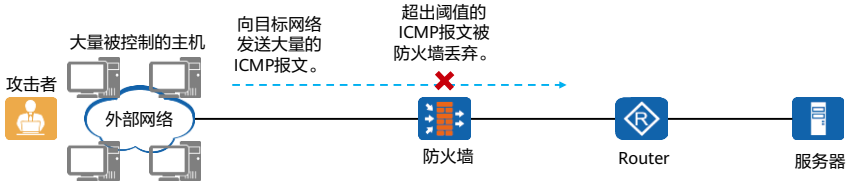
ICMP Flood攻击原理

- 实施ICMP Flood攻击的攻击者一般通过控制大量主机，在短时间内发送大量的超大ICMP报文到被攻击目标，占用被攻击目标的网络带宽和系统资源，最终导致资源耗尽，业务不可用。
- 此类型攻击也会导致依靠会话转发的网络设备会话耗尽，引发网络瘫痪。



ICMP Flood防范原理

- 针对ICMP Flood攻击，防火墙可以对ICMP报文进行限流，将ICMP报文速率限制在一个较小的阈值范围内，超出阈值的ICMP报文被防火墙直接丢弃。
- 防火墙可以基于接口对ICMP报文进行限流，也可基于目的IP地址对ICMP报文进行限流。



目录

配置DDoS防范参数

- 开启每种DDoS攻击防御前，需先配置防范参数。
  - 在接口下开启流量统计功能：

```
[FW] interface interface GigabitEthernet0/0/1
[FW-GigabitEthernet0/0/1] anti-ddos flow-statistic enable
```

  - 设置流量的检测和清洗方式：

```
[FW] ddos-mode { detect-clean | detect-only }
```

  - 配置DDoS流量统计抽样比：

```
[FW] anti-ddos statistic sampling-fraction sampling-fraction
```

  - 设置启动攻击防范和停止攻击防范的时间延迟：

```
[FW] anti-ddos defend-time start-delay start-delay end-delay end-delay
```

  - 配置流量进入DDoS防范流程的告警阈值：

```
[FW] anti-ddos destination-ip alert-rate alert-rate
```

  - 配置源IP监控表的老化时间：

```
[FW] anti-ddos source-ip detect aging-time time
```

DDoS攻击防范配置 (1)

- 配置全局SYN Flood攻击防范功能：

```
[FW] anti-ddos syn-flood source-detect
```

- 配置全局HTTP Flood防范功能：

```
[FW] anti-ddos http-flood source-detect [ mode { basic | advanced | redirect } ]
[FW] anti-ddos http-flood defend alert-rate alert-rate
```

- 配置全局HTTPS Flood防范功能：

```
[FW] anti-ddos https-flood source-detect [ alert-rate alert-rate ]
```

- 配置全局DNS Request Flood防范功能：

```
[FW] anti-ddos dns-request-flood source-detect mode { basic | auth-ns } [ alert-rate alert-rate ]
```

- 配置全局DNS Reply Flood防范功能：

```
[FW] anti-ddos dns-reply-flood source-detect [ alert-rate alert-rate ]
```

- 配置全局SIP Flood防范功能：

```
[FW] anti-ddos sip-flood source-detect [ alert-rate alert-rate ]
```

DDoS攻击防范配置 (2)

- 配置全局UDP Flood攻击防范功能：

```
[FW] anti-ddos udp-flood dynamic-fingerprint-learn [ alert-speed alert-speed ]
```

- 配置全局UDP分片攻击防范功能：

```
[FW] anti-ddos udp-frag-flood dynamic-fingerprint-learn [ alert-speed alert-speed ]
```

- 配置ICMP Flood攻击防范功能：
  - 配置接口防范功能：

```
[FW] interface interface GigabitEthernet0/0/1
[FW-GigabitEthernet0/0/1] anti-ddos icmp-flood [ alert-rate alert-rate ]
```

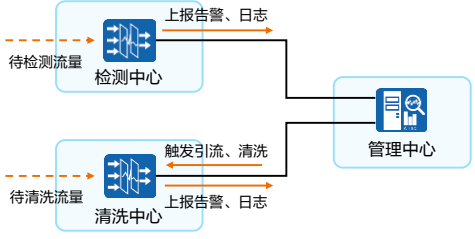
  - 配置基于目的IP的限速功能：

```
[FW] bandwidth-limit destination-ip type icmp max-speed max-speed
```

目录

AntiDDoS方案概述

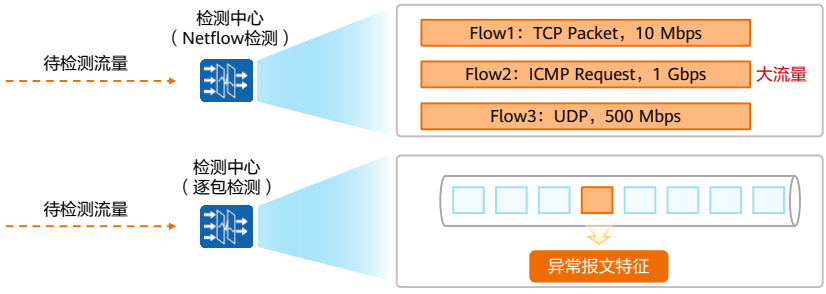
- AntiDDoS解决方案由华为自主研发的AntiDDoS和管理中心组成。其中AntiDDoS包含检测中心和清洗中心两部分，整个方案包括检测中心、清洗中心和SecoManager管理中心三大部分。
  - 检测中心：负责对流量进行检测，发现异常后上报管理中心，由管理中心下发引流策略至清洗中心进行引流清洗。
  - 清洗中心：根据管理中心下发的策略进行引流、清洗，并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。
  - 管理中心：负责检测中心和清洗中心的统一管理，是AntiDDoS解决方案的管理中枢。提供设备管理、策略管理、性能管理、告警管理、报表管理等功能。



- ATIC为SecoManager中的功能模块。

检测中心

- 检测中心的检测技术主要分为两种，一是基于Netflow的流量检测技术，二是基于应用的逐包检测技术，前者仅能检测大流量攻击，后者不仅能检测出大流量攻击还能够检测出小流量攻击和应用层攻击（如SQL注入）。
- 其中Netflow的流量检测技术因较大的抽样比和Netflow协议的限制，适合做大流量检测，无法检测小流量攻击。但由于大多数骨干网、城域网已经部署了Netflow设备，故Netflow设备联动方案部署成本相对较低，适合在城域网及骨干网做流量型攻击检测。

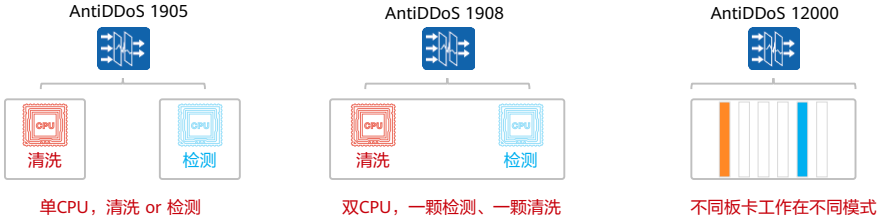


HUAWEI

- 可通过在网络中部署分流设备（针对光纤传输）或者部署流量镜像将流量复制到流量探针或者检测中心。

清洗中心

- 清洗中心主要根据管理中心下发的策略进行引流、清洗，并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。清洗中心提供多种DDoS流量清洗手段，可以准确识别正常流量，清洗各类异常流量，包括流量型攻击、应用层攻击、扫描窥探型攻击及畸形包攻击。
- 对于AntiDDoS盒式设备而言，单CPU的设备只能作为检测中心或者清洗中心，对于双CPU的设备，可以通过设备CPU类型同时作为检测设备和清洗设备，而对于AntiDDoS框式设备，可以指定具体某个板卡为检测、清洗模式。



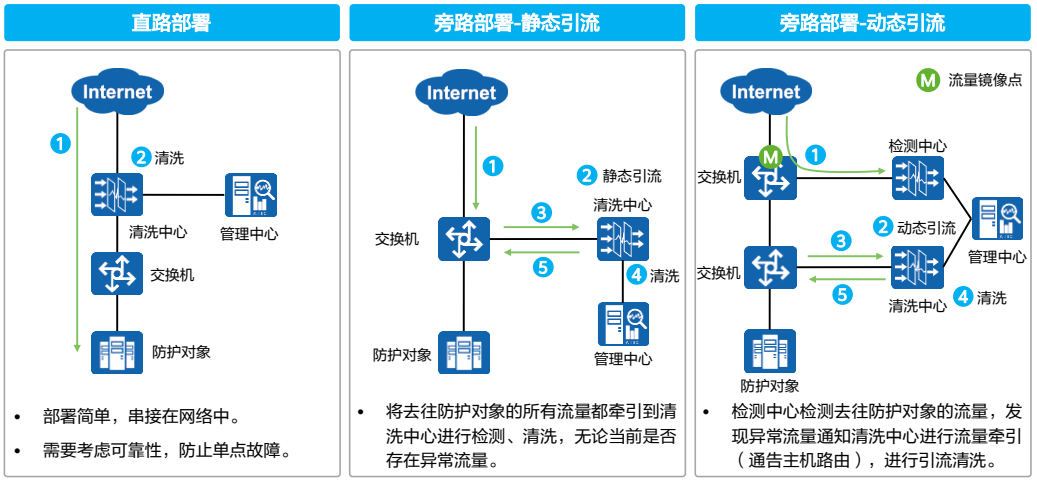
单CPU，清洗 or 检测　　双CPU，一颗检测、一颗清洗　　不同板卡工作在不同模式

ATIC系统架构

- SecoManager作为管理中心（主要为其中的ATIC功能模块）采用B/S架构，部署简单方便，需要将软件安装在独立的服务器上即可完成业务的管理和监控。一个管理中心可以集中管理多地域分散部署的多台检测和清洗设备。
- ATIC软件包含2部分：管理服务器和采集器。
  - ATIC管理服务器：管理检测和清洗中心设备，攻击防御策略配置，生成报表；
  - ATIC采集器：接收，汇总，分析采集器发来的攻击日志，上报给ATIC服务器；存储抓包文件，供管理员深入分析。

目录

AntiDDoS方案组网方式

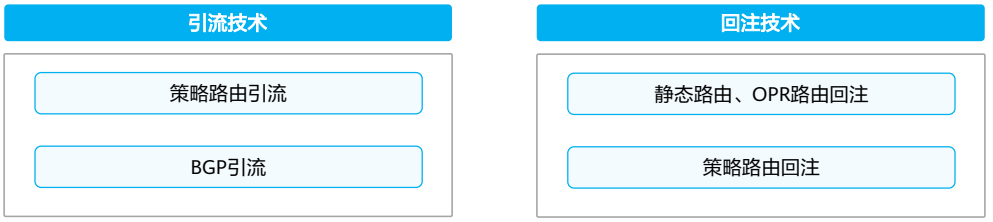


HUAWEI

- 在实际部署中，除了通过流量镜像的方式将流量复制到检测中心，还可通过部署分流设备将流量分流到检测中心。

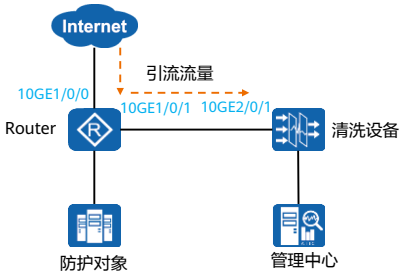
引流与回注

- 在直连部署组网中，所有的业务流量都需要经过清洗中心，清洗后根据路由表转发至防护对象。
- 在旁路部署组网中，缺省情况下，流量不经过清洗中心，需要配置引流和回注功能，才可实现流量清洗。
  - 引流：网络设备（路由器/交换机等）把原本发往防护对象的流量发往清洗中心的过程，称为引流；
  - 回注：清洗中心把清洗后的流量发回网络设备的过程，称为回注。
- 常用的引流、回注方法如下所示，它们之间通过自由组合搭配，共同实现流量清洗功能。



策略路由引流

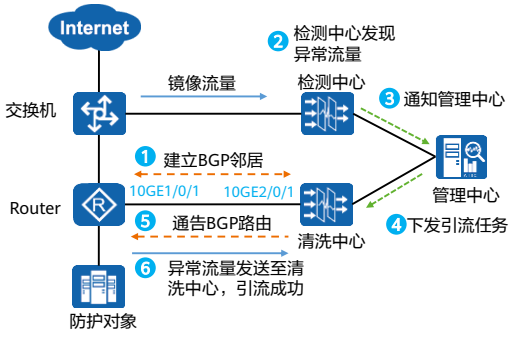
- 策略路由引流是指在核心交换机/路由器（旁挂清洗设备）上配置策略路由，将符合条件的流量通过策略路由的方式送到清洗设备。只需要在引流路由器上配置，无需在清洗设备上配置。
- 策略路由通常用于静态引流方式，采用该方式一般指定所牵引流量的入接口，流量由清洗设备清洗完成之后送回牵引设备，由路由表指导转发，并不会产生路由环路。



- 将Router的10GE1/0/1接口与清洗设备的10GE2/0/1接口之间建立引流通道，10GE2/0/1为清洗口；
- 在Router的Internet流量入接口10GE1/0/0上应用策略路由，使符合条件的报文不通过路由表转发，而是通过策略路由从接口10GE1/0/1转发到清洗设备进行清洗，从而实现对到达指定防护对象流量的强制引流。

BGP引流

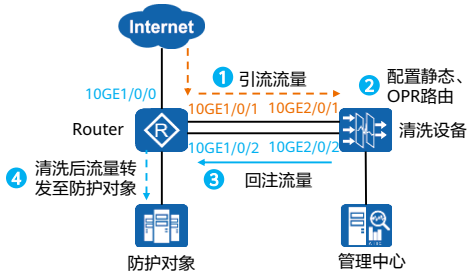
- BGP引流是一种常用的动态引流方式，需要事先在路由器和清洗设备上配置BGP协议，建立BGP邻居关系。管理中心监测到异常时，会向清洗设备下发引流任务，在清洗设备上生成一条32位OPR路由，通过BGP通告给路由设备，路由设备查找路由表中的BGP路由，将原本发往防护对象的流量发向清洗中心，实现引流。



1. 路由器与清洗中心事先通过互联线路建立BGP邻居关系；
2. 检测中心发现镜像流量中存在异常；
3. 检测中心将异常情况上报给管理中心；
4. 管理中心向清洗中心下发引流任务；
5. 清洗中心生成32位OPR路由，并通过BGP协议通告给路由器设备；
6. 路由器学习到此BGP路由，依据路由表将异常流量转发至清洗中心，完成引流。

静态路由、OPR路由回注

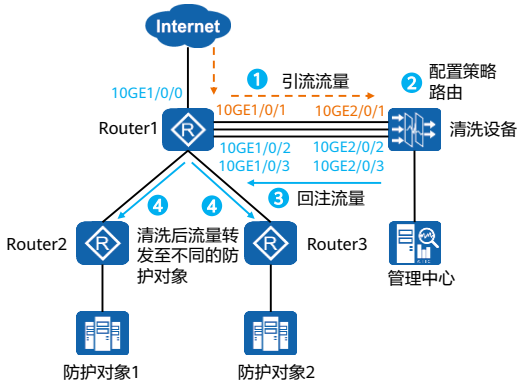
- 通过在清洗设备上配置静态路由或OPR路由，将清洗后的流量回注到网络设备（路由器、交换机等），网络设备根据自身的转发机制将清洗后的流量发送到防护对象。



1. 路由器使用引流技术（策略路由或BGP）将需要清洗的流量引流至清洗设备。
2. 清洗设备上配置静态路由或OPR路由，指向回注通道；
3. 清洗设备对流量进行清洗，然后把清洗后的流量通过回注通道发送至网络设备；
4. 网络设备将清洗后流量转发至防护对象，完成流量回注。

策略路由回注

- 通过在清洗设备上配置策略路由，可以将清洗后的流量回注到不同的路径，最后由网络设备转发至防护对象。

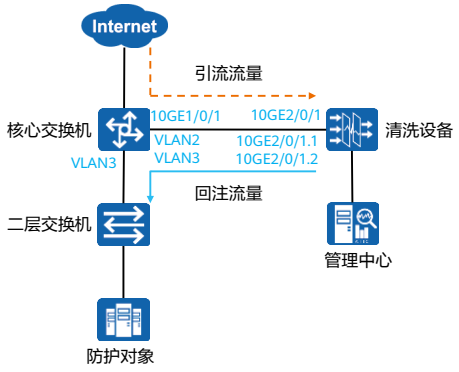


1. Router1为引流路由器，Router1的10GE1/0/1接口与清洗设备的10GE2/0/1接口之间的通道为引流通道，其余两个接口为回注通道。引流流量通过Router1的10GE1/0/1接口发送至清洗设备；
2. 在清洗设备的引流入接口10GE2/0/1上应用策略路由；
3. 清洗设备根据策略路由，将不同防护对象的流量回注到Router1不同的接口（10GE1/0/2和10GE1/0/3）；
4. 回注流量到达Router1后，Router1根据自身转发机制将流量分别发送至下行路由器Router2或Router3，流量最终到达不同的防护对象。

- 流量回注时，如果引流方式为BGP引流，为了避免路由环路，需要同时在Router1回注入接口10GE1/0/2和10GE1/0/3上应用策略路由，使得回注流量不会再发给清洗设备。

二层组网场景的引流和回注

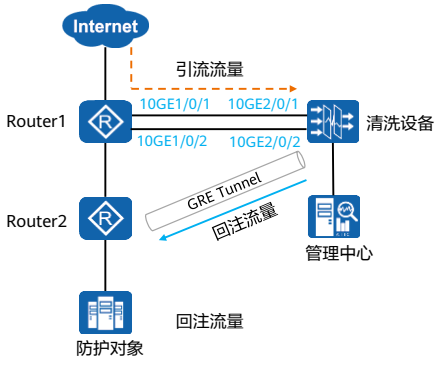
- 当核心交换机与防护对象之间只有二层转发设备，没有三层转发设备时，引流和回注的方式可以通过划分VLAN来解决。



- 核心交换机的10GE1/0/1接口与清洗设备的10GE2/0/1接口直连。交换机上创建两个VLAN，例如：VLAN2和VLAN3；
- 清洗设备的两个子接口10GE2/0/1.1和10GE2/0/1.2分别关联VLAN2和VLAN3，一个用作引流，一个用作回注；
- 引流流量在核心交换机通过VLAN2引导至清洗设备进行清洗。清洗完成后，清洗设备通过VLAN3将流量回注到防护对象。

GRE隧道场景的引流和回注

- 当引流策略采用BGP引流时，为了避免发生环路，可以通过GRE隧道将回注流量直接送到回注路由器（下图中的Router2），最后转发至防护对象。



- Router1为引流路由器。Router1的10GE1/0/1接口与清洗设备的10GE2/0/1接口之间的通道为引流通道；
- 流量通过Router1的10GE1/0/1接口引导至清洗设备的10GE2/0/1接口进行清洗；
- Router2为回注路由器。清洗设备与Router2之间建立GRE隧道，在清洗设备和Router2上分别创建Tunnel接口，并指定Tunnel的源地址和目的地址，Tunnel的源地址是发送报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址；源地址和目的地址之间必须路由可达；
- 清洗后的流量直接进入GRE隧道，送到Router2转发，最后送到防护对象。

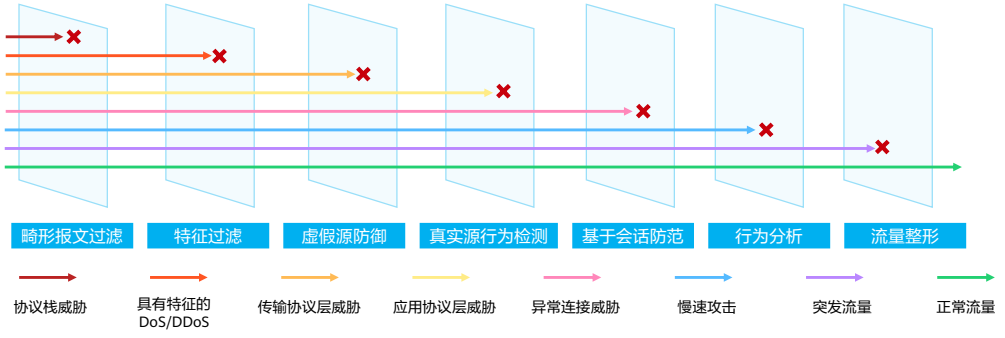
HUAWEI

- MPLS LSP/VPN方式部署较为复杂，并且需要设备支持MPLS，现网使用非常少，这里不详细展开。

目录

AntiDDoS清洗中心多层流量检测机制

- 华为AntiDDoS防护设备深入分析报文的每个字节，采用畸形报文过滤、特征过滤、虚假源防御、真实源行为检测、基于会话防范、行为分析和流量整形等精心打造的“七层净化”架构，可以有效识别流量型攻击、应用型攻击、扫描窥探型攻击和畸形包攻击等多种攻击类型，实现了对多种DoS/DDoS攻击流量精确清洗。

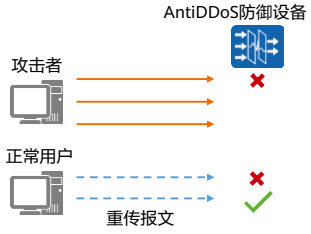


HUAWEI

- 第一步，畸形报文过滤：过滤利用协议栈漏洞的畸形报文攻击、特殊控制报文过滤；
- 第二步，特征过滤：首先基于报文内容特征的静态匹配过滤，主要针对没有连接状态的攻击进行防范，如UDP Flood、UDP类反射放大攻击（包括DNS反射放大，NTP反射放大等），ICMP Flood；然后基于黑白名单静态过滤；
- 第三步，虚假源防御：用于防范虚假源发起的SYN Flood；
- 第四步，真实源行为检测：用于防范虚假源或僵尸工具的DNS Query Flood、DNS Reply Flood、HTTP get/post Flood、HTTPS Flood、SIP Flood；
- 第五步，基于会话防范：基于会话检查可防范ACK Flood、FIN/RST Flood、TCP连接耗尽攻击、TCP异常会话攻击（socktress、重传攻击、空连接攻击）、DNS Cache Poisoning、SSL-DoS/SSL-DDoS、 HTTP slow headers/post attack；
- 第六步，行为分析：僵尸网络发起的攻击流量和用户访问业务流量行为上存在很大差异，用户访问业务流量具有突发性，访问资源比较分散；而僵尸网络攻击因属于僵尸工具攻击，流量最大特征是访问频率恒定，访问资源固定。可基于行为分析防范CC攻击、TCP慢速攻击、真实源发起的TCP Flood；
- 第七步，流量整形：经过上述层层过滤后，如果流量还很大，超过服务器的实际带宽，则采用流量整形使到达服务器的流量处于服务器的安全带宽范围内,包括源限速和目的IP限速。

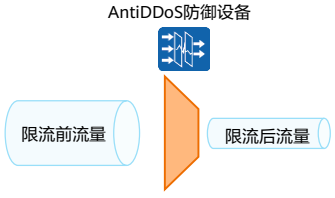
通用防御原理 (1)

首包丢弃



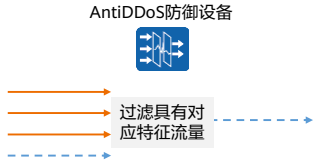
- 针对一个数据流（五元组信息不一致），收到的第一个报文不响应，直接丢弃，正常的业务报文会进行重传，而攻击者发送的大量随机报文并不会重传。

限流



- 针对一个数据流（五元组信息不一致）进行连接限制，可限制流量大小或者针对连接数进行限制。

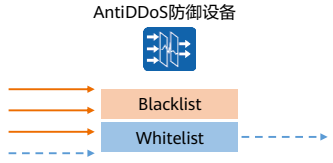
过滤器



- 在AntiDDoS设备上自定义报文的源IP、目的IP、协议、TTL等特征，将这些特征组合在一起作为过滤条件。后续对到达AntiDDoS设备的报文进行匹配，如果特征匹配，则表示命中过滤器，并对匹配的报文执行相应操作。

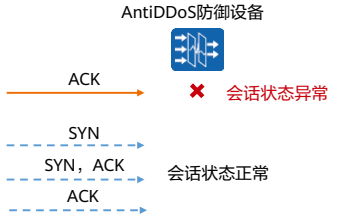
通用防御原理 (2)

黑白名单



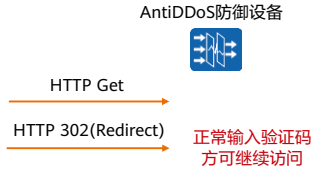
- 将一些不可信任的源IP地址加入黑名单，对此源发出的报文禁止通过；将信任的源IP地址加入到白名单，对此源发出的报文允许通过。

会话检查



- 检测会话状态（TCP、ICMP等），根据会话状态判断报文是否合法，如并未存在TCP SYN报文，直接收到一个全新五元组的ACK报文，不符合会话状态，该报文将被丢弃。

验证



- 针对HTTP类业务，进行页面重定向，在重定向页面中需输入验证码方可继续访问，可过滤掉非正常用户的HTTP报文。

防御功能总览

IP防御

- IP Flood限流
- IP Flood防御

TCP防御

- TCP异常报文防御
- SYN Flood防御
- SYN-ACK Flood防御
- ACK Flood防御
- FIN/RST Flood防御
- TCP连接攻击防御
- TCP限流

UDP防御

- UDP异常报文防御
- UDP Flood防御
- UDP限流

ICMP防御

- ICMP限流

DNS防御

- DNS异常报文防御
- DNS Query Flood防御
- DNS Reply Flood防御
- DNS限速

SIP防御

- SIP Flood防御
- SIP限速

HTTP防御

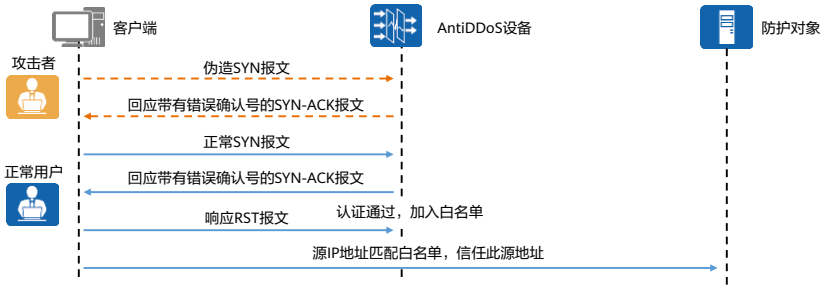
- HTTP Flood防御
- HTTP 异常连接防御

HTTPS防御

- TLS加密攻击防御
- TLS会话攻击防御

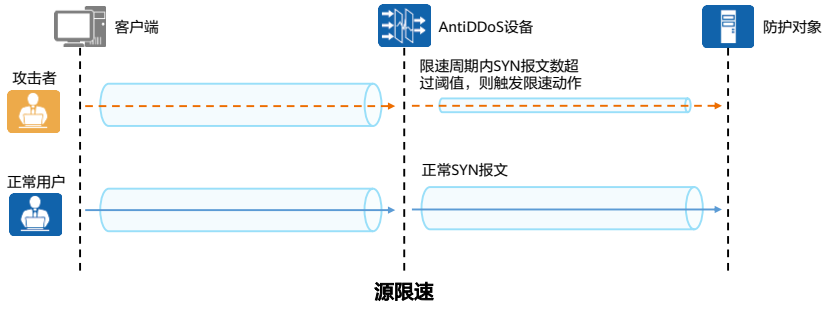
TCP防御原理 - SYN Flood (1)

- 源认证：清洗设备接收到SYN报文，发送SYN-ACK探测报文到SYN报文中的源IP地址。清洗设备通过源IP地址对探测报文的响应报文校验源是否合法，以防止虚假源攻击。
  - 如果客户端是虚假源，则不会对错误的SYN-ACK报文进行回应，认证失败，AntiDDoS设备丢弃后续此源地址的SYN报文；
  - 如果客户端是真实源，则会响应一个RST报文，认证通过， AntiDDoS设备把此源地址加入白名单，并放行后续的SYN报文。



TCP防御原理 - SYN Flood (2)

- 源IP监控：源IP加入白名单之后将继续对真实源IP进行统计分析，对异常的源IP进行限速，以防止真实源发起攻击。
  - 源限速：限速周期内SYN报文数超过阈值，则触发限速动作。
  - 异常源阻断：连续检测周期内，异常次数超过阈值，则将源IP加入动态黑名单。

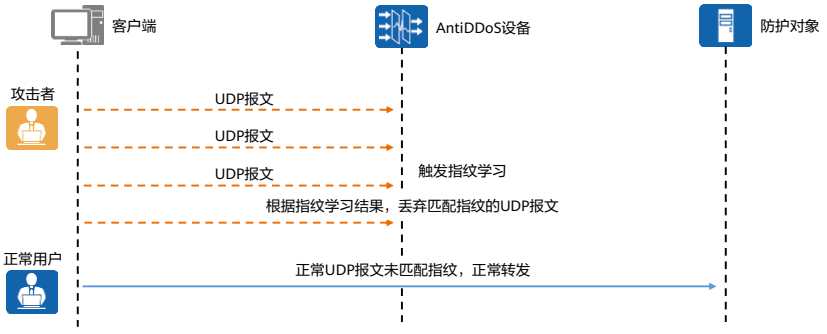


HUAWEI

- 异常源阻断：
  - 统计源地址SYN/(ACK+SYN) 报文比例，作为检测周期内异常判定条件。
  - 检测周期内SYN报文数超阈值视为一次异常。
  - 连续检测周期内，异常次数超过阈值，则将源IP加入动态黑名单。

UDP防御原理 - UDP Flood (1)

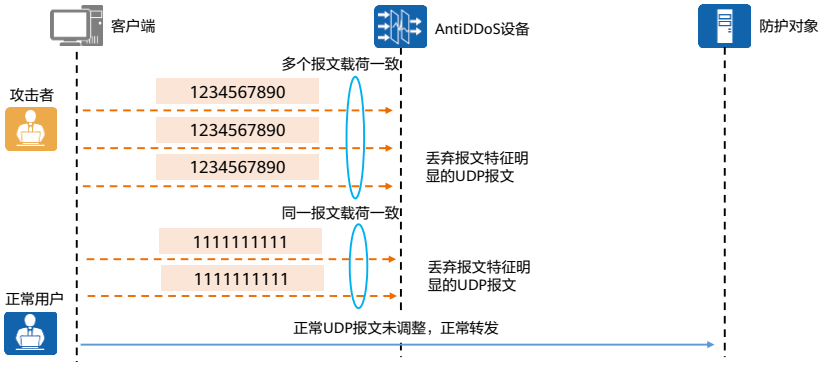
- 指纹学习：当UDP流量超过阈值时，会触发指纹学习。指纹由清洗设备动态学习生成，将攻击报文的一段显著特征学习为指纹后，匹配指纹的报文会被丢弃。



- 水印：检查报文携带的水印字段，丢弃不符合水印算法的报文。水印算法配置内容：关键字1、关键字2、目的端口。

UDP防御原理 - UDP Flood (2)

- 载荷检查：当UDP流量超过阈值时，会触发载荷检查，如果UDP报文数据段内容完全一样，则会被认为是攻击而丢弃报文。



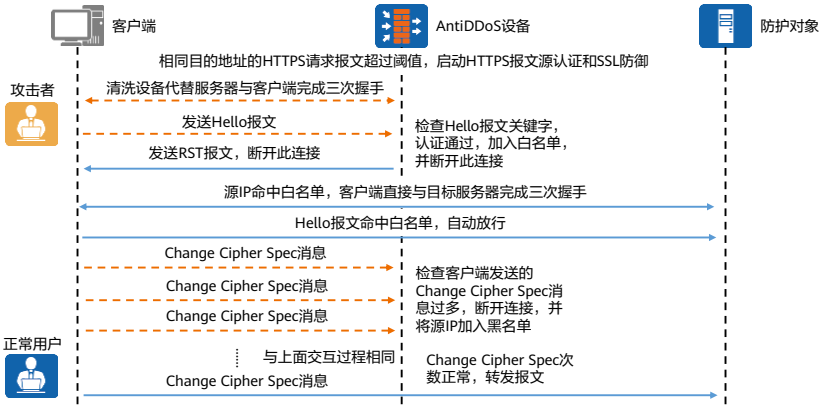
UDP防御原理 - UDP Flood (3)

- 其他防御原理：
  - 会话行为检测：基于会话检查拦截恶意流量。后续报文有效期超过阈值“报文间隔（秒）”，触发拦截动作。
  - 关联防御：检查UDP会话中的“前序报文”和“后序报文”是否满足的匹配规则。
    - 若不满足匹配规则，则直接丢弃UDP报文。
    - 若满足匹配规则，则将UDP报文的源IP加入白名单。
    - 前序报文匹配规则内容：目的IP、协议、目的端口、报文长度、载荷。
    - 后序报文匹配规则内容：目的IP、目的端口、报文长度、载荷。
  - 水印：检查报文携带的水印字段，丢弃不符合水印字段的报文。
    - 水印字段配置内容： 关键字1、关键字2、目的端口。

- 关联防御需和会话检测配合使用，且后续报文间隔配置时间为1-2秒；针对独立的游戏防护对象开启该功能。

HTTPS防御原理 - SSL

- 清洗设备基于目的地址对HTTPS请求报文速率进行统计，当HTTPS请求速率超过阈值时，启动源认证防御和SSL防御。



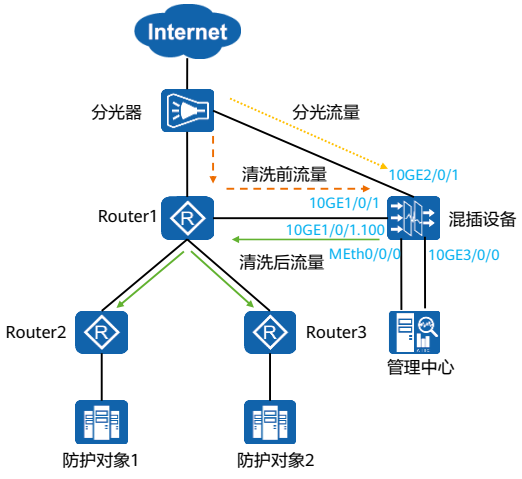
HUAWEI

- SSL防御：在检查周期内，如果某个源IP地址到目的IP地址的协商次数超过最大值，则将此会话标记为异常会话，在异常会话检查周期内，如果异常会话数超过最大值时，判定该源IP地址异常，将该源IP地址加入黑名单。

目录

配置AntiDDoS1900旁路部署（混插设备）

- 需求描述：
  - 混插设备旁路部署在网络节点处，对到达防护对象的下行流量进行检测和清洗。混插设备先通过分光方式，将链路中的流量复制到检测口，对流量进行实时检测，当检测到异常后通告给管理中心；管理中心向清洗业务板下发引流任务，流量被引流至清洗口进行清洗，清洗完成后再将正常流量从回注口回注到原链路，继续转发。
  - 清洗设备的接口10GE2/0/1用于接收分光流量，从此接口达到的流量送到检测业务板进行统计分析；接口10GE1/0/1用于接收引流流量，清洗业务板对接口接收的流量进行清洗防御，清洗完成后，通过子接口10GE1/0/1.100回注到Router，继续转发。



HUAWEI

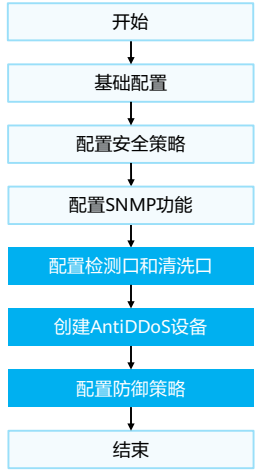
- 注意：仅部分款型支持混插设备。

业务规划

设备名称	接口	IP地址	说明
混插设备	10GE2/0/1	/	检测口： 接收链路中的分光流量，无需配置IP地址。
	10GE1/0/1	10.1.2.1/24	清洗口： 即引流流量入口，混插设备对从该口进入的流量应用各种防御策略，对流量进行分析和清洗。
	10GE1/0/1.100	10.1.3.1/24	回注口： 清洗后的正常流量通过此接口回注到原链路。
	10GE3/0/0	10.1.5.1/24	与管理中心通信的日志接口。
	MEth0/0/0	10.1.5.3/24	与管理中心通信的管理接口。
管理中心	/	10.1.5.2/24	管理中心IP地址。

配置思路

- 配置思路：
  - 登录混插设备，升级软件版本；
  - 加载License；
  - 指定检测业务CPU；
  - 更改缺省用户名和密码，并配置Stelnet功能；
  - 配置接口IP地址，接口加入安全区域，并打开域间缺省包过滤；
  - 配置SNMP功能使管理中心可以获取混插设备的状态；
  - 配置检测口和清洗口，并在检测口和清洗口开启流量统计功能；
  - 登录管理中心，创建AntiDDoS设备，添加防护对象；
  - 配置相应的防御策略。



- 本举例重点介绍混插设备和管理中心部署在网络中时的基本配置过程，对于后续的引流回注配置以及相关防御策略配置不做详细介绍。

混插设备配置 (1)

- 指定检测业务CPU，重启业务CPU，使其生效。

```
<AntiDDoS1900> system-view
[AntiDDoS1900] firewall ddos detect-spu slot 4 cpu 1
[AntiDDoS1900] quit
<AntiDDoS1900> save
<AntiDDoS1900> reset cpu slot 4 1
```

- 配置SNMP功能。

```
[AntiDDoS1900] snmp-agent
[AntiDDoS1900] snmp-agent sys-info version v3
[AntiDDoS1900] snmp-agent mib-view included ddos iso
[AntiDDoS1900] snmp-agent group v3 atic privacy read-view ddos write-view ddos notify-view ddos
[AntiDDoS1900] snmp-agent group v3 atic privacy
[AntiDDoS1900] snmp-agent usm-user v3 atic
[AntiDDoS1900] snmp-agent usm-user v3 atic group atic
[AntiDDoS1900] snmp-agent usm-user v3 atic authentication-mode sha2-512
[AntiDDoS1900] snmp-agent usm-user v3 atic privacy-mode aes256
[AntiDDoS1900] snmp-agent protocol source-interface MEth0/0/0
```


- SNMPv2c方式有一定安全风险，如果对安全性要求很高，建议使用SNMPv3方式。本举例以SNMPv3为例介绍配置步骤。

混插设备配置 (2)

- 配置检测口。

```
[AntiDDoS1900] interface 10GE 2/0/1
[AntiDDoS1900-10GE2/0/1] anti-ddos detect enable
[AntiDDoS1900-10GE2/0/1] anti-ddos flow-statistic enable
[AntiDDoS1900-10GE2/0/1] quit
```

- 配置清洗口。

```
[AntiDDoS1900] interface 10GE 1/0/1
[AntiDDoS1900-10GE1/0/1] anti-ddos clean enable
[AntiDDoS1900-10GE1/0/1] anti-ddos flow-statistic enable
[AntiDDoS1900-10GE1/0/1] quit
```

管理中心配置 (1)

- 添加AntiDDoS设备。
  - 选择“设备管理 > 设备 > 设备”。单击“自动发现”，添加AntiDDoS设备，添加SNMP和Stelnet参数。

HUAWEI

管理中心配置 (2)

- 防护对象即需要保护的设备。
  - 选择“攻击防御 > 策略配置 > 防护对象”。单击“创建”，新建防护对象，关联AntiDDoS设备，添加防护对象地址。

管理中心配置 (3)

- 完成基本策略的配置后，防护对象的各关联设备上会分别自动生成一条基本防御策略，需要根据现网流量配置该防御策略。
  - 选择“AntiDDoS攻击防御 > 攻击防御 > 防护对象”，单击对应防护对象的 ，单击操作列的“编辑”，可查看该防护对象的基线学习和防御策略的信息，并对防御策略进行修改。
  - 配置防御策略后，需要将该配置部署到关联设备上才能生效，选中防护对象前的复选框，单击“部署”，即可使该策略生效。

思考题

1. （单选题）以下不属于畸形报文攻击的是哪一项？（　　）

   A. Teardrop攻击

   B. Smurf攻击

   C. Land攻击

   D. Tracert攻击

2. （判断题）Ping of Death攻击与ICMP Flood攻击都是利用ICMP报文发起的攻击，其区别在于前者是通过伪造畸形ICMP报文实现攻击，而后者通过DDoS方式实现攻击。（　　）

   A. 正确

   B. 错误

1. D
2. A

本章总结

- 本章介绍了防火墙的攻击防范技术，包括传统的单包攻击和DDoS攻击。单包攻击主要包括扫描类攻击、畸形报文类攻击和特殊报文类攻击； DDoS攻击主要包括包括SYN Flood、HTTP Flood、HTTPS Flood、DNS Request Flood、DNS Reply Flood、SIP Flood、UDP Flood、ICMP Flood等。
- 本章介绍了AntiDDoS解决方案、组网方式、防御原理和配置。
- 通过本章的学习，您将能够描述常见的网络攻击原理和防范原理，并熟悉相关配置。

缩略语表 (1)

缩略语	英文全称	解释
ATIC	Abnormal Traffic Inspection & Control System	异常流量监管系统
B/S	Browser/Server	浏览器/服务器架构
BGP	Border Gateway Protocol	边界网关协议
DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name Server	域名服务器
DoS	Denial of Service	拒绝服务
GRE	Generic Routing Encapsulation	通用路由封装协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure	超文本传输安全协议
ICMP	Internet Control Message Protocol	互联网控制报文协议

缩略语表 (2)

缩略语	英文全称	解释
OPR	Open Programming Route	开放可编程路由
SIP	Session Initiation Protocol	会话发起协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SQL	Structured Query Language	结构化查询语言
SSL	Secure Sockets Layer	安全套接字层
SYN	Synchronous	同步序号
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全性协议
TTL	Time To Live	生存时间
UDP	User Datagram Protocol	用户数据报协议

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.

