HUAWEI NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 系列 V800R023C00SPC500

配置指南

文档版本 01

发布日期 2023-09-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

插图目录

表格目录

1 配置

1.1 安全加固指南

1.1.1 前 言

概述

本文档针对安全加固策略，从网络安全风险、HUAWEI NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X系列安全风险、HUAWEI NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X系列的安全架构和安全加固策略等方面指导用户加强网络安全和设备安全。

本文档与其它类型手册相结合，便于读者深入掌握安全加固策略。

产品版本

与本文档相对应的产品版本如下所示。

产品名称	产品版本
HUAWEI NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X系列	V800R023C00SPC500
iMaster NCE-IP	V100R023C00SPC100

读者对象

本文档主要适用于以下工程师：

- 网络规划工程师
- 调测工程师

- 数据配置工程师
- 系统维护工程师

安全声明

- 受限公开声明

  产品资料中主要介绍了您在使用华为设备时，在网络部署及维护时，需要使用的命令。对用于生产、装备、返厂检测维修的接口、命令，不在资料中说明。

  对于部分仅用于工程实施、定位故障的高级命令以及升级兼容命令，如使用不当，将可能导致设备异常或者业务中断，建议较高权限的工程师使用。如您需要，请向华为公司申请。

- 加密算法声明

  使用加密算法时，DES/3DES/RSA（3072位以下)/MD5（数字签名场景和口令加密）/SHA1（数字签名场景）加密算法安全性低，存在安全风险，在协议支持的加密算法选择范围内，建议使用更安全的加密算法，例如AES/RSA（3072位及以上）/SHA2/HMAC-SHA2。

  出于安全性考虑，不建议使用不安全协议Telnet、FTP、TFTP；不建议使用特性BGP、LDP、PECP、MSDP、DCN、TCP-AO、MSTP、VRRP、E-trunk、AAA、IPSEC、BFD、QX、端口扩展、SSH、SNMP、IS-IS、RIP、SSL、NTP、OSPF、Keychain中的弱安全算法。如果确实需要使用，请执行undo crypto weak-algorithm disable命令使能弱安全算法功能。详细步骤请参见《配置指南》。

- 密码配置声明
  - 当密码加密方式为cipher时，输入以%^%#.....%^%#为起始和结束符的合法密文（本设备可以解密的密文）时，在设备上查看配置文件时显示的是和配置相同的密文，请不要采用该方式直接配置密码。
  - 为保证设备安全，请定期修改密码。
- MAC地址、公网IP地址使用的声明
  - 出于特性介绍及配置示例的需要，产品资料中会使用真实设备的MAC地址、公网的IP地址，如无特殊说明，出现的真实设备的MAC地址、公网的IP地址均为示意，不指代任何实际意义。
  - 因开源及第三方软件中自带公网地址（包括公网IP地址、公网URL地址/域名、邮箱地址），本产品没有使用这些公网地址，这遵循业界实践，也符合开源软件使用规范。
  - 出于功能特性实现的需要，设备会使用如下公网地址

    表 1-1 公网地址列表

公网地址	说明
http://www.huawei.com	华为官方网站地址
support_e@huawei.com	华为企业用户服务邮箱

- 个人数据声明
  - 您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据，因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

  - 废弃、回收或者再利用设备时，请注意根据需要备份或清除设备中的数据，避免数据泄露的安全风险。如需支持，请联系售后技术支持人员。

- 预置证书使用声明

  在生产阶段预置于华为设备的华为证书是华为设备必备的出厂身份凭证，对其使用声明如下：

  - 华为预置证书仅用于部署阶段为设备接入客户网络建立初始安全通道以及设备对接，华为不对预置证书的安全性做承诺与保证。
  - 对于将华为预置证书作为业务证书使用而导致的安全风险和安全事件，由客户自行处置并承担后果。
  - 华为预置证书有效期自2041年起开始过期，可以通过**display pki cert_list domain default**命令查看实际的有效期。
  - 预置证书过期后，使用预置证书的业务会中断。
  - 华为建议客户通过部署PKI系统对现网设备、软件签发证书并做好证书的生命周期管理（为保证安全性推荐使用短有效期的证书）。
  - 华为产品中用于产品入网初始化配置和连接时使用的华为PKI根证书支持禁用（当验证华为新网元入网时，可配置重启该证书）。建议客户完成产品入网配置并为产品配置客户CA签发的证书后，将该根证书禁用。对于客户未禁用华为PKI根证书而带来的安全风险和安全事件，由客户自行处置并承担后果。

- 产品生命周期

  华为公司对产品生命周期的规定以“产品生命周期终止政策”为准，该政策可参考华为公司官方网站的网址：**https://support.huawei.com/ecolumnsweb/zh/warranty-policy**。

- 漏洞

  华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该政策可参考华为公司官方网站的网址：**https://www.huawei.com/cn/psirt/vul-response-process**

  如企业客户须获取漏洞信息，请访问：**https://securitybulletin.huawei.com/enterprise/cn/security-advisory**

- 产品资料生命周期声明

  华为公司针对随产品版本发布的售后客户资料（产品资料），发布了“产品资料生命周期政策”，该政策的内容请参见华为公司官方网站的网址：**https://support.huawei.com/enterprise/zh/bulletins-website/ENEWS2000017760**。

- 预置数字证书声明

  华为公司对随设备出厂的预置数字证书，发布了“华为预置数字证书免责声明”，声明内容详见华为公司官方网站的网址：**https://support.huawei.com/enterprise/zh/bulletins-service/ENEWS2000015766**。

- 设备升级、打补丁的声明

  对设备进行升级或打补丁操作时，请使用软件数字签名（OpenPGP）验证工具验证软件。为避免软件被篡改或替换，防止给用户带来安全风险，建议用户进行此项操作。

- 特性声明

  - NetStream功能，出于对网络流量的统计管理，可能涉及对最终用户的通信内容分析，建议您在所适用法律法规允许的目的和范围内方可启用相应的功能。在采集、存储用户通信内容的过程中，您应采取足够的措施以确保用户的通信内容受到严格保护。

  - 镜像功能，可能基于运维目的需要对某些最终用户的通信内容进行分析，建议您在所适用法律法规允许的目的和范围内方可启用相应的功能。在采集、存储用户通信内容的过程中，您应采取足够的措施以确保用户的通信内容受到严格保护。
  - 报文头获取功能，出于检测通信传输中的故障和错误的目的，可能涉及采集或存储个人用户某些通信内容。本公司无法单方采集或存储用户通信内容。建议您只有在所适用法律法规允许的目的和范围内方可启用相应的功能。在采集、存储用户通信内容的过程中，您应采取足够的措施以确保用户的通信内容受到严格保护。
- 可靠性设计声明

  对于网络规划和站点设计，必须严格遵守可靠性设计原则，具备设备级和方案级保护。设备级保护包括双网双平面，双机、跨板双链路的规划原则，避免出现单点，单链路故障。方案级指FRR、VRRP等快速收敛保护机制。在应用方案级保护时，应避免保护方案的主备路径经过相同链路或者传输，以免方案级保护不生效。

特别声明

- 本文档中包含了NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X支持的所有产品内容，如果需要了解在本国销售的设备或单板等硬件相关信息，请查阅硬件描述章节。
- 本手册仅作为使用指导，其内容依据实验室设备信息编写。手册提供的内容具有一般性的指导意义，并不确保涵盖所有使用场景。因版本升级、设备型号不同、板卡限制不同、配置文件不同等原因，可能造成手册中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本手册不再针对前述情况造成的差异一一说明。
- 本手册中提供的最大值是设备在实验室特定场景（例如被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因可能会使设备测试出的最大值与手册中提供的数据不一致。
- 本手册中出现的接口编号仅作示例，并不代表设备上实际具有此编号的接口，实际使用中请以设备上存在的接口编号为准。
- 本手册中的硬件照片仅供参考，具体请以发货的硬件实物为准。
- 本手册中体现设备支持的相关硬件板卡，存在特定客户定制的需求，实际支持以售前销售界面为准。
- 出于特性介绍及配置示例的需要，产品资料中会使用公网IP地址，如无特殊说明，资料里出现的公网IP地址均为示意，不指代任何实际意义。
- 本手册中配置指南出现的“XX配置注意事项”，请结合产品的实际特性支持情况来使用。
- 本手册中的日志参考和告警参考，记录的是对应产品上注册的日志和告警信息。实际应用中可触发的日志和告警，取决于当前产品所支持的业务功能。
- 本文档中描述的所有设备尺寸数据均为设计尺寸，不包含尺寸公差。在部件制造过程中，由于加工或测量等因素的影响，实际尺寸存在一定的偏差。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

修订记录

修改记录累积了每次文档变更的说明。最新版本的文档包含以前所有文档版本的更新内容。

产品版本	文档版本	发布日期
V800R023C00SPC500	01	2023-09-30

1.1.2 概述

1.1.2.1 信息安全概述

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

总体来讲，信息安全包括三个方面：机密性、完整性和可用性。

就路由器来说，信息安全包括：

- 路由器存储、处理和传输的信息，不会被泄漏到非授权的实体。
- 处理和传输的过程中，信息不会被篡改。
- 业务持续可用，满足电信级服务质量要求。

机密性

机密性是指网络信息不被泄露给非授权的用户、实体或过程。即信息只为授权用户使用。机密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

路由器机密性主要体现在：

- 各种配置数据不会被越权访问。
- 处理的数据不会被恶意用户截获导致公民通信隐私泄露。
- 系统仅限于授权用户可以登录操作。

完整性

完整性(Integration)是指信息未经授权不能进行改变的特性。即网络信息在路由器存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等行为破坏和丢失的特性。

可用性

可用性(Availability)是指在要求的外部资源得到保证的前提下，产品在规定的条件下和规定的时刻或时间区间内处于可执行规定功能状态的能力。它是产品可靠性、维修性和维修保障性的综合反映。

路由器的可用性在信息安全领域，尤其是网络安全领域，专指业务系统不会因为外部的攻击流量引发 系统过载、崩溃、异常，导致业务不可用。

1.1.2.2 网络安全的基本原则

在进行路由器安全加固的过程中，需要遵循以下的网络安全基本原则，以保证配置设计方案能够最大限度的满足安全的要求。

系统工程原则

电信网络是一个规模巨大的信息系统，保障电信网络的安全必然是一个系统工程。任何单点设备、节点、技术、配置，都不足以保证整个网络的安全。

网络安全是一个由很多物理设备、安全技术、安全领域最佳实践等通过合理的安全加固配置方案，有机组成的一个整体。

安全加固必须充分评估每一个系统的单元可能面临的安全威胁，综合运用各种安全防御措施，达成系统整体的安全能力最优。

业务优先原则

在安全与业务存在冲突时，首先必须保证业务的畅通运行。在进行安全加固配置过程中，安全人员必须与业务部门进行深入的沟通交流，确保理解业务的目标，安全加固的目标必须服从于业务的目标。

安全源于设计

任何安全的网络都是设计出来的，不是配置出来的。在进行安全加固之前，首先需要进行安全加固方案的设计，然后才是对设计方案的配置落地。

好的安全系统，行为是可预料的

在进行安全加固设计阶段，必须对系统面临的各种可能的威胁，系统自身的脆弱点，系统自身具备的各种安全防御能力，以及综合形成的安全风险，有一个非常清晰的了解。

在安全加固设计阶段，系统在面临各种安全攻击时，产生的响应和可能的状态均是可以预料的。

避免通过信息隐藏等方法保证安全

路由器系统庞大复杂，错误的思想认为，通过隐藏内部实现细节、隐匿数据存储位置等措施，让“攻击者”无法找到系统的脆弱点，来达到保证系统安全的目的。

网络安全实践证明，开放透明系统的内部细节，并不会比隐藏内部细节更不安全。经验表明，开放的体系更容易提前发现问题，从而针对性的采取应对措施。

木桶原则

路由器安全防御水平，取决于安全防护能力最薄弱的单元。

安全加固必须综合考虑路由器机密性、完整性、可用性，才能真正保证系统的安全，单一的安全防御措施无法保证系统高水平的安全能力。

1.1.3 网络安全威胁分析

拒绝服务

路由器转发处理能力强，但是控制面和管理面处理能力有限。攻击者通过向路由器发起海量的消息请求，导致路由器CPU无法实时处理消息，引发正常的业务交互流程、内部处理流程阻塞，达到拒绝服务的目的。

拒绝服务是路由器面临的最大的威胁，在安全加固配置时，要求重点考虑拒绝服务类攻击的防御。

信息泄漏

路由器面临的信息泄漏威胁，最重要的风险就是非授权的访问，可以分成如下几种情况：

- 利用系统配置疏忽：路由器为了某些特定场合的便利性，提供了免认证登录的模式，在现网部署时由于疏忽没有关闭此模式，导致恶意用户非授权访问。
- 利用管理流程疏忽：路由器为了开局方便，通常使用一套配置文件作为模板开局，由于管理员疏忽，没有修改管理员账号密码，引发非授权访问。
- 利用IP网络开放性的缺陷：恶意用户通过在网络上部署嗅探器、侦听设备，把传输的IP报文截获并进行解析，达到信息泄漏目的。
- 存储介质泄密：路由器单板、存储介质，从一个地方转移到另一个地方时，由于缺乏存储介质加密机制，造成泄密。

破坏信息完整性

IP网络的开放性，导致报文在传输过程中，可能会被中间转发节点进行恶意篡改，导致信息传输失真或者被中间人有意识的修改消息内容，达到攻击的目的。

设备上运行的软件和补丁，可能会在上传到设备之前被恶意篡改，设备如果运行被篡改后的软件，导致设备被控制，达到攻击的目的。

非授权访问

通过非授权访问，获得路由器控制权限，或者获取更高权限的信息。

- 利用网络配置漏洞：由于没有合理的配置防火墙访问控制策略，导致恶意用户从公网进行暴力破解等方式，强行进入系统。
- 非法利用系统提供的调试手段：路由器为了进行故障定位，提供了一些获取路由器内部信息处理流程中的信息查看方法。恶意用户通过利用这些诊断调试接口，越权获取信息。
- 由于路由器本身的命令行控制机制是基于用户角色而非账号的管理控制，导致某些用户操作远超其个人身份所需的命令行，读取通信数据，或者窃取系统配置信息。

身份欺骗

由于IP网络开放性，对MAC和IP地址缺乏有力的认证鉴权机制，极易产生基于ARP/IP的地址欺骗攻击，导致路由器需要不断刷新转发流程必须的地址表项，处理来自欺骗地址的请求，由于地址表项错误导致转发中断，由于表项学习能力不足引发拒绝服务。

重放攻击

IP网络的开放性导致通信终端在L3及以下层面无法对端进行认证。黑客利用这一特性，通过重复发送特定报文，引发拒绝服务攻击。

计算机病毒

路由器在网络系统中除了作为转发节点同时也是一个可以被管理的网络单元。当同一个网络区域的计算机感染病毒，发送大量垃圾流量，耗尽网络带宽。此时，路由器作为一个网元节点，将无法获得网络资源，导致业务不可用。

人员不慎

在网络建设阶段为了便利业务开通部署而设置的策略，在业务开通之后并没有及时清除，导致遗留的配置成为后门，被攻击者利用。

在网络整改过程中，由于操作人员的不慎或者技能不足，导致配置出错，引发事故。例如：网线插错导致环路，协议配错引发业务中断，访问控制策略配置错误引发异常阻断或者开启了不该开启的访问通道等等。

管理员不慎将账户口令共享给他人。

物理入侵

路由器无法防止机房管理员物理接入设备，直接物理连接容易获取高优先级权限。恶意攻击者通过避开门禁、监控等防护措施，接入路由器。

1.1.4 路由器安全脆弱性分析

控制平面与管理平面处理能力局限

随着技术的发展，以及网络带宽需求的迅速增长，路由器转发处理能力得到了极大的提升。近10年来，网络带宽经历了10M到100G的万倍跨越，转发平面的处理能力急剧提升。

路由器控制和管理平面运行在CPU上，软件处理能力的增长有限。超宽带时代终端与网元之间的通道得到极大增强，极易出现基于流量泛洪等方式的拒绝服务攻击。

存在安全性不足的访问通道

路由器由于业界标准、管理便利性、历史继承性等原因，存在大量安全性不足的访问通道，例如：SNMP v1/v2，Telnet等，这些协议早期对安全性考虑不足，而新的协议（SNMP v3，SSH）并没有强制性替换老的协议。因此，如果用户不恰当的使用了这些安全不足的访问通道，容易造成信息泄密，被恶意用户利用时，容易产生非授权的访问行为。

同时，由于这些安全性不足的协议，没有进行任何完整性校验，容易引起中间人攻击，恶意攻击者可以通过篡改协议消息，达成攻击的目的。

IP 网络开放性带来的安全隐患

IP网络的开放性带来网络架构便利性的同时，也带来了巨大的安全隐患。

首先，IP网络对接入终端无认证授权机制，导致任何终端均可以随意接入网络。恶意攻击者可以轻易的进入IP网络，只要探测到路由器的IP地址，即可发起攻击行为。而且容易采用地址欺骗的方法，模拟海量源IP地址路由器进行攻击。

其次，IP网络在TCP/IP的第四层及以下，没有安全防御能力，所有消息的完整性、认证鉴权、协议一致性，都由应用层自行保障。因此，当攻击发生在第四层及以下时，路由器往往成为攻击的对象。

再次，以太网架构本身的身份认证能力缺乏，容易引发基于MAC地址欺骗的攻击。

最后，IP协议栈本身的安全能力薄弱，协议设计时没有完整的安全策略架构，导致基于协议本身的攻击也频繁发生。

以上这些安全隐患，容易引发诸如地址欺骗、重放攻击、畸形报文、网络病毒、消息篡改、流量泛洪等一系列的安全攻击，引发各种各样的安全问题。

电信网络复杂性带来的管理挑战

由于电信网络规模庞大，系统构造复杂，导致网络节点数量众多、访问通道灵活复杂、通信协议层出不穷。

电信网络的管理也变得极其复杂，安全性和业务能力，安全性和业务灵活性，安全性和管理维护便利性，矛盾无处不在。不同技术能力、管理水平的运营商和管理人员，对这些矛盾的处理能力也参差不齐。

因此，电信网络的安全策略难以保持高水平的一致性，往往会暴露出部分安全隐患，引发诸如感染病毒、非授权访问、以某个网元为跳板进行渗透攻击等问题。

路由器本身的复杂性带来的挑战

路由器配置模型复杂，管理员往往追求业务可用性，而忽略了安全防御能力，导致必要的安全措施没有得到妥善的配置，路由器本身的安全能力无法发挥。

路由器安全配置模型复杂，需要极高的技能才能完全掌握，对资深技术人员的依赖较大，容易造成在用户技能不足的情况下，以牺牲安全来达到业务可用。

1.1.5 路由器安全风险评估

综合网络安全隐患、路由器的脆弱性，可以评估出路由器面临的安全风险，并给出安全风险抑制建议，如下表所示：

表 1-2 路由器安全风险和风险抑制措施

安全隐患	路由器脆弱点	风险评估	风险抑制措施
拒绝服务	1. 控制和管理平面处理能力有限 2. IP网络开放性导致源地址无法认证，导致流量泛洪和地址欺骗	控制管理平面能力有限，流量泛洪触发条件简单，导致攻击极易发生，且对路由器造成的损害巨大 风险评价：高	1. 加强网络访问控制策略 2. 在转发平面限制上送控制管理平面的流量
信息泄漏	1. 存在安全性不足的访问通道 2. IP网络开放性导致访问控制能力不足	安全性不足的访问通道极易被攻击者利用成为攻击武器，路由器账号权限控制措施不足，IP网络开放性，都容易产生攻击 风险评价：高	1. 关闭安全性不足的访问通道 2. 加强账号权限管理 3. 合理规划访问控制策略

安全隐患	路由器脆弱点	风险评估	风险抑制措施
破坏信息完整性	IP报文传输过程中，缺乏完整性检查的必要措施。	大量的通信协议没有完整性检查机制，而IP网络开放性也无法避免信息篡改 风险评价：中	1. 对消息进行完整性检查 2. 使用安全的通道传输重要信息
非授权访问	1. 路由器本身系统的复杂性，导致命令行、MIB等无法基于单个用户授权 2. 诊断调试系统需要查看系统内部信息，也会带来安全隐患 3. IP网络开放性带来访问路径的不可控，可能遭受来自不可信网络的非授权访问	某个用户获得某个等级的权限后，由于没有更细粒度的信息隔离措施，导致可能访问到超出角色需求的信息 IP网络开放可能会受到来自不可信网络的非授权访问 风险评价：中	1. 采用TACACS命令行授权机制，避免命令行滥用 2. 选择SNMP v3并配置MIB VIEW，限制MIB访问范围 3. 加强网络访问控制策略
身份欺骗	IP网络开放性，导致路由器对源地址认证能力不足	易受到地址欺骗攻击，引发转发中断或者系统过载 风险评估：中	使能URPF、DHCP Snooping等特性，避免成为攻击目标
重放攻击	TCP/IP协议中，L3层及L3层以下无法处理序列号，导致重放攻击易实施，路由器会话请求处理能力不足，引发系统过载	对会话请求处理能力不足，引发系统过载 风险评估：高	利用硬件NP响应请求消息，利用动态白名单解决新建会话抑制与已建会话流量保持
计算机病毒	路由器对网络病毒引发的流量泛洪处理能力不足，引发系统过载	计算机等感染网络病毒，发出流量泛洪，耗尽带宽资源，冲击系统CPU过载 风险评估：高	1. 加强运营商IT管理 2. 配置速率限制，避免冲击过载
人员不慎	1. 路由器系统极其复杂，易配置出错 2. 路由器对网络拓扑震荡和环路引发的流量泛洪处理能力不足	错误的配置会导致业务受损 拓扑震荡和环路可能导致路由器处理过载 风险评估：中	加强人员培训，提升技能，提升运营商IT管理水平，避免人为出错 配置环路检测抑制等机制，智能防御人为差错

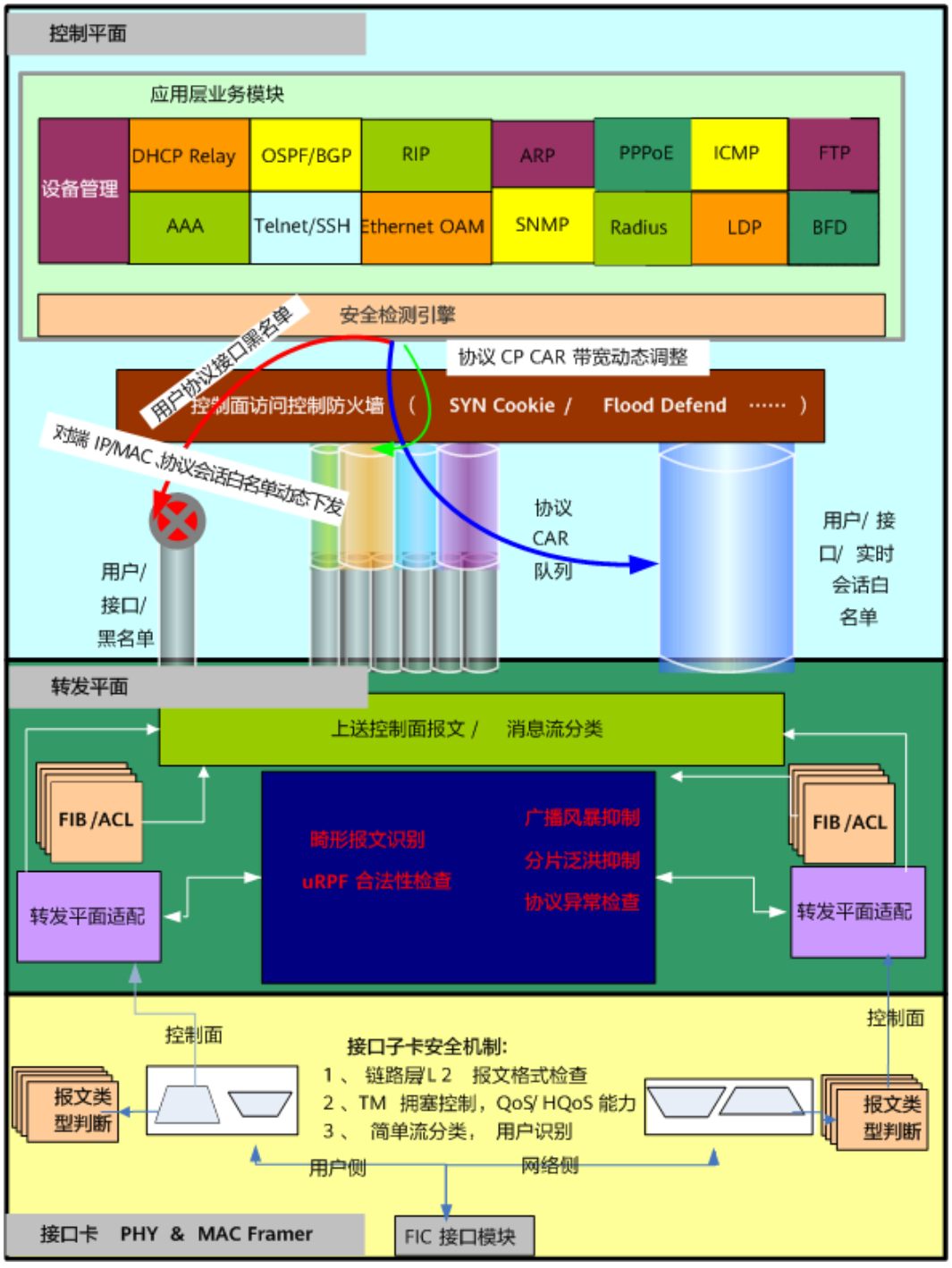
安全隐患	路由器脆弱点	风险评估	风险抑制措施
物理入侵	路由器对面板接口等方式物理接入的用户，权限等级天然较高，一旦被攻击者利用，容易引发误操作或者恶意配置	对于面板接口等物理接入方式登录的用户，如果进行恶意配置，引发严重问题。但是电信网络通常对物理访问控制严格。 风险评估：低	加强物理与环境安全控制，避免由于物理接入、环境事故等，引发安全事故

1.1.6 路由器安全体系架构

1.1.6.1 概述

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X的安全防御体系结构如下图所示：

图 1-1 NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 安全防御体系结构



在路由器中，安全防御体系主要包括如下几种类型：

转发引擎安全防御机制

路由器转发引擎，由于处理性能高，如果能够在转发面实现安全检测，把非法的报文识别出来并合理的处理，对网络安全来说是最好的方案。

但是转发引擎一般都是硬件实现，灵活性不如纯软件。因此，转发引擎只能检测具有固定特征、无需复杂的计算和处理的非法报文，安全处理机制要求较为简单且流程相对固定。

例如：

畸形报文检测，把明显违反协议规则的报文检测出来并丢弃；

广播风暴抑制，检测到广播风暴之后，直接在转发面把风暴来源利用动态ACL等方法，丢弃或者限速广播报文；

URPF直接在这方面查找端口和源地址匹配信息，不匹配直接丢弃；

分片报文泛洪时，由转发面直接进行分片报文限速；

对简单的ARP、ICMP、PPP Keep Alive等报文，直接由转发面应答客户端的请求，避免上送控制面。

采用转发引擎来实施安全策略，由于性能高，因此对流量泛洪攻击类的安全事件，能够非常好的应对，避免转发面把报文发给CPU处理，由于CPU的处理能力局限导致CPU过载，影响路由器可靠性。

转发面与控制面上送管道安全防御机制

转发面相对于控制面来说，其处理能力可以认为是无限的。因此，转发面能够轻易的上送海量的报文，把控制面直接冲击过载。

为了防止转发面上送过多的报文给控制面，需要对上送管道进行限速；同时为了不影响正常的业务运行，也需要对高优先级的和通过安全检测的正常业务放行。综合了安全性和可用性，路由器使用了如下几种机制，来综合保障在路由器可靠运行的前提下，尽可能提供高性能的业务处理能力：

- 协议CPCAR：针对每一种协议（或者协议的某种典型的消息，如ARP Request和ARP Reply分开设置CPCAR），设置一个上送控制面的带宽限制；
- 动态/静态黑名单：当动态检测到存在攻击事件，或者静态配置拒绝访问的策略，黑名单策略拒绝所有报文上送，防止被非法攻击；
- 动态/静态白名单：当控制面的通信会话已经通过安全检查证明是可靠的，或者静态配置某些访问对象是可信的，通过白名单保证它们的报文不受限速控制；
- Session-CAR：针对协议的每个会话邻居，设置一个上送控制面的带宽限制，隔离不同会话邻居间的相互影响；
- 微隔离CAR：针对从不同端口建立的协议会话，设置一个上送控制面的带宽限制，隔离不同端口协议会话间的相互影响；

综合以上措施，能够保证转发面上送控制面的报文不会把CPU冲击过载，同时也保证CPU尽最大能力为业务服务不会造成资源浪费。

应用层业务内嵌的安全检测与防御机制

转发面由于无法感知每一种协议内部的机制，因此复杂的、深层次的安全攻击无法被转发面检测并控制。

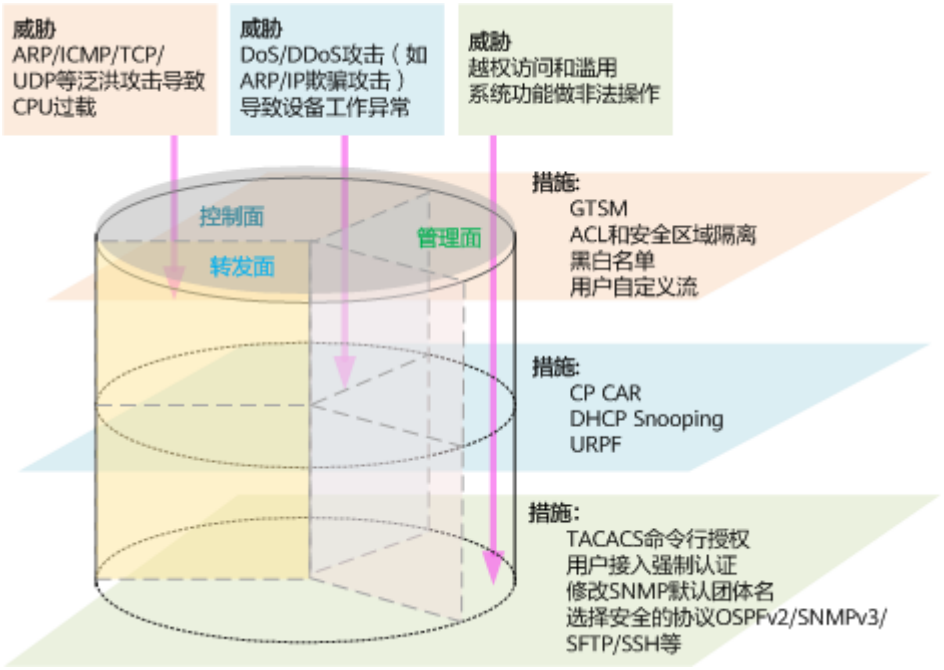
转发面与控制面间的管道控制机制只能保证CPU不会被攻击过载，并不感知上送的报文是否存在安全隐患。

因此，需要在应用层模块内部，内嵌的安全检测引擎：每一个协议栈模块，都需要能够动态检查报文和会话的合法性，需要把非法的报文或者会话及时丢弃，以防造成协议栈的安全危害。

1.1.6.2 遵循 X.805 的三面安全隔离与防御机制

如下图所示，NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X遵循X.805的三面安全隔离机制，其体系架构如下：

图 1-2 NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 三面安全体系结构



通过将控制平面、管理平面和转发平面进行隔离，路由器能够保证任何一个平面在遭受攻击时，不会影响其他平面的正常运行。

1.1.6.3 路由器控制面安全防御能力

在NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X控制平面，为了保障控制协议和业务的正常运行，提供了如下的安全防御能力：

- 应用层联动
- 畸形报文防攻击
- 路由协议认证核验
- GTSM(Generalized TTL Security Mechanism)
- 攻击溯源与告警
- 黑名单和白名单
- 安全管理中心
- Session-CAR
- 微隔离CAR

应用层联动

应用层联动指的是将控制层面的协议开关状态和底层转发引擎的协议上送关联起来。通过在上层和底层建立联系，在协议开关状态上保持一致，对于设备没有开启业务的

协议，底层硬件默认是以小带宽上送其协议报文，也可以配置为完全不上送，这样就将攻击者的攻击范围尽可能缩小，增加了攻击的成本，减少了设备的安全风险。

畸形报文防攻击

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X当前能够对如下的畸形报文进行攻击检测，并在检测到攻击后，丢弃攻击报文：

- Null IP payload flooding attack
- IGMP null payload attack
- TCP illegal flags attack
- Duplicated fragment attack
- Fragment flooding
- Tear Drop
- Syndrop
- Nesta
- Fawx
- Bonk
- NewTear
- Rose
- Jolt
- Big offset
- Fraggle

路由协议认证校验

一些路由协议支持安全认证，在设备间报文交互时，采用HASH算法计算报文摘要，接收时重新计算摘要进行比较，能够及时识别出被篡改的报文。

路由协议安全认证算法根据协议自身的机制，更新使用业界最安全的SHA2算法（协议明确不支持的除外），保证了协议报文不会被篡改，增强了路由协议的安全性。

协议认证的密钥在设备的存储采用了业界最安全的AES256算法。大大提升了被破解的难度，更不容易泄露。

白名单与黑名单

白名单指合法用户或者是高优先级用户的集合。通过设定白名单信息可主动保护现有业务、高优先级用户业务。可将确定为正常使用设备的合法用户或者是高优先级用户业务设置到白名单中，匹配白名单特征的报文会被采用高速率高优先级上送。

黑名单指非法用户的集合。通过设定ACL，可将确定为攻击的非法用户设置到黑名单中，匹配黑名单特征的报文会被丢弃或者低优先级上送。

GTSM

GTSM(Generalized TTL Security Mechanism)是通用跳数检测机制的缩写，即通过检测上送报文的TTL值合法与否，来保护CPU免受CPU-utilization（CPU overload）类型的攻击。

根据路由器组网的特点，发给路由器控制面的报文，历经的网络节点条数是有限的，用户可以根据组网情况，限制发给控制面的报文历经的节点条数，避免网络上恶意的用户从远端发起攻击。

攻击溯源与告警

当路由器受到攻击，可以利用攻击溯源功能记录攻击报文，通过对攻击报文的分析，进行攻击定位和攻击防范。

攻击溯源对攻击报文的信息进行分析，对攻击位置、等级、原因等进行提取，并输出记录和告警。

安全管理中心

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 路由器为了保证自身系统的可靠性，同时为了保证运行在系统中的业务系统不受安全攻击（有意和无意的）事件的影响，设计了诸如CAR速率限制、攻击检测、攻击隔离等技术手段。所有这些技术特性要求一个全局的管理中心，能够汇总分析所有安全攻击的信息，智能分析出攻击的源头、攻击的原因、攻击的影响严重程度，并根据内嵌的安全专家分析知识库，给出合理的攻击抑制解决方案。

安全管理中心站在NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 路由器系统全局，能够统一汇总分析各个安全检测单元的上报信息，汇总分析后，以简洁的形式，呈现出攻击源、根因分析、解决建议。

Session-CAR

协议多会话的场景下，为每一个会话设置一个上送控制面的带宽限制，当单个会话受到攻击时，不影响其它会话的建连和报文上送。

微隔离 CAR

协议通过不同端口建立会话时，为每一个端口设置一个上送控制面的带宽限制，当单个端口受到攻击时，不影响其它端口协议的建连和报文上送。

1.1.6.4 路由器转发面安全防御能力

在NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X转发平面，为了保障路由器的CPU系统能够正常运行，提供了如下的安全防御能力：

- ACL访问控制列表
- URPF(Unicast Reverse Path Forwarding)
- DHCP Snooping
- CPU报文速率限制(CPCAR)
- 用户自定义流(基于ACL)

ACL 访问控制列表

访问控制列表是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL通过规则对数据包进行分类，这些规则应用到路由设备上，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

例如可以用访问列表描述：拒绝任何用户终端使用Telnet登录本机。允许每个用户终端经由SMTP向本机发送电子邮件。

每个ACL中可以定义多个规则，根据规则的功能分为接口ACL规则、基本ACL规则和高级ACL规则和MPLS ACL规则。ACL规则是一个匹配选项的集合，由用户根据不同业务进行选择配置。

ACL（Access Control List）的类型划分方式有两种，如下表所示：

表 1-3 ACL 类型划分方式

ACL类型划分依据	ACL类型
按照对IPv4和IPv6的支持情况	● ACL4 ● ACL6
按照ACL规则的功能	● 接口ACL：限制数据包“允许”或“拒绝”通过接口。数字范围是1000～1999，即支持1000个接口ACL。 ● 基本ACL：限制数据包的源地址。数字范围是2000～2999，即支持1000个基本ACL。 ● 高级ACL：限制数据包的源地址、目的地址、协议号（TCP、UDP）、源端口和目的端口号的五元组。 包括数字型高级ACL和命名型ACL： – 数字型高级ACL的编号范围是3000～3999，即支持1000个数字型高级ACL。 – 命名型ACL的编号范围是42768～75535，即支持32768个命名型ACL。 ● MPLS ACL:限制MPLS报文的Exp值、label值、TTL值。编号范围是10000～10999，即支持1000个MPLS ACL。

根据ACL功能划分的四种类型ACL，分别支持的过滤选项如下表：

表 1-4 不同类型 ACL 所支持的过滤选项

ACL规则类型	支持的过滤选项
接口ACL	接口名：指定数据包是从该接口进入的。或者用“any”代表所有的接口。 生效时间段：指定规则生效的时间范围。如果不配置，表示规则配置后马上生效。

ACL规则类型	支持的过滤选项
基本ACL	源IP地址：指定ACL规则的源地址信息。如果不配置，表示任何源地址的报文都匹配。 生效时间段：指定规则生效的时间范围。如果不配置，表示规则配置后马上生效。

ACL规则类型	支持的过滤选项
高级ACL	协议类型：用名字或数字表示的协议类型。如果用整数形式，取值范围是1～255；如果用字符串形式，可以选取：gre、icmp、igmp、ip、ipinip、ospf、tcp、udp。对不同的协议类型，有不同的参数组合，TCP和UDP有源端口和目的端口可选项，其它协议类型没有。 源IP地址：指定ACL规则的源地址信息。如果不配置，表示报文的任何源地址都匹配。 目的IP地址：指定ACL规则的目的地址信息。如果不配置，表示报文的任何目的地址都匹配。 源端口和目的端口：指定UDP或者TCP报文的目的端口信息，仅仅在规则指定的协议号是TCP或者UDP时有效。如果不指定，表示TCP/UDP报文的任何目的端口信息都匹配。 DSCP：指定区分服务代码点（Differentiated Services Code Point，IP头ToS字段的高6位）的取值，取值范围是0～63。 分片报文类型：指定该规则是否仅对非首片分片报文有效。当包含此参数时表示该规则仅对非首片分片报文有效。 优先级：数据包可以依据优先级字段（IP包ToS字段的高3位）进行过滤。用关键字或数字表示，数字的取值范围是0～7的整数。 TCP flag：指定TCP-FLAG的值，取值范围是0～63。 ToS：数据包可以依据服务类型字段进行过滤。 ICMP：ICMP包可以依据ICMP的消息名称、消息类型或消息码进行过滤，仅仅在报文协议是ICMP的情况下有效。如果不配置，表示任何ICMP类型的报文都匹配。 生效时间段：指定规则生效的时间范围。如果不配置，表示规则配置后马上生效。

ACL规则类型	支持的过滤选项
MPLS ACL	MPLS报文的Exp值。如果不配置，表示Exp为任何值的MPLS报文都匹配。 MPLS报文的label值。如果不配置，表示label为任何值的MPLS报文都匹配。 MPLS报文的TTL值。如果不配置，表示TTL为任何值的MPLS报文都匹配。

URPF

URPF(Unicast Reverse Path Forwarding)是单播反向路径检查的缩写，分为严格模式和松散模式，其原理是数据报文从网络接口进入到NP，对于三层IP报文，查找路由表FIB，如果是本机路由则转发CP处理，在转发之前需要做URPF检查，检查数据报文的源IP地址是否合法，检查的原理是根据数据包的源IP地址查路由表。

支持配置检查模式为严格模式和松散模式，以及允许匹配缺省路由的方式。

- 对于严格模式：如果报文能匹配明细路由，并且入接口跟匹配路由的出接口一致，则允许报文转发，否则丢弃报文。
- 对于松散模式：如果报文匹配上明细路由，则允许报文转发，否则丢弃报文。默认情况下，会认为缺省路由不存在，不会去匹配缺省路由，只有进行了配置后，才会去匹配缺省路由。

对允许匹配缺省路由的模式，必须和严格模式一起配置，报文匹配明细路由或者缺省路由，并且报文入接口跟匹配路由的出接口一致才转发，否则丢弃。松散模式和严格模式互斥，只能配置一种模式。

基于访问控制的安全防御

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X提供了较为完善的ACL访问控制能力，基于ACL，能够实现CPCAR流量速率限制，用户自定义流。

- CPCAR用来设置上送CPU的报文的分类限速上送规则，针对每类报文可设置均值速率、承诺突发尺寸、优先级信息等。通过对不同的报文设置不同的CAR规则，可以降低报文的相互影响，达到保护CPU的目的。CAR还可以设置上送CPU报文的整体速率，当整体上送速率超过阈值后，报文将被丢弃，避免CPU过载。
- 用户自定义流指用户自定义防攻击ACL规则。主要应用于当后续网络中出现不明攻击时，用户可灵活指明攻击流数据特征，将符合此特征的数据流进行上送限制。

  为了避免NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X遭受非法用户控制设备，或者进行管理报文的泛洪攻击，可以部署管理控制平面功能。这样只有用户指定的接口可以接收管理报文，其他接口接收的管理报文将直接丢弃，从而有效地减少资源浪费。用户还可以配置对应接口可以接收的管理类报文，其他的协议报文直接丢弃，避免无关协议报文的攻击。

1.1.6.5 路由器管理面安全防御能力

在NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X管理平面，为了保障路由器操作系统和管理应用能够正常运行，提供了如下安全防御能力：

- 安全启动
- 系统权限管理控制
- 账户权限管理控制
- 日志记录系统
- 安全管理通道，SNMPv3、SSH、SFTP等
- 高级加密算法
- 分级信息隔离
- TACACS授权管理
- AAA鉴权授权
- HWTACACS授权管理

管理平面通过基于角色的用户权限控制，能够保证不同等级的用户具有不同的权限。

基于AAA的鉴权授权能够满足在不同的应用场景下，对系统权限的控制。

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X有完备的日志记录系统，保证对系统的任何配置操作、系统运行过程中的各种异常状态，都能够记录且不会侵犯用户隐私，便于事后审计。

1.1.7 路由器安全加固策略

在进行路由器安全加固配置之前，你需要了解如下的信息，以免对本手册列出的安全加固策略建议进行机械的照搬，从而影响你的业务。

安全是一个持续改进的过程，从来没有一蹴而就的安全，也没有一劳永逸的安全。任何企图依靠某个策略就可以保证高枕无忧，或者任何企图依靠一次安全加固配置就万事大吉的想法，都是不合理的。

在进行安全加固之前，需要执行如下步骤：

- 深入了解业务需求：安全永远是为业务服务的，需要深入了解业务系统对安全防护的要求，才能合理的制定安全策略
- 全面的风险评估：需要综合分析业务系统面临的安全威胁，权衡业务系统的脆弱点，权衡业务系统的价值与安全加固的代价，全面实施安全风险评估，把不可接受的安全风险进行防护，把能够接受的风险作为残留风险接纳，并在业务系统生命周期中定期审视这些残留风险，评估其是否需要进行升级处理
- 安全加固方案设计：在全面的风险评估基础上，设计切实满足业务需求，并满足安全的代价和收益后，设计合理的方案。安全是设计出来的，不是配置出来的，希望每一个进行安全加固的工程师，深刻理解这一原则
- 安全策略实施：将安全加固策略实施之前，请务必评估因为安全策略对业务带来的影响，避免由于不合理的安全策略造成业务损伤

在完成安全加固之后，需要不断的监控和维护业务系统，以确保安全策略已经切实发挥作用并达到安全加固方案预期的效果，及时发现问题，并调整安全策略。

安全加固是一个持续的改进过程。

按照网络安全需求，可以将路由器的安全加固策略分为Level-1、Level-2两个级别。

- Level-1：代表的是从安全本身角度评估设备最基础的安全加固策略。
- Level-2：代表的是加强的安全加固策略，用户可以根据自己的业务有选择的进行配置。

1.1.7.1 Level-1 的安全加固策略（必配）

1.1.7.1.1 管理平面

设备定制及缺省帐号与密码清单

须知

系统交付使用后，请立即修改各缺省账户的密码，以降低安全风险。

密码长期使用会增加被盗窃和破解的风险，而且使用的时间越长，被盗窃和破解的风险越高。定期修改密码可以有效防范这种情况的发生，因此强烈建议您定期修改密码。

您可以通过下方路径获取文档中的各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

运营商客户：**定制及缺省帐号与密码**

企业网客户：**定制及缺省帐号与密码**

接入认证安全描述

?.1. CONSOLE

安全策略介绍

串口（即CONSOLE口）属于物理接口，在设备部署、组网上通过物理隔离，可防止恶意用户通过串口登录设备。

串口登录支持密码认证和AAA认证，用户必须通过认证才能登录设备。认证没有默认配置，必须正确配置后才能使用。密码采用不可逆方式加密。

当设备第一次启用时，设备没有任何配置，需要通过串口进行第一次配置：

1. 插入串口，在终端上输入“回车Enter”键，提示用户配置密码，并确认。配置成功后，用户进入命令行界面。
2. 用户设置的密码已经作为配置保存，用户需要记录该密码。串口用户界面的认证方式为密码认证，用户权限为管理级权限。

说明

用户必须记录此时配置的密码，以便后续管理登录串口时使用。如果用户忘记该密码，且没有正确配置Telnet、SSH等登录，那么用户将无法登录设备。

攻击方法介绍

在没有串口服务器的情况下，攻击者尝试突破物理隔离。接触到串口后，设备将暴露给攻击者，设备将无法保障安全。即使该攻击者没有破解用户名和密码，也能够对设备造成损害。

在使用串口服务器的情况下，可能有潜在的攻击者通过网络连接尝试破解用户名和密码，获取系统管理权限。

配置维护方法

首次登录设备，设置AAA验证

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**aaa**，进入AAA视图。
3. 执行命令**local-user** *user-name* **password** [**cipher** *password* | **irreversible-cipher** *irreversible-cipher-password*]，并交互输入密码，配置本地用户名和密码。
4. 执行命令**local-user** *user-name* **service-type terminal**，配置用户的接入类型为终端用户。
5. 执行命令**quit**，退出AAA视图。
6. 执行命令**user-interface console** *interface-number*，进入Console用户界面视图。
7. 执行命令**authentication-mode aaa**，设置用户验证方式为AAA验证。
8. 执行命令**local-user** *user-name* **user-group manage-ug**，将该用户权限设置为管理级权限。

配置维护建议

为保证串口安全，建议正确配置串口的认证方式：

- 串口认证支持密码认证和AAA认证，建议用户使用AAA认证，通过用户名和密码验证用户。
- 在串口没有认证配置的情况下，设备允许用户登录并配置密码，建议用户此时，将串口用户界面（user-interface console 0）的认证方式修改为AAA认证，并在AAA视图下配置正确的用户名和密码。

说明

由于设备密码采用密文保存，所以需要用户记录自己配置的密码，用户忘记将无法恢复。

检查加固结果

执行命令**display current-configuration configuration** aaa，查看AAA的配置情况。

?.2. AAA 用户管理

AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称。它提供对用户进行认证、授权和计费三种功能。具体如下：

认证（Authentication）：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（Authorization）：授权用户可以使用哪些服务。

计费（Accounting）：记录用户使用网络资源的情况。

由于涉及到用户的认证、授权和计费，和业务强相关，配置也是非常灵活的。

安全策略介绍

- 支持远端认证、授权：将用户信息（包括本地用户的用户名、密码和各种属性）配置在认证服务器上。支持通过RADIUS（Remote Authentication Dial In User Service）协议或HWTACACS （HUAWEI Terminal Access Controller Access Control System，是在TACACS+协议1.78版本的草案基础上进行了功能增强的一种安全协议）协议进行远端认证和远端授权；
- 支持远端命令行鉴权：可配置某一指定等级用户的命令行鉴权方式为远端鉴权，用户的命令权限信息保存在远端服务器上，当用户执行命令操作时，由服务器判断用户是否有执行该命令的权限。当前远端鉴权只支持HWTACACS鉴权；
- 支持限制本地用户的连续认证失败次数：可配置用户可认证失败次数和可再次进行认证的时间间隔的参数来防止非法用户登录。配置了这个功能后，在用户指定时间长度内登录失败N次后，会暂时将用户阻塞一段时间，降低试探成功的机率，增强设备的安全性；
- 系统保存的本地用户密码和提升等级密码均采用高级加密算法进行加密保存；
- 屏蔽了管理类型用户的无认证方式(none)。

攻击方法介绍

- 非法用户可能通过用户名、密码等关键信息进行遍历尝试来获取系统用户的登录权限；
- 非法用户可能对远端服务器进行攻击，以获取保存在服务器上的用户名、密码等关键信息；
- 非法用户可能对用户—设备之间的网络进行攻击，以劫取用户输入的密码等关键信息；设备—服务器之间的网络传输，虽然用户信息已经被加密，但非法用户仍可能通过加密碰撞、明文密文字典遍历查找等方法进行加密破解。

配置维护方法

- 配置用户的认证、授权方式为远端认证、远端授权。以HWTACACS认证、授权为例：

  # 创建HWTACACS模板，配置认证、授权服务器，配置共享密钥：

  ```
  [~HUAWEI] hwtacacs-server template 1
  [*HUAWEI-hwtacacs-1] hwtacacs-server authentication 10.138.90.141
  [*HUAWEI-hwtacacs-1] hwtacacs-server authorization 10.138.90.141
  [*HUAWEI-hwtacacs-1] hwtacacs-server shared-key YsHsjx_202206
  [*HUAWEI-hwtacacs-1] commit
  ```

  # 在认证方案中配置认证方式为HWTACACS认证：

  ```
  [~HUAWEI] aaa
  [~HUAWEI-aaa] authentication-scheme 1
  [*HUAWEI-aaa-authen-1] authentication-mode hwtacacs
  [*HUAWEI-aaa-authen-1] commit
  ```

  # 在授权方案中配置授权方式为HWTACACS授权：

  ```
  [~HUAWEI-aaa] authorization-scheme 1
  [*HUAWEI-aaa-author-1] authorization-mode hwtacacs
  [*HUAWEI-aaa-author-1] commit
  ```

  # 在域中认证方案、授权方案和HWTACACS模板：

  ```
  [~HUAWEI-aaa] domain dom1
  [*HUAWEI-aaa-domain-dom1] authentication-scheme 1
  [*HUAWEI-aaa-domain-dom1] authorization-scheme 1
  [*HUAWEI-aaa-domain-dom1] hwtacacs-server 1
  [*HUAWEI-aaa-domain-dom1] commit
  ```

  # 至此，域dom1下用户登录的认证、授权方式即为远端HWTACACS认证。

说明

注：RADIUS不支持认证、授权分离，用户只需将认证方式配置为远端RADIUS认证，系统会自动完成远程RADIUS认证、授权过程。

- 支持配置用户的命令鉴权方式为远端鉴权

  # 在授权方案中配置等级为3的用户的鉴权方式为远端鉴权：

  ```
  [~HUAWEI] aaa
  [~HUAWEI-aaa] authorization-scheme 1
  [*HUAWEI-aaa-author-1] authorization-cmd 3 hwtacacs
  [*HUAWEI-aaa-author-1] commit
  ```

  说明

  当配置用户的鉴权方式为远端鉴权之后，用户每次执行命令，系统都会向远端服务器发送鉴权请求，由服务器判断用户是否有执行该命令的权限，因此设备—服务器之间的网络状态将会影响用户执行命令的响应时间。

- 支持限制本地用户的连续认证失败次数：

  # 配置指定时间长度内本地用户的连续认证失败次数上限，限制用户在1分钟之内最大连续认证失败次数为3次：

  ```
  [~HUAWEI] aaa
  [~HUAWEI-aaa] user-block failed-times 3 period 1
  [*HUAWEI-aaa] commit
  ```

  说明

  failed-times配置为0则表示不限制用户的连续认证失败次数。

  # 配置锁定用户的自动解锁时间，当用户因超过最大连续认证失败次数而被锁定之后，系统将在一段时间之后自动为该用户解锁：

  ```
  [~HUAWEI-aaa] user-block reactive 30
  [*HUAWEI-aaa] commit
  ```

  说明

  配置时间为0则表示锁定用户不会自动解锁，只能通过管理员手动为锁定用户解锁；时间单位为分钟。

  # 手动为锁定用户解锁：

  ```
  <HUAWEI> activate aaa local-user root
  ```

- 配置密码复杂度开关

  ```
  [~HUAWEI] user-security-policy enable
  [*HUAWEI-aaa] commit
  ```

配置维护建议

当系统提示密码存在风险需要修改时，请及时按照提示信息修改。

检查加固结果

- 执行**display authentication-scheme** [*authentication-scheme-name*]命令查看认证方案的配置情况。
- 执行**display accounting-scheme**命令查看计费方案的配置情况。
- 执行**display authorization-scheme** [*authorization-scheme-name*]命令查看授权方案的配置情况。
- 执行**display domain** *domain-name*命令查看域的配置信息。

- 执行**display aaa configuration**命令查看AAA的概要信息。

?.3. SSH

安全策略介绍

- 支持认证

  SSH Server支持AAA认证、Public-Key认证以及PKI证书认证，只有通过认证的用户才能登录设备，进入命令行界面。AAA认证支持远端认证和本地认证，且远端认证优先。

- 支持关闭服务

  当开启SSH Server服务器时，设备将开启Socket侦听，易被攻击者扫描。当不使用SSH Server时，可以关闭SSH Server和相应的端口号。

- 支持关闭SSHv1服务

  SSHv1服务存在被攻击的风险，且使用算法已不安全。可以通过关闭SSHv1降低被攻击的风险。

- 支持变更端口号

  SSH Server 22号端口属于知名端口号，易被扫描和攻击。可以修改SSH Server的端口为私有端口，端口号范围为<22,1025-65535>，减小被扫描攻击的概率。

- 支持ACL

  在SSH Server上，可以配置ACL过滤规则，用于控制允许通过STELNET、SFTP、SCP或者SNETCONF方式登录到设备的客户端IP。

  在用户界面视图（user-interface）可以配置各个VTY通道的ACL过滤规则，用于控制允许通过STELNET方式登录到设备的客户端IP，其他登录方式不控制。

  推荐配置在SSH Server上，不建议配置在VTY通道上。

- 支持源接口配置

  可以配置SSH Server支持的源接口，仅允许用户通过此接口的IP登录设备，限制访问范围，提高设备安全性。

- 支持IPv6源地址配置

  可以配置SSH Server支持的IPv6源地址，仅允许用户通过此IPv6地址登录设备，限制访问范围，提高设备安全性。

- 支持基于CPCAR的泛洪攻击保护配置

  在部署连接互联网公网地址的场景下，设备本身可能会遭受管理控制平面的流量泛洪攻击，对此，可以配置CPU防护策略对设备进行流量攻击防护。

攻击方法介绍

- 暴力破解密码

  攻击者在侦听到SSH端口后，尝试进行连接，设备提示认证，则其会进行暴力破解尝试通过认证，获取访问权限。

- 拒绝服务式攻击

  SSH Server支持的用户数有限，在用户登录达到上限后，其他用户将无法登录。这个可能是正常使用造成，也可能是攻击者造成。

配置维护方法

- 配置认证方式为AAA认证

  说明

  验证方式配置为AAA验证时，必须指定本地用户的接入类型。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**aaa**，进入AAA视图。
  c. 执行命令**local-user** *user-name* **password** [**cipher** *password* | **irreversible-cipher** *irreversible-cipher-password*]，配置本地用户名并交互输入密码。
  d. 执行命令**local-user** *user-name* **user-group manage-ug**，配置本地用户具有管理权力。
  e. 执行命令**local-user** *user-name* **service-type ssh**，配置本地用户的接入类型为SSH。
  f. 执行命令**quit**，退出AAA视图。
  g. 执行命令**user-interface vty** *first-ui-number* [*last-ui-number*]，进入VTY用户界面视图。
  h. 执行命令**authentication-mode aaa**，设置用户验证方式为AAA验证。
  i. 执行命令**commit**，提交配置。

