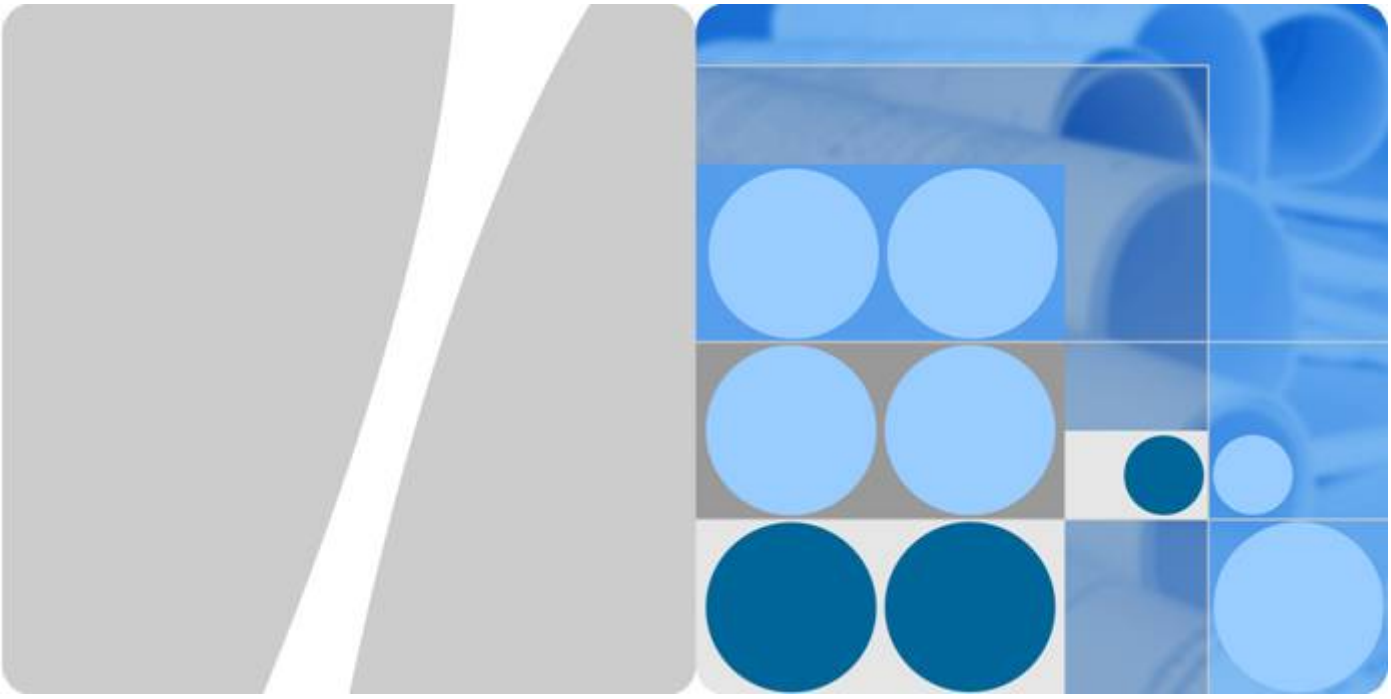


NetEngine AR5700, AR6700, AR8000
V600R022C10

配置指南-安全配置

文档版本　02

发布日期　2023-09-22

华为技术有限公司

HUAWEI

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://e.huawei.com

目 录

1 前言

读者对象

本文档适用于负责管理和维护AR路由器的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络管理经验。此外，您应该非常了解您的网络，包括组网拓扑，已部署的网络业务等。

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
危险	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。
警告	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。
注意	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。
须知	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、设备性能降低或其他不可预知的结果。 “须知”不涉及人身伤害。
说明	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。

命令行格式约定

在本文中可能出现下列命令行格式，它们所代表的含义如下。

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&的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

接口编号约定

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。

安全约定

- 密码和认证配置的声明
  - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
  - 配置显示模式的密码时，请不要以“%@%#.....%@%#”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的显示密码。
  - 文中出现的密码仅为配置示例，请自行配置符合密码复杂度要求的密码并妥善保管，避免密码泄露。
  - 不同特性的密文密码不能互相使用，例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。
  - BootLoader中可清空Console接口密码。请妥善管理BootLoader密码，以免泄露后导致Console接口密码被恶意串改。
  - 如果使用**authentication-mode**命令配置认证方式为不认证方式（none）时，则任何用户只要输入任意的用户名和密码后都会认证成功。因此，为保护设备或网络安全，建议开启认证方式，保证用户经过认证后才可以访问设备或网络。
- 加密算法的声明

  目前设备采用的加密算法包括DES、3DES、AES、DSA、RSA、DH、ECDH、HMAC、SHA1、SHA2、MD5，具体采用哪种加密算法请根据场景而定。请优先采用我们的建议，否则会造成无法满足您安全防御的要求。
  - 对称加密算法建议使用AES（128位及以上密钥）。

  - 非对称加密算法建议使用RSA（2048位及以上密钥），使用非对称算法时，加密和签名要使用不同的密钥对。
  - 数字签名建议使用RSA（2048位及以上密钥）。
  - 密钥协商建议使用DH（3072位及以上密钥）或者ECDH（256位及以上密钥）。
  - 哈希算法建议使用SHA2（256及以上密钥）。
  - HMAC（基于哈希算法的消息验证码）算法建议使用HMAC-SHA2。
  - SHA1、SHA2和MD5加密算法是不可逆的，DES、3DES、RSA和AES加密算法是可逆的。
  - SSH协议支持SSH1.X（SSH2.0之前的版本）和SSH2.0版本，建议使用SSH2.0版本。SSH2.0版本中，使用CBC模式的对称加密算法可能存在数据受到明文恢复攻击而泄露加密传输的内容，因此，在SSH2.0中不建议使用CBC模式对数据加密。
  - SSL通过握手在客户端和服务器之间建立会话，完成双方身份的验证、密钥和加密套件的协商，在通信过程中建议使用TLS1.2及以上版本的安全套件。TLS版本中，使用CBC模式的对称加密算法可能存在数据受到明文恢复攻击而泄露加密传输的内容，因此，在TLS版本中不建议使用CBC模式对数据加密。

- 个人数据的声明

  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（如终端用户的IP地址或MAC地址），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。在使用、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。

- 系统主密钥的声明

  系统主密钥是对本地保存的数据进行加解密时使用的密钥。设备出厂时会使用缺省的主密钥对数据进行加密，由于此密钥是系统随机生成的密钥，比较安全，不建议用户经常修改。如果用户需要使用自己的密钥对本地保存的数据进行加解密，可以修改系统主密钥。

参考标准和协议

请登录**华为网站**，搜索“标准协议顺从表”，获取《华为AR产品协议顺从表》。

特性使用的声明

- 本手册仅作为使用指导，其内容（如CLI命令格式、命令输出）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，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、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会使设备测试出的最大值与手册中提供的数据不一致。
- 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，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。
- 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。

- 设备支持通过FTP、TFTP、SFTPv1&v2及FTPS传输文件。使用FTP、TFTP、SFTPv1协议存在安全风险，建议您使用SFTPv2或FTPS方式进行文件操作。
- 设备支持通过Telnet协议和STelnetv1&v2协议登录。使用Telnet和STelnetv1协议存在安全风险，建议您使用STelnetv2登录设备。
- 设备支持通过SNMPv1&v2c&v3协议管理设备。使用SNMPv1&v2c存在安全风险，建议您使用SNMPv3管理设备。
- 设备支持镜像功能，该功能主要用于网络检测和故障管理，可能涉及使用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。在使用、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。
- 设备支持报文捕获功能，该功能主要用于检测通信传输中的故障和错误。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。

产品软件和网管软件版本配套关系

产品软件和网管软件版本配套关系如下所示。

AR产品软件版本	eSight网管软件版本
V600R022C10	eSight 22.1.0

产品软件和控制器软件版本配套关系

AR产品软件版本	控制器软件版本
V600R022C10	iMaster NCE-Campus V300R022C10

2 安全综述

网络安全威胁

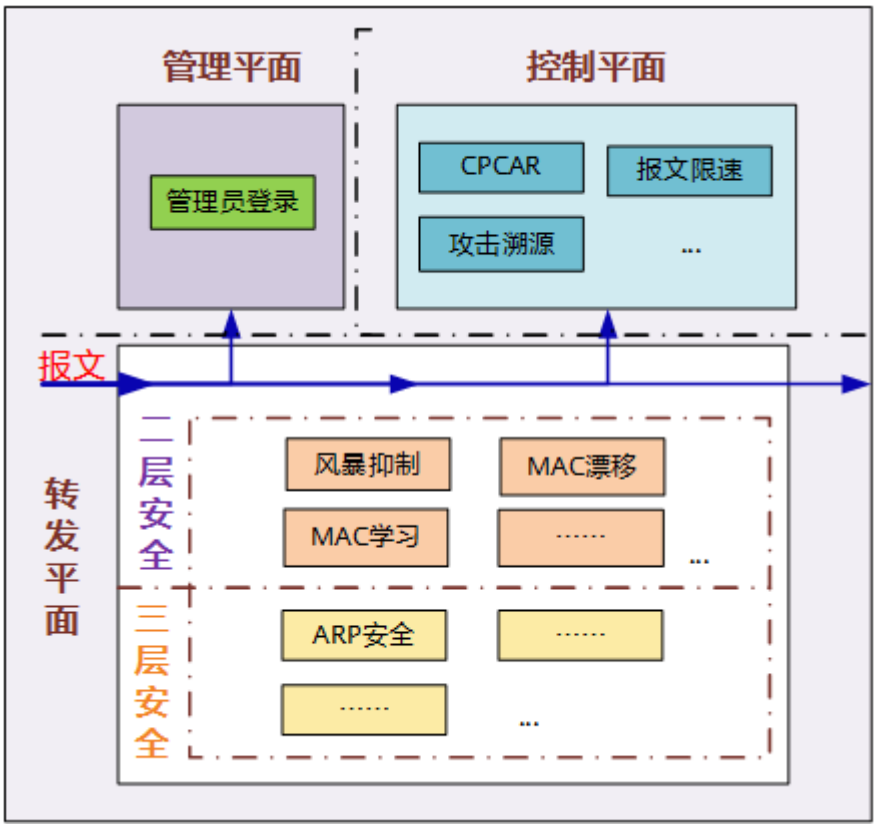
网络安全威胁是指网络系统所面临的，由已经发生的或潜在的安全事件对某一资源的保密性、完整性、可用性或合法使用所造成的威胁。能够在不同程度、不同范围内解决或者缓解网络安全威胁的手段和措施就是网络安全服务。

设备安全最重要的任务就是能够正常转发数据，并保证数据在传输过程中不被截获或者篡改。设备的网络安全主要包括以下三个方面：

- 保密性：设备存储、处理和传输的信息，不会被泄露到非授权的用户、实体或过程。即信息只为授权用户使用。
- 完整性：信息未经授权不能进行改变的特性。即网络信息在设备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：在要求的外部资源得到保证的前提下，设备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。业务持续可用，满足电信级服务质量要求。

为了满足上述要求，从以下三个平面对网络安全进行规划和部署。

图 2-1 安全规划部署图



管理平面

管理平面的安全重点在于确保设备能够被合法管理，包括哪些用户可以登录设备，登录到设备上的用户又可以进行哪些操作等。如图1所示，设备管理平面的安全主要通过只允许管理员登录设备来实现。管理员登录就是保证管理员安全的管理设备，设备通过设置用户名和密码、ACL限制用户登录，通过STelnet登录方式保证管理员登录过程安全，通过设置用户的级别控制用户操作权限。详细的原理和配置可以参见登录设备命令行界面。

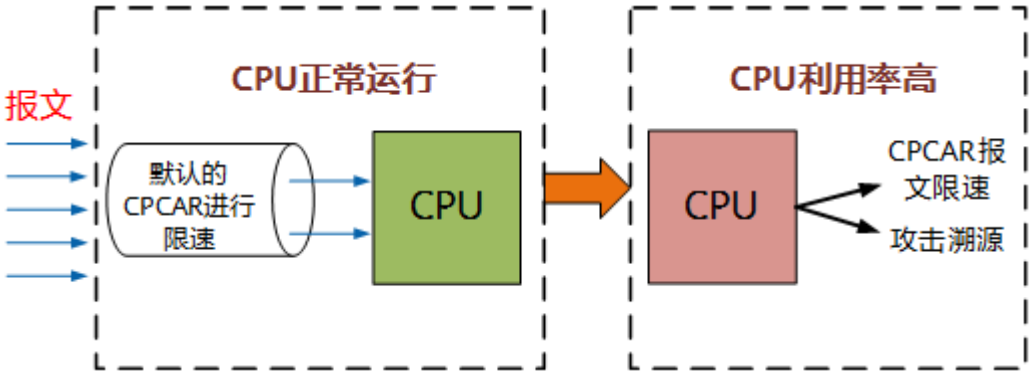
控制平面

控制平面主要通过CPU实现转发控制。CPU就像我们的大脑，指挥着设备各项机能的正常运转。CPU的安全是设备和协议正常运行的前提。如果上送CPU处理的协议报文过多导致CPU繁忙，设备性能就会下降，业务就会中断。因此，作为设备的核心部件，CPU也就成为非法用户攻击的对象。设备支持的控制平面的安全配置主要包括**本机防攻击**。

如图2所示，为了保证CPU的正常运行，设备使用默认的CPCAR值对上送的协议报文进行限速。如果经过设备默认的CPCAR限速后，上送CPU的报文依然超过了CPU可以处理的范围，CPU利用率很高，还可以通过以下方式做进一步的处理：

- 调整CPCAR值：缩小CPCAR值，减少上送CPU的协议报文的数量。
- 攻击溯源：对上送CPU的报文进行分析统计，设置检查阈值，对于超过检查阈值的报文执行相应的惩罚措施，如丢弃报文、Shutdown接口、设置黑名单等。

图 2-2 CPU 防攻击处理流程



转发平面

转发平面的作用就是通过查询转发表项指导数据流量正确转发，因此针对转发平面的攻击主要为以下两种：

- 耗尽转发表资源，导致合法用户的转发表无法被学习，合法用户的流量无法被转发。
- 篡改转发表，导致合法用户的流量转发至错误的地方。

基于设备网络部署位置，主要分为二层网络的防攻击方法和三层网络的防攻击方法。

- 二层网络：二层网络数据转发依赖MAC表，所有数据流量的转发都需要查找MAC表，因此MAC表也就成为非法用户攻击二层网络的主要目标。非法用户通过发送大量的报文，迅速耗尽MAC表资源，使报文因查找不到MAC表项进行广播，从而占用带宽资源，产生广播风暴。设备支持通过**风暴抑制**等方式来保护MAC表的安全。
- 三层网络：三层网络数据转发依赖ARP表和路由表。路由表是通过路由协议协商生成的，因此非法用户很难对此进行攻击。ARP表是通过协议报文生成的，非法用户可以发送大量的协议报文或者伪造协议报文使ARP表项出现异常。因此ARP表是设备在三层网络中保护的主要对象。设备支持通过ARP安全

3 安全区域配置

3.1 安全区域简介

定义

安全区域是绑定了一个或多个物理接口或逻辑接口的逻辑实体，绑定了同一个安全区域的接口下的网络具有相同的安全属性。

目的

通过将各接口下连接的网络划分到不同的安全区域，可以将设备连接的网络划分为不同的安全等级。

可以通过配置基于源、目的安全区域匹配条件的策略对跨安全区域的业务流量进行集中管控，无需将逐个IP或逐个网段作为匹配条件配置安全策略，大大降低了策略配置的复杂度。

3.2 安全区域原理描述

设备中的安全区域分为预定义安全区域和自定义安全区域，所有的安全区域按照安全级别的不同从1到100划分优先级，数字越大表示优先级越高。管理员可以使用设备上缺省存在的预定义安全区域（详见**表3-1**），也可以根据实际需求创建自定义安全区域并为其设置优先级（如**图3-1**所示，“公共区域”网络划分到优先级为30的自定义安全区域“zone1”下）。

MEth管理接口不属于任何安全区域，也不能加入任何安全区域（如**图3-1**中的“MEth0/0/0”）。一个接口只能加入到一个安全区域，一个安全区域下可以加入多个接口（如**图3-1**所示，除管理口外的每个接口都只加入到了一个安全区域，“trust”

安全区域下加入了两个接口，分别对应了“办公区域1”和“办公区域2”两个网络）。

图 3-1 安全区域、接口和网络的关系

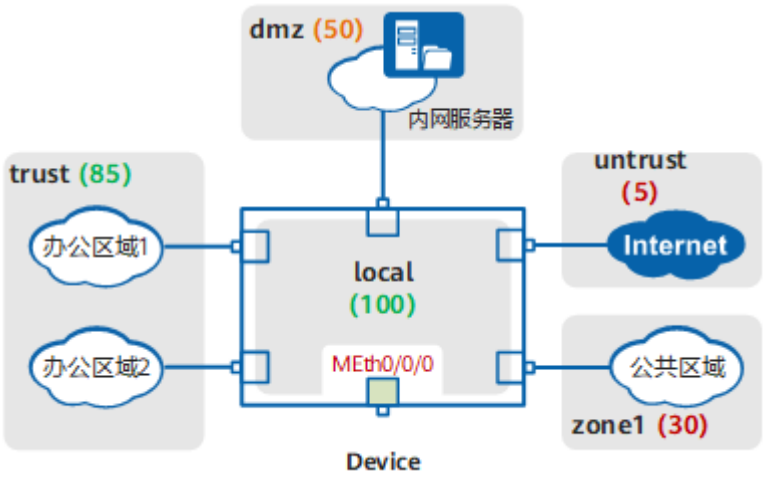


表 3-1 设备上缺省存在的预定义安全区域

区域名称	优先级	说明
非受信区域（untrust）	低安全级别的安全区域，优先级为5。	untrust安全区域通常用于定义Internet等不安全的网络。
非军事化区域（dmz）	中等安全级别的安全区域，优先级为50。	dmz安全区域通常用于定义内网服务器所在区域。 该安全区域可以放置需要对外提供网络服务的设备，如WWW服务器、FTP服务器等。这些设备虽然部署在内网，但是经常需要被外网访问，外部恶意用户可能会利用这些服务器中的某些安全漏洞攻击内部网络。同时，由于这些设备一般不被允许主动访问外网，所以需要将其部署在一个优先级低于trust、高于untrust的安全区域中。 **说明** dmz（Demilitarized Zone）起源于军方，是介于严格的军事管制区和松散的公共区域之间的一种有着部分管制的区域。设备引用了这一术语，指代一个逻辑上和物理上都与内部网络和外部网络分离的安全区域，解决了服务器的放置问题。
受信区域（trust）	较高安全级别的安全区域，优先级为85。	trust安全区域通常用于定义内网终端用户所在区域。

区域名称	优先级	说明
本地区域（local）	最高安全级别的安全区域，优先级为100。	local安全区域定义的是设备自身，包括设备的各接口。 凡是由设备构造并主动发出的报文均可认为是从local安全区域中发出，凡是需要设备响应并处理（而不仅是检测或直接转发）的报文均可认为是由local安全区域接收。 **说明** 向安全区域中添加接口，是定义该接口所连的网络属于该安全区域，而接口本身还是属于local安全区域。 由于local区域的特殊性，在很多需要设备本身进行报文收发的业务中，需要放开对端所在安全区域与local安全区域之间的安全策略。包括： • 需要对设备本身进行管理的情况。例如Telnet登录、接入SNMP网管等。 • 设备本身作为某种服务的客户端或服务器，需要主动向对端发起请求或处理对端发起的请求的情况。例如FTP、NTP等。

3.3 安全区域配置注意事项

License 依赖

安全区域无需License许可即可使用。

硬件依赖

表 3-2 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 3-3 本特性的使用限制

特性限制	系列	涉及产品
预定义安全区域不能被删除，优先级也无法被重新配置或清除。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG /AR8700-8
不能修改本地安全区域local下的任何配置，包括向local区域中添加接口。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG /AR8700-8
不同的安全区域不能配置相同的名称和优先级。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG /AR8700-8
已经分配给策略使用的自定义安全区域不能被删除 ，但可以进行修改优先级、增删绑定的接口等操作。删除安全区域时，该安全区域的所有配置都将被删除。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG /AR8700-8
接口绑定某自定义安全区域后，如果该自定义安全区域被删除，则接口上的安全区域配置信息会被清空，接口处于未绑定安全区域的状态。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG /AR8700-8

特性限制	系列	涉及产品
接口退出安全区域后，已经生成的会话需要等待老化删除或手动删除会话，可执行命令display session aging-time查看会话老化周期。删除会话可能会导致业务中断，请谨慎操作。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG /AR8700-8

3.4 安全区域缺省配置

安全区域的缺省配置如表3-4所示。

表 3-4 安全区域缺省配置

参数	缺省配置
预定义安全区域及其优先级	非受信区域（untrust），优先级为5。
	非军事化区域（dmz），优先级为50。
	受信区域（trust），优先级为85。
	本地区域（local），优先级为100。
接口下网络所属的安全区域	接口下的网络不属于任何安全区域。

3.5 配置安全区域

背景信息

设备上的安全区域分为预定义安全区域和自定义安全区域。如果需要在预定义的四个安全区域之外为网络划分更多的安全等级，可以在设备上创建自定义安全区域并设置安全区域的优先级。安全区域创建完成后，需要将接口加入其所属的安全区域中，从该接口接收或发送的报文即会被判定为属于该安全区域。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建安全区域，并进入安全区域视图。

```
firewall zone [ name ] zone-name
```

根据以*zone-name*为名的安全区域是否已经存在于系统中，分为如下两种情况：

- 若安全区域已经存在，不必配置关键字**name**，执行该命令后将直接进入安全区域视图。

- 若安全区域不存在，则需要配置关键字**name**，以创建该安全区域，并进入安全区域视图。此外，可以通过**firewall zone name** *zone-name* **id** *id* 命令指定安全区域的ID。未指定ID时，系统会自动为创建的安全区域分配未被占用的ID。

预定义安全区域无需创建，也不能删除。可以通过**firewall zone** *zone-name*命令进入其安全区域视图。

步骤3 配置安全区域的描述信息。

description *description-text*

为便于识别和维护创建的自定义安全区域，可以为自定义安全区域配置描述信息。

步骤4 **可选:**（可选）为自定义安全区域配置优先级。

set priority *security-priority*

缺省情况下，自定义安全区域未配置优先级。

安全区域优先级的取值越大，优先级越高。

步骤5 将接口加入安全区域。

add interface *interface-type* { *interface-number* | *interface-number.subinterface-number* }

MEth管理接口不属于任何安全区域，也不能加入任何安全区域。一个接口只能加入到一个安全区域，一个安全区域下可以多次使用此命令加入多个接口。

说明

local安全区域定义的是设备自身，包括设备的各接口本身，因此：

- local安全区域下不能加入任何接口；
- 向local以外的其他安全区域中添加接口，是将接口下所连的网络加入该安全区域，接口本身还是属于local安全区域。

----结束

检查配置结果

执行命令**display zone** [*zone-name*] [**interface** | **priority**]，查看安全区域的配置信息。

后续处理

配置基于安全区域的策略，对不同安全区域间传输的流量进行管控。

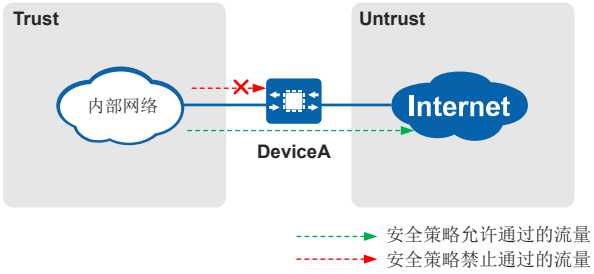
4 安全策略配置

4.1 安全策略简介

定义

安全策略对通过设备的数据流进行检验，控制设备对流量的转发。如**图4-1**所示：

图 4-1 通过安全策略控制流量



安全策略是由匹配条件（例如五元组、时间段等）和动作组成的控制规则，设备收到流量后，对流量的属性（五元组、时间段等）进行识别，并将流量的属性与安全策略的匹配条件进行匹配。如果所有条件都匹配，则此流量成功匹配安全策略。流量匹配安全策略后，设备将会执行安全策略的动作。

- 如果动作为“允许”，则对流量进行如下处理：

  - 如果没有配置内容安全检测，则允许流量通过。
  - 如果配置内容安全检测，最终根据内容安全检测的结论来判断是否对流量进行放行。
- 如果动作为“禁止”，则禁止流量通过。

目的

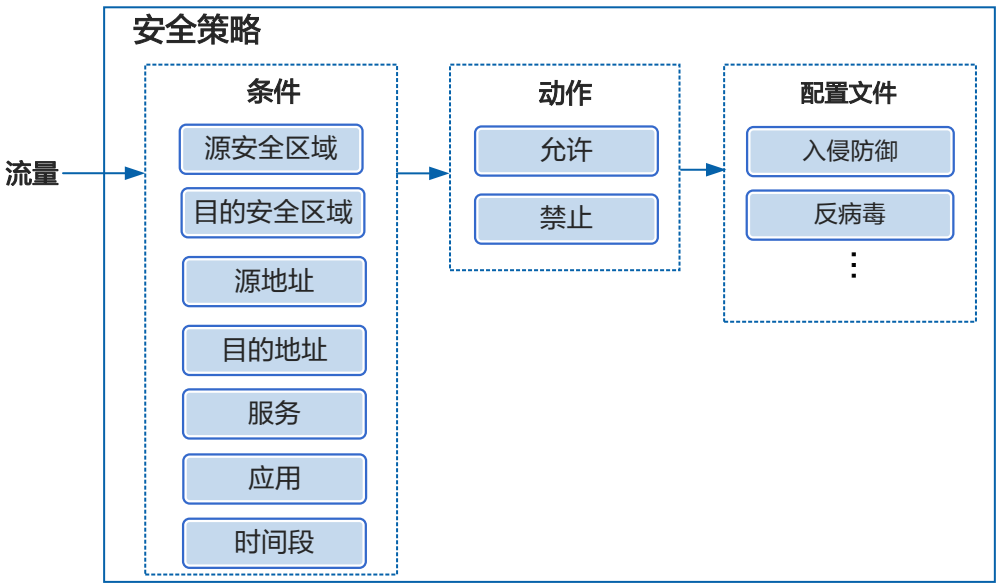
为了对进出网络的访问行为进行控制，保护特定网络免受“不信任”网络的攻击，同时允许两个网络之间可以进行合法的通信，可以通过安全策略技术来实现设备的访问控制。

4.2 安全策略原理描述

4.2.1 安全策略的组成

安全策略是由匹配条件和动作组成的控制规则。设备接收流量后，对流量的属性（五元组、时间段等）进行识别，并将流量的属性与安全策略的匹配条件进行匹配。如果所有条件都匹配，则此流量成功匹配安全策略。流量匹配安全策略后，设备将会执行安全策略的动作。

图 4-2 安全策略的组成



安全策略的匹配条件

安全策略的匹配条件均为可选，如果不选，默认为any，表示该安全策略与任意报文匹配。安全策略的匹配条件具体如表4-1所示：

表 4-1 安全策略的匹配条件

匹配条件	作用	举例
源安全区域 目的安全区域	指定流量发出/去往的安全区域。	假设内网用户所在的安全区域为trust，外网所在的安全区域为untrust，如果希望控制内网用户访问外网的权限，则可以配置安全策略规则，指定源安全区域为trust，目的安全区域为untrust。
源地址 目的地址	指定流量发出/去往的地址，取值可以是地址、地址组、域名组。	举例1：如果希望企业员工能够访问公网的web服务器，则可以配置安全策略规则，指定源地址为企业员工所在的地址，目的地址为any。 举例2：如果希望企业员工仅能访问企业内部的web服务器，则可以配置安全策略规则，指定源地址为企业员工所在的地址，目的地址为企业内部的web服务器所在的地址。 举例3：如果希望企业员工仅能访问几个搜索网站，则可以将这些搜索网站的域名加入域名组。配置安全策略规则，指定源地址为企业员工所在的地址，目的地址为配置的域名组。
服务	指定流量的协议类型或端口号。	假设某企业部署两台业务服务器，其中Server1通过TCP 8888端口对外提供服务，Server2通过UDP 6666端口对外提供服务。为了控制PC访问这两台服务器，需要在安全策略中配置服务的协议类型和端口号。

匹配条件	作用	举例
应用	指定流量的应用类型。通过应用，设备能够区分使用相同协议和端口号的不同应用程序，使网络管理更加精细。 通常情况下，某一应用可能包含了多种服务，而某个服务也可能被多个不同的应用所使用。与服务相比，应用的匹配粒度更加精细，可以细化到某一具体的应用程序。由于服务匹配条件的控制粒度较为粗犷，当安全策略的动作为“阻断”时，可能会导致其他采用相同协议的应用也被阻断，因此推荐采用应用作为策略的匹配条件。	假设某学校希望禁止学生使用网页IM和网页游戏应用，则可以配置安全策略规则，指定匹配条件应用为网页IM和网页游戏，动作为禁止。
时间段	指定安全策略生效的时间段。	如果企业希望工作时间内（8:30～12:00，13:00～17:30）不允许员工上网，午休时间（12:00～13:00）允许员工上网，则可以配置安全策略规则，指定匹配条件时间段。

安全策略的动作

如果安全策略配置的所有匹配条件都匹配，则此流量成功匹配该安全策略规则。流量匹配安全策略后，设备将会执行安全策略的动作。安全策略的动作包括：

- 允许：如果动作为“允许”，则对流量进行如下处理：
  - 如果没有配置内容安全检测，则允许流量通过。
  - 如果配置内容安全检测，最终根据内容安全检测的结论来判断是否对流量进行放行。内容安全检测包括反病毒、入侵防御等，它是通过在安全策略中引用安全配置文件实现的。如果其中一个安全配置文件阻断该流量，则设备阻断该流量。如果所有的安全配置文件都允许该流量转发，则设备允许该流量转发。
- 禁止：表示拒绝符合条件的流量通过。

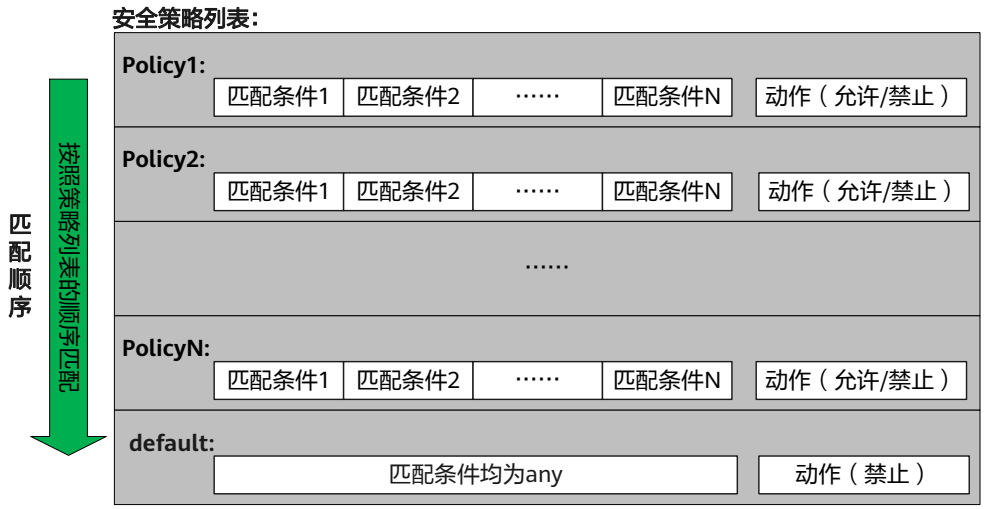
4.2.2 安全策略的匹配过程

只有当流量的出入接口均为加入安全区域的三层接口时，设备才会对其进行安全策略匹配，二层报文不进行安全策略匹配。如果想要控制流量转发，可以创建安全策略。一般针对不同的业务流量，设备上会配置多条安全策略，下面将具体介绍下多条安全策略的匹配顺序和匹配规则等。

安全策略的匹配规则

安全策略的匹配规则如图4-3所示，每条安全策略中包含多个匹配条件，各个匹配条件之间是“与”的关系，报文的属性与各个条件必须全部匹配，才认为该报文匹配这条规则。一个匹配条件中可以配置多个值，多个值之间是“或”的关系，报文的属性只要匹配任意一个值，就认为报文的属性匹配了这个条件。

图 4-3 安全策略的匹配规则



当配置多条安全策略规则时，安全策略列表默认是按照配置顺序排列的，越先配置的安全策略规则位置越靠前，优先级越高。安全策略的匹配就是按照策略列表的顺序执行的，即从策略列表顶端开始逐条向下匹配，如果流量匹配了某个安全策略，将不再进行下一个策略的匹配。所以安全策略的配置顺序很重要，需要先配置条件精确的策略，再配置宽泛的策略。如果某条具体的安全策略放在通用的安全策略之后，可能永远不会被命中。例如：

FTP服务器地址为10.1.1.1，允许IP网段为10.2.1.0/24的办公区访问，但要求禁止两台临时办公PC（10.2.1.1、10.2.1.2）访问FTP服务器。需要按照如下顺序配置安全策略：

序号	名称	源地址	目的地址	动作
1	policy1	10.2.1.1 10.2.1.2	10.1.1.1	禁止

序号	名称	源地址	目的地址	动作
2	policy2	10.2.1.0/24	10.1.1.1	允许

对比两条安全策略，policy1条件细化，policy2条件宽泛，如果不按照上述顺序配置安全策略，则policy1永远不会被命中，就无法满足禁止两台临时办公PC（10.2.1.1、10.2.1.2）访问FTP服务器的需求。

通常的业务情况是先有通用规则，后有例外规则。在初始规划时，可以尽可能地同时把通用规则和例外规则列出来，按照正确的顺序配置。但是在维护阶段可能还会添加例外规则，因此需要在配置后调整顺序。

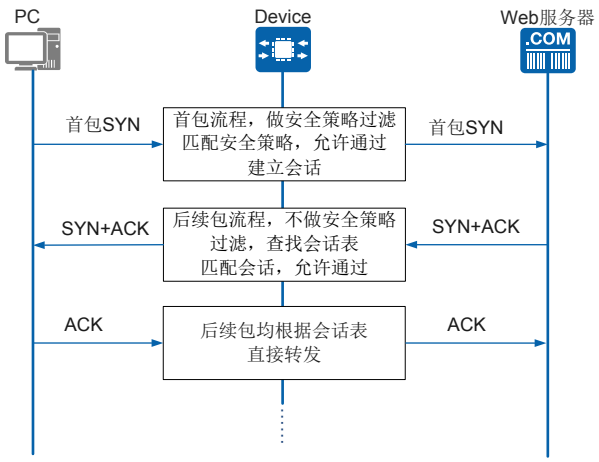
如果所有配置的策略都未匹配，则将匹配缺省安全策略。缺省安全策略位于策略列表的最底部，优先级最低，所有匹配条件均为any，动作缺省为允许。缺省安全策略可以修改默认动作。有一个例外，对于同一安全区域内的流量，默认不受缺省安全策略控制，缺省转发动作为允许。也可以修改为同域流量默认受缺省安全策略控制。

安全策略的过滤机制

对于同一条数据流，只需在访问发起的方向上配置安全策略，反向流量无需配置安全策略。即首包匹配安全策略，通过安全策略过滤后建立会话表，后续包直接匹配会话表，无需再匹配安全策略，提高业务处理效率。以客户端PC访问Web服务器为例，说明安全策略的过滤机制：

如图4-4所示，客户端PC访问Web服务器，当流量到达设备后，执行首包流程，做安全策略过滤，匹配安全策略，设备允许报文通过，同时建立会话，会话包含了PC发出报文的信息，如源/目的地址、源/目的端口号等。当Web服务器回应请求报文时，设备会查找会话表，将回应请求报文中的信息与会话表中的会话信息进行比对，如果该报文中的信息与会话中的信息相匹配，且符合协议规范对后续包的定义，则认为这个报文属于PC访问Web服务器行为的后续回应报文，直接允许这个报文通过。

图 4-4 客户端 PC 访问 Web 服务器



4.2.3 本地安全策略

安全策略不仅可以控制通过设备的流量，也可以控制本地流量。本地流量是指目的为设备自身或者从设备自身发出的流量。

在很多需要设备本身进行报文收发的应用中，需要放开本地流量的安全策略。包括：

- 需要对设备进行管理的情况。例如Telnet登录、接入SNMP网管等。
- 设备作为某种服务的客户端或服务器，需要主动向对端发起请求或处理对端发起的请求的情况。例如FTP、NTP、DNS、升级服务、邮件外发等。

设备本身所在安全区域为Local区域，这是控制本地流量的安全策略的配置关键点。

4.2.4 安全策略的例外情况

对于出入接口均为三层接口且都加入安全区域的流量，也存在不受安全策略控制的情况：

- 安全策略仅对单播报文进行控制，对广播和组播报文不做控制。
- 下表中的协议均为网络互联互通协议，为了安全起见，这些协议的单播报文默认受安全策略控制。如果希望设备能够快速接入网络，可以配置**undo firewall packet-filter basic-protocol enable**命令，使这些协议的单播报文不受安全策略控制。

表 4-2 网络互联互通协议受安全策略控制情况

协议类型	经过设备的报文	到设备自身的报文/从设备发出的报文	说明
BGP	受控	受控	BGP只存在单播报文。
DHCPv4	• 单播报文(UDP端口号67/68)：受控 • 广播报文(UDP端口号67/68)：不受控	• 单播报文(UDP端口号67/68)：受控 • 广播报文(UDP端口号67/68)：不受控	可以依据目的IP地址来区分是单播报文或广播报文。
OSPF	• 单播报文：受控	• 单播报文：受控 • 组播报文：不受控	• 经过设备的OSPF报文只有配置虚连接时才会出现，且该场景下只存在OSPF单播报文。 • 可以依据目的IP地址来区分是单播报文或组播报文。
BFD	• 单播报文：受控 • 组播报文：不受控	• 单播报文：受控 • 组播报文：不受控	可以依据目的IP地址来区分是单播报文或组播报文。

协议类型	经过设备的报文	到设备自身的报文/从设备发出的报文	说明
HRP	不涉及	受控	管理报文：UDP，源端口号49152，目的端口号18514 数据报文：UDP，源端口不固定（每CPU不同），目的端口号18514

- 多通道协议在配置ASPF功能后，设备对数据通道的报文不受安全策略控制。

4.3 安全策略配置注意事项

License 依赖

安全策略无需License许可即可使用。

硬件依赖

表 4-3 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 4-4 本特性的使用限制

特性	特性限制	系列	涉及产品
一体化策略规则管理	rule name不支持中文字符。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8
一体化策略规则管理	设备中存在多种策略，策略类型包括安全策略和NAT策略，多种策略间规格共享，并相互抢占资源。到达规格上限后，无法配置新的策略。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8
安全策略	设备对流量进行IPS/AV/应用识别等内容安全的一体化检测时，会对整机的性能有一定的影响。在配置安全策略和引用内容安全的配置文件时，请根据实际需求有选择性的进行配置。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8

特性	特性限制	系列	涉及产品
安全策略	只有当流量的出入接口均为加入安全区域的三层接口时，设备才会对其进行安全策略匹配，二层报文不进行安全策略匹配。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
安全策略	安全策略功能仅支持处理IPv4报文。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

4.4 安全策略缺省配置

安全策略的缺省配置如表4-5所示。

表 4-5 安全策略缺省配置

参数	缺省配置
缺省安全策略	匹配条件为any，动作为允许。
缺省安全策略控制同一安全区域内的流量	关闭
基于BGP、BFD、HRP、DHCP单播报文以及OSPF单播报文受安全策略的控制	开启
策略备份加速功能	开启

4.5 配置安全策略基本功能

4.5.1 配置安全策略基本功能

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 **可选:** 开启安全策略必配条件的校验功能。

```
security-policy required-object check enable
```

安全策略必配条件校验功能关闭的情况下，源IP、目的IP和服务匹配条件是否配置不影响策略规则是否生效。

开启安全策略必配条件校验开关后：

- 对于已配置的安全策略规则，不会影响其是否生效。
- 对于新配置的安全策略规则当安全策略规则中源IP、目的IP和服务这3个条件中任意一个条件未配置时，该安全策略不生效。但这3个条件均配置为any时，该策略仍然生效。

步骤3 进入安全策略视图。

```
security-policy
```

步骤4 **可选:** 配置缺省安全策略的动作。

```
default action { permit | deny }
```

缺省安全策略的匹配条件均为any，动作缺省为允许。如果流量没有匹配到管理员定义的安全策略，就会命中缺省安全策略。

步骤5 **可选:** 配置缺省安全策略控制同一安全区域内的流量。

```
default packet-filter intrazone enable
```

缺省情况下，同一安全区域内的流量如果没有匹配到管理员定义的安全策略，也不会受缺省安全策略的影响，设备允许其通过。可配置该命令使缺省安全策略控制同一安全区域内的流量。

步骤6 创建安全策略规则，并进入安全策略规则视图。

```
rule name rule-name
```

在命令行配置中，安全策略以“rule”的形式存在，所以在某些描述中的“安全策略规则”与“安全策略”含义相同。

步骤7 **可选:** 配置安全策略规则的描述信息。

```
description description
```

合理填写描述信息有助于管理员正确理解安全策略规则的功能，便于查找和维护。

步骤8 配置安全策略规则的匹配条件。

操作	命令	说明
配置源安全区域	**source-zone** { *zone-name* &<1-6> | **any** }	-
配置目的安全区域	**destination-zone** { *zone-name* &<1-6> | **any** }	-

操作	命令	说明
配置源地址	• **source-address address-set** *address-set-name* &<1-6> • **source-address domain-set** *domain-set-name* &<1-6> • **source-address-exclude address-set** *address-set-name* &<1-6> • **source-address** { *ipv4-address* { *ipv4-mask-length* | **mask** *mask-address* | **wildcard** *wildcard* } | **range** *ipv4-start-address ipv4-end-address* | **any** } • **source-address-exclude** { *ipv4-address* { *ipv4-mask-length* | **mask** *mask-address* | **wildcard** *wildcard* } | **range** *ipv4-start-address ipv4-end-address* } • **source-address none**	可以直接配置IP地址，也可以引用已经存在的地址对象、地址组和域名组。 源地址条件配置为none时，该规则不生效。 当安全策略必配条件校验功能开启的情况（**security-policy required-object check enable**命令）下，对于新创建的规则，源地址、目的地址和服务任意一个条件未配置或配置为none时，该规则不生效；对于已经创建的规则，清空源地址、目的地址和服务任意一类条件后，该条件会被设置为none，导致该规则失效。 **说明** 不要仅引用空的地址对象、地址组或域名组，否则该匹配条件无法匹配。

操作	命令	说明
配置目的地址	• **destination-address address-set** *address-set-name* &<1-6> • **destination-address domain-set** *domain-set-name* &<1-6> • **destination-address-exclude address-set** *address-set-name* &<1-6> • **destination-address** { *ipv4-address* { *ipv4-mask-length* | **mask** *mask-address* | **wildcard** *wildcard* } | **range** *ipv4-start-address ipv4-end-address* | **any** } • **destination-address-exclude** { *ipv4-address* { *ipv4-mask-length* | **mask** *mask-address* | **wildcard** *wildcard* } | **range** *ipv4-start-address ipv4-end-address* | **any** } • **destination-address none**	可以直接配置IP地址，也可以引用已经存在的地址对象、地址组和域名组。 目的地址条件配置为none时，该规则不生效。 当安全策略必配条件校验功能开启的情况（**security-policy required-object check enable**命令）下，对于新创建的规则，源地址、目的地址和服务任意一个条件未配置或配置为none时，该规则不生效；对于已经创建的规则，清空源地址、目的地址和服务任意一类条件后，该条件会被设置为none，导致该规则失效。 **说明** 不要仅引用空的地址对象、地址组或域名组，否则该匹配条件无法匹配。
配置应用	**application** { **any** | **app** *app-name* | **app-group** *app-group-name* }	策略配置应用识别后，会对设备的整机性能有一定的影响，请根据实际需求有选择性的配置。 **说明** 安全策略规则下配置了应用的情况下，需在接口视图下配置**sa enable**命令，开启对流量报文的应用识别功能。否则设备无法识别流量中的应用，导致配置了应用的安全策略规则无法匹配。

操作	命令	说明
配置服务	• **service protocol** { **udp** | **tcp** } [**source-port** { *source-port* | *start-source-port* **to** *end-source-port* } &<1-64> | **destination-port** { *destination-port* | *start-destination-port* **to** *end-destination-port* } &<1-64>] * • **service protocol sctp** • **service protocol icmp** [**icmp-type** { *icmp-name* | *icmp-type-number* { *icmp-code-number* [**to** *icmp-code-number*] } &<1-64> }] • **service protocol** *protocol-number* • **service-exclude protocol** { **udp** | **tcp** } [**source-port** { *source-port* | *start-source-port* **to** *end-source-port* } &<1-64> | **destination-port** { *destination-port* | *start-destination-port* **to** *end-destination-port* } &<1-64>] * • **service-exclude protocol sctp** • **service-exclude protocol icmp** [**icmp-type** { *icmp-name* | *icmp-type-number* { *icmp-code-number* [**to** *icmp-code-number*] } &<1-64> }] • **service-exclude protocol** *protocol-number* • **service any** • **service none**	配置协议和端口。 服务条件配置为none时，该规则不生效。 当安全策略必配条件校验功能开启的情况（**security-policy required-object check enable**命令）下，对于新创建的规则，源地址、目的地址和服务任意一个条件未配置或配置为none时，该规则不生效；对于已经创建的规则，清空源地址、目的地址和服务任意一类条件后，该条件会被设置为none，导致该规则失效。
配置生效时间	**time-range** *time-range*	-

步骤9 配置安全策略规则的动作。

```
action { permit | deny }
```

步骤10 配置安全策略规则引用内容安全的配置文件。

```
profile { av | ips | url-filter } profile-name
```

说明

- 设备对流量进行内容安全的一体化检测时，会对整机的性能有一定的影响，请根据实际需求有选择性的进行配置。
- 只有动作为**permit**的安全策略规则引用的配置文件才会生效。
- 对内容安全的配置文件进行新建、修改和删除操作时，需要在系统视图下通过**engine configuration commit**进行提交使之生效，进而保证引用其的安全策略也生效。

----结束

检查配置结果

- 在安全策略视图下执行命令**display this**，查看安全策略的配置信息。
- 在任意视图下执行命令**display security-policy rule all**，查看安全策略的配置信息和命中情况。

4.5.2 调整安全策略规则

背景信息

安全策略配置完成后，可以对已创建的规则进行重命名、移动、复制、启用/禁用等维护操作。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 进入安全策略视图。

```
security-policy
```

步骤3 调整规则。

操作	命令	说明
重命名规则。	**rule rename** *old-name new-name*	为已经存在的策略规则重新命名。
移动规则。	**rule move** *rule-name1* { **up** | **down** | **top** | **bottom** } **rule move** *rule-name1* { **after** | **before** } *rule-name2*	一般情况下，越先配置的策略规则位置越靠前，优先级越高。使用**rule move**命令可以移动策略规则，从而改变策略规则的优先级。
复制规则。	**rule copy** *rule-name new-rule-name*	当要新建的策略规则和已存在的策略规则较相似时，可通过复制已经存在的策略规则来创建新的策略规则。
启用/禁用当前规则。	**rule name** *rule-name* **enable** / **disable**	可在对应规则视图下启用/禁用该规则。

----结束

4.5.3 举例：配置基于 IP 地址和端口的安全策略

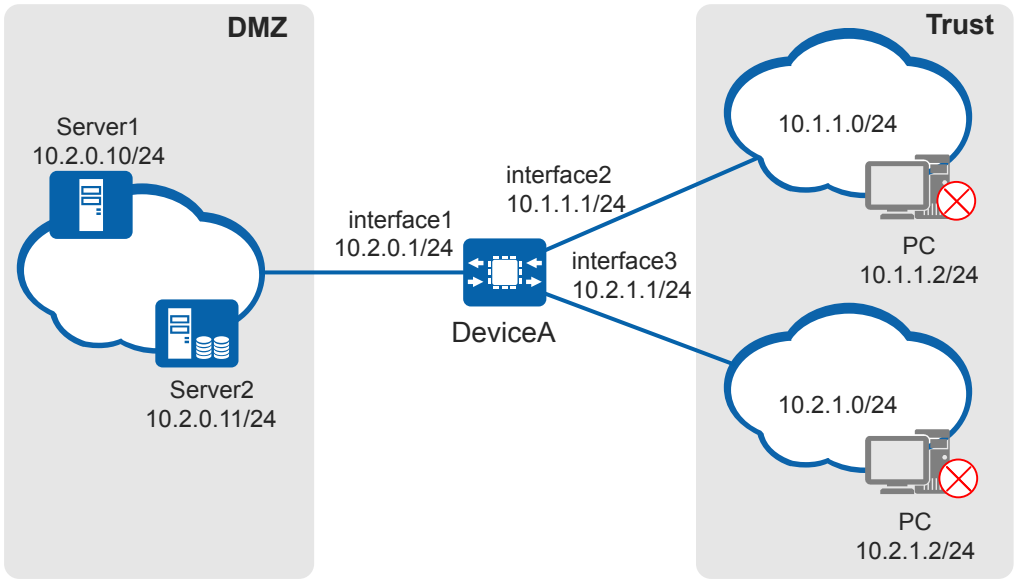
组网需求

如图4-5所示，组网中有两台业务服务器，其中Server1通过TCP 8888端口提供服务，Server2通过UDP 6666端口提供服务。需要通过设备DeviceA进行访问控制，8:00～17:00的时间段内禁止IP地址为10.1.1.2、10.2.1.2的两台PC使用这两台服务器提供的服务。其他PC在任何时间都可以访问这两台服务器。

图 4-5 配置基于 IP 地址和端口的安全策略组网图

说明

本例中interface1，interface2和interface3分别代表10GE0/0/1，10GE0/0/2和10GE0/0/3。



操作步骤

步骤1 配置接口IP地址和安全区域，完成网络基本参数配置。

配置10GE0/0/1接口IP地址，将接口加入dmz域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] undo portswitch
[DeviceA-10GE0/0/1] ip address 10.2.0.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface 10ge 0/0/1
[DeviceA-zone-dmz] quit
```

配置10GE0/0/2接口IP地址，将接口加入trust域。

```
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] undo portswitch
[DeviceA-10GE0/0/2] ip address 10.1.1.1 24
[DeviceA-10GE0/0/2] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/2
[DeviceA-zone-trust] quit
```

配置10GE0/0/3接口IP地址，将接口加入trust域。

```
[DeviceA] interface 10ge 0/0/3
[DeviceA-10GE0/0/3] undo portswitch
[DeviceA-10GE0/0/3] ip address 10.2.1.1 24
[DeviceA-10GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/3
[DeviceA-zone-trust] quit
```

步骤2 配置名称为server_deny的地址对象，将不允许访问服务器的IP地址加入地址对象。

```
[DeviceA] ip address-set server_deny type object
[DeviceA-object-address-set-server_deny] address 10.1.1.2 mask 32
```

```
[DeviceA-object-address-set-server_deny] address 10.2.1.2 mask 32
[DeviceA-object-address-set-server_deny] quit
```

步骤3 配置名称为time_deny的时间段，为特定PC不允许访问服务器的时间。

```
[DeviceA] time-range time_deny 08:00 to 17:00 daily
```

步骤4 配置安全策略规则。

配置限制特定PC使用Server1对外提供的服务的安全策略。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_deny1
[DeviceA-policy-security-rule-policy_sec_deny1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_deny1] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_deny1] source-address address-set server_deny
[DeviceA-policy-security-rule-policy_sec_deny1] destination-address 10.2.0.10 32
[DeviceA-policy-security-rule-policy_sec_deny1] service protocol tcp source-port 0 to 65535 destination-port 8888
[DeviceA-policy-security-rule-policy_sec_deny1] time-range time_deny
[DeviceA-policy-security-rule-policy_sec_deny1] action deny
[DeviceA-policy-security-rule-policy_sec_deny1] quit
```

配置限制特定PC使用Server2对外提供的服务的安全策略。

```
[DeviceA-policy-security] rule name policy_sec_deny2
[DeviceA-policy-security-rule-policy_sec_deny2] source-zone trust
[DeviceA-policy-security-rule-policy_sec_deny2] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_deny2] source-address address-set server_deny
[DeviceA-policy-security-rule-policy_sec_deny2] destination-address 10.2.0.11 32
[DeviceA-policy-security-rule-policy_sec_deny2] service protocol udp source-port 0 to 65535 destination-port 6666
[DeviceA-policy-security-rule-policy_sec_deny2] time-range time_deny
[DeviceA-policy-security-rule-policy_sec_deny2] action deny
[DeviceA-policy-security-rule-policy_sec_deny2] quit
```

安全策略是按照配置顺序匹配的，注意先配置细化的后配置宽泛的策略。

----结束

检查配置结果

在08:00到17:00时间段内，IP地址为10.1.1.2、10.2.1.2的两台PC无法使用这两台服务器对外提供的服务，在其他时间段可以使用。其他PC在任何时间都可以使用这两台服务器对外提供的服务。

配置脚本

```
#
sysname DeviceA
#
ip address-set server_deny type object
 address 0 10.1.1.2 mask 32
 address 1 10.2.1.2 mask 32
#
time-range time_deny 08:00 to 17:00 daily
#
interface 10GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface 10GE0/0/3
 ip address 10.2.1.1 255.255.255.0
#
firewall zone trust
```



```
 set priority 85
 add interface 10GE0/0/2
 add interface 10GE0/0/3
#
firewall zone dmz
 set priority 50
 add interface 10GE0/0/1
#
security-policy
 rule name policy_sec_deny1
  source-zone trust
  destination-zone dmz
  source-address address-set server_deny
  destination-address 10.2.0.10 mask 255.255.255.255
  service protocol tcp source-port 0 to 65535 destination-port 8888
  time-range time_deny
  action deny
 rule name policy_sec_deny2
  source-zone trust
  destination-zone dmz
  source-address address-set server_deny
  destination-address 10.2.0.11 mask 255.255.255.255
  service protocol udp source-port 0 to 65535 destination-port 6666
  time-range time_deny
  action deny
#
return
```

4.5.4 举例：配置基于应用的安全策略

组网需求

如图4-6所示，某企业在网络边界处部署了设备DeviceA作为安全网关。企业根据员工级别和职能不同划分了三类用户：高层管理者、市场员工、研发员工。三类用户能够访问Internet的权限不同，具体如下表4-6所示。

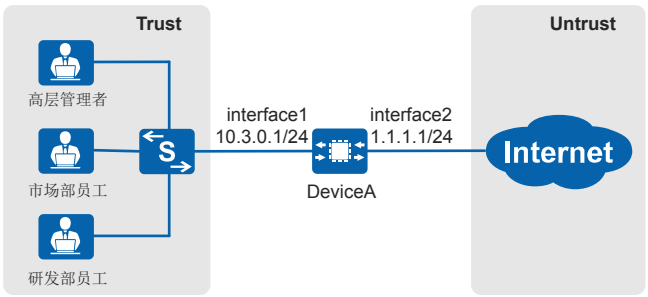
表 4-6 用户与权限关系

用户	IP地址	权限
高层管理者	10.3.0.2~10.3.0.20	自由访问Internet。
市场员工	10.3.0.21~10.3.0.120	能够访问Internet，但不能使用聊天软件（此例中以QQ为例）。
研发员工	10.3.0.121~10.3.0.220	只能使用TortoiseSVN应用。

图 4-6 配置基于应用的安全策略组网图

说明

本例中interface1和interface2分别代表10GE0/0/1和10GE0/0/2。



操作步骤

步骤1 配置接口IP地址和安全区域，完成网络基本参数配置。

配置10GE0/0/1接口IP地址，将接口加入trust域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
```

```
[DeviceA-10GE0/0/1] undo portswitch
[DeviceA-10GE0/0/1] ip address 10.3.0.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/1
[DeviceA-zone-trust] quit
```

配置10GE0/0/2接口IP地址，将接口加入untrust域。

```
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] undo portswitch
[DeviceA-10GE0/0/2] ip address 1.1.1.1 24
[DeviceA-10GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface 10ge 0/0/2
[DeviceA-zone-untrust] quit
```

步骤2 配置三类用户的地址对象。

配置高层管理者的地址对象。

```
[DeviceA] ip address-set management type object
[DeviceA-object-address-set-management] address range 10.3.0.2 10.3.0.20
[DeviceA-object-address-set-management] quit
```

配置市场员工的地址对象。

```
[DeviceA] ip address-set marketing type object
[DeviceA-object-address-set-marketing] address range 10.3.0.21 10.3.0.120
[DeviceA-object-address-set-marketing] quit
```

配置研发员工的地址对象。

```
[DeviceA] ip address-set research type object
[DeviceA-object-address-set-research] address range 10.3.0.121 10.3.0.220
[DeviceA-object-address-set-research] quit
```

步骤3 配置高层管理者的安全策略。允许其自由访问Internet。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_management
[DeviceA-policy-security-rule-policy_sec_management] source-zone trust
[DeviceA-policy-security-rule-policy_sec_management] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_management] source-address address-set management
[DeviceA-policy-security-rule-policy_sec_management] action permit
[DeviceA-policy-security-rule-policy_sec_management] quit
```

步骤4 配置市场员工的安全策略，禁止使用聊天软件（此例中以QQ为例）。

```
[DeviceA-policy-security] rule name policy_sec_marketing_1
[DeviceA-policy-security-rule-policy_sec_marketing_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_marketing_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_marketing_1] source-address address-set marketing
[DeviceA-policy-security-rule-policy_sec_marketing_1] application app QQ_IM
[DeviceA-policy-security-rule-policy_sec_marketing_1] application app QQ_VoIP
[DeviceA-policy-security-rule-policy_sec_marketing_1] action deny
[DeviceA-policy-security-rule-policy_sec_marketing_1] quit
```

步骤5 配置研发员工的安全策略。只允许其使用TortoiseSVN应用。

```
[DeviceA-policy-security] rule name policy_sec_research
[DeviceA-policy-security-rule-policy_sec_research] source-zone trust
[DeviceA-policy-security-rule-policy_sec_research] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_research] source-address address-set research
[DeviceA-policy-security-rule-policy_sec_research] application app TortoiseSVN
[DeviceA-policy-security-rule-policy_sec_research] action permit
[DeviceA-policy-security-rule-policy_sec_research] quit
```

研发员工的访问Internet的其他流量会命中缺省安全策略而被阻断。

步骤6 配置缺省安全策略的动作为禁止。

```
[DeviceA-policy-security] default action deny
```

----结束

检查配置结果

- 使用高层管理者网段的PC，尝试是否无限制访问Internet。
- 使用市场员工网段的PC，尝试是否无法使用QQ聊天，但是可以正常访问其他网络应用。
- 使用研发员工网段的PC，尝试是否除了TortoiseSVN应用以外都无法访问Internet。

配置脚本

```
#
sysname DeviceA
#
ip address-set management type object
 address 0 range 10.3.0.2 10.3.0.20
#
ip address-set marketing type object
 address 0 range 10.3.0.21 10.3.0.120
#
ip address-set research type object
 address 0 range 10.3.0.121 10.3.0.220
#
interface 10GE 0/0/1
 ip address 10.3.0.1 255.255.255.0
#
interface 10GE 0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface 10GE 0/0/1
#
firewall zone untrust
 set priority 5
 add interface 10GE 0/0/2
#
security-policy
 default action deny
 rule name policy_sec_management
  source-zone trust
  destination-zone untrust
  source-address address-set management
  action permit
 rule name policy_sec_marketing_1
  source-zone trust
  destination-zone untrust
  source-address address-set marketing
  application app QQ_IM
  application app QQ_VoIP
  action deny
 rule name policy_sec_marketing_2
  source-zone trust
  destination-zone untrust
  source-address address-set marketing
  action permit
 rule name policy_sec_research
  source-zone trust
  destination-zone untrust
  source-address address-set research
  application app TortoiseSVN
  action permit
```



```
#
return
```

4.6 配置安全策略备份加速延迟时间

背景信息

设备通过对多条策略生成索引并采用一定的加速算法完成安全策略的快速匹配。当策略改动（包括新建、修改、删除策略）时，索引需要重新建立。设备会先备份当前索引，在新索引生成之前仍然使用备份的索引进行策略匹配，保证了较高的处理性能。但是，改动后的新策略不会立即生效。在策略修改以后加速延迟时间（缺省值为10s）内如果没有再改动策略，开始生成新的策略索引，新索引生成后新的策略生效。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 调整新建、修改或删除策略后启动策略备份加速的延迟时间。

```
policy accelerate delay delay-time
```

----结束

4.7 维护安全策略

安全策略的相关维护操作如表4-7所示。

表 4-7 维护安全策略

操作	命令
开启策略匹配条件配置的校验提示功能。	**policy configuration-verification enable**
查看已开启的策略模块调试开关。	**display debugging policy**
重置安全策略规则的命中次数。	**reset security-policy counter** { **all** | **rule** *rule-name* }

5 URL 过滤配置

5.1 URL 过滤简介

定义

URL过滤也可以称为Web过滤，是指对用户的URL访问请求进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的。

目的

随着互联网应用的迅速发展，计算机网络在经济和生活的各个领域迅速普及，使得信息的获取、共享和传播更加方便，但同时也带来了威胁，如：

- 企业员工随意访问与工作无关的网站，严重影响工作效率。
- 员工随意访问非法或恶意的网站，造成公司机密信息泄露，甚至会带来病毒、木马和蠕虫等威胁攻击。
- 在内部网络拥堵时段，无法保证员工正常访问与工作相关的网站（如公司主页、搜索引擎等），影响工作效率。

URL过滤可以解决上述问题，对用户访问的URL进行控制，放行用户访问合法网站的请求，阻断访问非法网站的请求。

5.2 URL 过滤原理描述

5.2.1 URL 过滤方式

设备支持多种URL过滤方式。当用户的URL访问请求匹配到某条URL规则时，设备根据URL过滤配置文件中的配置对URL访问请求作出相应的处理。

URL 黑名单和 URL 白名单

URL黑名单和URL白名单可以看做是一种特殊的自定义URL分类，只是黑名单和白名单的控制动作是固定的无法更改。

URL黑名单和URL白名单通常用于过滤简单固定的网站，黑名单是不允许用户访问的URL列表，白名单是允许用户访问的URL列表。设备将URL访问请求报文中提取的URL与黑名单和白名单规则进行匹配，匹配白名单规则则放行访问请求，匹配黑名单规则则阻断访问请求。

预定义 URL 分类

预定义URL分类是URL预置库加载到设备上后存在于设备上的一种形式。URL预置库中维护了大量主流Web网站的URL及其分类，这些URL分类不能被修改或删除。设备收到URL访问请求后，在URL分类中查询该URL所属的分类，查询到该URL的分类后，设备根据URL过滤配置文件中配置的分类控制动作，对该请求进行相应的处理。

设备查询URL所属分类时有URL本地查询和URL远程查询两种方式。设备初次上电时，自动将URL分类预置库加载到本地缓存里。设备首先在本地缓存中查询URL所属分类，如果查询不到，则到远程查询服务器上继续查询，远程查询提供更大数量级的URL分类。

为了保证缓存中预定义URL分类的有效性，预定义URL分类缓存的内容会通过远程查询不断更新，如果缓存已满，新的URL将会取代最少访问的URL，预定义URL分类缓存的内容定期以文件的形式保存到存储介质中，当设备重启后，系统会自动加载最新保存的缓存信息，减少自学习的工作量，提高检测效率。

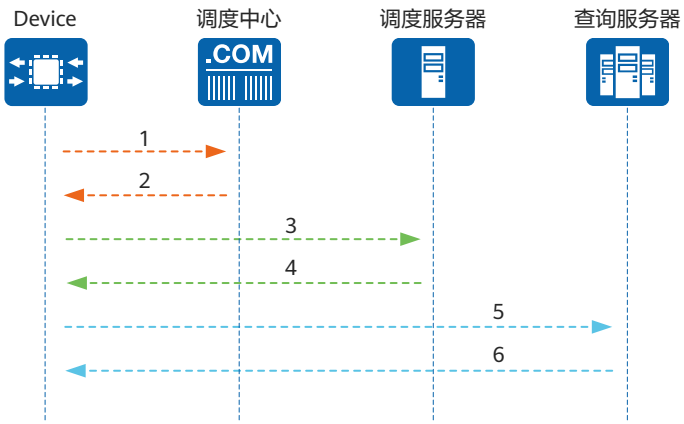
5.2.2 URL 远程查询过程

一般来说，URL远程查询由调度中心、调度服务器和查询服务器共同完成。各服务器的作用如下：

- 调度中心：调度中心的作用是对设备进行认证。如果认证通过，调度中心将根据设备所在的国家/地区信息，向设备提供该区域内的调度服务器地址和端口。
- 调度服务器：调度服务器的作用是向设备提供区域内的查询服务器地址和端口。由于调度服务器是分区域部署的，所以设备上必须配置正确的国家/地区信息，否则无法成功获取到调度服务器的地址和端口。
- 查询服务器：查询服务器的作用是处理查询请求，并将查询结果返回给设备。查询服务器也是分区域部署的，且和调度服务器存在配套关系，即调度服务器只能向设备提供同一区域内的查询服务器地址和端口。

URL远程查询的交互过程如**图5-1**所示。

图 5-1 URL 远程查询过程

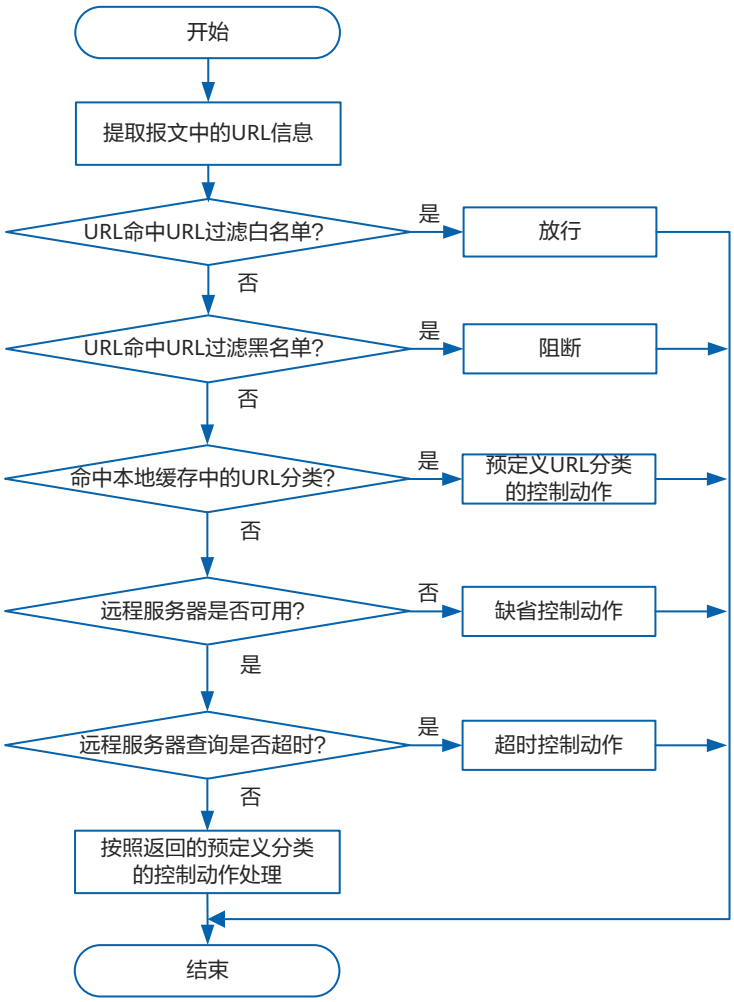


1. 设备向调度中心发起认证请求，并请求调度服务器的地址。
2. 认证通过后，调度中心根据设备的国家/地区信息，向设备提供该区域内的调度服务器地址和端口。
3. 设备向调度服务器请求查询服务器的地址和端口。
4. 调度服务器确认设备信息无误后，向设备提供查询服务器的地址和端口。一般来说，设备将收到多个查询服务器的地址和端口。
5. 设备向所有查询服务器发起测速消息，并根据响应速度从中选出最优服务器，然后向该服务器请求URL分类信息。
6. 查询服务器反馈URL分类信息，设备将根据此分类信息进行URL过滤。

5.2.3 URL 过滤处理流程

开启URL过滤功能的情况下，当用户通过URL访问某个网络资源时，设备将对此URL访问请求报文进行URL过滤。URL过滤处理流程如图5-2所示：

图 5-2 URL 过滤处理流程图



1. 用户发起URL访问请求，如果数据流匹配了动作为允许的安全策略，且安全策略中引用了URL过滤配置文件，则进行URL过滤处理流程。
2. 设备从用户的URL访问请求报文中提取URL。
3. 将URL信息与白名单进行匹配。
   - 如果匹配，则允许该请求通过。
   - 如果未匹配，则进行下一步处理。
4. 将URL信息与黑名单进行匹配。
   - 如果匹配，则阻断该请求。
   - 如果未匹配，则进行下一步处理。
5. 将URL信息与本地缓存中的预定义URL分类进行匹配。
   - 如果匹配，则按照预定义URL分类的控制动作进行处理。
   - 如果未匹配，则进行下一步处理。
6. URL远程服务器是否可用。
   - 远程服务器不可用，则按照缺省动作处理。
   - 远程服务器可用，则进行URL分类远程查询。
7. URL远程服务器查询是否超时。

- 未超时，按照返回的预定义分类对应的控制动作处理。
- 超时，按照配置的超时控制动作处理。

5.2.4 URL 过滤配置文件

URL过滤配置文件是一系列URL过滤规则的集合，所有URL过滤配置都是通过URL过滤配置文件承载的。通过配置URL过滤配置文件，并在安全策略中引用URL过滤配置文件才能实现URL过滤功能。

URL过滤配置文件中的配置组成如表5-1所示。

表 5-1 URL 过滤配置文件的组成

过滤方式	动作
URL黑名单	默认阻断，无需配置动作。
URL白名单	默认允许，无需配置动作。
URL分类	有两种配置方式： • 指定控制动作级别。指定控制动作级别后，不同的URL分类有默认动作无需手动配置。 – 低：阻断成人网站分类的访问，允许其他分类访问。 – 中：阻断所有成人网站和非法网站分类的访问，允许其他分类访问。 – 高：阻断所有成人网站、非法网站、社交网络、视频共享等网站分类的访问，允许其他分类访问。 • 为每个分类分别自定义动作。 – 允许：指允许用户访问请求的URL。 – 告警：指允许用户访问请求的URL，同时记录日志。 – 阻断：指阻断用户访问请求的URL，同时记录日志。
URL未匹配任何过滤方式	采用缺省动作。 • 允许：指允许用户访问请求的URL。 • 告警：指允许用户访问请求的URL，同时记录日志。 • 阻断：指阻断用户访问请求的URL，同时记录日志。

设备上存在一个名称为default的缺省URL过滤配置文件，缺省配置文件不能被修改和删除，过滤方式为URL分类，URL分类控制动作级别为自定义，缺省动作为允许。

5.2.5 URL 匹配规则

URL 格式

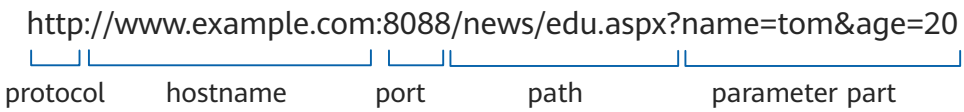
URL（Uniform Resource Locator，统一资源定位符）用来唯一标识Internet上网页和其他资源位置的地址。URL的一般格式为：“protocol://hostname:port/path?query”，各参数含义如表5-2所示。

表 5-2 URL 参数解释

字段	含义
protocol	使用的应用协议，最常用的是HTTP或HTTPS协议。
hostname	Web服务器的域名或者IP地址。
:port	可选，通信端口。各种应用协议都有默认的端口号，如HTTP协议的默认端口号为80、HTTPS协议的默认端口号为443。当服务器采用默认端口号时，URL过滤规则中不用配置端口号。当服务器采用非默认端口号时，URL过滤规则中不能省略端口号。
path	由零个或多个“/”符号隔开的字符串，一般用来表示主机上的一个目录或文件地址。
?query	可选，用于给动态网页传递参数。

例如，如图5-3所示：

图 5-3 URL 格式介绍



- http为协议。
- www.example.com为主机名。
- 8088为通信端口。
- news/edu.aspx为路径。
- name=tom&age=20为参数部分。

URL 规则和匹配方式

管理员可以在黑名单和白名单中配置URL规则和HOST规则，其中URL规则的匹配范围是全部URL，HOST规则的匹配范围只是hostname（域名或者IP地址）部分。两者的使用场景如下：

- 如果允许或阻断的URL为域名形式，如www.example.com，大多数情况下可以配置URL规则或HOST规则，两者的过滤效果相同。
- 如果允许或阻断的URL带有目录或参数内容，如www.example.com/news，则只能配置成URL规则，不能配置成HOST规则。

配置URL规则和HOST规则时需满足一定条件，否则配置不会生效，两者具体条件如下：

- URL规则以字符串形式进行添加，长度范围为4~255，会区分大小写。

  - 不能包含字符“？”。
  - 不能以字符“/”或“\”开头。
  - 使用“*”时，“*”前或后至少要有3个不是“*”的字符，且最后一个字符不是“.”，例如不支持“ab.*”，或者“*ab.”。
  - 使用“#”时，“#”前至少要有3个不是“#”的字符，且最后一个字符不是“.”，例如不支持“ab.#”。
  - 使用空格时，需要在空格外使用双引号""，且保证双引号成对配对，例如"abc def"。
  - 如果输入的字符串中包含前缀"http://" 或 "https://"，设备在存储该规则时会进行预处理去除该前缀。
  - 当URL规则中包括双引号时，需要使用%22进行字符串的转义，例如“abc %22def”。
- HOST规则以字符串形式进行添加，长度范围为4~255，不区分大小写。
  - 不能包含字符“/”、“\”、“#”、“?”和空格等特殊字符。
  - 使用“*”时，“*”前后至少要有3个不是“*”的字符，且最后一个字符不是“.”，例如不支持“ab.*”，或者“*ab.”。
  - 如果输入的字符串中包含前缀"http://" 或 "https://"，设备在存储该规则时会进行预处理去除该前缀。

URL匹配方式包括前缀匹配、后缀匹配、关键字匹配、精确匹配。URL规则和HOST规则支持相同的匹配方式。URL匹配方式的比较如表5-3所示：

表 5-3 URL 匹配方式

匹配方式	定义	使用示例
前缀匹配	匹配所有以指定字符串开头的URL，例如www.example*。	如果想控制访问所有以www.example开头的网站，配置URL过滤规则为www.example*。
后缀匹配	匹配所有以指定字符串结尾的URL，例如*aspx。	如果想控制访问所有图片类网页，配置URL过滤规则为*.jpg，*.jpeg，*.gif，*.png和*.bmp。
关键字匹配	匹配所有包含指定字符串的URL，例如*sport*。	如果想控制访问包含sport的所有网站，配置URL过滤规则为*sport*。
精确匹配	首先判断URL和指定字符串是否匹配，如果未匹配，则去除URL的最后一个目录，再和指定字符串进行匹配；如果还未匹配，则继续去除URL的最后一个目录，再和指定字符串进行匹配。以此类推，直到用域名去匹配指定的字符串为止，例如www.example.com。	如果想控制访问某个固定网站www.example.com/news，配置URL过滤的URL规则为www.example.com/news。

5.3 URL 过滤配置注意事项

License 依赖

URL远程查询功能受URL远程查询License控制，License控制项未激活时，URL远程查询功能不可用。License控制项激活后，可以进行URL远程查询。License到期后URL远程查询功能不可用，其余功能无需License许可即可使用。

硬件依赖

表 5-4 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 5-5 本特性的使用限制

特性限制	系列	涉及产品
设备使用URL过滤功能对流量进行内容安全检测时，会对整机的性能有一定的影响，请根据实际需求有选择性的进行配置。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
在报文来回路径不一致的组网环境中，URL过滤功能不可用。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

特性限制	系列	涉及产品
URL过滤功能目前不能过滤在线代理后的URL请求。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
设备上协议栈代理功能不可用，当用户访问的URL被阻断时，设备无法推送阻断提示页面。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
如果浏览器缓存过网页主页面，短时间内浏览器不会再向网页服务器发起访问请求，而是使用本地的缓存信息，这样可能导致URL过滤推送页面无法正常显示。因此建议在使用URL过滤推送页面功能之前清理浏览器的缓存。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

特性限制	系列	涉及产品
URL过滤功能只能过滤HTTP或HTTPS协议的URL请求。当过滤HTTPS协议的URL请求时，还需要配置加密流量过滤功能。加密流量过滤功能是通过从客户端Client Hello报文的SNI（Server Name Indication）字段、服务器Certificate报文的CN（Common Name）字段中获取用户访问的网站域名实现URL过滤的，由于是基于域名级别的过滤，因此不够精确，如果用户使用加密流量过滤功能实现HTTPS URL过滤，请先阅读以下使用限制： - 在浏览器存在代理的情况下，当用户访问某些网站时，设备从客户端Client Hello报文的SNI字段、服务器Certificate报文的CN字段中提取的网站域名可能与实际网站的域名不匹配，这会导致URL过滤功能不生效。例如当用户通过手机的UC浏览器访问优酷网站时，URL过滤功能不生效，通过关闭手机UC浏览器的云加速功能可以解决。 - 当某些浏览器传输数据采用私有协议时，可能导致URL过滤功能不生效。例如谷歌浏览器默认使用私有协议QUIC（Quick UDP Internet Connection）进行数据传输，该协议使用专门的加密方式，设备不能解密，导致URL过滤无法过滤通过谷歌浏览器访问的HTTPS网站，通过配置安全策略将QUIC应用阻断可以解决。 - SNI与CN有可能是不一致的，如果白名单中只配置了其中一个，那么白名单过滤功能可能不生效，需要将两者都加入到白名单中。 - 由于加密流量过滤功能是通过SSL握手报文实现URL过滤的，客户端尚未发起HTTP请求，因此无法发送URL推送信息。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
URL过滤规则针对的是网页自身的URL地址，不能对网页内嵌URL进行过滤。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
当一条会话中含有多个URL时，设备会对每个URL分别进行过滤处理，只要其中任一URL被阻断，则整个会话将会被阻断。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

特性限制	系列	涉及产品
URL规则中如果包含字符“#”，则“#”及“#”后面的字符串在匹配时不会生效；用户访问的URL地址中如果包含字符“#”，则“#”及“#”后面的字符串不会送入URL模块进行匹配处理。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

5.4 URL 过滤缺省配置

URL过滤的主要缺省配置如表5-6所示。

表 5-6 URL 过滤缺省配置

参数	缺省配置
URL过滤功能	未配置
URL过滤配置文件	文件名称为default，缺省动作为允许，未配置黑名单和白名单，URL分类控制动作级别为自定义
加密流量过滤功能	关闭
白名单模式的URL过滤功能	关闭
预定义URL分类的控制动作级别	控制动作级别为低
URL远程查询超时时间	3s
URL远程查询超时动作	允许

5.5 配置基于黑名单和白名单的 URL 过滤

5.5.1 配置基于黑名单和白名单的 URL 过滤

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 （可选）配置设备的业务性能模式。

```
forward performance mode { routing | security }
```

当设备业务性能模式处于路由模式时，设备的安全业务处理性能较低，建议将设备业务性能模式切换到安全模式。用户可通过命令**display forward performance mode**查看设备当前的业务性能模式。

设备业务性能模式缺省情况如下：

- 对于AR5700系列和AR6700系列：缺省情况下，设备业务性能模式处于安全模式。
- 对于AR8000系列：缺省情况下，设备业务性能模式处于路由模式。

步骤3 配置推送页面使用的语言。

push-info module url-filter template { **english** | **hindi** | **spanish** | **french** | **arabic** | **bengali** | **russian** | **portuguese** | **indonesian** | **german** }

设备的URL过滤推送页面支持10种语言模板，缺省情况下推送页面使用语言为英语。

步骤4 创建URL过滤配置文件。

profile type url-filter name *name*

步骤5 配置URL过滤配置文件的缺省动作。

default action { **allow** | **block** | **alert** }

当用户访问的URL未匹配任何URL分类、黑名单和白名单时，设备将按照缺省动作处理该请求。

步骤6 向URL过滤配置文件中添加白名单规则。

add whitelist { **url** *url-text* | **host** *host-text* }

白名单是允许用户访问的URL列表，设备将URL请求报文中提取的URL和白名单中的URL或HOST规则进行匹配，如果匹配则允许该URL访问请求。白名单的优先级高于黑名单。

步骤7 **可选:** 开启白名单模式的URL过滤。

whitelist-only enable

如果只想通过白名单进行URL过滤，不想进行其他复杂配置（如黑名单、URL分类等）时，可以开启该功能。开启该功能后，如果URL请求命中白名单，则放行；未命中白名单，则阻断。