漏洞防御与渗透测试

HUAWEI

前言

- 现代社会，企业网络都面临着各类安全威胁，如网站攻击、拖库等，作为网络安全工程师，需要了解常见的网络威胁，以便能合理地防范威胁，在运维时能及时预防、识别以及阻断威胁。
- 漏洞是造成安全威胁的主要原因之一，本章节以漏洞为例，介绍如何在安全方案部署和安全运维时防范安全威胁。

目标

- 学完本课程后，您将能够：
  - 描述网络攻击链
  - 描述漏洞的危害性
  - 掌握漏洞防御措施
  - 阐明IPS及WAF的工作原理
  - 描述渗透测试工作流程

目录

网络攻击链

- 著名军工企业洛克希德·马丁公司（Lockheed Martin）提出了“网络攻击链”（Cyber Kill Chain）的概念，将网络攻击的生命周期分为了七个阶段。
- 在网络攻击链中，漏洞是攻击者侵入网络的入口，当网络存在漏洞，则意味着信息系统存在安全隐患，面临安全风险。

侦查追踪	武器构建	载荷投递	漏洞利用	安装植入	持续控制	目标达成
研究目标，获取目标信息。	制作针对网络漏洞的武器，即载荷。	将载荷通过电子邮件等方式投递到目标环境。	载荷被触发，利用漏洞向目标主机发起攻击。	在目标主机中安装木马等工具，获得访问权限。	攻击者连接并操纵目标主机，获得持续控制权限。	发动规模攻击、破坏信息系统或窃取数据。

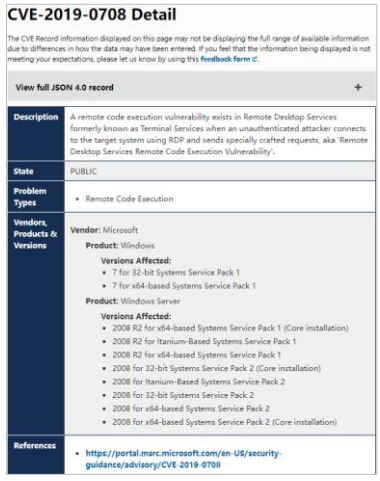
漏洞概述

- 漏洞指的是信息系统中软件、硬件或通信协议中存在的缺陷或不适当的配置，从而可以使攻击者在未授权的状态下访问或者破坏系统，导致信息系统面临安全风险。
- 漏洞通常代表了计算机系统安全方面的缺陷，使得系统或其应用数据的保密性、完整性、可用性和访问控制等方面面临威胁。

- 在《GB/T 25069-2022信息安全技术术语》中，将漏洞（即脆弱性）定义为可能被一个或多个威胁利用的资产或控制的弱点。

漏洞编号

- 当漏洞被发现并被厂商公布时，同时会发布漏洞的编号来唯一标识该漏洞。漏洞被收录在各机构的漏洞库中。
- CVE（Common Vulnerabilities and Exposures）是一个业界公开披露的漏洞库。CVE漏洞编号的表示方法如下：
  - CVE为每一个漏洞分配唯一的漏洞编号，格式为“CVE-年份-编号”，如CVE-2019-0708。
  - 每个CVE漏洞主要包含以下信息：
    - 描述：漏洞的来源、攻击方式等简要描述；
    - 参考：漏洞的相关参考信息链接，如供应商的漏洞公告、建议等；
    - CNA：发布此漏洞的CNA组织；
    - 发布日期：此漏洞的发布日期。



- CVE的发布主体是CVE编号机构（CVE Numbering Authority，CNA），当前大约有100个CNA，由来自世界各地的IT供应商、安全公司和安全研究组织组成。任何机构或个人都可以向CNA提交漏洞报告，CNA中的安全厂商往往也会鼓励人们寻找漏洞，以增强产品的安全性。
- 不是所有漏洞都能被录入CVE，CNA主要根据如下规则判定是否为漏洞分配CVE编号：
  - 漏洞可独立修复，与其他漏洞没有耦合；
  - 软件或硬件供应商承认此漏洞的存在或有书面公告；
  - 漏洞只影响一个代码库，若影响多个产品，则为每个产品中的漏洞独立分配CVE编号。
- CVE漏洞信息由CVE组织机构的网站呈现（http://cve.mitre.org/）。
- 其他公共网络安全漏洞库：
  - CNCVE: China National Common Vulnerabilities and Exposures，中国国家通用漏洞披露，https://www.cert.org.cn/；
  - NVD：National Vulnerability Database，美国国家信息安全漏洞库，https://nvd.nist.gov/；
  - CNVD：China National Vulnerability Database，国家信息安全漏洞共享平台，https://www.cnvd.org.cn/；
  - CNNVD：China National Vulnerability Database of Information Security，

国家信息安全漏洞库，http://www.cnnvd.org.cn/。

漏洞评估

- 通用漏洞评估系统（Common Vulnerability Scoring System，CVSS）是广泛应用的漏洞评分开放标准。
- CVSS的分值代表漏洞的严重程度，分值范围为0.0到10.0，数字越大漏洞的严重程度越高。

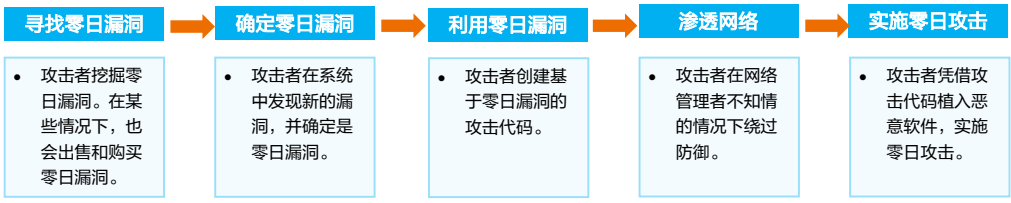
等级	分值
严重（Critical）	9.0-10.0
高（High）	7.0-8.9
中（Medium）	4.0-6.9
低（Low）	0-3.9

- CVSS 采用了模块化评分体系，包含三个部分：
  - 基本维度（Base Metric Group）：核心特性不随时间和用户环境改变，如可利用性、影响对象；
  - 时间维度（Temporal Metric Group）：随着时间推移而改变的特性，如漏洞攻击代码成熟度；
  - 环境维度（Environmental Metric Group）：漏洞对其所在机构或相关机构造成的影响，如机密性影响。

- CVSS由事件响应与安全组论坛（Forum of Incident Response and Security Teams，FIRST）维护，评分标准公布在https://www.first.org/cvss/。
- CVE与CVSS的关系：
  - CVE单纯是漏洞的字典库，CVE列表中不包含CVSS分值，需要使用其他漏洞管理系统（例如https://www.cvedetails.com/）查阅CVSS分值。
  - IT人员结合CVE信息和CVSS确定漏洞解决优先级。
- 漏洞类型：
  - 严重漏洞：可获取服务器权限，造成严重信息泄露，影响范围大；
  - 高危漏洞：需要用户交互才可利用的漏洞，造成敏感信息泄露，影响范围较大；
  - 中危漏洞：造成中度影响的信息泄露漏洞或逻辑漏洞；
  - 低危漏洞：造成轻微影响的信息泄露漏洞或逻辑漏洞。

零日漏洞

- 零日漏洞：也可以称为零时差漏洞，通常是指还没有对应补丁的漏洞。
- 零日攻击：利用零日漏洞对系统或软件应用发动的网络攻击。
- 零日攻击的目标：
  - 高价值的目标：金融机构、医疗机构、国家机构或军队机构等。
  - 影响范围大的目标：浏览器、操作系统、常用应用软件等。



零日漏洞转化为零日攻击的过程

HUAWEI

- 零日漏洞：零日漏洞中的“零日”得名于漏洞被公开后，补丁未出现的天数。漏洞被公开当天，一般来讲都不会及时推出补丁，所以称为零日漏洞。如果N日后仍然没有补丁，则称为N日漏洞。实际上，“零日”现在已经不再局限于漏洞被公开的时间长短。所谓“零日”不一定是真的刚刚发现，黑客完全有可能在很久之前发现了漏洞，但就是没有公开。那么对于外界来说，漏洞公开的那一刻才能称为零日漏洞。所以，“零日”往往可以理解为“软件供应商和公众未知”，但是“黑客或漏洞交易者已知”。

攻击领域

- 在网络安全领域，攻击和防御是最常见的两个话题，攻击是矛，防御是盾，此消彼长。随着网络的发展，新的攻击手段层出不穷，业界中，颇具代表性的CAPEC（The Common Attack Pattern Enumeration and Classification，通用攻击模式枚举和分类）将攻击分为以下六个领域：

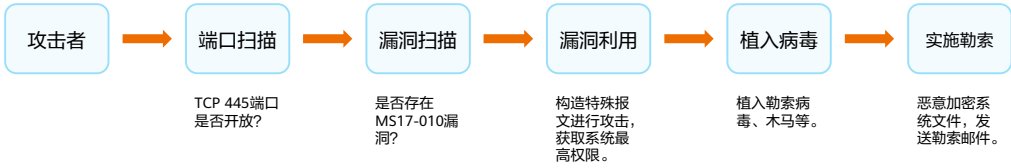
软件	硬件	通信	供应链	社会工程学	物理安全
攻击目标的软件系统，常见的攻击方式有：缓冲区溢出攻击、命令注入、代码注入、SQL注入、暴力破解、身份欺骗等。	攻击目标的硬件系统，如：基础设施操纵、资源操纵、硬件故障注入、恶意逻辑插入、功能滥用等。	嗅探监听通信流量，窃取或篡改通信信息，如：嗅探攻击、中间人攻击、身份欺骗攻击、通信信道操纵、协议操纵等。	通过操纵计算机软硬件系统及服务破坏供应链生命周期，如：非法植入恶意代码、软件完整性攻击等。	利用人的弱点、行为特征、心理特征等实施攻击，如：钓鱼攻击、密码破解等。	直接攻击物理设施、设备等，如：物理盗窃、绕过物理安全等。

- 基于漏洞的攻击方式有很多，常见的有：
  - 口令破解：利用常见口令、薄弱口令、通用口令等对常见应用进行尝试登录，登录成功或可直接获取服务器管理权限。
  - 溢出攻击：利用操作系统或常用软件存在的漏洞，攻击成功可能导致主机被远程控制、安装恶意软件、宕机、重启等。
  - 权限提升：获取系统更高权限，进行下一步攻击，如发送转账指令。
  - 病毒入侵：植入病毒，或进行勒索，或进行权限控制，或进一步扩散病毒影响其他主机系统。
  - 破坏系统：破坏系统可用性。如利用微软MS14-064漏洞可导致系统蓝屏。
  - 拒绝服务：耗尽系统资源，使目标主机无法对外提供服务。
  - 窃取数据：获取机密信息，勒索或转卖信息。

目录

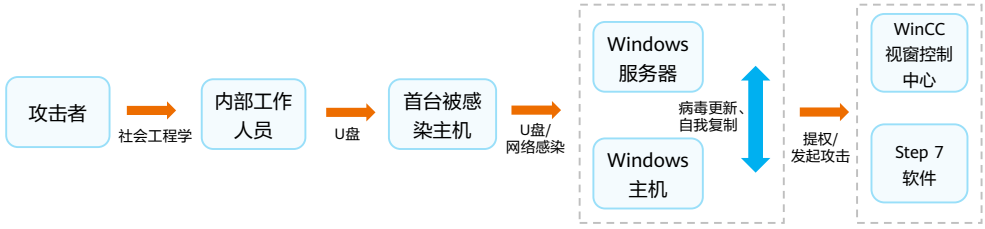
“永恒之蓝”漏洞

- “永恒之蓝”漏洞是Windows操作系统的一种漏洞，漏洞编号为MS17-010，其利用Windows系统中SMB协议的漏洞发起攻击，获取系统最高权限，进而在主机中植入勒索软件、远程控制木马、虚拟货币挖矿程序等恶意代码。
- “永恒之蓝”的攻击过程如下：



“震网”病毒

- “震网”病毒又名“Stuxnet”病毒，是一个席卷全球工业界的病毒，也是已知的第一个以关键工业基础设施为攻击目标的蠕虫病毒。
- “震网”病毒传播能力强，隐蔽性高，破坏性大，其攻击过程如下：



HUAWEI

- 震网病毒攻击过程如下：
  - 攻击者收集目标网络的信息，包括组织架构与工作人员信息，利用社会工程学突破工作人员防线；
  - 使用U盘的快捷方式文件解析漏洞(MS10-046)感染第一台受害主机；
  - 利用U盘的快捷方式文件解析漏洞(MS10-046)和打印机后台程序服务漏洞(MS10-061)传播病毒，感染Windows主机和共享打印机的服务器；
  - 主机之间利用RPC远程执行漏洞(MS08-067)更新病毒版本；
  - Windows主机感染后，尝试查找WinCC视窗控制中心或西门子Step 7软件；
  - 若发现WinCC视窗控制中心或西门子Step 7软件，则尝试利用DLL加载缺陷与系统自动密码保存机制篡改WinCC或Step 7软件；
  - 若发现无权篡改，则使用内核模式驱动程序权限提升漏洞(MS10-073)和任务计划程序权限提升漏洞(MS10-092)提升权限，再次篡改西门子控制软件；
  - 控制软件被更改后，离心机工作频率被提升至临界值，导致过热报废。
- 在该攻击事件中，使用的快捷方式文件解析漏洞(MS10-046)、打印机后台程序服务漏洞(MS10-061)、内核模式驱动程序权限提升漏洞(MS10-073)和任务计划程序权限提升漏洞(MSIO-092)皆为零日漏洞。

SQL注入 (1)

- SQL注入指的是攻击者利用Web应用对用户输入数据过滤不够严格的弱点，构造特殊的字符串作为输入，欺骗数据库服务器执行未授权的恶意查询，最终导致数据信息泄露。
- SQL注入的攻击过程如下：

SQL注入 (2)

- SQL注入获取Web应用管理员账号的示例如下：
  - 攻击者在登录界面输入用户名1‘ or 1=1 #，在Web网站执行则会变成如下的SQL语句：

    select * from database.users where title like ‘%1’or 1=1 # %

  - 符号“#”会将随后的代码注释掉，where条件就变成title like ‘%1’ or 1=1，是一个永真条件，此时SQL语句返回所有的用户名。

HUAWEI

- 正文仅展示SQL注入获取管理员账号及口令的部分过程。

目录

Linux系统加固

- 系统加固也称主机加固，指的是通过一系列安全措施提高操作系统的安全性，降低被攻击的风险。
- Linux操作系统主要从以下几个方面来加固：

账户安全设置	• 锁定或清除多余账号 • 设置口令策略，如密码复杂度	• 设置口令过期时间 • 设置“连续登陆失败锁定”功能
系统安全设置	• 设置访问控制策略，限制远程登录 • 禁止root用户远程登录	• 修改账号自动注销时间 • 修改远程登录监听端口
服务启动管理	• 关闭不必要的服务 • 使用iptables设置访问规则	• 使用具备加密功能的服务
日志安全设置	• 配置用户登录日志 • 配置用户操作日志	• 配置系统安全日志

Windows系统加固

- Windows操作系统主要从以下几个方面来加固：

安全配置	• 取消默认共享 • 开启审核策略，记录操作日志	• 修改默认TTL值，防范探测攻击 • 关闭不必要的服务
账户安全设置	• 限制用户数量 • 开启帐户锁定策略	• 开启密码策略 • 拒绝远程访问
用户权限设置	• 遵循最小授权原则 • 不同级别用户设置不同权限	• 定期审核账号权限
安全中心设置	• 病毒和威胁防护 • 防火墙和网络保护	• 账户保护、应用和浏览器控制 • 设备安全性、设备性能和运行状况

补丁管理

- 网络安全运维工程师应根据需要及时进行补丁升级，保障系统安全。

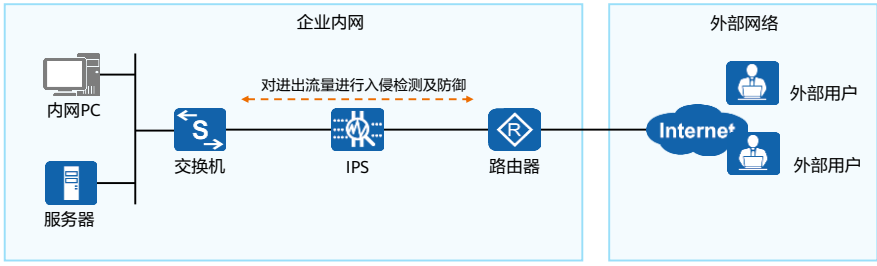
通用补丁管理	• 各个漏洞组织（如CVE、CNVD、CNNVD）在发布漏洞时，通常会给出对应厂商的修复建议、补丁，可进行参考。
Linux补丁管理	• Linux为开源操作系统，不同的发行版（如RedHat、Ubuntu、SUSE等）均会定期发布系统补丁，可根据官网补丁进行系统更新。
Windows补丁管理	• Microsoft在每个月的第二个星期二为其操作系统和应用程序发布补丁，通常称为Patch Tuesday。此外，微软会发布安全公告来解决操作系统和应用程序中的关键问题。
应用补丁管理	• 根据应用程序官方发布的补丁进行更新升级。 • 有必要时，可以更新软件的版本，来提高安全性。

- 网络安全工程师可以借助终端安全工具下发补丁，也可以通过邮件等方式通知内部用户加载补丁。

目录

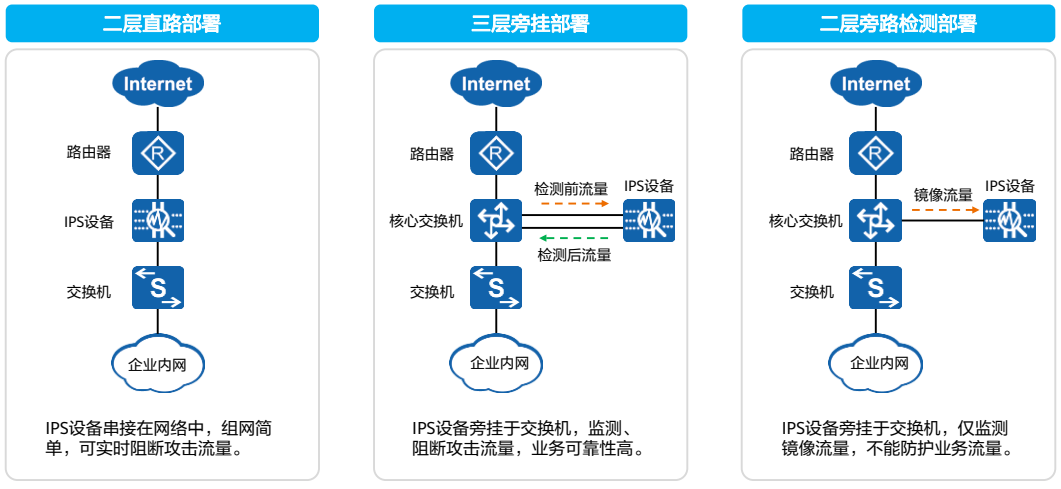
入侵防御系统概述

- 入侵防御系统（Intrusion Prevention System，IPS）是一种基于攻击特征库对网络流量进行入侵检测、防御的系统。它可以是软件系统，也可以是硬件设备。
- 华为IPS系列产品是一种网络安全硬件设备，通常部署在企业内网，对进出流量进行检测，抵御多种漏洞攻击。



- 当外网用户访问企业内网时，IPS设备对访问流量进行检测。如果发现入侵行为则阻断连接；反之则放行。
- 当内网用户访问外网时，如果访问的网页或服务器包含恶意代码，IPS设备将阻断连接；反之则放行。
- 入侵防御的主要优势如下：
  - 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，还可以防止发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。

IPS设备部署方式

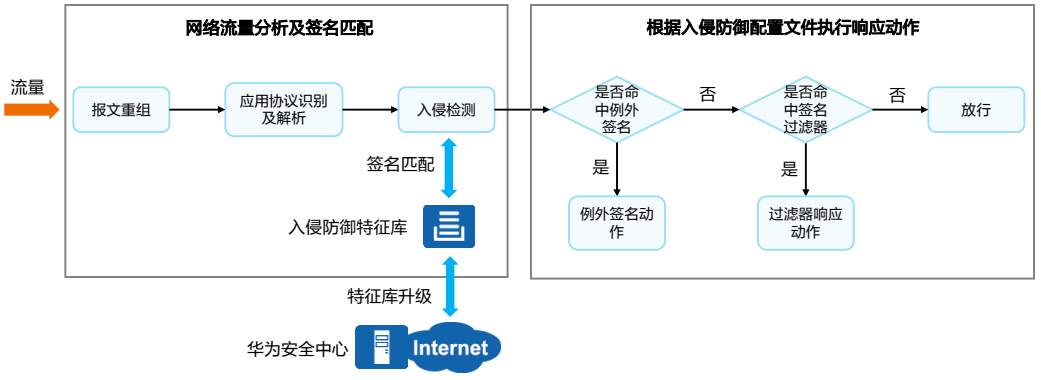


HUAWEI

- 二层直路部署：
  - IPS使用固定二层接口对接入网络，上下行设备不用做任何配置调整。如果有多条不同链路需要接入，可以使用多个接口对。
  - 当需要对攻击实时阻断时选择此种部署方式。
- 三层旁挂部署：
  - IPS使用三层接口旁挂在交换机上，交换机将流量转发至IPS，IPS检测后再转发回交换机。
  - 当IPS故障时，流量可以直接通过交换机转发，业务可靠性高。
- 二层旁路检测部署：
  - IPS接收交换机镜像或分光器分光流量，分析攻击事件并记录日志。旁路部署方式IPS不参与流量转发。
  - 这种部署方式不阻断攻击，适用于安全事件审计和攻击行为分析场景。

入侵防御处理流程

- 入侵防御处理流程主要包括攻击检测、攻击响应两部分。



- 报文重组：收到流量后，设备首先进行IP分片报文重组以及TCP流重组，确保应用层数据的连续性，有效检测出逃避入侵防御检测的攻击行为。
- 应用协议识别和解析：设备根据报文内容识别出具体的应用层协议，并对协议进行深度解析从而提取报文特征。与传统只能根据IP地址和端口识别协议相比，大大提高了对应用层攻击行为的检测率。
- 签名匹配：将解析后的报文特征与入侵防御签名进行匹配，如果匹配了签名，则进行响应处理。设备支持定期从华为安全中心（isecurity.huawei.com）下载最新的入侵防御特征库，及时有效防御网络入侵。
- 响应处理：报文匹配了签名后，是否进行响应处理、如何进行响应处理（告警还是阻断）由入侵防御配置文件文件决定。入侵防御配置文件主要包含例外签名、签名过滤器两部分。
  - 判断匹配的签名是否属于例外签名，如果属于例外签名，执行例外签名的响应动作，否则进入下一步处理。
  - 判断匹配的签名是否属于签名过滤器筛选出的签名，如果属于则执行签名过滤器的响应动作，否则直接放行报文。

入侵防御签名

- 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网络攻击。
- 如果某个数据流匹配了某个签名中的特征项时，设备会按照签名的动作来处理数据流。
- 入侵防御签名分为预定义签名和自定义签名两种类型。

IPS设备预置的入侵防御特征库（签名库），包含针对各种已知入侵行为的签名信息，这些签名称为预定义签名。

自定义签名是指管理员根据网络流量特点对特定的入侵行为自行定义的签名。通常用于防御新型的入侵攻击或阻断特定行为的数据报文。

- 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。
- 自定义签名创建后，系统会自动对自定义规则的合法性和正则表达式进行检查，避免低效签名浪费系统资源。

预定义签名

- 在使用预定义签名时，建议定期从华为安全中心（isecurity.huawei.com）下载最新的入侵防御特征库，使设备持续拥有最新的入侵防御能力。
- 预定义签名的示例如下所示。

HUAWEI

- 基本信息：预定义签名的基本描述信息。
  - ID：预定义签名的ID。
  - 状态：预定义签名在特征库中的状态。设备只能检测处于启用状态的签名对应的攻击。
  - 对象：攻击行为所针对目标的角色，包括：服务端和客户端。
  - 严重性：用来描述攻击后果的严重性，分为高、中、低、提示四种。
  - 操作系统：描述网络威胁所攻击的操作系统。
  - 协议：预定义签名的协议，用来描述网络威胁使用的协议类型。
  - 威胁类别：描述网络威胁的类别。包括木马、蠕虫、注入攻击、溢出攻击等。
  - 动作：预定义签名的缺省动作。
    - 放行：当报文命中此签名时，允许通过，且不会记录日志；
    - 告警：当报文命中此签名时，允许通过，但会记录日志；
    - 阻断：当报文命中此签名时，丢弃报文，并记录日志。
  - 应用程序：描述网络威胁使用的应用程序。
- 参考信息：其他参考信息，包括漏洞在权威漏洞机构的编号及漏洞介绍的网站信息。

入侵防御配置文件

- 入侵防御配置文件是入侵防御功能的核心，用于决定设备对哪些攻击进行防御，以及如何防御。
- 入侵防御配置文件分为签名过滤器和例外签名两个组成部分。

签名过滤器

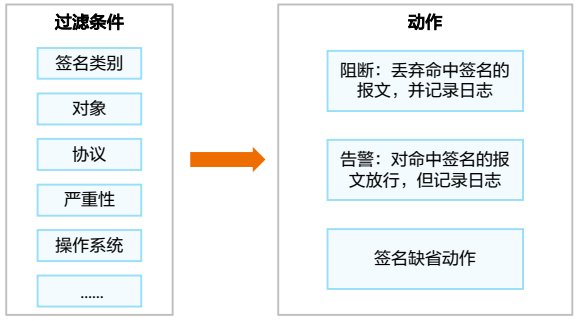
签名过滤器是一系列过滤签名的条件集合。只有符合所有过滤条件的签名才能够匹配签名过滤器。

例外签名

例外签名是指独立于签名过滤器之外，优先被处理的签名，可以单独配置处理动作。

签名过滤器

- 入侵防御特征库中包含针对各种攻击行为的海量签名信息，但实际网络环境中不需要使用所有的签名。此时需要配置签名过滤器，IPS设备只防御签名过滤器筛选出的签名。



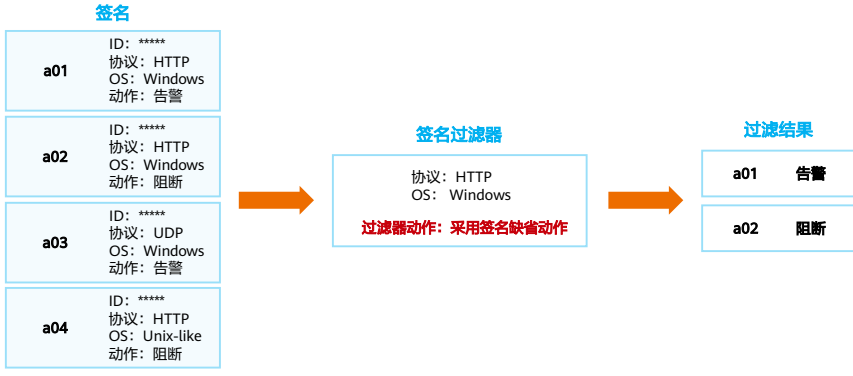
签名过滤器

HUAWEI

- 配置签名过滤器需要对网络和业务非常了解，有一定难度。IPS设备提供满足常见场景的缺省入侵防御配置文件。
- 需要注意的是，同类型的过滤条件中如果配置多个值，多个值之间是“或”的关系。
- 通常情况下，对于筛选出来的这些签名，在签名过滤器中配置沿用签名本身的缺省动作即可。同时也支持在过滤器中为所有签名统一设置动作。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）。如果一个配置文件中的多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。
- 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。

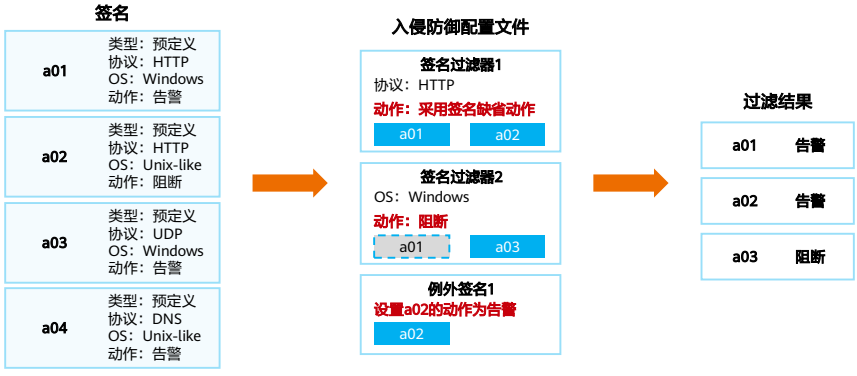
签名过滤器示例

- 例如：设备的保护对象是运行Windows操作系统的Web服务器，则可以配置签名过滤器筛选操作系统是Windows、协议是HTTP的签名。



例外签名

- 签名过滤器中设置的签名动作是统一的，无法修改单个签名动作。考虑到各种例外情况，IPS设备提供例外签名功能。例外签名的动作优先级高于签名过滤器。

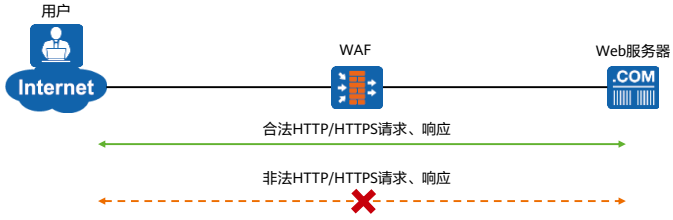


- 例外签名的动作分为阻断、告警、放行和添加黑名单。其中，添加黑名单是指在阻断流量的同时，将报文的源地址或目的地址添加至黑名单隔离访问。
- 一个入侵防御配置文件中可以配置多个签名过滤器、多个例外签名，签名最终的响应动作由这些配置决定，优先级从高到低依次为：例外签名动作、签名过滤器动作、签名自身的缺省动作。

目录

Web应用防火墙概述

- 随着Web技术的广泛应用，很多业务系统由C/S模式转向B/S模式，Web技术的功能也由简单的网页浏览转变为重要业务系统的主要载体，Web应用安全越来越受到人们的重视。
- 为了使Web应用系统免受攻击，在网络中部署WAF（Web Application Firewall，Web应用防火墙）设备成为首选的安全方案，WAF内置的安全规则可以阻挡绝大部分的HTTP/HTTPS应用层攻击。

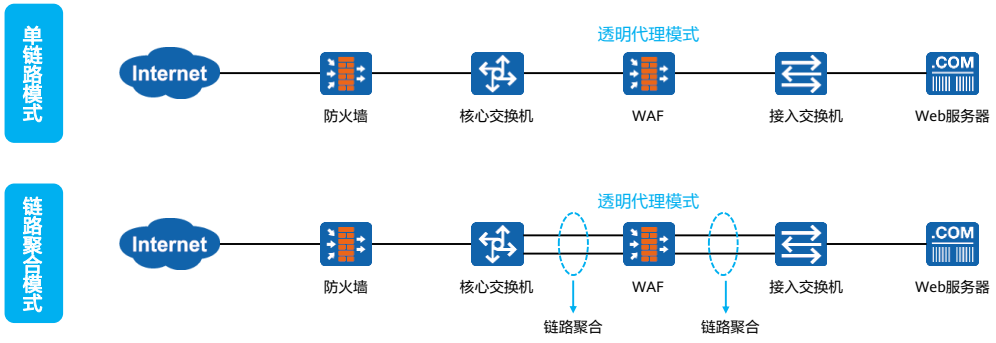


HUAWEI

- WAF只能处理HTTP/HTTPS协议，其他协议不会处理，若将其他流量牵引到WAF上，会导致数据流量丢弃。

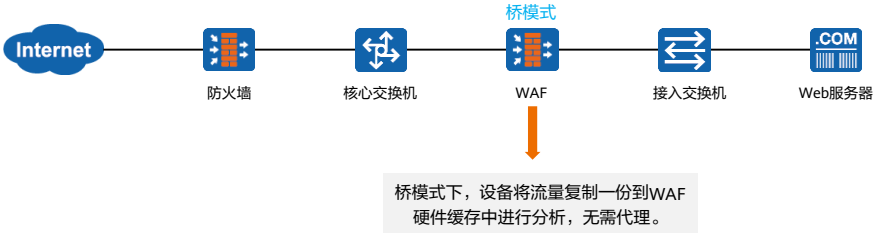
WAF组网方式 - 透明代理

- 透明代理采用串接部署方式，支持即插即用，无需更改网站DNS和服务器配置。用户以Web服务器的IP地址访问网站，简单易用。



WAF组网方式 - 桥模式

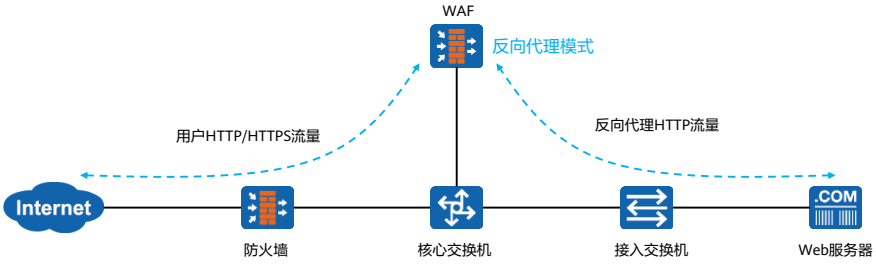
- 桥模式是真正意义上的透明模式，WAF串接在网络中，用户无需更改网络设备与服务器的配置，即插即用。
- WAF在桥模式下，只对请求流量进行检测，可以对攻击执行阻断，但是不处理响应流量。即使响应流量不经过WAF，也可以工作。



- 桥模式与透明代理模式的区别在于，桥模式是MAC层的透明代理，WAF不会更改数据包任何内容，如源IP、源MAC、端口号、TCP序列号、HTTP协议版本等内容。
- 桥模式下，WAF对原始数据包没有拆解，且无法对响应包的处理，导致无法使用站点侦测，CC攻击（Challenge Collapsar Attack）防护，应用层访问控制等，敏感信息过滤、响应包检测也无法使用。串接部署时，建议使用透明代理模式。

WAF组网方式 - 反向代理

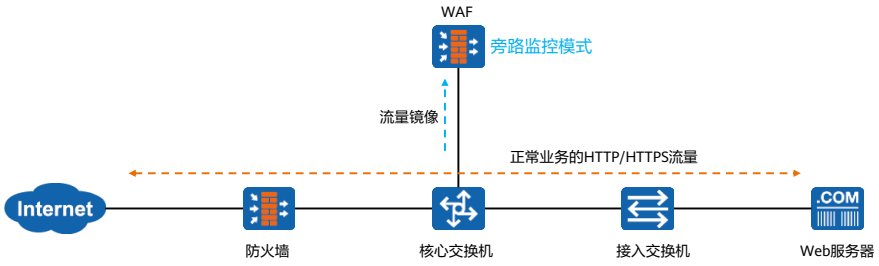
- 反向代理采用旁路部署方式，网站地址可以位于WAF设备上，也可以位于Web服务器上，适合网络环境较为复杂的场景。



- 反向代理模式可细分为两种链路模式：
  - 代理模式：网站的地址部署在WAF设备上，用户访问的是WAF设备上的地址。用户的请求通过路由转发至WAF，WAF设备再通过反向代理向真实Web服务器发送请求，此过程中需要修改数据包的目的地址。
  - 牵引模式：网站的地址部署在Web服务器上，用户直接访问Web服务器的地址。部署时，通常在交换机设备上配置策略路由，将访问Web服务器的流量牵引至WAF设备，WAF设备再通过反向代理向Web服务器发送请求，此过程中无需修改数据包的目的地址。

WAF组网方式 - 旁路监控

- 旁路监控模式通常将WAF旁挂于交换机上，交换机配置流量镜像功能，把流量复制一份到WAF上，不影响在线业务，不对Web服务器进行防护，通常用于只需要对应用流量进行分析或日志审计的场景中。



WAF主要功能

- WAF设备的主要作用是保护企业内网的HTTP/HTTPS站点，使其避免受到来自于互联网的各种网络攻击，其主要防护功能如下：

基于安全规则的防护

WAF安全规则可对HTTP/HTTPS协议规范性进行检查，并可抵御多种网络攻击，如跨站攻击、恶意软件、信息泄露、注入攻击、网络爬虫等。

Web加速及防篡改

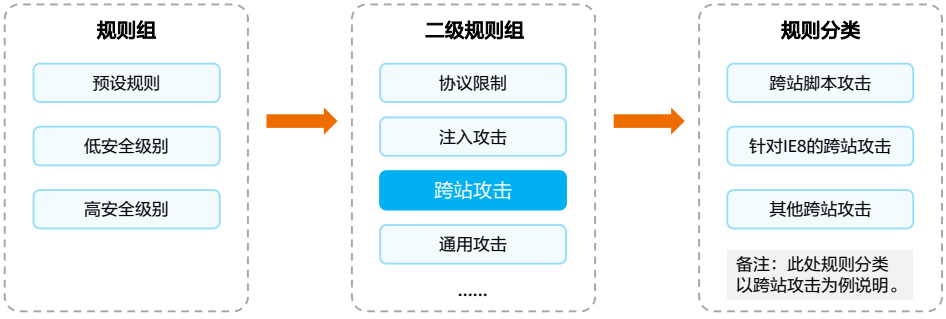
WAF设备内置的缓存可以保存服务器响应的Web页面信息，提高用户访问Web页面的速度，另外还支持数据压缩和网页防篡改功能。

访问审计功能

启用访问审计功能后，WAF设备可以对用户的正常访问进行记录并形成审计报表，用于安全审计。

WAF安全规则

- WAF对HTTP/HTTPS流量的防护主要通过安全规则（也称策略规则）来实现，安全规则以规则组、二级规则组、规则分类的形式进行组织，形成一个三级结构。
- 规则组表示一套预置规则的集合，有三套规则组：“预设规则”、低安全级别”、“高安全级别”。不同规则组内涵盖的二级规则组内容不同，即能够防御的攻击类型不同。



HUAWEI

- 每个二级规则组中包含不同的规则分类，可以手动设置是否启用，只有启用了对应的规则分类，WAF设备才会对流量进行对应的检查。

WAF安全规则举例

- 以二级规则组“注入攻击”为例，其对应的规则分类和详细规则条目如下所示。

规则编号	规则名称(点击切换到规则描述)	启用	动作	威胁	返回码	操作
12010002	阻止sql注入攻击，防'msdasql'字符	☑	阻断并告警	高	403	配置
12010003	阻止sql注入攻击，防xp_makecab字符	☑	阻断并告警	高	403	配置
12010004	阻止sql注入攻击，防butl_http字符	☑	阻断并告警	高	403	配置
12010005	阻止sql注入攻击，防类似"SELECT TO_NUMBER('dd32	☑	阻断并告警	高	403	配置

规则条目

目录

渗透测试概述

- **概念**：渗透测试工程师完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标网络、主机、应用的安全作深入的探测，发现系统最脆弱的环节。
- **目的**：渗透测试目的是防御，安全专家针对漏洞产生的原因进行分析，提出修复建议，以防御恶意攻击者的攻击。
- **分类**：白盒测试、黑盒测试和灰盒测试。

- 2017年6月1日颁布的《网络安全法》中，在相关安全测试过程中，首先要获得目标系统客户的授权才可以实施测试，如果未经授权，直接进行测试的话，是一种违法的行为。
- 渗透测试分类：
  - 白盒测试：在知道目标网站源码、逻辑架构和其他一些信息的情况下对其进行渗透，有点类似于代码分析；
  - 黑盒测试：只告诉网站信息，其他均隐藏，再去渗透，只关注结果；
  - 灰盒测试：介于白盒测试与黑盒测试之间的一种测试，灰盒测试多用于集成测试阶段，不仅关注输出、输入的正确性，同时也关注程序内部的情况。灰盒测试不像白盒那样详细、完整，但又比黑盒测试更关注程序的内部逻辑，常常是通过一些表征性的现象、事件、标志来判断内部的运行状态。

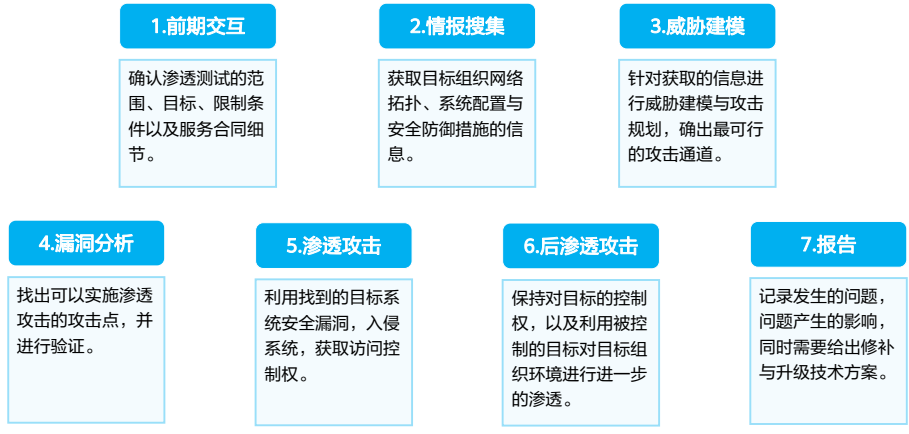
渗透测试框架

- 渗透测试是实施安全评估的具体手段，不同的行业、不同的评估对象使用的渗透测试方法区别较大，经过长时间的摸索和论证，业界内逐渐总结出一系列适用于网络、应用、系统等领域的安全测试方法。一些较为著名的安全评估方法论列举如下。

渗透测试执行标准	• Penetration Testing Execution Standard，PTES
开源安全测试方法论	• Open Source Security Testing Methodology Manual，OSSTMM
信息系统安全评估框架	• Information Systems Security Assessment Framework，ISSAF
开放Web应用安全项目	• Open Web Application Security Project，OWASP
Web应用安全联合威胁分类	• Web Application Security Consortium Threat Classification，WASC-TC

