目 录

1 对象策略

1.1 对象策略简介

对象策略是一种安全策略，它基于全局进行配置，基于安全域间实例进行应用。安全域间实例用于指定安全策略所需检测报文流的源安全域和目的安全域，即首个报文要进入的安全域和要离开的安全域。在安全域间实例上应用对象策略可实现对报文流的检查，并根据检查结果允许或拒绝其通过。对象策略通过配置对象策略规则实现。

说明

有关安全域间实例和安全域的详细介绍和配置，请参见“基础配置指导”中的“安全域”。

1.1.1 对象策略规则

一个对象策略中可以包含多条用于识别报文流的规则，我们称之为对象策略规则。这里的规则是指通过指定对象组来描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、服务类型等。设备依照这些规则识别出特定的报文，并根据预先设定的策略对其进行处理。

1. 对象策略规则的编号

一个对象策略中可包含多条规则，每条规则都拥有唯一的编号以便区分，此编号在创建规则时由用户手工指定或由系统自动分配。在自动分配编号时，系统会将对应对象策略中已使用的最大编号加一作为新的编号，若新编号超出了编号上限（65534），则选择当前未使用的最小编号作为新的编号。

2. 对象策略规则的匹配顺序

当一个对象策略中包含多条规则时，报文会按照一定的顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。对象策略规则的匹配顺序与规则的创建顺序有关，先创建的规则优先进行匹配。对象策略规则的显示顺序与匹配顺序一致，即按照对象策略视图下通过 **display this** 命令显示的顺序，从上到下依次匹配。同时，对象策略支持通过命令移动规则位置来调整规则的匹配顺序。

3. 对象策略规则的描述

在一个对象策略中用户可以创建多条规则，为了方便标识这些规则的用途，用户可以为每条规则添加描述信息对单条规则进行标识。

1.2 配置对象策略

1.2.1 配置任务简介

表1-1 配置任务简介

配置任务	说明	详细配置
创建对象策略	必选	1.2.3
配置对象策略规则	必选	1.2.4

配置任务	说明	详细配置
安全域间实例应用对象策略	必选	1.2.5
移动对象策略规则	可选	1.2.6
使能对象策略加速功能	可选	1.2.7

1.2.2 配置准备

在配置对象策略规则之前，需完成以下任务：

- 配置时间段（请参见“ACL 和 QoS 配置指导/ACL”）
- 配置 IP 地址对象和服务对象（请参见“安全配置指导/对象组”）

1.2.3 创建对象策略

表1-2 创建 IPV4 对象策略

操作	命令	说明
进入系统视图	**system-view**	-
创建一个IPv4对象策略	**object-policy ip** object-policy-name	缺省情况下，不存在任何IPv4对象策略
（可选）配置对象策略的描述信息	**description** *text*	缺省情况下，对象策略没有任何描述信息

1.2.4 配置对象策略规则

IPv4 对象策略规则可以指定引用的对象组，包括以下几种：

- 源 IP 地址对象组：用于与报文的源 IP 地址进行匹配。
- 目的 IP 地址对象组：用于与报文的目的 IP 地址进行匹配。
- 服务对象组：用于与报文携带的服务类型进行匹配。
- VRF：用于与报文的 VRF 进行匹配。

需要注意的是，如果配置对象策略规则时指定引用对象组，若该对象组不存在，则该规则将不匹配任何报文。如果配置对象策略规则时不指定引用的对象组，则该规则将匹配任意报文。

说明

有关这些对象组的详细介绍和配置，请参见“基础配置指导”中的“对象组”。

表1-3 配置对象策略规则

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建IPv4对象策略，并进入其视图	**object-policy ip** *object-policy-name*	-
配置对象策略规则	**rule** [*rule-id*] { **drop** | **pass** } [[**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，不存在任何规则
（可选）配置规则的描述信息	**rule** *rule-id* **comment** *text*	缺省情况下，规则没有任何描述信息

1.2.5 安全域间实例应用对象策略

安全域间实例上同种类型的对象策略只能应用一个，即只能同时应用一个 IPv4 对象策略。如果安全域间实例已应用同种类型的其他对象策略，则会配置失败。若要应用新的对象策略，需要先将已经应用的对象策略删掉。

表1-4 安全域间实例应用对象策略

操作	命令	说明
进入系统视图	**system-view**	-
创建源安全域和目的安全域	**security-zone name** *zone-name*	缺省情况下，不存在任何安全域 运行两次该命令分别创建源安全域和目的安全域
创建安全域间实例，并进入安全域间实例视图	**zone-pair security souce** *souce-zone-name* **destination** *destination-zone-name*	缺省情况下，不存在任何安全域间实例
应用对象策略	**object-policy apply ip** *object-policy-name*	缺省情况下，安全域间实例内不应用任何对象策略规则

1.2.6 移动对象策略规则

由于对象策略规则是按照配置先后顺序进行匹配的，因此为了使用户能够灵活调整规则的匹配顺序，可通过本配置来移动对象策略规则的位置。

表1-5 移动对象策略规则

操作		命令	说明
进入系统视图		**system-view**	-
创建对象策略，并进入其视图	进入IPv4对象策略视图	**object-policy ip** *object-policy-name*	-
移动对象策略规则		**move rule** *rule-id* **before** *insert-rule-id*	-

1.2.7 使能对象策略加速功能

在对基于会话的业务报文（如 NAT、ASPF 等）进行规则匹配时，通常只对首个报文进行匹配以加快报文的处理速度，但这有时并不足以解决报文匹配的效率问题。譬如，当有大量用户同时与设备新建连接时，需要对每个新建连接都进行规则匹配，如果对象策略内包含有大量规则，那么这个匹配过程将很长，这会导致用户建立连接时间超长，从而影响设备新建连接的性能。

对象策略加速功能则可以解决上述问题，当对包含大量规则的对象策略使能了加速功能之后，其规则匹配速度将大大提高，从而提高了设备的转发性能以及新建连接的性能。

表1-6 使能对象策略加速功能

操作		命令	说明
进入系统视图		**system-view**	-
创建对象策略，并进入其视图	进入IPv4对象策略视图	**object-policy ip** *object-policy-name*	-
使能加速功能		**accelerate**	缺省情况下，所有对象策略的加速功能均处于关闭状态

1.3 对象策略显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示对象策略的配置信息，通过查看显示信息验证配置的效果。

表1-7 对象策略显示和维护

配置	命令
显示对象策略的加速状态	**display object-policy accelerate** { **summary ip** | **verbose** { **ip** *object-policy-name* } }
显示IPv4对象策略的配置信息	**display object-policy ip** [*object-policy-name*]
显示指定安全域间实例应用对象策略的配置信息。	**display object-policy zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]
显示指定安全域间实例的统计信息。	**display object-policy statistics zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [**ip**]
清除对象策略在安全域间实例中的统计信息	**reset object-policy statistics** [**zone-pair security source** *source-zone-name* **destination** *destination-zone-name*] [**ip**]