步骤8 向URL过滤配置文件中添加黑名单规则。

add blacklist { **url** *url-text* | **host** *host-text* }

黑名单是不允许用户访问的URL列表，设备将URL请求报文中提取的URL和黑名单中的URL或HOST规则进行匹配，如果匹配则阻断该URL访问请求。

步骤9 返回系统视图。

quit

步骤10 提交配置。

engine configuration commit

创建或修改URL过滤配置文件后，配置内容不会立即生效，需要执行提交操作来激活。

步骤11 进入安全策略视图。

security-policy

步骤12 创建安全策略规则，并进入安全策略规则视图。

rule name *rule-name*

步骤13 配置安全策略规则的动作为**permit**。

```
action permit
```

步骤14 在安全策略中引用URL过滤配置文件。

```
profile url-filter profile-name
```

此处仅体现了在安全策略中引用URL过滤配置文件的配置步骤，安全策略的匹配条件配置未给出，具体请参见《配置指南-安全配置》中的“安全策略配置”。

步骤15 返回系统视图。

```
quit
quit
```

----结束

检查配置结果

执行**display profile type url-filter** [**name** *name* [**blacklist** [**url** *url-text* | **host** *host-text*] | **whitelist** [**url** *url-text* | **host** *host-text*]]]命令查看URL过滤配置文件的配置信息。

5.5.2 举例：通过黑名单和白名单控制用户访问的网站

组网需求

如图5-4所示，DeviceA作为企业网关部署在网络边界，对用户访问外部网络的URL访问请求进行URL过滤。

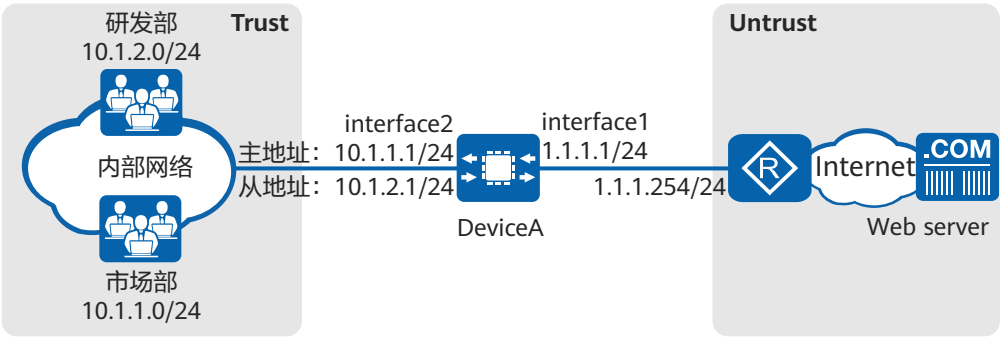
公司有研发部门员工和市场部门员工两类，具体需求如下：

- 对研发部门员工实行白名单管理，只允许访问与工作相关的URL（以www.example.com/working开头的URL）和hostname为www.example.org的URL，除此之外，其他URL均不允许访问。
- 对市场部门员工实行黑名单管理，除了以www.example.net开头的URL不允许访问之外，其他URL均可以正常访问。

图 5-4 通过黑名单和白名单控制用户访问的网站

说明

本例中interface1、interface2分别代表10GE0/0/1、10GE0/0/2。



配置思路

1. 配置接口IP地址和安全区域，完成网络基本参数配置。
2. 针对研发部门员工，新建URL过滤配置文件profile_url_research，增加白名单URL规则（www.example.com/working/*）和HOST规则（www.example.org），并设置所有预定义分类的动作为阻断，同时设置缺省动作为阻断（URL未匹配白名单和预定义分类时，设备采取缺省动作，以此实现对白名单之外的URL进行访问控制）。
3. 针对市场部门员工，新建URL过滤配置文件profile_url_marketing，增加黑名单URL规则（www.example.net*），并设置所有预定义分类的动作为允许，同时设置缺省动作为允许（URL未匹配黑名单和预定义分类时，设备采取缺省动作，以此实现对黑名单之外的URL进行访问控制）。
4. 配置两个安全策略，分别引用URL过滤配置文件，实现对来自不同部门的员工的URL访问控制。

操作步骤

步骤1 配置接口IP地址和安全区域，完成网络基本参数配置。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] ip address 1.1.1.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] ip address 10.1.1.1 255.255.255.0
[DeviceA-10GE0/0/2] ip address 10.1.2.1 255.255.255.0 sub
[DeviceA-10GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface 10ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/2
[DeviceA-zone-trust] quit
```

步骤2 配置URL过滤配置文件。

1. 为研发部门配置URL过滤配置文件。

```
[DeviceA] profile type url-filter name profile_url_research
[DeviceA-profile-url-filter-profile_url_research] default action block
[DeviceA-profile-url-filter-profile_url_research] category pre-defined action block
[DeviceA-profile-url-filter-profile_url_research] add whitelist url www.example.com/working/*
[DeviceA-profile-url-filter-profile_url_research] add whitelist host www.example.org
[DeviceA-profile-url-filter-profile_url_research] quit
```

2. 为市场部门配置URL过滤配置文件。

```
[DeviceA] profile type url-filter name profile_url_marketing
[DeviceA-profile-url-filter-profile_url_marketing] default action allow
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined action allow
[DeviceA-profile-url-filter-profile_url_marketing] add blacklist url www.example.net*
[DeviceA-profile-url-filter-profile_url_marketing] quit
```

步骤3 在安全策略中应用URL过滤配置文件。

1. 为研发部门配置安全策略。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_research
[DeviceA-policy-security-rule-policy_sec_research] description Security policy of web access protect
for research.
[DeviceA-policy-security-rule-policy_sec_research] source-zone trust
[DeviceA-policy-security-rule-policy_sec_research] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_research] source-address 10.1.2.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_research] action permit
```



```
[DeviceA-policy-security-rule-policy_sec_research] profile url-filter profile_url_research
[DeviceA-policy-security-rule-policy_sec_research] quit
```

2. 为市场部门配置安全策略。

```
[DeviceA-policy-security] rule name policy_sec_marketing
[DeviceA-policy-security-rule-policy_sec_marketing] description Security policy of web access protect for marketing.
[DeviceA-policy-security-rule-policy_sec_marketing] source-zone trust
[DeviceA-policy-security-rule-policy_sec_marketing] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_marketing] source-address 10.1.1.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_marketing] action permit
[DeviceA-policy-security-rule-policy_sec_marketing] profile url-filter profile_url_marketing
[DeviceA-policy-security-rule-policy_sec_marketing] quit
[DeviceA-policy-security] quit
```

步骤4 提交内容安全配置文件。

```
[DeviceA] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: URL submitted configurations successfully.
Info: Finish committing engine compiling.
```

----结束

检查配置结果

- 研发部门任何员工只能正常访问与工作相关的URL（以www.example.com/working开头的URL）和hostname为www.example.org的URL，其余均被阻断。可访问URL举例：
  - www.example.com/working/index.htm
  - www.example.com/working/todo
  - www.example.org
  - www.example.org/network

  研发部门员工访问其他网站时，管理员可以看到Type（过滤类型）为“Timeout or default action”或“Pre-defined”，Action（动作）为“Block”的URL日志信息（URL/4/FILTER）。
- 市场部门任何员工访问以www.example.net开头的URL均被阻断，其余网站均可以正常访问。不可访问URL举例：
  - www.example.net
  - www.example.net/index.html
  - www.example.net/game

  市场部门员工访问以www.example.net开头的URL时， 管理员可以看到Type（过滤类型）为“Blacklist”，Action（动作）为“Block”的URL日志信息（URL/4/FILTER）。

配置脚本

```
#
 sysname DeviceA
#
interface 10GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.1.1.1 255.255.255.0
 ip address 10.1.2.1 255.255.255.0 sub
#
firewall zone trust
 set priority 85
```

```
 add interface 10GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface 10GE0/0/1
#
profile type url-filter name profile_url_research
 add whitelist url www.example.com/working/*
 add whitelist host www.example.org
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
 category pre-defined subcategory-id 103 action block
 category pre-defined subcategory-id 166 action block
 category pre-defined subcategory-id 167 action block
 category pre-defined subcategory-id 168 action block
 category pre-defined subcategory-id 104 action block
 category pre-defined subcategory-id 169 action block
 category pre-defined subcategory-id 170 action block
 category pre-defined subcategory-id 105 action block
 category pre-defined subcategory-id 171 action block
 category pre-defined subcategory-id 172 action block
 category pre-defined subcategory-id 173 action block
 category pre-defined subcategory-id 174 action block
 category pre-defined subcategory-id 106 action block
 category pre-defined subcategory-id 108 action block
 category pre-defined subcategory-id 251 action block
 category pre-defined subcategory-id 177 action block
 category pre-defined subcategory-id 109 action block
 category pre-defined subcategory-id 110 action block
 category pre-defined subcategory-id 248 action block
 category pre-defined subcategory-id 178 action block
 category pre-defined subcategory-id 111 action block
 category pre-defined subcategory-id 112 action block
 category pre-defined subcategory-id 179 action block
 category pre-defined subcategory-id 114 action block
 category pre-defined subcategory-id 115 action block
 category pre-defined subcategory-id 180 action block
 category pre-defined subcategory-id 181 action block
 category pre-defined subcategory-id 117 action block
 category pre-defined subcategory-id 118 action block
 category pre-defined subcategory-id 119 action block
 category pre-defined subcategory-id 122 action block
 category pre-defined subcategory-id 182 action block
 category pre-defined subcategory-id 183 action block
 category pre-defined subcategory-id 184 action block
 category pre-defined subcategory-id 123 action block
 category pre-defined subcategory-id 186 action block
 category pre-defined subcategory-id 187 action block
 category pre-defined subcategory-id 188 action block
 category pre-defined subcategory-id 189 action block
 category pre-defined subcategory-id 124 action block
 category pre-defined subcategory-id 125 action block
 category pre-defined subcategory-id 126 action block
 category pre-defined subcategory-id 190 action block
 category pre-defined subcategory-id 127 action block
 category pre-defined subcategory-id 128 action block
 category pre-defined subcategory-id 191 action block
 category pre-defined subcategory-id 192 action block
 category pre-defined subcategory-id 193 action block
 category pre-defined subcategory-id 194 action block
 category pre-defined subcategory-id 195 action block
 category pre-defined subcategory-id 196 action block
 category pre-defined subcategory-id 129 action block
 category pre-defined subcategory-id 130 action block
 category pre-defined subcategory-id 131 action block
```

```
category pre-defined subcategory-id 197 action block
category pre-defined subcategory-id 198 action block
category pre-defined subcategory-id 199 action block
category pre-defined subcategory-id 132 action block
category pre-defined subcategory-id 227 action block
category pre-defined subcategory-id 228 action block
category pre-defined subcategory-id 200 action block
category pre-defined subcategory-id 133 action block
category pre-defined subcategory-id 201 action block
category pre-defined subcategory-id 202 action block
category pre-defined subcategory-id 204 action block
category pre-defined subcategory-id 205 action block
category pre-defined subcategory-id 134 action block
category pre-defined subcategory-id 135 action block
category pre-defined subcategory-id 136 action block
category pre-defined subcategory-id 206 action block
category pre-defined subcategory-id 207 action block
category pre-defined subcategory-id 208 action block
category pre-defined subcategory-id 137 action block
category pre-defined subcategory-id 209 action block
category pre-defined subcategory-id 210 action block
category pre-defined subcategory-id 138 action block
category pre-defined subcategory-id 139 action block
category pre-defined subcategory-id 229 action block
category pre-defined subcategory-id 140 action block
category pre-defined subcategory-id 141 action block
category pre-defined subcategory-id 142 action block
category pre-defined subcategory-id 211 action block
category pre-defined subcategory-id 212 action block
category pre-defined subcategory-id 143 action block
category pre-defined subcategory-id 144 action block
category pre-defined subcategory-id 145 action block
category pre-defined subcategory-id 240 action block
category pre-defined subcategory-id 146 action block
category pre-defined subcategory-id 213 action block
category pre-defined subcategory-id 147 action block
category pre-defined subcategory-id 253 action block
category pre-defined subcategory-id 149 action block
category pre-defined subcategory-id 150 action block
category pre-defined subcategory-id 214 action block
category pre-defined subcategory-id 215 action block
category pre-defined subcategory-id 216 action block
category pre-defined subcategory-id 217 action block
category pre-defined subcategory-id 218 action block
category pre-defined subcategory-id 219 action block
category pre-defined subcategory-id 220 action block
category pre-defined subcategory-id 221 action block
category pre-defined subcategory-id 222 action block
category pre-defined subcategory-id 223 action block
category pre-defined subcategory-id 252 action block
category pre-defined subcategory-id 151 action block
category pre-defined subcategory-id 230 action block
category pre-defined subcategory-id 152 action block
category pre-defined subcategory-id 238 action block
category pre-defined subcategory-id 153 action block
category pre-defined subcategory-id 154 action block
category pre-defined subcategory-id 155 action block
category pre-defined subcategory-id 224 action block
category pre-defined subcategory-id 225 action block
category pre-defined subcategory-id 156 action block
category pre-defined subcategory-id 157 action block
category pre-defined subcategory-id 158 action block
category pre-defined subcategory-id 231 action block
category pre-defined subcategory-id 232 action block
category pre-defined subcategory-id 159 action block
category pre-defined subcategory-id 254 action block
category pre-defined subcategory-id 160 action block
category pre-defined subcategory-id 161 action block
category pre-defined subcategory-id 176 action block
```

```
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
 default action block
profile type url-filter name profile_url_marketing
 add blacklist url www.example.net*
#
security-policy
 rule name policy_sec_research
  description Security policy of web access protect for research.
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  profile url-filter profile_url_research
  action permit
 rule name policy_sec_marketing
  description Security policy of web access protect for marketing.
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  profile url-filter profile_url_marketing
  action permit
#
return
```

5.6 配置基于 URL 分类的 URL 过滤

5.6.1 配置基于 URL 分类的 URL 过滤

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 （可选）配置设备的业务性能模式。

```
forward performance mode { routing | security }
```

当设备业务性能模式处于路由模式时，设备的安全业务处理性能较低，建议将设备业务性能模式切换到安全模式。用户可通过命令**display forward performance mode**查看设备当前的业务性能模式。

设备业务性能模式缺省情况如下：

- 对于AR5700系列和AR6700系列：缺省情况下，设备业务性能模式处于安全模式。
- 对于AR8000系列：缺省情况下，设备业务性能模式处于路由模式。

步骤3 配置推送页面使用的语言。

```
push-info module url-filter template { english | hindi | spanish | french | arabic | bengali | russian | portuguese | indonesian | german }
```

设备的URL过滤推送页面支持10种语言模板，缺省情况下推送页面使用语言为英语。

步骤4 创建URL过滤配置文件。

```
profile type url-filter name name
```

步骤5 配置URL过滤配置文件的缺省动作。

```
default action { allow | block | alert }
```

当用户访问的URL未匹配任何URL分类、黑名单和白名单时，设备将按照缺省动作处理该请求。

步骤6 配置预定义URL分类的控制动作。设备提供两种配置URL分类控制动作的方法，如果某个URL同时属于以下两种配置的控制范围，以第二种配置优先：

- 配置预定义URL分类的控制动作级别，此方法操作简单，适用于对URL分类控制无特殊需求的场景。

  ```
  category pre-defined control-level { high | low | medium }
  ```

  不同级别下，设备对不同类别的网站控制动作不同。具体可以执行**display url-filter category pre-defined control-level** [**high** | **low** | **medium**]命令查看指定级别下的分类控制信息。

- 为每个分类分别指定控制动作，此方法适用于清楚知道需要限制哪些URL分类的场景。

  ```
  category pre-defined [ category-id category-id-value | subcategory-id subcategory-id-value ]
  action { allow | block | alert }
  ```

  如果不清楚分类ID，需要先执行**display url-filter category pre-defined**命令查看所有预定义URL分类的大类ID（CID）和小类ID（SID）。

说明

正常情况下，URL分类预置库是出厂预置的，无需用户手动加载。如果执行命令时提示未加载URL预置库，请通过**import url-sdb file** *filename*命令加载URL分类预置库，如：import url-sdb file flash:/url.sdb。

如果本地没有URL分类预置库，请登录安全中心平台（isecurity.huawei.com）进行下载。在网站首页选择“特征库升级 > 特征库升级”，然后选择对应的产品型号和版本号等信息，在“URL预置库”页签中下载URL分类预置库，最后将URL分类预置库上传到设备。

步骤7 返回系统视图。

```
quit
```

步骤8 提交配置。

```
engine configuration commit
```

创建或修改URL过滤配置文件后，配置内容不会立即生效，需要执行提交操作来激活。

步骤9 进入安全策略视图。

```
security-policy
```

步骤10 创建安全策略规则，并进入安全策略规则视图。

```
rule name rule-name
```

步骤11 配置安全策略规则的动作为**permit**。

```
action permit
```

步骤12 在安全策略中引用URL过滤配置文件。

```
profile url-filter profile-name
```

此处仅体现了在安全策略中引用URL过滤配置文件的配置步骤，安全策略的匹配条件配置未给出，具体请参见《配置指南-安全配置》中的“安全策略配置”。

步骤13 返回系统视图。

```
quit
quit
```

----结束

检查配置结果

- 执行**display profile type url-filter** [**name** *name* [**pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id*]]]命令查看URL过滤配置文件的配置信息。
- 执行**display url-filter category pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id*]命令查看URL分类列表信息。
- 执行**display url-filter category pre-defined control-level** [**high** | **low** | **medium**]命令查看指定级别的所有预定义分类的信息。

5.6.2 （可选）查询 URL 分类

背景信息

在配置URL分类的控制动作之前，如果不清楚某个URL所属的分类，可以先通过华为安全中心平台查询。

如果用户访问的URL没有匹配URL预置库中的URL，设备还可以通过配置远程查询扩充本地的URL分类，远程查询提供更大数量级的URL分类。

操作步骤

- 查询URL所属分类。

  登录华为安全中心平台（**isecurity.huawei.com**），选择“知识库查询 > URL分类查询”。然后在文本框中输入URL，单击“查询”即可得到该URL的分类信息。

- 配置URL远程查询服务。
  a. 进入系统视图。
  ```
  system-view
  ```
  b. 配置国家信息。
  ```
  country country-code
  ```
  使用URL远程查询服务，必须使用该命令配置国家信息，没有配置国家信息或配置信息与设备实际所在地不一致，都会导致URL远程查询服务不可用。除此之外，还需要确保完成如下工作：
  - URL远程查询License已经激活并且在有效服务期内。
  - 设备与isecurity.huawei.com路由可达。
  - 已配置DNS服务器地址，并可以正确解析isecurity.huawei.com。
  - 已配置安全策略，允许访问isecurity.huawei.com的流量通过设备。

c. 配置URL远程查询的超时时间和超时动作。

url-filter query timeout { **time** *time-value* | **action** { **allow** | **block** | **alert** } } *

当URL远程查询时长超过*time-value*指定的超时时间时，设备按照该命令指定的超时动作处理报文。

----结束

检查配置结果

执行**display cloud-query configuration**命令查看URL远程查询的配置信息。

5.6.3 举例：通过 URL 分类控制用户访问的网站

组网需求

如图5-5所示，DeviceA作为企业网关部署在网络边界，对用户访问外部网络的URL访问请求进行URL过滤。

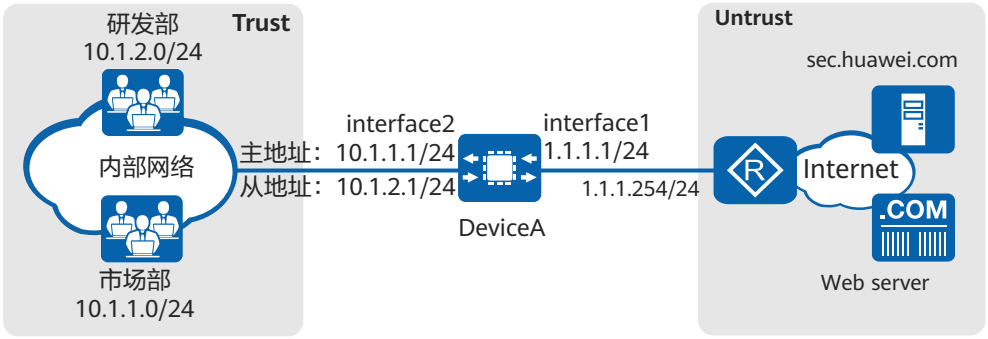
公司有研发部门员工和市场部门员工两类，具体需求如下：

- 研发部门员工只可以在每天的09：00～17：00访问教育/科学类、搜索/门户类网站。其他网站均不能访问。
- 市场部门员工只可以在每天的09：00～17：00访问教育/科学类、搜索/门户类、社会焦点类网站。其他网站均不能访问。

图 5-5 通过 URL 分类控制用户访问的网站

说明

本例中interface1、interface2分别代表10GE0/0/1、10GE0/0/2。



配置思路

1. 配置接口IP地址和安全区域，完成网络基本参数配置。
2. 配置远程查询服务器，用来获取URL与预定义分类的对应关系。本例中教育/科学类、搜索/门户类、社会焦点类网站可以通过预定义分类来进行URL过滤控制。为了可以正常使用远程查询功能，需要进行如下配置：
   a. 激活URL远程查询License并且确保该License在有效服务期内。
   b. 配置DNS服务器，确保DeviceA可以正确解析isecurity.huawei.com。
   c. 配置远程查询服务器的相关参数，包括查询方式、国家名称和超时时间。

d. 配置安全策略允许DeviceA访问调度中心isecurity.huawei.com。

3. 针对研发部门员工和市场部门员工，新建两个URL过滤配置文件profile_url_research和profile_url_marketing，设置URL预定义分类的控制动作。
4. 配置时间段。
5. 配置两个安全策略，引用时间段和URL过滤配置文件等信息，实现对来自不同部门的员工的URL访问控制。

操作步骤

步骤1 配置接口IP地址和安全区域，完成网络基本参数配置。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] ip address 1.1.1.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] ip address 10.1.1.1 255.255.255.0
[DeviceA-10GE0/0/2] ip address 10.1.2.1 255.255.255.0 sub
[DeviceA-10GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface 10ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/2
[DeviceA-zone-trust] quit
```

步骤2 配置远程查询服务器，用来获取URL与预定义分类的对应关系。

1. 激活License并且确保该License在有效服务期内。
2. 配置DNS服务器。

   ```
   [DeviceA] dns resolve
   [DeviceA] dns server 10.2.0.70
   ```

3. 配置远程查询服务器的相关参数，包括国家名称、超时时间和超时动作。

   ```
   [DeviceA] country CN
   [DeviceA] url-filter query timeout time 3 action allow
   ```

4. 配置安全策略，允许DeviceA访问调度中心。

   ```
   [DeviceA] security-policy
   [DeviceA-policy-security] rule name policy_sec_huawei_com
   [DeviceA-policy-security-rule-policy_sec_huawei_com] source-zone local
   [DeviceA-policy-security-rule-policy_sec_huawei_com] destination-zone untrust
   [DeviceA-policy-security-rule-policy_sec_huawei_com] action permit
   [DeviceA-policy-security-rule-policy_sec_huawei_com] quit
   [DeviceA-policy-security] quit
   ```

步骤3 配置URL过滤配置文件。

说明

通过**display url-filter category pre-defined**命令，可以查询到如下预定义分类和ID的对应关系。

- 17：教育/科学类（Education/Science）
- 15：搜索/门户类（Search Engines/Portals）
- 5：社会焦点类（Social Focus）

1. 为研发部门配置URL过滤配置文件。

   ```
   [DeviceA] profile type url-filter name profile_url_research
   [DeviceA-profile-url-filter-profile_url_research] category pre-defined action block
   [DeviceA-profile-url-filter-profile_url_research] category pre-defined category-id 15 action allow
   [DeviceA-profile-url-filter-profile_url_research] category pre-defined category-id 17 action allow
   [DeviceA-profile-url-filter-profile_url_research] quit
   ```

2. 为市场部门配置URL过滤配置文件。

```
[DeviceA] profile type url-filter name profile_url_marketing
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined action block
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined category-id 5 action allow
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined category-id 15 action allow
[DeviceA-profile-url-filter-profile_url_marketing] category pre-defined category-id 17 action allow
[DeviceA-profile-url-filter-profile_url_marketing] quit
```

步骤4 配置时间段。

```
[DeviceA] time-range time_range 09:00 to 17:00 daily
```

步骤5 在安全策略中应用URL过滤配置文件。

1. 为研发部门配置安全策略。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_research
[DeviceA-policy-security-rule-policy_sec_research] description Security policy of web access protect for research.
[DeviceA-policy-security-rule-policy_sec_research] source-zone trust
[DeviceA-policy-security-rule-policy_sec_research] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_research] source-address 10.1.2.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_research] time-range time_range
[DeviceA-policy-security-rule-policy_sec_research] action permit
[DeviceA-policy-security-rule-policy_sec_research] profile url-filter profile_url_research
[DeviceA-policy-security-rule-policy_sec_research] quit
```

2. 为市场部门配置安全策略。

```
[DeviceA-policy-security] rule name policy_sec_marketing
[DeviceA-policy-security-rule-policy_sec_marketing] description Security policy of web access protect for marketing.
[DeviceA-policy-security-rule-policy_sec_marketing] source-zone trust
[DeviceA-policy-security-rule-policy_sec_marketing] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_marketing] source-address 10.1.1.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_marketing] time-range time_range
[DeviceA-policy-security-rule-policy_sec_marketing] action permit
[DeviceA-policy-security-rule-policy_sec_marketing] profile url-filter profile_url_marketing
[DeviceA-policy-security-rule-policy_sec_marketing] quit
[DeviceA-policy-security] quit
```

步骤6 提交内容安全配置文件。

```
[DeviceA] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: URL submitted configurations successfully.
Info: Finish committing engine compiling.
```

----结束

检查配置结果

- 研发部门任何员工在09：00～17：00之间，可以访问教育/科学类、搜索/门户类网站，但是访问社会焦点类等其他网站时，都被阻断不能访问。

  研发部门员工访问社会焦点类等其他网站时，管理员可以看到Type（过滤类型）为“Pre-defined”，Action（动作）为“Block”的URL日志信息（URL/4/FILTER）。

- 市场部门任何员工在09：00～17：00之间，可以访问教育/科学类、搜索/门户类、社会焦点类网站，但是访问其他网站时，都被阻断不能访问。

  市场部门员工访问其他网站时，管理员可以看到Type（过滤类型）为“Pre-defined”，Action（动作）为“Block”的URL日志信息（URL/4/FILTER）。

配置脚本

```
#
sysname DeviceA
```



```
#
 dns resolve
 dns server 10.2.0.70
#
 country CN
#
 time-range time_range 09:00 to 17:00 daily
#
interface 10GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.1.1.1 255.255.255.0
 ip address 10.1.2.1 255.255.255.0 sub
#
firewall zone trust
 set priority 85
 add interface 10GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface 10GE0/0/1
#
profile type url-filter name profile_url_research
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
 category pre-defined subcategory-id 103 action block
 category pre-defined subcategory-id 166 action block
 category pre-defined subcategory-id 167 action block
 category pre-defined subcategory-id 168 action block
 category pre-defined subcategory-id 104 action block
 category pre-defined subcategory-id 169 action block
 category pre-defined subcategory-id 170 action block
 category pre-defined subcategory-id 105 action block
 category pre-defined subcategory-id 171 action block
 category pre-defined subcategory-id 172 action block
 category pre-defined subcategory-id 173 action block
 category pre-defined subcategory-id 174 action block
 category pre-defined subcategory-id 106 action block
 category pre-defined subcategory-id 108 action block
 category pre-defined subcategory-id 177 action block
 category pre-defined subcategory-id 251 action block
 category pre-defined subcategory-id 109 action block
 category pre-defined subcategory-id 110 action block
 category pre-defined subcategory-id 111 action block
 category pre-defined subcategory-id 112 action block
 category pre-defined subcategory-id 114 action block
 category pre-defined subcategory-id 115 action block
 category pre-defined subcategory-id 117 action block
 category pre-defined subcategory-id 178 action block
 category pre-defined subcategory-id 179 action block
 category pre-defined subcategory-id 180 action block
 category pre-defined subcategory-id 181 action block
 category pre-defined subcategory-id 248 action block
 category pre-defined subcategory-id 118 action block
 category pre-defined subcategory-id 119 action block
 category pre-defined subcategory-id 122 action block
 category pre-defined subcategory-id 182 action block
 category pre-defined subcategory-id 183 action block
 category pre-defined subcategory-id 184 action block
 category pre-defined subcategory-id 123 action block
 category pre-defined subcategory-id 124 action block
 category pre-defined subcategory-id 186 action block
 category pre-defined subcategory-id 187 action block
 category pre-defined subcategory-id 188 action block
```

```
category pre-defined subcategory-id 189 action block
category pre-defined subcategory-id 125 action block
category pre-defined subcategory-id 127 action block
category pre-defined subcategory-id 128 action block
category pre-defined subcategory-id 130 action block
category pre-defined subcategory-id 131 action block
category pre-defined subcategory-id 132 action block
category pre-defined subcategory-id 197 action block
category pre-defined subcategory-id 198 action block
category pre-defined subcategory-id 199 action block
category pre-defined subcategory-id 200 action block
category pre-defined subcategory-id 227 action block
category pre-defined subcategory-id 228 action block
category pre-defined subcategory-id 133 action block
category pre-defined subcategory-id 201 action block
category pre-defined subcategory-id 202 action block
category pre-defined subcategory-id 204 action block
category pre-defined subcategory-id 205 action block
category pre-defined subcategory-id 134 action block
category pre-defined subcategory-id 135 action block
category pre-defined subcategory-id 136 action block
category pre-defined subcategory-id 137 action block
category pre-defined subcategory-id 138 action block
category pre-defined subcategory-id 139 action block
category pre-defined subcategory-id 140 action block
category pre-defined subcategory-id 141 action block
category pre-defined subcategory-id 206 action block
category pre-defined subcategory-id 207 action block
category pre-defined subcategory-id 208 action block
category pre-defined subcategory-id 209 action block
category pre-defined subcategory-id 210 action block
category pre-defined subcategory-id 229 action block
category pre-defined subcategory-id 142 action block
category pre-defined subcategory-id 143 action block
category pre-defined subcategory-id 144 action block
category pre-defined subcategory-id 145 action block
category pre-defined subcategory-id 146 action block
category pre-defined subcategory-id 147 action block
category pre-defined subcategory-id 211 action block
category pre-defined subcategory-id 212 action block
category pre-defined subcategory-id 213 action block
category pre-defined subcategory-id 240 action block
category pre-defined subcategory-id 253 action block
category pre-defined subcategory-id 149 action block
category pre-defined subcategory-id 150 action block
category pre-defined subcategory-id 214 action block
category pre-defined subcategory-id 215 action block
category pre-defined subcategory-id 216 action block
category pre-defined subcategory-id 217 action block
category pre-defined subcategory-id 151 action block
category pre-defined subcategory-id 218 action block
category pre-defined subcategory-id 219 action block
category pre-defined subcategory-id 220 action block
category pre-defined subcategory-id 221 action block
category pre-defined subcategory-id 222 action block
category pre-defined subcategory-id 223 action block
category pre-defined subcategory-id 230 action block
category pre-defined subcategory-id 252 action block
category pre-defined subcategory-id 152 action block
category pre-defined subcategory-id 153 action block
category pre-defined subcategory-id 238 action block
category pre-defined subcategory-id 154 action block
category pre-defined subcategory-id 155 action block
category pre-defined subcategory-id 224 action block
category pre-defined subcategory-id 225 action block
category pre-defined subcategory-id 156 action block
category pre-defined subcategory-id 157 action block
category pre-defined subcategory-id 158 action block
category pre-defined subcategory-id 231 action block
```

```
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
profile type url-filter name profile_url_marketing
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
 category pre-defined subcategory-id 103 action block
 category pre-defined subcategory-id 166 action block
 category pre-defined subcategory-id 167 action block
 category pre-defined subcategory-id 168 action block
 category pre-defined subcategory-id 104 action block
 category pre-defined subcategory-id 169 action block
 category pre-defined subcategory-id 170 action block
 category pre-defined subcategory-id 106 action block
 category pre-defined subcategory-id 108 action block
 category pre-defined subcategory-id 177 action block
 category pre-defined subcategory-id 251 action block
 category pre-defined subcategory-id 109 action block
 category pre-defined subcategory-id 110 action block
 category pre-defined subcategory-id 111 action block
 category pre-defined subcategory-id 112 action block
 category pre-defined subcategory-id 114 action block
 category pre-defined subcategory-id 115 action block
 category pre-defined subcategory-id 117 action block
 category pre-defined subcategory-id 178 action block
 category pre-defined subcategory-id 179 action block
 category pre-defined subcategory-id 180 action block
 category pre-defined subcategory-id 181 action block
 category pre-defined subcategory-id 248 action block
 category pre-defined subcategory-id 118 action block
 category pre-defined subcategory-id 119 action block
 category pre-defined subcategory-id 122 action block
 category pre-defined subcategory-id 182 action block
 category pre-defined subcategory-id 183 action block
 category pre-defined subcategory-id 184 action block
 category pre-defined subcategory-id 123 action block
 category pre-defined subcategory-id 124 action block
 category pre-defined subcategory-id 186 action block
 category pre-defined subcategory-id 187 action block
 category pre-defined subcategory-id 188 action block
 category pre-defined subcategory-id 189 action block
 category pre-defined subcategory-id 125 action block
 category pre-defined subcategory-id 127 action block
 category pre-defined subcategory-id 128 action block
 category pre-defined subcategory-id 130 action block
 category pre-defined subcategory-id 131 action block
 category pre-defined subcategory-id 132 action block
 category pre-defined subcategory-id 197 action block
 category pre-defined subcategory-id 198 action block
 category pre-defined subcategory-id 199 action block
 category pre-defined subcategory-id 200 action block
 category pre-defined subcategory-id 227 action block
 category pre-defined subcategory-id 228 action block
 category pre-defined subcategory-id 133 action block
```

```
category pre-defined subcategory-id 201 action block
category pre-defined subcategory-id 202 action block
category pre-defined subcategory-id 204 action block
category pre-defined subcategory-id 205 action block
category pre-defined subcategory-id 134 action block
category pre-defined subcategory-id 135 action block
category pre-defined subcategory-id 136 action block
category pre-defined subcategory-id 137 action block
category pre-defined subcategory-id 138 action block
category pre-defined subcategory-id 139 action block
category pre-defined subcategory-id 140 action block
category pre-defined subcategory-id 141 action block
category pre-defined subcategory-id 206 action block
category pre-defined subcategory-id 207 action block
category pre-defined subcategory-id 208 action block
category pre-defined subcategory-id 209 action block
category pre-defined subcategory-id 210 action block
category pre-defined subcategory-id 229 action block
category pre-defined subcategory-id 142 action block
category pre-defined subcategory-id 143 action block
category pre-defined subcategory-id 144 action block
category pre-defined subcategory-id 145 action block
category pre-defined subcategory-id 146 action block
category pre-defined subcategory-id 147 action block
category pre-defined subcategory-id 211 action block
category pre-defined subcategory-id 212 action block
category pre-defined subcategory-id 213 action block
category pre-defined subcategory-id 240 action block
category pre-defined subcategory-id 253 action block
category pre-defined subcategory-id 149 action block
category pre-defined subcategory-id 150 action block
category pre-defined subcategory-id 214 action block
category pre-defined subcategory-id 215 action block
category pre-defined subcategory-id 216 action block
category pre-defined subcategory-id 217 action block
category pre-defined subcategory-id 151 action block
category pre-defined subcategory-id 218 action block
category pre-defined subcategory-id 219 action block
category pre-defined subcategory-id 220 action block
category pre-defined subcategory-id 221 action block
category pre-defined subcategory-id 222 action block
category pre-defined subcategory-id 223 action block
category pre-defined subcategory-id 230 action block
category pre-defined subcategory-id 252 action block
category pre-defined subcategory-id 152 action block
category pre-defined subcategory-id 153 action block
category pre-defined subcategory-id 238 action block
category pre-defined subcategory-id 154 action block
category pre-defined subcategory-id 155 action block
category pre-defined subcategory-id 224 action block
category pre-defined subcategory-id 225 action block
category pre-defined subcategory-id 156 action block
category pre-defined subcategory-id 157 action block
category pre-defined subcategory-id 158 action block
category pre-defined subcategory-id 231 action block
category pre-defined subcategory-id 232 action block
category pre-defined subcategory-id 159 action block
category pre-defined subcategory-id 254 action block
category pre-defined subcategory-id 160 action block
category pre-defined subcategory-id 161 action block
category pre-defined subcategory-id 176 action block
category pre-defined subcategory-id 226 action block
category pre-defined subcategory-id 234 action block
category pre-defined subcategory-id 235 action block
category pre-defined subcategory-id 236 action block
category pre-defined subcategory-id 237 action block
category pre-defined subcategory-id 239 action block
category pre-defined subcategory-id 241 action block
category pre-defined subcategory-id 233 action block
```

```
#
security-policy
 rule name policy_sec_huawei_com
  source-zone local
  destination-zone untrust
  action permit
 rule name policy_sec_research
  description Security policy of web access protect for research.
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  time-range time_range
  profile url-filter profile_url_research
  action permit
 rule name policy_sec_marketing
  description Security policy of web access protect for marketing.
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  time-range time_range
  profile url-filter profile_url_marketing
  action permit
#
return
```

5.6.4 举例：通过 URL 分类、黑名单和白名单控制用户访问的网站

组网需求

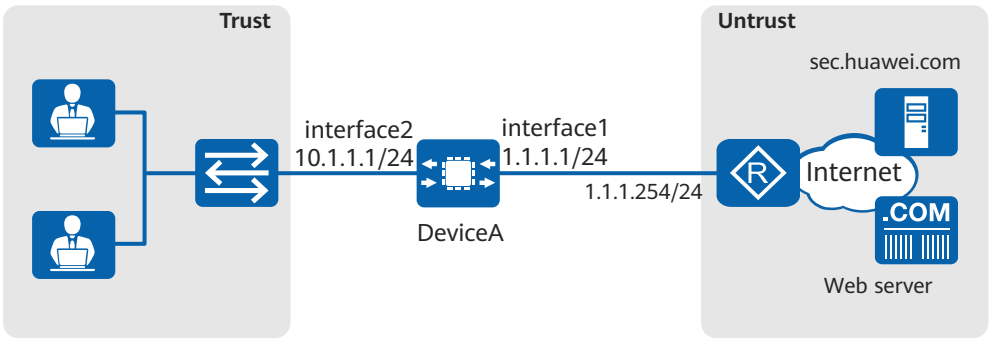
如图5-6所示，DeviceA作为企业网关部署在网络边界，对用户访问外部网络的URL访问请求进行URL过滤。企业只允许员工访问教育/科学类、搜索/门户类网站和社交网络，其他网站均不能访问。此外，企业希望对如下几个网站进行单独的控制：

- 允许员工访问内部论坛网站www.example3.com和www.example4.com。
- 不允许员工访问教育/科学类中的www.example2.com和社交网络类中的www.example1.com。

图 5-6 通过 URL 分类、黑名单和白名单控制用户访问的网站

说明

本例中interface1、interface2分别代表10GE0/0/1、10GE0/0/2。



配置思路

1. 配置接口IP地址和安全区域，完成网络基本参数配置。
2. 新建URL过滤配置文件“url_profile_01”，然后将www.example1.com和www.example2.com添加到黑名单中，将www.example3.com和

www.example4.com添加到白名单中。利用预定义URL分类，将教育/科学类、搜索/门户类网站和社交网络的控制动作设置为允许，其他网站设置为阻断。

3. 配置安全策略，引用URL过滤配置文件url_profile_01，实现URL访问控制。

操作步骤

步骤1 配置接口IP地址和安全区域，完成网络基本参数配置。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] ip address 1.1.1.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] ip address 10.1.1.1 255.255.255.0
[DeviceA-10GE0/0/2] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface 10ge 0/0/1
[DeviceA-zone-untrust] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/2
[DeviceA-zone-trust] quit
```

步骤2 配置URL过滤配置文件。

说明

通过**display url-filter category pre-defined**命令，可以查询到如下预定义分类和ID的对应关系。

- 17：教育/科学类（Education/Science）
- 15：搜索/门户类（Search Engines/Portals）
- 7：社交网络类（Social Network）

```
[DeviceA] profile type url-filter name url_profile_01
[DeviceA-profile-url-filter-url_profile_01] add blacklist url www.example1.com
[DeviceA-profile-url-filter-url_profile_01] add blacklist url www.example2.com
[DeviceA-profile-url-filter-url_profile_01] add whitelist url www.example3.com
[DeviceA-profile-url-filter-url_profile_01] add whitelist url www.example4.com
[DeviceA-profile-url-filter-url_profile_01] category pre-defined action block
[DeviceA-profile-url-filter-url_profile_01] category pre-defined category-id 15 action allow
[DeviceA-profile-url-filter-url_profile_01] category pre-defined category-id 17 action allow
[DeviceA-profile-url-filter-url_profile_01] category pre-defined category-id 7 action allow
[DeviceA-profile-url-filter-url_profile_01] quit
```

说明

如果用户希望阻断白名单之外的URL，则可以设置缺省动作为阻断，以便远程查询服务不可用时，DeviceA采取缺省动作，以此实现对白名单之外的URL进行阻断。

如果用户希望允许黑名单之外的URL，则可以设置缺省动作为允许，以便远程查询服务不可用时，DeviceA采取缺省动作，以此实现对黑名单之外的URL进行放行。

步骤3 在安全策略中应用URL过滤配置文件。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_01
[DeviceA-policy-security-rule-policy_sec_01] source-zone trust
[DeviceA-policy-security-rule-policy_sec_01] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_01] source-address 10.1.1.0 mask 255.255.255.0
[DeviceA-policy-security-rule-policy_sec_01] action permit
[DeviceA-policy-security-rule-policy_sec_01] profile url-filter url_profile_01
[DeviceA-policy-security-rule-policy_sec_01] quit
[DeviceA-policy-security] quit
```

步骤4 提交内容安全配置文件。

```
[DeviceA] engine configuration commit
Info: The operation may last for several minutes, please wait.
```

```
Info: URL submitted configurations successfully.
Info: Finish committing engine compiling.
```

----结束

检查配置结果

- 企业员工可以访问“教育/科学类”、“搜索/门户类”和“社交网络”，其他网站不允许访问。

  企业员工访问其他网站时，管理员可以看到Type（过滤类型）为“Pre-defined”，Action（动作）为“Block”的URL日志信息（URL/4/FILTER）。
- 企业员工可以访问www.example3.com和www.example4.com，不可以访问www.example1.com和www.example2.com。

  企业员工访问www.example3.com或www.example4.com时，管理员可以看到Type（过滤类型）为“Whitelist”，Action（动作）为“Allow”的URL日志信息（URL/4/FILTER）。

  企业员工访问www.example1.com或www.example2.com时，管理员可以看到Type（过滤类型）为“Blacklist”，Action（动作）为“Block”的URL日志信息（URL/4/FILTER）。

配置脚本

```
#
sysname DeviceA
#
interface 10GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface 10GE0/0/2
#
firewall zone untrust
 set priority 5
 add interface 10GE0/0/1
#
profile type url-filter name url_profile_01
 add blacklist url www.example1.com
 add blacklist url www.example2.com
 add whitelist url www.example3.com
 add whitelist url www.example4.com
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 category pre-defined subcategory-id 163 action block
 category pre-defined subcategory-id 164 action block
 category pre-defined subcategory-id 165 action block
 category pre-defined subcategory-id 103 action block
 category pre-defined subcategory-id 166 action block
 category pre-defined subcategory-id 167 action block
 category pre-defined subcategory-id 168 action block
 category pre-defined subcategory-id 104 action block
 category pre-defined subcategory-id 169 action block
 category pre-defined subcategory-id 170 action block
 category pre-defined subcategory-id 105 action block
 category pre-defined subcategory-id 171 action block
 category pre-defined subcategory-id 172 action block
 category pre-defined subcategory-id 173 action block
 category pre-defined subcategory-id 174 action block
 category pre-defined subcategory-id 106 action block
```

```
category pre-defined subcategory-id 109 action block
category pre-defined subcategory-id 110 action block
category pre-defined subcategory-id 111 action block
category pre-defined subcategory-id 112 action block
category pre-defined subcategory-id 114 action block
category pre-defined subcategory-id 115 action block
category pre-defined subcategory-id 117 action block
category pre-defined subcategory-id 178 action block
category pre-defined subcategory-id 179 action block
category pre-defined subcategory-id 180 action block
category pre-defined subcategory-id 181 action block
category pre-defined subcategory-id 248 action block
category pre-defined subcategory-id 118 action block
category pre-defined subcategory-id 119 action block
category pre-defined subcategory-id 122 action block
category pre-defined subcategory-id 182 action block
category pre-defined subcategory-id 183 action block
category pre-defined subcategory-id 184 action block
category pre-defined subcategory-id 123 action block
category pre-defined subcategory-id 124 action block
category pre-defined subcategory-id 186 action block
category pre-defined subcategory-id 187 action block
category pre-defined subcategory-id 188 action block
category pre-defined subcategory-id 189 action block
category pre-defined subcategory-id 125 action block
category pre-defined subcategory-id 127 action block
category pre-defined subcategory-id 128 action block
category pre-defined subcategory-id 130 action block
category pre-defined subcategory-id 131 action block
category pre-defined subcategory-id 132 action block
category pre-defined subcategory-id 197 action block
category pre-defined subcategory-id 198 action block
category pre-defined subcategory-id 199 action block
category pre-defined subcategory-id 200 action block
category pre-defined subcategory-id 227 action block
category pre-defined subcategory-id 228 action block
category pre-defined subcategory-id 133 action block
category pre-defined subcategory-id 201 action block
category pre-defined subcategory-id 202 action block
category pre-defined subcategory-id 204 action block
category pre-defined subcategory-id 205 action block
category pre-defined subcategory-id 134 action block
category pre-defined subcategory-id 135 action block
category pre-defined subcategory-id 136 action block
category pre-defined subcategory-id 137 action block
category pre-defined subcategory-id 138 action block
category pre-defined subcategory-id 139 action block
category pre-defined subcategory-id 140 action block
category pre-defined subcategory-id 141 action block
category pre-defined subcategory-id 206 action block
category pre-defined subcategory-id 207 action block
category pre-defined subcategory-id 208 action block
category pre-defined subcategory-id 209 action block
category pre-defined subcategory-id 210 action block
category pre-defined subcategory-id 229 action block
category pre-defined subcategory-id 142 action block
category pre-defined subcategory-id 143 action block
category pre-defined subcategory-id 144 action block
category pre-defined subcategory-id 145 action block
category pre-defined subcategory-id 146 action block
category pre-defined subcategory-id 147 action block
category pre-defined subcategory-id 211 action block
category pre-defined subcategory-id 212 action block
category pre-defined subcategory-id 213 action block
category pre-defined subcategory-id 240 action block
category pre-defined subcategory-id 253 action block
category pre-defined subcategory-id 149 action block
category pre-defined subcategory-id 150 action block
category pre-defined subcategory-id 214 action block
```

```
 category pre-defined subcategory-id 215 action block
 category pre-defined subcategory-id 216 action block
 category pre-defined subcategory-id 217 action block
 category pre-defined subcategory-id 151 action block
 category pre-defined subcategory-id 218 action block
 category pre-defined subcategory-id 219 action block
 category pre-defined subcategory-id 220 action block
 category pre-defined subcategory-id 221 action block
 category pre-defined subcategory-id 222 action block
 category pre-defined subcategory-id 223 action block
 category pre-defined subcategory-id 230 action block
 category pre-defined subcategory-id 252 action block
 category pre-defined subcategory-id 152 action block
 category pre-defined subcategory-id 153 action block
 category pre-defined subcategory-id 238 action block
 category pre-defined subcategory-id 154 action block
 category pre-defined subcategory-id 155 action block
 category pre-defined subcategory-id 224 action block
 category pre-defined subcategory-id 225 action block
 category pre-defined subcategory-id 156 action block
 category pre-defined subcategory-id 157 action block
 category pre-defined subcategory-id 158 action block
 category pre-defined subcategory-id 231 action block
 category pre-defined subcategory-id 232 action block
 category pre-defined subcategory-id 159 action block
 category pre-defined subcategory-id 254 action block
 category pre-defined subcategory-id 160 action block
 category pre-defined subcategory-id 161 action block
 category pre-defined subcategory-id 176 action block
 category pre-defined subcategory-id 226 action block
 category pre-defined subcategory-id 234 action block
 category pre-defined subcategory-id 235 action block
 category pre-defined subcategory-id 236 action block
 category pre-defined subcategory-id 237 action block
 category pre-defined subcategory-id 239 action block
 category pre-defined subcategory-id 241 action block
 category pre-defined subcategory-id 233 action block
#
security-policy
 rule name policy_sec_01
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  profile url-filter url_profile_01
  action permit
```

5.7 配置不解密方式的 HTTPS URL 过滤

背景信息

URL过滤功能支持通过配置加密流量过滤功能实现不解密方式的HTTPS流量的URL过滤功能。

加密流量过滤功能不对HTTPS流量进行解密，而是通过从客户端Client Hello报文的SNI（Server Name Indication）字段、服务器Certificate报文的CN（Common Name）字段中获取用户访问的网站域名（hostname）实现URL过滤的。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 （可选）配置设备的业务性能模式。

forward performance mode { **routing** | **security** }

当设备业务性能模式处于路由模式时，设备的安全业务处理性能较低，建议将设备业务性能模式切换到安全模式。用户可通过命令**display forward performance mode**查看设备当前的业务性能模式。

设备业务性能模式缺省情况如下：

- 对于AR5700系列和AR6700系列：缺省情况下，设备业务性能模式处于安全模式。
- 对于AR8000系列：缺省情况下，设备业务性能模式处于路由模式。

步骤3 创建URL过滤配置文件。

profile type url-filter name *name*

步骤4 开启加密流量过滤功能。

https-filter enable

加密流量过滤功能的生效范围仅为所在的URL过滤配置文件，不是全局生效的。

步骤5 返回系统视图。

quit

步骤6 提交配置。

engine configuration commit

创建或修改URL过滤配置文件后，配置内容不会立即生效，需要执行提交操作来激活。

----结束

后续处理

此处仅提供在URL过滤配置文件中开启加密流量检测过滤的配置，实际使用过程中，还需要配置黑名单、白名单或URL分类，然后在安全策略中引用URL过滤配置文件，该功能才会生效。详细配置请参考**5.5.1 配置基于黑名单和白名单的URL过滤**和**5.6.1 配置基于URL分类的URL过滤**。

5.8 维护 URL 过滤

常用维护命令

表 5-7 维护 URL 过滤

操作	命令
查看URL分类的统计信息	**display url-filter category pre-defined** [**subcategory-id** *subcategory-id*] **statistics**
查看URL过滤的统计信息	**display url-filter statistics** [**slot** *slot-id* **cpu** *cpu-id*]
清除URL过滤的统计信息	**reset url-filter statistics** { **blacklist** | **whitelist** | **all** }

查看日志

在安全策略中引用URL过滤配置文件后，设备对命中安全策略的流量进行内容检测。当用户访问的URL命中了URL过滤配置文件中定义的过滤规则时，则产生内容日志。一条URL过滤日志的实例如下：

```
URL/4/FILTER(l): The URL filtering policy was matched.(SyslogId=100, VSys="vsys_1", Policy="rule_1", SrcIp=192.168.0.100, DstIp=172.16.10.100, SrcPort=6096, DstPort=80, SrcZone=trust, DstZone=untrust, User="user_1", Protocol=TCP, Application="HTTP", Profile="profile_l", Type=Blacklist, EventNum=1, Category="none", SubCategory="none", Page="*ath", Host="www.example1.com", Referer="www.example2.com", Item="www.examole1.com", Action=Block)
```

日志中各字段的含义请参见《日志参考-URL-URL/4/FILTER》。

6 入侵防御（IPS）配置

6.1 入侵防御简介

定义

入侵防御（Intrusion Prevention System，IPS）是一种基于攻击特征库检测入侵行为，并采取一定响应措施实时中止入侵的安全机制。

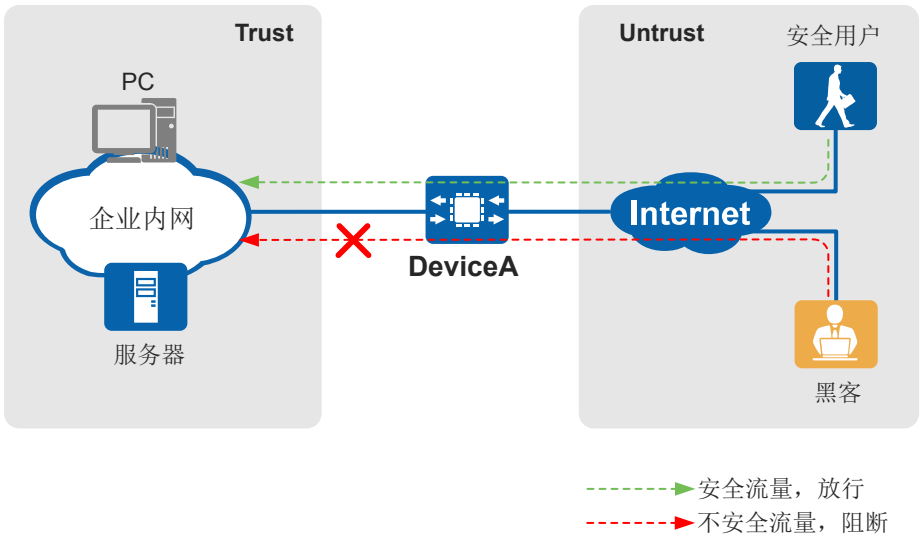
目的

木马、蠕虫、僵尸网络、间谍软件、溢出攻击以及注入攻击等层出不穷，时刻威胁网络安全。另外操作系统、应用程序的安全漏洞，也给黑客提供了可乘之机。针对此问题，华为提供入侵防御功能，全方位防御各种攻击行为，保护网络免受侵害。

如**图6-1**所示，当外网用户访问企业内网时，设备对访问流量进行检测。如果发现入侵行为则阻断连接；反之则放行。

同样当内网用户访问外网时，如果访问的网页或服务器包含恶意代码时，设备将阻断连接；反之则放行。

图 6-1 入侵防御示意图



受益

入侵防御的主要优势如下：

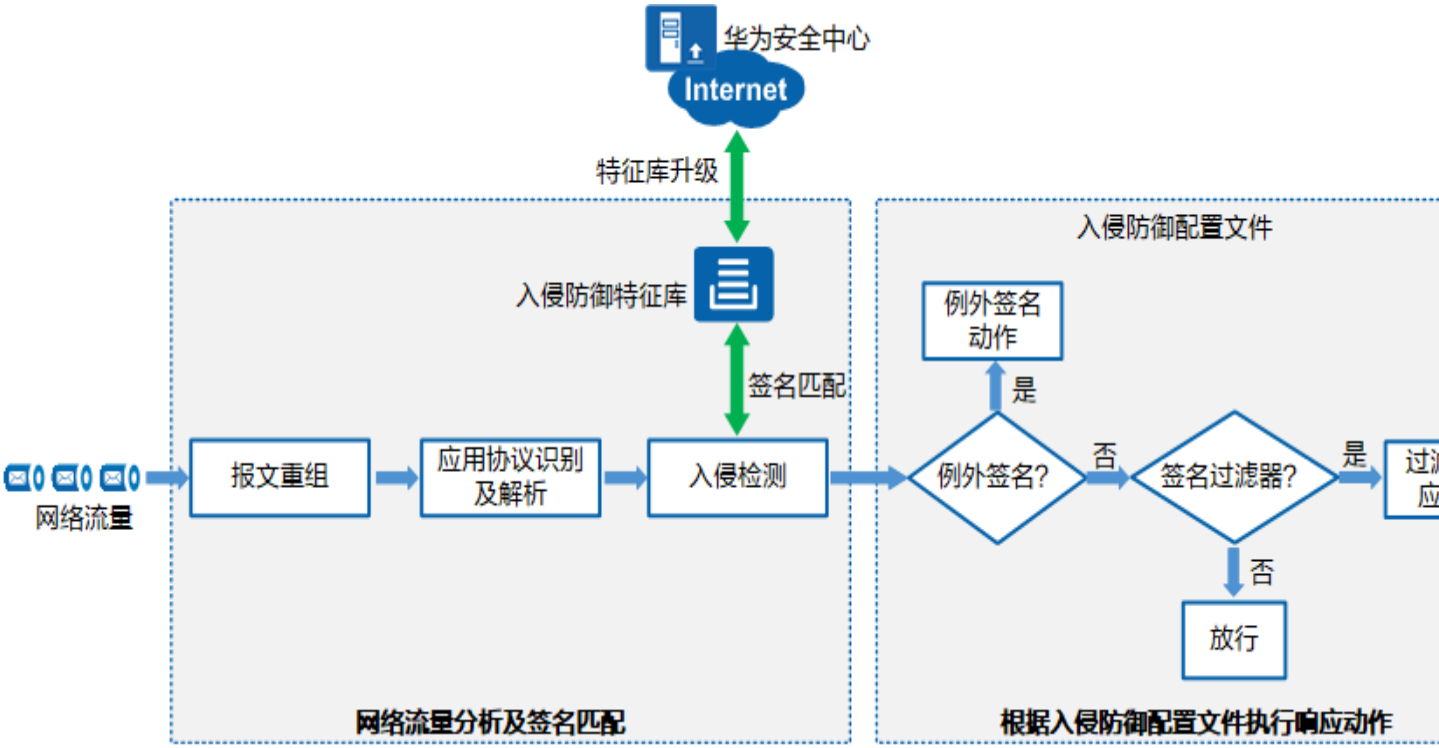
- 实时阻断攻击：设备直路部署在网络中，能够实时对入侵活动和攻击性网络流量进行拦截，将对网络的影响降到最低。
- 深层防护：新型的攻击都隐藏在TCP/IP协议的应用层里，入侵防御不但能检测报文应用层的内容，还可以对网络数据流重组进行协议分析和检测，并根据攻击类型、策略等确定应该被拦截的流量。
- 全方位防护：入侵防御可以提供针对蠕虫、病毒、木马、僵尸网络、间谍软件、广告软件、CGI（Common Gateway Interface）攻击、跨站脚本攻击、注入攻击、目录遍历、信息泄露、远程文件包含攻击、溢出攻击、代码执行、拒绝服务、扫描工具等多种攻击的防护措施，全方位保护网络安全。
- 内外兼防：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

6.2 入侵防御原理描述

6.2.1 入侵防御处理流程

如图6-2所示，入侵防御处理流程主要包括通过签名匹配检测攻击、攻击响应处理两部分。

图 6-2 入侵防御处理流程



1. 报文重组

   收到流量后，设备首先进行IP分片报文重组以及TCP流重组，确保了应用层数据的连续性，有效检测出逃避入侵防御检测的攻击行为。

2. 应用协议识别和解析

   设备根据报文内容识别出具体的应用层协议，并对协议进行深度解析以提取报文特征。

   与传统只能根据IP地址和端口识别协议相比，大大提高了对应用层攻击行为的检测率。

3. 签名匹配

   将解析后的报文特征与**6.2.2 入侵防御签名**进行匹配，如果匹配了签名，则进行响应处理。

   设备支持定期从华为安全中心（**isecurity.huawei.com**）下载最新的入侵防御特征库，及时有效防御网络入侵。

4. 响应处理

   报文匹配了签名后，是否进行响应处理、如何进行响应处理（告警还是阻断）由**6.2.3 入侵防御配置文件**决定。入侵防御配置文件主要包含例外签名、签名过滤器两部分。

   a. 判断匹配的签名是否属于例外签名，如果属于例外签名，执行例外签名的响应动作。否则进入下一步处理。

   b. 判断匹配的签名是否属于签名过滤器筛选出的签名，如果属于则执行签名过滤器的响应动作。否则直接放行报文。

   签名过滤器是管理员根据网络和业务状况配置的，筛选签名的过滤条件集合。设备只有针对性地防御过滤器筛选出的签名对应的攻击，避免海量攻击日志淹没关键攻击。

另外，设备还提供例外签名功能，当过滤器统一设置的动作不满足需要时，供管理员修改单个签名的动作。例外签名动作的优先级高于签名过滤器。

6.2.2 入侵防御签名

入侵防御签名用来描述网络入侵行为的特征，入侵防御功能的核心是将报文内容和签名进行比较来检测入侵行为。

预定义签名

云端华为安全中心（**isecurity.huawei.com**）提供入侵防御特征库（签名库），里面包含针对各种已知入侵行为的签名信息，这些签名称为预定义签名。使用时需要将最新特征库下载到设备，使设备持续拥有最新的入侵防御能力。

图6-3是一个签名的信息，具体介绍见表6-1。

图 6-3 预定义签名

表 6-1 预定义签名信息

项目	含义
ID	ID用来唯一标识签名。
状态	签名当前是否启用，设备只能检测处于启用状态的签名对应的攻击。
对象	攻击行为所针对目标的角色，包括： ● 服务端：表示攻击行为是针对服务器发起的。 ● 客户端：表示攻击行为是针对客户端发起的。
严重性	攻击后果的严重性，分为高、中、低、提示四种。
操作系统	攻击行为所针对的操作系统。
协议	攻击行为使用的协议类型。
威胁类别	攻击行为的类别，包括木马、蠕虫、注入攻击、溢出攻击等。

项目	含义
动作	对匹配签名的攻击报文的缺省处理动作，包括： ● 告警：允许通过，但会记录日志。 ● 阻断：丢弃报文，并记录日志。
参考信息	其他参考信息，包括漏洞在权威漏洞机构的编号及漏洞介绍的网站信息。例如CVE表示漏洞在Common Vulnerabilities and Exposures中的编号。

自定义签名

须知

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

自定义签名是指管理员根据网络流量特点对特定的入侵行为自行定义的签名。网络中出现新的入侵后，其对应的攻击签名通常会晚一点才会更新到预定义特征库中，管理员可以在深入分析入侵特征后创建自定义签名以便实时防御入侵。待预定义特征库更新后，便可使用预定义签名。另外，当管理员出于某种原因要阻止特定的行为（可能并非入侵行为），也可以根据报文的行为特征创建一个动作为阻断的自定义签名。

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

6.2.3 入侵防御配置文件

入侵防御配置文件是入侵防御功能的核心，用于决定设备对哪些攻击进行防御，如何防御。

入侵防御配置文件的组成

签名过滤器

入侵防御特征库中包含针对各种攻击行为的海量签名信息，但是在实际网络环境中，业务类型可能比较集中，不需要使用所有的签名。如果设备对所有签名都进行防御，可能产生大量无关攻击日志，影响对关键攻击事件的处理和调测。此时需要配置签名过滤器，根据业务情况筛选出需要关注的签名并配置攻击响应动作。设备只防御签名过滤器筛选出的签名。

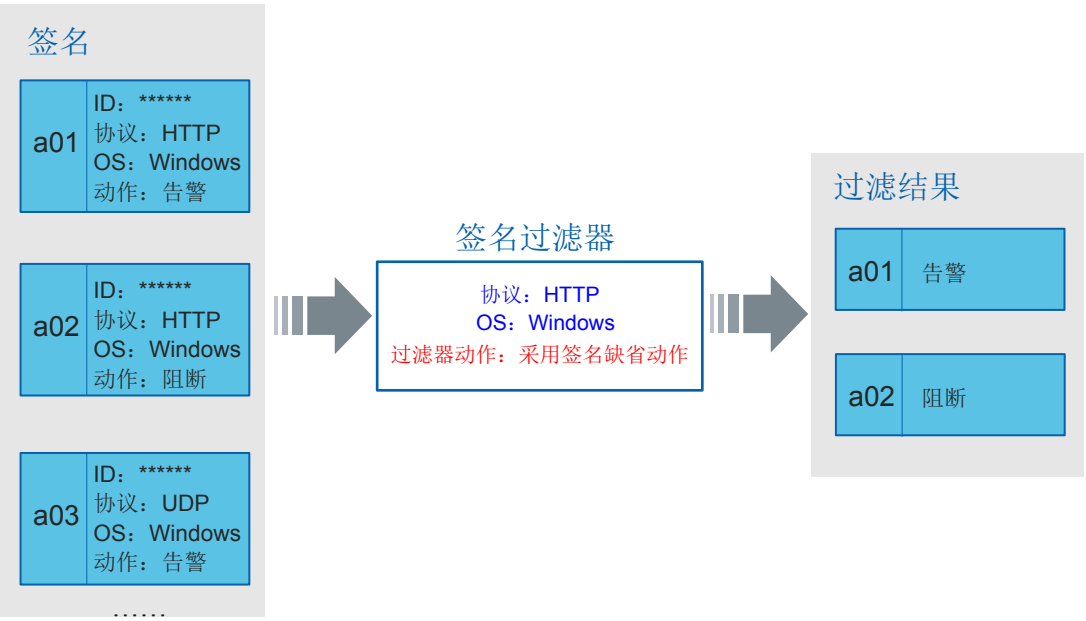
签名过滤器是一系列过滤签名的条件集合，过滤条件包括：签名的威胁类别、对象、协议、严重性、操作系统等。只有同时满足所有过滤条件的签名才符合条件。一个过滤条件中如果配置多个值，多个值之间是“或”的关系，只要匹配任意一个值，就认为匹配了这个条件。

通常情况下，对于筛选出来的这些签名，在签名过滤器中配置沿用签名本身的缺省动作即可。同时也支持在过滤器中为所有签名统一设置动作。签名过滤器的动作优先级高于签名缺省动作，当签名过滤器的动作不采用签名缺省动作时，以签名过滤器设置的动作为准。

各签名过滤器之间存在优先关系（按照配置顺序，先配置的优先）。如果一个配置文件中的多个签名过滤器包含同一个签名，当报文命中此签名后，设备将根据优先级高的签名过滤器的动作对报文进行处理。

如图6-4所示，例如设备的保护对象是运行Windows操作系统的Web服务器，则可以配置签名过滤器筛选操作系统是Windows、协议是HTTP的签名。

图 6-4 签名过滤器



例外签名

在签名过滤器中设置的签名动作是统一的，无法修改单个签名动作。考虑到各种例外情况，设备提供例外签名功能。管理员在入侵防御配置文件中将特定签名指定为例外签名，并单独设置动作。例如查看日志发现，正常使用的某个应用软件命中了签名过滤器中某个签名，被误阻断了。此时管理员可将此签名指定为例外签名，并修改动作为放行。

例外签名的动作分为阻断、告警、放行和添加黑名单。其中，添加黑名单是指在阻断流量的同时，将报文的源地址或目的地址添加至黑名单隔离访问。

例外签名的动作优先级高于签名过滤器。如果一个签名同时命中例外签名和签名过滤器，则以例外签名的动作为准。

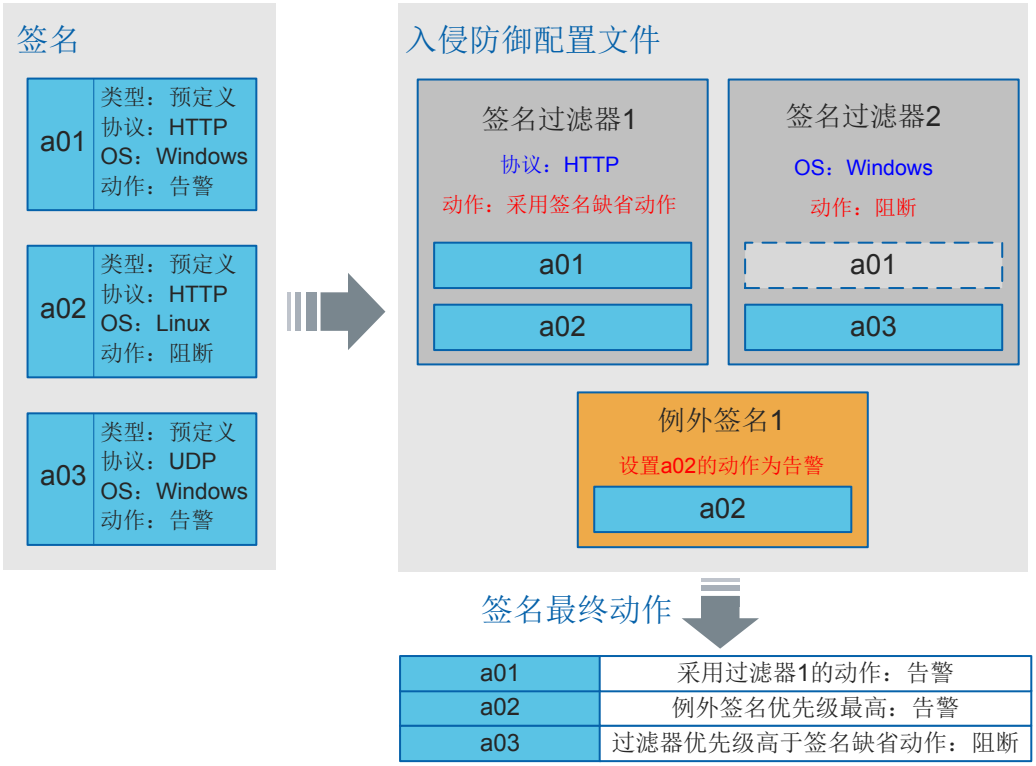
如何确定签名最终响应动作

一个入侵防御配置文件中可以配置多个签名过滤器、多个例外签名，签名最终的响应动作由这些配置决定，优先级从高到低依次为：例外签名动作、签名过滤器动作、签名自身的缺省动作。

如图6-5所示，入侵防御配置文件中配置了两个签名过滤器和一个例外签名，签名最终的响应动作如下：

- 签名a01：当入侵防御配置文件中配置多个签名过滤器时，签名过滤器的优先级按照配置顺序从高到低排列。签名按照签名过滤器的顺序依次匹配过滤器，一旦匹配一个就不再继续。因此对于图6-5，签名a01只会匹配签名过滤器1，动作是告警。
- 签名a02：例外签名优先级高于签名过滤器1的优先级，因此签名a02的动作为告警。
- 签名a03：匹配签名过滤器2，动作为阻断。签名过滤器的统一动作优先级高于签名的缺省动作。

图 6-5 签名的响应动作



当数据流命中多个签名，对该数据流的处理方式如下：

- 如果这些签名的实际动作都为**告警**时，最终动作为告警。
- 如果这些签名中至少有一个签名的实际动作为**阻断**时，最终动作为阻断。

缺省入侵防御配置文件

配置签名过滤器需要对网络和业务非常了解，有一定难度。设备缺省提供满足常见场景的入侵防御配置文件。每个缺省配置文件筛选签名的条件和处理动作如表6-2所示。

表 6-2 缺省入侵防御配置文件

配置文件名称	对象	严重性	操作系统	协议	威胁类别	动作	应用场景
video_surveillance	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	DNS、HTTP、FTP、TELNET、SSH、RTSP、SSL、UDP、TCP	全部	采用签名的缺省动作	该配置文件适用于当设备部署在视频监控的场景。
strict	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	全部	全部	阻断	该配置文件适用于需要设备阻断所有命中签名的报文场景。
web_server	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	DNS、HTTP、FTP	全部	采用签名的缺省动作	该配置文件适用于当设备部署在Web服务器前面的场景。

配置文件名称	对象	严重性	操作系统	协议	威胁类别	动作	应用场景
file_server	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	DNS、SMB、NETBIOS、NFS、SUNRPC、MSRPC、FILE、TELNET	全部	采用签名的缺省动作	该配置文件适用于当设备部署在File服务器前面的场景。
dns_server	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	DNS	全部	采用签名的缺省动作	该配置文件适用于当设备部署在DNS服务器前面的场景。
mail_server	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	DNS、IMAP4、SMTP、POP3	全部	采用签名的缺省动作	该配置文件适用于当设备部署在Mail服务器前面的场景。

配置文件名称	对象	严重性	操作系统	协议	威胁类别	动作	应用场景
inside_firewall	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	除TELNET和TFTP之外的协议	全部	采用签名的缺省动作	该配置文件适用于当设备部署在防火墙内侧的场景。
dmz	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	除NETBIOS、NFS、SMB、TELNET和TFTP之外的协议	全部	采用签名的缺省动作	该配置文件适用于当设备部署在DMZ区域前的场景。
outside_firewall	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	全部	除扫描工具之外的威胁类别	采用签名的缺省动作	该配置文件适用于当设备部署在防火墙外侧的场景。

配置文件名称	对象	严重性	操作系统	协议	威胁类别	动作	应用场景
ids	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	全部	全部	告警	该配置文件适用于当设备以IDS（旁路）模式部署时的通用场景。
default	全部	低、中、高	Unix-like、Windows、Android、iOS、Other	全部	全部	采用签名的缺省动作	该配置文件适用于当设备以IPS（直路）模式部署时的通用场景。

应用入侵防御配置文件

需要在安全策略中引用入侵防御配置文件，入侵防御功能才生效。也就是设备对符合安全策略匹配条件的流量，进行入侵防御。

当配置引用入侵防御配置文件的安全策略时，注意安全策略的方向是访问发起的方向，而非攻击发起的方向。例如：企业内网PC访问外网服务器遭到恶意攻击，虽然攻击方向是从外网到内网，但是因为发起访问的方向是从内网到外网，因此入侵防御配置文件需要应用到内网访问外网的安全策略中，具体配置如**表6-3**所示。

表 6-3 保护内网 PC 的安全策略

源安全区域	源地址	目的安全区域	目的地址	动作	入侵防御配置文件
内网trust区域	内网网段	外网untrust区域	any	允许	应用入侵防御配置文件

6.3 入侵防御（IPS）配置注意事项

License 依赖

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

硬件依赖

表 6-4 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 6-5 本特性的使用限制

特性限制	系列	涉及产品
设备使用入侵防御功能对流量进行内容安全检测时，会对整机的性能有一定的影响，请根据实际需求有选择性的进行配置。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

特性限制	系列	涉及产品
在双机热备组网环境中，推荐在主备备份方式下开启入侵防御功能。在逐流负载分担组网环境下，可配置入侵防御功能，但检测率会有所下降。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
当入侵防御功能部署在两台路由设备中间的安全设备上，且两台路由设备通过BFD互相探测时，网络如果发生偶发性拥塞会导致BFD震荡。建议将路由设备上的BFD检测时间适当调大（建议大于100ms），避免网络偶发性拥塞时导致BFD震荡。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
在报文来回路径不一致的组网环境中，设备无法接收到一条数据流的所有报文，因此很可能无法有效检测到网络入侵。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
入侵防御特征库升级之后，如果原有预定义签名在新的特征库中已经不存在，则该签名涉及的所有配置信息将失效。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

6.4 入侵防御缺省配置

入侵防御的缺省配置如表6-6所示。

表 6-6 入侵防御缺省配置

参数	缺省配置
入侵防御功能	未开启
入侵防御配置文件	设备缺省提供的入侵防御配置文件见表6-2
关联检测功能	开启
入侵防御日志归并功能	开启

6.5 升级入侵防御特征库

前提条件

- 特征库升级前准备请参见《配置指南-系统管理配置-特征库升级配置》中的“特征库升级前准备”。
- 通过在线升级的方式升级入侵防御特征库前，需要先配置设备与华为安全中心通信，详细配置请参见《配置指南-系统管理配置-特征库升级配置-配置特征库在线升级》中的“配置设备与华为安全中心通信”。

背景信息

华为安全中心（**isecurity.huawei.com**）定期发布入侵防御特征库，及时将设备的入侵防御特征库升级到最新版本，才能更及时有效地防御网络入侵。

此处仅提供了特征库在线升级的基本步骤，特征库离线升级及其他特征库升级的相关信息请参见《配置指南-系统管理配置》中的“特征库升级配置”。

操作步骤

步骤1 配置DNS服务器，确保设备可以正确解析安全中心域名。

```
system-view
dns resolve
dns server ip-address
```

步骤2 手动立即升级入侵防御特征库到最新版本。

```
update online ips-sdb
```

设备定时每周升级一次入侵防御特征库。

步骤3 配置定时升级入侵防御特征库功能。

1. 开启定时升级功能

   ```
   update schedule ips-sdb enable
   ```

2. 配置定时升级时间

   ```
   update schedule ips-sdb { hourly minute | { daily | weekly { mon | tue | wed | thu | fri | sat | sun } } time }
   ```

   入侵防御特征库定时升级功能缺省开启，设备在22：00～08：00之间随机选择一个时间作为入侵防御特征库每天进行定时升级的时间，可以手动进行配置。

   建议入侵防御特征库每周升级一次。

----结束

6.6 配置入侵防御

6.6.1 使用缺省入侵防御配置文件

背景信息

为简化管理员配置，设备缺省存在多个入侵防御配置文件以适应不同的应用场景，具体介绍如表6-2所示。管理员只需在安全策略中引用缺省入侵防御配置文件即完成配置。缺省入侵防御配置文件不允许修改和删除。

如果您对网络和业务情况比较熟悉，还可以6.6.2 手动创建入侵防御配置文件，管理员自行配置签名过滤器，筛选关注的签名进行防御。

说明

通过命令**display profile type ips name** *name*可以查看到缺省配置文件中的配置信息。通过命令行配置安全策略引用缺省配置文件时，需要输入完整的配置文件名称（如**default**），否则无法成功引用。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 （可选）配置设备的业务性能模式。

```
forward performance mode { routing | security }
```

当设备业务性能模式处于路由模式时，设备的安全业务处理性能较低，建议将设备业务性能模式切换到安全模式。用户可通过命令**display forward performance mode**查看设备当前的业务性能模式。

设备业务性能模式缺省情况如下：

- 对于AR5700系列和AR6700系列：缺省情况下，设备业务性能模式处于安全模式。
- 对于AR8000系列：缺省情况下，设备业务性能模式处于路由模式。

步骤3 进入安全策略视图。

```
security-policy
```

步骤4 创建安全策略规则，并进入安全策略规则视图。

```
rule name rule-name
```

步骤5 在安全策略中引用缺省入侵防御配置文件。

```
profile ips profile-name
```

此处仅体现了在安全策略中引用缺省入侵防御配置文件的配置步骤，安全策略的匹配条件配置未给出，具体请参见《配置指南-安全配置》中的“安全策略配置”。

步骤6 配置安全策略规则的动作为**permit**。

```
action permit
```

步骤7 退回系统视图。

```
quit
quit
```

----结束

6.6.2 手动创建入侵防御配置文件

背景信息

当管理员需要根据实际网络和业务情况，筛选需要关注的签名时，可以手动创建入侵防御文件，然后在安全策略中引用。

另外手动创建的入侵防御文件，还提供例外签名功能，可以调整单个签名的动作。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 （可选）配置设备的业务性能模式。

```
forward performance mode { routing | security }
```

当设备业务性能模式处于路由模式时，设备的安全业务处理性能较低，建议将设备业务性能模式切换到安全模式。用户可通过命令**display forward performance mode**查看设备当前的业务性能模式。

设备业务性能模式缺省情况如下：

- 对于AR5700系列和AR6700系列：缺省情况下，设备业务性能模式处于安全模式。
- 对于AR8000系列：缺省情况下，设备业务性能模式处于路由模式。

步骤3 创建入侵防御配置文件。

```
profile type ips name name
```

步骤4 创建IPS签名过滤器。

```
signature-set name name
```

步骤5 配置IPS签名过滤器的过滤条件和动作。

配置项	命令
签名针对的攻击目标	**target** { **both** | **client** | **server** }
签名的严重性等级	**severity** { **high** | **medium** | **low** | **information** } *
签名针对的操作系统	**os** { **android** | **ios** | **unix-like** | **windows** | **other** } *
签名针对的协议	**protocol** { *protocol-name* &<1-10> | **all** } **说明** 如果执行**protocol all**命令指定为所有协议后需要修改为指定协议，则需要先执行**undo protocol all**命令取消指定所有协议，再执行**protocol** *protocol-name*命令。
签名的攻击类型	**category** { *category-name* &<1-10> | **all** } **说明** 如果执行**category all**命令指定为所有类型后需要修改为指定类型，则需要先执行**undo category all**命令取消指定所有类型，再执行**category** *category-name*命令。
IPS签名过滤器的动作	**action** { **alert** | **block** | **default** }

通常情况下，签名过滤器的动作使用default也就是签名缺省动作即可。

步骤6 退回入侵防御配置文件视图。

```
quit
```

步骤7 **可选:** 在入侵防御配置文件视图下配置例外签名。

```
exception ips-signature-id ips-signature-id [ action { alert | allow | block } ]
```

设备支持配置例外签名的响应动作，包括告警、放行、阻断和直接将命中例外签名的流量的源/目的地址添加进黑名单。另外，可通过参数**timeout** *timeout*配置该黑名单的超时时间。

步骤8 退回到系统视图。

```
quit
```

步骤9 在安全策略中引用入侵防御配置文件。

1. 进入安全策略视图。
   ```
   security-policy
   ```
2. 创建安全策略规则，并进入安全策略规则视图。
   ```
   rule name rule-name
   ```
3. 引用入侵防御配置文件。
   ```
   profile ips profile-name
   ```
   此处仅体现了在安全策略中引用入侵防御配置文件的配置步骤，安全策略的匹配条件配置未给出，具体请参见《配置指南-安全配置》中的“安全策略配置”。
4. 配置安全策略规则的动作为**permit**。
   ```
   action permit
   ```
5. 退回系统视图。
   ```
   quit
   quit
   ```