渗透测试流程

- 本节主要介绍渗透测试执行标准（PTES）的测试流程如下所示。



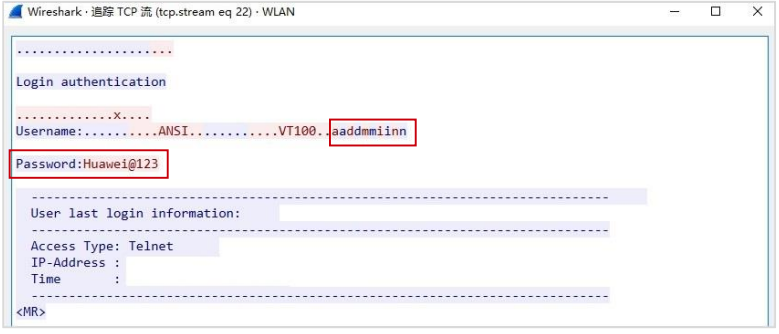
渗透测试常用工具

HUAWEI

- Wireshark：开源多平台网络协议分析器，以交互方式浏览所捕获的数据，查看数据包详细信息。
- Tcpdump：抓包、分析数据包工具，用于网络嗅探。
- Nessus：适用于UNIX系统的漏洞扫描程序。
- Snort：一个开源的入侵检测和防御系统，擅长对网络流量进行抓包、分析、记录，并支持漏洞扫描。
- Aircrack：破解无线网络密钥的一款工具。
- John the Ripper：快速密码破解程序，可用于检测系统中的弱密码。
- Metasploit：开源的漏洞检测工具，同时也是一个用于渗透测试的软件框架。
- Kali Linux：一个Linux发行版，提供各种各样的安全和取证工具，并提供丰富的开发环境。

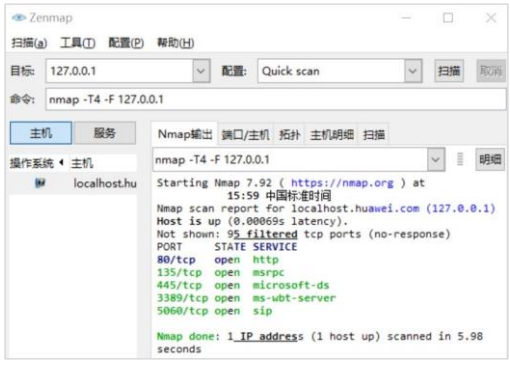
渗透测试工具举例 - Wireshark

- 如图所示，用户使用Telnet登录网络设备时，使用Wireshark抓包，可以获取用户登录密码。



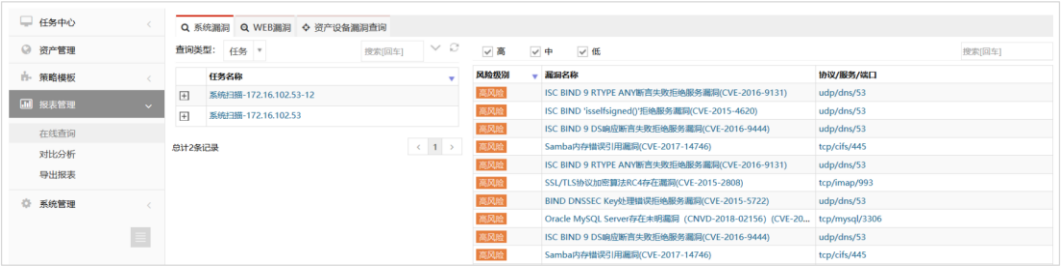
渗透测试工具举例 - Nmap

- Nmap，即Network Mapper，最早是Linux下的网络扫描与嗅探工具，现发展为跨平台的综合扫描软件，支持Windows、Linux、macOS等多种操作系统。
- Nmap具备如下扫描功能：
  - 主机发现：检测目标主机是否在线；
  - 端口扫描：检测端口状态和提供的服务；
  - 操作系统侦测：检测主机使用的操作系统。



渗透测试工具举例 - VSCAN

- VSCAN是华为公司的一款漏洞扫描产品，主要用于发现和评估网络设备、Web应用和数据库等存在的安全漏洞，并提供相应解决建议。具备如下扫描功能：系统漏洞扫描、Web漏洞扫描、数据库漏洞扫描、安全基线检查及弱口令扫描。
- VSCAN设备部署：传统的组网中，常采用VSCAN单机组网，根据扫描目标的不同，可以把漏洞扫描系统部署在某一个区域进行单区域扫描，或者是旁挂在核心交换机进行全网扫描。



HUAWEI

- 华为VSCAN扫描功能：
  - 系统漏洞扫描：对全网网元如网络主机、操作系统、网络设备、安全设备、应用系统等进行安全检查、发现安全漏洞，并提供安全解决建议。
  - Web漏洞扫描：能发现涵盖Web2.0、HTML5、HTTP1.0、HTTP1.1等形式Web站点中的安全漏洞，并提供安全解决建议，对网站SQL注入、Cookie注入、盲注、跨站、文件包含、敏感信息泄露等漏洞进行发现检查，提供测试用例及解决办法。
  - 数据库漏洞扫描：发现主流数据库的安全漏洞，并可以通过登录扫描，对数据库的表、字段进行安全检查；对数据库设置、系统软件本身及完整性进行检查。
  - 安全基线检查：设备的合规安全检查、日常安全检查。基于不同安全模板，不同设备类型对主机进行安全基线配置核查，并可自定义配置核查参数。
  - 弱口令扫描：对主流协议及数据库按照内置的口令安全性字典进行检查。

思考题

1. （多选题）以下哪些措施可以防范系统漏洞带来的安全威胁？（　　）
   A. 补丁管理
   B. 关闭不必要的服务
   C. 部署IPS设备
   D. 部署防火墙设备
2. （判断题）未经授权的渗透测试实则是一次攻击行为。（　　）
   A. 正确
   B. 错误

1. ABCD
2. A

本章总结

- 本章以漏洞为例，介绍了网络中常见的安全威胁，同时介绍了系统加固、部署IPS设备、部署WAF设备等漏洞防御方案，最后介绍了渗透测试流程与工具。
- 通过本课程的学习，您将对网络中常见的安全威胁有一定的了解，并有助于在安全部署与安全运维工作中全面地防御常见的安全威胁。

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
B/S	Browser/Server	浏览器/服务器模式
C/S	Client/Server	客户端/服务器模型
CGI	Common Gateway Interface	公共网关接口
CVE	Common Vulnerabilities and Exposures	公共漏洞和暴露
DNS	Domain Name Server	域名服务器
OS	Operating System	操作系统
SMB	Server Message Block	服务消息块
SQL	Structured Query Language	结构化查询语言
TCP	Transmission Control Protocol	传输控制协议
TTL	Time to Live	生存时间

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.

内容安全过滤技术

HUAWEI

前言

- 随着时代的发展，社会进入了移动互联网时代。安全威胁逐步向应用层延伸，企业越来越多的开始关注企业内部信息的安全问题，如核心机密信息泄漏问题。因此企业希望管理员根据业务安全需求，识别业务场景中出现的风险信息内容，并执行相应的风险管控措施。华为防火墙的内容安全过滤技术可以帮助企业完成对内容安全的管控。
- 本课程主要介绍防火墙内容安全过滤技术的概念及其实现原理。

目标

- 学完本课程后，您将能够：
  - 描述内容安全过滤技术的技术背景
  - 描述内容安全过滤技术的基本原理
  - 掌握内容安全过滤技术的配置

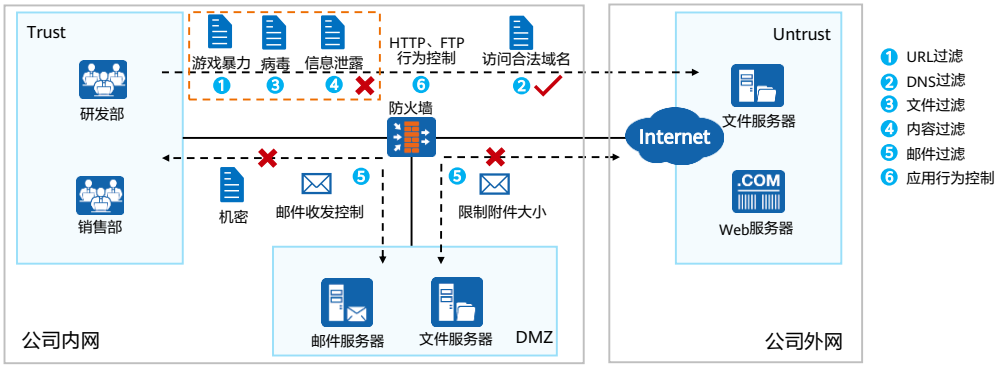
目录

内容安全过滤技术背景

- 随着通信的发展，安全威胁也从单纯的网络威胁向应用与数据安全威胁演进，企业内部业务安全的需求日益增长。如何识别业务场景中出现的机密信息或违法低质的信息，并进行告警、拦截等处理，是企业所面临的一个巨大挑战。
- 用户行为管控是解决上述企业安全问题强有力的措施，而在华为防火墙上部署内容安全过滤技术，可以对用户行为进行精细化的管控。

内容安全过滤技术介绍

- 华为防火墙内容安全过滤技术可以针对各个场景需求，设计不同安全防范方案。通过内容安全过滤技术可以帮助企业完成对内容安全方面的管控，防止企业内部核心信息泄露以及用户不当行为带来的不良影响。
- 通过内容安全过滤技术可以帮助企业完成对内容安全方面的管控，防止企业内部核心信息泄露。



HUAWEI

- 通过内容安全过滤技术可以管控企业用户行为：比如不允许访问非法网站，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，提高工作效率等。
- 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。

目录

URL过滤功能简介

- URL过滤功能可以对用户访问的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，满足企业精细化分配互联网带宽资源和准确控制员工上网权限的需求。

禁止访问无关网站

- 通过URL分类、黑白名单等功能，可以实现仅能访问特定URL的功能，从而提高企业办公的效率。

阻断低信誉和恶意URL

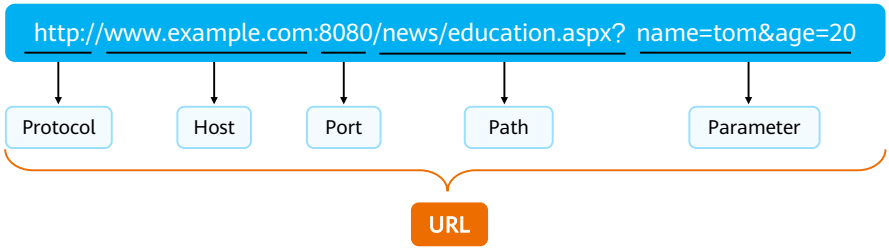
- 通过对低信誉和恶意URL的识别，可以有效阻断恶意网站的网络攻击，加强网络安全防护。

基于时间段控制URL访问

- 通过定义不同时间段的URL访问策略，可以实现基于时间段的URL访问控制，更加有效的利用企业网络带宽资源。

URL地址结构

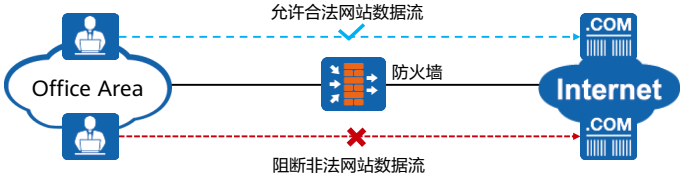
- Internet上的每一个网页都具有一个唯一的标识，称为URL（Uniform Resource Locator）地址。 URL是分配给网络上每个可用资源的特定地址，以便可以定位或标识这些资源。因此，互联网上每个资源（页面，站点，文档，文件，文件夹）都有一个URL 。
- URL通常是由Protocol、Host、Path、Parameter等字段组成。



- 其中各个字段的含义如下：
  - Protocol：方案/协议，它告诉浏览器如何处理将要打开的文件。最常使用的是HTTP协议。对于HTTP协议，一般可不输入。
  - Host：表示Web服务器的域名或IP地址。如果Web服务器使用非标准端口（非80端口，如8080），则Host字段还应包含端口号，如www.example.com:8080。
  - Path：表示Web服务器上的目录或文件名，以斜杠“/”隔开。
  - Parameter：表示传递给网页的参数，通常用于从数据库中动态查询数据。

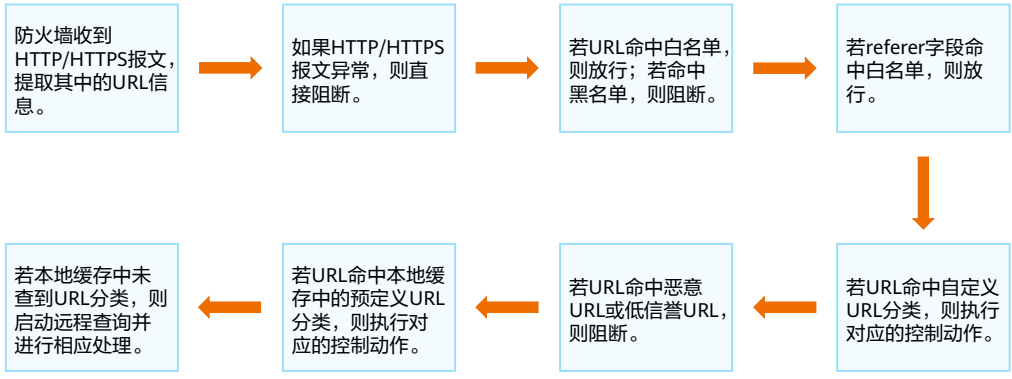
URL过滤原理

- 防火墙URL过滤的基本原理如下：
  - 用户使用浏览器发起网站访问请求，请求报文经过企业内部网络到达防火墙设备；
  - 防火墙对收到的HTTP/HTTPS请求报文进行解析，获取其中的URL信息，并对URL信息进行分析；
  - 若URL合法，则该HTTP请求被放行，用户可以浏览网站；
  - 若URL不合法，则对该HTTP请求进行阻断，并进行告警页面推送。



URL过滤处理流程

- 在防火墙启用URL过滤功能的情况下，当用户通过防火墙使用HTTP或HTTPS访问某个网络资源时，防火墙将进行URL过滤。处理流程如下图所示：



URL过滤方式

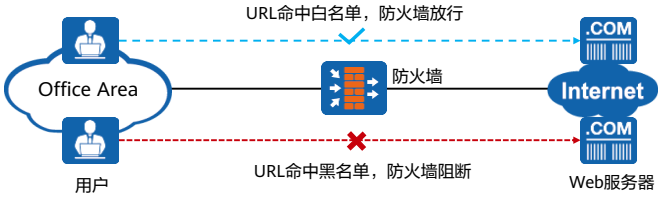
- 当用户的URL访问请求匹配到某条URL规则后，防火墙会根据URL过滤方式对此URL访问请求作出相应的处理。URL过滤主要有以下四种方式。

黑白名单	URL分类	低信誉或恶意URL	外部动态恶意URL
• 黑名单是不允许用户访问的URL列表； • 白名单是允许用户访问的URL列表； • 白名单的处理优先级高于黑名单。	• URL分类是指将大量的URL划分为不同的类别，实现对某类网站的控制； • URL分类可以分为预定义分类和自定义分类两种类型； • 自定义URL分类的处理优先级高于预定义URL分类。	• URL信誉反映了用户访问的URL是否值得信赖。开启URL信誉检测功能后，可以对低信誉的URL进行阻断。 • 恶意URL是指包含恶意信息的URL，开启恶意URL检测功能后，可以对恶意URL进行阻断。	• 外部动态恶意URL列表是外部官方网站发布的一些恶意URL的文本文件，用户可以通过加载外部动态恶意URL列表，识别并阻断最新的恶意URL，防止用户遭受新型攻击。

黑白名单 > URL分类 > 低信誉或恶意URL > 外部动态恶意URL

URL黑白名单

- 黑名单是不允许用户访问的URL列表，白名单是允许用户访问的URL列表。黑白名单一般用于过滤简单固定的网站。
- 当用户请求访问URL时，设备将提取出的URL信息与黑白名单进行匹配。若URL命中白名单，则放行；若命中黑名单，则阻断。
- 由于黑白名单对URL的识别颗粒度更细，所以在URL过滤中，黑白名单过滤方式的优先级要高于自定义URL分类和预定义URL分类。其中白名单的优先级高于黑名单的优先级。

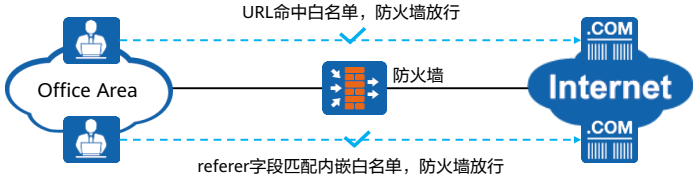


HUAWEI

- 黑白名单一般用于过滤简单固定的网站。相对于URL分类，黑白名单的分类粒度更细。当用户请求访问URL时，设备将提取出的URL信息与黑白名单进行匹配。
  - 如果匹配白名单则允许该URL请求。例如，企业只允许员工访问与工作相关的一些网站，其他网站不允许访问。通过将与工作相关的一些网站加入白名单，可以达到该企业的要求；
  - 如果匹配黑名单则阻断该URL请求。例如，企业为了提高员工上班时间的工作效率，优化公司的网络带宽，需要对员工的上网行为进行控制，不允许访问一些娱乐、游戏、视频等网站。通过将娱乐、游戏、视频等网站加入黑名单，可以达到该企业的要求。

内嵌白名单功能

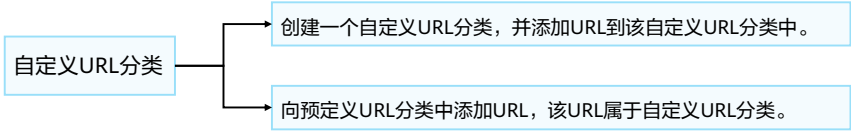
- 一般大的网页都会内嵌其他的网页链接，如果只将主网页加入白名单，则该主网页下的内嵌网页部分将无法正常访问。除非把内嵌网页全部加入白名单才能正常访问，但是配置复杂。
- 为解决以上问题，新增了内嵌白名单功能。该功能将用户HTTP请求中的referer字段去匹配内嵌白名单，如果匹配，用户就可以访问该网页。因此只要把某个网页加入内嵌白名单，用户就可以访问该网页下的所有内嵌网页，简化了配置。



- 内嵌白名单功能有两种实现方式，具体如下：
  - 使用用户手工配置的referer-host与HTTP请求中的referer字段进行匹配，如果匹配则允许该URL请求。如果HTTP请求中的referer字段没有匹配配置的referer-host，用户还可以选择是否将referer字段去匹配所有配置的白名单规则。开启referer字段匹配白名单功能后，如果referer字段匹配白名单规则，则允许该URL请求。
  - 开启referer字段匹配白名单功能后，直接使用配置的白名单与HTTP请求中的referer字段进行匹配，如果匹配命中，则允许该URL请求。
- referer字段匹配白名单功能默认开启，用户也可以选择关闭该功能。

URL分类

- URL分类是指将大量的URL划分为不同的分类，一个URL分类可以包含若干条URL，通过URL分类可以实现对某一类网站的控制。URL分类可以分为预定义分类和自定义分类两种类型。自定义URL分类优先级高于预定义URL分类。
  - 预定义URL分类：华为维护了大量的主流web网站，并对这些网站进行了分类，内置于防火墙系统中，被称为预定义URL分类，主要用来对一些常见的网站进行访问控制。预定义URL分类不能创建、删除和重命名。
  - 自定义URL分类：管理员手工配置的URL分类，主要用于覆盖新出现的网站，以及满足特殊的过滤需求。
- 自定义URL分类的配置方式有以下两种：



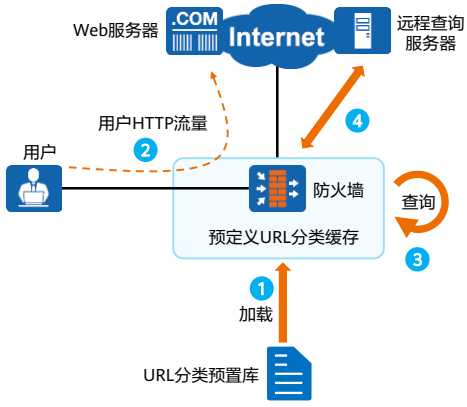
URL分类的处理动作

- 防火墙根据URL分类信息，可以执行不同的分类处理动作：
  - 允许：允许用户访问此类网站。
  - 告警：允许用户访问并记录日志。
  - 阻断：禁止用户访问。
- 为了简化操作，华为防火墙提供了三个缺省的URL过滤级别，定义了各个URL分类的处理动作。
  - 高：对所有成人网站、非法网站、社交网络、视频共享等网站进行严格的限制。
  - 中：对所有成人网站和非法网站进行控制。
  - 低：对色情网站进行控制。

- 当管理员使用过滤级别后，所有URL分类的动作都会根据过滤级别自动生成。
- 预定义分类中，大类中还包含了小类。但是在安全策略中，处理动作的应用始终以小类为基准。企业管理员可以设置大类的处理动作，让所有小类都继承；企业管理员也可以继续调整某个小类的处理动作，实现差异化的管控需求。如图所示：IT相关大类中包含了各个小类，都继承了大类的处理动作允许，也可以单独设置处理动作。

URL预定义分类查询流程

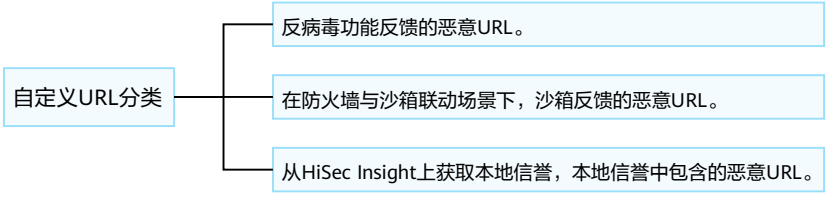
- 预定义URL分类的查询分为两种方式：预定义URL分类缓存和远程查询服务器。其查询流程如下：
  1. 防火墙上电启动后，会自动将URL分类预置库加载到预定义URL分类缓存中。URL分类预置库是出厂预置的，无需用户手动加载；
  2. 用户请求访问URL资源，防火墙收到后，提取请求报文中的URL信息；
  3. 防火墙在预定义URL分类缓存中查询该URL所属的分类，若查询到，则按照该URL分类配置的响应动作进行处理；
  4. 若防火墙在预定义URL分类缓存中未查询到该URL所属的分类，则到远程查询服务器上继续查询，根据查询结果进行相应处理，并将查询到的URL和其所属的分类信息保存到预定义URL分类缓存中，以便下次快速查询。



黑白名单 > URL分类 > 低信誉或恶意URL > 外部动态恶意URL

URL信誉和恶意URL

- URL信誉反映了用户访问的URL是否值得信赖。 URL信誉值的查询分为两种方式：URL信誉热点库和远程查询服务器。
  - URL信誉热点库： URL信誉热点库是由sec.huawei.com发布的，用来快速获取云端最新的URL信誉，以便对不可信的URL进行及时阻断。
  - 远程查询服务器：若防火墙未启用URL信誉热点库升级功能，在预定义URL分类缓存查询不到URL信誉值时，可通过URL远程查询功能来获取最新的URL信誉值。
- 恶意URL是指包含恶意信息的URL。恶意URL的来源包括：

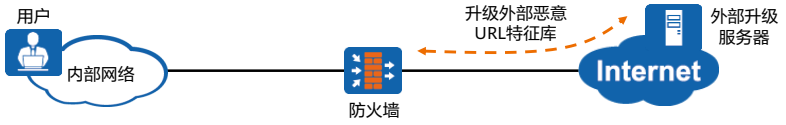


HUAWEI

- 沙箱又叫沙盘，即是一个虚拟系统程序，允许你在沙盘环境中运行浏览器或其他程序，因此运行所产生的变化可以随后删除。它创造了一个类似沙盒的独立作业环境，在其内部运行的程序并不能对硬盘产生永久性的影响。其为一个独立的虚拟环境，可用以测试不受信任的应用程序或上网行为。
- 华为的推出基于大数据的APT（Advanced Persistent Threat，高级长期威胁）防御产品HiSec Insight高级威胁分析系统，能够对网络中的流量及各类设备的网络、安全日志等海量网络基础数据执行有效采集，通过大数据实时及离线分析，结合机器学习技术、专家信誉、情报驱动，有效的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，同时可以结合华为HiSec解决方案高效地完成威胁的处置闭环，防患未然。

外部动态恶意URL列表

- 外部动态恶意URL列表是外部官方网站发布的一些恶意URL的文本文件。防火墙可以通过升级外部恶意URL特征库，不断从外部官方网站下载最新的外部动态恶意URL列表到本地，并将其加载到设备缓存中。
- 开启外部动态恶意URL过滤功能后，当用户请求访问URL时，防火墙将URL信息与缓存中的外部动态恶意URL列表进行匹配，如果匹配，则直接阻断该URL请求。
- 外部恶意URL特征库仅支持在线升级。在线升级可分为定时升级和立即升级两种方式。



- 定时升级：定期连接外部升级服务器检查是否存在新的外部恶意URL特征库版本。如果存在新版本的外部恶意URL特征库，防火墙会根据设定的时间自动下载并更新本地的外部恶意URL特征库。
- 立即升级：当用户发现网络上出现新的外部恶意URL特征库，而防火墙定时更新时间还没达到，或防火墙未启用定时更新，此时可以选择立即升级。立即升级使用的下载地址就是定时升级的下载地址，升级流程也与定时升级完全相同，区别在于立即升级不受时间限制，可以在任何时刻执行立即升级动作。

URL匹配规则（1）

- 防火墙根据白名单、黑名单、自定义分类和预定义分类过滤URL时，都需要遵循URL匹配规则。URL匹配主要有以下四种匹配方式。

匹配方式	定义	使用示例
前缀匹配	匹配所有以指定字符串开头的URL，例如www.example*。	如果想控制访问所有以www.example开头的网站，配置URL过滤规则为www.example*。
后缀匹配	匹配所有以指定字符串结尾的URL，例如*aspx。	如果想控制访问www.example.com网站下的所有图片类网页，配置URL过滤规则为*.jpg，*.jpeg，*.gif，*.png和*.bmp。
关键字匹配	匹配所有包含指定字符串的URL，例如*sport*。	如果想控制访问包含sport的所有网站，配置URL过滤规则为*sport*。
精确匹配	首先判断URL和指定字符串是否匹配，如果未匹配，则去除URL的最后一个目录，再和指定字符串进行匹配；如果还未匹配，则继续去除URL的最后一个目录，再和指定字符串进行匹配。以此类推，直到用域名去匹配指定的字符串为止，例如www.example.com。	如果想控制访问www.example.com域名下的所有网站，配置URL过滤规则为www.example.com。

- 管理员可以在白名单、黑名单、自定义分类和预定义分类中配置URL规则和host规则，其中URL规则的匹配范围是全部URL，host规则的匹配范围只是域名（或者IP地址）部分。两者的使用场景如下：
  - 如果允许或阻断的URL为域名形式，大多数情况下可以配置URL规则或host规则，两者的过滤效果相同。例如，允许或阻断访问域名www.example.com。
  - 如果允许或阻断的URL为二级域名形式，当配置的URL条目比较少时，配置URL规则或host规则都可以；当配置的URL条目比较多时，配置host规则更简单。例如允许或阻断访问域名news.example.com。
  - 如果允许或阻断的URL带有目录和参数内容，只能配置成URL规则，不能配置成host规则。例如，允许或阻断访问URL地址www.example.com/news。

URL匹配规则 (2)

- URL进行匹配时，不同的匹配方式存在如下优先级顺序，由高至低如下所示：
  - 精确匹配 > 后缀匹配 > 前缀匹配 > 关键字匹配
- 例如：URL“www.example.com/news”，可以同时匹配以下三种方式，按照优先级顺序，最终以精确匹配条件“www.example.com/news”对应的URL分类为准。
  - 精确匹配：www.example.com/news
  - 前缀匹配：www.example.com/*
  - 关键字匹配：*example*
- 在同一种匹配方式下，匹配规则越长优先级越高。例如：以下条目均属于前缀匹配方式，则URL“www.example.com/news/index.html”会优先匹配“www.example.com/news/*”条目。
  - www.example.com/news/*
  - www.example.com/*

URL匹配规则 (3)

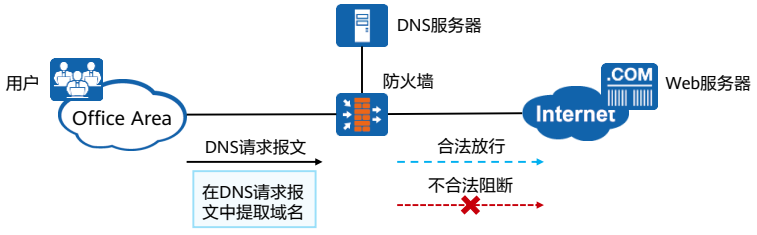
- 在同一种匹配方式下，如果匹配规则长度也相同，则最终以配置的动作模式为准。
  - 当动作模式为“严格模式”时，则最终查询结果以动作最为严格的URL分类为准。
  - 当动作模式为“松散模式”时，则最终查询结果以动作最为宽松的URL分类为准。
- 如表所示，两个条目均属于“关键字匹配”方式，且匹配规则长度相同。对于URL“www.example.com”来说，如果同时可以匹配两个分类，但控制动作却不同时：
  - 当动作模式为“严格模式”时，则最终查询结果以动作最为严格的URL分类为准，本例中URL匹配分类B，动作为阻断。
  - 当动作模式为“松散模式”时，则最终查询结果以动作最为宽松的URL分类为准，本例中URL匹配分类A，动作为允许。

分类	控制动作
www.example.com/A	允许
www.example.com/B	阻断

目录

DNS过滤应用场景

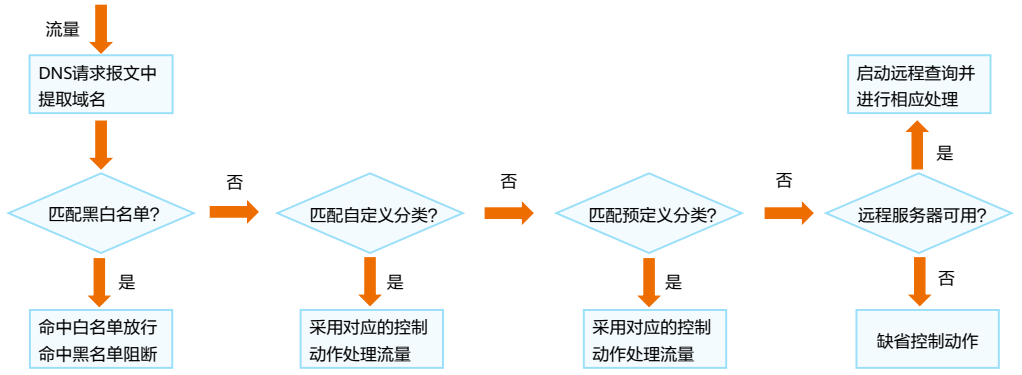
- DNS过滤功能是对DNS请求报文中的域名进行过滤，允许或禁止用户访问某些网站，规范上网行为。
- 防火墙作为企业网关部署在网络边界，当企业用户发起Web请求时，通过对DNS请求报文中的域名进行过滤，可以实现对用户的请求进行放行、告警或者阻断。
- 如图所示，使用DNS过滤后：
  - 当用户访问合法域名的网站时，放行此请求。
  - 当用户访问非法域名的网站时，阻断此请求。



- DNS过滤还可以通过引用时间段或用户/组等配置项，实现针对不同时间段或不同用户/组的请求进行放行或者阻断，达到更加精细化和准确化控制员工上网权限的需求。

DNS过滤处理流程

- 流量命中安全策略，且安全策略配置了DNS过滤配置文件时，从DNS请求报文中提取域名并送往DNS过滤处理。DNS过滤的具体流程如下图所示：



HUAWEI

- 和URL相同，DNS分类分为自定义分类和预定义分类，管理员可以利用系统提供的预定义分类，也可以创建自定义分类，达到对域名进行过滤的目的。
- 预定义分类：
  - 预定义分类已经预先对大量常见的域名进行了分类，管理员可以根据这些分类轻松地控制内网用户禁止访问哪些类别的域名、允许访问哪些类别的域名。
  - 预定义DNS分类是系统内置的，跟预定义URL分类是同一个。管理员不能够创建、删除和重命名预定义DNS分类，也不能向预定义DNS分类中添加自定义的域名规则。
- 自定义分类：
  - 虽然预定义分类覆盖了主流的Web网站，但很多新出现的网站可能覆盖不到。另一方面，管理员出于特殊的过滤需求或者增强预定义DNS分类等目的，也会按需创建一些自定义分类。

URL过滤与DNS过滤对比

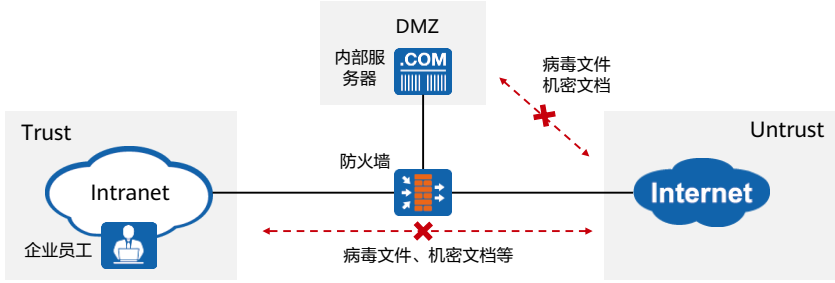
- DNS过滤功能是对DNS请求报文中的域名进行过滤，允许或禁止用户访问某些网站，达到规范上网行为的目的。相比于URL过滤更早的进行访问控制，可以有效降低整网HTTP报文的流量。
- URL过滤相比于DNS过滤可以进行更精细控制用户对网络资源的访问。

对比项	URL过滤	DNS过滤
控制访问阶段	在发起HTTP/HTTPS的URL请求阶段进行控制	在域名解析阶段进行控制
控制粒度	控制粒度细，可以控制到目录和文件级别	控制粒度粗，只能控制到域名级别
性能影响	性能影响大	性能影响小
控制范围	仅控制HTTP/HTTPS访问	该域名对应的所有服务都可以控制

目录

文件过滤简介

- 文件过滤是一种根据文件类型对文件进行过滤的安全机制。防火墙通过识别自身传输的文件类型，可以实现对特定类型的文件进行阻断或告警。
- 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。

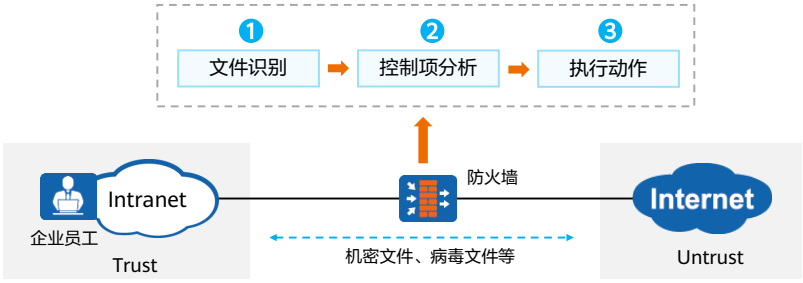


HUAWEI

- 防火墙能够识别通过自身传输的文件的类型，并且可以对特定类型的文件进行阻断或告警。
- 当通过防火墙的文件（流量）匹配了一条安全策略规则，规则的动作为permit且引用了文件过滤配置文件时，此文件需要进行文件过滤检测。
- 管理员在防火墙上部署了文件过滤功能，可以实现如下安全保护效果：
  - 降低机密信息泄露的风险。
    - 机密信息一般保存在文档中，而且文档可以被压缩形成压缩文件。员工上传包含机密的文档到外网或者黑客从内网服务器窃取机密文档，都会导致公司机密或用户信息的泄露。因此，阻止内网用户上传文档文件和压缩文件到外网，以及阻止外网用户从内网服务器下载文档文件和压缩文件，可以大大降低机密信息泄露的风险。
  - 降低病毒文件进入公司内部网络的风险。
    - 病毒常常包含在可执行文件中，且病毒的反检测和渗透防火墙的能力越来越强。因此，阻止内网用户从外网下载可执行文件或阻断外网用户上传可执行文件到内网服务器，可以大大降低病毒进入内网的风险。
  - 阻止占用带宽和影响员工工作效率的文件传输。
    - 公司员工下载大量与工作无关的视频和图片文件，占用公司网络带宽，降低工作效率。因此，阻止内网用户从外网下载视频、图片和压缩文件，可以保证正常业务的带宽和员工的工作效率。

文件过滤处理流程

- 在企业网关配置文件过滤后，员工上传或下载的文件都会去匹配配置的文件过滤，根据识别结果执行相应的动作。



HUAWEI

- 控制项代表用户定义的文件类型、扩展名和文件传输方向，根据这些设置进行文件分析。

文件过滤技术原理 (1)

- 防火墙针对接收的文件能够做出以下识别：
  - 承载文件的应用协议：文件是承载在应用协议上传输的，例如HTTP、FTP、SMTP、POP3、IMAP。
  - 文件传输方向：包括上传和下载。
  - 文件类型：防火墙能够识别文件真正的类型，例如：一个Word文档file.doc可以将文件名修改为file.exe，但是它的文件类型仍然为doc。
  - 文件扩展名：文件名称（包含压缩文件）的后缀，例如：file.doc和file.exe中的doc和exe为文件扩展名。
- 如果防火墙文件识别结果异常，需要配置额外的下一步处理动作，通常采用默认值即可。文件类型识别有三种异常情况：
  - 文件扩展名不匹配：文件类型与文件扩展名不一致。
  - 文件类型无法识别：无法识别文件类型，且没有文件扩展名。
  - 文件损坏：由于文件被破坏而无法进行文件类型识别。

文件过滤技术原理 (2)

- 防火墙会根据文件识别的结果和文件识别异常的响应动作来决定：是否进行文件过滤规则匹配以及规则匹配成功后的执行动作。

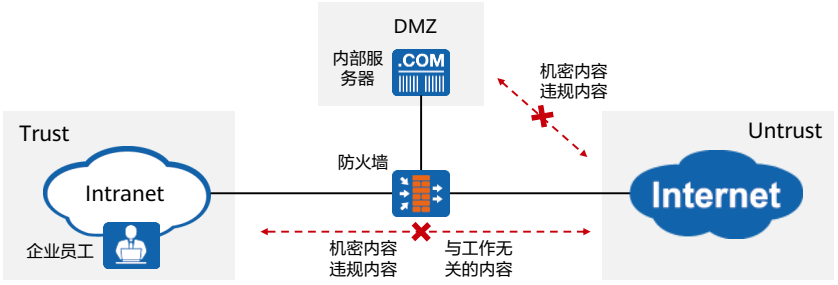
文件识别结果	文件识别异常的响应动作	文件过滤规则匹配
文件类型与文件扩展名一致	——	根据文件类型进行文件过滤规则匹配，匹配条件为“应用”、“文件类型”、“方向”。
文件类型与文件扩展名不一致	执行“文件扩展名不匹配时动作”。 • 允许：允许文件传输，然后进行文件过滤规则匹配。 • 告警：允许文件传输并记录日志，然后进行文件过滤规则匹配。 • 阻断：阻断文件传输并记录日志。	根据文件类型进行文件过滤规则匹配，匹配条件为“应用”、“文件类型”、“方向”。
无法识别出文件类型，但存在文件扩展名	——	根据文件扩展名进行文件过滤规则匹配，匹配条件为“应用”、“自定义扩展名”、“方向”。
无法识别出文件类型，且没有文件扩展名	执行“文件类型无法识别时动作”。 • 允许：允许文件传输。 • 告警：允许文件传输并记录日志。 • 阻断：阻断文件传输并记录日志。	——
文件损坏	执行“文件损坏时动作”。 • 允许：允许文件传输。 • 告警：允许文件传输并记录日志。 • 阻断：阻断文件传输并记录日志。	——

- 防火墙为文件识别异常设置了执行动作，根据执行动作决定下一步的处理步骤。
- 如果需要进行文件过滤规则匹配，则防火墙会将识别出的文件属性（应用、方向、文件类型、文件扩展名）与管理员定义的文件过滤配置文件的规则进行匹配：
  - 如果文件的属性与规则的匹配条件全部匹配，则此文件成功匹配文件过滤配置文件的规则。如果其中有一个条件不匹配，则继续匹配下一条规则。以此类推，如果所有规则都不匹配，则防火墙会允许此文件传输。
  - 如果文件成功匹配一条规则，防火墙将会执行此规则的动作。如果动作为“阻断”，则防火墙会阻断此文件传输。如果动作为“告警”，则防火墙会允许此文件传输并记录日志。
- 注意：在无法识别文件类型时，先判断是否存在文件扩展名，如果存在按照文件过滤规则匹配。如果不存在再按照没有文件扩展名的响应动作进行处理。

目录

内容过滤简介

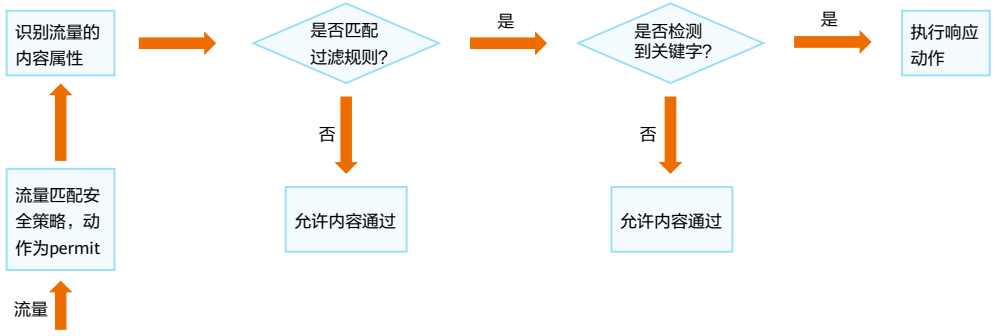
- 内容过滤是一种对文件或应用的内容进行过滤的安全机制。通过深度识别流量中包含的内容，防火墙可以对包含特定关键字的流量进行阻断或告警。
- 内容过滤可以防止机密信息的泄露及违规信息的传输。