- 配置关闭SSH服务（SSH服务默认开启）

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**undo stelnet server enable**，关闭Stelnet服务。
  c. 执行命令**commit**，提交配置。

- 配置变更端口号为53555

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ssh server port 53555**，调整端口号为53555。
  c. 执行命令**commit**，提交配置。

- 配置通过ACL设置呼入呼出权限限制

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**acl** { [**number**] *acl-number* | **name** *acl-name* [**advance**] [**number** *acl-number*] } [**match-order** { **auto** | **config** }]，创建一个高级ACL，并进入高级ACL视图。
  c. 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } *protocol* [**destination** { *destination-ip-address destination-wildcard* | **any** } | **fragment** | **source** { *source-ip-address source-wildcard* | **any** } | **time-range** *time-name* | **dscp** *dscp* **vpn-instance** *vpn-instance-name*]，配置ACL规则。
  d. 执行命令**quit**，退出ACL视图。
  e. 执行命令**user-interface vty** *first-ui-number* [*last-ui-number*]，进入VTY用户界面视图。
  f. 执行命令**acl** *acl-number* { **inbound** | **outbound** }，配置VTY类型用户界面的呼入呼出限制。

     当需要限制某个地址或地址段的用户登录到路由器时，使用**inbound**。

     当需要限制已经登录的用户登录到其它路由器时，使用**outbound**。

g. 执行命令**quit**，退出VTY用户界面视图。

h. 执行命令**ssh server acl** { *acl-number* | *acl-name* }，配置允许通过SSH协议登录到设备的客户端IP地址。

i. 执行命令**commit**，提交配置。

- 配置用户通过指定源接口登录服务器

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**ssh server-source -i loopback** *interface-number*，指定SSH服务器端的源接口。

说明

指定SSH服务器端的源接口前，必须已经成功创建LoopBack接口，否则会导致本配置无法成功执行。

c. 执行命令**commit**，提交配置。

- 配置用户通过指定Ipv6源地址登录服务器

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**ssh ipv6 server-source -a** *ipv6-address* [**-vpn-instance** *vpn-instance-name*]，指定SSH服务器端的IPv6源地址。

说明

如果指定SSH服务器端的VPN实例，必须已经成功创建VPN，否则会导致命令无法执行成功。

c. 执行命令**commit**，提交配置。

- 配置基于CPCAR的泛洪攻击防护

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**acl** { **name** *advance-acl-name* [**advance** | [**advance**] **number** *advance-acl-number*] | [**number**] *advance-acl-number* } [**match-order** { **config** | **auto** }]，创建高级ACL，并进入ACL视图。

说明

SSH是基于TCP的协议，用户可使用SSH协议登录设备，为保证其安全性，建议配置一个单独的ACL中进行保护。设备支持SSH协议的动态链路保护，对于已经生成的链接，协议报文走动态白名单上送。这里使用ACL对还未生成链接的SSH协议报文进行限速，管理协议建议直接对未知源的访问流量进行过滤丢弃。

c. 执行如下三条命令，配置ACL的规则，允许上送指定源接口地址范围内的SSH报文，拒绝上送其他SSH协议报文。

- 执行命令**rule** [*rule-id*] [**name** *rule-name*] **permit tcp source** *source-ip-address source-wildcard* **source-port eq 22**，配置允许上送指定源地址且源接口类型为SSH的协议报文。
- 执行命令**rule** [*rule-id*] [**name** *rule-name*] **permit tcp source** *source-ip-address source-wildcard* **destination-port eq 22**，配置允许上送指定源地址且目的接口类型为SSH的协议报文。
- 执行命令**rule** [*rule-id*] [**name** *rule-name*] **deny tcp destination-port eq 22**，配置拒绝上送其他不在白名单范围中的SSH协议报文。

d. 执行命令**quit**，退出ACL视图。

e. 执行命令**cpu-defend policy** *policy-number*，创建防攻击策略。

f. 执行命令**tcpsyn-flood enable**，使能TCP SYN泛洪攻击防范功能。
g. 执行命令**fragment-flood enable**，使能分片报文攻击防范功能。
h. 执行命令**udp-packet-defend enable**，使能UDP报文的攻击防范功能。
i. 执行命令**abnormal-packet-defend enable**，使能畸形报文的攻击防护功能。
j. 执行命令**user-defined-flow** *flow-id* **acl** { *acl-number* | **name** *acl-name* } [**prior**]，配置用户自定义流，并与ACL相关联。
k. 执行命令**car user-defined-flow** *flow-id* { **cir** *cir-value* | **cbs** *cbs-value* | **min-packet-length** *min-packet-length-value* }，配置用户自定义流中报文的CAR动作规则。
l. 执行命令**priority** { *protocol-name* | **index** *index* | **whitelist** | **whitelist-v6** | **blacklist** | **tcpsyn** | **fragment** | **user-defined-flow** *flow-id* } { **high** | **middle** | **low** | **be** | **af1** | **af2** | **af3** | **af4** | **ef** | **cs6** }，配置上送CPU报文的优先级。

说明

SSH协议是访问协议，所需的处理带宽较少，实时性要求不高，这里建议将优先级设置为中即可。

m. 执行命令**quit**，退出防攻击策略视图。
n. 执行命令**slot** *slot-id*，进入指定槽位。
o. 执行命令**cpu-defend-policy** *policy-number*，在指定接口板上应用防护攻击策略。
p. 执行命令**commit**，提交配置。

配置维护建议

- 单独规划设备管理的网络IP，防止设备被扫描和窃听。
- 修改SSH Server端口号。
- 配置ACL策略，限定SSH允许访问的IP。
- 建议对SSH用户增加Public-key的认证。

检查加固结果

- 执行命令**display current-configuration configuration** aaa，查看AAA的配置情况。
- 执行命令**display ssh server status**，查看SSH服务器的全局配置信息。
- 执行命令**display cpu-defend policy** *policy-number*, 查看防攻击策略信息。

?.4. SNMP

SNMP是用于管理网络设备的协议。网络管理员需要从设备获取数据或向设备执行设置操作，都可以通过SNMP来完成。SNMP还提供了Trap和Inform操作，当设备的重要状态发生改变时，可以向网管通报事件的发生。

安全策略介绍

对于SNMPv1、v2c、v3，SNMP有不同的安全策略。

对于SNMPv1/SNMPv2c，支持ACL和VACM（基于视图的访问控制）。通过给团体名关联acl和mib-view，将允许访问设备的网管和允许访问的节点限定在一定范围内。从而在一定程度上提供了系统安全的保护。SNMPv1/SNMPv2c不支持加密算法。

对于SNMPv3，增加了支持USM（基于用户的安全模型）的安全机制，当前支持MD5/SHA鉴权和DES/3DES/AES加密算法。通过对通信的数据进行鉴别和加密，解决消息被伪装、篡改、泄密等安全问题。

SNMP具备防攻击锁定机制，如果用户认证失败，则进行锁定操作。（默认使能）

说明

为了保证更好的安全性，建议使用SHA鉴权。建议不要使用DES或3DES算法作为SNMPv3的加密算法。

对于泛洪攻击支持基于CPCAR的安全策略，在部署连接到互联网公网地址空间的场景下，设备的管理控制平面可能遭受流量泛洪攻击，可以通过部署CPU防护策略对设备自身进行流量攻击的防护。

攻击方法介绍

- 暴力破解场景攻击

  通过不断发送SNMPv1/v2c团体名、SNMPv3用户名和密码，进而获得用户名和密码。

- 通过非法手段获取用户权限，从而执行未经授权的管理操作
  - 攻击者通过改变发送报文的源IP，获取到授权用户的权限，从而执行未经授权的管理操作。
  - 侦听管理站和SNMP代理间的通信，获取到用户名、密码，团体名等信息，获取非法授权。
  - 拦截SNMP消息，进行重排序、延迟、重发，从而影响正常操作，直到攻击者获得非法的未授权访问权限。
- 拒绝服务式攻击

  非法IP攻击会减慢设备的响应速度。例如：海量报文攻击，导致SNMP消息缓存表满，无法处理网管请求。

- 非法报文攻击
  - 非法报文攻击。例如：报文过大、版本错误、读团体名进行写操作、SNMPv3用户contextname校验失败、安全模型错误、安全级别错误。
  - 非法inform回应报文攻击。
- SNMP getbulk反射放大DOS攻击

  SNMP报文基于UDP协议，UDP协议是面向无连接的，即客户端和服务端的数据收发都不会记录对方的状态，也就是说不会对“对方”进行数据校验。这样客户端发送来的请求包的源IP地址容易被伪造，服务器端返回的响应包就返回到“被伪造的IP端”，这样就形成了一次反射攻击。放大攻击是指一次小的请求包最终会收到多个数倍于己的响应包，如果进行多次如上攻击，可能导致流量泛洪。

配置维护方法

出于安全考虑，建议关闭不安全的SNMPv1和SNMPv2c版本，配置鉴权加密的SNMPv3用户，并使用v3鉴权加密方式来管理设备，并通过给用户关联acl，mib-view限制用户的访问权限。

1. 配置关闭不安全的SNMPv1和SNMPv2c版本（如果不使用的情况下）。

```
[~HUAWEI] undo snmp-agent sys-info version v1 v2c
[*HUAWEI] commit
```

2. 配置acl规则acl 2001，允许或拒绝某些IP。

```
[~HUAWEI] acl 2001
[*HUAWEI-acl4-basic-2001] rule 5 permit
[*HUAWEI-acl4-basic-2001] rule 10 deny source 10.138.90.111 0
[*HUAWEI-acl4-basic-2001] commit
```

3. 配置SNMP访问控制列表。

```
[~HUAWEI] snmp-agent acl 2001
[*HUAWEI] commit
```

4. 配置mib-view，view名是iso-view，可访问iso为根的子树下的节点。

```
[~HUAWEI] snmp-agent
[*HUAWEI] snmp-agent mib-view included iso-view iso
[*HUAWEI] commit
```

5. 配置v3组，组名是v3group，关联的读视图、写视图、通知视图都为iso-view，并关联acl 2001。

```
[~HUAWEI] snmp-agent group v3 v3group privacy read-view iso-view write-view iso-view notify-view iso-view acl 2001
[*HUAWEI] commit
```

6. 配置一个snmpv3用户，用户名为v3user，归属于v3group组。该用户的鉴权方式为sha2-256，密码为hello-1234，加密方式为aes256，密码为Hello-2012，关联acl 2001。

```
[~HUAWEI] snmp-agent usm-user v3 v3user v3group
[*HUAWEI] snmp-agent usm-user v3 v3user v3group acl 2001
[*HUAWEI] snmp-agent usm-user v3 v3user v3group authentication-mode sha2-256 Hello-1234 privacy-mode aes256 Hello-2012
[*HUAWEI] commit
```

7. 查看当前的SNMP配置。

```
[~HUAWEI] display current-configuration | include snmp
```

```
snmp-agent
snmp-agent acl 2001
snmp-agent local-engineid 800007DB0338BA376BEA01
undo snmp-agent sys-info version v3
snmp-agent group v3 v3group privacy read-view iso-view write-view iso-view notify-view iso-view acl 2001
snmp-agent mib-view included iso-view iso
snmp-agent usm-user v3 v3user
snmp-agent usm-user v3 v3user group v3group
snmp-agent usm-user v3 v3user authentication-mode sha2-256 cipher %^%#!h7X2jV15~c13:~1|(V-:ea+I&v*X8[V;Z61$y];%^%#
snmp-agent usm-user v3 v3user privacy-mode aes256 cipher %^%#Ko$vVUNO[A3t4O%KX6I5nv\4N_o%b#GL'K#dYTZ'%^%#
snmp-agent usm-user v3 v3user acl 2001
```

SNMP还支持v1、v2c的团体字配置。并且通过ACL、Mib-view、团体字限制用户的访问权限。

1. 配置acl规则acl 2001，允许或拒绝某些IP。

```
[~HUAWEI-acl-basic-2001] display this
#
acl number 2001
 rule 5 permit
 rule 10 permit source 10.138.90.111 0
#
return
[~HUAWEI-acl-basic-2001]
```

2. 配置mib-view，view名是iso-view，可访问iso为根的子树下的节点。

```
[~HUAWEI] snmp-agent
```



```
[*HUAWEI] snmp-agent mib-view included iso-view iso
[*HUAWEI] commit
```

3. 配置读写团体字。

```
[~HUAWEI] snmp-agent community read cipher Public-123456 mib-view iso-view acl 2001
[*HUAWEI] snmp-agent community write cipher Private-123456 mib-view iso-view acl 2001
[*HUAWEI] snmp-agent sys-info version all
[*HUAWEI] commit
```

4. 查看SNMP的配置。

```
[~HUAWEI] display this | include snmp
```

```
snmp-agent
snmp-agent local-engineid 800007DB0338BA376BEA01
snmp-agent community read cipher %^%#{H1SU1d}/A{%ZQ8eZwr1,7#s<+=_J$q+G8C|_
$m5wG62/.GguS`8ur>lpTzGS[hHLQitwV9Ih*MQcC>W%^%# mib-view iso-viewiso acl 2001
snmp-agent community write cipher %^%#~]`4X&Vz`#6W1^8<h<L*gBDu3T/^IXLQ
%]7=O@1<'jHCF4o=-KBCH{,8JC~!"v':C8y'sPCq["-/\29G%^%# mib-view iso-viewiso acl 2001
snmp-agent sys-info version all
snmp-agent mib-view included iso-view iso
```

配置基于CPCAR的泛洪攻击防护策略

1. 创建CPU防攻击策略。

```
<HUAWEI> system-view
[~HUAWEI] cpu-defend policy 10
[*HUAWEI-cpu-defend-policy-10] commit
```

2. 配置TCP/IP攻击防范。

   如果当前为去使能状态，请执行如下命令使能该功能。

```
[~HUAWEI-cpu-defend-policy-10] ctcpsyn-flood enable
[*HUAWEI-cpu-defend-policy-10] fragment-flood enable
[*HUAWEI-cpu-defend-policy-10] udp-packet-defend enable
[*HUAWEI-cpu-defend-policy-10] abnormal-packet-defend enable
[*HUAWEI-cpu-defend-policy-10] quit
[*HUAWEI] commit
```

3. 创建ACL。

   在ACL 3341中加入SNMP协议。

```
[~HUAWEI] acl number 3341
[*HUAWEI-acl-adv-3341] rule permit udp source 10.20.20.0 0.0.0.255 source-port eq snmp
[*HUAWEI-acl-adv-3341] rule permit udp source 10.20.20.0 0.0.0.255 destination-port eq snmp
[*HUAWEI-acl-adv-3341] rule deny udp destination-port eq snmp
[*HUAWEI-acl-adv-3341] commit
```

4. 创建用户自定义流。

   在使用ACL对协议报文归类后，通过应用ACL创建自定义流，使不同的协议报文使用不同的上送通道进行传输。

   用户自定义流11对应的ACL为3341，用来保护SNMP协议。由于SNMP协议报文量较大，但实时性要求不高，因此优先级设置为低，带宽设为1M。

```
[~HUAWEI] cpu-defend policy 10
[*HUAWEI-cpu-defend-policy-10] user-defined-flow 11 acl 3341
[*HUAWEI-cpu-defend-policy-10] car user-defined-flow 11 cir 1000
[*HUAWEI-cpu-defend-policy-10] priority user-defined-flow 11 low
[*HUAWEI-cpu-defend-policy-10] quit
[*HUAWEI] commit
```

5. 应用防攻击策略。

```
[~HUAWEI] slot 10
[*HUAWEI-slot-10] cpu-defend-policy 10
[*HUAWEI-slot-10] quit
[*HUAWEI] commit
```


配置维护建议

- 对于SNMPv1、v2c团体字配置，采用了加密存储的方式。配置的团体字不回显，且只能高级别的命令查询团体字的密文字符串。
- 团体名、用户密码的密文存储，有效的从配置上防止配置团体名、用户密码泄漏。
- 在SNMP、CLI、NETCONF的操作日志中对团体名、密码记录时为******，有效防止用户通过读取操作日志获取的团体名和用户密码等安全信息。
- SNMPv1/v2c协议不安全，建议使用更安全的SNMPv3协议。
- 如果设备上不需要SNMP功能，请将SNMP去使能。（SNMP默认未使能）
- 使用SNMPv3，密码要符合复杂度要求，认证密码和加密密码必须要不一样。如果必须使用v1/v2c，SNMP community属性要符合复杂度检查。
- SNMP具备防攻击锁定机制，如果用户认证失败，则进行锁定操作。（默认使能）
- 边缘设备配置URPF隔绝反射攻击。

检查加固结果

- 在系统视图下，执行命令**display this | include snmp**查看SNMP的配置。
- 执行**display cpu-defend tcpip-defend statistics** [**slot** *slot-id*] [**ap-id** *ap-id*] 命令查看TCP/IP攻击防范情况。

废弃不安全的访问通道

在业务需求分析的基础上，优先满足业务的访问需求。在同一个访问需求有多种访问通道服务的情况下，废弃不安全的访问通道，而选择安全的访问通道。

下表列出了各种访问通道的安全水平，优先选择高安全等级的访问通道。

表 1-5 访问通道安全能力评估

访问需求	安全的通道	不安全的通道
远程管理	SSH v2	Telnet
文件传输	SFTP	FTP，TFTP
网管	SNMP v3	SNMP v1/v2
RIP路由	RIP v2	RIP

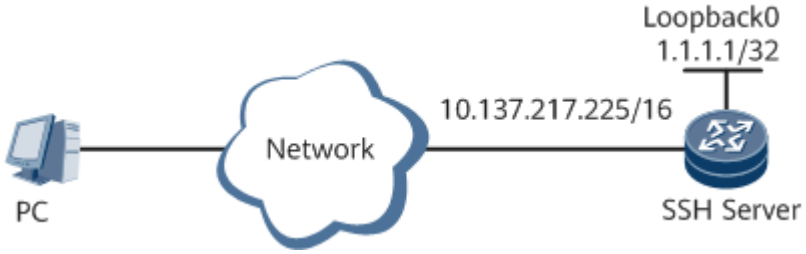
?.1. 配置通过 SFTP 进行文件操作举例

组网需求

如图1-3所示，在作为SSH服务器的设备上使能SFTP服务器功能后，SFTP客户端PC可以通过password、RSA、password-rsa、DSA、password-dsa或all等认证的方式连接到SSH服务器端。

配置用户通过password认证方式登录SSH Server。

图 1-3 配置通过 SFTP 进行文件操作组网图



设备名称	接口	IP地址
SSH Server	GE1/0/1	10.137.217.225/16
SSH Server	Loopback0	1.1.1.1/32

配置思路

采用如下的思路配置用户通过SFTP进行文件操作：

1. 在SSH服务器端生成本地密钥对，实现在服务器端和客户端进行安全地数据交互。
2. 配置SSH用户，包括认证方式，用户名和密码以及授权目录。
3. 在SSH服务器端使能SFTP服务器功能以及配置用户的服务类型。
4. SSH服务器配置源接口。

数据准备

为完成此配置举例，需准备如下的数据：

- SSH用户的认证方式为password，用户名为“client001”，密码为“YsHsjx_202206”。
- client001的用户级别为3。
- SSH服务器端的IP地址为10.137.217.225。
- SSH服务器端的Loopback地址为1.1.1.1。

操作步骤

1. 在服务器端生成本地密钥对

```
<HUAWEI> system-view
[~HUAWEI] sysname SSH Server
[*HUAWEI] commit
[~SSH Server] rsa local-key-pair create
The key name will be: HUAWEI_Host
The range of public key size is (2048, 3072).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

2. 在服务器端配置SSH用户的用户名和密码

```
[*SSH Server] aaa
[*SSH Server-aaa] local-user client001 password
Please configure the password (8-128)
Enter Password:
```



```
Confirm Password:
Info: A new user is added.
[*SSH Server-aaa] local-user client001 level 3
[*SSH Server-aaa] local-user client001 service-type ssh
[*SSH Server-aaa] commit
[~SSH Server-aaa] quit
```

3. 使能SFTP功能，并配置用户的服务类型为SFTP

```
[~SSH Server] interface loopback 0
[~SSH Server-LoopBack0] ip address 1.1.1.1 255.255.255.255
[*SSH Server-LoopBack0] quit
[*SSH Server] sftp server enable
[*SSH Server] ssh server-source -i loopback 0
[*SSH Server] ssh user client001
[*SSH Server] ssh user client001 authentication-type password
[*SSH Server] ssh user client001 service-type sftp
[*SSH Server] commit
```

4. 配置SSH用户的授权目录

```
[~SSH Server] ssh user client001 sftp-directory cfcard:
[*SSH Server] commit
```

5. 验证配置结果

   打开客户端的SFTP软件，输入用户名、密码、端口号（默认为22），访问SSH服务器，并进行文件传输。

配置文件

- SSH服务器的配置文件

```
#
 sysname SSH Server
#
aaa
 local-user client001 password irreversible-cipher $1a$jbB7=)5o.6$::j(W-#|XF&f6"M0>X**1bD0%2_"{4XX!
lO="Sn0$
 local-user client001 level 3
 local-user client001 service-type ssh
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.137.217.225 255.255.0.0
#
interface loopback 0
 ip address 1.1.1.1 255.255.255.255
sftp server enable
ssh server-source -i loopback 0
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory cfcard:
#
return
```

关闭不使用的业务和端口

在分析路由器的业务需求的基础上，按照最小授权原则（除非有明确的访问需求，否则默认关闭访问通道），关闭不使用的业务，关闭不需要开启的TCP/UDP端口。

?.1. 配置关闭 FTP 端口操作举例

组网需求

为了保证文件传输的可靠性，用户采用SFTP方式进行文件操作。同时为了保障设备的安全性，避免非法用户通过FTP端口对设备进行攻击，需要在设备上关闭FTP端口。

配置思路

采用如下的思路配置关闭FTP端口操作举例：

1. 查看设备FTP端口是否打开，确认是否需要关闭FTP端口。
2. 关闭FTP端口，禁止用户通过FTP进行文件操作。
3. 查看设备FTP端口状态，确认FTP端口是否成功关闭。

数据准备

无

操作步骤

1. 查看FTP的IPv4端口状态

```
<HUAWEI> display tcp status
------------------------------------------------------------------------------
Cid/SocketID        Local Addr:Port      Foreign Addr:Port   VPNID     State
------------------------------------------------------------------------------
0x80932724/131216   0.0.0.0:22           0.0.0.0:0           1         LISTEN
0x80C8272A/131218   0.0.0.0:23           0.0.0.0:0           1         LISTEN
0x80952725/131219   0.0.0.0:21           0.0.0.0:0           1         LISTEN
```

FTP端口处于打开状态。

说明

FTP Server可能侦听的是其他端口，可以通过下面的命令行查看FTP侦听的端口号。

```
<HUAWEI> display ftp-server
Server state             : disabled
IPv6 server state        : disabled
Timeout value (mins)     : 30
IPv6 Timeout value (mins): 30
Listen port              : 21
IPv6 listen port         : 21
ACL name                 :
IPv6 ACL name            :
ACL number               :
IPv6 ACL number          :
Current user count       : 0
Max user number          : 15
```

2. 关闭FTP端口

```
<HUAWEI> system-view
[~HUAWEI] undo ftp server
Warning: The operation will stop the FTP server. Do you want to continue? [Y/N]:y
Info: Succeeded in closing the FTP server.
[*HUAWEI] commit
```

3. 查看FTP端口是否成功关闭

```
<HUAWEI> display tcp status
------------------------------------------------------------------------------
Cid/SocketID        Local Addr:Port      Foreign Addr:Port   VPNID     State
------------------------------------------------------------------------------
0x80932724/131216   0.0.0.0:22           0.0.0.0:0           1         LISTEN
0x80C8272A/131218   0.0.0.0:23           0.0.0.0:0           1         LISTEN
```

FTP端口处于关闭状态。

检查加固结果

- 执行命令**display tcp status**，查看FTP端口的状态。
- 执行命令**display ftp-server**，查看FTP服务器的当前的状态。

三面隔离

?.1. 带外网管

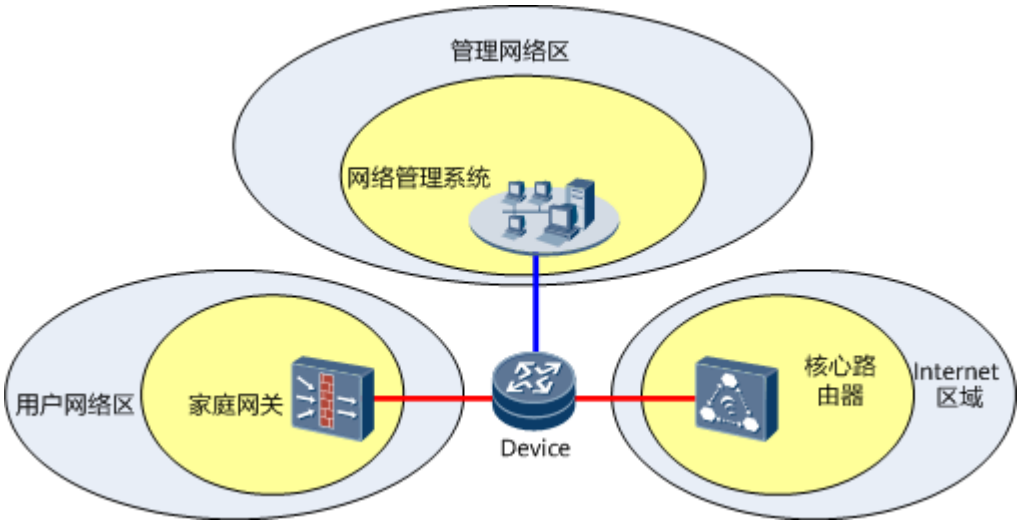
当前默认隔离ICMP协议报文，即报文从管理网口入设备，回应的ICMP报文（包含ICMP差错报文）不会从业务口出设备；反之，报文从业务口入设备，回应的ICMP报文（包含ICMP差错报文）不会从管理网口出设备。

?.1. 管理口绑定 VPN

组网需求

三面隔离的组网图，如图1-4所示。

图 1-4 三面隔离示意图



配置思路

管理网口和管理用Loopback接口绑定特定的管理VPN，业务口配置其他的VPN。业务口的VPN和管理VPN不能互访。

数据准备

无

操作步骤

1. 创建管理VPN

```
<HUAWEI> system-view
[~HUAWEI] ip vpn-instance management
[*HUAWEI-vpn-instance-management] ipv4-family
[*HUAWEI-vpn-instance-management-af-ipv4] commit
[~HUAWEI-vpn-instance-management-af-ipv4] quit
[~HUAWEI-vpn-instance-management] display this
#
ip vpn-instance management
 ipv4-family
#
```

```
return
[~HUAWEI-vpn-instance-management] quit
```

2. 在管理接口和管理用Loopback接口绑定VPN

```
[~HUAWEI] interface GigabitEthernet0/0/0
[~HUAWEI-GigabitEthernet0/0/0] ip binding vpn-instance management
[*HUAWEI-GigabitEthernet0/0/0] commit
[~HUAWEI-GigabitEthernet0/0/0] quit
[~HUAWEI] interface LoopBack0
[~HUAWEI-LoopBack0] ip binding vpn-instance management
[*HUAWEI-LoopBack0] commit
[~HUAWEI-LoopBack0] quit
```

3. 在管理接口和管理用Loopback接口下配置IP地址

```
[~HUAWEI] interface GigabitEthernet0/0/0
[~HUAWEI-GigabitEthernet0/0/0] ip address 10.10.11.100 24
[*HUAWEI-GigabitEthernet0/0/0] commit
[~HUAWEI-GigabitEthernet0/0/0] display this
#
interface GigabitEthernet0/0/0
 undo shutdown
 ip binding vpn-instance management
 ip address 10.10.11.100 255.255.255.0
#
[~HUAWEI] interface LoopBack0
[~HUAWEI-LoopBack0] ip address 1.1.1.1 32
[*HUAWEI-LoopBack0] commit
[~HUAWEI-LoopBack0] display this
#
interface LoopBack0
 ip binding vpn-instance management
 ip address 1.1.1.1 255.255.255.255
#
return
[~HUAWEI-LoopBack0] quit
```

4. 可以通过查看路由表检验管理平面路由是否与控制平面路由隔离

```
[~HUAWEI] display ip routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table: Public
         Destinations : 2        Routes : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[~HUAWEI] display ip routing-table vpn-instance management
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table: management
         Destinations : 3        Routes : 3

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
    10.10.11.0/24  Direct  0    0           D   10.10.11.100    GigabitEthernet0/0/0
  10.10.11.100/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
```

5. 也可以通过ping的方式来查看路由是否隔离

```
<HUAWEI> ping 10.10.11.100
PING 10.10.11.100: 56  data bytes, press CTRL_C to break
   Request time out
   Request time out
   Request time out
   Request time out
   Request time out

 --- 10.10.11.100 ping statistics ---
```



```
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
<HUAWEI> ping -vpn-instance management 10.10.11.100
PING 10.10.11.100: 56  data bytes, press CTRL_C to break
  Reply from 10.10.11.100: bytes=56 Sequence=1 ttl=255 time=1 ms
  Reply from 10.10.11.100: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.10.11.100: bytes=56 Sequence=3 ttl=255 time=10 ms
  Reply from 10.10.11.100: bytes=56 Sequence=4 ttl=255 time=30 ms
  Reply from 10.10.11.100: bytes=56 Sequence=5 ttl=255 time=30 ms

 --- 10.10.11.100 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/20/30 ms
```

检查加固结果

- 执行命令**display this**，查看配置信息。
- 执行命令**display ip routing-table vpn-instance** *vpn-instance-name*，查看管理平面的路由信息。
- 执行命令**display ip routing-table**，查看控制平面的路由信息。

?.2. 通过 MPAC 禁止从业务面上送管理协议报文

组网需求

为了保证只从管理网口接收管理协议报文，可以禁止从业务面上送管理协议报文。

配置思路

创建两个MPAC策略视图，一个用于全局绑定，一个用于接口绑定。全局绑定的策略模板配置禁止上送管理协议报文管理协议的rule。接口绑定的策略配置允许特定管理协议上送的rule，其他管理协议配置为禁止上送。可以采用如下的配置思路：

1. 系统视图下，创建MPAC策略视图global，以及interface。
2. Global视图配置禁止管理协议上送的rule，interface视图配置允管理协议上送的rule。
3. 将MPAC global策略全局绑定，将interface策略绑定到管理网口GigabitEthernet0/0/0。
4. 查看配置结果以及丢弃报文计数。

操作步骤

1. 系统视图下，创建MPAC策略视图global，以及interface

```
[~HUAWEI] service-security policy ipv4 global
[*HUAWEI-service-sec-global] commit
[~HUAWEI] service-security policy ipv4 interface
[*HUAWEI-service-sec-interface] commit
```

2. global视图配置禁止上送ftp、snmp、ssh、telnet、tftp管理协议的rule，interface视图配置允许上送ftp、snmp、ssh、telnet、tftp管理协议的rule

```
[*HUAWEI-service-sec-global] rule deny protocol ftp
[*HUAWEI-service-sec-global] rule deny protocol snmp
[*HUAWEI-service-sec-global] rule deny protocol ssh
[*HUAWEI-service-sec-global] rule deny protocol telnet
[*HUAWEI-service-sec-global] rule deny protocol tftp
```

```
[*HUAWEI-service-sec-global] commit
[~HUAWEI-service-sec-global] quit
[*HUAWEI-service-sec-interface] rule permit protocol ftp
[*HUAWEI-service-sec-interface] rule permit protocol snmp
[*HUAWEI-service-sec-interface] rule permit protocol ssh
[*HUAWEI-service-sec-interface] rule permit protocol telnet
[*HUAWEI-service-sec-interface] rule permit protocol tftp
[*HUAWEI-service-sec-interface] commit
[~HUAWEI-service-sec-interface] quit
```

3. 将interface策略绑定到管理网口GigabitEthernet0/0/0，将MPAC global策略全局绑定

```
[~HUAWEI] interface GigabitEthernet0/0/0
[*HUAWEI-GigabitEthernet0/0/0] service-security binding ipv4 interface
[*HUAWEI-GigabitEthernet0/0/0] commit
[~HUAWEI-GigabitEthernet0/0/0] quit
[*HUAWEI] service-security global-binding ipv4 global
[*HUAWEI] commit
```

说明

如果只配置全局策略，并且全局策略不允许管理协议通过，则会导致设备托管。为了防止设备托管，应该先配置某些口上允许管理协议通过，而且要保证这些接口是UP。

检查加固结果

- 执行命令**display service-security statistics ipv4**查看是否所有业务口均不能上送管理协议，管理协议均被丢弃（可以查看统计计数）。
- 执行命令**display service-security binding ipv4**查看接口的管理平面接入控制策略信息。
- 执行命令**display service-security policy ipv4**查看IPv4管理平面接入控制策略的配置信息。

?.2. 基于 VPN 的带内网管

?.1. 选择一个业务口绑定管理 VPN

组网需求

为了保证只从某一个业务口接收管理协议报文，可以将业务口绑定到一个独立的VPN中。

配置思路

创建管理VPN，将选定的业务口和loopback接口绑定到该管理VPN中。其他业务口配置其他的VPN。两个VPN不能互访。

数据准备

无

操作步骤

1. 创建管理VPN

```
[~HUAWEI] ip vpn-instance management
[*HUAWEI-vpn-instance-management] ipv4-family
[*HUAWEI-vpn-instance-management] commit
```

```
[~HUAWEI-vpn-instance-management-af-ipv4] quit
[~HUAWEI-vpn-instance-management] display this
#
ip vpn-instance management
 ipv4-family
#
return
```

2. 在业务接口和管理用Loopback接口绑定VPN

```
[~HUAWEI] interface gigabitethernet3/0/1
[~HUAWEI-GigabitEthernet3/0/1] ip binding vpn-instance management
Info: All IPv4 and IPv6 related configurations on this interface are removed.
[*HUAWEI-GigabitEthernet3/0/1] commit
[~HUAWEI-GigabitEthernet3/0/1] quit
[~HUAWEI] interface LoopBack0
[~HUAWEI-LoopBack0]ip binding vpn-instance management
Info: All IPv4 and IPv6 related configurations on this interface are removed.
[*HUAWEI-LoopBack0]commit
```

3. 在业务接口和管理用Loopback接口下配置IP地址

```
[~HUAWEI-GigabitEthernet3/0/1] ip address 10.3.1.1 24
[*HUAWEI-GigabitEthernet3/0/1] commit
[~HUAWEI-GigabitEthernet3/0/1] display this
#
interface GigabitEthernet3/0/1
 undo shutdown
 ip binding vpn-instance management
 ip address 10.3.1.1 255.255.255.0
#
[~HUAWEI]interface LoopBack 0
[~HUAWEI-LoopBack0] ip address 1.1.1.1 32
[*HUAWEI-LoopBack0] commit
[~HUAWEI-LoopBack0] display this
#
interface LoopBack0
 ip binding vpn-instance management
 ip address 1.1.1.1 255.255.255.255
#
return
```

检查加固结果

- 执行命令**display this**，查看配置信息。
- 执行命令**display ip routing-table vpn-instance** *vpn-instance-name*，查看VPN实例IPv4地址族的路由信息。

?.2. 通过 MPAC 禁止从其他业务口上送管理协议报文

组网需求

为了保证只从某些业务口上接收管理协议报文，可以只放开部分特定业务口接收某些管理协议报文的能力，而禁止其他业务口上送管理协议报文。

配置思路

创建两个MPAC策略视图，一个用于全局绑定，一个用于接口绑定。全局绑定的策略模板配置禁止上送管理协议报文管理协议的rule。接口绑定的策略配置允许特定管理协议上送的rule，其他管理协议配置为禁止上送。可以采用如下的配置思路：

1. 系统视图下，创建MPAC策略视图global，以及interface。
2. Global视图配置禁止管理协议上送的rule，interface视图配置允管理协议上送的rule。

3. 将MPAC global策略全局绑定，将interface策略绑定到接口GE3/0/1以及管理网口GigabitEthernet0/0/0。
4. 查看配置结果以及丢弃报文计数。

操作步骤

1. 系统视图下，创建MPAC策略视图global，以及interface

```
[~HUAWEI] service-security policy ipv4 global
[*HUAWEI-service-sec-global] commit
[*HUAWEI-service-sec-global] quit
[~HUAWEI] service-security policy ipv4 interface
[*HUAWEI-service-sec-interface] commit
[*HUAWEI-service-sec-global] quit
```

2. global视图配置禁止上送ftp、snmp、ssh、telnet、tftp管理协议的rule，interface视图配置允许上送ftp、snmp、ssh、telnet、tftp管理协议的rule

```
[*HUAWEI-service-sec-global] rule deny protocol ftp
[*HUAWEI-service-sec-global] rule deny protocol snmp
[*HUAWEI-service-sec-global] rule deny protocol ssh
[*HUAWEI-service-sec-global] rule deny protocol telnet
[*HUAWEI-service-sec-global] rule deny protocol tftp
[*HUAWEI-service-sec-global] commit
[~HUAWEI-service-sec-global] quit
[*HUAWEI-service-sec-interface] rule permit protocol ftp
[*HUAWEI-service-sec-interface] rule permit protocol snmp
[*HUAWEI-service-sec-interface] rule permit protocol ssh
[*HUAWEI-service-sec-interface] rule permit protocol telnet
[*HUAWEI-service-sec-interface] rule permit protocol tftp
[*HUAWEI-service-sec-interface] commit
[~HUAWEI-service-sec-interface] quit
```

3. 将interface策略绑定到接口GE3/0/1以及管理网口GigabitEthernet0/0/0，将MPAC global策略全局绑定

```
[~HUAWEI] interface GigabitEthernet0/0/0
[*HUAWEI-GigabitEthernet0/0/0] service-security binding ipv4 interface
[*HUAWEI-GigabitEthernet0/0/0] commit
[~HUAWEI-GigabitEthernet0/0/0] quit
[~HUAWEI] interface GigabitEthernet 3/0/1
[*HUAWEI-GigabitEthernet3/0/1] service-security binding ipv4 interface
[*HUAWEI-GigabitEthernet3/0/1] commit
[~HUAWEI-GigabitEthernet3/0/1] quit
[*HUAWEI] service-security global-binding ipv4 global
[*HUAWEI] commit
```

4. 查看配置结果

```
[~HUAWEI] display service-security binding ipv4
  Configured : Global
  Policy Name: global

Interface  : GigabitEthernet0/0/0
  Policy Name: interface

Interface  : GigabitEthernet3/0/1
  Policy Name: interface
[~HUAWEI] display service-security policy ipv4
  Policy Name : global
  Step        : 5
   rule 5 deny protocol ftp
   rule 10 deny protocol snmp
   rule 15 deny protocol ssh
   rule 20 deny protocol tftp
   rule 25 deny protocol telnet

Policy Name : interface
Step        : 5
 rule 5 permit protocol ftp
 rule 10 permit protocol snmp
 rule 15 permit protocol ssh
```



```
rule 20 permit protocol tftp
rule 25 permit protocol telnet
```

检查加固结果

- 执行**display service-security statistics ipv4**命令查看是否所有业务口均不能上送管理协议，管理协议均被丢弃（可以查看统计计数）。
- 执行**display service-security binding ipv4**命令查看接口的管理平面接入控制策略信息。
- 执行**display service-security policy ipv4**命令查看IPv4管理平面接入控制策略的配置信息。

?.3. 基于公网的带内网管

?.1. 选择一个业务接口和 Loopback 接口，作为管理接口

组网需求

无

配置思路

在业务接口和管理用Loopback接口下配置IP地址，并且都不绑定VPN。

数据准备

无

操作步骤

在业务接口和管理用Loopback接口下配置IP地址

```
[*HUAWEI-GigabitEthernet3/0/1] ip address 10.3.1.1 24
[*HUAWEI-GigabitEthernet3/0/1] commit
[~HUAWEI-GigabitEthernet3/0/1] display this
#
interface GigabitEthernet3/0/1
 undo shutdown
 ip address 10.3.1.1 255.255.255.0
#
[~HUAWEI-GigabitEthernet3/0/1] quit
[~HUAWEI] interface LoopBack 0
[~HUAWEI-LoopBack0] ip address 1.1.1.1 32
[*HUAWEI-LoopBack0] commit
[~HUAWEI-LoopBack0] display this
#
interface LoopBack0
  ip address 1.1.1.1 255.255.255.255
#
```

检查加固结果

- 执行命令**display this**，查看配置信息。
- 执行命令**display ip routing-table**，查看路由信息。

?.2. 通过 MPAC 禁止从其他业务口上送管理协议报文

组网需求

为了保证只从某些业务口上接收管理协议报文，可以只放开部分特定业务口接收某些管理协议报文的能力，而禁止其他业务口上送管理协议报文。

配置思路

创建两个MPAC策略视图，一个用于全局绑定，一个用于接口绑定。全局绑定的策略模板配置禁止上送管理协议报文管理协议的rule。接口绑定的策略配置允许特定管理协议上送的rule，其他管理协议配置为禁止上送。可以采用如下的配置思路：

1. 系统视图下，创建MPAC策略视图global，以及interface。
2. Global视图配置禁止管理协议上送的rule，interface视图配置允许管理协议上送的rule。
3. 将MPAC global策略全局绑定，将interface策略绑定到接口GE3/0/1以及管理网口GigabitEthernet0/0/0。
4. 查看配置结果以及丢弃报文计数。

操作步骤

1. 系统视图下，创建MPAC策略视图global，以及interface
```
[~HUAWEI] service-security policy ipv4 global
[*HUAWEI-service-sec-global] commit
[*HUAWEI-service-sec-global] quit
[~HUAWEI] service-security policy ipv4 interface
[*HUAWEI-service-sec-interface] commit
[*HUAWEI-service-sec-global] quit
```
2. global视图配置禁止上送ftp、snmp、ssh、telnet、tftp管理协议的rule，interface视图配置允许上送ftp、snmp、ssh、telnet、tftp管理协议的rule
```
[*HUAWEI-service-sec-global] rule deny protocol ftp
[*HUAWEI-service-sec-global] rule deny protocol snmp
[*HUAWEI-service-sec-global] rule deny protocol ssh
[*HUAWEI-service-sec-global] rule deny protocol telnet
[*HUAWEI-service-sec-global] rule deny protocol tftp
[*HUAWEI-service-sec-global] commit
[~HUAWEI-service-sec-global] quit
[*HUAWEI-service-sec-interface] rule permit protocol ftp
[*HUAWEI-service-sec-interface] rule permit protocol snmp
[*HUAWEI-service-sec-interface] rule permit protocol ssh
[*HUAWEI-service-sec-interface] rule permit protocol telnet
[*HUAWEI-service-sec-interface] rule permit protocol tftp
[*HUAWEI-service-sec-interface] commit
[~HUAWEI-service-sec-interface] quit
```
3. 将interface策略绑定到接口GE3/0/1以及管理网口GigabitEthernet0/0/0，将MPAC global策略全局绑定。
```
[~HUAWEI] interface GigabitEthernet0/0/0
[*HUAWEI-GigabitEthernet0/0/0] service-security binding ipv4 interface
[*HUAWEI-GigabitEthernet0/0/0] commit
[~HUAWEI-GigabitEthernet0/0/0] quit
[~HUAWEI] interface GigabitEthernet 3/0/1
[*HUAWEI-GigabitEthernet3/0/1] service-security binding ipv4 interface
[*HUAWEI-GigabitEthernet3/0/1] commit
[~HUAWEI-GigabitEthernet3/0/1] quit
[*HUAWEI] service-security global-binding ipv4 global
[*HUAWEI] commit
```
4. 查看配置结果


```
[~HUAWEI] display service-security binding ipv4
 Configured : Global
 Policy Name: global

Interface  : GigabitEthernet0/0/0
 Policy Name: interface

Interface  : GigabitEthernet3/0/1
 Policy Name: interface
[~HUAWEI] display service-security policy ipv4
 Policy Name : global
 Step        : 5
  rule 5 deny protocol ftp
  rule 10 deny protocol snmp
  rule 15 deny protocol ssh
  rule 20 deny protocol tftp
  rule 25 deny protocol telnet

Policy Name : interface
Step        : 5
 rule 5 permit protocol ftp
 rule 10 permit protocol snmp
 rule 15 permit protocol ssh
 rule 20 permit protocol tftp
 rule 25 permit protocol telnet
```

检查加固结果

- 执行**display service-security statistics ipv4**命令查看是否所有业务口均不能上送管理协议，管理协议均被丢弃（可以查看统计计数）。
- 执行**display service-security binding ipv4**命令查看接口的管理平面接入控制策略信息。
- 执行**display service-security policy ipv4**命令查看IPv4管理平面接入控制策略的配置信息。

?.3. 服务器对呼入呼出的限制

组网需求

为了提高系统安全性，可以通过指定服务器端的源接口、源地址，增加登录受限功能，只有通过指定源接口、源地址才可以登录服务器。

配置思路

采用如下的思路配置服务器端源接口、源地址。

- 配置客户端与所要设置的源接口三层互通。
- 为各服务器配置源接口、源地址。
- 如果服务器仅接受从指定源接口、源地址进来的连接，则配置成功。

数据准备

无

telnet server

设置源接口之后，客户端将只能通过该接口登录Telnet服务器。


```
[~HUAWEI] telnet server-source -i LoopBack 1
```

设置源IPv6地址之后，客户端将只能通过该地址登录Telnet服务器。

```
[~HUAWEI] telnet ipv6 server-source -a 2001:db8::1
```

设置源接口，并同时配置接口隔离。

```
[~HUAWEI] telnet server-source physic-isolate -i GigabitEthernet 1/0/0 -a 10.1.1.1
```

设置源IPv6接口，并同时配置接口隔离。

```
[~HUAWEI] telnet ipv6 server-source physic-isolate -i GigabitEthernet 1/0/0 -a 2001:db8::1
```

SSH server

设置源接口之后，客户端将只能通过该接口登录SSH服务器。

```
[~HUAWEI] ssh server-source -i LoopBack 1
```

设置源IPv6地址之后，客户端将只能通过该地址登录SSH服务器。

```
[~HUAWEI] ssh ipv6 server-source -a 2001:db8::1
```

设置源接口，并同时配置接口隔离。

```
[~HUAWEI] ssh server-source physic-isolate -i GigabitEthernet 1/0/0 -a 10.1.1.1
```

设置源IPv6接口，并同时配置接口隔离。

```
[~HUAWEI] ssh ipv6 server-source physic-isolate -i GigabitEthernet 1/0/0 -a 2001:db8::1
```

FTP server

设置源地址之后，客户端将只能通过该地址登录FTP服务器。

```
[~HUAWEI] ftp server-source -a 10.1.1.1
```

设置源IPv6地址之后，客户端将只能通过该地址登录FTP服务器。

```
[~HUAWEI] ftp ipv6 server-source -a 2001:db8::1
```

设置源接口之后，客户端将只能通过该接口登录FTP服务器。

```
[~HUAWEI] ftp server-source -i LoopBack 1
```

设置源接口，并同时配置接口隔离。

```
[~HUAWEI] ftp server-source physic-isolate -i GigabitEthernet 1/0/0 -a 10.1.1.1
```

设置源IPv6接口，并同时配置接口隔离。

```
[~HUAWEI] ftp ipv6 server-source physic-isolate -i GigabitEthernet 1/0/0 -a 2001:db8::1
```

检查加固结果

- 执行命令**display current-configuration configuration** telnet，查看telnet的配置情况。
- 执行命令**display current-configuration configuration** ssh，查看SSH的配置情况。
- 执行命令**display current-configuration configuration** ftp，查看FTP的配置情况。

NTP

安全策略介绍

网络技术的快速发展对网络安全提出了更高的要求。在网络中传递的NTP（Network Time Protocol）报文有可能被修改。 报文攻击可能会引起网络中断，扰乱同步，造成网络数据的丢失。所以，需要有安全措施来保障报文的安全传递。

NTP在协议层面上提供了以下安全策略：

- NTP支持验证功能，从而避免接收到错误的报文和来自网络的重放攻击。
- NTP支持白名单功能，协议会给每个已知端口建立一个“白名单安全”标签，实现更快速地互换报文。这对保证网络中的快速收敛是非常必要的。若发送报文的端口不在“白名单安全”列表中，则只有有限的缺省带宽资源分配给这些端口，从而避免DOS攻击。
- NTP支持通过命令行修改接收NTP报文的缺省端口号来避免DOS攻击。
- 通过设置访问权限保护本地NTP服务，是设备提供的一种比较简单的安全措施。

攻击方法介绍

客户端和服务器配置验证功能后，NTP只接收经过验证的报文，从而避免来自未经认证者的报文攻击。

防止子网攻击可以通过选择可信赖的时间服务器并且只允许这些时间服务器成为同步源来实现。

配置维护方法

NTP支持HMAC-SHA256进行密钥认证来提高安全性。

1. # 在客户端上将密钥的验证密钥设置为“Huawei-12345”，验证算法为HMAC-SHA256。

   ```
   [~HUAWEI] ntp-service authentication enable
   [*HUAWEI] ntp-service authentication-keyid 1 authentication-mode hmac-sha256 Huawei-12345
   [*HUAWEI] ntp-service reliable authentication-keyid 1
   [*HUAWEI] commit
   [~HUAWEI] display current-configuration | include ntp
   #
   ntp-service authentication-keyid 1 authentication-mode hmac-sha256 cipher %^%#5_TD
   +l')]GVp>0:^0zBMN{%V;<_rw:v7E3,1X}C/%^%#
   ntp-service reliable authentication-keyid 1
   ntp-service authentication enable
   #
   ```

2. # 在服务器上将密钥的验证密钥设置为“Huawei-12345”，验证算法为HMAC-SHA256。

   ```
   [~HUAWEI] ntp-service authentication enable
   [*HUAWEI] ntp-service authentication-keyid 1 authentication-mode hmac-sha256 Huawei-12345
   [*HUAWEI] commit
   [~HUAWEI] display current-configuration | include ntp
   #
   ntp-service authentication-keyid 1 authentication-mode hmac-sha256 cipher %@%@rob
   %'[{S0IcI6$Y.xM]+,1e*%@%@
   ntp-service authentication enable
   #
   ```

3. # 设置允许匹配ACL 2000 IPv4和ACL 2002 IPv6的peer可以对本地设备进行时间请求、查询控制、时间同步。

   ```
   [~HUAWEI] ntp-service access peer 2000 ipv6 2002
   [*HUAWEI] commit
   [~HUAWEI] display current-configuration | include ntp
   #
   ```



```
ntp-service access peer 2000 ipv6 2002
#
```

NTP支持通过命令行修改接收NTP报文的缺省端口号来避免DOS攻击。

1. 将接收NTP报文的端口号修改为1026。
   [~HUAWEI] **ntp-service port 1026**

配置维护建议

HMAC-SHA256算法的安全性高，推荐使用HMAC-SHA256算法进行NTP密钥验证。

ACL需要在最后一条rule规则deny所有IP地址，如果ACL过滤VPN内的地址，需要在ACL内配置**rule** [*rule-id*] **deny vpn-instance** *vpn-instance-name*。

检查加固结果

- 执行命令**display ntp-service sessions** [**verbose**]命令查看NTP服务维护的会话状态。
- 执行命令**display ntp-service statistics packet** 命令查看全局NTP报文的统计信息。

安全风险查询

背景信息

由于协议自身的安全性能不同，用户配置时使用的某些协议可能存在安全风险。通过**display security risk**命令可查看系统中存在的安全风险，并根据给出的修复建议解除风险。例如，用户配置了SNMPv1功能，该功能存在安全风险，系统会提示并建议使用SNMPv3协议。

操作步骤

步骤1 在用户视图下，执行命令**display security risk** [[**feature** *feature-name*] | [**level** *level-para*] | [**type** *type-para*]]*，查询当前系统中存在的安全风险信息及风险的修复建议。

说明

不同级别的用户查看到的安全风险信息也不相同。管理级用户能够查看到系统中所有风险信息，其他级别用户只能看到低于或等于自己级别的风险信息。

----结束

检查加固结果

执行命令**display security risk**，查看系统中存在的安全风险信息。

数字证书管理

功能介绍

数字证书由用户向其信任的证书颁发机构申请，为IPSec、SSH、SSL等安全特性提供多种服务，如身份验证、访问控制、完整性和机密性的保障。

为了安全，数字证书在颁发时会规定其有效期，过期的数字证书在校验时会失效，无法正常使用。因此，为了避免因为证书过期导致网络业务受损，需要定期通过命令或者告警来有效识别即将过期或者已经过期的证书。

设备提供的预置数字证书详见下表。根据业务需求，若需要配置新的证书，可通过命令行进行配置和更新。

表 1-6 预置数字证书

证书类型	证书功能	说明
预置CA证书	验证对端华为设备身份。	预置CA证书的导入和查询： 执行**pki load preset-ca domain** *default*命令将预置设备CA证书导入，默认未导入预置CA证书。可通过**display pki ca_list domain** *default*来查询证书内容。 预置CA证书的删除和替换： 将预置CA证书导入default域后，执行**undo pki load preset-ca domain** *default*命令将预置CA证书从default域移除。如果需要使用其他CA证书，可以导入到default域参与证书认证。
预置本地证书	供其他设备验证本端设备身份。	预置本地证书的导入和查询： 执行**pki load preset-local domain** *default* 命令将预置设备证书导入，默认已导入预置本地证书。可通过**display pki cert_list domain** *default*来查询证书内容。 预置本地证书的删除和替换： 将预置设备证书导入default域后，执行**undo pki load preset-local domain** *default*命令将预置设备证书从default域移除。Default域不支持导入其他证书，如果需要使用其他用户证书替换设备预置证书，可新建一个pki域，将用户证书导入到新建的域，业务绑定新建域来替换。

表 1-7 证书使用情况

使用证书的特性/模块	证书用途	是否默认使用预置证书	是否支持用户替换为自己的证书	是否涉及申请多个证书、加载顺序是否有要求	自行申请证书时对格式、名称的要求	自行申请证书时对Common Name等字段的要求
QX业务	控制器访问设备的DCN管理通道加密数据使用	是	是	否	格式为x509	无

使用证书的特性/模块	证书用途	是否默认使用预置证书	是否支持用户替换为自己的证书	是否涉及申请多个证书、加载顺序是否有要求	自行申请证书时对格式、名称的要求	自行申请证书时对Common Name等字段的要求
SZTP业务	当传输网络不安全时，可以通过ssl-policy参数配置SZTP服务使用SSL加密传输方式。	是	否	否	无	设备证书的Common Name使用ESN作为标识

配置维护方法

证书过期的查询方法

- 通过命令查询

```
<HUAWEI> display pki ca_list
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            49:71:c8:f9:31:04:3e:1b:42:bc:29:f6:bb:06:40:33:b3:f7:53:d9
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=root,OU=HW,O=HW,L=NJ,ST=JS,C=CN
        Validity
            Not Before: Jun  16  01:01:45 2021 GMT
            Not After : Jun  16  01:01:45 2022 GMT
```

- 通过告警查询