步骤10 在系统视图下提交配置。

```
engine configuration commit
```

创建或修改入侵防御配置文件后，配置内容不会立即生效，需要执行提交操作来激活。因为激活过程所需时间较长，建议您完成所有对入侵防御配置文件的操作后再统一进行提交。

----结束

6.7 （可选）配置签名

配置预定义签名状态

预定义签名的状态分为启用和禁用，管理员可以批量修改它们的状态，也可以单独修改某个预定义签名的状态。

查看威胁日志时如果发现某些攻击是误报时，可以修改对应签名的状态为禁用。

步骤1 进入系统视图。

```
system-view
```

步骤2 根据需要设置预定义签名状态。

- 设置所有预定义签名的状态。
  ```
  ips signature-state { enabled | disabled }
  ```


- 设置特定预定义签名的状态。
  ips signature-state signature-id *signature-id* { **enabled** | **disabled** }

步骤3 提交配置生效。

engine configuration commit

----结束

配置自定义签名

自定义签名主要由基本特征和规则组成，基本特征用来描述签名的特征，规则用来描述签名的匹配规则。

步骤1 进入系统视图。

system-view

步骤2 创建自定义签名。

ips signature-id *signature-id*

步骤3 **可选:** 配置自定义签名的名称。

name *name*

步骤4 配置自定义签名的基本特征。

基本特征主要用来描述签名的特征，而不是用来定义签名，这些特征是在签名过滤器批量过滤签名时使用。数据流匹配签名时会与签名规则进行匹配，不会与基本特征项进行匹配，所以基本特征项不需要完全跟签名对应的入侵实际情况匹配。

配置项	命令
配置自定义签名检测目标	**target** { **both** | **client** | **server** }
配置自定义签名的协议	**protocol** *protocol-name*
配置自定义签名的威胁等级	**severity** { **high** | **medium** | **low** | **information** }
配置自定义签名的动作	**action** { **alert** | **block** | **allow** }

步骤5 创建自定义签名的规则。

rule name *name*

一个自定义签名中可以配置多条规则，多条规则互不影响，没有先后顺序，只要报文命中了至少一条规则即命中了此签名。

步骤6 配置自定义签名规则的检查项。

condition value *text*

每条规则只能配置一个检查项，检查项的配置使用的IPS第三代引擎语法提供了更加丰富的配置。

自定义签名规则的检查项配置使用IPS第三代引擎语法，IPS第三代引擎语法在保留已有语法检测精度的情况下，大幅提高了处理效率，同时可以兼容业界常见的语法，具有更好的开放性。关于IPS第三代引擎语法的介绍请参见**IPS新语法手册**。

说明

当待检测协议是HTTP时，指定特征串时必须同时指定协议字段，例如content value content:"abc";http_uri，否则无法检测成功。

步骤7 返回到系统视图。

```
quit
quit
```

步骤8 在系统视图下提交配置。

```
engine configuration commit
```

创建或修改自定义签名后，配置内容不会立即生效，需要执行提交操作来激活。因为激活过程所需时间较长，建议您完成所有对自定义签名的操作后再统一进行提交。

----结束

查看签名信息

通过**display**命令可以了解签名对应的入侵行为的特征，方便后续进行配置。

- 查看预定义签名或自定义签名的信息。

  display ips-signature [{ **pre-defined** | **user-defined** } [**associated**]] [**category** { *category-name* | **all** } | **os** { **all** | **android** | **ios** | **unix-like** | **windows** | **other** } * | **protocol** { *protocol-name* | **all** } | **severity** { **information** | **low** | **medium** | **high** } * | **state** { **disabled** | **enabled** } | **target** { **server** | **client** | **both** }] *

- 查看特定签名的信息。

  display ips-signature *ips-signature-id*

- 查看指定名字的自定义签名规则的内容。

  display ips signature-id *signature-id* **rule** { **name** *rule-name* | **all** }

----结束

6.8 （可选）配置关联检测

背景信息

某些攻击行为非常复杂，基于单包的签名匹配无法准确检测攻击，需要关联检测一条数据流甚至多条数据流的报文才能检测出攻击。针对此类攻击，设备提供关联检测功能，将某些攻击签名设置为关联签名，然后基于某种条件统计流量命中关联签名的次数，命中次数超出阈值才算匹配这个签名对应的攻击。

可以执行命令**display ips-signature pre-defined associated**，查看设备预置了哪些关联签名。然后再执行命令**display ips-signature** *ips-signature-id*，通过ID查看签名的详细信息，包括命中签名次数的阈值、命中统计时间范围、基于源地址还是目的地址统计等参数。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 进入入侵防御配置文件视图。

profile type ips name *name*

步骤3 **可选:** 配置关联检测功能。

```
assoc-check enable
```

缺省情况下，已经开启关联检测功能。

----结束

6.9 查看威胁日志并调整配置

设备对匹配安全策略的流量进行入侵检测，如果检测到入侵行为，则按照入侵防御配置文件中的动作处理数据流并生成威胁日志。管理员要经常分析日志了解网络中的攻击，不断调整配置使设备达到最佳防御效果并减少不必要的日志。

以下是一条威胁日志，从日志中既可以获取到流量的地址、协议等基本信息，还可以获取到攻击签名、响应动作等信息：

```
IPS/4/DETECT(l):An intrusion was detected. (SyslogId=2, VSys="public",Policy="policy1", SrcIp=192.168.1.2,
DstIp=192.168.0.2, SrcPort=80,
DstPort=53319,SrcZone=untrust, DstZone=trust, Protocol=TCP, Application="HTTP",Profile="default",
SignName="Microsoft Internet Explorer CVE-2014-1815 Use After Free",SignId=263490, EventNum=1,
Target=client, Severity=high, Os=windows,
Category=Code-execution, Reference=CVE-2013-1234, Action=Alert)
```

说明

此处以DETECT威胁日志为例进行介绍，其他威胁日志的详细介绍请参见《日志参考》中IPS模块的日志。

有一些威胁还会存在相应的CVE（Common Vulnerabilities and Exposures）、BID（Bugtraq ID）或CNNVD（China National Vulnerability Database of Information Security）编号，管理员可以访问**https://cve.mitre.org/**或**https://www.cnnvd.org.cn/**网站，通过查询CVE、BID或CNNVD编号，进一步了解该威胁的详细信息。

说明

CNNVD兼容性是指通过使用CNNVD标识，在各类安全工具、漏洞数据存储库及信息安全服务之间，以及与其他漏洞披露平台之间，实现漏洞信息交叉关联的方式。通过CNNVD兼容性服务的信息安全产品/服务，其漏洞信息拥有统一的规范性命名与标准化描述，提高和加强了信息安全行业漏洞信息资源的共享与服务能力。

无论管理员配置入侵防御时使用了缺省入侵防御配置文件，还是自行配置的入侵防御配置文件，入侵防御的配置都不是一蹴而就的。管理员需要持续监控日志，分析网络中的攻击类型、攻击源、受攻击目标等，并采取适当措施处理威胁事件或调整配置。

1. **圈定集中发生、日志量大的攻击日志，及时采取措施阻断攻击源。**

   结合日志中的IP地址、攻击类型等发现异常点。 例如：查看日志发现大量威胁日志的源IP都是一个外网IP地址，但又不是正常业务需求，可以在安全策略中禁止这个IP的流量。如果某个内网PC或服务器地址的日志很多，说明内网机器很可能被入侵，建议断网隔离并杀毒。

2. **进一步了解攻击的详细信息，分析攻击的影响。**

   日志信息中已经包含签名ID、协议、应用、攻击类型等信息，管理员还可以访问华为安全中心（**isecurity.huawei.com**）查看处理建议等更进一步的信息。

   在华为安全中心选择“知识库查询 > IPS威胁百科”，查询的签名信息如下，信息中包含针对此攻击的处理建议。

根据签名的信息，常用判断方法如下：

- **判断是否误报：**根据攻击类型和受攻击目标实际运行的业务判断是否误报。例如：发现很多攻击类型为SQL注入的攻击，而被攻击的目标服务器上并没有运行SQL数据库，此时SQL注入攻击是误报的。或者判断为攻击的事件就是企业正常要使用的业务，此时也相当于误报，例如，企业内部的一些安全扫描软件会被检测为攻击。此类攻击不需要检测。
- **根据签名的处理建议信息进行加固或升级：**某些类型的攻击是由于系统漏洞造成的，例如：很多针对操作系统、软件的攻击数据库的攻击都是因为系统加固不到位，此时执行安装补丁或升级软件等系统加固操作。
- **判断高危攻击：**木马、信息泄露等高危攻击，需要立即阻断。
- **不确定如何处理的攻击**：有些攻击无法确认阻断流量是否影响业务，可以持续监控。

3. **按以上步骤持续监控威胁日志并调整配置。**

   通过持续监控日志，管理员将掌握当前网络中需要防御的协议类型、应用类型和攻击类型。此时管理员可以有针对地**6.6.2 手动创建入侵防御配置文件**，只防御筛选出的签名。

   手动创建入侵防御配置文件后，仍需要继续监控日志，按需调整配置：

   - 对于误报的攻击，主要可以采取的措施如下：

     如果存在针对某类操作系统或业务的大量误报，例如：有很多对Linux操作系统的攻击但是网络中没Linux操作系统的机器，可以检查入侵防御配置文件中签名过滤器是否过滤了Linux操作系统的签名，如果是可以取消这个过滤条件。

     如果集中存在某个签名的攻击误报，可以在入侵防御配置文件中将此签名配置为例外签名，设置签名动作为放行。也可以全局禁用这个签名。

     ```
     [Device] profile type ips name profile_ips
     [Device-profile-ips-profile_profile_ips] exception ips-signature-id id action allow
     ```

     如果误报的IP地址固定，例如：安装了安全扫描软件的机器被检测为攻击，可以直接配置对这些IP的流量不进行检测（引用入侵防御配置文件的安全策略中排除对应IP地址）。
   - 由于系统漏洞造成的攻击，在主机上开启杀毒软件，并安装补丁或升级软件。
   - 对于高危攻击，确保及时阻断流量。一般此类签名的缺省动作就是阻断，如果发现日志中响应动作是告警，在不影响业务的基础上配置例外签名，设置动作为阻断或加入黑名单。

- 对于不清楚攻击源，也不清楚如果阻断是否影响业务的攻击，可以保持动作为告警，持续观察，明确后再处理。
- 如果日常发现某些正常业务受影响，也需要反查威胁日志，看被影响的业务类型是否在日志中有记录，从而进一步调整入侵防御配置文件的配置。

6.10 举例：配置入侵防御

组网需求

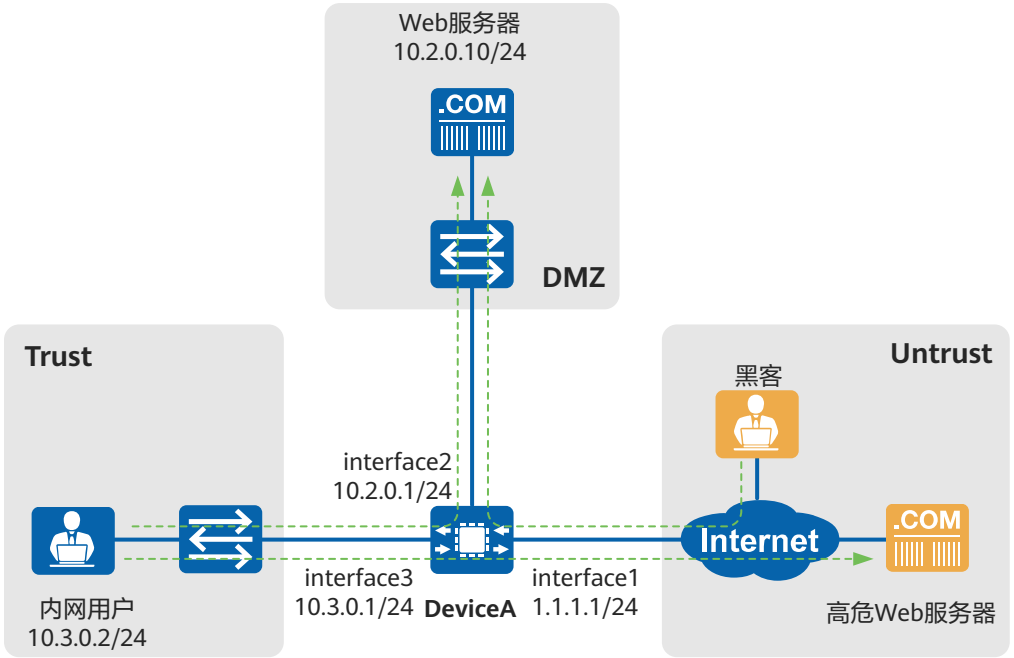
如图6-6所示，某企业在网络边界处部署DeviceA作为安全网关。在该组网中：

- 内网用户可以访问Internet的Web服务器。
- 内网的Web服务器向内网用户和Internet用户同时提供服务。

图 6-6 入侵防御组网图

说明

本例中interface1、interface2、interface3分别代表10GE0/0/1、10GE0/0/2、10GE0/0/3。



该企业需要在DeviceA上配置入侵防御功能，具体要求如下：

- 保护内网用户
  避免内网用户访问Internet的Web服务器时受到攻击。例如，Web网站含有恶意代码。
- 保护内部网络的Web服务器
  防范Internet用户和内网用户对内部网络的Web服务器发起攻击。

配置思路

1. 配置接口IP地址和安全区域，完成网络基本参数配置。
2. 创建安全策略policy_sec_1，并引用缺省的入侵防御配置文件default，保护内网用户免受来自Internet的攻击。
3. 创建安全策略policy_sec_2，并引用缺省的入侵防御配置文件web_server，保护内网Web服务器免受来自内网用户和Internet的攻击。

操作步骤

步骤1 配置接口IP地址和安全区域，完成网络基本参数配置。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-10GE0/0/1] quit
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] ip address 10.2.0.1 255.255.255.0
[DeviceA-10GE0/0/2] quit
[DeviceA] interface 10ge 0/0/3
[DeviceA-10GE0/0/3] ip address 10.3.0.1 255.255.255.0
[DeviceA-10GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/3
[DeviceA-zone-trust] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface 10ge 0/0/2
[DeviceA-zone-dmz] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface 10ge 0/0/1
[DeviceA-zone-untrust] quit
```

步骤2 配置Trust区域和Untrust区域之间的安全策略，引用入侵防御配置文件default。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_1] profile ips default
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] quit
```

步骤3 配置从Trust区域到DMZ区域、从Untrust区域到DMZ区域的安全策略，引用入侵防御配置文件web_server。

```
[DeviceA-policy-security] rule name policy_sec_2
[DeviceA-policy-security-rule-policy_sec_2] source-zone trust untrust
[DeviceA-policy-security-rule-policy_sec_2] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_2] destination-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sec_2] profile ips web_server
[DeviceA-policy-security-rule-policy_sec_2] action permit
[DeviceA-policy-security-rule-policy_sec_2] quit
[DeviceA-policy-security] quit
```

步骤4 保存配置信息，以便设备下次启动时自动加载上述配置信息。

```
[DeviceA] quit
<DeviceA> save
```

----结束

检查配置结果

- 当发生攻击事件时，访问连接被阻断，并且在设备上可以查看到IPS模块的威胁日志。

- 执行**display ips statistics**命令可以查看入侵防御的统计信息。

配置脚本

```
#
sysname DeviceA
#
interface 10GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface 10GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
 add interface 10GE0/0/3
#
firewall zone untrust
 add interface 10GE0/0/1
#
firewall zone dmz
 add interface 10GE0/0/2
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 24
  profile ips default
  action permit
 rule name policy_sec_2
  source-zone trust
  source-zone untrust
  destination-zone dmz
  destination-address 10.2.0.0 24
  profile ips web_server
  action permit
```

7 反病毒（AV）配置

7.1 反病毒简介

定义

病毒是一种恶意代码，一般通过邮件或文件共享的相关协议进行传播，可感染或附着在应用程序或文件中。有些病毒会耗尽主机资源、占用网络带宽，有些病毒会控制主机权限、窃取数据，有些病毒甚至会对主机硬件造成破坏，严重威胁用户主机和网络的安全。

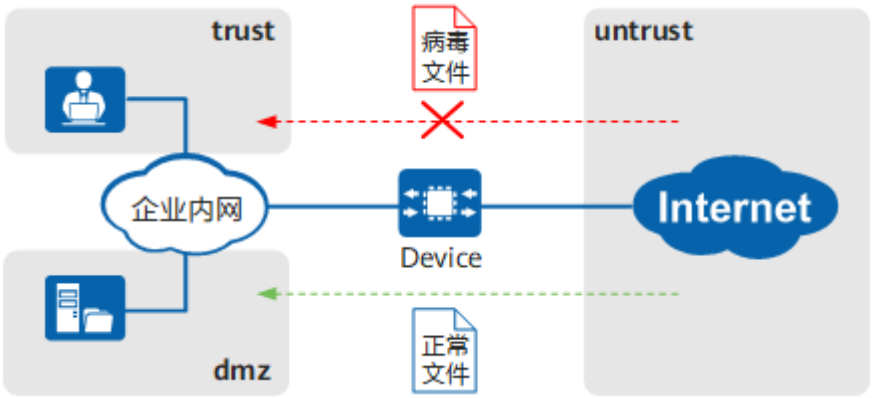
反病毒（Antivirus）是一种基于病毒特征检测和处理病毒文件的安全机制，可以有效避免病毒文件引起的数据破坏、权限更改和系统崩溃等情况的发生，保证了网络的安全。

目的

随着网络技术的不断发展，企业用户越来越频繁地在网络上传输、下载和共享文件，随之而来的病毒威胁也越来越大。

如**图7-1**所示，内网用户经常需要访问外网并从外网下载文件，同时，内网部署的服务器也经常会接收到外网用户上传的文件。将设备部署在企业网络的入口处并配置反病毒功能后，设备会放行正常文件进入内部网络，并通过阻断、告警等手段对检测出的病毒文件进行干预或提醒。

图 7-1 反病毒示意图



受益

反病毒特性凭借庞大且不断更新的病毒特征库有效保护内网用户和服务器免受病毒文件侵害，保护网络安全。

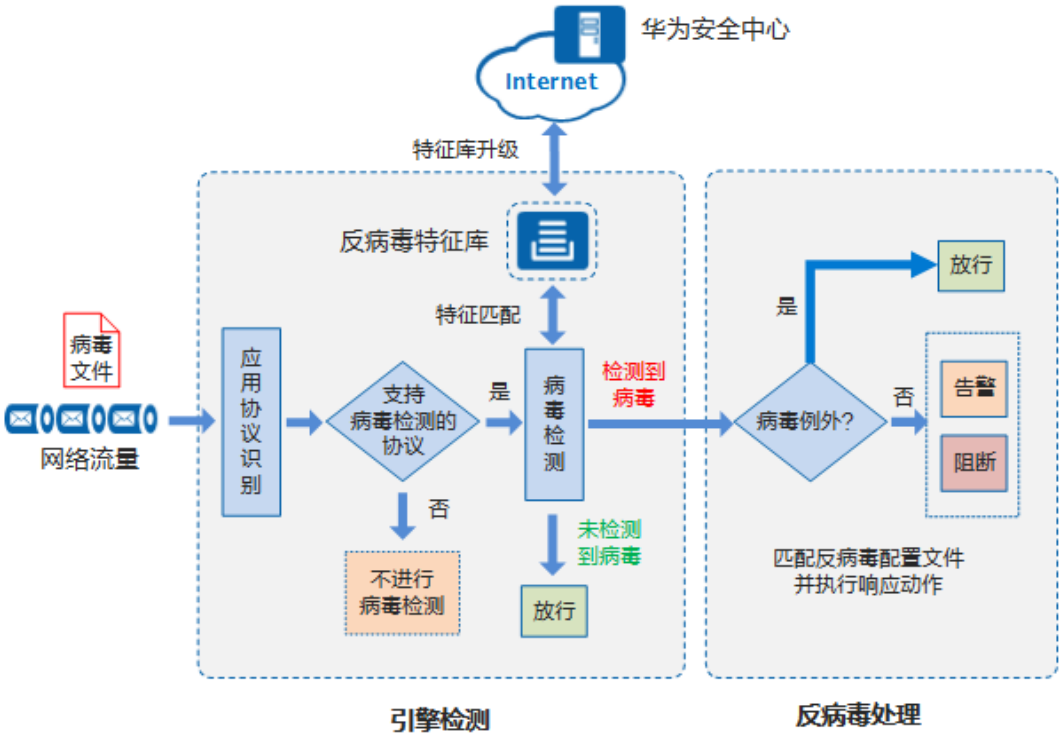
此外，设备上配置的反病毒功能和用户主机上安装的防病毒软件在功能上协作互补，由于部署位置和所用的特征库不同，二者同时使用可以更有力的保障用户主机和网络的安全。

7.2 反病毒原理描述

7.2.1 反病毒处理流程

如图7-2所示，反病毒的处理流程主要包括自适应安全引擎（Adaptive Security Engine，以下简称ASE）检测和反病毒处理两部分。其中，ASE检测部分需要先对流量中包含的应用协议进行识别，并对支持病毒检测的协议类型的流量进行检测。

图 7-2 反病毒处理流程



1. **应用协议识别**

   反病毒特性的病毒检测能力是依靠自适应安全引擎来实现的。流量进入引擎后，会先进行深层分析，识别出流量的协议类型和文件传输的方向。引擎根据反病毒配置文件中定义的各协议类型在不同传输方向上的病毒检测功能开启情况，判断在当前文件传输方向上文件传输所使用的协议类型是否支持病毒检测，支持病毒检测的流量将被送往病毒检测模块。

   - 设备支持对使用以下协议传输的文件进行病毒检测：FTP、HTTP、POP3、SMTP、IMAP、NFS、SMB。
   - 设备支持对上传和下载两个传输方向上的文件进行病毒检测。其中，上传是指客户端向服务器发送文件；下载是指服务器向客户端发送文件。

2. **病毒检测**

   设备对支持病毒检测的文件进行特征提取，并将提取后的特征与病毒特征库中的特征进行匹配。如果特征匹配，则判定该文件为病毒文件，并送往反病毒处理模块进行处理；如果特征不匹配，则直接放行该文件。

   病毒特征库中包含了网络中常见病毒文件的特征信息，供反病毒特性进行病毒检测时使用。通过定期升级设备的病毒特征库，可以有效提升设备对新型病毒的检测能力，详细信息请参见**7.5 升级反病毒特征库**。

3. **响应处理**

   设备检测出传输的文件为病毒文件后，会根据反病毒配置文件中的配置进行如下处理：

   a. 判断该病毒文件是否命中病毒例外。如果是病毒例外，则允许该文件通过。

      为了避免由于系统误报等原因造成文件传输失败等情况的发生，当用户认为已检测到的某个病毒为误报时，可以将该病毒对应的病毒名称添加到病毒例外，使该病毒规则失效。如果检测结果命中了病毒例外，则该文件的响应动作为放行。

b. 如果不是病毒例外，则按照配置文件中配置的响应动作进行处理。

- 告警：允许病毒文件通过，同时生成病毒日志。
- 阻断：禁止病毒文件通过，同时生成病毒日志。

7.2.2 反病毒配置文件

反病毒配置文件用于决定设备对哪些协议和哪些文件类型的流量进行病毒检测，以及对检测出的病毒文件执行何种处理动作。

缺省反病毒配置文件

为了便于管理员使用，设备缺省提供了满足常见场景的反病毒配置文件，名称为**default**。缺省配置文件中定义了每种协议在上传或下载方向上的缺省动作，如表7-1所示。缺省配置文件不能被修改和删除。

表 7-1 缺省反病毒配置文件

名称	协议	上传方向的病毒检测	下载方向的病毒检测	缺省的动作
default	HTTP	开启	开启	阻断
	FTP	开启	开启	阻断
	SMTP	开启	-	告警
	POP3	-	开启	告警
	IMAP	开启	开启	告警
	NFS	开启	开启	告警
	SMB	开启	开启	阻断
检测文件类型：OFFICE、PE、ELF、SCRIPT、EICAR、EML、FLASH、PDF、RTF、MACOS、JAR、APK、ARCHIVE。 病毒例外：未配置				

说明

通过命令**display profile type av name default**可以查看到反病毒缺省配置文件中的配置信息。

自定义反病毒配置文件

管理员可根据实际网络和业务情况，配置自定义反病毒配置文件筛选关注的协议和文件类型。自定义反病毒配置文件支持的配置项如表7-2所示。

表 7-2 自定义反病毒配置文件

名称	协议	说明	缺省情况
支持检测的协议	HTTP	方向：支持上传和下载方向的协议检测。 动作：支持阻断和告警的处理动作。	缺省情况下，开启上传和下载方向的HTTP协议检测功能，动作为阻断。
	FTP	方向：支持上传和下载方向的协议检测。 动作：支持阻断和告警的处理动作。	缺省情况下，开启上传和下载方向的FTP协议检测功能，动作是阻断。
	SMTP	方向：仅支持上传的协议检测。 动作：仅支持告警的处理动作。	缺省情况下，开启上传方向的SMTP协议检测功能，动作是告警。
	POP3	方向：仅支持下载的协议检测。 动作：仅支持告警的处理动作。	缺省情况下，开启下载方向的POP3协议检测功能，动作是告警。
	MAP	方向：支持上传和下载方向的协议检测。 动作：仅支持告警的处理动作。	缺省情况下，开启上传和下载方向的IMAP协议检测功能，动作是告警。
	NFS	方向：支持上传和下载方向的协议检测。 动作：仅支持告警的处理动作。	缺省情况下，开启上传和下载方向的NFS协议检测功能，动作是告警。
	SMB	方向：支持上传和下载方向的协议检测。 动作：支持阻断和告警的处理动作。	缺省情况下，开启上传和下载方向的SMB协议检测功能，动作是阻断。
支持检测的文件类型	-	基于特征库的反病毒支持检测的文件类型：OFFICE、PE、ELF、SCRIPT、EICAR、EML、FLASH、PDF、RTF、MACOS、JAR、APK、ARCHIVE、WEB、IMAGE、VIDEO、AUDIO、OTHER。	缺省情况下，基于特征库的反病毒支持检测的文件类型包括OFFICE、PE、ELF、SCRIPT、EICAR、EML、FLASH、PDF、RTF、MACOS、JAR、APK、ARCHIVE。
病毒例外	-	当用户认为已检测到的某个病毒为误报时，可以将该病毒添加到病毒例外，设备会对该文件流量直接放行。	缺省情况下，未配置病毒例外。

应用反病毒配置文件

需要在安全策略中引用反病毒配置文件，反病毒功能才生效。设备会对符合安全策略匹配条件的流量进行反病毒处理。

由于协议的连接请求均由客户端发起，为了使连接可以成功建立，引用反病毒配置文件的安全策略的方向应该是访问发起的方向（源安全区域需要配置为客户端所在的安全区域；目的安全区域需要配置为服务器所在的安全区域）。

例如：保护企业内网PC免受病毒威胁，虽然病毒文件的传输方向是从外网到内网，但是因为发起访问的方向是从内网到外网，因此反病毒配置文件需要应用到内网访问外网的安全策略中，具体配置如表7-3所示。

表 7-3 保护内网 PC 的安全策略

源安全区域	源地址	目的安全区域	目的地址	动作	反病毒配置文件
内网trust区域	PC所在的内网网段	外网untrust区域	any	允许	应用缺省反病毒配置文件 **default**

如果保护的是企业内网服务器，由于发起访问的方向是从外网到内网，此时发起访问的方向与病毒文件的传输方向一致，反病毒配置文件需要应用到外网访问内网的安全策略中，具体配置如表7-4所示。

表 7-4 保护内网服务器的安全策略

源安全区域	源地址	目的安全区域	目的地址	动作	反病毒配置文件
外网untrust区域	any	内网dmz区域	服务器所在的内网网段	允许	应用缺省反病毒配置文件 **default**

7.3 反病毒（AV）配置注意事项

License 依赖

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

硬件依赖

表 7-5 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1

系列	支持产品
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 7-6 本特性的使用限制

特性限制	系列	涉及产品
设备使用反病毒功能对流量进行内容安全检测时，会对整机的性能有一定的影响，请根据实际需求有选择性的进行配置。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
设备部署在两台路由设备间，且两台路由设备通过BFD互相探测时，网络如果产生偶发性拥塞会导致BFD震荡。BFD震荡会消耗链路资源。建议将路由设备上的BFD检测时间适当调大（建议大于100ms）。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
针对不包含数据的FTP协议的FIN报文，反病毒检测不能阻断，仅可告警。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
当前反病毒功能仅能在流模式生效，会阻断最后一个报文，大部分可执行病毒文件会因缺失最后一个报文的内容，导致病毒文件不可执行。使用FTP传输文件且最后一个fin报文不带数据报文时，可能导致文件传输成功。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

7.4 反病毒缺省配置

反病毒的缺省配置如表7-7所示。

表 7-7 反病毒缺省配置

参数	缺省配置
反病毒功能	未开启
反病毒配置文件	参见缺省反病毒配置文件
反病毒日志发送功能	开启
反病毒日志归并功能	开启
全类型文件检测功能	关闭
反病毒特征库	未加载

7.5 升级反病毒特征库

前提条件

- 特征库升级前准备请参见《配置指南-系统管理配置-特征库升级配置》中的“特征库升级前准备”。
- 通过在线升级的方式升级反病毒特征库前，需要先配置设备与华为安全中心通信，详细配置请参见《配置指南-系统管理配置-特征库升级配置-配置特征库在线升级》中的“配置设备与华为安全中心通信”。

背景信息

华为安全中心（isecurity.huawei.com）定期发布反病毒特征库，及时将设备的反病毒特征库升级到最新版本，可以有效提升对病毒的检测能力和检测效率。

此处仅提供了特征库在线升级的基本步骤，特征库离线升级及其他特征库升级的相关信息请参见《配置指南-系统管理配置》中的“特征库升级配置”。

操作步骤

步骤1 配置DNS服务器，确保设备可以正确解析安全中心域名。

```
system-view
dns resolve
dns server ip-address
```

步骤2 手动立即升级反病毒特征库到最新版本。

```
update online av-sdb
```

命令下发后，设备会立即查询、下载特征库并将特征库升级到最新版本。

步骤3 配置定时升级反病毒特征库功能。

1. 开启定时升级功能
   update schedule av-sdb enable
2. 配置定时升级时间
   update schedule av-sdb { **hourly** *minute* | { **daily** | **weekly** { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } } *time* }

   反病毒特征库定时升级功能缺省开启，设备在22：00～08：00之间随机选择一个时间作为反病毒特征库每天进行定时升级的时间，可以手动进行配置。

   建议反病毒特征库每天升级一次，请根据网络的实际情况进行调整。

----结束

检查配置结果

- 执行**display update configuration**命令，查看特征库升级的配置信息，检查配置是否有误。
- 特征库升级完成后，执行**display engine information**命令，查看ASE引擎的运行状态和特征库的版本信息，确认特征库已升级到最新版本。

7.6 配置反病毒

前提条件

通过**7.5 升级反病毒特征库**，获取最新的病毒特征信息。

背景信息

设备存在一个缺省的反病毒配置文件**default**，也可以创建自定义反病毒配置文件，然后在安全策略中引用反病毒配置文件即可。

操作步骤

步骤1 进入系统视图。
system-view

步骤2 （可选）配置设备的业务性能模式。
forward performance mode { **routing** | **security** }

当设备业务性能模式处于路由模式时，设备的安全业务处理性能较低，建议将设备业务性能模式切换到安全模式。用户可通过命令**display forward performance mode**查看设备当前的业务性能模式。

设备业务性能模式缺省情况如下：

- 对于AR5700系列和AR6700系列：缺省情况下，设备业务性能模式处于安全模式。
- 对于AR8000系列：缺省情况下，设备业务性能模式处于路由模式。

步骤3 配置每个CPU上的每个ASE业务进程同时在检的最大文件数和ASE检测的单个文件大小的最大值。
av full-scan-mode { **max-file-number** *max-number*-value | **max-file-size** *max-size-value* }

步骤4 配置自定义反病毒配置文件。

1. 创建自定义反病毒配置文件。
   profile type av name *name*
2. 配置反病毒文件检测类型。
   file-type av { **items** *file-type-name* &<1-18> | **all** }
   缺省情况下，反病毒默认文件检测类型为OFFICE、PE、ELF、SCRIPT、EICAR、EML、FLASH、PDF、RTF、MACOS、JAR、APK、ARCHIVE。
3. 配置检测协议。

协议	命令	缺省情况
HTTP	**http-detect enable** **http-detect** { **direction** { **upload** | **download** | **both** } | **action** { **block** | **alert** } }*	缺省情况下，开启上传和下载方向的HTTP协议检测功能，动作为阻断。
FTP	**ftp-detect enable** **ftp-detect** { **direction** { **upload** | **download** | **both** } | **action** { **block** | **alert** } }*	缺省情况下，开启上传和下载方向的FTP协议检测功能，动作是阻断。
SMTP	**smtp-detect enable** **undo smtp-detect enable**	缺省情况下，开启上传方向的SMTP协议检测功能，动作是告警。
POP3	**pop3-detect enable** **undo pop3-detect enable**	缺省情况下，开启下载方向的POP3协议检测功能，动作是告警。
IMAP	**imap-detect enable** **imap-detect direction** { **upload** | **download** | **both** }*	缺省情况下，开启上传和下载方向的IMAP协议检测功能，动作是告警。
NFS	**nfs-detect enable** **nfs-detect direction** { **upload** | **download** | **both** }*	缺省情况下，开启上传和下载方向的NFS协议检测功能，动作是告警。
SMB	**smb-detect enable** **smb-detect** { **direction** { **upload** | **download** | **both** } | **action** { **block** | **alert** } }*	缺省情况下，开启上传和下载方向的SMB协议检测功能，动作是阻断。

   协议具体支持的检测方向和处理动作，请参见**表2 自定义反病毒配置文件**。
4. **可选:** 配置病毒例外。
   exception av-signature-name *av-signature-name*
5. 返回系统视图。
   quit

步骤5 提交配置。

engine configuration commit

修改反病毒相关配置后，配置内容不会立即生效，需要执行提交操作来激活。

步骤6 进入安全策略视图。

```
security-policy
```

步骤7 创建安全策略规则，并进入安全策略规则视图。

```
rule name rule-name
```

步骤8 在安全策略中引用反病毒配置文件。

```
profile av profile-name
```

通过命令行配置安全策略引用配置文件时，需要输入完整的配置文件名称，否则配置文件无法成功引用。

此处仅体现了在安全策略中引用缺省反病毒配置文件的配置步骤，安全策略的其他匹配条件未具体给出，具体配置请参见《配置指南-安全配置》中的《安全策略配置》。

步骤9 配置安全策略规则的动作。

```
action permit
quit
```

----结束

7.7 查看病毒威胁日志

背景信息

在安全策略中引用反病毒配置文件后，设备对匹配安全策略的流量进行病毒检测，如果检测到流量中带有病毒，会生成病毒威胁日志。通过查看病毒威胁日志，可以了解病毒的基本信息，便于进一步部署相关防护动作。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启反病毒模块的日志发送功能。

```
engine log av enable
```

缺省情况下，系统开启反病毒模块的日志发送功能。

步骤3 **可选:** 开启反病毒日志归并功能。

```
av log merge enable
```

缺省情况下，系统开启反病毒日志归并功能。

开启反病毒日志归并功能后，当短时间内产生多条相同的反病毒日志时，系统会将多条日志归并成一条进行输出。

----结束

任务示例

从日志信息中既可以获取到流量的地址、协议等基本信息，还可以获取到病毒名称、病毒文件类型以及病毒文件名称等信息。

以下是一条基于反病毒特征库的反病毒功能检测出的病毒威胁日志：

```
AV/4/VIRUS(l):CID=0x814f0421;A virus was detected. (SyslogId=1, VSys="public", Policy="policy1",
SrcIp=192.168.1.2, DstIp=192.168.0.2, SrcPort=21, DstPort=53038, SrcZone=untrust, DstZone=trust,
```

```
User="unknown", Protocol=TCP, Application="FTP", Profile="default", EventNum=1, SignatureId=16424404,
VirusName="EICAR.Test.FILE.1", DetectionType="full-scan virus detect", Direction=download,
FileName="eicar.com", FileType="eicar", Action=Block, Hash="267D772D8ED87333", Severity="high")
```

后续处理

执行**display av-signature database**命令，查看支持检测的病毒。

7.8 举例：配置反病毒

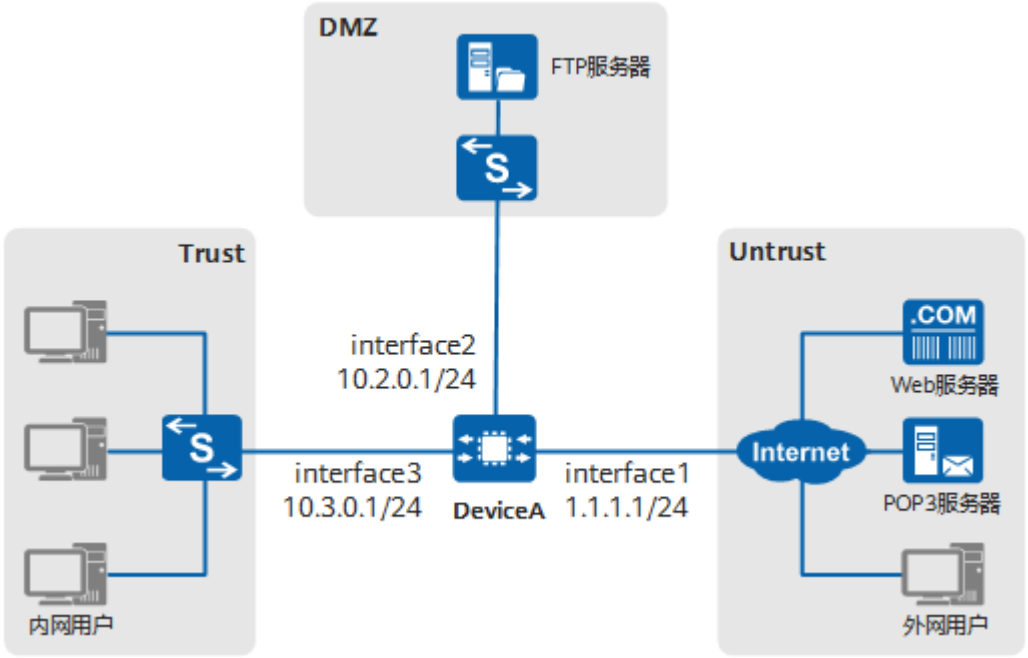
组网需求

如图7-3所示，某企业在网络边界处部署了DeviceA。内网用户可以通过Web服务器和POP3服务器下载文件和邮件，内网FTP服务器需要接收外网用户上传的文件。公司利用设备提供的反病毒功能阻止病毒文件进入受保护网络，保障内网用户和服务器的安全。其中，内网用户在通过Web服务器下载某重要软件时失败，排查发现该软件因被设备判定为病毒而被阻断（病毒ID为16424404），考虑到该软件的重要性和对该软件来源的信任，管理员决定临时放行该类病毒文件，以使用户可以成功下载该软件。

图 7-3 反病毒组网图

说明

本例中interface1，interface2和interface3分别代表10GE0/0/1，10GE0/0/2和10GE0/0/3。



配置思路

1. 配置接口IP地址和安全区域，完成网络基本参数配置。
2. 配置反病毒配置文件。
   - 配置反病毒配置文件profile_http_pop3，针对HTTP和POP3协议设置匹配条件和响应动作，并检测所有支持的文件类型，在该配置文件中配置病毒ID为16424404的病毒例外。

- 配置反病毒配置文件profile_ftp，针对FTP协议设置匹配条件和响应动作，并检测所有支持的文件类型。

3. 配置安全策略，在trust到untrust和untrust到dmz方向分别引用反病毒配置文件。
   - 配置安全策略policy_sec_1，在trust到untrust方向上引用反病毒配置文件profile_http_pop3，对内网用户从Internet下载的文件和邮件进行病毒检测和防护。
   - 配置安全策略policy_sec_2，在dmz到untrust方向上引用反病毒配置文件profile_ftp，对内网FTP服务器从Internet接收到的文件进行病毒检测和防护。

操作步骤

步骤1 配置接口IP地址和安全区域，完成网络基本参数配置。

1. 配置10GE0/0/1接口IP地址，将接口加入untrust域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] undo portswitch
[DeviceA-10GE0/0/1] ip address 1.1.1.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface 10ge 0/0/1
[DeviceA-zone-untrust] quit
```

2. 配置10GE0/0/2接口IP地址，将接口加入dmz域。

```
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] undo portswitch
[DeviceA-10GE0/0/2] ip address 10.2.0.1 24
[DeviceA-10GE0/0/2] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface 10ge 0/0/2
[DeviceA-zone-dmz] quit
```

3. 配置10GE0/0/3接口IP地址，将接口加入trust域。

```
[DeviceA] interface 10ge 0/0/3
[DeviceA-10GE0/0/3] undo portswitch
[DeviceA-10GE0/0/3] ip address 10.3.0.1 24
[DeviceA-10GE0/0/3] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/3
[DeviceA-zone-trust] quit
```

步骤2 配置反病毒配置文件。

1. 配置针对HTTP和POP3协议的反病毒配置文件，并在该配置文件中配置病毒ID为16424404的病毒例外。由于该反病毒配置文件只针对HTTP和POP3协议进行病毒检测，因此关闭其他协议的病毒检测功能。

```
[DeviceA] profile type av name profile_http_pop3
[DeviceA-profile-av-profile_http_pop3] http-detect direction download action block
[DeviceA-profile-av-profile_http_pop3] pop3-detect enable
[DeviceA-profile-av-profile_http_pop3] file-type av all
[DeviceA-profile-av-profile_http_pop3] exception av-signature-id 16424404
[DeviceA-profile-av-profile_http_pop3] undo ftp-detect enable
[DeviceA-profile-av-profile_http_pop3] undo smtp-detect enable
[DeviceA-profile-av-profile_http_pop3] undo imap-detect enable
[DeviceA-profile-av-profile_http_pop3] undo nfs-detect enable
[DeviceA-profile-av-profile_http_pop3] undo smb-detect enable
[DeviceA-profile-av-profile_http_pop3] quit
```

2. 配置针对FTP协议的反病毒配置文件。由于该反病毒配置文件只针对FTP协议进行病毒检测，因此同时关闭其他协议的病毒检测功能。

```
[DeviceA] profile type av name profile_ftp
[DeviceA-profile-av-profile_http_pop3] ftp-detect direction upload action block
```



```
[DeviceA-profile-av-profile_http_pop3] file-type av all
[DeviceA-profile-av-profile_http_pop3] undo http-detect enable
[DeviceA-profile-av-profile_http_pop3] undo smtp-detect enable
[DeviceA-profile-av-profile_http_pop3] undo pop3-detect enable
[DeviceA-profile-av-profile_http_pop3] undo imap-detect enable
[DeviceA-profile-av-profile_http_pop3] undo nfs-detect enable
[DeviceA-profile-av-profile_http_pop3] undo smb-detect enable
[DeviceA-profile-av-profile_http_pop3] quit
```

步骤3 配置安全策略。

1. 配置trust到untrust方向上的安全策略，引用缺省的反病毒配置文件default。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_1
[DeviceA-policy-security-rule-policy_sec_1] source-zone trust
[DeviceA-policy-security-rule-policy_sec_1] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_1] source-address 10.3.0.0 24
[DeviceA-policy-security-rule-policy_sec_1] action permit
[DeviceA-policy-security-rule-policy_sec_1] profile av profile_http_pop3
[DeviceA-policy-security-rule-policy_sec_1] quit
```

2. 配置dmz到untrust方向上的安全策略，引用缺省的反病毒配置文件default。

```
[DeviceA-policy-security] rule name policy_sec_2
[DeviceA-policy-security-rule-policy_sec_2] source-zone dmz
[DeviceA-policy-security-rule-policy_sec_2] destination-zone untrust
[DeviceA-policy-security-rule-policy_sec_2] source-address 10.2.0.0 24
[DeviceA-policy-security-rule-policy_sec_2] action permit
[DeviceA-policy-security-rule-policy_sec_2] profile av profile_ftp
[DeviceA-policy-security-rule-policy_sec_2] quit
[DeviceA-policy-security] quit
```

步骤4 在系统视图下提交配置。

```
[DeviceA] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: URL submitted configurations successfully.
Info: Finish committing engine compiling.
```

步骤5 保存配置信息，以便设备下次启动时自动加载上述配置信息。

```
[DeviceA] quit
<DeviceA> save
```

----结束

检查配置结果

- 当内网用户通过POP3协议下载带有病毒的邮件时，设备生成病毒威胁日志。
- 当外网用户通过FTP协议上传带有病毒的文件时，上传连接被阻断，设备生成病毒威胁日志。
- 执行**display file-frame statistics** [**slot** *slot-id* **cpu** *cpu-id*]命令可以查看反病毒相关的统计信息。

配置脚本

```
#
sysname DeviceA
#
interface 10GE0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.2.0.1 255.255.255.0
#
interface 10GE0/0/3
 ip address 10.3.0.1 255.255.255.0
#
```



```
firewall zone trust
 add interface 10GE0/0/3
#
firewall zone untrust
 add interface 10GE0/0/1
#
firewall zone dmz
 add interface 10GE0/0/2
#
profile type av name profile_http_pop3
 file-type av all
 http-detect direction download action block
 undo ftp-detect enable
 undo smtp-detect enable
 pop3-detect enable
 undo imap-detect enable
 undo nfs-detect enable
 undo smb-detect enable
 exception av-signature-id 16424404
profile type av name profile_ftp
 file-type av all
 undo http-detect enable
 ftp-detect direction upload action block
 undo smtp-detect enable
 undo pop3-detect enable
 undo imap-detect enable
 undo nfs-detect enable
 undo smb-detect enable
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  source-address 10.3.0.0 mask 255.255.255.0
  profile av profile_http_pop3
  action permit
 rule name policy_sec_2
  source-zone untrust
  destination-zone dmz
  source-address 10.2.0.0 mask 255.255.255.0
  profile av profile_ftp
  action permit
```

7.9 维护反病毒

查看配置信息

表 7-8 查看配置信息

操作	命令
查看每个CPU上的每个ASE进程同时在检的最大文件数和单个文件大小的最大值	**display av full-scan-mode** { **max-file-number** | **max-file-size** }
查看支持检测的病毒家族	**display av-signature database**
查看反病毒配置文件的信息	**display profile type av** [**name** *name*]

查看统计信息

表 7-9 查看统计信息

操作	命令
查看文件框架统计信息	**display file-frame statistics** [**slot** *slot-id* **cpu** *cpu-id*]

清除统计信息

表 7-10 清除统计信息

操作	命令
清除文件框架统计信息	**reset file-frame statistics**

8 本机防攻击配置

8.1 本机防攻击简介

定义

本机防攻击是为了保证CPU对正常业务的处理而设计的一种CPU保护机制。网络中存在着大量需要正常上送CPU的报文和针对CPU（Central Processing Unit）的恶意攻击报文。

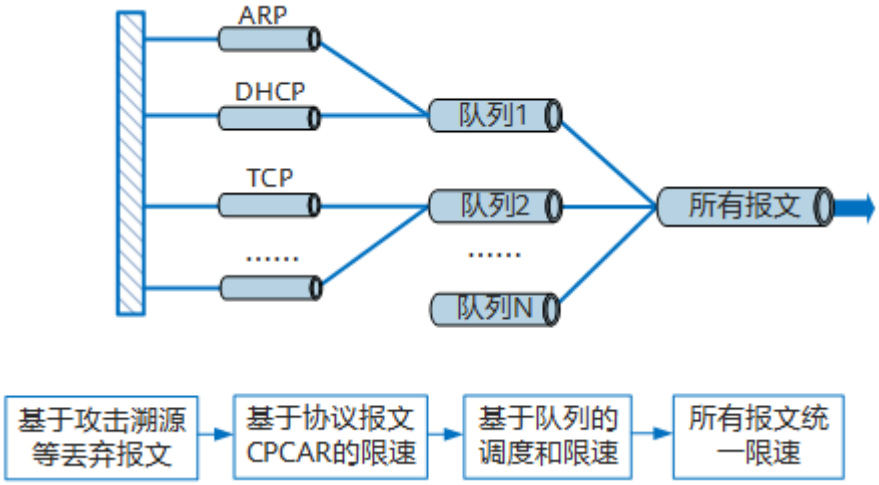
- 如果正常上送CPU的报文如果数量巨大，会导致CPU占用率过高，设备性能下降，从而影响业务正常运行。
- 如果CPU长时间繁忙的处理恶意攻击报文，会导致其他业务中断甚至系统中断。

基于上面两种情况考虑，设备提供了本机防攻击功能。当CPU接收的正常业务报文或恶意攻击报文数量较多时，确保CPU能够正常运行，从而保证业务的正常运行。

功能简介

本机防攻击的基本功能包括CPU防攻击、用户级限速、攻击溯源和攻击防范等。如图8-1所示，本机防攻击通过多级安全机制，实现对设备的分级保护。

图 8-1 本机防攻击的防护分级



第一级：通过攻击溯源惩罚丢弃功能等直接丢弃上送CPU的恶意报文。

第二级：基于协议报文CPCAR（Control Plane Committed Access Rate）的限速。对上送CPU的报文按照协议类型进行速率限制，保证每种协议上送CPU的报文不会过多。

控制CPCAR是CPU防攻击的核心部分。CPCAR是基于设备对协议报文进行限速，用户级限速是基于发起攻击的用户MAC地址对协议报文进行限速。

第三级：基于队列的调度和限速。协议报文CPCAR限速之后，设备可对一类协议再分配一个队列，各个队列之间按照权重或优先级方式调度，在有冲突的情况下高优先级的队列优先处理。同时，可以针对每个队列进行限速，限制各个队列向CPU上送报文的最大速率。对于超过队列最大速率的协议报文，设备会直接丢弃。

第四级：所有报文统一限速。该功能是为了限制CPU处理的报文总数，保证CPU在其正常处理能力范围内尽可能多的处理报文。

在进行所有报文统一限速之前，设备支持通过分析上送CPU处理的报文的内容和行为，判断报文是否具有攻击特性，并对具有攻击特性的报文执行丢弃或限速等攻击防范措施。攻击防范主要包含畸形报文攻击防范、分片报文攻击防范、TCP SYN泛洪攻击防范、UDP泛洪攻击防范和ICMP泛洪攻击防范。

8.2 本机防攻击配置注意事项

License 依赖

本机防攻击无需License许可即可使用。

硬件依赖

表 8-1 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

无

8.3 本机防攻击缺省配置

本机防攻击的主要缺省配置如下表所示。

表 8-2 CPU 防攻击缺省配置

参数	缺省配置
防攻击策略	设备自带的一个名称为**default**的防攻击策略，并且该策略已被应用。
协议报文的CPCAR值	设备对上送CPU的报文按照**default**策略缺省的限速值进行限速，可通过命令**display cpu-defend configuration**查看。
上送到CPU的所有报文的CPCAR值	设备上送设备CPU的报文CAR速率，可通过命令**display cpu-defend configuration**查看。
协议联动功能	具体可通过命令**application-apperceive enable**查看支持的报文类型。
动态自适应调整协议报文的默认CPCAR值	具体可通过命令**cpu-defend dynamic-adjust enable**查看支持的报文类型。

表 8-3 用户级限速缺省配置

参数	缺省配置
用户级限速支持限制的报文类型	具体可通过命令**cpu-defend host-car**查看支持的报文类型。

参数	缺省配置
用户级限速功能的状态	全局和接口下的用户级限速功能均未开启。
用户级限速的限速值	10pps。

表 8-4 攻击溯源缺省配置

参数	缺省配置
攻击溯源防范的报文类型	具体可通过命令**auto-defend protocol**查看支持的报文类型。
攻击溯源功能的状态	已开启。
攻击溯源的检查阈值	缺省情况下，攻击溯源事件上报阈值为128pps。
攻击溯源的采样比	采样比为8，即每8个报文采样1个报文。
攻击溯源的溯源模式	基于源IP地址和基于源MAC地址溯源。
攻击溯源的惩罚措施	未开启。

表 8-5 畸形报文攻击防范、分片报文攻击防范、TCP SYN 泛洪攻击防范、UDP 泛洪攻击防范和 ICMP 泛洪攻击防范的缺省配置

参数	缺省配置
畸形报文攻击防范功能	已开启
分片报文攻击防范功能	已开启
分片报文限制速率	155000000bit/s
TCP Syn攻击防范功能	已开启
TCP Syn泛洪报文限制速率	155000000bit/s
UDP泛洪攻击防范功能	已开启
ICMP泛洪攻击防范功能	已开启
ICMP泛洪报文限制速率	155000000bit/s

8.4 配置 CPU 防攻击

8.4.1 了解 CPU 防攻击

CPU防攻击的核心是CPCAR。设备支持通过命令行修改CPCAR，包括协议报文的CPCAR、上送到CPU的所有报文的CPCAR以及协议联动后的CPCAR。并且，在默认CPCAR不能满足业务需求时，支持动态自适应调整协议报文的默认CPCAR。

协议联动功能

协议联动是指设备对基于会话连接的应用层数据的保护功能。当协议会话连接建立后，基于协议的默认CPCAR就不再起作用，设备以协议联动设定的CPCAR对建立会话连接的报文进行限速。通常，协议联动设定的CPCAR要比默认CPCAR大很多，以此来保证业务运行的可靠性和稳定性。

例如，FTP协议，当协议启动但没有文件传输的情况下，设备通过默认CPCAR对FTP报文进行限速；当设备进行文件传输时，设备检测到协议会话连接建立，对建立会话连接的FTP报文通过协议联动设定的CPCAR进行限速，以避免文件传输时出现报文流量瞬间激增超过默认CPCAR，导致传输失败的情况出现。

动态自适应调整协议报文的默认CPCAR值

动态自适应调整协议报文的默认CPCAR值应用在用户接入相关的协议报文上，主要解决协议报文默认CPCAR值无法满足上送速率的场景。开启该功能后，设备会根据协议报文的丢包情况和CPU占用率调整默认CPCAR值。

例如，用户通过ARP请求报文触发认证上线，当大规模用户认证的情况下，设备收到的ARP请求报文速率超过默认CPCAR值导致丢包，此时设备会根据丢包率和CPU占用率调整协议报文的CPCAR值。

8.4.2 配置 CPCAR 值

背景信息

为了减少上送CPU的报文数量，降低不同类型报文的相互影响以达到保护CPU的目的，设备支持对上送CPU的报文进行分类限速，主要分为协议报文CPCAR限速、上送CPU的所有协议报文限速和协议联动限速。

- 协议联动限速的优先级最高，如果还配置了协议报文CPCAR限速和上送CPU的所有协议报文限速，则设备以协议联动限速值为准。
- 如果没有配置协议联动限速，但同时配置了协议报文CPCAR限速和上送CPU的所有协议报文限速，则设备以二者中的最小限速值为准。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建防攻击策略并进入防攻击策略视图。

```
cpu-defend policy policy-name
```

步骤3 配置上送CPU报文的限速方式。

- 配置协议报文CPCAR限速。
  ```
  car packet-type packet-type pps pps-value
  ```
- 配置上送到CPU的所有报文的CPCAR。
  ```
  car all-packets pps pps-value
  ```
- 配置协议联动限速。

a. 开启协议联动功能。
application-apperceive { **bgp** | **bgp4plus** | **isis** | **ftp** | **ssh** | **telnet** | **tftp** | **ospf** | **ospfv3** } **enable**

b. 配置协议连接建立时协议报文的CPCAR值。
linkup-car packet-type { **bgp** | **bgp4plus** | **isis** | **ftp** | **ssh** | **telnet** | **tftp** | **ospf** | **ospfv3** } **pps** *pps-value*

c. 配置协议联动触发惩罚的比例阈值。
linkup session anti-attack ratio-threshold *rate-value-percent*

缺省情况下，触发惩罚的比例阈值为50%。

步骤4 （可选）配置丢弃上送CPU的报文。
deny packet-type *packet-type*

缺省情况下，设备不会丢弃上送CPU的报文。

步骤5 （可选）配置防攻击策略的描述信息。
description *description*

缺省情况下，防攻击策略没有配置描述信息。

步骤6 返回系统视图。
quit

步骤7 应用防攻击策略。

- 批量配置防攻击策略。
cpu-defend-policy *policy-name* **batch slot** { *start-slot* [**to** *end-slot*] } &<1-12>
AR8700系列不支持批量配置防攻击策略。
- 单独配置防攻击策略。
对于AR5700、AR6700、AR8100系列：
cpu-defend-policy *policy-name* [**slot** *slot-id*]
对于AR8700系列：
cpu-defend-policy *policy-name* [**mcu**]

创建防攻击策略之后，必须将策略在系统视图下应用，否则防攻击策略不会生效。

----结束

8.4.3 （可选）配置动态自适应调整协议报文的默认 CPCAR 值

背景信息

协议报文默认CPCAR值无法满足报文上送速率时，可以配置动态自适应调整协议报文的默认CPCAR值功能。CPCAR值的动态自适应调整记录可通过**display cpu-defend dynamic-adjust history-record**命令进行查看。

设备支持的CPCAR值动态自适应调整功能的协议报文类型及其调整后的最大CPCAR值如下表所示：

协议报文类型	协议报文说明	调整后的最大CPCAR值
arp-reply	ARP响应报文	2倍默认值
arp-request	ARP请求报文	2倍默认值
arp-request-uc	单播ARP请求报文	2倍默认值

协议报文类型	协议报文说明	调整后的最大CPCAR值
dhcp-reply	DHCP应答报文	1.5倍默认值
dhcp-request	DHCP请求报文	1.5倍默认值
dhcp-discovery	DHCP发现报文	1.5倍默认值
nd	IPv6邻居发现协议报文	2倍默认值

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启动态自适应调整协议报文的默认CPCAR值。

```
cpu-defend dynamic-adjust [ packet-type { arp-reply | arp-request | arp-request-uc | dhcp-reply | dhcp-request | nd | dhcp-discovery } ] enable
```

如果不指定**packet-type**参数，则所有支持该功能的协议报文类型均开启该功能。

----结束

8.4.4 检查配置结果

操作步骤

- 执行命令**display cpu-defend policy** [*policy-name*]，查看防攻击策略的配置信息。
- 执行命令**display cpu-defend configuration** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* | **mcu** }，查看上送CPU的协议报文的速率配置信息。

  AR8700系列仅支持在主控板查看CAR的配置信息，即仅支持mcu字段。

  AR5700、AR6700、AR8100系列不支持在主控板查看CAR的配置信息，即不支持mcu字段。

  AR8700不支持指定槽位号slot-id。
- 执行命令**display cpu-defend dynamic-adjust history-record** [**packet-type** { **arp-reply** | **arp-request** | **arp-request-uc** | **dhcp-request** | **dhcp-reply** | **nd** | **dhcp-discovery** }] { **all** | **slot** *slot-id* }，查看协议报文CPCAR值的动态自适应调整的历史记录。
- 执行命令**display cpu-defend linkup statistics** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }，查看协议联动功能的统计信息。

  AR8700不支持指定槽位号slot-id。
- 执行命令**display cpu-defend linkup configuration** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }，查看协议联动功能的配置信息。

  AR8700不支持指定槽位号slot-id。
- 执行命令**display cpu-defend rate** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }，查看协议报文的CPCAR。

  AR8700不支持指定槽位号slot-id。

- 执行命令**display cpu-defend statistics** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }，查看上送CPU的报文统计信息。

  ICMP快回功能开启的情况下，不区分统计ICMPv4和ICMPv6报文，ICMPv4和ICMPv6报文的总统计计数记录在回显字段**icmp**中。

  AR8700不支持指定槽位号slot-id。

----结束

8.4.5 举例：配置 CPU 防攻击

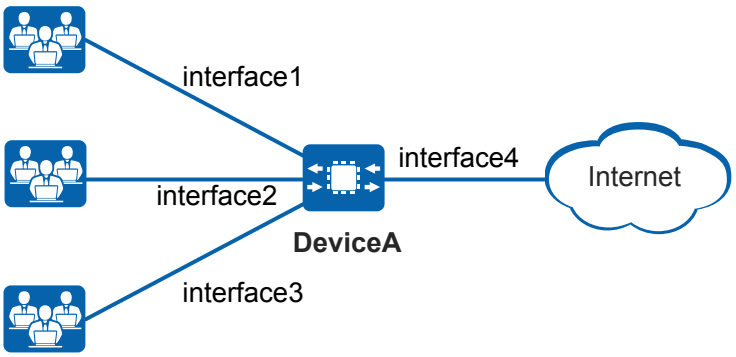
组网需求

如图8-2所示，大量用户通过DeviceA访问Internet，管理员发现攻击者发送大量的ARP Request报文，影响CPU的正常工作，希望能够减小ARP报文对CPU处理正常业务的影响。

图 8-2 配置本机防攻击示例组网图

说明

本例中interface1，interface2，interface3和interface4分别代表10GE0/0/1，10GE0/0/2，10GE0/0/3，10GE0/0/4。



操作步骤

步骤1 配置防攻击策略。

创建防攻击策略。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] cpu-defend policy test1
```

配置ARP Request报文上送CPU的速率限制。

```
[DeviceA-cpu-defend-policy-test1] car packet-type arp-request pps 128
[DeviceA-cpu-defend-policy-test1] quit
```

步骤2 全局应用防攻击策略。

```
[DeviceA] cpu-defend-policy test1
```

----结束

检查配置结果

查看配置的防攻击策略的信息。

```
[DeviceA] display cpu-defend policy test1
=============================================
Policy name: test1
Policy applys on slot: <0>
Car packet-type arp-request(pps) : 128
=============================================
```

查看配置的CAR的信息。

```
[DeviceA] display cpu-defend configuration all
Car configurations on slot 0 :
------------------------------------------------------------------------
PacketType            Status      Current(pps) Default(pps)      Queue
------------------------------------------------------------------------
arp-miss              Enabled            1536        1536         13
arp-reply             Enabled            2048        2048         23
arp-request           Enabled             128        2048         23
arp-request-uc        Enabled            2048        2048         23
......
```

配置文件

DeviceA的配置文件

```
#
sysname DeviceA
#
cpu-defend policy test1
 car packet-type arp-request pps 128
#
cpu-defend-policy test1
#
return
```

8.5 配置用户级限速

8.5.1 了解用户级限速

用户侧主机容易遭受病毒攻击，借此向网络中发送大量的协议报文，导致设备的CPU占用率过高，性能下降，从而影响正常的业务，此时，管理员可以配置用户级限速功能。用户级限速功能是指基于用户MAC地址识别用户，对用户的特定报文进行限速，使得单个用户发起攻击时只对该用户进行限速，从而不影响其他用户。与CPCAR基于设备相比，基于用户MAC地址进行限速能够精确到每个用户，对正常用户的影响更小。

用户级限速的处理流程如下：

1. 设备对收到的用户协议报文的源MAC地址进行哈希计算，将收到的不同源MAC地址的报文放到不同的限速桶中。
2. 当单位时间限速桶内的报文超过了限速值时，该限速桶会丢弃收到的报文，并且每隔10分钟对限速桶内的丢包数目进行统计。如果10分钟内限速桶丢弃的报文数

目超过2000个，设备会发送该限速桶的丢包日志。如果同时存在多个限速桶丢包数目超过2000个，设备只发送丢包数目最多的10个限速桶的丢包日志。

8.5.2 配置用户级限速

背景信息

配置用户级限速功能，基于用户MAC地址进行精确限速，减少对正常用户的影响。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启用户级限速功能。

```
cpu-defend host-car enable
```

步骤3 配置用户级限速的限速值。

```
cpu-defend host-car [ mac-address mac-address | car-id car-id ] pps pps-value
```

步骤4 配置用户级限速可以限制的报文类型。

```
cpu-defend host-car { { arp | dhcp-request | dhcpv6-request | nd } * | all }
```

步骤5 进入指定的接口视图。

```
interface interface-type interface-number
```

步骤6 开启接口下的用户级限速功能。

```
undo host-car disable
```

缺省情况下，接口下的用户级限速功能未开启。

----结束

任务示例

开启接口10GE0/0/1下的用户级限速功能，并配置用户级限速的限速值为15pps、仅限制ARP报文的速率。

```
<HUAWEI> system-view
[HUAWEI] cpu-defend host-car enable
[HUAWEI] cpu-defend host-car pps 15
[HUAWEI] cpu-defend host-car arp
[HUAWEI] interface 10ge 0/0/1
[HUAWEI-10GE0/0/1] undo host-car disable
[HUAWEI-10GE0/0/1] quit
```

8.5.3 检查配置结果

操作步骤

- 执行命令**display cpu-defend host-car** [**mac-address** *mac-address*] **statistics** [**slot** *slot-id*]，查看用户级限速丢弃的报文数。

  AR8700不支持指定槽位号slot-id。

----结束

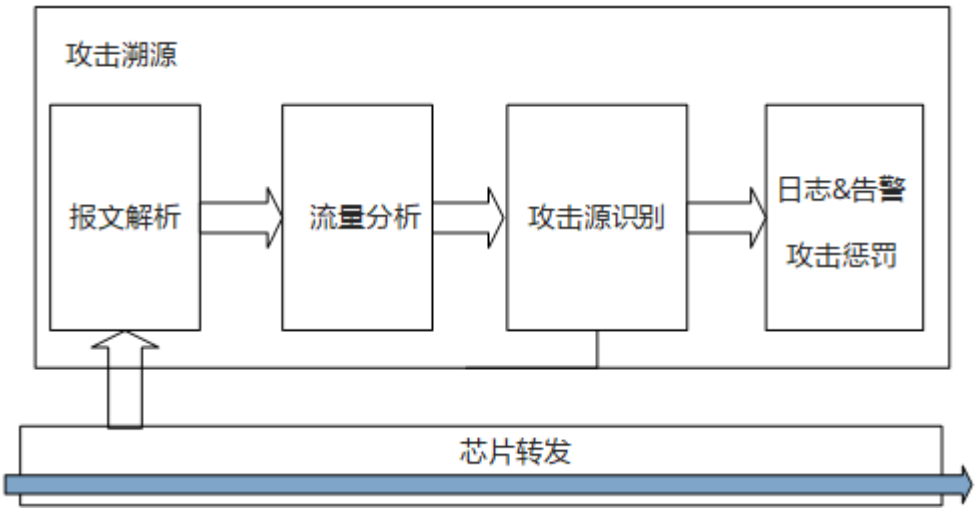
8.6 配置攻击溯源

8.6.1 了解攻击溯源

攻击溯源能够防御DoS攻击。如图8-3所示，攻击溯源包括报文解析、流量分析、攻击源识别和发送日志告警通知管理员以及实施惩罚四个过程。

1. 从IP地址、MAC地址以及端口三个维度对上送CPU的报文进行报文解析，其中端口通过“物理端口+VLAN”标识。
2. 根据IP地址、MAC地址或者端口信息统计接收到的协议报文数量。
3. 当单位时间上送CPU的报文数量超过了阈值时，则认为是攻击。
4. 当检测到攻击后，会发送日志、告警通知管理员或者直接实施惩罚，如丢弃攻击报文。

图 8-3 攻击溯源原理



此外，攻击溯源还提供了白名单功能。将合法用户加入到通过白名单中，设备不对白名单内的用户报文进行溯源和攻击惩罚处理，从而保证合法用户的报文能够正常上送CPU处理。白名单可以通过ACL或端口灵活设置。

8.6.2 配置攻击溯源

背景信息

配置攻击溯源功能后，设备能够通过分析上送CPU的报文是否会对CPU造成攻击，追溯攻击源并以日志或告警的方式通知管理员，以便管理员采取措施对攻击源进行防御部署。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建防攻击策略并进入防攻击策略视图。

```
cpu-defend policy policy-name
```

步骤3 开启攻击溯源功能。

```
auto-defend enable
```

步骤4 配置攻击溯源检查阈值。

```
auto-defend threshold threshold-value
```

步骤5 配置攻击溯源的采样比。

```
auto-defend attack-packet sample sample-value
```

步骤6 配置攻击溯源防范的报文类型。

```
auto-defend protocol { { arp | icmp | dhcp | ttl-expired | tcp | udp | telnet | dhcpv6 | dns | nd | icmpv6 | tcpv6 | vrrp | vrrp6 } * | all }
```

步骤7 配置攻击溯源的溯源模式。

```
auto-defend trace-type { source-mac | source-ip | source-portvlan } *
```

溯源模式的优先级由高到低为：基于MAC地址>基于IP地址>基于接口和VLAN信息，配置多种溯源模式时，按照上述优先级生效。

步骤8 （可选）配置攻击溯源的白名单。

```
auto-defend whitelist whitelist-id { acl acl-number | acl ipv6 ipv6-acl-number | interface interface-type interface-number }
```

缺省情况下，没有攻击溯源的白名单。

说明

通过ACL设置攻击溯源白名单时需要注意以下几点：

- 使用ACL设置白名单时，需要配置ACL和对应的rule，如果ACL中配置rule为空，即没有配置rule的动作，则白名单功能不生效。
- ACL可以是基本ACL、高级ACL、二层ACL、基本ACL6和高级ACL6。
- ACL中配置的rule，其动作无论配置为**permit**还是**deny**，命中该ACL的报文均会被当作合法报文，不对其进行溯源和攻击惩罚处理。
- 如果ACL的rule通过某协议定义，则需要保证攻击溯源功能支持该协议。
- 设备ACL资源不足，可能会导致白名单功能失效。

步骤9 （可选）配置攻击溯源事件上报功能。

1. 开启攻击溯源事件上报功能。

   ```
   auto-defend alarm enable
   ```

   缺省情况下，攻击溯源事件上报功能处于关闭状态。

2. 配置攻击溯源事件上报阈值。

   ```
   auto-defend alarm threshold alarm-threshold
   ```

步骤10 配置攻击溯源惩罚措施。

```
auto-defend action { deny [ timeout timeout-num ] | error-down }
```


说明

- Error-Down是指设备检测到故障后将接口状态设置为ERROR DOWN状态，此时接口不能收发报文，接口指示灯为常灭。

  如果配置攻击溯源的惩罚措施是将攻击报文进入的接口ERROR DOWN，则会造成设备业务的中断，接口下合法的用户会受牵连，请谨慎使用。
- 设备不对攻击溯源的白名单用户进行攻击溯源的惩罚。

步骤11 返回系统视图。

```
quit
```

步骤12 应用防攻击策略。

- 批量配置防攻击策略。

  cpu-defend-policy *policy-name* **batch slot** { *start-slot* [**to** *end-slot*] } &<1-12>

  AR8700系列不支持批量配置防攻击策略。
- 单独配置防攻击策略。

  对于AR5700、AR6700、AR8100系列：

  cpu-defend-policy *policy-name* [**slot** *slot-id*]

  对于AR8700系列：

  cpu-defend-policy *policy-name* [**mcu**]

创建防攻击策略之后，必须将策略在系统视图下应用，否则防攻击策略不会生效。

----结束

任务示例

在名称为test的防攻击策略下，开启攻击溯源功能，并配置攻击溯源的检查阈值为200pps、采样比是7、溯源模式是基于源IP地址溯源，并且配置攻击溯源的惩罚措施为丢弃攻击报文。

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend threshold 200
[HUAWEI-cpu-defend-policy-test] auto-defend attack-packet sample 7
[HUAWEI-cpu-defend-policy-test] auto-defend trace-type source-ip
[HUAWEI-cpu-defend-policy-test] auto-defend action deny
[HUAWEI-cpu-defend-policy-test] quit
[HUAWEI] cpu-defend-policy test
```

后续处理

配置攻击溯源的惩罚措施为ERROR DOWN时，设备在识别出攻击源后，会将攻击报文进入的接口状态置为Down。接口状态被置为Down后，建议先排除攻击，再将接口状态恢复Up。

表 8-6 将接口状态恢复 Up 的方法

方法	适用场景	处理步骤
手动恢复	• 预期Down状态的接口数量较少。 • 接口已经被置为Down状态。	对应接口视图下依次执行命令**shutdown**和**undo shutdown**，或者执行命令**restart**，重启接口。

方法	适用场景	处理步骤
自动恢复	• 预期Down状态的接口数量较多，逐一手动恢复接口状态工作量大，且可能遗漏部分接口。 • 接口还未被置为Down状态。该方式对已经是Down状态的接口不生效。	在系统视图下执行命令**error-down auto-recovery cause auto-defend interval**开启接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间。可以通过命令**display error-down recovery**，查看接口状态自动恢复信息。

8.6.3 检查配置结果

操作步骤

- 执行命令**display cpu-defend policy** [*policy-name*]，查看防攻击策略的配置信息。
- 执行命令**display auto-defend attack-source** [**slot** *slot-id* | **history** [**slot** *slot-id*] | **trace-type** { **source-mac** | **source-ip** | **source-portvlan** } [**slot** *slot-id*]]，查看攻击源信息。

  AR8700不支持指定槽位号slot-id。
- 执行命令**display auto-defend configuration** [**cpu-defend policy** *policy-name* | **slot** *slot-id*]，查看防攻击策略的攻击溯源配置信息。

  AR8700不支持指定槽位号slot-id。
- 执行命令**display auto-defend whitelist slot** *slot-id*，查看攻击溯源的白名单信息。

  AR8700不支持指定槽位号slot-id。

----结束

8.6.4 举例：配置攻击溯源

组网需求

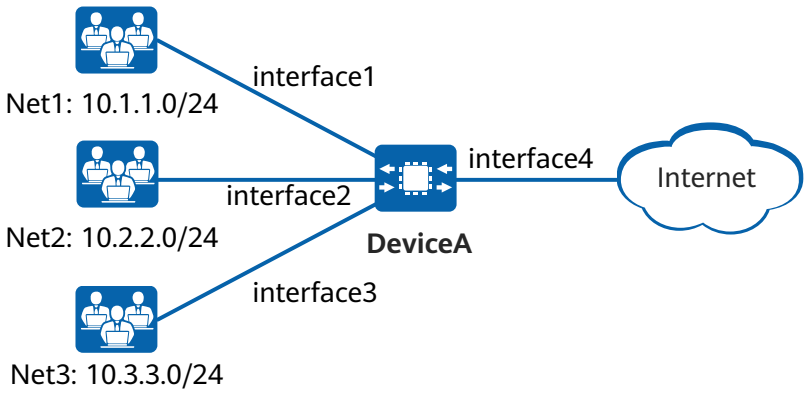
如图8-4所示，位于不同网段的用户通过DeviceA访问Internet。由于接入的用户数量多，DeviceA经常因为处理大量的ARP报文导致CPU使用率高，影响正确业务。

管理员希望设备能够对上送CPU的ARP报文进行分析，将超过阈值的报文判定为攻击报文，并找出攻击源用户或者源接口，通过日志、告警的方式通知管理员，以便管理员采取一定的安全措施来保护CPU。此外，Net2网段的用户为固定合法用户，需要确保该网段用户的ARP报文能够正常上送CPU。

图 8-4 配置攻击溯源示例组网图

说明

本例中interface1，interface2，interface3和interface4分别代表10GE0/0/1，10GE0/0/2，10GE0/0/3，10GE0/0/4。



操作步骤

步骤1 配置防攻击策略。

创建防攻击策略。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] cpu-defend policy test1
```

开启攻击溯源功能。

```
[DeviceA-cpu-defend-policy-test1] auto-defend enable
```

配置攻击溯源检查阈值为100pps。

```
[DeviceA-cpu-defend-policy-test1] auto-defend threshold 100
```

配置攻击溯源的采样比为7，即每7个报文采样1个报文。

```
[DeviceA-cpu-defend-policy-test1] auto-defend attack-packet sample 7
```

配置攻击溯源防范的报文类型为ARP报文。

```
[DeviceA-cpu-defend-policy-test1] auto-defend protocol arp
```

配置攻击溯源的溯源模式为基于源MAC地址和源IP地址。

```
[DeviceA-cpu-defend-policy-test1] auto-defend trace-type source-mac source-ip
```

开启攻击溯源事件上报功能。

```
[DeviceA-cpu-defend-policy-test1] auto-defend alarm enable
```

配置攻击溯源惩罚措施，设备受到攻击时丢弃报文，持续时长为360s。在配置攻击溯源惩罚措施之前，请确保设备受到了非法攻击，避免因误丢弃大量正常协议报文而影响正常业务。

```
[DeviceA-cpu-defend-policy-test1] auto-defend action deny timeout 360
[DeviceA-cpu-defend-policy-test1] quit
```

配置攻击溯源白名单。

```
[DeviceA] acl number 2001
[DeviceA-acl-basic-2001] rule permit source 10.2.2.0 0.0.0.255
```

```
[DeviceA-acl-basic-2001] quit
[DeviceA] cpu-defend policy test1
[DeviceA-cpu-defend-policy-test1] auto-defend whitelist 1 acl 2001
[DeviceA-cpu-defend-policy-test1] quit
```

步骤2 应用防攻击策略。

```
[DeviceA] cpu-defend-policy test1
```

----结束

检查配置结果

查看攻击溯源的配置信息。

```
[DeviceA] display auto-defend configuration cpu-defend policy
test1
-------------------------------------------------------------------------
 Name  : test1
 Related slot : ***
 auto-defend                    : enable
 auto-defend threshold          : 100 (pps)
 auto-defend attack-packet sample : 7 (pps)
 auto-defend alarm              : enable
 auto-defend alarm threshold    : 128 (pps)
 auto-defend action             : deny timer: 360 (second)
 auto-defend trace-type         : source-mac source-ip
 auto-defend protocol           : arp
 auto-defend whitelist 1        : acl number 2001
-------------------------------------------------------------------------
```

配置文件

DeviceA的配置文件

```
#
sysname DeviceA
#
cpu-defend policy test1
 auto-defend action deny timeout 360
 auto-defend alarm enable
 auto-defend attack-packet sample 7
 auto-defend threshold 100
 auto-defend protocol arp
 auto-defend whitelist 1 acl 2001
#
cpu-defend-policy test1
#
acl number 2001
 rule 5 permit source 10.2.2.0 0.0.0.255
#
return
```

8.7 配置畸形报文攻击防范

8.7.1 了解畸形报文攻击防范

畸形报文攻击是通过向目标设备发送有缺陷的IP报文，使得目标设备在处理这样的IP报文时出错和崩溃，影响目标设备承载的业务正常运行。畸形报文攻击防范是指设备实时检测出畸形报文并予以丢弃，实现对设备的保护。

畸形报文攻击主要分为以下几类：

没有 IP 载荷的泛洪

如果IP报文只有20字节的IP报文头，没有数据部分，就认为是没有IP载荷的报文。攻击者经常构造只有IP头部，没有携带任何高层数据的IP报文，目标设备在处理这些没有IP载荷的报文时会出错和崩溃，影响目标设备承载的业务正常运行。

启用畸形报文攻击防范后，设备检测接收到的IP报文是否有载荷，如果没有载荷，则直接将其丢弃。

IGMP 空报文

正常的IGMP报文由20字节的IP报文头加上8字节的数据部分组成，总长28个字节。总长度小于28字节的IGMP报文称为IGMP空报文。设备在处理IGMP空报文时会出错和崩溃，影响目标设备承载的业务正常运行。

启用畸形报文攻击防范后，设备检测接收到的IGMP报文是否为空报文，如果是空报文，则直接将其丢弃。

LAND 攻击

LAND攻击是攻击者利用TCP连接三次握手机制中的缺陷，向目标主机发送一个源地址和目的地址均为目标主机、源端口和目的端口相同的SYN报文，目标主机接收到该报文后，将创建一个源地址和目的地址均为自己的TCP空连接，直至连接超时。在这种攻击方式下，目标主机将会创建大量无用的TCP空连接，耗费大量资源，直至设备瘫痪。

启用畸形报文攻击防范后，设备采用检测TCP SYN报文的源地址和目的地址是否一致或源端口和目的端口是否一致的方法来避免LAND攻击。如果TCP SYN报文中的源地址和目的地址一致，或者源端口和目的端口一致，则认为是畸形报文攻击，丢弃该报文。

Smurf 攻击

Smurf攻击是指攻击者向目标网络发送源地址为目标主机地址、目的地址为目标网络广播地址的ICMP请求报文，目标网络中的所有主机接收到该报文后，都会向目标主机发送ICMP响应报文，导致目标主机收到过多报文而消耗大量资源，甚至导致设备瘫痪或网络阻塞。

启用畸形报文攻击防范后，设备通过检测ICMP请求报文的目标地址是否是广播地址或子网广播地址来判断是否是Smurf攻击。如果检测到此类报文，直接将其丢弃。

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个标志位全部为1，就是圣诞树攻击。设备在受到圣诞树攻击时，会造成系统崩溃。
- SYN和FIN同时为1，如果端口是关闭的，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(主机在线或者下线)和端口探测（端口打开或者关闭）。
- 6个标志位全部为0，如果端口是关闭的，会使接收方应答一个RST | ACK消息，这可以用于探测主机；如果端口是开放的，Linux和UNIX系统不会应答，而Windows系统将回答RST | ACK消息，这可以探测操作系统类型（Windows系统，Linux和UNIX系统等）。

启用畸形报文攻击防范后，设备会检查TCP报文的各个标志位避免TCP标志位非法攻击。如果符合下面条件之一，则将该TCP报文丢弃：

- 6个标志位全部为1；
- SYN和FIN位同时为1；
- 6个标志位全部为0。

8.7.2 配置畸形报文攻击防范

背景信息

配置畸形报文攻击防范功能后，设备将对收到的上送CPU的报文进行分析处理，判断其是否是几种畸形报文攻击报文类型之一，若是，则直接丢弃畸形报文。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启畸形报文攻击防范功能。