- 管理员在防火墙上部署了内容过滤功能，可以实现如下安全保护效果：
  - 降低公司机密泄露的风险。
  - 降低因员工浏览、发布、传播违规信息而给公司带来的法律风险。
  - 阻止员工浏览和搜索与工作无关的内容，提高工作效率。

内容过滤处理流程

- 当通过设备的流量匹配了一条安全策略，策略的动作为permit且引用了内容过滤配置文件时，此流量需要进行内容过滤检测，处理流程如下所示。

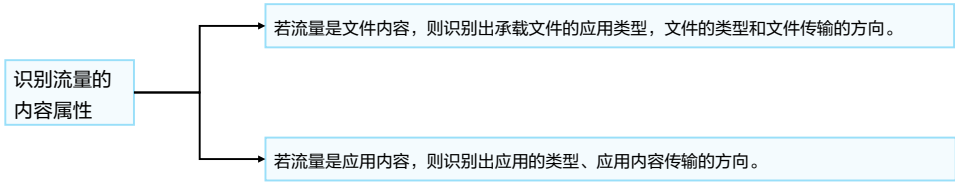


HUAWEI

- 内容过滤的处理流程如下：
  - 设备对流量的内容进行检测，识别出流量的内容属性。
    - 如果是应用内容则识别出应用的类型和应用内容传输的方向。
    - 如果是文件内容则识别出承载文件的应用类型、文件的类型和文件传输的方向。
  - 设备将流量的内容属性与内容过滤规则的条件进行匹配。如果所有条件都匹配，则此内容成功匹配此规则。如果其中有一个条件不匹配，则继续执行下一条规则。以此类推，如果所有内容过滤规则都不匹配，则设备允许此内容通过。
  - 如果内容成功匹配一条内容过滤规则，则设备会对此内容进行关键字检测，检测内容中是否存在内容过滤规则定义的关键字。如果检测时识别出关键字，则设备会执行响应动作。如果没有识别出关键字，则设备允许此内容通过。

内容过滤的流量识别

- 内容过滤技术通过深度识别流量中包含的内容，设备可以对包含特定关键字的流量进行阻断或告警。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。

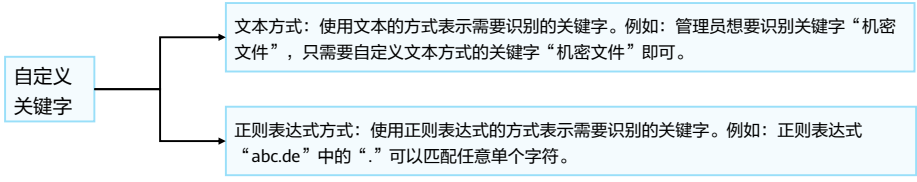


常见协议支持的过滤内容

协议名称	支持的过滤内容
HTTP	上传方向：用户发布微博的内容、用户发帖的内容、用户搜索输入的内容、用户提交信息的内容、上传文件的名称等； 下载方向：用户浏览网页的内容、使用HTTP协议下载文件的名称。
FTP	上传和下载文件的名称和文件内容。
SMTP	发送的邮件的标题、正文和附件名称。
POP3	接收的邮件的标题、正文和附件名称。
IMAP	接收的邮件的标题、正文和附件名称。
NFS	上传和下载的文件内容。
SMB	上传和下载的文件内容。

内容过滤的关键字检测

- 关键字是内容过滤时设备需要识别的内容，如果在文件或应用中识别出关键字，设备会对此文件或应用执行响应动作。关键字通常为机密信息（公司商业机密、用户个人信息的报告）或违规信息（色情、暴力、敏感或公司规定的违规信息等）。
- 关键字包括预定义关键字和自定义关键字。
  - 预定义关键字是系统默认存在的可以识别的关键字，包括：银行卡号、信用卡号、社会安全号、身份证号、机密关键字（包括“秘密”、“机密”、“绝密”）。
  - 自定义关键字是管理员自定义的需要识别的关键字，有文本和正则表达式两种定义方式。



HUAWEI

- 以下是常用的字符：
  - . 代表匹配任意非换行字符。
  - （ ）代表标记一个子表达式的开始和结束位置。
  - * 代表匹配前面的字符或表达式零次或多次。
  - \d 代表匹配一个数字字符。等价于[0-9]。
  - \w 代表匹配数字、字母和下划线。

内容过滤的响应动作

- 设备在内容过滤检测时识别出关键字，会执行响应动作。

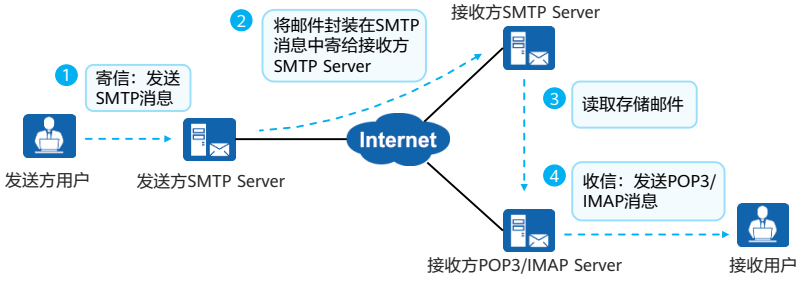
动作	说明
告警	识别出关键字后，记录日志但不阻断内容传输。
阻断	识别出关键字后，阻断内容传输并记录日志。在用户看来则是无法显示网页、上传或下载文件失败、邮件发送或接收失败。
按权重操作	每个关键字都存在一个权重值，当设备检测的内容中出现关键字时，设备会将这些关键字的权重值按出现次数累加。如果权重值的和大于等于“告警阈值”小于“阻断阈值”，则设备会执行“告警”动作，“告警”动作仅执行一次；如果权重值的和大于等于“阻断阈值”，则设备会执行“阻断”动作。

- 按权重操作举例：
  - 管理员在设备上定义了两个需要识别的关键字，关键字a的权重值为1，关键字b的权重值为2；定义了内容过滤的告警阈值为1，阻断阈值为5。如果设备检测出用户浏览的网页中存在一次关键字a，这时权重值的和为1，等于告警阈值1，则设备会记录日志，用户仍然能正常浏览网页。如果设备检测出用户浏览的网页中出现了三次关键字a和两次关键字b，这时权重值的和为7（3×1+2×2=7），大于阻断阈值5，则设备会阻断此网页并记录日志，用户看到的是无法显示网页。

目录

邮件传输流程

- 电子邮件的发送和接收机制如下图所示：
  - 用户将邮件内容封装在SMTP消息中寄给发送方SMTP Server；
  - 发送方SMTP Server将邮件封装在SMTP消息中寄给接收方SMTP Server，接收方SMTP Server储存起来；
  - POP3/IMAP Server收到用户的请求后，读取SMTP Server储存的邮件；
  - POP3/IMAP Server将邮件封装到POP3/IMAP消息中发送给接收方。

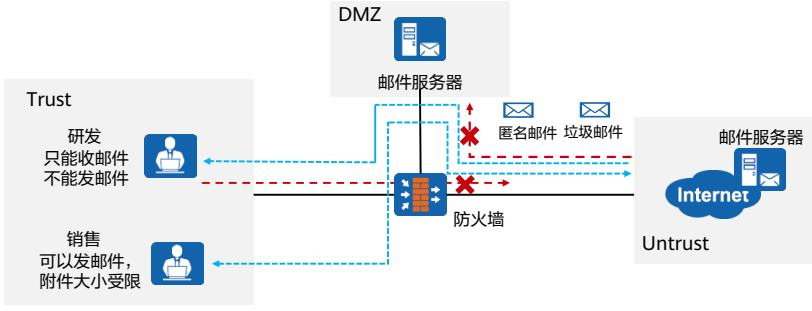


HUAWEI

- 邮件传输要求网络管理员需要在邮件服务器上部署SMTP服务、POP3服务（或IMAP服务）；终端用户需要在PC上安装邮件客户端软件（例如Microsoft Outlook、Foxmail等邮件管理软件）。
- 邮件传输协议：
  - SMTP定义了计算机如何将邮件发送到SMTP Server，SMTP Server之间如何中转邮件。
  - POP3（Post Office Protocol 3，邮局协议版本3）和IMAP（Internet Mail Access Protocol，交互式邮件存取协议）规定计算机如何通过客户端软件管理、下载邮件服务器上的电子邮件。
  - IMAP与POP3主要区别在于：使用POP3，客户端软件会将所有未阅读邮件下载到计算机，并且邮件服务器会删除该邮件。使用IMAP，用户直接对服务器上的邮件进行操作，不需要把所有邮件下载到本地再进行各项操作。

邮件过滤简介

- 邮件过滤是指对邮件收发行为进行管控，包括防止垃圾邮件和匿名邮件泛滥，控制违规收发等。
- 邮件过滤主要使用IP地址检查和邮件内容过滤技术，它可以帮助局域网用户提高邮件系统的安全性：
  - IP地址检查可以防止垃圾邮件在内网泛滥。
  - 邮件内容过滤既可以过滤掉匿名邮件，也可以通过检查邮件内容控制内网用户的邮件发送或接收权限。

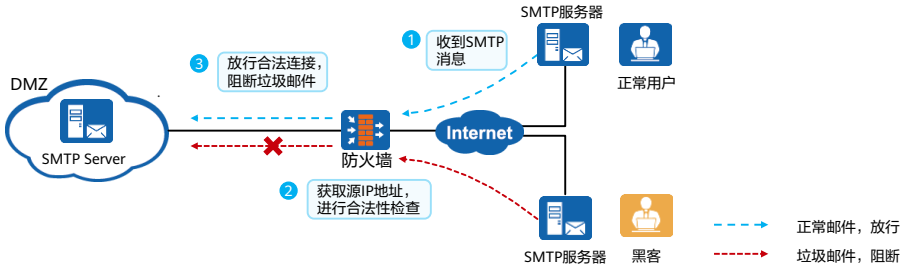


HUAWEI

- 如图所示，防火墙作为一个办公网络的安全网关，邮件服务器部署在内网，内部网络用户通过部署在内网的邮件服务器收发邮件。
- 在防火墙上配置邮件过滤，可以收到如下邮件安全保护效果：
  - 开启垃圾邮件防范，防止内网的SMTP服务器收到大量垃圾邮件。
  - 开启匿名邮件检查，防止违法信息通过匿名邮件方式在整个网络内部传播。
  - 开启邮箱地址检查，只允许指定邮箱地址发送或接收电子邮件，从发送和接收权限上进行控制，防止内部用户泄露重要信息。
  - 开启邮件附件控制，对附件的大小和个数进行控制，防止大量信息通过附件泄露出去。

基于IP过滤 (1)

- 从邮件工作机制中可以了解到，在整个邮件发送过程中，PC与邮件服务器、邮件服务器与邮件服务器之间都不做认证，攻击者可以通过互联网上任意一台SMTP Server来发送邮件。
- 为防止垃圾邮件泛滥可以通过检查发送方SMTP Server源IP的合法性：
  - 查询本地黑白名单
  - 查询RBL（ Real-time Blackhole List，实时黑名单列表 ）黑名单

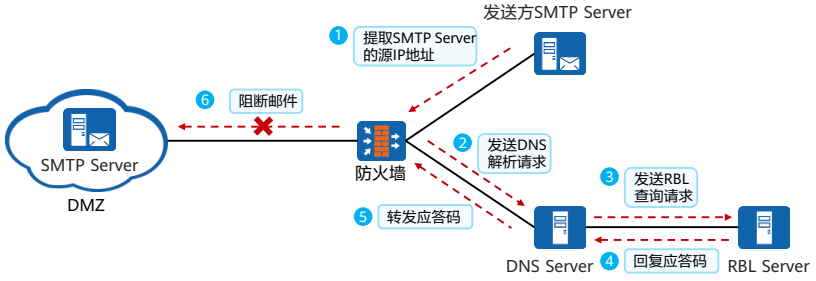


HUAWEI

- RBL黑名单是由反垃圾邮件组织联合收集的一个庞大的在线数据库，收集、保存频繁发送垃圾邮件SMTP Server的IP地址。
- 垃圾邮件指的是未经用户许可强行发送到用户邮箱的电子邮件，内容一般是广告、宣传资料等，甚至带有病毒程序。大量的垃圾邮件不但消耗网络带宽，占用邮箱空间，还带来了安全隐患。
- IP地址检查是指防火墙对发送方SMTP Server的源IP进行检查，具体实现过程如下：
  1. 防火墙收到其他SMTP Server发送的SMTP消息，包括正常邮件和垃圾邮件。
  2. 防火墙执行IP地址检查：
     - 解析SMTP消息，从SMTP消息中获取发送方SMTP Server的源IP。
     - 检查源IP合法性。防火墙将IP地址与黑名单、白名单进行比较，来判断IP地址的合法性：
       - 如果源IP命中了本地白名单，判定为合法邮件，否则查找本地黑名单；
       - 如果命中本地黑名单，判定为垃圾邮件，否则查询RBL黑名单；
       - 如果命中RBL黑名单判断为垃圾邮件，否则判定为合法邮件。
  3. 放行合法邮件，阻断垃圾邮件。

基于IP过滤 (2)

- RBL黑名单查询机制：
  - 防火墙获取邮件发送方SMTP服务器的IP地址，向RBL服务器发起查询；
  - RBL服务器维护着实时黑名单列表，列表中的SMTP服务器都发送过垃圾邮件；
  - 防火墙根据RBL服务器的返回结果判断该IP地址是否属于垃圾邮件服务器，进而采取相应的处理动作。

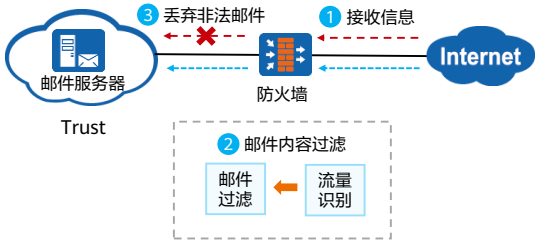


HUAWEI

- 具体查询流程如下：
  1. 防火墙收到SMTP消息后，提取发送方SMTP Server的IP地址；
  2. 防火墙将步骤1解析出来的IP地址和由第三方RBL服务器指定的RBL服务名放到一条信息中，向DNS Server发送解析请求。如，SMTP Server的源IP为1.2.3.4，RBL服务名为”sbl.spamhaus.org”，则防火墙将信息”4.3.2.1.sbl.spamhaus.org”发送给DNS Server；
  3. DNS Server收到防火墙发送的信息后，读取RBL服务名，解析出RBL服务器对应的IP地址，将查询请求转发给RBL服务器；
  4. RBL服务器收到DNS服务器转发的查询请求后，将结果以应答码的形式反馈给DNS Server。应答码是一个IP地址，标识此次RBL查询是否有结果；
  5. DNS Server将从RBL服务器获取的应答码转发给防火墙；
  6. 防火墙根据应答码判断来自该SMTP Server的邮件是否为垃圾邮件。
     - 如果从RBL服务器获得的应答码与防火墙上配置的应答码一致，该SMTP邮件将被视为垃圾邮件；
     - 如果从RBL服务器获得的应答码与防火墙上配置的应答码不一致，该SMTP邮件将被放行。

基于邮件内容过滤

- 防火墙作为安全网关时，所有的数据信息都要经过防火墙中转，防火墙在中转信息前，对信息进行检查，过滤掉包含非法邮件的信息。具体实现过程：
  1. 数据信息到达防火墙；
  2. 防火墙进行邮件内容过滤：
     - 流量识别：防火墙根据匹配条件（例如数据流量的源安全区域、目的安全区域、源地址、目的地址等）识别出要进行邮件过滤的流量；
     - 邮件过滤：防火墙分析出哪些流量包含邮件内容，检查邮箱地址、附件大小，识别出非法邮件；
  3. 丢弃包含非法邮件的信息。



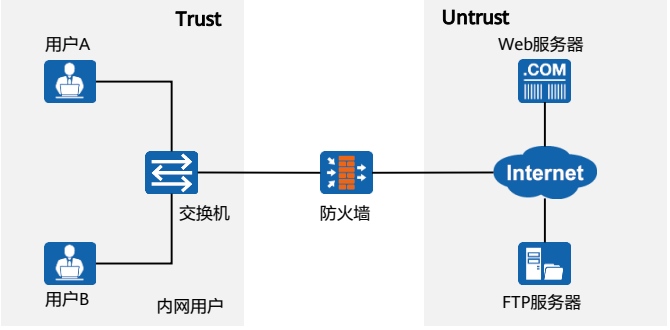
HUAWEI

- 匿名邮件检测、邮箱地址检查、邮件附件控制都是基于邮件内容的过滤，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。
- 邮件内容过滤检测方向分为发送方向和接收方向。
  - 如果邮件内容封装在SMTP消息中，防火墙执行发送方向检测。
  - 如果邮件内容封装在POP3消息或IMAP消息中，防火墙会判断为接收方向，执行接收方向的检测。

目录

应用行为控制应用场景

- 在企业内部通常需要对内网用户的HTTP行为和FTP行为进行管理，不同的用户使用HTTP和FTP访问网络资源需要不同的权限，同一用户在不同的时间段具有的权限往往也不同。
- 防火墙的应用行为控制功能可以对用户的HTTP行为、FTP行为和IM行为进行精确的控制，满足以上需求。

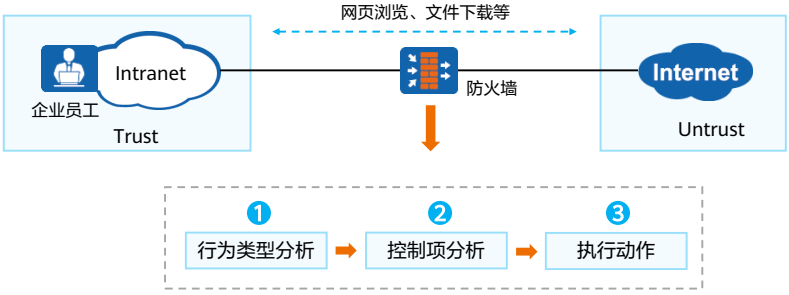


HUAWEI

- 防火墙作为企业的出口网关部署在内网出口处，通过在FW上配置应用行为控制功能，当内网用户访问外网时，能够有效管理内网用户的HTTP行为、FTP行为和IM行为。
- 在防火墙上创建多个应用行为控制配置文件，每个应用行为控制配置文件用来控制用户具有不同的HTTP、FTP和IM权限。然后通过在安全策略里面引用应用行为控制配置文件、用户和时间段（工作时间、非工作时间）等对象，可以达到对内网用户的HTTP行为、FTP行为和IM行为差异化、精细化管理的目的。

应用行为控制流程

- 与传统设备使用协议或端口号来控制HTTP和FTP协议不同，防火墙的应用行为控制功能可以对HTTP和FTP进行更精细的控制。
- 如图所示，防火墙通过分析行为类型，再执行应用行为控制项所对应的动作，甚至可以针对不同用户不同时间段进行控制。



HUAWEI

- 防火墙针对应用行为通过以下步骤进行控制：
  - 先进行行为类型分析，判断是哪一种行为类型（HTTP、FTP等）；
  - 再根据行为类型进行控制项分析，比如文件上传或下载；
  - 最后执行相应的动作（允许、禁止、告警或阻断）。

HTTP行为控制技术

行为类型	控制项	说明	动作
HTTP行为	POST操作	HTTP POST一般用于通过网页向服务器发送信息，例如论坛发帖、表单提交、用户名/密码登录。	允许/禁止
	浏览网页	采用浏览器进行网页浏览。	
	代理上网	代理上网是指用户使用代理服务器访问特定网站，使用该功能时防火墙需部署在内网用户和代理服务器之间。	
	文件上传/下载	上传或下载文件。	
	POST操作的内容大小(告警/阻断阈值)	当允许HTTP POST操作时，可以配置告警阈值和阻断阈值，对POST操作的内容大小进行控制。	告警/阻断
	文件上传/下载大小(告警/阻断阈值)	当允许文件上传操作时，可以配置告警阈值和阻断阈值，对上传/下载的文件大小进行控制。	

- 告警阈值：当上传或下载的文件大小、POST操作的内容大小达到告警阈值时，系统会产生日志信息对设备管理员进行提示。
- 阻断阈值：当上传或下载的文件大小、POST操作的内容大小达到阻断阈值时，系统将阻断上传或下载的文件、POST操作，并产生日志信息对设备管理员进行提示。
- 在创建安全策略时，可以把应用行为控制配置文件同用户、时间段等对象结合起来，达到不同用户、不同时间段的应用行为差异化管理的目的。

FTP行为控制技术

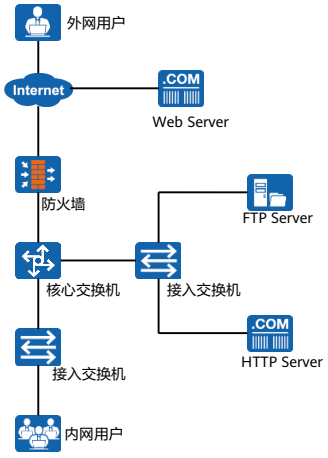
行为类型	控制项	说明	动作
FTP行为	文件上传	当允许文件上传操作时，可以配置告警阈值和阻断阈值，对上传的文件大小进行控制。	允许/禁止
	文件下载	当允许文件下载操作时，可以配置告警阈值和阻断阈值，对下载的文件大小进行控制。	
	文件删除	删除FTP服务器上的文件。	

- 缺省情况下，系统未配置告警阈值和阻断阈值，不对上传或下载的文件大小、POST操作的内容大小进行控制。
- 可以单独配置告警阈值或阻断阈值，也可以同时配置告警阈值和阻断阈值。同时配置告警阈值和阻断阈值时，告警阈值必须小于阻断阈值。

目录

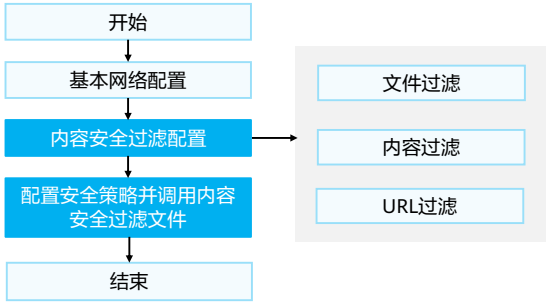
内容安全配置举例 - 需求描述

- 某公司在网络出口处部署了防火墙作为安全网关。公司希望在保证网络能够正常使用的同时实现以下需求：
  - 为了降低病毒进入公司内部的风险，禁止员工上传可执行文件到内网服务器；
  - 公司希望在保证网络正常使用的同时，防止内部员工泄露公司机密信息；
  - 某外网网站www.example.com疑似有安全隐患，内网员工不能访问该网站且不能访问社交网络等网站。



内容安全配置举例 - 配置思路

- 配置思路：
  - 配置设备的IP地址和路由，保证互联互通；
  - 配置文件过滤，禁止员工上传可疑文件；
  - 配置内容过滤，防止员工泄露机密信息；
  - 配置URL过滤，防止员工访问非法网站；
  - 配置URL远程查询，扩充本地的预定义URL分类库，便于下一次的快速查询；
  - 配置安全策略并调用内容安全过滤文件。



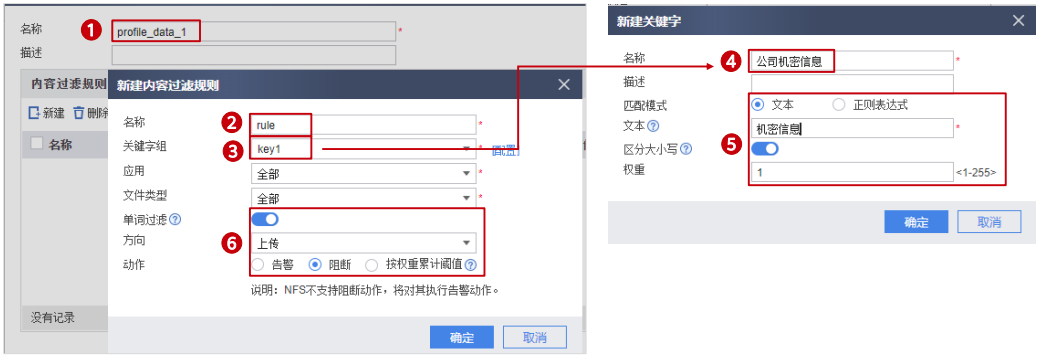
配置文件过滤

- 单击“对象 > 安全配置文件 > 文件过滤”，配置如下：
  - 新建文件过滤配置文件“profile_file_1”；
  - 新建文件过滤规则“rule1”，并配置策略，阻断可执行文件上传。

HUAWEI

配置内容过滤

- 单击“对象 > 安全配置文件 > 内容过滤”，配置如下：
  - 新建内容过滤配置文件“profile_data_1”和内容过滤规则“rule”；
  - 新建关键字组“key1”，并新建关键字“公司机密信息”，匹配文本“机密信息”。



HUAWEI

配置URL过滤 (1)

- 选择“对象 > 安全配置文件 > URL过滤”，新建URL过滤配置文件，过滤级别选择“自定义”。

HUAWEI

配置URL过滤 (2)

- 根据实际需求配置URL分类对应的动作（允许/告警/阻断），同时新建URL分类“untrust”，匹配URL“www.example.com”，动作设置为阻断。

HUAWEI

配置URL远程查询 (1)

- 为了保证本地防火墙能正常和远端服务器进行通信，需要配置安全策略，允许以下服务的流量通过防火墙：
  - 选择“对象 > 服务 > 服务 ”，创建自定义服务；
  - 选择“策略 > 安全策略 > 新建安全策略”，引用自定义服务。

HUAWEI

- 如需使用URL远程查询服务，请确保已完成以下其它工作：
  - License已经激活并且在有效服务期内；
  - 防火墙与sec.huawei.com路由可达；
  - 已配置DNS服务器地址，并可以正确解析sec.huawei.com。
- 说明：sec.huawei.com是华为安全中心平台网址。

配置URL远程查询 (2)

- 设置URL远程查询服务器的相关参数：
  - 选择“对象 > 安全配置文件 > 全局配置”。

引用内容安全配置文件

- 选择“策略 > 安全策略 > 安全策略 > 新建安全策略”：
  - 设置安全策略名称为“to_Internet”、配置源/目的安全区域，并引用内容安全配置文件。

思考题

1. （判断题）HTTP文件下载动作配置为禁止时，可以配置阻断阈值。（　　）
   A. 正确
   B. 错误
2. （多选题）内容安全过滤技术包括以下哪些选项？（　　）
   A. 文件过滤
   B. 内容过滤
   C. 邮件过滤
   D. 应用行为控制

1. B
2. ABCD

本章总结

- 本章主要介绍了内容安全过滤相关功能，通过在防火墙上部署内容安全过滤功能，可以对企业用户进行精细化管理和控制。例如：不允许访问非法网站，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；防止核心机密信息泄露，防患于未然等。
- 通过本课程的学习，您将了解相关安全过滤技术实现原理，能够独立配置华为防火墙URL过滤、文件过滤、内容过滤等功能。

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

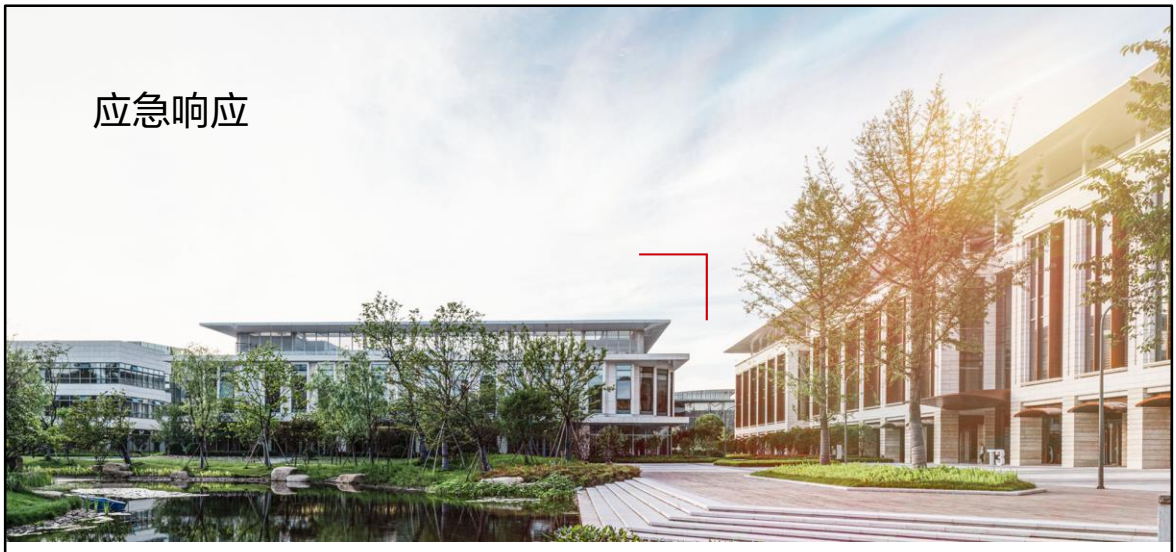
缩略语	英文全称	解释
DNS	Domain Name Service	网域名称解析服务
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure	加密的超文本传输协议
IM	Instant Messaging	即时消息
IMAP	Interactive Mail Access Protocol	交互邮件访问协议
NFS	Networked File System	标准文件协议
POP3	Post Office Protocol 3	邮局协议第3版
RBL	Real-time Blackhole List	实时黑名单列表
SMB	Server Message Block	服务器消息块
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
URL	Uniform Resource Locator	统一资源定位符

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.

应急响应



HUAWEI

前言

- 物联网、移动互联网、云计算、大数据、区块链等新兴技术的蓬勃发展，为整个IT行业注入了新的活力，提高了生产效率，为生活带来诸多便利。但是，新技术的出现也为网络攻击提供了新的攻击手段和途径，攻击范围逐年扩大，造成的影响也愈发严重，给网络安全带来新的挑战。
- 俗话说，“没有绝对安全的系统，也没有绝对安全的网络”。面对复杂多变的网络环境，我们急需建立一套行之有效的应急响应机制，确保企业、组织的网络安全，守住企业的数据资产。
- 本章主要介绍网络安全应急响应的相关流程和技术。

目标

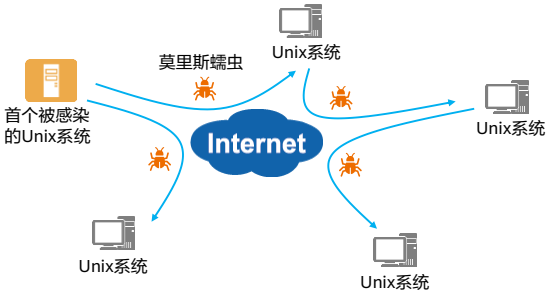
- 学完本课程后，您将能够：
  - 描述网络安全应急响应的基本概念
  - 描述网络安全应急响应的处理流程
  - 了解网络安全应急响应的相关技术

- 后文中，统一将“网络安全应急响应” 简称为“应急响应”。

目录

产生背景

- 1988年11月发生的莫里斯蠕虫病毒事件（Morris Worm Incident）致使当时的互联网络超过10%的系统不能工作。该案件轰动了全世界，并且在计算机科学界引起了强烈的反响。
- 为此，1989年，美国国防部高级研究计划署资助卡内基·梅隆大学建立了世界上第一个计算机紧急事件响应小组协调中心（Computer Emergency Response Team/Coordination Center）来应对网络攻击事件。



什么是应急响应

- 应急响应是一项需要充分准备和严密组织的工作。它必须避免不正确的操作、可能导致灾难性后果的动作、忽略关键步骤等情况发生。
- 应急响应的目标通常包括：采取紧急措施和行动，将业务恢复到正常服务状态；调查安全事件发生的原因，避免同类安全事件再次发生；在需要司法机关介入时，提供法律认可的数字证据等。

- 相关标准：
  - GB/T 24363-2009《信息安全技术 信息安全应急响应计划规范》
  - GB/T 20985.1-2017《信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理》
  - GB/T 20985.2-2020《信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南》
  - GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》
  - GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》

安全事件分类

- 分类分级是有效防范和响应信息安全事件的基础，能够使事前准备、事中应对和事后处理的各项工作更具针对性和有效性。
- 《国家网络安全事件应急预案》中对网络安全事件进行了分类。

分类	具体事件
有害程序事件	计算机病毒、蠕虫、特洛伊木马、僵尸网络、混合型程序攻击、网页内嵌恶意代码等。
网络攻击事件	拒绝服务攻击、后门攻击、漏洞攻击、网络扫描窃听、网络钓鱼、干扰事件等。
信息破坏事件	信息篡改、信息假冒、信息泄露、信息窃取、信息丢失事件等。
信息内容安全事件	通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。
设备设施故障	软硬件自身故障、外围保障设施故障、人为破坏事故等。
灾害性事件	由自然灾害等其他突发事件导致的网络安全事件。
其他事件类型	不能归为以上分类的网络安全事件。

安全预警与应急响应等级

- 《国家网络安全事件应急预案》明确了《网络安全法》第五章“检测预警和应急预案”的具体实践方案，并将网络安全事件分为四级，对应四级预警等级和四级应急响应等级。

网络安全事件等级	预警等级	应急响应等级
特别重大网络安全事件	红色预警	I级响应
重大网络安全事件	橙色预警	II级响应
较大网络安全事件	黄色预警	III级响应
一般网络安全事件	蓝色预警	IV级响应

- 《国家网络安全事件应急预案》适用于网络安全事件的应对工作。其中，有关信息内容安全事件的应对方法，各单位或公司需根据具体情况另行制定专项预案。
- 不同类型的应急预案，对于安全事件等级、预警等级以及应急响应等级定义的范围不同，可参考《国家网络安全事件应急预案》进行学习和理解，规定如下：
  - 特别重大网络安全事件：
    - 重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力；
    - 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁；
    - 其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。
  - 重大网络安全事件：
    - 重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响；
    - 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁；
    - 其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

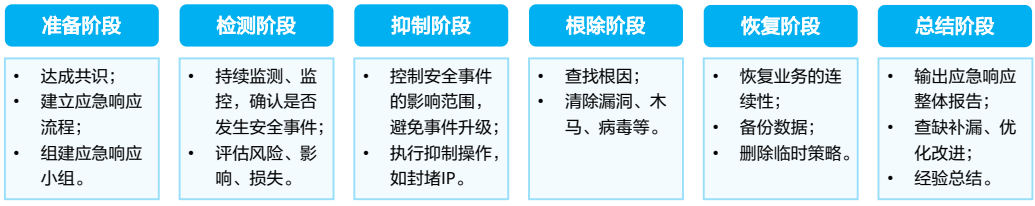
- 较大网络安全事件：
  - 其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件；
  - 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁；
  - 其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。
- 一般网络安全事件：
  - 除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。

- 预警响应：
  - 红色预警启动Ⅰ级响应：
    - 应急办组织预警响应工作，联系专家和有关机构，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作；
    - 有关部门网络安全事件应急指挥机构实施24小时值班，相关人员保持通信联络畅通，并加强网络安全事件检测和事态发展信息搜集工作。组织应急支撑队伍开展应急处置或准备，风险评估和控制等工作；
    - 国家网络安全应急技术支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆，设备，软件工具等处于良好状态。
  - 橙色预警启动Ⅱ级响应：
    - 有关部门网路安全事件应急指挥机构启动相应预案，组织展开预警响应工作，做好风险评估，应急准备和风险控制工作；
    - 有关部门及时将事态发展情况报告应急办，应急办密切关注事态发展，有关重大事项及时通报相关部门；
    - 国家网络安全应急技术支撑队伍保持联络畅通，检查应急车辆，设备，软件工具等处于良好状态。
  - 黄色和蓝色预警启动Ⅲ级响应和启动IV级响应：
    - 有关地区和部门网络安全事件应急指挥机构启动相应应急预案，指导组织开展预警响应。

目录

应急响应阶段划分

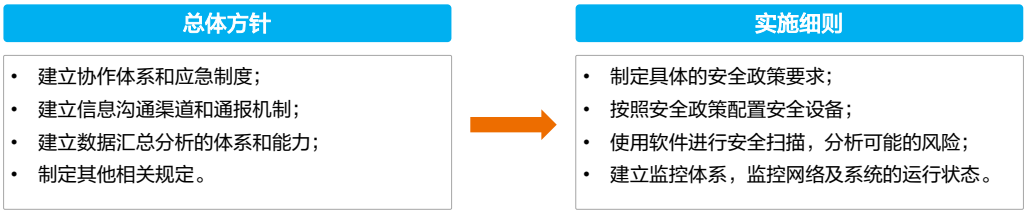
- 网络安全应急响应预案能够在网络安全事件发生后，快速、高效的跟踪、处理与防范各类安全事件，确保企业/组织的信息安全。网络安全应急响应流程可分为以下几个阶段。



- 应急响应处理流程并非固定不变，需要应急响应服务人员在实际中灵活变通，可适当简化，但任何变通都必须纪录有关的原因。
- 规范性引用文件：
  - GB/T 20984-2007《信息安全技术 信息安全风险评估规范》
  - GB/T 20985.1-2017《信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理》
  - GB/T 20985.2-2020《信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南》
  - GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》
  - GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》
  - GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》
  - GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》

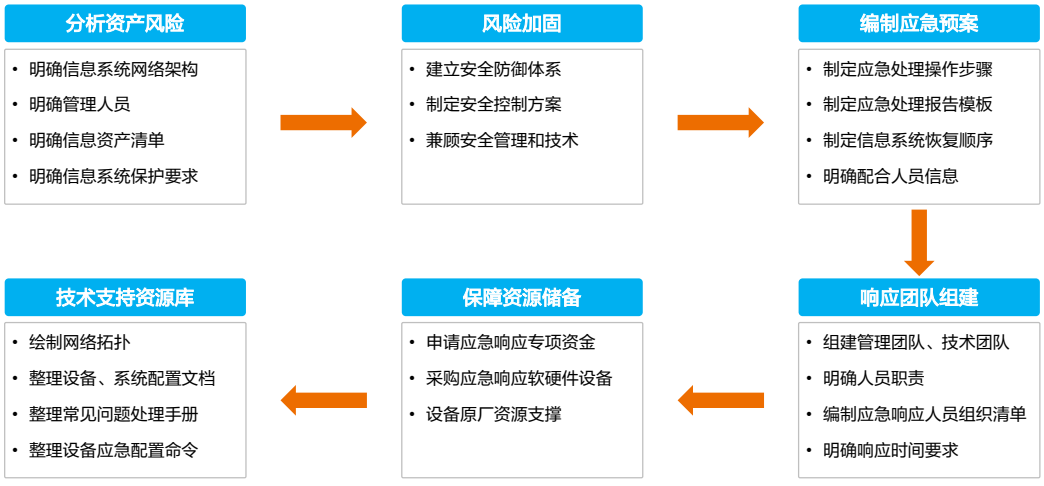
准备阶段

- 在网络安全事件发生前，对可能发生的安全事件进行评估，制定相应的应急策略和预案。



- 在准备阶段，我们需要定制具体的应急响应计划，并进行相应的资源准备，如：
  - 人员：应急操作人员、技术专家，以及硬件厂家、软件系统的支撑人员。
  - 部署相关软硬件设备（安全设备）：用于安全检测以及后续的溯源分析。
  - 业务连续性的保障：组建业务的灾容系统。

准备阶段内容细则



检测阶段

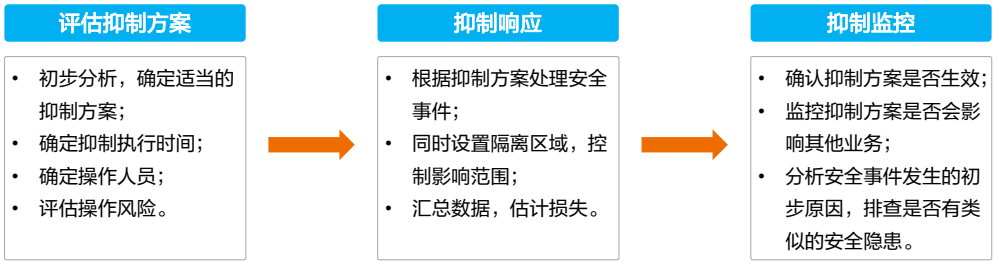
- 检测阶段：检测并确认安全事件的发生，判断事件性质和影响。
- 一般检测流程如下：

HUAWEI

- 检测阶段：在紧急事件发生前，产生安全的预警报告；在紧急情况发生时，产生安警报，并报告给应急响应中心。应急响应中心根据事件的级别，采取响应的措施。
- 在检测阶段我们会通过相应的技术手段以及现象，判断是否有安全事件发生，如：业务系统访问异常，存在异常的网络流量，大量可疑邮件等，同时通过安全检测设备（如IPS、沙箱），主机上的防病毒软件，业务主机的日志等综合判断是否有安全事件发生。

抑制阶段

- 抑制阶段主要从多个方面采用必要手段对网络攻击进行限制，尽可能把攻击限制在一定范围内，降低损失。
- 当确认安全事件发生时，启动应急响应预案，根据预先制定的规则，采取应急措施。抑制流程如下：



HUAWEI

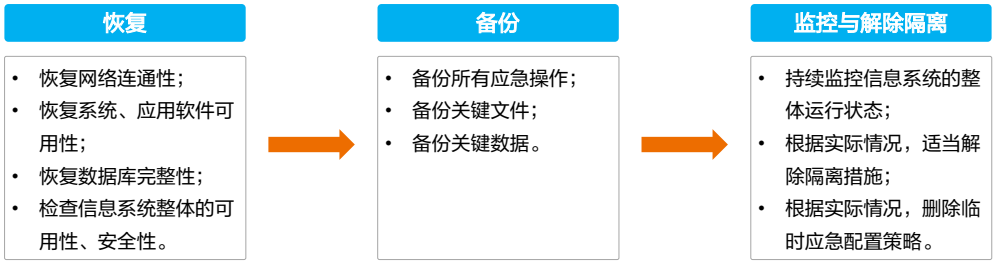
- 根据不同的场景，抑制阶段采取的动作不同，常见抑制动作如下：
  - 确定适当的遏制方法，如阻断正在发起攻击的行为，缓解系统的负载，通过路由器、防火墙封堵入侵的源地址，隔离被病毒感染的系统等；
  - 修改所有防火墙和路由器的过滤规则，拒绝来自看起来是发起攻击的主机的流量；
  - 封锁或删除被攻击的登录账号；
  - 提高系统或网络行为的监控级别；
  - 设置蜜罐并关闭被利用的服务；
  - 汇总数据，估算损失和隔离效果。