```
<HUAWEI> display alarm active
1:Critical  2:Major  3:Minor  4:Warning
------------------------------------------------------------------------------
Sequence   AlarmId    Level Date Time  Description
------------------------------------------------------------------------------
1393       0xF10091   1     2024-01-02 The CA certificate is invalid. (CACertSta
                            20:53:26  rtTime=2022-02-14 06:48:00, CACertFinishT
                            ime=2023-02-14 06:48:00, CACertIssuer=CN=
                            11,OU=11,O=11,C=11,E=11, CACertSubject=CN
                            =11,O=11,C=11, FileName=huawei1.cer, Inva
                            lidReason=The current time is not within
                            the validity period of the certificate)
------------------------------------------------------------------------------
```

证书更新的操作步骤

详细步骤可以参考“配置->安全->PKI配置->维护PKI”中的“更新过期的本地证书和CRL证书”页面。

证书更新的方法包括离线方式和CMP方式，下面以CMP方式自动更新证书为例，介绍证书更新的操作步骤。配置前，需要先确保CA服务器已经完成配置，可以自动进行证书的颁发；初始认证时设备已经预制了与CA服务器相互认证的外部证书，例如1中的abc.cer。

1. 配置CMP方式证书申请

```
[~HUAWEI] rsa pki local-key-pair abc create
Info: The name of the new RSA key will be:abc.
Info: The name of the new RSA key will be:abc.
The range of public key size is (2048 ~ 4096).
NOTES: If the key modulus is greater than 2048,
it will take a few minutes.
Input the bits in the modulus[default = 3072]:
Info: Operating, please wait for a moment.....done.
Info: Create RSA local-key-pair success.
<HUAWEI> system-view
[~HUAWEI] pki entity abc
[*HUAWEI] commit
[~HUAWEI-pki-entity-abc] common-name HUAWEI
[*HUAWEI-pki-entity-abc] commit
[~HUAWEI-pki-entity-abc] quit
[~HUAWEI] pki domain abc
[*HUAWEI-pki-domain-abc] pki cmp session abc
[*HUAWEI-pki-domain-abc-pki-cmp-session-abc] cmp request entity abc
[*HUAWEI-pki-domain-abc-pki-cmp-session-abc] cmp request rsa local-key-pair abc regenerate
4096
[*HUAWEI-pki-domain-abc-pki-cmp-session-abc] cmp request ca-name "/C=CN/O=JIT/
CN=CMPSignCert"
[*HUAWEI-pki-domain-abc-pki-cmp-session-abc] cmp request authentication-cert abc.cer
[*HUAWEI-pki-domain-abc-pki-cmp-session-abc] cmp request server url http://10.10.10.10:10000/
cmp
[*HUAWEI-pki-domain-abc-pki-cmp-session-abc] commit
[~HUAWEI-pki-domain-abc-pki-cmp-session-abc] quit
[~HUAWEI-pki-domain-abc] pki cmp initial-request
[~HUAWEI-pki-domain-abc] quit
```

2. 导入CA和本地证书

```
[~HUAWEI] pki import-certificate local filename abc_ir.cer
[~HUAWEI] pki import-certificate ca filename abc_ca0.cer
[~HUAWEI] pki import-certificate ca filename abc_ca1.cer
```

3. 开启PKI严格校验模式

```
[~HUAWEI] pki strict-mode
```

4. 使能证书自动更新功能

```
[~HUAWEI] pki domain abc
[~HUAWEI-pki-domain-abc] pki cmp session abc
[~HUAWEI-pki-domain-abc-pki-cmp-session-abc] cmp request authentication-cert abc_ir.cer
[~HUAWEI-pki-domain-abc-pki-cmp-session-abc] certificate auto-update enable
```

检查加固结果

1. 执行命令**display rsa pki local-key-pair public**，查看RSA密钥对信息。
2. 执行命令**display pki match-rsa-key certificate-filename** *file-name*，查看证书所使用的密钥。
3. 执行命令**display pki cert-req filename** *file-name*查看指定文件名的证书请求文件的内容。
4. 执行命令**display pki certificate filename** *file-name*查看指定文件名的证书的内容。
5. 执行命令**display pki crl filename** *file-name*查看指定文件名的CRL的内容。
6. 执行命令**display pki ca_list** [**domain** *domainName*]查看导入到内存中的CA证书和CRL的内容。
7. 执行命令**display pki cert_list** [**domain** *domainName*]查看导入到内存中的本地证书的内容。

日志信息安全

功能介绍

日志主要用于记录设备上用户操作，设备运行状态等信息，以日志文件的形式存在设备上，为网络管理员监控路由器的运行情况和定位网络故障提供了有力的支持。

安全策略介绍

日志的安全由各种接入方式的认证和SOCKET安全来保证，仅有管理员权限支持查看。日志的查看方式有三种：

- 用户登录设备通过命令行查看日志。
- 通过SFTP方式将日志文件取到本地查看。
- 通过日志主机方式，将日志信息发送到日志服务器。

以上三种查看方式，均需要用户能通过密码认证、SSL证书认证、AAA认证或Public-Key认证，成功的登录设备，进行在线查看及获取日志文件等操作。

为了保证日志传输的安全性，建议使用基于TCP的SSL加密传输方式。

配置维护方法

参考CONSOLE/TELNET/SSH/FTP/TFTP/SOCKET等配置维护方法。

建议使用VPN网络基于TCP的SSL加密方式进行日志传输。

1. 配置VPN。
```
[~HUAWEI] ip vpn-instance vrf2
[*HUAWEI-vpn-instance-vrf2] route-distinguisher 2:2
[*HUAWEI-vpn-instance-vrf2-af-ipv4] commit
[~HUAWEI-vpn-instance-vrf2-af-ipv4] quit
[~HUAWEI-vpn-instance-vrf2] vpn-target 2:2
IVT Assignment result:
Info: VPN-Target assignment is successful.
EVT Assignment result:
Info: VPN-Target assignment is successful.
[*HUAWEI-vpn-instance-vrf2] commit
[~HUAWEI-vpn-instance-vrf2] quit
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-GigabitEthernet1/0/0] ip binding vpn-instance vrf2
[*HUAWEI-GigabitEthernet1/0/0] ip address 10.137.130.245 255.255.254.0
[*HUAWEI-GigabitEthernet1/0/0] commit
```
2. 配置SSL策略并加载证书。
```
[~HUAWEI] ssl policy huawei2014
[*HUAWEI-ssl-policy-huawei2014] certificate load pem-cert servercert.pem key-pair dsa key-file serverkey.pem auth-code cipher huawei-123456
[*HUAWEI-ssl-policy-huawei2014] crl load pem-crl server.pem
[*HUAWEI-ssl-policy-huawei2014] trusted-ca load asn1-ca servercert.der
[*HUAWEI-ssl-policy-huawei2014] commit
[~HUAWEI-ssl-policy-huawei2014] quit
```
3. 配置携带VPN属性的日志主机，传输方式选择基于TCP的SSL加密方式。
```
[~HUAWEI] info-center loghost 10.137.130.245 vpn-instance vrf2 transport tcp ssl-policy huawei2014
[*HUAWEI] commit
```

配置维护建议

参考CONSOLE/TELNET/SSH/FTP/TFTP/SOCKET等配置维护建议。日志传输使用基于TCP的SSL加密方式，避免报文被非法截取。

检查加固结果

- 执行命令**display info-center** [**statistics**]查看信息管理记录的各项信息。
- 执行命令**display channel** [*channel-number* | *channel-name*]查看信息通道的内容。

安全审计

背景信息

安全审计包括识别、记录、存储和分析与安全行为有关的信息。安全审计的检查结果用来判断发生了哪些安全行为，以及哪些用户要对这些行为负责。审计需要的信息需要能够单独日志存储，并分配独立的安全通道，确保这些日志能够防篡改、防删除，防破译。审计相关的日志的安全等级需要比普通日志等级要高，即使系统被攻击，日志模块也不会被篡改。后续要使用这些安全日志来分析和溯源设备所遭到的攻击。

安全日志可以用来做安全审计溯源，安全日志范畴包括系统启动校验日志、账户登录日志(如AAA日志)、账户管理日志、网络安全事件记录日志，证书秘钥管理等操作日志。

操作步骤

在发现设备被攻击或系统存在不安全时，可以在系统视图下，执行命令**display logfile cfcard:/logfile/security/security.log**，过滤查看对应日志ID，就可以查看对应日志，通过时间点可以观察系统运行过程中是否有异常越权访问。

执行命令**display logfile cfcard:/logfile/security/security.log**，查看具体安全日志详细信息，包括日志产生时间，事件类型，事件内容，事件触发源等。

```
<HUAWEI> display logfile cfcard:/logfile/security/security.log
################################################################################
#####
#     This logfile is generated at slot 1
#
Digest(0000029124):aea3e0df5dd7b86e5db512c1f67d950299e1f88e3b605526ddc3bcc2c50acac4
################################################################################
#####
Jun 11 2019 07:41:21 HUAWEI %%01OPS/5/OPS_LOGIN(s):CID=0x80b40431;Succeeded in establishing the
OPS connection.(ServiceType=embedding-script, UserName=_SYSTEM_, Ip=0.0.0.0, VpnName=_public_)
```

1.1.7.1.2 转发平面

泛洪攻击防护

路由器作为网络流量的承载节点，需要通过管理控制协议完成业务策略的部署以控制报文按照预期的路径转发。在部署到互联网公网地址空间的场景下，路由器本身也可能遭受管理控制平面的流量泛洪攻击，因此需要部署CPU防护策略对路由器自身进行流量攻击防护。

对于转发流量的泛洪攻击，攻击目标为特定互联网站点，路由器自身通常不受直接影响，路由器通常只作为防攻击的辅助网元用于检测发现流量异常并执行流量策略，对攻击流量进行丢弃或调度，此部分在此不再详述。

?.1. 基于 CPCAR 报文速率限制的 CPU 防护

基于CPCAR报文速率限制防攻击，是指通过对上送报文根据协议类型进行分类，用CPCAR控制转发平面送往CPU的报文的带宽、优先级和包长，同时控制总的上送带宽，以达到控制上送报文的数量，优先保证高优先级业务，防止单板CPU过载以及攻击产生时发出告警以达到防御的目的。

目前CPU被攻击时对业务的影响主要来自于三方面原因：

1. 没有区分合法协议报文和非法协议报文，CPU忙于处理大量非法协议报文利用率大幅升高，影响了对正常协议报文的处理。
2. 部分协议报文使用同一通道上送CPU处理，当其中一个协议由于网络发生环路，导致海量报文被“链式反应”复制堵塞了上送CPU的通道，影响了其他协议
3. 协议报文的上送通道带宽不合理（要么太大，要么太小），发生流量冲击时影响其他上送通道的协议处理。

   为了避免由于人因差错、IT管理导致的安全事故，要求做到：

   a. 收集设备上运行的各种业务涉及的协议，并进行归类
   b. 用ACL对三层报文进行过滤，合法协议报文入白名单和用户自定义流，其他报文走黑名单
   c. 对黑名单、白名单和用户自定义流这三类名单的优先级，上送带宽，告警功能进行规划
   d. 非三层业务进行带宽限制，设备上不部署的业务有选择地关闭

本文档根据当前现网业务和被攻击情况，对目前常见的协议进行归类并制定了其处理建议。本文档下述的配置方案也以该处理建议进行介绍。

?.1. CPCAR 的配置方法和步骤

下面通过一个CPCAR配置实例，讲解如何将信任网段加入到白名单。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**acl** { [**number**] *acl-number* | **name** *acl-name* [**number** *acl-number*] } [**match-order** { **auto** | **config** }]，创建高级ACL。
3. 执行命令**rule** [*rule-id*] **permit** [**fragment-type** *fragment-type-name* | **source** { *source-ip-address source-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *，配置ACL规则明确的信任网段。
4. 执行命令**rule** [*rule-id*] **deny** [**fragment-type** *fragment-type-name* | **source** { *source-ip-address source-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *，配置ACL规则明确的不信任网段。
5. 执行命令**commit**，提交配置。
6. 执行命令**quit**，返回到系统视图。
7. 执行命令**cpu-defend policy** *policy-number*，创建防攻击策略。
8. 执行命令**whitelist acl** *acl-number*，创建白名单。

   要去使能白名单功能，执行命令**whitelist disable**。
9. 执行命令**car whitelist** { **cir** *cir-value* | **cbs** *cbs-value* } *，配置白名单上送带宽。
10. 执行命令**priority whitelist** { **high** | **middle** | **low** }，配置白名单上送优先级。
11. 执行命令**commit**，提交配置。
12. 执行命令**quit**，退出策略视图。
13. 执行命令**slot** *slotl-number*，进入接口板视图。

14. 执行命令**cpu-defend-policy** *policy-number*，将攻防策略和接口板绑定。

    配置完成防攻击策略后，必须在接口板上应用防攻击策略，本机防攻击功能才能生效

15. 执行命令**commit**，提交配置。

检查加固结果

执行**display current-configuration configuration cpu-defend-policy**命令查看防攻击策略的配置情况。

?.2. CPCAR 配置示例

组网需求

对路由器安全性要求如下：

- 不能出现CPU资源占用率太高，尽可能节约系统资源。
- 防止攻击者通过管理报文管理路由器导致设备脱管。
- 能够记录攻击报文信息用于受攻击时分析定位。
- 丢弃报文时产生告警知会用户干预。

配置思路

采用如下的思路配置本机防攻击的基本功能：

- 收集设备上运行的各种业务涉及的协议，并进行归类，即识别正常要保护协议流量、明确的恶意流量。
- 配置CPU防攻击策略，对上送CPU的流量进行顺序匹配：
  a. 配置TCP/IP攻击防范检查，防止TCP/IP攻击。
  b. 配置应用层联动检查。对上送的报文流量进行应用层联动的带宽检查。
  c. 配置合法流量处理策略。即将正常协议流量和需要保护的流量加入白名单和用户自定义流，如果匹配，保证高优先级，分不同通道、不同带宽上送CPU处理。
  d. 配置非法报文和未知报文处理策略。即对明确的恶意流量或未知流量加入黑名单，如果匹配就直接丢弃，或者设置小带宽、低优先级上送CPU。
  e. 配置攻击溯源功能，当发现有丢弃报文时，攻击溯源功能就记录报文的丢弃情况，方便问题定位和分析。
  f. 打开报文丢弃告警功能。

须知

系统使能TCP SYN泛洪攻击防范功能，此功能优先级高于用户配置的黑名单功能。因此，TCP SYN报文会优先匹配TCP SYN泛洪攻击防范功能的ACL规则，不再匹配用户配置**blacklist acl**命令中指定的ACL规则。

如果用户需要将匹配指定ACL规则的TCP SYN报文匹配到黑名单中，需要先配置命令**undo tcpsyn-flood enable**，去使能对TCP SYN泛洪攻击的防范功能。

去使能TCP SYN泛洪攻击后，未匹配黑名单ACL规则的TCP SYN攻击报文将上送，请谨慎操作。

- 配置管理业务平面防护，保护管理接口（管理业务平面），防止非法用户从非管理接口控制设备或者发起管理报文攻击。

数据准备

说明

本示例所用数据仅供参考，实际组网中配置的数据要求请咨询华为工程师后决定。

表 1-8 Device 涉及到的业务信息

分类	流量内容	优先级	动作策略（单位bps）	备注说明
信任网段	源IP	高	自定义名单1 限速1M	允许访问本设备的信任网段，用ACL 3331过滤
路由协议	BGP	高	自定义名单2 限速512K	用ACL 3332过滤 **说明** 设备支持BGP协议的动态链路保护，对于已经生成链接的协议报文走动态白名单上送。这里限速的是还未生成链接的BGP协议报文。
	LDP	高	自定义名单3 限速512K	LDP协议对端的Peer和直连地址的源IP，用ACL 3333过滤
	OSPF,RIP	高	自定义名单4 限速1M	OSPF协议对端Peer的源IP，用ACL 3334过滤
	ISIS	NA	NA	ISIS是二层协议，这里不涉及ACL
可靠性协议	VRRP	高	自定义名单5 限速1300K	虚拟路由器协议，用ACL 3335过滤
组播协议	PIM	高	自定义名单6 限速1M	用ACL 3336过滤

分类	流量内容	优先级	动作策略（单位bps）	备注说明
	IGMP	高	自定义名单7 限速512K	用ACL 3337过滤
	MSDP	低	自定义名单8 限速512K	用ACL 3338过滤
	保留组播	高	自定义名单9 限速512K	保留组播地址范围段224.0.0.0～224.0.0.255，用ACL3339过滤
	保留广播	低	自定义名单10 限速512K	广播地址255.255.255.255，用ACL3340过滤
访问协议	SSH	中	自定义名单11 限速512K	用ACL 3341过滤
	TELNET **说明** 该协议不安全，建议使用STelnet。			
	FTP **说明** 该协议不安全，建议使用SFTP。	低	自定义名单12 限速512K	用ACL 3342过滤
	TFTP **说明** 该协议不安全，建议使用SFTP。			
网管协议	SNMP	低	自定义名单13 限速1M	用ACL 3343过滤
服务协议	TACACS	低	自定义名单14 限速1M	用ACL 3344过滤
	NTP	低	自定义名单15 限速150K	用ACL 3345过滤
工具协议	ICMP	低	自定义名单16 限速512K	ICMP TTL越限报文、端口不可达报文、响应报文、响应回复报文，用ACL 3346过滤

分类	流量内容	优先级	动作策略（单位bps）	备注说明
	LSPPING	高	自定义名单17限速1M	用ACL 3347过滤
其他	未知协议报文	低	预留512K逃生带宽	用ACL 3348过滤
	攻击报文或非法协议报文(黑名单)	低	黑名单带宽配置为0	用ACL 3330过滤

操作步骤

1. 创建CPU防攻击策略

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceA
   [*HUAWEI] commit
   [~DeviceA] cpu-defend policy 10
   [*DeviceA-cpu-defend-policy-10] commit
   ```

2. 配置TCP/IP攻击防范

   ```
   [*DeviceA-cpu-defend-policy-10] fragment-flood enable
   [*DeviceA-cpu-defend-policy-10] udp-packet-defend enable
   [*DeviceA-cpu-defend-policy-10] abnormal-packet-defend enable
   [*DeviceA-cpu-defend-policy-10] commit
   ```

3. 配置上送CPU报文的匹配顺序

   将上送CPU的报文匹配顺序设置为TCPSYN报文——〉分片报文——〉动态链路保护——〉管理协议ACL——〉白名单——〉用户自定义流——〉黑名单。

   ```
   [~DeviceA-cpu-defend-policy-10] process-sequence tcpsyn-flood fragment-flood dynamic-link-protection management-acl whitelist user-defined-flow blacklist
   [*DeviceA-cpu-defend-policy-10] commit
   ```

4. 配置黑名单的匹配规则

   对于确定的非法用户报文、非法协议报文、攻击报文等设备需要拒绝上送处理的报文，建议将其加入黑名单，配置规则动作为丢弃。使用ACL3330来匹配上述报文。

   ```
   [~DeviceA] acl number 3330
   [*DeviceA-acl-adv-3330] rule deny ip source 10.1.1.0 0.0.0.255
   [*DeviceA-acl-adv-3330] commit
   [~DeviceA-acl-adv-3330] quit
   ```

5. 配置黑名单的动作

   ```
   [~DeviceA] cpu-defend policy 10
   [~DeviceA-cpu-defend-policy-10] blacklist acl 3330
   [*DeviceA-cpu-defend-policy-10] car blacklist cir 0
   [*DeviceA-cpu-defend-policy-10] commit
   ```

6. 配置用户自定义流

   - 信任网段源IP地址加入ACL 3331

     ```
     <DeviceA> system-view
     [~DeviceA] acl number 3331
     [*DeviceA-acl-adv-3331] rule permit ip source 10.1.2.0 0.0.0.255
     [*DeviceA-acl-adv-3331] rule permit ip source 10.1.3.0 0.0.0.255
     [*DeviceA-acl-adv-3331] commit
     [~DeviceA-acl-adv-3331] quit
     ```

   - BGP协议加入ACL 3332。

设备支持bgp协议的动态链路保护，对于已经生成的链接，协议报文走动态白名单上送。这里使用ACL对还未生成链接的bgp peer协议报文进行限速。

```
[~DeviceA] acl number 3332
[*DeviceA-acl-adv-3332] rule permit tcp source 10.12.1.0 0.0.0.255 destination-port eq bgp
[*DeviceA-acl-adv-3332] rule permit tcp source 10.12.1.0 0.0.0.255 source-port eq bgp
[*DeviceA-acl-adv-3332] commit
```

- LDP协议加入ACL 3333

  说明

  LDP协议较BGP协议的建立比较特殊，其不仅依赖于TCP连接，还要依赖UDP来维护邻居关系，不仅涉及建邻居的Peer地址，还涉及到直连端口的IP地址，要分为以下几步进行：

  执行display mpls ldp peer获取对端信息。

```
[*DeviceA-acl-adv-3332] display mpls ldp peer
      LDP Peer Information in Public network
-------------------------------------------------------------------------------
Peer-ID              TransportAddress   DiscoverySource
-------------------------------------------------------------------------------
1.1.1.32:0           1.1.1.32           GigabitEthernet3/0/1
-------------------------------------------------------------------------------
TOTAL: 1 Peer(s) Found.
```

  查看本机直连接口的IP地址。

```
[*DeviceA-GigabitEthernet3/0/1]display this
#
interface GigabitEthernet3/0/1
undo shutdown
ip address 11.11.11.2 255.255.255.0
mpls
mpls ldp
#
```

  本地LDP通过双向Hello报文发现邻居，Hello报文为UDP报文，源地址为本地接口地址，目的地址为组播IP。远端LDP与此类似，只不过目的地址变更为配置的远端对等体地址。首先将邻居Hello报文加入ACL：

```
[~DeviceA] acl number 3333
[*DeviceA-acl-adv-3333] rule permit udp source 11.11.11.1 0 destination-port eq 646
[*DeviceA-acl-adv-3333] rule permit udp source 11.11.11.1 0 source-port eq 646
[*DeviceA-acl-adv-3333] commit
```

  在Hello报文载荷中携带本端LDP传输地址，在使用LDP Hello报文发现邻居并获取对方的传输地址后，设备就开始尝试TCP建立LDP会话，用以传递notification等消息。在TCP交互中，传输地址大的一方发起TCP连接建立请求，目的端口号是646，源端口号随机。实际配置时可以忽略该比较步骤，可以直接添加两条对等ACL：

```
[*DeviceA-acl-adv-3333] rule permit tcp source 1.1.1.32 0 destination-port eq 646
[*DeviceA-acl-adv-3333] rule permit tcp source 1.1.1.32 0 source-port eq 646
[*DeviceA-acl-adv-3333] commit
```


说明

- 如果设备上存在多个LDP邻居，则要按照上述操作对每个Peer地址添加四条ACL规则。
- 对于ACL规则的配置分为精确配置（基于源IP地址+端口号）和简化配置（基于端口号）两种。精确配置的安全程度高，但信息收集复杂。简化配置的安全程度较低，但配置过程简单。用户可以根据自己的实际情况选择配置方式。简化配置过程如下：

```
[~DeviceA-acl-adv-3332] acl number 3333
[*DeviceA-acl-adv-3333] rule permit tcp source-port eq 646
[*DeviceA-acl-adv-3333] rule permit tcp destination-port eq 646
[*DeviceA-acl-adv-3333] rule permit udp source-port eq 646
[*DeviceA-acl-adv-3333] rule permit udp destination-port eq 646
[*DeviceA-acl-adv-3333] commit
```

- OSPF和RIP协议加入ACL 3334

```
[~DeviceA] acl number 3334
```

说明

设备支持OSPF协议的动态链路保护，对于已经生成的链接，协议报文走动态白名单上送。这里使用ACL对还未生成链接的OSPF协议报文进行限速。

```
[*DeviceA-acl-adv-3334] rule 5 permit ospf
[*DeviceA-acl-adv-3334] commit
```

RIP协议的ACL配置方法与OSPF一样，不再赘述。

- VRRP协议加入ACL 3335

说明

VRRP基于IP协议，协议号为112，由于其以对端虚IP地址发送报文，因此以该虚IP地址+协议号加入到ACL中。在设备上通过命令**display vrrp**获取VRRP Peer信息。

```
[~DeviceA] acl number 3335
[*DeviceA-acl-adv-3335] rule permit 112 source 11.11.11.100 0
[*DeviceA-acl-adv-3335] quit
```

说明

- 如果设备上存在多个VRRP邻居，则要按照上述操作对每个VRRP Peer地址添加一条ACL规则。
- 对于ACL规则的配置分为精确配置（基于源IP地址+端口号）和简化配置（基于端口号）两种。精确配置的安全程度高，但信息收集复杂。简化配置的安全程度较低，但配置过程简单。用户可以根据自己的实际情况选择配置方式。简化配置过程如下：

```
[~DeviceA-acl-adv-3335] rule 5 permit 112
[*DeviceA-acl-adv-3335] commit
```

- 组播相关协议

说明

PIM是一种组播协议，其协议号为103。

```
[~DeviceA] acl number 3336
[*DeviceA-acl-adv-3336] rule permit 103
[*DeviceA-acl-adv-3336] quit
[~DeviceA] acl number 3337
[*DeviceA-acl-adv-3337] rule permit igmp
[*DeviceA-acl-adv-3337] commit
[~DeviceA-acl-adv-3337] quit
[~DeviceA] acl number 3338
[*DeviceA-acl-adv-3338] rule permit udp destination-port eq 639
[*DeviceA-acl-adv-3338] rule permit udp source-port eq 639
[*DeviceA-acl-adv-3338] rule permit tcp destination-port eq 639
```

```
[*DeviceA-acl-adv-3338] rule permit tcp source-port eq 639
[*DeviceA-acl-adv-3338] commit
[~DeviceA-acl-adv-3338] quit
```

- 保留组播地址224.0.0.0～224.0.0.255加入ACL 3339。

```
[~DeviceA] acl number 3339
[*DeviceA-acl-adv-3339] rule permit ip destination 224.0.0.0 0.0.0.255
[*DeviceA-acl-adv-3339] commit
[~DeviceA-acl-adv-3339] quit
```

- 保留广播地址255.255.255.255加入ACL3340。

```
[~DeviceA] acl number 3340
[*DeviceA-acl-adv-3340] rule permit ip destination 255.255.255.255 0
[*DeviceA-acl-adv-3340] commit
[~DeviceA-acl-adv-3340] quit
```

- TELNET，SSH协议加入ACL 3341

  说明

  Telnet和SSH协议都是基于TCP的协议，平常用于登录设备，或是研发登录定位，非常重要，因此放入一个单独的ACL中进行保护。设备支持TELNET和SSH协议的动态链路保护，对于已经生成的链接，协议报文走动态白名单上送。这里使用ACL对还未生成链接的TELNET、SSH协议报文进行限速。SSH的端口号为22。管理协议建议直接对未知源的访问流量进行过滤丢弃。

```
[~DeviceA] acl number 3341
[*DeviceA-acl-adv-3341] rule permit tcp source 192.168.1.0 0.0.0.255 source-port eq telnet
[*DeviceA-acl-adv-3341] rule permit tcp source 192.168.1.0 0.0.0.255 destination-port eq
telnet
[*DeviceA-acl-adv-3341] rule permit tcp source 192.168.1.0 0.0.0.255 source-port eq 22
[*DeviceA-acl-adv-3341] rule permit tcp source 192.168.1.0 0.0.0.255 destination-port eq 22
[*DeviceA-acl-adv-3341] quit
[*DeviceA-acl-adv-3341] rule deny tcp destination-port eq telnet
[*DeviceA-acl-adv-3341] rule deny tcp destination-port eq 22
[*DeviceA-acl-adv-3341] commit
```

- FTP/TFTP协议加入ACL 3342

  说明

  FTP基于TCP，而TFTP基于UDP协议，因此每个源地址需要配置三条规则。

```
[~DeviceA] acl number 3342
[*DeviceA-acl-adv-3342] rule permit udp source 192.168.1.0 0.0.0.255 destination-port eq
tftp
[*DeviceA-acl-adv-3342] rule permit tcp source 192.168.1.0 0.0.0.255 source-port eq ftp
[*DeviceA-acl-adv-3342] rule permit tcp source 192.168.1.0 0.0.0.255 destination-port eq ftp
[*DeviceA-acl-adv-3342] quit
```

  说明

  - FTP和TFTP源地址段范围必须获取客户的确认。
  - 对于ACL规则的配置分为精确配置（基于源IP地址+端口号）和简化配置（基于端口号）两种。精确配置的安全程度高，但信息收集复杂。简化配置的安全程度较低，但配置过程简单。用户可以根据自己的实际情况选择配置方式。简化配置过程如下：

```
[*DeviceA-acl-adv-3342] rule permit udp destination-port eq tftp
[*DeviceA-acl-adv-3342] rule permit tcp source-port eq ftp
[*DeviceA-acl-adv-3342] rule permit tcp destination-port eq ftp
[*DeviceA-acl-adv-3342] commit
```

- SNMP协议加入ACL 3343

说明

现网一般都会部署网管功能，网管服务器会发送大量UDP请求报文，设备则以SNMP协议端口号进行回应，由于信息量较大，因此要把这些网管主机加入到一个单独的ACL中加以保护。

加入ACL的网管源地址段必须得到用户的确认，否则会导致漏掉的源IP对应的网管服务器无法管理该设备。SNMP协议为系统管理协议，建议在增加配置直接对未知源的协议报文进行丢弃。

```
[~DeviceA] acl number 3343
[*DeviceA-acl-adv-3343] rule permit udp source 10.20.20.0 0.0.0.255 source-port eq snmp
[*DeviceA-acl-adv-3343] rule permit udp source 10.20.20.0 0.0.0.255 destination-port eq snmp
[*DeviceA-acl-adv-3343] rule deny udp destination-port eq snmp
[*DeviceA-acl-adv-3343] commit
```

- Tacacs协议加入ACL 3344

说明

Tacacs归属于服务类型协议，要注意其包含两种：一种是基于TCP的华为加强Tacacs，另一种是基于UDP的标准Tacacs，建议全部添加。

```
[~DeviceA] acl number 3344
[*DeviceA-acl-adv-3344] rule permit tcp source 5.5.5.5 0 source-port eq tacacs
[*DeviceA-acl-adv-3344] rule permit tcp source 6.6.6.6 0 destination-port eq tacacs
[*DeviceA-acl-adv-3344] rule permit udp source 5.5.5.5 0 source-port eq tacacs-ds
[*DeviceA-acl-adv-3344] rule permit udp source 6.6.6.6 0 destination-port eq tacacs-ds
[*DeviceA-acl-adv-3344] quit
```

说明

- TACACS的源地址段必须获取客户的确认。
- 对于ACL规则的配置分为精确配置（基于源IP地址+端口号）和简化配置（基于端口号）两种。精确配置的安全程度高，但信息收集复杂。简化配置的安全程度较低，但配置过程简单。用户可以根据自己的实际情况选择配置方式。简化配置过程如下：

```
acl number 3344
 rule permit tcp source-port eq tacacs
 rule permit tcp destination-port eq tacacs
 rule permit udp source-port eq tacacs-ds
 rule permit udp destination-port eq tacacs-ds
```

- NTP协议加入ACL 3345

说明

NTP归属于服务类型协议，端口号为123。

```
[~DeviceA] acl number 3345
[*DeviceA-acl-adv-3345] rule permit udp source 172.16.0.0 0.0.255.255 source-port eq 123
[*DeviceA-acl-adv-3345] rule permit udp source 172.16.0.0 0.0.255.255 destination-port eq 123
[*DeviceA-acl-adv-3345] commit
[~DeviceA-acl-adv-3345] quit
```

说明

- NTP的源地址段必须获取客户的确认。
- 对于ACL规则的配置分为精确配置（基于源IP地址+端口号）和简化配置（基于端口号）两种。精确配置的安全程度高，但信息收集复杂。简化配置的安全程度较低，但配置过程简单。用户可以根据自己的实际情况选择配置方式。简化配置过程如下：

```
acl number 3345
 rule permit udp source- port eq 123
 rule permit udp destination- port eq 123
```


- ICMP，Tracert加入ACL 3346

```
[~DeviceA] acl number 3346
[*DeviceA-acl-adv-3346] rule permit icmp icmp-type echo
[*DeviceA-acl-adv-3346] rule permit icmp icmp-type echo-reply
[*DeviceA-acl-adv-3346] rule permit icmp icmp-type ttl-exceeded
[*DeviceA-acl-adv-3346] rule permit icmp icmp-type port-unreachable
[*DeviceA-acl-adv-3346] rule permit icmp icmp-type Fragmentneed-DFset
[*DeviceA-acl-adv-3346] rule permit icmp
[*DeviceA-acl-adv-3346] rule permit udp destination-port range 33434 33678
[*DeviceA-acl-adv-3346] quit
```

- Ping-LSP加入ACL 3347

```
[~DeviceA] acl number 3347
[*DeviceA-acl-adv-3347] rule permit udp destination-port eq 3503
[*DeviceA-acl-adv-3347] commit
[~DeviceA-acl-adv-3347] quit
```

- 未知协议加入ACL 3348

  说明

  如果确认非法协议报文和攻击报文归到了黑名单绑定的ACL3330，并且正常的协议报文及信任网段全部归到了ACL 3331～ACL 3347，其它的协议报文可以认其未知，这些报文用ACL 3348来过滤。对应的用户自定义流将为这些报文配置一定的逃生带宽，以低优先级上送CPU处理。

  这部分配置属于可选项，如果不配置ACL过滤未知报文，这些报文会从设备默认为其指定的上送通道上送CPU处理。必须确认前述的配置已经能够识别所有已知的业务和协议报文，否则不推荐配置此ACL及对应的用户自定义流。

```
[~DeviceA] acl number 3348
[*DeviceA-acl-adv-3348] rule permit udp
[*DeviceA-acl-adv-3348] rule permit tcp
[*DeviceA-acl-adv-3348] rule permit ip
[*DeviceA-acl-adv-3348] commit
[~DeviceA-acl-adv-3348] quit
```

7. 配置用户自定义流及动作

   使用ACL对协议报文归类后，要建立用户自定义流把ACL指定给用户自定义流，让不同的协议报文走不同的上送通道。

   - 配置自定义名单1的动作

     自定义名单1对应的acl为3331，它用来保护允许访问本设备的信任网段；优先级设置为高，带宽为1M，对于访问来说已经足够。

```
[~DeviceA] cpu-defend policy 10
[~DeviceA-cpu-defend-policy-10] user-defined-flow 1 acl 3331
[*DeviceA-cpu-defend-policy-10] car user-defined-flow 1 cir 1000
[*DeviceA-cpu-defend-policy-10] priority user-defined-flow 1 high
```

   - 配置自定义名单2的动作

     自定义名单2对应的acl为3332，用来保护BGP协议；因为是路由协议所以优先级要设置为高；带宽也要得到相应保障，这里设置为512K；并且部署防攻击告警功能。报文丢弃告警阈值和告警时间间隔需要根据实际网络情况进行调整。

```
[*DeviceA-cpu-defend-policy-10] user-defined-flow 2 acl 3332
[*DeviceA-cpu-defend-policy-10] car user-defined-flow 2 cir 512 cbs 1000000
[*DeviceA-cpu-defend-policy-10] priority user-defined-flow 2 high
[*DeviceA-cpu-defend-policy-10] alarm drop-rate user-defined-flow 2 enable
[*DeviceA-cpu-defend-policy-10] alarm drop-rate user-defined-flow 2 threshold 100 interval 60
```

   - 配置自定义名单3的动作

     自定义名单3对应的acl为3333，用来保护LDP协议；优先级设置为高，带宽设置为512K，并且部署防攻击告警功能。报文丢弃告警阈值和告警时间间隔需要根据实际网络情况进行调整。


```
[*DeviceA-cpu-defend-policy-10] user-defined-flow 3 acl 3333
[*DeviceA-cpu-defend-policy-10] car user-defined-flow 3 cir 512 cbs 1000000
[*DeviceA-cpu-defend-policy-10] priority user-defined-flow 3 high
[*DeviceA-cpu-defend-policy-10] alarm drop-rate user-defined-flow 3 enable
[*DeviceA-cpu-defend-policy-10] alarm drop-rate user-defined-flow 3 threshold 100 interval 60
```

说明

LDP协议是最容易发生震荡的协议之一，一般情况下LDP丢包超过3个就有可能发生DOWN，因此配置防攻击告警功能十分有必要。

- 配置自定义名单4的动作

  自定义名单4对应的acl为3334，用来保护OSPF和RIP协议；优先级设置为高，带宽设置为1M，并且部署防攻击告警功能。报文丢弃告警阈值和告警时间间隔需要根据实际网络情况进行调整

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 4 acl 3334
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 4 cir 1000 cbs 1000000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 4 high
  [*DeviceA-cpu-defend-policy-10] alarm drop-rate user-defined-flow 4 enable
  [*DeviceA-cpu-defend-policy-10] alarm drop-rate user-defined-flow 4 threshold 100 interval 60
  ```

- 配置自定义名单5的动作

  自定义名单5对应的acl为3335，用来保护VRRP协议；因为VRRP是一种可靠性协议，优先级设置为高即可,，带宽设置为1.3M。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 5 acl 3335
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 5 cir 1300 cbs 1000000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 5 high
  ```

- 配置自定义名单6的动作

  自定义名单6对应的acl为3336，用来限制PIM协议的上送带宽。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 6 acl 3336
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 6 cir 1000 cbs 1000000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 6 high
  ```

- 配置自定义名单7的动作

  自定义名单7对应的acl为3337，用来限制IGMP协议的上送带宽。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 7 acl 3337
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 7 cir 512 cbs 512000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 7 high
  ```

- 配置自定义名单8的动作

  自定义名单8对应的acl为3338，用来限制MSDP协议的上送带宽。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 8 acl 3338
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 8 cir 512 cbs 512000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 8 low
  ```

- 配置自定义名单9的动作

  自定义名单9对应的acl为3339。因为现网比较容易遭受到利用缺省保留组播地址的攻击，因此这些保留组播单独放到一个ACL中，限制处理带宽为512K，以保护其他协议。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 9 acl 3339
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 9 cir 512 cbs 40000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 9 high
  ```

- 配置自定义名单10的动作

  自定义名单10对应的acl为3340。用来限制目的IP地址为广播地址255.255.255.255的报文上送带宽。限制处理带宽为512Kbps，优先级设置为低，以保护其他协议。


```
[*DeviceA-cpu-defend-policy-10] user-defined-flow 10 acl 3339
[*DeviceA-cpu-defend-policy-10] car user-defined-flow cir 512 cbs 20000
[*DeviceA-cpu-defend-policy-10] priority user-defined-flow 10 low
```

- 配置自定义名单11的动作

  自定义名单11对应的acl为3341，用来保护SSH和Telnet，因为是访问协议类，所需处理带宽较少，不需要实时性，因此一般把这类协议报文设置的优先级为中即可。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 11 acl 3341
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 11 cir 512 cbs 300000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 11 middle
  ```

- 配置自定义名单12的动作

  自定义名单12对应的acl为3342，用来保护FTP和TFTP。优先级设置为低，带宽限为512K即可甚至更小都可以。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 12 acl 3342
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 12 cir 512 cbs 5120
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 12 low
  ```

- 配置自定义名单13的动作

  自定义名单13对应的acl为3343，用来保护SNMP协议。SNMP协议报文量较大，但实时性要求不高，因此优先级设置为低，带宽设为1M。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 13 acl 3343
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 13 cir 1000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 13 low
  ```

- 配置自定义名单14的动作

  自定义名单14对应的acl为3341，用来保护TACACS协议。TACACS协议对实时性要求不高， 因此优先级设置为低，处理带宽设为1M。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 14 acl 3344
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 14 cir 1000 cbs 1000000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 14 low
  ```

- 配置自定义名单15的动作

  自定义名单15对应的acl为3345，用来限制NTP协议的上送带宽。带宽设为150Kbps，优先级设置为低。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 15 acl 3345
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 15 cir 150 cbs 15000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 15 low
  ```

- 配置自定义名单16的动作

  自定义名单16对应的acl为3346，用来保护ICMP协议。ICMP网上使用非常频繁，因此带宽设为512K，优先级设置为低。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 16 acl 3346
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 16 cir 512 cbs 256000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 16 low
  ```

- 配置自定义名单17的动作

  自定义名单17对应的acl为3347，用来保护LSP PING协议。上送带宽和优先级设置成ME设备默认为其指定的上送通道一样，带宽设为1M，优先级设置为高。

  ```
  [*DeviceA-cpu-defend-policy-10] user-defined-flow 17 acl 3347
  [*DeviceA-cpu-defend-policy-10] car user-defined-flow 17 cir 1000 cbs 40000
  [*DeviceA-cpu-defend-policy-10] priority user-defined-flow 17 high
  ```

- 配置自定义名单18的动作

  自定义名单18对应的acl为3348，用来限制未知协议报文的上送带宽。配置此自定义名单之前，务必确认当前设备必须的业务和协议都已全部通过前面的自定义名单进行匹配。否则，不能配置该自定义名单，让未知协议报文走设备默认为其指定的上送通道。


```
[*DeviceA-cpu-defend-policy-10] user-defined-flow 18 acl 3348
[*DeviceA-cpu-defend-policy-10] car user-defined-flow 18 cir 512 cbs 1000000
[*DeviceA-cpu-defend-policy-10] priority user-defined-flow 18 low
[*DeviceA-cpu-defend-policy-10] commit
```

8. 应用防攻击策略

```
[~DeviceA] slot 1
[*DeviceA-slot-1] cpu-defend-policy 10
[*DeviceA-slot-1] commit
[~DeviceA-slot-1] quit
```

配置文件

```
#
 sysname DeviceA
#
cpu-defend policy 10
 blacklist acl 3330
 user-defined-flow 1 acl 3331
 user-defined-flow 2 acl 3332
 user-defined-flow 3 acl 3333
 user-defined-flow 4 acl 3334
 user-defined-flow 5 acl 3335
 user-defined-flow 6 acl 3336
 user-defined-flow 7 acl 3337
 user-defined-flow 8 acl 3338
 user-defined-flow 9 acl 3339
 user-defined-flow 10 acl 3340
 user-defined-flow 11 acl 3341
 user-defined-flow 12 acl 3342
 user-defined-flow 13 acl 3343
 user-defined-flow 14 acl 3344
 user-defined-flow 15 acl 3345
 user-defined-flow 16 acl 3346
 user-defined-flow 17 acl 3347
 user-defined-flow 18 acl 3348
 alarm drop-rate user-defined-flow 2 threshold 100 interval 60
 alarm drop-rate user-defined-flow 3 threshold 100 interval 60
 alarm drop-rate user-defined-flow 4 threshold 100 interval 60
 car blacklist cir 0
 car user-defined-flow 1 cir 1000
 car user-defined-flow 2 cir 512 cbs 1000000
 car user-defined-flow 3 cir 512 cbs 1000000
 car user-defined-flow 4 cir 1000 cbs 1000000
 car user-defined-flow 5 cir 1300 cbs 1000000
 car user-defined-flow 6 cir 1000 cbs 1000000
 car user-defined-flow 7 cir 512 cbs 512000
 car user-defined-flow 8 cir 512 cbs 5120
 car user-defined-flow 9 cir 512 cbs 40000
 car user-defined-flow 10 cir 512
 car user-defined-flow 11 cir 512 cbs 300000
 car user-defined-flow 12 cir 512 cbs 5120
 car user-defined-flow 13 cir 1000
 car user-defined-flow 14 cir 1000 cbs 1000000
 car user-defined-flow 15 cir 150 cbs 15000
 car user-defined-flow 16 cir 512 cbs 256000
 car user-defined-flow 17 cir 1000 cbs 40000
 car user-defined-flow 18 cir 512 cbs 1000000
 priority user-defined-flow 1 high
 priority user-defined-flow 2 high
 priority user-defined-flow 3 high
 priority user-defined-flow 4 high
 priority user-defined-flow 5 high
 priority user-defined-flow 6 high
 priority user-defined-flow 7 high
 priority user-defined-flow 8 low
 priority user-defined-flow 9 high
 priority user-defined-flow 10 low
 priority user-defined-flow 11 middle
 priority user-defined-flow 12 low
```



```
 priority user-defined-flow 13 low
 priority user-defined-flow 14 low
 priority user-defined-flow 15 low
 priority user-defined-flow 16 low
 priority user-defined-flow 17 high
 priority user-defined-flow 18 low
 process-sequence tcpsyn-flood fragment-flood dynamic-link-protection management-acl whitelist user-
defined-flow blacklist
#
acl number 3330
 rule 5 deny ip source 10.1.1.0 0.0.0.255
#
acl number 3331
 rule 5 permit ip source 10.1.2.0 0.0.0.255
 rule 10 permit ip source 10.1.3.0 0.0.0.255
#
acl number 3332
 rule 5 permit tcp  source 10.12.1.0 0.0.0.255 destination-port eq bgp
 rule 10 permit tcp  source 10.12.1.0 0.0.0.255 source-port eq bgp
#
acl number 3333
 rule 5 permit udp source 11.11.11.1 0 destination-port eq 646
 rule 10 permit udp source 11.11.11.1 0 source-port eq 646
 rule 15 permit tcp source 1.1.1.32 0 destination-port eq 646
 rule 20 permit tcp source 1.1.1.32 0 source-port eq 646
#
acl number 3334
 rule 5 permit ospf
#
acl number 3335
 rule 5 permit 112 source 11.11.11.100 0
#
acl number 3336
 rule 5 permit 103
#
acl number 3337
 rule 5 permit igmp
#
acl number 3338
 rule 5 permit udp destination-port eq 639
 rule 10 permit udp source-port eq 639
 rule 15 permit tcp destination-port eq 639
 rule 20 permit tcp source-port eq 639
#
acl number 3339
 rule 5 permit ip destination 224.0.0.0 0.0.0.255
#
acl number 3340
 rule 5 permit ip destination 255.255.255.255 0
#
acl number 3341
 rule 5 permit tcp source 192.168.1.0 0.0.0.255 source-port eq telnet
 rule 10 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq telnet
 rule 15 permit tcp source 192.168.1.0 0.0.0.255 source-port eq 22
 rule 20 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq 22
 rule 100 deny tcp destination-port eq telnet
 rule 105 deny tcp destination-port eq 22
#
acl number 3342
 rule 5 permit udp source 192.168.1.0 0.0.0.255 destination-port eq tftp
 rule 10 permit tcp source 192.168.1.0 0.0.0.255 source-port eq ftp
 rule 15 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq ftp
#
acl number 3343
 rule 5 permit udp source 10.20.20.0 0.0.0.255 source-port eq snmp
 rule 10 permit udp source 10.20.20.0 0.0.0.255 destination-port eq snmp
 rule 100 deny udp destination-port eq snmp
#
acl number 3344
```

```
 rule 5 permit tcp source 5.5.5.5 0 source-port eq tacacs
 rule 10 permit tcp source 6.6.6.6 0 destination-port eq tacacs
 rule 15 permit udp source 5.5.5.5 0 source-port eq tacacs-ds
 rule 20 permit udp source 6.6.6.6 0 destination-port eq tacacs-ds
#
acl number 3345
 rule 5 permit udp source 172.16.0.0 0.0.255.255 source-port eq ntp
 rule 10 permit udp source 172.16.0.0 0.0.255.255 destination-port eq ntp
#
acl number 3346
 rule 5 permit icmp icmp-type echo
 rule 10 permit icmp icmp-type echo-reply
 rule 15 permit icmp icmp-type ttl-exceeded
 rule 20 permit icmp icmp-type port-unreachable
 rule 25 permit icmp icmp-type fragmentneed-DFset
 rule 30 permit icmp
 rule 35 permit udp destination-port range 33434 33678
#
acl number 3347
 rule 5 permit udp destination-port eq 3503
#
acl number 3348
 rule 5 permit udp
 rule 10 permit tcp
 rule 15 permit ip
#
slot 1
 cpu-defend-policy 10
#
return
```

检查加固结果

- 执行命令**display cpu-defend policy** *policy-number*可以查看配置上送CPU报文的过滤规则。
- 执行命令**display cpu-defend car** { **blacklist** | **index** *index* | *protocol* | **user-defined-flow** *flow-id* | **whitelist** } **statistics** [**slot** *slot-id*]可以查看CAR功能丢弃报文的统计信息。

1.1.7.2 Level-2 的安全加固策略（选配）

1.1.7.2.1 管理平面

Telnet

安全策略介绍

- 支持认证

  Telnet Server支持密码认证和AAA认证，只有通过认证的用户才能登录设备，进入命令行界面。AAA认证支持远端认证和本地认证，且远端认证优先。密码采用不可逆方式加密。
- 支持关闭服务

  当开启Telnet Server服务器时，设备将开启Socket侦听，易被攻击者扫描。当不使用Telnet Server时，可以关闭Telnet Server和相应的端口号。
- 支持变更端口号

Telnet Server 23号端口属于知名端口号，易被扫描和攻击。可以修改Telnet Server的端口为私有端口，端口号范围为<23,1025-65535>，减小被扫描攻击的概率。

- 支持ACL

  在用户界面视图（user-interface）可以配置各个VTY通道的ACL过滤规则，通过ACL控制允许登录的客户端IP。不建议用户在此界面下配置ACL过滤规则。

  ACL规则还能配置在Telnet Server上，用于控制允许通过Telnet方式登录到设备的客户端IP。建议用户在Telnet Server上配置ACL规则。

- 支持源接口配置

  可以配置Telnet Server支持的源接口，仅允许用户通过此接口的IP登录设备，限制访问范围，提高设备安全性。

- 支持IPv6源地址配置

  可以配置Telnet Server支持的源IPv6地址，仅允许用户通过此IPv6地址登录设备，限制访问范围，提高设备安全性。

- IP黑名单

  网络攻击者通过发送大量的Telnet请求导致通过临时会话登录的真实用户无法登录。为了避免这种攻击，攻击者的IP地址将会被系统暂时锁定一段时间，一边真实的用户可以正常登录。

- 支持基于CPCAR的泛洪攻击保护配置

  在部署连接互联网公网地址的场景下，设备本身可能会遭受管理控制平面的流量泛洪攻击，对此，可以配置CPU防护策略对设备进行流量攻击防护。

- 支持分段VTY配置

  设备可能遭受拒绝服务式攻击，可以配置分段VTY，用户界面所支持的协议，至少配置一个SSH，不能全为Telnet，所有协议类型或者不配置。

攻击方法介绍

- 端口扫描

  针对设备网端的网络扫描和侦听，尝试获取用户交互报文，由于Telnet是简单密码交互，设备的信息会被窃取。

- 暴力破解密码

  攻击者在侦听到Telnet端口后，尝试进行连接，设备提示认证，则其会进行暴力破解尝试通过认证，获取访问权限。

- 拒绝服务式攻击

  Telnet Server支持的用户数有限，在用户登录达到上限后，其他用户将无法登录。这个可能是正常使用造成，也可能是攻击者造成。

配置维护方法

- 配置认证方式为AAA认证

  说明

  验证方式配置为AAA验证时，必须指定本地用户的接入类型。

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**aaa**，进入AAA视图。

c. 执行命令**local-user** *user-name* **password** [**cipher** *password* | **irreversible-cipher** *irreversible-cipher-password*]，并交互输入密码，配置本地用户名和密码。

d. 执行命令**local-user** *user-name* **service-type telnet**，配置本地用户的接入类型为Telnet。

e. 执行命令**local-user** *user-name* **user-group manage-ug**，配置本地用户具有管理权力。

f. 执行命令**quit**，退出AAA视图。

g. 执行命令**user-interface vty** *first-ui-number* [*last-ui-number*]，进入VTY用户界面视图。

h. 执行命令**authentication-mode aaa**，设置用户验证方式为AAA验证。

i. 执行命令**commit**，提交配置。

- 配置关闭Telnet服务

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**undo telnet** [**ipv6**] **server enable**，关闭Telnet服务。

  c. 执行命令**commit**，提交配置。

- 配置变更端口号为53555

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**telnet server port 53555**，调整端口号为53555。

  c. 执行命令**commit**，提交配置。

- 配置通过ACL设置呼入呼出权限限制

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**acl** { [**number**] *acl-number* | **name** *acl-name* [**advance**] [**number** *acl-number*] } [**match-order** { **auto** | **config** }]，创建一个高级ACL，并进入高级ACL视图。

  说明

  Telnet是基于TCP的协议，用户可使用Telnet协议登录设备，为保证其安全性，建议配置一个单独的ACL中进行保护。设备支持Telnet协议的动态链路保护，对于已经生成的链接，协议报文走动态白名单上送。这里使用ACL对还未生成链接的Telnet协议报文进行限速，管理协议建议直接对未知源的访问流量进行过滤丢弃。

  c. 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } *protocol* [**destination** { *destination-ip-address destination-wildcard* | **any** } | **fragment** | **source** { *source-ip-address source-wildcard* | **any** } | **time-range** *time-name* | **dscp** *dscp* **vpn-instance** *vpn-instance-name*]，配置ACL规则。

  d. 执行命令**quit**，退出ACL视图。

  e. 执行命令**user-interface vty** *first-ui-number* [*last-ui-number*]，进入VTY用户界面视图。

  f. 执行命令**acl** *acl-number* { **inbound** | **outbound** }，配置VTY类型用户界面的呼入呼出限制。

  当需要限制某个地址或地址段的用户登录到路由器时，使用**inbound**。

  当需要限制已经登录的用户登录到其它路由器时，使用**outbound**。

  g. 执行命令**quit**，退出VTY用户界面视图。

h. 执行命令**telnet server acl** { *acl-number* | *acl-name* }，配置允许通过Telnet方式登录到设备的客户端IP地址。

i. 执行命令**commit**，提交配置。

- 配置用户通过指定源接口登录服务器

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**telnet server-source -i loopback** *interface-number*，指定Telnet服务器端的源接口。

说明

指定Telnet服务器端的源接口前，必须已经成功创建LoopBack接口，否则会导致本配置无法成功执行。

c. 执行命令**commit**，提交配置。

- 配置用户通过指定IPv6源地址登录服务器

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**telnet ipv6 server-source -a** *ipv6-address* [**-vpn-instance** *vpn-instance-name*]，指定Telnet服务器端的IPv6源地址。

说明

指定SSH服务器端的VPN实例，必须已经成功创建VPN，否则会导致命令无法执行成功。

c. 执行命令**commit**，提交配置。

- 配置基于CPCAR的泛洪攻击防护

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**acl** { **name** *advance-acl-name* [**advance** | [**advance**] **number** *advance-acl-number*] | [**number**] *advance-acl-number* } [**match-order** { **config** | **auto** }]，创建高级ACL，并进入ACL视图。

说明

Telnet是基于TCP的协议，用户可使用Telnet协议登录设备，为保证其安全性，建议配置一个单独的ACL中进行保护。设备支持Telnet协议的动态链路保护，对于已经生成的链接，协议报文走动态白名单上送。这里使用ACL对还未生成链接的Telnet协议报文进行限速，管理协议建议直接对未知源的访问流量进行过滤丢弃。

c. 执行如下三条命令，配置ACL的规则，允许上送指定源接口地址范围内的Telnet报文，拒绝上送其他Telnet协议报文。

- 执行命令**rule** [*rule-id*] [**name** *rule-name*] **permit tcp source** *source-ip-address source-wildcard* **source-port eq 23**，配置允许上送指定源地址且源接口类型为Telnet的协议报文。
- 执行命令**rule** [*rule-id*] [**name** *rule-name*] **permit tcp source** *source-ip-address source-wildcard* **destination-port eq 23**，配置允许上送指定源地址且目的接口类型为Telnet的协议报文。
- 执行命令**rule** [*rule-id*] [**name** *rule-name*] **deny tcp destination-port eq 23**，配置拒绝上送其他不在白名单范围中的Telnet协议报文。

d. 执行命令**quit**，退出ACL视图。

e. 执行命令**cpu-defend policy** *policy-number*，创建防攻击策略。

f. 执行命令**tcpsyn-flood enable**，使能TCP SYN泛洪攻击防范功能。

g. 执行命令**fragment-flood enable**，使能分片报文攻击防范功能。

h. 执行命令**udp-packet-defend enable**，使能UDP报文的攻击防范功能。

i. 执行命令**abnormal-packet-defend enable**，使能畸形报文的攻击防护功能。

j. 执行命令**user-defined-flow** *flow-id* **acl** { *acl-number* | **name** *acl-name* } [**prior**]，配置用户自定义流，并与ACL相关联。

k. 执行命令**car user-defined-flow** *flow-id* { **cir** *cir-value* | **cbs** *cbs-value* | **min-packet-length** *min-packet-length-value* }，配置用户自定义流中报文的CAR动作规则。

l. 执行命令**priority** { *protocol-name* | **index** *index* | **whitelist** | **whitelist-v6** | **blacklist** | **tcpsyn** | **fragment** | **user-defined-flow** *flow-id* } { **high** | **middle** | **low** | **be** | **af1** | **af2** | **af3** | **af4** | **ef** | **cs6** }，配置上送CPU报文的优先级。