```
anti-attack abnormal enable
```

说明

在系统视图下，执行命令**anti-attack enable**可以开启所有的攻击防范功能（包括畸形报文攻击防范功能）。

----结束

检查配置结果

执行命令**display anti-attack statistics abnormal**，查看设备上畸形报文攻击防范的统计数据。

8.8 配置分片报文攻击防范

8.8.1 了解分片报文攻击防范

分片报文攻击是通过向目标设备发送分片出错的报文，使得目标设备在处理分片错误的报文时崩溃、重启或消耗大量的CPU资源，影响目标设备承载的业务正常运行。分片报文攻击防范是指设备实时检测出分片报文并予以丢弃或者限速处理，实现对本设备的保护。

分片报文攻击主要分为以下几类：

分片数量巨大攻击

IP报文中的偏移量是以8字节为单位的。正常情况下，IP报文的头部有20个字节，IP报文的最大载荷为65515。对这些数据进行分片，分片个数最大可以达到8189片，对于超过8189的分片报文，设备在重组这些分片报文时会消耗大量的CPU资源。

针对分片数量巨大攻击，如果同一报文的分片数目超过8189个，则设备认为是恶意报文，丢弃该报文的所有分片。

巨大 Offset 攻击

攻击者向目标设备发送一个Offset值超大的分片报文，导致目标设备需要分配巨大的内存空间来存放所有分片报文，消耗大量资源。

Offset字段占13个bit，单位为8字节，所以Offset的最大取值为8191。但是在正常情况下，Offset值不会超过8190。这是因为IP报文的最大载荷为65515个字节，如果Offset=8190，8190*8=65520，就超过了65515。所以，正常Offset的最大值是8189，8189*8=65512，最后一片报文最多只有3个字节IP载荷。

设备在收到分片报文时判断Offset是否大于8189，如果大于就当作恶意分片报文直接丢弃。

重复分片攻击

重复分片攻击就是把同样的分片报文多次向目标主机发送，存在两种情况：

- 多次发送的分片完全相同，这样会造成目标主机的CPU和内存使用不正常；
- 多次发送的分片报文不相同，但Offset相同，目标主机就会处于无法处理的状态：哪一个分片应该保留，哪一个分片应该丢弃，还是都丢弃。这样就会造成目标主机的CPU和内存使用不正常。

启用分片报文攻击防范后，对于重复分片类报文的攻击，设备实现对分片报文进行CAR（Committed Access Rate）限速，保留首片，丢弃其余所有相同的重复分片，保证不对CPU造成攻击。

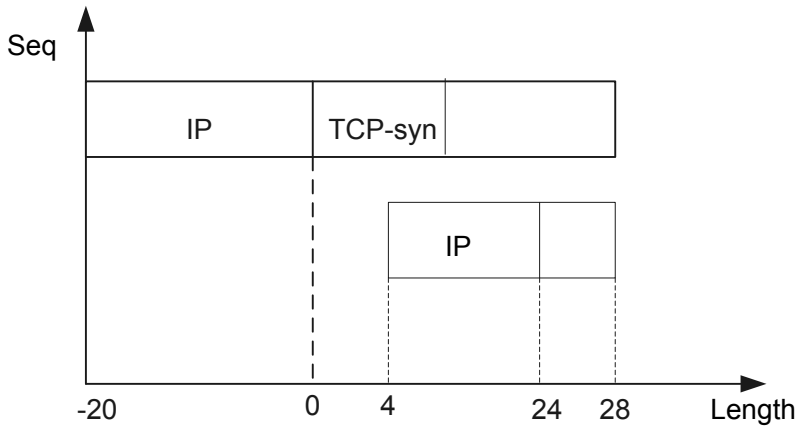
Syndrop 攻击

Syndrop攻击的原理是IP分片错误，第二片包含在第一片之中。即数据包中第二片IP包的偏移量小于第一片结束的位移，而且算上第二片IP包的Data，也未超过第一片的尾部。Syndrop攻击使用了TCP协议，Flag为SYN，而且带有载荷。

如图8-5所示：

- 第一片IP载荷为28字节，IP头部20字节；
- 第二片IP载荷为4字节，IP头部20字节，Offset=24（错误，正确应该是28）。

图 8-5 Syndrop 攻击分片示意图



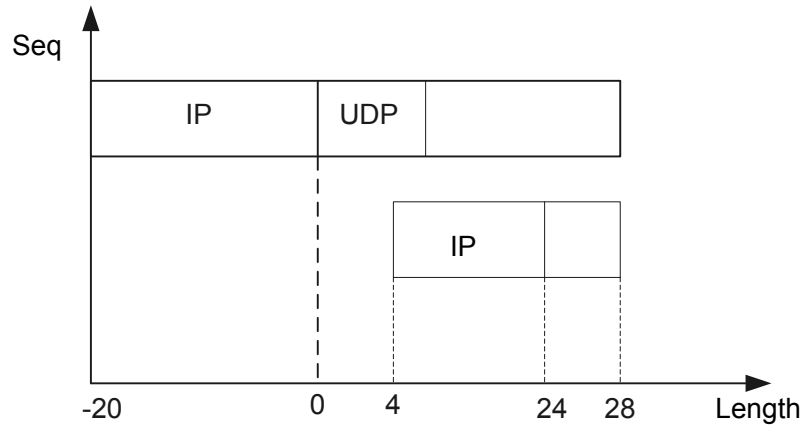
Syndrop攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Syndrop攻击，设备会直接丢弃所有分片报文。

NewTear 攻击

NewTear攻击是分片错误的攻击。如图8-6所示，protocol使用UDP。

- 第一片IP载荷28字节（包含UDP头部，UDP检验和为0）；
- 第二片IP载荷4字节，offset=24（错误，正确应该是28）。

图 8-6 NewTear 攻击分片示意图



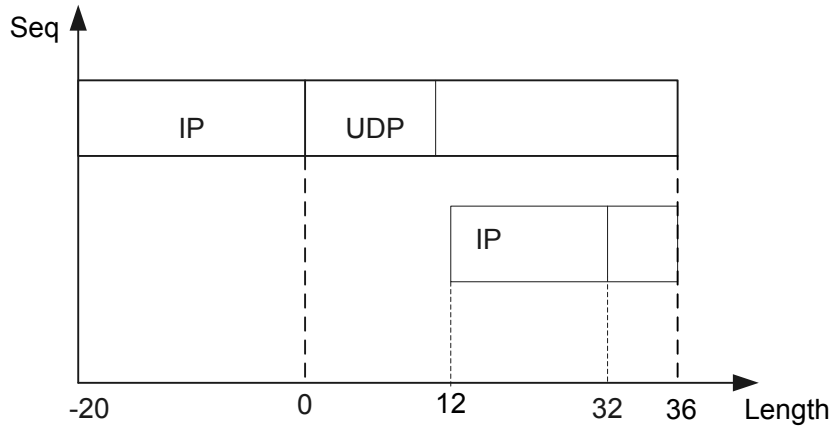
NewTear攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于NewTear攻击，设备会直接丢弃所有分片报文。

Bonk 攻击

Bonk攻击是分片错误的攻击。如图8-7所示，protocol使用UDP。

- 第一片IP载荷为36字节（包含UDP头部，UDP检验和为0）；
- 第二片IP载荷为4字节，offset=32（错误，正确应该是36）。

图 8-7 Bonk 攻击分片示意图



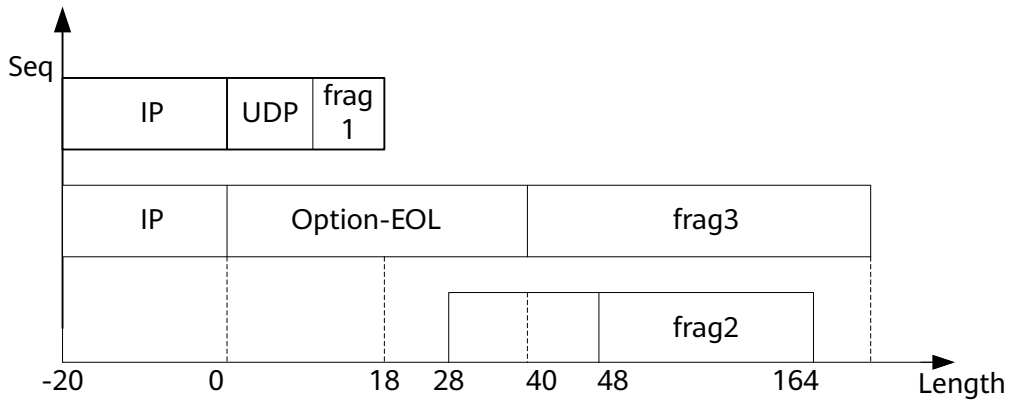
Bonk攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Bonk攻击，设备会直接丢弃所有分片报文。

Nesta 攻击

Nesta攻击是分片错误的攻击。如图8-8所示：

- 第一片IP载荷为18，protocol为UDP，检验和为0；
- 第二片offset为48，IP载荷为116字节；
- 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。

图 8-8 Nesta 攻击分片示意图



Nesta攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Nesta攻击，设备会直接丢弃所有分片报文。

8.8.2 配置分片报文攻击防范

背景信息

配置分片报文攻击防范功能后，设备将对收到的分片报文进行限速处理。对于超出限速值的分片报文，设备直接丢弃。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启分片报文攻击防范功能。

```
anti-attack fragment enable
```

说明

在系统视图下，执行命令**anti-attack enable**可以开启所有的攻击防范功能（包括分片报文攻击防范功能）。

步骤3 配置分片报文的限制速率。

```
anti-attack fragment car cir cir-num
```

----结束

检查配置结果

执行命令**display anti-attack statistics fragment**，查看设备上分片报文攻击防范的统计数据。

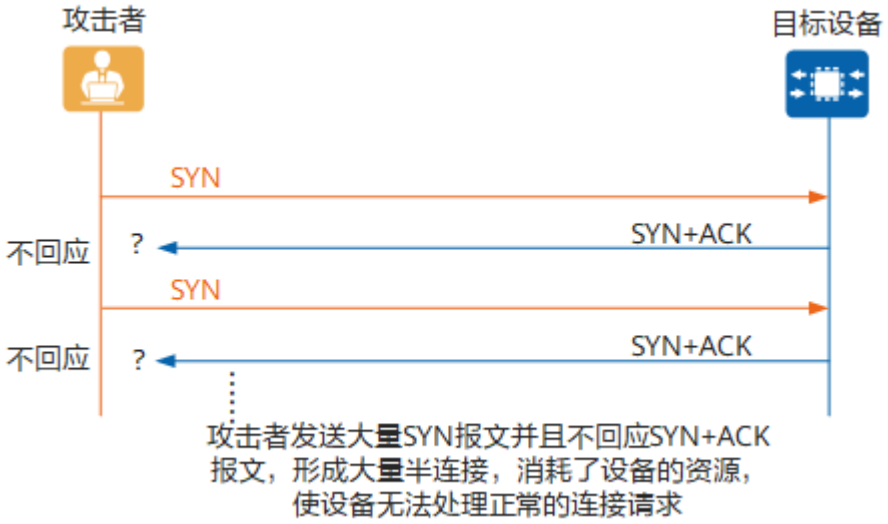
8.9 配置 TCP SYN 泛洪攻击防范

8.9.1 了解 TCP SYN 泛洪攻击防范

TCP SYN攻击利用了TCP三次握手的漏洞。如图8-9所示，在TCP的3次握手期间，当接收端（目标设备）收到来自发送端（攻击者）的初始SYN报文时，向发送端返回一个SYN+ACK报文。接收端在等待发送端的最终ACK报文时，该连接一直处于半连接状态。如果接收端最终没有收到ACK报文包，则重新发送一个SYN+ACK到发送端。如果经过多次重试，发送端始终没有返回ACK报文，则接收端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。

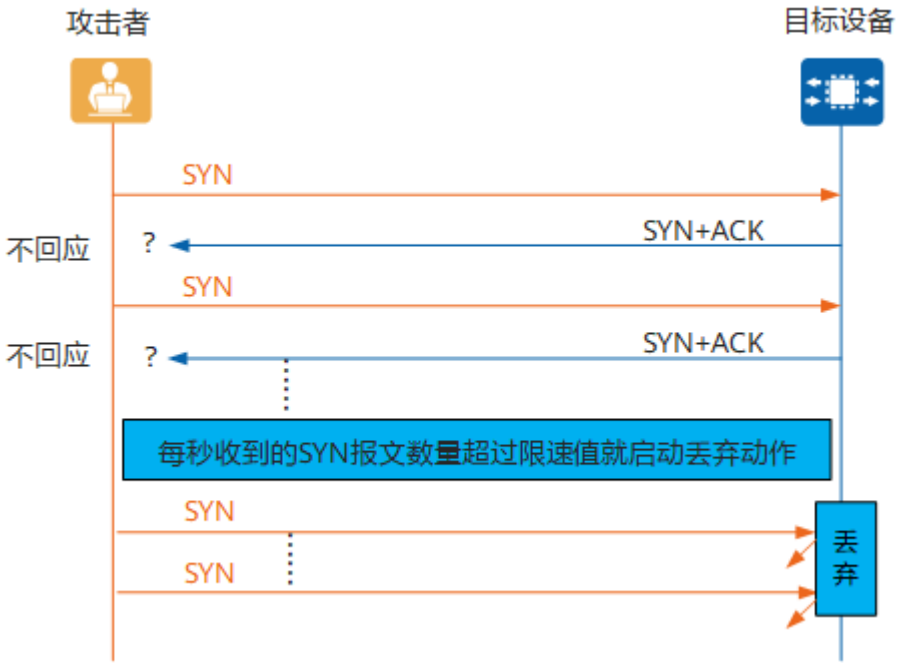
在这段时间内，攻击者可能发送大量SYN报文到开放的端口，并且不回应接收端的SYN+ACK报文。接收端内存很快就会超过负荷，且无法再接收任何新的连接，并将现有的连接断开。

图 8-9 TCP SYN 泛洪攻击



设备对TCP SYN攻击的处理方式如图8-10所示。开启TCP SYN泛洪攻击防范后，设备对TCP SYN报文进行速率限制，保证设备受到攻击时资源不被耗尽。

图 8-10 TCP SYN 泛洪攻击防范



8.9.2 配置 TCP SYN 泛洪攻击防范

背景信息

配置TCP SYN泛洪攻击防范功能后，设备将对收到的TCP SYN报文进行限速处理。对于超出限速值的TCP SYN报文，设备直接丢弃。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启TCP SYN泛洪攻击防范功能。

```
anti-attack tcp-syn enable
```

说明

在系统视图下，执行命令**anti-attack enable**可以开启所有的攻击防范功能（包括TCP SYN泛洪攻击防范功能）。

步骤3 配置TCP SYN报文的限制速率。

```
anti-attack tcp-syn car cir cir-num
```

----结束

检查配置结果

执行命令**display anti-attack statistics tcp-syn**，查看TCP SYN泛洪攻击防范的统计数据。

8.10 配置 UDP 泛洪攻击防范

8.10.1 了解 UDP 泛洪攻击防范

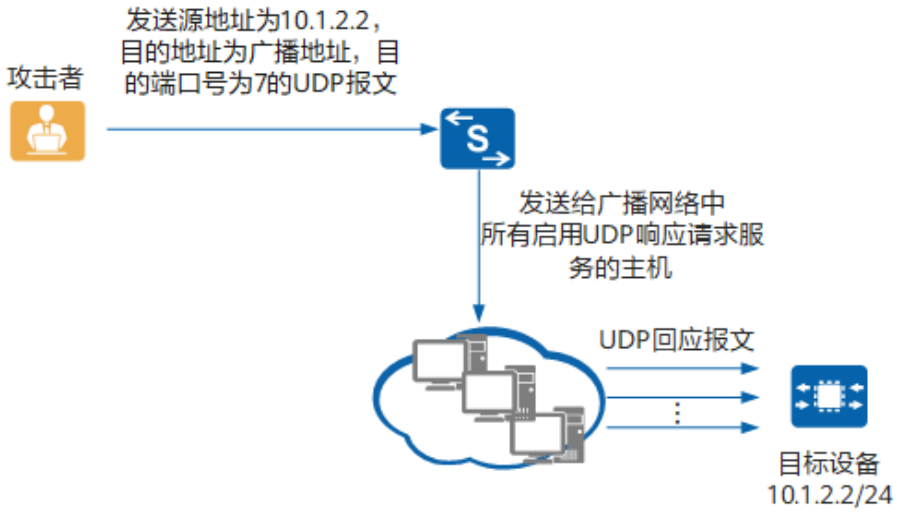
UDP泛洪攻击是指攻击者在短时间内向目标设备发送大量的UDP报文，导致目标设备负担过重而不能处理正常的业务。UDP泛洪攻击分为以下两类：

- Fraggle攻击

  Fraggle攻击的原理如图8-11所示。攻击者发送源地址为目标设备IP地址，目的地址为广播地址，目的端口号为7的UDP报文。如果该广播网络中有很多主机都启用了UDP响应请求服务，目标设备将会收到很多主机发送的UDP回应报文，设备处理这些报文会消耗CPU资源，造成系统繁忙，从而达到攻击效果。

  开启泛洪攻击防范功能后，设备默认UDP端口号为7的报文是攻击报文，直接将其丢弃。

  图 8-11 Fraggle 攻击

- UDP诊断端口攻击

  攻击者向目标设备的UDP诊断端口（7-echo，13-daytime，19-Chargen等UDP端口）发送大量UDP请求报文，形成泛洪，消耗网络带宽资源，并且目标设备为这些请求提供服务回应UDP报文时会消耗CPU资源，造成负担过重而不能处理正常的业务。

  开启泛洪攻击防范功能后，设备将UDP端口为7、13和19的报文认为是攻击报文，直接丢弃。

8.10.2 配置 UDP 泛洪攻击防范

背景信息

配置UDP泛洪攻击防范功能后，对于收到的端口号为7、13和19的报文，设备直接丢弃。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启UDP泛洪攻击防范功能。

```
anti-attack udp-flood enable
```

说明

在系统视图下，执行命令**anti-attack enable**可以开启所有的攻击防范功能（包括UDP泛洪攻击防范功能）。

----结束

检查配置结果

执行命令**display anti-attack statistics udp-flood**，查看UDP泛洪攻击防范的统计数据。

8.11 配置 ICMP 泛洪攻击防范

8.11.1 了解 ICMP 泛洪攻击防范

通常情况下，网络管理员会用Ping程序对网络进行监控和故障排除，大概过程如下：

1. 源设备向接收设备发出ICMP请求报文；
2. 接收设备接收到ICMP请求报文后，会向源设备回应一个ICMP响应报文。

如图8-12所示，如果攻击者向目标设备发送大量的ICMP请求报文，则目标设备会忙于处理这些请求，而无法继续处理其他的数据报文，造成对正常业务的冲击。

图 8-12 ICMP 泛洪攻击

设备对ICMP泛洪攻击的处理方式如图8-13所示。开启ICMP泛洪攻击防范后，设备针对ICMP报文进行速率限制，保证设备受到攻击时资源不被耗尽。

图 8-13 ICMP 泛洪攻击防范

8.11.2 配置 ICMP 泛洪攻击防范

背景信息

配置ICMP泛洪攻击防范功能后，设备将对收到的ICMP报文进行限速处理。对于超出限速值的ICMP报文，设备直接丢弃。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启ICMP泛洪攻击防范功能。

```
anti-attack icmp-flood enable
```

说明

在系统视图下，执行命令**anti-attack enable**可以开启所有的攻击防范功能（包括ICMP泛洪攻击防范功能）。

步骤3 配置ICMP泛洪攻击报文的限制速率。

```
anti-attack icmp-flood car cir cir-num
```

----结束

检查配置结果

执行命令**display anti-attack statistics icmp-flood**，查看ICMP泛洪攻击防范的统计数据。

8.12 维护本机防攻击

日常维护中，还可以清除本机防攻击的相关统计信息。如有需要，可在用户视图下执行以下命令。

须知

清除本机防攻击相关的统计信息后，以前的信息将无法恢复，务必仔细确认。

表 8-7 清除本机防攻击相关的统计信息

操作	命令
清除上送CPU的报文统计信息	**reset cpu-defend statistics** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }
清除协议联动的统计信息	**reset cpu-defend linkup statistics** [**packet-type** *packet-type*] { **slot** *slot-id* | **all** }
清除用户级限速的报文统计信息	**reset cpu-defend host-car** [**mac-address** *mac-address*] **statistics** [**slot** *slot-id*]
清除攻击溯源统计信息	**reset auto-defend attack-source** [**slot** *slot-id*]
清除攻击溯源历史统计信息	**reset auto-defend attack-source history** [**slot** *slot-id*]
基于溯源模式清除攻击溯源统计信息	**reset auto-defend attack-source trace-type** { **source-mac** [*mac-address*] | **source-ip** [*ip-address* | *ipv6-address*] | **source-portvlan** [**interface** *interface-type interface-number* **vlan** *vlan-id*] } [**slot** *slot-id*]
清除攻击防范的报文统计信息	**reset anti-attack statistics** [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood**]

说明

AR8700不支持指定槽位号slot-id。

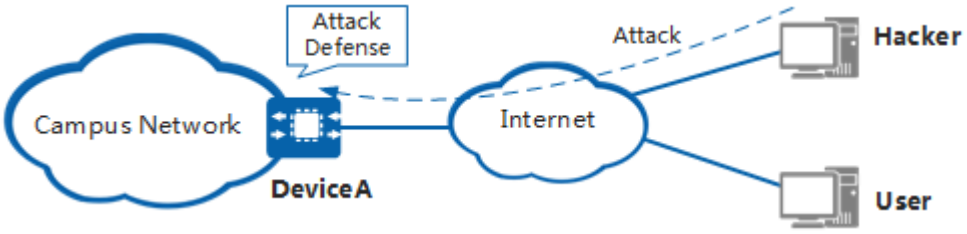
8.13 本机防攻击配置举例

8.13.1 举例：配置攻击防范

组网需求

如图1所示，如果DeviceA受到来自Internet网络不同类型的网络攻击，如畸形报文攻击、分片报文攻击和泛洪攻击，将会造成DeviceA瘫痪。为了预防这种情况，管理员希望通过在DeviceA上部署各种攻击防范措施来为用户提供安全的网络环境，保障正常的网络服务。

图 8-14 配置畸形报文攻击、分片报文攻击与泛洪攻击防范组网图



操作步骤

步骤1 配置畸形报文攻击防范。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] anti-attack abnormal enable
```

步骤2 配置分片报文攻击防范，分片报文的限制速率为15000bit/s。

```
[DeviceA] anti-attack fragment enable
[DeviceA] anti-attack fragment car cir 15000
```

步骤3 配置泛洪攻击防范。

配置TCP SYN泛洪攻击防范，TCP SYN报文的限制速率为15000bit/s。

```
[DeviceA] anti-attack tcp-syn enable
[DeviceA] anti-attack tcp-syn car cir 15000
```

配置UDP泛洪攻击防范，对特定端口发送的UDP报文直接丢弃。

```
[DeviceA] anti-attack udp-flood enable
```

配置ICMP泛洪攻击防范，ICMP泛洪报文的限制速率为15000bit/s。

```
[DeviceA] anti-attack icmp-flood enable
[DeviceA] anti-attack icmp-flood car cir 15000
```

----结束

检查配置结果

配置完成后，可以通过执行命令**display anti-attack statistics**查看报文攻击防范的统计数据。

```
<DeviceA> display anti-attack statistics
Packets Statistic Information:
-------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum       DropPacketNum       PassPacketNum
             (H)       (L)       (H)       (L)       (H)       (L)
-------------------------------------------------------------------------------
Abnormal     0         0         0         0         0         0
```

```
Fragment     0         0         0         0         0         0
Icmp-flood   0         0         0         0         0         0
Tcp-syn      0        58         0         0         0        58
Udp-flood    0         0         0         0         0         0
------------------------------------------------------------------------------
```

配置文件

DeviceA的配置文件

```
#
sysname DeviceA
#
anti-attack abnormal enable
anti-attack fragment enable
anti-attack fragment car cir 15000
anti-attack tcp-syn enable
anti-attack tcp-syn car cir 15000
anti-attack udp-flood enable
anti-attack icmp-flood enable
anti-attack icmp-flood car cir 15000
#
return
```

8.14 常见配置错误

8.14.1 攻击溯源功能不生效

故障现象

配置了攻击溯源功能后，攻击溯源功能不生效。

可能原因

本类故障的常见原因主要包括：

- 配置攻击溯源的防攻击策略没有被应用。
- 攻击溯源的检测阈值过大造成设备不认为该报文为攻击报文。

操作步骤

1. 执行命令**display current-configuration**，确定防攻击策略是否被应用。
   - 如果显示信息中包含配置**cpu-defend-policy**，则表示已应用了防攻击策略。此时，执行步骤2。
   - 如果显示信息中没有配置**cpu-defend-policy**，则表示防攻击策略没有被应用。此时，需要在系统视图下执行命令**cpu-defend-policy**，应用防攻击策略。
2. 检查攻击溯源检测阈值是否过大。

   执行命令**display auto-defend configuration**查看“auto-defend threshold”字段取值。如果攻击溯源的检查阈值较大，则在防攻击策略视图下执行命令**auto-defend threshold**命令减小攻击溯源的检查阈值。

8.14.2 协议报文没有上送 CPU

故障现象

配置了CPU防攻击功能后，协议报文没有上送CPU。

可能原因

本类故障的常见原因主要包括：

- 配置了匹配协议报文且动作为丢弃的规则（如针对该类协议报文的上送规则为deny）。
- 非法报文攻击CPU，导致协议报文无法上送。

操作步骤

1. 检查设备上是否配置了匹配协议报文且动作为丢弃的规则。
   a. 在系统视图下，执行命令**display current-configuration**，查看配置的防攻击策略。
   b. 然后执行命令**display cpu-defend policy** [*policy-name*]，检查防攻击策略下是否配置了针对此协议报文的上送CPU规则是否为**deny**。

      如果针对此协议报文的上送CPU规则为**deny**，请在防攻击策略视图下执行命令**car**，将上送规则修改为CAR。

      如果针对此协议报文的上送CPU规则不是**deny**，请继续执行以下检查。
2. 检查上送CPU的统计信息。

   执行命令**display cpu-defend statistics**，检查上送CPU的统计信息。如果有大量协议报文被丢弃，则该协议报文可能为非法攻击报文，请分析报文是否为非法攻击报文（如通过攻击溯源功能），如果确定是非法攻击报文，请使用流策略阻止此协议报文上送CPU。

9 风暴抑制配置

9.1 风暴抑制简介

定义

风暴抑制是用于控制广播、未知组播以及未知单播报文，防止这类报文引起广播风暴的安全技术。

风暴抑制包括流量抑制和风暴控制两个子功能：

- 流量抑制通过配置阈值来限制广播、未知组播未知单播报文的速率。当流量超过阈值时，系统将丢弃多余的流量，阈值范围内的报文可以正常通过，从而将流量限制在合理的范围内。此外，流量抑制还支持对接口出方向的流量进行阻塞。
- 风暴控制通过阻塞报文或关闭接口来阻断广播、未知组播或未知单播报文的流量。此外，风暴控制还支持通过抑制报文来控制报文的平均速率。当流量超过指定的阈值时，系统会执行对应的风暴控制动作。

流量抑制和风暴控制功能均用于控制广播风暴，二者之间的对比如**表9-1**所述。

表 9-1 流量抑制和风暴控制对比

对比项	流量抑制	风暴控制
流量控制机制	• 如果配置接口出方向的流量抑制功能，系统将直接阻塞对应报文类型的流量。 • 其他情况下，系统将丢弃超过阈值的流量，阈值范围内的报文可以正常通过。	• 如果风暴控制的动作是抑制报文，当接口上接收的报文平均速率超过配置的高阈值时，系统将丢弃超额的流量，直至报文平均速率不超过该阈值。 • 其他情况下，当流量超过指定的阈值时，系统会阻塞该接口收到的流量或者直接将该接口关闭。
流量检测机制	• 基于芯片进行检测。 • 流量超过阈值，流量抑制功能立即生效。	• 基于软件进行检测。 • 在检测时间间隔内，报文平均速率超过阈值，风暴控制功能生效。

说明

本设备仅支持流量抑制功能。

目的

当设备某个二层以太网接口收到广播、未知组播或未知单播报文时，如果根据报文的目的MAC地址设备不能明确报文的出接口，设备会向同一VLAN内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低设备转发性能。

风暴抑制特性中的流量抑制和风暴控制功能，可以有效地控制这几类报文流量。

9.2 风暴抑制配置注意事项

License 依赖

风暴抑制无需License许可即可使用。

硬件依赖

表 9-2 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 9-3 本特性的使用限制

特性	特性限制	系列	涉及产品
流量抑制	当在VLAN上配置流量抑制时，如果VLAN包含的接口属于N个芯片，则实际流量抑制的阈值为所配置的流量抑制阈值的N倍。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8
流量抑制	流量抑制只对二层流量生效。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8

9.3 风暴抑制缺省配置

风暴抑制的缺省配置如表9-4所示。

表 9-4 风暴抑制缺省配置

参数	缺省配置
接口入方向的流量抑制功能	已启用
接口入方向的流量抑制方式	百分比方式
百分比抑制比例值	• 广播报文的流量抑制：10% • 未知组播报文、未知单播报文的流量抑制：100% • MAC漂移联动未知单播流量抑制：1%

参数	缺省配置
接口出方向的流量抑制功能	未启用
VLAN的流量抑制功能	未启用
ICMP报文的流量抑制功能	已启用
ICMP报文接口限速阈值	1500pps
MAC漂移联动流量抑制功能	已启用
MAC漂移联动流量抑制的方式	百分比方式

9.4 配置流量抑制

9.4.1 了解流量抑制

流量抑制按以下三种形式来限制广播、未知组播或未知单播报文：

- 在接口视图下，入方向上，设备支持对广播、未知组播及未知单播报文按百分比或报文速率进行流量抑制。

  设备监控接口下的各类报文速率，当入口流量超过配置的阈值时，设备会丢弃超额的流量。
- 在接口视图下，出方向上，设备支持对广播、未知组播和未知单播报文的阻塞。
- 在VLAN视图下，设备支持对广播、未知组播和未知单播报文按比特速率进行流量抑制。

  设备监控同一VLAN内各类报文的速率，当VLAN内流量超过配置的阈值时，设备会丢弃超额的流量。

此外，设备支持以下流量抑制相关功能：

- ICMP报文流量抑制。通过指定限速阈值对ICMP报文进行限速，防止大量ICMP报文上送CPU处理，导致其他业务功能异常。
- MAC漂移联动流量抑制。在设备开启MAC漂移检测功能后，若检测到MAC地址发生漂移，将触发对漂移端口的流量抑制功能。

9.4.2 配置接口入方向的流量抑制

背景信息

为了防止广播风暴，可以配置接口入方向的流量抑制。设备支持对广播、未知组播或未知单播报文按百分比或报文速率进行流量抑制。当广播、未知组播或未知单播流量超过配置的阈值时，系统将丢弃超额的流量，使流量降低到合理的范围内。

操作步骤

步骤1 进入系统视图。

```
system-view
```


步骤2 进入接口视图。

```
interface interface-type interface-number
```

步骤3 配置接口从三层模式切换到二层模式。

```
portswitch
```

请用户根据实际接口类型自行选择是否要执行此步骤。

步骤4 配置接口入方向的流量抑制。

```
storm suppression { broadcast | multicast | unknown-unicast } { percent-value | cir cir-value [ gbps | kbps | mbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] ] | packets packets-per-second }
```

如果对同一类型报文多次配置接口入方向的流量抑制，且分别指定参数*percent-value*和**cir** *cir-value*，那么只有最后配置的命令会生效。

----结束

检查配置结果

执行命令**display storm suppression** { **broadcast** | **multicast** | **unknown-unicast** } [**interface** *interface-type interface-number*]命令，查看接口入方向的流量抑制配置阈值和实际生效的阈值。

说明

流量抑制的限速阈值与实际限速效果之间存在误差，请以报文实际通过的速率为准。

9.4.3 配置接口出方向的流量抑制

背景信息

对于某些下接网络不希望接收任何广播、未知组播或未知单播流量的接口（比如此接口下的用户较为固定，且对安全性要求较高），可以配置接口出方向的流量抑制，将该接口的广播、未知组播或未知单播报文完全阻断。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 进入接口视图。

```
interface interface-type interface-number
```

步骤3 配置接口从三层模式切换到二层模式。

```
portswitch
```

请用户根据实际接口类型自行选择是否要执行此步骤。

步骤4 配置接口出方向的流量抑制。

```
storm suppression { broadcast | multicast | unknown-unicast } block outbound
```

----结束

9.4.4 配置 VLAN 的流量抑制

背景信息

为了限制进入VLAN的广播、未知组播或未知单播类型报文的速率，防止广播风暴，可以在该VLAN内配置对应报文类型的流量抑制功能，超过限制速率的报文将被丢弃。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 进入VLAN视图。

```
vlan vlan-id
```

步骤3 配置VLAN的流量抑制。

```
storm suppression { broadcast | multicast | unknown-unicast } cir cir-value [ gbps | kbps | mbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] ]
```

----结束

9.4.5 配置 MAC 漂移联动流量抑制

背景信息

在设备开启MAC漂移检测功能后，若检测到MAC地址发生漂移，将触发对漂移接口的流量抑制功能。通过配置MAC漂移联动流量抑制，可以按照承诺信息速率CIR或百分比指定流量抑制的阈值，并可以使报文强制按照MAC漂移联动流量抑制的阈值进行转发。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 配置MAC漂移联动流量抑制的阈值。

```
storm suppression mac-address flapping { percent-value | cir cir-value [ kbps | mbps | gbps ] } [ force ]
```

缺省情况下，MAC漂移联动流量抑制的阈值按照百分比进行配置，比例值为1%。

说明

当接口发生MAC地址漂移且配置了相应接口的流量抑制功能时：

- 若已配置该命令且已指定**force**参数，那么MAC漂移联动流量抑制功能生效。
- 若未配置该命令行或未指定**force**参数，那么接口的流量抑制功能生效。

----结束

9.4.6 举例：配置接口入方向的流量抑制

组网需求

如图9-1所示，DeviceA作为二层网络到三层设备的衔接点，需要通过接口入方向的流量抑制功能限制二层网络转发的广播、未知组播和未知单播报文，防止产生广播风暴。

图 9-1 配置接口入方向的流量抑制组网图

说明

本例中interface1代表10GE0/0/1。

操作步骤

步骤1 进入接口视图。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] portswitch
```

步骤2 配置广播流量抑制，按承诺信息速率CIR进行抑制，限制广播报文的最大速率为100kbit/s。

```
[DeviceA-10GE0/0/1] storm suppression broadcast cir 100
```

步骤3 配置未知组播流量抑制，按百分比（即报文速率和接口速率的比值）抑制，百分比值为80%。

```
[DeviceA-10GE0/0/1] storm suppression multicast 80
```

步骤4 配置未知单播流量抑制，按承诺信息速率CIR进行抑制，限制未知单播报文的最大速率为100kbit/s。

```
[DeviceA-10GE0/0/1] storm suppression unknown-unicast cir 100
[DeviceA-10GE0/0/1] quit
```

----结束

检查配置结果

查看接口入方向流量抑制的配置信息。

```
[DeviceA] display storm suppression broadcast interface 10ge 0/0/1
-------------------------------------------------------------------------------
                    Configured                          Current
interface       percent(%) cir(kbps) cbs(bytes)    pps percent(%) cir(kbps) cbs(bytes)     pps
-------------------------------------------------------------------------------
10GE0/0/1               --      100      18800     --         --      100      18800      --
-------------------------------------------------------------------------------
[DeviceA] display storm suppression multicast interface 10ge 0/0/1
-------------------------------------------------------------------------------
                    Configured                          Current
interface       percent(%) cir(kbps) cbs(bytes)    pps percent(%) cir(kbps) cbs(bytes)     pps
-------------------------------------------------------------------------------
10GE0/0/1               80       --       --      --         80       --       --      --
-------------------------------------------------------------------------------
```

```
[DeviceA] display storm suppression unknown-unicast interface 10ge 0/0/1
-------------------------------------------------------------------------------------------------
                        Configured                          Current
interface       percent(%) cir(kbps) cbs(bytes)    pps percent(%) cir(kbps) cbs(bytes)     pps
-------------------------------------------------------------------------------------------------
10GE0/0/1               --      100      18800     --        --      100      18800      --
-------------------------------------------------------------------------------------------------
```

其中，**Configured**字段显示已配置的流量抑制百分比值、承诺信息速率和承诺突发尺寸，**Current**字段显示实际生效的流量抑制百分比值、承诺信息速率和承诺突发尺寸。可以看出，DeviceA的接口10GE0/0/1在入方向限制广播报文的最大速率为100kbit/s，限制未知组播报文速率和接口速率的比值不超过80%，限制未知单播报文的最大速率为100kbit/s。

配置脚本

DeviceA

```
#
sysname DeviceA
#
interface 10GE0/0/1
 portswitch
 storm suppression broadcast cir 100 kbps
 storm suppression multicast 80
 storm suppression unknown-unicast cir 100 kbps
#
return
```

9.5 风暴抑制常见配置错误

9.5.1 接口入方向的流量抑制无效

故障现象

接口配置了广播、未知组播或未知单播报文的流量抑制功能后，仍然出现了对应类型的报文引起的广播风暴，导致正常流量中断。

可能原因

- 接口下没有配置对应类型报文的流量抑制或者配置的流量抑制阈值过大。
- 对应类型的报文在入接口没有被丢弃。

操作步骤

步骤1 检查接口入方向的流量抑制配置。

- 任意视图下执行命令**display storm suppression** { **broadcast** | **multicast** | **unknown-unicast** } [**interface** *interface-type interface-number*]查看流量抑制信息，或者在接口视图下使用命令**display this**查看该接口的流量抑制配置信息。
  a. 检查有无配置对应类型报文的流量抑制。
  b. 确认流量抑制阈值是否过大：
     - 如果流量抑制阈值过大，请在接口视图下执行命令**storm suppression** { **broadcast** | **multicast** | **unknown-unicast** } { *percent-value* | **cir** *cir-*

value [**gbps** | **kbps** | **mbps**] [**cbs** *cbs-value* [**bytes** | **kbytes** | **mbytes**]] | **packets** *packets-per-second* }修改流量抑制参数。

- 如果流量抑制阈值合适，请继续执行以下检查。

步骤2 检查报文在接口入方向是否被丢弃。有以下两种方法：

- 用户视图下执行命令**display interface** *interface-type interface-number*，查看输出信息中输出带宽占用率是否在抑制前后有较大变化。正常情况下，在配置流量抑制之后，接口丢弃超过阈值限制的报文，接口带宽利用率会降低。如果没有变化或变化很小，请执行后续步骤。
- 准备另外一个接口B，将要检查的接口A（即配置流量抑制的接口）和接口B加入相同VLAN，查看接口B的出方向流量是否为接口A上配置的抑制后的流量。如果不是，说明报文没有在接口A的入方向被丢弃。请执行后续步骤。

步骤3 请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

10 URPF 配置

10.1 URPF 简介

定义

URPF（Unicast Reverse Path Forwarding）是单播逆向路径转发的简称，其主要功能是防止基于源IP地址欺骗的网络攻击行为。

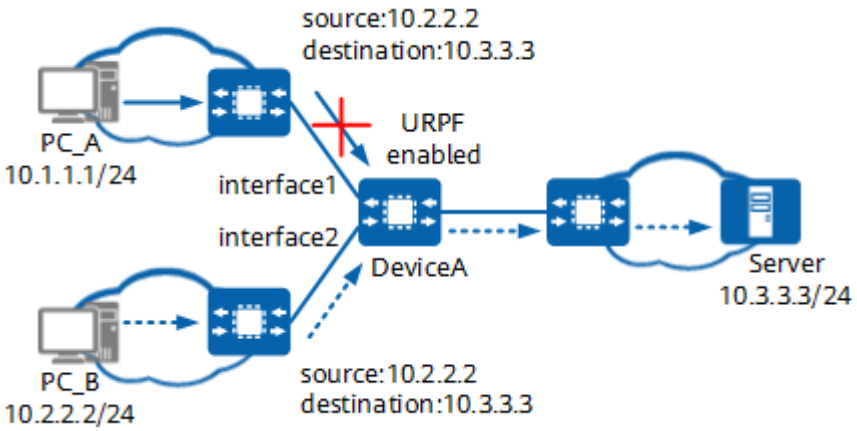
URPF根据报文的源IP地址查找FIB（Forwarding Information Base）表中是否存在去往该地址的路由，并判断报文入接口与路由出接口是否一致。如果FIB表不存在去往该源IP地址的路由或报文入接口与路由出接口不一致，则丢弃该报文，从而有效防范网络中通过修改报文源IP地址而进行恶意攻击行为的发生。

目的

拒绝服务DoS（Denial of Service）攻击是一种阻止连接服务的网络攻击，它的攻击方式有很多种，最基本的DoS攻击就是利用大量合法或伪造的请求占用过多的服务资源，从而使合法用户无法得到正常服务，URPF技术针对伪造源IP地址的DoS攻击非常有效。

如**图10-1**所示，PC_A伪造源地址为10.2.2.2的报文，向Server发起请求，若DeviceA上没有开启URPF功能，Server在收到请求报文后会向PC_B（10.2.2.2）发送回应报文，PC_A发起的这种伪造报文对Server和PC_B都造成攻击。若在DeviceA上开启了URPF功能，DeviceA在接收到这个报文后，检查其入接口是否匹配，发现源地址为10.2.2.2的报文应该从interface2进入，则DeviceA认为该报文源地址是伪造的，直接丢弃该报文。而从PC_B发向Server的正常报文，检查通过后，被正常转发。

图 10-1 URPF 防止基于源地址欺骗示意图



10.2 URPF 原理描述

工作模式

在复杂的网络环境中，会遇到对端设备记录的路由路径与本端不一致的情况，此时使能URPF的设备可能会丢弃从合法路径接收的报文，为了解决该问题，设备实现了两种URPF模式：

- **严格模式**

  严格模式下，设备不仅要求FIB表中存在去往报文源IP地址的路由，还要求报文入接口与路由出接口一致。

  建议在对端与本端记录的路由路径一致的环境下使用严格模式。例如两台网络边界设备之间只有一条路径，此时使用严格模式能够保证网络的安全性。

- **松散模式**

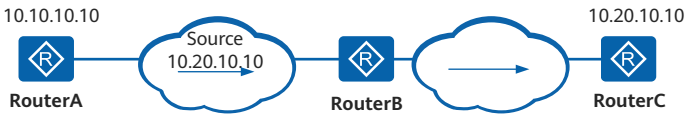
  松散模式下，设备仅要求FIB表中存在去往报文源IP地址的路由，不要求报文入接口与路由出接口一致。

  建议在不能保证对端与本端记录的路由路径一致的环境下使用松散模式。例如两个网络边界设备之间有多条路径，此时松散模式既可以有效地阻止网络攻击，又可以避免合法报文被错误丢弃。

工作机制

URPF通过获取报文的源地址和入接口，在FIB表中查找源地址对应的接口是否与入接口匹配。如果不匹配，则认为源地址是伪装的，丢弃该报文。通过这种工作方式，URPF能有效地防范网络中通过修改源地址而进行的恶意攻击行为。

图 10-2 URPF 原理



如图10-2所示，在RouterA上伪造源地址为10.20.10.10的报文向RouterB发起请求，RouterB响应请求时将向真正的“10.20.10.10”即RouterC发送报文。这种非法报文对RouterB和RouterC都造成了攻击。

如果在RouterB上启用URPF严格检查，则RouterB在收到源地址为10.20.10.10的报文时，URPF检查到以此报文源地址对应的接口与收到该报文的接口不匹配，报文会被丢弃。

应用场景

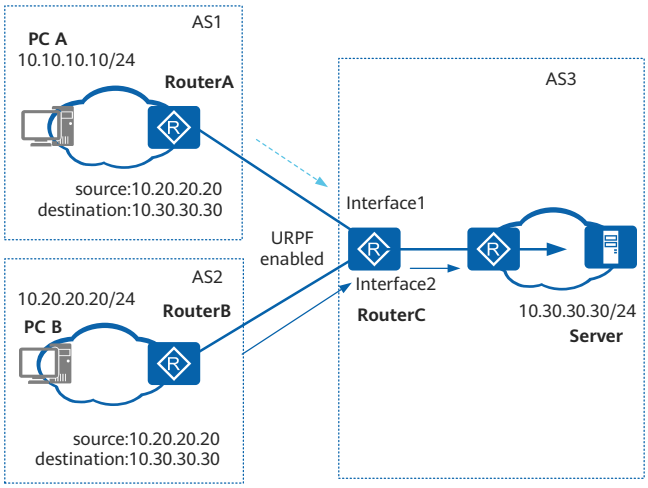
- 严格模式下的URPF应用

  如图10-4所示，AS1和AS2与AS3之间为单连接。在RouterC的Interface1接口和Interface2接口上配置URPF，可以保护AS3免受来自AS1和AS2的源地址欺骗攻击。

  如果AS1中的主机PC A伪造了一个源地址为10.20.20.20的报文，向AS3中的Server发送请求。RouterC在接收到这个报文后，检查其入接口是否匹配，发现源地址为10.20.20.20的报文应该从Interface2进入，则RouterC认为该报文源地址是伪造的，直接丢弃该报文。

  从AS2发向Server的正常报文，检查通过后，被正常的转发。

图 10-3 URPF 单宿主客户应用环境示意图

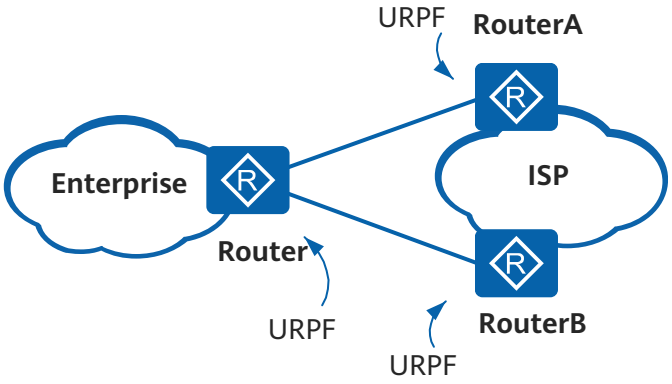


- 松散模式下的URPF应用

  两个网络边界设备之间多个连接有单宿主单ISP客户和多宿主多ISP客户两种情况。

  – 单宿主单ISP客户

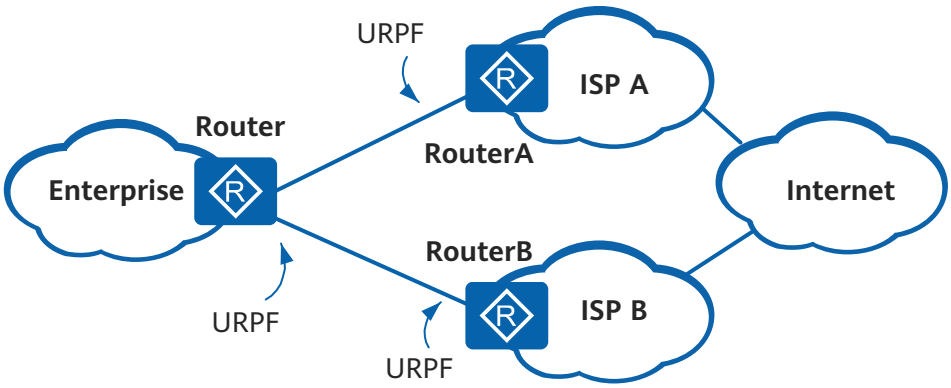
图 10-4 URPF 单宿主单 ISP 客户应用环境示意图



如图10-4所示，为了保证可靠性，某公司网络和某个ISP之间有两条连接。这时就不能够保证Enterprise和ISP之间路由的对称性，必须使用URPF松散模式。

- 多宿主多ISP客户

图 10-5 URPF 多宿主多 ISP 客户应用环境示意图



在图10-5所示环境中，客户与多个ISP连接，很难保证Enterprise和两个ISP之间路由的对称性，必须使用URPF松散模式。

客户与多个ISP连接下的URPF可以具有以下应用：

如果用户希望某些特殊报文任何情况都可以通过URPF的检查，可以在利用ACL指定这些特殊的源地址允许通过。

许多用户连接的设备可能只有一条缺省路由指向ISP，此时，需要配置允许匹配缺省路由选项。

10.3 URPF 配置注意事项

License 依赖

URPF无需License许可即可使用。

硬件依赖

表 10-1 支持本特性的硬件

系列	支持产品

特性限制

无

10.4 URPF 缺省配置

URPF的缺省配置如表10-2所示。

表 10-2 URPF 缺省配置

参数	缺省值
URPF检查功能	未使能

10.5 配置 URPF

前提条件

在配置URPF之前，需完成以下任务：

- 配置接口的链路层属性。
- 配置接口的IP地址。
- 如果使用ACL作为匹配规则，配置URPF所针对报文的ACL。

背景信息

URPF检查分为严格模式和松散模式，并通过配置参数**allow default-route**允许报文匹配的路由为缺省路由。若报文被拒绝，则进行ACL匹配。

URPF的处理流程如下：

1. 如果报文的源地址在设备的FIB表中存在。
   - 严格模式下，反向查找报文出接口，若只有一个出接口和报文的入接口一一匹配，则报文通过检查；否则报文将被丢弃。当有多个出接口和报文的入接口相匹配时，必须使用松散模式。（反向查找是指查找以该报文源IP地址为目的IP地址的报文的出接口。）
   - 松散模式下，若报文的源地址在设备的FIB表中存在（无论反向查找的出接口和报文的入接口是否一致），报文就通过检查；否则报文将被丢弃。
2. 如果报文的源地址在设备的FIB表中不存在，则检查是否配置了缺省路由及URPF的**allow default-route**参数。

- 对于配置了缺省路由，但没有配置参数**allow default-route**的情况。

  无论是严格模式还是松散模式，只要报文的源地址在设备的FIB表中不存在，该报文都会被拒绝。

- 对于配置了缺省路由，同时又配置了参数**allow default-route**的情况。

  - 严格模式下，当缺省路由的出接口与报文入接口一致时，报文通过URPF的检查，被正常转发；否则报文被拒绝。
  - 松散模式下，报文通过URPF的检查，被正常转发。

3. 当且仅当报文被拒绝后，才去匹配ACL。如果ACL允许通过，则报文被正常转发；如果被ACL拒绝，则报文被丢弃。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 进入接口视图。

```
interface interface-type interface-number
```

步骤3 将接口从二层模式切换到三层模式。

```
undo portswitch
```

请用户根据实际接口类型自行选择是否要执行此步骤。

步骤4 配置对接口的报文进行URPF检查。支持基本ACL和高级ACL（编号范围为2000~3999）。

IPv4网络：

```
ip urpf { loose | strict } [ allow default-route ] [ acl acl-number ]
```

IPv6网络：

```
ipv6 urpf { loose | strict } [ allow default-route ] [ acl6 acl-number ]
```

说明

如果需要配置对接口的IPv6报文进行URPF检查的功能，需要先使能接口的IPv6功能。请在接口视图下执行命令**ipv6 enable**。

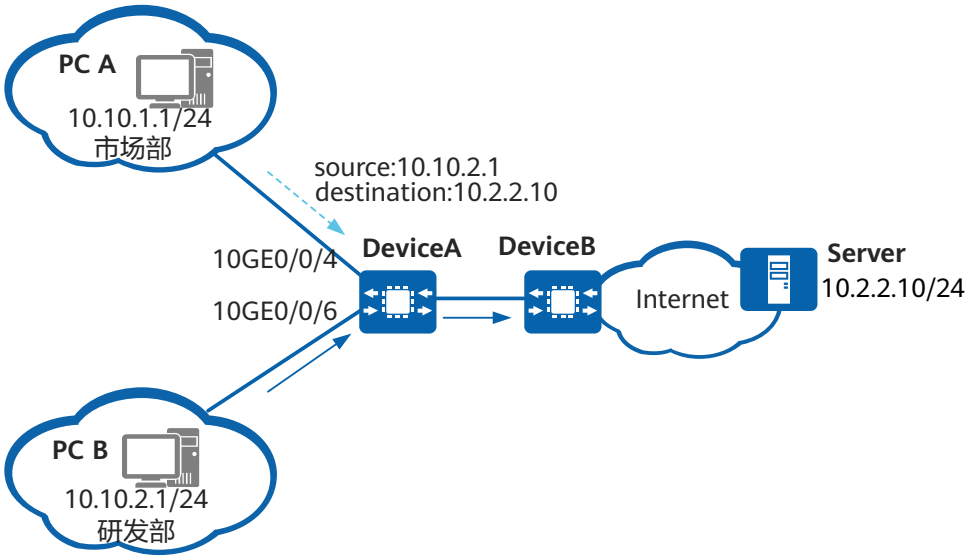
----结束

10.6 举例：配置 URPF 功能

组网需求

如图10-6所示，某企业研发部和市场部通过接口10GE0/0/6和接口10GE0/0/4与DeviceA连接，DeviceA与外部的某个Server之间路由可达，研发部员工和市场部员工都可以通过DeviceA访问该Server。公司希望在DeviceA上进行配置，防止不同部门的员工利用源IP地址欺骗的方法超越权限，非法获取Server的服务。

图 10-6 配置 URPF 组网图



配置思路

该组网的配置思路如下：

在接口10GE0/0/4和接口10GE0/0/6配置URPF功能，并允许对缺省路由进行特殊处理。

操作步骤

步骤1 配置接口的URPF检查模式

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/4
[DeviceA-10GE0/0/4] ip urpf strict allow default-route
[DeviceA-10GE0/0/4] ip address 10.10.1.5 24
[DeviceA-10GE0/0/4] quit
[DeviceA] interface 10ge 0/0/6
[DeviceA-10GE0/0/6] ip address 10.10.2.5 24
[DeviceA-10GE0/0/6] ip urpf strict allow default-route
```

步骤2 验证配置结果

在10GE0/0/4接口视图下执行命令**display this**查看URPF配置。

```
[DeviceA-10GE0/0/4] display this
#
interface 10GE 0/0/4
 ip address 10.10.1.5 255.255.255.0
 ip urpf strict allow default-route
#
return
```

在10GE0/0/6接口视图下执行命令**display this**查看URPF配置。

```
[DeviceA-10GE0/0/6] display this
#
interface 10GE 0/0/6
 ip address 10.10.2.5 255.255.255.0
 ip urpf strict allow default-route
```

```
#
return
```

----结束

配置文件

DeviceA的配置文件

```
#
sysname DeviceA
#
interface 10GE0/0/4
 ip address 10.10.1.5 255.255.255.0
 ip urpf strict allow default-route
#
interface 10GE0/0/6
 ip address 10.10.2.5 255.255.255.0
 ip urpf strict allow default-route
#
return
```

11 业务和管理隔离配置

背景信息

为了保证设备的网络安全性，本着最小化攻击面的原则，设备遵循X.805的三层三面安全隔离机制：

- 管理平面：承载设备的操作维护数据流，也称为O&M平面。
- 控制平面：承载设备协议交互的数据流，也称为信令平面。
- 业务平面：承载设备信息转发的数据流，也称为转发平面或用户平面。

三面隔离后，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和安全。例如，业务平面受到DoS攻击，不会影响管理平面，此时管理员可以通过管理平面登录来解决问题；如果不隔离，数据平面的处理任务会进一步占用CPU、内存等资源直至耗尽，导致管理员无法对设备进行管理。

业务平面与管理平面的隔离，即是业务接口流量与管理接口流量的隔离，其实现原理是：

- 禁止从业务接口上送管理数据，业务网络的用户无法通过业务接口访问设备管理接口连接的管理网络，实现业务接口与管理接口的物理隔离。
- 业务接口和管理接口分别绑定不同的VPN，数据不能互访，实现业务接口与管理接口的逻辑隔离。

操作步骤

- 使能业务平面与管理平面的隔离功能，禁止从业务平面上送管理数据。

  ```
  system-view
  undo management-plane isolate disable
  ```

  缺省情况下，设备的隔离功能默认使能。
- 配置业务接口和管理接口分别绑定不同的VPN，确保数据不能互访。
  a. 创建并配置VPN实例**management**。

     ```
     system-view
     ip vpn-instance management
      ipv4-family
      quit
     ```

     此处实例名称以**management**为例代表管理平面的VPN，实际配置时可以自己定义。
  b. 创建并配置VPN实例**service**。


```
ip vpn-instance service
 ipv4-family
 quit
```

此处实例名称以**service**为例代表业务平面的VPN，实际配置时可以自己定义。

c. 将管理接口绑定到**management**；将业务接口绑定到**service**。

```
interface meth 0/0/0
 ip binding vpn-instance management
 quit
interface interface-type interface-number
 ip binding vpn-instance service
 quit
```

说明

- 建议根据业务实际需求，将业务接口绑定不同的VPN实例，即具体的业务只被绑定到必须的业务接口，实现更细粒度的业务隔离。
- 管理设备使用的LoopBack逻辑接口，也可以绑定到**management**。
- 若需隔离IPv6网络，需要在VPN实例视图下执行**ipv6-family** [**unicast**]命令使能VPN实例的IPv6地址族。

----结束

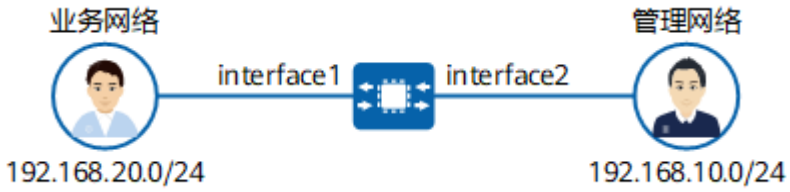
任务示例

如图11-1所示，192.168.20.0/24网段的业务网络和设备的业务接口interface1相连；192.168.10.0/24网段的管理网络和设备的管理接口interface2相连。在设备上采用VPN逻辑隔离的配置方式来实现业务平面与管理平面的隔离，防止出现192.168.20.0/24可以Ping通192.168.10.0/24的现象，避免设备因管理接口地址泄露而遭受攻击。

图 11-1 业务与管理隔离示例组网图

说明

本例中interface1、interface2分别代表10GE0/0/1、MEth0/0/0。



本例中设备的配置脚本：

```
#
ip vpn-instance management
 ipv4-family
#
ip vpn-instance service
 ipv4-family
#
interface MEth0/0/0
 ip binding vpn-instance management
 ip address 192.168.10.1 255.255.255.0
#
interface 10GE0/0/1
 ip binding vpn-instance service
 ip address 192.168.20.1 255.255.255.0
```

```
#
return
```


12 PKI 配置

12.1 PKI 简介

定义

公钥基础设施PKI（Public Key Infrastructure），是一种遵循既定标准的证书管理平台，它利用公钥技术为所有网络应用提供安全服务。PKI技术是信息安全技术的核心，也是电子商务的关键和基础技术。

目的

随着网络技术和信息技术的发展，电子商务已逐步被人们所接受，并得到不断普及。但通过网络进行电子商务交易时，存在如下问题：

- 交易双方并不现场交易，无法确认双方的合法身份。
- 通过网络传输时信息易被窃取和篡改，无法保证信息的安全性。

- 交易双方发生纠纷时没有凭证可依，无法提供仲裁。

为了解决上述问题，PKI技术应运而生，其利用公钥技术保证在交易过程中能够实现身份认证、保密、数据完整性和不可否认性。因而在网络通信和网络交易中，特别是电子政务和电子商务业务，PKI技术得到了广泛的应用。

受益

- 通过PKI证书认证技术，用户可以验证其他设备的合法性，从而可以保证用户接入安全、合法的网络中。
- 通过PKI加密技术，可以保证网络中传输数据的安全性，数据不会被窥探。
- 通过PKI签名技术，可以保证网络中传输数据的安全性，数据不会被篡改。
- 企业可以防止非法用户接入企业网络中。
- 企业分支之间可以建立安全通道，保证企业数据的安全性。

12.2 PKI 原理描述

12.2.1 PKI 基本概念

12.2.1.1 加密

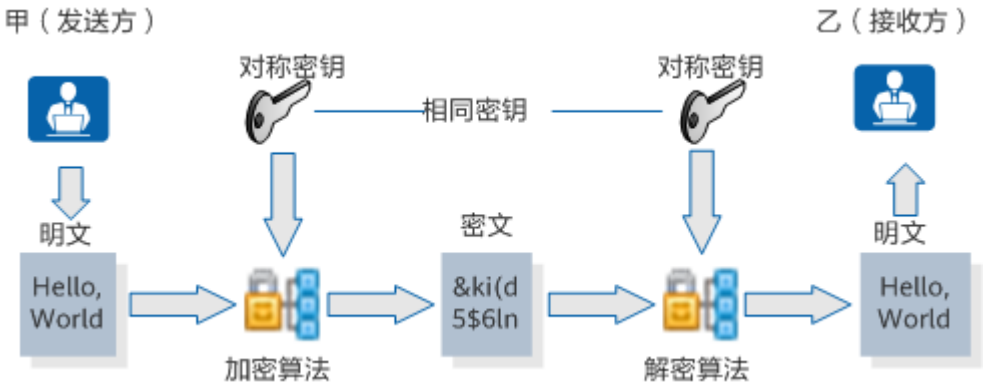
加密是通过网络传输信息的基础。通俗地讲，加密就是利用数学方法将明文（需要被隐蔽的数据）转换为密文（不可读的数据），从而达到保护数据的目的。

对称密钥加密

对称密钥加密又称共享密钥加密，是指使用同一个密钥对数据进行加密和解密。

对称密钥的加解密过程如图12-1所示。

图 12-1 对称密钥加解密过程示意图



甲和乙事先协商好对称密钥，具体加解密过程如下：

1. 甲使用对称密钥对明文加密，并将密文发送给乙。
2. 乙接收到密文后，使用对称密钥对密文解密，得到最初的明文。

   对称密钥加密的优点是效率高、算法简单、系统开销小，适合加密大量数据。缺点是实现困难且扩展性差，实现困难的原因在于进行安全通信前需要以安全方式

进行密钥交换；扩展性差表现在每两个通信用户之间都需要协商密钥，n个用户就需要协商n*(n-1)/2个不同的密钥。

目前比较常用的对称密钥加密算法主要包含DES（Data Encryption Standard）、3DES（Triple Data Encryption Standard）和AES（Advance Encrypt Standard）算法。

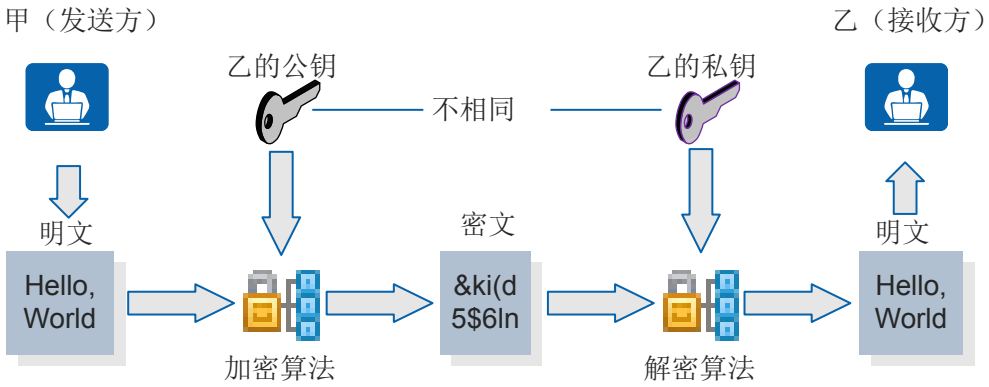
公钥加密

公钥加密又称非对称密钥加密，它使用了两个不同的密钥：一个可对外界公开，称为“公钥”；一个只有所有者知道，称为“私钥”。

公钥加密解决了对称密钥的发布和管理问题，一个用于加密信息，另一个用于解密信息，通信双方无需事先交换密钥就可进行保密通信。通常以公钥作为加密密钥，以私钥作为解密密钥。由于其他人没有对应的私钥，发送的加密信息仅该用户可以解读，从而实现信息的加密传输。

公钥加解密的过程如图12-2所示。

图 12-2 公钥加解密过程示意图



甲事先获得乙的公钥，具体加解密过程如下：

1. 甲使用乙的公钥对明文加密，并将密文发送给乙。
2. 乙收到密文后，使用自己的私钥对密文解密，得到最初的明文。

公钥加密的优点是无法从一个密钥推导出另一个密钥；公钥加密的信息只能用私钥进行解密。缺点是算法非常复杂，导致加密大量数据所用的时间较长，而且加密后的报文较长，不利于网络传输。

基于上述优缺点，公钥加密适合对密钥或身份信息等敏感信息加密，在安全性上满足用户的需求。

目前比较常用的公钥加密算法主要包含DH（Diffie-Hellman）、RSA（Ron Rivest、Adi Shamirh、LenAdleman）和DSA（Digital Signature Algorithm）算法。

12.2.1.2 数字信封和数字签名

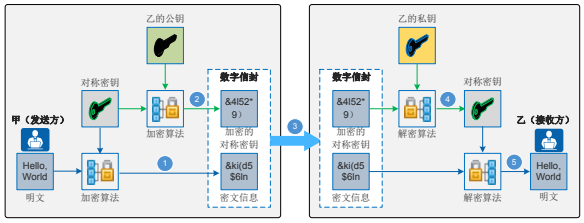
数字信封

数字信封是指发送方采用接收方的公钥加密对称密钥后与密文组合在一起所得的数据。采用数字信封时，接收方需要使用自己的私钥才能打开数字信封，得到对称密

钥。数字信封技术结合了对称密钥加密和公钥加密的优点，解决了对称密钥发布和公钥加密速度慢等问题，提高了安全性、扩展性和网络传输效率。

数字信封的加解密过程如图12-3所示。

图 12-3 数字信封的加解密过程示意图



甲事先获得乙的公钥，具体加解密过程如下：

1. 甲使用对称密钥对明文进行加密，生成密文信息。
2. 甲使用乙的公钥加密对称密钥，生成数字信封。
3. 甲将数字信封和密文信息一起发送给乙。
4. 乙接收到甲的加密信息后，使用自己的私钥打开数字信封，得到对称密钥。
5. 乙使用对称密钥对密文信息进行解密，得到最初的明文。

从加解密的过程中可以发现，其实数字信封技术也存在问题，如果攻击者拦截甲的信息，用自己的对称密钥加密伪造的信息，并用乙的公钥加密自己的对称密钥，然后发送给乙。乙收到加密信息后，解密得到的明文会被误认为是甲发送的信息。此时，需要一种方法确保接收方收到的信息就是指定的发送方发送的。

数字签名

数字信封无法保证接收方收到的信息就是指定的发送方发送的，数字签名可以解决这个问题。它不但可以验证信息是否被篡改，还可以证明发送方的身份。

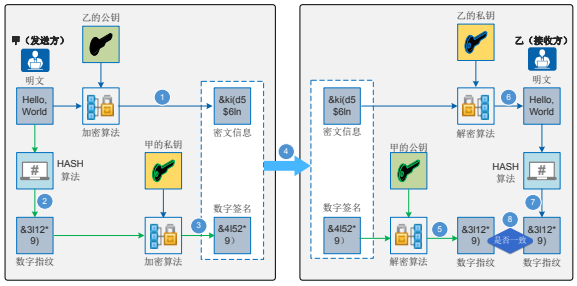
数字签名是指发送方用自己的私钥对数字指纹进行加密后所得的数据，接收方需要使用发送方的公钥才能解开数字签名，得到数字指纹。

数字指纹又称信息摘要，是指发送方通过HASH算法对明文信息计算后得出的数据。采用数字指纹时，发送方会将数字指纹和明文一起发送给接收方，接收方用同样的HASH

算法对明文计算生成的数据指纹，与收到的数字指纹进行匹配，如果一致，便可确定明文信息没有被篡改。

数字签名的加解密过程如图12-4所示。

图 12-4 数字签名的加解密过程示意图



甲事先获得乙的公钥，具体加解密过程如下：

1. 甲使用乙的公钥对明文进行加密，生成密文信息。
2. 甲使用HASH算法对明文进行HASH运算，生成数字指纹。
3. 甲使用自己的私钥对数字指纹进行加密，生成数字签名。
4. 甲将密文信息和数字签名一起发送给乙。
5. 乙使用甲的公钥对数字签名进行解密，得到数字指纹。
6. 乙接收到甲的加密信息后，使用自己的私钥对密文信息进行解密，得到最初的明文。
7. 乙使用HASH算法对明文进行HASH运算，生成数字指纹。
8. 乙将生成的数字指纹与得到的数字指纹进行比较，如果一致，乙接收明文；如果不一致，乙丢弃明文。

从加解密的过程中可以看出，数字签名技术不但可以验证信息是否被篡改，还可以证明发送方的身份。数字签名和数字信封技术也可以组合使用。

但是，数字签名技术还有个问题，如果攻击者更改乙的公钥，甲获得的是攻击者的公钥，攻击者拦截乙发送给甲的信息，用自己的私钥对伪造的信息进行数字签名，然后与使用甲的公钥的加密伪造的信息一起发送给甲。甲收到加密信息后，解密得到的明文，并验证明文没有被篡改，则甲始终认为是乙发送的信息。

12.2.1.3 数字证书

数字签名无法确定某个特定的公钥属于特定的拥有者，因为谁都可以生成公钥和私钥，仅凭一个公钥无法判断收到的公钥是不是对方的。因此需要一个安全可信的载体来交换公钥，这个载体就是数字证书。

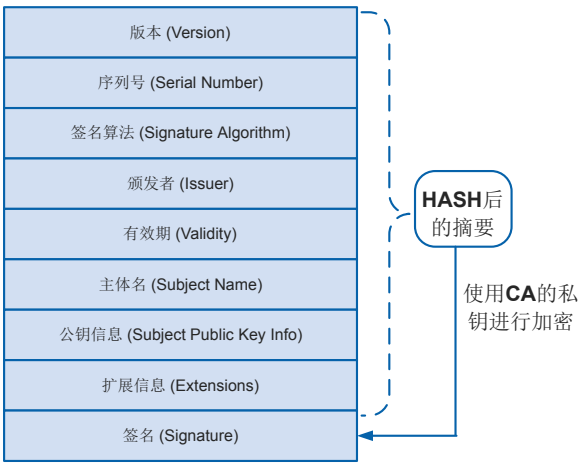
数字证书简称证书，它是一个经证书授权中心数字签名的文件，包含拥有者的公钥及相关身份信息。

数字证书可以说是网络上的安全护照或身份证，提供的是网络上的身份证明。数字证书技术解决了数字签名技术中无法确定公钥是指定拥有者的问题。

证书结构

最简单的证书包含一个公钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效期、颁发者（证书授权中心）的名称和该证书的序列号等信息。证书的结构遵循X.509 v3版本的规范。**图12-5**展示了一种常见的证书结构。

图 12-5 证书结构示意图



证书的各字段解释如下：

- 版本：即使用X.509的版本，目前普遍使用的是v3版本（0x2）。
- 序列号：颁发者分配给证书的一个正整数，同一颁发者颁发的证书序列号各不相同，可与颁发者名称一起作为证书的唯一标识。

- 签名算法：颁发者颁发证书时使用的签名算法。
- 颁发者：颁发该证书的设备名称，必须与颁发者证书中的主体名一致。通常为CA服务器的名称。
- 有效期：包含有效的起、止日期，不在有效期范围内的证书为无效证书。
- 主体名：证书拥有者的名称，如果与颁发者相同则该证书是一个自签名证书。
- 公钥信息：用户对外公开的公钥以及公钥算法信息。
- 扩展信息：通常包含证书的用法、CRL的发布地址、OCSP服务器的URL等可选字段。
- 签名：颁发者用私钥对证书信息的签名。

证书签名的形成过程如下：首先，CA使用签名算法中的HASH密码学算法生成证书的摘要信息，然后使用签名算法中的公钥密码学算法，配合CA的私钥对摘要信息进行加密，最终形成签名。这些操作都是证书颁发之前在CA上进行的。

证书分类

证书有三种类型，如表12-1所示。

表 12-1 证书类型

类型	描述	说明
CA证书	CA自身的证书。如果PKI系统中没有多层级CA，CA证书就是自签名证书；如果有多层级CA，则会形成一个CA层次结构，最上层的CA是根CA，它拥有一个CA“自签名”的证书。	申请者通过验证CA的数字签名从而信任CA，任何申请者都可以得到CA的证书（含公钥），用以验证它所颁发的本地证书。
本地证书	CA颁发给申请者的证书。	-
自签名证书	• 自签名证书是设备为自己颁发的证书，由设备的预置CA进行签名。即证书颁发者和证书主体相同，自签名证书带有签名信息，不需要向其他机构申请签名。 • 不带签名的证书是在设备上生成一本证书，但不进行签名，需要向CA机构申请签名，证书颁发者是CA。	通过设备生成自签名证书和不带签名的证书，可以实现简单的证书颁发功能。 设备不支持对其生成的自签名证书进行生命周期管理（如证书更新、证书撤销等），为了确保设备和证书的安全，建议用户替换为自己的本地证书。

证书格式

设备支持三种文件格式保存，如表12-2所示。

表 12-2 证书格式

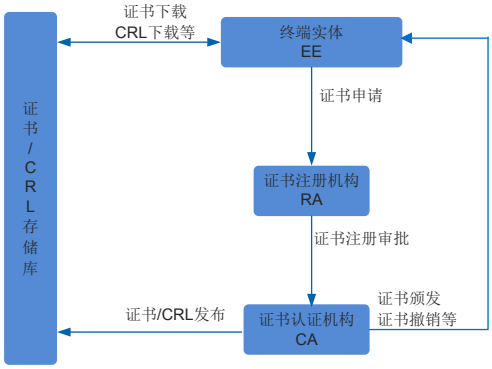
格式	描述	说明
PKCS#12	以二进制格式保存证书，可以包含私钥，也可以不包含私钥。常用的后缀有.P12和.PFX。	如果证书后缀为.CER或.CRT，可以用记事本打开证书，通过查看证书内容来区分格式。 • 如果有类似 " -----BEGIN CERTIFICATE----- " 和 " -----END CERTIFICATE----- " 的头尾标记，则证书格式为PEM。 • 如果是乱码，则证书格式为DER。
DER	以二进制格式保存证书，不包含私钥。常用的后缀有.DER、.CER和.CRT。	
PEM	以ASCII码格式保存证书，可以包含私钥，也可以不包含私钥。常用的后缀有.PEM、.CER和.CRT。	

12.2.2 PKI 体系架构

PKI 的体系组成

如图12-6所示，一个PKI体系由终端实体、证书注册机构、证书认证机构和证书/CRL存储库四部分组成。

图 12-6 PKI 体系组成



终端实体EE（End Entity）

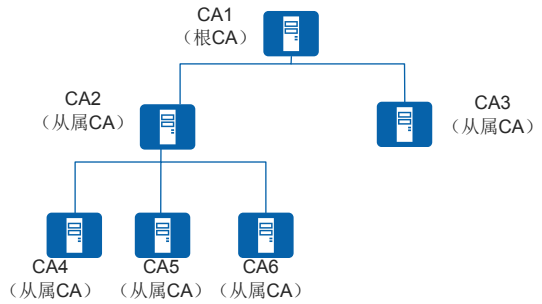
终端实体也称为PKI实体，它是PKI产品或服务的最终使用者，可以是个人、组织、设备（如路由器、防火墙）或计算机中运行的进程。

证书认证机构CA（Certificate Authority）

CA是PKI的信任基础，是一个用于颁发并管理数字证书的可信实体。它是一种具备权威性、可信任性和公正性的第三方机构。CA颁发证书的功能由CA服务器实现。

如**图12-7**所示，CA通常采用多层次的分级结构，根据证书颁发机构的层次，可以划分为根CA和从属CA。

图 12-7 CA 层次示意图



- 根CA是公钥体系中的第一个证书颁发机构，它是信任的起源。根CA可以为其他CA颁发证书，也可以为其他计算机、用户、服务颁发证书。对大多数基于证书的应用程序来说，使用证书的认证都可以通过证书链追溯到根CA。根CA通常持有一个自签名证书。
- 从属CA必须从上级CA处获取证书。上级CA可以是根CA或者是一个已由根CA授权可颁发从属CA证书的从属CA。上级CA负责签发和管理下级CA的证书，最下一级的CA直接面向用户。例如，CA2和CA3是从属CA，持有CA1发行的CA证书；CA4、CA5和CA6是从属CA，持有CA2发行的CA证书。

当某个PKI实体信任一个CA，则可以通过证书链来传递信任，证书链就是从用户的证书到根证书所经过的一系列证书的集合。当通信的PKI实体收到待验证的证书时，会沿着证书链依次验证其颁发者的合法性。

CA的核心功能就是发放和管理数字证书，包括：证书的颁发、撤销、查询、归档和证书废除列表CRL（Certificate Revocation List）的发布等。

证书注册机构RA（Registration Authority）

RA是数字证书注册审批机构，是CA面对用户的窗口和CA证书发放、管理功能的延伸，它负责接收用户的证书注册和撤销申请，对用户的身份信息进行审查，并决定是否向CA提交签发或撤销数字证书的申请。

在实际应用中，RA通常与CA合并在一起。RA也可以独立出来，减轻CA的压力，增强CA系统的安全性。

证书/CRL存储库

证书/CRL存储库用于对证书和CRL等信息进行存储和管理，并提供查询功能。

由于用户名称改变、私钥泄露或业务中止等原因，需要一种方法将现行的证书吊销，即撤销公钥与PKI实体身份信息的绑定关系。这种方法为证书废除列表CRL。

任何一个证书被撤销以后，CA就要发布CRL来声明该证书是无效的，并列出所有被废除的证书的序列号。因此，CRL提供了一种检验证书有效性的方式。

证书相关操作

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

证书申请

证书申请即证书注册，是PKI实体向CA自我介绍并获取证书的过程。通常情况下，PKI实体会生成一对公私钥。公钥和PKI实体的身份信息（包含在证书注册请求消息中）被发送给CA，用来生成本地证书。私钥由PKI实体自己保存，用来生成数字签名和解密对端实体发送过来的密文。当前设备支持离线申请证书和通过CMPv2协议在线申请证书。

证书颁发

PKI实体向CA申请本地证书时，如果有RA，则先由RA审核PKI实体的身份信息，审核通过后，RA将申请信息发送给CA，CA再根据PKI实体的公钥和身份信息生成本地证书，并将本地证书信息发送给RA。如果没有RA，则直接由CA审核PKI实体身份信息。

此外，PKI实体可以为自己颁发一个自签名证书或不带签名的证书，实现简单的证书颁发功能。

证书存储

CA生成本地证书后，CA/RA会将本地证书发布到证书/CRL存储库中，为用户提供下载服务和目录浏览服务。

证书下载

PKI实体通过LDAP或带外方式下载已颁发的证书。该证书可以是自己的本地证书，也可以是CA/RA证书，或其他PKI实体的本地证书。

证书安装

PKI实体下载证书后还需安装证书，即将证书导入到设备的内存中，否则证书不生效。该证书可以是自己的本地证书，也可以是CA/RA证书，或其他PKI实体的本地证书。

证书验证

安装CA/RA证书和本地证书以后，使用之前必须对本地设备的证书进行验证，确保证书的合法性。证书验证的核心是检查CA在证书上的签名，并确定证书仍在有效期内且未被撤销。

证书更新

当证书过期或密钥泄露时，PKI实体必须更换证书，可以通过手动申请或配置CMPv2协议自动更新证书来实现。

证书撤销

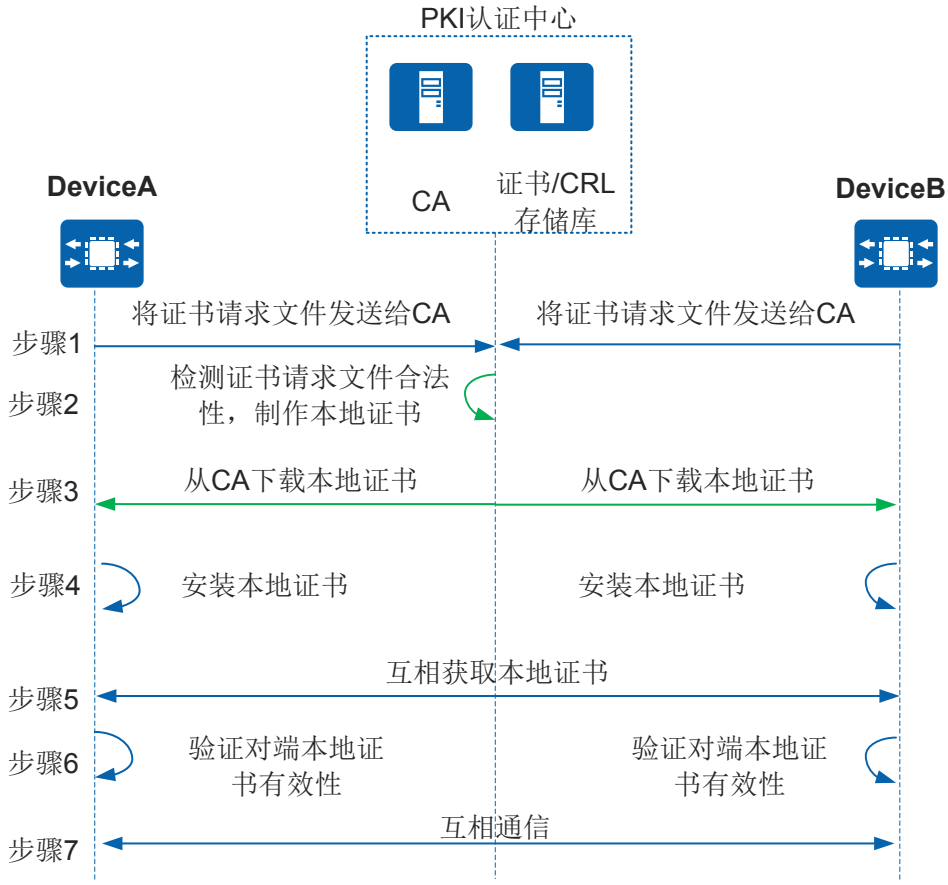
当用户的身份、信息、公钥发生改变或业务中止时，用户需要将自己的数字证书撤销，即撤销公钥与用户身份信息的绑定关系。CA机构提供证书撤销功能。当PKI实体通过带外方式申请撤销自己的证书时，CA会将这些证书存储在CRL存储库或OCSP服务器中。