根除阶段

- 根除阶段：找出导致安全事件发生的根因，采用相应措施彻底根除类似的安全隐患。
- 根除阶段一般流程如下：

恢复阶段

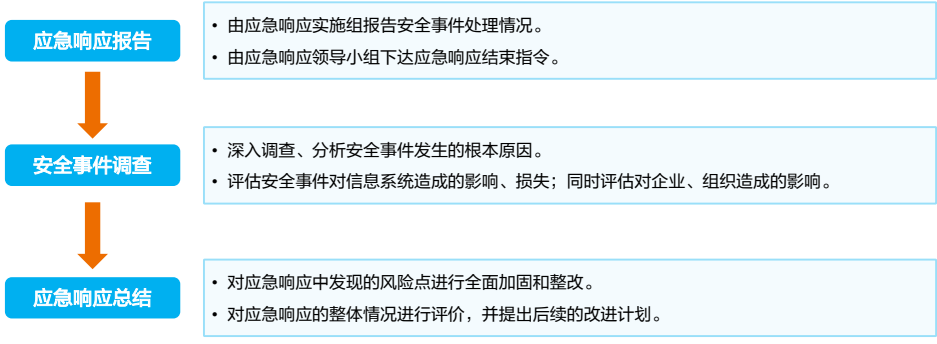
- 恢复阶段：恢复被入侵、破坏的网络、系统、应用、数据库等信息资产，并及时备份、解除隔离等。
- 恢复阶段具体工作如下：



- 可恢复程度依赖于前期准备是否充分、攻击的破坏程度，以及信息系统的备份情况。

总结阶段

- 总结阶段：从已发生的安全事件出发，吸取安全事件响应过程中的经验教训，回顾并总结发生安全事件的相关信息。
- 总结阶段具体工作如下：



目录

应急响应技术

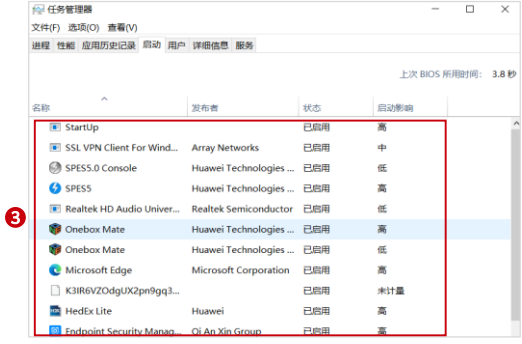
- 应急响应技术是指在应对网络攻击事件过程中使用的技术和方法。
- 在应急响应流程的检测、抑制、根除和恢复阶段均需要使用应急响应技术，常见的应急响应技术有：

文件排查	• 查看是否存在攻击者留下的异常文件，或者系统关键文件，判断业务主机是否被入侵。
进程排查	• 查看是否存在异常进程，判断业务主机是否被入侵、植入木马或后门程序等。
系统信息排查	• 查看系统的环境变量，定时任务等，判断是否存在攻击者添加的变量以及任务。
日志分析	• 分析是否有攻击者登陆以及攻击过的痕迹，同时也可用于溯源分析和取证。

- 文件排查、进程排查及系统信息排查，下文分别针对Windows及Linux系统来介绍。
- 其他应急响应技术有：
  - 用户分析：查看用户登录记录，是否被添加了攻击者用于后门登录的非法账号。
  - 网络连接分析：查看是否存在异常的网络连接，一些常见的后门连接都有固定的端口号，可通过网络连接判断出系统是否被攻击的可能。

文件排查 (1)

- 系统异常启动文件排查：在Windows系统中执行“开始 > 运行 > msconfig”，在打开的界面中查看系统启动项，检查是否有未知异常启动项。



文件排查 (2)

- 检查系统中各个磁盘的Temp（或tmp）相关目录（如C:\Windows\Temp）下是否存在异常文件（如后缀为.exe的可执行文件），该目录通常存放Windows系统产生的临时文件，可能被攻击者利用。

Windows主机 Linux主机

文件排查 (3)

- 检查系统中最近使用的文件，在“开始 > 运行 > %UserProfile%\Recent”中打开Recent文件夹，按照“修改日期”进行排序，检查最近修改的文件中是否有未知异常文件。

HUAWEI

- 在该步骤可以右键查看文件的“创建时间”、“修改时间”、“访问时间”，一般黑客会对文件的“修改时间”做改动，以绕过检测，如果文件的修改时间在创建时间之前，大概率为可疑文件。
- 在此处还可以判断是否存在一些Windows系统文件被修改，如.dll结尾的文件（一般在system路径下）。

进程排查 (1)

- 常见的木马、病毒、恶意代码通常会依赖网络进行传播，进而感染局域网中的大量终端。通过进程排查，确认是否存在一些病毒常用的端口。
- 在进程排查中，可以使用系统自带的网络连接分析工具（netstat）进行网络连接分析。netstat命令使用介绍如下：

```
netstat –{a,n,o,r,s}
        -a      显示所有网络连接、路由表和网络接口信息
        -n      以数字形式显示地址和端口号
        -o      显示与每个连接相关的所属进程 ID
        -r      显示路由表
        -s      显示按协议统计信息、默认地、显示IP
```

Windows主机 Linux主机

进程排查 (2)

- netstat命令输出示例如下：

```
C:\Users\PC1> netstat -ano
  活动连接
```

协议	本地地址	外部地址	状态	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	900
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1028
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	5516
TCP	0.0.0.0:8900	0.0.0.0:0	LISTENING	2848
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	680
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	524
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1204
TCP	127.0.0.1:8900	127.0.0.1:49669	ESTABLISHED	2848
TCP	127.0.0.1:8900	127.0.0.1:49672	ESTABLISHED	2848
TCP	127.0.0.1:8900	127.0.0.1:49673	ESTABLISHED	2848

- PID为Process ID，即进程的ID信息。
- netstat命令输出的常见状态说明：
  - LISTENING，侦听状态；
  - ESTABLISHED，建立连接；
  - CLOSE_WAIT，对方主动关闭连接或网络异常导致连接中断。

Windows主机 Linux主机

进程排查 (3)

- 根据端口号发现异常连接后，使用tasklist命令定位进程名称。

```
C:\Users\PC1> tasklist | findstr 3816   ——→ PID
spoolsv.exe              3816 Services              0     17,452 K
```

- 使用wmic process命令获取进程的全路径信息。

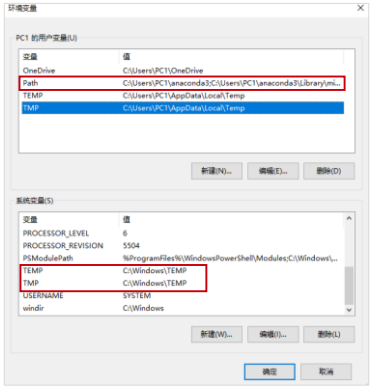
```
C:\Users\PC1> wmic  process | findstr spoolsv.exe   ——→ 进程名称
spoolsv.exe
                                                          Win32_Process      20211028123614.065414+480
Win32_ComputerSystem  DESKTOP-DUOAB0V  spoolsv.exe
                                                        3816    702                    157812500
spoolsv.exe              Win32_OperatingSystem  Microsoft Windows 10 ???|C:\Windows|\Device\Harddisk0\Partition3
141847          1823255          566354      9500        640          12404           2203474538496    27668
8       9728000         3816      29                    209              34                      225                    31270
11761418         0                           7          97500000      2203462455296  10.0.19042      17870848        138386
7831604
```


HUAWEI

Windows主机 Linux主机

系统信息排查 (1)

- 检查Windows系统的环境变量（系统变量、用户变量）是否存在异常。例如：查看系统变量“TEMP”或“TMP”的值是否为“C:\Windows\TEMP”，用户变量“Path”中是否添加了其他的非法路径。



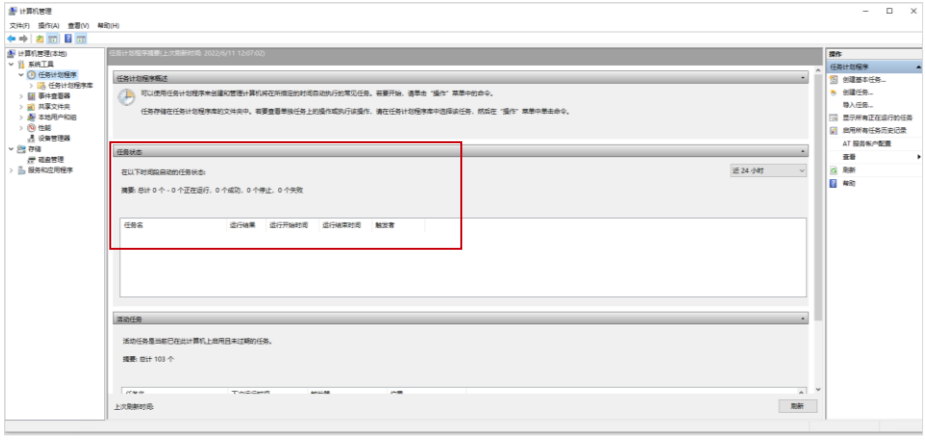
HUAWEI

- 环境变量查看：“我的电脑 > 属性 > 高级系统设置 > 高级 > 环境变量”。

Windows主机 Linux主机

系统信息排查 (2)

- 在“此电脑 > 管理 > 系统工具 > 任务计划程序”中查看是否存在非用户自己创建的任务计划程序。



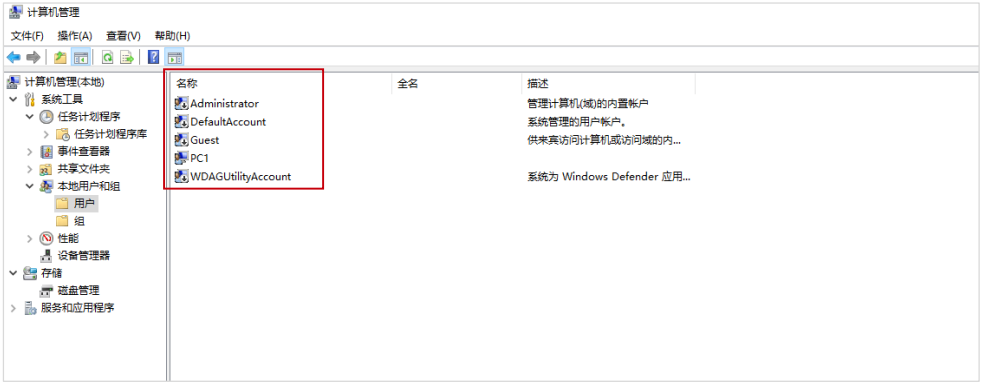
HUAWEI

- 本页的路径示例以Windows 10系统为例。

Windows主机 Linux主机

系统信息排查 (3)

- 在“此电脑 > 管理 > 系统工具 > 本地用户和组”中查看是否存在隐藏帐号，用户名以$结尾的为隐藏用户。



HUAWEI

- 除此以外，还可以在命令行中使用命令查询用户信息，如使用“query user” 命令可以查看系统当前已登录用户的会话连接，以判断是否有人正在远程登录该终端。

文件排查 (1)

- 使用ls命令查看/tmp、/usr/bin、/usr/sbin等目录是否存在异常文件，如后缀为.sh的脚本文件。

```
[root@iMaster-NCE ~]# ls -alt /tmp/
total 116
drwx------   2  omm       wheel     4096   17:13 hsperfdata_omm
drwxrwxrwx. 11  root      root      20480  17:13 .
drwx------   2  ommdba    wheel     4096   17:13 hsperfdata_ommdba
-rw-------   1  omm       wheel     3002   17:13 report.json
-rwxrwxrwx   2  sysus     sysus     23570  17:13 sysauto.sh        //可执行脚本文件需要重点排查
-rw-r--r--   1  root      root      30044  17:13 cronlock.log
drwxr-x---   2  omm       wheel     4096   17:12 omm
drwxr-x---   2  ossadm    ossgroup  4096   17:08 hsperfdata_ossadm
drwxr-x---   2  ossuser   ossgroup  4096   16:31 hsperfdata_ossuser
```

文件排查 (2)

- 查看开机启动项，重点检查是否存在异常程序被加入开机启动项。

```
[root@iMaster-NCE ~]# ls -alt /etc/init.d/          //此目录存放开启启动项文件
total 52
drwxr-xr-x.  10 root root   4096    12:58 ..
drwxr-xr-x.  2   root root   4096    20:28 .
-rwxr-x---    1  root root   658     20:28  ossipmc01
-rw-r-----    1  root root   46      20:20  boot.local
-rw-r--r--.   1  root root   18325   20:21  functions
-rwxr-xr-x.   1  root root   9363    20:21  network
-rw-r--r--.   1  root root   1161    20:21  README
```


- /etc/init.d是/etc/rc.d/init.d的软链接，是Linux的系统启动目录。

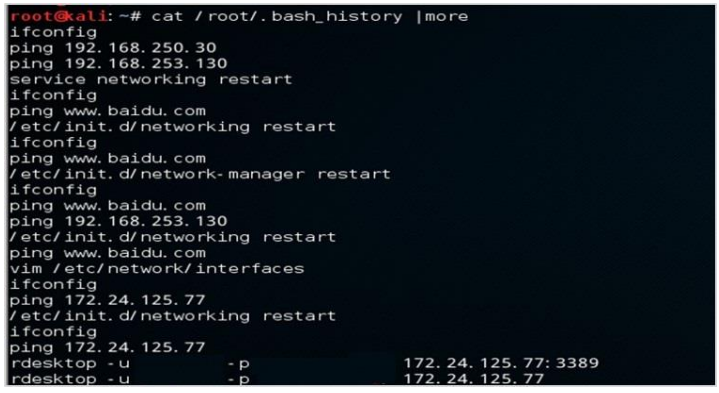
文件排查 (3)

- 查看特定目录下的文件，以时间排序，确定是否有文件被恶意改动，如查看/bin、/sbin、/usr/bin、/usr/sbin等系统关键目录。

```
[root@iMaster-NCE sbin]# ls -alt | head -n 10        //仅显示前10行输出
total 50768
dr-xr-xr-x.  2 root root   20480 12:04  .
lrwxrwxrwx.  1 root root      26 12:47  ebtables -> /etc/alternatives/ebtables
lrwxrwxrwx.  1 root root      24 12:47  ifdown -> /etc/alternatives/ifdown
lrwxrwxrwx.  1 root root      22 12:47  ifup -> /etc/alternatives/ifup
lrwxrwxrwx.  1 root root      27 12:47  ip6tables -> /etc/alternatives/ip6tables
lrwxrwxrwx.  1 root root      35 12:47  ip6tables-restore -> /etc/alternatives/ip6tables-restore
lrwxrwxrwx.  1 root root      32 12:47  ip6tables-save -> /etc/alternatives/ip6tables-save
lrwxrwxrwx.  1 root root      26 12:47  iptables -> /etc/alternatives/iptables
lrwxrwxrwx.  1 root root      34 12:47  iptables-restore -> /etc/alternatives/iptables-restore
```

文件排查 (4)

- 查看用户的历史命令记录文件。在Linux系统中，用户执行过的命令均会保存在该用户home目录下的“.bash_history”文件中，通过查看该文件，检查此用户是否执行过异常命令。



- 当安全事件发生时，可通过该文件查询用户执行的历史命令，判断是否存在过异常操作，恶意命令。之后可以根据执行该操作的用户信息进行下一步的排查。

Windows主机 Linux主机

文件排查 (5)

- Linux系统中所有的用户名信息被存放在“/etc/passwd”文件中，通过检查此文件，可以判断是否存在非法用户名。此文件也可以查看用户的登陆权限，如“/sbin/nologin”代表用户不可登陆。

```
[sopuser@iMaster-NCE ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
ftpuser:x:4001:2000::/opt/backup/ftpboot:/usr/libexec/openssh/sftp-server
sopuser:x:3008:2000::/home/sopuser:/bin/bash
dbuser:x:3002:1999::/home/dbuser:/bin/bash
tcpdump:x:72:72::/:/sbin/nologin
```

第一列代表用户名

最后一列代表用户登陆权限

- 若发现一个异常用户，并且最后一列为nologin，可继续查询该用户的历史执行命令，通过查询该用户的.bash_history文件判断是否存在异常命令执行。

Windows主机 Linux主机

进程排查 (1)

- 使用top命令可以实时动态地查看系统的整体运行情况，检查是否有异常进程占用大量CPU和内存资源。

```
top- 18:24:39 up 56 days, 21:59,  1 user,  load average: 29.33, 27.29, 27.78
Tasks: 1094 total,   6 running, 1086 sleeping,   0 stopped,   2 zombie
%Cpu(s): 41.3 us, 12.8 sy,  0.0 ni, 44.6 id,  0.0 wa,  0.8 hi,  0.5 si,  0.0 st
MiB Mem : 257185.4 total,   6202.1 free,  98947.1 used, 152036.2 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used. 145111.7 avail Mem
   PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
190837 omm       20   0   35.7g 492048  45900 S 220.9   0.2   0:06.76 java
 15062 ossuser   20   0   17.5g   1.4g  18912 S 220.6   0.6  65690:23 java
117849 omm       20   0 8510652 900868  77220 S 113.4   0.3  84099:47 java
182155 dbuser    20   0 2136612   1.2g  15848 S 102.9   0.5  22028:32 zengine
221290 ossuser   20   0 9917328   3.9g  32708 S  33.3   1.6  26992:00 java
 55004 ossadm    20   0  885908  95656  12940 S  18.0   0.0  14357:43 python
182557 dbuser    20   0 3236032   1.9g  16092 S  14.1   0.8   4739:08 zengine
```


HUAWEI

- 显示的CPU利用率为所有核心相加，所以会超过100%，如一个应用程序在四个核心上都使用了30%的CPU资源，那么在显示中将会超过100%。
- top显示结果参数含义：
  - PID：进程ID；
  - USER：所属用户；
  - PR：优先级；
  - NI：nice值，负值表示高优先级，正值表示低优先级；
  - SHR：共享内存大小，单位kb；
  - S：进程状态。其中S代表睡眠；
  - %CPU：CPU占用率；
  - %MEM：进程使用的物理内存百分比；
  - TIME+：进程使用的CPU时间总计，单位1/100秒；
  - COMMAND：命令名/命令行。

Windows主机 Linux主机

进程排查 (2)

- 使用netstat命令查看网络连接，检查是否存在可疑的监听端口。

```
[root@iMaster-NCE ~]# netstat -antlp | more
Active Internet connections (serversand established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.10.103:22885    0.0.0.0:*               LISTEN      143720/java
tcp        0      0 192.168.10.103:22853    0.0.0.0:*               LISTEN      97346/java
tcp        0      0 127.0.0.1:25925         0.0.0.0:*               LISTEN      150759/java
tcp        0      0 192.168.10.103:27333    0.0.0.0:*               LISTEN      76275/traffic_manag
tcp        0      0 192.168.10.103:26533    0.0.0.0:*               LISTEN      186711/redis-server
tcp        0      0 192.168.10.103:26661    0.0.0.0:*               LISTEN      186090/redis-server
tcp        0      0 192.168.10.103:21093    0.0.0.0:*               LISTEN      117849/java
tcp        0      0 127.0.0.1:22501         0.0.0.0:*               LISTEN      65649/java
tcp        0      0 127.0.0.1:20006         0.0.0.0:*               LISTEN      101554/java
```


HUAWEI

- 命令netstat的参数含义：
  - -a，显示所有连线中的Socket；
  - -n，直接使用IP地址，而不通过域名服务器；
  - -t，显示TCP传输协议的连线状况；
  - -u，显示UDP传输协议的连线状况；
  - -v，显示指令执行过程；
  - -p，显示正在使用Socket的程序识别码和程序名称；
  - -s，显示网络工作信息统计表。
- 上文显示中的Recv-Q，Send-Q代表接收队列和发送队列。

Windows主机 Linux主机

进程排查 (3)

- 若从“top”或“netstat”命令的输出显示中发现异常进程，可以进一步使用“ps”命令查看进程的详细信息。可以搭配管道符“|”和“grep”命令对输出信息进行过滤，仅显示某一进程的信息。

```
[root@iMaster-NCE ~]# ps -aux | grep 166878
dbuser   166878  0.0  0.0 253532  5372 ?        Ssl  Apr14  77:36 /opt/redis/bin/redis-server 192.168.10.103:26532
root     241285  0.0  0.0 213136  828 pts/2     S+   21:09   0:00 grep --color=auto 166878
```

进程ID

HUAWEI

- “ps”命令的参数含义：
  - -a，显示所有用户的进程；
  - -u，显示用户名或者用户ID；
  - -x，显示所有进程，不以终端机来区分。

系统信息排查 (1)

- 通过“crontab”命令查看是否存在异常的定时任务。

```
[root@iMaster-NCE ~]# crontab -l
0 */2 * * * /bin/bash /etc/timing_task.sh        //定时任务
```

- 通过查看“/etc/rc.local”文件，检查是否存在异常的开机启动程序。

```
[root@iMaster-NCE ~]# cat /etc/rc.local          //开机自动执行rc.local文件
touch /var/lock/subsys/local
systemctl stop ntpd
ntpdate 192.168.10.103 >>/var/log/NCE/logs/time_sync.log
hwclock
systemctl start ntpd
iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP
iptables -A OUTPUT -p icmp --icmp-type timestamp-reply -j DROPd
```

系统信息排查 (2)

- 查看系统中所有用户的最近一次登陆时间，检查最近是否有异常的用户登陆情况。

```
[root@iMaster-NCE ~]# lastlog
Username         Port     From             Latest
root             pts/2                     Fri Jun10  21:03:02 +0800 XXXX      //此处XXXX代表年份
bin                                        **Never logged  in**
daemon                                     **Never logged  in**
adm                                        **Never logged  in**
```

- 查看“$PATH”环境变量，检查是否存在非法路径、风险路径等。

```
[root@iMaster-NCE ~]# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin
```

日志分析

- 日志是设备、系统在运行过程中产生的记录信息，这些信息记录了设备、业务系统的历史运行状况，包括正常信息、异常信息等。通过查看日志，可以了解某段时间内设备、业务系统的整体运行状态，同时还能够在发生安全事件后，进行溯源取证。

信息记录	• 日志记录计算机软硬件运行过程中的大量信息，可用于问题分析、业务统计、提供决策依据等。
故障定位	• 通过日志记录，可以帮助工程师定位故障原因，缩短故障排查时间，提高运维效率。
故障分析	• 故障恢复后，查看全过程的日志记录，有助于分析故障根因，为后续优化整改提供参考依据。
攻击溯源	• 网络攻击行为通常都留有一定攻击痕迹，通过查看日志，可以发现攻击的源头和攻击方式。

- 以安全设备为例，系统日志会记录下各种攻击事件，包括攻击源IP、攻击特征、是否被阻断等。
- 以操作系统为例，系统日志会记录下系统整体信息、用户登录/授权信息、安全事件信息等。
- 以业务系统为例，业务日志会记录下用户的各种访问行为。例如：一台Nginx服务器，其业务日志通常会记录访问者的IP地址、请求类型、请求时间等信息，可用于故障定位、攻击回溯等场景。

日志格式 - 网络设备

- 网络设备的系统日志通常以syslog形式存储，如路由器、交换机、防火墙等，具备较好的阅读性。
- 日志格式说明：
  - Jul XX XXXX 15:55:06：时间戳，该条日志产生的时间；
  - SW4-S57：设备名称，产生该日志的设备名称；
  - %%01：厂家标志，其中%%为固定字段，01字段代表特定厂家；
  - IFNET：业务模块名称，代表该日志所属的业务功能模块；
  - 4：日志等级，取值范围是0~7，数字越小代表日志对应的严重程度越高；
  - IF_ENABLE(l)[68]：信息摘要，该日志的概述信息；
  - Interface GigabitEthernet0/0/1 has been available.：日志内容。

Jul XX XXXX 15:55:06 SW4-S57 %%01 IFNET/4/IF_ENABLE(l)[68]:Interface GigabitEthernet0/0/1 has been available.

- 除syslog外，传统通信设备、安全设备的日志格式还有二进制、dataflow、netflow等格式，这些格式设计的初衷更多是为了方便计算机处理以及在网络上进行传输，并不适合工程师阅读，因此在安全攻击溯源中使用syslog进行分析更为常见。

日志格式 - Windows系统

- 在Windows主机的“事件查看器”中可查看Window日志。常见的日志有系统日志、安全日志、设置日志、应用程序日志等。

HUAWEI

- 在Windows日志中可以看到诸如：日志名称（log name）、日志来源（source）、事件ID（event ID）、级别（level）、用户（user）、记录时间（logged）等信息。
- 为方便处理以及分析，可将Windows日志另存为文本文件，之后使用文本编辑器打开，进行搜索，查看特定源IP进行日志过滤。

日志格式 - Linux系统

- Linux系统通常将不同类型的日志分别存储在不同的目录下，Linux系统常见的日志类型如下表所示：

日志类型	说明
/var/log/messages	记录整体系统信息。
/var/log/auth.log	记录系统授权信息，包括用户登录和使用的权限机制等。
/var/log/userlog	记录所有等级用户信息的相关日志。
/var/log/cron	记录crontab命令执行情况的相关日志。
/var/log/vsftpd.log	记录Linux FTP应用的相关日志。
/var/log/lastlog	记录用户最近一次登录的日志信息，可以使用命令lastlog查看。
/var/log/secure	记录大多数应用输入的账号与密码，以及登录成功与否的相关日志。
/var/log/wtmp或/var/log/utmp	记录成功登录系统的账户信息。
/var/log/faillog	记录未成功登录系统的账号信息。

- 某Linux服务器的日志示例如下：

```
Jun XX XXXX 18:22:35 iMaster-NCE sudo[260687]:     omm : TTY=unknown ; PWD=/opt/huawei/Bigdata/om-server_8.0.2.1/OMS/workspace0/ha/module/harm/plugin/script ; USER=root ; COMMAND=/var/lib/sudo/Bigdata/sudo/runtime/sudoExecute.sh  m_arping bond0 192.168.10.103
```

通过日志进行溯源取证 (1)

操作系统日志

Linux系统中“/var/log/secure”日志：

```
[root@iMaster-NCE log]# tail -n 10 secure
Jun 16 10:19:17 iMaster-NCE su[188909]: pam_unix(su-l:session): session opened for user ommdba by (uid=0)
Jun 16 10:19:17 iMaster-NCE su[188909]: pam_unix(su-l:session): session closed for user ommdba
Jun 16 10:19:17 iMaster-NCE su[188950]: pam_unix(su-l:session): session opened for user omm by (uid=0)
Jun 16 10:19:17 iMaster-NCE su[188950]: pam_unix(su-l:session): session closed for user omm
```

- “/var/log/secure”日志包含验证和授权方面信息，通过查看该日志，可以了解是否有人尝试暴力破解登录主机。
- 通过操作系统日志，可分析是否存在可疑用户登录，判断系统是否已经被侵入并留下了后门账号。

业务系统日志

应用程序Nginx中的“access.log”日志：

```
192.168.10.103 - - [XX/Apr/XXXX:09:14:15 +0800] "GET /campusLogin/images/logo_huawei.ico?v=1649983171392 HTTP/1.1" 200 1150 "https://10.154.176.119:8447/unisso/login.action?service=%2Funisess%2Fv1%2Fauth%3Fservice%3D%252FcampusNCE%252FcampusNCEIndex.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36" "192.168.10.200" - 0.000 -
```

- “access.log”日志会记录用户的访问信息，包括访问者IP地址、访问时间、HTTP请求方法与URL、客户端类型等。
- 通过业务系统日志（如Apache、Nginx）可判断是否存在攻击行为，如注入攻击，脚本执行等。

通过日志进行溯源取证 (2)

安全设备日志

IPS设备中的syslog日志：

Jun XX XXXX 11:12:13 FW3 %%01IPS/4/DETECT(l)[0]:An intrusion was detected. (SyslogId=1, VSys="public", Policy="pass", SrcIp=100.100.1.10, DstIp=10.3.0.100, SrcPort=55411, DstPort=80, SrcZone=trust, DstZone=trust, User="unknown", Protocol=TCP, Application="HTTP", Profile="icmp", SignName="SQL Injection Attack - Bool-Based Blind Injection", SignId=6159300, EventNum=1, Target=server, Severity=medium, Os=all, Category=Injection, Reference=NA, Action=Block)

- IPS日志记录了攻击的源目IP地址、协议号、源目端口号、应用类型、所匹配的签名等信息。
- 通过查看安全设备日志，可以判断信息系统是否遭受了入侵，以便制定有效措施，抵御攻击。同时可以根据日志信息进行溯源取证。

目录

WannaCry应急响应 - 检测阶段 (1)

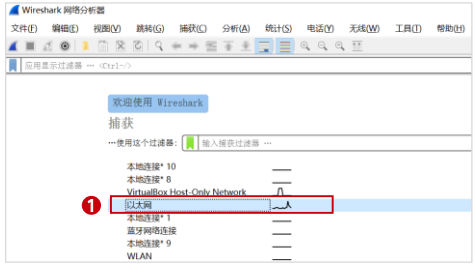
- 当组织遭受到WannaCry病毒攻击后，通过华为HiSec Insight安全态势感知系统的告警信息或者从组织内部员工的反馈可以得知病毒攻击的发生。
- 如下图所示，HiSec Insight显示高危的病毒攻击已经成功突破。应急响应相关人员需要及时对安全事件进行定级上报，若有应急响应预案，则启动预案；若无预案，则按照应急响应流程采取措施。

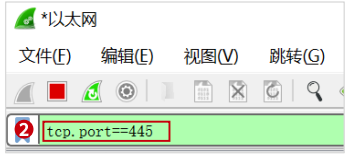
HUAWEI

- 针对金融、政府、运营商等大、中、小型企业，华为推出基于大数据的APT防御产品HiSec Insight高级威胁分析系统（简称HiSec Insight），能够对网络中的流量及各类设备的网络、安全日志等海量网络基础数据执行有效采集，通过大数据实时及离线分析，结合机器学习技术、专家信誉库、情报检索，有效的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。

WannaCry应急响应 - 检测阶段 (2)

- 全面排查网络中的病毒感染情况：
  - IPS检测：将流量镜像到IPS设备，并配置检测策略；
  - 抓包分析：通过Wireshark抓包，分析网络流量；
  - 利用其他专用检测工具进行检测。
- 网络层抓包分析步骤：
  - 将待检测PC接入网络，打开445端口；
  - 使用Wireshark，监控本地网络；
  - 设置流量过滤规则tcp.port==445，抓取流量；
  - 分析流量是否存在异常。





WannaCry应急响应 - 抑制阶段 (1)

- 检测到病毒攻击发生后，需要立刻抑制病毒的扩散，通常采取以下措施：
  - 隔离已知感染主机，禁止其接入网络；
  - 隔离网络，在防火墙/路由器等设备上封堵445端口，防止蠕虫病毒在网络间进一步传播。

防火墙封堵SMB协议

路由器封堵TCP 445端口

```
<Huawei> system-view
[Huawei] acl number 3001
[Huawei-acl-3001] rule deny tcp destination-port eq 445
[Huawei-acl-3001] rule permit ip
```

注：需要在路由器相应的接口引用此ACL。

WannaCry应急响应 - 抑制阶段 (2)

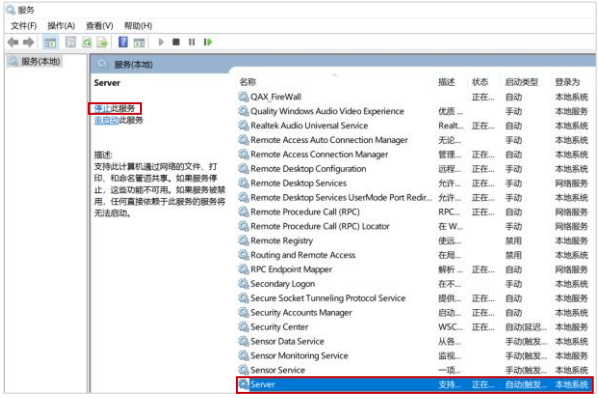
- 使用线下组织/及时通信软件/短信/邮箱等方式进行内部通告，组织员工配合采取应急响应措施：
  - 隔离被感染的主机：若主机为有线网络连接，可以拔除网线；若主机为无线网络连接，则断开无线网络。
  - 自行检查办公PC是否已感染病毒，检查文件后缀是否为“.wncry”，是否提示勒索界面。
    - 若PC已感染病毒，需要立即上报，由专业网络安全工程师进行后续处理；
    - 若PC暂未感染病毒，建议第一时间对系统进行加固。

WannaCry应急响应 - 抑制阶段 (3)

- 未感染病毒的Windows主机系统加固：配置防火墙策略，封堵TCP 445端口。

WannaCry应急响应 - 抑制阶段 (4)

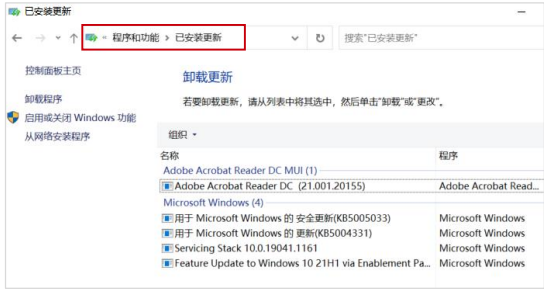
- 未感染病毒的Windows主机系统加固：禁用文件共享与打印服务。



WannaCry应急响应 - 抑制阶段 (5)

- 未感染病毒的Windows主机系统加固：
  - 升级系统：Windows 2003、2008和XP系统已停止安全补丁服务，需要升级系统至最新版本；
  - 补丁修复：安装微软官方发布的专用补丁，不同系统版本的补丁编号不同。

系统版本	补丁号
Windows 7 Windows Server 2008 R2	KB4012212
	KB4012215
Windows Server2012	KB4012214
	KB4012217
Windows Server2012 R2	KB4012213
	KB4012216
Windows 10	KB4012606



WannaCry应急响应 - 根除阶段

- 对已感染的主机采取如下措施：
  - 断网隔离；
  - 判断加密文件的重要性。
    - 若非重要文件或文件已备份，则低格磁盘重装系统；
    - 若文件较重要且文件无备份，则等待解密进度。

- 在该案例中，针对已加密文件，不建议缴纳赎金。

WannaCry应急响应 - 恢复阶段

- 针对重要文件被加密的主机：尝试恢复文件。
- 针对网络：
  - 将WannaCry病毒加入安全设备病毒特征库，设置反病毒策略，阻断病毒入侵及传播；
  - 针对需要文件共享或打印的网络，逐步放开445端口；
  - 持续监控网络流量，复查病毒感染情况；
  - 统一下发最新的系统补丁，对主机进行加固。

WannaCry应急响应 - 总结阶段

- 总结本次应急响应的处理流程与措施、记录问题与解决方案。
- 提升全体员工安全意识，普及病毒危害性、常见传播途经及预防措施。
- 定期检测网络漏洞，关注最新补丁发放，及时修复补丁。

思考题

1. （单选题）通过分析操作系统日志以及安全设备日志，确定攻击者源IP地址之后，管理员修改安全设备的策略，封堵源IP，该操作属于应急响应的哪一个阶段？（　　）

   A. 检测阶段

   B. 抑制阶段

   C. 根除阶段

   D. 恢复阶段

1. B

本章总结

- 本章节主要介绍了应急响应的必要性和标准流程，以及当面对安全事件时的通用处理方法。同时介绍了应急响应的相关技术和案例。
- 通过本章节的学习，您将能够了解应急响应不同阶段的目标和处理方法，掌握常用的应急响应技术，提高应对网络攻击的能力。

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
IPS	Intrusion Prevention System	入侵防御系统
UDP	User Datagram Protocol	用户数据报协议
TCP	Transmission Control Protocol	传输控制协议
PID	Process ID	进程的ID信息

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.