说明

Telnet协议是访问协议，所需的处理带宽较少，实时性要求不高，这里建议将优先级设置为中即可。

m. 执行命令**quit**，退出防攻击策略视图。

n. 执行命令**slot** *slot-id*，进入指定槽位。

o. 执行命令**cpu-defend-policy** *policy-number*，在指定接口板上应用防护攻击策略。

p. 执行命令**commit**，提交配置。

- 配置分段VTY，防止拒绝服务式攻击

  用户界面所支持的协议，至少配置一个SSH，不能全为Telnet，所有协议类型或者不配置。

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**user-interface maximum-vty** *number*，配置VTY登录用户的最大数目。

  c. 执行命令**user-interface vty** *first-ui-number* [*last-ui-number*]，进入VTY用户接口视图。

  d. 执行命令**protocol inbound ssh**，配置用户界面所支持的协议。

  e. 执行命令**quit**，退出VTY用户接口视图视图。

  f. 执行命令**user-interface vty** *first-ui-number* [*last-ui-number*]，进入VTY用户接口视图。

  g. 执行命令**protocol inbound telnet**，配置用户界面所支持的协议。

  h. 执行命令**quit**，退出VTY用户接口视图视图。

  i. 执行命令**commit**，提交配置。

配置维护建议

- 单独规划设备管理的网络IP，防止设备被扫描和窃听。
- 修改Telnet Server端口号。
- 配置ACL策略，限定Telnet允许访问的IP。
- 建议使用SSH替换Telnet，提供安全的管理通道。

检查加固结果

- 执行命令**display current-configuration configuration** aaa，查看AAA的配置情况。
- 执行命令**display telnet server**，查看Telnet服务器的配置信息。
- 执行命令**display cpu-defend policy** *policy-number*，查看防攻击策略信息。

TFTP

安全策略介绍

TFTP协议不支持认证，属于不安全的文件拷贝协议，所以设备仅支持TFTP Client，不支持TFTP Server。

TFTP Client的命令是3级管理级命令，即仅具有管理级权限的用户才有权限操作设备的文件。

攻击方法介绍

N/A

配置维护方法

- 支持ACL

```
[~HUAWEI] acl 2000
[~HUAWEI-acl-basic-2000] display this
#
acl number 2000
 rule 15 permit source 10.1.1.1 0
 rule 20 deny
#
return
[~HUAWEI] tftp-server acl 2000
[*HUAWEI] commit
```

- 支持IPv6 ACL

```
[~HUAWEI] acl ipv6 2001
[~HUAWEI-acl6-basic-2001] display this
#
acl ipv6 number 2001
 rule 5 permit source 2001:db8:1::1/64
 rule 10 deny
#
return
[~HUAWEI-acl6-basic-2001] quit
[~HUAWEI] tftp-server ipv6 acl 2001
[*HUAWEI] commit
```

- 支持源接口配置

```
[~HUAWEI] interface LoopBack 0
[~HUAWEI-LoopBack0] display this
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ipv6 enable
 ip address 10.1.1.1 255.255.255.255
#
return
[~HUAWEI-LoopBack0] quit
[~HUAWEI] tftp client-source -i LoopBack 1
Info: Succeeded in setting the source interface of the TFTP client to LoopBack1.
```



```
[*HUAWEI] commit
```

配置维护建议

TFTP协议不安全，建议使用更安全的SFTP协议。

检查加固结果

执行命令**display tftp-client**，查看设备作为TFTP客户端的配置。

FTP

安全策略介绍

- 支持认证

  FTP Server支持AAA认证，只有通过认证的用户才能登录设备，进行文件相关操作。

- 支持关闭服务

  当开启FTP Server服务器时，设备将开启Socket侦听，易被攻击者扫描。当不使用FTP Server时，可以关闭FTP Server和相应的端口号。

  FTP Server默认关闭。

- 支持变更端口号

  FTP Server 21号端口属于知名端口号，易被扫描和攻击。可以修改FTP Server的端口为私有端口，减小被扫描攻击的概率。

- 支持ACL

  在系统视图可以配置FTP Server的ACL过滤规则，通过ACL控制允许登录的客户端IP。

- 支持源接口配置

  可以配置FTP Server支持的源接口，仅允许用户通过此接口的IP登录设备，限制访问范围，提高设备安全性。

- 支持基于CPCAR的泛洪攻击保护配置

  在部署连接互联网公网地址的场景下，设备本身可能会遭受管理控制平面的流量泛洪攻击，对此，可以配置CPU防护策略对设备进行流量攻击防护。

攻击方法介绍

- 暴力破解密码

  攻击者在侦听到FTP端口后，尝试进行连接，设备提示认证，则其会进行暴力破解尝试通过认证，获取访问权限。

- 拒绝服务式攻击

  FTP Server支持的用户数有限，在用户登录达到上限后，其他用户将无法登录。这个可能是正常使用造成，也可能是攻击者造成。

配置维护方法

- 支持关闭服务

```
<HUAWEI> system-view
[~HUAWEI] undo ftp server
```

```
Warning: The operation will stop the FTP server. Do you want to continue? [Y/N]:y
Info: Succeeded in closing the FTP server.
[*HUAWEI] commit
```

- 支持变更端口号

```
<HUAWEI> system-view
[~HUAWEI] ftp server port 5553
Info: Port change successful. Please start the FTP service.
[*HUAWEI] commit
```

- 支持ACL

```
<HUAWEI> system-view
[~HUAWEI] acl 2000
[*HUAWEI-acl-basic-2000] display this
#
acl number 2000
 rule 15 permit source 10.1.1.1 0
 rule 20 deny
#
return
[*HUAWEI-acl-basic-2000] quit
[*HUAWEI] ftp acl 2000
[*HUAWEI] commit
```

- 支持IPv6 ACL

```
<HUAWEI> system-view
[~HUAWEI] acl ipv6 2001
[*HUAWEI-acl6-basic-2001] display this
#
acl ipv6 number 2001
 rule 5 permit source 2001:db8:1::1/64
 rule 10 deny
#
return
[*HUAWEI-acl6-basic-2001] quit
[*HUAWEI] ftp ipv6 acl 2001
[*HUAWEI] commit
```

- 支持源接口配置

```
<HUAWEI> system-view
[~HUAWEI] interface LoopBack 0
[*HUAWEI-LoopBack0] display this
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 10.1.1.1 255.255.255.255
#
return
[*HUAWEI-LoopBack0] quit
[*HUAWEI] ftp server-source -i loopback 0
Warning: To make the server source configuration take effect, the FTP server will be restarted.
Continue? [Y/N]:Y
Info: Succeeded in setting the source interface of the FTP server to LoopBack0.
Info: Succeeded in starting the FTP secure server.
[*HUAWEI] commit
```

- 支持IPv6源IP配置

```
<HUAWEI> system-view
[~HUAWEI] ftp ipv6 server-source -a 2001:db8:1::1
Warning: To make the server source configuration take effect, the FTP server will be restarted.
Continue? [Y/N]:y
[*HUAWEI] commit
```

- 配置基于CPCAR的泛洪攻击防护

  a. 创建CPU防攻击策略。

  ```
  <HUAWEI> system-view
  [~HUAWEI] cpu-defend policy 10
  [*HUAWEI-cpu-defend-policy-10] commit
  ```


b. 配置TCP/IP攻击防范。

```
[~HUAWEI-cpu-defend-policy-10] tcpsyn-flood enable
[*HUAWEI-cpu-defend-policy-10] fragment-flood enable
[*HUAWEI-cpu-defend-policy-10] udp-packet-defend enable
[*HUAWEI-cpu-defend-policy-10] abnormal-packet-defend enable
[*HUAWEI-cpu-defend-policy-10] quit
[*HUAWEI] commit
```

c. 创建ACL。

创建高级ACL 3341，并配置对FTP协议限制的规则,允许上送指定源接口地址范围内的FTP报文，拒绝上送其他FTP协议报文。

```
[~HUAWEI] acl number 3341
[*HUAWEI-acl-adv-3341] rule permit udp source 192.168.1.0 0.0.0.255 source-port eq ftp
[*HUAWEI-acl-adv-3341] rule permit udp source 192.168.1.0 0.0.0.255 destination-port eq
ftp
[*HUAWEI-acl-adv-3341] rule deny udp destination-port eq ftp
[*HUAWEI-acl-adv-3341] commit
```

d. 创建用户自定义流。

在使用ACL对协议报文归类后，通过应用ACL创建自定义流，使不同的协议报文使用不同的上送通道进行传输。

FTP协议是访问协议，所需的处理带宽较少，实时性要求不高，这里建议将限制带宽设置为512K，优先级设置为低即可。

```
[~HUAWEI] cpu-defend policy 10
[*HUAWEI-cpu-defend-policy-10] user-defined-flow 11 acl 3341
[*HUAWEI-cpu-defend-policy-10] car user-defined-flow 11 cir 512 cbs 5120
[*HUAWEI-cpu-defend-policy-10] priority user-defined-flow 11 low
[*HUAWEI-cpu-defend-policy-10] quit
[*HUAWEI] commit
```

e. 应用防攻击策略。

```
[~HUAWEI] slot 1
[~HUAWEI-slot-1] cpu-defend-policy 10
[*HUAWEI-slot-1] quit
[*HUAWEI] commit
```

配置维护建议

- 当不使用FTP Server的时候，将该服务关闭。
- 当使用FTP Server时，修改其端口号。
- 配置ACL访问控制策略。
- FTP协议不安全，建议使用更安全的SFTP协议。

检查加固结果

- 执行命令**display current-configuration configuration** ftp，查看FTP的配置情况。
- 执行命令**display ftp-server**，查看FTP服务器的状态和配置信息。
- 执行命令**display cpu-defend policy** *policy-number*，查看防攻击策略信息。

SSH 配置双向证书认证进行 NETCONF 连接

安全策略介绍

1. 支持SSH组件与PKI组件之间证书认证请求与证书获取请求交互。
2. SSH收到连接请求时，如果协商出的主机认证方法是证书认证，发送CERT Req消息给PKI组件，获取证书以及对应的KEY文件。

3. 启动定时器，用于在未收到CERT RSP ACK消息时，重发证书请求消息，定时器时间间隔5s，重传3次，认证场景下消息不能一直等待，以防止DOS攻击。
4. 3次超时后，SSH连接断开，记录SSH登录失败的原因为：主机认证，PKI组件未响应。
5. SSH组件收到用户证书认证请求时，给PKI组件发送认证请求消息。
6. 启动定时器，用于在未收到AUTH RSP ACK消息时，重发认证请求消息，定时器时间间隔5s，重传3次，认证场景下消息不能一直等待，以防止DOS攻击。
7. 3次超时后，SSH连接断开, 记录SSH登录失败的原因为：用户认证，PKI组件未响应。

配置维护方法

1. 执行命令**ssh server assign pki** *pki-keyname*，绑定主机证书认证需要的证书来源，需要用到PKI域的用户证书。
2. 执行命令**ssh server publickey x509v3-ssh-rsa**，指定主机认证方法为x509格式的证书认证。
3. 执行命令**ssh user** *user-name* **authentication-type** { **password-x509v3-rsa** | **x509v3-rsa** }，指定SSH用户的认证行策略为x509格式的证书认证。
4. 执行命令**ssh user** *user-name* **assign pki** *pki-name*，指定SSH用户绑定PKI域。
5. 执行命令**commit**，提交配置。

检查加固结果

- 执行命令**display ssh server status**，查看SSH服务器的全局配置信息。
- 执行命令**display ssh server session**，查看SSH服务端的会话连接信息。
- 执行命令**display ssh server-info**，设备作为SSH客户端时，查看与其相连的SSH服务器以及公钥绑定信息。

HWTACACS 用户管理

HWTACACS是在TACACS+基础上进行了功能增强的一种安全协议。该协议与RADIUS协议类似，主要是通过“客户端—服务器”模式与HWTACACS服务器通信来实现多种用户的AAA功能，可用于PPP用户和Login用户的认证、授权和计费。

安全策略介绍

HWTACACS使用TCP协议传输，客户端与HWTACACS服务器之间的交互是通过共享密钥来进行相互认证的，共享密钥不会通过网络传送。另外，会基于共享密钥对报文主体全部进行加密，保证了传输过程中高安全性。

设备上配置的共享密钥默认是通过高强度加密算法保存的。

攻击方法介绍

很少有针对TACACS协议的攻击。

- 攻击者能改变传输报文的内容。目前无法提供完整的报文信息。
- 攻击者能够发现明文形式的TACACS协议报文。因此推荐对报文进行加密。

配置维护方法

对每个HWTACACS组，通过命令**hwtacacs-server shared-key cipher** *key-string*配置共享密钥，该密钥用于对HWTACACS传输的报文进行MD5加密，增加传输安全性。同时配置密钥的时候采用cipher关键字，查看配置的时候显示的是经过加密以后的密钥，增加密钥的安全性。

说明

MD5加密算法安全性低，存在安全风险。

配置维护建议

hwtacacs-server shared-key cipher *key-string*配置对报文体加密的密钥。

检查加固结果

执行命令**display hwtacacs-server template**，查看HWTACACS服务器的配置信息

RADIUS 用户管理

RADIUS（Remote Authentication Dial In User Service，远程认证拨号用户服务协议）是目前使用最广泛、也是最流行的用于实现对远程电话拨号用户的身份认证、授权和计费的协议。Radius基于UDP协议，认证端口号为1812，计费端口号为1813。RADIUS over DTLS基于DTLS协议，认证端口号为2083，计费端口号为2083。RADIUS主要是通过“客户端—服务器”模式与RADIUS服务器通信来实现多种用户的AAA功能。

安全策略介绍

- 支持关闭服务器。
- 支持通过共享秘钥对RADIUS over UDP报文进行认证。

  RADIUS使用UDP协议进行传输。客户端与RADIUS服务器之间的交互是通过共享密钥来进行相互认证的，共享密钥不会通过网络传送。另外，为了减少在不安全的网络中侦听到用户密码的可能性，在客户端和RADIUS服务器之间传送的密码都是基于共享密钥进行了加密的。
- 支持DTLS服务。

  RADIUS over DTLS支持DTLS证书鉴权操作。

攻击方法介绍

- 篡改

  攻击者能改变传输报文的内容。RADIUS over DTLS提供完整性保护，可以防止报文篡改。
- 信息泄露
- 攻击者能够发现明文形式的RADIUS协议报文。密码属性只隐藏在RADIUS的接入请求报文里。RADIUS over DTLS提供身份认证机制，可以防止信息泄露。

配置维护方法

1. 支持关闭RADIUS服务器

```
[~HUAWEI] undo radius enable
[*HUAWEI] commit
```

2. 支持基于服务器组粒度，配置RADIUS over UDP服务器的共享秘钥。

```
[~HUAWEI] radius-server group test
[*HUAWEI-radius-test] radius-server authentication 10.1.1.1 1812 shared-key YsHsjx_202206
[*HUAWEI-radius-test] commit
```

3. 支持基于服务器粒度，配置RADIUS over UDP服务器的共享秘钥。

```
[~HUAWEI] radius-server group test
[*HUAWEI-radius-test] radius-server shared-key YsHsjx_202206
[*HUAWEI-radius-test] commit
```

4. 支持配置RADIUS over DTLS服务器。

   # 配置PKI实体。

```
[~HUAWEI] pki entity entity1
[*HUAWEI-pki-entity-entity1] common-name test
[*HUAWEI-pki-entity-entity1] country CN
[*HUAWEI-pki-entity-entity1] locality HZ
[*HUAWEI-pki-entity-entity1] organization HW
[*HUAWEI-pki-entity-entity1] organization-unit HW
[*HUAWEI-pki-entity-entity1] state ZJ
[*HUAWEI-pki-entity-entity1] commit
[~HUAWEI-pki-entity-entity1] quit
```

   # 创建公私密钥对。

```
[~HUAWEI] rsa pki local-key-pair key1 create
[*HUAWEI] commit
```

   # 配置PKI域。

```
[~HUAWEI] pki domain domain1
[*HUAWEI-pki-domain-domain1] certificate request entity entity1
[*HUAWEI-pki-domain-domain1] pki cmp session session1
[*HUAWEI-pki-domain-domain1-pki-cmp-session-session1] cmp request rsa local-key-pair key1
[*HUAWEI-pki-domain-domain1-pki-cmp-session-session1] commit
[~HUAWEI-pki-domain-domain1-pki-cmp-session-session1] quit
[~HUAWEI-pki-domain-domain1] quit
```

   # 导入本地证书和CA证书，本地证书为root-cert.cer，CA证书为local-cert.cer。

```
[~HUAWEI] pki import-certificate ca domain test filename root-cert.cer
[~HUAWEI] pki import-certificate local domain test filename local-cert.cer
```

   # 配置SSL策略加密算法套。

```
[~HUAWEI] ssl cipher-suite-list suite1
[*HUAWEI-ssl-cipher-suite-suite1] set cipher-suite tls12_ck_ecdhe_rsa_with_aes_128_gcm_sha256
[*HUAWEI-ssl-cipher-suite-suite1] commit
[~HUAWEI-ssl-cipher-suite-suite1] quit
```

   # 配置DTLS策略。

```
[~HUAWEI] dtls policy policy1
[*HUAWEI-dtls-policy-policy1] pki-domain domain1
[*HUAWEI-dtls-policy-policy1] diffie-hellman modulus 2048
[*HUAWEI-dtls-policy-policy1] binding cipher-suite-customization suite1
[*HUAWEI-dtls-policy-policy1] signature algorithm-list rsa-pkcs1-sha256
[*HUAWEI-dtls-policy-policy1] commit
[~HUAWEI-dtls-policy-policy1] quit
```

   # 配置RADIUS over DTLS服务器。

```
[~HUAWEI] radius-server group group1
[*HUAWEI-radius-group1] radius-server authentication 1.1.1.1 dtls-policy policy1 2083
[*HUAWEI-radius-group1] radius-server accounting 1.1.1.1 dtls-policy policy1 2083
[*HUAWEI-radius-group1] commit
```

5. 支持配置RADIUS over DTLS会话的idle-timeout时长。

```
[~HUAWEI] radius-server dtls idle-timeout 120
[*HUAWEI] commit
```


配置维护建议

对于RADIUS over UDP服务器，建议配置复杂的共享秘钥。

对于RADIUS over DTLS服务器，建议使用安全的证书、加密套件、签名算法。

建议使用RADIUS over DTLS服务器。

检查加固结果

执行命令**display radius-server configuration** [**group** *group-name*]，查看RADIUS服务器的配置信息。

gRPC

安全策略介绍

- 支持认证

  gRPC Server支持AAA认证，只有通过认证的用户才能登录设备，进行相关操作，如果用户重复登录暴力破解密码，Server会强行根据密码鉴权超时时间拒绝登录。
- 支持SSL服务

  gRPC Server支持SSL证书鉴权操作。
- 支持关闭服务

  当开启gRPC Server时，设备将开启Socket侦听，易被攻击者扫描。当不使用gRPC Server时，可以关闭gRPC Server和侦听端口号。gRPC Server默认关闭。
- 支持变更端口号

  可以修改gRPC Server的端口为私有端口，减小被扫描攻击的概率。
- 支持ACL

  在系统视图下，可以配置gRPC Server的ACL过滤规则，通过ACL控制允许登录的客户端IP。
- 支持源接口配置

  可以配置gRPC Server支持的源接口，仅允许用户通过此接口的IP登录设备，限制访问范围，提高设备安全性。

攻击方法介绍

- 拒绝服务式攻击

  gRPC Server支持的用户数有限，在用户登录数达到上限后，其他用户将无法登录。这个可能是正常使用者造成，也可能是攻击者造成。

配置维护方法

- 支持关闭服务

  ```
  [~HUAWEI-grpc-server] undo server enable
  [*HUAWEI-grpc-server] commit
  ```
- 支持变更端口号

  ```
  [~HUAWEI-grpc-server] server-port 5000
  [*HUAWEI-grpc-server] commit
  ```
- 支持ACL

```
[~HUAWEI] acl 2000
[~HUAWEI-acl-basic-2000] display this
#
acl number 2000
 rule 15 permit source 10.1.1.1 0
 rule 20 deny
#
return
[~HUAWEI-acl-basic-2000] quit
[~HUAWEI] grpc
[~HUAWEI-grpc] grpc server
[~HUAWEI-grpc-server] acl 2000
[*HUAWEI-grpc-server] commit
```

- 支持源接口、SSL策略和空闲超时时间配置

```
[~HUAWEI] ssl policy huawei2018
[*HUAWEI-ssl-policy-huawei2018] certificate load asn1-cert servercert.der key-pair rsa key-file
serverkey.der
[*HUAWEI-ssl-policy-huawei2018] crl load pem-crl server.pem
[*HUAWEI-ssl-policy-huawei2018] trusted-ca load asn1-ca servercert.der
[*HUAWEI-ssl-policy-huawei2018] commit
[~HUAWEI-ssl-policy-huawei2018] quit
[~HUAWEI] grpc
[~HUAWEI-grpc] grpc server
[~HUAWEI-grpc-server] source-ip 10.1.1.1
[*HUAWEI-grpc-server] ssl-policy huawei2018
[*HUAWEI-grpc-server] ssl-verify peer
[*HUAWEI-grpc-server] idle-timeout 60
[*HUAWEI-grpc-server] display this
 #
 grpc server
  source-ip 10.1.1.1
  server-port 5000
  idle-timeout 60
  ssl-policy huawei2018
  ssl-verify peer
  server enable
#
return
[*HUAWEI-grpc-server] commit
```

检查加固结果

使用**display current-configuration configuration grpc**命令查看gRPC的配置情况。

配置维护建议

- 当不使用gRPC Server时，将该服务关闭。
- 当使用gRPC Server时，修改其端口号。
- 配置ACL访问控制策略。
- 默认使用TLS证书。

网管和 GNE 设备之间 SSL 连接证书有效期查询

通过SSL策略查询命令和安全风险查询命令可查看GNE设备和网管之间建立的SSL安全连接的证书有效期，并根据有效期及时解除风险。

背景信息

DCN特性支持GNE设备和网管之间建立安全SSL连接，同时根据策略指定安全证书，但是安全证书存在有效期，在安全证书有效期过期后会导致网管无法正常管理设备。用户可以通过使用SSL策略查询命令和安全风险查询命令查看证书有效期。

操作步骤

步骤1 在任意视图下，执行命令**display ssl policy** [*policy-name*]，查询当前系统中配置的SSL策略信息。

步骤2 在SSL策略失效时可以通过安全风险查询命令查看证书是否过期，具体请参见安全风险查询。

步骤3 在设备SSL策略证书失效时，请在DCN视图下，执行命令**bind ssl-policy** *ssl-policy-name*，为DCN绑定新的SSL策略。

----结束

操作结果

执行命令**display ssl policy**，查看系统中配置的SSL策略信息。

设置系统主密钥

系统主密钥是设备在传输数据时使用的，设备通过主密钥对数据进行加密，保证数据传输的安全。设备出厂时会存在一个固定的缺省主密钥，在实际网络环境中，缺省主密钥长期使用会存在被盗窃或破解的风险。管理员可以根据需要手工修改主密钥，提高数据的安全。

安全策略介绍

- 支持修改缺省主密钥，手工设置自定义主密钥，提高数据的安全。
- 支持通过清除自定义主密钥将主密钥回退成缺省主密钥。

  说明

  管理员忘记了本设备已配置的自定义主密钥，其他设备无法通过配置相同主密钥来与本设备的加密数据通道互连。此时，设备间的配置文件共享和数据解密将会失败。
- 支持查询主密钥的状态，当前使用的是缺省主密钥，还是自定义主密钥。

攻击方法介绍

攻击者通过分析大量密文破解固定的缺省主密钥，造成设备信息泄露。

配置维护方法

- 设置自定义主密钥

```
<HUAWEI> set master-key
Warning: This operation will automatically save configurations. Are you sure you want to perform it? [Y/N]:y
Enter a new master key:
Confirm the new master key:
Warning: Keep the new master key well.
Enter the user password:
Info: Operating, please wait for a moment.....
Info: Operation succeeded.
```

- 使能系统主密钥的自动更新功能，系统会定期生成新的32位字符串的主密钥。

```
<HUAWEI> systen-view
[HUAWEI] set master-key auto-update interval 5
Warning: If automatic master key update is enabled, the configured master key will be cleared, and the system will automatically generate a master key. The configuration will be automatically saved when the master key is updated. Are you sure you want to continue? [Y/N]:y
```

- 清除历史的系统主密钥
```
<HUAWEI> clear master-key
Warning: This operation will delete all historical master keys. Are you sure you want to perform it? [Y/N]:y
Enter the user password:
Info: Operating, please wait for a moment...done.
Info: Operation succeeded.
```

说明

执行clear master-key命令不能清除历史的缺省的主密钥，仅能清除历史的自动生成的密钥和用户定义的密钥。 清除历史的系统主密钥后，除了当前主密钥下生成的配置文件可以正确解密，其他历史主密钥下生成的配置文件将无法解密。

检查加固结果

执行**display master-key configuration**命令查询主密钥的类型。

配置维护建议

- 建议初始使用设备时设置自定义主密钥，保证数据安全，避免设备敏感信息泄露。
- 建议定期更新自定义主密钥，保证主密钥安全，避免主密钥长期使用被盗窃或破解。

设置弱口令字典

弱口令字典是在设备上加载用户期望的弱口令字典，对设备后续配置的口令进行弱口令匹配校验，不允许创建弱口令，降低设备口令被暴力破解的风险。

安全策略介绍

- 支持加载弱口令字典文件。
- 支持清除弱口令字典文件。
- 支持查询弱口令列表。

攻击方法介绍

攻击者通过攻破设备使用管理员权限后清除弱口令字典。

配置维护方法

- 加载弱口令字典文件
```
<HUAWEI> load security weak-password-dictionary wkpass.txt
```
- 清除弱口令字典文件
```
<HUAWEI> unload security weak-password-dictionary
```

配置维护建议

- 建议用户根据实际使用自动弱口令字典文件上传设备后加载。
- 建议定期更新弱口令字典文件，降低被工具风险。

检查加固结果

执行**display security weak-password-dictionary**命令查询弱口令列表

弱安全算法/协议列表

协议和算法自身的安全性能是不同的，出于安全性考虑，不建议使用弱安全协议和弱安全算法。如果确实需要使用弱安全协议，需安装弱安全协议特性包WEAKEA，具体请参见弱安全协议特性包WEAKEA。如果确实需要使用弱安全算法，需开启弱安全算法，具体请参见弱安全算法关闭。

- 弱安全协议：Telnet、FTP、TFTP、TLS1.0、TLS1.1、DTLS1.0、SSHv1、SNMPv1、SNMPv2c。
- 弱算法列表，如下表所示：

表 1-9 弱算法列表

用途	算法
对称加密	aes-cbc-128
	aes-cbc-192
	aes-cbc-256
	blowfish
	cylink_mek
	des
	2des
	3des
	desx
	rc2
	rc4
	seal
	sm4_cbc
	tea
	2tdea
哈希算法	md2
	md4
	md5
	hmac-md5
	hmac-sha1
	ripemd
	ripemd-128
	sha0

用途	算法
	sha-1
非对称加密	ecies-160
	rsa-512-oaep
	rsa-1024-oaep
数字签名	dsa-1024
	dsa-2048
	ecdsa-160
	rsa-512-pss
	rsa-1024-pss
密钥协商	dh-1024
	ecdh-160

- 基于协议的弱算法列表，如下表所示：

  表 1-10 基于协议的弱算法列表

协议	算法
TLS1.2	tls_dh_dss_with_aes_128_cbc_sha256
	tls_dh_dss_with_aes_128_gcm_sha256
	tls_dh_dss_with_aes_256_cbc_sha256
	tls_dh_dss_with_aes_256_gcm_sha384
	tls_dhe_dss_aes_128_cbc_sha
	tls_dhe_dss_aes_128_cbc_sha256
	tls_dhe_dss_aes_256_cbc_sha
	tls_dhe_dss_aes_256_cbc_sha256
	tls_dhe_dss_with_aes_128_cbc_sha
	tls_dhe_dss_with_aes_128_cbc_sha256
	tls_dhe_dss_with_aes_256_cbc_sha
	tls_dhe_dss_with_aes_256_cbc_sha256
	tls_dhe_psk_with_aes_128_cbc_sha

协议	算法
	tls_dhe_psk_with_aes_128_cbc_sha256
	tls_dhe_psk_with_aes_256_cbc_sha
	tls_dhe_psk_with_aes_256_cbc_sha384
	tls_dhe_rsa_aes_128_cbc_sha
	tls_dhe_rsa_aes_128_cbc_sha256
	tls_dhe_rsa_aes_256_cbc_sha
	tls_dhe_rsa_aes_256_cbc_sha256
	tls_dhe_rsa_with_aes_128_cbc_sha
	tls_dhe_rsa_with_aes_128_cbc_sha256
	tls_dhe_rsa_with_aes_256_cbc_sha
	tls_dhe_rsa_with_aes_256_cbc_sha256
	tls_dh_rsa_with_aes_128_cbc_sha256
	tls_dh_rsa_with_aes_128_gcm_sha256
	tls_dh_rsa_with_aes_256_cbc_sha256
	tls_dh_rsa_with_aes_256_gcm_sha384
	tls_ecdh_ecdsa_with_aes_128_cbc_sha256
	tls_ecdh_ecdsa_with_aes_128_gcm_sha256
	tls_ecdh_ecdsa_with_aes_256_cbc_sha384
	tls_ecdh_ecdsa_with_aes_256_gcm_sha384
	tls_ecdhe_ecdsa_with_aes_128_cbc_sha
	tls_ecdhe_ecdsa_with_aes_128_cbc_sha256
	tls_ecdhe_ecdsa_with_aes_256_cbc_sha

协议	算法
	tls_ecdhe_ecdsa_with_aes_256_cbc_sha384
	tls_ecdhe_psk_with_aes_128_cbc_sha
	tls_ecdhe_psk_with_aes_128_cbc_sha256
	tls_ecdhe_psk_with_aes_256_cbc_sha
	tls_ecdhe_psk_with_aes_256_cbc_sha384
	tls_ecdhe_rsa_with_aes_128_cbc_sha
	tls_ecdhe_rsa_with_aes_128_cbc_sha256
	tls_ecdhe_rsa_with_aes_256_cbc_sha
	tls_ecdhe_rsa_with_aes_256_cbc_sha384
	tls_ecdh_rsa_with_aes_128_cbc_sha256
	tls_ecdh_rsa_with_aes_128_gcm_sha256
	tls_ecdh_rsa_with_aes_256_cbc_sha384
	tls_ecdh_rsa_with_aes_256_gcm_sha384
	tls_psk_with_aes_128_cbc_sha
	tls_psk_with_aes_128_cbc_sha256
	tls_psk_with_aes_256_cbc_sha
	tls_psk_with_aes_256_cbc_sha384
	tls_rsa_aes_128_cbc_sha
	tls_rsa_aes_128_cbc_sha256
	tls_rsa_aes_256_cbc_sha
	tls_rsa_aes_256_cbc_sha256
	tls_rsa_psk_with_aes_128_cbc_sha256
	tls_rsa_psk_with_aes_128_gcm_sha256

协议	算法
	tls_rsa_psk_with_aes_256_cbc_sha384
	tls_rsa_psk_with_aes_256_gcm_sha384
	tls_rsa_with_aes_128_gcm_sha256
	tls_rsa_with_aes_256_gcm_sha384
DTLS1.2	tls_dh_dss_with_aes_128_cbc_sha256
	tls_dh_dss_with_aes_128_gcm_sha256
	tls_dh_dss_with_aes_256_cbc_sha256
	tls_dh_dss_with_aes_256_gcm_sha384
	tls_dhe_dss_with_aes_128_cbc_sha
	tls_dhe_dss_with_aes_128_cbc_sha256
	tls_dhe_dss_with_aes_256_cbc_sha
	tls_dhe_dss_with_aes_256_cbc_sha256
	tls_dhe_psk_with_aes_128_cbc_sha
	tls_dhe_psk_with_aes_128_cbc_sha256
	tls_dhe_psk_with_aes_256_cbc_sha
	tls_dhe_psk_with_aes_256_cbc_sha384
	tls_dhe_rsa_with_aes_128_cbc_sha
	tls_dhe_rsa_with_aes_128_cbc_sha256
	tls_dhe_rsa_with_aes_256_cbc_sha
	tls_dhe_rsa_with_aes_256_cbc_sha256
	tls_dh_rsa_with_aes_128_cbc_sha256
	tls_dh_rsa_with_aes_128_gcm_sha256
	tls_dh_rsa_with_aes_256_cbc_sha256

协议	算法
	tls_dh_rsa_with_aes_256_gcm_sha384
	tls_ecdh_ecdsa_with_aes_128_cbc_sha256
	tls_ecdh_ecdsa_with_aes_128_gcm_sha256
	tls_ecdh_ecdsa_with_aes_256_cbc_sha384
	tls_ecdh_ecdsa_with_aes_256_gcm_sha384
	tls_ecdhe_ecdsa_with_aes_128_cbc_sha
	tls_ecdhe_ecdsa_with_aes_128_cbc_sha256
	tls_ecdhe_ecdsa_with_aes_256_cbc_sha
	tls_ecdhe_ecdsa_with_aes_256_cbc_sha384
	tls_ecdhe_psk_with_aes_128_cbc_sha
	tls_ecdhe_psk_with_aes_128_cbc_sha256
	tls_ecdhe_psk_with_aes_256_cbc_sha
	tls_ecdhe_psk_with_aes_256_cbc_sha384
	tls_ecdhe_rsa_with_aes_128_cbc_sha
	tls_ecdhe_rsa_with_aes_128_cbc_sha256
	tls_ecdhe_rsa_with_aes_256_cbc_sha
	tls_ecdhe_rsa_with_aes_256_cbc_sha384
	tls_ecdh_rsa_with_aes_128_cbc_sha256
	tls_ecdh_rsa_with_aes_128_gcm_sha256
	tls_ecdh_rsa_with_aes_256_cbc_sha384

协议	算法
	tls_ecdh_rsa_with_aes_256_gcm_sha384
	tls_psk_with_aes_128_cbc_sha
	tls_psk_with_aes_128_cbc_sha256
	tls_psk_with_aes_256_cbc_sha
	tls_psk_with_aes_256_cbc_sha384
	tls_rsa_psk_with_aes_128_cbc_sha256
	tls_rsa_psk_with_aes_128_gcm_sha256
	tls_rsa_psk_with_aes_256_cbc_sha384
	tls_rsa_psk_with_aes_256_gcm_sha384
SSH2.0	3des_cbc
	aes128-cbc
	aes192-cbc
	aes256-cbc
	blowfish_cbc
	des_cbc
	dh_group1_sha1
	dh_group_exchange_sha1
	diffie-hellman-group14-sha1
	dsa_2048
	hmac-sha1
	hmac-sha1-etm@openssh.com
	md5
	md5_96
	pgp-sign-dss
	pgp-sign-rsa
	rc4_128
	rc4_256

协议	算法
	rsa2048-sha256
	sha1_96
	sha2_256_96
	sm2kep-sha2-nistp256
	sm4_cbc
	ssh-rsa
	ssh-rsa-cert-v01@openssh.com
SNMPV3	3des168
	des56
	md5
	sha
	sha2-224
NTP	md5
RADIUS	md5

弱安全协议特性包 WEAKEA

简介

由于协议自身的安全性能不同，用户配置时使用的某些协议可能存在安全风险。出于安全性考虑，不建议使用不安全协议，如果确实需要使用，需安装弱安全协议特性包WEAKEA。设备默认自带弱安全协议特性包WEAKEA。

操作步骤

- 安装弱安全协议特性包WEAKEA。
  install feature-software WEAKEA
- 卸载弱安全协议特性包WEAKEA。
  uninstall feature-software WEAKEA

说明

FTP协议本身存在安全风险，建议使用SFTP安全协议。

如系统中有弱安全协议相关的配置，系统会提示弱安全协议特性包卸载失败，此时需要先删除弱安全协议相关的配置（多VS场景需要删除每个VS下的弱协议配置）。

- 可以执行**display security risk type insecure-protocol**查询弱协议信息，根据弱协议相关的配置，执行删除弱协议配置操作。
- 可以执行**display security risk type insecure-algorithm**查询弱算法信息，根据弱算法相关的配置，执行删除弱算法配置操作。

弱安全协议特性包WEAKEA卸载后，如需要使用即插即用功能，请使用安全协议。

----结束

任务示例

安装和卸载弱安全协议特性包WEAKEA的样例如下。

- 样例一：未安装弱安全协议特性包WEAKEA时，开启设备的FTP功能失败，安装弱安全协议特性包WEAKEA后，再开启设备的FTP功能成功。

  # 开启设备的FTP功能失败。

  ```
  <HUAWEI> system-view
  [~HUAWEI]ftp server enable
  Error: This protocol is insecure. To use it, please execute the commond "install feature-software WEAKEA".
  ```

  # 执行安装WEAKEA包命令。

  ```
  <HUAWEI> install feature-software WEAKEA
  Info: Operating, please wait for a moment.....done.
  Info: Succeeded in installing the software.
  ```

  # 重新开启设备的FTP功能成功。

  ```
  <HUAWEI> system-view
  [~HUAWEI] ftp server enable
  [*HUAWEI] commit
  [*HUAWEI] quit
  ```

- 样例二：系统中有弱协议相关的配置时，执行卸载弱安全协议特性包WEAKEA操作失败。删除弱协议配置后，再执行卸载弱安全协议特性包WEAKEA操作成功。

  # 系统中有弱协议相关的配置时，执行卸载WEAKEA包命令，操作失败。

  ```
  <HUAWEI> uninstall feature-software WEAKEA
  Warning: This will uninstall the package WEAKEA, Continue? [Y/N]:Y
  Info: Operating, please wait for a moment...
  Error: WEAKEA feature-related configurations are running in the system. Delete those configurations before performing this operation.
  Error: Failed to check before uninstalling the feature software package.
  ```

  # 关闭设备的FTP功能。

  ```
  <HUAWEI> system-view
  [~HUAWEI] undo ftp server
  [*HUAWEI] commit
  [*HUAWEI] quit
  ```

  # 再执行卸载WEAKEA包命令，操作成功。

  ```
  <HUAWEI> uninstall feature-software WEAKEA
  Warning: This will uninstall the package WEAKEA, Continue? [Y/N]:Y
  Info: Operating, please wait for a moment.....done.
  Info: Succeeded in uninstalling the software.
  ```


检查加固结果

执行命令**display startup**或**display startup feature-software**，查看显示信息是否与用户所需特性包名称一致。

弱安全算法关闭

简介

由于算法自身的安全性能不同，用户配置时使用的某些算法可能存在安全风险。出于安全性考虑，不建议使用弱安全算法，为避免风险，设备提供了弱安全算法去使能功能。用户可以通过配置弱安全算法去使能 ，减少误操作等导致的安全风险。在缺省情况下，设备默认开启弱安全算法。

操作步骤

- 去使能弱安全算法

  crypto weak-algorithm disable

- 使能弱安全算法。

  undo crypto weak-algorithm disable

----结束

任务示例

说明

FTP协议本身存在安全风险，建议使用SFTP安全协议。

- 去使能弱安全算法。

  # 当SSH特性HMAC认证算法使用了弱安全算法时，执行去使能命令失败。

  ```
  <HUAWEI> system-view
  [~HUAWEI] ssh server hmac md5
  [*HUAWEI] commit
  [~HUAWEI] crypto weak-algorithm disable
  Error: The weak algorithm is currently in use by (SSHC,SSHS).
  ```

  # 当SSH特性HMAC认证算法改为默认的安全性更高的算法时，执行去使能命令成功。

  ```
  [~HUAWEI] undo ssh server hmac md5
  [*HUAWEI] commit
  [~HUAWEI] crypto weak-algorithm disable
  [*HUAWEI] commit
  ```

  # 去使能弱安全算法后，再配置弱安全算法时失败。

  ```
  [~HUAWEI] ssh server hmac md5
  Error: This algorithm is insecure. To use it, please execute the command "undo crypto weak-algorithm disable".
  ```

- 使能弱安全算法。

  # 当弱安全算法去使能情况下，想使用弱安全，可以执行使能弱安全算法的命令行。

  ```
  <HUAWEI> system-view
  [~HUAWEI] ssh server hmac md5
  Error: This algorithm is insecure. To use it, please execute the command "undo crypto weak-algorithm disable".
  [~HUAWEI] undo crypto weak-algorithm disable
  [*HUAWEI] commit
  ```

  # 执行使能弱算法命令行后，再配置弱安全算法时成功。


```
[~HUAWEI] ssh server hmac md5
[*HUAWEI] commit
```

设置 DCN 接口的 OSPF 验证模式

安全策略介绍

OSPF/OSPFv3支持报文验证功能，只有通过验证的报文才能接收，否则将不能正常建立邻居关系。使用区域验证时，一个区域中所有的路由器在该区域下的验证模式和口令必须一致。接口验证方式用于在相邻的路由器之间设置验证模式和口令，优先级高于区域验证方式。

DCN Serial接口默认会运行OSPF协议，在对安全性要求较高的网络中，可在DCN Serial接口上设置相邻路由器之间的OSPF验证模式及验证字提高网络的安全性。

攻击方法介绍

网络上对OSPF协议的攻击方法主要为伪造报文攻击，可以通过配置报文认证手段来识别并丢弃这些报文。

可能的攻击手段有：

- 修改报文老化时间到最大老化时间，导致所有路由器废弃这个报文。
- 发布合法的Max Sequence Number的LSA或者接近Max Seq Num的报文。
- 邻居路由器重启时复位其加密序列号状态的时机，更改序列号。
- 修改Hello报文中的邻居列表。

配置维护方法

- DCN Serial接口OSPF认证。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**dcn**，动态生成DCN Serial接口。
  d. 请根据需求，配置DCN Serial接口OSPF验证方式。
     - 执行命令**dcn ospf authentication-mode simple** [[**plain**] *plain-text* | [**cipher**] *cipher-text*]，配置DCN Serial接口的OSPF协议验证模式（简单验证）。
     - 执行命令**dcn ospf authentication-mode** { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }]，配置DCN Serial接口的OSPF协议密文验证模式。
     - 执行命令**dcn ospf authentication-mode keychain** *keychain-name*，配置DCN Serial接口的OSPF协议Keychain验证模式。

       说明

       使用Keychain验证模式，需要首先通过**keychain**命令创建一个keychain，并分别通过**key-id**、**key-string**和**algorithm**命令配置该keychain采用的key-id、密码及其认证算法，否则会造成OSPF认证始终为失败状态。

       为了保证更好的安全性，建议不要使用MD5和HMAC-MD5算法，如需配置，需执行**undo crypto weak-algorithm disable**命令使能弱安全算法功能。为避免安全风险，建议使用HMAC-SHA256算法。

- 执行命令**dcn ospf authentication-mode null**，不对DCN Serial接口的OSPF协议进行验证。

e. 执行命令**commit**，提交配置。

检查加固结果

执行命令**display ospf peer**，查看DCN Serial接口的建立的OSPF邻居信息。

设置 QX 服务只运行在 NEIP 上

安全策略介绍

QX是主机软件与网关之间自定义的应用层协议。利用QX的报文格式和机制，GNE可以将从控制平面收到的报文转发到管理平面。同时通过为NE和GNE上的APP协议提供一套接口和机制，使管理平面的APP和控制平面的网管能够相互通信。

如果QX服务运行在所有接口上，即QX报文监听端口的本端地址是任意地址，存在安全风险。一般情况下，网管使用NEIP连接网元，因此建议用户配置**qx server all interface disable**命令，使QX业务只运行在NEIP上，降低安全风险。

攻击方法介绍

攻击者通过构造任意目的地址的非法QX报文对设备进行暴力攻击，消耗系统资源，影响正常的QX服务。

配置维护方法

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**dcn**，进入DCN视图。
3. 执行命令**qx server all-interface disable**，设置QX服务只运行在NEIP上。
4. 执行命令**commit**，提交配置。

检查加固结果

执行命令**display tcp status**查看IPv4的TCP连接状态，命令回显中5432端口的local Addr显示为设备的NEIP地址。

执行命令**display udp status**查看IPv4的UDP连接状态，命令回显中1400和1500端口的local Addr显示为设备的NEIP地址。

1.1.7.2.2 控制平面

ARP

?.1. ARP 欺骗攻击

安全策略介绍

采用ARP欺骗防攻击可以防止恶意用户仿冒其他用户进行ARP攻击，防止恶意用户仿冒网关进行攻击，防止恶意用户构造畸形ARP报文攻击。

- ARP表项严格学习

  设备仅学习本端发送的ARP请求报文的应答报文，并不学习其它设备向路由器发送的ARP请求报文和非本端发送的ARP请求报文的应答报文。可以拒绝掉ARP请求报文攻击和非自己发送的ARP请求报文对应的应答报文攻击，有效防止恶意用户仿冒其他用户或者网关对网络或者网络设备的攻击。

- ARP报文合法性检测

  设备收到ARP报文时，对以太报文头中的源、目的MAC地址和ARP报文数据区中的源、目的MAC地址进行一致性检查。如果以太报文头中的源、目的MAC地址和ARP报文数据区中的源、目的MAC地址不一致，则直接丢弃该ARP报文。可以有效防止恶意用户通过构造畸形ARP报文对网络或者网络设备的攻击。

攻击方法介绍

ARP欺骗指恶意用户通过发送伪造的ARP报文，恶意修改网关或网络内其他主机的ARP表项，造成用户或网络的报文转发异常。

- 恶意用户仿冒其他用户向网关发送ARP报文，导致网关学习到错误的用户ARP表项。
- 恶意用户仿冒网关发出ARP报文，使网络中其他用户学习到错误的网关ARP表项。
- 恶意用户通过构造畸形的ARP报文进行攻击，可导致设备学习到错误的ARP表项，从而影响业务。

配置维护方法

- **配置ARP表项严格学习**

  ARP表项严格学习既可以基于全局，也可以基于指定的接口配置，两者有如下的关系：

  - 当全局和接口同时配置了ARP严格学习功能时，采用接口下配置的策略。
  - 当接口下没有配置ARP严格学习功能时，采用全局下配置的ARP严格学习策略。

  使能全局的ARP表项严格学习功能。

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp learning strict
  ```

  使能指定接口的ARP表项严格学习功能。

  ```
  <HUAWEI> system-view
  [~HUAWEI] interface gigabitethernet 2/0/3
  [~HUAWEI-GigabitEthernet2/0/3] arp learning strict force-enable
  ```

- **配置ARP报文合法性检测**

  ARP报文合法性检测既可以只检测源MAC地址或者目的地址，也可以同时检测源MAC地址和目的MAC地址，选取原则如下：

  - 选择参数**source-mac**：
    - 当接口收到ARP请求报文时，对报文中的源MAC地址进行一致性检查。

- 当接口收到ARP应答报文时，只对报文中的源MAC地址进行一致性检查。

– 选择参数**destination-mac**：

- 当接口收到ARP请求报文时，不对报文进行一致性检查。
  因为ARP请求报文是广播报文，故无需检查。
- 当接口收到ARP应答报文时，对报文中的目的MAC地址进行一致性检查。

– 选择参数**source-mac**和**destination-mac**：

- 当接口收到ARP请求报文时，只对报文中的源MAC地址进行一致性检查。
- 当接口收到ARP应答报文时，对报文中的源、目的MAC地址都进行一致性检查。

使能指定接口的ARP报文合法性检测功能。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet 1/0/1
[~HUAWEI-GigabitEthernet1/0/1] arp validate source-mac destination-mac
```

配置维护建议

对于多端口VLANIF场景，由于网络拓扑变化可能导致用户在不同端口间迁移，一旦迁移将可能导致下行流量不通。因此建议该场景下配置静态ARP时，即不指定ARP表项的出端口，出端口信息可以由ARP报文学习到。

如果恶意用户长期存在，需要人工进行干预，设备自身发送免费ARP只能对攻击起到抑制作用，会导致用户业务时断时通，网络质量下降。

有些场景下有学习组播MAC的ARP表项的应用，配置时需要区分场景进行分析。

检查加固结果

使用**display arp learning strict**命令查看ARP表项严格学习的情况。

使用**display arp-limit** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]命令查看ARP表项限制的配置情况。

使用**display arp speed-limit** { **destination-ip** | **source-ip** } [**slot** *slot-id*]命令查看对ARP报文限速的配置情况。

?.2. ARP 泛洪攻击

安全策略介绍

通过ARP表项限制、ARP速率抑制、ARP表项严格学习，可以有效防止ARP报文泛洪攻击。

- ARP表项限制
  设备基于接口限制学习ARP表项的总数目，可以有效地防止ARP表项溢出，保证ARP表项的安全性。
- ARP速率抑制

设备对单位时间内收到的ARP报文进行数量统计，如果ARP报文的数量超过了配置的阈值，超出部分的ARP报文将被忽略，设备不作任何处理，有效防止ARP表项溢出。

- ARP表项严格学习

  设备仅学习本端发送的ARP请求报文的应答报文，并不学习其它设备向路由器发送的ARP请求报文和非本端发送的ARP请求报文的应答报文，可以拒绝掉ARP请求报文攻击和非自己发送的ARP请求报文对应的应答报文攻击。

配置假表项老化时间，采用ARP惩罚机制防止不可解析的IP报文攻击。即在ARP假表项的老化超时时间内，设备对收到的不可解析的IP报文不再进行处理，避免设备遭受攻击。

ARP学习时，判断系统占用内存的比例，防止ARP内存资源耗尽。

攻击方法介绍

恶意用户发送大量的ARP报文，侵占设备ARP表项资源，从而使正常用户业务受到影响。

设备在转发IP报文时，如果下一跳IP没有对应的ARP表项，需要发送ARP请求对该下一跳IP进行学习，指定转发。恶意用户利用这一点，发送大量的IP地址不可达报文对设备进行攻击。

通过学习大量的ARP表项，导致系统资源耗尽，严重时导致设备重启。

- ARP请求泛洪攻击

  攻击者连续向目的主机发送大量伪造的源IP和MAC地址的ARP请求，占用整个设备的ARP表项，并导致设备CPU升高，导致目的主机瘫痪，无法处理合法的ARP报文，导致DOS攻击。

  说明

  攻击者通过伪造大量源IP地址或MAC变化的ARP报文，连续向目的主机发送大量的ARP请求。目的主机就需要不断的响应ARP请求报文，并刷新本地的ARP表项。ARP表项需要占用系统资源，同时为了保证查找ARP表效率的要求，一般网络设备或者主机会限制ARP表的大小，攻击者就会利用这一点，通过伪造大量源IP地址变化的ARP报文，占满设备ARP表，这样如果此时有合法用户的ARP报文上来，也就不能生成有效的ARP表项，导致正常通信中断。达成DOS攻击目的。

- ARP响应泛洪攻击

  攻击者以非常高的速度进行ARP响应，通过不断刷新目的主机ARP缓存中目的IP和MAC地址的映射关系，从而使目的主机的正常通信受到干扰，间接达到DOS攻击效果。

  说明

  一般情况下，子网中的主机的ARP缓存中都存有子网网关IP地址及其MAC地址的映射关系，即ARP表。攻击者模拟“受害者”-子网网关（或在同一子网的另外一台主机），以ARP广播报文的形式发送错误的MAC地址给其他主机或设备，使得子网内所有设备的ARP表中“受害者”的MAC地址都是错误的，最终子网内设备都无法和“受害者”设备通信，间接达到DOS的目的。

配置维护方法

- **配置ARP表项限制**

  基于接口配置接口能够学些到的ARP表项的阈值，超出部分的表项将无法生成，避免ARP表项溢出。

配置指定接口最多可以学习到的ARP表项数量。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-GigabitEthernet1/0/0] arp-limit maximum 20
```

- **配置ARP速率抑制**

  基于全局配置设备在单位时间内能够处理的ARP报文的阈值，超出部分的ARP报文将直接被设备丢弃，避免ARP表项溢出。

  ARP速率抑制既可以基于源IP地址，也可以基于目的IP地址，选取原则如下：

  - 选择**source-ip**，则基于源IP地址进行ARP速率限制。
  - 选择**destination-ip**，则基于目的IP地址进行ARP速率限制。

  对ARP报文采用基于目的IP地址进行时间戳抑制，速率为每秒50个ARP报文。

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp speed-limit destination-ip maximum 50
  ```

- **配置ARP表项严格学习**

  ARP表项严格学习既可以基于全局，也可以基于指定的接口配置，两者有如下的关系：

  - 当全局和接口同时配置了ARP严格学习功能时，采用接口下配置的策略。
  - 当接口下没有配置ARP严格学习功能时，采用全局下配置的ARP严格学习策略。

  使能全局的ARP表项严格学习功能。

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp learning strict
  ```

  使能指定接口的ARP表项严格学习功能。

  ```
  <HUAWEI> system-view
  [~HUAWEI] interface gigabitethernet 2/0/3
  [~HUAWEI-GigabitEthernet2/0/3] arp learning strict force-enable
  ```

加长ARP假表项的老化时间（默认5秒），可能对正常的业务收敛产生影响。建议一般情况下利用系统内部默认的ARP假表项动态惩罚机制。

设置指定接口的动态ARP假表项超时时间为10秒。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-GigabitEthernet1/0/0] arp-fake expire-time 10
```

如果在内存占用率很高时用户流量不通，可查看下ARP表项是否学习到。

配置维护建议

配置多个维度的ARP表项、速率限制会导致ARP学习速率稍有降低。

加长ARP假表项的老化时间（默认5秒），可能对正常的业务收敛产生影响。建议一般情况下利用系统内部默认的ARP假表项动态惩罚机制。

如果在内存占用率很高时用户流量不通，可查看下ARP表项是否学习到。

检查加固结果

使用**display arp learning strict**命令查看ARP表项严格学习的情况。

使用**display arp-limit** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]命令查看ARP表项限制的配置情况。

使用**display arp speed-limit** { **destination-ip** | **source-ip** } [**slot** *slot-id*]命令查看对ARP报文限速的配置情况。

?.3. 大规格 Q 对接口下 ARP 广播报文复制

安全策略介绍

- 订阅DHCP Relay用户信息指定VLAN发送报文

  DHCP Relay存放了上线用户的VLAN信息，当接口下MISS触发ARP发送广播请求报文时，如果存在DHCP Relay用户就只在指定的VLAN内发送广播报文，不在其他VLAN下进行复制。

- 对于大Q对的接口增加假表项的惩罚步长以及最大老化时间

  接口Q对超过4K，接口下MISS持续触发ARP发送广播请求时，每次生成假表项的老化时间以15秒的步长递增，最长老化时间为3分钟。

- 控制单板发包速率

  接口Q对超过64，当接口下发ARP广播报文的时，ARP根据HAL复制能力分段携带VLAN信息给HAL进行复制，整体控制单板的ARP广播报文发送速率，最大值为每秒30000个报文。

攻击方法介绍

三层终结子接口配置大规格Q对，打IP流量持续触发接口发送ARP广播请求报文。ARP广播报文会在接口配置的所有Q对下进行复制，原先的一份报文可能被复制成上万份（依赖接口配置Q对个数）。