12.2.3 PKI 工作机制

离线申请证书和在线申请证书的工作流程不同，具体如下。

离线申请证书工作流程

图 12-8 PKI 离线申请工作过程示意图

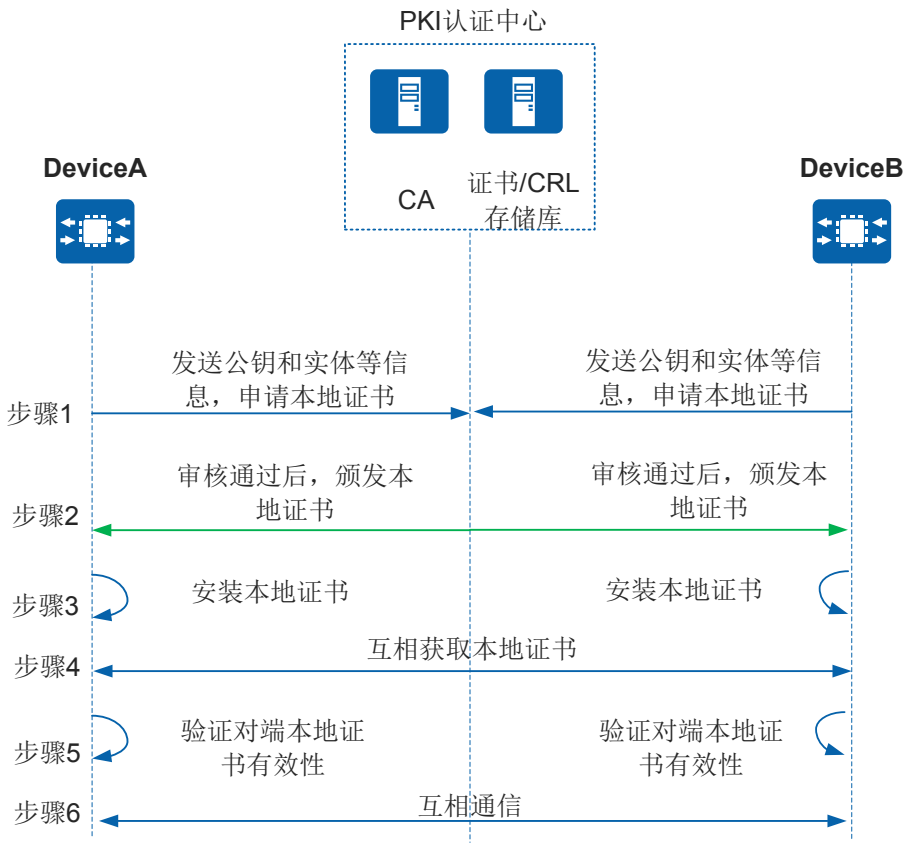


1. PKI实体通过磁盘、电子邮件等方式将证书请求文件发送给CA，请求制作证书。
2. CA检测证书请求文件合法性，如果通过，则根据证书请求文件制作证书。
3. PKI实体通过磁盘、电子邮件等方式将证书下载到本地。
4. 安装本地证书到设备的内存中。
5. **可选:**

   PKI实体间互相通信时，需获取对端实体的本地证书和CA证书。（IPSec场景下，PKI实体会把各自的本地证书发送给对端，不需安装对端实体的证书到本地设备。）
6. 通过CRL或OCSP方式验证对端实体的本地证书的有效性。
7. 对端实体的本地证书有效时，PKI实体间才可以使用对端证书的公钥进行加密通信。

通过 CMPv2 协议在线申请证书工作流程

图 12-9 PKI 在线申请证书工作过程示意图



1. PKI实体向CA发送证书注册请求消息（包括RSA密钥对中的公钥和PKI实体信息）。

   当PKI实体通过CMPv2协议申请本地证书时，PKI实体可以使用签名或消息认证码方式向CA机构进行身份认证。

   - 签名方式：PKI实体对证书注册请求消息使用CA证书的公钥进行加密；使用PKI实体的额外证书（其他CA颁发的本地证书）相对应的私钥进行数字签名。
   - 消息认证码方式：PKI实体对证书注册请求消息使用CA证书的公钥进行加密，证书注册请求消息必须包含消息认证码的参考值和秘密值（与CA的消息认证码的参考值和秘密值一致）。

2. CA收到PKI实体的证书注册请求消息，审核证书注册请求消息并颁发证书。

   - 签名方式：CA使用自己的私钥解密，使用PKI实体的额外证书中的公钥解密数字签名，并验证数字指纹。当数字指纹一致时，CA才会审核PKI实体身份等信息，审核通过后，同意PKI实体的申请，颁发本地证书。然后CA使用PKI实体的额外证书中的公钥进行加密，使用自己的私钥进行数字签名后将证书发送给PKI实体，同时也会发送到证书/CRL存储库。
   - 消息认证码方式：CA使用自己的私钥解密并验证消息认证码的参考值和秘密值，当两者和CA的参考值、秘密值一致时，CA才会审核PKI实体身份等信

息，审核通过后，同意PKI实体的申请，颁发本地证书。然后CA使用PKI实体的公钥进行加密，将证书发送给PKI实体，同时也会发送到证书/CRL存储库。

3. PKI实体收到CA发送的证书信息，安装本地证书到设备的内存中。
   - 签名方式：PKI实体使用额外证书相对应的私钥解密，并使用CA的公钥解密数字签名并验证数字指纹。数字指纹一致时，PKI实体确认证书信息，然后安装本地证书到设备的内存中。
   - 消息认证码方式：PKI实体使用自己的私钥解密，并验证消息认证码的参考值和秘密值。参考值和秘密值均一致时，PKI实体确认证书信息，然后安装本地证书到设备的内存中。
4. **可选:**

   PKI实体间互相通信时，需各自获取对端实体的本地证书和CA证书。（IPSec场景下，PKI实体会把各自的本地证书发送给对端，不需安装对端实体的证书到本地设备。）
5. PKI实体通过CRL或OCSP方式验证对端实体的本地证书有效性。
6. 对端实体的本地证书有效时，PKI实体间才可以使用对端证书的公钥进行加密通信。

如果PKI认证中心有RA，则PKI实体也会下载RA证书。由RA审核PKI实体的本地证书申请，审核通过后将申请信息发送给CA来颁发本地证书。

12.3 PKI 配置注意事项

License 依赖

PKI无需License许可即可使用。

硬件依赖

表 12-3 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 12-4 本特性的使用限制

特性	特性限制	系列	涉及产品
公钥管理	必须在当前证书过期之前将证书导入到所有需要导入证书的设备上。如果证书已过期，管理员没有及时安装新的证书，证书验证会失败。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8
公钥管理	由于Windows Server 2003服务器处理能力有限，与该型号服务器对接时，设备上不能配置过多实体信息或携带密钥对位数过大的密钥对。否则可能导致设备与服务器对接失败。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8
公钥管理	在申请证书前需要确认设备上的时钟是否正确。设备会检查当前时间是否在证书的有效范围内。如果在有效范围之外，证书会注册失败。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8

12.4 PKI 缺省配置

PKI的主要缺省配置如表12-5所示。

表 12-5 PKI 的缺省配置

参数	缺省配置
PKI域	设备缺省存在一个域名为default的PKI域，此域可以修改但不能删除。
RSA密钥对	设备缺省存在一个名称为default的RSA密钥对文件
设备保存证书请求、证书和CRL时的文件格式	PEM
证书状态检查方式	CRL方式
本地证书/CA证书的过期预告警时间	90天

12.5 申请证书的预配置

12.5.1 配置 RSA/SM2 密钥对

背景信息

本地证书由CA进行数字签名并颁发，是公钥与PKI实体身份信息的绑定。申请本地证书时，需先配置RSA/SM2密钥对，生成公钥和私钥。公钥由PKI实体发送给CA，用来加密明文；私钥由PKI实体保留，用来进行数字签名和解密对端发送过来的密文。

配置RSA/SM2密钥对有以下两种方式：

- 创建RSA/SM2密钥对。

  设备上可以直接创建密钥对，无需再将密钥对导入到设备的内存中。创建RSA/SM2密钥对的过程中，系统会提示输入公钥的位数，长度范围从2048到4096。公钥的长度越大，其安全性就越高，但计算速度相对来说比较慢。
- 导入RSA/SM2密钥对。

  当需要使用其他PKI实体产生的密钥对时，可以通过FTP/SFTP传到设备上，然后将密钥对导入到内存中，否则密钥对不生效。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 根据实际情况选择配置RSA/SM2密钥对的方法。

表 12-6

操作	命令	说明
创建RSA/SM2密钥对	**pki rsa local-key-pair create** *key-name* [**modulus** *modulus-size*] [**exportable**]	仅当配置**exportable**参数时，创建的RSA密钥对才是可导出的。

操作	命令	说明
	pki sm2 local-key-pair create *key-name* [**exportable**]	仅当配置**exportable**参数时，创建的SM2密钥对才是可导出的。
导入RSA/SM2密钥对	**pki import rsa-key-pair** *keyname* [**exclude-cert**] { **pem** | **pkcs12** } *filename* [**exportable**] [**password** *password*]	配置**exclude-cert**参数时，系统不会导入文件中存在的证书。
	pki import sm2-key-pair *keyname* **pem** *filename* [**exportable**] **signkey** *signkey-name* [**certificate** *certificate-name*]	仅当配置**exportable**参数时，导入的SM2密钥对才是可导出的。

----结束

检查配置结果

- 执行命令**display pki rsa local-key-pair** { **pem** | **pkcs12** } *file-name* [**password** *password*]，查看RSA密钥对信息。
- 执行命令**display pki rsa local-key-pair** [**name** *key-name*] **public**，查看RSA公钥信息。
- 执行命令**display pki sm2 local-key-pair** [**name** *key-name*] **public**，查看SM2密钥对及公钥信息。

后续处理

表 12-7

操作	命令	说明
导出RSA/SM2密钥对	**pki export rsa-key-pair** *key-name* [**and-certificate** *certificate-name*] { **pem** *file-name* [**aes**] | **pkcs12** *file-name* } **password** *password*	当需要备份RSA密钥对或者需要将RSA密钥对导出给其他设备使用时，可以在系统视图下执行此命令，将RSA密钥对导出到设备的存储介质中，同时支持导出与其关联的证书及证书链，然后可以通过FTP/SFTP获取RSA密钥对。
	pki export sm2-key-pair *keyname* **pem** *filename* [**password** *password*]	当需要备份SM2密钥对或者需要将SM2密钥对导出给其他设备使用时，可以在系统视图下执行此命令，将SM2密钥对导出到设备的存储介质中，然后可以通过FTP/SFTP获取SM2密钥对。

操作	命令	说明
销毁指定的RSA/SM2密钥对	**pki rsa local-key-pair destroy** *key-name*	RSA密钥对泄露、损坏、不用或丢失时，可以在系统视图下执行此命令，销毁指定的RSA密钥对。配置后，系统会销毁设备中对应名称的RSA密钥对。
	pki sm2 local-key-pair destroy *key-name*	SM2密钥对泄露、损坏、不用或丢失时，可以在系统视图下执行此命令，销毁指定的SM2密钥对。配置后，系统会销毁设备中对应名称的SM2密钥对。
查找证书所对应的RSA/SM2密钥对	**pki match-rsa-key certificate-filename** *file-name*	用户不知道证书所对应的RSA密钥对时，可以在系统视图下执行此命令，查找证书所对应的RSA密钥对。
	pki match-sm2-key certificate-filename *file-name*	用户不知道证书所对应的SM2密钥对时，可以在系统视图下执行此命令，查找证书所对应的SM2密钥对。

12.5.2 配置 PKI 实体信息

背景信息

本地证书由CA进行数字签名并颁发，是公钥与PKI实体身份信息的绑定。PKI实体身份信息即为PKI实体信息，CA根据PKI实体提供的身份信息来唯一标识证书申请者，因此在申请本地证书时必须将PKI实体信息发送给CA。

PKI实体信息包括：通用名称（Common Name）、FQDN（Fully Qualified Domain Name）名称、IP地址、电子邮箱地址等，其中通用名称必须配置，其他几项是可选配置。这些信息都将包含在证书中。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建PKI实体并进入PKI实体视图，或者直接进入PKI实体视图。

```
pki entity entity-name
```

步骤3 配置PKI实体的通用名称。

```
common-name common-name
```

步骤4 **可选:** 配置PKI实体的其他参数。

为了更好的标识证书申请者的唯一身份，还可配置以下可选参数作为PKI实体的别名。否则，当PKI实体间的通用名称相同时，会导致PKI实体申请证书失败。

操作	命令
配置PKI实体的IP地址。	**ip-address** { *ipv4-address* | *ipv6-address* | *interface-type interface-number* [**ipv6**] }
配置PKI实体的FQDN名称。	**fqdn** *fqdn-name*
配置PKI实体的电子邮箱地址。	**email** *email-address*
配置PKI实体所属的国家代码。	**country** *country-code*
配置PKI实体所在的地理区域名称。	**locality** *locality-name*
配置PKI实体所属的州或省。	**state** *state-name*
配置PKI实体所属的组织名称。	**organization** *organization-name*
配置PKI实体所属的部门名称。	**organization-unit** *organization-unit-name*

步骤5 退出PKI实体视图。

```
quit
```

----结束

检查配置结果

执行命令**display pki entity** [*entity-name*]，查看PKI实体信息。

12.5.3 下载 CA 证书

背景信息

申请本地证书时，PKI实体会将证书注册请求消息发送给CA。为了提高传输过程中的安全性，PKI实体必须使用CA的公钥对证书注册请求消息进行加密保护。因此，PKI实体必须先下载并获取CA证书后从中获取CA的公钥。

下载CA证书有如下几种方式，可根据CA提供的服务方式进行选择。

- 通过LDAP协议从存放证书的服务器上下载CA证书，设备会自动将CA证书保存到设备的**flash:/pki/public**存储路径下。
- 通过带外方式（磁盘、电子邮件等）获得CA证书后，上传到设备的存储介质中。

操作步骤

- 通过LDAP方式下载CA证书。

  ```
  system-view
  pki ldap-server-template template-name attribute attr-value save-name dn dn-value
  ```

- 通过带外方式下载CA证书。

  用户通过磁盘、电子邮件等方式获得CA证书后，需要手工上传到设备的存储介质中。此外，也可以选择通过管理PC下载证书后，使用FTP/SFTP方式上传到设备的存储介质中。由于FTP协议本身存在安全风险，建议使用SFTP安全协议。

----结束

12.5.4 安装 CA 证书

背景信息

通过LDAP协议下载CA证书后，设备会自动将CA证书存放在**flash:/pki/public**存储路径下。

通过带外方式（磁盘、电子邮件等）获得CA证书后，需要将CA证书上传到设备指定的存储路径下。安装CA证书前，需要先将CA证书上传到**flash:/pki/public**存储路径下。

CA证书存放在上述指定路径后，还需手动导入到设备的内存中。只有将CA证书导入到设备的内存中，设备重启后系统才能自动加载证书文件。

说明

请确保CA证书文件不超过1M，避免安装失败。

缺省情况下存在名称为**default**的PKI域。default域可以修改但不能删除。

操作步骤

步骤1 **可选:** 进入用户视图，将CA证书下载到**flash:/pki/public**目录下。

通过带外方式获取到CA证书，然后使用FTP/SFTP上传到设备的存储介质中时，需执行以下操作。由于FTP协议本身存在安全风险，建议使用SFTP安全协议。通过LDAP协议方式获取CA证书时不需要执行如下操作。

```
cd pki
cd public/
ftp 172.16.104.110
Trying 172.16.104.110...
Press CTRL+K to abort
Connected to 172.16.104.110.
220 FTP service ready.
User(172.16.104.110:(none)):ftpuser
331 Password required for ftpuser
Enter password:
230 User logged in.
get ca.cer
200 Port command okay.
150 Opening ASCII mode data connection for temp1.c.
226 Transfer complete.
FTP: 4 byte(s) received in 8.190 second(s) .48byte(s)/sec.
```

步骤2 进入系统视图。

```
system-view
```

步骤3 **可选:** 将预置的CA证书导入到default域下。

```
pki import-certificate default_ca realm default
```

设备出厂前会将预置的CA证书存放在NVRAM内存中，如需使用预置CA证书，可以执行此命令将证书加载到default域下。预置CA证书可以被删除，删除后可以在default域下导入其他CA证书，由于default_ca.cer为系统预留的预置CA证书名称，导入的证书不能命名为default_ca.cer。如果想要恢复被删除的预置CA证书，也可以执行此命令将证书加载到default域下。

步骤4 创建PKI域。

```
pki realm realm-name
quit
```

步骤5 将CA证书导入到设备的内存中。

```
pki import-certificate ca [ [ realm realm-name ] { der | pkcs12 | pem } ] filename file-name [ cert-name cert-name ] [ no-check-same-name ] [ no-check-hash-alg ]
```

步骤6 （可选）配置内存中的CA证书的过期预告警时间。

```
pki set-certificate expire-prewarning day
```

----结束

检查配置结果

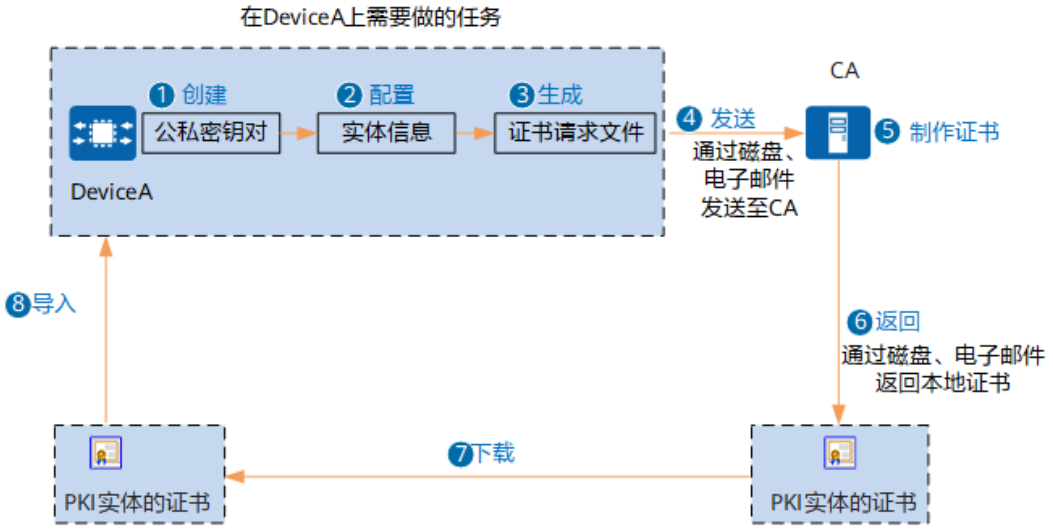
执行命令**display pki certificate ca** [**realm** *realm-name* | **filename** *file-name*]，查看设备上已加载的CA证书的内容。

12.6 离线申请证书

12.6.1 了解离线证书申请

证书申请即证书注册，就是一个PKI实体向CA自我介绍并获取证书的过程。离线申请本地证书需要配置PKI实体信息、RSA密钥对、申请本地证书、安装本地证书。离线方式申请证书流程如图12-10所示。

图 12-10 离线证书申请流程



1. 创建公私密钥对。首先，在DeviceA上创建的公私密钥对，因为在申请证书时会用到公钥信息。
2. 配置实体信息。申请证书时，DeviceA必须向CA提供能够证明自己身份的信息，实体信息代表的就是设备的身份信息，包括：通用名称（Common Name）、FQDN（Fully Qualified Domain Name）名称、IP地址、电子邮箱地址等。其中，通用名称是必须配置的，而其他几项是可选配置的。实体信息配置完成后，还需要在PKI域中引用实体信息。
3. 生成证书请求文件。生成的证书请求文件以“*PKI域名*.req”的名字保存在DeviceA的存储介质中。
4. 证书请求文件生成后，可以将该文件通过磁盘、电子邮件等方式将该文件发送给CA。

5. CA审核通过后，根据证书请求文件制作证书。
6. 证书生成后，通过磁盘、电子邮件等方式获取到DeviceA的本地证书**DeviceA.cer**。
7. 将**DeviceA.cer**下载到DeviceA的**flash:/pki/public**存储路径下。
8. 将**DeviceA.cer**证书导入到DeviceA的内存中。

12.6.2 离线申请本地证书

前提条件

已完成申请本地证书的预配置操作，具体可以参见**申请证书预配置**。

背景信息

离线申请本地证书需要用户在设备上生成证书申请文件，然后通过磁盘、电子邮件等带外方式将证书申请文件发送给CA，向CA申请本地证书。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建PKI域并进入PKI域视图，或者直接进入已存在的PKI域视图。

```
pki realm realm-name
```

缺省情况下，系统下存在名称为**default**的PKI域，该域可以修改但不能删除。

PKI域是一个本地概念，一个设备上配置的PKI域对CA和其他设备是不可见的，每一个PKI域有单独的参数配置信息。

步骤3 指定申请证书的PKI实体。

```
entity entity-name
```

*entity-name*是一个已经通过**pki entity**命令创建的PKI实体。

步骤4 根据实际情况选择配置使用离线方式申请证书时使用的密钥对。

- 配置使用离线方式申请证书时使用的RSA密钥对。
  ```
  rsa local-key-pair key-name
  ```
- 配置使用离线方式申请证书时使用的SM2密钥对。
  ```
  sm2 local-key-pair key-name
  ```

步骤5 配置签名证书注册请求消息使用的摘要算法。

```
enrollment-request signature message-digest-method { md5 | sha1| sha-256 | sha-384 | sha-512 | sm3 }
```

缺省情况下，签名证书注册请求消息使用的摘要算法为**sha-256**。

PKI实体使用的摘要算法必须与CA服务器上的摘要算法一致。由于**MD5**和**SHA1**算法为不安全算法，建议使用SHA2算法（SHA-256、SHA-384和SHA-512）。

在某个PKI域下，当使用SM2密钥对离线申请证书时，签名证书注册请求消息使用的摘要算法必须配置为SM3；当使用RSA密钥对离线申请证书时，签名证书注册请求消息使用的摘要算法不可配置为SM3，否则会导致离线申请证书失败。

说明

出于安全性考虑，不建议使用该特性提供的弱安全算法或弱安全协议。如果确实需要使用，请执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包WEAKEA。设备默认自带弱安全算法/协议特性包WEAKEA，特性包安装或卸载的详细步骤请参见《配置指南-系统管理 配置》中的“升级维护配置”。

步骤6 **可选:** 配置证书公钥用途属性。

```
key-usage { encipherment | signature }
quit
```

步骤7 在系统视图下，配置设备保存证书和证书请求时的文件格式。

```
pki file-format { der | pem }
```

缺省情况下，设备保存证书和证书请求时的文件格式为PEM。

步骤8 配置以PKCS#10格式保存证书申请信息到文件中。

```
pki enroll-certificate realm realm-name pkcs10 [ filename filename ] [ password password ]
```

PKI实体使用的挑战密码必须与CA服务器上设置的密码一致。如果CA服务器不要求使用挑战密码，则不用配置挑战密码。

步骤9 通过磁盘、电子邮件等带外方式将证书申请文件发送给CA，向CA申请本地证书。

----结束

检查配置结果

- 执行命令**display pki realm** [*realm-name*]，查看PKI域的信息。
- 执行命令**display pki cert-req filename** *file-name*，查看证书请求文件的内容。

12.6.3 下载本地证书

背景信息

通常采用以下方式获得本地证书，设备采用哪种方式下载证书，取决于CA服务器提供的服务方式：

- 通过LDAP协议从存放证书的服务器上下载本地证书，设备会自动将本地证书保存到设备的**flash:/pki/public**存储路径下。
- 通过带外方式（磁盘、电子邮件等）获得本地证书后，上传到设备的存储介质中。

操作步骤

- 通过LDAP方式下载本地证书。

  ```
  system-view
  pki ldap ip ip-address port port version version [ attribute attr-value ] [ authentication ldap-dn ldap-password ] save-name dn dn-value
  ```

- 通过带外方式下载本地证书。

  用户通过磁盘、电子邮件等方式获得本地证书后，需要手工上传到设备的存储介质中。也可以选择通过管理PC下载证书后，使用FTP/SFTP方式上传到设备的存储介质中。由于FTP协议本身存在安全风险，建议使用SFTP安全协议。

----结束

检查配置结果

- 执行命令**display pki credential-storage-path**，查看证书的缺省保存路径。
- 执行命令**dir（用户视图）**，查看存储介质中的本地证书文件。

12.6.4 安装本地证书

背景信息

通过带外方式（磁盘、电子邮件等）获取到本地证书，需要将本地证书上传到设备的指定存储路径下。安装本地证书需要先将证书上传到**flash:/pki/public**存储路径下。

通过LDAP协议下载本地证书，设备会自动将本地证书存放在**flash:/pki/public**存储路径下。

本地证书存放在上述指定路径下后，还需手动导入到设备的内存中。只有将本地证书导入到设备的内存中，在设备重启后系统才能自动加载证书文件。

说明

请确保本地证书文件不超过1M，避免安装失败。

缺省情况下，根系统下存在名称为**default**的PKI域。设备预置的本地证书默认存放在default域下。default域可以修改但不能删除。

预置的本地证书作为华为设备的身份标识，缺省情况下为设备中的用户登录业务提供证书认证。

操作步骤

步骤1 **可选:** 进入用户视图，将本地证书下载到**flash:/pki/public**目录下。

通过带外方式获取到本地证书，然后使用FTP/SFTP上传到设备的存储介质中时，需执行以下操作，由于FTP协议本身存在安全风险，建议使用SFTP安全协议。通过LDAP协议方式获取本地证书不需要执行如下操作。

```
cd pki
cd public/
ftp 172.16.104.110
Trying 172.16.104.110...
Press CTRL+K to abort
Connected to 172.16.104.110.
220 FTP service ready.
User(172.16.104.110:(none)):ftpuser
331 Password required for ftpuser
Enter password:
230 User logged in.
get device.cer
200 Port command okay.
150 Opening ASCII mode data connection for temp1.c.
226 Transfer complete.
FTP: 4 byte(s) received in 8.190 second(s) .48byte(s)/sec.
```

步骤2 进入系统视图。

```
system-view
```

步骤3 **可选:** 将预置的本地证书导入到default域下。

```
pki import-certificate default_local realm default
```

预置的本地证书可以被删除，如果想要恢复被删除的预置Local证书，可以执行此命令将证书从NVRAM中加载到default域下。

步骤4 创建PKI域。

```
pki realm realm-name
quit
```

步骤5 在系统视图下，将本地证书导入到设备的内存中。

- 当在本PKI实体下创建RSA密钥对，通过PKI实体信息和RSA密钥对去CA申请本地证书时，只需执行如下命令，导入本地证书到内存中即可，因为在本地创建RSA密钥对时RSA密钥已经默认导入到设备的内存中。
  ```
  pki import-certificate local [ [ realm realm-name ] { der | pkcs12 | pem } ] filename file-name
  [ cert-name cert-name ] [ no-check-same-name ] [ no-check-hash-alg ]
  ```
- 当使用其他PKI实体产生的密钥对和其他PKI实体的证书时，需要导入证书和密钥对文件。一般证书及其密钥对有两种存在形式，一种是证书文件中包含密钥对文件，两者以一个文件的形式存在；另一种是证书和密钥对相互独立以两个文件形式存在。不同形式下，将其导入内存使用的方法不同，具体如下。
  - 证书文件中包含密钥对文件。
    ```
    pki import rsa-key-pair keyname { pem | pkcs12 } file-name [ exportable ] [ password password ]
    ```
  - 证书文件和密钥对文件独立存在。

    # 导入证书文件。
    ```
    pki import-certificate local [ [ realm realm-name ] { der | pkcs12 | pem } ] filename file-name [ cert-name cert-name ] [ no-check-same-name ] [ no-check-hash-alg ]
    ```

    # 导入密钥对文件。
    ```
    pki import rsa-key-pair keyname exclude-cert { pem | pkcs12 } file-name [ exportable ] [ password password ]
    ```

说明

若不指定待导入证书的格式，系统将自行识别导入。

步骤6 （可选）配置内存中的本地证书的过期预告警时间。

```
pki set-certificate expire-prewarning day
```

----结束

检查配置结果

执行命令**display pki certificate local** [**realm** *realm-name* | **filename** *filename*]，查看设备上已加载的本地证书的内容。

12.6.5 检查证书有效性

前提条件

已在设备上安装CA证书和本地证书。

背景信息

在安装CA证书和本地证书以后，使用每一个证书之前，必须对本地设备的证书进行验证，以确保证书的合法性。证书验证包括对签发时间、签发者信息以及证书的有效性几方面进行验证。证书验证的核心是检查CA在证书上的签名，并确定证书仍在有效期内，而且未被撤销。

为完成证书验证，本地设备需要下面的信息：CA证书、CRL、本地证书及其私钥及证书认证相关配置信息。

本地证书验证的主要过程如下：

1. 使用CA证书的公钥验证CA的签名是否正确。

   为验证一个证书的合法性，首先需要获得颁发这个证书的CA的公钥（即获得CA证书），以便检查该证书上CA的签名。一个CA可以让另一个更高层次的CA来证明其证书的合法性，这样顺着证书链，验证证书就变成了一个迭代过程，最终这个链必须在某个“信任点”（一般是持有自签名证书的根CA或者是PKI实体信任的中间CA）处结束。

   任何PKI实体，如果它们共享相同的根CA或子CA，并且已获取CA证书，都可以验证对端证书。

   证书链的验证过程是一个从目标证书（待验证的PKI实体证书）到信任点证书逐层验证的过程。一般情况下，当验证对端证书链时，验证过程在碰到第一个可信任的证书或CA机构时结束。
2. 根据证书的有效期，验证证书是否过期。
3. 检查证书的状态，即通过CRL、OCSP和None方式检查证书是否被撤销。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 检查CA证书或本地证书的有效性。

```
pki validate-certificate { ca | local } { realm realm-name | filename file-name }
```

pki validate-certificate ca命令只能验证根CA的CA证书有效性，不能验证从属CA的CA证书有效性。在多级CA的环境中，当设备上导入了多个CA证书时，只能使用**pki validate-certificate local**命令来验证从属CA的CA证书有效性。

----结束

12.6.6 举例：为 PKI 实体离线申请本地证书

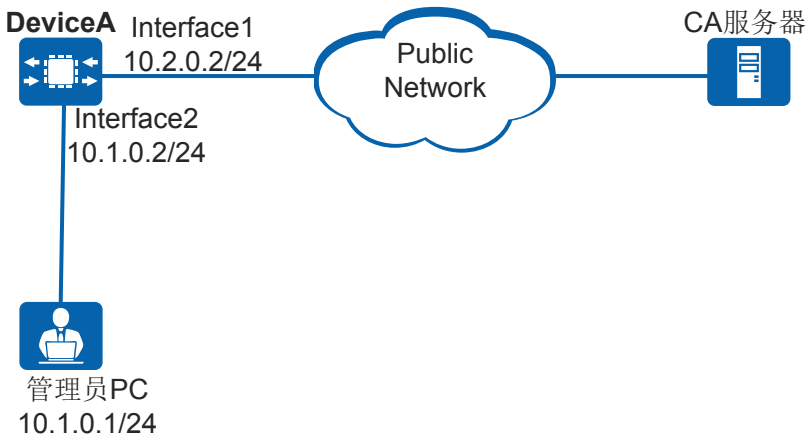
组网需求

如图12-11所示，设备向公网上的CA服务器离线申请本地证书。

说明

本例中interface1、interface2分别代表10GE0/0/1、10GE0/0/2。

图 12-11 配置为 PKI 实体离线申请本地证书组网图



配置思路

采用如下思路配置为PKI实体离线申请本地证书：

1. 创建RSA密钥对，实现申请本地证书时携带的公钥。
2. 配置PKI实体，实现申请本地证书时携带的PKI实体信息，用来标识PKI实体的身份。
3. 配置为PKI实体离线申请本地证书，生成本地证书请求文件。
4. 通过带外方式发送本地证书请求文件来申请本地证书，并通过带外方式下载本地证书。
5. 安装本地证书，使得设备可以使用证书来保护通信。

操作步骤

步骤1 配置接口的IP地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] ip address 10.2.0.2 24
[DeviceA-10GE0/0/1] quit
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] ip address 10.1.0.2  24
[DeviceA-10GE0/0/2] quit
```

步骤2 创建RSA密钥对。

创建一个2048位的RSA密钥对rsakey，并设置为可以从设备上导出。

```
[DeviceA] pki rsa local-key-pair create rsakey exportable
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
 Generating key-pairs finished
```

步骤3 配置PKI实体，标识申请证书PKI实体的身份信息。

配置PKI实体为user01。

```
[DeviceA] pki entity user01
[DeviceA-pki-entity-user01] common-name hello
[DeviceA-pki-entity-user01] country cn
[DeviceA-pki-entity-user01] email user@test.abc.com
[DeviceA-pki-entity-user01] fqdn test.abc.com
[DeviceA-pki-entity-user01] ip-address 10.2.0.2
[DeviceA-pki-entity-user01] state jiangsu
[DeviceA-pki-entity-user01] organization huawei
[DeviceA-pki-entity-user01] organization-unit info
[DeviceA-pki-entity-user01] quit
```

步骤4 配置为PKI实体离线申请本地证书。

```
[DeviceA] pki realm abc
[DeviceA-pki-realm-abc] entity user01
[DeviceA-pki-realm-abc] rsa local-key-pair rsakey
[DeviceA-pki-realm-abc] quit
[DeviceA] pki enroll-certificate realm abc pkcs10 filename cer_req
 Info: Creating certificate request file...
 Info: Create certificate request file successfully.
```

已完成配置后，可执行命令**display pki cert-req**查看证书请求文件的内容。

```
[DeviceA] display pki cert-req filename cer_req
Certificate Request:
```



```
Data:
    Version: 1 (0x0)
    Subject: C=cn, ST=jiangsu, O=huawei, OU=info, CN=hello
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bits)
            Modulus:
                00:a2:db:e3:30:17:8e:f6:2d:2e:64:15:46:51:ad:
                70:86:dd:32:c4:bb:6b:58:3a:8c:5f:a0:06:a1:e1:
                56:2e:a4:eb:7e:12:06:05:04:28:b2:6d:64:7a:9c:
                4f:85:24:c1:aa:b8:99:dc:e9:bb:c4:1e:e2:9d:a0:
                18:51:1f:ad:b5:2f:60:18:06:8b:c1:cc:6f:32:58:
                f2:21:2c:16:e8:29:c2:a8:c5:aa:9d:6c:1e:ca:14:
                fc:7a:e9:bc:07:91:ce:ed:a0:c0:52:d9:0c:e9:ba:
                9b:64:43:e0:9a:3f:c5:d1:2c:86:36:96:6b:4b:4f:
                d4:df:05:d0:4b:41:2c:ec:0a:d7:0e:45:83:ed:cd:
                07:78:40:ed:d5:3d:7f:fe:0f:08:90:04:2e:ac:e5:
                42:b9:81:ea:ec:77:e2:cc:04:6e:e4:63:9f:69:ed:
                60:06:5e:c7:e8:bf:30:57:6a:5d:e0:46:68:d3:ee:
                b0:da:47:24:e3:b6:a5:f3:20:d8:5a:75:92:70:c2:
                a9:a6:97:07:07:0d:1c:94:9a:03:6f:f7:8c:db:6f:
                b7:06:de:51:50:9e:71:fd:86:f3:b5:c9:99:05:bf:
                f1:10:20:28:d3:a6:29:3d:e0:f4:a7:ba:1e:27:85:
                a9:66:fc:a9:90:49:f0:35:f7:d9:6d:06:a2:43:3f:
                18:87
            Exponent: 65537 (0x10001)
    Attributes:
    Requested Extensions:
        X509v3 Key Usage:
            Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
        X509v3 Subject Alternative Name:
            IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
Signature Algorithm: sha256WithRSAEncryption
     0e:0a:a5:b7:d5:54:11:10:c4:ea:ff:77:da:f9:24:4b:a9:98:
     a1:75:36:08:10:59:60:fa:1a:30:70:2c:b7:f6:5f:5e:31:b7:
     55:a5:7a:26:e5:af:4a:cd:83:c5:f3:90:f3:b9:d5:f9:0a:6d:
     6e:8f:25:b4:ed:95:9c:75:a5:d7:b6:25:fc:8d:39:89:fb:af:
     37:fc:01:7b:09:07:9c:96:7c:fa:28:6d:e2:11:49:a7:95:94:
     ed:26:5b:ca:f8:98:b0:e7:64:7e:dd:2d:75:ff:89:03:b7:0a:
     92:53:25:d4:a1:23:b9:5c:eb:5b:29:1d:8a:92:8f:36:68:7b:
     77:32:bc:48:92:48:84:fa:87:5a:d7:2e:3e:be:d5:6b:e4:df:
     b1:f2:02:35:91:6a:eb:cd:fc:5a:ea:37:85:6c:12:74:5f:a5:
     5c:c0:05:09:cd:34:59:0d:c6:c8:75:ca:1c:18:d6:48:e5:4b:
     e7:8e:e3:ff:25:99:0f:2e:a8:b4:c5:8e:4d:8f:dd:64:c5:1f:
     61:3c:58:21:4f:d5:35:ba:c8:8e:5f:76:41:9f:27:41:0a:94:
     59:2c:59:25:2d:de:60:5c:92:07:ac:8a:a5:7a:ba:75:af:2c:
     82:5f:bb:55:a8:48:49:54:0f:99:54:af:8d:12:4d:4b:7d:8b:
     95:28:ce:dc
```

步骤5 通过磁盘、电子邮件等带外方式将证书申请文件发送给CA服务器，向CA服务器申请本地证书。

本地证书注册成功后，可以通过带外方式下载本地证书abc_local.cer。下载后，可以通过文件传输协议导入到设备的**flash:/pki/public**存储路径下。

步骤6 安装本地证书。

证书导入成功后，**flash:/pki/public**存储路径下的**abc_local.cer**默认删除，如果不需删除，请根据设备上的提示信息选择N进行保留。

```
[DeviceA] pki import-certificate local realm abc pem filename abc_local.cer
 Info: Succeeded in importing the certificate.
 Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select [Y/N]:y
 Info: Delete Success.
```

----结束

检查配置结果

安装本地证书后，两端设备可以使用证书来保护通信。

```
[DeviceA] display pki certificate local filename abc_local.cer
Info: It will take a few seconds or more to collect data for displaying. Please wait a moment.
Total Number: 1

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8372560407419635446 (0x74314f54b0bf46f6)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=HUAWEI BRAS CA, O=HUAWEI BRAS, C=AT
        Validity
            Not Before: Sep 12 22:18:27 2022 GMT
            Not After : Sep  7 22:18:27 2042 GMT
        Subject: C=cn, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bits)
                Modulus:
                    00:c8:4f:09:9d:6a:53:95:6d:98:fa:22:f4:7c:5e:
                    f7:4b:08:3b:d2:19:3b:2d:4c:6c:0d:5f:b7:a2:91:
                    e8:99:de:91:12:df:3d:f5:c4:89:00:30:e7:7c:a6:
                    7a:03:18:1e:31:6a:65:34:05:cb:8a:29:f8:65:49:
                    7c:bd:81:cd:93:8d:be:63:e5:87:99:5d:28:6f:b6:
                    5c:c6:5c:4e:85:dc:26:26:db:a9:81:1a:19:b4:c4:
                    72:b7:8f:01:8d:55:8c:a0:58:cd:ef:d2:bd:d2:04:
                    5c:62:ab:3a:c5:71:d8:46:68:db:30:11:9b:48:46:
                    f7:5a:f7:70:a9:bf:ce:df:67:50:31:6c:c5:b3:f7:
                    0c:73:74:33:94:69:18:5b:57:74:5b:6b:49:bf:15:
                    05:17:01:9f:d0:13:71:c0:fe:45:13:07:2d:95:42:
                    55:e8:9e:77:e8:4e:f8:80:42:97:4f:26:78:a9:81:
                    61:8e:d3:ac:e8:5e:e0:61:37:84:f4:82:fa:8a:f9:
                    08:df:c3:70:50:9a:8e:3b:78:a1:f2:5d:3d:0b:fb:
                    fa:f4:67:ec:31:35:ff:4a:70:29:86:8c:a8:e2:46:
                    97:39:f7:58:0e:9e:ff:26:f1:7f:10:6b:68:33:f3:
                    7e:fd:ce:f3:a2:b1:b5:a4:81:88:52:2f:82:e0:28:
                    d3:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:33:06:DB:08:3C:3F:61:9B:C4:04:A5:36:8C:FD:34:D3:4C:73:B9:92

            X509v3 Subject Key Identifier:
                78:4C:65:05:E7:F6:B5:C8:48:C3:9D:E5:CE:3F:83:3A:62:84:EA:F9
            X509v3 CRL Distribution Points:

                Full Name:
                  DirName:CN = pre_crl, OU = CRL, O = HUAWEI BRAS, C = AT

                Full Name:
                  URI:http://90.255.210.71:8080/allcrl/pre_crl.crl

                Full Name:
                  URI:ldap://www.jitldap.com:5389/CN=pre_crl,OU=CRL,O=HUAWEI BRAS,C=AT?
certificateRevocationList?base?objectclass=cRLDistributionPoint

    Signature Algorithm: sha256WithRSAEncryption
         80:34:0d:ea:a0:7f:b8:a8:cb:8b:ae:a9:b3:85:b3:af:b2:1c:
         15:fc:7e:75:70:be:ff:37:75:6e:67:f8:37:33:ed:5c:5e:5b:
         3b:13:dc:44:7e:12:b6:85:b3:5c:b9:49:90:6c:96:33:57:a8:
         f3:c7:c4:04:2d:36:2a:54:fe:52:9a:16:64:66:a0:2e:a6:f1:
         0e:e0:29:f0:ac:69:d6:8a:f6:0d:43:41:ff:df:fd:06:03:39:
         75:8c:36:50:99:c3:89:c7:59:8c:65:7c:0c:6b:86:66:f3:a1:
         b1:6a:b7:43:0b:6d:3f:7d:82:27:45:b0:75:da:95:07:1d:d2:
         59:78:88:12:67:26:0f:65:fd:4f:05:4c:7c:74:16:4b:7d:ac:
         f8:a9:d1:2f:d6:57:4a:ad:aa:a3:ac:7c:30:de:6f:cf:3f:b4:
```



```
      d6:c5:84:e1:55:88:a2:40:52:12:5f:08:d8:50:54:ea:e7:c3:
      43:e2:6e:98:2a:5d:a4:e9:38:06:36:d6:40:25:a2:2e:0f:e1:
      95:cc:e8:f9:25:37:75:dd:67:0e:b9:0f:a9:5a:83:9c:6b:6c:
      f6:e1:bc:9d:fc:c1:a7:76:3f:33:81:e9:6d:25:a2:9f:1b:4e:
      61:f8:a9:12:de:33:02:2a:98:9d:04:a1:87:98:94:c4:11:cc:
      af:07:1b:68


Pki realm name: abc
Certificate file name: abc_local.cer
Certificate peer name: -
```

配置脚本

```
#
sysname DeviceA
#
pki entity user01
 country cn
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
 fqdn test.abc.com
 ip-address 10.2.0.2
 email user@test.abc.com
#
pki realm abc
 entity user01
 rsa local-key-pair rsakey
#
interface 10GE0/0/1
 ip address 10.2.0.2 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.1.0.2 255.255.255.0
#
return
```

12.7 通过 CMPv2 协议在线申请和更新证书

12.7.1 了解通过 CMPv2 协议在线申请和更新证书

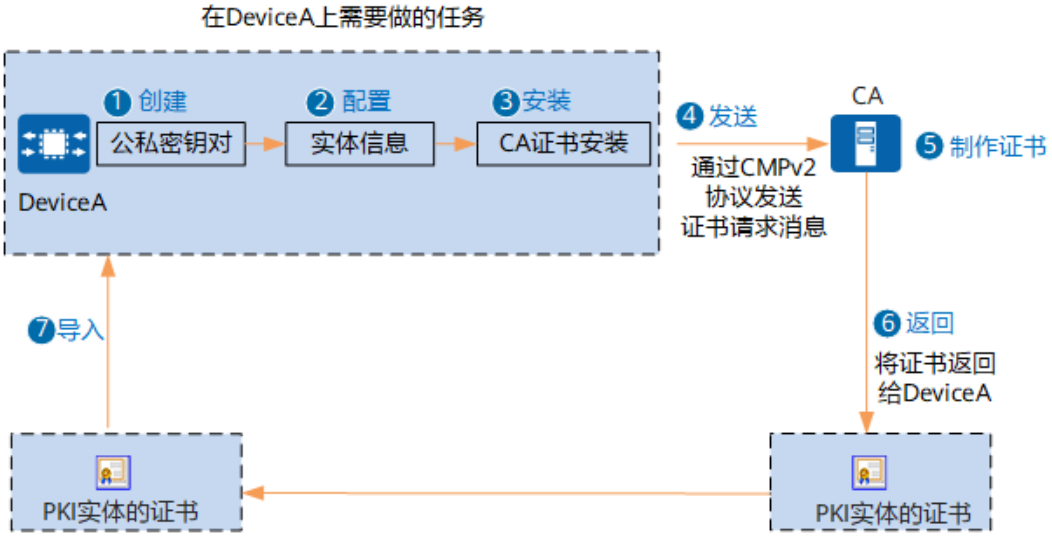
当设备可以访问CA，并且CA支持CMPv2协议时，可选择此方式申请和更新本地证书。

证书申请

证书申请即证书注册，就是一个PKI实体向CA自我介绍并获取证书的过程。用户可以通过CMPv2协议在线方式申请本地证书，CA根据证书注册请求消息为PKI实体制作证书。完成制作后，CA会自动触发将本地证书保存到设备的**flash:/pki/public**存储路径下，然后手动将本地证书保存到设备的内存中即可。

在线申请本地证书需要配置PKI实体信息、RSA密钥对、安装CA证书、申请本地证书、安装本地证书。通过CMPv2协议在线申请证书流程如**图12-12**所示。

图 12-12 在线证书申请流程



1. 创建公私密钥对。首先，在DeviceA上创建公私密钥对，因为在申请证书时会用到公钥信息。
2. 创建实体信息。申请证书时，DeviceA必须向CA提供能够证明自己身份的信息，实体信息代表的就是设备的身份信息，包括：通用名称（Common Name）、FQDN（Fully Qualified Domain Name）名称、IP地址、电子邮箱地址等。其中，通用名称是必须配置的，而其他几项是可选配置的。
3. 安装CA证书。PKI实体向CA发送证书注册请求消息时需要使用CA的公钥。
4. PKI实体向CA发送证书注册请求消息。

   通过CMPv2协议申请本地证书有首次申请本地证书和签名方式非首次申请本地证书两种方式。首次证书申请适用于设备第一次向CA申请证书的情况。CA制作完本地证书后，会返回CA证书和本地证书；签名方式非首次申请本地证书，CA只会返回本地证书，不会返回CA证书。

   - 首次申请本地证书IR（Initialization Request）

     首次申请本地证书提供以下两种CMPv2服务器认证PKI实体的方式。

     - 消息认证码方式：设备和CMPv2服务器共享一对消息认证码的参考值和秘密值。在进行首次证书申请的时候，设备会将这对参考值和秘密值加入到请求报文当中发送到CMPv2服务器，CMPv2服务器通过验证参考值和秘密值来鉴定设备的身份。
     - 签名方式：适用于当设备已经有了额外本地证书，向CA发起证书请求时，设备使用已有的额外本地证书的私钥来进行签名。

   - 签名方式非首次申请本地证书CR（Certification Request）

     适用于当设备已经有了额外本地证书，需要再申请本地证书的情况。向CA发起证书请求时，设备使用已有的额外本地证书的私钥来进行签名。
5. CA根据证书注册请求消息制作证书。经过CA的处理，最终获取到了DeviceA的证书**DeviceA.cer**。
6. CA自动将**DeviceA.cer**上传到DeviceA的**flash:/pki/public**存储路径下。
7. 导入证书。将证书导入到DeviceA的内存中。

证书更新

当证书过期、密钥泄露时，PKI实体必须更换证书，此时可以通过重新申请来达到更新的目的。通过CMPv2协议更新本地证书有两种方式：

- 手工更新证书，即密钥更新请求KUR（Key Update Request）

  密钥更新请求又称为证书更新请求，是对设备已有的证书（尚未过期且没有被吊销）进行更新操作。在更新过程中，使用现有的证书作为身份认证的手段。更新操作可以使用新的公钥，也可以使用原来的公钥。

- 自动更新证书

  为了避免业务的中断，在有效期截止前必须申请新的证书，而使用手工更新证书的方式容易出现忘记更新证书的情况。设备支持证书的自动更新功能，当系统检测到时间超过了设置的证书自动更新时间之后，会自动向CMPv2服务器发起证书的更新请求。申请的新证书会同时替换存储介质中的证书文件和内存中对应的证书，业务不会中断。

  此方式可以对IR方式申请的本地证书或KUR方式更新的本地证书进行自动更新。

12.7.2 通过 CMPv2 协议在线申请和更新本地证书

前提条件

已完成申请证书的预配置操作，具体可以参见**申请证书预配置**。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 配置设备保存证书时的文件格式。

```
pki file-format { der | pem }
```

步骤3 创建CMP会话并进入CMP会话视图，或者直接进入CMP会话视图。

```
pki cmp session session-name
```

CMP会话是一个本地概念，一个设备上配置的CMP会话对CA和其他设备是不可见的。

步骤4 配置设备使用CMPv2方式申请证书时使用的PKI实体名称。

```
cmp-request entity entity-name
```

步骤5 为CMP会话配置CA的名称。

```
cmp-request ca-name ca-name
```

配置的CA名称中各个字段的顺序必须要和实际CA证书中的顺序保持一致，否则CMPv2服务器会认为是错误的。

步骤6 配置CMPv2服务器的URL。

```
cmp-request server url [ esc ] url-addr
```

步骤7 配置CMPv2方式申请证书时使用的RSA密钥对。

```
cmp-request rsa local-key-pair key-name [ regenerate [ key-bit ] ]
```

如果配置了**regenerate**参数，则证书自动更新时，系统会生成新的RSA密钥对去申请新证书，并且用新的证书和RSA密钥对替换原有的证书和RSA密钥对。否则证书自动更新时，系统会继续使用原来的RSA密钥对。

步骤8 **可选:** 配置建立TCP连接使用的源地址。

```
source { interface interface-type interface-number | ip-address }
```

如果指定接口，请确保该接口为三层接口，且接口下已经配置了IP地址。

步骤9 **可选:** 配置使用CMPv2协议进行证书申请的报文加密方式。

```
cmp-request integrity-algorithm { hmac-sha256 | hmac-sha1 }
```

使用CMPv2协议进行证书申请时，报文需要哈希算法进行加密。缺省情况下，使用CMPv2协议进行证书申请时使用的加密算法为SHA256。

说明

出于安全性考虑，不建议使用该特性提供的弱安全算法或弱安全协议。如果确实需要使用，请执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包WEAKEA。设备默认自带弱安全算法/协议特性包WEAKEA，特性包安装或卸载的详细步骤请参见《配置指南-系统管理配置》中的“升级维护配置”。

步骤10 **可选:** 配置验证CA响应签名的证书文件。

当使用签名方式申请本地证书时，设备需要验证本地证书是否是合法CA颁发的，此时需要执行以下操作。消息认证码方式不需执行如下操作。

```
cmp-request verification-cert cert-file-name
```

- 如果配置了此命令，并且CMPv2服务器的响应报文是签名方式时，则设备使用该命令行配置的*cert-file-name*证书来验证CMPv2服务器的响应签名。此处配置的证书为CA证书，即CA自身的证书。

  说明

  如果存在RA，且证书注册请求消息由RA机构进行签发，此时*cert-file-name*需要配置为RA机构的CA证书，否则证书校验失败，证书申请失败。

- 如果未配置此命令，并且CMPv2服务器的响应报文是签名方式时，则依据设备以及CMPv2服务器响应中的证书构建证书链，验证CMPv2服务器的响应签名。

步骤11 根据实际情况配置申请本地证书的方式。

- 使用消息认证码方式首次申请本地证书（IR）。

  a. 配置使用CMPv2协议进行首次证书申请（IR）的认证方式。

  ```
  cmp-request origin-authentication-method message-authentication-code
  ```

  缺省情况下，使用CMPv2协议进行首次证书申请（IR）的认证方式为消息认证码方式。

  b. 配置消息认证码的参考值和秘密值。

  ```
  cmp-request message-authentication-code reference-value [ secret-value ]
  quit
  ```

  说明

  消息认证码的秘密值，可以从CMPv2服务器Web界面下的“CMP secret key”参数获取。参考值用户可以自己设置：输入字符串形式，区分大小写，不支持问号，明文时输入长度范围是1～128，密文时输入长度范围是48～188。

  c. 在系统视图下，根据CMP会话的配置信息向CMPv2服务器进行首次证书申请（IR）。

  ```
  pki cmp initial-request session session-name
  ```

  配置后，系统首先会检查CMP会话中的配置是否可以进行证书申请。如果条件不满足，会给出错误的提示信息。如果条件满足，会依据配置内容发起首次证书请求。申请下来的证书将以文件的形式保存到存储介质中，不会执行

导入内存的操作。同时，若服务器端在响应中给出CA证书，则CA证书也会以文件形式保存起来。

- 使用签名方式首次申请本地证书（IR）。
  a. 配置使用CMPv2协议进行首次证书申请（IR）的认证方式。
  ```
  cmp-request origin-authentication-method signature
  ```
  b. 配置CMPv2请求中用于证明身份的证书。
  ```
  cmp-request authentication-cert cert-name
  quit
  ```
  此证书是额外证书，并且必须由受CA信任的证书申请机构为设备颁发。
  c. 在系统视图下，根据CMP会话的配置信息向CMPv2服务器进行首次证书申请（IR）。
  ```
  pki cmp initial-request session session-name
  ```
  配置后，系统首先会检查CMP会话中的配置是否可以进行证书申请。如果条件不满足，会给出错误的提示信息。如果条件满足，会依据配置内容发起首次证书请求。申请下来的证书将以文件的形式保存到**flash:/pki/public**存储路径下，不会执行导入到设备内存的操作。同时，若服务器端在响应中给出CA证书，则CA证书也会以文件形式保存起来。
- 使用签名方式非首次申请本地证书（CR）
  a. 配置CMPv2请求中用于证明身份的证书。
  ```
  cmp-request authentication-cert cert-name
  quit
  ```
  此证书是额外证书，并且必须由受CA信任的证书申请机构为设备颁发。
  b. 在系统视图下，根据CMP会话的配置信息向CMPv2服务器进行证书申请（CR）。
  ```
  pki cmp certificate-request session session-name
  ```
  配置后，系统首先会检查CMP会话中的配置是否可以进行证书申请。如果条件不满足，会给出错误的提示信息。如果条件满足，会依据配置内容发起证书请求。申请下来的证书将以文件的形式保存到存储介质中，不会执行导入内存的操作。

步骤12 根据实际情况选择更新本地证书的方式。

- 手动更新本地证书
  a. 进入CMP会话视图，配置CMPv2请求中用于证明身份的证书。
  ```
  pki cmp session session-name
  cmp-request authentication-cert cert-name
  quit
  ```
  此证书是CA已经颁发给设备的本地证书，同时也是将要被更新的本地证书。
  b. 在系统视图下，根据CMP会话的配置信息向CMPv2服务器进行密钥更新请求（KUR）。
  ```
  pki cmp keyupdate-request session session-name
  ```
  向CMPv2服务器进行密钥更新请求时，同时也会重新申请本地证书。

  配置后，系统首先会检查CMP会话中的配置是否可以进行证书更新申请。如果条件不满足，会给出错误的提示信息。如果条件满足，会依据配置内容发起证书更新请求。申请下来的证书将以文件的形式保存到存储介质中，不会执行导入内存的操作。
- 自动更新证书
  a. 进入CMP会话视图，配置CMPv2请求中用于证明身份的证书。
  ```
  pki cmp session session-name
  cmp-request authentication-cert cert-name
  ```
  此证书是CA已经颁发给设备的本地证书，同时也是将要被更新的本地证书。

b. 开启使用CMPv2方式自动更新证书功能。
```
certificate auto-update enable
```

c. 配置证书自动更新的时间，以当前使用证书有效期的百分比形式体现。
```
certificate update expire-time valid-percent
quit
```
缺省情况下，证书更新时间的默认百分比是50%。

配置后，当系统检测到时间达到*valid-percent*时，会自动发起证书更新请求，并依据**cmp-request rsa local-key-pair**命令的配置决定是否创建新的RSA密钥对。申请到新的证书后，系统会使用新的证书和RSA密钥对替换原有的证书和RSA密钥对。

----结束

检查配置结果

执行命令**display pki cmp statistics** [**session** *session-name*]，查看CMP会话的统计信息。

12.7.3 安装本地证书

背景信息

通过CMPv2协议在线申请本地证书，系统会自动将本地证书存放在**flash:/pki/public**存储路径下。

本地证书存放在上述指定路径下后，还需手动导入到设备的内存中。只有将本地证书导入到设备的内存中，在设备重启后系统才能自动加载证书文件。

说明

请确保本地证书文件不超过1M，避免安装失败。

预置的本地证书作为华为设备的身份标识，缺省情况下为设备中的用户登录业务提供证书认证。

操作步骤

步骤1 进入系统视图。
```
system-view
```

步骤2 **可选:** 将预置的本地证书导入到default域下。
```
pki import-certificate default_local realm default
```

预置的本地证书可以被删除，如果想要恢复被删除的预置Local证书，可以执行此命令将证书从NVRAM中加载到default域下。

步骤3 创建PKI域。
```
pki realm realm-name
quit
```

步骤4 在系统视图下，将本地证书导入到设备的内存中。

- 当在本PKI实体下创建RSA密钥对，通过PKI实体信息和RSA密钥对去CA申请本地证书时，只需执行如下命令导入本地证书到内存中即可，因为在本地创建RSA密钥对时RSA密钥已经默认导入到设备的内存中。
```
pki import-certificate local [ [ realm realm-name ] { der | pkcs12 | pem } ] filename file-name
[ cert-name cert-name ] [ no-check-same-name ] [ no-check-hash-alg ]
```

- 当使用其他PKI实体产生的密钥对和其他PKI实体的证书时，需要导入证书和密钥对文件。一般证书及其密钥对有两种存在形式，一种是证书文件中包含密钥对文件，两者以一个文件的形式存在；另一种是证书和密钥对相互独立以两个文件形式存在。

  不同形式下，将其导入内存所使用的方法不同，具体如下。

  - 证书文件中包含密钥对文件。
    pki import rsa-key-pair *keyname* { **pem** | **pkcs12** } *filename* [**exportable**] [**password** *password*]
  - 证书文件和密钥对文件独立存在。

    # 导入证书文件。
    pki import-certificate local [[**realm** *realm-name*] { **der** | **pkcs12** | **pem** }] **filename** *file-name* [**cert-name** *cert-name*] [**no-check-same-name**] [**no-check-hash-alg**]

    # 导入密钥对文件。
    pki import rsa-key-pair *keyname* **exclude-cert** { **pem** | **pkcs12** } *filename* [**exportable**] [**password** *password*]

说明

若不指定待导入证书的格式，系统将自行识别导入。

步骤5 （可选）配置内存中的本地证书的过期预告警时间。

pki set-certificate expire-prewarning *day*

----结束

检查配置结果

执行命令**display pki certificate local** [**realm** *realm-name* | **filename** *filename*]，查看设备上已加载的本地证书的内容。

12.7.4 检查证书有效性

前提条件

已在设备上安装CA证书和本地证书。

背景信息

在安装CA证书和本地证书以后，使用每一个证书之前，必须对本地设备的证书进行验证，以确保证书的合法性。证书验证包括对签发时间、签发者信息以及证书的有效性几方面进行验证。证书验证的核心是检查CA在证书上的签名，并确定证书仍在有效期内，而且未被撤销。

为完成证书验证，本地设备需要下面的信息：CA证书、CRL、本地证书及其私钥及证书认证相关配置信息。

本地证书验证的主要过程如下：

1. 使用CA证书的公钥验证CA的签名是否正确。

   为验证一个证书的合法性，首先需要获得颁发这个证书的CA的公钥（即获得CA证书），以便检查该证书上CA的签名。一个CA可以让另一个更高层次的CA来证明其证书的合法性，这样顺着证书链，验证证书就变成了一个迭代过程，最终这个链必须在某个“信任点”（一般是持有自签名证书的根CA或者是PKI实体信任的中间CA）处结束。

任何PKI实体，如果它们共享相同的根CA或子CA，并且已获取CA证书，都可以验证对端证书。

证书链的验证过程是一个从目标证书（待验证的PKI实体证书）到信任点证书逐层验证的过程。一般情况下，当验证对端证书链时，验证过程在碰到第一个可信任的证书或CA机构时结束。

2. 根据证书的有效期，验证证书是否过期。
3. 检查证书的状态，即通过CRL、OCSP和None方式检查证书是否被撤销。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 检查CA证书或本地证书的有效性。

```
pki validate-certificate { ca | local } { realm realm-name | filename file-name }
```

pki validate-certificate ca命令只能验证根CA的CA证书有效性，不能验证从属CA的CA证书有效性。在多级CA的环境中，当设备上导入了多个CA证书时，只能使用**pki validate-certificate local**命令来验证从属CA的CA证书有效性。

----结束

12.7.5 举例：通过 CMPv2 协议在线申请和更新本地证书

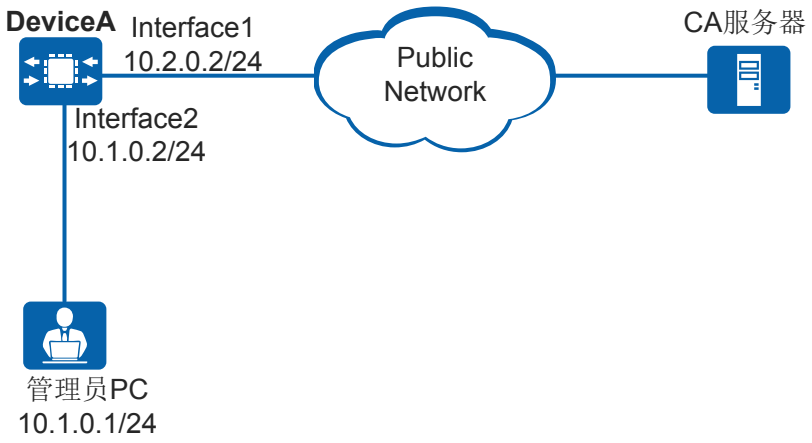
组网需求

如图所示，某企业在网络边界处部署了DeviceA作为出口网关，使用CMPv2协议向公网上的CA服务器在线首次申请证书，申请成功后自动将本地证书下载到设备存储介质中。当证书的有效期时间达到80%时，自动更新本地证书。

图 12-13 配置为 PKI 实体在线申请本地证书组网图

说明

本例中interface1、interface2分别代表10GE0/0/1、10GE0/0/2。



说明

配置前请确保各设备之间路由可达。

配置思路

采用如下思路配置通过CMPv2协议为PKI实体首次申请本地证书：

1. 配置接口的IP地址。
2. 创建RSA密钥对，实现申请本地证书时携带公钥。
3. 配置PKI实体，实现申请本地证书时携带PKI实体信息用来标识PKI实体的身份。
4. 通过CMPv2协议申请和自动更新证书，并使用消息认证码来验证消息，实现自动下载CA和本地证书。
5. 安装本地证书，实现证书生效，即设备可以使用证书来保护通信。

数据准备

为完成此配置示例，需准备如下的数据：

- CA名称：为CA证书的主题字段。
- 消息认证码的参考值和秘密值：需要从CMPv2服务器上获取消息认证码的参考值和秘密值。
- 在设备上导入CA服务器的CA证书。

操作步骤

步骤1 配置接口的IP地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] ip address 10.2.0.2 24
[DeviceA-10GE0/0/1] quit
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] ip address 10.1.0.2  24
[DeviceA-10GE0/0/2] quit
```

步骤2 创建RSA密钥对。

创建一个2048位的RSA密钥对rsa_cmp，并设置为可以从设备上导出。

```
[DeviceA] pki rsa local-key-pair create rsa_cmp exportable
 Info: The name of the new key-pair will be: rsa_cmp
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
 Generating key-pairs finished
```

步骤3 配置PKI实体，标识申请证书PKI实体的身份信息。

配置PKI实体为user01。

```
[DeviceA] pki entity user01
[DeviceA-pki-entity-user01] common-name hello
[DeviceA-pki-entity-user01] country cn
[DeviceA-pki-entity-user01] email user@test.abc.com
[DeviceA-pki-entity-user01] fqdn test.abc.com
[DeviceA-pki-entity-user01] ip-address 10.2.0.2
[DeviceA-pki-entity-user01] state jiangsu
[DeviceA-pki-entity-user01] organization huawei
[DeviceA-pki-entity-user01] organization-unit info
[DeviceA-pki-entity-user01] quit
```

步骤4 配置CMP会话。

创建CMP会话cmp。


```
[DeviceA] pki cmp session cmp
```

指定CMP会话引用的PKI实体名称。

```
[DeviceA-pki-cmp-session-cmp] cmp-request entity user01
```

配置CA的名称，举例中假设为“C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB”。

说明

配置的CA名称中各个字段的顺序必须要和实际CA证书中的顺序保持一致，否则服务器端会认为是错误的。

```
[DeviceA-pki-cmp-session-cmp] cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"
```

配置申请证书的URL。

```
[DeviceA-pki-cmp-session-cmp] cmp-request server url http://10.3.0.1:8080
```

指定申请证书时使用的RSA密钥对，并设置为证书自动更新时同时更新RSA密钥对。

```
[DeviceA-pki-cmp-session-cmp] cmp-request rsa local-key-pair rsa_cmp regenerate
```

首次申请证书时，使用消息认证码认证。配置消息认证码的参考值和秘密值，举例中假设分别为“1234”和“Huawei@RSA1234”。

```
[DeviceA-pki-cmp-session-cmp] cmp-request message-authentication-code 1234 Huawei@RSA1234
[DeviceA-pki-cmp-session-cmp] quit
[DeviceA] pki cmp initial-request session cmp
```

获取到的CA、本地证书将会分别被命名为cmp_ca1.cer和cmp_ir.cer保存在设备存储介质中。

步骤5 安装证书。

证书导入后，设备存储介质中cmp_ca1.cer和cmp_ir.cer默认删除，如果不需要删除，请根据设备提示信息选择N进行保留。

导入CA证书到内存。

```
[DeviceA] pki import-certificate ca filename cmp_ca1.cer
 The CA's Subject is /C=cn/ST=beijing/L=BB/O=BB/OU=BB/CN=BB
 The CA's fingerprint is:
   SHA1   fingerprint:2C:2B:C0:31:66:A6:95:A0:7A:AC:EF:3D:37:1C:9A:4D:01:BA:09:4D
   SHA256 fingerprint:CA:FC:6B:94:53:E9:E3:D7:D3:E1:F4:75:3F:DB:C4:0F:0A:B9:F1:AD:03:0B:A8:0D:EE:73:4A:
83:54:EF:1F:81
 Is the fingerprint correct?(Y/N):y
 Info: Succeeded in importing the certificate.
 Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select [Y/N]:y
 Info: Delete Success.
```

导入本地证书到内存。

```
[DeviceA] pki import-certificate local filename cmp_ir.cer
 Info: Succeeded in importing the certificate.
 Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select [Y/N]:y
 Info: Delete Success.
```

步骤6 配置自动更新证书功能。

在CMP会话视图下开启使用CMPv2方式自动更新证书功能。

```
[DeviceA] pki cmp session cmp
[DeviceA-pki-cmp-session-cmp] cmp-request authentication-cert cmp_ir.cer
[DeviceA-pki-cmp-session-cmp] certificate auto-update enable
[DeviceA-pki-cmp-session-cmp] quit
```

在CMP会话视图下配置证书自动更新的时间，设置为当前证书有效期的80%。

```
[DeviceA] pki cmp session cmp
[DeviceA-pki-cmp-session-cmp] certificate update expire-time 80
[DeviceA-pki-cmp-session-cmp] quit
```

----结束

检查配置结果

- 证书申请成功后，可执行命令**display pki certificate local**查看已经导入内存的本地证书的内容。

```
[DeviceA] display pki certificate local filename cmp_ir.cer
 The  x509_obj type is Cert:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1144733510 (0x443b3f46)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, ST=beijing, L=BB, O=BB, OU=BB, CN=BB
        Validity
            Not Before: Jun 12 09:33:10 2012 GMT
            Not After : Aug 13 02:38:27 2016 GMT
        Subject: C=cn, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d3:12:fe:57:48:c6:a5:10:12:e9:2f:f9:2a:ff:
                    7b:2a:d8:45:69:11:c4:85:30:c4:9a:4d:0f:ad:58:
                    e7:56:cd:5c:f0:18:e1:c3:6d:44:c2:c3:5e:64:22:
                    d1:28:c9:c3:37:3c:34:ed:28:04:7f:62:9e:8b:94:
                    af:bc:72:de:f6:72:7f:e4:d8:45:31:fd:f9:ac:ce:
                    5a:b9:c7:1b:23:53:00:28:a6:3b:f5:61:69:5d:ab:
                    67:cb:bb:e8:96:2f:ce:ab:2c:6b:91:5b:26:91:86:
                    8f:80:a9:b0:66:c1:16:3d:31:55:a2:d4:b5:5a:af:
                    85:88:6e:99:f8:f8:53:58:77:26:91:ed:0e:94:ad:
                    c5:8d:53:67:67:55:08:8d:90:38:e0:5e:96:37:b9:
                    64:0e:36:e7:cf:9a:d2:77:e4:b0:24:05:a6:eb:03:
                    6e:ff:f7:ab:be:93:9e:8c:66:7d:31:66:be:6d:c8:
                    f3:17:9d:86:19:88:21:2d:d9:69:86:5f:b2:55:a4:
                    db:bc:d7:d0:6b:ac:66:ac:e4:63:9c:66:79:9c:42:
                    5c:83:b8:9e:4b:6e:67:85:a2:47:19:f1:5c:c0:3c:
                    c9:a3:47:02:a8:53:69:59:9e:d9:c7:5e:90:83:8d:
                    ac:cd:21:3c:d5:31:39:49:84:e6:f8:f4:e0:44:dd:
                    5d:7b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
    Signature Algorithm: sha1WithRSAEncryption
        53:d5:79:31:7b:40:52:aa:ec:a9:35:ed:07:62:32:c4:ce:22:
        d3:37:0e:83:0c:4c:fa:61:dd:8c:db:a8:d3:fd:6a:ca:0e:3c:
        91:2c:91:ab:92:31:34:b5:87:1e:30:a4:ff:94:9c:d2:71:3c:
        6b:1f:4f:be:a7:20:f2:e1:c2:ad:71:8b:c2:79:0f:50:1f:3c:
        f9:87:df:1d:ee:3d:38:8c:f3:30:b7:3b:00:9b:72:38:b0:68:
        e1:c0:08:f4:02:91:81:a8:fa:51:9e:53:0d:03:b3:6b:0e:e2:
        62:80:ef:2a:a0:cb:9b:9b:91:21:7c:df:fe:6a:38:cc:03:36:
        9c:fc

Pki realm name: -abc
Certificate file name: cmp_ir.cer
Certificate peer name: -
```

- 证书申请成功后，可执行命令**display pki certificate ca**查看已经导入内存的CA证书的内容。

```
[DeviceA] display pki certificate ca filename cmp_ca1.cer
 The x509 object  type is certificate:
Certificate:
    Data:
```



```
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=cn, ST=beijing, L=BB, O=BB, OU=BB, CN=BB
    Validity
      Not Before: Aug 15 02:38:27 2011 GMT
      Not After : Aug 13 02:38:27 2016 GMT
    Subject: C=cn, ST=jiangsu, O=huawei, OU=info, CN=hello
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        RSA Public-Key: (1024 bit)
        Modulus:
          00:b7:3e:65:7f:3b:3c:18:b8:87:34:39:76:3c:87:
          39:f7:a9:b3:35:9b:e0:e0:5b:c7:4f:3c:bb:fa:dd:
          da:93:0b:55:6e:eb:ba:52:c8:86:d1:cf:14:1e:1c:
          35:c6:53:68:f3:51:e7:2c:d4:b8:fa:0f:b3:04:ef:
          3f:a0:b3:4d:78:c1:26:88:26:15:41:3d:14:7f:67:
          3e:2f:35:32:ce:c7:73:73:43:5c:12:d3:0f:a0:ec:
          96:ae:55:61:27:32:39:a4:f8:32:a1:68:50:e6:3d:
          2b:39:6d:42:e8:09:5d:4f:98:46:6e:fc:80:87:0e:
          36:ca:09:7a:ca:2f:dd:ad:d3
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE
      X509v3 Subject Key Identifier:
        4F:67:F4:CB:F4:C3:F7:61:2C:BD:FF:1D:D1:29:FD:39:28:9F:3B:8B
      X509v3 Key Usage:
        Certificate Sign, CRL Sign
      Netscape Cert Type:
        SSL CA, S/MIME CA, Object Signing CA
      Netscape Comment:
        xca certificate
  Signature Algorithm: sha1WithRSAEncryption
    75:43:24:eb:db:ee:7d:05:30:88:b8:1b:d5:32:ca:51:49:74:
    04:94:fe:d0:31:29:6f:72:c7:4a:86:ac:2a:4c:45:24:9d:3c:
    b4:30:b5:d1:43:88:29:f7:b4:88:b8:37:dc:dd:f4:fa:42:34:
    1c:e6:a5:bc:bb:0b:37:ef:db:8c:b2:b0:bd:97:7f:15:ae:6c:
    71:1b:ff:f1:90:13:74:a4:1f:7c:f7:4e:80:5b:42:aa:6b:22:
    2a:cf:04:48:29:20:c0:b2:95:38:11:06:be:76:f0:cb:8d:4a:
    c6:1a:50:af:31:81:58:ac:14:fe:89:f2:e0:bb:95:3c:94:d0:
    54:96

Pki realm name: -
Certificate file name: cmp_ca1.cer
Certificate peer name: -
```

配置脚本

DeviceA的配置文件

```
#
sysname DeviceA
#
pki entity user01
 country cn
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
 fqdn user@test.abc.com
 ip-address 10.2.0.2
 email user@user@test.abc.com
#
interface 10GE0/0/1
 ip address 10.2.0.2 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.1.0.2 255.255.255.0
```



```
#
pki import-certificate ca filename cmp_cal.cer
pki import-certificate local filename cmp_ir.cer
pki cmp session cmp
 cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"
 cmp-request authentication-cert cmp_ir.cer
 cmp-request entity user01
 cmp-request server url http://10.3.0.1:8080
 cmp-request rsa local-key-pair rsa_cmp regenerate
 cmp-request message-authentication-code 1234 %@%##!!!!!!!!!!"!!!!'!!!!*!!!!#-Yt'T`/_H5O<-:ydTz$hk./
U,Huq3[u0w8!!!!!!!!!!!!!!~!!!!h#a6(1U`jWv[fB3ZRI\7~b5jYCD+l0/R)RMFWV,:%@%#
 certificate auto-update enable
 certificate update expire-time 80
#
return
```

12.8 配置自签名证书

背景信息

如果设备无法向CA申请本地证书，可以通过设备生成自签名证书，生成的证书以文件形式保存在存储器中，实现简单的证书颁发功能。用户可以将证书导出供其他设备使用。自签名证书是设备为自己颁发的证书，由设备预置CA进行签名。即证书颁发者和证书主体相同，自签名证书带有签名信息，不需要向其他机构申请签名。

说明

设备不支持对其生成的自签名证书进行生命周期管理（如证书更新、证书撤销等），为了确保设备和证书的安全，建议用户替换为自己的本地证书。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建自签名证书或不带签名的证书。

```
pki create-certificate [ self-signed ] filename file-name
```

配置时，会提示用户输入证书的一些信息，比如PKI实体属性、证书文件名称、证书有效期和RSA密钥长度等。

指定**self-signed**参数时，创建自签名证书。不指定此参数时，创建不带签名的证书。不带签名的证书是在设备上生成一本证书，但不进行签名，需要向CA机构申请签名，证书颁发者是CA。

创建的自签名证书或不带签名的证书的文件格式为PEM。

----结束

12.9 验证对端实体证书

12.9.1 配置证书撤销状态检查

背景信息

PKI实体两端建立安全连接时，经常需要检查对端实体的本地证书是否有效，如果无效，两端就不能建立连接。但由于用户名称的改变、私钥泄露或业务中止等原因，有

时CA机构需要撤销公钥及相关的PKI实体的绑定关系。PKI实体需要及时获取到对端实体证书的状态才能保证两端的通信安全。

设备提供三种检查证书状态的方式：CRL方式、OCSP方式、None方式。

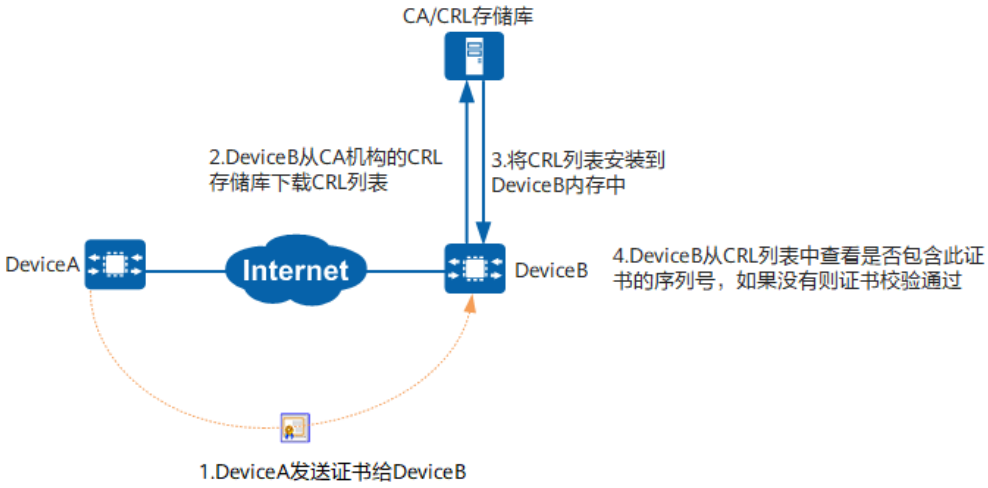
如果配置了多种撤销状态的检查方式，系统会按照配置的先后顺序执行。当前一种方式不可用（如服务器连接不上）时才会使用后边的方式。当前面配置的CRL方式、OCSP方式均不可用时，如果配置了None方式，此时认为证书有效。以配置了**certificate-check crl ocsp none**命令为例，先使用CRL方式检查证书是否有效，如果CRL方式不可用，则使用OCSP方式，如果两种方式都不可用，则认为证书是有效的。

用户可以根据实际需求灵活选取检查证书状态的方式。

- CRL方式

  CRL方式是利用CRL存储库对CRL信息存储的功能，通过查询证书是否包含在证书撤销列表中，确定证书的状态。任何一个证书被撤销以后，证书的序列号都会被记录在CRL证书撤销列表中。当PKI实体验证本地证书时，先查找本地内存的CRL，如果本地内存没有CRL，则需下载CRL并安装到本地内存中，如果对端实体的本地证书在CRL中，表示此证书已被撤销。