网络接入控制

HUAWEI

前言

- 随着网络的应用和发展，越来越多的重要信息通过网络进行传输和存储，与之对应的各种网络犯罪也相应急剧增加。开放自由的网络在设计之初并未考虑安全性的问题，为此我们在网络的边界部署防火墙以抵御来自外部网络的攻击。但是研究表明，80%的网络安全漏洞都存在于网络内部，它们引发的故障对网络造成了严重的破坏，如业务系统崩溃、网络瘫痪等。
- 身份认证是保障网络安全的第一道防线，它可以对用户的身份进行认证，并赋予用户相应的访问权限。对用户身份保持零信任的态度，始终授予最小的访问权限，可以极大保护内部网络的安全。
- 本章节我们将会介绍网络接入控制技术（也称为网络准入控制技术），了解如何通过接入与认证的结合保证内部网络的安全。

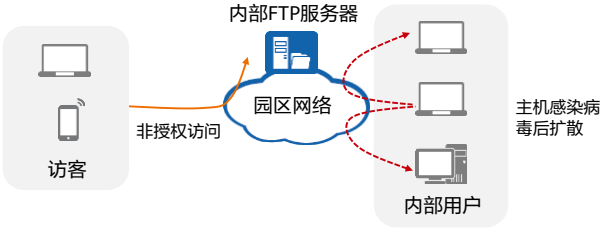
目标

- 学完本课程后，您将能够：
  - 描述网络接入控制的基本概念
  - 描述用户身份认证的工作原理
  - 描述常见的接入认证方式及其工作原理
  - 配置用户接入认证

目录

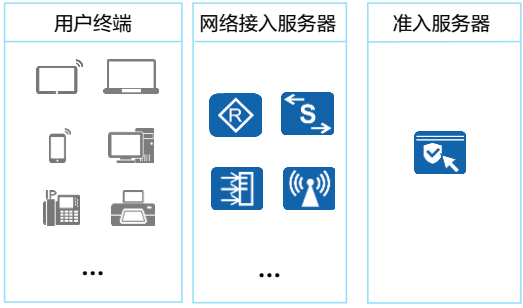
网络接入控制的技术背景

- 传统企业网络接入安全隐患：
  - 非法用户随意接入园区内部网络，会危害园区的信息安全；
  - 缺乏权限控制，访问不受限，导致企业风险增大；
  - 接入园区网络的终端种类多，且园区内用户行为难以管控，缺乏用户行为的记录，无法进行安全事件溯源。
- 出于对安全问题的考虑，园区网络不能对所有终端开放访问权限，需要对终端用户进行身份认证，不符合条件的终端不能接入网络，并对用户的权限进行限制，同时记录用户的网络访问行为。



网络接入控制概述 (1)

- NAC（Network Access Control，网络接入控制）通过对接入网络的客户端和用户进行认证来保证网络的安全，是一种“端到端”的安全技术。



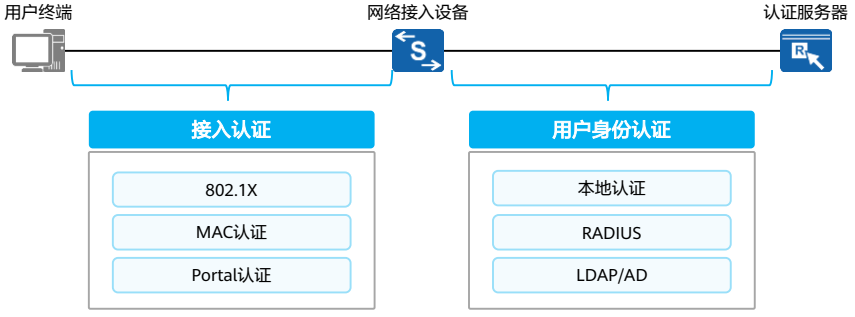
NAC系统架构

- 用户终端：各种终端设备，例如PC、手机、打印机、摄像头等。
- 网络接入服务器（Network Access Server，NAS）：也称为接入设备/准入设备，终端访问网络的认证控制点，接入设备对接入用户进行认证，是企业安全策略的实施者，按照网络制定的安全策略实施相应的准入控制（如允许接入网络或拒绝接入网络）。接入设备可以是交换机、路由器、无线接入控制器、无线接入点或者其他网络设备。
- 准入服务器：也称为AAA服务器，其主要功能是实现对用户的认证、授权和计费。

- 用户终端上一般安装有终端代理（或叫客户端软件），其与准入服务器联动进行用户身份认证、终端安全检查、系统修复升级，终端行为监控审计等工作。
- 网络准入设备可以是交换机、路由器、AP等网络设备，具备如下功能特性：
  - 用户身份认证；
  - 在各种常见认证方式（如802.1X、MAC、Portal）下，网络准入设备辅助客户端软件与准入服务器进行认证；
  - 实现用户权限控制。

网络接入控制概述 (2)

- 用户接入网络的整个过程可以分为两个部分：接入认证与用户身份认证。其中接入认证发生在用户终端与接入设备之间，用户身份认证发生在接入设备与认证服务器之间。
- 常见的接入认证方式有802.1X认证、MAC认证和Portal认证等。常见的用户身份认证方式有RADIUS、LDAP/AD、本地认证等。



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。

HUAWEI

- AAA采用客户端/服务器结构：
  - AAA客户端负责验证用户身份与管理用户接入；
  - AAA服务器负责集中管理用户信息。

AAA常用技术方案

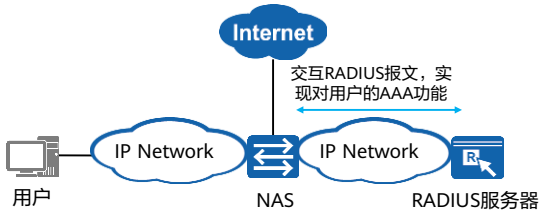
- 目前华为设备支持基于RADIUS、HWTACACS、LDAP或AD来实现AAA，在实际应用中，RADIUS最为常用。

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	/	✓	✓	✗

- 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。

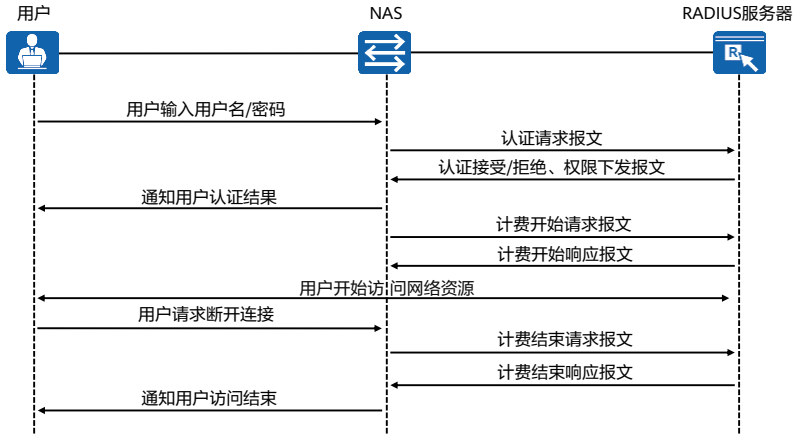
RADIUS协议概述

- AAA可以通过多种协议来实现，在实际应用中，RADIUS协议最为常用。
- 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。
- RADIUS采用典型的客户端/服务器模型，准入控制设备作为RADIUS协议的客户端，同时对于接入用户而言，准入控制设备也是接入认证的服务端。准入控制设备负责传输用户信息到指定的RADIUS服务器，然后根据从服务器返回的信息进行相应处理（如接入/挂断用户）。RADIUS服务器负责接收用户连接请求，认证用户，然后给准入控制设备返回所有需要的信息。

RADIUS认证、授权、计费流程



HUAWEI

- RADIUS客户端与服务器间的消息流程如下：
  - 当用户接入网络时，用户发起连接请求，向RADIUS客户端（即准入控制设备）发送用户名和密码。
  - RADIUS客户端向RADIUS服务器发送包含用户名和密码信息的认证请求报文。
  - RADIUS服务器接收到合法的请求后，完成认证，并把所需的用户授权信息返回给客户端；对于非法的请求，RADIUS服务器返回认证失败的信息给客户端。
  - RADIUS客户端通知用户认证是否成功。
  - RADIUS客户端根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则RADIUS客户端向RADIUS服务器发送计费开始请求报文。
  - RADIUS服务器返回计费开始响应报文，并开始计费。
  - 用户开始访问网络资源。
  - 当用户不再想要访问网络资源时，用户发起下线请求，请求停止访问网络资源。
  - RADIUS客户端向RADIUS服务器提交计费结束请求报文。
  - RADIUS服务器返回计费结束响应报文，并停止计费。
  - RADIUS客户端通知用户访问结束，用户结束访问网络资源。

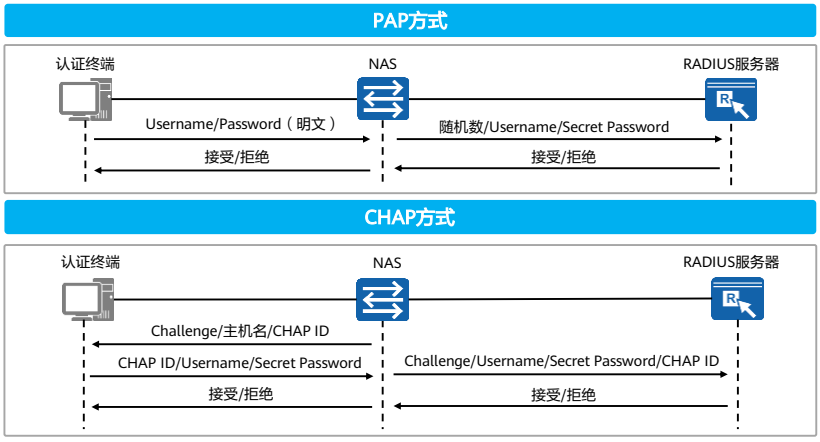
RADIUS报文

报文类型	报文说明
Access-Request认证请求包	方向Client -> Server，Client将用户信息传输到Server，Server判断是否接入该用户。
Access-Accept认证接受包	方向Server -> Client，如果Access-Request报文中所有Attribute值都是可以接受（即认证通过），则传输该类型报文。
Access-Reject认证拒绝包	方向Server -> Client，如果Access-Request报文中存在任何Attribute值无法被接受（即认证失败），则传输该类型报文。
Accounting-Request计费请求包	方向Client -> Server，Client将用户信息传输到Server，请求Server开始计费。
Accounting-Response计费响应包	方向Server -> Client，Server通知Client侧已经收到Accounting-Request报文并且已经正确记录计费信息。

RADIUS HWTACACS LDAP AD 本地认证授权

RADIUS用户认证方式

- RADIUS支持使用多种方式对用户的身份信息进行验证，其中最常见的是PAP以及CHAP方式。

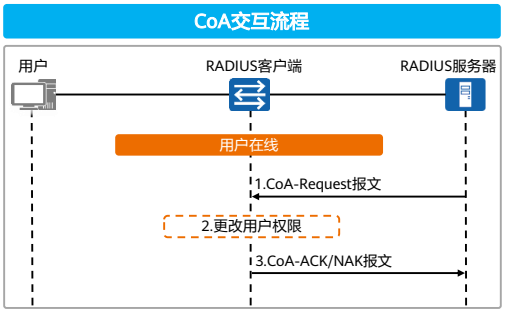


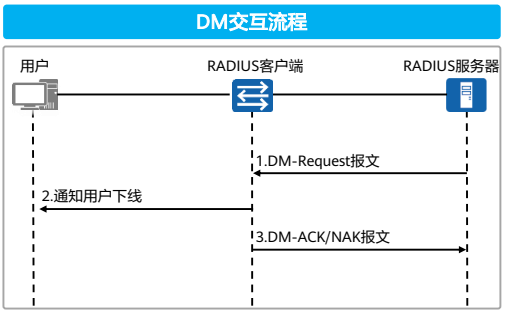
HUAWEI

- PAP方式中，准入控制设备通过RADIUS携带用户名，密码不直接明文携带，而是通过Secret Password携带，Secret Password为Password明文通过MD5（随机数＋Key）得到，其中随机数为RADIUS的authenticator字段，Key值为RADIUS客户端和服务器之间共同配置的相同密钥。
- 在CHAP方式中准入控制设备产生一个16字节的随机码给用户（同时还有一个ID号，本设备的Host name）。用户端得到这个包后使用自己独有的设备或软件客户端将CHAP ID、用户密码（口令字）、随机码使用MD5算法生成一个Secret Password，随同用户名Username一并传给准入控制设备。准入控制设备把传回来的Username和Secret Password分别作为用户名和密码，并把原来的16字节随机码以及CHAP ID传给RADIUS服务器。RADIUS根据用户名在服务器端查找数据库，得到和用户端进行加密所用的一样的密钥，用MD5算法对CHAP ID，密钥和传来的16字节的随机码进行加密，将其结果与传来的Password作比较，如果相匹配，服务器送回一个接入允许数据包，否则送回一个接入拒绝数据包。
- 以802.1X认证为例，如采用PAP方式，则在认证终端和网络接入设备之间交互的EAP报文会明文携带用户、密码信息。而如果采用CHAP方式，则EAP协议在认证终端和网络接入设备之间交互时会在EAP报文内携带CHAP ID、Username、Secret Password、Challenge等信息。

RADIUS用户动态授权

- 设备支持RADIUS CoA/DM功能，提供一种动态修改在线用户权限或者强制用户下线的机制。
- CoA (Change of Authorization，动态授权)指用户认证成功后，管理员可以通过RADIUS协议来修改在线用户的权限或对其进行重认证。
- DM (Disconnect Message，用户下线报文)指由RADIUS服务器主动发起的强制用户下线的报文。

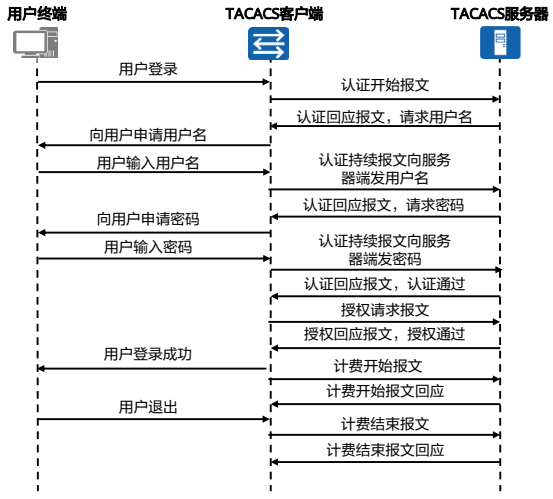




RADIUS | HWTACACS | LDAP | AD | 本地认证授权

HWTACACS协议介绍

- HWTACACS（华为终端访问控制器控制系统协议）是在TACACS（RFC 1492)基础上进行了功能增强的安全协议。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，TCP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。



HUAWEI

- HWTACACS协议与其他厂商支持的TACACS+协议都实现了认证、授权、计费的功能。HWTACACS和TACACS+的认证流程与实现方式是一致的，HWTACACS协议能够完全兼容TACACS+协议。

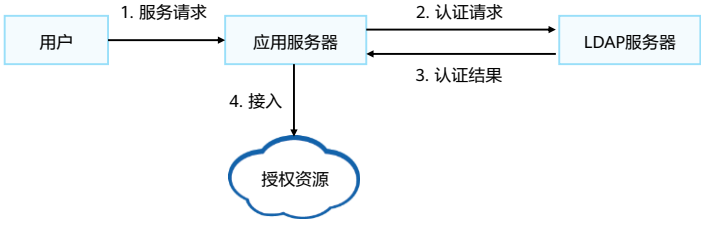
HWTACACS与RADIUS对比

项目	HWTACACS	RADIUS
数据传输	通过TCP传输，网络传输更可靠。	通过UDP传输，网络传输效率更高。
加密方式	共享密钥，除了标准的HWTACACS报文头，对报文主体全部进行加密。	共享密钥，只是对认证报文中的密码字段进行加密。
认证和授权	认证与授权分离，使得认证、授权服务可以在不同的安全服务器上实现。	认证与授权结合不能分离。
命令行授权	支持对设备上的配置命令进行授权使用。	不支持对设备上的配置命令进行授权使用。
应用场景	因命令行授权功能强大，多用于设备认证。	适用范围较广，终端认证以及设备认证均适用。

- HWTACACS协议与RADIUS协议的相似点包括：
  - 结构上都采用客户端/服务器模式；
  - 都使用共享密钥对传输的用户信息进行加密；
  - 都有较好的灵活性和可扩展性。

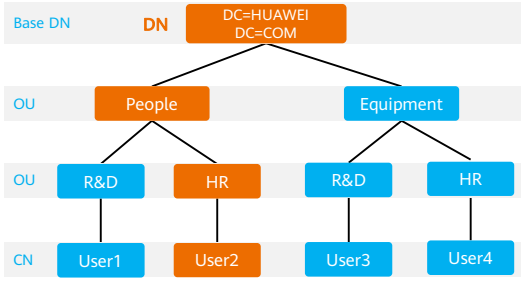
LDAP简介

- 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。



LDAP目录

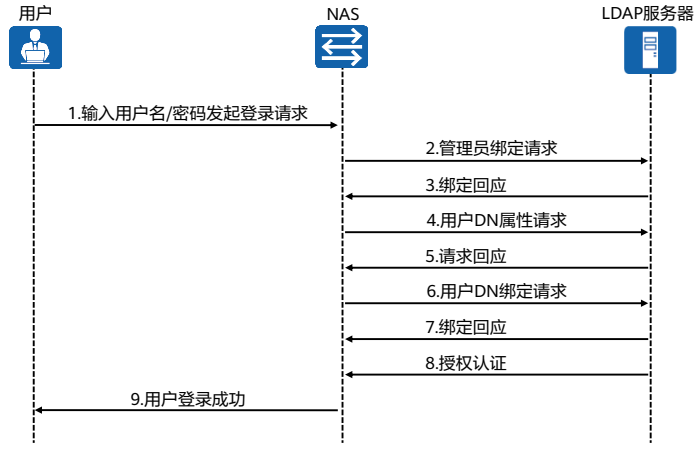
- 目录是一组具有类似属性、以一定逻辑和层次组合的信息。LDAP协议中目录是按照树型结构组织，目录由条目（Entry）组成，条目是具有区别名DN的属性集合。属性由类型和多个值组成。



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User2的DN为“CN=User2，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



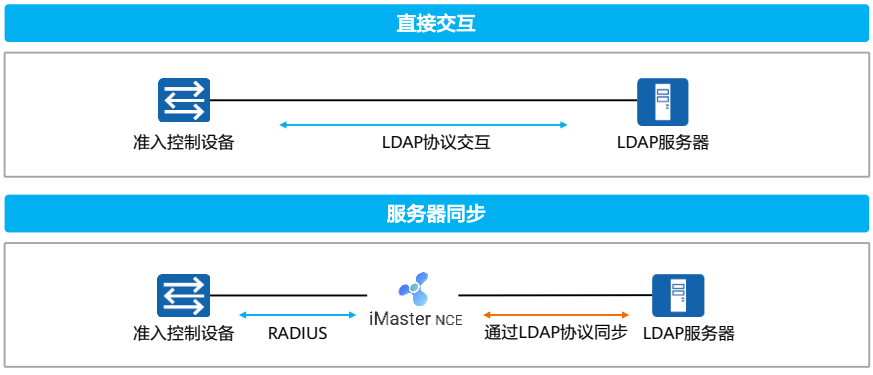
HUAWEI

- 认证流程描述如下：
  1. 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；
  2. 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；
  3. 绑定成功后，LDAP服务器向防火墙发送绑定回应报文；
  4. 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；
  5. 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；
  6. 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；
  7. 绑定成功后，LDAP服务器发送绑定回应报文；
  8. LDAP服务器对用户进行授权；
  9. 授权成功后，防火墙通知用户登录成功。

RADIUS HWTACACS LDAP AD 本地认证授权

LDAP典型架构

- 部分网络设备支持直接与LDAP服务器进行交互，同时iMaster NCE-Campus认证服务器支持作为客户端同步LDAP服务器上的用户信息，对于不支持直接与LDAP服务器进行交互的设备，可通过iMaster NCE-Campus作为客户端同步LDAP服务器上的用户信息，进行用户认证。

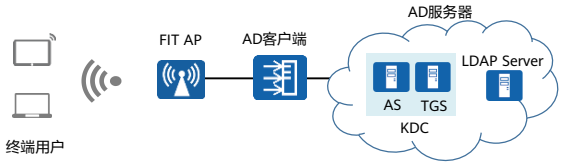


HUAWEI

- 在第二种方式中，iMaster NCE-Campus会查询LDAP服务器上相应的目录，并将用户信息转换为自身的用户信息数据库，之后准入控制设备可以通过RADIUS协议进行用户身份认证。
- iMaster NCE-Campus是华为智简园区解决方案的管理控制系统，支持网络业务管理、网络安全管理、用户准入管理等功能，在本认证课程中我们使用其作为认证服务器以及Portal服务器。

AD协议介绍

- Kerberos是一种通过密钥系统实现在不安全的开放网络中安全传输数据的网络认证协议，它不要求网络上所有主机安全，并假定网络上传送的数据可以被任意地读取和修改。该协议基于TCP，对应的端口号为88。
- Kerberos协议可集成到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。
- 用于网络接入设备和AD服务器对接场景。



AD服务器组成

- LDAP Server：LDAP服务器，服务器上存储了所有的目录信息。
- KDC (Key Distribution Center，密钥分配中心)：也就是Kerberos服务器，存储了所有客户端的密码和账户信息。KDC由AS和TGS组成。
- AS (Authentication Server，认证服务器)：提供访问TGS的凭证Ticket。
- TGS (Ticket-Granting Server，票据授予服务器)：提供访问AD服务器的凭证Ticket。

- AD客户端：集成了Kerberos和LDAP协议的接入设备。
- AD服务器：AD服务器是集成了Kerberos和LDAP认证的服务器，通常情况下，LDAP服务器和Kerberos服务器是合二为一的。

RADIUS HWTACACS LDAP AD 本地认证授权

AD认证、授权流程

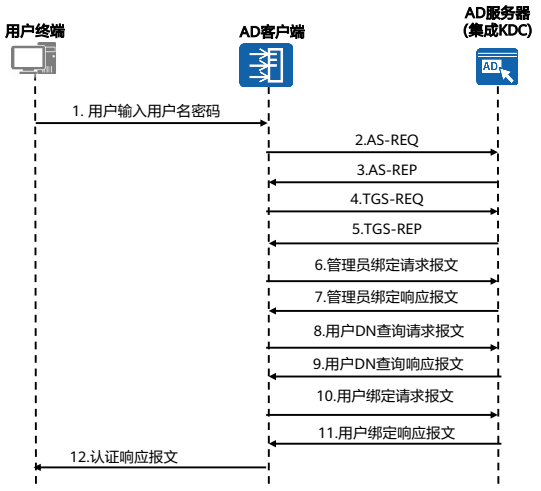
- 相比LDAP的认证、授权流程，AD的认证、授权流程增加了2~5加解密流程。

2. 向Kerberos服务器发送AS-REQ请求报文，该报文以明文形式向Kerberos服务器发送用户名。

3. AS服务器向客户端返回AS-REP报文，AS-REP报文中用AS和TGS服务器的共享密钥对Ticket进行加密，再用客户端的密码对加密后的Ticket和会话密钥Session key进行加密。

4. AD客户端用自己的密码解密AS-REP报文，获得Session key和加密后的Ticket。

5. Kerberos服务器用AS和TGS之间共享的密钥解密Ticket，提取Ticket中的Session key，利用Session key解密认证单Authenticator，获得认证单中的客户端名称和时间信息与Ticket中的信息一致的话，则验证通过，发送REP报文。



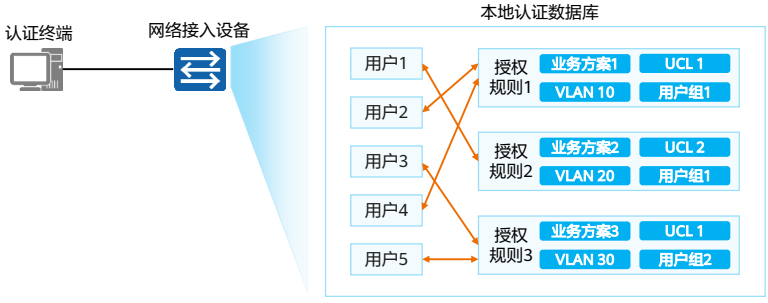
HUAWEI

- 第1步，当用户需要访问AD服务器时，用户发起认证请求，向AD客户端发送用户名和密码。
- 第2步，当AD客户端首次访问AD服务器时，需要向集成在AD服务器中的Kerberos服务器验证自己的身份，向Kerberos服务器发送AS-REQ请求报文，该报文以明文形式向Kerberos服务器发送用户名。
- 第3步，Kerberos服务器根据获取的用户名在数据库中查找此用户。如果查找成功，AS服务器会生成一个Kerberos服务器和客户端之间共享的会话密钥Session key。同时AS服务器会生成一个Ticket，AD客户端以后就可以凭这个Ticket向Kerberos服务器请求访问AD服务器的凭证，无需再验证自己的身份了。AS服务器向客户端返回AS-REP报文，AS-REP报文中用AS和TGS服务器的共享密钥对Ticket进行加密，再用客户端的密码对加密后的Ticket和会话密钥Session key进行加密。
- 第4步，AD客户端用自己的密码解密AS-REP报文，获得Session key和加密后的Ticket。AD客户端向Kerberos服务器发送TGS-REQ报文请求获得访问AD服务器的Ticket，报文中包括一个认证单Authenticator、加密后的Ticket、客户端名称、AD服务器名称等。认证单Authenticator是利用Session key加密的客户端用户名、IP地址、时间信息、域名等信息。

- 第5步，Kerberos服务器用AS和TGS之间共享的密钥解密Ticket，提取Ticket中的Session key，利用Session key解密认证单Authenticator，获得认证单中的客户端名称和时间信息与Ticket中的信息一致的话，则验证通过。Kerberos服务器会向客户端返回一个利用客户端密码加密的TGS-REP报文，报文包括客户端与AD服务器的会话密钥，以及利用AD服务器的密码加密后的Ticket。Ticket中包括会话密钥Session key、客户端名称、服务器名称、Ticket的有效期等。Kerberos客户端利用自身密码解密TGS-REP报文，获得客户端与AD服务器共享的Session key以及利用AD服务器密码加密后的可以访问AD服务器的Ticket。
- 第6步到第12步，与LDAP认证、授权流程的第2步到第8步基本一致，差异在于第10步用户绑定过程采用Session Key和凭证Ticket对用户密码进行加密和验证，提高了认证的安全性：第10步的用户绑定请求报文中，包含了AD客户端利用Session key对用户名和密码进行加密的认证单Authenticator，以及利用AD服务器密码加密后的访问AD服务器的凭证Ticket。
- AD服务器收到用户绑定请求报文，先用自己的服务器密码解开凭证Ticket，然后查看Ticket是否在有效期内，在有效期内，用Ticket中携带的会话密钥Session key解密认证单Authenticator，然后进行用户绑定请求报文的处理，检查用户输入的密码是否正确。

本地认证授权

- 用户身份认证、授权可以在接入控制设备上完成，也可以交由服务器完成。如果在接入控制设备上完成，则相当在接入控制设备上配置一个本地的用户认证服务器。
- 本地认证的优点是速度快，可以为运营降低成本，缺点是存储信息量受设备硬件条件限制，一般常用于设备登录认证。



HUAWEI

- 配置本地授权时，支持的授权参数有：VLAN、业务方案、用户组（或者UCL组）。
- 业务方案：包含了一系列网络资源，授权客户相对应的业务方案时即将对应的资源授予了用户，具体支持的网络资源如下：
  - ACL：可用于限制用户可访问的网络资源地址范围。
  - User-VLAN：用户的授权VLAN。
  - Admin-user privilege level：当用户作为管理员登录设备时，可指定用户的管理员级别。
  - 其他参数：如DNS地址、同一个用户名最多可以接入的用户数量等。
  - 用户组（UCL组）：具有相同属性的集合，例如相同的部分或者具有相同的网络访问权限，用户组（UCL组）可以作为后续进一步执行访问策略限制的条件，如匹配ACL限制网络访问权限时可使用UCL组作为源或者目的匹配条件。

目录

802.1X认证

- 802.1X认证是一种基于端口的网络接入控制协议，即在接入设备的端口这一级验证用户身份并控制其访问权限。802.1X认证使用EAP（Extensible Authentication Protocol，可扩展认证协议）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。

组网方式

- 802.1X客户端一般为用户终端设备，用户可以通过启动客户端软件发起802.1X认证。
- 网络接入设备通常为支持802.1X协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
- 认证服务器用于实现对用户进行认证、授权和计费，通常为RADIUS服务器。

应用场景

- 适用于对安全要求较高的办公用户认证场景。

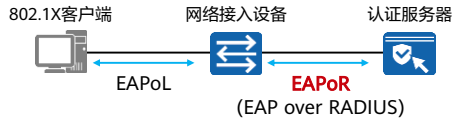
HUAWEI

- 802.1X协议为二层协议，不需要到达三层，对接入设备的整体性能要求不高，可以有效降低建网成本。
- 802.1X协议的认证报文和数据报文通过逻辑接口分离，提高安全性。

802.1X认证方式

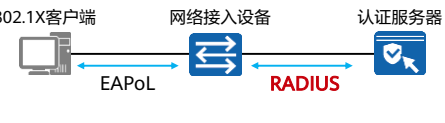
- 根据接入设备对802.1X客户端发送的EAPoL报文处理机制的不同，可将认证方式分为EAP中继方式和EAP终结方式。

EAP中继方式



- 接入设备将802.1X客户端发来的EAPoL报文直接封装到RADIUS报文中，无需对EAP内的数据进行处理。
- 这种方式对认证服务器的要求较高。

EAP终结方式



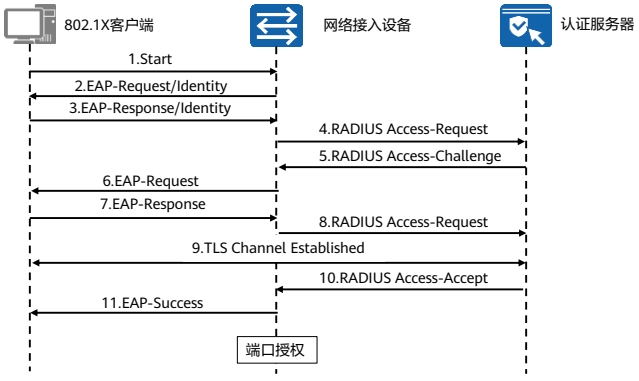
- 接入设备需要“提取”EAPoL报文中的信息并封装到RADIUS报文中发送给认证服务器。
- 这种方式对接入设备的要求较高。

HUAWEI

- EAP中继方式：
  - 其优点是设备端处理更简单，支持更多的认证方法，缺点则是认证服务器必须支持EAP，且处理能力要足够强。
  - 对于常用的EAP-TLS、EAP-TTLS、EAP-PEAP三种认证方式，EAP-TLS需要在客户端和服务器上加载证书，安全性最高，EAP-TTLS、EAP-PEAP需要在服务器上加载证书，但不需要在客户端加载证书，部署相对灵活，安全性较EAP-TLS低。
- EAP终结方式：
  - 其优点是现有的RADIUS服务器基本均支持PAP和CHAP认证，无需升级服务器，但设备端的工作比较繁重，因为在这种认证方式中，设备端不仅要从来自客户端的EAP报文中提取客户端认证信息，还要通过标准的RADIUS协议对这些信息进行封装，且不能支持除MD5-Challenge之外的其它EAP认证方法。
  - PAP与CHAP的主要区别是CHAP密码通过密文方式传输，而PAP密码通过明文的方式传输。因而PAP方式认证的安全性较低，实际应用通常采用CHAP方式认证。

802.1X认证流程

- 802.1X认证有以下触发方式：客户端发送EAPoL-Start报文触发认证、客户端关联设备触发认证。
- 以客户端关联触发802.1X认证为例，EAP中继方式的802.1X认证流程如图所示。



HUAWEI

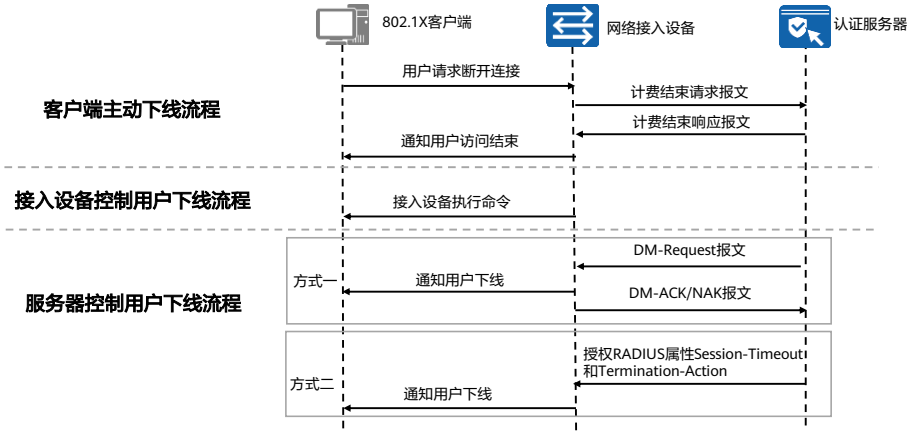
- EAP中继方式的认证流程：
  1. 客户端关联设备触发802.1X认证。
  2. 设备端发出一个Identity类型的请求报文（EAP-Request/Identity）请求客户端的身份信息。
  3. 客户端程序响应设备端发出的请求，将身份信息通过Identity类型的响应报文（EAP-Response/Identity）发送给设备端。
  4. 设备端响应报文中的EAP报文封装在RADIUS报文（RADIUS Access-Request）中，发送给认证服务器进行处理。
  5. RADIUS服务器收到设备端转发的身份信息后，启动和客户端EAP认证方法的协商。RADIUS服务器选择一个EAP认证方法，将认证方法封装在RADIUS Access-Challenge报文中，发送给设备端。
  6. 设备端收到RADIUS服务器发送的RADIUS Access-Challenge报文后，将其中的EAP信息转发给客户端。
  7. 客户端收到由设备端传来的EAP信息后，解析其中的EAP认证方法，如果支持该认证方法，客户端发送EAP-Response报文给设备端；如果不支持，客户端选择一个支持的EAP认证方法封装到EAP-Response报文中发送给设备端。

8. 设备将报文中的EAP信息封装到RADIUS报文中发给RADIUS服务器。
9. RADIUS服务器收到后，如果客户端与服务器选择的认证方法一致，EAP认证方法协商成功，开始认证。以EAP-PEAP认证方法为例，服务器将自己的证书封装到RADIUS报文中发送给设备端。设备收到后将证书转发给客户端。客户端校验服务器证书（可选），与RADIUS服务器协商TLS参数，建立TLS隧道。TLS隧道建立完成后，用户信息将通过TLS加密在客户端、设备端和RADIUS服务器之间传输。如果客户端与服务器的EAP认证方法协商失败，则终止认证流程，通知设备认证失败，设备去关联客户端。
10. RADIUS服务器完成对客户端身份验证之后，通知设备认证成功，并下发密钥用于设备和客户端之间握手。
11. 设备收到认证通过报文后向客户端发送认证成功报文（EAP-Success），并将端口改为授权状态，允许用户通过该端口访问网络。设备使用RADIUS服务器发下的密钥，完成和客户端的握手，握手成功后客户端关联成功。

- EAP终结方式与EAP中继方式的认证流程相比，不同之处在于EAP认证方法协商由客户端和设备端完成，之后设备端会把用户信息送给RADIUS服务器，进行相关的认证处理。而在EAP中继方式中，EAP认证方法协商由客户端和服务器完成，设备端只是负责将EAP报文封装在RADIUS报文中透传认证服务器，整个认证处理都由认证服务器来完成。

802.1X认证用户下线

- 用户下线方式分为客户端主动下线，接入设备控制用户下线和服务器控制用户下线。



- 接入设备控制用户下线：
  - 在接入设备上执行命令强制指定用户下线。当管理员发现非法用户在线，或在测试中想让某一用户下线后重新上线，可以通过在设备上执行命令强制该用户下线。
- 服务器控制用户下线有以下方式：
  - RADIUS服务器可通过DM报文（Disconnect Message）强制用户下线。DM是指用户离线报文，即由RADIUS服务器端主动发起的强迫用户下线的报文。
  - RADIUS服务器通过授权RADIUS标准属性Session-Timeout和Termination-Action。其中，Session-Timeout为用户在线时长定时器，Termination-Action属性值为0表示将用户下线。当用户在线的时长达到定时器指定的数值时，设备会将用户下线。

目录

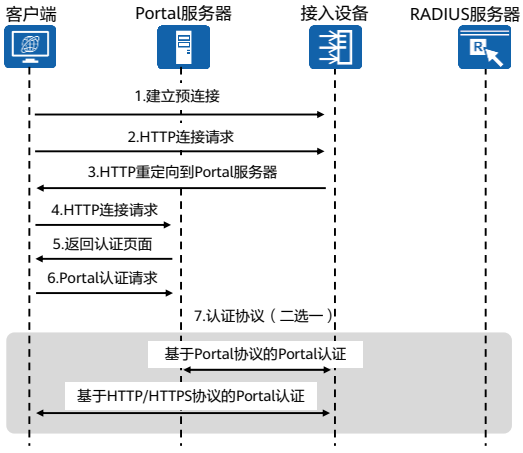
Portal认证

- Portal认证也称为Web认证。用户可以通过Web认证页面，输入用户帐号和密码信息，实现对终端用户身份的认证。用户可通过两种方式实现认证页面访问：
  - 主动认证：用户通过浏览器主动访问Portal认证网站。
  - 重定向认证：用户输入的访问地址不是Portal认证网站地址，被接入设备强制访问Portal认证网站（即重定向）。

- 客户端：一般情况下，客户端是安装有运行HTTP/HTTPS协议的浏览器的主机，有时也会有安装相应的客户端软件（如浏览器）。
- 接入设备：交换机、路由器等接入设备的统称，主要有三方面的作用。
  - 在认证之前，将认证网段内用户的所有HTTP/HTTPS请求都重定向到Portal服务器。
  - 在认证过程中，与Portal服务器、认证服务器交互，完成对用户身份认证、授权与计费的功能。
  - 在认证通过后，允许用户访问被管理员授权的网络资源。
- Portal服务器：接收客户端认证请求的服务器系统，提供门户（Portal）服务和认证界面，与接入设备交互客户端的认证信息。
- 认证服务器：与接入设备进行交互，完成对用户的认证、授权与计费。
- Portal认证不需要安装专门的客户端软件，因此主要用于无客户端软件要求的接入场景或访客接入场景。

Portal认证协议

- Portal协议包括Portal接入协议和Portal认证协议。
  - Portal接入协议：HTTP/HTTPS协议，描述了客户端和Portal服务器之间的协议交互。
  - Portal认证协议：支持如下两种认证协议。
    - Portal协议：描述了Portal服务器和接入设备之间的协议交互，可以用来传递用户名和密码等参数。其兼容中国移动Portal 2.0协议，支持该协议的基本功能。
    - HTTP/HTTPS协议：描述了客户端和接入设备之间的协议交互，可以用来传递用户名和密码等参数。

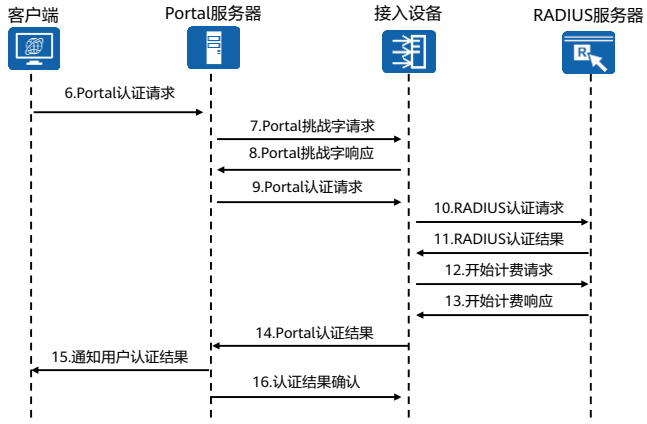


HUAWEI

- Portal认证认证流程如下：
  1. 在认证之前客户端与接入设备之间建立起预连接，即客户端用户在认证成功之前在接入设备上已建立用户在线表项，并且只有部分网络访问权限。
  2. 客户端发起HTTP连接请求。
  3. 接入设备收到HTTP连接请求报文时，如果是访问Portal服务器或免认证网络资源的HTTP报文，则接入设备允许其通过；如果是访问其它地址的HTTP报文，则接入设备将其URL (Uniform Resource Locator，统一资源定位符)地址重定向到Portal认证页面。
  4. 客户端根据获得的URL地址向Portal服务器发起HTTP连接请求。
  5. Portal服务器向客户端返回Portal认证页面。
  6. 用户在Portal认证页面输入用户名和密码后，客户端向Portal服务器发起Portal认证请求。
  7. 按照不同认证协议规定的协议交互流程进行用户名和密码等参数的传递。

Portal认证流程 - Portal协议

- 以CHAP认证方式为例，基于Portal协议的Portal认证流程如下：



HUAWEI

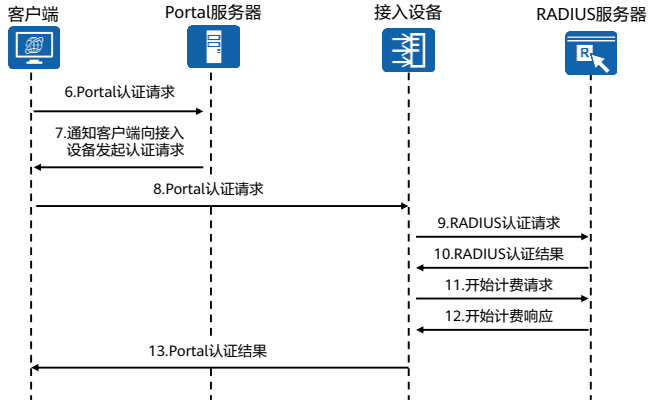
- 基于Portal协议的Portal认证，详细认证流程如下：

7. Portal服务器收到Portal认证请求后，如果Portal服务器与接入设备之间采用CHAP认证，则Portal服务器向接入设备发起Portal挑战字请求报文（REQ_CHALLENGE）；如果Portal服务器与接入设备之间采用PAP认证，则接入设备直接进行第9步。
8. 接入设备向Portal服务器回应Portal挑战字应答报文（ACK_CHALLENGE）。
9. Portal服务器将用户输入的用户名和密码封装在Portal认证请求报文（REQ_AUTH）中，并发送给接入设备。
10. 接入设备根据获取到的用户名和密码，向RADIUS服务器发送RADIUS认证请求（ACCESS-REQUEST）。
11. RADIUS服务器对用户名和密码进行认证。如果认证成功，则RADIUS服务器向接入设备发送认证接受报文（ACCESS-ACCEPT）；如果认证失败，则RADIUS服务器返回认证拒绝报文（ACCESS-REJECT）。由于RADIUS协议合并了认证和授权的过程，因此认证接受报文中也包含了用户的授权信息。
12. 接入设备根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则接入设备向RADIUS服务器发送计费开始请求报文（ACCOUNTING-REQUEST）。

13. RADIUS服务器返回计费开始响应报文（ACCOUNTING-RESPONSE），并开始计费，将用户加入自身在线用户列表。
14. 接入设备向Portal服务器返回Portal认证结果（ACK_AUTH），并将用户加入自身在线用户列表。
15. Portal服务器向客户端发送认证结果报文，通知客户端认证成功，并将用户加入自身在线用户列表。
16. Portal服务器向接入设备发送认证应答确认（AFF_ACK_AUTH）。

Portal认证流程 - HTTP/HTTPS协议

- 用户上线时的HTTP协议认证报文交互过程如图所示，HTTPS协议认证报文交互过程与HTTP类似，区别在于HTTPS报文经过加解密处理。

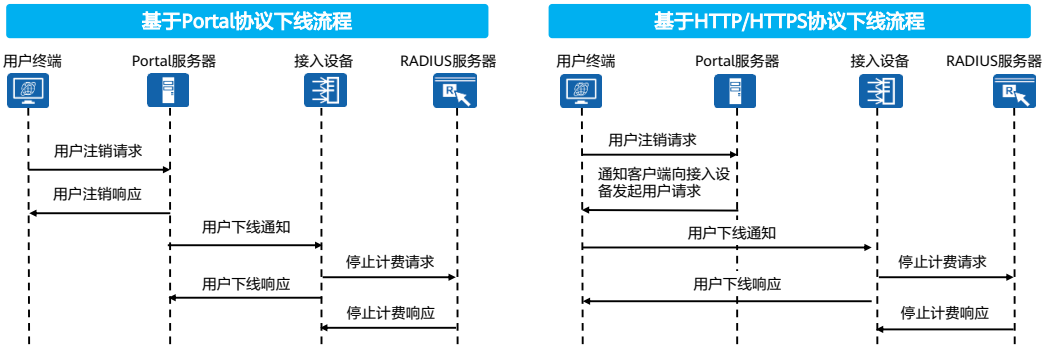


HUAWEI

- 基于HTTP/HTTPS协议的Portal认证，详细认证流程如下：
  7. Portal服务器通知客户端向接入设备发起Portal认证请求。
  8. 客户端向接入设备发起Portal认证请求（HTTP POST/GET）。
  9. 接入设备根据获取到的用户名和密码，向RADIUS服务器发送RADIUS认证请求（ACCESS-REQUEST）。
  10. RADIUS服务器对用户名和密码进行认证。如果认证成功，则RADIUS服务器向接入设备发送认证接受报文（ACCESS-ACCEPT）；如果认证失败，则RADIUS服务器返回认证拒绝报文（ACCESS-REJECT）。由于RADIUS协议合并了认证和授权的过程，因此认证接受报文中也包含了用户的授权信息。
  11. 接入设备根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则接入设备向RADIUS服务器发送计费开始请求报文（ACCOUNTING-REQUEST）。
  12. RADIUS服务器返回计费开始响应报文（ACCOUNTING-RESPONSE），并开始计费，将用户加入自身在线用户列表。
  13. 接入设备向客户端返回Portal认证结果，并将用户加入自身在线用户列表。

Portal认证用户下线 - 客户端主动下线

- 客户端主动下线由用户发起下线请求，例如用户点击注销按钮，客户端向Portal服务器发送用户注销请求。
- 基于Portal和HTTP/HTTPS协议的客户端主动下线流程不同，详细如下。

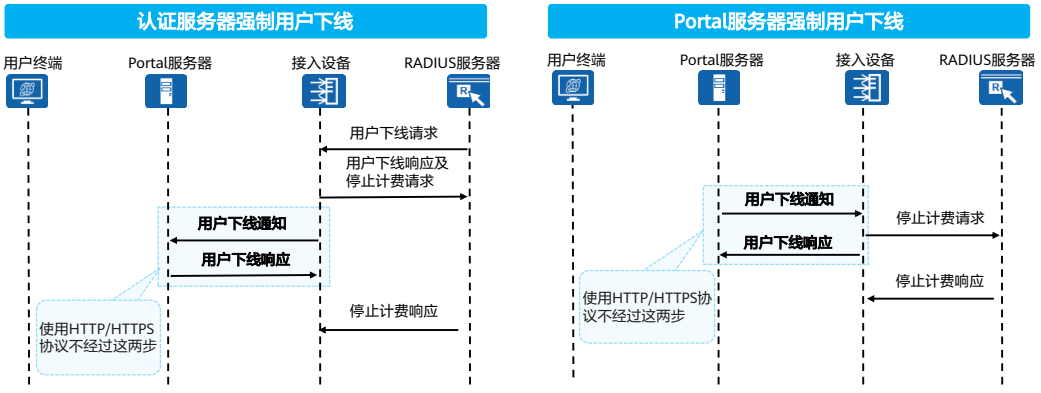


HUAWEI

- 用户下线方式分为客户端主动下线，接入设备控制用户下线和服务器控制用户下线。

Portal认证用户下线 - 服务器强制用户下线

- 在Portal认证组网中，涉及两类服务器，认证服务器和Portal服务器，两类服务器均可强制用户下线，流程如下。



HUAWEI

- Portal认证还支持接入设备控制用户下线，用户通过接入设备侧直接下发命令通知用户下线。

目录

MAC认证

- MAC地址认证（简称MAC认证）是一种基于端口和MAC地址对用户的网络访问权限进行控制的认证方法。以用户的MAC地址作为身份凭据到认证服务器进行认证。
- 缺省时，交换机收到DHCP/ARP/DHCPv6/ND报文后均能触发对用户进行MAC认证。支持通过配置，使交换机收到任意的数据帧后均触发MAC认证。