ARP广播报文在复制时会大量消耗系统CPU资源，导致其他业务受到影响。

配置维护方法

配置ARP发包速率

基于全局配置ARP发包速率，默认为500个报文每秒。配置后最大发包速率受到限制，多余的报文会缓存发送。

```
<HUAWEI> system-view
[~HUAWEI] arp broadcast-send maximum 500
```

配置维护建议

当设备上有接口配置大规格Q对后，持续发送ARP广播报文时，可以根据设备CPU的消耗情况调整发包速率。对于缓存满后发不出去的报文可以通过pads查看到丢弃统计。

检查加固结果

使用**display arp** 命令查看ARP表项情况。

IPv4 协议栈

?.1. GTSM

安全策略介绍

GTSM（Generalized TTL Security Mechanism），即通用TTL安全保护机制，保护建立在TCP/IP基础上的控制层面协议免受CPU过载攻击。

当前支持GTSM的协议有BGP，BGP4+，OSPF，OSPFv3，RIP，LDP：

- BGP/BGP4+策略基于邻居粒度，建立多少BGP的邻居，可以启用相应的GTSM策略。
- OSPF/OSPFv3支持协议粒度。公网只能有一种GTSM的策略，私网基于VPN实例的策略，每个OSPF VPN均可以配置相应的GTSM策略。
- LDP GTSM基于邻居粒度，建立多少LDP邻居，可以启用相应数目的GTSM策略。
- RIP支持协议粒度。公网只能有一种GTSM的策略，私网基于VPN实例的策略，每个RIP VPN均可以配置相应的GTSM策略。

业务模块配置GTSM命令后生成GTSM策略，不同协议的策略匹配条件不同。

- BGP/BGP4+的GTSM策略匹配条件：源地址、VRF索引，源端口或目的端口号。
- OSPF/OSPFv3的GTSM策略匹配条件：VRF索引。
- LDP的GTSM策略匹配条件：源地址、源端口或目的端口。
- RIP的GTSM策略匹配条件：VRF索引。

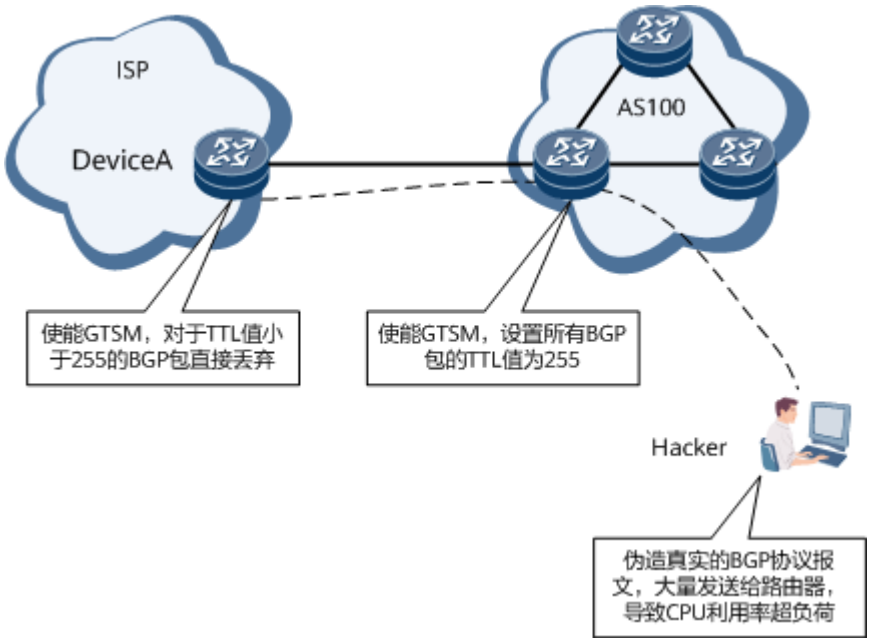
GTSM策略应用：

- 如果设备没有使能协议的GTSM功能，报文直接上送控制层面。
- 如果设备使能了协议的GTSM功能，首先进行GTSM策略匹配，如果匹配了GTSM策略，再判断报文的TTL是否在策略允许的范围内，超过则认为是攻击报文，丢弃。

攻击方法介绍

攻击者模拟真实的路由协议，对一台设备不断发送报文，导致设备因处理这些“合法”报文（攻击报文）而使系统异常繁忙，CPU占用率过高。为了避免CPU过载，采用GTSM策略，通过检查IP报文头中的TTL值是否在一个预先定义好的范围内以实现对采用IP转发的业务进行保护。

图 1-5 安全攻击



配置维护方法

以BGP为例，要求收到报文的TTL范围为[255,255]：

```
[~DeviceA] bgp 10
[*DeviceA-bgp] peer 10.1.1.2 valid-ttl-hops 1
[*DeviceA-bgp] commit
[~DeviceA-bgp] quit
```

检查加固结果

执行命令**display gtsm statistics all**，可以查看GTSM的统计信息，包括报文总数、通过的报文数量、丢弃的报文数量。例如：

```
<~DeviceA> display gtsm statistics all
GTSM Statistics Table
------------------------------------------------------------------
SlotId  Protocol   Total Counters  Drop Counters  Pass Counters
------------------------------------------------------------------
2       BGP                18             0             18
2       BGPv6               0             0              0
2       OSPF                0             0              0
2       LDP                 0             0              0
2       OSPFv3              0             0              0
2       RIP                 0             0              0
------------------------------------------------------------------
```

配置维护建议

适用小型网络，需要在整个网络部署GTSM策略才能达到防攻击效果。

?.2. 应用层联动

安全策略介绍

控制平面与转发平面联动，严格控制非法报文，减少因设备漏洞造成的攻击，保护设备控制转发安全；控制层面感知协议变化，统一处理变化特征，建立特征状态表并通知转发平面。

协议开关：提供灵活的三级安全策略配置，支持接口级、板级、全局三级策略应用，未开启协议开关的报文，丢弃或小带宽上送；可以保证CPU的资源不被耗尽，保证网络的正常运行。

白名单：协议动态session保护，一旦session连接成功（TCP或UDP），设备动态下发该协议的白名单，产品保证大带宽高可靠上送报文；白名单匹配条件是五元组（源地址、目的地址、源端口、目的端口、协议号）。

应用层联动模块在处理协议报文时，首先匹配白名单，对于匹配白名单的协议报文，以大带宽和高速率上送。其次匹配模块中使能的普通协议报文，以特定速率上送CPU，速率大小可以配置。对于模块中没有打开的协议报文按照小带宽上送。

应用层联动模块中没有匹配到的协议报文，比如ARP，可以通过设置报文策略，确定对报文进行丢弃或者上送，上送时速率较小且可以配置。

攻击方法介绍

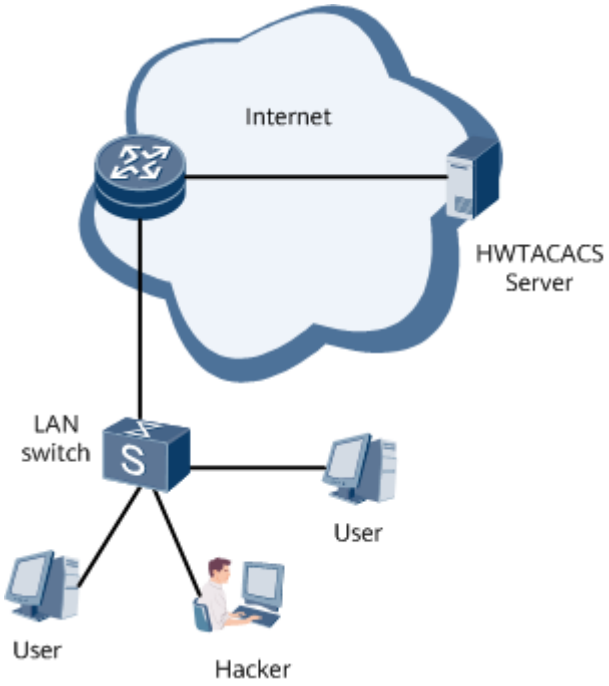
如下图所示，设备下面有很多用户，设备本身启用了很多业务，比如路由、HWTACACS、ICMP、IGMP、MPLS等，但不需要启用Telnet服务。为了防止Hacker发送大量的Telnet请求，导致设备耗费很多资源处理这些攻击报文，可以在设备上关闭掉Telnet服务，这样无论攻击者发送多少Telnet攻击报文，Telnet报文按照小带宽上送CPU，保证了系统和资源的正常工作。

说明

关闭Telnet服务后，用户可以通过命令行将处理方式修改为丢弃，以此取代默认的小带宽处理方式。此时对于攻击者发送的Telnet攻击报文，设备都不进行处理，直接丢弃。

对于已经开启的业务和协议，设备也可以通过限制其上送速率，使其以指定的速率上送，保证CPU不受攻击，保证网络的正常运行。

图 1-6 应用层联动



配置维护方法

application-apperceive default-action { **drop** | **min-to-cp** }，设置未匹配应用层联动开关策略的报文的缺省动作。

配置维护建议

与配置无关。

检查加固结果

- 执行**display application-apperceive** [**slot** *slot-id*] [**ap-id** *ap-id*]命令查看应用层联动功能的信息。
- 执行**display cpu-defend application-apperceive statistics** [**slot** *slot-id*] [**ap-id** *ap-id*]命令查看应用层联动报文丢弃情况。

?.3. 管理平面防护（IPv4）

安全策略介绍

管理平面防护MPAC（Management Plane Access Control）增强设备对拒绝服务型攻击的防范能力，可以增强系统的安全性，满足这些组网情况下的业务开展需求。

路由器可能同时启用多种服务，例如二层业务MSTP、RRPP，路由业务OSPF、BGP，MPLS业务LDP、RSVP，系统服务FTP Server，TFTP Server，诊断功能Ping、Tracert等。

在这种情况下，攻击者可以发送各种类型的报文攻击路由器，如果是目的地址是路由器自身接口（包括Loopback口）IP地址时，路由器就会直接将报文上送CPU。这样就会耗费路由器的CPU和系统资源，造成DoS攻击。

为了避免这种攻击，可以制定管理平面接入控制策略的规则，根据规则决定是否上送此协议报文。

路由器支持的MPAC包括：子接口应用管理平面接入控制策略、主接口应用管理平面接入控制策略、全局应用管理平面接入控制策略，可以对上送CPU的报文进行过滤。

设备根据子接口、主接口、全局上的管理平面接入控制策略的规则，决定报文是否上送CPU。如果子接口、主接口、全局上都没有配置管理平面接入控制策略的规则，则报文直接上送CPU。

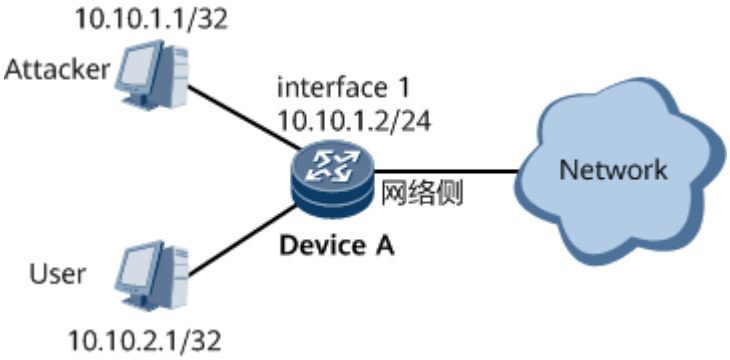
攻击方法介绍

如图1-7所示，为了防止Hacker发送各种TCP/IP攻击报文对DeviceA进行攻击，造成DeviceA瘫痪，需要在DeviceA上部署管理平面控制接入策略。

图 1-7 MPAC 组网图

说明

本例中interface1代表GE1/0/0。



配置维护方法

在DeviceA上配置：

```
<DeviceA> system-view
[~DeviceA] service-security policy ipv4 test
[*DeviceA-service-sec-test] rule 10 deny protocol ip source-ip 10.10.1.1 0
[*DeviceA-service-sec-test] step 10
[*DeviceA-service-sec-test] description rule 10 is deny ip packet which from 10.10.1.1
[*DeviceA-service-sec-test] commit
[~DeviceA-service-sec-test] quit
[~DeviceA] service-security global-binding ipv4 test
[*DeviceA] commit
[~DeviceA] interface gigabitethernet 1/0/0
[~DeviceA-GigabitEthernet1/0/0] service-security binding ipv4 test
[*DeviceA-GigabitEthernet1/0/0] commit
```

配置维护建议

无。

检查加固结果

- 执行命令**display service-security policy ipv4** [*security-policy-name* [**slot** *slot-id*]]，查看设备上所有的管理平面接入控制策略的配置信息。

- 执行命令**display service-security binding ipv4** [**interface** *interface-type interface-number* [**slot** *slot-id*]]，查看接口的管理平面接入控制策略信息。
- 执行命令**display service-security statistics ipv4** [*security-policy-name*]，查看匹配管理平面接入控制策略的统计信息。

?.4. 攻击防范

安全策略介绍

目前，网络的攻击日益增多，而通信协议本身的缺陷以及网络部署问题，导致网络攻击造成的影响越来越大。特别是网络设备的攻击，将会导致设备或者网络瘫痪等严重后果。

攻击防范通过分析本机上送IP报文的格式和内容，针对不同类型的攻击报文，采用不同的处理方法。如果是畸形报文，则对其进行丢弃处理；如果是泛洪类型的攻击，则对其进行限速的处理。

也就是说，攻击防范针对上送本机的报文，对报文采用丢弃或者限制流量的手段，保障设备不受攻击的影响，业务正常运行。

攻击方法介绍

- 畸形报文攻击
  a. 没有IP载荷的泛洪

     攻击者经常构造大量只有IP头部，没有携带任何高层数据的IP报文，这些大量没有载荷的IP报文构成了flood攻击。如果只有20字节的IP报文头的报文，就认为是没有IP载荷的报文，将其丢弃。

  b. IGMP空报文

     IGMP报文是20字节的IP头加上8字节的IGMP报文体。如果IGMP报文的总长度小于28字节，设备认为该IGMP报文是畸形报文，直接丢弃。

  c. LAND攻击

     Land攻击是由著名的黑客组织RootShell发现的，于1997年11月20日公布的。

     原理是利用TCP连接三次握手中的缺陷，向目的主机发送源地址与目的主机地址一致的数据包，造成目的主机解析Land包占用过多的资源，导致网络瘫痪。即Land攻击者构造一个特别的SYN包，其源地址和目的地址被设置成同一台计算机的地址，源端口与目的端口也被设置成同一个端口。该计算机接收到SYN包之后，将导致该计算机向它自己的地址发送SYN+ACK消息，结果这个地址又发回SYN+ACK消息并创建一个空连接，每个这样的连接都将保留直到超时。

  d. Smurf攻击

     Smurf攻击的原理是：攻击者发送ICMP echo request报文，报文的目的地址是广播地址，源地址是受害者地址。这样，网络上的所有主机都会向受害者发送reply报文，造成受害者收到过多报文，导致CPU利用率过高。

     设备将目的地址为广播地址或者子网广播地址的ICMP echo request报文，直接认为是畸形报文丢弃。

- UDP泛洪攻击
  a. Fraggle攻击

Fraggle攻击的原理是利用UDP 7号端口（UDP Echo Request），7端口的服务和ICMP echo基本一致，都是把收到的报文载荷原样返回，以测试源和目的之间的网络状况。

和Smurf攻击的原理一样，攻击者把源地址伪造成受害者地址，目点地址写为广播地址，目的端口为7。如果该广播网络中有很多主机都起用了UDP echo服务，受害者将收到很多回复报文，造成系统繁忙，达到攻击效果。设备默认UDP端口号为7的报文是攻击报文，直接将其丢弃。

b. UDP诊断端口攻击

攻击者对UDP诊断端口（7-echo，13-daytime，19-Chargen等）发送报文，如果同时发送的数据包数量很大，造成泛洪，可能影响网络设备的正常工作。设备将UDP端口为7，13，19的报文认为是攻击报文，直接丢弃。

配置维护方法

无

检查加固结果

无

配置维护建议

无

BGP/BGP4+

安全策略介绍

- BGP MD5验证

  BGP使用TCP作为传输协议，只要TCP数据包的源地址、目的地址、源端口、目的端口和TCP序号是正确的，BGP就会认为这个数据包有效，但数据包的大部分参数对于攻击者来说是不难获得的。为了保证BGP协议免受攻击，BGP邻居之间使用TCP的MD5认证来降低被攻击的可能性。

  两端配置的明文必须相同，两台设备配置完成时间间隔若大于**hold-time**，则邻居会中断，否则不会中断。

  为防止BGP对等体所设置的MD5密码被破解，需要周期性的更新MD5认证密码。

  说明

  为了保证更好的安全性，建议不要使用MD5算法。

- Keychain认证

  Keychain由多个认证密钥组成，每个密钥包含一个ID和密码。密钥存在生命期，通过密钥的生命期可以在Keychain中滚动选择不同的认证密钥。BGP会话两端绑定相同规则的Keychain后，Keychain可以滚动选择认证密钥来增强BGP防攻击性。

- TCP-AO认证

  TCP-AO认证用于对TCP会话建立以及数据交互过程中的收发报文进行认证，支持对报文完整性进行校验，防止TCP报文重放攻击。TCP-AO认证可以提高BGP对等体之间建立TCP连接的安全性，适用于对安全性要求较高的网络。

- BGP GTSM特性

GTSM机制通过TTL的检测来达到防止攻击的目的。如果攻击者模拟真实的BGP协议报文，对一台路由器不断的发送报文。路由器接口板收到这些报文后，发现是发送给本机的报文，则直接上送控制层面的BGP协议处理，而不加辨别其“合法性”。这样导致路由器控制层面因为处理这些“合法”报文，系统异常繁忙，CPU占用率高。

配置GTSM功能，通过检测IP报文头中的TTL值是否在一个预先定义好的特定范围内来对路由器进行保护，增强系统的安全性。

- BGP白名单特性

  应用层联动模块检测上送的协议报文，对匹配白名单的协议报文，允许其以大带宽和高速率上送。

- CP-CAR

  已经开启的业务和协议，设备也可以通过限制其上送速率，使其以指定的速率上送，保证CPU不受攻击，保证网络的正常运行。

- Session-CAR

  BGP协议的白名单Session-CAR功能是指针对BGP协议的每个会话独立设置一个CAR通道，以便保障每个BGP协议会话的带宽不会被其他流量抢占（其他流量包括相同协议的其他会话流量，也包括任何其他协议流量）。当出现BGP报文流量冲击时，可以配置此任务调整BGP白名单Session-CAR中BGP各会话的报文通道带宽，以保证BGP报文可以正常上送。

- 路由超限控制

  BGP路由表路由数量通常都很大，为了防止从对等体接收到大量路由而导致消耗过多系统资源，BGP使用邻居路由限定为一个BGP路由器设置允许从其对等体收到的最大路由数量。

- AS-PATH数量控制

  BGP接收路由时会检查AS_Path属性中的AS号是否超限。如果超限则丢弃路由，路由发布也会检查AS_Path属性中的AS号是否超限，如果超限，则不发布此路由，防止恶意构造超长AS-PATH属性的错误报文对路由器进行报文攻击。

- RPKI

  RPKI（Resource Public Key Infrastructure）通过验证BGP路由源AS的合法性、BGP路由AS_Path属性的正确性或路由发布者的合法性来保证BGP的安全性。

  RPKI主要用来解决路由传递过程中攻击者通过发布更详细的路由导致数据传输过程中流量被窃取的问题。例如，某运营商向用户发布了目的地址为10.10.0.0/16的合法路由，路由攻击者发布了目的地址为10.10.153.0/24的路由，由于攻击者发布的路由更详细，导致从用户端发往10.10.153.0/24的流量被攻击者窃取。

  为了解决上述问题，对路由进行路由起源认证ROA（Route Origin Authorization）、ASPA验证（Autonomous System Provider Authorization）或者区域验证来保证BGP的安全性。

- BMP

  通过配置BMP，可以对网络中设备的BGP/BGP4+运行状态进行实时监控，包括对等体关系的建立与解除、路由信息刷新等。

  BMP主要应用在存在监控服务器，需要对网络中设备的BGP/BGP4+运行状态进行监控的组网中。BMP的产生改变了以往只能通过人工查询方式来获得设备的BGP/BGP4+运行状态的状况，大大提高了网络监控的效率

- BGP TLS认证

  传输层安全性TLS（Transport Layer Security）协议，是在SSL协议的基础上提供的一种保证数据完整性和私密性的安全协议。执行该命令，对SSL服务器配置SSL/TLS认证，加密BGP协议报文，保证网络上数据传输的安全性。

攻击方法介绍

- DOS攻击

  攻击者可以发送各种类型的报文攻击设备，如果是多播协议报文、或者目的地址是设备自身接口（包括Loopback口）IP地址时，设备就会直接将报文上送CPU。这样就会耗费设备的CPU和系统资源，造成DoS攻击，BGP会话创建后通过下发白名单，应用层联动模块检测上送的协议报文，对匹配白名单的协议报文，允许其以大带宽和高速率上送，对于不在白名单内报文，限制其以默认带宽和速率上送，从而避免Dos报文攻击；同时在接口上应用CP-CAR限制BGP报文上送速率，保证CPU不受攻击，保证网络的正常运行。

- 注入大量BGP路由

  BGP协议运行于各种形态的设备，如接入网IAS，NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X等，BGP路由量的多少取决于设备的CPU和内存。如果设备接收BGP路由数量超过其极限容量，会导致内存耗尽从而设备无法运行，影响业务正常运行。BGP通过单邻居路由数量限定手段，如果攻击者注入大量路由，超过邻居路由限定值的，超限路由被直接丢弃，防止设备资源耗尽。

- 构造错误BGP协议报文

  攻击者通过构造各种类型的错误报文，如超长的as-path属性个数报文、报文头错误报文、错误长度报文、下一跳非法报文等，进行错误报文攻击。BGP执行宽进严出，丢弃错误报文，但是不中断邻居关系，保证业务不中断，对于超长as-path报文，执行as-path-limit限定，路由接收和发布如果发现as-path超限，则拒绝接收和发布。

  Update报文包含各类路径属性，若收到任何格式错误的Update报文，可能会造成BGP会话震荡等问题。为了增强可靠性，用户可以配置peer path-attribute-treat对定BGP路径属性做特殊处理。

- 网络报文攻击

  数据包五元组参数的大部分参数对于攻击者来说是不难获得的，为了保证BGP协议免受攻击，可以采用如下手段进行防攻击：

  - BGP邻居之间使用TCP的MD5认证来降低被攻击的可能性。
  - BGP会话设置Keychain密钥认证增强BGP防攻击性。
  - 设置GTSM，通过TTL的检测来达到防止攻击的目的。

操作步骤

- 配置MD5认证

  BGP的MD5认证只是为TCP连接设置MD5认证密码，由TCP完成认证。如果认证失败，则不建立TCP连接。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**bgp** *as-number*，进入BGP视图。
  c. 执行命令**peer** { *ipv4-address* | *group-name* } **password** { **cipher** *cipher-password* | **simple** *simple-password* }，配置MD5认证密码。

     在用户设置密码时可以选择两种输入方式：

     - 配置**cipher** *cipher-password*参数表示输入密文字符串设置密码。
     - 配置**simple** *simple-password*参数表示输入明文字符串设置密码。

说明

- 密码需要符合密码复杂度规则：大写、小写、数字、特殊字符中至少有2种，并且长度不能小于8。
- 为避免高安全风险，配置时请尽量选择密文模式。为保证设备安全，请定期修改密码。在BGP视图下配置的MD5认证，对BGP的扩展地址族视图同样有效，因为它们使用同一个TCP连接。BGP MD5认证与BGP Keychain认证互斥。

d. 执行命令**commit**，提交配置。

- 配置Keychain认证

  BGP对等体两端必须都配置Keychain认证，且配置的Keychain必须使用相同的加密算法和密码，才能正常建立TCP连接，交互BGP消息。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**bgp** *as-number*，进入BGP视图。
  c. 执行命令**peer** { *ipv4-address* | *group-name* } **keychain** *keychain-name*，配置Keychain认证。

     BGP对等体两端必须都配置针对使用TCP连接的应用程序的Keychain认证，且配置的Keychain必须使用相同的加密算法和密码，才能正常建立TCP连接，交互BGP消息。

     配置BGP Keychain认证前，必须配置*keychain-name*对应的Keychain认证，否则TCP连接不能正常建立。Keychain的详细配置方法请参见《HUAWEI NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X系列 配置指南-安全》中Keychain配置章节。

     说明

     - 在BGP视图下配置的Keychain认证，对BGP的扩展地址族视图同样有效，因为它们使用同一个TCP连接。
     - BGP MD5认证与BGP Keychain认证互斥。

  d. 执行命令**commit**，提交配置。

- 配置TCP-AO认证

  BGP对等体两端必须都配置TCP-AO认证。为TCP连接设置TCP-AO认证密码，由TCP完成认证。如果认证失败，则不建立TCP连接。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**tcp ao** *tcpaoname*，创建一条TCP-AO，并进入tcp-ao policy视图。
  c. 执行命令**binding keychain** *kcName*，在TCP-AO中绑定一条对应的Keychain。

     说明

     在配置此步骤之前，需要先通过keychain命令创建一个Keychain。

  d. 执行命令**key-id** *keyId*，在TCP-AO中创建一个Key-id，并进入tcp-ao key-id视图。
  e. 执行命令**send-id** *sndId* **receive-id** *rcvId*，在Key-id中配置send-id、receive-id。
  f. 执行命令**quit**，进入tcp-ao policy视图。

g. 执行命令**quit**，进入系统视图。

h. 执行命令**bgp** *as-number*，进入BGP视图。

i. 执行命令**peer** *ipv4-address* **as-number** *as-number*，指定对等体的IP地址及其所属的AS编号。

j. 执行命令**peer** *ipv4-address* **tcp-ao policy** *tcp-ao-name*，配置BGP对等体建立TCP连接时的TCP-AO认证。

参数*tcp-ao-name*须使用步骤2中创建的TCP-AO。

说明

针对同一个对等体，TCP-AO认证与MD5认证、Keychain认证是两两互斥的。

k. 执行命令**commit**，提交配置。

- 配置BGP GTSM功能

配置GTSM功能，通过检测IP报文头中的TTL值是否在一个预先定义好的特定范围内来对路由器进行保护。

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**bgp** *as-number*，进入BGP视图。

c. 执行命令**peer** { *group-name* | *ipv4-address* } **valid-ttl-hops** [*hops*]，配置BGP GTSM功能。

被检测报文的TTL值有效范围为[255–*hops*+1, 255]。例如，对于EBGP直连路由，*hops*的取值为1，即有效的TTL值设为255。

说明

- 当在BGP视图下配置时，对MP-BGP的VPNv4扩展同样有效，因为它们使用同一个TCP连接。
- GTSM和EBGP-MAX-HOP功能均会影响到发送出去的BGP报文的TTL值，存在冲突，只能对同一对等体或对等体组使能两种功能中的一种。

使能BGP的GTSM策略后，接口板对所有BGP报文的TTL值进行检查,根据实际组网的需要，对于不符合GTSM策略中指定的TTL值范围的报文，直接丢弃。对于没有配置GTSM策略的报文，如果BGP Peer配置存在，直接上送。没有配置BGP Peer的BGP报文直接丢弃。这样就避免了网络攻击者模拟的“合法”BGP报文占用CPU。

d. 执行命令**commit**，提交配置。

- 设置GTSM缺省动作

请在配置了GTSM功能的路由器上进行以下配置。

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**gtsm default-action** { **drop** | **pass** }，设置未匹配GTSM策略的报文的缺省动作。

说明

如果仅仅配置了缺省动作，但没有配置GTSM策略时，GTSM不生效。

该命令仅在Admin-VS支持，无法在其它VS中配置，功能对所有VS生效。

c. 执行命令**commit**，提交配置。

- 配置ROA

a. 请根据应用场景选择以下一种配置。

- 当本端设备需要通过与RPKI服务器建连来获取ROA数据库时，请执行下述配置：

  1) 执行命令**system-view**，进入系统视图。
  2) 执行命令**rpki**，启动RPKI并进入RPKI视图。
  3) 执行命令**session** *ipv4-address*，配置RPKI与RPKI服务器建立TCP连接的会话信息。
  4) 执行命令**tcp port** *port-number* [**password md5** *cipher-password* | **keychain** *keychain-name*]，配置RPKI与RPKI服务器建立TCP连接的连接信息。

     说明

     为了保证更好的安全性，建议不要使用MD5算法。

     密码需要符合密码复杂度规则：大写、小写、数字、特殊字符(不包括？和空格)中至少有2种，并且长度不能小于8。

     为避免高安全风险，配置时请尽量选择密文模式。为保证设备安全，请定期修改密码。

  5) （可选）执行命令**timer** { **aging** *aging-time* | **refresh** *refresh-time* }，配置RPKI会话的时间参数。

     可配置的时间参数包括验证数据的老化时间*aging-time*和会话的定时刷新时间*refresh-time*。用户可根据对BGP安全性的要求，对验证数据的老化时间和会话的定时刷新时间进行设置。对BGP安全性要求越高越应设置较小的时间值。但频繁的数据刷新会占用部分网络带宽。

  6) （可选）执行命令**rpki-limit** *limit* [**alert-only** | **idle-forever** | **idle-timeout** *times*]，设置允许从特定会话中收到的最大ROA（Route Origin Authorization）数量。

     通常服务器上ROA数量都很大，为了防止从服务器接收到大量ROA而导致消耗过多系统资源，可以使用**rpki-limit**命令来为一个BGP设备设置允许从会话收到的最大ROA数量。这样就对接收服务器发送的ROA数据又增加了一个控制机制。

  7) （可选）执行命令**connect-interface** { *interface-name* | *ipv4-source-address* | *interface-type interface-number* | *interface-type ipv4-source-address* | *interface-type interface-number ipv4-source-address* }，指定发送RPKI报文的源接口。
  8) （可选）执行命令**ssl-policy** *policy-name*，配置RPKI与RPKI服务器建立TCP连接时绑定的SSL策略。
  9) 执行命令**quit**，进入RPKI视图。
  10) 执行命令**quit**，进入系统视图。
  11) 执行命令**commit**，提交配置。

     说明

     当RPKI会话的配置发生变化后，如果需要使新的配置立即生效，可以执行**reset rpki session**命令复位指定的RPKI连接。

- 当本端设备配置静态ROA数据库时，请执行下述配置：

  1) 执行命令**system-view**，进入系统视图。

2) 执行命令**rpki**，启动RPKI并进入RPKI视图。
3) 执行命令**origin-validation**，创建静态ROA数据库，并进入RPKI origin-validation视图。
4) 执行命令**static record** *ipv4-address mask-length* **max-length** *max-mask-length* **origin-as** *as-number*，配置静态ROA数据库。
5) 执行命令**quit**，进入RPKI视图。
6) 执行命令**quit**，进入系统视图。
7) 执行命令**commit**，提交配置。

b. 执行命令**bgp** *as-number*，进入BGP视图。

c. 请根据需要选择下面的命令来配置入口或出口ROA校验。

- 对于本端设备从EBGP邻居接收的路由，可以执行下述配置，对从EBGP邻居接收的路由进行入口ROA校验，校验结果不影响路由接收。
  1) 执行命令**prefix origin-validation enable**，使能RPKI的起源AS验证功能。该功能仅对从EBGP对等体收到的路由进行验证，不对从IBGP对等体收到的路由进行验证。使能起源AS验证功能后，设备通过将从EBGP对等体收到的路由的起源AS和数据库中记录的匹配的路由的起源AS数据进行对比，并给出验证结果：Valid（起源AS正确）、NotFound（无结果）或Invalid（起源AS错误）。
  2) （可选）执行命令**bestroute origin-as-validation** [**allow-invalid**]，配置将RPKI的BGP路由起源AS验证结果应用在BGP选路过程中。

     应用起源AS验证结果后的BGP路由优先级顺序为Valid > NotFound > Invalid。若不配置**allow-invalid**参数，则验证结果为invalid的BGP路由不参与选路。
  3) （可选）执行命令**peer** { *ipv4-address* | *group-name* } **advertise-ext-community**，配置将扩展团体属性发布给对等体。
  4) （可选）执行命令**peer** { *ipv4-address* | *group-name* } **advertise origin-as-validation**，将RPKI的BGP路由起源AS验证结果发布给指定对等体（组）。

     说明

     RPKI的BGP路由起源AS验证结果只发布给IBGP对等体。

- 对于本端设备向EBGP邻居发布的路由，可以执行下述配置，对向EBGP邻居发布的路由进行出口ROA校验，校验结果会影响路由发布。

  执行命令**peer** { *peerIpv4Addr* | *peerGroupName* } **origin-validation export** [**include-not-found** [**external**]]，配置本端设备对发往EBGP邻居的路由进行ROA出口校验。

  配置本端设备对向EBGP邻居发布的路由进行ROA出口校验后，设备通过将路由的起源AS和数据库中记录的匹配的路由的起源AS数据进行对比，校验结果有：Valid（起源AS正确）、NotFound（无结果）或Invalid（起源AS错误）。设备默认只对外发布校验结果为Valid的路由；如果需要对外发布校验结果为Valid和NotFound的路由，则可以配置include-not-found关键字；如果需要对外发布校验结果为Valid和NotFound的路由（且NotFound的路由是从其他AS域发布给本端设备的），则可以配置include-not-found external关键字。

d. 执行命令**commit**，提交配置。

- 配置ASPA
  a. 请根据应用场景选择以下一种配置。
     - 当本端设备需要通过与RPKI服务器建连来获取ASPA数据库时，请执行下述配置：
       1) 执行命令**system-view**，进入系统视图。
       2) 执行命令**rpki**，启动RPKI并进入RPKI视图。
       3) 执行命令**session** *ipv4-address*，配置RPKI与RPKI服务器建立TCP连接的会话信息。
       4) 执行命令**tcp port** *port-number* [**password md5** *cipher-password* | **keychain** *keychain-name*]，配置RPKI与RPKI服务器建立TCP连接的连接信息。

          说明

          出于安全性考虑，不建议使用该特性中的弱安全算法，如果确实需要使用，请先执行**undo crypto weak-algorithm disable**命令使能弱安全算法功能。

          为了保证更好的安全性，建议不要使用MD5算法。

          密码需要符合密码复杂度规则：大写、小写、数字、特殊字符(不包括？和空格)中至少有2种，并且长度不能小于8。

          为避免高安全风险，配置时请尽量选择密文模式。为保证设备安全，请定期修改密码。
       5) 执行命令**version** *version-num*，配置RPKI的版本号，RPKI版本2支持接收ASPA数据，需要设备和RPKI服务器都支持RPKI版本2。
       6) （可选）执行命令**timer** { **aging** *aging-time* | **refresh** *refresh-time* }，配置RPKI会话的时间参数。

          可配置的时间参数包括验证数据的老化时间*aging-time*和会话的定时刷新时间*refresh-time*。用户可根据对BGP安全性的要求，对验证数据的老化时间和会话的定时刷新时间进行设置。对BGP安全性要求越高越应设置较小的时间值。但频繁的数据刷新会占用部分网络带宽。
       7) （可选）执行命令**aspa-limit** *limit* [*percentage*] [**alert-only** | **idle-forever** | **idle-timeout** *times*]，设置允许从特定会话中收到的最大ASPA数量。

          通常服务器上ASPA数量都很大，为了防止从服务器接收到大量ASPA而导致消耗过多系统资源，可以使用**aspa-limit**命令来为一个BGP设备设置允许从会话收到的最大ASPA数量。这样就对接收服务器发送的ASPA数据又增加了一个控制机制。
       8) （可选）执行命令**connect-interface** { *interface-name* | *ipv4-source-address* | *interface-type interface-number* | *interface-type ipv4-source-address* | *interface-type interface-number ipv4-source-address* }，指定发送RPKI报文的源接口。
       9) （可选）执行命令**ssl-policy** *policy-name*，配置RPKI与RPKI服务器建立TCP连接时绑定的SSL策略。
       10) 执行命令**quit**，进入RPKI视图。
       11) 执行命令**quit**，进入系统视图。
       12) 执行命令**commit**，提交配置。

说明

当RPKI会话的配置发生变化后，如果需要使新的配置立即生效，可以执行**reset rpki session**命令复位指定的RPKI连接。

- 当本端设备配置静态ASPA数据库时，请执行下述配置：
  1) 执行命令**system-view**，进入系统视图。
  2) 执行命令**rpki**，启动RPKI并进入RPKI视图。
  3) 执行命令**aspa-validation**，创建静态ASPA数据库，并进入RPKI aspa-validation视图。
  4) 执行命令**static record** *customer-as* **provider** *as-number* { **ipv4** | **ipv6** }，配置静态ASPA数据库。
  5) 执行命令**quit**，进入RPKI视图。
  6) 执行命令**quit**，进入系统视图。
  7) 执行命令**commit**，提交配置。

b. 执行命令**bgp** *as-number*，进入BGP视图。

c. 请根据需要选择下面的命令来配置入口ASPA校验。对于本端设备从EBGP邻居接收的路由，可以执行下述配置，对从EBGP邻居接收的路由进行入口ASPA校验，校验结果不影响路由接收。

i. 执行命令**peer** { *peerIpv4Addr* | *peerIpv6Addr* } **role** { **provider** | **rs** | **rs-client** | **customer** | **lateral-peer** | **sibling** }，配置BGP邻居的角色。

ii. 执行命令**aspa-validation enable**，使能RPKI的ASPA验证功能。使能ASPA验证功能后，设备通过将路由的AS_Path和数据库中记录的匹配的ASPA对进行对比，并给出验证结果：Valid（有效）、NotFound（无结果）或Invalid（无效）。

iii. （可选）执行命令**bestroute aspa-validation** [**allow-invalid**]，配置将RPKI的BGP路由ASPA验证结果应用在BGP选路过程中。应用ASPA验证结果后的BGP路由优先级顺序为Valid > NotFound > Invalid。若不配置**allow-invalid**参数，则验证结果为Invalid的BGP路由不参与选路。

d. 执行命令**commit**，提交配置。

- 配置区域验证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**rpki**，启动RPKI并进入RPKI视图。

c. 执行命令**region-validation**，使能区域验证功能并进入region-validation视图。

d. 可根据需要配置区域或区域联盟。

- 创建区域
  1) 执行命令**region** *region-id*，创建区域。
  2) 执行命令**description** *description-text*，为区域配置描述信息。
  3) 执行命令**as-number** { *asn* } &<1-100>，配置AS号列表，可将AS域加入区域中。
  4) 执行命令**quit**，进入region-validation视图。
  5) 执行命令**quit**，进入RPKI视图。
  6) 执行命令**quit**，进入系统视图。

- 创建区域联盟
  1) 执行命令**region** *region-id*，创建区域。
  2) 执行命令**quit**，进入region-validation视图。
  3) 执行命令**region-confederation** *region-confederation-id*，创建区域联盟。
  4) 执行命令**description** *description-text*，为区域联盟配置描述信息。
  5) 执行命令**region** { *region-id* } &<1-100>，在区域联盟下配置区域ID列表，可将区域加入区域联盟中。
  6) 执行命令**quit**，退出RPKI region-validation-confederation视图，进入region-validation视图。
  7) 执行命令**quit**，进入RPKI视图。
  8) 执行命令**quit**，进入系统视图。

e. 执行命令**bgp** *as-number*，进入BGP视图。

f. 根据需要使能区域或区域联盟功能。

- 执行命令**region-validation**，使能BGP路由区域验证功能。
- 执行命令**region-validation confed-check strict**，使能BGP路由严格的区域验证规则。

g. 执行命令**bestroute region-validation** [**allow-invalid**]命令，配置将RPKI的BGP路由区域验证结果应用在BGP选路过程中。

区域验证通过，路由有效，可以参与选路；区域验证失败，路由无效，无法参加选路。如果用户希望当区域验证失败时，路由也可以参与选路，则可以配置**allow-invalid**，配置此关键字后，即使区域验证失败，路由也被认为是有效的，可以参与选路，在选路时会降低其优先级。

h. 执行命令**commit**，提交配置。

- 配置BMP

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**bmp**，启动BMP并进入BMP视图。

c. （可选）执行命令**statistics-timer** *time*，配置BMP向监控服务器上报BGP/BGP4+运行状态统计信息的时间间隔。

用户可根据对BGP/BGP4+运行状态稳定性的要求，配置BMP向监控服务器上报BGP/BGP4+运行状态统计信息的时间间隔。通常情况下，如对网络质量要求比较高，需要配置较小的统计信息上报时间间隔。但频繁的上报统计信息会占用部分网络带宽。

d. 执行命令**bmp-session** [**vpn-instance** *vrf-name*] { *ipv4-address* | *ipv6-address* } [**alias** *alias-name*]，配置BMP与监控服务器建立TCP连接的IPv4/IPv6会话地址。

alias *alias-name*用来指定会话的别名。通过指定不同的**alias** *alias-name*参数，BMP可以与相同的目的IP地址不同目的端口号的监控服务器建立TCP连接。

e. 配置BMP向监控服务器上报的路由类型。

- 配置BMP向监控服务器上报指定地址族下BGP/BGP4+对等体的RIB-IN路由的路由类型。

1) 根据需要选择其中一条命令进入BMP-Monitor视图：
   - **monitor public**：进入BMP-Monitor视图并监控公网地址族下的所有BGP/BGP4+对等体的运行状态。
   - **monitor all-vpn-instance**：进入BMP-Monitor视图并监控私网地址族下的所有BGP/BGP4+对等体的运行状态。
   - **monitor peer**：进入BMP-Monitor视图并监控公网地址族下特定BGP/BGP4+对等体的运行状态。
   - **monitor vpn-instance**：进入BMP-Monitor视图并监控指定VPN实例下的所有BGP/BGP4+对等体的运行状态。
   - **monitor vpn-instance peer**：进入BMP-Monitor视图并监控指定VPN实例下特定BGP/BGP4+对等体的运行状态。
2) 执行命令**route-mode** { **ipv4-family unicast** | **ipv4-family labeled-unicast** | **ipv4-family vpnv4** | **ipv6-family unicast** | **ipv6-family vpnv6** } **adj-rib-in** { **pre-policy** | **post-policy** }，配置BMP向监控服务器上报指定地址族下BGP/BGP4+对等体的RIB-IN路由的路由类型。

   当用户希望监控服务器对通过入口策略前的路由（即设备从邻居收到的所有路由）进行监控时，可以指定参数**pre-policy**；当用户希望监控服务器只对通过入口策略后的路由（即通过路由策略筛选后，实际下发到路由表中的路由）进行监控时，可以指定参数**post-policy**。

   说明

   若配置向监控服务器上报的路由类型为**pre-policy**，需要在BGP视图下通过**keep-all-routes**或**peer keep-all-routes**命令保存自BGP连接建立起来之后的所有来自对等体（组）的BGP/BGP4+路由更新信息，即使这些路由没有通过已配置的入口策略。

- 配置BMP向监控服务器上报指定地址族下BGP/BGP4+对等体的RIB-OUT路由的路由类型。

  根据需要选择其中一条命令进入BMP-Monitor视图：
  - **monitor public**：进入BMP-Monitor视图并监控公网地址族下的所有BGP/BGP4+对等体的运行状态。
  - **monitor all-vpn-instance**：进入BMP-Monitor视图并监控私网地址族下的所有BGP/BGP4+对等体的运行状态。
  - **monitor peer**：进入BMP-Monitor视图并监控公网地址族下特定BGP/BGP4+对等体的运行状态。
  - **monitor vpn-instance**：进入BMP-Monitor视图并监控指定VPN实例下的所有BGP/BGP4+对等体的运行状态。
  - **monitor vpn-instance peer**：进入BMP-Monitor视图并监控指定VPN实例下特定BGP/BGP4+对等体的运行状态。

  执行命令**route-mode** { **ipv4-family unicast** | **ipv4-family labeled-unicast** | **ipv4-family vpnv4** | **ipv6-family unicast** | **ipv6-family vpnv6** } **adj-rib-out** { **pre-policy** | **post-policy** }，配置BMP向监控服务器上报指定地址族下BGP/BGP4+对等体的RIB-OUT路由的路由类型。

  当用户希望监控服务器对通过出口策略前的路由（即设备将要发送给邻居的所有路由）进行监控时，可以指定参数**pre-policy**；当用户希望监

控服务器只对通过出口策略后的路由（即通过路由策略筛选后，实际发送给邻居的路由）进行监控时，可以指定参数**post-policy**。

- 配置BMP向监控服务器上报指定地址族下BGP/BGP4+对等体的Local-rib路由的路由类型。
  1) 根据需要选择其中一条命令进入BMP-Monitor视图：
     - **monitor public**：进入BMP-Monitor视图并监控公网地址族下的所有BGP/BGP4+对等体的运行状态。
     - **monitor vpn-instance**：进入BMP-Monitor视图并监控指定VPN实例下的所有BGP/BGP4+对等体的运行状态。
  2) 根据需要选择其中一条命令：
     - 执行命令**route-mode** { **ipv4-family unicast** | **ipv4-family labeled-unicast** | **ipv4-family vpnv4** | **ipv6-family unicast** | **ipv6-family vpnv6** } **local-rib** [**add-path** | **all**] [**path-marking**]，配置BMP向监控服务器上报指定地址族下BGP/BGP4+对等体的Local-rib路由信息。
     - 执行命令**route-mode** { **ipv4-family** | **ipv6-family** } **flow local-rib** [**report route-identifier**]，配置BMP向监控服务器上报BGP-Flow地址族下BGP/BGP4+对等体的Local-rib路由信息。

f. 执行命令**quit**，进入BMP Session视图。

g. 执行命令**tcp connect port** *port-number* [**password md5** *cipher-password* | **keychain** *keychain-name*]，配置与监控服务器建立TCP连接的连接信息。

说明

为了保证更好的安全性，建议不要使用MD5算法。

h. （可选）执行命令**ssl-policy name** *policy-name*，配置BMP的SSL策略。

说明

配置该命令前，需要先在系统视图下执行**ssl policy** *policy-name*创建SSL策略。

i. （可选）执行命令**connect-interface** { *interface-type interface-number* | *ip-source-address* | *interface-type interface-number ip-source-address* }，指定发送BMP报文的源接口。

j. 执行命令**commit**，提交配置。

说明

当BMP会话的配置发生变化后，如果需要使新的配置立即生效，可以执行**reset bmp session**命令复位指定的BMP连接。

- 配置TLS认证

  安全套接层SSL（Secure Sockets Layer）协议是在Internet基础上提供的一种保证私密性的安全协议，它能使客户端与服务器之间的通信不被攻击者窃听。执行该命令，将BGP对等体（组）设置成SSL客户端或服务器，利用SSL数据加密、身份验证和消息完整性验证机制，保证网络上数据传输的安全性。

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**bgp** *as-number*，进入BGP视图。

  c. 执行命令**peer** { *group-name* | *ipv4-address* } **ssl-server certificate**，对SSL服务器配置SSL/TLS认证。

d. 执行命令**peer** { *group-name* | *ipv4-address* } **ssl-policy name** *ssl-policy-name*，对SSL客户端或服务器应用SSL策略。

e. 执行命令**peer** { *group-name* | *ipv4-address* } **ssl-policy role** { **client** | **server** }，将对等体（组）设置成SSL客户端或服务器。

f. 执行命令**commit**，提交配置。

说明

配置该命令前，需要先执行peer as-number命令建立相应的对等体关系。

SSL/TLS认证功能仅支持在服务器配置。BGP MD5认证与BGP Keychain认证互斥。

对等体级别和对等体组级别的该配置遵从个体优先的原则，即对等体上的配置优先级高于对等体组上的配置。

配置SSL角色、应用SSL策略和SSL/TLS认证（客户端不需配置SSL/TLS认证）同时配置，整体功能才会生效。

TLS认证仅支持BGP单实例，不支持BGP多实例。

----结束

操作结果

- 使用**display bgp peer** [*ipv4-address*] **verbose**命令查看BGP对等体的认证信息。
- 使用**display gtsm statistics** { *slot-id* | **all** }命令查看GTSM的统计信息。

  说明

  VS模式下，该命令仅在Admin VS支持。
- 使用**display rpki session** *ipv4-address* **verbose**命令查看RPKI会话的配置信息。
- 使用**display rpki table**命令查看路由起源的相关数据ROA。
- 使用**display bmp session** [**vpn-instance** *vrf-name*] [*ipv4-address* [**alias** *alias-name*] **verbose**]命令查看BMP会话的配置信息。
- 使用**display bgp bmp-monitor** { **all** | { **ipv4** | **vpnv4 vpn-instance** *vpn-instance-name* | **vpnv4** } *ipv4-address* }命令查看BMP监控所有BGP邻居或指定不同地址族下的BGP邻居信息。
- 使用**display cpu-defend whitelist session-car bgp statistics slot** *slot-id*命令查看指定接口板的BGP白名单Session-CAR的统计信息。

OSPF/OSPFv3

安全策略介绍

OSPF/OSPFv3报文验证

OSPF/OSPFv3支持报文验证功能，只有通过验证的报文才能接收，否则将不能正常建立邻居关系。使用区域验证时，一个区域中所有的路由器在该区域下的验证模式和口令必须一致。接口验证方式用于在相邻的路由器之间设置验证模式和口令，优先级高于区域验证方式。

OSPFv3 IPSec验证

相关协议（OSPFv3的验证）定义了使用IPSec（IP Security）机制认证OSPFv3报文的方法。

- 机密性：ESP用来提供机密性。使能ESP后，不被ESP保护的OSPFv3报文和没有通过机密性检查的报文将会被丢弃。
- 数据验证：使能OSPFv3验证后，不被AH或ESP保护的OSPFv3报文和没有通过验证检查的报文将会被丢弃。

在同一个端口上运行的OSPFv3实例只能使用相同的SA。

OSPFv3应用IPSec验证并发送报文，同时通知下层设备根据IPSec验证来检查接收到的报文。下层设备对接收到的所有报文都进行检测，自动丢弃没有通过检测的报文。

攻击方法介绍

OSPF

网络上对OSPF协议的攻击方法主要为伪造报文攻击，可以通过配置报文认证手段来识别并丢弃这些报文。

可能的攻击手段有：

- 修改报文老化时间到最大老化时间，导致所有路由器废弃这个报文。
- 发布合法的Max Sequence Number的LSA或者接近Max Seq Num的报文。
- 邻居路由器重启时复位其加密序列号状态的时机，更改序列号。
- 修改Hello报文中的邻居列表。

OSPFv3

- DOS攻击：

  存在DOS攻击时，路由器将会从较远路径调取OSPFv3协议报文。IO单板处理这些报文并将它们发送给主板，主板会基于OSPFv3将它们丢弃。这样会造成带宽资源和CPU的浪费，并降低系统性能。
- 错误路由信息的注入：

  OSPFv3接收所有来自合法设备的报文。所以，OSPFv3报文中携带的非法或错误路由信息可能对设备造成攻击，这些信息会造成路由数据库运算错误，引起网络故障。OSPFv3 IPSec认证机制可以避免这个问题。在通信两端对等体的OSPFv3上应用IPSec，OSPFv3只处理通过验证的报文。这样，OSPFv3可以避免接收来自未经验证对等体的错误路由数据。

配置维护方法

- OSPF区域认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ospf** [*process-id*]，进入OSPF进程视图。
  c. 执行命令**area** *area-id*，进入OSPF区域视图。
  d. 请根据需求，配置OSPF区域的验证模式。
     - 执行命令**authentication-mode simple** [[**plain**] *plain-text* | [**cipher**] *cipher-text*]，配置OSPF区域的验证模式（简单验证）。
     - 执行命令**authentication-mode** { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }]，配置OSPF区域的密文验证模式。

- 执行命令**authentication-mode keychain** *keychain-name*，配置OSPF区域的Keychain验证模式。

  说明

  使用Keychain验证模式，需要首先通过**keychain**命令创建一个keychain，并分别通过**key-id**、**key-string**和**algorithm**命令配置该keychain采用的key-id、密码及其认证算法，否则会造成OSPF认证始终为失败状态。

  为了保证更好的安全性，建议不要使用MD5和HMAC-MD5算法，推荐使用HMAC-SHA256等安全性较高的算法。

e. 执行命令**commit**，提交配置。

- OSPF接口认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入运行OSPF的接口视图。
  c. 请根据需求，配置接口验证方式。
     - 执行命令**ospf authentication-mode simple** [[**plain**] *plain-text* | [**cipher**] *cipher-text*]，配置OSPF接口的验证模式（简单验证）。
     - 执行命令**ospf authentication-mode** { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }]，配置OSPF接口的密文验证模式。
     - 执行命令**ospf authentication-mode keychain** *keychain-name*，配置OSPF接口的Keychain验证模式。

       说明

       使用Keychain验证模式，需要首先通过**keychain**命令创建一个keychain，并分别通过**key-id**、**key-string**和**algorithm**命令配置该keychain采用的key-id、密码及其认证算法，否则会造成OSPF认证始终为失败状态。

       为了保证更好的安全性，建议不要使用MD5和HMAC-MD5算法，推荐使用HMAC-SHA256等安全性较高的算法。

     - 执行命令**ospf authentication-mode null**，不对OSPF接口进行验证。
  d. 执行命令**commit**，提交配置。
- OSPFv3区域认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ospfv3** [*process-id*]，进入OSPFv3进程视图。
  c. 执行命令**area** *area-id*，进入OSPFv3区域视图。
  d. 请根据需求，配置OSPFv3区域的验证模式。
     - 执行命令**authentication-mode** { **hmac-sha256** | **hmac-sm3** } **key-id** *KeyId* { **plain** *PlainText* | [**cipher**] *CipherText* }，配置OSPFv3区域的HMAC-SHA256认证或HMAC-SM3认证模式。

       配置认证密码时，请尽量选择密文模式，因为简单口令会以明文的方式保存在配置文件中，有高安全风险。为保证设备安全，请定期修改密码。
     - 执行命令**authentication-mode** { **keychain** *Keychain-Name* }，配置OSPFv3区域的Keychain认证模式。

说明

使用Keychain验证模式，需要首先通过**keychain**命令创建一个keychain，并分别通过**key-id**、**key-string**和**algorithm**命令配置该keychain采用的key-id、密码及其认证算法，否则会造成OSPF认证始终为失败状态。

使用区域验证时，一个区域中所有的路由器在该区域下的验证模式和口令必须一致。

e. 执行命令**commit**，提交配置。

- OSPFv3进程认证

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**ospfv3** [*process-id*]，进入OSPFv3进程视图。

  c. 请根据需求，配置OSPFv3进程的验证模式。

  - 执行命令**authentication-mode** { **hmac-sha256** | **hmac-sm3** } **key-id** *KeyId* { **plain** *PlainText* | [**cipher**] *CipherText* }，配置OSPFv3进程的HMAC-SHA256认证或HMAC-SM3认证模式。

    配置认证密码时，请尽量选择密文模式，因为简单口令会以明文的方式保存在配置文件中，有高安全风险。为保证设备安全，请定期修改密码。

  - 执行命令**authentication-mode** { **keychain** *Keychain-Name* }，配置OSPFv3进程的Keychain认证模式。

    说明

    使用Keychain验证模式，需要首先通过**keychain**命令创建一个keychain，并分别通过**key-id**、**key-string**和**algorithm**命令配置该keychain采用的key-id、密码及其认证算法，否则会造成OSPFv3认证始终为失败状态。

  d. 执行命令**commit**，提交配置。

- OSPFv3接口认证

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

  c. 请根据需求，配置OSPFv3接口的验证模式。

  - 执行命令**authentication-mode** { **hmac-sha256** | **hmac-sm3** } **key-id** *KeyId* { **plain** *PlainText* | [**cipher**] *CipherText* }，配置OSPFv3接口的HMAC-SHA256认证或HMAC-SM3认证模式。

    配置认证密码时，请尽量选择密文模式，因为简单口令会以明文的方式保存在配置文件中，有高安全风险。为保证设备安全，请定期修改密码。

  - 执行命令**ospfv3 authentication-mode** { **keychain** *Keychain-Name* }，配置OSPFv3接口的Keychain认证模式。