  图 12-14 CRL 方式证书验证流程

  说明

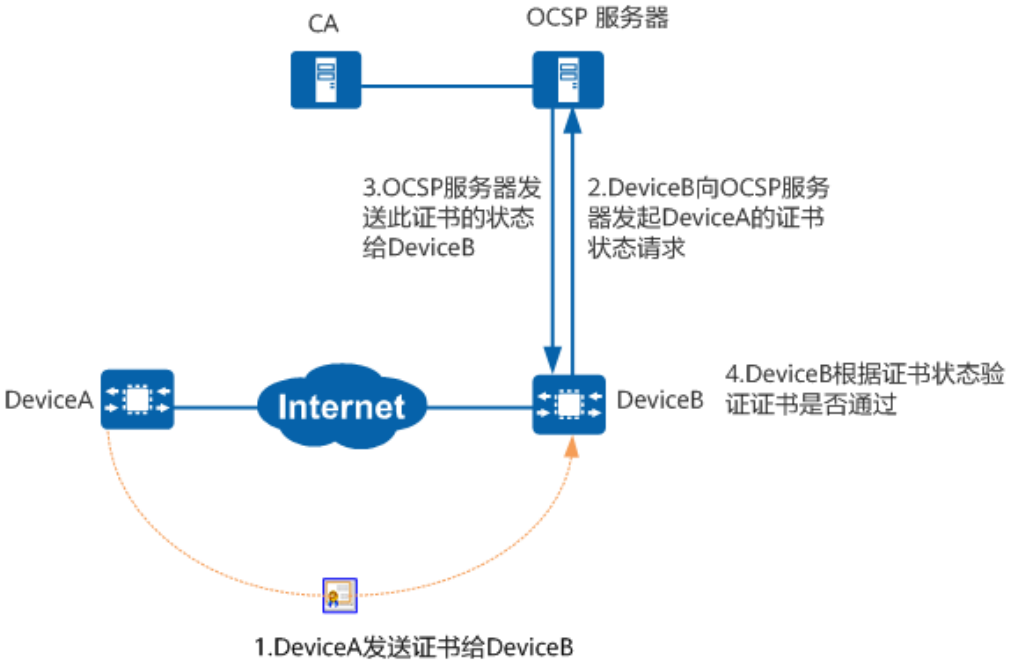
  PKI实体可以通过LDAPv3模板方式下载CRL。PKI实体必须经常下载CRL以确保列表的更新。设备缺省分配了大约5K的内存空间用于处理和缓存CRL，如果超出设备给CRL预留的存储空间大小，则新的证书撤销数据不能导入进去。如果想要导入新的证书撤销数据，需要删除旧的证书撤销数据。

- OCSP方式

  PKI实体间使用证书方式进行消息协商时，可以通过OCSP方式实时检查对端实体的证书状态。OCSP克服了CRL的主要缺陷：PKI实体必须经常下载CRL以确保列表的更新。当PKI实体访问OCSP服务器时，会发送一个对于证书状态信息的请求。OCSP服务器会回复一个“有效”、“过期”或“未知”的响应。

  - 有效表示证书没有被撤销。
  - 过期表示证书已被撤销。
  - 未知表示OCSP服务器不能判断请求的证书状态。

图 12-15 OCSP 服务器方式证书验证流程



- None方式

  如果PKI实体没有可用的CRL和OCSP服务器，或者不需要检查PKI实体的本地证书状态，可以采用None方式，即不检查证书是否被撤销。

说明

全局证书撤销状态检查方式有CRL方式和None方式。

PKI域中的证书撤销状态检查方式有CRL方式、OCSP方式和None方式。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建PKI域并进入PKI域视图，或者直接进入PKI域视图。

```
pki realm realm-name
```

缺省情况下，系统下存在名称为**default**的PKI域，该域可以修改但不能删除。

步骤3 配置PKI域中证书撤销状态的检查方式。

```
certificate-check { { crl | ocsp } * [ none ] | none }
```

缺省情况下，系统未配置PKI域中证书撤销状态的检查方式。

如果没有配置本命令，将以全局的证书撤销状态检查方式为准，即以在系统视图下配置的**pki certificate-check crl** [**none**]命令、**pki certificate-check none**命令或**undo pki certificate-check**命令为准。

步骤4 请根据CA提供的服务方式选择配置检查对端实体本地证书状态的方式。

- 自动更新CRL方式

  a. 退出到系统视图。

  ```
  quit
  ```

b. 配置设备保存CRL时的文件格式。
pki file-format { **der** |**pem** }

说明

缺省情况下，设备保存CRL时的文件格式为PEM。

c. （可选）开启全局证书撤销状态CRL方式检查功能。
pki certificate-check crl [**none**]

缺省情况下，全局证书吊销状态的CRL检查处于开启状态，且当CRL方式不可用时认为证书有效。

d. 进入PKI域视图，开启CRL自动更新功能。
pki realm *realm-name*
crl auto-update enable

缺省情况下，CRL自动更新功能处于关闭状态。

e. 配置CRL自动更新的时间间隔。
crl update-period *interval*

缺省情况下，CRL自动更新的时间间隔为8小时。

f. 配置向LDAP服务器获取CRL时使用的属性和标识符。
crl ldap [**attribute** *attr-value*] **dn** *dn-value*

缺省情况下，系统未配置向LDAP服务器获取CRL时使用的属性和标识符。

g. 配置通过LDAPv3模板方式自动更新CRL。
ldap-server-template *template-name*

ldap-server-template *template-name*用来在PKI域下引用LDAP服务器模板。LDAP服务器模板的具体配置，请参见《配置指南-用户接入与认证配置》的“AAA配置”中的“配置对接的LDAP服务器”节点。

h. **可选:** 立即更新CRL，将CRL导入设备的内存中。

自动更新CRL需要达到CRL自动更新的时间时才能更新，如果想要立刻更新CRL信息，则可以使用立即更新CRL功能。
pki get-crl realm *realm-name*
pki import-crl realm *realm-name* **filename** *file-name*

立即更新CRL后，新的CRL会替换设备存储介质中原来的CRL，同时新的CRL也会被自动导入设备内存中替换原来的CRL。

- 手动更新CRL方式

a. 退出到系统视图。
quit

b. 配置设备保存CRL时的文件格式。
pki file-format { **der** | **pem** }

c. 根据LDAP方式下载CRL。
pki ldap-server-template *template-name* **attribute** *attr-value save-name* **dn** *dn-value*

d. 将CRL导入设备的内存中。
pki import-crl [**realm** *realm-name*] **filename** *file-name*

- OCSP方式

a. 在PKI域视图下，为PKI域配置CA的名称。
pki realm *realm-name*
ca-name { *name-string* | **from-certificate filename** *file-name* }

缺省情况下，系统没有为PKI域配置CA的名称。

指定PKI域中的CA证书名称前必须将CA证书导入该域下。在PKI域中指定了CA的名称后，就会将该PKI域和特定的CA关联起来，通过CA的名称可以确定对应的PKI域，进而可以确定证书撤销状态的检查方式等配置。

配置*name-string*参数时，必须确保配置的CA名称与CA证书的主题（subject name）中CN、O、OU等单元的位置顺序完全一致。为了避免手工配置带来的错误，可以配置**from-certificate**参数从CA证书中读取CA的名称。

b. **可选:** 配置建立TCP连接使用的源地址。
source { **interface** *interface-type interface-number* | *ip-address* }

缺省情况下，设备使用出接口的IP地址作为建立TCP连接的源地址。

如果指定接口，请确保该接口为三层接口，且接口下已经配置了IP地址。

c. 配置OCSP服务器的URL。
ocsp url [**esc**] *url-address*

或者配置从CA证书的AIA选项中获取OCSP服务器的URL。
ocsp-url from-ca

d. **可选:** 配置PKI实体发送OCSP请求时带有Nonce扩展。
ocsp nonce enable

缺省情况下，PKI实体发送OCSP请求时带有Nonce扩展。

通过该功能可以增强PKI实体与OCSP服务器通信时的安全性和可靠性。配置后，PKI实体与OCSP服务器通信时发送的OCSP请求中带有Nonce扩展，内容为随机数。对于OCSP服务器发出的响应报文，可以不包含Nonce扩展，但是如果包含了Nonce扩展，则必须与OCSP请求中的Nonce扩展一致。

e. **可选:** 开启OCSP请求消息签名功能。
ocsp signature enable
quit

缺省情况下，OCSP请求消息签名功能处于关闭状态。

如果OCSP服务器要求对OCSP请求消息进行签名验证，此时需要配置本命令。

f. **可选:** 在系统视图下将OCSP服务器证书导入到设备的内存中。
pki import-certificate ocsp [**realm** *realm-name*] { **der** | **pkcs12** | **pem** } **filename** *file-name* [**cert-name** *cert-name*] [**no-check-same-name**]

g. **可选:** 开启OCSP证书校验OCSP服务器报文的功能。
pki validate ocsp-server-certificate enable

缺省情况下，OCSP证书校验OCSP服务器报文的功能处于开启状态。

h. 开启PKI实体缓存OCSP响应的功能。
pki ocsp response cache enable

缺省情况下，PKI实体缓存OCSP响应的功能处于关闭状态。

开启缓存OCSP响应功能后，PKI实体在使用OCSP检查证书的吊销状态时，会先查找缓存，如果查找失败则再向OCSP服务器发起请求。同时，PKI实体会将有效的OCSP响应缓存起来，以便下次查找。

OCSP响应是有生效期限的，开启缓存OCSP响应功能后，PKI实体会每隔1分钟刷新缓存的OCSP响应，清除其中过期的OCSP响应。

i. **可选:** 配置PKI实体可以缓存的OCSP响应的最大数量。
pki ocsp response cache number *number*

缺省情况下，PKI实体可以缓存的OCSP响应的最大数量是1000。

j. **可选:** 配置PKI实体刷新OCSP响应缓存的周期。
pki ocsp response cache refresh interval *interval*

缺省情况下，PKI实体刷新OCSP响应缓存的周期为5分钟。

----结束

检查配置结果

- 执行命令**display pki crl** [**realm** *realm-name* | **filename** *filename*]，查看设备中的CRL内容。
- 执行命令**display pki certificate ocsp** [**realm** *realm-name* | **filename** *filename*]，查看设备上已加载的OCSP服务器证书的内容。
- 执行命令**display pki ocsp cache statistics slot** *slot-id* **cpu** *cpu-id*，查看OCSP响应缓存的统计信息。
- 执行命令**display pki ocsp server down-information slot** *slot-id* **cpu** *cpu-id*，查看设备上记录的OCSP服务器DOWN状态信息。
- 执行命令**display pki ocsp cache detail slot** *slot-id* **cpu** *cpu-id*，查看OCSP响应缓存的详细信息。

后续处理

如果CRL过期或者不使用时，可以执行命令**pki delete-crl** { **realm** *realm-name* | **filename** *filename* }，从内存中删除CRL。

12.9.2 配置证书属性过滤实现访问控制

背景信息

证书属性过滤是证书验证的一种方式，通过配置证书属性访问控制策略，使得只有符合特定属性条件的证书才能通过验证，进而对访问权限进行精细化控制。例如，在使用证书验证机制建立IPSec隧道的场景中，可能会要求只有某个CA颁发的证书才能通过验证，然后建立IPSec隧道，进一步控制访问权限。

证书属性访问控制策略是由证书属性组、证书属性条件和证书属性控制原则组成，通过在证书属性组里定义证书的属性条件，当某个证书与所有的证书条件匹配时，证书属性控制规则决定是否允许此证书通过。

证书属性条件包含如下：

证书属性条件	说明
证书有效期的开始和结束的时间	PKI实体本地证书的有效的起、止日期
FQDN名称（域名）	PKI实体本地证书的FQDN名称 FQDN由一个主机名和域名组成，例如www.example.com。
证书的IP地址	PKI实体本地证书的IP地址
证书颁发者名	PKI实体本地证书的颁发者名称
证书主题名	PKI实体本地证书的主题名

证书属性控制规则包含**permit**和**deny**两种动作。他决定对满足证书属性条件的证书是允许通过还是阻断，用户可以根据不同场景灵活使用。

通过证书属性过滤实现访问控制的匹配规则如下：

- 如果业务已经指定了证书属性访问控制策略，则使用其指定的证书属性访问控制策略，否则使用缺省的证书属性访问策略。缺省情况下，设备上缺省的证书属性访问控制策略中的证书属性控制规则动作为Permit，即允许证书通过验证。
- 如果一个证书属性访问控制策略中配置了多条控制规则，它们之间的关系为“或”，即待验证的证书匹配上了一条属性规则，并执行相应的动作后，不再继续匹配余下的属性规则。
- 如果一个证书属性组中配置了多条证书属性条件，它们之间的关系为“与”，即待验证的证书匹配上了所有的证书属性条件后，才会执行相应的证书属性控制规则中定义的动作。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 配置缺省的证书属性访问控制策略。

```
pki certificate access-control-policy default { deny | permit }
```

缺省情况下，缺省的证书属性访问控制策略中的动作为permit，即允许证书通过验证。

步骤3 创建证书属性组并进入证书属性组视图，或者直接进入证书属性组视图。

```
pki certificate attribute-group group-name
```

步骤4 配置证书的属性条件。

操作	命令
配置证书有效期的开始和结束的时间	**attribute** *id* **validity from** *begintime begindate* **to** *endtime enddate*
配置FQDN名称	**attribute** *id* **alt-subject-name fqdn** { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*
配置证书的IP地址	**attribute** *id* **alt-subject-name ip** { **ctn** | **equ** | **nctn** | **nequ** } *ip-address*
配置证书颁发者名	**attribute** *id* **issuer-name dn** { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*
配置证书主题名	**attribute** *id* **subject-name dn** { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

步骤5 返回至系统视图。

```
quit
```

步骤6 创建证书属性访问控制策略并进入证书属性访问控制策略视图，或者直接进入证书属性访问控制策略视图。

```
pki certificate access-control-policy name policy-name
```

缺省情况下，未创建证书属性访问控制策略。

步骤7 配置证书属性控制规则。

```
rule id { permit | deny } group-name
```


缺省情况下，系统未配置证书属性控制规则。

步骤8 配置证书属性访问控制策略的描述信息。

```
description description
```

缺省情况下，系统没有配置证书属性访问控制策略的描述信息。

步骤9 调整证书属性访问控制策略规则的先后顺序。

```
pki certificate access-control-policy [ policy-name policy-name ] rule move rule-id1 { before | after } rule-id2
```

调整证书属性访问控制策略规则时，*rule-id*保持不变，只是进行内容交换。例如：

原证书属性访问控制策略a的规则如下：

```
pki certificate access-control-policy name a
 rule 5 permit test1
 rule 20 permit test2
```

执行**pki certificate access-control-policy policy-name a rule move 20 before 5**命令后，规则如下：

```
pki certificate access-control-policy name a
 rule 5 permit test2
 rule 20 permit test1
```

步骤10 退出证书属性访问控制策略视图。

```
quit
```

----结束

检查配置结果

- 在用户视图下执行命令**display pki certificate access-control-policy all**，查看所有访问控制策略的信息。
- 在用户视图下执行命令**display pki certificate attribute-group all**，查看所有的证书属性组信息。

12.9.3 配置证书白名单实现访问控制

前提条件

证书白名单文件需要提前存放在设备的**flash:/pki/public**存储路径下。

背景信息

证书白名单是指将基站证书的通用名称（CN）或序列号加入到白名单列表中。当本端设备收到对端设备的证书认证时，如果对端证书的通用名称或序列号可以匹配设备中的证书白名单，则证书认证就会通过。

要使PKI证书白名单检查功能生效，需将证书白名单导入到设备的内存中。

操作步骤

- 导入证书白名单到设备的内存中。

  ```
  system-view
  pki import whitelist filename file-name
  ```

- 删除证书白名单。


```
system-view
pki delete whitelist filename file-name
```

----结束

检查配置结果

执行命令**display pki whitelist** { **all** | **filename** *file-name* }，查看设备上证书白名单的内容。

12.9.4 举例：通过证书属性过滤实现访问控制

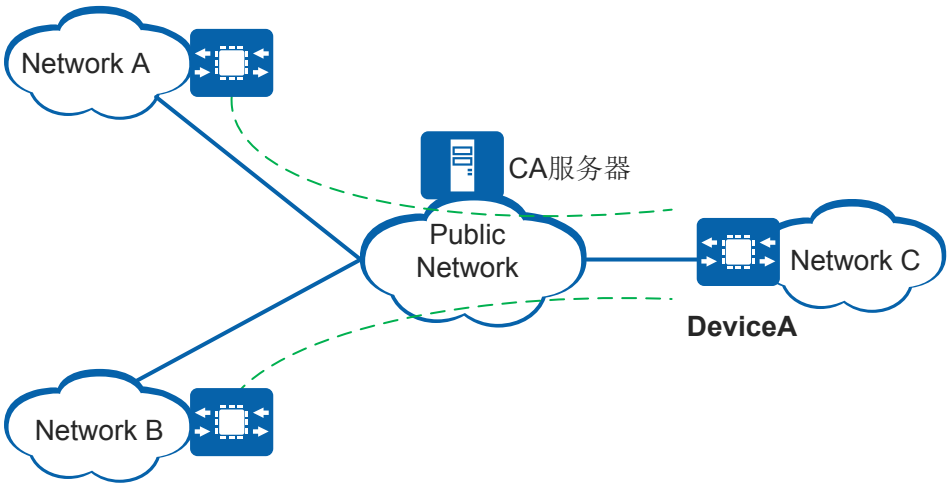
组网需求

如图12-16所示，设备作为内部网络的网关，网络A和网络B中的设备通过证书方式与设备进行身份验证，通过证书过滤的设备才可以建立IPSec连接，访问网络C资源。

基于证书属性的访问控制策略，符合如下要求的证书才能通过验证：

- 证书颁发者的名称为networkb_ca。
- 证书的主题名为cert_ca。

图 12-16 配置证书过滤实现访问控制组网图



说明

本举例只列出了证书属性的访问控制策略的相关配置。

配置思路

采用如下思路配置证书过滤实现访问控制：

1. 创建证书属性组，并在证书属性组中创建属性规则指定证书颁发者的名称和证书的主题名。
2. 创建证书属性访问控制策略，并允许证书属性组中的属性规则通过。

操作步骤

步骤1 配置缺省的证书属性访问控制策略中的动作为Deny，即不允许证书通过验证。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] pki certificate access-control-policy default deny
```

步骤2 创建证书属性组group。

```
[DeviceA] pki certificate attribute-group group
```

步骤3 创建属性规则，配置证书颁发者的名称为networkb_ca，证书的主题名为cert_ca。

```
[DeviceA-pki-attribute-group] attribute 1 issuer-name dn equ networkb_ca
[DeviceA-pki-attribute-group] attribute 2 subject-name dn equ cert_ca
[DeviceA-pki-attribute-group] quit
```

步骤4 创建证书属性访问控制策略policy。

```
[DeviceA] pki certificate access-control-policy name policy
```

步骤5 配置证书属性控制规则，匹配证书属性组中的属性规则允许通过。

```
[DeviceA-pki-access-policy] rule 1 permit group
[DeviceA-pki-access-policy] quit
```

----结束

检查配置结果

完成配置后，只有证书颁发者的名称为networkb_ca和证书的主题名为cert_ca的设备与DeviceA建立IPSec隧道。

配置脚本

```
#
sysname DeviceA
#
pki certificate access-control-policy default deny
#
pki certificate attribute-group group
 attribute 1 issuer-name dn equ networkb_ca
 attribute 2 subject-name dn equ cert_ca
#
pki certificate access-control-policy name policy
 rule 1 permit group
#
return
```

12.10 导入导出证书

12.10.1 导入其他设备的 RSA 密钥对和证书

背景信息

现网场景中，如果自己的设备没有申请证书需要将其他设备的证书导入到自己设备中使用，可以通过导入其他设备的RSA密钥对和证书功能实现。

操作步骤

步骤1 在设备A上导出RSA密钥对和证书。


```
pki export rsa-key-pair keyname [ and-certificate certificate-name ] { pem filename [ aes ] | pkcs12 filename } password password
```

步骤2 通过SFTP等方式将设备A存储卡中的密钥文件保存到PC。

步骤3 通过SFTP等方式将PC中密钥文件保存到设备B的存储卡中。

步骤4 在设备B上导入设备A上的RSA密钥对和证书。

```
pki import rsa-key-pair keyname [ exclude-cert ] { pem | pkcs12 } filename [ exportable ] [ password password ]
```

----结束

12.10.2 导入对端实体的证书

背景信息

导入对端实体的证书场景适合在大规模网络时部署。一般应用于IPsec场景，设备支持直接导入对端实体的证书。

当导入的对端实体的证书不需要使用时，可以将对端实体的证书释放。

操作步骤

- 导入对端实体的证书到设备的内存中。

  ```
  system-view
  pki import-certificate peer peer-name { der | pem | pkcs12 } filename filename [ cert-name cert-name ] [ no-check-same-name ]
  ```

- 释放对端实体的证书。

  ```
  system-view
  pki release-certificate peer { name peer-name | all }
  ```

----结束

检查配置结果

执行命令**display pki peer-certificate** { **name** *peer-name* | **all** }，查看已导入的对端实体证书。

12.10.3 导出证书

背景信息

设备支持把CA证书、本地证书、OCSP服务器证书拷贝到其他设备上使用，证书可以灵活导出，方便其他设备使用。执行如下命令操作可以将证书导出到设备存储介质中，然后用户可以通过FTP/SFTP取出证书。

操作步骤

- 在系统视图下将CA证书导出，拷贝到其他设备上使用。

  ```
  pki export-certificate ca realm realm-name { pem | pkcs12 }
  ```

- 在系统视图下将系统缺省内置的CA证书拷贝到其他设备上使用。

  ```
  pki export-certificate default ca filename file-name
  ```

- 在系统视图下将本地证书拷贝到其他设备上使用。

  ```
  pki export-certificate local realm realm-name { pem | pkcs12 }
  ```


- 在系统视图下将OCSP服务器证书拷贝到其他设备上使用。
  pki export-certificate ocsp realm *realm-name* { **pem** | **pkcs12** }

----结束

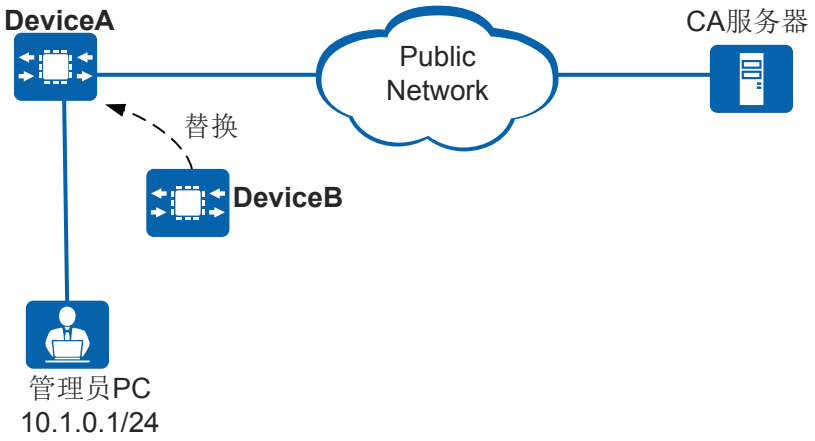
12.10.4 举例：配置手工导入其他设备的 RSA 密钥对和证书

组网需求

如图12-17所示，某企业在网络边界处部署了DeviceA作为出口网关，DeviceA已向公网上的CA服务器申请到本地证书。

因为DeviceA设备太旧，用户希望使用DeviceB设备替换DeviceA，但是由于网络的原因，用户无法手动更新证书和RSA密钥对，只能在DeviceB上手工导入DeviceA的RSA密钥对和证书。

图 12-17 配置手工导入其他设备的 RSA 密钥对和证书组网图



说明

DeviceA设备为其他厂商设备时，相关命令请参见其配置手册。

配置思路

采用如下思路配置手工导入其他设备的RSA密钥对和证书：

1. 将DeviceA的RSA密钥对和证书导出到存储卡中。
2. 通过SFTP等方式将DeviceA存储卡中的RSA密钥对和证书文件保存到PC。
3. 通过SFTP等方式将PC中DeviceA的RSA密钥对和证书文件保存到DeviceB存储卡中。
4. 将DeviceB存储卡中的RSA密钥对和证书导入到内存中。

操作步骤

步骤1 导出DeviceA的RSA密钥对和证书。

将RSA密钥对rsa_key和其对应的证书cer_test.cer按PEM格式导出到文件test02.pem，加密方式为AES。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] pki export rsa-key-pair rsa_key and-certificate cer_test.cer pem test02.pem aes password
YsHsjx_202206
 Warning: Exporting the key pair impose security risks, are you sure you want to
 export it? [y/n]:y
 Info: Succeeded in exporting the RSA key pair in PEM format.
```

说明

在DeviceA上执行命令**pki rsa local-key-pair create**创建RSA密钥对时，如果未配置**exportable**参数，则该RSA密钥对不允许被导出。

检查存储卡中是否存在test02.pem文件。

```
[DeviceA] quit
<DeviceA> dir flash:/pki/public/
Directory of flash:/pki/public/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         3,016   Jun 15 2017 18:48:26   test02.pem

1,179,616 KB total (434,592 KB free)
```

步骤2 通过SFTP等方式将DeviceA存储卡中的test02.pem文件保存到PC。

步骤3 通过SFTP等方式将PC中test02.pem文件保存到DeviceB存储卡中。

步骤4 在DeviceB上导入DeviceA的RSA密钥对和证书。

导入PEM格式的RSA密钥对文件test02.pem，RSA密钥对在系统中的名称为rsakey，密码为YsHsjx_202206，且标记为可导出。

导入test02.pem后，存储卡中的test02.pem默认删除，如不需删除，请根据设备上的提示信息选择N进行保留。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] pki import rsa-key-pair rsakey pem test02.pem exportable password YsHsjx_202206
 Info: Succeeded in importing the RSA key pair in PEM format.
 Warning: The file in the flash will be deleted. Please select 'N' if you want to keep it. Please select [Y/N]:y
 Info: Delete Success.
```

导入test02.pem后，DeviceB内存中生成RSA密钥对rsakey、本地证书rsakey_local.cer和CA证书rsakey_ca.cer文件。

说明

DeviceA导出的test02.pem文件里不包含CA证书时，DeviceB导入test02.pem文件后，内存中不会生成CA证书。如果用户需导入CA证书，则可以按照上面步骤逻辑来执行命令**pki export-certificate ca**和**pki import-certificate ca**。

----结束

检查配置结果

1. 执行命令**display pki rsa local-key-pair**查看到已导入内存的RSA密钥对信息。

```
[DeviceB] display pki rsa local-key-pair name rsakey public
Info: It will take a few seconds or more. Please wait a moment.
Total Number: 1
=====================================================
Time of Key pair created: 10:40:22  2021/3/13
Key Name: rsakey
Key Modules: 2048 bits
Key Exportable: Yes
=====================================================
```



```
RSA Public-Key: (2048 bits)
Modulus:
    00:9d:e2:3b:3b:d9:19:48:3a:62:59:11:c4:af:08:
    03:dd:9c:4a:61:e8:ed:a3:4b:a2:44:7f:a6:ea:10:
    12:04:8f:93:f2:ab:dc:09:f9:bc:e5:6b:4c:d3:29:
    f6:22:9e:da:83:bf:17:b2:8e:6b:65:6c:17:7e:83:
    dc:8e:33:1f:33:2d:96:4f:3d:ed:03:6d:91:45:47:
    49:79:8b:89:8a:7b:e5:f8:12:c0:41:45:77:ff:30:
    4c:a1:d4:f2:d0:9f:02:84:82:6d:02:10:bd:f1:5a:
    64:d0:8d:21:aa:a5:e6:61:ee:bb:55:a1:99:3f:ad:
    fb:6c:13:c9:dd:23:c6:ab:02:24:07:e4:76:4b:ef:
    3e:fa:56:31:80:b2:75:a2:b5:cc:12:0b:33:0a:e7:
    19:ed:6b:36:93:9f:78:e1:37:13:e2:b5:47:6f:d1:
    f1:7c:d8:01:49:f6:82:d9:3a:d6:1a:fd:bb:c4:71:
    05:fd:a4:ea:73:5b:db:b5:1a:2b:a5:e3:e2:78:b4:
    ec:9b:92:36:72:35:4f:7b:cc:05:91:db:14:1f:da:
    c5:22:89:f0:64:4a:76:b3:27:69:cf:b6:a6:1d:bd:
    ec:4c:24:0d:9e:ff:27:46:94:2e:b0:68:61:c6:ce:
    bd:e3:b0:4b:26:66:ee:f1:8a:3f:8c:30:7f:6f:bd:
    77:d1
Exponent: 65537 (0x10001)
```

2. 执行命令**display pki certificate local filename**查看到已导入内存的本地证书的内容。

```
[DeviceB] display pki certificate local filename rsakey_local.cer
 The  x509_obj type is Cert:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1144733510 (0x443b3f46)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, ST=beijing, L=BB, O=BB, OU=BB, CN=BB
        Validity
            Not Before: Jun 12 09:33:10 2012 GMT
            Not After : Aug 13 02:38:27 2016 GMT
        Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d3:12:fe:57:48:c6:a5:10:12:e9:2f:f9:2a:ff:
                    7b:2a:d8:45:69:11:c4:85:30:c4:9a:4d:0f:ad:58:
                    e7:56:cd:5c:f0:18:e1:c3:6d:44:c2:c3:5e:64:22:
                    d1:28:c9:c3:37:3c:34:ed:28:04:7f:62:9e:8b:94:
                    af:bc:72:de:f6:72:7f:e4:d8:45:31:fd:f9:ac:ce:
                    5a:b9:c7:1b:23:53:00:28:a6:3b:f5:61:69:5d:ab:
                    67:cb:bb:e8:96:2f:ce:ab:2c:6b:91:5b:26:91:86:
                    8f:80:a9:b0:66:c1:16:3d:31:55:a2:d4:b5:5a:af:
                    85:88:6e:99:f8:f8:53:58:77:26:91:ed:0e:94:ad:
                    c5:8d:53:67:67:55:08:8d:90:38:e0:5e:96:37:b9:
                    64:0e:36:e7:cf:9a:d2:77:e4:b0:24:05:a6:eb:03:
                    6e:ff:f7:ab:be:93:9e:8c:66:7d:31:66:be:6d:c8:
                    f3:17:9d:86:19:88:21:2d:d9:69:86:5f:b2:55:a4:
                    db:bc:d7:d0:6b:ac:66:ac:e4:63:9c:66:79:9c:42:
                    5c:83:b8:9e:4b:6e:67:85:a2:47:19:f1:5c:c0:3c:
                    c9:a3:47:02:a8:53:69:59:9e:d9:c7:5e:90:83:8d:
                    ac:cd:21:3c:d5:31:39:49:84:e6:f8:f4:e0:44:dd:
                    5d:7b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.2.0.2, DNS:test.abc.com
    Signature Algorithm: sha1WithRSAEncryption
        53:d5:79:31:7b:40:52:aa:ec:a9:35:ed:07:62:32:c4:ce:22:
        d3:37:0e:83:0c:4c:fa:61:dd:8c:db:a8:d3:fd:6a:ca:0e:3c:
        91:2c:91:ab:92:31:34:b5:87:1e:30:a4:ff:94:9c:d2:71:3c:
        6b:1f:4f:be:a7:20:f2:e1:c2:ad:71:8b:c2:79:0f:50:1f:3c:
        f9:87:df:1d:ee:3d:38:8c:f3:30:b7:3b:00:9b:72:38:b0:68:
        e1:c0:08:f4:02:91:81:a8:fa:51:9e:53:0d:03:b3:6b:0e:e2:
        62:80:ef:2a:a0:cb:9b:9b:91:21:7c:df:fe:6a:38:cc:03:36:
```

```
    9c:fc

Pki realm name: -
Certificate file name: rsakey_local.cer
Certificate peer name: -
```

3. 执行命令**display pki certificate ca filename**查看到已导入内存的CA证书的内容。

```
[DeviceB] display pki certificate ca filename rsakey_ca.cer
 The x509 object  type is certificate:
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 2 (0x2)
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: C=cn, ST=beijing, L=BB, O=BB, OU=BB, CN=BB
      Validity
         Not Before: Aug 15 02:38:27 2011 GMT
         Not After : Aug 13 02:38:27 2016 GMT
      Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            RSA Public-Key: (1024 bit)
            Modulus:
               00:b7:3e:65:7f:3b:3c:18:b8:87:34:39:76:3c:87:
               39:f7:a9:b3:35:9b:e0:e0:5b:c7:4f:3c:bb:fa:dd:
               da:93:0b:55:6e:eb:ba:52:c8:86:d1:cf:14:1e:1c:
               35:c6:53:68:f3:51:e7:2c:d4:b8:fa:0f:b3:04:ef:
               3f:a0:b3:4d:78:c1:26:88:26:15:41:3d:14:7f:67:
               3e:2f:35:32:ce:c7:73:73:43:5c:12:d3:0f:a0:ec:
               96:ae:55:61:27:32:39:a4:f8:32:a1:68:50:e6:3d:
               2b:39:6d:42:e8:09:5d:4f:98:46:6e:fc:80:87:0e:
               36:ca:09:7a:ca:2f:dd:ad:d3
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Basic Constraints: critical
            CA:TRUE
         X509v3 Subject Key Identifier:
            4F:67:F4:CB:F4:C3:F7:61:2C:BD:FF:1D:D1:29:FD:39:28:9F:3B:8B
         X509v3 Key Usage:
            Certificate Sign, CRL Sign
         Netscape Cert Type:
            SSL CA, S/MIME CA, Object Signing CA
         Netscape Comment:
            xca certificate
   Signature Algorithm: sha1WithRSAEncryption
      75:43:24:eb:db:ee:7d:05:30:88:b8:1b:d5:32:ca:51:49:74:
      04:94:fe:d0:31:29:6f:72:c7:4a:86:ac:2a:4c:45:24:9d:3c:
      b4:30:b5:d1:43:88:29:f7:b4:88:b8:37:dc:dd:f4:fa:42:34:
      1c:e6:a5:bc:bb:0b:37:ef:db:8c:b2:b0:bd:97:7f:15:ae:6c:
      71:1b:ff:f1:90:13:74:a4:1f:7c:f7:4e:80:5b:42:aa:6b:22:
      2a:cf:04:48:29:20:c0:b2:95:38:11:06:be:76:f0:cb:8d:4a:
      c6:1a:50:af:31:81:58:ac:14:fe:89:f2:e0:bb:95:3c:94:d0:
      54:96

Pki realm name: -
Certificate file name: rsakey_ca.cer
Certificate peer name: -
```

12.11 维护 PKI

12.11.1 删除证书

背景信息

本地证书过期或者重新申请新的证书时，可以删除设备内存中的本地证书。如果需要删除内存中的证书，可选择在系统视图下执行以下命令。

表 12-8 删除证书和 RSA 密钥对

操作	命令
从内存中删除本地证书	**pki delete-certificate local** { **realm** *realm-name* | **filename** *file-name* }
从内存中删除CA证书	**pki delete-certificate ca** { **realm** *realm-name* | **filename** *file-name* }
从内存中删除OCSP服务器证书	**pki delete-certificate ocsp** { **realm** *realm-name* | **filename** *file-name* }

12.11.2 清除 PKI 信息

背景信息

清空PKI信息后，以前的信息将无法恢复，务必仔细确认。请在用户视图下执行以下命令。

操作步骤

- 清除OCSP响应缓存。
  reset pki ocsp response cache
- 清除设备上记录的OCSP服务器DOWN状态信息。
  reset pki ocsp server down-information [**url** [**esc**] *url-addr*]
- 清除已经导入内存的CA证书、CRL、本地证书和OCSP响应器证书的内容。
  reset pki global-ca

  说明

  该命令行将删除已经导入设备内存中的所有CA证书、CRL和本地证书、OCSP响应器证书等内容，请谨慎操作。

----结束

12.11.3 将被覆盖的文件移动到回收站

背景信息

覆盖文件时，被覆盖的文件默认彻底删除，无法恢复。如果用户希望被覆盖的文件能够恢复，以防止新文件不可用，此时可以配置被覆盖的文件删除到回收站功能。

该功能仅适用于以下场景：

- 执行命令**pki get-crl**、**pki import-crl**覆盖已有的CRL。
- 执行命令**pki enroll-certificate**、**pki create-certificate**、**pki export-certificate**、**pki export-certificate default**、**pki import-certificate peer**覆盖已有的证书。
- 执行命令**pki import rsa-key-pair**、**pki export rsa-key-pair**覆盖已有的RSA密钥对、证书。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启被覆盖的文件删除到回收站功能。

```
pki recycle-bin enable
```

缺省情况下，被覆盖的文件被彻底删除。

----结束

12.11.4 配置 PKI 加入到指定的 VPN 内

背景信息

当CA等服务器位于某个VPN内时，为了让设备可以与这些服务器进行通信以实现证书的获取或有效性校验等功能，此时需配置PKI域加入到指定的VPN内。

操作步骤

- PKI域视图
  a. 进入系统视图。
     ```
     system-view
     ```
  b. 创建PKI域并进入PKI域视图，或者直接进入PKI域视图。
     ```
     pki realm realm-name
     ```
  c. 将PKI加入到指定的VPN内。
     ```
     vpn-instance { vpn-instance-name }
     ```
     缺省情况下，系统未将PKI加入到任何VPN内。

     *vpn-instance-name*参数可通过命令**ip vpn-instance**配置。
  d. 退出PKI实体视图。
     ```
     quit
     ```
- CMP会话视图

  CMP会话视图下，将PKI到指定的VPN内。仅在通过CMPv2在线申请和更新证书场景下使用。

  a. 进入系统视图。
     ```
     system-view
     ```
  b. 创建CMP会话并进入CMP会话视图，或者直接进入CMP会话视图。
     ```
     pki cmp session session-name
     ```
     缺省情况下，系统未创建CMP会话。

CMP会话是一个本地概念，一个设备上配置的CMP会话对CA和其他设备是不可见的。

c. 将PKI加入到指定的VPN内。

```
vpn-instance vpn-name { vpn-instance-name }
quit
```

缺省情况下，系统未将PKI加入到任何VPN内。

*vpn-instance-name*参数可通过命令**ip vpn-instance**配置。

----结束

12.11.5 校验和查看预置证书

背景信息

设备出厂时，设备会预置CA证书和本地证书，并存放到NVRAM内存中，且不支持删除和修改。该预置证书可以作为设备的身份标识，导入到default域中，保证设备及外部通信的安全性。

缺省情况下，设备出厂时已校验预置证书的有效性，一般情况下，用户无需对预置证书进行校验。

操作步骤

- 校验预置证书有效性。

  ```
  pki validate-certificate device slot slot-id
  ```

- 查看预置证书的内容。

  ```
  display pki certificate device slot slot-id
  ```

----结束

12.12 PKI 常见配置错误

12.12.1 获取 CA 证书失败

故障现象

通过手工方式获取CA证书，查看设备存储介质中没有下载到CA证书，其失败的原因为通过LDAP方式下载CA证书时配置的不正确。

操作步骤

- 检查LDAP方式下载CA证书的配置是否正确。如果不正确，请修改相应的内容。详情请参见命令**pki ldap ip** *ip-address* **port** *port* **version** *version* [**attribute** *attr-value*] [**authentication** *ldap-dn ldap-password*] *save-name* **dn** *dn-value*。

----结束

12.12.2 获取本地证书失败

故障现象

- 通过手工方式离线获取本地证书，查看设备存储介质中没有下载到本地证书，其失败的原因如下：
  - 指定的PKI实体配置不正确。
  - 挑战密码配置的不正确或未配置。
  - 通过LDAP方式下载本地证书时配置不正确。
- 通过CMPv2协议获取本地证书，查看设备存储介质中没有下载到本地证书，其失败的原因如下：
  - 执行获取操作之前PKI域中没有CA证书。
  - 指定的PKI实体配置不正确或未配置。
  - 信任的CA名称配置不正确或未配置。
  - 证书注册服务器的URL配置不正确或未配置。
  - 使用的RSA密钥对未配置。
  - TCP连接使用的源接口配置不正确。
  - 签名证书注册请求消息使用的摘要算法配置的不正确。
  - 挑战密码配置的不正确或未配置。
  - 消息认证码的参考值和秘密值配置不正确或未配置。
  - 用于证明身份的证书配置不正确。

操作步骤

- 通过手工方式获取本地证书
  a. 检查配置的PKI实体配置是否正确。

     在PKI域下指定的PKI实体，可以执行命令**display pki entity**查看配置的PKI实体信息。

     如果某些内容配置错误，例如PKI实体所属的国家代码配置错误，请修改相应的内容。
  b. 检查挑战密码配置是否正确。

     请先确定CA服务器是否要验证挑战密码，如果是，请配置CA服务器的挑战密码，两者要一致。详情请参见命令**pki enroll-certificate**。
  c. 检查LDAP方式下载本地证书的配置是否正确。

     如果不正确，请修改相应的内容。详情请参见命令**pki ldap ip** *ip-address* **port** *port* **version** *version* [**attribute** *attr-value*] [**authentication** *ldap-dn ldap-password*] *save-name* **dn** *dn-value*。
- 通过CMPv2协议获取本地证书
  a. 检查CA证书是否已导入设备的内存中。

     可以执行命令**display pki certificate**查看设备内存中的CA证书。

     如果没有请获取CA证书并执行命令**pki import-certificate**将CA证书导入设备的内存中。

b. 检查配置的PKI实体配置是否正确。

在PKI域下指定的PKI实体，可以执行命令**display pki entity**查看配置的PKI实体信息。

如果某些内容配置错误，例如PKI实体所属的国家代码配置错误，请修改相应的内容。

c. 检查CMP会话下配置的申请CA证书的相关配置是否正确。

可以在CMP会话下执行命令**display this**查看。

如下所示，这里例举申请CA证书所需的配置。

```
pki cmp session cmp
 cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"   //配置CA的名称，CA名称中各个字段的顺序必须要和实际CA证书中的顺序保持一致
 cmp-request authentication-cert local.cer   //配置CMPv2请求中用于证明身份的证书，用于更新证书或为其他设备申请证书等
 cmp-request entity user01   //指定使用的PKI实体
 cmp-request server url http://10.3.0.1:8080   //配置CMPv2服务器的URL
 cmp-request rsa local-key-pair rsa regenerate   //指定使用的RSA密钥对
 cmp-request message-authentication-code 1234 %^%#ZodFBGH[^BkU2(~>[NRBv|#b>se|@I7"'A,llG_B%^%#   //配置消息认证码的参考值和秘密值，与CA服务器一致
```

如果相关配置不正确，请修改相应的内容。

----结束

13 SSL 配置

13.1 SSL 简介

定义

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。SSL能使客户端与服务器之间的通信不被窃听，还能验证通信双方身份，保证网络上数据传输的安全性。

目的

基于万维网的电子商务和网上银行等新兴应用极大地方便了人们的日常生活，受到人们的青睐。由于这些应用都需要在网络上进行在线交易，它们对网络通信的安全性提出了更高的要求。传统的万维网协议HTTP（Hypertext Transfer Protocol ）不具备安全机制——采用明文的形式传输数据、不能验证通信双方的身份、无法防止传输的数据被篡改等，导致HTTP无法满足电子商务和网上银行等应用的安全性要求。Netscape公司提出的安全协议SSL，利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证。SSL可以为HTTP提供安全连接，从而很大程度上改善了万维网的安全性问题。

虽然SSL设计的初衷是为了解决万维网的安全性问题，但是由于SSL位于应用层和传输层之间，它可以为任何基于TCP等可靠连接的应用层协议提供安全性保证。

13.2 SSL 原理描述

13.2.1 协议安全机制

SSL协议实现的安全机制包括：

- **身份验证机制**：基于证书利用数字签名方法对服务器和客户端进行身份验证，其中客户端的身份验证是可选的。
- **数据传输的机密性**：利用对称密钥算法对传输的数据进行加密。
- **消息完整性验证**：消息传输过程中使用消息验证码MAC（Message Authentication Code）算法来检验消息的完整性。

身份验证机制

客户端必须保证SSL服务器是真实的，以免重要信息被非法窃取。SSL利用数字签名来验证通信双方的身份。

数字签名可以通过非对称密钥算法实现。由于通过私钥加密后的数据只能利用对应的公钥进行解密，因此根据解密是否成功，就可以判断发送者的身份，如同发送者对数据进行了“签名”。例如，Alice使用自己的私钥对一段固定的信息加密后发给Bob，Bob利用Alice的公钥解密，如果解密结果与固定信息相同，那么就能够确认信息的发送者为Alice，这个过程就称为数字签名。

使用数字签名验证身份时，需要确保被验证者的公钥是真实的，否则，非法用户可能会冒充被验证者与验证者通信。通过数字证书来发布用户的公钥，可以保证公钥的真实性。

数字证书（简称证书）是一个包含用户的公钥及其身份信息的文件，证明了用户与公钥的关联。数字证书由CA（Certificate Authority）证书机构签发，CA签发证书的同时会提供证书机构文件，证明CA的身份也保证所颁发证书的真实性。

验证SSL服务器/SSL客户端的身份时，SSL服务器/SSL客户端需要将从CA获取的证书发送给对端，对端利用证书机构文件判断该证书的真实性。如果该证书确实属于SSL服务器/SSL客户端，则对端利用该证书中的公钥验证SSL服务器/SSL客户端的身份。

数据传输的机密性

网络上传输的数据很容易被非法用户窃取，SSL采用在通信双方之间建立加密通道的方法保证数据传输的机密性。

所谓加密通道，是指发送方在发送数据前，使用加密算法和加密密钥对数据进行加密，然后将数据发送给对方；接收方接收到数据后，利用解密算法和解密密钥从密文中获取明文。没有解密密钥的第三方，无法将密文恢复为明文，从而保证数据传输的机密性。

加解密算法分为两类：

- 非对称密钥算法：数据加密和解密时使用不同的密钥，一个是公开的公钥，一个是由用户秘密保存的私钥。利用公钥（或私钥）加密的数据只能用相应的私钥（或公钥）才能解密。非对称密钥算法一般用于对较少的信息进行加密。
- 对称密钥算法：数据加密和解密时使用相同的密钥。对称密钥算法具有计算速度快的优点，通常用于对大量信息进行加密（如对所有报文加密）。

SSL利用非对称密钥算法RSA、Diffie-Hellman和ECDHE加密客户端随机生成的密钥premaster secret，两端根据premaster secret生成对称密钥算法使用的密钥，然后利用对称密钥算法对传输数据进行加密。

消息完整性验证

为了避免网络中传输的数据被非法篡改，SSL利用基于密钥的MAC算法来保证消息的完整性。

MAC算法是将密钥和任意长度的数据转换为固定长度数据的一种算法。

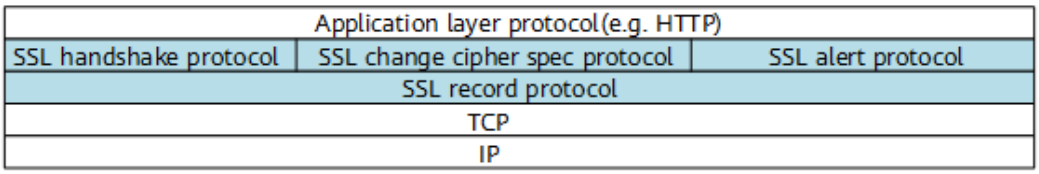
- 发送端在密钥参与下，利用MAC算法计算出消息的MAC值，并将其加在消息之后发送给接收端。
- 接收端利用同样的密钥和MAC算法计算出消息的MAC值，并与接收到的MAC值比较。

如果二者相同，则报文没有改变。否则，报文在传输过程中被修改，接收端将丢弃该报文。

13.2.2 协议结构

如图13-1所示，SSL位于应用层和传输层之间。SSL协议分为两层：底层是SSL记录协议（SSL record protocol）；上层是SSL握手协议（SSL handshake protocol）、SSL密码变化协议（SSL change cipher spec protocol）和SSL警告协议（SSL alert protocol）。

图 13-1 SSL 协议栈



- SSL记录协议：主要负责对上层的数据进行分块、计算并添加MAC、加密后形成记录块，最后把记录块传输给对方。实际的数据传输是使用SSL记录协议来实现的。
- SSL握手协议：握手协议是在应用程序的数据传输之前使用的。用来协商通信过程中使用的加密套件（数据加密算法、密钥交换算法和MAC算法等），实现服务器和客户端的身份验证，并在服务器和客户端之间安全地交换密钥。
- SSL密码变化协议：客户端和服务器端通过密码变化协议通知对端，随后的报文都将使用新协商的加密套件和密钥进行保护和传输。
- SSL警告协议：用来向对端报告握手过程或应用数据传输过程中发生的告警信息，以便对端进行相应的处理。告警消息中包含告警的严重级别和描述。

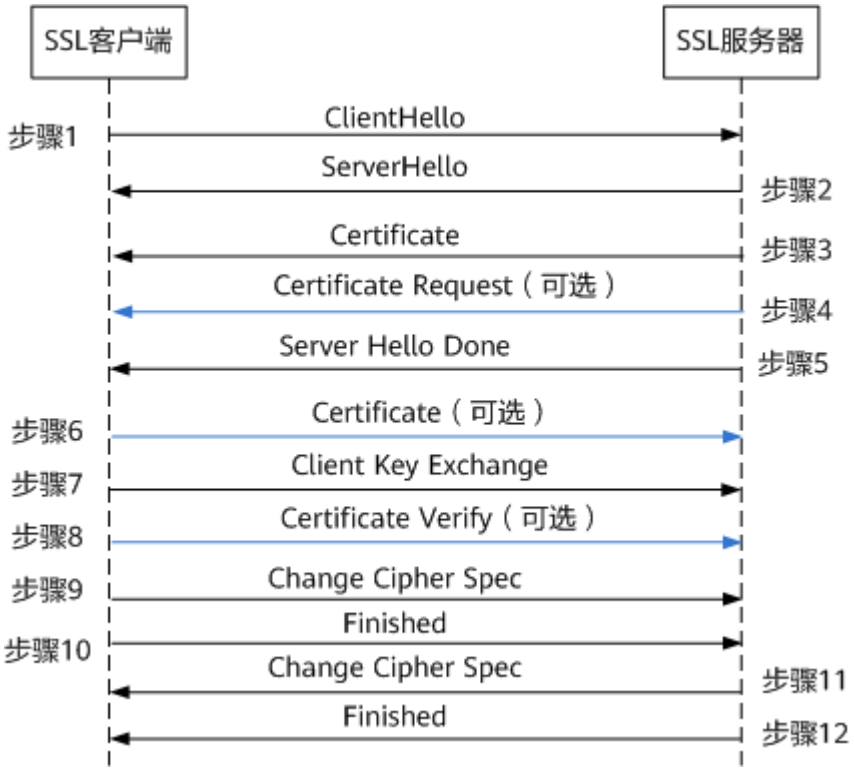
13.2.3 协议工作过程

握手过程

SSL通过握手在客户端和服务器之间建立会话，完成双方身份的验证、密钥和加密套件的协商。 握手过程如图13-2所示。除Change Cipher Spec消息属于SSL密码变化协议外，其他握手过程交互的消息均属于SSL握手协议，统称为SSL握手消息。

其中，服务器对SSL客户端的身份验证是可选的，即图13-2中蓝色部分标识的内容（步骤4、6和8）为可选。

图 13-2 握手过程示意图



1. SSL客户端发送消息给SSL服务器启动握手，携带它支持的SSL版本和加密套件等信息。
2. SSL服务器响应SSL客户端，携带选定的版本、加密套件。如果SSL服务器允许SSL客户端在以后的通信中重用本次会话，SSL服务器还会为本次会话分配会话ID。
3. SSL服务器将携带自己公钥信息的数字证书发送给SSL客户端，以便客户端对服务器进行身份认证。
4. （可选）SSL服务器要求SSL客户端提供证书，以便服务器对客户端进行身份认证。
5. SSL服务器通知SSL客户端版本和加密套件协商结束，开始进行密钥交换。
6. （可选）SSL客户端发送自己的证书给SSL服务器。
7. SSL客户端验证SSL服务器的证书合法后，利用证书中的公钥加密SSL客户端随机生成的密钥发给SSL服务器。

   实际上，这个随机生成的密钥不能直接用来加密数据或计算MAC值，该密钥是用来计算对称密钥和MAC密钥的信息，称为premaster secret。SSL客户端和SSL服务器利用premaster secret计算出相同的主密钥（master secret），再利用master secret生成用于对称密钥算法、MAC算法的密钥。premaster secret是计算对称密钥、MAC算法密钥的关键。
8. （可选）SSL客户端发送验证消息给服务器，以便服务器对客户端进行身份认证。

   客户端通过计算已交互的握手消息、主密钥的Hash值，利用自己的私钥对其进行加密，通过Certificate Verify消息发给服务器。服务器同样计算已交互的握手消息、主密钥的Hash值，利用客户端证书中的公钥解密Certificate Verify消息，并将解密结果与计算出的Hash值比较。如果二者相同，则客户端身份验证成功。
9. SSL客户端通知SSL服务器后续报文将采用协商好的密钥（利用master secret生成的密钥）和加密套件进行加密和MAC计算。

10. SSL客户端通知SSL服务器，让服务器验证握手过程的安全。

    SSL客户端计算已交互的握手消息的Hash值，利用协商好的密钥和加密套件处理Hash值（计算并添加MAC值、加密等），并通过Finished消息发送给SSL服务器。SSL服务器利用同样的方法计算已交互的握手消息的Hash值，并与Finished消息的解密结果比较，如果二者相同，且MAC值验证成功，则证明密钥和加密套件协商成功。

    说明

    Hash值指的是利用Hash算法（MD5或SHA）将任意长度的数据转换为固定长度的数据。

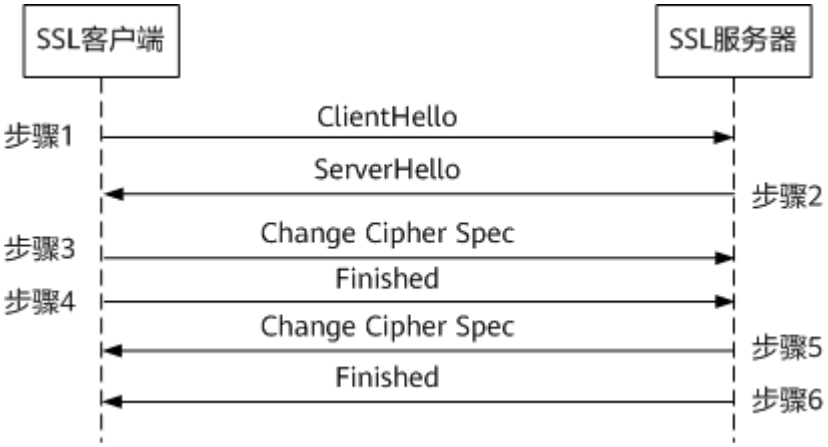
11. SSL服务器通知SSL客户端后续报文将采用协商好的密钥（利用master secret生成的密钥）和加密套件进行加密和MAC计算。
12. SSL服务器通知SSL客户端，让客户端验证握手过程的安全。

    SSL服务器计算已交互的握手消息的Hash值，利用协商好的密钥和加密套件处理Hash值（计算并添加MAC值、加密等），并通过Finished消息发送给SSL客户端。SSL客户端利用同样的方法计算已交互的握手消息的Hash值，并与Finished消息的解密结果比较，如果二者相同，且MAC值验证成功，则证明密钥和加密套件协商成功。

握手成功后，SSL客户端也就完成了对SSL服务器的身份验证。因为只有拥有私钥的SSL服务器才能从Client Key Exchange消息中解密得到premaster secret，才有后续握手的成功。

客户端和服务器握手过程中，需要使用非对称密钥算法来加密密钥、验证通信对端的身份，计算量较大，占用了大量的系统资源。为了简化SSL握手过程，SSL允许重用已经协商过的会话，如图13-3所示，具体过程如下：

图 13-3 恢复原有会话的 SSL 握手过程示意图



1. SSL客户端发送Client Hello消息，消息中的会话ID设置为计划重用的会话的ID。
2. SSL服务器如果允许重用该会话，则通过在Server Hello消息中设置相同的会话ID来应答。这样，SSL客户端和SSL服务器就可以利用原有会话的密钥和加密套件，不必重新协商。
3. SSL客户端发送Change Cipher Spec消息，通知SSL服务器后续报文将采用原有会话的密钥和加密套件进行加密和MAC计算。
4. SSL客户端计算已交互的握手消息的Hash值，利用原有会话的密钥和加密套件处理Hash值，并通过Finished消息发送给SSL服务器，以便SSL服务器判断密钥和加密套件是否正确。

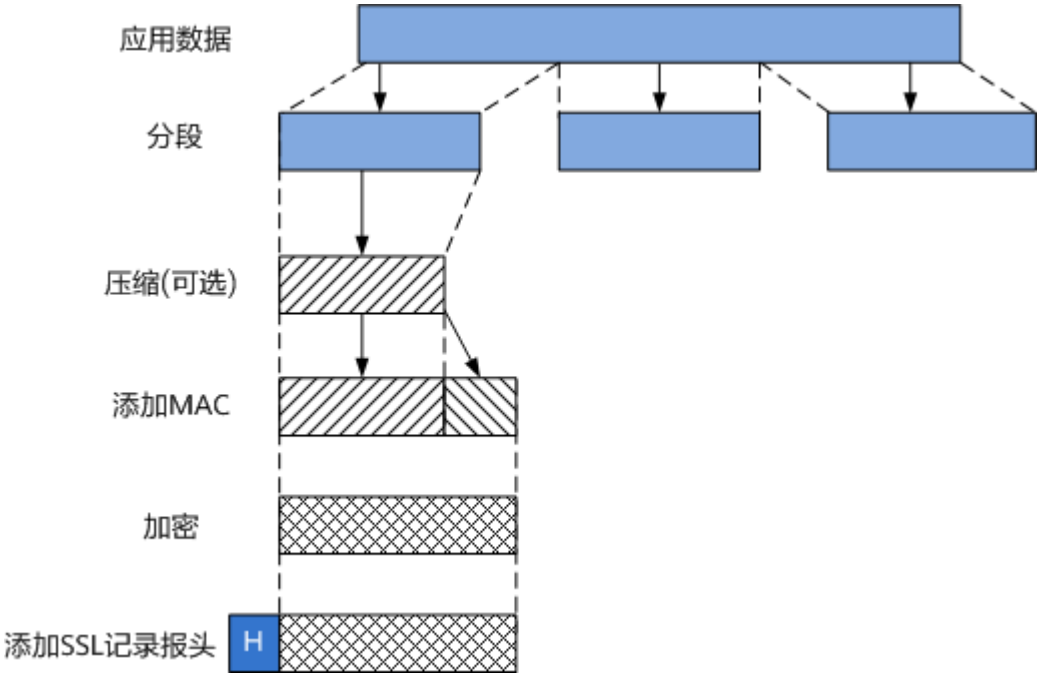
5. 同样地，SSL服务器发送Change Cipher Spec消息，通知SSL客户端后续报文将采用原有会话的密钥和加密套件进行加密和MAC计算。
6. SSL服务器计算已交互的握手消息的Hash值，利用原有会话的密钥和加密套件处理Hash值，并通过Finished消息发送给SSL客户端，以便SSL客户端判断密钥和加密套件是否正确。

数据传输过程

握手完成后，客户端和服务器即可以交换应用层数据。在SSL中，实际的数据传输是使用SSL记录协议来实现的。

图13-4描述了数据传输过程。记录协议接收传输的应用数据，将数据分片成可管理的块，进行数据压缩（可选），添加MAC，接着利用加密算法进行数据加密，最后增加SSL记录报头。被接收的数据刚好与接收数据的工作过程相反，依次被解密、验证、解压缩和重新装配。

图 13-4 数据传输过程示意图



13.3 SSL 配置注意事项

License 依赖

SSL无需License许可即可使用。

硬件依赖

表 13-1 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 13-2 本特性的使用限制

特性限制	系列	涉及产品
创建SSL策略，DH模数默认值为3072，可配置2048、3072、4096；签名算法默认开启ed25519，ed448，rsa-pss-pss-sha256，rsa-pss-pss-sha384，rsa-pss-pss-sha512，rsa-pss-rsae-sha256，rsa-pss-rsae-sha384，rsa-pss-rsae-sha512，可单独配置，增加安全性。 创建SSL策略后，如果是签名算法不匹配或者DH模数长度过长导致的SSL握手失败，可以通过diffie-hellman modulus命令调整DH模数长度；通过signature algorithm-list命令调整签名算法。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
SSL加载证书文件（身份证书、CA、吊销列表）存在文件大小限制，文件大小不能超过（包含）50K。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

13.4 SSL 缺省配置

SSL的主要缺省配置如表13-3所示。

表 13-3 SSL 缺省配置

参数	缺省配置
SSL策略加密套件	未配置

参数	缺省配置
SSL策略加密套件中支持的加密算法	未配置
SSL策略	未配置
当前SSL策略所采用的最低版本	TLS1.2
SSL策略加载证书	SSL策略未加载数字证书
SSL策略加载数字证书撤销列表CRL	SSL策略未加载CRL
SSL策略加载信任证书机构文件	SSL策略未加载信任证书机构文件
SSL策略绑定加密套件	SSL策略未绑定加密套件

13.5 配置 SSL

13.5.1 （可选）配置 SSL 策略加密套件

背景信息

加密套件是指在SSL通信中，服务器和客户端所使用的加密算法的组合。在SSL握手初期，客户端将自身支持的加密套件列表发送给服务器；在握手阶段，服务器根据自己的配置从中尽可能的选出一个套件，作为之后所要使用的加密方式。

每种加密套件中支持的加密算法大多包含了如下信息：

- 密钥交换算法：用于决定客户端与服务器之间在握手的过程中如何认证。使用非对称加密算法来生成会话密钥，因为非对称算法不会将重要数据在通信中传输。用到的算法包括RSA、Diffie-Hellman和ECDHE。
- 签名算法：用于CA证书签名。用到的算法包括RSA和DSS。
- 加密算法：用于对数据进行加密传输。一般有对称加和非对称加密，但是非对称加密算法太耗性能，再者有些非对称加密算法有内容长度的限制，所以真正要传输的数据会使用对称加密来进行加密。算法名称后通常带密钥的长度和加密模式（GCM和CBC）。用到的算法包括：AES_128、AES_256、AES_128_CBC、AES_256_CBC、AES_128_GCM、AES_256_GCM和ChaCha20-Poly1305。
- 完整性校验算法：用于校验消息的完整性。用到的算法包括SHA、SHA256和SHA384。

例如加密套件中支持的加密算法**tls12_ck_rsa_aes_128_cbc_sha**，此算法是基于**TLS**协议，使用的密钥交换算法为**RSA**，加密算法为**AES_128_CBC**（密钥长度为128，加密模式为CBC），完整性校验算法为**SHA**。

表 13-4 加密套件中支持的加密算法

TLS版本	加密套件中支持的加密算法	描述
TLS1.1、TLS1.2和TLS1.3	tls1_ck_rsa_with_aes_256_sha	此算法中的密钥交换算法为RSA，签名算法为RSA，加密算法为AES_256，完整性校验算法为SHA。
	tls1_ck_rsa_with_aes_128_sha	此算法中的密钥交换算法为RSA，签名算法为RSA，加密算法为AES_128，完整性校验算法为SHA。
	tls1_ck_dhe_rsa_with_aes_256_sha	此算法中的密钥交换算法为Diffie-Hellman和RSA，签名算法为RSA，加密算法为AES_256，完整性校验算法为SHA。
	tls1_ck_dhe_dss_with_aes_256_sha	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_256，完整性校验算法为SHA。
	tls1_ck_dhe_rsa_with_aes_128_sha	此算法中的密钥交换算法为Diffie-Hellman，签名算法为RSA，加密算法为AES_128，完整性校验算法为SHA。
	tls1_ck_dhe_dss_with_aes_128_sha	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_128，完整性校验算法为SHA。
TLS1.2和TLS1.3	tls12_ck_rsa_aes_128_cbc_sha	此算法中的密钥交换算法为RSA，签名算法为RSA，加密算法为AES_128_CBC（密钥长度为128，加密模式为CBC），完整性校验算法为SHA。
	tls12_ck_rsa_aes_256_cbc_sha	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_256_CBC（密钥长度为256，加密模式为CBC），完整性校验算法为SHA。
	tls12_ck_rsa_aes_128_cbc_sha256	此算法中的密钥交换算法为Diffie-Hellman，签名算法为RSA，加密算法为AES_128_CBC（密钥长度为256，加密模式为CBC），完整性校验算法为SHA256。
	tls12_ck_dhe_rsa_aes_128_cbc_sha	此算法中的密钥交换算法为Diffie-Hellman，签名算法为RSA，加密算法为AES_128_CBC（密钥长度为128，加密模式为CBC），完整性校验算法为SHA。

TLS版本	加密套件中支持的加密算法	描述
	tls12_ck_dhe_dss_aes_128_cbc_sha	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_128_CBC（密钥长度为128，加密模式为CBC），完整性校验算法为SHA。
	tls12_ck_dhe_dss_aes_256_cbc_sha	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_256_CBC（密钥长度为256，加密模式为CBC），完整性校验算法为SHA。
	tls12_ck_dhe_rsa_aes_256_cbc_sha	此算法中的密钥交换算法为Diffie-Hellman，签名算法为RSA，加密算法为AES_256_CBC（密钥长度为256，加密模式为CBC），完整性校验算法为SHA。
	tls12_ck_dhe_dss_aes_128_cbc_sha256	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_128_CBC（密钥长度为128，加密模式为CBC），完整性校验算法为SHA256。
	tls12_ck_dhe_rsa_aes_128_cbc_sha256	此算法中的密钥交换算法为Diffie-Hellman，签名算法为RSA，加密算法为AES_128_CBC（密钥长度为128，加密模式为CBC），完整性校验算法为SHA256。
	tls12_ck_dhe_dss_aes_256_cbc_sha256	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_256_CBC（密钥长度为256，加密模式为CBC），完整性校验算法为SHA256。
	tls12_ck_dhe_rsa_aes_256_cbc_sha256	此算法中的密钥交换算法为Diffie-Hellman，签名算法为RSA，加密算法为AES_256_CBC（密钥长度为256，加密模式为CBC），完整性校验算法为SHA256。
	tls12_ck_rsa_with_aes_128_gcm_sha256	此算法中的密钥交换算法为RSA，签名算法为RSA，加密算法为AES_128_gcm（密钥长度为128，加密模式为GCM），完整性校验算法为SHA256。
	tls12_ck_rsa_with_aes_256_gcm_sha384	此算法中的密钥交换算法为RSA，签名算法为RSA，加密算法为AES_256_gcm（密钥长度为256，加密模式为GCM），完整性校验算法为SHA384。

TLS版本	加密套件中支持的加密算法	描述
	tls12_ck_dhe_rsa_with_aes_128_gcm_sha256	此算法中的密钥交换算法为Diffie-Hellman，签名算法为RSA，加密算法为AES_128_gcm（密钥长度为128，加密模式为GCM），完整性校验算法为SHA256。
	tls12_ck_dhe_rsa_with_aes_256_gcm_sha384	此算法中的密钥交换算法为Diffie-Hellman，签名算法为RSA，加密算法为AES_256_gcm（密钥长度为256，加密模式为GCM），完整性校验算法为SHA384。
	tls12_ck_dhe_dss_with_aes_128_gcm_sha256	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_128_gcm（密钥长度为128，加密模式为GCM），完整性校验算法为SHA256。
	tls12_ck_dhe_dss_with_aes_256_gcm_sha384	此算法中的密钥交换算法为Diffie-Hellman，签名算法为DSS，加密算法为AES_256_gcm（密钥长度为256，加密模式为GCM），完整性校验算法为SHA384。
	tls12_ck_rsa_aes_256_cbc_sha256	此算法中的密钥交换算法为RSA，签名算法为RSA，加密算法为AES_256_cbc（密钥长度为256，加密模式为CBC），完整性校验算法为SHA256。
	tls12_ck_ecdhe_rsa_with_aes_128_gcm_sha256	此算法中的密钥交换算法为ECDHE，签名算法为RSA，加密算法为AES_128_gcm（密钥长度为128，加密模式为GCM），完整性校验算法为SHA256。
	tls12_ck_ecdhe_rsa_with_aes_256_gcm_sha384	此算法中的密钥交换算法为ECDHE，签名算法为RSA，加密算法为AES_256_gcm（密钥长度为256，加密模式为GCM），完整性校验算法为SHA384。
TLS1.3	tls13_aes_128_gcm_sha256	此算法中的加密算法为AES_128_gcm（密钥长度为128，加密模式为GCM），完整性校验算法为SHA256。
	tls13_aes_256_gcm_sha384	此算法中的加密算法为AES_256_gcm（密钥长度为256，加密模式为GCM），完整性校验算法为SHA256。
	tls13_chacha20_poly1305_sha256	此算法中的加密算法为ChaCha20-Poly1305，完整性校验算法为SHA256。

TLS版本	加密套件中支持的加密算法	描述
	tls13_aes_128_ccm_sha256	此算法中的加密算法为AES_128_ccm（密钥长度为128，加密模式为CCM），完整性校验算法为SHA256。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建SSL策略加密套件并进入SSL策略加密套件定制视图。

```
ssl cipher-suite-list customization-policy-name
```

缺省情况下，没有创建SSL策略加密套件。

步骤3 配置SSL策略加密算法套中支持的加密算法。

```
set cipher-suite { tls1_ck_rsa_with_aes_256_sha | tls1_ck_rsa_with_aes_128_sha |
tls1_ck_dhe_rsa_with_aes_256_sha | tls1_ck_dhe_dss_with_aes_256_sha |
tls1_ck_dhe_rsa_with_aes_128_sha | tls1_ck_dhe_dss_with_aes_128_sha | tls12_ck_rsa_aes_128_cbc_sha |
tls12_ck_rsa_aes_256_cbc_sha | tls12_ck_rsa_aes_128_cbc_sha256 | tls12_ck_rsa_aes_256_cbc_sha256 |
tls12_ck_dhe_dss_aes_128_cbc_sha | tls12_ck_dhe_rsa_aes_128_cbc_sha |
tls12_ck_dhe_dss_aes_256_cbc_sha | tls12_ck_dhe_rsa_aes_256_cbc_sha |
tls12_ck_dhe_dss_aes_128_cbc_sha256 | tls12_ck_dhe_rsa_aes_128_cbc_sha256 |
tls12_ck_dhe_dss_aes_256_cbc_sha256 | tls12_ck_dhe_rsa_aes_256_cbc_sha256 |
tls12_ck_rsa_with_aes_128_gcm_sha256 | tls12_ck_rsa_with_aes_256_gcm_sha384 |
tls12_ck_dhe_rsa_with_aes_128_gcm_sha256 | tls12_ck_dhe_rsa_with_aes_256_gcm_sha384 |
tls12_ck_dhe_dss_with_aes_128_gcm_sha256 | tls12_ck_dhe_dss_with_aes_256_gcm_sha384 |
tls12_ck_ecdhe_rsa_with_aes_128_gcm_sha256 | tls12_ck_ecdhe_rsa_with_aes_256_gcm_sha384|
tls13_aes_128_gcm_sha256 | tls13_aes_256_gcm_sha384 | tls13_chacha20_poly1305_sha256 |
tls13_aes_128_ccm_sha256 }
```

缺省情况下，SSL策略加密套件中没有配置任何加密算法。

说明

出于安全性考虑，不建议使用该特性提供的弱安全算法或弱安全协议。如果确实需要使用，请执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包WEAKEA。设备默认自带弱安全算法/协议特性包WEAKEA，特性包安装或卸载的详细步骤请参见《配置指南-系统管理配置》中的“升级维护配置”。

该特性中需要安装弱安全算法/协议特性包后才能使用命令如下所示：

命令	安装特性包后才能使用的参数
set cipher-suite	tls12_ck_dhe_dss_aes_128_cbc_sha、 tls12_ck_dhe_dss_aes_128_cbc_sha256、 tls12_ck_dhe_dss_aes_256_cbc_sha、 tls12_ck_dhe_dss_aes_256_cbc_sha256、 tls12_ck_dhe_rsa_aes_128_cbc_sha、 tls12_ck_dhe_rsa_aes_128_cbc_sha256、 tls12_ck_dhe_rsa_aes_256_cbc_sha、 tls12_ck_dhe_rsa_aes_256_cbc_sha256、 tls12_ck_rsa_aes_128_cbc_sha、 tls12_ck_rsa_aes_128_cbc_sha256、 tls12_ck_rsa_aes_256_cbc_sha、 tls12_ck_rsa_aes_256_cbc_sha256、 tls12_ck_rsa_with_aes_128_gcm_sha256、 tls12_ck_rsa_with_aes_256_gcm_sha384、 tls1_ck_dhe_dss_with_aes_128_sha、 tls1_ck_dhe_dss_with_aes_256_sha、 tls1_ck_dhe_rsa_with_aes_128_sha、 tls1_ck_dhe_rsa_with_aes_256_sha、 tls1_ck_rsa_with_aes_128_sha、 tls1_ck_rsa_with_aes_256_sha
ssl minimum version	tls1.1

SSL通过握手在客户端和服务器之间建立会话，完成双方身份的验证、密钥和加密套件的协商，在通信过程中建议使用TLS1.2及以上版本的安全套件。TLS版本中，使用CBC模式的对称加密算法可能存在数据受到明文恢复攻击而泄露加密传输的内容，因此，在TLS版本中不建议使用CBC模式对数据加密。

----结束

13.5.2 配置 SSL 策略（手工加载证书）

前提条件

在为SSL策略加载信任证书机构文件之前，需完成以下任务：

客户端或服务器已从CA（Certificate Authority，证书机构）申请了证书文件，并将证书上传到系统目录下名为**security**的子目录下。

背景信息

SSL利用数据加密、身份验证和消息完整性验证机制，为基于TCP可靠连接的应用层协议提供安全性保证。应用层协议可以关联SSL策略，使应用层协议与SSL结合，从而为应用层协议提供安全连接。

操作步骤

步骤1 进入系统视图。

```
system-view
```


步骤2 配置SSL策略并进入SSL策略视图。

ssl policy *policy-name*

缺省情况下，没有配置SSL策略。

步骤3 （可选）配置ECDHE算法的椭圆曲线参数。

ecdh group { **nist** | **curve** | **brainpool** } *

缺省情况下，ECDHE算法椭圆曲线参数为Curve和Brainpool。

步骤4 （可选）配置当前SSL策略所采用的最低版本。

ssl minimum version { **tls1.1** | **tls1.2** | **tls1.3** }

缺省情况下，SSL策略所采用的最低版本为TLS1.2。

说明

SSL策略所支持的SSL版本包括TLS1.1、TLS1.2和TLS1.3，其安全性依次升高，建议用户使用TLS1.2或者TLS1.3。

该命令中的参数tls1.1需要执行命令install feature-software WEAKEA安装弱安全算法/协议特性包（WEAKEA）后才能使。

步骤5 为SSL策略加载证书。

缺省情况下，SSL策略未加载证书。

- 为SSL策略加载PEM格式的证书
  certificate load pem-cert *certFile* **key-pair** *keyType* **key-file** *keyFile* **auth-code** [**cipher** *authCode*]
- 为SSL策略加载PEM格式的证书链
  certificate load pem-chain *certFile* **key-pair** *keyType* **key-file** *keyFile* **auth-code** [**cipher** *authCode*]
- 为SSL策略加载PFX格式的证书

  形式一：

  certificate load pfx-cert *certFile* **key-pair** *keyType* **key-file** *keyFile* **auth-code** [**cipher** *authCode*]

  形式二：

  certificate load pfx-cert *certFile* **key-pair** *keyType* **mac** [**cipher** *macCode* **auth-code cipher** *authCode*]

步骤6 （可选）为SSL策略加载数字证书撤销列表CRL（Certificate Revocation List）。

crl load *crlType crlFile*

缺省情况下，SSL策略未加载CRL。

步骤7 （可选）为SSL策略加载信任证书机构文件。

缺省情况下，SSL策略未加载信任证书机构文件。

信任证书机构文件用于验证服务器发送的数字证书的真实性。一个SSL策略最多可以同时加载4个信任证书机构文件。

说明

如果需要对对端进行身份认证需要配置此步骤。

- 为SSL策略加载ASN1格式信任证书机构文件
  trusted-ca load asn1-ca *caFile*
- 为SSL策略加载PEM格式信任证书机构文件
  trusted-ca load pem-ca *caFile*
- 为SSL策略加载PFX格式信任证书机构文件
  trusted-ca load pfx-ca *caFile* **auth-code** [**cipher** *authCode*]

步骤8 （可选）为SSL策略绑定加密套件。

```
binding cipher-suite-customization customization-name
```

缺省情况下，SSL策略没有绑定加密套件。默认所有的加密算法都可以使用。

绑定加密套件中的加密算法之前需已完成SSL策略加密套件的配置，配置过程请参见13.5.1 （可选）配置SSL策略加密套件。

步骤9 （可选）设置证书过期的告警阈值和检查间隔。

```
quit
ssl certificate alarm-threshold early-alarm time check-interval check-period
```

缺省情况下，证书过期提前告警阈值为90天，证书过期告警检查周期为24小时。

----结束

13.5.3 配置 SSL 策略（PKI 加载证书）

背景信息

SSL利用数据加密、身份验证和消息完整性验证机制，为基于TCP可靠连接的应用层协议提供安全性保证。应用层协议可以关联SSL策略，使应用层协议与SSL结合，从而为应用层协议提供安全连接。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 配置SSL策略并进入SSL策略视图。

```
ssl policy policy-name
```

缺省情况下，没有配置SSL策略。

步骤3 （可选）配置ECDHE算法的椭圆曲线参数。

```
ecdh group { nist | curve | brainpool } *
```

缺省情况下，ECDHE算法椭圆曲线参数为Curve和Brainpool。

步骤4 （可选）配置当前SSL策略所采用的最低版本。

```
ssl minimum version { tls1.1 | tls1.2 | tls1.3 }
```

缺省情况下，SSL策略所采用的最低版本为TLS1.2。

说明

SSL策略所支持的SSL版本包括TLS1.1、TLS1.2和TLS1.3，其安全性依次升高，建议用户使用TLS1.2或者TLS1.3。

该命令中的参数tls1.1需要执行命令install feature-software WEAKEA安装弱安全算法/协议特性包（WEAKEA）后才能使。

步骤5 为SSL策略绑定PKI域名。绑定PKI域后，SSL策略使用PKI域下的证书、证书撤销列表。