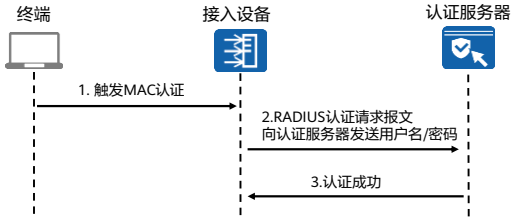
- 终端：尝试接入网络的终端设备。
- 接入设备：是终端访问网络的网络控制点，安全策略的实施者，负责按照客户网络制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）。
- 认证服务器：用于确认尝试接入网络的终端身份是否合法，还可以指定身份合法的终端所能拥有的网络访问权限。

HUAWEI

- MAC认证不需要用户安装任何客户端软件，适用于IP电话、打印机等哑终端接入的场景。
- 哑终端：哑终端表示相对于其他终端而言功能较为有限、交互方式比较单一。其具体的含义根据不同的场合（语境）而变化。这里的哑终端泛指无法输入用户名和密码等认证信息的终端。
- MAC认证优点：
  - 用户终端不需要安装任何客户端软件；
  - MAC认证过程中，不需要用户手动输入用户名和密码；
  - 能够对不具备802.1X认证能力的终端进行认证，如打印机和传真机等哑终端。

MAC认证流程

- 对于MAC认证用户密码的处理，有PAP和CHAP两种方式：
  - PAP：设备将MAC地址、共享密钥、随机值依次排列顺序后，经过MD5算法进行HASH处理后封装在属性名“User-Password”中。
  - CHAP：设备将CHAP ID、MAC地址、随机值依次排列顺序后，经过MD5算法进行HASH处理后封装在属性名“CHAP-Password”和“CHAP-Challenge”中。



HUAWEI

- 以PAP方式介绍MAC认证流程：
  1. 接入设备收到终端发送的DHCP/ARP/DHCPv6/ND报文，触发MAC认证。
  2. 设备随机生成一个随机值，并对MAC认证用户的MAC地址、共享密钥、随机值依次排列后经过MD5算法进行HASH处理，然后将用户名、HASH处理结果以及随机值封装在RADIUS认证请求报文中发送给RADIUS服务器，请求RADIUS服务器对该终端进行MAC认证。
  3. RADIUS服务器使用收到的随机值对本地数据库中对应MAC认证用户进行MAC地址、共享密钥、随机值依次排列后经过MD5算法进行HASH处理，如果与设备发来的值相同，则向设备发送认证接受报文，表示终端MAC认证成功，允许该终端访问网络。
- CHAP方式的MAC认证与PAP方式的MAC认证相比，不同之处在于是对MAC认证用户的CHAP ID、MAC地址、随机值依次排列后进行MD5算法加密。
- MAC认证用户下线方式与802.1X认证基本一致：用户主动下线、接入设备控制用户下线、服务器控制用户下线。这里不再赘述。

三种认证方式比较

- 由于三种认证方式认证原理不同，各自适合的场景也有所差异，实际应用中，可以根据场景部署某一种合适的认证方式，也可以部署几种认证方式组成的混合认证。

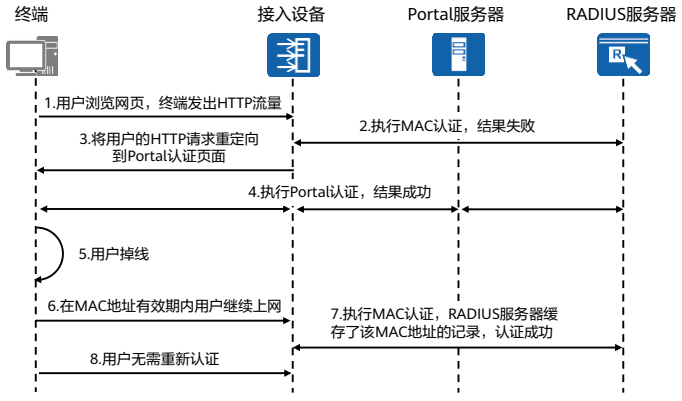
对比项	802.1X认证	MAC认证	Portal认证
适合场景	新建网络、用户集中、信息安全要求严格的场景	打印机、传真机等哑终端接入认证的场景	用户分散、用户流动性大的场景
客户端需求	需要	不需要	不需要
优点	安全性高	无需安装客户端	部署灵活
缺点	需部署专用的认证服务器，复杂程度较高	需登记MAC地址，管理复杂	安全性不高

- 当前支持的混合认证有：
  - MAC优先的Portal认证；
  - MAC和802.1X混合认证。

目录

混合认证 - MAC优先的Portal认证

- MAC优先的Portal认证：用户进行Portal认证成功后，在一定时间内断开网络重新连接，能够直接通过MAC认证接入，无需输入用户名、密码重新进行Portal认证。

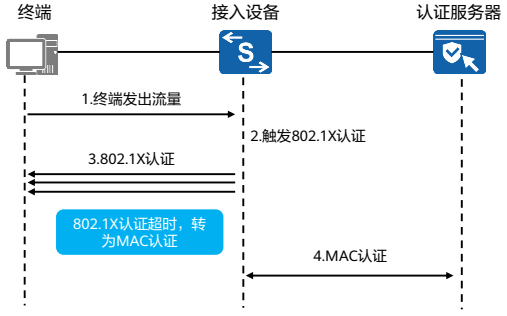


HUAWEI

- MAC优先的Portal认证用来解决在无线环境下终端用户通过Portal认证之后，因无线信号不稳定或终端用户离开无线信号覆盖区域导致终端用户掉线，终端用户需要频繁在Web浏览器上输入帐号和密码重新认证才能接入网络。
- 该功能需要在设备配置MAC + Portal的混合认证，同时在认证服务器上开启MAC优先的Portal认证功能并配置MAC地址有效时间。

混合认证 - MAC旁路认证

- 当接入设备接口下同时存在PC和打印机/传真机等哑终端时，可以配置MAC旁路认证功能，使不具备802.1X认证能力的哑终端能够通过MAC认证方式接入网络。
- MAC旁路认证比单纯的MAC认证多一个802.1X认证环节，故时间要比MAC认证时间长。



HUAWEI

- 以上MAC旁路认证方式仅针对通过有线方式接入网络的终端，MAC认证和802.1X认证有一种认证通过即用户认证通过。当终端采用无线接入网络时，同样支持MAC和802.1X混合认证，但是设备首先会对终端用户进行MAC认证，MAC认证成功后，再进行802.1X认证，两种认证方式均通过后，用户认证通过。具体的认证流程可以参考802.1X认证和MAC认证流程。

目录

用户授权

- 以RADIUS服务器授权为例，常见的授权信息有：
  - VLAN：为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和未认证的用户划分到不同的VLAN。用户认证成功后，认证服务器将指定VLAN授权给用户。
  - ACL：用户认证成功后，认证服务器将指定ACL授权给用户，则设备会根据该ACL对用户报文进行控制。
  - UCL：用户控制列表UCL组（User Control List）是网络成员的集合。UCL组里面的成员，可以是PC、手机等网络终端设备。借助UCL组，管理员可以将具有相同网络访问策略的一类用户划分为同一个组，然后为其部署一组网络访问策略，满足该类别所有用户的网络访问需求。相对于为每个用户部署网络访问策略，基于UCL组的网络控制方案能够极大的减少管理员的工作量。

状态	802.1x	MAC认证	Portal认证
动态VLAN	√	√	×
动态ACL	√	√	√
UCL	√	√	√

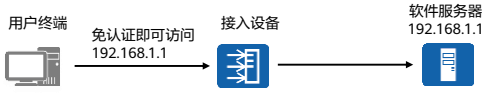
- 由于RADIUS协议合并了认证和授权的过程，因此当采用RADIUS作为认证服务器时，认证接受报文中也包含了用户的授权信息。
- 授权VLAN：用户认证成功后，认证服务器将指定VLAN授权给用户。此时，设备会将用户所属的VLAN修改为授权的VLAN，授权的VLAN并不改变接口的配置。但是，授权的VLAN优先级高于用户配置的VLAN，即用户认证成功后生效的VLAN是授权的VLAN，用户配置的VLAN在用户下线后生效。
- RADIUS服务器授权ACL有两种方法：
  - 授权静态ACL：RADIUS服务器通过RADIUS标准属性Filter-Id将ACL ID授权给用户。为使授权的ACL生效，需要提前在设备上配置相应的ACL及规则。
  - 授权动态ACL：RADIUS服务器通过华为RADIUS扩展属性HW-Data-Filter将ACL ID及其ACL规则授权给用户。ACL ID及其ACL规则需要在RADIUS服务器上配置，设备上不需要配置。
- RADIUS服务器授权UCL组有两种方式：
  - 授权UCL组名称：RADIUS服务器通过RADIUS标准属性Filter-Id将UCL组名称授权给指定用户。
  - 授权UCL组ID：RADIUS服务器通过华为RADIUS扩展属性HW-UCL-Group将UCL组ID授权给指定用户。
  - 无论是哪一种授权UCL组方式，都必须提前在设备上配置相应的UCL组及UCL组的网络访问策略。

免认证与认证事件授权

免认证（free-rule）

用户认证成功之前，为满足用户基本的网络访问需求，如下载802.1X客户端、更新病毒库等，需要用户免认证就能获取部分网络访问权限。

免认证规则模板（free-rule-template）
- 方式1：普通的免认证规则，由IP地址、MAC地址、源接口、VLAN等参数确定。
- 方式2：关联ACL。

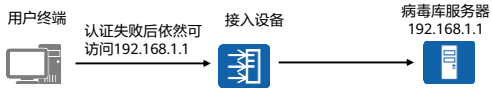


允许用户在认证成功之前访问192.168.1.1下载客户端

认证事件授权

用户在认证过程中遇到不同事件时（如认证前、认证失败、认证服务器失效等），需要拥有一定的权限。

授权参数
- VLAN：授予用户相应VLAN内的资源访问权限。
- 用户组（UCL）：根据用户组对具有相同特征的用户进行权限下发。
- 业务方案（service-scheme）：可在业务方案内绑定UCL、VLAN、QoS-profile等参数。

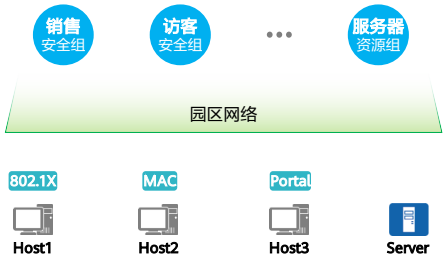


允许用户在认证失败后访问192.168.1.1更新病毒库

HUAWEI

- 根据认证事件授权的方式（一般是非认证成功状态的授权），又被称为逃生，对于不同的认证方式，有不同的逃生方案，有些逃生方案是共有的，有些逃生方案只有特定的认证方式才支持。详细内容请查阅相应产品文档中“NAC逃生”相关内容。

安全组



什么是安全组?

1. 安全组是拥有相同网络访问策略的一组用户或资源。安全组仅与用户身份有关，与用户VLAN、IP等网络信息完全解耦。
2. 安全组既可以根据5W1H条件授权给用户，符合5W1H条件的用户授权到指定安全组（动态安全组），也可以通过静态绑定IP地址的方式定义安全组（静态安全组）。

什么是资源组?

1. 对于静态的服务器资源，可以通过在安全组中绑定IP地址段的方式进行表达。但是对于IP地址集有重合的服务资源，无法通过安全组进行区分。
2. 资源组可以解决这个问题，资源组之间允许IP地址允许重复，资源组可以作为组间策略的目的地址。

HUAWEI

- 5W1H:
  - Who：接入用户的身份，例如公司的领导、普通员工、访客。
  - Where：接入用户的地点，例如园区内接入。
  - What：接入用户使用的终端类型，例如是手机接入，还是PC/便携机接入。
  - When：接入用户的时间，例如是白天接入，还是晚上接入。
  - Whose：设备归属，例如是公司终端的还是自带终端。
  - How：接入用户的方式，例如是有线接入，还是无线接入。

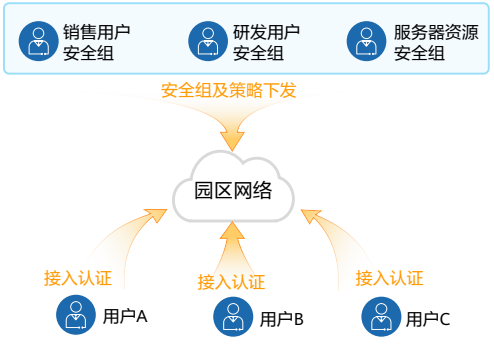
策略控制

- 安全组和资源组定义完成之后，管理员就可以基于组来定义全网的组间策略。
- 策略矩阵用于承载组间策略的配置。组间权限策略主要控制组到组之间的访问权限。

HUAWEI

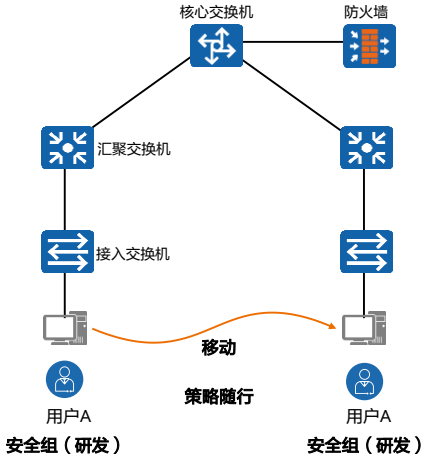
基于安全组的策略管理

- 基于安全组的策略管理，不管用户身处何地，使用哪个IP地址，都可以保证该用户获得相同的网络权限，对其执行对应的用户策略。



1. 定义基于安全组的权限控制策略，将策略下发到网络设备。
2. 用户的流量进入网络后，网络设备根据流量对应的源、目的安全组执行策略。
3. 用户执行接入认证后，获得授权的安全组。

基于安全组的权限控制



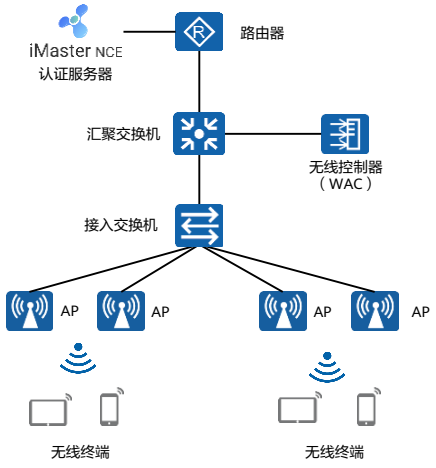
用户权限控制

- 用户权限控制都基于安全组执行。
- 用户互访权限控制：
  - 同认证点的用户互访权限控制。
  - 跨认证点的用户互访权限控制。
- 资源访问权限控制：
  - 内外网资源访问权限控制。

目录

无线用户准入控制方案

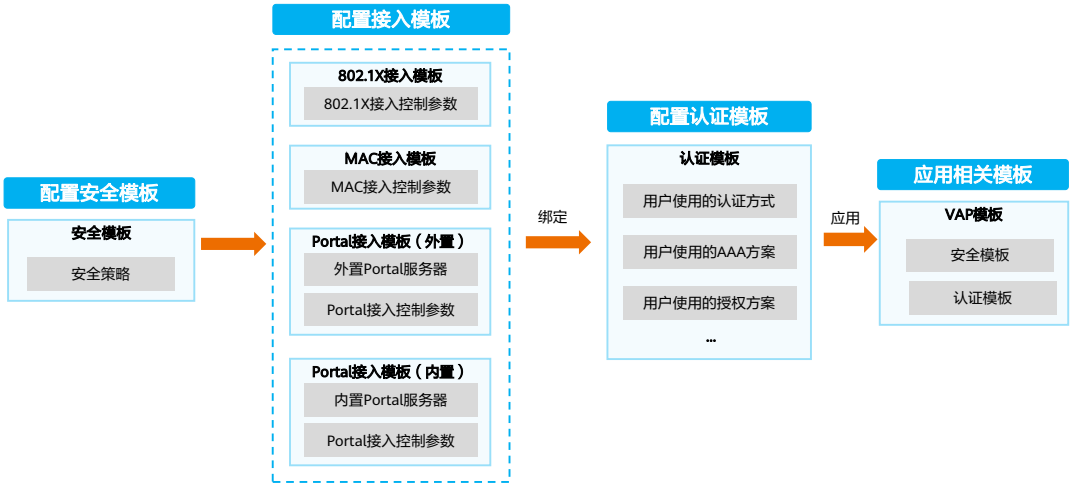
- 无线用户准入控制方案架构：
  - 客户端：笔记本电脑、手机、打印机等自带无线网卡的终端，可通过关联无线信号接入网络。
  - 接入设备：无线控制器（WAC）。
    - 终端访问网络的网络控制点；
    - 责按照客户网络制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）；
    - 授权策略的执行点。
  - 认证服务器：iMaster NCE-Campus。
    - 用于确认尝试接入网络的终端身份是否合法；
    - 指定身份合法的终端所能拥有的网络访问权限。



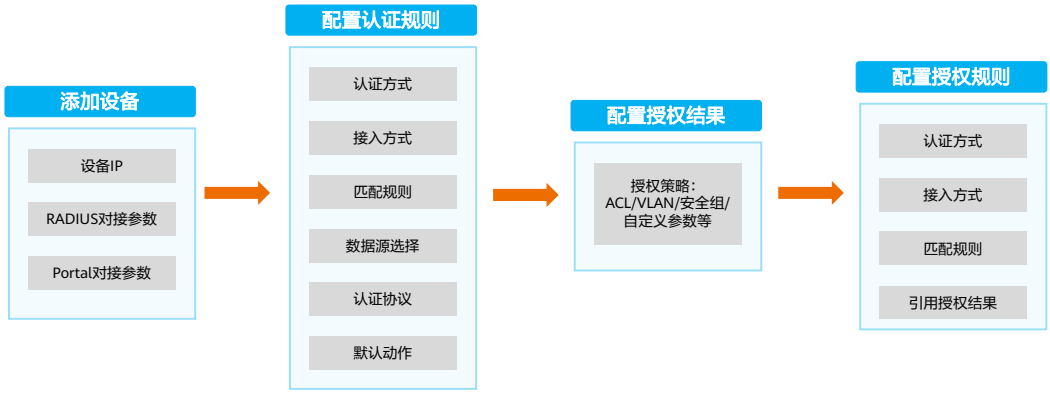
HUAWEI

- 随着无线设备的进一步普及，当前已进入全无线办公时代，以无线为中心。在办公环境中，使用无线网络替代有线网络，笔记本电脑、手机、打印机等终端更多的采用无线方式接入网络。故本课程准入控制配置方案基于无线场景介绍。

准入控制配置流程 - WAC



准入控制配置流程 - NCE



802.1X认证配置 - WAC (1)

- 配置安全模板。

```
[WAC] wlan
[WAC-wlan] security-profile name test
[WAC-wlan-sec-prof-test] security wpa-wpa2 dot1x aes （配置安全策略为WPA/WPA2-8021.X）
[WAC-wlan-sec-prof-test] quit
```

- 配置接入模板。

```
[WAC] dot1x-access-profile name test
[WAC-dot1x-access-profile-acc_test] quit
```

- 配置RADIUS服务器。

```
[WAC] radius-server template test
[WAC-radius-test] radius-server authentication X.X.X.X（RADIUS server 的IP地址) 1812
[WAC-radius-test] radius-server accounting X.X.X.X（RADIUS server 的IP地址) 1813
[WAC-radius-test] radius-server shared-key cipher Huawei@123（共享密钥，必须和RADIUS server上配置一致）
[WAC-radius-test] quit
[WAC] radius-server authorization X.X.X.X (RADIUS server 的IP地址) shared-key cipher Huawei@123（共享密钥）
```

802.1X认证配置 - WAC (2)

- 配置AAA方案。

```
[WAC-aaa] authentication-scheme test
[WAC-aaa-authen-test] authentication-mode radius
[WAC-aaa] accounting-scheme test
[WAC-aaa-authen-test] accounting-mode radius
[WAC-aaa] domain test
[WAC-aaa-domain-test] authentication-scheme test
[WAC-aaa-domain-test] accounting-scheme test
[WAC-aaa-domain-test] radius-server test
```

- 配置认证模板。

```
[WAC] authentication-profile name test
[WAC-authentication-profile-test] dot1x-access-profile test
[WAC-authentication-profile-test] access-domain test
```

- 应用认证模板、安全模板。

```
[WAC-wlan-view] vap-profile name
[WAC-wlan-vap-prof-dot1x] authentication-profile test
[WAC-wlan-vap-prof-dot1x] security-profile test
[WAC-wlan-vap-prof-dot1x] quit
```

802.1X认证配置 - NCE (1)

- 添加准入设备。选择“准入 > 准入设备 > 准入设备管理 > 创建”，示例如下。

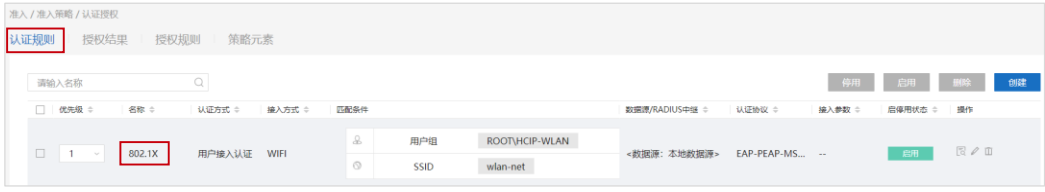
- 添加认证用户，选择“准入 > 用户管理 > 用户 > 创建”，示例如下。

HUAWEI

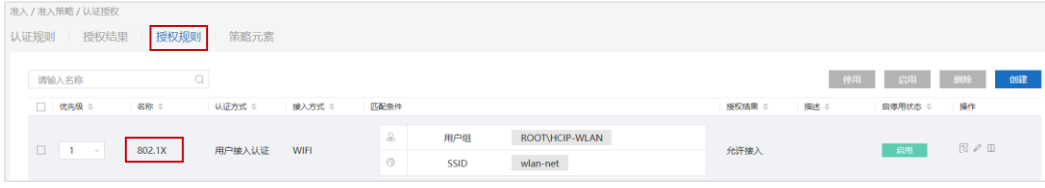
- 认证规则中的数据源如果采用本地数据源，则需要在NCE上创建认证用户（用户名、密码等信息），也可以采用外部数据源，与AD/LDAP服务器同步账号。

802.1X认证配置 - NCE (2)

- 配置认证授权，终端用户根据条件匹配认证授权规则。
  - 选择“准入 > 准入策略 > 认证授权 > 认证规则”，修改缺省认证规则或新建认证规则。



  - 选择“准入 > 准入控制 > 认证授权 > 授权规则”，关联授权结果，指定用户认证通过后允许访问的资源。



HUAWEI

- 授权结果可选用NCE默认的授权结果，如果需要下发定制的授权结果，需提前配置授权结果规则。

802.1X认证失败故障排查

- 检查认证模板是否绑定了接入模板。
  - 易错配置：security-profile配置的是security wpa-wpa2 dot1x aes，但认证模板下没有绑定dot1x接入模板。
  - 处理建议：在认证模板下绑定相应的接入模板。
- 检查WAC上是否创建了业务VLAN。
  - 易错配置：802.1X认证场景下，由于EAP报文属于控制报文需要通过CAPWAP隧道发送到WAC，所以无论是直接转发还是隧道转发，都需要确保WAC上创建了相应VLAN。
  - 处理建议：在WAC上创建相应的业务VLAN。
- 不同终端进行802.1X认证时，需要在终端上进行相关配置，详情可参考华为官网相关文档资料，本文不再详细介绍。

802.1X认证 Portal认证 MAC认证

Portal认证配置 - WAC (1)

- 配置安全模板。

```
[WAC-wlan] security-profile name test
[WAC-wlan-sec-prof-test] security open
[WAC-wlan-sec-prof-test] quit
```

- 配置接入模板。

```
[WAC] url-template name portal
[WAC-url-template-portal] url https://X.X.X.X:19008/portal （X.X.X.X为Portal服务器IP地址）
[WAC-url-template-portal] url-parameter redirect-url redirect-url ssid ssid user-ipaddress userip user-mac umac device-ip ac-ip
[WAC-url-template-portal] quit

[WAC] web-auth-server portal
[WAC-web-auth-server-portal] server-ip X.X.X.X（X.X.X.X为Portal服务器IP地址）
[WAC-web-auth-server-portal] source-ip Y.Y.Y.Y（Y.Y.Y.Y为WAC源IP地址）
[WAC-web-auth-server-portal] shared-key cipher Huawei@123（共享密钥，必须和Portal服务配置一致）
[WAC-web-auth-server-portal] url-template portal
[WAC-web-auth-server-portal] quit

[WAC] portal-access-profile name portal
[WAC-portal-access-profile-portal] web-auth-server portal direct
[WAC-portal-access-profile-portal] quit
```


HUAWEI

- 设备配置的URL参数名称需要与Portal认证服务器支持的参数名称一致，iMaster NCE-Campus支持的URL参数名称如下：
  - redirect-url参数：名称为url或者redirect-url；
  - user-ipaddress参数：名称为userip；
  - user-mac参数： 名称为usermac或者umac；
  - ssid参数： 名称为ssid；
  - device-ip参数： 名称为ac-ip；
  - ap-mac参数： 名称为apmac或者ap-mac。

Portal认证配置 - WAC (2)

- 配置RADIUS服务器（与802.1X认证配置一致）。
- 配置AAA方案（与802.1X认证配置一致）。
- 配置认证模板。

```
[WAC] authentication-profile name portal
[WAC-authentication-profile-portal] portal-access-profile portal
[WAC-authentication-profile-portal] access-domain test
[WAC-authentication-profile-portal] quit
```

- 应用认证模板、安全模板。

```
[WAC-wlan-view] vap-profile name portal
[WAC-wlan-vap-prof-portal] authentication-profile portal
[WAC-wlan-vap-prof-portal] security-profile test
[WAC-wlan-vap-prof-portal] quit
```

Portal认证配置 - NCE

- 添加准入设备。选择“准入 > 准入设备 > 创建”，添加WAC。需同时配置Radius和Portal认证参数。
- 添加认证用户、认证规则、授权规则的配置请参考802.1X认证的配置方法。

HUAWEI

Portal认证问题 - 无法认证成功

- 检查WAC上是否配置了共享密钥。
  - 易错配置：WAC上的shared-key配置需要和服务器保持一致。
  - 处理建议：建议重新配置共享密钥，再进行Portal用户认证测试。

```
[WAC] web-auth-server portal
[WAC-web-auth-server-portal] share-key cipher XXXX（共享密钥，必须和portal服务配置一致）
[WAC-web-auth-server-portal] quit
```

- 检查WAC是否关闭了STA地址学习功能。
  - 易错配置：WAC处理Portal服务器认证请求时，需要根据用户IP地址查找用户MAC，若AP不上报终端用户的IP地址，则WAC不会记录用户IP地址信息，在根据IP地址查找MAC时会失败，导致WAC无法处理Portal服务器认证请求。
  - 处理建议：开启STA地址学习功能。

```
[WAC-wlan-view] vap-profile name portal
[WAC-wlan-vap-prof-portal] undo learn-client-address ipv4 disable
```

Portal认证问题 - Portal服务器不自动推送认证页面

- 检查web-auth-server模板下是否开启了探测功能。
  - 易错配置：WAC上开启了探测功能，Portal服务器未开启，导致设备上Portal服务器的状态为Abnormal。

```
[WAC] web-auth-server portal
[WAC-web-auth-server-portal] server-detect
[WAC-web-auth-server-portal] quit
```

  - 处理建议：若Portal服务器不支持或未开启心跳探测功能，WAC上需要关闭探测功能。

```
[WAC] web-auth-server portal
[WAC-web-auth-server-portal] undo server-detect
[WAC-web-auth-server-portal] quit
```

Portal认证问题 - iOS终端不自动弹出认证页面

- 检查WAC上是否配置了Portal旁路功能。
  - 易错配置：WAC上开启了Portal旁路功能。

    ```
    [WAC] portal captive-bypass enable
    ```

  - 处理建议：建议关闭Portal旁路功能后重新测试。

    ```
    [WAC] undo portal captive-bypass enable
    ```

- 确认Portal服务器是否使用HTTPS协议推送页面。
  - 易错配置：若Portal服务器使用HTTPS协议推送页面，且Portal服务器未安装证书机构颁发的合法证书，则iOS终端不会自动弹出Portal认证页面。
  - 处理建议：检查Portal服务器是否使用HTTPS协议推送认证页面，若使用HTTPS协议，则建议安装合法证书。或者修改为HTTP协议推送。

MAC认证配置 - WAC

- 配置安全模板（与Portal认证配置一致）。
- 配置接入模板。

```
[WAC] mac-access-profile name test
[WAC-mac-access-profile-test] quit
```

- 配置RADIUS服务器（与802.1X认证配置一致）。
- 配置AAA方案（与802.1X认证配置一致）。
- 配置认证模板。

```
[WAC] authentication-profile name mac
[WAC-authentication-profile-mac] mac-access-profile mac
[WAC-authentication-profile-mac] access-domain test
[WAC-authentication-profile-mac] quit
```

- 应用认证模板、安全模板。

```
[WAC-wlan-view] vap-profile name mac
[WAC-wlan-vap-prof-mac] authentication-profile mac
[WAC-wlan-vap-prof-mac] security-profile test
[WAC-wlan-vap-prof-mac] quit
```

MAC认证配置 - NCE (1)

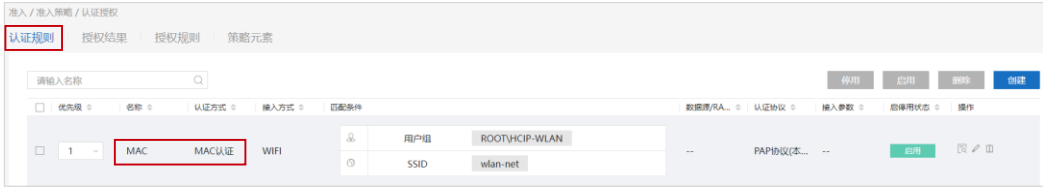
- 添加准入设备。选择“准入 > 准入设备 > 准入设备管理 > 创建”，示例如下。

- 添加认证用户，选择“准入 > 用户管理 > MAC账号 > 创建 ”，示例如下。

HUAWEI

MAC认证配置 - NCE (2)

- 配置认证授权，终端用户根据条件匹配认证授权规则。
  - 选择“准入 > 准入策略 > 认证授权 > 认证规则”，修改缺省认证规则或新建认证规则。



  - 选择“准入 > 准入控制 > 认证授权 > 授权规则”，关联授权结果，指定用户认证通过后允许访问的资源。

HUAWEI

思考题

1. （多选题）用户通过认证后，华为设备支持以下哪些权限的下发？（　　）
   A. VLAN
   B. IP地址
   C. ACL
   D. UCL组

1. ACD

本章总结

- 网络接入控制是网络安全的第一道“大门”。为了把守好这扇大门，可以在网络中部署MAC认证、802.1X认证与Portal认证等用户认证方式。这些技术的实现方式与应用场景不尽相同，需要根据网络的特点及需求进行选择与部署。
- 通过本章课程的学习，您将了解各类接入认证技术的实现原理，同时您将能够独立搭建华为准入控制网络。

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
AAA	Authentication, Authorization, and Accounting	认证，授权，计费
ACL	Access Control List	访问控制列表
AD	Active Directory	活动目录
ARP	Address Resolution Protocol	地址解析协议
C/S	Client/Server	客户端/服务器
CHAP	Challenge Handshake Authentication Protocol	挑战握手认证协议
CoA	Change of Authorization	动态授权
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHCPv6	Dynamic Host Configuration Protocol version 6	动态主机配置协议版本6
DM	Disconnect Message	用户下线报文
EAP	Extensible Authentication Protocol	扩展认证协议

缩略语表 (2)

缩略语	英文全称	解释
EAP-MD5	EAP-Message Digest Algorithm 5	基于MD5的EAP
EAPoL	EAP over LAN	EAP协议承载于局域网
EAPoR	EAP over RADIUS	EAP协议承载于RADIUS协议
EAP-PEAP	EAP-Protected Extensible Authentication Protocol	基于防护扩展验证协议的EAP
EAP-TLS	EAP-Transport Layer Security	基于传输层安全的EAP
EAP-TTLS	EAP-Tunneled Transport Layer Security	基于隧道传输层安全的EAP
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure	超文本传输安全协议
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
MAC	Media Access Control	媒体接入控制
ND	Neighbor Discovery	邻居发现

缩略语表 (3)

缩略语	英文全称	解释
PAP	Password Authentication Protocol	密码验证协议
PPP	Point-to-Point Protocol	点到点协议
QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial-In User Service	远程身份验证拨号用户服务
STA	Station	终端
TCP	Transmission Control Protocol	传输控制协议
UCL	User Control List	用户控制列表
UDP	User Datagram Protocol	用户数据报协议
VLAN	Virtual Local Area Network	虚拟局域网
VPDN	Virtual Private Dial-up Network	虚拟私有拨号网络
WAC	Wireless Access Controller	无线接入控制器

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.

企业网络安全综合案例

HUAWEI

前言

- 经过前面章节的学习，您已能掌握单个技术的部署与应用。但是在真实网络场景中，通常面临各种各样的安全挑战，安全实施工程师通常需要综合考虑各类安全威胁与应对措施，辅助设计网络安全方案，并确定方案的可行性，最终实施方案。作为网络安全运维工程师，需要时刻关注网络安全的态势，根据发现的安全威胁及时作出响应，保护企业网络安全，减少企业财产损失。
- 本章课程将介绍如何根据现网的需求，使用前面学到的技术，综合设计、实施一个网络安全方案。

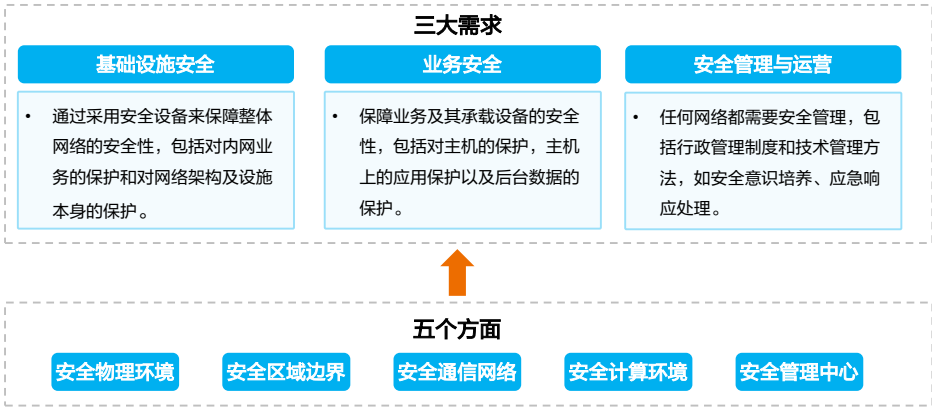
目标

- 学完本课程后，您将能够：
  - 应用各类网络安全技术
  - 设计网络安全方案
  - 部署网络安全方案
  - 熟悉网络安全运维

目录

企业网络安全需求概述

- 企业网络安全需求大致分为三部分，但是在设计对应的网络安全技术方案时，通常根据企业结构划分网络，从五个方面制定方案。

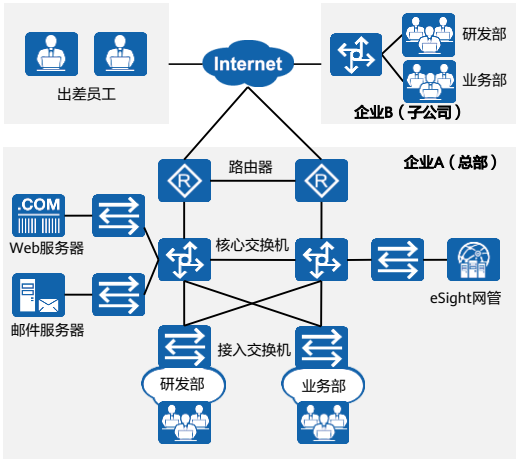


- 本章节将根据上述的安全需求和方案进行综合考虑，使用本课程学到的技术知识，模拟设计和部署一个企业网络。

目录

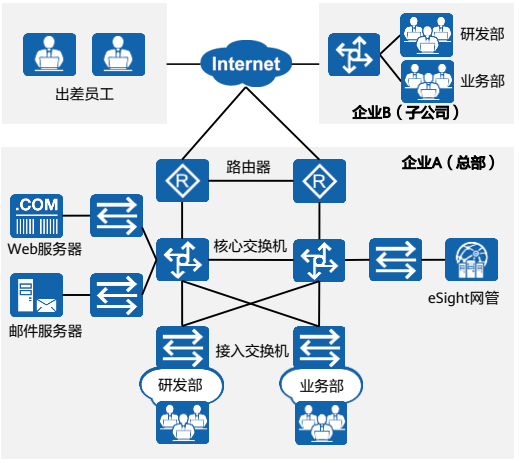
企业网络安全需求举例（1）

- 某游戏公司当前的企业网络拓扑如右图所示，考虑到该公司运行的业务可能面临众多安全威胁，需要网络实施工程师针对安全方面进行设计改造：
  - 安全需求1：企业A网络关键节点需要部署冗余设备与链路，同时质量好的链路承载较多流量；
  - 安全需求2：企业B为企业A的子公司，企业A和企业B之间有业务交流，需要保障通信安全；
  - 安全需求3：对出差员工进行身份认证，确保外部访问内网的安全；
  - 安全需求4：为了保障员工的工作效率，两家企业都需要限制员工在工作期间的流量和带宽使用，同时保障邮件、文件传输等业务的带宽；



企业网络安全需求举例 (2)

- 安全需求5：企业B专营产品研发，同时存在对接外部的业务部，需要严格隔离研发部，保障核心业务的数据安全；
- 安全需求6：作为新兴行业的企业，可能面临DDoS攻击、黑客入侵、病毒攻击等威胁，需要提前做好安全部署，同时考虑后续运维工作，如应急响应的可行性与便利性；
- 安全需求7：内部员工接入内网时，需进行身份认证，限制访问权限，同时也需要管控用户的行为，比如限制特定网站的访问权限，以免员工泄密或发布违规信息给公司造成不好的影响；
- 安全需求8：防止员工通过邮件泄露机密信息，也需要防范垃圾邮件过多占用资源或影响员工正常邮件收发。

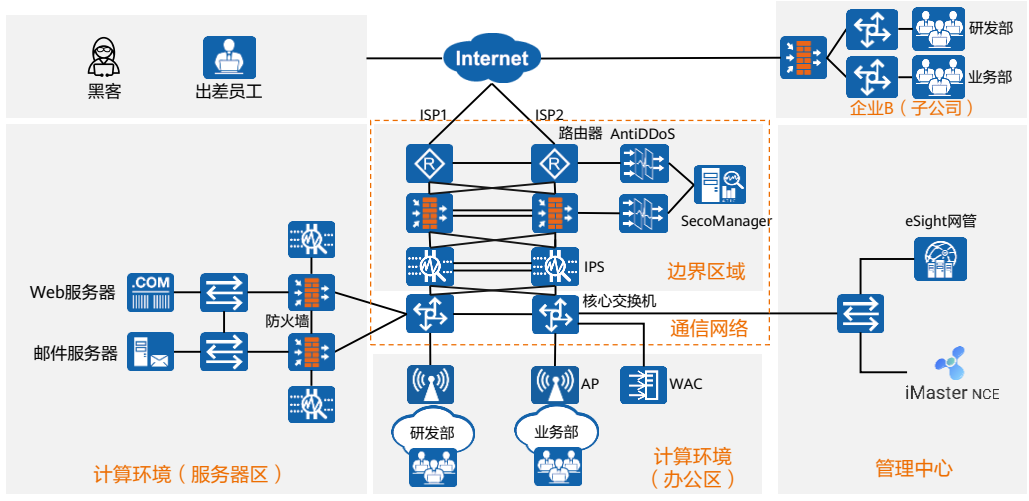


企业网络安全方案设计思路

- 设计一个企业网络安全方案需要考虑如下因素，以上述案例为例：

- 企业网络安全设计需要考虑企业架构、网络架构、企业资产、企业业务和安全风险，同时也需要考虑网络运维的可行性与便利性。
- 上述企业资产及业务等企业情况均为本案例情况。
  - 企业架构：总部分研发部和业务部，子公司同样分研发部和业务部，总部人数和网络规模较大，子公司目前处于起步阶段，总部将游戏的一个模块分给子公司开发，子公司的人数和网络规模较小。
  - 网络架构：按照网络安全的区分规则，网络架构一般分为通信网络、边界区域、计算环境和管理中心。
  - 企业资产：企业资产一般有服务器、计算机等终端和网络设备等。
  - 企业业务：该公司具备一般企业的内部管理系统、官网网站以及游戏公司特有的开发系统。
  - 安全风险：该公司具备一般企业可能遭遇的数据泄露、病毒攻击等威胁，以及游戏公司常见的DDoS攻击等。