    说明

    使用Keychain验证模式，需要首先通过**keychain**命令创建一个keychain，并分别通过**key-id**、**key-string**和**algorithm**命令配置该keychain采用的key-id、密码及其认证算法，否则会造成OSPFv3认证始终为失败状态。

    接口验证方式的优先级高于区域验证方式的优先级。同一网段的接口的验证模式和口令必须相同，不同网段可以不同。

d. 执行命令**commit**，提交配置。

- OSPFv3 IPsec认证
  a. 配置IPSec安全提议
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**ipsec proposal** *proposal-name*，创建安全提议并进入安全提议视图。
     iii. （可选）执行命令**transform** { **ah** | **esp** | **ah-esp** }，配置安全协议。
     iv. 执行命令**esp authentication-algorithm** { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }，设置ESP协议采用的验证算法。

     说明

     为了保证更好的安全性，建议不要使用MD5算法作为ESP协议的认证算法。

     需要首先通过**transform**命令选择了相应的安全协议后，才能配置该安全协议所需的安全算法。

     v. 执行命令**esp encryption-algorithm** { **3des** | **des** | **aes** [**128** | **192** | **256**] }，设置ESP协议采用的加密算法。

     说明

     使用加密算法时，DES/3DES加密算法安全性低，存在安全风险，在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES。

     vi. 执行命令**encapsulation-mode transport**，配置报文封装形式。
     vii. 执行命令**commit**，提交配置。
  b. 配置IPSec安全联盟
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**ipsec sa** *sa-name*，创建安全联盟。
     iii. 执行命令**proposal** *proposal-name*，在安全联盟中引用安全提议。
     iv. 执行命令**sa spi** { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*，配置安全联盟的SPI。

     说明

     在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的SPI必须和对端的出方向安全联盟的SPI一样；本端的出方向安全联盟的SPI必须和对端的入方向安全联盟的SPI一样。

     v. 选择一种方式配置协议的认证密钥。
        1) 执行命令**sa authentication-hex** { **inbound** | **outbound** } { **ah** | **esp** } [**cipher**] *hex-cipher-key*，配置协议的认证密钥（以16进制方式输入）。
        2) 执行命令**sa string-key** { **inbound** | **outbound** } { **ah** | **esp** } [**cipher**] *string-cipher-key*，配置协议的认证密钥（以字符串方式输入）。
     vi. 执行命令**commit**，提交配置。
  c. 使能OSPFv3 IPSec
     - 在OSPFv3进程上使能IPSec。
       1) 执行命令**system-view**，进入系统视图。
       2) 执行命令**ospfv3** [*process-id*]，进入OSPFv3视图。

3) 执行命令**ipsec sa** *sa-name*，在进程级别使能安全联盟。

说明

一个OSPFv3进程可以跟多个OSPFv3区域相关联。因此，应用在某个OSPFv3进程中的安全联盟同样可以应用于该进程关联的所有区域。

4) 执行命令**commit**，提交配置。

- 在OSPFv3区域上使能IPSec。
  1) 执行命令**system-view**，进入系统视图。
  2) 执行命令**ospfv3** [*process-id*]，进入OSPFv3视图。
  3) 执行命令**area** *area-id*，进入OSPFv3区域视图。
  4) 执行命令**ipsec sa** *sa-name*，在区域级别使能安全联盟。

说明

OSPFv3区域中安全联盟的优先级高于OSPFv3进程中安全联盟的优先级。

  5) 执行命令**commit**，提交配置。

检查加固结果

- 执行命令**display this**，查看报文验证信息。
- 执行命令**display ospfv3** [*process-id*]，查看在进程中应用的安全联盟。
- 执行命令**display ospfv3** [*process-id*] **area** [*area-id*]，查看在区域中应用的安全联盟。

RIP/RIPng

安全策略介绍

网络技术的快速发展对网络安全提出了更高的要求。在网络中传递的路由协议报文有可能被窃听、修改或伪造，报文攻击可能会引起网络中断。所以，需要有安全措施来保障报文的安全传递。

- 协议安全机制

  RIP/RIPng在协议层面上提供了以下安全策略。

  – TTL/跳数限制机制：

    RIP/RIPng报文总是在距离源设备一跳的范围内传递。所以，当RIP/RIPng报文在广播或组播网络（单播网络除外）中传递时，RIP/RIPng会将TTL/跳数值设置为1。

  – 白名单安全策略：

    RIP/RIPng为邻居端口提供“白名单安全”支持，避免CP-CAR策略引起的丢包。

  – GTSM安全策略

    RIP利用GTSM策略通过TTL检测来达到防止报文攻击的目的。TTL字段存在于IP报文头里，用于设置数据包可以经过的最多设备数。邻居转发层面将超出这个TTL范围的协议报文直接过滤掉，从而避免了控制层面受到攻击。

  – 认证策略：

    RIPV2提供报文认证机制，以避免错误的路由数据，错误报文和来自网络的重放攻击。

RIPng没有定义任何避免这些问题的认证机制，而是通过使用IPSec机制来验证RIPng报文。

- 路由限制：

  RIP/RIPng限制存入RIP/RIPng数据库的路径数目，从而达到根据设备的内存限制路径信息的目的。

- 大量错误报文攻击的应对策略描述：

  RIP采用白名单安全策略来避免大量错误报文的攻击。

- 其它策略：

  从系统层面上来说，系统通过在每个接口上支持基于CP的策略（CAR），来定义用于接收陌生来源报文的带宽。

攻击方法介绍

- DOS攻击：

  RIP采用白名单安全策略来避免DOS攻击。

  存在DOS攻击时，设备将会从较远路径调取RIP协议报文。IO单板处理这些报文并将它们发送给主板，主板会基于RIP/RIPng将它们丢弃。这样会造成带宽资源和CPU的浪费，并降低系统性能。

  为了避免处理这些来源不明的报文，RIP/RIPng提供“白名单安全”特性。协议会给每个已知端口建立一个“白名单安全”标签，实现更快速地互换报文。这对保证网络中的快速收敛是非常必要的。若发送报文的端口不在“白名单安全”列表中，则只有有限的缺省带宽资源分配给这些端口。

- 大量路由信息的注入：

  RIP可用于各种级别的设备，设备的CPU和内存决定了用于处理RIP/RIPng的路径的数量。若接收到的路径数量超出设备的承受能力，会造成设备CPU和内存的过度使用，从而造成设备运行不稳定。为避免造成设备运行的不稳定，RIP/RIPng通过配置设置接收路径数目的最大值。

- 错误路由信息的注入：

  对于合法来源的报文，若发送地址与网络匹配，RIP/RIPng将会接收。将直达线路数据直接携带在报文中，所以，在RIP报文中携带的路由数据中可能存在非法或错误路由信息的攻击。这会造成计算路由数据库不准确，引起网络故障。

  若在RIP端口的两侧配置验证特性，则RIP只接收经过验证的报文，这样就可以避免接受来自未经验证设备的路径。

  若在使能RIPng的端口的两侧配置IPSec，则RIPng只接受经过验证的报文，这样就可以避免接受来自未经验证设备的路径。

- 重放攻击：

  RIP识别MD5验证报文中的序列数，避免了来自网络的重放攻击。

操作步骤

- 配置RIP报文认证

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

  c. 请根据实际需要进行如下配置：

     - 执行命令**rip authentication-mode simple** { **plain** *plain-text* | [**cipher**] *password-key* }，配置用于RIP-2报文的简单明文认证方式。

简单认证方式下，明文的密码字符随认证报文一同传送。所以，在对安全性要求较高的网络环境中，不建议配置简单认证方式。

- 执行命令**rip authentication-mode md5** { **nonstandard** { { **plain** *plain-text* | [**cipher**] *password-key* } *key-id* | **keychain** *keychain-name* } | **usual** { **plain** *plain-text* | [**cipher**] *password-key* } }，配置用于RIP-2报文的MD5（Message Digest 5）密文认证方式。

  MD5密文认证方式下，MD5密码用来为报文加密和解密。这种认证方式比简单认证更安全。

  nonstandard类型支持非标准认证报文格式。

  usual表示支持IETF标准认证报文格式。

- 执行命令**rip authentication-mode hmac-sha256** { **plain** *plain-text* | [**cipher**] *password-key* } *key-id*，配置HMAC-SHA256（Hash Message Authentication Code for Secure Hash Algorithm 256）认证。

须知

配置认证密码时，请尽量选择密文模式，因为明文格式密码会以明文的方式保存在配置文件中，有高安全风险。为保证设备安全，请定期修改密码。

d. 执行命令**commit**，提交配置。

- 配置RIPng进程下的IPSec认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ripng** [*process-id*]，进入RIPng视图。
  c. 执行命令**ipsec sa** *sa-name*，使能RIPng的IPSec认证功能，并指定所采用的安全联盟的名称。
  d. 执行命令**commit**，提交配置。
- 配置RIPng接口的IPSec认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**ripng ipsec sa** *sa-name*，使能该接口的RIPng IPSec认证功能，并指定所采用的安全联盟的名称。

  说明

  ripng ipsec sa命令的优先级高于**ipsec sa**命令。即如果接口下和进程下同时配置了IPSec认证，并指定了不同的安全联盟名称，则以接口下的**ripng ipsec sa**配置为准。

  d. 执行命令**commit**，提交配置。
- 白名单安全策略：

  无需RIP/RIPng的特殊配置。

配置建议

- RIP验证支持：

在MD5验证中，华为支持的普通验证是基于相关标准实现的，RIP报文携带的checksum代替了密码。非标准验证是基于相关标准实现的，支持与相关标准中相同的报文格式。（只支持MD5算法）

配置keychain验证，提高了RIP关联的安全性。必须在两条链路上都配置keychain。注意：加密算法和对等体keychain配置的密码必须相同。否则，RIP对等体间无法关联，RIP报文不能正常传递。

建议配置HMAC-SHA256验证模式，以提高网络安全性。

- 使用IPSec的RIPng验证支持

  RIPng支持IPSec验证在为RIPng配置IPSec验证之前，熟悉IPSec的基础配置。

- RIP/RIPng端口安全：

  无需RIP/RIPng的特殊配置。

- 白名单安全策略：

  初次接收到相邻端口的回复报文时，RIP会把相邻端口加入白名单。但在加入时并不会检查相邻端口是否可信。在使能RIP的端口上配置验证特性，这样，可信任的相邻端口就会被加入到白名单中。

- RIP/RIPng路由限制：

  支持的最大路径数是由设备使用范围，内存和所支持的CP-CAR值决定的。

检查加固结果

- 执行命令**display rip** *process-id* **interface** [*interface-type interface-number*] [**verbose**]，命令查看RIP接口信息。
- 执行命令**display rip** *process-id*，查看RIP进程的当前运行状态及配置信息。
- 执行命令**display ripng** *process-id* **interface** [*interface-type interface-number*] [**verbose**]，查看IPSec认证所采用的安全联盟。
- 执行命令**display ripng** *process-id* **statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor** *neighbor-ipv6-address*] }，查看未通过认证的RIPng报文数量。

ISIS/ISISv6

安全策略介绍

IS-IS认证是基于网络安全性的要求而实现的一种加密手段，通过在IS-IS报文中增加认证字段对报文进行加密。当本地路由器接收到远端路由器发送过来的IS-IS报文，如果发现认证密码不匹配，则将收到的报文进行丢弃，达到自我保护的目的。

攻击方法介绍

拒绝错误报文：攻击方可以获取网络中的正确hello报文或者链路状态报文，然后构造ISIS可以识别的攻击报文发送到路由器。虽然路由器可以通过认证信息识别出这些攻击报文并丢弃，但仍可能导致正确的报文因不能及时处理而被丢弃，影响网络稳定。

操作步骤

- 配置IS-IS区域认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**isis** [*process-id*]，进入IS-IS视图。

c. 执行命令(根据加密类型任选其一)，配置IS-IS的区域认证。

- **area-authentication-mode** { **simple** { **plain** *plain* | [**cipher**] *cipher* } | **md5** { [**cipher**] *cipher* | **plain** *plain* } } [**ip** | **osi**] [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]
- **area-authentication-mode keychain** *keychain-name* [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]
- **area-authentication-mode hmac-sha256 key-id** *key-id* { **plain** *plain* | [**cipher**] *cipher* } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

须知

配置**area-authentication-mode**命令后，IS-IS对本地LSDB中所有未通过认证的Level-1 LSP报文以及新收到的没有通过认证的Level-1 LSP报文和SNP报文不做任何处理，等待其自动老化之后丢弃。因此，为避免配置认证之前的报文丢失，可以在已有业务的网络中部署认证时使用**send-only**参数。

为了保证更好的安全性，建议不要使用MD5算法。建议启用认证并使用HMAC-SHA256等安全性较高的算法提升安全性，以避免路由信息被非法篡改。

路由域认证支持以下几种组合形式：

- 对发送的LSP和SNP都封装认证信息，并检查收到的LSP和SNP是否通过认证，丢弃没有通过认证的报文。该情况下不配置参数**snp-packet**或**all-send-only**。
- 对发送的LSP封装认证信息并检查收到的LSP，对发送的SNP不封装认证信息，也不检查收到的SNP。该情况下需要配置参数**snp-packet authentication-avoid**。
- 对发送的LSP和SNP都封装认证信息，只检查收到的LSP，不检查收到的SNP。该情况下需要配置参数**snp-packet send-only**。
- 对发送的LSP和SNP都封装认证信息，不检查收到的LSP和SNP。该情况下需要配置参数**all-send-only**。

d. 执行命令**commit**，提交配置。

- 配置IS-IS路由域认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**isis** [*process-id*]，进入IS-IS视图。
  c. 执行命令(根据加密类型任选其一)，配置IS-IS路由域认证。
  - **domain-authentication-mode** { **simple** { **plain** *plain* | **cipher** *cipher* } | **md5** { [**cipher**] *cipher* | **plain** *plain* } } [**ip** | **osi**] [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]
  - **domain-authentication-mode keychain** *keychain-name* [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

- **domain-authentication-mode hmac-sha256 key-id** *key-id* { **plain** *plain* | [**cipher**] *cipher* } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

  须知

  配置**domain-authentication-mode**命令后，IS-IS对本地LSDB中所有未通过认证的Level-2 LSP报文以及新收到的没有通过认证的Level-2 LSP报文和SNP报文不做任何处理，等待其自动老化之后丢弃。因此，为避免配置认证之前的报文丢失，可以在已有业务的网络中部署认证时使用**send-only**参数。

  为了保证更好的安全性，建议不要使用MD5算法。建议启用认证并使用HMAC-SHA256等安全性较高的算法提升安全性，以避免路由信息被非法篡改。

  路由域认证支持以下几种组合形式：

  - 对发送的LSP和SNP都封装认证信息，并检查收到的LSP和SNP是否通过认证，丢弃没有通过认证的报文。该情况下不配置参数**snp-packet**或**all-send-only**。
  - 对发送的LSP封装认证信息并检查收到的LSP，对发送的SNP不封装认证信息，也不检查收到的SNP。该情况下需要配置参数**snp-packet authentication-avoid**。
  - 对发送的LSP和SNP都封装认证信息，只检查收到的LSP，不检查收到的SNP。该情况下需要配置参数**snp-packet send-only**。
  - 对发送的LSP和SNP都封装认证信息，不检查收到的LSP和SNP。该情况下需要配置参数**all-send-only**。

d. 执行命令**commit**，提交配置。

- 配置IS-IS接口认证

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

  c. 执行命令（根据加密类型任选其一），配置接口的IS-IS认证模式和密码。

  - **isis authentication-mode** { **simple** { **plain** *plain* | **cipher** *cipher* } | **md5** { [**cipher**] *cipher* | **plain** *plain* } } [**level-1** | **level-2**] [**ip** | **osi**] [**send-only**]
  - **isis authentication-mode keychain** *keychain-name* [**level-1** | **level-2**] [**send-only**]
  - **isis authentication-mode hmac-sha256 key-id** *key-id* { **plain** *plain* | [**cipher**] *cipher* } [**level-1** | **level-2**] [**send-only**]

    说明

    为了保证更好的安全性，建议不要使用MD5算法。建议启用认证并使用HMAC-SHA256等安全性较高的算法提升安全性，以避免路由信息被非法篡改。

  关于参数的选举，请注意以下原则：

- 如果配置了**send-only**则表示仅对发送的Hello封装认证信息，而不检查收到的Hello报文是否通过了认证。只有不需要进行认证检查或者认证通过才能建立起邻居关系。
- 如果没有配置**send-only**，此时应保证同一网络所有接口的相同级别的认证密码一致。
- 参数**level-1**和**level-2**仅在以太网接口上是可见的。
- 当IS-IS接口链路类型为Level-1-2时，如果不选择参数**level-1**或**level-2**，则为Level-1和Level-2的Hello报文都配置认证模式和密码。

d. 执行命令**commit**，提交配置。

检查加固结果

执行命令**display isis lsdb verbose**，查看IS-IS的链路状态数据库信息。

MPLS

?.1. RSVP

安全策略介绍

RSVP使用RawIP传递协议报文，而RawIP本身不提供安全性，报文容易被篡改，设备容易受到攻击。RSVP消息通过验证摘要信息的正确性，来防止消息被篡改或伪造的恶意攻击，增强网络的可靠性和安全性。

- 基本原理

  在需要认证的两个节点上，用户需要配置相同的密钥。在发送报文时，节点使用密钥为报文计算得到一个摘要（通过HMAC-MD5算法），摘要信息作为报文的一个对象（Integrity对象），随着报文一起发送到对端节点。对端节点使用相同的密钥、相同的算法重新计算报文摘要，然后比较两个摘要是否相同，如果相同则接受，否则丢弃。RSVP认证不能防止回放攻击，也无法解决因RSVP报文的失序导致邻居之间认证关系终止的问题。为了解决该问题，引入了RSVP认证增强功能。RSVP认证增强是在基于原有认证的基础上增加了认证生存时间、握手和消息滑窗等特性，这样使得RSVP自身的安全性得到很大的提高，并大大加强了在网络阻塞等恶劣网络环境时对用户进行身份验证的能力。

- RSVP密钥管理方式

  RSVP密钥管理包括以下两种方式：

  说明

  HMAC-MD5认证安全性低，为了保证更好的安全性，建议使用Keychain认证，并且使用安全性较高的算法，例如HMAC-SHA-256。

  – HMAC-MD5密钥

    用户可以在RSVP接口、邻居下，以明文或者密文的方式输入密钥，密钥算法为HMAC-MD5。这种密钥管理方式的特点是：

    i. 每个协议特性都需要配置自己的密钥，密钥不能共享。
    ii. 每个接口、邻居只能配置一个密钥，要更换密钥必须重新配置。

- Keychain密钥

  Keychain是一种增强型加密算法，允许用户定义一组密码，形成一个密码串，并且分别为每个密码指定加解密算法及密码使用的有效时间。在收发报文时，系统会按照用户的配置选出一个当前有效的密码，并按照与此密码相匹配的加密解密算法，进行发送时加密和接收时解密报文。此外，系统可以依据密码使用的有效时间，自动完成有效密码的切换，避免了长时间不更改密码导致的密码易破解问题。

  这种密钥管理方式的特点是：

  i. Keychain的密码、所使用的加解密算法以及密码使用的有效时间可以单独配置，形成一个Keychain配置节点，每个Keychain配置节点至少需要配置一个密码，并指定加解密算法。

  ii. Keychain可以被各个协议特性引用，实现密钥集中管理、多特性共享。

  RSVP支持在接口、邻居下引用Keychain。

- RSVP的认证级别

  RSVP的认证级别分为两种：

  - 面向邻居的认证

    该级别的认证是指用户可以根据不同的邻居地址配置认证密钥等信息，RSVP会针对每个邻居进行单独的认证。

    有两种配置方式：

    i. 以邻居设备的某接口的IP地址作为邻居地址进行配置。

    ii. 以邻居设备的LSR ID作为邻居地址进行配置。

  - 面向接口的认证
  - 用户在接口上配置认证，RSVP会根据消息的入接口进行认证处理。
  - 这两个认证级别的优先级顺序由高到低依次为：面向邻居的认证、面向接口的认证。只有当高优先级没有使能认证的情况下才会进行低优先级的认证处理，一旦高优先级认证没有通过，则丢弃该报文。

攻击方法介绍

攻击方法介绍如果有可能，最好介绍下通过此种认证方式的可能攻击方法及对应的防范措施。

- 重放攻击

  RSVP在处理报文时，会检查报文的参数、格式、类型等各种信息，但这些参数对于攻击者来说是不难获得的，一种常用的攻击手段就是截获RSVP的报文，之后重复向设备发送报文，增加设备的负担。RSVP消息通过增加认证对象，并验证对象的正确性，来防止消息被篡改或伪造的恶意攻击，增强网络的可靠性和安全性。

- 错误报文攻击

  攻击者通过构造各种类型的错误报文，如超长报文、报文头错误报文、错误长度报文、下一跳非法报文等，进行错误报文攻击。RSVP协议执行宽进严出，丢弃错误报文，但是不中断邻居关系，保证业务不中断，对于严重错误报文，如报文长度超长、报文类型非法等，则拒绝接收和发布。

操作步骤

- 配置基于RSVP邻居接口之间的密钥认证

  a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入MPLS TE链路的接口视图。

c. 执行命令**mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* }，配置RSVP认证密钥。

可以根据选用的参数，配置HMAC-MD5认证或者Keychain认证：

- **cipher**：配置HMAC-MD5认证，并使用密文方式显示认证密钥。
- **plain**：配置HMAC-MD5认证，并使用明文方式显示认证密钥。
- **keychain**：配置Keychain认证，引用全局配置的Keychain。

须知

配置认证密钥时，如果选择**plain**模式，密码将会以明文的方式保存在配置文件中。这种格式有高安全风险，配置时请尽量选择**cipher**模式。为保证设备安全，请定期修改密码。

HMAC-MD5认证安全性低，为了保证更好的安全性，建议使用Keychain认证，并且使用安全性较高的算法，例如HMAC-SHA-256。

要求在三个刷新周期内，在直连的两个接口都完成配置。如果在三个刷新周期内没有在两个接口都完成配置，则会导致RSVP会话Down。

d. 执行命令**commit**，提交配置。

- 配置基于RSVP邻居的密钥认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**mpls**，进入MPLS视图。

c. （可选）执行命令**mpls rsvp-te challenge-lost** *max-miss-times*，设置RSVP认证过程中认证方允许被认证方发送的challenge消息被丢失的最大次数。

d. （可选）执行命令**mpls rsvp-te retrans-timer challenge** *retransmission-interval*，配置challenge消息重传间隔。

e. 执行命令**mpls rsvp-te peer** *peer-addr*，进入RSVP邻居视图。

f. 执行命令**mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* }，配置RSVP认证密钥。

可以根据选用的参数，配置HMAC-MD5认证或者Keychain认证：

- **cipher**：配置HMAC-MD5认证，并使用密文方式显示认证密钥。
- **plain**：配置HMAC-MD5认证，并使用明文方式显示认证密钥。
- **keychain**：配置Keychain认证，引用全局配置的Keychain。

须知

配置认证密钥时，如果选择**plain**模式，密码将会以明文的方式保存在配置文件中。这种格式有高安全风险，配置时请尽量选择**cipher**模式。为保证设备安全，请定期修改密码。

HMAC-MD5认证安全性低，为了保证更好的安全性，建议使用Keychain认证，并且使用安全性较高的算法，例如HMAC-SHA-256。

要求在三个刷新周期内，在两个邻居节点都完成配置。如果在三个刷新周期内没有在两个邻居节点都完成配置，则会导致RSVP会话Down。

g. 执行命令**commit**，提交配置。

- 配置RSVP邻居直连接口之间密钥认证的生存时间（可选）

  RSVP认证时间的功能是：当RSVP邻居之间不存在CR-LSP时可以保持RSVP邻居关系，直到RSVP认证生存时间超时。RSVP认证时间不影响已存在的CR-LSP的状态。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入MPLS TE链路的接口视图。
  c. 执行命令**mpls rsvp-te authentication lifetime** *lifetime*，设置RSVP认证生存时间。
  d. 执行命令**commit**，提交配置。

- 配置RSVP邻居之间密钥认证的生存时间（可选）
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls**，进入MPLS视图。
  c. 执行命令**mpls rsvp-te peer** *peer-addr*，进入MPLS RSVP-TE邻居视图。

  当*peer-addr*为邻居的接口地址，且与其LSR-ID不相同时，则配置的RSVP认证生存时间是基于邻居接口地址的配置。这种配置方式只对该接口生效。

  当*peer-addr*与邻居LSR-ID相同时，则配置的RSVP认证生存时间是基于邻居LSR-ID的配置。这种配置方式将使这个配置在整台设备上生效。
  d. 执行命令**mpls rsvp-te authentication lifetime** *lifetime*，设置RSVP认证生存时间。
  e. 执行命令**commit**，提交配置。

- 在接口视图下配置handshake功能（可选）

  配置handshake功能可以解决RSVP密钥验证不能防止回放攻击的问题。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入MPLS TE链路的接口视图。
  c. 执行命令**mpls rsvp-te authentication handshake**，配置handshake功能。

  说明

  必须先"配置RSVP认证方式"，才能配置handshake功能，且需要在RSVP认证双方均配置handshake功能，该功能才能生效。

在本端配置handshake功能后，如果本端收到一个没有与自己建立RSVP认证关系的邻居所发送的RSVP消息，则本端会发送携带本端标识信息的Challenge消息给该邻居，邻居收到Challenge消息后回应一个Response消息。Response消息中携带了收到的Challenge消息的标识信息。本端收到邻居发来的Response消息，如果其中携带的标识信息与本端的一致，就确定可以与该邻居建立RSVP认证关系。

d. 执行命令**commit**，提交配置。

- 在MPLS RSVP-TE邻居视图下配置handshake功能（可选）
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls**，进入MPLS视图。
  c. 执行命令**mpls rsvp-te peer** *peer-addr*，进入MPLS RSVP-TE邻居视图。
     - 当*ip-address*为邻居的接口地址，且与其LSR-ID不相同时，则配置的handshake功能是基于邻居接口地址的配置。这种配置方式只对该接口生效。
     - 当*ip-address*与邻居LSR-ID相同时，则配置的handshake功能是基于邻居LSR-ID的配置。这种配置方式将使handshake功能在整台设备上生效。
  d. 执行命令**mpls rsvp-te authentication handshake**，配置handshake功能。

     说明

     必须先"配置RSVP认证方式"，才能配置handshake功能，且需要在RSVP认证双方均配置handshake功能，该功能才能生效。

     在本端配置handshake功能后，如果本端收到一个没有与自己建立RSVP认证关系的邻居所发送的RSVP消息，则本端会发送携带本端标识信息的Challenge消息给该邻居，邻居收到Challenge消息后回应一个Response消息。Response消息中携带了收到的Challenge消息的标识信息。本端收到邻居发来的Response消息，如果其中携带的标识信息与本端的一致，就确定可以与该邻居建立RSVP认证关系。
  e. 执行命令**commit**，提交配置。

  说明

  如果在邻居之间配置了Handshake功能，则当需要配置认证生存时间，那么认证生存时间的时长需要大于RSVP刷新消息的发送时间间隔。如果认证生存时间小于RSVP刷新消息的发送时间间隔，就可能造成在认证生存时间内收不到RSVP刷新消息而删除认证关系。这样，当下一个刷新消息到来的时候就需要重新进行Handshake机制的检测，如此反复可能会造成TE隧道无法建立或者被删除。

- 在接口视图下配置message window功能（可选）

  Message window功能主要是用来解决报文失序问题。

  缺省情况下，RSVP消息窗口大小是1，即本地设备只能保存邻居RSVP消息的一个最近的最大的序列号。

  当配置的window-size大于1时，本地就可以保存邻居RSVP消息的最近多个有效序列号。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入MPLS TE链路的接口视图。

c. 执行命令**mpls rsvp-te authentication handshake**，配置handshake功能。

说明

必须先"配置RSVP认证方式"，才能配置handshake功能，且需要在RSVP认证双方均配置handshake功能，该功能才能生效。

d. 执行命令**mpls rsvp-te authentication window-size** *window-size*，配置message window功能，即指定本地设备可保存的邻居RSVP消息有效序列号的个数。

当RSVP接口类型为Trunk时，RSVP邻居之间只在Trunk链路上建立一个邻居关系。RSVP消息可以从Trunk的任意一个成员接口接收，且各个成员口不是按顺序接收报文的，这样可能造成RSVP消息失序，因此必须配置RSVP消息滑动窗口。如果滑动窗口设置过小，收到的失序的RSVP消息有些可能不在窗口范围内而被丢弃，这样会导致RSVP邻居认证关系终止。

e. 执行命令**commit**，提交配置。

- 在MPLS RSVP-TE邻居视图下配置message window功能（可选）
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls**，进入MPLS视图。
  c. 执行命令**mpls rsvp-te peer** *peer-addr*，进入MPLS RSVP-TE邻居视图。
     - 当*peer-addr*为邻居的接口地址，且与其LSR-ID不相同时，则配置的Message window功能是基于邻居接口地址的配置。这种配置方式只对该接口生效。
     - 当*peer-addr*与邻居LSR-ID相同时，则配置的Message window功能是基于邻居LSR-ID的配置。这种配置方式将使该配置在整台设备上生效。
  d. 执行命令**mpls rsvp-te authentication handshake**，配置handshake功能。

说明

必须先"配置RSVP认证方式"，才能配置handshake功能，且需要在RSVP认证双方均配置handshake功能，该功能才能生效。

  e. 执行命令**mpls rsvp-te authentication window-size** *window-size*，配置message window功能，即指定本地设备可保存的邻居RSVP消息有效序列号的个数。

当RSVP接口类型为Trunk时，RSVP邻居之间只在Trunk链路上建立一个邻居关系。RSVP消息可以从Trunk的任意一个成员接口接收，且各个成员口不是按顺序接收报文的，这样可能造成RSVP消息失序，因此必须配置RSVP消息滑动窗口。如果滑动窗口设置过小，收到的失序的RSVP消息有些可能不在窗口范围内而被丢弃，这样会导致RSVP邻居认证关系终止。

  f. 执行命令**commit**，提交配置。

----结束

检查配置结果

- 使用**display mpls rsvp-te**命令查看接口的RSVP-TE配置信息。
- 使用**display mpls rsvp-te peer** [**interface** *interface-type interface-number* | *peer-address*]命令查看使能RSVP-TE的接口的RSVP-TE邻居信息。

?.2. LDP

安全策略介绍

- LDP MD5验证

  MD5称为Message-Digest Algorithm 5，是相关标准定义的国际标准摘要密码算法。MD5的典型应用是针对一段信息计算出对应的信息摘要，从而防止信息被篡改。MD5信息摘要是通过不可逆的字符串变换算法产生的，结果唯一。因此，不管信息内容在传输过程中发生任何形式的改变，只要重新计算就会产生不同的信息摘要，接收端就可以由此判定收到的是一个不正确的报文。

  LDP MD5应用其对同一信息段产生唯一摘要信息的特点来实现LDP报文防篡改校验，比一般意义上TCP校验和更为严格。

  LDP MD5验证是在TCP发出去之前进行的：LDP消息在经TCP发出前，会在TCP头后面填充一个唯一的信息摘要再发出。而这个信息摘要就是把TCP头、LDP消息、以及用户设置的密码一起作为原始信息，通过MD5算法计算出的。

  当接收端收到这个TCP报文时，首先会取得报文的TCP头、信息摘要、LDP消息，并结合TCP头、LDP消息以及本地保存的密码，利用MD5计算出信息摘要，然后与报文携带的信息摘要进行比较，从而检验报文是否被篡改过。

  在用户设置密码时有明文和密文两种形式选择，这里的明文密文是对用户设置的密码在配置文件中的记录形式而言的。明文就是直接在配置文件中记录用户设置的字符串，密文就是在配置文件中记录经过特殊算法加密后的字符串。

  但无论用户选择密码记录形态是明文还是密文形式，参与摘要计算时都是直接使用用户输入的字符串。由于明文和密文的转化算法各厂商私有，此种实现做到了私有算法对其他厂商透明。

  说明

  MD5算法安全性低，存在安全风险，建议改用更安全的验证方法。

- LDP Keychain认证

  Keychain是一种增强型加密算法，类似于MD5，Keychain也是针对同一段信息计算出对应的信息摘要，实现LDP报文防篡改校验。

  Keychain允许用户定义一组密码，形成一个密码串，并且分别为每个密码指定加解密算法（包括MD5，SHA-1等）及密码使用的有效时间。在收发报文时，系统会按照用户的配置选出一个当前有效的密码，并按照与此密码相匹配的加密解密算法以及密码的有效时间，进行发送时加密和接收时解密报文。此外，系统可以依据密码使用的有效时间，自动完成有效密码的切换，避免了长时间不更改密码导致的密码易破解问题。

  Keychain的密码、所使用的加解密算法以及密码使用的有效时间可以单独配置，形成一个Keychain配置节点，每个Keychain配置节点至少需要配置一个密码，并指定加解密算法。

  Keychain节点配置完成后，在全局MPLS LDP视图下指定需要引用Keychain节点的对等体和Keychain节点名称，对Keychain进行引用，即可实现对LDP会话的加密。不同的对等体可以引用同一个Keychain配置节点。

说明

LDP安全认证的配置，按生效优先级从高到低的排序是：对单对等体的配置、按对等体组批量配置、对所有对等体批量配置。对于同一优先级的配置，Keychain认证和MD5认证是互斥的。对于不同优先级的配置，Keychain认证和MD5认证可以同时配置，但对同一对等体来说，只有高优先级的配置生效。例如：对单对等体Peer1配置了MD5认证后，再对所有对等体批量配置Keychain认证，则Peer1仍采用MD5认证。其他对等体会采用Keychain认证。

可以根据需求的不同选择配置LDP MD5认证或者LDP Keychain认证。

- MD5算法配置简单，配置后生成单一密码，需要人为干预才可以切换密码，适用于需要短时间加密的网络。
- Keychain具有一组密码，可以根据配置自动切换，但是配置过程较为复杂，适用于对安全性能要求比较高的网络。

- LDP GTSM特性

  LDP GTSM是GTSM在LDP方面的具体应用。

  GTSM通过判定报文的TTL值，确定报文是否有效，从而保护设备免受攻击。GTSM For LDP即是对相邻或相近（基于只要跳数确定的原则）设备间的LDP消息报文应用此种机制，预先在各路由上设定好针对其他设备报文的有效范围，使能GTSM，这样当相应设备之间应用LDP时，如果LDP消息报文的TTL不符合之前设置的范围要求，就认为此报文为非法攻击报文予以丢弃，进而实现对上层协议的保护。

- LDP TCP-AO认证

  TCP-AO认证选项用于对TCP会话建立以及数据交互过程中的收发报文进行认证，支持对报文完整性进行校验，防止TCP报文重放攻击。

攻击方法介绍

无

操作步骤

- 对单对等体配置LDP MD5认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls ldp**，进入MPLS-LDP视图。
  c. 执行命令**md5-password** { **plain** | **cipher** } *peer-lsr-id password*，使能MD5认证，并配置认证密码。

     出于安全性考虑，不建议使用该特性中的弱安全算法，如果确实需要使用，请先执行**undo crypto weak-algorithm disable**命令使能弱安全算法功能。

     说明

     - 密码需要符合密码复杂度规则：大写、小写、数字、特殊字符(不包括？和空格)中至少有2种，并且长度不能小于8。
     - 为避免高安全风险，配置时请尽量选择密文模式。为保证设备安全，请定期修改密码。

     在用户配置认证密码时有明文和密文两种形式选择，这里的明文密文是对用户设置的认证密码在配置文件中的记录形式而言的。明文就是直接记录用户设置的字符串，密文就是记录经过特殊算法加密后的字符串。

须知

- 配置密码时，如果选择明文模式，密码将会以明文的方式保存在配置文件中。这种格式有高安全风险，配置时请尽量选择密文模式。为保证设备安全，请定期修改密码。
- 配置LDP MD5认证会导致LDP会话重建，与原来会话相关的LSP将被删除。

d. 执行命令**commit**，提交配置。

- 按对等体组批量配置LDP MD5认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls ldp**，进入MPLS-LDP视图。
  c. 执行命令**md5-password** { **plain** | **cipher** } **peer-group** *ip-prefix-name password*，按对等体组批量使能MD5认证，并配置认证密码。

     其中，对等体组包含的对等体IP地址范围，由IP地址前缀列表*ip-prefix-name*来限定。因此，执行此步骤前需要先配置名称为*ip-prefix-name*的IP地址前缀列表。

     出于安全性考虑，不建议使用该特性中的弱安全算法，如果确实需要使用，请先执行**undo crypto weak-algorithm disable**命令使能弱安全算法功能。

     说明

     - 密码需要符合密码复杂度规则：大写、小写、数字、特殊字符(不包括? 和空格)中至少有2种，并且长度不能小于8。
     - 为避免高安全风险，配置时请尽量选择密文模式。为保证设备安全，请定期修改密码。

  d. （可选）执行命令**authentication exclude peer** *peer-id*，指定不认证的对等体。
  e. 执行命令**commit**，提交配置。
- 对所有对等体批量配置LDP MD5认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls ldp**，进入MPLS-LDP视图。
  c. 执行命令**md5-password** { **plain** | **cipher** } **all** *password*，对所有对等体批量使能MD5认证，并配置认证密码。

     出于安全性考虑，不建议使用该特性中的弱安全算法，如果确实需要使用，请先执行**undo crypto weak-algorithm disable**命令使能弱安全算法功能。

     说明

     - 密码需要符合密码复杂度规则：大写、小写、数字、特殊字符(不包括? 和空格)中至少有2种，并且长度不能小于8。
     - 为避免高安全风险，配置时请尽量选择密文模式。为保证设备安全，请定期修改密码。

  d. （可选）执行命令**authentication exclude peer** *peer-id*，指定不认证的对等体。
  e. 执行命令**commit**，提交配置。

- 对单对等体配置基于TCP连接的LDP Keychain认证

  配置LDP Keychain认证之前，首先要配置全局Keychain。具体配置过程参见《NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 配置指南-安全》。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls ldp**，进入MPLS-LDP视图。
  c. 执行命令**authentication key-chain peer** *peer-id* **name** *keychain-name*，使能LDP Keychain认证，并引用配置的Keychain名称。

  须知

  配置LDP Keychain认证会导致LDP会话重建，与原来会话相关的LSP将被删除。

  d. 执行命令**commit**，提交配置。
- 按对等体组批量配置基于TCP连接的LDP Keychain认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls ldp**，进入MPLS-LDP视图。
  c. 执行命令**authentication key-chain peer-group** *ip-prefix-name* **name** *keychain-name*，按对等体组批量使能LDP Keychain认证，并引用配置的Keychain名称。

     其中，对等体组包含的对等体IP地址范围，由IP地址前缀列表*ip-prefix-name*来限定。因此，执行此步骤前需要先配置名称为*ip-prefix-name*的IP地址前缀列表。
  d. （可选）执行命令**authentication exclude peer** *peer-id*，指定不认证的对等体。
  e. 执行命令**commit**，提交配置。
- 对所有对等体批量配置基于TCP连接的LDP Keychain认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls ldp**，进入MPLS-LDP视图。
  c. 执行命令**authentication key-chain all name** *keychain-name*，对所有对等体批量使能LDP Keychain认证，并引用配置的Keychain名称。
  d. （可选）执行命令**authentication exclude peer** *peer-id*，指定不认证的对等体。
  e. 执行命令**commit**，提交配置。
- 对指定对等体配置基于UDP连接的LDP Keychain认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls ldp**，进入MPLS-LDP视图。
  c. 执行命令**gtsm peer** *ip-address* **valid-ttl-hops** *hops*，配置LDP GTSM功能。

     配置成功后，会对指定的对等体使用配置的Keychain认证。如果认证不通过，则LDP会话无法建立成功。

说明

当前命令只支持配置强加密算法的Keychain（算法类型包括：SHA-256、HMAC-SHA-256、SM3），不支持配置弱加密算法的Keychain。

d. 执行命令**commit**，提交配置。

- 配置LDP GTSM
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**mpls ldp**，进入MPLS LDP视图。
  c. 执行命令**gtsm peer** *ip-address* **valid-ttl-hops** *hops*，配置LDP GTSM功能。

     如果将hops设置为GTSM功能允许的最大有效跳数，当LDP对等体发来报文的TTL值在[255–hops+1，255]范围内，则接收该报文，否则丢弃该报文。
  d. 执行命令**commit**，提交配置。
- 配置LDP TCP-AO认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**tcp ao** *tcpaoname*，创建一条TCP-AO，并进入相应视图。
  c. 执行命令**binding keychain** *kcName*，在TCP-AO中绑定一条对应的Keychain。

     说明

     在配置此步骤之前，需要先配置全局的Keychain认证，创建当前步骤中要绑定的Keychain名称。
  d. 执行命令**key-id** *keyId*，在TCP-AO中创建一个Key-id，并进入TCP-AO Key-id视图。
  e. 执行命令**send-id** *sndId* **receive-id** *rcvId*，在Key-id中配置send-id、receive-id。
  f. 执行命令**quit**，返回上一级视图。
  g. 执行命令**quit**，返回系统视图。
  h. 执行命令**mpls ldp**，进入MPLS-LDP视图。
  i. 执行命令**authentication tcp-ao peer** *peer-id* **name** *tcpaoname*，使能LDP协议的TCP-AO认证。

     参数*tcpaoname*须使用步骤2中创建的TCP-AO。

     说明

     针对同一个对等体，TCP-AO认证与MD5认证、Keychain认证是两两互斥的。

     配置LDP TCP-AO认证可能会导致LDP会话重建。
  j. 执行命令**commit**，提交配置。

----结束

检查加固结果

- 执行命令**display mpls ldp session verbose**，查看LDP MD5认证、LDP Keychain认证、LDP TCP-AO认证的配置情况。
- 执行命令**display gtsm statistics** { *slot-id* | **all** }，查看GTSM的统计信息。

PCEP

安全策略介绍

- PCEP Keychain认证

  Keychain是一种增强型加密算法，也是针对同一段信息计算出对应的信息摘要，实现PCEP报文防篡改校验。

  Keychain允许用户定义一组密码，形成一个密码串，并且分别为每个密码指定加解密算法（包括SHA-2等）及密码使用的有效时间。在收发报文时，系统会按照用户的配置选出一个当前有效的密码，并按照与此密码相匹配的加密解密算法以及密码的有效时间，进行发送时加密和接收时解密报文。此外，系统可以依据密码使用的有效时间，自动完成有效密码的切换，避免了长时间不更改密码导致的密码易破解问题。

  Keychain的密码、所使用的加解密算法以及密码使用的有效时间可以单独配置，形成一个Keychain配置节点，每个Keychain配置节点至少需要配置一个密码，并指定加解密算法。

  通过配置PCEP会话认证能够提高网络的安全性，防止网络攻击。具体就是PCE Server和Client在建立会话时，可以配置Keychain认证。

- PCEP TLS认证

  TLS传输层安全性协议，是在SSL协议的基础上提供的一种保证数据完整性和私密性的安全协议，可以使客户端与服务器之间的通信不被攻击者窃听。

  PCE Server和Client在建立会话时，可以配置TLS认证，提高网络安全性，防止网络攻击。

- PCEP MD5认证

  通过在PCE Client端的会话上配置MD5认证功能，进行安全保护。PCE Server和Client两侧必须都使能MD5认证，且配置的密码相同。配置该功能后，双方发送的PCEP报文进行MD5加密，再通过TCP连接传送到对端，接收端根据统一的MD5加密规则以及报文中包含的密钥，对该PCEP报文进行解密，成功后上送给对应的模块处理该PCEP报文。只有通过MD5认证的PCEP报文，才进行处理，从而阻止非法的恶意报文攻击。

  说明

  MD5算法安全性低，存在安全风险，建议改用更安全的认证方法，比如PCEP Keychain认证或者PCEP TLS认证。

- TCP-AO认证

  TCP-AO认证选项用于对TCP会话建立以及数据交互过程中的收发报文进行认证，支持对报文完整性进行校验，防止TCP报文重放攻击。TCP-AO创建完成后，配置PCEP对TCP-AO进行引用，即可实现对PCEP会话的加密。不同的PCEP会话可以引用同一个TCP-AO。

  TCP-AO使用的是所绑定的Keychain下配置的密码，可以根据配置自动切换，但是配置过程较为复杂，适用于对安全性能要求比较高的网络。

- PCEP白名单特性

  应用层联动模块检测上送的协议报文，对匹配白名单的协议报文，允许其以大带宽和高速率上送。PCEP白名单特性默认开启，无需配置。

- Session-CAR

  PCEP协议的白名单Session-CAR功能是默认开启的，可以对PCEP会话间的报文通道隔离。

- 微隔离Car

  PCEP协议的微隔离CAR功能是默认开启，可以对PCEP建连报文进行微隔离保护。当遭受攻击时，可能存在PCEP不同会话间报文发生互相抢占带宽的情况，因此，一般情况下，不建议关闭该功能。

攻击方法介绍

无

操作步骤

- 配置PCEP Keychain认证

  配置PCEP Keychain认证之前，首先要配置全局Keychain。具体配置过程参见《NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 配置指南-安全》。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pce-client**，进入PCE Client视图。
  c. 执行命令**connect-server** *ip-address*，指定候选Server，并进入连接PCE服务器视图。
  d. 执行命令**authentication keychain** *keychain-name*，配置Client与各个PCE Server间的会话认证。
  e. 执行命令**commit**，提交配置。

- 配置PCEP TLS认证

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ssl policy** *policy-name*，创建SSL策略并进入SSL策略视图。
  c. 执行命令**ssl minimum version** { **tls1.1** | **tls1.2** | **tls1.3** }，配置当前SSL策略所采用的最低版本。

     SSL策略视图下的其他具体配置请参考《NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 配置指南-基础配置-配置用户登录》中的“配置绑定SSL Policy”。
  d. 执行命令**quit**，返回系统视图。
  e. 执行命令**pce-client**，进入PCE Client视图。
  f. 执行命令**connect-server** *ip-address*，指定候选Server，并进入连接PCE服务器视图。
  g. 执行命令**bind ssl-policy** *policy-name* [**pceps**]，指定策略名称。

     pceps参数用来指定TLS协商模式为PCEPS，即开始TLS协商之前两端先进行StartTLS协商（符合RFC 8253）。
  h. 执行命令**commit**，提交配置。

- 配置PCEP MD5认证

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pce-client**，进入PCE Client视图。
  c. 执行命令**connect-server** *ip-address*，指定候选Server，并进入连接PCE服务器视图。
  d. 执行命令**authentication md5 cipher** *md5text*，配置PCE Server与Client之间建立PCEP会话时采用MD5认证。

说明

- 密码需要符合密码复杂度规则：大写、小写、数字、特殊字符（不包括？和空格）中至少有2种，并且长度不能小于8。
- 为避免高安全风险，为保证设备安全，请定期修改密码。

e. 执行命令**commit**，提交配置。

- 配置PCEP TCP-AO认证

  配置TCP-AO认证之前，首先要配置TCP-AO。具体配置过程参见《NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 配置指南-安全》里的《TCP-AO配置》。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pce-client**，进入PCE Client视图。
  c. 执行命令**connect-server** *ip-address*，指定候选Server，并进入连接PCE服务器视图。
  d. 执行命令**authentication tcp-ao** *tcp-ao-name*，使能PCEP的TCP-AO认证。
  e. 执行命令**commit**，提交配置。

- 配置PCEP白名单Session-CAR功能

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**whitelist session-car pcep-ipv4 disable**，去使能PCEP的白名单Session-CAR功能。

     只有当该功能异常时，才需要去使能。正常情况下，建议保持开启PCEP的白名单Session-CAR功能。
  c. （可选）执行命令**whitelist session-car pcep-ipv4** { **cir** *cir-value* | **cbs** *cbs-value* | **pir** *pir-value* | **pbs** *pbs-value* } *，配置PCEP的白名单Session-CAR功能相关参数。
  d. 执行命令**commit**，提交配置。

- 配置PCEP的微隔离协议CAR功能

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**micro-isolation protocol-car pcep-ipv4** { **cir** *cir-value* | **cbs** *cbs-value* | **pir** *pir-value* | **pbs** *pbs-value* } *，配置PCEP的微隔离CAR的参数值。

     正常情况下，建议使用默认参数。*pir-value*应该大于等于*cir-value*，*pbs-value*应该大于等于*cbs-value*。
  c. （可选）执行命令**micro-isolation protocol-car pcep-ipv4 disable**，去使能PCEP的微隔离CAR功能。

     PCEP的微隔离CAR功能默认开启。执行**micro-isolation protocol-car pcep-ipv4 disable**命令后可以关闭该功能，此时不再对PCEP报文进行微隔离保护。正常情况下，建议保持开启PCEP的微隔离CAR功能。
  d. 执行命令**commit**，提交配置。

----结束

检查配置结果

- 执行命令**display pce protocol session** [*ip-address* | **verbose**]，查看PCEP会话的相关信息，包括对端设备的IP，会话双方的参数，会话状态以及会话发生错误的原因。

- 执行命令**display cpu-defend whitelist session-car pcep statistics slot** *slot-id*，查看指定接口板PCEP的白名单Session-CAR的统计信息。

MCAST 组播

?.1. 三层组播

安全策略介绍

- PIM邻居过滤

  支持在接口配置ACL策略对在该接口接收到的Hello报文进行过滤，通过过滤后，才能建立邻居关系。

  当存在大量恶意Hello报文时，可以通过在接口配置只允许指定的Hello报文通过的策略，丢弃其他恶意报文。

- PIM加入过滤

  支持在接口配置ACL策略对在该接口接收到的Join报文进行过滤检查，防止恶意的Join报文攻击。

  当存在大量恶意Join报文时，可以通过在接口配置只允许指定的Join报文通过的策略，丢弃其他恶意报文。

- IPv4/IPv6 PIM IPSec验证

  支持在接口配置IPv4/IPv6 PIM报文的IPSec认证，配置IPv4/IPv6 PIM IPSec后，不被IPSec保护的IPv4/IPv6 PIM报文和没有通过认证检查的IPv4/IPv6 PIM报文将被丢弃。

- MSDP白名单

  MSDP实现基于白名单，MSDP与对端建立稳定状态的链接关系，构建包括peer远端地址，本端接口地址，远端端口号，本端端口号，IP协议号(TCP)，调用组件接口通知底层，对收到满足此条件的报文优先进行上送（优先策略取决于底层的实现）。MSDP与对端邻居关系断开，调用组件接口通知底层，删除优先上送的策略。

  不满足白名单的恶意报文，不会进行上送，从而防止恶意攻击。

- MSDP MD5认证

  通过在MSDP Peer对等体上配置MD5认证功能，进行安全保护。Peer两侧必须都使能MD5认证，且配置的密码相同。配置该功能后，发送端Peer发送的MSDP报文进行MD5加密，再通过TCP连接传送到接收端Peer，接收端Peer根据统一的MD5加密规则以及报文中包含的密钥，对该MSDP报文进行解密，成功后上送给MSDP模块处理该MSDP报文。只有通过MD5认证的MSDP报文，才进行处理，从而阻止非法的恶意报文攻击。

  说明

  MD5属于不安全认证，建议优先采用Keychain认证。

- MSDP keychain认证

  组播MSDP支持Keychain，通过使用Keychain和新的TCP扩展选项，每条TCP连接能够让用户配置一组密码，每个密码可以设置不同加密算法和有效期限，密码可以随时更换，大大提高了加密报文的安全性。只有通过了keychain认证的报文，才进行处理，从而阻止非法的恶意报文攻击。

- TCP-AO认证

TCP-AO认证可以提高MSDP对等体之间建立TCP连接的安全性。相对于MD5（Message-Digest Algorithm 5）认证，MSDP TCP-AO认证适用于对安全性要求较高的网络。

- IGMP/MLD协议报文源地址过滤

  支持在接口配置ACL策略对在该接口接收到的IGMP/MLD协议报文进行过滤，防止伪造的恶意报文攻击。

  当存在伪造的IGMP/MLD协议报文时，可以通过在接口配置只允许指定IP源地址的IGMP/MLD协议报文通过的策略，丢弃其他恶意报文。

- IGMP/MLD IPSec认证

  支持在接口配置IGMP/MLD报文的IPSec认证，配置IGMP/MLD IPSec后，不被IPSec保护的IGMP/MLD报文和没有通过认证检查的IGMP/MLD报文将被丢弃。

- Session-CAR

  PIM协议的白名单Session-CAR功能是指针对PIM协议的每个邻居独立设置一个CAR通道，以便保障每个PIM邻居的带宽不会被其他流量抢占（其他流量包括相同协议的其他邻居流量，也包括任何其他协议流量）。当PIM报文发生流量冲击时，可以调整PIM白名单Session-CAR中PIM各会话的报文通道带宽，以保证PIM报文可以正常上送。

  MSDP协议的白名单Session-CAR功能是指针对MSDP协议的每个邻居独立设置一个CAR通道，以便保障每个MSDP邻居的带宽不会被其他流量抢占（其他流量包括相同协议的其他邻居流量，也包括任何其他协议流量）。当MSDP报文发生流量冲击时，可以调整MSDP白名单Session-CAR中MSDP各会话的报文通道带宽，以保证MSDP报文可以正常上送。

- IGMP/MLD 微隔离CAR

  IGMP/MLD协议的微隔离CAR功能是默认开启，可以对IGMP/MLD建连报文进行微隔离保护。当遭受攻击时，可能存在IGMP/MLD不同会话间报文发生互相抢占带宽的情况，因此，一般情况下，不建议关闭该功能。

攻击方法介绍

网络上可以通过伪造IGMP/MLD报文的形式攻击，可通过配置源地址过滤，将伪造报文丢弃。可能的攻击方式如下：

- 伪造低版本report加入，使组播组进入低版本兼容模式，此时如果收到离开报文不做处理，导致没有成员的组播组多转发流量直到该组超时。
- 伪造leave报文或者IGMPv3状态变化报告，仅导致路由器和所有组播组成员需要额外处理并响应指定组或源组查询，不会引起该组或源组流量的业务中断。
- 伪造IP地址相对较小的IGMP查询报文，使真正的查询器失效，无法响应组成员快速离开，造成没有成员的组播组流量会多转发至多一个组成员超时时间。
- 通过侦听通用查询发现有哪些组成员，然后发送大量的指定源组查询，每个查询包含大量源列表和指定很长的查询响应时间，造成所有主机在响应的延迟时间内消耗大量的CPU和内存处理所有这些指定源组查询的源列表，以便回应查询。

操作步骤

- PIM邻居过滤
  a. 执行命令**system-view**，进入系统视图。
  b. 配置基本数字或命名ACL，请根据情况选择如下配置之一：

- 配置基本数字ACL：
  1) 执行命令**acl** [**number**] *basic-acl-number* [**match-order** { **auto** | **config** }]，创建基本数字ACL，并进入相应的ACL视图。
  2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } **source** { *source-ip-address* { *source-wildcard* | **0** } | **any** }，配置基本数字ACL规则。
- 配置命名ACL：
  1) 执行命令**acl name** *acl-name* **basic** [**match-order** { **auto** | **config** }]，创建命名ACL，并进入相应的ACL视图。
  2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } **source** { *source-ip-address* { *source-wildcard* | **0** } | **any** }，配置命名ACL规则。

c. 执行命令**quit**，返回系统视图。

d. 执行命令**interface** *interface-type interface-number*，进入PIM接口视图。

e. 执行命令**pim neighbor-policy** { *basic-acl-number* | **acl-name** *acl-name* }，配置邻居过滤策略。