```
pki-domain pki-domain
```

步骤6 （可选）为SSL策略绑定加密套件。

```
binding cipher-suite-customization customization-name
```

缺省情况下，SSL策略没有绑定加密套件。默认所有的加密算法都可以使用。

绑定加密套件中的加密算法之前需已完成SSL策略加密套件的配置，配置过程请参见**13.5.1 （可选）配置SSL策略加密套件**。

----结束

13.5.4 应用 SSL 策略

背景信息

SSL本身只是一种安全协议，SSL策略只有与各种应用关联后才能生效。

操作步骤

步骤1 应用SSL策略。SSL策略的具体应用请参见**表13-5**。

表 13-5 SSL 策略的主要应用

SSL策略的主要应用	具体应用示例
在BGP中应用SSL	《配置指南-IP路由配置》中的“配置BGP的SSL/TLS认证”
在HTTPS中应用SSL	《配置指南-系统管理》中的“举例：通过使用RESTCONF管理设备”

----结束

14 SSH 配置

背景信息

说明

SSH2.0版本中，使用CBC模式的对称加密算法可能受到明文恢复攻击而泄露加密传输的内容，因此，在SSH2.0中不建议使用CBC模式对数据加密。

14.1 SSH 简介

定义

SSH是Secure Shell（安全外壳）的简称，是一种在不安全的网络环境中，通过加密机制和认证机制，实现安全的访问以及文件传输等业务的网络安全协议。

SSH协议有SSH1.X（SSH2.0之前的版本）和SSH2.0版本。SSH2.0协议相比SSH1.X协议来说，在结构上做了扩展，可以支持更多的认证方法和密钥交换方法，同时提高了服务能力（如SFTP）。

目的

Telnet缺少安全的认证方式，而且传输过程采用TCP进行明文传输，存在很大的安全隐患。单纯提供Telnet服务容易招致DoS（Deny of Service）、主机IP地址欺骗、路由欺骗等恶意攻击。随着人们对网络安全的重视，传统的Telnet通过明文传送密码和数据的方式，已经慢慢不被人接受。SSH是一个网络安全协议，通过对网络数据的加密，解决了这个问题。它在一个不安全的网络环境中，提供了安全的登录和其他安全网络服务。

SSH通过TCP进行数据交互，它在TCP之上构建了一个安全的通道。另外SSH服务除了支持标准端口22外，还支持其他服务端口，以防止受到非法攻击。

14.2 SSH 工作过程

本小节以SSH2.0为例介绍SSH工作的过程，具体分为所述的几个阶段。

表 14-1 工作过程

阶段	说明
连接建立	SSH服务器在22号端口侦听客户端的连接请求，在客户端向服务器端发起连接请求后，双方建立一个TCP连接。
版本协商	双方通过版本协商确定最终使用的SSH版本号。
算法协商	SSH支持多种算法，双方根据本端和对端支持的算法，协商出最终用于产生会话密钥的密钥交换算法、用于数据信息加密的加密算法、用于进行数字签名和认证的公钥算法，以及用于数据完整性保护的HMAC算法。
密钥交换	双方通过DH（Diffie-Hellman Exchange）交换，动态地生成用于保护数据传输的会话密钥和用来标识该SSH连接的会话ID，并完成客户端对服务器端的身份认证。
用户认证	SSH客户端向服务器端发起认证请求，服务器端对客户端进行认证。
会话请求	认证通过后，SSH客户端向服务器端发送会话请求，请求服务器提供某种类型的服务（Stelnet、SFTP或SCP），即请求与服务器建立相应的会话。
会话交互	会话建立后，SSH服务器端和客户端在该会话上进行数据信息的交互。

14.3 SSH 配置注意事项

License 依赖

SSH无需License许可即可使用。

硬件依赖

表 14-2 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2

系列	支持产品
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 14-3 本特性的使用限制

特性限制	系列	涉及产品
出于安全性考虑，不建议使用该特性提供的弱安全算法或弱安全协议。设备默认自带弱安全算法/协议特性包WEAKEA，如果确实需要使用，请执行命令install feature-software WEAKEA安装弱安全算法/协议特性包WEAKEA。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

14.4 SSH 缺省配置

SSH的主要缺省配置如**14.4 SSH缺省配置**所示。

表 14-4 SSH 缺省配置

参数	缺省配置
STelnet服务器功能	关闭
SSH服务器端口号	22
SSH服务器密钥对的更新周期	0小时，表示永不更新
SSH连接认证超时时间	60秒
SSH连接的认证重试次数	3
VTY用户界面的认证方式	没有配置认证方式
VTY用户界面所支持的协议	支持所有协议类型
SSH用户的认证方式	认证方式是空，即不支持任何认证方式
SSH用户的服务方式	服务方式是空，即不支持任何服务方式
SSH服务器为用户分配公钥	没有为用户分配公钥
用户级别	VTY用户界面对应的默认命令访问级别是0
SSH客户端首次登录	关闭

参数	缺省配置
SSH客户端给SSH服务器分配RSA、DSA或ECC公钥	没有为SSH服务器分配RSA、DSA或ECC公钥

14.5 配置 SSH 服务器

14.5.1 配置 SSH 服务器功能及参数

背景信息

配置SSH服务器功能及参数包括配置服务器本地密钥对生成、SSH服务器功能的开启以及服务器参数的配置：端口号、密钥对更新时间、SSH认证超时时间或SSH认证重试次数等。

说明

- 为了保证更好的安全性，建议定期修改密钥。
- 为了保证SSH算法协商成功，SSH服务器配置的密钥交换算法、加密算法、公钥算法和HMAC算法，SSH客户端也必须要支持，否则会导致协商失败。
- SSH服务器不支持兼容SSH1.X版本。
- 为了保证更好的安全性，建议不要使用小于2048位的RSA算法作为SSH用户的认证方式，建议您使用更安全的ECC认证算法。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 生成本地密钥对。

方式一：生成本地RSA、DSA或ECC密钥对。

- 生成本地RSA密钥对。
  ```
  rsa local-key-pair create
  ```
- 生成DSA密钥对。
  ```
  dsa local-key-pair create
  ```
- 生成ECC密钥对。
  ```
  ecc local-key-pair create
  ```

密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看本地密钥对中RSA、DSA或ECC的公钥信息。

方式二：生成带标签的SM2、RSA、DSA或ECC密钥对。

说明

方式二可以最多生成20对密钥对，用户可以在不同时期使用不同的密钥对，更好地确保了通信的安全性。设备最多可生成的密钥对数，可以通过**rsa key-pair maximum**、**dsa key-pair maximum**和**ecc key-pair maximum**命令配置。

1. 生成带标签的RSA、DSA、SM2或ECC密钥对。
   - 生成带标签的RSA密钥对。
     rsa key-pair label *label-name* [**modulus** *modulus-bits*]
   - 生成带标签的DSA密钥对。
     dsa key-pair label *label-name* [**modulus** *modulus-bits*]
   - 生成带标签的ECC密钥对。
     ecc key-pair label *label-name* [**modulus** *modulus-bits*]
   - 生成带标签的SM2密钥对。
     sm2 key-pair label *label-name*
2. 为SSH服务器分配主机密钥或者PKI证书。
   ssh server assign { **rsa-host-key** *key-name* | **dsa-host-key** *key-name* | **ecc-host-key** *key-name* | **sm2-host-key** *key-name* | **pki** *key-name* }

密钥对生成后，可以执行**display rsa key-pair** [**brief** | **label** *label-name*]、**display dsa key-pair** [**brief** | **label** *label-name*]、**display ecc key-pair** [**brief** | **label** *label-name*]、**display sm2 key-pair** [**brief** | **label** *label-name*]命令查看带标签的RSA、DSA、SM2或ECC密钥对信息。

步骤3 使能SSH服务器公钥算法。

ssh server publickey { **dsa** | **ecc** | **rsa** | **x509v3-ssh-rsa** | **rsa_sha2_256** | **rsa_sha2_512** | **sm2** | **x509v3-rsa2048-sha256** } *

缺省情况下，

- 设备以空配置启动时，RSA_SHA2_256、RSA_SHA2_512公钥算法是开启的，SM2、RSA、ECC、DSA、X509-SSH-RSA和X509-RSA-SHA2-256算法关闭。
- 当设备加载配置文件启动时，且配置文件中不存在ssh server publickey的配置时，ECC、RSA、RSA_SHA2_256、RSA_SHA2_512、DSA公钥算法是开启的，SM2、X509-SSH-RSA和X509-RSA-SHA2-256算法关闭。

说明

命令中的参数**dsa**和**rsa**需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包后才能使用。

当使用公钥认证登录设备时，SSH服务器支持的公钥算法需要与命令**ssh user authentication-type**配置SSH用户的认证方式相同，否则用户无法登录设备。

步骤4 使能SSH服务器功能。

- 设备作为STelnet服务器。
  stelnet [**ipv4** | **ipv6**] **server enable**
  缺省情况下，STelnet服务为关闭状态。
- 设备作为SFTP服务器。
  sftp [**ipv4** | **ipv6**] **server enable**
  缺省情况下，SFTP服务为关闭状态。
- 设备作为SCP服务器。
  scp [**ipv4** | **ipv6**] **server enable**
  缺省情况下，SCP服务为关闭状态。

步骤5 配置SSH服务器端口号。

ssh [**ipv4** | **ipv6**] **server port** *port-number*

缺省情况下，SSH服务器端的端口号是22。

如果配置了新的端口号，SSH服务器端先断开当前已经建立的所有SSH连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对SSH服务标准端口的访问，确保安全性。

步骤6 使能SSH服务器上的keepalive特性。

```
undo ssh server keepalive disable
```

缺省情况下，SSH服务器上的keepalive特性处于使能状态。

SSH服务器在使能keepalive特性之后，若收到SSH客户端的keepalive报文之后，会进行响应。这样防止在SSH客户端收不到keepalive响应报文时断开与SSH服务器的连接，避免造成客户端重新连接服务器浪费服务器资源。

步骤7 （可选）配置SSH服务器的扩展属性。

1. 配置SSH服务器端的密钥交换算法列表。

   ```
   ssh server key-exchange { curve25519_sha256 | dh_group16_sha512 | dh_group14_sha1 | dh_group1_sha1 | dh_group_exchange_sha1 | dh_group_exchange_sha256 | ecdh_sha2_nistp256 | ecdh_sha2_nistp384 | ecdh_sha2_nistp521 | sm2_kep } *
   ```

   缺省情况下，SSH服务器使用dh_group_exchange_sha256、dh_group16_sha512、curve25519_sha256密钥交换算法。

   在客户端与服务器协商的过程中，二者对报文传输的密钥交换算法进行协商，服务器端根据客户端发来的密钥交换算法列表与自身的密钥交换算法列表进行对比，选择客户端与自己相匹配的第一个密钥交换算法作为报文传输的密钥交换算法，如果客户端的密钥交换算法列表与服务器端的密钥交换算法列表没有相匹配的算法，则协商失败。

   说明

   为保证更好的安全性，建议使用以下安全性更高的密钥交换算法：curve25519_sha256。

   命令中的参数**dh_group_exchange_sha1**、**dh_group1_sha1**、**sm2_kep**和**dh_group14_sha1**，需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包后才能使用。

2. 配置SSH会话密钥重协商条件。

   ```
   ssh server rekey { data-limit data-limit | max-packet max-packet | time minutes } *
   ```

   为了提高传输安全性，SSH服务器可以启动密钥重协商，如果重协商失败，就会断开SSH连接。缺省情况下，满足以下三个条件中的至少一个时，SSH服务器即触发密钥重协商：

   - 使用当前密钥传输报文总数据量达到1000兆字节。
   - 发送和接收的报文总个数达到2147483648个。
   - SSH连接时长达到60分钟。

3. 配置与SSH客户端进行Diffie-hellman-group-exchange密钥交换时支持的最小密钥长度。

   ```
   ssh server dh-exchange min-len min-len
   ```

   缺省情况下，SSH服务器与客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度为3072比特。为了提高安全性，建议配置为3072比特。

   说明

   Diffie-hellman-group-exchange密钥交换算法的最小长度小于等于2048bits时，存在安全风险，需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包（WEAKEA）后才能使用。建议将最小长度设置为3072bits。此命令对IPv4和IPv6均生效。

4. 配置SSH服务器端的加密算法列表。

   ```
   ssh server cipher { des_cbc | 3des_cbc | aes128_cbc | aes256_cbc | aes128_ctr | aes256_ctr | arcfour128 | arcfour256 | aes192_cbc | aes192_ctr | aes128_gcm | aes256_gcm | blowfish_cbc | sm4_cbc } *
   ```

   缺省情况下，SSH服务器使用的加密算法为AES128_CTR、AES256_CTR、AES192_CTR、AES128_GCM、AES256_GCM。

说明

为保证更好的安全性，建议使用以下安全性更高的加密算法：AES128_CTR、AES256_CTR、AES192_CTR、AES128_GCM、AES256_GCM、SM4_GCM。

命令中的参数**blowfish_cbc**、**des_cbc**、**3des_cbc**、**aes128_cbc**、**aes256_cbc**、**arcfour128**、**arcfour256**、**aes192_cbc**和**sm4_cbc**，需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包后才能使用。

5. 配置SSH服务器上的校验算法列表。
   ssh server hmac { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** | **sha2_512** | **sm3** } *
   缺省情况下，SSH服务器使用的HMAC认证算法为SHA2_256和SHA2_512。

   说明

   为保证更好的安全性，建议使用以下安全性更高的HMAC算法：SHA2_256、SHA2_512、SM3。

   命令中的参数**md5**、**md5_96**、**sha1**、**sha1_96**和**sha2_256_96**，需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包后才能使用。
6. 关闭SSH服务端使用不安全算法时的风险提示功能。
   ssh server security-banner disable
   缺省情况下，SSH服务端使用不安全算法时的风险提示功能处于使能状态。
7. 配置SSH认证超时时间。
   ssh server timeout *seconds*
   缺省情况下，SSH连接认证超时时间是60秒。
   当设置的SSH认证超时时间到达后，如果用户还未登录成功，则终止当前连接，确保了安全性。
8. 配置SSH认证重试次数。
   ssh server authentication-retries *times*
   缺省情况下，SSH连接的认证重试次数是3。
   配置SSH认证重试次数用来设置SSH用户请求连接的认证重试次数，防止非法用户登录。
9. 配置访问控制列表。
   ssh [**ipv6**] **server acl** { *acl-number* | *acl-name* }
   缺省情况下，没有配置访问控制列表。
   配置了访问控制列表，可控制哪些客户端能以SSH方式访问本设备。
10. 配置SSH服务器认证时允许使用的RSA最小公钥长度。
    ssh server rsa-key min-length *min-length-val*

步骤8 配置SSH服务器的源接口或源地址。

缺省情况下，未指定SSH服务器端的源接口和IPv6源地址。

- 配置SSH服务器的源接口为指定接口。
  ssh server-source -i *interface-type interface-number*
- 配置SSH服务器源接口为设备上所有有效接口。
  ssh server-source all-interface
- 配置SSH服务器的IPv6源地址。
  ssh ipv6 server-source -a *ipv6-address* [**-vpn-instance** *vpn-instance-name*]
- 配置SSH服务器的IPv6源接口为所有有效接口。
  ssh ipv6 server-source all-interface

说明

配置**ssh server-source all-interface**或**ssh ipv6 server-source all-interface**命令后，将不会指定SSH服务器的源接口，用户可从所有有效接口登录，增加系统安全风险，建议用户谨慎使用。

步骤9 配置单个IP地址连接SSH服务器的最大连接数。

```
ssh server ip-limit-session limit-session-num
```

缺省情况下，单个IP地址连接SSH服务器的最大连接数是256。

步骤10 开启SSH服务器的键盘交互认证方式。

```
ssh server authentication-type keyboard-interactive enable
```

缺省情况下，SSH服务器的键盘交互认证方式已开启。

使用口令卡认证方式的SSH用户登录，必须开启键盘交互认证方式。

步骤11 （可选）使能SSH服务器上的客户端IP地址锁定功能。

```
undo ssh server ip-block disable
```

缺省情况下，SSH服务器上的客户端IP地址锁定功能处于使能状态。

- 如果SSH服务器上的客户端IP地址锁定功能处于使能状态，则被锁定的客户端IP地址不能被认证通过，同时会在**display ssh server ip-block list**命令回显中显示被锁定的客户端IP地址。
- 如果SSH服务器上的客户端IP地址锁定功能处于去使能状态，则**display ssh server ip-block list**命令回显中会把先前锁定的客户端IP地址记录删除，新的认证失败的客户端IP地址也不会被记录显示。

说明

在SSH连接中，如果用户在5分钟内连续6次认证失败，则IP地址将会被锁定5分钟，可以通过执行命令**activate ssh server ip-block ip-address** *ip-address* [**vpn-instance** *vpn-name*]提前对被锁定的IP地址进行解锁。

步骤12 （可选）配置在一定时间内通过SSH登录服务器失败次数的告警上报门限和告警恢复门限。

```
ssh server login-failed threshold-alarm upper-limit report-times lower-limit resume-times period period-time
```

缺省情况下，在5分钟内发生30次或30次以上次数登录失败，产生告警；在5分钟内登录失败次数小于20，取消告警。

步骤13 （可选）配置SSH协议报文的DSCP优先级。

```
ssh server dscp value
```

缺省情况下，SSH协议报文的DSCP优先级值为48。

步骤14 （可选）使能SSH服务器的本地端口转发服务。

```
ssh server tcp forwarding enable
```

缺省情况下，SSH服务器的本地端口转发服务没有使能。

----结束

14.5.2 配置 VTY 用户界面支持 SSH 协议

背景信息

在通过SSH方式登录设备前，需要配置登录时采用的VTY用户界面，使其支持SSH协议。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 进入VTY用户界面视图。

```
user-interface vty first-ui-number [ last-ui-number ]
```

步骤3 配置VTY用户界面的认证方式为AAA。

```
authentication-mode aaa
```

缺省情况下，VTY用户界面没有验证方式。

如果配置用户界面支持的协议是SSH，必须设置VTY用户界面认证方式为AAA认证，否则**protocol inbound ssh**将不能配置成功。

步骤4 配置VTY用户界面支持SSH协议。

```
protocol inbound { all | ssh }
```

缺省情况下，用户界面支持所有协议类型，包括SSH。

----结束

14.5.3 配置 SSH 用户

背景信息

配置SSH用户包括创建SSH用户和配置SSH用户的认证方式，设备支持的认证方式包括RSA、password、password-rsa、DSA、password-dsa、ECC、password-ecc、password-x509v3-rsa、x509v3-rsa、sm2、password-sm2和all。其中：

- password-rsa认证需要同时满足password认证和RSA认证。
- password-dsa认证需要同时满足password认证和DSA认证。
- password-ecc认证需要同时满足password认证和ECC认证。
- password-x509v3-rsa认证需要同时满足password认证和X509V3-SSH-RSA认证。
- password-sm2需要同时满足password认证和SM2认证。
- all认证是指所有认证方式满足其中一种即可。

说明

为了保证更好的安全性，建议不要使用小于2048位的RSA算法作为SSH用户的认证方式，建议您使用更安全的ECC认证算法。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建SSH用户。

```
ssh user user-name
```

步骤3 配置SSH用户的认证方式。

```
ssh user user-name authentication-type { password | rsa | password-rsa | all | dsa | password-dsa | ecc | password-ecc | password-x509v3-rsa | x509v3-rsa | sm2 | password-sm2 }
```

如果没有使用**ssh user** *user-name*命令配置相应的SSH用户，则可以直接执行**ssh authentication-type default password**命令为用户配置SSH认证缺省采用密码认证，在用户数量比较多时，对用户使用缺省的密码认证方式可以简化配置，此时只需再配置AAA用户即可。

- password认证依靠AAA实现，当用户使用password、password-rsa、password-x509v3-rsa、password-dsa或password-ecc、password-sm2认证方式登录设备时，需要在AAA视图下创建同名的本地用户。
- 如果SSH用户使用RSA、DSA、SM2或ECC认证，需要在服务器端和客户端都需要生成本地RSA、DSA、SM2或ECC密钥对，并且服务器端和客户端都需要将对方的公钥配置到本地。

根据上面配置的认证方式，进行选择配置，具体操作见**表14-5**。

表 14-5 不同认证方式的配置

认证方式	配置说明
password认证	创建AAA同名用户，请根据**表14-6**进行配置。
RSA、DSA或ECC认证	生成本地RSA、DSA、SM2或ECC密钥对，请根据**表14-7**进行配置。
password-rsa、password-dsa、password-sm2或password-ecc认证	创建AAA同名用户并生成本地RSA、DSA、SM2或ECC密钥对，请根据**表14-6**和**表14-7**进行配置。
x509v3-rsa	对SSH用户绑定PKI域，请根据**表14-8**进行配置。
password-x509v3-rsa	创建AAA同名用户并绑定PKI域，请根据**表14-6**和**表14-8**进行配置。

表 14-6 在 AAA 视图下创建同名的本地用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	为充分保证设备安全，请用户定期修改密码。
配置本地用户的服务方式	**local-user** *user-name* **service-type ssh**	-

操作步骤	命令	说明
配置本地用户的级别	**local-user** *user-name* **privilege level** *level*	-
退回到系统视图	**quit**	-

表 14-7 配置 SSH 用户的本地 RSA、DSA、SM2 或 ECC 密钥

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置SSH连接的认证类型	**ssh authorization-type default** { **aaa** | **root** }	缺省情况下，SSH连接的缺省类型为AAA。 当配置为AAA类型时，只允许配置为password认证方式；如果需要使用公钥认证方式，可以通过以下两种方式任意一种实现： ● 执行此命令，配置为root类型。 ● 在AAA视图下，创建同名的本地用户。
进入RSA、DSA、ECC、SM2公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** *enc-type*] 或 **dsa peer-public-key** *key-name* **encoding-type** *enc-type* 或 **ecc peer-public-key** *key-name* [**encoding-type** *enc-type*] 或 **sm2 peer-public-key** *key-name*	-
进入公共密钥编辑视图	**public-key-code begin**	-

操作步骤	命令	说明
编辑公共密钥	*hex-data*	• 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由支持SSH的客户端软件生成。具体操作参见相应的SSH客户端软件的帮助文档。 • 请将RSA、DSA、SM2或ECC公钥输入到作为SSH服务器的设备上。
退出公共密钥编辑视图	**public-key-code end**	• 如果未输入合法的密钥编码hex-data，执行本步骤后，将无法生成密钥。 • 如果指定的密钥*key-name*已经在别的窗口下被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH用户分配RSA、DSA、SM2或ECC公钥	**ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** | **sm2-key**} *key-name*	-

表 14-8 配置对 SSH 用户绑定 PKI 域

操作步骤	命令	说明
进入系统视图	**system-view**	-
为SSH用户绑定PKI域	**ssh user** *user-name* **assign pki** *pki-name*	为SSH服务器分配PKI证书。 前提条件是PKI配置已完成。

步骤4 配置SSH用户的服务方式。

```
ssh user user-name service-type { all | { sftp | stelnet | snetconf }*}
```

缺省情况下，SSH用户的服务方式是空，即不支持任何服务方式。

步骤5 （可选）配置SSH用户的SAN/CN校验。

```
ssh user user-name cert-verify-san enable
```

当配置SSH用户绑定PKI域后，可校验PKI证书中SAN（Subject Alternative Name）或者CN（common name）中是否包含该认证用户的域名，增强安全性。

----结束

14.5.4 应用 SSH

背景信息

SSH本身只是一种安全协议，SSH策略只有与各种应用关联后才能生效。

操作步骤

步骤1 应用SSH策略。设备作为SSH服务器对应的具体应用请参见**表14-9**。

表 14-9 设备作为 SSH 服务器的主要应用

SSH策略的主要应用	具体应用示例
SSH在Stelnet登录中的应用	举例：配置用户通过STelnet登录设备
SSH在SFTP中的应用	举例：配置设备作为SFTP服务器
SSH在SCP中的应用	配置设备作为SCP服务器
SSH在Netconf中的应用	举例：通过使用NETCONF与ncclient通信

----结束

14.6 配置 SSH 客户端

14.6.1 配置设备首次连接 SSH 服务器的方式

背景信息

作为客户端的设备首次连接SSH服务器时，因为客户端还没有保存过SSH服务器的公钥或没有绑定相关的PKI证书，无法对SSH服务器有效性进行检查，这样会导致连接不成功。

用户可以根据需求选择以下一种方式来解决：

- 使能SSH客户端首次登录功能方式：不对SSH服务器进行有效性检查，确保首次连接成功。成功连接后，系统将自动分配并保存公钥，为下次连接时认证使用。
- SSH客户端绑定指定SSH服务器公钥方式：将服务器端产生的公钥直接保存至客户端，保证在首次连接时SSH服务器有效性检查能够通过。
- SSH客户端分配PKI证书方式：将用于与服务器端进行认证的PKI域绑定在客户端上，保证在首次连接时SSH服务器的证书验证合法。

第一种方式配置比较简单，后两种方式配置比较复杂，但是安全性更高。

说明

- 为了保证更好的安全性，建议定期修改密钥。
- 为了保证更好的安全性，建议不要使用小于2048位的RSA算法作为SSH用户的认证方式，建议您使用更安全的ECC认证算法。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 （可选）生成本地秘钥对。

此步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，设备以password方式登录SSH服务器，则无需执行。

- 生成本地RSA密钥对。
  ```
  rsa local-key-pair create
  ```
- 生成DSA密钥对。
  ```
  dsa local-key-pair create
  ```
- 生成ECC密钥对。
  ```
  ecc local-key-pair create
  ```

密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看本地密钥对中RSA、DSA或ECC的公钥信息。

步骤3 配置设备首次连接SSH服务器的方式。

- 使能SSH客户端首次登录功能方式
  ```
  ssh client first-time enable
  ```
  缺省情况下，SSH客户端首次登录功能是关闭的。
- SSH客户端绑定指定SSH服务器公钥方式
  a. 进入RSA、DSA、ECC、SM2公共密钥视图。
     - 进入RSA公共密钥视图。
       ```
       rsa peer-public-key key-name [ encoding-type enc-type ]
       ```
     - 进入DSA公共密钥视图。
       ```
       dsa peer-public-key key-name encoding-type enc-type
       ```
     - 进入ECC公共密钥视图。
       ```
       ecc peer-public-key key-name [ encoding-type enc-type ]
       ```
     - 进入SM2公共密钥视图。
       ```
       sm2 peer-public-key key-name
       ```

  b. 进入公共密钥编辑视图。
     ```
     public-key-code begin
     ```
  c. 编辑公共密钥。
     ```
     hex-data
     ```
     - 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由SSH服务器随机生成。
     - 进入公共密钥编辑视图后，即可将服务器上产生的RSA、DSA或ECC公钥输入到客户端。

d. 退出公共密钥编辑视图。
public-key-code end

- 如果输入的密钥编码hex-data不合法，执行本步骤后，将无法生成密钥。
- 如果指定的密钥key-name已经被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。

e. 退出公共密钥视图，回到系统视图。
peer-public-key end

f. 为SSH服务器绑定RSA、DSA或ECC公钥。
ssh client peer *server-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** | **sm2-key** } *key-name*

如果SSH客户端保存的SSH服务器公钥失效，执行命令**undo ssh client peer** *server-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** | **sm2-key** }，取消SSH服务器与RSA、DSA或ECC公钥的绑定关系，再执行本命令，为SSH服务器重新分配RSA、DSA或ECC公钥。

- SSH客户端绑定用于与SSH服务器进行认证的PKI域。
ssh client assign pki *pki-domain*

步骤4 （可选）使能SSH客户端公钥算法。

ssh client publickey { **dsa** | **ecc** | **rsa** | **rsa_sha2_256** | **rsa_sha2_512**| **sm2** | **x509v3-ssh-rsa**} *

缺省情况下，

- 设备以空配置启动时，RSA_SHA2_256、RSA_SHA2_512公钥算法是开启的。
- 当设备加载配置文件启动时，且配置文件中不存在ssh client publickey的配置时，ECC、RSA_SHA2_256、RSA_SHA2_512公钥算法是开启的。

执行此命令可以配置使用更安全的公钥算法登录设备，同时拒绝使用其他公钥算法，从而提升设备安全性。推荐使用RSA_SHA2_256或RSA_SHA2_512公钥算法。

- 如果**ssh client first-time enable**命令功能使能，客户端登录服务器时会提示保存服务器公钥，执行保存操作时，SSH客户端会自动根据**ssh client publickey**命令配置的公钥算法，选择能够与SSH客户端协商成功的公钥算法分配给SSH服务器。
- 如果**ssh client first-time enable**命令功能关闭，则必须执行**ssh client peer assign**命令为SSH服务器分配公钥，且分配的公钥算法必须能和**ssh client publickey**命令配置的公钥算法协商成功。这样SSH客户端对SSH服务器的公钥验证才会通过。

说明

命令中的参数**dsa**、**ecc**和**rsa**，需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包后才能使用。

----结束

14.6.2 配置 SSH 客户端参数

背景信息

配置SSH客户端参数包括配置SSH客户端发送keepalive报文的时间间隔和SSH客户端发送的keepalive报文的最大数目等。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 配置SSH客户端发送keepalive报文的时间间隔。

```
ssh client keepalive-interval seconds
```

缺省情况下，SSH客户端发送keepalive报文的时间间隔为0秒，即不发送keepalive报文。

如果设置发送报文的时间间隔是0秒，那么配置的最大keepalive报文数量将无效。

如果SSH客户端在周期内没有收到来自服务器的任何数据，客户端则在周期之后发送keepalive报文给服务器，直到达到配置的最大数目。如果客户端收不到服务器的keepalive的响应报文，它就会断开与服务器的连接。

步骤3 配置SSH客户端发送的keepalive报文的最大数目。

```
ssh client keepalive-maxcount count
```

缺省情况下，SSH客户端发送的keepalive报文的最大数目为3。

如果SSH客户端在周期内没有收到来自服务器的任何数据，客户端则在周期之后发送keepalive报文给服务器，直到达到配置的最大数目。如果客户端收不到服务器的keepalive的响应报文，它就会断开与服务器的连接。

步骤4 （可选）配置SSH客户端上的密钥交换算法列表。

```
ssh client key-exchange { dh_group14_sha1 | dh_group1_sha1 | dh_group_exchange_sha1 | dh_group_exchange_sha256 | ecdh_sha2_nistp256 | ecdh_sha2_nistp384 | ecdh_sha2_nistp521 | sm2_kep | dh_group16_sha512 | curve25519_sha256 } *
```

缺省情况下，SSH客户端使用dh_group_exchange_sha256、dh_group16_sha512、curve25519_sha256密钥交换算法。

说明

- 为保证更好的安全性，建议使用安全性更高的**curve25519_sha256**、**dh_group_exchange_sha256**、**sm2_kep**、**dh_group16_sha512**密钥交换算法。
- 命令中的参数**dh_group_exchange_sha1**、**dh_group1_sha1**、**sm2_kep**和**dh_group14_sha1**，需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包后才能使用。

步骤5 （可选）配置SSH会话密钥重协商条件。

```
ssh client rekey { data-limit data-limit | max-packet max-packet | time minutes } *
```

为了提高传输安全性，SSH客户端可以启动密钥重协商，如果重协商失败，就会断开SSH连接。缺省情况下，满足以下三个条件中的至少一个时，SSH客户端即触发密钥重协商：

- 使用当前密钥传输报文总数据量达到1000兆字节。
- 发送和接收的报文总个数达到2147483648个。
- SSH连接时长达到60分钟。

步骤6 （可选）配置SSH客户端的加密算法列表。

```
ssh client cipher { des_cbc | 3des_cbc | aes128_cbc | aes256_cbc | aes128_ctr | aes256_ctr | arcfour128 | arcfour256 | aes192_cbc | aes192_ctr | aes128_gcm | aes256_gcm | sm4_cbc } *
```

缺省情况下，

- 设备以空配置启动时，SSH客户端使用的加密算法为：AES256_GCM、AES128_GCM、AES256_CTR、AES192_CTR、AES128_CTR加密算法。
- 当设备加载配置文件启动时，且配置文件中不存在**ssh client cipher**的配置时，SSH客户端使用的加密算法为：AES128_CTR、AES256_CTR、AES192_CTR、AES128_GCM、AES256_GCM加密算法。

说明

为保证更好的安全性，建议使用以下安全性更高的算法：AES128_CTR、AES256_CTR、AES192_CTR、AES128_GCM、AES256_GCM、SM4_GCM。

命令中的参数**des_cbc**、**3des_cbc**、**aes128_cbc**、**aes256_cbc**、**arcfour128**、**arcfour256**、**aes192_cbc**和**sm4_cbc**，需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包后才能使用。

步骤7 （可选）配置SSH客户端上的校验算法列表。

ssh client hmac { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** | **sha2_512** | **sm3** } *

缺省情况下，

- 设备以空配置启动时，SSH客户端HMAC认证算法支持SHA2_512、SHA2_256。
- 当设备加载配置文件启动时，且配置文件中不存在**ssh client hmac**的配置时，SSH客户端HMAC认证算法支持MD5、MD5_96、SHA2_512、SHA1、SHA1_96、SHA2_256和SHA2_256_96。

说明

为保证更好的安全性，建议使用以下安全性更高的HMAC算法：SHA2_256、SHA2_512、SM3，不要使用SHA2_256_96、SHA1、SHA1_96、MD5和MD5_96等不安全的HMAC算法。

命令中的参数**md5**、**md5_96**、**sha1**、**sha1_96**和**sha2_256_96**，需要执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包后才能使用。

步骤8 （可选）配置SSH协议报文的DSCP优先级。

ssh client dscp *value*

缺省情况下，SSH协议报文的DSCP优先级值为48。

----结束

14.6.3 应用 SSH

背景信息

SSH本身只是一种安全协议，SSH策略只有与各种应用关联后才能生效。

操作步骤

步骤1 应用SSH策略。设备作为SSH客户端对应的具体应用请参见**表14-10**。

表 14-10 设备作为 SSH 客户端的主要应用

SSH策略的主要应用	具体应用示例
SSH在Stelnet登录中的应用	举例：配置设备作为STelnet客户端登录其他设备

SSH策略的主要应用	具体应用示例
SSH在SFTP中的应用	举例：配置设备作为SFTP客户端
SSH在SCP中的应用	举例：配置设备作为SCP客户端

----结束

15 HTTPS 配置

15.1 HTTPS 简介

定义

HTTP（Hypertext Transfer Protocol）即超文本传输协议，是用于从WWW服务器传输超文本到本地浏览器的传输协议。HTTP位于应用层，基于TCP/IP协议来传输各种数据，例如Web页面，HTTP由请求和响应构成，是一个标准的客户端/服务器模型。

HTTPS（Secure HTTP）是支持安全套接层SSL（Secure Sockets Layer）协议的HTTP协议。

目的

HTTP功能为用户和使用HTTP协议传输数据的特性提供了统一的接口。但是HTTP协议不具备安全机制，采用明文形式传输数据，不能验证通信双方的身份，无法防止传输的数据被篡改，安全性很低。HTTPS是在HTTP上建立SSL加密层，并对传输数据进行加密，是HTTP协议的安全版。HTTPS从以下几方面提高了设备的安全性：

- 客户端与服务器之间交互的数据需要经过加密，保证了数据传输的安全性和完整性，从而实现了对设备的安全管理。
- 对服务器和客户端进行基于证书的身份认证。
- 消息传输过程中使用消息验证码MAC（Message Authentication Code）算法来检验消息的完整性。

当前需要开启HTTPS客户端功能的特性有：

- NETCONF场景下，通过HTTPS协议从HTTPS服务器加载指定YANG文件的配置数据到配置数据库。

15.2 HTTPS 原理描述

HTTP 报文格式

HTTP是一种请求/响应协议，HTTP报文包括请求报文和响应报文。

请求报文

HTTP客户端向服务器端发送一个请求，请求报文中包含三部分：请求行、请求头部和请求数据，如图15-1所示。

图 15-1 请求报文格式

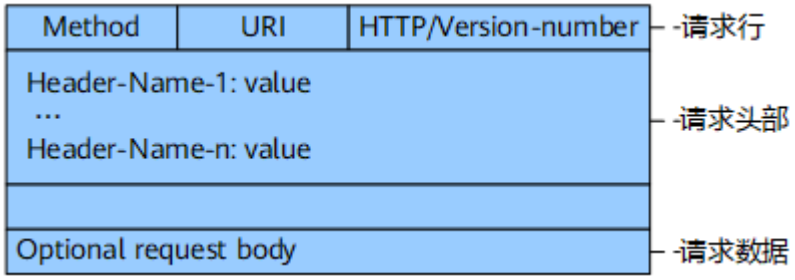


表 15-1 请求报文各字段解释

字段名	含义
Method	HTTP操作方法，作用于URI中指定的目标资源。包括GET、HEAD、PUT、POST、TRACE、OPTIONS、DELETE以及扩展方法。
URI	URL地址。
HTTP/Version-number	HTTP协议版本。
Header-Name-n:value	头部字段名：值。
Optional request body	（可选）请求消息体。

响应报文

HTTP服务器收到客户端发送的请求后，会返回响应报文给客户端。响应报文也包含三部分：响应行、响应头部和响应数据，如图15-2所示。

图 15-2 响应报文格式

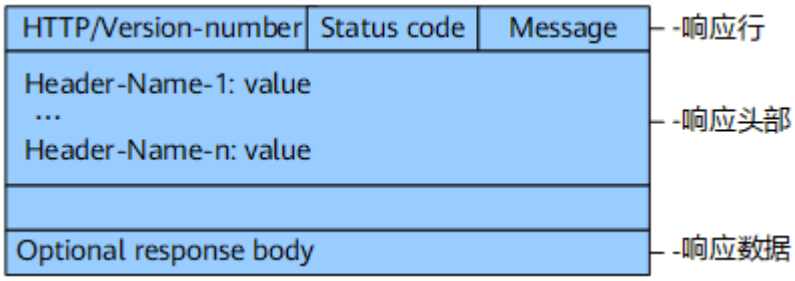


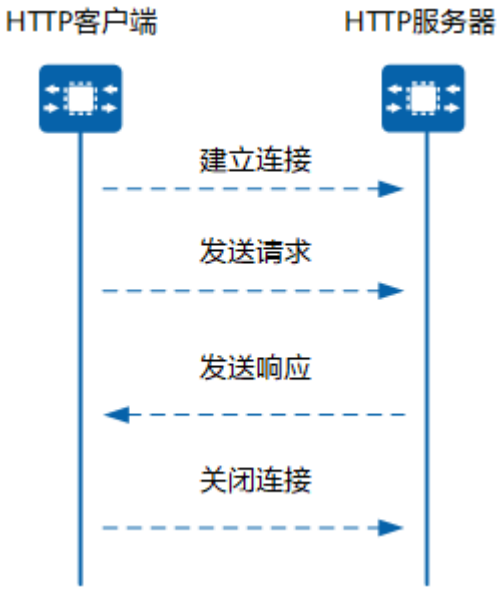
表 15-2 响应报文各字段解释

字段名	含义
HTTP/Version-number	HTTP协议版本。
Status code	HTTP状态码。 状态代码为3位数字，200~299的状态码表示成功，300~399的状态码指资源重定向，400~499的状态码指客户端请求出错，500~599的状态码指服务端出错。
Message	HTTP状态消息。
Header-Name-n:value	头部字段名：值。
Optional response body	（可选）响应消息体。

HTTP 协议通信过程

基于HTTP协议的客户/服务器模式的信息交换过程如图15-3所示，它分四个过程：建立连接、发送请求、发送响应、关闭连接。

图 15-3 HTTP 协议通信过程



1. HTTP客户端向HTTP服务器发起连接请求。
2. 建立连接后，HTTP客户端发送一个请求报文给HTTP服务器。
3. HTTP服务器接到请求报文后，发送响应报文给HTTP客户端。
4. HTTP客户端接收服务器返回的信息后，一般由HTTP客户端请求关闭连接。

HTTP 应用 SSL

HTTP协议不具备安全机制，采用明文形式传输数据，不能验证通信双方的身份，无法防止传输的数据被篡改，安全性很低。安全协议SSL利用数据加密、身份验证和消息完整性验证机制，为基于TCP可靠连接的应用层协议提供了安全性保证。HTTPS是在HTTP上应用SSL来保障HTTP的安全性，对HTTPS可以简单理解为HTTPS = HTTP +SSL。安全连接的URL将以https://而不是以http://开头。

HTTP应用SSL进行数据传输时，HTTP客户端首先向HTTP服务器的适当端口发起一个连接，然后发送ClientHello来开始SSL握手。当SSL握手完成，客户端就初始化第一个HTTP请求。所有的HTTP数据必须作为SSL的“应用数据”发送。

HTTPS连接时需要进行证书申请，申请证书前需要了解以下相关概念：

数字证书

数字证书是由CA签发的一个声明，证明证书主体（证书申请者拥有了证书后即成为证书主体）与证书中所包含的公钥的惟一对应关系。数字证书中包括证书申请者的名称及相关信息、申请者的公钥、签发数字证书的CA的数字签名及数字证书的有效期等内容。数字证书使网上通信双方的身份得到了互相验证，提高了通信的可靠性。

设备可以加载PEM、ASN1和PFX三种格式的数字证书文件。不同格式的数字证书文件的内容是一样的。

- PEM是最常用的一种数字证书格式，文件的扩展名是.pem，适用于系统之间的文本模式传输。
- ASN1是通用的数字证书格式之一，文件的扩展名是.der，是大多数浏览器的默认格式。
- PFX是通用的数字证书格式之一，文件的扩展名是.pfx，是可移植的二进制格式，可以转换为PEM或ASN1格式。

CA

CA是发放、管理、废除数字证书的机构。CA的作用是检查数字证书持有者身份的合法性，并签发数字证书（在证书上签字），以防证书被伪造或篡改，以及对证书和密钥进行管理。国际上被广泛信任的CA，被称之为根CA。根CA可授权其他CA为其下级CA。CA的身份也需要证明，而证明信息在信任证书机构文件中描述。

例如：CA1作为最上级CA也叫根证书，签发下一级CA2证书，CA2又可以给它的下一级CA3签发证书，以此下去，最终由CAn签发服务器的证书。

如果服务器端的证书由CA3签发，则在客户端验证证书的过程从服务器端的证书有效性验证开始。先由CA3证书验证服务器端证书的有效性，如果通过则再由CA2证书验证CA3证书的有效性，最后由最上级CA1证书验证CA2证书的有效性。只有通过最上级CA证书即根证书的验证，服务器证书才会验证成功。

证书撤销列表CRL（Certificate Revocation List）

CRL由CA发布，它指定了一套证书发布者认为无效的证书。

数字证书的寿命是有限的，但CA可通过证书撤销过程缩短证书的寿命。CRL指定的寿命通常比数字证书指定的寿命要短。由CA撤销数字证书，意味着CA在数字证书正常到期之前撤销允许使用密钥对的有关声明。在撤销证书到期后，CRL中的有关数据被删除，以缩短CRL列表的大小。

15.3 HTTP 配置注意事项

License 依赖

HTTPS无需License许可即可使用。

硬件依赖

表 15-3 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

无

15.4 HTTPS 缺省配置

HTTPS的主要缺省配置如表15-4所示。

表 15-4 HTTPS 缺省配置

参数	缺省配置
HTTP	关闭

15.5 配置 HTTPS 客户端

15.5.1 配置 SSL 策略

背景信息

在配置HTTPS前，需要在设备上部署SSL策略，并加载相应的数字证书。SSL策略是指设备启动时使用的SSL参数。只有与应用层协议（如HTTP协议）关联后，SSL策略才能生效。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 配置SSL策略并进入SSL策略视图。

```
ssl policy policy-name
```

步骤3 HTTPS客户端需要根据HTTPS服务器加载的证书格式为SSL策略加载证书。

- 为SSL策略加载PEM格式的证书。
  ```
  certificate load pem-cert certFile key-pair keyType key-file keyFile auth-code [ cipher authCode ]
  ```
- 为SSL策略加载PFX格式的证书。
  ```
  certificate load pfx-cert certFile key-pair keyType mac [ cipher macCode auth-code cipher authCode ]
  certificate load pfx-cert certFile key-pair keyType key-file keyFile auth-code [ cipher authCode ]
  ```
- 为SSL策略加载PEM格式的证书链。
  ```
  certificate load pem-chain certFile key-pair keyType key-file keyFile auth-code [ cipher authCode ]
  ```

步骤4 HTTPS客户端需要根据HTTPS服务器加载的信任证书机构文件为SSL策略加载信任证书机构文件。

- 为SSL策略加载PEM格式信任证书机构文件。
  ```
  trusted-ca load pem-ca caFile
  ```
- 为SSL策略加载PFX格式信任证书机构文件。
  ```
  trusted-ca load pfx-ca caFile auth-code [ cipher authCode ]
  ```
- 为SSL策略加载ASN1格式信任证书机构文件。
  ```
  trusted-ca load asn1-ca caFile
  ```

----结束

15.5.2 配置 HTTPS 客户端

前提条件

在配置HTTPS客户端之前，需要完成以下任务：

- 设备与HTTPS服务器之间路由可达。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 使能HTTP功能，并进入HTTP视图。

```
http
```

步骤3 为HTTPS客户端配置SSL策略。

```
client ssl-policy policy-name
```

步骤4 配置HTTPS客户端对服务器端进行合法性校验。

```
client ssl-verify peer
```

步骤5 （可选）配置HTTPS客户端绑定的源接口。

```
client source-interface { interface-name | interface-type interface-number }
```

缺省情况下，未绑定客户端源接口。

步骤6 （可选）配置HTTP客户端的源IPv6地址和VPN。

client ipv6 source-address *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*]

----结束

15.5.3 配置 HTTPS 下载系统软件

前提条件

在配置HTTPS下载系统软件之前，需要完成以下任务：

- 配置SSL策略。

背景信息

设备可通过HTTPS方式下载系统软件，如果不指定SSL策略，则使用HTTPS客户端配置的SSL策略。

操作步骤

步骤1 下载文件。

download *file-url* [**save-as** *file-path* | [**ssl-policy** *policy-name* [**ssl-verify peer** [**verify-dns**]] | **verify-dns**] | **vpn-instance** *vpn-name* | **source-ip** *ip-address*] *

----结束

15.5.4 配置 HTTPS 上传本地文件

前提条件

在配置HTTPS上传本地文件之前，需要完成以下任务：

- 配置SSL策略。

背景信息

设备可通过HTTPS方式上传本地文件到服务器，如果不指定SSL策略，则使用HTTPS客户端配置的SSL策略。在服务器端可根据本地文件分析设备运行状态。

操作步骤

步骤1 上传文件。

upload *file-url* **local-file** *file-path* [[**ssl-policy** *policy-name* [**ssl-verify peer** [**verify-dns**]] | **verify-dns**] | **user-name** *name-value* **password** *password-value* | **vpn-instance** *vpn-name* | **source-ip** *ip-address*] *

----结束

15.5.5 举例：配置设备作为 HTTPS 客户端

组网需求

如图15-4所示，在配置HTTPS客户端之前，需要在设备上部署SSL策略，并加载相应的数字证书，与应用层协议HTTP协议关联后，用户才可以通过HTTPS客户端登录HTTPS服务器。

图 15-4 配置通过 HTTPS 访问其他设备文件组网图

配置思路

采用如下的思路配置通过HTTPS访问其他设备文件：

1. 配置HTTPS客户端的SSL策略。
2. 配置HTTPS客户端。

操作步骤

步骤1 配置HTTPS客户端的SSL策略。

配置PKI域。

```
<HUAWEI> system-view
[HUAWEI] pki realm domain1
[HUAWEI-pki-n-domain1] quit
[HUAWEI] pki import-certificate ca realm domain1 pem filename capki.cer
```

配置SSL绑定PKI域。

```
<HUAWEI> system-view
[HUAWEI] ssl policy policy1
[HUAWEI-ssl-policy-policy1] pki-domain domain1
[HUAWEI-ssl-policy-policy1] quit
```

步骤2 配置HTTPS客户端。

```
[HUAWEI] http
[HUAWEI-http] client ssl-policy policy1
[HUAWEI-http] client ssl-verify peer
[HUAWEI-http] quit
```

----结束

检查配置结果

执行命令**display ssl policy**查看HTTPS客户端是否配置成功。

```
[HUAWEI] display ssl policy
      SSL Policy Name: policy1
          PKI domain: domain_name
    Policy Applicants: HTTP-CLIENT
        Key-pair Type:
 Certificate File Type:
     Certificate Type:
  Certificate Filename:
    Key-file Filename:
            CRL File:
     Trusted-CA File:
```

配置脚本

```
#
ssl policy policy1
 pki-domain domain1
#
```

```
http
 client ssl-policy policy1
 client ssl-verify peer
#
pki realm domain1
#
return
```


16 Keychain 配置

Keychain本身只对加密和认证的Key进行管理，只有在被应用程序使用时，Keychain才能发挥作用。

16.1 Keychain 简介

定义

Keychain即“钥匙串”，形象地说，当应用程序不断地变换自己的加密锁时，就需要不同的钥匙，才能打开。

Keychain中的Key，不是算法，也不是密钥，而是一套加密和认证的规则。keychain通过对它拥有的一系列Key进行集中控制和灵活管理，为应用程序提供动态的安全认证服务。

目的

RIP、IS-IS、OSPF、BGP等应用程序在和对端进行会话之前，需要首先建立传输层的连接。

为了保证应用程序会话连接和交互数据的安全性，可以对报文进行MD5算法的认证，但MD5认证存在如下缺点：

- MD5算法相对简单，无法满足安全性要求高的网络。
- 考虑到密钥安全，应定期更换密钥。MD5算法和密钥直接在应用程序中配置，与应用程序之间是一对一的静态绑定。因此，需要分别在两端设备的多个应用程序上逐个进行手动更换。

为了替代MD5，Keychain定义了应用程序认证的Key的集合：

- Keychain中的每个Key中可以灵活挑选相对MD5更安全的算法，后续还能扩展选择更安全的算法。
- Keychain中的每个Key拥有独立的算法、密钥和活跃时间。两端设备的应用程序使用了Keychain认证，即会匹配多个Key。因此可以根据Key的活跃时间实现在两端设备的多个应用程序上定期自动更换认证算法和密钥。
- Keychain中的Key在进行动态更换时，不需要断开重连正在使用的传输层连接，可以始终保持应用程序会话连接的稳定性，不会中断业务。

16.2 Keychain 原理描述

16.2.1 Keychain 的基本概念

Keychain拥有一系列的加密和认证的规则Key，即Key的集合。

Key 的三要素

Keychain中的每个Key包含三个要素：

- 认证算法：支持MD5、SHA-1、HMAC-MD5、HMAC-SHA1-12、HMAC-SHA1-20、HMAC-SHA-256、SHA-256、SM3、HMAC-SHA-384、HMAC-SHA-512算法。
- 认证密钥：一段用于加密的字符串。同一明文信息使用不同的密钥加密，会得到不同的密文；只有使用同一个密钥加密，才会得到相同的密文。
- Key的活跃时间：代表了这个Key生效的时间段，当一个Key没有处于活跃时间时，会由另一个活跃的Key来替代。

说明

使用认证算法和密钥对报文进行加密计算，会得到一串长度固定的信息摘要字符串，即Message Authentication Code（信息认证码，简称MAC）。

Key 的 ID 和分类

为了对设备中的Key的集合进行管理，Keychain定义了Key的ID以便进行区分。而设备中的Key分为发送Key和接收Key两类：

- 发送Key：用于设备在发送报文前进行加密。
- 接收Key：用于设备在接收报文后进行解密。

说明

- 本设备的发送Key需要与对端设备的接收Key一致，这样才能在对端设备上使用同种算法和同个密钥来解密收到的加密报文。
- 设备上的发送Key和接收Key可以是同一个，也可以不是。在某一时间段，使用哪个Key进行发送加密只取决于哪个Key当前正处于发送活跃时间，使用哪个Key进行接收解密只取决于哪个Key当前正处于接收活跃时间。

Key 的活跃时间

为了对设备中的Key的集合进行控制，即决定哪个Key是当前生效的Key，生效时间段是多久，哪个Key是接下来准备用来替代的Key，Keychain定义了Key的活跃时间。

Key的活跃时间代表了这个Key生效的时间段：

- 某个Key处于发送活跃时间，即为当前生效的发送Key。
- 某个Key处于接收活跃时间，即为当前生效的接收Key。

不论是发送还是接收活跃时间，都可以采用两种时间模式来进行定义：

- 绝对时间模式：表示Keychain中的Key只能在一个指定的时间段内生效，例如2019年12月10日的12:00-18:00。
- 周期时间模式：如表16-1所示，表示Keychain中的Key可以周期性地在一个指定的时间段内生效。

表 16-1 周期时间模式

周期	时间段
每日	每日的指定时间，例如12:00-18:00。
每周	每周的指定周几，例如周一、周三、周五、周日。
每月	每月的指定日期，例如3号到8号。
每年	每年的指定月份，例如六月到九月。

说明

- 缺省发送Key：如果在某个时间段内没有活跃的发送Key，此时设备发送的报文将无法进行加密，无法为应用程序提供安全认证服务。为避免这种情况，设备支持配置缺省发送Key，在某个时间段内没有其他活跃的发送Key时生效。
- 接收容忍时间：当对端设备的发送Key进行更换时，本端设备的接收Key也必须同步进行对应更换，否则本端设备接收到的报文会因为无法解密而丢包。两端设备在同时更换Key时，由于报文传输的过程存在一个时间差，本端更换新Key后可能才接收到对端使用老Key加密的报文。同时，还考虑到网络中两端设备的时钟可能出现不同步的情况，设备支持配置接收容忍时间，保证在更换Key时有一个平滑的时间过渡。接收容忍时间只对接收Key生效，配置以后，接收Key的真实活跃时间=接收容忍时间+Key原来的活跃时间+接收容忍时间。即，对接收key的启动和结束时间都将会进行相应的延长。

Key 的集合

Keychain是Key的集合，相同类型的多个Key可以放到1个集合中，称为1条Keychain。

这里的相同类型，一般指的是Key的活跃时间的模式。例如每年指定月份活跃的Key和每月指定日期活跃的key就不属于相同类型，因为把这2个Key放在1条Keychain中，无法进行时间上的切换。

根据业务需求，设备支持配套多条Keychain，提供给多个应用程序选择使用。

例如表16-2中的6条Key，Key1、Key3属于相同类型，可以放到1个集合KeychainA中；Key2、Key4属于相同类型，可以放到1个集合KeychainB中；Key5只能单独放到1个集合KeychainC中；Key6只能单独放到1个集合KeychainD中。

表 16-2 Key 的集合示例

Key	认证算法	认证密钥（加密字符串）	活跃时间	Key的集合
Key1	HMAC-SHA1-20	AbCdEfGh	2019年12月10日12:00-15:00	KeychainA
Key2	HMAC-SHA1-20	HgFeDcBa	每周一、周三、周五、周日	KeychainB
Key3	HMAC-SHA-256	AcEgHfDb	2019年12月10日15:00-18:00	KeychainA
Key4	HMAC-SHA-256	HeBgDfCa	每周二、周四、周六	KeychainB
Key5	HMAC-SHA-256	DhAgBfCe	每月3号到8号	KeychainC
Key6	HMAC-SHA-256	EaHgBcFd	每年六月到九月	KeychainD

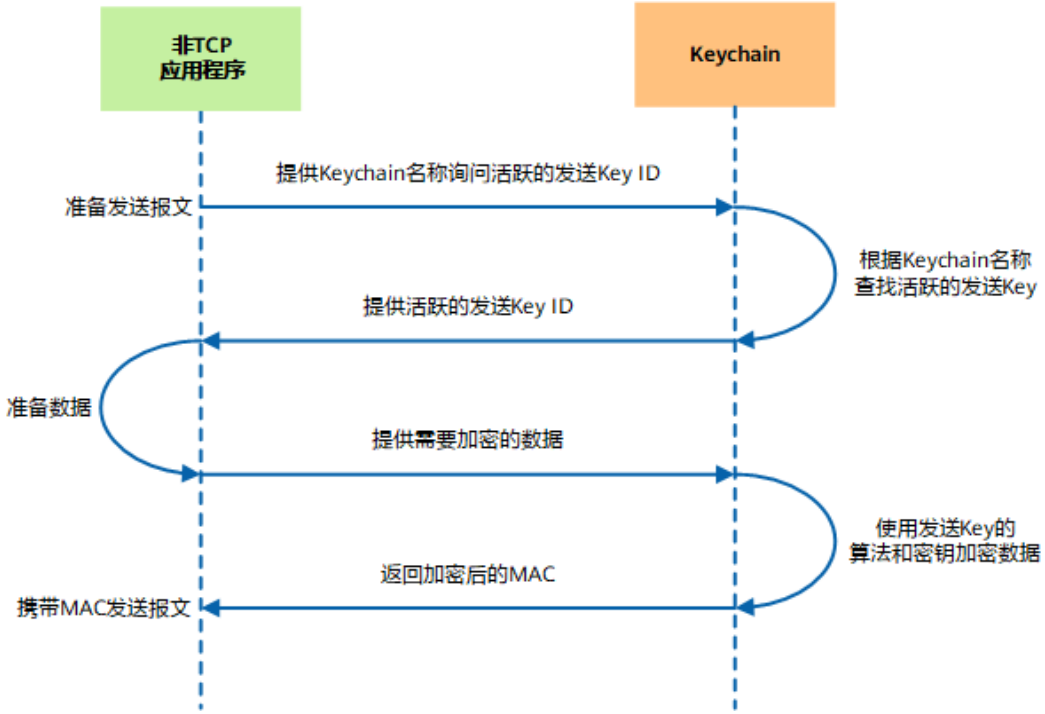
16.2.2 Keychain 的实现原理（非 TCP）

Keychain本身只对加密和认证的Key进行管理，只有在被应用程序使用时，Keychain才能发挥作用。

应用程序在使用Keychain认证时，是通过绑定一条Keychain来实现，例如绑定KeychainA，则可以使用这条Keychain中的Key集合来进行加密和解密。

加密过程

图 16-1 非 TCP 应用程序使用 Keychain 认证的加密过程

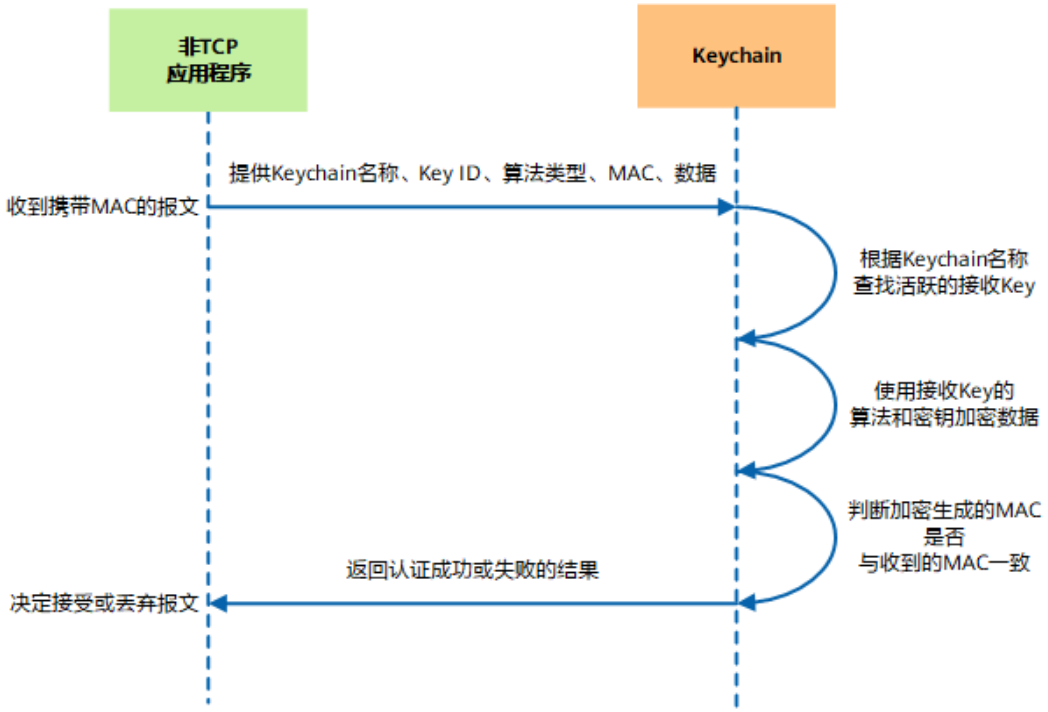


说明

如果应用程序向Keychain询问未获得活跃的发送Key，应用程序在发送报文时将无法使用Keychain认证，即不做加密正常发送。

解密过程

图 16-2 非 TCP 应用程序使用 Keychain 认证的解密过程



说明

- 解密过程并非解开密码，而是重新加密后判断新的加密结果与收到的老的解密结果是否一致，一致则表示可以正确解密。
- 特别地，当IS-IS使用Keychain认证时，解密过程中IS-IS不向Keychain提供Key ID，Keychain会查找所有活跃的接收key，找一个算法相同的进行解密。

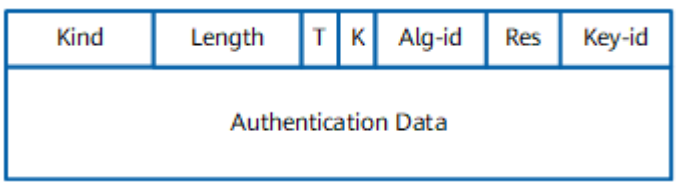
16.2.3 Keychain 的实现原理（TCP）

TCP应用程序使用Keychain认证的原理与非TCP应用程序类似，只是增加了TCP增强认证选项。

TCP 增强认证选项

TCP增强认证选项的格式如图16-3所示，TCP报文头中会携带此认证选项，专门用于为TCP连接提供认证保护。

图 16-3 TCP 增强认证选项的格式



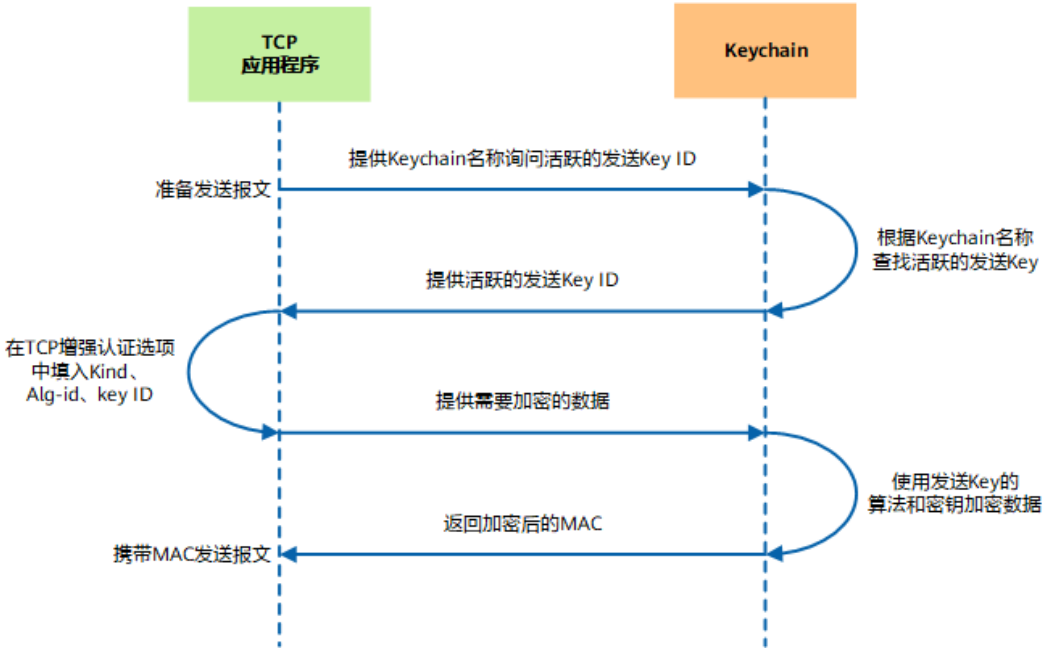
- Kind：8个比特，用于标识此选项的类型，由IANA分配。

- Length：8个比特，用于标识此选项的总长度。
- T：1个比特，用于标识此选项是否被包含在TCP增强认证计算的对象中，0表示包含，默认值是0。
- K：1个比特，为以后预留，当前值是0。
- Alg-id：6个比特，用于标识TCP增强认证的算法。
- Res：2个比特，为以后预留，当前值是0。
- Key-id：6个比特，用于标识Keychain认证的Key。
- Authentication Data：长度可变，至少包含TCP增强认证计算的结果。

由于IANA没有统一定义Kind和Alg-id字段的取值，各设备商使用不同的取值。为了使不同厂商的设备能够互通，Keychain支持配置TCP Kind和TCP algrithm-id。

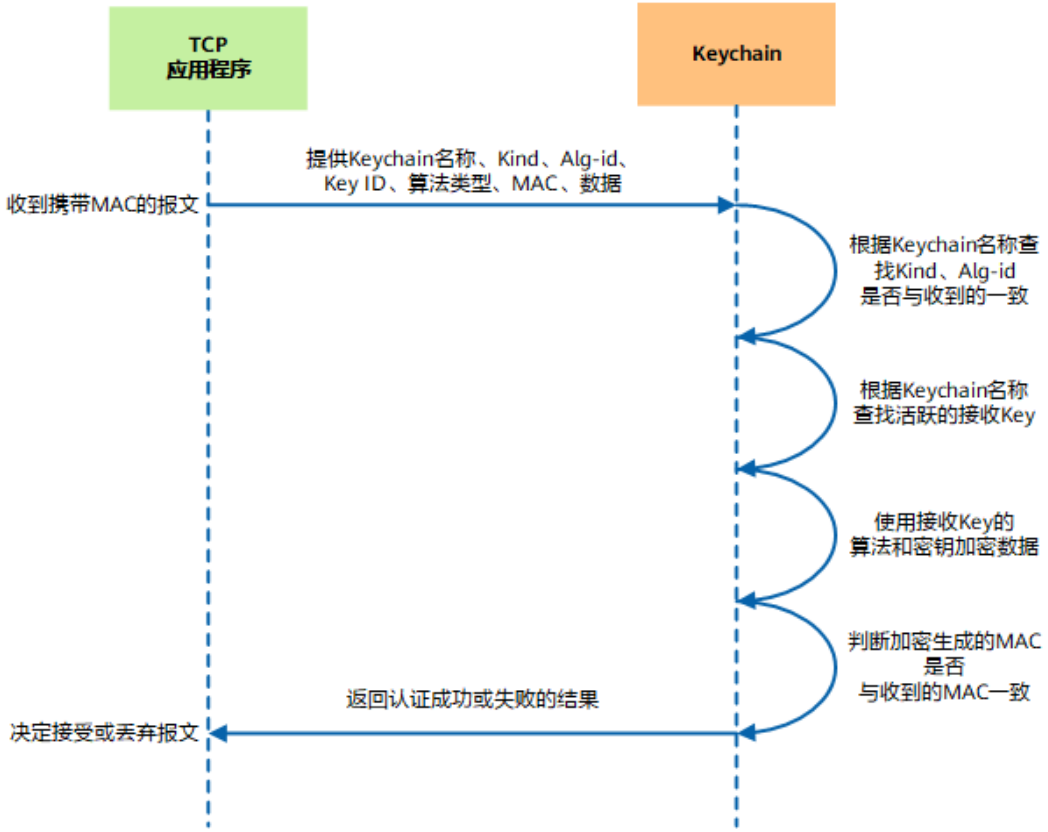
加密过程

图 16-4 TCP 应用程序使用 Keychain 认证的加密过程



解密过程

图 16-5 TCP 应用程序使用 Keychain 认证的解密过程



16.3 Keychain 配置注意事项

License 依赖

Keychain无需License许可即可使用。

硬件依赖

表 16-3 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR8000 series	AR8140-12G10XG/AR8700-8
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2

特性限制

无

16.4 Keychain 缺省配置

Keychain的缺省配置如表16-4所示。

表 16-4 Keychain 缺省配置

参数	缺省值
认证算法加密后的摘要长度	HMAC-SHA-256：32字节 SHA-256：32字节 HMAC-SHA1-20：20字节
接收容忍时间	0：不容忍
TCP增强认证选项中的类型值：TCP Kind	254
TCP认证的算法ID：TCP algorithm-id	HMAC-SHA1-12：2 MD5：3 SHA-1：4 HMAC-MD5：5 HMAC-SHA1-20：6 HMAC-SHA-256：7 SHA-256：8 SM3：9 HMAC-SHA-384：11 HMAC-SHA-512：12
时间格式	LMT（当地平均时间，Local Mean Time）

16.5 配置 Keychain

16.5.1 创建 Keychain

前提条件

在配置Keychain任务之前，需要提前完成NTP配置，保证发送端和接收端时间一致。

背景信息

配置Keychain首先需要创建Keychain，可以根据需要创建1条或多条Keychain。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 创建Keychain，并进入Keychain视图。

```
keychain keychain-name mode { absolute | periodic { daily | weekly | monthly | yearly }
```

创建Keychain时，时间模式是必配的。Keychain创建成功后，再进入Keychain视图，时间模式可以不用指定，即可以直接输入**keychain** *Keychain-name*去进入已创建的Keychain的视图。

步骤3 （可选）配置Keychain的接收容忍时间。

```
receive-tolerance { value | infinite | seconds secvalue }
```

建议配置接收容忍时间，避免因时钟抖动造成丢包。

配置容忍时间可以采用两种方式：

- 指定一个具体的时间，单位是分钟或秒，其中分钟的最大值是14400分钟（10天），秒的最大值是864000秒（十天）。缺省情况下，接收容忍时间均是0，即不容忍。所以，建议配置接收容忍时间，避免因时钟抖动造成丢包。
- 配置**infinite**，容忍时间为无限大，即Key-id的接收永久生效。

步骤4 （可选）配置Keychain的时间格式：LMT（当地平均时间，Local Mean Time）或者UTC（通用协调时间，Universal Time Coordinated）。

```
time mode { lmt | utc }
```

缺省情况下，Keychain的时间格式是LMT。

步骤5 在TCP的应用程序中使用Keychain，还需要配置TCP增强认证选项中的类型值（TCP Kind）和TCP认证的算法ID（TCP algrithm-id）。在非TCP的应用程序中使用Keychain，则不需要配置此步骤。

```
tcp-kind kind-value
tcp-algorithm-id { md5 | sha-1 | hmac-md5 | hmac-sha1-12 | hmac-sha1-20 | hmac-sha-256 | sha-256 | sm3 | hmac-sha-384 | hmac-sha-512 } algorithm-id
```

说明

为了保证更好的安全性，建议不要使用MD5和SHA-1算法。

步骤6 退出Keychain视图。

```
quit
```

----结束

16.5.2 配置 Keychain 中的 Key

背景信息

创建Keychain以后，需要创建Keychain中的Key并对其进行配置，可以根据需要在每条Keychain中创建1个或多个Key。

操作步骤

步骤1 进入系统视图。

```
system-view
```


步骤2 进入已创建的Keychain视图。

keychain *keychain-name*

步骤3 创建Key，并进入Key视图。

key-id *key-id*

步骤4 配置Key的认证算法。

algorithm { **md5** | **sha-1** | **hmac-md5** | **hmac-sha1-12** | **hmac-sha1-20** | **hmac-sha-256** | **sha-256** | **sm3** | **hmac-sha-384** | **hmac-sha-512** }

说明

为了保证更好的安全性，建议不要使用MD5和SHA-1算法。

此命令中的**md5**、**sha-1**、**hmac-md5**、**hmac-sha1-12**和**hmac-sha1-20**参数需要安装弱安全算法/协议特性包后才能使用。

出于安全性考虑，不建议使用该特性提供的弱安全算法或弱安全协议。如果确实需要使用，请执行命令**install feature-software WEAKEA**安装弱安全算法/协议特性包WEAKEA。设备默认自带弱安全算法/协议特性包WEAKEA，特性包安装或卸载的详细步骤请参见《配置指南-系统管理 配置》中的“升级维护配置”。

步骤5 配置Key的认证密钥（加密字符串）。

key-string { *plain-cipher-text* | **plain** *plain-text* | **cipher** *plain-cipher-text* }

说明

为了保证更好的安全性，建议使用**cipher**类型，在查看配置文件时，配置的密钥会以密文方式显示。

步骤6 配置Key的发送活跃时间，如表16-5所示，需要根据已配置的Keychain的时间模式来进行对应的配置。

Key的活跃时间，依赖时钟同步。

表 16-5 配置 Key 的发送活跃时间

Keychain的时间模式	Key的发送活跃时间的配置命令
绝对时间模式：**absolute**	**send-time** *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } }
周期时间模式（每天）：**periodic daily**	**send-time daily** *start-time* **to** *end-time*
周期时间模式（每周）：**periodic weekly**	**send-time day** { *start-day* **to** *end-day* | *start-day &<1-7>* }
周期时间模式（每月）：**periodic monthly**	**send-time date** { *start-date* **to** *end-date* | *start-date &<1-31>* }
周期时间模式（每年）：**periodic yearly**	**send-time month** { *start-month* **to** *end-month* | *start-month &<1-12>* }

步骤7 配置Key的接收活跃时间，如表16-6所示，需要根据已配置的Keychain的时间模式来进行对应的配置。

Key的活跃时间，依赖时钟同步。

表 16-6 配置 Key 的接收活跃时间

Keychain的时间模式	Key的接收活跃时间的配置命令
绝对时间模式：**absolute**	**receive-time** *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } }
周期时间模式（每天）：**periodic daily**	**receive-time daily** *start-time* **to** *end-time*
周期时间模式（每周）：**periodic weekly**	**receive-time day** { *start-day* **to** *end-day* | *start-day &<1-7>* }
周期时间模式（每月）：**periodic monthly**	**receive-time date** { *start-date* **to** *end-date* | *start-date &<1-31>* }
周期时间模式（每年）：**periodic yearly**	**receive-time month** { *start-month* **to** *end-month* | *start-month &<1-12>* }

步骤8 （可选）配置该key为缺省发送key。

```
default send-key-id
```

每条Keychain中只能存在1个缺省的发送key。

步骤9 （可选）配置认证算法加密后的摘要长度。

```
digest-length { hmac-sha1-20 | hmac-sha-256 | sha-256 } length
```

缺省情况下，认证算法加密后的摘要长度是：

- HMAC-SHA1-20：20字节
- HMAC-SHA-256：32字节
- SHA-256：32字节

步骤10 退出Key视图。

```
quit
```

步骤11 退出Keychain视图。

```
quit
```

----结束

16.5.3 使用 Keychain

背景信息

Keychain本身只对加密和认证的Key进行管理，只有在被应用程序使用时，Keychain才能发挥作用。如表16-7所示，在这些应用程序中可以使用Keychain。

表 16-7 在应用程序中使用 Keychain

传输层协议	应用程序	视图	生效范围	配置参考章节
非TCP	RIP	接口视图	接口	IP路由配置>RIP配置>提升RIP网络安全性>配置RIP-2报文的认证方式
	IS-IS/IS-ISv6	IS-IS视图	IS-IS区域	IP路由配置>IS-IS配置>配置IS-IS认证 IP路由配置>IS-ISv6配置>配置IPv6 IS-IS认证
		IS-IS视图	IS-IS路由域	
		接口视图	接口	
	OSPF/OSPFv3	OSPF区域视图	OSPF区域	IP路由配置>OSPF配置>配置OSPF认证 IP路由配置>OSPFv3配置>配置OSPFv3认证
		接口	接口	
		OSPF区域视图	虚连接	
TCP	BGP/BGP4+	BGP视图及相关视图	对等体或对等体组	IP路由配置>BGP配置>配置BGP认证>配置Keychain认证 IP路由配置>BGP4+配置>配置BGP4+认证

下面以RIP为例，介绍使用Keychain的配置。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 进入接口视图。

```
interface interface-type interface-number
```

步骤3 将接口从二层模式切换到三层模式。

```
undo portswitch
```

请用户根据实际接口类型自行选择是否要执行此步骤。

步骤4 配置RIP使用Keychain认证。

```
rip authentication-mode md5 nonstandard keychain keychain-name
```

步骤5 退出接口视图。

```
quit
```

----结束

16.5.4 检查 Keychain 配置结果

操作步骤

- 执行命令**display keychain** *keychain-name*，查看Keychain的配置信息。
- 执行命令**display keychain** *keychain-name* **key-id** *key-id*，查看Keychain中key的配置信息。

----结束

16.5.5 举例：配置 IS-IS 使用 Keychain 认证

组网需求

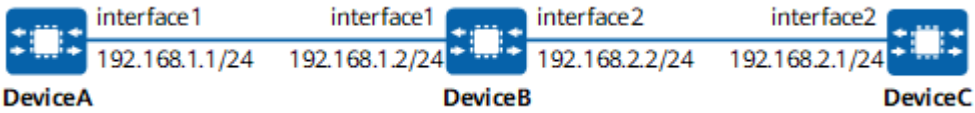
如图16-6所示，网络中DeviceA、DeviceB和DeviceC通过IS-IS实现互通。

为了确保IS-IS连接的稳定和安全，配置Keychain为IS-IS提供动态的安全认证服务。

图 16-6 Keychain 组网图

说明

本例中interface1，interface2分别代表10GE0/0/1，10GE0/0/2。



配置本例，需要准备以下数据：

- IS-IS进程号
- IS-IS进程的NET（网络实体名称，Network Entity Title）
- Keychain名称
- Keychain的接收容忍时间
- Keychain中Key的ID
- Key的认证算法和认证密钥（加密字符串）
- Key的活跃发送时间和活跃接收时间

配置注意事项

- 配置本例前，需要提前完成NTP配置。
- 使用Keychain认证的两端之间的配置需要对应，以DeviceA和DeviceB为例：
  - DeviceA和DeviceB配置的Keychain名称需要相同。
  - DeviceA和DeviceB配置的Keychain的时间模式需要相同。
  - DeviceA和DeviceB配置的Keychain的Key的ID需要相同。配置多个Key时，两端都需要配置相同ID的多个Key。
  - 对于同一个Key，DeviceA和DeviceB配置的认证算法和认证密钥（加密字符串）需要相同。

  - 对于同一个Key，DeviceA和DeviceB配置的活跃发送时间和接收活跃时间需要对应。例如，DeviceB的活跃接收时间至少需要包含DeviceA的活跃发送时间，以避免丢包。反之亦然。
- 如果Keychain中配置多个Key时，其中只能有1个Key配置为缺省发送key。

配置思路

1. 配置IS-IS。
2. 创建Keychain。
3. 配置Keychain中的Key，以及Key-id的认证算法为hmac-sha-256。
4. 配置IS-IS使用Keychain认证。

操作步骤

步骤1 配置IS-IS。

配置DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] isis 1
[DeviceA-isis-1] is-level level-1
[DeviceA-isis-1] network-entity 10.0000.0000.0001.00
[DeviceA-isis-1] quit
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] undo portswitch
[DeviceA-10GE0/0/1] ip address 192.168.1.1 24
[DeviceA-10GE0/0/1] isis enable 1
[DeviceA-10GE0/0/1] quit
```

配置DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] isis 1
[DeviceB-isis-1] is-level level-1
[DeviceB-isis-1] network-entity 10.0000.0000.0002.00
[DeviceB-isis-1] quit
[DeviceB] interface 10ge 0/0/1

[DeviceB-10GE0/0/1] ip address 192.168.1.2 24
[DeviceB-10GE0/0/1] isis enable 1
[DeviceB-10GE0/0/1] quit
[DeviceB] interface 10ge 0/0/2
[DeviceB-10GE0/0/2] ip address 192.168.2.2 24
[DeviceB-10GE0/0/2] isis enable 1
[DeviceB-10GE0/0/2] quit
```

配置DeviceC。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] isis 1
[DeviceC-isis-1] is-level level-1
[DeviceC-isis-1] network-entity 10.0000.0000.0003.00
[DeviceC-isis-1] quit
[DeviceC] interface 10ge 0/0/2
[DeviceC-10GE0/0/2] ip address 192.168.2.1 24
[DeviceC-10GE0/0/2] isis enable 1
[DeviceC-10GE0/0/2] quit
```

步骤2 创建Keychain。

配置DeviceA。

```
[DeviceA] keychain huawei mode absolute
[DeviceA-keychain-huawei] receive-tolerance 10
[DeviceA-keychain-huawei] quit
```

配置DeviceB。

```
[DeviceB] keychain huawei mode absolute
[DeviceB-keychain-huawei] receive-tolerance 10
[DeviceB-keychain-huawei] quit
```

配置DeviceC。

```
[DeviceC] keychain huawei mode absolute
[DeviceC-keychain-huawei] receive-tolerance 10
[DeviceC-keychain-huawei] quit
```

步骤3 配置Keychain中的Key。

配置DeviceA。

```
[DeviceA] keychain huawei
[DeviceA-keychain-huawei] key-id 1
[DeviceA-keychain-huawei-keyid-1] algorithm hmac-sha-256
[DeviceA-keychain-huawei-keyid-1] key-string cipher YsHsjx_202206
[DeviceA-keychain-huawei-keyid-1] send-time 12:00 2019-12-10 to 18:00 2019-12-10
[DeviceA-keychain-huawei-keyid-1] receive-time 12:00 2019-12-10 to 18:00 2019-12-10
[DeviceA-keychain-huawei-keyid-1] default send-key-id
[DeviceA-keychain-huawei-keyid-1] quit
[DeviceA-keychain-huawei] quit
```

配置DeviceB。

```
[DeviceB] keychain huawei
[DeviceB-keychain-huawei] key-id 1
[DeviceB-keychain-huawei-keyid-1] algorithm hmac-sha-256
[DeviceB-keychain-huawei-keyid-1] key-string cipher YsHsjx_202206
[DeviceB-keychain-huawei-keyid-1] send-time 12:00 2019-12-10 to 18:00 2019-12-10
[DeviceB-keychain-huawei-keyid-1] receive-time 12:00 2019-12-10 to 18:00 2019-12-10
[DeviceB-keychain-huawei-keyid-1] default send-key-id
[DeviceB-keychain-huawei-keyid-1] quit
[DeviceB-keychain-huawei] quit
```

配置DeviceC。

```
[DeviceC] keychain huawei
[DeviceC-keychain-huawei] key-id 1
[DeviceC-keychain-huawei-keyid-1] algorithm hmac-sha-256
[DeviceC-keychain-huawei-keyid-1] key-string cipher YsHsjx_202206
[DeviceC-keychain-huawei-keyid-1] send-time 12:00 2019-12-10 to 18:00 2019-12-10
[DeviceC-keychain-huawei-keyid-1] receive-time 12:00 2019-12-10 to 18:00 2019-12-10
[DeviceC-keychain-huawei-keyid-1] default send-key-id
[DeviceC-keychain-huawei-keyid-1] quit
[DeviceC-keychain-huawei] quit
```

步骤4 配置IS-IS使用Keychain认证。

配置DeviceA。

```
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] isis authentication-mode keychain huawei
[DeviceA-10GE0/0/1] quit
[DeviceA] quit
```

配置DeviceB。

```
[DeviceB] interface 10ge 0/0/1
[DeviceB-10GE0/0/1] isis authentication-mode keychain huawei
[DeviceB-10GE0/0/1] quit
[DeviceB] interface 10ge 0/0/2
[DeviceB-10GE0/0/2] isis authentication-mode keychain huawei
```

```
[DeviceB-10GE0/0/2] quit
[DeviceB] quit
```

配置DeviceC。

```
[DeviceC] interface 10ge 0/0/2
[DeviceC-10GE0/0/2] isis authentication-mode keychain huawei
[DeviceC-10GE0/0/2] quit
[DeviceC] quit
```

----结束

检查配置结果

以DeviceA为例查看IS-IS使用Keychain认证是否配置成功。

- 执行**display keychain** *keychain-name*，查看当前处于**Active**状态的Key-id。

```
<DeviceA> display keychain huawei
 Keychain Information:
 ----------------------
 Keychain Name             : huawei
   Timer Mode              : Absolute
   Receive Tolerance(min)  : 10
   Digest Length           : 32
   Time Zone               : LMT
   TCP Kind                : 254
   TCP Algorithm IDs       :
     HMAC-MD5              : 5
     HMAC-SHA1-12          : 2
     HMAC-SHA1-20          : 6
     MD5                   : 3
     SHA1                  : 4
     HMAC-SHA-256          : 7
     SHA-256               : 8
     SM3                   : 9
     HMAC-SHA-384          : 11
     HMAC-SHA-512          : 12
 Number of Key ID          : 1
 Active Send Key ID        : 1
 Active Receive Key ID     : 01
 Default send Key ID       : 1

 Key ID Information:
     SHA1                  : 4
     HMAC-SHA-256          : 7
     SHA-256               : 8
     SM3                   : 9
 Number of Key ID          : 1
 Active Send Key ID        : 1
 Active Receive Key ID     : 01
 Default send Key ID       : 1

 Key ID Information:
 ----------------------
 Key ID                    : 1
   Key string              : ******
   Algorithm               : HMAC-SHA-256
   SEND TIMER              :
     Start time            : 2019-12-10 12:00
     End time              : 2019-12-10 18:00
     Status                : Active
   RECEIVE TIMER           :
     Start time            : 2019-12-10 12:00
     End time              : 2019-12-10 18:00
     Status                : Active
```