企业网络安全方案设计



HUAWEI

- 根据五个方面将企业架构进行划分，便于后续针对提出的需求进行技术设计。

目录

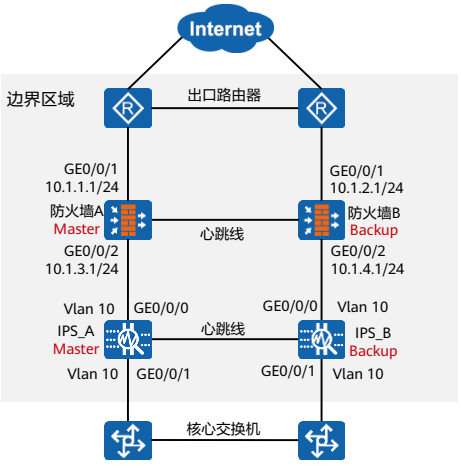
设备冗余

- 根据安全需求1，设计设备冗余安全方案：在设计该企业网络安全方案时，通常考虑在出口区域冗余部署防火墙和IPS设备。
  - 防火墙：采用三层部署方式，上连三层路由器，下连三层交换机，可以隔离区域，控制流量，同时实现冗余备份。
  - IPS设备：采用双机直路部署，上连防火墙，下连三层交换机，可以进行网络基础防护，包括反病毒与入侵防御。
- 防火墙双机热备关键配置，以防火墙A为例：
  - 采用基于动态路由协议实现双机热备业务口监控：

```
[FW_A] hrp adjust ospf-cost enable
[FW_A] hrp track interface GE0/0/1
[FW_A] hrp track interface GE0/0/2
```

- IPS双机热备关键配置，以IPS_A为例：
  - 业务口监控：

```
[IPS_A] hrp track vlan GE0/0/1
```



HUAWEI

- IPS设备与防火墙的双机热备原理一致。

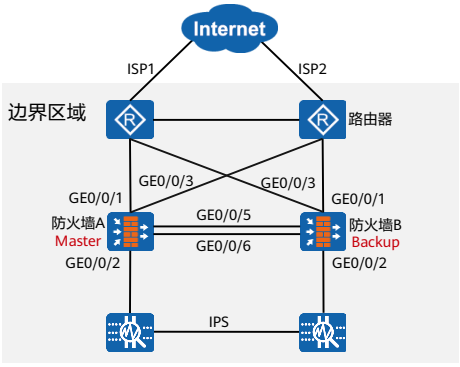
链路冗余

- 根据安全需求1，设计链路冗余安全方案：对于核心区域的设备需要冗余部署通信链路。在冗余部署链路时，通常需要考虑部署相应辅助技术，以防火墙A为例，需要部署选路技术和链路聚合技术。
  - 智能选路：根据链路质量负载分担流量，健康探测结果表示ISP1的丢包率、时延和时延抖动最低。关键配置如下：

```
[FW_A] multi-interface
[FW_A-multi-inter] mode priority-of-link-quality
[FW_A-multi-inter] add interface GigabitEthernet 0/0/1
[FW_A-multi-inter] add interface GigabitEthernet 0/0/3
```

  - 链路聚合：提高心跳线可靠性，手动聚合，成员接口数为2，最小活动链路为2。关键配置如下：

```
[FW_A] interface Eth-Trunk 1
[FW_A-Eth-Trunk1] trunkport GigabitEthernet 0/0/5
[FW_A-Eth-Trunk1] trunkport GigabitEthernet 0/0/6
```



HUAWEI

- 对于二层直路部署的IPS设备，需要考虑部署链路聚合技术增加心跳线可靠性。
- 对于核心交换机，则需要考虑路由部署和路由选路。

加密传输（1）

- 根据安全需求2：保障企业A与企业B之间的通信安全，设计安全方案：在企业B出口处部署防火墙，并在企业A和企业B的防火墙之间部署IPSec VPN。
- IPSec VPN关键配置如下，以防火墙A为例：
  - 配置需加密流量：

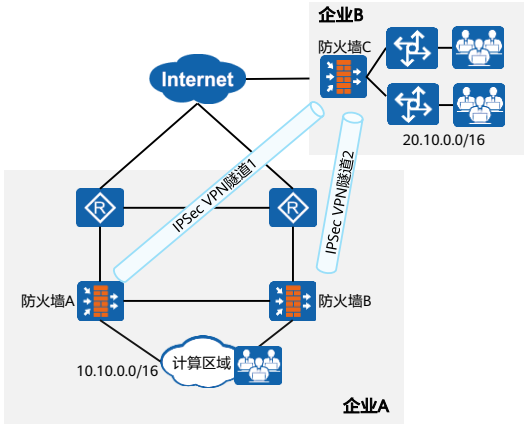
```
[FW_A] acl 3001
[FW_A-acl-adv-3001] rule permit ip source 10.10.0.0 0.0.255.255
destination 20.10.0.0 0.0.255.255
```

  - 配置NAT穿越：

```
[FW_A] ike peer FW
[FW_A-ike-peer-FW] nat traversal
```

  - DPD（Dead Peer Detection）配置：

```
[FW_A] ike peer FW
[FW_A-ike-peer-FW] dpd type on-demand
```

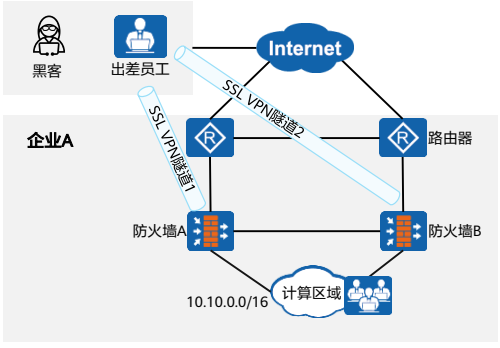


HUAWEI

- 企业B部署IPSec VPN，不一定需要防火墙，也可在路由器和交换机上完成。此处部署防火墙，可为企业B的网络增加一道基础安全防线。
- 此处企业A和企业B交流皆为IP单播业务，考虑部署IPSec VPN；如实际部署时企业交互存在非IP单播业务（如组播业务），可考虑部署GRE over IPSec。
- 企业A的防火墙A和防火墙B形成负载均衡，分别与企业B的防火墙C建立点到点IPSec VPN，隧道不备份，同时部署DPD。当防火墙A去往防火墙C的链路故障时，从隧道1转发的流量自动切换到隧道2转发，提升IPSec VPN隧道的可靠性。

加密传输 (2)

- 安全需求3：对出差员工进行身份认证，确保外部访问内网的安全。
- 安全方案：L2TP over IPSec或SSL VPN均可满足员工身份认证和访问机密性的需求。相较于L2TP over IPSec，SSL VPN具备部署和配置简单、精细化控制权限的优点。本方案中采用SSL VPN。



加密传输 (3)

- SSL VPN关键配置如下，以防火墙A为例：
  - 虚拟网关

  - 网络扩展

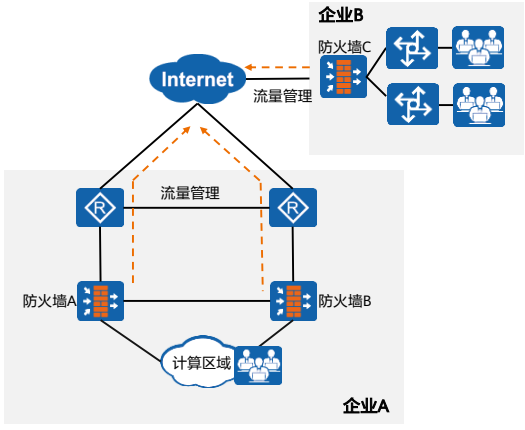
加密传输 (4)

- 安全策略
  - 允许外网用户登录虚拟网关；

  - 允许网络扩展用户访问内网资源。

流量管理 (1)

- 安全需求4：为了保障员工的工作效率，两家企业都需要限制员工在工作期间的流量和带宽使用，同时保障邮件、文件传输等业务的带宽。
- 安全方案：通过在企业A和企业B的防火墙上配置带宽管理和配额控制策略，保障关键业务的带宽。
  - 带宽管理：通过设置最大带宽，限制P2P、在线视频的流量；通过保证带宽，保障邮件、文件传输的流量。
  - 配额控制：限制普通员工每日上网流量500 MB，当上网流量超过500 MB时，限制其最大速率为200 Kbps。



流量管理 (2)

- 带宽管理关键配置如下，以防火墙A为例：
  - 针对Email、文件传输配置保证带宽：

```
[FW_A] traffic-policy
[FW_A-policy-traffic] profile profile_p2p
[FW_A-policy-traffic-profile-profile_p2p] bandwidth maximum-bandwidth whole both 30000
[FW_A-policy-traffic-profile-profile_p2p] bandwidth connection-limit whole both 10000
```

  - 针对P2P、在线视频配置最大带宽：

```
[FW_A-policy-traffic] profile profile_email
[FW_A-policy-traffic-profile-profile_email] bandwidth guaranteed-bandwidth whole both 60000
```

- 配额控制关键配置如下：
  - 限制员工每日上网流量：

```
[FW_A] quota-policy
[FW_A-policy-quota] profile quota_employee
[FW_A-policy-quota-profile-quota_employee] stream-daily 500
[FW_A-policy-quota-profile-quota_employee] limit-bandwidth 200
```

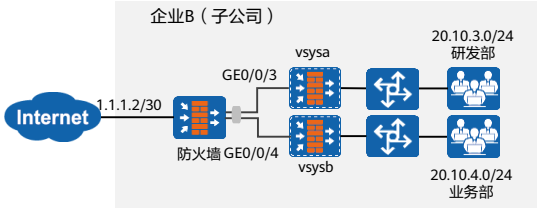
网络隔离

- 安全需求5：企业B专营产品研发，同时需要对接业务部，需要严格隔离研发部，保障核心数据的安全。
- 安全方案：企业B网络架构较简单，仅有一台防火墙。通过防火墙上部署虚拟系统，对业务部和研发部进行隔离。针对研发部和业务部分别创建独立的虚拟系统vsysa和vsysb。业务部可以访问互联网，研发部无法访问互联网；业务部和研发部互不相通。
- 虚拟系统关键配置，以vsysa为例：
  - 访问互联网，vsysa路由配置：

    ```
    [vsysa] ip route-static 0.0.0.0 0.0.0.0 public
    ```

  - 访问互联网，根系统路由配置（假设1.1.1.2是根系统到Internet到的下一跳）：

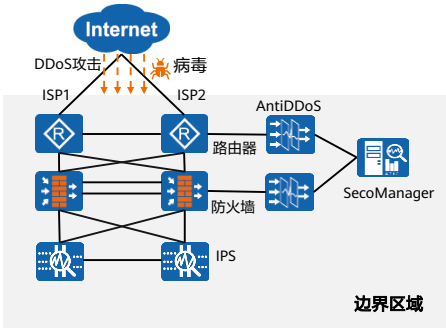
    ```
    [FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
    ```



目录

攻击防范 (1)

- 安全需求6：对网络攻击进行防范，如DDoS攻击、黑客入侵、病毒攻击等威胁。
- 安全方案：采用AntiDDoS设备防范DDoS攻击，在IPS设备上部署入侵防御、反病毒等功能。

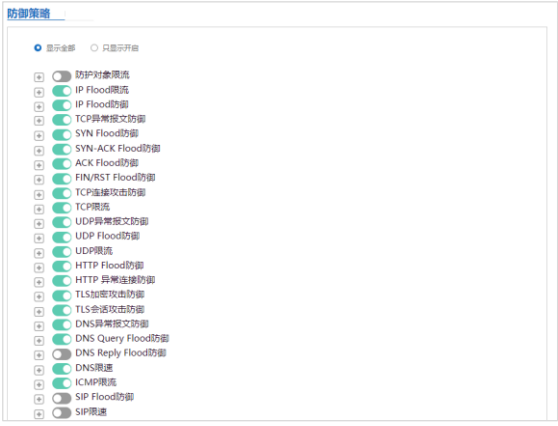


HUAWEI

- IPS入侵防御技术：在IPS设备上部署，保护计算区域和管理中心。检测并防御服务器/客户端上传或下载方向的入侵行为，如黑客对内网Web服务器进行SQL注入。
- IPS反病毒技术：在IPS设备上部署，保护计算区域和管理中心。检测并防御用户在访问外网的过程中、或服务器对外网开放访问时遭受的病毒、蠕虫、木马等恶意代码攻击，如内网用户收到病毒邮件。
- 如企业需要防范APT攻击，不仅需要在IPS设备上部署入侵防御和病毒防范技术，还需要IPS设备与沙箱联动，沙箱非本课程知识点，此处不再详细介绍。

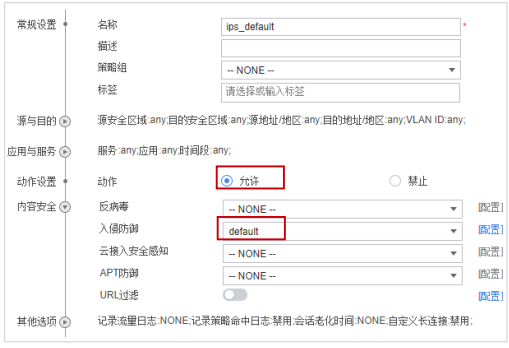
攻击防范 (2)

- AntiDDoS关键配置，以防护Web服务器为例，根据需求开启相关防御策略：



攻击防范 (3)

- IPS设备入侵防御技术关键配置：

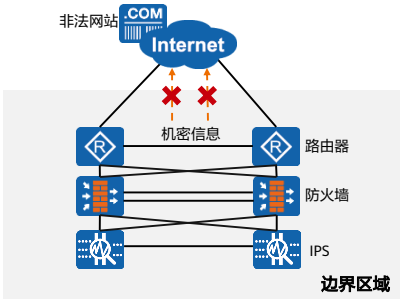


- IPS设备反病毒技术关键配置：

HUAWEI

内容安全 (1)

- 安全需求7：内部员工接入内网时需要管控用户的行为，比如限制特定网站的访问权限。
- 安全方案：通过在防火墙上部署内容安全过滤技术，通过技术手段限制用户的不恰当行为。
  - 内容过滤：当内网用户上传企业机密信息或发布违规信息时，防火墙及时识别并阻断信息的传播。
  - URL过滤：企业允许员工访问门户类网站、科学类网站；禁止访问娱乐类网站和非法网站。



- 内容安全过滤技术包括URL过滤、DNS过滤、文件过滤、应用行为控制、邮件过滤、内容过滤等，此处仅根据本案例需求部署了内容过滤、URL过滤和邮件过滤。网络工程师在现网环境具体设计实施时，根据企业真实需求和安全风险制定相关措施。

内容安全 (2)

- 防火墙内容过滤关键配置：

- 防火墙URL过滤关键配置：

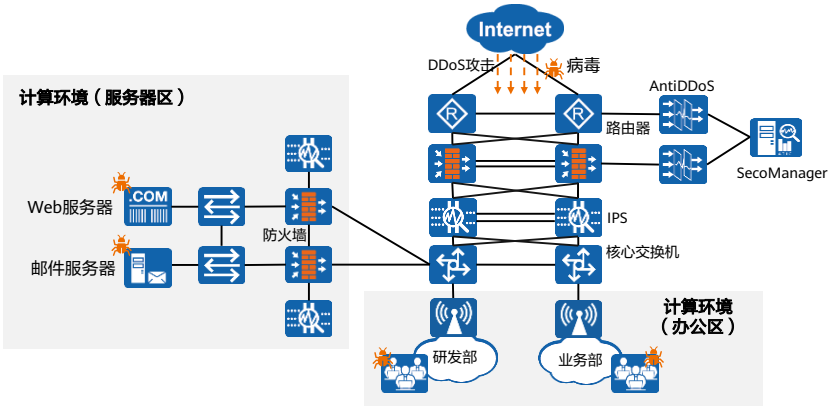
HUAWEI

- 注：在配置URL过滤策略时，需要配置两条URL过滤配置文件，一条设置URL过滤级别为中，对所有非法网站进行阻断，同时允许访问搜索/门户类网站和休闲类网站，应用在安全策略中，安全策略动作为允许；另一条URL过滤配置文件禁止访问休闲类网站，应用在安全策略中，时间段为工作时间，安全策略动作为允许，将该条安全策略前置。

目录

攻击防范

- 安全需求6：对网络攻击进行防范，如DDoS攻击、黑客入侵、病毒攻击等威胁。
- 安全方案：采用AntiDDoS设备防范DDoS攻击，在IPS设备上部署入侵防御、反病毒等功能。

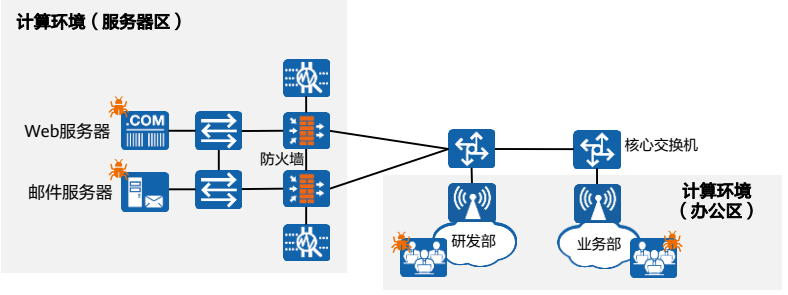


HUAWEI

- 设备关键配置与边界区域设计中的AntiDDoS及IPS配置基本一致，不再赘述。

内容安全 (1)

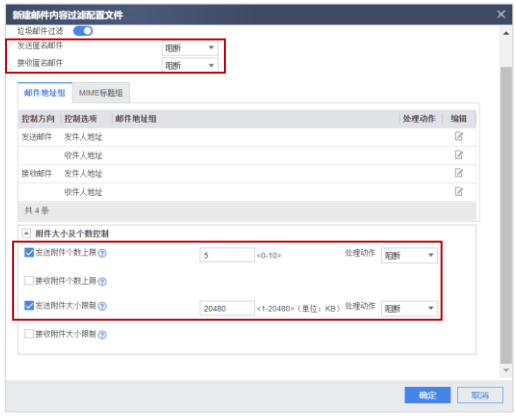
- 安全需求7：内部员工接入内网时需要管控用户的行为，比如限制特定网站的访问权限。
- 安全需求8：防止员工通过邮件泄露机密信息，也需要防范垃圾邮件过多占用资源或影响正常邮件收发。
- 安全方案：通过在防火墙上部署内容安全过滤技术，通过技术手段限制用户的不恰当行为。
  - 邮件过滤：对邮件收发行为进行管控，包括防止垃圾邮件和匿名邮件泛滥，控制违规收发等。



- 针对计算环境区域也存在安全需求6和7，相关配置和边界区域类似，不再介绍。

内容安全 (2)

- 邮件过滤关键配置：在防火墙上限制邮件发送附件大小不超过20 MB，数量不超过5个；不允许收发匿名邮件，需要过滤垃圾邮件。

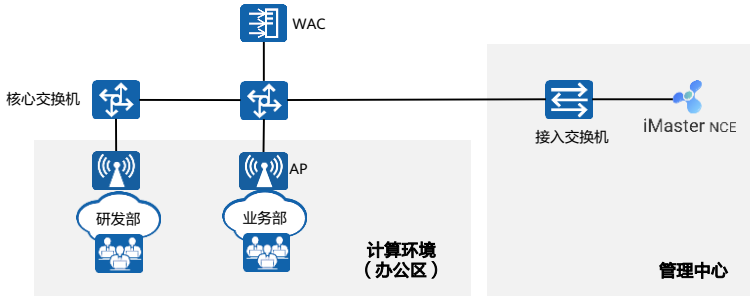


HUAWEI

目录

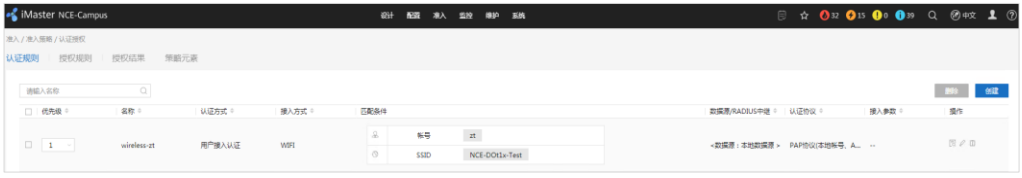
准入控制 (1)

- 安全需求7：内部员工接入内网时，需要进行身份认证，认证通过后方可接入网络，同时对用户行为进行管控。
- 安全方案：管理中心设计部署准入服务器iMaster NCE-Campus，要求内部员工接入内网时，需要认证身份，并且根据员工角色授予不同访问权限。另外需要为访客提供接入网络，限制访客访问权限。



准入控制 (2)

- iMaster-NCE关键配置：根据认证方式及访问网络访问权限的不同创建认证规则、授权规则。



准入控制 (3)

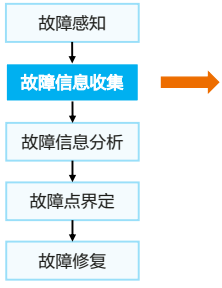
- WAC关键配置：完成相关认证配置后，为保证授权权限成功下发，需在设备上配置对应的权限。以通过用户组授权为例：

```
[WAC] acl 3001
[WAC-acl-adv-3001] rule 1 permit ip destination 10.23.200.2 0
[WAC-acl-adv-3001] rule 2 deny ip destination any
[WAC-acl-adv-3001] quit
[WAC] user-group group1
[WAC-user-group-group1] acl-id 3001
[WAC-user-group-group1] quit
```

目录

故障处理流程

- 故障处理的基本思想是：将导致故障的所有可能原因缩减或隔离成几个小的子集，从而使问题的复杂度迅速下降。故障处理需要遵循按照合理的步骤找出故障原因并解决故障的总体原则。
- 故障的发生可以从用户侧感知（比如，无法上网），也可以从网络侧感知（比如，设备出现异常告警）。感知到故障后，需要第一时间收集各设备的故障信息，然后对故障信息进行分析，定界故障点后进行恢复处理。对于方案级的整网故障处理，关键是根据故障现象快速将故障发生点定界到部件，然后再进行恢复处理。



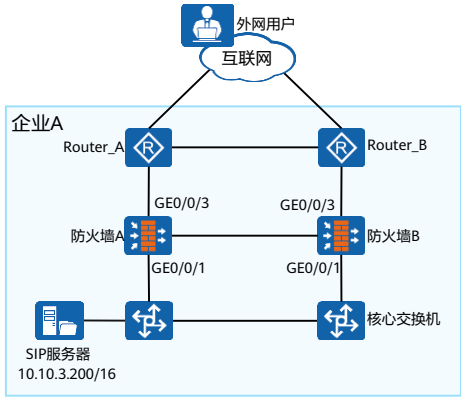
故障信息收集
- 故障基本信息：故障时间、故障现象、严重程度、组网信息及已采取的措施等；
- 运行状态信息：启动配置、当前配置、接口信息、系统版本等；
- 设备日志信息：设备发生故障时产生的日志信息；
- 智能诊断信息：智能诊断工具对设备或用户诊断后产生的诊断信息。

HUAWEI

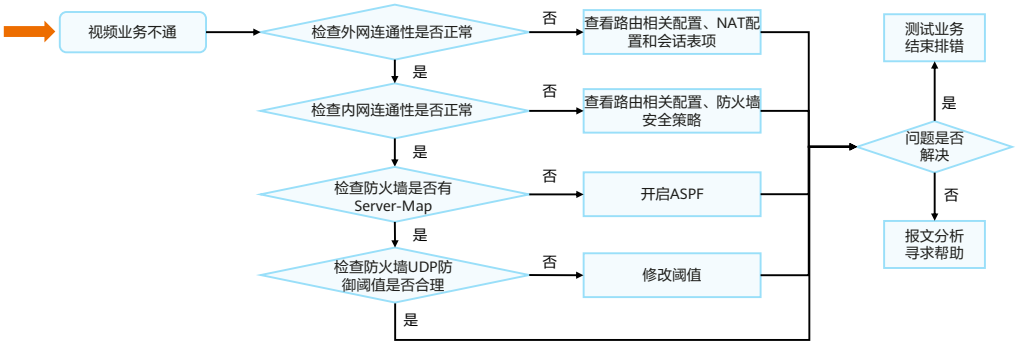
- 故障处理原则：
  - 以尽快恢复系统为原则。
  - 定位故障时，应及时采集故障数据信息，并尽量将采集到的故障数据信息保存在移动存储介质或网络中的其它计算机中。
  - 在确定故障处理的方案时，应先评估影响，优先保证业务的正常传送。

故障1：视频业务无法正常通信 (1)

- 故障现象：该企业需要增设视频会议，用于内部会议或与外部客户沟通，在进行业务割接验证时，发现外网用户不能正常使用视频业务。



故障1：视频业务无法正常通信 (2)



视频业务故障排查技巧 - 检查连通性

- 检查外网连通性：
  - 使用Ping、Tracet命令检查外网连通性是否正常，如果出现错误先检查相关路由配置信息。
  - 检查NAT策略和映射，如果配置错误需要进行修改：

```
[FW_A] display nat-policy rule all
[FW_A] display nat server
```

  - 检查防火墙会话：

```
[FW_A] display firewall session table
Current Total Sessions : 1
 SIP  VPN: public --> public  100.1.1.100:2052 --> 10.10.3.200:5060
```

  - 如果NAT配置错误，重新配置后需要立即生效可以清除会话表信息：

```
[FW_A] reset firewall session table
```


- 注意事项：清除会话表信息后，所有当前需要通过查找会话表才能转发报文的连接及业务会被强行中断。终端用户需要重新发起连接才能通信。所以若无必要，请不要清除会话表信息。
- 检查内网连通性：
  - 在测试内网连通性时，可使用Ping或直接访问服务测试，若使用Ping测试，需要在防火墙上短暂放通Ping行为，测试完毕即刻删除。
  - 在安全策略排障过程中，如果发现两台防火墙安全策略不一致，则需要检查防火墙双机热备相关配置。

视频业务故障排查技巧 - 检查表项

- 检查防火墙Server-Map表：

```
[FW_A] display firewall server-map
```

- 检查防火墙是否开启SIP协议的ASPF功能，若未开启，则需要手动开启：

```
[FW_A] firewall detect sip
```

  - 再次查看防火墙的Server-Map表；
  - 再次查看防火墙的会话表；
  - 验证外网用户使用视频会议的效果。

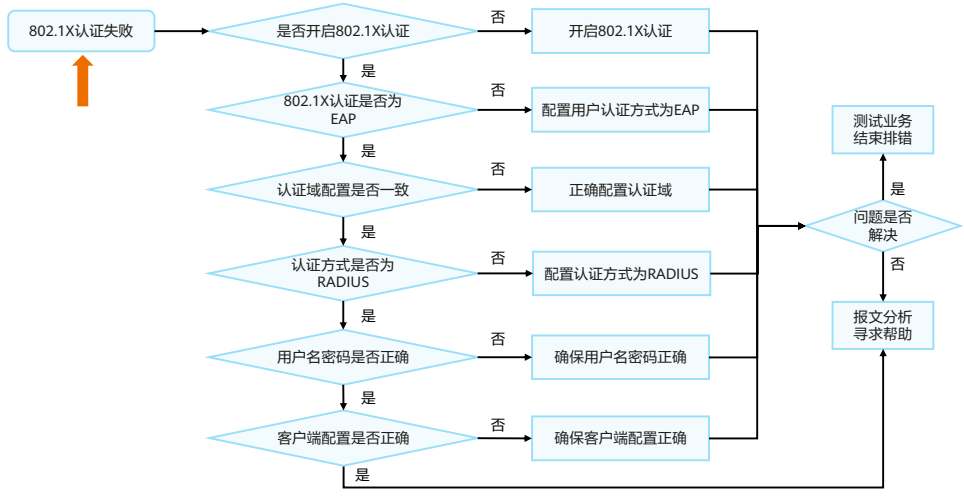
视频业务故障排查技巧 - 检查防火墙UDP攻击防范设置

- 检查防火墙UDP限流阈值：

```
[FW_A] display anti-ddos baseline-learn information
 Baseline Learn Information Table
 ------------------------------------------------------------------------------------------
 AttackType                DefendDeployed     AlertRate     LearnResult          Unit
 ------------------------------------------------------------------------------------------
 Syn   flood attack        Yes                2000          0                    pps
 UDP   flood attack limit  Yes                1             ---                  Mbps
 Icmp flood attack         Yes                2000          0                    pps
 ------------------------------------------------------------------------------------------
```

- 发现UDP限流的阈值设置不合理，导致防火墙直接丢弃超过阈值的UDP报文，修改方案如下：
  - 可以根据业务实际情况，对UDP限流阈值进行调整，或者可以关闭UDP限流功能。

故障2：内网用户接入网络失败 - 802.1X认证



HUAWEI

查看是否开启了802.1X认证

- 查看认证模板“dot1x” 下是否引用了802.1X接入模板“dot1x”。

```
<WAC> system-view
[WAC] authentication-profile name dot1x
[WAC-authentication-profile-dot1x] display this
#
authentication-profile name dot1x
 dot1x-access-profile dot1x
```

- 如果未引用802.1X接入模板，则在认证模板视图下引用802.1X接入模板。

```
[WAC-authentication-profile-dot1x] dot1x-access-profile dot1x
```

- 查看VAP模板“dot1x”下是否引用了认证模板“dot1x”。

```
[WAC-wlan] vap-profile name dot1x
[WAC-wlan-vap-prof-dot1x] display this
#
 forward-mode tunnel
 service-vlan vlan-id 101
 ssid-profile 1
 security-profile 1
 authentication-profile dot1x
```

- 如果未引用认证模板，则在VAP模板视图下引用认证模板。

```
[WAC-wlan-vap-prof-dot1x] authentication-profile dot1x
```

检查用户认证方式是否为EAP

- 802.1X认证包括EAP、CHAP和PAP三种方式，需保证客户端与服务器均支持该种方式，否则用户无法通过认证。
- 手机等移动终端仅支持EAP方式，所以设备上也应配置为EAP方式，EAP方式为设备的默认配置。
- 查看802.1X接入模板下配置的用户认证方式。

```
<WAC> display dot1x-access-profile configuration name dot1x
  Profile Name                    : dot1x
  Authentication method           : EAP
  Re-Authen                       : Disable
  Client-no-response authorize    : -
  Max retry value                 : 2
  Reauthen Period                 : 3600s
  Client Timeout                  : 5s
  Bound authentication profile    : dot1x
```

- 如果认证方式不是“EAP”，则配置为“EAP”。

```
<WAC> system-view
[WAC] dot1x-access-profile name dot1x
[WAC-dot1x-access-profile-dot1x] dot1x authentication-method eap
```

检查认证域配置是否正确

- 在802.1X认证配置中，需要配置AAA方案，可以包括认证方案模板、计费方案模板、授权方案模板和业务方案模板。认证方案选用RADIUS认证，还需要配置RADIUS服务器模板，设置和服务器对接的参数。
- 查看认证模板下的配置方式，方案直接引用到认证模板。

```
[WAC] authentication-profile name dot1x
[WAC-authentication-profile-dot1x] display this
#
authentication-profile name dot1x
 dot1x-access-profile dot1x
 authentication-scheme radius
 accounting-scheme radius
 radius-server radius
#
```

- 域引用到认证模板。

```
[WAC-aaa] domain radius
[WAC-aaa-domain-radius] display this
#
 domain radius
  authentication-scheme radius
  accounting-scheme radius
  radius-server radius
#
```

```
[WAC] authentication-profile name dot1x
[WAC-authentication-profile-dot1x] display this
#
authentication-profile name dot1x
 dot1x-access-profile dot1x
 access-domain radius
#
```


HUAWEI

- 实现上述配置有两种方式：
  - 将方案直接引用到认证模板。
  - 先将方案引用到域，再将域引用到认证模板。
- 如果两种方式同时配置，则方案直接引用到认证模板的方式，优先级更高。所以先查看认证模板下的配置方式，再进入到对应的视图下查看配置是否正确。

检查认证方式和用户名密码

- 若不使用认证域进行认证，需要检查认证模板下绑定的认证方案模板下配置的认证方式是否为RADIUS认证。
- 若使用认证域进行认证，需要检查认证域下绑定的认证方案模板下配置的认证方式是否为RADIUS认证。
- 通过命令行查看认证方案模板下认证方式。

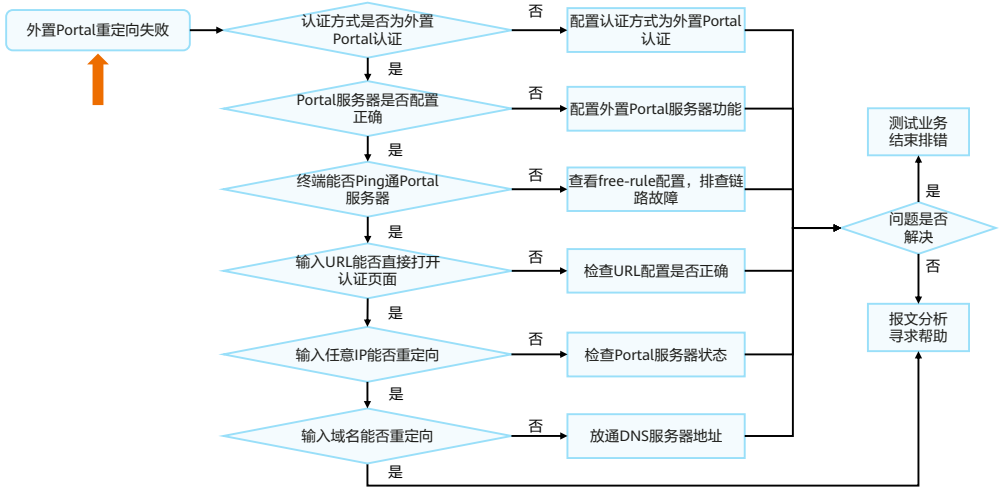
```
[WAC-aaa] authentication-scheme radius
[WAC-aaa-authen-radius] display this
#
 authentication-scheme radius
  authentication-mode radius
#
```

- 执行命令**test-aaa**查看设备与RADIUS服务器是否可达，并可验证用户名密码是否正确。

```
[WAC] test-aaa test huawei123 radius-template radius
```

- 执行命令后，根据提示信息判断：
  - 若提示信息显示为“Account test succeed”，则说明设备与RADIUS服务器链路正常，且测试用户名密码正确。
  - 若提示信息显示为“User name or password is wrong”，则说明设备与RADIUS服务器链路正常，但用户名密码信息错误，需要检查用户名密码信息。
  - 若提示信息显示为“Account test time out”，则说明认证设备与RADIUS服务器不可达或RADIUS服务器模板配置不正确。

故障3：访客接入网络重定向页面失败 - Portal认证



检查Portal认证配置是否正确

- 通过命令行查看Portal接入模板下是否开启外置Portal服务器功能。

```
[WAC] portal-access-profile name portal_access_profile
[WAC-portal-access-profile-portal_access_profile] display this
#
portal-access-profile name portal_access_profile
 web-auth-server portal direct
```

- 查看Portal接入模板是否绑定在认证模板下。

```
[WAC] authentication-profile name portal_authen_profile
[WAC-authentication-profile-portal_authen_profile] display this
#
authentication-profile name portal_authen_profile
 portal-access-profile portal_access_profile
 free-rule-template default_free_rule
#
```

- 查看认证模板是否绑定在VAP模板下。

```
[WAC-wlan-view] vap-profile name portal_authen_test
[WAC-wlan-vap-prof-portal_authen_test] display this
#
 forward-mode tunnel
 service-vlan vlan-id 200
 ssid-profile portal_authen_test
 authentication-profile portal_authen_profile
#
```

检查Portal服务器是否配置正确

- 查看外置Portal服务器配置。

```
[WAC] display web-auth-server configuration
 Listening port: 2000
 Portal: version 1, version 2
 Include reply message : enabled
 ------------------------------------------------------------------------
 Web-auth-server Name : portal
 IP-address           : 192.168.13.1
 Shared-key           : %^%#xZD=PF^$,"+n#W3@LRoB!x^~Hco42X\p@UJaw]h#%^%#
 Source-IP            : -
 Port / PortFlag      : 50100 / NO
 URL                  : http://192.168.13.1:8080/PortalServer
 URL Template         : portal
 Redirection          : Enable
 Sync                 : Disable
 Sync Seconds         : 0
 Sync Max-times       : 0
 Detect               : Disable
 Detect Seconds       : 60
 Detect Max-times     : 3
 Detect Critical-num  : 0
 Detect Action        :
 Bound Portal profile : portal_test
 ------------------------------------------------------------------------
1 Web authentication server(s) in total
```

检查终端是否能Ping通Portal服务器

- 若不能Ping通外置Portal服务器地址，则检查free-rule是否在AP上应用。

```
[AP] diagnose
[AP-diagnose] display portal free-rule
-------------------------------------------------------------------------------------------------------
Dynamic free rule
 destination ip 10.10.10.10 mask 255.255.255.255 source ip x.x.x.x mask 255.255.255.255 vlan x
Total 1
-------------------------------------------------------------------------------------------------------
......
```

- 查看终端网关是否有指向外置Portal服务器的路由，若没有，请添加路由。
- 查看Portal服务器是否有指向终端网关的路由，若没有，请添加路由。

URL跳转测试

- 在终端浏览器直接输入外置Portal服务器URL，查看能否打开认证页面。
- 若不能打开认证页面，则检查设备上外置Portal服务器URL配置是否正确。
- 若是在web-auth-server模板下配置了URL模板，则执行命令display url-template查看配置是否正确。

```
[WAC] display url-template name portal
 Name                 : portal
 URL                  : http://192.168.13.1:8080/PortalServer
 Start mark           : ?
 Assignment mark      : =
 Isolate mark         : &
 AC IP                :
 AC MAC               :
 AP IP                :
 AP MAC               :
 SSID                 :
 User MAC             :
 Redirect URL         :
 User IP address      :
 Sysname              :
 Delimiter            :
 Format               :
......
```

检查URL中参数配置是否正确

- 对接第三方Portal服务器时，URL中可能需要携带指定参数，Portal服务器可根据URL中的参数获取到用户终端的信息，并根据获取到的用户终端信息为不同用户提供不同的Web认证界面。
- 设备支持在URL中携带的参数包括WAC的系统名称、WAC的IP地址、WAC的MAC地址、AP的IP地址、AP的MAC地址、用户关联的SSID、用户的IP地址、用户的MAC地址和用户访问的原始URL地址等参数。
- 当URL中需要携带参数时，只能通过URL模板配置。

```
[WAC] url-template name portal
[WAC-url-template-portal] url-parameter ac-ip acip ap-ip apip user-mac usermac
```

IP地址跳转测试

- Portal认证时，在浏览器中输入任意IP地址（非免认证规则放通的地址），都可以跳转到Portal认证页面进行认证。
- 在终端浏览器输入任意IP地址（非免认证规则放通的地址），查看能否重定向出Portal认证页面。
- 在终端浏览器输入HTTPS协议的网站时无法打开重定向页面，需要使能Portal认证HTTPS重定向功能。

```
[WAC] portal https-redirect enable
```

- 若不能重定向出Portal认证页面，则在WAC上通过命令行查看Portal服务器状态。

```
<WAC> display server-detect state
 Web-auth-server          :portal
 Total-servers            :1
 Live-servers             :1
 Critical-num             :0
 Status                   :Normal
 IP-address               Status
 192.168.13.1             UP
```


- 用户访问HTTPS协议的网站触发Portal认证时，浏览器会弹出安全提示，需要用户点击继续才能完成Portal认证。
- 执行HSTS的浏览器或网站不能进行重定向。
- 如果用户发送的HTTPS请求报文的目的端口号是非知名端口（443），则不能进行重定向。
- WAC上通过命令行查看Portal服务器状态。
  - 若服务器状态为Abnormal，需要确认Portal服务器侧是否支持探测及是否开启探测。
  - 若服务器支持探测，则需要开启探测。
  - 若服务器侧不支持探测，则需要在设备侧通过以下命令行关闭探测。
    - [WAC] **web-auth-server portal**
    - [WAC-web-auth-server-portal] **undo server-detect**

检查DNS相关配置

- 如果直接输入IP地址能够重定向出认证页面，但输入域名无法重定向，查看DNS服务器IP地址是否加入到免认证规则中。
- 查看DNS服务器IP是否加入到免认证规则中。

```
[WAC] free-rule-template name portal_free_rule
[WAC-free-rule-portal_free_rule] display this
#
free-rule-template name portal_free_rule
 free-rule 1 destination ip 10.72.55.101 mask 255.255.255.255
#
```

思考题

1. （多选题）针对企业的安全需求，在设计的时候可以从以下哪些方面进行考虑？（　　）
   A. 安全物理环境
   B. 安全区域边界
   C. 安全通信网络
   D. 安全计算环境
   E. 安全管理中心

1. ABCDE

本章总结

- 本章节通过案例的形式，介绍了企业网络安全的方案设计与技术部署，以及故障处理思路与关键步骤。
- 通过本课程的学习，您将能够面对真实的网络需求，设计安全方案、部署安全技术以及进行故障处理，同时对网络实施工程师与网络安全运维工程师的工作职责与内容具备更直观的了解。

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
AP	Access Point	接入点
ASPF	Application Specific Packet Filter	基于应用的包过滤
CHAP	Challenge Handshake Authentication Protocol	挑战握手认证协议
DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name Server	域名服务器
DPD	Dead Peer Detection	失效对等体检测
EAP	Extensible Authentication Protocol	扩展认证协议
ERP	Enterprise Resource Planning	企业资源计划
IPS	Intrusion Prevention System	入侵防御系统
ISP	Internet Service Provider	互联网服务提供商

缩略语表 (2)

缩略语	英文全称	解释
NAT	Network Address Translation	网络地址转换
OA	Office Automation	办公自动化
P2P	Point-to-Point	点对点
PAP	Password Authentication Protocol	密码验证协议
SIP	Session Initiation Protocol	会话发起协议
SSID	Service Set Identifier	服务集标识符
URL	Uniform Resource Locator	统一资源定位符
WAC	Wireless Access Controller	无线接入控制器

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.