邻居过滤策略限定了合法的邻居地址范围，路由器将丢弃来自该地址范围之外的Hello消息。

说明

- 如果匹配上ACL规则，动作是**permit**，则设备与此范围的地址建立邻居关系。
- 如果匹配上ACL规则，动作是**deny**，则设备拒绝与此范围的地址建立邻居关系。
- 如果没有匹配上ACL规则，则设备拒绝与此范围的地址建立邻居关系。
- 如果引用的ACL不存在或者ACL下的rule不存在，则设备拒绝与所有地址建立邻居关系。

f. 执行命令**commit**，提交配置。

- PIM加入过滤
  a. 执行命令**system-view**，进入系统视图。
  b. 配置基本或高级ACL，请根据情况选择如下配置之一：
     - 配置基本ACL：
       1) 执行命令**acl** [**number**] *basic-acl-number* [**match-order** { **auto** | **config** }]，创建基本ACL，并进入相应的ACL视图。
       2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } **source** { *source-ip-address* { *source-wildcard* | **0** } | **any** }，配置基本ACL规则。
     - 配置高级ACL：
       1) 执行命令**acl** { **name** *advance-acl-name* [**advance** | [**advance**] **number** *advance-acl-number*] | [**number**] *advance-acl-number* } [**match-order** { **config** | **auto** }]，创建高级ACL，并进入相应的ACL视图。
       2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } **ip** [**destination** { *destination-ip-address* { *destination-wildcard* | **0** } | **any** } | **source** { *source-ip-address* { *source-wildcard* | **0** } | **any** }] *，配置高级ACL规则。

c. 执行命令**quit**，返回系统视图。

d. 执行命令**interface** *interface-type interface-number*，进入PIM接口视图。

e. 执行命令**pim join-policy** { { *advanced-acl-number* | **acl-name** *acl-name* } | **asm** { *basic-acl-number* | **acl-name** *acl-name* } | **ssm** { *advanced-acl-number* | **acl-name** *acl-name* } }，配置Join/Prune消息中的Join信息过滤策略。

路由器根据源地址或源/组地址过滤Join/Prune消息中的Join信息。

若使用**asm**参数，在基本ACL视图下，通过**rule**命令的**source**参数定义Join信息的组地址范围。

若使用**ssm**参数，在高级ACL视图下，通过**rule**命令的**source**参数定义Join信息的源地址范围，**destination**参数定义Join信息的组地址范围。

说明

- 如果匹配上ACL规则，动作是**permit**，则允许设备接收此范围内的Join信息。
- 如果匹配上ACL规则，动作是**deny**，则拒绝设备接收此范围内的Join信息。
- 如果没有匹配上ACL规则，则拒绝设备接收此范围内的Join信息。
- 如果引用的ACL不存在或者ACL下的rule不存在，则拒绝设备接收所有的Join信息。

f. 执行命令**commit**，提交配置。

- 配置全局IPv4 PIM IPSec
  - 配置IPv4 PIM协议报文使用IPSec安全认证

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**pim** [**vpn-instance** *vpn-instance-name*]，进入PIM视图。

  c. 执行命令**ipsec** [**unicast-message**] **sa** *sa-name*，配置全局IPv4 PIM IPSec，发送和接收IPv4 PIM协议报文时按指定的安全联盟对报文进行认证检查。若指定关键字**unicast-message**，则配置对IPv4 PIM单播协议报文进行认证检查。

  d. 执行命令**commit**，提交配置。

  - 配置仅对IPv4 PIM Hello报文使用IPSec安全认证

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**pim** [**vpn-instance** *vpn-instance-name*]，进入PIM视图。

  c. 执行命令**hello ipsec sa** *sa-name*，配置全局IPv4 PIM IPSec，仅对发送和接收IPv4 PIM Hello报文按指定的安全联盟对报文进行认证检查。

  d. 执行命令**commit**，提交配置。

  说明

  命令**ipsec sa**与命令**hello ipsec sa**相互覆盖，即最后配置的命令才生效。

- 配置接口IPv4 PIM IPSec
  - 配置IPv4 PIM协议报文使用IPSec安全认证

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

  c. 执行命令**pim ipsec sa** *sa-name*，在接口上配置IPv4 PIM IPSec，该接口发送和接收IPv4 PIM协议报文时按指定的安全联盟对报文进行认证检查。

d. 执行命令**commit**，提交配置。

– 配置IPv4 PIM Hello报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**pim hello ipsec sa** *sa-name*，在接口上配置IPv4 PIM IPSec，该接口发送和接收IPv4 PIM Hello报文时按指定的安全联盟对报文进行认证检查。

d. 执行命令**commit**，提交配置。

说明

命令**pim ipsec sa**与命令**pim hello ipsec sa**相互覆盖，即最后配置的命令才生效。

- 配置全局IPv6 PIM IPSec

– 配置IPv6 PIM协议报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**pim-ipv6**，进入IPv6 PIM视图。

c. 执行命令**ipsec** [**unicast-message**] **sa** *sa-name*，配置全局IPv6 PIM IPSec，发送和接收PIM协议报文时按指定的安全策略对报文进行认证检查。若指定关键字**unicast-message**，则配置对IPv6 PIM单播协议报文使用IPSec进行认证检查。

d. 执行命令**commit**，提交配置。

– 配置仅对IPv6 PIM Hello报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**pim-ipv6**，进入IPv6 PIM视图。

c. 执行命令**hello ipsec sa** *sa-name*，配置全局IPv6 PIM IPSec，仅对发送和接收IPv6 PIM Hello报文按指定的安全策略对报文进行认证检查。

d. 执行命令**commit**，提交配置。

说明

命令**ipsec sa**与命令**hello ipsec sa**相互覆盖，即最后配置的命令才生效。

- 配置接口IPv6 PIM IPSec

– 配置IPv6 PIM协议报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**pim ipv6 ipsec sa** *sa-name*，在接口上配置IPv6 PIM IPSec，该接口发送和接收PIM协议报文时按指定的安全策略对报文进行认证检查。

d. 执行命令**commit**，提交配置。

– 配置IPv6 PIM Hello报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**pim ipv6 hello ipsec sa** *sa-name*，在接口上配置IPv6 PIM IPSec，该接口发送和接收PIM Hello报文时按指定的安全策略对报文进行认证检查。

d. 执行命令**commit**，提交配置。

说明

命令**pim ipv6 ipsec sa**与命令**pim ipv6 hello ipsec sa**相互覆盖，即最后配置的命令才生效。

- MSDP白名单

  在路由器上MSDP与对端建立稳定状态的链接关系。

- MSDP MD5认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**undo crypto weak-algorithm disable**，加载弱算法插件。
  c. 执行命令**msdp** [**vpn-instance** *vpn-instance-name*]，进入MSDP视图。
  d. 执行命令**peer** *peer-address* **password** { **cipher** *cipher-password* | **simple** *simple-password* }，配置MSDP MD5认证。

     说明

     - 密码需要符合密码复杂度规则：大写、小写、数字、特殊字符(不包括？和空格)中至少有2种，并且长度不能小于8。
     - 为避免高安全风险，配置时请尽量选择密文模式。为保证设备安全，请定期修改密码。
     - 出于安全性考虑，不建议使用该特性中的弱安全算法，如果确实需要使用，请先执行**undo crypto weak-algorithm disable**命令使能弱安全算法功能。

     通过在MSDP Peer对等体上配置MD5认证功能，进行安全保护。Peer两侧必须都使能MD5认证，且配置的密码相同。配置该功能后，发送端Peer发送的MSDP报文进行MD5加密，再通过TCP连接传送到接收端Peer，接收端Peer根据统一的MD5加密规则以及报文中包含的密钥，对该MSDP报文进行解密，成功后上送给MSDP模块处理该MSDP报文。只有通过MD5认证的MSDP报文，才进行处理，从而阻止非法的恶意报文攻击。
  e. 执行命令**commit**，提交配置。
- MSDP Keychain认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**msdp** [**vpn-instance** *vpn-instance-name*]，进入MSDP视图。
  c. 执行命令**peer** *peer-address* **keychain** *keychain-name*，配置MSDP Keychain认证。

     组播MSDP支持Keychain，通过使用Keychain和新的TCP扩展选项，每条TCP连接能够让用户配置一组密码，每个密码可以设置不同加密算法和有效期限，密码可以随时更换，大大提高了加密报文的安全性。只有通过了keychain认证的报文，才进行处理，从而阻止非法的恶意报文攻击。

     MSDP对等体两端必须都配置Keychain认证，且配置的Keychain必须使用相同的加密算法和密码，才能正常建立TCP连接，交互MSDP报文。

     配置MSDP Keychain认证前，必须配置*keychain-name*对应的Keychain，否则TCP连接不能正常建立。

     说明

     MSDP MD5认证与MSDP Keychain认证互斥。

     MD5加密算法安全性低，存在安全风险，在协议支持的加密算法选择范围内，建议使用更安全的加密算法。

- TCP-AO认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**msdp** [**vpn-instance** *vpn-instance-name*]，进入MSDP视图。
  c. 执行命令**peer** *peer-address* **tcp-ao** *tcpAoName*，配置TCP-AO认证。

     配置MSDP TCP-AO认证前，必须使用tcp ao命令配置TCP-AO名称，否则TCP连接不能正常建立。MSDP对等体两端必须都配置TCP-AO认证，且配置的TCP-AO必须使用相同的加密算法和密码，才能正常建立TCP连接，交互MSDP消息。

     说明

     TCP-AO、MD5以及Keychain认证方式相互互斥。
- 配置IGMP Report或Leave报文源地址过滤策略
  a. 执行命令**system-view**，进入系统视图。
  b. 配置基本数字或命名ACL，请根据情况选择如下配置之一：
     - 配置基本数字ACL：
       1) 执行命令**acl** [**number**] *basic-acl-number* [**match-order** { **auto** | **config** }]，创建基本数字ACL，并进入相应的ACL视图。
       2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } **source** { *source-ip-address* { *source-wildcard* | **0** } | **any** }，配置基本数字ACL规则。
     - 配置命名ACL：
       1) 执行命令**acl name** *acl-name* **basic** [**match-order** { **auto** | **config** }]，创建命名ACL，并进入相应的ACL视图。
       2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } **source** { *source-ip-address* { *source-wildcard* | **0** } | **any** }，配置命名ACL规则。
  c. 执行命令**quit**，返回系统视图。
  d. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  e. 执行命令**igmp ip-source-policy** [*basic-acl-number* | **acl-name** *acl-name*]，配置IGMP Report或Leave报文的源地址过滤。

     说明

     - 如果配置此命令但不配置ACL规则时，则设备仅处理源地址和接收报文的接口地址在同一网段，或者源地址是0.0.0.0的IGMP Report或leave报文，丢弃源地址和接收报文的接口地址不在同一网段的IGMP Report或leave报文。
     - 如果配置ACL，将按照ACL规则对IGMP Report或leave报文进行源地址过滤。
       - 如果匹配上ACL规则，动作是**permit**，则接口接收此范围内的IGMP Report或Leave报文。
       - 如果匹配上ACL规则，动作是**deny**，则接口拒绝接收此范围内的IGMP Report或Leave报文。
       - 如果没有匹配上ACL规则，则接口拒绝接收此范围内的IGMP Report或Leave报文。
       - 如果引用的ACL不存在或者ACL下的rule不存在，则接口拒绝所有的IGMP Report或Leave报文。
  f. 执行命令**commit**，提交配置。

- 配置IGMP Query报文源地址过滤策略
  a. 执行命令**system-view**，进入系统视图。
  b. 配置基本数字或命名ACL，请根据情况选择如下配置之一：
     - 配置基本数字ACL：
       1) 执行命令**acl** [**number**] *basic-acl-number* [**match-order** { **auto** | **config** }]，创建基本数字ACL，并进入相应的ACL视图。
       2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } **source** { *source-ip-address* { *source-wildcard* | **0** } | **any** }，配置基本数字ACL规则。
     - 配置命名ACL：
       1) 执行命令**acl name** *acl-name* **basic** [**match-order** { **auto** | **config** }]，创建命名ACL，并进入相应的ACL视图。
       2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } **source** { *source-ip-address* { *source-wildcard* | **0** } | **any** }，配置命名ACL规则。
  c. 执行命令**quit**，返回系统视图。
  d. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  e. 执行命令**igmp query ip-source-policy** { *basic-acl-number* | **acl-name** *acl-name* }，配置IGMP Query报文的源地址过滤，从而控制查询器的选举。

     说明

     - 如果匹配上ACL规则，动作是**permit**，则接口接收此范围内的IGMP Query报文。
     - 如果匹配上ACL规则，动作是**deny**，则接口拒绝接收此范围内的IGMP Query报文。
     - 如果没有匹配上ACL规则，则接口拒绝接收此范围内的IGMP Query报文。
     - 如果引用的ACL不存在或者ACL下的rule不存在，则接口拒绝接收所有的IGMP Query报文。
  f. 执行命令**commit**，提交配置。
- 配置MLD Report或Done报文源地址过滤策略。
  a. 执行命令**system-view**，进入系统视图。
  b. 配置基本数字或命名ACL6，请根据情况选择如下配置之一：
     - 配置基本数字ACL6：
       1) 执行命令**acl ipv6** [**number**] *basic-acl6-number* [**match-order** { **auto** | **config** }]，创建基本数字ACL6，并进入相应的ACL6视图。
       2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } [**fragment** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address*|*prefix-length* | **any** }] *，配置基本数字ACL6规则。
     - 配置命名ACL6：
       1) 执行命令**acl ipv6 name** *acl6-name* **basic** [**match-order** { **auto** | **config** }]，创建命名ACL6，并进入相应的ACL6视图。
       2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } [**fragment** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address*|*prefix-length* | **any** }] *，配置命名ACL6规则。

c. 执行命令**quit**，返回系统视图。

d. 执行命令**interface** *interface-type interface-number*，进入接口视图。

e. 执行命令**mld ip-source-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* }，配置MLD Report或Done报文源地址过滤。

说明

- 如果匹配上ACL规则，动作是**permit**，则接口接收此范围内的MLD Report或Done报文。
- 如果匹配上ACL规则，动作是**deny**，则接口拒绝接收此范围内的MLD Report或Done报文。
- 如果没有匹配上ACL规则，则接口拒绝接收此范围内的MLD Report或Done报文。
- 如果引用的ACL不存在或者ACL下的rule不存在，则接口拒绝接收所有的MLD Report或Done报文。

f. 执行命令**commit**，提交配置。

- 配置MLD Query报文源地址过滤策略。

a. 执行命令**system-view**，进入系统视图。

b. 配置基本数字或命名ACL6，请根据情况选择如下配置之一：

- 配置基本数字ACL6：
  1) 执行命令**acl ipv6** [**number**] *basic-acl6-number* [**match-order** { **auto** | **config** }]，创建基本数字ACL6，并进入相应的ACL6视图。
  2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } [**fragment** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address*/*prefix-length* | **any** }] *，配置基本数字ACL6规则。
- 配置命名ACL6：
  1) 执行命令**acl ipv6 name** *acl6-name* **basic** [**match-order** { **auto** | **config** }]，创建命名ACL6，并进入相应的ACL6视图。
  2) 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } [**fragment** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address*/*prefix-length* | **any** }] *，配置命名ACL6规则。

c. 执行命令**quit**，返回系统视图。

d. 执行命令**interface** *interface-type interface-number*，进入接口视图。

e. 执行命令**mld query ip-source-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* }，配置MLD Query报文的源地址过滤，从而控制查询器的选举。

说明

- 如果匹配上ACL规则，动作是**permit**，则接口接收此范围内的MLD Query报文。
- 如果匹配上ACL规则，动作是**deny**，则接口拒绝接收此范围内的MLD Query报文。
- 如果没有匹配上ACL规则，则接口拒绝接收此范围内的MLD Query报文。
- 如果引用的ACL不存在或者ACL下的rule不存在，则接口拒绝接收所有的MLD Query报文。

f. 执行命令**commit**，提交配置。

- 配置全局IGMP IPSec

– 配置IGMP协议报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**igmp** [**vpn-instance** *vpn-instance-name*]，进入IGMP视图。

c. 执行命令**ipsec sa** *sa-name*，配置全局IGMP IPSec，发送和接收IGMP报文时按指定的安全联盟对报文进行认证检查。

d. 执行命令**commit**，提交配置。

– 配置IGMP Query报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**igmp** [**vpn-instance** *vpn-instance-name*]，进入IGMP视图。

c. 执行命令**query ipsec sa** *sa-name*，配置全局IGMP IPSec，发送和接收IGMP Query报文时按指定的安全联盟对报文进行认证检查。

d. 执行命令**commit**，提交配置。

说明

命令**ipsec sa**与命令**query ipsec sa**相互覆盖，即最后配置的命令才生效。

- 配置接口IGMP IPSec

– 配置IGMP协议报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**igmp ipsec sa** *sa-name*，在接口上配置IGMP IPSec，使该接口发送和接收IGMP报文时按照指定的安全联盟对报文进行认证检查。

d. 执行命令**commit**，提交配置。

– 配置IGMP Query报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**igmp query ipsec sa** *sa-name*，在接口上配置IGMP IPSec，使该接口发送和接收IGMP Query报文时按照指定的安全联盟对报文进行认证检查。

d. 执行命令**commit**，提交配置。

说明

命令**igmp ipsec sa**与命令**igmp query ipsec sa**相互覆盖，即最后配置的命令生效。

- 配置全局MLD IPSec

– 配置MLD协议报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**mld**，进入MLD视图。

c. 执行命令**ipsec sa** *sa-name*，配置全局MLD IPSec，发送和接收MLD报文时按指定的安全策略对报文进行认证检查。

d. 执行命令**commit**，提交配置。

– 配置MLD Query报文使用IPSec安全认证

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**mld**，进入MLD视图。

c. 执行命令**query ipsec sa** *sa-name*，配置全局MLD IPSec，发送和接收MLD Query报文时按指定的安全策略对报文进行认证检查。

d. 执行命令**commit**，提交配置。

说明

命令**ipsec sa**与命令**query ipsec sa**相互覆盖，即最后配置的命令才生效。

- 配置接口MLD IPSec
  - 配置MLD协议报文使用IPSec安全认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**mld ipsec sa** *sa-name*，在接口上配置MLD IPSec，使该接口发送和接收MLD报文时按照指定的安全策略对报文进行认证检查。
  d. 执行命令**commit**，提交配置。
  - 配置MLD Query报文使用IPSec安全认证
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**mld query ipsec sa** *sa-name*，在接口上配置MLD IPSec，使该接口发送和接收MLD Query报文时按照指定的安全策略对报文进行认证检查。
  d. 执行命令**commit**，提交配置。

说明

命令**mld ipsec sa**与命令**mld query ipsec sa**相互覆盖，即最后配置的命令生效。

- 配置PIM的白名单Session-CAR功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**whitelist session-car pim** { **cir** *cir-value* | **cbs** *cbs-value* | **pir** *pir-value* | **pbs** *pbs-value* } *，配置PIM的白名单Session-CAR功能的参数值。
  c. （可选）执行命令**whitelist session-car pim disable**，去使能PIM的白名单Session-car功能。

     当功能异常或者影响其它业务时，则关闭此功能。正常情况下，建议保持开启PIM的白名单Session-CAR功能。
  d. 执行命令**commit**，提交配置。
- 配置IPv6 PIM的白名单Session-CAR功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**whitelist session-car pim-ipv6** { **cir** *cir-value* | **cbs** *cbs-value* | **pir** *pir-value* | **pbs** *pbs-value* } *，配置IPv6 PIM的白名单Session-CAR功能的参数值。
  c. （可选）执行命令**whitelist session-car pim-ipv6 disable**，去使能IPv6 PIM的白名单Session-car功能。

     当功能异常或者影响其它业务时，则关闭此功能。正常情况下，建议保持开启IPv6 PIM的白名单Session-CAR功能。
  d. 执行命令**commit**，提交配置。
- 配置MSDP的白名单Session-CAR功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**whitelist session-car msdp** { **cir** *cir-value* | **cbs** *cbs-value* | **pir** *pir-value* | **pbs** *pbs-value* } *，配置MSDP的白名单Session-CAR功能的参数值。

c. （可选）执行命令**whitelist session-car msdp disable**，去使能MSDP的白名单Session-car功能。

当功能异常或者影响其它业务时，则关闭此功能。正常情况下，建议保持开启MSDP的白名单Session-CAR功能。

d. 执行命令**commit**，提交配置。

- 配置IGMP的微隔离协议CAR功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**micro-isolation protocol-car igmp** { **cir** *cir-value* | **cbs** *cbs-value* | **pir** *pir-value* | **pbs** *pbs-value* } *，配置IGMP的微隔离CAR的参数值。

  正常情况下，建议使用默认参数。*pir-value*应该大于等于*cir-value*，*pbs-value*应该大于等于*cbs-value*。
  c. （可选）执行命令**micro-isolation protocol-car igmp disable**，去使能IGMP的微隔离CAR功能。

  正常情况下，建议保持开启IGMP的微隔离CAR功能。
  d. 执行命令**commit**，提交配置。
- 配置MLD的微隔离协议CAR功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**micro-isolation protocol-car MLD** { **cir** *cir-value* | **cbs** *cbs-value* | **pir** *pir-value* | **pbs** *pbs-value* } *，配置MLD的微隔离CAR的参数值。

  正常情况下，建议使用默认参数。*pir-value*应该大于等于*cir-value*，*pbs-value*应该大于等于*cbs-value*。
  c. （可选）执行命令**micro-isolation protocol-car MLD disable**，去使能MLD的微隔离CAR功能。

  正常情况下，建议保持开启MLD的微隔离CAR功能。
  d. 执行命令**commit**，提交配置。

----结束

配置维护建议

无

检查加固结果

- 执行命令**display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看PIM接口信息。
- 执行命令**display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **neighbor** [**interface** *interface-type interface-number* | *neighbor-address* | **verbose**] *，查看PIM邻居信息。
- 执行命令**display mld interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看接口的配置信息。
- 执行命令**display igmp** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number* | **up** | **down**] **verbose**命令，查看接口的配置信息。

- 执行命令**display cpu-defend whitelist-v6 session-car pimv6 statistics slot** *slot-id*，查看IPv6 PIM的白名单Session-CAR当前的各单板生效情况。
- 执行命令**display cpu-defend whitelist session-car msdp resource slot** *slot-id*，查看指定接口板的MSDP的白名单Session-car统计信息。

?.2. 二层组播

介绍二层组播的安全策略、攻击方法、配置维护方法及配置维护建议。

安全策略介绍

- L2MC可以通过group-policy，设定组策略，用来限定某个VLAN或某个接口下允许哪些组播组（组播源组）的加入。
- L2MC可以通过ip-policy，设定基于源IP（IP头中源IP地址，即用户的主机IP地址）的策略，用来限定某个VLAN/VSI下允许哪些源IP的加入。
- L2MC可以通过设置端口不学习，设定不通过协议报文学习端口。

攻击方法介绍

网络上可以通过伪造IGMP/MLD报文的形式攻击，可通过配置组播组策略、源策略，将伪造报文丢弃。可能的攻击方式如下：

- 恶意用户通过变换组地址加入，使用一些无效组播组频道加入，造成设备上建立大量无效表项，占用大量系统资源，导致正常用户的点播无法成功；可以通过设置组播组策略，允许用户加入的组播组范围。
- 变换用户源IP地址攻击，可以通过设置源IP策略，限制合法的源IP地址范围。
- Query报文攻击，让设备建立组播端口，接收所有组播组的流量，造成大量流量通过该用户所在的端口发出，对接口带宽消耗很大；可以通过配置静态端口配置，并且设定不通过协议报文学习端口。

配置维护方法

- 基于VLAN/VSI配置**igmp-snooping group-policy**，设置组播组策略。
- 基于VLAN/VSI配置**igmp-snooping ip-policy**，设置源IP策略。
- 基于VLAN/VSI配置**undo igmp-snooping router-learning**，设置路由器端口不学习。

配置维护建议

根据业务部署，建议针对IPTV的组播组地址范围，配置VLAN/VSI的group-policy。

- 在VLAN/VSI视图下配置：**igmp-snooping group-policy** *acl-number*。
- 在ACL 2000视图下配置对应IPTV组范围：**rule** [*rule-id*] { **deny** | **permit** } **source** *source-ip-address source-wildcard*。

检查加固结果

- 执行命令**display igmp-snooping** [**vlan** [*vlan-id*] | **vsi** [*vsi-name*]] **configuration**，查看IGMP Snooping的配置信息。
- 执行命令**display igmp-snooping** [**vlan** [*vlan-id*] | **vsi** [*vsi-name*]]，查看IGMP Snooping的运行参数信息。

- 执行命令**display igmp-snooping router-port** [**vlan** [*vlan-id*] | **vsi** [*vsi-name*]]，查看设备端口信息。

VRRP

安全策略介绍

- 协议安全策略：
  - 认证方式：VRRP支持的认证方式有无认证、简单文本认证（仅组播VRRP支持）、HMAC-MD5以及HMAC-SHA256（仅单播VRRP支持）的增强认证。
  - 报文校验：对备份组号、校验和、TTL、版本号、报文类型检测、定时器检测、虚拟地址个数、虚拟地址和报文长度检测。
- 系统安全策略：

  攻击报文抑制：如果单位时间内收到的报文数量大于20个或者为本机发出的报文，就认为该报文为攻击报文，直接丢弃。

攻击方法介绍

- 单位时间内发送大量的正确的VRRP协议报文对设备进行攻击。
- 构造不满足VRRP协议安全策略中的报文校验要求的VRRP协议报文对设备进行攻击。

配置维护方法

- 认证方式：VRRP可以选择无认证方式、Simple认证方式（仅组播VRRP支持）、HMAC-MD5认证方式、HMAC-SHA256认证方式（仅单播VRRP支持）。其中Simple认证方式可以选择简单密码保存和密文密码保存，HMAC-MD5认证和HMAC-SHA256默认为密文方式保存。
- 报文校验：该功能是默认支持的功能，不需要进行额外配置。

配置维护建议

认证方式：非单播VRRP建议选择HMAC-MD5安全认证以增加协议的安全性，单播VRRP建议选择HMAC-SHA256安全认证以增加协议的安全性。

检查加固结果

执行命令**display vrrp** [**interface** { *interface-name* | *interface-type interface-number* }] [*virtual-id*] **verbose**，查看示VRRP报文认证的配置信息。

E-TRUNK

介绍E-TRUNK的安全策略、攻击方法、配置维护方法及配置维护建议。

安全策略介绍

- 为了提高系统的安全性，E-Trunk提供可配置认证的功能。E-Trunk在发送端将心跳报文使用设置的密码进行报文摘要的计算，在接收端收到心跳报文之后计算重新计算报文摘要进行校验，如果摘要一致则认为合法，否则丢弃报文。
- 为了防止攻击者获取E-Trunk的报文特征信息重放攻击，导致对业务流量的影响，E-Trunk提供可配置序列号校验功能。缺省情况下，序列号校验功能关闭。为了保

证系统安全和流量正常转发，可通过命令sequence enable手动配置E-Trunk序列号校验功能，识别非法攻击报文。

- 在收到错误报文时，E-Trunk会对报文进行报文长度、报文摘要、以及重要参数进行合法性检查，不合法的报文将被丢弃。
- E-Trunk默认使用UDP 1025端口号收发协议报文。为提高安全性，E-Trunk提供可配置端口号的功能，让用户调整E-Trunk协议报文的端口号。

攻击方法介绍

- 采用配置协议认证的方式防范攻击。为了防止被攻击，认证算法可采用HMAC-SHA1、HMAC-SHA256加密方式或ENHANCED-HMAC-SHA256。
- 采用配置序列号校验功能防范攻击。可通过命令sequence enable手动配置E-Trunk序列号校验功能。

配置维护方法

1. 在E-Trunk视图下，通过命令**authentication-mode**配置E-Trunk的认证加密方式。
2. 在E-Trunk视图下，配置认证命令。命令行为：**security-key** { **simple** *simple-key* | **cipher** { *cipher-key1* | *cipher-key2* | *cipher-key3* } }。

   用户可以选择采用明文加密或密文加密：

   - 明文加密时，在配置文件中采用明文形式显示。
   - 密文加密时，在配置文件中采用加密后的乱码显示，不显示真正的密码。
     - *cipher-key1*：密码以密文形式输入，密码长度必须是32～432个连续字符串。
     - *cipher-key2*：如果升级前版本支持设置长度为24的密文密码，则升级时会自动兼容。
     - *cipher-key3*：密码以明文形式输入，字符串形式，区分大小写，不支持空格，长度范围是1～255。

   须知

   如果使用simple选项，密码将以明文形式保存在配置文件中，以低级别登录的用户可以通过查看配置方式获取密码，造成安全隐患。因此，建议使用cipher选项，将密码加密保存。

   E-Trunk中的两台设备上的加密密码必须配置一致。用户创建Etrunk后，需要手工配置加密密钥，否则Etrunk无法正常协商。

3. 在E-Trunk视图下，通过命令**sequence enable**配置使能序列号校验功能。

   须知

   E-Trunk的主用和备用设备需要都通过命令**sequence enable**进行配置，否则仅一台设备配置该功能会导致序列号校验失败并丢弃报文，使得E-Trunk的两台设备都成为主用设备。

4. 在系统视图下，配置E-Trunk的端口号。命令为：**e-trunk port** *port-number*，端口号可在1025～65535间配置，默认为1025。

配置维护建议

为增强安全性，建议配置为cipher类型的密文。

推荐使用ENHANCED-HMAC-SHA256的认证加密方式。

推荐在E-Trunk的两端使能序列号校验功能。

检查加固结果

执行命令**display e-trunk** *etrunk-id*，查看E-Trunk的详细信息。

MSTP

安全策略介绍

- Root protection

  对于启用根保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用根保护功能的指定端口收到优先级更高的RST BPDU时，端口状态将进入Discarding状态，不再转发报文。在经过一段时间（通常为两倍的Forward Delay），如果端口一直没有再收到优先级较高的RST BPDU，端口会自动恢复到正常的Forwarding状态。

- BPDU protection

  设备上启动了BPDU保护功能后，如果边缘端口收到RST BPDU，边缘端口将被shutdown，但是边缘端口属性不变，同时通知网管系统。

- TC protection

  启用防TC-BPDU报文攻击功能后，在单位时间内，设备处理拓扑变化报文的次数可配置。如果在单位时间内，设备在收到拓扑变化报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的拓扑变化报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁的删除MAC地址表项和ARP表项，从而达到保护设备的目的。

- Loop protection

  在启动了环路保护功能后，如果根端口或Alternate端口长时间收不到来自上游的RST BPDU，则向网管发出通知信息（如果是根端口则进入Discarding状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到RST BPDU，端口状态才恢复正常到Forwarding状态。

攻击方法介绍

- Root bridge change attack

  由于维护人员的错误配置或网络中的恶意攻击，根桥收到优先级更高的BPDU，会失去根桥的地位，重新进行生成树的计算，并且由于拓扑结构的变化，可能造成高速流量迁移到低速链路上，引起网络拥塞。

- BPDU attack

  边缘端口在收到BPDU以后端口状态将变为非边缘端口，此时就会造成生成树的重新计算，如果攻击者伪造配置消息恶意攻击设备，就会引起网络震荡。

- TC protection

  设备在接收到拓扑变化报文后，会执行MAC地址表项和ARP表项的删除操作，如果频繁操作则会对CPU的冲击很大。

- Loop protection

  当出现链路拥塞或者单向链路故障，根端口和Alternate端口会老化。根端口老化，会导致系统重新选择根端口（而这有可能是错误的），Alternate端口老化，将迁移到Forwarding状态，这样会产生环路。

配置维护建议

- 根保护

  指定端口使能根保护。

- BPDU保护

  在系统视图下配置BPDU保护。

- TC保护

  在系统视图下配置TC保护。

- 环路保护

  根端口和Alternate端口使能环路保护。

检查加固结果

- 使用命令**display stp** [**instance** *instance-id*][**interface** { *interface-type interface-number* }] [**brief**]，查看生成树的状态信息与统计信息。
- 执行命令**display stp region-configuration**，查看已经生效的MST域的配置信息。
- 执行命令**display stp region-configuration digest**，查看已经生效的MST域配置的摘要。

DSVPN

安全策略介绍

NHRP协商认证

NHRP（Next Hop Resolution Protocol）在DSVPN中用于解决公共网络上的源Spoke如何动态获取目的Spoke公网地址的问题。分支Spoke接入公网时使用当前物理接口的公网地址向总部Hub发送NHRP注册请求进行注册，总部Hub根据这些请求信息，创建或刷新NHRP peer表。Spoke间通过NHRP地址解析请求和应答，创建和刷新NHRP peer表。

为了防止分支节点在总部节点进行非法注册，可以开启分支节点和总部节点之间的NHRP协商认证。当分支节点在总部节点注册时，根据注册请求报文中的认证字符串来判定总部节点是否处理该注册报文。如果总部节点上配置的认证字符串与注册请求报文中的认证字符串不一致，则总部节点不会处理该分支的注册请求；如果总部节点上配置的认证字符串与注册请求报文中的认证字符串一致，总部节点则会处理该分支的注册请求。

DSVPN IPSec保护

当企业需要对总部和分支机构以及分支机构间传输的数据进行加密保护的时候，可以在部署DSVPN的同时绑定IPSec安全框架，实现分支间同时动态建立起mGRE隧道和IPSec隧道：

- mGRE隧道建立的同时会立即触发IPsec隧道建立。
- 普通IPSec技术使用ACL识别待加密的单播流量。在IPSec安全策略下，需进行复杂的ACL定义，实施困难。DSVPN使用NHRP和mGRE技术，与IPSec联合部署时可以简化设备的配置，使得数据传输的安全性得到保障的同时，网络部署更加简单。
- 由于动态建立了分支机构间的IPSec隧道，使得分支Spoke间的IPSec数据交互不用通过总部Hub进行解密和加密操作，降低了数据传输时延。

攻击方法介绍

- 侦听分支与总部之间、分支与分支之间传输的数据。
- 仿冒合法分支节点向总部节点注册。总部节点接收来自分支节点的注册，因此如果有分支节点进行非法注册，则会占用NHRP表项资源，导致其超过资源限定值，最终使得超限的表项被丢弃。

操作步骤

- 配置NHRP协商认证

  请在分支Spoke和总部Hub上进行如下配置。

  a. 配置总部Hub。

     i. 执行命令**system-view**，进入系统视图。

     ii. 执行命令**nhrp enable**，全局使能nhrp。

     iii. 执行命令**interface tunnel** *interface-number*，进入Tunnel接口视图。

     iv. 执行命令**nhrp enable**，接口使能NHRP。

     v. （可选）执行命令**nhrp network-id** *netId*，配置接口所属NHRP域。

     vi. 执行命令**nhrp entry multicast dynamic**，配置NHRP组播成员表。

     vii. 执行命令**nhrp authentication** [**hash** { **sha2-256** | **sha2-384** | **sha2-512** }] **cipher** *authenString*，配置NHRP协商的认证字符串。

     viii. （可选）执行命令**nhrp entry holdtime** *holdtime*，配置NHRP表项保持时长。

     ix. （可选）执行命令**nhrp redirect**，使能NHRP redirect功能。

     只在DSVPN采用shortcut方式时配置，此时总部节点转发同一DSVPN的分支流量时会向源分支节点发送nhrp redirect报文，触发源分支发起NHRP地址解析请求，建立隧道进行分支间直接通信。

     x. 执行命令**commit**，提交配置。

  b. 配置分支Spoke。

     i. 执行命令**system-view**，进入系统视图。

     ii. 执行命令**nhrp enable**，全局使能nhrp。

     iii. 执行命令**interface tunnel** *interface-number*，进入Tunnel接口视图。

     iv. 执行命令**nhrp enable**，接口使能NHRP。

     v. （可选）执行命令**nhrp network-id** *netId*，配置接口所属NHRP域。

vi. 可选）执行命令**nhrp shortcut**，shortcut场景DSVPN时，在分支节点上需要使能nhrp shortcut功能。

vii. 执行命令**nhrp entry multicast dynamic**，配置NHRP组播成员表。

viii. 执行命令**nhrp entry** *protocol-address nbma-address* [**register**]配置NHRP地址映射表。

ix. （可选）执行命令**nhrp registration no-unique**，配置设备发送的NHRP报文携带no-unique标志，通知对端覆盖冲突的NHRP peer表项。

x. 执行命令**nhrp authentication** [**hash** { **sha2-256** | **sha2-384** | **sha2-512** }] **cipher** *authenString*，配置NHRP协商的认证字符串。

说明

如果总部Hub执行了该配置，分支Spoke必须执行该配置。

xi. （可选）执行命令**nhrp registration interval** *regInterval*，配置NHRP注册间隔。

xii. （可选）执行命令**nhrp entry holdtime** *holdtime*，配置NHRP表项保持时长。

xiii. 执行命令**commit**，提交配置。

- 配置DSVPN IPSec保护

a. 请参考配置IKE安全提议。

b. 请参考配置IKE对等体。

c. （可选）配置IKE过滤集。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**ike identity** *name*，配置进行IKE协商时本机的过滤集，并进入IKE对等体过滤集视图。

iii. 执行命令**ip address** *ip-address* { *mask* | *mask-length* }，配置指定允许接入的IKE对等体的IP地址。

iv. 执行命令**fqdn** *fqdn*，配置指定允许接入的IKE对等体的域名。

v. 执行命令**user-fqdn** *user-fqdn*，配置指定允许接入的IKE对等体的主机域名。

vi. 执行命令**dn** *dn*，配置指定允许接入的IKE对等体的数字证书可识别名。

vii. 执行命令**quit**，退出IKE过滤集视图。

viii. 执行命令**commit**，提交配置。

d. 配置IPSec安全框架。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**ipsec policy** *policy-name* **profile**，配置进入IPSec安全框架视图。

iii. 执行命令**proposal** *proposal-name* ，引用安全提议。

iv. 执行命令**ike-peer** *peer-name*，引用IKE Peer。

v. （可选）执行命令**pfs** { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** | **group15** | **group16** | **dh-group19** | **dh-group20** | **dh-group21** }，配置协商时使用的PFS特性。如果本端配置了PFS，对端在发起协商时必须为PFS交换。本端和对端指定的DH组必须一致，否则协商失败。

vi. （可选）执行命令**remote ike-identity** *name*，配置指定允许接入的IKE对等体过滤集。

说明

当IPSec安全框架中引用之前定义的IKE过滤集（ike identity）时，协商根据IKE过滤集进行过滤，否则不进行过滤。

vii. 执行命令**quit**，退出IPSec安全框架视图。

viii. 执行命令**commit**，提交配置。

e. 应用IPSec安全框架。

请参考应用IPSec安全策略。

----结束

检查加固结果

- 执行**display nhrp peer**命令，查看NHRP peer表信息。
- 执行**display ipsec sa**命令，查看当前安全联盟的配置信息。

BFD

介绍BFD的安全策略、攻击方法、配置维护方法及配置维护建议。

安全策略介绍

- 为了提高系统的安全性，BFD提供可配置的协商报文认证功能。支持静态组播BFD协商报文认证、BFD for IP单跳会话协商报文认证、BFD for IP多跳会话协商报文认证、BFD for LSP主动会话协商报文认证、BFD for LSP被动会话协商报文认证。
- 发送端和接收端需要配置相同的认证方式，**key-id**字段，认证密码和认证超时间隔。
  - 其中*key-id*为1～255的整数。
  - 当认证密码为明文形式时，长度范围是1～20；当认证密码为密文形式时，长度范围是20～148。
  - 静态组播BFD报文认证协商超时时间范围为1～10000秒。
- 配置协商报文认证后，BFD的报文头中A标记置为1，净荷增加28字节认证字段。
- 接收端解封装报文，报文头中A标记与本地设备不一致则丢弃报文；A标记一致时，将认证字段取出与本端配置的比对，不一致则认为错误。
- 认证密码有两种配置方式，明文模式和密文模式，两种模式配置文件中均显示为密文。

攻击方法介绍

伪造BFD报文进行转发或上送。

配置维护方法

- 在BFD会话视图配置认证功能，仅支持静态组播BFD会话和组播auto会话。

  执行命令**authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet** [**enhanced**] [**timeout-interval** <*interval-value*>]，配置BFD会话认证功能。

  在特定接入场景下，如组播BFD联动接口协议状态时，在此BFD会话下配置认证功能，只有两端BFD认证信息一致，才能协商成功，BFD联动的接口协议状态才能激活，用户才能通过此接口接入到设备。

- 在BFD视图可配置BFD for IP单跳会话协商报文认证、BFD for IP多跳会话协商报文认证、BFD for LSP主动会话协商报文认证和BFD for LSP被动会话协商报文认证。
  - 执行命令**bfd single-hop peer-ip** *ip-address* [**vpn-instance** *vpn-name*] **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置BFD for IPv4单跳会话协商报文认证。
  - 执行命令**bfd single-hop peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-name*] **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置BFD for IPv6单跳会话协商报文认证。
  - 执行命令**bfd multi-hop peer-ip** *ip-address* [**vpn-instance** *vpn-name*] **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置BFD for IPv4多跳会话协商报文认证。
  - 执行命令**bfd multi-hop peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-name*] **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置BFD for IPv6多跳会话协商报文认证。
  - 执行命令**bfd mpls-passive peer-ip** *ip-address* **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置BFD for LSP被动会话协商报文认证。
  - 执行命令**bfd lsp-tunnel peer-ip** *ip-address* **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置BFD for LSP主动会话协商报文认证。

配置维护建议

为增强安全性，在安全要求高的网络中，可以启用BFD协商报文认证功能。

检查加固结果

执行命令**display current-configuration configuration bfd**，查看BFD的配置情况。

SBFD

介绍SBFD的安全策略、攻击方法、配置维护方法及配置维护建议。

安全策略介绍

- 为了提高系统的安全性，SBFD提供可配置的协商报文认证功能。支持SBFD for IP场景的SBFD会话协商报文认证、SBFD for LSP/Tunnel场景的SBFD会话协商报文认证、SBFD for SR-MPLS TE Policy场景SBFD会话协商报文认证、SBFD for SRv6 TE Policy 场景SBFD会话协商报文认证。
- 仅SBFD发起端需要配置认证，key-id字段，认证密码。
  - 其中*key-id*为1～255的整数。
  - 当认证密码为明文形式时，长度范围是1～20；当认证密码为密文形式时，长度范围是20～148。
- 配置协商报文认证后，SBFD的报文头中A标记置为1，净荷增加28字节认证字段。
- SBFD发起端解封装报文，报文头中A标记与本地设备不一致则丢弃报文；A标记一致时，将认证字段取出与本端配置的比对，不一致则认为错误。
- SBFD反射端不支持对报文进行认证校验。
- 认证密码有两种配置方式，明文模式和密文模式，两种模式配置文件中均显示为密文。

攻击方法介绍

伪造SBFD报文进行转发或上送。

配置维护方法

在SBFD视图，根据业务场景配置SBFD会话协商报文认证。

- 执行命令**sbfd multi-hop peer-ipv6** *ipv6-address* **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置SBFD for IPv6多跳会话协商报文认证。
- 执行命令**sbfd lsp-tunnel peer-ip** *ip-address* **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置SBFD for LSP/Tunnel会话协商报文认证。
- 执行命令**sbfd sr-te-policy segment-list endpoint** *endpoint-address* **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置SBFD for SR-MPLS TE POLICY segmentlist会话协商报文认证。
- 执行命令**sbfd srv6-te-policy segment-list endpoint** *endpoint-address* **authentication-mode met-sha1 key-id** *key-id-value* **cipher** *cipher-text* **nego-packet**，配置SBFD for SRV6 TE POLICY segmentlist会话协商报文认证。

配置维护建议

为增强安全性，在安全要求高的网络中，可以启用SBFD协商报文认证功能。

检查加固结果

执行命令**display current-configuration configuration bfd**，查看SBFD的配置情况。

IP FPM

介绍IP FPM的安全策略、攻击方法、配置维护方法及配置维护建议。

说明

安全策略介绍

为了提高系统的安全性，IP FPM提供可配置的报文认证功能。通过在MCP和DCP上配置相同的认证模式和认证密码，MCP只接收通过认证的DCP发送的报文，从而提高网络的安全性和网络性能统计的可靠性。执行命令**authentication-mode hmac-sha256 key-id** *key-id* [**cipher**] *password*，可以在IP FPM统计实例上配置认证模式和认证密码，其中：

- 发送端和接收端需要配置相同的认证密码：
  - *key-id*取值为1～64的整数。
  - 当认证密码为明文形式时，长度范围是1～255；当认证密码为密文形式时，长度范围是24或32～432。
- 配置报文认证后，DCP发送的报文中增加认证数据段。
- MCP接收端解封装报文，报文中解析出的认证密文与本地设备不一致则丢弃报文；一致时，继续解析丢包时延数据部分。

- 认证密码有明文模式和密文模式两种配置方式，两种模式在配置文件中均显示为密文。

攻击方法介绍

伪造IP FPM报文进行转发或上送。

配置维护方法

- 在IPFPM DCP视图下配置认证功能：

  执行命令**authentication-mode hmac-sha256 key-id** *key-id* [**cipher**] *password*，若IPFPM DCP实例视图下没有配置认证密码，IPFPM DCP视图下配置了认证密码，则使用IPFPM DCP视图下配置的认证密码。只有当两端DCP和MCP认证信息一致时，MCP才能正常解析报文。
- 在IPFPM DCP实例视图下配置认证功能：

  执行命令**authentication-mode hmac-sha256 key-id** *key-id* [**cipher**] *password*，若IPFPM DCP实例视图下配置了认证密码，IPFPM DCP视图下也配置了认证密码，则使用IPFPM DCP实例视图下配置的认证密码。只有当两端DCP和MCP认证信息一致时，MCP才能正常解析报文。
- 在IPFPM MCP视图下配置认证功能：

  执行命令**authentication-mode hmac-sha256 key-id** *key-id* [**cipher**] *password*，只有当两端DCP和MCP认证信息一致时，MCP才能正常解析报文。

检查加固结果

使用**display ipfpm dcp**和**display ipfpm mcp**命令查看IP FPM安全认证的配置情况。

配置维护建议

为增强安全性，在安全要求高的网络中，可以启用IP FPM报文认证功能。

PPP

安全策略介绍

协议安全策略：认证方式PPP协议也提供了可选的认证配置参数选项，认证协议支持PAP（Password Authentication Protocol）和CHAP（Challenge Hand Authentication Protocol），并且支持简单口令配置方式以及密文密码配置方式。

攻击方法介绍

单位时间内发送大量的正确的PPP协议报文对设备进行攻击。

配置维护方法

- 认证方式：可以选择无认证方式，PAP认证方式，CHAP认证方式。
- 报文校验：该功能是默认支持的功能，不需要进行额外配置。

配置维护建议

认证方式：建议选择CHAP安全认证以增加协议的安全性。

检查加固结果

使用**display interface** [*interface-type* [*interface-number*]]命令查看接口的配置和运行状态。

IPv6 协议栈

?.1. IPv6 安全邻居发现

安全策略介绍

IPv6安全邻居发现功能SEND（SEcure Neighbor Discovery）特性用来解决在邻居发现协议NDP（Neighbor Discovery Protocol）中涉及的安全问题。

在IPv6的协议族中，ND（Neighbor Discovery）用来保证本链路内邻居的可达性，具有举足轻重的地位。随着网络安全问题的日益突出，为应对这些威胁，相关标准SEND（Secure Neighbor Discovery）对ND协议进行了扩展。SEND定义了CGA地址和CGA选项、RSA选项，用来验证ND消息的发送者对消息源地址的合法拥有权。SEND还定义了Timestamp和Nonce选项用来防止重放攻击。

- CGA地址（Cryptographically Generated Address）：IPv6地址的接口ID部分由公钥和附加参数，使用单向hash函数计算生成。
- CGA选项：包含接收方在验证发送方的CGA地址时需要的一些信息，包括发送方的公钥等。用来验证ND报文的发送者是其IPv6源地址的合法拥有者。
- RSA签名选项（Rivest Shamir Adleman）：包含发送方公钥的hash值，以及根据发送方私钥和ND报文，使用算法生成的数字签名。用来验证ND报文的完整性和发送者的真实性。

  说明

  当攻击者声称其为某地址的拥有者时（实际上此地址属于某合法节点），它必须使用合法节点的公钥进行加密，否则接收者可以通过CGA选项的校验发现其攻击行为，即使攻击者获取到了合法节点的公钥，但接收者通过对数字签名的校验，可以发现其攻击行为，因为攻击者也许并不知道消息发送者用来制作数字签名的私钥。
- 时间戳选项（Timestamp）：包含一个时间戳的64位无符号整数，表示从1970年1月1号零时（UTC）以来的秒数。用来保护非请求的通告报文和重定向报文不会被重放。接收者应确保每个收到的报文其时间戳都比上一个收到的报文要新。
- 随机数选项（Nonce）：包含了由请求消息的发送者所生成的一个随机数。用来在请求和回应交互中防止重放攻击，比如在NS和NA报文的交互中，NS报文中携带Nonce选项，回应的NA报文中也携带此选项，发送者根据收到的选项判断是否为合法的回应报文。

攻击方法介绍

针对ND的安全性问题，相关标准总结了若干种威胁类型，例举如下：

表 1-11 IPv6 ND 攻击

攻击方法	说明
NS/NA欺骗	攻击者向合法节点（主机或者路由器）发送包含不同源链路层地址选项的NS报文，或者包含不同目标链路层地址选项的NA报文，通过NS/NA欺骗，使合法节点的报文发往其他的链路层地址达到攻击的目的。
邻居不可达探测（NUD）失败	攻击者连续不断的发送伪造的NA报文来响应NUD检测中合法节点发送的NS报文，使得合法节点无法探测到邻居节点不可达。这种攻击的后果取决于邻居节点不可达的原因，以及节点在知道邻居节点不可达后所采取的具体行为。
DAD攻击	攻击者对每个接入网络的主机所发送的重复地址检测（DAD）都进行响应，宣称拥有DAD检测的地址，使主机无法获得该地址。
虚假的重定向报文	攻击者使用当前第一跳路由器的链路本地地址向合法主机发送重定向消息，使合法主机将该重定向消息误认为是来自第一跳路由器的消息，从而接收该重定向消息。
重放攻击	攻击者通过捕获合法的消息并且不断重放这些消息来达到攻击的目的。所以，即使NDP消息受到签名或证书的保护而使得其内容不能被伪造，但还是会受到重放攻击。
虚假的直连前缀攻击	攻击者发送伪造的RA报文指定某些地址前缀是直连的，使得主机不再向路由器发送这个地址前缀的报文。相反，该主机将试图通过发送NS报文来执行地址解析，但是实际上NS报文将不会被响应，主机将会受到拒绝服务的攻击。
恶意的最后一跳路由器	攻击者向试图发现合法的最后一跳路由器的主机发送伪造的多播RA报文，或者对该主机发送的多播RS报文回应伪造的单播RA报文，使主机将攻击者误认为最后一跳路由器。一旦主机选择攻击者作为它的缺省路由器，攻击者就可以拦截通讯双方的通话并插入新的内容。

配置维护方法

- 配置CGA类型的IPv6地址

  当需要实现IPv6安全邻居发现功能时，需要先在接口上配置CGA类型的IPv6地址，从而该接口发送的ND报文就会携带CGA和RSA选项，对端收到报文后，通过CGA和RSA选项判断发送者的合法性、报文的完整性。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**rsa key-pair label** *label-name* **modulus** *modulus-bits*，创建RSA密钥。
  c. 执行命令**interface** *interface-type interface-number*，进入要配置CGA类型的IPv6地址的接口视图。
  d. 执行命令**ipv6 security rsakey-pair** *key-label*，将RSA密钥对与本接口绑定，用于生成CGA地址。
  e. 执行命令**ipv6 security modifier sec-level** *sec-value* [*modifier-value*]，配置CGA地址的修正值和安全级别。

     只有当CGA地址的安全级别是0时，才能手动配置修正值。

f. 执行命令**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **cga** [**tag** *tag-value*]或**ipv6 address** *ipv6-address* **link-local cga** [**tag** *tag-value*]，配置CGA类型的IPv6地址。

g. 执行命令**commit**，提交配置。

- 使能IPv6安全邻居发现功能

  设置系统一段时间内(1s)计算或验证RSA签名的速率上限值和接口可以接受的密钥长度、ND报文的时间戳参数后，如果接收的报文不符合以上要求，则被视为非法报文。

  a. 执行命令**system-view**，进入系统视图。

  b. （可选）执行命令**ipv6 nd security rate-limit** *ratelimit-value*，设置系统一段时间内(1s)计算或验证RSA签名的速率上限值。

  c. 执行命令**interface** *interface-type interface-number*，进入接口视图。

  d. （可选）执行命令**ipv6 nd security key-length** { **minimum** *keylen-value* | **maximum** *keylen-value* } *，配置接口可以接受的密钥长度。

  e. （可选）执行命令**ipv6 nd security timestamp** { **fuzz-factor** *fuzz-value* | **delta** *delta-value* | **drift** *drift-value* } *，配置ND报文的时间戳参数。

  f. 执行命令**ipv6 nd security strict**，使能接口的严格安全模式功能。

  g. 执行命令**commit**，提交配置。

检查加固结果

使用**display ipv6 security interface** *interface-type interface-number*命令查看接口下ND安全相关的配置信息。

配置维护建议

配置IPv6安全邻居发现会降低邻居表项的学习速率。

?.2. 管理平面防护（IPv6）

安全策略介绍

管理平面防护MPAC（Management Plane Access Control）增强设备对拒绝服务型攻击的防范能力，可以增强系统的安全性，满足这些组网情况下的业务开展需求。

路由器可能同时启用多种服务，例如二层业务MSTP，路由业务OSPF、BGP，MPLS业务LDP、RSVP，系统服务FTP Server，TFTP Server，诊断功能Ping、Tracert等。

在这种情况下，攻击者可以发送各种类型的报文攻击路由器，如果是目的地址是路由器自身接口（包括Loopback口）IP地址时，路由器就会直接将报文上送CPU。这样就会耗费路由器的CPU和系统资源，造成DoS攻击。

为了避免这种攻击，可以制定管理平面接入控制策略的规则，根据规则决定是否上送此协议报文。

路由器支持的MPAC包括：子接口应用管理平面接入控制策略、主接口应用管理平面接入控制策略、全局应用管理平面接入控制策略，可以对上送CPU的报文进行过滤。

设备根据子接口、主接口、全局上的管理平面接入控制策略的规则，决定报文是否上送CPU。如果子接口、主接口、全局上都没有配置管理平面接入控制策略的规则，则报文直接上送CPU。

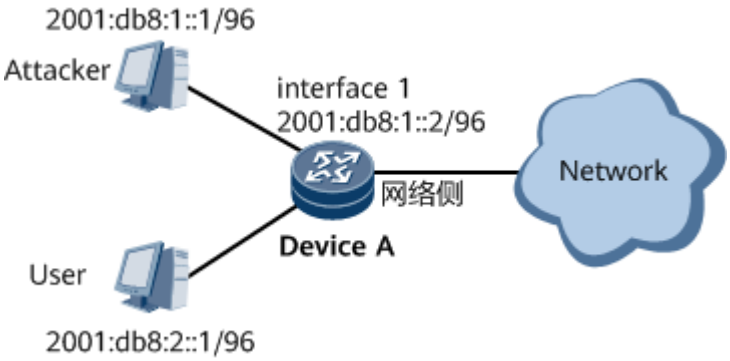
攻击方法介绍

如图1-8所示，为了防止Hacker发送各种TCP/IP攻击报文对DeviceA进行攻击，造成DeviceA瘫痪，需要在DeviceA上部署管理平面控制接入策略。

图 1-8 MPAC 组网图

说明

本例中interface1代表GE1/0/0。



配置维护方法

在DeviceA上配置：

```
<DeviceA> system-view
[DeviceA] service-security policy ipv6 test
[DeviceA-service-sec-test] rule 10 deny protocol ip source-ip 2001:db8:1::1 64
[DeviceA-service-sec-test] step 10
[DeviceA-service-sec-test] description rule 10 is deny ip packet which from 2001:db8:1::1
[DeviceA-service-sec-test] commit
[DeviceA-service-sec-test] quit
[DeviceA] service-security global-binding ipv6 test
[DeviceA] commit
[DeviceA] interface gigabitethernet 1/0/0
[DeviceA-GigabitEthernet1/0/0] service-security binding ipv6 test
[DeviceA-GigabitEthernet1/0/0] commit
```