- 执行**display isis lsdb verbose**查看IS-IS的链路状态数据库的详细信息。

```
<DeviceA> display isis lsdb verbose
                    Database information for ISIS(1)
```

```
                  -----------------------------------


                    Level-1 Link State Database

LSPID                 Seq Num    Checksum   HoldTime      Length   ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00* 0x0000020a 0x94e6     409           68       0/0/0
 SOURCE       0000.0000.0001.00
 NLPID        IPV4
 AREA ADDR    10
 INTF ADDR    192.168.1.1
 NBR  ID      0000.0000.0002.01  COST: 10
 IP-Internal  192.168.1.0     255.255.255.0    COST: 10

0000.0000.0002.00-00  0x00000219 0xfa60     431           95       0/0/0
 SOURCE       0000.0000.0002.00
 NLPID        IPV4
 AREA ADDR    10
 INTF ADDR    192.168.1.2
 INTF ADDR    192.168.2.2
 NBR  ID      0000.0000.0002.01  COST: 10
 NBR  ID      0000.0000.0003.01  COST: 10
 IP-Internal  192.168.1.0     255.255.255.0    COST: 10
 IP-Internal  192.168.2.0     255.255.255.0    COST: 10

0000.0000.0002.01-00  0x0000007e 0xa767     305           55       0/0/0
 SOURCE       0000.0000.0002.01
 NLPID        IPV4
 NBR  ID      0000.0000.0002.00  COST: 0
 NBR  ID      0000.0000.0001.00  COST: 0

0000.0000.0003.00-00  0x0000020c 0xd59e     322           68       0/0/0
 SOURCE       0000.0000.0003.00
 NLPID        IPV4
 AREA ADDR    10
 INTF ADDR    192.168.2.1
 NBR  ID      0000.0000.0003.01  COST: 10
 IP-Internal  192.168.2.0     255.255.255.0    COST: 10

0000.0000.0003.01-00  0x0000007e 0xcc3f     322           55       0/0/0
 SOURCE       0000.0000.0003.01
 NLPID        IPV4
 NBR  ID      0000.0000.0003.00  COST: 0
 SOURCE       0000.0000.0002.01
 NLPID        IPV4
 NBR  ID      0000.0000.0002.00  COST: 0
 NBR  ID      0000.0000.0001.00  COST: 0

0000.0000.0003.00-00  0x0000020c 0xd59e     322           68       0/0/0
 SOURCE       0000.0000.0003.00
 NLPID        IPV4
 AREA ADDR    10
 INTF ADDR    192.168.2.1
 NBR  ID      0000.0000.0003.01  COST: 10
 IP-Internal  192.168.2.0     255.255.255.0    COST: 10

0000.0000.0003.01-00  0x0000007e 0xcc3f     322           55       0/0/0
 SOURCE       0000.0000.0003.01
 NLPID        IPV4
 NBR  ID      0000.0000.0003.00  COST: 0
 NBR  ID      0000.0000.0002.00  COST: 0

Total LSP(s): 5
   *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
         ATT-Attached, P-Partition, OL-Overload
```


配置脚本

- DeviceA

```
#
sysname DeviceA
#
keychain huawei mode absolute
 receive-tolerance 10
 #
 key-id 1
  algorithm hmac-sha-256
  key-string cipher %+%#)teP2/_7j#@>|r-p:jgDgyKC%=80dRNA,;Cjwwv~%+%#
  send-time 12:00 2019-12-10 to 18:00 2019-12-10
  receive-time 12:00 2019-12-10 to 18:00 2019-12-10
  default send-key-id
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0001.00
#
#
interface 10GE0/0/1
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
 isis authentication-mode keychain huawei
#
return
```

- DeviceB

```
#
sysname DeviceB
#
keychain huawei mode absolute
 receive-tolerance 10
 #
 key-id 1
  algorithm hmac-sha-256
  key-string cipher %+%#$V_<R'XnL6F&H`P2DLn#IE7-+'~ks9~\acM<OSf)%+%#
  send-time 12:00 2019-12-10 to 18:00 2019-12-10
  receive-time 12:00 2019-12-10 to 18:00 2019-12-10
  default send-key-id
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0002.00
#
#
interface 10GE0/0/1
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
 isis authentication-mode keychain huawei
#

#
interface 10GE0/0/2
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
 isis authentication-mode keychain huawei
#
return
```

- DeviceC

```
#
sysname DeviceC
#
keychain huawei mode absolute
 receive-tolerance 10
 #
 key-id 1
```



```
 algorithm hmac-sha-256
 key-string cipher %+%#v@>@B\eP.Ruug(%b,;fS!5}]GV:rLU3(]U'zd9|>%+%#
 send-time 12:00 2019-12-10 to 18:00 2019-12-10
 receive-time 12:00 2019-12-10 to 18:00 2019-12-10
 default send-key-id
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0003.00
#
#
interface 10GE0/0/2
 ip address 192.168.2.1 255.255.255.0
 isis enable 1
 isis authentication-mode keychain huawei
#
return
```

16.5.6 举例：配置 BGP 使用 Keychain 认证

组网需求

如图16-7所示，网络中DeviceA和DeviceB通过BGP实现互通。

为了确保BGP连接的稳定和安全，配置Keychain为BGP提供动态的安全认证服务。

图 16-7 Keychain 组网图

说明

本例中interface1代表10GE0/0/1。

配置本例，需要准备以下数据：

- Keychain名称
- Keychain的接收容忍时间
- TCP增强认证选项中的类型值（TCP Kind）和TCP认证的算法ID（TCP algrithm-id）
- Keychain中Key的ID
- Key的认证算法和认证密钥（加密字符串）
- Key的活跃发送时间和活跃接收时间

配置注意事项

- 配置本例前，需要提前完成NTP和BGP配置。
- DeviceA和DeviceB配置的Keychain名称需要相同。
- DeviceA和DeviceB配置的Keychain的时间模式需要相同。
- DeviceA和DeviceB配置的Keychain的Key的ID需要相同。配置多个Key时，两端都需要配置相同ID的多个Key。
- 对于同一个Key，DeviceA和DeviceB配置的认证算法和认证密钥（加密字符串）需要相同。

- 对于同一个Key，DeviceA和DeviceB配置的活跃发送时间和接收活跃时间需要对应。例如，DeviceB的活跃接收时间至少需要包含DeviceA的活跃发送时间，以避免丢包。反之亦然。
- 如果Keychain中配置多个Key时，其中只能有1个Key配置为缺省发送key。

配置思路

1. 创建Keychain。
2. 配置Keychain中的Key，以及Key-id的认证算法为hmac-sha-256。
3. 配置BGP使用Keychain认证。

操作步骤

步骤1 创建Keychain。

配置DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] keychain huawei mode absolute
[DeviceA-keychain-huawei] receive-tolerance 10
[DeviceA-keychain-huawei] tcp-kind 182
[DeviceA-keychain-huawei] tcp-algorithm-id hmac-sha-256 17
[DeviceA-keychain-huawei] quit
```

配置DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] keychain huawei mode absolute
[DeviceB-keychain-huawei] receive-tolerance 10
[DeviceB-keychain-huawei] tcp-kind 182
[DeviceB-keychain-huawei] tcp-algorithm-id hmac-sha-256 17
[DeviceB-keychain-huawei] quit
```

步骤2 配置Keychain中的Key。

配置DeviceA。

```
[DeviceA] keychain huawei
[DeviceA-keychain-huawei] key-id 1
[DeviceA-keychain-huawei-keyid-1] algorithm hmac-sha-256
[DeviceA-keychain-huawei-keyid-1] key-string cipher YsHsjx_202207
[DeviceA-keychain-huawei-keyid-1] send-time 12:00 2019-12-10 to 15:00 2019-12-10
[DeviceA-keychain-huawei-keyid-1] receive-time 12:00 2019-12-10 to 15:00 2019-12-10
[DeviceA-keychain-huawei-keyid-1] default send-key-id
[DeviceA-keychain-huawei-keyid-1] quit
[DeviceA-keychain-huawei] key-id 2
[DeviceA-keychain-huawei-keyid-2] algorithm hmac-sha-256
[DeviceA-keychain-huawei-keyid-2] key-string cipher YsHsjx_202206
[DeviceA-keychain-huawei-keyid-2] send-time 15:05 2019-12-10 to 18:00 2019-12-10
[DeviceA-keychain-huawei-keyid-2] receive-time 15:05 2019-12-10 to 18:00 2019-12-10
[DeviceA-keychain-huawei-keyid-2] quit
[DeviceA-keychain-huawei] quit
```

配置DeviceB。

```
[DeviceB] keychain huawei
[DeviceB-keychain-huawei] key-id 1
[DeviceB-keychain-huawei-keyid-1] algorithm hmac-sha-256
[DeviceB-keychain-huawei-keyid-1] key-string cipher YsHsjx_202207
[DeviceB-keychain-huawei-keyid-1] send-time 12:00 2019-12-10 to 15:00 2019-12-10
[DeviceB-keychain-huawei-keyid-1] receive-time 12:00 2019-12-10 to 15:00 2019-12-10
[DeviceB-keychain-huawei-keyid-1] default send-key-id
```



```
[DeviceB-keychain-huawei-keyid-1] quit
[DeviceB-keychain-huawei] key-id 2
[DeviceB-keychain-huawei-keyid-2] algorithm hmac-sha-256
[DeviceB-keychain-huawei-keyid-2] key-string cipher YsHsjx_202206
[DeviceB-keychain-huawei-keyid-2] send-time 15:05 2019-12-10 to 18:00 2019-12-10
[DeviceB-keychain-huawei-keyid-2] receive-time 15:05 2019-12-10 to 18:00 2019-12-10
[DeviceB-keychain-huawei-keyid-2] quit
[DeviceB-keychain-huawei] quit
```

步骤3 配置BGP使用Keychain认证。

配置DeviceA。

```
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] ip address 192.168.1.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] bgp 1
[DeviceA-bgp] router-id 1.1.1.1
[DeviceA-bgp] peer 192.168.1.2 as-number 1
[DeviceA-bgp] peer 192.168.1.2 keychain huawei
[DeviceA-bgp] quit
[DeviceA] quit
```

配置DeviceB。

```
[DeviceB] interface 10ge 0/0/1
[DeviceB-10GE0/0/1] ip address 192.168.1.2 24
[DeviceB-10GE0/0/1] quit
[DeviceB] bgp 1
[DeviceB-bgp] router-id 2.2.2.2
[DeviceB-bgp] peer 192.168.1.1 as-number 1
[DeviceB-bgp] peer 192.168.1.1 keychain huawei
[DeviceB-bgp] quit
[DeviceB] quit
```

----结束

检查配置结果

以DeviceA为例查看BGP使用Keychain认证是否配置成功。

- 执行**display keychain** *keychain-name*，查看当前处于**Active**状态的Key-id。

```
<DeviceA> display keychain huawei
 Keychain Information:
 ----------------------
 Keychain Name             : huawei
   Timer Mode              : Absolute
   Receive Tolerance(min)  : 10
   Digest Length           : 32
   Time Zone               : LMT
   TCP Kind                : 182
   TCP Algorithm IDs       :
     HMAC-MD5              : 5
     HMAC-SHA1-12          : 2
     HMAC-SHA1-20          : 6
     MD5                   : 3
     SHA1                  : 4
     HMAC-SHA-256          : 17
     SHA-256               : 8
     SM3                   : 9
     HMAC-SHA-384          : 11
     HMAC-SHA-512          : 12
 Number of Key ID          : 2
 Active Send Key ID        : 1
 Active Receive Key ID     : 01
 Default send Key ID       : 1

 Key ID Information:
```

```
----------------------
Key ID                : 1
  Key string          : ******
  Algorithm           : HMAC-SHA-256
  SEND TIMER          :
    Start time        : 2019-12-10 12:00
    End time          : 2019-12-10 15:00
    Status            : Active
  RECEIVE TIMER       :
    Start time        : 2019-12-10 12:00
    End time          : 2019-12-10 15:00
    Status            : Active

Key ID                : 2
  Key string          : ******
  Algorithm           : HMAC-SHA-256
  SEND TIMER          :
    Start time        : 2019-12-10 15:05
    End time          : 2019-12-10 18:00
    Status            : Inactive
  RECEIVE TIMER       :
    Start time        : 2019-12-10 15:05
    End time          : 2019-12-10 18:00
    Status            : Inactive
```

- 执行**display bgp peer** *ipv4-address* **verbose**查看BGP对等体已配置的认证类型是**Keychain(huawei)**。

```
<DeviceA> display bgp peer 192.168.1.2 verbose
  BGP Peer is 192.168.1.2,  remote AS 1
  Type: IBGP link
  BGP version 4, Remote router ID 2.2.2.2
  Update-group ID: 3
  BGP current state: Established, Up for 00h27m26s
  BGP current event: RecvKeepalive
  BGP last state: OpenConfirm
  BGP Peer Up count: 2
  Received total routes: 0
  Received active routes total: 0
  Advertised total routes: 0
  Port: Local - 58168        Remote - 179
  Configured: Connect-retry Time: 32 sec
  Configured: Min Hold Time: 0 sec
  Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
  Received  : Active Hold Time: 180 sec
  Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
  Peer optional capabilities:
  Peer supports bgp multi-protocol extension
  Peer supports bgp route refresh capability
  Peer supports bgp 4-byte-as capability
  Address family IPv4 Unicast: advertised and received
Received: Total 34 messages
            Update messages              1
            Open messages                1
            KeepAlive messages           32
            Notification messages        0
            Refresh messages             0
Sent: Total 33 messages
            Update messages              1
            Open messages                1
            KeepAlive messages           31
            Notification messages        0
            Refresh messages             0
Authentication type configured: Keychain(huawei)
Last keepalive received: 2019-12-10 10:12:29+00:00
Last keepalive sent    : 2019-12-10 10:12:04+00:00
Last update    received: 2019-12-10 09:45:14+00:00
Last update    sent    : 2019-12-10 09:45:14+00:00
No refresh received since peer has been configured
No refresh sent since peer has been configured
Minimum route advertisement interval is 15 seconds
```

```
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured
```

配置脚本

- DeviceA

```
#
sysname DeviceA
#
keychain huawei mode absolute
 receive-tolerance 10
 tcp-kind 182
 tcp-algorithm-id hmac-sha-256 17
 #
 key-id 1
  algorithm hmac-sha-256
  key-string cipher %+%#1h29-c>>[H,XTu>Q}##;"}JOQOK#c>TD6>~d-BaJ%+%#
  send-time 12:00 2019-12-10 to 15:00 2019-12-10
  receive-time 12:00 2019-12-10 to 15:00 2019-12-10
  default send-key-id
 #
 key-id 2
  algorithm hmac-sha-256
  key-string cipher %+%#^<Sn.IK2iK'N%[VnMhv-I)|C4d<K$F$a.6%jEN@K%+%#
  send-time 15:05 2019-12-10 to 18:00 2019-12-10
  receive-time 15:05 2019-12-10 to 18:00 2019-12-10
#
interface 10GE0/0/1
 ip address 192.168.1.1 255.255.255.0
#
bgp 1
 router-id 1.1.1.1
 peer 192.168.1.2 as-number 1
 peer 192.168.1.2 keychain huawei
 #
 ipv4-family unicast
  peer 192.168.1.2 enable
#
return
```

- DeviceB

```
#
sysname DeviceB
#
keychain huawei mode absolute
 receive-tolerance 10
 tcp-kind 182
 tcp-algorithm-id hmac-sha-256 17
 #
 key-id 1
  algorithm hmac-sha-256
  key-string cipher %+%#p8cb/;OMFES0Wx@PY^"Ka{6q2MB;oG|[ZO-_]u}&%+%#
  send-time 12:00 2019-12-10 to 15:00 2019-12-10
  receive-time 12:00 2019-12-10 to 15:00 2019-12-10
  default send-key-id
 #
 key-id 2
  algorithm hmac-sha-256
  key-string cipher %+%#&Yq4=s*P:L<"8iG-|o1ZB*Qi0qCn%N{Y3a&Z-zuD%+%#
  send-time 15:05 2019-12-10 to 18:00 2019-12-10
  receive-time 15:05 2019-12-10 to 18:00 2019-12-10
#
interface 10GE0/0/1
 ip address 192.168.1.2 255.255.255.0
```



```
#
bgp 1
 router-id 2.2.2.2
 peer 192.168.1.1 as-number 1
 peer 192.168.1.1 keychain huawei
 #
 ipv4-family unicast
  peer 192.168.1.1 enable
#
return
```


17 ASPF/ALG 配置

17.1 ASPF/ALG 简介

ASPF 定义

ASPF（Application Specific Packet Filter，应用层的包过滤）是一种针对应用层的包过滤技术，也称为基于状态的报文过滤。

ASPF 目的

ASPF功能可以自动检测某些报文的应用层信息并根据应用层信息放开相应的访问规则（生成Server-map表）。生成的Server-map表，用于放行后续数据通道中的报文，相当于自动创建了一条精细的“安全策略”。

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

ALG 定义

ALG（Application Level Gateway，应用层网关）是一种NAT穿越技术。

ALG 目的

ALG功能用于NAT场景下自动检测某些报文的应用层信息，根据应用层信息放开相应的访问规则（生成Server-map表），并自动转换报文载荷中的IP地址和端口信息。

NAT只能转换报文头中的IP地址和端口，无法对应用层的数据进行转换。在许多应用层协议中，报文载荷中也带有地址或端口信息，如果这些数据不进行转换，可能导致后续通信异常。

ASPF 和 ALG 对比

ASPF和ALG都是对应用层报文进行处理，它们使用的是同一个配置。设备会根据是否存在NAT环境以及各个协议的特征来判断何时需要ASPF处理，何时需要ALG处理，何时配置两者同时处理。而对用户来说，只需要配置一次命令，设备会根据不同场景下对报文进行不同处理。

表 17-1 ASPF 和 ALG 功能对比

是否NAT场景	生效的功能	作用
非NAT场景	ASPF	生成Server-map表项，保证其他主机访问FTP、SIP等主机的报文能穿越设备。
NAT场景	ALG	对报文载荷中的IP地址进行地址转换。
	ASPF	生成Server-map表项（带地址转换信息），保证其他主机访问FTP、SIP等主机的报文能穿越设备。

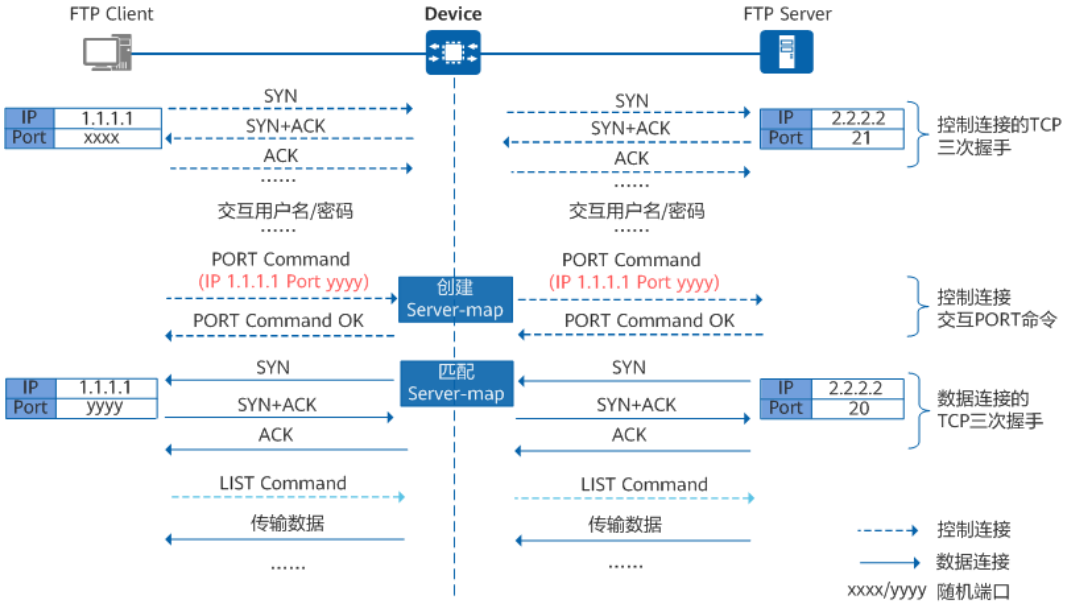
17.2 ASPF/ALG 原理描述

ASPF/ALG功能可以检测某些报文的应用层信息，并将应用层信息中的关键数据记录在Server-map表中。后续报文命中Server-map表直接放行或进行NAT，并建立会话，不受安全策略控制。

以多通道协议（如FTP、SIP等）的ASPF为例，这些多通道协议的应用通常需要建立控制通道和数据通道两个连接。控制通道建立后，通过控制通道协商后续数据通道的地址和端口，然后根据协商结果建立数据通道。设备通过动态检测协商报文的应用层携带的地址和端口信息，自动生成相应的Server-map表。后续的数据报文命中Server-map表被放行，从而成功建立数据通道。

以FTP协议的主动模式（服务器主动访问客户端）为例，设备检测PORT命令报文的应用层信息，将应用层携带的IP地址和端口记录在Server-map表中。

图 17-1 FTP 主动模式的 ASPF



在设备上查看生成的Server-map表。

```
<HUAWEI> display firewall server-map
Type: ASPF, 2.2.2.2 -> 1.1.1.1:yyyy, Zone: ---
  Protocol: tcp(Appro: ftp-data), Left-Time: 00:00:57
  VPN: public -> public
```

yyyy端口即客户端通过控制通道向服务器开放的数据端口。后续服务器（2.2.2.2）主动访问客户端（1.1.1.1）的yyyy端口数据报文由于匹配了该Server-map表而被放行。

说明

对于ASPF/ALG类型的Server-map表，只有相应的流量经过设备时，才会生成相应的Server-map表。

17.3 ASPF/ALG 配置注意事项

License 依赖

ASPF/ALG无需License许可即可使用。

硬件依赖

表 17-2 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 17-3 本特性的使用限制

特性	特性限制	系列	涉及产品
ASPF4	ALG和源NAT策略结合使用时，如果配置了多通道协议如FTP等的ALG功能，则源NAT策略中不建议指定相应的服务匹配条件，否则可能导致无法正常通信。由于数据通道的端口信息是动态协商出来的，如果源NAT策略中指定了服务，可能会导致数据报文无法命中源NAT策略，从而导致无法正常通信。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
ASPF4	ASPF/ALG功能仅可处理IPv4报文。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
ASPF4	设备仅适用于RFC标准SIP协议的ASPF/ALG，但不适用于扩展SIP协议（SIP-I和SIP-T）和GB标准等其他SIP协议的ASPF/ALG。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

特性	特性限制	系列	涉及产品
ASPF 4	ASPF和ALG功能使用相同的配置，开启其中一个，另一个功能同时生效。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8
ASPF 4	对于SIP协议，如果通信方所在的安全区域在3个及以上，则ASPF/ALG功能不生效。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG/ AR8700-8

17.4 ASPF/ALG 缺省配置

ASPF/ALG的缺省配置如表17-4所示。

表 17-4 ASPF/ALG 缺省配置

参数	缺省配置
ASPF/ALG功能	关闭。

17.5 配置 ASPF/ALG

17.5.1 了解 FTP ASPF/ALG

FTP 主动模式的 ASPF

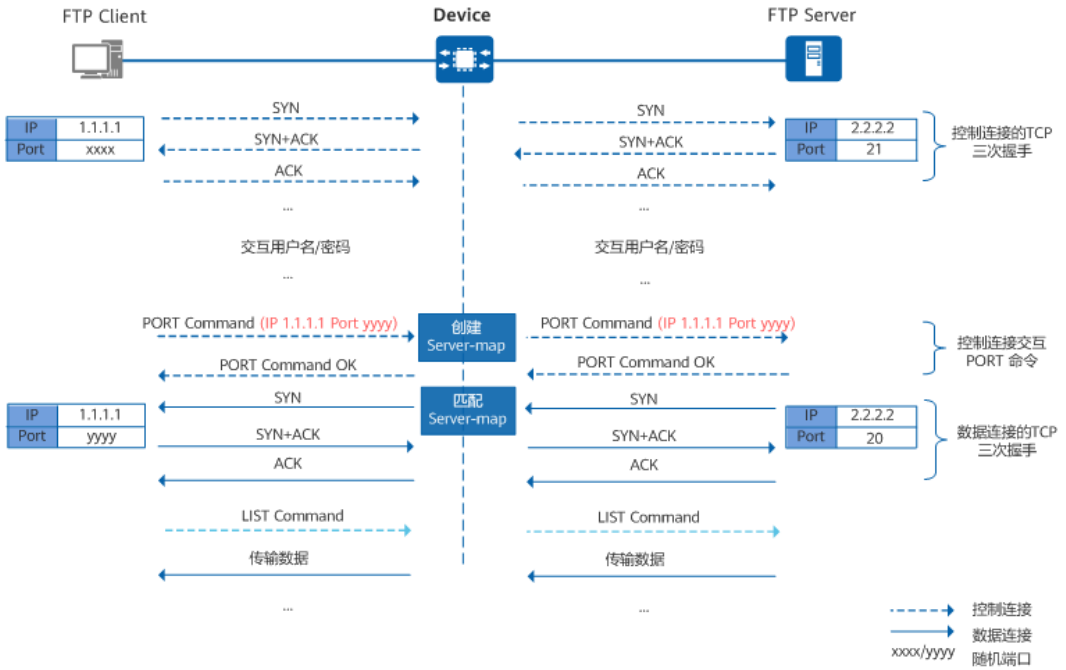
FTP主动模式下，客户端使用随机端口xxxx向服务器的21端口发起连接请求建立控制通道，然后使用PORT命令协商两者建立数据通道的端口号，协商出来的端口是yyyy。然

后服务器主动向客户端的yyyy端口发起连接请求，建立数据通道。数据通道建立成功后再进行数据传输。

在配置安全策略时，如果只配置了允许客户端访问服务器的21端口的安全策略，即控制连接能成功建立。但是当服务器访问客户端yyyy端口的报文到达设备后，对于设备来说，这个报文不是前一条连接的后续报文，而是代表着一条新的连接。要想使这个报文顺利到达FTP客户端，设备上就必须配置了安全策略允许其通过，如果没有配置服务器到客户端这个方向上的安全策略，该报文无法通过设备，导致数据通道建立失败。结果是用户能访问服务器，但无法请求数据。

如果通过安全策略解决此问题，数据通道使用的端口是在控制通道中临时协商出来的，具有随机性，无法精确预知，所以只能开放客户端的所有端口，这样就会给客户端带来安全隐患。ASPF功能正是为了解决此问题，如**图 FTP主动模式下的ASPF处理过程**所示。

图 17-2 FTP 主动模式下的 ASPF 处理过程



由于PORT命令的应用层信息中携带了客户端的IP地址和向服务器随机开放的端口，设备通过分析PORT命令的应用层信息，提前预测到后续报文的行为方式，根据应用层信息中的IP和端口创建Server-map表。服务器向客户端发起数据连接的报文到达设备后命中该Server-map表项，不再受安全策略的控制。

查看Device上生成的Server-map表。

```
<HUAWEI> display firewall server-map
Type: ASPF, 2.2.2.2 -> 1.1.1.1:yyyy, Zone: ---
  Protocol: tcp(Appro: ftp-data), Left-Time: 00:00:57
  VPN: public -> public
```

yyyy端口即客户端通过控制通道向服务器开放的数据端口。服务器（2.2.2.2）主动访问客户端（1.1.1.1）的yyyy端口的数据报文由于命中该Server-map表而被放行。

FTP 被动模式的 ASPF

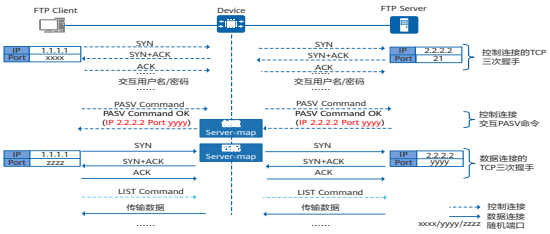
FTP被动模式（客户端主动访问服务器）下，客户端使用随机端口xxxx向服务器的21端口发起连接请求建立控制通道，然后使用PASV命令协商两者建立数据通道的端口号，

协商出来的端口是yyyy。然后客户端主动向服务器的yyyy端口发起连接请求，建立数据通道。数据通道建立成功后再进行数据传输。

在配置安全策略时，如果只配置了允许客户端访问服务器的21端口的安全策略，即控制连接能成功建立。但是当客户端访问服务器yyyy端口的报文到达设备后，对于设备来说，这个报文不是前一条连接的后续报文，而是代表着一条新的连接。要想使这个报文顺利到达服务器，设备上就必须配置了安全策略允许其通过，如果没有配置客户端到服务器的yyyy端口的安全策略，该报文无法通过设备，导致数据通道建立失败。结果是用户能访问FTP服务器，但无法请求数据。

如果通过安全策略解决此问题，数据通道使用的端口是在控制通道中临时协商出来的，具有随机性，无法精确预知，所以只能开放服务器的所有端口，这样就会给服务器带来安全隐患。ASPF功能正是为了解决此问题，如图17-3所示。

图 17-3 FTP 被动模式下的 ASPF 处理过程



由于PASV Command OK命令的应用层信息中携带了服务器的IP地址和向客户端随机开放的端口，设备通过分析PASV Command OK命令的应用层信息，提前预测到后续报文的行为方式，根据应用层信息中的IP和端口创建Server-map表。客户端向服务器发起数据连接的报文到达设备后命中该Server-map表项，不再受安全策略的控制。

查看Device上生成的Server-map表。

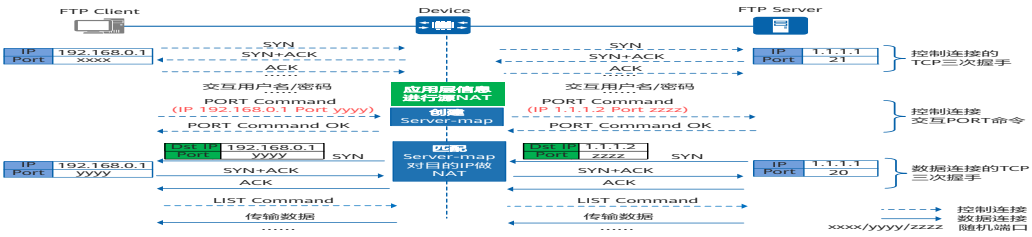
```
<HUAWEI> display firewall server-map
Type: ASPF, 1.1.1.1 -> 2.2.2.2:yyyy, Zone: ---
  Protocol: tcp(Appro: ftp-data), Left-Time: 00:00:57
  VPN: public -> public
```

yyyy端口即服务器通过控制通道向客户端开放的数据端口。客户端（1.1.1.1）主动访问服务器（2.2.2.2）的yyyy端口的数据报文由于命中该Server-map表而被放行。

FTP 主动模式的 ALG

如图17-4所示，客户端位于私网，服务器位于公网。为了使客户端能正常访问服务器，在设备上配置源NAT策略，用于将客户端的私网地址转换为公网地址，并允许端口转换。客户端和服务器经过TCP三次握手建立控制通道后，客户端通过PORT命令向服务器发送私网IP地址和开放的私网端口用于建立数据通道。

图 17-4 FTP 主动模式下的 ALG 处理过程



未配置ALG功能前，设备在进行源NAT转换时，只转换了报文头中的IP地址和端口信息。而报文载荷中携带的IP地址和端口信息并未改变。由于两者的IP地址和端口信息不一致会导致FTP功能无法正常工作。

配置了ALG功能后，设备通过分析PORT命令的应用层信息，将命令中携带的私网IP和私网端口转换成公网地址和公网端口后再转发给服务器，并创建Server-map表。服务器向转换后的公网地址和公网端口发起数据连接，报文到达设备后命中该Server-map表项，自动将目的地址和端口转换为真实的私网地址，不再受安全策略控制。

说明

NAT只能转换报文的传输层信息，ALG功能可以转换报文的应用层信息。

配置了ALG的情况下，设备上只需配置允许从客户端的任意端口到服务器的21端口的安全策略即可。

查看Device上生成的Server-map表。

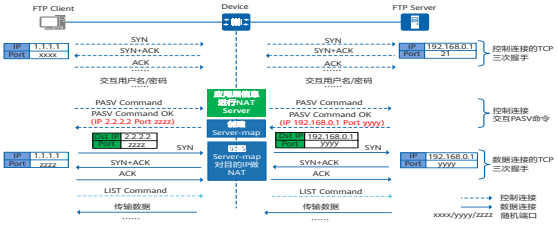
```
<HUAWEI> display firewall server-map
Type: ASPF, 1.1.1.1 -> 1.1.1.2:zzzz[192.168.0.1:yyyy], Zone: ---
  Protocol: tcp(Appro: ftp-data), Left-Time: 00:00:57
  VPN: public -> public
```

服务器（1.1.1.1）主动访问客户端公网地址和公网端口的数据报文由于命中该Server-map表而被放行，且目的公网地址和公网端口被转换为真实的私网地址（192.168.0.1）和私网端口（yyyy）。

FTP 被动模式的 ALG

如图17-5所示，客户端位于公网，服务器位于私网。为了使客户端能正常访问服务器，在设备上配置NAT Server，用于将服务器的公网地址转换为私网地址，并允许端口转换。客户端和服务器经过TCP三次握手建立控制通道后，服务器通过PASV Command OK命令向客户端发送私网IP地址和开放的私网端口用于建立数据通道。

图 17-5 FTP 被动模式下的 ALG 处理过程



未配置ALG功能前，设备在进行目的NAT转换时，只转换了报文头中的IP地址和端口信息。而报文载荷中携带的IP地址和端口信息并未改变。由于两者的IP地址和端口信息不一致会导致FTP功能无法正常工作。

配置了ALG功能后，设备通过分析PASV Command OK命令的应用层信息，将命令中携带的私网IP和私网端口转换成公网地址和公网端口后再转发给客户端，并创建Server-map表。客户端向转换后的公网地址和公网端口发起数据连接，报文到达设备后命中该Server-map表项，自动将目的地址和端口转换为真实的私网地址，不再受安全策略控制。

配置了ALG的情况下，设备上只需配置允许从客户端的任意端口到服务器的21端口的安全策略即可。

说明

NAT只能转换报文的传输层信息，ALG功能可以转换报文的应用层信息。

配置了ALG的情况下，设备上只需配置允许从客户端的任意端口到服务器的21端口的安全策略即可。

查看Device上生成的Server-map表。

```
<HUAWEI> display firewall server-map
Type: ASPF, 1.1.1.1 -> 2.2.2.2:zzzz[192.168.0.1:yyyy], Zone: ---
  Protocol: tcp(Appro: ftp-data), Left-Time: 00:00:57
  VPN: public -> public
```

客户端（1.1.1.1）主动访问服务器公网地址和公网端口的数据报文由于命中该Server-map表而被放行，且目的公网地址和公网端口被转换为真实的私网地址（192.168.0.1）和私网端口（yyyy）。

17.5.2 了解 PPTP ALG

PPTP（Point-to-Point Tunneling Protocol，点对点隧道协议）是在PPP协议基础上开发的一种新的增强型安全协议，是实现VPN（Virtual Private Network，虚拟专用网）的方式之一。

PPTP协议是一种多通道协议，PPTP使用TCP创建控制通道来发送控制命令，使用GRE来封装数据包以在数据通道中发送数据。

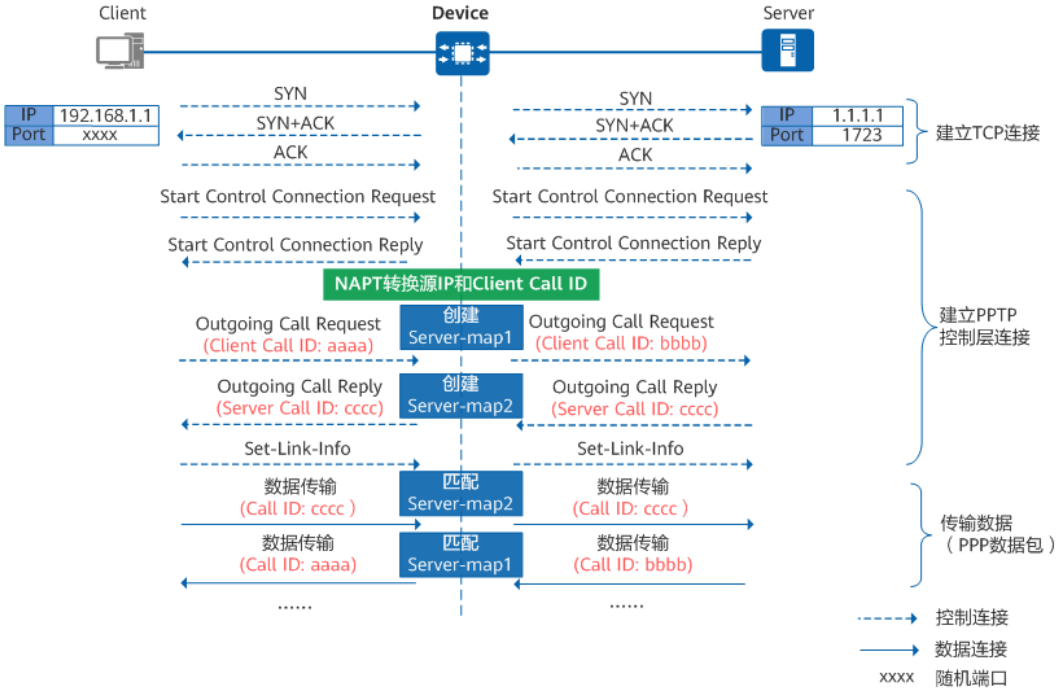
PPTP采用客户端/服务器模式，PPTP客户端首先和PPTP服务器建立一条TCP连接，然后在该TCP连接上建立PPTP控制层连接，之后的PPP数据包通过GRE封装后在隧道中传输。PPTP ALG场景下客户端和服务器的关键交互流程如图17-6所示。

在同时转换源IP和源端口的NAT场景下，客户端和服务器之间的通信可能会出现异常。PPTP采用GRE封装数据包，而GRE头中是没有端口信息的，NAT只能识别并转换客户端的源IP信息，当内网有多个客户端和同一个服务器交互时，设备收到服务器的回应报文时，仅通过目的公网地址无法区分应该发送给哪个客户端从而导致丢包。

另一方面，PPTP是基于GRE头部中的源IP和Call ID来区分隧道的，由于不同的客户端之间是没有协商的，所以它们可能会携带相同的Call ID。经过NAT转换源IP后，不同的客户端对应了相同的公网地址和Call ID，导致隧道建立失败。

因此在同时转换源IP和源端口的NAT场景（NAPT）下，需要在设备上开启PPTP ALG功能，转换源IP的同时转换Call ID，并为后续的数据传输开辟“隐形通道”（创建Server-map）。如果没有这个“隐形通道”，在精细的安全策略控制下（仅允许从客户端到服务器的1723端口的报文通过），数据报文将会被阻断。

图 17-6 PPTP ALG



1. 客户端和服务器先通过三次握手建立TCP连接，设备上生成对应的控制连接会话。客户端的IP地址192.168.1.1经过源NAT转换为1.1.1.2，端口xxxx转换为yyyy。
2. 客户端和服务器在TCP连接基础上继续建立PPTP控制层连接，报文匹配控制连接会话被放行。
   a. 客户端在Outgoing Call Request报文中携带了本端的Call ID，经过设备时进行源IP和Call ID转换后发送给服务器，同时创建**Server-map1**。

      ```
      <HUAWEI> display firewall server-map aspf
      Type: ASPF, 1.1.1.1 -> 1.1.1.2:bbbb[192.168.1.1:aaaa], Zone: ---
        Protocol: tcp(Appro: pptp-gre), Left-Time: 00:03:09
        VPN: public -> public
      ```

      由此Server-map可知，客户端的IP地址由192.168.1.1转换为1.1.1.2，客户端的Call ID由aaaa转换为bbbb。

b. 服务器在对应的Outgoing Call Reply报文中携带了本端的Call ID，经过设备时进行目的IP转换后发送给相应的客户端，同时创建**Server-map2**。服务器端的Call ID相当于“目的端口”，在源NAT场景下是不需要转换“目的端口”的，所以此时设备不会转换服务器的Call ID。

```
<HUAWEI> display firewall server-map aspf
Type: ASPF, 192.168.1.1[1.1.1.2] -> 1.1.1.1:cccc, Zone: ---
  Protocol: tcp(Appro: pptp-gre), Left-Time: 00:03:09
  VPN: public -> public
```

由此Server-map可知，服务器的Call ID为cccc。

3. 客户端和服务器通过隧道传输数据。每对客户端和服务器交换数据包时都会生成2条隧道，1条隧道是为了从客户端到服务器方向的通信，1条隧道是为了从服务器到客户端方向的通信。

   当客户端到服务器方向的数据到达设备时，命中**Server-map2**，将源地址转换为公网地址1.1.1.2，然后放行该报文并创建会话，不再受安全策略的控制。

   当服务器到客户端方向的数据到达设备时，命中**Server-map1**，将目的地址转换为客户端的真实IP地址192.168.1.1，Call ID也转换为真实的Call ID，然后放行该报文并创建会话，不再受安全策略的控制。

17.5.3 了解 SIP ASPF/ALG

SIP（Session Initiation Protocol，会话发起协议）是一个IETF标准协议，用于创建、修改和释放一个或多个参与者的会话，这些会话可以是语音通话、多媒体会议或虚拟现实等多媒体元素的交互用户会话。

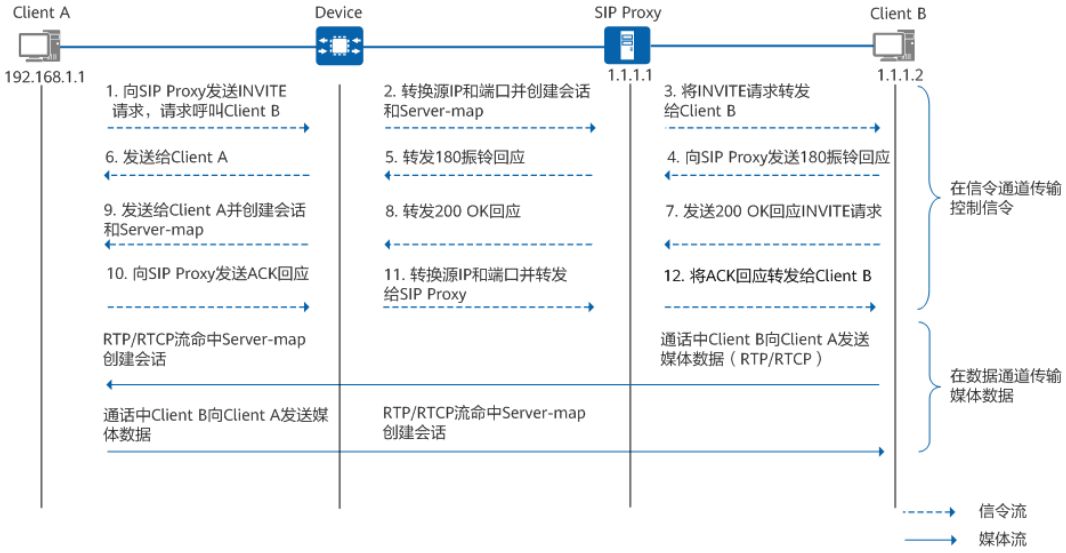
SIP是一种多通道协议，呼叫双方除了建立信令通道用于传输信令外，还会建立数据通道用于传输语音、视频等媒体数据。因此SIP流量分为信令流和媒体流。信令流通过UDP或TCP传输，包括呼叫双方的请求和响应报文。媒体流通过RTP和RTCP传输，包括语音或视频等媒体数据报文。

SIP可以采用UDP 5060端口或者TCP 5060端口（非加密）/5061端口（TLS加密）来传输信令流，为了使信令流能顺利通过设备，需要在设备上配置一条安全策略允许SIP信令流量通过。但是，媒体流采用动态协商的端口传输，由于端口号无法提前预知，管理员无法通过配置精细的安全策略控制媒体流的转发。

另一方面，NAT场景下，NAT只能转换报文网络层的IP地址和传输层的端口，无法转换应用层中的IP地址和端口信息，导致后续的信令流和媒体流交互无法正常进行。此时，需要在设备上开启SIP ASPF/ALG功能，检测并转换报文应用层信息中携带的IP和端口信息，并记录在Server-map中，媒体数据报文经过设备时命中Server-map而被放行，不再受安全策略控制。

如图17-7所示，以Client A位于内网，Client B和SIP Proxy位于外网的源NAT场景为例，介绍Client A、ClientB和SIP Proxy之间的关键交互流程以及设备开启ASPF/ALG功能后对报文的处理。

图 17-7 SIP ASPF/ALG



1. Client A向SIP Proxy的5060端口发送INVITE请求，请求呼叫Client B。INVITE请求的消息头中Via字段包含发送者的地址信息（假设为192.168.1.1:2000），消息体中包含由SDP（Session Description Protocol，会话描述协议）描述的媒体控制信息（Connection Information和Media Description字段指示的自身的IP地址和端口），表示告诉对方后续将媒体流发往该地址和端口，此处假设为192.168.1.1:3000。
2. Device收到INVITE请求报文，转换IP地址和端口号后转发给SIP Proxy并创建信令通道会话，同时分别根据INVITE消息中消息头和消息体中的IP地址和端口创建Server-map，用于放行后续的交互报文。

   说明

   Device会根据消息体中的媒体连接地址创建2个Server-map，分别用于放行RTP流和RTCP流。RTCP流使用的端口号 = RTP流端口号+1。

   ```
   <HUAWEI> display firewall server-map aspf
   Type: ASPF, ANY -> 1.1.1.10:2222[192.168.1.1:2000], Zone: ---
     Protocol: udp(Appro: sip), Left-Time: 00:02:00
     VPN: public -> public

   Type: ASPF, ANY -> 1.1.1.10:3333[192.168.1.1:3000], Zone: ---
     Protocol: udp(Appro: sip-rtp), Left-Time: 00:00:50
     VPN: public -> public

   Type: ASPF, ANY -> 1.1.1.10:3334[192.168.1.1:3001], Zone: ---
     Protocol: udp(Appro: sip-rtcp), Left-Time: 00:00:50
     VPN: public -> public
   ```

   Device为信令流创建了1个Server-map（第1个Server-map），用于放行后续由Client B发送给Client A的信令数据。同时，还为数据流创建了2个Server-map（第2和3个Server-map），用于放行后续Client B向Client A发送的媒体数据。
3. SIP Proxy将INVITE请求转发给Client B，请求Client B加入通话，并通过该INVITE消息携带Client A的会话描述给Client B。
4. Client B振铃，并向SIP Proxy发送180振铃回应。
5. SIP Proxy转发180振铃回应。
6. Device收到180振铃回应，命中信令通道会话，将报文目的地址转换为Client A的真实IP地址和端口然后转发给Client A，Client A听回铃音。

7. Client B接听电话，Client B向SIP Proxy发送200 OK回应，表示SIP Proxy发过来的INVITE请求已经被成功接收并处理。消息头中Via字段包含发送者的地址信息（假设为1.1.1.2:3000），消息体中包含由SDP（Session Description Protocol，会话描述协议）描述的媒体控制信息（Connection Information和Media Description字段指示的自身的IP地址和端口），表示告诉对方后续将媒体流发往该地址和端口，此处假设为1.1.1.2:4000。
8. SIP Proxy转发200 OK回应，表示INVITE请求已被成功接收并处理，并通过该消息携带Client B的会话描述。
9. Device收到200 OK回应，将报文目的地址转换为Client A的真实IP地址和端口然后转发给Client A。同时分别根据200 OK消息中消息头和消息体中的IP地址和端口创建Server-map，用于放行后续的交互报文。

   说明

   Device会根据消息体中的媒体连接地址创建2个Server-map，分别用于放行RTP流和RTCP流。RTCP流使用的端口号 = RTP流端口号+1。

   ```
   <HUAWEI> display firewall server-map aspf
   Type: ASPF, ANY -> 1.1.1.2:3000, Zone: ---
     Protocol: udp(Appro: sip), Left-Time: 00:02:00
     VPN: public -> public

   Type: ASPF, ANY -> 1.1.1.2:4000, Zone: ---
     Protocol: udp(Appro: sip-rtp), Left-Time: 00:00:50
     VPN: public -> public

   Type: ASPF, ANY -> 1.1.1.2:4001, Zone: ---
     Protocol: udp(Appro: sip-rtcp), Left-Time: 00:00:50
     VPN: public -> public
   ```

   此处仅展示该阶段Device上创建的Server-map。

   Device为信令流创建了1个Server-map（第1个Server-map），用于放行后续由Client A发送给Client B的信令数据。同时，还为数据流创建了2个Server-map（第2和3个Server-map），用于放行后续Client A向Client B发送的媒体数据。
10. Client A向SIP Proxy发送ACK消息，表示已经收到SIP Proxy对INVITE请求的最终响应。
11. Device收到ACK消息，转换IP地址和端口号后转发给SIP Proxy。
12. SIP Proxy将ACK消息转发给Client B，表示已经收到Client B对于INVITE请求的最终响应。此时，主被叫双方都知道了对方的媒体连接地址，可以启动通话。
13. Client A和Client B通话中，媒体流命中Server-map，Device分别为Client A到Client B的方向和Client B到Client A的方向创建RTP会话和RTCP会话。

17.5.4 配置 ASPF/ALG

背景信息

为了简化配置，ASPF和ALG功能使用的是同一个配置命令，无须重复配置。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 配置ASPF/ALG功能。

```
firewall detect protocol
```

配置时请注意以下几点：

- 如果需要对多种协议的流量进行ASPF/ALG处理，重复执行该命令。
- **firewall detect sip**命令配置的针对SIP协议的ASPF/ALG功能仅对基于UDP协议的SIP流量生效。
- 请根据实际使用需求开启对应协议类型的ASPF/ALG功能，对于不需要开启ASPF/ALG功能的协议类型请及时关闭此功能。

----结束

检查配置结果

执行命令**display firewall detect global**，查看ASPF/ALG的配置信息。

17.5.5 举例：配置 FTP 协议的 ASPF

组网需求

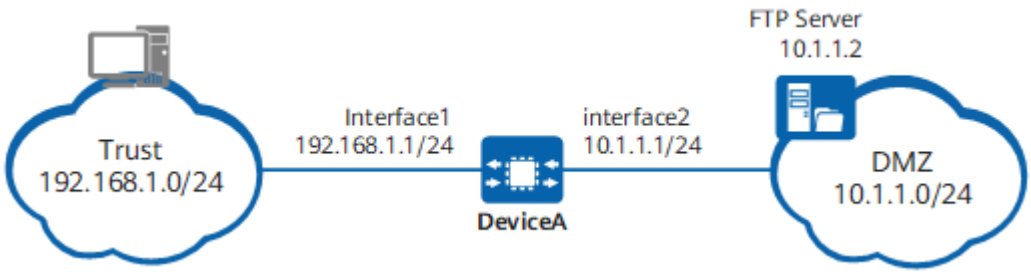
如图17-8所示，DeviceA部署在某公司的出口，公司提供FTP服务。

为了使内网用户能正常访问FTP服务器，除了配置安全策略允许内网用户和FTP服务器之间建立控制连接外，还需要开启FTP协议的ASPF，保证内网用户和FTP服务器之间数据连接的成功建立。

图 17-8 配置 ASPF 组网图

说明

本图中interface1、interface2分别代表10GE0/0/1、10GE0/0/2。



项目	数据	说明
10GE0/0/1	IP地址：192.168.1.1 安全区域：Trust	该接口与员工PC相连，与员工PC位于同一网段。
10GE0/0/2	IP地址：10.1.1.1 安全区域：DMZ	该接口与服务器相连，与服务器位于同一网段。
用户地址范围	192.168.1.0/24	将所有员工PC的IP地址划为这个网段，并且部署于Trust区域。
FTP服务器	10.1.1.2/24	将服务器部署于DMZ区域。

配置思路

1. 配置接口IP地址和安全区域，完成网络基本参数配置。
2. 配置安全策略，允许内网用户访问FTP服务器。
3. 配置ASPF，实现FTP报文的正常转发。

操作步骤

步骤1 配置各个接口的IP，并划入相应的安全区域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] undo portswitch
[DeviceA-10GE0/0/1] ip address 192.168.1.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] undo portswitch
[DeviceA-10GE0/0/2] ip address 10.1.1.1 24
[DeviceA-10GE0/0/2] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/1
[DeviceA-zone-trust] quit
[DeviceA] firewall zone dmz
[DeviceA-zone-dmz] add interface 10ge 0/0/2
[DeviceA-zone-dmz] quit
```

步骤2 配置安全策略，允许内网用户访问FTP服务器。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec_ftp
[DeviceA-policy-security-rule-policy_sec_ftp] source-zone trust
[DeviceA-policy-security-rule-policy_sec_ftp] source-address 192.168.1.0 24
[DeviceA-policy-security-rule-policy_sec_ftp] destination-zone dmz
[DeviceA-policy-security-rule-policy_sec_ftp] destination-address 10.1.1.2 32
[DeviceA-policy-security-rule-policy_sec_ftp] service protocol tcp destination-port 21
[DeviceA-policy-security-rule-policy_sec_ftp] action permit
[DeviceA-policy-security-rule-policy_sec_ftp] quit
```

说明

为了保护FTP服务器，建议安全策略中配置精细的匹配条件，只允许内网用户访问FTP服务器的21号端口。此例中FTP服务器采用知名端口（TCP 21）提供FTP服务。

步骤3 应用**firewall detect ftp**，实现FTP报文的正常转发。

```
[DeviceA] firewall detect ftp
```

----结束

检查配置结果

- 内网用户正常访问FTP服务器。
- 在DeviceA上执行命令**display session all**查看会话表。

```
<DeviceA> display session all
 Session Table Information:
   Protocol          : 6(TCP)
   SrcAddr  Port Vpn : 192.168.1.2 2051
   DestAddr Port Vpn : 10.1.1.2 21
   Time To Live      : 60s

   Protocol          : 6(TCP)
   SrcAddr  Port Vpn : 10.1.1.2 20
   DestAddr Port Vpn : 192.168.1.2 2052
   Time To Live      : 60s
```

```
Total : 2
```

配置脚本

以下仅给出与本案例有关的脚本。

```
#
 sysname DeviceA
#
interface 10GE0/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface 10GE0/0/2
 ip address 10.1.1.1 255.255.255.0
#
 firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface 10GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface 10GE0/0/2
#
security-policy
 rule name policy_sec_ftp
  source-zone trust
  destination-zone dmz
  source-address 192.168.1.0 24
  destination-address 10.1.1.2 32
  service protocol tcp destination-port 21
  action permit
#
 firewall detect ftp
#
return
```

17.5.6 举例：配置 SIP 协议的 ALG

组网需求

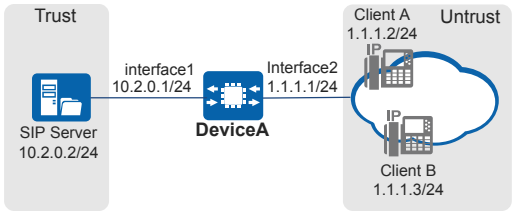
如图17-9所示，某企业内部部署了一台SIP服务器。每个SIP客户端上线时都需要向SIP服务器发送注册消息，这些消息均是承载在SIP协议之上。

设备部署在SIP客户端和SIP服务器之间，对传输的SIP消息进行NAT ALG处理。

图 17-9 配置 SIP 的 ALG

说明

本例中interface1、interface2分别代表10GE0/0/1、10GE0/0/2。



项目	数据	说明
10GE0/0/1	IP地址：10.2.0.1 安全区域：Trust	该接口与服务器相连，与服务器位于同一网段。

项目	数据	说明
10GE0/0/2	IP地址：1.1.1.1 安全区域：Untrust	该接口与客户端相连，与客户端位于同一网段。
SIP服务器	10.2.0.2/24	将服务器部署于DMZ区域。

配置思路

1. 配置接口IP地址和安全区域，完成网络基本参数配置。
2. 配置安全策略，允许SIP客户端和SIP服务器之间互相通信。
3. 配置目的NAT，使私网的SIP服务器能够对外提供服务（公网地址：1.1.1.10）。
4. 配置ALG，实现SIP报文的正常转发。

操作步骤

步骤1 配置各个接口的IP，并加入相应的安全区域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 0/0/1
[DeviceA-10GE0/0/1] undo portswitch
[DeviceA-10GE0/0/1] ip address 10.2.0.1 24
[DeviceA-10GE0/0/1] quit
[DeviceA] interface 10ge 0/0/2
[DeviceA-10GE0/0/2] undo portswitch
[DeviceA-10GE0/0/2] ip address 1.1.1.1 24
[DeviceA-10GE0/0/2] quit
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface 10ge 0/0/1
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface 10ge 0/0/2
[DeviceA-zone-untrust] quit
```

步骤2 配置安全策略，允许SIP客户端向SIP服务器发送消息。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name policy_sec1
[DeviceA-policy-security-rule-policy_sec1] source-zone untrust
[DeviceA-policy-security-rule-policy_sec1] destination-zone trust
[DeviceA-policy-security-rule-policy_sec1] source-address 1.1.1.0 24
[DeviceA-policy-security-rule-policy_sec1] destination-address 10.2.0.2 32
[DeviceA-policy-security-rule-policy_sec1] service protocol tcp destination-port 5060
[DeviceA-policy-security-rule-policy_sec1] service protocol udp destination-port 5060
[DeviceA-policy-security-rule-policy_sec1] action permit
[DeviceA-policy-security-rule-policy_sec1] quit
```

步骤3 配置目的NAT，使私网的SIP服务器能够对外提供服务。

```
[DeviceA] nat server policy_sip protocol tcp global 1.1.1.10 5060 inside 10.2.0.2 5060
[DeviceA] nat server policy_sip protocol udp global 1.1.1.10 5060 inside 10.2.0.2 5060
```

步骤4 配置ALG，实现SIP报文的正常转发。

```
[DeviceA] firewall detect sip
```

----结束

检查配置结果

- Client A和Client B在服务器上注册成功。
- 在DeviceA上执行命令**display session all**查看会话表。

```
<DeviceA> display session all
 Session Table Information:
   Protocol          : 17(UDP)
   SrcAddr  Port Vpn : 1.1.1.2 2107
   DestAddr Port Vpn : 1.1.1.10 5060
   Time To Live      : 60s
   NAT Info
     New SrcAddr     : -
     New SrcPort     : -
     New DestAddr    : 10.2.0.2
     New DestPort    : 5060

   Protocol          : 17(UDP)
   SrcAddr  Port Vpn : 1.1.1.3 4936
   DestAddr Port Vpn : 1.1.1.10 5060
   Time To Live      : 60s
   NAT Info
     New SrcAddr     : -
     New SrcPort     : -
     New DestAddr    : 10.2.0.2
     New DestPort    : 5060

 Total : 2
```

配置脚本

以下仅给出与本案例有关的脚本。

```
#
 sysname DeviceA
#
interface 10GE0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface 10GE0/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface 10GE0/0/1
#
 firewall zone untrust
 set priority 5
 add interface 10GE0/0/2
#
firewall detect sip
#
security-policy
 rule name policy_sec1
  source-zone untrust
  destination-zone trust
  source-address 1.1.1.0 mask 255.255.255.0
  destination-address 10.2.0.2 mask 255.255.255.255
  service protocol tcp destination-port 5060
  service protocol udp destination-port 5060
  action permit
#
 nat server policy_sip protocol tcp global 1.1.1.10 5060 inside 10.2.0.2 5060
 nat server policy_sip protocol udp global 1.1.1.10 5060 inside 10.2.0.2 5060
#
return
```


18 ASE 配置

当前资料中的ASE为基础软件包支持的能力，基础软件包中默认包含，不支持卸载。该特性支持升级，如需升级，请登录华为技术支持网站，在软件下载专区中搜索对应产品和版本，下载ASE特性包。特性包的安装升级步骤请参见《配置指南-系统管理配置》中的“升级维护配置"。

18.1 ASE 简介

定义

ASE（Adaptive Security Engine，自适应安全引擎）是一个高性能的内容安全一体化检测引擎，用于对报文进行各种内容安全检测和过滤的集成处理。

目的

当前设备支持入侵防御（IPS）、反病毒（AV）和URL过滤等各种报文内容检测和过滤的功能。在内容安全引擎出现之前，各业务模块分别对报文进行内容检测和过滤，报文每经过一个业务模块就要进行一次内容检测，非常消耗设备性能。

ASE将内容安全相关的业务功能集成在一起，对报文进行一体化检测和处理，只需对报文进行一次检测就能完成多种内容安全功能的处理，各业务模块间并行处理，大大提升了设备性能。

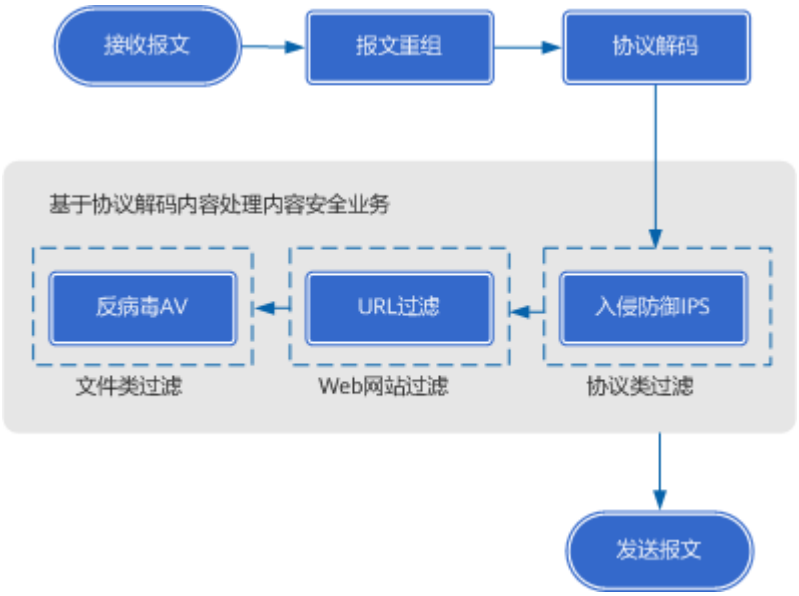
18.2 ASE 原理描述

ASE 报文处理流程

如果流量匹配的策略中配置了内容安全相关的业务，则需要将报文上送到ASE进行内容安全检测和处理。

内容安全检测和处理涉及一系列处理过程，如图18-1所示。

图 18-1 ASE 报文处理流程



1. 业务报文上送到ASE后，首先需要进行分片重组和流重组，保证后续业务模块处理的报文是顺序的、无重叠的。
2. 识别出协议后，设备对协议进行深度解码。此阶段一次性解析出后续内容安全业务所需的字段或文件，极大提高了检测效率。
3. 根据用户配置的内容安全业务进行相应的处理。

说明

不同业务检测的对象不同，比如AV检测文件、URL过滤检测URL，因此业务处理没有严格的先后顺序，图中仅示意大概的业务分类。

ASE 特性范围

当前ASE支持的特性如表18-1所示。

表 18-1 ASE 特性范围

特性名称	描述
入侵防御（IPS）	入侵防御是一种基于攻击特征库检测入侵行为，并采取一定响应措施实时中止入侵的安全机制。

特性名称	描述
反病毒（AV）	反病毒（Antivirus）是一种基于病毒特征检测和处理病毒文件的安全机制，可以有效避免病毒文件引起的数据破坏、权限更改和系统崩溃等情况的发生，保证了网络的安全。
URL过滤	URL过滤是指对用户的URL访问请求进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的。

18.3 ASE 配置注意事项

License 依赖

ASE无需License许可即可使用，ASE相关业务特性的License依赖情况请参考各业务特性的配置指南。

硬件依赖

表 18-2 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 18-3 本特性的使用限制

特性限制	系列	涉及产品
ASE引擎的HTTP协议解码仅可对HTTP1.0/HTTP1.1版本进行协议解码，不能对HTTP2.0版本进行协议解码；因此相关的内容安全特性均不可对HTTP2.0版本的协议版本进行检测，包括入侵防御、反病毒检测等。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

特性限制	系列	涉及产品
ASE相关的配置（包括全局配置和业务特性配置）进行配置回退后，需要执行engine configuration commit命令提交配置，否则配置不生效。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8
对于上送到ASE的流量，如果策略已决后安全策略配置发生了变更， 不会在引擎上进行策略重查，只有新建流量会按照新的策略进行处理。	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2 AR8140-12G10XG/AR8700-8

18.4 ASE 缺省配置

ASE的缺省配置如表18-4所示。

表 18-4 ASE 缺省配置

参数	缺省配置
ASE Bypass状态	关闭
ASE过载时的处理动作	转发报文
ASE增强模式	对RTSP协议采用增强检测模式，对除RTSP之外的其他协议采用普通检测模式。
ASE引擎通透模式	关闭
ASE业务模块日志生成功能	开启

18.5 调整 ASE 配置

背景信息

通常情况下，ASE无需进行任何配置即可正常运行，只有在定位问题或者某些测试场景下才需要临时进行配置。

操作步骤

- 设置引擎工作模式。

表 18-5 设置引擎工作模式

操作	命令	说明
配置ASE威胁处置动作为告警	**engine action-mode warning**	缺省情况下，ASE威胁处置动作未配置为告警模式。 使用该命令后，ASE威胁处置动作配置为告警模式，即内容安全业务在流量中检测到威胁，也无法进行阻断，只会生成相关日志。
手动将ASE设置为Bypass或Stop状态	**engine** { **bypass** | **stop** } [**slot** *slot-id* **cpu** *cpu-id*]	正常情况下，如果不需要使用ASE相关的业务特性，取消相关特性配置即可，不建议通过该命令进行配置，该命令仅在特定的故障排除场景中使用。 ● **bypass**：需要进行内容安全检测的流量不会上送ASE处理，直接转发。 ● **stop**：所有报文不再经过ASE处理，ASE上承载的业务均无法进行。
设置ASE工作在增强检测模式	**engine enhanced-detection**	如果业务量较大，希望提升设备的安全检测能力，且能接受一定程度的检测速率降低，可以开启增强检测模式。
配置ASE内容安全业务的分流模式	**engine deliver mode** { **round-robin** | **source-ip-hash** }	结合现网流量模型和ASE的实际使用情况调整分流模式。

- 设置报文重组

表 18-6 设置报文重组

操作	命令	说明
配置TCP报文乱序场景下流重组时单条流的最大缓存	**stream-reassemble session-cache** *session-cache-value*	在严重乱序场景或来回路径不一致的场景下，配置流重组时单条流的缓存规格。

操作	命令	说明
配置TCP乱序检测的超时时间	**stream-reassemble session-timeout** *session-timeout*	只有TCP乱序时间小于等于*session-timeout*时，ASE才会尝试重组流量；当TCP乱序时间大于*session-timeout*，且配置了ASE过载时的处理动作为转发报文时，则ASE不再对该条流量做检测，优先保证业务传输。

----结束

后续处理

- 执行**display debugging**命令，查看ASE各业务模块的调试开关状态。

18.6 维护 ASE

查看统计信息

表 18-7 查看统计信息

操作	命令
查看引擎会话统计信息	**display engine session statistics**
查看引擎会话表详细内容	**display engine session table**

清除统计信息

表 18-8 清除统计信息

操作	命令
清除引擎会话表信息	**reset engine session table**

19 HIPS 配置

19.1 HIPS 简介

定义

主机入侵防御系统（HIPS，Host-based Intrusion Prevention System）用于监控本机系统是否被入侵和感染。与IPS不同，IPS是对经过设备的流量进行分析和处理，以保护内网的设备和用户，而HIPS旨在保护设备自身的系统。

目的

网络设备是重要的ICT基础设施，网络设备的安全直接关系到整个基础网络的安全。网络设备通常部署在服务器和终端用户之前，所以非常容易成为黑客攻击和入侵的目标。入侵成功后，黑客可以通过该设备进一步渗透到网络内部。HIPS监控设备操作系统，一旦发现疑似入侵和感染的事件立即发送日志，提示管理员执行隔离和防护处理，避免设备被进一步的入侵甚至危害其他设备的安全。

19.2 HIPS 原理描述

黑客入侵设备底层操作系统后会对系统进行配置和调整，以便长期控制设备和进一步渗透。HIPS实时监控设备底层操作系统，提供如**表19-1**所示的检测模块，一旦发现可疑事件，立即发送对应日志。

表 19-1 HIPS 检测模块说明

检测模块名称	说明
文件提权检测	添加可执行文件的SUID/SGID权限位后，即使后续用普通用户登录也可以执行高危的命令。HIPS检测到可执行文件被添加SUID/SGID权限位时会发送相关日志。
异常shell检测	黑客入侵成功后可能对设备已有的shell进行修改，方便后续建立反弹shell的控制通道。HIPS检测到shell被修改时会发送相关日志。
rootkit检测	rootkit是黑客在攻击时用来隐藏自己的踪迹和保留root访问权限的工具。HIPS检测到设备中存在符合rootkit特征的系统文件时会发送相关日志。
关键文件篡改检测	黑客入侵成功后可能会修改关键文件或者留下恶意文件。HIPS检测到设备中关键文件被篡改或者关键路径中出现可疑文件时会发送相关日志。
非法root用户检测	UID是用户身份标识，UID 0是保留给root用户的，设备中出现UID为0的非root帐号是十分可疑的。HIPS检测到设备中出现UID为0的非root帐号时会发送相关日志。

19.3 HIPS 配置注意事项

License 依赖

HIPS无需License许可即可使用。

硬件依赖

表 19-2 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

无

19.4 HIPS 缺省配置

HIPS的缺省配置如表19-3所示。

表 19-3 HIPS 缺省配置

参数	缺省配置
主机入侵防御系统（HIPS功能总开关）	启用
文件提权检测模块	启用
异常shell检测模块	启用
rootkit检测模块	启用
关键文件篡改检测模块	启用
非法root用户检测模块	启用

19.5 启用 HIPS

背景信息

开启主机入侵防御系统后，各检测模块的配置和启用情况由HIPS策略文件决定，设备上无法修改策略文件内容，缺省情况下各检测模块全部启用。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 启用主机入侵防御系统。

```
hips enable
```

----结束

检查配置结果

在任意视图下执行命令**display hips state**，查看HIPS各检测模块的启用情况。

20 FIPS 配置

20.1 FIPS 简介

定义

联邦信息处理标准（Federal Information Processing Standards，FIPS）是由美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）发布的一种针对密码模块的安全需求标准。设备支持FIPS 140-2，即该标准目前的最新版本，本文档中的FIPS即表示FIPS 140-2。

目的

FIPS规定了一个安全系统中的密码模块应该满足的安全性要求，以确保该模块保护的信息的机密性和完整性。通过部署FIPS，保证设备通过FIPS认证，能够提高设备的安全性。

20.2 FIPS 配置注意事项

License 依赖

FIPS无需License许可即可使用。

硬件依赖

表 20-1 支持本特性的硬件

系列	支持产品
AR5700 series	AR5710-H8T2TS1

系列	支持产品
AR6700 series	AR6710-L26T2X4/AR6710-L50T2X4/AR6710-L8T3TS1X2
AR8000 series	AR8140-12G10XG/AR8700-8

特性限制

表 20-2 本特性的使用限制

特性限制	系列	涉及产品
FIPS模式切换是重启后生效	AR5700 series AR6700 series AR8000 series	AR5710-H8T2TS1 AR6710-L26T2X4/ AR6710-L50T2X4/ AR6710-L8T3TS1X2 AR8140-12G10XG /AR8700-8

20.3 开启 FIPS 模式

背景信息

FIPS模式下的设备将具有更为严格的安全性要求，并会对密码模块使用的算法是否符合FIPS标准进行自检，以确保密码模块处于正常的运行状态。

说明

切换FIPS模式会清空设备下次启动使用的配置文件，并立即重启设备，请谨慎使用。

开启FIPS模式后，设备可以安装弱安全算法/协议特性包，但弱安全算法/协议特性包不生效，即弱安全算法/协议仍然不可以使用。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 开启FIPS模式。

```
fips-mode enable
```

缺省情况下，设备未开启FIPS模式。

----结束

检查配置结果

- 在系统视图下执行**display fips-mode**命令，查看设备是否开启FIPS模式。

- 在系统视图下执行**display fips-mode algorithm self-check**命令，检查设备密码模块提供的算法是否符合FIPS标准。
- 在系统视图下执行**display fips-mode finite-state**命令，查看FIPS模式状态变化的历史记录。

21 GTSM 配置

21.1 GTSM 简介

定义

GTSM（通用TTL安全保护机制，Generalized TTL Security Mechanism）是一种基于TTL的安全保护机制。GTSM通过检查IP报文头中的TTL（Time To Live）值是否在预先定义的范围来确认报文合法性，丢弃非法报文，保护建立在TCP/IP基础上的控制层面协议免受CPU过载攻击。

目的

攻击者模拟真实的路由协议，对一台设备不断发送报文。设备如果无法判断报文的合法性，会因为持续处理攻击报文而异常繁忙，造成CPU过载。

针对这种情况，需要有一种方法来判断报文的合法性。GTSM就是其中的一种方法，判断依据为报文头中的TTL值。

TTL的主要作用是避免IP报文在网络中被无限循环收发。TTL的最大值为255，每经过一跳设备TTL值减1。而根据网络的规模和结构，使用路由协议的邻居设备之间报文中转的跳数是有一定范围的，设备之间接收到的报文中的TTL值也就应该在一定的范围内。

因此，根据网络情况，可以使用GTSM来预先定义邻居设备之间TTL值的范围，检查报文TTL值的合理性，判断报文的合法性，过滤非法的攻击报文。

原理

如**图21-1**所示：

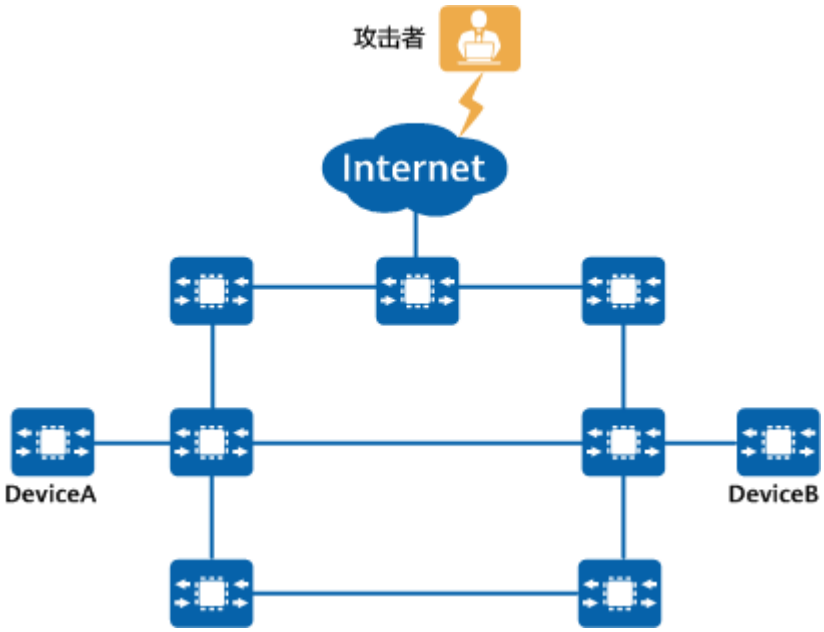
- 所有设备之间建立IGP连接。
- DeviceA和DeviceB之间建立BGP连接。

- 攻击者从Internet远端接入，模拟BGP协议，对DeviceA或DeviceB不断发送报文。

DeviceA和DeviceB之间进行BGP对等体协商时，可以选择3条路径进行转发，报文经过的中间设备跳数（包含到达设备的最后1跳）可能为3跳、5跳、6跳，即最多6跳。

使用GTSM来预先定义TTL值的范围为[255-6+1，255]，即[250，255]。TTL值不在此范围内的远端BGP攻击报文被认定为非法报文，直接丢弃。

图 21-1 GTSM 防攻击原理图



在复杂的网络中，TTL值的范围判断也会相对复杂。但是，根据网络情况，还是可以定义一个大致的合理范围，通过GSTM过滤很大一部分范围外的非法攻击报文。

21.2 使能 GTSM

背景信息

设备使能GTSM之前，协议报文直接上送控制层面。对于某个协议使能GTSM之后：

- 协议报文匹配GTSM的策略：检查报文中的TTL值。如在允许范围内，则上送控制层面；如不在范围内，则丢弃。
- 协议报文未匹配GTSM的策略：缺省处理动作为通过，上送控制层面。处理动作也可以配置为丢弃，请参考**21.3 （可选）配置未匹配GTSM策略的报文的处理动作**。

如**表21-1**所示，设备支持对于这些协议使能GTSM：

表 21-1 支持 GTSM 的协议

协议	GTSM匹配策略的粒度	配置参考章节
RIP	公网或私网VPN实例	IP路由配置>RIP配置>提升RIP网络安全性>配置RIP GTSM功能

协议	GTSM匹配策略的粒度	配置参考章节
OSPF/ OSPFv3	公网或私网VPN实例	IP路由配置>OSPF配置>配置OSPF GTSM功能 IP路由配置>OSPFv3配置>配置OSPFv3 GTSM功能
BGP/ BGP4+	公网或私网VPN实例 可以精确到对等体IP地址或对等体组	IP路由配置>BGP配置>配置BGP GTSM IP路由配置>BGP4+配置>配置BGP4+ GTSM

下面以RIP为例，介绍使能RIP GTSM的配置。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 使能RIP GTSM，包括TTL值范围和匹配策略。

```
rip valid-ttl-hops valid-ttl-hops-value [ vpn-instance vpn-instance-name ]
```

说明

TTL值定义的范围是[255–*valid-ttl-hops-value*+1，255]。

----结束

检查配置结果

- 执行命令**display gtsm statistics** { *slot-id* | **all** }，查看GTSM统计信息。
- 执行命令**reset gtsm statistics** { *slot-id* | **all** }，清除GTSM统计信息。

21.3 （可选）配置未匹配 GTSM 策略的报文的处理动作

背景信息

使能GTSM以后，报文未匹配GTSM的策略，处理动作可以配置为丢弃或通过。

操作步骤

步骤1 进入系统视图。

```
system-view
```

步骤2 配置未匹配GTSM策略的报文的处理动作为丢弃或通过。

```
gtsm default-action { drop | pass }
```

说明

- 需要先使能GTSM以后，处理动作配置才能生效。
- 请确认已使能GTSM的匹配策略的配置粒度。如果粒度过小，不建议处理动作配置为丢弃，以免大量不匹配的报文被错误的丢弃。
- 处理动作配置为丢弃时，可以通过LOG信息开关，控制是否对报文被丢弃的情况记录日志，以方便故障的定位。

----结束

22 安全风险查询配置

背景信息

由于协议或者算法自身的安全性能不同，用户配置时使用的某些协议或算法可能存在安全风险。通过安全风险查询命令可查看系统中存在的安全风险配置信息，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

- 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。

- 在用户视图下，执行命令**display security configuration** [**feature** *feature-name*]，查询系统中存在的安全配置信息。

----结束

23 弱密码字典维护配置

背景信息

弱密码是指简单的，容易被猜测或在短时间内就可以被暴力破解的密码。为了避免设置的密码过于简单而导致安全问题，设备提供弱密码字典维护的功能。用户可以提前设置不希望使用的弱密码字典并加载到设备上，后续在添加新用户或修改密码时，系统会禁止使用字典中的弱密码。

弱密码字典以文本的形式存储，仅支持txt格式，每行存储一个密码。弱密码字典pwd_dict.txt示例如下。

```
Abcd@123
Huawei@123
Aaabb@321
Raatr@321
```

当加载了弱密码字典后，会对ZTP开局配置、登录设备命令行界面、配置文件管理、SNMP配置、AAA配置、系统主密钥配置中的密码设置造成影响，详细信息请参见相应特性的配置的注意事项和相关命令参考。

License 依赖

弱密码字典维护无需License许可即可使用。

硬件依赖

所有产品均支持弱密码字典维护功能。

特性限制

弱密码字典文件内容约束：

- 弱密码文件大小限制为1MB。
- 每条弱密码最大长度是128。
- 设备上加载的弱密码最大规格是1000条。

操作步骤

- 加载弱密码字典。
  load security weak-password-dictionary *filePath*

在加载之前，需要按格式制作txt格式的弱密码字典，并上传到设备上。

- 卸载弱密码字典。
  ```
  unload security weak-password-dictionary
  ```

----结束

检查配置结果

执行命令**display security weak-password-dictionary**，查看设备上禁止使用的弱密码。