配置维护建议

无。

检查加固结果

- 执行命令**display service-security policy ipv6** [*security-policy-name* [**slot** *slot-id*]]，查看设备上所有的管理平面接入控制策略的配置信息。
- 执行命令**display service-security binding ipv6** [**interface** *interface-type interface-number* [**slot** *slot-id*]]，查看接口的管理平面接入控制策略信息。
- 执行命令**display service-security statistics ipv6** [*security-policy-name*]，查看匹配管理平面接入控制策略的统计信息。

DHCP

?.1. 伪服务器检测

安全策略介绍

使用DHCP Snooping的“信任（Trusted）/不信任（Untrusted）”工作模式来隔离DHCP服务器仿冒者攻击。

- 在DHCP Snooping的流程中处理。
- 基于信任端口和非信任端口分别记录服务器信息并记录日志，各自规格为64个，满规格时随机覆盖，且存在老化机制，老化时间为24小时。
- 配置上依赖于全局dhcp Snooping的使能。

攻击方法介绍

当网络中存在DHCP Server仿冒者时，会回应给DHCP Client仿冒信息，如错误的网关地址、错误的DNS服务器、错误的IP等，从而使Client无法访问网络或访问到不正确的网络。

配置维护方法

配置接口GE1/0/0为信任接口。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-Gigabitethernet1/0/0] dhcp snooping trusted
[*HUAWEI-Gigabitethernet1/0/0] commit
```

配置维护建议

配置在离DHCP Server最近的设备上效果最好。

检查加固结果

执行命令**display dhcp snooping interface** *interface-type interface-number*，查看DHCP Snooping的配置信息。

?.2. DoS 攻击

安全策略介绍

攻击者通过改变DHCP报文中的CHADDR（Client Hardware Address）值来不断申请IP地址，造成DHCP Server地址耗尽，实现Dos攻击，可以通过在设备上检查DHCP请求报文中的CHADDR字段来防止攻击。

攻击方法介绍

对于攻击者不断改变数据帧头部源MAC的攻击方式，可以通过MAC地址限制来解决，但如果攻击者改变的不是数据帧头部的源MAC，而是通过改变DHCP报文中的CHADDR（Client Hardware Address）值来不断申请IP地址，而设备仅根据数据帧头部的源MAC来判断该报文是否合法，那么MAC地址限制不能完全起作用，这样的攻击报文还是可以被正常转发。

配置维护方法

接口上配置CHADDR检查。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-Gigabitethernet1/0/0] dhcp check chaddr enable
[*HUAWEI-Gigabitethernet1/0/0] commit
```

配置维护建议

配置后影响用户接入性能。

检查加固结果

执行命令**display dhcp snooping interface** *interface-type interface-number*，查看DHCP Snooping的配置信息。

?.3. 仿冒续租报文

安全策略介绍

攻击者通过不断发送DHCP Request报文来冒充用户续租IP地址，会导致一些到期的IP地址无法正常回收，可以在设备上使能防止仿冒DHCP续租报文攻击功能，检查请求报文中携带的信息是否与绑定表匹配。

攻击方法介绍

攻击者通过发送大量携带错误源MAC地址、源IP地址、VLAN ID、接口信息的报文攻击DHCP服务器。

配置维护方法

接口上配置仿冒续租报文检查。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-Gigabitethernet1/0/0] dhcp snooping check dhcp-request enable
[*HUAWEI-Gigabitethernet1/0/0] commit
```

配置维护建议

配置后影响用户接入性能。

检查加固结果

执行命令**display dhcp snooping interface** *interface-type interface-number*，查看DHCP Snooping的配置信息。

?.4. 非法 ARP 报文攻击

安全策略介绍

DHCP Snooping ARP报文检查功能，有些产品上称为DAI功能，两者实现的功能类似。

攻击方法介绍

基于绑定表对ARP报文进行匹配检查。设备在转发ARP报文时，将此ARP报文中的发送者IP、发送者MAC、端口、VLAN信息和绑定表的信息进行比较，如果信息匹配，说明是合法ARP报文，则转发该ARP，否则认为是攻击，丢弃该ARP报文。

配置维护方法

接口上配置ARP报文检查。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-Gigabitethernet1/0/0] dhcp snooping check arp enable
[*HUAWEI-Gigabitethernet1/0/0] commit
```

配置维护建议

配置后影响用户接入性能。

检查加固结果

执行命令**display dhcp snooping interface** *interface-type interface-number*，查看DHCP Snooping的配置信息。

?.5. 非法 IP 报文攻击

安全策略介绍

设备在转发IP报文时，将此IP报文中的源IP、源MAC、端口、VLAN信息和绑定表的信息进行比较，如果信息匹配，说明是合法用户，则允许此用户正常转发，否则认为是攻击，丢弃该IP报文。

DHCP Snooping IP报文检查功能，有些产品上称为IP Source Guard功能，两者实现的功能类似。

攻击方法介绍

攻击者通过发送携带非法的源MAC、源IP、VLAN ID或者接口信息的大量IP报文攻击DHCP服务器。

配置维护方法

接口上配置仿冒非法IP报文检查。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-Gigabitethernet1/0/0] dhcp snooping check ip enable
[*HUAWEI-Gigabitethernet1/0/0] commit
```

配置维护建议

配置后影响用户接入性能。

检查加固结果

执行命令**display dhcp snooping interface** *interface-type interface-number*，查看DHCP Snooping的配置信息。

?.6. 配置 DHCP 的 IPSec 认证

安全策略介绍

使能DHCPv4中继和服务器上的IPSec认证功能后，DHCPv4中继和服务器发送DHCPv4报文时，DHCPv4报文中会插入绑定的IPSec SA中的SPI，并基于绑定的IPSec SA的安全提议进行加密。DHCPv4中继和服务器接收到DHCPv4报文后，先进行IPSec解密和认证，若解密或认证失败则丢弃报文，再检查报文中的SPI是否与绑定的IPSec SA中的SPI一致，若不一致则丢弃报文。

攻击方法介绍

当网络中存在DHCPv4服务器仿冒者时，DHCPv4中继会收到虚假的DHCPv4报文，可能会导致DHCPv4中继受到拒绝服务攻击。当网络中存在DHCPv4中继仿冒者时，DHCPv4服务器会收到虚假的DHCPv4报文，可能会导致DHCPv4服务器受到拒绝服务攻击。

配置维护方法

系统视图配置DHCPv4 IPSec认证功能。

```
<HUAWEI> system-view
[~HUAWEI] dhcp ipsec sa sa1
[*HUAWEI] commit
```

说明

在执行**dhcp ipsec**命令前，必须先配置IPSec安全联盟，具体配置请参见IPSec配置。

配置维护建议

配置后影响用户接入性能。

检查加固结果

执行命令**display dhcp relay statistics** [**interface** { *interface-type interface-number* | *interface-name* }]，查看DHCP中继的相关报文统计信息。

?.7. 配置 DHCP Snooping 文件完整性校验

安全策略介绍

为防止设备发生意外导致数据丢失，用户可以使能对DHCP Snooping绑定表的自动备份功能，系统将生成备份文件。为了防止备份文件被篡改，备份文件中会增加加密过的文件完整性校验码。在设备重启后，系统从备份文件中恢复绑定表之前，系统对文件完整性校验码进行解密，并基于解密后的文件完整性校验码对文件完整性进行校验。若校验通过，则恢复数据，若校验失败，则丢弃数据，记录日志。

攻击方法介绍

攻击者对绑定表备份文件进行数据篡改，设备重启后生成错误的绑定表，从而导致非法报文可以被转发。

配置维护方法

系统视图配置文件完整性校验模式为force-check。

```
<HUAWEI> system-view
[~HUAWEI] dhcp snooping database authentication-mode force-check
[*HUAWEI] commit
```

配置维护建议

若需要用其他设备上生成的备份文件恢复数据，则需要在重启之前配置**dhcp snooping database authentication-mode no-check**命令将文件完整性认证模式设置为不检查模式，再进行重启恢复。

为了防止基于历史版本文件进行数据篡改，可以在重启之前配置**dhcp snooping database authentication-mode force-check**命令将文件完整性认证模式设置为强制检查模式。

检查加固结果

执行命令**display dhcp snooping global**，查看DHCPv4 Snooping文件完整性校验模式。

?.8. 配置 DHCP Server 备份文件的完整性校验

安全策略介绍

为防止设备发生意外导致数据丢失，用户可以使用**dhcp server database**命令启用DHCP数据保存功能，系统将生成lease.txt和conflict.txt两个文件存放在CF卡的DHCP文件夹中，分别保存正常的地址租借信息和地址冲突信息。当设备使能一MAC多Session功能后，会生成一个option82_index.data文件来保存用户的option82信息。

为了防止“lease.txt”和“conflict.txt”两个文件被篡改，用户可以配置**dhcp server database authentication-mode**命令，“lease.txt”和“conflict.txt”两个文件中会增加加密过的文件完整性校验码。在设备重启后，系统从“lease.txt”和“conflict.txt”两个文件恢复地址租借信息和地址冲突信息之前，系统对文件完整性校验码进行解密，并基于解密后的文件完整性校验码对文件完整性进行校验。若校验通过，则恢复数据，若校验失败，则丢弃数据，记录DHCP_FILE_RECOVER_FAIL日志。

攻击方法介绍

攻击者对“lease.txt”、“conflict.txt”文件进行数据篡改，设备重启后地址池地址租借信息和地址冲突信息错误，可能会造成服务器无法分配地址。

配置维护方法

系统视图配置文件完整性校验模式为force-check。

```
<HUAWEI> system-view
[~HUAWEI] dhcp server database authentication-mode force-check
[*HUAWEI] commit
```


配置维护建议

若需要用其他设备上生成的备份文件恢复数据，则需要在重启之前配置为no-check模式将文件完整性认证模式设置为不检查模式，再进行重启恢复。

为了升级兼容，不携带文件完整性校验码的历史版本文件可以重启恢复数据。为了防止基于历史版本文件进行数据篡改，可以在重启之前配置force-check模式将文件完整性认证模式设置为强制检查模式。

检查加固结果

执行命令**display dhcp server database**，查看DHCPv4 Server文件完整性校验模式。

DHCPv6

?.1. 非法 IPv6 报文攻击

安全策略介绍

设备在转发IPv6报文时，如果通过IPv6报文中的源IPv6地址、Prefix、VLAN ID、VPN信息查找不到DHCPv6 Snooping绑定表，则直接丢弃该IPv6报文。如果通过IPv6报文中的源IPv6地址、Prefix、VLAN ID、VPN信息查找到DHCPv6 Snooping绑定表，并且源MAC、接口信息匹配，说明是合法用户，则允许此用户正常转发，否则认为是攻击，丢弃该IPv6报文。

攻击方法介绍

攻击者通过发送携带非法的源MAC、接口信息的大量IPv6报文攻击DHCPv6服务器。

配置维护方法

接口上配置仿冒非法IPv6报文检查。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet1/0/0
[~HUAWEI-Gigabitethernet1/0/0] dhcpv6 snooping check ipv6 enable
[*HUAWEI-Gigabitethernet1/0/0] commit
```

配置维护建议

配置后影响用户接入性能。

?.2. 配置 DHCPv6 的 IPSec 认证

安全策略介绍

使能DHCPv6中继和服务器上的IPSec认证功能后，DHCPv6中继和服务器发送DHCPv6报文时，DHCPv6报文中会插入绑定的IPSec SA中的SPI，并基于绑定的IPSec SA的安全提议进行加密。DHCPv6中继和服务器接收到DHCPv6报文后，先进行IPSec解密和认证，若解密或认证失败则丢弃报文，再检查报文中的SPI是否与绑定的IPSec SA中的SPI一致，若不一致则丢弃报文。

攻击方法介绍

当网络中存在DHCPv6服务器仿冒者时，DHCPv6中继会收到虚假的DHCPv6报文，可能会导致DHCPv6中继受到拒绝服务攻击。当网络中存在DHCPv6中继仿冒者时，DHCPv6服务器会收到虚假的DHCPv6报文，可能会导致DHCPv6服务器受到拒绝服务攻击。

配置维护方法

系统视图配置DHCPv6 IPSec认证功能。

```
<HUAWEI> system-view
[~HUAWEI] dhcpv6 ipsec sa sa1
[*HUAWEI] commit
```

说明

在执行**dhcpv6 ipsec**命令前，必须先配置IPSec安全联盟，具体配置请参见IPSec配置。

配置维护建议

配置后影响用户接入性能。

检查加固结果

- 执行命令**display dhcpv6 relay statistics** [**interface** { *interface-name* | *interface-type interface-number* }]，查看DHCPv6中继代理的报文统计信息。
- 执行命令**display dhcpv6 server** { **database** | **interface** { *interface-name* | *interface-type interface-number* } | **statistics** [**interface** { *interface-name* | *interface-type interface-number* }] }，查看DHCPv6服务器功能相关信息。

?.3. 配置 DHCPv6 Server 文件完整性校验

安全策略介绍

为防止设备发生意外导致数据丢失，用户可以使能DHCPv6地址池的数据保存以及数据恢复的功能，系统将生成lease.txt和conflict.txt两个文件存放在dhcpv6文件夹中，分别保存正常的地址租借信息和地址冲突信息。为了防止lease.txt和conflict.txt两个文件被篡改，lease.txt和conflict.txt两个文件中会增加加密过的文件完整性校验码。在设备重启后，系统从lease.txt和conflict.txt两个文件恢复地址租借信息和地址冲突信息之前，系统对文件完整性校验码进行解密，并基于解密后的文件完整性校验码对文件完整性进行校验。若校验通过，则恢复数据，若校验失败，则丢弃数据，记录日志。

攻击方法介绍

攻击者对lease.txt和conflict.txt文件进行数据篡改，设备重启后地址池地址租借信息和地址冲突信息错误，可能会造成服务器无法分配地址。

配置维护方法

系统视图配置文件完整性校验模式为force-check。

```
<HUAWEI> system-view
[~HUAWEI] dhcpv6 server database authentication-mode force-check
[*HUAWEI] commit
```


配置维护建议

若需要用其他设备上生成的备份文件恢复数据，则需要在重启之前配置**dhcpv6 server database authentication-mode no-check**命令将文件完整性认证模式设置为不检查模式，再进行重启恢复。

为了升级兼容，不携带文件完整性校验码的历史版本文件可以重启恢复数据。为了防止基于历史版本文件进行数据篡改，可以在重启之前配置**dhcpv6 server database authentication-mode force-check**命令将文件完整性认证模式设置为强制检查模式。

检查加固结果

执行命令**display dhcpv6 server database**，查看DHCPv6 Server文件完整性校验模式。

?.4. 配置 DHCPv6 Relay 文件完整性校验

安全策略介绍

为防止设备发生意外导致数据丢失，用户可以使能对前缀路由信息的自动备份功能，系统将生成备份文件。为了防止备份文件被篡改，备份文件中会增加加密过的文件完整性校验码。在设备重启后，系统从备份文件中恢复前缀路由信息之前，系统对文件完整性校验码进行解密，并基于解密后的文件完整性校验码对文件完整性进行校验。若校验通过，则恢复数据，若校验失败，则丢弃数据，记录日志。

攻击方法介绍

攻击者对备份文件进行数据篡改，设备重启后会丢失前缀路由信息，导致客户端的下行流量不通。

配置维护方法

系统视图配置文件完整性校验模式为force-check。

```
<HUAWEI> system-view
[~HUAWEI] dhcpv6 relay database authentication-mode force-check
[*HUAWEI] commit
```

配置维护建议

若需要用其他设备上生成的备份文件恢复数据，则需要在重启之前配置**dhcpv6 relay database authentication-mode no-check**命令将文件完整性认证模式设置为不检查模式，再进行重启恢复。

为了升级兼容，不携带文件完整性校验码的历史版本文件可以重启恢复数据。为了防止基于历史版本文件进行数据篡改，可以在重启之前配置**dhcpv6 relay database authentication-mode force-check**命令将文件完整性认证模式设置为强制检查模式。

检查加固结果

执行命令**display dhcpv6 relay configuration**，查看DHCPv6 Relay文件完整性校验模式。

?.5. 配置 DHCPv6 Snooping 文件完整性校验

安全策略介绍

为防止设备发生意外导致数据丢失，用户可以使能对DHCPv6 Snooping绑定表的自动备份功能，系统将生成备份文件。为了防止备份文件被篡改，备份文件中会增加加密过的文件完整性校验码。在设备重启后，系统从备份文件中恢复绑定表之前，系统对文件完整性校验码进行解密，并基于解密后的文件完整性校验码对文件完整性进行校验。若校验通过，则恢复数据，若校验失败，则丢弃数据，记录日志。

攻击方法介绍

攻击者对绑定表备份文件进行数据篡改，设备重启后生成错误的绑定表，从而导致非法报文可以被转发。

配置维护方法

系统视图配置文件完整性校验模式为force-check。

```
<HUAWEI> system-view
[~HUAWEI] dhcpv6 snooping database authentication-mode force-check
[*HUAWEI] commit
```

配置维护建议

若需要用其他设备上生成的备份文件恢复数据，则需要在重启之前配置**dhcpv6 snooping database authentication-mode no-check**命令将文件完整性认证模式设置为不检查模式，再进行重启恢复。

为了防止基于历史版本文件进行数据篡改，可以在重启之前配置**dhcpv6 snooping database authentication-mode force-check**命令将文件完整性认证模式设置为强制检查模式。

安全管理中心

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X为了保证自身系统的可靠性，使运行在系统中的业务系统不受安全攻击事件的影响，提供了诸如CAR速率限制、攻击检测、攻击防范等技术手段。但所有这些技术缺乏一个全局的管理中心，来汇总分析所有安全攻击的信息，因此在进行攻击检测和防御时，存在“只见树木，不见森林”的片面性。

安全管理中心就是为了解决该问题，站在系统全局，统一汇总分析各个安全检测单元的上报信息，之后以简洁的形式为用户呈现出一键式的攻击事件报告、攻击溯源、根因分析、以及解决建议等。

说明

安全管理中心不处理轻微程度的攻击事件的信息显示，例如对系统整体运行危害不大，仅影响某个局部功能的攻击事件；或者利用特殊构造的畸形报文攻击导致系统崩溃；或者利用系统内部的bug用很小的流量导致系统崩溃等诸如此类的系统质量层面的事件，此类事件的显示由各业务模块、网管、日志、攻击溯源等功能完成。

安全管理中心只显示存在系统级风险的攻击事件的信息，此类攻击事件一般有以下几个典型特征：

- CPU利用率高，显著高于正常运行时的CPU利用率水平
- 已经引起CPCAR丢包，丢包率超过了正常阈值
- 协议模块检测到设备收到大量的非法报文或者非法会话，非法报文或者非法会话比例超过了正常阈值

攻击检测

攻击检测功能通过安全管理中心收集到的统计数据，判定设备是否受到攻击。

安全管理中心通过定时器定时收集CPU利用率、各个协议模块的状态数据（包括非法报文和非法会话数）、以及CPCAR的丢包计数。在攻击检测功能使能后，当CPU利用率达到检测门限值，并且协议模块的非法报文或非法会话的百分比、或者报文丢包率等达到攻击检测门限值时，则判定设备受到攻击，启动攻击溯源。攻击检测功能未使能时，安全管理中心依然会通过定时器定时收集和统计数据，但不会进行攻击判定，也不会启动攻击溯源。

攻击溯源

攻击溯源功能用于判定攻击事件发生的位置、概率和原因。

当攻击检测功能判定设备受到攻击后，安全管理中心对攻击报文进行采样，然后对采样的报文进行多维度（针对源MAC地址、源IP地址、广播报文、变源报文、协议类型、物理接口、逻辑接口、VLAN、QinQ）的统计分析，排出按每个维度进行统计的前N名。然后利用攻击溯源的攻击事件判定门限参数，筛选出可能与安全攻击相关的对象，生成攻击事件报告并产生告警。

攻击防范

攻击防范功能通过自动下发防范策略，对攻击报文进行丢弃，达到防范目的。

攻击防范功能使能后，安全管理中心会对攻击报文进行分类，提取出攻击报文的特征，然后根据攻击报文的特征下发ACL规则。该ACL规则包含攻击报文的特征、受攻击的接口、以及此ACL规则与某个CAR的对应关系。

安全管理中心实时统计命中该ACL规则的报文的上送和丢弃计数，如果丢弃报文速率小于一定值时，则取消该ACL规则。

?.1. 安全管理中心的配置方案和步骤

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**soc**，使能攻击检测和攻击溯源功能，并进入SOC视图。

步骤3 （可选）执行命令**attack-defend enable**，使能攻击防范功能。

如果通过分析攻击事件后确定发生了攻击，则可以使能攻击防范功能。

步骤4 执行命令**commit**，提交配置。

步骤5 （可选）执行命令**display soc attack-defend statistics slot** *slot-id* **port-vlan-car**，查看指定单板上受到攻击的接口通过和丢弃报文的统计信息。

当安全管理中心的攻击防范策略使能后，若受到攻击，则可以通过此命令查看指定槽位的每个接口上通过和丢弃报文的统计信息。

步骤6 配置判定攻击事件的门限参数

- 执行命令**attack-trace location-type** { **interface** | **qinq** | **source-ip** | **source-mac** | **sub-interface** | **vlan** } **threshold** *threshold-value*，配置判定攻击事件位置的门限参数。
- 执行命令**attack-trace probability** { **top5-user** | **top5-source-mac** | **top5-source-ip** | **broadcast-flood** | **app-error-percent** } { **determined** | **notification** | **suspicion** } *threshold-value*，配置判定攻击事件概率的门限参数。
- 执行命令**attack-trace reason** { **app-packet** | **broadcast-flood** | **change-source-packet** } **percentage** *percentage-value*，配置判定攻击事件原因的门限参数。

步骤7 执行命令**commit**，提交配置。

----结束

检查加固结果

1. 查看攻击事件报告
   a. 执行命令**display soc attack-event**，查看攻击事件报告的概要信息。
   b. 执行命令**display soc attack-event** [{ **slot***slot-id* [**event-number***event-number*] [**verbose**] | **event-number***event-number* [**verbose**] }]，查看指定槽位的攻击事件报告。可根据概要信息中的**Location**字段选择指定槽位，查看发生的攻击事件报告。指定**verbose**参数时可查看详细信息。
   c. 执行命令**display soc attack-event event-number** *event-number* [**verbose**]，查看指定攻击事件报告。可以根据攻击事件报告概要信息中的**Seq.**字段或者指定槽位攻击事件报告里的回显信息选择要查看的攻击事件序号，通过指定攻击事件序号查看此事件的报告以及详细报告。
2. 查看历史统计信息

   说明

   下面命令中的*slot-id*和*protocol-name*分别对应**display soc attack-event**命令中的*slot-id*和**display soc attack-event**命令回显中的**Reasons**字段。

   查看CPCAR的统计信息

   a. 执行命令**display soc attack-detect statistics car slot** *slot-id* **protocol** *protocol-name*，查看所有安全管理中心监控的CPCAR的统计信息，找出丢包率最严重的CPCAR，或者丢包累计个数最大的CPCAR，并找到它们对应的协议报文类型**CarName**。CAR为流量监管的一个实例。CPCAR是对上送CPU的主机报文执行CAR动作。
   b. 执行命令**display soc attack-detect statistics car slot** *slot-id* **protocol** *protocol-name* [*cpcar-name* **history** { **15-minute** | **60-minutes** | **72-hour** }]，查看此*cpcar-name*对应的协议报文在过去某个时间段内的丢包率。

c. 执行命令**display soc attack-detect cpu-usage slot** *slot-id* **history** { **15-minutes** | **60-minutes** | **72-hours** }，查看此时间段内CPU的利用率，如果在这个时间段内的CPU利用率趋势与丢包率趋势恰好存在显著的相关性，由此可以确定此时间段内CPU过载的原因是由于此*cpcar-name*类型的协议报文引起的。

查看协议模块的统计信息

a. 执行命令**display soc attack-detect statistics application slot** *slot-id*，查看指定槽位单板上协议模块的报文和会话的统计信息，找出非法报文和非法会话比例最大的协议模块，初步判定此类协议模块的安全状态最差。

b. 执行命令**display soc attack-detect statistics application slot** *slot-id* **protocol** *protocol-name* **history** { **15-minute** | **60-minutes** | **72-hour** }，查看此类安全模块在过去的15分钟、1小时或72小时内对报文和会话的平均统计数据以及CPU平均利用率的历史统计数据，如果发现当非法报文或者会话的百分比突发偏高，而此时CPU利用率也随着偏高，通常情况下，就可以判断CPU过载的原因就是这种协议模块遭受攻击导致的。若通过CPU平均利用率无法准确判断，则可以通过下面的命令查看此时间段范围内详细的CPU利用率。

c. （可选）执行命令**display soc attack-detect cpu-usage slot** *slot-id* **history** { **15-minutes** | **60-minutes** | **72-hours** }，命令查看此时间段内详细CPU的利用率。

DNS

安全策略介绍

- DNS TLS认证

  动态域名解析支持基于TCP的TLS的报文加密传输，用户可以预先在DNS客户端和服务器上部署SSL策略并加载数字证书，在域名解析的时候，DNS会根据指定的SSL策略对报文进行加密、解密，以提高DNS报文传输的安全性。

攻击方法介绍

当网络中存在DNS Server仿冒者时，会回应给DNS Client仿冒信息，如错误的IP地址，从而使Client无法访问网络或访问到不正确的网络。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**dns resolve**，使能动态域名解析功能。
3. 执行命令**dns server** *ip-address* [**vpn-instance** *vpn-name*] **tcp ssl-policy** *ssl-policy-name* ，增加域名服务器并绑定SSL策略名。

   说明

   DNS域名解析使用基于TCP的SSL加密方式，避免报文被非法截取或者仿冒。

4. （可选）执行命令**dns server source-ip** [**vpn-instance** *vpn-name*] *ipv4Addr* ，指定本端路由器的IP地址。

   指定本端路由器的IP地址，以指定的IP地址与DNS服务器端通信，从而保证通信的安全。

5. 执行命令**dns domain** *domain-name* [**vpn-instance** *vpn-name*]，增加域名后缀。
6. （可选）执行命令**dns timeout** *interval-time*，配置DNS客户端等待查询响应的超时时间。
7. （可选）执行命令**dns try** *times*，配置DNS客户端域名查询的重传次数。
8. 执行命令**commit**，提交配置。

检查加固结果

使用**display dns server** [**vpn-instance** *vpn-instance-name*]命令查看配置的TLS策略名称。

1.1.7.2.3 转发平面

典型垃圾流量过滤

安全策略介绍

通过使用接口ACL技术，可以有效地阻止一些有害的流量进入用户终端，也阻止终端有害流量进入网络。需要阻止的流量主要有常见及危害程度较大的病毒、木马端口。

说明

具体过滤的端口必须根据现网实际情况部署，并且由用户最终确认，以下配置和举例仅用作参考。

配置维护方法

1. 定义ACL，匹配到病毒、木马端口等报文后进行丢弃处理。
   a. 执行命令**acl** { **name** *interface-based-acl-name* { **interface** | [**interface**] **number** *interface-based-acl-number* } | [**number**] *interface-based-acl-number* }，进入基于接口的ACL视图。

      基于接口的ACL的编号范围是1000～1999。
   b. 执行命令**rule** [*rule-id*] [**name** *rule-name*] { **permit** | **deny** } **interface** { *interface-type interface-number* | **any** } [**time-range** *time-name*] *，配置基于接口的ACL的规则。
2. 定义流策略。
   a. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，定义流分类并进入流分类视图。
   b. 执行命令**if-match** [**ipv6**] **acl** { *acl-number* | **name** *acl-name* }，定义ACL匹配规则。
3. 定义流行为。
   a. 执行命令**traffic behavior** *behavior–name*，定义流行为进入流行为视图。
   b. 执行命令**permit/deny**，允许/禁止报文的通过。
4. 定义流策略。
   a. 执行命令**traffic policy** *policy-name*，定义流量策略并进入策略视图。

b. 执行命令**classifier** *classifier-name* **behavior** *behavior-name* ，在流量策略中为流分类指定采用的行为。

5. 在接口上应用流策略。
   a. 执行命令**interface** *interface-type interface-number*，进入接口视图。
   b. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** } ，在接口下应用流策略。

      说明

      在接口的入方向和出方向可以分别应用不同的流策略。

配置举例

配置ACL 3300和ACL ipv6 3400，用于匹配病毒、木马端口等报文后进行丢弃处理。

```
acl number 3300
 rule 5 deny udp source-port range 135 netbios-ssn
 rule 10 deny udp destination-port range 135 netbios-ssn
 rule 15 deny udp source-port eq 445
 rule 20 deny udp destination-port eq 445
 rule 25 deny tcp source-port eq 445
 rule 30 deny tcp destination-port eq 445

acl ipv6 number 3400
 rule 5 deny udp source-port range 135 netbios-ssn
 rule 10 deny udp destination-port range 135 netbios-ssn
 rule 15 deny udp source-port eq 445
 rule 20 deny udp destination-port eq 445
 rule 25 deny tcp source-port eq 445
 rule 30 deny tcp destination-port eq 445
```

设备上行口入方向过滤非法报文。

```
traffic classifier tcAntivirusIn operator or
 if-match acl 3300
 if-match ipv6 acl 3400
traffic behavior tbAntivirusIn

traffic policy tpAntivirusIn
 share-mode
 statistics enable
 classifier tcAntivirusIn behavior tbAntivirusIn precedence 1

//在设备上行口入方向应用策略
interface GigabitEthernet1/0/0
 undo shutdown
 traffic-policy tpAntivirusIn inbound
```

设备上行口出方向过滤非法报文。

```
traffic classifier tcAntivirusOut operator or
 if-match acl 3300
 if-match ipv6 acl 3400
traffic behavior tbAntivirusOut

traffic policy tpAntivirusOut
 share-mode
 statistics enable
 classifier tcAntivirusOut behavior tbAntivirusOut precedence 1

//设备上行口出方向应用策略
interface GigabitEthernet1/0/0
 undo shutdown
 traffic-policy tpAntivirusOut outbound
```


检查加固结果

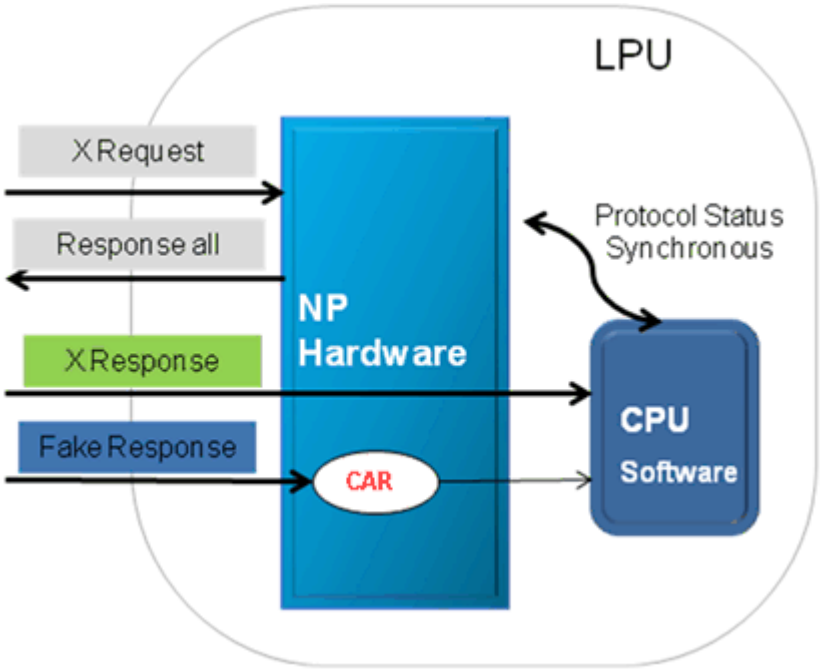
- 执行**display interface** [*interface-type* [*interface-number*]]命令查看接口的流量信息。
- 执行**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]命令查看流行为的配置信息。
- 执行**display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]命令查看流分类的配置信息。
- 执行**display traffic policy statistics interface** *interface-type interface-number* [*.sub-interface*] { **inbound** | **outbound** } [**verbose** { **classifier-based** [**class** *class-name*] | **rule-based** [**class** *class-name*] [**filter**] }]命令查看接口的流量策略统计信息。

利用硬件实现会话自动应答的 CPU 防护

如图1-9所述，路由器的转发平面由硬件实现，因此其性能极高。而控制和管理平面运行在CPU之上，属于软件系统，其处理能力远远低于转发平面。因此，在遭受安全攻击时，控制和管理平面容易出现处理能力不足，产生拒绝服务，达成攻击者的目标。

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X利用转发平面强大的处理能力，将严重威胁CPU安全的几种协议，实现了由硬件智能应答协议请求，减轻了CPU的负担，避免了CPU成为拒绝服务攻击的目标。

图 1-9 基于硬件实现智能消息应答的 CPU 防护



如上所示，利用路由器转发平面的NP网络处理器硬件，将送给CPU的消息进行自动智能应答，避免了消息上送CPU的性能消耗。同时，在路由器遭受X Flood攻击的时候，能够利用NP硬件的无限性能，保障CPU的运行性能。

- 请参考《 配置指南-安全 》中的使能ARP双向分离功能和配置ARP双向分离和ARP VLAN CAR功能示例。

- 请参考《 配置指南-IP业务 》中的配置ICMP报文快回。

SRv6 信任域

安全策略介绍

SRv6基于源路由在网络上转发IPv6数据包，继承了源路由安全风险、IPv6安全风险和SDN集中管控安全风险，面临着攻击者修改报文头来操纵流量路径的一系列攻击。因此，SRv6将网络分为不可信的SRv6域外网络和可信的SRv6域；并在信任域边界节点做流量过滤，防止攻击者通过伪造报文向信任域内节点发送攻击报文。

定义SRv6信任域的安全要求如下：

1. 定义明确的SRv6信任域边界，区分SRv6域内外网络。
2. 在SRv6信任域边界节点对流量进行过滤，丢弃源地址、目的地址是SRv6域内的SID空间地址的报文。
3. SRv6信任域内节点，丢弃目的地址是本地Local SID，源地址不是SRv6域内地址的报文。

配置维护方法

SRv6通过在SRv6信任域边界节点对流量进行过滤，丢弃违反上述安全要求的报文来提高安全性。

1. 在SRv6信任域边界节点设置ACL6策略，丢弃目的地址是SRv6域内的SID空间地址的报文

```
<HUAWEI> system-view
[~HUAWEI] acl ipv6-pool srv6_deny_destination_address
[*HUAWEI-acl-ipv6-pool-srv6_deny_destination_address] ipv6 address 2001:DB8:: 32
[*HUAWEI-acl-ipv6-pool-srv6_deny_destination_address] quit
[*HUAWEI] acl ipv6-pool srv6_deny_source_address
[*HUAWEI-acl-ipv6-pool-srv6_deny_source_address] ipv6 address 2001:DB8:: 32
[*HUAWEI-acl-ipv6-pool-srv6_deny_source_address] quit
[*HUAWEI] acl ipv6 3200
[*HUAWEI-acl6-advance-3200] rule 10 deny ipv6 source-pool srv6_deny_source_address destination-pool srv6_deny_destination_address
[*HUAWEI-acl6-advance-3200] quit
[*HUAWEI] commit
```

2. 配置流策略

```
[~HUAWEI] traffic classifier tcSrv6TrustDomain operator or
[*HUAWEI-classifier-tcSrv6TrustDomain] if-match ipv6 acl 3200
[*HUAWEI-classifier-tcSrv6TrustDomain] quit
[*HUAWEI] traffic behavior tbSrv6TrustDomain
[*HUAWEI-behavior-tbSrv6TrustDomain] quit
[*HUAWEI] traffic policy tpSrv6TrustDomain
[*HUAWEI-trafficpolicy-tpSrv6TrustDomain] share-mode
[*HUAWEI-trafficpolicy-tpSrv6TrustDomain] statistics enable
[*HUAWEI-trafficpolicy-tpSrv6TrustDomain] classifier tcSrv6TrustDomain behavior tbSrv6TrustDomain precedence 1
[*HUAWEI-trafficpolicy-tpSrv6TrustDomain] quit
[*HUAWEI] commit
```

3. 在节点上行口入方向应用流策略

```
[*HUAWEI] interface GigabitEthernet1/0/0
[*HUAWEI-GigabitEthernet1/0/0] undo shutdown
[*HUAWEI-GigabitEthernet1/0/0] traffic-policy tpSrv6TrustDomain inbound
[*HUAWEI-GigabitEthernet1/0/0] quit
[*HUAWEI] commit
```


检查加固结果

- 执行命令**display current-configuration configuration acl-ipv6-pool**，查看配置的IPv6地址池。
- 执行命令**display current-configuration configuration acl6-adv**，查看ACL6全局配置信息。
- 执行命令**display current-configuration configuration segment-routing-ipv6**，查看SRv6的配置信息。
- 执行命令**display interface** [*interface-type* [*interface-number*]]，查看接口的流量信息。
- 执行命令**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看流行为的配置信息。
- 执行命令**display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]，查看流分类的配置信息。
- 执行命令**display traffic policy statistics interface** *interface-type interface-number* [*.sub-interface*] { **inbound** | **outbound** } [**verbose** { **classifier-based** [**class** *class-name*] | **rule-based** [**class** *class-name*] [**filter**] }]，查看接口的流量策略统计信息。

本机防攻击

- 安全策略介绍:
  - 协议栈支持加密认证，支持telnet黑名单(具体请参考telnet特性的黑名单介绍)，GTSM(请参考各协议栈的GTSM配置)。
  - 大量报文、错误报文攻击时对于需要回应icmp差错等的报文，接口板LDM做了一级CAR限速然后上送主控板协议栈，主控板协议栈还会做一级CAR确保CPU不被打死 。
- 攻击方法介绍：
  - 无。
- 配置维护方法：
  - 具体参考各协议相关的安全配置。
- 配置维护建议：
  - 报文防攻击默认开启，不用配置。

?.1. 畸形报文攻击防范

安全策略介绍

畸形报文攻击是通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP包时会出现崩溃，给目标系统带来损失。

主要的畸形报文攻击有：

- 没有IP载荷的泛洪攻击
- IGMP空报文攻击
- LAND攻击
- Smurf攻击

- TCP标志位非法攻击

攻击方法介绍

- 没有IP载荷的泛洪

  攻击者经常构造大量只有IP头部，没有携带任何高层数据的IP报文，这些大量没有载荷的IP报文构成了flood攻击。因为这些没有高层数据的IP报文是没有作用的，需要将其丢弃。

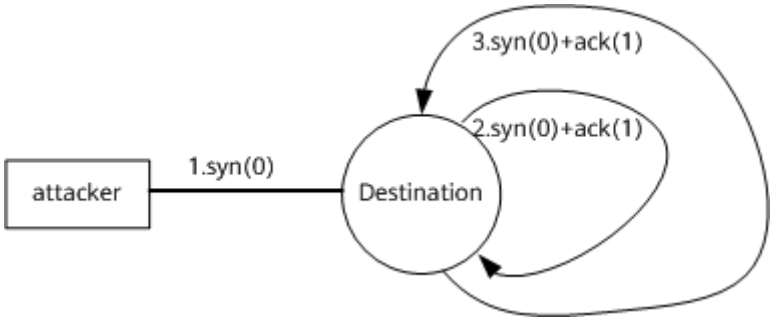
- IGMP空报文

  IGMP报文是20字节的IP头加上8字节的IGMP报文体。如果IGMP报文的总长度小于28字节，则认为该IGMP报文是畸形报文，直接丢弃。

- LAND攻击

  Land攻击是由著名的黑客组织RootShell发现的，于1997年11月20日公布的。原理是利用TCP连接三次握手中的缺陷，向目的主机发送源地址与目的主机地址一致的数据包，造成目的主机解析Land包占用过多的资源，导致网络瘫痪。即Land攻击者打造一个特别的SYN包，其源地址和目的地址被设置成同一台计算机的地址，源端口与目的端口也被设置成同一个端口。该计算机接收到SYN包之后，将导致该计算机向它自己的地址发送SYN+ACK消息，结果这个地址又发回SYN+ACK消息并创建一个空连接，每个这样的连接都将保留直到超时。

  图 1-10 LAND 攻击

  如上图所示，如果目的主机接收到自己的SYN+ACK后，认为这是一次连接请求（忽略ACK），它还会给自己回应SYN+ACK，这个ACK确认的是上一个SYN，新发出的SYN和前一个没有任何关系，目的主机再次认为自己收到一个连接请求，如此循环。

  即使目的主机没有把SYN+ACK当成一次连接请求，也会认为自己建立了半连接，因为本身发出了SYN+ACK，如果攻击数据包量很大，就造成了SYN Flood，建立了大量的半连接，导致系统瘫痪。

  对于LAND攻击确认是一种畸形报文攻击，通过检测TCP Syn报文中的源地址和目的地址是否一致，确认是否是攻击报文，如果一致，就会丢弃。

- Smurf攻击

  Smurf攻击的原理是：攻击者发送目的地址是广播地址，源地址是受害者地址的ICMP echo request报文。这样，网络上的所有主机都会向受害者发送reply报文，造成受害者收到过多报文，导致CPU利用率过高。对于目的地址为广播地址或者子网广播地址的ICMP echo request报文，直接认为是畸形报文丢弃。

- TCP标志位非法攻击

  TCP报文包含6个标志位：URG、ACK、PSH、RST、SYN、FIN ，不同的系统对这些标志位组合的应答是不同的。

6个标志全部为1，也就是圣诞树攻击。

6个标志全部为0，如果端口是关闭的，会使接收方应答一个RST | ACK消息。而对于一个开放端口，Linux和UNIX机器不会应答，而Windows机器将回答RST | ACK消息。这可用于操作系统探测。

不管端口是打开还是关闭，ACK与除RST外的其它任何一个状态位组合在一起，都会引起一个还没有发送请求的接收方的一个RST应答。这可用于探测主机的存在。

不管端口是打开还是关闭，SYN | FIN | URG 会让接收方发送一个 RST | ACK 应答，这可用于探测主机的存在。

如果端口是关闭的，SYN、SYN | FIN、SYN | PUSH、SYN | FIN | PUSH、SYN| URG、SYN | URG | PUSH、SYN | FIN | URG | PUSH 会使接收方应答一个RST | ACK消息；如果端口是打开的，会使接收方应答一个 SYN | ACK消息，这可用于主机探测和端口探测。

如果端口是关闭的，FIN 、URG、PUSH、URG|FIN 、URG|PUSH 、FIN|PUSH 、URG|FIN|PUSH 会使接收方应答一个RST | ACK消息。而对于一个开放端口，Linux和UNIX机器不会应答，而Windows机器将回答RST | ACK消息。这可用于操作系统探测。

检查TCP报文的各个标志位，若出现满足以下任一条件的报文，直接丢弃：

- 6个标志位全为1。
- 6个标志位全为0。
- SYN和FIN位同时为1。

配置维护方法

- 使能、去使能畸形报文防攻击。
  abnormal-packet-defend enable
  undo abnormal-packet-defend enable
  ipv6-abnormal-packet-defend enable
  undo ipv6-abnormal-packet-defend enable
- 清除所有接口板或指定的接口板上畸形报文攻击的统计数据
  reset cpu-defend tcpip-defend statistics [**slot** *slot-number*]
  reset cpu-defend tcpip-defend-v6 statistics [**slot** *slot-number*]

检查加固结果

查看所有接口板或指定的接口板上畸形报文攻击的统计数据。

display cpu-defend tcpip-defend statistics [**slot** *slot-number*]

display cpu-defend tcpip-defend-v6 statistics [**slot** *slot-number*]

配置维护建议

无

?.2. 分片报文攻击防范

安全策略介绍

对于分片报文攻击，teardrop类攻击主要是攻击系统对分片报文重组可能出现问题，系统保证对分片报文重组正确，丢弃重组有重叠的报文。对于重复分片类报文的攻

击，没有什么好方法，由于IP网络上的trunk，负载分担等会造成接口板收不到所有分片，所以不能在接口板上重组，在主控板上就必然涉及到主控板的cpu和板间通讯资源的占用。防范方法是转发引擎在接口板上对分片报文进行单独的car，保证不对cpu造成攻击。Car大小可配置。

攻击方法介绍

分片报文攻击一共包含如下12种

- 分片数量巨大

  攻击者制造大量的小分片，最小为8字节。如果考虑正常情况下，IP头部20个字节，IP载荷最大65515，对这些数据进行分片，每个IP载荷为8，那么一共有：8189. 375片（8189则没有65515，8190则超过65515），这样庞大的分片，这么小的碎片，一般来说都是恶意的。发到路由器上路由器会试图重组这些分片报文，从而消耗大量的CPU资源。

- Tear Drop攻击

  Tear Drop攻击是最著名的IP分片攻击，原理是UDP报文的IP分片错误，第二片包含在第一片之中。第一个分片IP载荷为36字节，IP总长度为56（正确），protocol为UDP，UDP检验和为0（没有检验）；第二片IP载荷为4字节，IP总长度为24（正确），protocol为UDP，offset=3*8=24（错误，正确应该为36）。

- syndrop攻击

  与teardrop的原理类似，只是使用了TCP协议，flag为SYN，而且带有pading。第一片28载荷（0～27，包含TCP头部），IP头部20字节；第二片offset＝24，载荷总长度＝4（24～27），IP头部20字节。

- nesta攻击

  一共三片分片，第一片IP载荷为18（0～17），protocol为UDP，校验和为0；第二片offset为6×8＝48，IP载荷为116字节；没有更多的分片，也就是结束片。第三片offset为0，more frag为1，也就是还有分片，40字节的IP option，都是EOL，IP载荷为224字节。

- fawx攻击

  是一种分片错误的IGMP报文。特征是：发送IGMP报文分片，一共两片，第一片9个bytes，第二个分片offset＝8，IP载荷长度为16字节，没有结束分片。

- bonk攻击

  Bonk攻击和newtear攻击相似，只是第一片IP载荷为36bytes，UDP checksum为0；第二片offset＝32，长度为4字节。

- 死亡之ping攻击

  ICMP echo request总长度大于65535，导致协议栈崩溃。此攻击的方法就是通过简单的IP分片，使IP载荷加上IP头部长度大于65535。

- Jolt攻击

  和死亡之ping很相似，一共173个分片，每个分片380的IP载荷，那么总长度：173*380+20＝65760，远远超过65535。

- 重复分片攻击

  把同样的分片再次发送（可能发送多于2次），这里有两种情况：前后分片相同，因为IP报文传输过程可能会有重传；前后分片不相同，那么，哪一个分片才是应该保留，哪个应该丢弃，还是都丢弃。

- NewTear攻击

Newtear攻击分片方面和syndrop相似，但是protocol使用UDP，第一片28载荷（0～27，包含UDP头部，UDP checksum为0），第二片offset＝24，载荷总长度＝4（24～27）。

- Rose攻击

  IP protocol可以是UDP或者TCP，可以选择。

  – （1）TCP：一共两片分片，第一片IP载荷长度48bytes，第二片IP载荷长度是32bytes，但是offset＝65408，more frag＝0，表示最后一片。

  – （2）UDP：一共两片分片，第一片IP载荷长度40bytes，第二片IP载荷长度是32bytes，但是offset＝65408，more frag＝0，表示最后一片。

配置维护方法

- 使能、去使能分片报文防攻击：

  fragment-flood enable

  undo fragment-flood enable

- 清除所有接口板或指定的接口板上分片报文攻击的统计数据

  reset cpu-defend car fragment statistics

检查加固结果

- 查看所有接口板或指定的接口板上分片报文攻击的统计数据

  display cpu-defend car fragment statistics

- 查看攻击溯源的详细信息

  display attack-source-trace verbose

配置维护建议

无

?.3. TCP Syn Flood 攻击

安全策略介绍

TCP Syn泛洪攻击是一种古老而有效的攻击方式。它属于拒绝服务攻击，这类攻击完全依赖于TCP连接的建立方式。

对于TCP Syn泛洪攻击，华为公司采取对TCP SYN报文总的速率进行限制，保证受到攻击时系统资源不被耗尽。

攻击方法介绍

在TCP的3次握手期间，当服务器收到来自客户端的初始SYN信息时，向客户端返回一个SYN+ACK报文并在内存中创建一个入口。服务器在等待客户端的最终ACK信息时，该连接一直处于半连接状态。如果服务器最终没有收到ACK信息包，则重新发送一个SYN+ACK到客户端。如果经过多次重试，客户端始终没有返回ACK信息，则服务器关闭会话并从内存中刷新会话。从传输第一个SYN+ACK到会话关闭大约需要30秒。

在这段时间内，攻击者可能将数十万个SYN信息发送到开放的端口，并且不回应服务器的SYN+ACK信息。服务器内存很快就会超过负荷，且无法再接受任何新的连接，并将现有的连接断开。

攻击者通常不接收来自服务器的SYN-ACK信息，因此可以伪造SYN信息的源地址，这就使发现攻击的真实来源更加困难。

因为SYN+ACK信息没有发送到攻击者，因此为攻击者节省了带宽。

配置维护方法

- 使能、去使能TCP Syn Flood报文防攻击。

  tcpsyn-flood enable

  undo tcpsyn-flood enable

  ipv6-tcpsyn-flood enable

  undo ipv6-tcpsyn-flood enable

  car tcpsyn cir 1000 cbs 10000

  undo car tcpsyn
- 清除所有接口板或指定的接口板上TCP Syn Flood报文攻击的统计数据。

  reset cpu-defend car index 48 statistics [slot *slot-number* **]**

检查加固结果

查看所有接口板或指定的接口板上TCP Syn Flood报文攻击的统计数据。

display cpu-defend car index 48 statistics [slot *slot-number* **]**

配置维护建议

无

?.4. UDP Flood 攻击

安全策略介绍

对于UDP端口7，13，19的报文，认为是攻击报文，直接丢弃。

实现命令行使能UDP FLOOD防攻击。

攻击方法介绍

- Fraggle攻击

  Fraggle攻击的原理就是利用UDP 7号端口（UDP Echo Request），7端口的服务和ICMP echo基本一样，都是把收到的报文载荷原封不动的回复回去，以测试源和目的之间的网络状况。和Smurf攻击的原理一样，把源地址伪造成受害者地址，目点地址写成某个广播地址，目的端口为7，源端口可以不是7，也可以是7。如果该广播网络有很多主机都起了UDP echo服务，那么受害者将收到很多回复报文，达到攻击的效果。
- UDP诊断端口攻击

  对诊断端口（7-echo，13-daytime，19-Chargen等）随机发包，如果同时发送的数据包数量很大，造成泛洪，可能影响网络设备正常工作。很多设备厂家都会默认打开一些small server，以进行网络诊断，设备管理等作用，但同时也是暴露给攻击者一个很好的攻击机会。Pepsi攻击就是利用设备的诊断端口，在设备的诊断端口进行泛洪，造成设备拒绝服务。

配置维护方法

- 使能、去使能UDP Flood报文防攻击。
  udp-packet-defend enable
  undo udp-packet-defend enable
  ipv6-udp-packet-defend enable
  undo ipv6-udp-packet-defend enable
- 清除所有接口板或指定的接口板上UDP Flood报文攻击的统计数据。
  reset cpu-defend tcpip-defend statistics [**slot** *slot-number*]
  reset cpu-defend tcpip-defend-v6 statistics [**slot** *slot-number*]

检查加固结果

查看所有接口板或指定的接口板上UDP Flood报文攻击的统计数据。

display cpu-defend tcpip-defend statistics [**slot** *slot-number*]

display cpu-defend tcpip-defend-v6 statistics [**slot** *slot-number*]

配置维护建议

无

?.5. ICMP Flood 攻击

安全策略介绍

在接口板对总的ICMP报文进行速率控制。实现命令行对ICMP速率可配置，实现命令行实现单板粒度使能ICMP Flood防攻击。

攻击方法介绍

ICMP Flood攻击发送速度极快的ICMP报文，当一个程序发送数据包的速度达到了每秒1000个以上，它的性质就成了洪水产生器，大量的ICMP Echo Request报文发送给攻击被测对象，被测对象主机就即回复很多ICMP Echo Reply或ICMP不可达报文，攻击者伪造了虚假源地址后，被测对象主机就会徒劳的回复大量ICMP报文给虚假地址，从而消耗自身的系统资源，最终可能导致服务器停止响应。同时也可能存在ICMP其他类型的报文攻击

配置维护方法

- 使能、去使能ICMP Flood报文防攻击。
  car icmp cir 100 cbs 3000
  undo car icmp
- 清除所有接口板或指定的接口板上ICMP Flood报文攻击的统计数据。
  reset cpu-defend car protocol icmp statistics

检查加固结果

查看所有接口板或指定的接口板上ICMP Flood报文攻击的统计数据。

display cpu-defend car protocol icmp statistics

配置维护建议

无

?.6. ND 非法报文攻击防范

安全策略介绍

ND非法报文攻击防范是指控制非法ND报文(IPv6 NS/NA/RS/RA/Redirect/CPS)的上送。转发引擎支持NS/NA/RS/RA/Redirect/CPS六种报文的过滤，其中分片报文固定丢弃，非分片报文未命中本机路由的丢弃，默认行为是不丢弃，通过安全命令行进行控制丢弃。

攻击方法介绍

表 1-12 RS/RA/NS/NA/Redirect/CPS 六种报文的 ICMP 头

报文类型	ICMP type
RS	0x85
RA	0x86
NS	0x87
NA	0x88
Redirect	0x89
CPS	0x94

- 非分片：RS/RA/NS/NA/Redirect/CPS，IPv6头nextheader=0x3A或源IP非linklocal地址。
- 分片：RS/RA/NS/NA/Redirect/CPS，IPv6头nextheader=0x2C，IPv6扩展头里的NextHeader=0x3A。

以上报文为非法ND报文，上送后会造成资源浪费，存在安全风险。

当使能了ND非法报文的攻击防范功能时，直接丢弃满足以上条件的报文。

配置维护方法

- 清除所有接口板或指定的接口板上ND非法报文攻击防范功能的统计计数信息。
  reset nd packet filter statistics [**slot** *slot-id*]

检查加固结果

查看所有接口板或指定的接口板上ND非法报文攻击防范功能的统计计数信息。

display nd packet filter statistics [**slot** *slot-id*]

配置维护建议

无

1.1.8 缩略语表

表 1-13 缩略语清单

英文缩写	英文全称	中文全称
AAA	Authentication, Authorization, Accounting	认证、授权、记账
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
BFD	Bidirectional Forwarding Detection	双向转发检测
BGP	Border Gateway Protocol	边界网关协议
CAR	Committed Access Rate	接入速率限制
CP	Central Process	集中处理
CPCAR	Central Process CAR	CPU速率限制
CPU	Center Process Unit	中央处理器
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DOS	Deny of Service	拒绝服务(攻击)
FTP	File Transfer Protocol	文件传输协议
GTSM	The Generalized TTL Security Mechanism	基于TTL限制的安全防护策略
GRE	Generic Routing Encapsulation	通用路由封装
GRPC	Google Remote Procedure Call Protocol	Google远程过程调用协议
HTTP	Hypertext Transport Protocol	超级文本传送协议
IS-IS	Intermedia System-Intermedia System	中间系统－中间系统
MPLS	Multi-Protocol Label Switch	多协议标签交换
NTP	Network Time Protocol	网络时间协议

英文缩写	英文全称	中文全称
OSPF	Open Shortest Path First	开放最短路径优先
RADIUS	Remote Authentication Dial in User Service	远端用户拨入鉴权服务
RIP	Routing Information Protocol	选路信息协议
SNMP	Simple Network Management Protocol	简单网管协议
SOC	Security Operating Center	安全管理中心
TACACS	Terminal Access Controller Access-Control System	终端访问控制器访问控制系统
TCP	Transmission Control Protocol	传输控制协议
URPF	Unicast Reverse Path Forwarding	单播反向路径转发
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议